

iES-S2026C 交换机

Web 操作手册

出版日期：2019 年 3 月

版 本： V1.0

免责声明

本公司竭力使本手册中的信息尽可能准确、最新。然而本公司不能保证本手册完全没有任何技术错误或笔误，并保留在未通知用户的情况下对其修改的权利。

保留所有权限

本手册著作权属本公司所有。未经著作权人书面许可，任何单位或个人不得以任何方式摘录、翻版、复制、翻译或者用于商业目的的分发等行为。

侵权必究。

Copyright © All rights reserved.

目 录

前言.....	1
1 产品介绍.....	2
1.1 概述.....	2
1.2 软件特性.....	2
2 交换机的访问方式.....	3
2.1 调试串口访问.....	4
2.2 Telnet 和 SSH 访问.....	8
2.3 Web 访问.....	9
3 设备配置.....	11
3.1 系统配置.....	11
3.1.1 系统信息配置.....	11
3.1.2 管理 IP 配置.....	11
3.1.3 网络授时服务器配置.....	12
3.1.4 Syslog 服务器配置.....	13
3.1.5 告警配置.....	14
3.2 安全配置.....	15
3.2.1 用户管理配置.....	15
3.2.2 访问权限配置.....	16
3.2.3 Web/Telnet/SSH 设置.....	17
3.2.4 访问管理.....	19
3.2.5 SNMP 配置.....	19
3.2.6 RMON 配置.....	22
3.2.7 端口 MAC 数目限制.....	27
3.2.8 VLAN MAC 数目限制.....	28
3.2.9 NAS 配置（802.1X）.....	29
3.2.10 ACL 配置.....	32
3.2.11 IP 源保护.....	36
3.2.12 ARP 检测.....	38

3.2.13 AAA 配置.....	39
3.2.14 DOS 攻击防御.....	39
3.3 功能配置.....	42
3.3.1 流量越限告警配置.....	42
3.3.2 端口配置.....	43
3.3.3 聚合配置.....	45
3.3.4 STP 配置.....	48
3.3.5 LLDP 配置.....	50
3.3.6 端口镜像.....	52
3.3.7 VLANs 配置.....	52
3.3.8 Private VLANs 配置.....	55
3.3.9 MAC 地址表.....	56
3.3.10 Qos 配置.....	57
3.3.11 风暴抑制配置.....	62
3.3.12 IGMP Snooping 配置.....	62
3.3.13 GMRP 配置.....	65
3.3.14 MEP 配置.....	67
3.3.15 ERPS 配置.....	67
3.3.16 IEC61850 配置.....	67
4 设备状态.....	68
4.1 系统基本信息.....	68
4.1.1 自检信息.....	68
4.1.2 端口流量总览.....	71
4.1.3 端口详细统计.....	71
4.1.4 SFP 光口状态.....	72
4.1.5 日志信息.....	72
4.2 安全信息.....	74
4.2.1 RMON 信息.....	74
4.2.2 端口 MAC 数目限制.....	75
4.2.3 VLAN MAC 数目限制.....	76

4.2.4 NAS.....	76
4.2.5 ACL 信息.....	77
4.2.6 IP 源地址防护信息.....	78
4.2.7 ARP 信息.....	78
4.2.8 AAA.....	78
4.3 功能信息.....	79
4.3.1 LACP 信息.....	79
4.3.2 STP.....	80
4.3.3 LLDP 信息.....	81
4.3.4 VLANs.....	81
4.3.5 MAC 地址表.....	82
4.3.6 IGMP Snooping 状态.....	83
4.3.7 GMRP.....	84
5 设备维护.....	85
5.1 重启设备.....	85
5.2 恢复出厂设置.....	85
5.3 升级软件.....	85
5.4 版本切换.....	86
5.5 61850 配置保存.....	86
5.6 配置保存.....	86
5.7 配置上传.....	87

前言

本手册主要介绍了变电站网络交换机的访问方式和软件特性，并通过 Web 界面详细介绍了该系列交换机的配置使用方法。

1、标志约定

标志	说明
 注意	提醒操作、配置中应注意的事项，对操作内容描述的补充。
 说明	对操作内容进行必要的说明。
 警告	需格外注意的地方，不正确的操作可能会导致数据丢失或者设备损坏。

产品配套资料

变电站网络交换机的配套资料包括以下内容：

资料名称	内容介绍
iES-S2026C 交换机用户手册	详细了解站控层-外型结构、硬件规格以及安装拆卸方法
iES-S2026C 交换机 Web 操作手册	了解交换机软件功能并掌握各功能模块的 Web 配置方法及配置步骤

资料的获取方式

用户可以从以下途径及时获得产品的相关资料和文档：

- 通过随机光盘、随机印刷手册获取；

1 产品介绍

1.1 概述

该系列交换机主要应用在电力、交通、煤炭、冶金、油气、船舶等多个行业，能够适应严酷而危险的环境；支持 ERPs 环网保护协议，环网恢复时间小于 20ms，为系统的可靠运行提供多重保证；符合 IEC61850-3 和 IEEE1613 标准。

1.2 软件特性

该系列交换机具有丰富的软件特性，可以满足客户的不同需求。

- 冗余协议：RSTP/STP 和 ERPs；
- 组播协议：IGMP Snooping、GMRP 和静态组播；
- 交换属性：VLAN、PVLAN、QoS、ARP；
- 带宽管理：端口聚合、端口流量配置；
- 安全管理：IEEE802.1x、RADIUS、HTTPS、SSH、用户分级管理、端口隔离、ACL、MAC 地址数量限制、MAC 地址过滤、来源访问限制、管理端口绑定；
- 同步协议：SNTP；
- 设备管理：软件升级，配置上传/下载、日志记录；
- 设备诊断：端口镜像、LLDP；
- 告警功能：端口告警、电源告警、温度告警；
- 网络管理：支持 CLI、Telnet、Web 管理、SNMP 和 IEC61850 管理；

2 交换机的访问方式

iES-S2026C 交换机支持 4 种方式访问交换机：

- 调试串口访问；
- Telnet 访问；
- SSH 访问；
- Web 浏览器访问；

在默认出厂配置下，交换机只开放了调试串口作为访问接口。如果用户需要通过 Web 方式访问交换机，步骤如下：

- 1) 连接交换机调试串口到 PC；
- 2) 按照下面调试串口的方式进入命令行终端；
- 3) 输入命令 `ip conf` 获取交换机 IP 地址，比如默认的 IP 地址如下：

```
IP Configuration:
```

```
=====
```

```
DHCP Client      : Disabled
IP Address       : 192.168.2.254
IP Mask          : 255.255.255.0
IP Router        : 192.168.2.1
VLAN ID          : 1
```

- 4) 输入命令 `sec sw http mode enable` 使能交换机 Web 访问；
- 5) 输入命令 `sec sw http mode disable` 禁止 Web 访问交换机；
- 6) 输入命令 `sys reboot` 重启交换机，应用更改；
- 7) 输入命令 `sys res def` 恢复出厂设置；
- 8) 按回车，可显示所有命令行菜单；

```

Switch:/>
General Commands:
-----
Help/?: Get help on a group or a specific com
Up      : Move one command level up
Logout: Exit CLI

Command Groups:
-----
System      : System settings and reset optio
IP          : IP configuration and Ping
Port       : Port management
MAC        : MAC address table
VLAN       : Virtual LAN
PVLAN      : Private VLAN
Security    : Security management
STP        : Spanning Tree Protocol
Aggr       : Link Aggregation
Link Aggr  : Link Aggregation Control Protoc

```

9) 输入 / 可以返回主目录;

```

Switch:/security/switch>/
Switch:/>

```

10) 输入 ip setup 192.168.2.253 255.255.255.0 192.168.2.1, 可以修改交换机 ip;

2.1 调试串口访问

可以使用 Windows XP 系统的超级终端或者其他支持串口连接的软件通过调试串口访问交换机。下面以超级终端为例介绍怎样通过调试串口访问到交换机。使用其他字符串终端工具访问交换机的方法是类似的。

- 1、用 DB9-RJ45 电缆线连接 PC 机的串行通信口和交换机的 Console 口;
- 2、从 Windows XP 桌面打开超级终端, [开始]→[程序]→[附件]→[通讯]→[超级终端], 如图 1.1.所示;



图 1.1 超级终端

3、建立一个新连接“qq”，如图 1.2；

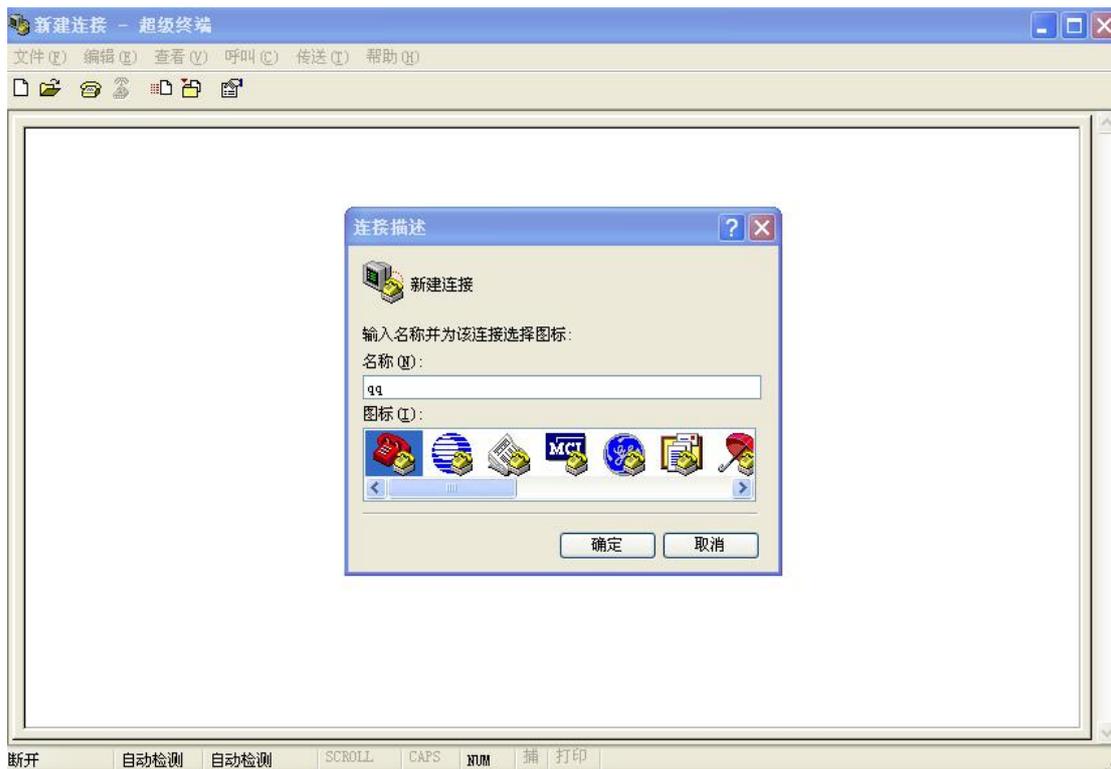


图 1.2 新建连接

4、选择正确的通信端口进行连接，如图 1.3 所示；

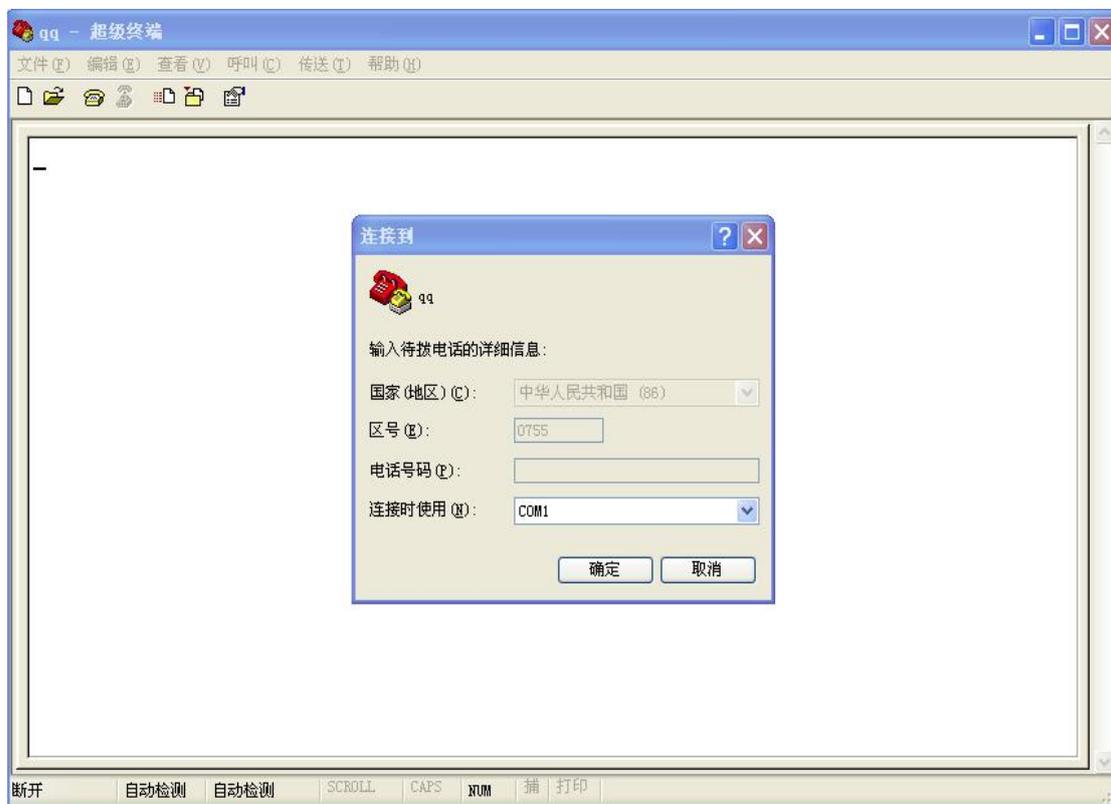


图 1.3 通信端口

**说明:**

如果不清楚当前设备的通信端口，可以右击[我的电脑]→[属性]→[硬件]→[设备管理器]→[端口]查看 Console 口使用的通信端口。

5、串口参数配置如图 1.4 所示，每秒位数(波特率)：115200；数据位：8；奇偶校验：无；停止位：1；数据流控制：无；

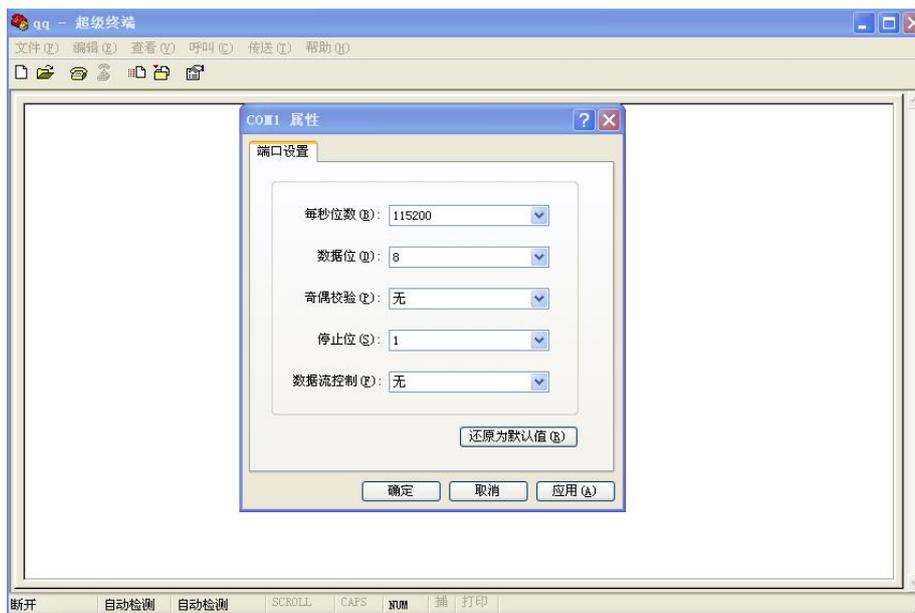


图 1.4 属性配置

6、点击<确定>按钮，可以成功进入交换机的命令行界面，按<回车>键进入用户视图，如图 1.5 所示；

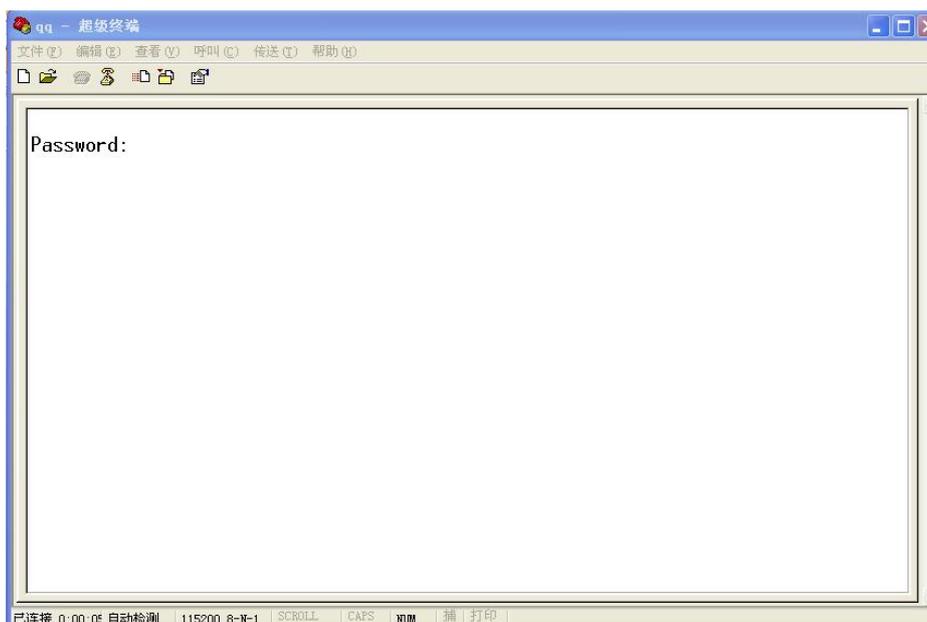


图 1.5 CLI 界面

7、再次按<回车>键，会提示 Username:输入 admin 然后按<回车>键，会提示 Password:输入 123456q! @然后按<回车>键，进入 CLI 管理界面，如图 1.6 所示；

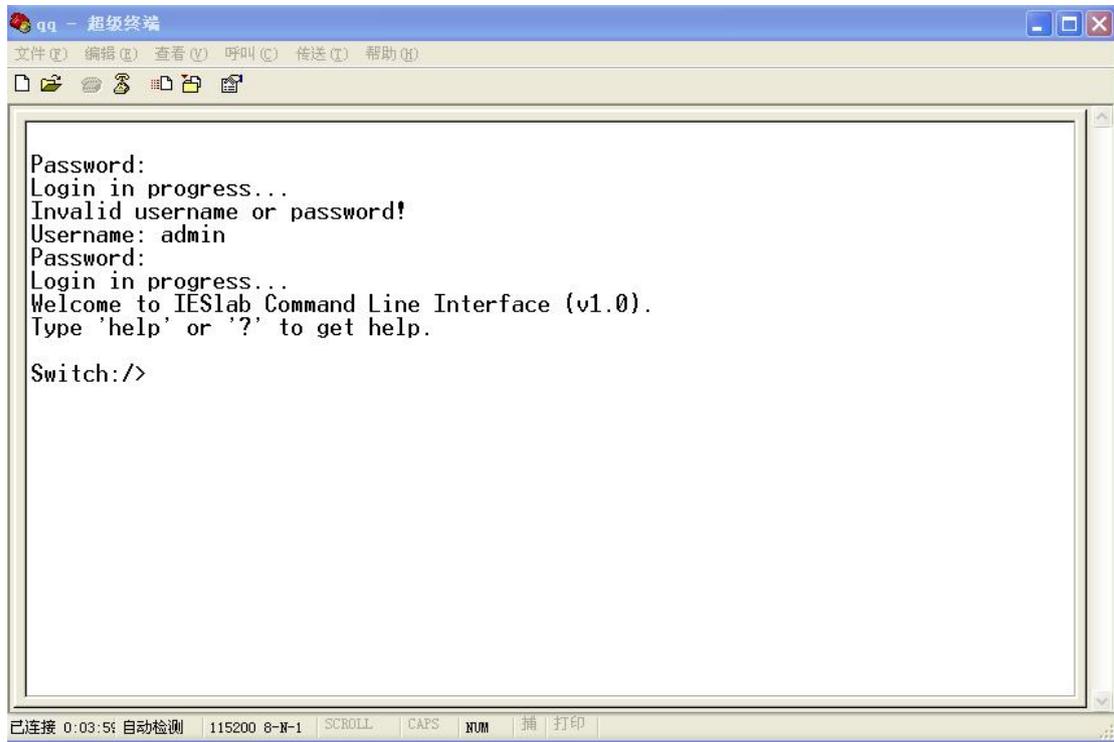


图 1.6 进入 CLI 界面

2.2 Telnet 和 SSH 访问

Telnet 登录要求 PC 机和交换机能够正常通信。SSH 的访问方式与之类似，下面以 Telnet 为例。



说明：

Windows 7 系统中需要通过控制面板开启 Telnet 客户端服务，即可访问。

- 1、在运行对话框中输入“telnet IP 地址”，如图 1.7 所示；



图 1.7 Telnet 访问



说明：

如果不清楚当前交换机的 IP 地址，请参考“3.1.2 管理 IP 配置”章节获取 IP 地址。

- 2、登录到 Telnet 界面，回车即可进入交换机命令行界面，如图 1.8 所示；

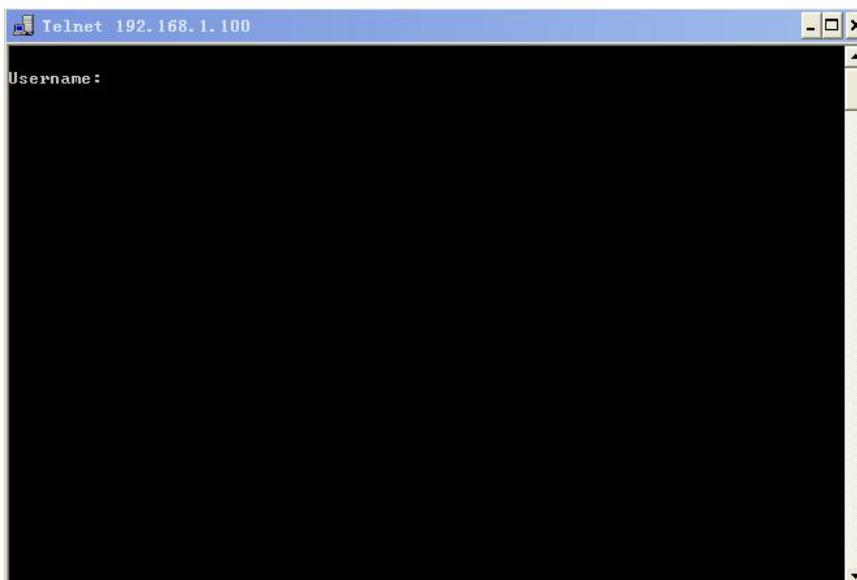


图 1.8 Telnet 界面

3、输入 **admin** 然后按<回车>键，会提示输入密码，输入 **123456q!@**然后按<回车>键即可进入系统，如图 1.9 所示；

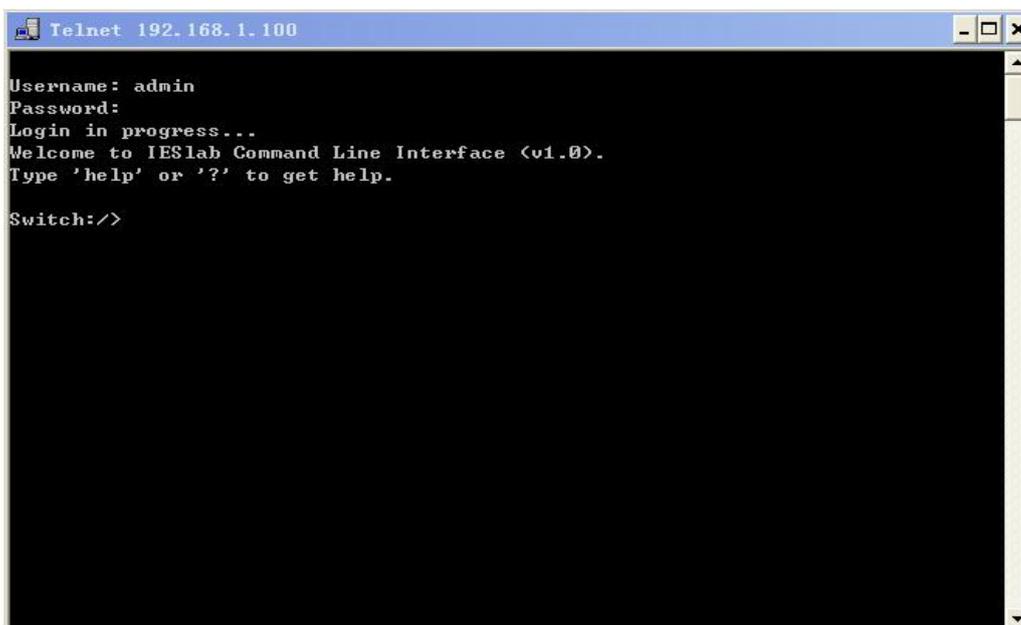


图 1.9 进入 Telnet 界面

2.3 Web 访问

默认情况下交换机 Web 访问关闭，通过串口输入命令 `sec sw http mode enable` 使能交换机 Web 访问；输入命令 `sys reboot` 重启交换机，应用更改；之后便可以通过浏览器访问交换机的维护页面。通过串口输入命令 `sec sw http mode disable` 禁止 Web 访问交换机。

Web 登录要求 PC 机和交换机能够正常通信。



说明：

推荐使用 IE8.0 或以上版本浏览器，使 Web 管理界面更加友好。

1、在浏览器地址栏中输入“*IP 地址*”（交换机出厂 IP 为 192.168.2.254），出现登录对话框如图 1.10 所示，输入默认用户名为“admin”，初始密码“123456q!@”，验证码，点击<登录系统>按钮；



图 1.10 Web 登录

**说明:**

- 如果不清楚当前交换机的 IP 地址,请参考“3.1.2 管理 IP 配置”章节获取 IP 地址;
- 建议用户及时修改设备的登录密码以防非法用户登录。

2、此时成功登录到交换机页面,左边是配置导航树,如图 1.11 所示;

端口状态概述

图 1.11 Web 界面

点击导航树顶端的<打开>、<关闭>按钮,可以使所有导航树打开、关闭。点击右上角的<帮助>可以进行相应页面的导航帮助,点击<退出系统>可以退出当前 Web 管理系统,如需要再次进入系统,则需要重新登录。

3 设备配置

3.1 系统配置

3.1.1 系统信息配置

系统可配置信息包括联系人、装置描述、系统位置、交换机工作电源数量、出厂时间、投运时间、系统时间、以及时区配置，如图 3.1 所示。以上信息根据现场情况进行修改，修改完之后点击<保存>按钮，保存设置。

系统信息配置

联系人	IESLAB
装置描述	Switch
系统位置	Jinan,Shandong, P.R.China(250100)
工作电源数量	2
出厂时间(YYYY-MM-DD hh:mm:ss)	2018-01-01 12:00:00
投运时间(YYYY-MM-DD hh:mm:ss)	2018-01-01 12:00:00
系统时间(YYYY-MM-DD hh:mm:ss)	2019-02-27 19:07:47

时区配置

时区配置	
时区	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi ▼
<input type="button" value="保存"/> <input type="button" value="撤销"/>	

图 3.1 系统信息配置

3.1.2 管理 IP 配置

1、通过调试串口查看交换机 IP 地址

调试串口访问交换机登录到命令行界面时，在管理视图下输入命令“**ip conf**”可以查看交换机的 IP 地址，如图 3.2 所示；

```
Switch:/>ip conf
IP Configuration:
=====
DHCP Client      : Disabled
IP Address       : 192.168.2.254
IP Mask          : 255.255.255.0
IP Router        : 192.168.2.1
VLAN ID          : 1
```

图 3.2 查看 IP 地址

2、IP 地址配置

交换机的 IP 地址和网关可以通过手动配置如图 3.3 所示。页面中 VLAN ID 选项是划分管理 IP 的 VLAN，可以将管理 VLAN 和数据 VLAN 区分开来，但为了管理交换机将此 VLAN ID 修改之后，还需要在级联端口和管理端口下面添加相应的 VLAN ID，比如用 23、24 作为级联口，24 作为管理口，VLAN ID 设为 10，则需要在 Port 23、24 下面添加 VLAN ID10（参考 3.3.8 节 VLAN Trunk 配置）。

IP设置

	可配置	当前配置
DHCP客户端	<input type="checkbox"/>	<input type="button" value="更新"/>
IP地址	192.168.2.254	192.168.2.254
IP子网掩码	255.255.255.0	255.255.255.0
IP路由	192.168.2.1	192.168.2.1
VLAN ID	1	1

图 3.3 IP 地址



注意：

- IP 地址和网关必须在同一网段中，否则无法修改 IP 地址。
- 页面中 VLAN ID 修改之后，不能通过 PC 直接连接管理口来管理交换机，必须通过 VPN 或者其他级联方式来管理交换机

3.1.3 网络授时服务器配置

网络授时服务器配置如图 3.4 所示，如果需要使用 NTP 对时，选择<模式>“使能”，<服务器>如“202.120.2.101”（须为交换机所能访问的 NTP 服务器的地址），配置完成可点击<保存>按钮保存设置，点击<更新时间>按钮，系统会立即更新时间。如果不点击<更新时间>系统会定期和服务器对时。

NTP配置

模式	禁用 ▼
轮询间隔	4
服务器	

图 3.4 网络授时服务器配置

3.1.4 Syslog 服务器配置

Syslog 服务器配置如图 3.5 所示,如果需要启用 **syslog** 服务器,<服务模式>选择“使能”,<服务器地址>设置为 **syslog** 服务器的地址,<日志级别>设置为需要上传的日志级别。如果选择“重要”,只上传“重要”级别的信息;如果选择“次要”,将上传“重要”、“次要”级别的信息;如果选择“通告”,将上传“重要”、“次要”、“通告”级别的信息。

系统日志配置

服务器模式	禁用 ▼
服务器地址	
日志级别	通告 ▼

图 3.5 syslog 服务器配置

使用 **tftpd32** 作为 **syslog** 服务器,设置完成后可以收到交换机发出的告警信息,如图 3.6 所示。

系统日志配置

服务器模式	使能
服务器地址	192.168.2.77
日志级别	通告

保存 撤销

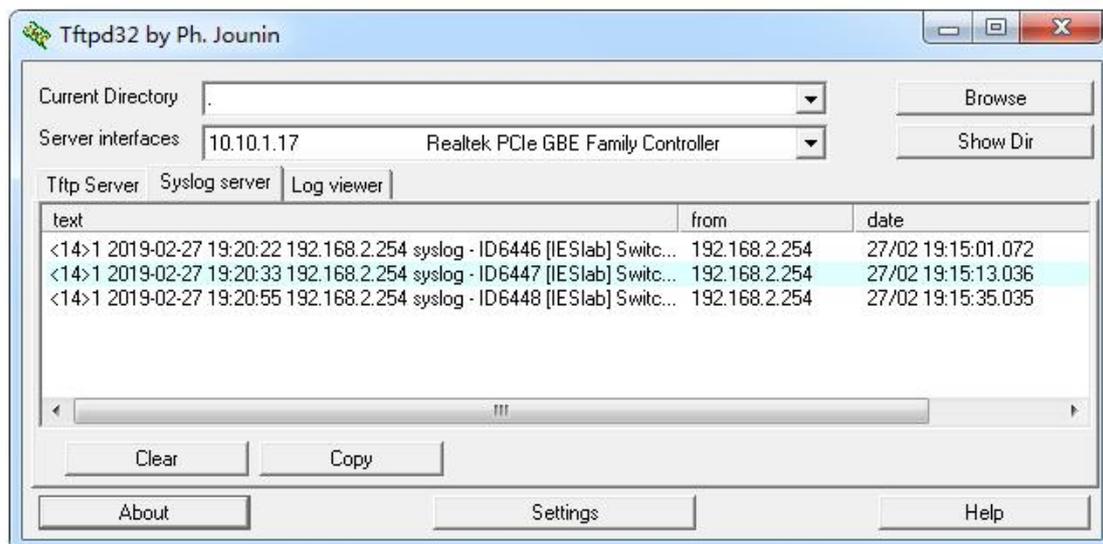


图 3.6 syslog 服务器配置

3.1.5 告警配置

告警配置如图 3.7 所示，根据需要设置预警配置和告警配置，有以下类型 CPU 温度、主板温度 CPU 负载、工作电压，预警配置的定值一定比告警配置的定值要小，当实际温度高于预警值时，就会发出预警信息，当实际温度高于告警温度时将发出告警信息。

预警配置

类型	定值	
CPU温度	75	°C
主板温度	65	°C
CPU负载	80	%
工作电压	12	V

告警配置

类型	定值	
CPU温度	80	°C
主板温度	70	°C
CPU负载	90	%
工作电压	14	V

保存 撤销

图 3.7 告警配置

3.2 安全配置

3.2.1 用户管理配置

用户管理配置如图 3.8 所示，系统默认的用户名为“admin”，权限级别为“15”。

用户配置

用户名	权限级别
admin	15

添加新用户

图 3.8 用户配置界面

点击“admin”可以修改用户密码，和密码过期时间，是否为审计用户，密码过期时间的 0 表示密码永远有效，如图 3.9 所示。

编辑用户

用户设置	
用户名称	admin
用户密码
再次输入密码
权限级别	15 ▼
审计用户	否 ▼
密码过期时间(天)	0 ▼

保存 撤销 取消

图 3.9 编辑用户

点击<添加新用户>按钮，如图 3.10 所示，可以新加用户。用户密码需 8 位以上数字和字母组合，权限级别为 1-15，数字越大权限越高。

添加用户

用户设置	
用户名称	user1
用户密码
再次输入密码
权限级别	10 ▼
审计用户	否 ▼
密码过期时间(天)	30 ▼

保存 撤销 取消

图 3.10 添加新用户

3.2.2 访问权限配置

访问权限配置如图 3.11 所示，可以根据需要，调整查看、配置交换机各项功能对应的权限级别。

权限级别配置

组的名称	权限级别			
	配置 只读	配置/执行 读/写	状态/统计 只读	状态/统计 读/写
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼
Debug	15 ▼	15 ▼	15 ▼	15 ▼
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼
EEE	5 ▼	10 ▼	5 ▼	10 ▼
ERPS	5 ▼	10 ▼	5 ▼	10 ▼
ETH_LINK_OAM	5 ▼	10 ▼	5 ▼	10 ▼
EVC	5 ▼	10 ▼	5 ▼	10 ▼
GMRP	5 ▼	10 ▼	5 ▼	10 ▼
IP	5 ▼	10 ▼	5 ▼	10 ▼
IPMC_LIB	5 ▼	10 ▼	5 ▼	10 ▼
IPMC_Snooping	5 ▼	10 ▼	5 ▼	10 ▼
LACP	5 ▼	10 ▼	5 ▼	10 ▼
LLDP	5 ▼	10 ▼	5 ▼	10 ▼
LLDP_MED	5 ▼	10 ▼	5 ▼	10 ▼
MAC_Table	5 ▼	10 ▼	5 ▼	10 ▼

图 3.11 权限级别配置

3.2.3 Web/Telnet/SSH 设置

1、方法配置

认证方法配置如图 3.12 所示，默认为本地认证，可以选择“none”、“local”、“RADIUS”、“TACACS+”认证。

认证方法配置

客户端	认证方法	回退	权限级别
console	local ▼	<input type="checkbox"/>	1 ▼
telnet	local ▼	<input type="checkbox"/>	1 ▼
ssh	local ▼	<input type="checkbox"/>	1 ▼
web	local ▼	<input type="checkbox"/>	1 ▼

保存 撤销

图 3.12 认证方法配置

2、管理端口配置

管理端口配置如图 30 所示，默认配置为全端口管理，可以选择 1-26 号任一端口作为交换机的管理端口。

管理端口配置

管理端口	全端口
------	-----

保存 撤销

图 3.13 管理端口配置



注意:

- 选择单一端口管理交换机后，只有指定端口可以管理交换机，其它端口将不能访问交换机。指定端口管理在开启 802.1X 或者 RADIUS 等需要安全认证的管理方式后，将自动转为全端口管理。

3、SSH 配置

SSH 配置如图 3.14 所示，可以选择 SSH 版本，使能或不使能 SSH，SSH 的最大登录数，SSH 的登录超时时间（默认为 10 分钟）。

SSH配置

版本	SSH版本2
模式	使能
最大登录数	4
SSH超时时间(分钟)	10

保存 撤销

图 3.14SSH 配置

4、Telnet 配置

Telnet 配置如图 3.15 所示，可以使能或不使能 Telnet，设置最大登录数，设置登录超时时间。

TELNET配置

模式	使能
最大登录数	4
超时时间(分钟)	10

保存 撤销

图 3.15 Telnet 配置

5、HTTPS 配置

HTTPS 如图 3.16 所示，可以使能或不使能 HTTPS，启用或禁用自动重定向功能，设置登录超时时间。

HTTPS配置

模式	使能
自动重定向	禁用
自动超时时间(分钟)	10

保存 撤销

图 3.16 HTTPS 配置

**注意：**

▶ 当使能自动重定向功能之后，使用 http 登录会自动转到 https 登录。

6、HTTP 配置

HTTP 如图 3.17 所示，可以选择使能或不使能 HTTP，配置登录超时时间。

HTTP配置

模式	使能
超时时间(分钟)	10

保存 撤销

图 3.17 HTTP 配置

3.2.4 访问管理

访问管理配置如图 3.18 所示，在“模式”后可以选择禁用或使能此项功能，点击<添加新实例>按钮，添加起始 IP、结束 IP，根据需要选择管理方式，配置完成后点击<保存>按钮保存设置。配置完成后，只有选中的管理方式在指定的地址段才能管理交换机。

访问管理配置

模式	禁用
----	----

删除	起始IP地址	结束IP地址	HTTP/HTTPS	SNMP	TELNET/SSH
添加新实例					

保存 撤销

图 3.18 访问管理配置

3.2.5 SNMP 配置**1、SNMPv2 配置**

进入 SNMP->基本配置，如图 3.19 所示，默认 SNMP 是使能的，使用的版本是 SNMPv2，SNMP Trap 是不使能的。

SNMP系统配置

SNMP使能	使能
SNMP版本	SNMP v2c
只读团体名	public
读写团体名	private
Engine ID	800007e5017f000001

SNMP Trap配置

Trap开关	不使能
Trap版本	SNMP v1
Trap团体名	public
Trap目的IP地址	
Trap认证失败	使能
Trap连接和断开	使能
Trap通知模式	使能
Trap通知超时时间(秒)	1
Trap通知重试次数	5

图 3.19 SNMP 基本配置

使能 Trap 开关，选择 Trap 版本 SNMPv2，Trap 目的 IP 地址为 SNMP 服务器地址，其他保持默认设置，即可完成 SNMPv2 配置，点击<保存>按钮保存设置。

2、SNMPv3 配置

进入 SNMP->基本配置，如图 3.19 所示，默认 SNMP 是使能的，使用的版本是 SNMPv2，选择版本为 SNMPv3。

使能 Trap 开关，选择 Trap 版本 SNMPv3，Trap 目的 IP 地址为 SNMP 服务器地址，Trap Probe Security Engine ID 不使能，Trap Security Engine ID，需要填写 10 位以上数字或数字字母组合。其他保持默认设置，点击<保存>按钮保存设置，如图 3.19 所示。

SNMP系统配置

SNMP使能	使能
SNMP版本	SNMP v3
只读团体名	public
读写团体名	private
Engine ID	800007e5017f000001

SNMP Trap配置

Trap开关	使能
Trap版本	SNMP v3
Trap团体名	public
Trap目的IP地址	192.168.1.125
Trap认证失败	使能
Trap连接和断开	使能
Trap通知模式	使能
Trap通知超时时间(秒)	1
Trap通知重试次数	5
Trap Probe Security Engine ID	不使能
Trap Security Engine ID	1234567890
Trap安全名称	None

保存

撤销

图 3.19 SNMPv3 基本配置

进入 SNMP->用户配置页面，点击<添加新条目>按钮，设置 Engine ID 为基本配置里设置的 ID，用户名为“aaa”可根据需要设置，认证密码和密钥，点击<保存>按钮保存设置，如图 3.20 所示。

SNMPv3用户配置

删除	Engine ID	用户名	安全级别	认证协议	认证密码	密钥协议	密钥
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
<input type="checkbox"/>	1234567890	aaa	Auth, Priv	MD5	DES

添加新条目

保存

撤销

图 38 SNMPv3 用户配置

回到 SNMP->基本配置，选择 Trap 安全名称为刚设置的用户名，点击<保存>按

钮保存设置，如图 3.21 所示。

SNMP Trap配置

Trap开关	使能
Trap版本	SNMP v3
Trap团体名	public
Trap目的IP地址	192.168.1.125
Trap认证失败	使能
Trap连接和断开	使能
Trap通知模式	使能
Trap通知超时时间(秒)	1
Trap通知重试次数	5
Trap Probe Security Engine ID	不使能
Trap Security Engine ID	1234567890
Trap安全名称	aaa

保存 撤销

图 3.21 SNMPv3 用户名设置

3.2.6 RMON 配置

1、介绍

RMON(Remote Network Monitoring, 远程网络监视)基于SNMP体系结构使网络中管理设备能够积极主动的对被管理设备进行监控和管理。RMON包括网络管理站和网络上的Agent, 管理站对网络中的Agent进行管理; Agent可以统计端口上的各种流量信息。

RMON 主要实现统计和告警功能, 统计功能指 Agent 可以按周期统计端口的各种流量信息, 比如某段时间内某网段上收到的报文总数等。告警功能指 Agent 能监控指定 MIB 变量的值, 当该值达到告警阈值时(比如报文总数达到指定值), 能自动记录告警事件到 RMON 日志或者向管理设备发送 Trap 消息。

2、RMON 组

RMON 规范(RFC2819)中定义了多个RMON 组, 该系列设备实现了公有 MIB 中支持的统计组、历史组、事件组和告警组, 每个组最多支持32个表项。

➤ 统计组

统计组指系统对端口的各种流量信息进行统计，并将统计结果存储在以太网统计表中以便管理设备随时查看。统计信息包括网络冲突数、CRC 校验错误报文数、过小(或超大)的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。

➤ 历史组

历史组规定系统定期对端口各种流量信息进行采样，并将采样值存储在历史记录表中以便管理设备随时查看。历史组统计的是采样间隔内各种数据的统计值。

➤ 告警组

RMON 告警管理可对指定的告警变量进行监视。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

➤ 事件组

事件组用来定义事件索引号及事件处理方式。事件组定义的事件用于告警组配置项中，当监控对象达到告警条件时，就会触发事件，事件有如下几种处理方式：

Log: 将事件相关信息记录在本设备**RMON**日志表中。

Trap: 向网管站发送**Trap**消息告知该事件的发生。

Log-Trap: 既在本设备上记录**RMON**日志，又向网管站发送**Trap**消息。

None: 不做任何处理。

3、Web 配置

➤ **RMON**统计配置

进入**RMON**->**RMON**统计，点击<添加新条目>按钮，ID范围 1 到 65535，数据源表明想要监控的端口 ID（如端口10），点击<保存>按钮，如图3.22所示。

RMON统计配置

删除	ID	数据源
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. 10

图 3.22 RMON 统计配置

➤ RMON历史配置

进入RMON->RMON历史，点击<添加新条目>按钮，ID范围 1 到 65535，数据源表明想要监控的端口 ID（如端口10），其他保持默认设置，点击<保存>按钮保存设置，如图3.23所示。

RMON历史配置

删除	ID	数据源	间隔	桶	桶授予
<input type="checkbox"/>	1	.1.3.6.1.2.1.2.2.1.1. 10	1800	50	50

图 3.23 RMON 历史配置

➤ RMON告警配置

进入RMON->RMON告警，点击<添加新条目>按钮，如图3.24所示。

RMON告警配置

删除	ID	间隔	变量	样本类型	值	启动告警	上升阈值	上升指数	下降阈值	下降指数
<input type="checkbox"/>	1	30	.1.3.6.1.2.1.2.2.1.1. 10.10	Delta	0	RisingOrFalling	100	1	50	1

图 3.24 RMON 告警配置表

ID

配置范围：1~65535

间隔

配置范围：1~65535

功能：配置端口信息的采样周期，该值最好与历史表中的采样间隔配置保持一致。

变量

数据格式为 xx.xx，小数点前面表示变量，可能的变量如下面所示，InOctets

为 10，InUcastPkts 为 11，依次加 1；小数点后面表示端口号。
如.1.3.6.1.2.1.2.2.1.10.1 表示 1 号端口的 InOctets 变量。

可能的变量有：

InOctets: 在接口接收到的字节总数，包括帧字符。

InUcastPkts: 转发到上层协议的单播个数。

InNUcastPkts: 转发到上层协议的广播和组播个数。

InDiscards: 丢弃的进入数据包的个数，即使数据包正常。

InErrors: 接收到的包含错误的进入数据包，阻止他们被转发到上层协议。

InUnknownProtos:由于未知或不支持的协议，丢弃的进入数据包的个数。

OutOctets: 从这个接口发送字节的个数，包括帧字符。

OutUcastPkts: 要求发送的单播数据包的个数。

OutNUcastPkts: 要求发送的广播和多播数据包的个数。

OutDiscards: 丢弃的出站数据包的个数，即使数据包正常。

OutErrors: 由于错误，不能发送的出站数据包的个数。

OutQLen: 输出数据包队列的长度（以数据包为单位）。

样本类型

选择变量，和计算与阈值相比较的数值，采样方法。可能的采样类型有：

Absolute: 直接获取采样。

Delta: 计算采样之间的区别（默认）。

值

上一次采样周期统计的数值。

启动告警

选择变量，和计算与阈值相比较的数值，采样方法。可能的采样类型有：

Rising 上升触发告警，当数值第一次大于上升阈值。

FallingTrigger 下降触发告警，当数值第一次小于下降阈值。

RisingOrFalling 上升或下降触发告警，当数值第一次大于上升阈值或小于下降阈值（默认）。

上升阈值

配置范围：-2147483648~2147483647

功能：配置上升沿阈值，当采样值超过该上升沿阈值并且报警类型为

RisingAlarm 或者 **RisOrFallAlarm** 时，将会报警并激活上升事件索引。

上升事件索引

配置范围：1~65535

功能：配置上升事件的索引，即对上升沿告警的处理方式。

下降阈值

配置范围：-2147483648~2147483647

功能：配置下降沿阈值，当采样值低于该下降沿阈值并且报警类型为 FallingAlarm 或者 RisOrFallAlarm 时，将会报警并激活下降事件索引。

下降事件索引

配置范围：1~65535

功能：配置下降事件的索引，即对下降沿告警的处理方式。

➤ RMON事件配置

进入RMON->RMON事件，点击<添加新条目>按钮，如图3.25所示。

RMON事件配置

删除	ID	Desc	类型	团体名	事件持续时间
<input type="checkbox"/>	1	alarm	none	public	11822

图 3.25 RMON 事件配置表

ID

配置范围：1~65535。需要和 RMON 告警里的上升指数、下降指数一致。

Desc

配置范围：0~127 个字符

功能：对事件的描述。

事件类型

配置选项：NONE/LOG/Snmp-Trap/Log and Trap

默认配置：NONE

功能：配置当告警发生时所采用的事件类型，即对告警的处理方式。

事件团体

配置范围：1~127 个字符

3.2.7 端口 MAC 数目限制

端口 MAC 数目限制如图 3.26 所示。

端口MAC数目限制配置

系统配置

开关	不使能
老化使能	<input type="checkbox"/>
老化时间	3600 秒

端口配置

端口	使能	限制	动作	状态	重开
*	<>	4	<>		
1	不使能	4	None	不使能	重开
2	不使能	4	None	不使能	重开
3	不使能	4	None	不使能	重开
4	不使能	4	None	不使能	重开
5	不使能	4	None	不使能	重开
6	不使能	4	None	不使能	重开
7	不使能	4	None	不使能	重开
8	不使能	4	None	不使能	重开
9	不使能	4	None	不使能	重开
10	不使能	4	None	不使能	重开
11	不使能	4	None	不使能	重开

图 3.26 端口 MAC 数目限制配置

开关

使能或不使能，默认不使能。

老化使能

如果选中，安全的 MAC 地址将进行老化。

老化时间

老化周期可以设置一个数值，在 10 和 10,000,000 秒之间。默认为 3600 秒。

端口配置

使能：使能或不使能端口的 MAC 数目限制，默认不使能。

限制：限制端口的 MAC 数目，范围为 1-1024，默认为 4。

动作

如果已经达到限制，交换机可以采取下面几种操作之一：

None:不允许在这个端口超过限制的 MAC 地址，但是不采取行动。

Trap: 如果 Limit + 1 MAC 地址发现在这个端口，发送一个 SNMP trap。

如果老化关闭，只有一个 SNMP trap 将会发送，但是，老化使能，在每次超过限制时新的 SNMP traps 都会被发送。

Shutdown: 如果 Limit + 1 MAC 地址在这个端口被发现，关闭这个端口。

这就意味着，所有的安全 MAC 地址都会再这个端口移除，同时，不会有新的地址会被学习。即使，端口连接被物理断开和重新连接（通过端口电缆），端口都会保持关闭（shut down）。这里有 3 种方法，可以重新打开端口：

- 1) 重启交换机。
- 2) 交换机或端口关闭或重新使能 Limit Control。
- 3) 点击“重开”按钮。

Trap & Shutdown: 如果 Limit + 1 MAC 地址被发现在这个端口，上边描述的 "Trap" 和 "Shutdown" 操作将会被执行。

3.2.8 VLAN MAC 数目限制

VLAN MAC 数目限制如图 3.27 所示。

系统配置

全局使能	不使能 <input type="button" value="v"/>
老化使能	<input type="checkbox"/>
老化时间	10 秒

Vlan配置

Vlan ID	使能	限制数目
1	不使能 <input type="button" value="v"/>	1
2	不使能 <input type="button" value="v"/>	1
3	不使能 <input type="button" value="v"/>	1
4	不使能 <input type="button" value="v"/>	1

图 3.27 VLAN MAC 数目限制配置

开关

使能或不使能，默认不使能。

老化使能

如果选中，安全的 MAC 地址将进行老化。

老化时间

老化周期可以设置一个数值，在 10 和 10,000,000 秒之间。默认为 10 秒。

VLAN 配置

使能：使能或不使能 VLAN 的 MAC 数目限制，默认不使能。

限制：限制 VLAN 的 MAC 数目，范围为 1-1024，默认为 4。

3.2.9 NAS 配置（802.1X）

NAS 配置如图 3.28 所示。

网络访问服务器配置
更新

系统配置

开关	不使能
重认证使能	<input type="checkbox"/>
重认证周期	3600 秒
EAPOL超时时间	30 秒
老化周期	300 秒
持续时间	10 秒
RADIUS-Assigned QoS使能	<input type="checkbox"/>
RADIUS-Assigned VLAN使能	<input type="checkbox"/>
客户VLAN使能	<input type="checkbox"/>
客户VLAN ID	1
最大重认证次数	2
允许客户VLAN如果EAPOL可见	<input type="checkbox"/>

端口配置

端口	管理员状态	RADIUS-Assigned QoS使能	RADIUS-Assigned VLAN使能	Guest VLAN使能	端口状态	重启
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	强制认证	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	全局禁用	重认证 重新初始化
2	强制认证	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	全局禁用	重认证 重新初始化

图 3.28 NAS 配置

1、802.1X 本地认证

进入设备配置->功能配置->STP 配置->CIST 端口配置页面(使能 NAS 之前需要先关掉 STP)，将 STP 使能下方框里的“√”去掉，然后点击<保存>按钮保存设置，如图 3.29 所示。

生成树协议(STP)/公共和内部生成树(CIST)端口配置

公共和内部生成树(CIST)聚合端口配置							
端口	STP 使能	路径消耗	优先级	管理边缘	自动边缘	限制	
						角色	T
-	<input type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

公共和内部生成树(CIST)普通端口配置							
端口	STP 使能	路径消耗	优先级	管理边缘	自动边缘	限制	
						角色	T
*	<input type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1	<input type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	<input type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	<input type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	<input type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	<input type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

图 3.29 禁止 STP

然后进入设备配置->安全配置->NAS 配置页面，使能系统配置及端口的 802.1X 本地认证，如图 3.30 所示。

网络访问服务器配置

系统配置

开关	使能
重认证使能	<input checked="" type="checkbox"/>
重认证周期	3600 秒
EAPOL超时时间	30 秒
老化周期	300 秒
持续时间	10 秒
RADIUS-Assigned QoS使能	<input type="checkbox"/>
RADIUS-Assigned VLAN使能	<input type="checkbox"/>
客户VLAN使能	<input type="checkbox"/>
客户VLAN ID	1
最大重认证次数	2
允许客户VLAN如果EAPOL可见	<input type="checkbox"/>

端口配置

端口	管理员状态	RADIUS-Assigned QoS使能	RADIUS-Assigned VLAN使能
*	<>	<input type="checkbox"/>	<input type="checkbox"/>
1	本地802.1X	<input type="checkbox"/>	<input type="checkbox"/>
2	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
3	强制认证	<input type="checkbox"/>	<input type="checkbox"/>

图 3.30 开启端口 1 的本地 802.1X 认证

2、802.1X RADIUS 认证

进入设备配置->功能配置->STP 配置->CIST 端口配置页面(使能 NAS 之前需要先关掉 STP)，将 STP 使能下方框里的“√”去掉，然后点击<保存>按钮保存设置，如图 3.29 所示。

然后进入设备配置->安全配置->NAS 配置页面，使能系统配置及端口的 802.1X Radius 认证，如图 3.31 所示。

网络访问服务器配置

系统配置

开关	使能
重认证使能	<input checked="" type="checkbox"/>
重认证周期	3600 秒
EAPOL超时时间	30 秒
老化周期	300 秒
持续时间	10 秒
RADIUS- Assigned QoS使能	<input type="checkbox"/>
RADIUS- Assigned VLAN使能	<input type="checkbox"/>
客户VLAN使能	<input type="checkbox"/>
客户VLAN ID	1
最大重认证次数	2
允许客户VLAN如果EAPOL可见	<input type="checkbox"/>

端口配置

端口	管理员状态	RADIUS- Assigned QoS使能	RADIUS- Assigned VLAN使能
*	<>	<input type="checkbox"/>	<input type="checkbox"/>
1	基于端口802.1X	<input type="checkbox"/>	<input type="checkbox"/>
2	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
3	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
4	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
5	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
6	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
7	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
8	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
9	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
10	强制认证	<input type="checkbox"/>	<input type="checkbox"/>
11	强制认证	<input type="checkbox"/>	<input type="checkbox"/>

图 3.31 开启端口 1 的 802.1X Radius 认证

最后进入设备配置->安全配置->AAA 页面，配置 Radius 服务器的 IP 及密

码，如图 3.32 所示。

认证服务器配置

通用服务器配置

超时时间	15	秒
停滞时间	300	秒

RADIUS认证服务器配置

#	使能	IP地址	端口	Secret
1	<input checked="" type="checkbox"/>	192.168.1.125	1812	*****
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

图 3.32 Radius 服务器配置

3.2.10 ACL 配置

ACL(Access Control List)指访问控制列表，通常用来规划网络中的访问层次，以期达到优化网络流量，加强网络安全的作用。

ACL 是一张规则表，交换机按照顺序执行这些规则，并且处理每一个进入端口的数据包。每条规则根据数据包的属性(如源地址、目的地址和协议)要么允许、要么拒绝数据包通过。由于规则是按照一定顺序处理的，因此每条规则的相对位置对于确定允许和不允许什么样的数据包通过网络至关重要。当我们要想阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者想要拒绝某一协议簇的所有通信流量时，可以使用 ACL 来实现这一目标。利用 ACL 也可检查数据包的源地址，目的地址，以及数据包的特定协议类型、端口号等。可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其它协议的流量通过，可灵活多变的设计 ACL 的测试条件。

ACL 配置共 3 个界面：

速率限定：端口限速，每秒允许通过的报文个数

访问控制列表：配置交换机访问控制列表，即过滤规则

端口：端口 ACL 规则选择

1、ACL 速率限定

ACL 速率限定配置如图 3.33 所示。

ACL速率限定配置

速率限定ID	速率	单位
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

保存 撤销

图 3.33 ACL 速率限定

速率限定 ID

交换机支持 16 条限速规则，若端口需要加载限速规则，该 ID 号为标识符。

速率

允许数值:0-128k in pps 或者 0, 100, 100, 100, ..., 1000000 in kbps.。

单位

指定速率单位，允许数值如下：

pps: 包每秒.

kbps: 千比特（Kbits）每秒.

2、访问控制列表

ACL 访问控制列表配置如图 3.34 所示，每台交换机支持 128 个 ACEs。

访问控制列表配置

Ingress端口	优先级/位掩码	数据帧类型	动作	速率限定	端口重定向	镜像	计数器
+							

图 3.34 ACL 访问控制列表

点击  图标，新加 ACE 列表，具体配置内容随选项不同而区别，如图 3.35 所示。

ACE配置

Ingress端口	全部 Port 1 Port 2 Port 3 Port 4
过滤规则	任何
帧类型	任何

动作	允许
速率限定	不使能
EVC Policer	不使能
端口重定向	不使能 Port 1 Port 2 Port 3 Port 4
镜像	不使能
日志	不使能
关闭	不使能
计数器	42

VLAN参数

802.1Q Tagged	任何
VLAN ID过滤	任何
Tag优先级	任何

保存 撤销 取消

图 3.35 新加 ACE 列表

3、ACL 端口配置

ACL 端口配置如图 3.36 所示。

ACL端口配置 刷新 清除

端口	Policy ID	动作	速率限制 ID	EVC Policer	EVC Policer ID	端口重定向	镜像	日志	关闭
*	<input type="text" value="0"/>	<> ▾	▾	<> ▾	<input type="text" value="1"/>	不使能 ▴ Port 1 Port 2 Port 3 ▾	<> ▾	<> ▾	<> ▾
1	<input type="text" value="1"/>	允许 ▾	▾	使能 ▾	<input type="text" value="1"/>	不使能 ▴ Port 1 Port 2 Port 3 ▾	不使能 ▾	不使能 ▾	不使能 ▾
2	<input type="text" value="0"/>	允许 ▾	▾	不使能 ▾	<input type="text" value="1"/>	不使能 ▴ Port 1 Port 2 Port 3 ▾	不使能 ▾	不使能 ▾	不使能 ▾
3	<input type="text" value="0"/>	允许 ▾	▾	不使能 ▾	<input type="text" value="1"/>	不使能 ▴ Port 1 Port 2 Port 3 ▾	不使能 ▾	不使能 ▾	不使能 ▾
4	<input type="text" value="0"/>	允许 ▾	▾	不使能 ▾	<input type="text" value="1"/>	不使能 ▴ Port 1 Port 2 Port 3 ▾	不使能 ▾	不使能 ▾	不使能 ▾

图 3.36 ACL 端口配置

Policy ID

选择优先级应用在这个端口上。范围 0-7. 默认值是 0.

动作

选择转发规则：允许("Permit")或者拒绝("Deny").默认值：允许 "Permit".

速率限制 ID

设置端口的速率限制。有效值：Disabled 或者 数值 1 -16.默认值是："不使能".

EVC Policer

设置 EVC 策略状态使能或者关闭。默认是关闭"Disabled".

EVC Policer ID

设置端口的 EVC 策略的 ID。有效值：Disabled 或者 1 – 128.

端口重定向

选择数据帧可以重定向的端口，如果行动(action)设置为 permitted，此时不能设置，默认值为"Disabled".

镜像

指定镜像操作的端口，默认值是："不使能"，不被镜像。

日志

指定日志操作的端口，默认值是："不使能"。请注意系统日志内存的大小和写日志文件的速率的限制。

关闭

指定关闭操作的端口，默认值是："不使能"。

状态

指定端口的状态，有效值: 使能: 通过修改 ACL 用户模式的端口配置来重新打开端口。不使能: 通过修改 ACL 用户模式的端口配置来关闭端口。默认值："使能"。

3.2.11 IP 源保护

1、IP 源保护使能配置

可以通过设置 IP 源保护来限制访问的客户端，IP 源检测使能配置如图 3.37 所示。

IP源检测配置

开关 不使能

动态转化为静态

端口模式配置

端口	模式	最大动态客户端数
*	<>	<>
1	不使能	无限制
2	不使能	无限制
3	不使能	无限制
4	不使能	无限制
5	不使能	无限制
6	不使能	无限制

图 3.37 IP 源保护使能配置

IP 源检测开关

全局使能开关，默认为不使能。当模式设置为使能” Enabled “时，所有配置的 ACEs 将会丢失。

端口模式

指定 IP 源检测 使能的端口号。只有在全局 Global 模式和端口 Port 模式都使能的情况下，端口的 IP 源检测 功能才会打开。

最大动态客户端数

指定端口可以学习的动态客户端的最大个数。可能的数值有 0、1、2 或者 无限。如果端口模式使能，并且最大动态客户端数数值等于 0，这就意味着，在指定端口，只能转发与静态实例匹配的 IP 数据包。

2、静态 IP 检测表

IP 源保护静态 IP 源检测表如图 3.38 所示。

静态IP源检测表

删除	端口	VLAN ID	IP地址	MAC地址
<input type="button" value="添加新实例"/>				
<input type="button" value="保存"/>		<input type="button" value="撤销"/>		

图 3.38 静态 IP 检测表

点击<添加新实例>按钮，选择端口号，VLAN，允许访问的客户端 IP，允许访问的客户端 MAC，点击<保存>按钮，如图 3.39 所示。配置完成之后，接在端口的客户端只有与静态表里相符才能访问。

静态IP源检测表

删除	端口	VLAN ID	IP地址	MAC地址
<input type="checkbox"/>	1	1	192.168.1.125	10-78-d2-78-88-51
<input type="button" value="添加新实例"/>				
<input type="button" value="保存"/>		<input type="button" value="撤销"/>		

图 3.39 新加静态 IP 检测表

3.2.12 ARP 检测

1、ARP 配置

ARP 使能配置如图 3.40 所示。

ARP Inspection配置

开关

端口模式配置

端口	开关
*	<>
1	不使能
2	不使能
3	不使能
4	不使能

图 3.40 ARP 使能

2、ARP 静态表

ARP 静态表配置如图 3.41 所示。

静态ARP检测表

删除	端口	VLAN ID	MAC地址	IP地址
<input type="button" value="添加新实例"/>				
<input type="button" value="保存"/>	<input type="button" value="撤销"/>			

图 3.41 ARP 静态表配置

点击<添加新实例>按钮，选择端口号、VLAN、IP、MAC，点击<保存>按钮，如图 3.42 所示。

静态ARP检测表

删除	端口	VLAN ID	MAC地址	IP地址
<input type="checkbox"/>	1	1	10-78-d2-78-88-51	192.168.1.125

图 3.42 新加 ARP 静态表

3.2.13 AAA 配置

AAA 配置如图 3.43 所示，可以设置服务器的 IP 及密码，具体应用见 4.2.9 NAS 配置（802.1X）。

认证服务器配置

通用服务器配置

超时时间	15	秒
停滞时间	300	秒

RADIUS认证服务器配置

#	使能	IP地址	端口	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

RADIUS计数服务器配置

#	使能	IP地址	端口	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

TACACS+认证服务器配置

#	使能	IP地址	端口	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

图 3.43 AAA 配置

3.2.14 DOS 攻击防御

通过配置 DOS 攻击防御，可以避免黑客或不良组织利用 DOS 攻击造成电力设备符合过大而导致整个电力系统瘫痪。DOS 攻击防御配置分为 6 个子项，DOS 攻击防御的配置通过配置 ACE 完成。

UDP Flood 攻击防御配置示例完成后的状态如图 3.44 所示,可以根据图示说明进行在开始或者结尾处插入新 ACE 配置,编辑当前 ACE 配置,上移或者下移当前 ACE 配置,删除当前 ACE 配置。

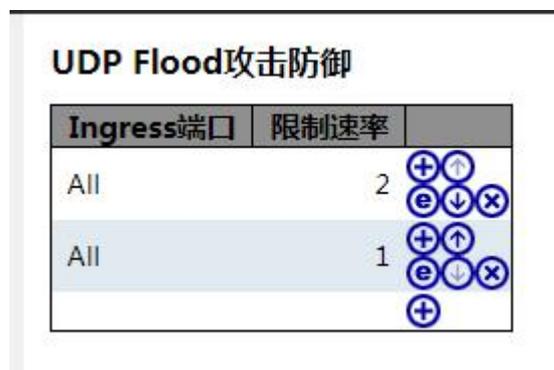


图 3.44 UDP Flood 攻击防御配置示例

Ping Of Death 攻击防御配置示例完成后的状态如图 3.45 所示,可以根据图示说明进行在开始或者结尾处插入新 ACE 配置,编辑当前 ACE 配置,上移或者下移当前 ACE 配置,删除当前 ACE 配置。

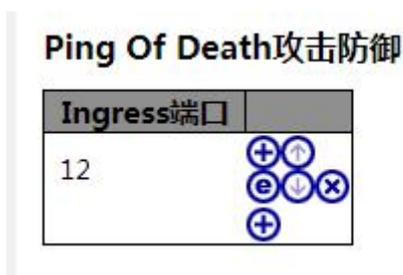


图 3.45 Ping Of Death 攻击防御配置示例

Ping Flood 攻击防御配置示例完成后的状态如图 3.46 所示,可以根据图示说明进行在开始或者结尾处插入新 ACE 配置,编辑当前 ACE 配置,上移或者下移当前 ACE 配置,删除当前 ACE 配置。



图 3.46 Ping Flood 攻击防御配置示例

SYN Flood 攻击防御配置示例完成后的状态如图 3.47 所示,可以根据图示说明进行在

开始或者结尾处插入新 ACE 配置，编辑当前 ACE 配置，上移或者下移当前 ACE 配置，删除当前 ACE 配置。

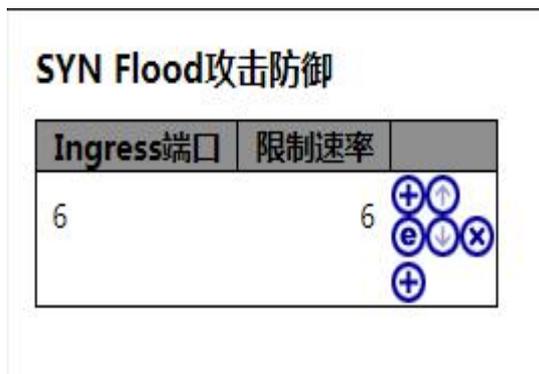


图 3.47 SYN Flood 攻击防御配置示例

Smurf 攻击防御配置示例完成后的状态如图 3.48 所示，可以根据图示说明进行在开始或者结尾处插入新 ACE 配置，编辑当前 ACE 配置，上移或者下移当前 ACE 配置，删除当前 ACE 配置。

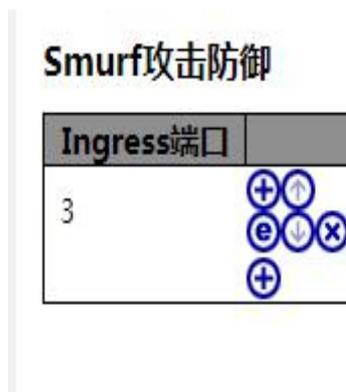


图 3.48 Smurf 攻击防御配置示例

Tear Drop 攻击防御配置示例完成后的状态如图 3.49 所示，可以根据图示说明进行在开始或者结尾处插入新 ACE 配置，编辑当前 ACE 配置，上移或者下移当前 ACE 配置，删除当前 ACE 配置。



图 3.49 Tear Drop 攻击防御配置示例



说明:

⊕: 插入一个新 ACE 配置, 在当前行的顶端; ⊖: 编辑当前 ACE 配置; ↑: 上移当前 ACE 配置; ↓: 下移当前 ACE 配置; ✕: 删除当前 ACE 配置; ⊕: 插入一个新 ACE 配置, 在当前行的底端

UDP Flood 攻击防御、Ping Flood 攻击防御、SYN Flood 攻击防御, 点击⊕进行配置, 端口有全选和 1~26Port (单选), 限定速率, 不使能和 1~16 的速率, 配置后点击保存即可。

Ping Of Death 攻击防御、Smurg 攻击防御、Tear Drop 攻击防御, 点击⊕进行配置, 端口有全选和 1~26Port (单选), 配置后点击保存即可。

3.3 功能配置

3.3.1 流量越限告警配置

设置好端口告警速录, 取消告警速率和采用周期后, 勾选使能复选框, 点击保存, 即配置好某一端口的流量越限告警配置。配置结果如图 3.51 所示。

流量越限告警设置

端口	使能	告警速率	取消告警速率	单位	采样周期(秒)
*	<input type="checkbox"/>	80000	70000	*	10
1	<input type="checkbox"/>	80000	70000	Kbps	10
2	<input type="checkbox"/>	80000	70000	Kbps	10
3	<input type="checkbox"/>	80000	70000	Kbps	10
4	<input type="checkbox"/>	80000	70000	Kbps	10
5	<input checked="" type="checkbox"/>	82000	77000	Kbps	10
6	<input type="checkbox"/>	80000	70000	Kbps	10
7	<input type="checkbox"/>	80000	70000	Kbps	10
8	<input type="checkbox"/>	80000	70000	Kbps	10
9	<input type="checkbox"/>	80000	70000	Kbps	10
10	<input type="checkbox"/>	80000	70000	Kbps	10
11	<input type="checkbox"/>	80000	70000	Kbps	10
12	<input type="checkbox"/>	80000	70000	Kbps	10
13	<input type="checkbox"/>	80000	70000	Kbps	10
14	<input type="checkbox"/>	80000	70000	Kbps	10
15	<input type="checkbox"/>	80000	70000	Kbps	10
16	<input type="checkbox"/>	80000	70000	Kbps	10
17	<input type="checkbox"/>	80000	70000	Kbps	10
18	<input type="checkbox"/>	80000	70000	Kbps	10
19	<input type="checkbox"/>	80000	70000	Kbps	10
20	<input type="checkbox"/>	80000	70000	Kbps	10
21	<input type="checkbox"/>	80000	70000	Kbps	10
22	<input type="checkbox"/>	80000	70000	Kbps	10
23	<input type="checkbox"/>	80000	70000	Kbps	10
24	<input type="checkbox"/>	80000	70000	Kbps	10
25	<input type="checkbox"/>	80000	70000	Kbps	10
26	<input type="checkbox"/>	80000	70000	Kbps	10

保存 撤销

图 3.51 流量越限告警配置



注意：

- 流量越限告警功能要在 SNMP 系统配置使能的情况下才可以开启
- 本机在出厂默认设置中，SNMP/RMON 功能为关闭状态，若需要开启流量越限告警功能，则应当配合 SNMP/RMON 功能使能状态

3.3.2 端口配置

端口配置页面如图 3.52 所示。

端口配置

更新

端口	连接	速率		流控制			最大帧长	过度冲突模式	功率控制
		当前状态	可配置速率	当前Rx	当前Tx	可配置			
*		<>	<>			<input type="checkbox"/>	9600	<>	<>
1	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
2	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
3	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
4	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
5	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
6	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
7	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
8	● 100fdx	100fdx	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
9	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
10	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
11	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
12	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
13	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
14	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
15	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
16	● 100fdx	100fdx	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
17	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
18	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
19	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
20	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
21	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
22	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
23	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
24	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600	丢弃	禁用
25	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600		
26	● 断开	断开	自动	×	×	<input type="checkbox"/>	9600		

保存

撤销

图 3.52 端口配置页面

连接

以图形的形式显示当前的连接状态。绿色指示连接，红色指示断开。

当前状态

提供本端口当前的连接速率。

可配置模式

为指定端口选择任何可用的连接速率，可能的速率：

禁用 - 关闭交换机端口的操作；

自动 - Cu 端口和连接对方自动协商连接速率，然后选择一个最高的速率；

10Mbps HDX - 强制 cu 端口在 10Mbps half duplex 模式；

10Mbps FDX - 强制 cu 端口在 10Mbps full duplex 模式；

100Mbps HDX - 强制 cu 端口在 100Mbps half duplex 模式；

100Mbps FDX - 强制 cu 端口在 100Mbps full duplex 模式；

1Gbps FDX - 强制 cu 端口在 1Gbps full duplex 模式;

100-FX - SFP 端口速率设置为 100-FX;

1000-X - SFP 端口速率设置为 1000-X。

流量控制

当前 rx : 当外部数据量涌入超过网卡本身的数据处理量之后, 会暂停接收新的数据请求, 直到处理完当前数据, 并主动发送管理信息告知通信链路对端。

当前tx : 当收到通信链路对端降低速率的请求, 则暂时关闭或降低发送数据速率。

配置: 启用端口流量控制功能。

过度冲突模式

当过量冲突(默认为16次)发生后, 交换机对报文的处理方式:

丢弃: 丢弃该报文

重启: 重新启动backoff 算法, 说明之前的计数值无法保证数据在16次的碰撞内发送出去。

功率控制

电源节能控制, 减少不必要的端口功率输出, 参数如下:

禁用: 关闭节能功能。

ActiPHY: 当发现交换机端口未存在通信链路的情况下会自动关闭该端口电源或进入待机模式。本交换机和对端交换机均开启了流量控制且工作在全双工模式下, 此功能才会正常工作。

PerfectReach: 若端口存在通信链路, 则交换机会智能自动计算并检测电缆长度后调整功率大小。

使能: 始终都启用端口节能功能。

3.3.3 聚合配置

按照聚合方式的不同, 端口汇聚可以分为“静态聚合”, “静态 LACP 聚合”, “动态 LACP 聚合”三类。

➤ 静态聚合

只需将感兴趣的端口加入指定聚合组即可。这里需要注意的是, 同一端口, 当已加入静态汇聚中后, 将不能再开启 LACP 协议, 反之当不能把已开启 LACP 协议的端口加入到静态聚合组中。

➤ 静态 LACP 聚合

端口操作 key 的工作模式决定采用 LACP 协议的端口是静态聚合还是动态聚合, 若为感兴趣的端口指定键值, 即为静态聚合; 反之则为动态聚合。

➤ 动态 LACP 聚合

动态 LACP 协商的过程如下:

1) 通过 LACP 的报文交互, 确定哪台交换机为主机, lacp 报文中优先级

越小则越优先级越高。

2) 确定主机之后，再确定交换机上的哪个端口为主端口，lacp 中端口优先级越小则优先级越高，然后以此端口为参考，表明可以加入聚合组（准入）

3) 确定参考端口后，本机的其他端口如果配置了使能 LACP 且属性和参考端口一致，也可以加入聚合组。

4) 对端收到 LACP 报文后，按照主机定义的规矩选择可以成为聚合组的成员。

1、静态聚合配置

静态聚合模式配置分成两部分：“负载均衡”及“聚合组配置”。

通过改变负载分担的模式可以灵活地实现聚合组流量的负载分担，系统利用 Hash 算法来计算负载分担的模式，该算法可依据报文中携带的服务端口号、IP 地址、MAC 地址、报文入端口等信息及其组合进行计算。

站控层-交换机支持以下工作模式：

- 基于源 MAC
- 基于目的 MAC
- 基于 IP
- 基于 TCP/UDP 端口号

应根据不同的网络环境设置合适的流量分配方式，以便能把流量较均匀地分配到聚合组的各个链路上，充分利用网络的带宽。

聚合模式配置（负载均衡）如图 3.53 所示。

聚合模式配置

Hash编码参与者	
源MAC地址	<input checked="" type="checkbox"/>
目的MAC地址	<input type="checkbox"/>
IP地址	<input checked="" type="checkbox"/>
TCP/UDP端口号	<input checked="" type="checkbox"/>

图 3.53 聚合模式配置

聚合组成员端口处于同一交换机中，每个本地聚合组可以包含最高 16 个成员端口。聚合组配置如图 3.54 所示（图中将 25 和 26 号端口加入聚合组 1）。

聚合组管理配置

组ID	端口成员																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
普通	<input checked="" type="checkbox"/>																									
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																							
2	<input type="checkbox"/>																									
3	<input type="checkbox"/>																									
4	<input type="checkbox"/>																									
5	<input type="checkbox"/>																									
6	<input type="checkbox"/>																									
7	<input type="checkbox"/>																									
8	<input type="checkbox"/>																									
9	<input type="checkbox"/>																									
10	<input type="checkbox"/>																									
11	<input type="checkbox"/>																									
12	<input type="checkbox"/>																									
13	<input type="checkbox"/>																									

保存 撤销

图 3.54 聚合组配置

2、LACP

LACP 端口配置如图 3.55 所示，端口 2、3 键值为 1 是一个静态 LACP 组，端口 4、5 键值为 2 是另一个静态 LACP 组，端口 7、8、9 是一个动态 LACP 组。

LACP端口配置

端口	LACP使能	键值	角色	超时时间	优先级	
*	<input type="checkbox"/>	<> ▾	<> ▾	<> ▾	32768	
1	<input type="checkbox"/>	自动 ▾	主动 ▾	快速 ▾	32768	
2	<input checked="" type="checkbox"/>	指定 ▾	1	主动 ▾	快速 ▾	32768
3	<input checked="" type="checkbox"/>	指定 ▾	1	主动 ▾	快速 ▾	32768
4	<input checked="" type="checkbox"/>	指定 ▾	2	主动 ▾	快速 ▾	32768
5	<input checked="" type="checkbox"/>	指定 ▾	2	主动 ▾	快速 ▾	32768
6	<input type="checkbox"/>	自动 ▾	主动 ▾	快速 ▾	32768	
7	<input checked="" type="checkbox"/>	自动 ▾	主动 ▾	快速 ▾	32768	
8	<input checked="" type="checkbox"/>	自动 ▾	主动 ▾	快速 ▾	32768	
9	<input checked="" type="checkbox"/>	自动 ▾	主动 ▾	快速 ▾	32768	

图 3.55 LACP 端口配置

3.3.4 STP 配置

1、STP 桥配置

STP 桥配置如图 3.56 所示。

生成树协议桥配置

基本设置

协议版本	RSTP ▼
桥优先级	32768 ▼
转发延迟	15
生存期	20
最大跳数	20
传输有效次数	6

图 3.56 STP 桥配置

协议版本

协议版本设置，有效值：STP 和 RSTP，默认为 RSTP。

桥优先级

控制网桥优先级，越低的数字，具有越高的优先级，默认为 32768。

转发延时

有效值范围 4 到 30 秒，默认为 15 秒。

生存期

当网桥是 Root Bridge 时，信息传输最大的老化时间。有效值：6 到 40 秒，最大值 MaxAge 必须 $\leq (FwdDelay-1)*2$ 。默认为 20 秒。

最大跳数

有效值：6 到 40 hops，默认为 20。

传输有效次数

每秒钟，一个网桥端口可以发送的 BPDU 数量。如果超过，发送的下一个 BPDU 将会延时。有效的数值范围是，1 到 10 BPDU 每秒。默认为 6。

2、端口配置

STP 端口配置如图 3.57 所示。

生成树协议(STP)/公共和内部生成树(CIST)端口配置

公共和内部生成树(CIST)聚合端口配置										
端口	STP 使能	路径消耗	优先级	管理边缘	自动边缘	限制		BPDU(桥数据协议单元) 保护	点对点	
						角色	TCN			
-	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	强制正确	

公共和内部生成树(CIST)普通端口配置										
端口	STP 使能	路径消耗	优先级	管理边缘	自动边缘	限制		BPDU(桥数据协议单元) 保护	点对点	
						角色	TCN			
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>	
1	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
2	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
3	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
4	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
5	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
6	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
7	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
8	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	
9	<input checked="" type="checkbox"/>	自动	128	无边缘	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	自动	

图 3.57 端口配置

STP使能

控制是否在这个交换机端口上使能，默认为使能。

路径消耗

端口路径开销成本设置，取值范围 1 ~ 200000000。只有在 **specific** 状态下才可输入 **path cost** 值，**auto** 下采用 802.1D 规则。

优先级

控制端口的优先级。取值范围 0/16/32/48/.../224/240。

管理边缘

边缘端口设置。

自动边缘

在这个桥端口，桥是否应该使能自动边缘检测。

限制角色

如果使能，这个端口不能被选择作为 CIST 或者 MSTI 的 Root 端口，即使它拥有最高的生成树优先级。在 Root 端口被选择之后，这样的端口将会被选择作为备用端口（Alternate Port）。如果设置，它将会导致生成树缺少连通性。它可以被一个网络管理员设置，用来防止桥扩展（external）到一个网络的核心区域（core region），影响生成树的有效拓扑结构。

限制TCN

如果使能，端口不能传播接收拓扑更改的通知，和拓扑修改到其他端口。如

果设置，在修改生成树有效的拓扑结构之后，它将导致临时损失连通性，结果产生一个持续的错误的学习状态本地信息。

BPDU保护

如果使能，导致一个端口不能接收有效的 BPDU。与之相反，相似的桥设置，端口边缘的状态不会影响本设置。

点对点

控制端口是否连接到一个点到点的 LAN，而非一个共享介质。这个可以自动决定，或者强制 true 或者 false。

3.3.5 LLDP 配置

目前，网络设备的种类日益繁多且各自的配置错综复杂，为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息，需要有一个标准的信息交流平台。LLDP（Link Layer Discovery Protocol，链路层发现协议）就是在这样的背景下产生的，它提供了一种标准的链路层发现方式，可以将本端设备的主要能力、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 参数配置如图 3.58 所示。

LLDP参数

Tx间隔	30	秒
Tx持续	4	次数
Tx延迟	2	秒
Tx重初始化	2	秒

图 3.58 LLDP 参数

Tx间隔

设备定期发送 LLDP 时间，范围是 5 – 32768s。

Tx持续

设备保存 LLDP 的次数，则 TTL 是 hold*interval，范围是 2-10 次。

Tx延迟

即当设备配置发生变化时，发送 LLDP 的延迟时间，范围是 1-8192s。

Tx重初始化

当端口设为禁用，或关闭端口 LLDP 功能或交换机重启时，设备会告知邻居设备在接下来的 reinit 时间内，LLDP 报文无效。范围是 1-10s。

LLDP 端口配置如图 3.59 所示。

LLDP端口配置

端口	模式	CDP发现	可选的TLVs				
			端口描述符	系统名称	系统描述符	系统容量	管理地址
*	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
1	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
2	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
3	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
4	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
5	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
6	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
7	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
8	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
9	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
10	使能	<input type="checkbox"/>	<input checked="" type="checkbox"/>				

图 3.59 LLDP 端口配置

模式

使能：设备不仅发送 LLDP 报文，同时接收并分析收到的 LLDP 报文

RX：只接收并分析收到的 LLDP 报文

TX：只发送 LLDP 报文，丢弃收到的 LLDP 报文

不使能：关闭 LLDP 报文的接收和发送

端口描述符

Optional TLV: 当选中，"端口描述符" 被包含进 LLDP 信息。

系统名称

Optional TLV: 当选中，"系统名称" 被包含进 LLDP 信息。

系统描述符

Optional TLV: 当选中，"系统描述符" 被包含进 LLDP 信息。

系统容量

Optional TLV: 当选中，"系统容量" 被包含进 LLDP 信息。

管理地址

Optional TLV:当选中，"管理地址" 被包含进 LLDP 信息。

3.3.6 端口镜像

1、单端口镜像配置

将端口 1 镜像到端口 2 的配置如图 3.60 所示。

端口镜像配置

端口镜像到

镜像端口配置

端口	模式
*	<>
1	使能
2	不使能
3	不使能

图 3.60 单端口镜像配置

2、多端口镜像配置

将端口 1、2、3 镜像到端口 4 的配置如图 3.61 所示。

端口镜像配置

端口镜像到

镜像端口配置

端口	模式
*	<>
1	使能
2	使能
3	使能
4	不使能
5	不使能

图 3.61 多端口镜像配置

3.3.7 VLANs 配置

VLAN（Virtual LAN）中文叫做虚拟局域网，它的作用就是将物理上互连的网络在逻辑上划分为多个互不相干的网络，这些网络之间是无法通讯的，就好像互相之间没有连接一样，因此广播也就隔离开了。

为了理解 VLAN 内报文的转发，就必须要知道交换机对于不同 VLAN 报文

的 tag/untag 的处理原则。首先，需要明确一点就是，在交换机的内部，为了快速高效的处理，报文都是带 tag 转发的。

下面从报文入和报文出两个方向来介绍。

报文入方向：

在入方向上，交换机的根本任务就是决定该报文是否允许进入该端口，根据入报文的 tag/untag 的属性以及端口属性，细分为如下情况：

1) 报文为 untag：允许报文进入该端口，并打上 PVID 的 VLAN tag,与端口属性无关；

2) 报文为 tag：在这种情况下，需要交换机来判断是否允许该报文进入端口；

➤ Unaware 端口： PVID 和报文中 tag 标明的 VLAN 一致，接收并处理报文；否则丢弃。

➤ C-port (Vlan aware) 端口：如果端口允许 tag 中标明的 VLAN 通过，则接收并处理报文；否则丢弃。

报文出方向：

在出方向上，交换机已经完成对报文的转发，其根本任务就是在转发出端口时，是否携带 tag 转发出去，根据出端口属性，细分为如下情况：

1) Unaware 端口：将标签剥掉，不带 tag 转发；

2) C-port (Vlan aware) 端口：报文所在 VLAN 和 PVID 相同，则报文不带 tag；否则带 tag；

1、VLAN Access 成员配置

VLAN Access 成员配置如图 3.62 所示，交换机默认配置的 VLAN ID 为 1，并且所有端口均在 VLAN 1 中。

VLAN成员配置

起始VLAN: ,每页显示: 个条目.

删除	VLAN ID	VLAN名称	端口成员																										
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>																										

图 3.62 VLAN 成员配置

2、VLAN Trunk 成员配置

Vlan Trunk 是为了级联等功能需要在一个端口下面支持添加多个 VLAN ID，配置的过程为，仍然在 VLANs 配置页面中，点击<添加新 VLAN>，在端口 1、2 上新加 VLAN 2，在端口 3、4 上新加 VLAN 3 如图 3.63 所示。

VLAN成员配置

起始VLAN: 1, 每页显示: 20 个条目.

删除	VLAN ID	VLAN名称	端口成员																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>																									
<input type="checkbox"/>	2		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

图 3.63 添加 VLAN 成员

3、VLAN 端口配置

VLAN 端口配置如图 3.64 所示。

以太网类型自定义为 S-ports 0x

VLAN端口配置

端口	端口状态	Ingress过滤	帧类型	端口VLAN		Tx Tag
				模式	ID	
*	<>	<input type="checkbox"/>	<>	<>	1	<>
1	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
2	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid

图 3.64 VLAN 端口配置

以太网类型自定义为 S-ports

本字段指定自定义 S-ports 中使用的以太网类型。在需要用到公网 VLAN 时才需要配置此项。

端口类型

端口可以是以下几种类型：Unaware，Customer port(C-port)，Service port(S-port)，Custom Service port(S-custom-port)。默认为 C-port，即识别 VLAN tag，可以根据需要设置成 Unaware 模式，S-port 和 S-custom-port 只有在公网 VLAN 才会用到。

Ingress 过滤

除非需要对交换机进行 debug 调试，否则不需要启用 ingress filtering 功能。

帧类型

如果配置成 Tagged 只接收含 vlan tag 标签的报文，否则丢弃；如果配置成 Untagged 只接受不含 vlan tag 的报文；默认配置为 ALL，所有报文都接收。

端口 VLAN 模式

配置端口 VLAN 模式。允许的数值：None 或 Specific。本参数影响 VLAN ingress 和 egress 的处理过程。

PVID mode 为 specific 时，表示可手动指定该值，范围为 1~4095。

端口 VLAN ID

配置端口的 VLAN 标识号。允许值：1 到 4095。默认值是：1。

Tx Tag

Untag_pvid - 所有 VLAN，除了被配置的 PVID，都会被 Tag。Tag_all - 所有的 VLAN 都会被 Tag。Untag_all - 所有的 VLAN 都不会被 Tag。

3.3.8 Private VLANs 配置

私有 (Private) VLAN 是一种能够为同一 VLAN 内不同端口之间提供隔离，每个 private VLAN 能包含多个私有端口，在同一个 private VLAN 里的端口可以相互通信，在不同 private VLAN 里的端口不能相互通信。

在同一 private VLAN 里的端口还可以采用端口隔离，互相隔离的端口不能通信，没有隔离的端口可以和在同一 private VLAN 里的隔离端口进行通信。

通过 VLAN，private VLAN，以及端口隔离，可以实现 3 级隔离。

1、Private VLAN 成员配置

默认所有端口都在 private VLAN 1 里，将端口 1、2、3、4 加入 private VLAN 2，如图 3.65 所示，端口 1、2、3、4 相互可以通信，但不能与其他端口通信。

私有VLAN成员配置

		端口成员																										
删除	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
<input type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

图 3.65 private Vlan 成员配置

2、端口隔离配置

默认所有端口都没有隔离，将端口 2、3、4 隔离，如图 3.66 所示。端口 2、3、4 都在 private VLAN 2 里，由于进行了隔离，所以端口 2、3、4 相互间不能通信；端口 2、3、4 与端口 1 可以相互通信。

端口隔离配置

端口成员																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																					

图 3.66 端口隔离配置

3.3.9 MAC 地址表

在每个以太网帧的帧头，都包含有一个目的 MAC 地址和一个源 MAC 地址，它的作用是标志帧的源节点和目的节点的物理地址。一个 MAC 地址有 48bit（6 个字节），从应用上可以分为单播地址、组播地址、广播地址：

(1) 单播地址：第 1 字节的最低位为 0，比如 0000-0EF3-0038，一般用于标志唯一的设备；

(2) 组播地址：第 1 字节的最低位为 1，比如 0100-5E00-0001，一般用于标志同属一组的多个设备；

(3) 广播地址：所有 48bit 全为 1，即 FFFF-FFFF-FFFF，它用于标志同一网段中的所有设备。

二层交换机通过解析和学习以太网帧的源 MAC 来维护 MAC 地址与端口的对应关系（保存 MAC 与端口对应关系的表称为 MAC 表），通过其目的 MAC 来查找 MAC 表决定向哪个端口转发，基本流程如下：

(1) 二层交换机收到以太网帧，将其源 MAC 与接收端口的对应关系写入 MAC 表，作为以后的二层转发依据。如果 MAC 表中已有相同表项，那么就刷新该表项的老化时间。MAC 表表项采取一定的老化更新机制，老化时间内未得到刷新的表项将被删除掉；

(2) 据以太网帧的目的 MAC 去查找 MAC 表，如果没有找到匹配表项，那么向所有端口转发（接收端口除外）；如果目的 MAC 是广播地址，那么向所

有端口转发（接收端口除外）；如果能够找到匹配表项，则向表项所示的对应端口转发，但是如果表项所示端口与收到以太网帧的端口相同，则丢弃该帧。

从上述流程可以看出，二层交换通过维护 MAC 表以及根据目的 MAC 查表转发，有效的利用了网络带宽，改善了网络性能。

MAC 地址表配置如图 3.67 所示。添加新静态条目时，GRP ID 和 APP ID 不必理会，保持默认值 0 即可，用户只要输入 VLAN ID、MAC 地址和勾选端口成员。

MAC地址表配置

老化配置

自动老化失效	<input type="checkbox"/>
老化时间	300 秒

MAC地址表学习

	端口成员																										
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
自动	<input type="checkbox"/>																										
失效	<input type="checkbox"/>																										
安全	<input type="checkbox"/>																										

静态MAC地址表配置

删除	GRP ID	APP ID	VLAN ID	MAC地址	端口成员																										
删除	0	0	1	01-00-00-00-00-01	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
<input type="checkbox"/>					<input type="checkbox"/>																										

添加新静态条目

保存 撤销

图 3.67 MAC 地址表配置

➤老化配置

自动老化失效：选择该box，表示禁用交换机老化功能。

老化时间：时间范围为10~1000000s。

➤MAC地址学习

自动：开启交换机端口的自动学习MAC 功能

失效：禁用自动学习MAC 地址功能

安全：只有在同一VLAN，且报文源MAC 地址出现在静态MAC 表内的，交换机可接收该报文，其它报文一律丢弃

➤静态MAC地址表配置

添加静态MAC 地址条目，手动添加最多支持64 条记录。

3.3.10 Qos 配置

QoS 旨在针对各种应用的不同需求，为其提供不同的服务质量。例如提供专用带宽减少报文丢失率、降低报文传送时延及时延抖动等。为实现上述目的，QoS 提供了下述功能：

➤ 报文分类

为不同类别/服务的报文进行归类，并后续提供标记以及进入相应权限队列。

➤ 队列管理和调度

用以满足不同应用要求下的不同数据报文服务质量。

➤ 流量策略和流量整形

整形是指创建一个具有带宽限值的流量，超过配置速率的流量被缓存并在以后发送，由此可以有效的防止远程链路缓冲队列移出的问题。

策略类似于整形，区别在于超过匹配速率的流量不会被缓存（通常被丢弃）。

➤ 风暴抑制

1、绝对优先级设置

1) 设置入端口的 QoS 类型

在 Qos 配置->Port Classification 里设置端口的 Qos 类型，默认所有端口的 QoS 类型全为 0，设置 1、2、3、4 号端口的 QoS 类型分别为 1、3、5、7，如图 3.68 所示。

QoS Ingress端口分类

端口	QoS类型	DP级别	PCP	DEI	Tag类型	基于DSCP
*	<>	<>	<>	<>		<input type="checkbox"/>
1	1	0	0	0	不使能	<input type="checkbox"/>
2	3	0	0	0	不使能	<input type="checkbox"/>
3	5	0	0	0	不使能	<input type="checkbox"/>
4	7	0	0	0	不使能	<input type="checkbox"/>
5	0	0	0	0	不使能	<input type="checkbox"/>

图 3.68 QoS 类型设置

2) 设置出端口的优先级权重

进入 Qos 配置->Port Scheduler 页面，如图 3.69 所示，默认所有端口调度模式为绝对优先级。

QoS出端口调度

端口	模式	权重					
		Q0	Q1	Q2	Q3	Q4	Q5
1	绝对优先级	-	-	-	-	-	-
2	绝对优先级	-	-	-	-	-	-
3	绝对优先级	-	-	-	-	-	-
4	绝对优先级	-	-	-	-	-	-
5	绝对优先级	-	-	-	-	-	-
6	绝对优先级	-	-	-	-	-	-

图 3.69 QoS 出端口调度

点击要配置的出端口，在这里点击 5 进入端口 5 的配置页面，如图 3.70 所示。

QoS出端口调度和塑造 Port 5

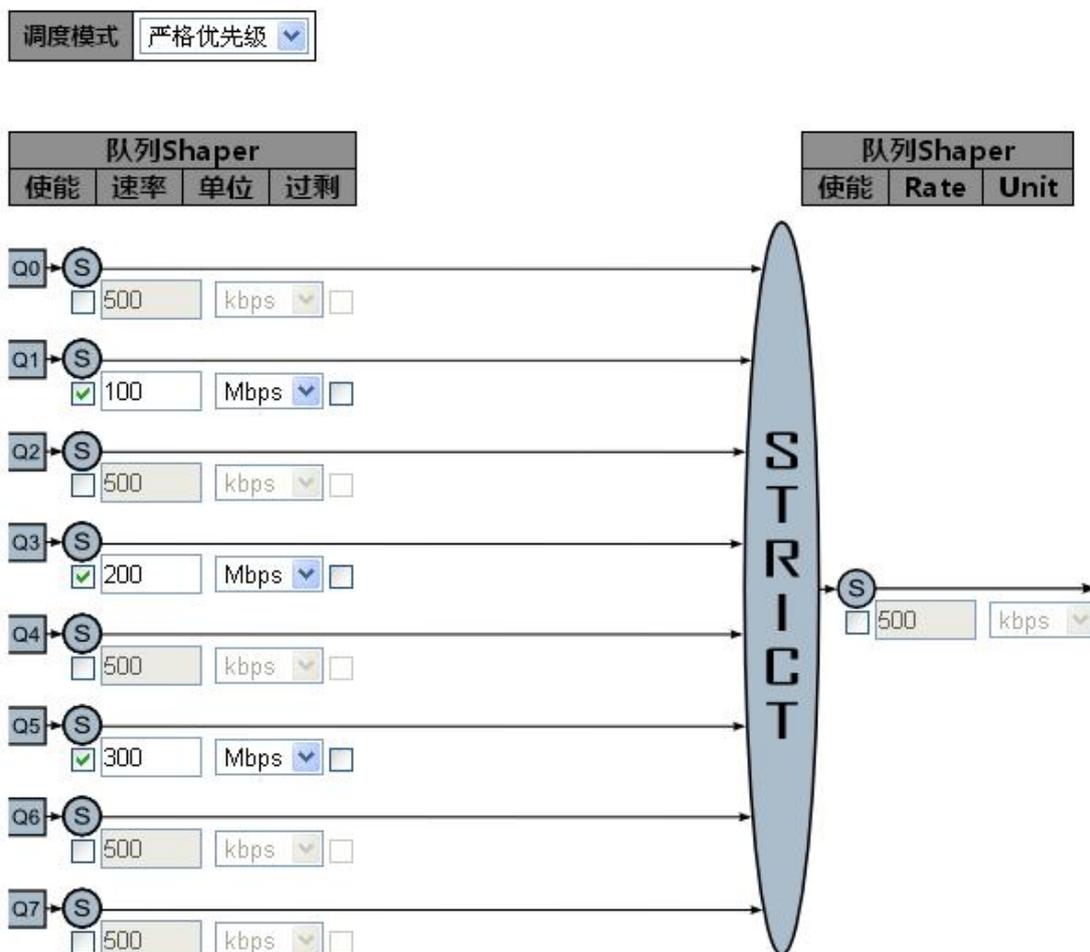


图 3.70 QoS 出端口调度配置

默认 Q1、Q3、Q5 的出口速率为 100、200、300Mbps，Q7 的出口速率为端口的最大速率，在流量超过端口速率时，Q7 的数据流会全部通过，Q1、Q3、Q5 的数据流会按照设定的流量通过，可以通过设置 Q1、Q3、Q5 的速率来调整 Q1、Q3、Q5 的数据流通过量。

2、相对优先级设置

入端口的设置见绝对优先级设置，进入 QoS 配置->Port Scheduler 页面，如图 79 所示，默认所有端口调度模式为绝对优先级。点击要配置的出端口，在这里点击 5 进入端口 5 的配置页面，如图 3.70 所示。选择调度模式为相对优先级，如图 3.71 所示。

QoS出端口调度和塑造 Port 5

调度模式

队列Shaper				队列调度		队列Shaper		
使能	速率	单位	过剩	权重	百分比	使能	Rate	Unit
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	7	7%			
<input type="checkbox"/>	100	Mbps	<input type="checkbox"/>	7	7%			
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	15	14%			
<input type="checkbox"/>	200	Mbps	<input type="checkbox"/>	15	14%			
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>	28	29%			
<input type="checkbox"/>	300	Mbps	<input type="checkbox"/>	28	29%			
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>					
<input checked="" type="checkbox"/>	500	Mbps	<input type="checkbox"/>			<input type="checkbox"/>	500	kbps

保存 撤销 取消

图 3.71 相对优先级 QoS 出端口调度配置

默认 Q1、Q3、Q5 的权重为 7%、15%、28%，Q7 的速率为 500Mbps，可以通过设置 Q1、Q3、Q5 的权重和 Q7 的速率来调整不同优先级是数据流通过率。

3、Port Policing 设置

Policer 在端口的入队列之前，用于限制接收帧的带宽。使能之后将会限制端口接收帧的速率，如图 3.72 所示。

QoS Ingress端口监控器

端口	使能	速率	单位	流控制
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

图 3.72 port policing 设置

速率

控制这个监控 的速率。默认是 500。当 速率单位 是"kbps" 或 "fps", 这个数值被限制在 100-1000000。当速率单位是 "Mbps" 或 "kfps", 这个值被限制在 1-3300。

单位

控制监控速率测量的单位，有 kbps, Mbps, fps 或 kfps。默认值是 kbps。

流控制

如果流控使能，端口处于流控模式，则 **pause** 数据帧被发送，来代替丢弃的数据帧。

4、Storm Control 设置

在以太网中，所有的报文可分为三类，广播（broadcast）、组播（Multicast）、单播（Unicast）。

➤ 广播报文

目的 mac 地址为 ff.ff.ff.ff.ff.ff，这类报文的大量出现，必然会导致网络主机受到严重影响，甚至是网络瘫痪，所以必须加以限制。

➤ 组播报文

目的 mac 地址范围 01:00:5E:00:00:00 ~ 01:00:5E:7F:FF:FF，这种报文相对比较少，但也会扩散到多个端口，因此也要加以控制。

➤ 单播报文

网络中绝大部分数据都是单播数据。单播风暴抑制并不等于禁止单播报文的转发。依据交换机转发报文原理，如果某个单播报文在交换机的 MAC 地址表中找不到对应的表项，那么交换机就会将该报文进行广播扩散。

因此所谓的单播抑制，就是指在地址表中找不到对应条目的单播数据帧。

3.3.11 风暴抑制配置

风暴抑制配置页面如图 3.73 所示，可以根据配置需要针对不同的帧类型进行风暴抑制。



图 3.73 风暴控制

3.3.12 IGMP Snooping 配置

IGMP Snooping 运行在数据链路层，是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。

在二层(Layer2)设备下，组播帧是作为广播转发的，这样容易造成组播流风暴，浪费网络带宽。网络上典型的组播帧是视频流，在某个 VLAN 中，如果有用户注册了某组视频流，那么该 VLAN 中的所有成员都能收到这个视频流，无论他们是否想要。

IGMP Snooping 的作用便是解决这个问题的，它能使视频流只朝注册用户所在的端口转发，从而不会影响到其它的用户。

当二层以太网交换机收到主机和路由器之间传递的 IGMP 报文时，IGMP Snooping 分析 IGMP 报文所带的信息。当监听到主机发出的 IGMP 主机报告报文时，交换机就将该主机加入到相应的组播表中；当监听到主机发出的 IGMP

离开报文时，交换机就将删除与该主机对应的组播表项。通过不断地监听 IGMP 报文，为主机及其对应端口与相应的组播组地址建立映射关系，交换机就可以在二层建立和维护 mac 组播地址表。之后，交换机就可以根据 mac 组播地址表转发从路由器下发的组播报文。

没有运行 IGMP Snooping 时，组播报文将在二层广播，运行 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者，未知组播数据仍然会在二层广播。

1、基本配置

在设备配置 -> 功能配置 -> IGMP Snooping -> 基本配置页面中使能 Snooping，配置路由端口，如图 3.74 所示。

IGMP Snooping配置

全局设置	
Snooping使能	<input checked="" type="checkbox"/>
未注册IPMCv4泛洪使能	<input checked="" type="checkbox"/>
IGMP SSM范围	232.0.0.0 / 8
离开代理使能	<input type="checkbox"/>
代理使能	<input type="checkbox"/>

端口相关的配置

端口	路由端口	快速离开	节流
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▾
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	无限制 ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	无限制 ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	无限制 ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	无限制 ▾
5	<input type="checkbox"/>	<input type="checkbox"/>	无限制 ▾

图 3.74 IGMP Snooping 基本配置

未注册IPMCv4泛洪使能

使能未注册的 IPMCv4 数据流洪泛。只有在 IGMP Snooping 使能时，洪泛的控制才有效，当 IGMP Snooping 关闭，不管这个设置，未注册的 IPMCv4 数据流洪泛一直有效。

IGMP SSM范围

SSM (源指定组播) 范围，允许 SSM 可识别的主机和路由，为地址范围内的组，运行 SSM 服务模型。

离开代理使能

使能 IGMP 离开代理。这个性能可以用于避免转发不必要的离开信息，到路由那边。

代理使能

使能 IGMP 代理。这个性能可以用于避免转发不必要的加入和离开信息，到路由那边。

路由端口

指定哪一个端口作为路由端口。一个路由端口，是一个以太网交换机端口，它可以引导转向，三层组播设备或 IGMP 查询器。如果一个汇聚成员端口被选择作为一个路由端口，整个汇聚将会作为一个路由端口。

快速离开

端口快速离开，当端口收到 leave group 报文时立即断开组播流量，而不必进行 group-specify query 查询，以及一系列的超时。Fast-leave 程序给交换网络中的主机保证最佳的带宽管理。即使同时有多个组播组在应用。

节流

使能，限制一个交换机端口上的组播组的个数。

2、VLAN 配置

进入设备配置->功能配置->IGMP Snooping->VLAN 配置页面中，如图 3.75 所示。

IGMP Snooping VLAN配置

起始VLAN: ,每页显示: 个条目.

删除	VLAN ID	Snooping使能	IGMP查询器	兼容	RV	QI (秒)	QRI (0.1秒)	LLQI (0.1秒)	URI (秒)
----	---------	------------	---------	----	----	--------	------------	-------------	---------

图 3.75 IGMP VLAN 配置

点击<添加新 IGMP VLAN>按钮，添加 VLAN 1，并使能 Snooping 功能，如图 3.76 所示。

IGMP Snooping VLAN配置

起始VLAN: ,每页显示: 个条目.

删除	VLAN ID	Snooping使能	IGMP查询器	兼容	RV	QI (秒)	QRI (0.1秒)	LLQI (0.1秒)	URI (秒)
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	IGMP-Auto	2	125	100	10	1

图 3.76 添加新 IGMP VLAN

3、端口组过滤配置

如需配置组播过滤功能，在设备配置->功能配置->IGMP Snooping->端口组过滤页面中配置，如图 3.77 所示。

IGMP Snooping 端口组过滤配置



图 3.77 端口组过滤配置

点击<添加新过滤组>，在端口 1 上添加过滤组 224.2.2.1，如图 3.78 所示。

IGMP Snooping 端口组过滤配置

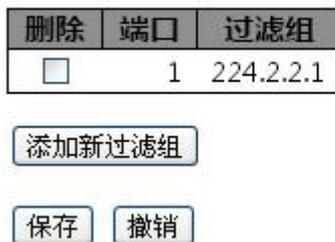


图 3.78 添加过滤组

3.3.13 GMRP 配置

GMRP : GARP Multicast Registration Protocol, GARP 提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息(如 VLAN、组播地址等)。GARP 本身不作为一个实体存在于设备中，遵循 GARP 协议的应用实体称为 GARP 应用，GMRP 就是 GARP 应用的一种。当 GARP 应用实体存在于设备的某个端口上时，该端口对应于一个 GARP 应用实体。

GMRP 帧结构

GMRP(GARP Multicast Registration Protocol)帧结构:

01-80-C2	源地	长度	LLC 头	Protocol	Message	...	Message	End	FCS
-00-00-20	址		42-42-03	ID 00-01	1		N	Mark	

GMRP Address: 01-80-C2-00-00-20 (IEEE 802.1D)。

源地址：产生 GMRP 数据帧的设备的单播地址。

长度：46~1500。

LLC 头：所有 GARP 应用都是用源地址和目的地址为 0X42 的 LLC 服务接入点，控制字段为 03 表示无连接服务。

GMRP 配置如图 3.79 所示，全局使能之后必须先保存配置，然后再使能端口。

GMRP配置

全局使能

 全局使能

端口使能配置

端口	使能	Hold定时器(毫秒)	Join定时器(毫秒)	Leave定时器(毫秒)	LeaveAll定时器(毫秒)
1	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="1200000"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="1200000"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="1200000"/>
4	<input type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="1200000"/>
5	<input type="checkbox"/>	<input type="text" value="100"/>	<input type="text" value="200"/>	<input type="text" value="600"/>	<input type="text" value="1200000"/>

图 3.79 GMRP 配置

使能

开启逻辑端口的 GMRP 功能(注:打开全局使能才有效).

Hold定时器(毫秒)

设置 Hold 定时器的时间,单位为毫秒.可设置范围为:大于 0, 小于或等于 100 毫秒。

Join定时器(毫秒)

设置 Join 定时器的时间,单位为毫秒.可设置范围为:大于或等于两倍的 Hold 定时器时间, 小于等于 200 毫秒。

Leave定时器(毫秒)

设置 Leave 定时器的时间,单位为毫秒.可设置范围为:大于或等于三倍的 Join 定时器时间,小于等于 600 毫秒。

LeaveAll定时器(毫秒)

设置 LeaveAll 定时器的时间,单位为毫秒.可设置范围为:大于或等于 10000 毫秒,小于或等于 3600000 毫秒。

3.3.14 MEP 配置

通过 WEB 管理页面中设备配置->功能配置->MEP 配置页面，点击增加新 MEP 按键，添加新的 MEP，如图 3.80 所示（在端口 1 上新加 VLAN 为 3001 的 MEP 1）。MEP 的详细配置见《交换机 ERPS 环网配置》。

维护实体终点

删除	实例	域名	模式	流向	停留端口	级别	流实例	Tagged VID	This MAC	告警
<input type="checkbox"/>	1	Port	Mep	Ingress	1	0	1	3001	00-00-00-03-00-02	●

图 3.80 MEP 配置

3.3.15 ERPS 配置

通过 WEB 管理页面，设备配置->功能配置->ERPS 配置可以进入 ERPS 管理页面，然后通过添加新保护组 按键添加新的 ERPS 实例，如图 3.81 所示。ERPS 的详细配置见《交换机 ERPS 环网配置》。

以太网环保护倒换

删除	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	环类型	互连节点	虚拟通道	主环ID	告警
<input type="checkbox"/>	1	1	2	1	2	1	2	Major	No	No	1	●

图 3.81 ERPS 配置

3.3.16 IEC61850 配置

通过 WEB 管理页面，设备配置->功能配置->IEC61850 配置可以进入 IEC61850 管理页面，如图 3.82 所示。主要的功能是使能或者关闭 IEC61850 服务和日志文件记录。修改后，IEC61850 服务的使能和关闭需重启交换机才能生效。而日志文件记录的使能和关闭则立即生效。

IEC61850

IEC61850服务(需重启)	使能 ▼
日志功能	使能 ▼
系统日志名称	systemlog.log
告警日志名称	alarmlog.log

图 3.82 IEC61850 配置

4 设备状态

4.1 系统基本信息

4.1.1 自检信息

1. 台账信息

进入设备状态->系统基本信息->台账信息，可以查看系统信息，如图 4.1 所示。

台账信息

装置型号	iES-S2026-Z-E24G2
装置描述	Switch
生产厂商	IESLAB
设备识别代码	IESLAB
端口数量	26
硬件版本	V3.00
固件版本	V2.80E
IP地址	192.168.2.254
MAC地址	00:0E:EA:22:F6:63
管理VLAN	1
出厂时间	2018-01-01 12:00:00
投运时间	2018-01-01 12:00:00
软件版本	V1.00
软件版本校验码	132B434E
软件生成时间	2019-02-27 16:52:22
CID模型版本	V1.00
CID模型校验码	3A6A892A
ICD模型版本	V1.00
ICD模型校验码	DD3E6D60

图 4.1 系统台账信息

2. 通信状态

进入设备状态->功能信息->端口信息-> 端口状态页面，可以查看交换机的端口状态，如图 4.2 所示。

端口状态概述



图 4.2 端口通信状态

3. 自检告警

进入设备状态-->系统基本信息->自检信息-->自检告警，查看自检告警状态
如图 4.3、图 4.4 所示。

自检告警

系统告警

类型	状态
装置告警	
电源1失电告警	
电源2失电告警	
装置配置变更告警	

端口告警

端口	异常中断	MAC变更	流量越限
1			
2			
3			

图 4.3 系统告警状态

端口告警

端口	异常中断	MAC变更	流量越限
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

图 4.4 端口告警状态

4.设备资源

进入设备状态->系统基本信息->CPU 负载页面，可以实时查看 CPU 的使用状态，如图 4.5 所示。



图 4.5 CPU 负载

5. 内部环境

进入设备状态->系统基本信息->自检信息->内部环境页面信息如图 4.6 所示。在设备配置->系统配置->告警配置中进行设置预告警的阈值，根据实际采集值判断是否触发告警。

内部环境

参数	值	单位	预警	告警
CPU温度	70	°C	●	●
主板温度	52	°C	●	●
CPU负载	20	%	●	●
工作电压	11.9	V	●	●

图 4.6 内部环境状态

6. 对时状态

进入设备状态->系统基本信息->自检信息->对时状态，页面信息如图 4.7

对时状态

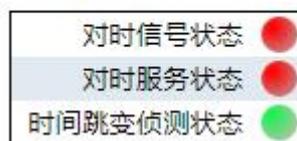


图 4.7 对时状态

4.1.2 端口流量总览

进入设备状态->系统基本信息->端口流量总览，可以查看交换机的端口数据包统计状态，如图 4.8 所示。

端口统计数据概述 自动更新 更新 清除

端口	数据包数		字节数		错误数		Drops		Filtered
	已接收	已发送	已接收	已发送	已接收	已发送	已接收	已发送	已接收
1	0	0	0	0	0	0	0	0	0
2	0	1525	0	97600	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	110894	15903	22361132	1597367	0	0	0	0	82570
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0

图 4.8 端口数据统计状态

4.1.3 端口详细统计

进入设备状态->系统基本信息->端口详细统计，可以查看端口数据包详细统计状态，如图 4.9 所示

详细端口统计 Port 1

Port 1 ▼ 自动更新 更新 清除

接收总数		发送总数	
Rx数据包数	0	Tx包数	0
Rx字节数	0	Tx字节数	0
Rx单播数	0	Tx单播数	0
Rx多播数	0	Tx多播数	0
Rx广播数	0	Tx广播数	0
Rx终止数	0	Tx终止数	0
接收字节统计		发送字节统计	
Rx 64字节数	0	Tx 64字节数	0
Rx 65-127字节数	0	Tx 65-127字节数	0
Rx 128-255字节数	0	Tx 128-255字节数	0
Rx 256-511字节数	0	Tx 256-511字节数	0
Rx 512-1023字节数	0	Tx 512-1023字节数	0
Rx 1024-1526字节数	0	Tx 1024-1526字节数	0
Rx 1527-字节数	0	Tx 1527-字节数	0
接受队列统计		传输队列统计	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
接收错误统计		发送错误统计	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

图 4.9 详细端口统计

4.1.4 SFP 光口状态

进入设备状态-->系统基本信息-->SFP 光口状态查看光口状态（由于未连接所以无数据），如图 4.10 所示。

SFP光口状态

端口	模块温度(C)	模块电压(V)	发送光强(mW)	接收光强(mW)
25	34.0	3.3	0.0	0.0

图 4.10 光口状态

4.1.5 日志信息

进入设备状态-->日志信息-->系统日志页面，如图 4.11、图 4.22 所示，通过日志级别的下拉菜单中根据日志级别筛选日志。

系统日志

自动刷新 刷新 |<< << >> >>|

日志级别 ALL

起始ID: 1, 每页显示: 20 个条目.

保存

ID	日志级别	时间	IED Name	设备型号	内容描述
1	NOTICE	2018-08-14 09:24:54	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
2	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
3	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
4	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
5	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
6	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
7	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
8	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
9	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
10	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
11	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
12	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
13	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
14	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
15	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
16	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
17	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
18	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
19	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)
20	NOTICE	2018-08-14 09:26:11	Switch	iES-S2026-Z-E24G2	port config (admin 192.168.1.87 HTTP)

图 4.11 系统日志

告警日志

自动刷新 刷新 |<< << >> >>|

日志级别 ALL

起始ID: 1, 每页显示: 20 个条目.

保存

ID	日志级别	时间	IED Name	设备型号	内容描述
1	ERROR	2019-02-12 13:52:01	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
2	NOTICE	2019-02-12 13:52:11	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit
3	WARNING	2019-02-12 13:52:11	Switch	iES-S2026-Z-E24G2	CPU temperature >= warning limit(50 C)
4	ERROR	2019-02-12 13:52:21	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
5	NOTICE	2019-02-12 13:52:26	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit
6	WARNING	2019-02-12 13:52:26	Switch	iES-S2026-Z-E24G2	CPU temperature >= warning limit(50 C)
7	ERROR	2019-02-12 13:52:31	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
8	NOTICE	2019-02-12 13:52:41	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit
9	WARNING	2019-02-12 13:52:41	Switch	iES-S2026-Z-E24G2	CPU temperature >= warning limit(50 C)
10	ERROR	2019-02-12 13:52:46	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
11	NOTICE	2019-02-12 13:52:56	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit
12	WARNING	2019-02-12 13:52:56	Switch	iES-S2026-Z-E24G2	CPU temperature >= warning limit(50 C)
13	ERROR	2019-02-12 13:53:01	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
14	NOTICE	2019-02-12 13:53:11	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit
15	WARNING	2019-02-12 13:53:11	Switch	iES-S2026-Z-E24G2	CPU temperature >= warning limit(50 C)
16	ERROR	2019-02-12 13:53:16	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
17	NOTICE	2019-02-12 13:53:31	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit
18	WARNING	2019-02-12 13:53:31	Switch	iES-S2026-Z-E24G2	CPU temperature >= warning limit(50 C)
19	ERROR	2019-02-12 13:53:36	Switch	iES-S2026-Z-E24G2	CPU temperature >= alarm limit(60 C)
20	NOTICE	2019-02-12 13:54:01	Switch	iES-S2026-Z-E24G2	CPU temperature < alarm limit

图 4.12 告警日志

日志级别分为以下几个等级

All: 表示全部的日志, 包括 NOTICE、WARNING、ERROR

NOTICE: 通告级别的、日志

WARNING: 次要级别的日志。

ERROR: 重要级别的日志

起始 ID: 设置 ID 后然后点击刷新, 则第一条则是设置的 ID。

每页显示: 设置每一页所显示日志的条数, 设置条数后点击刷新即可。

保存按钮: 保存日志到文件并下载。

自动刷新: 自动刷新勾选后是每 3 秒进行一次刷新。

刷新按钮: 也是指手动刷新。

|<< 表示首页、<< 表示上一页、>> 下一页、>>| 表示尾页。

4.2 安全信息

4.2.1 RMON 信息

1、RMON 统计

进入设备状态->安全信息->RMON->RMON 统计页面, 可以实时查看 RMON 统计信息, 如图 4.13 所示。

RMON统计状态综述 自动更新

起始控制索引: , 每页显示: 个条目.

ID	数据源 (ifindex)	Drop	八位字节数	包数	广播数	多播数	CRC 错误	过小尺寸	过大尺寸	Frag.	Jabb.	Coll.	64 字节	65 - 127	128 - 255	256 - 511	512 - 1023	1024 - 1588
无条目可显示																		

图 4.13 RMON 统计信息

2、RMON 历史

进入设备状态->安全信息->RMON->RMON 历史页面, 可以实时查看 RMON 历史信息, 如图 4.14 所示。

RMON历史综述 自动更新

起始控制索引: , 样本索引: , 每页显示: 个条目.

历史指数	样本指数	样品开始	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
无条目可显示														

图 4.14 RMON 历史信息

3、RMON 告警

进入设备状态->安全信息->RMON->RMON 告警页面, 可以实时查看

RMON 告警信息，如图 4.15 所示。

RMON告警综述

起始控制索引: , 每页显示: 个条目.

ID	间隔	变量	样本类型	值	启动告警	上升阈值	上升指数	下降阈值	下降指数
无可显示的条目!									

图 4.15 RMON 告警信息

4、RMON 事件

进入设备状态->安全信息->RMON->RMON 事件页面，可以实时查看 RMON 事件信息，如图 4.16 所示。

RMON事件简介

起始控制索引: , 样本索引: , 每页显示: 个条目.

事件指数	Log指数	Log时间	Log描述
无条目可显示			

图 4.16 RMON 事件信息

4.2.2 端口 MAC 数目限制

1、基本信息

进入设备状态->安全信息->端口 MAC 数目限制->基本信息页面，可以查看端口 MAC 数目限制的状态，如图 4.17 所示。

交换机端口安全状态

用户模块说明

用户模块名称	缩写词
Limit Control	L
802.1X	8
DHCP Snooping	D

端口状态

端口	用户	状态	MAC总数	
			当前MAC数	MAC限制数
1	---	不使能	-	-
2	---	不使能	-	-
3	---	不使能	-	-

图 4.17 交换机端口 MAC 数目限制状态

2、端口信息

进入设备状态->安全信息->端口 MAC 数目限制->端口信息页面，可以查看端口的 MAC 数目表，如图 4.18 所示。

安全端口状态 Port 1

MAC地址	VLAN ID	状态	加入时间	Age/Hold
无MAC地址可显示！				

图 4.18 端口 MAC 数目限制表

4.2.3 VLAN MAC 数目限制

1、VLAN MAC 信息

进入设备状态->安全信息->VLAN MAC 数目限制->VLAN MAC 信息页面，可以查看 VLAN MAC 数目限制的状态，如图 4.19 所示。

VLAN安全状态 Vlan 1 输入你要显示的VLAN: 自动更新 更新

端口	MAC地址	VLAN ID	状态	加入时间	Age/Hold
没有MAC地址附加					

图 4.19 VLAN 安全状态

2、总体信息

进入设备状态->安全信息->VLAN MAC 数目限制->总体信息页面，可以查看 VLAN 下的 MAC 数目表，如图 4.20 所示。

Vlan交换机安全状态

Vlan状态

Vlan	状态	MAC总数	
		当前MAC数	限制MAC数
没有附加的Vlan			

图 4.20 VLAN MAC 数目限制表

4.2.4 NAS

1、基本信息

进入设备状态->安全信息->NAS->基本信息页面，可以查看端口网络访问配置状态，如图 4.21 所示。

交换机网络访问服务器状态

端口	管理员状态	端口状态	上一个源	上一个ID	QoS类别	端口VLAN ID
1	强制授权	全局禁用				
2	强制授权	全局禁用				
3	强制授权	全局禁用				
4	强制授权	全局禁用				
5	强制授权	全局禁用				
6	强制授权	全局禁用				
7	强制授权	全局禁用				
8	强制授权	全局禁用				
9	强制授权	全局禁用				
10	强制授权	全局禁用				
11	强制授权	全局禁用				
12	强制授权	全局禁用				
13	强制授权	全局禁用				
14	强制授权	全局禁用				
15	强制授权	全局禁用				
16	强制授权	全局禁用				
17	强制授权	全局禁用				
18	强制授权	全局禁用				

图 4.21 交换机端口网络访问配置状态

2、端口信息

进入设备状态->安全信息->NAS->端口信息页面，可以查看端口的网络访问器计数，如图 4.22 所示。

网络访问服务器计数 Port 1

端口状态

管理员状态	强制授权
端口状态	全局禁用

图 4.22 端口网络访问状态

4.2.5 ACL 信息

进入设备状态->安全信息->ACL 信息页面，可以查看交换机的 ACL 状态，如图 4.23 所示。

ACL状态

用户	Ingress端口	帧类型	动作	速率限制	端口重定向	镜像	CPU	CPU Once	计数器	冲突
MEP	1	EType- 0x8902	拒绝	不使能	Disabled	不使能	否	是	0	否
MEP	1	EType- 0x8902	拒绝	不使能	Disabled	不使能	是	否	0	否
IP Management	All	ARP	允许	不使能	Disabled	不使能	是	否	1932	否
IP Management	All	IPv4/UDP 68 DHCP Server	允许	不使能	Disabled	不使能	是	否	0	否

图 4.23 ACL 状态

4.2.6 IP 源地址防护信息

进入设备状态->安全信息->IP 源保护页面, 可以查看交换机的 IP 源监视表, 如图 4.24 所示。

动态IP源监视表

起始端口: , 起始VLAN: , 起始IP地址: 每页显示: 个条目。

端口	VLAN ID	IP地址	MAC地址
无可显示的条目!			

图 4.24 IP 源监视表

4.2.7 ARP 信息

进入设备状态->安全信息->ARP 检测页面, 可以查看交换机的 ARP 检测表, 如图 4.25 所示。

动态ARP检测表

起始端口: , 起始VLAN: , 起始MAC: , 起始IP地址: , 每页显示: 个实例。

端口	VLAN ID	MAC地址	IP地址
无可显示的实例			

图 4.25 ARP 检测表

4.2.8 AAA

1、Radius 概述

进入设备状态->安全信息->AAA-> Radius 概述页面, 可以查看 Radius 服务器的状态, 如图 4.26 所示。

认证服务器状态概述

#	IP地址	状态
1	0.0.0.0:1812	不使能
2	0.0.0.0:1812	不使能
3	0.0.0.0:1812	不使能
4	0.0.0.0:1812	不使能
5	0.0.0.0:1812	不使能

RADIUS计费服务器状态概述

#	IP地址	状态
1	0.0.0.0:1813	不使能
2	0.0.0.0:1813	不使能
3	0.0.0.0:1813	不使能
4	0.0.0.0:1813	不使能
5	0.0.0.0:1813	不使能

图 4.26 Radius 状态

2、Radius 详细信息

进入设备状态->安全信息->AAA-> Radius 详细信息页面，可以查看 Radius 详细信息，如图 4.27 所示。

验证统计,服务器: #1

接收数据包		发送数据包	
接受访问数	0	访问请求数	0
拒绝访问数	0	访问重传数	0
访问挑战数	0	挂起请求数	0
畸形接入响应数	0	发送超时数	0
错误身份认证数	0		
未知类型数	0		
丢弃报文数	0		
其他信息			
IP地址		0.0.0.0:1812	
状态		不使能	
往返时间		0 ms	

RADIUS计费统计, 服务器: #1

接收数据包		发送数据包	
响应数	0	请求数	0
畸形响应数	0	丢弃数	0

图 4.27 Radius 详细信息

4.3 功能信息

4.3.1 LACP 信息

1、系统状态

进入设备状态->功能信息->LACP->系统状态页面，可以查看 LACP 的系统状态，如图 4.28 所示。

LACP系统状态

Aggr ID	伙伴系统ID	伙伴键值	伙伴优先级	上一次改变	本地端口
无端口使能或无存在的伙伴					

图 4.28 LACP 系统状态

2、端口状态

进入设备状态->功能信息->LACP->端口状态页面，可以查看 LACP 的端口状态，如图 4.29 所示。

LACP状态

端口	LACP	键值	Aggr ID	伙伴系统ID	伙伴端口	伙伴优先级
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-

图 4.29 LACP 端口状态

3、端口统计

进入设备状态->功能信息->端口信息-> 端口统计页面，可以查看 LACP 端口数据统计状态，如图 4.30 所示。

LACP统计

端口	LACP接收	LACP发送	丢弃	
			未知	非法
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0

图 4.30 LACP 端口统计

4.3.2 STP**1、桥状态**

进入设备状态->功能信息->STP->桥状态页面，可以查看 STP 桥的状态，如图 4.31 所示。

STP桥

桥ID	根树			拓扑标记	拓扑上次改变
	ID	端口	消耗		
32768.00-00-00-03-00-01	32768.00-00-00-03-00-01	-	0	Steady	0d 00:43:23

图 4.31 STP 桥状态

2、端口状态

进入设备状态->功能信息->STP->端口状态页面，可以查看 STP 的端口状

态，如图 4.32 所示。

STP端口状态

端口	CIST角色	CIST状态	工作时间
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	DesignatedPort	Forwarding	0d 01:18:47
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-

图 4.32 STP 端口状态

3、端口统计

进入设备状态->功能信息->STP->端口统计页面，可以查看 STP 端口数据统计状态，如图 4.33 所示。

生成树协议(STP)统计

端口	发送			接收			丢弃	
	RSTP 快速生成树协议	STP 生成树协议	TCN 拓扑改变通知	RSTP 快速生成树协议	STP 生成树协议	TCN 拓扑改变通知	未知	非法
3	2436	0	0	0	0	0	0	0
20	5455	0	0	0	0	0	0	0

图 4.33 STP 端口统计

4.3.3 LLDP 信息

进入设备状态->功能信息->LLDP 信息页面，可以查看 LLDP 邻居信息，如图 4.34 所示。

LLDP邻居信息

本地端口	底盘ID	远程端口ID	系统名称	端口描述	系统性能	管理地址
Port 3	00-01-C1-FF-FF-FF	10		Port #10	Bridge(+)	192.168.1.2 (IPv4)

图 4.34 LLDP 邻居信息

4.3.4 VLANs

1、VLAN 成员状态

进入设备状态->功能信息->VLANs->VLAN 成员状态页面，可以查看 VLAN 成员的状态，如图 4.35 所示。

VLAN成员的状态 Combined users

起始VLAN : , 每页显示 : 个条目.

VLAN ID	端口成员																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	<input checked="" type="checkbox"/>																									
3001	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

图 4.35 VLAN 成员状态

2、VLAN 端口状态

进入设备状态->功能信息->VLANs->VLAN 端口状态页面，可以查看 VLAN 端口的状态，如图 4.36 所示。

VLAN端口状态 Static user

端口	PVID	端口类型	Ingress过滤	帧类型	Tx Tag	UVID	冲突
1	1	C-Port	不使能	All	Untag_this	1	No
2	1	C-Port	不使能	All	Untag_this	1	No
3	1	C-Port	不使能	All	Untag_this	1	No
4	1	C-Port	不使能	All	Untag_this	1	No
5	1	C-Port	不使能	All	Untag_this	1	No
6	1	C-Port	不使能	All	Untag_this	1	No
7	1	C-Port	不使能	All	Untag_this	1	No
8	1	C-Port	不使能	All	Untag_this	1	No

图 4.36 VLAN 端口状态

4.3.5 MAC 地址表

进入设备状态->功能信息->MAC 地址表页面，可以查看交换机的 MAC 地址表信息，如图 4.37 所示。

MAC地址表起始VLAN： ，起始MAC地址： ，每页显示： 个条目。

类型	VLAN	MAC地址	端口成员																											
			CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
静态	1	00-00-00-03-00-01	✓																											
动态	1	00-00-01-00-00-00		✓																										
动态	1	00-01-C1-00-00-09		✓																										
动态	1	00-01-C1-FF-FF-FF		✓																										
动态	1	00-0B-AB-40-43-0C		✓																										
动态	1	00-1D-0F-81-5D-16		✓																										
动态	1	10-78-D2-78-49-BA		✓																										
动态	1	10-78-D2-78-88-51																											✓	
动态	1	20-7C-8F-70-82-C6		✓																										
动态	1	74-DE-2B-E0-DD-7B		✓																										
动态	1	C8-9C-DC-21-45-ED		✓																										
动态	1	F4-CE-46-42-21-BA		✓																										

动态MAC地址总数: 静态MAC地址总数: 总MAC地址数:

图 4.37 MAC 地址表

4.3.6 IGMP Snooping 状态**1、状态**

进入设备状态->功能信息->IGMP Snooping->状态页面，可以查看 IGMP Snooping 的状态，如图 4.38 所示。

IGMP Snooping状态**统计**

VLAN ID	查询器版本	主机版本	查询器状态	查询器发送	查询器接收	V1报告接收	V2报告接收	V3报告接收	V2离开接收
1	v3	v2	ACTIVE	3	0	0	12	7	0

路由端口

端口	状态
1	全部
2	全部
3	-

图 4.38 IGMP Snooping 状态

2、组信息

进入设备状态->功能信息->IGMP Snooping->组信息页面，可以查看 IGMP Snooping 的组信息，如图 4.39 所示。

IGMP Snooping组信息起始VLAN： ，起始组地址： ，每页显示： 个条目。

VLAN ID	组	端口成员																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
1	224.0.1.60			✓																								
1	224.0.1.242			✓																								
1	224.1.10.10			✓																								
1	239.255.255.250			✓																								✓

图 4.39 IGMP Snooping 组信息

3、组信息

进入设备状态->功能信息->IGMP Snooping->IPV4 SFM Information 页面，
可以查看 IGMP SFM 信息，如图 4.40 所示。

IGMP SFM信息起始VLAN： ，组地址： ，每页显示： 个条目。

VLAN ID	组	端口	模式	源地址	类型	硬件过滤/交换机
1	224.0.1.60	3	Exclude	None	拒绝	是
1	224.0.1.242	3	Exclude	None	拒绝	是
1	224.1.10.10	3	Exclude	None	拒绝	是
1	239.255.255.250	3	Exclude	None	拒绝	是
1	239.255.255.250	20	Exclude	None	拒绝	是

图 4.40 IGMP SFM 信息

4.3.7 GMRP

进入设备状态->功能信息->GMRP 页面，可以查看 GMRP MAC 组地址表，
如图 4.41 所示。

GMRP MAC组地址表起始VLAN： ，起始MAC地址： ，每页显示： 个条目。

索引	VLAN	组地址	端口成员																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
无条目可显示																												

图 4.41 GMRP MAC 组地址表

5 设备维护

5.1 重启设备

点击[设备维护]->[重启设备], 进入重启设备页面, 如图 5.1 所示, 点击<是>按钮, 交换机将重启。

重启设备



图 5.1 重启设备

5.2 恢复出厂设置

点击[设备维护]->[恢复出厂设置], 进入恢复出厂设置页面, 如图 5.2 所示, 点击<是>按钮, 交换机将恢复出厂设置。

出厂默认值



图 5.2 恢复出厂设置

5.3 升级软件

点击[设备维护]->[升级软件], 进入软件升级页面, 如图 5.3 所示, 点击<浏览>按钮, 选择文件, 然后点击<上传>按钮, 交换机将进行软件升级。

软件上传



图 5.3 升级软件

5.4 版本切换

点击[设备维护]->[版本切换]，进入软件版本切换页面，如图 5.4 所示，点击<启用备用镜像>按钮，将会切换到备用版本。



图 5.4 软件版本切换

5.5 61850 配置保存

点击[设备维护]->[61850 配置保存]，进入上传 61850 配置文件的页面，如图 5.5 所示。这里的配置文件主要是指 CID 文件。点击<Choose File>按钮，选择文件，然后点击<上传 CID 文件>按钮，交换机将写入 CID 文件。注意新的 CID 文件在下次交换机重启时生效。Startup 文件用于内部维护，用户不必理会。

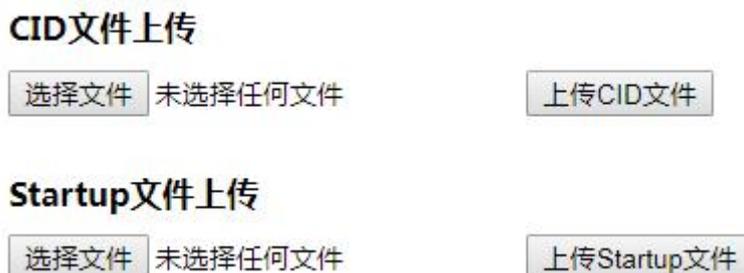


图 5.5 61850 配置保存

5.6 配置保存

点击[设备维护]->[配置保存]，进入保存交换机配置页面，如图 5.5 所示，点

击<保存配置>按钮，将会保存交换机的配置文件。

配置保存

保存配置

图 5.6 配置保存

5.7 配置上传

点击[设备维护]->[配置上传]，进入配置文件上传页面，如图 5.6 所示，点击<选择文件>按钮选择要上传的配置文件，然后点击<上传>即可上传配置文件。

配置上传

选择文件 未选择任何文件

上传

图 5.7 配置上传