F-NS100-9M 系列
三层网管型工业以太网交换机
使用手册

文档版本：01

发布日期：2025-08-28

厦门四信智慧电力科技有限公司

总部地址：厦门集美区软件园三期诚毅大街 370 号

A06 栋 11 层

客服电话：400-8838-199

官方网站：http://www.four-faith.net

1 前　言

交换机使用手册介绍了本交换机：

- 产品特性
- 网络管理方法
- 网络管理相关原理概述


说明

本手册的截图参考型号为 24 路千兆 PoE+4 路万兆 SFP+，该系列其它型号产品除支持的电源和端口的数量与类型有差异外，界面功能和界面操作相同。

读者对象

本手册主要适用于以下工程师：

- 负责网络配置和维护的网络管理员
- 现场技术支持与维护人员
- 网络工程师

端口约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

文本格式约定

格式	说明
“”	带“”的文字代表界面词。如：“端口号”。
>	多级路径用“>”隔开。如打开本地连接路径描述：打开“控制面板 > 网络连接 > 本地连接”。
浅蓝色字体	代表单击可实现超链接的文字。字体颜色如：“浅蓝色”。

格式	说明
关于本章	在“关于本章”小节中，提供本章各小节的链接，以及本章对应的原理/操作章节的链接。

图标约定

格式	说明
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作，或使用设备的技巧、小窍门。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。

按钮操作约定

格式	说明
	网页右上角有退出登录按钮，单击后网页退回登录页面。
	网页右上角有端口按钮，单击或按 F2 键可查看端口状态，按 F2 或 Esc 键可关闭端口状态页面。
	网页右上角有重启按钮，单击后弹出重启确认框，确认后设备将重启。
	网页右上角有存盘按钮，单击可保存当前设备配置。对设备进行设置后，存盘图标会闪烁以提醒用户保存配置，避免因重启等操作而丢失未保存的配置信息。
	单击添加按钮添加一行配置，注意重复配置可能会出现数据覆盖。
	勾选要删除的行，再单击删除按钮删除该行配置。
	勾选要配置的行，再单击配置按钮，进入配置页面。
	单击功能状态按钮，可以切换功能状态，  表示开启，  表示关闭。

格式	说明
设置	单击设置按钮，提交当前配置。
清除	单击清除按钮，清除当前页面的信息。
刷新	单击刷新按钮，刷新当前页面的信息。

修改记录

版本号	修订日期	修订说明
01	2024-08-02	产品发布
02	2024-12-02	产品增加 PoE 型号

目　录

1 登录 WEB 界面

1.1 WEB 浏览的系统需求

使用该设备，系统应该满足如下条件。

硬件与软件	系统需求
CPU	奔腾 586 以上
内存	128MB 以上
分辨率	1024x768 以上
颜色	256 色以上
浏览器	Internet Explorer 9.0 以上
操作系统	Windows 7/8/10 以上

1.2 设置 PC 的 IP 地址

设备的缺省管理 IP 地址如下：

IP 设置	缺省值
IP 地址	192.168.1.254
子网掩码	255.255.255.0

通过 WEB 来配置设备时：

- 进行远程配置前，请确认计算机和设备之间路由可达。
- 进行本地配置前，请确认计算机的IP地址与设备在同一子网中。

  说明：

  对设备进行首次配置，如果是本地配置方式，请先确认当前 PC 的网段是 1。

例如：假设当前 PC 的 IP 地址是 192.168.5.60，现将 IP 地址的网段“5”修改为“1”。

操作步骤

修改步骤如下：

步骤 1 打开“控制面板 > 网络连接 > 本地连接 > 属性 > Internet 协议版本 4（TCP/IPv4）> 属性”。

步骤 2 将图中红框选定的“5”改为“1”。

步骤 3 单击“确定”，修改成功。

步骤 4 结束。

1.3 登录 WEB 配置界面

操作步骤

登录 WEB 配置界面的操作步骤如下：

步骤 1 运行计算机浏览器。

步骤 2 在浏览器的地址栏中输入设备的地址“http://192.168.1.254”。

步骤 3 单击回车键。

步骤 4 弹出如下图所示对话框，在登录窗口中输入用户名和密码。

说明：

- 设备默认的用户名和密码均为“admin123”，请在输入时严格区分大小写。
- 默认用户具有管理员权限。
- 当用户长时间没有操作 Web 网管配置页面时，系统超时将退出本次登录，并返回到 Web 登录页面；缺省情况下，Web 页面登录的超时时间为 15 分钟。
- 当用户连续密码登录错误达到限制次数（默认为 5 次），在后续的时间（默认 10 分钟）内，该用户将被限制登录。

步骤 5 单击“登录”。

步骤 6 结束。

成功登录后，可以根据需要配置 WEB 界面相关参数及信息。

2 系统信息

功能说明

查看端口状态如端口类型和连接状态。

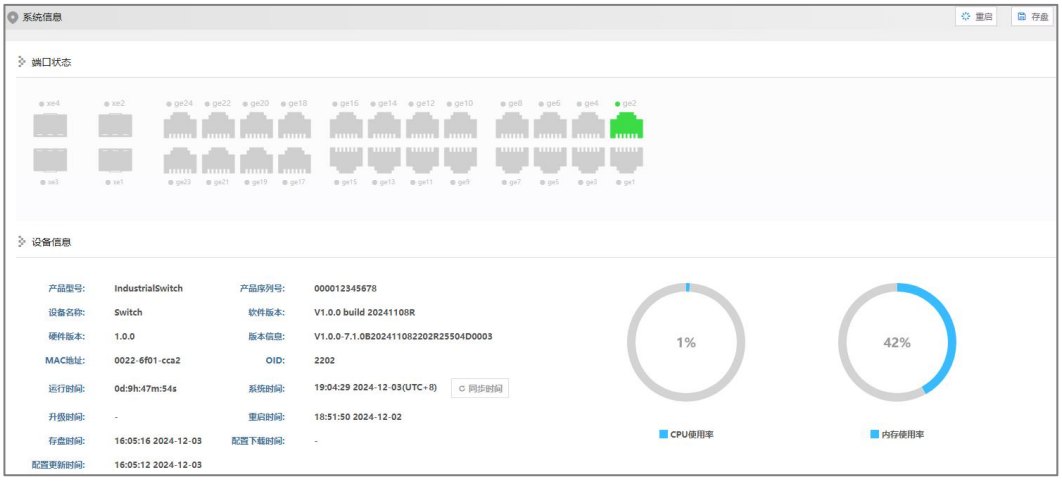
查看设备信息如产品型号、软硬件版本等。

操作路径

在导航栏打开：“系统信息”。

界面说明

系统信息界面如下所示：



系统信息界面主要元素配置说明：

界面元素	说明
端口状态	显示设备的端口图标和端口的连接状态。 •  电口图标，高亮表示端口已连接。 • 电口图标，灰化表示端口未连接或禁用。

界面元素	说明
	•  光口图标，高亮表示端口已连接。 • 光口图标，灰化表示端口未连接或禁用。
设备信息	设备软件、硬件和运行的基本信息。 • 产品型号 • 设备名称 • 硬件版本 • MAC 地址 • 系统时间 • 重启时间 • 产品序列号 • 软件版本 • 版本信息 • 运行时间 • 升级时间 • 存盘时间 • 配置下载时间 • 配置更新时间 • CPU 利用率 • 内存利用率

3 登录配置

3.1 IP 地址

3.1.1 IPv4

功能说明

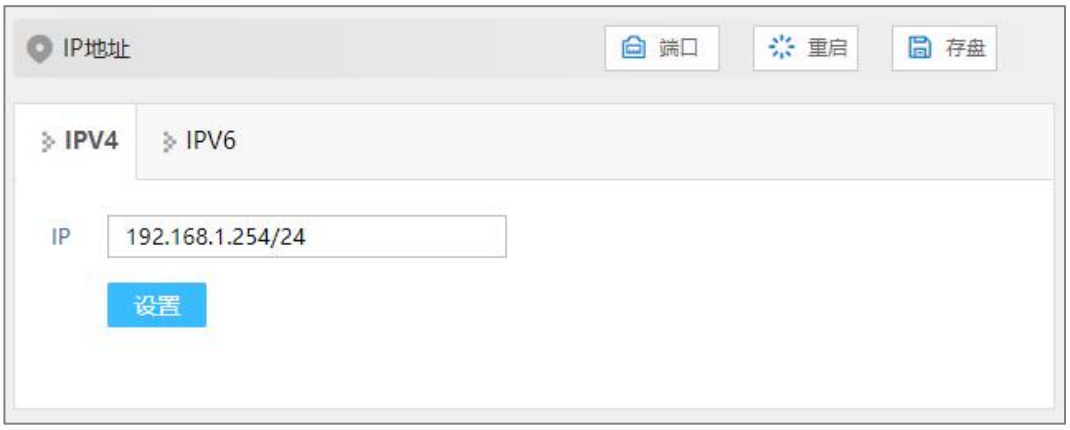
配置 vlanif1 接口的主 IPv4 地址。

操作路径

按顺序依次打开：“登录配置 > IP 地址 > IPV4”。

界面说明

IPV4 界面如下所示：



IPV4 界面主要元素配置说明：

界面元素	说明
IP	设备 vlanif1 接口的 IPv4 地址与子网掩码，默认 IP 为 192.168.1.254/24。 说明：

界面元素	说明
	修改设备的 IP 后，需重新输入相应的 IP 地址访问 WEB 界面。

3.1.2 IPv6

功能说明

添加或删除 vlanif1 接口的 IPv6 地址。

IPv6 地址总长度为 128 比特，通常分为 8 组，每组为 4 个十六进制数的形式，每组十六进制数间用冒号分隔。为了书写方便，IPv6 还提供了压缩格式，具体压缩规则为：

- 每组中的前导“0”都可以省略。
- 地址中包含的连续两个或多个均为0的组，可以用双冒号“::”来代替。

操作路径

按顺序依次打开：“登录配置 > IP 地址 > IPV6”。

界面说明

IPV6 界面如下所示：

IPV6 界面主要元素配置说明：

界面元素	说明
IPV6	设备 vlanif1 接口的 IPv6 地址与前缀长度。

3.2 用户

功能说明

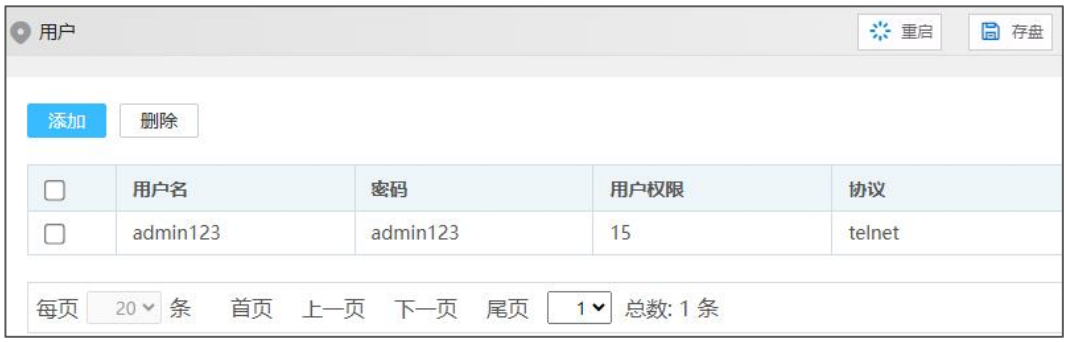
添加和删除用户，用户需要通过用户名、密码的登录方式访问设备，初始用户名和密码均为：admin123。

操作路径

按顺序依次打开：“登录配置 > 用户”。

界面说明

用户界面如下所示：



用户界面主要元素配置说明：

界面元素	说明
用户名	访问者的标识。 说明： • 用户名支持 1-16 位有效字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。 • 用户名不支持敏感字符，如 root、daemon、bin、sys、sync、mail、proxy、www-data、backup、operator、haldaemon、dbus、ftp、nobody、sshd、default 等。
密码	访问者使用的密码。 说明： • 密码支持 8-16 位有效字符，由大写字母、小写字母、数字、特殊字符（~!@#$%_-.）中两种及以上混合组成。 • 密码有效期默认为 90 天，密码过期后需重新修改密码。
用户权限	访问者的权限为 0-15，支持 16 个优先级，分成四大类。 • 0：参观级别；只能查看设备的系统信息、IP 地址、日志信息，进行网络诊断（Ping、Traceroute）操作。 • 1：查看级别；可以查看设备的配置信息，但不能修改设备的配置。 • 2：配置级别；既可以查看设备的配置信息，也可以配置设备的部分功能参数，但不能管理设备。

界面元素	说明
	• 3-15：管理级别；拥有设备所有权限，可以下载、上传、重启、修改设备信息等操作。 注意： • 用户可以查看、删除或添加优先级不超过自身的其他用户。 • 若添加的用户名已存在，则原有的用户信息会被覆盖。
协议	提供用户远程登录的协议，可选项如下： • Telnet • SSH

3.3 协议授权

功能说明

配置设备 TELNET 服务和 SSH 服务。

通过 TELNET 协议和 SSH2.0 协议可以访问设备的 CLI 界面。TELNET 传输过程采用 TCP 协议进行明文传输，而 SSH（Secure Shell）协议提供安全的远程登录，保证了数据的安全传输。

操作路径

按顺序依次打开：“登录配置 > 协议授权”。

界面说明

协议授权界面如下所示：

协议授权界面主要元素配置说明：

界面元素	说明
Telnet 使能开关	TELNET 服务使能开关按钮，默认为开启。
SSH 使能开关	SSH 服务使能开关按钮，默认为关闭。

4 端口配置

4.1 端口设置

功能说明

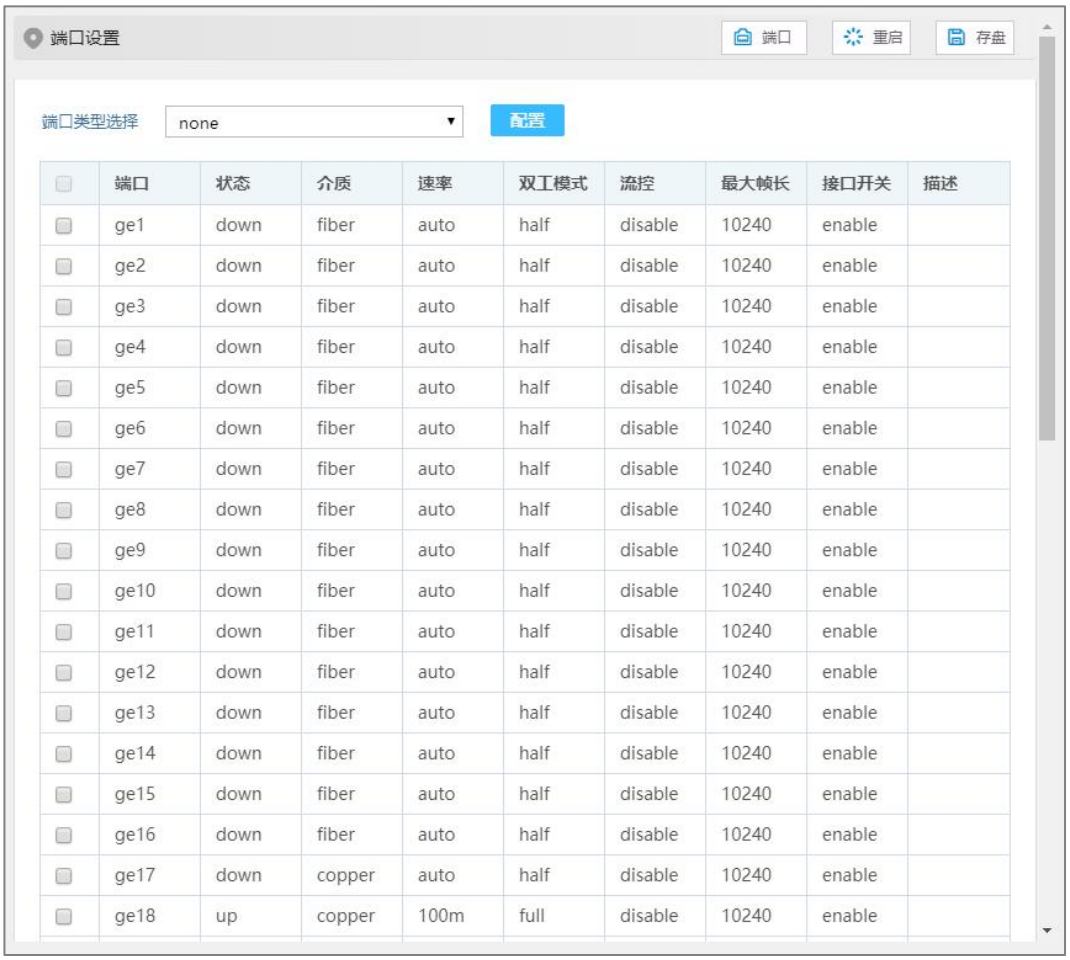
单个或批量设置端口参数。

操作路径

按顺序依次打开：“端口配置 > 端口设置”。

界面说明

端口设置界面如下所示：



端口	状态	介质	速率	双工模式	流控	最大帧长	接口开关	描述
ge1	down	fiber	auto	half	disable	10240	enable	
ge2	down	fiber	auto	half	disable	10240	enable	
ge3	down	fiber	auto	half	disable	10240	enable	
ge4	down	fiber	auto	half	disable	10240	enable	
ge5	down	fiber	auto	half	disable	10240	enable	
ge6	down	fiber	auto	half	disable	10240	enable	
ge7	down	fiber	auto	half	disable	10240	enable	
ge8	down	fiber	auto	half	disable	10240	enable	
ge9	down	fiber	auto	half	disable	10240	enable	
ge10	down	fiber	auto	half	disable	10240	enable	
ge11	down	fiber	auto	half	disable	10240	enable	
ge12	down	fiber	auto	half	disable	10240	enable	
ge13	down	fiber	auto	half	disable	10240	enable	
ge14	down	fiber	auto	half	disable	10240	enable	
ge15	down	fiber	auto	half	disable	10240	enable	
ge16	down	fiber	auto	half	disable	10240	enable	
ge17	down	copper	auto	half	disable	10240	enable	
ge18	up	copper	100m	full	disable	10240	enable	

端口设置界面主要元素配置说明：

界面元素	说明
端口类型选择	批量选择同类型端口进行配置，可选择如下： • none • fe：百兆端口 • ge：千兆端口 • xe：万兆端口 • sa：静态聚合组 • po：动态聚合组 说明： 端口类型以设备实际存在的端口为准。
端口	该设备以太网端口对应的端口名称。
状态	以太网端口的连接状态，显示状态如下： • down：表示该端口未连接 • up：表示该端口已连接
介质	以太网端口的连接类型，显示状态如下： • fiber：光口介质 • copper：电口介质

界面元素	说明
速率	默认为自适应模式，显示状态如下： • auto：自适应 • 10m：十兆 • 100m：百兆 • 1g：千兆 • 2500m：2.5G • 10g：万兆
双工模式	默认为自适应模式,，显示状态如下： • auto：自适应 • half：半双工 • full：全双工
流控	端口流量控制状态，显示状态如下： • disable：禁用 • both：开启端口发送与接收数据流控 • send on：开启端口发送数据流控 • send off：关闭端口发送数据流控 • receive on：开启端口接收数据流控 • receive off：关闭端口接收数据流控
最大帧长	以太网端口通过的最大以太网数据帧长，取值范围为 64-10240。
接口开关	启用或者禁用以太网端口。可选项如下： • enable：启用 • disable：禁用
描述	端口描述信息，支持 0-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。

4.2 链路聚合

4.2.1 链路聚合

功能说明

以太网链路聚合简称链路聚合，它通过将多条以太网物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽的目的。同时，这些捆绑在一起的链路通过相互间的动态备份，可以有效地提高链路的可靠性。

基于 IEEE802.3ad 标准的 LACP（Link Aggregation Control Protocol，链路聚合控制协议）协议是一种实现链路动态聚合的协议，运行该协议的设备之间通过互发 LACPDU

（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）来交互链路聚合的相关信息。

根据成员端口上是否启用了 LACP 协议，可以将链路聚合分为静态聚合和动态聚合两种模式。

操作路径

按顺序依次打开：“端口配置 > 链路聚合 > 链路聚合”。

界面说明

链路聚合界面如下所示：

链路聚合界面主要元素配置说明：

界面元素	说明
Lacp 优先级	动态聚合系统优先级设置，设置范围 1-65535，默认为 32768。 说明： 系统 LACP 优先级值越小，优先级越高，则聚合链路两端选择系统优先级高的设备为活动接口。
工作模式	配置聚合组的负载均衡模式，可选项如下： • source-mac：负载均衡模式基于源 MAC • destination-mac：负载均衡模式基于目的 MAC • source-dest-ip：负载均衡模式基于源和目的 IP • source-dest-mac：负载均衡模式基于源和目的 MAC • source-dest-port：负载均衡模式基于源和目的 TCP/UDP 端口
聚合组名称	聚合组类型及 ID，sa 为静态聚合组，po 为动态聚合组，聚合组 ID 最大支持 12 组，每个组最多配置 8 个端口加入汇聚。
端口成员	参与该链路聚合组的端口成员。

界面说明：添加

链路聚合-添加界面如下所示：

链路聚合-添加界面主要元素配置说明：

界面元素	说明
组 ID	聚合组的 ID 号，最大支持 12 组。
类型	聚合组类型： • static：静态聚合 • dynamic：动态聚合
聚合模式	动态聚合组模式： • active：主动模式，在该模式下端口主动发起聚合协商过程。 • passive：被动模式，在该模式下端口被动接收聚合协商过程。 说明： 在 dynamic 类型下，显示此项配置。
端口	该聚合组内的端口成员，每个组最多配置 8 个端口加入汇聚。

4.2.2 聚合保护

功能说明

配置静态聚合保护。

操作路径

按顺序依次打开：“端口配置 > 链路聚合 > 聚合保护”。

界面说明

聚合保护界面如下所示：

聚合保护界面主要元素配置说明：

界面元素	说明
聚合组名称	在“链路聚合”中设置的静态聚合组名称。
接口开关	聚合组的启用状态。 • Enable • Disable
状态	聚合组端口的状态。 • Up：只要有端口成员处于 Up，则聚合组的状态为 Up； • Down：全部的端口成员均为 Down，则聚合组的状态为 Down。
端口成员	聚合组的端口成员。
聚合保护	聚合保护的启用状态。 • Enable • Disable
缺省 VLAN ID	聚合组端口所在 VLAN。
邻居	聚合组对端设备的 MAC 地址。 说明： 如果对端未连接设备，则 MAC 地址显示为 0000.0000.0000。
角色	在本设备和对端设备中选举得出的角色： • Master：MAC 地址小的被选举为 Master • Slave：MAC 地址大的被选举为 Slave
主端口	主设备的第二个 link 端口为主端口。
错误状态	聚合保护的错误信息提示：

界面元素	说明
	• 邻居超时 • loop：成环 • 链路错误（比如产生大量的错误帧）

4.3 端口限速

功能说明

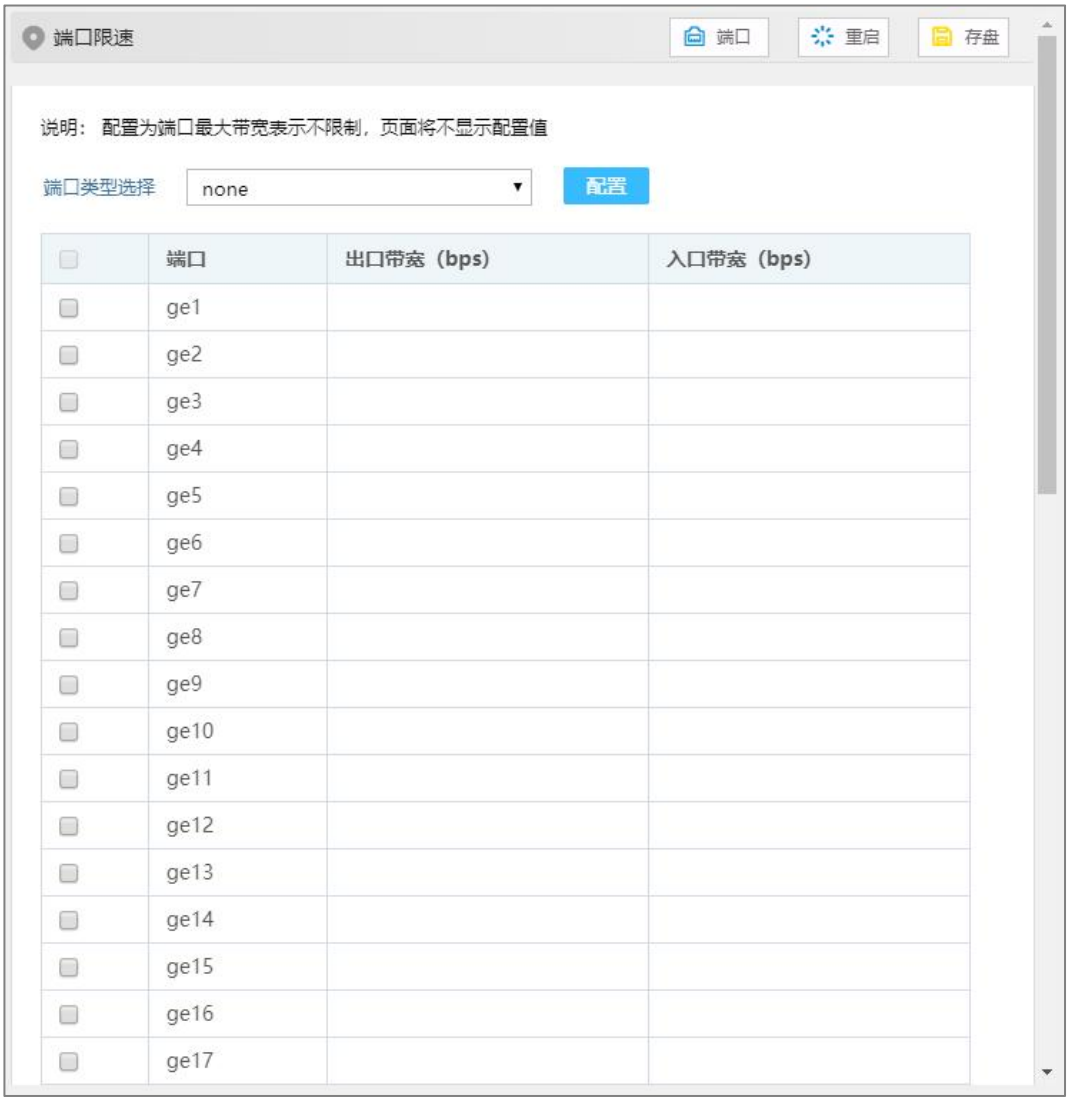
限制端口的出口带宽和入口带宽。

操作路径

按顺序依次打开：“端口配置 > 端口限速”。

界面说明

端口限速界面如下所示：



端口限速界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
出口带宽（bps）	端口对出口数据传输带宽的限制。
入口带宽（bps）	端口对入口数据传输带宽的限制。 说明： 配置带宽时，支持单位 K/M/G 选择。WEB 显示时，会根据输入值和单位，进行单位换算和取相近的数值。

说明

- 使用端口限速时，流控应该被启用，否则设备之间的速度将不再是平稳曲线；
- 使用端口限速时，不应该丢包除非流控被禁用。丢包的表象是传递速度忽快忽慢；
- 端口限速对网线质量要求较高，否则将出现大量的冲突包和破碎的包。

4.4 风暴抑制

功能说明

配置端口允许通过的最大广播、组播或未知单播报文流量。

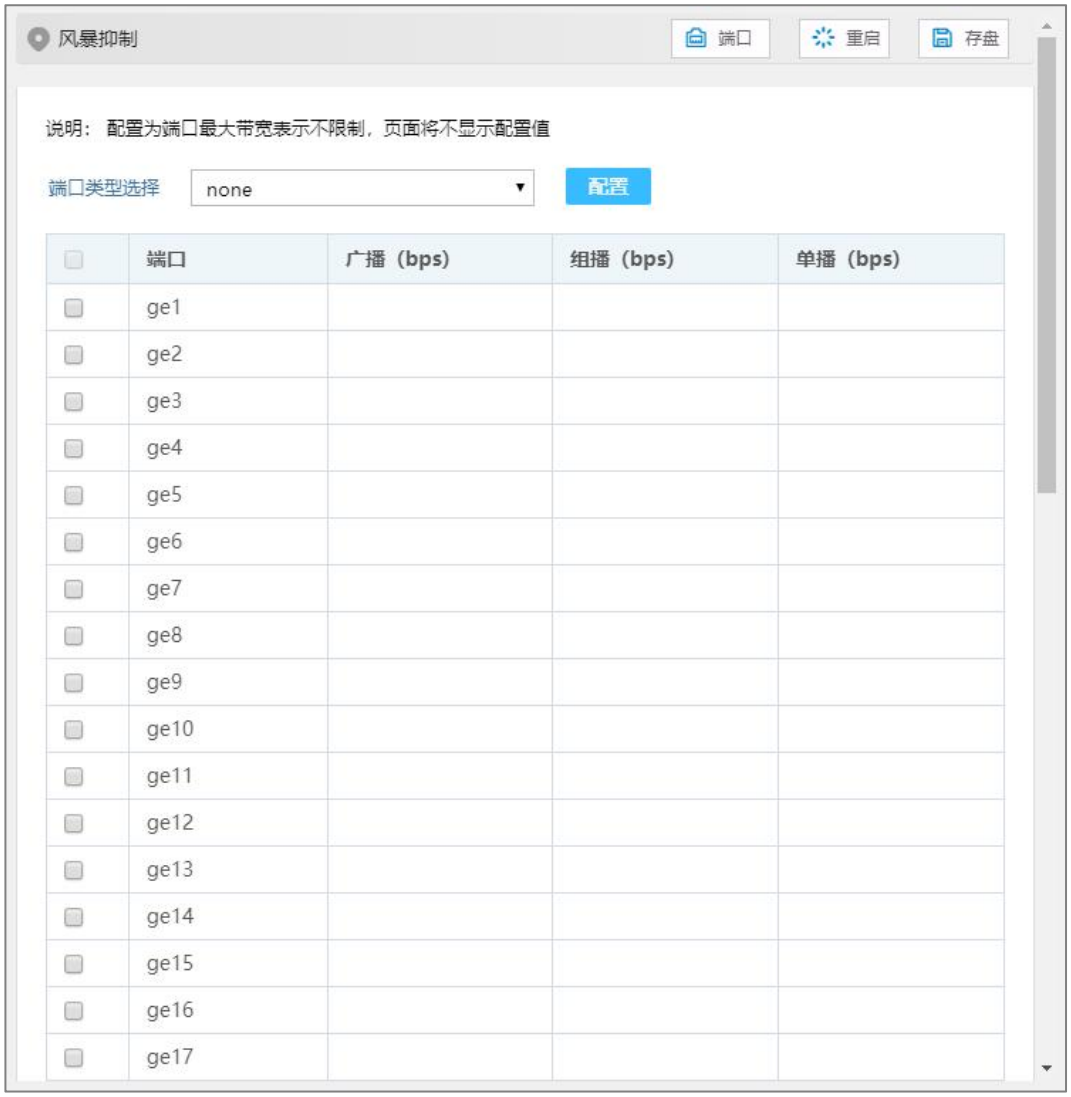
当各端口上的广播、未知组播或未知单播流量之和达到用户设置的值后，系统将丢弃超出广播、未知组播或未知单播流量限制的报文，从而使总体广播、未知组播或未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

操作路径

按顺序依次打开：“端口配置 > 风暴抑制”。

界面说明

风暴抑制界面如下所示：



风暴抑制界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
广播（bps）	该端口对广播包传输速率的抑制。 说明： 广播包，即目的地址为 FF-FF-FF-FF-FF-FF 的数据帧。
组播（bps）	该端口对未知组播数据包传输速率的抑制。 说明： 组播包，即目的地址为 XX-XX-XX-XX-XX-XX 的数据帧，第二个 X 为奇数数字如：1、3、5、7、9、B、D、F，其他 X 表示任意数字。
单播（bps）	该端口对未知单播数据包传输速率的抑制。 说明： 未知单播包，即该数据帧的 MAC 地址不存在设备的 MAC 地址表中，需要向所有端口转发。

说明

单击“配置”按钮，配置速率时，支持单位 K/M/G 选择。WEB 显示时，会根据输入值和单位，进行单位换算和取相近的数值。

4.5 端口镜像

功能说明

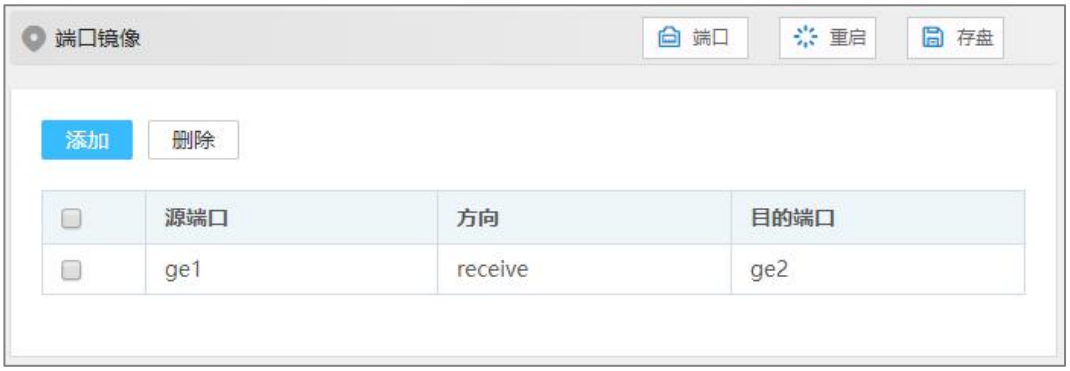
将源端口上的数据复制到指定的目的端口，对数据进行分析和监视。

操作路径

按顺序依次打开：“端口配置 > 端口镜像”。

界面说明

端口镜像界面如下所示：



端口镜像界面主要元素配置说明：

界面元素	说明
源端口	数据源端口，可以是一个或者多个，设备将从这些端口采集指定方向的数据。
方向	源端口的数据方向，可选项如下： • transmit：源端口发送的报文会被镜像到目的端口。 • receive：源端口接收的报文会被镜像到目的端口。 • both：源端口接收和发送的报文被镜像到目的端口。
目的端口	设备镜像的目的端口，仅支持一个目的端口。

说明

- 该功能必须在正常使用中被关闭，否则所有基于端口的高级管理功能均无法使用，如 RSTP、IGMP Snooping 等；

- 镜像功能只处理 FCS 正常的包，不能处理各种错误的数据帧。

4.6 端口隔离

功能说明

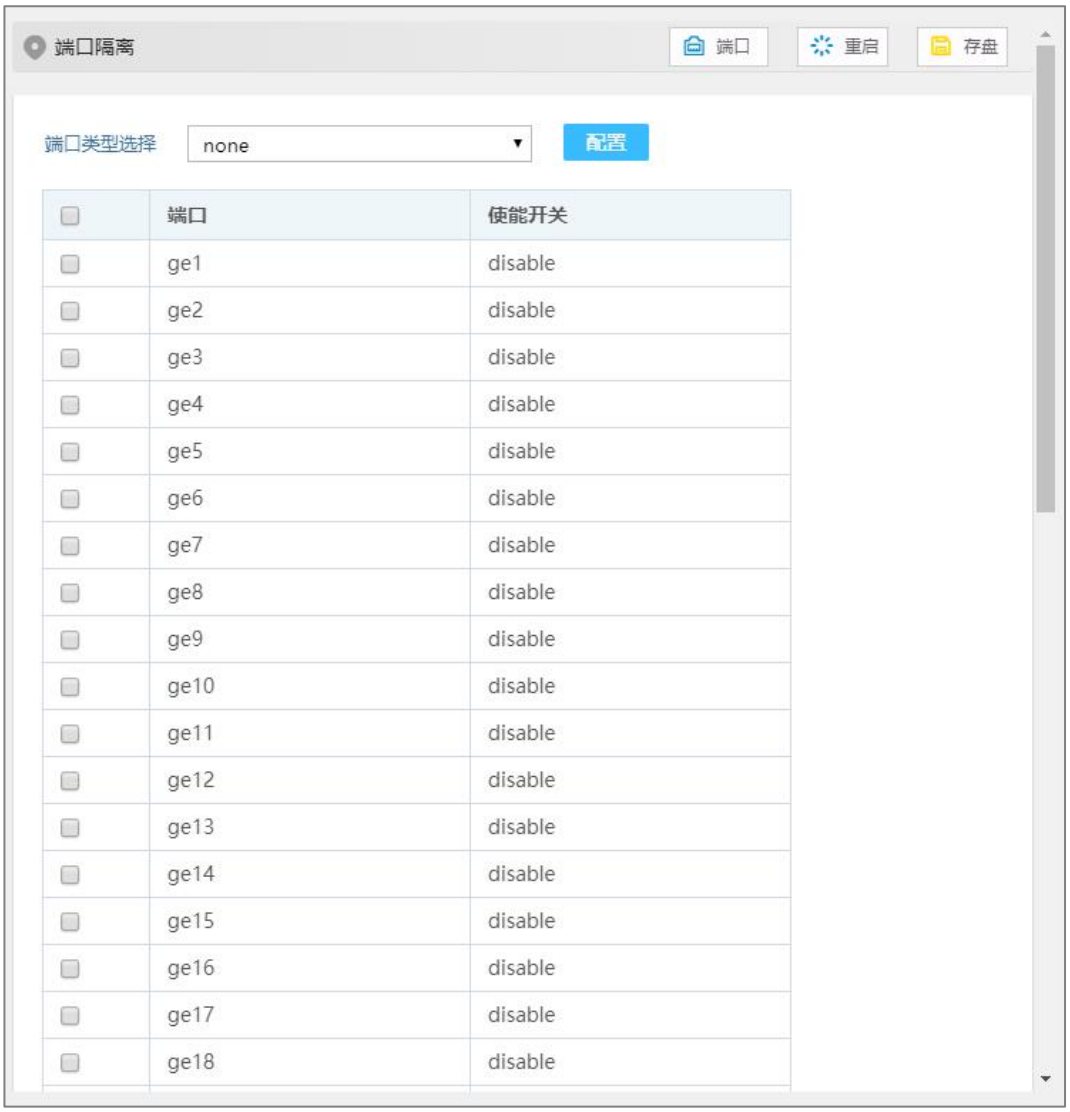
端口隔离是为了实现报文之间的二层隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

操作路径

按顺序依次打开：“端口配置 > 端口隔离”。

界面说明

端口隔离界面如下所示：



端口隔离界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
使能开关	端口隔离使能状态，可显示如下： • disable • enable

4.7 端口统计

4.7.1 端口统计-总览

功能说明

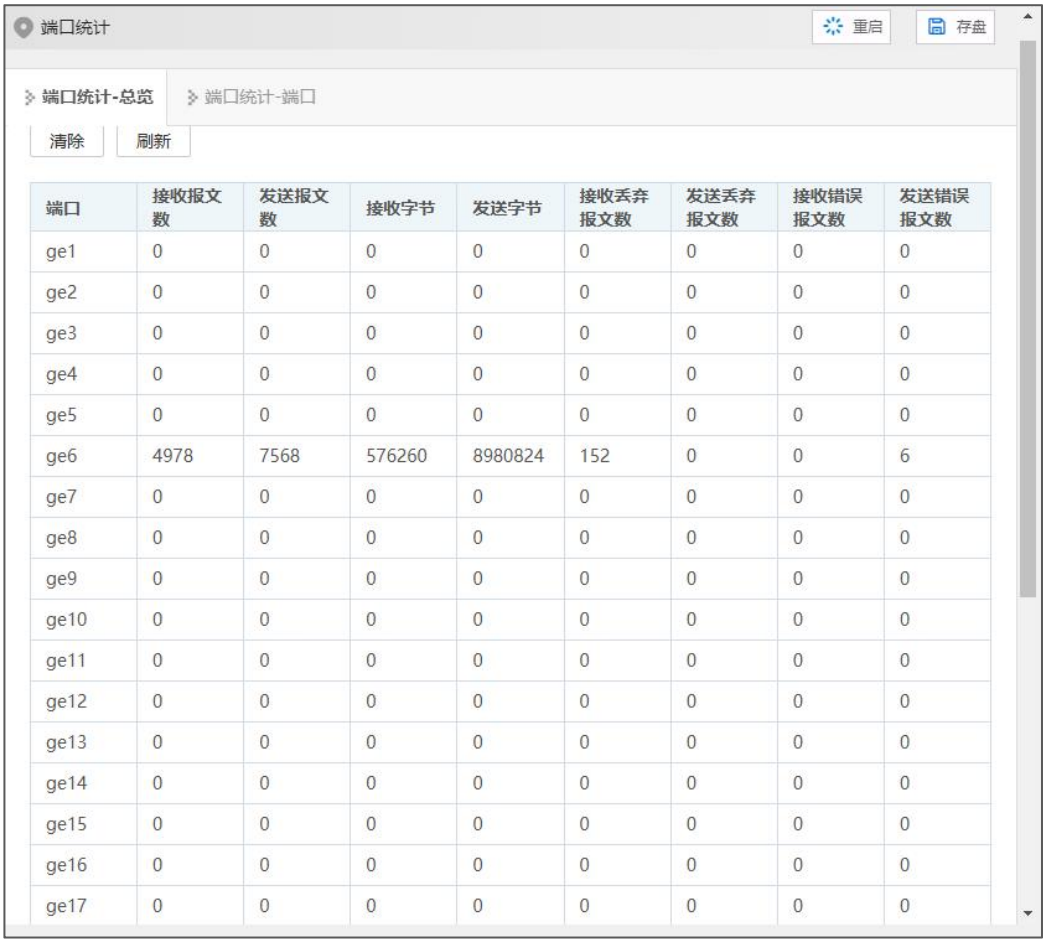
查看各端口发送和接收的报文数、字节数、丢弃报文数、错误报文数。

操作路径

按顺序依次打开：“端口配置 > 端口统计 > 端口统计-总览”。

界面说明

端口统计-总览界面如下所示：



端口	接收报文数	发送报文数	接收字节	发送字节	接收丢弃报文数	发送丢弃报文数	接收错误报文数	发送错误报文数
ge1	0	0	0	0	0	0	0	0
ge2	0	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0	0
ge5	0	0	0	0	0	0	0	0
ge6	4978	7568	576260	8980824	152	0	0	6
ge7	0	0	0	0	0	0	0	0
ge8	0	0	0	0	0	0	0	0
ge9	0	0	0	0	0	0	0	0
ge10	0	0	0	0	0	0	0	0
ge11	0	0	0	0	0	0	0	0
ge12	0	0	0	0	0	0	0	0
ge13	0	0	0	0	0	0	0	0
ge14	0	0	0	0	0	0	0	0
ge15	0	0	0	0	0	0	0	0
ge16	0	0	0	0	0	0	0	0
ge17	0	0	0	0	0	0	0	0

4.7.2 端口统计-端口

功能说明

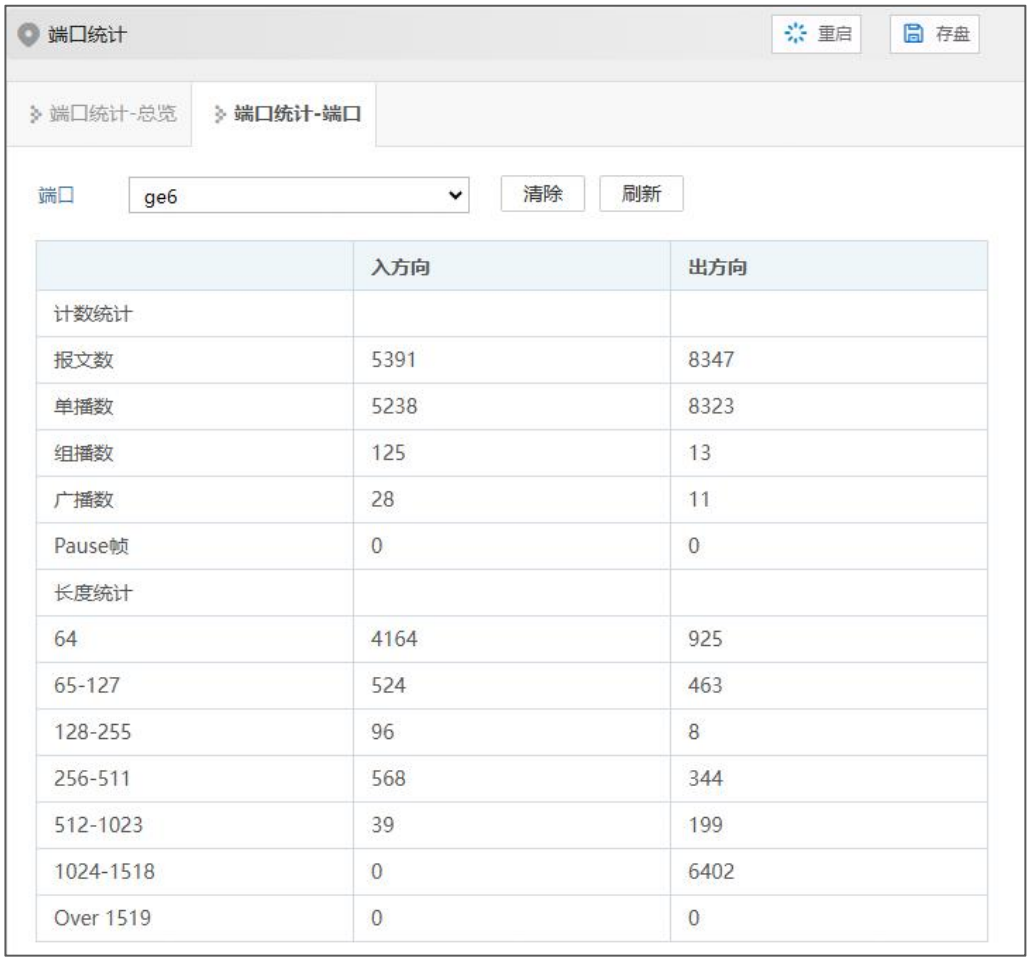
查看指定端口发送和接收的报文总数和报文字节数的分类统计。

操作路径

按顺序依次打开：“端口配置 > 端口统计 > 端口统计-端口”。

界面说明

端口统计-端口界面如下所示：



	入方向	出方向
计数统计		
报文数	5391	8347
单播数	5238	8323
组播数	125	13
广播数	28	11
Pause帧	0	0
长度统计		
64	4164	925
65-127	524	463
128-255	96	8
256-511	568	344
512-1023	39	199
1024-1518	0	6402
Over 1519	0	0

4.8 POE 管理

以太网供电 PoE（Power over Ethernet）是指通过以太网网络进行供电。PoE 是一种有线以太网供电技术，允许电功率通过传输数据的线路或空闲线路传输到终端设备。

PoE 供电系统包括：

- 供电设备PSE（Power-sourcing Equipment）：通过以太网给受电设备供电的PoE设备。
- 受电设备PD（Powered Device）：如无线AP（Access Point）、刷卡机、摄像头等受电方设备。
- PoE电源：PoE电源为整个PoE系统供电，PSE下接的PD数量受制于PoE电源的功率。

说明

只有带 PoE 接口的设备支持此功能，非 PoE 设备不显示此界面。

4.8.1 全局配置

功能说明

在“全局配置”页面，可以配置设备最大 PoE 输出功率。

操作路径

按顺序依次打开：“端口配置 > POE 管理 > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明（选定功率的复选框，单击“配置”按钮，可进行配置。）
PSE ID	当前设备 PSE 模块 ID 显示。
当前总功率	当前设备 PoE 输出总功率值显示，单位为 W。
最大功率	当前设备 PoE 输出最大功率限制值，单位为 W。

4.8.2 端口配置

功能说明

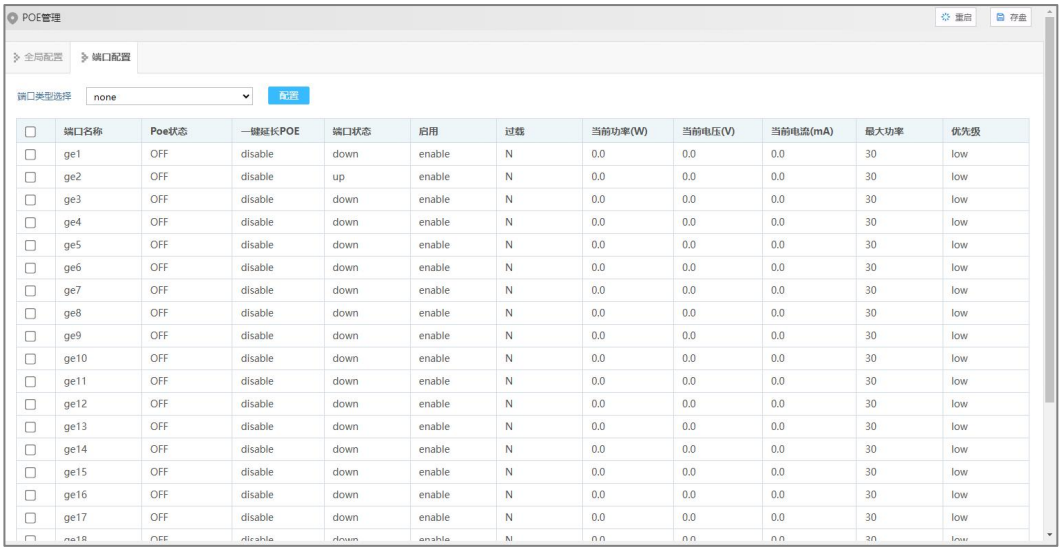
在“端口配置”页面，可以配置设备各 PoE 端口的使能、输出最大功率和供电优先级等。

操作路径

按顺序依次打开：“端口配置 > POE 管理 > 端口配置”。

界面说明

端口配置界面如下所示：



端口配置界面主要元素配置说明：

界面元素	说明（选定端口的复选框，单击“配置”按钮，可进行配置。）
端口名称	该设备 PoE 以太网端口对应的端口名称。
Poe 状态	当前设备端口 PoE 供电状态，显示状态如下： • ON：PoE 口对 PD 设备供电； • OFF：PoE 口未供电或 PD 设备未连接。
一键延长 POE	通过开启一键延长 PoE 设置，来延长 PoE 技术传输距离，显示状态如下： • disable：禁用； • enable：启用。
端口状态	以太网端口的连接状态，显示状态如下： • down：表示该端口未连接； • up：表示该端口已连接。
启用	端口使能复选框，勾选该复选框，PoE 端口使能；未勾选该复选框，PoE 端口禁用，无法使用。
过载	当前设备 PoE 端口过载状态，可显示如下： • Y：当前 PoE 端口输出功率大于最大功率。 • N：当前 PoE 端口输出功率小于或等于最大功率。
当前功率（W）	当前设备 PoE 端口输出功率值显示，单位 W。
当前电压（V）	当前设备 PoE 端口输出电压值显示，单位 V。
当前电流（mA）	当前设备 PoE 端口电流值显示，单位 mA。

界面元素	说明（选定端口的复选框，单击“配置”按钮，可进行配置。）
最大功率	当前设备 PoE 输出最大功率值配置，取值范围 0-30，单位为 W。
优先级	PoE 端口供电优先级配置，在总功率限制下端口功率分配优先级，优先级下拉列表可选项如下： • 高：高优先级； • 中：中等优先级； • 低：低优先级。 说明： 在交换机对外供电接近满负荷的情况下，优先对优先级为 High 的端口连接的 PD 设备进行供电；次之为优先级为 Medium 的端口连接的 PD 设备供电。

5 二层配置

5.1 VLAN

VLAN（Virtual Local Area Network），即虚拟局域网。VLAN 是一种将局域网（LAN）设备从逻辑上划分（注意，不是从物理上划分）成一个个网段（或者说是更小的局域网 LAN），从而实现虚拟工作组（单元）的数据交换技术。

VLAN 的好处主要有：

- 端口的分隔。即便在同一个交换机上，处于不同VLAN的端口也是不能通信的。这样一个物理的交换机可以当作多个逻辑的交换机使用。
- 网络的安全。不同VLAN不能直接通信，杜绝了广播信息的不安全性。
- 灵活的管理。更改用户所属的网络不必换端口和连线，只需更改软件配置。

也就是说处于同一个 VLAN 可以相互通信，处于不同的 VLAN 不能相互通信。一个 VLAN 用 VLAN ID 来标识，具有相同的 VLAN ID 就属于同一个 VLAN。

5.1.1 VLAN 配置

功能说明

创建 VLAN 和编辑 VLAN 描述。

操作路径

按顺序依次打开：“二层配置 > VLAN > VLAN 配置”。

界面说明

VLAN 配置界面如下所示：

VLAN 配置界面主要元素配置说明：

界面元素	说明
VLAN	VLAN ID 号，取值范围 1-4094。
Untagged 端口	Untag 端口成员，对发送的数据帧进行不带标记处理。
Tagged 端口	Tag 端口成员，对发送的数据帧进行带标记处理。
状态	VLAN 状态： • Static：静态 VLAN • Dynamic：动态 VLAN
描述	VLAN 描述信息，支持 0-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。

5.1.2 Access 配置

功能说明

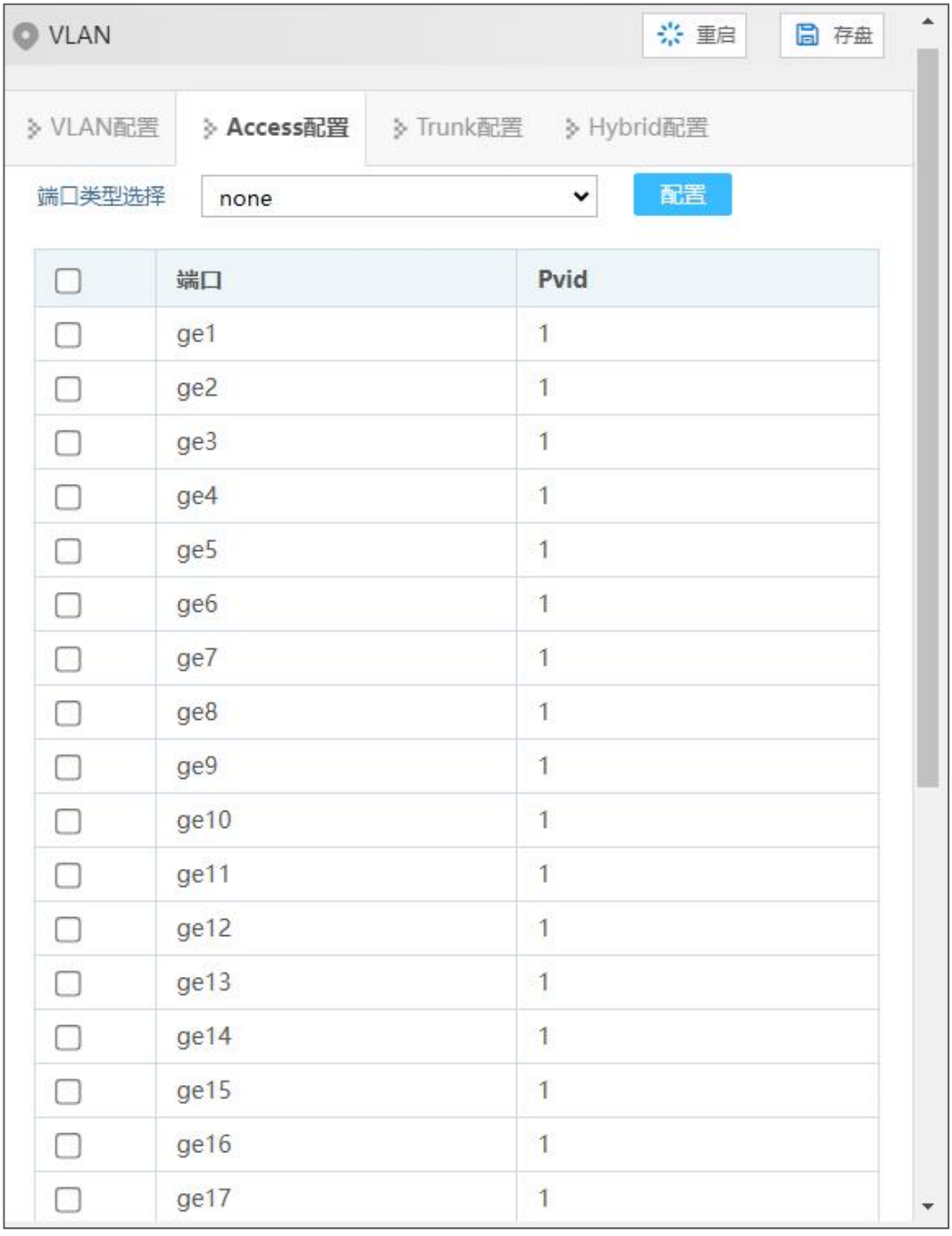
配置 Access 接口的 PVID（Port Default VLAN ID），或修改为 Trunk 接口。

操作路径

按顺序依次打开：“二层配置 > VLAN > Access 配置”。

界面说明

Access 配置界面如下所示：



Access 配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
PVID	Port Default Vlan ID，也就是端口的缺省 VLAN。默认为 1，取值范围：1-4094。 说明： 每个端口都有一个 PVID 属性，当端口收到 Untag 报文时，根据 PVID 为报文添加 Tag 标记。当端口发送数据报文的 Tag 标记与 PVID 相同，会将 Tag 标记去掉，然后再将报文发送出去。默认所有端口的 PVID 均为 1。

界面元素	说明
配置	勾选端口，单击“配置”按钮，可重新设置 PVID 和端口模式。 • Access：端口只能属于 1 个 VLAN（即缺省 VLAN），默认情况下交换机所有端口都为 Access 模式，并且 PVID 均为 1。 • Trunk：端口可以属于多个 VLAN，Trunk 端口可以允许多个 VLAN 的报文带 Tag 通过，但只允许一个 VLAN 的报文从该类接口上发出时不带 Tag（即剥除 Tag）。一般用于网络设备之间连接。

5.1.3 Trunk 配置

功能说明

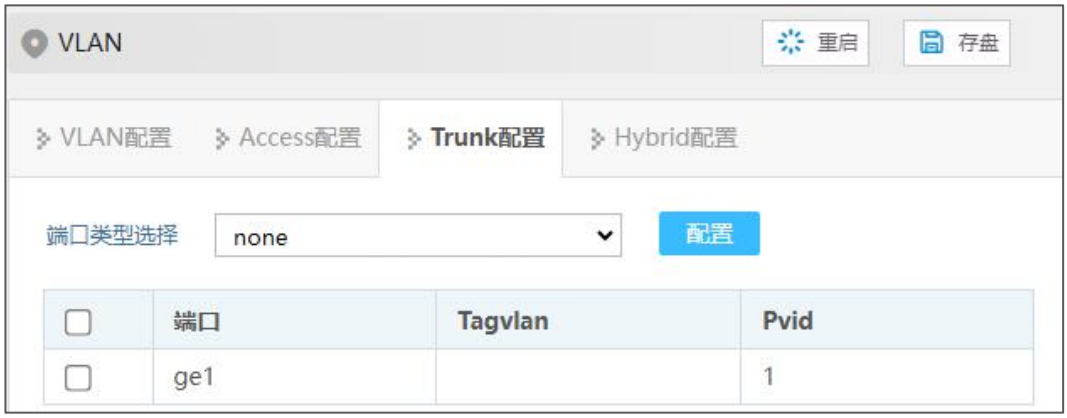
配置 Trunk 端口的 pvid 值与 tagvlan，或修改为 Access 接口。

操作路径

按顺序依次打开：“二层配置 > VLAN > Trunk 配置”。

界面说明

Trunk 配置界面如下所示：



Trunk 配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
Tagvlan	端口允许通过的 VLAN ID。
Pvid	Port Default Vlan ID，也就是端口的缺省 VLAN。默认为 1，取值范围：1-4094。
配置	勾选端口，单击“配置”按钮，可以配置端口所属的 VLAN 和 PVID，以及发送报文时对 PVID 的处理。

5.1.4 Hybrid 配置

功能说明

在“Hybrid 配置”页面，用户可以配置 Hybrid 的相关参数。

操作路径

按顺序依次打开：“二层配置 > VLAN 配置 > Hybrid 配置”。

界面说明

Hybrid 配置界面如下所示：

Hybrid 配置界面主要元素配置说明：

界面元素	说明
端口类型选择	通过下拉列表筛选要配置的端口。
配置	勾选或者筛选需要重新配置的条目，单击配置，可重新设置 pvid、tagvlan 和 untagvlan 的参数。
Pvid	VLAN ID 号，取值范围 1-4094。
Untagvlan	去标记的值，单独的一个数值或者范围(用"-"表示范围)。如：9 或者 10-15。
Tagvlan	带标记的值，单独的一个数值或者范围(用"-"表示范围)。如：9 或者 10-15。
模式设置	单击模式设置，可以将模式设置成 access 或 trunk。

端口对接收报文的处理

接口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理
Access	接收该报文，并打上缺省的	• 当 VLAN ID 与缺省 VLAN ID 相同时，

接口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理
	VLAN ID。	接收该报文。 • 当VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文。
Trunk Hybrid	接收该报文，并打上缺省的 VLAN ID。	• 当VLAN ID在接口允许通过的VLAN ID 列表里时，接收该报文。 • 当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。

端口对发送报文的处理

接口类型	发送帧处理过程
Access	先剥离报文的 PVID Tag，然后再发送。
Trunk	• 当 VLAN ID 与缺省 VLAN ID 相同，且是该接口允许通过的 VLAN ID 时，去掉 Tag，发送该报文。 • 当 VLAN ID 与缺省 VLAN ID 不同，且是该接口允许通过的 VLAN ID 时，保持原有 Tag，发送该报文。
Hybrid	当 VLAN ID 是该接口允许通过的 VLAN ID 时，发送该报文。可以设置发送时是否携带 Tag。

5.2 MAC

MAC（Media Access Control）地址是网络设备的硬件标识，交换机根据 MAC 地址进行报文转发。MAC 地址具有唯一性，这保证了报文的正确转发。每个交换机都维护着一张 MAC 地址表。在这张表中，MAC 地址和交换机的端口一一对应。当交换机收到数据帧时，根据 MAC 地址表来决定对该数据帧进行过滤还是转发到交换机的相应端口。MAC 地址表是交换机实现快速转发的基础和前提。

5.2.1 全局配置

功能说明

设置动态 MAC 地址的老化时间。

交换机中各端口具有自动学习地址的功能，通过端口发送和接收的帧的源地址（源 MAC 地址、交换机端口号）将存储到地址表中。老化时间是一个影响交换机学习进程的参数，默认为 300 秒。从一个地址记录加入地址表以后开始计时，如果在老化时间内各端口未收到源地址为该 MAC 地址的帧，那么，这些地址将从动态转发地址表（由源 MAC 地址、目的 MAC 地址和它们相对应的交换机的端口号）中被删除。

操作路径

按顺序依次打开：“二层配置 > MAC > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
老化使能	MAC 地址老化使能开关。
老化时间	MAC 地址的老化时间，单位秒，默认值为 300，取值范围 10-1000000。

5.2.2 静态单播 MAC

功能说明

源单播 MAC 地址绑定与过滤，不会老化。

操作路径

按顺序依次打开：“二层配置 > MAC > 静态单播 MAC”。

界面说明

静态单播 MAC 界面如下所示：

静态单播 MAC 界面主要元素配置说明：

界面元素	说明
MAC	接口绑定的单播 MAC 地址，例如 0001.0001.0001。
转发类型	MAC 转发类型，可显示如下： • Discard：丢弃 • Forward：转发
端口	绑定的端口号。
VLAN ID	该 MAC 地址发送的数据所属的 VLAN ID 号，例如 1-4094。 说明： 输入的 VLAN ID 是已存在的 ID。

说明

- 这个功能是一种安全机制，请谨慎确认设置，否则，将导致部分设备无法通信；
- 请不要使用多播地址作为输入地址；
- 请不要输入保留的 MAC 地址，如本机的 MAC 地址。

5.2.3 静态组播 MAC

功能说明

源组播 MAC 地址绑定，不会老化。

操作路径

按顺序依次打开：“二层配置 > MAC > 静态组播 MAC”。

界面说明

静态组播 MAC 界面如下所示：

静态组播 MAC 界面主要元素配置说明：

界面元素	说明
MAC	接口绑定的组播 MAC 地址，例如 0100.5e01.0001。
接口	绑定的端口号。
VLAN ID	该 MAC 地址发送的数据所属的 VLAN ID 号，例如 1-4094。 说明： 输入的 VLAN ID 是已存在的 ID。

5.2.4 MAC 信息

功能说明

查看 MAC 地址表信息。

操作路径

按顺序依次打开：“二层配置 > MAC > MAC 信息”。

界面说明

MAC 信息界面如下所示：

MAC 信息界面主要元素配置说明：

界面元素	说明
过滤模式	MAC 过滤模式选择下拉列表，筛选指定类型 MAC 地址列表显示，可选项如下： • 全部 • 动态单播 • 动态组播 • 静态组播 • 静态单播
MAC	设备学习到的动态 MAC 地址或用户配置的静态 MAC 地址信息。
转发类型	MAC 转发类型，显示如下： • Discard：丢弃 • Forward：转发
端口	该 MAC 地址对应的端口号。
VLAN ID	该 MAC 地址发送的数据所属的 VLAN ID 号。
类型	MAC 地址类型，显示如下： • dynamic：动态 • static：静态

5.2.5 MAC 学习

功能说明

MAC 学习的主要功能是限制端口的 MAC 学习数量。当交换机的 MAC 地址表满后，就无法学习到新的 MAC 地址，此时如果出现大量伪造的不同源 MAC 地址的报文发送到

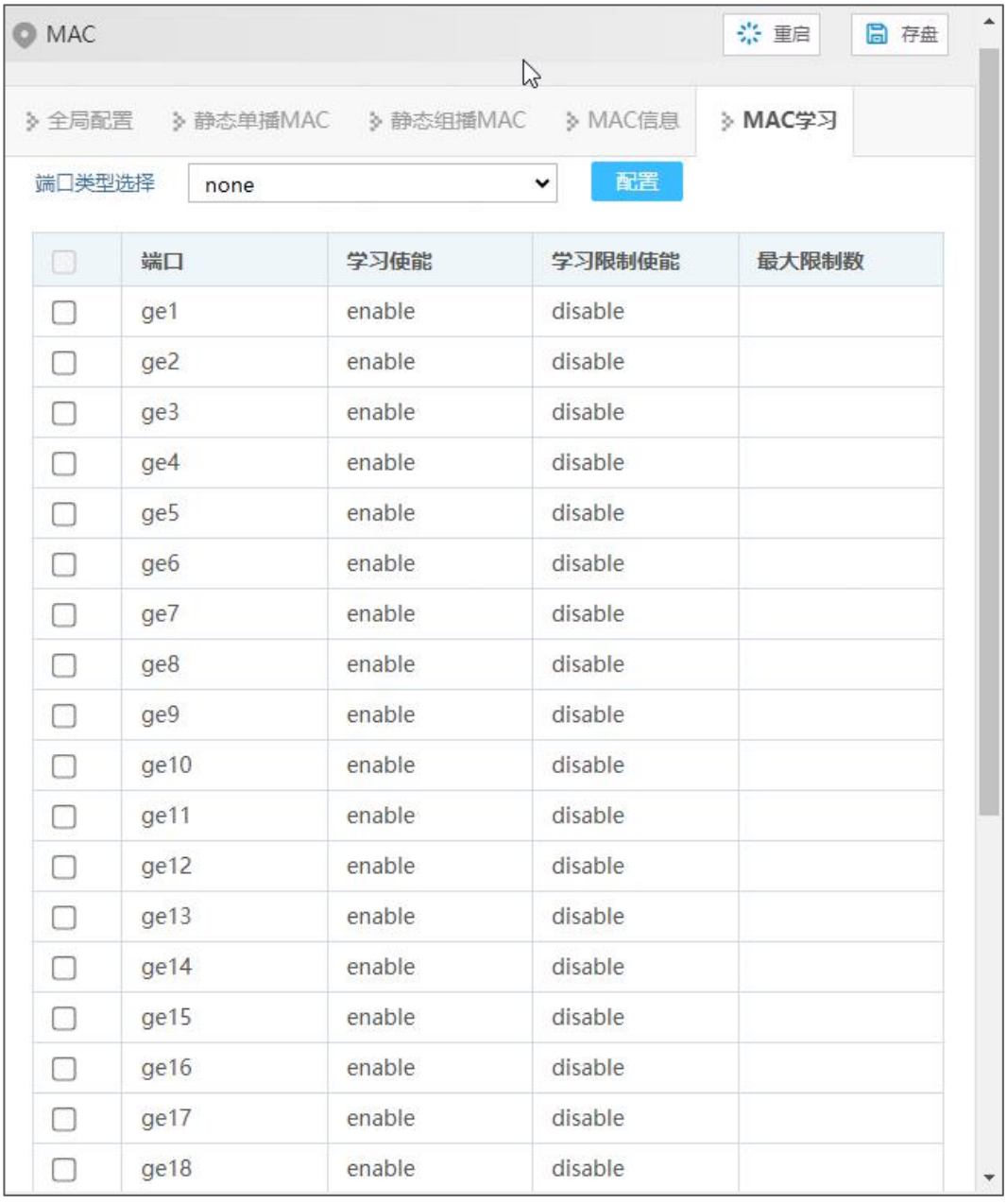
交换机，就会耗尽交换机的 MAC 地址表项资源，导致正常 MAC 地址无法学习，因此，限制交换机的 MAC 学习数量可以防止这种情况的发生，提高交换机与网络的安全性。

操作路径

按顺序依次打开：“二层配置 > MAC > MAC 学习”。

界面说明

MAC 学习界面如下所示：



MAC 学习界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。

界面元素	说明
学习使能开关	“学习使能”是指交换机开启或关闭对 MAC 地址的学习功能。当 MAC 学习使能开启时，交换机会学习并记录从各个端口收到的 MAC 地址，以建立 MAC 地址表，用于转发数据包。当 MAC 学习使能关闭时，交换机将停止学习新的 MAC 地址，只会使用已经学习到的 MAC 地址进行转发。 “学习使能开关”操作如下： • Disable：关闭学习限制使能开关； • Enable：打开学习限制使能开关。
学习限制使能开关	“学习限制使能”是指交换机开启或关闭某个 VLAN 学习限制和某个端口上学习的 MAC 地址数量的功能。当学习限制使能开启时，交换机会限制某个端口上学习的 MAC 地址数量，超过限制数量的 MAC 地址可能会被丢弃或忽略。当学习限制使能关闭时，交换机不对某个端口上学习的 MAC 地址数量进行限制。 “学习限制使能开关”操作如下： • Disable：关闭学习限制使能开关； • Enable：打开学习限制使能开关。 说明： “学习使能开关”和“学习限制使能开关”可以同时开启或关闭，但只有在“学习使能开关”开启的情况下，“学习限制使能开关”才有实际影响。
最大限制数	最大限制数是指“学习限制使能开关”限制某个端口上学习的 MAC 地址数量。

5.3 生成树

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。这里介绍三种生成树协议：

- STP（Spanning Tree Protocol，生成树协议）
- RSTP（rapid spanning Tree Protocol，快速生成树协议）
- MSTP（Multiple Spanning Tree Protocol，多生成树协议）

生成树协议的主要功能有两个：

- 一是在利用生成树算法、在以太网络中，创建一个以某台交换机的某个端口为根的生成树，避免环路。
- 二是在以太网络拓扑发生变化时，通过生成树协议达到收敛保护的目的。

MSTP 相比于 STP，RSTP 在网络结构发生变化时，MSTP 能更快的收敛网络；MSTP 兼容 STP 和 RSTP，并优于 STP 和 RSTP。它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

5.3.1 全局配置

功能说明

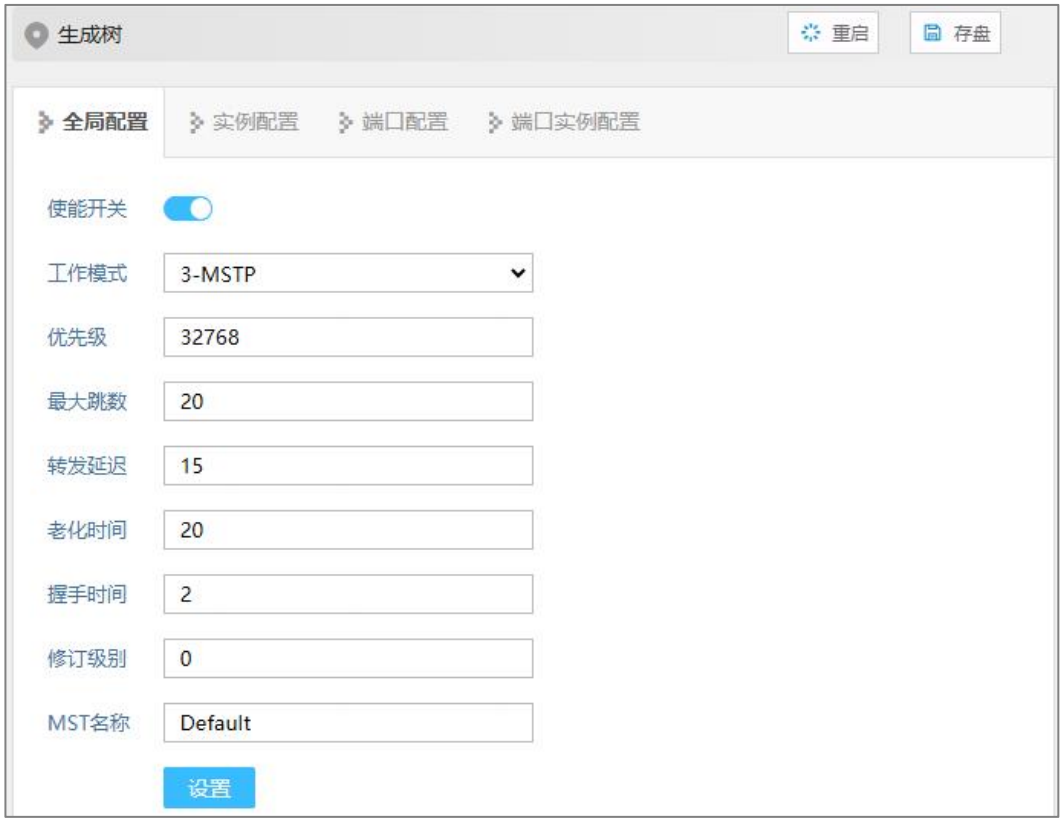
配置生成树的相关参数。

操作路径

按顺序依次打开：“二层配置 > 生成树 > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
使能开关	生成树使能开关，默认为 disable。
工作模式	生成树协议选择，默认为 MSTP，生成树三种模式： • 0-STP：生成树 • 2-RSTP：快速生成树

界面元素	说明
	• 3-MSTP：多生成树 说明： 在 RSTP 或 MSTP 模式下，当发现与 STP 设备相连时，端口会自动迁移到 STP 兼容模式下工作。
优先级	网桥的优先级，取值范围为 0-61440。 说明： 优先级的值越小，优先级越高，需为 4096 的倍数。
最大跳数	MST 域的最大跳数，默认为 20，取值范围为 1-40。 说明： MST 域的最大跳数限制了 MST 域的规模，配置在域根上的最大跳数将作为 MST 域的最大跳数。
转发延迟	端口状态迁移的延迟时间，默认为 15s，取值范围为 4-30。
老化时间	消息在设备中的最大生存期，默认为 20s，取值范围为 6-40。 用于确定配置消息是否超时。
握手时间	消息的发送周期，默认为 2s，取值范围为 1-10。 说明： • 生成树协议每隔 Hello Time 时间会发送配置消息，以确认链路是否存在故障。 • 为了避免网络频繁震荡，转发延迟、老化时间和握手时间应满足以下公式：2×（转发延迟-1）≥老化时间≥2×（握手时间-1）。
MST 名称	MST 域的域名，默认为 Default，最多 32 字符。

5.3.2 实例配置

功能说明

配置实例与 VLAN 的映射。

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台设备以及它们之间的网段所构成。

一个 MST 域内可以通过 MSTP 生成多棵生成树，各生成树之间彼此独立并分别与相应的 VLAN 对应，每棵生成树都称为一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。

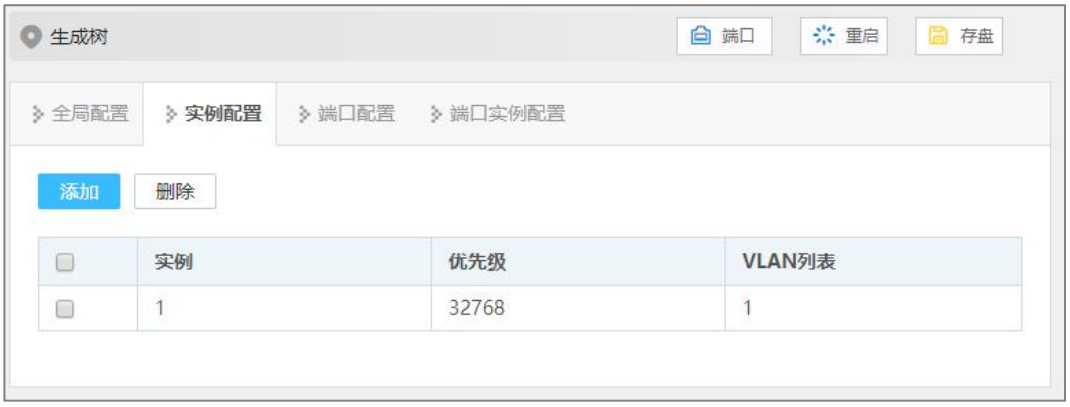
VLAN 映射表是 MST 域的一个属性，用来描述 VLAN 与 MSTI 间的映射关系。

操作路径

按顺序依次打开：“二层配置 > 生成树 > 实例配置”。

界面说明

实例配置界面如下所示：



实例配置界面主要元素配置说明：

界面元素	说明
实例	多生成树实例 ID 号，取值范围：1-16。
优先级	设备的优先级，取值范围为 0-61440，默认 32769，步长 4096。 在添加时，可选择基于 4096 上 0-15 倍数值的优先级。 说明： 设备的优先级参与生成树计算，其大小决定了该设备是否能够被选作生成树的根桥。
VLAN 列表	映射到 MSTI 实例的 VLAN 列表，每个 VLAN 只能对应一个 MSTI。 说明： VLAN 映射表是 MST 域的一个属性，用来描述 VLAN 与 MSTI 间的映射关系。MSTP 根据 VLAN 映射表来实现负载分担。

5.3.3 端口配置

功能说明

启用端口参加生成树，配置端口类型、链路类型和 BPDU 保护功能。

操作路径

按顺序依次打开：“二层配置 > 生成树 > 端口配置”。

界面说明

端口配置界面如下所示：

端口配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
使能开关	端口参与生成树使能状态，可显示如下： • Enable：启用 • Disable：禁用
BPDU Guard	BPDU 网桥协议数据单元（Bridge Protocol Data Unit）保护功能。启动 BPDU 保护后，如果边缘端口收到不应存在的 BPDU 报文，边缘端口将被关闭，可在一定时间后恢复正常。边缘端口 BPDU 保护状态： • Default：全局配置保护状态 • Enable：启用 • Disable：禁用

界面元素	说明
边缘端口	直接与终端相连而不是与其它交换机相连的端口。边缘端口不参与生成树运算，可以由 Disable 直接转到 Forwarding 状态。边缘端口使能状态： • Enable：启用 • Disable：禁用
连接类型	端口快速进入转发态要求端口必须是点对点链路，而不能是共享介质链路。端口链路类型： • Auto：若端口为全双工，则判别是点对点链路；若为半双工，则判别为非点对点链路。 • Point-to-point：点对点链路。 • Shared：非点对点链路。

5.3.4 实例端口配置

功能说明

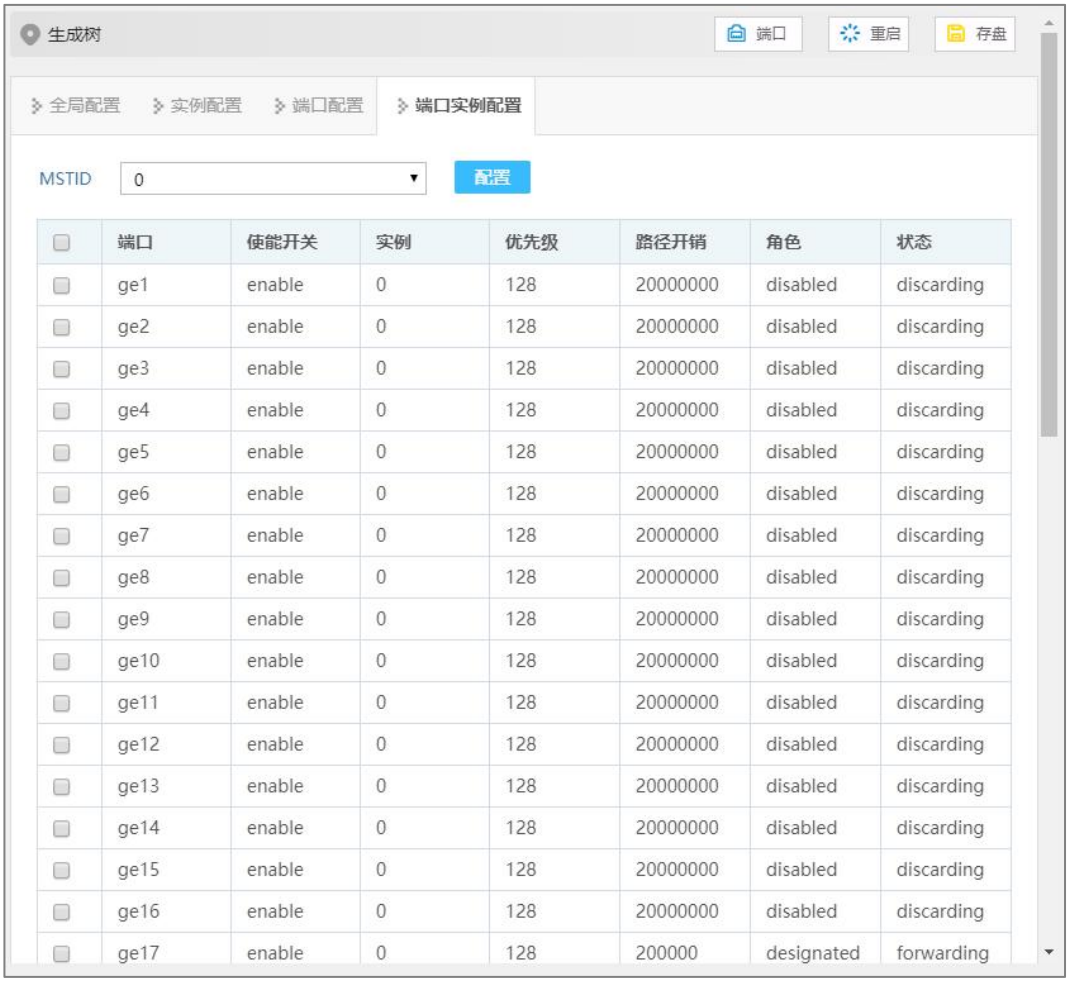
配置端口优先级和花销。

操作路径

按顺序依次打开：“二层配置 > 生成树 > 实例端口配置”。

界面说明

实例端口配置界面如下所示：



端口	使能开关	实例	优先级	路径开销	角色	状态
ge1	enable	0	128	20000000	disabled	discarding
ge2	enable	0	128	20000000	disabled	discarding
ge3	enable	0	128	20000000	disabled	discarding
ge4	enable	0	128	20000000	disabled	discarding
ge5	enable	0	128	20000000	disabled	discarding
ge6	enable	0	128	20000000	disabled	discarding
ge7	enable	0	128	20000000	disabled	discarding
ge8	enable	0	128	20000000	disabled	discarding
ge9	enable	0	128	20000000	disabled	discarding
ge10	enable	0	128	20000000	disabled	discarding
ge11	enable	0	128	20000000	disabled	discarding
ge12	enable	0	128	20000000	disabled	discarding
ge13	enable	0	128	20000000	disabled	discarding
ge14	enable	0	128	20000000	disabled	discarding
ge15	enable	0	128	20000000	disabled	discarding
ge16	enable	0	128	20000000	disabled	discarding
ge17	enable	0	128	200000	designated	forwarding

实例端口配置界面主要元素配置说明：

界面元素	说明
MSTID	选择多生成树 ID 号。
端口	该设备以太网端口对应的端口名称。
使能开关	端口的启用状态： • enable：启用，参与生成树 • disable：未启用，不参与生成树
实例	端口所属实例 ID 号。
优先级	端口优先级，取值范围 0-240，步长 16，默认为 128，可选择基于 16 上 0-15 倍数值的优先级。 说明： 端口在网桥之中的优先级，值越小，端口的优先级就越高。端口的优先级越高，才越有可能成为根端口。
配置花销	网桥到根桥的路径开销，默认为 20000000，取值范围：1-200000000。 说明： 当配置花销为默认值时，link up 的端口实际花费根据端口速率来换算，速率 10M 对应花销 2000000，100M 对应花销 200000。

界面元素	说明
角色	端口角色： • unkn：未知 • root：根端口 • desg：指定端口 • altn：替代端口 • back：备份端口 • disa：未启用端口
状态	端口在生成树中的状态： • Disable：端口关闭状态 • Blocking：阻塞状态 • Listening：监听状态 • Discarding：丢弃状态 • Learning：学习状态 • Forwarding：转发状态

5.4 Ring

Ring 是专为高可靠性的需要链路冗余备份的工业控制网络应用而开发设计的私有网环网算法。其设计理念完全遵照国际通用标准（STP 和 RSTP）实现，并专门针对工业控制应用做了必要的优化，具有以太网链路冗余，故障快速自动恢复能力。

Ring 采用无主站设计，运行 Ring 协议的设备通过彼此交互信息发现网络中的环路，并对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断循环，避免设备由于重复接收相同的报文造成处理能力下降。在 250 台交换机组成的多环网络中，当网络中断或网络产生故障时，Ring 能够确保用户网络在 20ms 以内自动恢复链路通信。

Ring 需提前手动划分环网端口，支持单环、耦合环、链和 Dual Homing 多种环网类型，并提供网络拓扑可视化管理。在单环中，Ring 支持主站/从站与无主站配置，满足多种网络环境需求。

5.4.1 全局配置

功能说明

配置 Ring 私有协议环网。

操作路径

按顺序依次打开：“二层配置 > 全局配置”。

界面说明

全局配置界面如下所示：

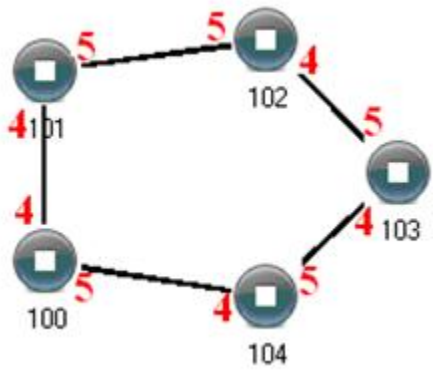
全局配置界面主要元素配置说明：

界面元素	说明
使能开关	使能开关，开启后可启用 Ring 环网功能。
环网组	支持环网组 1-12，可同时创建多个环网。
网络标识	当多个交换机设备组成一个环网时，该环网当前的环网标识即网络标识，不同环网的网络标识不相同。取值范围：1-255。 说明： 在同一个环网中，环网标识必须保持一致。
环网端口 1	交换机设备上用于组成环网的网络端口 1。 说明： 在环网类型为“Couple”时，“环网端口 1”为“耦合端口”。耦合端口是连接不同网络标识的端口。
端口 1 状态	环网端口 1 的导通状态。
环网端口 2	交换机设备上用于组成环网的网络端口 2。 说明： 在环网类型为“Couple”时，“环网端口 2”为“控制端口”。控制端口是两环相交的那条链路中的端口。
端口 2 状态	环网端口 2 的导通状态。
环网类型	根据现场环境需求，可选择不同的环网类型。 • Single：单环，使用一个连续的环将每台设备连接在一起。 • Couple：耦合环，是为了连接两个相互独立的网络而提出的一种冗余结构。 • Chain：链，通过一种先进的软件技术增强用户构建任何类型的冗余网络拓扑结构的灵活性。 • Dual-homing：两个相邻的环共用一个交换机，用户可以将同一台交换机分别搭载在两个不同的网络或同一个网络的两个不同的交换设备上。
Hello Time(100ms)	Hello_time 即 Hello 包发送时间间隔，由 CPU 通过环网端口向相邻的设备发出的问询包，用来确认连接是否正常。取值范围：0-300。

界面元素	说明
主从模式	单环支持无主站与一主多从模式可选： • 无主站模式：当单环设备均为从站时，单环为无主站结构。 • 一主多从模式：将设备为主设备时，该环路主设备的一端为备份链路，当环网发生故障时从主站启用备份链路，保障网络的正常运行。
心跳	心跳检测机制，启用该配置，环网协议会周期性的发送心跳报文，检测相应设备是否处于 live 状态，从而增强环网的可靠性。

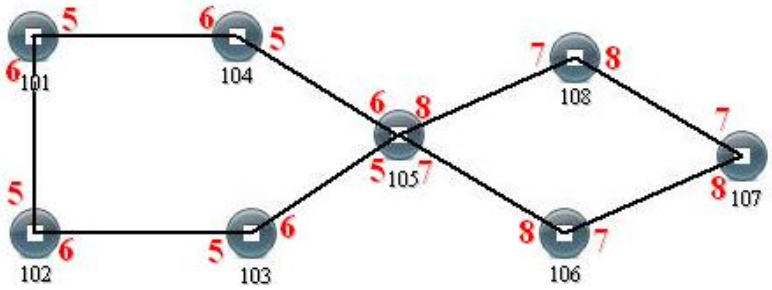
单环配置

启用 Single，启用环网组 1（其他环网组也可），设置设备端口 4 和端口 5 为环网口，设置其他交换机与上交换机配置一致，重启这些设备，再用网线把交换的端口 4 和端口 5 用网线连接起来，使用网管软件搜索，环网拓扑结构图如下：



双环配置

双环如下图所示，从图中可以看出双环为两个环网相切，切点为 105 号交换机。



配置方法：

步骤 1 使用配置单环的方法分别配置交换机 101、102、103、104、105 的端口 5 和端口 6 为环网口，且环网组为 1；

步骤 2 使用配置单环的方法分别配置交换机 105、106、107、108 的端口 7 和端口 8 为环网口，

且环网组 2；

步骤 3 使用网线将环网组 1 连接起来；

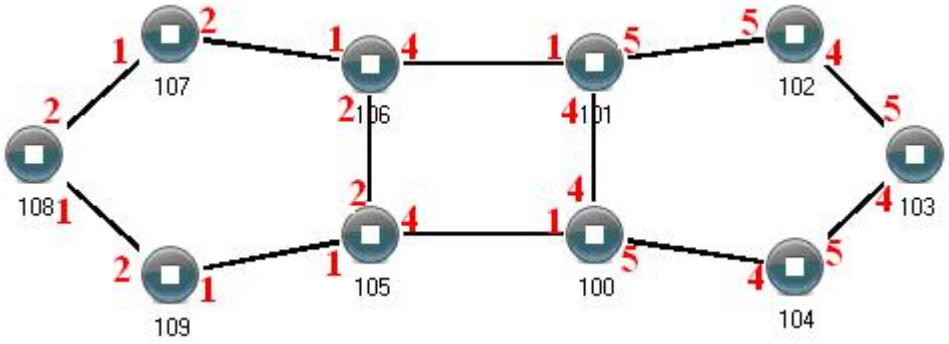
步骤 4 使用网线将环网组 2 连接起来；

步骤 5 使用网管软件搜索其拓扑结构图；

由于 105 号设备属于两个环网组，所以两个环网组的网络标识不能相同。

耦合环配置

耦合环基本架构如下图所示：



操作方法：

步骤 1 启用环网组 1 和环网组 2；（Hello_time 可以不开启，但设置的时间不能使得 Hello 包发送太快，否则会严重影响 CPU 处理速度）；

步骤 2 设置 105、106 号设备的环网组 1 的环网口为端口 1 和端口 2，网络标识为 1，环网类型为 Single；设置环网组 2 的耦合端口为端口 4，控制端口为 2，环网标识为 3，环网类型为 Coupling。

步骤 3 设置 100、101 号设备的环网组 1 的环网口为端口 4 和端口 5，网络标识为 2，环网类型为 Single；设置环网组 2 的耦合端口为端口 1，控制端口为端口 4，环网标识为 3，环网类型为 Coupling。

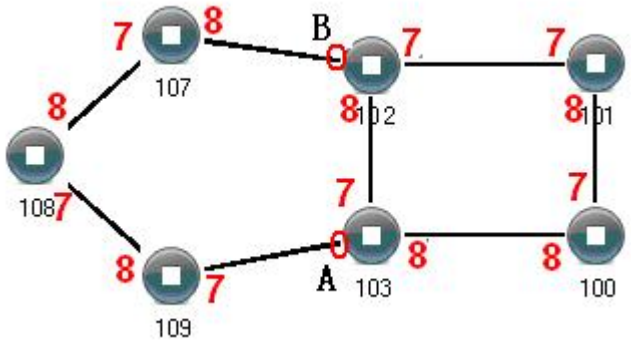
步骤 4 设置设备 107，108，109 的环网组 1 的环网口为端口 1 和端口 2，网络标识为 1，环网类型为 Single；设置设备 102，103，104 的环网组 1 的环网口为端口 4 和端口 5，环网标识为 2，环网类型为 Single。

步骤 5 用网线将设备 100-104 五台设备的端口 4、5 依次顺接组成单环，用网线将设备 105-109 四台设备的端口 1、2 依次顺接组成单环，再用网线连接设备 106 号的端口 4 和设备 101 号的端口 1，设备 105 号的端口 4 和设备 100 号的端口 1，耦合环组合完毕。

控制端口为如上图中设备 105 和设备 106 相连的两个口，同样设备 100 和设备 101 相连的两个口也称之为控制端口。

链配置

链基本架构如下图所示：



操作方法：

步骤 1 启用环网组 1；（Hello_time 可以不开启，但设置的时间不能使得 Hello 包发送太快，否则会严重 CPU 处理速度）；

步骤 2 设置 100、101、102 和 103 号设备的环网组 1 的环网端口为端口 7 和端口 8，网络标识为 1，环网类型为 Single。设置 107、108 和 109 号设备的环网组 1 的环网端口为端口 7 和端口 8，网络标识为 2，环网类型为 Chain。

步骤 3 用网线将设备 107-109 三台设备的端口 7、8 依次顺接级联，用网线将设备 100-103 四台设备的端口 7、8 依次顺接组成单环，再用网线连接将设备 107 号的端口 7 和设备 109 号的端口 7 分别连到设备 102 和 103 的普通端口，链组合完毕。

说明

- 已设置成端口聚合的端口不能再设置成快速环网端口，一个端口不能同时属于多个环网；
- 同一单环内网络标识必须一致，否则无法正常组成环且无法正常通讯；
- 不同环网的网络标识必须不同；
- 组成双环等较复杂的环网时候，应注意环网标识是否遵循单环网络标识一致，不同单环网络标识必须不同。

5.4.2 Ring 信息

功能说明

系统提供该功能，您可以通过“Ring 信息”页面查看。

操作路径

按顺序依次打开：“二层配置 > Ring 信息”。

界面说明

Ring 信息界面如下所示：

Ring 信息界面主要元素配置说明：

界面元素	说明
环网组	支持展示环网组 1-12。
本地环网端口 1	交换机设备上用于组成环网的网络端口 1。 说明： 在环网类型为“Couple”时，“环网端口 1”为“耦合端口”。 耦合端口是连接不同网络标识的端口。
邻居环网端口 1	邻居环网端口 1 的端口号，例如：3。
收敛设备 MAC 地址 1	收敛设备 MAC 地址 1，就是环网后设备的 MAC 地址 1，例如：00:22:6f:01:d0:a2。
邻居 MAC 地址 1	环网组的邻居设备 MAC 地址 1，例如：00:22:6f:01:cc:a2。
本地环网端口 2	交换机设备上用于组成环网的网络端口 2。 说明： 在环网类型为“Couple”时，“环网端口 2”为“控制端口”。 控制端口是两环相交的那条链路中的端口。
邻居环网端口 2	邻居环网端口 2 的端口号，例如：5。
收敛设备 MAC 地址 2	收敛设备 MAC 地址 2，就是环网后设备的 MAC 地址 2，例如：00:22:6f:01:d0:a2。
邻居 MAC 地址 2	环网组的邻居设备 MAC 地址 2，例如：00:22:6f:01:cc:a2。
环网状态	环网状态展示的情况： ● stable：表示当前环网组网络处于稳定状态； ● open：表示当前环网组网络处于开路状态。

5.5 MRP

MRP（Media Redundancy Protocol）介质冗余协议，在 MRP 环网中，一台设备作为冗余管理器，其它设备作为冗余客户端。MRP 支持至多 50 台设备组环，当环网中断后，环网重新组态时间小于 200ms。

功能说明

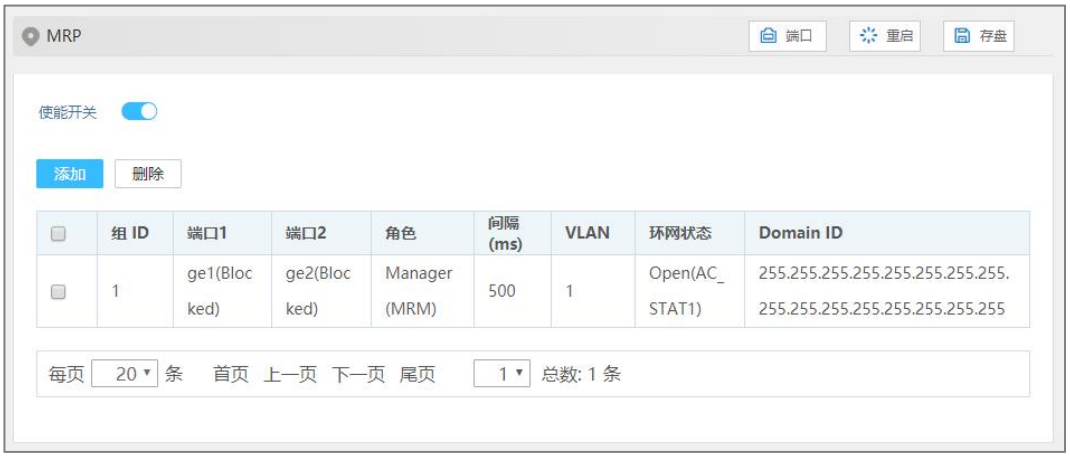
配置 MRP 环网。

操作路径

按顺序依次打开：“二层配置 > MRP”。

界面说明

MRP 界面如下所示：



MRP 界面主要元素配置说明：

界面元素	说明
使能开关	使能开关，开启后可启用 MRP 环网功能。
组 ID	环网组 ID，取值范围为 1-50。
端口 1	环网端口 1，组成环网的端口以及端口数据的转发状态。
端口 2	环网端口 2，组成环网的端口以及端口数据的转发状态。
角色	设备在环网中的冗余角色，可选项如下： • manager：介质冗余管理器 • client：介质冗余客户端
间隔（ms）	当 MRP 环网断开后，环网重新组态收敛时间，可选项如下： • 200ms • 500ms
VLAN	MRP 管理报文使用的 VLAN ID，取值范围为 1-4094。
环网状态	MRP 环网的状态，Open 或 Close。
Domain ID	MRP 环网组域 ID，格式为 X.X.X.X.X.X.X.X.X.X.X.X.X.X.X.X。

5.6 ERPS

ERPS（Ethernet Ring Protection Switching，以太环网保护倒换）是具备高可靠性和稳定性的以太环网链路层技术。ERPS 是 ITU-T（International Telecommunication Union Telecommunication Standardization Sector）定义的一种二层破环协议标准，标准号为 ITU-T G.8032/Y1344，因此又称为 G.8032。它定义了 RAPS（Ring Auto Protection Switching）协议报文和保护倒换机制。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环发生链路故障时能迅速恢复环网上各个节点之间的通信通路，具备较高的收敛速度。

5.6.1 定时器配置

功能说明

配置 ERPS 环网定时器参数。ERPS 环中节点设备或链路故障恢复后，为了防止出现震荡，会启用到 ERPS 环定时器，帮助减少业务流量的中断时间。

ERPS 协议中使用的定时器主要有 WTR（Wait to Restore）Timer 定时器、Guard Timer 定时器和 Hold Timer 定时器。

- WTR Timer
  RPL owner 端口由于其他设备或链路故障而被放开后，当故障恢复时，有的端口可能还未由 Down 状态变为 Up 状态。为了防止立即阻塞 RPL owner 端口而引起网络震荡，当 RPL owner 端口收到某端口的 NR RAPS 报文后，会启动 WTR Timer 定时器。如果在定时器未超时前收到其他端口的 SF（Signal Fail，信号失败） RAPS 报文，则关闭 WTR Timer 定时器。如果在 WTR Timer 定时器超时前始终没有收到其他端口的 SF RAPS 报文，则当 WTR Timer 定时器超时后，阻塞 RPL owner 端口，发送 NR-RB（RPL Block，RPL 阻塞）RAPS 报文。其他端口在收到该报文后，再将自己端口的转发状态设置为 Forwarding 状态。
- Guard Timer
  链路故障或节点故障所涉及到的设备在故障恢复或执行清除操作后，向其他设备发送 NR（No Request，链路恢复） RAPS 报文，并同时启动 Guard Timer 定时器，在该定时器超时前不处理 NR RAPS 报文，目的是防止收到过期的 NR RAPS 报文。如果定时器超时后还能收到其他端口发送的 NR RAPS 报文，则本端口的转发状态变为 Forwarding 状态。
- Hold Timer
  对于运行 ERPS 的二层网络，保护倒换的顺序可能会有不同的要求，例如：多层业务的应用中，服务器出现故障后，用户可能会希望能有一段时间恢复服务器的故障，而客户端感知不到，即不会立即进行保护倒换。可设置合适的 Hold Timer 定时器，

当发生故障时，故障并不会立即上报 ERPS，而只有当 Hold Timer 定时器超时后，如果故障仍未能恢复才会上报。

操作路径

按顺序依次打开：“二层配置 > ERPS > 定时器配置”。

界面说明

定时器配置界面如下所示：

定时器配置界面主要元素配置说明：

界面元素	说明
定时器名	ERPS 定时器的名称，支持 1-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。
WTR（m）	WTR 定时器，取值范围为 1-12，单位分钟。
Guard Timer（单位:10ms）	Guard 定时器，取值范围为 1-200，单位 10 毫秒。
Hold Timer(单位:100ms）	Hold 定时器，取值范围为 0-100，单位 100 毫秒。
可逆	ERPS 可逆模式状态，可选项如下： • enable：启用。如果故障链路恢复，等待 WTR 时间后，会重新阻塞 RPL owner 端口。阻塞链路会重新切回到 RPL 上。 • disable：禁用。如果故障链路恢复，不启动 WTR Timer 定时器，而且阻塞链路还保持在原来的故障链路上，不会重新切回到 RPL 上。

5.6.2 环网配置

功能说明

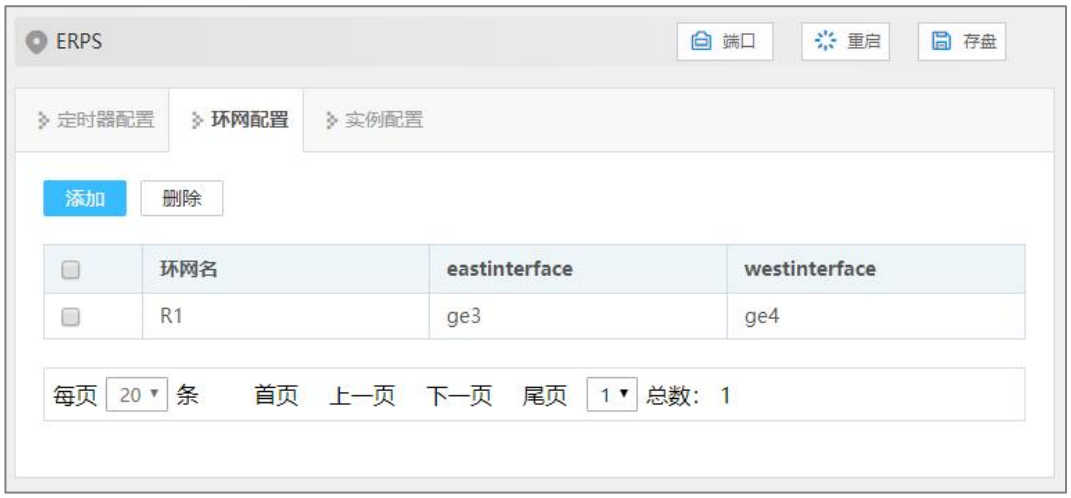
配置 ERPS 环网端口。

操作路径

按顺序依次打开：“二层配置 > ERPS 配置 > 环网配置”。

界面说明

环网配置界面如下所示：



环网配置界面主要元素配置说明：

界面元素	说明
环网名	ERPS 环网的名称，支持 1-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。
EastInterface	ERPS 环网端口。 说明： 当设备为相交节点时，子环部分端口可只配置 EastInterface。
WestInterface	ERPS 环网端口。 注意： • ERPS 环端口可以是普通物理端口或者静态聚合组。 • ERPS 环端口不能与其他二层环网协议同时开启端口，当 ERPS 保护实例不为 0 时，可以与 MSTP 同时开启。 • ERPS 环端口不能为同一端口。 • ERPS 环端口必须为 trunk 端口且允许该环实例 VLAN 通过。

5.6.3 实例配置

功能说明

配置 ERPS 环网实例。

操作路径

按顺序依次打开：“二层配置 > ERPS 配置 > 实例配置”。

界面说明

实例配置界面如下所示：

实例配置界面主要元素配置说明：

界面元素	说明
实例名称	ERPS 实例的名称，支持 1-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。
环网类型	ERPS 实例环网类型，可选项如下： • Major-ring：主环，封闭的环。 • Sub-ring：子环，非封闭的环，与主环形成相交环等多环组网。
环网名	ERPS 环网的名称。 说明： 环网名需在 ERPS“环网配置”中提前创建，并指定环网端口。
实例 ID	ERPS 保护实例的 ID，取值范围为 0-16。传递 ERPS 协议报文和数据报文的 VLAN 必须映射到保护实例中，这样 ERPS 协议才会按照其阻塞原则对这些报文进行转发或阻塞。 说明： • 默认情况下，MST 域内所有的 VLAN 都映射到实例 0。 • VLAN 与实例的映射，可在生成树实例配置中创建。
环网 ID	ERPS 环网的 ID，取值范围为 1-239。环网 ID 用来唯一标识一个 ERPS 环，在同一 ERPS 环上的所有节点上应配置相同的环网 ID。 说明： ERPS 环网 ID 将会作为 RAPS 报文目的 MAC 的最后一个字节。
定时器名	定时器的名称，支持默认参数定时器或在定时器配置中自定义。
RPL 角色	ERPS环上的每台设备都称为一个节点。节点角色由用户的配置来决定，可选项有如下几种： • owner：主节点，负责阻塞和放开本节点上位于 RPL 上的端口，防止形成环路，从而进行链路倒换。 • neighbor：邻居节点，RPL 上和 Owner 节点相连的节点，协

界面元素	说明
	同 Owner 节点阻塞和放开本节点上位于 RPL 上的端口，进行链路倒换。 • non-owner：非主节点，负责接收和转发链路中的协议报文和数据报文。
RPL 端口	RPL 链路连接的端口，可选项如下： • West-interface • East-interface
拓扑变化通告	将本 ERPS 环的网络拓扑变化通知到其它 ERPS 环，使能状态如下： • Enable：启用 • Disable：禁用
管理 VLAN	协议报文的 VLAN 通道，取值范围为：1-4094。
等级	ERPS 环网等级，取值范围为 0-7。环网等级越高值越大。当 R-APS 消息需要跨环传输消息时，只能由等级高的跨过等级低的环。
状态	ERPS 的实例状态，状态有如下几种： • ERPS_INIT：初始状态，协议启动时初始化的状态； • ERPS_IDLE：空闲状态，环拓扑完整时会进入该状态； • ERPS_FS：强制倒换状态，执行 force-switch 命令后进入该状态； • ERPS_MS：手工倒换状态，执行 manual-switch 命令后进入该状态； • ERPS_PROTECTION：保护状态，环链路故障后会进入该状态； • ERPS_PENDING：就绪状态，环链路故障恢复后会进入该状态。
启动	ERPS 实例启动状态： • start：启用 • stop：停用

5.7 IGMP-Snooping

IGMP Snooping (Internet Group Management Protocol Snooping)是一种 IPv4 二层组播协议，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出接口信息，从而管理和控制组播数据报文在数据链路层的转发。

5.7.1 全局配置

功能说明

启用/禁用 IGMP-Snooping 和常驻组播。

操作路径

按顺序依次打开：“二层配置 > IGMP-Snooping > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
全局使能开关	IGMP-Snooping 全局使能配置。通过使能 IGMP Snooping，二层设备就可以通过侦听 IGMP 查询器与用户主机间的 IGMP 协议报文，动态建立二层组播转发表项，实现二层组播。
常驻组播	对收到的 IGMP 报告成员组不进行老化。
Vlan-id	接收组播信息端口所属的 VALN ID。
组播地址或源地址	根据网络环境，可显示组播地址和源地址信息。
端口	接收组播信息的端口号。
类型	组播成员端口加入组播组的方式。可能的显示项为： • Remote：动态加组，通过接口所连接终端设备发送报文的方式加组播组。 • Static：静态加组，通过命令配置端口加入组播组。 • Remote(static)：动态静态，通过静态或者动态方式加入组播组。
uptime	接收到组播信息的时间。
Expire	组播信息过期的时间。可能的显示项为： • Static：静态地址，组播不会自动过期，需要手动删除或重新配置。

界面元素	说明
	• Permanent：永久组播，即使组播组成员发生变化，组播路由也不会自动删除。 • Include：当网络设备接收到组播数据时，它会检查这些数据是否属于 include 列表中的组播组。如果是，则允许这些数据通过；如果不是，则丢弃这些数据。 • Exclude：当网络设备接收到组播数据时，它会检查这些数据是否属于 exclude 列表中的组播组。如果是，则丢弃这些数据；如果不是，则允许这些数据通过。
Last Reporter	最后一个发送 report 报文加入组播组的组播成员 IP 地址。
版本	IGMP Snooping 的版本。

5.7.2 接口配置

功能说明

配置 VLANIF 接口 IGMP Snooping 相关参数。

操作路径

按顺序依次打开：“二层配置 > IGMP-Snooping > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。
版本	不同版本的 IGMP Snooping 可以处理相应版本的 IGMP 协议版本。 IGMP Snooping 协议版本，可选项如下：

界面元素	说明
	• 1 • 2 • 3
快速离开	组播组快速离开使能状态。开启快速离开后，当交换机从某端口收到主机发送的离开某组播组的 IGMP 离开报文后，不等待端口老化，直接把端口从该组播转发表项中删除，可节约带宽和资源。 说明： 当端口下有多个接收者时，该功能会造成同一组播组中的其他接收者中断接收组播数据。建议在只连接有一个接收者的端口上配置此功能。
查询器	IGMP Snooping 查询器使能状态。使能 IGMP Snooping 查询器功能后，交换机会定时以广播的方式向 VLAN 内所有接口（包括路由器端口）发送 IGMP Query 报文，如果组播网络中已经存在 IGMP 查询器，会引起 IGMP 查询器重新选举。
查询器地址	IGMP Snooping 查询器发送查询报文时的源 IP 地址。
查询器选举	IGMP Snooping 查询器选举使能状态。IGMPv2 使用独立的查询器选举机制，当共享网段上存在多个组播路由器时，IP 地址最小的路由器成为查询器，而非查询器则不再发送普遍组查询报文。
使能状态	IGMP Snooping 使能状态，可在全局或者 VLAN 接口上使能 IGMP snooping。 说明： 只有在全局和 VLAN 接口上使能了 IGMP snooping，在该接口上对其它 IGMP snooping 特性所作的配置才能生效。

5.7.3 路由口配置

功能说明

配置组播路由器端口。

操作路径

按顺序依次打开：“二层配置 > IGMP-Snooping > 路由口配置”。

界面说明

路由口配置界面如下所示：

路由口配置界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。
端口	VLAN 内的静态路由器端口，一般是二层设备上朝向上游三层组播设备的接口。如果需要长期稳定的从一个接口转发 IGMP Report/Leave 报文到上游 IGMP 查询器，可以将该接口配置为静态路由器端口。

5.7.4 路由口信息

功能说明

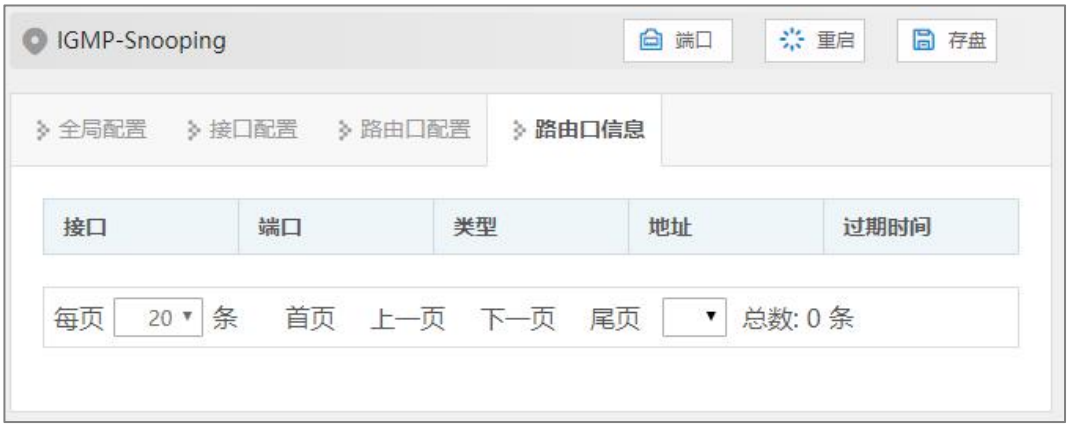
查看 VLAN 内 IGMP Snooping 的路由器端口信息，包括静态路由器端口和动态路由器端口。

操作路径

按顺序依次打开：“二层配置 > IGMP-Snooping > 路由口信息”。

界面说明

路由口信息界面如下所示：



路由口信息界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。
端口	VLAN 内的路由器端口。
类型	路由器端口的类型，包含动态与静态。
地址	IP 地址。
过期时间	动态路由器端口剩余老化时间。

5.8 IPv6 MLD-Snooping

MLD Snooping (Multicast Listener Discovery Snooping)是一种 IPv6 二层组播协议，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出端口信息，从而管理和控制组播数据报文在数据链路层的转发。

5.8.1 全局配置

功能说明

启用/禁用 Mld-Snooping 和常驻组播。

操作路径

按顺序依次打开：“二层配置 > Mld-Snooping > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
全局使能	MLD-Snooping 全局使能配置。通过使能 MLD Snooping，二层设备就可以通过侦听 MLD 查询器与用户主机间的 MLD 协议报文，动态建立二层组播转发表项，实现二层组播。
常驻组播	配置组播组为常驻组播组，不老化，不离开。
vlan	接收组播信息端口所属的 VALN ID。
组播地址或源地址	根据网络环境，可显示组播地址和源地址信息。
端口	接收组播信息的端口号。
uptime	接收到组播信息的时间。
老化时间	组播信息过期的时间。可能的显示项为： • Static：静态地址，组播不会自动过期，需要手动删除或重新配置。 • Permanent：永久组播，即使组播组成员发生变化，组播路由也不会自动删除。 • Include：当网络设备接收到组播数据时，它会检查这些数据是否属于 include 列表中的组播组。如果是，则允许这些数据通过；如果不是，则丢弃这些数据。 • Exclude：当网络设备接收到组播数据时，它会检查这些数据是否属于 exclude 列表中的组播组。如果是，则丢弃这些数据；如果不是，则允许这些数据通过。
Last Reporter	最后一个发送 report 报文加入组播组的组播成员 IP 地址。

5.8.2 接口配置

功能说明

配置 VLANIF 接口 MLD Snooping 相关参数。

操作路径

按顺序依次打开：“二层配置 > Mld-Snooping > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。
使能状态	MLD Snooping 使能状态，可在全局或者 VLAN 接口上使能 MLD snooping。 说明： 只有在全局和 VLAN 接口上使能了 MLD snooping，在该接口上对其它 MLD snooping 特性所作的配置才能生效。
版本	不同版本的 MLD Snooping 可以处理相应版本的 MLD 协议版本。 MLD Snooping 协议版本，可选项如下： • 1 • 2
快速离开	组播组快速离开使能状态。开启快速离开后，当交换机从某端口收到主机发送的离开某组播组的 MLD Done 报文后，不等待端口老化，直接把端口从该组播转发表项中删除，可节约带宽和资源。 说明： 当端口下有多个接收者时，该功能会造成同一组播组中的其他接收者中断接收组播数据。建议在只连接有一个接收者的端口上配置此功能。
查询器	MLD Snooping 查询器使能状态。使能 MLD Snooping 查询器功能后，交换机会定时以广播的方式向 VLAN 内所有接口（包括路由器端口）发送 MLD Query 报文，如果组播网络中已经存在 MLD 查询器，会引起 MLD 查询器重新选举。

界面元素	说明
查询器选举	MLD Snooping 查询器选举使能状态。当共享网段上存在多个组播路由器时，IPv6 地址最小的路由器成为查询器，而非查询器则不再发送普遍组查询报文。

5.8.3 路由口配置

功能说明

配置组播路由器端口。

操作路径

按顺序依次打开：“二层配置 > Mld-Snooping > 路由口配置”。

界面说明

路由口配置界面如下所示：

路由口配置界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。
端口	VLAN 内的静态路由器端口，一般是二层设备上朝向上游三层组播设备的接口。当需要长期稳定的从某接口接收和转发组播数据时，可以配置该接口为静态路由器端口。

5.8.4 路由口信息

功能说明

查看 VLAN 内 MLD Snooping 的路由器端口信息，包括静态路由器端口和动态路由器端口。

操作路径

按顺序依次打开：“二层配置 > Mld-Snooping > 路由口信息”。

界面说明

路由口信息界面如下所示：

路由口信息界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。
端口	VLAN 内的路由器端口。
类型	路由器端口的类型，包含动态与静态。
地址	IP 地址。
过期时间	动态路由器端口剩余老化时间。

5.9 链路震荡保护

网络抖动或链路网线故障等原因会引起设备接口物理状态频繁 Up/Down 变化，导致链路震荡，致使网络拓扑结构频繁变化，影响用户通信。例如，在主备链路应用中，当主链路接口物理状态频繁 Up/Down 变化时，业务将在主备链路之间来回切换，不仅会增加设备负担，还可能造成业务数据丢失。

为了解决上述问题，用户可以配置链路震荡保护功能，将物理状态频繁 Up/Down 变化的接口关闭，使之处于 Down 状态，这样网络拓扑结构将停止来回频繁变化。

5.9.1 全局配置

功能说明

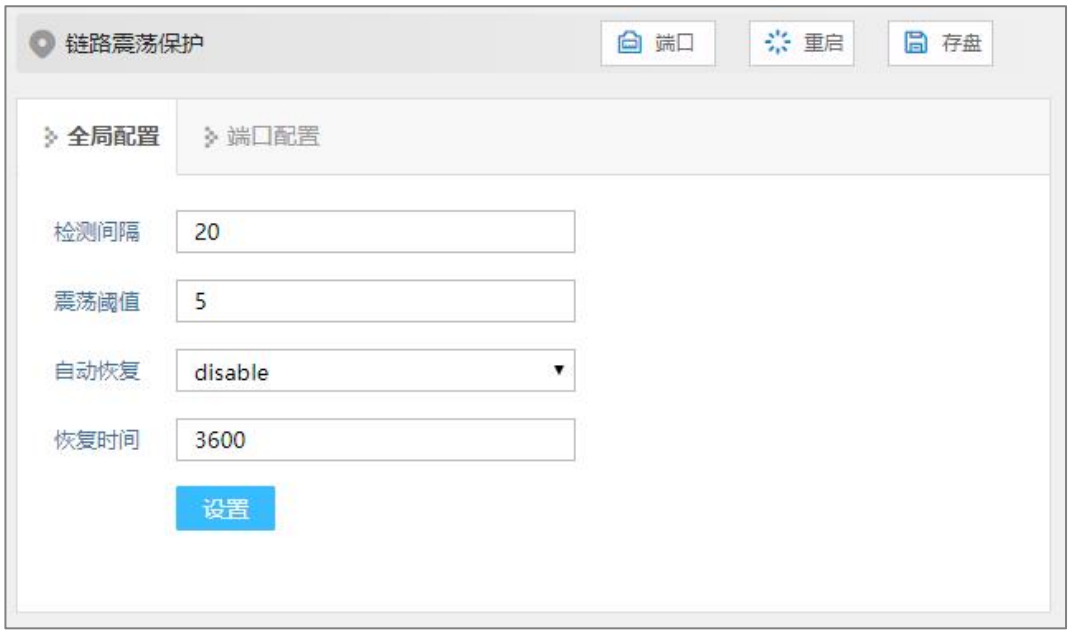
配置链路震荡保护的相关参数。

操作路径

按顺序依次打开：“二层配置 > 链路震荡保护 > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
检测间隔	链路检测的时间间隔，取值范围为：10-100s，默认值为 20s。
震荡阈值	链路检测的震荡次数阈值，在“检测间隔”指定的时间内震荡次数超过阈值时，会产生告警日志，并且将端口设置为 shutdown 的状态。取值范围：3-100，默认值为 5。
自动恢复	自动恢复使能配置，启用后端口在指定时间内自动恢复正常。
恢复时间	端口自动恢复正常的时间，取值范围：30-86400s，默认值为 3600s。

5.9.2 端口配置

功能说明

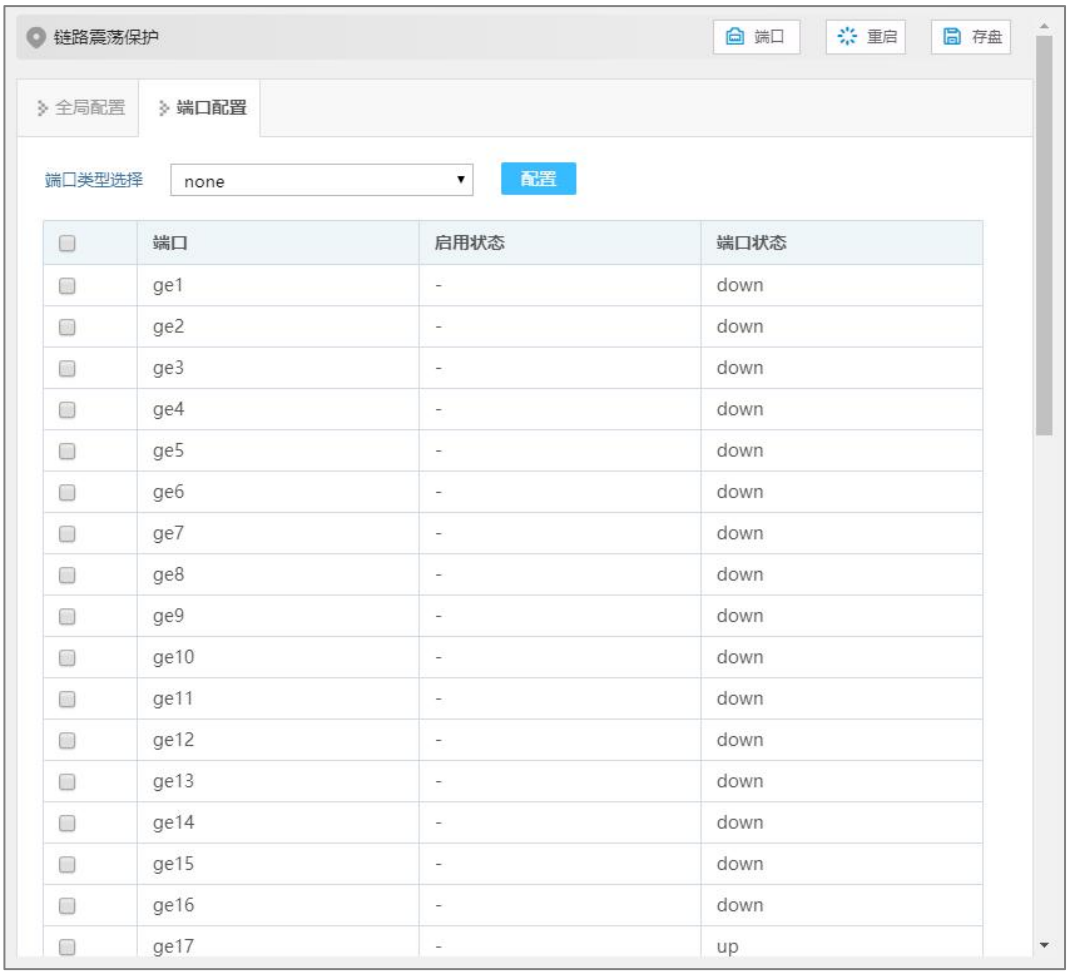
开启端口链路震荡保护。

操作路径

按顺序依次打开：“二层配置 > 链路震荡保护 > 端口配置”。

界面说明

端口配置界面如下所示：



端口配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口号。
启用状态	端口链路震荡保护的启用状态，可显示如下： • ON：表示启用 • -：表示禁用
端口状态	以太网端口的连接状态，可显示如下：

界面元素	说明
	• down：端口未连接或被强制 shutdown • up：端口已连接

5.10 端口环路检测

环路检测作用是检测交换机的单个端口外部网络是否存在环路。如果端口存在环路，会导致地址学习错误，且容易造成广播风暴，严重时会导致交换机及网络瘫痪。启用端口的协议，关闭有环路的端口，可以有效的消除端口环路造成的影响。

功能说明

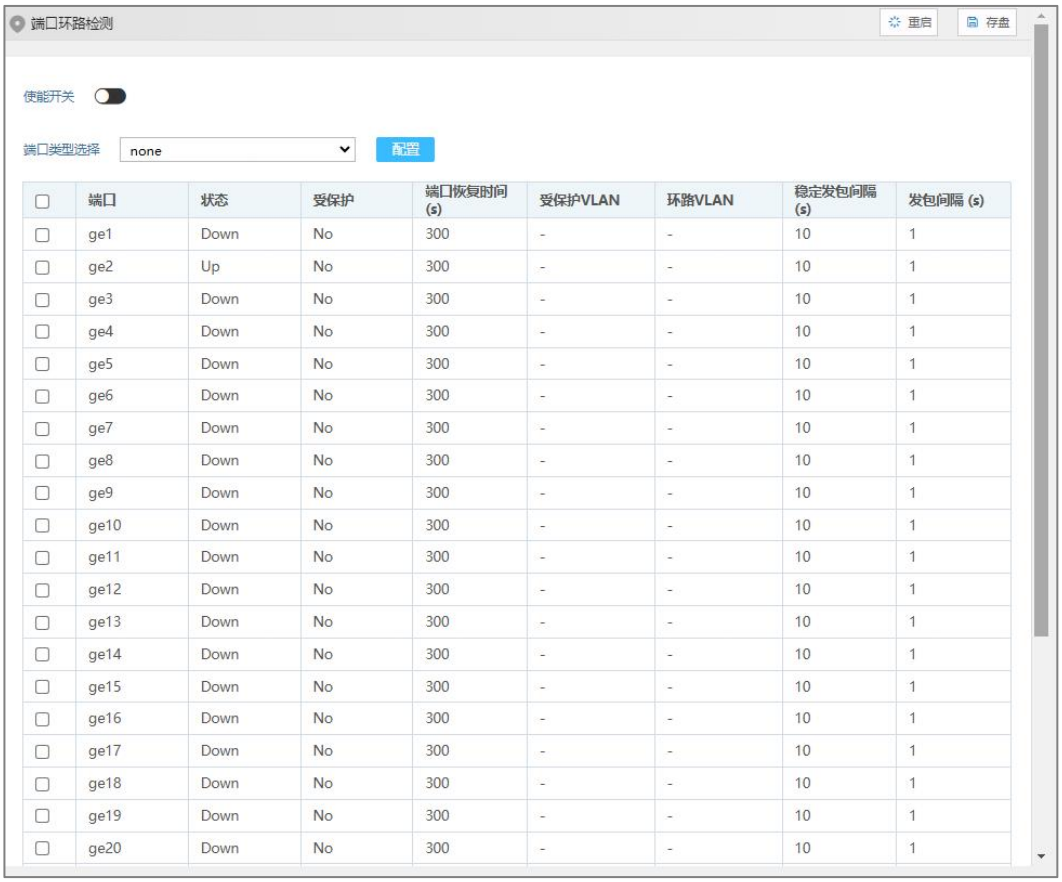
启用端口环路检测。

操作路径

按顺序依次打开：“二层配置 > 端口环路检测”。

界面说明

端口环路检测界面如下所示：



端口	状态	受保护	端口恢复时间(s)	受保护VLAN	环路VLAN	稳定发包间隔(s)	发包间隔 (s)
ge1	Down	No	300	-	-	10	1
ge2	Up	No	300	-	-	10	1
ge3	Down	No	300	-	-	10	1
ge4	Down	No	300	-	-	10	1
ge5	Down	No	300	-	-	10	1
ge6	Down	No	300	-	-	10	1
ge7	Down	No	300	-	-	10	1
ge8	Down	No	300	-	-	10	1
ge9	Down	No	300	-	-	10	1
ge10	Down	No	300	-	-	10	1
ge11	Down	No	300	-	-	10	1
ge12	Down	No	300	-	-	10	1
ge13	Down	No	300	-	-	10	1
ge14	Down	No	300	-	-	10	1
ge15	Down	No	300	-	-	10	1
ge16	Down	No	300	-	-	10	1
ge17	Down	No	300	-	-	10	1
ge18	Down	No	300	-	-	10	1
ge19	Down	No	300	-	-	10	1
ge20	Down	No	300	-	-	10	1

端口环路检测界面主要元素配置说明：

界面元素	说明
使能开关	端口环路检测全局使能配置。
端口	该设备以太网端口对应的端口号。
状态	该端口的连接状态，取值有： • Down：端口物理掉线 • Up：端口连接上 • Shutdown：端口关闭 • No Shutdown：端口未关闭
受保护	端口受保护状态，可显示如下： • Yes • No
端口恢复时间（s）	检测到环路后被 shutdown 的端口自动恢复正常的延迟时间，取值范围为 300-776000 秒。
受保护 VLAN	环路保护的 VLAN ID，取值范围为：1-4094，VLAN ID 个数≤16。 说明： 此参数必须配置，否则下发数据会报错。
环路 VLAN	当前产生环路的 VLAN ID。
稳定发包间隔（s）	正常发送环路检测数据包的间隔时间，取值范围为 10-300 秒。
发包间隔（s）	端口连接后，发送环路检测数据包的间隔时间。在该间隔内会向外发送 3 个检测报文，而后发包间隔恢复正常发包间隔。

5.11 IPDT

功能说明

配置 IPDT（IP-Detection）对指定的目的 IP 地址进行（ICMP）探测，并与其它功能进行联动，如 VRRP。

操作路径

按顺序依次打开：“二层配置 > IPDT”。

界面说明

IPDT 界面如下所示：

IPDT 界面主要元素配置说明：

界面元素	说明
IPDT ID	IPDT 会话 ID，取值范围 1-8。
状态	IPDT 功能使能状态。
源 IP	发送 ICMP 探测包的源 IP 地址。
目的 IP	ICMP 探测包的目的 IP 地址。
一次探测请求数	每一次探测所发送的请求包个数，取值范围为 1-3。
请求间隔（100ms）	每次探测请求的时间间隔，单位为 100ms，取值范围是 5-15。
对端设备状态	对端设备的状态，显示如下： • UP：对端设备正常在线。 • DOWN：对端设备无响应，可能设备掉线或链路故障。 • not be detected：未检测。
请求数	显示发送探测包的数量。
应答数	显示目的 IP 对探测包应答的数量。
请求失败	显示请求失败的数量。
其它应答数	显示其它设备对探测包应答的数量。

5.12 IPv6DT

功能说明

配置 IPv6DT（IPv6-Detection）对指定的目的 IPv6 地址进行（ICMPv6）探测，并与其它功能进行联动，如 IPv6 VRRP。

操作路径

按顺序依次打开：“二层配置 > IPv6DT”。

界面说明

IPv6DT 界面如下所示：

IPv6DT 界面主要元素配置说明：

界面元素	说明
IPV6DT ID	IPv6DT 会话 ID，取值范围 1-8。
状态	IPv6DT 功能使能状态。
源 IPv6	发送 ICMPv6 探测包的源 IPv6 地址。
目的 IPv6	ICMPv6 探测包的目的 IPv6 地址。
一次探测请求数	每一次探测所发送的请求包个数，取值范围为 1-3。
请求间隔（100ms）	每次探测请求的时间间隔，单位为 100ms，取值范围是 5-15。
对端设备状态	对端设备的状态，显示如下： • UP：对端设备正常在线。 • DOWN：对端设备无响应，可能设备掉线或链路故障。 • not be detected：未检测。
请求数	显示发送探测包的数量。
应答数	显示目的 IPv6 对探测包应答的数量。
请求失败	显示请求失败的数量。
其它应答数	显示其它设备对探测包应答的数量。

5.13 Smart-link

Smart Link，又叫做备份链路。一个 Smart Link 由两个接口组成，其中一个接口作为另一个的备份。Smart Link 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。

5.13.1 全局配置

功能说明

配置 Smart-link 相关参数。

操作路径

按顺序依次打开：“二层配置 > Smart-link > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
组 ID	Smart Link 组 ID，取值范围为 1-16。
发送控制 VLAN	发送控制 VLAN 是 Smart Link 组用于广播 Flush 报文的 VLAN，取值范围为 1-4094。当 Smart Link 发生链路切换后，Smart Link 通过发送 Flush 报文通知相关设备进行 MAC 表和 ARP 表项的刷新操作。 说明： • 若配置有发送控制 VLAN，则对端设备需配置接收控制 VLAN。 • 不同设备制造商可能对 Flush 报文格式的定义不同，建议在同一制造商的设备间使用该功能。
主端口	当 Smart Link 组中的两个接口都处于 Up 状态时，主接口将优先进入转发状态，而从接口将保持待命状态。 说明： Smart Link 组端口不可作为环网、汇聚组等成员端口。
从端口/优先级	• 从端口：Smart Link 组中的从接口在 Smart Link 组启动后会被阻塞。当主接口所在链路发生故障时，从接口将切换为转发状态。 • 优先级：从端口的优先级，取值范围为 1-63。优先级的值越小，优先级越高。
负载分担	负载分担实例 ID，取值范围为 0-16。在负载分担模式下，备份链路转发指定负载分担实例内所映射的 VLAN 数据流量，可以提高链路的利用率。
回切使能	当原主链路故障恢复后，为了保持流量稳定，它将维持在阻塞状态，不进行抢占。如果需要将其恢复为主链路，可以使能 Smart

界面元素	说明
	Link 组回切功能，在回切定时器超时后会自动倒换主链路。回切使能状态，可显示如下： • Enable：启用 • Disable：禁用
回切时间(s)	回切延迟时间，可抑制由于链路闪断导致的 Smart link 倒换，取值范围为 30-1200 秒。
主链路探测 VLAN	当链路中存在多个 VLAN 时，主链路探测需要对某 VLAN 的数据传输路径进行监控和故障检测，VLAN 的取值范围为 1-4094。
探测时间间隔(ms)	主链路对 VLAN 的数据传输路径进行实时监控和故障检测的探测时间间隔，取值范围为 10-10000ms，默认 10ms。
使能开关	Smart Link 功能使能状态，可显示如下： • Enable：启用 • Disable：禁用

5.13.2 接口配置

功能说明

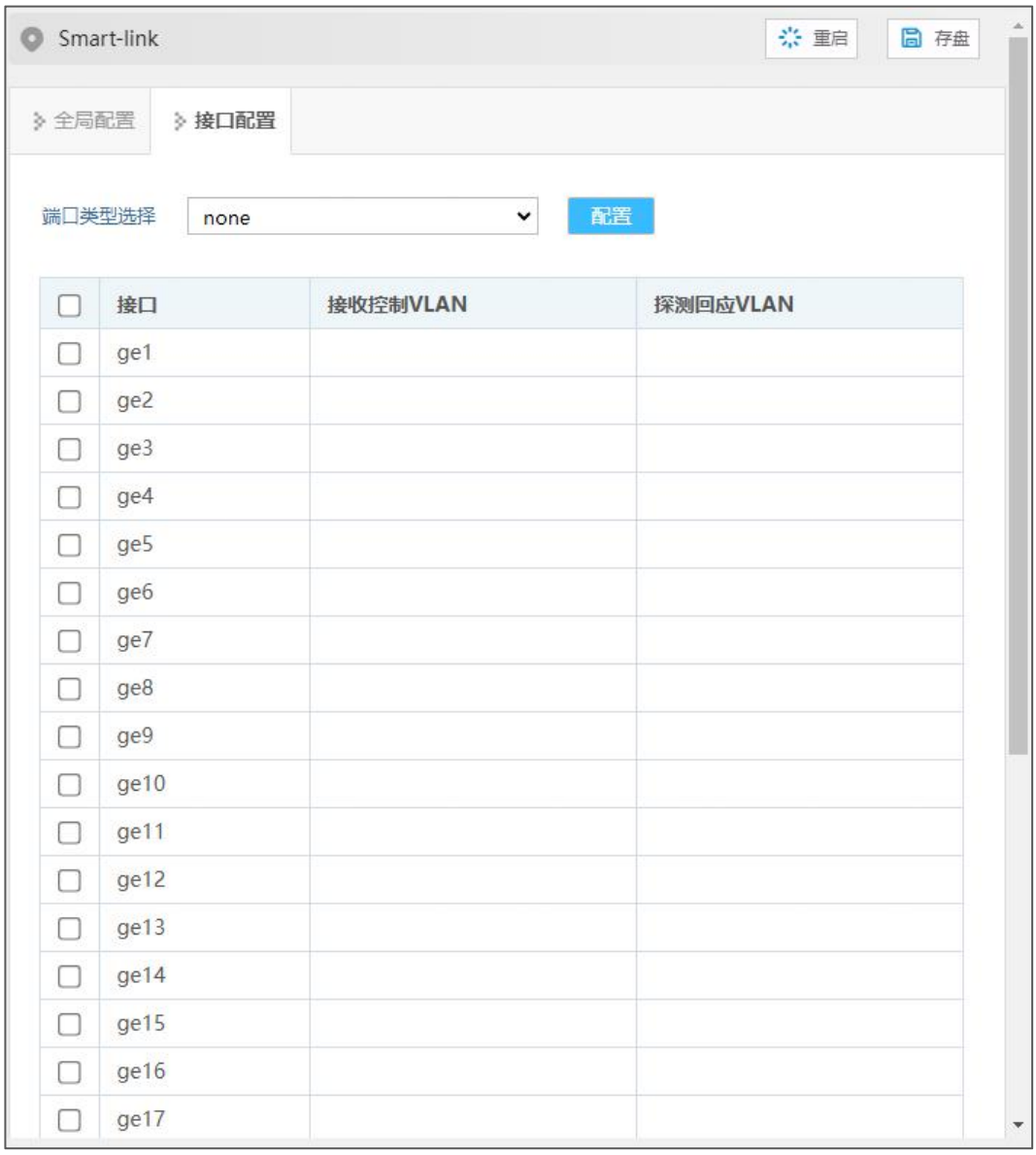
配置 Smart-link 接口接收控制 VLAN。

操作路径

按顺序依次打开：“二层配置 > Smart-link > 接口配置”。

界面说明

接口配置界面如下所示：



接口配置界面主要元素配置说明：

界面元素	说明
接口	该设备以太网端口对应的端口号。
接收控制 VLAN	接收控制 VLAN 是用于接收并处理 Flush 报文的 VLAN，取值范围为 1-4094。当 Smart Link 发生链路切换后，设备会处理收到的属于接收控制 VLAN 的 Flush 报文，进而刷新 MAC 表和 ARP 表。
探测回应 VLAN	在网络链路备份中，需要有一种机制来检测主链路的健康状态，这种探测机制可能通过发送特定的探测报文来实现。当探测报文被发送后，如果这些回应报文同样在特定的 VLAN 中处理和转发，探测和回应机制限制在特定的 VLAN 中进行，可以确保这些操作不会干扰到其他 VLAN 的正常通信。

6 IP 网络配置

6.1 接口

6.1.1 三层接口

功能说明

创建三层 VLANIF 接口，配置接口 IP 地址。

操作路径

按顺序依次打开：“IP 网络配置 > 接口 > 三层接口”。

界面说明

三层接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	VLANIF 接口，取值范围为 1-4094。VLANIF 接口是具有三层特性的逻辑接口，通过配置 VLANIF 接口的 IP 地址，可以实现 VLAN 间互访和部署三层业务。
状态	VLANIF接口的连接状态，可显示如下： • Up：已连接

界面元素	说明
	• Down：连接断开
主地址	VLANIF 接口的主 IPv4 地址和子网掩码，例如 192.168.1.1/24。
从地址	VLANIF 接口的从 IPv4 地址和子网掩码，例如 192.168.8.1/24。为了使交换机的一个接口能够与多个子网相连，可以在一个接口上配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址。
IPV6	VLANIF 接口的 IPv6 地址及前缀长度，例如 1::1/127。
接口开关	VLANIF 接口使能状态，可显示如下： • enable：启用 • disable：禁用

6.1.2 环回接口

环回接口是虚拟接口，大多数平台都支持使用这种接口模拟真正的接口。该接口为虚拟永远 UP 状态，比任何其他的物理接口更稳定，只要路由器启动，环回接口就处于活动状态。若有多条达到该环回地址的路由，不会因为该设备的一个接口 DOWN 掉而路由不可达，只有这个 router 失效时才会失效。

功能说明

配置环回接口的参数。

操作路径

按顺序依次打开：“IP 网络配置 > 接口 > 环回接口”。

界面说明

环回接口配置界面如下所示：

环回接口配置界面主要元素配置说明：

界面元素	说明
接口	环回接口名称，取值：loopback0 或 loopback1。

界面元素	说明
状态	环回接口的连接状态，可显示如下： • Up • Down
主地址	环回接口的主 IPv4 地址和子网掩码，例如 10.1.1.0/24。
IPV6	环回接口的 IPv6 地址及前缀长度，例如 1::1/127。
接口开关	环回接口使能状态，可显示如下： • enable：启用 • disable：禁用

6.2 ARP

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

在局域网中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报文必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。ARP 就是实现这个功能的协议。

6.2.1 ARP 信息

功能说明

通过 ARP 表项，查看下挂用户的 IP 地址、MAC 地址和接口等信息。

操作路径

按顺序依次打开：“IP 网络配置 > ARP > ARP 信息”。

界面说明

ARP 信息界面如下所示：

ARP 信息界面主要元素配置说明：

界面元素	说明
目的 IP	静态绑定或 ARP 解析动态学习的 IP 地址。
目的 MAC	静态绑定或 ARP 解析动态学习的 MAC 地址。
接口	ARP 表项所属的 VLANIF 接口。
类型	ARP 表项类型，可显示如下： • Static：静态 • Dynamic：动态
到期时间(s)	动态 ARP 表项的剩余存活时间，单位秒。
端口	学习到 ARP 表项的端口。

6.2.2 静态 ARP

功能说明

配置静态 ARP 表项，绑定 IP 地址和 MAC 地址，避免老化防止 ARP 攻击。

操作路径

按顺序依次打开：“IP 网络配置 > ARP > 静态 ARP”。

界面说明

静态 ARP 界面如下所示：

静态 ARP 界面主要元素配置说明：

界面元素	说明
IP	静态 ARP 表项的 IP 地址，如 192.168.1.1。
MAC	与静态 IP 地址绑定的 MAC 地址，如 0001.0001.0001。
接口	显示静态 ARP 表项所属的 VLANIF 接口。

6.2.3 ARP 参数配置

功能说明

配置动态 ARP 老化时间。

操作路径

按顺序依次打开：“IP 网络配置 > ARP > ARP 参数配置”。

界面说明

ARP 参数配置界面如下所示：

ARP 老化时间界面主要元素配置说明：

界面元素	说明
接口	显示 ARP 表项中 VLANIF 接口名称。
老化时间(s)	配置动态 ARP 表项老化时间，取值范围为 1-3000 秒。

6.3 NAT

NAT（Network Address Translation，网络地址转换）是将 IP 数据报头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问公共网络的功能。这种通过使用少量的公网 IP 地址代表较多的私网 IP 地址的方式，将有助于减缓可用 IP 地址空间的枯竭。

功能说明

添加或删除 NAT 条目，并设置设备的内网接口和外网接口。

操作路径

按顺序依次打开：“IP 网络配置 > NAT”。

界面说明

NAT 界面如下所示：

NAT 界面主要元素配置说明。

界面元素	说明
名称	NAT 条目名称，支持 1-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。
激活状态	NAT 规则是否被激活，状态如下： • up • down
内网接口	连接内网设备的 VLAN，接入这个 VLAN 的 IP，可以通过 NAT 访问公共网络。
内网 IP	能通过 NAT 映射到外网的内网 IP。
内网端口号	端口映射协议对应的内网 VLAN 的端口号。 说明： tcp/udp:1-65535/不填表示任意端口;all/icmp:不区分端口号。

界面元素	说明
外网接口	连接外网设备的 VLAN，通过这个 VLAN，可以通过 NAT 实现外网访问内网设备。
外网 IP	内网 IP 通过 NAT 映射到的外网 IP。
外网端口号	端口映射协议对应的外网 VLAN 的端口号。 说明： tcp/udp:1-65535/不填表示任意端口;all/icmp:不区分端口号。
协议	映射端口协议，可选项如下： • all：支持 tcp、udp 和 icmp 协议转发； • tcp：支持 tcp 协议转发； • udp：支持 udp 协议转发； • icmp：支持 icmp 协议转发。 说明： 选择 all 和 icmp 协议时，不支持输入内网端口和外网端口，请保持内网端口和外网端口为空。
VRID	VRID 即 VRRP ID，取值范围 1-255。当 VRRP 备份组的设备都配置了 NAT 地址池后，可能出现两台设备都对报文做 NAT 转换，导致冲突。配置 VRID 可以选择指定 Master 设备做 NAT 转换，有效避免冲突。
目的网络	内部终端设备对外通信的目的网络，即目的网络的 IP 地址及子网掩码，如 10.1.1.0/24。

7 单播路由

7.1 IPv4

7.1.1 IPv4 路由表

功能说明

查看 IPv4 路由表信息。

操作路径

按顺序依次打开：“单播路由 > IPv4 > IPv4 路由表”。

界面说明

IPv4 路由表界面如下所示：

IPv4 路由表界面主要元素配置说明：

界面元素	说明
目的 IP	目的IP地址。

界面元素	说明
目的 IP 掩码长度	目的子网掩码的长度大小。
协议类型	当前连接的路由协议类型。
下一跳	下一跳的网关地址信息。
出接口	接口名称。

7.1.2 IPv4 静态路由

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

功能说明

配置 IPv4 静态路由。

操作路径

按顺序依次打开：“单播路由 > IPv4 > IPv4 静态路由”。

界面说明

IPv4 静态路由配置界面如下所示：

IPv4 静态路由配置界面主要元素配置说明：

界面元素	说明
目的 IP 地址	目的网络 IP 地址，例如目的地址为 10.1.1.0。
目的 IP 掩码长度	目的 IP 掩码长度，取值范围：0-32。
下一跳	下一跳的网关地址，格式：不输入或者 192.3.3.3。
出接口	接口名称。
路由距离值	路由距离值是用于优先级判定，当路由器收到来自多个路由协

界面元素	说明
	议的路由信息时，它会根据这些路由信息的管理距离值来决定哪个路由信息应该被优先采用。管理距离值越小，表示该路由信息的可信度越高，路由器就越倾向于采用该路由信息。取值范围 1-255，默认值为 1。
标签	IPv4 静态路由标签，取值范围为 0-4294967295，默认值为 0。

7.2 IPv6

7.2.1 IPv6 路由表

功能说明

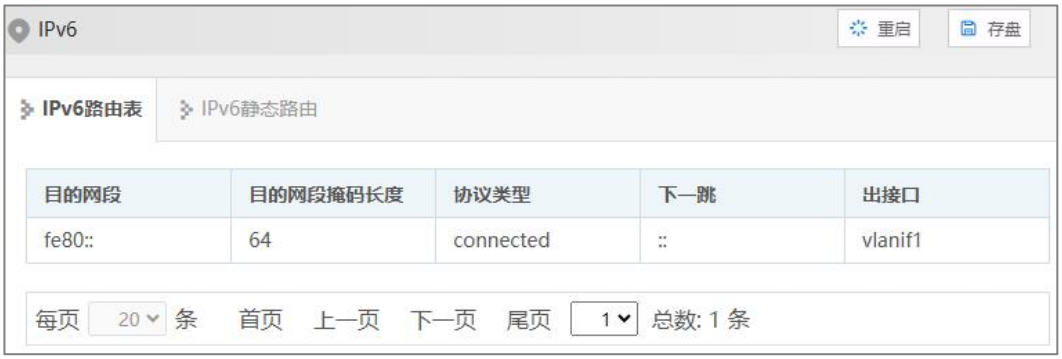
查看 IPv6 路由表信息。

操作路径

按顺序依次打开：“单播路由 > IPv6 > IPv6 路由表”。

界面说明

IPv6 路由表界面如下所示：



IPv4 路由表界面主要元素配置说明：

界面元素	说明
目的 IP	目的IP地址。
目的 IP 掩码长度	目的子网掩码的长度大小。
协议类型	当前连接的路由协议类型。
下一跳	下一跳的网关地址信息。
出接口	接口名称。

7.2.2 IPv6 静态路由

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

功能说明

配置 IPv6 静态路由。

操作路径

按顺序依次打开：“单播路由 > IPv6 > IPv6 静态路由”。

界面说明

IPv6 静态路由配置界面如下所示：

IPv6 静态路由配置界面主要元素配置说明：

界面元素	说明
目的 IP 地址	目的网络 IPv6 地址，例如目的地址为 0001::01。
目的 IP 掩码长度	目的 IPv6 掩码长度，取值范围：0-128。
下一跳	下一跳的网关地址，可以为空，IPv6 地址格式有以下类似两种： • 0001:0000:0000:0000:085b:3c51:f5ff:ffdb • 0001::01
网关接口名称	网关接口名称。
路由距离值	路由距离值是用于优先级判定，当路由器收到来自多个路由协议的路由信息时，它会根据这些路由信息的管理距离值来决定哪个路由信息应该被优先采用。管理距离值越小，表示该路由信息的可信度越高，路由器就越倾向于采用该路由信息。取值范围 1-255，默认值为 1。

7.3 RIP

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中，比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。

由于 RIP 的实现较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，因此在实际组网中仍有广泛的应用。

7.3.1 全局配置

功能说明

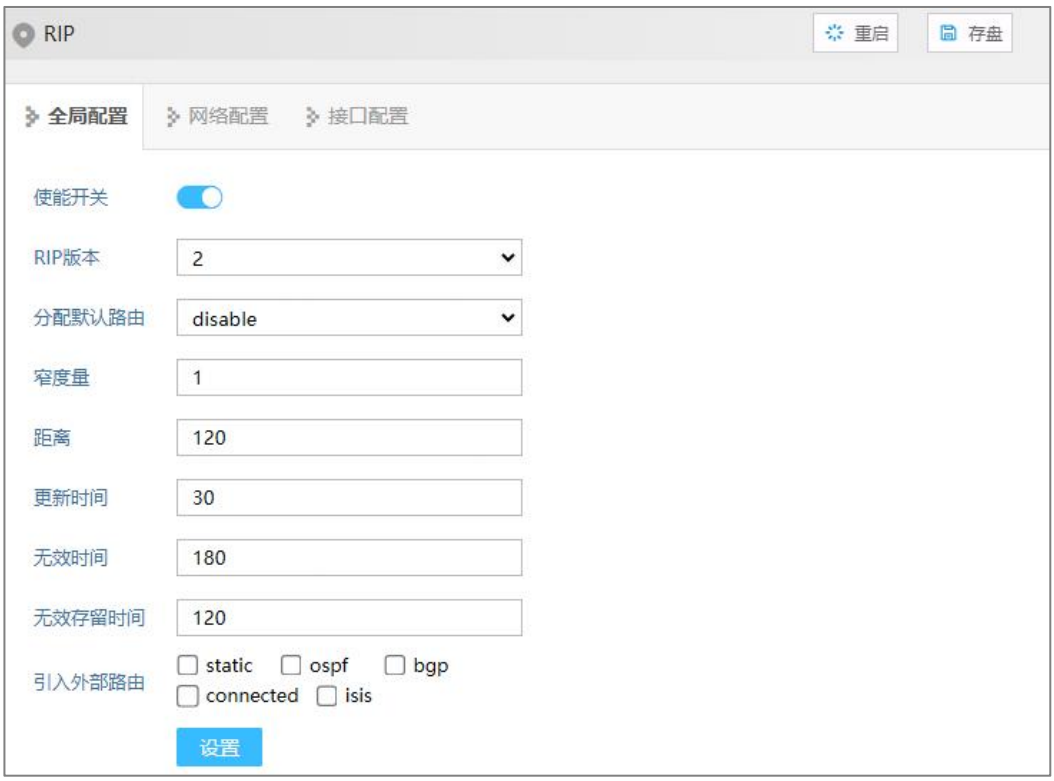
配置 RIP 全局相关参数。

操作路径

按顺序依次打开：“单播路由 > RIP > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
使能开关	RIP 功能使能开关。开启后，将出现 RIP 相关参数配置。

界面元素	说明
RIP 版本	RIP 版本下拉列表，默认版本为 RIP-2，版本可选项如下： • 1：RIP-1 是有类别路由协议，只支持以广播方式发布协议报文，只能识别 A、B、C 类这样的自然网段的路由。 • 2：RIP-2 是无分类路由协议，在 RIP-1 基础上进行了扩充。 说明： 接口只能发送/接收所配置 RIP 版本的数据报文。
分配默认路由器	分配目的地址为 0.0.0.0 的默认路由进入 RIP 路由数据库中，默认禁用，可选项如下： • enable：启用 • disable：禁止
窄度量	窄度量等于从本路由到达目的路由的设备数量，默认值为 1，取值范围 1-15。
距离	RIP 路由管理距离，默认距离为 120，取值范围为 1-255。当到达同一目的地存在来自于两个不同路由协议的路由时，路由协议的管理距离值越小，表明由该协议得到的路由越可靠。
更新时间	路由信息更新时间，当该定时器超时时，立即发送更新报文，默认每 30 秒发送一次更新报文。取值范围 5-2147483647 秒。 说明： 当路由信息发生变化时，立即向邻居设备发送触发更新报文，而不用等待更新定时器超时，从而避免产生路由环路。
无效时间	如果在无效时间内没有收到邻居发来的路由更新报文，则认为该路由不可达。默认为 180 秒，取值范围 5-2147483647 秒。
无效存留时间	如果在无效存留时间定时器倒计时结束前，不可达路由没有收到来自同一邻居的更新报文，则该路由将从 RIP 路由表中彻底被删除。默认为 120 秒，取值范围 5-2147483647 秒。
引入外部路由	引入外部路由从其它路由协议学习到的路由到 RIP 中，可选项如下： • static：静态路由 • ospf：开放式最短路径优先 • bgp：边界网关协议 • connected：直连路由 • isis：中间系统到中间系统 IS-IS 属于内部网关协议

7.3.2 网络配置

功能说明

配置 RIP 工作网段。

操作路径

按顺序依次打开：“单播路由 > RIP > 网络配置”。

界面说明

网络配置界面如下所示：

网络配置界面主要元素配置说明：

界面元素	说明
网络	运行 RIP 协议的网段。

7.3.3 接口配置

功能说明

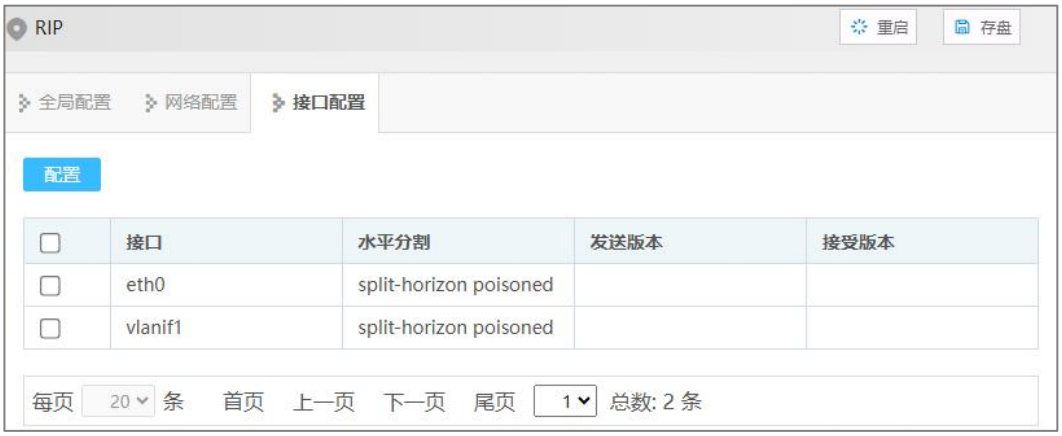
配置 RIP 接口参数。

操作路径

按顺序依次打开：“单播路由 > RIP > 接口配置”。

界面说明

接口配置界面如下所示：



接口配置界面主要元素配置说明：

界面元素	说明
接口	RIP 接口信息。
水平分割	水平分割，可选项如下： • - • Split-horizon：水平分割。RIP 从某个接口学到的路由，不会从该接口再发回给邻居路由器。 • Poison-reverse：毒性反转。RIP 从某个接口学到路由后，将该路由的开销值设置为不可达，并从原接口发回邻居设备。
发送版本	发送数据的 RIP 协议版本，可选项如下： • - • 1 • 2 • 1 & 2 • 1-compatible
接受版本	接收数据的 RIP 协议版本，可选项如下： • - • 1 • 2 • 1 & 2

7.4 RIPNG

RIPng（RIP next generation，下一代 RIP 协议）是一种较为简单的内部网关协议，是 RIP 在 IPv6 网络中的应用。

7.4.1 全局配置

功能说明

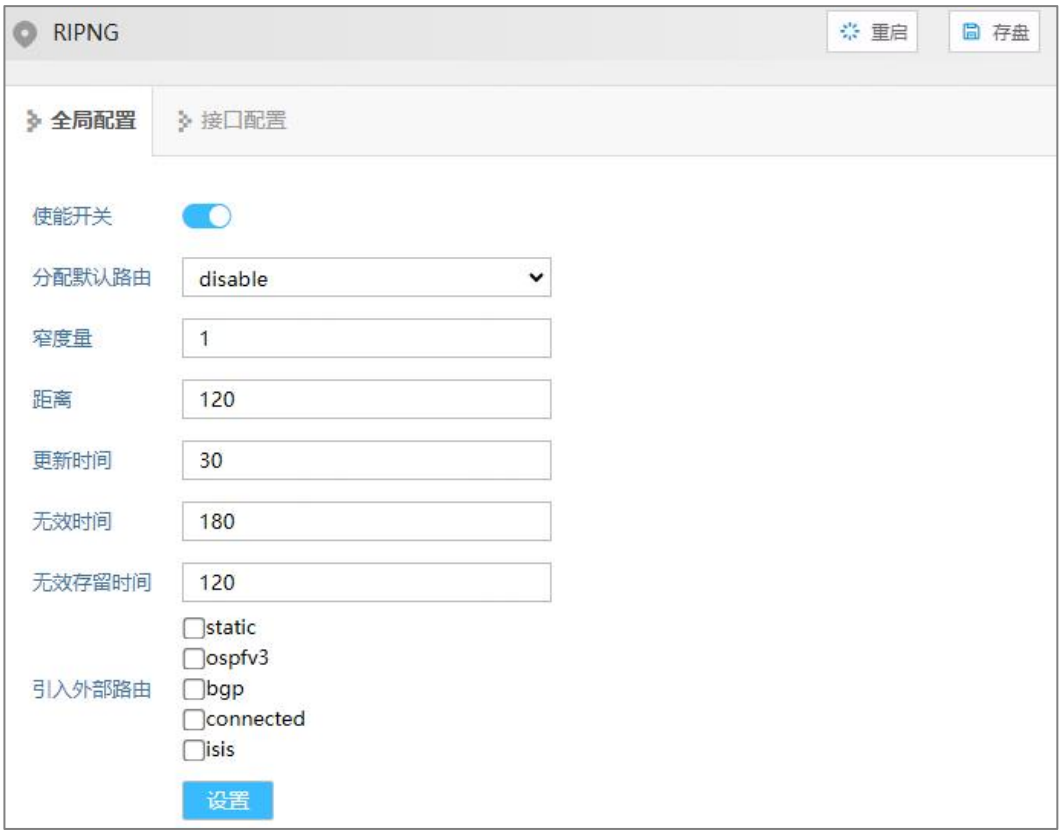
配置 RIPng 全局参数。

操作路径

按顺序依次打开：“单播路由 > RIPNG > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
使能开关	RIPng 使能开关，启用后，出现 RIPng 相关参数配置。
分配默认路由器	发布 RIPng 缺省路由（::/0），可选项如下： • enable：启用 • disable：禁止 说明： 当报文的目的地址不能与路由表的任何目的地址相匹配时，路由器将选取缺省路由转发该报文。
窄度量	引入外部路由协议的路由至 RIPng 时使用的缺省度量值。度量值

界面元素	说明
	等于从本路由到达目的路由的设备数量，默认值为 1，取值范围 1-16。
距离	RIPng 路由管理距离，默认距离为 120，取值范围为 1-255。当到达同一目的地存在来自于两个不同路由协议的路由时，路由协议的管理距离值越小，表明由该协议得到的路由越可靠。
更新时间	路由信息更新时间，当该定时器超时时，立即发送更新报文，默认每 30 秒发送一次更新报文。取值范围 5-2147483647 秒。 说明： 当路由信息发生变化时，立即向邻居设备发送触发更新报文，而不用等待更新定时器超时，从而避免产生路由环路。
无效时间	如果在无效时间内没有收到邻居发来的路由更新报文，则认为该路由不可达。默认为 180 秒，取值范围 5-2147483647 秒。
无效存留时间	如果在无效存留时间定时器倒计时结束前，不可达路由没有收到来自同一邻居的更新报文，则该路由将从 RIPng 路由表中彻底被删除。默认为 120 秒，取值范围 5-2147483647 秒。
引入外部路由	引入外部路由从其它路由协议学习到的路由到 RIPng 中，可选项如下： • static：静态路由 • ospfv3：OSPFv3 路由 • bgp：BGP 边界网关协议 • connected：直连路由 • isis：外部网关协议

7.4.2 接口配置

功能说明

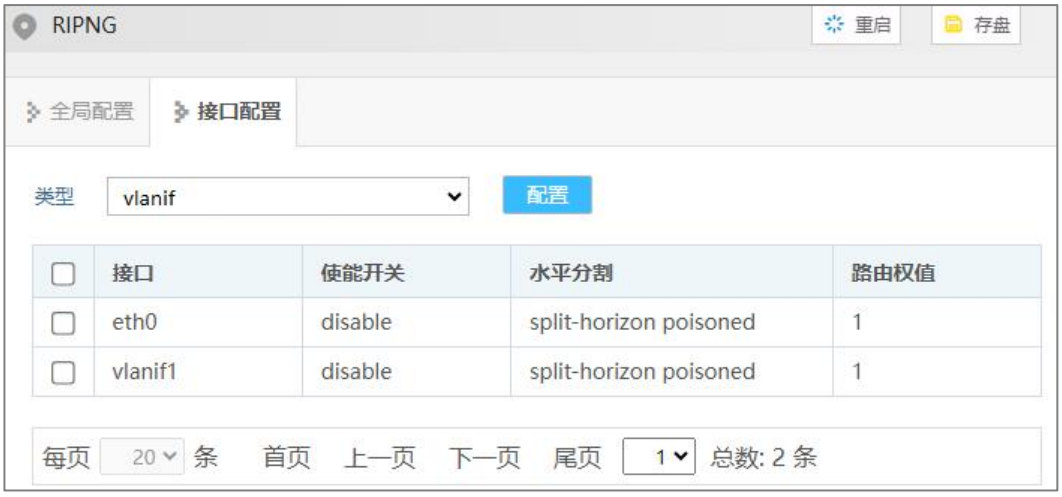
配置 RIPng 接口参数。

操作路径

按顺序依次打开：“单播路由 > RIPNG > 接口配置”。

界面说明

接口配置界面如下所示：



接口配置界面主要元素配置说明：

界面元素	说明
接口	RIPng 接口信息。
使能状态	RIPng 使能状态，可选项如下： • Disable：禁用 • Enable：启用
水平分割	水平分割，可选项如下： • Split-horizon：水平分割。RIPng 从某个接口学到的路由，不会从该接口再发回给邻居路由器。 • Split-horizon poisoned：带毒性反转的水平分割。RIPng 从某个接口学到路由后，将该路由的开销值设置为不可达，并从原接口发回邻居设备。
路由权值	附加路由度量值，取值范围为 1-16。在 RIPng 路由原来度量值的基础上所增加的度量值（跳数），可影响路由的选择。

7.5 OSPF

开放式最短路径优先 OSPF（Open Shortest Path First）是 IETF 组织开发的一个基于链路状态的内部网关协议（Interior Gateway Protocol）。

目前针对 IPv4 协议使用的是 OSPF Version 2（RFC2328）。

- OSPF把自治系统AS（Autonomous System）划分成逻辑意义上的一个或多个区域；
- OSPF通过LSA（Link State Advertisement）的形式发布路由；
- OSPF依靠在OSPF区域内各设备间交互OSPF报文来达到路由信息的统一；
- OSPF报文封装在IP报文内，可以采用单播或组播的形式发送。

由于 RIP 是基于距离矢量算法的路由协议，存在着收敛慢、路由环路、可扩展性差等问题，OSPF 成为了网络上使用最广泛的 IGP 协议。

OSPF 作为基于链路状态的协议，能够解决 RIP 所面临的诸多问题。此外，OSPF 还有以下优点：

- OSPF采用组播形式收发报文，这样可以减少对其它不运行OSPF路由器的影响。
- OSPF支持无类型域间选路（CIDR）。
- OSPF支持对等价路由进行负载分担。
- OSPF支持报文认证。

7.5.1 全局配置

功能说明

配置 OSPF 进程 ID、路由器 ID、默认路由和引入外部路由等信息。

操作路径

按顺序依次打开：“单播路由 > OSPF > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
进程 ID	OSPF 进程 ID，取值范围 0-65535。OSPF 支持多进程，在同一台路由器上可以运行多个不同的 OSPF 进程，它们之间互不影响，彼此独立。路由器的一个接口只能调用一个 OSPF 进程。
路由器 ID	路由器 ID 是用于在自治系统中唯一标识一台运行 OSPF 的路由器，ID 格式和 IP 地址的格式一样。每个运行 OSPF 的路由器都有一个

界面元素	说明
	路由器 ID。
分配默认路由	默认路由是指目的地址和掩码都是 0 的路由。当设备无精确匹配的路由时，就可以通过默认路由进行报文转发。
引入外部路由	引入其它路由协议学习到的路由到 OSPF 路由表中，适用于自治系统边界路由器。外部路由描述了如何选择到 AS 以外目的地址的路由。 • connected：直连路由 • static：静态路由 • rip：RIP 路由 • bgp • isis

7.5.2 网络配置

功能说明

配置设备的各个网络接口所属 OSPF 区域。

操作路径

按顺序依次打开：“单播路由 > OSPF > 网络配置”。

界面说明

网络配置界面如下所示：

网络配置界面主要元素配置说明：

界面元素	说明
进程 ID	OSPF 进程 ID，取值范围 1-65535。

界面元素	说明
IP	OSPF 进程的网络地址，或网络地址/网络前缀。
通配符	网络地址的通配符。
区域	设置网络接口所属的 OSPF 区域，OSPF 区域的标识支持 IP 地址格式或 0-4294967295 范围的整数值。

7.5.3 接口配置

功能说明

配置设备接口的开销、失效时间、Hello 间隔和 DR 优先级。

操作路径

按顺序依次打开：“单播路由 > OSPF > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	设备的 VLANIF 接口。
开销	接口上运行 OSPF 协议所需的开销，取值范围 1-65535。
邻居失效时间（s）	OSPF 邻居的失效时间，单位为秒，取值范围 1-65535。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。如果相邻两台路由器的失效时间不同，则不能建立邻居关系。
HELLO 间隔(s)	接口发送 Hello 报文的时间间隔，单位为秒，取值范围 1-65535。Hello 报文周期性的发送给邻居路由器用来维持邻居关系以及 DR（Designated Router）/BDR（Backup Designated Router）的选举。

界面元素	说明
DR 优先级	接口的 DR 优先级，取值范围为 1-255。DR 优先级决定了该接口在选举 DR/BDR 时所具有的资格，数值越大，优先级越高。优先级高的在选举权发生冲突时被首先考虑。
网络类型	OSPFv3 接口的网络类型，对应不同类型的链路层协议，网络类型如下： • Broadcast：广播类型 • Non-broadcast：非广播点到多点 NBMA 类型 • Point-to-multipoint：点到多点 P2M 类型 • Point-to-point：点到点 P2P 类型

7.6 OSPFV3

OSPFv3 是运行于 IPv6 的 OSPF 路由协议，在 OSPFv2 基础上进行了修改，是一个独立的路由协议。

7.6.1 全局配置

功能说明

配置 OSPFv3 进程 ID、路由器 ID、默认路由和引入外部路由等信息。

操作路径

按顺序依次打开：“单播路由 > OSPFV3 > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
进程标识	OSPFv3 进程标识。OSPFv3 支持多进程，在同一台路由器上可以运行多个不同的 OSPFv3 进程，它们之间互不影响，彼此独立。
路由器 ID	路由器 ID 是用于在自治系统中唯一标识一台运行 OSPFv3 的路由器。ID 格式和 IP 地址的格式一样。每个 OSPFv3 进程都有一个路由器 ID。
分配默认路由	默认路由是指目的地址和掩码都是 0 的路由。当设备无精确匹配的路由时，就可以通过默认路由进行报文转发。
引入外部路由	引入其它路由协议学习到的路由到 OSPFv3 路由表中，适用于自治系统边界路由器。外部路由描述了如何选择到 AS 以外目的地址的路由。 • connected：直连路由 • static：静态路由 • rip：RIP/RIPng 路由信息协议 • bgp：BGP 边界网关协议 • isis：IS-IS 中间系统到中间系统

7.6.2 接口配置

功能说明

配置设备接口的开销、失效时间、Hello 间隔和 DR 优先级。

操作路径

按顺序依次打开：“单播路由 > OSPFV3 > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明

界面元素	说明
接口	设备的 VLANIF 接口。
进程标识	OSPFv3 进程标识。
区域	OSPFv3 区域的 ID，取值范围为 0-4294967295 或 IPv4 地址格式。OSPFv3 协议把自治系统划分成逻辑意义上的一个或多个区域，通过区域内各设备间交互 OSPFv3 报文来达到路由信息的统一。
实例 ID	接口所属的实例 ID。OSPFv3 支持一个链路上多个进程，一个物理接口可以和多个多实例绑定，并用不同的 Instance ID 区分。
开销	接口上运行 OSPF 协议所需的开销，取值范围 1-65535。
邻居失效时间	OSPF 邻居的失效时间，单位为秒，取值范围 1-65535。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。如果相邻两台路由器的失效时间不同，则不能建立邻居关系。
HELLO 间隔	接口发送 Hello 报文的时间间隔，单位为秒，取值范围 1-65535。Hello 报文周期性的发送给邻居路由器用来维持邻居关系以及 DR（Designated Router）/BDR（Backup Designated Router）的选举。
DR 优先级	接口的 DR 优先级，取值范围为 1-255。DR 优先级决定了该接口在选举 DR/BDR 时所具有的资格，数值越大，优先级越高。优先级高的在选举权发生冲突时被首先考虑。
网络类型	OSPFv3 接口的网络类型，对应不同类型的链路层协议，网络类型如下： • Broadcast：广播类型 • Non-broadcast：非广播点到多点 NBMA 类型 • Point-to-multipoint：点到多点 P2M 类型 • Point-to-point：点到点 P2P 类型

7.7 ISIS

中间系统到中间系统 IS-IS（Intermediate System to Intermediate System）属于内部网关协议 IGP（Interior Gateway Protocol），用于自治系统内部。IS-IS 也是一种链路状态协议，使用最短路径优先 SPF（Shortest Path First）算法进行路由计算。

7.7.1 全局配置

功能说明

配置 IS-IS 全局参数。

操作路径

按顺序依次打开：“单播路由 > ISIS > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明
标识	IS-IS 进程标识。IS-IS 支持多进程，在同一台路由器上可以运行多个不同的 IS-IS 进程，它们之间互不影响，彼此独立。
类型	IS-IS 设备的类型，可选项如下： • Level-1：设备只与属于同一区域的 Level-1 和 Level-1-2 设备形成邻居关系，并且只负责维护 Level-1 的链路状态数据库 LSDB。 • Level-2：设备可以与同一或者不同区域的 Level-2 设备或者其它区域的 Level-1-2 设备形成邻居关系，并且只维护一个 Level-2 的 LSDB。 • Level-1-2：设备会为 Level-1 和 Level-2 分别建立邻居，分别维护 Level-1 和 Level-2 两份 LSDB。
网络	IS-IS 进程的网络实体名称 NET（Network Entity Title），格式为 X…X.XXXX.XXXX.XXXX.00，前面的“X…X”是区域地址，中间的 12 个“X”是设备的系统 ID，最后的“00”是 SEL。 说明： • 区域地址用来唯一标识路由域中的不同区域，同一 Level-1 区域内所有交换机必须具有相同的区域地址，Level-2 区域内的交换机可以具有不同的区域地址。 • 在整个区域和骨干区域中，要求保持系统 ID 唯一。
引入外部路由	引入其它路由协议学习到的路由到 IS-IS 路由表中，适用于边界路由器。实现 IS-IS 路由域内的流量到达 IS-IS 路由域外。 • connected：直连路由

界面元素	说明
	• static：静态路由 • ospf：OSPF 开放式最短路径优先 • bgp：BGP 边界网关协议 • rip：RIP 路由信息协议 • isis level-2 into level-1：从 Level-2 向 Level-1 进行路由渗透

7.7.2 接口配置

功能说明

配置 IS-IS 接口参数。

操作路径

按顺序依次打开：“单播路由 > ISIS > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	设备的 VLANIF 接口。
标识	IS-IS 进程标识。
窄度量	窄度量是 IS-IS 接口开销的默认度量值计算方式。默认是 10，取值范围为 1-63。
宽度量	宽度量是 IS-IS 接口开销的扩展度量值计算方式。默认是 10，取值范围为 1-16777214。 说明： 在 IS-IS 路由协议全局配置中，默认采用的是“窄度量”模式进行接口开销计算，此处的“宽度量”仅作为一种信息展示存在，并未

界面元素	说明
	启用实际的宽度量计算功能。
电路类型	IS-IS 设备接口的电路类型，可选项如下： • Level-1：设备只与属于同一区域的 Level-1 和 Level-1-2 设备形成邻居关系，并且只负责维护 Level-1 的链路状态数据库 LSDB。 • Level-2：设备可以与同一或者不同区域的 Level-2 设备或者其它区域的 Level-1-2 设备形成邻居关系，并且只维护一个 Level-2 的 LSDB。 • Level-1-2：设备会为 Level-1 和 Level-2 分别建立邻居，分别维护 Level-1 和 Level-2 两份 LSDB。
HELLO 间隔（s）	接口发送 Hello 报文的时间间隔，单位为秒，取值范围 1-65535。Hello 报文周期性的发送给邻居路由器用来维持邻居关系。
HELLO 乘数	邻居保持时间即 Hello 报文的发送间隔时间的倍数，取值范围为 2-100。如果在邻居保持时间内，链路一端的设备没有接收到对端设备发送的 Hello 报文，则认为对端邻居失效。
网络	IS-IS 接口的网络类型，对应不同类型的链路层协议，网络类型如下： • Broadcast：广播类型 • Point-to-point：点到点 P2P 类型
优先级	接口的 DIS 优先级，默认是 64，取值范围为 1-127。DIS 优先级决定了该接口在选举 DIS 时所具有的资格，数值越大，优先级越高。

7.8 VRRP

虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，将虚拟路由设备的 IP 地址作为用户的默认网关实现与外部网络通信。当网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。VRRP 协议包括两个版本：VRRPv2 和 VRRPv3。VRRPv2 仅适用于 IPv4 网络，VRRPv3 适用于 IPv4 和 IPv6 两种网络。

功能说明

配置 IPv4 VRRP 参数。

操作路径

按顺序依次打开：“单播路由 > VRRP”。

界面说明

VRRP 界面如下所示：

VRRP 界面主要元素配置说明：

界面元素	说明
VRID	虚拟路由 ID，有效范围为 1-255。
三层接口	三层接口信息，例如：vlanif1。
状态	当前的状态，可选项有： • Init • Master • Backup
虚拟 IP	虚拟路由IP地址，如192.168.1.253。
Ip 地址拥有者	IP地址拥有者将虚拟路由器IP地址作为真实的接口地址。
优先级	优先级默认 100，有效范围为 1-255。 说明： 当配置了 IP 地址拥有者后，优先级默认只能为 255。
通告时间间隔（厘秒）	VRRP 备份组中的 Master 路由器会定时发送 VRRP 通告报文，通知备份组内的路由器自己工作正常，单位：厘秒，有效范围为 5-4095（5 的倍数）。
抢占模式	在抢占方式下，一旦备份组中的路由器发现自己的优先级比当前的 Master 路由器的优先级高，就会对外发送 VRRP 通告报文。导致备份组内路由器重新选举 Master 路由器，并最终取代原有的 Master 路由器。相应地，原来的 Master 路由器将会变成 Backup 路由器。抢占模式，可选项如下： • false • true
IPDT ID	IPDT ID 取值范围是 1-8。
类型	IPDT 优先级类型，可选项如下： • Increased：启用“Track”后，当 IPDT 链路发生故障时，VRRP 优先级值等于原有 VRRP 优先级值加上 IPDT 优先级值。 • Reduced：启用“Track”后，当 IPDT 链路发生故障时，

界面元素	说明
	VRRP 优先级值等于原有 VRRP 优先级值减去 IPDT 优先级值。
IPDT 优先级	IPDT 优先级，取值范围是 1-253。
使能开关	VRRP 使能状态，可选项如下： • enable：启用 • disable：禁用

7.9 IPv6 VRRP

功能说明

配置 IPv6 VRRP 参数。

操作路径

按顺序依次打开：“单播路由 > IPv6 VRRP”。

界面说明

IPv6 VRRP 界面如下所示：

IPv6 VRRP 界面主要元素配置说明：

界面元素	说明
VRID	虚拟路由 ID，有效范围为 1-255。
三层接口	三层接口信息，例如：vlanif1。
状态	当前的状态，可选项有： • Init • Master • Backup
虚拟 IP	虚拟路由IPv6地址，链路本地地址范围内的地址，如fe80::1。
Ip 地址拥有者	IP地址拥有者将虚拟路由器IP地址作为真实的接口地址。
通告时间间隔	VRRP 备份组中的 Master 路由器会定时发送 VRRP 通告报文，通知备份组内的路由器自己工作正常，单位：厘秒，有效范围为 5-4095（5 的倍数）。

界面元素	说明
优先级	优先级默认 100，有效范围为 1-255。 说明： 当配置了 IP 地址拥有者后，优先级默认只能为 255。
抢占模式	在抢占方式下，一旦备份组中的路由器发现自己的优先级比当前的 Master 路由器的优先级高，就会对外发送 VRRP 通告报文。导致备份组内路由器重新选举 Master 路由器，并最终取代原有的 Master 路由器。相应地，原来的 Master 路由器将会变成 Backup 路由器。抢占模式，可选项如下： • false • true
抢占延时	设置 VRRP 备份组的抢占时延，可以避免备份组内的成员频繁进行主备状态转换。有效范围为 0-255s，缺省 0s。
使能开关	VRRP 使能状态，可选项如下： • enable：启用 • disable：禁用

8 组播路由

8.1 组播路由

8.1.1 组播路由开关

功能说明

开启或关闭三层 IPv4 组播路由功能。

操作路径

按顺序依次打开：“组播路由 > 组播路由 > 组播路由开关”。

界面说明

组播路由开关界面如下所示：

组播路由开关界面主要元素配置说明：

界面元素	说明
使能开关	单击按钮开启或关闭组播路由功能，向右滑动开启，向左滑动关闭。

8.1.2 组播路由信息

功能说明

查看三层组播路由信息。

操作路径

按顺序依次打开：“组播路由 > 组播路由 > 组播路由信息”。

界面说明

组播路由信息界面如下所示：

组播路由信息界面主要元素配置说明：

界面元素	说明
源地址	组播源地址。
组地址	组播组地址。
启动时间	组播路由已存在的时间。
老化时间	组播路由老化时间。
拥有者	组播路由的拥有者，可能是某个组播路由协议。
标志	组播路由协议标志： • I：Immediate Stat（立即统计） • T：Timed Stat（定时统计） • F：Forwarder installed（已设置到转发表）
入口接口	组播数据入接口，本地设备上接收到组播数据的接口。
出口接口（TTL）	组播数据出接口，将组播数据转发出去的接口。

8.2 IPv6 组播路由

8.2.1 组播路由开关

功能说明

全局使能 IPv6 三层组播路由功能。使能组播路由功能之后，可配 PIM（IPv6）、MLD 等一些 IPv6 三层组播协议以及其它 IPv6 三层组播功能。

操作路径

按顺序依次打开：“组播路由 > IPv6 组播路由 > 组播路由开关”。

界面说明

组播路由开关界面如下所示：

组播路由开关界面主要元素配置说明：

界面元素	说明
使能开关	IPv6 三层组播路由使能开关。

8.2.2 组播路由信息

功能说明

查看三层组播路由信息。

操作路径

按顺序依次打开：“组播路由 > IPV6 组播路由 > 组播路由信息”。

界面说明

组播路由信息界面如下所示：

组播路由信息界面主要元素配置说明：

界面元素	说明
源地址	组播源地址。
组地址	组播组地址。
启动时间	组播路由已存在的时间。
老化时间	组播路由老化时间。
拥有者	组播路由的拥有者，可能是某个组播路由协议。
标志	组播路由协议标志： • I：Immediate Stat（立即统计） • T：Timed Stat（定时统计） • F：Forwarder installed（已设置到转发表）
入口接口	组播数据入接口，本地设备上接收到组播数据的接口。
出口接口（TTL）	组播数据出接口，将组播数据转发出去的接口。

8.3 IGMP

8.3.1 接口配置

功能说明

配置 VLANIF 接口的 IGMP 参数。

操作路径

按顺序依次打开：“组播路由 > IGMP > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	三层接口，例如 vlanif1。
IGMP	IGMP 状态： • enable • disable
版本	IGMP 的版本，可选项为： • 1：IGMPv1，定义了基本的组成员查询和报告过程； • 2：IGMPv2，在 IGMPv1 上添加了查询器选举和组成员离开的机制； • 3：IGMPv3，在 IGMPv2 上添加了成员可以指定接收或指定不接收某些组播源的报文。
丢弃未携带 RA	RA（Router-Alert）路由器警告，网络设备收到报文时，只有目的 IP 地址为本设备接口地址的报文才会上送给相应的协议模块处理。如果协议报文的目的地址不是本设备的接口地址，则检查 IP 报文头中是否携带 Router-Alert 选项，如果携带会直接上送给相应的协议模块处理，而不检查目的地址。 说明： 出于兼容性考虑，当前交换机在收到 IGMP 报文后，无论其 IP 报文头是否包含 Router-Alert 选项，缺省情况下都会上送给 IGMP 协议模块处理。
不限制同一子网	限制组播源和接口在同一个子网，否则端口不能接收组播报文。
健壮性系数	指定 IGMP 查询器的健壮系数，取值范围为 2-7。该系数用来规定 IGMP 查询器在启动时发送普遍组查询报文次数的缺省值，以及 IGMP 查询器在收到离开组报文后发送特定组查询报文的次数。
其它查询器时间	非查询器的定时器时间。 • 在该定时器超时前，如果收到了来自查询器的查询报文，则重置该定时器； • 否则，就认为原查询器失效，并发起新的查询器选举过程。
快速离开 ACL	缺省情况下，接口工作在 IGMP v2 或 v3 时，收到 IGMP 离开报文

界面元素	说明
	后，会先发送特定组查询报文，以确定是否老化组播成员表项。配置了快速离开 ACL 后，如果离开报文所指定的组地址在 ACL 指定的组地址范围内，则可以马上老化组播成员表项。
非法组播 ACL	限制加入的组播组列表。
组播组 Max	支持的最大组播数。

8.3.2 SSM-Map 配置

SSM（Source-Specific Multicast）称为指定源组播，要求路由器能了解成员主机加入组播组时所指定的组播源。如果成员主机上运行 IGMPv3，可以在 IGMPv3 报告报文中直接指定组播源地址。但是某些情况下，成员主机只能运行 IGMPv1 或 IGMPv2，为了使其也能够使用 SSM 服务，路由器上需要提供 IGMP SSM Mapping 功能。

IGMP SSM Mapping 的机制是：通过在路由器上静态配置 SSM 地址的映射规则，将 IGMPv1 和 IGMPv2 报告报文中的信息转化为对应的信息，以提供 SSM 组播服务。

配置了 SSM Mapping 规则后，当 IGMP 查询器收到来自成员主机的 IGMPv1 或 IGMPv2 报告报文时，首先检查该报文中所携带的组播组地址，然后根据检查结果的不同分别进行处理。

- 如果该组播组在ASM（Any-Source Multicast）范围内，则只提供ASM服务。
- 如果该组播组在SSM组地址范围内（缺省情况下为232.0.0.0～232.255.255.255）：
  - 如果路由器上没有该组播组对应的 SSM Mapping 规则，则无法提供 SSM 服务，丢弃该报文。
  - 如果路由器上有该组播组对应的 SSM Mapping 规则，则依据规则将报告报文中所包含的（成员，组播组）信息映射为（组播组，INCLUDE，成员）信息，提供 SSM 服务。

功能说明

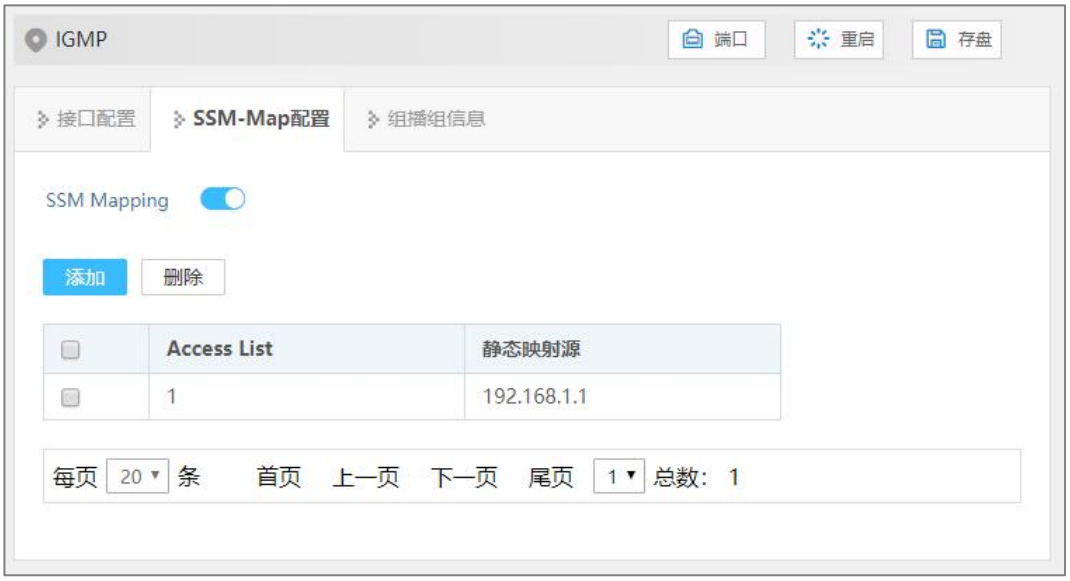
配置 SSM Mapping 规则。

操作路径

按顺序依次打开：“组播路由 > IGMP > SSM-Map 配置”。

界面说明

SSM-Map 配置界面如下所示：



SSM-Map 配置界面主要元素配置说明：

界面元素	说明
SSM Mapping	IGMP SSM Mapping 使能开关。
Access List	接入列表。
静态映射源	接入列表内的指定组播源地址。

8.3.3 组播组信息

功能说明

显示设备接口接收到的组播信息。

操作路径

按顺序依次打开：“组播路由 > IGMP >组播组信息”。

界面说明

组播组信息界面如下所示：

组播组信息界面主要元素配置说明：

界面元素	说明
接口	以太网接口。
组播地址	接口接收到的组播地址。
类型	组播类型： • dynamic：动态 • static：静态

8.4 IPv6 MLD

组播侦听者发现协议 MLD（Multicast Listener Discovery）是负责 IPv6 组播成员管理的协议，用来在 IPv6 成员主机和与其直接相邻的组播路由器之间建立和维护组播组成员关系。MLD 通过在成员主机和组播路由器之间交互 MLD 报文实现组成员管理功能，MLD 报文封装在 IPv6 报文中。

8.4.1 接口配置

功能说明

配置 VLANIF 接口的 MLD 参数。

操作路径

按顺序依次打开：“组播路由 > IPv6 MLD > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	三层接口，例如 vlanif1。
使能状态	MLD 使能状态，可显示如下： • enable • disable
版本	MLD 的版本，可选项为： • 1：MLDv1 的工作机制与 IGMPv2 相同。 • 2：MLDv2 在 MLDv1 的基础上，增加的主要功能是成员主机可以指定接收或不接收某些组播源的报文，对应 IGMPv3。
健壮性系数	指定 MLD 查询器的健壮系数，取值范围为 2-7。该系数用来规定 MLD 查询器在启动时发送普遍组查询报文次数的缺省值，以及 MLD 查询器在收到离开组报文后发送特定组查询报文的次数。
其它查询器时间（s）	其他 MLD 查询器的存活时间。如果非查询器在“其他 MLD 查询器的存活时间”内收不到查询报文，就认为查询器失效，自动发起查询器选举。
快速离开 ACL	缺省情况下，收到 MLD 离开报文后，会先发送特定组查询报文，以确定是否老化组播成员表项。配置了快速离开 ACL 后，如果离开报文所指定的组地址在 ACL 指定的组地址范围内，则可以马上老化组播成员表项。
非法组播 ACL	限制加入的组播组列表。
组播组 Max	支持的最大组播数。

8.4.2 SSM-Map 配置

SSM（Source-Specific Multicast）称为指定源组播，要求路由器能了解成员主机加入组播组时所指定的组播源。如果成员主机上运行 MLDv2，可以在 MLDv2 报告报文中直

接指定组播源地址。但是某些情况下，成员主机只能运行 MLDv1，为了使其也能够使用 SSM 服务，组播路由器上需要提供 MLD SSM Mapping 功能。

功能说明

配置 MLD SSM Mapping 规则。

操作路径

按顺序依次打开：“组播路由 > IPv6 MLD > SSM-Map 配置”。

界面说明

SSM-Map 配置界面如下所示：

SSM-Map 配置界面主要元素配置说明：

界面元素	说明
SSM Mapping	MLD SSM Mapping 使能开关。
Access List	接入列表。
静态映射源	接入列表内的指定组播源 IPv6 地址。

8.4.3 组播组信息

功能说明

显示设备接口接收到的组播信息。

操作路径

按顺序依次打开：“组播路由 > IPv6 MLD >组播组信息”。

界面说明

组播组信息界面如下所示：

组播组信息界面主要元素配置说明：

界面元素	说明
接口	以太网接口。
组播地址	接口接收到的组播地址。
类型	组播类型： • dynamic：动态 • static：静态

8.5 PIM-SM

PIM（Protocol Independent Multicast）称为协议无关组播，与单播路由协议无关，利用单播路由表的路由信息，对组播报文执行 RPF（Reverse Path Forwarding，逆向路径转发）检查，检查通过后创建组播路由表项，从而转发组播报文。

PIM 协议包括：PIM-DM（PIM-Dense Mode）、PIM-SM（PIM-Sparse Mode）。

PIM-SM 属于稀疏模式的组播路由协议，使用“拉（Pull）模式”传送组播数据，通常适用于组播组成员分布相对分散、范围较广的大中型网络，其基本原理如下：

- PIM-SM假设所有主机都不需要接收组播数据，只向明确提出需要组播数据的主机转发。PIM-SM实现组播转发的核心任务就是构造并维护RPT（Rendezvous Point Tree，共享树或汇集树），RPT选择PIM域中某台路由器作为公用的根节点RP（Rendezvous Point，汇集点），组播数据通过RP沿着RPT转发给接收者；
- 连接接收者的路由器向某组播组对应的RP发送加入报文（Join Message），该报文被逐跳送达RP，所经过的路径就形成了RPT的分支；
- 组播源如果要向某组播组发送组播数据，首先由组播源侧DR（Designated Router，指定路由器）负责向RP进行注册，把注册报文（Register Message）通过单播方式发送给RP，该报文到达RP后触发建立SPT。之后组播源把组播数据沿着SPT发

向RP，当组播数据到达RP后，被复制并沿着RPT发送给接收者。

PIM-SM 的工作机制可以概括如下：

- 邻居发现
- DR选举
- RP发现
- 构建RPT
- 组播源注
- SPT切换
- 断言

8.5.1 全局配置

功能说明

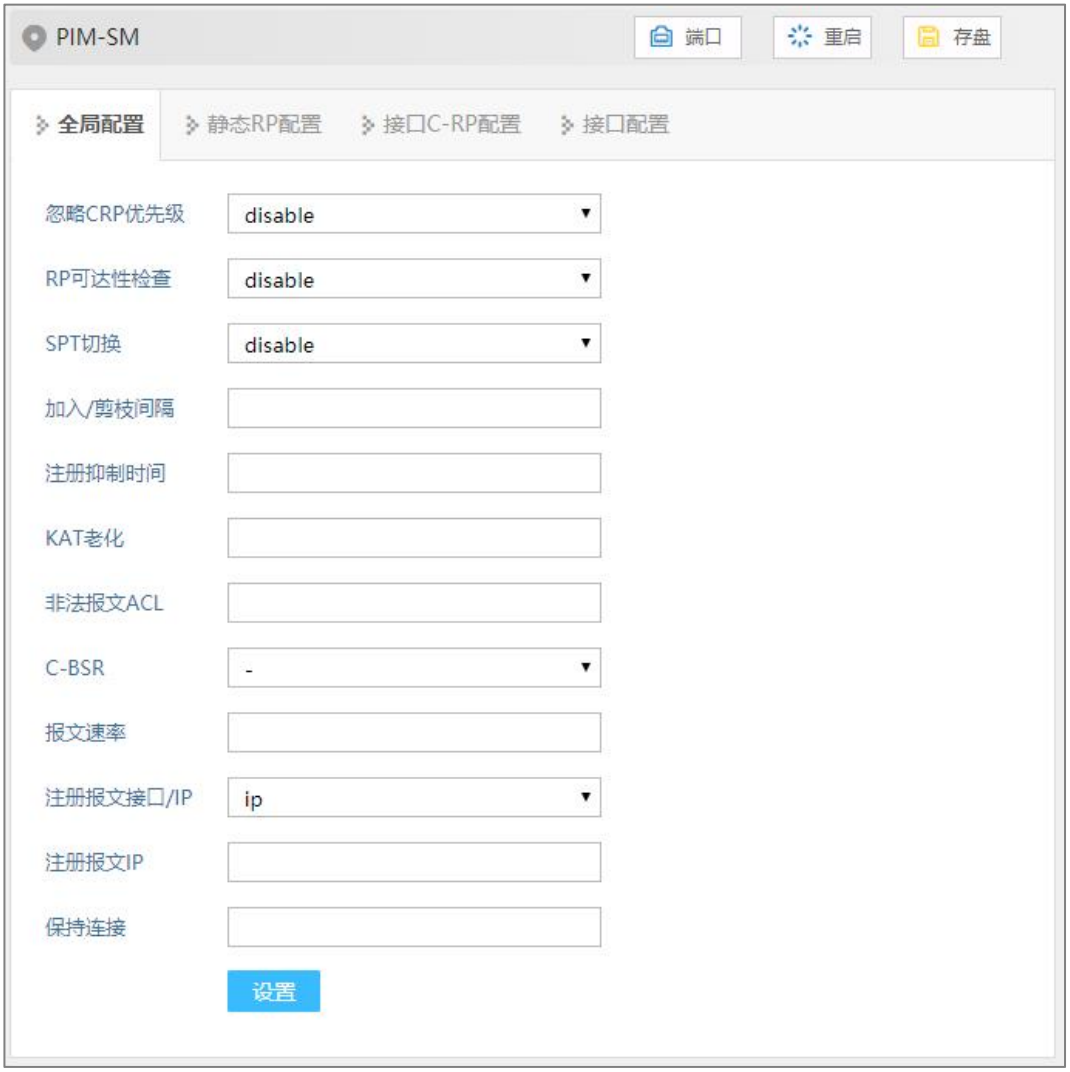
配置 PIM-SM 的全局参数。

操作路径

按顺序依次打开：“组播路由 > PIM-SM > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
忽略 CRP 优先级	在选择组播对应的 RP 时，是否忽略 CRP 的优先级，按照 IP 地址选举。IP 地址大的当选。
RP 可达性检查	发送注册报文时是否需要检查 RP 的可达性，如果不可达，则表示不能注册。
SPT 切换	RP 是所有组播报文必经的中转站，当组播报文速率逐渐变大时，对 RP 形成巨大的负担。PIM-SM 允许 RP 或组成员端 DR 通过触发 SPT 切换来减轻 RP 的负担。
加入/剪枝间隔	PIM 路由器发送加入/剪枝报文的时间间隔。
注册抑制时间	收到注册停止报文后再次发送注册报文的时间间隔，取值范围为 1～65535 秒。
KAT 老化	收到注册报文后的 KAT 定时器的老化时间，取值范围为 1～65535，单位为秒。 说明：

界面元素	说明
	缺省情况下，收到注册报文后，KAT 定时器的老化时间 = 注册抑制时间* 3 + 注册探测时间。
非法报文 ACL	配置非法的邻居源地址范围。 说明： 缺省情况下，接口可学习的邻居源地址不受任何限制。
C-BSR	C-BSR 接口配置。 • vlanif：vlanif 接口 • loopback：loopback 接口
报文速率	接收处理组播业务报文的速率，取值范围为 1～65535，单位为个/秒。
注册报文接口/IP	发送注册报文的 VLAN 接口、源 IP 地址或 loopback 接口。
注册报文 IP	注册报文的源 IP 地址。
保存连接	组播源生存时间，取值范围为 60-65535 秒。

8.5.2 静态 RP 配置

功能说明

手动设置静态 RP。

操作路径

按顺序依次打开：“组播路由 > PIM-SM > 静态 RP 配置”。

界面说明

静态 RP 配置界面如下所示：

静态 RP 配置界面主要元素配置说明：

界面元素	说明

界面元素	说明
IP 地址	配置静态 RP 的 IP 地址。 说明： • 该地址必须是合法的单播 IP 地址，请勿配置为 127.0.0.0/8 网段的地址。 • 当网络内仅有一个 RP 时，可以手工配置静态 RP 而不使用动态 RP，这样可以避免 C-RP 和 BSR 之间频繁的信息交互占用带宽。

8.5.3 接口 C-RP 配置

功能说明

新增、删除 C-RP 接口。

操作路径

按顺序依次打开：“组播路由 > PIM-SM > 接口 C-RP 配置”。

界面说明

接口 C-RP 配置界面如下所示：

接口 C-RP 配置界面主要元素配置说明：

界面元素	说明
C-RP 接口	配置 C-RP 接口： • vlanif：vlanif 接口 • loopback：loopback 接口

8.5.4 接口配置

功能说明

设置接口 PIM-SM 参数。

操作路径

按顺序依次打开：“组播路由 > PIM-SM > 接口配置”。

界面说明

接口配置界面如下所示：

接口配置界面主要元素配置说明：

界面元素	说明
接口	配置接口： • vlanif：vlanif 接口 • loopback：loopback 接口
不携带 GenID	在接口上配置发送 hello 报文时不携带 GenID 信息。 说明： GenID 是接口初始创建时的随机值，用于标识唯一的接口信息。通过此信息，可以检测到邻居设备是否已经重启。
DR 优先级	指定竞选 DR 的优先级，取值范围为 0～4294967294。 说明： 该数值越大，优先级越高。
邻居可达时间(s)	指定保持 PIM 邻居可达状态的时间，取值范围为 1～65535，单位为秒。 说明： 如果指定为 65535 秒，则表示 PIM 邻居永远可达。
HELLO 间隔(s)	PIM 路由器之间发送 Hello 报文的时间周期。
非法邻居 ACL	非法的邻居源地址范围。

8.6 PIM-DM

PIM-DM 属于密集模式的组播路由协议，使用“推（Push）模式”传送组播数据，通常适用于组播组成员相对比较密集的小型网络，其基本原理如下：

- PIM-DM假设网络中的每个子网都存在至少一个组播组成员，因此组播数据将被扩散（Flooding）到网络中的所有节点。然后，PIM-DM对没有组播数据转发的分支进行剪枝（Prune），只保留包含接收者的分支。这种“扩散—剪枝”现象周期性地发生，被剪枝的分支也可以周期性地恢复成转发状态。
- 当被剪枝分支的节点上出现了组播组的成员时，为了减少该节点恢复成转发状态所需的时间，PIM-DM使用嫁接（Graft）机制主动恢复其对组播数据的转发。

一般说来，密集模式下数据包的转发路径是有源树（Source Tree，即以组播源为“根”、组播组成员为“枝叶”的一棵转发树）。由于有源树使用的是从组播源到接收者的最短路径，因此也称为 SPT（Shortest Path Tree，最短路径树）。

PIM-DM 的工作机制可以概括如下：

- 邻居发现
- 构建SPT
- 嫁接
- 断言

功能说明

配置 PIM-DM 参数。

操作路径

按顺序依次打开：“组播路由 > PIM-DM”。

界面说明

PIM-DM 界面如下所示：

PIM-DM 界面主要元素配置说明：

界面元素	说明
接口	配置接口： • vlanif：vlanif 接口 • loopback：loopback 接口

界面元素	说明
使能状态	接口 PIM-DM 使能状态。
不携带 GenID	在接口上配置发送 hello 报文时不携带 GenID 信息。 说明： GenID 是接口初始创建时的随机值，用于标识唯一的接口信息。通过此信息，可以检测到邻居设备是否已经重启。
DR 优先级	指定竞选 DR 的优先级，取值范围为 0～4294967294。 说明： 该数值越大，优先级越高。
邻居可达时间(s)	指定保持 PIM 邻居可达状态的时间，取值范围为 1～65535，单位为秒。 说明： 如果指定为 65535 秒，则表示 PIM 邻居永远可达。
HELLO 间隔(s)	PIM 路由器之间发送 Hello 报文的时间周期。
状态刷新(s)	剪枝定时器状态刷新的时间间隔，避免被裁剪的接口因为剪枝定时器超时而恢复转发，取值范围为 1-100 秒。
Prune 报文延时(ms)	共享网段上传输 Prune 报文的延迟时间，取值范围为 0-32767 毫秒。
非法邻居 ACL	非法的邻居源地址范围。

8.7 IPv6-PIM-SM

8.7.1 全局配置

功能说明

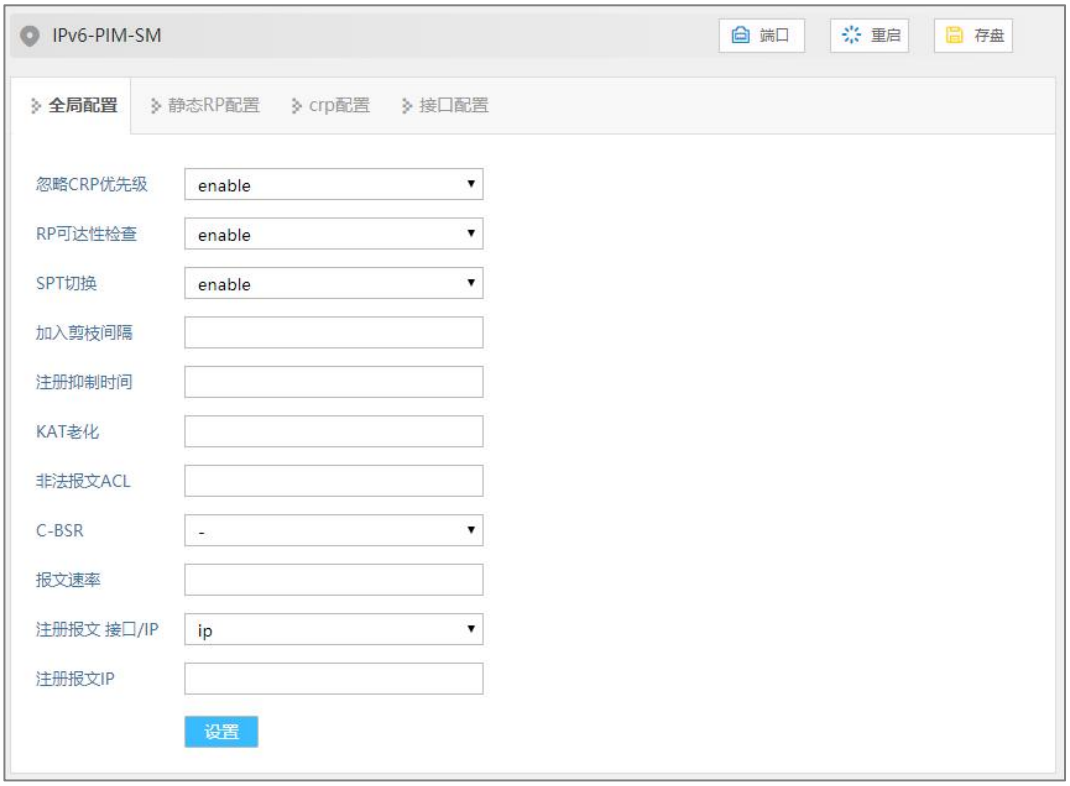
配置 IPv6-PIM-SM 的全局参数。

操作路径

按顺序依次打开：“组播路由 > IPv6-PIM-SM > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
忽略 CRP 优先级	在选择组播对应的 RP 时，是否忽略 CRP 的优先级，按照 IP 地址选举。IP 地址大的当选。
RP 可达性检查	发送注册报文时是否需要检查 RP 的可达性，如果不可达，则表示不能注册。
SPT 切换	RP 是所有组播报文必经的中转站，当组播报文速率逐渐变大时，对 RP 形成巨大的负担。PIM-SM 允许 RP 或组成员端 DR 通过触发 SPT 切换来减轻 RP 的负担。
加入/剪枝间隔	PIM 路由器发送加入/剪枝报文的时间间隔。
注册抑制时间	收到注册停止报文后再次发送注册报文的时间间隔，取值范围为 1～65535 秒。
KAT 老化	收到注册报文后的 KAT 定时器的老化时间，取值范围为 1～65535，单位为秒。 说明： 缺省情况下，收到注册报文后，KAT 定时器的老化时间 = 注册抑制时间* 3 + 注册探测时间。
非法报文 ACL	配置非法的邻居源地址范围。 说明： 缺省情况下，接口可学习的邻居源地址不受任何限制。
C-BSR	C-BSR 接口配置。 • vlanif：vlanif 接口

界面元素	说明
	• loopback：loopback 接口
报文速率	接收处理组播业务报文的速率，取值范围为 1～65535，单位为个/秒。
注册报文接口/IP	发送注册报文的 VLAN 接口、源 IP 地址或 loopback 接口。
注册报文 IP	注册报文的源 IP 地址。

8.7.2 静态 RP 配置

功能说明

手动设置静态 RP。

操作路径

按顺序依次打开：“组播路由 > IPv6-PIM-SM > 静态 RP 配置”。

界面说明

静态 RP 配置界面如下所示：

静态 RP 配置界面主要元素配置说明：

界面元素	说明
IP 地址	配置静态 RP 的 IPv6 地址。 说明： 当网络内仅有一个 RP 时，可以手工配置静态 RP 而不使用动态 RP，这样可以避免 C-RP 和 BSR 之间频繁的信息交互占用带宽。

8.7.3 接口 C-RP 配置

功能说明

新增、删除 C-RP 接口。

操作路径

按顺序依次打开：“组播路由 > IPv6-PIM-SM > 接口 C-RP 配置”。

界面说明

接口 C-RP 配置界面如下所示：

接口 C-RP 配置界面主要元素配置说明：

界面元素	说明
C-RP 接口	配置 C-RP 接口： • vlanif：vlanif 接口

8.7.4 接口配置

功能说明

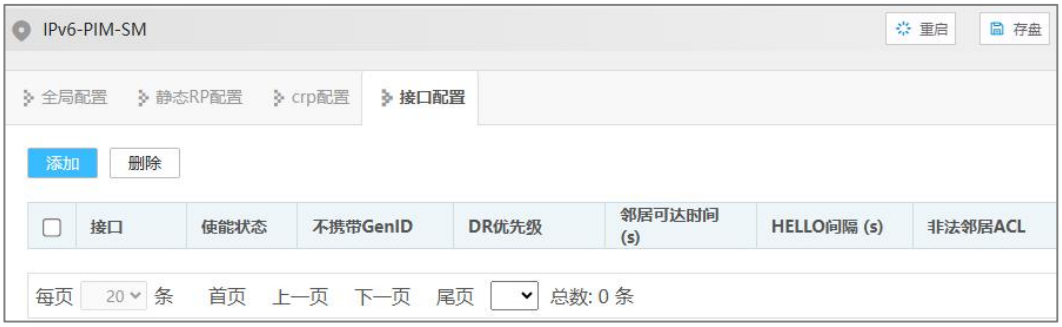
设置接口 IPv6-PIM-SM 参数。

操作路径

按顺序依次打开：“组播路由 > IPv6-PIM-SM > 接口配置”。

界面说明

接口配置界面如下所示：



接口配置界面主要元素配置说明：

界面元素	说明
接口	配置接口： • vlanif：vlanif 接口
使能状态	PIM-SM 状态。 • enable • disable
不携带 GenID	在接口上配置发送 hello 报文时不携带 GenID 信息。 说明： GenID 是接口初始创建时的随机值，用于标识唯一的接口信息。通过此信息，可以检测到邻居设备是否已经重启。
DR 优先级	指定竞选 DR 的优先级，取值范围为 0～4294967294。 说明： 该数值越大，优先级越高。
邻居可达时间(s)	指定保持 PIM 邻居可达状态的时间，取值范围为 1～65535，单位为秒。 说明： 如果指定为 65535 秒，则表示 PIM 邻居永远可达。
Hello 间隔(s)	PIM 路由器之间发送 Hello 报文的时间周期。
非法邻居 ACL	非法的邻居源地址范围。

8.8 IPv6-PIM-DM

功能说明

配置 IPv6-PIM-DM 参数。

操作路径

按顺序依次打开：“组播路由 > IPv6-PIM-DM”。

界面说明

IPv6-PIM-DM 界面如下所示：

IPv6-PIM-DM 界面主要元素配置说明：

界面元素	说明
接口	配置接口：

界面元素	说明
	• vlanif：vlanif 接口
使能状态	接口 PIM-DM 使能状态。
不携带 GenID	在接口上配置发送 hello 报文时不携带 GenID 信息。 说明： GenID 是接口初始创建时的随机值，用于标识唯一的接口信息。通过此信息，可以检测到邻居设备是否已经重启。
DR 优先级	指定竞选 DR 的优先级，取值范围为 0～4294967294。 说明： 该数值越大，优先级越高。
邻居可达时间(s)	指定保持 PIM 邻居可达状态的时间，取值范围为 1～65535，单位为秒。 说明： 如果指定为 65535 秒，则表示 PIM 邻居永远可达。
HELLO 间隔(s)	PIM 路由器之间发送 Hello 报文的时间周期。
状态刷新(s)	剪枝定时器状态刷新的时间间隔，避免被裁剪的接口因为剪枝定时器超时而恢复转发，取值范围为 1-100 秒。
Prune 报文延时(ms)	共享网段上传输 Prune 报文的延迟时间，取值范围为 0-32767 毫秒。
非法邻居 ACL	非法的邻居源地址范围。

9 网络管理

9.1 ACL

ACL（Access Control List）访问控制列表是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。通过 ACL 可以实现对网络中报文流的精确识别和控制，达到控制网络访问行为、防止网络攻击和提高网络带宽利用率的目的，从而切实保障网络环境的安全性和网络服务质量的可靠性。

9.1.1 ACL 生效时段配置

功能说明

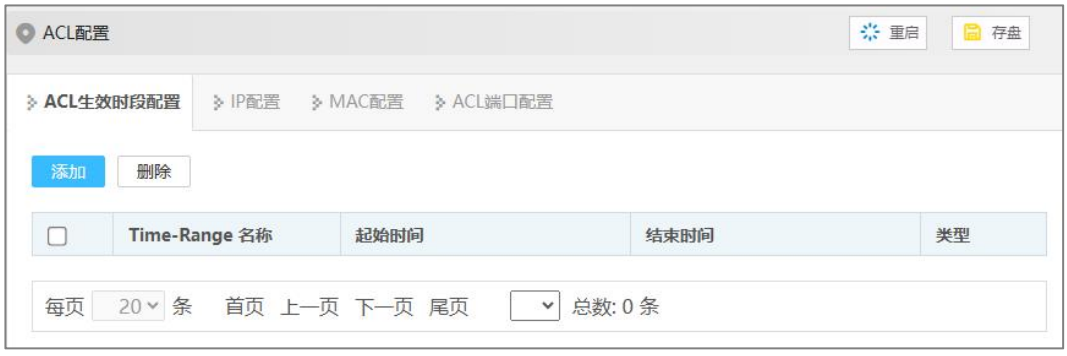
在“ACL 生效时段配置”页面，可以配置 ACL 规则的生效时间段。

操作路径

按顺序依次打开：“网络管理 > ACL > ACL 生效时段配置”。

界面说明

ACL 生效时段配置界面如下所示：



ACL 生效时段配置界面主要元素配置说明：

界面元素	说明
添加	单击“添加”按钮，可新增时间段条目。
删除	勾选时间段条目，单击“删除”按钮，可批量删除指定条目。
Time-Range 名称	ACL 生效时间段的名称，支持绝对时间与周期时间。
起始时间	绝对时间或周期时间范围的起始时间。
结束时间	绝对时间或周期时间范围的结束时间。
类型	时间类型，可选项如下： • 绝对时间； • 周期时间。
操作	删除：单击“删除”，可删除当前条目。

单击“添加”按钮，可添加时间条目。

在“添加”界面，选择“绝对时间”单选框。

界面说明 1：添加-绝对时间

添加-绝对时间界面如下所示：

添加-绝对时间界面主要元素配置说明：

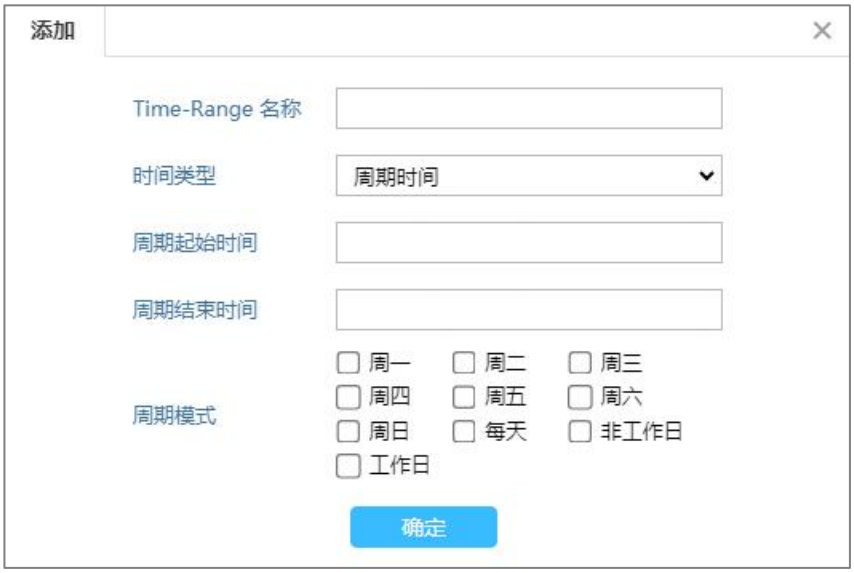
界面元素	说明
Time-Range 名称	ACL 生效时间段的名称。生效时间段存在两种模式，可勾选项为： • 绝对时间：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。 • 周期时间：以星期或工作日为参数来定义时间范围，表示规则以一周为周期（如每周一的 8 至 12 点）循环生效。
时间类型	时间类型，可选项如下： • 绝对时间； • 周期时间。
起始日期	绝对时间的起始日期，格式：yyyy-mm-dd（年-月-日）。

界面元素	说明
起始时间	绝对时间的起始时间，格式：hh:mm:ss（时:分:秒）。
结束日期	绝对时间的结束日期，格式：yyyy-mm-dd（年-月-日）。
结束时间	绝对时间的结束时间，格式：hh:mm:ss（时:分:秒）。

在“添加”界面，选择“周期时间”单选框。

界面说明 2：添加-周期时间

添加-周期时间界面如下所示：



添加-周期时间界面主要元素配置说明：

界面元素	说明
Time-Range 名称	ACL 生效时间段的名称。生效时间段存在两种模式，可勾选项为： • 绝对时间：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。 • 周期时间：以星期或工作日为参数来定义时间范围，表示规则以一周为周期（如每周一的 8 至 12 点）循环生效。
时间类型	时间类型，可选项如下： • 绝对时间； • 周期时间。
周期起始时间	周期时间的起始时间范围，格式：hh:mm:ss- hh:mm:ss（时:分:秒）。
周期结束时间	周期时间的结束时间，格式：hh:mm:ss- hh:mm:ss（时:分:秒）。
周期模式	可勾选星期、每天、非工作日或工作日单选框，可指定需重复的日期，可选项如下： • 周一

界面元素	说明
	• 周二 • 周三 • 周四 • 周五 • 周六 • 周日 • 每天 • 非工作日 • 工作日

9.1.2 IP 配置

功能说明

在“IP 配置”页面，可以创建 IP ACL 规则。用户在创建 ACL 时可以为其指定编号，不同的编号对应不同类型的 ACL。同时，为了便于记忆和识别，用户还可以创建命名型 ACL，即在创建 ACL 时为其设置名称。

操作路径

按顺序依次打开：“网络管理 > ACL > IP 配置”。

界面说明

IP 配置界面如下所示：

IP 配置界面主要元素配置说明：

界面元素	说明
添加	单击“添加”按钮，可新增 IP 规则。
删除规则	勾选规则条目，单击“删除规则”按钮，可批量删除指定规则。
删除系列	勾选规则条目，单击“删除序列”按钮，可批量删除同一个规则下的系列条目。
删除 TimeRange	清除已经绑定 TimeRange 的规则条目。

界面元素	说明
规则名称	IP 规则名称或编号。
序列	同一条规则名称下面，不同规则的内容。 说明： 同一个规则名称下面最多支持 32 条序列。
动作	IP 规则的动作，包括 permit/deny 两种动作，表示允许/拒绝。
协议	数据包的协议类型。
源 IP	数据包的源 IP 地址信息。
源通配符	源 IP 地址通配符掩码。
源端口号	源 IP 地址端口号。
目的 IP	数据包的目的 IP 地址信息。
目的通配符	目的 IP 地址通配符掩码。
目的端口号	目的 IP 地址端口号。
Time Range	IP 规则的生效时间段名称。

单击“添加”按钮，可添加 IP 规则条目。

界面说明：添加

添加界面如下所示：

添加界面主要元素配置说明：

界面元素	说明

界面元素	说明
规则类型	IP 规则类型下拉列表，可选项为： • 名称：通过名称代替编号来标识 ACL。 • 编号：创建 ACL 时，指定一个唯一的数字标识该 ACL。
规则名称	IP 规则名称或编号。当规则类型为名称时，支持输入@、!、_、数字和字母组合不超过 16 位。当规则类型为编号时，支持 1-199 或 1300-2699。 说明： • 标准 ACL（1-99、1300-1999）：仅使用报文的源 IP 地址、分片信息和生效时间段信息来定义规则。 • 拓展 ACL（100-199、2000-2699）：既可使用 IPv4 报文的源 IP 地址，也可使用目的 IP 地址、协议类型、生效时间段等来定义规则。
动作	ACL 规则的动作下拉列表，可选项为： • Permit：允许 • Deny：拒绝
协议	扩展 ACL 规则的协议类型，支持基于协议类型过滤报文，协议号取值范围 0-255。可单击“协议”下拉列表，选择现有协议名称。
源 IP	数据包的源 IP 地址信息，如 192.168.1.1，不输入表示任意 IP 地址。
源通配符	源 IP 地址通配符掩码，如 0.0.0.255。IP 地址通配符掩码是一个 32 比特位的数字字符串，用于指示 IP 地址中的哪些位将被检查。“0”表示“检查相应的位”，“1”表示“不检查相应的位”。
目的 IP	数据包的目的 IP 地址信息，如 192.168.1.1，不输入表示任意 IP 地址。
目的通配符	目的 IP 地址通配符掩码，如 0.0.0.255。IP 地址通配符掩码是一个 32 比特位的数字字符串，用于指示 IP 地址中的哪些位将被检查。“0”表示“检查相应的位”，“1”表示“不检查相应的位”。
Time Range	IP 规则的生效时间段名称。

9.1.3 MAC 配置

功能说明

在“MAC 配置”页面，可以创建 MAC 规则。二层 ACL 使用报文的以太网帧头信息来定义规则，如根据源 MAC（Media Access Control）地址、目的 MAC 地址等。

操作路径

按顺序依次打开：“网络管理 > ACL > MAC 配置”。

界面说明

MAC 配置界面如下所示：

MAC 配置界面主要元素配置说明：

界面元素	说明
添加	单击“添加”按钮，可新增 MAC 规则。
删除	勾选规则条目，单击“删除规则”按钮，可批量删除指定条目。
删除系列	勾选规则条目，单击“删除序列”按钮，可批量删除同一个规则下的系列条目。
删除 TimeRange	清除已经绑定 TimeRange 的规则条目。
规则名称	MAC 规则编号。
序列	同一条规则名称下面，不同规则的内容。 说明： 同一个规则名称下面最多支持 32 条序列。
动作	MAC 规则的动作，包括 permit/deny 两种动作，表示允许/拒绝。
源 MAC	数据包的源 MAC 地址信息。
源通配符	源 MAC 地址通配符掩码。
目的 MAC	数据包的目的 MAC 地址信息。
目的通配符	目的 MAC 地址通配符掩码。
以太网类型	数据包的以太网类型。
Time Range	MAC 规则的生效时间段名称。

单击“添加”按钮，可添加 MAC 规则条目。

界面说明：添加

添加界面如下所示：

添加界面主要元素配置说明：

界面元素	说明
规则名称	MAC 规则编号，取值范围 100-199 或者 2000-2699。
动作	ACL 规则的动作下拉列表，可选项为： • Permit：允许 • Deny：拒绝
源 MAC	数据包的源 MAC 地址信息，如 0001.0001.0001，不输入表示任意 MAC 地址。
源通配符	源 MAC 地址通配符掩码，如 0001.0001.0001。MAC 地址通配符掩码，用于指示 MAC 地址中的哪些位将被检查。“0”表示“检查相应的位”，“1”表示“不检查相应的位”。
目的 MAC	数据包的目的 MAC 地址信息，如 0001.0001.0001，不输入表示任意 MAC 地址。
目的通配符	目的 MAC 地址通配符掩码，如 0001.0001.0001。MAC 地址通配符掩码，用于指示 MAC 地址中的哪些位将被检查。“0”表示“检查相应的位”，“1”表示“不检查相应的位”。
以太网类型	数据包的以太网类型，取值范围 1536-65535（0x0600-0xffff）。
Time Range	MAC 规则的生效时间段名称。

9.1.4 ACL 端口配置

功能说明

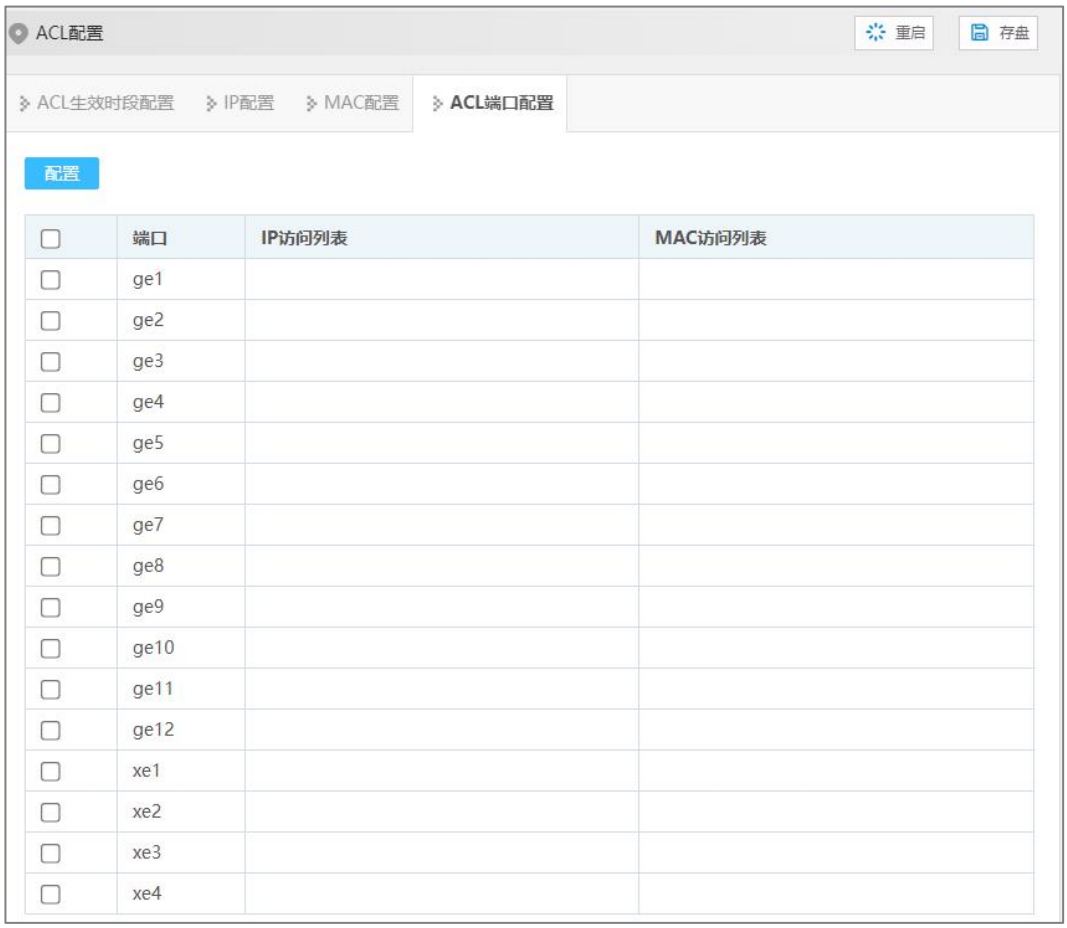
在“ACL 端口配置”页面，可以配置端口启用 IP ACL 和 MAC ACL 规则。

操作路径

按顺序依次打开：“网络管理 > ACL > ACL 端口配置”。

界面说明

ACL 端口配置界面如下所示：



ACL 端口配置界面主要元素配置说明：

界面元素	说明
端口	设备的以太网端口编号。
IP 访问列表	端口支持 IP ACL 规则，支持： • in：数据入口方向 • out：数据出口方向
MAC 访问列表	端口支持 MAC ACL 规则，支持 in：数据入口方向。

9.2 SNMP

目前网络中用得最广泛的网络管理协议是 SNMP（Simple Network Management Protocol，简单网络管理协议）。SNMP 是被广泛接受并投入使用的工业标准，用于保证管理信息在网络中任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、定位故障、完成故障诊断、进行容量规划和生成报告。SNMP 采用轮询机制，只提供最基本的功能集，特别适合在小型、快速和低价格的环境中使用。SNMP 的实现基于无连接的传输层协议 UDP，因此可以实现和众多产品的无障碍连接。

9.2.1 SNMP 开关

功能说明

启用或禁用 SNMP 功能。

操作路径

按顺序依次打开：“网络管理 > SNMP > SNMP 开关”。

界面说明

SNMP 开关界面如下所示：

SNMP 开关界面主要元素配置说明：

界面元素	说明
使能开关	SNMP 使能开关，默认为开启。 说明： 如果代理端已打开，不能关闭 SNMP 服务器。

9.2.2 视图

功能说明

添加/删除 SNMP 视图。

操作路径

按顺序依次打开：“网络管理 > SNMP > 视图”。

界面说明

视图界面如下所示：

视图界面主要元素配置说明：

界面元素	说明
名称	SNMP 视图名称定义，支持 32 个字符输入。
OID	该设备所处 MIB 树的节点位置信息。 说明： • OID 对象标识符，MIB 的组成结点，由一串表示路径的数字唯一地识别。 • OID 的信息可以从第三方软件 MG-SOFT MIB Browser 中查看。
模式	节点 OID 的处理方式，可选项如下： • Included：包含该节点子树下的所有对象； • Excluded：排除该节点子树以外的所有对象。

9.2.3 团体

功能说明

添加/删除 SNMP 团体。定义团体名可以访问的 MIB 视图，设置团体名对 MIB 对象的访问权限为写权限（write）或者只读权限（read）。

操作路径

按顺序依次打开：“网络管理 > SNMP > 团体”。

界面说明

团体界面如下所示：

团体界面主要元素配置说明：

界面元素	说明
名称	团体名称，包含数字或字母，长度不超过 32 字符。
视图名	SNMP 视图名称。
读写类型	视图读写权限，可选项如下： • 只读 • 读写

9.2.4 SNMP 组

功能说明

配置一个新的 SNMP 组，并设置 SNMP 组的安全模式和相应的 SNMP 视图。

操作路径

按顺序依次打开：“网络管理 > SNMP > SNMP 组”。

界面说明

SNMP 组界面如下所示：

SNMP 组界面主要元素配置说明：

界面元素	说明
名称	SNMP 组名称，取值范围为 1-32 个字符。
加密模式	是否对报文进行认证和加密，可取值： • auth：指对报文进行认证但不加密； • noauth：指对报文不进行认证也不加密； • priv ：指对报文进行认证和加密。
读视图	指定组的读取视图。
写视图	指定组的读写视图。
通知视图	指定组的通知视图。

9.2.5 V3 用户

功能说明

SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以设置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。采用认证和加密功能，可以为 NMS 和 Agent 之间的通信提供更高的安全性。

操作路径

按顺序依次打开：“网络管理 > SNMP > V3 用户”。

界面说明

V3 用户界面如下所示：

V3 用户界面主要元素配置说明：

界面元素	说明
用户名	SNMP v3 版本用户名称定义，只能包含数字、字母或@_!，长度不超过 32 字符。
组名	组名，取值范围为 1-32 个字节。 说明： 组名必须是已创建的 snmp 组，只有已创建的组才能创建 SNMP v3 用户。
安全模式	是否对报文进行认证和加密，可取值： • auth：指对报文进行认证但不加密； • noauth：指对报文不进行认证也不加密； • priv ：指对报文进行认证和加密。
认证模式	认证模式类型，可取值： • Md5：信息摘要算法 5； • Sha：安全哈希算法。
加密模式	V3 用户数据加密算法，可选项如下： • Des：采用数据加密算法加密； • Aes：采用高级加密标准加密。
用户权限	用户权限类型，可选项如下： • ro：只读权限，允许用户查询（get）SNMP 对象的值，但不允许用户修改（set）这些值。用户可以通过该权限获取设备的状态和信息，但无法对其进行更改； • rw：读写权限，允许用户查询（get）和修改（set）SNMP 对象的值。用户可以读取设备的状态和信息，并且有权对其进行更改，包括设置参数、启用或禁用功能等。

9.2.6 Trap 告警

功能说明

基于 TCP/IP 协议，SNMP 通常使用 UDP 端口 161（SNMP）和 162（SNMP-traps），SNMP 协议代理存在于网络设备里，使用 MIBs（information specific to the device）作为设备接口，通过代理，这些网络设备可以被监控或控制。当一个 trap 事件发生时，消息被 SNMP Trap 传输，此时，一个可用的 trap 接收器可以收到这个 trap 消息。

操作路径

按顺序依次打开：“网络管理 > SNMP > trap 告警”。

界面说明

trap 告警界面如下所示：

trap 告警界面主要元素配置说明：

界面元素	说明
使能开关	SNMP Trap 告警使能开关。
地址	SNMP 管理设备 IP 地址，用于接收告警信息，如 PC。
模式	SNMP 管理设备版本，可选如下： • 1 • 2c • 3
团队名	团体名称。
端口号	Trap 端口号，默认为 162，取值范围 0-65535。

9.3 RMON

RMON（Remote Network Monitoring，远程网络监视）主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。统计功能指的是被管理设备可以按周期或者持续跟踪统计其端口所连接的网段上的各种流量信息，比如某段时间内某网段上收到的报文总数，或收到的超长报文的总数等。告警功能指的是被管理设备能监控指定 MIB 变量的值，当该值达到告警阈值时（比如端口速率达到指定值，或者广播报文的比例达到指定值），能自动记录日志、向管理设备发送 Trap 消息。

9.3.1 事件组

功能说明

在“事件组”页面，可以添加、删除事件组以及查看事件组的配置信息。

操作路径

按顺序依次打开：“网络管理 > RMON > 事件组”。

界面说明

事件组界面如下所示：

事件组界面主要元素配置说明：

界面元素	说明
序号	当监控的 MIB 对象超过阈值时所触发的事件序号。 说明： 该序号与 RMON 告警信息配置中所设置的上升事件索引和下降事件索引相对应。
描述	用来描述该事件的一些描述性信息。
类型	事件处理方式，可选项如下： • log：该事件被引发时将事件记录在日志表中； • trap：该事件被引发时将向网管站发送 Trap 消息告知该事件的发生；

界面元素	说明
	• log，trap：该事件被引发时将事件记录在日志表中并产生一条 trap 消息。
团队名	接收告警信息的网管站的团体名。
最近发生的时间	最近一次事件发生的时间。
拥有者	该表项的创建者。
操作	可勾选条目，点击“删除”按钮进行删除。

9.3.2 统计组

功能说明

在“统计组”页面，您可以添加、删除统计组以及查看统计组的配置信息。

操作路径

按顺序依次打开：“网络管理 > RMON > 统计组”。

界面说明

统计组界面如下所示：

统计组界面主要元素配置说明：

界面元素	说明
序号	序号用来标识一个具体应用接口，当序号与之前设置的应用接口的序号相同时，先前的配置将被取代。
端口号	被统计的端口序号。
端口名	被统计的端口的名称。
拥有者	该表项的创建者。
操作	可勾选条目，点击“删除”按钮进行删除。

9.3.3 历史组

功能说明

在“历史组”页面，您可以添加、删除历史组以及查看历史组的配置信息。

操作路径

按顺序依次打开：“网络管理 > RMON >历史组”。

界面说明

历史组界面如下所示：

历史组界面主要元素配置说明：

界面元素	说明
序号	序号用来标识一个具体应用接口，当序号与之前设置的应用接口的序号相同时，先前的配置将被取代。
实际配置采样条数	设置历史组对应的历史统计表容量，范围为 1-65535。
端口名	被记录的端口名称。
最大可配置采样条数	设备能够支持的最大历史统计表容量。
采样周期	每两次获取统计数据的间隔时间。
拥有者	该表项的创建者。
操作	可勾选条目，点击“删除”按钮进行删除。

9.3.4 告警组

功能说明

在“告警组”页面，您可以添加、删除告警组以及查看告警组的配置信息。 报警类型使用 absolute 来直接监测 MIB 对象的取值；报警类型使用 delta 来监测两次取样之间 MIB 对象值的变化；

- 当监控的MIB对象到达或超过上升阈值时，将触发上升事件索引对应的事件；

- 当监控的MIB对象到达或超过下降阈值时，将触发下降事件索引对应的事件；

操作路径

按顺序依次打开：“网络管理 > RMON > 告警组”。

界面说明

告警组配置界面如下所示：

告警组配置界面主要元素配置说明：

界面元素	说明
序号	当监控的 MIB 对象超过阈值时所触发的事件序号。 说明： 该序号与 RMON 告警信息配置中所设置的上升事件索引和下降事件索引相对应。
状态	告警表项的状态，配置告警表项时状态不可配且缺省为 VALID。
采样间隔	采样时间间隔值，取值范围为 1-4294967295 之间，单位：秒。
采样类型	两种采样方式，可选项如下： • Absolute：当告警变量值达到告警阈值时，触发一次告警；若再次采样发现与上次采样告警类型相同，则不再触发告警； • Delte：每次采样时，当告警变量值达到告警阈值都会触发一次告警。
告警参数	即被监控的 MIB 节点，支持字符串格式，非 oid 格式。
统计值	即定义的所属统计组。
上升沿阈值	告警变量的值，上限告警，阈值在 1～2147483647 之间。 说明： 在告警变量值上升过程中，当超过上升沿阈值时，至少发生一次告警。
上升沿事件	事件组索引，当告警变量的值达到或超过上升沿阈值时，将激活事件组相应事件，取值范围为 1-65535。
下降沿阈值	告警变量的值，下限告警，阈值在 1～2147483647 之间。 说明： 在告警变量值下降过程中，当达到下降沿阈值时，至少发生一次告警。
下降沿事件	事件组索引，当告警变量的值达到或低于下降沿阈值时，将激活事件组相应事件，取值范围为 1-65535。

界面元素	说明
告警生效类型	三种告警生效类型，可选项如下： • 上升沿生效 • 下降沿生效 • 上升沿和下降沿都生效
拥有者	该表项的创建者。
操作	可勾选条目，点击“删除”按钮进行删除。

9.4 LLDP

LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的链路层发现协议。LLDP 是一种标准的二层发现方式，可以将本端设备的管理地址、设备标识、接口标识等信息组织起来，并发布给自己的邻居设备，邻居设备收到这些信息后将其以标准的管理信息库 MIB（Management Information Base）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

9.4.1 全局配置

功能说明

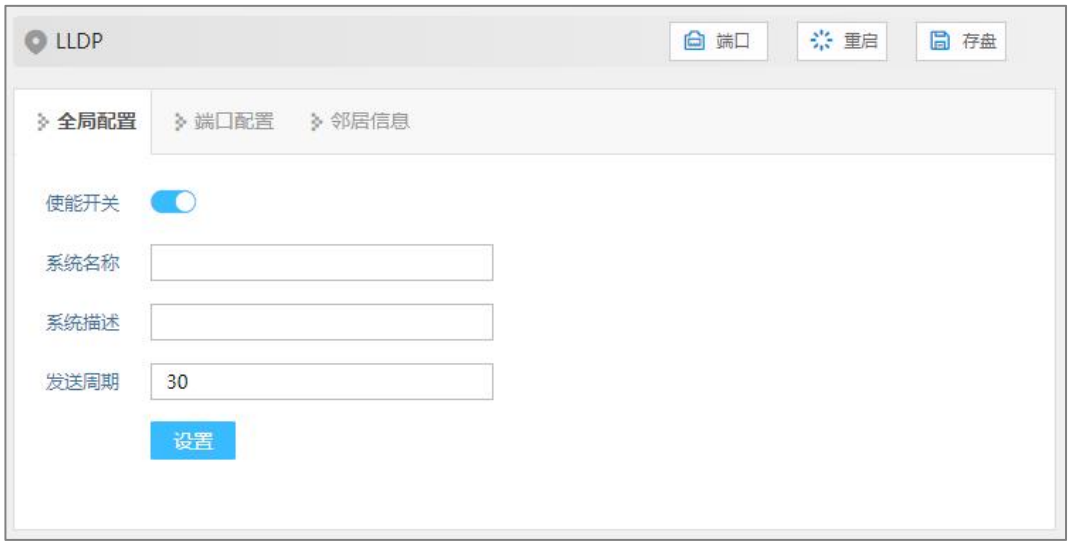
配置 LLDP 全局参数。

操作路径

按顺序依次打开：“网络管理 > LLDP > 全局配置”。

界面说明

全局配置界面如下所示：



全局配置界面主要元素配置说明：

界面元素	说明
使能开关	LLDP 使能开关。
系统名称	系统的名称，支持 0-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。
系统描述	系统的描述信息，支持 0-32 个字符，由大写字母、小写字母、数字或特殊字符（!@_-）组成。
发送周期	LLDP 报文的发送周期，取值范围为 5-32768 秒。设备状态没有变化的情况下，设备周期性的向邻居节点发送 LLDP 报文。 说明： LLDP 报文封装的 TLV（Type/Length/Value）类型，可包含系统名称和系统描述。

9.4.2 端口配置

功能说明

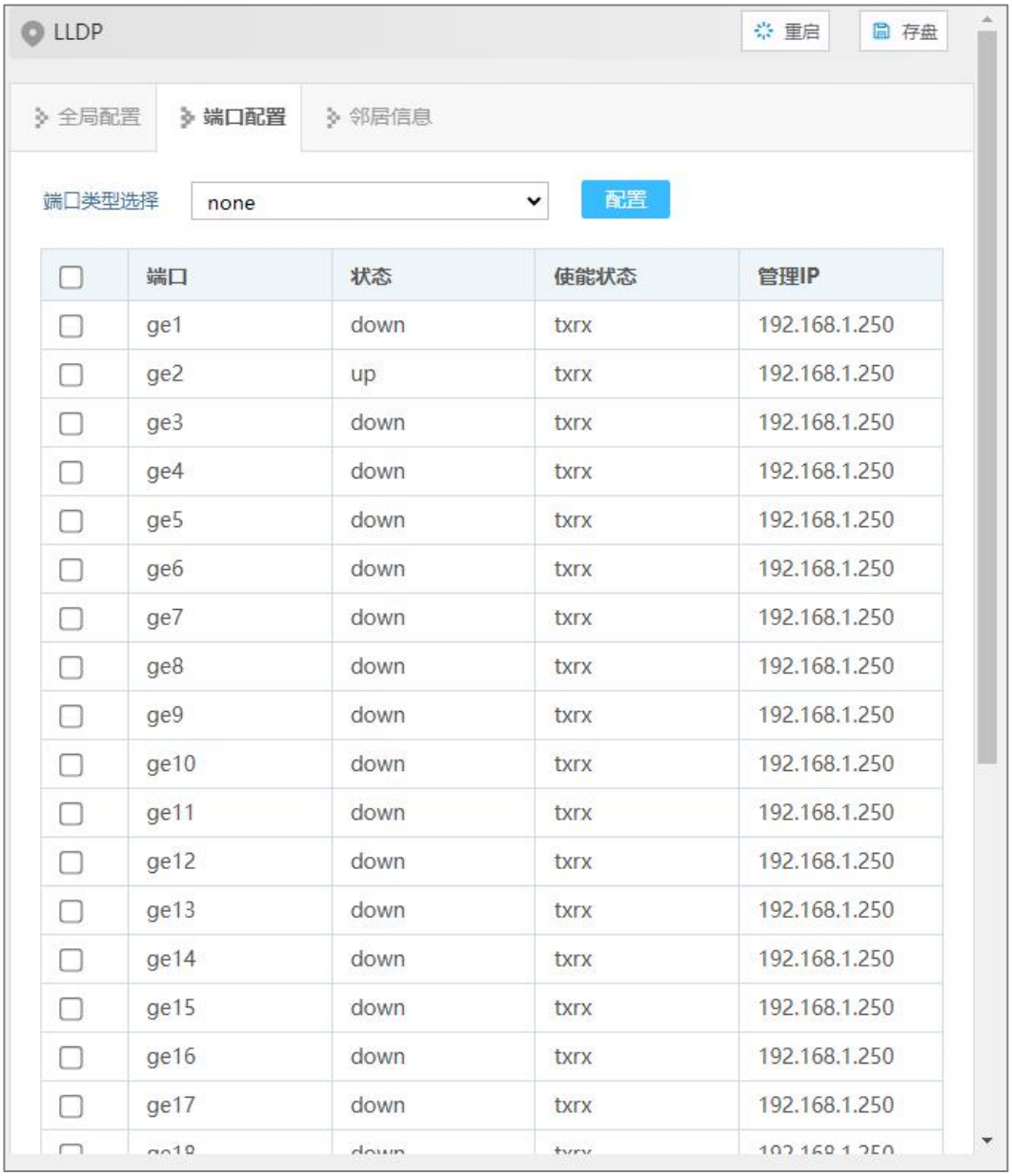
配置端口的发送、接收模式和管理地址。

操作路径

按顺序依次打开：“网络管理 > LLDP > 端口配置”。

界面说明

端口配置界面如下所示：



端口配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
端口状态	以太网端口的连接状态，显示状态如下： • down：端口未连接 • up：端口已连接
使能状态	该设备端口的 LLDP 工作状态，可选项有： • txonly：工作模式为 Tx，只发送不接收 LLDP 报文。 • rxonly：工作模式为 Rx，只接收不发送 LLDP 报文。 • txrx：工作模式为 TxRx，既发送也接收 LLDP 报文。 • disable：工作模式为 Disable，既不接收也不发送 LLDP 报文。 说明：

界面元素	说明
	缺省情况下，当全局 LLDP 使能的时候，LLDP 的工作模式为 TxRx。
管理 IP	该端口对应的 LLDP 管理 IP 地址。 说明： • LLDP 管理地址是供网管系统标识并进行管理的地址。管理地址可以明确地标识一台设备，有利于网络拓扑的绘制，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 字段中传送给邻居节点。 • 缺省情况下，端口在 LLDP 报文中发布的管理地址，默认为该端口所在 VLAN 中的最小 VLAN 的主 IP 地址，如果该 VLAN 未配置主 IP 地址，则为 0.0.0.0。

9.4.3 邻居信息

功能说明

查看邻居的相关信息。

操作路径

按顺序依次打开：“网络管理 > LLDP > 邻居信息”。

界面说明

邻居信息界面如下所示：

邻居信息界面主要元素配置说明：

界面元素	说明
本地端口	本地交换机连接邻居设备的本地端口号。
邻居设备 ID 类型	邻居设备 ID 类型。
邻居设备 ID	邻居设备 ID。
邻居端口 ID 类型	邻居端口 ID 类型。
邻居端口 ID	邻居设备的端口 ID。
系统名称	邻居设备的系统名称。
管理 IP	邻居设备或端口的管理 IP 地址。

9.5 DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通常被应用在大型的局域网络环境中，主要作用是集中的管理、分配 IP 地址，使网络环境中的主机动态的获得 IP 地址、Gateway 地址、DNS 服务器地址等信息，并能够提升地址的使用率。

9.5.1 DHCP 开关

功能说明

启用/禁用 DHCP 服务器。

操作路径

按顺序依次打开：“网络管理 > DHCP > DHCP 开关”。

界面说明

DHCP 开关界面如下所示：

DHCP 开关界面主要元素配置说明：

界面元素	说明
使能开关	DHCP 服务器使能开关，启用后，可向其它与本设备相连的设备分配 IP 地址。

9.5.2 Server-地址池配置

在用户定义了 DHCP 范围及排除范围后，剩余的地址构成了一个地址池，地址池中的地址可以动态的分配给网络中的客户机使用。地址池仅对自动获取 IP 的方式有效，手动设置 IP 只要符合规则可无视此项。

功能说明

添加、删除地址池以及查看地址池配置信息。

操作路径

按顺序依次打开：“网络管理 > DHCP > Server-地址池配置”。

界面说明

Server-地址池配置界面如下所示：

Server-地址池配置界面主要元素配置说明：

界面元素	说明
地址池名称	地址池的名称，最多 32 个字符。
分配网段	地址池分配客户端的 IP 地址网段，例如：192.168.0.1/24。
租赁时间	客户端的 IP 地址使用有效时间，格式为：天:时:分，取值范围：0-30 天 0-24 时 0-59 分，天时分用冒号分开。 说明： 当 dhcp client 获取的 ip 地址的时长将要达到该租赁时间时需要续租，否则会导致 ip 地址失效，dhcp client 需重新请求 ip 地址。
默认网关	客户端的默认网关地址，例如：192.168.1.0/24
分配 IP 范围	DHCP 地址池的最低地址与最高地址，属于该范围的地址是 DHCP 可以有效进行分配的。
DNS 服务器 IP	DNS 服务器的 IP 地址。

9.5.3 Server-MAC 绑定

功能说明

绑定地址池分配的 IP 地址和设备的 MAC 地址。

操作路径

按顺序依次打开：“网络管理 > DHCP > Server-MAC 绑定”。

界面说明

Server-MAC 绑定界面如下所示：

Server-MAC 绑定界面主要元素配置说明：

界面元素	说明
地址池名称	DHCP 地址池的名称。
IP	DHCP 地址池分配的 IP 地址，该 MAC 地址获取的 IP 地址。
MAC	绑定 IP 的设备 MAC 地址。

9.5.4 Server-端口绑定

功能说明

绑定端口所能分配的 IP 地址。

操作路径

按顺序依次打开：“网络管理 > DHCP > Server-端口绑定”。

界面说明

Server-端口绑定界面如下所示：

Server-端口绑定界面主要元素配置说明：

界面元素	说明
地址池名称	DHCP 地址池的名称。
端口	该设备以太网端口对应的端口名称。

界面元素	说明
IP 地址	DHCP 地址池分配的 IP 地址，该端口上客户端获取的 IP 地址。

9.5.5 Server-客户端列表

功能说明

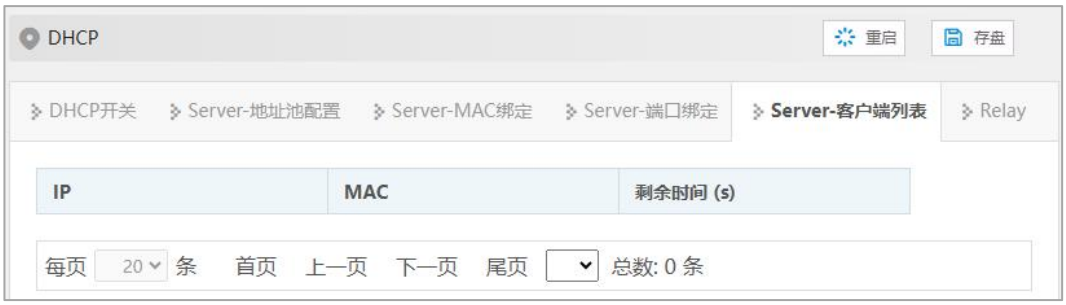
查看 DHCP 客户端的信息。

操作路径

按顺序依次打开：“网络管理 > DHCP > Server-客户端列表”。

界面说明

Server-客户端列表界面如下所示：



Server-客户端列表界面主要元素配置说明：

界面元素	说明
IP	DHCP 客户端设备的 IP 地址。
MAC	DHCP 客户端设备的 MAC 地址。
剩余时间(s)	DHCP 客户端获取的 IP 地址老化剩余时间。

9.5.6 Relay

DHCP 中继负责转发 DHCP 服务器和 DHCP 客户端之间的 DHCP 报文，协助 DHCP 服务器向 DHCP 客户端动态分配网络参数的设备。当 DHCP 客户端和 DHCP 服务器不在同一个网段，DHCP 服务器无法接收来自客户端的请求报文，此时，需要通过 DHCP 中继来转发 DHCP 报文。

功能说明

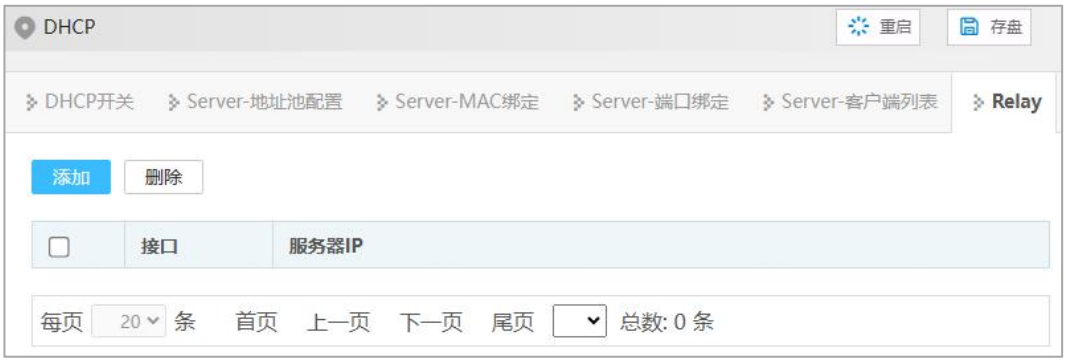
配置 Relay 接口的相关参数。

操作路径

按顺序依次打开：“网络管理 > DHCP > Relay”。

界面说明

Relay 界面如下所示：



Relay 界面主要元素配置说明：

界面元素	说明
接口	接口名称。
服务器 IP	DHCP 中继所代理的 DHCP 服务器的 IP 地址。

9.6 DHCP-Snooping

DHCP Snooping 的作用

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

1 保证客户端从合法的服务器获取 IP 地址。

网络中如果存在私自架设的伪 DHCP 服务器，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。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

连接 DHCP 服务器和其他 DHCP Snooping 设备的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系

DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、获取到的 IP 地址、与 DHCP 客户端连接的端口及该端口所属的 VLAN 等信息。利用这些信息可以实现：

- ARP Detection：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。
- IP Source Guard：通过动态获取 DHCP Snooping 表项对端口转发的报文进行过滤，防止非法报文通过该端口。

Option 82

Option 82 称为中继代理信息选项，该选项记录了 DHCP 客户端的位置信息。DHCP 中继或 DHCP Snooping 设备接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。

管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制定 IP 地址和其他参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前，DHCP 中继支持 3 个子选项：sub-option 1（Circuit ID，电路 ID 子选项）、sub-option 2（Remote ID，远程 ID 子选项）和 sub-option 3（Subscriber ID，用户 ID 子选项）。

9.6.1 全局配置

功能说明

在“全局配置”页面，可以启用/禁用 DHCP Snooping。

操作路径

按顺序依次打开：“网络管理 > DHCP Snooping > 全局配置”。

界面说明

全局配置界面如下所示：

全局配置界面主要元素配置说明：

界面元素	说明

界面元素	说明
使能开关	向右滑动可启用 DHCP-Snooping 功能。
MAC 检查	开启 DHCP 客户端 MAC 地址检查。 说明： 启用 DHCP-Snooping 功能，将自动开启 DHCP 客户端 MAC 地址检查。
端口禁用时长使能	当端口的 DHCP 报文速率低于端口配置的速率时，端口将被禁用“端口禁用时长”。
端口禁用时长	端口禁用时间，输入范围为 1-3600，单位为 s，默认为 30s。

9.6.2 VLAN 使能配置

功能说明

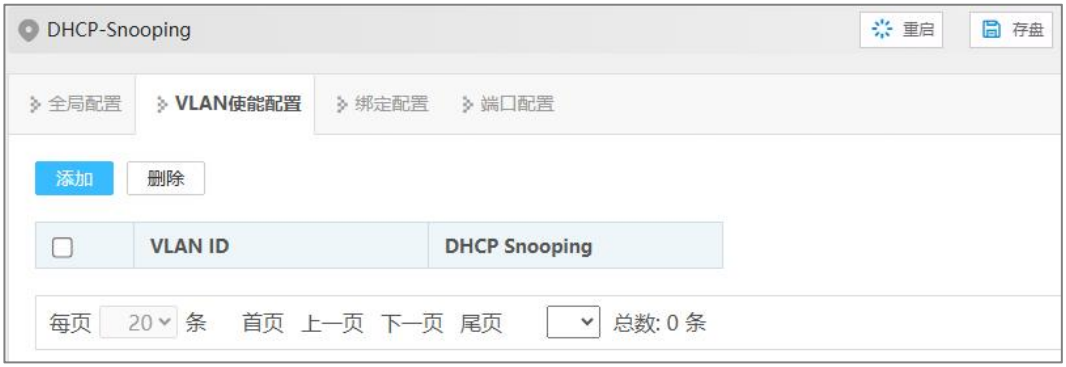
在“VLAN 使能配置”页面，可以指定 VLAN 启用 DHCP Snooping 功能。

操作路径

按顺序依次打开：“网络管理 > DHCP Snooping > VLAN 使能配置”。

界面说明

VLAN 使能配置界面如下所示：



VLAN 使能配置界面主要元素配置说明：

界面元素	说明
VLAN ID	VLAN 号。
DHCP Snooping	DHCP Snooping 使能状态。 • enable • disalbe

9.6.3 绑定配置

功能说明

在“绑定配置”页面，可以绑定端口、IP 地址和 MAC 地址。

操作路径

按顺序依次打开：“网络管理 > DHCP Snooping > 绑定配置”。

界面说明

绑定配置界面如下所示：

绑定配置界面主要元素配置说明：

界面元素	说明
VLAN ID	绑定的 VLAN ID 号信息，例如：1-4096。
端口	该设备以太网端口对应的端口名称。
IP 地址	绑定的 IP 地址，例如：192.168.1.1。
MAC	绑定的 MAC 地址，例如：0001-0001-0001。
类型	端口类型： • Static • Dynamic
老化时间	端口老化时间。

9.6.4 端口配置

功能说明

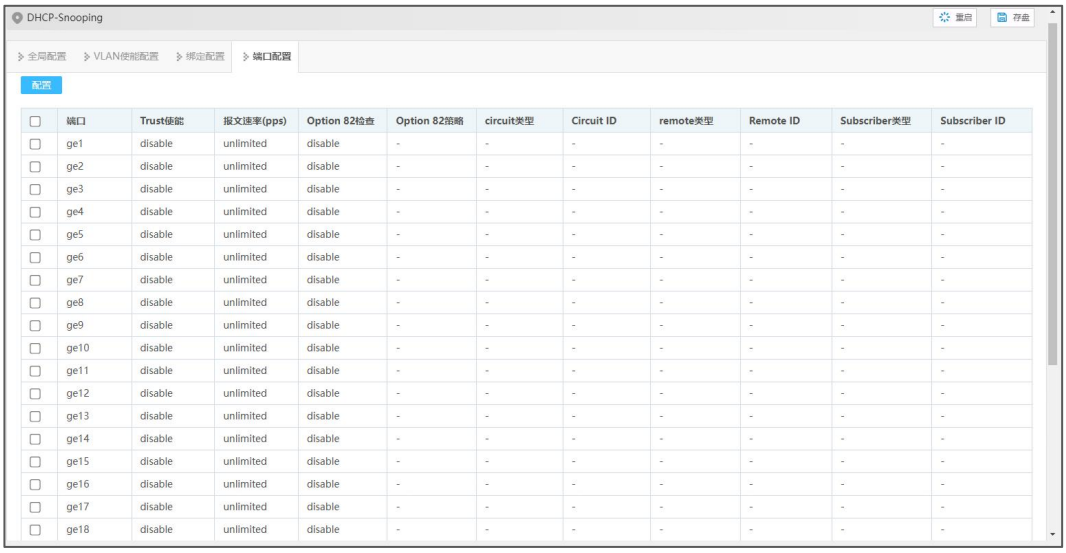
在“端口配置”页面，可以配置 DHCP Snooping 端口信息。

操作路径

按顺序依次打开：“网络管理 > DHCP Snooping > 端口配置”。

界面说明

端口配置界面如下所示：



端口配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
Trust 使能	端口信任使能，信任端口对接收到的 DHCP 报文正常转发。
报文速率	端口的报文传输速度，输入范围为 10 - 1000 (s)，默认值为 1000s。
Option 82 检查	开启 Option 82 检查后，可从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端。
Option 82 策略	Option 82 的处理策略，可选项如下： • Drop：丢弃报文。 • Keep：采用不同的模式填充 Option 82，替换报文中原有的 Option 82 并进行转发，填充模式下面会描述到。 • Replace：保持报文中的 Option 82 不变并进行转发。
circuit 类型	电路 ID 子选项填充类型，可选项如下： • Normal：正常模式； • String：详细模式。
Circuit ID	电路 ID 子选项的填充内容，支持 ASCII 和 HEX 格式。 说明： • 输入长度限制在 2-64 之间； • 选择 Hex 时，输入内容为大小写字母和数字的组合。 • 选择 ASCII 时，内容不做限制。
remote 类型	远端 ID 子选项填充类型，可选项如下： • Normal：正常模式； • Sysname：直接使用设备系统名称来填充 Option 82； • String：详细模式。

界面元素	说明
Remote ID	远程 ID 子选项的填充内容，支持 ASCII 和 HEX 格式。 说明： • 输入长度限制在 2-64 之间； • 选择 Hex 时，输入内容为大小写字母和数字的组合。 • 选择 ASCII 时，内容不做限制。
Subscriber 类型	用户选项填充类型，支持 ASCII 格式。
Subscriber ID	Subscriber ID 子选项的填充内容，支持 ASCII 和 HEX 格式。 说明： • 输入长度限制在 2-64 之间； • 选择 Hex 时，输入内容为大小写字母和数字的组合。 • 选择 ASCII 时，内容不做限制。

10 系统维护

10.1 网络诊断

10.1.1 Ping

功能说明

用 Ping 命令来检查网络是否通畅或者网络连接速度。Ping 命令利用网络上机器 IP 地址的唯一性，给目标 IP 地址发送一个数据包，再要求对方返回一个同样大小的数据包来确定两台网络机器是否连接相通，时延是多少。

操作路径

按顺序依次打开：“系统维护 > 网络诊断 > Ping”。

界面说明

Ping 界面如下所示：

Ping 界面主要元素配置说明：

界面元素	说明
IP	被检测设备的 IPv4 或 IPv6 地址，即目的地址，可通过 ping 命令检测与其他设备之间网络的互通性。

10.1.2 Traceroute

功能说明

测试交换机与目标主机之间的网络情况。Traceroute 通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。一条路径上的每个设备 Traceroute 返回三次测试结果。输出结果中包括每次测试的时间（ms）、设备的名称（如有的话）及其 IP 地址。

操作路径

按顺序依次打开：“系统维护 > 网络诊断 > Traceroute”。

界面说明

Traceroute 界面如下所示：

Traceroute 界面主要元素配置说明：

界面元素	说明
IP	目的设备 IPv4 或 IPv6 地址，填写需要检测的对端设备 IP 地址。

10.1.3 网线诊断

功能说明

可以检测设备电口所使用的电缆是否存在故障。当电缆状态正常时，检测信息中的长度是指该电缆的总长度。当电缆状态异常时，检测信息中的长度是指从本接口到故障位置的长度。8 线制的网线具有 4 组差分线，设备可检测每组差分线的长度和状态。

说明

- 检测电缆长度精度约 5 米，测试结果仅供参考，不同类型或不同厂商的网线检测

结果可能存在差异。

- 检测时，会在短时间内影响该接口的业务正常使用，也可能导致 UP 的接口发生震荡。

操作路径

按顺序依次打开：“系统维护 > 网络诊断> 网线诊断”。

界面说明

网线诊断界面如下所示：

网线诊断界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
差分线 A/B/C/D 状态	差分线的状态，如 OK（正常）、OPEN（开路）、SHORT（短路）、CROSS（交叉/串扰）等。
差分线 A/B/C/D 长度（m）	差分线的长度，单位米。

10.1.4 SFP 数字诊断

功能说明

实时监测 SFP 参数。该功能极大地方便了光纤链路的故障处理过程，降低了现场调试的成本。

操作路径

按顺序依次打开：“系统维护 > 网络诊断> SFP 数字诊断”。

界面说明

SFP 数字诊断界面如下所示：

SFP 数字诊断界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
模块	光模块的相关参数信息。
温度（℃）	该设备 SFP 的温度，单位为℃。SFP 模块的工作温度不应超过模块的正常工作温度范围。
电压（V）	该设备提供给 SFP 的电压，单位为 V。电压过高会带来 CMOS 器件的击穿；电压过低会导致激光器不能正常工作。
偏置电流（mA）	激光偏置电流。
接收功率（mW）	光输入功率，指在一定速率、误码率情况下光模块的最小接收光功率。
发送功率（mW）	光输出功率，指光模块发送端光源的输出功率。

10.2 时间

10.2.1 NTP 配置

NTP 协议全称网络时间协议（Network Time Procotol）。它的目的是在国际互联网上传递统一、标准的时间。具体的实现方案是在网络上指定若干时钟源网站，为用户提供授时服务，并且这些网站间应该能够相互比对，提高准确度。它可以提供毫秒级的时间校正，并采用加密确认的方式来防止恶毒的协议攻击。

功能说明

配置设备时间和 NTP 服务器信息。

操作路径

按顺序依次打开：“系统维护 > 时间 > NTP 配置”。

界面说明

NTP 配置界面如下所示：

NTP 配置界面主要元素配置说明：

界面元素	说明
NTP 使能开关	NTP 协议使能开关。
Master 使能开关	Master 使能开关，启用后，设备开启 NTP 服务，并使用设备本地时钟作为 NTP 主时钟，为其它设备提供时钟源。
服务器	NTP 服务器的 IP 地址，例如：192.168.1.1。 说明： 系统作为 NTP 客户端，将每隔 11 分钟与 NTP 服务器进行一次时间同步。

10.2.2 时间配置

功能说明

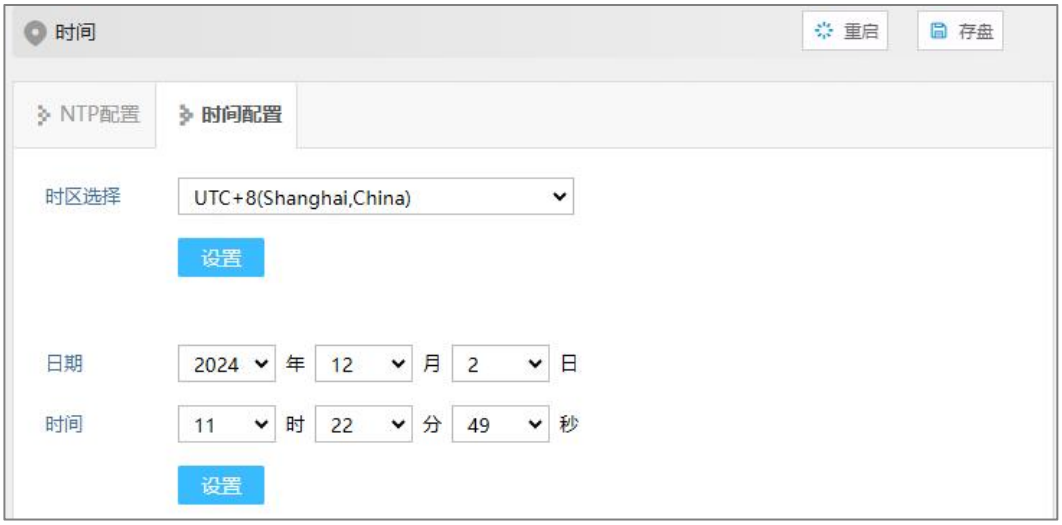
配置设备时间。

操作路径

按顺序依次打开：“系统维护 > 时间 > 时间配置”。

界面说明

时间配置界面如下所示：



时间配置界面主要元素配置说明：

界面元素	说明
时区选择	通用协调时间 UTC（Universal Time Coordinated）时区。由于地域的不同，用户可以根据本国或本地区的规定，自由设置系统时钟。
日期	日期配置，年/月/日。
时间	时间配置，时/分/秒。

10.3 告警

10.3.1 告警触发

功能说明

设备系统提供了多种告警触发源，包括端口状态、温度异常、电源故障以及网络负载过高。当这些触发源被激活时，用户可以通过配置 LED 指示灯、继电器、Trap 消息或邮件报警模式来触发告警，以便及时响应并处理潜在问题。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警触发”。

界面说明

告警触发界面如下所示：

告警触发配置界面主要元素配置说明：

界面元素	说明
ID	告警触发的条目。
告警触发	设备告警触发包括端口、温度、电源以及网络负载。
告警接收	设备报警模式包括 LED、继电器、Trap 和邮件。

10.3.1.1 端口告警

功能说明

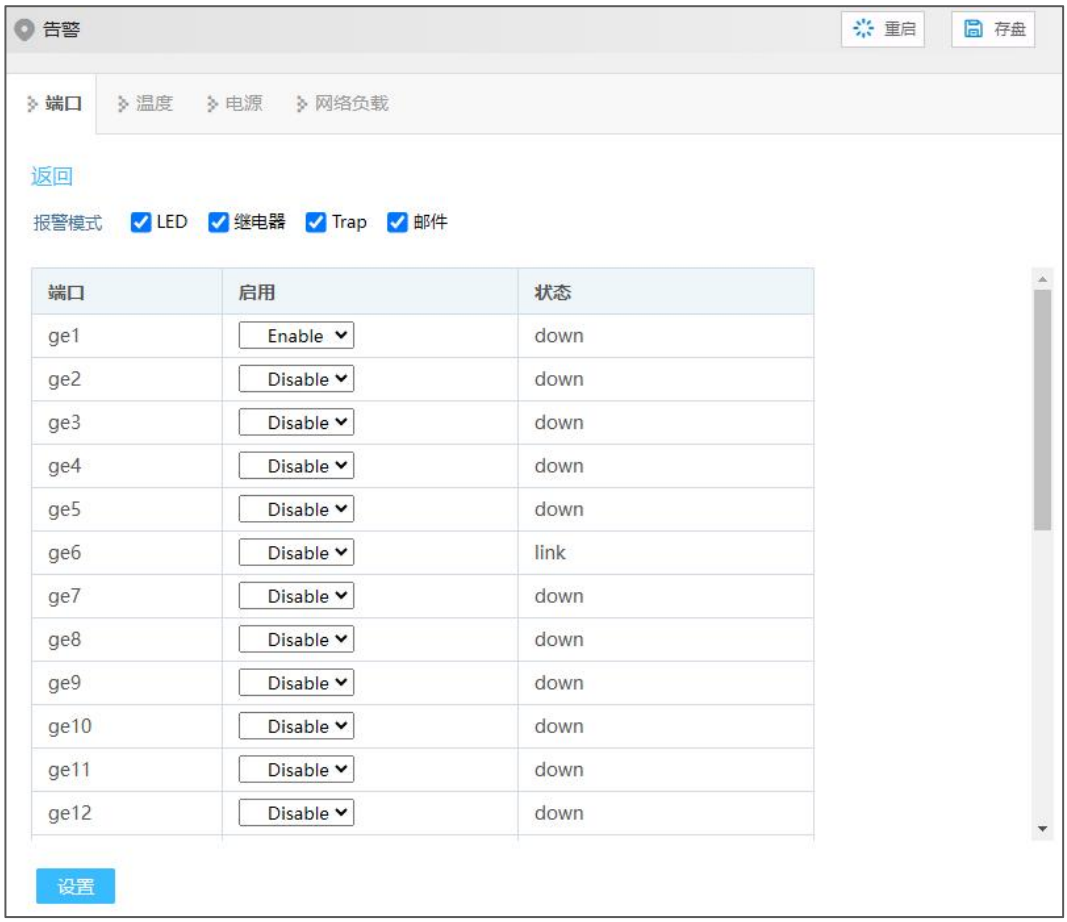
设置端口告警功能。当设备端口处于异常状态时，能及时的通知管理员，并快速修复设备状态，避免过大损失。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警触发 > 端口”。

界面说明

端口告警界面如下所示：



端口告警配置界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
状态	设备端口连接状态，显示项如下： • link • down
告警开关	端口告警功能状态，可选项： • Enable • Disable 说明： 启用端口告警后，当端口出现异常状态时，如连接断开时，设备会输出一个告警信号，通过设置 LED 指示灯、继电器、Trap 消息或邮件提示设备端口异常。
报警模式	端口告警的报警模式，可选项： • LED • 继电器 • Trap • 邮件 说明： 勾选则开启 LED 指示灯、继电器、Trap 消息或邮件报警模式来触发告

界面元素	说明
	警。

10.3.1.2 温度告警

功能说明

设置温度告警功能。当设备温度处于异常状态时，能及时的通知管理员，并快速保护设备，避免造成设备损坏。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警触发 > 温度”。

界面说明

温度告警界面如下所示：

温度告警配置界面主要元素配置说明：

界面元素	说明
状态	温度告警开关状态，可选项： • 启用 • 禁用 说明： 启用温度告警后，当设备温度出现异常状态时，如温度超过设置的上限或下限值时，设备会输出一个告警信号，通过设置 LED 指示灯、继电器、Trap 消息或邮件提示设备温度异常。
温度上限	设置设备的上限温度，范围为-40~120 °C。
温度下限	设置设备的下限温度，范围为-40~120 °C。
当前温度	设备当前的温度状态。

界面元素	说明
报警模式	温度告警的报警模式，可选项： • LED • 继电器 • Trap • 邮件 说明： 勾选则开启 LED 指示灯、继电器、Trap 消息或邮件报警模式来触发告警。

10.3.1.3 电源告警

功能说明

设备系统提供该功能，您可以设置电源告警功能。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警触发 > 电源”。

界面说明

电源告警界面如下所示：

电源告警界面主要元素配置说明：

界面元素	说明
电源号	该设备电源对应的电源名称。
启用	电源告警开关状态，可选项： • Enable • Disable 说明：

界面元素	说明
	电源告警适用于双电源，启用后，当其中一路电源断开或故障时，设备会输出一个告警信号，通过设置 LED 指示灯、继电器、Trap 消息或邮件提示设备电源异常。
状态	设备电源连接状态，显示项如下： • Normal：正常 • Absent：异常
报警模式	电源告警的报警模式，可选项： • LED • 继电器 • Trap • 邮件 说明： 勾选则开启 LED 指示灯、继电器、Trap 消息或邮件报警模式来触发告警。

10.3.1.4 网络负载告警

功能说明

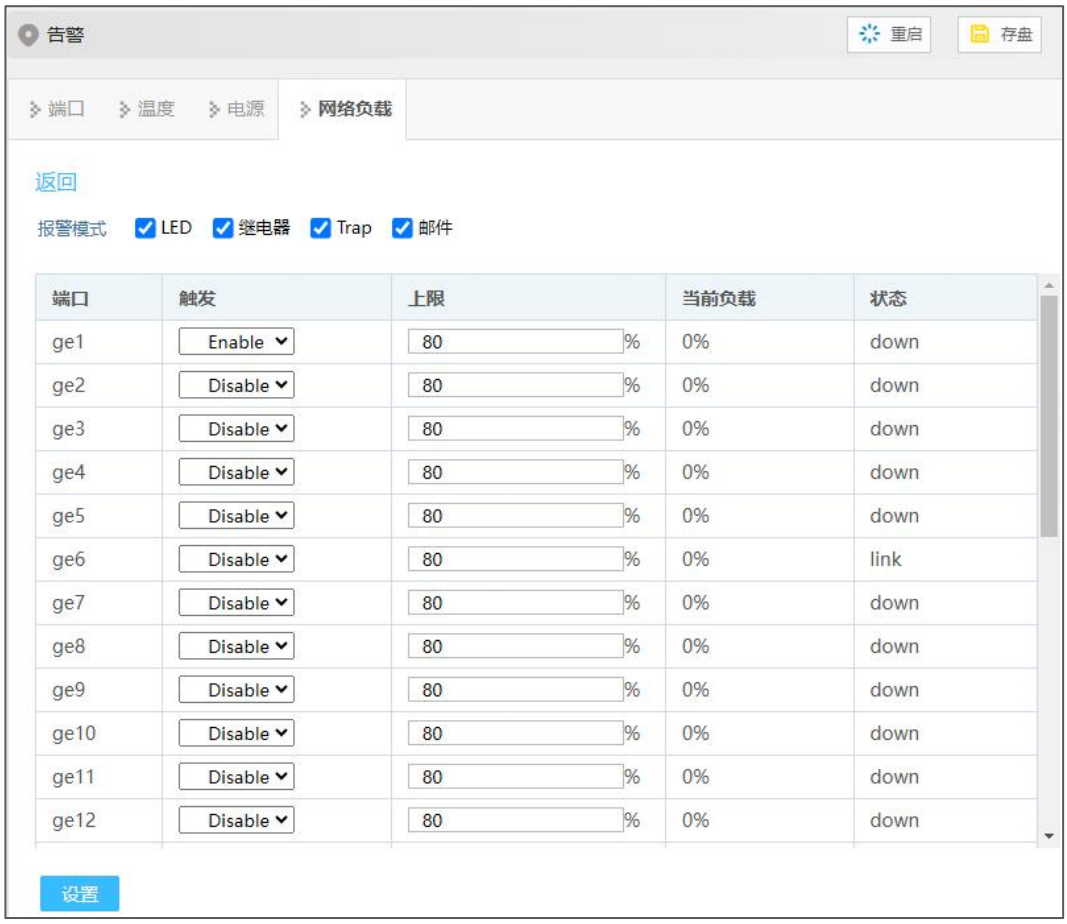
设备系统提供该功能，您可以设置网络负载告警功能。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警触发 > 网络负载”。

界面说明

网络负载告警界面如下所示：



网络负载告警界面主要元素配置说明：

界面元素	说明
端口	该设备以太网端口对应的端口名称。
触发	网络负载告警开关状态，可选项： • Enable • Disable 说明： 启用网络负载告警后，当设备网络负载异常时，如设备当前网络负载超上限值时，设备会输出一个告警信号，通过设置 LED 指示灯、继电器 Trap 消息或邮件提升设备异常。
上限	设置设备网络负载的上限值，范围 0-100。
当前负载	设备当前的网络负载值，若超过上限值，则会触发告警。
状态	设备端口连接状态，显示项如下： • link • down
报警模式	网络负载告警的报警模式，可选项： • LED • 继电器 • Trap

界面元素	说明
	• 邮件 说明： 勾选则开启 LED 指示灯、继电器、Trap 消息或邮件报警模式来触发告警。

10.3.2 告警接收

功能说明

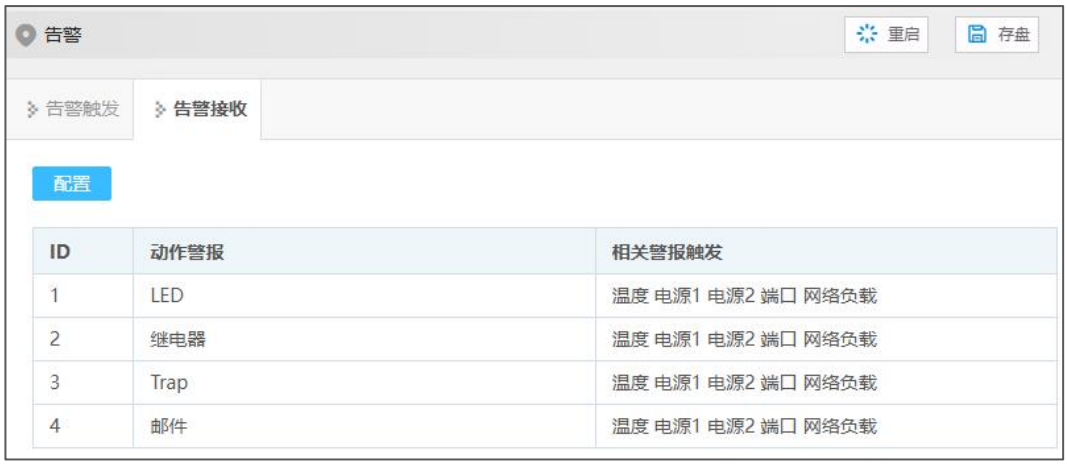
用户可以查看配置的 LED 指示灯、继电器、Trap 或邮件报警模式，以便及时了解设备不同的报警模式。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警接收”。

界面说明

告警接收界面如下所示：



告警接收界面主要元素配置说明：

界面元素	说明
ID	报警模式的条目。
动作报警	设备报警模式包括 LED 指示灯、继电器、Trap 和邮件。
相关警告触发	设备告警触发包括端口、温度、电源以及网络负载。

10.3.2.1 陷阱设置

功能说明

通过 Trap 消息陷阱设置，管理员可以实现对设备或系统状态的实时监控和快速响应，从而能够更及时地发现问题和处理问题。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警接收 > 陷阱设置”。

界面说明

陷阱设置界面如下所示：

陷阱设置界面主要元素配置说明：

界面元素	说明
地址	SNMP 管理设备 IP 地址，用于接收告警信息，如 PC。
模式	SNMP 管理设备版本，可选如下： • v1 • v2c
团队名	团体名称。
端口号	该设备以太网端口对应的端口名称。

10.3.2.2 电子邮件警报

功能说明

在“电子邮件警报”页面，可配置邮件发件人、收件人和邮箱服务器等参数。系统可以使用邮件形式告知设备的热启动、冷启动、登录失败、静态 IP 修改和密码修改等信息。

操作路径

按顺序依次打开：“系统维护 > 告警 > 告警接收 > 电子邮件警报”。

界面说明

电子邮件警报配置设置界面如下所示：

电子邮件警报配置界面主要元素配置说明：

界面元素	说明
使能状态	启用/禁用邮件告警功能。
邮件服务器	使用邮件的服务器地址，要依据使用的邮箱账号填写。为设备提供邮件投递服务的主机 IP 地址或者使用的主机名。
收件人地址	用于接收告警邮件的邮箱地址。
发件人地址	用于发送告警邮件的邮箱地址。
端口号	邮箱服务器的端口号。
TLS	TLS（Transport Layer Security）是一种传输层安全加密协议，用于在网络通信中提供数据的机密性和完整性。通过使用 TLS 协议，邮件的传输过程将被加密，防止敏感信息在传输过程中被窃听或篡改。 “TLS”该项操作如下： • Off：关闭 TLS 加密协议； • On：启用 TLS 传输层安全加密协议。
认证	认证是指是否验证邮箱密码。 “认证”该项操作如下： • Off：关闭验证邮箱密码； • On：启用验证邮箱密码。
登录邮箱地址	登录到邮箱服务器的用户名。
登录邮箱密码	登录到邮箱服务器的用户名密码。

10.4 配置文件管理

10.4.1 当前配置

功能说明

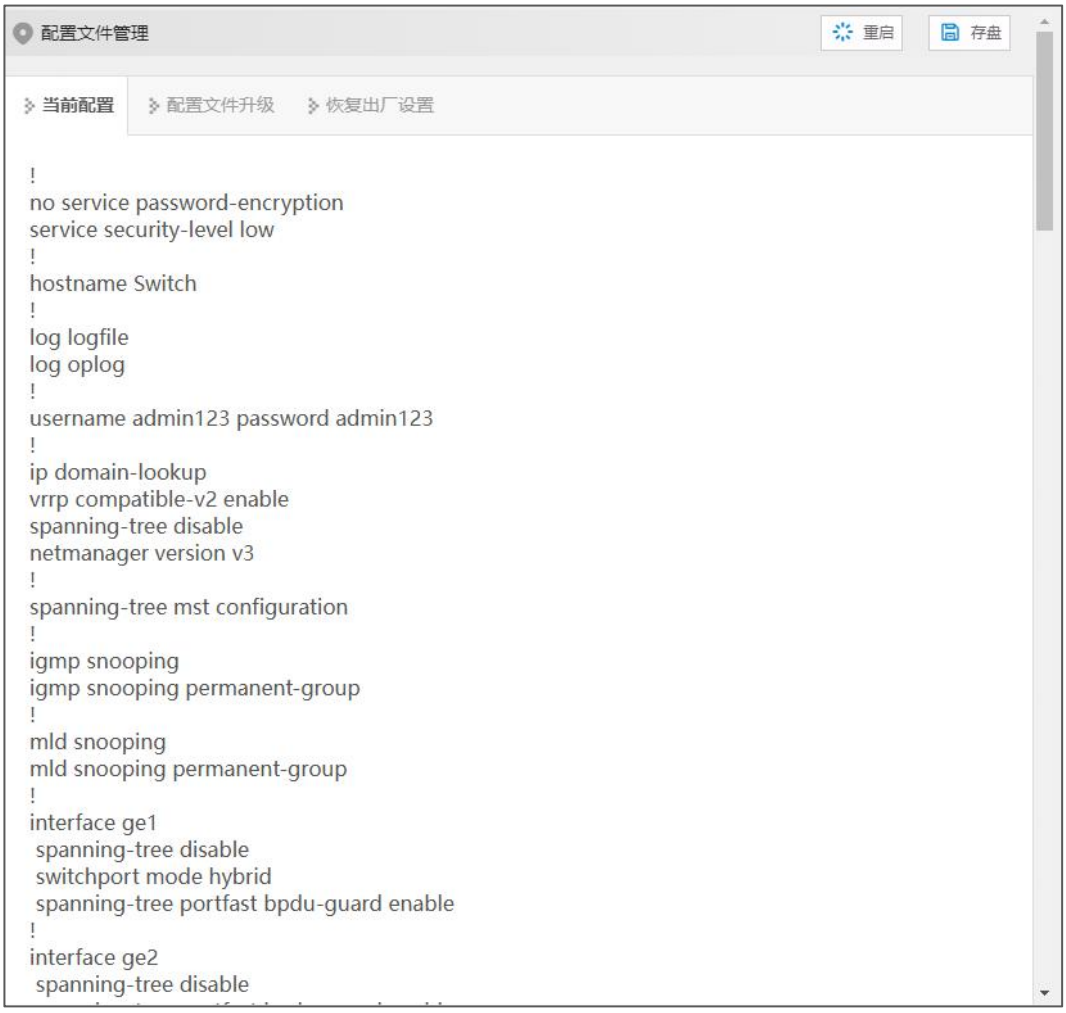
查看当前的配置信息。

操作路径

按顺序依次打开：“系统维护 > 配置文件管理 > 当前配置”。

界面说明

当前配置界面如下所示：



10.4.2 配置文件升级

功能说明

下载、上传配置文件。

操作路径

按顺序依次打开：“系统维护 > 配置文件管理 > 配置文件升级”。

界面说明

配置文件升级界面如下所示：

配置文件升级界面主要元素配置说明：

界面元素	说明
选择文件，或将文件拖入	选择上传的配置文件，可点击该区域选择本地配置文件，或直接拖入本地配置文件至该区域。
上传	选择完上传的配置文件后，单击“上传”按钮，开始上传配置。
点此下载配置文件	单击可下载当前设备的配置文件，默认文件名为“device.conf”。

10.4.3 恢复出厂设置

功能说明

设备恢复到出厂配置。

操作路径

按顺序依次打开：“系统维护 > 配置文件管理 > 恢复出厂设置”。

界面说明

恢复出厂设置界面如下所示：

恢复出厂设置界面主要元素配置说明：

界面元素	说明
一键还原	单击“一键还原”按钮，配置文件将还原为出厂配置。

10.5 软件升级

功能说明

对设备程序进行更新与升级。

操作路径

按顺序依次打开：“系统维护 > 软件升级”。

界面说明

软件升级界面如下所示：

软件升级界面主要元素配置说明：

界面元素	说明
选择文件，或将文件拖入	选择升级的文件，可点击该区域选择本地升级文件，或直接拖入本地升级文件至该区域。
升级	选择完升级的文件后，单击“升级”按钮，开始升级程序。 说明：

界面元素	说明
	一般升级固件为“.bin”格式文件。

10.6 日志信息

10.6.1 日志信息

功能说明

查看设备系统日志信息。日志信息主要记录用户操作、系统故障、系统安全等信息，包括用户日志、安全日志和诊断日志。

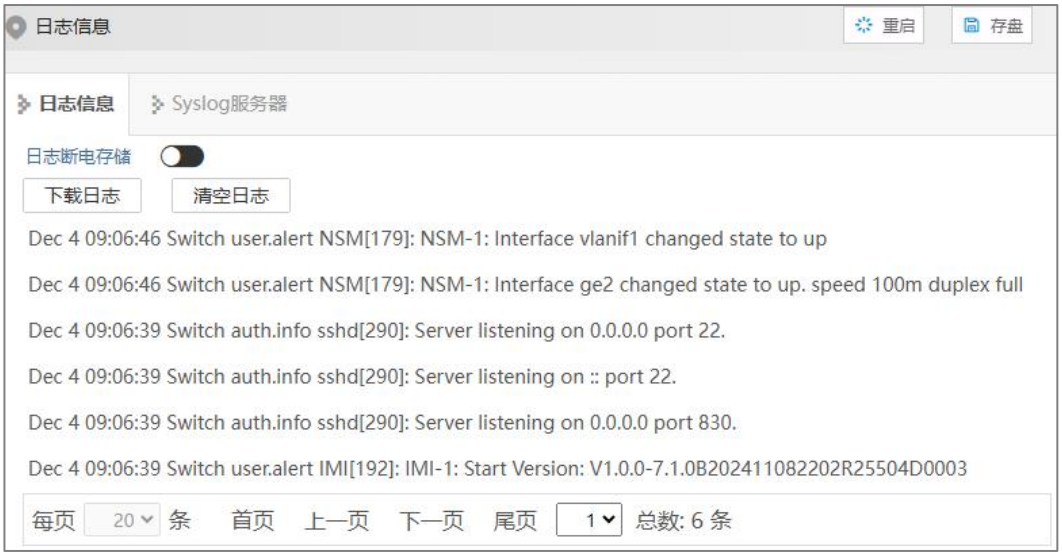
- 用户日志：记录用户操作和系统运行信息。
- 安全日志：记录包含账号管理、协议、防攻击和状态等内容的信息。
- 诊断日志：记录协助进行问题定位的信息。

操作路径

按顺序依次打开：“系统维护 > 日志信息 > 日志信息”。

界面说明

日志信息界面如下所示：



日志信息界面主要元素配置说明：

界面元素	说明
日志断电存储	把日志信息存储到 FLASH，断电后日志信息不会丢失。
下载日志	单击“下载日志”按钮，可下载当前日志信息到本地。
清空日志	单击“清空日志”按钮，可清除当前日志信息记录。

10.6.2 Syslog 服务器

功能说明

配置 syslog 服务器 IP 地址，配置完后系统日志信息能够发送到所配置的 syslog 服务器上。

操作路径

按顺序依次打开：“系统维护 > 日志信息 > Syslog 服务器”。

界面说明

Syslog 服务器界面如下所示：

Syslog 服务器界面主要元素配置说明：

界面元素	说明
Syslog 服务器	Syslog 服务器 IP 地址。 说明： • 支持带端口配置，输入格式为 IP:port，例如：192.168.1.1:80。 • 最多可以同时配置 4 个 syslog 服务器，如果需要取消其中一个或几个 syslog 服务器配置，可以删除输入框内容后点击设置。

11 FAQ 常见问题解答

11.1 登录问题

1. **为什么通过 WEB 浏览配置时显示页面不正常？**

   访问 WEB 前，请先清除 IE 的缓存和 cookies。否则可能导致网页显示不正常。

2. **忘记登录密码怎么办？**

   忘记登录密码可以通过恢复出厂设置初始化密码，具体方法通过 BlueEyes_Ⅱ软件搜索，并使用恢复出厂设置功能即可初始化密码。初始用户名和密码都为“admin123”。

3. **通过 WEB 浏览器配置是否和通过 BlueEyes_Ⅱ软件配置等效？**

   两者配置是一样的，并不冲突。

11.2 配置问题

1. **为什么配置完 Trunking（端口汇聚）功能后，却不能增加带宽？**

   检查设置为 Trunking 的端口属性是否保存一致，例如速率、双工模式、VLAN 等属性。

2. **该如何处理交换机出现部分端口不通的问题？**

   当交换机上出现部分端口不通时，可能是网线故障、网卡故障和交换机端口故障，可通过如下测试定位故障：

   - 连接的计算机和交换机端口保持不变，更换其它网线；
   - 连接的网线和交换机端口保持不变，更换其它计算机；
   - 连接的网线和计算机保持不变，更换其它交换机端口；
   - 若确认为交换机端口故障，请联系供应商维修。

3. **端口自适应状态检测的顺序如何？**

端口自适应状态检测是按如下顺序进行：1000Mbps 全双工，100Mbps 全双工，100Mbps 半双工，10Mbps 全双工，10Mbps 半双工，从高到低依次检测，并自动以所支持的最高速度连接。

11.3 指示灯问题

1. **电源指示灯不亮，是什么原因？**

可能的原因有：

- 未接电源插座或接触不良；故障排除，重新连接电源插座。
- 电源故障或者指示灯故障；故障排除，更换电源或更换设备测试。
- 电源电压无法满足设备要求；故障排除，按照设备说明书配置电源电压。

2. **Link/Act 指示灯不亮，是什么原因？**

可能的原因有：

- 以太网电口的网线部分未连接或接触不良；故障排除，重新连接网线。
- 以太网终端设备或网卡工作不正常；故障排除，排除终端设备故障。
- 未接电源插座或接触不良；故障排除，重新连接电源插座。
- 接口速率模式不匹配；故障排除，检查设备传输速率，双工模式是否匹配。

3. **以太网电口与光口指示灯连接正常，无法传输数据是什么原因？**

系统刚上电或网络配置有所改变时，本设备和网络中的交换机的配置过程需要一定时间。故障排除，本设备和交换机都配置完成后即可传输以太网数据；如未能接通，则将系统断电，重新上电。

4. **通信一段时间后死机，即不能通信，重启后恢复正常？**

原因可能是：

- 周围环境对产品干扰；故障排除，产品接地处理，采用屏蔽线或屏蔽干扰源。
- 现场布线不规范；故障排除，光纤、网线、光缆不能和电源线、高压线一起走线。
- 网线受到静电或浪涌干扰；故障排除，更换屏蔽网线或者装一个防雷器。
- 高低温影响；故障排除，查看设备的温度使用范围。

12 维修和服务

自产品发货之日起，本公司提供 5 年产品质保。依据本公司产品规范，在质保期间，如果产品有任何故障或功能操作失败，本公司将无偿为用户维修或替换该产品。但以上承诺并不覆盖由于不正当使用、意外事故、天然灾难、不正确的操作或不正确的安装所造成的损坏。

为确保消费者受益于本公司管理型交换机产品，通过下面的方式可以得到帮助和问题解决：

- Internet服务；
- 客服热线；
- 产品返修或更换。

12.1 Internet 服务

通过本公司网站可以得到更多有用的信息和使用技巧。网址：http://www.four-faith.net。

12.2 客服热线

使用本公司产品的用户，可以打电话到本公司技术支持办公室，公司有专业的技术工程师回答您的问题，帮助您在第一时间解决您遇到的产品或使用问题。免费服务热线：400-8838-199。

12.3 产品返修或更换

产品维修、更换或退货，应先和公司的技术人员进行确认，然后再和公司销售人员联系并得到问题处理。以上应按照公司的处理程序，与公司的技术人员和销售人员进行协商处理，来完成产品的维修、更换或退货