

用户手册

SW-5010

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

第一章	产品介绍	1
1.1 1.2	产品概述 性能特征	1
1.3	父换机囬权况明	2
	1.3.1 交换机前面板	2
	1.3.2 父换机后面板	3
1.4	坏境	4
1.5	初品清毕	4
第二章	安装、使用方法	5
21	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
***· · <u>-</u> **		
第三章	登录交换机	8
31	连 控 列 态	0
0.1	足) 安 邦 乂] 犬 们	0
3.1	如何登录交换机	o 8
3.2	如何登录交换机	0 8
3.2 第四章	如何登录交换机	0 8 0
3.2 第四章 4.1	杜爾玛又採柳 如何登录交换机	0 8 0
3.2 第四章 4.1 4.2	建安玛文珠和 如何登录交换机	8 0 0 3
3.2 第四章 4.1 4.2	建国建筑大阪和 如何登录交换机	0 3 3
3.2 第四章 4.1 4.2	建国国家交换机	8 0 3 3 4
3.2 第四章 4.1 4.2	建国建筑大阪和 如何登录交换机	0 3 3 4 5
3.2 第四章 4.1 4.2	建国建筑建筑 如何登录交换机	0 3 3 4 5 7
3.2 第四章 4.1 4.2	建国建筑交换机 1 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1	8 0 3 4 5 7 8
3.2 第四章 4.1 4.2	建国建筑交换机 1 文换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1	8 0 3 4 5 7 8 9
3.2 第四章 4.1 4.2	建国建筑交换机 1 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2	0 3 3 4 5 7 8 9 0
3.2 第四章 4.1 4.2 4.3	建安玛文诗秋/L 如何登录交换机 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2 VLAN 管理 2	8 0 3 3 4 5 7 8 9 20
3.2 第四章 4.1 4.2 4.3	建运式文诀机 如何登录交换机 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2 VLAN 管理 2 4.3.1 VLAN 设置 2	0 3 3 4 5 7 8 9 0 1
3.2 第四章 4.1 4.2 4.3	社运过入扶机 如何登录交换机 交换机配置 1 快速配置 二 端口管理 1 4.2.1 基本设置 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2 4.3.1 VLAN 设置 2 4.3.2 Trunk 口设置	0 3 3 4 5 7 8 9 0 1 2 1 2 2
3.2 第四章 4.1 4.2 4.3	定按均又按印 如何登录交换机. 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2 VLAN 管理 2 4.3.1 VLAN 设置 2 4.3.2 Trunk 口设置 2 4.3.3 Hybrid 口设置 2	0 3 3 4 5 7 8 9 2 1 2 3 1 1 2 3 3 4 5 7 8 9 2 1 2 3
3.2 第四章 4.1 4.2 4.3 4.3	定安均文沃和 如何登录交换机. 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2 VLAN 管理 2 4.3.1 VLAN 设置 2 4.3.2 Trunk 口设置 2 故障/安全 2	0 0 0 0 0 0 0 0 0 0 0 0 0 0
3.2 第四章 4.1 4.2 4.3 4.3	在该时又快机 如何登录交换机 交换机配置 1 快速配置 1 端口管理 1 4.2.1 基本设置 1 4.2.2 端口聚合 1 4.2.3 端口镜像 1 4.2.4 端口限速 1 4.2.5 广播风暴 1 4.2.6 端口隔离 1 4.2.7 端口信息 2 VLAN 管理 2 4.3.1 VLAN 设置 2 4.3.2 Trunk 口设置 2 故障/安全 2 4.4.1 防攻击 2	0 0 0 0 0 0 0 0 0 0 0 0 0 0

4.4.1.2 防 DOS 攻击	
4.4.1.3 IP 源防护	
4.4.1.4 三元绑定	
4.4.2 通路检测	31
4.4.2.1 ping 检测	31
4.4.2.2 tracert 检测	
4.4.2.3 线缆检测	
4.4.3 ACL 访问控制	
4.4.4 802.1x	35
4.5 POE 管理	
4.5.1 POE 管理	
4.5.1.1 高级管理	
4.5.1.2 温度配置	
4.5.2 POE 端口配置	
4.5.3 POE 延迟	
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	
4.8.5 缺省网关配置	
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	
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	
4.12 QoS 管理	60
4.12.1 队列设置	
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	
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	
4.16.3.3 恢复出厂配置	
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。

O SUNDRAY			: :	:	: :	S Link/Act	àààà	Consta	
SW-5010	Reset 10	PWR		:	::	POE S Link/Act POE		-	-05

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

LED	颜色	状态	状态描述	
中派灯	UT A	长亮	通电	
电源灯	红巴	熄灭	断电	
	橙色	长亮	对应端口己连接	
Link/Act	ink/Act (10/100Mbps) (1~8) 绿色	鸠灭	对应进口去连接	
(1~8)		がいノく	/□/□/□/□/□/□/□/□/□/□/□/□/□/□/□	
	(1000Mbps)	闪烁	对应端口已连接并收发数据	
Link/Act		长亮	对应光纤端口己连接	
SFP	绿色	熄灭	对应光纤端口未连接	
(9 S~10S)		闪烁	对应光纤端口己连接并收发数据	
PoE (1~8)		长亮	对应端口己连接 PD 且 PoE 正常供电	
	黄色	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	

下表描述了交换机的每个指示灯的详细指示说明。

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的内部高能效电源供电,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;
- 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;



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)。

SUNDRAY	8-Port Gigabit Managed PoE Switch with 2 SFP Slots
请输入您的)交换机的用户名和密码!
用户名:	admin
密码:	•••••
语言	简体中文 ▼
	登录

	Y .	当前用户名: admin						▶ 退出	切换语言
系统省页	设备型号: SW-5010 序列号: G1GB0U	5007211	软件版本: D16111 硬件版本: 1.00	16	运行时间: 10 min				
 端口管理 VLAN管理 校時/支全 PoE管理 STP DHCP申 DHCP 指 DHCP 指 HCACS+ RADIUS AAA QoS管理 地址表 Samp管理 LACP 	¥IG2	设备配置 第日统计	1		7 8 Console 9F	10F) 100K	202 Diconsec	t 💼 Closed
▶ 系统管理	关键字 输入端口号或	《端口描述进行查询	查询	☑ 实时刷新流量					
		描述		输入流量(Bps)	輸出流量(Bps)	开启状态	连接状态	所属vian	trunk□
	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
							首	页上一页[1] 下一页 周	题 <mark>1 /1页</mark>

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。

	Y	当前用户名: admin						▶ 退出	切换语言
夏 系统首页 夏 失速配置	设备型号: SW-5010 序列号: G1GB0US	5007211	软件版本: D161116 硬件版本: 1.00	6	运行时间: 10 min				
 ※ は口管理 > VLAN管理 > 故肉/皮全 > PoE管理 > STP > DHCP庫券 > DHCP庫券 > DHCP庫券 > TACACS+ > RADIUS > AAA > QoS管理 > 均址表 	ĺ	-	ů	2 3 4 5 6	7 8 Console 9F	10F	с 1004 с 10004 (PDZ 💼 Unconnect	: Closed
▶ Snmp管理 ▶ LACP	端口信息	设备配置 端口统计							
▶ 系统管理	关键字 输入端口号或	湖口描述进行查询	查询	☑ 实时刷新流量					
		描述		输入流里(Bps)	输出流壁(Bps)	开启状态	连接状态	所属vian	trunk
	Gi 0/1		(0.00K	0.00K	开启	🍀 未连接	1	否
	Gi 0/2		C	0.00K	0.00K	开启	🍀 未连接	1	否
	Gi 0/3		4	460.54K	1.79M	开启	💛 连接	1	否
	Gi 0/4		0	0.00K	0.00K	开启	😽 未连接	1	否
	Gi 0/5		0	0.00K	0.00K	开启	😽 未连接	1	否
	Gi 0/6		0	0.00K	0.00K	开启	未连接	1	否
	Gi 0/7		0	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] 下一页属	页 <mark>1</mark> /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:

	Y	当前用户名: adm	in		B	退出 切换语言
📑 系統首页	VLAN设	置 其他设置				
🦷 快速配置	VLAN设置					
▶ 端口管理		VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作
▶ VLAN官理 ▶ 故陵/安全		1	VLAN0001	192.168.0.1/24	1-10	
▶ PoE管理	◎ 新建VL	AN 🤤 删除选择VLAN			首页 上一页 [1]	下一页 尾页1 /1页
► STP	Trunk设置	1				
▶ DHCP申维		端口名称	端口描述	允许	通过的Vian	操作
 TACACS+ 	◎ 新建工の	unkロ 🤤 删除洗择Trunk口				
RADIUS						
 AAA 						
▶ QoS管理 ▶ 协计表						
▶ Snmp管理						
▶ LACP						
▶ 系统管理						
				一 モーザ		

【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。

VLAN设置 其他设置								
VLAN设置								
VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作				
1	新建VLAN			×				
③ 新建VLAN ⑤ 删除选择VLAN Trunk设置	VLAN ID(1~4094): VLAN 名称(1-32字符): 选择加入本VLAN的端口:	2 VLANOO2						
 □ 満口名称 ③ 新建Trunk□ ○ 酬除选择Trunk□ 	端口名称 1 3 5 7 9 ③ 新建Trunk口 ● 删除选择Trunk口 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □							
	4	111		►.				
	保存设置 退出							
		テー歩						

VLAN设置 其他	设置					
VLAN设置						
VLAN ID		VLAN 名称	VLAN IP 地址	300 []	操作	
1		VI AN0001	192 168 0 1/24	1-10		
こことの 全部設でLAN の開始法 Trunk设置	新建Trunk山 送称 立立立い フロマロ(1 2 4 6	端口進行设置: 7 9 8 10			▲ ※ ▲ ※ ▲ ※ ▲ ※ ▲ ※ ▲ ※ ★ ※	
			→ 下一歩			

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。

VLAN设置	其他设置		
设备基本信息			
管理VLAN: 管理IP: 子 阿揸码: 保存设置	1 192.166.0.12 255.255.255.0 设置管理Vlan	设备名称: 默认网关: DNS服务器:	Switch-123 172.16.1.241 172.16.1.241

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

修改web管理员密码	
密码类型	密文密码 🔍
旧密码:	****
新密码:	****
确认新密码:	****
	➡ 上一步

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:

TRUCH DA	端口基本设置	Ē							
快速配置									
日管理	1 3 5	7 9							
端口聚合									
端口镜像		8 10							
端口限速		🕎 不可选端口 💼 选中端口 🚮 聚合端口 🖸	Trunk						
广播风暴	提示:可按住)	生罐拖拽选取多个端口 全选 反选 取消选择							
端口隔离	谱	口描述(0-80字符):		端口	状态: 开启	•			
端口信息		端口速率: 自协商 💌		工作	模式: 自协商	•			
AN管理	(m. etc.) (7, 60)	流 望控制: 关闭 ▼		交叉	线序: 自协商	•			
摩/安全	保存设置								
E管理	端口列表								
~ CP中维	端口	端口描述	端口状态	端口速率	工作模式	巨型幀	交叉线序	流重控制	操作
CP服务器	Gi0/1		开启	1000M	双工	5000	自协商	关闭	
CACS+	Gi0/2		开启	100M	双工	5000	自协商	关闭	
DIUS	Gi0/3		开启	自协商	自协商	5000	自协商	关闭	
、 5管理	Gi0/4		开启	自协商	自协商	5000	自协商	关闭	
上表	Gi0/5		开启	自协商	自协商	5000	自协商	关闭	
Adv with	Gi0/6		开启	自协商	自协商	5000	自协商	关闭	
np管理 CP			开启	自协商	自协商	5000	自协商	关闭	
np管理 CP 夜管理	Gi0/7		тè	自协商	自协商	5000	自协商	关闭	
np管理 CP &管理	Gi0/7 Gi0/8		井 启						
np管理 CP &管理	Gi0/7 Gi0/8 Gi0/9		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
	可选以下几种:
	自动协商
端口速率	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
	可选择模式有以下几种:
态叉维定	自动协商
人入线门	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。

端口基本设置		

🖸 可选端口 💼 不可选端口 💼	选中端口 🞦 聚合端口 💭 TrunkD	1	
提示: 可按住左键拖拽选取多个端口	□ 全选 反选 取消选择		
端口描述(0-80字符):		端口状态:	开启
端口速室:	10M 💌	工作模式:	¥72. ▼
流里控制:	开启 💌	交叉线序:	自协商
保存设置			

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:

	Y 当前用户名:admin		Ð	退出切]换语言
🗾 系统首页	端口聚合				
 ■ 快速電置 ▶ 端口管理 • 基本设置 	聚合端口编号(1-8):* 请选择端口加入聚合口:		1		
 ・ 端口聚合 ・ 端口镜像 ・ 端口阻滞 					
・ 广播风暴 ・ 端口隔离	① 可透離口 <>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		I		
 端口信息 MAN管理 	保存设置				
▶ 故障/安全 ▶ PoF管理	端口紫合列表 聚合端口	成员端口		操作	
► STP			首页 上一页 [1]	下一页 尾页1 /1	1页
▶ DHCP服务器					
 RADIUS AAAA 					
▶ QoS管理 ▶ 地址表					
▶ Snmp管理 ▶ LACP ▶ 系统管理					

【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。

端口聚合		
聚合端口编号(1-8): 1 *		
请选择端口加入聚合口:		
500 可选端口 💼 不可选端口 💼 选中端口 510 聚合端口 510 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		
保存设置		
端口聚合列表		
聚合端口	成员端口	操作
		首页 上一页 [1] 下一页 尾页 1 /1页

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:

15■ 配置指南

	Y 当前用户名	: admin		▶ 退出 切换语言
🛃 系統首页	端口镜像			
 ● 端口管理 ・ 基本设置 	镜像组编号(1-4 请选择源端口):。]: (允许选择多个满口,源满口过多可能会影响设备性能)		
 ・ 端口聚合 ・ 端口復慶 ・ 端口復慶 				
 ・ 端口限速 ・ 广播风暴 ・ 端口隔离 	○ 可送端口 (型 不可送端口) 提示:可按住左键拖拽选取多个的	▶️选中端口 <u>;î]</u> 聚合端口 <u>;</u>]Trunk口 <mark>第口</mark> 全造 反迭 取消选择		
 端口信息 VLAN管理 故障/安全 		1: (只能选择一个端口)		
▶ PoE管理 ▶ STP ▶ DHCP中维	2 4 6 8 10 ○ 可送端口 豊不可送端口 5 2 4 6 8 10	送中端口 ∫① Shakin ∫□ Trunk口		
▶ DHCP服务器 ▶ TACACS+ ▶ RADIUS	味仔 反血 端口鏡像列表		目的端口	糧作
▶ AAA ▶ QoS管理 ▶ 地址表	N/10 C/F *A	9009		2000 T
 ▶ Snmp管理 ▶ LACP ▶ 系绕管理 				

【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】

己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。

端口镜像			
	*		
请选择源端口: (分	许选择多个端口,源端口过多可能会影响设备性能)		
🛄 可选端口 💼 不可选端口 💼 选中	端口 <u>「1</u> 聚合端口 <u>「</u>] 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		
请选择目的端口: (只	2能选择—个端口)		
门 可选端口 📃 不可选端口 📄 选中	端口 <u>〔</u>]聚合端口 🛄 Trunk口		
保存设置			
端口镜像列表			
镜像组	源端口	目的端口	操作

4.2.4 端口限速

🗾 系統首页	端口限速						
🤜 快速配置							
▶ 端口管理	(
 基本设置 							
 ・ 端口 罷合 							
 端口镜像 	2 4 6 8 10						
・ 端口限速	🛄 可送端口 💼 不可送端口 💼 迭	中端口 [1]聚合端口 [] Trunk口					
• 广播风暴	提示: 可按住左键拖拽选取多个端口	全选 反选 取消选择					
 ・	输入限速(16的倍数):	* 0,16-1,000,000kb/s					
 端口信息 	输出限速(16的倍数):	* 0,16-1,000,000kb/s					
▶ VLAN管理	保存设置						
▶ 故障/安全	端口限速列表						
▶ PoE管理	避口	给入阻滞	输出阻滞	過作			
STP		387 (196.)2	THE ALL PLACE.	2811			
▶ DHCP中维	1	1000Mb/s	1000Mb/s	1			
 DHCP服务器 TAGAGE 	2	1000Mb/s	1000Mb/s				
 RADIUS 	3	1000Mb/s	1000Mb/s				
AAA	4	1000Mb/s	1000Mb/s				
▶ QoS管理	5	1000Mb/s	1000Mb/s				
▶ Snmp管理	6	1000Mb/s	1000Mb/s				
▶ LACP	7	1000Mb/s	1000Mb/s				
▶ 系统管理	8	1000Mb/s	1000Mb/s				
	9	1000Mb/s	1000Mb/s				
	10	1000Mb/s	1000Mb/s				
			首页 上一页 [1] 下	一页 尾页 <mark>1 /1页</mark>			

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:

【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。

端口限速	
$ \begin{bmatrix} 1 & 3 & 5 & 7 & 9 \\ \hline 1 & 2 & 2 & 2 & - \\ \hline 2 & 4 & 6 & 8 & 10 \end{bmatrix} $	
🛄 可选端口 💼 不可选端口 💼 j	中端口 517聚合端口 5
提示: 可按住左键拖拽选取多个端□	全迭 反选 取消选择
输入限速(16的倍数):	6400 * 0,16-1,000,000Kb/s
输出限速(16的倍数):	3200 * 0,16-1,000,000Kb/s
保存设置	

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:

系统首页	广播风暴						
快速配置							
端口管理							
• 基本设置							
・ 端口聚合	33330						
 端口镜像 	2 4 6 8 10						
 端口限速 	可选端口 💼 不可选端	印 💼 选中端口 î 聚合端	Trunk				
・ 广播风暴	提示: 可按住左键拖拽选取	19多个端口 全选 反选 取消; 	选择				
 端口隔离 	广播	抑制值:	* 0-262143(pps)				
・ 端口信息	组播	抑制值:	* 0-262143(pps)	Multicast 类型包:	未知名包 💌		
VLAN管理	単播	抑制值:	* 0-262143(pps)	Unicast 类型包:	未知名包 ▼		
故障/安全	保存设置						
PoE管理	广播风暴列表						
DHCP中维	端口	广播抑制值(pps)	狙播抑制值(pps)	组播类型包	单播抑制值(pps)	单播类型包	操作
DHCP服务器	1	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	1
TACACS+	2	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	1
AAA	3	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	1
QoS管理	4	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	2
・ 地址表 ・ Snmp管理	5	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	1
LACP	6	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	
系统管理	7	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	1
	8	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	2
	9	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	1
	10	0 (OFF)	0 (OFF)	Unknown-only	0 (OFF)	Unknown-only	2
						首页上一页[1] 下一页 尾顶	〔1 /1页

【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
	未知名:以组播组中不存在的 ip 为目的地址的流。
Multicast 类型包	知名及不知名:任一组播流。
	未知名:设备 MAC 表中没有该单播帧的目的 MAC
	条目。
Unicast 类型包	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。

广播风暴					
门 可选端口 💼 不可选端口 💼	选中端口 [1] 聚合端口	Trunk			
提示: 可按住左键拖拽选取多个端口	〕 全选 反选 取消选择				_
广播抑制值:	5000	* 0-262143pp/s			
组播抑制值:	5000	* 0-262143pp/s	Multicast 类型包:	知名及不知名包 🔻	
单播抑制值:	5000	* 0-262143pp/s	Unicast 类型包:	未知名包 💌	
保存设置					

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:

🛃 系统首页	端口隔离		
🔜 快速配置	请选择需隔离的端口:		
▶ 端口管理	[
 基本设置 			
・ 端口聚合			
・ 端口鏡像	2 4 6 8 10		
・ 端口限速	□ 可送端口 💼 不可送端口 💼 送中端口 î 聚合端口	Trunk	
 广播风暴 	提示:可按住左键拖拽选取多个端口 全选 反选 取消选择	¥.	
・ 満口隔离	保存编辑		
 ・ 端口信息 	端口隔离列表		
▶ VLAN管理		區會港口	調作
▶ 故障/安全	ויים מקוג צבע.	I-I EVICESTERI	3k IF
▶ PoE管理			首页 上一页 [1] 下一页 尾页1 /1页
STP			
▶ DHCP中继			
▶ DHCP服务器			
TACACS+			
RADIUS			
AAA			
▶ QoS管理			
▶ 地址表			
▶ Snmp管理			
LACP			

【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。

己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:				
1 3 5 7 9 2 2 9 10 2 4 6 10 2 7 7 7 2 4 6 10 2 7 7 7 2 4 6 10 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 2 7 7 7 3 7 7 7 3 7 7 7				
端口隔离列表				
源端口	隔离端口	操作		
3	45678	×		
4	35678	×		
5	34678	×		
6	3 4 5 7 8	×		
7	3 4 5 6 8	×		
8	3 4 5 6 7	×		
	20			

配置成功后,端口 3/4/5/6 相互隔离。

4.2.7 端口信息

📑 系统首页	端口信息									
🤜 快速配置	关键字 输入端	口号或端口描述进行查询	打查询 查询 又 实时别新流量							
▶ 端口管理 . 其太沿署		描述	输入流量(Bps)	输出流量(Bps)	开启状态	连接状态	所属vian	trunk口		
 端口聚合 	Gi 0/1		4.08M	6.04M	开启	💡 连接	1	否		
・ 端口鏡像	Gi 0/2		175.99M	65.12M	开启	💡 连接	1	哲		
 ・	Gi 0/3		0.00K	0.00K	开启	未连接	1	否		
 「 描 以 暴 	Gi 0/4		0.00K	0.00K	开启	💛 未连接	1	否		
• 端口信息	Gi 0/5		0.00K	0.00K	开启	😽 未连接	1	否		
▶ VLAN管理	Gi 0/6		0.00K	0.00K	开启	💛 未连接	1	舌		
▶ 故障/安全	Gi 0/7		0.00K	0.00K	开启	💛 未连接	1	否		
► STP	Gi 0/8		0.00K	0.00K	开启	💛 未连接	1	否		
▶ DHCP中继	Gi 0/9		0.00K	0.00K	开启	💛 未连接	1	否		
▶ DHCP服务器	Gi 0/10		0.00K	0.00K	开启	💛 未连接	1	否		
 RADIUS 								首页 上	一页[1] 下一页 尾页 <mark>1</mark>	/1页
AAA										
▶ QoS管理 ▶ 地址表										
▶ Snmp管理										
▶ LACP ▶ 系统管理										

在导航栏选择"端口管理>端口隔离",可查询端口信息,如下图:

【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 1		查询	👿 实时刷新流里						
	描述	输入流量(Bps)	输出流量(Bps)	开启状态	连接状态	所属vlan	trunk		
Gi 0/1		4.21M	6.26M	开启	💛 连接	1	桁		
Gi 0/10		0.00K	0.00K	开启	💛 未连接	1	桁		
							首页 上	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。

🛃 系统首页	VLAN	VLAN设置 Trunk口设置 Hybrid口设置									
🤜 快速配置	VLAN	VLAN列表									
▶ 端口管理		VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作					
▶ VLAN管理		1	VI AN0001	192 168 0 1/24	1-10						
• VLAN管理			12410001	102.100.0.1124	1.10						
▶ 故障/安全	◎ 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:

🛃 系统首页	VLAN	W设置 Trunk口设置	Hybrid口设置			
🤜 快速配置	VLAN 3	表				
▶ 端口管理 ▶ \/I AN管理		VLAN ID	VLAN 名称	VLAN IP 地址	満口	操作
・ VLAN管理		1	VLAN0001	192.168.0.1/24	1-10	
▶ 故障/安全	③ 新建	VLAN 🤤 删除选择VLAN			首页 上一页 [1]	下一页 尾页1 /1页
 D C 446 100 						

【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。

21 ■ 配置指南

VLAN设置	Trunk口设置		Hybri	id口设置	E				
VLAN列表		新建V	LAN						
	VLAN ID			VLA	N ID(1~40	094) :	2		*
	1		١	VLAN 名	称(1-32号	字符):	VLANOO	02	
	·····································		选	择加入本	VLAN的	端口:	\sim		
					9 	1 <u>-</u> 1	先中端口	5 <u>17</u> 聚合端口	<u>, Trun</u>
		保存	F设置	退	Щ				
操作									
	-								
X	可点击页面操作	乍中编	辑、删	除按钮	1进行相	回操	作。		

4.3.2 Trunk 口设置

📑 系统首页	VLAN设置	f TrunkDi	设置 Hybrid口设置			
🔜 快速配置	Trunk口列表	ŧ				
▶ 端口管理		端口	端口描述	本地VLAN	允许通过的VLAN	操作
▶ VLAN管理						
・ VLAN管理	◎ 新建Trun	ik口 🥥 删除选择T	runk		首页上一页[1]下一页]	尾页1 /1页
▶ 故障/安全						
▶ PoE管理						

【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。

VLAN	1设置	Tru	nk口设置	Hybrid口设置						
VLAN	表									
		VLAN ID		VLAN 名称		VLAN IP	地址	端口	操作	
		1		VLAN0001		192.168.0	.1/24	1-7,9-10		
		2		VLAN0002				8	2 🔀	t
③ 新建	VLAN 🤤	刪除选	¥VLAN					首页上一页[1]	下一页尾页1	/1页
VLA	N设置	Tru	nk口设置	Hybrid口设置						
Trunk	口列表									
	端口 端口描述 本地VLAN 允许通过的VLAN								操作	F
 新建TrunkD 制度 新建TrunkD 工 工 定页1 								× 尾页1	/1页	
				选择端口进行设置:					^	
			$ \begin{array}{c} 1 & 3\\ \hline \hline & \\ \hline & \\ 2 & 4 \end{array} $	5 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 9 7 7 7 7 9 7					E	
			[]]可选辑	们 💼 不可选端口 💼 选中	端口 抭	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				
			1	Native Vlan(1-4094): 2						
			允许通过	的VLAN(如3-5,8,10): 1					-	
			保友	沿署 退出		m		•		
			(IA1)							

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:

🗾 系统首页	VLAN设置 Tr	unk口设置	口设置			
🔜 快速配置						
▶ 端口管理	Hybrid口列表					
▶ VLAN管理	📄 端口	端口描述	本地VLAN	加TAG的VLAN	去TAG的VLAN	操作
・ VLAN管理	③ 新建Hybrid□ ◎ 刷	除法择Hybrid日				/1页
▶ 故障/安全	• 491 XE - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -	MAZH- J				1100
▶ PoE管理						
STP						
▶ DHCP中维						
▶ DHCP服务器						
TACACS+						
RADIUS						
► AAA						
▶ QoS管理						
▶ 地址表						
▶ Snmp管理						
LACP						
▶ 系统管理						

【使用说明】

23■ 配置指南

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	1设置 1	runk口设置	Hybrid口设置						
VLAN列表									
	VLA	N ID	VLAN 名称		VLAN IP 地址	端口	操作		
		1	VLAN0001		192.168.0.1/24	1-10			
	1	0	VLAN0010				D 🗙		
	2	0	VLAN0020				2 🗙		
③ 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									
第日 第年林ybrid1 ● <t< th=""></t<>									
VLAN设置 Trunk口设置 Hybrid口设置									
	端口	端口描	it لل	也VLAN	加TAG的VLAN	去TAG的VLAN	操作		
	7			10	1	10,20	× ×		
	8			20	1	10,20	2 ×		
◎ 新建	Hybrid 🗖 🥥 🗑	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->p2 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。

۲	故障/安全						
	•	防攻击					
	•	通路检测					
	•	ACL访问控制					
	•	802.1x					

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
	信任端口正常转发接收 DHCP 报文,不信任端口将丢弃 DHCP
DHCP 信任端口	响应报文
DHCP 抑制端口	拒绝端口下所有 DHCP 请求报文
	对 DHCP CLIENT 发出的请求报文,检查链路层头部 MAC 地址
源 mac 效验	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。
	将在 DHCP 请求报文中添加 option82 信息,转发给服务器,
Option82 使能	DHCP 服务器可根据该选项信息进行灵活的地址分配。
	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
客户端 option82 使能	报文时,将丢弃该报文。
	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
电路控制	和端口。
	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
代理远程	类型的,内容为交换机 mac 地址。
	依据 DHCP 报文所走的 vlan 选择使用该 vlan 下所配置的 IP 子
lp 地址	选项内容,如果没有配置的话,不发送该选项。
	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
绑定表	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
	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
Dhcp Snooping 服务	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
器 IP 地址	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。

防护状态
Open开启后可自定义设置DHCP信任口。
2.设置 dhcp snooping vlan。
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
Dhcp Snooping Vlan: 1 *

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	选择加入DHCP信任端口:								
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$									
	① 可选端口 1 不可选端口 1 选中端口 1 2 聚合端口 1 Trunk口 5 [2] ip源使能开启端口 提示:可按住左键拖拽选取多个端口								
DHCP信任端口设置 禁止DHCP申请地址 源MAC校验 OPTI									
选择禁止D	HCP申请地址端口:								
⑦ 可选端口 1 不可选端口 1 选中端口 1 聚合端口 1 Trunk口 1 p 源									
4.效验源 mac F0:D	E:F1:12:98:D2,	将服务器设置	置为 192.168	.0.1。					

DHCP信任端口设置	禁止DHCP申请地址 爱MAC校验 OPTION82 绑定表 其他配置							
避MAC技能使能:(図) Mac地址 10:00:F1:12:99:02 * 校验 不校验								
源mac校验列表								
序号	macj使j止	状态	操作					
1	f0:de:f1:12:98:d2	校验						
Dhcp Snooping服务器IP她指: 192, 168.0.1 *								

	Dirch	SHOOPINY服务盔P吧里:	(192.100.0.1	
	\frown			
l	添加			
Y	ALC: NO			

5.设置 option82 信息。

Option82使能: 🕢 客户域Option82使能: 🗹								
电路控制 代理	远程 IP地址							
电路控制名: 123 添加	电路论制名: 223 · VLANID: 1 · 流加							
序号	电路控制名	电路控制ID	VLAN ID	操作				
1	123	1	1	2 🗙				
电路控制 代理	版程 IP地址							
道程代理名 (very) ・ VLAN II(:1) ・ 添加								
序号	远程代理名	远程代理ID	VLAN ID	操作				
1	wery	1	1	2 🗙				

电路控制代理远程	地址					
IP地址: 192.166.2.30 添加	* (LANID: 1	±				
序号	IP地址			VLAN ID		操作
6.将端口7进行约	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 所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:	开月	言防	DOS	攻击。
<u>∽</u> ⊢•			200	· <u> </u>

防DH	нср攻击	防DOS	IP源防护	三元绑定
DOS政	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 三元绑定				
P)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				
□ 可送端口 豐 还中端口 11 聚合端口 □1 聚合端口 □1 Trunk口 12 IP 液使能开启端口				
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。

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:						
$\begin{array}{c}1\\1\\2\\2\\2\\4\\6\\8\end{array}$						
💭 可选端口 💼 不可选端口 💼 选中端	ロ 「「「「「「Trunkロ 」」「」「「源使能开启端口					
提示 :可按住左键拖拽选取多个端口						
保存						
防衛防迫港口体影響等	『蘇防护 二九神史					
"家例证"项目 医肥脂血						
请选择PP源防护使能端口:	X					
	Vian ID: 30/19/2011: 192.168.0.30 30/101:15:09:35:37					
保存						
IP源防护端口安全配置	2 4 6 8 10					
索引 ♀️□□送端口 壹/不可选端口 壹/这中端口 ⑦ 聚台端口 ① Trunk口 ② ID爆使能开启端口						
③ 新建安全端口		页				
	保存设置 退出					

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:

🛃 系統首页	防DHCP攻击	防DOS IP源防护 三元绑定		
🔜 快速配置	检测列表			
▶ 端口管理	绑定使能 📃			
▶ VLAN管理		maalitala	indedd	油口島
▶ 故障/安全		machen	ibadall.	潤口ち
・ 防攻击			首	页 上一页 [1] 下一页 尾页 1 /1页
 通路检测 	扫描 绑定			
• ACL访问控制	14.04			
• 802.1x				
▶ PoE管理	应用列表			
N CTD	•			
▶ DHCP由维		mac地址	ip地址	端口号
▶ DHCP服务器	🤤 删除所选项		Ĭ	页 上一页 [1] 下一页 尾页 1 / 1 页
TACACS+				
RADIUS				
RADIUSAAA				
▶ RADIUS ▶ AAA ▶ QoS管理				
▶ RADIUS ▶ AAA ▶ QoS管理 ▶ 地址表				
▶ RADIUS ▶ AAA ▶ QoS管理 ▶ 地址表 ▶ Snmp管理				
 RADIUS AAA QoS管理 地址表 Snmp管理 LACP 				

【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。

绑定	使能 🔽 🛛 🖓 🖽	绑定	
	mac搜加	ip地址	端口号
	F0:DE:F1:12:98:D2	192.168.13.133	2
	F0:DE:F1:12:98:D2	192.168.168.20	2
	00:01:15:09:37:35	192.168.2.33	7
	00:01:15:09:37:35	192.168.168.30	7
	00:01:15:09:37:35	10.10.10	7
	00:01:15:09:37:35	192.168.0.12	7
	00:01:15:09:37:35	192.168.13.13	7
	00:01:15:09:37:35	192.168.1.111	7
			首页 上一页 [1] 下一页 尾页1 /1页
扫描 绑定			
应用列表			
	mac地址	ip地址	端口号
	00:01:15:09:37:35	192.168.2.30	7
😂 删除所选项			首页 上一页 [1] 下一页 尾页1 /1页

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:

🛃 系統首页	ping检测 tracert检测 线缆检测
🌉 快速配置	
▶ 端口管理	
▶ VLAN管理	
▶ 故障/安全	开始绘测
 防攻击 通路检测 	检测结果:
• ACL访问控制	A
• 802.1x	
▶ PoE管理	
▶ STP	
▶ DHCP中继	
▶ DHCP服务器	v
TACACS+	
RADIUS	
AAA	
▶ QoS管理	
▶ 地址表	
▶ Snmp管理	

【参数说明】

▶ LACP ▶ 系绕管理

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。

ping检测 tracert检测 线缆检测						
目的IP地址:	192.168.0.64					
超时时间(1-10):	2					
重复次数(1-100):	5					
开始检测						
检测结果:						
PING 192.168.0.64 (192.168.0.64): 56 data bytes						

4.4.2.2 tracert 检测

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

ping检测 tracert检测 线缆检测	
目的IP地址:	
超时时间(1-10): 2	
开始检测	
刘结果:	
	*
	Ψ.

【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。

ping检测 tracert检测 线缆检测						
目的P地址: 超时时间(1-10): 平始检测)						
佐嗣结果: fraceroute to 192.168.0.64 (192.168.0.64), 30 hops max, 40 byte packets 1 192.168.0.64 (192.168.0.64) 10 ms * 0 ms	A					
11 traceroute: wrote 192.168.1.4 40 chars, ret=-1						
	~					

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:

ping检测 tracert检测 线缆检测	
法释检测的端口:	
1ំនំភ្នំ ជុំជំជំជំ ជុងគុជ	
2 4 6 8 [○]可迭端口 (雪) 还可透端口 (雪) 送中端口 (①) 聚合端口 (○) Trunk口 开始检测	

【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】

ping检测 tracert检测 线缆检测	
选择检测的端口:	
1 3 5 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 2 4 6 8 1 可送端口 1 1 1 1 1 1 1 1	
开始检测	
检测结果	
端口	状态
2	正常
	首页 上一页 [1] 下一页 尾页 1 /1页

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:

- 系統首页	ACL生效时间 ACL访问控制	应用ACL		
🔜 快速配置	对象名:			
▶ 端口管理	选择日期: 🗌 星期— 🔲 县	副二 🗆 星期三 🔲 星期四 🔲 星期五 🗐 星期六 🗐 🛚	星期日	
▶ VLAN管理	时间段:	· · · · ·		
▶ 故障/安全	保存配置			
 防攻击 		时间周	时间段	操作
 通路检测 	H-REA	1 F3/F3	*1PHA	Jak II*
• ACL访问控制			首页 上-	-页[1] 下页尾页1 /1页
• 802.1x				
▶ PoE管理				
► STP				
▶ DHCP中维				
▶ DHCP服务器				
TACACS+				
RADIUS				
AAA				
▶ QoS管理				
▶ 地址表				
▶ Snmp管理				
LACP				
▶ 系统管理				

【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 这 法 保存配置 对象·	ACL访问控制 付象名: 译日期: 型星期 型星 时间段 ^{9:00} 名	这用ACL 明二 ▽ 星期三 ▽ 星期四 ▽ 星期五 □ 星期六 □ 回 - [16:00 □ ● + 时间周]星期日 时间段 首页上-	操作 -页【1]下-页尾页1 /1页
ACL生效时间 创建ACL 规则顺序 ACI规则 考	ACL访问控制 加作 投值 助行 新建ACL访问规则	 	目的呼渡码 目的端口 生效时间对	状态 剛除 文 尾页1 /1页
		目的呼地址任意: 🗹 🕧		
	保存			

ACL生	ACL生效时间 ACL访问控制 应用ACL										
创建ACL	03BACL										
规则顺序	Acl <mark>规则</mark> 号	动作	权值	协议	源IP/掩码	源端口	目的IP/撤码	目的端口	生效时间对 象	状态	刪除
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 ① ① ① ① □ 2 4 6 10 ① □ ○ □ □ 2 4 6 8 10 ① □ □ □ □ □ 2 4 6 8 10 □ ② □ ○ □ □ □ ② □ ○ □ □ □ ② □ ○ □ □ □ 2 4 6 8 10 □ □ ② □ <	a中端口 <u>〔1</u>]聚合端口 <u>〔1</u> Trunk□ 全选 反选 取消选择 400 ₩/4/2文 ▼		
ACL访问控制列表			
ACL	应用于接口	过滤方向	操作
100	3	收报文	2 🗙
		首页上一页[1]	下一页 尾页1 /1页

4.4.4 802.1x

📑 系统首页	802.1x设置
🤜 快速配置	44X0024v. Disable
▶ 端口管理	remoorke Disable ■ ∰itirefas: ♥
▶ VLAN管理	重い正の期: 3600 (60-7200)s
▶ 故障/安全	使用Pae组炮址: 🕑
 防攻击 	认证重传最大次数: 2 💌
· 通路检测	认证失败vian次数: 3
• ACL访问控制	应用
• 802.1x	送释端口进行设置:
▶ PoE管理	
STP	
▶ DHCP中继	
▶ DHCP服务器	2 4 6 8 10
TACACS+	全可透漏口 🧝 不可透漏口 💼 法中漏口 抗 聚合漏口 🖾 Trunkロ
RADIUS	<mark>提示:</mark> 可按住左键抽线选现多个端口 全选 反选 取消选择
AAA	端口控制方式: Auto 💌
▶ QoS管理	端口认证方式: Mac Base 💌
▶ 地址表	最大用户数: (0-255)
▶ Snmp管理	MAB认证方式 Disable -
LACP	MAB认证周期 (0-65535)s
▶ 系统管理	GUEST VLAN: (1.4094)
	1人研究版VLAN: (1-4094)
	应用

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, 钩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。

802.1x设 <u>罟</u>	
使能802.1x:	Enable
重认证使能:	
重认证周期:	3600 (60-7200)s
使用Pae组地址:	
认证重传最大次数:	2
认证失败vian次数:	3
应用	

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:			
$ \begin{array}{c} 1 & 3 & 5 & 7 & 9 \\ \hline 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 \\ \hline 2 & 4 & 6 & 8 & 10 \end{array} $			
🛄 可选端口 💼 不可选端口 💼 🔅			
提示: 可按住左键拖拽选取多个端口	全选 反选 取消选择	7	
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。

۲	PoE管理	
	•	PoE管理
	•	PoE配置
	•	PoE延迟

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:

🖲 系统首页	高级管理 温度配置	
🔜 快速配置	POE状态信息	
▶ 端口管理	- T作状态: 在线	告題功室: 126.0W
▶ VLAN管理	杨宁首山东 • 140.0W	当日 / · · · · 5/ 7/
▶ 故障/安全		
▶ PoE管理	当前息功率: 0.0W	
・ PoE管理	POE高级管理	
• PoE配置		
• PoE延迟	告婴通告:	U 126W
▶ STP	告答遵告: 🔘 开启 💿 关闭	
▶ DHCP中维	保存设置	
▶ DHCP服务器		
TACACS+		
RADIUS		
AAA		
▶ QoS管理		
▶ 地址表		
▶ Snmp管理		

▶ LACP ▶ 系统管理

【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。

高级管理	温度配置
POE状态信息	
工作状态:	在线 告 警功车: 126.0W
额定总功率:	140.0W 当前电压: 54.7V
当前总功室:	0.0W
POE高级管理	
告攀通告:	120 W
告警通告	: ● 开启 ◎ 关闭
保存设置	

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 芯片的告警阀值。如下图:

高级管理 温度配置			
温度配置			
芯片温度列表			
芯片编号	实时温度	告警嗣值	操作
1	55°C	100°C	
		首页 上一页 [1] 下	—页 尾页 <mark>1 /1页</mark>

【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 告警阀值设置为 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:

📑 系統首页	PoE端口列表										
🤜 快速配置	端口	连接	状态	当前功率	当前电流	最大功室	PD类型	使能	优先级	检测模式	操作
▶ 端口管理	1	Disabled	禁用	-	-	32W	-	激活	低	AT&AF	
▶ VLAN官理 ▶ 故障/安全	2	Disabled	禁用			32W		激活	低	AT&AF	
▶ PoE管理	3	Disabled	禁用			32W		激活	低	AT&AF	
・ PoE管理	4	Disabled	禁用			32W		激活	低	AT&AF	
PoE配面 PoE証iR	5	Disabled	禁用			32W		激活	低	AT&AF	
▶ STP	6	Disabled	禁用	-	-	32W	-	激活	低	AT&AF	
▶ DHCP中维	7	Disabled	禁用	-	-	32W	-	激活	低	AT&AF	
▶ DHCP服务器	8	Disabled	禁用	-	-	32W	-	激活	低	AT&AF	
 RADIUS 	③ 编辑该页所	有端口							首页 上一	页[1] 下一页 尾	页1 /1页
► AAA											
▶ QoS管理 ▶ 地址表											
▶ Snmp管理											
► LACP											
▶ 系统管理											

【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23W、检测模式为AF、优先级为高。

Pol	E端口列表										
	端口	连接	状态	当前功率	当前电流	最大功率	PD类型	使能	优先级	检测模式	操作
		Disabled	益田			3211/	-	浙汪	×	AT&AF	
		16.61. à			7				▲ 既	AT&AF	
		調	口使能:激活	•					馬	AT&AF	
		端口伯	忧先级: 高	•					馬	AT&AF	
		检测最大功	則模式: AF 家(W): 23	•					賬	AT&AF	1
		正在编辑的	9端口:						≡ 16	AT&AF	2
	1 3 5 7 H. AT&AF								1		
0											
	∑?可选端口 □ 不可选端口 12 送中端口 512 聚合端口 5? Trunk口										
	4			III					•		
	保存编	<u>辑</u> 退出									

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:

📑 系统首页	PoE重启/延迟								
🔜 快速配置									
▶ 端口管理									
▶ VLAN管理	1222								
▶ 故障/安全									
▶ PoE管理	2 4 6 8								
・ PoE管理	门 可选端口 💼 不可送端口 💼 选	中端口 î 聚合端口 🛄 Trunk口							
 PoE配置 	提示:可按住左键拖拽选取多个端口								
• PoE延迟	当前系统时间: 2000-01-01 01:57:32	2.星期六							
STP	选择重启的星期:	■星期- ■星期二 ■星期三 ■星期四 ■星期五 ■星期六	■星期日						
▶ DHCP中继	重启时间段:	1							
▶ DHCP服务器	端口延迟时间:	秒(0-3600) *							
TACACS+	保存设置								
 RADIUS AAA 	端口延迟列表								
▶ QoS管理	端口	重启时间	延迟时间	操作					
▶ 地址表	1	0	0s						
LACP	2	0	0s						
▶ 系统管理	3	0	0s	1					
	4	0	0s						
	5	0	0s						
	6	0	0s						
	7	0	0s						
	8	0	0s						
			首页 上一页 [1] 下	一页尾页1 /1页					

【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。

PoE重启/延迟
Condeilan en the first
提示 : 可按住左鍵樁換选取多个滿口
当前系统时间: 2000-01-01 02:02:45,星期六
选择重启的星期: 🔤 星期一 🔄 星期三 💷 星期四 🔄 星期四
重自时间段: D0:57:33
端口延迟时间: 20 秒(0-3600) *
保存设置

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。

۲	S	ГР
	•	MSTP域
	•	STP桥端口

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:

📑 系统首页	MSTP域配置		
	域名:	D468BA0911DF * (1~32个字符)	
▶ 端口管理	修订级别:	0 (0~65535.默认=0)	
▶ VLAN管理	保存		
▶ 故障/安全	10 Million Bal		
▶ PoE管理	头例映射		
▶ STP ● MSTP域	实 例 D: Vian ID:	1 参約: 1.3.5.7-10	
• STP桥端口	保存 删除		
▶ DHCP中继	实例映射列表		
 TACACS+ 	实例ID	映射 Vīan	操作
RADIUS	0	1-4094	0
AAA		首页 上—页 [1] 下	- D SD1 /10
▶ QoS管理			- A 624
▶ 地址表			
▶ Snmp管理			
LACP			

【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。

MSTP域配置		
域名:	DEADBEEF0102 * (1~32个字符)	
修订级别	123 * (0~65535 慧认=0)	
保存		
实例映射		
实例ID:	4	
Vian ID:	2 例如1: 1,3,5,7-10	
保存删除		
实例映射列表		
实例ID	映射 Vian	操作
0	1-4094	Ø
	首页 上一页 [1] 下	一页 尾页 <mark>1 /1页</mark>

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:

📑 系統首页	STP桥配置	
🤜 快速配置	定制借牛犯:	
▶ 端口管理	sello:	优先级: 32768 🔍
▶ VLAN管理		Pu/uox.
▶ 故障/安全	使能: ◎ 开启 ◎ 关闭	模式: O STP O RSTP O MSTP
POLETE	握手时间: 2 (1-10s)	Max Age: 10 (6-40s)
• MSTP域	转发时延: 10 * (4-30s)	最大跳数: 10 * (1-40)
●STP桥端口	保存设置 查看桥配置	
▶ DHCP中继	STP端口配置	
▶ DHCP服务器		
TACACS+	头例: 0 ▼	优先级: 128 * (0-240,以16为步长)
RADIUS	快速端口: ◎ 开启 ● 关闭	链路开销: auto * (auto或1-20000000)
AAA	自动边缘: 💿 开启 💿 关闭	点对点: 🔘 开启 🔘 关闭 💿 自动
▶ QoS管理	Bpdu 保护: 〇 开启 💿 关闭	兼容性模式: [©] 开启 [®] 关闭
▶ 地址表	Bpdu 过渡: 💿 开启 💿 关闭	根保护: ◎ Root ◎ None
▶ Snmp管理	TC保护: ◎ 开启 ◎ 关闭	TC 过滤: ◎ 开启 ◎ 关闭
LACP	1 3 5 7 9	
▶ 系统管理		
	□」□」□	
	保存设置查看当前端口配置	

【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 1-20000000,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 quard 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	h用 tc-quard 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*(握手时间 + 1)<= 最大老化时间<= 2*(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: O STP O RSTP @ MSTP
握手时间:	2 * (1-10s)	Max Age: 15 * (6-40s)
转发时延:	10 * (4-30s)	最大跳薮: 20 * (1-40)
保存设置 查看材	- 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	

STP桥配置		
实例优先级 :	STP桥信息	
实例ID: 0 √ 使能: ● 开启 ◎ 关闭 握手时间: 2 转发时延: 10	StpVersion: mstp Sys5tpStatus: enable BridgeHaxAge: 15 BridgeHeiloTime: 2 BridgeForwardDelay: 10 MaxHops: 20 TxHoldCount: 6	
保存设置 重看術配置 STP端口配置 文例: ○ 快速端口: ○	Instance [0] E LocalFidge: 32768 - D4.68.BA:09:11:DF TimeSinceTopologyChange: 0d:0h:3m.8s TopologyChanges: 1 DesignatedRoot: 32768 - D4:68:BA:09:11:DF RootCost: 0 GisRegionRoot: 32768 - D4:68:BA:09:11:DF	
自动边缘: ⁽¹⁾ 开启 ⁽¹⁾ Bpdu保护: ⁽¹⁾ 开启 ⁽²⁾ Bpdu过道: ⁽¹⁾ 开启 ⁽²⁾ TC保护: ⁽¹⁾ 开启 ⁽²⁾	CistPathCost: 0 instance [4] LocaBridge: 8192 - D4:68:BA:09:11:DF TrueSinceTopologyChange: 01:0h::tm:38s TopologyChanges: 0	
1 3 5 7 9 2 2 2 2 2 2 2 4 6 10 2 2 2 4 6 10 2 2 2 4 6 10 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	关闭	
 2 可选端口 2 不可选端口 2 选中端口 保存设置 查看当前端口配置 	51. 聚合) And Trunkロ	

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)。

STP端口配置						
实例:	4	•	优先级:	128	* (0-240,1) 16	6为步长)
快速端口:	◎ 开启	◙ 关闭	锐路开销:	auto	* (auto或1-20	0000000)
自动边缘:	◉ 开启	◎ 关闭	点对点:	◎ 开启 ◎ ¥	闭 🍳 自动	
Bpdu保护:	◎ 开启	◎ 关闭	兼容性模式:	◎ 开启 🍳 关	闭	
Bpdu过滤:	◎ 开启	◎ 关闭	根保护:	🔘 Root 🔍 No	ne	
TC保护:	◎ 开启	◎ 关闭	TC过滤:	◎ 开启 ◎ 关	闭	
🖸 नऊंग्रेन 💼 रनउंग्रेन 💼 देनभ्रांग 🖸 ञ्चितेश्वन 💭 Trunkn						
保存设置 查看当前端口配置						

51PI侨配查			
实例优先级:	STP端口配置 [Gi0/4]		
实例ID: 0 🚽	[Gi0/4]	_	
使能: ④ 开启 ◎ 关闭	PortOperPortFast: disable PortAdminAutoEdae: enable		
握手时间: 2	PortOperAutoEdge: disable		
转发时延: 10	PortOperLinkType: point-to-point	E	
保存设置 查看桥配置	PortBPDUGuard: disable PortBPDUFilter: disable		
STP端口配置	PortTCGuard: disable		
	instance[0] VlanMap: 1,3-4094		
实例: 0 🗸	PortState: down PortPriority: 128		
快速端口: 🔘 开启 🔍 🕴	PortDesignatedRoot: 32768 - d4:68:ba:09:11:df		
自动边缘 : 💿 勇 💿 勇	PortDesignatedCost: 0 PortDesignatedBridge: 32768 - d4:68:ba:09:11:df		
Bpdu保护: 〇 开启 🔘 🤅	PortDesignatedPortPriority: 128		
Bpdu过滤: 🔘 开启 🔍	PortAdminPathCost: auto	*	
TC保护: 🔘 开启 🥖 🔅	PortOperPathCost: 5000000		
	关闭		
2 4 6 8 10			
🖸 可选靖口 👮 不可送端口 👮 选中靖口	11. 聚合端口 500 Trunk口		
保存设置			

.

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:

🛃 系统首页	DHCP中继领能状态
🔜 快速配置	DHCP中继使能:
▶ 端口管理	DHCP OPTION信任字段使能: 🗹
▶ VLAN管理	
▶ 故障/安全	
▶ PoE管理	
▶ STP	
▶ DHCP中维	
• DHCP中维	
Option82	
▶ DHCP服务器	
TACACS+	
RADIUS	
AAA	
▶ QoS管理	
▶ 地址表	
▶ Snmp管理	
▶ LACP	
▶ 玄绪管理	

【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
	开启时,当收到的客户端 DHCP 报文带 option82 信息时,保留,
DHCP option 信任	否则添加交换机自己的 option82 信息转发出去。 关闭时,丢弃
字段使能	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中维使能: 📝 DHCP OPTION信任字段使能: 📝	
DHCP中继配置	
DHCP服务器IP: 192.168.0.22 *	

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:

🛃 系統首页	Option82配置				
🤜 快速配置	电路控制	代理远程 IP地址			
▶ 端口管理					
▶ VLAN管理	电路控	約:			
▶ 故障/安全	VLAN	ID: *			
▶ PoE管理	添加				
STP	6 0	بخ الخبخا تلام م			19 0-
▶ DHCP中继	序写	电路控制名	电路控制ID	VLAN ID	·探1F
• DHCP中继				首页 上一页 [1]	下一页尾页1 /1页
• Option82					
▶ DHCP服务器					
TACACS+					
RADIUS					
AAA					
▶ QoS管理					
▶ 地址表					
▶ Snmp管理					
LACP					
▶ 系统管理					

【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 VLAN IE 添加				
电路控制	代理远程 IP 地址			
代理远看 VLAN IE	₽: 123 1			
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 IP地址 VLAN IC 添加	代理远程 192.168.0.35 1 1 1 1 1		首页 上—页 [1] 「	下─页 尾页 //1页
电路控制 IP地址 VLAN IC 添加 序号	代理远程 192.168.0.35 1 1 1 1 1 1 1 1 1 1 1 1 1	地址	首页 上一页 [1] 「 VLAN ID	►-页 尾页 1 /1页 器件

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:

🛃 系統首页	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
🤜 快速配置	DHCP使能
▶ 端口管理	
▶ VLAN管理	
▶ 故障/安全	
▶ PoE管理	
▶ STP	
▶ DHCP中继	
▶ DHCP服务器	
• DHCP服务器配置	
TACACS+	
RADIUS	
► AAA	
▶ QoS管理	
▶ 地址表	
▶ Snmp管理	
▶ LACP	
▶ 系统管理	

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。

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	
DHCP使能						
Open						

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:

dhcp服务器使能(dhcp地址池	option	定表 缺省网关配	置 DNS服务器配	置		
地址	也ID	* (1-65535)					
ł	或名						
7	Mip	*					
子网	葡码	*					
Я	台IP						
结	束IP						
租约	时间	Æ	84	分			
保存设置							
缓冲列表							
m 地址池ID	域名	子网ip	子网掩码	租约时间	开始IP	结束IP	操作
					首页 上	—页[1] 下—页 尾页1	/1页

【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。

dhcp服务器使能 dh	cp地址池 op	tion	缺省网关配置	DNS服务器配置	
地址池ID	1	* (1-65535)			
域名	work				
子网的	192.168.1.5	*			
子网掩码	255. 255. 255. 0	*			
开始IP	192. 168. 1. 100				
结束IP	192.168.1.199				
租约时间	1	<u></u> .	时	分	
保存设置					

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:

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 💌			
	代码 * (1-255)			
	代码值类型 hex 💌			
	代码值 *			
设置				
Option 列表				
	地址池ID	代码	代码值	操作
			首页 上一引	〔 <mark>1]</mark> 下一页 尾页1 /1页

【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。

dhcp服务器使能 dt	ncp地址池 optio	n 绑定表	缺省网关配置	DNS服务器配置	
地址池川	D 1 💌				
代码	₿ <mark>2</mark> *	(1-255)			
代码值类型	변 ip 💌				
代码值	192. 168. 1. 2 *				
设置					

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 DNSJ	服务器配置	
绑定列表				
	and bit also and	77 05 14 14	14 tion + 13	49. Ar-
IP地址	硬件类型	使幵地址	四世世	·深1F

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	p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	*		
网关2			
阿 关3			
网关4			
网 关5			
阿 关6			
网关7			
网关8			
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
地址地口
网关1 192.168.1.55
网关2
网关3
网关4
网关5
网关6
网关7
网关8
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:

dhcp服务器使能 dhcp地址池 op	tion	缺省网关配置 DNS服务	器配置
地址池ID 1 ▼			
DNS服务器1	*		
DNS服务器2]		
DNS服务器3]		
DNS服务器4]		
DNS服务器5]		
DNS服务器6]		
DNS服务器7]		
DNS服务器8]		
设置			

【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。

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
地址泡口 1 🔍
DNS服务器147.54.89.210
DNS服务器2
DNS服务器3
DNS服务器4
DNS服务器5
DNS服务器6
DNS服务器7
DNS服务器8

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。

😬 系统首页	TACACS+ 配置				
🤜 快速配置	全局配置				
 ▶ 端口管理 ▶ VLAN管理 ▶ 故障/安全 ▶ PoE管理 ▶ STP ▶ DHCP中继 	服务器超时 服务器重道 会话 保存设置	时长:5 (次数:3 (注教:◎ Only ◎ Multi 密钥:			
▶ DHCP服务器 ▶ TACACS+ • TACACS+配置	端口配置 服务 认证	경P:			
▶ AAA ▶ QoS管理 ▶ 地址表	服务器超时	时长:			
▶ Snmp管理	TACACS+服务器列表				
 ► 系统管理 	编号	服务器IP	端口	服务器超时时长	操作
				首页 上一页 [1]	下一页 尾页 1 / 1页

【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,密匙为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:	5
服务器重试次数	: 3
会话住接	: Only 🖲 Multi
密钥:	: 2644as
保存设置	
端口配置	
服务器IP	192.168.0.88
认证端口:	: 49
服务器超时时长	: 5
密钥:	: 2644as
保存设置	

4.10 RADIUS

在导航栏选择"RADIUS",你在此设置 RADIUS 认证相关配置。

🛃 系统首页	Radius全局配置 Radius服务器配置
🤜 快速配置	RADIUS全局配置信息
▶ 端口管理	
▶ VLAN管理	
▶ 故障/安全	
▶ PoE管理	加労益 伊思(1)日 (1)
► STP	dead-criteria重试次数: 0
▶ DHCP中继	dead-criteria 超时时间 : 0
▶ DHCP服务器	修改國畫
TACACS+	
RADIUS	
• RADIUS配置	
AAA	
▶ QoS管理	
▶ 地址表	
▶ Snmp管理	
N LACD	

4.10.1 RADIUS 配置

▶ 系统管理

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	
ADIUS全局配置信息	
服务器重传次数:3	
服务署超时时间:2	
服务器静默时间:0	
dead-criteria重试次数: 0	
dead-criteria超时时间: 0	
8改配置	

【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。

Radius全局配置 Radius	该务器配置		
RADIUS全局配置信息			
服务器重传次数:3			
服务器超时时间:2	RADIUS全局配置		×
服务器静默时间:0	服务器重传次数:	3 [1-100]	
dead-criteria重试次数:0	服务器超时时间:	2 [1-1000]	
dead-criteria 招时时间 : 0	服务器静默时间:	200 [1-1440]	
修改配置	dead-criteria招时时间:	5 [1-100]	
	and output the state of the sta	[] [] [] [] [] [] [] [] [] [] [] [] [] [
	保存 取消		

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。

Radius全局配置	Radius服务器配置				
服务器列表					
IP地址	认证端口	密钥	主动探测	统计信息	操作
◎ 新建服务器				 首页 上一页 [1] 下一页	尾页1 /1页

【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,认证端口和密匙为默认,开启主动探测并设置测试 名称我 test,空闲时间为 3。

Radius全局配置	Radius服务器配置				
服务器列表					
IP地址	认证端口	密钥	主动探测	统计信息	操作
③ 新建服务器	新建服务器			× [1] 下—3	5 尾页1 /1页
	添加了	服务器地址: 192.168. 认证端口: 密想: 主动探测: 型 开启 测试名称: セst 空用时间 3	0.68		

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:

►	A	AAA						
	•	AAA使能配置						
	•	域配置						
	•	服务器组配置						
	•	AAA认证配置						

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。

AAA模块使能:	
保存	状态: ¹ 开启 ¹ 关闭

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:

🗾 系统首页	域使能配置				
🔜 快速配置		状态: ● 开启 〇 关闭]		
▶ 端口管理	保存				
▶ VLAN管理	ISDHat				
▶ 故障/安全	13-13				
▶ PoE管理		域名:	(1-30个字符)		
► STP	认证田白县丕雄	伝念: DIUCK ・	-		
▶ DHCP中继	添加				
 DHCP服労器 TACACC 	201208				
	ISP域名列表				
, INDIGS	補々	拔态	是否携带域名	缩完方室	操作
AAA	A3440	0005		WALT JA.	
 AAA AAA使能配置 	default	active	without-domain	WALIJA.	×
 AAA AAA使能配置 域配置 	default	active	without-domain	前面上一页 [1]	★ 下一页 尾页1 /1页
 AAA AAA使能配置 域配置 ・ 販务器组配置 	default	active	without-domain	₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	★ 下一页 尾页 <mark>1 /1页</mark>
 AAA AAA使能配置 域配置 服务器组配置 AAA认证配置 	default	active	without-domain	前 页 上一页 [1]	★ 下一页 尾页 1 /1页
 AAA AAA使能取置 域配置 域配置 服务器组配置 AAA认证取置 QoS管理 	default	active	without-domain	首页 上一页 [1]	★ 下一页 尾页 <mark>↓ /1页</mark>
 AAA AAA使能配置 域配置 販売器组配置 AAAi从证配置 AAAi从证配置 QoS管理 地址表 	default	active	without-domain	首页 上一页 [1]	¥ 下─页
 > AAA · AAA(快能設置 · MGR置 · MGR置 · AAA(认证器置 · AAA(认证器置 · AAA(认证器置 · QoS管理 · 地址表 > Snmp管理 	default	active	without-domain	首页 上一页 [1]	★ 11页
 ▲ AAA ▲ AAA(使能說麼 ▲ MAK(使能說麼) ▲ MAK(加嚴置) ▲ AAA认证配置 ▲ ADAA认证配置 ▲ QoS管理 ▶ 地址表 > Snnp管理 > LACP 	default	active	without-domain	前页上一页 [1]	★ 11页

【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。

域使能震器							
状态: ● 开启) ◎ 关闭 【保存							
ISP域							
	域名: work	(1-30个字符)					
	状态: block 🔹						
认证用户是否携	带域名: with-domain 💽						
添加							
ISP域名列表							
域名	状态	是否携带域名	绑定方案	操作			
default	active	without-domain		×			
			首页 上一页 [1]	下一页 尾页1 /1页			

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:

🛃 系統首页	服务器组配置				
🔜 快速配置	服务器名:		选择服务器: radius 💌		
▶ 端口管理	服务器IP地址:	7	认证端口: (0-65535)		
▶ VLAN管理	保存				
▶ 故障/安全					
▶ PoE管理	当前服务者列表				
► STP	服务器名	协议	服务器地址	认证端口	操作
▶ DHCP中继				 首页 上一页 [1] 下	-页 尾页1 /1页
▶ DHCP服务器					
TACAUS+ DADUUS					
RADIUS					
 AAA使能配管 					
 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」 」					
・服务署组配置					
• AAA认证配置					
▶ QoS管理					
▶ 地址表					
▶ Snmp管理					
LACP					
▶ 系统管理					

【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 asa 选择服务器: lacacs+ ▼ 服务器IP地址 192.168.0.66				
保存				
当前服务器列表				
服务器名	协议	服务器地址	认证端口	操作
ааа	tacacs+	192.168.0.66		×
ааа	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。

当前服务署列表				
服务器名	协议	服务器地址	认证端口	操作
aaa	tacacs+	192.168.0.66		8
ааа	radius	192.168.0.65	49	×
			首页 上一页 [1] 下-	-页 尾页 <mark>1 /1页</mark>

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:

🛃 系統首页	Login认证 Enable认证 Dot1x认证		
🔜 快速配置	AAA的认证配置		
▶ 端口管理	- 法择—个城名 none ▼		
▶ VLAN管理			
▶ 故障/安全	LOGIN认证 方:	案名称: default	
▶ PoE管理	第一方法: 本地服务器组		
STP	第二方法:		
▶ DHCP中继	第三方法:		
▶ DHCP服务器	第四方法:		
TACACS+	保存		
RADIUS			
 AAA AAA(由於兩要) 	login认证列表		
· interest	方案名称	方法	操作
 - 成自血 - 服务契组酚署 	default	(local)	×
• AAA认证配置			首页 上一页 [1] 下一页 尾页 1 /1页
▶ QoS管理			
▶ 地址表			
▶ Snmp管理			
LACP			
▶ 系统管理			

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:

 系统首页 、 快速配置 、 端口管理 > VLAN管理 > 故障/安全 > PoE管理 > STP > DHCPm维 > DHCP服务器 > TACACS+ > RADIUS 	Cogin认证 Enable认证 Dottx认证 AAA的认证配置 法择一个场名 none ▼ LOGIN认证 第一方法: 本地服务器组 ▼ 第二方法: 本地服务器组 ▼ 第二方法: 「▼ 第三方法: 「▼ 第三方法: 「▼ 第四方法: 「▼	方案名称: @sfwilt	
► AAA	login认证列表		
• 域配置	方案名称	方法	操作
 服务器组配置 	default	(local) (none)	×
• AAA认证配置		首页	上一页[1] 下一页 尾页1 /1页
 > QoS管理 > 地址表 > Snmp管理 > LACP > 系统管理 			

【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, 钩选 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。

Login认证 Ena	ble认证 Dot1x认证	
AAA的认证配置		
选择一个域名 none		
🕜 LOGN认证	方案名称:default	
第一方法:本地服	済器组 ▼	
第二方法: RADIU	JS服务器组 ▼	
第三方法: TACA:	S+服务器组 ▼	
第四方法: 自定义	(服务器组 ▼ 服务器组: ss	
保存		
login认证列表		
方案名称	方法	操作
default	(local) (group radius) (group tacacs+) (group ss)	
	首页 上一页 [1] 下一页 尾页 1	/1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:

🛃 系統首页	Login认证 Enable认证 Dot1x认证		
🔜 快速配置	AAA的认证配置		
▶ 端口管理 ▶ VLAN管理	选择一个域名 none 💌		
 故障/安全 PoE管理 STP DHCP中继 DHCP服务器 	ENABLE以近 方: 第一方法: 本地服务器组 第二方法: - 第二方法: - 第三方法: - 第三方法: - 第三方法: -	案名称: [defoult	
TACACS+RADIUS	保存		
AAA	enable认证列表		
• AAA使能配置	方案名称	方法	操作
 ・ 域電置 ・ 服务器组配置 	default	(local)	X
 AAA认证配置 			
 ▶ QoS管理 ▶ 地址表 ▶ Snmp管理 ▶ LACP ▶ 系统管理 			

【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,钩选 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。

Login认证 Enab	e认证 Dot1x认证	
AAA的认证配置		
选择一个域名nor		
() ENABLEX, 证 第一方法:本地服 第二方法: 第二方法: 第三方法: 第回方法: 第四方法: 第四方法: 第四方法:	方案名称: dofault 予器组 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
enable认证列表		
方案名称	方法	操作
default	(local) (group radius) (group tacacs+) (group ss)	×
	首页 上一页 [1] 下一页 [電页 <mark>1 /1页</mark>

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:

📑 系统首页	Login认证 Enable认证 Dot1x认证		
🔜 快速配置	AAA认证配置		
▶ 端口管理	赋名 none 💌		
▶ 故障/安全	dot1x认证 方案	3称: default	
▶ PoE管理	第一方法: 本地服务器组		
STP	第二方法:		
▶ DHCP中维	第三方法:		
▶ DHCP服务器	第四方法:		
TACACS+	授加		
RADIUS			
AAA	dot1x认证列表		
• AAA使能配置	方案名称	方法	操作
 ・ 域配置 			首页 上一页 [1] 下一页 尾页 1 / 1 页
 服务器组配置 			HAT AN CARA
・ AAA认证配置			
▶ QoS管理			
▶ 地址表			
▶ Snmp管理			
▶ LACP			

【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, 钩选 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。

Login认订	E Enab	De认证 Dot1x认证	
AAA认证配置	Ē		
	域名none		
	dot1x认证	方案名称: default	
ÿ	第一方法 <mark>:</mark> 本地服	済器组 ▼	
ÿ	育二方法: RADIU	JS服务器组 💌	
ÿ	第三方法: TACAS	S+服务器组 ▼	
ÿ	第四方法: 自定义	服务器组 ▼ 服务器组: ss	
增加			
dot1x认证列	利表		
方第	案名称	方法	操作
default		(local) (group radius) (group tacacs+) (group ss)	×
		首页上一页 [1] 下一	页 尾页1 /1页

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。

Þ	Q	oS管理
	•	队列设置
	•	映射队列

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:

🗾 系统首页	队列设置		
🔜 快速配置	调度策略:	SP	•
▶ 端口管理	应用		
▶ VLAN管理			
▶ 故障/安全			
▶ PoE管理			
► STP			
▶ DHCP中继			
▶ DHCP服务器			
TACACS+			
RADIUS			
► AAA			
▶ QoS管理			
・队列设置			
 映射队列 			
▶ 地址表			
▶ Snmp管理			
▶ LACP			
▶ 系统管理			

【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。

队列设置									
	调度策略:	WRF	2		-				
	字节 权值(0~127):	10	11	12	13	14	15	16	17
应用									

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:

📑 系統首页	康 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
🌉 快速配置	映射队列状态信息
▶ 端口管理	
▶ VLAN管理	服务ID 0 1 2 3 4 5 6 7
▶ 故障/安全	₿ ⋏ ⋽∐D 0 w 1 w 2 w 3 w 4 w 5 w 6 w 7 w
▶ PoE管理	保存设票
▶ STP	
▶ DHCP中继	
▶ DHCP服务器	
TACACS+	
RADIUS	
AAA	
▶ QoS管理	
 队列设置 	
• 映射队列	
▶ 地址表	
▶ Snmp管理	
▶ LACP	
▶ 系统管理	

【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 • 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 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	村	差分開	6 务到服	员务类别	映射	端	口到服	务类别明	榭						
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	差分月	辰务到 册	最务类别	映射	端	口到服	务类别明	央射							
差分服务代码,	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	差分服务到服务结	た おいちょう くちょう しんしょう しんしょ しんしょ	端口到服务类别	映射								
端口COS映射	端口COS映射												
端口: 服务![信任相 式: 应用	1 D= 0 夏 Cos	•											
控制列表													
端口		服务ID 信任模式											
	0	1	2	3	4	5	6	7					
1	т												
2	т												
3	т												
4	т												
5	т												
6	т												
7	т												
8	т												
							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。

服务类别到队列时	東射	差分服务	创服务类别	映射	端口到服	多类别映	đ
端口COS映射							
端口: 4 ▼ 服务ID: 4 ▼							
服务类别到队列	山映射	差分服务	务到服务类 》	別映射	端口到	服务类别映	射
端口COS映射							
端口: 5 ▼ 服务ID: 5 ▼							
服务类别型队列纳制 差力服务到	B552EINN 4	和空間最多类別映射					
14日COSM991 14日:8 1日日日 1日日 1日日 1日日 1日日 1日日 1日日 1日日 1日日 1):						
拉顿列表					NR 45		
961-1	0	1	2	3	4	5	6
1	T						
2	Ŧ						
3	т				~		
4					(T)		
5						(†)	
7	т						\odot
	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。

🗾 系统首页	地址表配置				
🤜 快速配置	MAC添加和删除	MAC学习和老化 MAC地址过滤			
 端口管理 VLAN管理 故障/安全 PoE管理 STP 	素除細AC: 素除描描MAC地址 VLAN: 1 有效范围(1 to 4094) MAC地址: (保存 〇口 白 送州口 全 6 〇口 白 送州口 ① 愛古 山 ○ 〇口 白 送州口 ② 愛古 山 ○ 〇口 古 送州口 ② 愛古 山 ○ 〇田 送州口 ○ ○ 〇田 送州口 ○ ○ 〇田 送州口 ○ ○ 〇田 送州口 ○ ○ 〇田 送山 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○				
 DHCP中继 DHCP服务器 TACACS+ RADIUS AAA QoS管理 地址表 地址表 					
▶ Snmp管理	MAC地址列表: 全部 •				
 ► ACP ▶ 系统管理 	编号	MAC地址	VLAN ID	地址类型	端口
	1	D4:68:BA:09:11:DF	1	静态	Management
	2	50:BD:5F:C8:24:7E	1	动态	2
	3	00:E0:53:08:B2:32	1	动态	1
					首页 上一页 [1] 下一页 尾页 1 /1页

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:

🛃 系統首页	地址表配置				
🖏 快速電器	MAC添加和删除	MAC学习和老化 MAC地址过滤			
 端口管理 VLAN管理 放降皮全 PoE管理 STP DHCP中维 DHCP服务器 TACACS+ RADIUS AAA QoS管理 地址表 他出表 	清除指定ШAC地址 VLAN: 1 育效范围(1 to 4094) MAC地址: ① ① ① ○ □ ② ○ ○ □ ② ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○ □ ○ ○ ○				
▶ Snmp管理	MAC地址列表: 全部				
 ► 系统管理 	编号	MAC地址	VLAN ID	地址类型	端口
	1	D4:68:BA:09:11:DF	1	静态	Management
	2	50:BD:5F:C8:24:7E	1	动态	2
	3	00:E0:53:08:B2:32	1	动态	1
					首页 上一页 [1] 下一页 尾页 1/1页

【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
	単播 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。

	_			
)			
🗋 可选端口 💼 不可	±端口 💼 选中端口 ஹ 緊合端口 ஹ Trunk口			
VLAN:	1 有效范围(1 to 4094)			
MAC地址:	00:E0:53:08:E2:33			
保存				

2)清除端口6静态的 Mac 地址。

MAC添加和删除	MAC学习和老化 MAC地址过来
清除MAC: VLAN: MAC地址: 保存	濱条指定MAC地址 ▼ 1 00:E0:53:06:B2:33

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:

地址表配置					
MAC添加和删除 MAC学习和老化 MAC地址过滤					
88888					
2 4 6 8 10					
500 可选端口 100 不可选端口 100 近	选中端口 <u>517</u> 聚合端口 <u>5…7</u> Trunk口				
提示: 可按住左權把視选职多个端口	(0まって限制(0.9101)				
保存	(0351) (0351/J/460010101)				
MAC地址老化时间:	300 (0表示不老化,10-1000000秒)				
1來1丁	保住				
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					
	首页 上一页 [1] [2] 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添加和删除 MAC学习和老化 MAC地址过渡	
2 <u>4 6</u> 8 10 ○可送端口 壹 不可送端口 壹 选中端口 ① 聚合端口 … Trunk口	
提示:可技住左鍵相快速取多个端口 MAC/抱址学习限制: 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,10-100000秒)	
保存			

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:

地址表配置								
MAC添加和删除 MAC学习和老化 MAC地址过速								
MAC 地址: VLAN: 有效范围(1 to 4094) 过 波方向: 								
MAC地址 VLAN ID 地址类型 删除								
首页 上一页 [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。

Mac添加和删除	Mac学习和者化 MindBittel/Ce							
「 保存」 副除	Machalde : 00:20:15:09:13:12 Vian : (1-4094)							
编号	MAC地址	VLAN ID	地址类型	端口				
1	00:20:15:09:13:12	1	过增					

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。

Þ	Snmp管理							
	•	Snmp配置						
	• Rmon配置							

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:

📑 系統首页	SNMP设置 团体 组 用户 Trap 视图
🔜 快速配置	SMMPRE
▶ 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	
• Snmp配置	
• Rmon配置	
► LACP	
▶ 系统管理	

【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。
SNMP设置 团体 组 用户 Trap 视图
SNMP配置
(Spen)

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:

SNMP设置	团体组	用户	Trap	视图		
SNMP团体列表						
		团体名称			访问权限	操作
③ 新建团体 ◎ 删除选择团体 首页 上一页 [1] 下一页 属页 1 /1页						

【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。

SNMP设置	团体	(组) 用户	Trap	视图			
SNMP团体列表							
		团体。 SNMP团体配置	.称		沾词奴服	×	操作
◎ 新建团体 ◎ 刪	除选择团体	团体名称: 访问权限:	public Read Write	* 字	符串长度[1-16]		[1] 下一页 尾页1 /1页
		保存设置	退出				

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:

SNMP设置	团体组	用户 Trap 视图					
视图名称 * 字符串长度[1-16]							
新建视图	新建视图						
视图规则列表	視图規则列表 ■ 删除视图						
规则 MIB子树OID 子树撬码 操作							
◎ 新建视图规则 ◎ 删除选择视图规则 首页 上一页 [1] 下一页 尾页 1 /1页							

【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。

SNMP设置	团体	组	用户	Trap	视图
视图名称 (新建视图	123	*	字符串长度[1-1	6]	

SNMP设置团体	组 用户 Trap 视图	
視图名称 123	* 字符串长鹰[1-16]	
新建视图	编辑视图规则	
视图规则列表 123	excluded作用于included内容的子集,单独使用excluded不生效	
规则	規则 : 包含 排除 	操作
included	MIB子树OID: 1.3.6.1 * 字符串长度[1-64]	X
◎ 新建视图规则 🗇 删除选择被	子树撬码: 123456 * 字符串长度[1-31]	[1] 下一页 尾页1 /1页
	保存设置 退出	
祝聞規则列表 123 規則 前にはded 前は、日本の一部の目前には、 前は、 前は、 前は、 前は、 前は、 前は、 前に、	excluded作用于included内容的子集,单独使用excluded不生效 规则 ● 包含 ● 排除 MIB子树OID: 1.3.6.1 * 字符串长度[1-64] 子树掐码: 123456 * 字符串长度[1-31]	援作 2 X 11 下一页 尾页1 /1页

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:

SNMP	SNMP设置 团体 组 用户 Trap 视图					
SNMP组		Ŭ				
	组名称	安全级别	只读视图	读写视图	通知视图	操作
③ 新建组	🥥 刪除选择租				首页上一页[1] 下一页尾	页1 /1页

【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、	关联的视图名
通知视图	

【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。

视图规	则列表 123 💽 删除初	NB				
	规则	MIB子树OID	子树掩码	操作		
	included	1.3.6.1	123456	2 🗙		
③ 新建	② 新建视图规则 ◎ 删除选择视图规则 首页 上一页 [1] 下一页 尾页1 // 1页					

SNMP设置	团体	组用户Trap	视图			
SNMP组						
	组名称	安全级别	只读视图	读写视图	通知视图	操作
◎ 新建组 🤤	删除选择租	新建组			× 下一页 厚	页1 /1页
		组名称: goup	1 * 字符串长度	1-16]		
		安全级别: 只认	证不加密 💌			
		只读视图: 123				
		读与视图: 123 通知视图: 123				
		保存设置 退出				

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:

SN	MP设置团体	组用户	Тгар	视图				
SNM	P用户	\smile						
	用户名称 安全级别 组名称 认证模式 认证密码 加密模式 加密密码 操作							
③ 新	建用户 🤤 删除选择用户	4				首页上	:一页[1] 下一页 尾页 <mark>1</mark>	/1页

【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。

71■ 配置指南

SNMP用户		Mr 63	
用户名称	<u>安全纪别</u> 组 <u>久</u> 称 编辑 SNMP用户	は证模式 は证率語 加密模式 加密密码 ×	操作
② 新建用户	用户名称: 安全级别: 组名称:	vser1 (1) 下一页 尾页 1 只认证不加密: ・ goup1 ・ usc	/1页
	以证偿式: 认证密码: 确认认证密码: 加密模式:	NDS ▼ 12345878 * 字符串长度[8-60] 12345878 *	
	加密密码: 确认加密密码:	· · · · · · · · · · · · · · · · · · ·	
	保友设置 退出		

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:

SNMP	25日 一团体 组 用所	^コ Trap 视图			
Trap目标主	主机.				
	目的IP地址 安全名称 UDP端口号 安全視式 操作				
◎ 新建Tra	② 新建Trap				

【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阀值。

【配置举例】

如:设置主机 192.168.2.30 来接收 trap 消息。

SNMP设置团体组用户	Trap 视图
Trap目标主机	
目的IP地址 新建Trap	
目的P地址:	192, 168, 0, 30
安全名称: UDP端口号:	162 *
安全模式:	V1
保存设置	週出

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:

🛃 系統首页	统计组	历史组告警组	事件组		
🔜 快速配置	统计组列表				
▶ 端口管理		索引	接口名称	所有者	操作
▶ VLAN管理			TYPE BEAL	2011	200.00
▶ 故障/安全	◎ 新建统计组			首页 上一页	[1] 下一页 尾页1 /1页
▶ PoE管理					
▶ STP					
▶ DHCP中继					
▶ DHCP服务器					
TACACS+					
RADIUS					
AAA					
▶ QoS管理					
▶ 地址表					
▶ Snmp管理					
• Snmp配置					
• Rmon配置					
▶ LACP					
▶ 系统管理					

【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。

统计组 历史组	告警组 事件组	
统计组列表		
	索引 接口名称	所有者 操作
◎ 新建统计组) ◎ 删除选择统		
	索引: 777 *	
	接口名称: interface Gi0/4 💌 *	
	所有者: coco * 字符串长度[1-30]	
	保存设置 退出	
(统计和) 医内相	生物如 古州如	
统订组 历史组	古言组 争什组	
统计组列表		
☑ 索引	接口名称	操作
77	4 COCO	😔 📄 🗙
📀 新建统计组 😑 删除选择统	计组	🖌 首页上一页 [1] 下一页 尾页1 /1页
	统计信息	×
	Number of Packet Discarding Events :	0
	Number of Received Bytes :	0
	Number of Received Packets :	0
	Number of Received Broadcasting Packets :	0
	Number of Received Packets With CRC Check	
	Failed :	0
	Number of Received Packets Larger Than 1518	U T
	退出	

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:

统计组	l 历史组	告警组 事(牛组						
历史组列	历史组列表								
	索引	接口名称	最大采样条数	采样周期	所有者	状态	操作		
 ③ 新建历史组 ◎ 删除选择历史组 首页 上一页 [1] 下一页 尾页 1 /1页 									

【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。

统计组 历史组 告警组	事件组					
历史组列表						
索引 接口名	<u>称 最大</u>	<u> 采样条</u> 動	委样周期	所有去	状态	操作
新建历史组 图除法择历史组	かえて出れ」正 索引: 塗口名称: 最大采祥条数: 采祥周期: 所有者: 復存设置 週出	222 Interface Gi0/4 • 2222 300 coco	。 。 。 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	文 上一步	瓦 [1] 下一页 尾页1	/1页

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:

统计组	历史组告警线	组 事件组					
事件组配置							
	索引	描述	所有者	动作	状态	操作	
 ③ 新建事件组 ◎ 删除选择事件组 首页 上一页 [1] 下一页 尾页 1 							

【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。

统计组 历史组 告	警组 事件	组			
事件组配置					
□ 索引	^{描述} 事件组配置	新有考	zhft	<u>本</u> 北 ×	
9 99 4 9 1 - 10 9 19 4 9 - 10 9 19 19 19 19 19 19 19 19 19 19 19 19 19	索引: 描述: 所有者: 动作: 保存设置	345 212 coco ☑ Log ☑ Trap 遐出	0] [C		

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:

1	统计组		历史组	告警组	事件	组							
告	警组列	间表											
	索引	静态表 项	统计组索 引	采样时间间 隔	采样类 型	最近一次采样 值	告警阀值上 限	超过阈值上限所执行的事 件	告警嗣值下 限	低于阈值下限所执行的事 件	所有 者	状态	操作
0	◎ 新建报警组 ◎ 删除选择报警组 首页 上一页 [1] 下一页 尾页 1 /1 页												

【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:CRCAlignErrors;
	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
告警阀值上限	设置上限参数值
告警阀值下限	设置下限参数值
超过/低于阈值下限所	上限/下限达到时,各自对应的事件号
执行的事件	
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。

统计组	历史组	告警组	事件组										
告響组列表													
富 都 御 御 御 御 御 御 御 御 御 御 御 御 御 御 御 御 御 御	态表 统计组索	采样时间间	采样类 最近	一次采祥	告警阀值上	超	过调值上限所执行的事	告響阈值下	低于阈值下限所执	.行的事	所有	状态	操作
()新建报题	10 🖉 🖉	统计组配置							×	下_石	日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	765	IF 否
WINE IN C		索引:		12	:3		* [1-65535]				JEDA I		
		静态表项:		D	ropEvents				•				
		统计组索引:		7	7	•							
		采样时间间隔	:	55	i		* 秒						
		采样类型:		A	bsolute	•							
		所有者:		co	000		* 字符串长度[1-30]						
		告警阀值上限	:	30	00		* [0-2147483647]						
		超过阈值上限月	所执行的事件:	3	45	•							
		告響阈值下限	:	10	100		* [0-2147483647]						
		低于阈值下限」	所执行的事件:	3	45	•							
		保存设置	退出										

4.15 LACP

在导航栏中选择"LACP",您可以设置"LACP设置"和"LACP显示"。

🗾 系统首页	LACP设置
🔜 快速配置	
▶ 端口管理	LACP状态
▶ VLAN管理	开启LACP:
▶ 故障/安全	应用
▶ PoE管理	LACP公共参数设置
▶ STP	系统优先级: 1 (1-66535)
▶ DHCP中维	应用
▶ DHCP服务器	
TACACS+	LACP進名端口參劃役置
RADIUS	选择端口进行设置:
► AAA	1 3 5 7 9
▶ QoS管理	
▶ 地址表	
▶ Snmp管理	2 4 6 8 10
▶ LACP	空可递溯口 🧝 不可递溯口 💼 选中端口 迎 繁谷渊口 🖳 Тгилкд
• Lacp	<mark>提示:</mark> 可按住左键掩摸选取多个端口 全选 反迭 取消选择
▶ 系统管理	諸口优先级: 1 (1-65535)
	江裂端口编号: 1 💌
	聚合模式: active ▼
	应用

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。

📑 系統首页	LACP设置 LACP显示
🖏 快速配置	
▶ 端口管理	LAUPAO
▶ VLAN管理	+ HELAUP:
▶ 故障/安全	12/11
▶ PoE管理	LACP公共参数设置
STP	系统优先级: 1 (1-65535)
▶ DHCP中继	应用
▶ DHCP服务器	
TACACS+	LACP邀去端口参数设置
RADIUS	选择端口进行设置:
► AAA	1 3 5 7 9
▶ U05官理	
▶ Compting	
	Contesting (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Lacp	
▶ 系统管理	
	Water Contract Cont
	应用

【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。

LACP设置	LACP显示
LACP状态	
应用	开启LACP:

2.设置系统优先级。

LACP公共参数设置			
- 系统优先级: 1	(1-65535)		
应用			

3.设置端口 LACP 功能。

LACP激活端口参数设置				
选择端口进行设置:				
1 3 5 7 9 $1 2 7 7$ $2 4 6 8 10$				
🛄 可选端口 💼 不可选端口 💼 ;	选中端口 <u>517</u> 聚合端口 <u>5</u> Trunk口			
提示: 可按住左键拖拽选取多个端口	1 全选 反选 取消选择			
端口优先级:	I (1-65535)			
汇聚端口编号:	1			
聚合模式:	active			
应用				

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设置									
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 属页 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. 删除己 LACP 功能的端口。

LACP设置 LACP显示									
LACP列表	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	X
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。



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:

📑 系統首页	系统设置 系统重启 密码修改 EEE快能 ssh登录 Teinet登录 系统日志
🤜 快速配置	系统基本信息
端口管理	
VLAN管理	ELECTRIC I KIIMAC. PRODUCTION IN THE
故障/安全	管理IP: 132.168.0.1 ipv6地址:
PoE管理	撞码: 255.255.0 * 设备名称: Switch
STP	默认网关: 0.0.0.0 设备位置:
DHCP中维	巨型特: 1518 (1518-9216) 联系方式(含脚箱):
DHCP服务器	DNS服务器: 0.0.0.0
TACACS+	登陆超时(分): 30
RADIUS	保存设置 设责管理vian
AAA	
QoS管理	系统时间
地址表	当前系统时间: 2000-01-01 03:05:10
Snmp管理	重新设置时间:
LACP	自动与Internet时间服务器同步
系统管理	保存设置
 系统设置 	
• 系统升级	
 配置管理 	
 配置保存 	

【参数说明】

管理员权限
 一键信息收集

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。

VLAN	V设置 Trunk口设置	Hybrid口设置						
VLAN	VLAN列表							
	VLAN ID	VLAN 名称	VLAN IP 地址	端口	操作			
	1	VLAN0001	192.168.0.1/24	1-4,7-10				
	2	VLAN0002		5-6	2 🗙			
O 新建	VLAN 🥥 删除选择VLAN			首页 上一页 [1]	下一页 尾页1 /1页			
(- * 1)								
条统i	发置 系统重启	密码修改 EEE使能	ssh登录 Teinet登录 系统日	志				
系统基本	本信息							
	管理VLAN: 2	* <u>5</u>	备MAC: [D4:68:BA:09:11:DF]					
	管理IP: 192.168.0.1	* ip	v6地址:					
	掩码: 255.255.255.0	* <u>'</u>	备名称: Switch					
	默认网关: 0.0.0.0	<u></u> 近	备位置:					
	巨型轴: [1518 (1518-9216) 联系方式(含邮箱):							
0	DNS服务器: 0.0.0.0							
登	登陆超时(分): 30							
保存设	保存设置 取消设置							

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按批:						
撞码:	255.255.255.0 * 设备名称: yoyo						
默认网关:	0.0.0 设备位置:						
巨型帧:	5000 (15 ¹ 8-9216) 联系方式(含邮箱):						
DNS服务器:	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	200	0-01	01 0	3:09:	04		
里利吱直时间		4	1 -			_	
保存设置	-	•	+_	_	2016 m	Ŧ	- m
	27	28	29	30	1	2	3
	4	5	6	7	8	9	10
	11	12	13 20	14 21	15 22	16 23	17 24
	25	26	27	28	29	30	31
	1	2	3	4	5	6	7
	时间	19	: 1	: 1	-	4	Ð
	时间	a 19	: 1 清空	: 1	; 今天	前	₽ 碇

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	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
🖏 快速配置	大明道白辺為
▶ 端口管理	医学習の言葉
▶ VLAN管理	
▶ 故障/安全	
▶ PoE管理	
▶ STP	
▶ DHCP中维	
▶ DHCP服务器	
TACACS+	
RADIUS	
AAA	
▶ QoS管理	
▶ 地址表	
▶ Snmp管理	
▶ LACP	
 系统管理 不分別間 	
• 杀狁设立	
 系统升级 	
 配置管理 	
 配置保存 	
 管理员权限 	
 一键信息收集 	

【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】

81■ 配置指南

如:点击"立即重启设备"按钮。

系统设置	系统重启	密码修改	EEE使能	ssh <u>登</u> 录	Teinet登录	系统日志	
立即重启设备							

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:

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	
修改超级用户密码			
密码类型:	密文密码 🔻		
旧密码:	*		
新密码: 确认新密码:	*		
保存修改 清 空			

【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。

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
修改超级用户密码		
密码类型:	密文密码 🔻	
旧密码:	*****	3
新密码:	••••	*
确认新密码:	••••	Ż
保存修改 清 空		

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:

🖲 系统首页	系统设置 系统重启 密码修改 EEE使能 ssh萤录 Telnet萤录 系统日志
🤜 快速配置	EEE RX
▶ 端口管理	
▶ VLAN管理	Open
▶ 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	
【使用说明	明】

【配置举例】

例如: EEE 开启,可以高效节能以太网。

系统设置系统重启 密码修改	EEE使能 Ssh登录 Teinet登录 系统日志	
EEE 酌置		
Open		

4.16.1.5 SSH 登录

📑 系统首页	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
🔜 快速配置	ssher 🕅
▶ 端口管理	
▶ VLAN管理	Open
▶ 故障/安全	SSH 都时设置: 3 。
▶ PoE管理	保存配置
STP	
▶ DHCP中维	
▶ 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	

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。

系统设置 系统重启 密码修改 EEE使能 Ssh叠录 Telnet叠录 系统日志
ssh <u>戰</u> 置
Open
SSH 超时设置:3 " 使存配置

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:

🛃 系统首页	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
🦏 快速配置	Teine國法
▶ 端口管理	
▶ VLAN管理	
▶ 故障/安全	
▶ PoE管理	
▶ STP	
▶ DHCP甲進	
▶ 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	

【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。

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
Teinet <u>跟</u> 書
Open
Telnet趨时设置:3

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:

🖲 系統首页	系统设置 系统重启 密码修改 EEE使能 ssh叠录 Telnet叠录 系统日志					
🌉 快速配置	日志祝法					
▶ 端口管理	日志开关:					
▶ VLAN管理	服务器IP:					
故障/安全	发送日志等					
▶ PoE管理	3& Informational(6)					
STP	像存设素					
▶ DHCP中维	当前日志信息					
▶ DHCP服务器	关键字 查询 青空日志					
TACACS+						
RADIUS	Syslog logging: enabled					
AAA	Console logging: disabled Monitor logging: disabled					
▶ QoS管理	Buffer logging level debugging 2100 messages logged Timestamp debug messages: datelime Timestamp log messages: adtelime					
▶ 地址表						
▶ Snmp管理	Sequence-number log messages: disable Systame log messages: disable					
▶ LACP	Trap logging level informational, 2190 message lines logged, 0 fail to participate and 1006 Brieser's					
▶ 系统管理	Log Duner (rolar voor bres), Dec 21190/341 %PDE-Warnings-send_trap: The IC temperature is greater than the alarm temperature					
 系统设置 	Dec 21 1903.46 % POE-Warnings-send_Tap: The IC temperature is greater than the alarm temperature Dec 21 1903.47 % SNIMP-Notifications-ALARINTRAP: Send alarm trap: Failing:1.3.6.12.11.61.11.3.77=0 <= 1000:123, 345. Dec 21 1903.52 % POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature					
• 系统升级						
 配置管理 	Dec 21 19/0357 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature Dec 21 19/0402 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature Dec 21 19/0407 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature Dec 21 19/0417 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature Dec 21 19/0417 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature					
 配置保存 						
 管理员权限 	Dec 21 19/04/18 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature Dec 21 19/04/18 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature Dec 21 19/04/28 %POE-Warnings-send_trap: The IC temperature is greater than the alarm temperature version of the temperature version of temperature version					
• 一键信息收集						

【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。

系统设置	統重启 密码修改	EEE使能 ssh登录	Telnet登录	志
日志配置				
日志开关:	Open			
服务器IP:	192. 168. 0. 2			
发送日志等 级:	Errors(3)			
保存设置				

2) 输入 fial 关键字,进行查看,点击"清空日志"按钮,可清空日志

当前日志信息	
关键字〔1]	
Trap logging: level errors, 2204 message lines logged, 0 fail	•
	·

4.16.2 系统升级

📑 系统首页	体地升级
🤜 快速配置	当前软件版本是= D161116
▶ 端口管理	文件名: [396] 所如升级
▶ VLAN管理	
▶ 故障/安全	
▶ PoE管理	
STP	
▶ DHCP中维	
▶ 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 	

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。

本地升级				
当前软件版本是: D161116				
文件名:	浏览开始升级			
文件名:	減災 所給升級 ● 透得憂加愛的文件 ● 圆 桌面 → ・ ● 圖 桌面 → ・ ● 一 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	QQ電磁2010121/1105425.png Kankan PING 間像 339 K8 QQ電型20161219081601.png Kankan PING 間像 107 K8 QQ電型20161219081614.png Kankan PING 間像 1151 K8 QQ電型20161219081614.png Kankan PING 間像 191 K8 Image: State Sta	<u>援票 貞</u> 図 <u>日</u> 二 日 日 日 日 日 日 日 日 日 日 日 日 日	
	文件名(N): sw-2016.bix	所有文件(**) 打开(Q) 取消 :::	

4.16.3 配置管理

4.16.3.1 当前配置

📑 系统首页 当前配置 配置备份 恢复出厂配置 🔜 快速配置 查看当前配置 导出配置 ▶ 端口管理 ● 备份 ○ 导入配置 文件名: ▶ VLAN管理 .conf ▶ 故障/安全 确定备份 ▶ PoE管理 ► STP 备份文件列表 ▶ DHCP中继 名称 大小 修改时间 ▶ DHCP服务器 12357.conf 5.66K 15:38:34 2016-12-20 TACACS+ ► RADIUS ► AAA ▶ QoS管理 ▶ 地址表 ▶ Snmp管理 ▶ LACP
 ▶ 系绕管理
 ● 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

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。

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 ○ 時入 				
确定备份				
备份文件列表				
名称		大小		修改时间
12357.conf		5 RRK		15:38:34 2016-12-20
3	猎豹高速下载		×	
4	保存到: 📃 桌面	剩余空间:36.096 ▼	更改	
3	文件名: switch.conf	文件大小:未知		
	网址来源: 192.168.0.1			
	直接打开	下载取消		
			-	

2) 导入配置

当前配置 配	出置备份 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! 白田新的翻署,满方太百五 重白恐為 不回翻署去也	- 1 24				
证小: 守八郎直后, 安. 文件々。		-288				
2010						
备份文件列表						
	运 选择要加载的文件		×	修改时间		
12357.conf		- +→ 搜索 桌面	م م	34 2016-12-20		
	组织 ▼ 新建文件夹		₩ - ▼ - 0			
	 ○ 库 ● 視频 ● 副片 ● 首乐 ● 首乐 ● 甘茸丸 ● 本地磁盘(P:) ● 本地磁盘(P:) ● 本地磁盘(P:) ● 本地磁盘(P:) ● 本地磁盘(P:) ● CO 驱动器(F:) ● 网络 ○ 文件名(N: switch.conf 	2 10.FR-S3010PEGMF-C Jnstall Suide, V1.0_2016.12.15(中英 ioft Word 97 - 2003 文档 conf 文件 3 ssMon 式 5 5 3 4[V05W6]]529ZQGX5.png 新有文件(** 打开(血)	日、「「「」」「」」「」」「「」」」」「「」」」」」」」			
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 🧕 🌘	◎ 备份 ◎ 导入配置					
导入过程中 <mark>提示:</mark> 导	不能关闭或者刷新页面,召 入配置后,要启用新的配置	3则导入将失败! 3,请在本页面 重启 设	否则配置7	~生效		
文件名:	浏览… 未选择文件。	导入配置	5			
 3)备份文件						
当前配置	置 配置备份	恢复出厂配置				
查看当前配	置 导出配置					

 查看当則配面 导出配面 ● 备份 ○ 导入配置 文件名: switch123 	Conf	
确定备份		
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:

当前配置 配置备份 恢复出厂配置				
名称	大小	修改时间		
12357.conf 5.66K 15.38:34 2016-12-20				
 ◎ 恢复备份 ◎ 歸除备份 ◎ 見存备份 ◎ 重命名备份 确定恢复 				

【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。

当前配置 配置备份 恢复出厂配置				
名称	大小	修改时间		
12357.conf 5.66K 15:38:34 2016-12-20				
● 恢夏备份 ● 账除备份 ● 另存备份 ● 重命名备份 重合名: switch2 conf 餐定重命名				

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:

 当前配置
 配置备份
 快复出厂配置

 号出当前配置
 恢复出厂配置

【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。

当前配置 配置备份 恢复出厂配置 导出当前配置 恢复出厂配置

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:

📑 系统首页
🔜 快速配置
▶ 端口管理
▶ VLAN管理
▶ 故陵/安全
▶ PoF管理
) STP
▶ DHCP由维
▶ DHCP服务器
> DADULS
▶ Weitt≠
▶ 旭川波
▶ Snmp官理
► LACP
▶ 杀说官理
• 杀绒收直
 系统升级
 ・
• 配置保存
 管理员权限
 一键信息收集

【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。

保存配置

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:

🗾 系统首页	管理员权限	
🔜 快速配置	海四未到· 您立您四 -	
▶ 端口管理	田内2・ 	
▶ VLAN管理	· · · · · · · · · · · · · · · · · · ·	
▶ 故障/安全		
▶ PoE管理		
▶ STP	^{添加用户}	
▶ DHCP中维	用户列表	
▶ DHCP服务器	用户名	操作
TACACS+		
RADIUS	user	
AAA	admin	Ø
▶ QoS管理		首页 上一页 [1] 下一页 尾页 1 /1页
▶ 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 		

【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:

📑 系统首页	b 集信員
🤜 快速配置	- Constitution
▶ 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 	
 一緒信息收集 	

📴 系统关西

【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		
		8 个 10/100/1000Mbps 自适应 RJ45 端口(Auto MDI/MDIX)		
端口		2 个 1000Mbps SFP 接口		
		1 个 Console 口		
		10Base-T: 3 类或 3 类以上 UTP		
网络媒介		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		
	每台	Power		
指示灯	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(L×W×H)		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

 1.1 Product Overview 1.2 Features 1.3 External Component Description 1.3.1 Front Panel 1.3.2 Rear Panel 1.4 Package Contents 	1 1 1 3 4
Chapter 2 Installing and Connecting the Switch	5
 2.1 Installation	5 5 6 6
Chapter 3 How to Login the Switch	8
3.1 Switch to End Node 3.2 How to Login the Switch	8 8
3.1 Switch to End Node 3.2 How to Login the Switch Chapter 4 Switch Configuration	8 8 10
 3.1 Switch to End Node	8 8 10 12 13 14
 3.1 Switch to End Node 3.2 How to Login the Switch Chapter 4 Switch Configuration 4.1 Quickly set 4.2 PORT 4.2.1 Basic config 4.2.2 Port Aggregation 4.2.3 Port Mirroring 	8 8 10 12 13 14 15
 3.1 Switch to End Node	8 8 10 12 13 14 15 16 17 18
 3.1 Switch to End Node	8 8 10 12 13 14 15 16 17 18 19 20 21
 3.1 Switch to End Node 3.2 How to Login the Switch Chapter 4 Switch Configuration 4.1 Quickly set 4.2 PORT 4.2.1 Basic config 4.2.2 Port Aggregation 4.2.3 Port Mirroring 4.2.4 Port Limit 4.2.5 Storm control 4.2.6 Port isolation 4.2.7 Port information 4.3 VLAN 4.3.1 VLAN config 4.3.2 Trunk-port setting 4.3.3 Hybrid-port setting 	8 8 10 12 13 14 15 16 17 18 19 20 21 22
3.1 Switch to End Node 3.2 How to Login the Switch Chapter 4 Switch Configuration 4.1 Quickly set 4.2 PORT 4.2.1 Basic config 4.2.2 Port Aggregation 4.2.3 Port Mirroring 4.2.4 Port Limit 4.2.5 Storm control 4.2.6 Port isolation 4.2.7 Port information 4.3 VLAN 4.3.1 VLAN config 4.3.2 Trunk-port setting 4.3.3 Hybrid-port setting 4.4.1 Anti Attack 4.4.1 DHCP	8 8 10 12 13 14 15 16 17 18 19 20 21 22 23 24 24

4.4.2 Channel detection	28
4.4.2.1 Ping	
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	
4.5.1.2 Temperature distribution	
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	
4.7 DHCP RELAY	
4.7.1 DHCP Relay	
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	
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	
4.12.2.3 Port COS Map	
4.13 Address table	60

Appendix: Technical Specifications	87
4 16 6 Info Collect	20 AR
4 16 5 Administrator Privileges	04 פק
4 16 4 Config Save	
4 16 3 3 Restore factory configuration	۵4 ۸۸
4.16.3.2 Configuration backup	۵۷ م
4.10.3 CUTIII Wallagement	82 دە
4.16.2 Config Management	81
4.16.2 System log	80
4.16.1.6 leinet login	
4.16.1.5 SSH login	
4.16.1.4 EEE Enable	
4.16.1.3 Password change	
4.16.1.2 System restart	77
4.16.1.1 System settings	
4.16.1 System Config	75
4.16 SYSTEM	74
4.15.2 LACP Display	74
4.15.1 LACP Setting	73
4.15 LACP	72
4.14.2.4 Alarm Group	71
4.14.2.3 Event Group	70
4.14.2.2 History Group	69
4.14.2.1 Statistics Group	68
4.14.2 Rmon Config	68
4.14.1.6 Trap	67
4.14.1.5 User config	
4.14.1.4 Group Config	65
4.14.1.3 View Config	65
4.14.1.2 Community config	64
4.14.1.1 Snmp config	63
4.14.1 Snmp config	63
4.14 SNMP	63
4.13.3 Mac address filtering	62
4.13.2 Mac study and aging	61
4.13.1 Mac Management	60

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	STATU S	STATUS DESCRIPTION
PWR	Green	On	Power On
		Off	Power Off
Link/Act/ (1-8)	10/100M:	On	A device is connected to the port
	Orange	Off	A device is disconnected to the part
	1000M:	Oli	A device is disconnected to the port
	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.





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.

	P Networks				×
<	>	Ø	5	☆	192.168.0.1/index.htm

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.

	8-Port Gigabit Managed PoE Switch with 2 SFP SI	ots
Please input u	user name and password !	
User Name:	admin	
Password:	•••••	
Language:	English 🗸	
	LOGIN	

	Y	Current username: admi	n				▶ Exit	Language
Home Guickly Set PORT	Device Type: SW-5 Serial Number: G1GE	5010 30U S007211	Software Version: D161116 Hardware Version: 1.00	Uptime: <mark>11 min</mark>				
 VLAN Fault/Safety PoE STP DHCP RELAY DHCPRELAY DHCPREVY TACACS* RADIUS AAA QOS Addr Table SMMP 				5 6 7 8 Console 9F	10F 	сон 💼 100ж 🤞	раз 💼 Улсане	ot 🖻 Closed
 LACP SYSTEM 	Port Information	Device Configuration	Port Statistics					
	Reyword Input port	number or port description	Input Flow	(Rns) Output Flow/Rns)	Port Status	Port Connection	VLAN	Trunk Port
	Gi 0/1	Description	0.00K	0.00K	ON	S 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
						Firs	st Back [1] Next Las	st1 / 1 Page

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.

	Y	Current username: admin					Exit	Language		
Home Quickly Set PORT VLAN Eault/Safety	Device Type: SW-5 Serial Number: G1GE	1010 Soft 30US007211 Harc	ware Version: D161116 tware Version: 1.00	Uptime: <mark>11 min</mark>						
 Padin Safety PoE STP DHCP RELAY DHCPserver TACACS+ RADIUS AAA QOS Addr Table SMMD 				7 8 Console 9F	10F	оам 💼 100ам 🧯	PDE 💼 Unconnec	ot 💼 Closed		
 SNMP LACP 	Port Information	Device Configuration	Port Statistics							
► SYSTEM	Keyword Input port	t number or port description	Search Refresh							
	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		
	First Back [1] Next Las(1 /1 Page									

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:

	Y	Current username	admin					Exit Languag	
E Home	VLAN S	etting Other setti	ngs						
PORTVLAN		VLAN ID		VLAN Name		VLAN IP	Port	Edit / Delete	
 Fault/Safety PoE STP 	O New VI	LAN 🤤 Delete VLAN				102.100.0.12.F	First Back [1]	Next Last ¹ / 1 Page	
 DHCP RELAY DHCPserver 	Trunk Settings Port Name		Description			Allowed Vlan		Edit / Delete	
 TACACS+ RADIUS AAA 	New Tr	runk Port 🤤 Delete Trunk P	ort						
QOSAddr Table									
 SNMP LACP SYSTEM 									
or or Lin					•	Next			

[Parameter Description]

VLAN number, 8GE default VLAN 1
VLAN mark
Manage the IP address of the VLAN
Switch name
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.

	Y	nt username:	admin		Þ	Exit Language
🛃 Home	VLAN setting	Other settin	ngs			
🖏 Quickly Set	VLAN Settings		1			
 PORT VLAN 		/LAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
Fault/Safety		1 Ne	ew VLAN			× 📝
PoE	O New VLAN O Del	oto 1/1-11	VLAN ID(1~4094): 2	¬.		ext Lasti / 1 Page
► STP	Trupk Settings		VLAN Name(1-31): VLAN0002			
DHCP RELAY	Trunk setungs		Select the ports to modify the			
DHCPserver		Port Na	VLAN:			it / Delete
TACACS+	🔘 New Trunk Port 🧲	Delete Tru	1 3 5 7 9			ext Last1 / 1 Page
RADIUS						
AAA			2 4 6 8 10			
▶ QOS		5	Optional 📰 Fixed port 🚍 Selected 51 Aggregation	Trunk		
Addr Table			Tip : Click and drag cursor over ports to select multiple port	s Select all Select all others Cancel		
► SNMP						
EACP SYSTEM						-
* aratem		4		m		<u>}</u>
		(Save			
				Next Next		

	Y Cur	rent username: adm	in			Exit Language
🛃 Home	VLAN setting	Other settings				
🆏 Quickly Set	VLAN Settings					
PORT VIAN		VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
Fault/Safety		1	VLAN0001	192.168.0.1/24	1-10	1
► PoE		2	VLAN0002		8	2 ×
 STP DHCP RELAY 	New VLAN	Delete VLAN			First Back	[1] Next Lasti /1 Page
DHCPserver	Trunk Settings					
TACACS+		Port Name	Edit Trunk port			×
RADIUS	New Trunk Port	Delete Trunk Port	configure:			A / 1 Page
▶ QOS			1 3 5 7 9			
Addr Table						
SNMP						
LACP			Optional 📰 Fixed port 💼 Selected 🚹 Ag	gregation 🛄 Trunk		
SYSTEM			Tip : Click and drag cursor over ports to select m	Itiple ports Select all Select all others Cancel		
			Native VLAN(1-4094): 2	0		
			Allowing VLAN(such as 3-5,8,10): 1			*
				III		•
			Save Exit			

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.

VLAN setting	Other settings						
Basic System Info	Basic System Information						
Management VLAN:	▼	Device Name: Default	Switch-123 *				
Management IP: 192 Subnet Mask: 255	2. 168. 2. 11	Gateway: DNS Server:	192. 168. 2. 22				
Save	Set Management VLAN						

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

Change Administrator Passwor	d			
Password type:	Encrypted passwi 🗸			
Old Password:				
New Password:				
Comfirm New Password:				
		G Back	Finish	
		Judak		

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**.

►	P	ORT
	•	Basic Config
	·	Port Aggregation
	·	Port Mirroring
	•	Port Limit
	•	Storm Control
	•	Port Isolation
		Port Information

4.2.1 Basic config

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

🛃 Home	Basic settings
S Quickly Set	
▶ PORT	
Basic Config	
 Port Aggregation 	
Port Mirroring	2 4 6 8 10
Port Limit	💭 Optional 🛄 Fixed port 💼 Selected 🕥 Aggregation 🛄 Trunk
Storm Control	Tip : Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
Port Isolation	Port Description(0-80 characters): Status: Enabled
Port Information	Port Speed: Auto
VLAN	Flow Control: On Cable Type Detection: Auto
Fault/Safety	Save

[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'.

	Y Current username; admin
🛃 Home	Basic settings
🖏 Quickly Set	
▶ PORT	
 Basic Config 	
Port Aggregation	
Port Mirroring	2 4 6 8 10
Port Limit	🗋 Optional 💼 Fixed port 💼 Selected î Aggregation 🛄 Trunk
Storm Control	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
Port Isolation	Port Description(0-80 characters): Status: Enabled
Port Information	Port Speed: 10M Duplex Mode: Duplex
► VLAN	Flow Control: On Cable Type Detection: Auto
Fault/Safety	Save

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:

SUNDRA'	Current username: admin		₽	Exit Language
🛃 Home	Port Aggregation			
Quickly Set PORT Basic Config	Aggregate Group Number(1-8): * Please select the port to join the Aggregate Group:			
Port Aggregation Port Mirroring Prot Limit				
Storm Control Port Isolation	Coptional E Fixed port Selected Aggregation Trunk Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel			
Port Information VLAN	Port Aggregation List			
 Fault/Safety PoE 	Aggregation Group Number	Group Memb	ers Eirat Back [4] h	Edit / Delete
STP			First Back [1] IN	Tipage

[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 .

	Current username: admin		Exit Language
🛃 Home	Port Aggregation		
Quickly Set PORT Basic Config Port Aggregation Port Mirroring Port Limit Storm Control Port Isolation Port Isolation	Aggregate Group Number(1-8): 1 * Please select the port to join the Aggregate Group: * 1 3 5 9 2 4 6 10 2 0 10 * Coptional Text the port so select fill Aggregation Cartuik Trunk Tp: Click and drag cursor over ports to select multiple ports Select all Select all others Save *		
VLAN	Port Aggregation List		
Fault/SafetyPoE	Aggregation Group Number	Group Members	Edit / Delete
STPDHCP RELAY			First Back [1] Next Last / 1 Page

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:

🛃 Home	Port Mirroring						
Quickly Set PORT	Mirror Group Number (1-4 Please choose the source p): * ort:(Selecting multiple source ports can affect the device performance)	e)				
Port Aggregation Port Mirroring							
Port Limit	2 4 6 8 10						
Storm Control	Optional 🚍 Fixed port 📻	Selected 517 Aggregation 57 Trunk					
Port Isolation	Tip: Click and drag cursor over	ports to select multiple ports Select all Select all others Cancel					
Port Information	Please choose the destination p	Please choose the destination port:(Can only choose one port)					
 VLAN Fault/Safety PoE 	$\begin{array}{cccccccccccccccccccccccccccccccccccc$						
	🖸 Optional 🚍 Fixed port 💼 Selected 抗 Aggregation 💭 Trunk						
 DHCP RELAT DHCPserver 	Save Port Mirror List						
TACACS+							
RADIUSAAA	Mirror Group	Source Port	Destination Port	Edit/Delete			
▶ QOS							

[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.

🛃 Home	Port Mirroring		
Quickly Set PORT Basic Config	Mirror group number(1-4 Please choose the source p): 1] * ort:(Allow multiple ports to select, Too much of the source port may a	ffect the device performance)
Port Aggregation Port Mirroring Port Limit	$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		
Storm Control Port Isolation	C Optional Not optional Please choose the destination p	Selected $\{\widehat{1}, Aggregation, \widehat{\dots}, Trunk, \widehat{E}\}$ ip source enable port ort: (Can only choose one port)	Tips : drag to select multiple ports Select-all Anti-select Car
 VLAN Fault/Safety PoE MSTP DHCP RELAY QOS Addr Table SNMP 	1 3 5 7 9 2 4 6 8 10 2 0ptional Not optional 5 Save edit Refresh Port mirror list	Selected 517 Aggregation 57 Trunk 527 ip source enable port	
► SYSTEM	Mirror group	source port	destination port

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:

🛃 Home	Port Speed Limit				
🖏 Quickly Set					
▶ PORT					
Basic Config					
 Port Aggregation 	88880				
Port Mirroring	2 4 6 8 10				
Port Limit	Optional 🚍 Fixed port 🚍 Sel	ected 🚹 Aggregation 🛄 Trunk			
Storm Control	Tip: Click and drag cursor over port	s to select multiple ports Select all Select all others Cancel			
Port Isolation	Input Speed Limit(multiple of 16):	* 0,16-1,000,000kb/s			
Port Information	Output Speed Limit(multiple of 16):	* 0,16-1,000,000kb/s			
VLAN	Save				
Fault/Safety	Port Speed Limit list				
PoE	Ports	Input Speed Limit	Output Spees Limit	Edit	
DHCP RELAY	1	1000Mb/s	1000Mb/s		
DHCPserver	2	1000Mb/s	1000Mb/s		
 RADIUS 	3	1000Mb/s	1000Mb/s		
	4	1000Mb/s	1000Mb/s		
QOS Addr Table	5	1000Mb/s	1000Mb/s		
► SNMP	6	1000Mb/s	1000Mb/s		
▶ LACP	7	1000Mb/s	1000Mb/s		
SYSTEM	8	1000Mb/s	1000Mb/s		
	9	1000Mb/s	1000Mb/s		
	10	1000Mb/s	1000Mb/s		
			First Back [1] Ne	xt Last1 / 1 Page	

[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.

🛃 Home	Port Speed Limit				
nuickly Set					
PORT					
Basic Config					
Port Aggregation	2 4 6 8 10				
Port Mirroring	🖸 Optional 🚍 Fixed port 💼 Sel	ected 1 Aggregation			
Port Limit	Tip: Click and drag cursor over port	s to select multiple ports Select all Select all others Cancel			
Storm Control	Input Speed Limit(multiple of 16):	6400 * 0,16-1,000,000Kb/s			
Port Isolation	Output Speed Limit(multiple of 16):	3200 * 0,16-1,000,000Kb/s			
Port Information	Save				
VLAN	Port Speed Limit list				
 Fault/Safety D=E 	Ports	Input Speed Limit	Output Spees Limit	Edit	
 STP 	1	1000Mb/s	1000Mb/s		
DHCP RELAY	2	1000Mb/s	1000Mb/s		
DHCPserver	3	1000Mb/s	1000Mb/s		
TACACS+		100000			
RADIUS	4	1000Mb/s	1000Mb/s	2	
AAA	5	6.4Mb/s	3.2Mb/s	1	
• 005					

4.2.5 Storm control

In the navigation bar to select "**PORT>Storm Control**", to port storm control config, the following ficture:

🛃 Home	Broadcast Control	
🌄 Quickly Set		
▶ PORT		
Basic Config		
Port Aggregation		
Port Mirroring	2 4 6 8 10	
Port Limit	💭 Optional 💼 Fixed port 🚍 Selected 🚮 Aggregation 🛄 Trunk	
Storm Control	Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel	
Port Isolation	Broadcast Limit: * 0-262143(pps)	
Port Information	Multicast Limit: * 0-262143(pps) Multicast type package: Unknow	in-only
VLAN	Unicast Limit: * 0-262143(pps) Unicast type package: Unknow	n-only
Fault/Safety	Save	

[Parameter Description]

Parameter	Description
Broadcast	Storm suppression value of the broadcast packets
suppression value	
Multicast suppression	Storm suppression value of the multipast peakets
value	Som suppression value of the municast packets
Unicast suppression	Storm suppression value of the unicast packate
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.

Broadcast Control
1 3 5 7, 9
Contional Prived out Steeded St Augregation Strunk
Tip: Click and drag cursor over ports to select multiple ports Select all Select all others Cancel
Broadcast Limit: 5000 * 0-262143pp/s
Multicast Limit: 5000 * 0-262143pp/s Multicast type package: Unknown-only
Unicast Limit: 5000 * 0-262143pp/s Unicast type package: Unknown-only
Save

4.2.6 Port isolation

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

📕 Home	Port Isolation						
🔜 Quickly Set	Please select two or more ports to						
PORT	configure:						
Basic Config	1 3 5 7 9						
Port Aggregation							
Port Mirroring							
Port Limit	🖓 Ontinnal 💭 Fixed not 💬 Selected 🞲 Angrenation 🖓 Truck						
Storm Control	Tin- Click and drag cursor over ports to select multiple por	ts Select all Select all others. Cancel					
Port Isolation							
Port Information	Save						
VLAN	Port Isolation List						
Fault/Safety	Source Port	Isolate Port	Delete				
PoE			First Back [1] Next Last 1 / 1 Page				
▶ STP							

[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.

🛃 Home	Port Isolation
 Quickly Set PORT 	Please select two or more ports to configure:
 Basic Config Port Aggregation 	
Port Mirroring Port Limit	
Storm Control	Coptional Fixed port Selected Aggregation Trunk Tip: Click and drag cursor over ports to select multiple ports Select all others Cancel
Port Isolation Port Information	Save

Port isolation list					
Source port	Isolate port	Operation			
3	456	×			
4	356	×			
5	346	×			
6	3 4 5	×			
	first page prev page [1] next page	e last page <mark>1 / 1page</mark>			

4.2.7 Port information

In the navigation bar to select "PORT>Port information", the following picture:

🛃 Home	Port informat	tion						
SQUICKIY Set	Keyword Input por	rt number or port descriptio	arch 🗷 Refr	resh				
 PORT Basic Config 	Port	Description	Input Flow(Bps)	Output Flow(Bps)	Port Status	Port Connection	VLAN	Trunk Port
Port Aggregation	Gi 0/1		0.00K	0.00K	ON	Nisconnecte d	1	No
Port Mirroring	Gi 0/2		23.20M	40.03M	ON	Connected	1	No
Storm Control	Gi 0/3		0.00K	0.00K	ON	Nisconnecte d	1	No
Port Isolation	Gi 0/4		0.00K	0.00K	ON	Nisconnecte d	1	No
 VLAN 	Gi 0/5		0.00K	0.00K	ON	Disconnecte d	1	No
 Fault/Safety PoE 	Gi 0/6		0.00K	0.00K	ON	💛 Disconnecte d	1	No
▶ STP	Gi 0/7		829.09K	271.39K	ON	💡 Connected	1	No
 DHCP RELAY DHCPserver 	Gi 0/8		0.00K	0.00K	ON	Nisconnecte d	1	No
TACACS+	Gi 0/9		0.00K	0.00K	ON	Disconnecte d	1	No
RADIUSAAA	Gi 0/10		0.00K	0.00K	ON	d	1	No
QOSAddr Table						First B	ack [1] Next Last	1 / 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 informa	tion						
Keyword	Search	Refres	h				
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 B	ack [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:

19 ■Configuration

VLAN setting		Trunk-port setting		Hybrid-port setting		
VLAN list						
		VLAN ID		VLAN name		
		1		VLAN0001		
📀 New VI	New VLAN					

4.3.1 VLAN config

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

🗮 Home	VLAN Settings Trunk Port Settings Hybrid Port Settings								
🖏 Quickly Set	VLAN IDs								
PORT		VLAN ID VLAN Name VLAN IP Port Edit / Delete							
VLAN			16 410004	100 160 0 1/04	1.10				
Vlan Config		1	VEANOUT	192.100.0.1/24	1-10				
Fault/Safety	New VLAN O Delete VLAN First Back [1] Next Last /1 Page								
PoE									
► STP									

[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.

VLAN setting	Trunk	-port setting Hybrid-port setting
VLAN list		New VLAN
New VLAN ©	VLAN 1 delete selec	VLAN ID(1~4094): 2 * VLAN name (1-32 character): VLAN0002 Choose to join the VLAN port: 1 3 5 7 9 1 3 5 7 9 2 4 6 8 10 Coptional Protoptional Selected (1) Aggregation ()1
		save quit

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:

VLAN Se	VLAN Settings Trunk Port Settings Hybrid Port Settings							
Trunk port	Trunk port list							
	Port	Port description Native VLAN Allowing VLAN Operation						
S New Trunk port S Delete selected Trunk port								

[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

21 ■Configuration

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 I	Ds						
	VLAN ID	VLAN ID VLAN Name VLAN IP		Port	Edit / Delete		
	1	VLAN0001	192.168.0.1/24		1-7,9-10		
	2	VLAN0002			8		
O New VLAN O Delete VLAN First Back [1] Next Last // / 1 Page							
VLA	N Settings Trunk	Port Settings Hybrid Port S	Settings				
Trunk	port list						
	Port	Port description	Native VLAN	AI	llowing VLAN	Operation	
O Nev	v Trunk port 🥥 Delete sele	cted Trunk port			First Back [1]	lext Last ¹ / 1 Page	
New Trunk port First Back [1] Next Last ¹ // Page New Trunk port * 1 3 5 2 4 6 10 2 4 6 10 2 0 Selected 1 Aggregation Trunk # Tp: Click and drag cursor over ports to select multiple ports Select all others Cancel Native Vian (1-4094) * * 58,10) :-2 * * * *							

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	VLAN Settings Trunk Port Settings Hybrid Port Settings							
Hybrid P	Hybrid Port List							
	Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete		
📀 New	S New Hybrid Port Selected Hybrid Port First Back [1] Next Last / / 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 I	Ds				
	VLAN ID	VLAN Name	VLAN IP	Port	Edit / Delete
	1	VLAN0001	192.168.0.1/24	1-10	
	10	VLAN0010			D 🔀
	20	VLAN0020			2 🗙

VLAN Settings	Trunk Port Sett	ings Hybrid Port	Settings		
Hybrid Port List					
Port	Port Name	Native VLAN	Added VLAN TAG	Removed VLAN TAG	Edit / Delete
New Hybrid Por	Delete Selected Hybri	d Port		First Back [1] N	ext Last ¹ /1 Page
	A New Hybrid Port	9 1 10 10 10 10 10 10 10 10 10	Aggregation [] Trunk nultiple ports Select all Select all other	ers Cancel	E
VLAN Settings Hybrid Port List	Trunk Port Sett	ings Hybrid Port	Settings		

 2
 20
 1
 10.20
 ≥ ×

 Image: Selected Hybrid Port
 First Back[1] Next Last¹
 /1 Page

 This system e0/1 and the receive system e0/2 PC can be exchanged, but when each data

Native VLAN

10

Added VLAN TAG

Removed VLAN TAG

10,20

Edit / Delete

📎 🗙

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

Port

Port Name

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

►	Fault/Safety						
	•	Anti Attack					
	•	Channel Detection					
	•	ACL					
	•	802.1x					

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.

DHCP configuration				
DHCP Trusted Port DHCP Restricted Ports	MAC Verification Option82	Binding Table	Other Configuration	
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 trus	sted ports:					
$\begin{bmatrix} 1 & 3 & 5 & 7 & 9 \\ \hline 1 & 2 & 2 & 2 & 2 \\ \hline 2 & 2 & 2 & 2 & 2 \\ \hline 2 & 4 & 6 & 8 & 11 \end{bmatrix}$]					
Optional 🚍 Fixed	port 🚍 Selected 🚹 Aggrega	ation 🛄 Trunk				
Tip: Click and drag cu	rsor over ports to select multiple	ports				
Save						
DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82	Binding Table	Other Configuration	
DHCP Rest	ricted Ports:					
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$						
C Optional E Fixed	port <u> </u>	ation 🛄 Trunk				
Tip: Click and drag cu	rsor 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 MAC A	Enable: ddress: F0:DE:F1:12:98:D2	*				
DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82	Binding Table	Other Configuration	
Dhcp Snoopi	ing Vlan:	×				
Server IP A	Address: 192, 168, 0, 1	*				

5. Set option82 information.

DHCP Trusted Port	DHCP Restricted Ports	MAC Verification	Option82	Binding Table	Other Configuration	
Option82 Enable:						
Circuit Control	Circuit Control Remote Agent IP Address					
Circuit Name: VLAN ID:	123					

DHCP Trusted Port	DHCP Restricted Ports MAC Verification Option82 Binding Table Other Configuration						
Option Client Option	Option82 Enable:						
Circuit Control	Remote Agent IP Address						
Remote Name:	wety						
VLAN ID:	1*						

DHCP Trusted Port	DHCP Restricted Ports MAC Verification Option82 Binding Table Other Configuration						
Option Client Option	Option82 Enable:						
Circuit Control	Remote Agent IP Address						
IP Address:	192.168.0.3 *						
VLAN ID:	i •						
Save							

6. The port 7 for binding.

DHCP Trusted Port DHCP F	Restricted Ports MAC Verification Option82 Binding Table Other Configuration
MAC Address:	F0:DE:F1:12:98:D3 *
VLAN ID:	1 .
Port Number:	7
Save	

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

HCP	DOS	IP Source Guard	IP/Mac/Port
DoS Attack F	k Protection		
Open	\supset		

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:

🛃 Home	DHCP DOS IP Source Guard IP/Mac/Port
🌄 Quickly Set	IP source protection port enable configuration
 PORT VLAN 	Please select a source port:
 Fault/Safety 	
Anti Attack Channel Detection	2 4 6 8 10
ACL	🖸 Optional 🚍 Fixed port 💼 Selected 🏦 Aggregation 🛄 Trunk 😰 IP Source Enable Port
• 802.1x	Tip: Click and drag cursor over ports to select multiple ports
PoE	Save

[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.

DHCP DOS IP Sour	ce Guard IP/Mac/Port						
IP source protection port enable configu	IP source protection port enable configuration						
Please select a source port:							
$ \begin{array}{c} 1 & 3 & 5 & 7 & 9 \\ \hline 1 & 2 & 5 & 5 \\ \hline 2 & 5 & 5 & 5 \\ 2 & 4 & 6 & 8 & 10 \end{array} $	$1 \xrightarrow{2}_{2} \xrightarrow{5}_{4} \xrightarrow{7}_{9} \xrightarrow{9}_{1}$						
Coptional Fixed port Selected	11 Aggregation <u>L.</u> Trunk <u>LE</u> IP Source Enable Port						
Tip: Click and drag cursor over ports to s	elect multiple pons						
Save							
DHCP DOS IP Sour	ce Guard IP/Mac/Port						
IP source protection port enable configu	ration						
Please select a source port:							
1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2							
Tin: Click and drag cursor over ports to	VLAN ID: 1						
Save	Source IP Address: 192, 168, 0, 30						
	3001Ce mile Audress 00.01.10.09.33.31						
Index Source Protection List							
	 Cobaoura Metrica horr Selected 71 (Addredation 2-4 Linux 2E (In Source Fusiole Fort 						
	Save Exit						

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 acheive the function of a key binding, the following picture:

🛃 Home	DHCP	OOS IP Source Guard IP/Mac/Port			
n Quickly Set	Test List				
PORT	Binding Enable 🔲				
VLAN		MAC Address	IP Address	Port Number	
Fault/Safety					
Anti Attack			Fi	st Back [1] Next Last1 /1 Page	
Channel Detection	Scanning Binding				
ACL					
• 802.1x					
▶ PoE	Application List				
STP					

[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.

DHCP	DOS	IP Source Guard	IP/Mac/Port			
Test List						
Binding Enable						
		MAC Address		IP Address	Port Number	
				Fir	st Back [1] Next Last1 /1 Page	
Scanning	Binding					
DHCP	DOS	IP Source Guard	IP/Mac/Port			
Test List						
Binding Enable	\checkmark					
		MAC Address		IP Address	Port Number	
		F0:1B:6C:5C:C9:72		192.168.55.100	7	
		00:E0:53:08:B2:32		192.168.0.64	4	
		00:E0:53:08:B2:32		192.168.1.100	4	
		34:02:9B:00:0D:56		192.168.1.7	7	
				Fi	rst Back [1] Next Last 1 / 1 Page	
Scanning (Binding					
	\smile					
Application L	ist					
		MAC Address		IP Address	Port Number	
		00:E0:53:08:B2:32		192.168.1.100	4	
Delete				Fir	st Back [1] Next Last1 /1 Page	

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 :

🗮 Home	Ping Tracert Cable Test	
Quickly Set PORT VLAN	Destination IP Address: * Timeout in Seconds (1-10): 2	
Fault/Safety Anti Attack	Ping Count (1.100): 5 Start	
Channel Detection ACL 802.1x	Result	
PoESTP		
DHCP RELAYDHCPserver	-	

[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	
of bytes from 192, 168.0.1.1cmp_seq=0.ttm=4.ttm=e.0.ms 64 bytes from 192,168.0.1.1cmp_seq=1.ttm=4.ttm=e.0.ms	
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.0 ms	
64 bytes from 192.188.0.1:cmp_seq=3 tit=64 time=0.0 ms 64 bytes from 192.188.0.1:cmp_seq=4 tit=64 time=0 cms	E
practis tationmaka, practis forma, or packet ross round-trip miniarg/max = 0.00,000 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	
	Ψ.

[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	*
	v

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:

Ping Tracert Cable Test	
Please select port to configure:	
COptional EFixed port Selected Aggregation CTrunk	
Start	

【Configuration example】

Ping Tracert Cable Test	
Please select port to configure:	
🖸 Optional 🚍 Fixed port 🚍 Selected 🚹 Aggregation 💭 Trunk	
Start	
Result	
Port	Status
4	Normal
	First Back [1] Next Last /1 Page

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.

🛃 Home	Timetable	L Apply ACL			
🌄 Quickly Set	Timetable Name:				
▶ PORT	Day Selection: 🗌 Monday 🗐 Tuesday 🗐 Wednesday 🗐 Thursday 🗐 Friday 🗐 Saturday 💭 Sunday				
VLAN	Time	Time Interval:			
Fault/Safety	Save				
Anti Attack Channel Detection	Time Name	Day	Time Interval	Edit / Delete	
• ACL	test	Monday Tuesday Wednesday Thursday Friday	08:00-18:00	2 🗙	
• 802.1x			First Back [1]	lext Last1 / 1 Page	
▶ PoE					
▶ STP					

[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.

Time]										
	table	ACL	Арріу	ACL	_						
	Ti	metable Name	test	u 🕅 Tueed	au 🕅 Wedneedeu 🕅 Thurse	day 🕅 Erida	Coturday Cunday				
		Time Interva	8:00	ay 🖭 Tuesu:	ay 🖭 wednesday 🖭 murst	Jay 🖭 Filoay] 🔔	Saturday El Sunday				
		rime interva	•			T					
Save											
Time	table	ACI	Apply								
Create /	ACL		(idd)								
Driority	AN	Derminaion	Indox	Drotocol	Source ID / Mack	Source	Destination ID / Mask	Destination	Timetable	Statuo	Deloto
Phoney	number	Permission	inuex	PIOLOCOI	Source IP / Mask	Port	Destination IP / Mask	Port	Name	Status	Delete
		The	new ACL	access r	ule						× /1 Page
				AC	L Number: 100	*	Protoco	Type: TCP		-	
				P	ermission: Permit	•	ACL	Name: test			
				4.00	v ere ID Address:	A					
				All		- B					
				An	y source port. 🛛 🕅						
				An	y dst IP Address: 🛛 🛛 🌘	D					
				An	y dst Port: 🛛 🕅	Ð					
			Save)							
			Save)							
			Save)					-		
Priority	Acl number	Permission	Save	Protocol	Source IP / Mask	Source Port	Destination IP / Mask	Destination Port	Timetable Name	Status	Delete
Priority 1	Acl number 100	Permission	Save Index 10	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test	Status inactive	Delete
Priority 1	Acl number 100	Permission	Save Index 10	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Last1	Delete X /1Page
Priority 1	Acl number 100	Permission	Save Index 10	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Lasi 1	Delete X /1 Page
Priority 1	Aci number 100	Permission permit	Save Index 10	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Las 1	Delete X /1 Page
Priority 1	Acl number 100 table	Permission permit	Save Index 10 Apply	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Las 1	Delete X /1 Page
Priority 1	Acl number 100	Permission permit ACL	Save Index 10 Apply	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Lasi 1	Delete X /1 Page
Priority 1	Acl number 100	Permission permit ACL	Save Index 10 Apply	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Last	Delete X /1Page
Priority 1	Acl number 100	Permission permit ACL	Save Index 10 Apply	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Las [1	Delete X /1 Page
Priority 1	Acl number 100	Permission permit ACL	Save Index 10 Apply	Protocol tcp	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Be	Status inactive ck [1] Next Last1	Delete X /1 Page
Priority 1	Acl number 100 table	Permission permit ACL	Save Index 10 Apply	Protocol tcp ACL	Source IP / Mask any/any	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Be	Status inactive ck [1] Next Last1	Delete X /1 Page
Priority 1 Time 2 Copti Tip: Cl	Acl number 100 table	Permission permit ACL	Index 10 Apply Selected 5 orts to selected	Protocol tcp ACL	Source IP / Mask any/any ionTrunk ports Select all Select all c	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Last1	Delete X /1 Page
Priority 1 Time 2 Copti Tip: C	Acl number 100 table	Permission permit ACL	Index 10 Apply Selected 5 orts to sele	Protocol tcp ACL	Source IP / Mask any/any ionTrunk ports Select all Select all C	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Last 1	Delete /1 Page
Priority 1 Time 2 2 4 Copti Tip: Cl	Acl number 100 table	Permission permit ACL	Save Index 10 Apply Selected ∑ orts to sele trs 100 m: Receiv	Protocol tcp ACL	Source IP / Mask any/any ion Trunk ports Select all Select all o	Source Port any	Destination IP / Mask any/any	Destination Port any	Timetable Name test First Ba	Status inactive ck [1] Next Las(1	Delete X /1Page

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

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	802.1x config
🖏 Quickly Set	Enable 802.1x: Disable
PORT	Re-auth enable: 🗹
VLAN	Re-auth cycles: 3600 (60-7200)s
Fault/Safety	Use Pae group address: 🗹
Anti Attack	Maximum number of auth
Channel Detection	Auth fail vlan attempts: 3
ACL	Apply
• 802.1x	
PoE	Select a port:
▶ STP	
DHCP RELAY	

31 ■Configuration

[Parameter Description]

Parameter	Description
Re-auth cycles	Set the Re-auth cycles to time
Maximum number of	Select the authentication value of the Maximum number
auth retransmission	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 ti meback to 3600 S, Auth the maximum number of retransmissions is 2, failed authentication VLAN number for 3 times.

802.1x config		
Enable 802.1x:	Enable 💌	
Re-auth enable:		
Re-auth cycles:	3600	(60-7200)s
Use Pae group address:	\checkmark	
Maximum number of auth retransmission:	2	
Auth fail vlan attempts:	3 💌	
Apply		1

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.

Select a port:	
1 3 5 7 9	
💭 Optional 🚍 Fixed port 🚍 Se	ected <u>[1]</u> Aggregation <u>[]</u> Trunk
Tip: Click and drag cursor over por	s to select multiple ports Select all Select all others Cancel
Port control method:	Auto 💌
Port auth method:	Mac Base 💌
Max user:	2 (0-255)
MAB auth	Multi-MAB
MAB auth cycles	256 (0-65535)s
GUEST VLAN:	1 (1-4094)
Auth failure VLAN:	2 (1-4094)
Apply	

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.

🛃 Home	(Management) Temperature Distribution
🖏 Quickly Set	POE Status Information
 PORT VLAN Fault/Safety PoE 	Working Status: Online Alarm Power: 128.0W Rated Total Power: 140.0W Voltage Level: 54.7V Power Output: 0.0W Voltage Level: 54.7V
• PoE Config	POE Alarm Configuration
PoE Port Config PoE Delay Config	Alarm Notification:
▶ STP	Aldrill Noullicauvili. Claure Ubiavie
DHCP RELAY	Save
DHCPserver	
TACACS+	
RADIUS	
► AAA	
▶ QOS	

[parameter description]

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

[instruction]

Addr Table
SNMP
LACP
SYSTEM

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.

Management Temperature Distribution		
POE Status Information		
Working Status: Online	Alarm Power: 126.0W	
Rated Total Power: 140.0W	Voltage Level: 54.7V	
Power Output: 0.0W		
POE Alarm Configuration		
Alarm Notification:	1 20 W	
Alarm Notification: (Enable Disable)		
Save		

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.

Management Temperature Distribution						
Temperature Config	Temperature Config					
Chip Temperature List	Chip Temperature List					
Chip Number	Current Temperature	Alarm Threshold	Edit			
1	55°C	110℃	1			
		first page prev page [1] next pag	e last page 1 / 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.

Management Temperate	ure Distribution		
Temperature Config			
Temperature Alarm	0 90°C		
Chip Temperature List			
Chip Number	Current Temperature	Alarm Threshold	Edit
1	55%	2°00	
		first page prev page [1] next page	e last page1 / 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.

🛃 Home	POE Port List										
SQuickly Set	Port	Output Status	Status	Power Level	Current Level	Power MAX	PD Type	POE Mode	Priority	Mode Detection	Edit
 PORT VLAN 	1	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
Fault/Safety	2	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
▶ PoE	3	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
PoE Config PoE Port Config	4	Disabled	Disabled	-		32W	-	Enabled	Low	AT&AF	
PoE Delay Config	5	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
► STP	6	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
DHCP RELAY	7	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
 DRCPserver TACACS+ 	8	Disabled	Disabled	-	-	32W	-	Enabled	Low	AT&AF	
RADIUS	O Multi-Port E	Edit							First Ba	ack [1] Next Last1	/ 1 Page
 Addr Table 											
► SNMP											
 LACP SYSTEM 											

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

[parameter description]

[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.

POE Port Configuration	×	Mode Detection	Edit
Port ID: 8	- Â	AT&AF	1
POE Mode: Enabled Port Priority: High		AT&AF	1
Detection Mode: AF		AT&AF	1
Maximum Power (W): 23	=	AT&AF	1
		AT&AF	
		AT&AF	
🖸 Optional 💼 Fixed port 💼 Selected 🖽 Aggregation 🛄 Trunk		AT&AF	
Tin + Click and dran cursor over nots to select multiple nots. Select all Select all others. Cancel	Ψ 	[1] Next Last1	/1P
Save Exit			

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.

🛃 Home	PoE Restart/Delay						
uickly Set							
PORT							
VLAN							
Fault/Safety							
▶ PoE	2 4 6 8						
 PoE Config 	Optional 🚍 Fixed port 🚍 Sel	ected 1 Aggregation 1 Trunk					
PoE Port Config	Tip : Click and drag cursor over ports	s to select multiple ports					
PoE Delay Config	Current System Time: 2016-12-20 15	:54:53, Tuesday					
► STP	Restart Weeks Selection:	Monday 🗖 Tuesday 🗖 Wednesday 🗖 Thursday 🗐 Friday	🗖 Saturday 🔲 Sunday				
DHCP RELAY	Restart Time:						
DHCPserver	Port Delay Time:	Seconds(0-3600) *					
TACACS+	Save	Save					
RADIUS	PoE Delay List	PoE Delay List					
► QOS	Ports	Port Restart Time	Port Delay Time	Operation			
Addr Table	1	0	0s				
SNMP	2	0	0s				
 SYSTEM 	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					
1 3 5 7 2 4 6 8 1 0 Optional Tip Ked port Selected 1 1 1 1 <t< td=""></t<>					
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	6 0 0s				
7	7 0 0s				
8	0	0s			
		First Back [1] Ne	ext Last1 / 1 Page		

4.6 STP

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

۲	STP		
	•	MSTP Region	
	•	STP Bridge	

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.

🛃 Home	MSTP Configuration		
🌄 Quickly Set	Region Name:	D466BA0911DF (1 to 32 characters)	
▶ PORT	Revision Level:	0 (0 to 65535,default 0)	
VLAN	Save		
Fault/Safety			
PoE	Instance Mapping		
► STP	Instance ID:	1	
• MSTP Region	VLAN ID:	* For example: 1,3,5,7-10	
 STP Bridge 	Save Delete		
DHCP RELAY	Mapping List		
 DHCPserver TACACS: 	Instance ID	Mapping VI AN	Edit
TACAUS+		mapping view	cur
 AAA 	0	1-4094	Ø
> QOS		First Back [1] Net	kt Last1 /1 Page

[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.

MSTP Configuration	1	
F	Region Name :	DEADBEEEF0102 * (1 to 32 characters)
R	evision Level:	123 * (0 to 65535,default 0)
Save		
Instance Mapping		
	Instance ID:	4
	VLAN ID:	2 * For example: 1,3,5,7-10
Save Delete		

4.6.2 STP Bridge

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

	Current username: admin 🕟 Exit Languag	je
SUNDRAY Home Coulds set PORT VLAN Fault/Safety PoE STP INSTP Region	Current username: admin Ent Latitude STP Bridge Config Instance Priority: Instance ID: 0 Priority: 32768 Enable: ON ® OFF Mode: STP ® RSTP ® MSTP Helio Time: 2 * (1-10s) MAX Age: 10 * (6-40s) Forward Delay: 10 * (4-30s) MAX Hops: 10 * (1-40)	
 DHCP RELAY DHCPserver TACACS+ RADIUS AAA QOS Addr Table SNMP LACP SYSTEM 	STP port config Instance: 0 Port Fast: 0 N 0 OFF Path Cost: exte * (0+240,step 16) Port Fast: 0 N 0 OFF Path Cost: exte * (auto or 1-20000000) Auto Edge: 0 N 0 OFF Point to Point: 0 N 0 OFF BPDU Guard: 0 N 0 OFF BPDU Filter: 0 N 0 OFF Root Guard: 0 N 0 OFF BPDU Filter: 0 N 0 OFF T Guardt: 0 N 0 OFF T Gu	

[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			
Dridge priority	Priority setting bridge example, the default			
впаде рнопку	instance bridge priority for 32768			
mode	The model is divided into: the STP, RSTP, MSTP			
Hello-time	Switches sends bpdus in packet interval			
Max aga	Ports are not yet received a message in the time,			
wax-age	will initiate topology changes			
Forward-delay	The state of the port switch time			
Port priority	Set port instance priority, defaults to 128, you must			
Pon-phonty	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) (hello_time+1)\times2<=max_age<=(f_delay-1)\times2, 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.

Instance:	1	J	Priority:	128	*	(0-240,step 16)				
Port Fast:	O ON	OFF	Path Cost:	auto	*	(auto or 1-20000	0000)			
Auto Edge:	O ON	OFF	Point to Poin	t: O ON O OFF	۲	Auto				
BPDU Guard:	O ON	OFF	Compatible:	ON OFF						
BPDU Filter:	ON	OFF	Root Guard:	🖲 Root 🔘 None						
TC Guard	ON ON ON ON	OFF	TC Ignore -	ON OFF						
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	ort <u> S</u> el	ected 1 Ag	igregation 💭 Trunk							
ve Show Current F	Port									
ve Show Current F	Port	S	[P Port Information [Gi0/4]						×	
Ve Show Current F	Port	S P P	TP Port Information [Gi0/4] (Gi0/4) ortAdmmPortFast disable ortOperPortFast (disable						×	
ve Show Current F port config Instance : 0 Port Fast : 0	Port	DFF P	TP Port Information [Gi0/4] (Gi0/4) ortAdmmPortFast disable ortAdmAut6dge: disable ortAdmAut6dge: disable						×	
port config	Port	DFF P	(30/4) (30/4) ortAdminPortFast disable ortAdminLantEdge: disable ortAdminLantEdge: disable ortAdminLantType: auto						×	
Port config Instance : 0 Port Fast : Auto Edge : BPDU Guard : BPDU Guard : 0 BPDU Filter : 0	Port	DFF P DFF P DFF P	IP Port Information [Gi0/4] Gi0/4]					E	×	
we Show Current F port config Instance : 0 Port Fast : Auto Edge : BPDU Guard : BPDU Filter : TC Guard : BPDU Filter : BPDU Filter : TC Guard : BPDU Filter	Port ON	DFF P DFF P DFF P DFF P DFF P DFF P	TP Port Information [Gi0/4] [Gi0/4] OrtAdminPortFast disable ortAdminAut6dge: disable ortAdminAut6dge: disable ortAdminLinType: auto ortAdminLinType: auto ortAdminLinType: auto ortBPUUGuer: disable ortBPUUGuer: disable ortBPUUGuer: disable ortBPUUGuer: disable					- III	×	

 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.

🛃 Home	DHCP Relay Enable
🌉 Quickly Set	DHCP Relay Enable:
▶ PORT	DHCP Option Trust Field Enable:
VLAN	
Fault/Safety	
PoE	
STP	
DHCP RELAY	
Dhcp Relay	
option82	
DHCPserver	
TACACS+	
RADIUS	
AAA	
▶ QOS	
Addr Table	
SNMP	
▶ LACP	
SYSTEM	

[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.

DHCP Relay Enal	ble						
D	DHCP Relay Enable:						
DHCP Option	Frust Field Enable: 📝						
DHCP Relay Con	lig						
Save	DHCP Server (9: 192. 168. 0. 22 *						
Number	Number IP Address Status Edit						
1 0.0.0.0 invalid 🗶							
		First Back [1]	vext Last / 1 Page				

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:

🛃 Home	Option82 Config			
🌄 Quickly Set	Circuit Control Proxy Remote IP Address			
▶ PORT				
VLAN	Circuit Control: *			
Fault/Safety	VLAN ID: *			
▶ PoE	Save			
► STP				
DHCP RELAY	Number Circuit Name	Circuit ID	VLAN ID	Edit / Delete
Dhcp Relay			First Back 🚹 N	lext Last ¹ / 1 Page
option82				
DHCPserver				

[Parameter Description]
Parameter	Description
VLAN id	the DHCP request message in the VLAN, value range is 1 \sim
	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

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 Cont VLAN I Save	trot/123 * 1 : *			
Number	Circuit Name	Circuit ID	VLAN ID	Edit / Delete
			First Back [1] N	ext Last / 1 Page
Ontion®2 Config				
Circuit Control	Proxy Remote IP Address			
Proxy Remo VLAN IE Save	ster swet			
Number	Proxy Remote Name	Proxy Remote ID	VLAN ID	Edit / Delete
			First Back [1] N	lext Last / 1 Page
Circuit Control	Proxy Remote IP Address			
IP Addre VLAN II Save	ss 192.168.0.35			
Number	IP Ad	dress	VLAN ID	Edit / Delete
			First Back [1] N	ext Last / 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.



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.

Enable Config	Pool Config	Option Config	Bind Config	Gateway Config	DNS Config	
DHCP Enable						
Open						

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 Gat	teway Config DN	S Config		
Pool ID	* (1-65535)					
Domain						
Network IP	*					
Network Mask	*					
Start IP						
End IP						
Lease Time	Days	Hours	Minutes			
Set Up						
Pool Table						
Pool ID Domain	Network IP	Network Mask	Lease Time	Start IP	End IP	Delete
				First Back	[1] Next Last ¹	/ 1 Page

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.

Enal	ole Config	Pool Co	nfig Option Confi	Bind Config	Gateway Confi	g DNS Config		
		Pool ID 1	* (1-65	535)				
		Domain Pub	lic					
		Network IP 192	. 168. 1. 6 *					
	Ne	twork Mask 255	. 255. 255. 0 *					
		Start IP 192.	. 168. 1. 100					
		End IP 192	. 168. 1. 200					
		Lease Time 1	Days 23	Hours	59 1	Minutes		
Set Up								
Pool Ta	able							
	Pool ID	Domain	Network IP	Network Mask	Lease Time	Start IP	End IP	Delete
	1	Public	192.168.1.0	255.255.255.0	172740secs	192.168.1.100	192.168.1.200	×
						Fir	st Back [1] Next Last	/ 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 Confi	g Gateway Config	DNS Config	
	Pool ID 1 Code *	(1-255)			
Code Set Up	Value Type hex Kode Value Kode Value				
Option List					
	Pool ID	Code	Code Value	e	Delete
				First E	Back [1] Next Last / 1 Page

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:Seting 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 Conf	fig DNS Config	
	Pool ID 1 👻			
	Code 2 * (1-255)			
Code Va	alue Type ip 🔻			
Co	ode Value 192. 168. 1. 2 *			
Set Up				
Option List				
	Pool ID	Code	Code Value	Delete
	1	option-2	192.168.1.2	×
			Firs	t Back [1] Next Last / 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	
Bind List				
IP Adress	Hardware Type	Hardware Adress	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.

Enable Config	Pool Config Option Config Bind Config Gateway Config DNS Config
	Pool ID 1
Gat	*
Gat	teway 2
Gat	teway 3
Gat	teway 4
Gat	teway 5
Gat	teway 6
Gat	teway 7
Gat	teway 8
Set Up	

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.

Enable Config	Pool Config Option Config	Bind Config Gateway Config DNS Config	
	Pool ID 1		
G	ateway 1 192. 168. 1. 55 *		
G	ateway 2		
G	ateway 3		
G	ateway 4		
G	ateway 5		
G	ateway 6		
G	ateway 7		
G	ateway 8		
Set Up			
Gateway List			
	Pool ID	Gateway	Delete
	1	192.168.1.55	×
		First Back [1]	Next Last / 1 Page

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.

Enable Config Pool Config Option Co	nfig Bind Config	Gateway Config DNS Cor	fig
Pool ID 1			
DNS Server 1 *			
DNS Server 2			
DNS Server 3			
DNS Server 4			
DNS Server 5			
DNS Server 6			
DNS Server 7			
DNS Server 8			
Set Up			

[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
	1		47.54.89.210		×
				First Back [1]	lext 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	TACACS+ Config							
🖏 Quickly Set	Global Config							
 PORT VLAN Fault/Safety POE STP DUCD DELAY 	Server 1 Server Retr Conversation/C	Imeout 5 y Count 3 onnect: O Only O Multi Key:						
 DHCP RELAT DHCPserver 	Port Config							
 TACACS+ TACACS+ Config RADIUS AAA QOS Addr Table 	Ing Server IP:							
▶ SNMP	TACACS+ Server List	TACACS+ Server List						
LACPSYSTEM	Servial Number	Server IP	Port	Server Timeout Value	Delete			
				First Back [1]	Vext 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	Global Config							
Server T	Timeout: 5 y Count: 3							
Conversation/C	Conversation/Connect O Only Multi Key: 2844sa							
Port Config								
Server IP: 192.188.0.98 Authentication Port Server Timeout Key: 2644sa								
TACACS+ Server List								
Servial Number	Server IP	Port	Server Timeout Value	Delete				
1	192.168.0.88	49	5	×				
First Back [1] Next Last / 1 Page								

4.10 RADIUS

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



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.

47 ■Configuration

[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.

adius General Config R	adius Server Config		
OIUS Global Config Information			
Server Repeat Number:3			
Server Timeout:2	RADIUS Global Config		
Server Quiet Time:0	Server Repeat Number: 3	[1-100]	
ad criteria Retry Count®	Server Timeout: 2	[1-1000]	
Deed enterin Time ente	Server Quiet Time: 5	[1-1440]	
Dead-criteria Timeouco	Dead-criteria Retry Count: 3	[1-100]	
inge Config	Dead-criteria Timeout: 2	[1-120]	
	Save Cancel		

4.10.2 Radius Server Config

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

Radius General Config Radius Server Config							
Server List							
IP Address	Authentication Port	Key	Active Detection	Statistical Information	Edit / Delele		
Create A New Server First Back [1] Next Last / 1 Page							

[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.

Radius General Co	onfig Rad	lius Server Conf	ig				
Server List							
IP Address	Authent	ication Port	Key	Active Detection	Statistical Information	Edit	/ Delele
Create A New Server		Create A New S	erver		×	t Last ¹	/ 1 Page
		Se	rver Address:	192. 168. 0. 68			
		Authe	ntication Port:	1812 Defau	iit		
			Key:	radius 🗹 Defau	ult		
		Act	ive Detection: Test Name	V On			
			Idle Time	3			
		Save	Cancel			1	
		Cano	ouncer				

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.



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.

🛃 Home	Domain enable config							
🔜 Quickly Set	Status: O OFF							
PORT	Save							
VLAN								
Fault/Safety	ISP domain							
PoE	Domain na	me:	(1-30bytes)					
STP	Sta	Status: block -						
DHCP RELAY	Verify that the user is carrying	Verify that the user is carrying the						
DHCPserver	uomain na	domain name: without-outhain •						
TACACS+	Add							
RADIUS	ISP domain list							
AAA	Domain name	Status	Whether to carry domain name	Binding scheme	Operation			
Enable Config	default	active	without-domain					
Region Config	deladit	donvo	Warderdonian					
 Server Config 				First Back [1]	Vext Last / 1 Page			
AAA Authenticatio								
▶ QOS								
Addr Table								

Addr TableSNMP

▶ LACP

► SYSTEM

[Parameter Description]

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

[Instruction]

Setting the Option parameter to the IP address pool.

【Configuration example】

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

Domain enable config							
Status: ON OFF Save							
ISP domain							
Domain name test Status active Verify that the user is carrying the domain name: with-domain Add							
ISP domain list							
Domain name	Status		Whether to carry domain name	Binding scheme	Operation		
default	active		without-domain		×		
	First Back [1] Next Last / 1 Page						

4.11.3 Server Config

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

🛃 Home	Server-group config				
🖏 Quickly Set	Server name:		Select server: radius 👻		
PORT	Server IP addr:	Au	thentication port:	(0-65535)	
VLAN	Save				
Fault/Safety	Current as much list				
▶ PoE	Current server list				
▶ STP	Server name	Agreement	Server addr	Certification of port	Operation
DHCP RELAY				First Back [1]	Next Last / 1 Page
 DHCPserver TACACC: 					
PADILIS					
 ΛΑΔΙΟ΄ ΔΔΔ 					
Enable Config					
Region Config					
Server Config					
AAA Authenticatio					
▶ QOS					
Addr Table					
► SNMP					
LACP					
SYSTEM					

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

Server-group config		
Server name: aaa	Select server; tacacs+ 💌	
Server IP addr: 192. 168. 0. 66		
Save		

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	Login authentication Enable authentication Dot	1x authentication	
🌄 Quickly Set	AAA accounting configuration		
PORT	Choose a domain DODP		
VLAN	Choose a domain mono		
Fault/Safety	LOGIN Authentication Proj	ect name default	
PoE	First method: Local 👻		
STP	Second method:		
DHCP RELAY	Third method:		
DHCPserver	Fourth method		
TACACS+			
RADIUS	OBVE		
AAA	Login Authentication list		
 Enable Config 	project name	Method	Operation
 Region Config 		a . b	••
Server Config	default	(local)	*
AAA Authenticati			First Back [1] Next Last / / 1 Page
▶ QOS			
Addr Table			
SNMP			
▶ LACP			
SYSTEM			

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 Dot	1x authentication	
AAA accounting configuration		
Choose a domain none 👻		
COGIN Authentication Proje First method; Local Second method; None Third method; Group RADIUS Fouth method; Group TACAS+	ect name default	
Login Authentication list		
project name	Method	Operation
default	(local)	×
		First Back [1] Next Last / 1 Page

[Parameter Description]

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

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

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+.

Login authentication Dot1x authentication		
AAA accounting configuration		
Choose a domain none 👻		
COGN Authentication Proje First method: Local Second method: None Third method: Group RADIUS Fouth method: Group TACAS+	ect name defailt	
Login Authentication list		
Login Autrenucation list		0
project name	Wethod	Operation
default	(local)	×
		First Back [1] Next Last / / 1 Page

4.11.4.2 Enable Authentication

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

Login authentication Enable authentication	Dot1x authentication	
AAA Authentication config		
Select a domain name none 👻		
Enable Authentication First method: Second method: Third method: Fourth method: Srays	Policy name: default	
Enable Authentication list		
Policy name	Method	Operation
default	(local)	×
		First Back [1] Next Last 1 /1 Page

[Parameter Description]

Parameter	Description	
First method	Can choose the following kinds:	
First method	Local	

53 ■Configuration

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

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	1x authentication	
AAA authentication configuration		
Domain none 🔻		
Dot1x authentication projection	ct 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 Page

Parameter	Description	
First mathed	Can choose the following kinds:	
	Local	
	None	
T IISt Method	Group Radius	
	Group Tacacs+	
	Custom server group	
	Can choose the following kinds:	
	Local	
Second method	None	
Oecona metrioa	Group Radius	
	Group Tacacs+	
	Custom server group	
	Can choose the following kinds:	
	Local	
Third method	None	
	Group Radius	
	Group Tacacs+	
	Custom server group	
	Can choose the following kinds:	
Fouth method	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+.

Login authentication Er	nable authentication	Dot1x authentication		
AAA authentication configuration				
Domain test 👻				
Dot1x authentication	-	project name: default		
Second method: None	•			
Third method: Group RADIUS	•			
Fouth method: Group TACAS+	•			
Add				
dot1x authentication list				
Project name		Method		Operation
default		(local) (none) (group radius) (grou	p tacacs+)	×
			First Back [1]	Next Last 1 / 1 Page

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

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

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	
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.

🛃 Home	COS Queue Map DSCP COS Map Port COS Map										
🖏 Quickly Set	Mapping Queue Status Information										
▶ PORT											
VLAN	281A41M 0 1 5 2 4 2 0 1										
Fault/Safety	Queue ID 0 • 1 • 2 • 3 • 4 • 5 • 6 • 7 •										
PoE											
▶ STP	Save										
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 Que	COS Queue Map DSCP COS Map Port COS Map							
Mapping Qu	Ilapping Queue Status Information							
Server ID	0	1	2	3	4	5	6	7
Queue ID	0 🔻	1 🔻	2 👻	7 -	4 👻	5 👻	6 👻	7 👻
Save	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:

COS Queu	COS Queue Map DSCP COS Map Port COS Map															
Differential se	rvice cod	le point n	napping t	eam list												
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 🔻
Save																

[Parameter Description]

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

COS Queu	COS Queue Map DSCP COS Map Port COS Map															
Differential ser	rvice cod	e point n	napping t	eam list												
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 🔻
Save																

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 DS0	CP COS Map	Port COS Map						
Port CoS mappi	Port CoS mapping								
Port:	Port: 1 ·								
Serve	Server ID: 0 🗸								
Trust	cos	-							
Apply									
Control list									
Port				Serv	ver ID				Trust Mode
	0	1	2	3	4	5	6	7	
1	т								
2	т								
3	т								
4	т								
5	т								
6	т								
7	т								
8	т								
							First Back	[1] [2] Next Last	/ 2 Page

Parameter	Description
Port	Select the port number (1-10)
	Mapped to the service ID, and then according to the service ID
Service ID	into the queue
	Can choose the following kinds:
Mode	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 $\cos 4$, $\cos 5$, dscp6.

ſ	COS Queue Ma	DSCP COS Map Port COS Map	
	Port CoS mapping		
	Port: Server ID Trust Mode:	4 • • 4 • • • • • • • • • • • • • • • •	

COS Queue Ma	p DSCP COS Map	Port COS Map
Port CoS mapping		
Port:	5 🗸	
Server ID	5 🗸	
Trust		
Mode:	cos 👻	
Apply		и

CO	S Queue Ma	p	DSCP COS M	ар	Port COS Map				
Port	CoS mapping								
Apr	Port: Server ID Trust Mode:	6 c 6 dscp	•						

Control list	Control list								
Port		Server ID							
	0	0 1 2 3 4 5 6 7							
1	т								
2	т								
3	т								
4					Т				cos
5						T			cos
6							Т		dscp
7	т								
8	т								
							First Back	(1) [2] Next Last	/ 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	Address Table Conf	ig			
🌄 Quickly Set	MAC Management	MAC Learning and Aging MA	C Filter		
 Cultory set PORT VLAN Fault/Safety PoE STP DHCP RELAY DHCP RELAY DHCPserver TACACS+ RADIUS AAA QOS Add Table 	MAC Management Clear M. VLAN: MAC Ad Save	MAC Learning and Aging MA AC: Clear appoint MAC ▼ 1 Valid Range (dress :	Trunk 1 to 4094)		
Address Table	MAC Ad	dress :			
► SNMP	Curc				
▶ LACP	M	AC Address List: All			
SYSTEM	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 pag	je [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:

ess Table Config C Management Clear MAC: VLAN: MAC Addre ave	MAC Learning and Aging MA Clear appoint MAC 1 Valid Range (555 :	IC Filter									
C Management Clear MAC: VLAN: MAC Addre	MAC Learning and Aging MA Clear appoint MAC I Valid Range (ss :	1 to 4094)									
Clear MAC: VLAN: MAC Addre	Clear appoint MAC I Valid Range (ss :	1 to 4094)									
Clear MAC: VLAN: MAC Addre	Clear appoint MAC 👻 1 Valid Range (ss :	1 to 4094)									
VLAN: MAC Addre	1 Valid Range (1 to 4094)									
MAC Addre	SS :										
ave											
			Save								
		DHCP RELAY									
102Ferver 1 3 5 7 9 102CACS+ 10 10 10 10 2 4 6 10 2 4 6 10 1000 10 10 10 1000 10 10 10											
							MAC Addre	valu Range (104084)		
							ave				
							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 pa	ge [1] nextpage lastpage 1 / 1 page							
2	3 5 7 4 6 8 0ptional Fixe VLAN: MAC Addre MAC Number 1 2	3 5 7 9 4 6 8 10 Optional Fixed port Selected £1 Apgregation £1 VLAN: 1 Valid Range (MAC Address Elst: All MAC Address List: All Number MAC Address 1 1 D4:58.BA.09.11.DF 2 2 00:E0:53.08:B2:32	3 5 7 9 4 6 8 10 Optional Fixed port Selected 1 Apgregation MAC Address Valid Range (1 to 4094) MAC Address Velanit Number MAC Address VLAN ID 1 D4:68 BA:09:11 DF 1 2 00:E0 53 08:B2:32 1	3 5 7 9 4 6 8 10 Optional Fixed port Selected Aggregation VLAN: 1 Valid Range (1 to 4094) MAC Address :							

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

Address Table Config								
MAC Management MAC Lea	arning and Aging MAC Filter							
88880								
2 4 6 8 10								
Coptional E Fixed port Se	Coptional Trixed port Selected 51, Aggregation 5(Trunk							
ILP: Click and drag cursor over ports to select multiple ports MAC Learning Limit: 8191 (Learning Range 0-8191)								
Save	Save							
MAC Address Aging Time	300 (0 indicates no aging 10-1000000 second)							
Save	(o indicates no aging, to-tooodo second)							
Number	Port	MAC Learning Limit Number						
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	010/0	0101						
	Glob	0101						

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.

Address Table Config
MAC Management MAC Learning and Aging MAC Filter
C Optional E Fixed port E Selected Aggregation C Trunk
Tip: Click and drag cursor over ports to select multiple ports
MAC Learning Limit 2000 (Learning Range 0-8191)

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

MAC Address Aging Time: 120 (0 indicates no aging,10-1000000 second)
Save

4.13.3 Mac address filtering

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

MAC Filter		
Valid Range (1 to 4094)		
VLAN ID	Address Type	Delete
	MAC Filter Valid Range (1 to 4094) VLAN ID	Valid Range (1 to 4094) VLAN ID Address Type

Parameter	Description			
Mac address	Can not add multicast Mac address			
VLAN	VLAN number			
	Can choose the following kinds:			
Filtoring direction	Both			
Fillening direction	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.

Address Table Config	
MAC Management MAC Learning and Ag	ng MAC Filter
MAC Address: 02:20:15:09: VLAN: 1 Filtering direction: Source filter	2:12 Valid Range (1 to 4094)

4.14 SNMP

In the navigation bar to select "SNMP", you can set to the Snmp 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:

🛃 Home	SNMP Config Community Config Group Config User Config Trap Config View Config
🌄 Quickly Set	SNMP Config
PORT	
VLAN	
Fault/Safety	
PoE	
STP	
DHCP RELAY	
DHCPserver	
TACACS+	
RADIUS	
AAA	
▶ QOS	
Addr Table	
► SNMP	
Snmp Config	
 Rmon Config 	
LACP	
SYSTEM	

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

【Configuration example】 Such as: open Snmp.

Such as, open Shimp.

SNMP Config	Community Config	Group Config	User Config	Trap Config	View Config	
SNMP Config						
Open						

4.14.1.2 Community config

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

SNMP Cont	fig Community Config Group Config	User Config Trap Config View Con	fig	
SNMP Commun	nity List			
	Community Name Access Authority Edit / Delete			
O New community O Delete Selected Community				

[Parameter Description]

Parameter	Description
	Community string, is equal to the NMS and Snmp agent
group	communication between the password
	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
Access authority	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.

SNMP Config	community Config Group Config	User Config Trap Config View Cor	ifig
SNMP Community List			
	Community Name	Access Authority	Edit / Delete
New community 🗢 De	lete Selected Community		First Back [1] Next Last // 1 Page
	SNMP Community Configuration	String Length (1-16)	

4.14.1.3 View Config

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

SNMP Config	Community Config	Group Config	User Config	Trap Config	View Config
View Name	* String leng	th[1-16]			
New view					

[Parameter Description]

Parameter	Description
View name	Wiew 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.

SNMP Config Co	mmunity Config	Group Config	User Config	Trap Config	View Config	
View Name 123	* String length	[1-16]				
New view						
SNMP Config Co	mmunity Config	Group Config	User Config	Trap Config	View Config	
View Name	* String length	1-16]				
New view						
View Rule List 123	 Delete View 					
Rule	Edit View Rule					× Jelete
🔘 New View Rule 🥥 Delete	Select Note: The use of	f "Exclude" in a rule is no	ot an effective method to :	ilter the view, this may c	ause undesired results.	st ¹ / 1 Page
	Rul	e: 🖲 Contain 🔘 Exc	lude			
	MIB Subtree OIE): . 1. 3. 6. 1	* String length[1-64]			
	Subtree Mask :	1	* String length[1-31]			
	Save	Exit				

4.14.1.4 Group Config

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

SNM	SNMP Config Community Config Group Config User Config Trap Config View Config						
SNMP G	SNMP Group						
	Croup Name Security Level Read View Read and Write View Notify View Edit / Delete						
O New	🕲 New Group 😂 Delete Selected Group First Back [1] Next Last / 1 Page						

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	The associated view name
write view study view	

[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.

View rul	View rule list 123 delete view									
	rule	MIB subtree OID	subtree mask	operation						
	included	.1.3.6.1		2 🕺						
📀 New vi	S New view rule Select View rule frist page prev page (1) next page last page 1									

SNMP Config Com	munity Config Group	Config User	Config Trap Config View	w Config	
SNMP Group					
Group Name	Security Level	Read View	Read and Write View	Notify View	Edit / Delete
🔾 New Group 🥥 Delete Selec	ted Group			First Back [1] Ne	ext Last ¹ / 1 Page
_	Group Name : Security Level : Auth Read View : Notify View: Save Exit	entication and I v e v e v	ing Length (1-16)		

4.14.1.5 User config

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

SN	SNMP Config Community Config Group Config User Config Trap Config View Config										
SNM	SNMP User										
	User Name	Security Level	Group Name	Authentication Mode	Authentication Password	Encrypt Mode	Encrypt password	Edit / Delete			
0 N	O New User O Delete Select User First Back [1] Next Last / 1 Page										

Configuration ∎66

Description
User name,range 1-16
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
Specified use MD5 authentication protocol or SHA authentication protocol
Range 8-10
Specified using AES encryption protocol or DES encryption protocol
A user group name
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.

SNMP Config	Community	Config	Group Config	User Config	Trap Config	View Confi	g		
SNMP User									
User Name	Security Level	Group Name	Authentication Mod	de Authenti	cation Password	Encrypt Mode	Encrypt password	Edit / Delete	
🔘 New User) 의 De	S New User Select User First Back [1] Next La								
	Edit	SNMP user					×		
	Use Gro Aut Co Enc Co	rr Name : zurity Level : up Name : hentication Mode : hentication Passw nfirm Authenticatio zrypt Mode : zrypted Password nfirm Encrypted Pa Save	user1 Authentic goup1 MD5 12345678 DES : assword : 12345678 DES :	* Str ation and i • • • • • • • • • • • • • • • • • • •	ing Length (1-16) ing Length (8-60) ing Length (8-60)				

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:

SNM	P Config Community Config	Group Config User	Config Trap Config	View Config					
Trap De	stination Host								
	Destination IP Address	Security Name	UDP Port Number	Security Mode	Edit / Delete				
O New	O New Trap O Delete Selected Trap								

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
Security mode	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 hoset 192.168.2.30 receive trap information.

SNMP Con	nfig Community Config	Group Config User	Config Trap Config	View Config	
Frap Destinati	ion Host				
	Destination IP Address	Security Name	UDP Port Number	Security Mode	Edit / Delete
New Trap	Delete Selected Trap			First Back [1] Ne	ext Last ¹ / 1 Page
	New Trap Destination IP Security Nam UDP Port Num	Address 192, 168, 0, 22 e: user1].].		×
	Security Mode	ə: v1 •			
	Save	Exit			

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:

🛃 Home	Statistics Group History Gro	oup Alarm Group Event Group		
uickly Set	Statistics Group List			
► PORT	Index	Interface Name	Owner	Edit / Delete
VLAN				
Fault/Safety	New Count Group Unlete Selected Count Group	count Group		First Back [1] Next Last / / 1 Page
PoE				
► STP				
DHCP RELAY				
DHCPserver				
TACACS+				
► RADIUS				
► AAA				
▶ QOS				
Addr Table				
SNMP				
Snmp Config				
Rmon Config				
► LACP				
SYSTEM				

Parameter	Description
index	The index number, the value range of statistical information
Index	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.

Statistics Group	History Group	Alarm Gro	up Ev	ent Group				
count group list								
	index		interfa	ce name			owner	etatus
🕼 new count group) 😅	delete select count grou	p stat	tistical grou	ip configurat	tion			
	2		index :	77	* [1	-65535]		
		in	nterface name :	interface Gi0/4	*			
			owner:	Coco	* st	tring length[1-30]		
			setting	quit				
Statistics Group	listory Group Ala	rm Group E	vent Group					
count group list								
		interface name		01	mor	status		operation
77		Statistical info	ormation					
	e select count group	N	lumber of Packet I	Discarding Events :		0		
V new count group V delete	e select count group		Number of R	of Received Bytes : eceived Packets 'l		989395	=	rst page prev page [1] next page 1
				Number of Received Broadcasting Packets :		4164		
		Nur	nber of Received I	Multicast Packets :		5222		
	Number			ber of Received Packets With CRC Check Failed		0		
		Number of Recei	ved Packets Sma	، : ller Than 64 Bytes		312		
		Number of	Received Packets	Larger Than 1518			-	
		quit						

4.14.2.2 History Group

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

69 ■Configuration

of an Ethernet interface information. The following picture.

Statis	tics Group	History Group	Alarm Group Event Group				
history g	roup list						
	index	interface name	maximum number of samples	sample period	owner	status	operation
🗿 new l	history group	😂 delete select history group			frist page prev page	e [1] next page last	page1 / 1page

[Parameter Description]

Parameter	Description
index	Historical control table item index number, value range is 1 ~
Index	65535
Interface name	To record the Ethernet interface
Maximum number of	Set the history control table item of the corresponding table
	capacity, namely the Max for number of records the history
samples	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]

Snmp 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.

Statistics Group History Group	Alarm Group	Event Group		
history group list				
index interface nam	histor	y group configurat	inher of samples	samle period
ew history group Gelete select history gro	inte	index: 222 rface name: Interface G Maximum number of samples: 22222 mple period 23	• [1-65535] • [1-65535] • [1-65535] • second	* E V

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.

Statistics Gro	Dup History Group	Alarm Group				
event group list						
	index	description	owner	action	status	operation
📀 new event gro	up 🤤 delete select event grou	p			frist page prev pag	e [1] next page last page1 / 1page

[Parameter Description]

	-
Parameter	Description

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

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.

Statistics Group	History Group	Alarm Group	Event Group			
event group list						
	index	event gr	oup configuration	owner	action	x status
new event group	v delete select event group		index: 345	* [1-65535]		
		de	owner: Coco	* string length[1-30] * string length[1-30]		
			action: 🗹 Log 🔽 Tra	ар		
		save	quit			

4.14.2.4 Alarm Group

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

	tatistic	cs Group	History	Group	Alarm Gro	oup	Event Group						
Ali	arm Grou	up List											
	Index	Statistical Event	Statistical Group Index	Sampling Time Interval	Sample Type	Last Sample Count	Upper Alarm Threshold Limit	Upper Alarm Threshold Limit Events	Lower Alarm Threshold Limit	Lower Alarm Threshold Limit Events	Ower	Status	Edit / Delete
٢	New Ala	arm Group (Delete Selecte	ed Alarm Group						First Back [1] Nex	t Last	1	1 Page

[Parameter Description]

Parameter	Description				
index	The alarm list items index number, value range is 1 ~ 65535				
	Statistical type values :3:DropEvents. 4:Octets. 5:Pkts.				
	6:BroadcastPkts. 7:MulticastPkts. 8:CRCAlignErrors.				
Statia tabla	9:UndersizePkts. 10:OversizePkts. 11:Fragments. 12:Jabbers.				
Static table	12:Collisions. 14:Pkts64Octets. 15:Pkts65to127Octets.				
	16:Pkts128to255Octets. 17:Pkts256to511Octets.				
	18:Pkts512to1023Octets. 19:Pkts1024to1518Octets				
statistical index	Set up the corresponding statistics statistical index number,				
statistical index	decided to statistics to monitor the port number				
Sampling interval	Sampling time interval, the scope for 5 ~ 65535, the unit for				
Sampling interval	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	Upper/lower limit reached, for each event
events	
owner	Set the table creator, ownername for 1 ~ 30 characters of a
	string

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.

Statistics Group History Group Alarm Group	Event Group
Alarm Group List	
Index Statistical Event Statistical Group Index Sampling Time Interval Sample Type Sample Group	Last Sample Count Threshold Limit Events Upper Alarm Threshold Limit Events Lower Alarm Threshold Limit Events Ower Alarm Threshold Limit Events Delete
New Alarm Group Sole Alarm Group Configuration	× 1 /1Page
Index:	123 * [1-65535]
Statistical Event:	DropEvents -
Statistical Group Index:	77 •
Sampling Time Interval:	123 * Second(s)[5-65535]
Sample Type:	Absolute -
Owner:	Coco * String length[1-30]
Upper Alarm Threshold Limit:	12 * [0-2147483647]
Upper Alarm Threshold Limit Events:	456 🗸
Lower Alarm Threshold Limit:	3 * [0-2147483647]
Lower Alarm Threshold Limit Events:	456 🗸
Save	

4.15 LACP

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

🛃 Home	LACP Setting LACP Display
🔜 Quickly Set	
 PORT VLAN Fault/Safety 	Open LACP : Apply
▶ PoE	LACP public parameter settings
STP DHCP RELAY DHCPserver	System priority 1 (1-65335) Apply
TACACS+	LACP activation port parameter settings
RADIUS	choose port to set up:
AAAQOS	1 3 5 7 g 宜宜宜口
 Addr Table SNMP 	2 4 6 8 10
► LACP	🗋 Optional 💼 Fixed port 💼 Selected 🕜 Aggregation 🕁 Trunk
Lacp Config	Tip : Click and drag cursor over ports to select multiple ports Select all Others Cancel
SYSTEM	Port priority: 1 (1-65335) Aggregate port number: 1 Aggregate model: active

4.15.1 LACP Setting

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

LACP Setting LACP Display
LACP status
Open LACP :
Apply
LACP public parameter settings
System priority 1 (1-65535)
Арріу
LACP activation port parameter settings
choose port to set up:
2 4 6 8 10
🗋 Optional 💼 Fixed port 🕋 Selected î 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:
Aggregate model: active
Apply

[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.

73 ■Configuration

LACP activation port parameter settings					
choose port to set up:					
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$					
🖸 Optional 💼 Fixed port 👚 Selected î 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.



[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	Prioricy	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:

🛃 Home	System Settings System Restart Password EEE Enable SSH Login Teinet Login System Log
🔜 Quickly Set	Basic System Information
 PORT VLAN Fault/Safety PoE STP DHCP RELAY DHCPserver TACACS+ RADIUS 	Management VLAN: Device MAC: [94:60:36:09:11:07] Management IP: 192:168.0.1 Ipv6 Address: Subhet Mask: 255:255:255.0 Device Name: Svi tah Device Ioaction: Jumbo Frame: 1518 (1518-9216) Contacts(include mailbox): DNS Server: 0.0.0 Login Timeout
 QOS 	Save Set management VDm
Addr Table SNMP	- Current System Time: 2000-01-01 15:43:01
► LACP	Set Time:
SYSTEM	NTP Server
System Config	- Super-
Config Managem Config Save	

[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:

Administrator Pri..
 Info Collect

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.

🗮 Home	VLAN Settings Trunk Port Settings Hybrid Port Settings								
🔜 Quickly Set	VLANIDS								
▶ PORT	VLAN ID VLAN Name VLAN IP Port Edit / Delete								
 VLAN Vlan Config 		1	VLAN0001	192.168.0.1/24	1-2,4-10				
Fault/Safety		2	VLAN0002		3	D 🗙			
PoE	O New VLAN O Delete VLAN First Back [1] Next Last /1 Page								

ĺ	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	m Restart Password EEE Enable SSH Login Telnet Login System Log	
Basic System Information	······································	
Management VLAN 2	* Device MAC: [D4:66:BA:09:11:DF	
Management IP: 192.168.0.2	* Ipv6 Address:	
Subnet Mask: 255, 255, 255, 0	* Device Name: Switch	
Default Gateway: 192. 168. 0. 221	Device Location:	
Jumbo Frame: 1518	(1518-9216) Contacts(include mailbox):	
DNS Server: 0.0.0.0		
(Minutes): 30		
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 💌 *	Device MAC: D4:	68:BA:09:11:DF				
Management IP:	192. 168. 0. 15 *	lpv6 Address:					
Subnet Mask:	255. 255. 255. 0 *	Device Name: yoy	0				
Default Gateway:	0. 0. 0. 0	Device Location:					
Jumbo Frame:	5000 (1518-9216)	Contacts(include mailbox):					
DNS Server:	0. 0. 0. 0						
Login Timeout							
(Minutes):	20						
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:

🛃 Home	System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log	
🌄 Quickly Set	Postart							
PORT	Restart							
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								

[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:

77 ■Configuration

🛃 Home	System Settings System Restart Password EEE Enable SSH Login Telnet Login System Log	
nuickly Set	Change Administrator Password	
 Quickly Set PORT VLAN Fault/Safety PoE STP DHCP RELAY DHCPRELAY TACACS+ RADIUS AAA QOS Addr Table SIMP LACP SYSTEM 	Change Administrator Password Password type: Encrypted passwor • Old Password: • New Password: • Confirm New Password: • Save Clear	
System Config		
System Update Config Managem Config Save Administrator Pri Info Collect		
[Instructio	on]	

- 1. If you set a new Web login password, then log in again after seting 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 Pas	ssword						
Passwi Old Pa New Pa	ord type: Encrypted passwo Issword: •••••						
Confirm New Pa	issword: 🕶 🍽 🕈						

4.16.1.4 EEE Enable

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

me	System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log
Quickly Set	EEE Config						
PORT	Oner						
LAN	open						
ault/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 							

[Instruction]

Energy Efficient Ethernet, Open the EEE features by default.

【Configuration example】

Such as: EEE closed.

System Settings System Restart	Password EEE Enable	SSH Login Telnet Login S	aystem Log
EEE Config			
Closed			

4.16.1.5 SSH login

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



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.

System Settings	System Restart	Password	EEE Enable	SSH Login	Telnet Login	System Log
SSH Config						
Open						
SSH Timeout: 3	*					

79 ■Configuration

4.16.1.6 Telnet login

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

Home	System Settings System Restart Password EEE Enable SSH Login Telnet Login System	m Log
Quickly Set	Teinet Config	
PORT		
VLAN		
Fault/Safety		
PoE		
STP		
DHCP RELAY		
DHCPserver		
TACACS+		
RADIUS		
ΑΑΑ		
QOS		
Addr Table		
SNMP		
LACP		
SYSTEM		
- System Colling		
 System Opdate 		
 Config Managem 		
 Config Save 		
Administrator Pri		

[Instruction]

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

【Configuration example】

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

System Settings System Restart Password EEE Enable SSH Login Telnet Login System Log	
Telnet Config	
Open	
Teinet Timeout 3 *	

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]

|--|

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.

System Settings	System Restart Password EEE Enable SSH Login Telnet Login System Log
Log Config	
Log Switch:	Open
Server IP:	192. 168. 0. 88
Send Log Level:	Errors(3)
Save setting	

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

Current Log Information	
Keyword fail Clear Syslog	
Trap logging: level informational, 231 message lines logged, 0 fail	
	Ŧ

4.16.2 System Upgrade

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

🛃 Home	System Upgrade
🔜 Quickly Set	Current Software Version: D161116
▶ PORT	File Name: Browse No file selected. Start Upgrade
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	
[Instructio	n

- 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:

🛃 Home	Import/Export Config Restore Config	Factory Reset	
🔜 Quickly Set			
▶ PORT	Show Current Config Export Config		
VLAN	Backup Import Configuration File Name:		
Fault/Safety	Con Cine Bacher		
PoE	Confirm Dackup		
STP	Backup File List		
DHCP RELAY	Name	Size	Time Stamp
DHCPserver			
TACACS+			
RADIUS			
AAA			
▶ QOS			
Addr Table			
▶ SNMP			
LACP			
SYSTEM			
 System Config 			
 System Update 			
Config Managem			
 Config Save 			
Administrator Pri			
Info Collect			
Lingtrustion	. 1		

[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.

Import/Export Config Resto	re Config Factory Reset	
Show Current Config		
Backup Import Configuration		
Do not refresh or close the page during the in Prompr: After the introduction of configuration	ort , the nable the new configuration, please in this page Restart device Oth	erwise configuration does not take effect
File Name: Browse No file selected.	Opening switch.conf You have chosen to open:	x
Backup File List	switch.conf	
Name	which is: conf File from: http://192.168.0.15	Time Stamp
	What should Firefox do with this file?	

2) Import configuration.

Show Current Config Export Config Backup Import Configuration Do not refresh or close the page during the import Prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect File Name: Browse No file selected. Import configuration	
Backup @ Import Configuration Do not refresh or close the page during the import Prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect File Name: Browse No file selected. Import configuration	
Do not refresh or close the page during the import Prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect File Name: Browsen Bo file selected. Import configuration	
Prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device Otherwise configuration does not take effect File Name: Browse. No file selected. Import configuration	
File Name: Browse No file selected. Import configuration	
Dealwar file Lief	
Backup rite List	
N → → → → → → → → → → → → → → → → → → →	
■ 桌面 「	
○ 庫 ■ 40-55	
Revend Compare 1	
■ 计算机	
Import/Export Config Restore Config Factory Reset	
Show Current Config Export Config	
Backup Import Configuration	
Do not refresh or close the page during the import	
Prompr: After the introduction of configuration, to enable the new configuration, please in this page Restart device therwise configuration does not take effect	
File Name: Browse No file selected. Import configuration	
Backup File List	
Name Size Time Stamp	

3) Backup.

Import/Export Config Restore Config Factor	/ Reset	
Show Current 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 R	Reset	
Name	Size	Time Stamp
12357.conf 12357.conf	5.66K	15:38:34 2016-12-20
Restore Backup O Delete Backup O 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 F	Reset	
Name	Size	Time Stamp
12357.conf	5.66K	15:38:34 2016-12-20
Restore Backup Delete Backup Save Backup Rename Backup 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
```

[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.



4.16.4 Config Save

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

😁 Home	Save Settings
🖏 Quickly Set	ouro octango
▶ 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	

[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.

🛃 Home	Administrator Settings	
🌄 Quickly Set	Password type: Encrypted password -	
▶ PORT	User Name:	
VLAN	New Password:	
Fault/Safety	Confirm Password:	
PoE	Add User	
▶ STP		
DHCP RELAY	User List	
DHCPserver	User Name	Edit / Delete
TACACS+	licor	
RADIUS	4961	
► AAA	admin	Ø
▶ QOS		First Back [1] Next Lasti / 1 Page
Addr Table		
SNMP		
▶ LACP		
SYSTEM		
 System Config 		
System Update		
Config Managem		
Config Save		
Administrator Pr		
Info Collect		

[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

85 ■Configuration

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:

Administrator Settings	
Password type: User Name: New Password: Confirm Password: Add User	
User Name	Edit / Delete
user	
admin	Ø
	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.

🛃 Home	523 av
🄜 Quickly Set	ULLECT
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	
[Instruction	n】

Collect useful infomation, it may take a few moment.

【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 \times W \times H)	280*180*44.3 mm
Environment	Operating Temperature: 0°C~45°C
	Storage Temperature: -40°C ~70°C
	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