



User Manual
用户手册

SW-5010

目 录

第一章 产品介绍	1
1.1 产品概述	1
1.2 性能特征	1
1.3 交换机面板说明.....	2
1.3.1 交换机前面板	2
1.3.2 交换机后面板	3
1.4 环境参数	4
1.5 物品清单	4
第二章 安装、使用方法	5
2.1 安装交换机	5
2.1.1 桌面安装	5
2.1.2 机架式安装.....	5
2.1.3 给交换机上电	6
2.2 连接计算机（NIC）到交换机	6
2.3 连接负载到交换机	7
第三章 登录交换机	8
3.1 连接到交换机	8
3.2 如何登录交换机.....	8
第四章 交换机配置	10
4.1 快速配置	10
4.2 端口管理.....	13
4.2.1 基本设置	13
4.2.2 端口聚合	14
4.2.3 端口镜像	15
4.2.4 端口限速	17
4.2.5 广播风暴	18
4.2.6 端口隔离	19
4.2.7 端口信息	20
4.3 VLAN 管理.....	21
4.3.1 VLAN 设置.....	21
4.3.2 Trunk 口设置.....	22
4.3.3 Hybrid 口设置	23
4.4 故障/安全	25
4.4.1 防攻击.....	25
4.4.1.1 防 DHCP 攻击	25

4.4.1.2 防 DOS 攻击	28
4.4.1.3 IP 源防护	28
4.4.1.4 三元绑定	29
4.4.2 通路检测	31
4.4.2.1 ping 检测	31
4.4.2.2 tracert 检测	32
4.4.2.3 线缆检测	32
4.4.3 ACL 访问控制	33
4.4.4 802.1x	35
4.5 POE 管理	36
4.5.1 POE 管理	36
4.5.1.1 高级管理	36
4.5.1.2 温度配置	37
4.5.2 POE 端口配置	38
4.5.3 POE 延迟	39
4.6 STP	40
4.6.1 MSTP 域	40
4.6.2 STP 桥/端口	41
4.7 DHCP 中继	44
4.7.1 DHCP 中继	44
4.7.2 Option82	45
4.8 DHCP 服务器	46
4.8.1 DHCP 服务器使能	46
4.8.2 DHCP 地址池	47
4.8.3 Option	48
4.8.4 绑定表	49
4.8.5 缺省网关配置	49
4.8.6 DNS 服务器配置	49
4.9 TACACS+	50
4.10 RADIUS	51
4.10.1 RADIUS 配置	51
4.10.2 RADIUS 服务器配置	52
4.11 AAA	52
4.11.1 AAA 使能配置	53
4.11.2 域配置	53
4.11.3 服务器组配置	54
4.11.4 AAA 认证配置	55
4.11.4.1 Login 认证	55
4.11.4.2 Enable 认证	57
4.11.4.3 Dot 1x 认证	58
4.12 QoS 管理	60
4.12.1 队列设置	60
4.12.3 映射队列	61
4.12.3.1 服务类别到队列映射	61

4.12.3.2 差分服务到服务类别映射	62
4.12.3.3 端口到服务类别映射	63
4.13 地址表	64
4.13.1 Mac 添加与删除	65
4.13.2 Mac 学习和老化	66
4.13.3 Mac 地址过滤	67
4.14 Snmp 管理	68
4.14.1 Snmp 配置	68
4.14.1.1 Snmp 配置	68
4.14.1.2 团体	68
4.14.1.3 视图	69
4.14.1.4 组	70
4.14.1.5 用户	71
4.14.1.6 Trap	72
4.14.2 Rmon 配置	73
4.14.2.1 统计组	73
4.14.2.2 历史组	74
4.14.2.3 事件组	75
4.14.2.4 告警组	76
4.15 LACP	77
4.15.1 LACP 设置	77
4.15.2 LACP 显示	78
4.16 系统管理	79
4.16.1 系统设置	79
4.16.1.1 系统设置	79
4.16.1.2 系统重启	81
4.16.1.3 密码修改	82
4.16.1.4 EEE	82
4.16.1.5 SSH 登录	83
4.16.1.6 Telnet 登录	84
4.16.1.7 系统日志	84
4.16.2 系统升级	86
4.16.3 配置管理	87
4.16.3.1 当前配置	87
4.16.3.2 配置备份	89
4.16.3.3 恢复出厂配置	89
4.16.4 配置保存	89
4.16.5 管理员权限	90
4.16.6 一键信息收集	91
附录：产品规格	1

第一章 产品介绍

感谢您购买此款千兆PoE管理型以太网交换机，在安装和使用本产品之前，请仔细阅读本手册，以便正确快速安装及充分使用这款产品。

1.1 产品概述

此款千兆 PoE 管理型以太网交换机产品，提供 8 个 10/100/1000Mbps 自适应 RJ-45 端口及 2 个 1000Mbps SFP 端口；支持所有端口线速转发，可为您提供更大的网络灵活性。支持基于端口的 VLAN ACL，轻松实现网络监控、流量监管、优先级重标记以及数据转发控制；支持传统的 STP/RSTP/MSTP 二层链路保护技术，极大提高链路的容错、冗余备份能力，保证网络的稳定运行；支持基于时间段的 ACL 控制，轻松实现对时间精确控制访问的需求；支持基于端口和基于 MAC 的 802.1x 认证，轻松设定用户访问权限；完善的 QoS 策略以及丰富的 VLAN 功能，易于管理维护，满足中小企业、智能小区、酒店、办公网及园区网的组网及接入要求。

交换机 8 个端口都具有 PoE 供电功能，支持 IEEE802.3at 标准，向下兼容 IEEE802.3af，可作以太网供电设备，能自动检测识别符合标准的受电设备，并通过网线为其供电。

1.2 性能特征

- 符合 IEEE802.3i, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, IEEE802.1q, IEEE802.1p 标准；
- 支持 IEEE802.3af、IEEE802.3at 标准；
- 单个端口功耗最大支持 30W，PoE 总功耗最大可以达到 140W；
- 支持 Web 界面管理；
- 8 个 10/100/1000Mbps 自适应 RJ45 端口，支持自动翻转功能（Auto MDI/MDIX）；
- 2 个 1000Mbps SFP 端口；
- 支持 IEEE802.3x 全双工流控功能和半双工背压流控功能；
- 支持 QoS（服务质量）、端口镜像、链路聚合协议；
- 8K 自动学习和自动老化的 MAC 地址表；
- 简单易懂的 LED 指示端口的链接、数据传输状况；
- 防雷保护，反应迅速，安全可靠；
- 内置电源，精巧结构设计，适于机架及桌面安装使用。

1.3 交换机面板说明

1.3.1 交换机前面板

交换机的前面板由 8 个 10/100/1000Mbps 的 RJ-45 端口, 2 个千兆 SFP 端口, 1 个 Console 口, 1 个复位按钮和一系列 LED 指示灯, 如下图 1 所示。



图1 交换机前面板

10/100/1000Mbps 自适应 RJ-45端口（1~8）：

交换机的 1~8 端口均支持 10/100/1000Mbps 带宽的设备连接。每个端口对应一组 Link/Act 指示灯。

2个 SFP 端口（9S, 10S）：

交换机有 2 个独立的 SFP 口, 支持 1000Mbps 的 SFP 连接。每个端口都对应一个 Link/Act 指示灯。

控制端口（Console）：

用于连接串行一台计算机或终端实行监控和配置交换机。

复位键（Reset）：

保持设备开机并按下按钮约 5 秒钟, 该系统恢复出厂默认设置。

LED 指示灯：

交换机前面板的指示灯用于设备工作状态监视, 指示灯面板, 如下图 2 所示。

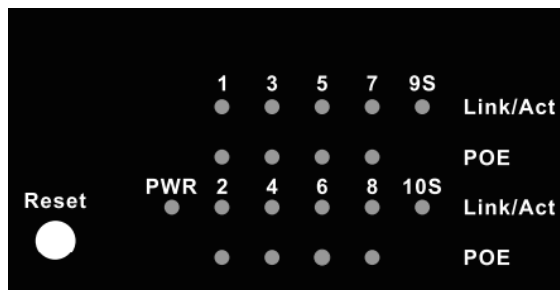


图2 LED 指示灯

下表描述了交换机的每个指示灯的详细指示说明。

LED	颜色	状态	状态描述
电源灯	红色	长亮	通电
		熄灭	断电
Link/Act (1~8)	橙色 (10/100Mbps)	长亮	对应端口已连接
		熄灭	对应端口未连接
	绿色 (1000Mbps)	闪烁	对应端口已连接并收发数据
Link/Act SFP (9S~10S)	绿色	长亮	对应光纤端口已连接
		熄灭	对应光纤端口未连接
		闪烁	对应光纤端口已连接并收发数据
PoE (1~8)	黄色	长亮	对应端口已连接 PD 且 PoE 正常供电
		熄灭	对应端口未连接PD或未提供PoE供电
		闪烁	PoE电源电路短路或电源电流过载

1.3.2 交换机后面板

交换机后面板由交流电源连接器和接地柱组成，如下图3所示：



图3 交换机后面板

交流电源连接器：

即是三芯交流电源插座，支持输入交流电压范围是100~240V AC，50/60Hz。

注：请用户在使用中将电源线三芯插头的安全地与大地连接好。

接地柱：

位于电源接口右侧，请使用导线接地，以防触电。

风扇通风口：

风扇散热口位于交换机后面板的中间位置，用于风扇通风，请勿遮挡。

1.4 环境参数

- 工作温度：0°C~45°C
- 存储温度：-40°C~70°C
- 工作湿度：10%~90% RH 不凝结
- 存储湿度：5%~90% RH 不凝结

1.5 物品清单

打开交换机的包装盒，盒内应包括以下产品和附件：

- 一台 PoE 管理型以太网交换机
- 一根 AC 电源线
- 一套安装组件
- 一本产品用户手册

注：打开产品包装后，若发现以上产品和附件有丢失或损坏，请及时与经销商联系。

第二章 安装、使用方法

2.1 安装交换机

请按照下面的说明进行安装，避免不正确的操作造成设备损坏和安全威胁：

- 把交换机放置在平稳的地方或桌面上以防跌落摔坏；
- 确保交换机连接的输入交流电源满足交换机背面标记的电压范围；
- 为了保持交换机远离电火花，请不要打开交换机的外壳，即使在不通电的情况下；
- 确保有足够的通风空间给交换机散热；
- 确保支撑交换机的台面能足够支撑交换机及其配件的重量。

2.1.1 桌面安装

如果用户没有19-英寸的标准机架，那么可以把交换机安装在平稳桌面上。请将附带的橡胶脚垫安装于交换机底面的四个角上，然后置于桌面指定位置，保留足够的通风空间给交换机散热。

2.1.2 机架式安装

交换机可安装在EIA标准尺寸19-英寸机架中，后者可同其它设备一起置于布线室中。安装交换机，请遵循以下步骤：

- a. 安装时，将安装支架附于交换机的侧面板（一边一个）并用随货提供的螺丝将其固定；



图4 安装支架

- b. 然后，用随设备机架提供的螺丝将交换机安装到机架上。

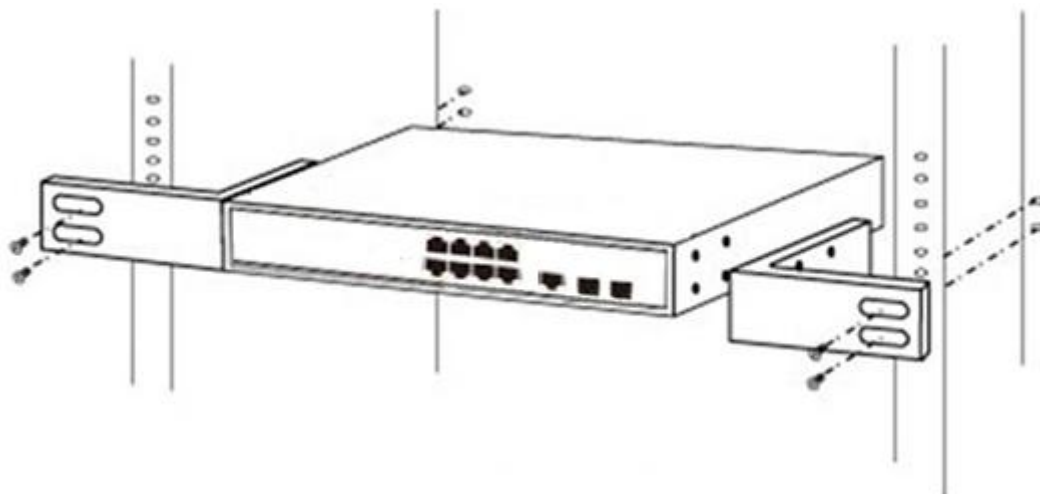


图5 安装到机架

2.1.3 给交换机上电

该交换机是通过交流100~240V 50/60Hz的内部高效电源供电，请按照以下步骤连接：

AC插座：

推荐使用单相三线插座与中性出口或多功能计算机专业的插座。请确认插座接地线完好且能正常工作。

AC电源线连接：

用标配的交流电源线一端插入 AC 电源插座，一端接到交换机后面板的电源接口。检查电源指示灯是否亮，如果电源指示灯亮，表明电源连接成功。

2.2连接计算机（NIC）到交换机

请将网卡插入电脑，安装网卡驱动程序后，请将双绞线的一端连接到您的电脑，另一端将连接到交换机的任意 RJ-45 口上，交换机和电脑连接距离最大支持 100 米。一旦连接成功，设备正常上电，则相对应的交换机端口 Link/Act/Speed 状态指示器灯工作。

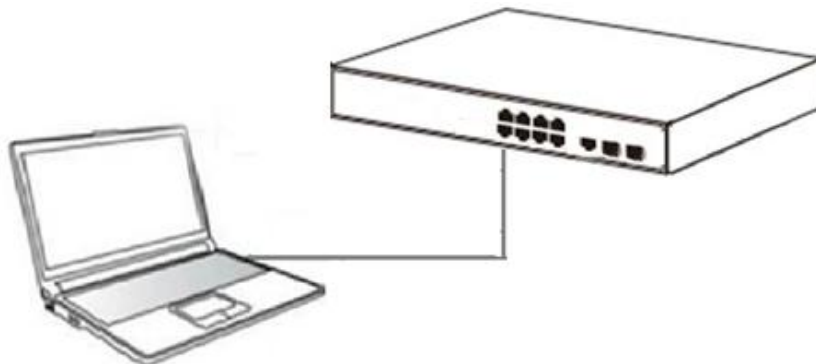


图6 连接 PC 到交换机

2.3 连接负载到交换机

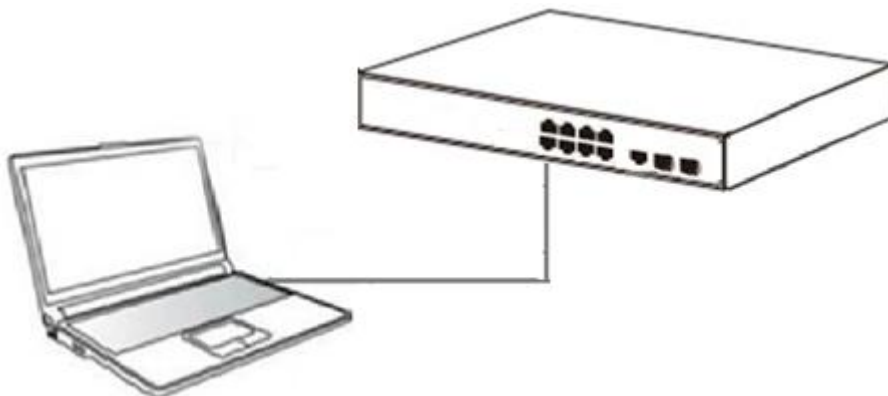
交换机的 1~8 端口都支持 PoE 供电功能，每个端口的最大输出功率是 30W。您仅需把支持 PoE 供电的受电设备（例如网络电话，网络摄像头，无线终端等）通过网线连接到该交换机上，交换机就能给此受电设备提供供电。

第三章 登录交换机

物理安装成功后，您可以使用Web浏览器来配置交换机，监控网络状态和显示统计信息。

3.1 连接到交换机

使用标准的5类或超5类网线（非屏蔽/屏蔽）把交换机和网络设备连接起来，交换机端口会自动适应（MDI / MDI-X、速度、双工）匹配设备进行连接，如下图所示。



一旦连接成功，请参阅LED指示灯规格，相对应的交换机端口Link/Act/Speed状态指示灯工作。

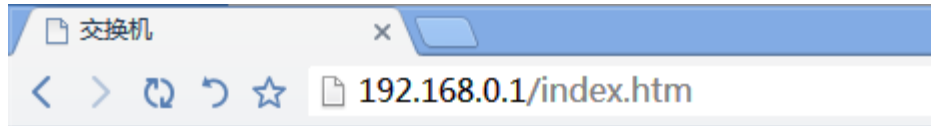
3.2 如何登录交换机

由于交换机提供基于Web的管理登录，您可以手动配置计算机的IP地址，登录到交换机。交换机的默认设置如下所示。

参数	默认值
默认IP地址	192.168.0.1
默认用户名	admin
默认密码	admin

您可以通过以下步骤登录到交换机的配置窗口：

1. 将交换机连接到计算机的网卡接口；
2. 交换机通上电源；
3. 检查计算机的IP地址是否是该网段中：192.168.0.xxx（“xxx”的范围2~254），如192.168.0.100；
4. 打开浏览器，输入<http://192.168.0.1>，然后按“Enter”键。出现交换机登录窗口，如下图所示；



5. 输入用户名和密码，然后点击“登陆”，就可登录到下面的交换机配置窗口。（可在页面右上角点击“切换语言”进行语言切换）。



端口	描述	输入流量(Bps)	输出流量(Bps)	开启状态	连接状态	所属Vlan	Trunk口
Gi 0/1		0.00K	0.00K	开启	未连接	1	否
Gi 0/2		0.00K	0.00K	开启	未连接	1	否
Gi 0/3		460.54K	1.79M	开启	连接	1	否
Gi 0/4		0.00K	0.00K	开启	未连接	1	否
Gi 0/5		0.00K	0.00K	开启	未连接	1	否
Gi 0/6		0.00K	0.00K	开启	未连接	1	否
Gi 0/7		0.00K	0.00K	开启	未连接	1	否
Gi 0/8		0.00K	0.00K	开启	未连接	1	否
Gi 0/9		0.00K	0.00K	开启	未连接	1	否
Gi 0/10		0.00K	0.00K	开启	未连接	1	否

第四章 交换机配置

本章描述了如何使用基于网页的管理接口切换交换机软件配置管理功能。

在网页管理界面，左列显示了配置菜单。上方可以看到交换机系统信息，如内存、软件版本。最中间一行显示交换机的端口现状。绿色方块显示端口已连接设备，而黑色方块显示端口未连接。配置菜单下方，您可以看到一个工具栏，可进行端口信息、流量走势、设备配置、端口统计信息查看。

The screenshot shows the SUNDRAY web management interface. The top navigation bar includes the SUNDRAY logo, the current user 'admin', and options for '退出' (Logout) and '切换语言' (Change Language). The main content area displays system information: '设备型号: SW-5010', '软件版本: D161116', '运行时间: 10 min', '序列号: G1GB0U5007211', and '硬件版本: 1.00'. Below this is a 3D model of the switch with port status indicators (1-8, Console, 9F, 10F). A toolbar below the model includes icons for '100M', '1000M', 'PDR', 'Unconnect', and 'Closed'. The '端口信息' (Port Information) tab is selected, showing a table of port configurations.

↑	描述	输入流量 (Bps)	输出流量 (Bps)	开启状态	连接状态	所属Vlan	trunk口
	Gi 0/1	0.00K	0.00K	开启	未连接	1	否
	Gi 0/2	0.00K	0.00K	开启	未连接	1	否
	Gi 0/3	460.54K	1.79M	开启	连接	1	否
	Gi 0/4	0.00K	0.00K	开启	未连接	1	否
	Gi 0/5	0.00K	0.00K	开启	未连接	1	否
	Gi 0/6	0.00K	0.00K	开启	未连接	1	否
	Gi 0/7	0.00K	0.00K	开启	未连接	1	否
	Gi 0/8	0.00K	0.00K	开启	未连接	1	否
	Gi 0/9	0.00K	0.00K	开启	未连接	1	否
	Gi 0/10	0.00K	0.00K	开启	未连接	1	否

At the bottom of the table, there are navigation links: '首页 上一页 (1) 下一页 尾页 1 / 1 页'.

4.1 快速配置

在导航栏中选择“快速配置”，可在此模块中创建 VLAN、将端口加入 VLAN 中、设置交换机基本信息以及修改登录密码。如下图：



【参数说明】

参数	描述
VLAN ID	VLAN 号, 8GE 默认 VLAN 1
VLAN 名称	VLAN 的标示
VLAN IP 地址	管理此 VLAN 的 ip 地址
设备名称	交换机名称
管理 VLAN	交换机管理使用 VLAN

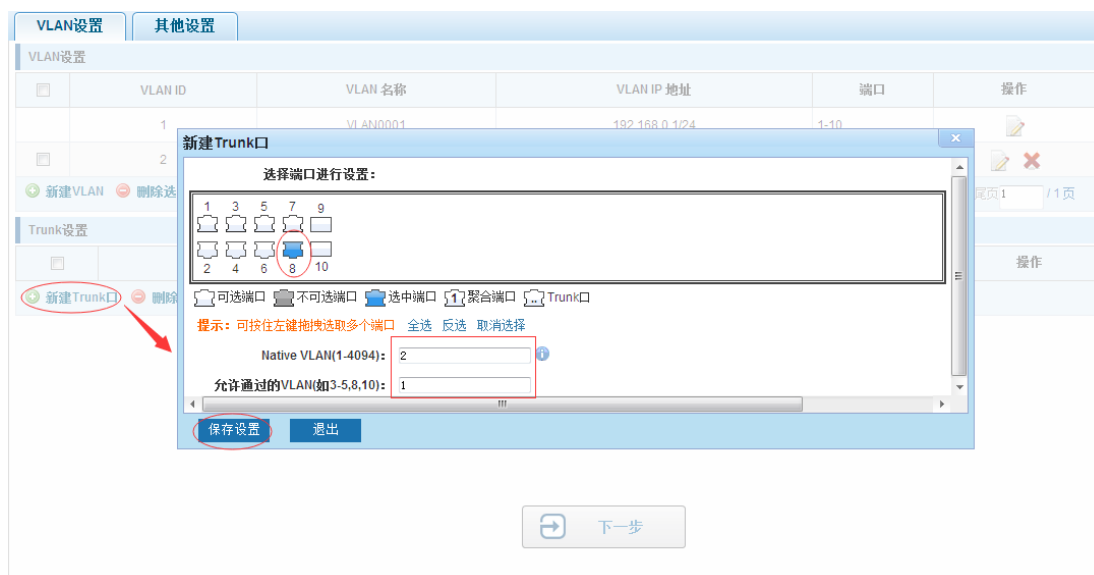
【使用指导】

Native VLAN: 作为 Trunk, 这个口要属于一个 Native VLAN。所谓 Native VLAN, 就是指在这个接口上收发的 UNTAG 报文, 都被认为是属于这个 VLAN 的。显然, 这个接口的缺省 VLAN ID (即 IEEE 802.1Q 中的 PVID) 就是 Native VLAN 的 VLAN ID。同时, 在 Trunk 上发送属于 Native VLAN 的帧, 则必然采用 UNTAG 的方式。

许可 VLAN 列表: 一个 Trunk 口缺省可以传输本设备支持的所有 VLAN (1—4094) 的流量。但是, 也可以通过设置 Trunk 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过这个 Trunk 口。

【配置举例】

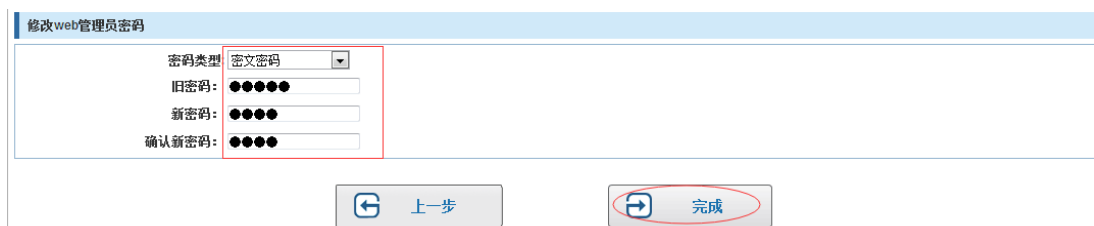
1) VLAN 设置: 如创建 VLAN 2, 将端口 8 设置为 Trunk 口, Native VLAN 为 2。



2) 点击“下一步”按钮，进入其他设置，如：将管理 ip 地址改为 192.168.0.12，设备名称改为 switch-123，默认网关及 dns 服务器设置为 172.16.1.241。

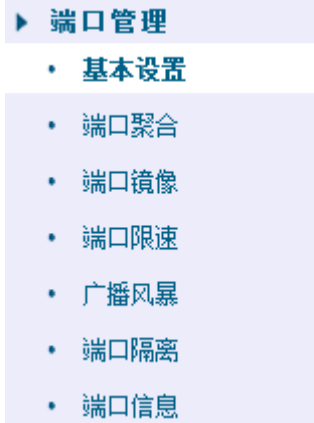


用 192.168.0.12 进行登录，选择密文密码，设置新密码为 1234。



4.2 端口管理

在导航栏选择“端口管理”，您可以进行基本设置、端口聚合、端口镜像、端口限速和端口隔离等设置。



4.2.1 基本设置

在导航栏中选择“端口管理>基本设置”，可对面板上端口进行端口描述、端口速率、端口状态、工作模式、流量控制、交叉线序配置，如下图：

The screenshot shows the '端口基本设置' (Port Basic Settings) page. At the top, there are icons for selecting ports: 1, 3, 5, 7, 9 in the first row and 2, 4, 6, 8, 10 in the second row. Below this are legends for '可选端口' (Selectable), '不可选端口' (Not selectable), '选中端口' (Selected), '聚合端口' (Aggregation), and 'Trunk口' (Trunk). A tip indicates that multiple ports can be selected by holding the left mouse button. Configuration fields include: '端口描述(0-80字符):' (Port description), '端口速率:' (Port rate), '流量控制:' (Flow control), '端口状态:' (Port status), '工作模式:' (Working mode), and '交叉线序:' (Crossover sequence). A '保存设置' (Save settings) button is present.

端口	端口描述	端口状态	端口速率	工作模式	巨型帧	交叉线序	流量控制	操作
Gi0/1		开启	1000M	双工	5000	自协商	关闭	
Gi0/2		开启	100M	双工	5000	自协商	关闭	
Gi0/3		开启	自协商	自协商	5000	自协商	关闭	
Gi0/4		开启	自协商	自协商	5000	自协商	关闭	
Gi0/5		开启	自协商	自协商	5000	自协商	关闭	
Gi0/6		开启	自协商	自协商	5000	自协商	关闭	
Gi0/7		开启	自协商	自协商	5000	自协商	关闭	
Gi0/8		开启	自协商	自协商	5000	自协商	关闭	
Gi0/9		开启	1000M	双工	5000	自协商	关闭	
Gi0/10		开启	1000M	双工	5000	自协商	关闭	

【参数说明】

参数	描述
端口	选择当前配置端口号

端口状态	选择是否关闭链路端口
流量控制	是否开启流控
端口速率	可选以下几种： 自动协商 10 M 100 M 1000 M
工作模式	可选择模式有以下几种： 自动协商 半双工 全双工
端口描述	对端口进行描述
交叉线序	可选择模式有以下几种： 自动协商 MDI MDIX

【使用指导】

开启流量控制需将自协商关闭，自协商关闭就是设置端口速率及工作模式；将端口速率设置超过端口实际速率，端口将掉线。

【配置举例】

如：将端口设置为 10M、半双工、开启流量控制及端口状态、设置交叉线序为自协商。



4.2.2 端口聚合

在导航栏中选择“端口管理>端口聚合”，可将多个物理口绑定到一个逻辑口来扩充端口带宽或实现带宽的冗余备份，如下图：



【参数说明】

参数	描述
聚合端口	8GE 交换机可设置 8 个链路汇聚组，group_1 到 group_8
成员端口	为每个组添加自己的成员端口，且不能和其他组的成员重合

【使用说明】

开启 ARP 检查功能的端口、重要设备 ARP 欺骗的端口、设置 Mac VLAN 功能的端口及端口镜像中的监控端口无法加入聚合！

【配置举例】

如：设置端口 7、8 为聚合端口 1，可让此聚合端口 1 与其他交换机聚合端口 1 相连来搭建交换机链路。



4.2.3 端口镜像

在导航栏选择“端口管理>端口镜像”，可将一个或多个源端口报文复制一份转发到一个目的端口中，如下图：



【参数说明】

参数	描述
源端口	对该端口的出入流量进行监管
目的端口	设置目的端口, 将源端口的流量数据进行复制转发到报文分析器分析报文情况转发给目的端口
镜像组	范围 1-4

【使用说明】

已加入聚合口的端口不能作为目的端口和源端口, 目的端口和源端口不能为同一个。页面上配置后默认是对源端口出入流量进行监管。

【配置举例】

如: 设置一镜像组用于端口 6 监管端口 2、3、4、5 端口出入流量情况。



4.2.4 端口限速

在导航栏选择“端口管理>端口限速”，可对端口输出、输入限速，如下图：

The screenshot displays the 'Port Rate Limiting' configuration interface. On the left is a navigation menu with 'Port Rate Limiting' selected. The main area contains a configuration form with two input fields: 'Input Rate Limit (10x multiplier):' and 'Output Rate Limit (10x multiplier):', both set to '1000'. Below the form is a 'Save Settings' button. A table titled 'Port Rate Limiting List' shows 10 ports, each with an input rate of 1000Mbit/s and an output rate of 1000Mbit/s. The table includes a 'Port' column, 'Input Rate Limit', 'Output Rate Limit', and 'Action' columns. The bottom right corner of the page shows navigation links: 'Home', 'Previous Page', 'Next Page', 'End Page', and '1/1 Page'.

端口	输入限速	输出限速	操作
1	1000Mbit/s	1000Mbit/s	
2	1000Mbit/s	1000Mbit/s	
3	1000Mbit/s	1000Mbit/s	
4	1000Mbit/s	1000Mbit/s	
5	1000Mbit/s	1000Mbit/s	
6	1000Mbit/s	1000Mbit/s	
7	1000Mbit/s	1000Mbit/s	
8	1000Mbit/s	1000Mbit/s	
9	1000Mbit/s	1000Mbit/s	
10	1000Mbit/s	1000Mbit/s	

【参数说明】

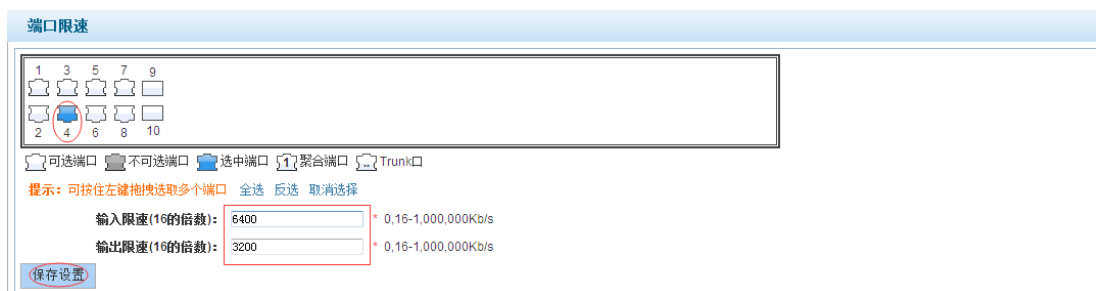
参数	描述
输入限速	设置端口输入的速度
输出限速	设置端口输出的速度

【使用说明】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s 。 即 1M 带宽对应的理论速率是 125KB/s 。

【配置举例】

如：将端口 4 输入速率设置为 6400 kb/s，将输出速率设置为 3200 kb/s。



4.2.5 广播风暴

在导航栏选择“端口管理>广播风暴”，可对端口进行风暴控制，如下图：



【参数说明】

参数	描述
广播抑制值	广播数据包的风暴抑制值
组播抑制值	组播数据包的风暴抑制值
单播抑制值	单播数据包的风暴抑制值
Multicast 类型包	未知名：以组播组中不存在的 ip 为目的地址的流。 知名及不知名：任一组播流。
Unicast 类型包	未知名：设备 MAC 表中没有该单播帧的目的 MAC 条目。 知名及不知名：任一单播流。

【使用说明】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s 。 即 1M 带宽对应的理论速率是 125KB/s 。

【配置举例】

如：需将转发到端口 1-8 的各种包转发速率为 5000 kb/s,组播类型包设置为知名及不知名，单播类型包设置仅未知包。



4.2.6 端口隔离

在导航栏选择“端口管理>端口隔离”，可设置端口相互隔离，如下图：



【参数说明】

参数	描述
源端口	选择一个端口，以配置隔离端口
隔离端口	将被隔离的端口

【使用说明】

开启端口隔离功能,源端口上的所有报文都不会从隔离端口转发,选择的端口之间相互隔离。

已加入聚合口的端口也能作为目的端口和源端口，目的端口和源端口不能为同一个。

【配置举例】

如：将端口 3、4、5、6 相互隔离。

端口隔离

请选择需隔离的端口：

可选端口
 不可选端口
 选中端口
 聚合端口
 Trunk口

提示：可按住左键拖拽选取多个端口 全选 反选 取消选择

[保存编辑](#)

端口隔离列表			
源端口	隔离端口	操作	
3	4 5 6 7 8		✘
4	3 5 6 7 8		✘
5	3 4 6 7 8		✘
6	3 4 5 7 8		✘
7	3 4 5 6 8		✘
8	3 4 5 6 7		✘

首页 上一页 (1) 下一页 尾页: /

配置成功后，端口 3/4/5/6 相互隔离。

4.2.7 端口信息

在导航栏选择“端口管理>端口隔离”，可查询端口信息，如下图：

- 系统首页
- 快速配置
- ▶ 端口管理
 - 基本设置
 - 端口聚合
 - 端口镜像
 - 端口限速
 - 广播风暴
 - 端口隔离
 - **端口信息**
- ▶ VLAN管理
- ▶ 故障/安全
- ▶ PoE管理
- ▶ STP
- ▶ DHCP中继
- ▶ DHCP服务器
- ▶ TACACS+
- ▶ RADIUS
- ▶ AAA
- ▶ QoS管理
- ▶ 地址表
- ▶ Snmp管理
- ▶ LACP
- ▶ 系统管理

端口信息

关键字 实时刷新流量

↑	描述	输入流量(Bps)	输出流量(Bps)	开启状态	连接状态	所属vlan	trunk口
Gi 0/1		4.08M	6.04M	开启	连接	1	否
Gi 0/2		175.99M	65.12M	开启	连接	1	否
Gi 0/3		0.00K	0.00K	开启	未连接	1	否
Gi 0/4		0.00K	0.00K	开启	未连接	1	否
Gi 0/5		0.00K	0.00K	开启	未连接	1	否
Gi 0/6		0.00K	0.00K	开启	未连接	1	否
Gi 0/7		0.00K	0.00K	开启	未连接	1	否
Gi 0/8		0.00K	0.00K	开启	未连接	1	否
Gi 0/9		0.00K	0.00K	开启	未连接	1	否
Gi 0/10		0.00K	0.00K	开启	未连接	1	否

首页 上一页 (1) 下一页 尾页 1 / 1页

【参数说明】

参数	描述
输入流量	统计端口输入流量
输出流量	统计端口输出流量

【使用说明】

显示端口的输入和输出流信息端口的连接状态，所属 VLAN。

【配置举例】

如：输入端口号 1 进行查询。

端口信息							
关键字	<input type="text" value="1"/>	<input type="button" value="查询"/>	<input checked="" type="checkbox"/> 实时刷新流量				
描述	输入流量(Bps)	输出流量(Bps)	开启状态	连接状态	所属vlan	trunk口	
Gi 0/1	4.21M	6.26M	开启	连接	1	否	
Gi 0/10	0.00K	0.00K	开启	未连接	1	否	

首页 上一页 1 下一页 尾页 1 / 1 页

4.3 VLAN管理

在导航栏选择“VLAN 管理”，您可以进行 VLAN 管理、Trunk 口设置和 Hybrid 口设置等设置。

VLAN列表						
VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作		
1	VLAN0001	192.168.0.1/24	1-10			

新建VLAN 删除选择VLAN

首页 上一页 1 下一页 尾页 1 / 1 页

4.3.1 VLAN 设置

在导航栏中选择“VLAN 管理”，可创建 VLAN 并将端口设置到 VLAN 中（端口默认状态为 access 模式），如下图：

VLAN列表						
VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作		
1	VLAN0001	192.168.0.1/24	1-10			

新建VLAN 删除选择VLAN

首页 上一页 1 下一页 尾页 1 / 1 页

【参数说明】

参数	描述
VLAN ID	VLAN 号，8GE 默认 VLAN 1
VLAN 名称	VLAN 的标示
VLAN IP 地址	管理此 VLAN 的 ip 地址

【使用说明】

管理 VLAN、default VLAN 不能被删除。添加端口为 access 口，access 模式下端口只能为一个 VLAN 的成员。

【配置举例】

如：让连接交换机下 pc1、pc2 不能相互访问，及将其中一个 pc 连接端口属于 VLAN 2 中。



操作



可点击页面操作中编辑、删除按钮进行相应操作。

4.3.2 Trunk 口设置

在导航栏中选择“VLAN 管理>Trunk 口设置”，可将端口设置为 Trunk 口



【参数说明】

参数	描述
Native VLAN	只可设置一个
允许通过的 VLAN	可设置多个

【使用指导】

Native VLAN: 作为 Trunk，这个口要属于一个 Native VLAN。所谓 Native VLAN，就是指在这个接口上收发的 UNTAG 报文，都被认为是属于这个 VLAN 的。显然，这个接口的缺省 VLAN ID（即 IEEE 802.1Q 中的 PVID）就是 Native VLAN 的 VLAN ID。同时，在 Trunk 上发送属于 Native VLAN 的帧，则必然采用 UNTAG 的方式。

许可 VLAN 列表: 一个 Trunk 口缺省可以传输本设备支持的所有 VLAN（1—4094）的流量。但是，也可以通过设置 Trunk 口的许可 VLAN 列表来限制某些 VLAN 的流量不能通过

这个 Trunk 口。

【配置举例】

如：PVID=VLAN2

PC1：192.168.0.2，端口 8，access VLAN2。

PC2：192.168.0.3，端口 7，Trunk allowed VLAN 1-2。

PC3：192.168.0.4，端口 6，access VLAN1（默认下端口属于 VLAN1）。

让 PC2 能 PING 通 PC1，不能 PING 通 PC3。



4.3.3 Hybrid 口设置

在导航栏中选择“VLAN 管理>Hybrid 口设置”，可将端口设置为带 tag 和不带 tag 的 Hybrid 口，如下图：



【使用说明】

Hybrid 端口收报文：

收到一个报文,判断是否有 VLAN 信息：如果没有则打上端口的 PVID，并进行交换转发，如果有则判断该 Hybrid 端口是否允许该 VLAN 的数据进入：如果可以则转发，否则丢弃(此时端口上的 untag 配置是不用考虑的， untag 配置只对发送报文时起作用)。

Hybrid 端口发报文：

- 1、判断该 VLAN 在本端口的属性（disp interface 即可看到该端口对哪些 VLAN 是 untag，哪些 VLAN 是 tag）。
- 2、如果是 untag 则剥离 VLAN 信息，再发送，如果是 tag 则直接发送。

【配置举例】

如：创建 VLAN 10、VLAN 20，将端口 1 Native VLAN 设置为 10，去 tag 的 VLAN 为 10、20，将端口 2 Native VLAN 设置为 20，去 tag 的 VLAN 为 10、20

VLAN设置		Trunk口设置		Hybrid口设置	
VLAN列表					
<input type="checkbox"/>	VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作
<input type="checkbox"/>	1	VLAN0001	192.168.0.1/24	1-10	
<input type="checkbox"/>	10	VLAN0010			
<input type="checkbox"/>	20	VLAN0020			
新建VLAN 删除选择VLAN 首页 上一页 [1] 下一页 尾页 1 / 1页					

VLAN设置		Trunk口设置		Hybrid口设置	
Hybrid口列表					
<input type="checkbox"/>	端口				操作
<input type="checkbox"/>					
新建Hybrid口 删除选择 / 1页					

新建Hybrid口

13579

246810

可选端口
 不可选端口
 选中端口
 聚合端口
 Trunk口

提示：可按住左键拖拽选取多个端口 全选 反选 取消选择

Native Vlan(1-4094):

加TAG的VLAN(如3-5,8,10):

去TAG的VLAN(如3-5,8,10):

VLAN设置		Trunk口设置		Hybrid口设置		
Hybrid口列表						
<input type="checkbox"/>	端口	端口描述	本地VLAN	加TAG的VLAN	去TAG的VLAN	操作
<input type="checkbox"/>	7		10	1	10,20	
<input type="checkbox"/>	8		20	1	10,20	
新建Hybrid口 删除选择Hybrid口 首页 上一页 [1] 下一页 尾页 1 / 1页						

此时 inter e0/1 和 inter e0/2 下的所接的 PC 是可以互通的,但互通时数据所走的往返 VLAN 是不同的。

pc1 所发出的数据，由 inter0/1 所在的 pvid VLAN10 封装 VLAN10 的标记后送入交换机，交换机发现 inter e0/2 允许 VLAN 10 的数据通过，于是数据被转发到 inter e0/2 上，由于 inter e0/2 上 VLAN 10 是 untagged 的，于是交换机此时去除数据包上 VLAN10 的标记，以普通包的形式发给 pc2，此时 pc1->pc2 走的是 VLAN10。

再来分析 pc2 给 pc1 回包的过程，pc2 所发出的数据，由 inter0/2 所在的 pvid VLAN20 封

装 VLAN20 的标记后送入交换机，交换机发现 inter e0/1 允许 VLAN 20 的数据通过，于是数据被转发到 inter e0/1 上，由于 inter e0/1 上 VLAN 20 是 untagged 的，于是交换机此时去除数据包上 VLAN20 的标记，以普通包的形式发给 pc1，此时 pc2->pc1 走的是 VLAN20。

4.4 故障/安全

在导航栏选择“故障/安全”，您可以进行防攻击、通路检测、ACL 访问控制和 802.1x 等设置。



4.4.1 防攻击

4.4.1.1 防 DHCP 攻击

在导航栏中选择“故障/安全> 防攻击>防 dhcp 攻击”，开启防 DHCP 攻击功能，拦截仿冒 DHCP 服务器及地址耗竭攻击报文，禁止私设 DHCP 服务器，如下图：



【参数说明】

参数	描述
DHCP 信任端口	信任端口正常转发接收 DHCP 报文，不信任端口将丢弃 DHCP 响应报文
DHCP 抑制端口	拒绝端口下所有 DHCP 请求报文
源 mac 效验	对 DHCP CLIENT 发出的请求报文，检查链路层头部 MAC 地址和 DHCP 报文中的 CLIENT MAC 字段是否相同。源 MAC 地址

	校验失败时，报文将被丢弃。
Option82 使能	将在 DHCP 请求报文中添加 option82 信息，转发给服务器，DHCP 服务器可根据该选项信息进行灵活的地址分配。
客户端 option82 使能	开启使能情况下会保留客户端的 option82 选项，并转发报文，而关闭使能情况下，如果收到客户端发来的带 option82 的 DHCP 报文时，将丢弃该报文。
电路控制	依据 DHCP 报文所走的 vlan 选择使用该 vlan 下所配置的电路 ID 子选项内容，如果没有配置的话，默认使用 circuit id 为 0 类型的，内容为 VLAN ID + interface number，即 DHCP 客户端所在 vlan 和端口。
代理远程	依据 DHCP 报文所走的 VLAN 选择使用该 VLAN 下所配置的远程 ID 子选项内容，如果没有配置的话，默认使用 remote id 为 0 类型的，内容为交换机 mac 地址。
Ip 地址	依据 DHCP 报文所走的 vlan 选择使用该 vlan 下所配置的 IP 子选项内容，如果没有配置的话，不发送该选项。
绑定表	静态绑定某客户端在某个端口和 VLAN 上，所以如果收到该客户端的 DHCP 请求报文来自其它端口或 VLAN 时，将会被丢弃。静态设置时，并没有对应的 IP 信息，这个 IP 信息需要通过动态监听学习获取服务器分配给该 MAC 客户端的 IP 地址。
DHCP snooping vlan	打开指定 VLAN 的 DHCP Snooping 功能
Dhcp Snooping 服务器 IP 地址	当有配置可信任的 DHCP 服务器地址时，在收到 DHCP 服务器发来的响应包时，需要对该服务器地址进行校验是否为配置的可信任服务器地址之一，如果校验失败的话，就会丢弃该包。没有配置任何可信任地址时，就不需要做这种校验。

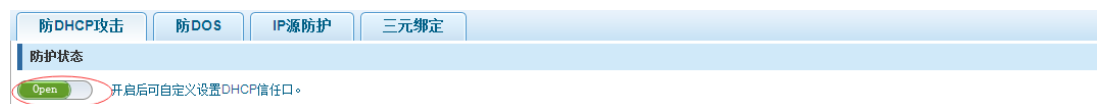
【使用说明】

DHCP 信任端口配置，选择端口作为信任端口。禁止 DHCP 方式申请地址，选择端口后保存，可禁用该端口的此项功能。

开启 DHCP 防攻击功能，需将 DHCP 防护 vlan 同时进行设置，其他功能才生效。

【配置举例】

如：1.将 dhcp snooping 打开。



2.设置 dhcp snooping vlan。



3.设置连接路由器 8 端口为信任，再将 6 端口设置为抑制。

DHCP信任端口设置 | 禁止DHCP申请地址 | 源MAC校验 | OPTION82 | 绑定表 | 其他配置

选择加入DHCP信任端口：

1	3	5	7	9
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

可选端口
 不可选端口
 选中端口
 聚合端口
 Trunk口
 ip源使能开启端口
 提示：可按住左键拖拽选取多个端口

保存配置

DHCP信任端口设置 | 禁止DHCP申请地址 | 源MAC校验 | OPTI

选择禁止DHCP申请地址端口：

1	3	5	7	9
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

可选端口
 不可选端口
 选中端口
 聚合端口
 Trunk口
 ip源

保存配置

4. 效验源 mac F0:DE:F1:12:98:D2，将服务器设置为 192.168.0.1。

DHCP信任端口设置 | 禁止DHCP申请地址 | 源MAC校验 | OPTION82 | 绑定表 | 其他配置

源MAC校验使能：

Mac地址：F0:DE:F1:12:98:D2

校验 不校验

序号	mac地址	状态	操作
1	f0:de:f1:12:98:d2	校验	

Dhcp Snooping 服务器IP地址：192.168.0.1

添加

5. 设置 option82 信息。

DHCP信任端口设置 | 禁止DHCP申请地址 | 源MAC校验 | OPTION82 | 绑定表 | 其他配置

Option82使能：

客户端Option82使能：

电路控制 | 代理远程 | IP地址

电路控制名：123 VLAN ID：1

添加

序号	电路控制名	电路控制ID	VLAN ID	操作
1	123	1	1	

代理远程 | IP地址

远程代理名：wery VLAN ID：1

添加

序号	远程代理名	远程代理ID	VLAN ID	操作
1	wery	1	1	

电路上控制 代理远程 IP地址

IP地址: 192.168.2.30 * VLAN ID: 1 *

添加

序号	IP地址	VLAN ID	操作
----	------	---------	----

6.将端口 7 进行绑定。

DHCP信任端口设置 禁止DHCP申请地址 源MAC校验 OPTION82 绑定表 其他配置

Mac地址: 00:01:15:09:37:35

VLAN ID: 1

端口号: 7

添加

4.4.1.2 防 DOS 攻击

在导航栏中选择“故障/安全> 防攻击>防 DOS 攻击”，开启防 DOS 攻击功能，拦截 Land 攻击报文、非法 TCP 报文，确保设备或服务器主机向合法用户提供正常的服务，如下图：

防DHCP攻击 防DOS IP源防护 三元绑定

DOS攻击防护状态

Closed

【使用说明】

开启防 DOS 攻击功能，拦截 Land 攻击报文、非法 TCP 报文，确保设备或服务器主机向合法用户提供正常的服务。

【配置举例】

如：开启防 DOS 攻击。

防DHCP攻击 防DOS IP源防护 三元绑定

DOS攻击防护状态

Open

4.4.1.3 IP 源防护

在导航栏中选择“故障/安全> 防攻击>IP 源防护”，通过源防护端口使能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用，提高了端口的安全性，如下图：

防DHCP攻击 防DOS IP源防护 三元绑定

IP源防护端口使能配置

请选择IP源防护使能端口:

1	3	5	7	9
2	4	6	8	10

可选端口
 不可选端口
 选中端口
 聚合端口
 Trunk口
 IP源使能开启端口

提示: 可按住左键拖拽选取多个端口

保存

【使用说明】

添加当前正在使用的端口作为 IP 源防护使能端口，端口将无法使用。可以对用户进行基于 IP+MAC+VLAN+Port 的检测，IP Source Guard 无法在 DHCP Snooping 的信任端口上开启。

【配置举例】

如：需先将 ip 源防护使能端口打开，再进行绑定。



4.4.1.4 三元绑定

在导航栏中选择“故障/安全> 防攻击>三元绑定”，自动探测出基于端口的 IP 地址，mac 地址的映射关系，然后实现一键绑定的功能，如下图：



【使用说明】

一键绑定之前一定要将绑定使能开关打开,并且若要访问交换机应绑定与交换机同网段的IP地址。ARP 检测防私有静态 IP 地址时,静态表项 IP+MAC+Port。

【配置举例】

如:需将先绑定使能开启,一键绑定端口 7。

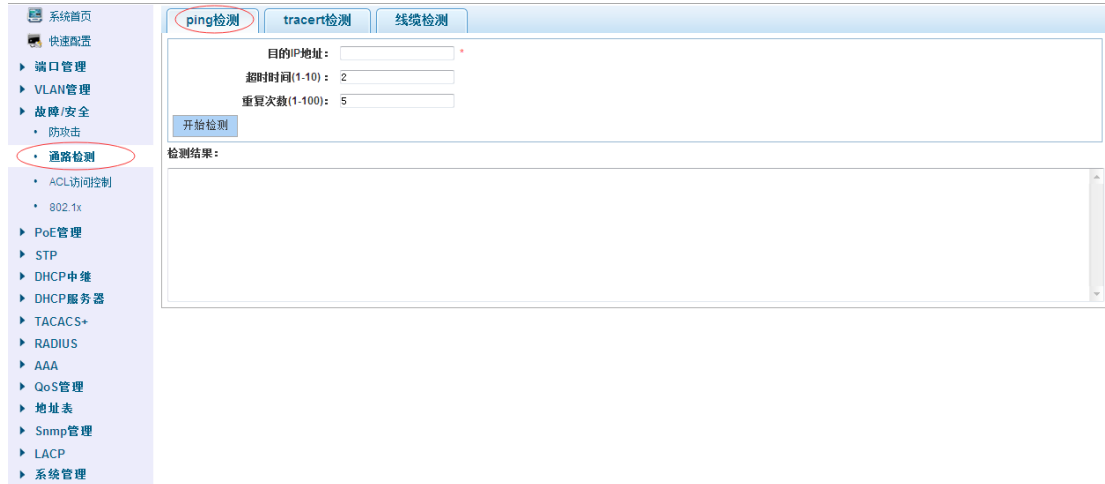


可勾选删除选项。

4.4.2 通路检测

4.4.2.1 ping 检测

在导航栏中选择“故障/安全> 通路检测”，可查看是否可 ping 通此 ip 地址，如下图：



【参数说明】

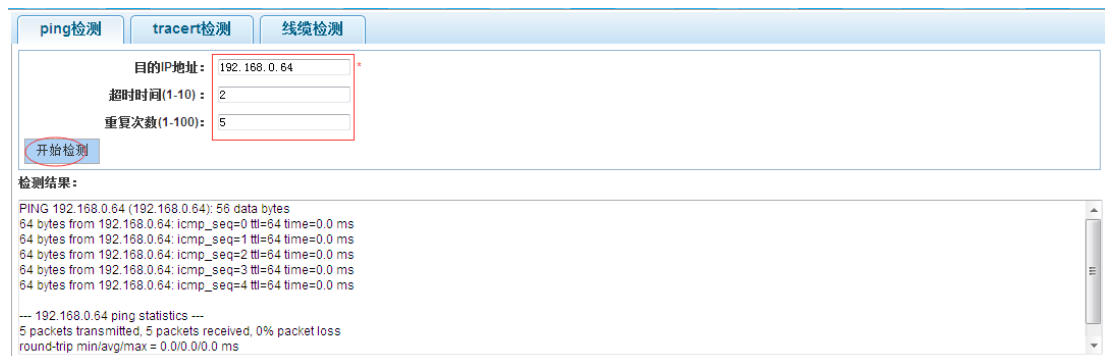
参数	描述
目的 ip 地址	填入需检测的 ip 地址
超时时间	范围 1-10
重复次数	检测次数

【使用说明】

使用 ping 功能检测网络连接及主机是否可达。

【配置举例】

如：PING 连接 pc 的 ip 地址。



4.4.2.2 tracert 检测

在导航栏中选择“故障/安全> 通路检测>tracert”，可以检测到目的地所经过的网关，如下图：

【参数说明】

参数	描述
目的 ip 地址	填入需检测的 ip 地址
超时时间	范围 1-10

【使用说明】

该功能用于检测目的地是否可达及到达目的地的路径，如果目的地不可达，诊断出问题点。

【配置举例】

如：检测目的 ip192.168.0.64。

4.4.2.3 线缆检测

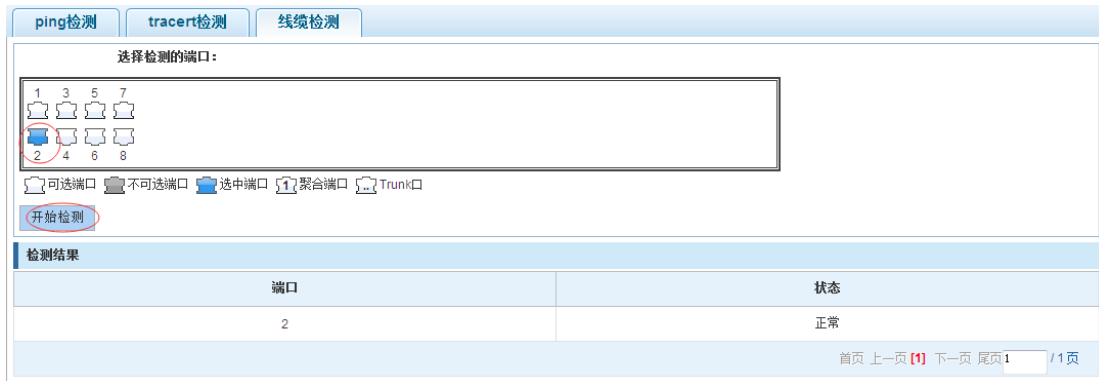
在导航栏中选择“故障/安全> 通路检测>线缆检测”，可以检测连接设备状态，如下图：

【使用说明】

检测结果中程度表示线缆状态非正常时距离故障点的长度（检测结果存在 5 米范围内的偏

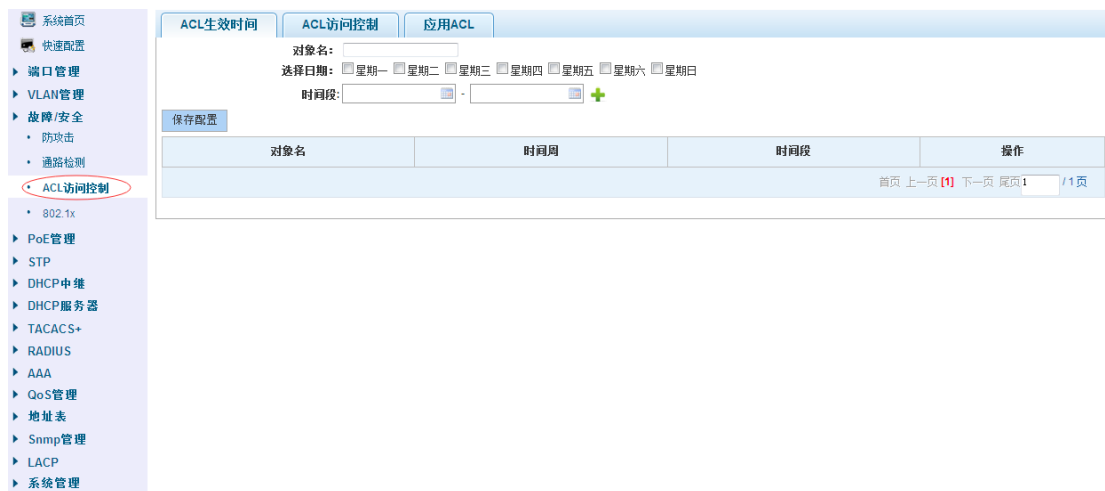
差)。

【配置举例】



4.4.3 ACL 访问控制

在导航栏中选择“故障/安全>ACL 访问控制”，可应用 ACL 规则到端口中并设置生效时间：



【参数说明】

参数	描述
目的 ip 地址	填入需检测的 ip 地址
超时时间	范围 1-10

【使用说明】

ACL 规则是有先后顺序的，排在前面的规则会优先匹配。如果策略条目很多，操作时间会相对变长。

基本原则：

- 1、按顺序执行，只要有一条满足，则不会继续查找。
- 2、隐含拒绝，如果都不匹配，那么一定匹配最后的隐含拒绝条目，思科默认的。
- 3、任何条件下只给用户能满足他们需求的最小权限。
- 4、不要忘记把 ACL 应用到端口上。

【配置举例】

如：测试生效时间为星期一到星期五每天9点到18点，设置端口3不能访问网络。

步骤：建ACL生效时间--建ACL规则--应用到端口。

ACL生效时间 ACL访问控制 应用ACL

对象名: Work

选择日期: 星期一 星期二 星期三 星期四 星期五 星期六 星期日

时间段: 9:00 - 18:00 +

保存配置

对象名	时间周	时间段	操作
Work	<input checked="" type="checkbox"/> 星期一 <input checked="" type="checkbox"/> 星期二 <input checked="" type="checkbox"/> 星期三 <input checked="" type="checkbox"/> 星期四 <input checked="" type="checkbox"/> 星期五	9:00 - 18:00	

首页 上一页 [1] 下一页 尾页 1 / 1页

ACL生效时间 ACL访问控制 应用ACL

创建ACL

新建ACL访问规则

ACL编号: 100 * 匹配的协议: IP

动作: 禁止 生效时间: Work

源IP地址任意: 目的IP地址任意:

保存

规则顺序	ACL规则号	动作	权值	协议	源IP掩码	源端口	目的IP掩码	目的端口	生效时间对象	状态	删除
1	100	deny	10	ip	any/any	any	any/any	any	Work	inactive	✖

首页 尾页 1 / 1页

ACL生效时间 ACL访问控制 应用ACL

创建ACL

规则顺序	ACL规则号	动作	权值	协议	源IP掩码	源端口	目的IP掩码	目的端口	生效时间对象	状态	删除
1	100	deny	10	ip	any/any	any	any/any	any	Work	inactive	✖

首页 上一页 [1] 下一页 尾页 1 / 1页

ACL生效时间 ACL访问控制 应用ACL

1 3 5 7 9
2 4 6 8 10

提示: 可按住左键拖拽选取多个端口 全选 反选 取消选择

ACL列表: 100

过滤方向: 收报文

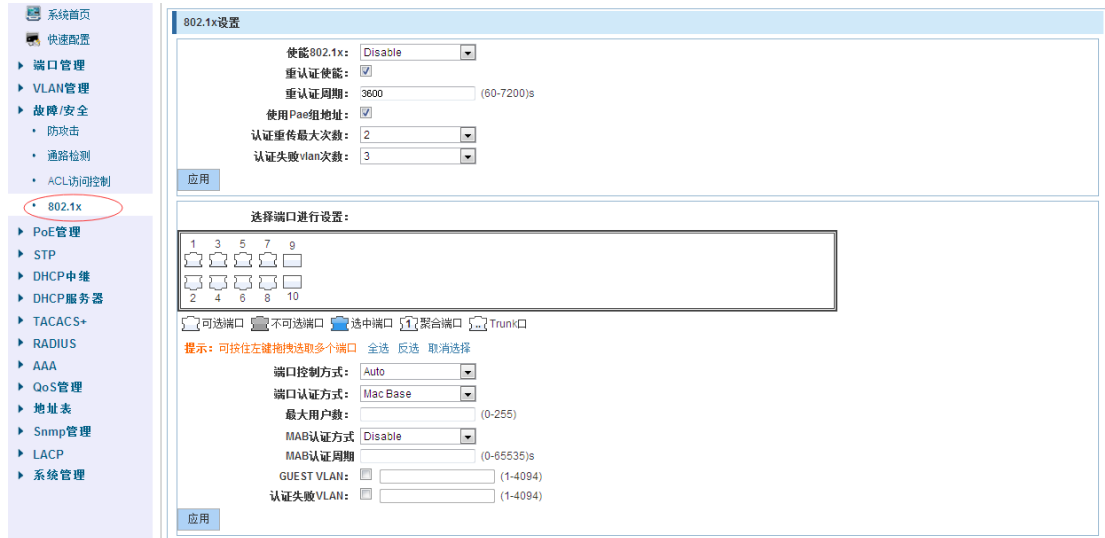
保存设置

ACL	应用于接口	过滤方向	操作
100	3	收报文	✖

首页 上一页 [1] 下一页 尾页 1 / 1页

4.4.4 802.1x

在导航栏中选择“故障/安全>802.1x”，可以在此处配置 802.1x 认证。



【参数说明】

参数	描述
重认证周期	设置重认证周期的时间，取值范围在 60~7200S 之间
认证重传最大次数	选择认证重传最大次数，取值范围在 1~10 之间
认证失败 vlan 次数	选择认证失败 Vlan 次数，取值范围在 1~3 之间

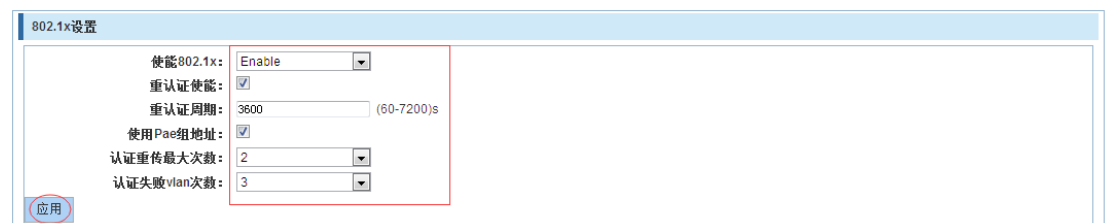
【使用说明】

802.1X 是基于客户机/服务器的访问控制和认证协议。它可以限制未经授权的用户或设备连接到端口访问 LAN / WLAN。

【配置举例】

步骤：开启 802.1x 功能--应用到端口。

如：1. 启用 802.1x 使能，勾选开启重认证使能和 Pae 组地址，设置重认证周期为 3600 秒，认证重传最大次数为 2，认证失败 Vlan 次数为 3。



2. 选配置端口 1，选择端口控制方式为 Auto，端口认证方式为 MAC-Base，最大用户数为 2，MAB 认证方式为 Multi-MAB，MAB 认证周期我 256 秒，guest vlan 为 1，认证失败 Vlan 为 1。

选择端口进行设置：

提示：可按住左键拖拽选取多个端口 全选 反选 取消选择

端口控制方式：Auto

端口认证方式：Mac Base

最大用户数：2 (0-255)

MAB认证方式：Multi-MAB

MAB认证周期：256 (0-65535)s

GUEST VLAN： 1 (1-4094)

认证失败VLAN： 2 (1-4094)

应用

4.5 POE 管理

在导航栏选择“POE 管理”，您可以进行 POE 管理、POE 配置和 POE 延迟等设置。



4.5.1 POE 管理

4.5.1.1 高级管理

在导航栏选择“POE 管理>高级管理”，可查看 POE 状态信息及设置配置。如下图：



【参数说明】

参数	描述
供电模式	选择 PSE 供电的模式
告警功率	配置的告警门限

保留功率	配置保留功率
告警通告	配置告警通告状态，

【使用说明】

实际应用中需要控制系统在功率变化和端口上下电时是否进行发送 trap 通告。
接收 Trap 通告需将 Snmp 开启，并设置 trap 目标主机。

【配置举例】

如：将告警通告设置为 120W，开启告警通告。



4.5.1.2 温度配置

在导航栏选择“POE 管理>高级管理”，可设置 POE 芯片的告警阈值。如下图：

芯片编号	实时温度	告警阈值	操作
1	55°C	100°C	

【参数说明】

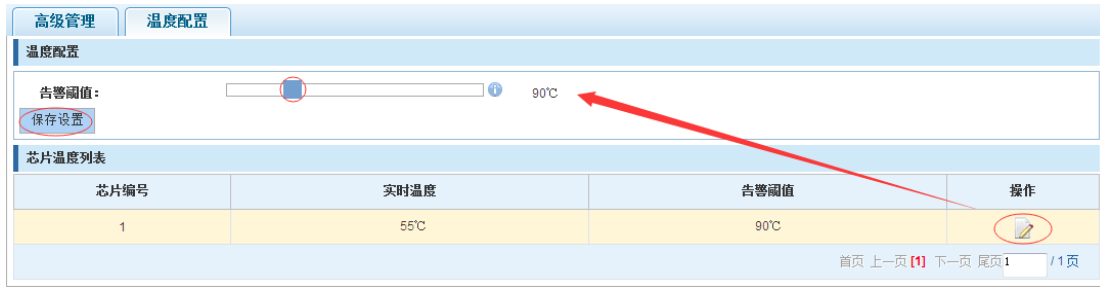
参数	描述
告警阈值	配置温度告警门限,范围 70-149

【使用说明】

接收 Trap 通告需将 Snmp 开启，并设置 trap 目标主机。

【配置举例】

如：将芯片 1 告警阈值设置为 90 度。



4.5.2 POE 端口配置

在导航栏选择“**POE 管理>POE 配置**”，可对端口 POE 进行设置。如下图：



【参数说明】

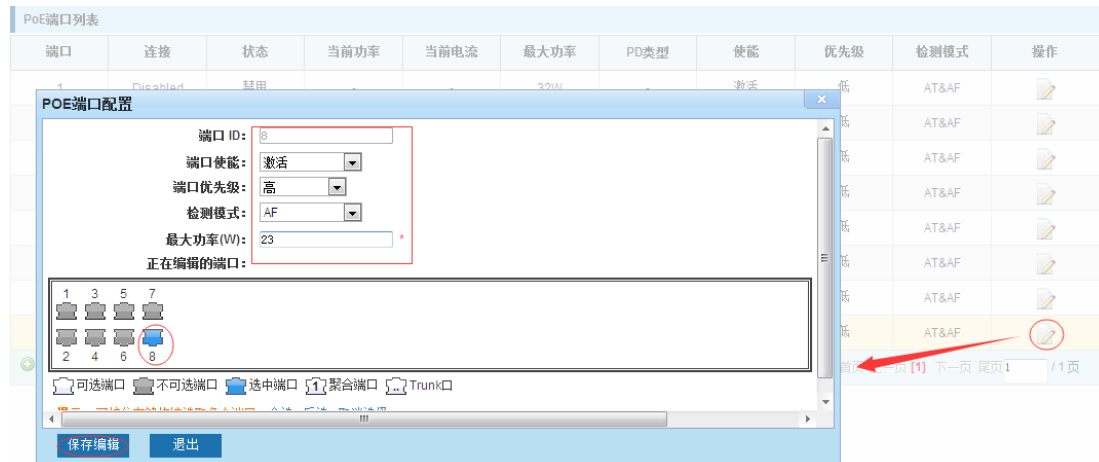
参数	描述
最大功率	选择配置的端口的最大功率
使能	选择配置的使能状态
优先级	配置端口的优先级，当负载超过 POE 最大功率时，优先级低的端口下设备将先掉线
检测模式	配置端口的检测模式

【使用说明】

接收 Trap 通告需将 Snmp 开启，并设置 trap 目标主机。

【配置举例】

如：将 8 口的端口使能打开，设置最大功率为 23 W、检测模式为 AF、优先级为高。



4.5.3 POE 延迟

在导航栏选择“POE 管理>POE 延迟”，可对端口 POE 延迟进行设置。如下图：



【参数说明】

参数	描述
重启时间段	设置端口重启的时间
端口延迟时间	设置端口延迟时间

【使用说明】

接收 Trap 通告需将 Snmp 开启，并设置 trap 目标主机。

【配置举例】

如：设置端口 1 的 POE 重启时间为每天的 9:57:33，端口延迟时间为 20 秒。



4.6 STP

在导航栏选择“STP”，您可以进行 **MSTP 域**和 **STP 桥/端口**等设置。



4.6.1 MSTP 域

在导航栏选择“STP>MSTP 域”，可修改域及域名，添加实例映射到 VLAN。如下图：



【参数说明】

参数	描述
域名	配置域的名称
修订级别	配置修订级别参数
实例 ID	选择配置实例 ID 号
VLAN ID	配置实例映射的 VLAN

【使用说明】

一个实例只能映射到一个 VLAN，实例和 VLAN 是一一对应的关系。

【配置举例】

如：将域改为 DEADBEEF0102，修订级别为 123，实例 4 映射到 VLAN 2 中，需先创建 VLAN 2。

The screenshot shows the MSTP configuration interface with the following details:

- MSTP域配置:** Domain: DEADBEEF0102 (1-32 characters), Revision: 123 (0-65535, default=0).
- 实例映射:** Instance ID: 4, Vlan ID: 2 (examples: 1,3,5,7-10).
- 实例映射列表:** A table showing Instance ID 0 mapped to Vlan 1-4094.

4.6.2 STP 桥/端口

在导航栏选择“STP>STP 桥/端口”，可对桥、端口进行相关配置，如下图：

The screenshot shows the STP configuration interface with the following details:

- STP桥配置:** Instance priority: 0, Priority: 32768. Mode: STP, RSTP, MSTP. Handshake time: 2s, Max Age: 10s, Forward delay: 10s, Max hops: 10.
- STP端口配置:** Instance: 0, Priority: 128. Bridge priority: auto. Port settings include: FastEthernet (disabled), Auto edge (enabled), Bpdu protection (enabled), Bpdu guard (enabled), TC protection (enabled), Root protection (None), and TC guard (disabled).

【参数说明】

参数	描述
实例优先级	是否开启实例优先级设置
实例 ID	选择已创建的实例 id 进行配置
使能	是否开启桥 STP 功能
桥优先级	设置桥实例优先级，默认桥实例优先级为 32768
模式	模式分为：STP、RSTP、MSTP
握手时间	交换机发送 BPDU 报文的时间间隔
最大老化时间	端口在该时间内未收到报文，会发起拓扑改变
转发延迟	端口的状态切换时间
端口优先级	设置端口实例优先级，默认为 128，必须输入 16 的

	倍数，范围 0-240
链路开销	auto or 1-200000000，用以决定各端口到根的路径花费
快速端口	PortFast 功能能够使得二层接入端口立即进入 Forwarding 状态
自动边缘	边缘端口的自动识别。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。
点对点	配置接口的连接类型是不是“点对点连接”
Bpdu 保护	开启该功能能够防止攻击者在直连终端的端口上发送 BPDU 导致网络震荡
Bpdu 过滤	开启 BPDU Filter 功能，将强制端口不参与生成树计算，端口不接收也不向外发送 BPDU 报文。
兼容性模式	根据当前端口的接口属性信息有选择性的携带 MSTI 的信息进行发送，以实现与其它产商之间的互连。
跟保护	启用 root guard 功能，能防止因错误配置或者非法报文的攻击导致当前根桥地地位的变化。
TC 保护	启用 tc-guard 功能，能防止 tc 报文的扩散。
TC 过滤	启用 tc 过滤功能，则端口收到的 TC 报文将不处理。

【使用说明】

- (1) $2 * (\text{握手时间} + 1) \leq \text{最大老化时间} \leq 2 * (\text{转发延迟} - 1)$ 。
 (2) 使能 STP 时，网页将等待 2 倍的转发延迟时间。

【配置举例】

如：1) 开启 stp，配置已创建的实例优先级，配置时间参数，将模式设为 mstp。

STP桥配置

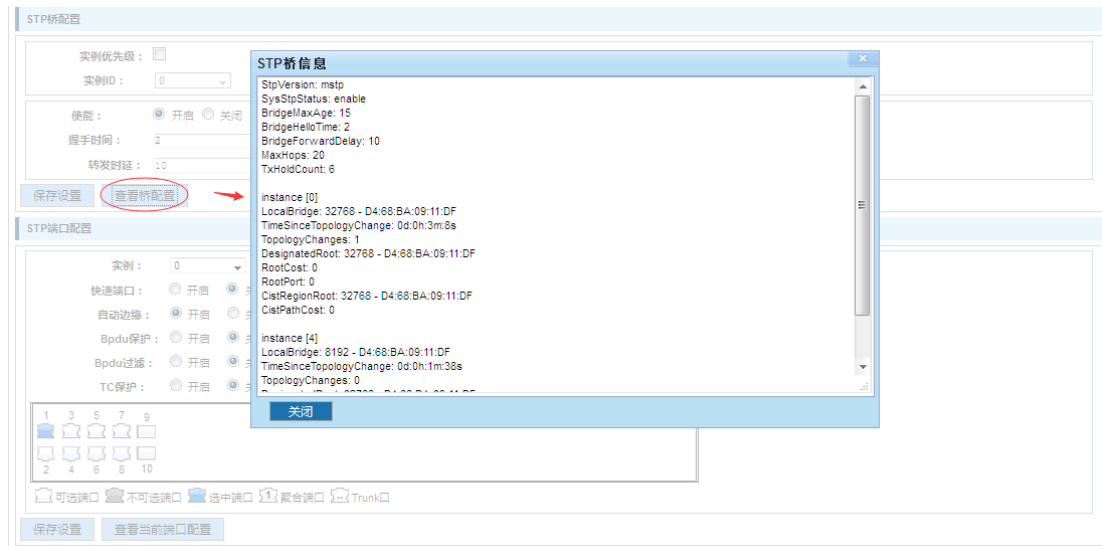
实例优先级: 实例ID: 4 优先级: 8192

使能: 开启 关闭 模式: STP RSTP MSTP

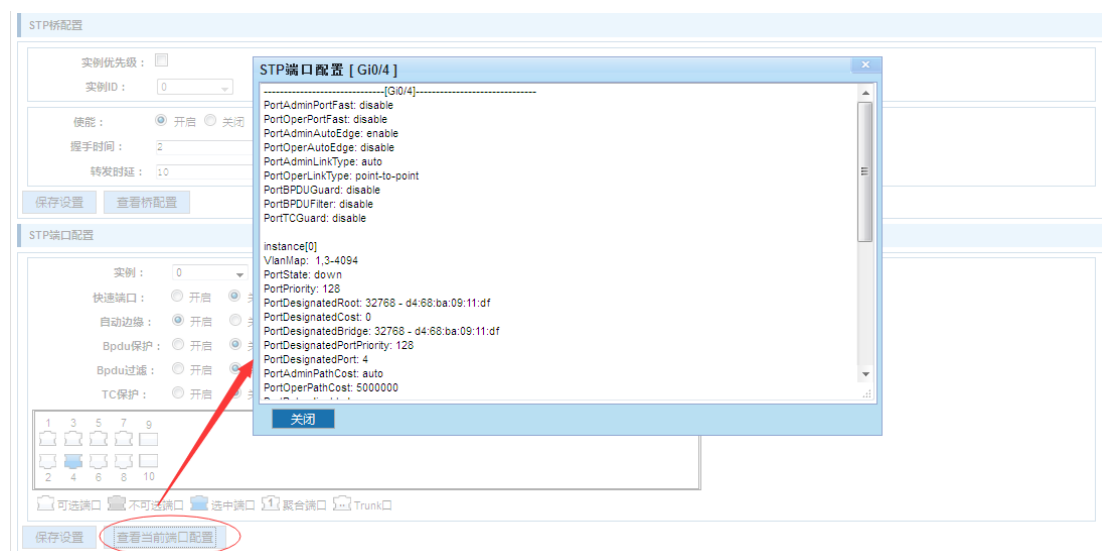
握手时间: 2 (1-10s) Max Age: 15 (6-40s)

转发时延: 10 (4-30s) 最大跳数: 20 (1-40)

保存设置 查看桥配置



2) 设置已上线端口 mstp 配置，选择已创建的实例，设置优先级（配置未上线的端口，需上线配置才会生效，才可点击“查看当前配置”按钮进行查看到已配置完成的）。



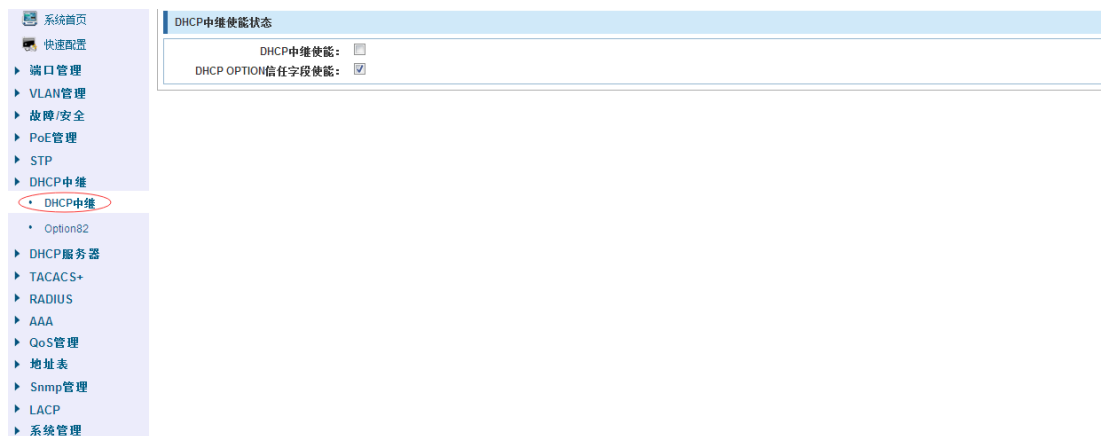
4.7 DHCP中继

在导航栏选择“DHCP 中继”，您可以进行 DHCP 中继和 option82 等设置。



4.7.1 DHCP 中继

在导航栏选择“DHCP 中继”，可开启 DHCP 中继功能，设置和查看中继服务器 IP 地址及其状态。如下图：



【参数说明】

参数	描述
IP 地址	DHCP 服务器地址
状态	生效和不生效
DHCP 中继使能	开启和关闭 DHCP 中继代理功能
DHCP option 信任字段使能	开启时，当收到的客户端 DHCP 报文带 option82 信息时，保留，否则添加交换机自己的 option82 信息转发出去。关闭时，丢弃客户端发来的带 option82 信息的报文。

【使用说明】

如果开启了中继代理功能，那么接收到的 DHCP 广播报文，将以单播形式发送到配置的服务器上。DHCP 服务器需和交换机 ip 在同一网段才会生效。

【配置举例】

如：设置 DHCP 服务器 ip 为 192.168.0.22 。

DHCP中继使能状态	
DHCP中继使能:	<input checked="" type="checkbox"/>
DHCP OPTION信任字段使能:	<input checked="" type="checkbox"/>
DHCP中继配置	
DHCP服务器IP:	192.168.0.22
<input type="button" value="增加"/>	

4.7.2 Option82

在导航栏选择“DHCP 中继>Option82”，可设置 OPTION82 代理电路、代理远程、ip 地址。如下图：

【参数说明】

参数	描述
VLAN id	DHCP 请求报文所在 VLAN，取值范围为 1~4094
电路控制	依据 DHCP 报文所走的 vlan 选择使用该 vlan 下所配置的电路 ID 子选项内容，如果没有配置的话，默认使用 circuit id 为 0 类型的，内容为 VLAN ID + interface number，即 DHCP 客户端所在 vlan 和端口。
远程代理	依据 DHCP 报文所走的 VLAN 选择使用该 VLAN 下所配置的远程 ID 子选项内容，如果没有配置的话，默认使用 remote id 为 0 类型的，内容为交换机 mac 地址。
IP 地址	依据 DHCP 报文所走的 vlan 选择使用该 vlan 下所配置的 IP 子选项内容，如果没有配置的话，不发送该选项。

【使用说明】

交换机中继到 dhcp 服务器会带上 option82 信息，需将 VLAN ID 配置成 dhcp 报文所走 VLAN 方可带上 option82 信息。

【配置举例】

如：添加电路控制、代理远程、ip 地址信息。

Option82配置

电路控制 代理远程 IP地址

电路控制: 123 *
VLAN ID: 1 *

添加

电路控制 代理远程 IP地址

代理远程: 123 *
VLAN ID: 1 *

添加

序号	远程代理名	远程代理ID	VLAN ID	操作
首页 上一页 1 下一页 尾页 1 /1页				

电路控制 代理远程 IP地址

IP地址: 192.168.0.35 *
VLAN ID: 1 *

添加

序号	IP地址	VLAN ID	操作
首页 上一页 1 下一页 尾页 1 /1页			

4.8 DHCP 服务器

在导航栏选择“DHCP 服务器”，可设置 DHCP 服务器使能、DHCP 地址池、Option、绑定表、缺省网关配置、DNS 服务器配置。如下图：



4.8.1 DHCP 服务器使能

在导航栏选择“DHCP 服务器>DHCP 服务器使能”，可在此开启或关闭 DHCP 服务器。如下图：



【使用说明】

开启 DHCP 服务器时必须先关闭 DHCP 中继功能。

【配置举例】

如：开启 DHCP 服务器。



4.8.2 DHCP 地址池

在导航栏选择“DHCP 服务器>DHCP 地址池”，可在此设置 DHCP 地址池。如下图：



【参数说明】

参数	描述
地址池 ID	设置地址池 ID 号范围在 1 ~ 65535 之间
子网 IP	设置子网 IP 地址，子网 IP 和开始 IP 需要在同一网段
子网掩码	设置子网掩码
开始 IP	设置开始 IP 地址
结束 IP	设置结束 IP 地址
租约时间	设置租约时间

【使用说明】

配置 DHCP 服务器地址池的功能，包括子网地址，子网掩码，租赁时间。

【配置举例】

如：设置地址池为 1，域名为 work，子网 IP 为 192.168.1.5，子网掩码为 255.255.255.0，开始 IP 为 192.168.1.100，结束 IP 为 192.168.1.199，租约时间为 1 天。

4.8.3 Option

在导航栏选择“DHCP 服务器>Option”，可在此设置 DHCP 服务器的 Option。如下图：

【参数说明】

参数	描述
地址池 ID	选择要配置地址池的 ID
代码	设置代码的值
代码值类型	可以选择以下几种类型： HEX ASCII IP
代码值	根据选择代码值类型设置代码值

【使用说明】

根据地址池的 ID 设置 DHCP 服务器的参数。

【配置举例】

如：选择地址池 ID 为 1，设置代码为 2，代码值类型为 IP 模式，代码值为 192.168.1.2。

4.8.4 绑定表

在导航栏选择“DHCP 服务器>地址表”，你可以在此查看或删除绑定的地址信息。如下图：

dhcp服务器使能 dhcp地址池 option 绑定表 缺省网关配置 DNS服务器配置				
绑定列表				
IP地址	硬件类型	硬件地址	过期时间	操作

4.8.5 缺省网关配置

在导航栏选择“DHCP 服务器>缺省网关配置”，你在此设置缺省网关。如下图：

dhcp服务器使能 dhcp地址池 option 绑定表 缺省网关配置 DNS服务器配置	
地址池ID	1
网关1	<input type="text"/>
网关2	<input type="text"/>
网关3	<input type="text"/>
网关4	<input type="text"/>
网关5	<input type="text"/>
网关6	<input type="text"/>
网关7	<input type="text"/>
网关8	<input type="text"/>
<input type="button" value="设置"/>	

【使用说明】

根据地址池的 ID 设置 DHCP 服务器的缺省网关。

【配置举例】

如：选择地址池 ID 为 1，设置网关为 192.168.1.55。

dhcp服务器使能 dhcp地址池 option 绑定表 缺省网关配置 DNS服务器配置	
地址池ID	1
网关1	192.168.1.55
网关2	<input type="text"/>
网关3	<input type="text"/>
网关4	<input type="text"/>
网关5	<input type="text"/>
网关6	<input type="text"/>
网关7	<input type="text"/>
网关8	<input type="text"/>
<input type="button" value="设置"/>	

4.8.6 DNS 服务器配置

在导航栏选择“DHCP 服务器>DNS 服务器配置”，你在此设置 DNS 服务器。如下图：

【使用说明】

根据地址池的 ID 设置 DHCP 服务器的 DNS 服务器。

【配置举例】

如：选择地址池 ID 为 1，设置网关为 47.54.89.210。

4.9 TACACS+

在导航栏选择“TACACS+>TACACS+配置”，你在此设置 TACACS+认证相关配置。

【使用说明】

对 TACACS+服务器参数设置。

【配置举例】

如：对全局和端口进行配置，设置服务器超时时长为 5，服务器重试次数为 3，会话/连接模式为 Multi，密钥为 2644as 服务器 IP 为 192.168.0.88，认证端口为 49。

TACACS+ 配置

全局配置

服务器超时时长:

服务器重试次数:

会话连接: Only Multi

密钥:

端口配置

服务器IP:

认证端口:

服务器超时时长:

密钥:

4.10 RADIUS

在导航栏选择“**RADIUS**”，你在此设置 RADIUS 认证相关配置。

RADIUS全局配置 RADIUS服务器配置

RADIUS全局配置信息

服务器重传次数: 3

服务器超时时间: 2

服务器静默时间: 0

dead-criteria重试次数: 0

dead-criteria超时时间: 0

系统首页

快速配置

端口管理

VLAN管理

故障/安全

PoE管理

STP

DHCP中继

DHCP服务器

TACACS+

RADIUS

RADIUS配置

AAA

QoS管理

地址表

Snmp管理

LACP

系统管理

4.10.1 RADIUS 配置

在导航栏选择“**RADIUS>RADIUS 配置**”，你在此设置 RADIUS 认证全局相关配置。

RADIUS全局配置 RADIUS服务器配置

RADIUS全局配置信息

服务器重传次数: 3

服务器超时时间: 2

服务器静默时间: 0

dead-criteria重试次数: 0

dead-criteria超时时间: 0

【使用说明】

对 RADIUS 服务器全局参数设置。

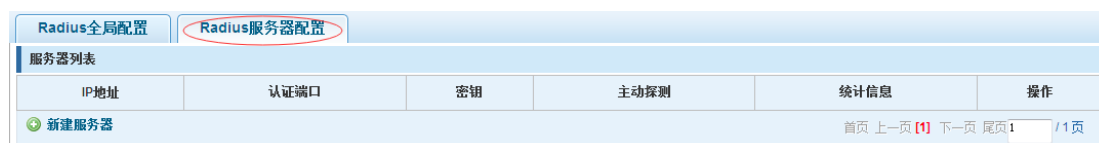
【配置举例】

如：设置 RADIUS 服务器重传次数为 3，服务器超时时间为 2，服务器静默时间为 200，Dead-criteria 重试次数为 3，Dead-criteria 超时时间为 5。



4.10.2 RADIUS 服务器配置

在导航栏选择“**RADIUS>RADIUS 服务器配置**”，你在此设置 RADIUS 服务器相关配置。



【使用说明】

对 RADIUS 服务器全局参数设置。

【配置举例】

如：设置服务器地址为 192.168.0.68，认证端口和密钥为默认，开启主动探测并设置测试名称我 test，空闲时间为 3。



4.11 AAA

在导航栏选择“**AAA**”，你在此设置**AAA使能**，**域**，**服务器组**，**AAA认证**相关配置。如下图所示：



4.11.1 AAA 使能配置

在导航栏选择“AAA>AAA 使能配置”，你在此开启或关闭 AAA 使能。如下图所示：

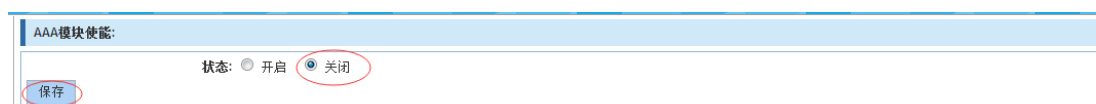


【使用说明】

开启或关闭 AAA 使能，默认为开启状态。

【配置举例】

如：关闭 AAA 使能。



4.11.2 域配置

在导航栏选择“AAA>域配置”，你在此设置域使能的相关参数。如下图所示：



【使用说明】

开启或关闭域使能，默认为开启状态，设置域使能相关参数。

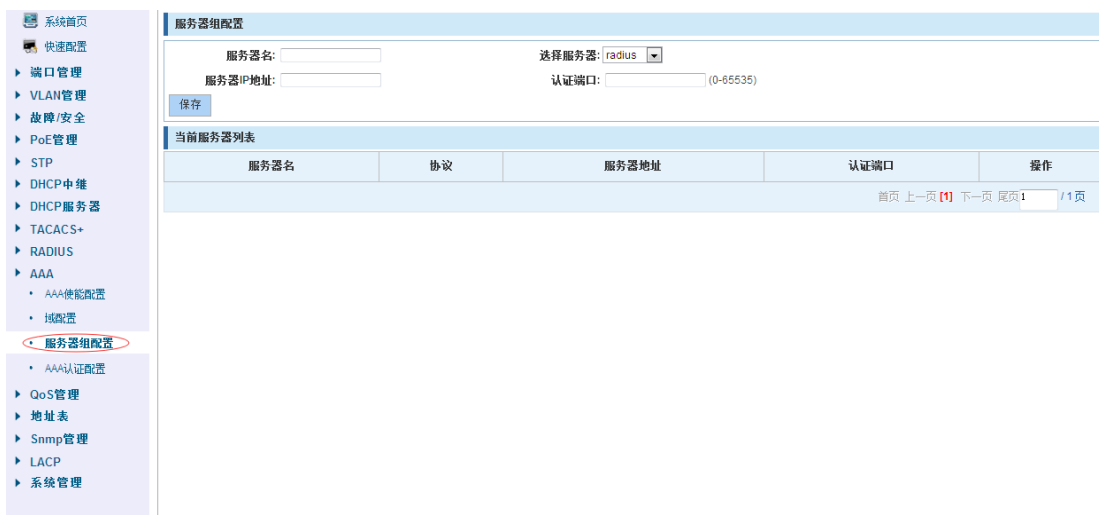
【配置举例】

如：开启域使能--设置 ISP 域。



4.11.3 服务器组配置

在导航栏选择“AAA>服务器组配置”，你在此设置多个服务器的相关参数。如下图所示：



【使用说明】

设置服务器的相关参数。

【配置举例】

如：

1. 设置服务器的相关参数。

服务器组配置

服务器名: 选择服务器:

服务器IP地址:

当前服务器列表

服务器名	协议	服务器地址	认证端口	操作
aaa	tacacs+	192.168.0.66		✘
aaa	radius	192.168.0.65	49	✘

首页 上一页 [1] 下一页 尾页 1 / 1页

2. 删除服务器。

当前服务器列表

服务器名	协议	服务器地址	认证端口	操作
aaa	tacacs+	192.168.0.66		✘
aaa	radius	192.168.0.65	49	✘

首页 上一页 [1] 下一页 尾页 1 / 1页

4.11.4 AAA 认证配置

在导航栏选择“**AAA>AAA 认证配置**”，你在此设置 AAA 认证的 **Login 认证**，**Enable 认证**，**Dot1x 认证**。如下图所示：

系统首页

快速配置

端口管理

VLAN管理

故障/安全

PoE管理

STP

DHCP中继

DHCP服务器

TACACS+

RADIUS

AAA

- AAA功能配置
- 域配置
- 服务器组配置
- AAA认证配置**

QoS管理

地址表

Snmp管理

LACP

系统管理

Login 认证 **Enable 认证** **Dot1x 认证**

AAA 认证配置

选择一个域名:

LOGIN 认证 方案名称:

第一方法:

第二方法:

第三方法:

第四方法:

login 认证列表

方案名称	方法	操作
default	(local)	✘

首页 上一页 [1] 下一页 尾页 1 / 1页

4.11.4.1 Login 认证

在导航栏选择“**AAA>AAA 认证配置>Login 认证**”，在此你可以设置 Login 认证的方法。如下图所示：

【参数说明】

参数	描述
第一方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第二方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第三方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第四方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无

【使用说明】

设置 Login 认证的方法。

【配置举例】

如：选择域名为 None，勾选 Login 认证，设置第一方法为本地服务器组，第二方法为 Radius

服务器组，第三方法为 TACACS+服务器组，第四方法为自定义服务器组。

The screenshot shows the 'AAA认证配置' (AAA Authentication Configuration) page. The 'Login认证' (Login Authentication) tab is selected. Under '选择一个域名' (Select a domain), 'none' is chosen. The 'LOGIN认证' (Login Authentication) section is checked. The '方案名称' (Scheme Name) is 'default'. The authentication methods are: 第一方法: 本地服务器组 (Local Server Group), 第二方法: RADIUS服务器组 (RADIUS Server Group), 第三方法: TACACS+服务器组 (TACACS+ Server Group), and 第四方法: 自定义服务器组 (Custom Server Group). The '服务器组' (Server Group) is set to 'ss'. A '保存' (Save) button is visible. Below the configuration is a table titled 'login认证列表' (Login Authentication List) with columns for '方案名称' (Scheme Name), '方法' (Method), and '操作' (Action). The table contains one entry: 'default' with method '(local) (group radius) (group tacacs+) (group ss)' and a delete icon. Navigation links at the bottom include '首页', '上一页', '下一页', and '尾页'.

4.11.4.2 Enable 认证

在导航栏选择“AAA>AAA 认证配置>Enable 认证”，在此你可以设置 Enable 认证的方法。如下图所示：

The screenshot shows the 'AAA认证配置' (AAA Authentication Configuration) page with the 'Enable认证' (Enable Authentication) tab selected. Under '选择一个域名' (Select a domain), 'none' is chosen. The 'ENABLE认证' (Enable Authentication) section is unchecked. The '方案名称' (Scheme Name) is 'default'. The authentication methods are: 第一方法: 本地服务器组 (Local Server Group), 第二方法: (empty), 第三方法: (empty), and 第四方法: (empty). A '保存' (Save) button is visible. Below the configuration is a table titled 'enable认证列表' (Enable Authentication List) with columns for '方案名称' (Scheme Name), '方法' (Method), and '操作' (Action). The table contains one entry: 'default' with method '(local)' and a delete icon. Navigation links at the bottom include '首页', '上一页', '下一页', and '尾页'.

【参数说明】

参数	描述
第一方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第二方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无

第三方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第四方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无

【使用说明】

设置 Enable 认证的方法。

【配置举例】

如：选择域名为 **None**，勾选 **Enable** 认证，设置第一方法为本地服务器组，第二方法为 **Radius 服务器组**，第三方法为 **TACACS+服务器组**，第四方法为自定义服务器组。

The screenshot shows the 'AAA authentication configuration' interface. At the top, there are tabs for 'Login authentication', 'Enable authentication', and 'Dot1x authentication'. The 'Enable authentication' tab is selected. Below the tabs, there is a section for 'AAA authentication configuration'. A dropdown menu for 'Select a domain' is set to 'none'. A checkbox for 'ENABLE authentication' is checked. The 'Scheme name' is 'default'. Below this, there are four dropdown menus for authentication methods: 'First method' is set to 'Local server group', 'Second method' is empty, 'Third method' is empty, and 'Fourth method' is empty. A 'Save' button is visible. Below the configuration area is a table titled 'enable authentication list' with columns for 'Scheme name', 'Method', and 'Operation'. The table contains one entry for 'default' with the method '(local) (group radius) (group tacacs+) (group ss)' and a red 'X' in the operation column. At the bottom right, there are navigation links: 'Home', 'Previous page (1)', 'Next page', 'End page 1', and '1/1 page'.

4.11.4.3 Dot 1x 认证

在导航栏选择“**AAA>AAA 认证配置>Dot 1x 认证**”，在此你可以设置 **Dot 1x** 认证的方法。如下图所示：



【参数说明】

参数	描述
第一方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第二方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第三方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无
第四方法	可以选择以下几种类型： 本地服务器组 Radius 服务器组 TACACS+服务器组 自定义服务器组 无

【使用说明】

设置 Enable 认证的方法。

【配置举例】

如：选择域名为 None，勾选 Enable 认证，设置第一方法为本地服务器组，第二方法为

Radius 服务器组，第三方法为 TACACS+服务器组，第四方法为自定义服务器组。

4.12 QoS管理

在导航栏选择“QoS 管理”，您可以进行队列设置和映射队列等设置。



4.12.1 队列设置

在导航栏选择“QoS>队列设置”，可设置队列的调度策略。如下图：

【参数说明】

参数	描述
调度策略	可选择 4 种模式：RR 循环调度 SP 绝对优先级调度 WRR 加权循环调度 WFQ 加权公平调度

WRR 权值	设置每个队列权值，他们将按比例占用带宽发送数据
--------	-------------------------

【使用说明】

队列 7 不能为 0。

【配置举例】

如：将调度策略设置为 WRR，权重值分别为 10、11、12、12、14、15、16、17。

4.12.3 映射队列

4.12.3.1 服务类别到队列映射

在导航栏选择“QoS>映射队列”，可将服务类别映射到相对应的队列。如下图：

服务ID	0	1	2	3	4	5	6	7
队列ID	0	1	2	3	4	5	6	7

【参数说明】

参数	描述
服务 ID	即 VLAN 的优先级 COS 字段 (0-7)
队列 ID	设置每个 COS 值映射的队列序号 (0-7)

【配置举例】

如：将 cos 3 映射到队列 7，将队列 7 的权值设置为 10。

服务类别到队列映射	差分服务到服务类别映射	端口到服务类别映射						
映射队列状态信息								
服务ID	0	1	2	3	4	5	6	7
队列ID	0	1	2	7	4	5	6	7
保存设置								
队列设置								
调度策略:	WRR							
字节 权值(0-127):	0	0	0	0	0	0	0	10
应用								

4.12.3.2 差分服务到服务类别映射

在导航栏选择“QoS>映射队列>差分服务到服务类别映射”，可将差分服务映射到相对应的服务类别。如下图：

服务类别到队列映射	差分服务到服务类别映射	端口到服务类别映射														
差分服务代码点映射队列表																
服务ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
服务列表1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
服务ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务列表2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3
服务ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
服务列表3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
服务ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
服务列表4	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7
保存设置																

【参数说明】

参数	描述
服务列表	dscp 字段有 7 位（0-63）分为 4 个表
队列 ID	将 DSCP 映射到 COS 字段（0-7），在根据 COS 映射到的队列

【使用说明】

Cos 优先级大于 dscp，dscp 优先级大于端口。

【配置举例】

如：将 dscp 值为 3、12、23 的全部映射到 cos5。

服务类别到队列映射	差分服务到服务类别映射	端口到服务类别映射														
差分服务代码点映射队列表																
服务ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
服务列表1	0	0	0	5	0	0	0	0	1	1	1	1	1	5	1	1
服务ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务列表2	2	2	2	2	2	2	2	5	3	3	3	3	3	3	3	3
服务ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
服务列表3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
服务ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
服务列表4	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7
保存设置																

4.12.3.3 端口到服务类别映射

在导航栏选择“QoS>映射队列>差分服务到服务类别”，可将端口映射到相对应的服务类别。如下图：

服务类别到队列映射	差分服务到服务类别映射	端口到服务类别映射							
端口COS映射									
端口:	1								
服务ID:	0								
信任模式:	COS								
应用									
控制列表									
端口	服务ID								信任模式
	0	1	2	3	4	5	6	7	
1	T								
2	T								
3	T								
4	T								
5	T								
6	T								
7	T								
8	T								
首页 上一页 (1) / 2 下一页 尾页 1 / 2 页									

【参数说明】

参数	描述
端口	选择端口号（0-8）
服务ID	映射到服务ID，然后根据服务ID进入队列

【使用说明】

Cos 优先级大于 dscp，dscp 优先级大于端口。

【配置举例】

如：将端口 4、5、6 分别映射到 cos4、cos5、cos6。

服务类别到队列映射
差分服务到服务类别映射
端口到服务类别映射

端口COS映射

端口 :

服务ID :

服务类别到队列映射
差分服务到服务类别映射
端口到服务类别映射

端口COS映射

端口 :

服务ID :

服务类别到队列映射
差分服务到服务类别映射
端口到服务类别映射

端口COS映射

端口 :

服务ID :

控制列表

端口	服务ID						
	0	1	2	3	4	5	6
1	T						
2	T						
3	T						
4					T		
5						T	
6							T
7	T						
8	T						

4.13 地址表

在导航栏选择“地址表”，您可以进行 **MAC 添加和删除**、**MAC 学习和老化**和 **MAC 地址过滤**等设置。

配置指南 ■ 64



4.13.1 Mac 添加与删除

在导航栏选择“地址表>Mac 添加与删除”，可添加静态 Mac 及删除 Mac 并查看到当前的 Mac 地址表。如下图：



【参数说明】

参数	描述
清除 Mac	可选择清除多播 Mac 地址、清除动态单播 Mac 地址、清除静态单播 Mac 地址、清除指定 Mac 地址、清除 Mac 地址表
VLAN	填入需添加或删除的 VLAN id, 未创建的 VLAN 需创建才可生效

【使用说明】

根据不同的条件清除 Mac 地址,查看/添加/学习 Mac 地址,Mac 地址过滤。

【配置举例】

如：1) 将端口 6 Mac 设置为静态的 Mac。

The screenshot shows a configuration window for a switch. At the top, there is a grid of 10 ports (1-10) with checkboxes. Port 6 is selected. Below the grid, there are radio buttons for port types: 可选端口 (Selected), 不可选端口 (Not Selected), 选中端口 (Selected), 聚合端口 (Aggregated), and Trunk口 (Trunk). The VLAN is set to 1, and the MAC address is 00:B0:53:08:B2:33. A '保存' (Save) button is at the bottom left.

2) 清除端口 6 静态的 Mac 地址。

The screenshot shows the '清除MAC' (Clear MAC) configuration window. The '清除MAC' dropdown is set to '清除指定MAC地址'. The VLAN is 1 and the MAC address is 00:B0:53:08:B2:33. A '保存' (Save) button is at the bottom left.

4.13.2 Mac 学习和老化

在导航栏选择“地址表>Mac 学习和老化”，可设置端口下 Mac 最大学习数及 Mac 地址老化时间。如下图：

The screenshot shows the '地址表配置' (Address Table Configuration) interface. The 'MAC学习和老化' (MAC Learning and Aging) tab is active. It shows a grid of 10 ports (1-10) with checkboxes. Below the grid, there are radio buttons for port types: 可选端口 (Selected), 不可选端口 (Not Selected), 选中端口 (Selected), 聚合端口 (Aggregated), and Trunk口 (Trunk). A tip says: 提示：可按住左键拖拽选取多个端口 (Tip: Hold the left button to select multiple ports). The 'MAC地址学习限制' (MAC Address Learning Limit) is set to 8191. The 'MAC地址老化时间' (MAC Address Aging Time) is set to 300. A table below shows the configuration for each port.

编号	端口	MAC地址学习限制数
1	Gi0/1	8191
2	Gi0/2	8191
3	Gi0/3	8191
4	Gi0/4	8191
5	Gi0/5	8191
6	Gi0/6	8191
7	Gi0/7	8191
8	Gi0/8	8191

At the bottom right, there are navigation buttons: 首页, 上一页, 1, 下一页, 尾页, 1, / 2页.

【参数说明】

参数	描述
Mac 地址学习限制	范围 0-8191，默认为 8191
Mac 地址老化时间	默认下为 300

【使用说明】

根据不同的条件清除 Mac 地址,查看/添加/学习 Mac 地址,Mac 地址过滤。

【配置举例】

如：1) 设置端口 5、6、3、4 最大学习数为 3000。

MAC地址学习限制: 3000 (0表示不限制,0-8191)

2) 将端口设备掉线或学习到的 Mac 地址过 2 分钟后从 Mac 地址表中自动消失。

MAC地址老化时间: 120 (0表示不老化,10-1000000秒)

4.13.3 Mac 地址过滤

在导航栏选择“地址表>Mac 地址过滤”，可根据条件过滤过不需要的 Mac 地址。如下图：

MAC地址	VLAN ID	地址类型	删除

首页 上一页 1 / 1 下一页 尾页 1 / 1 页

【参数说明】

参数	描述
Mac 地址	不能添加组播的 Mac 地址
VLAN	VLAN 号

【使用说明】

根据不同的条件设置 Mac 地址过滤。

【配置举例】

如：将 Mac 地址为 00:20:15:09:12:12 添加到过滤表中。

编号	MAC地址	VLAN ID	地址类型	端口
1	00:20:15:09:12:12	1	过滤	

4.14 Snmp管理

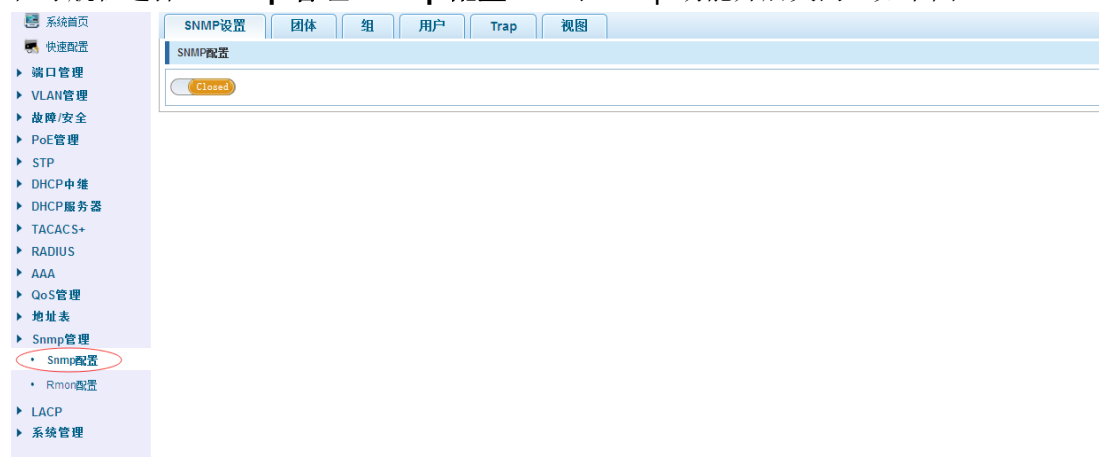
在导航栏选择“Snmp 管理”，您可以进行 Snmp 配置和 Rmon 配置等设置。



4.14.1 Snmp 配置

4.14.1.1 Snmp 配置

在导航栏选择“Snmp 管理>Snmp 配置”，可 Snmp 功能开启关闭。如下图：



【使用说明】

在配置 Rmon 的时候 Snmp 功能必须开启，否则会配置失败。

【配置举例】

如：开启 Snmp。



4.14.1.2 团体

在导航栏选择“Snmp 管理>Snmp 配置>团体”，可指定团体的访问权限。如下图：



【参数说明】

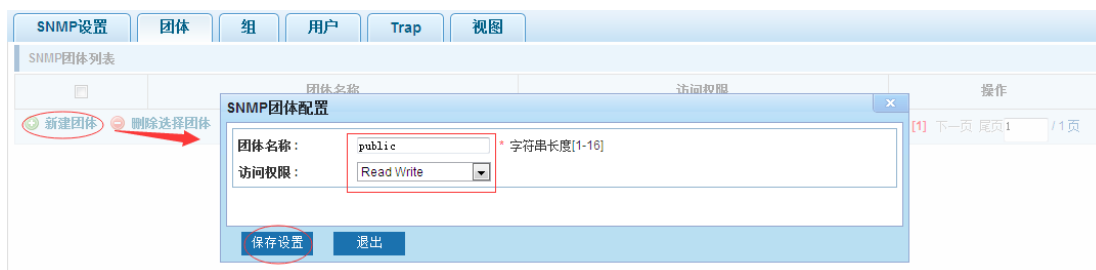
参数	描述
团体名称	团体字符串，相当于 NMS 和 Snmp 代理之间的通信密码
访问权限	只读：指定 NMS（Snmp 主机）对 MIB 的变量只能读，不能修改 只读可写：指定 NMS（Snmp 主机）对 MIB 的变量只能读，也可修改

【使用说明】

团体配置数量上限为 8。

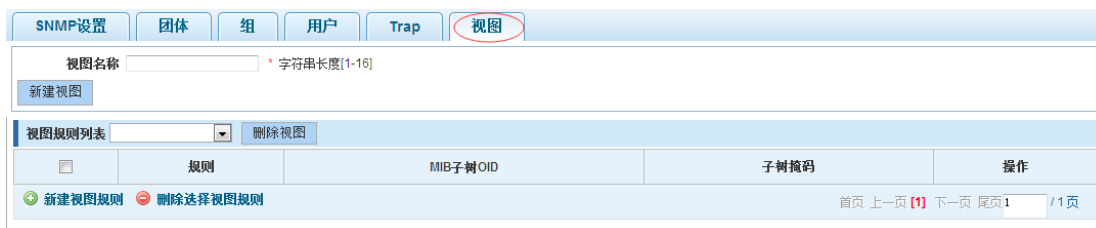
【配置举例】

如：添加一条名为 public 的可读写团体。



4.14.1.3 视图

在导航栏选择“Snmp 管理>Snmp 配置>视图”，设置视图规则来允许或禁用对某些 MIB 对象的访问。如下图：



【参数说明】

参数	描述
视图名称	视图名
包含	标明该 MIB 对象子数被包含在视图之内
排除	标明该 MIB 对象子数被排除在视图之外
MIB 子树 OID	视图关联的 MIB 对象，是一棵 MIB 子数
子树掩码	MIB OID 掩码

【使用说明】

每个视图最好配置一个视图规则，否则会影响 Snmp 功能。

【配置举例】

如：建立视图 123、将 MIB 子树 oid 1.3.6.1 包含其中。



4.14.1.4 组

在导航栏选择“Snmp 管理>Snmp 配置>组”，设置 Snmp 用户组。如下图：



【参数说明】

参数	描述
组名称	用户组名
安全级别	只认证不加密：该组的用户传输的消息需要验证但数据不需要保密 不认证不加密：该组用户传输的消息不需要验证数据也不需要保密 既认证又加密：该组用户传输的消息需要验证同时传输的数据需要保密
只读视图、读写视图、通知视图	关联的视图名

【使用说明】

组配置数量上限为 8，新建组之前需新建视图才可创建组。

【配置举例】

如：先新建视图 123，再新建组 goup1。



4.14.1.5 用户

在导航栏选择“Snmp 管理>Snmp 配置>用户”，设置 Snmp 用户。如下图：



【参数说明】

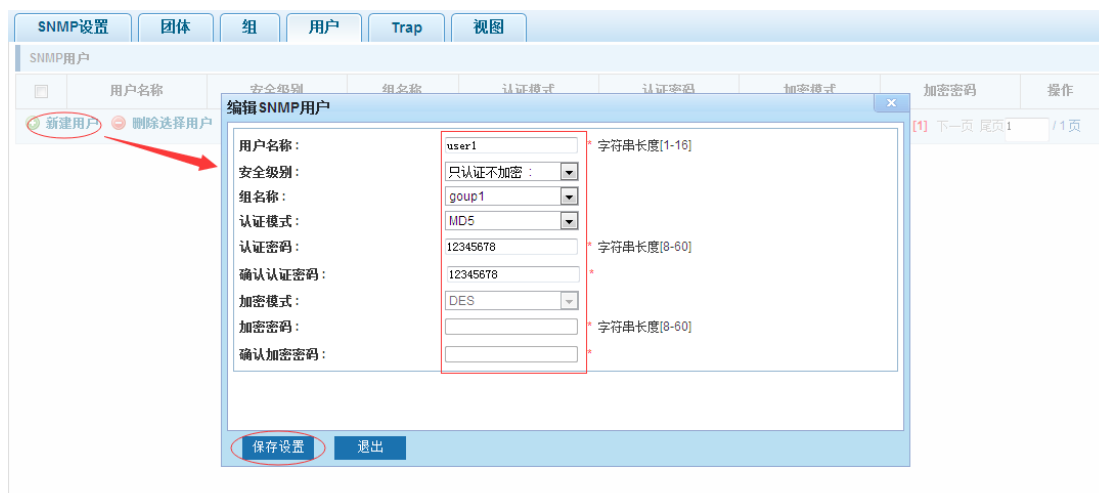
参数	描述
组名称	用户名，范围 1-16
安全级别	只认证不加密：该组的用户传输的消息需要验证但数据不需要保密 不认证不加密：该组用户传输的消息不需要验证数据也不需要保密 既认证又加密：该组用户传输的消息需要验证同时传输的数据需要保密
认证模式	指定使用 MD5 认证协议或 SHA 认证协议
认证密码	范围 8-60
加密模式	指定使用 AES 加密协议或 DES 加密协议
组名称	用户组名
加密密码	范围 8-60

【使用说明】

用户配置数量上限为 8，需新建视图及组才可使用，用户的安全级别需与组的安全级别一致。添加一个用户所使用的认证以及加密方式，并配置所属的用户组，该用户将用于 Snmpv3 连接。

【配置举例】

如：新建视图 123，新建组 group1，新建用户 user1。



4.14.1.6 Trap

在导航栏选择“Snmp 管理>Snmp 配置>Trap”，可指定发送陷阱消息的 Snmp 主机（NMS）。如下图：



【参数说明】

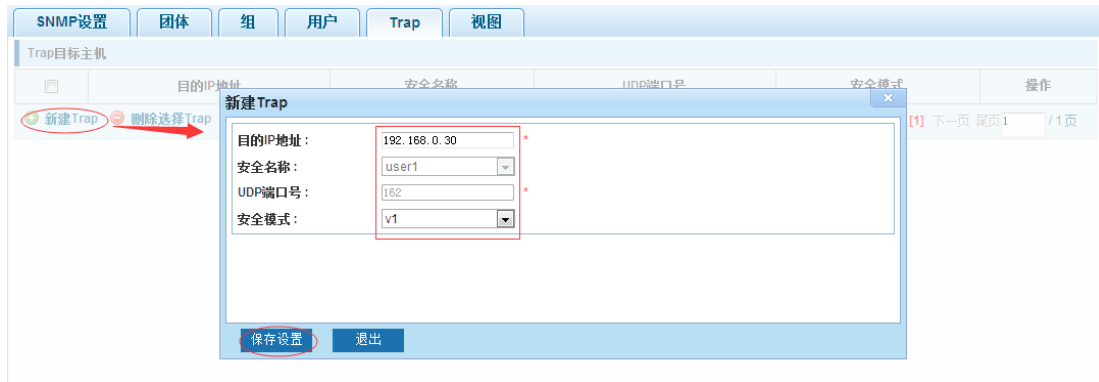
参数	描述
目的 ip 地址	Snmp 主机 ipv4 地址
安全名称	Snmp 用户名
安全模式	V1、V2、V3
认证密码	范围 8~60 字符
加密模式	指定使用 AES 加密协议或 DES 加密协议
组名称	用户组名
加密密码	范围 8~60 字符

【使用说明】

Trap 配置数量上限为 8，可以配置多个不同的 Snmp 主机用于接收陷阱消息。触发陷阱消息的时间有：端口的 Linkup/LinkDown，设备的 cold-start（掉电重启）/ warm-start（热重启），以及 Rmon 设置的端口端口统计的上下阈值。

【配置举例】

如：设置主机 192.168.2.30 来接收 trap 消息。



4.14.2 Rmon 配置

4.14.2.1 统计组

在导航栏选择“Snmp 管理>Rmon 配置>统计组”，设置监控某个以太网接口统计数据。如下图：



【参数说明】

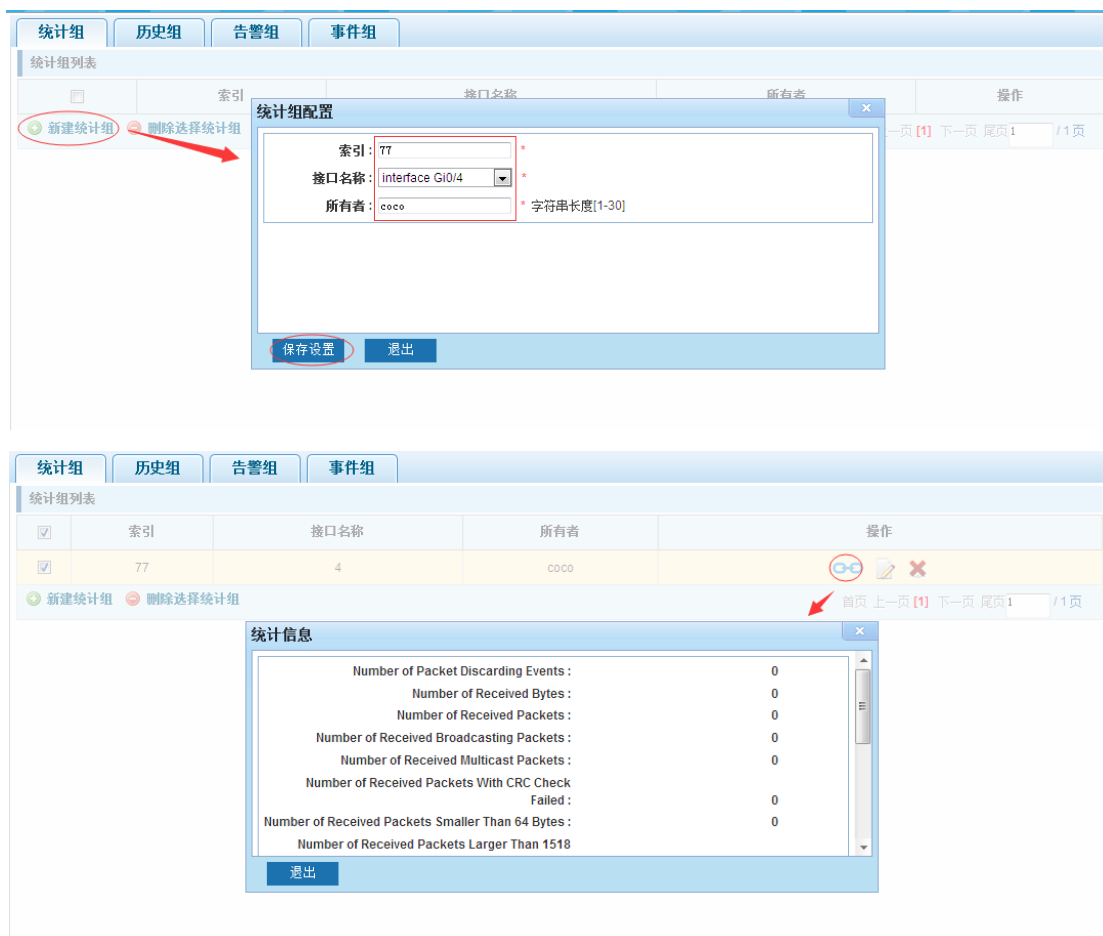
参数	描述
索引	统计信息表的索引号，取值范围为 1~65535
接口名称	要监听的源端口
所有者	设置表项创建者，范围：1~30 个字符的字符串

【使用说明】

在配置 Rmon 的时候 Snmp 功能必须开启，否则会弹出提示框。

【配置举例】

如：设置监控以太网端口 4 后查看数据。



4.14.2.2 历史组

在导航栏选择“Snmp 管理>Rmon 配置>历史组”，记录某个以太网接口的历史信息。如下图：



【参数说明】

参数	描述
索引	历史控制表项的索引号，取值范围为 1~65535
接口名称	要记录的以太网接口号
最大采样条数	设置历史控制表项对应的历史表容量，即历史表最多可容纳的记录数，取值范围为 1~65535
采样周期	设置统计周期，取值范围为 5~3600，单位为秒
所有者	设置表项创建者，范围：1~30 个字符的字符串

【使用说明】

在配置 Rmon 的时候 Snmp 功能必须开启，否则会弹出提示框。

【配置举例】

如：监控以太网端口 4 历史信息。



4.14.2.3 事件组

在导航栏选择“Snmp 管理>Rmon 配置>事件组”，定义事件触发时，记录事件的方式。如下图：



【参数说明】

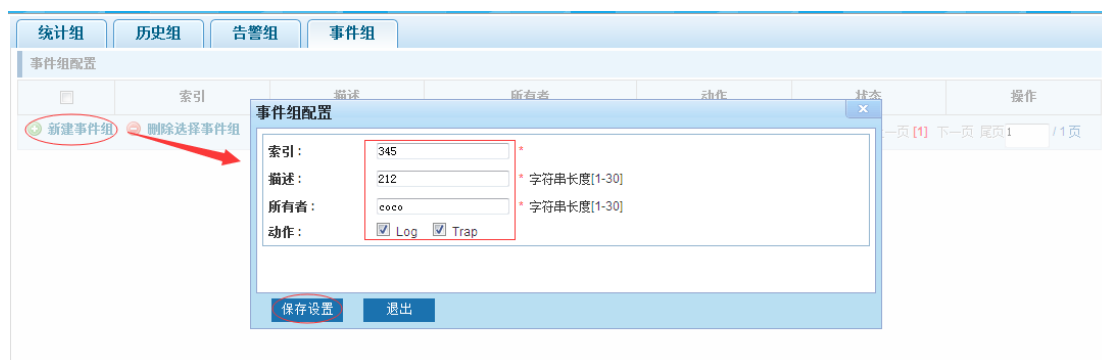
参数	描述
索引	事件表的索引号，取值范围为 1~65535
动作	Trap 事件，当事件被触发时，系统会发送 Trap 消息 日志事件，当事件被触发时，系统会记录日志
所有者	设置表项创建者，ownername 为 1~30 个字符的字符串

【使用说明】

在配置 Rmon 的时候 Snmp 功能必须开启，否则会弹出提示框。

【配置举例】

如：创建事件 345 触发时，系统发送 trap 消息及记录日志。



4.14.2.4 告警组

在导航栏选择“Snmp 管理>Rmon 配置>告警组”，定义告警组。如下图：



【参数说明】

参数	描述
索引	告警表项的索引号，取值范围为 1~65535
静态表项	统计类型值：3:DropEvents；4:Octets；5:Pkts；6:BroadcastPkts；7:MulticastPkts；8:CRCAAlignErrors；9:UndersizePkts；10:OversizePkts；11:Fragments；12:Jabbers；12:Collisions；14:Pkts64Octets；15:Pkts65to127Octets；16:Pkts128to255Octets；17:Pkts256to511Octets；18:Pkts512to1023Octets；19:Pkts1024to1518Octets
统计索引	设置统计对应的统计索引号，决定统计监听的端口号
采样时间间隔	采样间隔时间，取值范围为 5~65535，单位为秒
采样类型	采样类型为绝对值采样，即采样时间到达时直接提取变量的值
最近一次采样数	采样类型为变化值采样，即采样时间到达时提取的是变量在采样间隔内的变化值
告警阈值上限	设置上限参数值
告警阈值下限	设置下限参数值
超过/低于阈值下限所执行的事件	上限/下限达到时，各自对应的事件号
所有者	设置表项创建者，ownername 为 1~30 个字符的字符串

【使用说明】

在配置 Rmon 的时候 Snmp 功能必须开启，否则会弹出提示框。该配置需先配置统计组及事件组。

【配置举例】

如：新建统计组 77 和事件组 345，设置超过上限 3000 及低于下限 1000 告警。



4.15 LACP

在导航栏中选择“LACP”，您可以设置“LACP设置”和“LACP显示”。



4.15.1 LACP 设置

在导航栏中选择“LACP>LACP 设置”，您可以设置 LACP 配置相关信息。

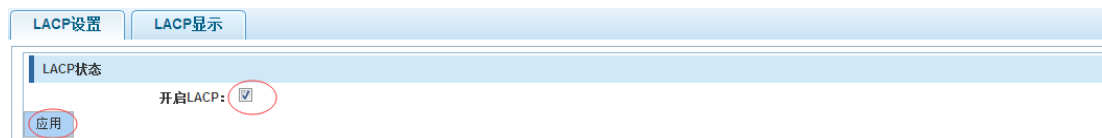


【使用说明】

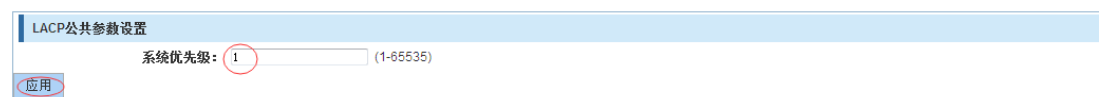
LACP，基于 IEEE802.3ax 标准的 LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。

【配置举例】

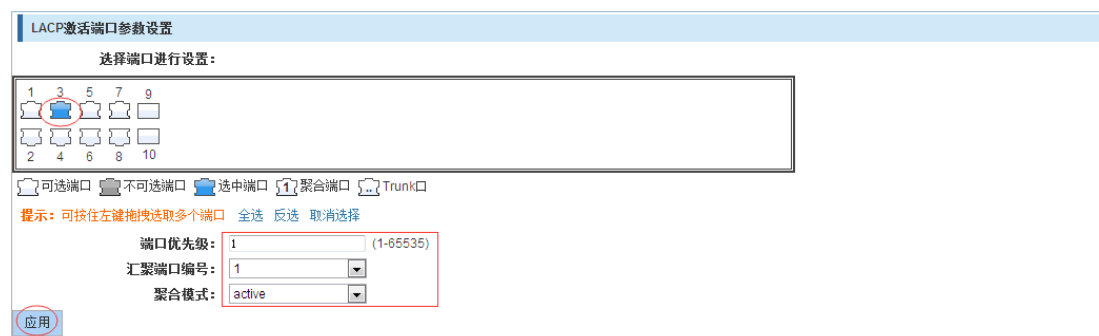
如：1. 开启 LACP 功能。



2. 设置系统优先级。



3. 设置端口 LACP 功能。



4.15.2 LACP 显示

在导航栏中选择“LACP>LACP 显示”，您可以查看 LACP 配置的相关信息。

LACP设置		LACP显示							
LACP列表									
所属聚合ID	端口ID	端口状态标志	端口状态	端口优先级	端口操作key	端口号	lacp协议状态	查看对端信息	操作
1	Gi0/4	SP	down	1	4	4	0x4c000000	0x41000000	✘
1	Gi0/3	SA	down	1	4	3	0x4d000000	0x41000000	✘

首页 上一页 1 下一页 尾页 1 / 1页

【使用说明】

LACP，基于 IEEE802.3ax 标准的 LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。

【配置举例】

如：1. 删除已 LACP 功能的端口。

LACP设置		LACP显示							
LACP列表									
所属聚合ID	端口ID	端口状态标志	端口状态	端口优先级	端口操作key	端口号	lacp协议状态	查看对端信息	操作
1	Gi0/4	SP	down	1	4	4	0x4c000000	0x41000000	✘
1	Gi0/3	SA	down	1	4	3	0x4d000000	0x41000000	✘

首页 上一页 1 下一页 尾页 1 / 1页

4.16 系统管理

在导航栏选择“系统管理”，您可以进行系统设置、系统升级、配置管理、配置保存、管理员权限和一键信息收集等设置。

- ▶ 系统管理
 - 系统设置
 - 系统升级
 - 配置管理
 - 配置保存
 - 管理员权限
 - 一键信息收集

4.16.1 系统设置

4.16.1.1 系统设置

在导航栏选择“系统管理>系统设置”，可对交换机基本信息进行设置。如下图：

The screenshot shows the 'System Settings' (系统设置) page. The left sidebar has 'System Management' (系统管理) selected, with 'System Settings' (系统设置) highlighted. The main content area is divided into two sections: 'System Basic Information' (系统基本信息) and 'System Time' (系统时间).

System Basic Information:

- 管理VLAN: 1
- 管理IP: 192.168.0.1
- 掩码: 255.255.255.0
- 默认网关: 0.0.0.0
- 巨型帧: 1518 (1518-9216)
- DNS服务器: 0.0.0.0
- 登录超时(分): 30
- 设备MAC: 04:68:BA:09:11:DF
- IPv6地址: (empty)
- 设备名称: Switch
- 设备位置: (empty)
- 联系方式(含邮箱): (empty)

System Time:

- 当前系统时间: 2000-01-01 03:05:10
- 重新设置时间: (empty)
- 自动与Internet时间服务器同步

【参数说明】

参数	描述
设备名称	交换机名称
管理 VLAN	交换机管理使用 VLAN
管理 ip	管理交换机 ip 地址
登录超时	登录后未使用超过登录超时后重新进行登录
巨型帧	范围 1518-9216

【配置举例】

如：1) 设置管理 VLAN 为 2 设置管理 VLAN，需先在 VLAN 设置中创建 VLAN，并将空闲端口设置到此 VLAN 中。

The screenshot shows the 'VLAN Settings' (VLAN设置) page. The 'VLAN List' (VLAN列表) table is visible:

VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作
1	VLAN0001	192.168.0.1/24	1-4,7-10	[Edit]
2	VLAN0002		5-6	[Delete]

Below the table are buttons for '新建VLAN' (New VLAN) and '删除选择VLAN' (Delete Selected VLAN). The page also shows navigation links: '首页 上一页 [1] 下一页 尾页 1 / 1页'.

The screenshot also shows the 'System Settings' (系统设置) page with the 'Management VLAN' (管理VLAN) field set to 2, circled in red. Other fields are the same as in the previous screenshot.

2) 将 pc 接口插入 5 或 6 端口, 设置管理 ip 为 192.168.0.12 , ipv6 设置为设备名称为 yoyo, 超时时间为 20 分钟, 巨型帧为 5000。

系统设置 | 系统重启 | 密码修改 | EEE使能 | ssh登录 | Telnet登录 | 系统日志

系统基本信息

管理VLAN: 2 * 设备MAC: D4:68:BA:09:11:DF

管理IP: 192.168.0.12 * ipv6地址:

掩码: 255.255.255.0 * 设备名称: yoyo

默认网关: 0.0.0.0 设备位置:

巨型帧: 5000 (1518-9216) 联系方式(含邮箱):

DNS服务器: 0.0.0.0

登陆超时(分): 20

保存设置 设置管理vlan

3) 用 192.168.0.12 进行访问，设置系统时间

系统时间

当前系统时间: 2000-01-01 03:09:04

重新设置时间:

自动与Internet同步

保存设置

日 一 二 三 四 五 六

27 28 29 30 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 27 28 29 30 31

1 2 3 4 5 6 7

时间 19: 1 : 1

清空 今天 确定

4.16.1.2 系统重启

在导航栏选择“系统管理>系统重启”，可对设备进行重启。如下图：

系统首页

快速配置

端口管理

VLAN管理

故障/安全

PoE管理

STP

DHCP中继

DHCP服务器

TACACS+

RADIUS

AAA

QoS管理

地址表

Snmp管理

LACP

系统管理

系统设置

系统升级

配置管理

配置保存

管理员权限

一键信息收集

系统设置 | 系统重启 | 密码修改 | EEE使能 | ssh登录 | Telnet登录 | 系统日志

立即重启设备

【使用说明】

点击重启按钮将使交换机重新启动，重启过程需要 2 分钟左右的时间，请耐心等待，设备重启后将会自动刷新页面。

【配置举例】

如：点击“立即重启设备”按钮。



4.16.1.3 密码修改

在导航栏选择“系统管理>密码修改”，可对设备进行密码修改。如下图：



【使用说明】

如果您设置了新的 Web 登录密码，则在设置之后使用新密码重新登录。密码只能包含英文、数字以及下划线。如忘记重设的密码，可在控制台进行重新设置。

```
yoyo(config)# password admin
```

New Password:1234。

Confirm Password:1234。

【配置举例】

如：选择密文密码，将密码修改为 1234。



4.16.1.4 EEE

在导航栏选择“系统管理>系统设置>EEE”，可将 EEE 开启。如下图：



【使用说明】

【配置举例】

例如：EEE 开启,可以高效节能以太网。



4.16.1.5 SSH 登录

在导航栏选择“系统管理>ssh 登录”，可开启 SSH。如下图：



【使用说明】

配置用户通过 ssh 登录设备需开启使能开关。

【配置举例】

如：将 SSH 开启，设置 SSH 超时为 3 分钟，可用 CRT 进行登录。

**4.16.1.6 Telnet 登录**

在导航栏选择“系统管理>Telnet 登录”，可开启 Telnet。如下图：

**【使用说明】**

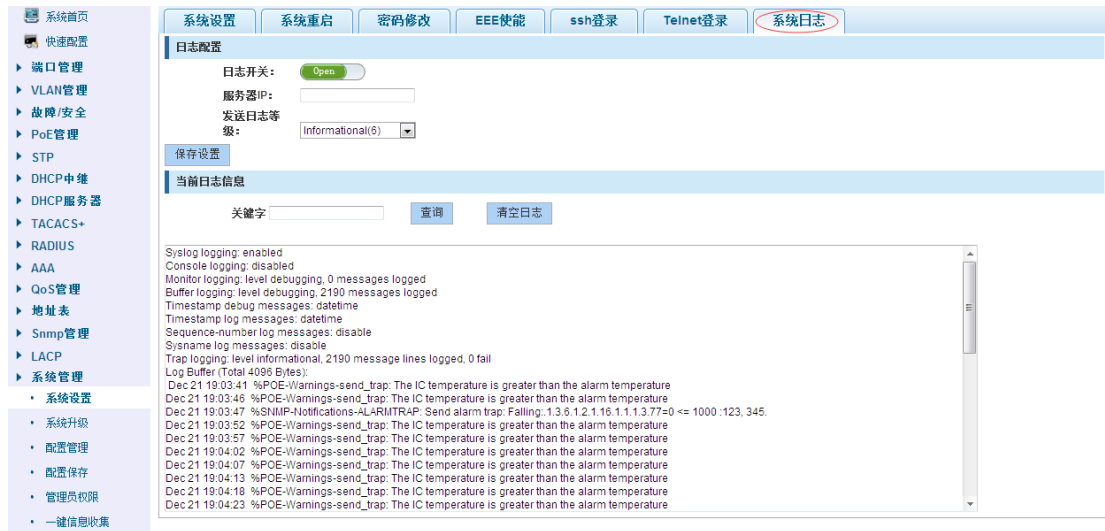
配置用户通过 Telnet 登录设备需开启使能开关。

【配置举例】

如：将 Telnet 开启，电脑 Telnet 功能开启，可进行登录。

**4.16.1.7 系统日志**

在导航栏选择“系统管理>系统日志”，可查看日志并设置日志服务器。如下图：



【参数说明】

参数	描述
日志开关	打开与关闭
服务器 ip	指定的服务器地址
发送日志等级	0-7
关键字	输入所需查询的字符

【使用说明】

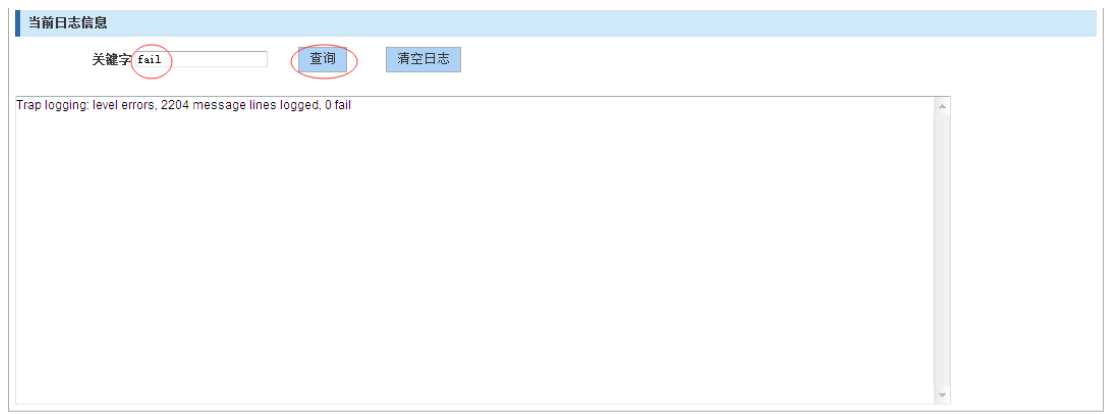
开启日志开关，设置 syslog 服务器，系统日志将自动推送到服务器中。

【配置举例】

如：1) 将错误的日志信息推送到服务器 192.168.0.2 中。

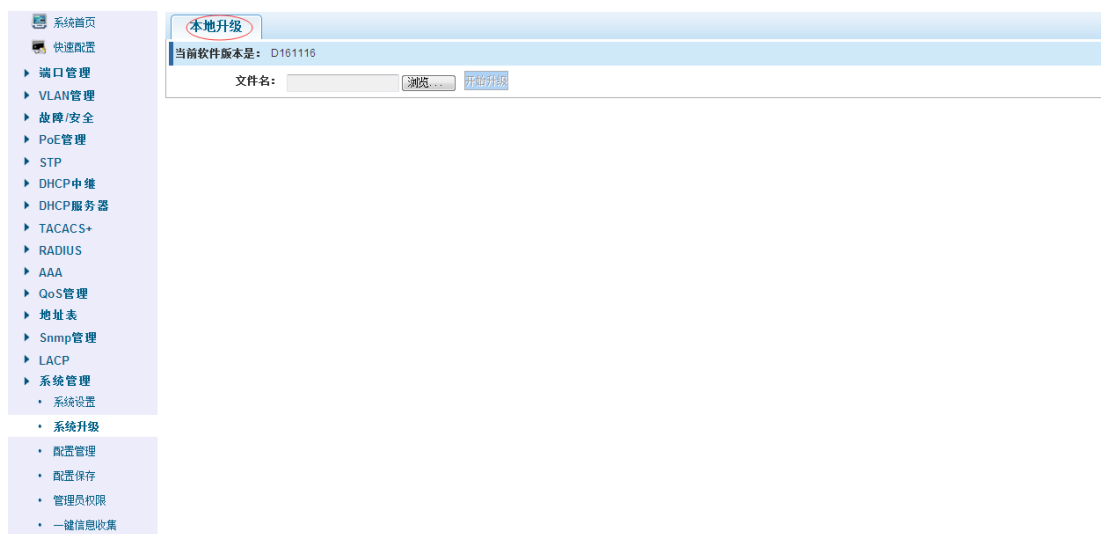


2) 输入 fail 关键字，进行查看，点击“清空日志”按钮，可清空日志



4.16.2 系统升级

在导航栏选择“系统管理>系统升级”，可查选择升级文件进行升级。如下图：

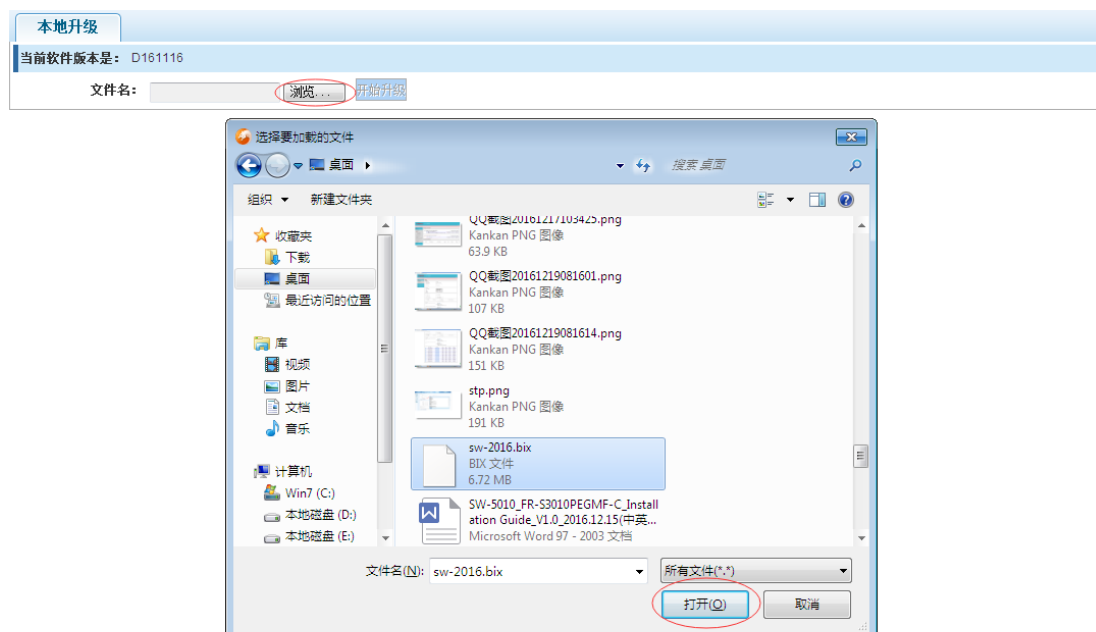


【使用说明】

- 1、请确认所升级的版本型号与本设备的型号相同。
- 2、在升级过程中，可能会遇到整理 flash 从而导致页面暂时没响应，此时不能断电或者重启设备，直到提示升级成功！

【配置举例】

如：选择文件进行升级。



4.16.3 配置管理

4.16.3.1 当前配置

在导航栏选择“系统管理>配置管理>当前配置”，可导入导出配置文件，备份文件。如下图：

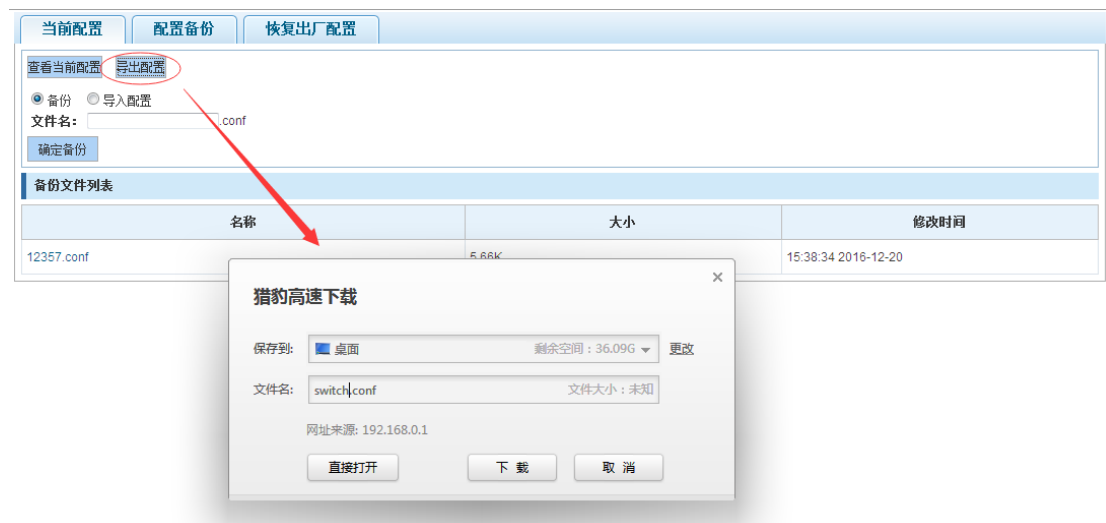


【使用说明】

导入配置后，要启用新的配置，请在当前配置页面 [重启设备](#) 否则配置不生效。

【配置举例】

如：1) 先在配置保存页面，点击保存配置，保存当前配置，再导出配置。



2) 导入配置

当前配置 | 配置备份 | 恢复出厂配置

查看当前配置 | 导出配置

备份 导入配置

导入过程中不能关闭或者刷新页面，否则导入将失败！

提示： 导入配置后，要启用新的配置，请在本页面 **重启设备** 否则配置不生效

文件名:

备份文件列表

名称	修改时间
12357.conf	8:34 2016-12-20

选择要加载的文件

组织 > 新建文件夹

库

- SW-5010_FR-S3010PEGMF-C_Installation Guide_V1.0_2016.12.15(中英...
- Microsoft Word 97 - 2003 文档
- switch.conf
CONF 文件
3.13 KB
- WirelessMon
快捷方式
899 字节
- wireshark
快捷方式
1.34 KB
- WPS HS
快捷方式
2.17 KB
- XJK7Z4[V05W6]529ZQGX5.png

文件名(N): switch.conf 所有文件 (*.*)

当前配置 | 配置备份 | 恢复出厂配置

查看当前配置 | 导出配置

备份 导入配置

导入过程中不能关闭或者刷新页面，否则导入将失败！

提示： 导入配置后，要启用新的配置，请在本页面 **重启设备** 否则配置不生效

文件名: 未选择文件。

3) 备份文件

当前配置 | 配置备份 | 恢复出厂配置

查看当前配置 | 导出配置

备份 导入配置

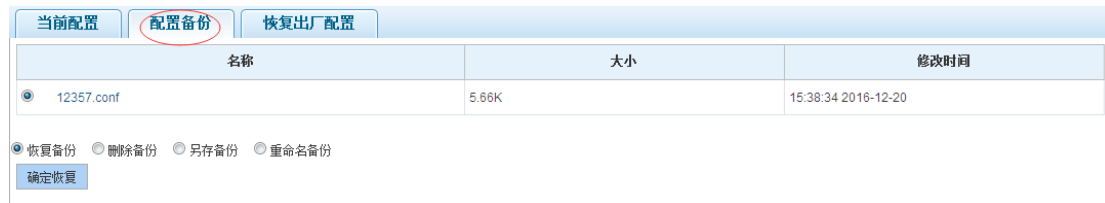
文件名: .conf

备份文件列表

名称

4.16.3.2 配置备份

在导航栏选择“系统管理>配置管理>配置备份”，可配置备份文件。如下图：

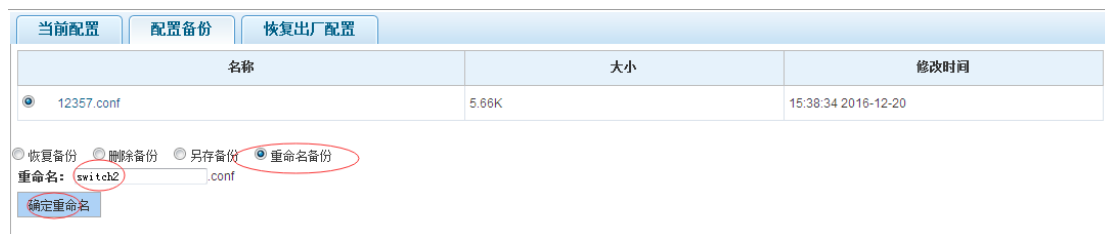


【使用说明】

操作此页面需先在当前配置页面，备份文件。

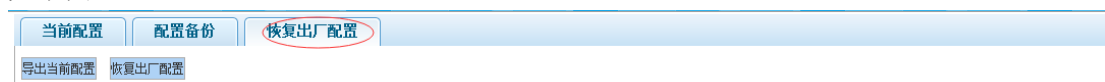
【配置举例】

如：重命名备份文件。



4.16.3.3 恢复出厂配置

在导航栏选择“系统管理>配置管理>恢复出厂配置”，可导出当前配置及恢复出厂配置。如下图：

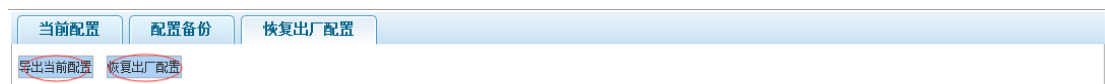


【使用说明】

恢复出厂配置，将删除当前所有配置。如果当前系统有有用的配置，可先导出当前配置后再恢复出厂配置。

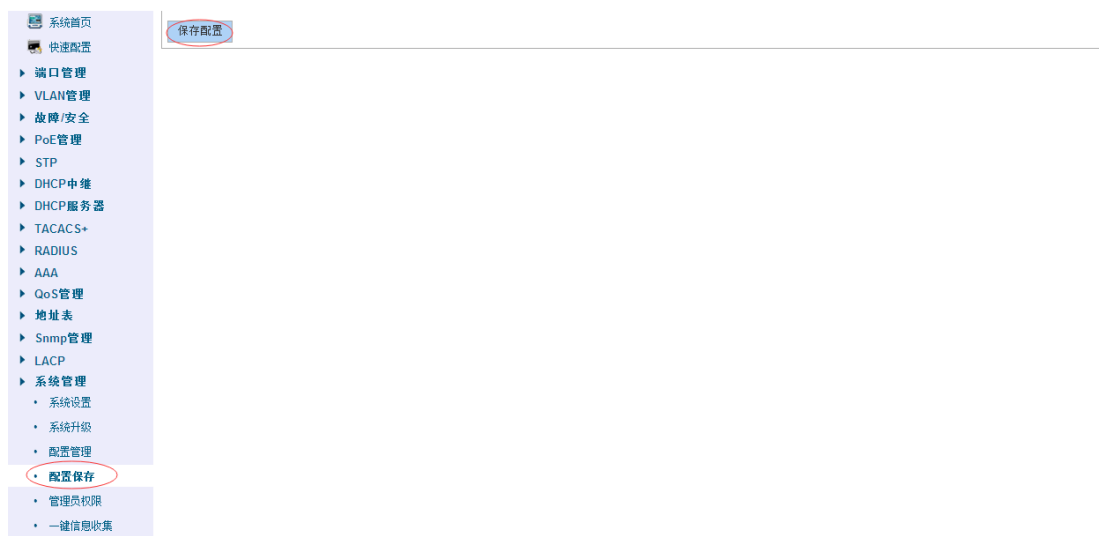
【配置举例】

如：恢复出厂配置前可先导出当前配置。



4.16.4 配置保存

在导航栏选择“系统管理>配置保存”，可保存当前配置。如下图：



【使用说明】

保存系统配置，将覆盖原有配置。如果当前系统有有用的配置，可先备份当前配置后再保存系统配置。

【配置举例】

如：点击“保存配置”按钮。



4.16.5 管理员权限

在导航栏选择“系统管理>管理员权限”，可配置普通用户。如下图：



【使用说明】

本页面只有超级管理员 admin 可以访问，用于管理用户和访客。用户可登录 Web 管理系统对设备进行日常维护。除了 admin 和 user，最多可添加 5 个用户。普通用户只可访问查

看系统首页信息。

【配置举例】

如：

管理员权限

密码类型: 密文密码

用户名: 1234

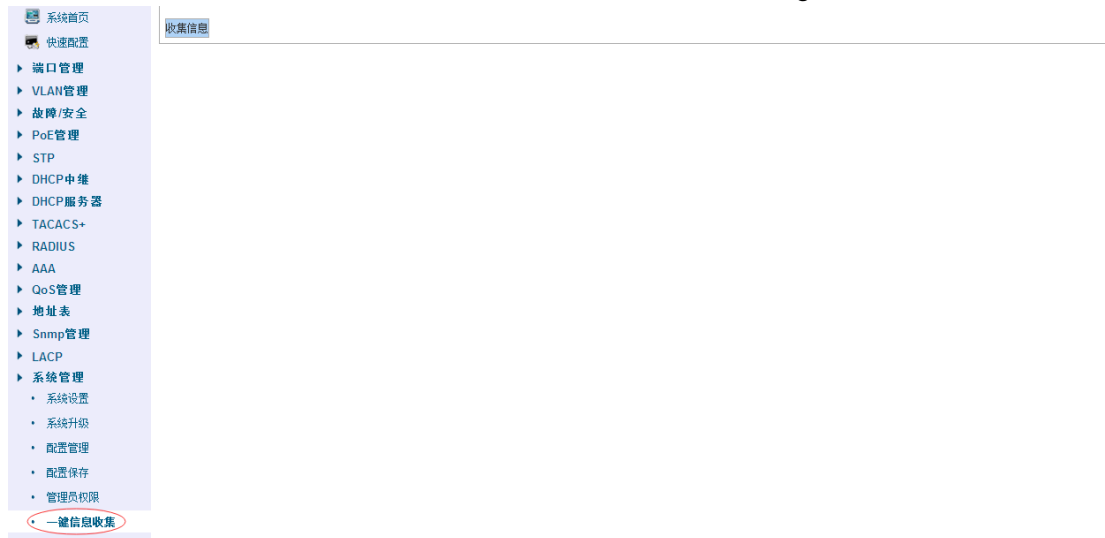
新密码: ●●●●

确认密码: ●●●●

添加用户

4.16.6 一键信息收集

在导航栏选择“系统管理>一键信息收集”，可收集到系统 debug 信息。如下图：



【使用说明】

收集系统有用信息，可能会花一段时间。

【配置举例】

如：点击“收集信息”按钮。



附录：产品规格

硬件规格		
支持的标准和协议	IEEE802.3i、IEEE802.3u、IEEE802.3ab、IEEE802.3x、IEEE802.3z、 IEEE802.3at、IEEE802.3af、IEEE802.1q、IEEE802.1p	
端口	8 个 10/100/1000Mbps 自适应 RJ45 端口 (Auto MDI/MDIX) 2 个 1000Mbps SFP 接口 1 个 Console 口	
网络媒介	10Base-T: 3 类或 3 类以上 UTP 100Base-TX: 5 类 UTP 1000Base-T: 超 5 类 UTP 1000Base-SX: 62.5μm/50μm MMF(2m~550m) 1000Base-LX: 62.5μm/50μm MMF(2m~550m) Or 10μm SMF(2m~5000m)	
传输方式	存储转发	
MAC 地址容量	8K	
交换容量	20Gbps	
包转发率	14.88Mpps	
包缓存	4.1Mbit	
巨型帧	9216Bytes	
PoE 接口 (RJ45)	8 个符合 IEEE802.3at/af 标准 PoE 端口	
供电引脚	1/2(+), 3/6(-)	
POE 输出功率	最大: 140W	
指示灯	每台	Power
	1-8 端口	Link/Act/Speed, PoE
	1-2 SFP	Link/Act
电源	100-240VAC, 50/60Hz, 150W	
功耗	最大(PoE 满载): 161W (220V/50Hz)	
外形尺寸 (LxWxH)	280*180*44.3mm	
使用环境	工作温度: 0°C~45°C 存储温度: -40°C~70°C 工作湿度: 10%~90% RH 不凝结 存储湿度: 5%~90% RH 不凝结	

Web:<http://www.sundray.com> Tel:400-878-3389

Table of Contents

Chapter 1 Product Introduction	1
1.1 Product Overview	1
1.2 Features	1
1.3 External Component Description	1
1.3.1 Front Panel.....	1
1.3.2 Rear Panel	3
1.4 Package Contents	4
Chapter 2 Installing and Connecting the Switch.....	5
2.1 Installation	5
2.1.1 Desktop Installation.....	5
2.1.2 Rack-mountable Installation in 19-inch Cabinet	5
2.1.3 Power on the Switch	6
2.2 Connect Computer (NIC) to the Switch.....	6
2.3 Switch connection to the PD	6
Chapter 3 How to Login the Switch.....	8
3.1 Switch to End Node	8
3.2 How to Login the Switch	8
Chapter 4 Switch Configuration	10
4.1 Quickly set	10
4.2 PORT.....	12
4.2.1 Basic config.....	13
4.2.2 Port Aggregation	14
4.2.3 Port Mirroring	15
4.2.4 Port Limit	16
4.2.5 Storm control	17
4.2.6 Port isolation	18
4.2.7 Port information.....	19
4.3 VLAN	19
4.3.1 VLAN config	20
4.3.2 Trunk-port setting	21
4.3.3 Hybrid-port setting.....	22
4.4 Fault/Safety	23
4.4.1 Anti Attack.....	24
4.4.1.1 DHCP.....	24
4.4.1.2 DOS	26
4.4.1.3 IP source Guard.....	26
4.4.1.4 IP/Mac/Port	27

4.4.2 Channel detection	28
4.4.2.1 Ping.....	28
4.4.2.2 Tracert.....	29
4.4.2.3 Cable Test.....	29
4.4.3 ACL.....	30
4.4.4 802.1x.....	31
4.5 POE	32
4.5.1 POE Config	33
4.5.1.1 Management	33
4.5.1.2 Temperature distribution.....	34
4.5.2 POE Port Config.....	34
4.5.3 POE Delay Config.....	35
4.6 STP.....	37
4.6.1 MSTP Region	37
4.6.2 STP Bridge	38
4.7 DHCP RELAY	39
4.7.1 DHCP Relay	39
4.7.2 Option82.....	40
4.8 DHCP Server	41
4.8.1 Enable Config.....	42
4.8.2 Pool Config.....	42
4.8.3 Option Config	43
4.8.4 Bind Config.....	44
4.8.5 Gateway Config.....	44
4.8.6 DNS Config	45
4.9 TACACS+	46
4.10 RADIUS	47
4.10.1 Radius General Config.....	47
4.10.2 Radius Server Config.....	48
4.11 AAA	48
4.11.1 Enable Config.....	49
4.11.2 Region Config.....	49
4.11.3 Server Config.....	50
4.11.4 AAA Authentication	51
4.11.4.1 Login Authentication	52
4.11.4.2 Enable Authentication.....	53
4.11.4.3 Dot1x Authentication	54
4.12 QoS	56
4.12.1 Queue Config.....	56
4.12.2 Mapping the queue	57
4.12.2.1 COS Queue Map.....	57
4.12.2.2 DSCP COS Map	58
4.12.2.3 Port COS Map.....	58
4.13 Address table	60

4.13.1 Mac Management	60
4.13.2 Mac study and aging	61
4.13.3 Mac address filtering	62
4.14 SNMP	63
4.14.1 Snmp config	63
4.14.1.1 Snmp config	63
4.14.1.2 Community config	64
4.14.1.3 View Config	65
4.14.1.4 Group Config	65
4.14.1.5 User config	66
4.14.1.6 Trap	67
4.14.2 Rmon Config	68
4.14.2.1 Statistics Group	68
4.14.2.2 History Group	69
4.14.2.3 Event Group	70
4.14.2.4 Alarm Group	71
4.15 LACP	72
4.15.1 LACP Setting	73
4.15.2 LACP Display	74
4.16 SYSTEM	74
4.16.1 System Config	75
4.16.1.1 System settings	75
4.16.1.2 System restart	77
4.16.1.3 Password change	77
4.16.1.4 EEE Enable	78
4.16.1.5 SSH login	79
4.16.1.6 Telnet login	80
4.16.1.7 System log	80
4.16.2 System Upgrade	81
4.16.3 Config Management	82
4.16.3.1 Current configuration	82
4.16.3.2 Configuration backup	84
4.16.3.3 Restore factory configuration	84
4.16.4 Config Save	84
4.16.5 Administrator Privileges	85
4.16.6 Info Collect	86
Appendix: Technical Specifications	87

Chapter 1 Product Introduction

Congratulations on your purchasing of the PoE Web Smart Ethernet Switch. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

1.1 Product Overview

The 8-port + 2SFP 10/100/1000Mbps PoE Web Smart Ethernet Switch provides the seamless network connection. It integrates 10/100/1000Mbps Ethernet network capabilities. These PoE ports can automatically detect and supply power with those IEEE 802.3at compliant Powered Devices (PDs). In this situation, the electrical power is transmitted along with data in one single cable allowing you to expand your network where there are no power lines or outlets, where you wish to fix devices such as APs, IP Cameras or IP Phones, etc.

The Web Smart Ethernet Switch, and can be configured by web based interface. Including administrator, port management, VLAN setting, each port statistics, trunking setting, QoS setting, security filter, configuration/ backup/recovery, log out, and so on.

1.2 Features

- Complies with IEEE802.3i,IEEE802.3u,IEEE802.3ab,IEEE802.3x,IEEE802.3z, IEEE802.1q ,IEEE802.1p standards.
- 8 x 10/100/1000Mbps Auto-Negotiation RJ45 ports supporting Auto-MDI/MDIX.
- Supports PoE power up to 30W for each PoE port.
- Supports All power up to 140W.
- Support the Console port management.
- Supports PoE IEEE802.3at compliant PDs.
- Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode.
- 8K entry MAC address table of the Switch with auto-learning and auto-aging.
- Supports WEB management interface.
- LED indicators for monitoring power, link, activity and speed.
- Internal power adapter supply.

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of 8 x 10/100/1000Mbps RJ-45 ports, 1x Console port,2 x SFP ports,1 x Reset button and a series of LED indicators as shown as below.



Figure 1 - Front Panel

10/100/1000Mbps RJ-45 ports (1~8):

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.

Console port (Console):

Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

SFP ports (SFP1, SFP2):

Designed to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Reset button (Reset):

Keep the device powered on and push a paper clip into the hole.

Press down the button for 2 seconds to reboot the Switch, Press down the button for 5 seconds to restore the Switch to its original factory default settings.

LED indicators:

The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.

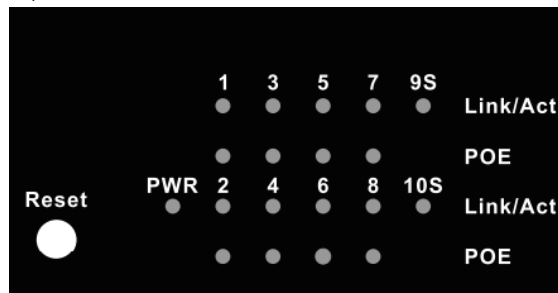


Figure 2 - LED Indicators

The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
PWR	Green	On	Power On
		Off	Power Off
Link/Act/ (1-8)	10/100M: Orange	On	A device is connected to the port
		Off	A device is disconnected to the port
	1000M: Green	Flashing	Sending or receiving data
PoE	Yellow	On	A Powered Device is connected to the port, which supply power successfully.
		Off	No PD is connected to the corresponding port, or no power is supplied according to the power limits of the port.
		Flashing	The PoE power circuit may be in short or the power current may be overloaded.
Link/Act/ SFP(9S-10S)	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

1.3.2 Rear Panel

The rear panel of the Switch contains AC power connector and one marker shown as below.



Figure 3 - Rear Panel

AC Power Connector:

Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.

Grounding Terminal:

Located on the right side of the power supply connector, use wire grounded to prevent

electric shock.

Fan heat-sink :

The fan heat sink is located on the midst of the switch. It is used for fan ventilation. Please do not block.

1.4 Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One PoE Web Smart Ethernet Switch.
- Four rubber feet, two mounting ears and eights screws.
- One AC power cord.
- One User Manual.

Chapter 2 Installing and Connecting the Switch

This part describes how to install your PoE Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1 Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

2.1.1 Desktop Installation

Sometimes users are not equipped with the 19-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

2.1.2 Rack-mountable Installation in 19-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

- a. attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.



Figure 4 - Bracket Installation

- b. use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.



Figure 5 - Rack Installation

2.1.3 Power on the Switch

The Switch is powered on by the AC 100-240V 50/60Hz internal high-performance power supply. Please follow the next tips to connect:

AC Electrical Outlet:

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

2.2 Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK/ACT/Speed status indicator lights corresponding ports of the Switch.

2.3 Switch connection to the PD

1-8 ports of the Switch have PoE power supply function, the maximum output power up to 30W each port, it can make PD devices, such as internet phone, network camera, wireless

access point work. You only need to connect the Switch PoE port directly connected to the PD port by network cable.

Chapter 3 How to Login the Switch

3.1 Switch to End Node

Use standard Cat.5/5e Ethernet cable (UTP/STP) to connect the Switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which is connected.

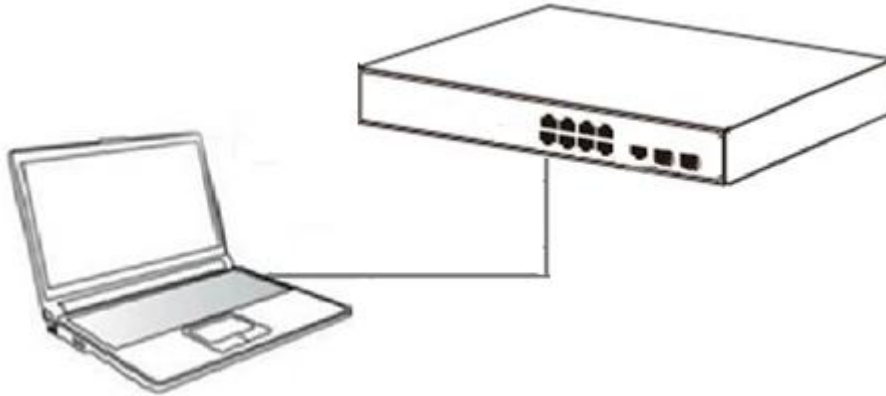


Figure 6 - PC Connect

Please refer to the **LED Indicators**. The LINK/ACT/Speed LEDs for each port lights on when the link is available.

3.2 How to Login the Switch

As the Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Switch. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.0.1
Default user name	admin
Default password	admin

You can log on to the configuration window of the Switch through following steps:

1. Connect the Switch with the computer NIC interface.
2. Power on the Switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.0.xxx ("xxx" ranges 2~254), for example, 192.168.0.100.
4. Open the browser, and enter <http://192.168.0.1> and then press "Enter". The Switch login window appears, as shown below.

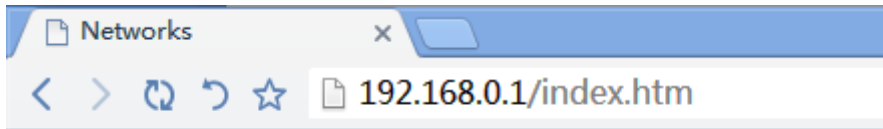
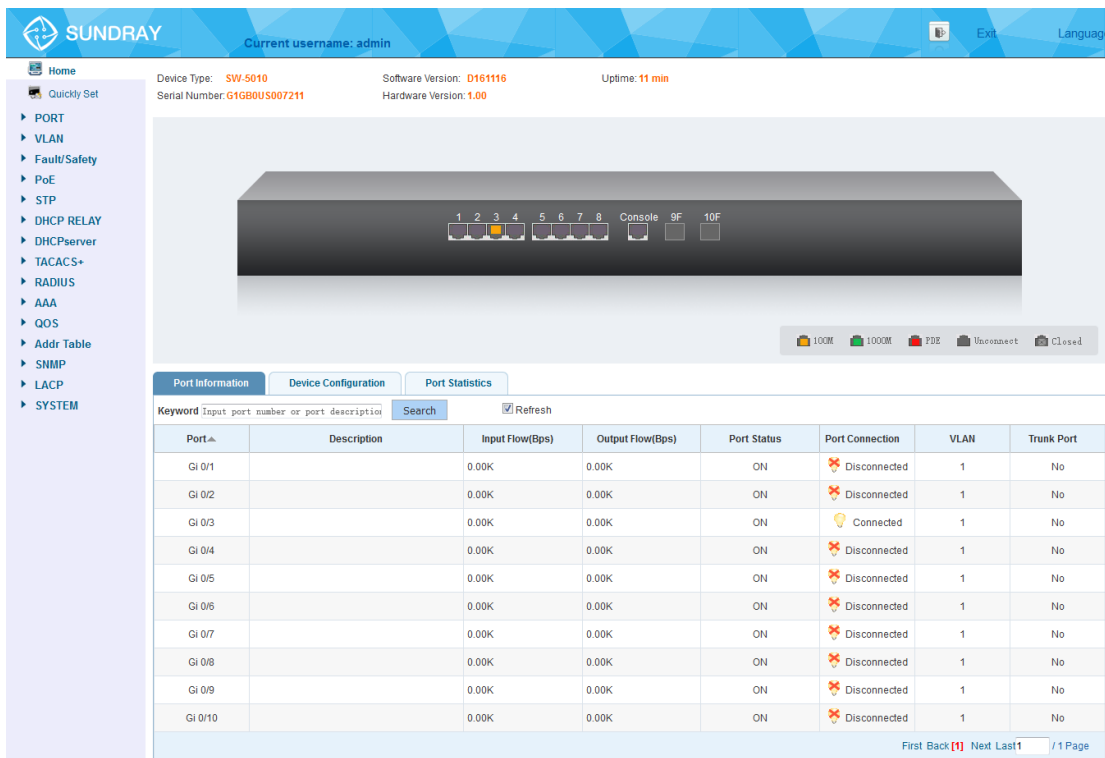


Figure 7- Login Windows

5. Switching language to english .Enter the Username and Password (The factory default Username is **admin** and Password is **admin**), and then click “login” to log in to the Switch configuration window as below.



Chapter 4 Switch Configuration

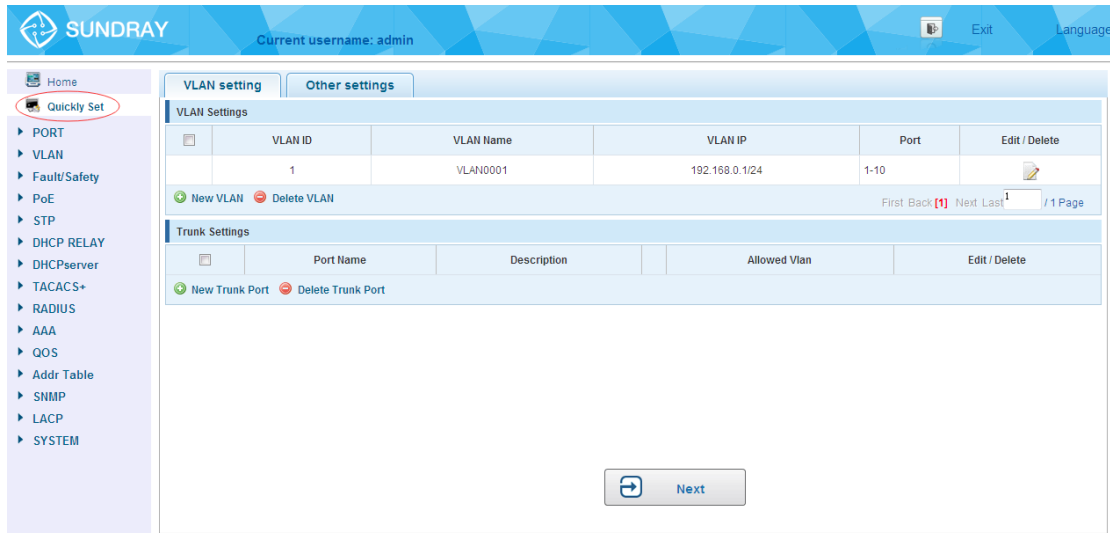
The Web Smart Ethernet Switch Managed switch software provides rich layer two functionality for switches in your networks. This chapter describes how to use Web-based management interface (Web UI) to this Switch configure managed switch software features. In the Web UI, the left column shows the configuration menu. You can find the information for switch system, software version on the top of the page. The middle shows the Switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.

The screenshot displays the SUNDAY Web UI. At the top, the current username is 'admin'. The device information includes: Device Type: SW-5010, Software Version: D161116, Uptime: 11 min, Serial Number: G1GB0US007211, and Hardware Version: 1.00. The central panel shows a 3D rendering of the switch with 10 ports (1-8, Console, 9F, 10F) and a toolbar with icons for 100M, 1000M, PoE, Unconnect, and Closed. Below the switch image is a 'Port Information' tab with a search bar and a 'Refresh' checkbox. The table below shows the status of 10 ports (Gi 0/1 to Gi 0/10).

Port	Description	Input Flow(Bps)	Output Flow(Bps)	Port Status	Port Connection	VLAN	Trunk Port
Gi 0/1		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/2		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/3		0.00K	0.00K	ON	Connected	1	No
Gi 0/4		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/5		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/6		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/7		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/8		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/9		0.00K	0.00K	ON	Disconnected	1	No
Gi 0/10		0.00K	0.00K	ON	Disconnected	1	No

4.1 Quickly set

Select “**Quickly Set**” in the navigation bar, you can create a VLAN, add the port in the VLAN, set the basic information and modify the Switch login password. the following picture:



【Parameter Description】

Parameter	Description
VLAN ID	VLAN number, 8GE default VLAN 1
VLAN name	VLAN mark
Manage IP	Manage the IP address of the VLAN
device name	Switch name
Manage VLAN	Switches management in use of the VLAN

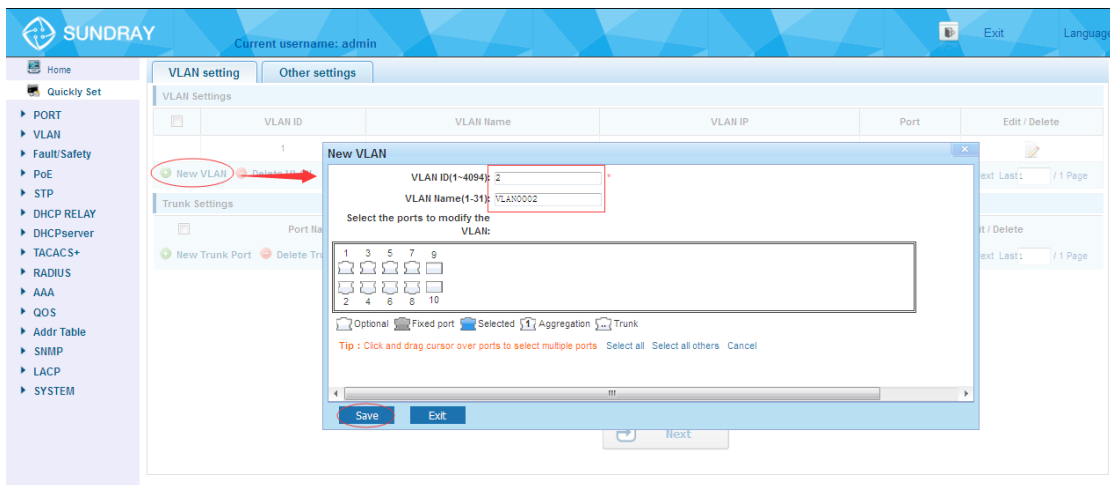
【Instructions】

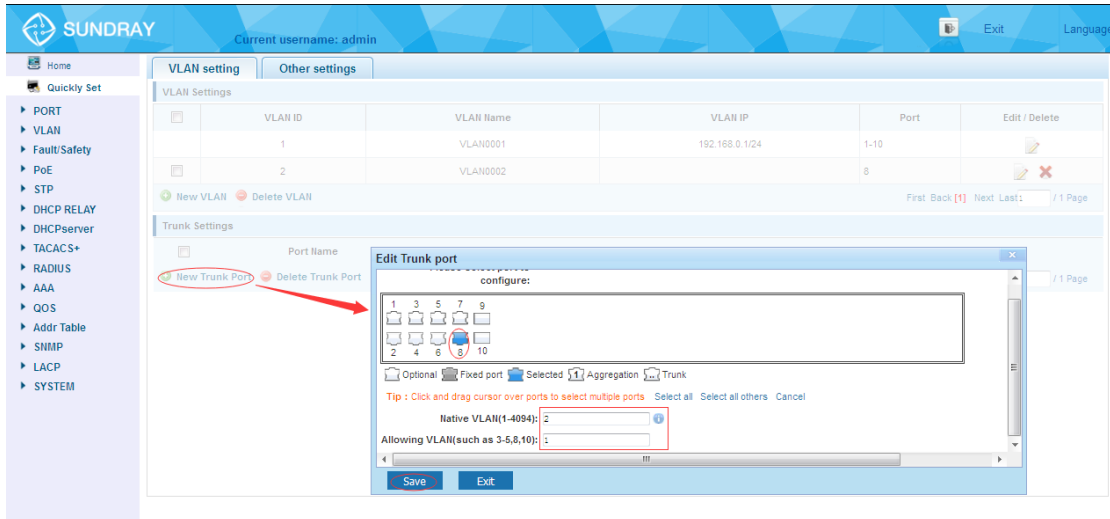
Native VLAN: as a Trunk, this port must belong to a Native VLAN. The so-called Native VLAN, refers to UNTAG send/receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1 Q VLAN ID is the Native VLAN. At the same time, send belong to Native VLAN frame on the Trunk, must adopt UNTAG way.

Allowed VLAN list: a Trunk can transport the equipment support by default all the VLAN traffic (1-4094). But also can by setting the permission VLAN Trunk at the mouth of the list to limit the flow of some VLAN can't through the Trunk.

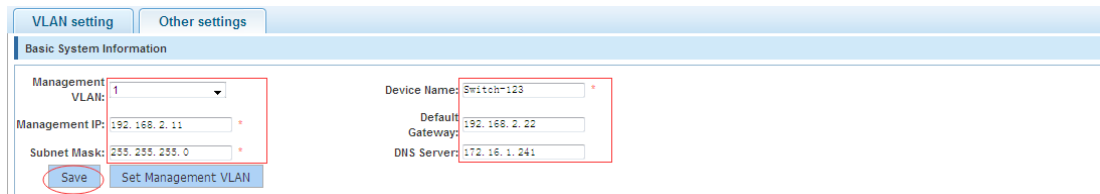
【Configuration example】

1) VLAN setting: Such as create VLAN 2, Sets the port 8 to Trunk, Native VLAN 2.

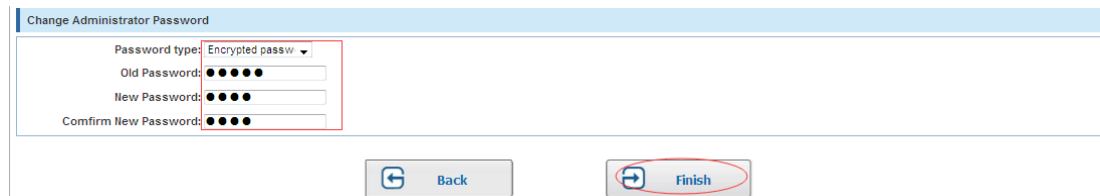




- 2) Click “**next step**” button, into other settings, such as manage ip address set as 192.168.2.11, device name set as switch-123, default gateway with the dns server set as 172.16.1.241.



- 3) Use 192.168.2.11 to log in, set a new password for 1234.



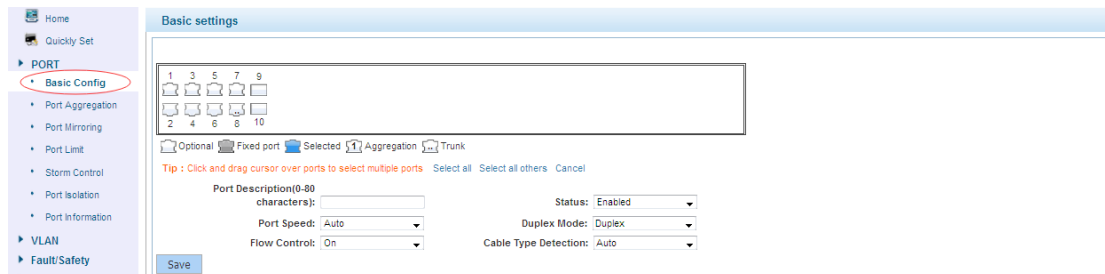
4.2 PORT

Selecting “PORT” in the navigation bar, you may conduct **Basic Config**, **Port Aggregation**, **Port Mirroring**, **Port Limit**, **Storm Control**, **Port Isolation** and **Port Information**.



4.2.1 Basic config

Selecting “**PORT>Basic Config**” in the navigation bar, you can configure Port description, Port speed, Port status, Working mode, Flow control, Cross line order configuration, the following picture:



【Parameter Description】

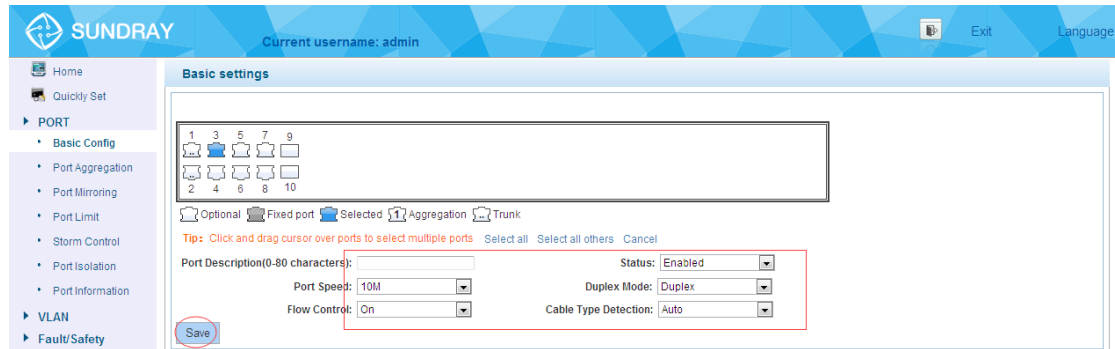
Parameter	Description
Port	Select the current configuration port number
Port status	Choose whether to close link port
Flow control	Whether open flow control
Port speed	Can choose the following kinds: Auto 10 M 100 M 1000 M
Working mode	Can choose the following kinds: Auto Duplex Half duplex
Port described	The port is described
Cable Type Detection	Can choose the following kinds: Auto MDI MDIX

【Instructions】

Open to traffic control will be auto negotiation closed, auto-negotiation is to set the port speed and working mode; the port rate set more than the actual rate of port, port will drop.

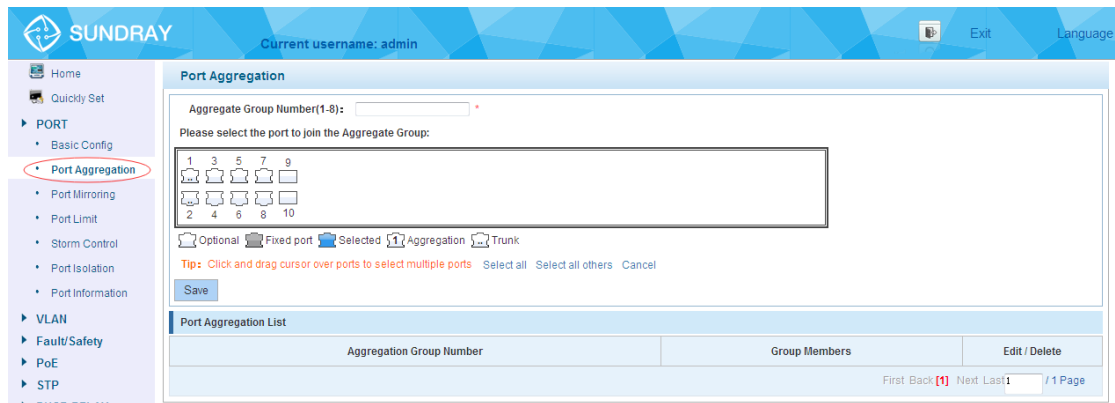
【Configuration example】

For example: Setting the Port speed as ‘10M’, Working mode as ‘Duplex’, Flow control as ‘On’, Cable Type Detection and Port status as ‘Auto’.



4.2.2 Port Aggregation

In the navigation bar to select “**PORT>Port Aggregation**”. In order to expand the port bandwidth or achieve the bandwidth of the redundancy backup, the following picture:



【Parameter Description】

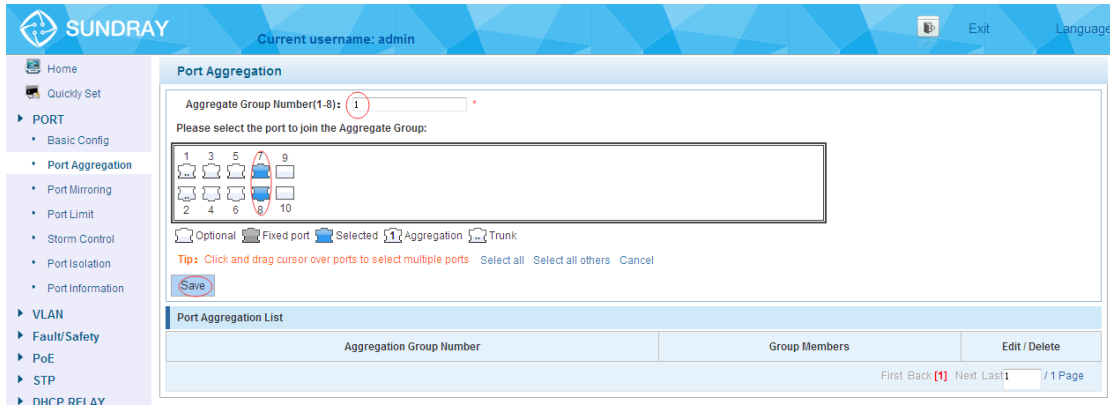
Parameter	Description
Aggregation port	8GE Switch can be set up 8 link trunk group, group_1 to group_8
Member port	For each of the members of the group and add your own port, and with members of other groups

【Instructions】

Open the port of the ARP check function, the port of the important device ARP, the port of the VLAN MAC function, and the monitor port in the port image can not be added.

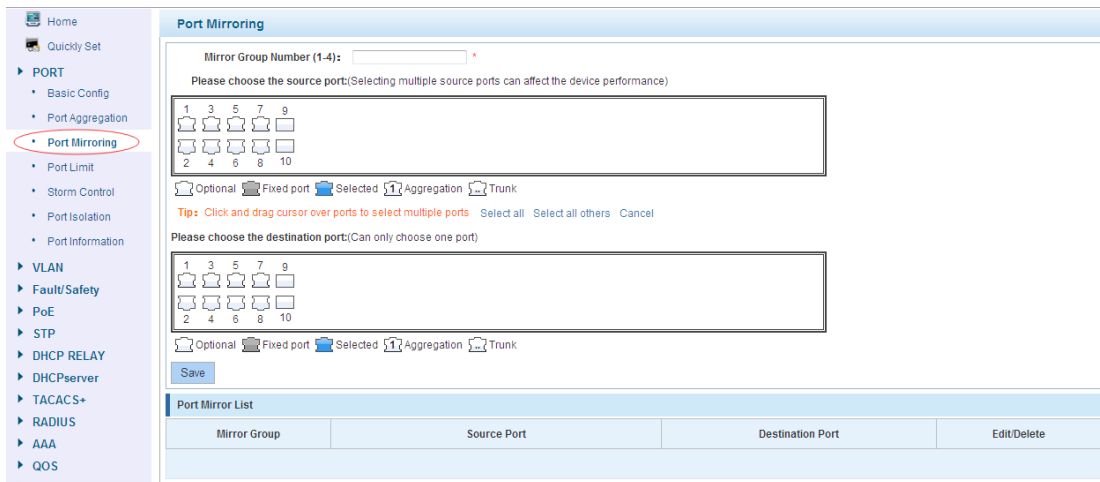
【Configuration example】

Such as: set the port as '7, 8', for aggregation port 1, lets this aggregation port 1 connected to other switch aggregation port 1 to build switch links .



4.2.3 Port Mirroring

In the navigation bar to select “**PORT>Port Mirroring**”, Open port mirror feature, All the packets on the source port are copied and forwarded to the destination port, destination port is usually connected to a packet analyzer to analyze the source port, multiple ports can be mirrored to a destination port, the following picture:



【Parameter Description】

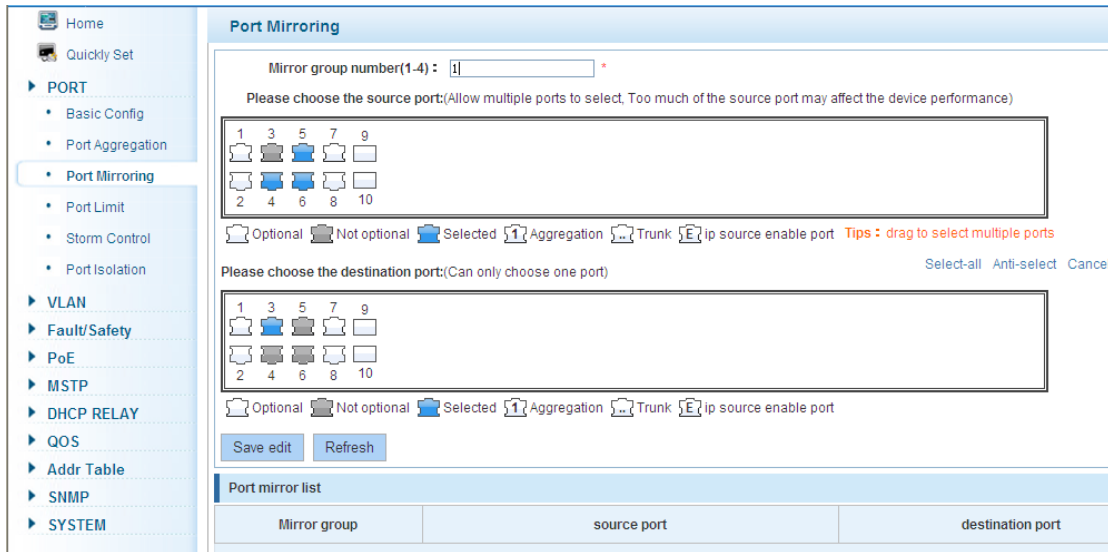
Parameter	Description
Source port	To monitor the port in and out of flow
Destination port	Set destination port, All packets on the source port are copied and forwarded to the destination port
Mirror group	Range: 1-4

【Instructions】

The port of the aggregating port can not be used as a destination port and the source port, destination port and source port can not be the same.

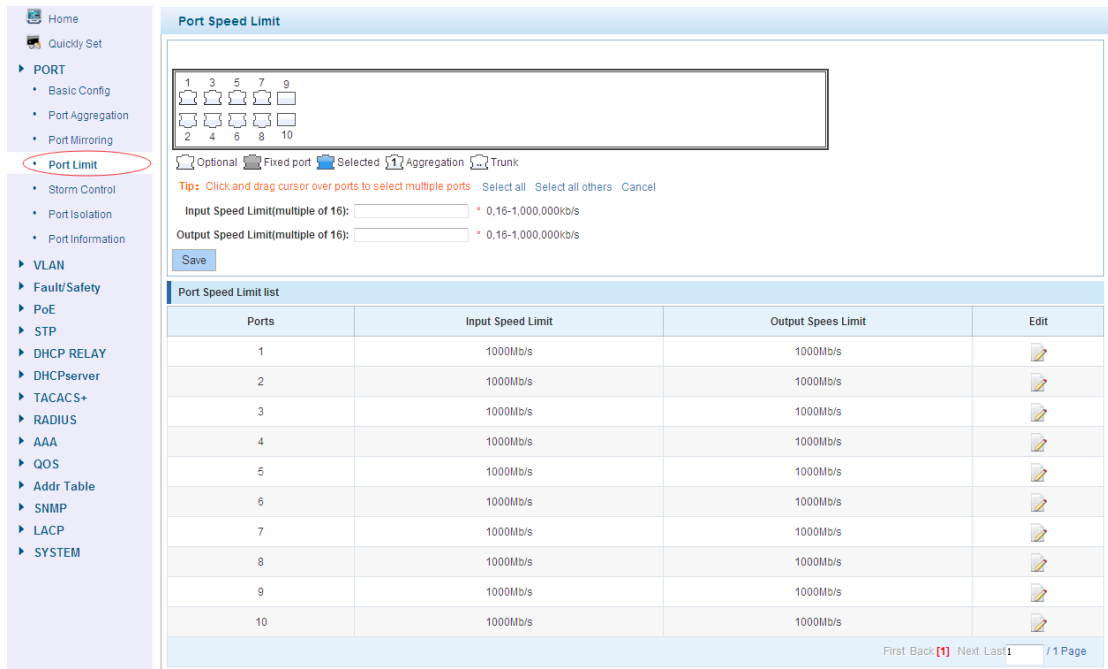
【Configuration example】

Such as: set a mirror group for port 3 regulatory port 4,5,6 on and out flow conditions.



4.2.4 Port Limit

In the navigation bar to select “**PORT>Port Limit**”. Limiting the speed of output and input rate of the ports, the following picture:



【Parameter Description】

Parameter	Description
Input speed limit	Set port input speed
Output speed limit	Set port output speed

【Instructions】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s. That is, the theoretical rate of 1M

bandwidth is 125 KB/s.

【Configuration example】

Such as: the port 5 input rate is set to 6400 KB/s, the output rate is set to 3200 KB/s.

Ports	Input Speed Limit	Output Speeds Limit	Edit
1	1000Mb/s	1000Mb/s	
2	1000Mb/s	1000Mb/s	
3	1000Mb/s	1000Mb/s	
4	1000Mb/s	1000Mb/s	
5	6.4Mb/s	3.2Mb/s	

4.2.5 Storm control

In the navigation bar to select “**PORT>Storm Control**”, to port storm control config, the following figure:

【Parameter Description】

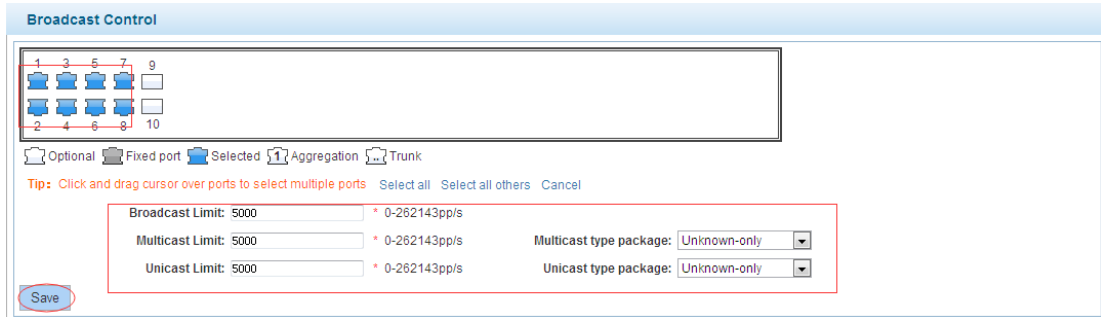
Parameter	Description
Broadcast suppression value	Storm suppression value of the broadcast packets
Multicast suppression value	Storm suppression value of the multicast packets
Unicast suppression value	Storm suppression value of the unicast packets

【Instructions】

1 Mbit/s = 1000 Kbit/s = 1000 / 8 KB/s = 125 KB/s. That is, the theoretical rate of 1M bandwidth is 125 KB/s.

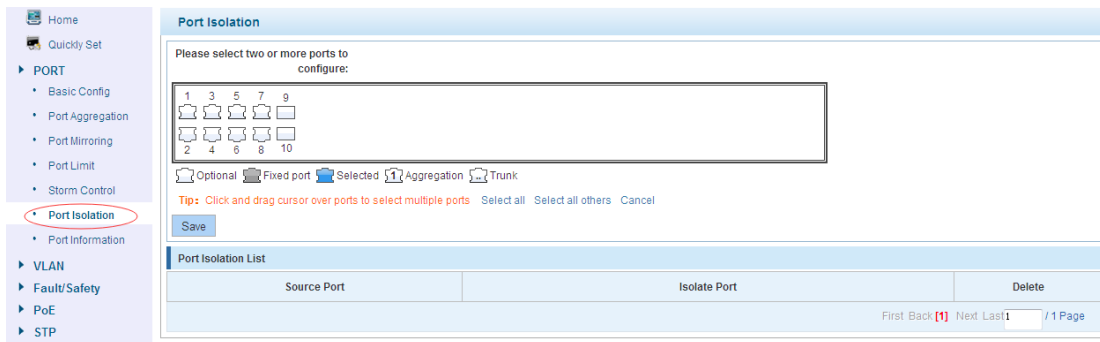
【Configuration example】

Such as: should be forwarded to the port 1-8 of all kinds of packet forwarding rate is 5000 KB/s.



4.2.6 Port isolation

In the navigation bar to select “**PORT>port isolation**”, the following picture:



【Parameter Description】

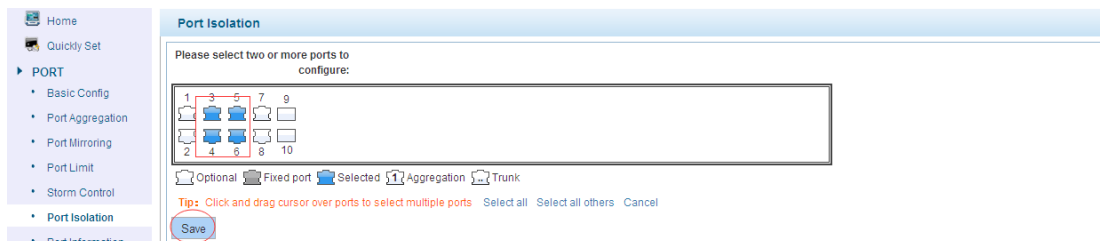
Parameter	Description
Source port	Choose a port, to configure the isolated port
Isolated port	Port will be isolated

【Instructions】

Open port isolation function, All packets on the source port are not forwarded from the isolated port, the selected ports are isolated. Ports that have been added to the aggregate port aren't also capable of being a destination port and source port, destination port and source port cannot be the same.

【Configuration example】

Such as: the port 3, 4, 5, and 6 ports isolated.



Port isolation list		
Source port	Isolate port	Operation
3	4 5 6	✘
4	3 5 6	✘
5	3 4 6	✘
6	3 4 5	✘

first page prev page **1** next page last page / 1 page

4.2.7 Port information

In the navigation bar to select “**PORT>Port information**”, the following picture:

Port	Description	Input Flow(Bps)	Output Flow(Bps)	Port Status	Port Connection	VLAN	Trunk Port
Gi 0/1		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/2		23.20M	40.03M	ON	💡 Connected	1	No
Gi 0/3		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/4		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/5		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/6		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/7		829.09K	271.39K	ON	💡 Connected	1	No
Gi 0/8		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/9		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/10		0.00K	0.00K	ON	✘ Disconnecte d	1	No

First Back **1** Next Last / 1 Page

【Parameter Description】

Parameter	Description
Input Flow	Port input flow statistics
Output Flow	Port output flow statistics

【Instructions】

Show port input and output streams information port connection status, belongs to VLAN.

【Configuration example】

Enter port number 1 for the query.

Port	Description	Input Flow(Bps)	Output Flow(Bps)	Port Status	Port Connection	VLAN	Trunk Port
Gi 0/10		0.00K	0.00K	ON	✘ Disconnecte d	1	No
Gi 0/1		0.00K	0.00K	ON	✘ Disconnecte d	1	No

First Back **1** Next Last / 1 Page

4.3 VLAN

In the navigation bar to select “**VLAN**”. You can manage the VLAN config, Trunk Settings and Hybrid Settings, the following picture:

VLAN setting	Trunk-port setting	Hybrid-port setting
VLAN list		
<input type="checkbox"/>	VLAN ID	VLAN name
	1	VLAN0001
+ New VLAN - delete selected VLAN		

4.3.1 VLAN config

In the navigation bar to select “**VLAN config**”, Vlan can be created and set the port to the VLAN (port default state for the access mode), the following picture:

The screenshot shows a web interface for VLAN configuration. On the left is a navigation menu with options: Home, Quickly Set, PORT, VLAN, Vlan Config (highlighted), Fault/Safety, PoE, and STP. The main content area has tabs for VLAN Settings (highlighted), Trunk Port Settings, and Hybrid Port Settings. Below the tabs is a table titled 'VLAN IDs' with columns: VLAN ID, VLAN Name, VLAN IP, Port, and Edit / Delete. The table contains one entry: VLAN ID 1, VLAN Name VLAN0001, VLAN IP 192.168.0.1/24, and Port 1-10. Below the table are buttons for 'New VLAN' and 'Delete VLAN', and a pagination control showing '1 / 1 Page'.

【Parameter Description】

Parameter	Description
VLAN ID	VLAN number, 8GE default VLAN 1
VLAN name	VLAN mark
VLAN IP address	Manage switch ip address

【Instructions】

Management VLAN, the default VLAN cannot be deleted. Add ports as access port, port access mode can only be a member of the VLAN.

【Configuration example】

Such as: connecting the same switches, pc1, pc2 couldn't ping each other, because one of the PC connection port belongs to a VLAN 2.

4.3.2 Trunk-port setting

In the navigation bar to select “**VLAN config>Trunk-port setting**”, can set port as Trunk Port, the following picture:

【Parameter Description】

Parameter	Description
Native VLAN	Only set one
Allowing vlan	Can set up multiple

【Instructions】

Native VLAN: As a Trunk, the port will belong to a Native VLAN. The so-called Native VLAN, is refers to UNTAG send or receive a message on the interface, is considered belongs to the VLAN. Obviously, the interface of the default VLAN ID (PVID) in the IEEE 802.1Q VLAN ID is the Native VLAN. At the same time, send belong to Native VLAN frame on the Trunk, must adopt UNTAG way.

Allowed VLAN list: A Trunk can transport the equipment support by default all the VLAN traffic (1-4094). But, also can by setting the permission VLAN Trunk at the mouth of the list to limit the flow of some VLAN can't through the Trunk.

【Configuration example】

Such as:PVID=VLAN2

PC1:192.168.2.122, port 8, access VLAN2

PC2:192.168.2.123, port 7, Trunk allowed VLAN 1-2

PC3:192.168.2.124, port 6, access VLAN1 (The default port belongs to VLAN1)

Can let the PC2 PING PC1, cannot PING PC3

VLAN IDs					
	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
<input type="checkbox"/>	1	VLAN0001	192.168.0.1/24	1-7,9-10	
<input type="checkbox"/>	2	VLAN0002		8	

New VLAN Delete VLAN

First Back [1] Next Last 1 / 1 Page

VLAN Settings Trunk Port Settings Hybrid Port Settings

Trunk port list

	Port	Port description	Native VLAN	Allowing VLAN	Operation
	New Trunk port				
	Delete selected Trunk port				

First Back [1] Next Last 1 / 1 Page

New Trunk port

Port selection grid:

1	3	5	9
2	4	6	10

Optional Fixed port Selected Aggregation Trunk

Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel

Native Vlan (1-4094): 2

Allowing VLAN(such as 3, 5,8,10): 1-2

Save settings Cancel

4.3.3 Hybrid-port setting

In the navigation bar to select “**VLAN config>Hybrid-port setting**”, Can set the port to take the tag and without the tag, the following picture:

VLAN Settings Trunk Port Settings Hybrid Port Settings

Hybrid Port List

	Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete
	New Hybrid Port					
	Delete Selected Hybrid Port					

First Back [1] Next Last 1 / 1 Page

【Instructions】

Hybrid port to packet:

Receives a packet, judge whether there is a VLAN information: if there is no play in port PVID, exchanged and forwarding, if have, whether the Hybrid port allows the VLAN data into: if can be forwarded, or discarded (untag on port configuration is not considered, untag configuration only work when to send it a message).

Hybrid port to send packet:

1. Determine the VLAN in this port attributes (disp interface can see the port to which VLAN untag, which VLAN tag).
2. If it is untag stripping VLAN information, send again, if the tag is sent directly.

【Configuration example】

Such as: create VLAN 10, VLAN 20, set port 1 Native VLAN as 10, tagged VLAN as 10, 20, sets the Native VLAN port 2 as 20, tagged VLAN as 10, 20.

VLAN IDs					
<input type="checkbox"/>	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
<input type="checkbox"/>	1	VLAN0001	192.168.0.1/24	1-10	
<input type="checkbox"/>	10	VLAN0010			
<input type="checkbox"/>	20	VLAN0020			

VLAN Settings | Trunk Port Settings | **Hybrid Port Settings**

Hybrid Port List

<input type="checkbox"/>	Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete
<input type="checkbox"/>	New Hybrid Port					

First Back [1] Next Last 1 / 1 Page

New Hybrid Port

1

3

5

7

9

2

4

6

8

10

Optional Fixed port Selected Aggregation Trunk

Tip: Click and drag cursors over ports to select multiple ports. Select all Select all others Cancel

Native Vlan(1-4094): 10

VLAN TAG (3-5,8,10): 1

Go to VLAN's TAG (such as 3-5,8,10): 10, 20

Save Cancel

VLAN Settings | Trunk Port Settings | **Hybrid Port Settings**

Hybrid Port List

<input type="checkbox"/>	Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete
<input type="checkbox"/>	1		10	1	10,20	
<input type="checkbox"/>	2		20	1	10,20	

New Hybrid Port Delete Selected Hybrid Port First Back [1] Next Last 1 / 1 Page

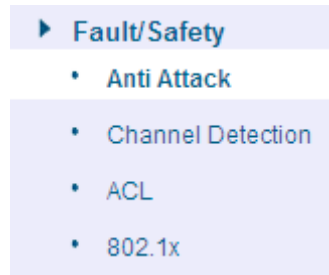
This system e0/1 and the receive system e0/2 PC can be exchanged, but when each data taken from a VLAN is different.

Data from the pc1, by inter0/1 pvid VLAN10 encapsulation VLAN10 labeled into switches, switch found system e0/2 allows 10 data through the VLAN, so the data is forwarded to the system e0/2, because the system e0/2 VLAN is untagged 10, then switches at this time to remove packet VLAN10 tag, in the form of ordinary package sent to pc2, pc1 -> p2 is VLAN10 walking at this time.

Again to analyze pc2 gave pc1 package process, data from the pc2, by inter0/2 pvid VLAN20 encapsulation VLAN20 labeled into switch, switch found system e0/1 allows VLAN by 20 data, so the data is forwarded to the system e0/1, because the system e0/1 on the VLAN is untagged 20, then switches remove packets on VLAN20 tag at this time, in the form of ordinary package sent to pc1, pc2 at this time -> pc1 is VLAN 20 .

4.4 Fault/Safety

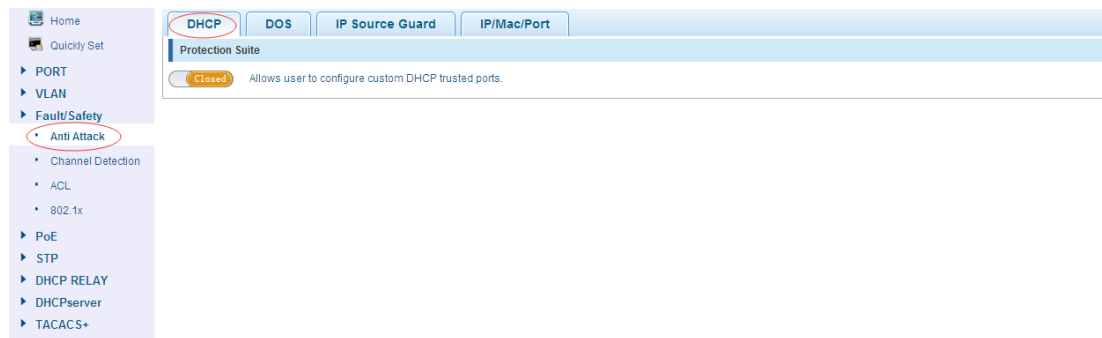
In the navigation bar to select "Fault/Safety", you can set anti attack, channle detection, ACL and 802.1x configuration.



4.4.1 Anti Attack

4.4.1.1 DHCP

In the navigation bar to select “**Fault/Safety>Anti Attack>DHCP**”, Open the DHCP anti-attack function, intercepting counterfeit DHCP server and address depletion attack packets ban kangaroo DHCP server, the following picture:



【Instructions】

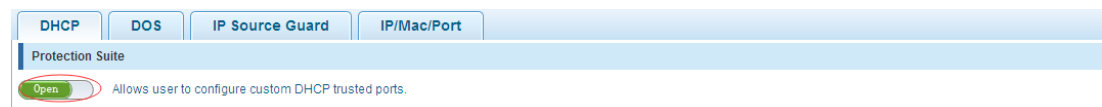
DHCP trusted port configuration, select the port as a trusted port. Prohibit DHCP for address, select the port and save, you can disable this feature for the port.

Open DHCP attack prevention function, need to set the DHCP protective vlan simultaneously, other functions to take effect.

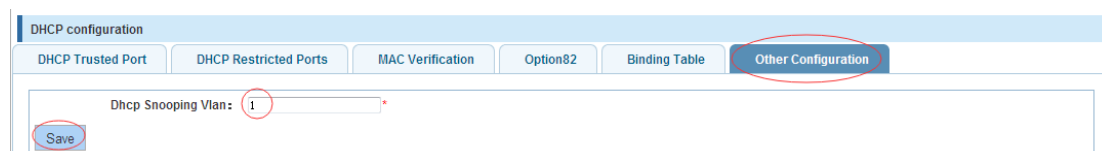
【Configuration example】

Such as:

1. DHCP snooping open.



2. Setting DHCP snooping vlan.



3. Set the connection router 8 ports for trust, then 6 port is set to the prohibit.

DHCP Trusted Port

DHCP Restricted Ports

MAC Verification

Option82

Binding Table

Other Configuration

DHCP trusted ports:

1	3	5	7	9
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Optional
 Fixed port
 Selected
 Aggregation
 Trunk

Tip: Click and drag cursor over ports to select multiple ports

Save

DHCP Trusted Port

DHCP Restricted Ports

MAC Verification

Option82

Binding Table

Other Configuration

DHCP Restricted Ports:

1	3	5	7	9
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Optional
 Fixed port
 Selected
 Aggregation
 Trunk

Tip: Click and drag cursor over ports to select multiple ports

Save

4. Verify source mac F0:DE:F1:12:98:D2,set server ip address to 192.168.2.1.

DHCP Trusted Port

DHCP Restricted Ports

MAC Verification

Option82

Binding Table

Other Configuration

MAC Verification Enable:

MAC Address: F0:DE:F1:12:98:D2 *

Save

DHCP Trusted Port

DHCP Restricted Ports

MAC Verification

Option82

Binding Table

Other Configuration

Dhcp Snooping Vlan: *

Save

Server IP Address: 192.168.0.1 *

Save

5. Set option82 information.

DHCP Trusted Port

DHCP Restricted Ports

MAC Verification

Option82

Binding Table

Other Configuration

Option82 Enable:

Client Option82 Enable:

Circuit Control

Remote Agent

IP Address

Circuit Name: 123

VLAN ID: 1

Save

DHCP Trusted Port

DHCP Restricted Ports

MAC Verification

Option82

Binding Table

Other Configuration

Option82 Enable:

Client Option82 Enable:

Circuit Control

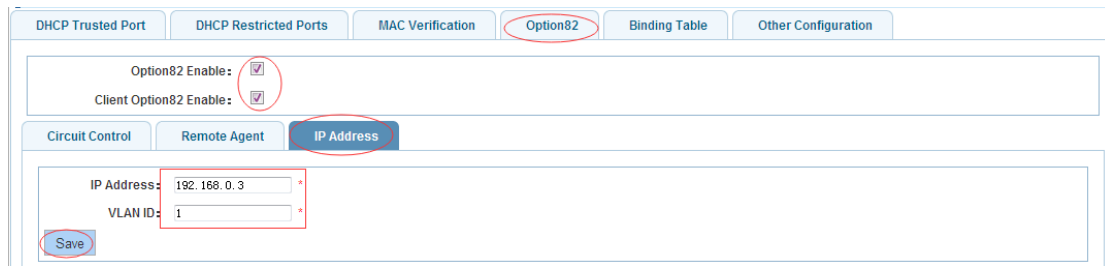
Remote Agent

IP Address

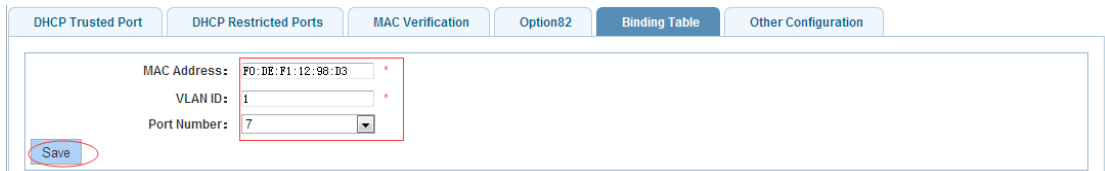
Remote Name: wety *

VLAN ID: 1 *

Save

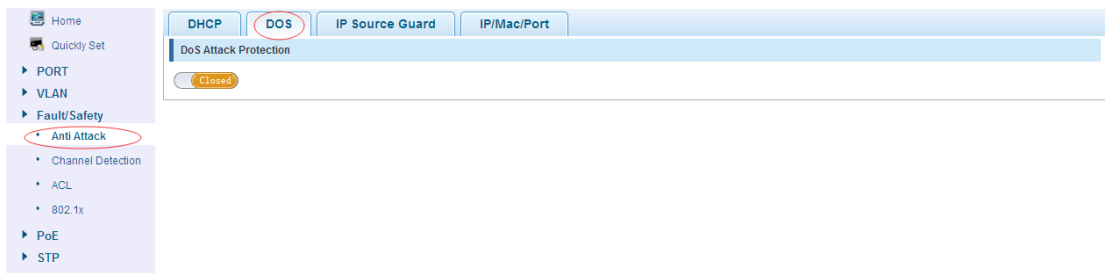


6. The port 7 for binding.



4.4.1.2 DOS

In the navigation bar to select “**Fault/Safety>Anti Attack>DOS**”, Open the anti DOS attack function, intercept Land attack packets, illegal TCP packets, to ensure that the device or the server providing normal service to legitimate users. The following picture:

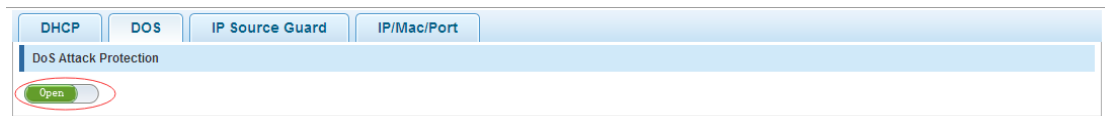


【Instructions】

Open the anti DOS attack function, intercept Land attack packets, illegal TCP packets, to ensure that the device or server to provide normal service to legitimate users.

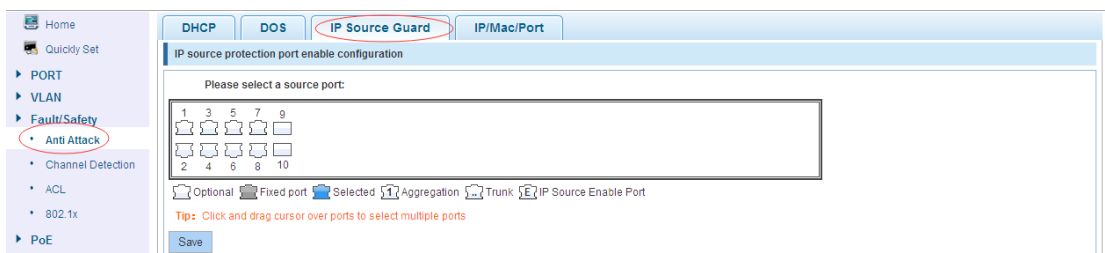
【Configuration example】

Such as:Open the Anti DOS attack function



4.4.1.3 IP source Guard

In the navigation bar to select “**Fault/Safety>Anti Attack>Ip Source Guard**”, Through the source port security is enabled, on port forwarding the packet filter control, prevent illegal message through the port, thereby limiting the illegal use of network resources, improve the safety of the port, the following picture:



【Instructions】

Add the port that is currently being used as a IP source protection enable port, the port will not be able to use.

【Configuration example】

Such as: to open source IP protection enabled port first, then to binding.

The top screenshot shows the 'IP source protection port enable configuration' page. It has tabs for DHCP, DOS, IP Source Guard, and IP/Mac/Port. Under 'IP source protection port enable configuration', there is a section 'Please select a source port:' with a grid of 10 ports (1-10). Port 3 is selected. Below the grid are options for 'Optional', 'Fixed port', 'Selected', 'Aggregation', 'Trunk', and 'IP Source Enable Port'. A tip says 'Click and drag cursor over ports to select multiple ports'. A 'Save' button is at the bottom.

The bottom screenshot shows the 'Manual IP Source Protection List' page. A 'New Security Port' button is highlighted with a red circle and an arrow pointing to a modal window. The modal window has fields for 'VLAN ID: 1', 'Source IP Address: 192.168.0.30', and 'Source MAC Address: 00:01:16:09:35:37'. It also has a port selection grid with port 3 selected and the same configuration options as the top screenshot. 'Save' and 'Exit' buttons are at the bottom of the modal.

4.4.1.4 IP/Mac/Port

In the navigation bar to select "Fault/Safety>Anti Attack>IP/Mac/Port", Automatically detect the mapping relationship of the ports based IP address, MAC address, and then achieve the function of a key binding, the following picture:

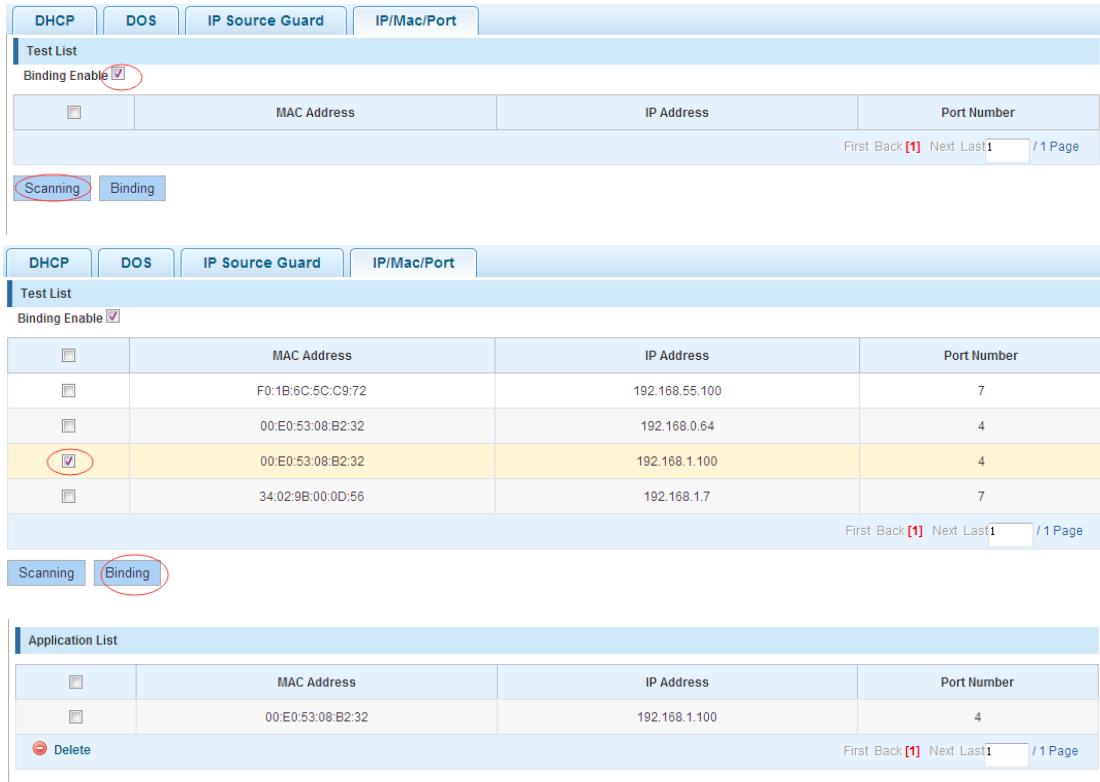
The screenshot shows the 'IP/Mac/Port' configuration page. The navigation bar includes 'Home', 'Quickly Set', 'PORT', 'VLAN', 'Fault/Safety', 'Anti Attack', 'Channel Detection', 'ACL', '802.1x', 'PoE', and 'STP'. The 'IP/Mac/Port' tab is selected. The 'Test List' section has a 'Binding Enable' checkbox. Below it is a table with columns for 'MAC Address', 'IP Address', and 'Port Number'. There are 'Scanning' and 'Binding' buttons. At the bottom, there is an 'Application List' section.

【Instructions】

A bond must be bounded before the binding to enable the switch to open, And if you want to access shall be binding and switch the IP address of the same network segment.

【Configuration example】

Such as: the binding to make first can open, must be a key bindings port 7.

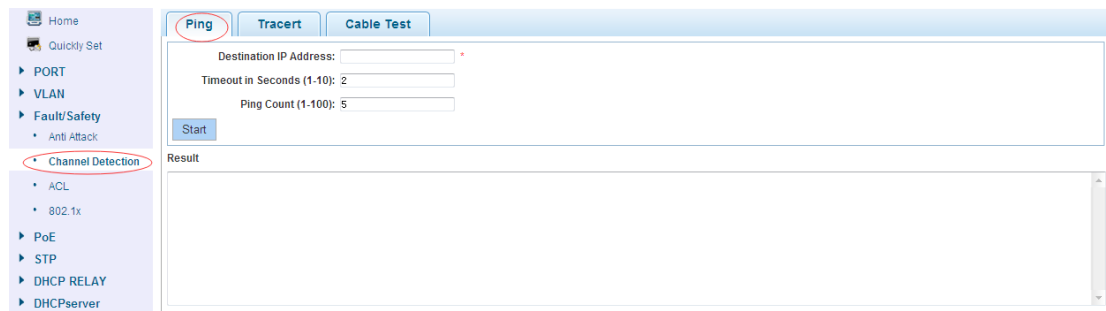


Can check the delete option.

4.4.2 Channel detection

4.4.2.1 Ping

In the navigation bar to select “**Fault/Safety>Channel Detection>Ping**”. Use ping function to test internet connect and host whether to arrive. The following picture :



【Parameter Description】

Parameter	Description
Destination IP address	Fill in the IP address of the need to detect
Timeout period	Range of 1 to 10
Repeat number	Testing number

【Instructions】

Use ping function to test internet connect and host whether to arrive.

【Configuration example】

Such as: PING connect the IP address of the PC.

Ping Tracert Cable Test

Destination IP Address: 192.168.0.1

Timeout in Seconds (1-10): 2

Ping Count (1-100): 5

Start

Result

```

PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.0 ms

--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

```

4.4.2.2 Tracert

In the navigation bar to select “**Fault/Safety>Channel Detection>Tracert**”, Tracert detection can detect to the destination through the. Following picture :

Ping Tracert Cable Test

Destination IP Address: *

Timeout in milliseconds (1-10): 2

Start

Result

【Parameter Description】

Parameter	Description
Destination IP address	Fill in the IP address of the need to detect
Timeout in milliseconds	Range of 1 to 10

【Instruction】

the function is used to detect more is up to and reach the destination path. If a destination unreachable, diagnose problems.

【Configuration example】

Such as: PING connect the IP address of the PC.

Ping Tracert Cable Test

Destination IP Address: 192.168.0.1

Timeout in milliseconds (1-10): 2

Start

Result

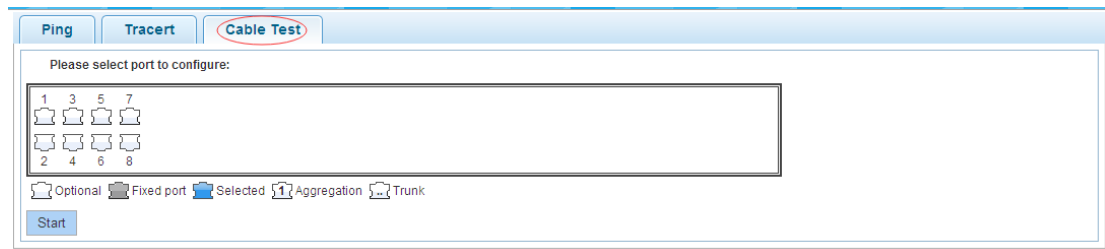
```

traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 40 byte packets
 1 192.168.0.1 (192.168.0.1) 20 ms 0 ms 10 ms

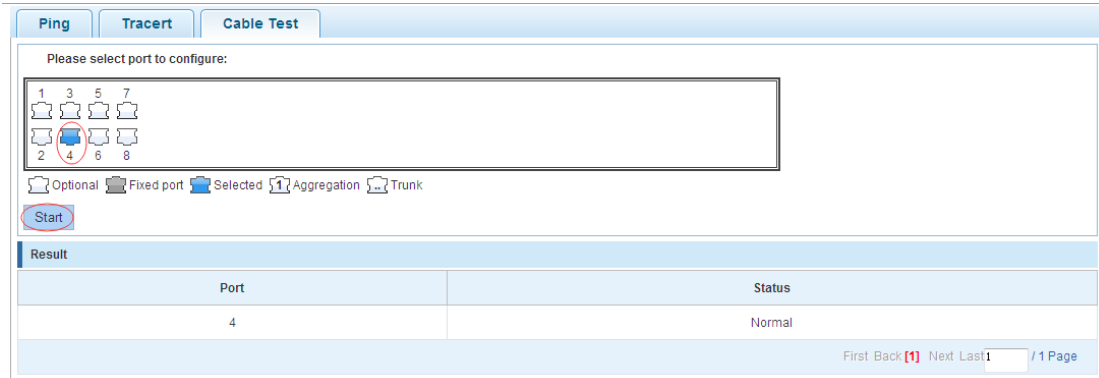
```

4.4.2.3 Cable Test

In the navigation bar to select “**Fault/Safety>Channel Detection>Cable Test**”, Can detect connection device status, the following picture:

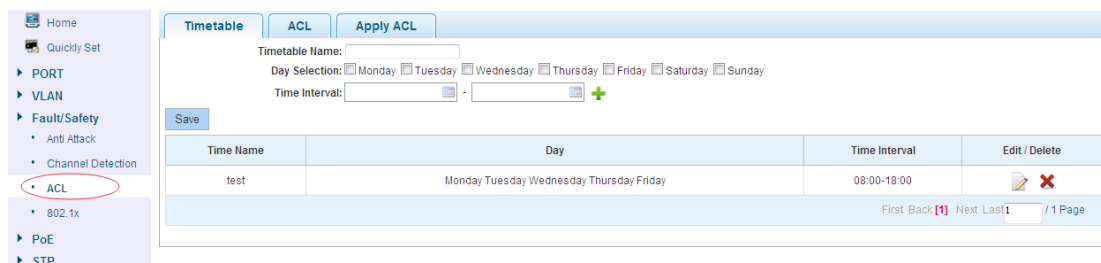


【Configuration example】



4.4.3 ACL

In the navigation bar to select “**Fault/Safety>ACL**”, ACL rules can be applied to the port and set the effective time.



【Instruction】

The ACL rules are sequenced, row in front of the match will be priority rule. If there are a lot of policy entries, the operation time will be relatively long.

Basic principles:

1. According to the order of execution, as long as there is a satisfaction, searching will be terminated.
2. Implied rejection, if both do not match, then must match the final implied denial of entry, CISCO's default.
3. Any only under the condition of the minimum permissions to the user can satisfy their demand.
4. Don't forget to apply the ACL to the port.

【Configuration example】

such as: Test effective time for Monday to Friday every day from 9 to 18, set the port 1-8 can not access the network.

steps: building ACL time - building ACL rules - is applied to the port.

Timetable ACL Apply ACL

Timetable Name: test

Day Selection: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Time Interval: 8:00 - 18:00 +

Save

Timetable ACL Apply ACL

Create ACL

Priority	Acl number	Permission	Index	Protocol	Source IP / Mask	Source Port	Destination IP / Mask	Destination Port	Timetable Name	Status	Delete
1	100	permit	10	tcp	any/any	any	any/any	any	test	inactive	✖

The new ACL access rule

ACL Number: 100 * Protocol Type: TCP

Permission: Permit ACL Name: test

Any src IP Address: *i*

Any source port: *i*

Any dst IP Address: *i*

Any dst Port: *i*

Save

First Back [1] Next Last 1 / 1 Page

Timetable ACL Apply ACL

Optional Fixed port Selected Aggregation Trunk

Tip: Click and drag cursor over ports to select multiple ports. Select all Select all others Cancel

ACL Number: 100

Filtering Direction: Receive message

Save

4.4.4 802.1x

In the navigation bar to select

“Fault/Safety>802.1x”, you can set the 802.1x information about the certification, The following picture:

Home Quickly Set

- PORT
- VLAN
- Fault/Safety
 - Anti Attack
 - Channel Detection
 - ACL
 - 802.1x
- PoE
- STP
- DHCP RELAY

802.1x config

Enable 802.1x: Disable

Re-auth enable:

Re-auth cycles: 3600 (60-7200)s

Use Pae group address:

Maximum number of auth retransmission: 2

Auth fail vlan attempts: 3

Apply

Select a port:

【Parameter Description】

Parameter	Description
Re-auth cycles	Set the Re-auth cycles to time
Maximum number of auth retransmission	Select the authentication value of the Maximum number of retransmissions
Auth fail vlan attempts	Number of attempts failed authentication VLAN

【Instruction】

802.1x is based on client / server access control and authentication protocol. It can restrict unauthorized user or device connection to port access LAN/WLAN.

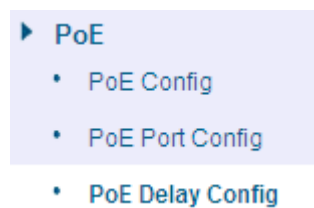
【Configuration example】

Suchas:Enable 802.1x, revalidation and using Pae group addresses, set the validation time back to 3600 S, Auth the maximum number of retransmissions is 2, failed authentication VLAN number for 3 times.

Suchas:Set port 1 of the control methods for automatic and port authentication method is based on MAC address, maximum users for 2, MBA validation for multiple authentication, MBA verification time 256s, Guest VLAN is 1, VLAN that failed validation is 2.

4.5 POE

In the navigation bar to select "POE", you can set to the **POE Config**, **POE Port Config** and **POE Delay Config** configuration.



4.5.1 POE Config

4.5.1.1 Management

In the navigation bar to select "POE>POE Config>Management", you can set POE configuration and status information, As follows.

【parameter description】

parameter	description
Alarm power	Configuration alarm threshold
Reserved power	Configuration reserved power
Alarm notification	Configure alert notification status

【instruction】

The actual application needs to control the system in the power change and the power of the port on whether to send a trap notification.

Receiving Trap notification required to open the Snmp, and set the trap target host.

【Configuration example】

Such as: For example: the alarm notification is set to 120W.

4.5.1.2 Temperature distribution

In the navigation bar to select **”POE>POE Config>Temperature distribution”**, POE chip can be set the temperature alarm threshold, As follows.

Chip Number	Current Temperature	Alarm Threshold	Edit
1	55°C	110°C	

first page prev page [1] next page last page: / 1 page

【parameter description】

parameter	description
Alarm threshold	Configuration temperature alarm threshold, range 70-149

【instruction】

Receiving Trap notification required to open the Snmp, and set the trap target host.

【Configuration example】

Such as:The 1 chip alarm threshold is set to 90°C.

Chip Number	Current Temperature	Alarm Threshold	Edit
1	55°C	90°C	

first page prev page [1] next page last page: / 1 page

4.5.2 POE Port Config

In the navigation bar to select **“POE>POE Port Config”**, you can be set to port POE, As follows.

Port	Output Status	Status	Power Level	Current Level	Power MAX	PD Type	POE Mode	Priority	Mode Detection	Edit
1	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
2	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
3	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
4	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
5	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
6	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
7	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
8	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	

Multi-Port Edit First Back [1] Next Last / 1 Page

【parameter description】

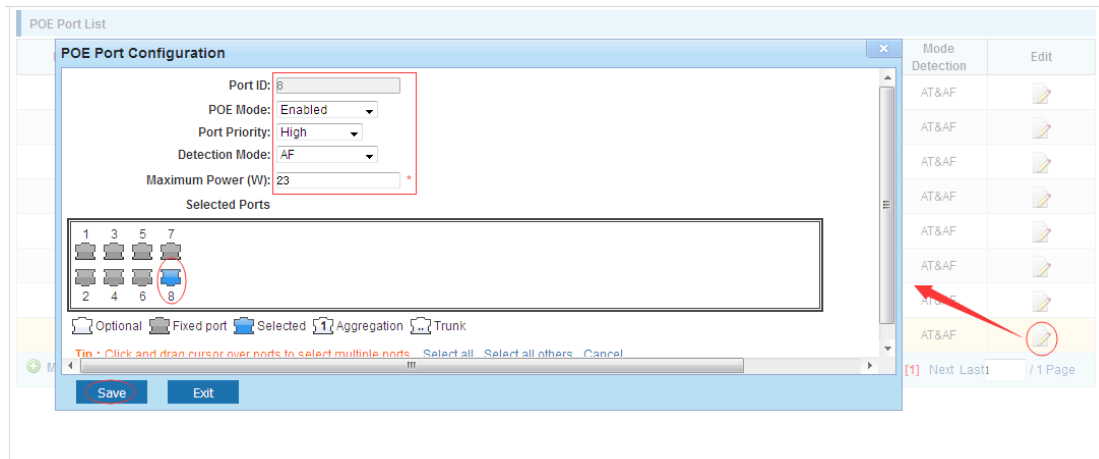
parameter	description
Power MAX	Select the maximum power of the configured port
POE mode	Enable state of the selected configuration
Priority	Configure port priority, when the load exceeds the maximum power POE, low priority port equipment will be dropped
Mode Detection	Power supply mode for configuration port detection

【instruction】

Receiving Trap notification required to open the Snmp, and set the trap target host.

【Configuration example】

Such as:The 8 port can be opened, the maximum power of 23 W, the detection mode is AF, the priority is high.



4.5.3 POE Delay Config

In the navigation bar to select “**POE>POE Delay Config**”, you can be set to port POE, As follows.

PoE Restart/Delay

Optional Fixed port Selected Aggregation Trunk

Tip : Click and drag cursor over ports to select multiple ports

Current System Time: 2016-12-20 15:54:53, Tuesday

Restart Weeks Selection: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Restart Time:

Port Delay Time: Seconds(0-3600) *

Save

PoE Delay List

Ports	Port Restart Time	Port Delay Time	Operation
1	0	0s	
2	0	0s	
3	0	0s	
4	0	0s	
5	0	0s	
6	0	0s	
7	0	0s	
8	0	0s	

First Back [1] Next Last / 1 Page

【parameter description】

parameter	description
Port Restart Time	Set port restart limit time
Port Delay Time	Set the delay time for port POE power supply

【instruction】

Receiving Trap notification required to open the Snmp, and set the trap target host.

【Configuration example】

Such as:Set port 1 port reset time is 15:56:59 in Every day, port delay time of 20 seconds.

PoE Restart/Delay

Optional Fixed port Selected Aggregation Trunk

Tip : Click and drag cursor over ports to select multiple ports

Current System Time: 2016-12-20 15:56:56, Tuesday

Restart Weeks Selection: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Restart Time: 15:56:59

Port Delay Time: 20 Seconds(0-3600) *

Save

PoE Delay List

Ports	Port Restart Time	Port Delay Time	Operation
1	Sun,Mon,Tues,Wed,Thur,Fri,Sat,15:56:59	20s	
2	0	0s	
3	0	0s	
4	0	0s	
5	0	0s	
6	0	0s	
7	0	0s	
8	0	0s	

First Back [1] Next Last / 1 Page

4.6 STP

In the navigation bar to select "STP", you can set to the **MSTP Region** and **STP Bridge** configuration.



4.6.1 MSTP Region

In the navigation bar to select "STP>MSTP Region". Can modify the domain and domain name, add instance is mapped to a VLAN. The following picture.

【Parameter Description】

Parameter	Description
Region name	Configure the region name
Revision level	Parameter configuration revision level
Instance ID	Select configuration instance ID
VLAN ID	Mapping of the VLAN configuration instance

【Instruction】

An instance can only be mapped to one VLAN, instance and VLAN is a one-to-one relationship.

【Configuration example】

Such as: change the region to DEADBEEF0102, region name as 123, instance 4 is mapped to a VLAN 2, in the first need to create a VLAN 2.

4.6.2 STP Bridge

In the navigation bar to select "STP>STP Bridge". Can be related to bridge, port configuration, the following picture:

The screenshot shows the SUNDRAY web interface for configuring STP. The left navigation menu has 'STP Bridge' selected. The main configuration area is split into two sections:

- STP Bridge Config:**
 - Instance Priority:
 - Instance ID:
 - Priority:
 - Enable: ON OFF
 - Mode: STP RSTP MSTP
 - Hello Time: (1-10s)
 - MAX Age: (6-40s)
 - Forward Delay: (4-30s)
 - MAX Hops: (1-40)
- STP port config:**
 - Instance:
 - Priority: (0-240, step 16)
 - Path Cost: (auto or 1-200000000)
 - Port Fast: ON OFF
 - Auto Edge: ON OFF
 - Point to Point: ON OFF Auto
 - BPDU Guard: ON OFF
 - Compatible: ON OFF
 - BPDU Filter: ON OFF
 - Root Guard: Root None
 - TC Guard: ON OFF
 - TC Ignore: ON OFF

At the bottom, there is a port selection grid with 10 ports (1-10) and a legend for port types: Optional, Fixed port, Selected, Aggregation, and Trunk.

【Parameter Description】

Parameter	Description
inst-priority	Whether open instance priority setting
Instance ID	Select the created instance id is configured
enable	Whether to open the STP bridge function
Bridge priority	Priority setting bridge example, the default instance bridge priority for 32768
mode	The model is divided into: the STP, RSTP, MSTP
Hello-time	Switches sends bpdus in packet interval
Max-age	Ports are not yet received a message in the time, will initiate topology changes
Forward-delay	The state of the port switch time
Port-priority	Set port instance priority, defaults to 128, you must enter multiple of 16, the range of 0-240
Path-cost	Configure port costs
Port-fast	Select configuration state
Auto-ege	Select configuration state
Point-to-point	Select configuration state
Bpdu guard	Select configuration state
Bpdu filter	Select configuration state
compatible	Select configuration state
Root guard	Select configuration state
TC guard	Select configuration state
TC filter	Select configuration state

【Instruction】

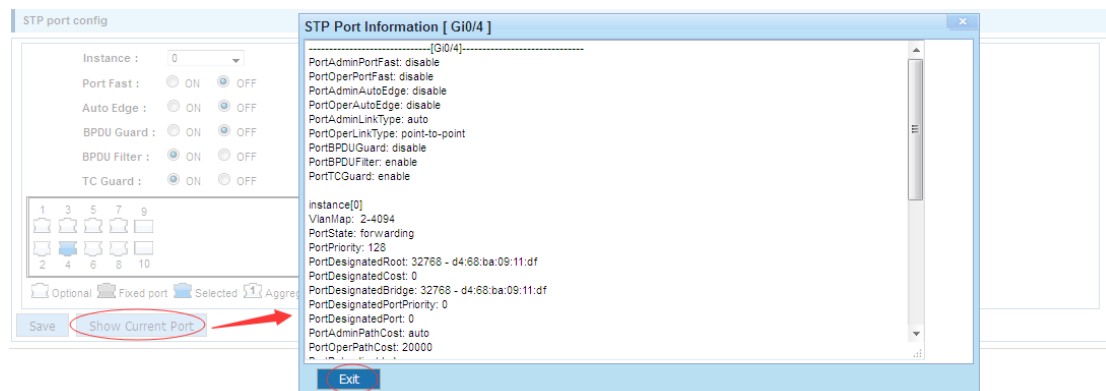
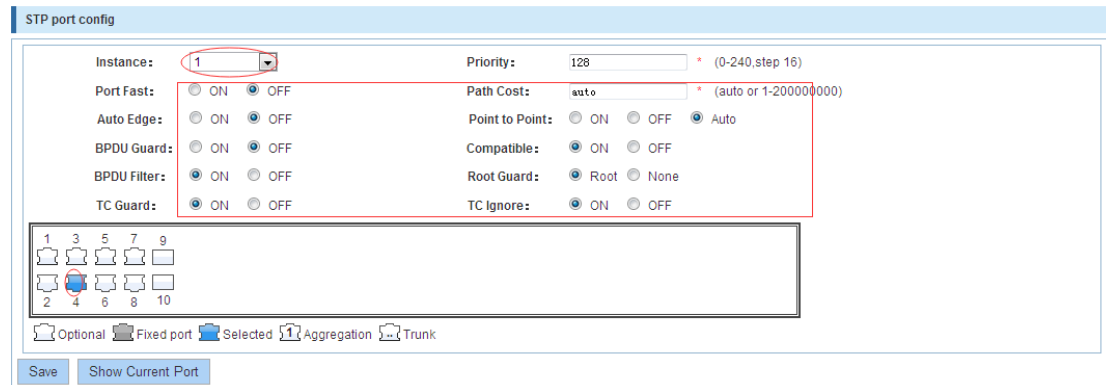
(1) $(\text{hello_time}+1) \times 2 \leq \text{max_age} \leq (\text{f_delay}-1) \times 2$, enable the switch to set instance priority.

(2) Enable STP or switch mode would spend 2 times of the forward delay time.

【Configuration example】

Such as:

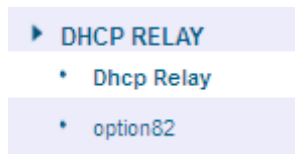
- 1) Open the STP, configuration has to create an instance of the priority, configuration time Parameters, set the pattern to MSTP.



- 2) Set MSTP has launched port configuration, select the created instance, set priority (port configuration is not online, on-line configuration will only take effect, can click on the "view the current configuration" button to view the configured completed).

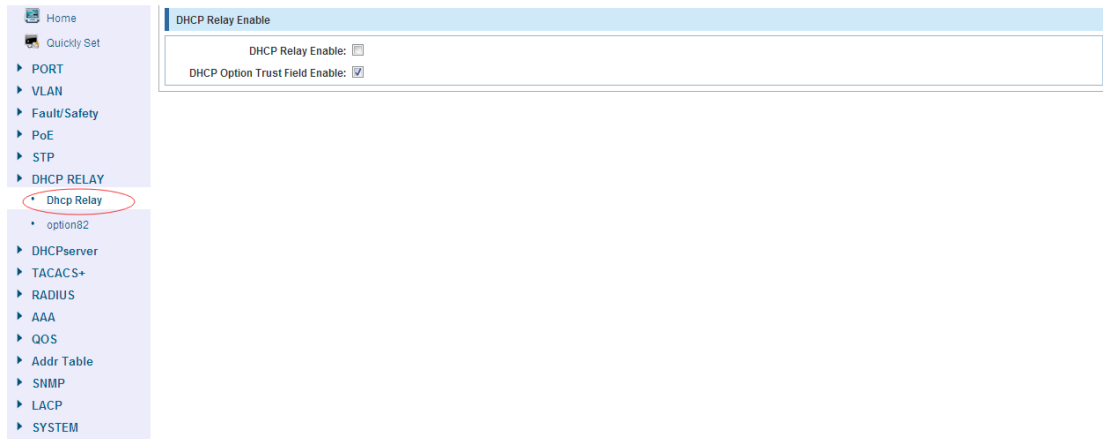
4.7 DHCP RELAY

In the navigation bar to select "DHCP RELAY", you can set to the DHCP relay and option82.



4.7.1 DHCP Relay

In the navigation bar to select "DHCP Relay", Open the DHCP relay function, set up and view the relay server IP address and its status. The following picture.



【Parameter Description】

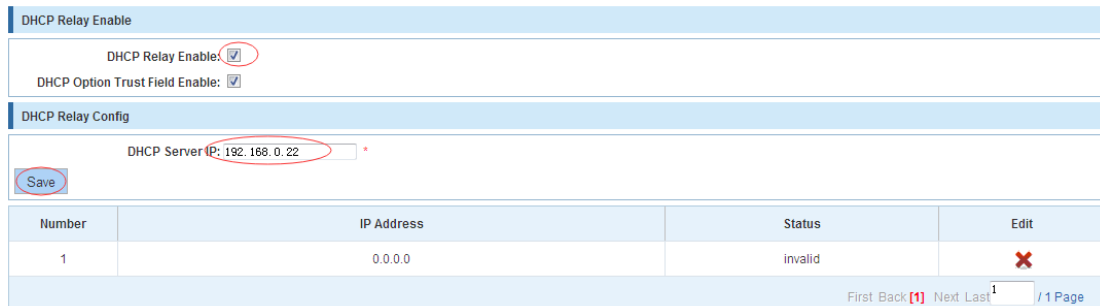
Parameter	Description
IP address	DHCP server address
status	Invalid and vaild

【Instruction】

If the function of relay agent is turned on, Then the received DHCP broadcast message will be sent to the server in the form of unicast. DHCP server and IP switches in the same network will take effect.

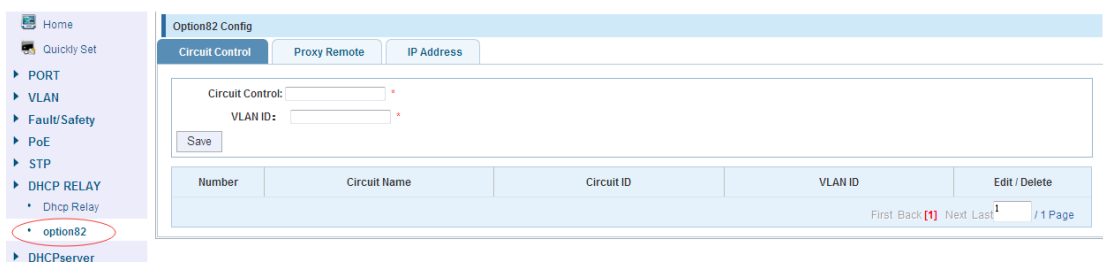
【Configuration example】

Such as: setting DHCP server ip for 192.168.0.22.



4.7.2 Option82

In the navigation bar to select "DHCP relay>option82", can set to option82 circuit control, proxy remote, ip address. The following picture:



【Parameter Description】

Parameter	Description
VLAN id	the DHCP request message in the VLAN, value range is 1 ~ 4094
Circuit control	Circuit ID to populate the user custom content, scope of string length is 3 ~ 63
Proxy remote	Configuration ASCII remote id string value, the length of the range of 1 ~ 63
IP address	Decimal IP address

【Instruction】

Switch relay to the DHCP server will bring the option82 information, ID VLAN need to be configured as DHCP packets go VLAN party can bring option82 information.

【Configuration example】

Such as: add circuit control, proxy remote, ip address information.

Circuit Control
Proxy Remote
IP Address

Circuit Control: *

VLAN ID: *

Number	Circuit Name	Circuit ID	VLAN ID	Edit / Delete
First Back 1 Next Last 1 / 1 Page				

Option82 Config

Circuit Control
Proxy Remote
IP Address

Proxy Remote: *

VLAN ID: *

Number	Proxy Remote Name	Proxy Remote ID	VLAN ID	Edit / Delete
First Back 1 Next Last 1 / 1 Page				

Circuit Control
Proxy Remote
IP Address

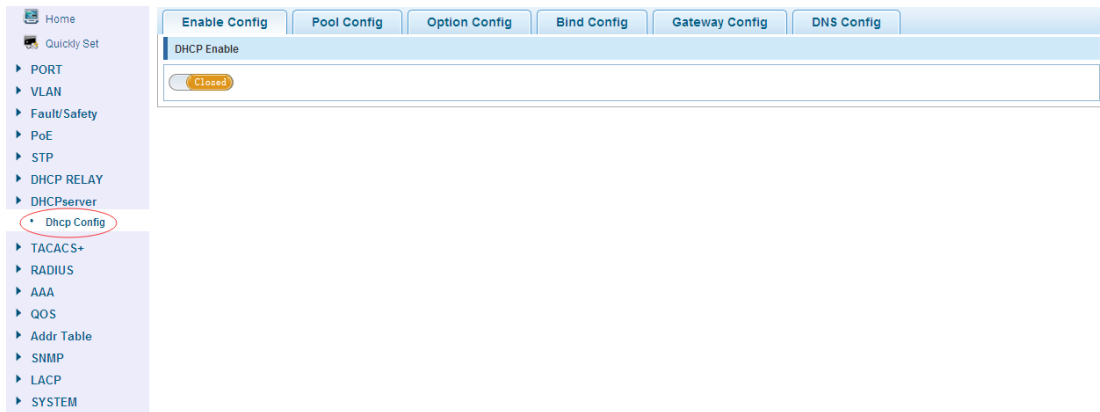
IP Address: *

VLAN ID: *

Number	IP Address	VLAN ID	Edit / Delete
First Back 1 Next Last 1 / 1 Page			

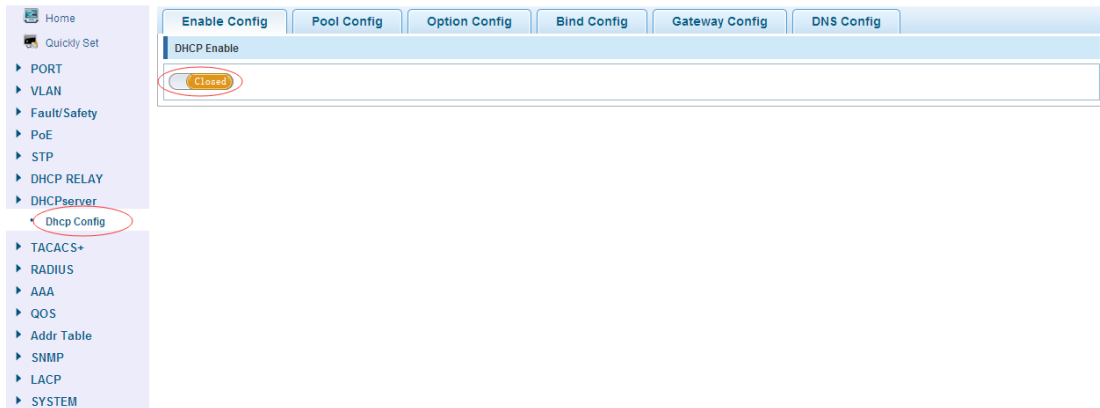
4.8 DHCP Server

In the navigation bar to select "DHCP Server", Here you can configure the DHCP server. The following picture:



4.8.1 Enable Config

In the navigation bar to select "DHCP Server>Enable Config", Here you can enable or disable the DHCP server.

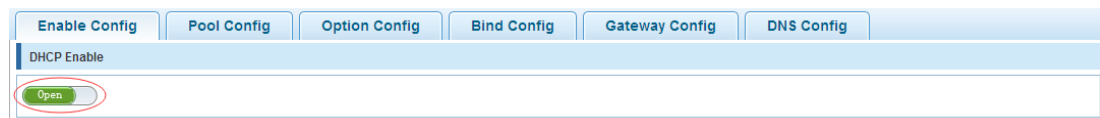


【Instructions】

Enable or disable the DHCP server, you can configure the DHCP server. When you start the DHCP server turn off DHCP-relay.

【Configuration example】

Such as: Open the DHCP Server.



4.8.2 Pool Config

In the navigation bar to select "DHCP Server>Pool Config", You can configure the IP address pool of information.

Enable Config	Pool Config	Option Config	Bind Config	Gateway Config	DNS Config			
Pool ID <input type="text"/> * (1-65535) Domain <input type="text"/> Network IP <input type="text"/> * Network Mask <input type="text"/> * Start IP <input type="text"/> End IP <input type="text"/> Lease Time <input type="text"/> Days <input type="text"/> Hours <input type="text"/> Minutes								
<input type="button" value="Set Up"/>								
Pool Table								
<input type="checkbox"/>	Pool ID	Domain	Network IP	Network Mask	Lease Time	Start IP	End IP	Delete
First Back [1] Next Last 1 / 1 Page								

【Parameter Description】

Parameter	Description
Pool ID	Setting address pool ID number range between 1~65535
Network IP	Setting the subnet IP address, subnet IP and Start IP need to be in the same network segment
Network Mask	Setting the net-mask
Start IP	Setting the starting IP address of the subnet
End IP	Setting the ending IP address of the subnet
Lease Time	Setting the length of the lease time

【Instruction】

Configuring the address pool feature to DHCP server, including subnet addresses, subnet masks, and lease time.

【Configuration example】

Such as: add Pool ID, Domain, Network IP, Network Mask, Start IP, End IP, Lease Time.

Enable Config	Pool Config	Option Config	Bind Config	Gateway Config	DNS Config			
Pool ID <input type="text" value="1"/> * (1-65535) Domain <input type="text" value="Public"/> Network IP <input type="text" value="192.168.1.6"/> * Network Mask <input type="text" value="255.255.255.0"/> * Start IP <input type="text" value="192.168.1.100"/> End IP <input type="text" value="192.168.1.200"/> Lease Time <input type="text" value="1"/> Days <input type="text" value="23"/> Hours <input type="text" value="59"/> Minutes								
<input type="button" value="Set Up"/>								
Pool Table								
<input type="checkbox"/>	Pool ID	Domain	Network IP	Network Mask	Lease Time	Start IP	End IP	Delete
<input checked="" type="checkbox"/>	1	Public	192.168.1.0	255.255.255.0	172740secs	192.168.1.100	192.168.1.200	<input checked="" type="checkbox"/>
First Back [1] Next Last 1 / 1 Page								

4.8.3 Option Config

In the navigation bar to select "DHCP Server>Option Config", You can Configure a Option parameters to DHCP Server.

Enable Config Pool Config **Option Config** Bind Config Gateway Config DNS Config

Pool ID 1
Code 2 * (1-255)
Code Value Type hex
Code Value 192.168.1.2 *

Set Up

Pool ID	Code	Code Value	Delete
---------	------	------------	--------

First Back [1] Next Last 1 / 1 Page

【Parameter Description】

Parameter	Description
Pool ID	Select the address you want to configure the pool ID
Code	Select the value of code
Code value Type	Can choose the following kinds: HEX ASCII IP
Code value	According choose code value type the setting code value

【Instruction】

Setting the Option parameter to the IP address pool.

【Configuration example】

Such as:Setting Pool ID is 1, Code is 2, Code value type choose is ip, Code value is 192.168.1.2.

Enable Config Pool Config **Option Config** Bind Config Gateway Config DNS Config

Pool ID 1
Code 2 * (1-255)
Code Value Type ip
Code Value 192.168.1.2 *

Set Up

Pool ID	Code	Code Value	Delete
1	option-2	192.168.1.2	X

First Back [1] Next Last 1 / 1 Page

4.8.4 Bind Config

In the navigation bar to select "DHCP Server>Bind Config",Here you can view or delete your IP/MAC address binding.

Enable Config Pool Config Option Config **Bind Config** Gateway Config DNS Config

IP Address	Hardware Type	Hardware Address	Expire Time	Delete
------------	---------------	------------------	-------------	--------

4.8.5 Gateway Config

In the navigation bar to select "DHCP Server>Gateway Config",Here you can set IP address pool the default gateway.

【Instruction】

According to the selected Pool ID to set the default gateway.

【Configuration example】

Such as:

According to the selected Pool ID is 1 to set the default gateway is 192.168.1.55.

Pool ID	Gateway	Delete
1	192.168.1.55	

4.8.6 DNS Config

In the navigation bar to select "DHCP Server>NDS Config", Here you can set IP address pool the DNS server.

【Instruction】

According to the selected Pool ID to set the DNS server.

【Configuration example】

Such as: According to the selected Pool ID is 1 to set the DNS server is 47.54.89.210.

Enable Config Pool Config Option Config Bind Config Gateway Config **DNS Config**

Pool ID 1

DNS Server 1 47.54.89.210

DNS Server 2

DNS Server 3

DNS Server 4

DNS Server 5

DNS Server 6

DNS Server 7

DNS Server 8

Set Up

DNS Server List			
	Pool ID	DNS Server	Operation
<input type="checkbox"/>	1	47.54.89.210	✘

First Back [1] Next Last 1 / 1 Page

4.9 TACACS+

In the navigation bar to select "TACACS+", you can to add, edit or delete TACACS+ Server settings.

Home Quickly Set

- PORT
- VLAN
- Fault/Safety
- PoE
- STP
- DHCP RELAY
- DHCPserver
- TACACS+
- TACACS+ Config**
- RADIUS
- AAA
- QOS
- Addr Table
- SNMP
- LACP
- SYSTEM

TACACS+ Config

Global Config

Server Timeout: 5

Server Retry Count: 3

Conversation/Connect: Only Multi

Key:

Save

Port Config

Server IP:

Authentication Port:

Server Timeout:

Key:

Save

TACACS+ Server List				
Serial Number	Server IP	Port	Server Timeout Value	Delete

First Back [1] Next Last 1 / 1 Page

【Instruction】

Setting parameters for the TACACS + Server.

【Configuration example】

Such as: Setting the TACACS + server connection timeout is 5, the server retry count is 3. Connection dialog for most, Key is 2644as, server IP is 192.168.0.88, authentication port is 49.

TACACS+ Config

Global Config

Server Timeout: 5
 Server Retry Count: 3
 Conversation/Connect: Only Multi
 Key: 2644sa

Save

Port Config

Server IP: 192.168.0.88
 Authentication Port: 49
 Server Timeout: 5
 Key: 2644sa

Save

TACACS+ Server List

Serial Number	Server IP	Port	Server Timeout Value	Delete
1	192.168.0.88	49	5	

First Back [1] Next Last 1 / 1 Page

4.10 RADIUS

In the navigation bar to select "RADIUS", You can to set about radius server.

Home

Quickly Set

- ▶ PORT
- ▶ VLAN
- ▶ Fault/Safety
- ▶ PoE
- ▶ STP
- ▶ DHCP RELAY
- ▶ DHCPserver
- ▶ TACACS+
- ▶ RADIUS
- ▶ RADIUS Global C...
- ▶ AAA
- ▶ QOS
- ▶ Addr Table
- ▶ SNMP
- ▶ LACP
- ▶ SYSTEM

Radius General Config | Radius Server Config

RADIUS Global Config Information

Server Repeat Number:3
 Server Timeout:2
 Server Quiet Time:0
 Dead-criteria Retry Count:0
 Dead-criteria Timeout:0

Change Config

4.10.1 Radius General Config

In the navigation bar to select "RADIUS> Radius General Config", You can setting radius general config.

Radius General Config | Radius Server Config

RADIUS Global Config Information

Server Repeat Number:3
 Server Timeout:2
 Server Quiet Time:0
 Dead-criteria Retry Count:0
 Dead-criteria Timeout:0

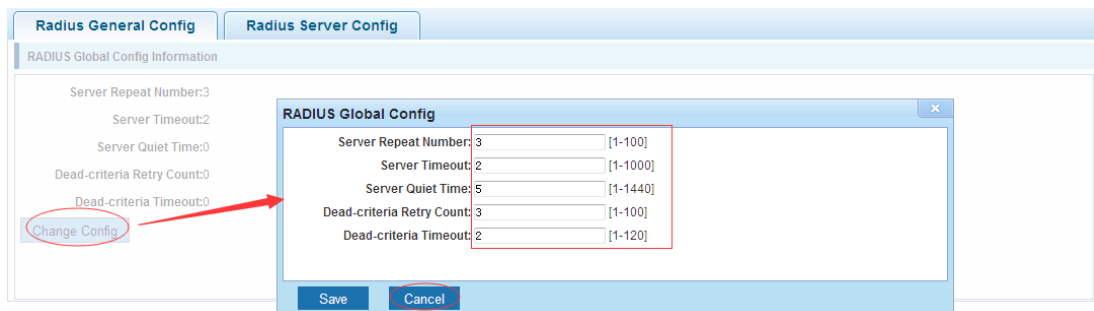
Change Config

【Instruction】

Setting parameters for the radius general config.

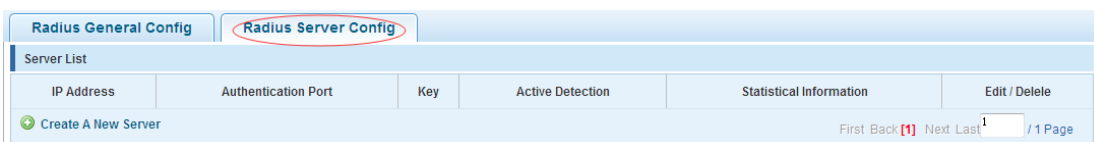
【Configuration example】

Such as: Setting RADIUS server the number of repetitions for 3, server timeout is 2, quiet time for 5, Dead-criteria the server Retry Count for 3, Dead-criteria Timeout is 2.



4.10.2 Radius Server Config

In the navigation bar to select "RADIUS> Radius Server Config", You can setting Radius Server.

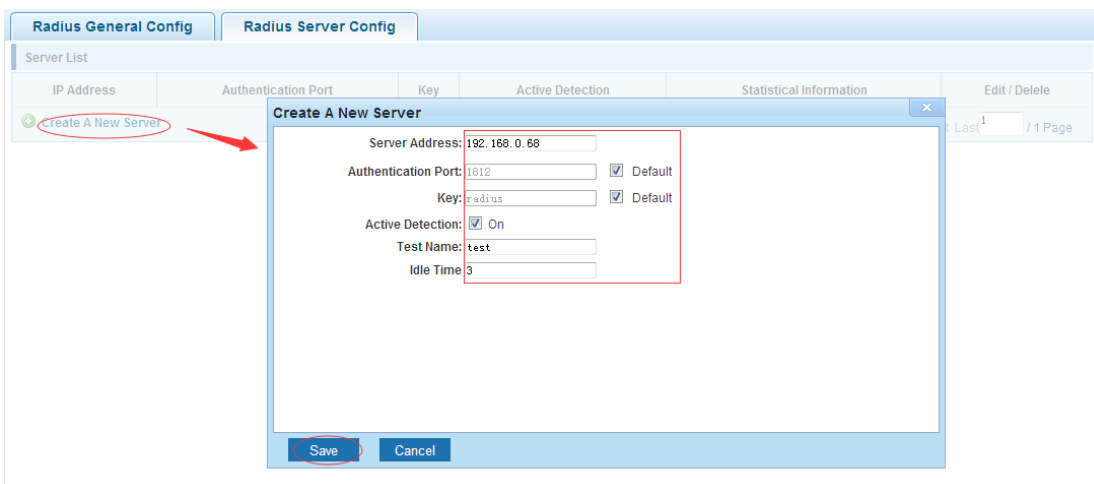


【Instruction】

Setting parameters for the radius server config.

【Configuration example】

Such as: Setting the Radius server address is 192.168.0.68, authentication port for 1812, key for RADIUS, test name for the Admin, idle time is 3.



4.11 AAA

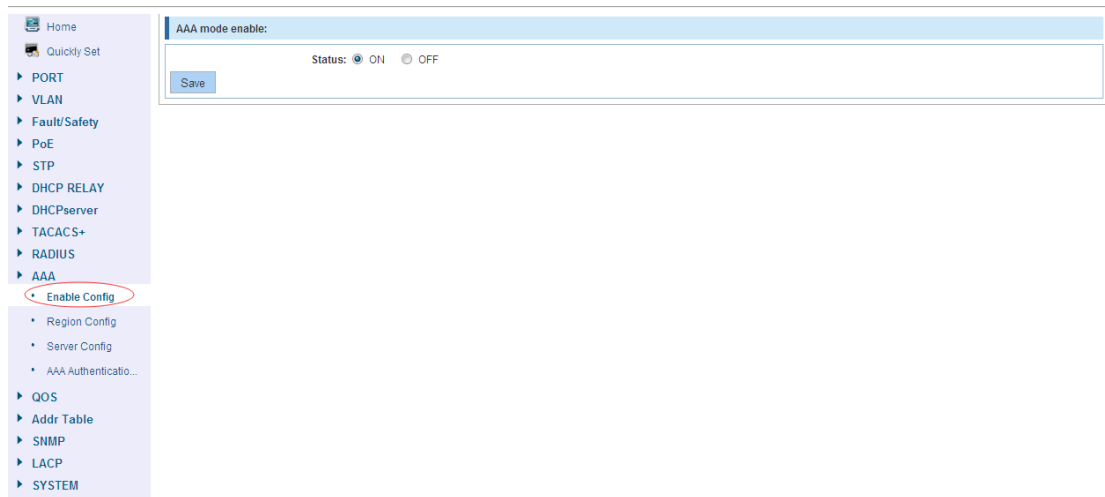
In the navigation bar to select "AAA", you can set to the **Enable Config, Region Config,**

Server Config and AAA Authentication.



4.11.1 Enable Config

In the navigation bar to select "AAA>Enable Config", You can on or off the AAA model.

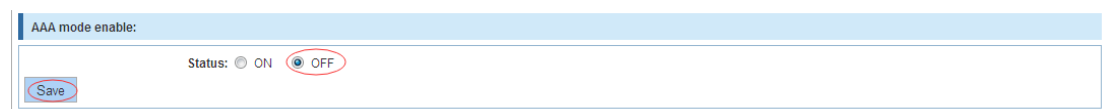


【Instruction】

Open or close the AAA model.

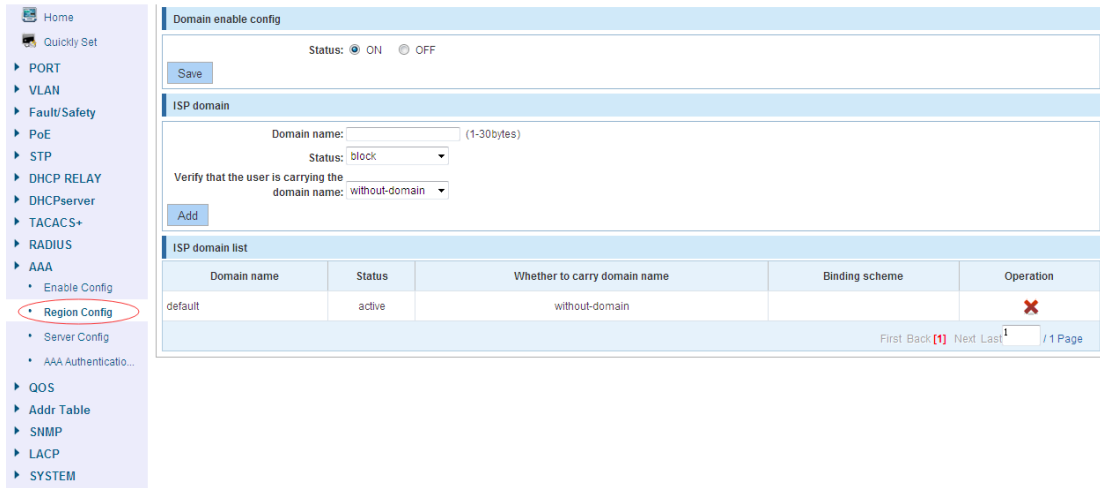
【Configuration example】

Such as: Close the AAA model.



4.11.2 Region Config

In the navigation bar to select "AAA>Region Config", You can turn on or off the domain and configure the other parameters.



【Parameter Description】

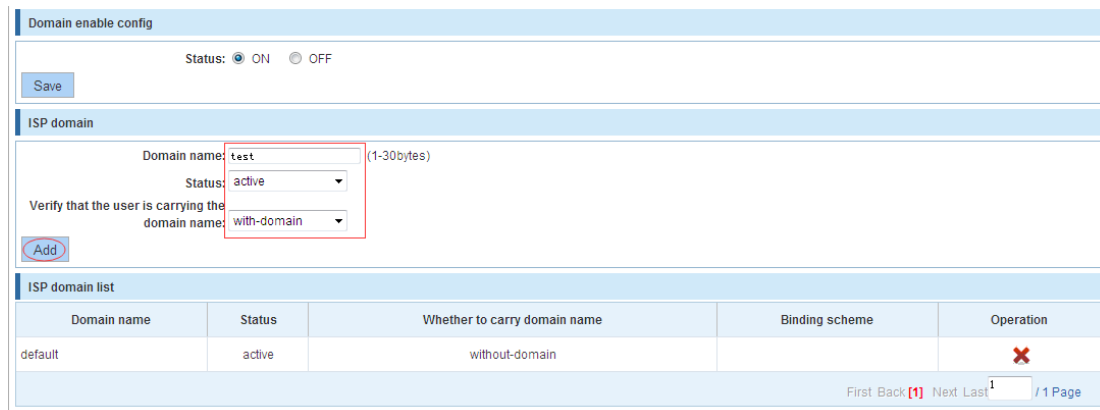
Parameter	Description
Domain name	Setting Domain name
Status	Can choose the following kinds: Block Active
Verify that the user is carrying the domain name	Can choose the following kinds: Without-domain With-domain

【Instruction】

Setting the Option parameter to the IP address pool.

【Configuration example】

Such as:Setting Domain name is test, Status choose for to active, Verify that the user is carrying the domain name choose is with-domain.



4.11.3 Server Config

In the navigation bar to select "AAA>Server Config", You can configure the server parameters.

【Parameter Description】

Parameter	Description
Server name	Setting Server name
Server IP address	Setting Server IP address
Select server	Can choose the following kinds: Radius Tacacs+

【Instruction】

Setting the server parameters.

【Configuration example】

Such as:Server name is aaa, Server IP address is 192.168.0.66,Server select tacacs+.

4.11.4 AAA Authentication

In the navigation bar to select "AAA>AAA Authentication", You can configure the AAA Authentication.Included Longin Authentication, Enable Authentication and Dot 1x Authentication.

Home
Quickly Set

- PORT
- VLAN
- Fault/Safety
- PoE
- STP
- DHCP RELAY
- DHCPserver
- TACACS+
- RADIUS
- AAA
 - Enable Config
 - Region Config
 - Server Config
 - AAA Authentica...**
- QOS
- Addr Table
- SNMP
- LACP
- SYSTEM

Login authentication Enable authentication Dot1x authentication

AAA accounting configuration

Choose a domain: none

LOGIN Authentication Project name: default

First method: Local
Second method:
Third method:
Fourth method:

Save

project name	Method	Operation
default	(local)	X

First Back [1] Next Last 1 / 1 Page

4.11.4.1 Login Authentication

In the navigation bar to select "AAA>AAA Authentication>Login Authentication", You can setting Login Authentication.

Login authentication Enable authentication Dot1x authentication

AAA accounting configuration

Choose a domain: none

LOGIN Authentication Project name: default

First method: Local
Second method: None
Third method: Group RADIUS
Fourth method: Group TACAS+

Save

project name	Method	Operation
default	(local)	X

First Back [1] Next Last 1 / 1 Page

【Parameter Description】

Parameter	Description
First method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Second method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Third method	Can choose the following kinds: Local None Group Radius

	Group Tacacs+ Custom server group
Fouth method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group

【Instruction】

Setting the Login Authentication.

【Configuration example】

Such as:First method choose the local, Second method choose the none, Third method choose the Group Radius, Fouth method the Group Tacacs+.

AAA accounting configuration

Choose a domain: none

LOGIN Authentication Project name: default

First method: Local

Second method: None

Third method: Group RADIUS

Fourth method: Group TACAS+

Save

project name	Method	Operation
default	(local)	X

First Back [1] Next Last 1 / 1 Page

4.11.4.2 Enable Authentication

In the navigation bar to select "AAA>AAA Authentication>Enable Authentication", You can setting Enable Authentication.

AAA Authentication config

Select a domain name: none

Enable Authentication Policy name: default

First method: Local

Second method:

Third method:

Fourth method:

Save

Policy name	Method	Operation
default	(local)	X

First Back [1] Next Last 1 / 1 Page

【Parameter Description】

Parameter	Description
First method	Can choose the following kinds: Local

	None Group Radius Group Tacacs+ Custom server group
Second method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Third method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Fouth method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group

【Instruction】

Setting the Login Authentication.

【Configuration example】

Such as: First method choose the local, Second method choose the none, Third method choose the Group Radius, Fouth method the Group Tacacs+.

4.11.4.3 Dot1x Authentication

In the navigation bar to select "AAA>AAA Authentication>Dot1x Authentication", You can setting Dot1x Authentication.

[Login authentication](#)
[Enable authentication](#)
[Dot1x authentication](#)

AAA authentication configuration

Domain: none

Dot1x authentication
 project name: default

First method: Local
 Second method:
 Third method:
 Fouth method:

[Add](#)

dot1x authentication list		
Project name	Method	Operation
First Back [1] Next Last 1 / 1 Page		

【Parameter Description】

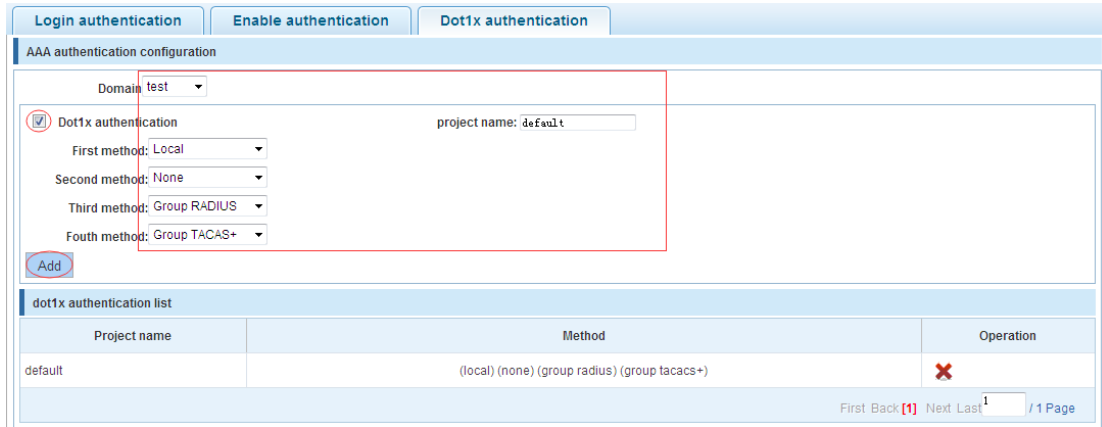
Parameter	Description
First method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Second method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Third method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group
Fouth method	Can choose the following kinds: Local None Group Radius Group Tacacs+ Custom server group

【Instruction】

Setting the Login Authentication.

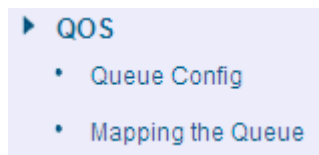
【Configuration example】

Such as: First method choose the local, Second method choose the none, Third method choose the Group Radius, Fouth method the Group Tacacs+.



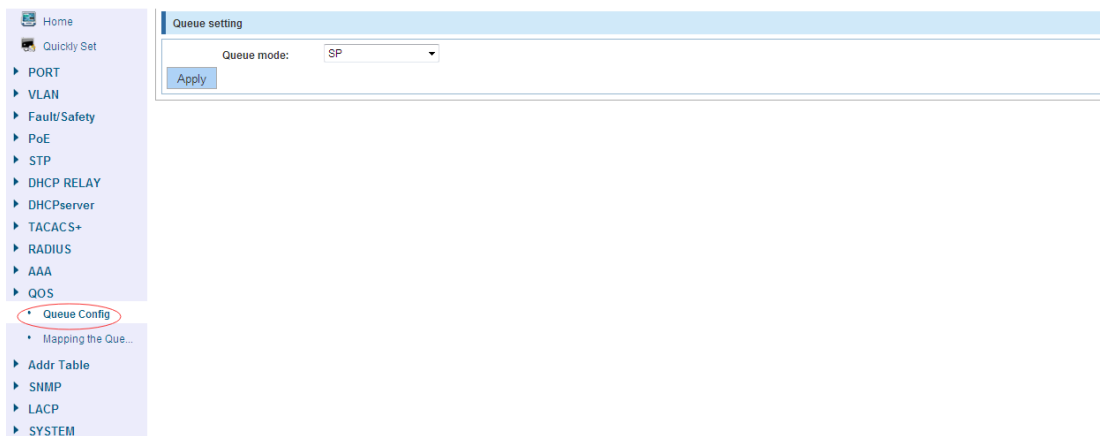
4.12 QoS

In the navigation bar to select "QOS", you can set to the **Remark**, **Queue Config** and **Mapping the Queue**.



4.12.1 Queue Config

In the navigation bar to select "QOS>Queue Config". Can be set up queue scheduling policy. The following picture:



【Parameter Description】

Parameter	Description
Scheduling strategy	Can choose four kinds of modes: RR round-robin scheduling SP absolute priority scheduling WRR weighted round-robin scheduling

	WFQ weighted fair scheduling
WRR-weights	Set the weights of each queue, they will be in proportion to occupy the bandwidth to send data

【Instruction】

Queue 7 can not for 0.

【Configuration example】

Such as: set the scheduling strategy for WRR, weight value respectively, 10, 11, 12, 12, 14, 15, 16, 17.

Queue setting

Scheduling strategy: WRR

Byte weight(0-127): 10 11 12 13 14 15 16 17

Apply

4.12.2 Mapping the queue

4.12.2.1 COS Queue Map

In the navigation bar to select "QOS>COS Queue Map", Service category can be mapped to the corresponding queue. The following picture.

COS Queue Map | DSCP COS Map | Port COS Map

Mapping Queue Status Information

Server ID	0	1	2	3	4	5	6	7
Queue ID	0	1	2	3	4	5	6	7

Save

Navigation: Home, Quickly Set, PORT, VLAN, Fault/Safety, PoE, STP, DHCP RELAY, DHCPserver, TACACS+, RADIUS, AAA, QOS, Queue Config, **Mapping the Que...**, Addr Table, SNMP, LACP, SYSTEM

【Parameter Description】

Parameter	Description
Server ID	COS the VLAN priority fields (0 to 7)
Queue ID	Set each cosine value mapping queue number (0 to 7)

【Configuration example】

Such as: cos 3 mapping to the queue 7, set the queue weight 7 to 10.

COS Queue Map | DSCP COS Map | Port COS Map

Mapping Queue Status Information

Server ID	0	1	2	3	4	5	6	7
Queue ID	0	1	2	7	4	5	6	7

Save

4.12.2.2 DSCP COS Map

In the navigation bar to select "QoS>Mapping the Queue>DSCP COS Map". Differential service can be mapped to the corresponding service categories. The following picture:

Server ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Server List 1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Server ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Server List 2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3
Server ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Server List 3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
Server ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Server List 4	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7

【Parameter Description】

Parameter	Description
Server list	DSCP field has seven (0-63) is divided into four tables
Queue ID	Map the DSCP to COS fields (0 to 7), based on the cosine is mapped to a queue

【Instruction】

Cos priority is greater than the DSCP, DSCP priority is greater than the port.

【Configuration example】

Such as: the DSCP value of 3, 12, 23 mapping to cos 5.

Server ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Server List 1	0	0	0	5	0	0	0	0	1	1	1	1	1	5	1	1
Server ID	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Server List 2	2	2	2	2	2	2	2	5	3	3	3	3	3	3	3	3
Server ID	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Server List 3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5
Server ID	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Server List 4	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7

4.12.2.3 Port COS Map

In the navigation bar to select "QoS>mapping the queue>Port COS Map", Port can be mapped to the corresponding service categories. The following picture:

COS Queue Map DSCP COS Map **Port COS Map**

Port CoS mapping

Port: 1
 Server ID: 0
 Trust Mode: COS
 Apply

Control list

Port	Server ID								Trust Mode
	0	1	2	3	4	5	6	7	
1	T								
2	T								
3	T								
4	T								
5	T								
6	T								
7	T								
8	T								

First Back [1] [2] Next Last 1 / 2 Page

【Parameter Description】

Parameter	Description
Port	Select the port number (1-10)
Service ID	Mapped to the service ID, and then according to the service ID into the queue
Mode	Can choose the following kinds: COS DSCP

【Instruction】

Cos priority is greater than the DSCP, DSCP priority is greater than the port.

【Configuration example】

Such as: port 4、5、6 respectively cos4、cos5、dscp6.

COS Queue Map DSCP COS Map **Port COS Map**

Port CoS mapping

Port: 4
 Server ID: 4
 Trust Mode: COS
 Apply

COS Queue Map DSCP COS Map **Port COS Map**

Port CoS mapping

Port: 5
 Server ID: 5
 Trust Mode: COS
 Apply

COS Queue Map DSCP COS Map **Port COS Map**

Port CoS mapping

Port: 6
 Server ID: 6
 Trust Mode: dscp

Apply

Control list

Port	Server ID								Trust Mode
	0	1	2	3	4	5	6	7	
1	T								
2	T								
3	T								
4					T				cos
5						T			cos
6							T		dscp
7	T								
8	T								

First Back [1] [2] Next Last 1 / 2 Page

4.13 Address table

In the navigation bar to select "Address table", you can set to **MAC Management**, **MAC Learning and Aging** and **MAC Filter**.

Home Quickly Set

- PORT
- VLAN
- Fault/Safety
- PoE
- STP
- DHCP RELAY
- DHCPserver
- TACACS+
- RADIUS
- AAA
- QOS
- Addr Table
- Address Table**
- SNMP
- LACP
- SYSTEM

Address Table Config

MAC Management MAC Learning and Aging MAC Filter

Clear MAC: Clear appoint MAC
 VLAN: 1 Valid Range (1 to 4094)
 MAC Address:

Save

1 3 5 7 9
 2 4 6 8 10

Optional Fixed port Selected Aggregation Trunk

VLAN: 1 Valid Range (1 to 4094)
 MAC Address:

Save

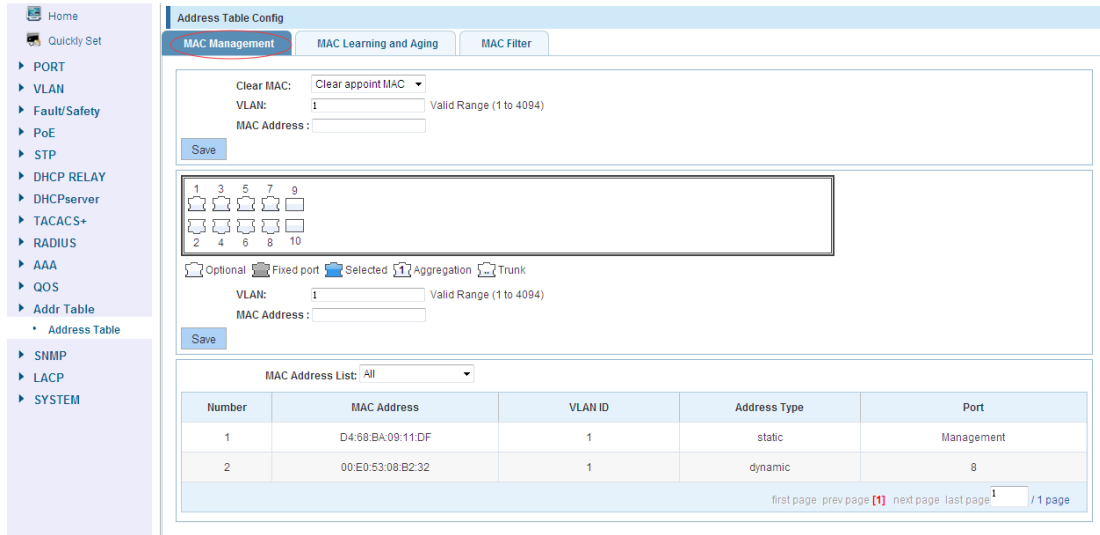
MAC Address List: All

Number	MAC Address	VLAN ID	Address Type	Port
1	D4:68:BA:09:11:DF	1	static	Management
2	00:E0:53:08:B2:32	1	dynamic	8

first page prev page [1] next page last page 1 / 1 page

4.13.1 Mac Management

In the navigation bar to select "Address table>Mac Management". You can add static Mac and delete Mac and view to the current of the Mac address table. The following picture:



【Parameter Description】

Parameter	Description
Clear Mac	Can choose to clear the multicast Mac address, clear dynamic unicast Mac address, clear static unicast Mac address, clear the specified Mac address, Mac address table
VLAN	Fill in the need to add or delete VLAN id, not create vlans to create can only take effect

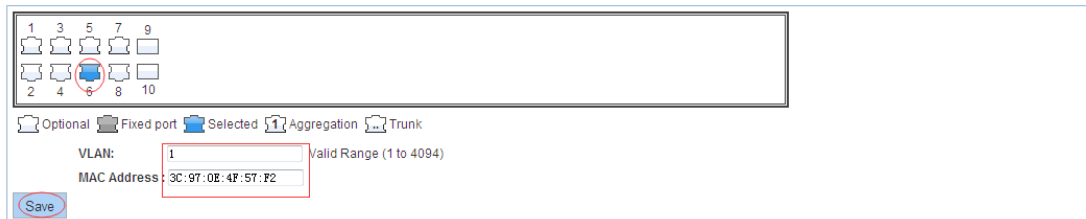
【Instruction】

Clear Mac address according to different conditions, view / add / learn Mac address, Mac address filtering.

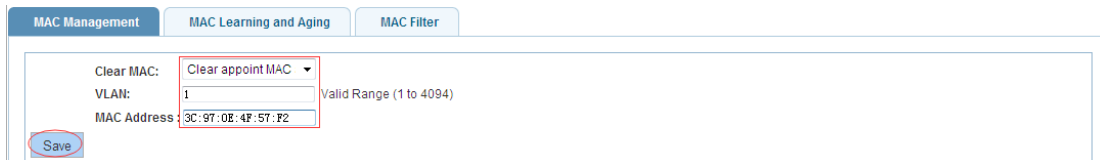
【Configuration example】

Such as:

- 1) The port 6 Mac set to static Mac.

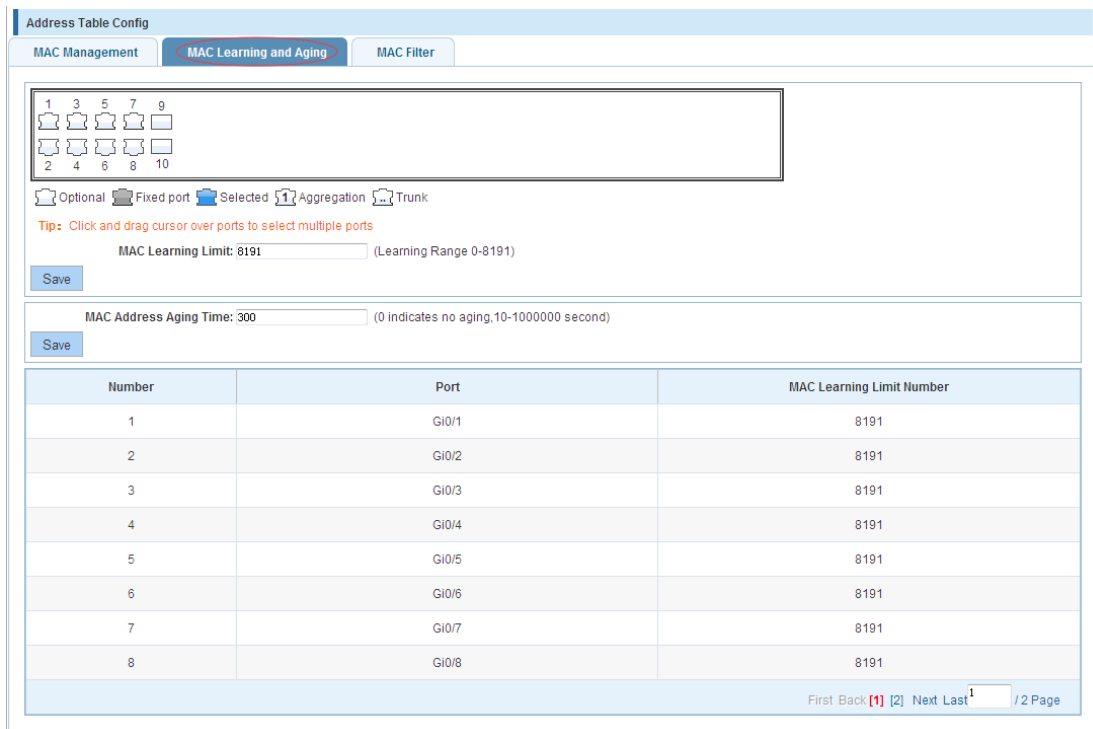


- 2) Clear port 6 static Mac addresses.



4.13.2 Mac study and aging

In the navigation bar to select "Address table>Mac study and aging". Can be set up port Mac address study limit and Mac address aging time. The following picture:



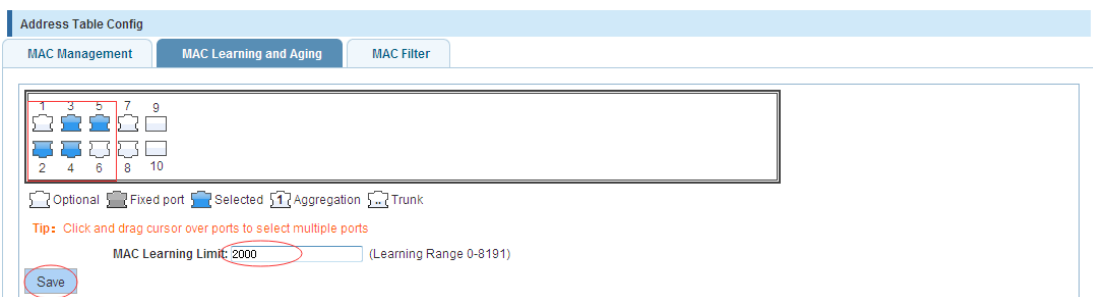
【Parameter Description】

Parameter	Description
Mac address	Range 0-8191,default 8191
Mac address study limit	Default 300

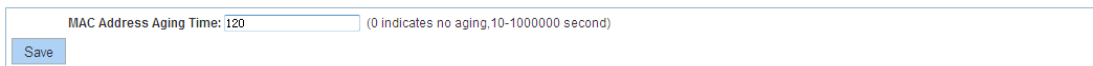
【Configuration example】

Such as:

Setting port 2,3,4,5 address study limit for 2000.



The port equipment dropped or to learn the Mac address after 2 minutes from the Mac address table automatically disappear.



4.13.3 Mac address filtering

In the navigation bar to select "Address table>Mac address filtering". Can be filtered according to the condition does not need the Mac address. The following picture:

【Parameter Description】

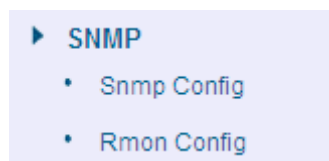
Parameter	Description
Mac address	Can not add multicast Mac address
VLAN	VLAN number
Filtering direction	Can choose the following kinds: Both Destination filter Source filter

【Configuration example】

Such as: the Mac address for 02:20:15:09:12:12 added to the filter in the table.

4.14 SNMP

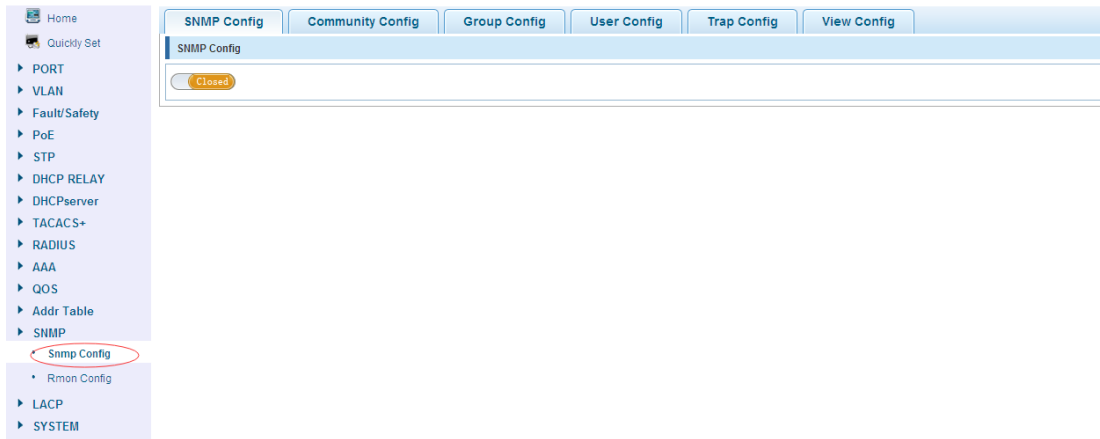
In the navigation bar to select "SNMP", you can set to the **Sntp config** and **Rmon config**.



4.14.1 Snmp config

4.14.1.1 Snmp config

In the navigation bar to select "Snmp >Snmp config", you can Snmp function enable.the following picture:



【Instruction】

The SNMP function must be turned on in the configuration RMON, otherwise it will be configured to fail.

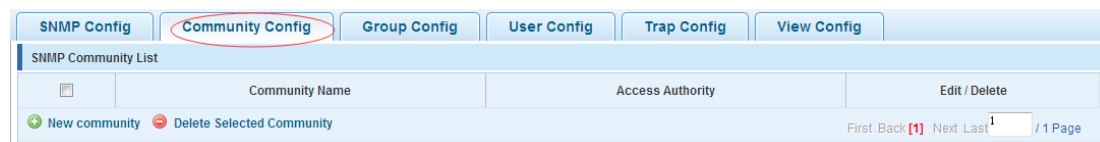
【Configuration example】

Such as: open Snmp.



4.14.1.2 Community config

In the navigation bar to select "Snmp >Snmp config>community config". Can specify group access. The following picture.



【Parameter Description】

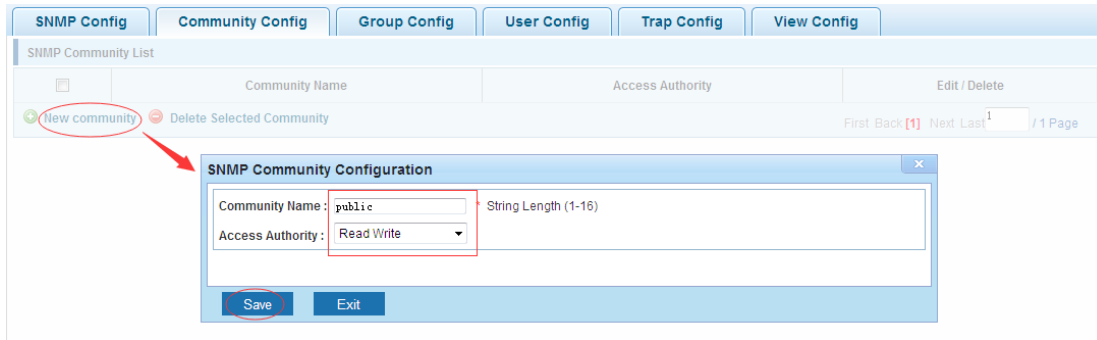
Parameter	Description
group	Community string, is equal to the NMS and Snmp agent communication between the password
Access authority	Read-only: specify the NMS (Snmp host) of MIB variables can only be read, cannot be modified Read-only can write: specify the NMS (Snmp host) of MIB variables can only read, can also be modified

【Instruction】

The upper limit of the number of groups is 8.

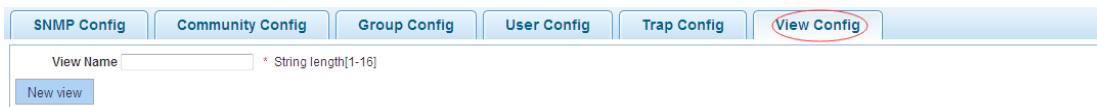
【Configuration example】

Such as: add a read-write group called public.



4.14.1.3 View Config

In the navigation bar to select "Snm > Snm Config > View Config". Set the view the rules to allow or disable access to some of the MIB object. The following picture.



【Parameter Description】

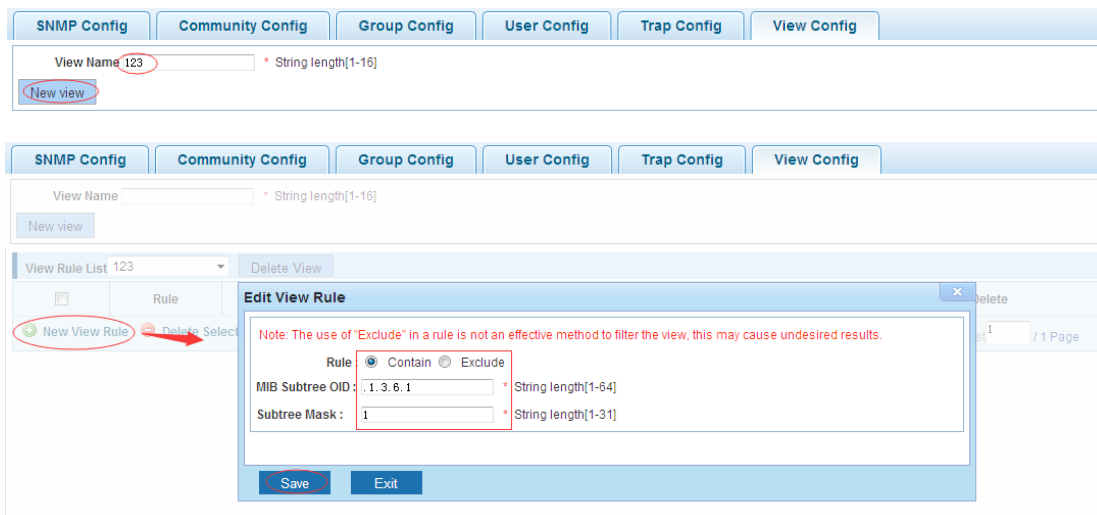
Parameter	Description
View name	View mane
include	Indicate the MIB object number contained within the view
exclude	Indicate the MIB object son number was left out of view
MIB subtree OID	View the associated MIB object, is a number of MIB
subtree mask	MIB OID mask

【Instruction】

Each view is best to configure a view rule, otherwise it will affect the SNMP function.

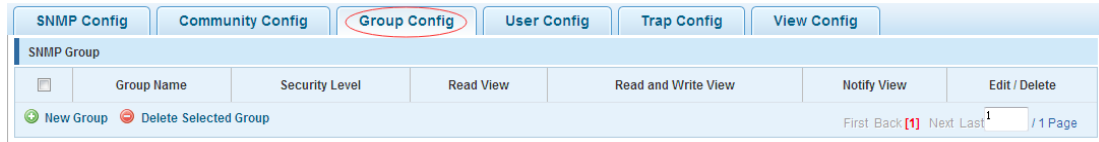
【Configuration example】

Such as: establish a view 123, MIB subtree oid .1.3.6.1 contain among them.



4.14.1.4 Group Config

In the navigation bar to select "Snm > Snm Config > Group Config", setting snmp group. The following picture.



【Parameter Description】

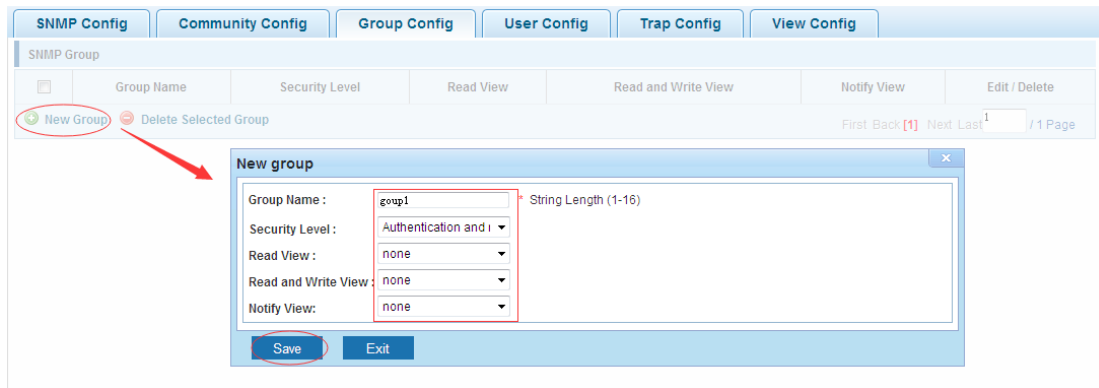
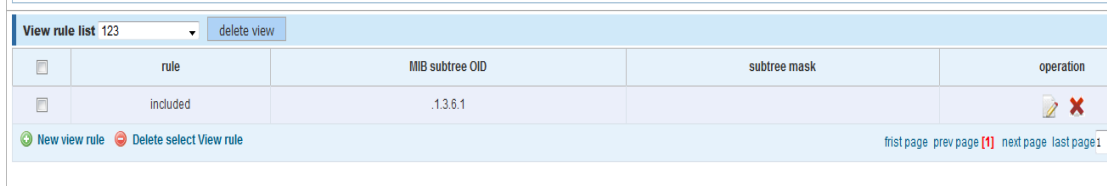
Parameter	Description
Group name	Group name
Security level	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: this group of users' messages don't need to verify data transmission also does not need to be kept secret Both authentication and encryption: this group of users need to verify the news of transmission and transmission of data need to be kept secret
Read view、read and write view、study view	The associated view name

【Instruction】

Before the cap on the number set of configuration of 8, the new group needs a new view to create a group.

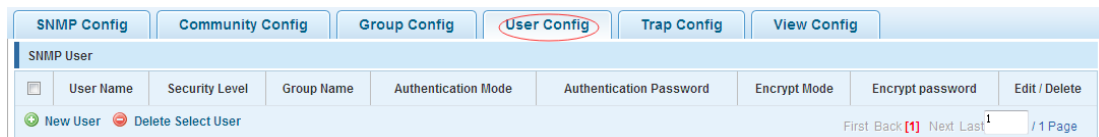
【Configuration example】

Such as: firstly, new view 123, then new group of goup1.



4.14.1.5 User config

In the navigation bar to select "Sntp>Sntp Config>User Config", setting Sntp user. The following picture:



【Parameter Description】

Parameter	Description
User name	User name,range 1-16
Security level	Attestation not only encryption: this group of users transmission of the message need to verify the data don't need to confidential No authentication encryption: this group of users' messages don't need to verify data transmission also does not need to be kept secret Both authentication and encryption: this group of users need to verify the news of transmission and transmission of data need to be kept secret
Authentication mode	Specified use MD5 authentication protocol or SHA authentication protocol
Authentication password	Range 8-10
encrypt mode	Specified using AES encryption protocol or DES encryption protocol
Group name	A user group name
encrypt password	Range 8-60

【Instruction】

The upper limit of the number of users is 8, the need to build a new view and the group can be used, the user's security level needs to be consistent with the group's security level. Add a user to use the authentication and encryption methods, and configure the user group, the user will be used for Snmpv3 connection.

【Configuration example】

Such as: new view 123, the newly built group group1, new users user1.

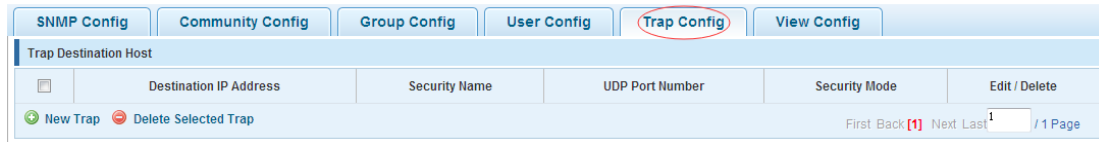
The screenshot shows the 'SNMP User' configuration page. At the top, there are tabs for 'SNMP Config', 'Community Config', 'Group Config', 'User Config', 'Trap Config', and 'View Config'. Below the tabs, there is a table with columns for 'User Name', 'Security Level', 'Group Name', 'Authentication Mode', 'Authentication Password', 'Encrypt Mode', 'Encrypt password', and 'Edit / Delete'. A 'New User' button is circled in red, and an arrow points to the 'Edit SNMP user' dialog box. The dialog box contains the following fields:

- User Name: user1 (String Length (1-16))
- Security Level: Authentication and (dropdown)
- Group Name: group1 (dropdown)
- Authentication Mode: MD5 (dropdown)
- Authentication Password: 12345678 (String Length (8-60))
- Confirm Authentication Password: 12345678
- Encrypt Mode: DES (dropdown)
- Encrypted Password: (String Length (8-60))
- Confirm Encrypted Password: (String Length (8-60))

At the bottom of the dialog box, there are 'Save' and 'Exit' buttons. The 'Save' button is circled in red.

4.14.1.6 Trap

In the navigation bar to select "Snmp>Snmp Config>Trap". Can specify sent the trap messages to Snmp host (NMS). The following picture:



【Parameter Description】

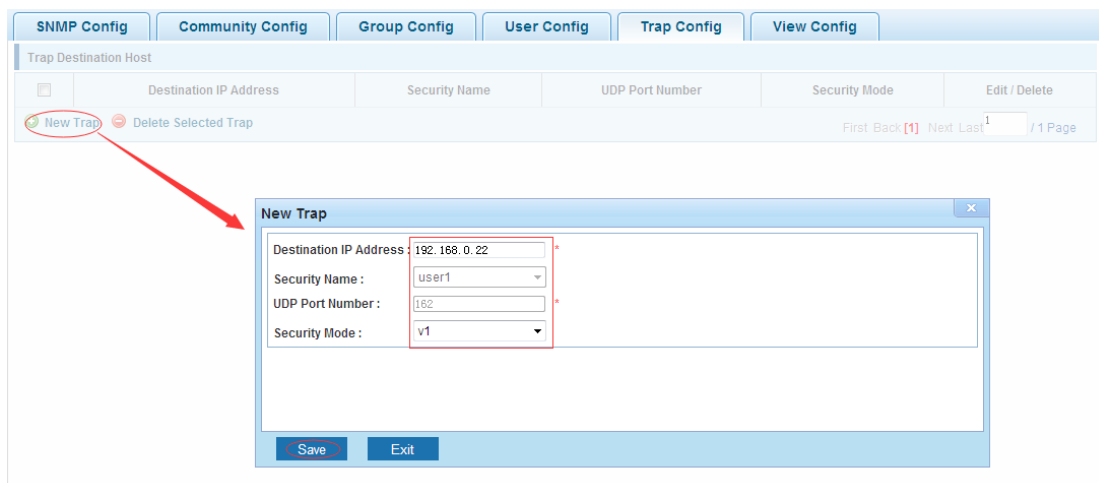
Parameter	Description
Destination ip address	Snmp host ipv4 address
Security name	Snmp user name
version	V1、 V2、 V3
Security mode	Specified using AES encryption protocol or DES encryption protocol
Group name	User group name

【Instruction】

The upper limit of the number of Trap configuration is 8, you can configure a number of different Snmp host to receive trap messages. Trigger the trap message: port Linkup/LinkDown and equipment of cold start (power down reset) / warm-start (hot restart), and Rmon set the port port statistical on under the threshold.

【Configuration example】

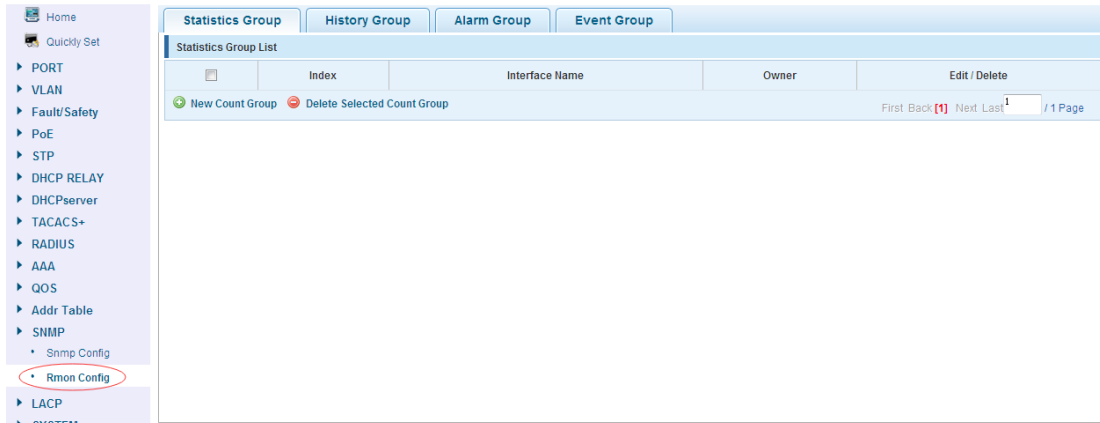
Such as: setting host 192.168.2.30 receive trap information.



4.14.2 Rmon Config

4.14.2.1 Statistics Group

In the navigation bar to select "**Snmp>Rmon Config>Statistics Group**", Set an Ethernet interface statistics. The following picture:



【Parameter Description】

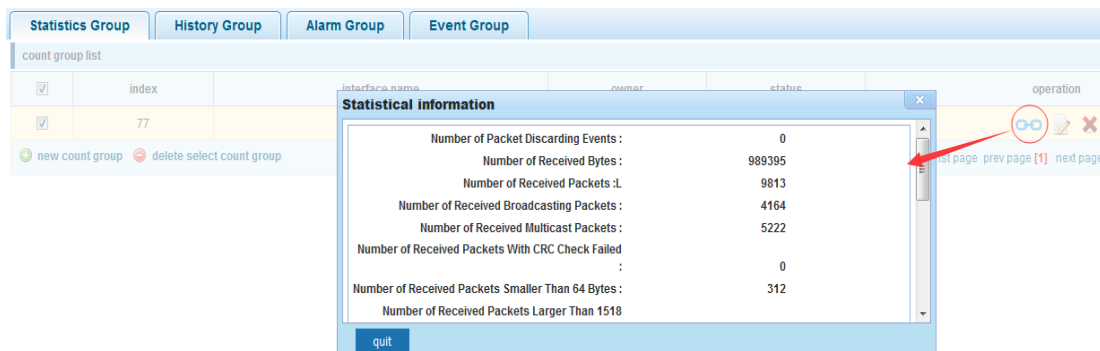
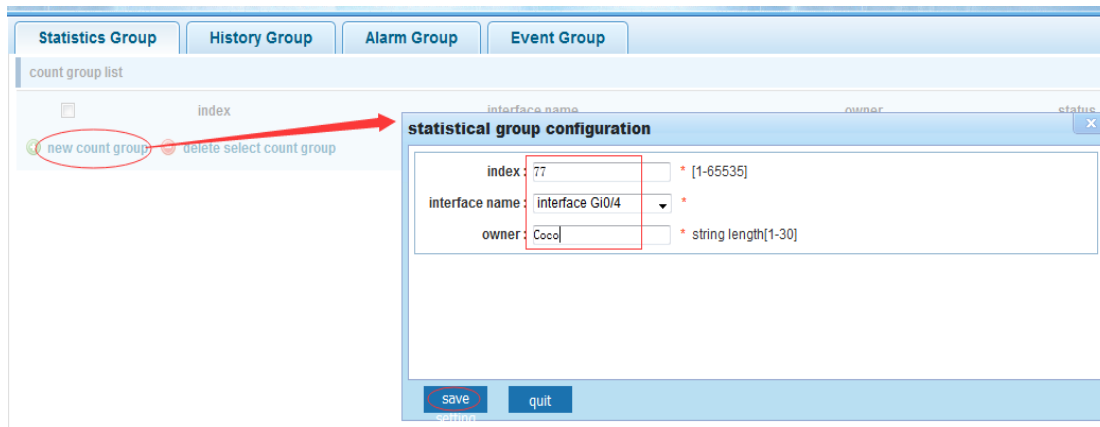
Parameter	Description
index	The index number, the value range of statistical information table is 1 ~ 65535
Interface mane	To monitor the source port
ower	Set the table creator, range: 1 ~ 30 characters of a string

【Instruction】

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will appear.

【Configuration example】

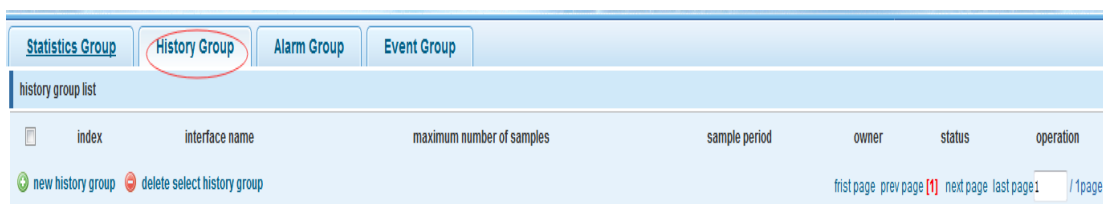
Such as: set up monitoring Ethernet port after 4 to check the data.



4.14.2.2 History Group

In the navigation bar to select "Snmp>Rmon Config>History Group". Record the history

of an Ethernet interface information. The following picture.



【Parameter Description】

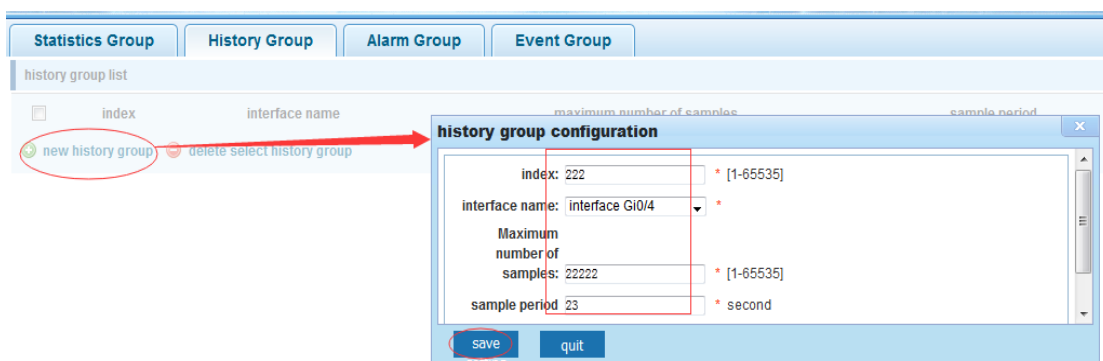
Parameter	Description
index	Historical control table item index number, value range is 1 ~ 65535
Interface name	To record the Ethernet interface
Maximum number of samples	Set the history control table item of the corresponding table capacity, namely the Max for number of records the history table, value range is 1 ~ 65535
Sample period	Set up the statistical period, scope for 5 ~ 3600, the unit is in seconds
owner	Set the table creator, range: 1 ~ 30 characters of a string

【Instruction】

Snm function must be turned on when configuring the Rmon, otherwise the prompt box will pop up.

【Configuration example】

Such as: monitor Ethernet port 4 historical information.



4.14.2.3 Event Group

In the navigation bar to select "Snmp > Rmon Config > Event Group". The way in which define events trigger and record them. The following picture.



【Parameter Description】

Parameter	Description
-----------	-------------

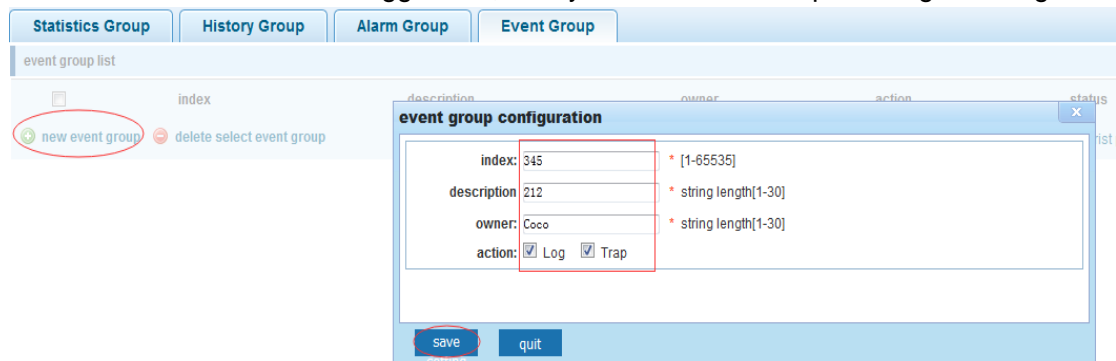
index	The index number, the value range of the event table is 1 ~ 65535
Description	The Trap events, when the event is triggered, the system will send the Trap message, Log events, when the event is triggered, the system will log
owner	Set the table creator, ownername for 1 ~ 30 characters of a string

【Instruction】

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will pop up.

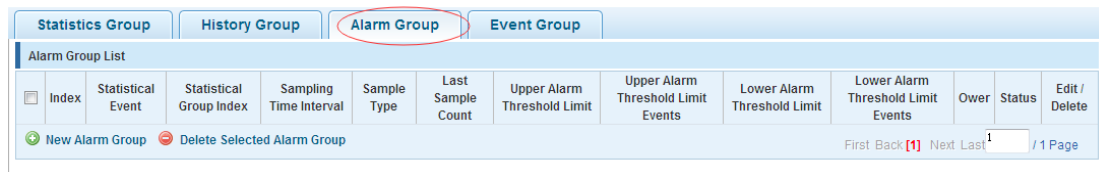
【Configuration example】

Such as: create an event to trigger 345, the system sends the trap message and log.



4.14.2.4 Alarm Group

In the navigation bar to select "Snmp>Rmon Config>Alarm Group", define alarm group. The following picture.



【Parameter Description】

Parameter	Description
index	The alarm list items index number, value range is 1 ~ 65535
Static table	Statistical type values :3:DropEvents. 4:Octets. 5:Pkts. 6:BroadcastPkts. 7:MulticastPkts. 8:CRCAAlignErrors. 9:UndersizePkts. 10:OversizePkts. 11:Fragments. 12:Jabbers. 12:Collisions. 14:Pkts64Octets. 15:Pkts65to127Octets. 16:Pkts128to255Octets. 17:Pkts256to511Octets. 18:Pkts512to1023Octets. 19:Pkts1024to1518Octets
statistical index	Set up the corresponding statistics statistical index number, decided to statistics to monitor the port number
Sampling interval	Sampling time interval, the scope for 5 ~ 65535, the unit for seconds

The sampling type	Sample types for the absolute value of sampling, the sampling time arrived directly extracting the value of a variable
The latest sampling	Sampling type for change value sampling, extraction of the arrival of the sampling time is variable in the change of the sampling interval value
The alarm threshold upper limit	Set the upper limit the Parameter values
The alarm threshold lower limit	Set the lower limit Parameter values
Above/below the threshold limit of events	Upper/lower limit reached, for each event
owner	Set the table creator, ownername for 1 ~ 30 characters of a string

【Instruction】

At the time of configuration Rmon Snmp functions must be open, otherwise the prompt dialog box will pop up. This configuration need to configure statistics groups and events.

【Configuration example】

Such as: new statistics group of 77 and the event group 345, set up more than 12 and below the lower limit 3, Beyond the scope of alarm.

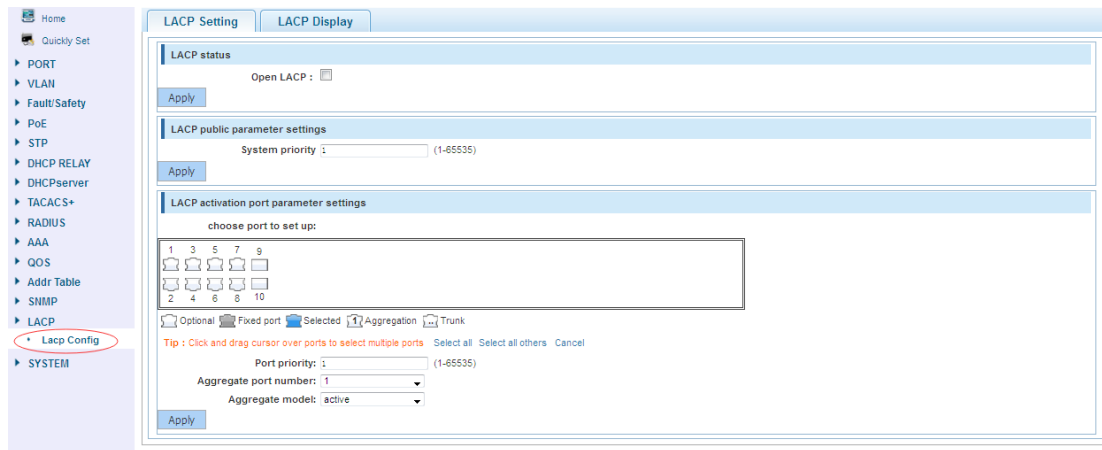
The screenshot shows the 'Alarm Group Configuration' dialog box. The fields are as follows:

- Index: 123
- Statistical Event: DropEvents
- Statistical Group Index: 77
- Sampling Time Interval: 123
- Sample Type: Absolute
- Owner: Coco
- Upper Alarm Threshold Limit: 12
- Upper Alarm Threshold Limit Events: 456
- Lower Alarm Threshold Limit: 3
- Lower Alarm Threshold Limit Events: 456

The 'Save' button at the bottom left of the dialog is circled in red. In the background, the 'New Alarm Group' button in the 'Alarm Group List' table is also circled in red.

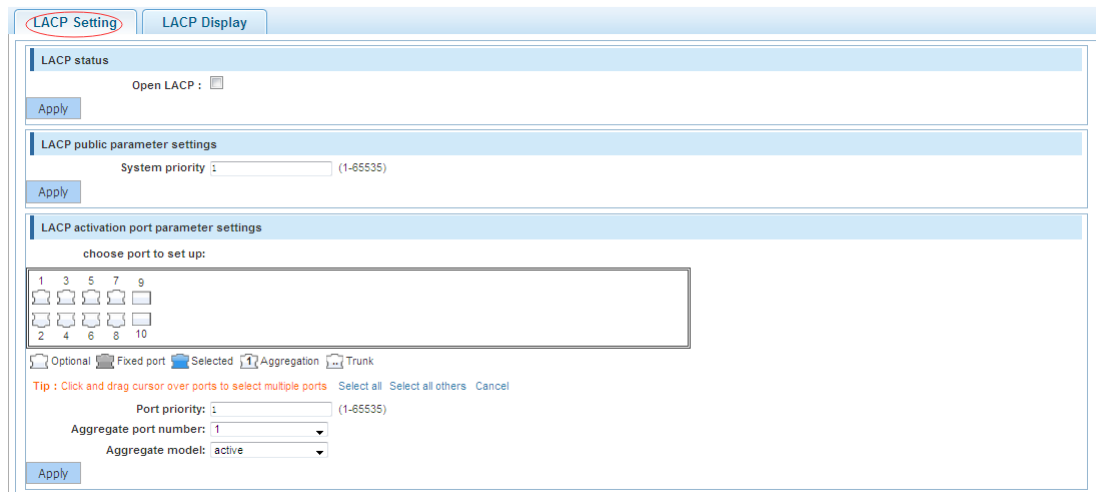
4.15 LACP

In the navigation bar to select "LACP", you can set to the "LACP Setting" and "LACP Display".



4.15.1 LACP Setting

In the navigation bar to select "LACP>LACP Setting", You can configure LACP information.



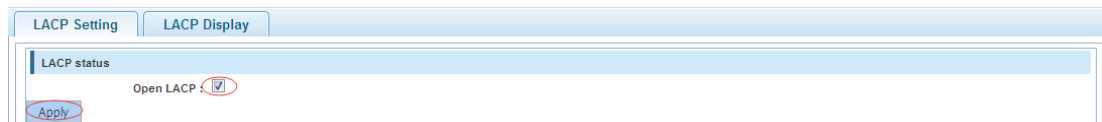
【Instruction】

LACP based on IEEE802.3ax is an implementation of dynamic link Aggregation Protocol. LACP Protocol LACPDU interacts with the side information.

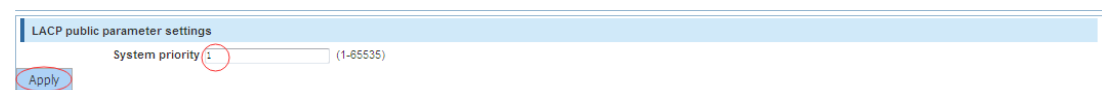
【Configuration example】

Such as:

1. LACP enabled features.



2. Setting the system priority of 1.



3. Select port 3, set priority to 1, select the aggregation port is 1, Aggregate model is active.

LACP activation port parameter settings

choose port to set up:

1	3	5	7	9
2	4	6	8	10

Optional Fixed port Selected Aggregation Trunk

Tip : Click and drag cursor over ports to select multiple ports. Select all Select all others Cancel

Port priority: 1 (1-65535)

Aggregate port number: 1

Aggregate model: active

Apply

4.15.2 LACP Display

In the navigation bar to select "LACP>LACP Display", This is where you can view or Delete LACP configurations.

LACP Setting **LACP Display**

LACP list

Aggregate ID	Port ID	Port status flag	Port state	Priority	Port operation key	Port number	Lacp Protocol state	Lacp Partner State	Operation
1	Gi0/3	SA	down	1	2	3	0x4d000000	0x41000000	
3	Gi0/5	SP	down	1	7	5	0x4c000000	0x41000000	

First Back [1] Next Last: / 1 Page

【Instruction】

LACP based on IEEE802.3ax is an implementation of dynamic link Aggregation Protocol. LACP Protocol LACPDU interacts with the side information.

【Configuration example】

Such as:Delete LACP configurations.

LACP Setting **LACP Display**

LACP list

Aggregate ID	Port ID	Port status flag	Port state	Priority	Port operation key	Port number	Lacp Protocol state	Lacp Partner State	Operation
1	Gi0/3	SA	down	1	2	3	0x4d000000	0x41000000	
3	Gi0/5	SP	down	1	7	5	0x4c000000	0x41000000	

First Back [1] Next Last: / 1 Page

4.16 SYSTEM

In the navigation bar to select "SYSTEM", you can set to the **System Config, System Update, Config Management, Config Save, Administor Privileges** and **Info Collect**.

- ▶ SYSTEM
 - System Config
 - System Update
 - Config Managem...
 - Config Save
 - Administrator Pri...
 - Info Collect

4.16.1 System Config

4.16.1.1 System settings

In the navigation bar to select "**SYSTEM>System Config>System settings**", Basic information set switch. The following picture:

【Parameter Description】

Parameter	Description
Device name	switch name
Manage VLAN	Switches use VLAN management
Manage ip	Switch IP address management
timeout	Don't use more than login timeout after login to log in again

【Configuration example】

Such as:

- 1) Set up the VLAN 2 is management VLAN, should first created vlan 2 the VLAN Settings and set a free port in the VLAN 2.

System Settings System Restart

Basic System Information

Management VLAN: 1 *

Management IP: 192.168.0.1 *

Subnet Mask: 255.255.255.0 *

Default Gateway: 192.168.0.221

Jumbo Frame: 1518 (1518-9216)

DNS Server: 0.0.0.0

Login Timeout
(Minutes): 30

Save Set Management VLAN

System Settings System Restart Password EEE Enable SSH Login Telnet Login System Log

Basic System Information

Management VLAN: 2 *

Management IP: 192.168.0.2 *

Subnet Mask: 255.255.255.0 *

Default Gateway: 192.168.0.221

Jumbo Frame: 1518 (1518-9216)

DNS Server: 0.0.0.0

Login Timeout
(Minutes): 30

Device MAC: D4:68:BA:09:11:DF

Ipv6 Address:

Device Name: Switch

Device Location:

Contacts(include mailbox):

Save Cancel settings

- 2) Insert the PC interface 3 ports, set up the management IP for 192.168.0.15, device name is yoyo, timeout for 20 minutes, Jumboframe for 5000.

System Settings System Restart Password EEE Enable SSH Login Telnet Login System Log

Basic System Information

Management VLAN: 2 *

Management IP: 192.168.0.15 *

Subnet Mask: 255.255.255.0 *

Default Gateway: 0.0.0.0

Jumbo Frame: 5000 (1518-9216)

DNS Server: 0.0.0.0

Login Timeout
(Minutes): 20

Device MAC: D4:68:BA:09:11:DF

Ipv6 Address:

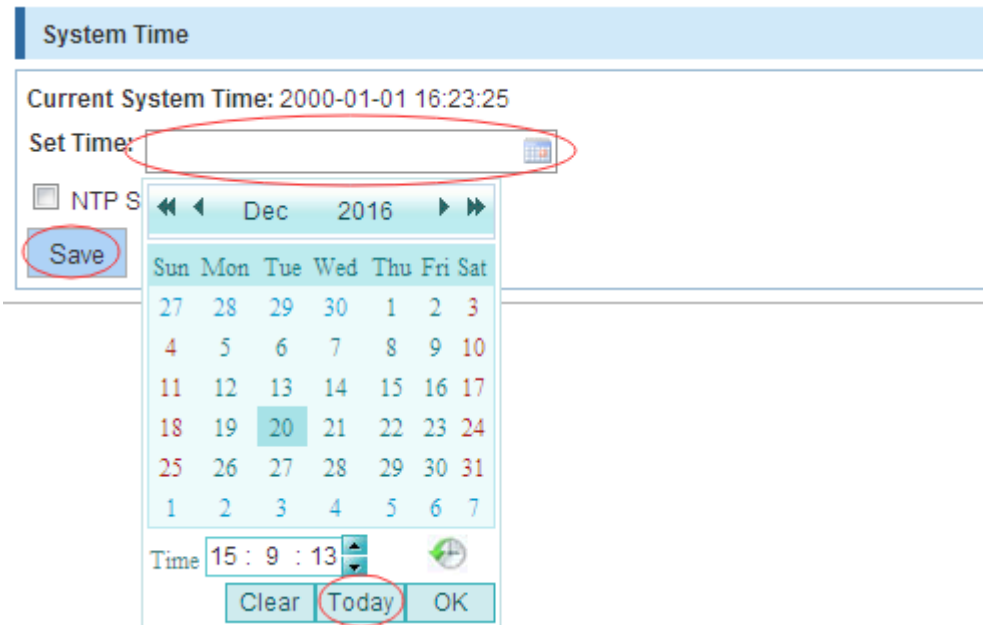
Device Name: yoyo

Device Location:

Contacts(include mailbox):

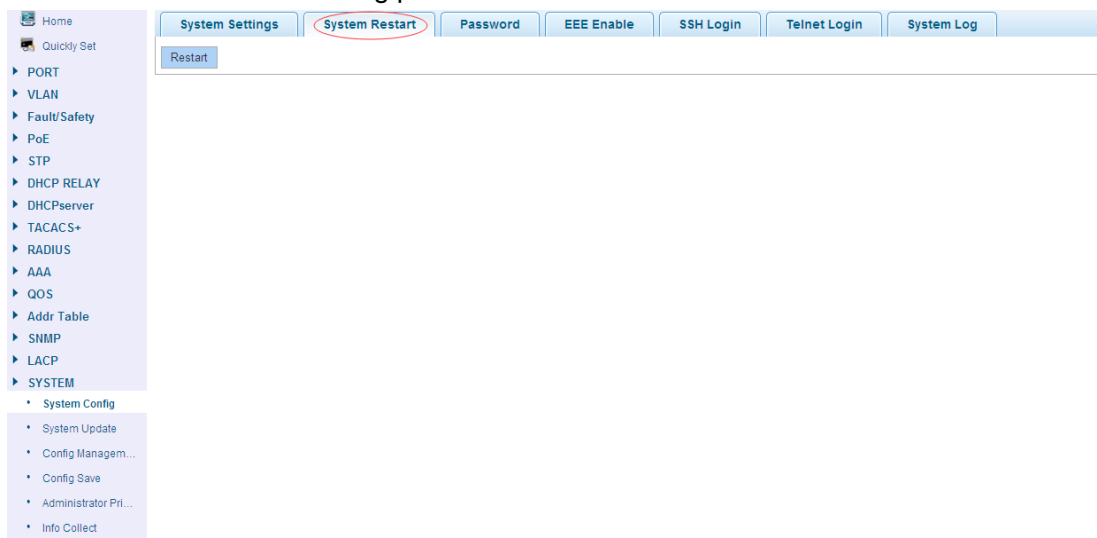
Save Set Management VLAN

- 3) Use 192.168.0.15 logging in, sets the system time.



4.16.1.2 System restart

In the navigation bar to select **"SYSTEM>System Config>System restart"**, equipment can be restarted. The following picture:

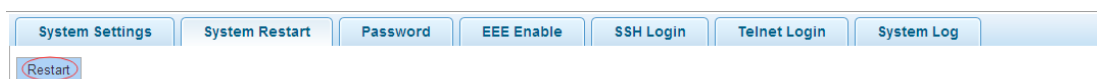


【Instruction】

Click the button to restart the switch. The restart process may take 1 minute. Please wait patiently. The page will be refreshed automatically after device restart.

【Configuration example】

Such as:click "Restart" button.



4.16.1.3 Password change

In the navigation bar to select **"SYSTEM>System Config>Password change"**, The password change to equipment. The following picture:

Home

Quickly Set

- PORT
- VLAN
- Fault/Safety
- PoE
- STP
- DHCP RELAY
- DHCPserver
- TACACS+
- RADIUS
- AAA
- QOS
- Addr Table
- SNMP
- LACP
- SYSTEM
 - System Config
 - System Update
 - Config Managem...
 - Config Save
 - Administrator Pri...
 - Info Collect

System Settings System Restart **Password** EEE Enable SSH Login Telnet Login System Log

Change Administrator Password

Password type: Encrypted password

Old Password: *

New Password: *

Confirm New Password: *

Save Clear

【Instruction】

1. If you set a new Web login password, then log in again after setting the new password.
2. Password can not contain Chinese, full-width characters, question marks and spaces.
3. If forget the password reset, can be reset in the console.

switch(config)# password **admin**

New Password: **1234**

Confirm Password: **1234**

【Configuration example】

Such as: amend the password to 1234.

System Settings System Restart Password EEE Enable SSH Login Telnet Login System Log

Change Administrator Password

Password type: Encrypted password

Old Password: ●●●●●

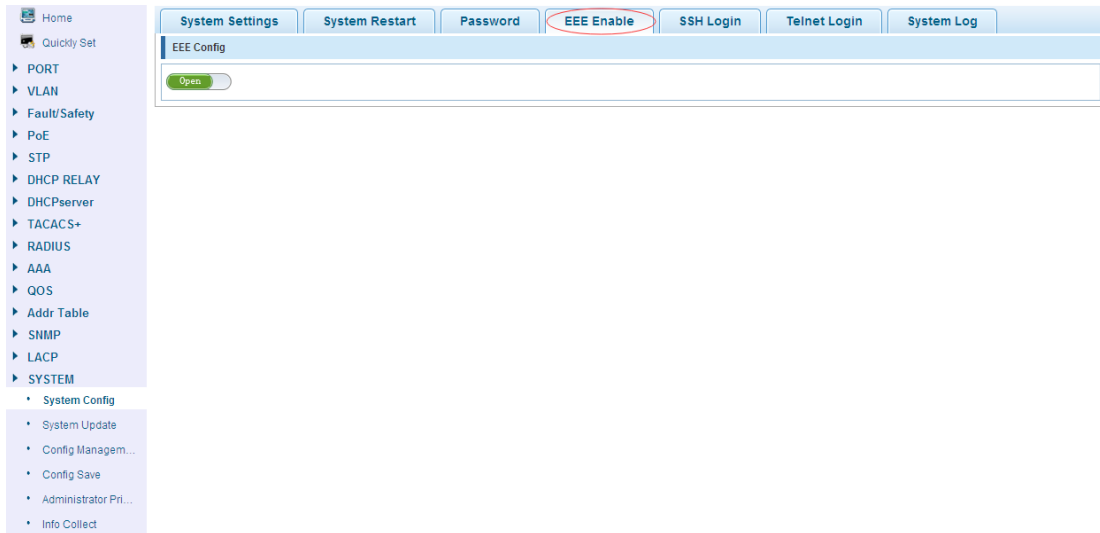
New Password: ●●●●●

Confirm New Password: ●●●●●

Save Clear

4.16.1.4 EEE Enable

In the navigation bar to select "SYSTEM>System Config>EEE Enable"EEE open. The following picture:

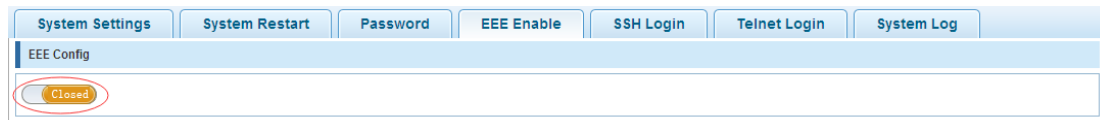


【Instruction】

Energy Efficient Ethernet, Open the EEE features by default.

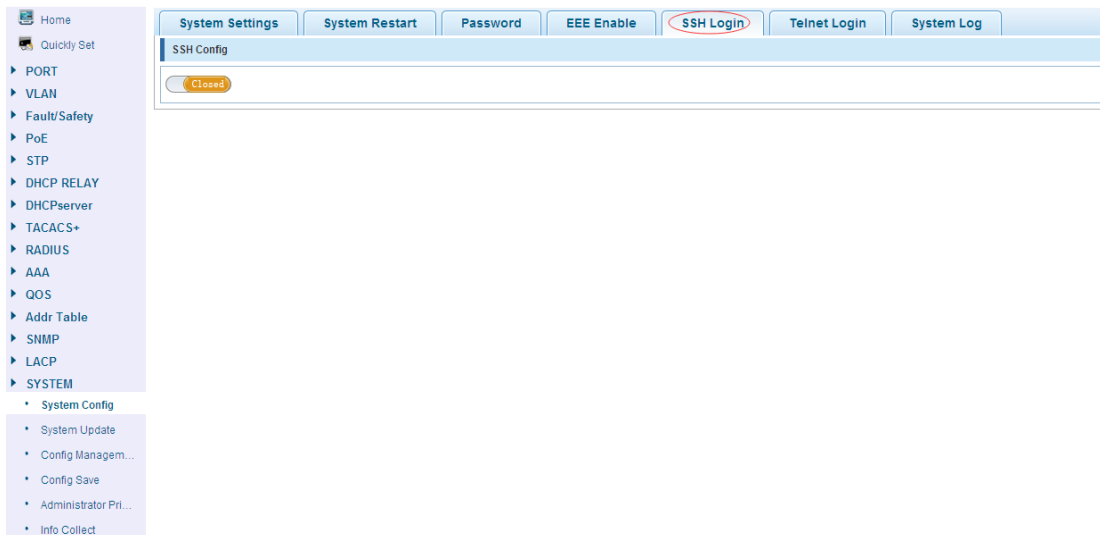
【Configuration example】

Such as: EEE closed.



4.16.1.5 SSH login

In the navigation bar to select "SYSTEM>System Config>ssh login", SSH open. The following picture:

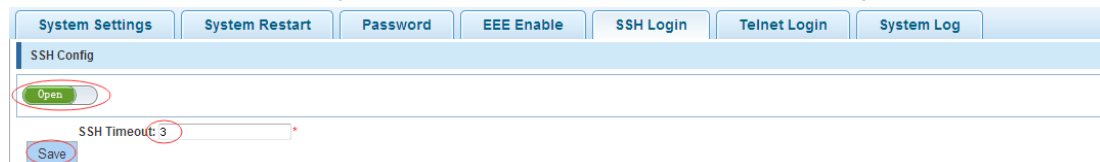


【Instruction】

Configure the user to be able to switch through the SSH login device.

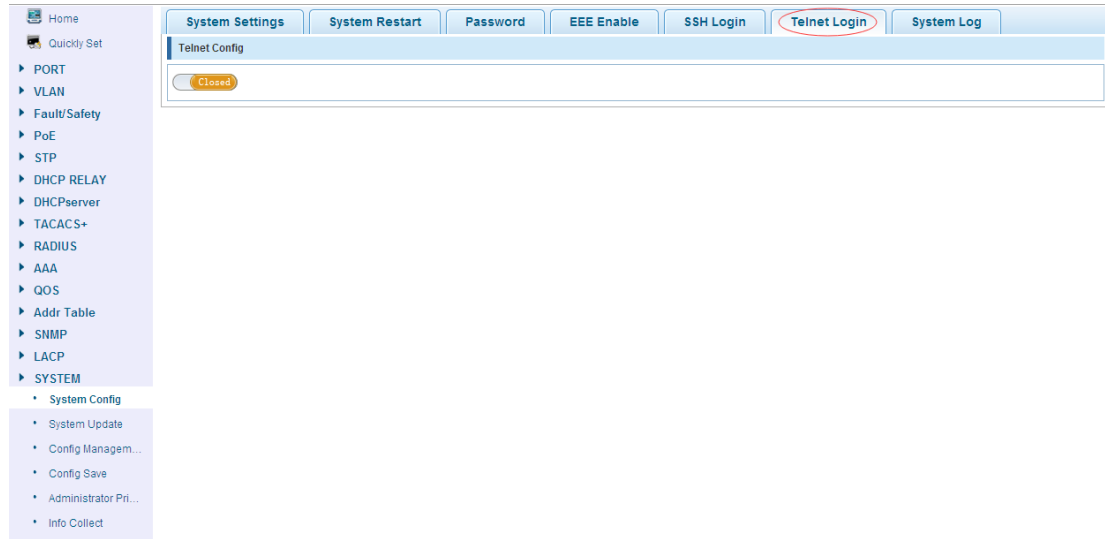
【Configuration example】

Such as: SSH open, setting the time-out time is 3, you can CRT to login.



4.16.1.6 Telnet login

In the navigation bar to select **"SYSTEM>system config>Telnet login"**. Telnet open. The following picture:



【Instruction】

Configure the user to be able to switch through the Telnet login device.

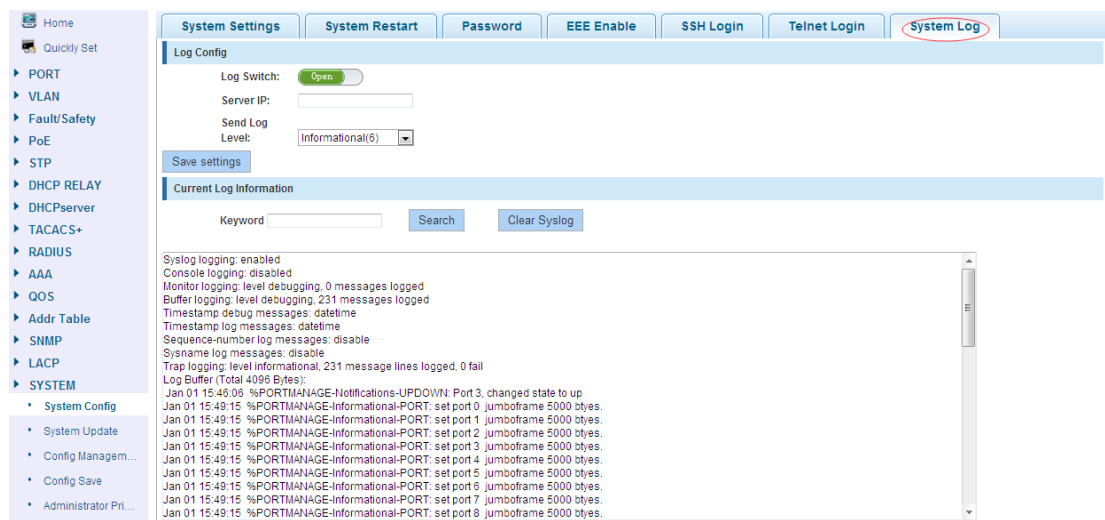
【Configuration example】

Such as: Telnet open, PC Telnet function open, setting the time-out time is 3, you can login.



4.16.1.7 System log

In the navigation bar to select **"SYSTEM>Password change>System log"**, to view the log and set up the log server. The following picture:



【Parameter Description】

Parameter	Description
-----------	-------------

Log switch	Open and close
Server ip	Appoint to server address
Send log level	0-7
key	Enter the required query of characters

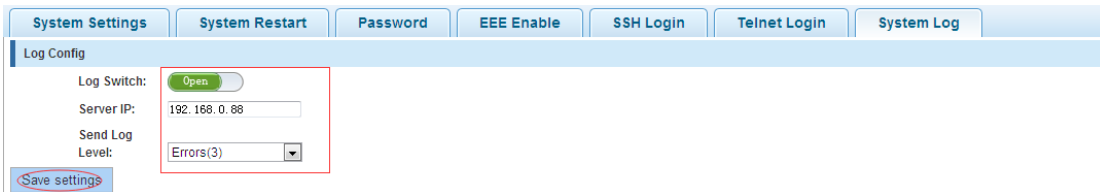
【Instruction】

Open log switch, set up the syslog server, system log will automatically be pushed to the server.

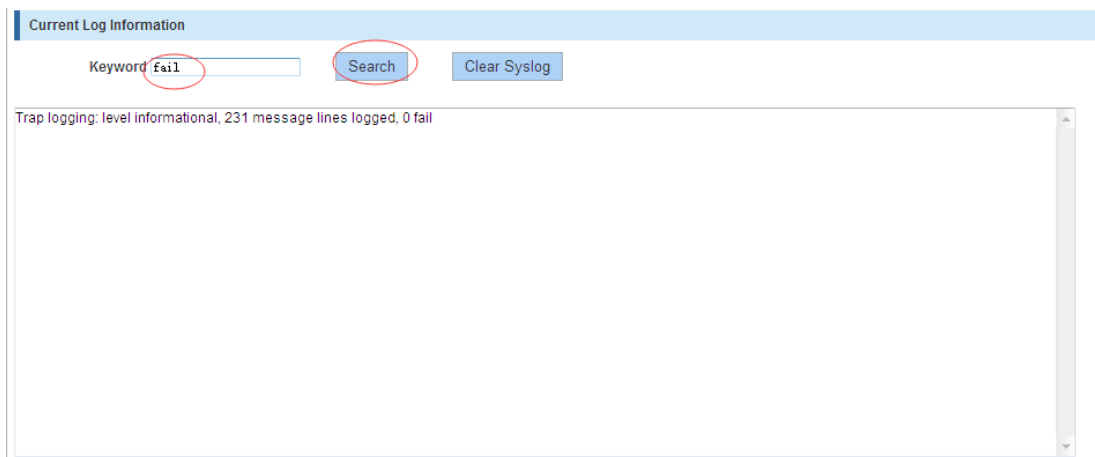
【Configuration example】

Such as:

- 1) The error log information in 192.168.0.88 pushed to the server.

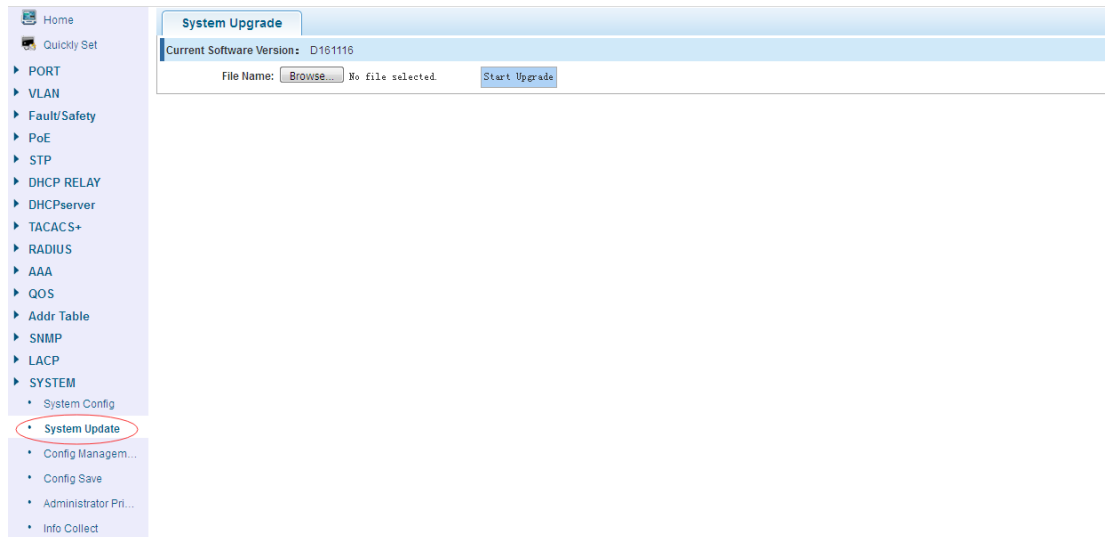


- 2) Input the fail keywords, click "Search" button, click on the "Clear Syslog" button, can clear the log.



4.16.2 System Upgrade

In the navigation bar to select "SYSTEM>system upgrade", Optional upgrade file to upgrade. the following picture.



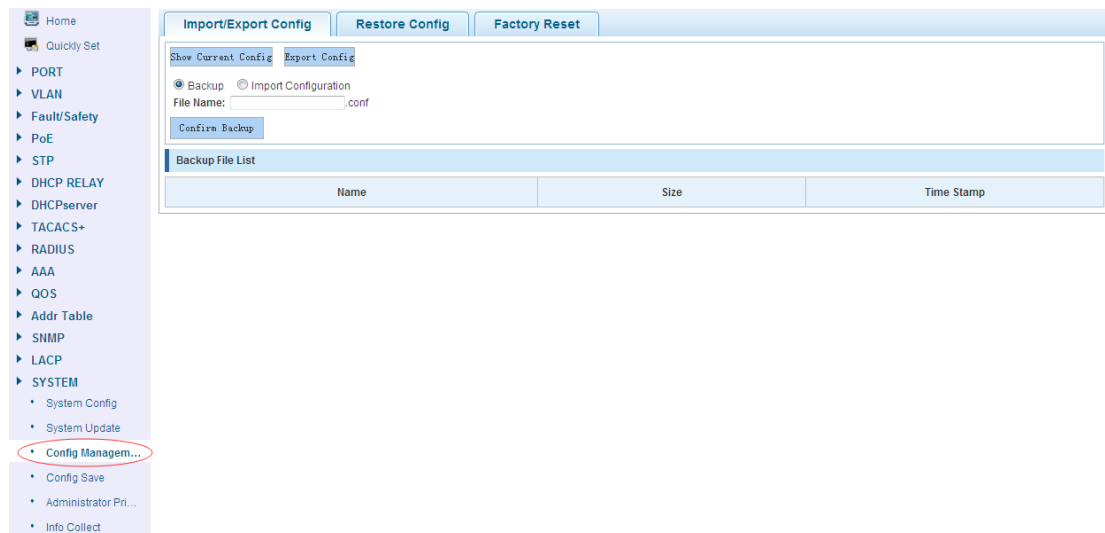
【Instruction】

1. please confirm that the upgraded version of the same model and the same model.
2. in the upgrade process, you may encounter flash to make the page is temporarily unable to respond to the page, this time can not power off or restart the device, until prompted to upgrade successfully.

4.16.3 Config Management

4.16.3.1 Current configuration

In the navigation bar to select “**SYSTEM>Config Management>Current configuration**”, can import and export configuration files, the backup file. The following picture:



【Instruction】

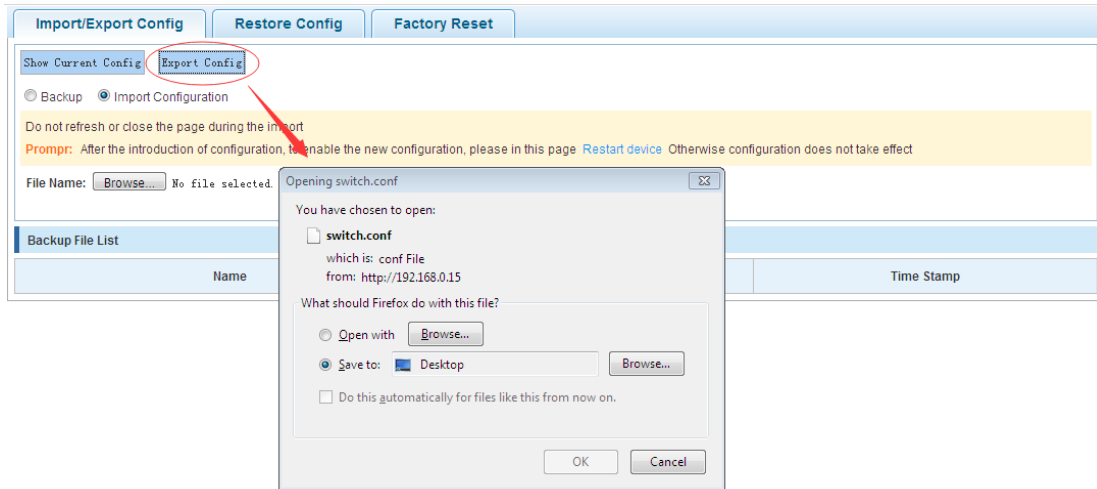
Import process can not be closed or refresh the page, or import will fail.

After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect.

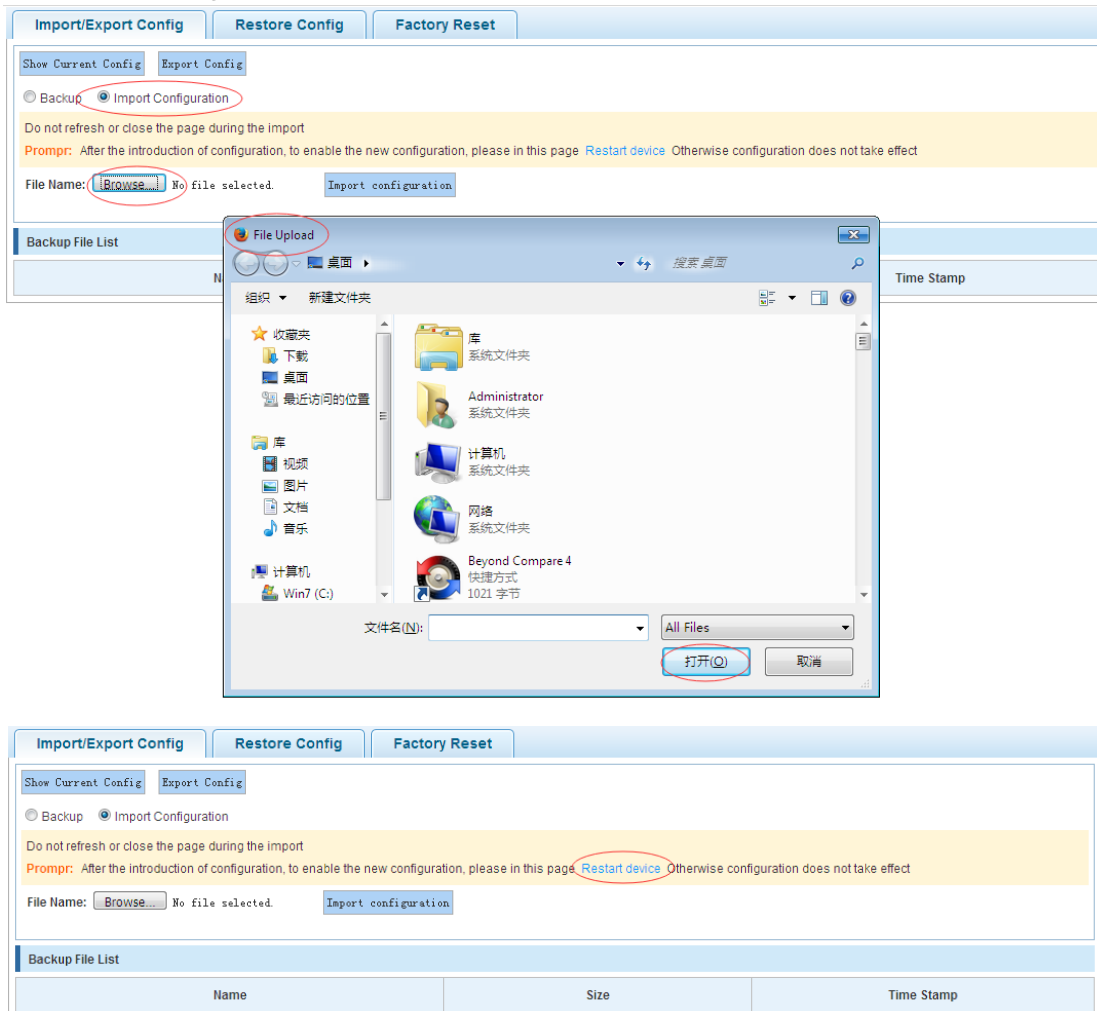
【Configuration example】

Such as:

- 1) In the configuration first save the page, click save configuration to save the current configuration, then export the configuration.



- 2) Import configuration.



- 3) Backup.

Import/Export Config Restore Config Factory Reset

Show Current Config Export Config

Backup Import Configuration

File Name: 12357 .conf

Confirm Backup

Backup File List

Name	Size	Time Stamp
------	------	------------

4.16.3.2 Configuration backup

In the navigation bar to select “**SYSTEM>Config Management>Configuration backup**”, you can configure backup file. The following picture:

Import/Export Config Restore Config Factory Reset

Name	Size	Time Stamp
<input checked="" type="radio"/> 12357.conf	5.66K	15:38:34 2016-12-20

Restore Backup Delete Backup Save Backup Rename Backup

Confirm Recovery

【Instruction】

Operating this page should be in the current configuration page first, the backup file.

【Configuration example】

Such as: restore backup.

Import/Export Config Restore Config Factory Reset

Name	Size	Time Stamp
<input checked="" type="radio"/> 12357.conf	5.66K	15:38:34 2016-12-20

Restore Backup Delete Backup Save Backup Rename Backup

Rename: swert .conf

Confirm Rename

4.16.3.3 Restore factory configuration

In the navigation bar to select “**SYSTEM>Config Management>Restore factory configuraton**”. Can export the current configuration and restore factory configuration.

The following picture:

Import/Export Config Restore Config Factory Reset

Export current config Restore to factory

【Instruction】

Restore the factory configuration, will delete the current all configuration. If the current system has a useful configuration, you can export the current configuration and then restore the factory configuration.

【Configuration example】

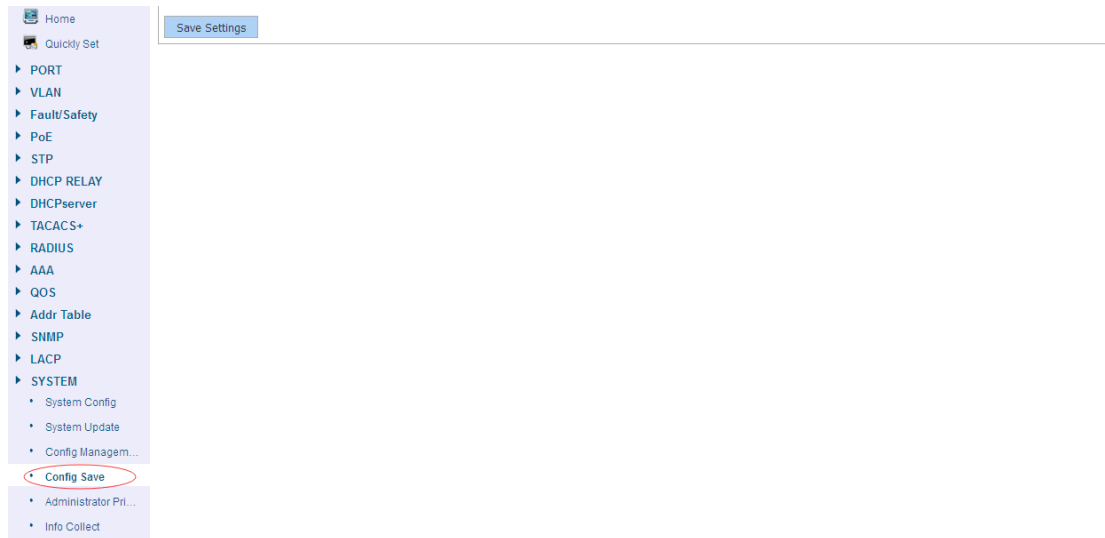
Such as: restore configuration can be the guide before they leave the current configuration.

Import/Export Config Restore Config Factory Reset

Export current config Restore to factory

4.16.4 Config Save

In the navigation bar to select “**SYSTEM>Config Save**”, you can save current configuration. The following picture.



【Instruction】

Save system configuration, will cover the original configuration. If the current system has a useful configuration, you can back up the current configuration and then save the system configuration.

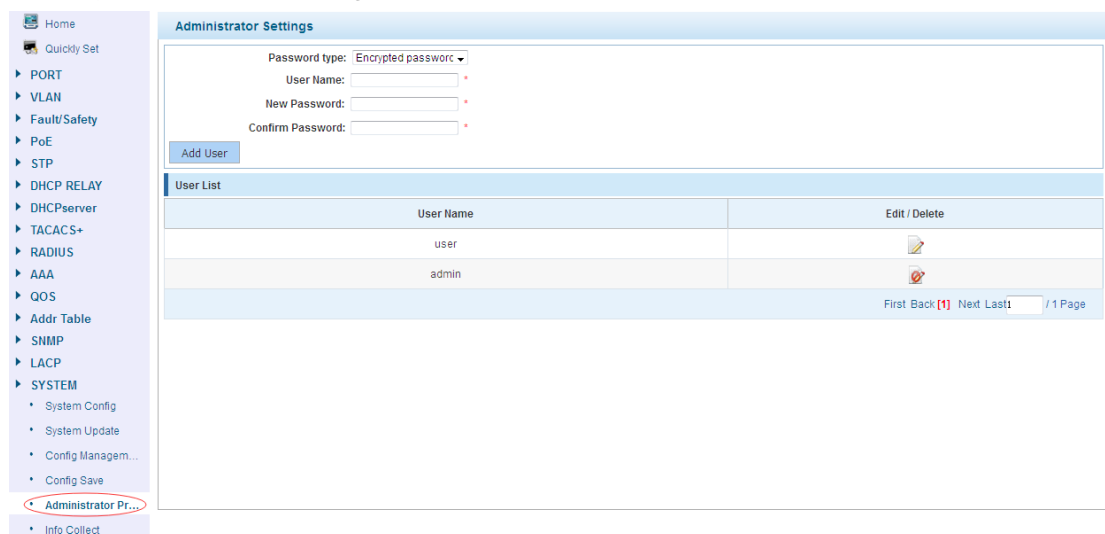
【Configuration example】

Such as: click “save settings” button.



4.16.5 Administrator Privileges

In the navigation bar to select “**SYSTEM>Administrator Privileges**”, Configurable ordinary users. The following picture.



【Instruction】

This page only the super administrator admin can access, for the management of users and visitors. The user can log on Web management system to carry on the daily

maintenance to the equipment. In addition to admin and user, up to 5 users can add. Ordinary users can only access to view the system home page information.

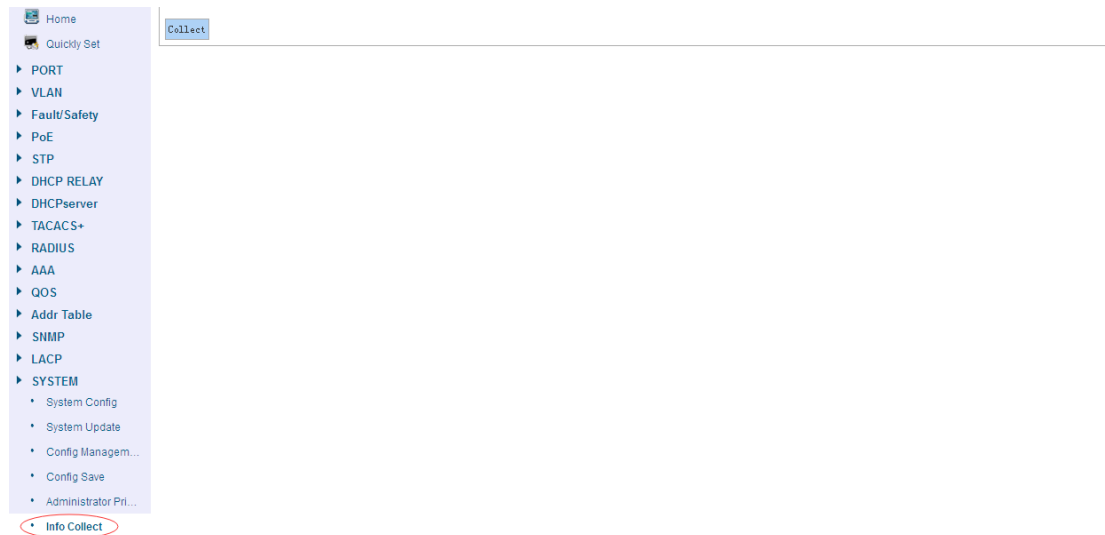
【Configuration example】

Such as:

The screenshot shows the 'Administrator Settings' interface. It includes a form for adding a user with the following fields: Password type (set to 'Encrypted password'), User Name (set to 'root'), New Password, and Confirm Password. An 'Add User' button is highlighted with a red circle. Below the form is a 'User List' table with columns for 'User Name' and 'Edit / Delete'. The table lists 'user' and 'admin' with corresponding edit and delete icons. A pagination bar at the bottom indicates 'First Back [1] Next Last1 / 1 Page'.

4.16.6 Info Collect

In the navigation bar to select “**SYSTEM>Info Collect**”. You can collect to the system debug information. The following picture.



【Instruction】

Collect useful information, it may take a few moments.

【Configuration example】

Such as: click on "Collect" button.



Appendix: Technical Specifications

Hardware Features	
Standards	IEEE 802.3i、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、IEEE 802.3z、IEEE 802.3at、IEEE 802.3af、IEEE 802.1q、IEEE 802.1p
Network Media (Cable)	10Base-T: UTP category 3, 4, 5 cable (maximum 100m) 100Base-Tx: UTP category 5, 5e cable (maximum 100m) 1000Base-T: UTP category 5e, 6 cable (maximum 100m) 1000Base-SX:62.5μ m/50μ m MMF(2m~550m) 1000Base-LX:62.5μ m/50μ m MMF(2m~550m) Or 10μ m SMF(2m~5000m)
Number of Ports	8 x 10/100/1000Mbps Auto-Negotiation ports 2 x 1000Mbps SFP ports 1 x Console port
Transfer Method	Store-and-Forward
Switching Capacity	20G
MAC Address Learning	Automatically learning, automatically update 8K Table
Frame Filtering and Forward Rate	10Mbps: 14880pps 100Mbps: 148800pps 1000Mbps: 1488000pps
Dimensions (L x W x H)	280*180*44.3 mm
Environment	Operating Temperature: 0℃~45℃ Storage Temperature: -40℃~70℃ Operating Humidity: 10%~90% non-condensing Storage humidity: 5%~90% non-condensing
Power Supply	AC 100V~240V 50/60Hz (Internal Power supply)
Power consumption	Max 161W

Web:<http://www.sundray.com> Tel:400-878-3389