RS608 千百兆系列
工业以太网交换机

WEB 说明书

深圳市源拓光电技术有限公司

Shenzhen Wintop Optical Technology Co., Ltd.

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 RS608 千百兆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 RS608 千百兆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

序号	说明书版本号	修　改　摘　要	初始软件版本号	修改日期
10				
9				
8				
7				
6				
5				
4				
3				
2	V1.1	修正本文中的错误描述	V1.0	2016/04
1	V1.0	RS608 千百兆系列	V1.0.0	2015/12

*　技术支持：电话（0755）26641737

*　　传真（0755）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

第 1 章 产品介绍

1.1. 概述

RS608 千百兆系列工业以太网交换机是一款 L2 层线速以太网交换产品，是为要求具备高性能、较大端口密度且易于安装的网络环境而设计的智能型可网管交换机。本文档描述 RS608 千百兆系列工业以太网交换机工业以太网交换机的产品特性、安装说明和命令行操作。详细的机型配置表如下：

机型配置表

型号	千兆光口（SFP）	百兆光口（1*9）	百兆电口（RJ45）	外壳
RS608-2GF6T	2	-	6	铝壳

1.2. 功能特性

表 1- 1 RS608 千百兆系列工业以太网交换机功能特性

模块	特性描述
CLI 命令行	同一时刻支持 1 个用户登录。
远程管理	同一时刻支持 5 个用户登录，支持 SSH 登录(端口 8022)方式。
WEB 管理	同一时刻不限制访问用户的数量，支持 http、https 两种访问方式。
用户管理	最多 8 个用户名，支持 admin、user 分级权限管理。
IP 地址管理	支持一个静态 IP 地址。
DHCP 客户端	可以自动获取 IP 地址。
DNS 客户端	设备可以网络解析域名。
IGMP Snooping	256 个多播地址表项。
VLAN	支持 VLAN ID 的范围 1- 4094，交换机最多可配置 64 个 VLAN。
MAC	MAC 地址深度为 8K，支持单播、多播地址转发表静态手工配置。
Mirror	1 个目的端口，其它端口可以仅接收、仅发送、接收发送双向、关闭四个选项的源端口。
QoS	支持 802.1p、DSCP 和 ToS 优先级。
RSTP/STP	支持 8 个物理端口+5 个汇聚端口。
MSTP	支持 8 个物理端口，支持 63 个生成树实例
ACL	支持 255 个基于 vlan，mac 的访问控制
SNMP	支持 V1/V2c/V3，支持 WT2000 综合网络管理。
TRUNK	最大支持 5 个静态汇聚组。

LACP	最大支持 4 个动态汇聚组。
LLDP	8 个邻居设备发现。
SNTP	支持网络获取时间。
系统日志	5000 条内置日志。
环网	环网自愈时间小于 50ms
RMON	支持统计、历史、告警、事件四组。
广播风暴抑制	支持分等级的广播风暴抑制。
软件升级	支持 TFTP 升级方式。
配置文件	支持上传、下载配置文件。
恢复出厂	支持恢复出厂设置。
复位设备	支持软件重启，断电复位。
PING	支持。
TRACERT	支持。

1.3. 系统特性

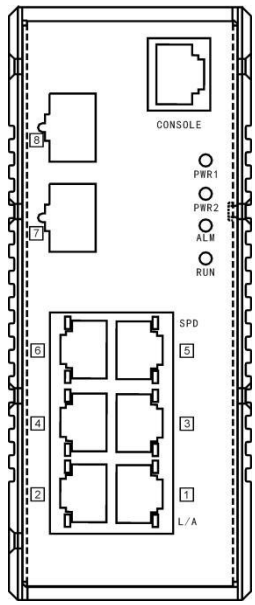
表 1- 2 RS608 千百兆系列工业以太网交换机系统特性

项目	RS608 千百兆系列
外形尺寸(长×宽×高) (单位：mm)	135mm*129mm*55mm
外壳	铝壳
管理端口	1 个 console 口
电源系统	支持双电源输入 电压范围：DC9-60V/AC110-240V
整机最大功耗	10W
工作环境温度	-40℃～85℃
工作环境相对湿度	5%～95%（无凝露）
防护等级	IP40
静电放电抗扰度	GB/T 17626.2　4B
电快速瞬变脉冲群抗扰度	GB/T 17626.4　4B
浪涌（冲击）抗扰度	GB/T 17626.5　4B
射频场感应的传导骚扰抗扰度	GB/T 17626.6　3A
工频磁场抗扰度	GB/T 17626.8　5A

阻尼振荡波抗扰度	GB/T 17626.12　　3B
交流电源暂时中断抗扰度	GB/T 17626.11　　A

1.4. 面板说明

1.4.1. 前面板



RS608-2GF6T

图 1. 1 RS608 千百兆系列工业以太网交换机前面板示意图

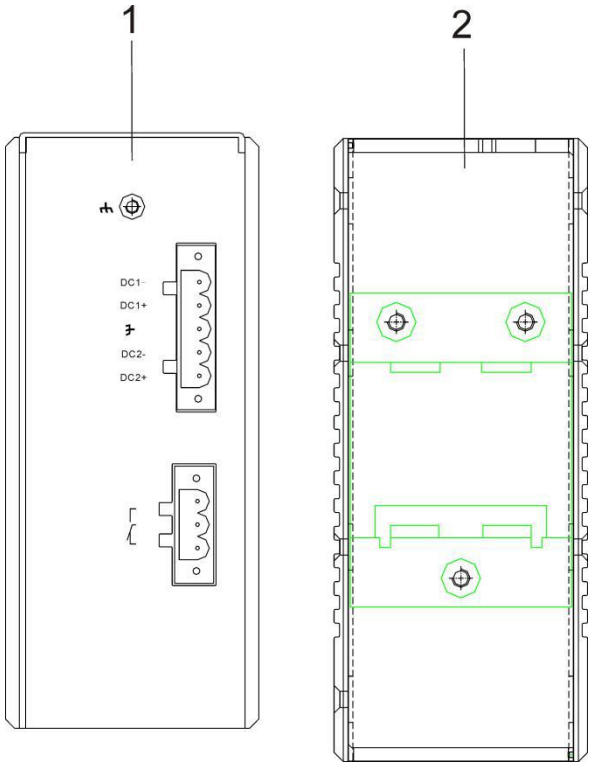
说明、提示：

对于前面板指示灯的具体说明，请参见“1.5 前面板指示灯介绍”。

1.4.2. 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



1.5. 电源系统

RS608 千百兆系列工业以太网交换机支持双电源输入。

电压范围：DC9-60V/ AC110-240V

1.6. 前面板指示灯介绍

指示灯	面板标示	状态	说明
电源指示灯	PWR	亮	交换机正常上电
		灭	交换机未上电
Link/Act 指示灯	L/A	亮	端口连接正确
		灭	端口无连接或连接错误
		闪烁	端口有流量通过
SPD 指示灯	SPD	亮	端口 100Mbps 状态

		灭	端口 10Mbps 状态
告警指示灯	ALM	灭	交换机工作正常
		亮	交换机有告警输出
运行指示灯	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

1.7. 物料清单

1. 交换机一台
2. 安装附件
3. U 盘一个，包含用户手册
4. 产品保修卡一张
5. 合格证一张

⚠ **注意：**打开产品包装纸盒后，若发现缺少以上某种配件，请及时与经销商联系。

第 2 章 产品安装

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：
- 请不要将交换机放在不稳定的箱子或桌子上，万一跌落，可能会对交换机造成严损害。
- 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，建议接地。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。
- 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。
- 确认机柜及工作台足够牢固，能够支撑交换机及其安装附件的重量。
- 在放置交换机时，请避开多尘及电磁干扰强的地区。

2.2. 安装方式

2.2.1. 导轨式安装

第一步，安装导轨：

将导轨固定在机架上，如图 2-1 所示：

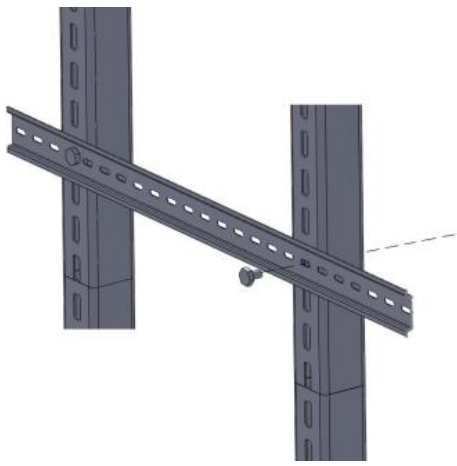


图 2. 1 安装导轨

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：

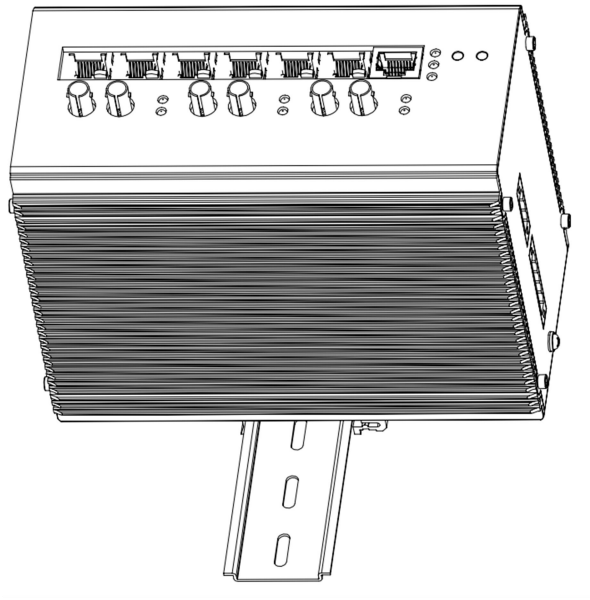


图 2.2 安装交换机

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。

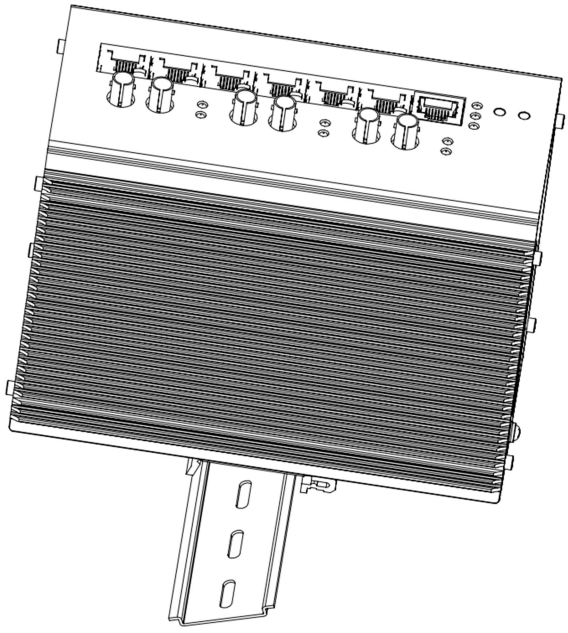


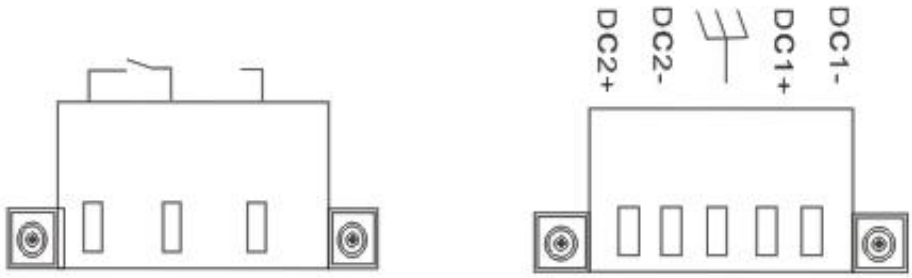
图 2.3 拆除交换机

2.3. 电源供电

2.3.1. 电源输入结构图

RS608 千百兆系列工业以太网交换机的电源输入范围：DC9-60V/ AC110-240V 。

RS608 千百兆系列工业以太网交换机的侧面板集成有电源输入端子、告警继电器输出端子。其结构如图 2-4 所示。



(1): 继电报警接口（FAIL SAFE） (2):电源接口

图 2. 4 电源输入结构图

2.3.2. 电源输入端子

RS608 千百兆系列工业以太网交换机交（直）流电源输入功能，输入电源为 DC9-60V/AC110-240V。使用该端子输入。建议使用 1.5mm2 以上的标准电源线。

接线顺序如图 2.4 所示。接线及安装步骤如下：

将电源线剥去 5mm 长的外皮，将露出的多股铜丝拧成一束；用一字螺丝刀将“电源线锁紧螺钉”松开，将电源线插入端子尾部的孔内，拧紧“电源线锁紧螺钉”；

将电源端子插入设备直流电源插座内，用一字螺丝刀拧紧两颗“端子锁紧螺钉”，使端子与电源连接器连接牢固。

2.3.3. 告警继电器输出端子

用于端口断开告警输出，交换机所有端口连接正常时，告警继电器常开端闭合，常闭端断开。当某端口断开连接时，常开端断开，常闭端闭合。继电器的常开点和常闭点通过绿色 3 芯 5.08mm 间距端子输出。

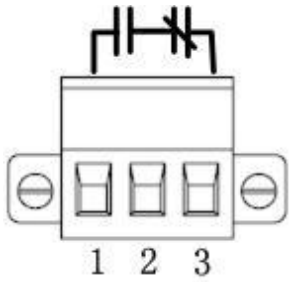


图 2. 5 告警端子

说明、提示：

在交换机正常通电的情况下，第 1 脚和第 2 脚为常闭开关，第 2 脚和第 3 脚为常开开关。当设备双电源上电时，第 1、2 脚短路，第 2、3 脚断开；任一路电源掉电后第 1、2 脚断开，第 2、3 脚短路。

2.3.4. RS232 控制端口（Console）

RS608 千百兆系列工业以太网交换机的网管口为一带屏蔽的 RS232 连接器，接口通信标准为 3 线 RS232，用户可以使用一端为母 RS232 接口另一端为 RJ45 接口的串口线，将交换机的 Console 与 PC 的 9 针串口相连。在控制计算机上运行超级终端，通过 CLI 命令对交换机进行配置，交换机的 Console 口与 PC 的 9 针串口接线顺序如下：

RJ -45		DB9
1	————	8
2	————	6
3	————	2
4	————	5
5	————	5
6	————	3
7	————	4
8	————	7

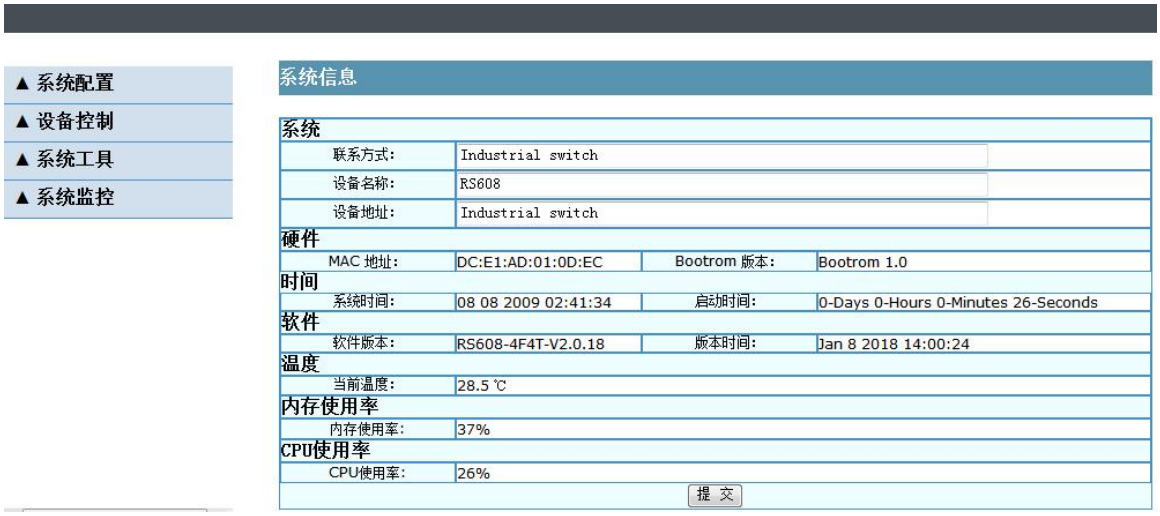
2.3.5. 接地

RS608 千百兆系列工业以太网交换机接地柱，将接地线的一端与冷压端子压接后用接地螺丝固定在机壳的接地柱处。接地线的另一端可靠地接入大地。建议接地线使用截面不小于 2.5mm2 的标准线。

第 3 章 系统设置

3.1. 系统信息

点击导航栏“系统设置→系统信息”，即可进入系统信息配置界面，如下图：



3.1.1. 系统

此部分内容用于设置设备名称和联系方式等。

配置项	说明
交换机联系方式	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）。
系统名	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。
系统位置	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）。

3.1.2. 硬件

此部分内容用于显示设备的 MAC 地址和当前的 bootrom 版本。

3.1.3. 时间

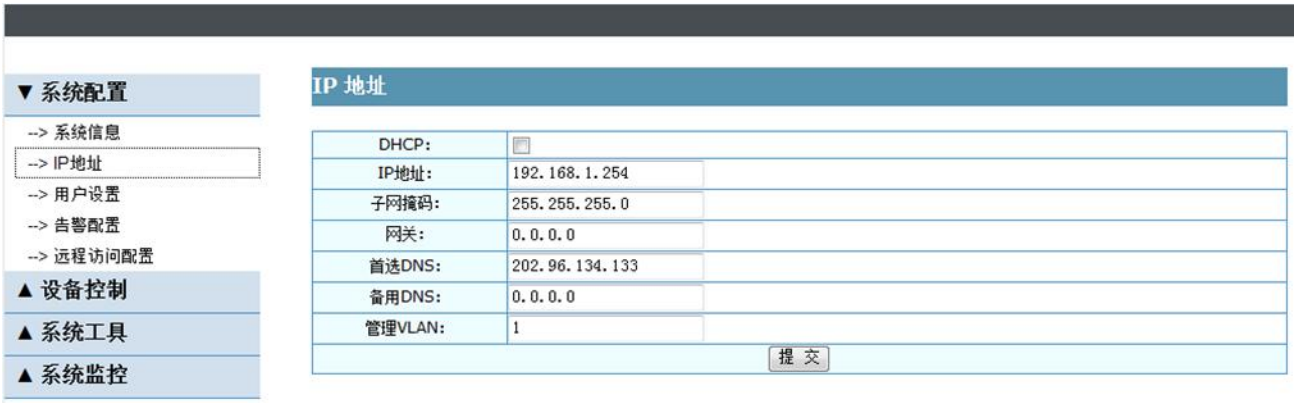
此部分内容用于显示当前的系统时间和设备启动时间。

3.1.4. 软件

此部分内容用于显示当前软件的版本和发布时间。

3.2. IP 地址

点击导航栏“系统设置→IP 地址”，即可进入 IP 地址配置界面，如下图：



IP 地址界面中修改各项参数的解释如下表所示：

配置项	说明
DHCP	选择单选框表示启用 DHCP 功能，不选表示禁用 DHCP 功能。启用 DHCP 后，交换机将从网络中的 DHCP Server 获得 IP 地址，若网络中不存在 DHCP Server，或有其它原因导致 IP 地址获取失败，则无法使用 IP 地址访问交换机。
IP 地址	用于设置和显示系统当前的 IP 地址，默认为 192.168.1.254。
子网掩码	用于设置和显示系统当前的子网掩码，默认为 255.255.255.0。
网关	用于设置和显示系统的网关地址，默认为 0.0.0.0。
首选 DNS	用于设置和显示系统的首选 DNS，默认为 202.96.134.133。
备用 DNS	用于设置和显示系统的备用 DNS，默认为 0.0.0.0。
管理 VLAN	用于设置和显示系统的管理 VLAN，默认为 1。

3.3. 用户设置

点击导航栏“系统设置→用户设置”，即可进入用户设置界面，如下图：

用户设置界面中修改各项参数的解释如下表所示：

配置项	说明
用户名	用于显示访问系统的用户名。
权限	用于显示系统用户的管理权限，分为管理员权限—Administrator，普通用户权限—User。
编辑/删除	用于修改用户密码和删除用户。 此操作请注意以下几条限制： 1) 修改密码设置只能用于当前用户。 2) 删除只能是具有管理员权限的用户才可以操作。 3) 系统默认的 admin 和 guest 用户不能删除，只能修改密码。

3.3.1. 添加用户

用于添加系统的管理用户，并分配相应的管理权限，只有管理员才可以添加用户。点击系统配置---> 用户设置 进入用户设置界面，点击添加用户按钮，如下图所示

添加用户界面中修改各项参数的解释如下表所示：

配置项	说明
用户名	用于设置管理用户的用户名。用户名由数字、字母和下划线组成，字符串长度为 1~16bytes。
密码	用于设置管理用户的密码。密码由 0~16 bytes 的 NVT ASCII

	字符(32-126)组成。
确认密码	用于确认用户的密码设置，以防输入错误造成设置的密码不可知。
权限	用于设置系统用户的管理权限，分为管理员权限—Administrator；普通用户权限—User。

3.4. 告警配置

点击导航栏“系统设置→告警配置”，即可进入告警设置界面，如下图：

告警配置界面中修改各项参数的解释如下表所示：

配置项	说明
电源告警	用于开启电源告警功能。当有某一路电源断电时，对应告警信息就会有信息显示，同时设备前面板告警灯会亮，设备上面板继电器长闭端断开，长开端闭合。此功能默认打开。
端口告警	用于检测端口 LinkDown 信息，当某个端口 down 时，就会有对应的告警信息， 同时设备前面板告警灯会亮，设备上面板继电器长闭端断开，长开端闭合。此功能默认关闭。

第 4 章 登录方式

4.1. 通过 Web 登录

由于工业以太网交换机提供WEB的管理方式，所以可以通过手动配置计算机的IP地址登录到交换机。交换机的默认参数如下表所示：

参数	默认值
默认 IP 地址	192.168.1.254
默认用户名	admin（管理用户）/guest（普通用户）

默认密码	admin（管理用户）/guest（普通用户）

在默认情况下，手动配置 IP 地址登录到交换机的管理界面步骤如下：

1. 用网线的一端连接交换机，一端连接计算机网卡；
2. 接通交换机的电源；
3. 手动设置计算机的 IP 地址属于 192.168.1.xxx 网段，如： 192.168.1.10（xxx 为 1～253）；
4. 打开浏览器，在地址栏输入 http://192.168.1.254 并回车，会出现交换机的登录页面，如下图所示：
5. 输入用户名和密码（管理用户 admin/admin；普通用户 guest/guest；）即可进入

第 5 章 设备控制

5.1. 端口

5.1.1. 端口设置

点击导航栏“设备控制→端口→端口设置”，即可进入端口设置界面，如下图：

端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
端口	表示交换机的逻辑端口号
描述	用于设置和显示端口的描述信息
状态	用于设置和显示端口的启用/禁用状态，所有端口默认为启用状态。
连接状态	用于显示端口的连接/断开状态。
类型	用于显示端口的光口/电口类型。
模式	当前模式：用于显示端口当前的速率和双工状态。 配置模式：用于设置和显示端口当前的速率/双工配置状态，配置的模式分为：100M 全双工、100M 半双工、自适应、10M 全双工、10M 半双工。
流控	用于配置和显示端口流量控制功能的启用/禁用状态，默认为禁用状态。
丢弃	用于配置和显示端口的丢弃模式状态，默认为 None 状态，分为以下 4 种模式： None：表示端口不丢弃任何数据帧。 All：表示端口丢弃任何数据帧。 Untag：表示端口丢弃所有 untag 数据帧。 Tag：表示端口丢弃所有 tag 数据帧

5.1.2. 端口统计

点击导航栏“设备控制→端口→端口统计”，即可进入端口统计界面，如下图：

端口统计界面中修改各项参数的解释如下表所示：

配置项	说明
选择	选择某端口，可以是物理端口或者是虚端口。rx 代表从该端口进入的数据包，tx 代表从该端口离开的数据包；
Octets	接收到的数据的字节数（包括出错包的数据字节）。
UnicastPkts	接收到的数据包的单播数据包。
rxBroadcastPkts	接收到的正常的广播数据包。
rxMulticastPkts	接收到的正常的多播数据包。
rxCRCAlignErrors	接收到的合适大小（64~1518 字节之间）但有 CRC 错误或对齐错误（不是整数字节）的数据包数量。
rxUndersizePkts	接收到的格式正确但小于 64 个字节的数据包数量。
rxOversizePkts	接收到的格式正确但大于 1518 个字节的数据包数量。
rxFragments	接收到的小于 64 字节且带有 CRC 错误或对齐错误（不是整数字节）的数据包数量。
rxJabbers	接收到的大于 1518 字节且带有 CRC 错误或对齐错误（不是整数字节）的数据包数量。
rx64	接收到的长度为 64 字节的数据包（包括出错包）数量。
rx65to127	接收到的长度在 65~127 字节之间的数据包（包括出错包）数量。
rx128to255	接收到的长度在 128~255 字节之间的数据包（包括出错包）数量。
rx256to511	接收到的长度在 256~511 字节之间的数据包（包括出错包）数量。
rx512to1023	接收到的长度在 512~1023 字节之间的数据包(包括出错包)数量。
rx1024to1518	接收到的长度在 1024~1518 字节之间的数据包（包括出错包）数量。
rx1519toMax	接收到的长度大于 1519 字节的数据包（包括出错包）数量。
ifInErrors：	进入该端口的错误数据的总数。

5.2. 虚拟局域网

5.2.1. 概述

VLAN（Virtual Local Area Network，虚拟局域网），是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

5.2.2. 划分策略

根据划分方式的不同，可以将 VLAN 分为不同类型，常用的几种划分方式如下：

1. 基于端口的 VLAN

基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法，这实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不管交换端口连接什么设备。

5.2.3. VLAN 的成员配置

点击导航栏“设备控制→VLAN→VLAN 成员”，即可进入 VLAN 成员设置界面，如下图：

VLAN 成员配置界面中修改各项参数的解释如下表所示：

配置项	说明
VLAN ID	表示交换机中 VLAN 组的编号。
Vlan 描述	表示该 Vlan 的描述信息。
U	表示该端口是 VLAN 的成员，而且是该 VLAN 的 untag 端口。
T	表示该端口是 VLAN 的成员，而且是该 VLAN 的 tag 端口。
提交	用于提交当前页面的配置信息。
选择	用于选择某 VLAN 进行成员端口的编辑。

删除	用于删除某 VLAN 组，Vlan 1 不能删除。

5.2.4. VLAN 的端口配置

点击导航栏“设备控制→VLAN→端口配置”，即可进入 VLAN 成员设置界面，如下图：

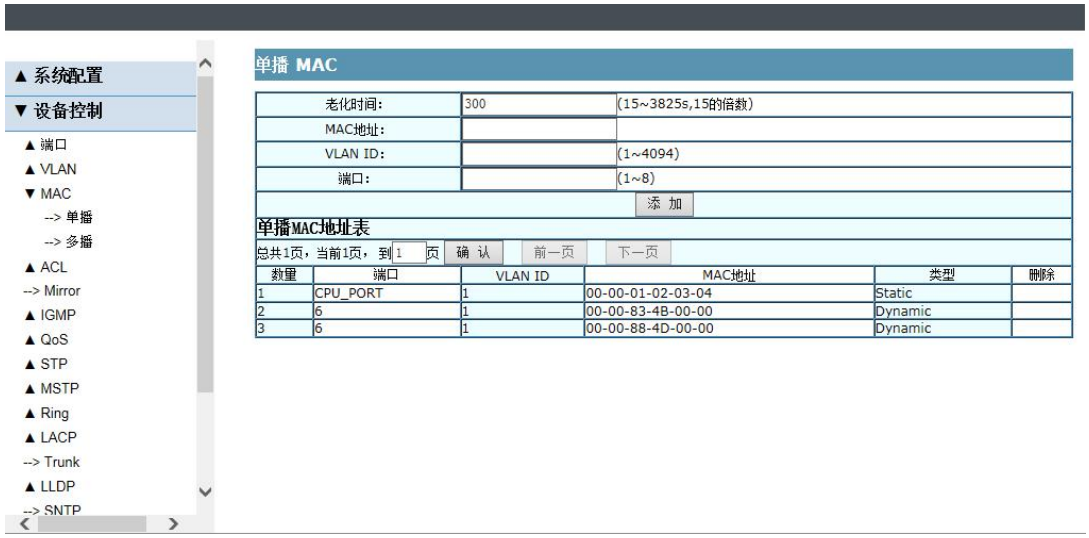
VLAN 端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
端口	交换机的逻辑端口号。
PVID	端口的 VLAN 标示，取值范围为：1~4094。
优先级	用于设置端口的 802.1p 优先级，若该端口是某 VLAN 的成员，那么进入该端口的 untag 数据帧都会打上 tag 标记，且 tag 标记中的 802.1p 优先级的值就是该端口设置的值。
提交	用于提交当前页面的配置信息。

5.3. MAC

5.3.1. 单播

点击导航栏“设备控制→MAC→单播”，即可进入单播 MAC 地址设置界面，如下图：

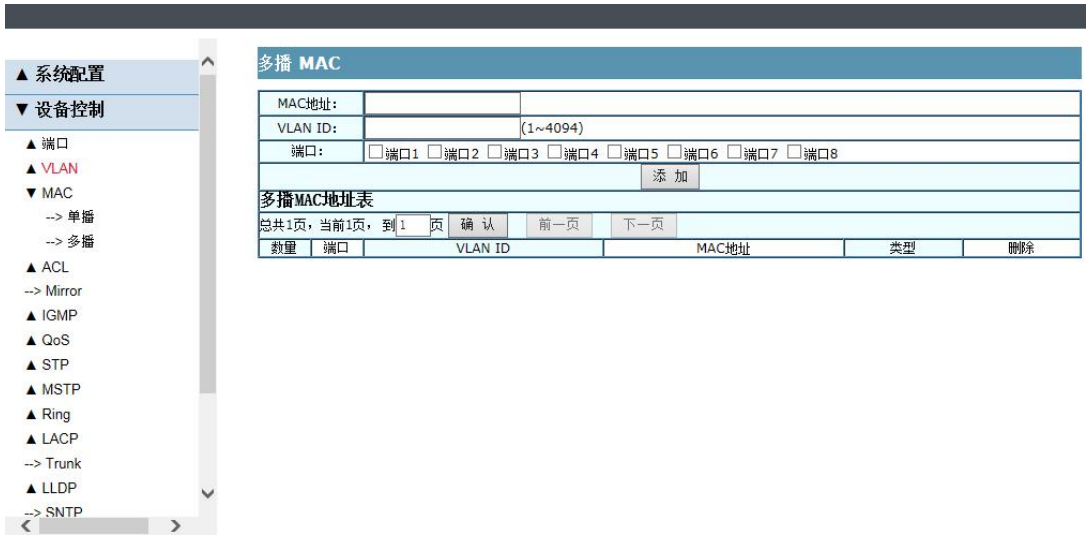


单播 MAC 界面中修改各项参数的解释如下表所示：

配置项	说明
老化时间	动态 MAC 地址条目在 MAC 地址表中的老化时间，默认为 300s。
MAC 地址	用于添加的静态 MAC 地址。
VLAN ID	MAC 地址对应的 VLAN ID。
端口	MAC 地址对应的端口号。
数量	MAC 地址的个数编号。
类型	MAC 地址在 MAC 地址表中的类型，分为动态和静态两种。
删除	用于删除 MAC 地址表中的静态 MAC 地址。

5.3.2. 多播

点击导航栏“设备控制→MAC→多播”，即可进入多播 MAC 地址设置界面，如下图：



多播 MAC 界面中修改各项参数的解释如下表所示：

配置项	说明
MAC 地址	用于添加的静态多播 MAC 地址。

VLAN ID	多播 MAC 地址对应的 VLAN ID。
端口	多播 MAC 地址对应的端口号。
数量	多播 MAC 地址的个数编号。
添加	用于提交本界面的配置信息。
删除	用于删除 MAC 地址表中的静态 MAC 地址。

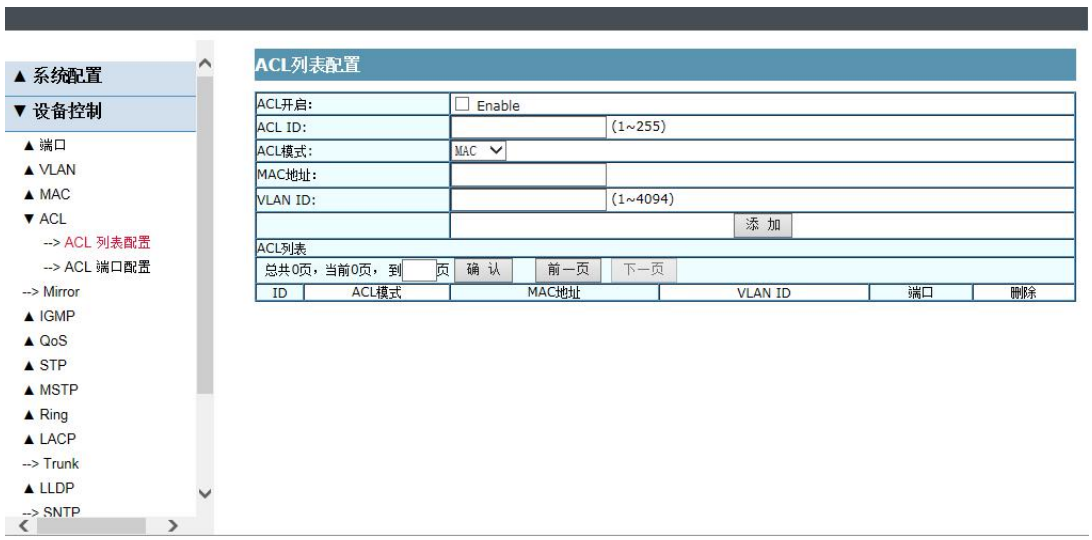
5.4. ACL

5.4.1. 概述

访问控制列表简称为 ACL，访问控制列表使用包过滤技术，在交换机上读取包头中的信息如源地址，目的地址，源端口，目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。

5.4.2. ACL 列表配置

点击导航栏“设备控制→ACL→ACL 列表配置”，即可进入 ACL 列表配置设置界面，如下图：



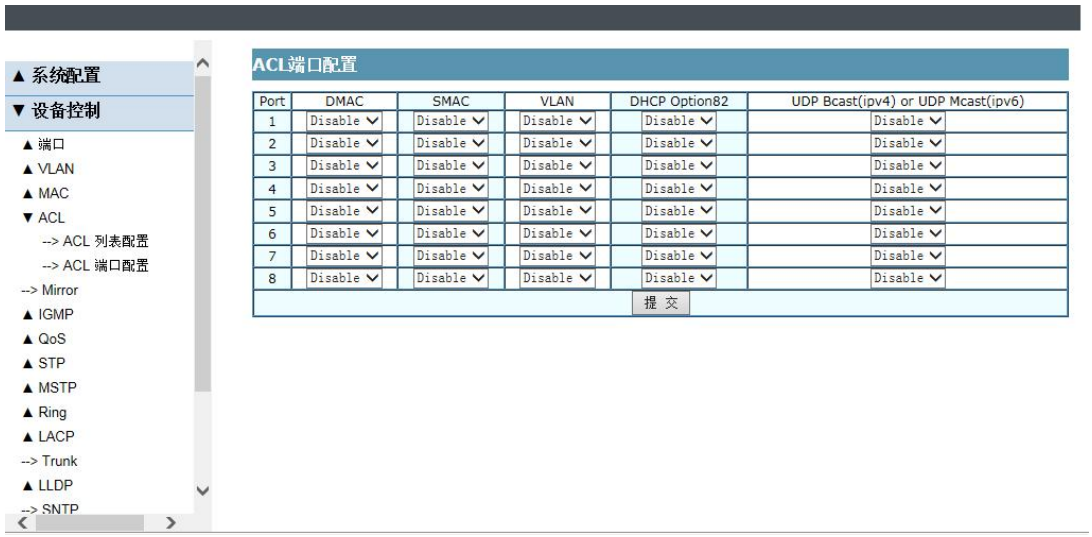
ACL 列表配置界面中修改各项参数的解释如下表所示：

配置项	说明
ACL 开启	用于启用或禁用 ACL。
ACL ID	ACL 编号,取值范围为：1~255。
ACL 模式	对应 ACL 的模式，MAC 或 Vlan。
MAC 地址	ACL 模式为 MAC 时的 MAC 地址。
Vlan ID	该 ACL 对应的 Vlan ID, 取值范围为：1~4094
端口	用于显示端口配置里 DMAC 和 SMAC 的配置情况。
删除	用于删除 ACL 列表配置中的 ACL 项目。

5.4.3. ACL 端口配置

在端口配置页面可以设置各种过滤规则，Deny 表示不允许该类型数据包通过，Permit 表示该类型数据包通过，Disable 表示不过滤该类型数据包（和 Permit 效果一样）。默认为 Disable，即允许类型数据通过。

点击导航栏“设备控制→ACL→ACL 端口配置”，即可进入 ACL 端口配置设置界面，如下图：



ACL 端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
端口	表示交换机的逻辑端口号。
DMAC	设置是否根据数据包的 DMAC 信息来过滤数据包。
SMAC	设置是否根据数据包的 SMAC 信息来过滤数据包。
VLAN	设置是否根据数据包的 VLAN 信息来过滤数据包。
DHCP Option82	设置是否根据数据包的 DHCP Option82 信息来过滤数据包。
UDP Bcast(ipv4) or UDP Mcast(ipv6)	设置是否根据数据包的 UDP Bcast(ipv4) or UDP Mcast(ipv6)信息来过滤数据包。

5.5. Mirror

5.5.1. 4.5.1 简介

镜像是将指定端口的报文复制到镜像端口，镜像端口会接入数据检测设备，用户利用数据检测设备分析镜像端口接收到的报文，进行网络监控和故障排除。镜像如图 4-1 所示：

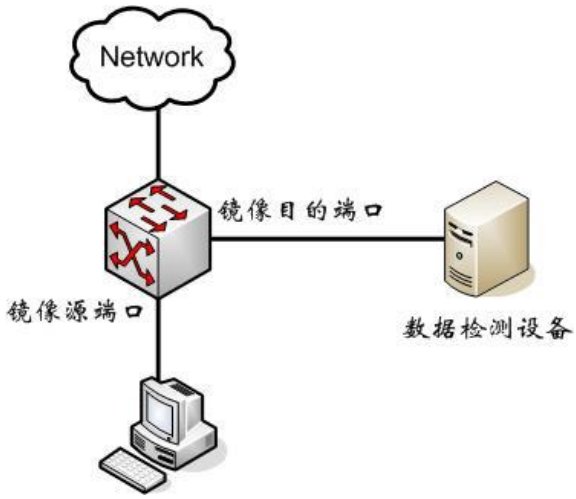
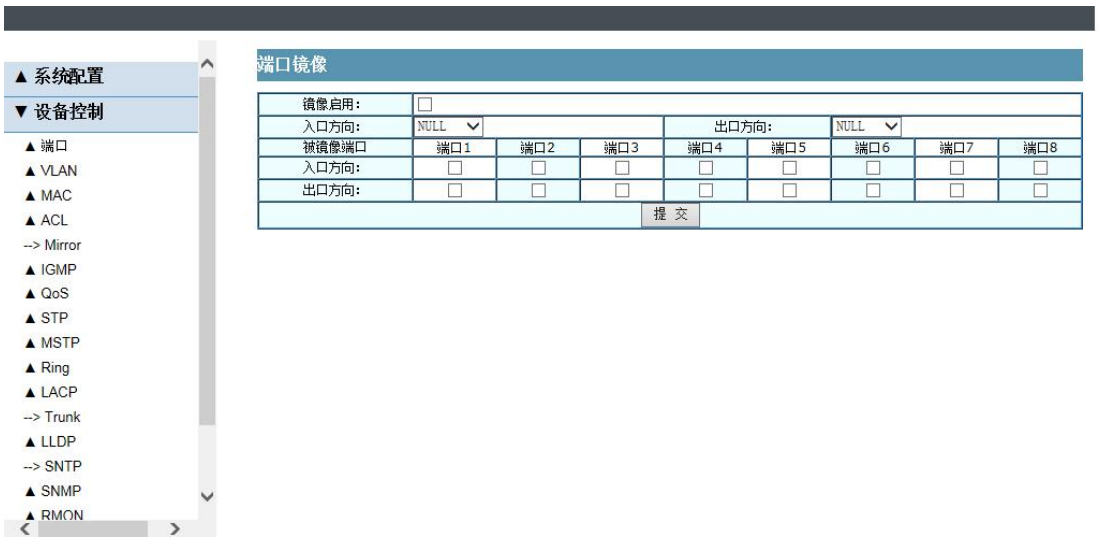


图 5. 1 镜像示意图

5.5.2. 配置说明

点击导航栏“设备控制→Mirror”，即可进入 Mirror 设置界面，如下图：



端口镜像界面中修改各项参数的解释如下表所示：

配置项	说明
镜像启用	用于启用系统的端口镜像功能。
入口镜像端口	用于监控的那个端口，被镜像端口的数据都会被复制到此端口。
出口镜像端口	用于监控的那个端口，被镜像端口的数据都会被复制到此端口。
被镜像端口	被监控的端口。
入口方向	表示监控入口方向的数据。
出口方向	表示监控出口方向的数据。
提交	用于提交当前页面的配置信息。

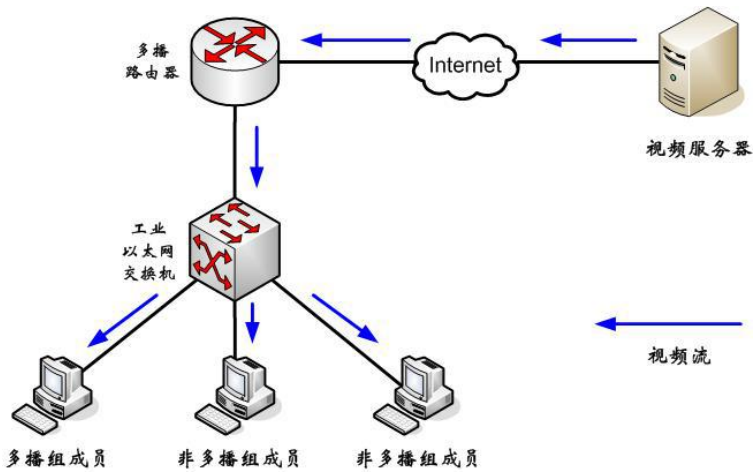
5.6. IGMP

5.6.1. IGMP 原理

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP 侦听）是运行在二层以太网交换机上的组播约束机制，用于管理和控制组播组。

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据包。当二层设备没有运行 IGMP Snooping 时，组播数据包在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据包不会在二层被广播，而在二层被组播给指定的接收者，但是未知组播数据包仍然会在二层广播。

没有启用 IGMP 功能图：



运行 IGMP Snooping 后,报文将不再在二层广播，而是进行二层组播。如图所示：

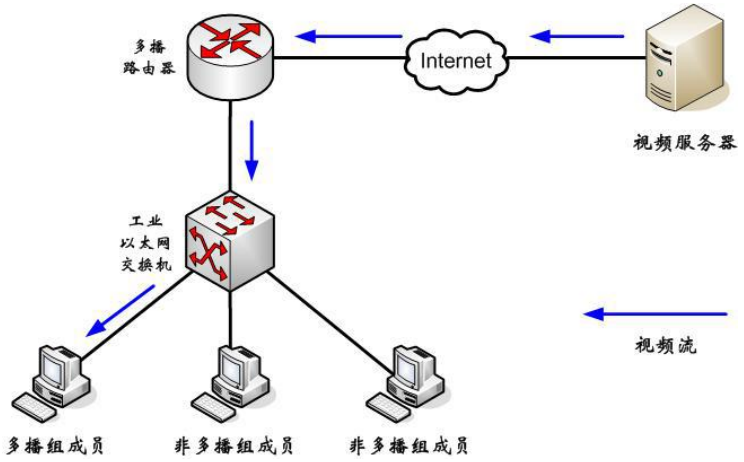
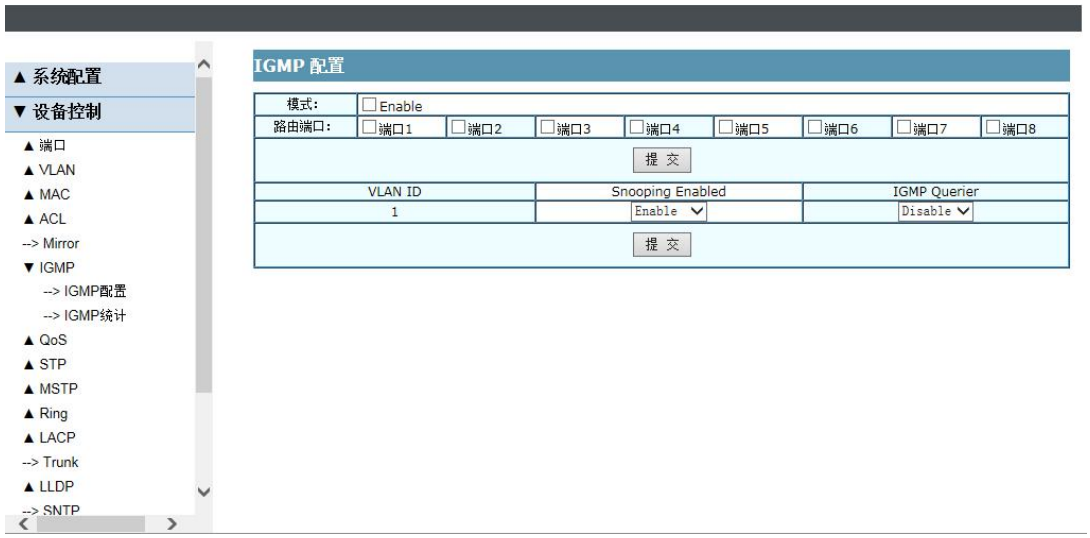


图 5. 2 IGMP 对比图

5.6.2. IGMP 配置

点击导航栏“设备控制→IGMP→IGMP 配置”，即可进入 IGMP 配置界面，如下图：

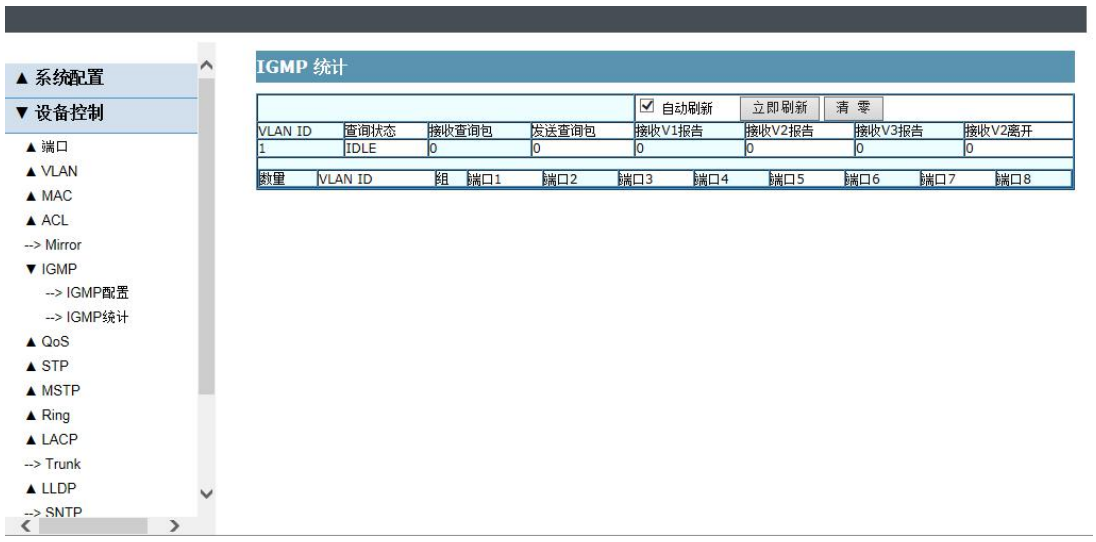


IGMP 配置界面中修改各项参数的解释如下表所示：

配置项	说明
模式	用于启用/禁用交换机的 IGMP Snooping 功能。
路由端口	用于设置交换机上连接组播路由器的端口。
VLAN ID	交换机中 VLAN 组的编号。
Snooping enabled	用于基于 VLAN 启用/禁用 IGMP Snooping 功能。
IGMP Querier	用于基于 VLAN 启用/禁用 IGMP Snooping 的查询功能。

5.6.3. IGMP 状态及统计

点击导航栏“设备控制→IGMP→IGMP 统计”，即可进入 IGMP 统计界面，如下图：



本页面提供了 IGMP 统计的相关信息。各参数信息描述如下：

配置项	说明
VLAN ID	条目的 VLAN ID
查询状态	显示 Querier 状态是“激活”还是“空闲”
发送查询包	已传输 Querier 的数量
接收查询包	已接收 Querier 的数量
接收 V1 报告	已接收的 V1 版报告数量
接收 V2 报告	已接收的 V2 版报告数量。
接收 V3 报告	已接收的 V3 版报告数量。
接收 V2 离开	已接收的 V2 版离开的报告数量。

5.7. QoS

5.7.1. QoS 概述

QoS 的英文全称为"Quality of Service"，中文名为"服务质量"。QoS 是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。

QoS 是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

5.7.2. 常用优先级介绍

1. 802.1p 优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。带有 802.1Q 标签的数据包才带有 802.1p 优先级，如下图所示，4 个位的 802.1Q 标签头包含了 2 个位的 TPID（Tag Protocol Identifier，标签协议标识，取值为 0x8100）和 2 个位的 TCI（Tag Control Information，标签控制信息）

图 5. 3 带有 802.1Q 标签头的以太网帧

下图显示了 802.1Q 标签头的详细内容，TCI 中 Priority 字段就是 802.1p 优先级，也称为 CoS 优先级。它由 3 个 bit 组成，取值范围为 0～7。

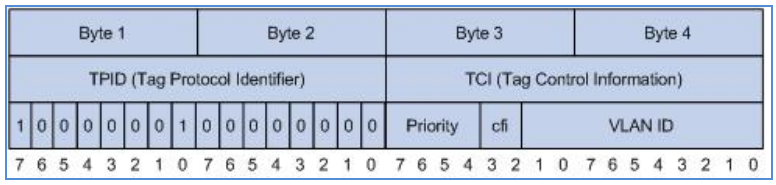


图 5. 4 802.1Q 标签头

2. IP 优先级、ToS 优先级和 DSCP 优先级

在 IP 数据包的包头带有 DSCP 优先级，IP header 的 ToS 字段有 8 个 bit，其中：

- 前 3 个 bit 表示的是 IP 优先级，取值范围为 0～7
- 第 3～6 这 4 个 bit 表示的是 ToS 优先级，取值范围为 0～15
- RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域，其中 DSCP（Differentiated Services Code point，差分服务编码点）优先级用该域的前 6 个 bit（0～5bit）表示，取值范围为 0～63，后 2 个 bit（6、7bit）是保留位。

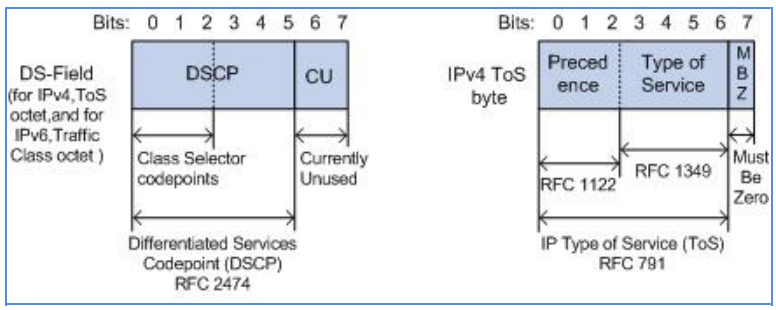


图 5. 5 DS 域和 ToS 字节

5.7.3. 队列调度介绍

1. WRR 队列

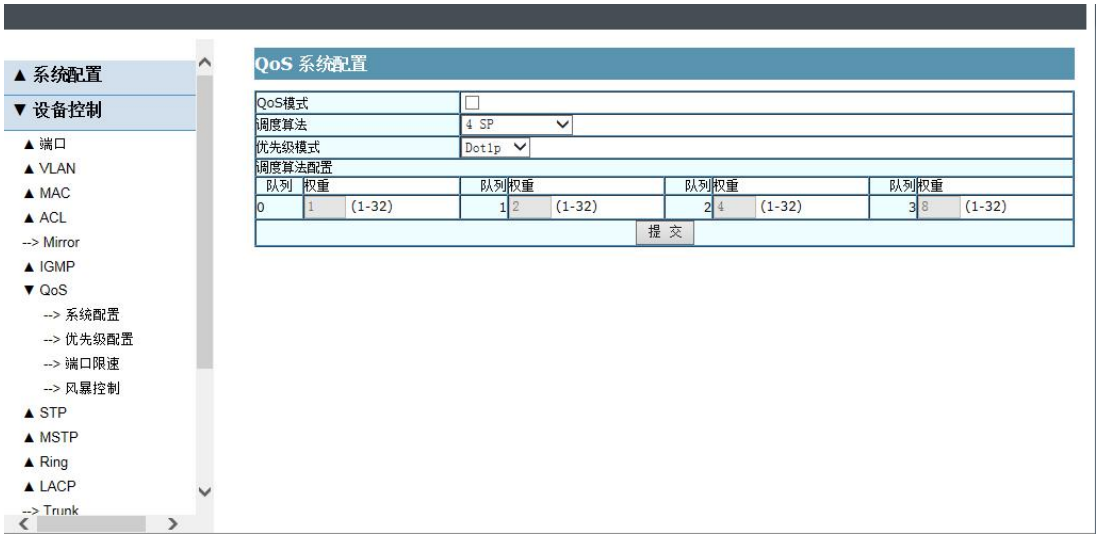
WRR 队列调度算法在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 4 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 8、4、2、1（依次对应 w3、w2、w1、w0），这样可以保证最低优先级队列也可以获得一定的带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。WRR 队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

2. HQ-WRR 队列

HQ-WRR 队列调度算法在 WRR 的基础上，在 4 个输出队列中选择队列 3 为高优先级队列。如果 4 个队列的占用的带宽超过了端口的能力，交换机首先保证队列 3 的报文优先发送出去，然后对其余 3 个队列实行 WRR 调度。

5.7.4. 系统配置界面

点击导航栏“设备控制→QoS→系统配置”，即可进入 QoS 的系统配置界面，如下图：



QoS 系统配置界面中修改各项参数的解释如下表所示：

配置项	说明
QoS 模式	用于启用/禁用系统的 QoS 功能。
调度算法	用于配置系统当前选用的调度算法，可以设置如下 4 种调度算法 4 WRR， 4 SP，1 SP - 3 WRR，2 SP- 2 WRR。
优先级模式	用于配置系统中优先级模式 Dscp 或 Dot1p。
队列	优先级队列的逻辑编号，系统分为“0~3”共 4 个队列。
权重	用于设置各个队列在单位时间里传输流量的比重，其范围为 1~32。

5.7.5. 优先级配置界面

点击导航栏“设备控制→QoS→优先级配置”，即可进入 QoS 的优先级配置界面，如下图：

本界面分为 3 部分，802.1p 优先级队列、ToS 优先级队列和 DSCP 优先级队列。以下分为 3 部分分别

介绍：

1. 802.1p 优先级队列：

此部分用于 802.1p 优先级与队列之间的映射关系，默认情况下，0 和 1 优先级映射 0 队列，2 和 3 优先级映射 1 队列，4 和 5 优先级映射 2 队列，6 和 7 优先级映射 3 队列。

2. ToS 优先级队列：

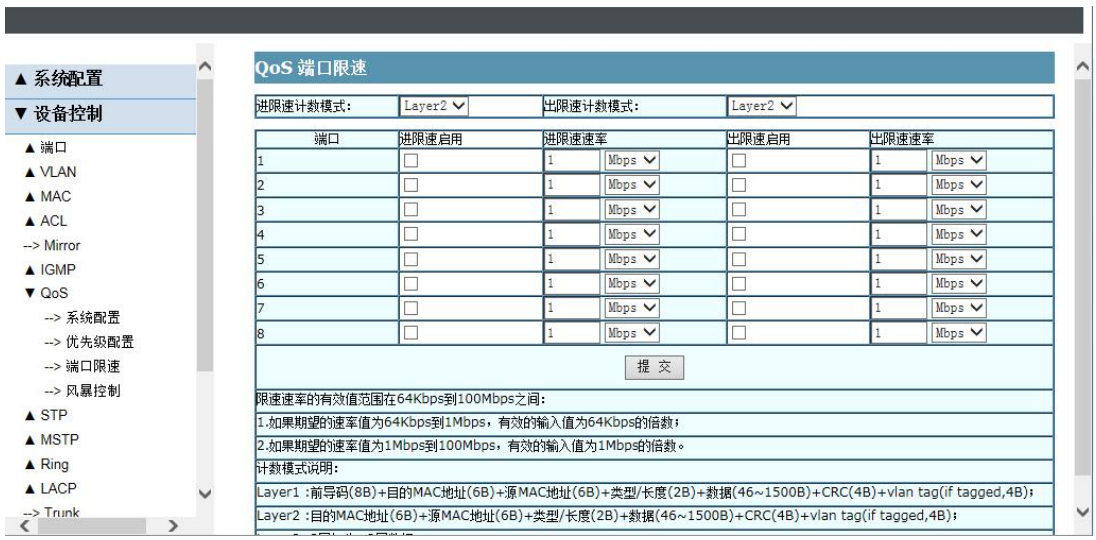
此部分用于 ToS 优先级与队列之间的映射关系，默认情况下，0 和 1 优先级映射 0 队列，2 和 3 优先级映射 1 队列，4 和 5 优先级映射 2 队列，6 和 7 优先级映射 3 队列。

3. DSCP 优先级队列：

此部分用于 DSCP 优先级与队列之间的映射关系，默认情况下，0~15 优先级映射 0 队列，16~31 优先级映射 1 队列，32~47 优先级映射 2 队列，48~63 优先级映射 3 队列。

5.7.6. 端口限速界面

点击导航栏“设备控制→QoS→端口限速”，即可进入 QoS 的端口限速配置界面，如下图：



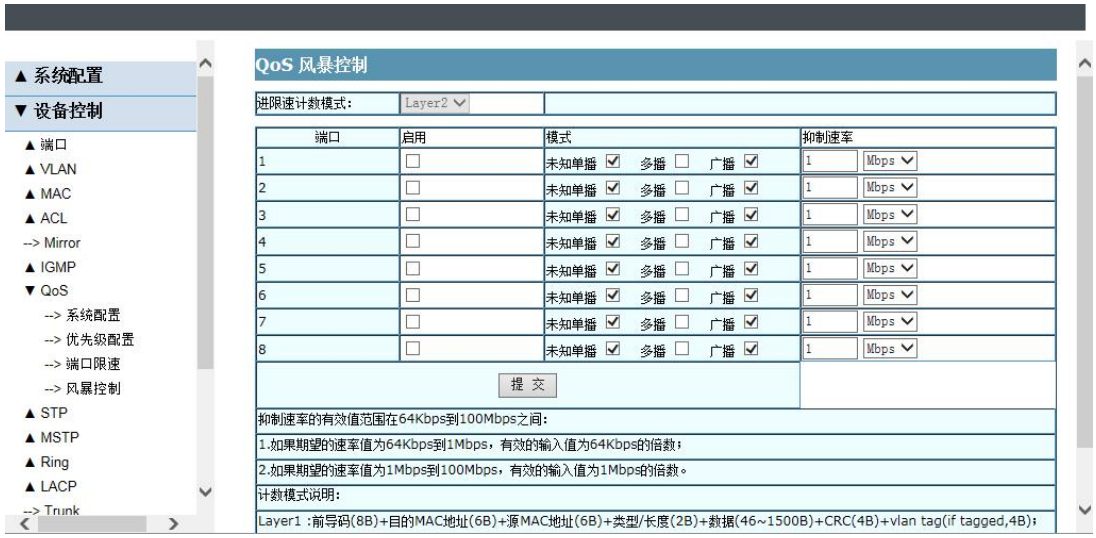
QoS 端口限速界面中修改各项参数的解释如下表所示：

配置项	说明
进限速计数模式	交换机端口的进限速计数模式（Layer1,Layer2,Layer3）。 Layer1 :前导码(8B)+目的 MAC 地址(6B)+源 MAC 地址(6B)+类型/长度(2B)+数据(46~1500B)+CRC(4B)+vlan tag(if tagged,4B); Layer2 :目的 MAC 地址(6B)+源 MAC 地址(6B)+类型/长度(2B)+数据(46~1500B)+CRC(4B)+vlan tag(if tagged,4B); Layer3 :3 层包头+3 层数据。
出限速计数模式	交换机端口的出限速计数模式（Layer1,Layer2,Layer3）。
端口	交换机端口的逻辑编号。
进限速启用	用于启用/禁用端口进入方向的速率限制。勾选该单选框表示启用速率限制，否则表示禁用速率限制。
出限速启用	用于启用/禁用端口出方向的速率限制。勾选该单选框表示启用速

	率限制，否则表示禁用速率限制。
速率	表示端口需要限制到的速率值，其范围为 64Kbps 到 100Mbps。 限速速率的有效值范围在 64Kbps 到 100Mbps 之间： 1.如果期望的速率值为 64Kbps 到 1Mbps，有效的输入值为 64Kbps 的倍数； 2.如果期望的速率值为 1Mbps 到 100Mbps，有效的输入值为 1Mbps 的倍数。

5.7.7. 风暴控制界面

点击导航栏“设备控制→QoS→风暴控制”，即可进入 QoS 的风暴控制配置界面，如下图：



QoS 风暴控制界面中修改各项参数的解释如下表所示：

配置项	说明
端口	交换机端口的逻辑编号
启用	用于启用/禁用端口风暴控制。勾选该单选框表示启用风暴控制，否则表示禁用风暴控制
模式	用于设置控制风暴的类型，包括广播、多播和未知单播。默认控制多播和未知单播
抑制速率	表示端口风暴控制的速率值，其范围为 64Kbps 到 100Mbps。 抑制速率的有效值范围在 64Kbps 到 100Mbps 之间： 1.如果期望的速率值为 64Kbps 到 1Mbps，有效的输入值为 64Kbps 的倍数； 2.如果期望的速率值为 1Mbps 到 100Mbps，有效的输入值为 1Mbps 的倍数。

5.8. STP

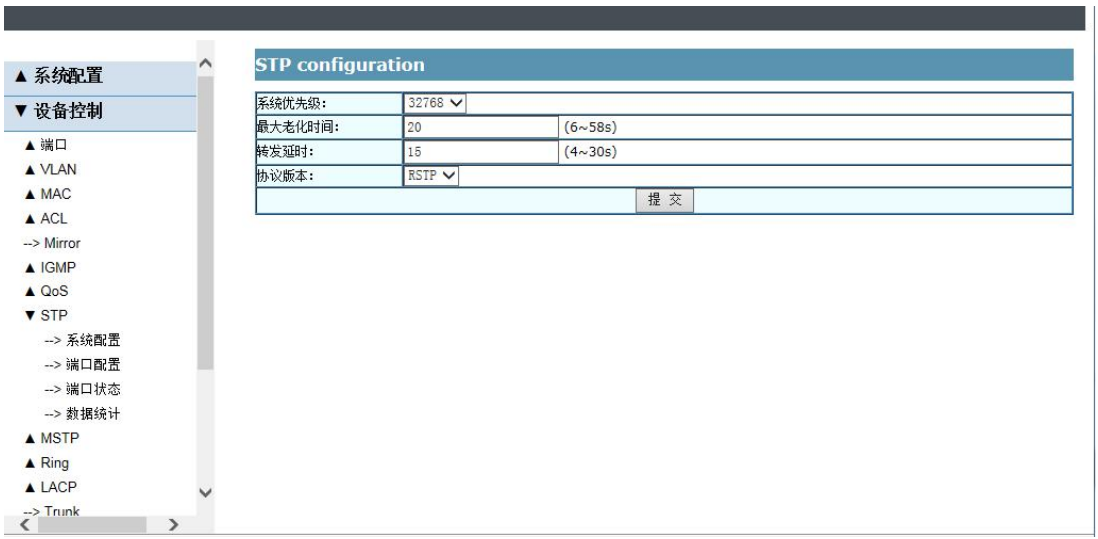
5.8.1. 生成树简介

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 协会制定的 802.1d 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互报文发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免主机由于重复接收相同的报文造成的报文处理能力下降的问题发生。

STP 包含了两个含义，狭义的 STP 是指 IEEE 802.1d 中定义的 STP 协议，广义的 STP 是指包括 IEEE 802.1d 定义的 STP 协议以及各种在它的基础上经过改进的生成树协议。

5.8.2. 系统配置

点击导航栏“设备控制→STP→系统配置”，即可进入 STP 的系统配置界面，如下图：



STP 配置界面中修改各项参数的解释如下表所示：

配置项	说明
系统优先级	用于设置系统的优先级，系统默认优先级为“32768”。系统优先级的范围为 0~61440；递增粒度为 4096；值越小表示优先级越高。
最大老化时间	设置生成树配置消息最大生存期。
转发延时	设置转发延时。
协议版本	用于设置系统当前使用的是 stp 协议还是 rstp 协议。

说明：

Hello Time 不能设置，系统默认为 2s。

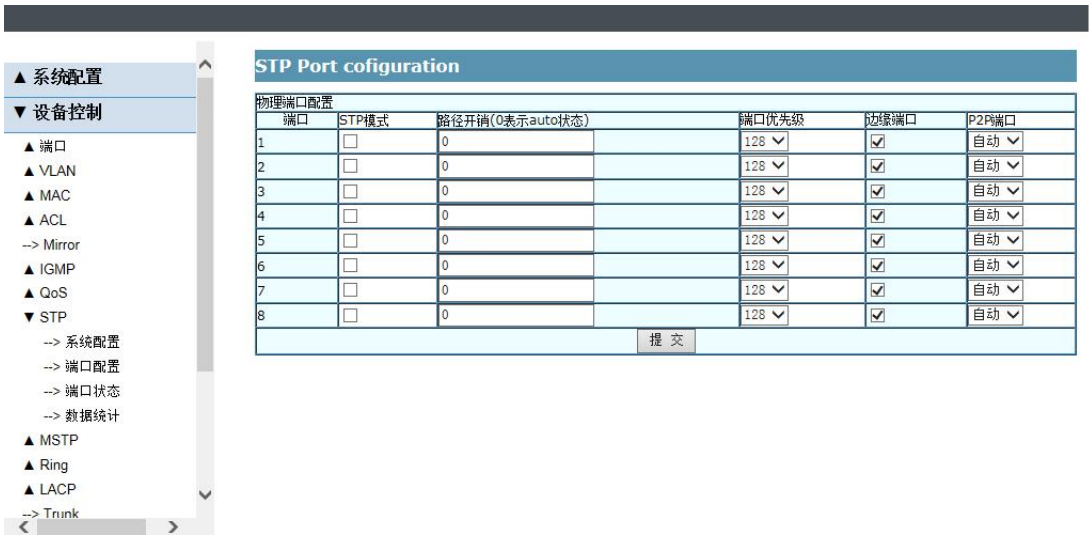
Hello 时间不能长于 Max Age。否则，设置发生错误。在设置上述参数时请参考下列公式。

Max Age ≤ 2 x (Forward Delay - 1 秒)

Max Age ≥ 2 x (Hello Time + 1 秒)

5.8.3. 端口配置

点击导航栏“设备控制→STP→端口配置”，即可进入 STP 的端口配置界面，如下图：



STP 端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
stp 模式	用于启用/禁用端口的 stp 功能。
路径开销	设置路径开销的值，“0”表示该端口处于 auto 状态。
优先级	设置端口优先级
边缘端口	边缘端口是指不直接与任何交换机连接，也不通过端口所连接的网络间接与任何交换机相连的端口。用户如果将某个端口指定为边缘端口，那么当该端口由阻塞状态向转发状态迁移时，这个端口可以实现快速迁移，而无需等待延迟时间，系统默认为启用状态。
P2P 端口	P2P 端口是两台交换机之间直接连接的端口。相连的两个 P2P 端口，如果端口角色满足一定条件，则可以通过传送同步报文快速迁移到转发状态，减少了不必要的转发延迟时间。可以设置为自动、启用、禁用状态，系统默认为自动状态。

5.8.4. 端口状态

点击导航栏“设备控制→STP→端口状态”，即可进入 STP 的端口状态界面，如下图：

STP 端口状态配置界面中修改各项参数的解释如下表所示：

配置项	说明
VLAN ID	表示交换机中 VLAN 组的编号。
桥 ID	由桥的优先级和 MAC 地址组成。
根桥 ID	由根桥的优先级和 MAC 地址组成。
根端口	所谓根端口，是指一个非根桥的设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。
根路径开销	到根桥的最短路径开销。
拓扑标记	用于显示拓扑当前的状态，分为 steady 和 changing 状态。steady 表示拓扑已经收敛，处于稳定状态。changing 表示拓扑正在改变，处于改变状态。
端口角色	分为以下六种： Disabled：表示该端口的 STP 功能处于禁用状态。 Alternate:替换端口。如果一个端口收到另外一个网桥的更好的 BPDU，但不是最好的，那么这个端口成为替换端口。 Backup：如果一个端口收到同一个网桥的更好 BPDU，那么这个端口成为备份端口。当两个端口被一个点到点链路的一个环路连在一起时，或者当一个交换机有两个或多个到共享局域网段的连接时，一个备份端口才能存在。 Root：非根桥收到最优的 BPDU 配置信息的端口为根端口，即到根桥开销最小的端口。 Designated：根桥上连接非根桥的那个端口，它和根端口对应。 Non-STP：表示端口不参与 RSTP 拓扑计算，直接进入 Forwarding 状态
端口状态	Disabled：表示该端口的 STP 功能处于禁用状态。 Blocking：表示该端口处于阻塞状态。 Listening：表示该端口处于侦听状态。 Learning：表示该端口处于学习状态。 Forwarding：表示该端口处于转发状态。

	Non-STP：表示端口不参与 RSTP 拓扑计算，直接进入 Forwarding 状态。
路径开销	路径开销是 STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。
边缘端口	一个边缘端口就像一个 Port Fast-enabled 端口，并且只在连接了一个单独的末端站点的端口上启用他。但它和 Port Fast-enabled 不一样，它不产生拓扑改变，但当它收到 BPDU 时，自动成为生成树端口。
P2P 端口	两台交换机之间只有一条链路，同时端口之间的连接为全双工，这样的链路类型叫点到点链路。
对端版本	该端口对端交换机的 STP 模式。

5.8.5. 数据统计

点击导航栏“设备控制→STP→数据统计”，即可进入 STP 的数据统计界面，如下图：

STP 数据统计界面中修改各项参数的解释如下表所示：

配置项	说明
端口	交换机端口的逻辑编号。
RSTP	BPDU 在端口接收/传输的计算和维护快速生成树拓扑的报文数目。
STP	BPDU 在端口接收/传输的计算和维护生成树拓扑的报文数目。
TCN	当拓扑结构发生变化时，在端口接收/传输的用于通知相关设备网络拓扑结构发生变化的报文数目。
Rx Unknown	在端口接收的未知生成树的 BPDU 数。
Rx Illegal	在端口接收的非法生成树的 BPDU 数。

5.9. MSTP

5.9.1. 概述

MSTP（Multiple Spanning Tree Protocol，多生成树协议）

将环路网络修剪成为一个无环的树型网络， 避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。MSTP 兼容 STP 和 RSTP，并且可以弥补 STP 和 RSTP 的缺陷。它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

5.9.2. 桥配置信息

点击导航栏“设备控制→MSTP→桥配置信息”，即可进入 MSTP 的桥配置信息界面，如下图：

STP 桥配置信息界面中修改各项参数的解释如下表所示：

配置项	说明
是否启用	设置是否启用 MSTP 功能。
转发延时	设置转发延时，取值范围：4~30 秒
Hello 时间	设置 Hello 时间，取值范围：0~10 秒。
最大老化时间	设置最大老化时间，取值范围：6~40 秒。
最大跳数	设置最大跳数，取值范围：1~40。
域名	设置域名。
修订级别	设置修订级别，取值范围：1~65535。

5.9.3. 桥端口配置和状态

点击导航栏“设备控制→MSTP→桥端口配置和状态”，即可进入 MSTP 的桥端口配置和状态，如下图：

MSTP 桥端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
状态	设置端口的状态（启用或禁用）。
边缘	设置端口是否是边缘端口（启用，禁用，自动）。
连接类型	设置端口的连接类型（P2P 或 Share）。
Bpdu 保护	设置端口的 bpdu 保护（启用，禁用，自动）。
Bpdu 过滤	设置端口的 bpdu 过滤（启用，禁用，自动）。
协议版本	显示端口使用的协议版本（STP，RSTP，MSTP）

5.9.4. CIST 配置信息

点击导航栏“设备控制→MSTP→CIST 配置信息”，即可进入 MSTP 的 CIST 配置信息界面，如下图：

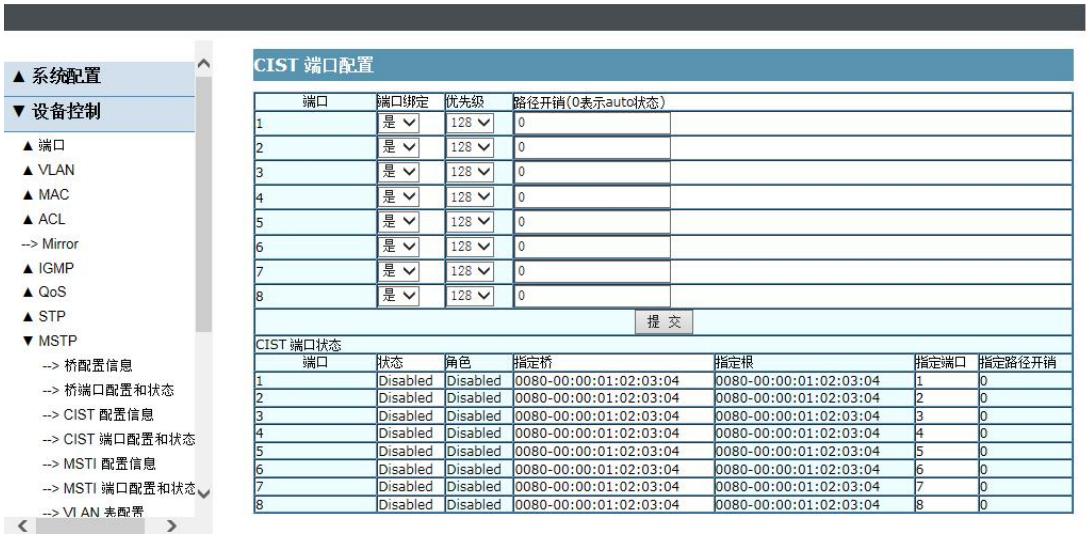
CIST 配置信息面中修改各项参数的解释如下表所示：

配置项	说明
优先级	设置 CIST 的优先级，取值范围 0~61440 之间 4096 的倍数。
跟路径开销	显示 CIST 的跟路径开销。

端口	显示 CIST 端口。
跟标识	显示 CIST 跟标识。
区域跟标识	显示 CIST 区域跟标识。
桥标识	显示 CIST 桥标识。

5.9.5. CIST 端口配置和状态

点击导航栏“设备控制→MSTP→CIST 端口配置和状态”，即可进入 MSTP 的 CIST 端口配置和状态界面，如下图：

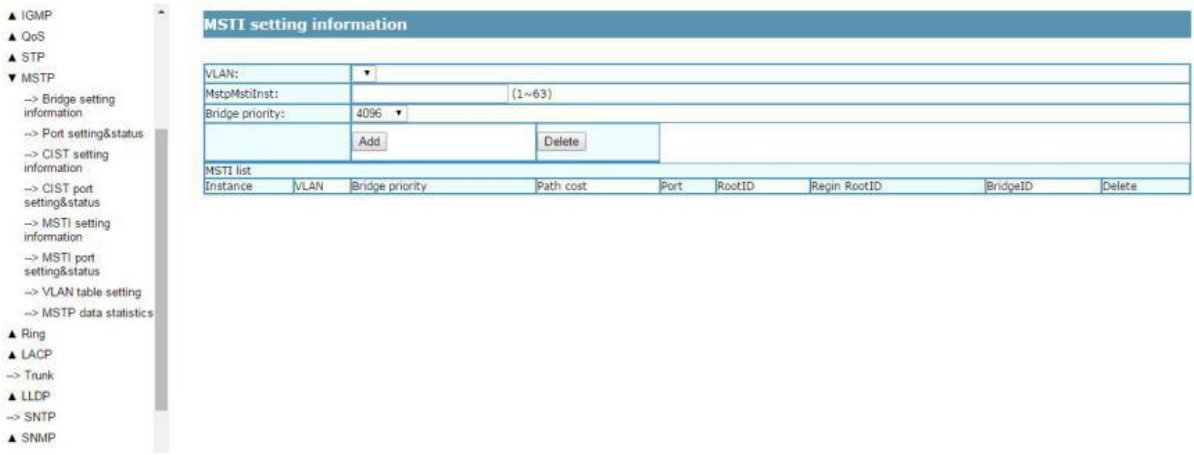


CIST 端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
端口	显示交换机的逻辑端口号。
端口绑定	设置是否绑定端口。
优先级	设置端口的优先级，取值范围：0~240 之间 16 的倍数。
路径开销	设置端口的路径开销，取值范围：0~200000000。
状态 角色	显示端口的状态（Disabled, Block, Learn, Forward, Blank, Error）。 显示端口的角色（Master, Alternate, Root, Designated, Disabled, Backup）。
指定桥	显示端口的指定桥地址。
指定跟	显示端口的指定跟地址。
指定端口	显示端口的指定端口号。
指定路径开销	显示端口的指定路径开销。

5.9.6. MSTI 配置信息

点击导航栏“设备控制→MSTP→MSTI 配置信息”，即可进入 MSTP 的 MSTI 配置信息界面，如下图：

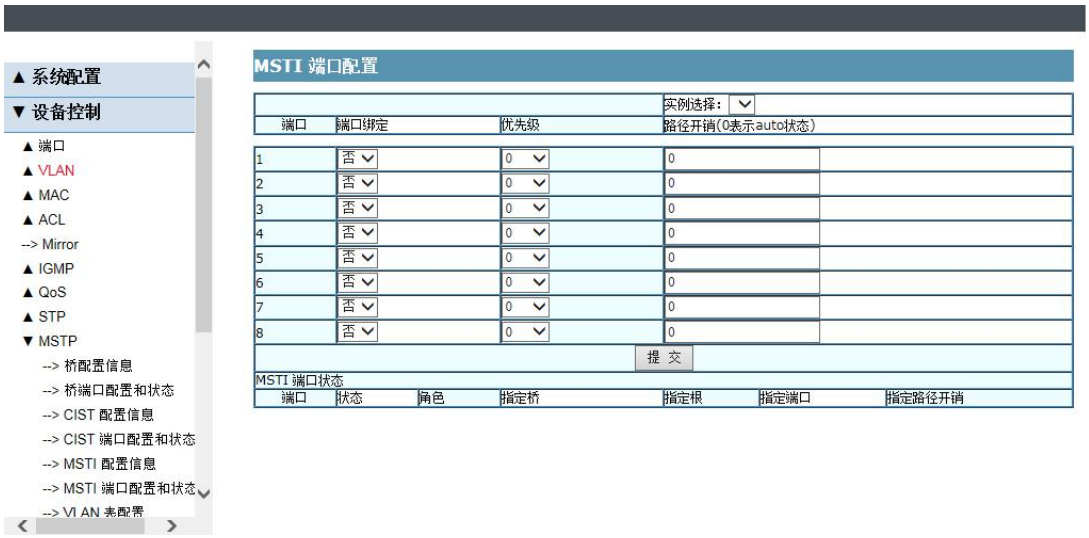


MSTI 配置信息界面中修改各项参数的解释如下表所示：

配置项	说明
Vlan	选择相应的 Vlan
实例	MSTI 实例编号（0~63）
添加	把选择的 Vlan 添加到相应的实例
删除	把选择的 Vlan 从相应的实例中删除
桥优先级	显示实例的桥优先级
跟路径开销	显示实例的跟路径开销
端口	显示实例的端口
跟标识：	显示实例的跟标识
区域跟标识	显示实例的区域跟标识
桥标识	显示实例的桥标识
删除	删除该 MSTI 实例

5.9.7. MSTI 端口配置和状态

点击导航栏“设备控制→MSTP→MSTI 端口配置和状态”，即可进入 MSTP 的 MSTI 端口配置和状态界面，如下图：

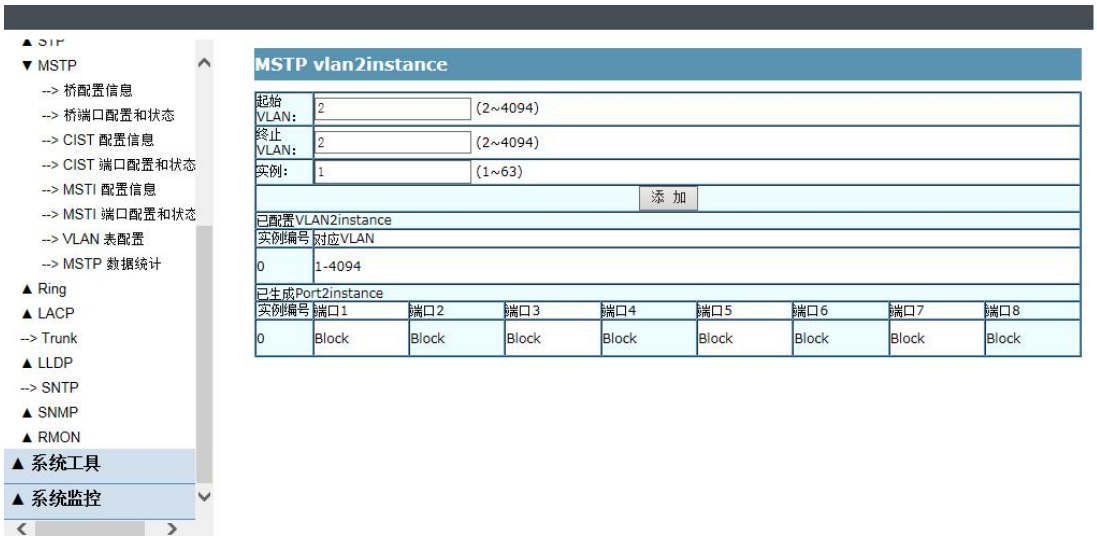


MSTI 端口配置界面中修改各项参数的解释如下表所示：

配置项	说明
实例选择	选择相应的实例
端口	交换机的逻辑端口号
端口绑定	设置是否绑定端口，只有在 CIST 端口配置里先绑定端口，才能在这里绑定端口
优先级	设置端口的优先级，取值范围：0~240 之间 16 的倍数
路径开销	设置端口的路径开销，取值范围：0~200000000
状态	显示端口的状态（Disabled, Block, Learn, Forward, Blank, Error）
角色	显示端口的角色（Master, Alternate, Root, Designated, Disabled, Backup）
指定桥	显示端口的指定桥地址
指定跟	显示端口的指定跟地址
指定端口	显示端口的指定端口号
指定路径开销	显示端口的指定路径开销

5.9.8. Vlan 表配置

点击导航栏“设备控制→MSTP→Vlan 表配置”，即可进入 MSTP 的 Vlan 表配置界面，如下图：

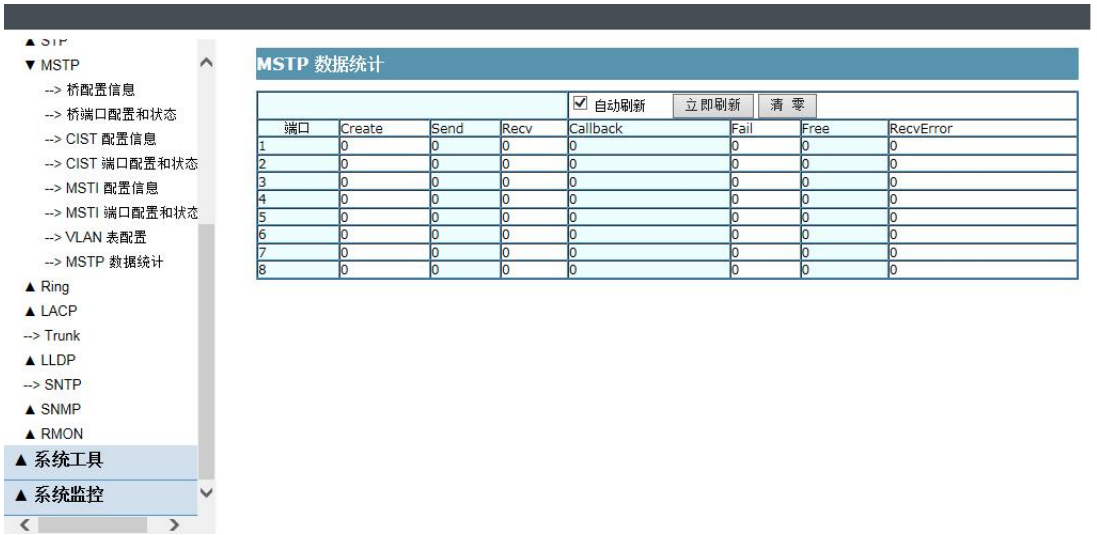


VLAN 表配置界面中修改各项参数的解释如下表所示：

配置项	说明
起始 VLAN	设置起始 Vlan
终止 VLAN	设置终止 Vlan，起始 Vlan 和终止 Vlan 之间的不能超过 10。
实例	需要添加的实例编号
添加	把起始 Vlan 和终止 Vlan 的 Vlan 添加到相应的实例
实例编号	显示已被配置的实例号
对应 Vlan	显示实例的对应 Vlan
端口 1~端口 9	显示 9 个端口的状态（Block, Learn, Forward）

5.9.9. MSTP 数据统计

点击导航栏“设备控制→MSTP→MSTP 数据统计”，即可进入 MSTP 的 MSTP 数据统计界面，如下图：



MSTP 数据统计界面中修改各项参数的解释如下表所示：

配置项	说明
端口	交换机的逻辑端口号
Create	显示端口产生的数据包数量。
Send	显示端口发送的数据包数量
Recv	显示端口接收的数据包数量
Callback	显示端口回调数据包数量。
Fail	显示端口发送和接收失败的数据包数量。
Free	显示端口释放数据包数量
RecvError	显示端口接收错误次数

5.10. WTOP_RING

5.10.1. 概述

5.10.1.1. 节点类型

一个 WTOP-RING 环物理上对应一个环形连接的以太网拓扑。WTOP-RING 环的角色由用户通过配置决定。

1. 主节点

主节点是 WTOP-RING 环上的主要决策和控制节点。每个 WTOP-RING 环上必须有一个主节点，而且只能有一个。

以太网环上每一台交换机都称为一个节点，每个 WTOP-RING 环上必须有一个主节点，而且只能有一

个。主节点是 Polling 机制（环网状态主动检测机制）的发起者，也是网络拓扑发生改变后执行操作的决策者。

主节点周期性的从其主端口发送 HELLO（健康检测报文）报文，依次经过各传输节点在环上传播。如果从主节点副端口能够收到自己发送的 HELLO 报文，说明环网链路完整；如果在规定时间内收不到 HELLO 报文，就认为环网发生链路故障。主节点有如下 2 种状态：

1) Complete State（完整状态）

当环网上所有的链路都处于 UP 状态，主节点可以从副端口收到自己发送的 HELLO 报文，就说主节点处于 Complete 状态。主节点的状态即反映了 WTOP-RING 环的状态，因此 WTOP-RING 环也处于 Complete 状态，此时主节点会阻塞副端口以防止数据报文在环形拓扑上形成广播环路。

2) Failed State（故障状态）

当环网上存在链路处于 Down 状态时，则主节点将处于 Failed 状态，此时主节点放开副端口以保证环网上各节点通信不被中断。

2. 传输节点

环上除主节点之外的其它节点都可以称为传输节点。一个 WTOP-RING 环上可以有多个传输节点，也可以没有传输节点（事实上这样的组网没有实际意义）。

每一个 WTOP-RING 环物理上对应一个环形连接的以太网拓扑，WTOP-RING 环同样由整数表示的 ID 来标识。

WTOP-RING 环上除主节点外的所有其它节点都是传输节点。传输节点负责监测自己的直连 WTOP-RING 链路的状态，并把链路变化通知主节点，然后由主节点来决策如何处理。传输节点有如下 3 种状态：

1) Link-Up State（UP 状态）

传输节点的主端口和副端口都处于 UP 状态时，就说传输节点处于 Link-Up 状态。

2) Link-Down State（Down 状态）

传输节点的主端口或副端口处于 Down 状态时，就说传输节点处于 Link-Down 状态。

3) Preforwarding State（临时阻塞状态）

传输节点的主端口或副端口处于阻塞状态时，就说传输节点处于 Preforwarding 状态。

处于 Link-Up 状态的传输节点检测到主端口或者副端口发生链路 Down 时，就从 Link-Up 迁移到 Link-Down 状态，并通过发送 Link-Down 报文通知主节点。

传输节点不从 Link-Down 状态直接迁移回 Link-Up 状态。当处于 Link-Down 状态的传输节点某端口发生链路 Up，并且由此主端口和副端口都恢复成 Up 状态，传输节点迁移到 Preforwarding 状态，并阻塞恢复的端口。传输节点主、副端口都恢复的瞬间，主节点还不能马上知道这一信息，因此其副端口还处于放开状态，如果传输节点立即迁移回 Link-Up 状态，势必造成数据报文在环网上形成广播环路，因此传输节点从 Link-Down 先迁移到 Preforwarding 状态。

当处于 Preforwarding 状态的传输节点收到主节点发送的 COMPLETE-FLUSH-FDB 报文时，将迁移到 Link-Up 状态。如果 COMPLETE-FLUSH-FDB 报文在传输过程中不幸丢失，WTOP-RING 协议还提供了一

种备份机制来恢复临时阻塞的端口并触发状态切换，就是传输节点在规定的时间内收不到COMPLETE-FLUSH-FDB 报文，自行迁移到 Link-Up 状态，并放开临时阻塞端口。

3. Edge (边缘节点)

边缘节点仅存在于相交环中，是机制的发起者和决策者，防止各单环之间形成环路。

边缘节点比传输节点多一种状态：Preforwarding_II State（临时阻塞状态 II），当相交链路断开，边缘节点上的各环端口将处于 Preforwarding_II State。为了防止形成环路，该状态不会因为超时变为 UP 状态，只有当其他链路断开或相交链路恢复时，才会转为 UP 状态。

4. Assistant(辅助边缘节点)

辅助边缘节点仅存在于相交环中，是通道状态的监听者，并负责把通道状态改变及时通知边缘节点。辅助边缘节点的端口状态与传输节点一致。当相交链路断开时辅助边缘节点会向 Edge (边缘节点)发送 WTOPR_FLAGS_FAULT 消息，边缘节点收到该消息后会阻塞相应端口。只要相交链路断开，辅助边缘节点便会周期性的向边缘节点发探测包，边缘节点若连续收到两个探测包说明存在环路，立即阻塞其中一个端口。

5.10.1.2. 端口角色

1. 主端口和副端口

主节点和传输节点接入以太网环的两个端口中，一个为主端口，另一个为副端口，端口的角色由用户的配置决定。

主节点的主端口和副端口在功能上是有区别的。主节点从其主端口发送环路状态探测报文，如果能够从副端口收到该报文，说明本节点所在 WTOP-RING 环网完整，因此需要阻塞副端口以防止数据环路；相反如果在规定时间内收不到探测报文，说明环网故障，此时需要放开副端口以保证环上所有节点的正常通信。传输节点的主端口和副端口在功能上没有区别。端口的角色同样由用户的配置决定。

2. EdgePort (边缘端口)

连接相交链路的端口称为边缘端口。

5.10.1.3. 拓扑类型

1. 单环

一个 WTOP-RING 环物理上对应一个环形连接的以太网拓扑，该环形拓扑中存在一个主交换机，而且只能有一个，该主交换机是是 Polling 机制（环网状态主动检测机制）的发起者，也是网络拓扑发生改变后执行操作的决策者。

典型拓扑图如下：

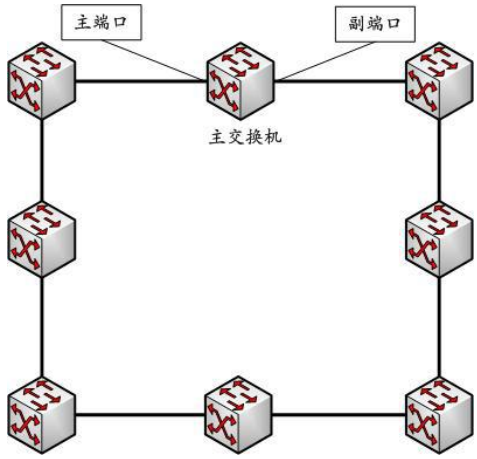


图 5.6 单环

2. 相切环

相切环即是两个或以上 WTOP-RING 有一个公共的交换机，但不存在公共的端口。相切环中的各 WTOP-RING 均遵循单环机制，互不影响。配置上和单环配置基本一致，不同的是需要在公共交换机上配置多个 WTOP-RING。

典型拓扑图如下：

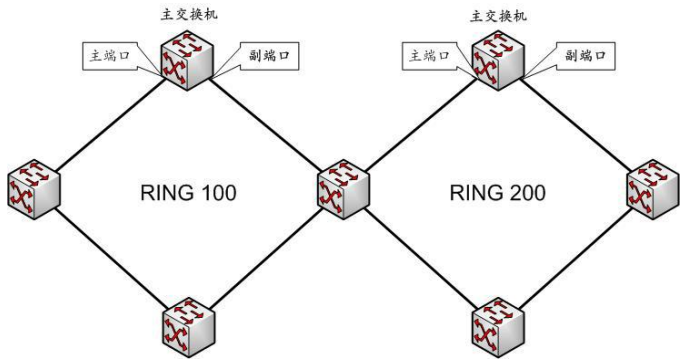


图 5.7 相切在传输节点的相切环

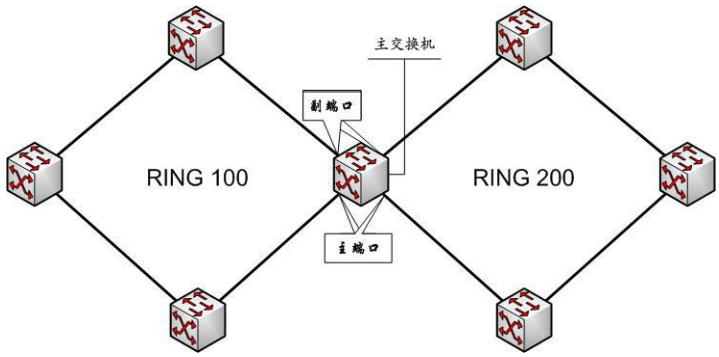


图 5.8 相切在主节点的相切环

3. 相交环

相交环即是两个或以上 WTOP-RING 有至少两个公共交换机，且每个公共交换机存在一端口被各单环

共用。正常情况下，各 WTOP-RING 均遵循单环机制，互不影响。

典型拓扑图如下：

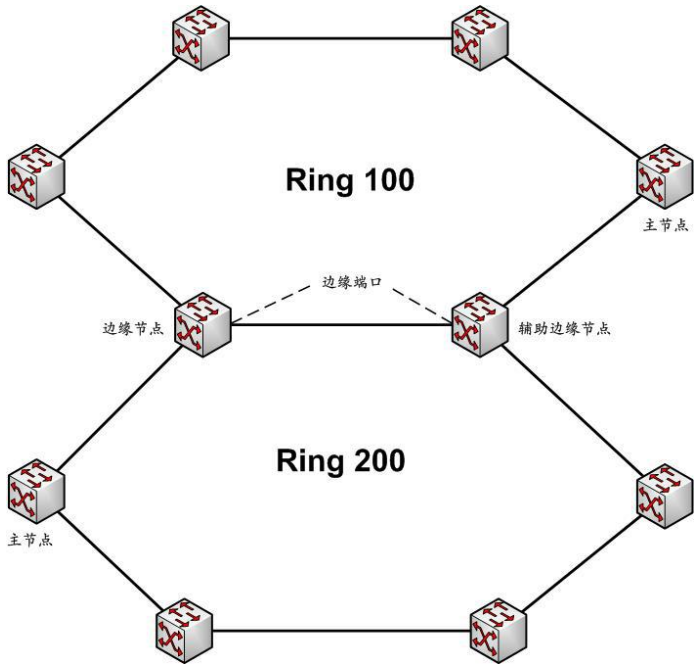


图 5.9 相交环

4. 耦合环

当拓扑中存在多个单环时，可以使用耦合环来实现环与环之间的链路备份。当主链路断开时，备份链路自动由阻塞状态切换到转发状态，当主链路恢复时立即通知备份链路阻塞。在此过程中不影响环与环之间的通讯。

配置主、备份链路实现的环需要注意以下几点：

1) 主、备份链路连接的端口不能是环端口或者 STP 端口。

2) 两环之间只能由一条主链路和一条备份链路连接。

3) 一个交换机中只能有一个主、备份链路端口。

典型的拓扑如下：

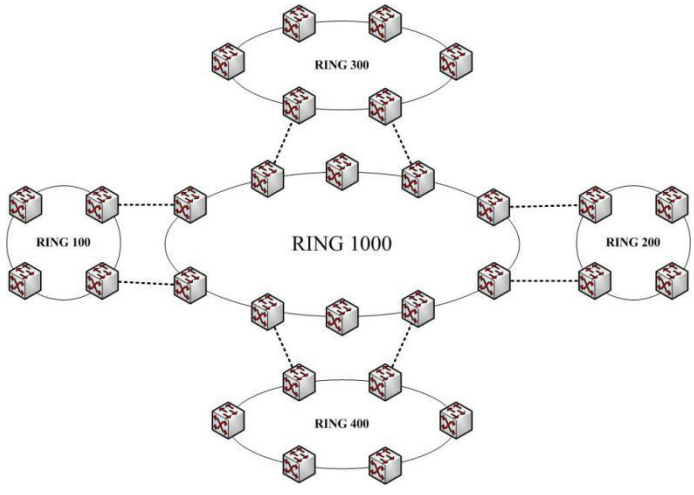


图 5. 10 耦合环

5.10.1.4. 消息类型

1. HEALTH(HELLO)

健康检测报文，由主节点发起，对网络进行环路完整性检测。

2. LINK-UP

链路 UP 报文，由发生直连链路状态 UP 的传输节点、边缘节点或者辅助边缘节点发起，通知主节点环路上有链路恢复。

3. LINK-DOWN

链路 DOWN 报文，由发生直连链路状态 DOWN 的传输节点、边缘节点或者辅助边缘节点发起，通知主节点环路上有链路 DOWN，物理环路消失。

4. WTOP_CONF_COMM_FD_FDB

刷新 FDB 报文，由主节点发起，通知传输节点、边缘节点或者辅助边缘节点更新各自 MAC 地址转发表。

5. WTOP_CONF_CPLT_FLD_FDB

环网恢复刷新 FDB 报文，由主节点发起，通知传输节点、边缘节点或者辅助边缘节点更新各自 MAC 地址转发表，同时通知传输节点放开临时阻塞端口。

6. WTOPR_FLAGS_FAULT

边缘节点与辅助边缘节点间的通道中断时，辅助边缘节点将该消息通知边缘节点，边缘节点收到后将阻塞对应的边缘端口，并通知该环的主节点打开其副端口。

7. WTOPR_FLAGS_RING_DETECT

该消息用于检测相交环整个拓扑是否存在环路，边缘节点与辅助边缘节点间的通道中断时，辅助边缘节点定时的将该消息通过各环发往边缘节点，边缘节点收到该消息后判断是存在环路，若存在则阻塞相应边缘端口。

边缘节点与辅助边缘节点间的通道中断时，各环主节点将收不到自己发出的 Hello 报文，于是 Fail 定时器超时，各环主节点迁移到 Failed 状态，放开副端口，所有环的主节点副端口放开，各环之间势必形成广播环路，为了消除这一缺陷，引入了通道状态检测机制，这一机制需要边缘节点和辅助边缘节点配合完成，目的就是在各环主节点副端口放开之前，阻塞边缘节点的边缘端口，从而避免各环间形成数据环路。

边缘节点与辅助边缘节点间的通道连通时，按照单环机制进行收敛，并打开各阻塞的边缘端口。

5.10.2. 端口配置

点击导航栏“设备控制→WTOP_RING→端口配置”，即可进入 WTOP_RING 的端口配置界面，如下图：

WT-Ring 配置界面中修改各项参数的解释如下表所示：

配置项	说明
环网类型	环网类型分为动态环网和静态环网。动态环网表示主交换机不确定，随拓扑的变化而变化，主要特点是当链路恢复时不需要收敛时间。静态环网主要特点是不管拓扑怎么变化，主交换机是确定不变的，但链路恢复时需要收敛时间。
ring ID	环网的编号，环与环之间可以根据 ring ID 进行区别，其范围为 1~4096。
端口成员 1	环网的第一个端口成员，每个环的成员最多包括两个端口，每个交换机可以有多个环。
端口成员 2	环网的第二个端口成员。
系统类型	系统类型分为 Transfer（传输节点）、Master（主节点）、Assistant（辅助边缘节点）和 Edge（边缘节点），每个类型在概述中有详细解释。
端口成员 1 类型	端口成员的类型根据系统类型改变而改变，当系统为 Master 时，其成员的类型为 Master 和 Subsidiary；当系统为 Transfer 时，其成员的类型为 None；当系统为 Assistant 时，其成员的类型为 Edgeport 和 None；当系统为 Edge 时，其成员的类型为 Edgeport 和 None。
端口成员 2 类型	端口成员的类型根据系统类型改变而改变，当系统为 Master 时，其成员的类型为 Master 和 Subsidiary；当系统为 Transfer 时，其成员的类型为 None；当系统为 Assistant 时，其成员的类型为 Edgeport 和 None；当系统为 Edge 时，其成员的类型为 Edgeport 和 None。
Master	此参数用于启用系统的 Master 状态。当系统为 Master 类型时，必须启用此参数，WTOP_ring 功能才可以正常使用。
WTOP-Ring 列表	当环的各参数设置成功后，此列表就会显示该环的各种信息。
WTOP-Ring 配置向导	WTOP-Ring 配置向导用于环网的分步配置，由于环网配置复杂，用向导引导客户按步骤进行配置，将会使环网配置变得简单易行。

5.10.3. 主备链路

点击导航栏“设备控制→WTOP_RING→主备链路”，即可进入 WTOP_RING 的主备链路配置界面，如下图：

此页面用于显示主备链路的状态信息，各参数的意义如下：

配置项	说明
链路 ID	主备链路的编号，范围是“1~1000”。
端口	主备链路的成员端口。
角色	主备链路的端口角色，分为主链路和备份链路。

5.10.4. 端口信息

点击导航栏“设备控制→WTOP_RING→端口信息”，即可进入 WTOP_RING 的端口信息界面，如下图：

此页面用于显示 wtop_ring 各成员端口的状态信息，各参数的意义如下：

配置项	说明
端口	wtop_ring 的端口成员。
状态	端口成员的链接状态，分为 linkup 和 linkdown。
环 ID	环网的编号，环与环之间可以根据 ring ID 进行区别，其范围为 1~4096。
环模式	环的状态，分为启用和禁用两种状态。
角色	端口成员的的角色，包括 Master、Subsidiary、Edgeport 和 None。
转发状态	端口成员的转发状态，分为 forwarding、blocking 和 disable 等状态。

5.10.5. 数据统计

点击导航栏“设备控制→WTOP_RING→数据统计”，即可进入 WTOP_RING 的数据统计界面，如下图：

此页面用于 WTOP-Ring 的数据统计，各参数的意义如下：

配置项	说明
端口	wtop_ring 的端口成员。
ERSTP	环网的探测包。
ETCN	环网的控制包，包括 MAC 地址清除等控制包。
Rx Ill	收到的错误的 wtop_ring 消息。
Rx Unk	收到的未知的 wtop_ring 消息。

5.10.6. 配置举例

5.10.6.1. 单环

1. 组网需求：

将 4 台交换机组成单环，环 ID=100，端口成员为 Port1 和 Port2。

2. 组网图：

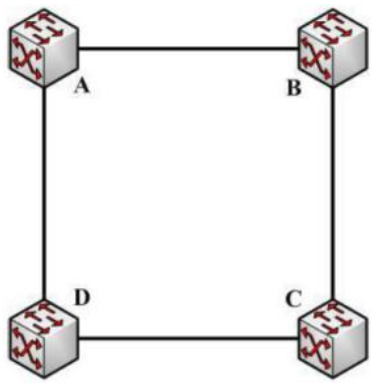


图 5. 11 单环组网示意图

3. 配置步骤：

1) 静态单环

静态单环中分为主交换机和传输交换机两种，具体配置如下：

a. 主交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Master（主交换机）。

- 设置端口成员的类型，这里设置 Port1 为 Master 端口，Port2 为 subsidiary（从端口）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

b. 传输交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Transfer（传输交换机）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

2) 动态单环：

在动态单环中，所有的交换机配置相同，选择其中任意交换机为例：

- 设置环类型为动态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

5.10.6.2. 相切环

1. 组网需求：

将 ring100 和 ring200 相切，在实际配置中分为以下两种方式：

- 相切在主交换机
- 相切在传输交换机

2. 组网图：

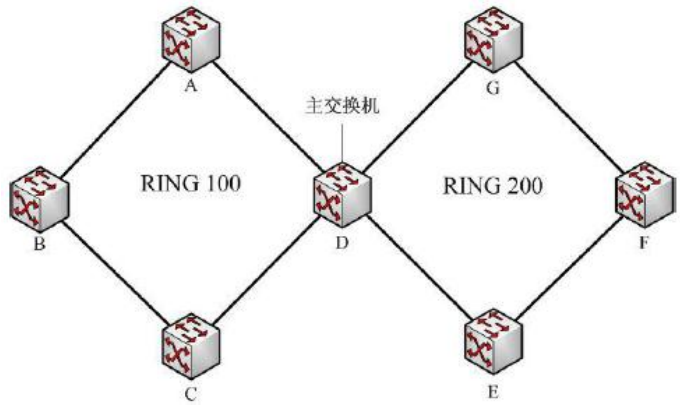


图 5. 12 相切于主交换机的相切环

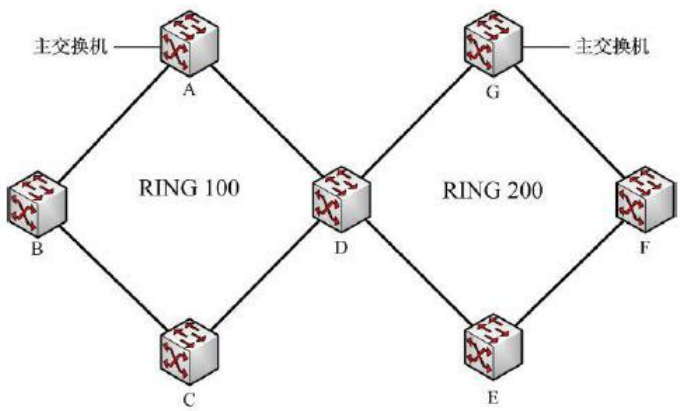


图 5. 13 相切于传输交换机的相切环

3. 配置步骤：

虽然相切环存在两种方式，但二者只是相切的交换机不同而已，在实际的配置中其实都是相似的，相切的交换机就是配置两个环网，非相切的交换机只有一个环网，以下就以相切的交换机和非相切的交换机来进行配置举例：

1) 相切的主交换机配置：

- 置环模式为静态环网
- 设置环 ID =100/200。
- 选择端口成员为 Port1 和 Port2/ Port3 和 Port4。
- 选择系统类型为 Master（主交换机）。
- 设置端口成员的类型，这里设置 Port1/ Port3 为 Master 端口，Port2 Port4 为 subsidiary（从端口）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

2) 非相切的主交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Master（主交换机）。
- 设置端口成员的类型，这里设置 Port1 为 Master 端口，Port2 为 subsidiary（从端口）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

3) 相切的传输交换机：

- 设置环类型为静态环网
- 设置环 ID =100/200。
- 选择端口成员为 Port1 和 Port2/ Port3 和 Port4。
- 选择系统类型为 Transfer（传输交换机）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

4) 非相切的传输交换机：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Transfer（传输交换机）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

5.10.6.3. 相交环

1. 组网需求：

ring100 和 ring200 相交于链路 a，每个环有 4 台交换机，相交的两个交换机的 2 端口为边缘端口。

2. 组网图：

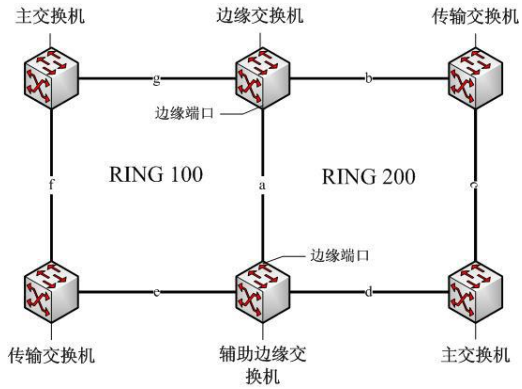


图 5. 14 相交环

3. 配置步骤：

在相交环的配置中，每个环除了 ring ID 不同之外，其它的配置都相同。相交环中分为主交换机、传输交换机、边缘交换机和辅助边缘交换机，以下分别以这三种交换机为例：

1) 主交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Master（主交换机）。
- 设置端口成员的类型，这里设置 Port1 为 Master 端口，Port2 为 subsidiary（从端口）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

2) 传输交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Transfer（传输交换机）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

3) 边缘交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Edge（边缘交换机）。
- 设置端口成员的类型，这里设置 Port1 为 Edgeport 端口，Port2 为 None。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

4) 辅助边缘交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Assitant（辅助边缘交换机）。
- 设置端口成员的类型，这里设置 Port1 为 Edgeport 端口，Port2 为 None。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

5.10.6.4. 耦合环

1. 组网需求：

单环 ring100、ring200、ring300、ring400 分别和单环 ring1000 进行耦合连接，各环之间有两条链路连接，这两条链路互为备份，当其中一条链路断开时，另外一条链路立刻变为转发状态保证两环之间的通讯。

2. 组网图：

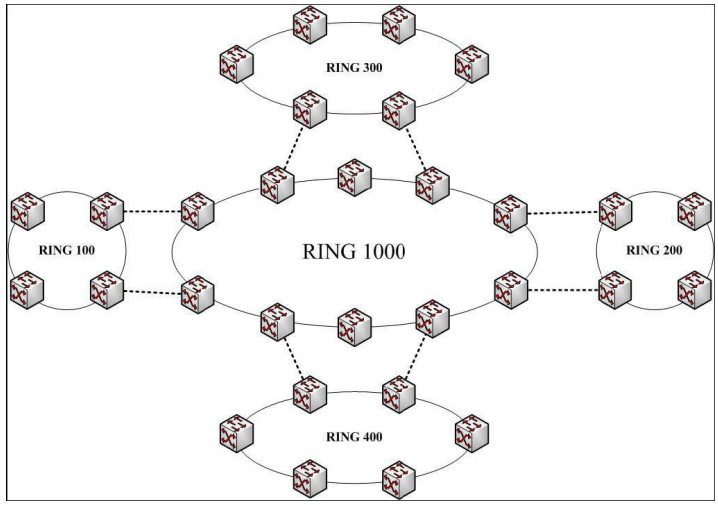


图 5. 15 相交环

3. 配置步骤：

在耦合环的配置中，各环的配置基本类似，分为环网的配置和耦合链路的配置，以下分别对这两部分进行距离说明，就以 ring100 为例：

1) 环网的配置：

a. 主交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。
- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Master（主交换机）。
- 设置端口成员的类型，这里设置 Port1 为 Master 端口，Port2 为 subsidiary（从端口）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

具体配置界面如下图：

b. 传输交换机配置：

- 设置环类型为静态环网
- 设置环 ID =100。

- 选择端口成员为 Port1 和 Port2。
- 选择系统类型为 Transfer（传输交换机）。
- 设置环状态为启用状态。
- 点击“提交”完成配置。

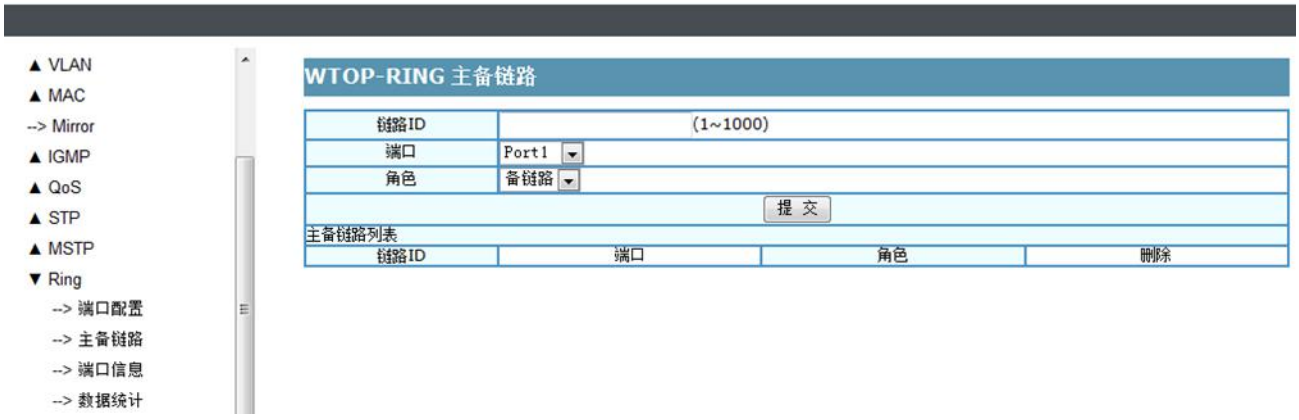
具体配置界面如下图：

2) 耦合链路的配置：

耦合链路也叫主备链路，用于环与环之间的双链路连接，在正常情况下，主链路处于通讯状态，备份链路处于阻塞状态。当主链路出现故障时，备份链路立刻进入转发状态进行环与环之间的通讯，主要配置如下：

- 设置链路 ID。
- 选择主备链路的端口。
- 设置链路的角色，主备链路的角色分为主链路和备份链路。
- 点击“提交”完成配置。

具体配置界面如下图：



5.11. 链路汇聚

5.11.1. 链路汇聚简介

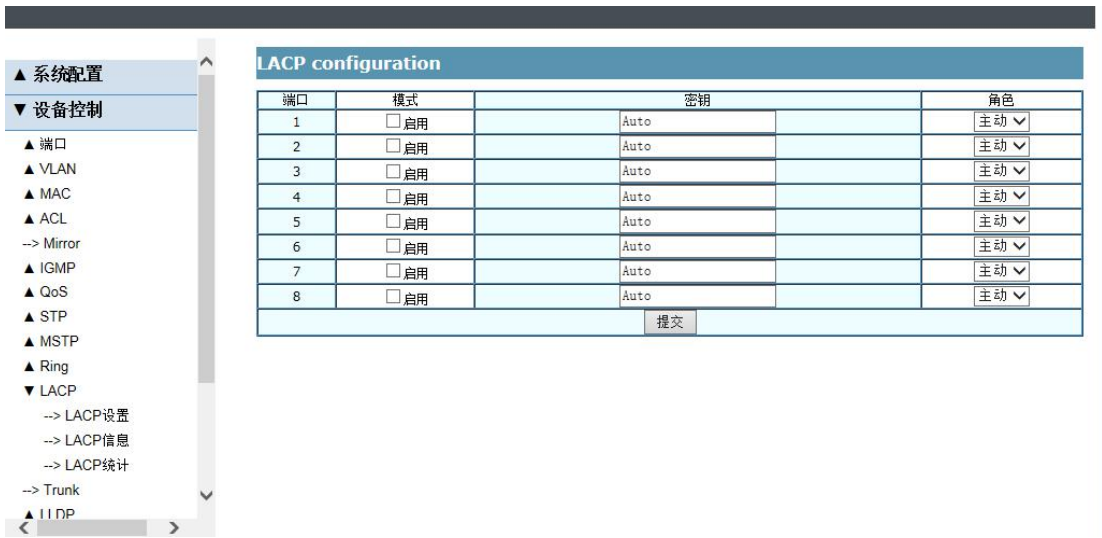
端口汇聚是将多个以太网端口汇聚在一起形成一个逻辑上的汇聚组，使用汇聚服务的上层实体把同一汇聚组内的多条物理链路视为一条逻辑链路。

端口汇聚可以实现出/入负荷在汇聚组中各个成员端口之间分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。

端口汇聚分为动态的 LACP 和静态的 Trunk，以下将对二者进行详细说明。

5.11.2. LACP 配置

点击导航栏“设备控制→LACP→LACP 配置”，即可进入 LACP 的配置界面，如下图：

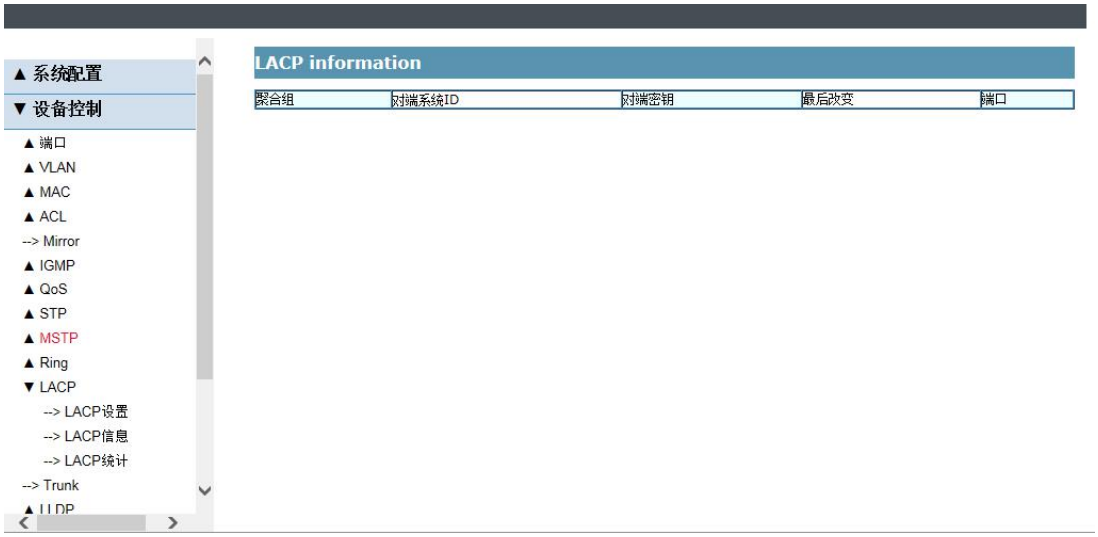


LACP 配置界面中修改各项参数的解释如下表所示：

配置项	说明
模式	用于配置动态链路汇聚端口的模式。勾选表示启用，否则表示禁用。
密钥	用于配置动态链路汇聚的密钥。范围为 0~65535，其中 0 表示自动。
角色	用于配置动态链路汇聚端口的角色。分为主动和被动方式。

5.11.3. LACP 信息

点击导航栏“设备控制→LACP→LACP 信息”，即可进入 LACP 的信息界面，如下图：

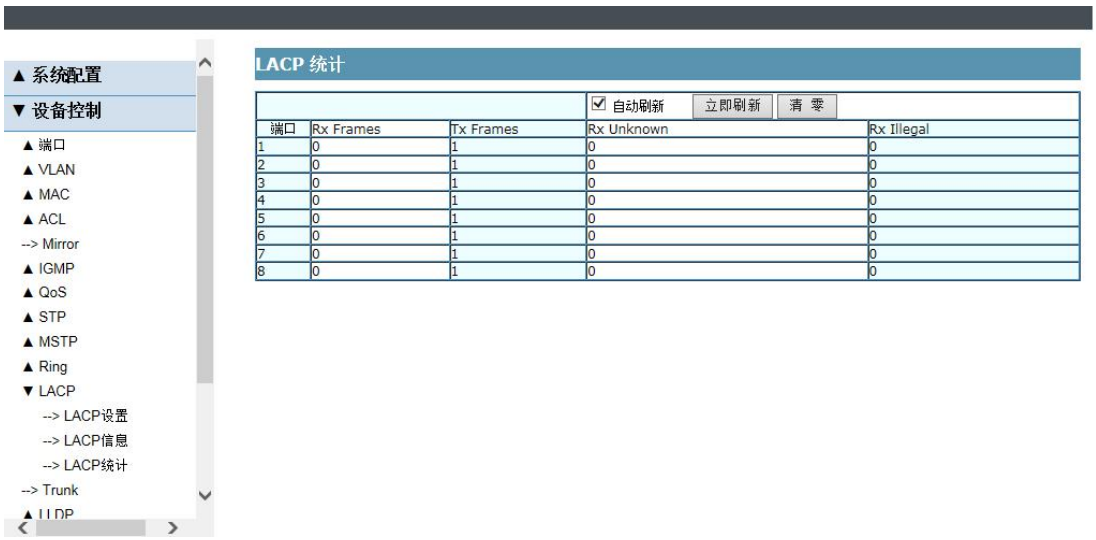


用于查看动态链路汇聚的汇聚信息，包括以下信息：

配置项	说明
聚合组	形成汇聚后的汇聚组编号，范围是 LLAG1~LLAG4。
对端系统 ID	对端系统的 MAC 地址。
对端密钥	对端汇聚组所设置的密钥值。
最后改变	最后一次改变的时间距离现在的时间长度。
端口	汇聚组包括的端口成员。

5.11.4. LACP 统计

点击导航栏“设备控制→LACP→LACP 统计”，即可进入 LACP 的统计界面，如下图：



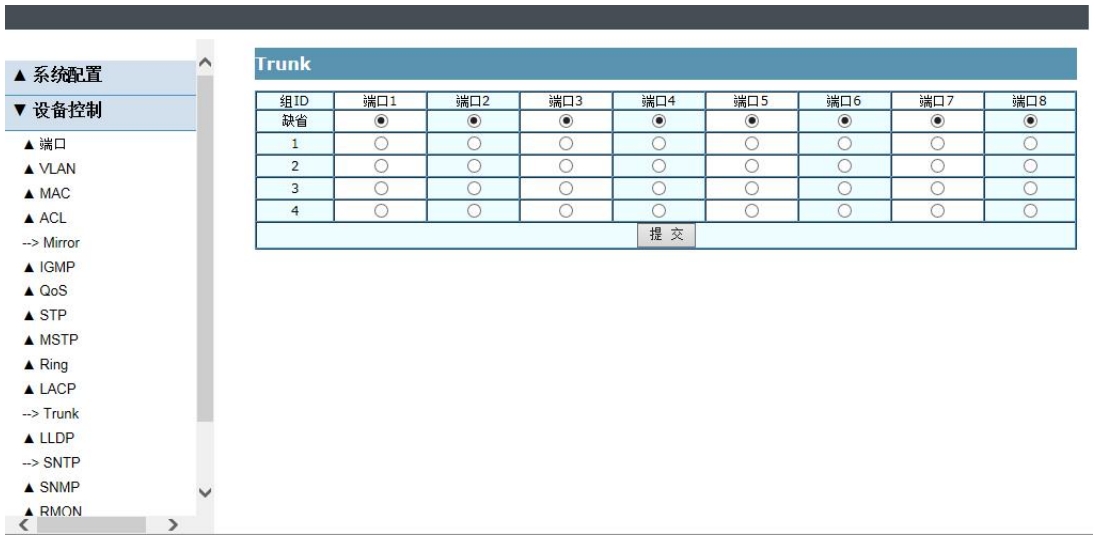
用于查看动态链路汇聚的数据统计信息，包括以下信息：

配置项	说明
端口	汇聚组包括的端口成员
Rx Frames	接收到对端系统的 LACP 数据帧数目。
Tx Frames	向对端系统发送的 LACP 数据帧数目。

Rx Unknown	接收到未知的 LACP 数据帧数目。
Rx Illegal	接收到非法的 LACP 数据帧数目。

5.11.5. TRUNK

点击导航栏“设备控制→Trunk”，即可进入 Trunk 配置界面，如下图：



此页面用于配置和查看静态汇聚的状态，最多支持 5 组，每组不少于两个端口或多于 8 个端口。当某个组的某单选框被选中时，表示该端口属于该静态汇聚组。当某端口属于缺省组时，表示该端口不是静态汇聚端口，默认情况下，所有端口都属于缺省组。

5.12. LLDP

5.12.1. LLDP 简介

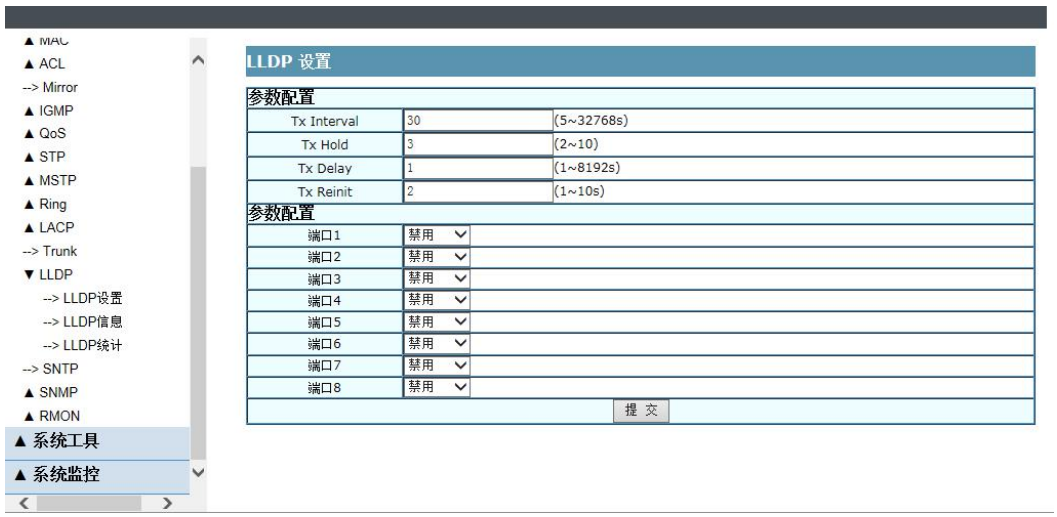
链路层发现协议（Link Layer Discovery Protocol，LLDP）是 802.1ab 中定义的新协议，它可使邻近设备向其他设备发出其状态信息的通知，并且所有设备的每个端口上都存储着定义自己的信息，如果需要还可以向与它们直接连接的近邻设备发送更新的信息，近邻的设备会将信息存储在标准的 SNMP MIBs。网络管理系统可从 MIB 处查询出当前第二层的连接情况。LLDP 不会配置也不会控制网络元素或流量，它只是报告第二层的配置。802.1ab 中的另一个内容是使网络管理软件利用 LLDP 所提供的信息去发现某些第二层的矛盾之处。IEEE 目前使用的是 IETF 现有的物理拓扑、接口和 Entity MIBs。与其他的草案标准一样，802.1ab 离正式成为网络设备和管理软件的一部分还有很长一段距离，但至少在现在，802.1ab 还是自动 Layer 2 Discovery 和更广泛的网络管理工具的最佳侯选。

简单说来，LLDP 是一种邻近设备发现协议。它为以太网网络设备，如交换机、路由器和无线局域网接入点定义了一种标准的方法，使其可以向网络中其他节点公告自身的存在，并保存各个邻近设备的发现信息。例如设备配置和设备识别等详细信息都可以用该协议进行公告。

具体来说，LLDP 定义了一个通用公告信息集、一个传输公告的协议和一种用来存储所收到的公告信息的方法。要公告自身信息的设备可以将多条公告信息放在一个局域网数据包内传输，传输的形式为类型长度值（TLV）域。

5.12.2. LLDP 设置

点击导航栏“设备控制→LLDP→LLDP 设置”，即可进入 LLDP 的 LLDP 设置界面，如下图：



本页面用于设置 LLDP 的传输延时、发送间隔、重新初始化时间间隔和 LLDP 端口的模式等。

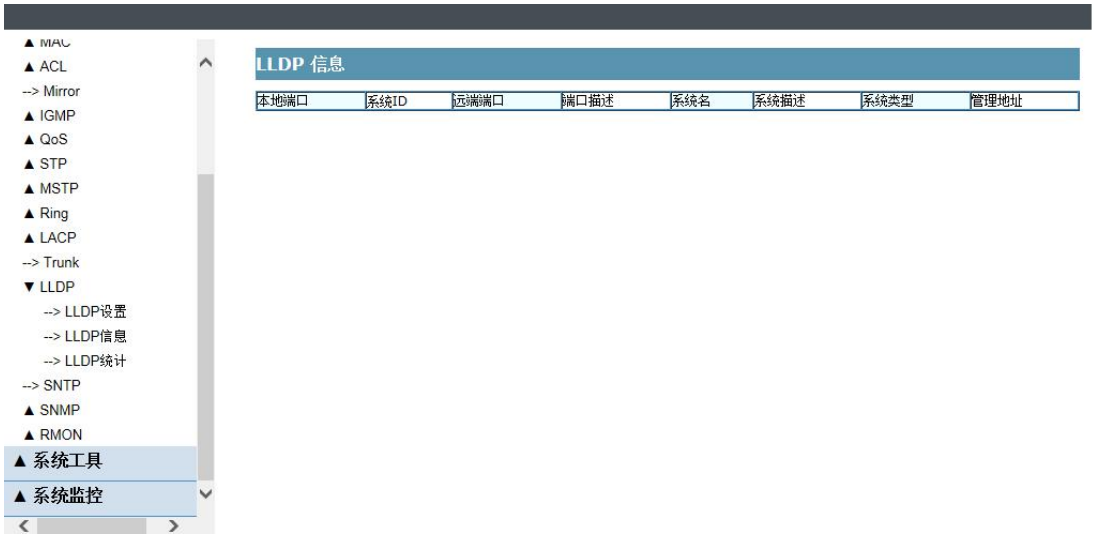
配置项	说明
Tx Interval	此参数用于设置交换机发送 LLDP 数据帧的周期，范围为 5~32768，系统默认为 30
Tx Hold	此参数用于设置 LLDP 信息老化时循环的次数，范围为 2~10，系统默认为 3
Tx Delay	此参数用于设置交换机发送 LLDP 数据帧的延时时长，范围为 1~8192，系统默认为 2
Tx Reinit	此参数用于设置 LLDP 端口的重新初始化的时长，范围为 1~10，系统默认为 2
禁用	选用此参数表示禁用端口的 LLDP 功能。
启用	选用此参数表示启用端口的 LLDP 功能。且此端口既可以发送自身的 LLDP 信息，也能识别对方发送过来的 LLDP 信息。
仅发送	选用此参数表示启用端口的 LLDP 功能。且此端口仅发送自身的 LLDP 信息，不能识别对方发送过来的 LLDP 信息。
仅接收	选用此参数表示启用端口的 LLDP 功能。且此端口既不能发送自身的 LLDP 信息，但可以识别对方发送过来的 LLDP 信息。

说明：在设置 Tx Delay 和 Tx Interval 参数时，应该遵循以下规则：

4×Tx Delay ≤ Tx Interval

5.12.3. LLDP 信息

点击导航栏“设备控制→LLDP→LLDP 信息”，即可进入 LLDP 的 LLDP 信息界面，如下图：



本界面用于查看 LLDP 端口的邻居设备信息。包括以下几个部分：

配置项	说明
本地端口	本设备启用 LLDP 功能的端口号
系统 ID	对端设备的 MAC 地址
远端端口	对应对端设备的端口号
端口描述	对端设备对应端口的描述
系统名	对端设备的系统名称
系统描述	对端设备的系统描述信息
系统类型	对端设备的系统类型，包括 Other、Repeater、Bridge、WLAN Access Point、Router、Telephone、DOCSIS cable device、Station only、Reserved 等。
管理地址	对端设备的 IP 地址，此 IP 地址链接到对端的 Web 管理界面，点击此链接就可以访问对端设备的 Web 管理界面。

5.12.4. LLDP 统计

点击导航栏“设备控制→LLDP→LLDP 统计”，即可进入 LLDP 的 LLDP 统计界面，如下图：

用于查看 LLDP 端口的统计信息，各参数描述如下：

配置项	说明
端口	LLDP 数据帧接收或发送的端口。
Tx Frames	在端口发出的 LLDP 数据帧数
Rx Frames	在端口接收的 LLDP 数据帧数
Rx Errors	已接收的 LLDP 数据帧中有某种错误的数量。
Rx Discarded	如果某个端口接收了 LLDP 数据帧，并且交换机的内部列表已经用完，则计算 LLDP 数据帧并将其丢弃。

5.13. SNTP

5.13.1. SNTP 简介

SNTP 是 Simple Network Time Protocol 的简称，RFC1769 详细定义了该协议的实现过程，简单网络时间协议（SNTP）是网络时间协议(NTP) 的一个改写本，NTP 协议适用于同步因特网上的计算机时钟。当不须要实现 RFC 1305 所描述的 NTP 完全功能的情况下，可以使用 SNTP。它能用单播方式(点对点)和广播方式(点对多点)操作。它也能在 IP 多播方式下

操作（可提供这种服务的地方）。SNTP 与当前及以前的 NTP 版本并没有大的不同。但它是更简单，是一个无状态的远程过程调用(RPC)，其准确和可靠性相似于 UDP/TIME 协议在 RFC868 描述中所预期的。

5.13.2. SNTP

点击导航栏“设备控制→SNTP”，即可进入 SNTP 界面，如下图：

本界面主要描述了各参数的显示和设置，各参数描述如下：

配置项	说明
模式	用于启用和禁用系统的 SNTP 功能
首选服务器	用于配置 SNTP 的首选服务器
备用服务器	用于配置 SNTP 的备用服务器
时区	用于设置系统的时区
系统时间配置	用于配置系统的日期和时间

5.14. SNMP

5.14.1. SNMP 简介

SNMP（Simple Network Management Protocol，简单网络管理协议），用于保证管理信息在网络中任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、定位故障、完成故障诊断、进行容量规划和生成报告。

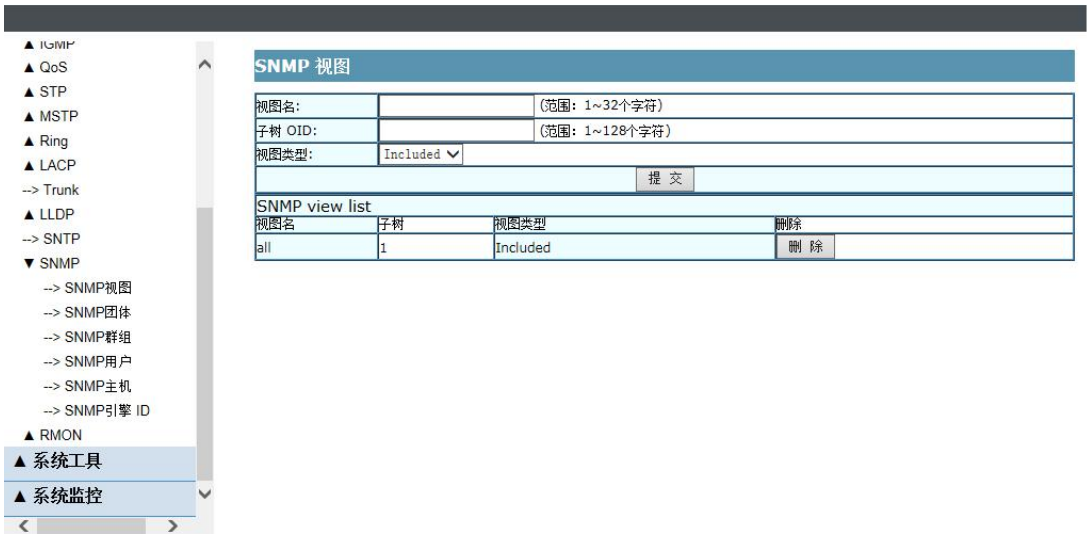
在典型的 SNMP 用法中，有许多系统被管理，而且是有一或多个系统在管理它们。每一个被管理的系统上有运行一个叫做代理者（agent）的软件组件，且透过 SNMP 对管理系统报告信息。

基本上，SNMP 代理者以变量呈现管理数据。管理系统透过 GET，GETNEXT 和 GETBULK 协议指令取回信息，或是代理者在没有被询问的情况下，使用 TRAP 或 INFORM 传送数据。管理系统也可以传送配置更新或控制的请求，透过 SET 协议指令达到主动管理系统的目的。配置和控制指令只有当网络基本结构需要改变的时候使用，而监控指令则通常是常态性的工作。

可透过 SNMP 存取的变量以阶层的方式结合。这些分层和其他元数据（例如变量的类型和描述）以管理信息库（MIBs）的方式描述。

5.14.2. SNMP 视图

点击导航栏“设备控制→SNMP→SNMP 视图”，即可进入 SNMP 视图界面，如下图：

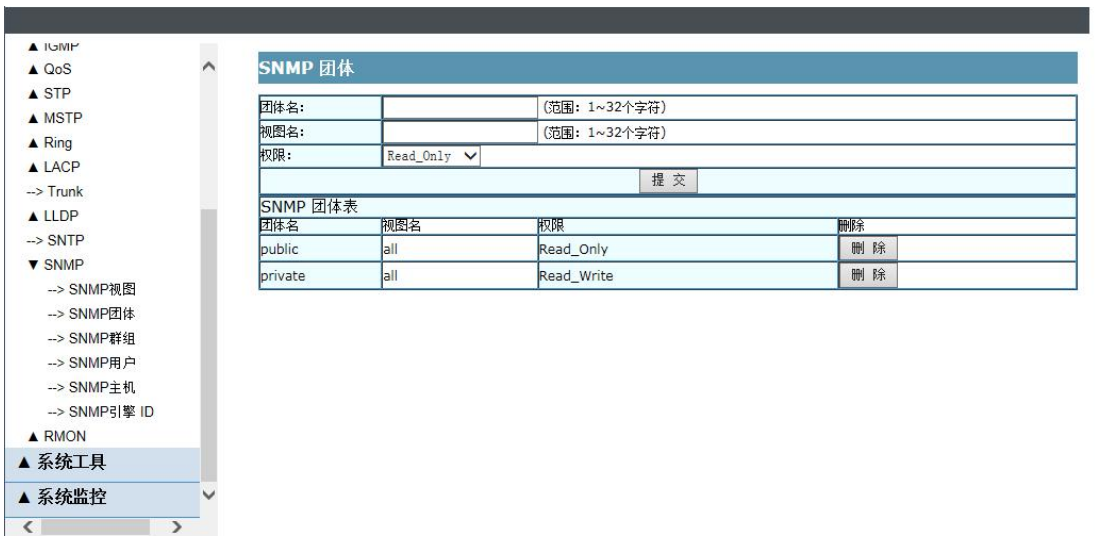


SNMP 配置界面中修改各项参数的解释如下表所示：

配置项	说明
视图名	创建由 1-32 位字母和数字组成的 SNMP 视图名。
子树 OID	用于识别对象树(MIB tree)的 ID。
视图类型	Included：表示包含子树 OID 确定的访问对象范围。 Excluded：表示在访问的对象范围中，不包含子树 OID 确定的访问对象范围。

5.14.3. SNMP 团体

点击导航栏“设备控制→SNMP→SNMP 团体”，即可进入 SNMP 团体界面，如下图：



SNMP 团体界面中修改各项参数的解释如下表所示：

配置项	说明
团体名	用于识别 SNMP 团体成员。
视图名	用于识别远程 SNMP 管理员访问交换机上 MIB 对象库。
权限	使得 SNMP 的团体成员仅允许读取或修改交换机上的 MIB 信息，分为 Read_Only 只读方式和 Read_Write 读写方式。

5.14.4. SNMP 群组

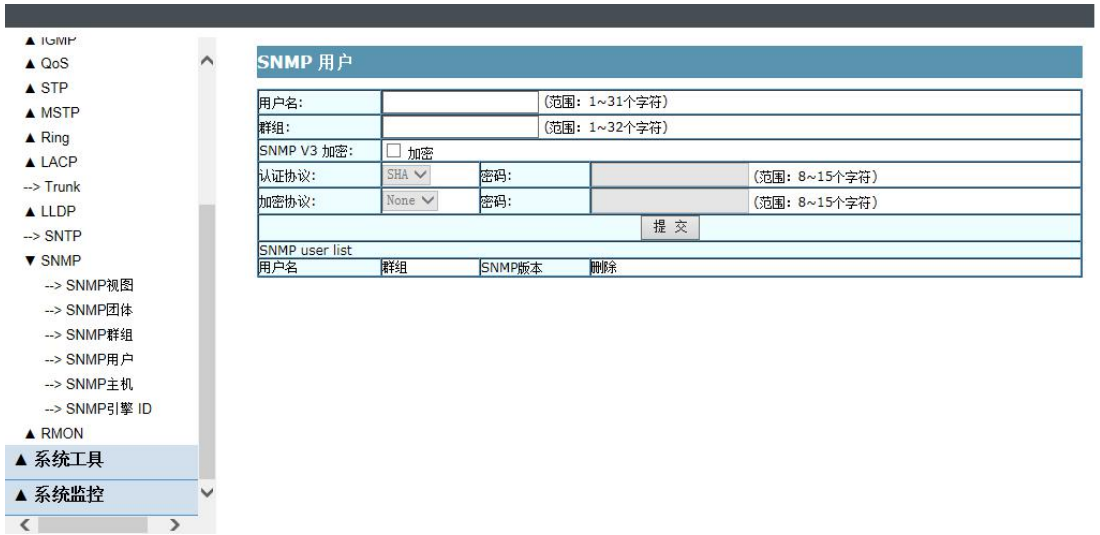
点击导航栏“设备控制→SNMP→SNMP 群组”，即可进入 SNMP 群组界面，如下图：

SNMP 群组界面中修改各项参数的解释如下表所示：

配置项	说明
群组	用于识别与 SNMP user 关联的 SNMP 群组。
只读视图	已经创建的 SNMP 群组可以发送 SNMP 读取请求
读写视图	已创建的 SNMP 群组有修改的特权
告警视图	已创建的 SNMP 群组可以在交换机的 SNMP 代理上接收到 SNMP trap 信息
安全模式	用于识别与 SNMP user 关联的 SNMP 群组。
安全等级	决定 SNMP 信息是否来自有效源。

5.14.5. SNMP 用户

点击导航栏“设备控制→SNMP→SNMP 用户”，即可进入 SNMP 用户界面，如下图：

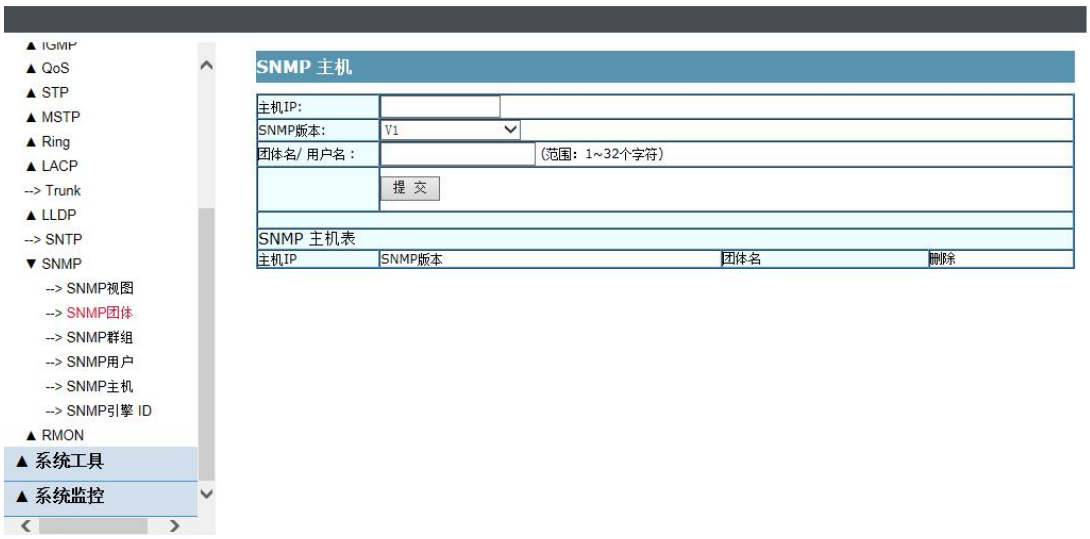


SNMP 用户界面中修改各项参数的解释如下表所示：

配置项	说明
用户名	用于识别新的 SNMP 用户
群组	用于新的 SNMP 用户与其关联
SNMP V3 加密	允许此用户使用 SNMP V3 认证，并选择一种认证方式
认证协议	用户可以选择一种认证算法对 SNMP 用户进行认证，包括 MD5 和 SHA 方式
加密协议	通过添加私有参数来进行加密，包括 DES 方式。

5.14.6. SNMP 主机

点击导航栏“设备控制→SNMP→SNMP 主机”，即可进入 SNMP 主机界面，如下图：



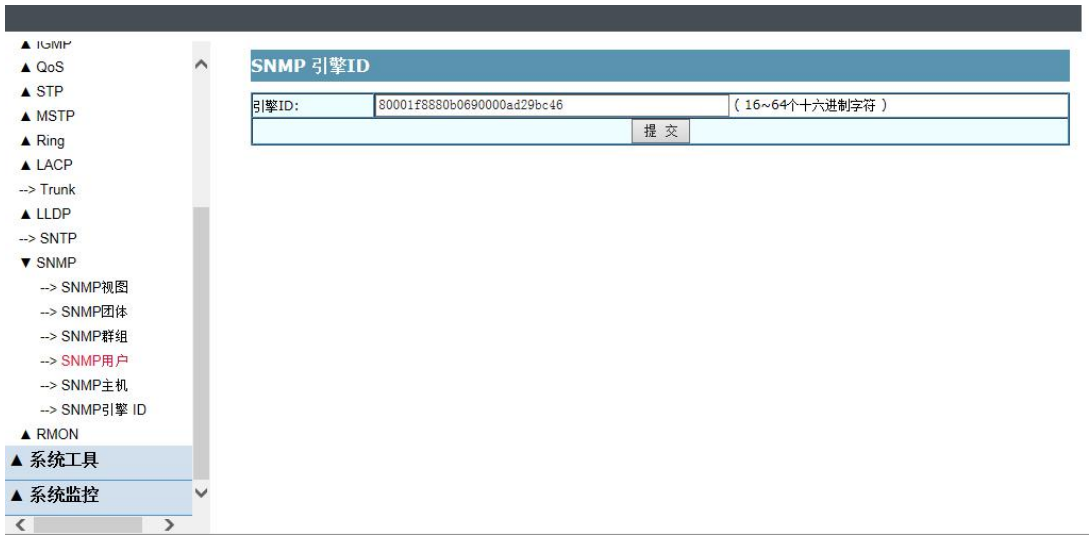
SNMP 主机界面中修改各项参数的解释如下表所示：

配置项	说明
主机 IP	远程管理站的 IP 地址，通常当作交换机的 SNMP 主机
SNMP 版本	表示使用 SNMP v1 还是 v2c 版本

团体名	用于识别 SNMP 的 trap 接收主机

5.14.7. SNMP 引擎 ID

点击导航栏“设备控制→SNMP→SNMP 引擎 ID”，即可进入 SNMP 引擎 ID 界面，如下图：



SNMP 引擎 ID 配置界面中修改各项参数的解释如下表所示：

配置项	说明
引擎 ID	用来设置交换机的 SNMP 引擎名，范围为 16~64 位的十六进制字符。

5.15. RMON

5.15.1. RMON 简介

RMON 是 Remote Monitoring MIBs 的简称，一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。 RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。

RMON 最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON 规范是由 SNMP MIB 扩展而来。 RMON 中，网络监视数据包含了一组统计数据和性能指标，它们在不同的监视器（或称探测器）和控制台系统之间相互交换。结果数据可用来监控网络利用率，以用于网络规划，性能优化和协助网络错误诊断。

当前 RMON 有两种版本： RMON v1 和 RMONv2 。 RMON v1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控； RMON v2 是 RMON 的扩展，专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。 RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 及其以下层的信息包。

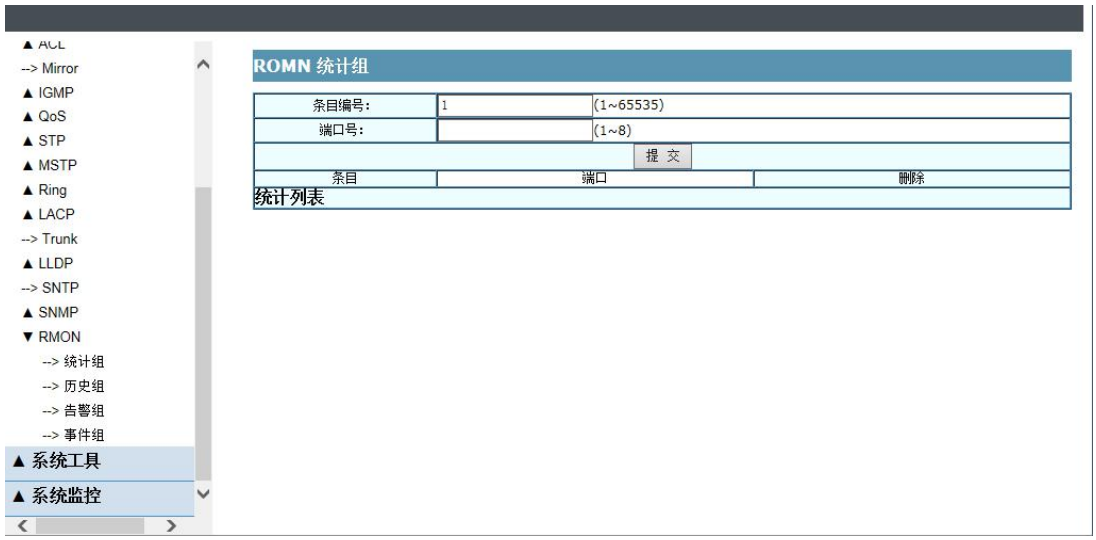
RMON 监视系统有两部分构成：探测器（代理或监视器）和管理站。 RMON 代理在 RMON MIB 中

存储网络信息，它们被直接植入网络设备（如路由器、交换机等），代理也可以是 PC 机上运行的一个程序。代理只能看到流经它们的流量，所以在每个被监控的 LAN 段或 WAN 链接点都要设置 RMON 代理，网管工作站用 SNMP 获取 RMON 数据信息。

RMON MIB 有不少变种。例如，令牌网 RMON MIB 提供了针对令牌网网络管理的对象。SMON MIB 是由 RMON 扩展而来，主要用来为交换网络提供 RMON 分析。

5.15.2. 统计组

点击导航栏“设备控制→RMON→统计组”，即可进入 RMON 统计组界面，如下图：

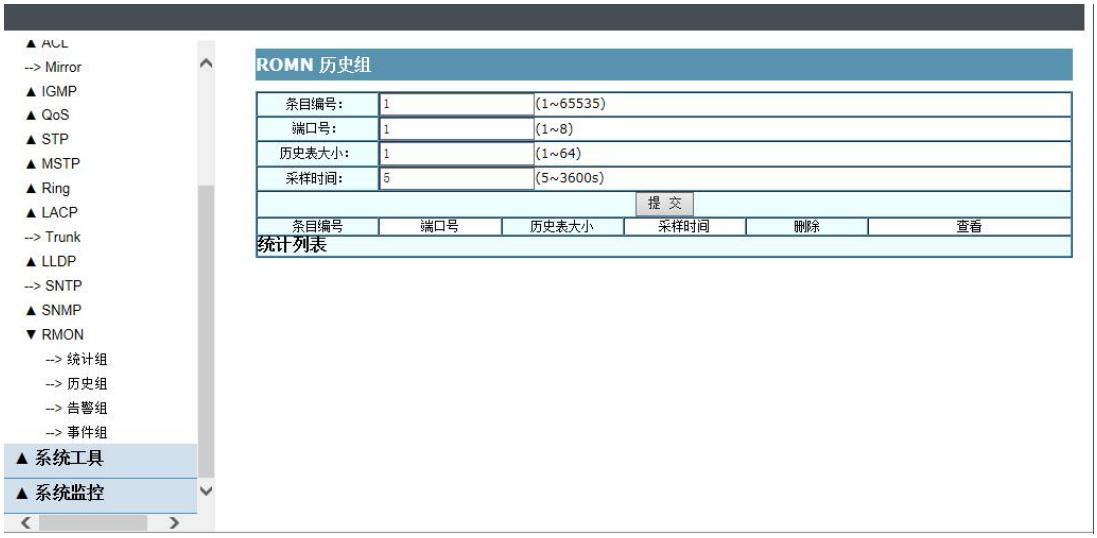


ROMN 统计组界面中修改各项参数的解释如下表所示：

配置项	说明
端口号	交换机端口的逻辑编号，范围是 1~9
条目编号	统计组的索引号，范围是 1~65535。

5.15.3. 历史组

点击导航栏“设备控制→RMON→历史组”，即可进入 RMON 历史组界面，如下图：

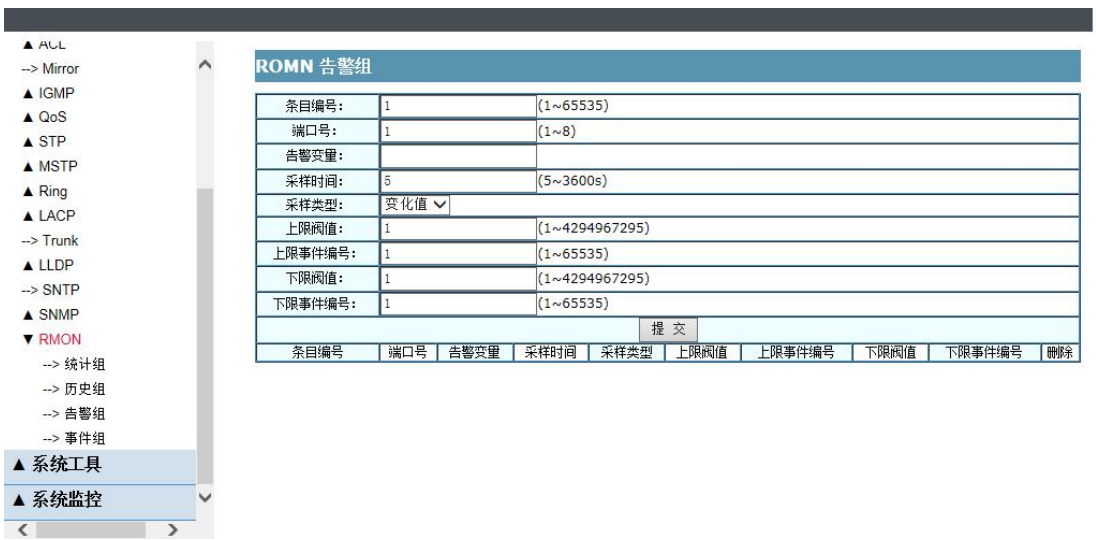


ROMN 历史组界面中修改各项参数的解释如下表所示：

配置项	说明
端口号	交换机端口的逻辑编号，范围是 1~9
条目编号	历史组的索引号，范围是 1~65535。
历史表大小	该条目对应历史表容量。取值范围为 1～65535
采样时间	采样时间长度，取值范围为 5～3600，单位为秒

5.15.4. 告警组

点击导航栏“设备控制→RMON→告警组”，即可进入 RMON 告警组界面，如下图：



ROMN 告警组界面中修改各项参数的解释如下表所示：

配置项	说明
条目编号	告警组的索引号，取值范围为 1～65535。
告警变量	字符串类型，长度为 1～256，格式为节点 OID 的点分格式，如 1.3.6.1.2.1.2.1.10.1，只有可以解析为 ASN.1 中 INTEGER (INTEGER, Counter, Gauge, or TimeTicks)的数据类型的变量才能

	作为告警变量。
采样时间	采样时间长度，取值范围为 5～3600，单位为秒
采样类型：	变化值：采样类型为变化值（选定变量的当前采样值相对于最近一次采样值的变化量）。 绝对值：采样类型为绝对值。
上限阀值	设置的上限值，取值范围为～4294967295
上限事件号	上限阈值相应的事件号，取值范围为 1～65535。
下限阀值	设置的下限值，取值范围为 1～4294967295。
下限事件号	下限阈值相应的事件号，取值范围为 1～65535。

5.15.5. 事件组

点击导航栏“设备控制→RMON→事件组”，即可进入 RMON 事件组界面，如下图：

ROMN 事件组界面中修改各项参数的解释如下表所示：

配置项	说明
条目编号	事件组的索引号，取值范围为 1～65535。
事件描述	事件的描述，字符串，长度为 1～32 个字符。
事件类型	事件的操作方式，分为 none、log、trap 和 log_trap。 log：日志事件。 trap：定义事件为 Trap 事件。 log-trap：定义事件为日志和 Trap 事件。 none：不产生动作的事件。
事件团体名	接收事件消息的网管站的团体名属性，字符串，长度为 1～32 个字符。

第 6 章 系统工具

6.1. 系统重启

点击导航栏“系统工具→系统重启”，即可进入系统重启界面，如下图：

点击“重启”按钮，系统会弹出确认对话框，如下图：

点击确定就会重启系统，此时，若设置的配置没有保存，重启后这些配置就会丢失。若想取消重启，则点击“取消”按钮即可。

6.2. 出厂设置

点击导航栏“系统工具→出厂设置”，即可进入出厂设置界面，如下图：

点击“恢复出厂值”按钮，系统会弹出确认对话框，如下图：

点击确定就会将系统恢复到出厂设置，但 IP 地址保持不变。若想取消此操作，则点击“取消”按钮即可。

6.3. 软件升级

点击导航栏“系统工具→软件升级”，即可进入软件升级界面，如下图：

这里的升级方式是 TFTP 方式，因此需要 TFTP Server 的支持，在架设好 TFTP Server 后，填写下列各参数的值即可进行升级：

配置项	说明
TFTP Server IP	TFTP Server 的 IP 地址，这里需要注意，TFTP Server 和交换机能够正常通讯。
文件名	升级文件的文件名，通常使用 vxWorks.Z。

6.4. 配置管理

点击导航栏“系统工具→配置管理”，即可进入配置管理界面，如下图：

配置管理也需要 TFTP Server 的支持，配置备份就是将存储在 flash 中的配置文件上传到 TFTP Server 中；配置恢复就是将 TFTP Server 中的配置文件下载到 flash 中。

配置项	说明
TFTP 服务器 IP	TFTP Server 的 IP 地址，这里需要注意，TFTP Server 和待升级的交换机能够正常通讯。
备份文件名	升级文件的文件名。

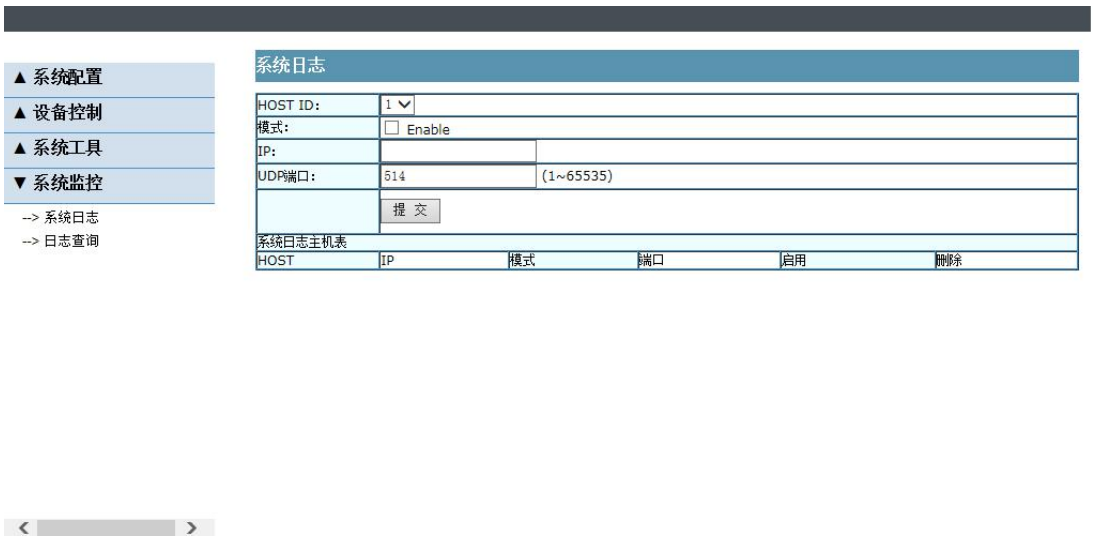
说明：

1. 备份配置文件时，需要先进行配置保存。
2. 恢复配置后，需要重启交换机才能使恢复的配置生效。

第 7 章 系统监控

7.1. 系统日志

点击导航栏“系统监控→系统日志”，即可进入系统日志界面，如下图：

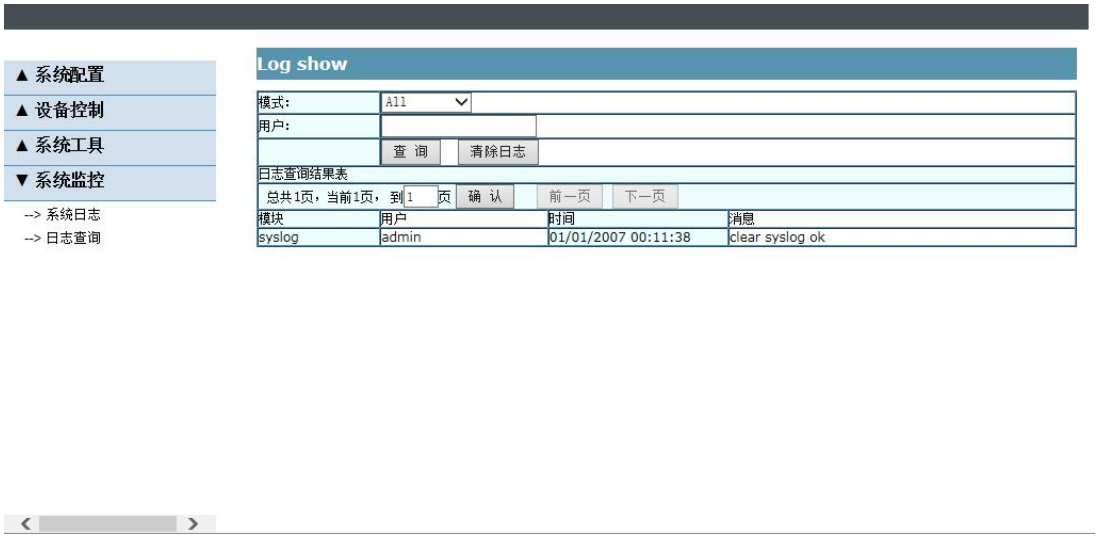


系统日志界面中修改各项参数的解释如下表所示：

配置项	说明
模式	用于设置是否启用该日志服务器
IP	用于设置日志服务器的 IP 地址
UDP 端口	用于设置系统日志所用的 UDP 端口
HOST	用于设置创建的日志服务器的编号
启用	用于启用或禁用该日志服务器
删除	删除该日志服务器

7.2. 日志查询

点击导航栏“系统监控→日志查询”，即可进入日志查询界面，如下图：



日志查询界面中修改各项参数的解释如下表所示：

配置项	说明
模式	设置按功能模块查询的查询条件。
用户	设置按用户类型查询的查询条件，可以和模式结合使用。
查询	根据模式和用户查询日志。
清除日志	清除所有日志信息。

第 8 章 附录

8.1. 出厂默认值

以下信息都是各个功能在出厂时的默认值，各个功能的参数详细描述如下：

8.1.1. 系统设置

系统信息：

联系方式：www.wintoptec.com.cn

设备名称：RS606（随产品型号的不同而不同）

公司地址：NanShan, Shenzhen, China

IP 地址：

DHCP：禁用状态。

IP 地址：192.168.1.254

子网掩码：255.255.255.0

网关：0.0.0.0

首选 DNS：202.96.134.133

备用 DNS：0.0.0.0

管理 VLAN：1

用户设置：

管理用户：admin；密码：admin；

普通用户：guest；密码：guest；

8.1.2. 功能设置

端口：

状态：启用

配置模式：自适应

流控：禁用

丢弃模式：None

VLAN:

所有端口属于 VLAN 1，且不能删除。

MAC:

MAC 地址老化时间默认 300s。

ACL：

默认为禁用状态。

Mirror：

默认为禁用状态。

IGMP：

默认为禁用状态。

QoS：

默认为禁用状态。

端口限速默认为禁用状态。

风暴控制默认将未知单播和广播抑制到 1M。

STP:

所有端口的 STP 都默认为禁用状态。

MSTP：

默认为禁用状态。

WTOP_RING:

默认为禁用状态。

LACP:

默认为禁用状态。

Trunk:

默认为禁用状态。

LLDP:

默认为禁用状态。

SNTP:

默认为禁用状态。

SNMP:

SNMP V 1 和 SNMP V2c 默认情况下可以使用团体名 public 和 private 进行访问。

SNMP V3 默认情况下不能使用。

RMON：

默认为禁用状态。

8.2. 专业术语介绍

1. ACL

ACL（Access Control List，访问控制列表)，其访问控制条目可用来对单个用户或群组，设置允许或拒绝特定的流量对象，如某个过程或项目。每个流量对象包含了 ACL 的标识符。这些权限决定了特定的流量对象是否有访问权限。ACL 的应用相对比较复杂，比如，对不同的情况，ACE 需要分清优先次序。在网络中，ACL 会参照主机或服务器上可用的服务端口和网络服务单，上面列举了主机和服务器可允许或拒绝使用的服务。通常，可设置 ACL 来控制网络内的流量，从这个角度来说，ACL 相当于防火墙。

2. 汇聚

使用多个平行端口增加单端口局限的链路速度，和增加更高可用的冗余。同时也叫端口汇聚，或链路汇聚。

3. ARP

ARP（Address Resolution Protocol，地址解析协议)，该协议用于转换 IP 地址到物理地址，如以太网地址。只有知道邻居的因特网地址，ARP 才可允许主机与其他的主机通讯。在使用 IP 之前，主机会发送一个 ARP 请求广播数据包，其中包含了欲到达目的系统的因特网地址。

4. 自适应

自适应是两个不同设备间建立操作模式和速度设置以供链路共享的过程。

5. DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议)，该协议用于分配动态 IP 地址到网络中的设备。网络中的电脑（客户端）使用 DHCP 来获取 IP 地址和其他参数，例如默认网关，子网掩码和 DNS 服务器的 IP 地址。DHCP 服务器确保所有的 IP 地址是唯一的，比如，当第一个客户分配到了有效的 IP 地址（租期未过期)，则该 IP 地址将不会再分配到第二个客户端上。因此，IP 地址池是由 DHCP 服务器，而不是由网管来管理。

6. DNS

DNS（Domain Name System，域名系统)，它存储和关联域名的多种信息类型。更重要的是，DNS 将域名和电脑主机名转换成 IP 地址。比如，域名 www.example.com 可能转换成 192.168.0.1。

7. Dotted Decimal Notation

Dotted Decimal Notation 指使用十进制小数和圆点来分割字节表示 IP 地址的一种方式。IPv4 的点十进制地址采用的格式为 x.y.z.w, 其中 x, y, z 和 w 是间于 0～255 的十进制数。

8. DSCP

DSCP 是由 Differentiated Services Code Point 首写字母而组成。它是 IP 包头的一个字段，由以太网的网络标准定义。可用来表示在以太网的数据帧中正在传输的协议。

9. Ethernet Type

Ethernet Type 是以太网 MAC 地址头部的一个字段，由以太网网络标准定义。用于显示传输以太网数据帧中的协议类型。

10. FTP

FTP（File Transfer Protocol，文件传输协议)，它是一种传输协议，结合传输控制协议（TCP）并提供文件的读写。同时也提供了目录服务和安全特征。

11. HTTP

HTTP（Hypertext Transfer Protocol，超文本传输协议)，这种协议用于在万维网传输或传送信息。HTTP 定义了信息采用的格式和传输方式，以及 Web 服务器和浏览器对不同需求应采取的操作。比如，当您在浏览器中输入一个 URL，实际上是发送了一个 HTTP 命令到 Web 服务器，Web 服务器收到该命令后发送所需的 Web 页面。控制万维网是如何工作的另一个主要标准是 HTML，它包含了 Web 页面是如何形成和显示的。任何 Web 服务器，除了 Web 页面文件，还包含了一个 HTTP daemon 后台程序。这个后台程序的设计就是等待 HTTP 的请求，然后在到达之后处理它们。Web 浏览器是一个 HTTP 的客户端，用于发送请求到服务器。通过在远程主机（默认为 80 端口）建立传输控制协议（TCP）连接到特定端口，HTTP 客户端可创建一个请求。则 HTTP 服务器会听取那个端口，并等待客户端发送的请求信息。

12. HTTPS

HTTPS（ Hypertext Transfer Protocol over Secure Socket Layer，超文本传输协议安全套接字层)，用于表示 HTTP 的安全连接。HTTPS 提供了认证和加密通讯，并大范围的使用在万维网上，用于安全敏感较高的通讯，如支付业务和法人登录。HTTPS 实际上就是使用 Netscape 的安全套接字层（SSL）作为子层放在常规的 HTTP 应用层下。在其与低层（TCP/IP）的通信中， HTTPS 使用的是 443 端口，而不是 HTTP 的 80 端口。）SSL 使用 40 位的密钥用于 RC4 流加密算法，对商业交易保障了充分的安全系数。

13. ICMP

ICMP（Internet Control Message Protocol，因特网控制信息协议)，该协议可生成错误回复，诊断或路由目的。ICMP 信息通常包含如路由困难或简单交互（时间戳或回复处理）的信息。比如，PING 命令就是使用 ICMP 来诊断网络的连接。

14. IGMP

IGMP（Internet Group Management Protocol，网络群组管理协议) ，它是一种通信协议用于管理网络协

议多播群组会员资格。IP 主机和相邻的多播路由器使用 IGMP 来建立多播群组会员资格。如同用于单播连接的 ICMP，IGMP 也仅是 IP 多播规范中的一部分。IGMP 也可用于在线视频和游戏，以允许资源更高效的使用。

15. IGMP Querier

路由器在特定链路上发送的 IGMP 询问信息。该路由器就叫做 Querier。

16. IP

IP（Internet Protocol，网际协议)，该协议用于在因特网网络中的数据通信。IP 是一个“最大努力”系统，意思就是说，没有数据包在网络上发送时，能保证在相同条件下到达目的地。与局域网或广域网相连的每个设备都有分配了一个网际协议地址。该 IP 地址用于在扩展网络上相连的其他设备中能唯一的标识。

当前使用的网际协议版本为 IPv4，这种 32 位的 IP 地址可以允许超过四百万个唯一的地址。由于 Web 站点管理员在区间大量的使用地址，其数量在急剧的减少，但是一些主干地址还仍未使用。所以逐渐推行新的网际协议版本 IPv6，它是 128 位的 IP 地址。但是，IPv4 依然是大多数网络选择的协议。

17. LACP

LACP 是 IEEE 802.3ad 的标准协议。链路汇聚控制协议可以捆绑多个物理端口而形成一个单独的逻辑端口。

18. LLDP

LLDP 是 IEEE 802.1ab 标准协议。链路层发现协议用于网络邻居设备发现，并与网络中邻居设备使用 LLDP 数据帧交互信息。

19. MAC Table

数据帧的转发是基于数据帧中的 DMAC 地址。交换机内建了一张表格，将 MAC 地址和交换端口作了一一对应。这样数据帧就知道从哪个端口转发。这个列表中包含了静态和动态条目。如果管理员需要在 DMAC 地址和交换机端口作静态映射，静态条目则由网络管理员来设置。

数据帧中也包含了 MAC 地址（SMAC 地址），显示的就是发送数据帧设备的 MAC 地址。交换机根据 SMAC 地址自动更新 MAC 地址表和动态 MAC 地址。如果在一段老化时间后没有看到相应 SMAC 地址的数据帧，则动态条目将从 MAC 地址表中移除。

20. 镜像

为了调试网络中的问题和监控网络流量，可设置交换机系统监控来自多个端口的数据帧到镜像端口。镜像数据帧在此等同于复制数据帧。入站（源）数据帧和出站（目的）数据帧都可以被镜像到镜像端口。

21. PING

Ping 就是指在网络或因特网上发送一系列的数据包到指定的计算机上，以便从该计算机上得到回复。计算机在收到 ping 发出的数据包后，会回复该计算机。使用 Ping 的目的就是核实是否网络上或因特网上的某计算机是否存在或连接上。Ping 使用的是网络控制信息协议（ICMP）的数据包。从源计算机上发出 Ping 请求数据包，从目的回应 Ping 回复数据包。

22. POP3

POP3（Post Office Protocol version 3，邮局协议版本 3)，该协议可对邮件用户从邮件服务器找回邮件信

息。只要用户下载了邮件，POP3 就可以把邮件从服务器上删除。但是，有些执行可允许用户或管理员来设置邮件保存一段时间。因此，POP 可以认为是“存储和转发”的服务。另外一个协议是网络信息访问协议 IMAP。IMAP 为用户提供了将邮件保留在服务器上的更多容量，并将它们组织在一起，放到服务器的文件夹中。IMAP 可以认为是远程文件服务器。POP 和 IMAP 应对的是邮件的接收，而并不会与 SMTP 混为一谈。您可以通过 SMTP 发送邮件，然后邮件处理员以接收者的身份接受该邮件。使用 POP 或 IMAP 来读取该邮件。IMAP4 和 POP3 是邮件重现的两个常见的网络标准协议。事实上，现代的邮件客户端和服务器通常都支持这两种协议。

23. QoS

QoS（Quality of Service ，QoS 服务质量) ，其保证了单个应用程序间或协议间的带宽关系。在通信网络上，传输着多个应用程序和数据，包含了高质量的视频和对延迟很敏感的数据，如实时语音。因此，网络必须要提供安全和有保障的服务。实现所需要的服务质量成为了端到端商务解决方案的成功的秘诀。所以，通过有技巧的设置 QoS，即可管理网络资源。

24. RARP

RARP(Reverse Address Resolution Protocol ,逆地址解析协议)，该协议用于从硬件地址获取 IP 地址，如以太网地址。RARP 是 ARP 协议的补充。

25. 路由端口

路由端口是以太网交换机上的一个端口，用于引导交换机面向 3 层多播设备。

26. RSTP

1998 年，IEEE 的 802.1w 文件引入了 STP 的升级版：快速生成树协议，在拓扑发生改变后，它提供了更快的生成树收敛时间。标准 IEEE 802.1D-2004 整合了 RSTP 和 STP，同时向后兼容 STP。

27. SNMP

SNMP（Simple Network Management Protocol ，简单网络管理协议)，它是用于管理的 TCP/IP 协议中的一部分。SNMP 允许逆向网络对象加入网络管理架构。它启用网络管理系统接收 trap 信息或通告来了解网络中的问题。

28. SNTP

SNTP（Simple Network Time Protocol，简单网络时间协议) ，这种网络协议可同步计算机系统的时钟。SNTP 使用的是传输层的 UDP datagrams 报文。

29. STP

生成树是 OSI 的二层协议，对所有桥接的局域网，可确保无环路的拓扑结构。随着 RSTP 的出现，原 STP 协议逐渐作废。

30. Tag Priority

标记优先级是 802.1Q 数据帧中的一个 3 位字段，当中存储的是优先级别。

31. TCP

TCP（Transmission Control Protocol，传输控制协议)，它是一种通信协议，结合网际协议(IP)在计算机间交互信息。

32. TELNET

TELNET（TELetype NETwork），它是一种终端仿真协议，使用的是 TCP 协议并提供了在 TELNET 服务器和 TELNET 客户端间的虚拟连接。

33. TFTP

TFTP（Trivial File Transfer Protocol，简单文件传输协议），大家可以从它的名称上看出，它适合传送“简单”的文件。与 FTP 不同的是，它使用的是 UDP 的 69 端口，因此它可以穿越许多防火墙。不过它也有缺点，比如传送不可靠、没有密码验证等。虽然如此，它还是非常适合传送小型文件的。

34. ToS

ToS（Type of Service ，服务类型），是 3 个 bit，范围 0-7，同样可当作优先级标记，另外 5 个实际指示 Delay，ThrouWTOPput，Reliability 等特性的 bit 位一般没有使用，现在为了更好的控制数据流分类，使用 DSCP（Differential Services Code Point），扩展了 ToS 的后三个 bit，因此，范围是 0-63。在实施 QoS 策略时，Cos 与 ToS 或 DSCP 之间通常要做映射机制。

35. UDP

UDP（User Datagram Protocol ，用户数据报文协议），它是一种通信协议，结合网际协议(IP)在计算机间交互信息。

36. User Priority

User Priority (用户优先级) 是 802.1Q 数据帧中的一个 3 位字段，当中存储的是优先级别。

37. VLAN

虚拟局域网是交换端口间限定通信的一种方式。

38. VLAN ID

VLAN ID 是一个 12 位(bit)的字段，用于描述数据帧属于哪个 VLAN。

订货须知

订货应注明：

1) 产品型号、名称、订货数量；
2) 交流电压、频率额定值；
3) 直流电源额定值；
4) 通信接口方式，采样单模光纤时必须特别说明；
5) 收货地址及时间；
6) 组屏要求及屏的尺寸及色标；
7) 用户要求配合事项；
8) 特别声明事项。

中国　深圳
深圳市源拓光电技术有限公司
Shenzhen Wintop Optical Technology CO.，LTD.
地址：深圳市宝安区石岩街道石龙仔社区森海诺科创大厦 12 楼
邮编：　528109
电话：（0755）26641737
传真：（0755）26640197
网址：　http://www.wintoptec.com
E-mail ：market @ wintoptec.com