



轻管理环网交换机软件使用手册

sDot

南京实点电子科技有限公司

版权所有 © 2026 南京实点电子科技有限公司。保留所有权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

 和其它实点商标均为南京实点电子科技有限公司的商标。

本文档提及的其它所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受实点公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，实点公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

南京实点电子科技有限公司

地址：江苏省南京市江宁区隐龙路 9-1 号 40 栋

邮编：211106

电话：4007788929

网址：<http://www.solidotech.com>

目录

1	产品概述.....	5
1.1.	产品简介.....	5
1.2.	基本参数.....	5
2.	硬件参数.....	7
2.1.	尺寸描述.....	7
2.2.	指示灯.....	8
3.	产品安装.....	9
3.1	DIN 卡轨安装.....	9
3.2.	设备上电.....	9
4.	设备登录访问.....	11
4.1	WEB 登录.....	11
4.2	Console 访问.....	11
5.	产品软件功能.....	13
5.1	系统管理.....	13
5.1.1	系统信息.....	13
5.1.2	IP 设置.....	13
5.1.3	账号设置.....	14
5.1.4	端口管理.....	15
5.1.5	光模块状态.....	16
5.2	系统配置.....	16
5.2.1	IGMP 侦听.....	16
5.2.2	汇聚管理.....	17
5.2.3	环回保护.....	18
5.2.4	端口镜像.....	18
5.2.5	端口限速.....	19
5.2.6	巨型帧设置.....	20
5.2.7	EEE 设置.....	21

5.2.8 简单网络管理	22
5.2.9 生成树	23
5.2.10 LLDP 设置	24
5.2.11 LLDP 邻居	25
5.3 VLAN 功能	25
5.3.1 MTU VLAN	25
5.3.2 端口 VLAN	26
5.3.3 802.1Q VLAN	26
5.3.4 802.1Q VLAN 配置示例	28
5.3.5 语音 VLAN	28
5.4 QoS 功能	29
5.4.1 QoS 基本配	30
5.4.2 QoS 高级配置	31
5.5 安全功能	33
5.5.1 MAC 管理	33
5.5.2 风暴抑制	34
5.5.3 流量监控	34
5.5.4 线缆检测	35
5.5.5 DHCP 侦听	35
5.6 诊断工具	36
5.6.1 系统升级	36
5.6.2 Ping 工具	36
5.6.3 备份还原	37
5.6.4 系统恢复	37
5.6.5 配置保存	37
5.6.6 系统重启	37

1 产品概述

1.1. 产品简介

该产品是一款管理型全千兆工业以太网交换机，该产品具备较高的交换指标性能，支持 2 个千兆 SFP 插槽+4 个 10/100/1000M 自适应电口，在转发性能上该产品满足 20Gbps 的交换带宽，包缓存高达 4Mbit，支持 8K 转发 MAC 地址表，并支持 VLAN、QoS、RSTP、风暴抑制、LACP 汇聚等功能。该产品采用工业级设计，工作温度支持-40℃~80℃环境温度，可以稳定的工作在恶劣的工业现场环境。是交通行业、安防监控行业、污水处理、能源化工等行业的工业通信首选产品。

1.2. 基本参数

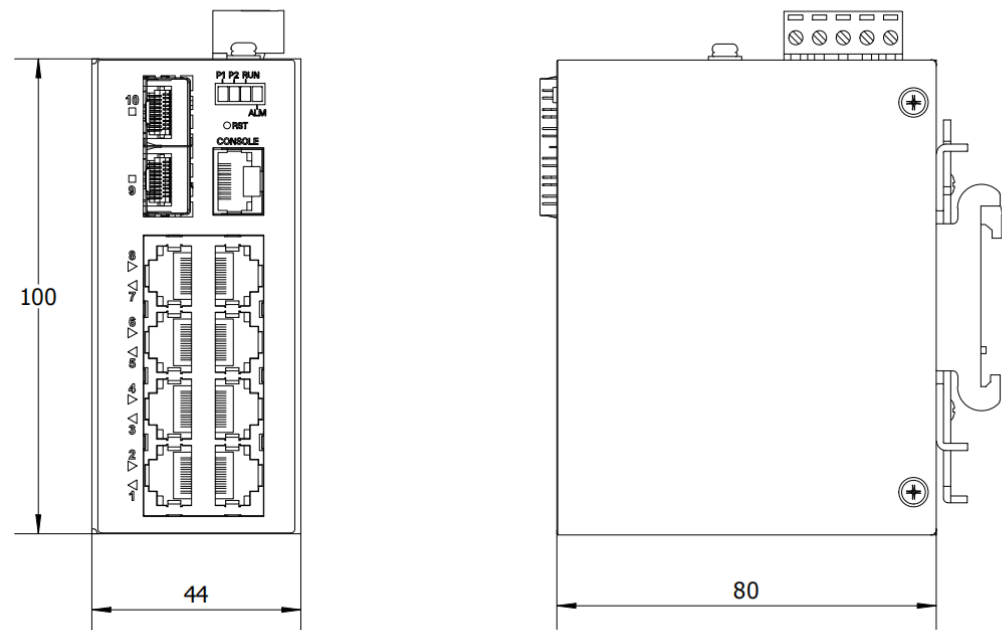
表 1：电气参数

分类	参数	数值
性能指标	MAC 地址	8K
	背板带宽	20Gbps
	交换缓存	4Mbit
	交换时延	≤7us
硬件指标	工作电压	DC9~56V 供电
	设备功耗	≤7.3W@DC12V（高温满载），空载≤2.5W
	尺寸	100mm×80mm×44mm（长×宽×高）
	安装方式	导轨安装
	接地螺丝	1 个
	工作温度	-40℃~80℃
	存储温度	-40℃~85℃

	工作湿度	5%~95% RH 无凝结
	存储湿度	5%~95% RH 无凝结
	光口数量	2 个 SFP 插槽，可适配千兆/百兆 SFP 光模块
	电口数量	4 个 10/100/1000M 自适应电口
	静电防护	接触放电 6KV；空气放电 8KV
	浪涌防护	电源回路 4KV；网口回路 2KV
	电快速脉冲群	电源回路 4KV；网口回路 2KV
	隔离耐压	电源 AC500V；网口 AC500V
软件功能	系统管理	系统信息、IP 设置、账号设置、端口管理、光模块状态
	系统配置	IGMP 侦听、汇聚管理、环回保护、端口镜像、端口限速、巨型帧设置、EEE 设置、简单网络管理、生成树、LLDP 配置、LLDP 邻居
	VLAN 功能	MTU VLAN、端口 VLAN、802.1Q VLAN、语音 VLAN、管理 VLAN
	QoS 功能	支持 SP、WRR、WFQ 策略、支持基于端口、802.1P、DSCP 模式
	安全管理	支持 MAC 管理、风暴抑制、流量监控、线缆检测、DHCP 侦听
	维护管理	在线升级、Ping 工具、备份还原、系统恢复、配置保存、系统重启控制

2. 硬件参数

2.1. 尺寸描述



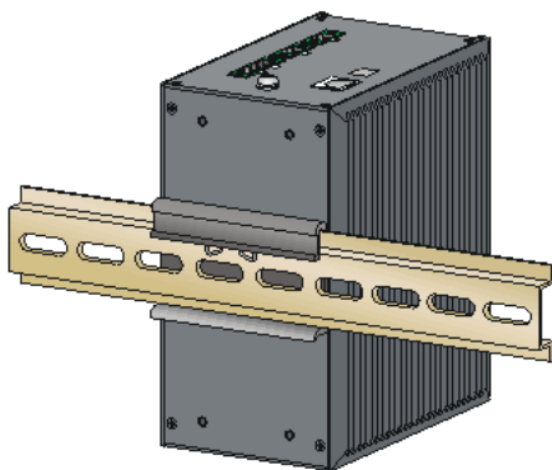
2.2. 指示灯

标识	说明	状态	
P1/P2	电源1指示灯	常亮	电源正常
		灭	电源异常/电源未供电
RUN	系统运行指示灯	闪烁	系统正常
		灭/常亮	系统异常
ALM	告警指示灯	常亮	系统有告警 如电源、端口等
		灭	系统无告警
1-4	电口状态指示灯	闪烁	端口正常收发数据
		常亮	千兆或者百兆速率
5-6	光口状态指示灯	闪烁	端口正常收发数据
		常亮	千兆或者百兆速率

3. 产品安装

3.1 DIN 卡轨安装

将 DIN 卡轨座的上部卡在 DIN 轨上，在设备的上端稍微用力向下压并向内转动设备，使得卡轨座下部卡在 DIN 轨上。如下图所示：



3.2. 设备上电

工业交换机输入电源支持 DC9~56V 和 AC24V，输入端子为凤凰压接端子，因此，该设备的供电电源区分为交流和直流供电两种规格。



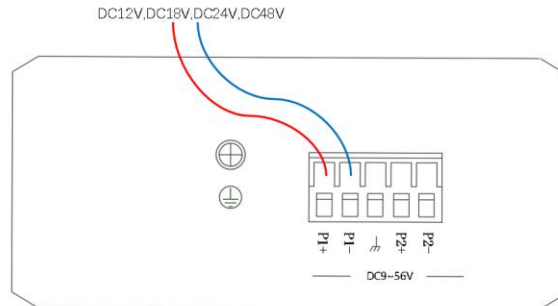
注意：

请在上电之前确认设备的供电规格，避免出现人员伤亡或设备损坏的情况。

安装过程如下：

- 1) 确保设备与电源断开；
- 2) 将保护接地线缆一端接到设备顶面板的接地螺钉上，另一端就近良好接地；

- 3) 针对直流供电产品，将直流电源线缆接入凤凰端子，（“P1+”接线柱连接直流电源线的正极，“P1-”接线柱连接直流电源线的负极），并用螺丝刀将凤凰端子顶侧的螺丝旋紧使其固定，如下图所示：



- 4) 针对交流供电产品，将交流电源线缆接入凤凰端子，（“P1+”接线柱连接交流电源的 L 线，“P1-”接线柱连接交流电源的 N 线），并用螺丝刀将凤凰端子顶侧的螺丝旋紧使其固定。

i 说明：

直流供电版本有两个直流电源接口，实际使用时可以选择其中一个或者两个接入，两个电源接口起到互相备份作用。交流供电版本有 2 个交流电源接口，两个电源接口起到互相备份作用

4. 设备登录访问

该交换机支持以下登录方式：

4.1 WEB 登录

通过 Web 登录设备，登录成功后，用户可以使用 Web 界面直观的配置和管理设备。Web 登录管理是一种便捷的传统管理模式，当用户未携带 Console 通信线缆或者 PC 机没有可用串口时，可以通过 Web 管理首次登录设备并进行配置管理。

交换机默认缺省地址：192.168.1.6/24，用户名：admin，密码：admin

在 PC 主机上打开浏览器，在地址栏中输入“192.168.1.6”，按回车键后显示用户登录界面，如下图所示。（下图请以实物为准）



4.2 Console 访问

通过 CLI 登录设备，登录成功后，可以直接输入命令行来配置和管理设备。CLI 方式下根据使用的登录接口和登录协议不同，该产品支持通过 Console 口进行访问。

Console 口登录管理是一种便捷的命令行管理模式，客户可以通过超级终端，例如：SecureCRT 软件进行串口登录。如下图所示



波特率：115200，数据位 8，奇偶校验 None，停止位 1，点击连接即可接入交换机命令行界面。



注意：

交换机不支持 CLI 命令行配置管理，提供 Console 接口主要用于设备升级、调试及重启操作用途。

5. 产品软件功能

 注意：

所有的软件功能配置完毕后，请在左侧栏→配置保存，进行保存操作，避免设备重启后导致配置未生效的问题。

5.1 系统管理

5.1.1 系统信息

系统信息主要是交换机系统的相关信息情况，包括了设备系统的系统名称、MAC地址、IPv4 管理地址、IPv6 管理地址（不支持修改）、子网掩码、默认网关以及软件版本和硬件版本等信息。如下图所示：

系统信息

系统名称	Switch
MAC地址	00:18:93:aa:bc:24
IPv4地址	192.168.1.6
IPv6链路本地地址	FE80::218:93FF:FEAA:BC24/64 (自动)
IPv6全球单播地址	无
子网掩码	255.255.255.0
默认网关	----
DNS服务器	----
软件版本	LMS1.0.4
硬件版本	V.0.0.1

应用

系统信息配置	
系统名称	: 默认 Switch，可支持自定义，32 个字符内

5.1.2 IP 设置

IP 设置页面主要用于设备的管理地址设置，支持固定 IP 和 DHCP 自动获取 IP 两种方法，DHCP 设置默认为禁用。如下图所示：

IP设置

DHCP设置	禁用
IP地址	192.168.1.6
子网掩码	255.255.255.0
默认网关	
自动DNS	禁用
DNS服务器	

应用

IP配置

DHCP 设置：默认关闭

IP 地址：设备管理地址，默认 192.168.1.6，由 4 个 0 到 255 之间的数字组成，用点号分隔，只支持 IPv4，不支持 IPv6 地址修改

子网掩码：由 4 个 0 到 255 之间的数字组成，用点号分隔，如 255.255.255.0，不支持 CIDR 表示法进行输入

默认网关：默认为空

自动 DNS：默认禁用

DHCP 主机：默认为空，DHCP 开启后，由主机地址获取 IP

 **注意：**

设备 IP 地址建议采用固定 IP，谨慎采用 DHCP 方式进行主机分配，避免设备因为未获取到 IP 地址或者未知 IP 地址段导致的设备无法访问问题。

5.1.3 账号设置

设备账号管理主要用于设备的访问用户名及密码的设置，如下图所示：

用户设置

用户名	admin
旧密码	
新密码	
确认密码	

应用

用户设置

用户名：默认 admin，可更改为其他任意用户名，16 位字符

旧密码：原始密码，默认为 admin，可更改为任意其他字符

新密码：更改后的新密码

确认密码：更改后的新密码

5.1.4 端口管理

端口管理包括端口配置和端口状态两个部分，其中端口配置主要是用来设置各个端口的状态、速率、双工模式以及流控等参数，端口状态则是显示设备端口的最终各个状态。如下图所示：

端口配置

端口	状态	自动	速率	流控
端口 1	启用	开启	10M 半双工	开启
端口 2			10M 全双工	
端口 3			100M 半双工	
端口 4			100M 全双工	

应用

端口	状态		速率		双工		流控	
	配置	实际	配置	实际	配置	实际	配置	实际
端口 1	启用	禁用	自动	N/A	自动	N/A	开启	N/A
端口 2	启用	启用	自动	1000M	自动	全双工	开启	开启
端口 3	启用	禁用	自动	N/A	自动	N/A	开启	N/A
端口 4	启用	启用	自动	100M	自动	全双工	开启	开启
端口 5	启用	禁用	自动	N/A	自动	N/A	开启	N/A
端口 6	启用	启用	自动	1000M	自动	全双工	开启	开启
端口 7	启用	禁用	自动	N/A	自动	N/A	开启	N/A
端口 8	启用	禁用	自动	N/A	自动	N/A	开启	N/A
端口 9 (SFP,SGMII)	启用	禁用	自动	N/A	自动	N/A	开启	N/A
端口 10 (SFP,SGMII)	启用	禁用	自动	N/A	自动	N/A	开启	N/A

端口管理

端口：可选对应设备的端口

状态：端口的启用或者禁用状态，默认启用

- 自动**：端口速率的匹配模式，默认自动，关闭后需要手动强制端口速率
- 速率**：自动模式下无需更改
- 流控**：流控功能开启或关闭

5.1.5 光模块状态

光模块状态主要包括模块的工作温度、电压、电流以及发射功率和接收灵敏度、告警状态等信息。

光模块状态						
端口	温度(°C)	电压(V)	电流(mA)	发射功率(mW)	接收功率(mW)	信号丢失
9	N/A	N/A	N/A	N/A	N/A	N/A
10	30.69	3.32	10.42	0.10	0.00	是

5.2 系统配置

5.2.1 IGMP 侦听

IGMP（IGMP Snooping）是一种网络交换机功能，用于优化组播流量传输，通过监听 IGMP 协议消息，了解哪些设备加入了组播组，从而将组播流量仅转发给相应的端口，避免了广播到整个网络，导致网络阻塞。如下图所示：

IGMP侦听

IGMP侦听	☒ 启用 ☐ 禁用
IGMP快速离开	☐ 启用 ☒ 禁用
IGMP Report抑制	☐ 启用 ☒ 禁用
VLAN ID	1
IGMP查询器状态	☐ 启用 ☒ 禁用
IGMP查询器选举	☒ 启用 ☐ 禁用
IGMP查询器版本	V2
IGMP查询器全局地址	(如果为空, 则采用默认IP地址!)

应用

IGMP 侦听
IGMP 侦听 ：IGMP 功能开关，默认禁用

IGMP 快速离开：默认禁用，IGMP 功能开启后可选择启用，通过 IGMP Leave 消息进行通知控制，交换机默认收到 Leave 消息后立即离开组播组，停止向该端口转发组播流量（注意：开启后，网络庞大的情况下会增加交换机处理负担）

IGMP Report 抑制：默认禁用，IGMP 功能开启后可选择启用，IGMP Report 抑制是一种网络优化机制，减少网络中不必要的 IGMP 报告消息，抑制重复的 IGMP 报告，降低网络负载，提高效率，主要针对多个主机加入同一个组播组时，发送相同的 IGMP 报告消息

VLAN ID：默认 VLAN1

IGMP 查询器状态：默认禁用，IGMP 功能开启后可选择启用，启用后，可查到定期发送的查询组报文至 224.0.0.1，查询子网上是否有任何主机需要接收到任何组播报文

IGMP 查询器选举：默认禁用，IGMP 功能开启后可选择启用

IGMP 查询器版本：默认 V2

IGMP 查询器全局地址：默认空，当查询器状态开启后，此处会显示源地址

5.2.2 汇聚管理

端口汇聚（Trunk）是一种通过软件配置将多个物理端口组合成一条逻辑链路的技术，主要用于增加交换机和网络节点之间的带宽，提供更高的传输性能和链路冗余。如下图所示：

汇聚配置

汇聚组	转发端口
汇聚 1	端口 1 端口 2 端口 3 端口 4

应用

汇聚组	转发端口	选择
汇聚 1	1,2	☐
汇聚 2	----	☐
汇聚 3	----	☐
汇聚 4	----	☐

全选 删除

汇聚配置

汇聚组

: 选择需要配置的汇聚组，最多支持 4 个汇聚组

转发端口

: 选择对应的物理端口，至少需要 2 个端口参与，选择的时候请按住键盘上的 ‘Ctrl’ 按键进行多次选择操作，每个汇聚组单口最多不超过 8 个

汇聚组的删除

: 勾选对应需要删除的汇聚组，点击删除按钮

5. 2. 3 环回保护

环回保护功能是给交换机提供一种环网检测的功能手段，主要是用来检测端口在环回的情况下，避免因为广播风暴导致的网络瘫痪的情况发生。

环回保护设置

环回保护状态

禁用

应用

端口	状态
端口3	正常
端口4	正常
端口5	正常
端口6	正常
端口7	正常
端口8	正常
端口9	正常
端口10	正常
汇聚1	正常

环回保护

环回保护状态

: 默认禁用，可以选择开启，注意，环回保护状态开启需要关闭设备的 RSTP 功能，开启环回保护功能后，交换机会持续发送广播报文到对应端口进行探测，相应一旦收到环回的信息，设备会自动将环回端口进行阻塞。

5. 2. 4 端口镜像

端口镜像（port Mirroring）功能是通过在交换机上进行配置，将一个或者多个源端口的数据流量转发到设备的某个指定端口来实现对网络的流量侦听，指定的

端口为镜像端口或者目的端口，在不严重影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络流量进行监控分析,或者在网络故障的时候进行定位故障分析。如下图所示：

端口镜像

镜像会话	端口镜像使能	镜像端口
1	禁用	
2	禁用	
3	禁用	
4	禁用	

镜像会话

被镜像端口

入口

出口

1

端口 1
端口 2
端口 3
端口 4

禁用

禁用

应用

被镜像端口	入口	出口
端口 1	禁用	禁用
端口 2	禁用	禁用
端口 3	禁用	禁用
端口 4	1	1
端口 5	禁用	禁用
端口 6	1	1
端口 7	禁用	禁用
端口 8	禁用	禁用
端口 9	禁用	禁用
端口 10	禁用	禁用

端口镜像

镜像会话

：本机最多支持 4 组镜像端口

端口镜像使能

：针对镜像会话进行对应的功能开启或者禁用

镜像端口

：选择镜像端口，每个镜像会话只能具备 1 个镜像端口

被镜像端口

：选择被镜像端口，可以选择多个端口，通过‘Ctrl’按键进行多选

入口

：被镜像端口的入口数据

出口

：被镜像端口的出口数据

5. 2. 5 端口限速

端口限速功能主要是针对端口进行传输速率的限制，用于均衡网络带宽、防止恶意攻击、保护服务器资源等作用，可以有效的控制网络的流量，如图所示：

端口限速

端口	入口速度	出口速度
端口 1 端口 2 端口 3 端口 4	* 32Kbps	* 32Kbps

应用

端口	入口速度	出口速度
端口 1	禁用	禁用
端口 2	禁用	禁用
端口 3	禁用	禁用
端口 4	禁用	禁用
端口 5	禁用	禁用
端口 6	禁用	禁用
端口 7	禁用	禁用
端口 8	禁用	禁用
端口 9	禁用	禁用
端口 10	禁用	禁用

端口限速

端口

：选择需要限速的对应端口，可以’ Ctrl1’ +端口进行批量选择

入口速率

：最小 1*32kbps，最大 10000*32kbps

出口速率

：最小 1*32kbps，最大 10000*32kbps

5. 2. 6 巨型帧设置

巨型帧是以太网帧的一种特殊型式，是有效负载超过标准 IEEE802.3 规定的 1500 字节，主要是为了提升交换机传输效率，单帧承载更多数据，减少协议开销和中断频率，特别是针对大文件传输以及流媒体传输应用，同时还可以降低 CPU 负载，减少数据分片和重组操作。

 注意：

注意，通常巨型帧的应用需要链路上的所有设备均开启巨型帧且 MTU 值保持一致，否则会引起性能下降或者丢包情况的发生。

巨型帧配置

巨型帧使能

☒ 启用 ☐ 禁用

MTU大小

15k

应用

巨型帧配置
巨型帧使能：默认禁用，可选择启用 MTU 大小：启用后可配置，最高支持 15K 巨型帧

5.2.7 EEE 设置

EEE 节能以太网是 IEEE802.3az 标准定义的技术，通过动态的调整网络设备功耗，在低负载或者空闲状态下降低设备能耗，当启用该功能的对应端口无数据传输时，MAC 层发送休眠信号，PHY 层会关闭部分电路进入低功耗状态。如下图所示：

EEE 配置

EEE状态

禁用

应用

端口	EEE状态	选中
1	未启用	☐
2	未启用	☐
3	未启用	☐
4	未启用	☐
5	未启用	☐
6	未启用	☐
7	未启用	☐
8	启用	☐
9	启用	☐
10	启用	☐

EEE 配置
EEE 状态：默认禁用，可通过启用开启 端口选中：选中端口，开启对应的 EEE 状态

5.2.8 简单网络管理

简单网络管理是通过 SNMP 应用协议实现的，主要用于在 IP 网络上进行设备网络的节点管理，SNMP 提供了一种统一的管理接口，采用 UDP 协议+162/163 端口的方式进行操作，可以使不同的厂商和种类的网络设备通过统一的协议进行管理，如下图所示：

The image shows a web-based configuration interface for SNMP. It is divided into three main sections: '版本' (Version), '团体名' (Community Name), and '陷阱' (Trap). Each section contains a table of settings and an '应用' (Apply) button.

版本	
SNMP v1	☒ 启用 ☐ 禁用
SNMP v2c	☒ 启用 ☐ 禁用
应用	

团体名	
读取团体名	public
写入团体名	private
陷阱团体名	public
应用	

陷阱	
SNMP v1 陷阱	☐ 启用 ☒ 禁用
SNMP v2c 陷阱	☐ 启用 ☒ 禁用
陷阱接收服务器	☐ 主机名 ☒ IP地址 192.168.0.1
陷阱类型	☐ 冷启动/热启动 ☐ 端口连接/端口断开 ☐ 身份验证失败
应用	

简单网络管理

版本：本机支持 SNMPv1 和 SNMPv2c 版本，默认启用。

读取团体名：默认“public”

写入团体名：默认“private”

陷阱团体名：用于验证 SNMP Trap 消息合法性的认证字符串，可以确保陷阱消息由受信设备发送至 NMS 管理站点，默认“public”

陷阱启用：可选择启用 SNMPv1 陷阱和 SNMPv2c 陷阱

陷阱接收服务器：可以选择主机 IP 地址方式或者主机名方式

陷阱类型：可选择的陷阱类型

5.2.9 生成树

生成树协议是一种工作在 OSI 网络模型中的数据链路层通信协议，基本应用在防止交换机冗余链路产生的环路，用于确保以太网中无环路的逻辑拓扑结构，从而避免了广播风暴大量占用交换机带宽资源的情况。

生成树配置

生成树状态:	☐ 启用	☒ 禁用
强制版本:	☐ 生成树	☒ 快速生成树
转发延迟:	15	秒 (4-30)
最长有效期:	20	秒 (6-40)
发送保持计数:	6	个 (1-10)
优先级:	32768	(0-61440, 倍数4096)

应用

端口配置

端口	优先级	开销
端口1		
端口2		
端口3		
端口4		

应用

端口	优先级	开销	状态	角色
端口1	128	2000	禁用	禁用
端口2	128	2000	禁用	禁用
端口3	128	2000	禁用	禁用
端口4	128	2000	禁用	禁用
端口5	128	2000	禁用	禁用
端口6	128	2000	禁用	禁用
端口7	128	2000	禁用	禁用

生成树配置

生成树状态：默认启用，可选禁用

强制版本：可以选择强制生成树 STP 版本，或者 RSTP 快速生成树版本

转发延迟：转发延迟是时间单位，默认 15 秒，是控制端口状态切换的计时器，确保环路消除后才允许数据转发

MAX Age：判定配置的 BPDU 报文是否超时的计时器单位，主要用于阻塞端口的超时时间，在规定的时间内没收到 BPDU 报文，会重新协商，其次是控制网络规模，防止 BPDU 报文转发过远，默认为 20 秒，最大不超过 40 秒。

发送保持计数：-

优先级：设备优先级，默认 32768，如果要设置根交换机，需要调小该值

端口优先级：默认 128，步长 16，端口选举决策参数，用于在交换机上选举根端口或指定端口角色，优先级越小越优先，默认一般以端口号进行选举

路径开销：千兆为 2000，万兆为 200，带宽自动计算，无需修改

5.2.10 LLDP 设置

LLDP 是链路发现协议，主要用于本设备管理中发现和自己直连邻居信息，供网络管理系统查询及判定链路的通信状态。如图所示：

LLDP配置

LLDP 全局

☒ 启用

☐ 禁用

发送间隔

30

秒(范围 5-32768,默认 30)

发送保持

4

秒(范围 2-10,默认 4)

重新初始化延迟

2

秒(范围 1-10,默认 2)

发送延迟

2

秒(范围 1-8192,默认 2)

应用

端口

端口 1

端口 2

端口 3

端口 4

管理控制

禁用

应用

端口	管理状态
端口 1	发送&接收
端口 2	发送&接收
端口 3	发送&接收
端口 4	发送&接收

LLDP 配置

LLDP 全局：默认启用，可以配置禁用

发送间隔：封装了 TLV 的 LLDPDU 报文的发送间隔时间，默认 30 秒

发送保持：保持时间系数，默认 4 秒，设备信息在邻居设备中保持的有效时间，默认保持时间为 30*4=120 秒

重新初始化延迟：去使能状态到重新使能状态的延迟时间，避免由于 LLDP 协议状态频繁变动导致邻居设备的拓扑连接振荡，默认 2 秒

发送延迟：设备状态频繁发生变化时，向邻居设备发送 LLDP 报文的最小延迟时间，默认 2 秒

端口管理控制：所有默认端口在开启了 LLDP 功能后，均保持管理和控制状态，可以发送和接收 LLDP 报文，可以通过该配置进行禁止 LLDP 发送或者接收的功能

5.2.11 LLDP 邻居

对应端口的邻居设备状态信息，如下图所示：

LLDP 邻居								
本地端口	机架 ID	端口 ID	系统名称	生存时间	Med 能力	Med 设备类型	Med 网络策略	基于MDI的扩展功率
port 6	00-08-09-55-a7-0d	00-08-09-55-a7-17	switch	120	----	notDefined	----	----

5.3 VLAN 功能

5.3.1 MTU VLAN

可以理解为端口隔离功能，设置一个上行端口，该端口可以保持和下面所有端口都有效进行通信，但是下面的其他端口之间互相隔离。注意，开启了 MTU 端口后，端口 VLAN 以及 802.1Q VLAN 等功能均禁用。如下图所示：

MTU VLAN设置

MTU VLAN使能: ☒ 启用 ☐ 禁用 应用

当前Uplink端口

更改Uplink端口

2

端口 1
端口 2
端口 3
端口 4

应用

MTU VLAN 设置

MTU VLAN 使能

: 默认禁用，可选择启用

更改 Uplink 端口

: 选择了端口后，该端口保持和其他端口通信，其他端口之间隔离，互不通信

5.3.2 端口 VLAN

基于端口的 VLAN，处于同一 VLAN 的端口之间可以互相通信，可以有效的屏蔽广播风暴，并提高网络的安全性，端口 VLAN 通常适用在同一个交换机下的 VLAN 划分，如果跨交换机，需要采用 802.1Q VLAN。如下图所示：

端口VLAN设置

端口VLAN使能: ☒ 启用 ☐ 禁用 应用

VLAN	(1-4094, 最大可配置个数: 10)									
端口	1	2	3	4	5	6	7	8	9	10
成员	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

应用 删除

VLAN	成员端口
1	1-10

LLDP 配置

端口 VLAN 使能：默认启用，可以配置禁用

VLAN：输入对应的 PVLAN 号，可以根据具体配置进行勾选对应端口

成员：根据对应的 VLAN，勾选对应的端口

5.3.3 802.1Q VLAN

VLAN（虚拟局域网）技术是一种通过局域网内的设备逻辑的进行划分为一个个单独的逻辑网络来实现隔离广播域的一种技术，划分 VLAN 的好处是控制网络的广播风暴、确保网络安全、简化网络管理、灵活的网络分组等。802.1Q VLAN 是 VLAN 标准，是将 VLAN ID 封装在帧头，使以太网帧跨越不同的设备，也能保持 VLAN 信息，采用 802.1Q VLAN 可以实现跨交换机进行统一的 VLAN 管理和通信。如下图所示：

802.1Q VLAN设置

802.1Q VLAN使能 ☒ 启用 ☐ 禁用 应用

802.1Q VLAN	(1-4094)	描述	
端口	Untagged端口	Tagged端口	非成员端口
全选	☐	☐	☐
端口 1	☐	☐	☐
端口 2	☐	☐	☐
端口 3	☐	☐	☐
端口 4	☐	☐	☐
端口 5	☐	☐	☐
端口 6	☐	☐	☐
端口 7	☐	☐	☐
端口 8	☐	☐	☐
端口 9	☐	☐	☐
端口 10	☐	☐	☐

应用 删除

VLAN	VLAN描述	成员端口	Tagged端口	Untagged端口
1		1-10	-	1-10

802. 1Q VLAN 设置

802. 1Q VLAN 使能

: 默认禁用，可以配置启用

802. 1Q VLAN 号

: 可填写，范围 1-4094

描述

: 可选填

端口的 VLAN 规则

: 针对所选的端口，可选 Untag、Tag 或者非成员端口

802.1Q端口设置

端口	PVID	入口过滤
端口 1 端口 2 端口 3 端口 4		

应用

802. 1Q 端口设置

端口

: 根据 802. 1Q VLAN 设置中的规格选择对应的端口

PVID

: 根据 802. 1Q VLAN 设置中的规则填写对应的 VLAN PVID 号

5.3.4 802.1Q VLAN 配置示例

示例 1：如图所示



配置要求：

- 1、交换机A端口1和交换机B端口1互联；
- 2、交换机A端口2-4和交换机B端口2-4互通；
- 3、交换机A端口5-6和交换机B端口5-6互通；

A 和 B 交换机配置如下：

VLAN	VLAN描述	成员端口	Tagged端口	Untagged端口
1		1-10	1	2-10
2		1,5-6	1	5-6

端口	PVID	入口过滤
端口 1	1	禁用
端口 2	1	禁用
端口 3	1	禁用
端口 4	1	禁用
端口 5	2	禁用
端口 6	2	禁用
端口 7	1	禁用
端口 8	1	禁用
端口 9	1	禁用
端口 10	1	禁用

5.3.5 语音 VLAN

Voice VLAN 是为用户的语音数据流划分的 VLAN，用户通过创建 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以使语音数据集中在 Voice VLAN 中进行传输，便于对语音流进行有针对性的 QoS 服务质量配置，提高语音流量的优先级传输，保证通话质量。

通过语音 VLAN 功能将 OUI 地址匹配进入端口的报文中的源 MAC 地址字段，如果源 MAC 地址符合系统预先设置的 OUI 地址表地址，则被认可为语音流数据，被划分到语音 VLAN 中进行传输，并可以设置语音流的优先级。如下图所示：

语音VLAN配置

语音VLAN使能 ☒ 启用 ☐ 禁用 应用

VLAN ID

优先级

0

应用

使能默认OUI ☒ 默认OUI描述 3com OUI 00:E0:BB

使能自定OUI ☐ 自定OUI描述 OUI 添加

序号	OUI 描述	OUI	删除
----	--------	-----	----

删除

注意：
每一OUI同一时间只能分配给语音VLAN或监视VLAN。

端口设置

选择	端口	端口模式	语音状态
☐		手动	
☐	端口1	自动	待用
☐	端口2	自动	待用
☐	端口3	自动	待用
☐	端口4	自动	待用
☐	端口5	自动	待用

语音 VLAN 配置

语音 VLAN 使能：默认禁用，可以配置启用

VLAN ID：根据 802.1Q VLAN 配置，确定语音走哪个 VLAN 后，进行填写

优先级：不同的语音 VLAN 可以具备不同的优先级，可以根据选择填写，数字越高优先级越高

OUI：根据 IP 电话厂家进行查询，固定唯一编号，可以自定义

端口设置：勾选对应的 IP 电话端口后，进行选择手动或者自动

5.4 QoS 功能

QoS 服务器质量能够满足用户对不同应用不同服务质量的要求，可以根据用户的要求进行分配和调度资源，对不同的报文提供不同的服务质量。在传统的 IP 网络中，设备对所有的报文都采用等同传输方式，按照报文到达时间的先后，先入先出的排队策略（FIFO）处理，尽力而为的将报文传输到目的地，当网络带宽发生拥塞

的时候，所有的报文都有被丢弃的风险。QoS 针对某种类别的报文，将报文赋予特殊的传输服务，提供了优先级转发策略、拥塞避免等机制，对实时性强且重要的报文优先处理。

5.4.1 QoS 基本配置

QoS 基本配置包含了端口选择以及策略选择部分，共 SP、WRR、WFQ 三个策略可选，其中 SP 为严格优先级，严格的按照队列优先级的高低顺序进行队列调度，优点是利于时间敏感应用，确保关键业务优先，缺点是容易造成低优先级无法传输或者网络抖动的情况。WRR 是加权轮询，按轮执行，权重以计时器方式进行每发送一个基本单位计数器减一，直到没有数据或者计数器归零，WRR 加权轮询策略的优点是避免低优先级队列的报文长时间得不到调度，所有的队列都能够按照比例进行带宽的占用。缺点是针对大数据包队列的时候，权重的比例会失衡。最后一个 WFQ 策略是一种基于流队列调度策略，实现流量公平性和带宽共享，为每个数据流分配一个加权值来控制数据流在队列中获得的带宽资源比例，因此流量的大小、类型和优先级都可以被用作计算加权值的因素，一般适用于响应时间和流量均衡有高要求的网络，例如多媒体网络、语音和视频会议网络等。

QoS端口选择

选择	端口
☐	
☐	端口 1
☐	端口 2
☐	端口 3
☐	端口 4
☒	端口 5
☐	端口 6
☐	端口 7
☐	端口 8
☐	端口 9
☐	端口 10

全局配置

QoS策略

☒ SP

☐ WRR

☐ WFQ

应用

QoS端口选择

选择	端口
☐	
☐	端口 1
☐	端口 2
☐	端口 3
☐	端口 4
☒	端口 5
☐	端口 6
☐	端口 7
☐	端口 8
☐	端口 9
☐	端口 10

全局配置

QoS策略

☐ SP

☒ WRR

☐ WFQ

应用

队列权重设置

选择	队列	权重
☐		
☐	Q0	1
☐	Q1	2
☐	Q2	3
☐	Q3	4
☐	Q4	5
☐	Q5	6
☐	Q6	7
☐	Q7	8

应用

QoS 基础配置

QoS 端口选择

：勾选端口后，对应相应的 QoS 策略

QoS 策略

：可选 SP 绝对优先级策略，或者 WRR、WFQ 权重轮询策略

队列权重设置

：只针对 WRR 或者 WFQ 生效，配置优先级队列的权重比例

5. 4. 2 QoS 高级配置

QoS 高级配置功能主要是进行设备的 QoS 全局配置，包括采用端口 QoS、802. 1p 和 DSCP 三种优先级方式，其中端口优先级是设备默认的优先级方式，当报文没有携

带其他优先级标记的时候，例如不带 VLAN Tag 的报文采用端口优先级。802.1p 优先级是位于二层 VLAN 标签的 TCI 字段，使用 3 位，范围是 0-7，用于在二层网络中标识帧的优先级。DSCP 优先级则是属于三层标记，位于 IPv4 的 TOS 字段或者 IPv6 的 Traffic Class 字段，使用 6 位，范围是 0-63，使用区分服务代码点（DSCP）主要是用来流量分类和策略应用。

全局配置

QoS模式 ☒ 基于端口 ☐ 基于802.1P ☐ 基于DSCP

应用

基于端口设置

选择	端口	优先级
☐		0
☐	端口 1	7
☐	端口 2	7
☐	端口 3	0
☐	端口 4	0
☐	端口 5	0
☐	端口 6	0
☐	端口 7	0
☐	端口 8	0
☐	端口 9	0
☐	端口 10	0

应用

优先级队列映射

选择	优先级	队列
☐		Q0
☐	0	Q1
☐	1	Q0
☐	2	Q2
☐	3	Q3
☐	4	Q4
☐	5	Q5
☐	6	Q6
☐	7	Q7

应用

全局配置

QoS模式 ☐ 基于端口 ☒ 基于802.1P ☐ 基于DSCP

应用

优先级队列映射

选择	优先级	队列
☐		Q0
☐	0	Q1
☐	1	Q0
☐	2	Q2
☐	3	Q3
☐	4	Q4
☐	5	Q5
☐	6	Q6
☐	7	Q7

应用

全局配置

QoS模式 ☐ 基于端口 ☐ 基于802.1P ☒ 基于DSCP

应用

基于DSCP设置

选择	DSCP	优先级
☐		0
☐	0	0
☐	1	0
☐	2	0
☐	3	0
☐	4	0
☐	5	0
☐	6	0
☐	7	0
☐	8	0
☐	9	0
☐	10	0
☐	11	0
☐	12	0
☐	13	0
☐	14	0
☐	15	0

QoS 高级配置

QoS 模式：可根据需要选择基于端口模式、基于 802.1p 模式和 DSCP 模式

基于端口设置 - 优先级：设置端口优先级

优先级队列映射：优先级和队列进行映射，一般不更改

基于 DSCP 设置 - 优先级：DSCP 模式下进行优先级设置

5.5 安全功能

5.5.1 MAC 管理

MAC 管理功能包含三个功能，一个是对应端口的 MAC 地址数量限制功能，其次是 MAC 地址静态手动增加功能，最后是动态 MAC 地址表项情况，可以监测对应端口的 MAC 地址学习的情况，供设备的维护和检查用。

MAC 配置

端口号: 最大MAC数: (0-100, 0: 禁用)

端口	最大MAC数
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0

端口号: VID: MAC 地址:

序号	VID	MAC	端口	选中
----	-----	-----	----	----

当设置了对应端口的最大 MAC 数量之后，设备有限转发手动绑定的静态 MAC 地址，当静态 MAC 地址绑定数量小于最大 MAC 数，才会动态学习其他 MAC 地址。

MAC 配置

MAC 配置：可选择对应的端口号，进行最大 MAC 地址学习的限制

端口号+VLAN+MAC 地址：可设置对应端口的固定静态 MAC 地址手动添加

5.5.2 风暴抑制

广播风暴抑制功能，可以针对广播包、未知单播报文和未知组播报文在交换机的出入口上提供流量抑制的功能，当这些报文转发超过了限制的阈值后，系统将会丢弃多余的报文进行控制。

风暴抑制

端口	未知单播包		组播包		广播包	
	状态	速率 kbps	状态	速率 kbps	状态	速率 kbps
端口 1	禁用		禁用		禁用	
端口 2						
端口 3						
端口 4						

应用

端口	未知单播包		组播包		广播包	
	状态	速率	状态	速率	状态	速率
端口 1	禁用	0pps	禁用	0pps	禁用	0pps
端口 2	禁用	0pps	禁用	0pps	禁用	0pps
端口 3	禁用	0pps	禁用	0pps	禁用	0pps
端口 4	禁用	0pps	禁用	0pps	禁用	0pps
端口 5	禁用	0pps	禁用	0pps	禁用	0pps
端口 6	禁用	0pps	禁用	0pps	禁用	0pps
端口 7	禁用	0pps	禁用	0pps	禁用	0pps
端口 8	禁用	0pps	禁用	0pps	禁用	0pps
端口 9	禁用	0pps	禁用	0pps	禁用	0pps
端口 10	禁用	0pps	禁用	0pps	禁用	0pps

风暴抑制配置

端口：选择对应需要操作的端口，按住‘Ctrl’按键可以进行批量选择

状态：默认禁用，可以选择启用

抑制速率：可选单位 kbps 或者 pps，

5.5.3 流量监控

流量监控功能主要提供各个端口在实际运行过程中的发送/接收字节数以及发送/接收报文数的累计数值。

流量监控

端口	发送字节数	接收字节数	发送报文数	接收报文数
端口 1	0	0	0	0
端口 2	16719462	2101116	83772	8055
端口 3	0	0	0	0
端口 4	0	0	0	0
端口 5	0	0	0	0
端口 6	2872424	17487257	9477	88823
端口 7	5804200	41613438	16119	252494
端口 8	29907154	8990531	173565	27782
端口 9	0	0	0	0
端口 10	675698	0	3762	0

清除

5.5.4 线缆检测

提供设备上各个电接口的电缆状态情况

线缆检测

端口号: 7 测试

线对	电缆状态	电缆长度 (米)
A	正常	4.0
B	正常	3.2
C	正常	4.0
D	正常	3.2

5.5.5 DHCP 侦听

DHCP 侦听（DHCP Snooping）是一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器端获取 IP 地址，通过监听 DHCP 请求和响应来实现，防止非法 DHCP 服务器在网络中活动。

DHCP侦听

DHCP侦听: ☒ 启用 ☐ 禁用 应用

端口配置

端口	信任	Option 82	模式	电路ID自定义	电路ID子选项	远程ID自定义	远程ID子选项
端口1 端口2 端口3 端口4							

应用

端口	信任	Option 82	模式	电路ID自定义	电路ID子选项	远程ID自定义	远程ID子选项
端口1	禁用	禁用	保留	默认		MAC地址	
端口2	禁用	禁用	保留	默认		MAC地址	
端口3	禁用	禁用	保留	默认		MAC地址	
端口4	禁用	禁用	保留	默认		MAC地址	
端口5	禁用	禁用	保留	默认		MAC地址	
端口6	禁用	禁用	保留	默认		MAC地址	
端口7	禁用	禁用	保留	默认		MAC地址	
端口8	禁用	禁用	保留	默认		MAC地址	
端口9	禁用	禁用	保留	默认		MAC地址	
端口10	禁用	禁用	保留	默认		MAC地址	

DHCP 侦听配置

DHCP 侦听功能：默认禁用，可选择启用

端口：选择对应的侦听端口

信任：选择侦听端口配置信任

Option 82：增强服务子选项，主要用于中继代理功能

5.6 诊断工具

5.6.1 系统升级

设备提供系统升级功能，当需要系统升级操作时，请采用我司提供的正确的升级文件进行升级操作，选择文件后，点击应用即可。

系统升级

已经准备好升级软件？升级完成后需要重启。

未选中文件 选择文件 应用

5.6.2 Ping 工具

设备集成了基于 Ping 应用命令，可通过 ICMP 协议进行请求报文和显示应答报文情况，来达到测试目的站点是否可达并获取连接丢包率和平均往返时间等相关状态信息。

Ping 工具

主机名/IP地址	ping次数
	☒ 默认: 4
	☐ 用户自定义: 4 范围: 1 - 65535

开始ping 取消

主机地址	0.0.0.0
已发送	0
已接收	0
丢包率	0 %
最短	0 ms
最长	0 ms
平均	0 ms
状态	N/A

5.6.3 备份还原

设备提供了配置文件下载及配置文件上传功能，可通过该功能进行配置保存、配置修改后上传配置等应用操作。

系统配置备份

点击配置备份按钮，备份上一次保存的配置。
建议在备份前先保存当前配置。

配置备份

系统配置还原

选择一个备份配置文件然后点击恢复配置按钮，紧接着
你可以恢复交换机到它之前的配置。

配置文件:

5.6.4 系统恢复

恢复出厂默认配置操作，请谨慎操作，避免造成不必要的配置丢失等情况发生，建议恢复出厂设置操作之前，请先进行配置保存操作。

系统恢复

恢复到出厂设置并重启系统。

复位

5.6.5 配置保存

所有的功能配置修改，均需要在设备断电前进行配置保存操作。

配置保存

点击保存按钮，将保存在此设备中所做的所有更改

保存

5.6.6 系统重启

设备重启功能，请注意，在设备重启操作之前，请确认设备配置是否已经进行保存，避免引起不必要的配置丢失情况的发生。

系统重启

请点击重启按钮来重新启动设备

重启

6. 设备 Console 端口使用

本交换机提供了 Console 接口，提供交换机简单维护和查询功能，主要应用于以下情况：

当交换机 IP 地址遗忘，可以通过 Console 端口进行查询；

如下图所示：

```
Username:admin
Password:*****
Login successful. welcome!

switch> help
help: Lists all the registered commands
debug: enter debug shell mode
tftp-fw-upgrade <server-ip> <firmware-name>: upgrade image using TFTP
reset: reset system

switch> █

debug#help
help: Lists all the registered commands
memr1 address: read 4 bytes from register or memory at the address
memw1 address value: write 4-byte value to register or memory at the address
ip_get: Show IP address
sysmac_get: Show System mac
model_get: Show Model string
```

Console 端口功能

Switch>help : 列出所有可操作命令

Switch>debug : 调试命令，可提供 IP 地址查询和 MAC 地址查询功能

Switch>tftp-fw-upgrade : 系统升级

Switch>reset : 软重启命令

debug>help : 列出所有可操作命令

debug>ip_get : 获取设备 IP 地址，通常在忘记 IP 地址的时候操作

debug>sysmac_get : 获取设备 MAC 地址