RS6012 千兆系列
工业以太网交换机

WEB 配置手册

使用手册

安全声明

为保证安全、正确、高效地使用装置，请务必阅读以下重要信息：

1. 装置的安装调试应由专业人员进行；

2. 装置上电使用前请仔细阅读说明书。应遵照国家和电力行业相关规程，并参照说明书对装置进行操作、调整和测试。如有随机材料，相关部分以资料为准；

3. 装置上电前，应明确连线与正确示图相一致；

4. 装置应该可靠接地；

5. 装置施加的额定操作电压应该与铭牌上标记的一致；

6. 严禁无防护措施触摸电子器件，严禁带电插拔端子、拆卸机箱；

7. 接触装置端子，要防止电触击；

8. 如要拆装装置，必须保证断开所有的外部端子连接。否则，触及装置内部带电部分，将可能造成人身伤害；

9. 对装置进行测试时，应使用可靠的测试仪；

10. 装置的运行参数和定值同样重要，应准确设定才能保证装置功能的正常运行。

版本声明

- 本说明书适用于 RS6012 千兆系列工业以太网交换机。
- 本说明书包含技术内容介绍和现场调试大纲。
- 本说明书仅适用于 RS6012 千兆系列工业以太网交换机 V1.0.0.1 及以上版本软件。

产品说明书版本修改记录表

10				
9				
8				
7				
6				
5				
4				
3				
2	V1.2	修正本文中的错误描述	V1.1	2016/04
1	V1.1	RS6012 千兆以太网交换机说明书初始版	V1.0	2015/12
序号	**说明书版本号**	**修 改 摘 要**	**初始软件版本号**	**修改日期**

＊ 技术支持：电话+86-755-26641737

＊ 传真+86-755-26640197

＊

＊ 本说明书可能会被修改，请注意核对实际产品与说明书是否相符

目录

物品清单

小心打开交换机包装盒，检查包装盒里面应有以下配件：

- 一台以太网交换机；
- 一根交流电源连接线；
- 一本使用说明书（电子文档）；
- 一张保修卡与合格证；
- 安装组件和其它配件；

如果发现有所损坏或者任何配件短缺情况，请及时和我们联系；

第一章 产品介绍

1.1. 产品概述

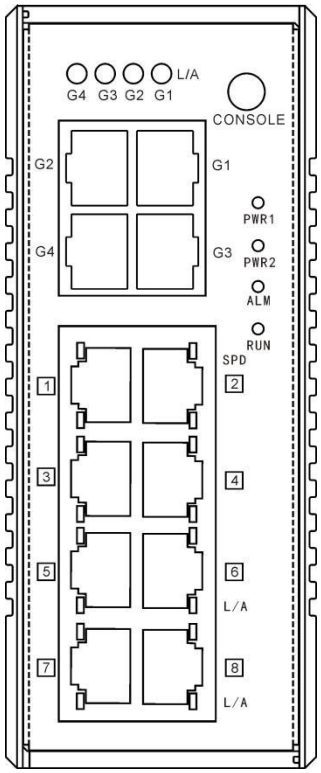
RS6012 千兆系列是针对网络高清监控、网络工程等需求而开发的安防监控专用以太网交换机。包含 RS6012-4GF8GT：提供 4 个千兆光口，8 个千兆电口；产品提供高速的包转发能力以及充裕的背板带宽，保证图像清晰，流畅的传输。嵌入静电、浪涌保护电路，提高产品稳定性。支持广播风暴控制、端口限速和流控等等功能，同时支持串口、Telnet、WEB、snmp 远程配置管理和维护功能。起到保护信息安全、防止病毒传播和网络攻击得作用，充分满足网络视频监控系统、网络工程的需求。

1.2. 产品特点

- 主要端口：提供 4 个千兆光口，8 个千兆电口，电口支持 MDI/MDIX；
- 特色功能：CLI 管理、WEB 管理、端口设置、端口隔离、广播风暴、流控、限速、VLAN、Qos、STP/RSTP/MSTP、ERPS、SNMP
- 电源输入：AC 100~240V / DC9~60V；
- 传输距离：下联电口 0-100 米，上联光口根据光模块性能决定；
- 符合标准：IEEE802.3，IEEE802.3u，IEEE802.3ab，IEEE802.3z，802.1q，802.1p，802.1d，802.1w 标准；
- 支持协议：SNMP v1、v2、v3，STP/RSTP/MSTP，HTTP；

1.3. 设备面板图

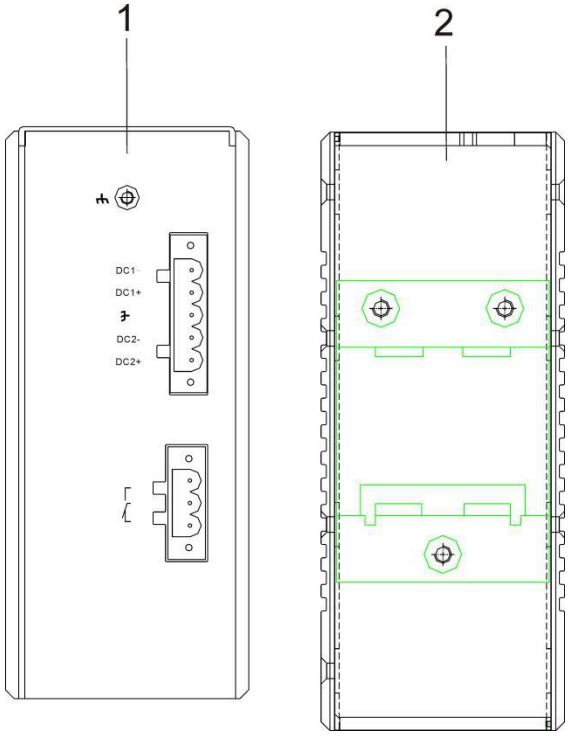
1) 前面板



2) 后面板

1：冗余电源输入端子和一组继电器端子

2：DIN 卡轨安装位置



1.4. 规格参数

项目		描述
型号		RS6012 千兆系列
电源部分	供电方式	交/直流供电
	适应电压范围	AC 100～240V/DC9~60V
	功耗	＜10W
网络端口参数	网络端口	电口：10/100/1000Mbps 光口：100/1000Mbps
	传输距离	电口： 0-100m 光口：20km
网络交换规格	网络标准	支持 IEEE 802.3/802.3u/802.3z/802.3ab
	报文缓存大小	4Mbits
	MAC 地址容量	8K
状态指示	电源灯	1 个（绿色）
	电口指示灯	亮灯指示 Link，闪烁指示 Act，灭灯显示无连接
	光口指示灯	亮灯指示 Link，闪烁指示 Act，灭灯显示无连接
防护等级	脉冲群	4 级 执行标准： IEC61000-4-4
	整机静电防护	1a 接触放电 4 级 1b 空气放电 4 级 执行标准： IEC61000-4-2
	浪涌抗扰度	4 级 执行标准： IEC61000-4-5
操作环境	工作温度	-40℃～85℃
	存储温度	-40℃～85℃
	湿度（无凝结）	5-95%
机体属性	尺寸(长×宽×高) 含接口	135mm*129mm*55mm
	材料	铝壳
	颜色	黑色
	重量	3.1kg
可靠性	平均故障间隔时 (MTBF)	≥500000h
	质保	5 年质保期

1.5. LED 指示灯

LED	指示	状态说明
PWR	亮	电源 PWR 连接运行正常
	灭	电源 PWR 未连接或运行不正常
L/A	亮	端口已建立有效的网络连接
	闪烁	端口处于网络运行状态
	灭	端口未建立有效的网络连接
SPD	亮	端口速率 1000Mbps
	灭	端口速率 10/100Mbps
ALM	亮	交换机有告警事件
	灭	交换机无告警事件
RUN	常灭或常亮	交换机工作异常或进入启动状态
	规律闪烁	交换机正常稳定工作

第二章 安装前的准备

2.1. 注意事项

为避免使用不当造成设备损坏及对人身的伤害，请遵从以下的注意事项：

- 在清洁交换机前，应先将交换机电源插头拔出。不要用湿润的布料擦拭交换机，不可用液体清洗交换机。
- 请不要将交换机放在水边或潮湿的地方，并防止水或湿气进入交换机机壳。
- 请不要将交换机放在不稳定的箱子或桌子上，万一跌落，会对交换机造成严重损害。
- 应保持室内通风良好并保持交换机通气孔畅通。
- 交换机要在正确的电压下才能正常工作，请确认工作电压同交换机所标示的电压相符。
- 为减少受电击的危险，在交换机工作时不要打开外壳，即使在不带电的情况下，也不要随意打开交换机机壳。
- 在更换接口板时一定要使用防静电手腕，防止静电损坏单板。

2.2. 检查安装场所

以太网交换机必须在室内使用，无论您将交换机安装在机柜内还是直接放在工作台上，

都需要保证以下条件：

- 确认交换机的入风口及通风口处留有空间，以利于交换机机箱的散热。
- 确认机柜和工作台自身有良好的通风散热系统。
- 确认机柜及工作台足够牢固，能够支撑交换机及其安装附件的重量。
- 确认机柜及工作台的良好接地。

2.3. 安装工具

- 一字螺丝刀
- 十字螺丝刀
- 防静电手腕

第三章 安装

3.1. 安装方式

第一步，安装导轨：

将导轨固定在机架上，如图 3.1 所示：

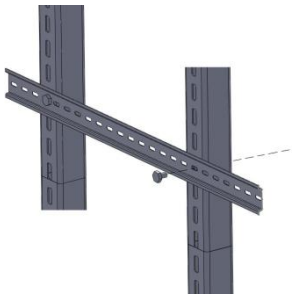


图 3. 1 安装导轨

第二步，安装交换机：

向下按压交换机，使其卡接在导轨上，如下图：

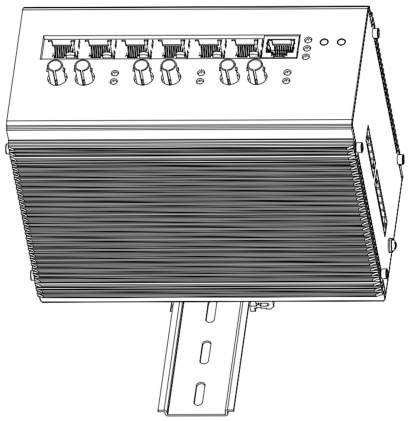


图 3. 2 安装交换机

第三步，拆除交换机：

先用力向下按压交换机，再向上将交换机从导轨上取下。

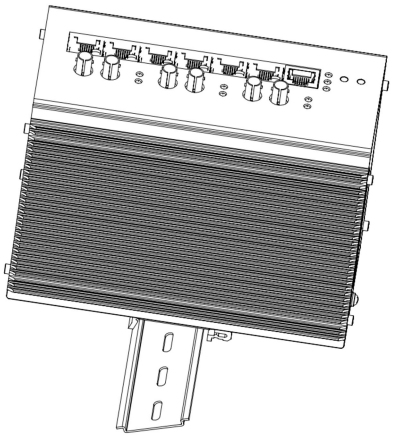


图 3. 3 拆除交换机

3.2. 连接线缆

(1) 安装前请关闭各个信号源和待显示设备的电源，带电安装可能会造成传输设备的损坏；

(2) 用网络电缆分别连接网络摄像机和设备的端口；

(3) 用光纤线连接设备的 UPLINK 光纤接口和上联设备的光纤接口。

(4) 连接设备的电源；

(5) 检查安装是否正确，设备有无损坏，确保所有连接可靠，给系统上电；

(6) 确认各网络设备是否有供电，工作是否正常。

第四章 附录-端口属性

4.1. 以太网端口属性

	描述
接口类型	RJ45
工作速率	10Mbit/s、100Mbit/s、1000Mbit/s 自适应
双工模式	半双工、全双工、自适应
网线标准	MDI/MDI-X
符合标准	IEEE802.3/802.3u/802.3ab
网线类型	10Base-T：3/4/5 类双绞线，支持最大传输距离 100m 100Base-TX：5/6 类双绞线，支持最大传输距离 100m 1000Base-TX：5/6 类双绞线，支持最大传输距离 100m

4.2. 光模块接口属性

	描述
接口类型	SFP
工作速率	100/1000Mbps
双工模式	全双工
符合标准	IEEE802.3u，IEEE802.3z
介质和传输距离	50/125um 多模光纤，支持 550m 传输距离 62.5/125um 多模光纤，支持 270m 传输距离 9/125um 单模光纤，支持 3-120KM 传输距离

4.3. 交换机 Console 口缺省配置

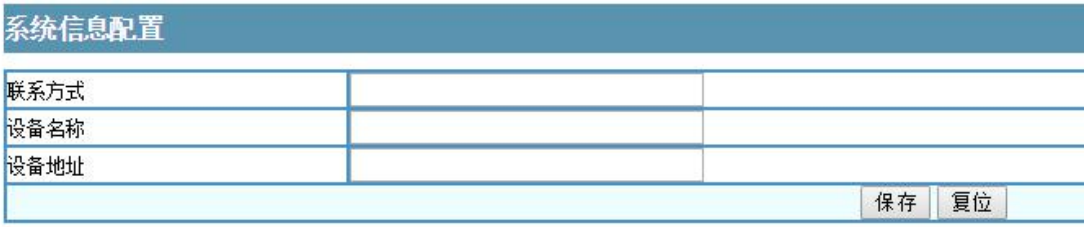
属性	缺省配置
传输速率	115200bits/s

流控方式	不进行流控
校验方式	不进行校验
停止位	1
数据位	8
默认用户名：admin，默认密码为空	

第五章 系统配置

5.1. 系统信息

在此页显示交换机的系统信息（交换机默认 IP:192.168.1.254，默认用户名：admin，默认密码为空）。

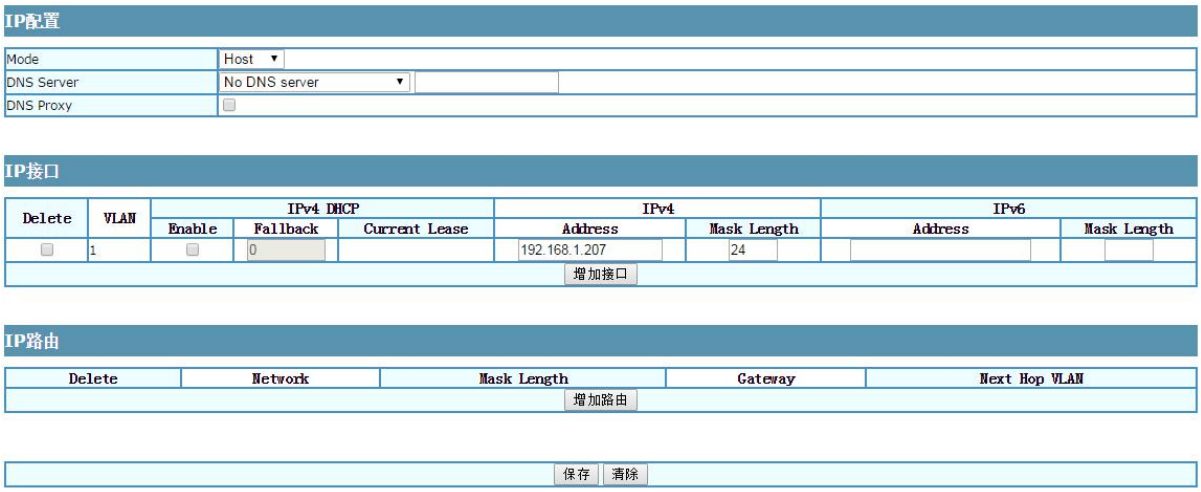


系统信息配置界面各项参数说明如下表所示：

配置项	说明
联系方式	本栏目填写的内容是对管理该节点的联系人的文本描述，以及如何联系该人的信息。可允许的字符串长为 0～255 个 NVT ASCII 字符（32-126）。
设备名称	本栏目填写的内容是对该管理节点分配的管理名。系统名是由字母（A-Z, a-z）和数字（0-9），减号（-）组成。其中，不能有空格或留空的字符出现。第一个字符必须是一个字母字符。第一个和最后一个字符不可以是减号字符。可允许的字符长为 0~255。
设备地址	本栏目填写的内容是本节点的物理位置（比如：电话橱，三楼）。可允许的字符串长为 0～255 个 NVT ASCII 字符（32-126）。

5.2. IP 地址

此页面提供 IP 基本设置，交换机默认 IP 地址为 192.168.1.254，默认掩码为 255.255.255.0，控制 IP 接口和 IP 路由。



本设备支持的最大接口数为 8，最大路由数为 32。

5.2.1. IP 设置

模式

配置 IP 栈是否应作为主机或路由器。 在主机模式下，接口之间的 IP 流量不会被路由。 在路由器模式下，流量在所有接口之间被路由。

DNS 服务器

此设置控制交换机完成的 DNS 名称解析。 本设备支持以下模式：

(1) 从任何 DHCP 接口

将使用从 DHCP 租期提供已给启用 DHCP 的接口的第一个 DNS 服务器。

(2) 不使用 DNS 服务器

不使用 DNS 服务器。

(3) 配置的

明确地提供 DNS 服务器的 IP 地址，此 IP 地址以点分十进制格式显示。

(4) 从此 DHCP 接口

指定应从哪个已启用 DHCP 的接口提供的 DNS 服务器。

DNS 代理

当启用 DNS 代理时，系统会将 DNS 请求中继到当前配置的 DNS 服务器，并作为 DNS 解析器回复到网络上的客户端设备。

IP 接口

(1) 删除

选择此选项可删除现有的 IP 接口。

(2) VLAN

与 IP 接口相关联的 VLAN。 只有此 VLAN 中的端口将能够访问 IP 接口。 此字段仅在创建新接口时可用于输入。

(3) 启用 IPv4 DHCP

选中此框以启用 DHCP 客户端。 如果启用此选项，系统将使用 DHCP 协议配置接口的 IPv4 地址和掩码。 DHCP 客户端将通知配置的系统名称作为主机名，以提供 DNS 查找。

(4) IPv4 DHCP fallback 超时

尝试获取 DHCP 租期的秒数。 该时间段过期后，已配置的 IPv4 地址将用作 IPv4 接口地址。 值为零将禁用 fallback 机制，以便 DHCP 将继续重试，直到获得有效的租期。 合法值为 0 到 4294967295 秒。

(5) IPv4 DHCP 当前租期

对于具有活动租期的 DHCP 接口，此列显示 DHCP 服务器提供的当前接口地址。

(6) IPv4 地址

接口的 IPv4 地址，以点分十进制格式显示。

如果启用 DHCP，则此字段配置 fallback 地址。 如果不希望在接口上进行 IPv4 操作，或者不需要 DHCP fallback 地址，则可以将该字段留空。

(7) IPv4 掩码

IPv4 网络掩码，以比特数（前缀长度）作为单位。 对于 IPv4 地址，有效值介于 0 和 30 位之间。

如果启用 DHCP，则此字段配置 fallback 地址网络掩码。 如果不希望在接口上进行 IPv4 操作，或者不需要 DHCP fallback 地址，则可以将该字段留空。

(8) IPv6 地址

接口的 IPv6 地址。 IPv6 的 128 位地址通常写成 8 组，每组为四个十六进制数的形式，每组（:)分隔一个冒号。 例如，AD80:0000:0000:0000:ABAA:0000:00C2:0002。 符号::是一种特殊语法，可用作表示多个 16 位零压缩法的简写方式; 但它只能出现一次。例如上述地址就可写成 AD80::ABAA:0000:00C2:0002。

系统仅接受有效的 IPv6 单播地址，但是接受 IPv4 兼容地址和 IPv4 映射地址。

如果不希望在接口上进行 IPv6 操作，则该字段可以留空。

(9) IPv6 掩码

IPv6 网络掩码，以位数（前缀长度）作为单位。 对于 IPv6 地址，有效值介于 1 和 128 位之间。

如果不希望在接口上进行 IPv6 操作，则该字段可以留空。

IP 路由

(1) 删除

选择此选项删除在现有的 IP 路由。

(2) 网络

该路由的目的 IP 网络或主机地址。有效的格式为点分十进制或有效的 IPv6 表示。缺省路由也可以使用值 0.0.0.0 或 IPv6::表示。

(3) 掩码长度

目的地 IP 网络或主机掩码，单位为比特（前缀长度）的数量。它定义了为了符合此路线多少位网络地址必须匹配。有效值为 0 位到 32 位，对于 IPv6 路由到 128 位。只有一条默认路由将有掩码长度 0（因为它会匹配任何地址）。

(4) 网关

IP 网关的 IP 地址。有效的格式为点分十进制或者有效的 IPv6 表示。网关和网络必须是同一类型的网络。

(5) 下一跳 VLAN（仅适用于 IPv6 的）

与网关关联的特定 IPv6 接口的 VLAN ID（VID）。

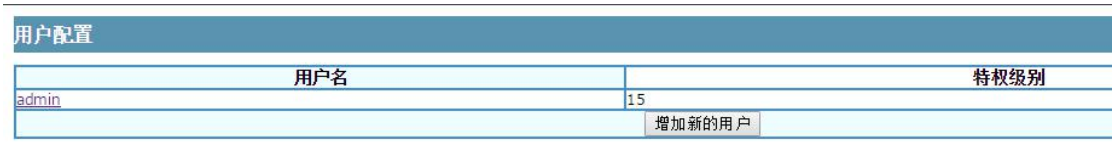
给定的 VID 范围从 1 到 4094，只有当相应的 IPv6 接口是有效的时候才起效。

如果 IPv6 网关地址是本地链路，它必须指定网关的下一跳 VLAN。

如果 IPv6 网关地址不是本地链路，系统会忽略网关的下一跳 VLAN。

5.3. 用户设置

此页面提供有关当前用户的概述。



用户配置页面各项参数说明如下表所示：

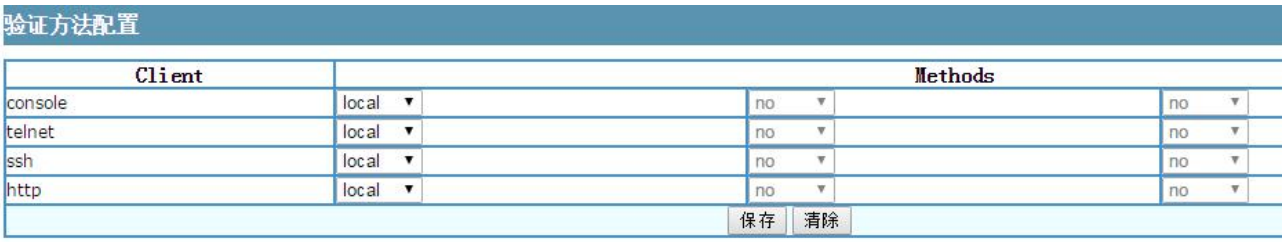
配置项	说明
用户名	标识用户的名称；这也是添加/编辑用户的链接
特权级别	用户的权限级别。 允许的范围是 1 到 15。如果特权级别值是 15，它可以访问所有组，即授予对设备的完全控制。但是其他值需要引用每个组的特权级别。用户的特权应该等于或大于组特权级别，以具有该组的访问权限。默认设置下，大多数组权限级别 5 具有只读访问权限，权限级别 10 具有读写权限。并且系统维护（软件上传，出厂默认值等）需要用户权限级别 15。通常，权限级别 15 可以用于管理员帐户，用于标准用户帐户的权限级别 10 和用于访客帐户的权限级别 5

第六章 设备控制

6.1. 用户安全

6.1.1. 验证方法配置

此页面允许您配置用户在通过其中一个管理客户端接口登录交换机时如何进行身份验证。



验证方法配置各项参数说明如下表所示：

配置项	说明
客户	管理客户端。
方法	方法可以设置为以下值之一： no：禁用身份验证，无法登录。 local：使用交换机上的本地用户数据库进行身份验证。 radius：使用远程 RADIUS 服务器进行认证。 tacacs +：使用远程 TACACS +服务器进行身份验证。 如果远程服务器脱机，则涉及远程服务器的方法将超时。在这种情况下，尝试下一个方法。每种方法从左到右进行尝试，并继续尝试直到方法批准或拒绝用户。如果远程服务器用于主身份验证，建议将辅助身份验证配置为“本地”。如果没有配置的认证服务器在线，这将使管理客户端能够通过本地用户数据库登录。

6.1.2. SSH

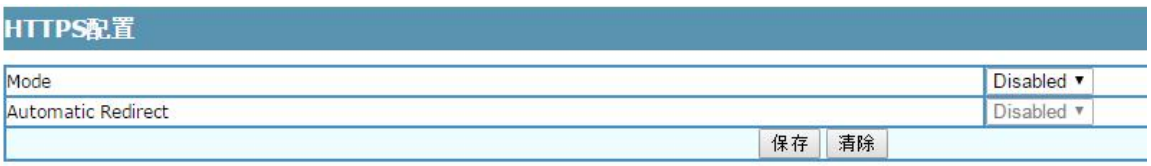
在此页面上配置 SSH。

SSH 配置各项参数说明如下表所示：

配置项	说明
模式	表示 SSH 模式操作。 可能的模式有： 启用：启用 SSH 模式操作。 禁用：禁用 SSH 模式操作。

6.1.3. HTTPS

在此页面上配置 HTTPS。



HTTPS 配置各项参数说明如下表所示：

配置项	说明
模式	表示 HTTPS 模式操作。 当前连接为 HTTPS 时，要应用 HTTPS 禁用模式操作，将自动将 Web 浏览器重定向到 HTTP 连接。 可能的模式有： 启用：启用 HTTPS 模式操作。 禁用：禁用 HTTPS 模式操作。
自动重定向	表示 HTTPS 重定向模式操作。 它仅在选择 HTTPS 模式“启用”时才能起效。 当启用 HTTPS 模式和自动重定向时，自动将 Web 浏览器重定向到 HTTPS 连接。 可能的模式有： 启用：启用 HTTPS 重定向模式操作。 禁用：禁用 HTTPS 重定向模式操作。

6.1.4. 访问管理配置

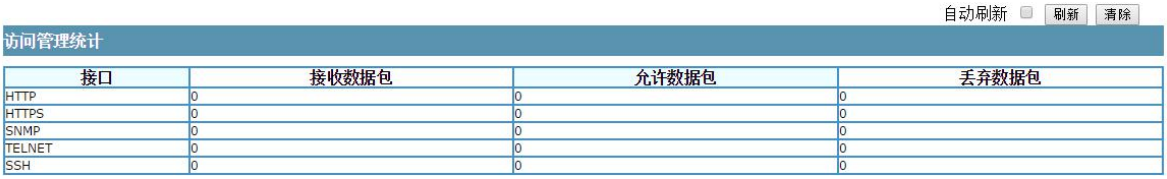
在此页面上配置访问管理表。最大条目数为 16。如果应用程序的类型匹配任一访问管理表项，它将允许访问交换机。

访问管理配置各项参数说明如下表所示：

配置项	说明
模式	表示访问管理模式操作。可能的模式有： 启用：启用访问管理模式操作。 禁用：禁用访问管理模式操作。
删除	选中以删除条目。它将在下次保存时被删除。
VLAN ID	表示访问管理表项的 VLAN ID
起始 IP 地址	表示访问管理表项的起始 IP 地址。
结束 IP 地址	表示访问管理表项的结束 IP 地址。
HTTP / HTTPS	表示如果主机 IP 地址与条目中提供的 IP 地址范围匹配，主机可以从 HTTP / HTTPS 接口访问交换机。
SNMP	表示如果主机 IP 地址与条目中提供的 IP 地址范围匹配，主机可以从 SNMP 接口访问交换机。
TELNET / SSH	表示如果主机 IP 地址与条目中提供的 IP 地址范围匹配，主机可以从 TELNET / SSH 接口访问交换机。

6.1.5. 访问管理统计

此页面提供了访问管理的统计信息。



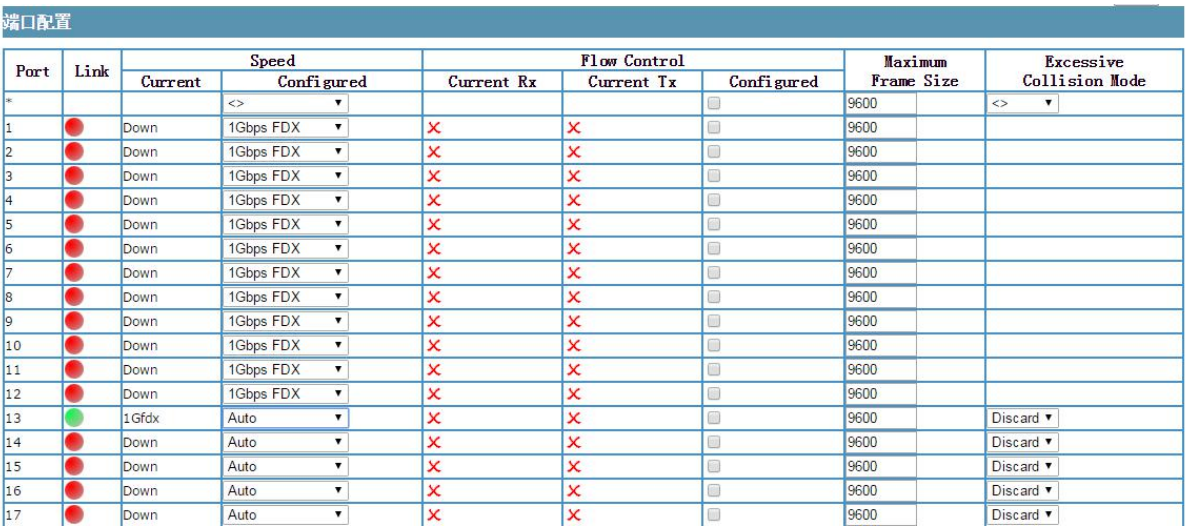
访问管理配置各项参数说明如下表所示：

配置项	说明
接口	远程主机可以通过其访问交换机的接口类型。
接收数据包	启用访问管理模式时从接口接收的数据包数。
允许数据包	启用访问管理模式时从接口允许的数据包数。
丢弃数据包	启用访问管理模式时从接口丢弃的数据包数。

6.2. 端口

6.2.1. 端口控制

此页面显示当前端口配置。 端口也可以在这里配置。



端口配置各项参数说明如下表所示：

配置项	说明
端口	这是此行的逻辑端口号。
链接	以图形方式显示当前链路状态。 绿色表示链接已关闭，红色表示链接已关闭。

当前链接速度	提供端口的当前链路速度。
配置的链路速度	选择给定交换机端口的任何可用链路速度。只显示特定端口支持的速度。可能的速度有： 禁用 - 禁用交换机端口。 自动 - 端口与链路其他设备的自动协商速度，并选择与链路其他设备兼容的最高速度。 10Mbps HDX - 强制 cu 端口在 10Mbps 半双工模式。 10Mbps FDX - 强制 cu 端口在 10Mbps 全双工模式。 100Mbps HDX - 强制 cu 端口在 100Mbps 半双工模式。 100Mbps FDX - 强制 cu 端口在 100Mbps 全双工模式。 1Gbps FDX - 强制端口在 1Gbps 全双工
流量控制	当在端口上选择自动速度时，此部分指示通告给链路其他设备的流控制能力。 当选择固定速度设置时，就是所使用的。 当前 Rx 列指示是否服从端口上的暂停帧，并且当前 Tx 列指示是否传输端口上的暂停帧。Rx 和 Tx 设置由上一次自动协商的结果决定。 检查已配置的列以使用流控制。 此设置与配置的链接速度的设置相关。 注意：100FX 标准不支持自动协商，因此在 100FX 模式下，流量控制功能将始终显示为“禁用”。
最大帧大小	输入交换机端口允许的最大帧大小，包括 FCS。
冗余模式	配置端口传输冲突行为。 丢弃：在 16 次碰撞后丢弃帧（默认值）。 重新启动：在 16 次冲突后重新启动退避算法

6.2.2. 端口统计概述

此页面提供所有交换机端口的一般流量统计信息的概述。

端口统计概述

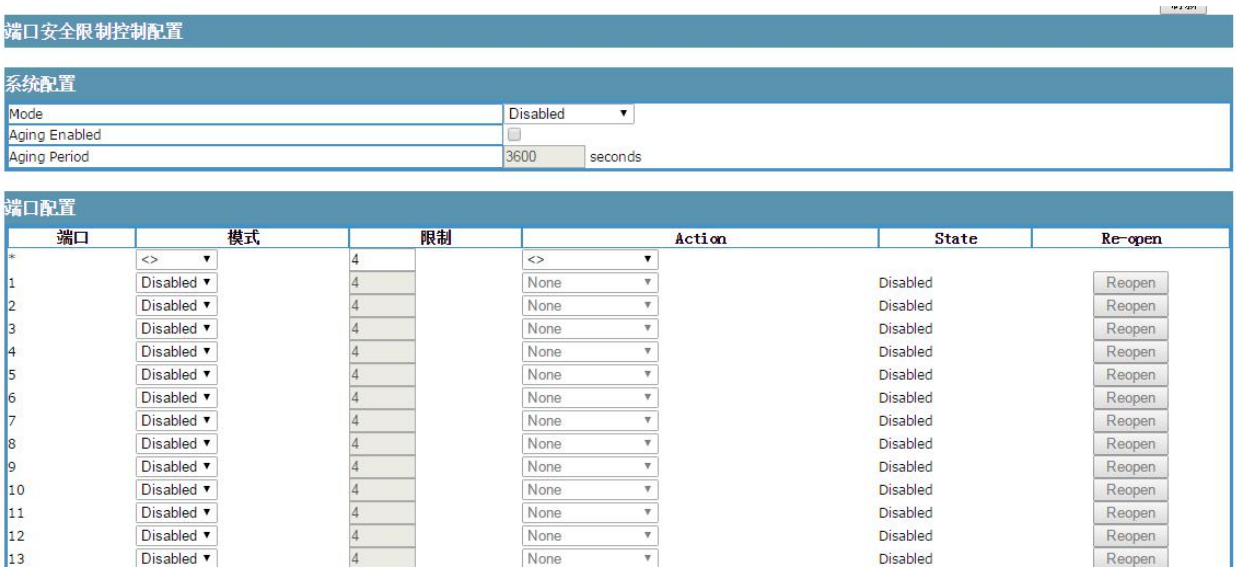
端口	Packets		Bytes		Errors		Drops		Filtered
	接收	发送	接收	发送	接收	发送	接收	发送	接收
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	8442	2452	1226550	644886	0	0	0	0	130
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

端口统计概述界面各项参数说明如下表所示：

配置项	说明
端口	同一行中包含的设置的逻辑端口。
数据包	每个端口接收和发送的数据包数。
字节	每个端口接收和传输的字节数。
错误	错误接收的帧数和每个端口不完整传输的数量。
丢弃	由于入口或出口拥塞而丢弃的帧数。
过滤	通过转发过程过滤的接收帧数。

6.2.3. 端口安全

此页面用于配置端口安全限制控制配置和端口配置。



端口安全限制控制配置

系统配置

Mode	Disabled
Aging Enabled	
Aging Period	3600 seconds

端口配置

端口	模式	限制	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9	Disabled	4	None	Disabled	Reopen
10	Disabled	4	None	Disabled	Reopen
11	Disabled	4	None	Disabled	Reopen
12	Disabled	4	None	Disabled	Reopen
13	Disabled	4	None	Disabled	Reopen

限制控制用于限制指定端口上的用户数。用户由 MAC 地址和 VLAN ID 来标识。如果在端口上启用“限制控制”，则该限制指定端口上的最大用户数。如果超过此数值，则采取措施。动作可以是如下所述的四个不同动作中的一个。

限制控制模块使用下层模块端口安全模块，该模块管理在端口上学习的 MAC 地址。

限制控制配置由两个部分组成，系统配置和端口配置。

6.2.3.1. 系统配置

系统配置项各参数说明如下表所示：

配置项	说明
模式	指明是否在交换机上全局启用或禁用“限制控制”。如果全局禁用，其他模块仍可以使用底层功能，但禁用限制检查和相应的操作。
启用老化	如果选中，受保护的 MAC 地址将在老化时间内进行讨论。
老化时间	如果选中“老化启用”，则使用此输入控制老化时间。如果其他模块使用底层端口安全性来保护 MAC 地址，则它们可能对老化时间有其他要求。底层端口安全将使用使用该功能的所有模块的较短的请求的老化时间。老化时间可以设置为 10 到 10,000,000 秒之间的数字。要了解为什么需要进行老化，请考虑以下情况： 假设终端主机连接到第三方交换机或集线器，该集线器或集线器又连接到启用了限制控制的此交换机上的端口。如果未超过限制，则允许终端主机转发。 现在假设终端主机注销或关闭电源。如果它不是老化的，则终端主机仍将占用该交换机上的资源，并且将被允许转发。要克服这种情况，请启用老化。启用老化后，一旦终端主机得到保护，定时器启动。当定时器期满时，交换机开始从端主机寻找帧，并且如果在下一个老化时间内看不到这样的帧，则假定终端主机断开，并且在交换机上释放相应的资源。

6.2.3.2. 端口配置

端口配置项各参数说明如下表所示：

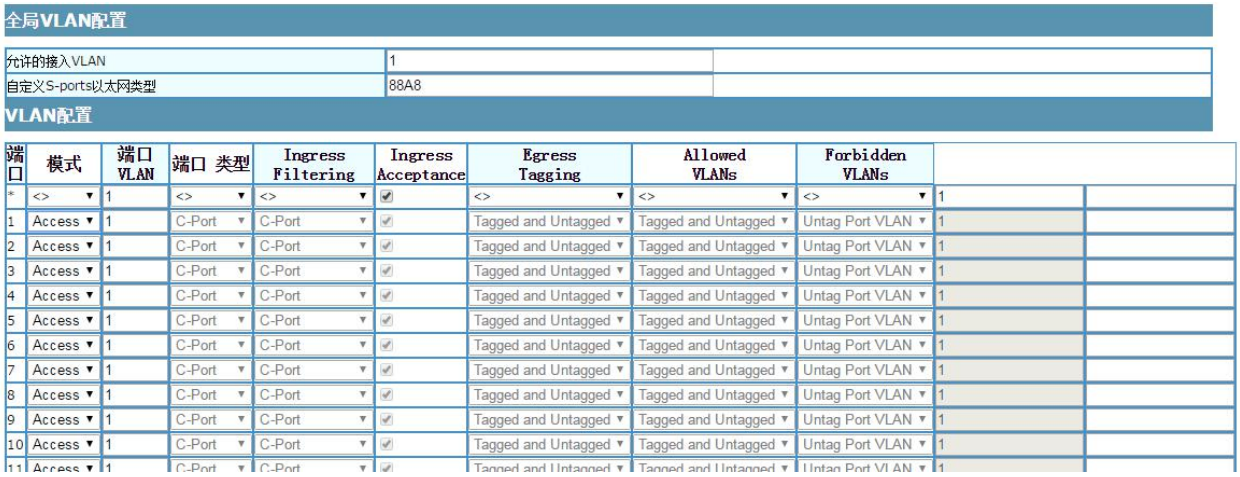
配置项	说明
端口	以下配置所适用的端口号。
模式	控制是否在此端口上启用“限制控制”。这个和全局模式必须设置为 Enabled 才能使限制控制生效。请注意，其他模块仍然可以使用底层端口安全功能，而不在给定端口上启用限制控制。
限制	此端口上可以保护的最大 MAC 地址数。此数字不能超过 1024.如果超出限制，则采取相应的动作； 交换机“承载”具有总数的 MAC 地址，当在启用端口安全的端口

	上看到新的 MAC 地址时，所有端口从该 MAC 地址抽取。由于所有端口都来自同一个池，因此如果其余端口已使用所有可用的 MAC 地址，则可能发生无法授予配置的最大值的情况。
动作	如果达到限制，交换机可以采取以下操作之一： None：在端口上不允许超过限制 MAC 地址，但不采取进一步操作。 Trap：如果在端口上看到 Limit + 1 个 MAC 地址，请发送 SNMP Trap 信息。如果禁用“老化”，则只会发送一个 SNMP Trap，但启用“老化”后，每次超出限制时都会发送新的 SNMP Trap。 Shutdown：如果在端口上看到 Limit + 1 个 MAC 地址，请关闭该端口。这意味着所有安全的 MAC 地址将从端口中删除，并且不会学习新的地址。即使链路物理断开并在端口上重新连接（通过断开电缆），端口仍将保持关闭。有三种方法可以重新打开端口： 1）启动交换机， 2）禁用并重新启用端口或交换机上的限制控制， 3）单击重新打开按钮。 Trap & Shutdown：如果在端口上看到 Limit + 1 个 MAC 地址，则将执行上述的“Trap”和“Shutdown”操作。
状态	此列显示从限制控制的角度观察到的端口的当前状态。状态采用以下四个值之一： Disabled：限制控制在端口上全局禁用或禁用。 Ready：尚未达到限制。这可以显示所有操作。 Limit Reached：表示在此端口上达到限制。只有当 Action 设置为 None 或 Trap 时，才能显示此状态。 Shutdown：表示端口由限制控制模块关闭。只有当 Action 设置为 Shutdown 或 Trap＆Shutdown 时，才能显示此状态。
重新打开	如果端口通过此模块关闭，您可以通过单击此按钮重新打开它，只有在这种情况下才会启用。有关其他方法，请参阅“动作”部分中的“Shutdown”。 请注意，单击重新打开按钮会导致页面被刷新，因此未提交的更改将丢失。

6.3. VLAN

6.3.1. VLAN 设置

此页面允许在交换机上控制 VLAN 配置。该页面分为全局部分和每个端口配置部分。如下图所示：



6.3.1.1. 全局 VLAN 配置

全局 VLAN 配置各项各参数说明如下表所示：

配置项	说明
允许的接入 VLAN	此字段显示允许的接入 VLAN，即它只影响配置为接入端口的端口。 其他模式下的端口是“允许的 VLAN”字段中指定的所有 VLAN 的成员。 缺省情况下，只有 VLAN 1 使能。 可以通过使用列表语法创建更多的 VLAN，其中各个元素由逗号分隔。 范围用分隔下限和上限的破折号指定。 以下示例将创建 VLAN 1，10，11，12，13，200 和 300：1,10-13,200,300。 在分隔符之间允许有空格。
自定义 S 端口的以太网类型	此字段指定用于自定义 S 端口的 ethertype / TPID（以十六进制指定）。 该设置对其端口类型设置为 S-Custom-Port 的所有端口有效。

6.3.1.2. VLAN 配置

VLAN 配置各项各参数说明如下表所示：

配置项	说明
端口	这是此行的逻辑端口号。
模式	端口模式（默认为 Access）确定所对应的端口的基本行为。端口可以是以

	下三种模式之一。 Access： Access 端口通常用于连接到终端。 Voice VLAN 之类的动态功能可以将端口添加更多 VLAN 中。 Access 端口具有以下特性： （1）只有一个 VLAN 成员，即端口 VLAN（也称为 Access VLAN），默认情况下为 1 （2）接受未标记和 C 标记的帧 （3）丢弃未归入 Access VLAN 的所有帧 （4）在出口上，分类到接入 VLAN 的所有帧均未标记传输。其他（动态添加的 VLAN）传输标记 Trunk： Trunk 端口可以同时承载多个 VLAN 的流量，通常用于连接其他交换机。 Trunk 端口具有以下特性： 缺省情况下，Trunk 端口是所有 VLAN 的成员（1-4095） Trunk 端口所属的 VLAN 可能受到允许 VLAN 的使用限制 被转发到端口而不是其成员的 VLAN 的帧将被丢弃 默认情况下，所有帧转发到端口 VLAN（也称为本地 VLAN）的帧在出口上被标记。转发到端口 VLAN 的帧在出口上不会得到 C 标记 所有帧出口标记可以更改，在这种情况下，入口只接受标记的帧 Hybrid： Hybrid 端口在许多方面类似于 Trunk 端口，但增加了额外的端口配置功能。除了 Trunk 端口描述的特性之外，Hybrid 端口还具有以下功能： 可以配置为 VLAN 标记不关注，关注 C 标记，关注 S 标记或关注 S 自定义标记 可以控制入口滤波 帧的入口接受和出口标记的配置可以独立配置
端口 VLAN	确定端口的 VLAN ID（也称为 PVID）。允许的 VLAN 范围为 1 到 4095，默认值为 1。 在入口时，如果端口配置为 VLAN 未知，帧未标记，或端口上启用了关注 VLAN，但帧优先标记（VLAN ID = 0），则帧被转发到端口 VLAN。 在出口，如果出口标记配置设置为 untag 端口 VLAN，则转发到端口 VLAN 的帧不会被标记。 端口 VLAN 对于处于 Access 模式的端口称为“Access VLAN”，对于 Trunk 或 Hybrid 的端口称为本地 VLAN。

端口类型	Hybrid 模式中的端口允许更改端口类型，即帧的 VLAN 标记是否用于将入口上的帧转发到特定 VLAN。如果是，则对那个 TPID 作出反应。同样，在出口，如果需要标记，则端口类型确定标记的 TPID。 不关注： 在入口处，所有帧（无论是否携带 VLAN 标记）都被转发到端口 VLAN，并且可能的标记在出口上不被移除。 C 端口： 在入口处，具有 TPID = 0x8100 的 VLAN 标记的帧被分类到嵌入在标记中的 VLAN ID。如果帧是未标记的或已标记优先级，则该帧将被转发到端口 VLAN。如果帧必须在出口上标记，则它们将被标记为 C 标记。 S 端口： 在入口处，具有 TPID = 0x8100 或 0x88A8 的 VLAN 标记的帧被转发到嵌入在标记中的 VLAN ID。如果帧是未标记的或已标记优先级，则该帧将被分类到端口 VLAN。如果帧必须在出口上标记，则它们将被标记有 S 标记。 S 自定义端口： 在入口处，具有 TPID = 0x8100 或等于为 Custom-S 端口配置的以太网类型的 VLAN 标记的帧将转发到嵌入在该标记中的 VLAN ID。如果帧是未标记的或已标记优先级，则该帧将被分类到端口 VLAN。如果帧必须在出口上标记，则它们将被标记有定制 S 标记。
入口过滤	Hybrid 端口允许更改入口过滤。Access 和 Trunk 端口始终启用入口过滤。 如果启用入口过滤（复选框选中），则会将丢弃转发到端口不是其成员的 VLAN 的帧。 如果禁用入口过滤，则转发到端口不是其成员的 VLAN 的帧，并将其转发到交换机引擎。但是，端口永远不会转发到它不是其成员的 VLAN 的帧。
入口检验	Hybrid 端口允许更改入口处接受的帧类型。 标记和未标记 接受标记帧和未标记帧。 仅标记 在入口只接受标记的帧。丢弃未标记的帧。 仅未标记 入口只接受未标记的帧。标记的帧被丢弃。
出口标记	端口在 Trunk 和 Hybrid 模式可以控制出口上的帧的标记。 Untag 端口 VLAN 转发到端口 VLAN 的帧以无标记的方式传输。其他帧与相关标记一起传输。 全部标记

	所有帧，无论是否转发到端口 VLAN，都使用标记传输。 全部取消标记 所有帧，无论是否转发到端口 VLAN，都是在没有标记的情况下传输的。 此选项仅适用于 Hybrid 模式下的端口。
允许的 VLAN	端口在 Trunk 和 Hybrid 模式可以控制哪些 VLAN 被允许成为成员。Access 端口只能是一个 VLAN 的成员，即 Access VLAN。 该字段的语法与“已启用 VLAN”字段中使用的语法相同。默认情况下，Trunk 或 Hybrid 端口将成为所有 VLAN 的成员，因此设置为 1-4095。 该字段可以留空，这意味着端口不会成为任何 VLAN 的成员。
禁止的 VLAN	端口可以配置为从不是一个或多个 VLAN 的成员。当必须防止动态 VLAN 协议（如 MVRP 和 GVRP）将端口动态添加到 VLAN 时，建议使用此配置。 这功能是将 VLAN 标记为在所对应的端口上被禁止。 语法与“已启用的 VLAN”字段中使用的语法相同。 默认情况下，该字段为空，表示端口可成为所有 VLAN 的成员。

6.3.2. 私有 VLAN 表

本页面可以在此监视和修改交换机的专用 VLAN 成员资格配置，也可以在此页添加或删除私有 VLAN。每个私有 VLAN 的端口成员都可以在此页添加或删除。

Private VLAN 基于源端口掩码，与 VLAN 没有关联。这意味着 VLAN ID 和 Private VLAN ID 可以相同。

端口必须是 VLAN 和 Private VLAN 的成员才能转发数据包。默认情况下，所有端口都是不关注 VLAN，VLAN 1 和 Private VLAN 1 的成员。

VLAN 不关注端口只能是一个 VLAN 的成员，但它可以是多个 Private VLAN 的成员。

私有 VLAN 成员配置各项各参数说明如下表所示：

配置项	说明
删除	要删除 Private VLAN 条目，请选中此框。该条目将在下次保存时被删除。
Private VLAN ID	表示此特定 Private VLAN 的 ID。
端口成员	每个 Private VLAN ID 显示每个端口的一行复选框。要在 Private VLAN 中包括端口，请选中复选框。要从 Private VLAN 中删除或

	排除端口，请确保未选中该框。默认情况下，没有端口是成员，并且所有框都未选中。
添加新的 Private VLAN	单击添加新的 Private VLAN 以添加新的 Private VLAN ID。向表中添加一个空行，并且可以根据需要配置 Private VLAN。Private VLAN ID 的允许范围与交换机端口号范围相同。不接受此范围之外的任何值，并显示警告消息。单击“确定”放弃不正确的条目，或单击“取消”返回编辑并进行更正。当您单击“保存”时，将启用 Private VLAN。删除按钮可用于撤消添加新的 Private VLAN。

6.3.3. VLAN 端口状态

此页面提供 VLAN 端口状态，如下图所示：

Combined users 的VLAN端口状态

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag PVID		No
2	C-Port	☑	All	1	Untag PVID		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag PVID		No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☑	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag PVID		No
10	C-Port	☑	All	1	Untag PVID		No
11	C-Port	☑	All	1	Untag PVID		No
12	C-Port	☑	All	1	Untag PVID		No
13	C-Port	☑	All	1	Untag PVID		No
14	C-Port	☑	All	1	Untag PVID		No
15	C-Port	☑	All	1	Untag PVID		No
16	C-Port	☑	All	1	Untag PVID		No
17	C-Port	☑	All	1	Untag PVID		No
18	C-Port	☑	All	1	Untag PVID		No

VLAN 端口状态界面各项各参数说明如下表所示：

配置项	说明
删除	要删除 Private VLAN 条目，请选中此框。该条目将在下次保存时被删除。
Private VLAN ID	表示此特定 Private VLAN 的 ID。
端口成员	每个 Private VLAN ID 显示每个端口的一行复选框。要在 Private VLAN 中包括端口，请选中复选框。要从 Private VLAN 中删除或排除端口，请确保未选中该框。默认情况下，没有端口是成员，并且所有框都未选中。
添加新的 Private VLAN	单击添加新的 Private VLAN 以添加新的 Private VLAN ID。向表中添加一个空行，并且可以根据需要配置 Private VLAN。Private VLAN ID 的允许范围与交换机端口号范围相同。不接受此范围之外的任何值，并显示警告消息。单击“确定”放弃不正确的条目，

	或单击“取消”返回编辑并进行更正。当您单击“保存”时，将启用 Private VLAN。删除按钮可用于撤消添加新的 Private VLAN。
VLAN 用户	各种内部软件模块可以使用 VLAN 服务来即时配置 VLAN 端口配置。 右侧的下拉列表允许在显示由管理员（Admin）配置的 VLAN 成员身份或由这些内部软件模块之一配置的 VLAN 成员关系之间进行选择。 “Combined”条目将显示管理员和内部软件模块配置的组合，并且基本上反映了在硬件中实际配置的内容。 如果给定的软件模块未覆盖任何端口设置，则表中将显示文本“所选用户没有数据”。
端口	同一行中包含的设置的逻辑端口。
端口类型	显示给定用户想要在端口上配置的端口类型（未知，C 端口，S 端口，S 自定义端口）。 如果选定用户未覆盖，该字段为空。
入口过滤	显示给定用户是否希望启用入口过滤。 如果选定用户未覆盖，该字段为空。
帧类型	显示给定用户想要在端口上配置的可接受的帧类型（全部，Taged，未标记）。 如果选定用户未覆盖，该字段为空。
端口 VLAN ID	显示给定用户希望端口具有的端口 VLAN ID（PVID）。 如果选定用户未覆盖，该字段为空。
Tx 标记	显示给定用户在端口上具有的 Tx 标记要求（Tag All，Tag PVID，Tag UVID，Untag All，Untag PVID，Untag UVID）。 如果选定用户未覆盖，该字段为空。
未标记的 VLAN ID	如果 Tx 标记被所选用户覆盖，并设置为 Tag 或 Untag UVID，则此字段将显示用户想要在出口上标记或取消标记的 VLAN ID。 如果选定用户未覆盖，该字段为空。
冲突	两个用户可能对端口的配置有冲突的要求。 例如，一个用户可能需要所有帧在出口上被标记，而另一个用户可能需要所有帧在出口上被去标记。 由于两个用户都不能赢，这会导致冲突，这是以优先级方式解决的。管理员优先级最低。其他软件模块根据其在下拉列表中的位置进行优先级排序：列表中的值越高，优先级越高。 如果存在冲突，“组合”用户和违规软件模块将显示为“是”。

	“组合”用户反映了硬件中实际配置的内容。

6.3.4. 端口隔离

此页面用于在专用 VLAN 中启用或禁用端口隔离，VLAN 的端口成员可以隔离到同一 VLAN 和 Private VLAN 上的其他隔离端口。如下图所示：

端口隔离 VLAN 配置界面各项各参数说明如下表所示：

配置项	说明
端口成员	为 Private VLAN 的每个端口提供一个复选框。 选中时，将在该端口上启用端口隔离。 取消选中时，将禁用该端口上的端口隔离。 缺省情况下，所有端口的端口隔离功能处于关闭状态。

6.4. VCL

6.4.1. 基于 MAC 的 VLAN

可以在此处配置基于 MAC 的 VLAN。此页面允许添加和删除基于 MAC 的 VLAN，并将分配给不同的端口。此页面仅显示静态 VLAN。

基于 MAC 的 VLAN 配置界面各项各参数说明如下表所示：

配置项	说明
删除	要删除基于 MAC 的 VLAN，请选中此框，然后按保存。
MAC 地址	表示 MAC 地址。
VLAN ID	表示 VLAN ID。
端口成员	每个基于 MAC 的 VLAN 显示每个端口的一行复选框。要在基于 MAC 的 VLAN 中包含对应端口，请选中该框。要从基于 MAC 的

	VLAN 中删除或排除端口，请确保未选中该框。默认情况下没有端口是其成员，并且所有框都未选中。
添加新的基于 MAC 的 VLAN	单击添加条目以添加新的基于 MAC 的 VLAN。表中将添加一个空行，并且可以根据需要配置基于 MAC 的 VLAN。可以为基于 MAC 的 VLAN 条目配置任何单播 MAC 地址。

注意：

不允许广播或多播 MAC 地址。

VLAN ID 的合法值为 1 到 4095。

单击“保存”时，将启用基于 MAC 的 VLAN。单击“保存”时，将删除没有任何端口成员的基于 MAC 的 VLAN。

删除按钮可用于撤消添加新的基于 MAC 的 VLAN。基于 MAC 的 VLAN 最大数量限制为 256。

6.4.2. 基于协议的 VLAN

6.4.2.1. 协议到组的映射

此页面允许添加新协议到组名（每个组的唯一）的映射，以及允许您查看和删除交换机已映射的条目。

协议到组配置界面各项各参数说明如下表所示：

配置项	说明
删除	要删除“组名称”映射条目的协议，请选中此框。在下一次保存期间，该条目将在交换机上被删除。
帧类型	帧类型可以具有以下值之一： 1) 以太网 2) LLC 3) SNAP 注意：在更改帧类型字段时，以下文本字段的有效值将根据您选择的新帧类型而有所不同。
值	可以在此文本字段中输入的有效值，取决于从前面的帧类型选择菜单中选择的选项。以下是三种不同框架类型的标准：

	1) 对于以太网：当选择以太网作为帧类型时，文本字段中的值称为 etype。 etype 的有效值范围为 0x0600-0xffff 2) 对于 LLC：在这种情况下，有效值由两个不同的子值 DSAP 和 SSAP 组成。 DSAP：1 字节长字符串（0x00-0xff） SSAP：1 字节长字符串（0x00-0xff） 3) 对于 SNAP：在这种情况下，有效值也由两个不同的子值 OUI 和 PID 组成。 4) OUI：OUI（Organizationally Unique Identifier）是 xx-xx-xx 格式的值，其中字符串中的每对（xx）是十六进制值，范围从 0x00-0xff。 5) PID：如果 OUI 是十六进制 000000，协议 ID 是在 SNAP 顶部运行的协议的以太网类型（EtherType）字段值；如果 OUI 是用于特定组织的 OUI，则协议 ID 是由该组织分配给在 SNAP 之上运行的协议的值。 换句话说，如果 OUI 字段的值是 00-00-00，则 PID 的值将是 etype（0x0600-0xffff），并且如果 OUI 的值不是 00-00-00，则 PID 的有效值将是来自 0x0000 至 0xffff。
组名	对于由字母（a-z 或 A-Z）和整数（0-9）的组合组成的每个条目，有效的组名称是唯一的 16 个字符的长字符串。 **注意：不允许使用特殊字符和下划线（_）。**
添加新组到 VLAN 映射表项	单击添加新条目以在映射表中添加新条目。将一个空行添加到表中; 帧类型，值和组名称可根据需要进行配置。删除按钮可用于撤消添加新条目。协议到组映射最大数量限制为 128。

6.4.2.2. 组到 VLAN 的映射

此页面允许您将已配置的组名称映射到交换机的 VLAN。

基于组到 VLAN 配置界面各项各参数说明如下表所示：

配置项	说明
删除	要删除组名称到 VLAN 映射条目，请选中此框。在下一次保存期间，该条目将在交换机上被删除。
组名	有效的组名称是最多 16 个字符的字符串，由字母（a-z 或 A-Z）和

	整数（0-9）的组合组成，不允许使用特殊字符。无论您尝试映射到 VLAN 的组名称必须存在于协议到组映射表中，并且不能由此页上的任何其他现有映射条目预先使用。
VLAN ID	指示组名称将映射到的 ID。有效的 VLAN ID 范围为 1-4095。
端口成员	每个组名称到 VLAN ID 映射显示每个端口的一行复选框。要在映射中包括端口，请选中该框。要从映射中删除或排除端口，请确保未选中该框。默认情况下没有端口是其成员，并且所有框都未选中。
添加新组到 VLAN 映射表项	单击添加新条目以在映射表中添加新条目。向表中添加空行，可以根据需要配置组名，VLAN ID 和端口成员。 VLAN ID 的合法值为 1 到 4095。删除按钮可用于撤消添加新条目。最大可能的组到 VLAN 映射被限制为 64。

6.4.3. 基于 IP 的 VLAN

可以在此处配置基于 IP 子网的 VLAN 条目。此页面允许添加，更新和删除基于 IP 子网的 VLAN 条目，并将条目分配给不同的端口。此页面仅显示静态条目。

基于 IP 的 VLAN 配置界面各项各参数说明如下表所示：

配置项	说明
删除	要删除基于 IP 子网的 VLAN 条目，请选中此框，然后按保存。
VCE ID	表示条目的索引。它是用户可配置的。它的取值范围是 0-128。如果 VCE ID 为 0，应用程序将自动生成该条目的 VCE ID。基于 IP 子网的 VLAN 的删除和查找基于 VCE ID。
IP 地址	表示 IP 地址。
掩码长度	表示网络掩码长度。
VLAN ID	表示 VLAN ID。可以为现有条目更改 VLAN ID。
端口成员	每个基于 IP 子网的 VLAN 条目显示每个端口的一行复选框。要在基于 IP 子网的 VLAN 中包括端口，请选中此框。要从基于 IP 子网的 VLAN 中删除或排除端口，请确保未选中该框。默认情况下没有端口是其成员，并且所有框都未选中。
添加新的基于 IP 子网	单击添加新条目以添加新的基于 IP 子网的 VLAN 条目。将向表中

的 VLAN	添加一个空行，并且可以根据需要配置基于 IP 子网的 VLAN 条目。可以为基于IP子网的VLAN条目配置任何IP地址/掩码。VLAN ID 的合法值为 1 到 4095。当您点击“保存”时，启用基于 IP 子网的 VLAN 条目。删除按钮可用于撤消添加新的基于 IP 子网的 VLAN。基于 IP 子网的最大 VLAN 条目数限制为 128。

6.5. ERPS 配置

6.5.1. EPS

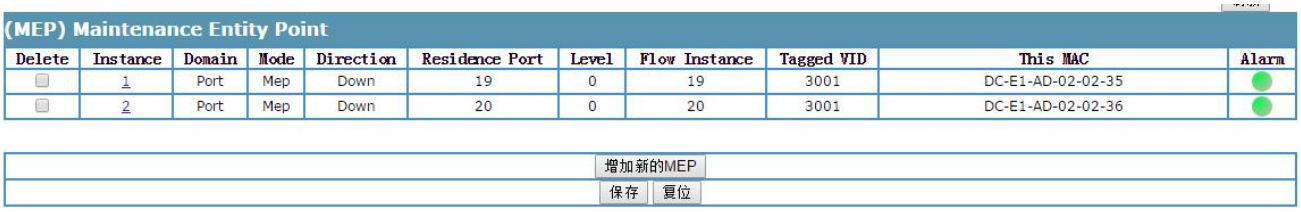
此页配置以太网（线性）保护交换机实例。如下图所示

EPS 配置界面各项各参数说明如下表所示：

配置项	说明
删除	此框用于在下次保存操作中标记要删除的 EPS。
EPS ID	EPS 的 ID。 单击 EPS 的 ID 进入配置页面。
域	端口：这将在端口域中创建 EPS。 'W / P 流量'是端口。 Evc：这将在 EVC 域中创建一个 EPS。 'W / P 流'是 EVC
Architecture	1+1：这将创建 1 + 1 EPS。 1:1：这将创建 1：1 的 EPS。
W 流	EPS 的工作流。
P 流	EPS 的保护流。
W SF MEP	工作信号失效报告 MEP。
P SF MEP	保护信号失效报告 MEP。
APS MEP	APS PDU 处理 MEP。
报警	表明 EPS 上有一个告警。

6.5.2. MEP

此处配置 MEP 实例。



MEP 配置界面各项各参数说明如下表所示：

配置项	说明
删除	此框用于在下一个保存操作中标记要删除的 MEP。
实例	MEP 的 ID。单击 MEP 的 ID 进入配置页面。
域	端口：这是端口域中的 MEP。 “流实例”是一个端口。 Evc：这是 EVC 域中的 MEP。 “流实例”是 EVC。必须创建 EVC VLAN：这是 VLAN 域中的 MEP。 “流实例”是一个 VLAN。必须创建 VLAN
模式	MEP：这是维护实体端点。 MIP：这是维护实体中间点。
方向	Down：这是一个 Down MEP - 监视入口 OAM 和“Residence Port”上的流量。 Up：这是一个 Up MEP - 监视出口 OAM 和“Residence Port”的流量。
Residence Port	MEP 正在监视的端口。对于 EVC MEP，端口必须是 EVC 中的端口。对于 VLAN MEP，端口必须是 VLAN 成员。
Level	本 MEP 的 MEG 级别。
流实例	MEP 与此流程相关。
标记的 VID	外部 C / S 标记（取决于 VLAN 端口类型）与此 VID 一起添加。输入“0”表示不添加 TAG。
MAC	此 MEP 的 MAC - 可以由其他 MEP 在选择单播时使用（仅信息）。
告警	表明 MEP 上有一个告警。

6.5.3. ERPS 配置

此处配置以太网环保护交换机实例。

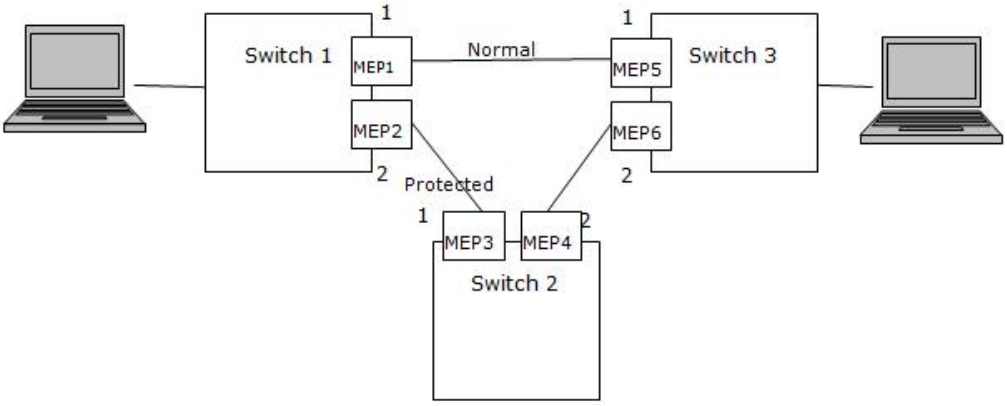
ERPS 配置界面各项各参数说明如下表所示：

配置项	说明

删除	此框用于在下一个保存操作中标记要删除的 ERPS。
保护组 ID	创建的保护组的 ID。单击保护组的 ID 进入配置页面。
端口 0	这将在环中创建交换机的端口 0。
端口 1	这将在环中创建交换机的“端口 1”。由于互连子环将仅具有一个环端口，因此对于互连子环，“端口 1”被配置为“0”。此字段中的“0”表示没有“端口 1”与此实例相关联
端口 0 SF MEP	端口 0 信号失败报告 MEP。
端口 1 SF MEP	端口 1 信号失败报告 MEP。由于只有一个 SF MEP 与没有虚拟通道的互连子环相关联，因此对于这种环实例将其配置为“0”。此字段中的“0”表示没有端口 1 SF MEP 与此实例相关联。
端口 0 APS MEP	端口 0 APS PDU 处理 MEP。
端口 1 APS MEP	端口 1 APS PDU 处理 MEP。由于只有一个 APS MEP 与没有虚拟信道的互连子环相关联，因此对于这样的环实例将其配置为“0”。此字段中的“0”表示没有端口 1 APS MEP 与此实例相关联。
环类型	保护环类型。它可以是主环或子环。
互连节点	互连节点指示环实例互连。单击复选框以配置此。 “是”表示它是此实例的互连节点。 “否”表示已配置的实例未互连。
虚拟频道	子环可以在互连节点上具有虚拟通道或不具有虚拟通道。这是使用“虚拟频道”复选框配置的。 “是”表示其为具有虚拟通道的子环。“否”表示子环没有虚拟通道。
主要环 ID	互联子环的主环组 ID。它用于在主环上发送拓扑更改更新。如果环是主要的，此值与此环的保护组 ID 相同。
报警	ERPS 上有一个活动报警。

6.5.4. ERPS 配置举例

本例子中使用三个交换机的网络，网络拓扑图如下图：



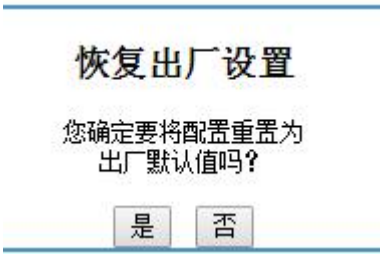
6.5.4.1. 初始化交换机配置

要通过 Web 配置 ERPS 功能，请按照下面列出的步骤操作。

注意：三台交换机都要进行以下操作！

将交换机 1 连接到交换机 2，将交换机 1 连接到交换机 3。不要连接交换机 2 和交换机 3 以避免网络风暴。 PC 连接到交换机 1,并登陆交换机 1，交换机 2 和交换机 3 的 Web 界面；

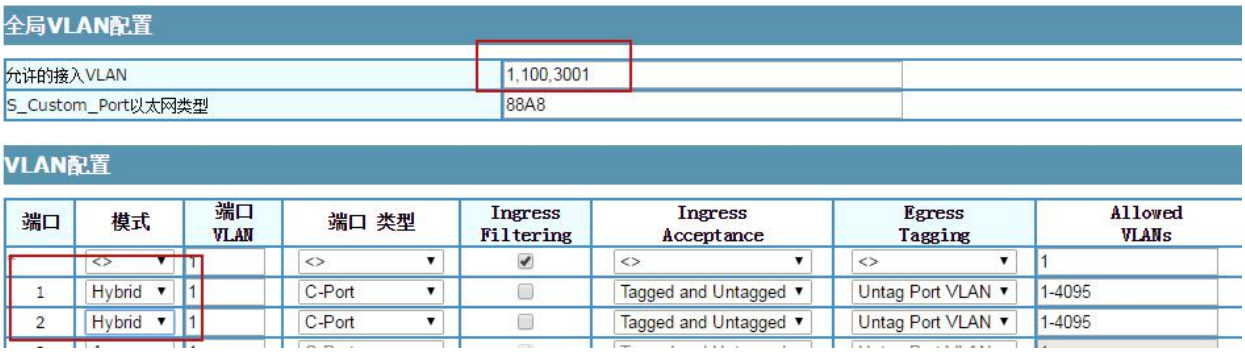
1. 将三台交换机恢复出厂设置。在导航栏中点击“系统工具”->“出厂设置”，如下图所示；



2. 将三台交换机配置在同一个网段。例如将交换机 1 的 IP 地址配置为 192.168.1.201，交换机 2 为 192.168.1.202，交换机 3 为 192.168.1.203；

3. 为了避免与 ERPS 冲突，禁用所有交换机上的 STP 和 LLDP（默认已启动）。在导航栏中点击“设备控制”->“STP”->“STP CIST 端口配置”和“设备控制”->“LLDP”->“LLDP 配置”，按下图配置并点击保存按钮；

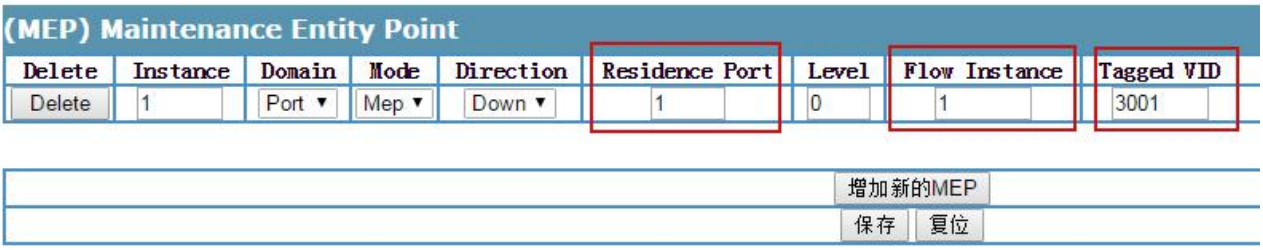
4. 创建控制 VLAN 和保护 VLAN 并将环网端口设置为 Hybrid。 本例子中控制 VLAN 设置为 3001，数据 VLAN 为 1 和 100，参与环网的端口为端口 1 和端口 2。在导航栏中点击“设备控制”->“VLAN”->“VLAN 配置”，并按照下图配置并点击保存按钮；



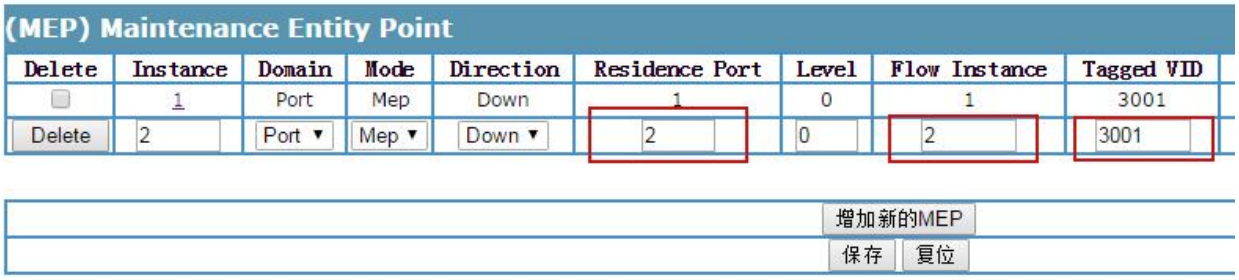
6.5.4.2. 在交换机 1 上创建 MEP

在导航栏中点击“设备控制”->“ERPS”->“MEP”，然后按照下面列出的步骤操作。

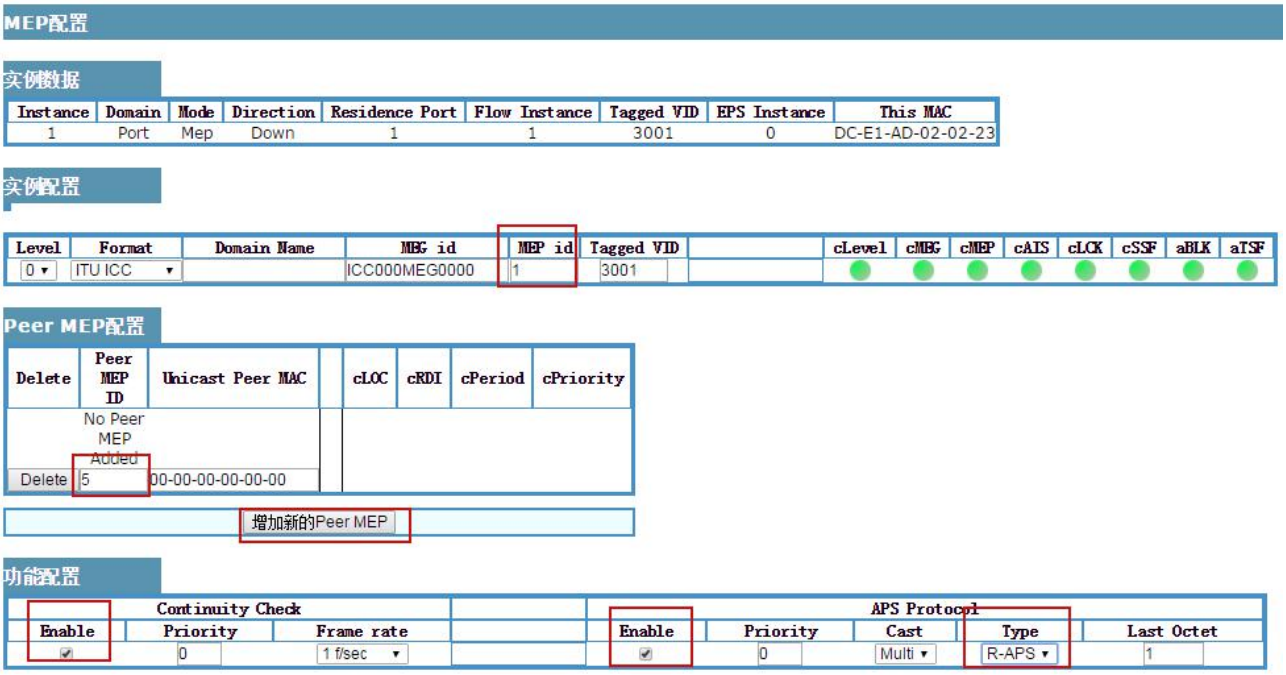
1.在端口 1 上添加一个新的 MEP，点击“增加新的 MEP”按钮并按照下图配置并点击保存按钮，Residence Port 和 Flow Instance 中填端口号，即 1；



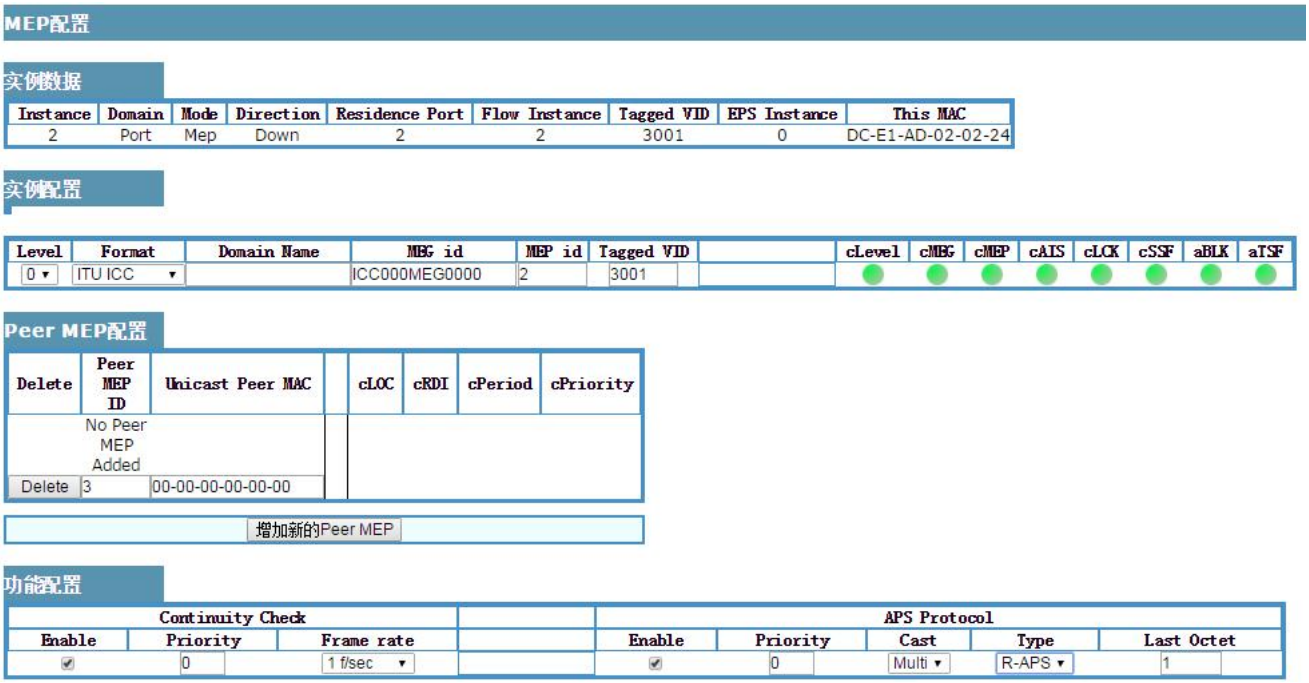
2.在端口 2 上添加一个新的 MEP，Residence Port 和 Flow Instance 中填端口号，即 2；



3.编辑 MEP1。点击“1”进入 MEP 配置界面并按照下图配置并点击保存按钮；



4.编辑 MEP2。点击“2”进入 MEP 配置界面并按照下图配置并点击保存按钮；



6.5.4.3. 在交换机 2 上创建 MEP

在导航栏中点击“设备控制”->“ERPS”->“MEP”，然后按照下面列出的步骤操作。

1.在端口 1 上添加一个新的 MEP，点击“增加新的 MEP”按钮并按照下图配置并点击保存按钮；

(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID
Delete	1	Port	Mep	Down	1	0	1	3001

增加新的MEP

保存 复位

2.在端口 2 上添加一个新的 MEP；

(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID
	1	Port	Mep	Down	1	0	1	3001
Delete	2	Port	Mep	Down	2	0	2	3001

增加新的MEP

保存 复位

3.编辑 MEP1。点击“1”进入 MEP 配置界面并按照下图配置并点击保存按钮；

MEP配置

实例数据

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
1	Port	Mep	Down	1	1	3001	0	DC-E1-AD-01-00-FF

实例配置

Level	Format	Domain Name	MEG id	MEP id	Tagged VID		cLevel	cMEG	cMEP	cAIS	cLCK
0	ITU ICC		ICC000MEG0000	3	3001						

Peer MEP配置

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	2	00-00-00-00-00-00					

增加新的Peer MEP

功能配置

Continuity Check				APS Protocol				
Enable	Priority	Frame rate		Enable	Priority	Cast	Type	Last Octet
	0	1 f/sec			0	Multi	R-APS	1

4.编辑 MEP2。点击“2”进入 MEP 配置界面并按照下图配置并点击保存按钮；

MEP配置

实例数据

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
2	Port	Mep	Down	2	2	3001	0	DC-E1-AD-01-01-00

实例配置

Level	Format	Domain Name	MEG id	MEP id	Tagged VID		cLevel	cMEG	cMEP	cAIS	cLCK
0	ITU ICC		ICC000MEG0000	4	3001						

Peer MEP配置

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	6	00-00-00-00-00-00					

增加新的Peer MEP

功能配置

Continuity Check				APS Protocol				
Enable	Priority	Frame rate		Enable	Priority	Cast	Type	Last Octet
	0	1 f/sec			0	Multi	R-APS	1

6.5.4.4. 在交换机 3 上创建 MEP

在导航栏中点击“设备控制”->“ERPS”->“MEP”，然后按照下面列出的步骤操作。

1.在端口 1 上添加一个新的 MEP，点击“增加新的 MEP”按钮并按照下图配置并点击保存按钮；

(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID
Delete	1	Port	Mep	Down	1	0	1	3001

增加新的MEP

保存 复位

2.在端口 2 上添加一个新的 MEP；

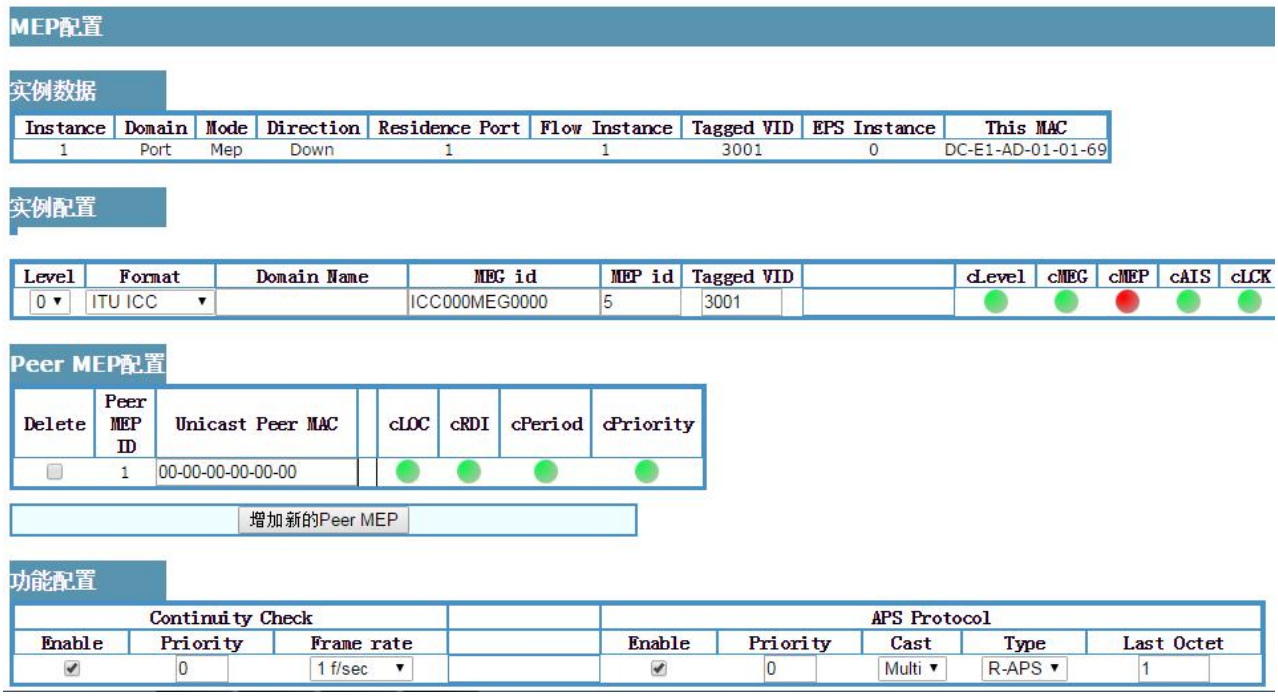
(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID
	1	Port	Mep	Down	1	0	1	3001
Delete	2	Port	Mep	Down	2	0	2	3001

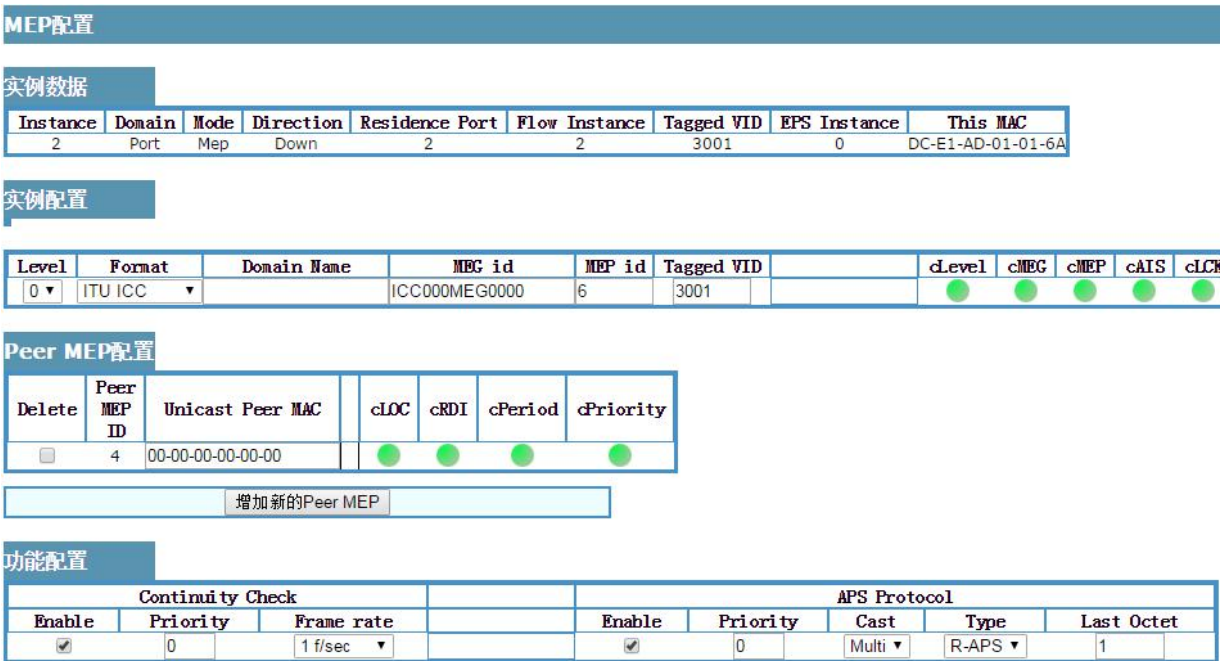
增加新的MEP

保存 复位

3.编辑 MEP1。点击“1”进入 MEP 配置界面并按照下图配置并点击保存按钮；



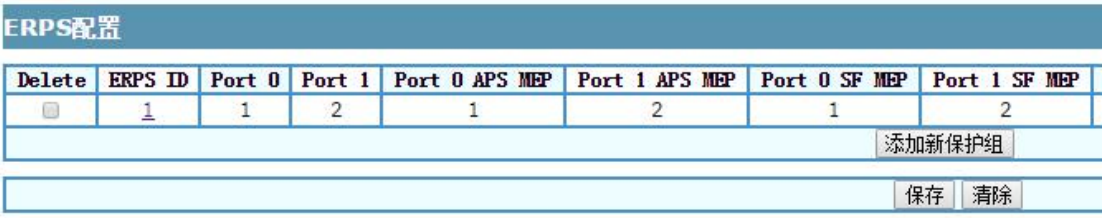
4.编辑 MEP2。点击“2”进入 MEP 配置界面并按照下图配置并点击保存按钮；



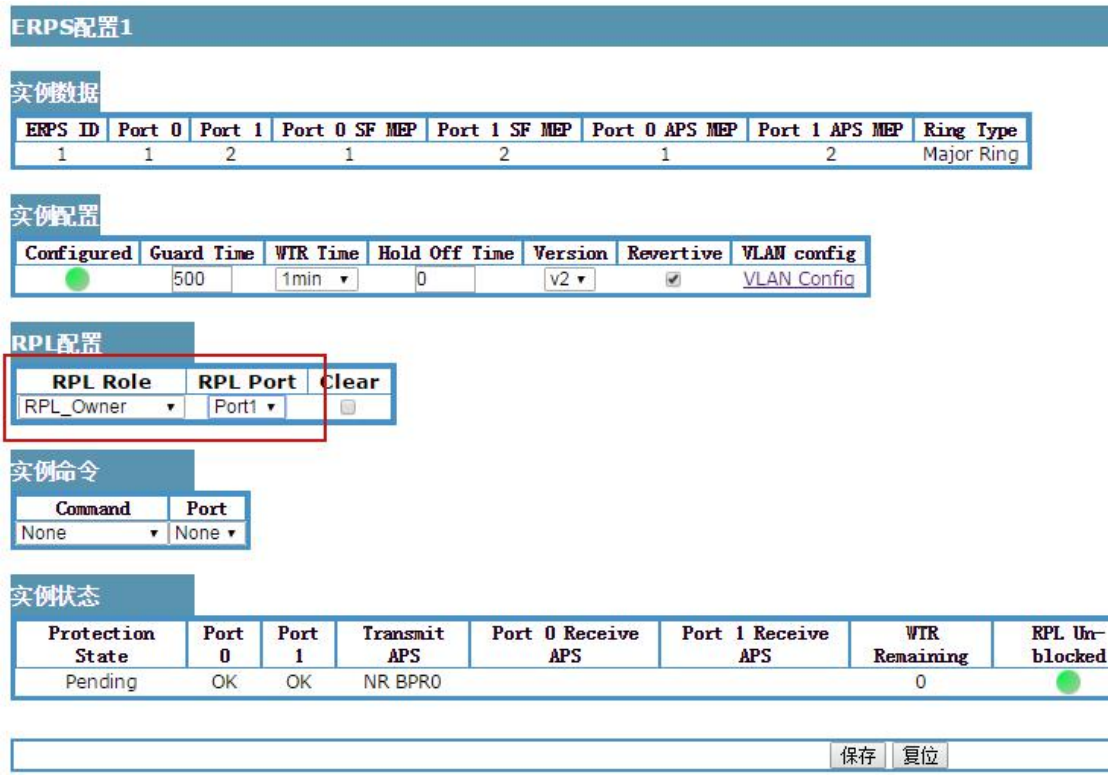
6.5.4.5. 在交换机 1 上创建 ERPS，RPL Owner

在导航栏中点击“设备控制”->“ERPS”->“ERPS”，然后按照下面列出的步骤操作。

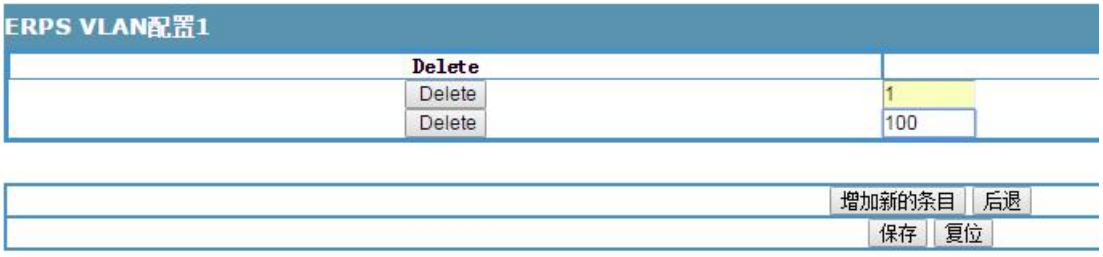
创建 ERPS。点击“添加新保护组”，并按照下图配置并点击保存按钮，其中 Port0 填端口 1，Port2 填端口 2，Port 0 APS MEP 和 Port 0 SF MEP 填写（MEP）1， Port 1 APS MEP 和 Port 1 SF MEP 填写 （MEP）2；



1. 编辑 ERPS。点击“1”进入 ERPS 配置 1 界面并按照下图配置并点击保存按钮；



2. 编辑保护 VLAN。在当前页面，即 ERPS 配置 1 界面，点击“VLAN Config”进入 ERPS VLAN 配置 1 界面。点击“增加新的条目”按钮并按照下图配置并点击保存按钮；



3. 连接交换机 2 和交换机 3。这是因为 RPL 已经断开连接，所以在交换机 2 和交换机 3 连接之前，已经无法通过交换机 1 访问交换机 2。

4. 连接交换机 2 和交换机 3 后，检查各个交换机的 MEP 表格，所有告警灯都应该显示为绿色，如下图所示。

交换机 1

(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
	1	Port	Mep	Down	1	0	1	3001	DC-E1-AD-02-02-23	
	2	Port	Mep	Down	2	0	2	3001	DC-E1-AD-02-02-24	

增加新的MEP
保存 复位

交换机 2

(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
	1	Port	Mep	Down	1	0	1	3001	DC-E1-AD-01-00-FF	
	2	Port	Mep	Down	2	0	2	3001	DC-E1-AD-01-01-00	

增加新的MEP
保存 复位

交换机 3

(MEP) Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
	1	Port	Mep	Down	1	0	1	3001	DC-E1-AD-01-01-69	
	2	Port	Mep	Down	2	0	2	3001	DC-E1-AD-01-01-6A	

增加新的MEP
保存 复位

6.5.4.6. 在交换机 2 上创建 ERPS，RPL Neighbor

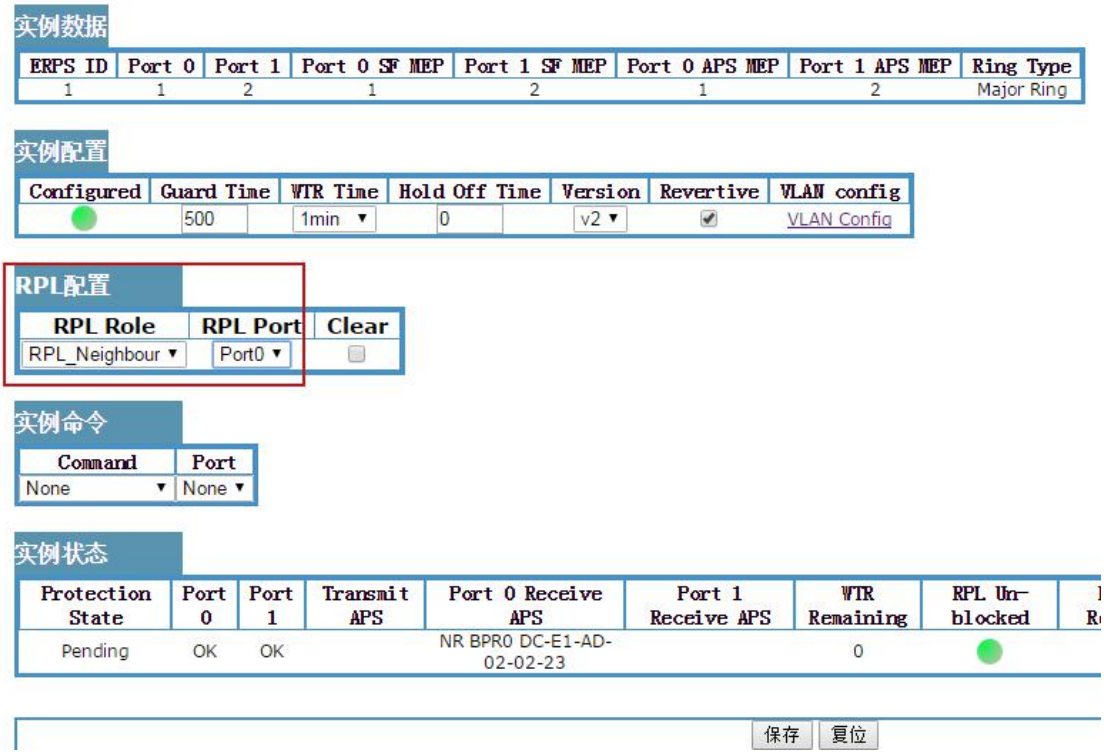
在导航栏中点击“设备控制”->“ERPS”->“ERPS”，然后按照下面列出的步骤操作。创建 ERPS。点击“添加新保护组”，并按照下图配置并点击保存按钮；

ERPS配置

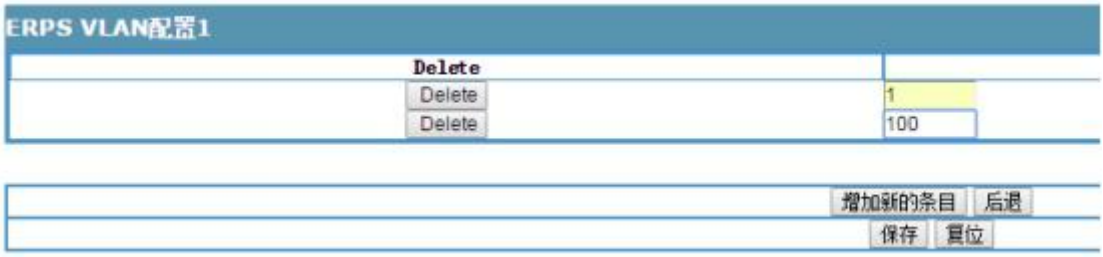
Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP
	1	1	2	1	2	1	2

添加新保护组
保存 清除

1.编辑 ERPS。点击“1”进入 ERPS 配置 1 界面并按照下图配置并点击保存按钮；

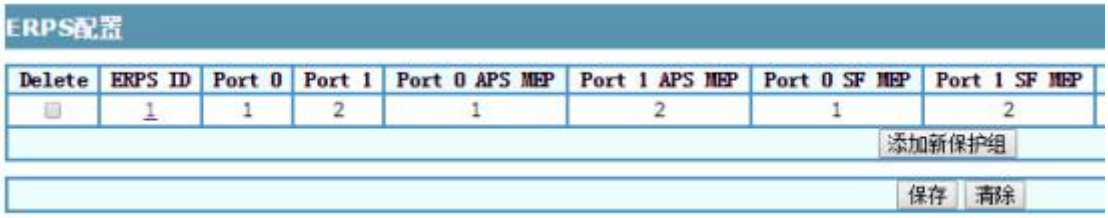


2.编辑保护 VLAN。在当前页面，即 ERPS 配置 1 界面，点击“VLAN Config”进入 ERPS VLAN 配置 1 界面。点击“增加新的条目”按钮并按照下图配置并点击保存按钮；

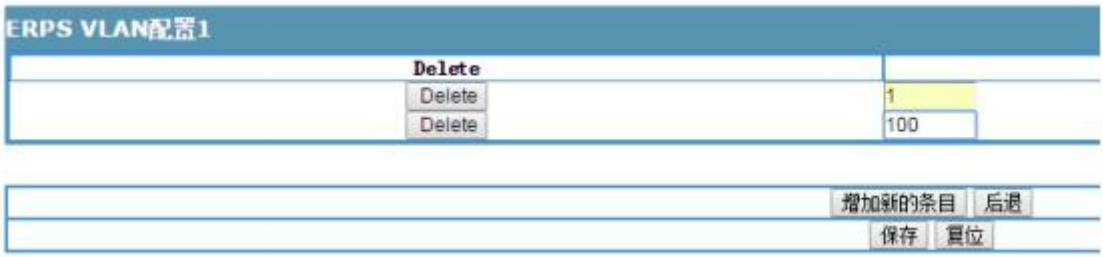


6.5.4.7. 在交换机 3 上创建 ERPS

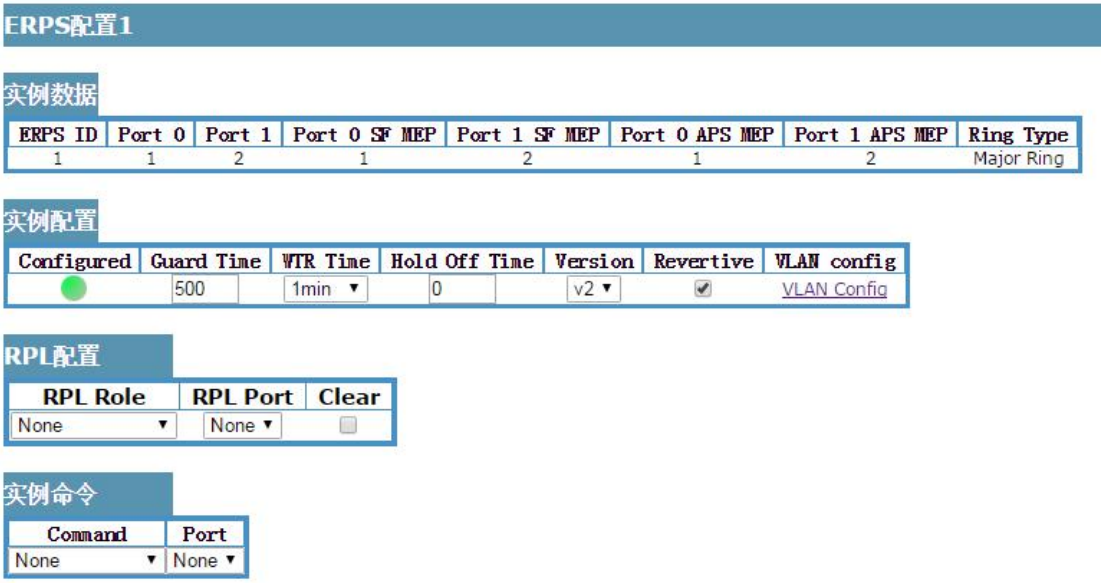
在导航栏中点击“设备控制”->“ERPS”->“ERPS”，然后按照下面列出的步骤操作。创建 ERPS。点击“添加新保护组”，并按照下图配置并点击保存按钮；



1. 编辑保护 VLAN。点击“1”进入 ERPS 配置 1 界面，点击“VLAN Config”进入 ERPS VLAN 配置 1 界面，点击“增加新的条目”按钮并按照下图配置并点击保存按钮；

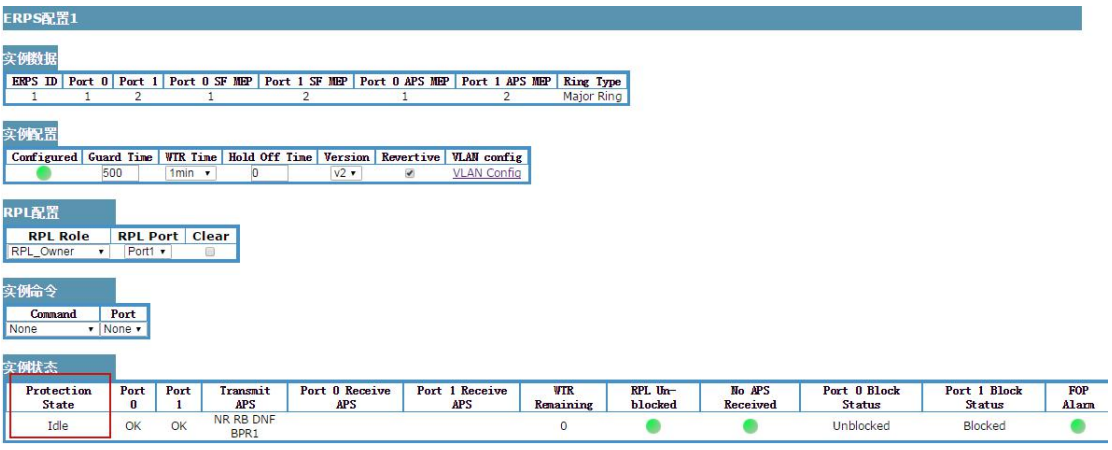


2. 点击后退后在 ERPS 配置 1 界面直接点击保存，此页面不需要配置。

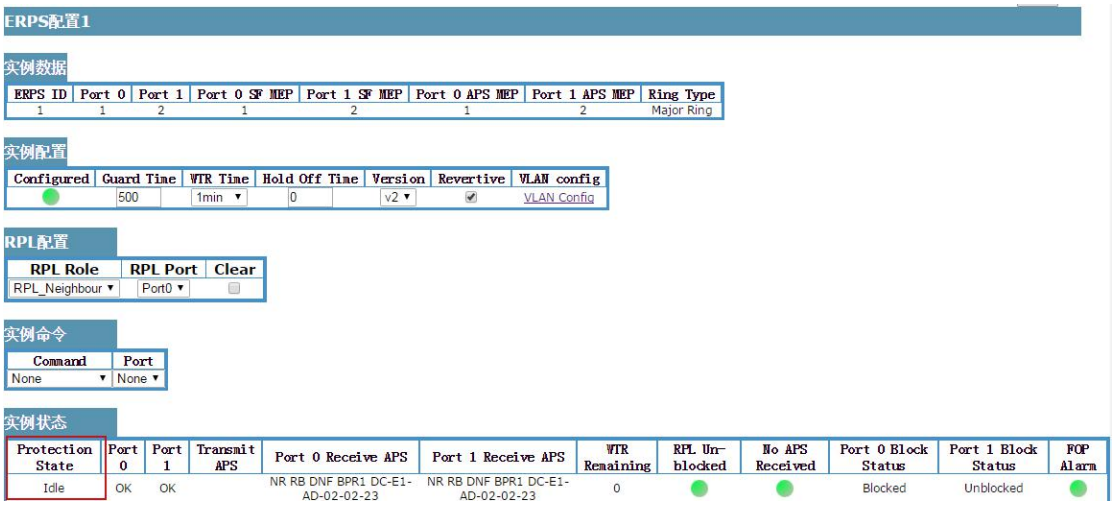


3. 点击保存后 ERPS 配置已完成，各个交换机应如下图显示，Protection State 为 Idle，告警灯绿色。

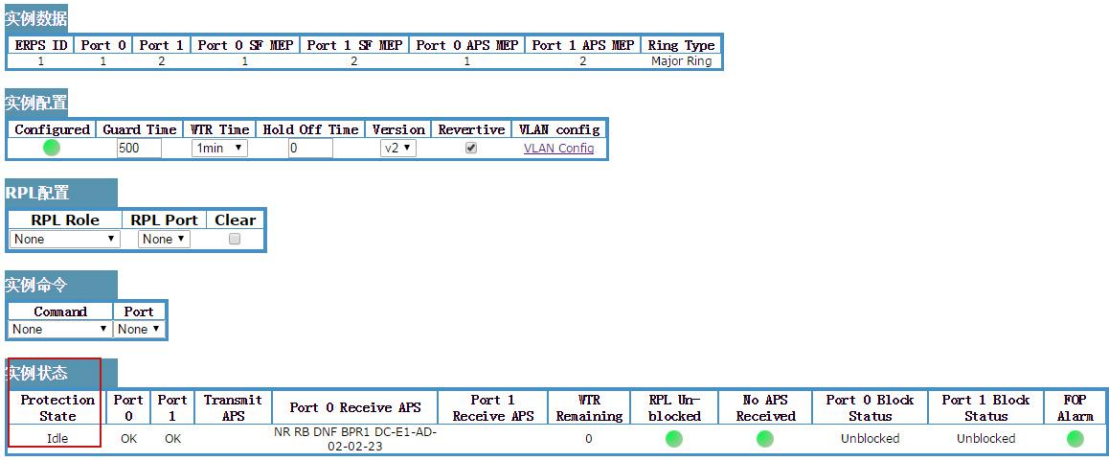
（1）交换机 1



（2）交换机 2



（3）交换机 3

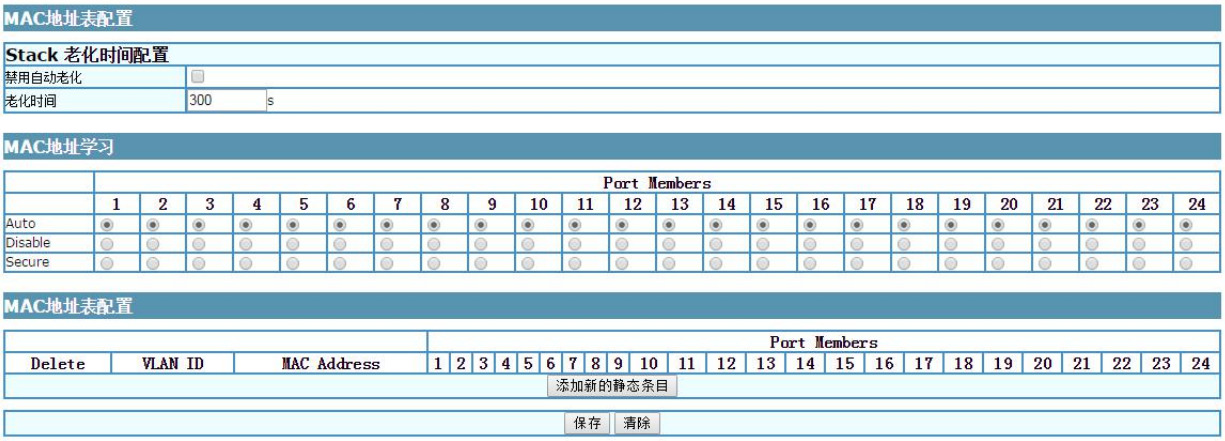


4. 断开交换机 1 和交换机 3 的连接，Protection State 显示为 Protected；然后重新连接交换机 1 和交换机 3，约 70 秒后 Protection State 仍为 Idle。表明 ERPS 已经配置成功。

6.6. MAC

6.6.1. MAC 地址表设置

在此页面上配置 MAC 地址表。在动态 MAC 表中设置条目的超时，并在此处配置静态 MAC 表。



MAC 地址表配置各项各参数说明如下表所示：

配置项	说明
老化时间	缺省情况下，动态表项在 300 秒后从 MAC 表中删除。 通过在此处输入值以秒为单位来配置老化时间。 允许的范围是 10 到 1000000 秒。 通过选中禁用自动老化来禁用动态条目的自动老化。
MAC 表学习	如果给定端口的学习模式是灰色的，则另一个模块控制该模式，使得它不能被用户改变，比如是在 802.1X 下的基于 MAC 的认证模块。 每个端口可以根据以下设置进行学习： Auto：一旦接收到具有未知 SMAC 的帧，就自动进行学习。 禁用：没有学习。 Secure：只有静态 MAC 条目被学习，所有其他帧被丢弃。 注意：确保用于管理交换机的链路在更改为安全学习模式之前添加到静态 Mac 表中，否则管理链路将丢失，并且只能通过使用另一个非安全端口或连接到交换机来恢复通过串行接口。
静态 MAC 表配置	MAC 表中的静态条目在此表中显示。静态 MAC 表可以包含 64 个条目。 MAC 表首先按 VLAN ID 排序，然后按 MAC 地址排序。
删除	选中以删除条目。它将在下次保存时被删除。
VLAN ID	条目的 VLAN ID。
MAC 地址	条目的 MAC 地址。
端口成员	复选标记指示哪些端口是条目的成员。根据需要选中或取消选中以修改条目。
添加新的静态条目	单击添加新静态条目以向静态 MAC 表添加新条目。指定新条目的

	VLAN ID，MAC 地址和端口成员。点击“保存”。

6.6.2. MAC 地址表

MAC 表中的条目显示在此页面上。 MAC 表包含最多 8192 个条目，并且首先按 VLAN ID 排序，然后按 MAC 地址排序。

MAC 地址表配置各项各参数说明如下表所示：

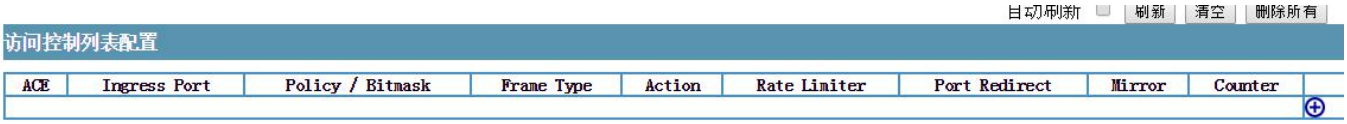
配置项	说明
导航 MAC 表	每个页面最多显示来自 MAC 表的 999 个条目，默认值为 20，通过“每页条目”输入字段选择。当首次访问时，网页将显示从 MAC 表的开始的前 20 个条目。第一个显示将是在 MAC 表中找到的具有最低 VLAN ID 和最低 MAC 地址的那个。 “从 MAC 地址开始”和“VLAN”输入字段允许用户选择 MAC 表中的起始点。单击刷新按钮将更新显示的表或从最接近的下一个 MAC 表匹配。此外，两个输入字段将在刷新按钮单击时采用第一个显示条目的值，从而允许使用相同的起始地址进行连续刷新。 >>将使用当前显示的 VLAN / MAC 地址对的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。
类型	表明 MAC 地址是静态的还是动态的。
MAC 地址	条目的 MAC 地址。
VLAN	条目的 VLAN ID。
端口成员	作为条目成员的端口。

6.7. ACL

6.7.1. ACL 配置

此页面显示访问控制列表（ACL），该 ACL 由此交换机上定义的 ACE 组成。每行描述定义的 ACE。每个交换机的最大 ACE 数为 256。

单击最右边的加号将新 ACE 添加到列表中。用于内部协议的保留 ACE 不能编辑或删除，无法更改顺序序列，且优先级最高。



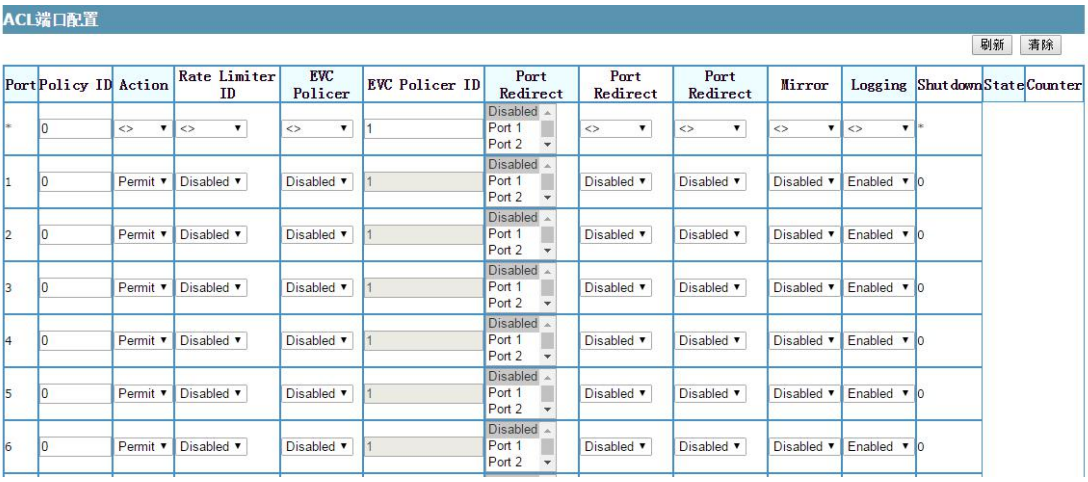
访问控制列表配置各项各参数说明如下表所示：

配置项	说明
ACE	表示 ACE ID。
入口端口	表示 ACE 的入端口。 全部：ACE 将匹配所有入口端口。 端口：ACE 将匹配特定的入口端口。
策略/位掩码	指示 ACE 的策略编号和位掩码。
框架类型	表示 ACE 的帧类型。 任意：ACE 将匹配任何帧类型。 EType：ACE 将匹配以太网类型帧。请注意，基于以太网类型的 ACE 将不会通过 IP 和 ARP 帧匹配。 ARP：ACE 将匹配 ARP / RARP 帧。 IPv4：ACE 将匹配所有 IPv4 帧。 IPv4 / ICMP：ACE 将使 IPv4 帧与 ICMP 协议匹配。 IPv4 / UDP：ACE 将使 IPv4 帧与 UDP 协议匹配。 IPv4 / TCP：ACE 将使 IPv4 帧与 TCP 协议匹配。 IPv4 /其他：ACE 将匹配 IPv4 帧，这不是 ICMP / UDP / TCP。 IPv6：ACE 将匹配所有 IPv6 标准帧。
动作	表示 ACE 的转发动作。 许可：可以转发和学习与 ACE 匹配的帧。 拒绝：匹配 ACE 的帧被丢弃。 过滤器：过滤与 ACE 匹配的帧。
速率限制器	表示 ACE 的速率限制器编号。允许的范围是 1 到 16。当显示 Disabled 时，禁止速率限制器操作。

端口重定向	表示 ACE 的端口重定向操作。与 ACE 匹配的帧将重定向到端口号。允许的值为 Disabled 或特定端口号。当显示“禁用”时，禁用端口重定向操作。 镜像：指定此端口的镜像操作。与 ACE 匹配的帧将镜像到目标镜像端口。 启用：端口上接收的帧被镜像。 禁用：端口上接收的帧未镜像。 默认值为“Disabled”。
计数器	计数器指示 ACE 被帧击中的次数。
修改按钮	您可以使用以下按钮修改表中的每个 ACE（访问控制条目）： 添加：在当前行之前插入新的 ACE。 编辑：编辑 ACE 行。 向上：将 ACE 向上移动列表。 向下：将 ACE 向下移动列表。 删除：删除 ACE。 添加：最低加号在 ACE 列表底部添加一个新条目。

6.7.2. ACL 端口配置

配置每个交换机端口的 ACL 参数（ACL 参数，即 ACE）。这些参数将影响端口上接收的帧，除非该帧与特定的 ACE 匹配。



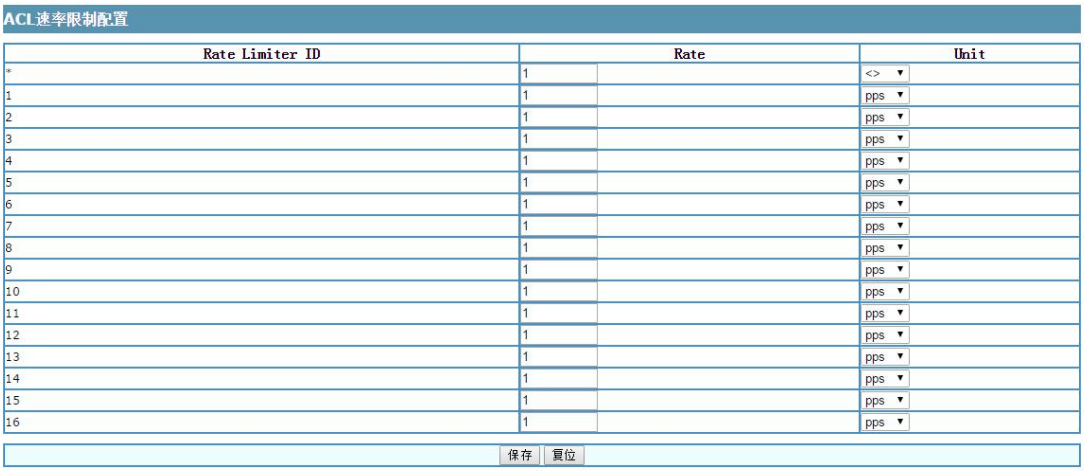
ACL 端口配置各项各参数说明如下表所示：

配置项	说明
端口	同一行中包含的设置的逻辑端口。
策略 ID	选择要应用于此端口的策略。允许的值为 0 到 255。默认值为 0。
行为	选择是允许转发（“允许”）还是拒绝转发（“拒绝”）。默认值为“允

	许”。
速率限制器 ID	选择要在此端口上应用的速率限制器。允许的值为 Disabled 或值 1 至 16。默认值为“Disabled”。
EVC 策略器	选择是启用还是禁用 EVC 策略器。默认值为“Disabled”。请注意，ACL 速率限制器和 EVC 策略器不能同时启用。
EVC 策略器 ID	选择要在此端口上应用的 EVC 策略器标识。允许的值为 Disabled 或值 1 到 256。
端口重定向	选择重定向的端口帧。允许的值为 Disabled 或特定端口号，并且在允许操作时无法设置。默认值为“Disabled”。
镜像	指定此端口的镜像操作。允许的值为： 启用：端口上接收的帧被镜像。 禁用：端口上接收的帧不镜像。 默认值为“Disabled”。
记录	指定此端口的日志记录操作。注意，日志消息不包括 4 字节 CRC。允许的值为： 启用：端口上接收的帧存储在系统日志中。 禁用：不记录端口上接收的帧。 默认值为“Disabled”。注意：日志记录功能仅在数据包长度小于 1518（无 VLAN 标记）且系统日志内存大小和日志记录速率受限时生效。
关闭	指定此端口的端口关闭操作。允许的值为： 启用：如果在端口上接收到帧，则端口将被禁用。 禁用：禁用端口关闭。 默认值为“Disabled”。 注意：关闭功能仅在包长度小于 1518（无 VLAN 标记）时有效。
状态	指定此端口的端口状态。允许的值为： 启用：通过更改 ACL 用户模块的易失性端口配置重新打开端口。 禁用：通过更改 ACL 用户模块的易失性端口配置关闭端口。 默认值为“Enabled”。
计数器	计算与此 ACE 匹配的帧数。

6.7.3. ACL 速率限制

配置交换机 ACL 的速率限制。

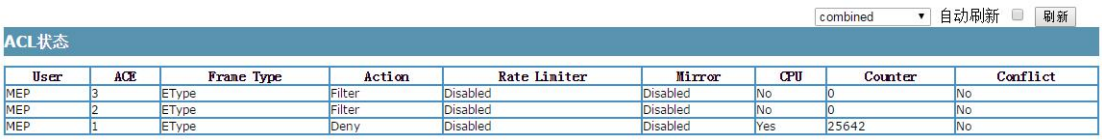


ACL 速率限制配置各项各参数说明如下表所示：

配置项	说明
速率限制器 ID	包含在同一行中的设置的速率限制器 ID。
速率	速率范围位于 0-3276700（以 pps 为单位）。 或以 kbps 为单位的 0,100,200,300，...，1000000。
单位	指定速率单位。 允许的值为： pps：每秒数据包。 kbps：Kbits /秒。

6.7.4. ACL 状态

此页面显示不同 ACL 用户的 ACL 状态。每行描述定义的 ACE。由于硬件限制，如果特定的 ACE 未应用于硬件，则这是一个冲突。每个交换机的最大 ACE 数为 256。



ACL 状态各项各参数说明如下表所示：

配置项	说明
用户	表示 ACL 用户。
ACE	表示本地交换机上的 ACE ID。
帧类型	表示 ACE 的帧类型。可能的值有：

	任意：ACE 将匹配任何帧类型。 EType：ACE 将匹配以太网类型帧。请注意，基于以太网类型的 ACE 将不会通过 IP 和 ARP 帧匹配。 ARP：ACE 将匹配 ARP / RARP 帧。 IPv4：ACE 将匹配所有 IPv4 帧。 IPv4 / ICMP：ACE 将使 IPv4 帧与 ICMP 协议匹配。 IPv4 / UDP：ACE 将使 IPv4 帧与 UDP 协议匹配。 IPv4 / TCP：ACE 将使 IPv4 帧与 TCP 协议匹配。 IPv4 /其他：ACE 将匹配 IPv4 帧，这不是 ICMP / UDP / TCP。 IPv6：ACE 将匹配所有 IPv6 标准帧。
动作	表示 ACE 的转发动作。 许可：可以转发和学习与 ACE 匹配的帧。 拒绝：匹配 ACE 的帧被丢弃。 过滤器：过滤与 ACE 匹配的帧。
速率限制器	表示 ACE 的速率限制器编号。允许的范围是 1 到 16.当显示 Disabled 时，禁止速率限制器操作。
CPU	将匹配特定 ACE 的数据包转发到 CPU。
计数器	计数器指示 ACE 被帧击中的次数。
冲突	表示特定 ACE 的硬件状态。由于硬件限制，特定的 ACE 不应用于硬件。

6.8. 2.8 NAS

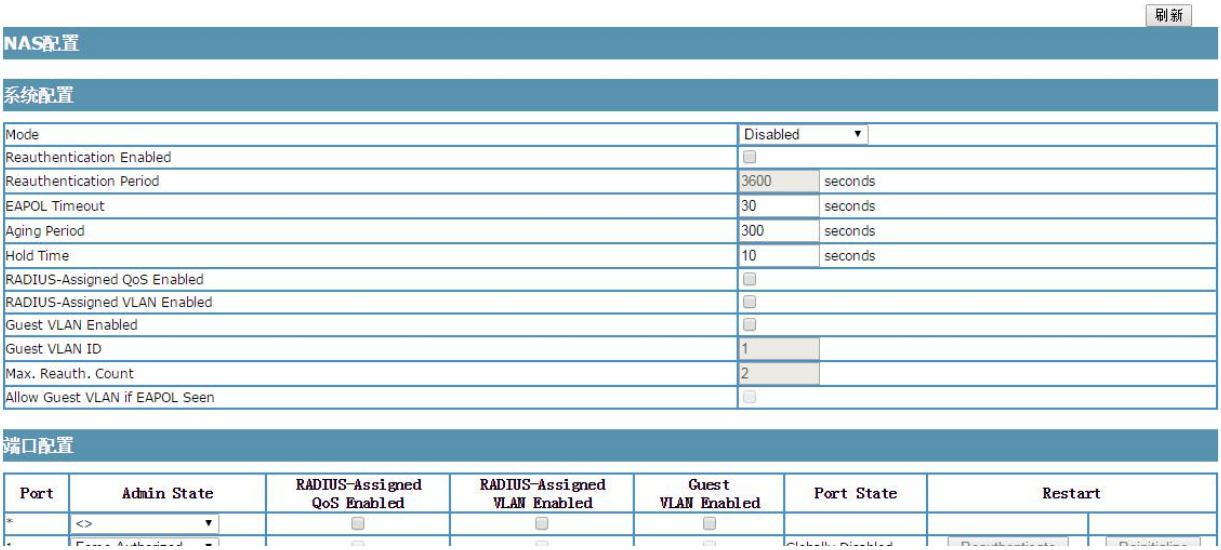
6.8.1. NAS 配置

此页面用于配置 IEEE 802.1X 和基于 MAC 的身份验证系统和端口设置。

IEEE 802.1X 标准定义了基于端口的访问控制过程，其通过要求用户首先提交用于认证的凭证来防止对网络的未授权访问。一个或多个中央服务器（后端服务器）确定用户是否被允许访问网络。在“配置→安全→AAA”页面上配置这些后端（RADIUS）服务器。 IEEE802.1X 标准定义基于端口的操作，但是非标准变体克服了下面将要探讨的安全限制。

基于 MAC 的认证允许在同一端口上对多个用户进行认证，并且不要求用户在其系统上安装特殊的 802.1X 请求方软件。交换机使用用户的 MAC 地址对后端服务器进行身份验证。入侵者可以创建伪造的 MAC 地址，这使得基于 MAC 的认证不如 802.1X 认证安全。

NAS 配置由两个部分组成，系统配置和端口配置。



6.8.1.1. 系统配置

系统配置各项各参数说明如下表所示：

配置项	说明
模式	指示 NAS 是否在交换机上全局启用或禁用。如果全局禁用，所有端口都允许转发帧。
启用重新认证	如果选中，则在重新认证期指定的时间间隔后，将重新认证成功通过身份验证的客户端。对启用了 802.1X 的端口的重新认证可用于检测新设备是否插入交换机端口或者是否不再连接请求者。 对于基于 MAC 的端口，重新认证仅在 RADIUS 服务器配置更改时有用。它不涉及交换机和客户端之间的通信，因此并不意味着客户端仍然存在于端口上（参见下面的老化周期）。
重新认证时间	确定连接的客户端必须重新验证的时间（以秒为单位）。只有选中重新认证启用复选框时，此选项才会激活。有效值的范围为 1 到 3600 秒。
EAPOL 超时	确定请求标识 EAPOL 帧的重传时间。 有效值的范围为 1 到 65535 秒。这对基于 MAC 的端口没有影响。
老化时间	此设置适用于以下模式，即使用端口安全功能保护 MAC 地址的模式：

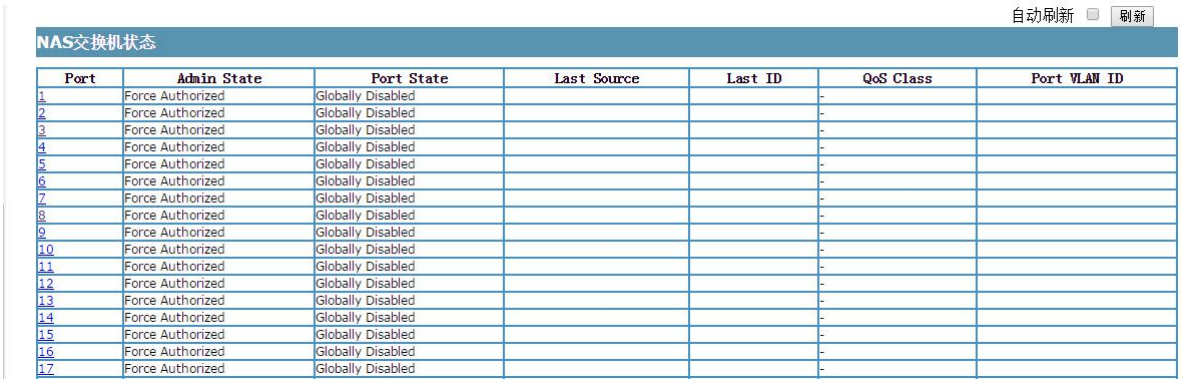
	•单个 802.1X •多 802.1X •基于 MAC 的验证。 当 NAS 模块使用端口安全模块保护 MAC 地址时，端口安全模块需要定期检查有问题的 MAC 地址上的活动，并且如果在给定时间段内没有活动，则释放资源。此参数精确控制此周期，可以设置为 10 到 1000000 秒之间的数字。 如果启用重新认证并且端口处于基于 802.1X 的模式，则这不是那么重要，因为不再连接到端口的请求者将在下一次重新认证时被删除，这将失败。但如果重新认证未启用，唯一的方式来释放资源是通过老化条目。 对于基于 MAC 的 Auth 中的端口。模式，重新认证不会导致交换机和客户端之间的直接通信，因此这将不会检测客户端是否仍然连接，释放任何资源的唯一方法是对条目进行老化。
保持时间	此设置适用于以下模式，即使用端口安全功能保护 MAC 地址的模式： •单个 802.1X •多 802.1X •基于 MAC 的验证。 如果客户端被拒绝访问 - 或者因为 RADIUS 服务器拒绝客户端访问，或者因为 RADIUS 服务器请求超时（根据在“配置→安全→AAA”页面指定的超时） - 客户端被搁置在未授权状态。保持定时器在正在进行的认证期间不计数。 在基于 MAC 的认证。模式，交换机将忽略在保持时间期间来自客户端的新帧。 保持时间可以设置为 10 到 1000000 秒之间的数字。
启用 RADIUS 分配的 QoS	RADIUS 分配的 QoS 提供了一种集中控制在交换机上分配来自成功认证的请求方的流量的流量类别的方法。 RADIUS 服务器必须配置为传输特殊的 RADIUS 属性以利用此功能（请参阅下面的 RADIUS 分配的 QoS 启用详细描述）。 “RADIUS 分配的 QoS 启用”复选框提供了全局启用/禁用 RADIUS 服务器分配的 QoS 类功能的快速方法。选中时，各个端口的同步设置确定是否在该端口上启用了 RADIUS 分配的 QoS 类别。取消

	选中时，在所有端口上禁用 RADIUS 服务器分配的 QoS 类。
启用 RADIUS 分配的 VLAN	RADIUS 分配的 VLAN 提供了一种方法来集中控制在交换机上放置成功认证的请求方的 VLAN。入局流量将分类到并分配给 RADIUS 分配的 VLAN。 RADIUS 服务器必须配置为传输特殊的 RADIUS 属性以利用此功能（请参阅下面的 RADIUS 分配的 VLAN 已启用详细描述）。 “RADIUS 分配的 VLAN 启用”复选框提供了全局启用/禁用 RADIUS 服务器分配的 VLAN 功能的快速方法。选中时，各个端口的同步设置确定是否在该端口上启用了 RADIUS 分配的 VLAN。取消选中时，在所有端口上禁用 RADIUS 服务器分配的 VLAN。
启用访客 VLAN	访客 VLAN 是一个特殊的 VLAN - 通常具有有限的网络访问 - 在网络管理员定义的超时后，802.1X 不知道的客户端被放置。交换机遵循一组用于进入和离开访客 VLAN 的规则，如下所示。 “访客 VLAN 启用”复选框提供了全局启用/禁用访客 VLAN 功能的快速方法。选中时，各个端口的同步设置确定该端口是否可以移入访客 VLAN。取消选中时，将在所有端口上禁用移动到访客 VLAN 的功能。
访客 VLAN ID	这是一个端口的端口 VLAN ID 设置为如果一个端口被移动到访客 VLAN 的值。只有在全局启用访客 VLAN 选项时，它才可更改。 有效值在[1; 4095]。
最大的 Reauth 计数	交换机在考虑进入访客 VLAN 之前发送 EAPOL 请求标识帧而没有响应的次数通过此设置进行调整。只有在全局启用访客 VLAN 选项时，才能更改该值。 有效值在[1; 255]。
如果 EAPOL 收到，则允许 Guest VLAN	交换机会记住在端口的生命周期内是否已收到 EAPOL 帧。一旦交换机考虑是否进入访客 VLAN，它将首先检查此选项是否启用或禁用。如果禁用（未选中;默认），交换机将仅输入访客 VLAN，如果在端口的生命周期内没有收到 EAPOL 帧。如果启用（选中），交换机将考虑输入访客 VLAN，即使在端口的生命周期内接收到

	EAPOL 帧。 只有在全局启用访客 VLAN 选项时，才能更改该值。

6.8.2. NAS 交换机状态

此页面提供当前 NAS 端口状态的概述。



NAS 交换机状态各项各参数说明如下表所示：

配置项	说明
端口	交换机端口号。单击导航到此端口的详细 NAS 统计信息。
管理状态	端口的当前管理状态。
端口状态	端口的当前状态。
最后来源	在最近接收的 EAPOL 帧中携带的用于基于 EAPOL 的认证的源 MAC 地址，以及最近从新客户端接收的用于基于 MAC 的认证的帧。
最后 ID	用于基于 EAPOL 的身份验证的最近收到的响应身份 EAPOL 帧中携带的用户名（请求方身份），以及来自最近收到的帧的源 MAC 地址，用于基于 MAC 的身份验证来自新客户端。
QoS 类	QoS 如果启用，RADIUS 服务器为端口分配的类别。
端口 VLAN ID	NAS 已将端口置于的 VLAN ID。如果端口 VLAN ID 未被 NAS 覆盖，则该字段为空。 如果 VLAN ID 由 RADIUS 服务器分配，则“（RADIUS 分配）”将附加到 VLAN ID。在此处了解有关 RADIUS 分配的 VLAN 的更多信息。 如果端口移动到访客 VLAN，“（访客）”将附加到 VLAN ID。

6.8.3. NAS 统计端口

此页面提供运行基于 EAPOL 的 IEEE 802.1X 身份验证的特定交换机端口的详细 NAS 统计信息。对于基于 MAC 的端口，仅显示选定的后端服务器（RADIUS 身份验证服务器）统计信息。

使用端口选择框选择要显示的端口详细信息。

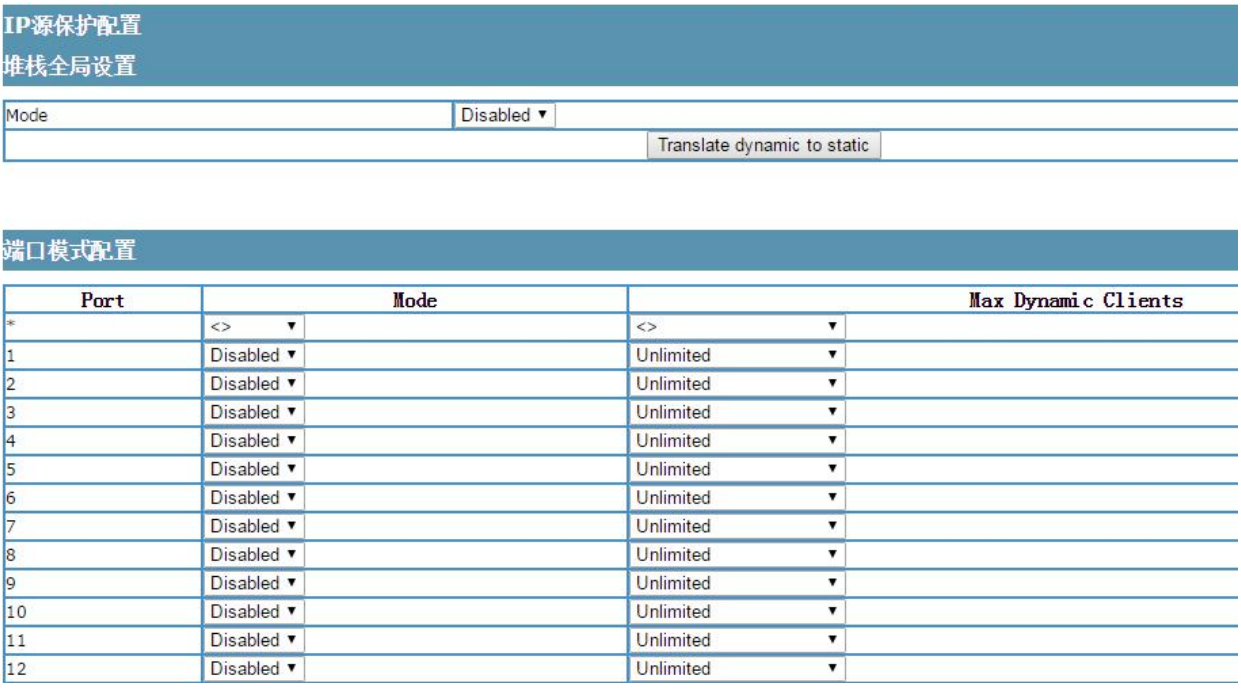
NAS 统计端口配置各项各参数说明如下表所示：

配置项	说明
管理状态	端口的当前管理状态。
端口状态	端口的当前状态。

6.9. IP 源保护

6.9.1. 配置

此页面提供 IP Source Guard 相关配置。

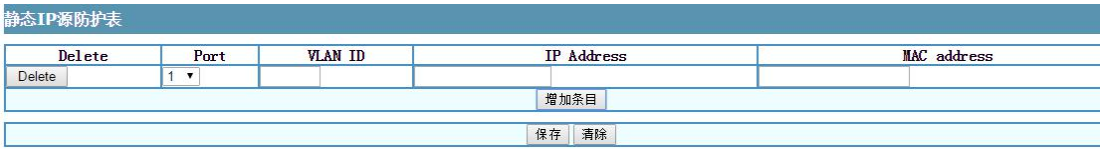


IP 源保护配置各项各参数说明如下表所示：

配置项	说明

IP Source Guard 配置模式	启用全局 IP 源保护或禁用全局 IP 源保护。 启用模式时，所有配置的 ACE 都将丢失。
端口模式配置	指定在哪些端口上启用 IP 源防护。 只有当给定端口上的全局模式和端口模式都启用时，才会在此给定端口上启用 IP Source Guard。
最大动态客户端	指定在给定端口上可以学习的动态客户端的最大数量。 此值可以是 0,1,2 或无限。 如果端口模式使能且 max dynamic client 的取值为 0，则表示只允许指定端口上静态表项匹配的 IP 报文转发。

6.9.2. 静态表



静态 IP 源防护表配置各项各参数说明如下表所示：

配置项	说明
删除	选中以删除条目。 它将在下次保存时被删除。
端口	设置的逻辑端口。
VLAN ID	设置的 vlan id。
IP 地址	允许的源 IP 地址。
MAC 地址	允许的源 MAC 地址。

6.9.3. 动态 IP 源防护表

动态 IP 源防护表中的条目显示在此页面上。 动态 IP 源保护表首先按端口排序，然后按 VLAN ID、IP 地址、MAC 地址排序。

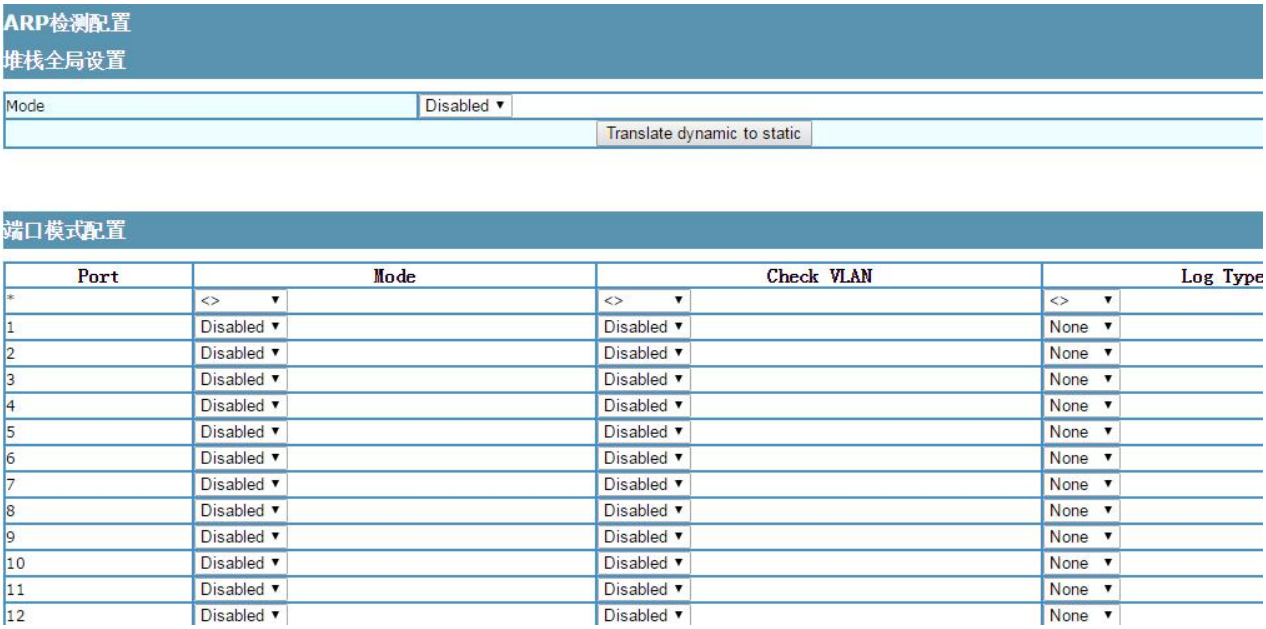
动态 IP 源防护表配置各项各参数说明如下表所示：

配置项	说明
端口	开关端口显示条目的端口号。
VLAN ID	允许 IP 流量的 VLAN-ID。
IP 地址	条目的用户 IP 地址。
MAC 地址	源 MAC 地址。

6.10. ARP

6.10.1. ARP 检测配置

本页提供 ARP 检测相关配置。



ARP 检测配置各项各参数说明如下表所示：

配置项	说明
ARP 检测配置模式	启用全局 ARP 检测或禁用全局 ARP 检测。
端口模式配置	指定 ARP 检测在哪些端口上启用。仅当给定端口上的全局模式和端口模式都启用时，才会在此给定端口上启用 ARP 检查。可能的模式有： 启用：启用 ARP 检测操作。 禁用：禁用 ARP 检测操作。 如果要检查 VLAN 配置，必须启用“检查 VLAN”的设置。默认设置“检查 VLAN”被禁用。当“检查 VLAN”的设置被禁用时，ARP 检查的日志类型将参考端口设置。启用“检查 VLAN”的设置后，ARP 检测的日志类型将参考 VLAN 设置。 “检查 VLAN”的可能设置包括： 启用：启用检查 VLAN 操作。 禁用：禁用检查 VLAN 操作。 只有在给定端口上的全局模式和端口模式被启用，并且“检查 VLAN”的设置被禁用，ARP 检查的日志类型将参考端口设置。有四种日志类型，可能的类型有：

	无：不记录。 拒绝：拒绝日志。 许可：记录允许的条目。 ALL：记录所有条目。

6.10.2. VLAN 模式配置

本页提供 ARP 检测相关配置。

VLAN 模式配置各项各参数说明如下表所示：

配置项	说明
VLAN 模式配置	指定 ARP 检测在哪些 VLAN 上启用。 首先，您必须在端口模式配置网页上启用端口设置。 仅当给定端口上的全局模式和端口模式都启用时，才会在此给定端口上启用 ARP 检查。 其次，您可以指定在 VLAN 模式配置网页上检查哪个 VLAN。
日志类型	无：不记录。 拒绝：拒绝日志。 许可：记录允许的条目。 ALL：记录所有条目。

6.10.3. 静态 ARP 检测表

静态 ARP 检测表配置各项各参数说明如下表所示：

配置项	说明
删除	选中以删除条目。 它将在下次保存时被删除。
端口	设置的逻辑端口。
VLAN ID	设置的 VLAN ID。
MAC 地址	允许 ARP 请求报文中的源 MAC 地址。

IP 地址	允许 ARP 请求报文中的源 IP 地址。

6.10.4. 动态 ARP 检测表配置

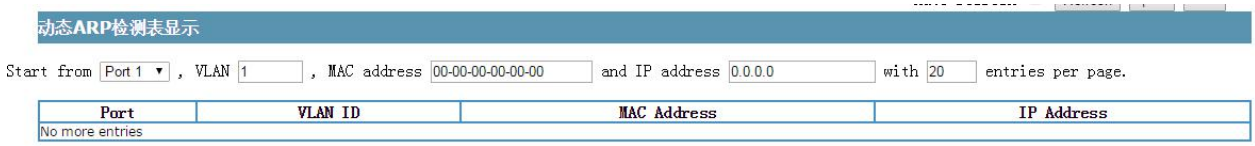
动态 ARP 检测表中的条目显示在此页面上。动态 ARP 检测表最多包含 1024 个条目，按端口排序，然后按 VLAN ID 排序，然后按 MAC 地址排序，然后按 IP 地址排序。

动态 ARP 检测表配置各项各参数说明如下表所示：

配置项	说明
ARP 检测表	每个页面最多显示来自动态 ARP 检查表的 99 个条目，默认值为 20，通过“每页条目”输入字段选择。首次访问时，网页将显示从动态 ARP 检查表开始的前 20 个条目。 “从端口起始地址”，“VLAN”，“MAC 地址”和“IP 地址”输入字段允许用户在动态 ARP 检测表中选择起始点。单击刷新按钮将更新显示的表或从最近的下一个动态 ARP 检测表匹配。此外，两个输入字段将在刷新按钮单击时采用第一个显示条目的值，从而允许使用相同的起始地址进行连续刷新。 >>将使用当前显示的表的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。
端口	开关端口显示条目的端口号。
VLAN ID	允许 ARP 流量的 VLAN-ID。
MAC 地址	用户 MAC 地址。
IP 地址	条目的用户 IP 地址。
翻译为静态	选中复选框以将条目转换为静态条目。

6.10.5. 动态 ARP 检测表显示

动态 ARP 检测表中的条目显示在此页面上。动态 ARP 检测表最多包含 1024 个条目，按端口排序，然后按 VLAN ID 排序，然后按 MAC 地址排序，然后按 IP 地址排序。



动态 ARP 检测表显示配置各项各参数说明如下表所示：

配置项	说明
浏览 ARP 检测表	每个页面最多显示来自动态 ARP 检查表的 99 个条目，默认值为 20，通过“每页条目”输入字段选择。首次访问时，网页将显示从动态 ARP 检查表开始的前 20 个条目。 “从端口起始地址”，“VLAN”，“MAC 地址”和“IP 地址”输入字段允许用户在动态 ARP 检测表中选择起始点。单击刷新按钮将更新显示的表或从最近的下一个动态 ARP 检测表匹配。此外，两个输入字段将在刷新按钮单击时采用第一个显示条目的值，从而允许使用相同的起始地址进行连续刷新。 >>将使用当前显示的表的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。
端口	开关端口显示条目的端口号。
VLAN ID	允许 ARP 流量的 VLAN-ID。
MAC 地址	用户 MAC 地址。
IP 地址	用户 IP 地址。

6.11. 镜像

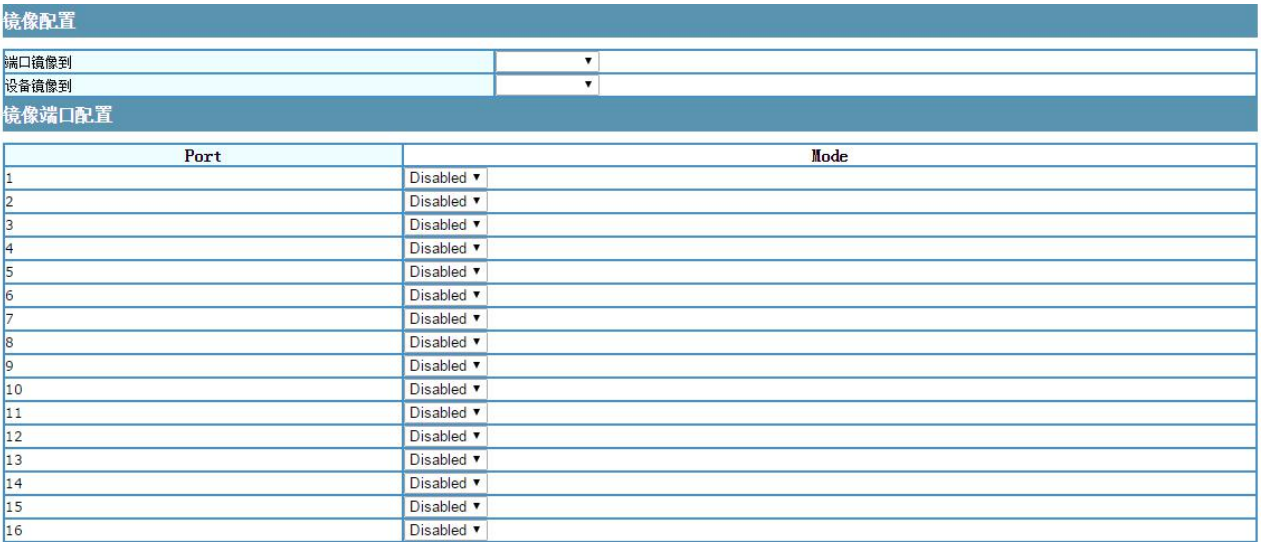
在此页面上配置端口镜像。

为了调试网络问题，可以在可连接帧分析器的镜像端口上复制或镜像选定的流量，以分析帧流。

要在镜像端口上复制的流量选择如下：

在给定端口上接收的所有帧（也称为入口或源镜像）。

在给定端口上传输的所有帧（也称为出口或目标镜像）。



镜像配置各项各参数说明如下表所示：

配置项	说明
要镜像的端口	端口到镜像也称为镜像端口。来自已启用源（rx）或目标（tx）镜像的端口的帧将镜像到此端口上。禁用禁用镜像。
镜像端口配置	下表用于 Rx 和 Tx 使能。
端口	同一行中包含的设置的逻辑端口。
模式	选择镜像模式。 Rx only--仅接收此端口上接收的帧在镜像端口上镜像。传输的帧不镜像。 Tx only--仅在此端口上传输的帧在镜像端口上镜像。接收的帧不镜像。 禁用--未镜像发送的帧或接收到的帧。 启用--接收的帧和传输的帧在镜像端口上镜像。

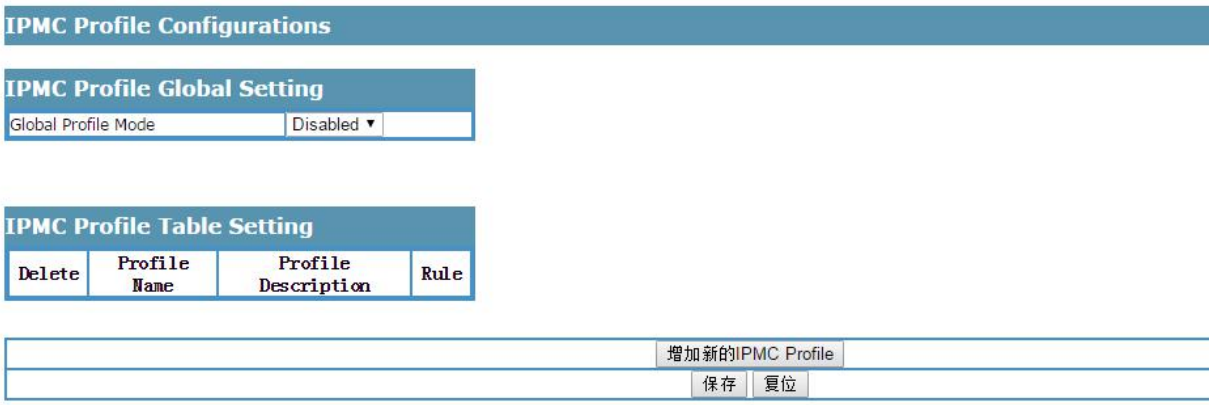
注意：对于给定端口，帧只传输一次。因此，不可能镜像镜像端口 Tx 帧。因此，所选镜像端口的模式仅限于 Disabled 或 Rx only。

6.12. IPMC

6.12.1. IPMC 文件配置

本页提供 IPMC Profile 相关配置。

IPMC 配置文件用于部署 IP 组播流的访问控制。允许创建最多 64 个配置文件，每个最多 128 个相应的规则。



IPMC 文件配置各项各参数说明如下表所示：

配置项	说明
全局配置文件模式	启用/禁用全局 IPMC 配置文件。 仅当启用全局配置文件模式时，系统才会根据配置文件设置开始进行过滤。
删除	选中以删除条目。 指定的条目将在下次保存时被删除。
配置文件名称	用于对概要文件表进行索引的名称。 每个条目都有唯一的名称，最多由 16 个字母和数字字符组成。必须至少有一个字母表。
配置文件描述	附加说明，由最多 64 个字母和数字字符组成，关于配置文件。 作为描述的一部分，不允许使用空格或空格字符。使用“_”或“ - ”分隔描述句。
规则	创建配置文件时，单击编辑按钮进入指定配置文件的规则设置页面。有关指定配置文件的摘要将通过单击视图按钮显示。您可以使用以下按钮管理或检查指定配置文件的规则： 导航：列出与指定配置文件关联的规则。 编辑：调整与指定配置文件关联的规则。

6.12.2. IPMC 地址条目

此页面提供 IPMC 配置文件中使用的地址范围设置。

地址条目用于指定将与 IPMC 配置文件相关联的地址范围。 允许在系统中最多创建 128 个地址条目。

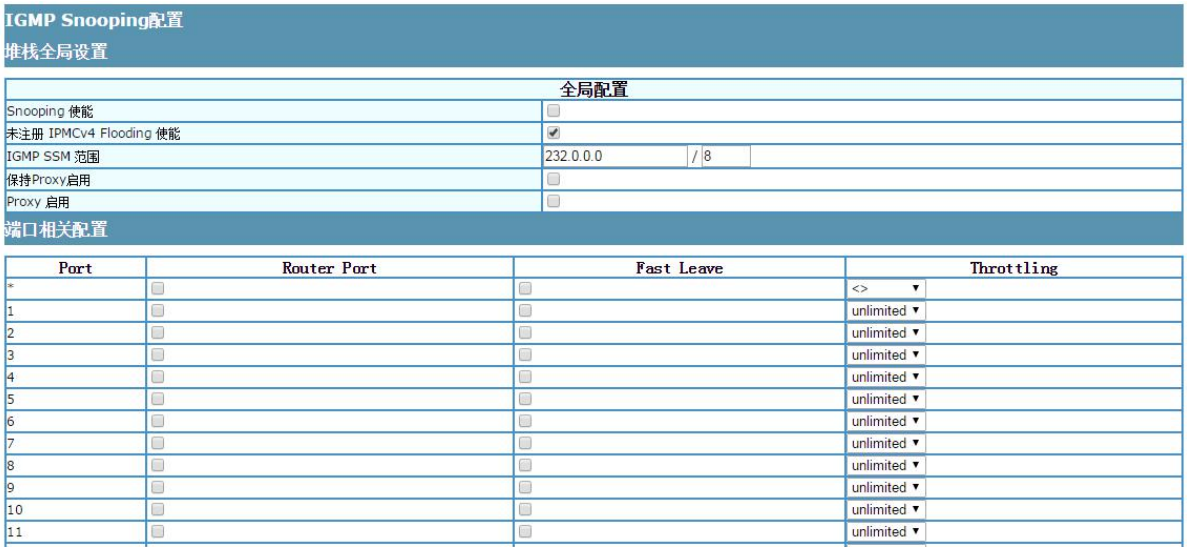
IPMC 地址条目配置各项各参数说明如下表所示：

配置项	说明
删除	选中以删除条目。 指定的条目将在下次保存时被删除。
条目名称	用于索引地址条目表的名称。 每个条目都有唯一的名称，最多由 16 个字母和数字字符组成。 必须至少有一个字母表。
开始地址	将用作地址范围的起始 IPv4 / IPv6 多播组地址。
结束地址	将用作地址范围的结束 IPv4 / IPv6 多播组地址。

6.12.3. IGMP Snooping

6.12.3.1. 基本配置

本页提供 IGMP Snooping 相关配置。



IGMP Snooping 配置各项各参数说明如下表所示：

配置项	说明
Snooping 使能	启用全局 IGMP 侦听。
未注册的 IPMCv4 洪泛	启用未注册的 IPMCv4 流量洪泛。

使能	只有启用 IGMP Snooping 时，洪泛控制才生效。 当 IGMP Snooping 被禁用时，尽管有此设置，未注册的 IPMCv4 流量洪泛始终处于活动状态。
IGMP SSM 范围	SSM（源特定组播）范围允许 SSM 感知主机和路由器为地址范围内的组运行 SSM 服务模型。
保持 Proxy 启用	启用 IGMP 离开代理。此功能可用于避免转发不必要的离开报文到路由器端。
Proxy 启用	启用 IGMP 代理。此功能可用于避免转发不必要的加入和离开报文到路由器端。
路由器端口	指定哪些端口充当路由器端口。路由器端口是以太网交换机上通向三层组播设备或 IGMP 查询器的端口。 如果选择聚合成员端口作为路由器端口，整个聚合将作为路由器端口。
快速离开	在端口上启用快速离开。
节流	启用以限制交换机端口可以属于的组播组的数量。

6.12.3.2. VLAN 配置

IGMP Snooping VLAN 介绍

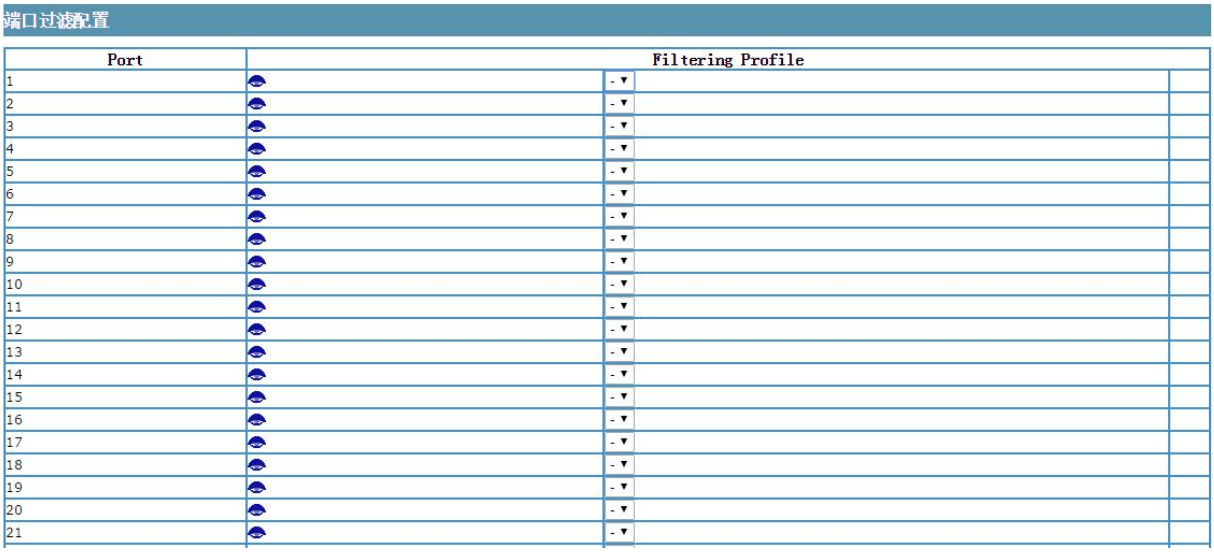
每个页面最多显示从 VLAN 表中的 99 个条目，默认值为 20，通过“每页输入项”输入字段选择。首次访问时，网页将显示 VLAN 表开头的前 20 个条目。第一个显示的将是 VLAN 表中找到的最低 VLAN ID。“VLAN”输入字段允许用户在 VLAN 表中选择起始点。单击刷新按钮将从该表或下一个最接近的 VLAN 表匹配开始更新显示的表。>>将使用当前显示条目的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。

QIGMP Snooping VLAN 配置各项各参数说明如下表所示：

配置项	说明
删除	选中以删除条目。指定的条目将在下次保存时被删除。
VLAN ID	条目的 VLAN ID。
IGMP Snooping 启用	启用对应 VLAN 的 IGMP Snooping。 IGMP Snooping 最多可以选择 32 个 VLAN。
查询者选举	启用在 VLAN 中加入 IGMP 查询器选举。禁用作为 IGMP 非查询

	器。
查询地址	定义 IPv4 地址作为 IGMP 查询器选举的 IP 头中使用的源地址。 当未设置 Querier 地址时，系统使用与该 VLAN 关联的 IP 接口的 IPv4 管理地址。 当未设置 IPv4 管理地址时，系统使用第一个可用的 IPv4 管理地址。否则，系统使用预定义的值。默认情况下，此值为 192.0.2.1。
兼容性	兼容性由主机和路由器根据在主机和网络中的路由器上运行的 IGMP 的版本采取适当的动作来维护。 允许的选择是 IGMP 自动，强制 IGMPv1，强制 IGMPv2，强制 IGMPv3，默认兼容性值是 IGMP 自动。
PRI	接口的优先级。 它表示系统生成的 IGMP 控制帧优先级。这些值可用于确定不同类别的流量的优先级。 允许的范围是 0（最大努力）到 7（最高），默认接口优先级值为 0。
RV	鲁棒性变量。 鲁棒性变量允许调整网络上的预期数据包丢失。 允许的范围是 1 到 255，默认鲁棒性变量值是 2。
QI	查询间隔。 查询间隔是由查询器发送的常规查询之间的间隔。 允许范围为 1～31744 秒，缺省值为 125 秒。
QRI	查询响应时间间隔。 用于计算插入到周期性常规查询中的最大响应代码的最大响应延迟。 允许范围是 0 到 31744 十分之几秒，默认查询响应间隔是 100 十分之几秒（10 秒）。
LLQI（用于 IGMP 的 LMQI）	最后成员查询间隔。 最后成员查询时间是由最后成员查询时间间隔表示的时间值乘以最后成员查询计数。 允许范围是 0 到 31744 十分之几秒，默认最后一个成员查询间隔是 10 十分之一秒（1 秒）。
URI	主动报告间隔。未经请求的报告间隔是主机在组中的成员资格的初始报告的重复之间的时间。 允许范围为 0 到 31744 秒，默认主动报告间隔为 1 秒。

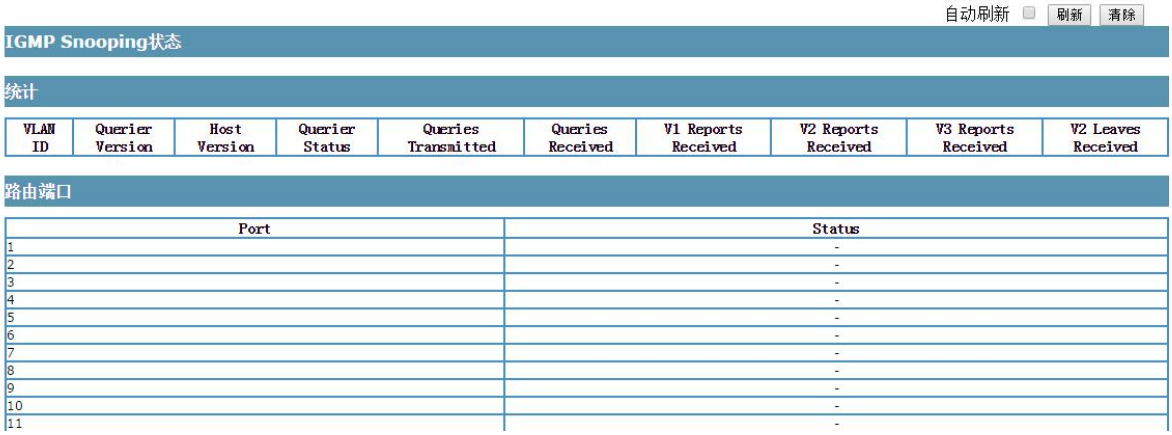
6.12.3.3. 端口过滤配置



端口过滤配置各项各参数说明如下表所示：

配置项	说明
端口	设备的逻辑端口。
过滤配置文件	选择 IPMC 配置文件作为特定端口的过滤条件。 有关指定配置文件的摘要将通过单击视图按钮显示。
配置文件管理按钮	您可以使用以下按钮检查指定配置文件的规则： ：列出与指定配置文件关联的规则。

6.12.3.4. IGMP 侦听状态



IGMP Snooping 状态配置各项各参数说明如下表所示：

配置项	说明
VLAN ID	条目的 VLAN ID。

查询版本	工作查询器版本。
主机版本	当前工作主机版本。
查询状态	显示查询器状态为“活动”或“空闲”。 “DISABLE”表示特定接口在管理上禁用。
传输的查询	传输的查询数。
收到的查询	接收的查询数。
接收的 V1 报告	接收的 V1 报告数。
已接收 V2 报告	接收的 V2 报告数。
已收到 V3 报告	接收的 V3 报告数。
V2 离开接收	接收的 V2 离开数。
路由器端口	显示哪些端口充当路由器端口。路由器端口是以太网交换机上通向三层组播设备或 IGMP 查询器的端口。 Static 表示特定端口配置为路由器端口。 Dynamic 表示特定端口被学习为路由器端口。 两者都表示特定端口被配置或学习为路由器端口。
端口	切换端口号。
状态	指示特定端口是否为路由器端口。

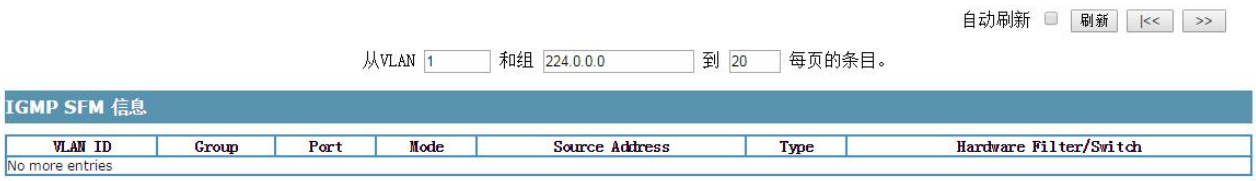
6.12.3.5. IGMP 组信息

IGMP Snooping 组信息配置各项各参数说明如下表所示：

配置项	说明
VLAN ID	组的 VLAN ID。
组	显示组的组地址。
端口成员	此组下的端口。

6.12.3.6. IGMP SFM 信息

IGMP SFM 信息表中的条目显示在此页面上。 IGMP SFM（源 - 过滤组播）信息表还包含 SSM（源特定组播）信息。 此表按 VLAN ID 排序，然后按组排序，然后按端口排序。 属于同一组的不同源地址被视为单个条目。



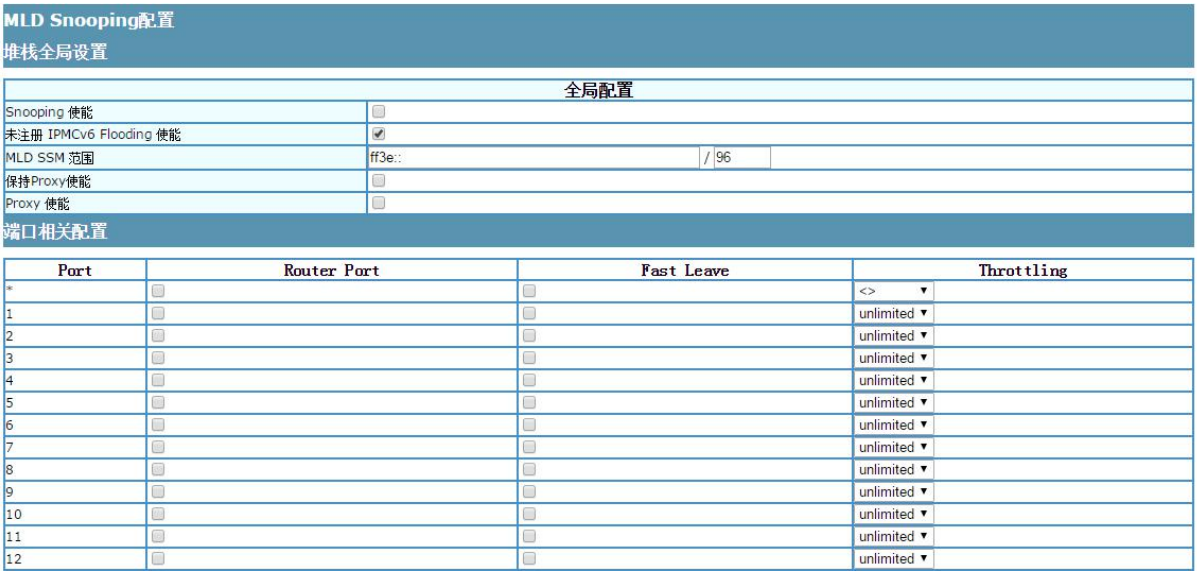
IGMP SFM 信息配置各项各参数说明如下表所示：

配置项	说明
VLAN ID	组的 VLAN ID。
组	显示组的组地址。
端口	切换端口号。
模式	指示维护的过滤模式（VLAN ID，端口号，组地址）。 它可以是 Include 或 Exclude。
源地址	源的 IP 地址。 目前，过滤（每组）的 IPv4 源地址的最大数量为 8。 当没有任何源过滤地址时，“源地址”字段中将显示文本“无”。
类型	表示类型。 它可以是“允许”或“拒绝”。
硬件滤波器/开关	指示从源 IPv4 地址发往特定组地址的数据平面是否可以由芯片处理。

6.12.4. MLD Snooping

6.12.4.1. 基本配置

本页提供 MLD Snooping 相关配置。



MLD Snooping 配置各项各参数说明如下表所示：

配置项	说明
Snooping 使能	启用全局 MLD Snooping。
未注册的 IPMCv6 Flooding 使能	启用未注册的 IPMCv6 流量洪泛。 只有启用 MLD Snooping 时，洪泛控制才生效。 当 MLD Snooping 被禁用时，尽管该设置，未注册的 IPMCv6 流量洪泛总是活动的。
MLD SSM 范围	SSM（源特定组播）范围允许 SSM 感知主机和路由器为地址范围内的组运行 SSM 服务模型。
保持 Proxy 启用	启用 MLD 离开 Proxy。此功能可用于避免转发不必要的离开报文到路由器端。
Proxy 使能	启用 MLD Proxy。此功能可用于避免转发不必要的加入和离开报文到路由器端。
路由器端口	指定哪些端口充当路由器端口。路由器端口是以太网交换机上通向三层组播设备或 MLD 查询器的端口。 如果选择聚合成员端口作为路由器端口，整个聚合将作为路由器端口。
快速离开	在端口上启用快速离开。
节流	启用以限制交换机端口可以属于的组播组的数量。

6.12.4.2. VLAN 配置

介绍 MLD Snooping VLAN 表

每个页面最多显示从 VLAN 表中的 99 个条目，默认值为 20，通过“每页输入项”输入字段选择。首次访问时，网页将显示 VLAN 表开头的前 20 个条目。第一个显示的将是 VLAN 表中找到的最低 VLAN ID。

“VLAN”输入字段允许用户在 VLAN 表中选择起始点。单击刷新按钮将从该表或下一个最接近的 VLAN 表匹配开始更新显示的表。

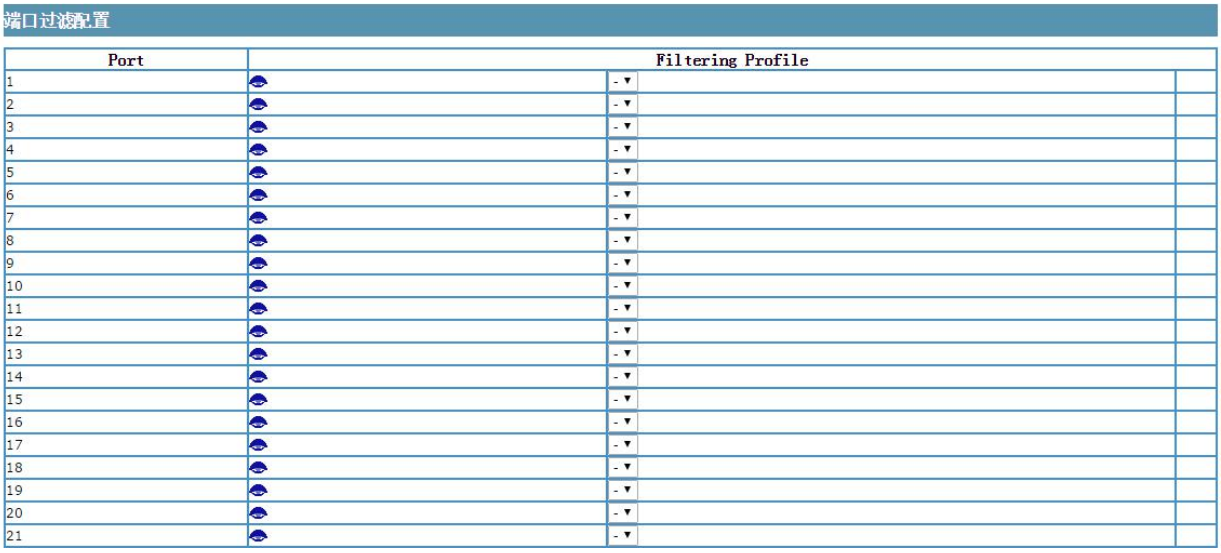
>>将使用当前显示条目的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。

MLD Snooping VLAN 表配置各项各参数说明如下表所示：

配置项	说明
删除	选中以删除条目。指定的条目将在下次保存时被删除。
VLAN ID	条目的 VLAN ID。
MLD Snooping 启用	启用每 VLAN MLD Snooping。 MLD Snooping 最多可以选择 32

	个 VLAN。
查询者选举	启用在 VLAN 中加入 MLD 查询器选举。禁用作为 MLD 非查询器。
兼容性	兼容性由主机和路由器根据在主机和网络中的路由器上操作的 MLD 的版本采取适当的动作来维护。 允许的选择是 MLD-Auto，Forced MLDv1，Forced MLDv2，默认兼容性值是 MLD-Auto。
PRI	接口的优先级。 它表示系统生成的 MLD 控制帧优先级。这些值可用于确定不同类别的流量的优先级。 允许的范围是 0（最大努力）到 7（最高），默认接口优先级值为 0。
RV	鲁棒性变量。 鲁棒性变量允许调整链路上的预期丢包率。 允许的范围是 1 到 255，默认鲁棒性变量值是 2。
QI	查询间隔。 查询间隔是由查询器发送的常规查询之间的间隔。 允许范围为 1～31744 秒，缺省值为 125 秒
QRI	查询响应时间间隔。 用于计算插入到周期性常规查询中的最大响应代码的最大响应延迟。 允许范围是 0 到 31744 十分之几秒，默认查询响应间隔是 100 十分之几秒（10 秒）。
LLQI	上次侦听器查询间隔。 最后侦听器查询间隔是用于计算响应于版本 1 多播监听器完成消息而发送的插入到多播地址特定查询中的最大响应代码的最大响应延迟。它也是用于计算插入到多播地址和源特定查询消息中的最大响应代码的最大响应延迟。 允许的范围是 0 到 31744 十分之几秒，默认最后侦听器查询间隔是 10 十分之一秒（1 秒）。
URI	主动报告间隔。 非请求报告间隔是在多播地址中关注的节点的初始报告的重复之间的时间。 允许范围为 0 到 31744 秒，默认主动报告间隔为 1 秒。

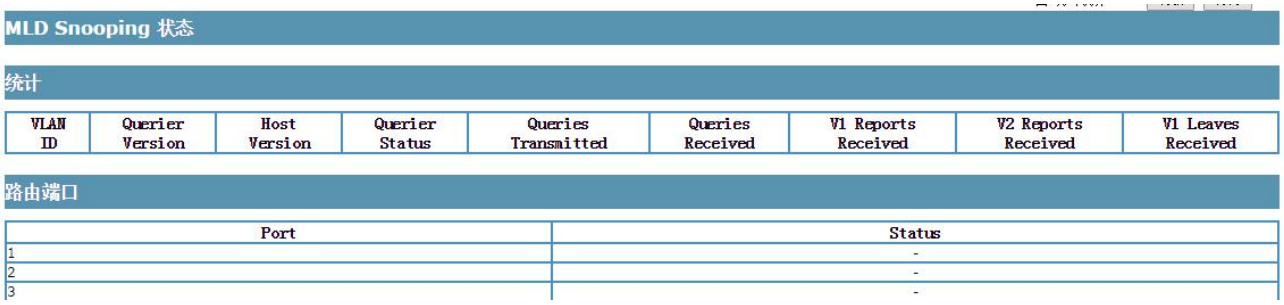
6.12.4.3. 端口过滤配置



端口过滤配置各项各参数说明如下表所示：

配置项	说明
端口	设置的逻辑端口。
过滤配置文件	选择 IPMC 配置文件作为特定端口的过滤条件。 有关指定配置文件的摘要将通过单击视图按钮显示。 您可以使用以下按钮检查指定配置文件的规则： ：列出与指定配置文件关联的规则。

6.12.4.4. MLD 侦听状态



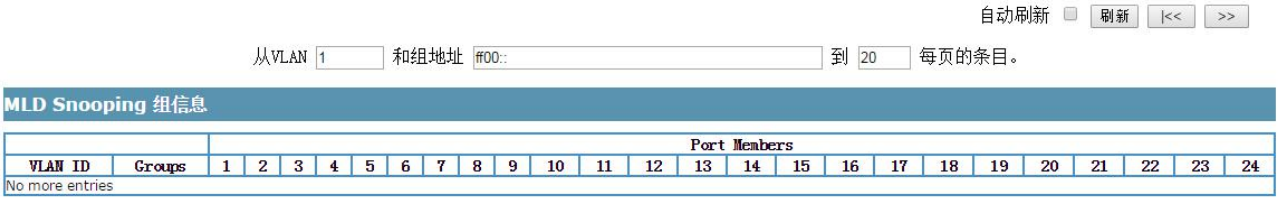
MLD 侦听状态各项各参数说明如下表所示：

配置项	说明
VLAN ID	条目的 VLAN ID。
查询版本	工作查询器版本。
主机版本	当前工作主机版本。

查询状态	显示查询器状态为“活动”或“空闲”。 “DISABLE”表示特定接口在管理上禁用。
传输的查询	传输的查询数。
收到的查询	接收的查询数。
接收的 V1 报告	接收的 V1 报告数。
已接收 V2 报告	接收的 V2 报告数。
接收到 V1 离开	接收的 V1 离开数。
路由器端口	显示哪些端口充当路由器端口。 路由器端口是以太网交换机上通向三层组播设备或 MLD 查询器的端口。 Static 表示特定端口被配置为路由器端口。 Dynamic 表示特定端口被学习为路由器端口。 两者都表示特定端口被配置或学习为路由器端口。
端口	切换端口号。
状态	指示特定端口是否为路由器端口。

6.12.4.5. MLD 组信息

MLD 组表中的条目显示在此页面上。 MLD 组表首先按 VLAN ID 排序，然后按组排序。

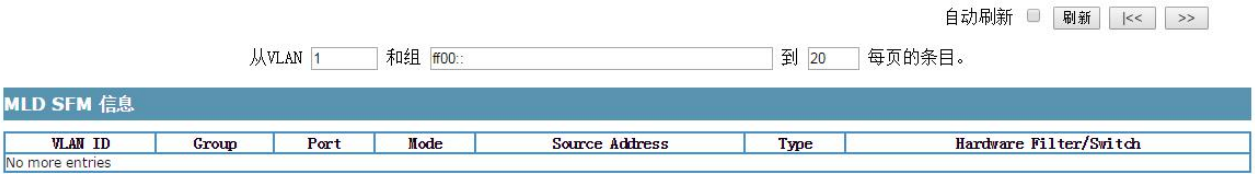


MLD Snooping 组信息各项各参数说明如下表所示：

配置项	说明
VLAN ID	组的 VLAN ID。
组	显示组的组地址。
端口成员	此组下的端口。

6.12.4.6. SFM 信息

MLD SFM 信息表中的条目显示在此页面上。 MLD SFM（源 - 过滤组播）信息表还包含 SSM（源特定组播）信息。 此表按 VLAN ID 排序，然后按组排序，然后按端口排序。 属于同一组的不同源地址被视为单个条目。



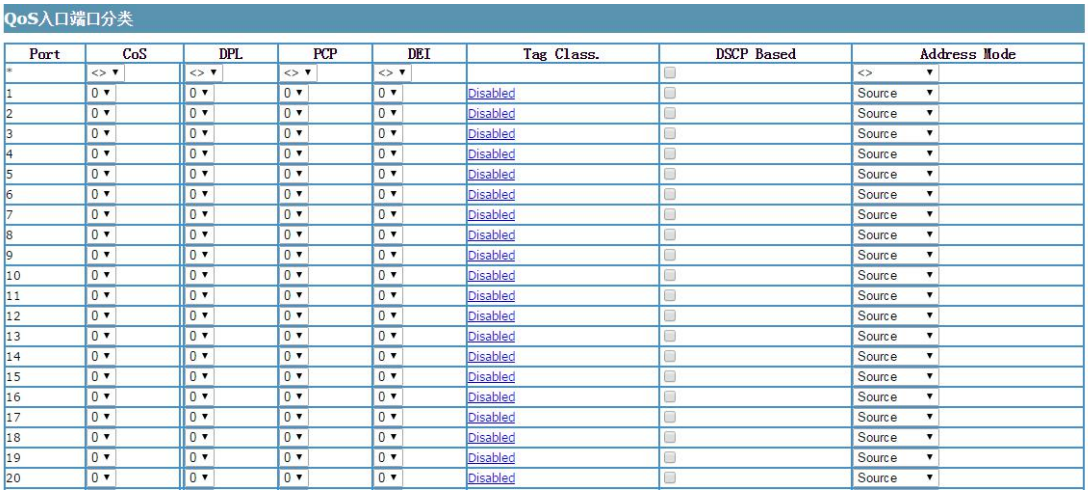
MLD SFM 信息各项各参数说明如下表所示：

配置项	说明
VLAN ID	组的 VLAN ID。
组	显示组的组地址。
端口	切换端口号。
模式	指示维护的过滤模式（VLAN ID，端口号，组地址）。 它可以是 Include 或 Exclude。
源地址	源的 IP 地址。 目前，过滤的 IPv6 源地址的最大数量（每组）为 8。 当没有任何源过滤地址时，“源地址”字段中将显示文本“无”。
类型	表示类型。 它可以是“允许”或“拒绝”。
硬件滤波器/开关	指示从源 IPv6 地址发往特定组地址的数据平面是否可以由芯片处理。

6.13. QoS

6.13.1. 入口端口分类

此页面允许您配置交换机所有端口的基本 QoS 入口分类设置。



QoS 入口端口分类各项各参数说明如下表所示：

配置项	说明

端口	以下配置所适用的端口号。
CoS	控制默认服务类别。 所有帧都分类为 CoS。在 CoS，队列和优先级之间存在一对一映射。0（零）的 CoS 具有最低的优先级。 如果端口是关注 VLAN 的，则帧被标记以及 Tag Class.被启用，然后该帧被分类到从标记中的 PCP 和 DEI 值映射的 CoS。否则，帧被分类到默认 CoS。 分类的 CoS 可以被 QCL 条目拒绝。 注意：如果默认 CoS 已动态修改，则实际默认 CoS 将显示在配置的默认 CoS 后面的括号中。
DPL	控制默认丢弃优先级。 所有帧都被分类为丢弃优先级。 如果端口是关注 VLAN 的，则帧被标记以及 Tag Class.被启用，然后该帧被分类到从标记中的 PCP 和 DEI 值映射的 DPL。否则，帧被分类到默认 DPL。 分类的 DPL 可以被 QCL 条目拒绝。
PCP	控制默认 PCP 值。 所有帧都分类为 PCP 值。 如果端口是关注 VLAN 的并且帧被标记，则该帧被分类到标记中的 PCP 值。否则，帧被分类为默认 PCP 值。
DEI	控制默认 DEI 值。所有帧都分类为 DEI 值。 如果端口是关注 VLAN 的并且帧被标记，则该帧被分类到标记中的 DEI 值。否则，帧被分类为默认 DEI 值。
Tag Class.	显示此端口上的标记帧的分类模式。 禁用：对标记的帧使用默认 CoS 和 DPL。 启用：使用映射版本的 PCP 和 DEI 用于标记的帧。 单击模式为了配置模式和/或映射。 注意：如果端口是 VLAN 未感知，此设置不起作用。在 VLAN 未知端口上接收的标记帧总是分类到默认 CoS 和 DPL。
基于 DSCP	单击启用基于 DSCP 的 QoS 入口端口分类。
地址模式	指定 QCL 分类是否必须基于此端口上的源（SMAC / SIP）或目标（DMAC / DIP）地址的 IP / MAC 地址模式。允许的值为： Source：启用 SMAC / SIP 匹配。 Destination：启用 DMAC / DIP 匹配。

6.13.2. 入口端口策略

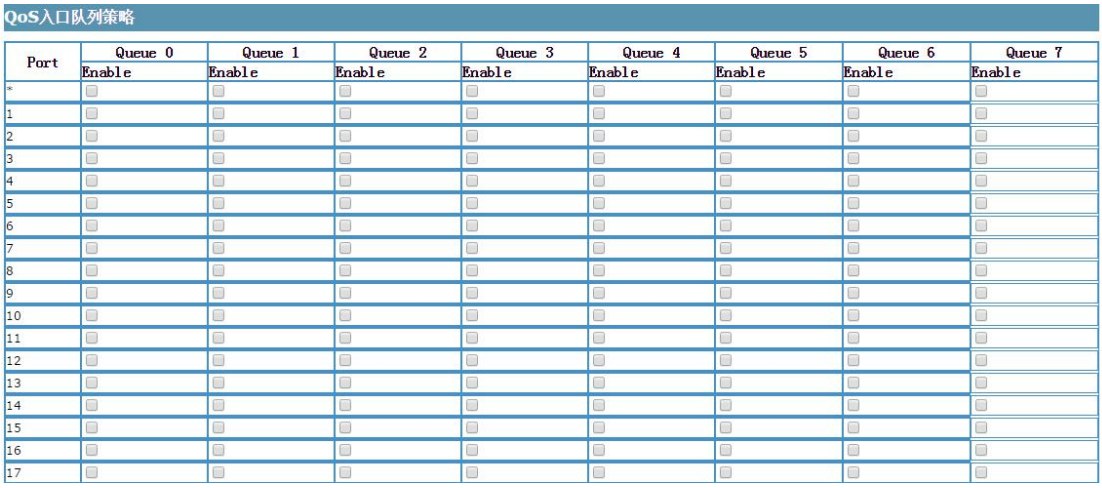
此页面允许您配置交换机所有端口的 Policer 设置。

QoS 入口端口策略各项各参数说明如下表所示：

配置项	说明
端口	以下配置所适用的端口号。
启用	控制是否在此交换机端口上启用策略器。
速率	控制策略器的速率。 默认值为 500。当“Unit”为“kbps”或“fps”时，此值限制为 100-1000000，当“Unit”为“Mbps”或“kfps”时，此值限制为 1-3300。
单位	控制策略器速率的测量单位为 kbps，Mbps，fps 或 kfps。 默认值为“kbps”。
流量控制	如果启用流量控制并且端口处于流控制模式，则发送暂停帧而不是丢弃帧。

6.13.3. 入口队列管理

此页面允许您配置交换机所有端口的队列策略器设置。

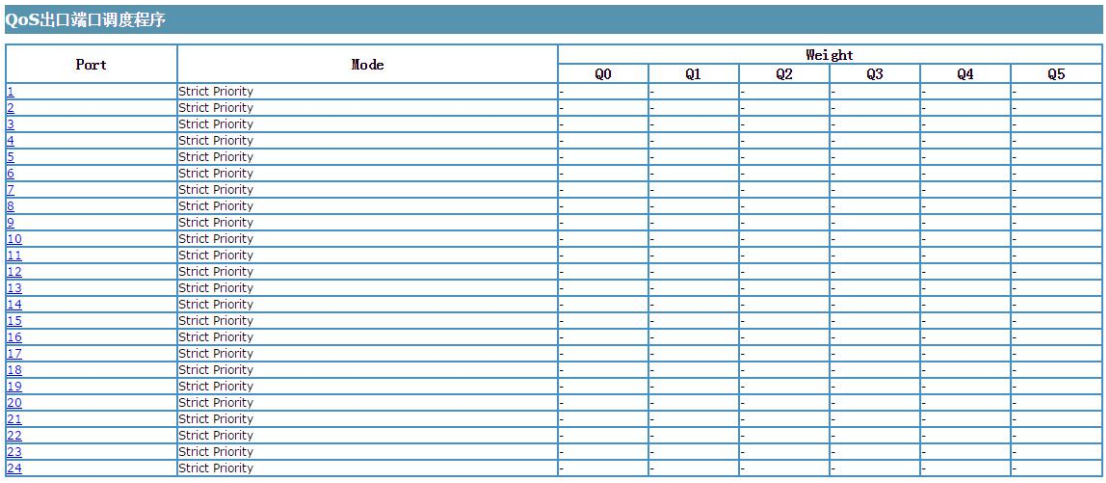


端口过滤配置各项各参数说明如下表所示：

配置项	说明
端口	以下配置所适用的端口号。
启用（E）	控制是否在此交换机端口上启用队列策略器。
速率	控制队列策略器的速率。 默认值为 500。当“Unit”为“kbps”时，此值限制为 100-1000000，当“Unit”为“Mbps”时，该值限制为 1-3300。 仅当至少启用了一个队列策略器时，才会显示此字段。
单位	将队列策略器速率的度量单位控制为 kbps 或 Mbps。 默认值为“kbps”。 仅当至少启用了一个队列策略器时，才会显示此字段。

6.13.4. 出口端口调度

此页面提供了交换机所有端口的 QoS 出口端口调度程序的概述。

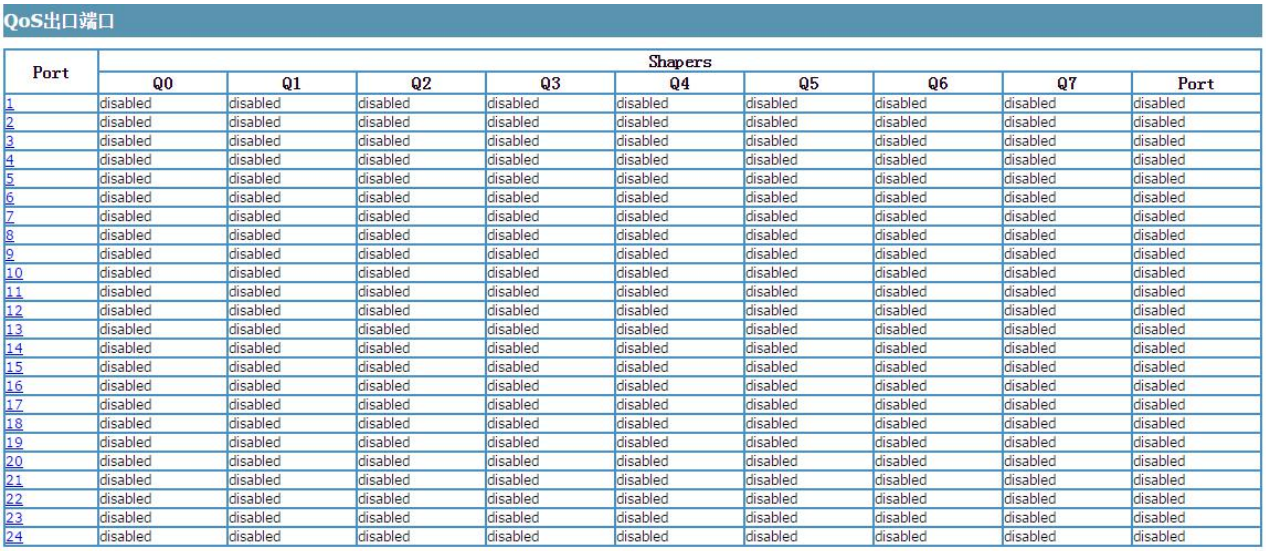


QoS 出口端口调度程序各项各参数说明如下表所示：

配置项	说明
端口	同一行中包含的设置的逻辑端口。 单击端口号为了配置调度程序
模式	显示此端口的调度模式。
Qn	显示此队列和端口的权重。

6.13.5. 出口端口调整

此页面提供交换机所有端口的 QoS 出口端口缩略图的概述。



QoS出口端口

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

QoS 出口端口各项各参数说明如下表所示：

配置项	说明
端口	同一行中包含的设置的逻辑端口。 单击端口号为了配置整形器。
Qn	显示“已禁用”或实际队列整形速率 - 例如 “800Mbps”。
端口	显示“禁用”或实际端口整形速率 - 例如 “800Mbps”。

6.13.6. 出口端口标记

此页面提供交换机所有端口的 QoS 出口端口标记备注的概述。

QoS出口端口标记备注

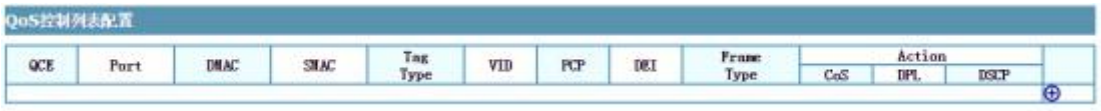
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified

QoS 出口端口标记备注各项各参数说明如下表所示：

配置项	说明
端口	同一行中包含的设置的逻辑端口。 单击端口号以配置标记注释。
模式	显示此端口的标记注释模式。 分类：使用分类的 PCP / DEI 值。 默认值：使用默认 PCP / DEI 值。 映射：使用 QoS 类和 DP 级别的映射版本。

6.13.7. 控制列表配置

此页面显示 QoS 控制列表（QCL），它由 QCE 组成。每行描述定义的 QCE。每个交换机的 QCE 的最大数量为 256。单击最低加号将新的 QCE 添加到列表中。



端口过滤配置各项各参数说明如下表所示：

配置项	说明
QCE	表示 QCE id。
端口	表示使用 QCE 配置的端口列表。
DMAC	表示目的 MAC 地址。可能的值有： 任何：匹配任何 DMAC。 单播：匹配单播 DMAC。 组播：匹配组播 DMAC。 广播：匹配广播 DMAC。

	默认值为“Any”。
SMAC	匹配特定源 MAC 地址或“任何”。 如果端口配置为在 DMAC / DIP 上匹配，则此字段指示 DMAC。 标签类型 表示代码类型。可能的值有： 任何：匹配标记和未标记的帧。 未标记：匹配未标记的帧。 标记：匹配标记的帧。 默认值为“Any”。
VID	指示（VLAN ID），特定 VID 或 VID 范围。 VID 可以在 1-4095 或“任意”
PCP	优先级代码点：PCP 的有效值是特定的（0,1,2,3,4,5,6,7）或范围（0-1,2-3,4-5,6-7,0-3， 4-7）或“任何”。
DEI	丢弃合格指示符：DEI 的有效值为 0,1 或'任何'。
Frame 类型	表示帧的类型。可能的值有： 任何：匹配任何帧类型。 以太网：匹配 EtherType 帧。 LLC：匹配（LLC）帧。 SNAP：匹配（SNAP）帧。 IPv4：匹配 IPv4 帧。 IPv6：匹配 IPv6 帧。
动作	表示如果配置的参数与帧的内容匹配，则对入口帧执行的分类操作。 可能的操作有： CoS：分类服务等级。 DPL：分类丢弃优先级。 DSCP：分类 DSCP 值。
修改按钮	您可以使用以下按钮修改表中的每个 QCE（QoS 控制条目）： 添加：在当前行之前插入新的 QCE。 编辑：编辑 QCE。 向上：将 QCE 向上移动列表。 向下：将 QCE 从列表中移开。 删除：删除 QCE。 添加：最低加号在 QCE 列表的底部添加一个新条目。

6.13.8. DSCP

6.13.8.1. DSCP 端口

此页面允许配置交换机所有端口的基本 QoS 端口 DSCP 配置设置。

QoS端口DSCP配置

Port	Ingress		Egress
	Translate	Classify	Rewrite
*		<>	<>
1		Disable	Disable
2		Disable	Disable
3		Disable	Disable
4		Disable	Disable
5		Disable	Disable
6		Disable	Disable
7		Disable	Disable
8		Disable	Disable
9		Disable	Disable
10		Disable	Disable
11		Disable	Disable
12		Disable	Disable
13		Disable	Disable
14		Disable	Disable
15		Disable	Disable
16		Disable	Disable
17		Disable	Disable
18		Disable	Disable
19		Disable	Disable

端口

“端口”列显示可以为其配置 dscp 入口和出口设置的端口列表。在 Ingress 设置中，您可以更改各个端口的入口翻译和分类设置。Ingress 提供了两个配置参数：

1.翻译：要启用 Ingress 翻译，请单击复选框。

2.分类：端口的分类有 4 个不同的值。

禁用：无入站 DSCP 分类。

DSCP = 0：如果传入（或翻译，如果启用）DSCP 为 0，则分类。

选择：仅对特定 DSCP 的 DSCP 转换窗口中指定的已启用分类的选定 DSCP 进行分类。

全部：分类所有 DSCP。

出口

端口出口重写可以是以下之一：

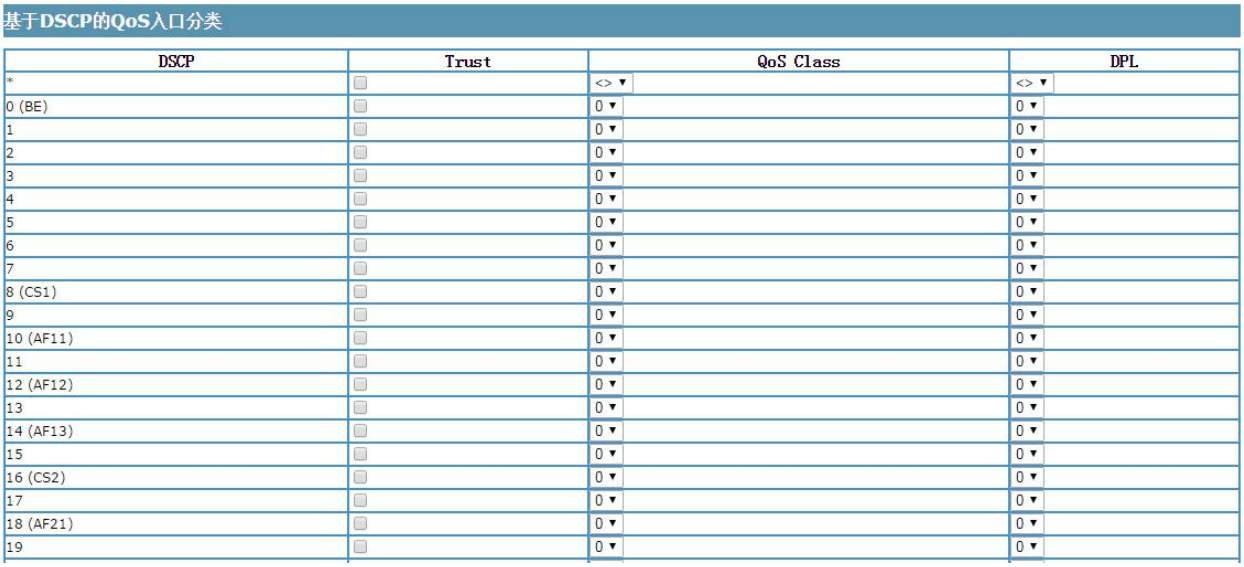
禁用：无出口重写。

启用：启用重写，而不重新映射。

重新映射 DP Unaware：重新映射来自分析器的 DSCP，并使用重新映射的 DSCP 值对帧进行映射。重映射的 DSCP 值始终取自“DSCP 转换 ->出口重映射 DP0”表。

重新映射 DP Aware：重新映射来自分析器的 DSCP，并使用重新映射的 DSCP 值对帧进行重新映射。根据帧的 DP 级别，重映射的 DSCP 值取自“DSCP 转换 ->出口重映射 DP0”表或“DSCP 转换 ->出口重映射 DP1”表。

6.13.8.2. DSCP 配置



基于DSCP的QoS入口分类

DSCP	Trust	QoS Class	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
10 (AF11)	☐	0	0
11	☐	0	0
12 (AF12)	☐	0	0
13	☐	0	0
14 (AF13)	☐	0	0
15	☐	0	0
16 (CS2)	☐	0	0
17	☐	0	0
18 (AF21)	☐	0	0
19	☐	0	0

此页面允许您为交换机所有配置基于 QoS DSCP 的 QoS 基本 QoS 入口分类设置。

DSCP

支持的最大 DSCP 值为 64。

Trust

控制特定 DSCP 值是否受 trust。 只有具有可信 DSCP 值的帧被映射到特定 QoS 类和丢弃优先级。 具有不可信 DSCP 值的帧被视为非 IP 帧。

QoS 类

QoS 类值可以是（0-7）

DPL

丢弃优先级（0-1）

6.13.8.3. DSCP 传输

DSCP 传输

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>		<>	<>
0 (BE)	0 (BE)		0 (BE)	0 (BE)
1	1		1	1
2	2		2	2
3	3		3	3
4	4		4	4
5	5		5	5
6	6		6	6
7	7		7	7
8 (CS1)	8 (CS1)		8 (CS1)	8 (CS1)
9	9		9	9
10 (AF11)	10 (AF11)		10 (AF11)	10 (AF11)
11	11		11	11
12 (AF12)	12 (AF12)		12 (AF12)	12 (AF12)
13	13		13	13
14 (AF13)	14 (AF13)		14 (AF13)	14 (AF13)
15	15		15	15
16 (CS2)	16 (CS2)		16 (CS2)	16 (CS2)
17	17		17	17
18 (AF21)	18 (AF21)		18 (AF21)	18 (AF21)

此页面允许您为交换机配置基本 QoS DSCP 转换设置。 DSCP 转换可以在入口或出口完成。

DSCP

支持的最大 DSCP 值为 64，有效 DSCP 值为 0～63。

入口

在使用 DSCP 用于 QoS 类和 DPL 映射之前，入口侧 DSCP 可以首先被转换为新的 DSCP。

DSCP 翻译有两个配置参数：

翻译：入口侧的 DSCP 可以转换为（0-63）DSCP 值中的任何一个。

分类：点击以在 Ingress 侧启用分类。

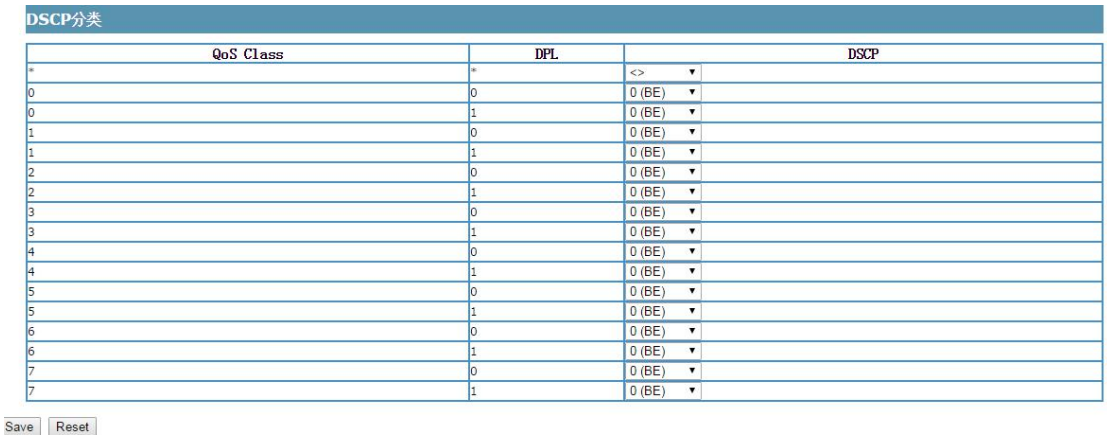
出口

出口侧有以下可配置参数：

重新映射 DP0 控制 DP 电平为 0 的帧的重映射：从要重新映射的选择菜单中选择 DSCP 值。 DSCP 取值范围为 0～63。

重新映射 DP1 控制 DP 电平为 1 的帧的重映射：从要重新映射的选择菜单中选择 DSCP 值。 DSCP 取值范围为 0～63。

6.13.8.4. DSCP 分类



此页面允许您配置 QoS 类别和丢弃优先级映射到 DSCP 值。

QoS 类

实际 QoS 类。

DPL

实际丢弃优先级。

DSCP

选择分类的 DSCP 值（0-63）。

6.13.9. 风暴控制

在此页面上配置交换机的风暴控制。

风暴控制有单播风暴速率控制，组播风暴速率控制和广播风暴速率控制。 这些仅影响泛洪帧，即具有（VLAN ID，DMAC）对的帧不存在于 MAC 地址表上。

这些配置指明跨交换机的未知单播，多播或广播流量的允许数据包速率。

帧类型

特定行中的设置适用于此处列出的帧类型：未知单播，多播或广播。

启用

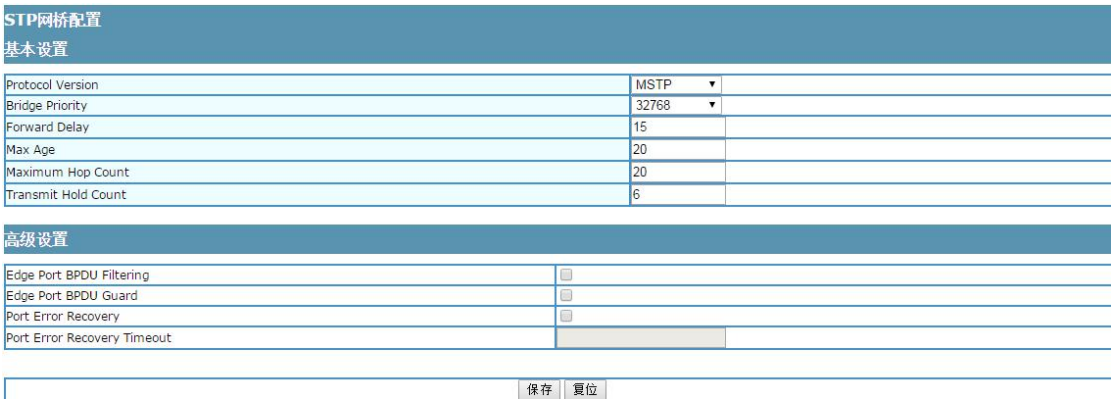
启用或禁用给定帧类型的风暴控制状态。

速率

速率单位是每秒数据包（pps）。 有效值是：1,2,4,8,16,32,64,128,256,512,1K，2K，4K，8K，16K，32K，64K，128K，256K，512K 或 1024K。

6.14. STP

6.14.1. 桥设置



此页面允许您配置 STP 系统设置。这些设置由交换机中的所有 STP 网桥实例使用。

6.14.1.1. 基本设置

协议版本

MSTP / RSTP / STP 协议版本设置。有效值为 STP，RSTP 和 MSTP。

桥接优先级

控制桥优先级。较低的数值具有较高的优先级。桥优先级加上 MSTI 实例编号，连接交换机的 6 字节 MAC 地址形成一个桥标识符。

对于 MSTP 操作，这是 CIST 的优先级。否则，这是 STP / RSTP 网桥的优先级。

转发延迟

STP 桥接器将根端口和指定端口传输到转发所使用的延迟（在 STP 兼容模式下使用）。有效值范围为 4 到 30 秒。

最大老化

当桥是根桥时，由桥传输的信息的最大年龄。有效值范围为 6 到 40 秒。

MaxAge 必须为<=（FwdDelay-1）* 2。

最大跳计数

这定义了在 MSTI 区域的边界处生成的 MSTI 信息的剩余 Hops 的初始值。它定义了根桥可以分配其 BPDU 信息的桥。有效值的范围为 6 到 40 跳。

发送保持计数

BPDU 的桥接端口的数量可以每秒发送。当超过时，下一个 BPDU 的传输将被延迟。有效值范围为 1 到 10 BPDU 每秒。

6.14.1.2. 高级设置

边缘端口 BPDU 过滤

控制明确配置为 Edge 的端口是否将传输和接收 BPDU。

边缘端口 BPDU 防护

控制是否显式配置为 Edge 的端口将在接收到 BPDU 时禁用自身。端口将进入错误禁用状态，并将从活动拓扑中移除。

端口错误恢复

控制是否在一定时间后自动启用处于错误禁用状态的端口。如果未启用恢复，则必须禁用端口，并重新启用正常的 STP 操作。该条件也会由系统重新启动清除。

端口错误恢复超时

可以启用处于错误禁止状态的端口之前经过的时间。有效值介于 30 到 86400 秒（24 小时）之间。

6.14.2. 多成树映射

此页面允许用户检查当前 STP MSTI 网桥实例优先级配置，并可能更改它们。

6.14.2.1. 配置标识

配置名称

标识 VLAN 到 MSTI 映射的名称。桥接必须共享名称和版本（见下文），以及 VLAN 到 MSTI 映射配置，以便共享 MSTI（区域内）的生成树。名称最多为 32 个字符。

配置修订

上面命名的 MSTI 配置的修订版本。它必须是介于 0 和 65535 之间的整数。

6.14.2.2. MSTI 映射

MSTI

桥接实例。 CIST 不可用于显式映射，因为它将接收未显式映射的 VLAN。

VLAN 映射

映射到 MSTI 的 VLAN 列表。 VLAN 可以作为单个（xx，xx 在 1 和 4094 之间）VLAN 或范围（xx-yy）给出，每个 VLAN 必须用逗号和/或空格分隔。 VLAN 只能映射到一个 MSTI。未使用的 MSTI 应该留空。 （即没有映射到它的任何 VLAN。）示例：2,5,20-40。

6.14.3. 多成树优先级

此页面允许用户检查当前 STP MSTI 网桥实例优先级配置，并可能更改它们。

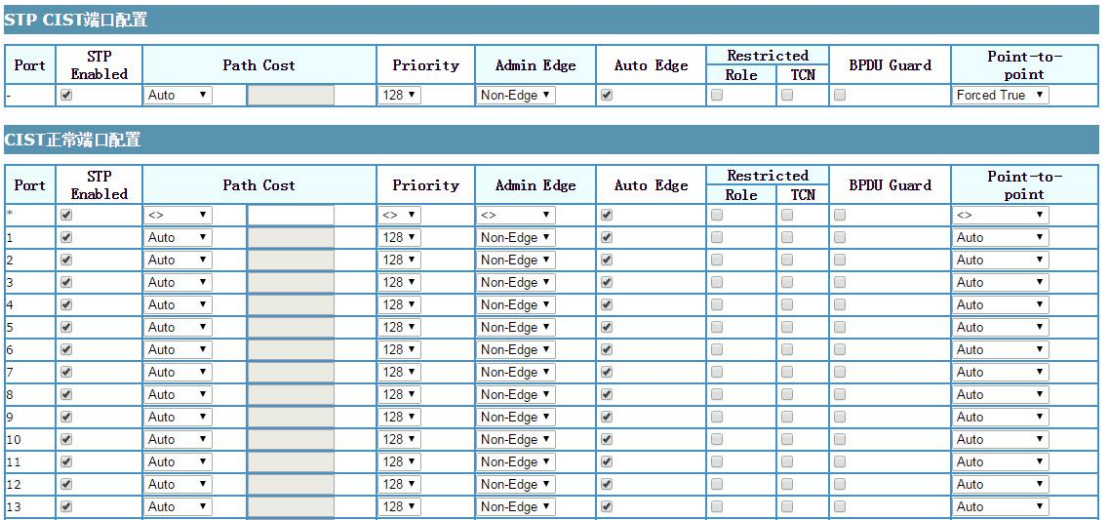
MSTI

桥接实例。 CIST 是默认实例，始终处于活动状态。

优先级

控制桥优先级。 较低的数值具有较高的优先级。 桥优先级加上 MSTI 实例编号，连接交换机的 6 字节 MAC 地址形成一个桥标识符。

6.14.4. STP CIST 端口配置



此页面允许用户检查当前 STP CIST 端口配置，并可能更改它们。

此页面包含物理端口和聚合端口的设置。

端口

逻辑 STP 端口的交换机端口号。

STP 使能

控制是否在此交换机端口上启用 STP。

路径成本

控制端口产生的路径开销。自动设置将根据物理链路速度（使用 802.1D 建议值）设置适当的路径开销。使用特定设置，可以输入用户定义的值。在建立网络的活动拓扑时使用路径成本。较低路径成本端口被选择为有利于较高路径成本端口的转发端口。有效值的范围为 1 到 200000000。

优先级

控制端口优先级。这可以用于控制具有相同端口成本的端口的优先级。

operEdge（状态标志）

描述端口是否直接连接到边缘设备的操作标志。 （无桥接）。转换到转发状态对于边缘端口（具有 operEdge 为真）比对于其他端口更快。此标志的值基于 AdminEdge 和 AutoEdge 字段。此标志在 Monitor - >生成树 - > STP 详细桥接状态中显示为边缘。

AdminEdge

控制 operEdge 标志是否应该以设置或清除开始。（端口初始化时的初始 operEdge 状态）。

AutoEdge

控制桥是否应在桥端口上启用自动边缘检测。这允许从是否在端口上接收到 BPDU 导出 operEdge。

受限角色

如果启用，导致端口不被选择为 CIST 或任何 MSTI 的根端口，即使它有最好的生成树优先级向量。在选择根端口后，将选择此类端口作为备用端口。如果设置，它可能导致生成树连接的缺乏。它可以由网络管理员设置，以防止网络的核心区域外部的网桥影响生成树活动拓扑，可能是因为这些网桥不受管理员的完全控制。此功能也称为 Root Guard。

受限 TCN

如果启用，则导致端口不将接收到的拓扑更改通知和拓扑更改传播到其他端口。如果设置，由于持续不正确的学习站位置信息，在生成树的活动拓扑中的变化之后可能导致临时的连接丢失。它由网络管理员设置以防止网络的核心区域外部的网桥，从而导致在该区域中的地址刷新，可能是因为这些网桥未处于管理员的完全控制下或者所连接的 LAN 的物理链路状态频繁地经过。

BPDU Guard

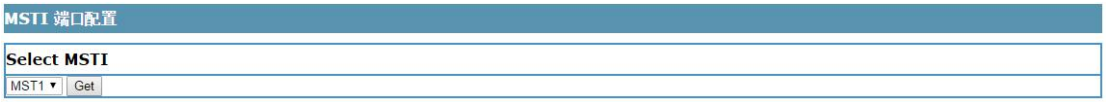
如果启用，则导致端口在接收到有效的 BPDU 时禁用自身。与类似的网桥设置相反，端口边缘状态不会影响此设置。

由于此设置，进入错误禁用状态的端口也受桥端口错误恢复设置的约束。

点对点

控制端口是否连接到点到点 LAN 而不是共享介质。这可以自动确定，或强制为真或假。转换到转发状态对于点到点 LAN 比对于共享介质更快。

6.14.5. MSTI 配置



此页面允许用户检查当前 STP MSTI 端口配置，并可以更改配置。

MSTI 端口是虚拟端口，为每个活动的 CIST（物理）端口单独实例化为配置并适用于该端口的每个 MSTI 实例。在显示实际 MSTI 端口配置选项之前，必须选择 MSTI 实例。

此页面包含物理端口和聚合端口的 MSTI 端口设置。

端口

对应的 STP CIST（和 MSTI）端口的交换机端口号。

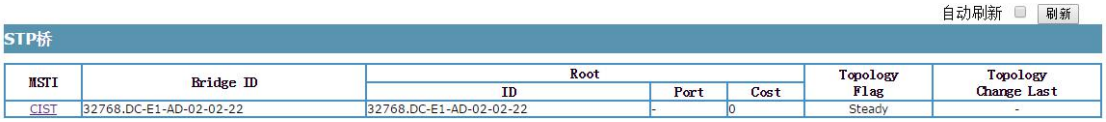
路径成本

控制端口产生的路径开销。自动设置将根据物理链路速度（使用 802.1D 建议值）设置适当的路径开销。使用特定设置，可以输入用户定义的值。在建立网络的活动拓扑时使用路径成本。较低路径成本端口被选择为有利于较高路径成本端口的转发端口。有效值的范围为 1 到 200000000。

优先级

控制端口优先级。这可以用于控制具有相同端口成本的端口的优先级。

6.14.6. STP 桥状态



此页面提供所有 STP 网桥实例的状态概述。

MSTI

桥接实例。 这也是指向 STP 详细网桥状态的链接。

桥 ID

此桥接实例的网桥 ID。

根 ID

当前选举的根桥的桥 ID。

根端口

交换机端口当前分配了根端口角色。

根成本

根路径成本。 对于根桥，它为零。 对于所有其他网桥，它是到根网桥的最低成本路径上的端口路径成本的总和。

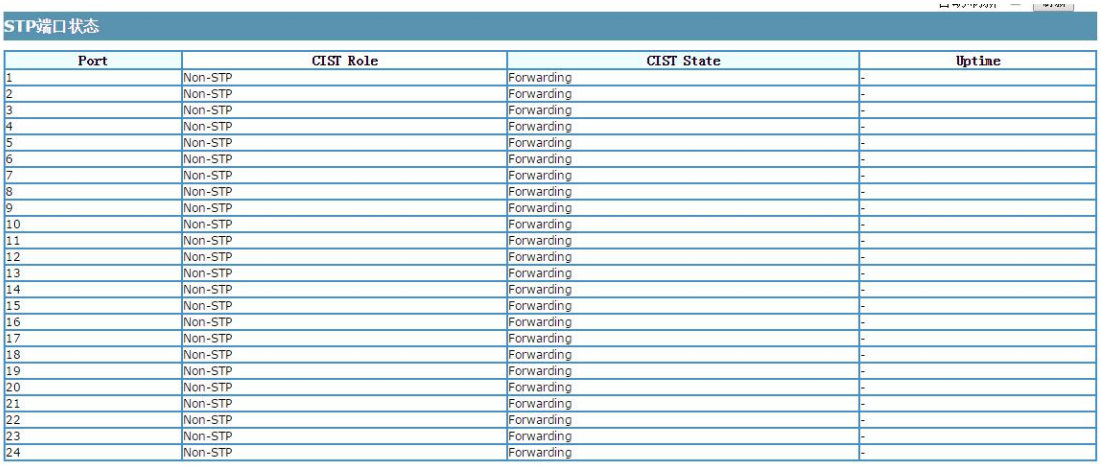
拓扑状态

此桥接实例的拓扑更改标志的当前状态。

拓扑更改最后

自上次拓扑更改发生以来的时间。

6.14.7. STP 端口状态



STP端口状态

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	Non-STP	Forwarding	-

此页面显示交换机物理端口的 STP CIST 端口状态。

端口

逻辑 STP 端口的交换机端口号。

CIST 角色

CIST 端口的当前 STP 端口角色。端口角色可以是以下值之一：Alternate Port，Backup Port，Root Port，Designated Port，已禁用。

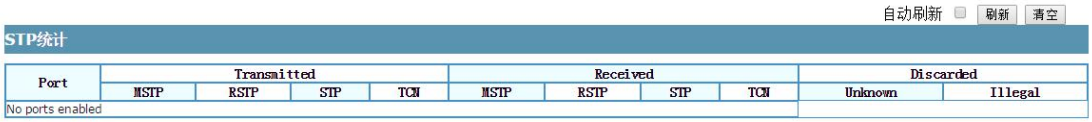
CIST 状态

CIST 端口的当前 STP 端口状态。 端口状态可以是以下值之一：丢弃学习转发。

正常运行时间

自上次初始化桥接端口以来的时间。

6.14.8. STP 统计



此页面显示交换机中网桥端口的 STP 端口统计信息计数器。

端口

逻辑 STP 端口的交换机端口号。

MSTP

在端口上收到/发送的 MSTP BPDU 的数量。

RSTP

在端口上接收/发送的 RSTP BPDU 的数量。

STP

在端口上接收/传输的传统 STP 配置 BPDU 的数量。

TCN

在端口上接收/传输的（传统）拓扑更改通知 BPDU 的数量。

丢弃未知

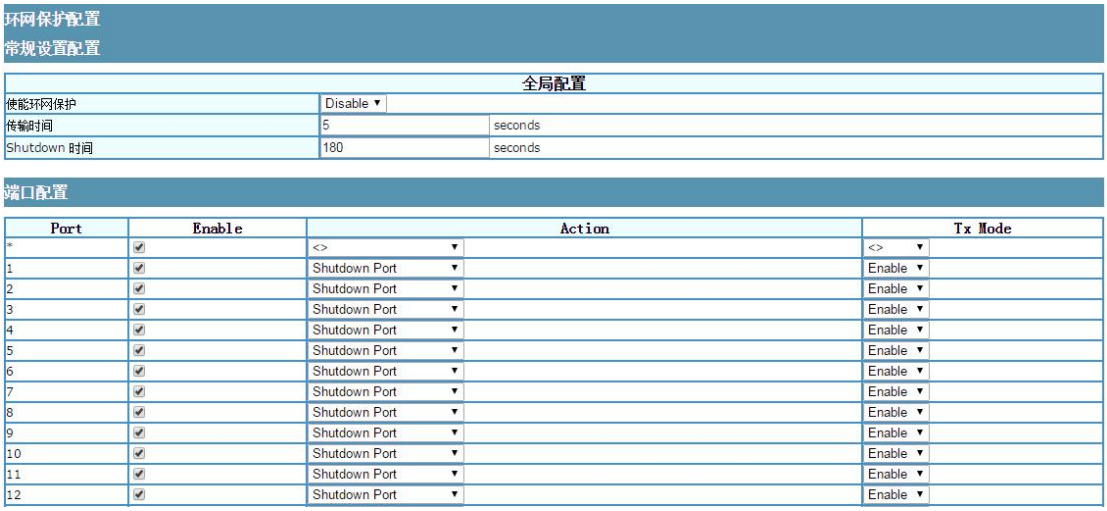
未知生成树 BPDU 在端口上接收（和丢弃）的数量。

丢弃非法

在端口上接收（和丢弃）的非法生成树 BPDU 的数量。

6.15. 环回保护

6.15.1. 环回保护配置


环网保护配置
常规设置配置

全局配置		
使能环网保护	Disable	
传输时间	5	seconds
Shutdown 时间	180	seconds

端口配置

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port	Enable
10	☑	Shutdown Port	Enable
11	☑	Shutdown Port	Enable
12	☑	Shutdown Port	Enable

此页面允许用户检查当前的环路保护配置，并可能更改它们。

6.15.1.1. 常规设置

启用环路保护

控制是否启用循环保护（作为一个整体）。

传输时间

每个端口上发送的每个环路保护 PDU 之间的间隔。有效值为 1 到 10 秒。

关机时间

检测到在循环的情况下端口将被保持禁用的周期(以秒为单位)(并且端口操作关闭端口)。有效值为 0 到 604800 秒（7 天）。值为零将保持端口禁用（直到下一次设备重新启动）。

6.15.1.2. 端口配置

端口

端口的交换机端口号。

使能

控制是否在此交换机端口上启用环路保护。

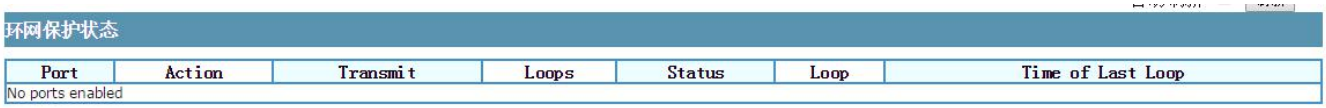
动作

配置在端口上检测到环路时执行的操作。有效值为关闭端口，关闭端口和日志或仅日志。

Tx 模式

控制端口是否主动生成环路保护 PDU，或者是否仅仅是被动寻找环路 PDU。

6.15.2. 环回保护状态



此页面显示交换机的端口的环路保护端口状态。

端口

逻辑端口的交换机端口号。

动作

当前配置的端口操作。

发送

当前配置的端口传输模式。

循环

此端口上检测到的环路数。

状态

端口的电流环路保护状态。

循环

当前是否在端口上检测到环路。

最后循环的时间

检测到最后一个循环事件的时间。

6.16. 链路聚合

6.16.1. 静态

聚合模式配置

堆栈全局设置

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☐
IP Address	☑
TCP/UDP Port Number	☑

聚合组配置

	Port Members																							
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
11	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

此页面用于配置聚合 hash 模式和聚合组。

源 MAC 地址

源 MAC 地址可用于计算帧的目标端口。选中以启用源 MAC 地址的使用，或取消选中以禁用。缺省情况下，源 MAC 地址使能。

目的 MAC 地址

目标 MAC 地址可用于计算帧的目标端口。选中以启用使用目标 MAC 地址，或取消选中以禁用。缺省情况下，目的 MAC 地址关闭。

IP 地址

IP 地址可用于计算帧的目标端口。选中以启用 IP 地址的使用，或取消选中以禁用。默认情况下，启用 IP 地址。

TCP / UDP 端口号

TCP / UDP 端口号可用于计算帧的目标端口。选中以启用使用 TCP / UDP 端口号，或取消选中以禁用。默认情况下，启用 TCP / UDP 端口号。

6.16.1.1. 聚合组配置

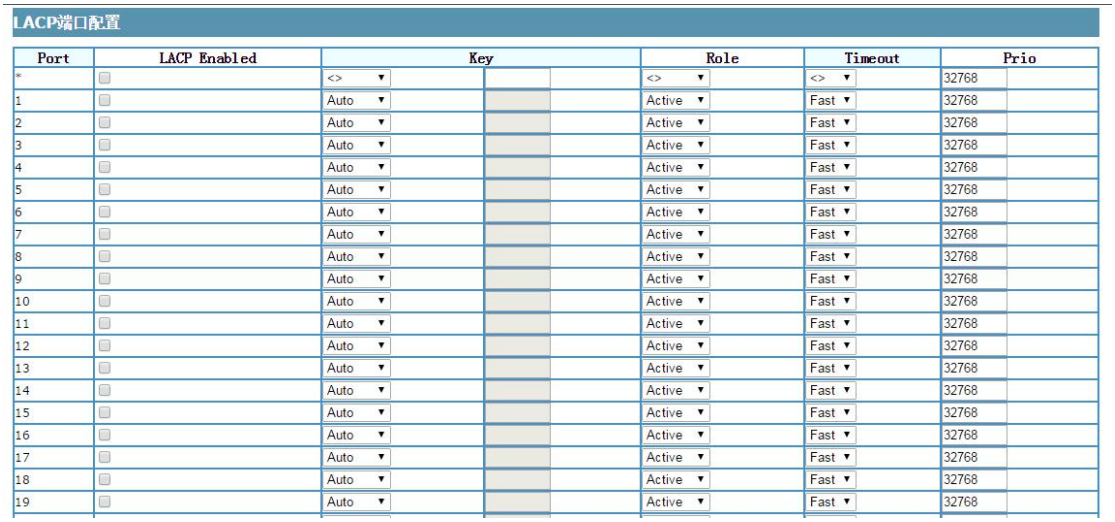
组 ID

表示包含在同一行中的设置的组 ID。组 ID“正常”表示没有聚合。每个端口只有一个组 ID 有效。

端口成员

每个组 ID 列出了每个交换机端口。选择单选按钮以在聚合中包括端口，或清除单选按钮以从聚合中删除端口。缺省情况下，没有端口属于任何聚合组。只有全双工端口可以加入聚合，并且每个组中的端口必须具有相同的速度。

6.16.2. LACP



此页面允许用户检查当前的 LACP 端口配置，并可以更改配置。

端口

交换机端口号。

LACP 使能

控制是否在此交换机端口上启用 LACP。当 2 个或更多端口连接到同一个设备时，LACP 将形成聚合。

Key

端口引发的 Key 值，范围为 1-65535。自动设置将根据物理链路速度（10Mb = 1,100Mb = 2，1Gb = 3）适当设置 Key。使用特定设置，可以输入用户定义的值。具有相同 Key 值的端口可以参与同一个聚合组，而具有不同 Key 的端口则不能。

角色

该角色显示 LACP 活动状态。 主动状态将每秒发送 LACP 数据包，而被动状态将等待来自合作伙伴的 LACP 数据包（如果说话）。

暂停

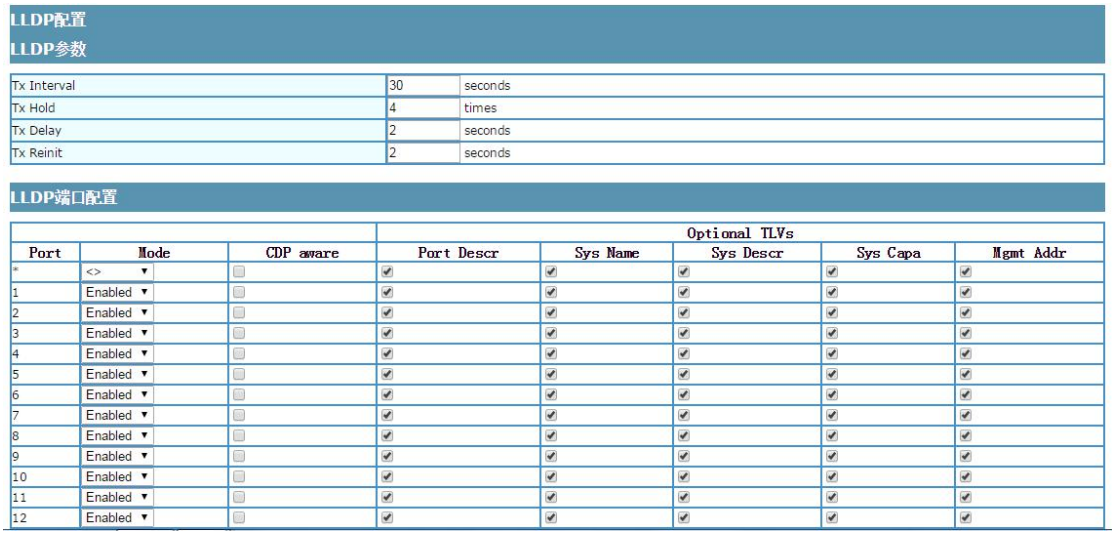
超时控制 BPDU 传输之间的时间间隔。 Fast 将每秒传输 LACP 数据包，而 Slow 将在发送 LACP 数据包之前等待 30 秒。

Prio

Prio 控制端口的优先级。如果 LACP 合作伙伴想要形成比此设备支持的更大的组，则此参数将控制哪些端口将处于活动状态，哪些端口将处于备份角色。较低的数字意味着更高的优先级。

6.17. LLDP

6.17.1. LLDP 配置



LLDP配置

LLDP参数

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP端口配置

			Optional TLVs				
Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>		☑	☑	☑	☑	☑
1	Enabled		☑	☑	☑	☑	☑
2	Enabled		☑	☑	☑	☑	☑
3	Enabled		☑	☑	☑	☑	☑
4	Enabled		☑	☑	☑	☑	☑
5	Enabled		☑	☑	☑	☑	☑
6	Enabled		☑	☑	☑	☑	☑
7	Enabled		☑	☑	☑	☑	☑
8	Enabled		☑	☑	☑	☑	☑
9	Enabled		☑	☑	☑	☑	☑
10	Enabled		☑	☑	☑	☑	☑
11	Enabled		☑	☑	☑	☑	☑
12	Enabled		☑	☑	☑	☑	☑

此页面允许用户检查和配置当前的 LLDP 端口设置。

6.17.1.1. LLDP 参数

Tx 间隔

交换机周期性地向其邻居发送 LLDP 帧，以使网络发现信息为最新的。每个 LLDP 帧之间的间隔由 Tx 间隔值确定。有效值限制为 5 - 32768 秒。

Tx 保持

每个 LLDP 帧包含关于 LLDP 帧中的信息应被视为有效时间的信息。LLDP 信息有效期设置为 Tx 保持乘以 Tx 间隔秒。有效值限制为 2 - 10 次。

Tx 延迟

如果一些配置被改变（例如 IP 地址），则发送新的 LLDP 帧，但是 LLDP 帧之间的时间将总是至少为 Tx 延迟秒的值。 Tx 延迟不能大于 Tx 间隔值的 1/4。有效值限制为 1 - 8192 秒。

Tx Reinit

当端口被禁用时，LLDP 被禁用或交换机重新启动，LLDP 关闭帧被传送到相邻单元，表明 LLDP 信息不再有效。 Tx Reinit 控制关闭帧和新的 LLDP 初始化之间的秒数。有效值限制为 1 - 10 秒。

6.17.1.2. LLDP 端口配置

端口

逻辑 LLDP 端口的交换机端口号。

模式

选择 LLDP 模式。

Rx only--交换机不发送 LLDP 信息，但是分析来自相邻单元的 LLDP 信息。

Tx only--交换机将丢弃从邻居收到的 LLDP 信息，但将发送 LLDP 信息。

禁用--交换机不会发送 LLDP 信息，并且将删除从邻居收到的 LLDP 信息。

Enabled--交换机将发送 LLDP 信息，并分析从邻居收到的 LLDP 信息。

CDP 关注

选择 CDP 关注。

CDP 操作被限制为解码输入的 CDP 帧（交换机不发送 CDP 帧）。仅当端口上的 LLDP 启用时，才会解码 CDP 帧。

只有可以映射到 LLDP 邻居表中的相应字段的 CDP TLV 被解码。所有其他 TLV 将被丢弃（无法识别的 CDP TLV 和丢弃的 CDP 帧未显示在 LLDP 统计信息中。CDP TLV 映射到 LLDP 邻居表，如下所示。

CDP TLV“设备 ID”映射到 LLDP“机箱 ID”字段。

CDP TLV“地址”映射到 LLDP“管理地址”字段。 CDP 地址 TLV 可以包含多个地址，但只有第一个地址显示在 LLDP 邻居表中。

CDP TLV“端口 ID”映射到 LLDP“端口 ID”字段。

CDP TLV“版本和平台”映射到 LLDP“系统描述”字段。

CDP 和 LLDP 都支持“系统功能”，但 CDP 功能包括不是 LLDP 的一部分的功能。这些能力在 LLDP 邻居表中显示为“其他”。

如果所有端口都禁用 CDP 关注，则交换机转发从邻居设备接收的 CDP 帧。如果至少一个端口启用了 CDP 关注，则交换机将终止所有 CDP 帧。

注意：当端口的 CDP 关注被禁用时，CDP 信息不会立即删除，而是在超过保持时间时删除。

端口描述

可选 TLV：选中时，“端口描述”包含在发送的 LLDP 信息中。

Sys 名称

可选 TLV：选中时，“系统名称”包含在发送的 LLDP 信息中。

系统描述

可选 TLV：选中时，“系统描述”包含在发送的 LLDP 信息中。

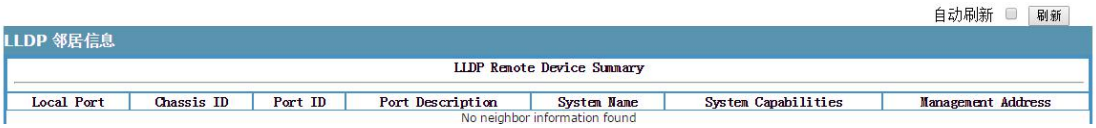
Sys Capa

可选 TLV：选中时，“系统能力”包含在发送的 LLDP 信息中。

地址

可选 TLV：选中时，“管理地址”包含在发送的 LLDP 信息中。

6.17.2. LLDP 邻居信息



本地端口

接收到 LLDP 帧的端口。

Chassis ID

Chassis ID 是邻居的 LLDP 帧的标识。

端口 ID

端口 ID 是邻居端口的标识。

端口描述

端口描述是邻居单元通告的端口描述。

系统名称

系统名称是相邻单元通告的名称。

系统能力

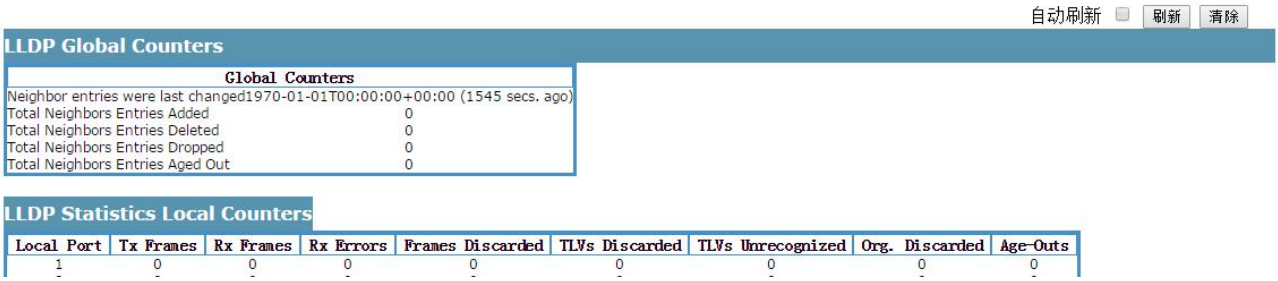
系统能力描述相邻单元的能力。 包括其他、中继器、Bridge、WLAN 接入点、路由器、电话、DOCSIS 电缆设备、Station only、保留

启用功能后，该功能后面紧跟（+）。 如果禁用该功能，则该功能后面为（ - ）。

管理地址

管理地址是相邻单元的地址，其用于较高层实体以辅助网络管理的发现。 这可以例如保持邻居的 IP 地址。

6.17.3. LLDP 端口统计



此页面提供所有 LLDP 流量的概述。

显示了两种类型的计数器。全局计数器是指整个交换机的计数器，而本地计数器是指当前所选交换机的每端口计数器。

6.17.3.1. 全局计数器

上次更改邻居条目

显示上次删除或添加最后一个条目的时间。它还显示自检测到上次更改以来经过的时间。

添加的邻居条目总数

显示自交换机重新启动以来添加的新条目的数量。

删除的邻居条目总数

显示自交换机重新启动以来删除的新条目数。

丢弃的邻居条目总数

显示由于条目表已满而丢弃的 LLDP 帧数。

过期的邻居条目总数

显示由于生存时间到期而删除的条目数。

6.17.3.2. 本地计数器

显示的表包含每个端口的一行。列包含以下信息：

本地端口

接收或传输 LLDP 帧的端口。

Tx 帧

端口上传输的 LLDP 帧数。

Rx 帧

端口上接收的 LLDP 帧数。

Rx 错误

接收的 LLDP 帧数包含某种错误。

帧丢弃

如果在端口上接收到 LLDP 帧，并且交换机的内部表已满，则 LLDP 帧将被计数并丢弃。这种情况在 LLDP 标准中称为“太多邻居”。当机箱 ID 或远程端口 ID 尚未包含在表中时，LLDP 帧需要表中的新条目。当给定端口的链路关闭，接收到 LLDP 关闭帧或者当条目老化时，从表中删除条目。

TLVs 丢弃

每个 LLDP 帧可以包含多条信息，称为 TLV（TLV 是“类型长度值”的缩写）。如果 TLV 格式错误，则计数并丢弃。

TLV 无法识别

形成良好的 TLV 的数量，但具有未知类型值。

Org. 丢弃

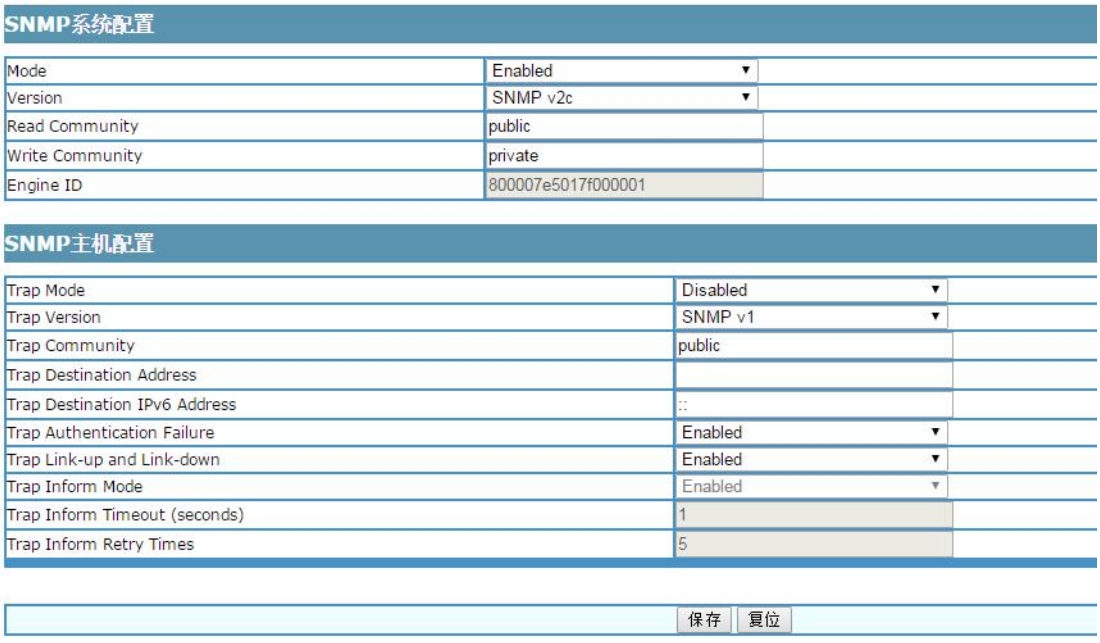
如果 LLDP 帧接收到组织 TLV，但不支持 TLV，则丢弃 TLV 并计数。

过期

每个 LLDP 帧包含关于 LLDP 信息有效的时间（老化时间）的信息。如果在老化时间内没有接收到新的 LLDP 帧，则去除 LLDP 信息，并且递增老化输出计数器。

6.18. SNMP

6.18.1. SNMP 系统



在此页面上配置 SNMP。

模式

表示 SNMP 模式操作。可以的模式有：

启用：启用 SNMP 模式操作。

禁用：禁用 SNMP 模式操作。

版本

表示 SNMP 支持的版本。可以的版本有：

SNMP v1：设置 SNMP 支持的版本 1。

SNMP v2c：设置 SNMP 支持的版本 2c。

SNMP v3：设置 SNMP 支持的版本 3。

读团体

表示允许访问 SNMP 代理的团体读访问字符串。允许的字符串长度为 0 到 255，允许的内容是 33 到 126 的 ASCII 字符。

该字段仅在 SNMP 版本为 SNMPv1 或 SNMPv2c 时适用。如果 SNMP 版本为 SNMPv3，则团体字符串将与 SNMPv3 社区表相关联。它提供了比 SNMPv1 或 SNMPv2c 团体字符串更多的配置安全名称的灵活性。除了团体字符串之外，可以使用特定范围的源地址来限制源子网。

写团体

表示允许访问 SNMP 代理的团体写访问字符串。允许的字符串长度为 0 到 255，允许的内容是 33 到 126 的 ASCII 字符。

该字段仅在 SNMP 版本为 SNMPv1 或 SNMPv2c 时适用。如果 SNMP 版本为 SNMPv3，则团体字符串将与 SNMPv3 社区表相关联。它提供了比 SNMPv1 或 SNMPv2c 团体字符串更多的配置安全名称的灵活性。除了团体字符串之外，可以使用特定范围的源地址来限制源子网。

引擎 ID

表示 SNMPv3 引擎 ID。该字符串必须包含一个偶数（十六进制格式），数字位数在 10 到 64 之间，但不允许全零和全'F'。更改引擎 ID 将清除所有原始本地用户。

6.18.2. SNMP 主机

在此页面上配置 SNMP trap。

6.18.2.1. 全局设置

在此页面上配置 SNMP trap。

模式

表示 trap 模式操作。可以的模式有：

启用：启用 SNMPtrap 模式操作。

禁用：禁用 SNMPtrap 模式操作。

6.18.2.2. trap 目标配置

在此页面上配置 trap 目标。

名称

表示 trap 配置的名称。表示 trap 目标的名称。

使能

表示 trap 目标模式操作：

启用：启用 SNMP trap 模式操作。

禁用：禁用 SNMP trap 模式操作。

版本

表示 SNMP trap 支持的版本：

SNMPv1：设置 SNMP trap 支持版本 1。

SNMPv2c：设置 SNMP trap 支持版本 2c。

SNMPv3：设置 SNMP trap 支持版本 3。

目的地址

表示 SNMP trap 目标地址。它允许使用点分十进制符号（'x.y.z.w'）的有效 IP 地址。

它还允许有效的主机名。有效主机名是从字母表（A-Za-z），数字（0-9），点（。），破折号（ - ）绘制的字符串。不允许使用空格，第一个字符必须是字母字符，第一个和最后一个字符不能是点或短划线。

表示 SNMPtrap 目的 IPv6 地址。 IPv6 地址是在 128 位记录中表示为八个字段，最多四个十六进制数字，每个字段（:)分隔一个冒号。例如，'fe80 :: 215：c5ff：fe03：4dc7'。符号“::”是一种特殊语法，可以用作表示多个 16 位连续零组的简写方式;但它只能出现一次。它还可以表示合法有效的 IPv4 地址。例如，':: 192.1.2.34'。

目的端口

表示 SNMPtrap 目标端口。 SNMP Agent 将通过此端口发送 SNMP 消息，端口范围为 1～65535。

6.18.3. SNMPv3 团体

在此页面上配置 SNMPv3 团体表。

团体

表示允许访问 SNMPv3 代理的社区访问字符串。 允许的字符串长度为 1 到 32，允许的内容为 33 到 126 之间的 ASCII 字符。团体字符串将被视为安全名称，并映射 SNMPv1 或 SNMPv2c 团体字符串。

源 IP

表示 SNMP 访问源地址。 当与源掩码组合时，可以使用特定范围的源地址来限制源子网。

源掩码

表示 SNMP 访问源地址掩码。

6.18.4. SNMPv3 用户

在此页面上配置 SNMPv3 用户表。

引擎 ID

标识此条目应属于的引擎 ID 的八位字节字符串。该字符串必须包含一个偶数（十六进制格式），数字位数在 10 到 64 之间，但不允许全零和全'F'。 SNMPv3 架构使用基于用户的安全模型（USM）用于消息安全性和基于视图的访问控制模型（VACM）用于访问控制。对于 USM 条目，usmUserEngineID 和 usmUserName 是条目的键。在简单的代理中，usmUserEngineID 总是代理自己的 snmpEngineID 值。该值还可以采用此用户可以与之通信的远程 SNMP 引擎的 snmpEngineID 的值。换句话说，如果用户引擎 ID 等于系统引擎 ID，则它是本地用户;否则为远程用户。

用户名

标识此条目应属于的用户名的字符串。允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

安全级别

指示此条目应属于的安全模型：

NoAuth，NoPriv：无身份验证和隐私。

Auth，NoPriv：验证，没有隐私。

Auth，Priv：身份验证和隐私。

如果条目已存在，则无法修改安全级别的值。这意味着必须首先确保值的设置正确。

认证协议

指示此条目应属于的认证协议：

无：无认证协议。

MD5：表示该用户使用 MD5 认证协议的可选标志。

SHA：用于指示此用户使用 SHA 认证协议的可选标志。

如果条目已存在，则无法修改安全级别的值。这意味着必须首先确保值设置正确。

验证密码

标识身份验证密码短语的字符串。对于 MD5 认证协议，允许的字符串长度为 8 到 32.对于 SHA 认证协议，允许的字符串长度为 8 到 40.允许的内容是从 33 到 126 的 ASCII 字符。

隐私协议

指示此条目应属于的隐私协议：

无：无隐私协议。

DES：用于指示此用户使用 DES 身份验证协议的可选标志。

AES：用于指示此用户使用 AES 身份验证协议的可选标志。

隐私密码

标识隐私密码短语的字符串。允许的字符串长度为 8 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

6.18.5. SNMPv3 群组

在此页面上配置 SNMPv3 群组表。

安全模型

指示此条目应属于的安全模型：

v1：保留用于 SNMPv1。

v2c：保留用于 SNMPv2c。

usm：基于用户的安全模型（USM）。

安全名称

标识此条目应属于的安全性名称的字符串。 允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

群组名

标识此条目应属于的组名称的字符串。 允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

6.18.6. SNMPv3 视图

在此页面上配置 SNMPv3 视图表。

视图名称

标识此条目应属于的视图名称的字符串。 允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

视图类型

指示此条目应属于的视图类型：

included：一个可选标志，指示应包括此视图子树。

excluded：用于指示应该排除此视图子树的可选标志。

一般来说，如果视图条目的视图类型是“excluded”，则应该存在另一个视图条目，其视图类型为“included”，并且它的 OID 子树应该超过“excluded”视图条目。

OID 子树

OID 定义要添加到命名视图的子树的根。 允许的 OID 长度为 1 到 128.允许的字符串内容是数字号或星号（*）。

6.18.7. SNMPv3 访问

在此页面上配置 SNMPv3 访问。

组名称

标识此条目应属于的组名称的字符串。允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

安全模型

指示此条目应属于的安全模型：

any：接受的任何安全模型（v1 | v2c | usm）。

v1：保留用于 SNMPv1。

v2c：保留用于 SNMPv2c。

usm：基于用户的安全模型（USM）。

安全级别

指示此条目应属于的安全模型：

NoAuth，NoPriv：无身份验证和隐私。

Auth，NoPriv：验证，没有隐私。

Auth，Priv：身份验证和隐私。

读视图名称

定义此请求可请求当前值的 MIB 对象的 MIB 视图的名称。允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

写视图名称

定义 MIB 请求的 MIB 视图的名称，此请求可能为其设置新值。允许的字符串长度为 1 到 32，允许的内容是从 33 到 126 的 ASCII 字符。

6.19. RMON 管理

6.19.1. 统计组配置

在此页面上配置 RMON 统计组。

ID

表示条目的索引。 取值范围为 1～65535。

数据源

表示要监视的端口 ID。 如果在堆叠交换机中，值必须添加 1000 *（交换机 ID-1），例如，如果端口是交换机 3 端口 5，则值为 2005。

6.19.2. 统计组查看

此页面提供 RMON 统计组概述。每个页面最多显示来自统计数据表中的 99 个条目，默认值为 20，通过“每页条目”输入字段选择。首次访问时，网页将显示统计组开头的前 20 个条目。第一个显示的将是统计组中找到的最低 ID 的那个。

“从控制索引索引”允许用户在统计组中选择起始点。单击刷新按钮将更新显示的表，或从下一个最接近的统计表匹配。

>>将使用当前显示条目的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。

ID

表示统计条目的索引。

数据源（ifIndex）

要监视的端口 ID。

丢弃

由于缺少资源，探测器丢弃数据包的事件总数。

Octets

在网络上接收的数据的八位字节总数（包括坏包中的数据）。

Pkts

接收的数据包总数（包括坏包，广播包和组播包）。

广播

接收到的传送到广播地址的好包的总数。

多播

接收的指向多播地址的好数据包的总数。

CRC 错误

接收的具有长度（不包括成帧比特，但包括 FCS 八位字节）在内的 64 和 1518 个八位字节之间，但是具有带有整数个八位字节的错误帧校验序列（FCS）（FCS 错误）的总分组数，或具有非整数个八位字节的错误 FCS（对准错误）。

Under-size

接收的数据包总数小于 64 个八位字节。

Over-size

接收的长于 1518 个八位字节的数据包总数。

Frag

大小小于 64 字节的帧数，接收到的 CRC 无效。

Jabb

大小大于 64 字节的帧数，接收到的 CRC 无效。

Coll

此以太网段上的冲突总数的最佳估计。

64

接收的长度为 64 个八位字节的分组（包括坏分组）的总数。

65～127

接收的长度在 65 到 127 个八位字节之间的分组（包括坏分组）的总数。

128～255

接收的长度在 128 到 255 个八位字节之间的分组（包括坏分组）的总数。

256～511

接收的长度在 256 到 511 个八位字节之间的分组（包括坏分组）的总数。

512～1023

接收的长度在 512 到 1023 个八位字节之间的分组（包括坏分组）的总数。

1024～1588

接收的长度在 1024 到 1588 个八位字节之间的分组（包括坏分组）的总数。

6.19.3. 历史组配置

在此页面上配置 RMON 历史组。

ID

表示条目的索引。 取值范围为 1～65535。

数据源

表示要监视的端口 ID。 如果在堆叠交换机中，值必须添加 1000 *（交换机 ID-1），例如，如果端口是交换机 3 端口 5，则值为 2005。

间隔

表示对历史统计数据进行采样的时间间隔（以秒为单位）。 取值范围为 1～3600，缺省值为 1800 秒。

Buckets

表示存储在 RMON 中的与此历史记录控制条目关联的最大数据条目。 取值范围为 1～3600，缺省值为 50。

Buckets Granted

数据的数量应保存在 RMON 中。

6.19.4. 历史组查看

此页面提供 RMON 历史组的概述。每个页面最多显示历史记录表中的 99 个条目，默认值为 20，通过“每页条目”输入字段选择。首次访问时，网页将显示历史组开头的前 20 个条目。第一个显示的将是历史组中找到的历史索引和样本索引最低的那个。

“从历史索引和样本索引开始”允许用户在历史记录表中选择起始点。单击刷新按钮将更新显示的表或从下一个最接近的历史表匹配。

>>将使用当前显示条目的最后一个条目作为下一次查找的基础。当到达结束时，在显示的表中显示文本“不再有条目”。使用| <<按钮重新开始。

历史索引

表示历史记录控制条目的索引。

样本索引

指示与控制条目关联的数据条目的索引。

样品开始

在此样本测量的间隔开始时的 sysUpTime 的值。

丢弃

由于缺少资源，探测器丢弃数据包的事件总数。

Octets

在网络上接收的数据的八位字节总数（包括坏包中的数据）。

Pkts

接收的数据包总数（包括坏包，广播包和组播包）。

广播

接收到的传送到广播地址的好包的总数。

组播

接收的指向多播地址的好数据包的总数。

CRC Errors

接收的具有长度（不包括成帧比特，但包括 FCS 八位字节）在内的 64 和 1518 个八位字节之间，但是具有带有整数个八位字节的错误帧校验序列（FCS）（FCS 错误）的总分组数，或具有非整数个八位字节的错误 FCS（对准错误）。

Undersize

接收的数据包总数小于 64 个八位字节。

Oversize

接收的长于 1518 个八位字节的数据包总数。

Frag

大小小于 64 字节的帧数，接收到的 CRC 无效。

Jabb

大小大于 64 字节的帧数，接收到的 CRC 无效。

Coll

此以太网段上的冲突总数的最佳估计。

利用率

在此采样间隔期间此接口上平均物理层网络利用率的最佳估计。

6.19.5. 告警组配置

RMON 告警配置

在此页面上配置 RMON 报警表。

删除

选中以删除条目。它将在下次保存时被删除。

ID

表示条目的索引。取值范围为 1～65535。

间隔

表示采样和比较上升和下降阈值的间隔（以秒为单位）。范围从 1 到 2 ^ 31-1。

变量

表示要采样的特定变量。

InOctets：接口上接收的八位位组的总数，包括成帧字符。

InUcastPkts：传递到更高层协议的单播数据包的数量。

InNUcastPkts：传送到更高层协议的广播和多播包数。

InDiscards：即使数据包正常也丢弃的入站数据包的数量。

InErrors：包含错误的入站数据包的数量，阻止它们传递到更高层协议。

InUnknownProtos：由于未知或不支持协议而丢弃的入站数据包的数量。

- ✓ OutOctets：从接口传输的八位字节数，包括成帧字符。
- ✓ OutUcastPkts：请求传输的单播数据包的数量。
- ✓ OutNUcastPkts：请求传输的广播和多播数据包的数量。
- ✓ OutDiscards：丢弃的出站数据包数量正常的事件数。
- ✓ OutErrors：由于出错而无法传输的出站数据包数。
- ✓ OutQLen：输出包队列的长度（以包为单位）。

样品类型

对所选变量进行采样并计算要与阈值进行比较的值的方法，可能的样本类型是：

绝对：直接获取样品。

Delta：计算样本之间的差异（默认）。

值

上一个采样周期内的统计值。

启动报警

对所选变量进行采样并计算要与阈值进行比较的值的方法，可能的样本类型是：

RisingTrigger 报警时，第一个值大于上升阈值。

FallingTrigger 报警当第一个值小于下降阈值。

当第一个值大于上升阈值或小于下降阈值（默认）时，RisingOrFallingTrigger 报警。

上升阈值

上升阈值（-2147483648-2147483647）。

上升指数

上升事件指数（1-65535）。

下降阈值

下降阈值（-2147483648-2147483647）

下降指数

下降事件指数（1-65535）。

6.19.6. 告警组查看

ID

表示告警控制项的索引。

间隔

表示采样和比较上升和下降阈值的间隔（以秒为单位）。

变量

指示要采样的特定变量

样品类型

对所选变量进行采样并计算要与阈值进行比较的值的方法。

值

上一个采样周期内的统计值。

启动报警

当此条目首次设置为有效时可能发送的警报。

上升阈值

上升阈值。

上升指数

上升事件指数。

下降阈值

下降阈值。

下降指数

下降事件指数。

6.19.7. 事件组配置

在此页面上配置 RMON 事件表。

删除

选中以删除条目。 它将在下次保存时被删除。

ID

表示条目的索引。 取值范围为 1～65535。

描述

表示此事件，字符串长度为 0 到 127，默认为空字符串。

类型

表示事件的通知，

- ✓ none：不创建 SNMP 日志，不发送 SNMP Trap。
- ✓ log：触发事件时创建 SNMP 日志条目。
- ✓ snmptrap：触发事件时发送 SNMP Trap。
- ✓ logandtrap：创建 SNMP 日志条目并在触发事件时发送 SNMP Trap。

团体

指定发送 Trap 时的团体，字符串长度为 0 到 127，默认为“public”。

事件上次时间

指示此事件条目上次生成事件时 sysUpTime 的值。

6.19.8. 事件组查看

事件索引

表示事件条目的索引。

日志索引

表示日志条目的索引。

日志时间

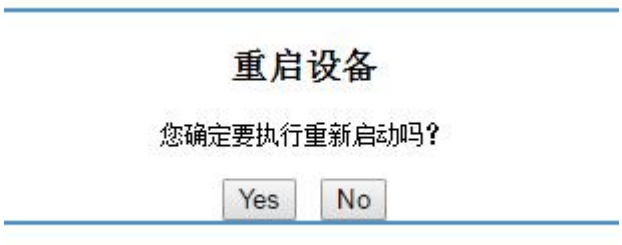
指示事件日志时间。

日志描述

表示事件描述。

第七章 系统工具

7.1. 系统重启



可以在此页面上重新启动交换机。 重启后，交换机将正常启动。

7.2. 保存配置

交换机将其配置存储在 CLI 格式的多个文本文件中。 这些文件是虚拟的（基于 RAM）或存储在交换机的闪存中。

有三个系统文件：

running-config：表示交换机上当前活动配置的虚拟文件。 此文件是易失的。

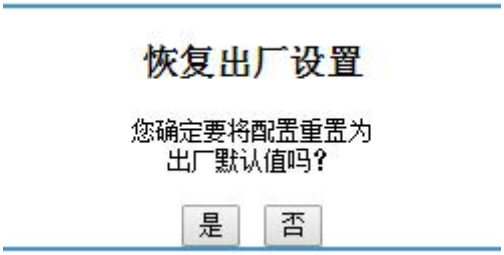
startup-config：交换机的启动配置，在引导时读取。

default-config：具有供应商特定配置的只读文件。当系统恢复为默认设置时读取此文件。也可以存储多达两个其他文件并将其应用于 running-config，从而切换配置。

保存 startup-config

这将 running-config 复制到 startup-config，从而确保当前活动的配置将在下次重新启动时使用。

7.3. 出厂设置



可以在此页面上重置交换机的配置。仅保留 IP 配置。

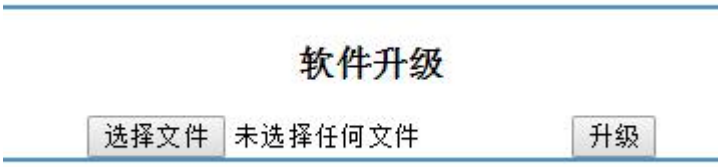
新配置可立即使用，这意味着不需要重新启动。

是：单击将配置重置为出厂默认值。

否：单击以返回“端口状态”页面，而不重置配置。

注意：恢复出厂默认值也可以通过在交换机重新启动后的第一分钟内在端口 1 和端口 2 之间进行物理回环来执行。 在引导后的第一分钟，“环回”数据包将在端口 1 发送。如果在端口 2 接收到“环回”数据包，交换机将执行恢复到默认。

7.4. 软件升级



此页面便于软件升级

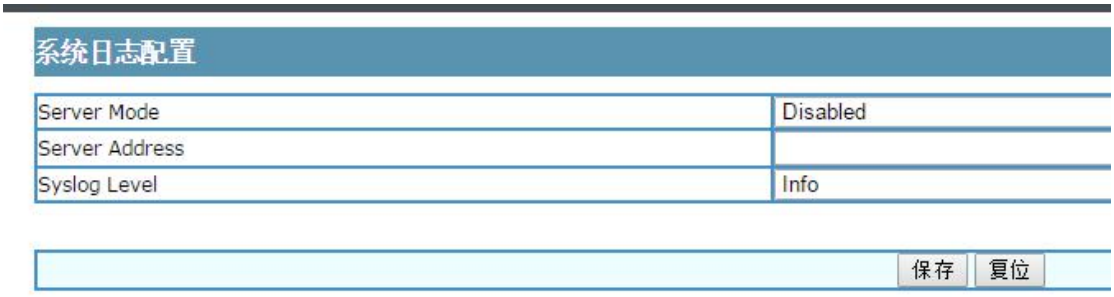
点击选择文件按钮到软件升级文件的位置，然后单击升级。

在上传软件升级文件之后，页面通知开始软件升级。 大约几分钟后，软件升级并且交换机重新启动。

警告：在软件升级时，Web 访问已停用。 软件升级正在进行时，LED 以 10 Hz 的频率闪烁绿色/熄灭。 此时不要重新启动或关闭设备，否则开关可能无法正常工作。

第八章 系统监控

8.1. 系统日志



在此页面上配置系统日志。

服务器模式

表示服务器模式操作。 当启用模式操作时，syslog 消息将发送到 syslog 服务器。 syslog 协议基于 UDP 通信，并在 UDP 端口 514 上接收，并且 syslog 服务器不会向发送方发送确认，因为 UDP 是无连接协议，并且不提供确认。 即使 syslog 服务器不存在，syslog 包也将始终发送。

启用：启用服务器模式操作。

- ✓ 禁用：禁用服务器模式操作。

服务器地址

表示 syslog 服务器的 IPv4 主机地址。 如果交换机提供 DNS 功能，它也可以是主机名。

系统日志级别

指示将发送到 syslog 服务器的消息类型。

信息：发送信息，警告和错误。

警告：发送警告和错误。

错误：发送错误。