源拓光电

RS6016 百兆系列
工业以太网交换机

WEB 说明书

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 RS6016 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 RS6016 百兆系列工业以太网交换机 V2.0 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	V2.0	修正本文中的错误描述	V1.2	2016/06
2	V1.2	修正本文中的错误描述	V1.1	2016/04
1	V1.1	RS6016 百兆系列工业以太网交换机说明书	V1.0	2015/12

* 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

安全声明 **2**
版本声明 **3**
第一章 概述 **1**
1.1. 性能特点 1
第二章 技术性能及指标 **1**
2.1. 电源系统 1
2.2. 主要技术性能及指标 1
2.3. 绝缘和耐湿热性能 3
2.4. 电磁兼容性能 3
2.5. 机械性能 4
2.6. 环境大气条件 4
第三章 硬件结构说明 **5**
3.1. 面板端子 5
3.2. 电源、告警连接端子示意图 6
3.3. 告警继电器输出端子 6
3.4. 安装方式 7
第四章 使用说明 **9**
4.1. Web 登录 9
4.2. 系统配置 9
4.3. 用户设置 11
4.4. IP 地址 12
第五章 Mirror **12**
5.1. 简介 12
5.2. 配置说明 13
第六章 SNTP **14**
6.1. SNTP 简介 14
6.2. SNTP 14
第七章 TRUNK **15**
第八章 告警 **15**
8.1. 简介 15
8.2. 告警设置 15
第九章 DoS 攻击防御 **16**
第十章 GMRP 设置 **16**
10.1. GMRP 定义 16
10.2. GMRP 的配置 16

第十一章 非法 IP 地址配置 17
第十二章 端口 17
12.1. 端口设置 17
12.2. 端口统计 18
12.3. 端口安全 20
12.4. VLAN LIMIT 21
第十三章 VLAN 21
13.1. 概述 21
13.2. 划分策略 21
13.3. VLAN 的成员配置 22
13.4. VLAN 的端口配置 22
第十四章 MAC 23
14.1. 单播 23
14.2. 多播 24
第十五章 QoS 24
15.1. QoS 概述 24
15.2. 常用优先级介绍 25
15.3. 队列调度介绍 25
15.4. 系统配置界面 26
15.5. 优先级配置界面 26
15.6. 端口限速界面 27
15.7. 风暴控制界面 28
第十六章 STP 29
16.1. 生成树简介 29
16.2. 系统配置 30
16.3. 端口配置 30
16.4. 端口状态 31
16.5. 数据统计 33
第十七章 MSTP 33
17.1. 概述 33
17.2. 桥配置信息 33
17.3. 桥端口配置和状态 34
17.4. CIST 配置信息 35
17.5. CIST 端口配置和状态 35
17.6. MSTI 配置信息 36
17.7. MSTI 端口配置和状态 37
17.8. Vlan 表配置 38

17.9. MSTP 数据统计.....38
第十八章 WTOP_RING.....39
18.1. 概述.....39
18.2. 端口配置.....42
第十九章 ACL.....45
19.1. 概述.....45
19.2. ACL 列表配置.....45
19.3. ACL 端口配置.....46
19.4. Ip Rule 配置.....47
第二十章 802.1X.....47
20.1. 简介.....47
20.2. 802.1X 系统配置.....47
20.3. 802.1X 本地认证.....47
20.4. 802.1x 端口配置.....48
20.5. 802.1X 端口统计.....48
第二十一章 IGMP.....48
21.1. IGMP 原理.....48
21.2. IGMP 配置.....49
21.3. IGMP 状态及统计.....49
21.4. IGMP 组.....50
第二十二章 LACP.....50
22.1. 链路汇聚简介.....50
22.2. LACP 配置.....50
22.3. LACP 信息.....51
22.4. LACP 统计.....52
第二十三章 LLDP.....52
23.1. LLDP 简介.....52
23.2. LLDP 设置.....53
23.3. LLDP 信息.....54
23.4. LLDP 统计.....54
第二十四章 SNMP.....55
24.1. SNMP 简介.....55
24.2. SNMP 视图.....55
24.3. SNMP 团体.....56
24.4. SNMP 群组.....56
24.5. SNMP 用户.....57
24.6. SNMP 主机.....57

24.7. SNMP 引擎 58
第二十五章 RMON 58
25.1. RMON 简介 58
25.2. 统计组 58
25.3. 历史组 59
25.4. 告警组 59
25.5. 事件组 60
第二十六章 系统工具 61
26.1. 系统重启 61
26.2. 出厂设置 61
26.3. 软件升级 62
26.4. 配置管理 62
26.5. 系统日志 63
26.6. 系统日志查询 63
第二十七章 装置调试大纲 64
27.1. 装置检查 64
27.2. 性能测试 64
27.3. 配置备份及恢复 64
第二十八章 订货须知 65

第一章 概述

RS6016 百兆系列工业以太网交换机适用于常规及智能变电站综合自动化系统、电厂监控系统、工业控制系统等领域。

RS6016 百兆系列工业以太网交换机产品的设计制造充分考虑了工业应用环境中各种恶劣条件和干扰因素，可保证数据在严苛环境下可靠传输。

RS6016 百兆系列工业以太网交换机包含 RS6016-16T：提供 16 个百兆电口，具有 IP40 等级防护的铝壳。

1.1. 性能特点

1) 全面工作状态指示灯，提供各个端口的活动信号以及运行、告警信号指示；
2) 全面符合 IEEE802.3 和 IEEE802.3u、IEEE 802.3z 等标准并支持 VLAN（802.1Q）以及 GMRP、SNTP 等功能协议；
3) 提供丰富的 QoS（802.1p）特性、灵活的用户业务安全特性，满足工业级以太网业务低时延抖动、高可靠性要求；
4) 提供多种网络冗余解决方案：支持 STP（802.1D）、RSTP（802.1w）、MSTP（802.1s）网络协议，支持链路聚合功能；
5) 支持双电源模块冗余运行；提供一组告警空接点实现电源模块告警和交换机告警功能；
6) 采用无风扇、低功耗设计，正常功耗不超过 30W；整机更可达-40℃～+85℃的超宽工作温度范围。

第二章 技术性能及指标

2.1. 电源系统

RS6016 百兆系列工业以太网交换机支持直(交)流电源输入（支持双电源输入）。

电压范围：DC9-60V /AC110-240V

2.2. 主要技术性能及指标

2.2.1. 主要技术指标

序号	名称	技术指标
1	交换方式	存储转发
2	接口标准	IEEE802.3；IEEE802.3u；
3	流量控制	半双工 Backpressure，全双工 IEEE802.3x
4	MAC 地址数	8K，自动学习，自动老化（默认 300 秒）
5	转发时延	<10us
6	指示灯	运行、告警、各个端口状态、电源状态；

7	工作温度	-40℃～+85℃
8	工作湿度	5%～95%（产品内部既不应凝露，也不应结冰）

2.2.2. 网络接口参数

1) 百兆 RJ45 电接口参数

序号	名称	接口参数
1	通信标准	10Base-T，100Base-TX
2	速率	10/100Mbps 自适应
3	传输介质	五类以上屏蔽双绞线
4	传输距离	≤100m
5	工作模式	自协商（可支持 10/100M，全双工/半双工）

2) 千兆 RJ45 电接口参数

序号	名称	接口参数
1	通信标准	1000Base-T
2	速率	10/100/1000 Mbps 自适应
3	传输介质	超五类以上屏蔽双绞线
4	传输距离	≤100m
5	工作模式	自协商（可支持 10/100/1000M，全双工/半双工）

3) 百兆 ST/SC/FC 单模光纤接口参数

序号	名称	接口参数
1	通信标准	100Base-FX
2	光纤种类	单模
3	发射波长	1270～1610 nm
4	发送光功率	-8～-3dBm
5	接收波长	1270～1610 nm
6	链路预算	22dBm
7	接收光功率灵敏度	-32dBm
8	连接光纤	9/125um 多模
9	传输距离	0~40km
10	工作模式	100M 全双工

4) 千兆 SFP 多模光纤接口根据插入的光收发模块不同，参数有所区别。常用推荐型号参数如下：

序号	名称	接口参数
1	通信标准	1000Base-LC
2	光纤种类	多模
3	发射波长	770～860 nm，典型值 850nm

序号	名称	接口参数
4	发送功率	-5～0.0dBm
5	链路预算	11dBm
6	接收光功率灵敏度	最大-17dBm，典型值-21 dBm
7	连接光纤	62.5/125um 或 50/125um 多模
8	传输距离	≤275m@62.5/125um，≤550m@50/125um
9	工作模式	自协商（可支持 1000M 全双工）

2.3. 绝缘和耐湿热性能

序号	试验项目	试 验 结 果
1	绝缘电阻	符合 GB/T14598.3-2006 标准：在正常试验大气条件下，装置的外引带电部分（通信接口回路除外）和外露非带电金属部分及外壳之间，以及电气上无联系的各回路之间，用开路电压为直流 1000V 的兆欧表测量其绝缘电阻值，不小于 50MΩ；通信接口回路对地，用开路电压为直流 500V 的兆欧表测量其绝缘电阻值，不小于 100MΩ。
2	介质强度	符合 GB/T14598.3-2006 标准：在正常试验大气条件下，装置能承受频率为 50Hz，电压 2000V（通信回路输入端子为 500V）历时 1min 的工频耐压试验而无击穿闪络及元件损坏现象。试验过程中，任一被试回路施加电压时其余回路等电位互联接地。
3	冲击电压	符合 GB/T14598.3-2006 标准：在正常试验大气条件下，装置的直流输入回路、交流输入回路、输出触点等各回路对地，以及电气上无联系的各回路之间，能承受 1.2/50μs 的标准雷电波的短时冲击电压试验。当额定绝缘电压大于 60V 时，开路试验电压为 5kV；当额定绝缘电压不大于 60V 时，开路试验电压 1kV。
4	耐湿热性能	装置能承受 GB/T 2423.3-2006 规定的恒定湿热试验。试验温度+40℃±2℃、相对湿度（93±3）%，试验时间为 48h，在试验结束前 2h 内，用开路电压为直流 500V 的兆欧表，测量各外引带电回路部分对外露非带电金属部分及外壳之间、以及电气上无联系的各回路之间的绝缘电阻不小于 1.5MΩ。

2.4. 电磁兼容性能

序号	试验项目	试 验 结 果
1	静电放电抗扰度试验	满足 GB/T 17626.2 规定的 4 级试验
2	射频电磁场辐射抗扰度试验	满足 GB/T 17626.3 规定的 3 级试验
3	电快速瞬变脉冲群抗扰度试验	满足 GB/T 17626.4 规定的 4 级试验
4	浪涌（冲击）抗扰度试验	满足 GB/T 17626.5 规定的 4 级试验
5	射频场感应的传导骚扰度	满足 GB/T 17626.6 规定的 3 级试验

6	工频磁场抗扰度试验	满足 GB/T 17626.8 规定的 5 级试验
7	脉冲磁场抗扰度试验	满足 GB/T 17626.9 规定的 5 级试验
8	阻尼振荡磁场抗扰度试验	满足 GB/T 17626.10 规定的 5 级试验
9	电压暂将、短时中断和电压变化的抗扰度试验	满足 GB/T 17626.29 规定的直流 0%中断持续 100ms 试验
10	阻尼振荡波抗扰度	满足 GB/T 17626.12 规定的 3 级试验

2.5. 机械性能

序号	名称	机械性能
1	机箱结构尺寸	137*128*91.5mm; 安装方式：导轨式安装；
2	振 动	满足 GB/T 15153.2-2000 标准 Cm 级： 位移 7mm@2~9Hz，加速度 20m/s²@9~200Hz、15m/s²@200~500Hz。
3	冲 击	满足 GB/T 15153.2-2000 标准 Cm 级： 峰值加速度 300m/ s²持续 11ms。
4	碰 撞	满足 GB/T 15153.2-2000 标准 Cm 级： 高度 0.25 米的自由跌落。

2.6. 环境大气条件

序号	名称	环境参数
1	正常工作大气条件	环境温度：-40℃～+85℃； 相对湿度：5%～95%（产品内部既不凝露，也不结冰）； 大气压力：66kPa～110kPa；
2	正常试验大气条件	环境温度：+15℃～+35℃； 相对湿度：45%～75%； 大气压力：86kPa～106kPa；
3	贮存及运输的极限大气环境	装置贮存、运输允许的环境条件为-40℃～+85℃，相对湿度不大于 85%，在不施加任何激励量的条件下，不出现不可逆变化。

第三章 硬件结构说明

3.1. 面板端子

3.1.1. 指示灯侧布置

(1) RS6016 指示灯侧图

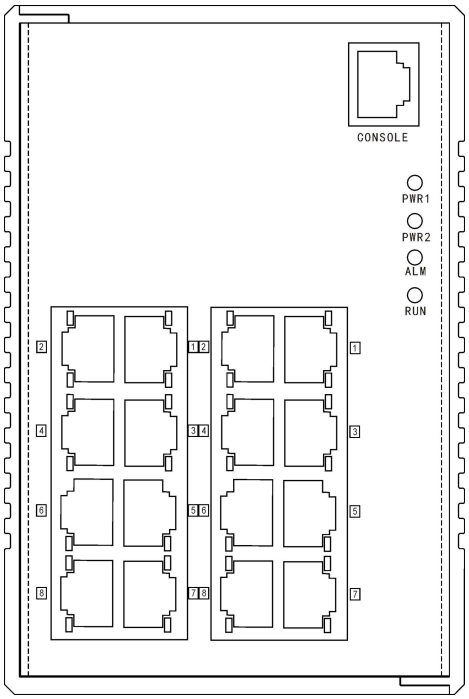


图 3.1 RS6016 百兆系列工业以太网交换机指示灯侧布置图

(2) 信号灯含义

RS6016 百兆系列工业以太网交换机提供的指示灯含义如表 4.1.1 所示。

表 3-1 交换机面板指示灯含义

灯类别	状态	含义
PWR1/2	点亮	交换机电源 1/2 工作正常
	熄灭	交换机未通电或交换机电源 1/2 工作异常
RUN	点亮	交换机正常稳定工作
	熄灭	交换机未通电或交换机异常
ALM	点亮	交换机有告警事件
	熄灭	交换机无告警事件

灯类别	状态	含义
Link/Act（绿灯）	点亮	指定标号的网络端口与连接方链接成功
	熄灭	指定标号的网络端口与连接方链接失败（或未接入）
	闪烁	指定标号的网络端口正在发送/接收数据
SPD 指示灯（黄灯）	点亮	端口 100Mbps 状态
	熄灭	端口 10Mbps 状态

3.2. 电源、告警连接端子示意图

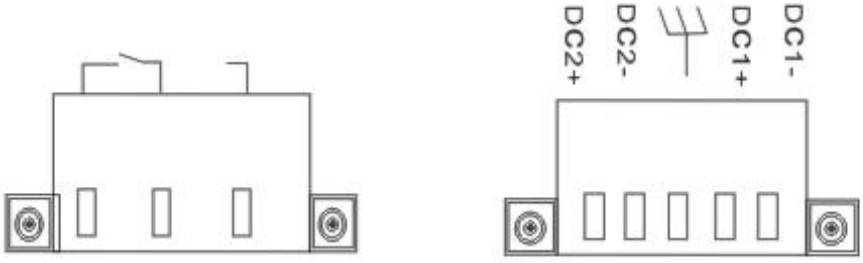


图3.3 电源、告警连接端子布置图

RS6016 百兆系列工业以太网交换机交（直）流电源输入功能（支持双电源），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 3.3 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。

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。

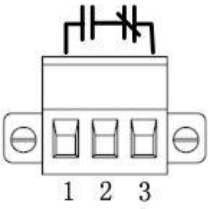


图3.4 告警端子

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。

3.3.1. RS232 控制端口（Console）

RS6016 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

3.3.2. 接地

RS6016 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。

3.4. 安装方式

3.4.1. 导轨式安装

第一步，安装导轨：

将导轨固定在机架上，如图 3.5 所示：

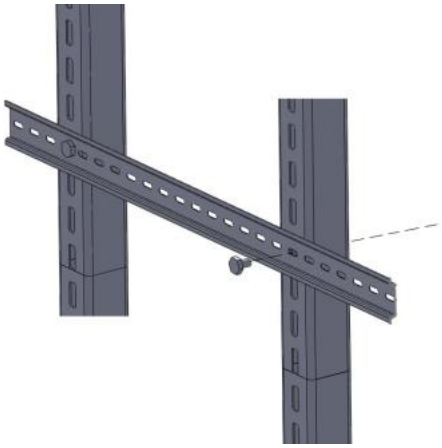


图3.5 安装导轨

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：

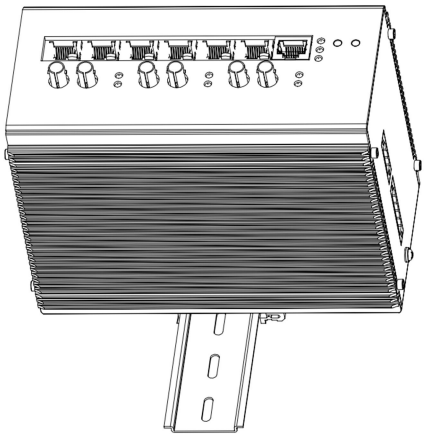


图3.6 安装交换机

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。

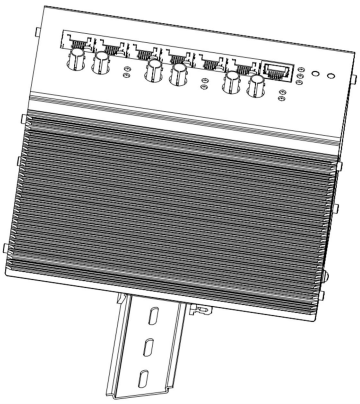


图3.7 拆除交换机

第四章 使用说明

4.1. Web登录

工业以太网交换机提供 WEB 管理， 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）/logger
默认密码	admin（管理用户）/guest（普通用户）/logger

输入正确的用户名、密码和验证码（管理用户 admin/admin）即可进入 Web 管理界面，如下：

4.2. 系统配置

4.2.1. 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：

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）。

4. 2. 2. 系统状态

配置项	说明
cpu 占用率	显示当前 cpu 使用百分比
内存占用率	显示当前内存使用百分比
MAC 地址	显示该设备的唯一物理地址
Bootrom 版本	显示系统启动软件版本
系统时间	显示系统当前时间
启动时间	显示系统运行时长

软件版本	显示该系统运行的软件版本
版本时间	显示该系统所运行软件版本的编译时间
当前温度	显示该设备机箱内当前温度

4.3. 用户设置

点击导航栏“系统配置→用户设置”，即可进入用户设置界面，如下图：

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： 修改密码设置只能用于当前用户。 删除只能是具有管理员权限的用户才可以操作。 系统默认的 admin、guest、logger 用户不能删除，只能修改密码。
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。

4.3.1. 添加用户

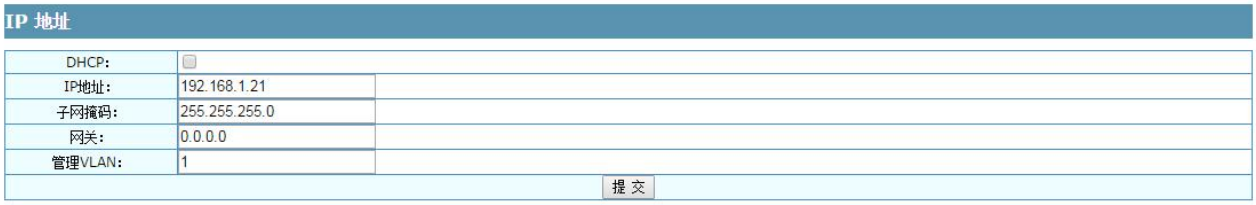
用于添加系统的管理用户，并分配相应的管理权限，只有管理员才可以添加用户。点击系统配置--->用户设置--->添加用户，就可以进入“添加用户”界面，如图：

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 1~16 字节。

密码	用于设置管理用户的密码。密码由 0~16 字节的 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。

4.4. IP地址

点击导航栏“系统配置→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。
管理 VLAN	用于设置和显示系统的管理 VLAN，默认为 1。

第五章 Mirror

5.1. 简介

交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口。镜像目的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 5.1 所示：

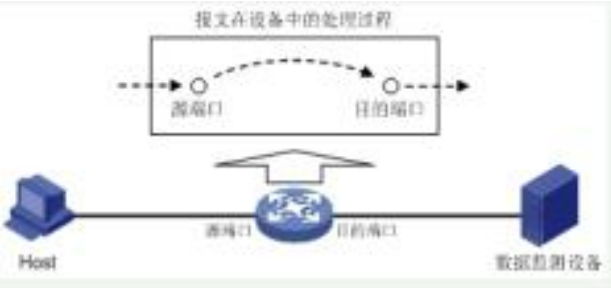
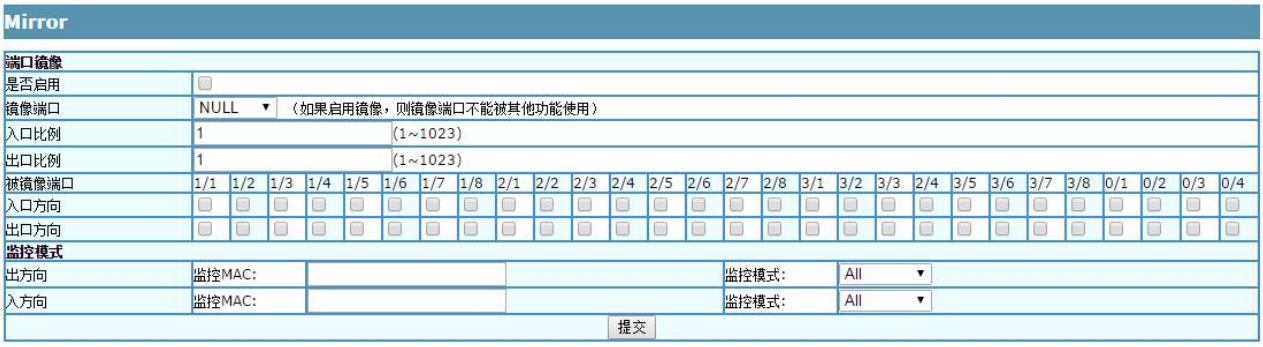


图5.1 镜像示意图

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：



配置项	说明
是否启用	用于启用系统的端口镜像功能
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。
入口比率	在入口方向，复制到镜像端口的数据流量占该端口全部流量的比例，实际被镜像的流量等于入口比例的倒数乘以该端口的总流量。
出口比率	在出口方向，复制到镜像端口的数据流量占该端口全部流量的比例，实际被镜像的流量等于出口比例的倒数乘以该端口的总流量
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
监控模式	All：表示监控被镜像端口的全部数据。 目的 MAC：监控以此 mac 为目的 mac 的数据。 源 MAC：监控以此 mac 为源 mac 的数据。
提交	用于提交当前页面的配置信息。

第六章　SNTP

6.1.　SNTP简介

目前，因特网上普遍采用了通讯协议来实现网络时间同步，即 NTP（Network Time Protocol--网络时间协议）。还有一种协议是 NTP 协议的简化版，即 SNTP（Simple Network Time Protocol，简单网络时间协议）。

NTP 协议可以跨越各种平台和操作系统，用非常精密的算法，因而几乎不受网络的延迟和抖动的影响，可以提供 1-50 ms 精度。NTP 同时提供认证机制，安全级别很高。但是 NTP 算法复杂，对系统要求较高。

SNTP（简单网络时间协议）是 NTP 的简化版本，在实现时，计算时间用了简单的算法，性能较高。而精确度一般也能达到 1 秒左右，基本满足绝大多数场合的需要。

由于 SNTP 的报文和 NTP 的报文是完全一致的，所以本设备实现的 SNTP Client 能完全兼容 NTP Server。

SNTP 协议采用客户/服务器工作方式，服务器通过接收 GPS 信号或自带的原子钟作为系统的时间基准，客户机通过定期访问服务器提供的时间服务获得准确的时间信息，并调整自己的系统时钟，达到网络时间同步的目的。

6.2.　SNTP

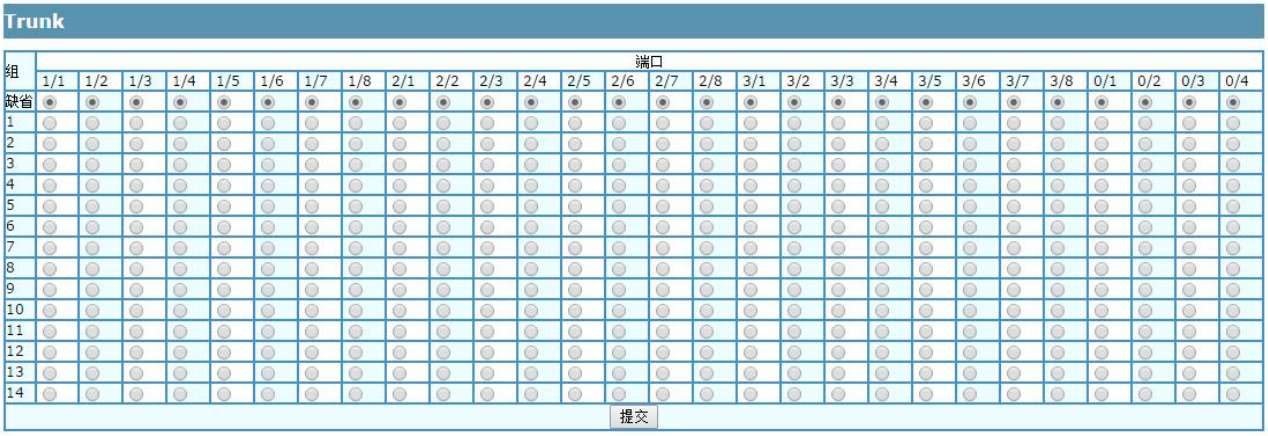
点击导航栏“设备控制→SNTP”，即可进入 SNTP 界面，如下图：

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。

第七章　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 14 组，每组不少于两个端口。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。

第八章　告警

8.1.　简介

主要实现了电源（电源出现故障进行切换）、端口（端口 down 掉）、温度（高低温告警）、环网告警（环网故障告警）。

8.2.　告警设置

点击导航栏“设备控制→告警配置”，即可进入告警设置界面，如下图：

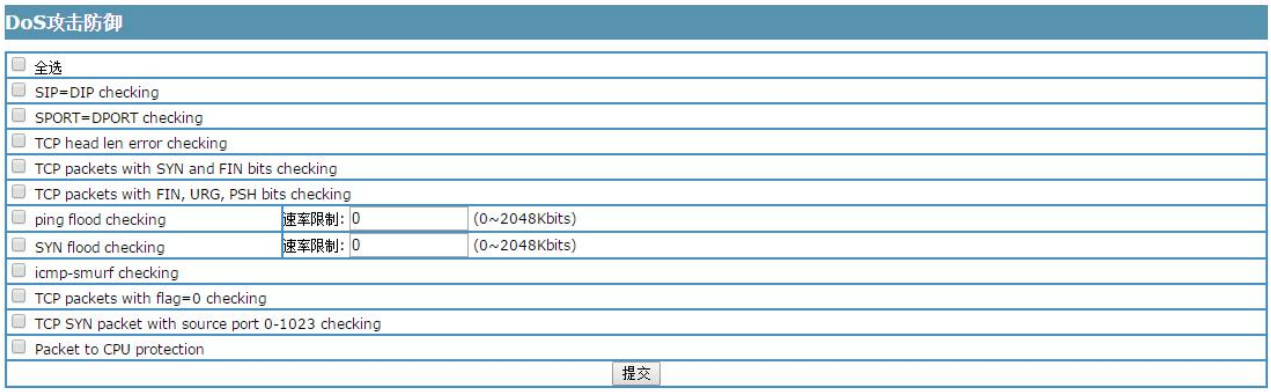
告警配置界面中修改各项参数的解释如下表所示：

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。

第九章　DoS 攻击防御

点击导航栏“设备控制→DoS 攻击防御”，即可进入 DoS 攻击防御界面，如下图：



第十章　GMRP 设置

10.1.　GMRP定义

GMRP 是基于 GARP 的组播注册协议，它支持网络设备间进行二层组播组的传递和注册。在智能电网的应用中，由于 GOOSE、采样值等报文是纯二层以太报文，只有目的组播 MAC 地址而没有 IP 地址，不能使用 IGMP 等的 IP 组播协议，所以只有应用 GMRP 才能建立二层组播组，对 GOOSE 等报文进行有效的组播复制和转发。可以说，GMRP 是工业以太网交换机在智能电网中的必要协议。

为什么需要二层组播协议呢？还有另外一个重要原因，与 IGMP 协议一样，如果我们在自己的局域网内成立一个组播组，可能我们的局域网包含了很多交换机。如果这些交换机没有实现二层组播协议的话，那么某个组员给其他组员发送数据包时，交换机就会将该数据包向所有的端口广播。因为交换机不知道哪个端口有人加入了该组播组，唯一的解决办法就是管理员配置交换机，只有这样才能将这种广播转发数据包的发送方式限制住。而组播本身是动态的，所以通过这种靠管理员的配置来实现组播的方式是不现实的。因此，就需要有一个二层组播协议来动态管理组员。

10.2.　GMRP的配置

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

只需要对端口进行启用禁用操作，即启用或禁用 GMRP 功能。

提交：

用于提交当前页面的配置信息。

第十一章　非法 IP 地址配置

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

配置非法 IP 地址段对 telnet、ssh、web 进行限制，非法 IP 地址段无法访问。

第十二章　端口

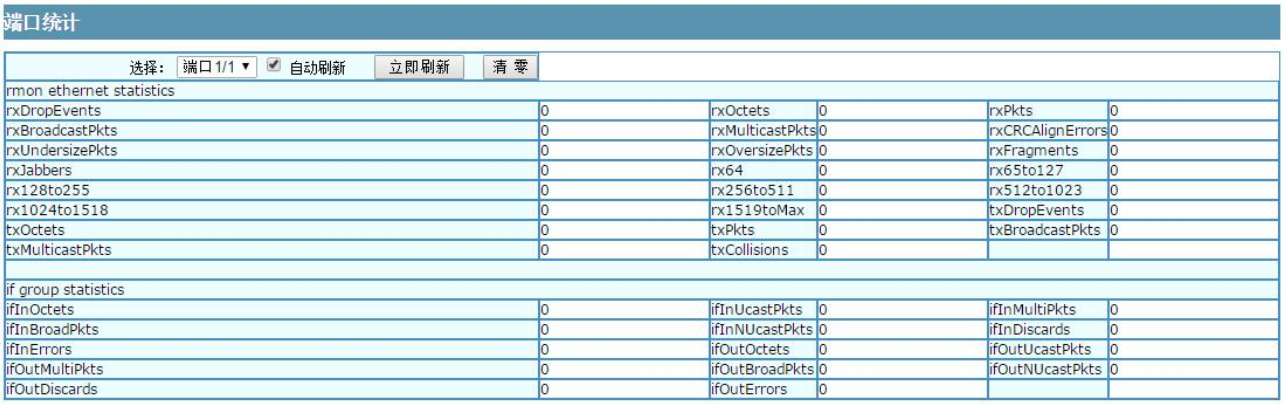
12.1.　端口设置

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：

配置项	说明
端口	表示交换机的逻辑端口号。
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 3 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。

12.2. 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：

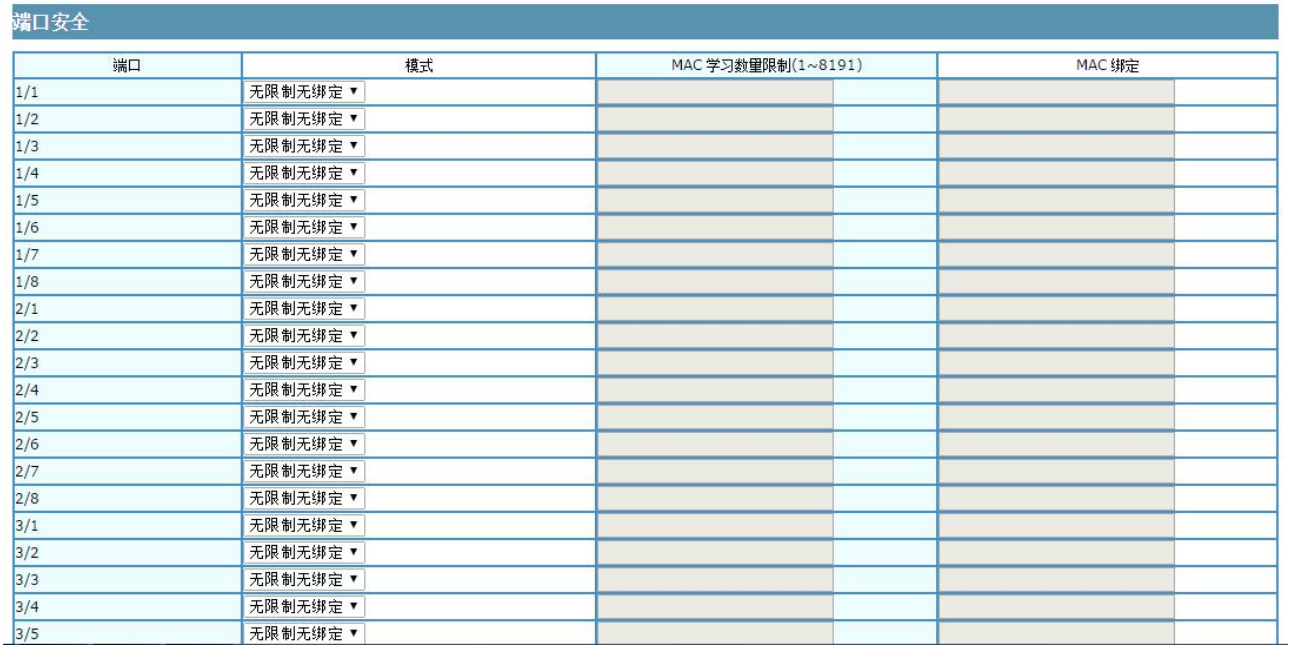


配置项	说明
选择	选择某端口，可以是物理端口或者是虚端口。rx 代表从该端口接收的数据包，tx 代表从该端口发出的数据包
rmon ethernet statistics	显示 RMON 统计组定义的各种统计信息。
DropEvents	由于缺少资源而丢弃的数据包数量。这不一定是丢弃的数据包的实际数量，而是探测到这种情况的次数
Octets	接收到的数据的字节数（包括出错包的数据字节）
Pkts	接收到的数据包的数量，包括出错包、广播数据包和多播数据包。
BroadcastPkts	接收到的正常的广播数据包
rxMulticastPkts	接收到的正常的多播数据包
rxCRCAlignErrors	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。
txCollisions	冲突总数，是一个估计值。
ifInOctets	进入该端口的数据的字节数（包括出错包的数据字节）。

ifInUcastPkts	进入该端口的单播数据报文的总数。
ifInMultiPkts	进入该端口的多播数据报文的总数。
ifInBroadPkts	进入该端口的广播数据报文的总数。
ifInNUcastPkts	进入该端口的未知单播数据报文的总数。
ifInDiscards	进入该端口但被丢弃的数据报文的总数。
ifInErrors	进入该端口的错误数据报文的总数。
ifOutOctets	从该端口出来的数据的总字节数（包括出错包的数据字节）。
ifOutUcastPkts	从该端口出来的单播数据的总数。
ifOutMultiPkts	从该端口出来的多播数据报文的总数
ifOutBroadPkts	从该端口出来的广播数据报文的总数
ifOutNUcastPkts	从该端口出来的未知单播数据报文的总数
ifOutDiscards	从该端口出来的被丢弃的数据报文的总数
ifOutErrors	从该端口出来的错误数据报文的总数
dot3InPauseFrames	该端口接收到的流控帧数量
dot3OutPauseFrames	该端口发送的流控帧数量
dot1dTpPortInDiscards	在转发中被丢弃的错误帧的数量

12.3. 端口安全

点击导航栏“设备控制→端口→端口安全”，即可进入端口安全界面，如下图：



12.4. VLAN LIMIT

点击导航栏“设备控制→端口→VLANLIMIT”，即可进入 VLANLIMIT 界面，如下图：

基于 VLAN 的 MAC 地址条目限制

第十三章 VLAN

13.1. 概述

VLAN（Virtual Local Area Network，虚拟局域网），VLAN 能将网络划分为多个广播域，从而有效地控制广播风暴的发生，以及使网络的拓扑结构变得非常灵活的优点外，还可以用于控制网络中不同部门、不同站点之间的互相访问。

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

13.2. 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。

2. 基于 MAC 地址的 VLAN

由于网卡分配有 MAC 地址，因此按 MAC 地址来划分 VLAN 实际上是将某些工作站和服务器划分于某个 VLAN。事实上，该类型的 VLAN 是一些 MAC 地址的集合。当设备移动时，VLAN 能够自动识别。网络管理需要管理和配置设备的 MAC 地址，显然当网络规模很大，设备很多时，会给管理带来难度。

3. 基于 IP 子网的 VLAN

基于 IP 子网的 VLAN 是指所有的流量根据源/目的 IP 子网进行分配。其中，局域网交换机允许一个子网扩展到多个局域网交换端口，甚至允许一个端口对应于多个子网。

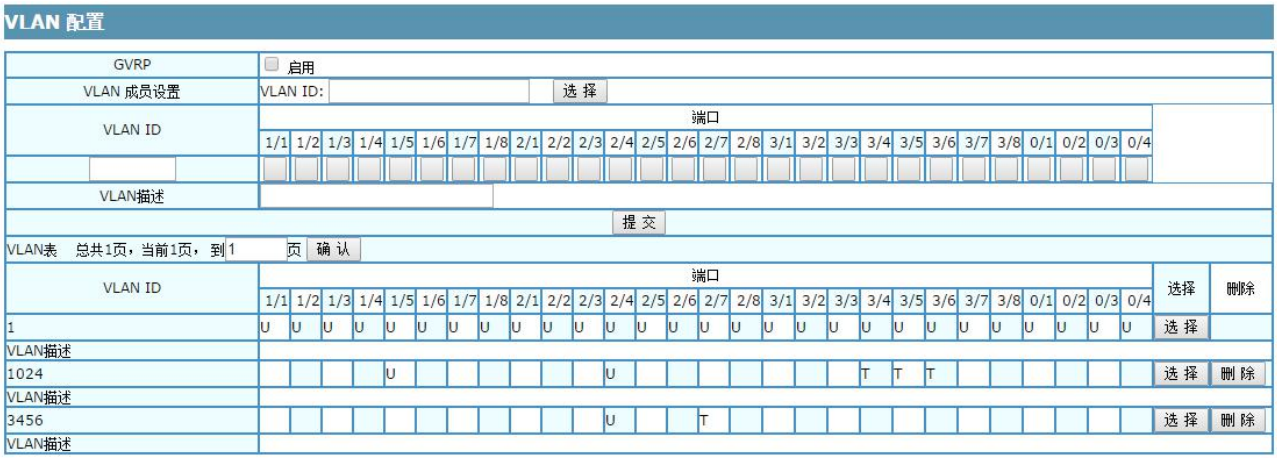
4. 基于协议的 VLAN

基于协议的 VLAN 是指，在 VLAN 中，流量的传送根据协议来分配。不同的端口可以指定不同的协议

类型。如 1 端口可以用来传送 IP 协议的数据包，而其他端口则可以传送其他协议类型的数据包。

13.3. VLAN的成员配置

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

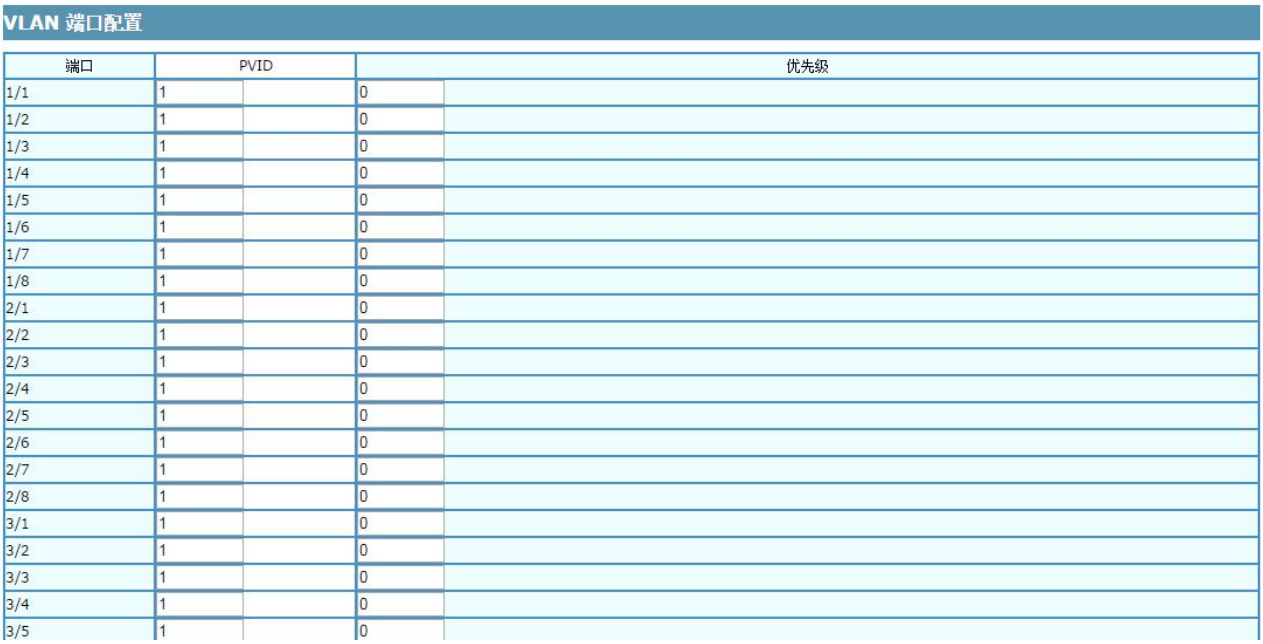


VLAN 成员配置界面中修改各项参数的解释如下表所示：

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。

13.4. 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：



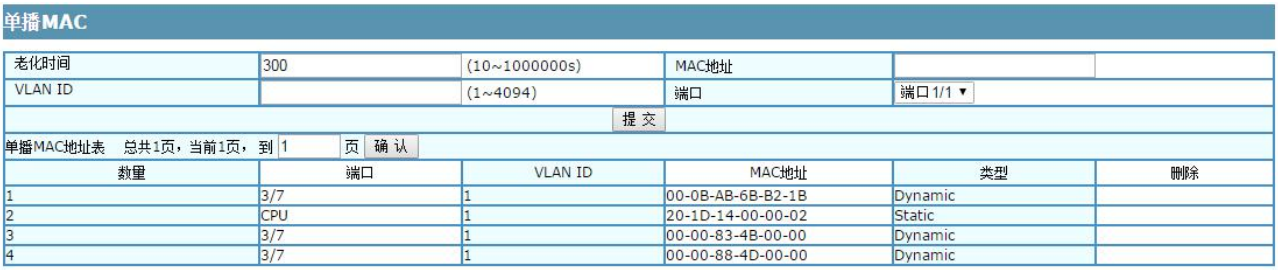
VLAN 端口配置界面中修改各项参数的解释如下表所示：

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。

第十四章　MAC

14.1.　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。

14.2. 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。
提交	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。

第十五章 QoS

15.1. 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。对于网络业务，服务质量包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。网络资源总是有限的，只要存在抢夺网络资源的情况，就会出现服务质量的要求。服务质量是相对网络业务而言的，在保证某类业务的服务质量的同时，可能就是在损害其它业务的服务质量。例如，在网络总带宽固定的情况下，如果某类业务占用的带宽越多，那么其他业务能使用的带宽就越少，可能会影响其他业务的使用。因此，网络管理者需要根据各种业务的特点来对网络资源进行合理的规划和分配，

从而使网络资源得到高效利用。

15.2. 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）

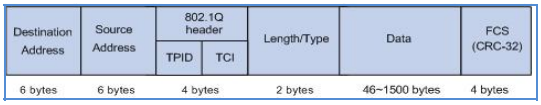


图 15.1 带有 802.1Q 标签头的以太网帧

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 15.2 802.1Q 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。

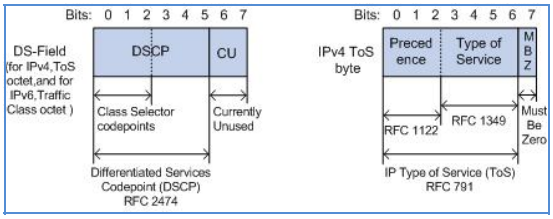


图 15.3 DS 域和 ToS 字节

15.3. 队列调度介绍

1. 严格优先队列(SPQ)

这是一种最简单的排队方式，它首先为最高优先级的队列进行服务，直到该队列为空，然后为下一个

次高优先级队列服务，依此类推。这种方法的优势是高优先级业务总是在低优先级业务之前处理。但是，低优先级业务有可能被高优先级业务完全阻塞。

2. 加权循环(WRR)

这种方法为所有业务队列服务，并且将优先权分配给较高优先级队列。在大多数情况下，相对低优先级，WRR 将首先处理高优先级，但是当高优先级业务很多时，较低优先级的业务并没有被完全阻塞。

15.4. 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：

配置项	说明
QoS 模式	用于启用/禁用系统的 QoS 功能
队列数	用于配置系统中当前起作用的队列个数。系统默认有 4 个队列
调度算法	用于配置系统当前选用的调度算法，分为 4WRR 队列调度算法、1SP-3WRR 队列调度算法、2SP-2WRR 队列调度算法、4SP 队列调度算法。
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 0~31。

15.5. 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 2 部分，802.1p 优先级队列和 DSCP 优先级队列。以下分为 2 部分分别介绍：

802.1p 优先级队列：

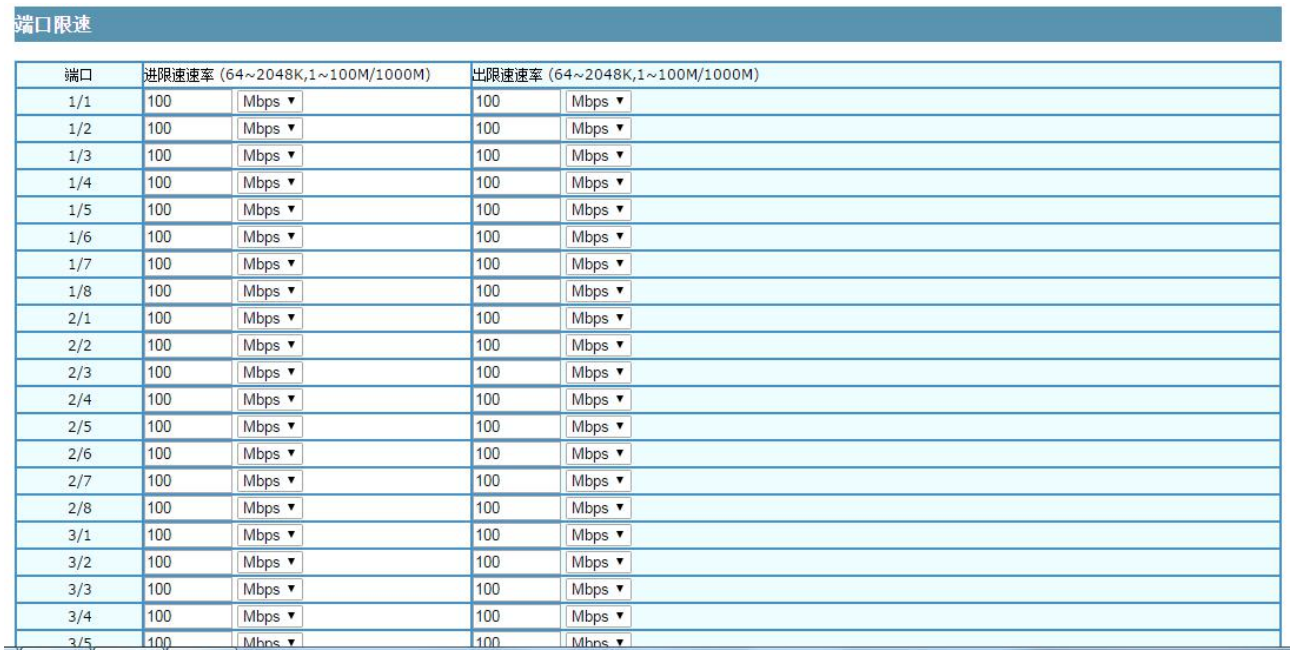
此部分用于 802.1p 优先级与队列之间的映射关系，默认情况下，0 和 1 优先级映射 0 队列，2 和 3 优先级映射 1 队列，4 和 5 优先级映射 2 队列，6 和 7 优先级映射 3 队列。

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。

15.6. 端口限速界面

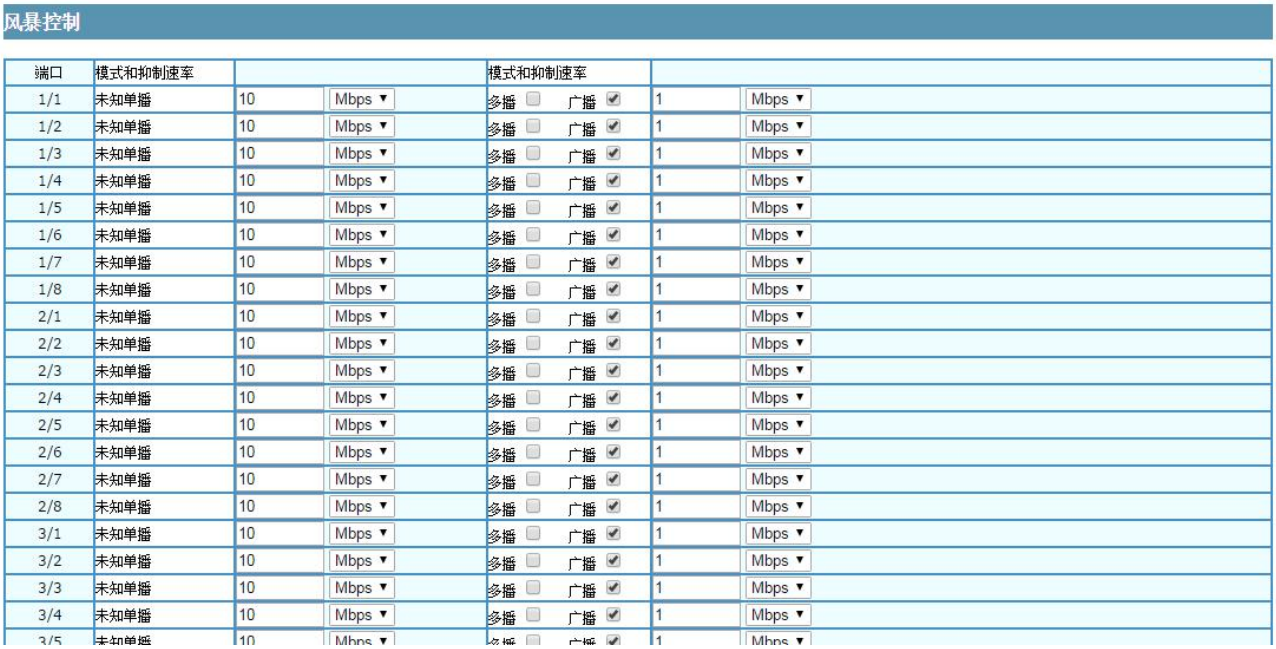
点击导航栏“设备控制→QoS→端口限速”，即可进入 QoS 的端口限速配置界面，如下图：



配置项	说明
端口	交换机端口的逻辑编号。
进限速	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	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 2Mbps 以下速率的限制粒度为 64kbps，2Mbps 以上速率的限制粒度为 1024kbps。

15.7. 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：



配置项	说明
端口	交换机端口的逻辑编号。
模式	用于设置控制风暴的类型，包括广播、多播和未知单播。默认控制以上三种风暴。
抑制速率	用于设置风暴的抑制速率，单位为 Kbps 或 Mbps，默认为 1Mbps。

第十六章 STP

16.1. 生成树简介

STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于在网络中建立树形拓扑，消除网络中的环路，并且可以通过一定的方法实现路径冗余，但不是一定可以实现路径冗余。生成树协议适合所有厂商的网络设备，在配置上和体现功能强度上有所差别，但是在原理和应用效果是一致的。

STP 的基本原理是，通过在交换机之间传递一种特殊的协议报文，网桥协议数据单元（Bridge Protocol Data Unit，简称 BPDU），来确定网络的拓扑结构。BPDU 有两种，配置 BPDU（Configuration BPDU）和 TCN BPDU。前者是用于计算无环的生成树的，后者则是用于在二层网络拓扑发生变化时产生用来缩短 CAM 表项的刷新时间的（由默认的 300s 缩短为 15s）。

Spanning Tree Protocol(STP)在 IEEE802.1D 文档中定义。该协议的原理是按照树的结构来构造网络拓扑，消除网络中的环路，避免由于环路的存在而造成广播风暴问题。

16.2. 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：

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。

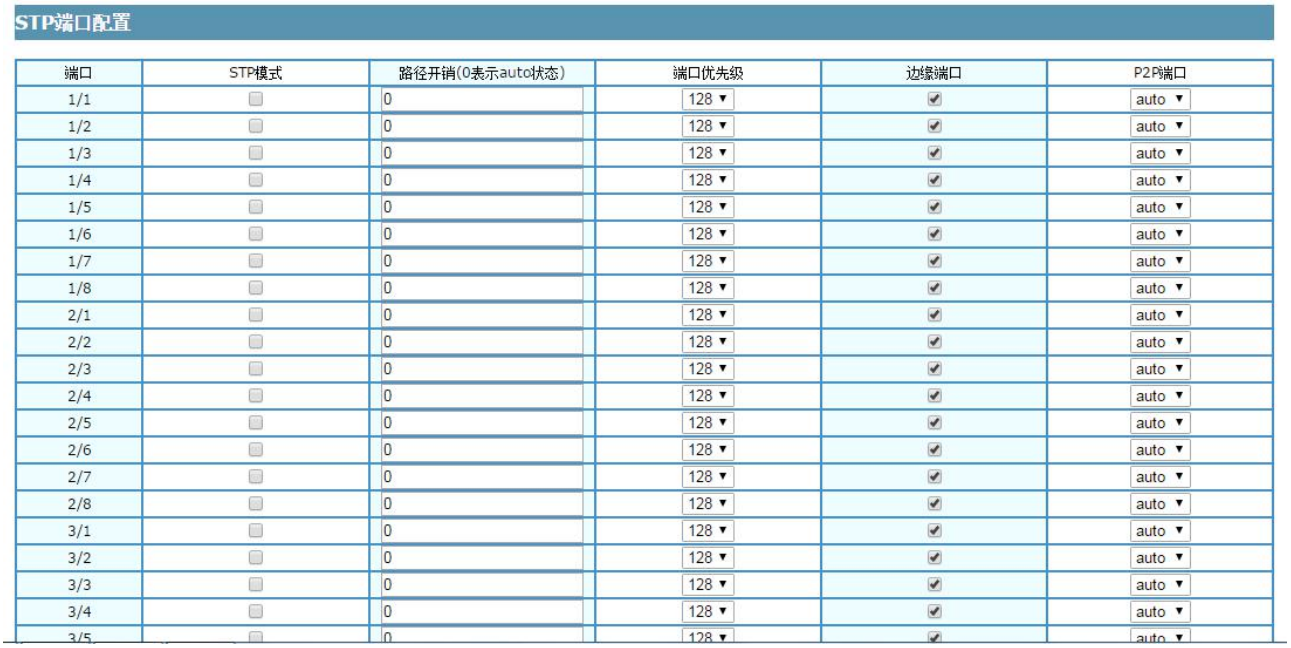
Hello 时间不能长于 Max Age。否则，设置发生错误。在设置上述参数时请参考下列公式。

Max Age ≤ 2 x (Forward Delay - 1 秒)

Max Age ≥ 2 x (Hello Time + 1 秒)

16.3. 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：



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 auto、true、false 状态，系统默认为 auto 状态。

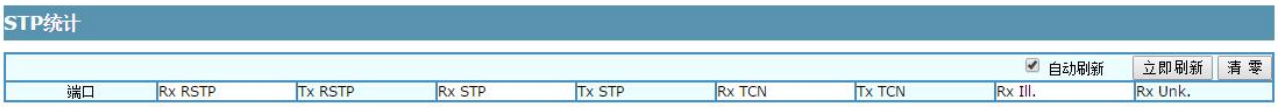
16.4. 端口状态

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：

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。

16.5. 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：



数据统计配置页面各项参数说明如下表所示：

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。

第十七章 MSTP

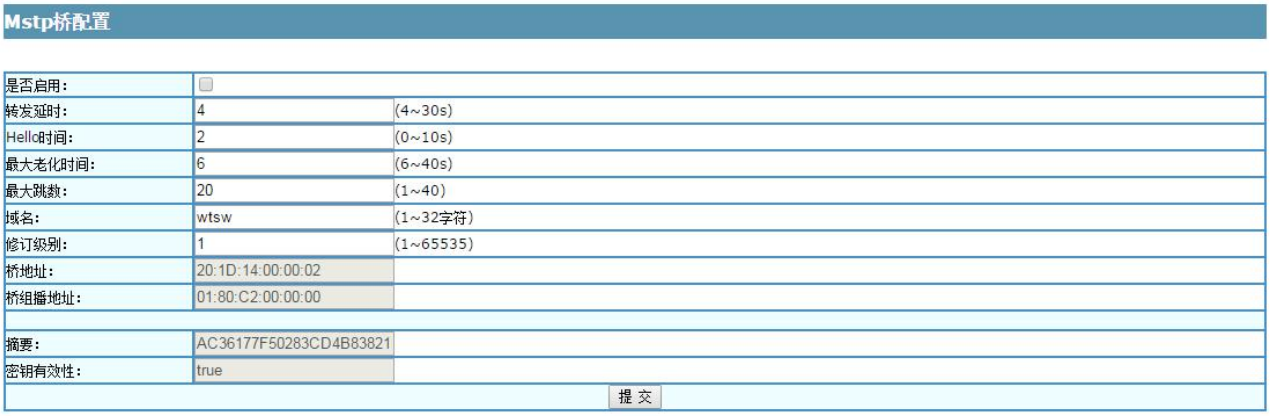
17.1. 概述

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。

17.2. 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：

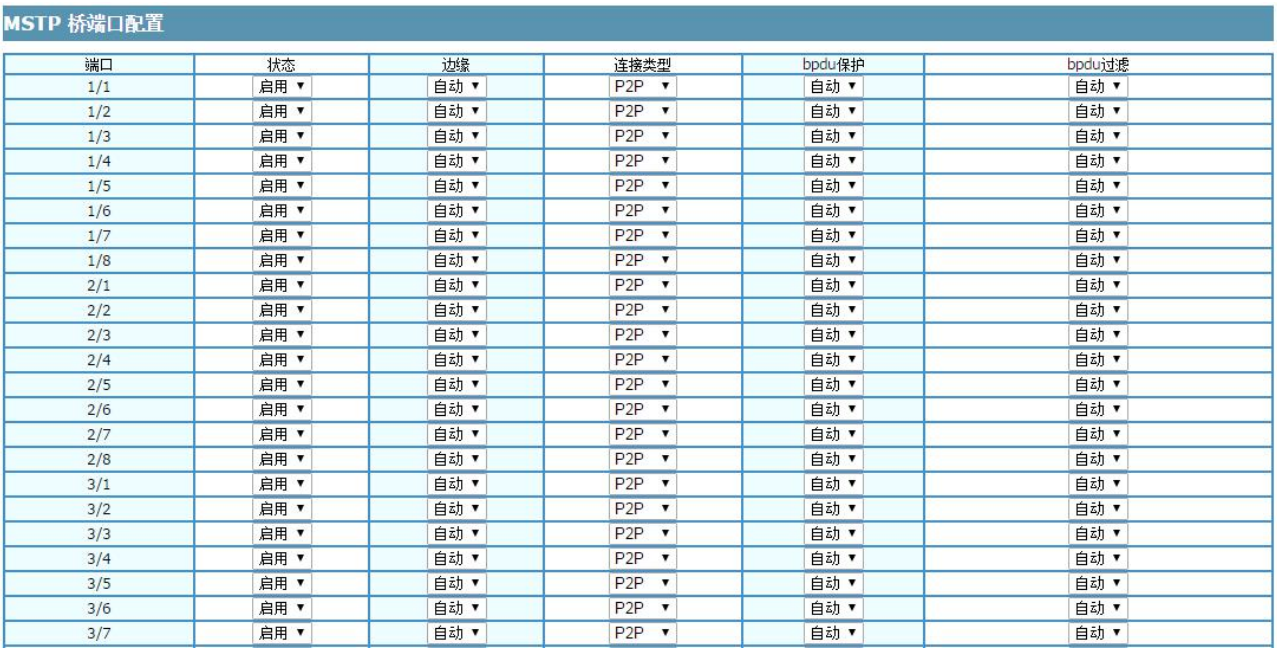


MSTP 桥配置页面各项参数说明如下表所示：

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。

17.3. 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 桥端口配置页面各项参数说明如下表所示：

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）

17.4. CIST配置信息

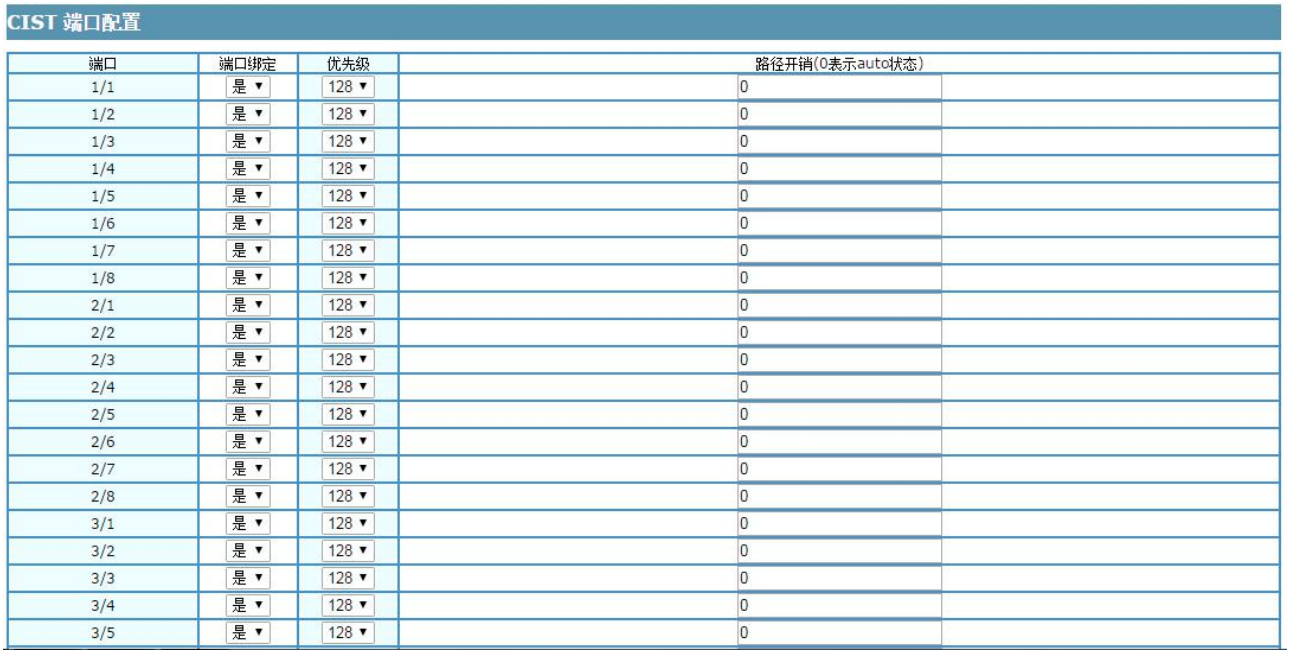
点击导航栏“设备控制→MSTP→CIST 配置信息”，即可进入 MSTP 的 CIST 配置信息界面，如下图：

CIST 配置信息页面各项参数说明如下表所示：

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

17.5. 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 端口配置页面各项参数说明如下表所示：

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	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

17.6. 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：

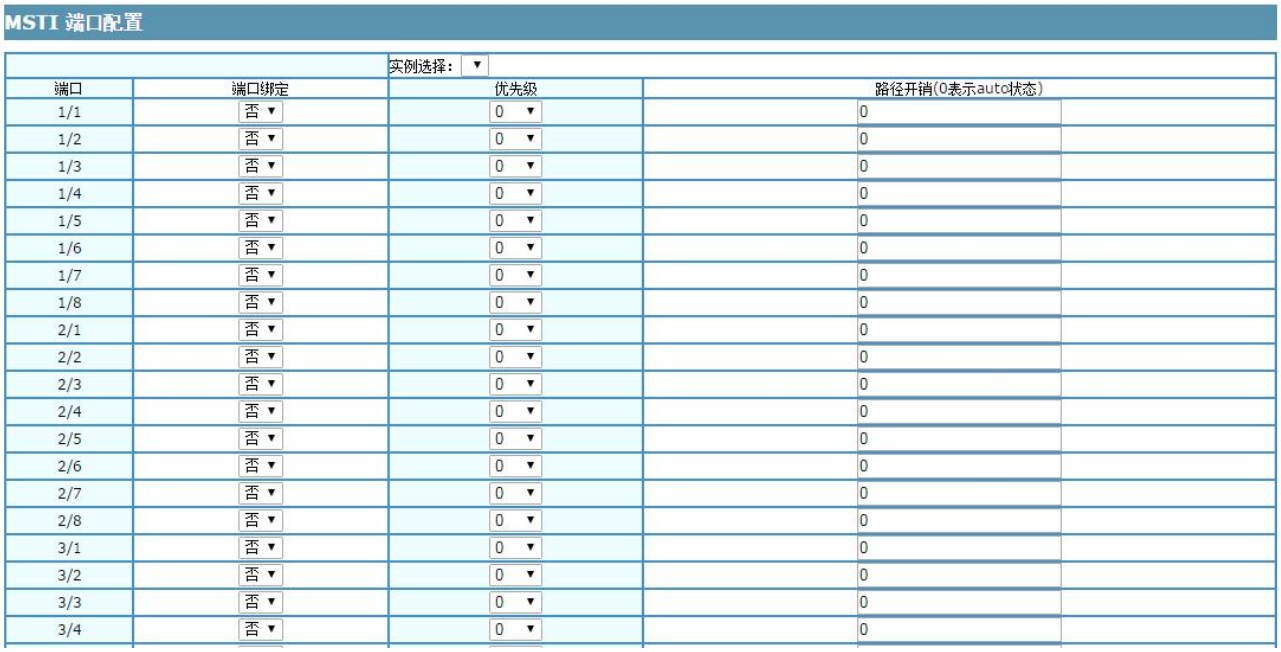
MSTI 配置信息页面各项参数说明如下表所示：

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

17.7. 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 端口配置页面各项参数说明如下表所示：

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

17.8. Vlan表配置

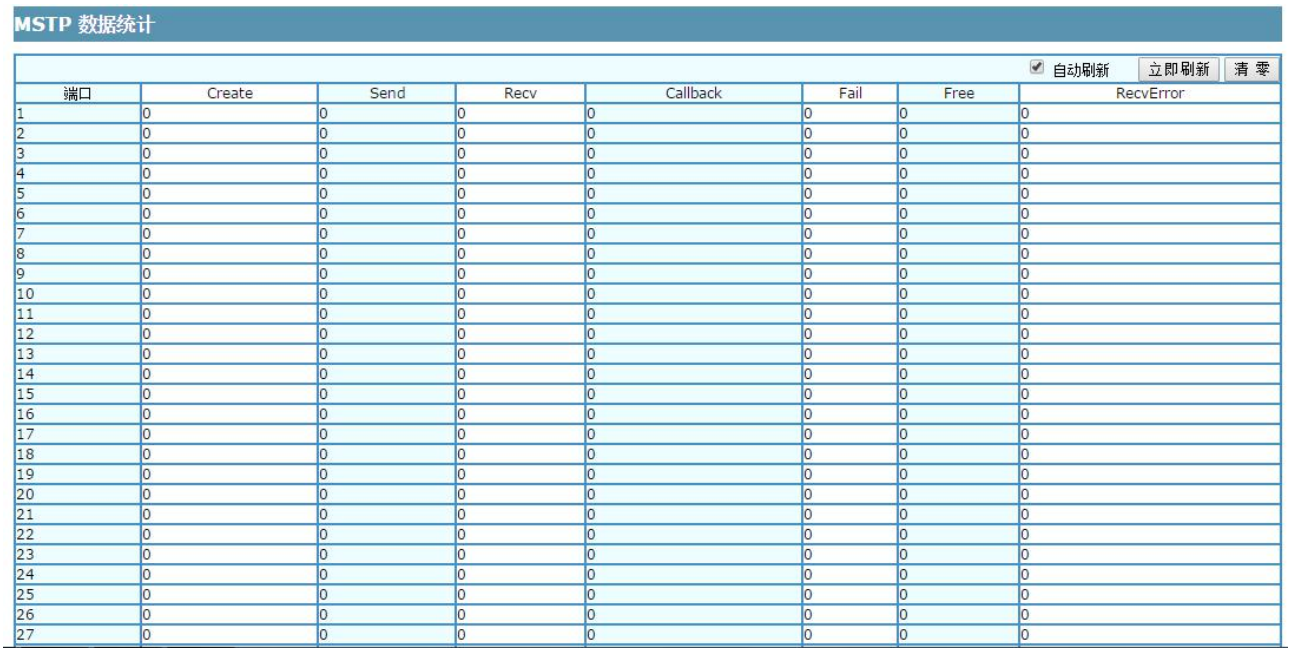
点击导航栏“设备控制→MSTP→Vlan 表配置”，即可进入 MSTP 的 Vlan 表配置界面，如下图：

Vlan 表配置页面各项参数说明如下表所示：

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）

17.9. 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：



端口	Create	Send	Recv	Callback	Fail	Free	RecvError
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0

MSTP 数据统计页面各项参数说明如下表所示：

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

第十八章 WTOP_RING

18.1. 概述

18.1.1. 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。

18.1.2. 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。

18.1.3. 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：

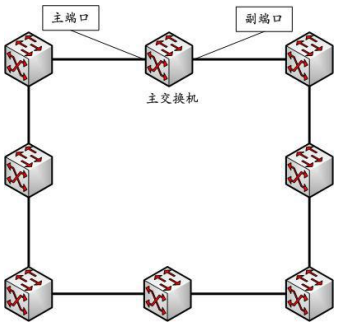


图4-5 单环

18.1.4. 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. RING_CONF_COMM_FD_FDB

刷新 FDB 报文，由主节点发起，通知传输节点更新各自 MAC 地址转发表。

5. RING_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。

18.2. 端口配置

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

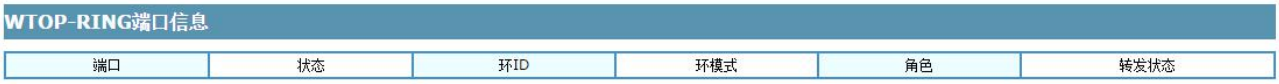
WTOP RING 的端口配置界面各项参数说明如下表所示：

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）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
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
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

18.2.1. 端口信息

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

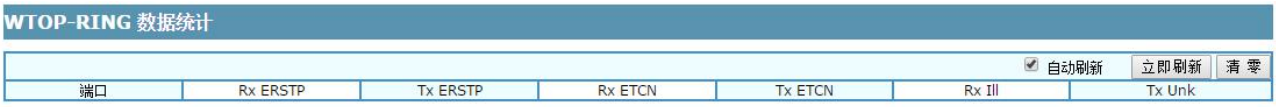


WTOP RING 的端口信息界面各项参数说明如下表所示：

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 和 None
转发状态	端口成员的转发状态，分为 forwarding、blocking 和 disable 等状态

18.2.2. 数据统计

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



WOTP_RING 的数据统计界面各项参数说明如下表所示：

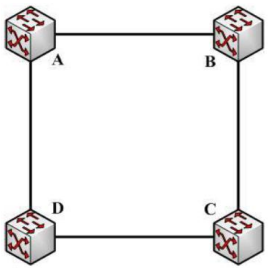
配置项	说明
端口	wtp_ring 的端口成员
ERSTP	环网的探测包
ETCN	环网的控制包，包括 MAC 地址清除等控制包
Rx Ill	收到的错误的 wotp_ring 消息
Rx Unk	收到的未知的 wotp_ring 消息

18.2.3. 配置举例

1. 单环组网需求：

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

2. 单环组网图：



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 =21。
- 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 =21。
- 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 =21。
- 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

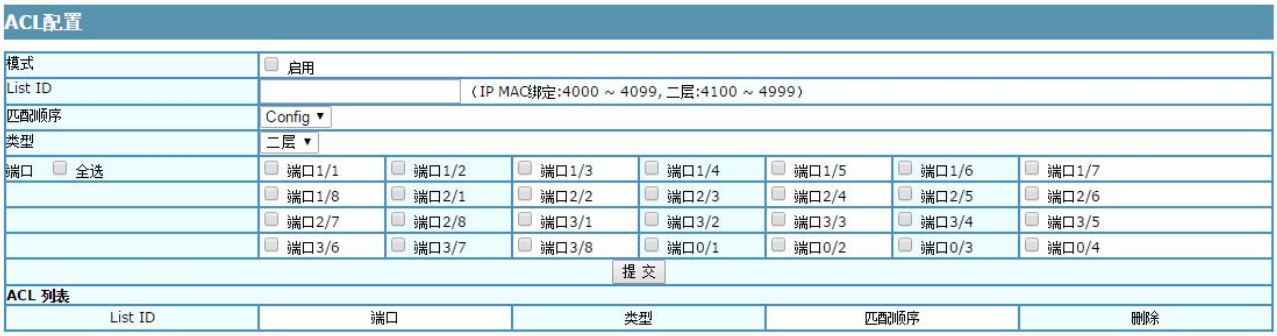
第十九章 ACL

19.1. 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。

19.2. ACL列表配置

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



ACL 列表配置设置界面各项参数说明如下表所示：

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：4000～4999
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

19.3. ACL端口配置

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

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。

ACL 端口配置界面各项参数说明如下表所示：

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

19.4. Ip Rule配置

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

第二十章 802.1X

20.1. 简介

802.1x 协议是一种基于端口的网络接入控制协议（Port Based Network Access Control）。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

使用 802.1x 的系统为典型的 Client/Server 体系结构，包括三个实体，分别为：Supplicant system（客户端）、Authenticator system（设备端）以及 Authentication server system（认证服务器）。

20.2. 802.1X 系统配置

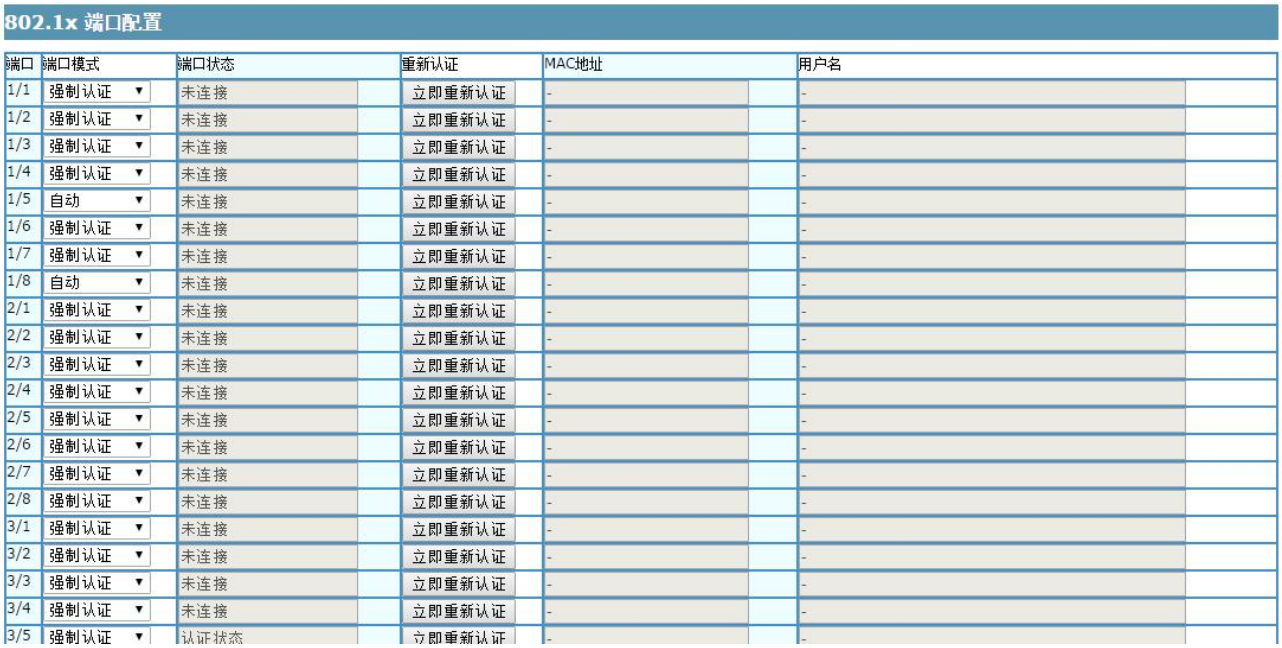
点击导航栏“设备控制→80.2.1X→802.1X 系统配置”，即可进入 802.1X 系统配置界面，如下图：

20.3. 802.1X本地认证

点击导航栏“设备控制→80.2.1X→802.1X 本地认证”，即可进入 802.1X 本地认证界面，如下图：

20.4. 802.1x 端口配置

点击导航栏“设备控制→80.2.1X→802.1x 端口配置”，即可进入 802.1x 端口配置界面，如下图：

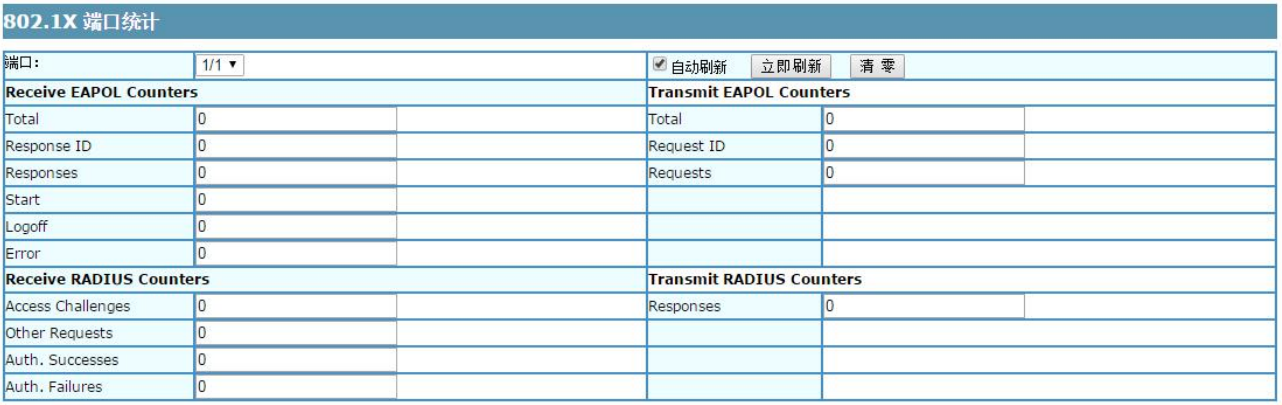


802.1x 端口配置

端口	端口模式	端口状态	重新认证	MAC地址	用户名
1/1	强制认证	未连接	立即重新认证	-	-
1/2	强制认证	未连接	立即重新认证	-	-
1/3	强制认证	未连接	立即重新认证	-	-
1/4	强制认证	未连接	立即重新认证	-	-
1/5	自动	未连接	立即重新认证	-	-
1/6	强制认证	未连接	立即重新认证	-	-
1/7	强制认证	未连接	立即重新认证	-	-
1/8	自动	未连接	立即重新认证	-	-
2/1	强制认证	未连接	立即重新认证	-	-
2/2	强制认证	未连接	立即重新认证	-	-
2/3	强制认证	未连接	立即重新认证	-	-
2/4	强制认证	未连接	立即重新认证	-	-
2/5	强制认证	未连接	立即重新认证	-	-
2/6	强制认证	未连接	立即重新认证	-	-
2/7	强制认证	未连接	立即重新认证	-	-
2/8	强制认证	未连接	立即重新认证	-	-
3/1	强制认证	未连接	立即重新认证	-	-
3/2	强制认证	未连接	立即重新认证	-	-
3/3	强制认证	未连接	立即重新认证	-	-
3/4	强制认证	未连接	立即重新认证	-	-
3/5	强制认证	认证状态	立即重新认证	-	-

20.5. 802.1X 端口统计

点击导航栏“设备控制→80.2.1X→802.1X 端口统计”，即可进入 802.1X 端口统计界面，如下图：



802.1X 端口统计

端口:	1/1	自动刷新	立即刷新	清 零
Receive EAPOL Counters		**Transmit EAPOL Counters**		
Total	0	Total	0	
Response ID	0	Request ID	0	
Responses	0	Requests	0	
Start	0			
Logoff	0			
Error	0			
Receive RADIUS Counters		**Transmit RADIUS Counters**		
Access Challenges	0	Responses	0	
Other Requests	0			
Auth. Successes	0			
Auth. Failures	0			

第二十一章 IGMP

21.1. 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。启用 IGMP 功能的前后对比如下图：

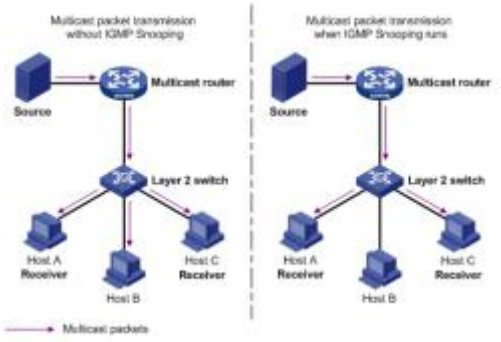


图 21.1 IGMP 对比图

21.2. 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 配置界面各项参数说明如下表所示：

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

21.3. 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：

IGMP 统计界面各项参数说明如下表所示：

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

21.4. IGMP组

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

第二十二章 LACP

22.1. 链路汇聚简介

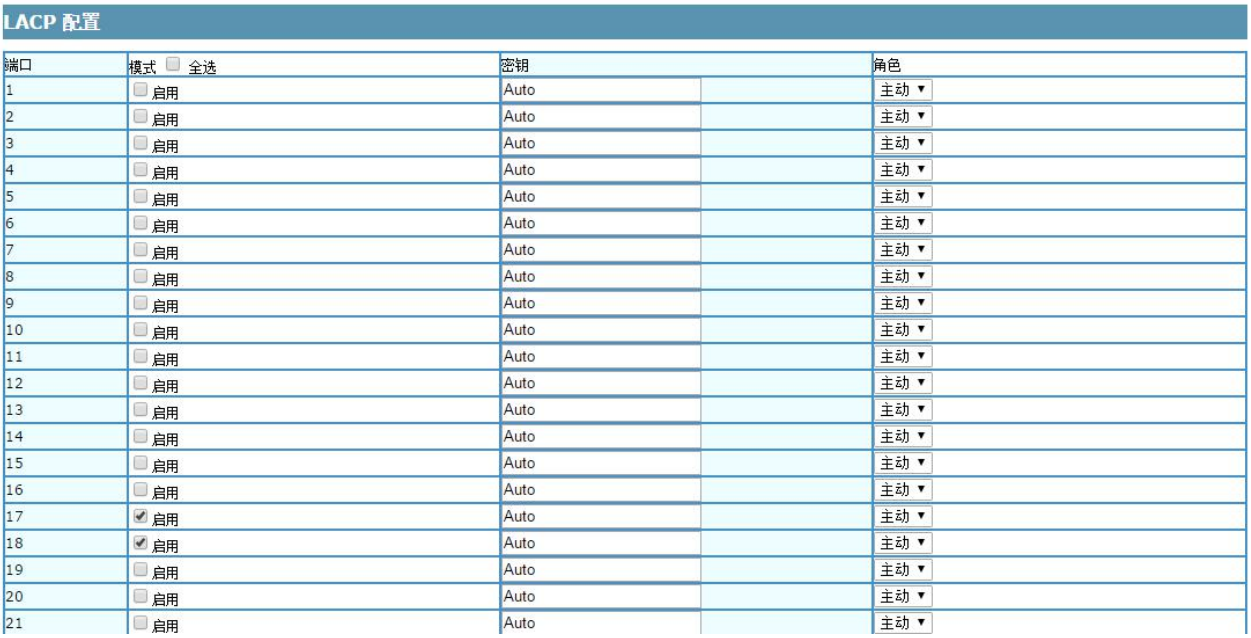
端口汇聚是将多个以太网端口汇聚在一起形成一个逻辑上的汇聚组，使用汇聚服务的上层实体把同一汇聚组内的多条物理链路视为一条逻辑链路。

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。

22.2. 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 配置界面各项参数说明如下表所示：

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

22.3. LACP信息

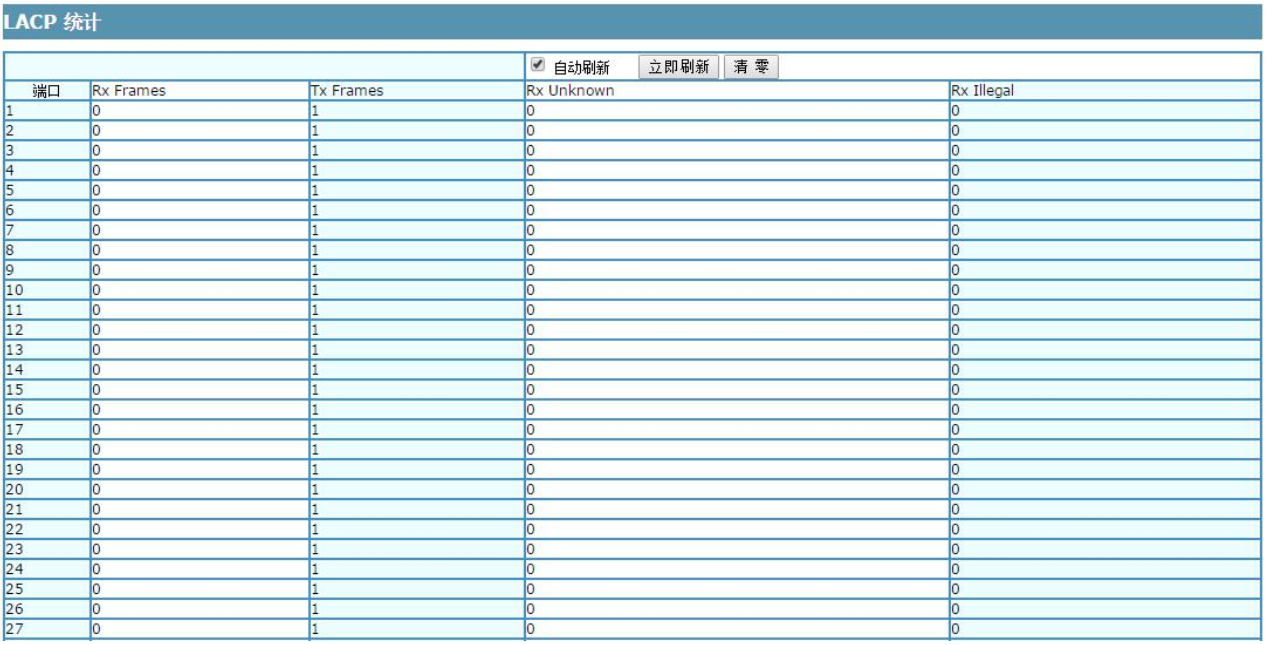
点击导航栏“设备控制→LACP→LACP 信息”，即可进入 LACP 的信息界面，如下图：

LACP 信息界面各项参数说明如下表所示：

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

22.4. 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：



端口	Rx Frames	Tx Frames	Rx Unknown	Rx Illegal
1	0	1	0	0
2	0	1	0	0
3	0	1	0	0
4	0	1	0	0
5	0	1	0	0
6	0	1	0	0
7	0	1	0	0
8	0	1	0	0
9	0	1	0	0
10	0	1	0	0
11	0	1	0	0
12	0	1	0	0
13	0	1	0	0
14	0	1	0	0
15	0	1	0	0
16	0	1	0	0
17	0	1	0	0
18	0	1	0	0
19	0	1	0	0
20	0	1	0	0
21	0	1	0	0
22	0	1	0	0
23	0	1	0	0
24	0	1	0	0
25	0	1	0	0
26	0	1	0	0
27	0	1	0	0

LACP 统计界面各项参数说明如下表所示：

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

第二十三章 LLDP

23.1. LLDP简介

LLDP（Link Layer Discovery Protocol，链路层发现协议），提供了一种标准的链路层发现方式，可以将本端设备的的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。LLDP 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。

23.2. LLDP设置

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。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：

LLDP 设置界面各项参数说明如下表所示：

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

23.3. LLDP信息

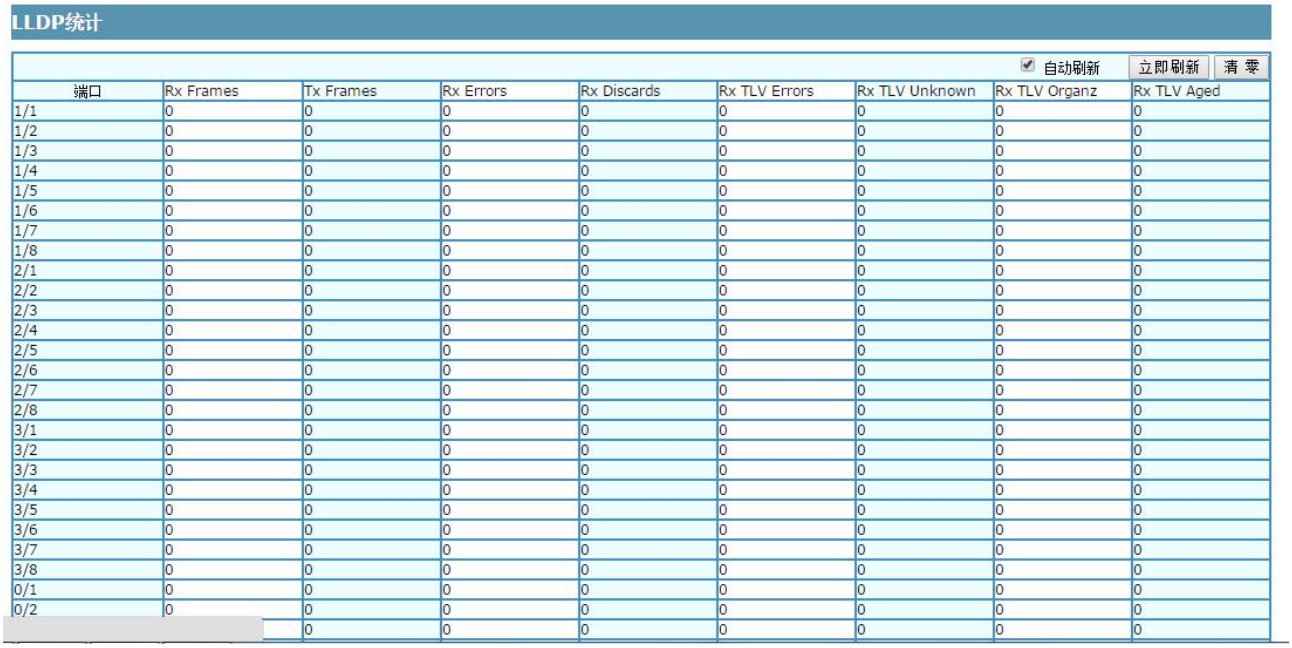
点击导航栏“设备控制→LLDP→LLDP 信息”，即可进入 LLDP 的 LLDP 信息界面，如下图：

LLDP 信息界面各项参数说明如下表所示：

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

23.4. 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：



LLDP 统计界面各项参数说明如下表所示：

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。

第二十四章　SNMP

24.1.　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。

SNMP 是目前最常用的环境管理协议。SNMP 被设计成与协议无关，所以它可以在 IP，IPX，AppleTalk，OSI 以及其他用到的传输协议上被使用。SNMP 是一系列协议组和规范，它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。

目前，几乎所有的网络设备生产厂家都实现了对 SNMP 的支持。领导潮流的 SNMP 是一个从网络上的设备收集管理信息的公用通信协议。设备的管理者收集这些信息并记录在管理信息库（MIB）中。这些信息报告设备的特性、数据吞吐量、通信超载和错误等。MIB 有公共的格式，所以来自多个厂商的 SNMP 管理工具可以收集 MIB 信息，在管理控制台上呈现给系统管理员。

SNMP 提供了一种统一的、跨平台的设备管理办法。

24.2.　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 视图界面各项参数说明如下表所示：

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

24.3. 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 团体界面各项参数说明如下表所示：

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

24.4. 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 群组界面各项参数说明如下表所示：

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

24.5. 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 用户界面各项参数说明如下表所示：

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

24.6. 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 主机界面各项参数说明如下表所示：

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、v2c 版本

团体名	用于识别 SNMP 的 trap 接收主机，当选择 v1 和 v2c 时使用相应的团体名

24.7. SNMP引擎

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：

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。

第二十五章 RMON

25.1. RMON简介

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

25.2. 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：

RMON 统计组界面各项参数说明如下表所示：

配置项	说明
端口号	交换机端口的逻辑编号，范围是 1~28
条目编号	统计组的索引号，范围是 1~65535

25.3. 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：

RMON 历史组界面各项参数说明如下表所示：

配置项	说明
端口号	交换机端口的逻辑编号，范围是 1~28
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

25.4. 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：

RMON 告警组界面各项参数说明如下表所示：

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， Dropevents 1.3.6.1.4.1.18000.3.1.1 Octets 1.3.6.1.4.1.18000.3.1.2 Packets 1.3.6.1.4.1.18000.3.1.3 Bcast_pkts 1.3.6.1.4.1.18000.3.1.4

	Mcast_pkts	1.3.6.1.4.1.18000.3.1.5
	Crc_align	1.3.6.1.4.1.18000.3.1.6
	Undersize	1.3.6.1.4.1.18000.3.1.7
	Oversize	1.3.6.1.4.1.18000.3.1.8
	Fragments	1.3.6.1.4.1.18000.3.1.9
	Jabbers	1.3.6.1.4.1.18000.3.1.10
	Collisions	1.3.6.1.4.1.18000.3.1.11
	Pkts_64	1.3.6.1.4.1.18000.3.1.12
	Pkts_65_127	1.3.6.1.4.1.18000.3.1.13
	Pkts_128_255	1.3.6.1.4.1.18000.3.1.14
	Pkts_256_511	1.3.6.1.4.1.18000.3.1.15
	Pkts_512_1023	1.3.6.1.4.1.18000.3.1.16
	Pkts_1024_1518	1.3.6.1.4.1.18000.3.1.17
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 0～2147483647	
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 0～2147483647	
下限事件号	下限阈值相应的事件号，取值范围为 1～65535	

25.5. 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：

RMON 告警组界面各项参数说明如下表所示：

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 1～127 个字符

事件类型	事件的操作方式，分为 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。
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 1～127 个字符

第二十六章　系统工具

26.1.　系统重启

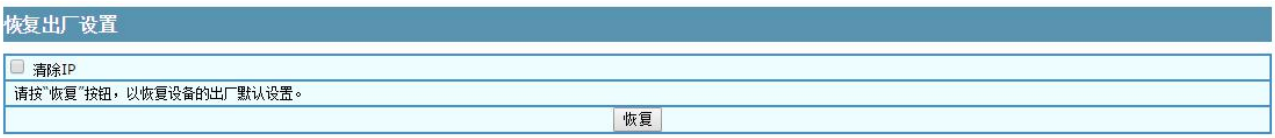
点击右上角“重启”，即可进入系统重启界面，如下图：

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。

26.2.　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：

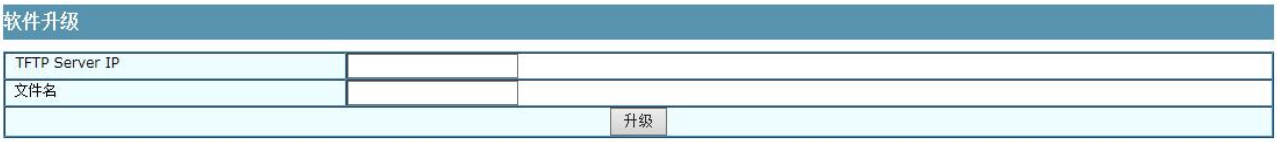


点击“恢复出厂值”按钮，系统会弹出确认对话框，如下图：

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。

26.3. 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：

TFTP Server IP：

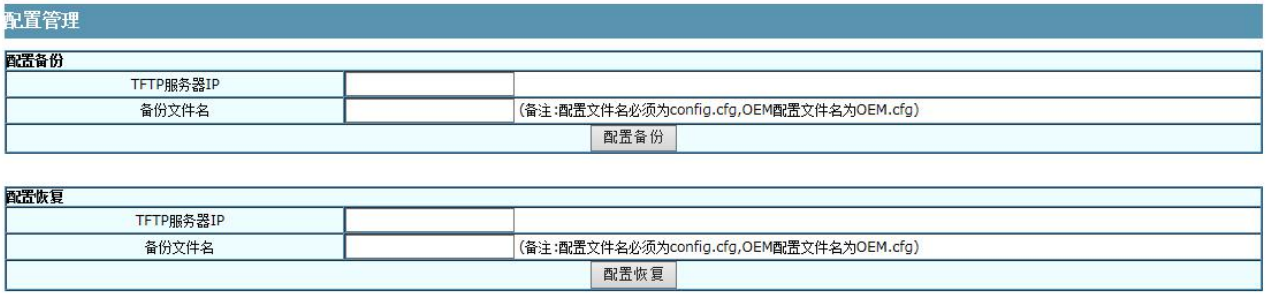
TFTP Server 的 IP 地址，这里需要注意，TFTP Server 和交换机能够正常通讯。

文件名：

升级文件的文件名，通常使用 vxworks.Z。

26.4. 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。

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。

26.5. 系统日志

使用 logger 用户登录，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：

系统日志界面各项参数说明如下表所示：

配置项	说明
模式	用于启用系统日志功能
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 ID	用于设置创建的日志服务器的编号

26.6. 系统日志查询

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：

系统日志界面各项参数说明如下表所示：

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

第二十七章　装置调试大纲

27.1.　装置检查

27.1.1.　装置通电前检查

开始调试前应对装置进行检查，装置外观应良好，端子排、网络接口、指示灯固定正确，无明显偏差、凹凸不平等状况。

装置正常出厂时已经进行绝缘检测，正常不需要进行绝缘检测。如购买后长期未用，必须在使用前进行绝缘检测，检测前必须断开装置直流电源。

确保装置独立接地端子可靠接地。

检查供电电压，确认数值在交换机规定正常工作电压范围内。

27.1.2.　装置通电后检查

(1)　正常运行时，运行灯常亮，没有告警灯点亮。

(2)　双电源配置时，分别检测两个电源、电源工作指示灯以及告警灯工作状况。

(3)　分别检测所有网络接口通信正常、对应前后指示灯闪烁正常。

(4)　检测CONSOLE接口通信正常。

27.2.　性能测试

使用专用网络测试仪如 IXIA 对设备进行功能、性能测试。

27.3.　配置备份及恢复

交换机在完成所有配置并联调正常后，应当对配置进行保存操作。此外，还应对配置进行备份操作，以便在错误设置情况下实现配置恢复，或用于对交换机故障替换时配置导入。配置备份数据还可用与错误配置情况下的故障分析。

第二十八章　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。