NLDK7710

网管型卡轨式工业以太网交换机

用户手册

- **wring**
- **VLAN**
- **Trunk**
- **QoS**
- **IGMP Snooping**
- 速率控制
- **SNMP**
- 诊断功能
- 继电器告警
- Log 日志
- 在线系统更新

上海纽琳克通信技术有限公司

版本号：**V2.0**

商标

KNEWLINK 是上海纽琳克通信技术有限公司品牌专用商标。

wring 是上海纽琳克通信技术有限公司链路冗余及自恢复技术专用商标。

Microsoft 和 **Windows** 是微软公司的注册商标。

本操作手册中所提到的所有相关商标分别属于相关的制造商所有。

说明

此用户手册适用于 NLDK7710 网管型卡轨式工业以太网交换机。

在使用本手册之前，请您认真阅读以下使用许可协议。只有在同意以下使用许可协议的情况下方能使用本手册中介绍的产品。

重要声明

本公司在本手册中提供的任何信息，并不代表对这些信息提供了相应的授权。

本公司努力使本手册中提供的信息准确和适用，然而本公司并不对这些信息的使用承担任何责任，也不对这些信息的使用承担任何连带责任。产品及使用手册可能包含技术或印刷上的错误。本公司保留在不事先通知情况下更改本使用手册全部或部分内容的权力。

声明：

由于产品和技术的不断更新、完善，本资料中的内容可能与实际产品不完全相符，敬请谅解。如需查询产品的更新情况，请查询本公司网站或直接与本公司业务代表联系。

修订历史：

版本号	日期	原因
V1.0	2014.06	创建文档
V2.0	2015.06	产品升级

安全使用须知

本产品在设计使用范围内具有良好可靠的性能，但需要避免人为对设备造成的损害或破坏。

- 仔细阅读本手册，并保存好本手册，以备将来参考用
- 不要将设备放置在接近水源或潮湿的地方
- 不要在电源电缆上放任何东西，应将其放在碰不到的地方
- 为避免引起火灾, 不要将电缆打结或包住
- 电源接头以及其他设备连接件应互相连接牢固，请经常检查
- 请注意保持光纤插座和插头的清洁。设备工作时，不要直视光纤断面
- 请注意设备清洁，必要时可用软棉布擦拭
- 请不要自己修理设备，除手册中有明确指示外

在下列情况下，请立即断开电源，并与我公司联系。

- 设备进水
- 设备摔坏
- 设备工作异常或展示的性能已完全改变
- 设备产生气味、烟雾或噪音

：在使用本网管软件过程中必要的解释信息

：在使用本网管软件需要特别注意的事项

目　录

第一章　系统概述

1.1 产品简介

上海纽琳克通信技术有限公司网管型卡轨式工业以太网交换机，是专为工业高速通信网络应用而设计开发的。此交换机为灵活多变的工业应用需求提供了一种高端工业以太网通信解决方案，突破了 100M 的主干网络通信瓶颈，使工业通信更加顺畅、更加可靠、更加快速，满足客户为提高附加值应用而不断创新的需求。

本交换机可以用于即插即用的简单应用方式，也可以用于复杂的网络管理的方式，满足用户多方面的需求。所有的电口均支持自动协商、10/100Mbps 全双工和半双工、流量控制、Auto-MDI/MDI-X 等功能。通过 Web 管理或 SNMP 网管，本交换机可提供高级管理功能，例如：WING、虚拟局域网、Trunk、服务质量 （Quality of Service）、IGMP Snooping、速率控制、端口镜像、静态 MAC 地址转发表、诊断功能、Email/Relay 故障报警和固件在线升级等一系列的常用高级管理功能。

WING 技术是由上海纽琳克通信技术有限公司为工业应用而设计开发的，它提供以太网通信链路断开后快速自恢复功能，其恢复时间低于 20 毫秒。本交换机可使用普通百兆或千兆口进行组环，以提供更快的恢复速率和通信带宽。WING 技术能够提供链路冗余备份的以太网络。

NLDK7710 网管型卡轨式工业以太网交换机有 8 个百兆、2 个千兆共 10 个端口。每个千兆端口均支持 SFP 光口模块，产品支持 802.1Q 的 VLAN，支持步长最小为 64K 的端口限速，交换带宽是 5.6G，支持 8K 条目的 MAC 地址表。

1.2 特性

1.2.1 工业网络性能

- 支持 8 路百兆和 2 路千兆以太网接口
- 支持 1 路可配置告警输出
- 基于 WING 技术的链路冗余自恢复技术，自愈时间<20ms
- 内嵌 Web 服务器，可通过浏览器远程管理和配置
- Trunk 端口汇聚
- 实时广播风暴监测控制（包括广播，多播，未知单播等风暴类型检测）
- 在线固件更新
- 动态 IGMP Snooping 支持，过滤多播流量
- 存储转发机制，交换带宽为 5.6Gbps
- 百兆电口 10/100M 自适应，全/半双工，MDI/MDIX 自适应模式

- 全双工流控和半双工背压流量控制
- 端口 VLAN 和 IEEE 802.1Q VLAN
- 支持 QoS，IEEE802.1p 和 ToS/DiffServe，提高通信质量
- 支持 SNMP V1/V2C 不同等级的网络管理
- 支持 RMON 和私有 MIB，有效的远程数据监控和预测能力
- 满足强电磁干扰环境下无故障工作的要求

1.2.2 工业应用设计

- 带宽管理，阻止不可预知的网络问题
- 系统配置参数备份与恢复
- 友好的图形接口，一键恢复出厂设置
- 端口镜像，用于在线调试
- 有效的网络诊断工具
- 掉线、风暴报警
- 端口换线连接快速恢复
- 实时网络时间同步
- 限制可访问 IP，管理网络中的交换机
- 卡轨安装
- 环网指示灯

1.2.3 远程管理配置

- 可使用 Web 页面、控制台程序和 Windows 应用程序进行管理配置
- 支持标准的 SNMP 协议管理

1.3 包装清单

本交换机包装清单如表 1-1 所示，所列物件中的任何一项丢失或被毁坏，请联系代理商或上海纽琳克通信技术有限公司客服中心，由他们协助您更换或补足。

表 1- 1　产品包装清单表

项　目	数　量
NLDK7710 网管型卡轨式工业以太网交换机	1
用户手册	1
RS-232 串口线缆	1
产品合格证与保修卡	1

1.4 性能规格

本交换机能够完成以太网信息交换，用户必须参考以下的数据进行合理选型和使用，才能使其表现出良好的工业特性和优良的网络信息交换能力。

技术指标：

IEEE 标准：802.3、802.3u、802.3z、802.3x、802.1p、802.1Q、802.1d/w

交换方式：存储转发

交换带宽：最大 5.6Gbps

流量控制：全双工流控，半双工背压控制

MAC 地址：8K

传输距离：双绞线 100m，千兆光纤最大 20km，百兆光纤最大 40km

管理方式：Web 管理和 SNMP

冗余恢复 ：恢复时间小于 20ms

广播风暴：实时广播风暴监测告警与控制

固件升级：Web 在线升级

管理功能：系统信息设置、Port-based VLAN（27 条）和 802.1Q VLAN（4K 条）、Trunk（5 组）、QoS, 802.1p/1Q and ToS/DiffServe、IGMP Snooping、广播风暴控制、速率限制、端口镜像、静态 MAC 地址转发（包括单播地址和多播地址）、SNMP V1/V2C

诊断功能：掉线掉电风暴报警、数据流量统计表、Log 日志

EMC 标准：

IEC61000-4-2 防静电（ESD）：±8 kV 接触放电，±15 kV 空气放电

IEC61000-4-3 电磁场（RS）：10V/m（80-1000MHz）

IEC61000-4-4 电快速瞬变脉冲群（EFT）：电源端口--±4 kV，数据端口--±2 kV

IEC61000-4-5 浪涌(Surge) ： ±2 kV(差模)，±4 kV(共模)

IEC61000-4-6 射频传导(CS)：3 V（10kHz~150 kHz），10V（150kHz~80 MHz）

IEC61000-4-8 工频磁场：100A/m

IEC61000-4-10 阻尼振荡磁场：10A/m

EN55022：EN55022 Class A

电气特性和环境参数：

表 1- 2 NLDK7710 产品电气特性和环境参数

电气特性				环境参数		
输入	电压	最大功率	频率	操作温度	存储温度	湿度
DC	12V	<10W	N/A	-40℃～85℃	-40℃～85℃	5～95%
	24V					
	48V					
AC	220V					

产品选型：

表 1- 3　NLDK7710 产品可选型号及对应的接口

可选型号	千兆光口	百兆光口	百兆电口	串口
NLDK7710-2GX	2	/	8	/
NLDK7710-2GX-2F	2	2	6	/
NLDK7710-2GX-4F	2	4	4	/
NLDK7710-2GX-8F	2	8	/	/
可选电源	**百兆光口参数选型**			
DC12	**模式**	**接头**	**传输距离**	
DC24	多模	SC/ST/FC	1310nm, 2km	
DC48	单模	ST/ST/FC	1550nm, 80km	
AC220	/	/	/	

第二章　产品外观及硬件安装

2.1 产品外观

2.1.1 NLDK7710 产品外观图

本系列产品机箱为卡轨式结构。整机采用六面全封闭结构。机箱的左、右侧板为单肋形铝型材制作，是整机散热系统的一部分。摒弃了传统的流风机散热形式，降低整机功耗的同时也提高了系统的稳定性。

外形如图 2-1，尺寸为：182 mm×62 mm×128.4mm。

图 2-1　NLDK7710 产品外观图

本系列交换机面板指示灯指示了交换机当前工作状态。具体说明如下表 2-1 所示。

表 2-1　前面板指示灯描述

功能	LED	条件	状态
电源指示灯	PWR1	亮	电源 1 连接并供电正常
		灭	电源 1 未连接或供电不正常
	PWR2	亮	电源 2 连接并供电正常
		灭	电源 2 未连接或供电不正常
运行指示灯	RUN	亮	系统运行异常
		闪烁	系统运行正常
		灭	系统未启动
环网状态指示灯	RING	亮	快速环网功能启用并成环
		闪烁	快速环网功能启用但未成环
		灭	快速环网功能禁用
百兆光口 Link/Act 指示灯	LINK7/8	亮	端口连接
		闪烁	端口有网络活动
百兆光口 Link/Act 指示灯	G1/G2	亮	端口连接
		闪烁	端口有网络活动
电口状态指示灯	L/A	灭	端口无连接
		亮	端口连接
		闪烁	端口有网络活动
	100M	亮	100M 连接
		灭	无连接或者 10M 连接

2. 2 各接口定义及描述

2.2.1 千兆光纤接口

SFP 千兆光纤接口

本产品具有 2 个 1000Base-LX 的全双工单模/多模光纤接口，端口号为 SFP1，SFP2，采用 SFP 热插拔器件，光纤接口采用 LC 接口，如图 2-2 所示。光纤接口需成对使用（TX 和 RX 为一对），TX 口为光发端，连接另一个远程交换机光接口的光收端 RX；RX 口为光收端，连接同一个远程交换机同一个光接口的光发端 TX 。利用 2 个冗余的 1000Base-LX 光纤接口可以组成光纤冗余环网，在系统出现故障时环网冗余倒换时间小于 20ms，可以有效提高网络运行的可靠性。

图 2-2　SFP 的光模块图

SFP 模块的热插拔步骤如下，示意图如图 2-3 所示。

热插步骤：

SFP 期间，观察有 PCB 金手指的一端。将金手指端插入 SFP 的金属屏蔽笼，听到咔的声音说明器件已经插到位，再将 SFP 的插拔拉手，放到接口平行的正常位置上，即可使用。

热拔步骤：

先将 SFP 的插拔拉手拨下与接口垂直，此时光器件应与 SFP 屏蔽笼的挂接钩脱开。将 SFP 模块平行拔出。

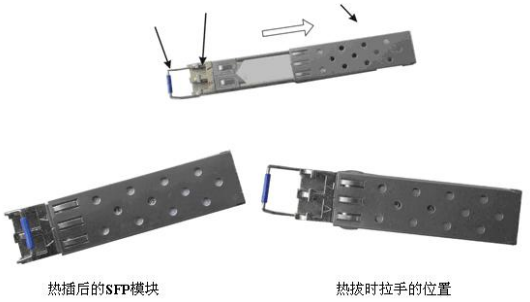


图 2-3　SFP 模块的热插拔示意图

2.2.2 百兆光纤接口

本产品可选多个 100Base-FX 全双工的单模或多模光纤接口，连接器可选 SC、ST 或 FC。光纤接口需成对使用（TX 和 RX 为一对），TX 口为光发端，连接另一个远程交换机光接口的光收端 RX；RX 口为光收端，连接同一个远程交换机同一个光接口的光发端 TX。

百兆光接口主要有：SC、ST、FC。如图 2-4 所示。

图 2-4　SC/ST/FC 接口光模块图

2.2.3 以太网 RJ45 接口

本产品可选多个以太网 RJ45 端口，每个 RJ45 端口都具有 10Base-T/100Base-TX 自适应功能，支持自动 MDI/MDI-X 连接。可直接将交换机连接到终端设备、服务器、集线器或其他交换机。每个端口都支持 IEEE802.3x 自适应，因此最适宜的传输模式（半双工或全双

工）和数据速率（10Mbps 或 100Mbps）都能被自动选择（所连设备必须也支持这个特性）。如果连接到这些端口的设备不支持自适应，那么端口将强制自己用与对方相同的速率工作，避免全/半双工不匹配，传输模式将默认为半双工，流控也会被自动禁止。

2.2.4 电源输入端子

本系列交换机产品标准配置使用双路直流 12/24/48V 电源供电，用 5.08mm 间距端子连接电源输入，如图 2-5 所示，整机功耗小于 10W。

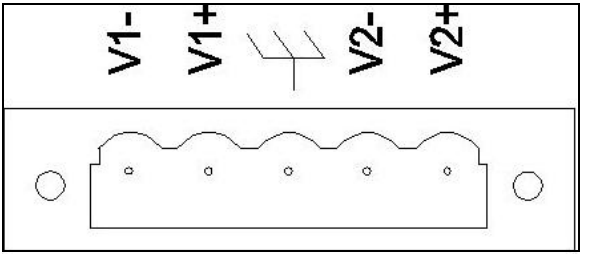


图 2-5　电源输入端子示意图

注意：

本设备支持的电源规格为 12VDC、24VDC、48VDC，与电源连接前，请确认电源供电与设备所标识的供电要求是否相符，以免损坏设备。

2.2.5 告警继电器

本系列交换机告警继电器，接线端子采用 2 位 3.81mm 间距端子。如图 2-6 所示，此继电器为常开继电器。当交换机正常工作时，继电器触点通电断开。当端口 link down 和出现网络风暴时，继电器掉电闭合。继电器推荐开关负载能力为 1A（24VDC）。

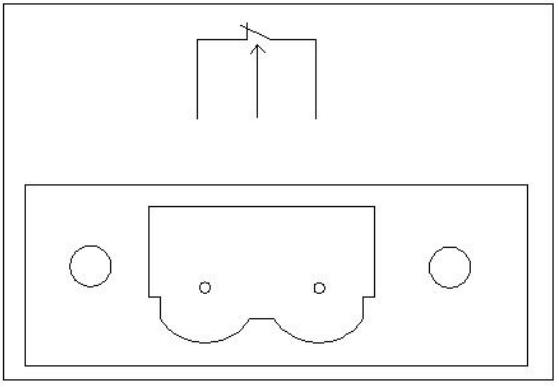


图 2-6 告警继电器示意图

2.2.6 串口网管口（CONSOLE）

网管口是一个 RJ45 的接口，如图 2-7 所示。请使用本公司提供的串口延长线连接到 PC 的串口。接口通信标准为 3 线制 RS-232。

串口的通信参数如下：波特率：9600，数据位：8，校验位：none，停止位：1，流控：none

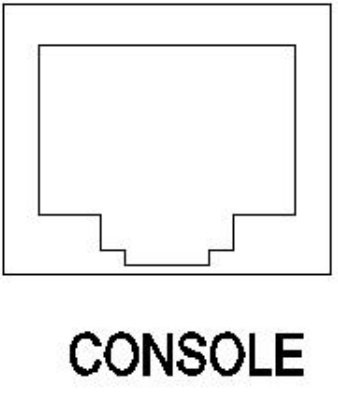


图 2-7 RJ45 接口的串口示意图

2.3 硬件安装

2.3.1 安装要求

本工业以太网交换机为一单体结构，可直接卡装到卡轨上。安装之前，要首先确认有合适的工作环境，包括电源需求、充分的空间、是否接近其他将要连接的网络设备及其他设备是否到位。

请确认如下安装要求：

- 电源要求：标准产品使用冗余 DC24V 电源供电，其他供电方式请参考产品标签、外壳上的电源标注以及相关说明书。
- 环境要求：温度-40℃～+85℃，相对湿度 5～95%（无凝露）。
- 接地电阻要求：<5Ω 。
- 根据合同配置要求，检查光缆铺设是否到位，光纤接头是否合适。
- 避免阳光直射，远离发热源或有强烈电磁干扰区域。
- 标准产品安装在卡轨上，检查是否有安装所需的电缆和接头。

注意

在安装或连接以太网交换机前必须确保断开电源线。计算每条电源线以及公共线中的最大可能电流，观察所有的电气信息，以获知不同宽度的线所允许的最大电流。如果电流超过最大额定电流，会使导线过热，对设备造成严重损坏。

同时还必须注意以下事项：

把电源线和设备线的路径分隔开来，如果两者路径必须交叉，必须确使这些线在交叉点是垂直的。不能把信号线或者通信线和电源线铺设在同一管道内，为避免干扰，不同信号特征的线应分隔开来。我们可以利用在一根线中传输的信号的类型来决定哪些线应该分隔开来。

拇指法则就是具有相同电气特性的线可以捆束在一起。把输入线和输出线分隔开来。强烈建议在必要的时候对系统内的所有设备线都做上标签。

交换机要接保护地：

接地和布线能有效的抑制由于电磁干扰带来的噪声影响。在连接设备前应该进行接地连接，从接地螺钉连到接地表面。

2.3.2 主机安装

卡轨式安装

从包装箱中取出设备时，交换机的后面板上应该已经固定好 DIN 卡轨的连接座。如果交换机需要卡装在 DIN 轨上，则在安装之前应该检查 DIN 轨的安装情况。主要包括以下两项内容：

（1）DIN 轨是否固定结实，DIN 轨上是否有足够的空间用于安装交换机。

（2）DIN 轨上是否有适合交换机工作的电源引入。

选定好交换机的安装位置后，按如下步骤将交换机安装到 DIN 轨上：

（1）将 DIN 轨的上部插入 DIN 卡轨连接座上部有卡簧的卡槽内。在交换机的上面板向下稍微用力并如图 2-8 中的 A 所示转动设备。

（2）如图 2-8 中的 B 所示，将 DIN 轨卡入 DIN 卡轨连接座，确认交换机设备可靠地安装到 DIN 轨上。

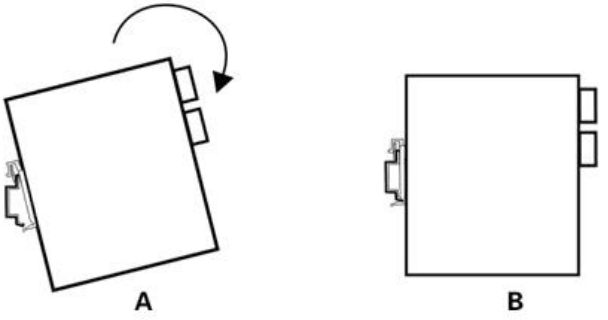


图 2-8　交换机的 DIN 导轨安装示意图

2.3.3 电缆连接

正确安装后，即可进行电缆的安装连接，主要包括以下接口的电缆连接。

- 业务接口

本产品提供的终端设备的百兆电口为 10Base-T/100Base-TX 以太网 RJ45 接口。使用直连网线与终端设备相连，使用交叉网线与网络设备相连。

- 连接网管口

本产品的 CONSOLE 口可与控制计算机的串口相连。

- 连接电源

当所有其他电缆连接完成后，即可连接产品标识规格的电源。

2.3.4 光纤连接

本产品提供 100Base-FX 的单模或多模光纤接口和 1000Base-LX 的单模/多模光纤接口，光纤接口的类型可根据要求选择 SC、ST、FC 或 LC。

注意

此交换机使用激光在光纤线缆上传输信号。激光符合 1 级激光产品的要求，常规操作对眼睛无害。但是设备通电时，切勿直视光传输端口和光纤终结器端面。

连接可插入光纤模块的步骤如下：

（1）除去并保留 LC、SC 或 FC 端口的橡皮套。不使用时，套上橡皮套以保护光纤终结器。

（2）检查光纤终结器是否干净。将干净的纸巾或棉球稍稍蘸湿，轻轻擦拭线缆插头。弄脏的光纤终结器会降低光传输的质量，使端口性能受到影响。

（3）将光缆的一端连接到交换机的光纤接口，另一端连到另一台设备的光纤接口。

（4）连接完成后，请检验交换机前面板对应的光口 LINK 指示灯，如果指示灯已亮，说明连接有效。

2.3.5 布放线缆

线缆的布放要符合以下条件：

（1）电缆布放前须核对所有电缆的规格，型号和数量是否和施工图设计及合同要求相符；

（2）电缆布放前需检查电缆是否有破损，是否有出厂记录和质量保证等证明其质量的凭证；

（3）所需布放线缆的规格，数量，路由走向，布放位置等，均应符合施工图设计要求，每条线缆的布线长度应根据实际位置而定；

（4）用户电缆与电源线分开布放；

（5）所布放线缆中间不得有断线，或中间有接头；

（6）线缆在走道内应顺直排放整齐，拐弯均匀、圆滑、平直；

（7）线缆在槽道中，应顺直，不得越出槽道，挡住其他进出线孔，在线缆出槽道部位或线缆拐弯处应予以绑扎、固定；

（8）电缆、电源线、地线同槽布放时，电缆、电源线和地线不能交迭，混放。线缆过长时，必须将线缆规整地盘放在走线架中间，不能压在其他线缆上；

（9）尾纤布放时，要防止光缆打结并应尽量减少转弯处，且转弯半径不能太小。绑扎应松紧适度，不得过紧。在走线架上布放时，应和其他线缆分开放置；

（10）线缆两端应有相应标识，标识内容简洁明了，便于维护。

注意

布放尾纤时，要防止光缆打结并应尽量减少转弯处，且转弯半径不能太小，转弯半径过小会导致链路光信号的严重损耗。影响通信的质量。

第三章　通过串口控制台配置基本参数

交换机可以通过 Web 来访问、配置和管理。在进行具体操作之前，必须保证访问的 http 客户网络设备能与被访问的交换机在同一网段内，交换机出厂时的默认 IP 地址为 192.168.16.253，用户可以通过 windows 的超级终端访问 console 接口或通过以太网连接访问 Web 网管来设置交换机的 IP 地址。

3.1 通过超级终端设置千兆工业以太网交换机的 IP 地址

将本交换机的 console 接口通过一根本公司的随机提供的串口线连接到 PC 的串口，然后从 PC 里打开超级终端，Windows 用户可以从：

开始→程序→附件→通信

找到超级终端。打开超级终端时你将需要创建一个新的连接，然后必须选择与交换机相连接的通信端口，使用下面的配置参数：

波特率：9600， 数据位：8， 校验位：none， 停止位：1， 流控：none

3.1.1 用户和密码

超级终端配置好后，敲击回车键，可以看到如图 3-1 显示的画面。

图 3-1　用户和密码设置界面图

输入用户名和密码，默认的用户名和密码都是：admin，每行输入完毕后均按回车键，

登录成功后即进入控制台程序。

3.1.2 控制台菜单

控制台菜单包括：1 基本信息，2 IP 设置，3 恢复厂家默认值，4 返回登录界面四项功能，如图 3-2 所示。移动键盘向上的“↑”箭头或“↓”箭头，进行选择，按回车键进入子功能模块。

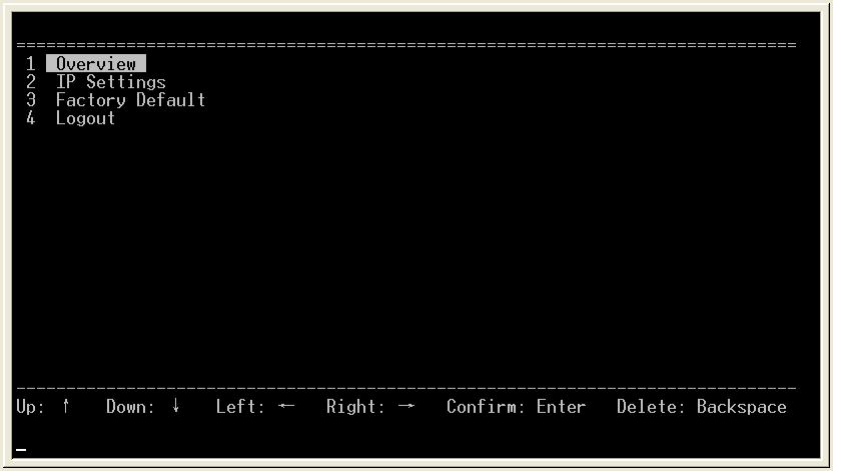


图 3-2　控制台菜单界面图

Overview：基本信息，即查看系统基本信息。

IP Settings：IP 设置，可使用 DHCP 自动分配一个 IP 地址，也可指定一个静态 IP 地址。

Factory Default：恢复出厂默认值。

Logout：返回登录界面，即退出控制台程序到登录界面。

3.1.3 基本信息（Overview）

在基本信息这个子项里可以看到这个交换机相关的一些系统信息，如：设备名称、设备描述、IP 地址、MAC 地址、固件版本等。详情如图 3-3 所示。

图 3-3 基本信息界面图

Device Name：设备名称，用户可以通过 Web 网管修改。

Device Description：设备描述，即设备型号，不同的型号此项内容不相同，用户不能修改。

Device IP Address：设备 IP 地址，用户可修改。

Device MAC Address：设备 MAC 地址，用户不可修改。

Firmware Version：设备固件版本，用户不可修改。

Press any key to continue：按任意键返回控制台主菜单界面。

3.1.4 IP 设置（IP Settings）

通过控制台程序设置 IP 地址时，选择“IP Settings”，弹出如图 3-4 画面。

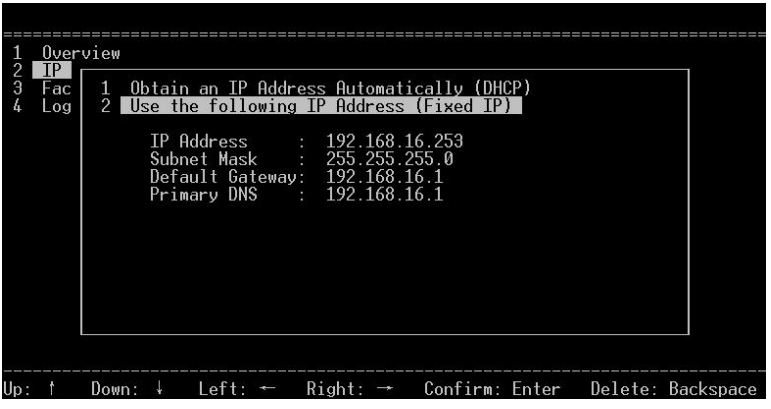


图 3-4 IP 设置界面图

对交换机设置一个新的 IP 地址。当选择“Obtain an IP Address Automatically (DHCP)”时，本交换机将通过 DHCP 的方式，由 DHCP 服务器自动分配一个 IP 地址；当选择“Use the following IP Address (Fixed IP)”时，可以编辑 IP 地址（IP Address）、子网掩码（Subnet Mask）、默认网关（Default Gateway）、DNS 服务器（Primary DNS）四项来设定一个固定的网络参数。

IP 地址应当与网关在同一网段中，访问 Web 网管的网络设备的 ip 地址也应在同一网段内。设置 IP 地址等网络参数时应该询问网管，以免设置不当造成 Web 网管无法登录。IP 地址设置好后，可以使用该 IP 地址访问交换机的 Web 页面。

3.1.5 恢复出厂值（Factory Default）

这个功能将恢复所有配置参数到出厂值。

注意

恢复成功后，交换机会自动的软件重启，但是仍然建议用户重上电一次交换机以清除 ram 中的内容。恢复到出厂配置后，请注意此时的 IP 地址为 192.168.16.253，用户可能需要修改相应网络参数才能访问 Web 网管。

3.1.6 退出控制台程序（Logout）

这个功能将退出交换机控制台程序。为了防止不经意的修改了交换机某些核心功能，控制台程序退出后只是重新回到其登录界面，而不会真正的退出此控制台程序，从而进入交换机的后台操作系统命令行界面。

第四章　WEB 管理功能

说明

以下所有功能的界面、配置皆以实物为准。

本交换机内置有 Web 服务器，为访问和配置交换机提供了一种便利的方式。用户可以使用 IE、Firefox 或谷歌浏览器来访问交换机。

通过 Web 来访问本模块模块，交换机和 PC 的 IP 必须在同一个网段中。修改 PC 的 IP 地址，确保它和交换机的 IP 同在一个局域网络中，Windows 用户请参考如下的操作步骤：

开始→控制面板→网络和 Internet 连接→网络连接→本地连接→属性→Internet 协议（TCP/IP）

上海纽琳克通信技术有限公司智能型千兆工业以太网交换机默认的 IP 地址是：192.168.16.253。设置 PC 的 IP 地址为：192.168.16.X（X 是除 253 外，1 到 254 中的任一值）。

具体的 Windows 系统操作页面如图 4-1 所示。

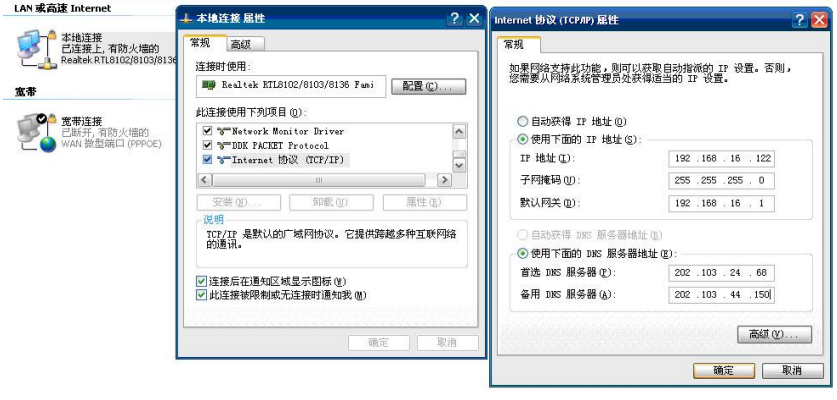


图 4-1　Windows 环境下的 IP 设置界面图

更改 PC 的 IP 地址后，便可用默认的 IP 地址：192.168.16.253，通过 Web 访问该千兆工业以太网交换机并对其进行相关的配置操作。

4.1 登录到 WEB

打开浏览器，在地址栏里输入本交换机的默认 IP 地址，如图 4-2 所示。

图 4-2　在地址栏输入 IP 地址界面图

敲击回车键之后，弹出如图 4-3 窗体，提示用户输入用户名和密码。

图 4-3　输入用户名和密码界面图

默认的用户名和密码都是“admin”。如果用户名或密码输入不正确，该智能型千兆工业以太网交换机的 WebServer 将提供三次机会输入用户名和密码，如果三次输入错误，浏览器显示“401 Unauthorized”错误信息，出现错误信息后需重新输入交换机 IP 地址。输入正确的用户名和密码，认证成功后即进入 Web 服务器的主页面，如图 4-4 所示。

图 4-4　Web 服务器的主界面图

注意

1. 用户可以使用 IE、Firefox、谷歌等浏览器来访问 Web 服务器，不同的浏览器显示的页面可能会有所不同，如果影响到正常使用，请更换为主流的浏览器，如 IE、Firefox、谷歌；
2. 本交换机用 IE、Firefox、谷歌主流浏览器进行过大量测试，都能正常使用，只是升级内核程序时建议使用 IE 浏览器，以免使用其他浏览器出现问题。

4.2 系统状态

4.2.1 设备信息

设备信息包括交换机名称、编号、描述、IP 地址、MAC 地址、硬件版本、软件版本等。页面如图 4-5 所示。

图 4-5 设备信息图

设备名称：为标示网络中的交换机类型名称（可以由用户修改）。

设备编号：描述交换机厂家设定的编号。

设备描述：对交换机进行一个概要描述，比如 NLDK7710 表示交换机有 10 个端口，其中有 8 个百兆口，2 个千兆口。

出厂 IP：交换机恢复出厂设置之后的 IP 地址。

MAC 地址：本交换机网管系统的 MAC 地址。

硬件版本：交换机当前的硬件版本。

软件版本：交换机当前安装的固件版本。

当前时间：交换机当前时间，当交换机刚上电时，为 1970 年的 linux 时间，用户可以修改，如启用了 ntp，交换机可以连接到互联网时，会自动与时钟服务器同步。

运行时间：从交换机上电算起，运行计时。当交换机被复位或断电重启时，这个时间也将从零开始重计。

4.2.2 设备状态

设备状态中，以绿色的条格表示了系统内存和 CPU 的使用率，如图 4-6 所示。此值的变化必须手动刷新本页面才能看到。

图 4-6　设备状态图

内存利用率：交换机设备内部的 CPU 扩展有外部 SDRAM，内存使用率反映了 CPU 使用了多少外部的 SDRAM。

CPU 利用率：交换机设备内部有一个高性能的 CPU，CPU 使用率反映了 CPU 的繁忙程度。

4.2.3 端口信息

对于不同的交换机型号，端口总数不同，对于 MIGE7100S 工业以太网交换机，端口信息显示了 1~8 个百兆口和千兆口 G1、G2。当端口连接正常时，端口号背景色显示为绿色，连接不好或者没有连接时背景色为白色，如图 4-7 所示。每当端口有新的连接状态变化必须手动刷新本页面才能看到。

图 4-7　端口信息图

4.2.4 菜单与辅助功能

网页上的菜单名称分别为系统状态，端口配置，二层特性，链路备份，访问控制，远程监控，端口统计，网络诊断，系统管理。如图 4-8 所示。

图 4-8　WEB 菜单界面图

其功能如表 4-1 所示。

表 4-1　菜单功能描述表

菜单项	页签	页面功能
系统状态	设备信息	设备信息，如：名称，编号，软件版本、IP 地址等
	设备状态	设备运行情况，如：CPU 使用率等
	端口信息	端口状态，如：数量，端口类型等
端口配置	端口设置	配置交换机各端口基本信息，如：速率模式、流控状态等
	速率设置	对交换机出入的数据类型和各端口进行速率控制管理
二层特性	QoS	设置 802.1p，端口优先级，DSCP 优先级等
	VLAN	显示 802.1Q VLAN 和端口 VLAN 的列表并可进行配置和管理，在 802.1Q VLAN 高级设置里有 VLAN TRUNK
	IGMP 侦听	设置 IGMP MAC 地址及其对应的端口
	静态组播	设置静态组播 MAC 地址及其对应的端口
链路备份	快速环网	设置快速环网端口及环网类型
	端口汇聚	设置端口的汇聚组
	快速生成树	设置快速生成树的详细信息
访问控制	用户密码	对用户权限和密码的管理
	登录控制	修改系统的防火墙来限制访问的客户端 IP 地址
	端口认证	实现业务与认证的分离
	认证数据库	对数据库中保存的用户名和密码进行增删
	MAC 端口锁定	可设置将某一 MAC 地址与某一端口绑定
监控报警	SNMP	提供 SNMP 代理来管理交换机设备
	Email 日志	电子邮件的形式周期性的给用户指定邮箱发送系统日志
	继电器告警	设置网络风暴告警及端口掉线告警
端口统计	接收帧统计	各端口接收的帧的统计，如单播，多播等
	发送帧统计	各端口发送的帧的统计，如单播，多播等
	总流量统计	各端口出入的帧的统计，如单播，多播等
	MAC 地址表	显示 MAC 地址情况
网络诊断	端口镜像	设置镜像端口和采集端口
	网络诊断	网络故障分析、网络测试或问题解决
系统管理	时间配置	设置系统时间等
	设置地址	对 IP 地址进行设置
	系统信息	设备型号，CPU 等相关参数设置或查看
	日志信息	显示日志信息，并可对其进行管理
	文件管理	进行交换机软件升级，获取、保存或恢复交换机的设置

菜单的右下方是帮助链接，在任一页面点击 帮助 就会弹出当前页面功能的帮助页面，如图 4-9 所示。

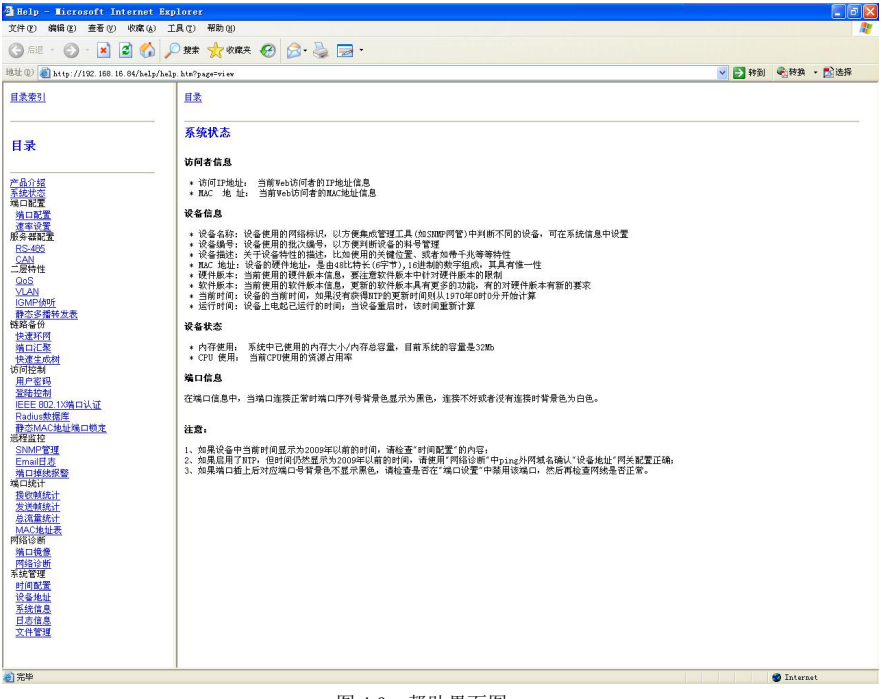


图 4-9　帮助界面图

每个页面的右上角都有 退出 × 链接，在任何时候用户都可以单击 退出 × 以退出登录，点击 退出 × 显示如图 4-10 所示页面。

图 4-10　退出登录界面图

单击 重新登录 按钮即会重新进入登录认证窗口。

菜单的右上方是 访问IP地址：192.168.16.60 MAC地址：00:e0:1c:3b:e7:62，显示的是访问交换机 Web 服务器的当前 PC 的 IP 地址和 MAC 地址。

4. 3 端口配置

端口配置包含两个子菜单：端口设置，速率设置。

4.3.1 端口设置

端口设置页面如图 4-11 所示。

图 4-11　端口设置界面图

图中的端口设置为默认配置，每个配置项目的说明如下：

端口号：显示本交换机的所有端口，如图所示共有 10 个端口。

接口类型：显示每个通信接口的媒体类型，如：RJ45 端口或光纤接口，上图中的电口和光口只与通信媒介有关，而与接口种类无关。G1，G2 是千兆光纤接口。

速率模式：是个多选一按钮，包括自动协商、十兆速率、百兆速率三种方式，自动协商是默认方式，允许通信接口使用 IEEE 802.3u 协议和相连的设备进行协商，协商结果将选择最好的速率进行通信，十兆和百兆方式为强制方式，即强制该端口以相应速率进行通讯。自动协商模式为默认模式，此时相连的网络设备也应采用自动协商模式，否则自动协商失败交换机会将端口设成默认的半双工模式，从而可能造成通信问题。

双工模式：有两个选项，全双工和半双工，只在强制速率模式下启用，当自动协商时不起作用。

端口启用：选中后将端口启用，不选则将这个端口禁用。

流量控制：在计算机网络，流控是用来处理两个传输节点之间的数据传输速率管理的，两节点都必须支持流控机制才能发挥它的作用，如果相连网络设备不支持流控机制，建议用户关闭此功能，因为过多的 pause 帧或冲突信号可能会造成通信问题。当数据流受到阻塞时，流控机制表现得相当明显。流控机制可以被启用或禁止，默认为启用。

极线变换：MDI（Medium Dependent Interface），MDIX（“X”是交叉线的意思），它是以太网口连接到路由器、HUB、交换机的接线方式。该交换机仅使用 Auto-MDI/MDIX，具备自动翻转功能，此选项用户不用更改。

关于端口配置，简单总结如表 4-2 所示。

表 4-2　端口配置信息

设置项目	描　述	默认值
接口类型	媒体接口类型，RJ45端口或光纤接口	由出厂设置
速率模式	两个网络节点之间的传输模式	自动协商
双工模式	两个端口之间的传输模式	全双工
流量控制	两个网络节点之间数据传输管理	使能
极线变换	媒体接口接线类型	自动翻转
端口启用	启用端口配置	启用

本交换机提供 Web 页面来配置，在点击 设置 按钮之后本页面的设置参数才会提交至交换机，在此之前退出本页面，则用户所作的任何修改都被取消。点击 取消 按钮即不提交用户所作的修改，并将设置还原成修改前的配置。

以下除特别的几个，其他相同，即都在点击后 设置 才保存设置。

1. G1，G2 口是千兆光口；
2. 光口不支持自动协商机制，全部采用强制成最高速率，全双工模式；
3. 自动协商模式为所有电口的默认模式，当电口采用自动协商模式时，与之相连的网络设备也应采用自动协商模式，否则自动协商失败交换机会将端口设成默认的半双工模式，从而可能造成通信问题；
4. 流控是用来处理两个传输节点之间的数据传输速率管理的，两节点都必须支持流控机制才能发挥它的作用，如果相连网络设备不支持流控机制，建议用户关闭此功能；
5. 流控机制可以被启用或禁止，默认为禁止。使用流控会发出很多暂停帧，数据量大时，可能发生暂停帧风暴，故请慎用流控功能。

4.3.2 速率设置

该设备提供基于端口的速度限制，包括入口和出口速度限制，如图 4-12 所示。用户能够限制每个端口的通信流量或取消端口流量限制。用户能够选择一个固定的速度，其范围在：64Kbps ~ 不受限制，最小的速度为 64Kbps。端口限制的类型包括所有的单播包、多播包和广播包（限制的类型只对入口有效，出口的限制对所有的数据都限制）。该设备提供两个方向的速率限制，其中入口速度是指从 PC 等其他设备流向交换机端口的实际速度。

出口速度是指交换机端口流向使用设备之间的实际速度。如果同时限制了两个设备连接端口之间的入口速度和出口速度，则实际的速度为两者中较小的数值。（限制的类型如下图所示，其中上一个限制包含下一个限制，比如广播+多播限制，包含了广播和多播，但是单独的多播限制则没有这种设置）

图 4-12　速率设置界面图

注意

1. 当端口达到指定速率时，交换机并不是立刻进行限速，这是因为入口和出口均有 128K 的数据缓冲区，只有当此缓冲区被耗尽才会真正的限速；
2. 使用端口限速时，如果相连双方均启用了流控，设备之间的速度变化将是一条平稳的曲线。交换机根据是否启用流控来决定是/否丢弃超流量的报文；
3. 使用端口限速时，如果通信双方都启用了流控，则不应该丢包，丢包的表象是传递速度忽快忽慢；
4. 端口限速对网线质量要求较高，否则将出现大量的冲突包和破碎的包。

4.4 二层特性

二层特性设置包括：QoS，VLAN，IGMP 侦听，静态组播表。

4.4.1 QoS

QoS（Quality of Service）即服务质量功能由交换芯片 4 个内部优先级队列来实现，处于高优先级队列的数据包在交换机里暂留的时间较短，对某些延迟敏感的通信量支持较低的潜伏期，处于低优先级队列的数据包则相反。根据端口 ID、MAC 地址、802.1p 优先级标签、DiffServ 和 IP TOS，本设备能够对数据包分类到某个相应的等级。QoS 全线速操作

机制，实际调度在基于有利方式轮转或和高优先级队列混和模式进行。

处理不同优先级的数据包，每个端口最多提供 4 个队列，当这个功能启用后，QoS 分类机制根据图 4-13 所示的规则将接收到的数据包转到适当的出口队列。

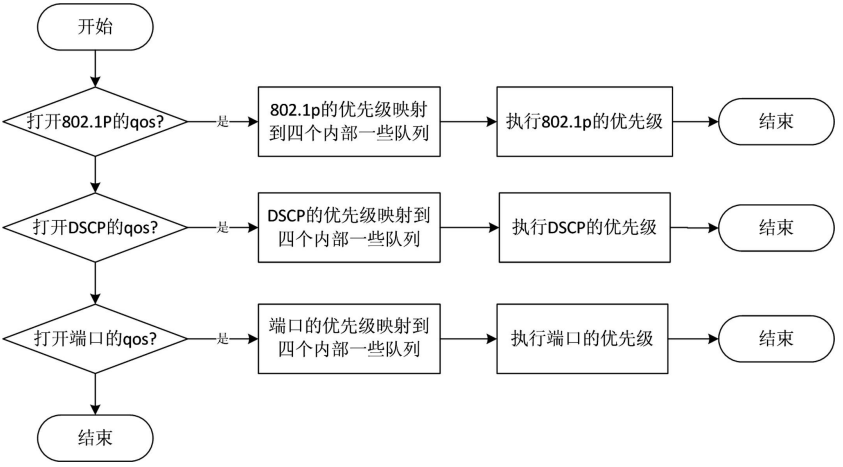


图 4-13　QoS 分类机制流程图

QoS 的配置页面如图 4-14 所示。

图 4-14　QoS 的配置界面图

当 QoS 禁用时，下面的所有选项都是禁用的，不启用 QoS 优先级，则所有的数据包都进入最低优先级队列,设置 QoS 先要选启用项，如图 4-15 所示。

图 4-15　QoS 设置界面图

然后选择采用绝对优先级还是相对优先级，当选择绝对优先级时，交换机将高优先级队列的数据包处理完后再处理低优先级队列的数据包，而相对优先级方式，交换机采用的是在优先处理高优先级队列数据的同时会兼顾处理一下低优先级队列中的数据，四个队列的转发的比例从高到低为 8：4：2：1，如图 4-16 所示。

图 4-16　QoS 控制类型界面图

优先级设置有三种方式：802.1p 优先级、端口优先级和 DSCP 优先级，可以任意启用若干种，（注意 802.1p 优先级的级别最高，DSCP 次之，端口优先级最低，就是说如果多个等级的优先级同时打开，只有等级最高的起作用），如图 4-17 所示。

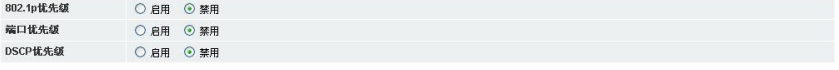


图 4-17　各优先级设置界面图

基于端口的优先级使用交换机的 4 个优先级队列，如果某一端口使用最高优先级队列，则所有从该端口进入的数据包，都将进入交换机的最高优先级队列，这个端口的数据将比其他端口有更大概率首先被转发（在相对优先级设置情况下），或者只有该端口数据发送完了，在发送其他端口的数据（绝对优先级设置情况下）。基于端口优先级配置界面如图 4-18 所示。

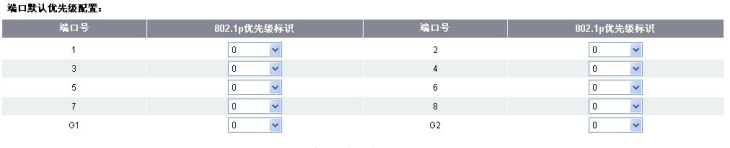
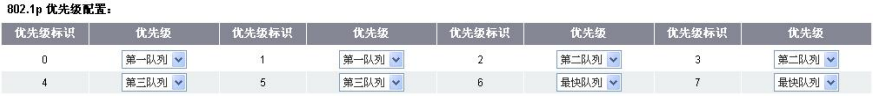


图 4-18　端口优先级配置界面图

802.1p 是 IEEE802.1Q（VLAN 标签技术）标准的扩充协议，它们协同工作。在本质上，它提供了一个在第二层 MAC（Media Access Control）层执行 QoS 的机制。VLAN 标签有两部分：VLAN ID（12 比特）和优先级（3 比特）。IEEE802.1Q VLAN 标准中没有定义和使用优先级字段，而 802.1p 中则定义了该字段，所以 IEEE802.1p 优先级可用的分类等级有 8

个（3 比特），在 IEEE802.1Q 标签里有 3 位作为用户优先级。如图 4-19 所示。


802.1p 优先级配置：

优先级标识	优先级	优先级标识	优先级	优先级标识	优先级	优先级标识	优先级
0	第一队列	1	第一队列	2	第二队列	3	第二队列
4	第三队列	5	第三队列	6	最快队列	7	最快队列

图 4-19　802.1p 优先级配置界面图

优先级 0 是缺省值，并在没有设置其他优先级值的情况下自动启用。设备默认设置中优先级 0 和优先级 1 映射到第一队列，即优先级最低的队列。优先级 2 和优先级 3 映射到第二队列，优先级 4 和优先级 5 映射到第三队列，优先级 6 和优先级 7 映射到优先级最高队列即转发最快的队列。

DiffServ，即区分服务，是被指定了一个简单的、可升级的、粗略划分的计算机网络体系，在近代 IP 网络中，在第三层用来管理网络通信和提供服务质量保证。例如，DiffServ 能用来提供较短的反应时间，确保诸如音频或视频之类的关键的网络数据顺利通过，提供简单的、最大努力的通信保证给诸如 Web 通信或文件传输等非关键的数据通信。

DiffServ 是一个用 IP 头中的 DSCP 域存储优先级信息三层表示方案，它使用了 IP 头 TOS 域 8 位中的 6 位（此处需注意一下位序），故总共有 64 种优先级划分，同时也与 TOS 兼容。DSCP 使用 64 个值映射到用户定义服务等级，允许在网络通信上建立更多的控制操作。当区分不同类别的通信量的优先级时，DSCP 是一个高级智能的方法。基于 IP 信息头中的 DSCP（DiffServ Code Point）值，该交换机能对通信数据包进行服务等级分类。交换机支持 IPv4 和 IPv6 的 DSCP。如果启用 DSCP 优先级，交换机将依据 DSCP 值对通信量进行等级划分。DSCP 配置见图 4-20 所示。


DSCP优先级配置：

DSCP标识	优先级	DSCP标识	优先级	DSCP标识	优先级	DSCP标识	优先级
0	第一队列	1	第一队列	2	第一队列	3	第一队列
4	第一队列	5	第一队列	6	第一队列	7	第一队列
8	第一队列	9	第一队列	10	第一队列	11	第一队列
12	第一队列	13	第一队列	14	第一队列	15	第一队列
16	第二队列	17	第二队列	18	第二队列	19	第二队列
20	第二队列	21	第二队列	22	第二队列	23	第二队列
24	第二队列	25	第二队列	26	第二队列	27	第二队列
28	第二队列	29	第二队列	30	第二队列	31	第二队列
32	第三队列	33	第三队列	34	第三队列	35	第三队列
36	第三队列	37	第三队列	38	第三队列	39	第三队列
40	第三队列	41	第三队列	42	第三队列	43	第三队列
44	第三队列	45	第三队列	46	第三队列	47	第三队列
48	最快队列	49	最快队列	50	最快队列	51	最快队列
52	最快队列	53	最快队列	54	最快队列	55	最快队列
56	最快队列	57	最快队列	58	最快队列	59	最快队列
60	最快队列	61	最快队列	62	最快队列	63	最快队列

图 4-20　DSCP 优先级配置图


注意

1. 交换机内部只有四个转发优先级队列，所以 802.1p 和 DSCP 虽然各有 8 个和 64 个优先级，但其最终要通过交换机来实现，所以默认设置中 802.1p 和 DSCP 的多个优先级会处于同一转发队列中，所有处于同一转发队列中的包都具有真正的“硬件”层面上的相同优先级，而不管他们在软件层面上可能被设置成不同的优先级。（8021.p 和 DSCP 优先级映射到四个交换机内部优先队列，是一个多对一得映射，有多个多个优先级映射到同一个队列这种情况出现，这是由交换芯片功能决定的，数据在交换机外部没有发送改变）
2. 绝对优先级是先处理完最快优先级队列的数据，然后才会处理优先级低一点的队列的数据，最后才会处理最低优先级队列的数据；而相对优先级是指在处理最快优先级队列数据的同时会兼顾处理一下低优先级队列中的数据，四个队列的转发的比例从高到低为 8：4：2：1；
3. 对三种优先级同时启用时，优先级高低排序为：802.1p >DSCP>端口优先级；
4. 802.1p 是对 802.1Q 的扩充，优先级标识存放于 VLAN Tag 中，故仅对于 802.1Q 的 VLAN 包有效；
5. DSCP 优先级标识存放于 IP 头中，故仅对于 IP 数据包有效；DSCP 数据帧的优先级可以穿越整个因特网。DSCP 向下和 IPv4 TOS 兼容，允许和使用三层 TOS 优先级方案的设备进行相应操作。
6. 当设置混合优先级时，端口优先级与 802.1p 优先级互斥，不能同时开启。

4.4.2 VLAN

VLAN 指虚拟局域网技术，通常被称作 vLAN 或 VLAN（Virtual Local Area Network）。虚拟局域网是从一个实际的物理网络中创建独立分离的逻辑网络的一种方法，此方法使几个虚拟的局域网能同时存在于一个实际的物理网络里。VLAN 能有效减少广播范围，通过不能进行数据交换的、分离的逻辑网段（如公司部门），便于网络管理。VLAN 可以有效的抑制广播风暴的发生。

本交换机支持端口 VLAN 和 IEEE 802.1Q VLAN，但两者不能同时使用，默认启用的是基于端口的 VLAN。关于 IEEE 802.1Q VLAN，请参考图 4-21 所示。

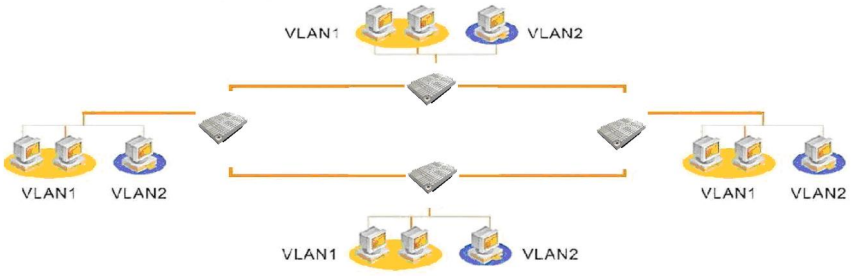


图 4-21　端口 VLAN 拓扑图

端口 VLAN

端口 VLAN 提供了一个能够把交换机端口划分到不同的虚拟私有域里去的解决方案。在不同的私有域之间是不允许进行数据交换的，所以各私有域里的数据维护变得相对安全。

本交换机为每个端口提供灵活的 VLAN 配置，端口 VLAN 作为一个过滤器，过滤掉非私有域的端口的通信量。在默认情况下启用端口 VLAN，且其中已添加了一条默认的 default 表项，将所有的端口放在此 VLAN 中，如图 4-22 所示。

图 4 -22　VLAN 表项与端口界面图

用户可以根据自身需求，如图 4-23 所示的 Web 页面，来配置端口 VLAN。

图 4-23　端口 VLAN 配置界面图

步骤如下：

- 要添加自己的 VLAN，首先要删除掉默认的 default 表项，否则所有端口仍在至少一个 VLAN 中从而起不到隔离通讯数据的作用，在表项中选择 default，点击 删除表项
- 在组名称框中输入要添加的 VLAN 名称，必须为数字或字母的组合，如 group1
- 在端口列表中选择要加入此 VLAN 的端口，右边的两个按钮 选择未用端口 和 全选 可以帮助用户方便选择所需端口，其中的 全选 按钮点击后时

会在 取消全选 两者中切换

- 选好端口后，点击 添加表项 即可将 VLAN 添加至表项中
- 用同样的方法添加新的 VLAN 组
- 当添加完成后，如果有剩余端口没有添加进任何 VLAN 中，需将这些端口也添加入一新的 VLAN 中
- 在组名称中填入 VLAN 名称，点击 选择未用端口 选择所有未用端口，再添加至表项
- 全部 VLAN 添加完毕，核对无误后，点击 保存设置 即自动刷新本页面，端口 VLAN 新配置生效

注意

1. 首先要删除默认的 default 表项，否则所有端口仍在至少一个 VLAN 中从而起不到隔离通讯数据的作用；
2. 所有端口都必须加入任一组 VLAN 中，如端口 1、2 没有加入任一 VLAN，则点击 保存设置 时，会弹出如下提示画面：

3. 任一端口都可以加入若干组 VLAN 中，此端口能与它所加入的所有 VLAN 组成员端口通信。

802.1Q VLAN

本交换机也支持 IEEE 802.1Q VLAN。虚拟局域网通过 IEEE802.1Q 协议可以跨越多个交换机进行划分。不同交换机的同一个 VLAN 可以通信，不同交换机的不同的 VLAN 不可以通信。本交换机支持标准的 IEEE802.1Q 协议，可以与其他支持 IEEE802.1Q 协议标准的交换机兼容，也支持 802.1Q 标签的修改，可以连接能识别 802.1Q 标签或不能识别 802.1Q 标签的设备。使用本交换机来配置 IEEE802.1Q VLAN 是非常方便的。IEEE 802.1Q VLAN 可以通过如图 4-24 所示的 Web 页面进行配置。

图 4-24　IEEE 802.1Q VLAN 配置界面图

802.1Q VLAN 的 VLAN 表项添加方法同端口 VLAN 一样，有一点要强调的是 VID 值必须为 1~4094 范围内的数字。默认时表项中已有一个 VID 为 1 的表项，所有的端口都处于此 VLAN 中。如图 4-25 所示。

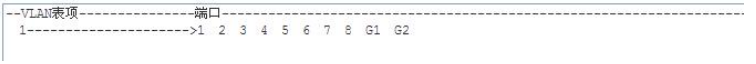


图 4-25　802.1Q VLAN 表项与端口界面图

设置步骤如下：

- 要添加自己的 VLAN，首先要删除掉默认的 VID 为 1 的表项，否则所有端口仍在至少一个 VLAN 中从而起不到隔离通讯数据的作用，在表项中选择 1，点击 删除表项
- 在 VID 值框中输入要添加的 VID，必须为整数，范围为 1~4094
- 在端口列表中选择要加入此 VLAN 的端口，右边的两个按钮 选择未用端口 和 全选 可以帮助用户方便选择所需端口，其中的 全选 按钮点击后时会在 取消全选 两者中切换
- 选好端口后，点击 添加表项 即可将 VLAN 添加至表项中
- 用同样的方法添加新的 VLAN 组
- 当添加完成后，如果有剩余端口没有添加进任何 VLAN 中，需要将这些端口也添加入一新的 VLAN 中
- 在 VID 值框中输入要添加的 VID，点击 选择未用端口 选择所有未用端口，再添加至表项
- 全部 VLAN 添加完毕，核对无误后，点击 保存设置 即自动刷新本页面，802.1Q VLAN 新配置生效

注意

1. 首先要删除掉默认的 VID 为 1 的表项，否则所有端口仍在至少一个 VLAN 中从而起不到隔离通讯数据的作用；
2. 所有端口都必须加入任一组 VLAN 中，如端口 1、2 没有加入任一 VLAN，则点击 保存设置 时，会弹出如下提示画面：

3. 任一端口都只能加入到一个 802.1Q VLAN 中。

在上面的 VLAN 配置的 Web 页面里，当选择 IEEE 802.1Q VLAN 时，高级设置 按钮被启用，在端口 VLAN 中是被禁用的，点击 高级设置 ，弹出如如图 4-26 所示的高级设置页面。

图 4-26　IEEE 802.1Q 高级设置页面

高级设置默认是禁用的，下面所有的选项都是灰色的被禁用状态，点击“启用”即可进行设置，用户可以通过本页面的设置，对 VLAN 功能进行一些更细微的操作。下面对设置的功能进行详细解释。

启用 802.1Q VLAN 高级规则：如图 4-27 所示。

图 4-27　启用 802.1Q VLAN 高级规则界面图

802.1Q 帧检查：VID 指添加 VLAN 时的组 id，范围在 1~4094 之间；PVID 指 port vid，即端口 VID，与下面的端口 VID 一致，PVID 可以由用户在下面进行设置；替换的功能是指某一端口用下面设置的 PVID 替换掉从此端口接收的 VLAN 包中的 VLAN Tag，不替换就是不执行这一动作。（替换操作会更改进来的包结构，建议慎用）

丢弃无 TAG 的帧：指定某一端口接收到无 VLAN Tag 的数据包时，即非 VLAN 的数据包时，丢弃该数据包。此功能用户需谨慎使用。

图 4-28 用于配置端口的 PVID、VLAN Tag 的处理方法。

图 4-28　基于端口的 802.1Q 的优先级、端口 VID（PVID）以及是否剥离 VLAN 的标记配置界面图

端口 VID：即上面所说的 PVID，设置端口默认的 VID，设置目的目前仅用于替换。

VLAN 标记：指从此端口发出去的 VLAN 包，对其中的 VLAN Tag 进行剥离或保留的操作。剥离功能一般在与此端口相连的为网络终端，如 PC 机时采用，因为 PC 机一般不能接收带 VLAN Tag 的数据包。

启用 802.1Q VLAN TRUNK：VLAN TRUNK 功能使得多台交换机能够在组成网络后再划分 VLAN。其 Web 网页如图 4-29 所示。

图 4-29　启用 802.1Q VLAN TRUNK 的 Web 网页图

Trunk 端口列表：用以指定进行 trunk 的列表；

管理端口列表：一个网络设置一个即可，用以对网络中交换机进行管理，通过 PC 可以访问本地和远程的交换机配置界面；

VLAN 列表：列出需要使用 trunk 端口的 VLAN 的 ID。

注意

1. 更改 VLAN 设置都要删除默认的 VLAN 组，因为其包含了所有端口；
2. IEEE 802.1Q VLAN 的包处理流程：数据进入端口→检查是否需要附加或替换 VLAN 标记→检查转发表是转发还是丢弃→检查是否需要去除 VLAN 标记→数据从端口出去；
3. IEEE 802.1Q VLAN 比端口 VLAN 多了 VLAN 标记的添加和去除的过程，对于这种 VLAN 只允许端口要么是上联口，要么是终端口。
4. 若开启了 802.1Q VLAN，那么 PVID 将会自动更新至和端口所在的 VLAN 的 vid 相等（注意默认情况下，端口的 pvid=1），随着端口加入 802.1Q 的 VLAN，那么 pvid 也会随之变化，pvid=vid。

4.4.3 IGMP 侦听

本交换机提供 Internet 组播管理协议，交换机可以自动侦听 IGMP 数据包、自动查询多播组成员，并根据多播组信息动态维护一个多播转发表。如图 4-30 所示。

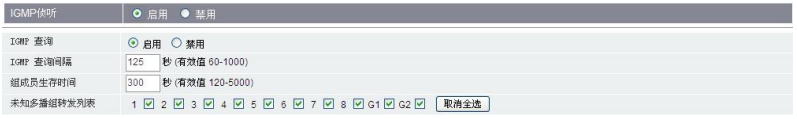


图 4-30　IGMP 侦听配置界面

IGMP Snooping 功能默认为禁用，要使用 IGMP 功能先要选择 启用 项，设置参数说明如下：

IGMP 查询：选择是否启用多播组成员查询功能，IGMP 查询包（query）用来查询现存的多播组，查询间隔时间用户可以设置。每当多播组成员收到此查询报文（query）后会回应一个应答包（report），交换机收到成员的应答包（report）后会更新多播表，重新计算该成员的生存时间，如果在多次查询后仍没收到该成员的应答包（report），则在超出成员生存时间后交换机将自动删除多播组中的该成员。

本功能可以让交换机在网络中没有路由器或路由器不支持多播的情况下充当 IGMP 状态机的角色，如果网络中已存在其他的 IGMP 查询设备，则可以禁用此查询功能，不启用此选项则不会周期性的查询多播组成员，可以降低网络负荷。

此功能默认为启用。

IGMP 查询间隔：此选项只有在 IGMP 查询选项启用后才会被启用，顾名思义就是设置发送 IGMP 查询包（query）的时间间隔，此间隔时间不能设置得太短，过短的时间会加重网络的负荷，同样也不能设置得太长，太长的时间会导致多播组的动态更新太慢。

间隔时间设置范围为 60~1000 秒，默认值为 125 秒。此时间为软件运算时间，不会非常的精确，但在误差允许范围之内。

组成员生存时间：多播组成员的生存时间，每当成员加入多播组或收到该成员的 report 报文即重新计时，超出此时间后，成员即从该多播组中删除。此时间也不能设得太长或太短，可设置范围为 120~5000 秒，默认值为 300 秒。

成员可以加入多个多播组，在每个多播组中都会分别计时，相互独立。此时间为软件运算时间，不会非常的精确，但在误差允许范围之内。

未知多播组转发列表：当交换机收到一个目的地址为多播地址的数据包，而此多播目的地址又不在已知多播表中，则此数据包就为未知多播组的数据包，本选项就是定义此类数据包的转发规则，默认选项为选择所有端口，即当交换机收到未知多播组的数据包时，将会从所有端口转发出去。用户可以根据具体的网络情况设置转发端口。

当启用 IGMP Snooping 功能后，交换机会动态的维护一张多播转发表。如图 4-31 所示。

图 4-31　未知多播组转发列表图

其中的第 2、3 项即为动态维护的多播地址转发项，第 1 项为后面将要讲述的手动添加的静态组播表项，其类型为“固定”。每当打开本 Web 页面，此表 4-3 中的显示内容就会更新一次。

表 4-3　IGMP 设置描述表

设置项目	描　述	默认值
IGMP Snooping 使能	启用IGMP Snooping	禁用
IGMP 查询使能	启用交换机IGMP查询配置	启用
IGMP 查询间隔	交换机查询间隔时间	125s（作为协议的标准时间）
组成员生存时间	交换机多播地址老化时间	300s
未知多播组转发列表	转发端口选择	所有端口

注意

1. 如果 PC 是一个网口带多个 IP 地址时，Windows 系统总是用最下面的 IP 地址应答，很可能会出现问题；
2. 网络中最好不要出现多个 IGMP 查询者，浪费资源；
3. 如果不确定未知多播组的转发关系，请选择全部的端口。

4.4.4 静态组播表

本交换机提供手工增删静态 MAC 多播地址转发功能，如图 4-32 所示。

图 4-32　静态组播转发表界面图

此静态组播表项与前面所述的 IGMP Snooping 动态组播表项共同使用一张多播表，内建在交换机芯片里的转发地址表，保持学习功能，二者的区别是 IGMP Snooping 根据 IGMP 协议动态的增删多播表项，并启用老化计时，对过时的多播组及其成员删除，而静态组播表项提供用户手工增删多播表项，此表项在多播表中定义为静态，静态 MAC 地址履行转发功能，但是它不受老化处理的支配，目的地址包含静态 MAC 地址的数据包将会被转发到指定的端口，设置参数说明如下：

静态组播 MAC 地址：在此方框中填入要添加的 MAC 多播地址，格式为 XX-XX-XX-XX-XX-XX，多播地址前三字节都是 16 进制的 01-00-5E，下面的多播地址为

本交换机保留，请不要使用：

01-00-5E-00-00-XX（保留的多组播管理 MAC 地址）

01-80-C2-XX-XX-XX（保留的以太网桥管理 MAC 地址）

端口列表：选择目的地址为此多播 MAC 地址的多播包默认的转发端口，要转发至哪个端口，就将其勾上即可。

处理列表：本栏用于操作多播表，按钮 添加 和 删除 用来添加/修改和删除静态 MAC 地址。已存在的静态多播表项会显示在下面的表框中，每当用户打开本 Web 页面或者执行添加和删除的操作就会更新表框，如图 4-33 所示已添加有一项静态多播转发地址（01-00-5E-01-02-03）。

图 4-33　静态多播转发地址表图

注意

1. 添加 和 删除 操作会立即生效，而不像其他页面需“保存”类似的操作；
2. 请不要使用单播地址作为输入地址；
3. 请不要输入保留的多播 MAC 地址，如：01-00-5E-00-00-XX（保留的多组播管理 MAC 地址）、01-80-C2-XX-XX-XX（保留的以太网桥管理 MAC 地址）。
4. 添加操作时，交换机会失去响应，添加成功后，请刷新页面。

4.5 链路备份

链路备份功能设置：WING 快速环网，Trunk 端口汇聚，RSTP 快速生成树。

4.5.1 快速环网

WING 可以让交换机之间以冗余的链路相连接，当其中一路断开时，另一链路能快速的自动恢复，在网络中断或网络产生故障时，它具有链路冗余、快速自恢复能力。WING 技术由上海纽琳克通信技术有限公司自主研发，专业为高可靠性的工业控制网络应用而开发设计。

WING 技术在一个由交换机组成的多环网络中，网络断开自恢复时间少于 20 毫秒。WING 技术允许用户将交换机的部分端口指定用做环网冗余端口，与其他交换机相连。当其中的一路网络连接发生中断时，WING 冗余机构启用备份链路，迅速恢复网络通信。下表 4-4 为基于冗余技术恢复时间比较，仅供参考。

表 4-4　基于冗余技术恢复时间比较表

冗余技术	WING	RSTP	STP
恢复时间	<20ms	>5s	>30s

通常，WING 技术需三个或三个以上的本交换机连接组成一个环。下图 4-34 是一个基于 WING 技术最典型的应用图例。

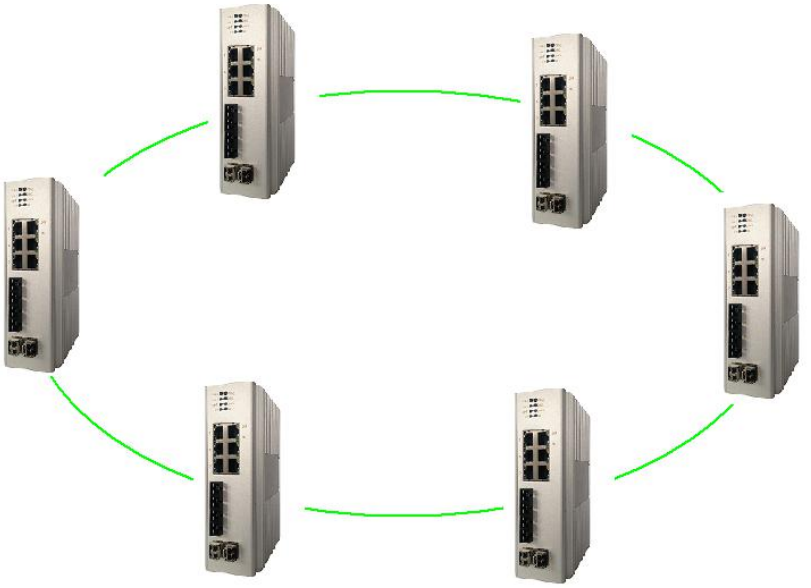


图 4-34　基于 WING 技术的典型应用图

WING 技术可以组建单环。单环是一个基本的单元，一个单环通常使用交换机的两个端口组成，如上图所示。

WING 技术允许同一网络同时存在一个或多个环，但必须为每个环配置唯一的 ID，此 ID 为环中的交换机共用，快速环网的 Web 页面如图 4-35 所示。

图 4-35　快速环网的配置界面图

环网组：每台交换机最多支持四组环网，三个单环和一个双环，可以任意的启用若干个，建议用户尽可能少的启用环网组数，如启用一个单环就能满足需要就不要启用两个单环，也不要启用双网，以免增加网络链路的复杂度。

网络标识：即上文所说的环 ID，范围为 1~254 之间的整数，每个环都必须有唯一的 ID，且此 ID 为组成此环的所有交换机共享，也就是说所有接在此环中的交换机都用此 ID 来进行网络标识。

端口列表：选择接入环的为哪些端口，接入单环需 2 个端口，环间耦合只需 1 个端口，不处于环中的端口一定要将后面的勾去掉，千兆端口和百兆端口之间也可以互相组环。

设置完保存配置参数，WING 功能将被激活。配置参数说明简单总结如表 4-5 所示。

表 4-5　WING 配置参数说明简单总结表

设置项目	描　述	默认值
网络标识	标示不同的环	250/251/252/4
端口列表	为不同的环类型指定不同的端口	1,2,3,4,5,6,7, 8,G1,G2
环网类型	连接交换机的环类型（单个环网、环间耦合）	单个环网
启用	启用WING 技术	禁用

注意

1. 快速环网协议属于本公司私有协议，只能在本公司同系列交换机中使用，与非本公司的交换机不能互相兼容；
2. 快速环网与 RSTP 不能同时启用，当用户启用快速环网时，RSTP 自动关闭，当启用 RSTP 时，快速环网也会自动关闭；
3. 当快速环网启用时，所有交换机都有个很短的时间快速的交换数据包，以阻塞冗余链路，然后环网会处于一种暂稳状态；一旦主链路断开，则交换机之间同样有个很短的时间快速的交换数据包，以将阻塞的冗余链路启用，达到自愈的目的，然后环网又会处于另一种暂稳状态，在这种状态过渡的时候会有丢包现象，但时间会很短（<20ms）；
4. 环网的自愈时间与组环的交换机数量及环网的复杂度成正比，小于 20ms 的自愈时间是在四台交换机组成一个单环的情况下测得的；
5. 注意，开启 WING 时，不要对参加组环的端口使用 Trunk 端口汇聚功能，端口镜像功能以及速率设置中的出入口限速功能。
6. 现将环网的第一组设置为默认开启，默认 ID 为 250，在组环时注意不要接错组网端口，否则可能形成风暴。
7. 当环网启用，但未成环时，RING 指示灯闪烁，当环网启用且处于成环状态时，RING 常亮。当环网功能禁用时，则 RING 指示灯灭。

4.5.2 端口汇聚

端口汇聚（TRUNK）的主要功能就是将多个物理端口（一般为 2－8 个）绑定为一个逻辑的通道，使其工作起来就像一个通道一样。将多个物理链路捆绑在一起后，不但提升了整个网络的带宽，具有链路冗余的作用，在网络出现故障或其他原因断开其中一条或多条链路时，剩下的链路还可以工作。Trunk 在组建冗余网络时，是一个非常有用的，也经常被使用的功能，使用起来也相当简单，下面图 4-36 是一个使用 Trunk 的案例图示。

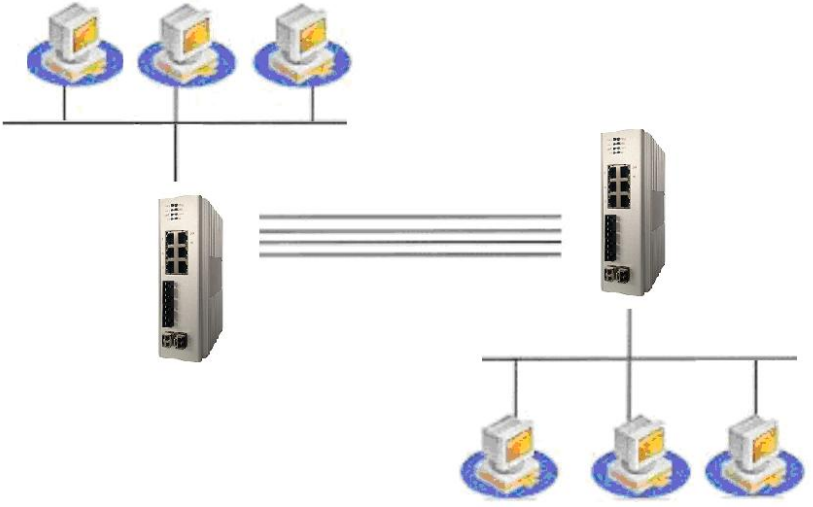


图 4-36　使用 Trunk 的案例示意图

上图在两个交换机之间通过一个 Trunk 组建了一个计算机网络，两台交换机之间用四个端口相连在一起，以达到提升带宽和实现链路冗余。

本交换机支持 Trunk 功能，它允许总共四组 Trunk，每组 Trunk 包含 2~8 个端口作为单个逻辑链路，用来提升带宽和链路冗余，当其中一个物理连接不能通信或出现故障时，Trunk 组中的其他链接立刻接管并维持通信，如此可以提供一个通信中断后快速恢复机制。配置 Trunk 功能需要通过图 4-37 所示的 Web 页面进行设置。

图 4-37　汇聚配置界面图

汇聚组：本交换机最多支持四组 Trunk，默认情况下，1~3 组由百兆端口组成，4 组由千兆端口组成。

端口列表：选择分配到每组 Trunk 中的端口，1~3 组 Trunk 每组可以分配 2~8 个端口。同一个端口不能同时存在于两个 Trunk 组里。要选择加入 Trunk 的端口，将其勾上即可；4 组 Trunk 默认由 G1、G2 两个千兆端口组成。

启用：选择是否启用本组 Trunk，打勾即启用。当使用 Trunk 时，必须先启用它，然后再进行物理连接。

注意

1. 本交换机最多支持四组 Trunk，1~3 组分别可由 2~8 个端口组成，4 组默认由 G1、G2 两个千兆端口组成；
2. 同一个端口不能同时存在于两个 Trunk 组中；
3. 使用 Trunk 时，必须先启用它，然后再进行物理连接；
4. 带宽的提升并不是简单的与端口数成倍数关系，相反往往表现为汇聚的总带宽没有增加，这是由交换芯片的转发机制决定的；
5. 端口汇聚的自愈时间很短，百兆速率下不丢包。

4.5.3 快速生成树

生成树协议（STP）简介：

生成树协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

快速生成树协议（RSTP）

在 IEEE 802.1w 标准里定义了快速生成树协议 RSTP（Rapid Spanning Tree Protocol），作为对 802.1d 标准的补充。

快速生成树（RSTP）的配置说明

在菜单上点击快速生成树子菜单，就会弹出如图 4-38 所示的配置界面。

图 4-38　快速生成树的配置界面

RSTP 配置：启用/禁用快速生成树功能，默认为禁用，快速生成树和快速环网功能不能同时启用，如启用了 RSTP，则会自动关闭快速环网，同理如果启用了快速环网，则会自动禁用 RSTP。当启用 RSTP 时，RSTP 会先禁用所有的端口，等收敛期完毕，才会使能和阻塞某些端口，在此期间 Web 服务器会失去响应，当收敛结束，网络树生成后，就可以重新使用 Web 服务器。如图 4-39 所示。

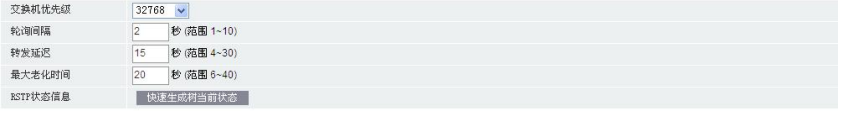


图 4-39　快速生成树的 WEB 服务器页面

交换机优先级：设置交换机（网桥）的优先级，交换机优先级和交换机的 MAC 地址组合成桥 ID，桥 ID 最小的交换机（网桥）将成为网络中的根桥。此值越小优先级越高，越有可能成为根桥，默认值为 32768。

轮询间隔：设定交换机多长时间发送一次 BPDU 的数据包，发包间隔小会加快 RSTP 的收敛速度，但会增加网络负担，设得太大，则会使 RSTP 的收敛时间变长。默认值为 2，取值范围为 1~10 之间的整数，单位为秒。

转发延迟：指交换机的端口状态在过渡状态下（listening 和 learning）下维持一个 forward delay 的时间，单位为秒。默认值为 15，取值范围为 4~30 之间的整数。

最大老化时间：指一个交换机从其他交换机收到一个 BPDU 数据包以后，这个数据包有效期多长，单位为秒。默认值为 20，取值范围为 6~40 之间的整数。

时间的设置值需满足如下公式：2*（转发延迟-1）>=最大老化时间。

转 RSTP 状态信息：点击 快速生成树当前状态 按钮可以查找 RSTP 的状态信息，页面如图 4-40 所示。

根交换机信息表:	
本交换机ID标识	F000-0002b3020202
根交换机ID标识	8000-0002b32e01c6
根端口号	5
根端口路径开销	200000

本交换机信息表:							
端口号	优先级	路径开销	点到点网络	边缘端口	相连网络	端口角色	转发状态
1	128	200000	Y	N	Rapid	Unknown	Disabled
2	128	200000	Y	N	Rapid	Unknown	Disabled
3	128	200000	Y	N	Rapid	Alternate	Discarding
4	128	200000	Y	N	Rapid	Unknown	Disabled
5	128	200000	Y	N	Rapid	Root	Forwarding
6	128	200000	Y	N	Rapid	Designated	Forwarding
7	128	200000	Y	N	Rapid	Unknown	Disabled
8	128	200000	Y	N	Rapid	Unknown	Disabled
G1	128	20000	Y	N	Rapid	Unknown	Disabled
G2	128	20000	Y	N	Rapid	Unknown	Disabled

图 4-40　RSTP 的状态信息界面图

此页面显示当前网络中根桥是 MAC 地址 00-02-b3-02-02-02 为交换机而不是本机，本机的根端口为 5，故端口 5 为转发状态（forwarding），另外端口 6 为指定端口，也处于转发状态，但端口 3 被阻塞，说明端口 3 为冗余链路。本页面的信息显示了 RSTP 的当前状态，RSTP 永远处于动态侦测、协商的过程中，所以每次刷新本页面，看到的都是最新状态，每次刷新本页面，得到的信息并不一定相同。

端口角色标注端口的角色，共有五种：

Root：接收根桥定时发送的配置报文的端口，即根桥是整个网络里唯一没有 Root 端口的设备；

Designated：表示指定端口，会在向它所连接的网段上发送最优配置报文，与 Root 端口相对；

Backup：表示备份端口，会由于收到自己的更优配置报文而被阻塞；

Alternate：表示预备端口，只是会由于收到其他交换机的更优配置报文而被阻塞；

Unknown：不是以上任何一种端口时。

转发状态指端口的运行状态，共有四种：

Disabled：禁用状态，表示此端口没有连接，没有连接的端口就处于此状态。

Discarding：阻塞状态，此时可接收 BPDU 数据包,如果期间没收到 BPDU 后转到学习

状态，链路刚接通时端口都处于阻塞状态。

Learning：学习状态，此时可以接收数据包，连通之后马上接通时交换机在阻塞状态下停留 max age=20s 的时间，判断交换机的这个端口有没有可能成为根端口或指定端口，期间收发 BPDU 数据包，完成生成树的根的选举、构造，完成端口状态去向的决定。如果决定是根端口或指定端口的话就停留 forward delay=15s 时间，并继续计算判断端口能不能成为根端口或者指定端口，此时具有学习 MAC 地址的功能。如果是根端口或指定商品后转换到转发状态，如不是的话转换到阻塞状态。

Forwarding：转发状态，此时端口可以正常的收发数据包。

为了加快 RSTP 的自愈过程，降低网络负荷，用户可以用下图 4-41 的页面详细配置端口信息。

端口号	端口路径开销	端口优先级	点到点网络连接	直接连接终端	参与生成树结构
1	200000	128	自动	否	否
2	200000	128	自动	否	否
3	200000	128	自动	否	否
4	200000	128	自动	否	否
5	200000	128	自动	否	否
6	200000	128	自动	否	否
7	200000	128	自动	否	否
8	200000	128	自动	否	否
G1	20000	128	自动	否	否
G2	20000	128	自动	否	否

图 4-41　RSTP 端口信息配置界面图

端口路径开销：端口路径开销，与端口优先级一起形成端口 ID 用于比较，路径开销由网络物理链路决定，用户应该根据具体的物理链路来修改此值。默认百兆端口的路径开销为 200000，千兆端口为 20000，为百兆端口的十分之一。

端口优先级：端口在网桥之中的优先级，与端口路径开销一起形成端口 ID 用于比较，此值越小优先级越高。默认为 128。

点到点网络连接：交换机端口和交换机端口之间只有直连，则该端口就是点到点接口。RSTP 针对点到点链路采用协商机制，可以实现端口状态的快速转换。

直接连接终端：处于网络边缘的交换机一般与终端设备相连，如 PC 机、工作站。将与这些终端设备相连的端口配置成为 Edge 端口，可以实现端口状态的快速转换，而不需要 Discarding，Learning，Forwarding 的转换过程，可以实现端口状态的快速转换。

参与生成树结构：指定该端口是否参与生成树协议的运行，这样可以减少端口数量，降低 RSTP 的运算复杂性，从而减少 RSTP 的自愈时间。

注意

1. RSTP 协议定义于 802.1w 标准中，是公开的标准协议，本公司的交换机的 RSTP 协议可

以与非本公司但支持标准 RSTP 协议的网络设备互相兼容；

2. 快速生成树和快速环网功能不能同时启用，如启用了 RSTP，则会自动关闭快速环网，同理如果启用了快速环网，则会自动禁用 RSTP；
3. 当启用 RSTP 时，RSTP 会先禁用所有的端口，等收敛期完毕，才会使能和阻塞某些端口，在此期间 Web 服务器会失去响应，当收敛结束（约 10s 以上），网络树生成后，就可以重新使用 Web 服务器；
4. 每当链路变换，RSTP 会有个时间不等的重新收敛过程，但也有可能造成 Web 服务器不能访问，等收敛结束，即可重新访问；
5. RSTP 启用后，每台交换机都会按用户设置的发包间隔周期性的从每个连接端口发送查询包，故会增加网络负荷；
6. 最大老化时间和转发延迟两者之间需满足以下条件：2*（转发延迟-1）≥ 最大老化时间；
7. 为了降低网络计算复杂度，减少收敛时间，建议用户设置端口信息，减少端口数量；减小转发延迟、最大老化时间可以加快 RSTP 的自愈。

4.6 访问控制

访问控制功能设置：用户密码，登录控制，端口认证，认证数据库，MAC 端口锁定。

4.6.1 用户密码

交换机的 Web 服务器提供三组不同的用户名和密码，每组都可以选择两个等级，用来保护对 Web 服务器的访问，只有知道用户名和密码才能登录入 Web 服务器，并对交换机进行管理。通过变更用户索引，用户名和密码可以被添加、删除和修改。如果用户名和密码都为空，则系统删除此索引所代表的用户名和密码。本交换机出厂时，默认的用户名和密码为“admin”，访问等级为管理员。

用户名和密码都必须是合法的字符，都可以由英文字母（区分大小写）和数字组成，用户名不能为空，但密码可以为空，用户名和密码的最大长度都是 32 个字节。如果当前登录的用户名或密码被修改成与原来不一样时，再次访问 Web 页面时将会提示你重新输入用户名和密码。如图 4-42 所示。

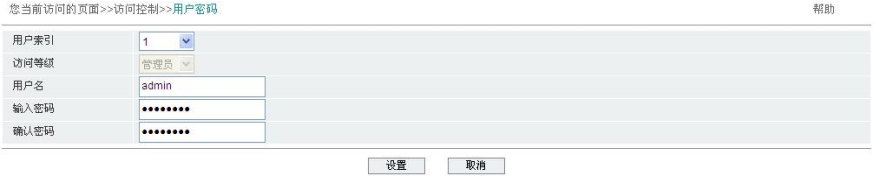


图 4-42　用户密码设置界面图

用户索引：用户名及密码组数索引，为数字 1~3，共三组。

访问等级：分为两个等级，分别为管理员和观察员，管理员具有对所有设置拥有查看和修改的权限；观察员对所有设置仅有查看的权限。对于第一组只能设置成管理员模式。

用户名：设置本组的用户名称，用户名称可以由英文字母（区分大小写）和数字组成，用户名不能为空，最大长度为 32 个字节。

输入密码：设置本组的用户密码，密码也可以由英文字母（区分大小写）和数字组成，密码可以为空，最大长度为 32 个字节。

确认密码：重复输入密码，以防密码输入错误。

注意

1. 第一组只能被设置成管理员模式，这是为了保证至少有一组是管理员模式；
2. 用户名和密码可以由英文字母和数字组成，建议用户不要使用中文；
3. 为了安全起见，建议管理员在首次登录后即修改默认的第一组用户名和密码；
4. 每当用户登录进入 Web 服务器后，服务器会在空闲约 5 分钟就会让本次有效登录认证失效，此时操作 Web 页面就会重新要求用户登录，这是为了防止管理员不在时别人对 Web 进行误操作，本时间为软件计算时间，不会很精确；
5. 用户随时可点击页面右上角的 退出 × 链接退出 Web 服务器，主动的让上次有效的登录认证失效，后续的任何 Web 操作都会重新激活登录认证。

4.6.2 登录控制

登录控制功能通过修改系统的防火墙来限制访问的客户端 IP 地址，从而对 Web 服务器的访问进行限制，如图 4-43 所示。

图 4-43　登录控制设置界面图

WEB 服务器传输协议：本选项用于使能 Web 服务器支持的传输协议，默认为支持 http 和 https 两种，建议用户不用修改此选项。

HTTP：HTTP（HyperTextTransferProtocol）是超文本传输协议的缩写，它用于传送 WWW 方式的数据，关于 HTTP 协议的详细内容请参考 RFC2616。HTTP 协议采用了请求/响应模型。客户端向服务器发送一个请求，请求头包含请求的方法、URL、协议版本、以及包含请求修饰符、客户信息和内容的类似于 MIME 的消息结构。服务器以一个状态行作为响应，相应的内容包括消息协议的版本，成功或者错误编码加上包含服务器信息、实体元信息以及可能的实体内容。

用户在浏览器的地址栏直接输入http://192.168.16.253即可使用 http 协议访问 Web 服务器。

HTTPS：HTTPS 是 HTTP 协议的安全版，出于保密的目的而研发，其安全基础是 SSL 协议。SSL 协议位于 TCP/IP 协议与各种应用层协议之间，为数据通信提供安全支持。SSL 协议可分为两层：SSL 记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL 握手协议（SSL Handshake Protocol）：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。

用户在浏览器的地址栏直接输入https://192.168.16.253，单击回车键，此时即是通过 https 协议访问 Web 服务器，可能会弹出如图 4 -44 所示的警告。

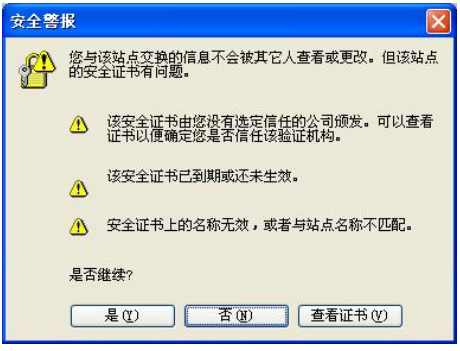


图 4-44　警告信息界面图

点击“是”即可继续，当首次登录时，有时会出现首页显示不正常，这是由于网页脚本程序运行不正常造成的，多刷新几次即可正常显示。

登陆 IP 地址控制：通过修改系统的防火墙，交换机提供高级的通信过滤功能。当启用这个功能的时候，仅被指定的 IP 地址的计算机才可以访问该设备，其他所有未被列出的 IP 地址都被禁止访问本交换机的 Web 服务器。

允许进入 IP 地址列表：在框中输入对允许访问 Web 的网络设备 IP 地址，总共允许 20 条记录，用户可以使用其中的若干条，用户至少要设置一条 IP 地址列表，且此地址不能为交换机自身地址，否则 Web 服务器将无法访问。

注意

1. HTTP、HTTPS 必须启用至少一种访问协议；
2. 个别浏览器使用 HTTPS 第一次打开时首页不能完全显示，多刷新几次后即正常显示，这是由于网页脚本程序运行不正常造成的；
3. 可访问的 IP 地址必须是一个合法的 IP 地址，至少应有一个地址与设备 IP 处于同一网段，否则设备将判定设置无效；
4. 地址列表中是允许进入的 IP 地址，而不是不允许进入的 IP 地址，故至少要设置一个地址，否则本交换机的 Web 服务器将无法访问；
5. 不要使用交换机的自身地址输入，因为如果错误地只允许这一条地址，就会造成无法访问 Web 服务器的问题。

4.6.3 端口认证

IEEE 802.1X 的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务与认证的分离。用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求，业务可以很灵活，尤其在开展宽带组播等方面的业务有很大的优势，所有业务都不受认证方式限制。

802.1X 结构主要有三部分组成：

- 申请者 supplicant：想得到认证的用户或客户
- 认证服务器 authentication server：典型例子为 RADIUS 服务器
- 认证系统 authenticator：对端间设备，如无线接入点、交换机等

我们设备可以同时扮演认证系统和认证服务器两个角色，也可以使用外部的认证服务器，同时支持外部的计费系统。端口认证的页面如图 4-45 所示。

图 4-45　IEEE 802.1X 认证设置界面图

定时更新认证：802.1X 的重认证周期时间，超过此时间后，上次成功认证失效，需重新认证，用来增强认证的安全性。设置范围为 60~40000000 秒，默认值为 3600 秒，即每 1 小时需重新认证一次。

Radius 服务器：即设置 Radius 认证服务器，有本地和远程两个选项。

本地是指使用本交换机作为 Radius 认证服务器，本交换机内建 Radius 服务器，申请者将只能使用交换机内部的 Radius 数据库的用户和密码，下面三项都被禁用；

远程是指使用交换机外部的 Radius 服务器来对本交换机的本地端口进行认证，外部的 Radius 认证服务器指非交换机内置的 Radius 服务器，本交换机的内置 Radius 服务器不能作为其他交换机的远程认证服务器。启用本选项后，下面三项都被启用，计费服务器可选填，其余为必填。

认证服务器设置：此选项在选用远程服务器后才会使能，填入远程服务器的 IP 和端口，设置的 IP 地址必须是本设备可以访问到的，默认端口是 1812。

认证共享密码值：此选项在选用远程服务器后才会使能，填入本交换机访问远程认证服务器的共享密码字符串。

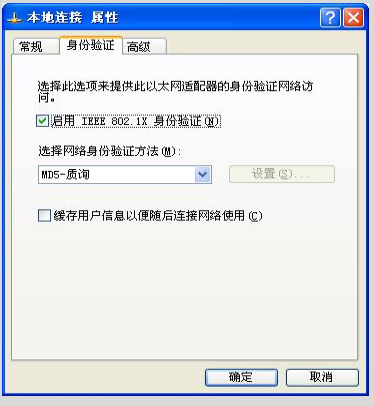
计费服务器设置：此选项在选用远程服务器后才会使能，为可选设置，计费服务器实现的功能是计费，设置的 IP 地址必须是本设备可以访问到的，默认端口是 1813，计费服务器设置错误会导致申请者无法通过身份认证，没有计费服务器就不需要设置。

如图 4-46 所示的部分用于设置是/否启用相应端口的 802.1X 认证功能，如果启用，则该端口在认证通过之前处于“失效”状态，认证通过后才会进入正常的转发状态，G1、G2 两个千兆口默认是不启用认证，用户无法设置。点击 重新认证 按钮会让上次认证失效，需重新对该端口进行认证。

图 4-46　相应端口的 IEEE 802.1X 认证配置界面图

注意

1. 在 windows 系统中，打开网络连接—>属性页：



如果没有 身份验证 标签，请选择“控制面板”→“管理工具”→“组件服务”→“服务”，启用“Wireless Zero Configuration”和“Wired AutoConfig”服务。在 选择网络身份验证方法(M): 选项中使用 MD-5 质询，其他方式不支持，如图中所示；

2. 如果启用了 802.1X 认证功能，并设置了认证数据库的用户名和密码，在 windows 系统中进行网络连接时会出现如下的认证对话框：

输入设置的用户名和密码即可通过认证；

3. 如果用户访问 Web 服务器使用的交换机端口启用了认证功能，则当认证功能一启动，用户就不能正常的访问 Web 服务器了，需通过认证才能重新访问 Web 服务器，这是正常现象，不是故障行为；
4. 所有的上联口、下联口和计费服务器端口必须强制通过认证，即“禁止”使用认证，否则无法使用远程服务器，除非使用内部认证服务器；
5. G1、G2 口作为上联口，默认是通过认证，用户无法设置，如果认证设置错误导致无法访问 Web 服务器的话，可以将网线切换至 G1、G2 口来正常访问；
6. 计费服务器设置错误同样会导致申请者无法通过身份认证，如果没有计费服务器就不需要设置；
7. 使用远程服务器时，管理员务必确认设备可以访问远程服务器，即"设备地址"中网关设置正确，如果使用域名则 DNS 必须设置正确；
8. 本交换机的内置认证服务器，不能作为另一交换机的远程认证服务器；
9. 如果认证数据库没有任何用户名和密码，则所有端口自动通过认证。

4.6.4 认证数据库

RADIUS 是一种远程用户拨号认证系统（RADIUS：Remote Authentication Dial In User Service），在网络接入服务器（Network Access Server）和共享认证服务器间传输认证、授权和配置信息的协议。RADIUS 使用 UDP 作为其传输协议。此外 RADIUS 也负责传送网络接入服务器和共享计费服务器间的计费信息。

RADIUS 认证数据库作为 802.1X 认证、授权的一部分，保存了用于认证的多组用户名和密码，用户可以通过此页面，对数据库中保存的用户名和密码进行增删。任何申请者的用户名和密码符合数据库的匹配规则时，设备的认证系统即授权于该申请者。RADIUS 认证数据库配置页面如图 4-47 所示。

图 4-47　RADIUS 认证数据库设置界面图

登陆帐户：设置新增的认证用户名，由一个不大于 16 字节的数字、字母（区分大小写）组成。

用户密码：新增的用户密码，也是是一个不大于 16 字节的数字和字母（区分大小写）组成。

处理列表：点击 添加用户 和 删除用户 用来在下面的表框中添加和删除用户名和密码，所有的增加和删除操作都要点击 保存设置 按钮来提交至交换机，并触发数据库的更新和整个 802.1X 认证的重新开始。在点击 保存设置 按钮前退出本页面，则所有的修改都被撤销。

注意

1. 点击 添加用户 和 删除用户 时，增删的表项在表框中显示已改变，但并没有保存，只有点击 保存设置 按钮这些变化才会提交至交换机，并会触发数据库的更新和整个 802.1X 认证的重新开始；
2. 请使用标准的 802.1X 的登陆工具如 windows 自带的工具，像 H3C 的 802.1X 登陆工具用户有一个字节的自定义字段,在本交换机上无法登陆；
3. 用户组的总数不大于 128；
4. 不启用本地 RADIUS 认证，该数据库内容实际上是无效的；
5. 如果认证数据库没有任何用户名和密码，则所有端口自动通过认证。

4.6.5 MAC 端口锁定

MAC 端口锁定是指在交换机的地址转发表中手工添加一条静态 MAC 地址，并将此地址与某一端口绑定，所有发给这个地址的数据只会转发给该端口，也称为 MAC 地址绑定。

静态 MAC 地址区别于学习得到的动态 MAC 地址，动态地址在最大的老化时间超过后即被删除，而静态地址一旦被加入，该地址不受最大老化时间的限制，如果不人为的删除它则将一直存在。静态地址表中一个 MAC 地址对应一个端口，也就是所谓的将静态地址与某一端口绑定，绑定的目的在于限制计算机的移动，凡是计算机的 MAC 和端口绑定的，此计算机移到其他非锁定端口则不能通信，而别的计算机移到这个绑定的端口还是可以通信的。绑定是针对 MAC 地址来的，所以限制了计算机，与此相对的是端口保护，它限制

了端口。本功能的配置页面如图 4-48 所示。

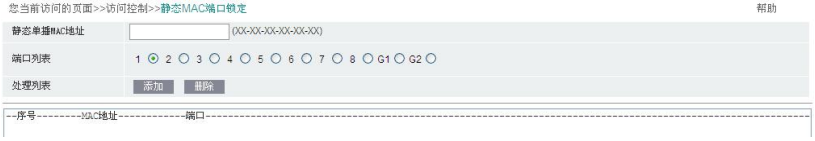


图 4-48　静态 MAC 端口锁定配置界面图

MAC 端口锁定的配置页面与静态组播表极为相似，操作方法也一致，只有一点区别就是前者是一对一的关系，就是说一个 MAC 地址只对应一个端口，而后者是一对多的关系。

静态单播 MAC 地址：在此方框中填入要添加的静态 MAC 单播地址，格式为 XX-XX-XX-XX-XX-XX，单播地址以 16 进制的 00 开头；

端口列表：选择此单播 MAC 地址的数据包的绑定转发端口，要转发至哪个端口，就将其选上即可，此处只允许选择一个端口。

处理列表：本栏目用于操作单播表，按钮 添加 和 删除 用来添加/修改和删除静态 MAC 地址。已存在的静态地址表项会显示在下面的表框中，每当用户打开本 Web 页面或者执行添加和删除的操作就会更新表框；

注意

1. 添加 和 删除 操作会立即生效，而不象其他页面需“保存”类似的操作；
2. 这个功能是一种安全机制，请谨慎确认设置，否则请慎用；
3. 请不要使用多播地址作为输入地址；
4. 请不要输入保留的 MAC 地址，如本机的 MAC 地址。

4. 7 监控报警

监控报警功能设置：SNMP 配置，Email 日志，继电器告警。

4.7.1 SNMP

简单网络管理协议（SNMP）由 Internet 工程任务组定义，是组成 Internet 协议的一部分。在关注某台网络设备的条件下，使用 SNMP 通过网络管理系统来监控网络设备。SNMP 协议由一系列标准网络管理、应用层协议、数据库、数据对象组成。SNMP 协议能够通过管理系统的窗体，显示管理数，如系统描述配置。这些配置描述可以通过一个支持 SNMP 的管理应用程序进行查询或设置。SNMP 协议基于 TCP/IP 协议，SNMP 通常使用 UDP 端口 161（SNMP）和 162（SNMP-Trap），SNMP 协议代理（SNMP Agent）存在于网络设备里，使用标准 MIBs（information specific to the device）作为设备接口，通过代理，这些网络设备可以被监控或控制。当一个 Trap 事件发生时，消息被 SNMP Trap 传输，此时，一个

可用的 Trap 接收器可以收到这个 Trap 消息。SNMP 的设置页面如图 4-49 所示。

图 4-49　SNMP 的配置界面图

SNMP 配置：启用或禁用 SNMP，默认为禁用。

只读团体名：用一个字符串来命名的 SNMP 团体名，该团体只有 get 操作的权限，默认为 public。

读写团体名：用一个字符串来命名的 SNMP 团体名，该团体有 get 操作和 set 操作的权限，默认为 private。

说明

上海纽琳克通信技术有限公司千兆工业以太网交换机支持 SNMP V1/V2C。SNMP V1 和 V2C 都使用公有字符串进行匹配认证，这意味着使用公有或私有字符串，SNMP 服务器允许只读方式或读写方式访问所有对象。SNMPV1、SNMPV2C 采用团体名认证。SNMP 团体（Community）用一个字符串来命名，称为团体名（Community Name）。SNMP 团体名用来定义 SNMP manager 和 SNMP Agent 的关系。团体名起到了类似于密码的作用，可以限制 SNMP manager 访问以太网交换机上的 SNMP Agent。

注意

1. 本交换机的 SNMP 不支持 SNMP Trap 功能，SNMP Trap 使用公开的 UDP 端口 162，本交换机使用私有的 7051 端口向上位机网管发送 Trap 包；
2. 本交换机的 SNMP Agent 支持标准 MIB-2 和 RMON 的一部份，且只能使用 get 操作；同时支持本公司私有的 MIBs，这部分 MIBs 可以采用 get 和 set 的操作，对交换机进行简单配置，但是私有的 MIBs 只具有 Web 网管的部分功能，建议用户不要使用；
3. 在 SNMP 浏览器中请注意读和写的权限问题，如果不能正常读写，请检查使用的团体名。

4.7.3 继电器告警

继电器告警配置功能包含网络风暴告警以及端口掉线告警。

网络风暴告警监控广播风暴和多播风暴。

端口掉线告警是监控对选定的告警端口是否掉线。

每种告警中有任何一种不处于正常状态，则产生继电器告警。配置页面如图 4-52 所示。

图 4-52 继电器告警配置页面

继电器告警：启用或禁用本功能，默认为禁用。

告警启用类型：选择需要监控的告警类型，勾选即可。

网络风暴告警：选择需要监控风暴的类型。

端口掉线告警：选择需要监控端口的类型。

当配置完成后，点击设置按钮立即生效。

当交换机监控的所有告警类型处于正常连接状态时，继电器常开，当任一种监控告警类型处于不正常状态时，继电器常闭，直到告警解除。

4.8 端口统计

端口统计功能设置：接收帧统计，发送帧统计，总流量统计，MAC 地址表。

4.8.1 接收帧统计

本交换机自动对每个端口进行监控，统计所有网络数据包，并在 Web 页面上显示这些统计数据，如图 4-53 所示。这些统计数据是自交换机上电以来的网络数据包的累计，当交换机软复位或断电重启后，这些数据将都被置零。

图 4-53　接收帧统计界面图

单播包：端口收到的地址为单播地址的数据包的个数。

多播包：端口收到的地址为多播地址的数据包的个数。

广播包：端口收到的地址为广播地址的数据包的个数。

丢弃包：端口收到的正常的但是因为安全控制的原因丢弃的包的个数。

暂停帧：端口收到的协议为 0x8808 的以太网控制帧，在全双工状态，该数据包是用来控制端口发送数据的频率。

超短帧：端口收到的包括 FCS 在内的长度小于 64 字节的包的个数。

超长帧：端口收到的包括 FCS 在内的长度大于 1518 或 1522（开启 VLAN）字节的包的个数。

错误的超短帧：端口收到的包括 FCS 在内的长度小于 64 字节 FCS 不正确或者非完整字符的包的个数。

错误的超长帧：端口收到的包括 FCS 在内的长度大于 1522 FCS 不正确或者非完整字符的包的个数。

错误的正常帧：端口收到的包括 FCS 在内的长度在 64 到 1518 或 1522（开启 VLAN）之间且 FCS 不正确或者非完整字符以及被检测到无效字符的包的个数。

4.8.2 发送帧统计

发送帧统计页面如图 4-54 所示。

端口	单播包	多播包	广播包	丢弃包	暂停帧	冲突检验	延迟发送	单次冲突	多次冲突	冲突丢弃
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	688	813	566	0	0	0	0	0	0	0
6	50	413	0	0	0	107	0	31	25	16
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
G1	0	0	0	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0	0	0	0

图 4-54　发送帧统计界面图

单播包：端口发送的地址为单播地址的数据包的个数。

多播包：端口发送的地址为多播地址的数据包的个数。

广播包：端口发送的地址为广播地址的数据包的个数。

丢弃包：端口发送的正常的但是因为资源不足原因或内部不满足解析条件丢弃的包的个数（不包括冲突丢弃的包）。

暂停帧：端口发送的协议为 0x8808 的以太网控制帧，在全双工状态，该数据包是用来控制端口发送数据的频率。

冲突检验：端口发送的数据时遇到的冲突的次数。

延迟发送：端口发送的数据时遇到的延迟发送的数据包的个数。

单次冲突：端口发送的数据时遇到的冲突的次数为 1 次且把数据成功传输出去的包的个数。

多次冲突：端口发送的数据时遇到的冲突的次数大于 1 次但仍然把数据成功传输出去的包的个数。

冲突丢弃：在冲突的次数大于 16 导致丢弃的包的个数。

4.8.3 总流量统计

总流量统计页面如图 4-55 所示。

端口	发送总字节	接收总字节	单播包总个数	多播包总个数	广播包总个数	错误包总个数
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	841503	108451	1162	1019	887	0
6	37306	43154	72	713	145	384
7	0	0	0	0	0	0
8	0	0	0	0	0	0
G1	0	0	0	0	0	0
G2	0	0	0	0	0	0

图 4-55 总流量统计界面图

发送总字节：端口发送所有数据包的总字节数目。

接收总字节：端口接收所有数据包的总字节数目。

单播包总个数：端口发送和接收地址为单播地址的数据包的个数。

多播包总个数：端口发送和接收地址为多播地址的数据包的个数。

广播包总个数：端口发送和接收地址为广播播地址的数据包的个数。

错误包总个数：端口发送和接收地址因为各种原因的错误的数据包的个数。

4.8.4 MAC 地址表

MAC（Media Access Control）地址是网络设备的硬件标识，交换机根据 MAC 地址进行报文转发。MAC 地址具有唯一性，这保证了报文的正确转发。每个交换机都维护着一张 MAC 地址表，如图 4-56 所示。在这张表中，MAC 地址和交换机的端口一一对应。当交换机收到数据帧时，根据 MAC 地址表来决定对该数据帧进行过滤还是转发到交换机的相应

端口。MAC 地址表是交换机实现快速转发的基础和前提。

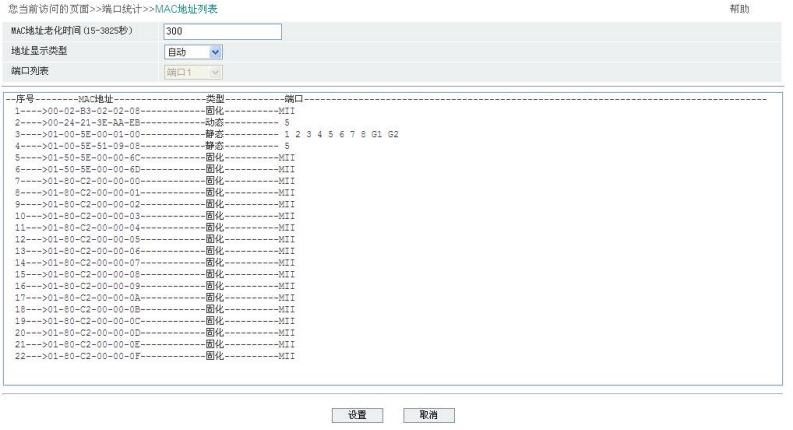


图 4-56　MAC 地址表界面图

MAC 地址老化时间：设置 MAC 地址老化时间间隔。

地址显示类型：指定 MAC 地址表的排序类型，可以选择“自动”和“端口”两种排序类型，选择“自动”时会将所有端口的所有 MAC 地址列出，选择“端口”则只会将相应端口的对应 MAC 地址列出。

端口列表：选择要显示的对应某个端口的 MAC 地址列表，本项只有在地址显示类型选项为“端口”时才会使能，选择“自动”时显示所有端口的所有 MAC。

本交换机的 MAC 地址分为以下三种类型：

- 动态 MAC 地址

此类地址在 MAC 地址列表中的类型字段为“动态”，动态 MAC 地址是交换机在网络中通过数据帧学习到的，当老化时间到来时会被删除。当设备所连接的交换机的端口发生变化时，MAC 地址表中相应的 MAC 地址和端口的对应关系也会随之改变。动态 MAC 地址在交换机断电重启后会消失，需要重新学习。

- 静态 MAC 地址

此类地址在 MAC 地址列表中的类型字段为“静态”，静态 MAC 地址是通过配置 IEEE 802.1X 认证后产生的，不会被交换机老化掉。不管设备所连接的交换机的端口发生怎样的变化，MAC 地址表中 MAC 地址和端口的对应关系始终不会改变，其关系完全由 IEEE 802.1X 认证服务器控制。静态 MAC 地址在交换机关电重启后也会消失。

- 永久静态（固化）MAC 地址

此类地址在 MAC 地址列表中的类型字段为“固化”，永久 MAC 地址也是通过配置产生的，不会被老化掉。不管设备所连接的交换机的端口发生怎样的变化，MAC 地址表中 MAC 地址和端口的对应关系始终不会改变。永久 MAC 地址在交换机关电重启后不会消失。

注意

1. 本设备中地址根据交换机的 MAC 地址计算索引，因此所有 MAC 的的显示中 VLAN 值均为 0；
2. 静态地址也可以在前面的静态 MAC 地址端口表中配置，端口变化时需要修改对应的表项；
3. 多播地址表的显示在 IGMP Snooping 多播列表中，此处地址表全是单播地址；
4. MAC 地址的默认老化时间为 300 秒（5 分钟），并且可通过 WEB 网管对老化时间进行设置。

4.9 网络诊断

网络诊断功能设置：端口镜像，网络 ping 诊断。

4.9.1 端口镜像

端口镜像功能就是将一个或多个端口的全部收发数据，拷贝至指定的另一端口。通过指定一个端口为其他端口的镜像端口，则可以通过此端口观察到其他端口的全部收发数据。端口镜像功能，通过用来对网络进行故障诊断、调试、分析。

本交换机端口镜像功能提供多个镜像规则，用户可以捕获入口、出口或所有数据。通过 Web 页面，可以进行镜像功能的相关动作。端口镜像就是将被监控端口上的数据复制到指定的监控端口，对数据进行分析和监视。以太网交换机支持多对一的镜像，即将多个端口的报文复制到一个监控端口上。用户可以指定受监控的报文的方向，如只监控指定端口发送的报文。本设备采用端口镜像组的方式来配置端口镜像功能。每个端口镜像组包含一个监控端口，和一组被监控端口。本功能的配置页面如图 4-57 所示。

图 4-57　端口镜像配置界面图

端口镜像：启用或禁用端口镜像功能，默认为禁用。

被镜像端口：指数据被收集端口，概念易混淆，从镜像的功能上理解就是指收发数据将被拷贝的端口，可以设置若干个。

镜像端口：指收集数据的端口，从镜像的功能上理解就是指收集被拷贝的数据的端口，只能选择一个，也就是同时只能存在一个镜像端口。

端口镜像模式：指采集数据的方向选择，是进口还是出口数据，也可以是全部数据，进和出的概念是针对采集端口来定义，而不是从镜像端口的角度来形容。

注意

1. 本功能必须在正常使用中被关闭，否则所有基于端口的高级管理功能均无法使用。如 RSTP，IGMP Snooping；
2. 镜像功能只处理 FCS 正常的包，不能处理各种错误的数据帧；
3. 端口镜像模式，是进口数据还是出口数据，也可以是全部数据，进和出的概念是针对交换机的交换芯片来定义，而不是从镜像端口的角度来形容。
4. 端口镜像功能一般用于诊断和调试功能，一般情况下建议慎用。

4.9.2 网络诊断

本交换机支持诊断功能，即进行网络故障分析、网络测试或问题解决。配置页面如图 4-58 所示。

图 4-58　Ping 测试配置界面图

Ping 功能使用简单的 ping 指令，给用户一个简单有力的网络问题诊断工具。这个功能最独特之处是可以通过 Web 页面输入一个 ping 指令，由交换机自己发送一个 ping 指令，并把结果输出到 Web 页面上。以这种方式，用户能方便的控制交换机向外发送 ping 命令并输出结果。

Ping 功能各设置项目如下表 4-6 所示。

表 4-6　Ping 功能设置描述表

设置项目	描　述	默认值
目的主机	Ping 的 IP 地址	Blank
报文大小	Ping 包的长度	60(字节)
报文数目	发送 Ping 包的数量	1(个)
报文间隔	发送 Ping 包的间隔	1000(毫秒)
应答超时	Ping 溢出时间	5000(毫秒)

注意

1. 在使用 ping 网络诊断功能之前，应确保目的主机 windows 防火墙的本地连接 ICMP 设置中的第一项“允许传入的回显请求”被勾选，否则该目的主机将无法被 ping 通；
2. “目的主机”的域名不支持无限扩展，只支持三级以下的域名，如“mail.sina.com”；
3. 出现全部“Request timeout”提示，则说明对方网卡工作不正常或网络线路有故障；
4. Ping 域名若出现“unknown host name”提示信息，则说明 DNS 配置出错；
5. Ping 域名若出现“Request timeout”提示，就说明网关设置有错误。

4.10 系统管理

系统管理功能设置：时间配置，设备地址，系统信息，日志信息，文件管理。

4.10.1 时间配置

通过时间配置功能设置交换机的系统时间。本交换机没有后备电池保存系统时间值，当其断电时，系统时间即丢失，上电重启后，交换机的系统时间即为 linux 的时间，为 1970 年 1 月 1 日，所以当每次上电重启交换机后都必须同步一下交换机时间。时间配置页面如图 4-59 所示。

图 4-59 时间配置界面图

时间配置：本交换机提供两个不同时间配置选项：本地时间和使用 NTP。

本地时间：本地时间（Local time）是使用用户设置的时间，一般是使用访问本页面的 PC 时间，当用户选择此项并点击“设置”时，会在最下面出现 更新时间至交换机 按钮，点击后就会将访问 PC 时间更新至交换机。

使用 NTP：使用 NTP 就是交换机自动与 Internet 上的时间服务器进行时间同步。NTP（The Network Time Protocol）是一个网络时间同步协议，使用 UDP 协议和 123 端口，NTP 协议可以抵制不稳定的网络反应时间，来提高校正时间的精度。

世界时区：世界时区的划分以本初子午线为标准。从西径 7.5°到东经 7.5°(经度间隔为 15°)为零地区。由零时区的两个边界分别向东和向西，每隔经度 15°划一个时区，东、西各划出 12 个时区，东十二时区与西十二时区相重合；全球共划分成 24 个时区。各时区都以中央经线的地方平太阳时作为本区的标准时。相邻两个时区的标准时相差一小时。时区界线原则上按照地理经线划分，但在具体实施中往往根据各国的行政区界或自然界线来确定，

以方便使用。

设备中可以根据典型的地域选择相关的时区，设备根据选择的时区自动调整内部时间的偏移。

自动调整夏令时：自动调整夏令时：夏令时比标准时早一个小时。例如，在夏令时的实施期间，标准时间的上午 10 点就成了夏令时的上午 11 点。夏令时，又称“日光节约时制”或“夏时制”，是一种为节约能源而人为规定地方时间的制度。目前全世界有近 110 个国家每年要实行夏令时，当选择特定的地域时，如果该地区允许“夏令时”，则该选项可设置，否则灰化无效。

NTP 服务器：可以提供 NTP 时间服务的主机名或 IP 地址，可以为空。

系统时间：设备自身的当前系统时间，上电后为为“1970 年 1 月 1 日 0:00:10 星期四”，可手动更新本地时间至交换机或自动使用 NTP 更新。

PC 时间：访问 Web 服务器的 PC 的系统时间，当选择本地时间时，会出现 更新时间至交换机 按钮，点击就会将此时间更新至交换机。

注意

1. 使用 NTP 时，NTP 服务器可以为空，交换机要能接入互联网，使用公开的互联网 NTP 服务器；
2. 更新时间至交换机 按钮只有在用户选择本地时间，并点击“设置”后才会弹出，当用户切换至使用 NTP 时，也必须在点击“设置”后才会消失；
3. 只有“管理员“才有权限手动配置设备的时间；
4. 时区和夏令时必须配置，无论是使用“本地时间”还是“NTP 时间”；
5. NTP 服务器或者访问者的 PC 的时间配置可能会导致显示不正常，可以改变“时间显示”格式来调整显示。

4.10.2 设备地址

这个功能将分配一个 IP 地址给交换机。通常 IP 地址有两种分配方式：自动分配（DHCP）或指定一个 IP 地址。本交换机出厂默认使用固定的 IP 地址，IP 地址为 192.168.16.253。配置页面如图 4-60 所示。

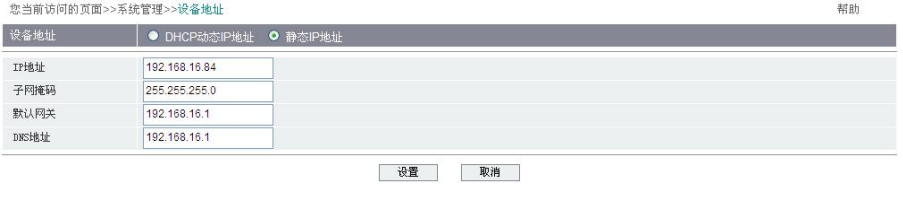


图 4-60 设备地址配置界面图

DHCP 动态 IP 地址：使用 DHCP 协议，从 DHCP 服务器动态分配一个 IP 地址，需要网络中有 DHCP 服务器，建议用户不要使用，因为访问 Web 服务器需要明确知道交换机的 IP 地址，而动态的 IP 地址在分配之前无法确定，而且每次重启都可能分配一个新的 IP 地址。

静态 IP 地址：手工设置一个固定的静态 IP 地址，建议用户使用此选项，手工设置一个固定的 IP 地址，方便 Web 网管的使用，设置的 IP 地址不能有冲突。

IP 地址：IP 地址是分配给连接在 Internet 上的设备的一个 32 比特长度的地址。IP 地址由两个字段组成：网络号码字段（net-id）和主机号码字段（host-id）。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。为了方便 IP 地址的管理，IP 地址分成五类。如下所示：

网络类型地址范围用户可用的 IP 网络范围

A	0.0.0.0～127.255.255.255	1.0.0.0～126.0.0.0
B	128.0.0.0～191.255.255.255	128.0.0.0～191.254.0.0
C	192.0.0.0～223.255.255.255	192.0.0.0～223.255.254.0
D	224.0.0.0～239.255.255.255	无
E	240.0.0.0～247.255.255.255	无

其他地址 255.255.255.255

其中 A、B、C 类地址为单播（unicast）地址；D 类地址为组播（multicast）地址；E 类地址为保留地址，以备将来的特殊用途。目前大量使用中的 IP 地址属于 A、B、C 三类地址。

IP 地址采用点分十进制方式记录。每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.110.50.101。

子网掩码：掩码是一个 IP 地址对应的 32 位数字，这些数字中一些为 1，另外一些为 0。原则上这些 1 和 0 可以任意组合，不过一般在设计掩码时，把掩码开始连续的几位设置为 1。掩码可以把 IP 地址分为两个部分：子网地址和主机地址。IP 地址与掩码中为 1 的位对应的部分为子网地址，其他的位则是主机地址。A 类地址对应的掩码为 255.0.0.0；B 类地址的掩码为 255.255.0.0；C 类地址的掩码为 255.255.255.0。

使用掩码把一个可以包括 1600 多万主机的 A 类网络或 6 万多台主机的 B 类网络分割成许多小的网络，每一个小的网络就称之为子网。

默认网关：主机里的默认网关通常被称作默认路由。默认路由（Default route），是对 IP 数据包中的目的地址找不到存在的其他路由时，路由器所选择的路由。目的地不在路由器的路由表里的所有数据包都会使用默认路由。这条路由一般会连去另一个路由器，而这个路由器也同样处理数据包，如果知道应该怎么路由这个数据包，则数据包会被转发到已知的路由；否则，数据包会被转发到默认路由，从而到达另一个路由器。

DNS 地址：DNS 的全称是 Domain Name Server，作用是将便于我们记忆的域名，解析成 Internet 可以识别的 IP 地址。如果我们设备需要访问某个主机名，则需要利用这个服务器解析成 IP 地址。

每当用户修改地址设置后需点击 设置 按钮才会提交至交换机，并切换进一个如图 4-61 所示的等待页面。

图 4-61 用户修改地址后的等待界面图

当画面中的进度条完毕后，交换机即使用新的 IP 地址并重启 Web 服务器。

注意

1. 我们可以设置的 IP 地址范围应该为 192.168.x.x，172.[16-31].x.x 或 10.x.x.x；
2. NTP 和 Email 将利用到 DNS 服务，如果应用这两个服务，请务必填写正确的 DNS 地址。

4.10.3 系统信息

通过图 4-62 所示的页面用户可以了解交换机的系统相关信息，设置交换机的名称。

图 4-62　系统信息配置界面图

设备名称：为标示网络中的每个交换机，给每个交换机取一个不同的名称，以便区分，并支持中文输入，交换机名称最长不超过 16 个字节。

设备位置：由客户自定义交换机的位置编号。

设备编号：描述交换机出厂编号，出厂时由厂家设定，用户不能修改。

设备描述：即交换机的型号，由硬件决定，用户不能修改。

内存使用：本栏目描述了交换机系统内存 RAM 的使用情况。

CPU 信息：本栏目描述了交换机系统主 CPU 的基本信息。

4.10.4 日志信息

设备提供日志功能，以供使用者参考可能遇到设置问题。当启用这个功能时，交换机将记录发生的相关事件，并保存至日志信息文件中，日志功能保存所有的记录到 SDRAM 里，最多可存储 2000 条记录，当超过 2000 条记录时，老的记录将会自动被删除，新的记录被添加。以下事件会被保存至日志文件中：

- 系统重启
- 端口 Link Down/Up
- 登录信息
- 广播风暴发生时
- 系统动作和操作记录
- NTP 时间同步信息
- 其他一些系统信息

日志信息页面如图 4-63 所示。

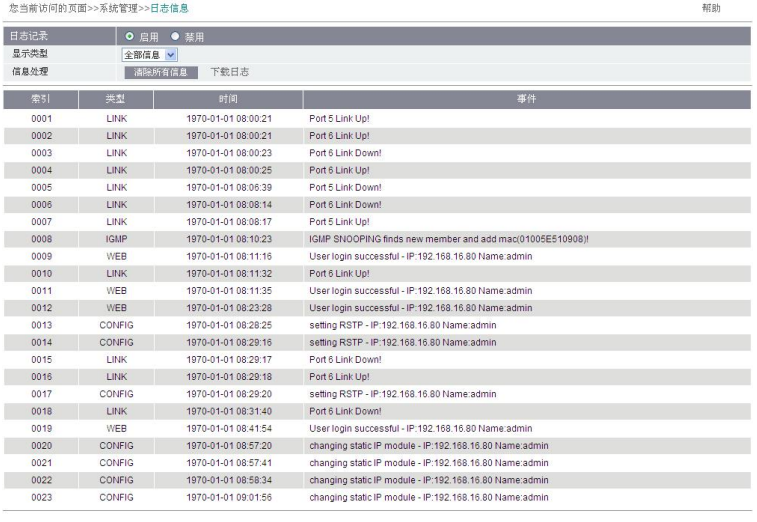


图 4-63　日志信息界面图

日志记录：启用或禁用日志记录功能，默认为启用，日志功能禁用后并不会删除日志内容，只是不再添加新的日志信息。

显示类型：显示某一类型的信息，可以在“全部信息”、“操作信息”、“连接信息”切

换。

清除所有信息：点击此按钮即清除掉所有日志信息。

下载日志：点击此按钮即从 Web 服务器下载日志信息，并保存至 PC 上，文件名称为 syslog.cfg，请使用浏览器直接下载，本交换机的 Web 服务器不支持迅雷等多线程下载工具。

4.10.5 文件管理

文件管理页面如图 4-64 所示。此页面对交换机进行一些非常规的系统操作，建议用户谨慎使用，操作不当可能损坏交换机。只有“管理员”才能执行这些操作。

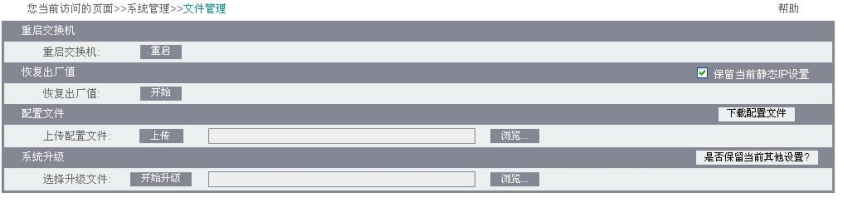


图 4-64 文件管理界面图

重启交换机：本操作用于软件重启交换机，在交换机完全重启成功之前，本交换机不起作用，不能转发任何数据包，这种重启有别于上电重启的硬件复位，只是交换机系统软件复位，就象 windows 操作系统的“热启动”。本功能的最大好处是提供一种远程重启交换机的功能，用户只要能远程访问到交换机就可以将其远程重启。单击 重启 按钮，即转至一个如图 4-65 所示的重启等待页面。

图 4-65　设备重启的等待界面图

当画面中的进度条完毕后，交换机即软件复位完毕。

恢复出厂值：本操作用于将交换机恢复成出厂设置，同时自动重启交换机，当交换机重启成功之前，本交换机不起作用，不能转发任何数据包。本功能是当用户一旦设置了错误的参数导致交换机工作不正常时，可以恢复为出厂默认配置值。出厂默认的 IP 地址为：192.168.16.253，当恢复出厂设置成功后，用户需要用此 IP 地址访问 Web 服务器。单击 开始 按钮，即转至一个如图 4-66 所示的等待页面。

图 4-66　设备恢复出厂值的等待界面图

当画面中的进度条完毕后，交换机即恢复出厂设置并重启完毕。

配置文件：本操作允许用户将本交换机的当前所有配置保存成一个文件，可以用此配置文件来备份和恢复交换机的所有配置。本功能可以让用户很方便的用一个配置文件很快的配置多台交换机。单击 下载配置文件 按钮，即可以将此配置文件下载至访问 PC 上，文件名称为：Switchcfg.cfg，本交换机不支持迅雷等多线程下载工具，请使用浏览器直接下载。要上传一个配置文件，需先点击 浏览... 按钮选择一个文件，请注意一定不要选择非交换机的配置文件，上传错误的文件可能造成交换机的损坏，点击 上传 按钮，即转至一个如图 4-67 所示的等待页面。

图 4-67　设备重新设置的等待界面图

当画面中的进度条完毕，交换机即用新的配置设置并重启交换机。本操作过程不能断电，否则可能损坏交换机。

系统升级：本操作用于对交换机的内核程序进行一次系统升级，用户可以通过邮件或本公司网站得到交换机的升级程序，请注意设备型号及版本的匹配，使用不匹配的升级程序可能导致交换机永久损坏。用户得到升级程序后单击 浏览... 按钮选择该升级程序，再单击 开始升级 按钮，即转入如图 4-68 所示的等待页面。

图 4-68　设备系统升级的等待界面图

当画面提示升级成功后，交换机即升级完毕，交换机升级后会自动恢复出厂设置，并重启。请注意，整个升级过程不能断电，否则可能损坏交换机。

注意

1. 恢复出厂值设置将导致设置的所有状态处于刚出厂的状态，其设置的 IP 是静态 IP 地址“192.168.16.253”，用户需用此 IP 地址才能访问 Web 服务器；
2. 上传配置文件操作中，一定不要选择非交换机的配置文件，上传不正确的文件可能造成交换机的损坏；
3. 上传配置文件操作过程不能断电，否则可能损坏交换机；
4. 上传配置文件时，新配置中如果静态的 IP 不在同一网段将导致网页无法刷新，原因

是无法重登录 Web 服务器；

5. 上传配置文件时，新配置中使用动态 IP 设置但网段中没有 DHCP 服务器，将导致 IP 相关的部分不会被更新；
6. 升级时，请注意设备型号及版本的匹配，使用不匹配的升级程序可能导致交换机永久损坏；
7. 整个升级过程不允许断电，断电可能造成交换机永久损坏，升级过程中如意外断电请立即将产品邮寄到本公司以寻求可能的解决方法。
8. 若设置紊乱，可考虑将交换机恢复出厂设置，则可以重新设置。切记恢复出厂设置后的 IP 为：192.168.16.253，最好修改交换机的 IP，以免发生冲突，影响使用。

第五章 维修和服务

自产品发货之日起，上海纽琳克通信技术有限公司提供五年产品质保。依据上海纽琳克通信技术有限公司产品规范，在质保期间，如果产品有任何故障或功能操作失败，上海纽琳克通信技术有限公司将无偿为用户维修或替换该产品。但以上承诺并不覆盖由于不正当使用、意外事故、天然灾难、不正确的操作或不正确的安装所造成的损坏。

为确保消费者受益于上海纽琳克通信技术有限公司的系列产品，通过下面的方式可以得到帮助和问题解决：

- Internet 服务
- 打电话到技术支持办公室
- 产品返修或更换。

5.1 INTERNET 服务

通过上海纽琳克通信技术有限公司网站技术支持部分，可以得到更多有用的信息和使用技巧。

5.2 技术支持电话服务

使用上海纽琳克通信技术有限公司产品的用户，可以打电话到上海纽琳克通信技术有限公司技术支持办公室，上海纽琳克通信技术有限公司有专业的技术工程师回答您的问题，帮助您在第一时间解决您遇到的产品或使用问题。

5.3 产品返修或更换

产品维修、更换或退货，按照上海纽琳克通信技术有限公司公司的处理程序，应先和上海纽琳克通信技术有限公司的技术人员进行确认，然后再和上海纽琳克通信技术有限公司销售人员进行协商处理，来完成产品的维修、更换或退货。

附　录

1. SNMP 性能参数

本交换机提供 SNMP 代理来管理交换机设备，本交换机支持下面 RFCs：

RFC 1157 – SNMP protocol
RFC 1213 – MIB-2
RFC 1573 – IF-MIB
RFC 1643 – Interface MIB
RFC 2819 – RMON