GigaX2024/2048

二层网管型交换机

用户手册

C2301

2006 年 2 月 V2.3

华硕联络信息

华捷联合信息（上海）有限公司（莘庄）

电话: 021-54421616
传真: 021-54420066/88/99
地址: 上海市莘庄工业区春东路508号
邮编: 201108

华捷联合科技(广州)有限公司

电话: 020-85572366
传真: 020-85572352/55
地址: 广州市中山大道西高新技术工业园建工路12号1-2楼
邮编: 510665

华捷联合信息(上海)有限公司成都办事处

电话: 028-82916655/56
传真: 028-82916659
地址: 成都市一环路南三段22号世纪电脑城三楼B座
邮编: 610041

华捷联合信息(上海)有限公司沈阳办事处

电话: 024-23988728
传真: 024-23988563
地址: 沈阳市和平区南三好街55号沈阳信息产业大厦1808号
邮编: 110004

华捷联合信息(上海)有限公司北京海淀分公司

电话: 010-82667575
传真: 010-82689352
地址: 北京市海淀区海淀路52号太平洋科技大厦12层
邮编: 100080

华硕技术支持:
免费咨询电话: 800-8206655（7*24小时人工接听）
Email: tsd@asus.com.cn
Netq论坛: Netq.asus.com.cn由华硕工程师提供在线服务

目录

图片目录

表格目录

1 简介

感谢您购买华硕 GigaX2024/2048 二层网管型交换机！您可以通过友好且功能强大的用户界面来管理您的局域网（LAN，local area network）。

本用户手册将向您介绍如何安装 GigaX2024/2048 交换机，以及如何配置交换机以获得更多的功能。

1.1 GigaX2024/2048 特色

- (GigaX 2048) 48 x 10/100BASE-TX 自适应高速以太网端口
- (GigaX 2024) 24 x 10/100BASE-TX 自适应高速以太网端口
- 两个 10/100/1000BASE-T 自适应千兆以太网交换端口
- 两个小型 (SFP) 千兆端口转换 (GBIC) 插槽
- 10/100BASE-TX 和 10/100/1000BASE-T 端口均支持自适应 MDI/MDIX
- 兼容 802.3u, 802.3z 和 802.3ab 规格
- 802.1D 透明桥接 / 生成树协议
- 802.1w RSTP (Rapid Spanning Tree Protocol)
- 802.1X 基于端口的网络访问控制
- RADIUS 远程认证拨号用户服务
- 8K MAC 地址缓存，基于硬件的地址老化时间
- 802.3x 流量控制
- 基于 802.1Q 标记的 VLAN, 最多支持 255 组 VLAN
- 802.1p 服务级别 , 每端口支持 4 个队列
- 支持 IGMP 侦测
- 802.3ad 链路汇聚（干线），最多支持 6 个干线群组
- LACP (Link Aggregation Control Protocol，链路汇聚控制协议）
- 端口镜像
- ACL(访问控制列表)
- RMON: 支持 4 个群组 (1, 2, 3, 9)
- SNMP v1, v2, v3
- MIB-II
- 企业 MIB: 电源、风扇、系统及电压

- Telnet/SSH2 远程登录
- 通过 FTP 进行固件升级和设置备份
- IEEE 802.1x 认证 (具有动态 VLAN 分配)
- DHCP 侦测
- 系统日志
- 通过控制终端、telnet 和 SSH 界面的命令行翻译器
- 网页图形界面 (GUI)
- 端口链路状态 LED 指示灯
- 系统、冗余电源 (RPS) 和风扇 LED 指示灯

1.2　手册使用说明

1.2.1　表示意义

- 缩写意义将在首次出现以及术语表中列出。
- 为简洁起见，GigaX 交换机简称“交换机”。
- 术语“LAN (局域网)”和“网络”将交替使用，表示某个区域内通过以太网连接的一组计算机。
- 如果没有特别说明，手册中的图片和网页界面屏幕截图同时适用于 GigaX 2048 和 GigaX 2024 机型。

1.2.2　排版字体

粗体字表示该文字是您从菜单或下拉菜单中选择的项目，或是程序提示字串。

1.2.3　符号说明

本用户手册使用以下图标表示特殊信息，以此引起用户的注意。

注意: *提供对当前叙述内容的说明或额外信息。*

定义: *解释用户可能不了解或不熟悉的术语或缩写。这些术语均可在术语表中查到。*

警告: *高重要性的信息，包括涉及人身安全或系统完整性的信息。*

2　认识 GigaX

2.1　包装内容

GigaX 2024/2048 交换机包装内包含以下内容:

- GigaX 2048 (48 端口) 或 GigaX 2024 (24 端口) 二层网管型交换机
- AC 电源线
- 控制终端连接线 (DB9)
- 机架安装工具包 (两个挂钩和六个 #6-32 螺丝)
- USB 线，用于控制终端接口
- 安装光盘
- 快速安装指南

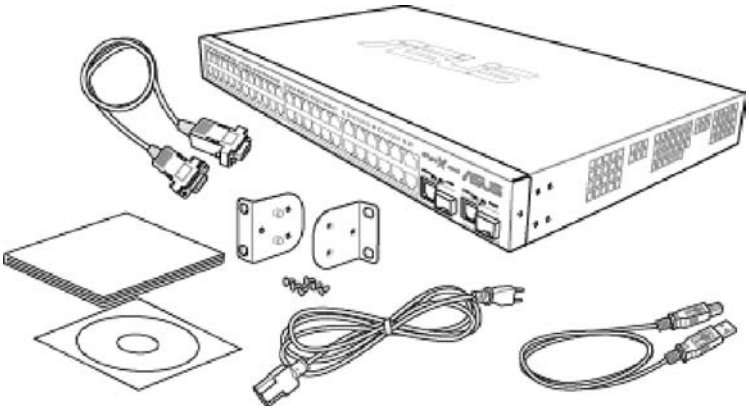

图 1. GigaX 二层网管型交换机包装内容

2.2　前面板

前面板包含 24/48 个 RJ-45 10/100Base-T 端口，2 个 10/100/1000Base-T 端口，2 个 SPF GBIC 端口，以及一组 LED 指示灯，用来显示系统、冗余电源、风扇和端口的状态。

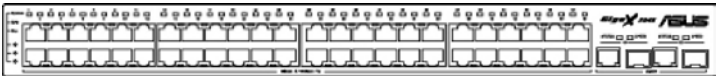

图 2. 前面板（GigaX 2048）

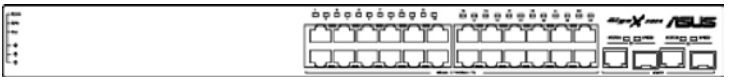

图 3. 前面板（GigaX 2024）

表 1. 前面板标识和 LED 指示灯

标识	颜色	状态	描述
SYSTEM	绿色	亮灯	系统电源已开启
		闪烁	自检，初始化或正在下载
	琥珀色	亮灯	温度或电压不正常
	熄灭		没有电源
RPS	绿色	亮灯	电源 (PSU) 工作正常，且交换机有良好的冗余电源供应
	琥珀色	亮灯	电源工作不正常，交换机正通过冗余电源 (RPS) 供电
	熄灭		没有电源（系统 LED 指示灯也熄灭）；冗余电源 (RPS) 工作不正常或没有安装（系统 LED 指示灯亮）
FAN	绿色	亮灯	两个风扇工作正常
	琥珀色	亮灯	两个风扇有一个或全部停止
10/100 ports	绿色	亮灯	以太网连接已建立
		闪烁	正在传送 / 接收数据
	熄灭		未建立以太网连接
10/100/1000 port status	绿色	亮灯	连接 (RJ-45 或 SFP) 已存在；端口可用
		闪烁	正在传送 / 接收数据
	琥珀色	亮灯	连接已存在，但是端口被手动或生成树禁用
		闪烁	端口处于 STP 阻塞、侦听或学习状态
	熄灭		没有建立以太网连接
10/100/1000 port speed	绿色	亮灯	1000Mbps
	琥珀色	亮灯	100Mbps
	熄灭		10Mbps

2.3 后面板

交换机的后面板包含了风扇模组、一个电源接口、两个终端控制接口（USB 和 DB9）和一个冗余电源 (RPS) 接口。

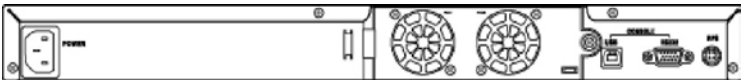

图 4. 后面板

表 2. 后面板标识

No.	项目	描述
1	电源接口	连接电源线
2	FAN1-FAN2	可置换的系统风扇
3	RS232 终端控制接口	用于终端管理的 RS232 串行端口
4	USB 终端控制接口	用于终端管理的 USB 端口
5	RPS	冗余电源接口

2.4 技术规格

表 3. 技术规格

物理尺寸	43.5mm(高) x 444 mm(宽) x 265mm(深)		
电源	输入	功耗	
	100-240V AC/ 2.5A 50-60Hz	< 90 瓦	
冗余电源 (RPS)	输入	输出	
	100-240V AC/ 1.8A 50-60Hz	12V DC/12.5A	
环境		操作	存储
	温度	-10 ~ 50°C (14 ~ 122°F)	-40 ~ 70°C (-40 ~ 158°F)
	湿度	15 ~ 90%	0 ~ 95%
	海拔	最高 3,000 米	最高 12,000 米
可置换式风扇	尺寸	电压和电流	速率
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

3　快速设置指南

本章节将介绍如何设置交换机的工作环境。您也可以参考 GigaX 2024/2048 的安装指南。

第一部分阐述如何将 GigaX 2024/2048 交换机安装在水平表面上或机架上。

第二部分阐述设置硬件的步骤。

第三部分阐述 GigaX 2024/2048 交换机的基本设置步骤。

在开始进行安装和设置之前，请先向网络管理员获取如下信息:

交换机的 IP 地址

网络的默认网关

网络的子网掩码

3.1　第一部分 — 安装硬件

3.1.1　将交换机安装在水平表面上

交换机可以安装在水平的，能够承受交换机及其附件重量的表面上。请将四个橡胶垫粘贴在交换机的底部。

3.1.2　将交换机安装在机架上

1. 将挂钩上的孔与交换机侧面的孔对准。
2. 用三颗螺丝将挂钩固定到交换机的一侧。
3. 重复上述步骤固定交换机另一侧的挂钩。
4. 用四个机架安装螺丝将交换机安装到机架上 (包装中没有提供机架安装螺丝)。

3.2　第二部分 — 安装交换机

3.2.1　连接控制终端接口

在使用控制终端对交换机进行管理之前，请使用 RS232 (DB9) 或 USB 线（需要安装随机光盘中的 USB 驱动） 连接交换机。若您想使用网页界面进行设置，请用以太网线连接您的 PC 和交换机。

3.2.2　连接计算机或局域网（LAN）

您可以使用以太网线将计算机、集线器和其他交换机连接到 GigaX 2024/2048 的交换端口。交叉型和直通型以太网线都可以用来连接这些设备。

请使用 5 类以太网线连接 1000BASE-T 端口。否则，连接速度不能达到 1Gbps。

3.2.3　连接冗余电源（RPS）模块

将冗余电源 (RPS) 模块（选购）连接到交换机后面板的 RPS 接头，并确保 RPS 的另一端连接了电源线。将电源线插到电源插座上。

3.2.4　连接电源适配器

1. 将 AC 电源线的一端插入交换机后面板的 POWER 接口，另一端插入电源插座。
2. 按照表 4 中的描述检查前面板的 LED 指示灯状态。若 LED 指示灯点亮，如表中描述，则代表交换机的硬件已经工作正常。

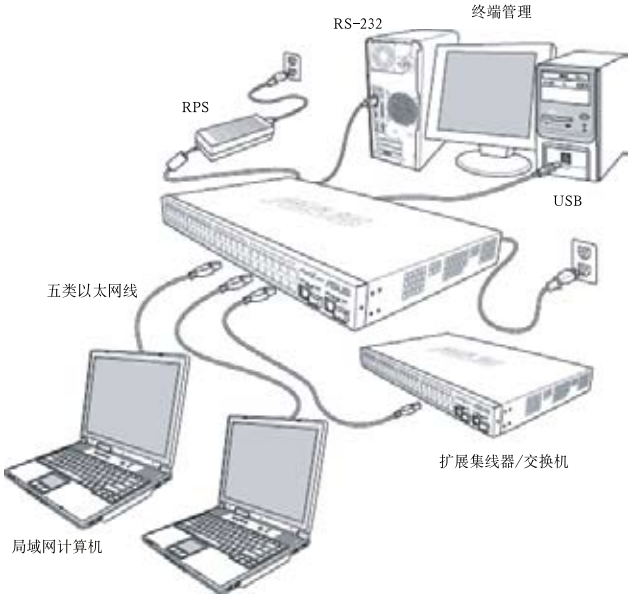

图 5. 硬件连接图

表 4. LED 指示灯

No.	LED	描述
1	System	稳定的绿色代表交换机已经开启。如果 LED 熄灭，请检查电源适配器是否已正确连接到交换机和外部电源插座。
2	Switch ports [1] to [50] (2048) [1] to [26] (2024)	稳定的绿色代表交换机和其他设备之间的连接已经建立。闪烁代表交换机正在传送数据。
3	RPS	稳定的绿色代表冗余电源（RPS）模块已正确安装。
4	Fan	稳定的绿色代表所有的风扇工作正常。

3.3　第三部分 — 基本管理设置

完成硬件连接后，您需要为交换机进行基础设置。您可以选择以下方法进行设置:

- 网页界面: 本交换机提供网页设置界面，您可以使用带 Java® 的 IE5.0 或更高版本的浏览器进行设置。
- 命令行界面: 使用控制终端接口来设置交换机。

3.3.1　通过控制终端进行设置

1. 请使用附带的 RS-232 交叉线连接交换机后面板的控制终端接口。这个接口为 DB-9 公接口，专门用于数据终端设备 (DTE) 的连接。将缆线接头上的紧固螺丝固定在控制终端接头上，将缆线的另一头连接到具备终端仿真软件，如 Hyper Terminal 的计算机上。
2. 使用 USB 线将交换机连接到 PC。在连接前您必须首先安装随机光盘中的 USB 驱动程序。USB 驱动可以在 Windows Me/2K/XP 系统下模拟额外的一个 COM 口。
3. 请确认控制终端的仿真软件的设置如下:

   a) 选择合适的串列端口号
   b) 将数据传输波特率设为 9600
   c) 将数据格式设为无配类， 8 位数据，1 位停止
   d) 无流量控制
   e) 将仿真模式设为 VT1000
4. 控制终端设置完毕后，您可以看到终端显示 “(ASUS)%” 提示符。
5. 键入 “login” 进入命令行界面。默认的用户名为 “admin”。按 <Enter> 跳过密码。

您可以通过命令行界面更改密码（参见 5.3.1）。为了保护您的交换机防止未授权用户登录，您需要尽快更改密码。

6. 请按照下列步骤为交换机配置 IP 地址:

a) 键入 net interface ip sw0 < **您的 IP 地址** > < **您的网络掩码** >。例如，若您的交换机的 IP 地址为 192.168.10.1，网络掩码为 255.255.255.0，则您需要键入 net interface ip sw0 192.168.10.1 255.255.255.0。

b) 若交换机需要跨网络管理，则需要设置默认网关或静态路由。键入 net route static add 0.0.0.0 < **您的网关** IP> 0.0.0.0 1 设置您的默认路由，如图 6 所示。

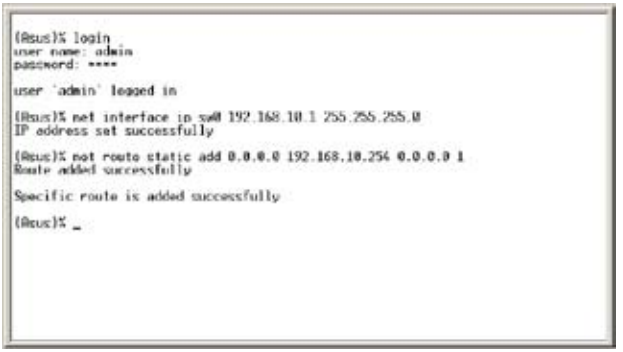

图 6. 登录和 IP 设置界面

3.3.2 通过网页界面进行设置

为了将计算机正确地与交换机相连，您的计算机必须具备一个在网络中有效的 IP 地址。请与您的网络管理员联系为交换机获取 IP 地址。如果您希望改变交换机的默认 IP 地址，请参见 3.3.1 章节。

1. 首次使用时不需要登录网页界面，因为默认情况下，网页访问认证是禁止的。为了保证系统设置的安全性，请在 System 下的 Administration 页面开启认证功能。若您选择了禁止登录认证，请跳过第 2 步。

2. 在交换机已连接且能访问的任何一台 PC 上，打开网页浏览器 (Internet Explorer)，然后在地址栏内键入以下 URL，并按下 <Enter>:

http://192.168.1.1

这是交换机出厂时的默认 IP 地址。

如图 7 的登录窗口将出现。

图 7. 登录

键入用户名和密码，然后按 OK 进入设置界面。当您第一次登录时，请使用默认用户名和密码:

默认用户名: admin

默认密码:（**无**）

您可在任何时间对密码进行修改（见 5.3.1 系统命令）

3. 设置新的 IP 地址时，点击 System，然后点击 IP Setup 页面（见图 8）。填入 IP 地址、网络掩码和默认网关，然后按 OK。
4. 如果交换机采用了新的 IP 地址，浏览器不能自动更新交换机的状态窗口，也不能退回之前的设置页面。您需要重新在网页地址栏中键入新的 IP 地址，然后按 <Enter>, 重新进入网页设置界面。
5. 要开启网页访问认证功能，请在菜单中点击 Administration，然后选择 Enabled 开启此项保护 。
6. 点击 OK 后，登录窗口会立即出现。图片见下页。

注意：除了顶部栏显示的前面板图片之外，GigaX 2048 和 2024 机型的网页界面是相同的（图片见下页）。

在下面的部分中，如果两个机型对应界面的内容相同，则只显示一幅图片（GigaX 2048 机型）。若两者存在区别，则会显示 GigaX 2048 和 2024 两幅图片。

图 8. IP 设置（GigaX 2048）

图 9. IP 设置（GigaX 2024）

4　网页界面下的设置

GigaX 2024/2048 交换机提供网页设置界面，这样您就可以通过网络对交换机进行设置。这个功能推荐配合带有 Java® 的 Microsoft Internet Explorer 5.0 及以后版本使用。 **注意**：不支持 Netscape。

4.1　登录到网页设置界面

1. 打开计算机上的浏览器，在地址栏内键入下列内容，然后按 <Enter>:

   http://192.168.1.1

   这是交换机出厂时默认的 IP 地址。图 10 显示的是登录窗口。

图 10. 设置界面登录窗口

若您没有启用网页访问认证功能，则不需要登录。(见 3.3.2)

2. 输入用户名和密码，然后按 OK。

   当您第一次登录到网页界面时，请使用下列默认参数。您可在命令行界面下随时更改密码。(请参考 57 页 5.3.1 的内容)

   默认用户名：admin

   默认密码：< 无 >

   每当您登录到网页设置界面时，您都会看到设置主页。(见图 11 和 12)。

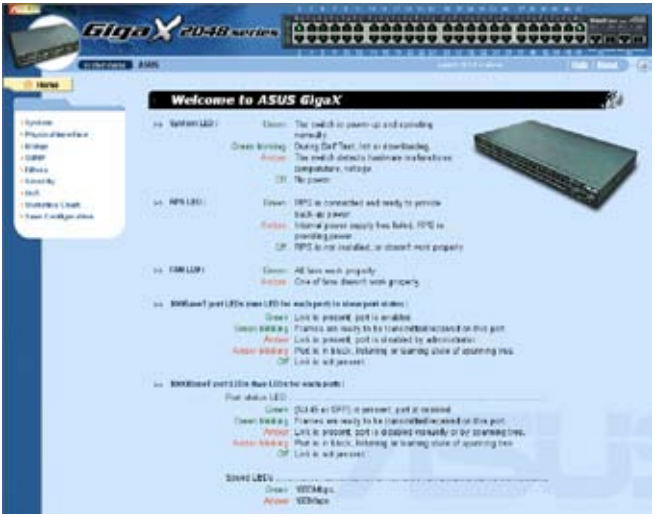

图 11. 主页（GigaX 2048）

图 12. 主页（GigaX 2024）

4.2　功能结构图

GigaX 2024/2048 交换机的网页设置界面分为三个部分。顶部栏包括了交换机的 logo 和前面板，如图 13 和图 14 所示。顶部栏将一直出现在设置过程中，并且每隔一段时间更新 LED 状态, 见表 4 中 LED 的表示意义以及表 5 的 LED 颜色意义。

图 13. 顶部栏（GigaX 2048）

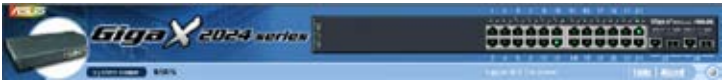

图 14.　顶部栏（GigaX 2024）

表 5. 端口颜色描述

端口颜色	描述
绿色	以太网连接已建立
黑色	没有以太网连接
琥珀色	连接已存在，但端口被手动或生成树禁用。

点击交换机图片上端口的图标，端口的设置情况将显示在窗口的右下部位。

左侧部分菜单，如图 15 所示，包含了交换机可设置的所有特性。这些特性都已经进行了分类，例如 System, Bridge。您可以点击其中的每一项以显示不同的设置页面。

图 15. 完整的菜单列表

点击上边栏对应的项目可以显示设置页面或统计的图表。参见 4.3 。

4.2.1 导航菜单

- 打开一组相关菜单，请点击相对应的分组条目。展开后，向右的箭头 ▸ 会变成向下的箭头 ▾。
- 收拢一组相关菜单，请点击相对应的分组条目。此时向右的箭头 ▸ 将会显示在群组名称旁。
- 打开一个设置页面，请点击您需要设定的页面条目。

4.2.2　常用按钮和图标

下表显示的是网页界面中的按钮和图标的功能。

表 6. 常用按钮和图标

按钮 / 图标	功能
	将当前页面中的设置进行保存。
	添加一条新的设置，如一个静态 MAC 地址或一个防火墙 ACL 规则等。
	修改已有的条目。
	修改系统已有的配置，如一个静态路由或一个 ACL 过滤规则。
	删除选择的项目，如一个静态路由或一个 ACL 过滤规则等。
	刷新当前页面查看更新的统计资料或设置。

4.3　System （系统）

系统页面包括 management(管理), IP setup(IP 设置)，administration(管理权限), reboot（重新启动），和 firmware update（固件升级）功能。

4.3.1　Management（管理）

Management（管理）页面包括以下信息:

Model Name（型号）: 产品名称

MAC Address（MAC 地址）: 交换机的 MAC 地址

System Name（系统名称）: 用户定义的用于区分系统的名称（可编辑）。系统名称不能包含字符 “ / ”。

System Contact（系统联系信息）:（可编辑）。系统联系信息不能包含字符 “ / ”。

System Location（系统方位）:（可编辑）。系统方位不能包含字符 “ / ”。

若要保存并立即应用设置，请点击 OK。点 Reload 刷新设置，如图 16 所示。要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 16. 管理

4.3.2　IP setup（IP 设置）

本交换机支持动态 IP 和静态 IP 分配。动态 IP 可以通过同一 VLAN 内的 DHCP 服务器获得。IP 设置页面包含了以下可编辑的信息:

VLAN ID: 在系统管理界面中设置一个 VLAN ID。管理的规则将应用于该 VLAN。若要用于管理，VLAN ID 必须在同一个 VLAN 内。

DHCP Client（DHCP 客户端）: 开启 DHCP 可以获得动态 IP 地址，或禁止 DHCP 而指定一个静态 IP 地址。DHCP 服务器必须存在于管理 VLAN 内，并可以连接。

IP Address（IP 地址）: 在交换机的管理界面中指定一个静态 IP 地址。

Network Mask（网络掩码）

Default Gateway（默认网关）

若要保存并立即应用设置，请点击 OK。点 Reload 刷新设置，如图 17 所示。要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 17. IP 设置

4.3.3　Administration（管理权限）

管理权限页面使用密码保护功能启用和禁用网页设置界面。默认下网页设置无须认证。

若要保存并立即应用设置，请点击 OK。点 Reload 刷新设置，如图 18 所示。若要启用密码保护，您需要立刻重新登录。

您可以在命令行界面下随时更改密码。

图 18. 管理

4.3.4　Reboot （重新启动）

重新启动页面中包括一个 Reboot 按钮。点击该按钮重新启动系统。

重新启动系统将中断网络并中止网页界面的连接。

图 19. 重新启动

4.3.5　Firmware Upgrade（固件升级）

Firmware Upgrade and Auto-config（固件升级和自动设置）页面包含了以下信息:

Hardware Version（硬件版本）: 显示硬件版本号

Boot ROM Version（Boot ROM 版本号）: 显示 Boot ROM 的版本

Firmware Version（固件版本）: 显示目前使用的固件版本。该序号在固件升级完毕后将自动更新。

直接在空白栏内输入固件（或 auto-config 文件）路径，或点击 Browse... 从弹出窗口中选择固件（或 auto-config 文件）的文件名。点击 Upload 来升级交换机固件（或 auto-config 文件）。参见图 20。

点击 Upload 按钮将指定的固件刷新到交换机，并在固件升级成功之后重新启动系统。重新启动后您需要重新登录。

不要在固件升级过程中切断电源供应。升级失败可能导致交换机无法启动。

Auto-config 文件名称必须是“config.bat”；　第一行必须是“#autoconfig”。

图 20. 固件升级

4.4　Physical interface（物理端口）

物理端口页面显示端口即时状态。您可以在下列栏目内对端口进行设置:

Port（端口）: 选择要进行设置的端口

Admin（管理）: 禁用 / 启用端口

Mode（模式）: 选择速度和双工模式

Flow Control（流量控制）: 启用 / 禁用 802.3x 流量控制机制

端口状态窗口: 显示每个端口的以下信息:

a) Link status（连接状态）: 连接速率和双工模式（若存在连接）

b) State（状态）: 生成树 (STP) 状态

c) Admin(管理): 禁用或启用端口的设置值

d) Mode（模式）: 连接速率和双工模式的设置值

e) Flow Control（流量控制）: 启用 / 禁用 802.3x 流量控制机制的设置值

选择相关端口进行设置，然后点击 Modify 按钮。您更改的设置将会在显示窗口中更新。点击 OK 将设置送往交换机（HTTP 服务器）。点击 Reload 刷新设置，要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

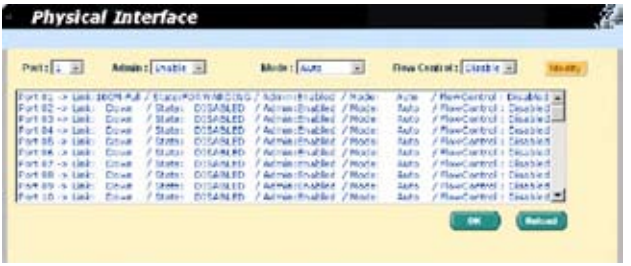

图 21. 物理端口

4.5　Bridge（桥接）

桥接页面包括了大部分的二层设置内容，如链路汇聚、STP 等。

4.5.1　Spanning Tree （生成树）

生成树页面的设置在交换机工作时生效。这个页面包括三个部分。

第一部分显示了根信息。它显示了当前根交换机 (root switch) 的 STP(生成树协议) 设置。

第二部分是 STP 设置。包括以下选项:

Disable/STP Enable/RSTP Enabled: 开启 / 关闭 STP/RSTP（快速生成树协议）。当您开启 STP/RSTP 时，若交换机为根交换机，STP/RSTP 将会使用下面的设置。

Hello Time:（Hello 时间）: 生成 BPDU 的时间间隔

Max Age:（最大寿命）: 局域网内所有网桥使用的超时值

Forward Delay:（转发延迟）: 局域网内网桥的转发延迟值

Bridge Priority（桥接优先）: 局域网内交换机的优先级

第三部分是端口的设置。它包括一个显示窗口，显示目前所有端口的设置情况。按 Modify 更改端口的生成树 / 快速生成树规则。您可以对以下内容进行设置:

Port（端口）: 选择需要进行设置的端口号。

Priority（优先级）交换机端口的优先级。数字越小表示优先级越高。 当侦测到环路时，优先级较低的端口号相比其他端口更容易被生成树阻塞。有效的优先范围是 0 到 240。

Cost（代价）：有效值范围 1 到 200000000。如果出现环路，数值越高越容易被生成树阻塞。

Edge Port（边缘端口）：默认下所有端口都设定为边缘端口。边缘端口在接收到 BPDU 后成为生成树端口。同样，边缘端口转为转发状态只需很短的时间。

Point to Point（点对点）：Auto/Yes/No（自动 / 是 / 否）。全双工连接一般被认为是点对点连接。此外还有共享连接。点对点连接的收敛时间更短。通常推荐选择自动模式。

点击 OK 激活设置，按 Reload 将设置进行刷新。要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 22. 生成树

4.5.2　Link Aggregation（链路汇聚）

本页面用于设置链路汇聚群组（端口群组）。GigaX 2024/2048 交换机可以支持 6 个链路汇聚群组。

Show Trunk（显示群组）：选择“Add a new Trunk”新建一个群组。或选择一个既存群组使之显示下列的条目和端口图标。

Port Selection Criterion（端口选择标准）：根据源 MAC 地址、目的地 MAC 地址、源和目的地 MAC 地址、源 IP 地址、目的地 IP 地址，或源和目的地 IP 地址，在链路汇聚群组中的端口之间分发封包的一种算法。

Name（名称）：链路汇聚群组名称。名称中不能包含“/”和空格。

Trunk ID(群组 ID): 除了群组名称之外另一个用来区分链路汇聚群组的数字。

LACP: 在选择的群组上启用 / 禁用 LCAP。 LACP 模式一直为活动。

Remove Trunk (取消群组): 取消选中的群组。

Port Icons (端口图标): 这些端口图标的排列方式类似交换机的前面板。您可以点击端口图标选择群组端口。再次点击选中端口可将端口从群组中去除。

点击 OK 将设置送往交换机 (HTTP 服务器)。点 Reload 刷新设定值。要激活设置，请进入 Save Configuration 页面点击 Save。

您需要检查系统运行时连接的速度和双工模式以保证群组实体已激活。进入 Physical Interface 页面检查实时环境窗口中连接模式。如果群组中所有端口都处于同样速度和双工模式，说明群组已成功建立。如果其中有任一端口的速度不同或未处于双工模式，说明群组未正确设置。检查连接端口，改变设置，使所有端口处于同样速度和全双工模式。

- *链路汇聚群组中所有端口的速度必须相同，并且全部处于双工模式。*
- *链路汇聚群组中所有端口必须是自适应模式或全双工模式。只有这样才能保证全双工模式。如果端口设定为全双工，那么与之连接的对象也必须是同样的设置。否则链路汇聚就会不正常。*
- *链路汇聚群组中所有端口的 VLAN 设置参数必须相同。*
- *链路汇聚群组中所有端口被当作一个逻辑连接。也就是说，如果群组中一个端口改变设置，其他的端口也会同时发生同样的改变。举例来说，一个链路汇聚群组包括端口 1 和 2。如果端口 1 的 VLAN 发生改变，端口 2 的 VLAN 设置也会随之改变。*

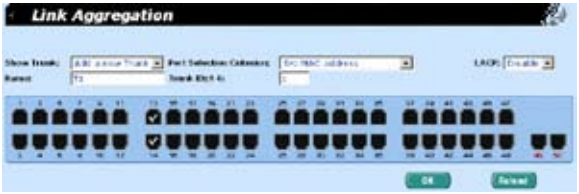

图 23. 链路汇聚（GigaX 2048）

图 24. 链路汇聚（GigaX 2024）

4.5.3　Mirroring（镜像）

镜像和网络流量分析器帮助您监测网络的流量。您可以检测选中端口的出入封包。

Mirror（镜像）：选择镜像群组。每个群组包含 24 个高速以太网端口和 1 个千兆端口。（仅 GigaX 2048）

Mirror Mode（镜像模式）：对选定端口组启用或禁用镜像功能。

Monitor Port（镜像端口）：获取选中端口的封包之副本。

GigaX 2048 有两个监视端口。每个端口可以监视 24 个高速以太网端口和 1 个千兆端口。

GigaX 2024 只有一个监视端口。这个端口可以监视 24 个高速以太网端口和 2 个千兆端口。

监视端口不能属于任何一个链路汇聚群组。

监视端口不能属于任何一个私有 VLAN。

监视端口不能像普通的交换端口一样使用。它不能进行封包交换，也不能进行地址学习。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

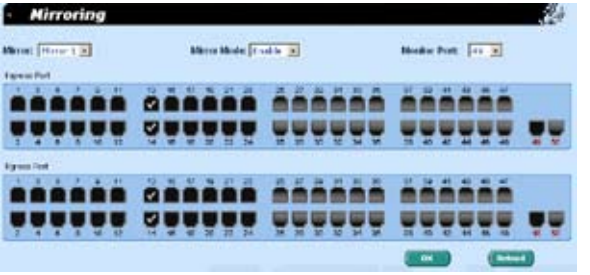

图 25. 镜像页面（GigaX 2048）

图 26. 镜像页面（GigaX 2024）

4.5.4　Static Multicast（静态组播）

本页面用于将组播地址添加到组播表中。交换机可以容纳 255 条组播条目。群组中所有端口就将把指定的组播包转发到群组中其他的端口。

Show Group:（显示群组）：选择 Add a new Group 输入一个新的条目，或选择一个既存群组来显示内容

MAC Address（MAC 地址）：选择组播地址

VLAN：选择 VLAN 群组。 若您选择了一个私有 VLAN，从隔离（isolated）端口发出的流量只能被转发到混杂模式（promiscuous）端口。

CoS: 给服务级别（CoS）设置优先级。

点击 OK 使设置立即生效。点击 Reload 刷新设置到当前值。要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 27. 静态组播（GigaX 2048）

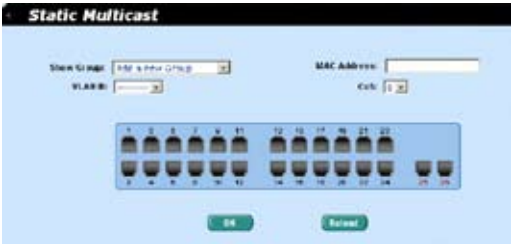

图 28. 静态组播（GigaX 2024）

4.5.5　IGMP Snooping（IGMP 侦测）

IGMP 侦测通过开启或关闭 IGMP 侦测功能，有效的减少了网络上的组播流量。当 IGMP 侦测功能开启时，交换机就会侦测 IGMP 封包并将新的群组添加到组播表中。然而，当静态组播表的条目超过 255 条时，IGMP 侦测就不能正常工作了。交换机只允许 255 个二层组播群组。

点击 OK 使设置立即生效。点击 Reload 刷新设置到当前值。要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 29. IGMP 侦测

4.5.6　Traffic Control（流量控制）

流量控制确保交换机的带宽不被泛洪封包，如广播封包，组播封包所阻塞。限制数值是用来显示某种封包总数量的上限值。例如，若广播和组播被启用，那么这两种类型的封包流量总和不能超过这个上限值。流量控制不适用于私有 VLAN 的隔离（isolated）端口。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 30. 流量控制

4.5.7　Dynamic Addresses（动态地址）

本页面显示基于端口，VLAN ID，或指定的 MAC 地址查找动态 MAC 地址的结果。动态地址指的是交换机自动学习的 MAC 地址，当地址在老化时间内不再学习，该地址就会过期。用户可以根据需要在 10 到 1,000,000 秒的有效区间内选择合适的老化时间。然后点击 OK 使设置立即生效。要永久保存设置，请进入 Save Configuration 页面点击 Save。

您可以通过端口，VLAN ID 或 / 和 MAC，按 Query 观察 MAC 地址状态。地址窗口将显示查找结果。

图 31. 动态地址

4.5.8 Static Addresses（静态地址）

您可以将 MAC 地址添加到交换机地址表中。通过这种方式添加的 MAC 地址不会因老化而过期。我们称之为静态地址。本交换机只支持 1024 个静态地址。

MAC Address（MAC 地址）：输入 MAC 地址

VLAN ID: 输入 MAC 地址所属的 VLAN ID

Port Selection（端口选择）：选择 MAC 地址所属的端口号

Discard（丢弃）：您可以通过封包中包含的目的地址、源地址或其中的任何一个进行封包过滤。

点击 Add 添加新的 MAC 地址。然后您就可以看到新记录已经添加到地址窗口中。要删除存在的地址，只需用鼠标选中该条目，然后点击 Remove。Modify 按钮用来更新已存在的 MAC 地址条目。您可以通过输入 MAC 地址和 VLAN ID，然后点击 Query 来查找静态地址条目。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 32. 静态地址

4.5.9 Tagged VLAN（标记 VLAN）

您可以设置 255 个 VLAN 群组并在本页中显示 VLAN 群组。交换机默认设置下有一个 VLAN，它是不能删除的。这项功能可以防止交换机出错。除了默认 VLAN 外，您可以删除任何其余的 VLAN。

您可以通过点击端口按钮来将端口设置为标记或未标记。一共有三种按钮显示:

“U” 型：未标记的端口，将把传输的封包上的 VLAN 标记删除。

“T” 型：从该端口传输的所有封包都会进行标记。

“blank” 型：该端口不属于 VLAN 群组。

如果一个未标记的端口同时属于两个或更多 VLAN，就会使交换机产生混淆从而造成流量泛洪。为了防止这种情况的发生，交换机只允许一个未标记端口只属于一个 VLAN。也就是说，未标记的端口属于一个叫做 “PVID” 的 VLAN 群组，并且在 Default Port VLAN & CoS 页面中进行设置。如果您希望将一个未标记的端口从一个 VLAN 分配到另一个 VLAN，您就必须将其从原来的 VLAN 中删除，或先将其变为标记端口。

Show VLAN（显示 VLAN）：选择已存在的 VLAN 显示其状态或选择 Add a new VLAN 来新建一个 VLAN 群组。

Name（名称）：VLAN 名称。VLAN 名称不能包含“/”和空格。

DHCP Snoop（DHCP 侦测）：在该 VLAN 中启用或禁用 DHCP 侦测功能。

VLAN ID: 本栏目要求用户在新建 VLAN 时输入 VLAN ID 。

Remove VLAN（删除 VLAN）：删除已存在的 VLAN，在新建 VLAN 时本栏目不会出现。

Private VLAN（私有 VLAN）：将 VLAN 设置为私有 VLAN (PVLAN)。 私有 VLAN 通过简明的 VLAN 设置来保证局域网安全。系统管理员可以减少 VLAN 和 IP 使用数量从而提供与局域网相同的安全。默认 VLAN (VLAN 1) 不能作为私有 VLAN。在系统中，私有 VLAN 的总数为四个。私有 VLAN 有两种类型的端口，以下是对这两种端口的描述:

a) Promiscuous Port（混杂端口）：私有 VLAN 必须且只能有一个混杂端口（Promiscuous Port）。这个端口与私有 VLAN 中的所有界面通信。

b) Isolated Port（隔离端口）：指私有 VLAN 中的非混杂端口。这类端口与同一私有 VLAN 中的其他端口在二层是完全隔离的，但不包括混杂端口。除了从混杂端口发出的流量外，私有 VLAN 阻塞其他所有发送到隔离端口的流量。 流量控制对于隔离端口来说是无效的。

Promiscuous Port（混杂端口）：为私有 VLAN 选择一个混杂端口。这个栏位在勾选了 Private VLAN 之后才有效。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 33. 标记 VLAN（GigaX 2048）

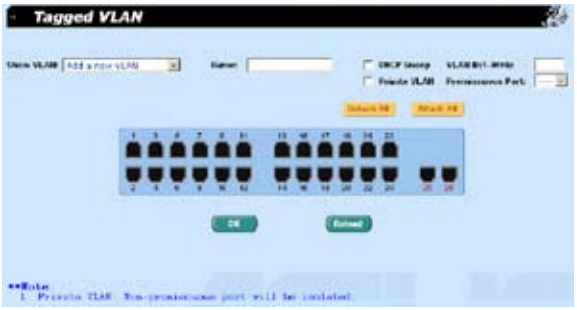

图 34. 标记 VLAN（GigaX 2024）

4.5.10 Default Port VLAN and CoS（默认端口 VLAN 和 CoS）

本页面包括了一些与 VLAN 标记相关的设置，包括:

Port（端口）: 选择需要进行设置的端口。

PVID: 基于端口的 VLAN ID。该端口接收到的未标记封包都将标记上这个 VLAN 群组的 ID。

CoS value(服务等级值): 该端口收到的所有未标记的封包都被分配到该标记 VLAN 的 CoS。

点击 Modify 更改端口列表中的内容， 点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 35. 默认端口 VLAN 和 CoS

4.5.11 DHCP Snooping（DHCP 侦测）

DHCP 侦测是一项 DHCP 安全功能，它通过过滤不可靠的 DHCP 信息和建立与维持 DHCP 绑定表来保证安全。您可以将一些端口设置为可信任端口。选中的（可信任）端口像一般端口一样转发 DHCP 封包，但是，当未选中的（不可靠）端口收到 DHCP ACK 封包时，这些封包将会被丢弃。

DHCP Snooping is: 启用或禁用 DHCP 侦测。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

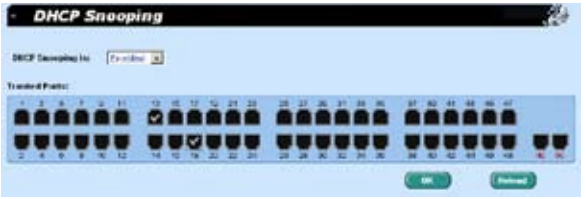

图 36. DHCP 侦测（GigaX 2048）

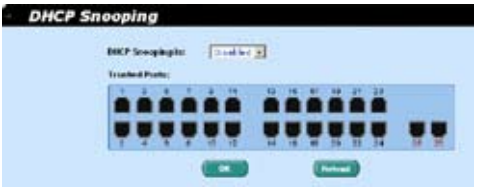

图 37. DHCP 侦测（GigaX 2024）

4.6 SNMP

本群组提供 SNMP（简单网络管理协议）设置，内容包括 Community Table（团体列表），Host Table（主机列表），以及 Trap Setting（Trap 设置）。为了提供更加安全的管理和访问控制，交换机支持 SNMPv3。

4.6.1 Community Table（团体列表）

您可以键入不同的团体名并指定该团体是否具有进行设置（写操作）的权限。 点击 OK 使设置立即生效，要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 38. 团体列表

4.6.2 Host Table（主机列表）

本页面将主机 IP 地址与在 Community Table 页面中设置的团体名称联系在一起。键入一个 IP 地址并从下拉菜单中选择团体名称。点击 OK 使设置立即生效，要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 39. 主机列表

4.6.3　Trap Setting（Trap 设置）

通过设置 trap 目的 IP 地址和团体名称，您可以启用 SNMP trap 功能来发送不同版本的 trap 封包 (v1 or v2c)。点击 OK 使设置立即生效，要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 40. Trap 设置

4.6.4　VACM Group（VACM 群组）

VACM, View-based Access Control Model,（基于视图的访问控制模型）群组是用于设置 SNMPV3 VACM 群组的相关信息。

Group Name（群组名）：输入安全群组名称。 允许多个相同的名称。SNMPv1 和 v2 的群组名（安全群组名）只能是 ro_noauth 或 rw_noauth。

Read View Name（读取视图名）：输入群组隶属的读取视图名称，与其相关的 SNMP 消息为 Get,GetNext,GetBulk。

Write View Name（写入视图名）：输入群组隶属的写入视图名称，与其相关的 SNMP 消息为 Set。

Notify View Name（通知视图名）：输入群组隶属的通知视图名称，与其相关的 SNMP 消息为 Trap，Report， Inform request。注意：此项目前不支持访问控制。

Security Model（安全模型）：输入群组隶属的安全模型， Any 适用于 v1,v2,v3。USM 与 SNMPv3 相关。

Security level（安全等级）：输入群组隶属的安全等级，选项只有 NoAuth, AuthNopriv, AuthPriv。

输入上述信息后，点击 Add 新增一个新的 VACM 群组。然后您就可以在群组窗口中看到新增的记录。您可以通过鼠标选中记录，点 Remove 删除一条记录。Modify 按钮用更新现有的 VACM 群组。点击 OK 使设置立即生效，要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 41. VACM 群组

4.6.5 VACM View

VACM（基于视图的访问控制模型）是用于观察 SNMPV3 VACM 群组的信息。

View Name（View 名）：输入安全群组名称。允许多个相同的名称。

View Type（View 类型）：选择 View 的类型。当 View 子树与 SNMPv3 信息的 Oid 相匹配时选择 Included 或 Excluded。

View Subtree（View 子树）：输入 View 子树。子树就是用于配对 SNMPv3 信息的 Oid 的 Oid。当子树长度小于 SNMPv3 信息中的 Oid，配对即成功。需要使用十进制数值。

View Mask（View 掩码）：输入 View 的掩码。掩码中的每一位表示的是 View 掩码自左向右数字。数位 '0' 表示 '无关'。数字的个数最好为偶数（例如， Ff, ffc0）。请使用十六进制数值。

点击 Add 添加一条新的 VACM View 记录，随后您就会在视图窗口看到这条记录。您可以通过选中一条记录，点 Remove 删除该记录。Modify 按钮则用于更新既存的 VACM View 记录。点击 OK 使设置立即生效，要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 42. VACM View

4.6.6　USM User（USM 用户）

USM（基于使用者的安全模型）是用于设置 SNMPV3 USM 使用者的信息。

Engine Id: 输入与 Manager 中 ID 符合的 Engine Id。

Name: 输入与 Engine ID 相结合的，与 Manager 中相应条目相符的名称。

Auth Protocol: 输入 Engine ID 和 Name 隶属的 Auth 协议。选项只有 NoAuth ,MD5, SHA1。如果选择 NoAuth 就不必输入密码。

Auth Password: 输入 Auth 协议的密码，密码是长度至少为 8 的字符或数字。

Priv Protocol: 输入 Engine ID 和 Name 隶属的 Priv 协议。选项只有 NoPriv 和 DES。如果选择 NoPriv，就无须输入密码。

Priv Password: 输入 Priv Protocol 的密码。密码是长度至少为 8 的字符或数字。

点击 Add 添加一条新的 USM 用户记录，随后您就会在视图窗口看到这条记录。您可以通过选中一条用户记录，点 Remove 删除该记录。Modify 按钮则用于更新既存的 VACM 视图记录。点击 OK 使设置立即生效，要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

图 43. USM 用户

4.7　Filter 页面

本交换机可以在二层到四层中根据封包报头信息过滤特定的流量类型。每个过滤器设置都包含一些规则 。您需要将过滤设置附加到特定的端口上，以保证过滤器正常工作。

4.7.1　Filter set （过滤集）

您可以通过设置名称、ID 和规则模式来创建一个过滤集。本交换机定义了两种模式的规则，一种是 MAC 模式，另一种是 IP 模式。只有相同模式的规则才能在一起构成一个过滤集。每种模式都有不同的项目需要设置。例如，您可以使用 IP 模式规则来过滤 FTP 封包。过滤集的名称不能包含“/”，“#”，“&” 和空格。

当您点击过滤集时，Filter Set 页面即会出现（图 39）。首先，键入名称和 ID，点击 Add 创建一个过滤集。其次，点击 按钮来选择您需要编辑或删除的过滤集。然后，点击 Edit 进入规则页面，如图 40 所示，或点击 Remove 删除过滤集。您必须按照规则设置有效的过滤集。

- 一个集由一个类型的规则组成。这些在相同范围内过滤封包的规则都属于一个类型。例如，两个规则都通过目的地 IP 地址过滤封包，则它们输入同一类型。但是通过源 IP 地址过滤封包的规则就不属于同一个类型。
- 一个端口可以同时应用四种类型的规则。如果为端口分配了四种以上的规则，系统会自动禁用这些规则。

图 44. 过滤集

Filter Rule （过滤规则）页面提供了规则模式的选项，一种是 MAC 规则（参见图 45），另一种是 IP 规则（参见图 46）。如果您没有在空白框内填入 MAC 地址，那么规则将对所有 MAC 地址有效。在 IP 规则设置中，您可以输入 5 种类型中的任何一种 source IP(源 IP 地址), destination IP(目的地 IP 地址), protocol(协议), source application port（源应用端口） 和 destination application port（目的地应用端口）。在 Action 区域您可以选择转发或丢弃符合规则的封包。如果一个封包符合两个规则，且两个规则对应的动作不同，这个封包将按照规则列表中显示的第一个规则执行。

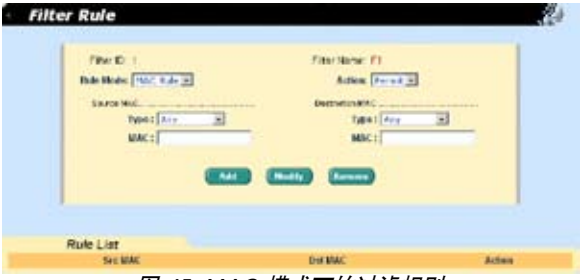

图 45. MAC 模式下的过滤规则

图 46. IP 模式下的过滤规则

4.7.2　Filter attach（过滤规则分配）

一套过滤规则如果没有分配给任何端口，那么这套规则是闲置的。请使用 Filter Attach 页面将过滤设置分配到入口或出口端口。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

请按照以下说明将过滤设置分配到端口:

- Attach to all ports（分配给所有端口）: 这个过滤规则将应用到系统中的所有端口。
- Attach to certain ports（分配给指定的端口）: 您可以将规则分配给指定的端口。对于 GigaX 2048 来说，出口和入口端口必须在端口 1-24 和 49，或者是端口 25-48 和 50。
- Detach from all ports（从端口删除）: 将规则从已分配的端口上删除。

当您选择了“Attach All”命令后，将无法将规则从指定的端口删除。如果您想要将规则从端口删除，请使用“Detach All”命令。

当过滤规则分配到入口和出口端口之后，它将根据入口端口，出口端口和规则中的封包范围进行封包过滤。例如，一个过滤设置是一个单一规则，即过滤进入口端口 1 和出口端口 2 的所有目的地 MAC 地址为 00:10:20:30:40:50 的封包。那么从端口 1 进入的目的地的 MAC 地址为 00:10:20:30:40:50 的封包不能被交换到端口 2。但是在泛洪情况下，这个封包可以交换到除了端口 2 以外的其他端口。

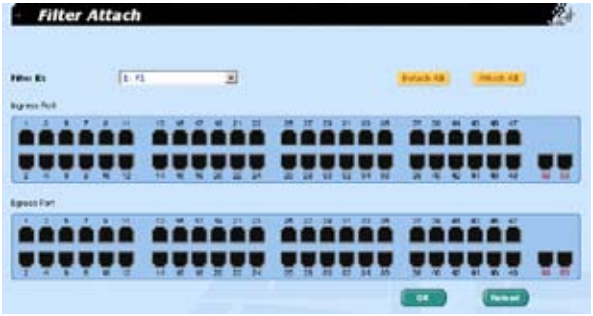

图 47. 过滤规则分配（GigaX 2048）

图 48. 过滤规则分配（GigaX 2024）

4.8　安全

本交换机支持 802.1x 基于端口的安全功能。只有经过授权的主机才能对交换机端口进行修改。当主机无法通过认证 , 端口即被堵塞。认证服务是由 RADIUS 服务器或本地交换机的数据库提供。

本交换机同样还支持通过 802.11x 认证过程建立的动态 VLAN 分配。VLAN 的用户 / 端口信息将在启用该功能前由服务器进行合理设置。

本交换机具有端口安全功能。用户可以通过禁止或指定可访问该端口的基站的 MAC 地址来限制一个界面的输入量。当您为一个安全端口分配了一个安全 MAC 地址后，这个端口不会转发除了已定义的源地址群组之外的其他封包。

4.8.1　Port Access Control（端口访问控制）

端口访问控制用于设置各种不同的 802.1x 参数。802.1x 的使用者可以通过 RADIUS 服务器或本地数据库（只支持 MD5 认证）来认证端口用户。

第一部分为桥接 (Global) 设置:

Reauthentication（重新认证）: 一旦启用，交换机就会在重新认证时间期满时要求重新认证端口的使用者。

Reauthentication Time: （重新认证时间）: 如果重新认证启用，这里定义的就是交换机发送认证信息到端口用户的时间间隔。

Authentication Method（认证方式）: RADIUS 或本地数据库可用于认证端口使用者。

Quiet Period: 如果 RADIUS 或本地数据库认证失败，交换机将在再次发送认证要求前等待的一端时间。

Retransmission Time(重传时间): 如果端口用户没有响应交换机的认证请求，

交换机将在再次发送请求前等待一端时间。

Max Reauthentication Attempts（最大重新认证次数）：重新认证请求失败后的重新尝试次数。

第二部分是端口设置。当更改完成时请点击 Modify。

Port（端口）：指定要进行设置的端口。

Multi-host（多主机）：如果启用该功能，连接到选定端口的所有主机在其中一个主机通过验证后均可使用端口。如果禁用，只有通过验证的主机才能访问该端口。

Authentication Control（认证控制）：如果选择“force authorized”，选定的端口都强制通过了认证。这样，所有主机的流量都可以通过该端口；如果选择“force unauthorized”，选定的端口就被堵塞，任何流量也不能通过。如果选择“Auto”选定端口的性质由 802.1x 协议进行控制。在一般情况下，所有的端口都被设为“Auto”。

Guest VLAN: 为访客指定一个无 802.1x 的 guest VLAN。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 49. 端口访问控制

4.8.2　Dial-In User(拨入用户)

Dial-in User 用于定义处于交换机本地数据库的用户。

User Name: 新的用户名

Password: 新用户的密码

Confirm Password（确认密码）: 再次输入密码

Dynamic VLAN（动态 VLAN）: 指定分配给 802.1x 认证用户的 VLAN ID

点击 Add 添加新的使用者，修改完毕后点击 Modify。要删除使用者时，选中该使用者后点击 Remove。点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 50. 拨入用户

4.8.3 RADIUS

为了使用外部 RADIUS 服务器，下列参数须进行设置:

Authentication Server IP: 认证服务器 IP 地址。

Authentication Server Port: RADIUS 侦听的端口号。

Authentication Server Key: GigaX 和 RADIUS 服务器通信密码

Confirm Authentication Key: 重新输入一遍上面的密码

连接交换机的 RADIUS 服务器必须与系统管理界面位于同一个 VLAN 内。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 51. RADIUS

4.8.4 端口安全

端口安全页面包括 port configuration（端口配置），port status（端口状态）和 secure MAC addresses （安全 MAC 地址）功能。

4.8.4.1 Port configuration（端口配置）

这个页面用来配置 Port Security（端口安全） 的各种参数。本交换机可用的安全 MAC 地址最多为 1024 个。用户可以设置以下栏位:

Port: 选择需要设置的端口。

Admin: 启用或禁用端口的安全功能

Violation Mode: 当与安全规则相违背时决定端口行为。这是当地址表中添加了最大数目的安全 MAC 地址，而不存在于地址表中的 MAC 地址企图访问该界面时端口的行为。您可以将端口设置为以下三种模式中的一种:

a) Protect: 在这种模式下，系统将不会通知您发生了违背规则的事件。

b) Restrict: 在这种模式下，如果发生了违背规则的事件，系统会通知您。系统会发送一个 SNMP trap，记录日志信息，并相应增加 Violation 计数器的数值。

c) Shutdown: 在这种模式下，端口违背安全规则的事件将导致端口立即阻塞。系统同样会发送 SNMP trap，记录系统日志，并相应增加 Violation 计数器的数值。

Max MAC Addresses: 设置安全 MAC 地址的最大值。有效值从 1 到 132。所有端口这个值的总和应该小于或等于本交换机允许的最大安全 MAC 地址数。

Aging Time: 设置老化时间。有效值为 0 ~ 1440（分钟）。老化机制只对动态安全地址有效。如果这个时间为 0，则该端口的老化机制被禁用。

Aging Type: 设置老化类型。老化类型决定了当安全 MAC 地址过期时的对应动作。每个端口支持两种老化类型:

a) Absolute: 在指定的老化时间结束后，端口的安全地址会被删除。

b) Inactivity: 只有在指定时间内安全源 MAC 地址没有数据流量的情况下才将该地址删除。

选择相应的端口号进行端口设置，然后点击 Modify 按钮。您更改的内容将会更新到显示窗口中。点击 OK 使设置立即生效。点击 Reload 刷新设置。要永久保存设置，请进入 Save Configuration 页面，并点击 Save。

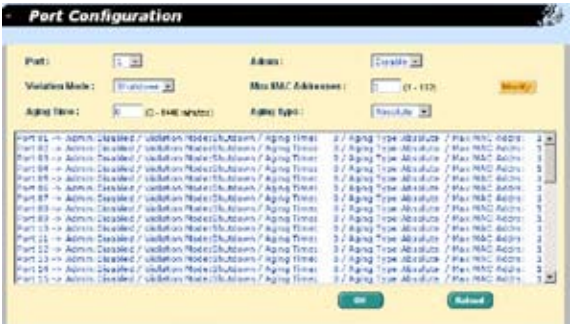

图 52. 端口配置

4.8.4.2 Port status（端口状态）

这个页面显示了当前所有端口的安全信息。以下这些信息会显示在窗口中:

Port: 端口号

Status（状态）:

a) NoOper: 表示本端口的端口安全设置为禁用。

b) SecureUp: 表示端口安全正在运行。

c) SecureDown: 表示端口安全没有运行。此时端口安全设置为启用，但是因为某些原因（如与其他功能冲突）而未能启用。

d) Restrict: 表示当 violation mode 为“restrict”时，端口出现端口安全违背事件。

e) Shutdown: 表示当 violation mode 为“shutdown”时，端口因为端口安全违背事件而阻塞。

Restart: 是否重新启动 shutdown 状态下的端口 (Yes/No)。

TotalMacAddrCount: 当前静态和动态安全 MAC 地址的总数。

StaticMacAddrCount: 当前静态安全 MAC 地址的总数。

ViolationCount: 安全违背事件（violation）的总数。

如果下列情况发生，端口安全状态会显示 SecureDown:

- 端口连接中断
- 管理网桥端口被禁止。
- 端口为链路汇聚端口。
- 端口为端口镜像中的监视端口。
- 端口正在运行 802.1x 且处于单主机模式。

如果端口状态为 “Shutdown”，用户可以选择相应的端口号并将 Restart 设置为 Yes，然后点击 Modify 按钮。您更改的内容将会更新在显示窗口中。点击 OK 使设置立即生效。点击 Reload 刷新设置。要永久保存设置，请进入 Save Configuration 页面，然后点击 Save。

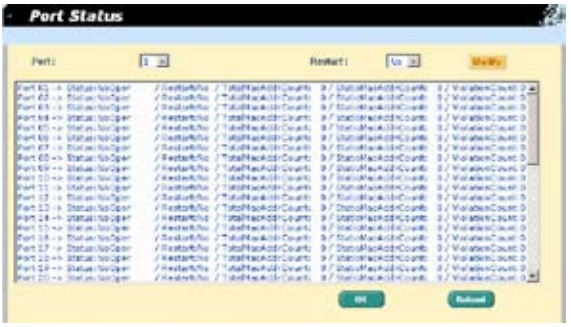

图 53. 端口状态

4.8.4.3 Secure MAC Address（安全 MAC 地址）

用户可以将 MAC 地址添加到端口的安全 MAC 地址表中。通过这种方式添加的 MAC 地址不会从安全 MAC 地址表中老化。我们称其为静态安全 MAC 地址。

MAC Address: 输入 MAC 地址。

Port Selection: 选择 MAC 地址所属的端口。

利用上述信息添加 MAC 地址后，请点击 Add。 然后您可以砍刀新增加的条目显示在了地址窗口中。

用户可以从 Port Selection 中选择端口，然后点击 Query 来查找，这个端口当前的所有安全 MAC 地址将会显示在地址窗口中。

用户可以用鼠标选中一个端口，然后点击 Remove 删除这个端口。如果您想选中多个条目，请按住键盘上的 <Shift> 键，然后用鼠标选择需要的条目。

点击 Add 或 Remove, 设置会立即生效。要永久保存安全 MAC 地址，请进入 Save Configuration 页面，然后点击 Save 。

图 54. 安全 MAC 地址

4.9 QoS

当设置 QoS 特性时，您可以选择特定的网络流量，并根据相对的重要性排定它们的优先级。这项功能使网络性能更方便预测，带宽利用更加合理。

QoS 页面包括 trust state, mapping, class set, policy set, policy attach, 和 CoS 这几项。

4.9.1 Trust State

这个页面利用端口的 Trust State（信任状态）来设置封包等级。用户可以设置下列区域:

Port: 选择需要设置的端口。

State: 设置 trust state。每个端口支持三种类型的状态。

a) No
入口封包没有 trust state 的分类。

b) CoS
用封包的 CoS 值对入口封包分类。

对于标记 IP 封包 – 封包的 DSCP 值基于 CoS-to-DSCP 映射而修改。

对于未标记 IP 封包 –封包的 DSCP 值基于默认的端口 CoS-to-DSCP 映射而修改。

c) DSCP
用封包的 DSCP 值对入口封包进行分类。

对于标记 IP 封包 – 封包的 CoS 值设为 0。

对于未标记 IP 封包 – 封包的 CoS 值设为默认端口 CoS。

对于 IP 封包 – 交换机使用 DSCP-to CoS 映射来修改 CoS 值。

CosOverride: 禁用 / 启用端口的 CoS Override。Cos Override 只有当 Trust State 为 “No” 时才可以启用。CoS Override 将会不考虑先前设置的 trust state 而将默认端口 CoS 值分配给所有的入口封包。如果一个端口先前被设置为 DSCP, 这条命令将会不考虑先前设置的 trust state, 而将默认端口 CoS 值分配给所有的入口封包。如果入口封包为标记封包, 封包的 CoS 值将会修改为默认端口 CoS。

用户可以选择相应的端口号进行设置, 然后点击 Modify 按钮。您更改的内容将会更新在显示窗口中。点击 OK 将设置送至交换机 (HTTP 服务器)。点击 Reload 将设置刷新到当前值。要使设置生效, 请进入 Save Configuration 页面, 然后点击 Save。

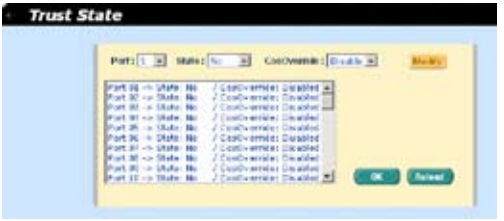

图 55. Trust State

4.9.2 Mapping（映射）

这个页面用来设置 CoS（服务等级）和 DSCP（差分服务代码点）映射。

Map CoS to DSCP: 每个 CoS 值都可以映射到一个 DSCP 值。用户可以使用 CoS-to-DSCP 映射来将入口封包的 CoS 值映射到一个 DSCP 值，QoS 用这个值来决定流量的优先级。

Map DSCP to CoS: 每个 DSCP 值都可以映射到一个 CoS 值。用户可以使用 DSCP-to-CoS 映射来将入口封包的 DSCP 值映射到 CoS 值，这个值用来选择四个出口队列中的一个。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 56. 映射

4.9.3 Class Set

这个设置页面用来创建 QoS 级别。Class set 是用来从其他流量中隔离指定流量（或类别）的一种机制。Class set 定义了用来匹配指定流量的标准（匹配模式），用来做进一步的分类。这个标准包括了在过滤集 ID 或 DSCP 列表中匹配 ACL 规则。每个级别只支持一个匹配模式和一个 ACL 规则。当一个封包与 class-map（类别映射）标准不匹配时，这个封包将根据相应的 policy set 进行进一步的分类。交换机只能具有 56 个级别。以下区域可以进行设置:

Class Name: 输入级别名称。级别名称不能重复也不能包含“/”和空格。

Match: 选择匹配模式。

Filter Set ID: 如果匹配模式为“Filter”，用户必须选择已存在的过滤集 ID。

DSCP: 如果匹配模式为“DSCP”，用户必须输入 DSCP 值。

当您输入以上信息创建新等级后，请点击 Add。此时您可以在 class list 中看到这个新增的条目。点击 选择您想要修改的级别，点击 Modify 进行修改。 您可以在 class list 中看到修改的条目。点击 选择需要删除的级别，然后点击 Remove 将其删除。 要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 57. Class Set

4.9.4 Policy Set

Policy set 指定了哪个 class set 将被使用。 Policy actions 包含在 traffic class 中设置 DSCP 值或指定流量速率上限，以及当流量速率超过上限时所采取的动作。

用户可以通过指定名称来创建一个 policy（策略）。策略名称不能重复，且不能包含 “/”，“#”，“&”和空格。交换机只支持 56 个策略和 256 个策略规则。

首先，您必须指定策略的名称来创建一个策略，然后点击 Add。 然后，点击 来选择您需要编辑或删除的策略，并点击 Edit 进入 Policy Edit 页面或点击 Remove 删除这个策略。一个策略只能具有 6 个 policy actions（策略行动）。

图 58. Policy Set

Policy Edit 页面用来创建 policy actions。添加到策略中的级别必须具有相同的匹配类型。一个策略最多可以拥有 6 个级别。可以设置的区域有:

Class ID: 选择已存在的 Class ID.

DSCP: 选择一个 DSCP 值。符合级别 ID 的入口封包将被分配这个 DSCP 值。

Traffic Rate: 设置流量速率。有效值从 1 到 125。对于千兆以太网端口，这个值需要乘以 8。例如，将流量速率设置为 10，则高速以太网端口的流量速率为 10 Mbps，但是千兆以太网端口的流量速率为 80Mbps。

Traffic Burst Size: 选择流量爆发大小。对于高速以太网端口来说，这个值最小为 4K。对于千兆以太网端口，流量爆发大小要乘以 8。例如，将流量爆发大小设置为 4K，则高速以太网端口的流量爆发大小为 4K 字节，但是千兆以太网端口的爆发大小为 32K 字节。

Exceed Action: 选择 exceed action。如果 exceed action 没有设置为 “None”，则用户必须键入或选择一个 traffic rate 和 traffic burst size。

Exceed DSCP: 如果 exceed action 设置为 “DSCP”，必须选择一个 exceed DSCP 值。

输入以上信息并点击 Add 来创建一个新的 policy action。然后您将在 policy action list 中看到新增的条目。点击  选择您需要修改的 policy action，编辑完成后点击 Modify。您可以在 policy action list 中看到修改后的条目。点击  选择您想要删除的 policy action，然后点击 Remove 将其删除。要想让设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 59. Policy 编辑

4.9.5 Policy Attach

若您没有将 policy 分配到端口，那么它将不起任何作用。您可以使用这个页面将 policy 分配到入口端口。一个端口只能分配一个 policy。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

以下是将 policy 分配到端口的一些方法:

- Attach to all ports: policy 将应用到系统中的所有端口。
- Attach to certain ports: 您可以指定需要应用此 policy 的入口端口。
- Detach all: 从已分配的端口删除此 policy。

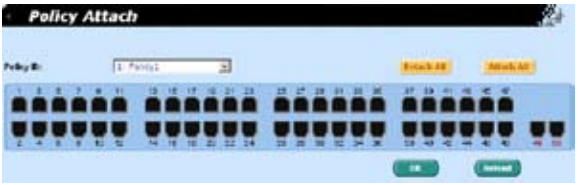

图 60. Policy Attach

4.9.6 CoS

本交换机支持每个入口端口四个 CoS 队列。对于每一个队列，您都可以指定如下的调度类型:

Strict priority scheduling: 每个 CoS 值都可以映射到四个队列中的一个。队列 4 在传输封包时具有最高的优先级。在低优先级队列中的封包需要等到所有高优先级队列为空时才能被传送。在 Strict priority 调度中， weight（权重）被设置为零。

Weighted round-robin (WRR，权重轮转）调度 : WRR 调度需要您为队列指定一个代表与其他 CoS 队列的相对重要性（权重）的数字。WRR 调度防止了低优先级队列在高优先级队列传送过程中完全被忽略的情况。WRR 调度依次传送每个队列中的一定数量的封包。传送封包的数量是根据每个队列的相对重要性来决定。例如，如果一个队列权重为 3，另一个队列权重为 4，那么每次从第一个队列传送三个封包，而从第二个队列传送四个封包。使用这种调度方法，低优先级队列中的封包在高优先级队列不为空的情况下也能被传送。有效的权重值从 1 到 255，权重设置只有在 WRR 调度中才有效。

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。要使设置生效，请进入 Save Configuration 页面，然后点击 Save。

图 61. CoS

4.10 Statistics Chart（统计表）

统计表页面提供在不同的统计表中观察网络流量情况。您可以指定刷新统计表的时间间隔。通过这些表单，您可以方便的监视网络流量情况。大多数 MIB-II 计数器都显示在这些表单中。

点击 Refresh Rate 设置从交换机获取信息的时间间隔。您可通过选择颜色来区分统计数据或端口。最后，点击 Draw 让浏览器显示图表。每次按下 Draw 就会刷新图表。

4.10.1 Traffic Comparison（流量比较）

本页在一个图表中显示所有端口的统计数据。指定数据选项然后按 Draw，浏览器就会显示更新数据并且每隔一段时间刷新图表。

图 62. 流量比较（GigaX 2048）

图 63. 流量比较（GigaX 2024）

4.10.2 Error Group（错误分组）

选择端口和显示颜色，然后点击 Draw，统计图表即会显示指定端口所有的丢弃或错误计数，并且图表每隔一端时间自动更新。

图 64. 错误分组

4.10.3 Historical Status（历史状态）

您可以对不同的端口和统计项目进行分别统计。由于本页显示的是历史统计信息，即使进行刷新，统计表仍保留旧的统计信息。

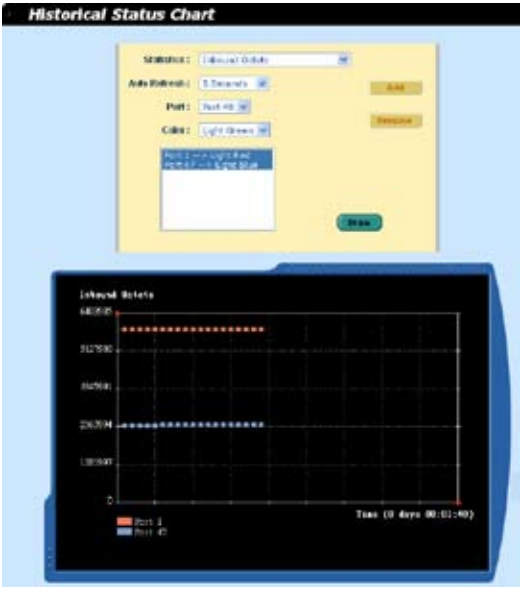

图 65. 历史状态

4.11 Save Configuration （保存设置）

要永久保存设置，您需要点击 Save。 设置在成功保存后才会生效。

有时您也许会希望恢复交换机的出厂设置，您可以点击 Restore 按钮将设置恢复到出厂值。在恢复后系统将自动重新启动。

当恢复出厂设置时，所有的设置均会丢失。

图 66. 保存设置

5　控制终端界面

本章将叙述如何使用控制终端界面对交换机进行设置。GigaX 2024/2048 交换机提供了 RS232 和 USB 两种接口来连接您的计算机。您的计算机需要运行一种终端仿真软件如 HyperTerminal，以及用于设置交换机的命令行翻译器。您需要将终端仿真器的波特率设置为 9600, 8 位数据，无配类， 1 个停止位，无流量控制。

当您进入命令行模式，键入 “?”，屏幕将显示所有可以使用的命令的帮助信息。如果您对命令行不熟悉，这将是一个相当有用的帮手。当空闲时间超过 10 分钟，命令行就会中止连接。这时您需要重新进入命令行模式。

所有的命令行命令都区分大小写。为了使命令易于使用，您可以键入完整命令进入命令分组，这样该命令分组就成为您的工作所在分组。这样以一来，您就无须在子命令中再打上命令分组名。举例说明，“sys” 是一个命令分组，其下包括许多子命令，当您键入 “sys” 进入 “sys” 命令组，您在调用其下子命令时就无须再键入 “sys”。此时，提示符将变为 “(system name) sys%”。

5.1　开机自检

POST（开机自检）是在系统启动时间进行的。它测试交换机主板上的系统内存，LED，以及硬件芯片等。检测完毕时，它就会现实系统测试和初始化的结果。当提示符 “(ASUS) %” 出现时，（如图 67），您即可忽略这些自检信息。

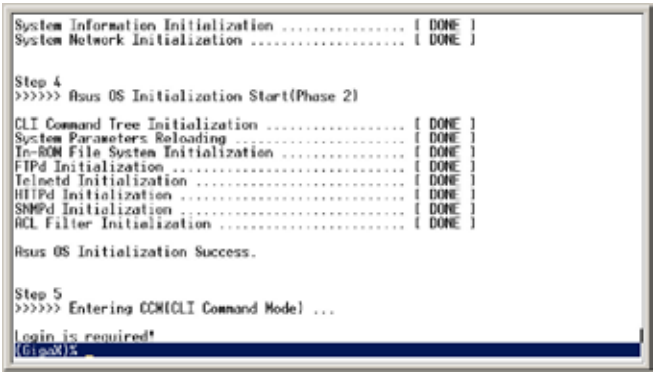

图 67. 命令行界面

5.1.1 Boot ROM 命令模式

在开机自检的过程中，按下 <ENTER> 可以进入 “Boot ROM Command” 模式，如图 68 所示。

图 68 显示交换机的双镜像备份。一个固件位于 Slot 0，另一个固件位于 Slot 1。 后者将自动被选中用于启动系统。

键入 “?” 显示所有可以使用命令的帮助信息。

尽管这些命令在某些情况下有所帮助，但如果您不了解这些命令的功能，我们强烈建议您不要使用他们。

图 68. Boot ROM 命令模式

5.1.2 Boot ROM 命令

键入 “?” 显示所有可以使用命令的列表。

表 7. Boot ROM 命令

命令	参数	用途	备注
d	Address [,length]	通过给定地址和长度转储内存内容	
p	NONE	可置换风扇	
g	NONE	两个风扇都工作正常	
a	NONE	两个风扇中有一个或全部停止	

命令	参数	用途	备注
b	0 or 1 or a	支持双固件备份。您可以通过指定 Slot ID 来选择固件，或使用“a”自动选择。自动选择将会执行最新固件。这是默认的设置。	当您升级固件失败时，您可以使用这条命令用旧的固件启动交换机。当固件升级成功后，请将设置恢复为自动选择(auto-select) 模式。
s	0, 1, 2, 3	设定控制终端的波特率。 0: 9600bps 1:38400bps 2:57600bps 3:115200bps	您必须将终端仿真器设置为相同的波特率，以保证正常工作。
x	NONE	将固件刷新到交换机	通过控制终端更新固件速度较慢。如果您的交换机没有连接网络，您也可以用这个方法更新固件。
r	NONE	Toggle 安全模式	当设置文件损坏或您忘记了密码，请使用安全模式来进入命令行模式。在这个模式中，您的设置文件会丢失。您需要恢复默认设置或重新设置系统。
w	NONE	重设 Toggle 管理员密码	重新设置 user ID 和密码到默认值。您的设置将不会更改。

5.2 登录和登出

键入“login”进入命令行模式后，你必须输入一个有效的用户名和密码。当您第一次登录时，用户名为 “admin”密码为空。为了安全考虑，请在登录后立刻修改密码。如果您忘记了用户名和密码，请与华硕技术支援人员联系，或在 Boot ROM 命令模式中清除设置文件。如果您选择第二种方式，那么删除文件的同时，所有的系统设置都会丢失，也就是说，您必须重新对交换机进行设置。

要离开命令行模式，请键入“logout”。这么做有助于保证命令行模式的安全性。下一位使用者必须使用经过认证的用户名和密码才能登录命令行界面。

5.3 CLI 命令

GigaX 2024/2048 交换机提供命令行命令来设置所有的网管功能。这些命令的排列方式同网页设置界面的排列方式。这样，您就能根据提示正确而轻松地设置交换机。“save”命令是用于将设置刷入交换机。有些命令行命令只有在进行“save”命令后才能生效。

请使用 “?” 获取可使用命令列表和帮助信息

请使用 “/” 回到根目录

请使用 “..” 回到上级目录

键入命令获取命令的帮助信息

5.3.1 系统命令

[System Name]

显示交换机被赋予的名称。这是 RFC-1213 中规定的系统 MIB 项目，在网管节点提供管理信息。

命令: sys info name <system name description>

如果您在 name description 处输入名称，那么交换机名就会更改为您键入的名称。

[System Contact]

显示交换机的详细联系信息。这是 RFC-1213 定义的系统 MIB 项目，提供网管节点处的联系信息。

命令: sys info contact <system contact description>

如果您在 contact description 处输入信息，交换机的联系信息即更改。

[System Location]

显示交换机的物理位置。这是 RFC-1213 定义的系统 MIB 项目提供网管节点的位置信息。

命令：sys info location <system location description>

在 location description 键入地点描述即更新地点信息。

图 69. SYS 命令

[VLAN ID]

显示交换机的 VLAN ID。交换机的 VLAN ID 必须与管理的网段处于同一 VLAN。

命令：net interface vlan sw0 <VLAN ID>

[DHCP Client]

启用 DHCP 获取动态 IP 地址；或禁用 DHCP 使用手动指定静态地址。如果启用 DHCP，您就能自动为交换机获取 IP 地址，使用 show 命令显示动态 IP 地址。

命令：net interface dhcp sw0 <enable/ disable/ renew/ release/ show>

[IP Address]

显示交换机的 IP 地址。这个地址是用于网管功能的，比如，网络应用如 http 服务器，SNMP 服务器，tftp 服务器，telnet 服务器和 SSH 服务器在 vlan1 中都使用这个地址。

命令：net interface ip sw0 < IP address> <netmask>

[Network Mask]

显示交换机的子网掩码。

命令：net interface ip sw0 < IP address> <netmask>

[Default Gateway]

显示默认网关的 IP 地址。当交换机网络包含一个或一个以上路由器时须添入相关

信息。

命 令：net route static add <destination subnet/IP> <gateway> <netmask> <metric>

[Password Protection is] [Enabled/Disabled]

当启用密码保护功能，在使用网页设置界面时，界面就会要求输入用户名和密码进行认证。

命令：sys web set <enable/disable>

[New Password]

[Verify Password]

默认用户名为 admin，密码为空。您可以通过设置以下内容设置密码。

命令：sys users modify <user name, 'admin' by default>

user name (old user name, 'admin' by default): <new user name>

password (old password): <new password>

[Reboot]

用户可以发出重启命令来重启交换机。

命令：sys reboot

[Upload]

命令行界面没有这个命令，请参见 Boot ROM 命令组的相关命令。

5.3.2 物理端口命令

[Admin] [Enable/Disable]

显示端口的管理状态，并允许用户启用或关闭该端口。

命令：l2 port admin <port number> <enable/disable>

[Mode] [Auto/10M-Half/10M-Full/100M-Half/100M-Full/1G-Full]

显示端口的当前速度和双工模式。当端口启用自适应功能，就能自动侦测速度和双工模式。

命令：l2 port autoneg <port number> <enable/disable>

命令：l2 port speed <port number> <10/100/1000>

命令：l2 port duplex <port number> <full/half>

[Flow Control] [Enable/Disable]

显示端口的 IEEE802.3x 流量控制设置。注意流量控制只在全双工端口上使用。

命令：l2 port flow <port number> <enable/disable>

[Reload]

从设置文件中恢复之前的端口设置。

命令：l2 port retrieve

5.3.3　桥接命令

[Spanning Tree is] [STP Enabled/ RSTP Enabled/ Disabled]

允许用户指定交换机是否使用生成树协议 (STP/ RSTP)。

命令：l2 stp start <stp / rstp>

命令：l2 stp stop

[Hello Time]
[Forward Delay]
[Max Age]
[Bridge Priority]

显示当前的 STP/RSTP 桥接设置参数。

命令：l2 stp bridge set

Hello Time (1..10 seconds): [old Hello Time] <new Hello Time>

Forward Delay (4..30 seconds): [old Forward Delay] <new Forward Delay>

Max Age (6..40 seconds): [old Max Age] <new Max Age>

Bridge Priority (0..61440): [old Bridge Priority] <new Bridge Priority>

[Priority]
[Path Cost]
[Edge Port]
[Point-to-point]

显示当前端口的 STP/RSTP 参数设置。

命令：l2 stp port set

Port Settings (all,...): [all] <select a port number, or just type 'all' to iteratively config>

Port <port number> Priority (0..240): [old port Priority] <new port Priority>

Port <port number> Path Cost (1..200000000): [old port Path Cost] <new port Path Cost>

Port <port number> EdgePort (yes/no): [old port EdgePort] <new port EdgePort >

Port <port number> Point-to-Point (yes/no/auto): [old port Point-to-Point] <new port Point-to-Point >

[Reload]

从设置文件恢复之前的设置。

命令: l2 stp retrieve

命令: l2 stp bridge retrieve

命令: l2 stp port retrieve

[Show Trunk]

显示指定的干线群组的设置。用户可以通过指定一个干线 ID，干线名描述，端口选择现象（rtag），LACP 模式（启用 / 禁用），和干线群组的端口号来新建一个新的干线群组。

命令: l2 trunk show <trunk id>

[Create Trunk]

通过指定干线 ID, rtag，名称，LACP 模式和端口号码来新建一个新的干线群组。“rtag”是干线群组的封包分发算法。

Rtag 值及相应的含义:

1: 通过源 MAC 地址选择端口

2: 通过目的地 MAC 地址选择端口

3. 通过源和目的地 MAC 地址选择端口

4. 通过源 IP 地址选择端口

5: 通过目的地 IP 地址选择端口

6. 通过源和目的地 IP 地址选择端口

命 令: l2 trunk create <trunk id> <rtag (1-6)> <trunk name> <lacp (enable/disable)> <port list>

[Add/Remove Trunk]

可以在干线群组中增加或删除端口。

命令：l2 trunk add <trunk id> <port list>

命令：l2 trunk remove <trunk id> <port list>

[LACP Action]

用户可以在干线群组中启用或禁用 LACP。

命令：l2 trunk lacp action <trunk id> <enable/disable>

[LACP System Priority]

用户可以为运行中的 LACP 设置系统优先级。

命令：l2 trunk lacp syspri <priority (1-65535)>

[LACP Port Priority]

用户可以为运行中的 LACP 分配端口优先级。

命令：l2 vlan add <vlan id> <port list>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 trunk retrieve

** 用于 GigaX 2048 **

[Mirror] [Mirror 1/Mirror 2]

[Mirror Mode] [Enable/Disable]

[Monitor Port] [port number]

显示交换机的镜像设置。用户最多可以在交换机上创建两个镜像端口。镜像 ID 1 用于 SoC 0, 镜像 ID 2 用于 SoC 1。因此，只有端口 1-24 可以作为监视端口被分配到镜像 ID 1，入口或出口端口。只有端口 25-48 只有端口 1-24 可以作为监视端口被分配到镜像 ID 2。

命令：l2 mirror create <mirror id (1 or 2)> <monitor port no> <enable/disable>

命令：l2 mirror ingress <mirror id (1 or 2)> <port list>

命令：l2 mirror egress <mirror id (1 or 2)> <port list>

命令：l2 mirror remove <mirror id (1 or 2)> <ingress/egress> <port list>

** 用于 GigaX 2024 **

[Mirror Mode] [Enable/Disable]

[Monitor Port] [port number]

显示交换机镜像设置。

命令：l2 mirror create <monitor port no> <enable/disable>

命令：l2 mirror ingress <port list>

命令：l2 mirror egress <port list>

命令：l2 mirror remove <ingress/egress> <port list>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 mirror retrieve

[Show Group]

显示静态组播群组列表中的群组。

命令：l2 mcast show

[MAC Address]

[VLAN]

[CoS] [0-7]

允许用户通过指定 MAC 地址，VLAN ID,CoS，VLAN 端口号，以及其未标记的端口号添加或修改一个静态组播群组。注意 MAC 地址和 VLAN ID 的组合是组播群组表中一个独有的条目。

命令：l2 mcast set

mac address [format: xx:xx:xx:xx:xx:xx]: <multicast mac address>

vlan id [1 by default]: <vlan id>

cos [0-7, 0 by default]: <Class of Service >

port list [format: 1 2 3 4-50/* for all ports]: <vlan port list>

untagged port list [format: 1 2 3 4-50/* for all ports]: <untagged port list>

[Remove Multicast Group]

允许用户通过指定 MAC 地址和 VLAN ID 从组播群组中删除一个组播记录。

命令：l2 mcast delete

mac address [format: xx:xx:xx:xx:xx:xx]: <multicast mac address>

vlan id: <vlan id>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 mcast retrieve

[IGMP is] [Enabled/Disabled]

Layer 2 IGMP 侦测功能可根据实际需要决定是否启用。

命令：l2 igmp <start/stop>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 igmp retrieve

[Broadcast] [Enabled/Disabled]

[Multicast] [Enabled/Disabled]

[Destination Lookup Failure] [Enabled/Disabled]

开启流量控制功能，用户可以限制广播、组播和泛洪（由于目的地寻址失败）流量。

命令：l2 rate set <1: bcast/2: mcast/3: dlf> <enable/disable>

[Limit]

显示当前交换机的速率限制。用户可以设置新的限制值来进行更改。这个值可用于上面提到的所有流量控制。

命令：l2 rate limit <limit rate>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 rate retrieve

[Aging Time]

用户可以通过设置制老化时间值来设置 ARL (Address Resolution Logic) 记录的老化时间。

命令：l2 arl age [aging time value]

[Query by Port]

ARL 表中的记录可以根据端口号进行搜索排序。

命令: l2 arl port <port number>

[Query by VLAN ID]

ARL 表中的记录可以根据 VLAN ID 进行搜索排序。

命令: l2 arl vlan <vlan id>

[Query by MAC Address]

ARL 表中的记录可以根据 MAC 地址进行搜索排序。

命令: l2 arl mac <mac address> [vlan id]

[MAC Address]

[VLAN ID]

[Port Selection]

[Discard] [none/source/destination/source & destination]

用户可以通过指定 MAC 地址, VLAN ID, 端口号和干线 ID 来新增或修改一条静态 ARL 记录。

命令: l2 arl static <mac> <vlan id> <port no> <trunk id> <discard: 0-3>

[Remove]

可以通过指定 MAC 地址和其 VLAN ID 删除静态 ARL 记录。这种双字段的组合方式是 ARL 表中所特有的。

命令: l2 arl delete <mac address> <vlan id>

[Reload]

从设置文件中恢复之前的设置。

命令: l2 arl retrieve

[Show VLAN]

显示交换机中现有的 VLAN 信息。

命令: l2 vlan show <vlan id>

[Name]

[VLAN ID]

[Private VLAN]

允许用户设置 VLAN 。用户可以通过定义一个独有的 VLAN ID，一个 VLAN 描述，其下的端口列表新建一个 VLAN。注意这里的端口号是标记的端口。 若要指定未标记的端口作为该 VLAN 的端口，命令行命令 utportadd 可以完成这个任务。用户可以使用命令行添加或删除 VLAN 中的端口。

命令：l2 vlan create <vlan id> <vlan name> [<vlan type:private>][<port list: * for all ports>]

命令：l2 vlan add <vlan id> <port list>

命令：l2 vlan remove <vlan id> <port list>

命令：l2 vlan utportadd <vlan id> <untagged port list>

[DHCP Snoop]

在 VLAN 中启用或禁用 DHCP 侦测。

命令：l2 dhcpsnoop enable <vlan id list>

命令：l2 dhcpsnoop disable <vlan id list>

[Remove VLAN]

允许用户完全删除整个 VLAN。

命令：l2 vlan delete <vlan id>

[Promiscuous Port]

为私有 VLAN 设置混杂端口。

命令：l2 vlan promisport <vlan id> <promiscuous port id>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 vlan retrieve

[PVID]

通过指定 VLAN ID 和其下的端口号列表为一个端口设置默认 VLAN。

命令：l2 port vlan <vlan id, 4095 to disable the port-based vlan> <port list>

[CoS Value]

通过制定优先级标准值（0-7）来设置服务级别

命令：l2 port priority <CoS> <port list>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 port retrieve

[Priority] [CoS Queue]

允许用户映射 CoS 优先级 (0-7) 用于缓冲队列 (4 个队列，队列 ID 分别为 1-4)。

命令：l2 cos map <queue id (1-4)> <cos (0-7)>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 cos retrieve

[DHCP Snooping is]

对指定的 VLAN 启用或禁用 DHCP 侦测功能。

命令：l2 dhcpsnoop enable <vlan id list>

命令：l2 dhcpsnoop disable <vlan id list>

[Add/Remove Trusted Port]

允许用户添加或删除指定的用于 DHCP 侦测的端口。

命令：l2 dhcpsnoop add <port list>

命令：l2 dhcpsnoop remove <port list>

[Reload]

从设置文件中恢复之前的设置。

命令：l2 dhcpsnoop retrieve

5.3.4 SNMP

[Community Name] [Set]

一个团体记录包含一个团体描述字串和一组特权。Get 权默认为启用，用户可以在新建记录时指定是否要给予 Set 特权。

命令：snmp community add

New community string: <new community string>

Get privileges: [y, always turn on by default]

Set privileges? (y/n):[n] <set privilege, y for ‘yes’ ; n for ‘no’ >

命令: snmp community set

用户可以通过重新分配团体字串和特权来修改团体记录。

Community entry (table index): <entry id to config>

Community string (old community string): <new community string>

这项操作将修改所有主机的团体字串。

Are you sure? (y/n): [y] <y for ‘yes’ ; n for ‘no’ >

Get privileges: [y, always turn on by default]

Set privileges? (y/n): [n] <set privilege, y for ‘yes’ ; n for ‘no’ >

命令: snmp community delete

允许用户从团体表中删除团体记录。

Community entry (table index): <entry id to delete>

This action will delete all hosts in community string with ‘delete community’ .

Are you sure? (y/n): [y] <y for ‘yes’ ; n for ‘no’ >

[Reload]

从设置文件中恢复之前的设置。

命令: snmp community retrieve

[Host IP Address] [Community]

每条主机记录包括一个主机 IP 地址，网络掩码，以及其团体字串。

命令: snmp host add

Host IP/Subnet: <IP address>

Netmask: <netmask>

Community: <community string>

命令: snmp host set

用户可以通过重新分配允许范围内的 IP 地址，网络掩码和团体字串对主机记录进行修改。

Host table entry (table index): <entry id to config>

Host IP/Subnet (old IP address): <new IP address>

Netmask (old netmask): <new netmask>

Community (old community string): <new community string>

命令: snmp host delete

允许用户从主机表中删除一个主机记录。

Entry id (table index): <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令: snmp host retrieve

[Trap Version] [v1/v2c]

[Destination]

[Community for Trap]

每个 trap 记录包括 SNMP 版本号 (目前支持 v1 和 v2c), 一个目的 IP 地址和远程团体字串。

命令: snmp trap add

SNMP version? (1/2c): [1, by default] <snmp version>

Destination IP: <IP address>

Community: <community string>

命令: snmp trap set

用户可以通过重新指定 SNMP 版本, 目的 IP 地址和团体字串来修改 trap 记录。

Trap table entry (table index): <entry id to config>

SNMP version? (1/2c): [old snmp version] <new snmp version>

Destination IP (old IP address): <new IP address>

Community (old community string): <new community string>

命令: snmp trap delete

允许用户从 trap 表中删除记录。

Trap table entry (table index): <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令：snmp trap retrieve

[Group Name]

[Read View Name]

[Write View Name]

[Notify View Name]

[Security Model]

[Security level]

VACM(View-based Access Control Model) 群组记录包括一个群组名, 只读view名, 写入 view 名，通知 view 名，安全模式，安全级别和先后匹配。

命令：snmp snmpv3 access add

Gruop Name: <group name string>

Security Model [0/1/2/3](any/v1/v2c/usm): <security model>

Security Level [1/2/3](noauth/authnopriv/authpriv): <security level>

Context Match [0/1](inexact/exact): <context match>

Read View Name: <read view name string>

Write View Name: <write view name string>

Notify View Name: <notify view name string>

命令：snmp snmpv3 access set

用户可以通过重新分配群组名, 只读 view 名, 写入 view 名, 通知 view 名, 安全模式, 安全级别和先后匹配来修改 VACM 记录。

Gruop Name: (old group name string) <new group name string>

Security Model [0/1/2/3](any/v1/v2c/usm): (old security model) <new security model>

Security Level [1/2/3](noauth/authnopriv/authpriv): (old security level) <new security level>

Context Match [0/1](inexact/exact): (old context match) <new context match>

Read View Name: (old read view name string) <new read view name string>

Write View Name: (old write view name string) <new write view name string>

Notify View Name: (old notify view name string) <new notify view name string>

命令: snmp snmpv3 access delete

允许用户删除 VACM 记录。

Access entry: <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令: snmp snmpv3 access retrieve

[View Name]

[View Type]

[View Subtree]

[View Mask]

VACM (View-based Access Control Model) view 是用于浏览 SNMPV3 VACM 群组的信息。VACM view 包括一个 view 名，view 类型，view 子树和 view 掩码。

命令: snmp snmpv3 view add

View Name: <view name string>

View Subtree [oid]: <view subtree>

View Mask: <view mask>

View Type[1/2](included/excluded): <view type>

命令: snmp snmpv3 view set

用户可以通过重新指定可用的 view 名，view 类型和 view 掩码来修改 VACM view 记录。

View Name: (old view name string) <new view name string >

View Subtree [oid]: (old view subtree) <new view subtree>

View Mask: (old view mask) <new view mask >

View Type[1/2] (included/excluded): (old view type) <new view type >

命令: snmp snmpv3 view delete

允许用户删除 VACM view 记录。

View entry: <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令：snmp snmpv3 view retrieve

[Engine Id]

[Name]

[Auth Protocol]

[Auth Password]

[Priv Protocol]

[Priv Password]

USM(User-based Security Model) User 命令可以用于设置 SNMPV3 USM User 的信息。USM User 记录包括 engine Id, name, auth protocol, auth password, priv protocol 以及 priv password。

命令：snmp snmpv3 usmuser add

EngineId: <engine id string >

Name: <user name string >

AuthProtocol [oid]: <auth protocol oid string >

AuthPassword: <auth password string>

Priv Protocol [oid]: <priv protocol oid string >

Priv Password: <priv password string >

命令：snmp snmpv3 usmuser set

用户可以通过重新指定 engine Id, name, auth protocol, auth password, priv protocol 和 priv password 修来改 USM User 记录。

EngineId: (old engine id string) <new engine id string >

Name: (old user name string) < new user name string >

AuthProtocol [oid]: (old auth protocol oid string) < new auth protocol oid string >

AuthPassword: (old auth password string) < new auth password string>

Priv Protocol [oid]: (old priv protocol oid string) < new priv protocol oid string >

Priv Password: (old priv password string) < new priv password string >

命令：snmp snmpv3 view delete

Allows user to delete a USM User entry.

USM user entry: <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令：snmp snmpv3 usmuser retrieve

5.3.5 过滤命令

[New]

通过指定唯一的 ACL ID 和描述名称来创建一个新的过滤集。

命令：filter set new <acl id> <acl name>

[Remove]

用户可以通过 ACL ID 删除一个过滤集。

命令：filter set delete <acl id>

[Edit]

[Rule Mode] [MAC Rule]

[Action] [Permit/Deny]

[Source MAC]

[Destination MAC]

[Add]

用户可以在过滤集中添加新的 MAC 地址规则。设置这些规则可允许或禁止 ICMP, TCP 或 UDP 协议。用户也可以通过 dstmac 和 srcmac 命令指定过滤规则的 MAC 地址（源地址或目的地址）。

命　令：filter rule new <set id> <rule id> <protocol: ICMP/TCP/UDP/any> <action: permit/deny>

命令：filter rule dstmac <set id> <rule id> <type: (any/[mac address])>

命令：filter rule srcmac <set id> <rule id> <type: (any/[mac address])>

[Rule Mode] [IP Rule]

[Action] [Permit/Deny]

[Source IP] [Type/IP, Mask]

[Destination IP] [Type/IP, Mask]

[Source Port] [Type/Port]

[Destination Port] [Type/Port]

[Protocol] [ICMP/TCP/UDP/ANY]

[Add]

用户可以在过滤集中新增一个新的 IP 规则。这些过滤规则用来允许或禁止 ICMP, TCP 或 UDP 协议。用户也可以通过 dstip/srcip 和 dstport/srcport 命令指定过滤规则的 IP 地址（源地址或目的地址）和端口号。

命　令：filter rule new <set id> <rule id> <protocol: ICMP/TCP/UDP/any> <action: permit/deny>

命令：filter rule dstip <set id> <rule id> <type: (any/[ip] [subnet])>

命令：filter rule srcip <set id> <rule id> <type: (any/[ip] [subnet])>

命令：filter rule dstport <set id> <rule id> <type: (any/[port])>

命令：filter rule srcport <set id> <rule id> <type: (any/[port])>

[Rule Mode] [MAC Rule]

[Action] [Permit/Deny]

[Source MAC]

[Destination MAC]

[Modify]

允许用户修改 MAC 过滤规则。

命令：filter rule modify <set id> <rule id> <protocol: ICMP/TCP/UDP/any> <action: permit/deny>

命令：filter rule dstmac <set id> <rule id> <type: (any/[mac address])>

命令：filter rule srcmac <set id> <rule id> <type: (any/[mac address])>

[Rule Mode] [IP Rule]

[Action] [Permit/Deny]

[Source IP] [Type/IP, Mask]

[Destination IP] [Type/IP, Mask]

[Source Port] [Type/Port]

[Destination Port] [Type/Port]

[Protocol] [ICMP/TCP/UDP/ANY]

[Modify]

允许用户修改 IP 过滤规则。

命令: filter rule modify <set id> <rule id> <protocol: ICMP/TCP/UDP/any> <action: permit/deny>

命令: filter rule dstip <set id> <rule id> <type: (any/[ip] [subnet])>

命令: filter rule srcip <set id> <rule id> <type: (any/[ip] [subnet])>

命令: filter rule dstport <set id> <rule id> <type: (any/[port])>

命令: filter rule srcport <set id> <rule id> <type: (any/[port])>

[Rule Mode] [MAC Rule]

[Action] [Permit/Deny]

[Source MAC]

[Destination MAC]

[Delete]

允许用户删除 MAC 过滤规则。

命令: filter rule delete <set id> <rule id>

[Rule Mode] [IP Rule]

[Action] [Permit/Deny]

[Source IP] [Type/IP, Mask]

[Destination IP] [Type/IP, Mask]

[Source Port] [Type/Port]

[Destination Port] [Type/Port]

[Protocol] [ICMP/TCP/UDP/ANY]

[Delete]

允许用户删除 IP 过滤规则。

命令: filter rule delete <set id> <rule id>

[Rule List]

显示过滤集和过滤规则设定。

命令：filter rule show <set id> <rule id>

Attach

将过滤集分配到入口 / 出口端口来允许过滤功能。

[Filter ID]

显示过滤设置。

命令：filter show

[Ingress Port]

将过滤设置应用到一个入口端口。

命令：filter apply ingress <filter set id> <any/none/[port number]>

[Egress Port]

将过滤设置应用到一个出口端口。

命令：filter apply egress <filter set id> <any/none/[port number]>

[Reload]

从设置文件中恢复之前的设置。

命令：filter retrieve

5.3.6　安全命令

[Reauthentication]

允许用户启用或禁用周期重新认证功能。

命令：security dot1x bridge reauth <enable / disable>

[Reauthentication Time]

允许用户设置重新认证时间。

命令：security dot1x bridge reauthtime <reauthentication time (1-4294967295 sec)>

[Authentication Method]

允许用户设置认证模式 (RADIUS 或本地数据库)。

命令：security dot1x bridge authmeth <type (1:local 2:radius)>

[Quiet Period]

允许用户设置安静时间。

命令: security dot1x bridge quietperiod <quiet period (1-65535 sec)>

[Retransmission Time]

允许用户设置重传时间。

命令: security dot1x bridge retxtime <retransmission time (1-65535 sec)>

[Max Reauthentication Attempts]

允许用户设置重新认证尝试最大次数。

命令: security dot1x bridge reauthmax <max reauthentication attemps (1-10)>

[Multi-host]

允许用户对指定端口启用或禁用多主机功能。

命令: security dot1x port multihost <enable/disable><port list/*>

[Authentication Control]

允许用户对指定端口设置认证控制。

命 令: security dot1x port authctrl <type (1: force_authorized 2: force_unauthorized 3: auto)><port list/*>

[Guest VLAN]

允许用户为指定端口设置 guest VLAN ID。

命 令: security dot1x bridge port guestvlan <vlan id (0:no guest vlan)> <port list/*>

[Reload]

从设置文件中恢复之前的设置。

命令: security dot1x retrieve

[User Name]

[Password]

[Confirm Password]

[Dynamic VLAN]

在交换机的本地数据库中新建用户用于 802.1x 认证。用户记录包括用户名，密码和动态 VLAN。

命令：security dialinuser create

User Name: <user name string>

Password: <password string>

Confirm Password: <confirm password string>

Dynamic VLAN: <dynamic VLAN>

命令：security dialinuser remove <user name/*>

允许用户从数据库删除用户记录。

命令：security dialinuser modify <user name/*>

允许用户从本地数据库中修改用户记录。记录包含用户名，密码和动态 VLAN。

User Name: <new user name string>

Password: <new password string>

Confirm Password: <new confirm password string>

Dynamic VLAN: <new dynamic VLAN>

[Reload]

从设置文件中恢复之前的设置。

命令：security dialinuser retrieve

[Authentication Server IP]

[Authentication Server Port]

[Authentication Server Key]

[Confirm Authentication Key]

允许用户设置 RADIUS 服务器 IP，服务器端口和服务器密码。

命令：security radius set

authentication server ip <ip/none>: (old server ip)<new server ip >

authentication server port <port/default>: (old server port)<new server port>

authentication server key <key/none>: <server key>

confirm authentication key <key/none>: <confirm server key>

[Reload]

从设置文件中恢复之前的设置。

命令: security radius retrieve

[Generate SSH key]

允许用户生成 SSH 密码。SSH (Secure SHell) 是用于通过 shell 进行远程登录的协议。它的功能和 telnet 相似，但是，不同于 telnet，SSH 的所有在客户端和服务器传输的数据均进行加密。加密措施保护数据免造网络安全风险的侵害。目前，我们的交换机支持 SSH 协议第二版，同一时间只允许一位用户登录。 系统的闪存装置将储存两组 SSH 密码，这两组密码分别为 RSA 和 DSA 公共 / 私有密码。

命令: security sshkey start

[Reset SSH key]

将 SSH 密码重设为默认值。

命令: security radius default

[Show Generating Status]

显示 SSH 密码的生成状态。显示的结果有下列几种：“success”，“SSH keys generated fail”，“system is generating keys ...”。

命令: security sshkey show[Admin] [Enable/Disable]

允许用户启用 / 禁用特定端口的端口安全功能。

命令: security portsecu admin <enable/disable> <port list/*>

[Violation Mode] [Protect/Restrict/Shutdown]

允许用户为特定端口设置安全违背（violation）模式

命　令: security portsecu violation violation <mode (1:protect 2:restrict 3: shutdown)> <port list/*>

[Max MAC Addresses]

允许用户设置安全 MAC 地址的最大数目。

命令: security portsecu maxaddr <max number of addresses > <port no>

[Aging Time]

允许用户为特定端口设置老化时间。

命令: security portsecu age <age time> <port list/*>

[Aging Type] [Absolute/Inactivity]

允许用户为特定端口设置老化类型。

命令：security portsecu agetype <type (1:absolute 2:inactivity)> <port list/*>

[Restart]

允许用户重新启动特定的处于“shutdown”状态下的端口。

命令：security portsecu restart <port list/*>

[Port Selection]

[Query]

显示当前一些特定端口的安全 MAC 地址。

命令：security portsecu mac display <port list/*>

[MAC Address]

[Port Selection]

[Add]

为端口新增一个静态 MAC 地址。

命令：security portsecu mac add <mac address> <port no>

[Remove]

通过给定 MAC 地址、VID 或端口号删除一个安全地址，或清除某些指定端口的所有安全地址。

命令：security portsecu mac delete <mac address > <vid> <port no>

命令：security portsecu mac clear <port list/*>

[Reload]

从设置文件中恢复之前的设置。

命令：security portsecu retrieve

5.3.7　QoS 命令

[State] [No/CoS/DSCP]

允许用户设置某些特定端口的信任状态（trust state）

命令：qos trust state <no/cos/dscp> <port list/*>

[CoSOverride] [Disable/Enable]

允许用户启用或禁用某些端口的 CoS override 功能。CoS override 只能在 trust state 为 “No” 的时候才能启用。

命令：qos trust override <enable/disable> <port list/*>

[CoS to DSCP]

允许用户设置 CoS to DSCP 映射。

命令：qos map cosdscp <dscp1> <dscp2> <dscp3> <dscp4> <dscp5> <dscp6> <dscp7> <dscp8>

[DSP to CoS]

允许用户设置 DSCP to CoS 映射。

命令：qos map dscpcos <dscp list> to <cos priority>

[Class Name]

[Match][None/Filter/DSCP]

[Filter Set ID]

[DSCP][0/8/10/16/18/24/26/32/34/40/46/48/56]

[Add]

通过指定唯一的等级名称和匹配模式来创建一个新的等级。如果匹配模式为 “Filter”，拥护必须输入一个既存的过滤集 ID。如果匹配模式为 “DSCP”，用户必须输入 DSCP 值。如果用户输入 <dscp list>, <acl id> 将不会显示，且 <acl id> 变为 0。

命令：qos class new <class name>

命令：qos class match <class id(1-56)>

dscp (0/8/10/16/18/24/26/32/34/40/46/48/56): <dscp value>

acl id: <acl id>

[Modify]

允许用户修改一个等级的匹配标准。如果用户输入 <new dscp list>, <new acl id> 将不会显示，且 <new acl id> 变为 0。

命令：qos class modify <class id(1-56)>

dscp (old DSCP): <new dscp list>

acl id (old ACL ID):<new Acl ID>

[Remove]

允许用户通过制订级别 ID 来删除一个级别。用户可以输入 “*” 来删除所有级别。

命令：qos class delete <class id(1-56): * for all classes>

[Policy Name]

[Add]

通过指定一个唯一的名称来创建一个 policy (策略)。

命令：qos policy new <policy name>

[Remove]

允许用户通过选定 policy ID 来删除一个 policy。用户可以输入 “*” 来删除所有 policy。

命令：qos class remove <policy id(1-56): * for all policies>

[Edit]

[Class ID]

[DSCP]

[Traffic Rate]

[Traffic Burst Size]

[Exceed Action][None/Drop/DSCP]

[Exceed DSCP]

[Add]

允许用户通过指定 policy ID 和等级 ID 来新增一个新的 policy action (策略动作)。一个 policy 只能有 6 个 policy action。如果用户没有输入流量速率，下面的所有提示将不会显示。如果用户没有在 exceed act 输入 “none” 或 “drop”，<exceed dscp> 将不会显示。

命令：qos policy add <policy id(1-56)> <class id(1-56)>

dscp (0/8/10/16/18/24/26/32/34/40/46/48/56):<dscp value>

traffic rate(1-125): <traffic rate>

traffic burst size: <traffic rate size>

exceed act(none/drop/dscp): <exceed action>

exceed dscp(0/8/10/16/18/24/26/32/34/40/46/48/56): <dscp value>

[Modify]

允许用户通过指定 policy ID 和等级 ID 来修改 policy action。

命令：qos policy add <policy id(1-56)> <class id(1-56)>

dscp (old dscp value): <new dscp value>

traffic rate(old traffic rate): <new traffic rate>

traffic burst size(old traffic rate size): <new traffic rate size>

exceed act(old exceed action): <new exceed action>

exceed dscp(old dscp value): <new dscp value>

[Remove]

允许用户通过指定 policy ID 和等级 ID 来删除 policy action。用户可以指定一个 policy ID 并键入“*”来删除一个 policy 中的所有 policy action。

命令：qos policy remove <policy id(1-56)> <class id: * for all classes>

[Policy ID]

[Attach/Detach]

将 policy 分配到入口端口或从入口端口上解除。

命令：qos policy attach <policy id(1-56)> <port list/*>

命令：qos policy detach <policy id(1-56)> <port list/*>

[Reload]

从设置文件中恢复之前的设置。

命令：qos retrieve

[Scheduling Algorithm]

[CoS Queue][Weight]

设置 scheduler（调度） 模式。队列的权重延迟只有在权重轮转算法（WRR）和 bounded delay 算法下才有效。权重延迟的范围为 1-255。

命令：l2 cos sched <mode (1:strict 2:weighted round robin 3:bounded delay)> <Q1-Q4: weight delay>

[Priority] [CoS Queue]

允许用户将 CoS 优先级（范围为 0-7）映射到缓冲队列（共 4 个队列，队列 ID 为 1-4）。

命令：l2 cos map <queue id (1-4)> <cos (0-7)>

5.4　其他命令

sys time uptime: 显示从系统启动以来经过的时间

sys time date: 显示当前日期和时间

sys time settime: 设置当前时间

sys files config backup: 备份设置文件

sys files config default: 恢复出厂默认值

sys baud: 设置控制终端波特率

net ping: 对远程主机使用 ping 命令

net route show: 显示路由表中的记录

6 IP 地址，网络掩码和子网

6.1 IP 地址

本章节讲述关于 IPv4 (version 4 of the Internet Protocol) 的内容，而不涉及 IPv6 地址的情况。

本章节设定您已经了解了二进制，比特，字节等基础知识。您可以在参考附录中寻找到这些内容的详细信息。

IP 地址就好像 Internet 版本的电话号码，用于区分 Internet 上的单个节点（计算机或网络设备）。每个 IP 地址包含 4 个数字，每个数字的范围都是 0 到 255，之间用点区分，如 20.56.0.211。这些数字自左向右地被称做 field1，field2，field3，和 field4。

书写 IP 地址的习惯一般用十进制数字，之间用点区分，这称为十进制表示。 IP 地址 20.56.0.211 读作：“二零点五六点零点二一一”。

6.1.1 IP 地址的结构

IP 地址的层次设计与电话号码很相像。举例说明，一个 7 位的电话号码的前 3 位表示的是一个电话群组，其中包含上千路电话，后面的 4 位表示的是该电话的身份号码。

类似地， IP 地址包含两种信息。

网络 ID

在 Internet 或 Intranet 确认网络身份。

主机 ID

在网络中确认主机身份。

每个 IP 地址的第一部分包含网络 ID，其余部分则是主机 ID。网络 ID 的长度取决于网络的级别（见下面的章节）。表 7 显示的是 IP 地址的结构。

表 8. IP 地址结构

	Field1	Field2	Field3	Field4
A 类	网络 ID	主机 ID		
B 类	网络 ID		主机 ID	
C 类	网络 ID			主机 ID

下面是有效的 IP 地址范例:

A 类: 10.30.6.125 (网络号 = 10, 主机号 = 30.6.125)
B 类: 129.88.16.49 (网络号 = 129.88, 主机号 = 16.49)
C 类: 192.60.201.11 (网络号 = 192.60.201, 主机号 = 11)

6.1.2 网络类型

三种常用的网络类型为 A 类 ,B 类和 C 类。 (事实上还有一种 D 类地址, 但是它的特殊用途与我们这里讨论的主题无关。) 这些分类有它们各自的作用和特性。

A 类网络是 Internet 上规模最大的网络, 每个都可以容纳 160 万个主机。这样的超级网络最多只有 126 个, 总共支持 20 亿个主机。由于它们的容量庞大, 这些网络用于广域网或某些处于网络架构的组织, 如您的 ISP。

B 类网络比 A 类小, 但是其容量仍然很大, 每个 B 类网络可以容纳 超过 65,000 个主机。这样的网络一共有 16,384 个。B 类网络适合大型组织, 如大型公司或政府机构。

C 类网络是最小的, 一个 C 类网络最多只能容纳 254 个主机, 但是网络的总数却超过了 200 万 (2,097,152 个)。连接到 Internet 的局域网通常是 C 类网络。

一些与 IP 地址相关的重要信息:

从 field1 可以轻松识别地址类型:

field1 = 1−126: A 类

field1 = 128−191: B 类

field1 = 192−223: C 类

(field1 值中缺少的部分留作特殊用途)

主机 ID 可以是范围内除 0 和 255 的任何值, 这些值已留作专用。

6.2 子网掩码

网络掩码看起来像普通的 IP 地址, 但实际上它包含了一系列的比特表示 IP 地址的哪个部分是网络 ID, 哪些是主机 ID: 转换为比特后 1 表示 " 这是网络 ID", 0 表示 " 这是主机 ID"。

子网掩码是用来定义子网的 (用来将网络分为更小的部分)。一个子网的网络 ID 是从主机 ID" 借位 " 实现的。 子网掩码用于识别这些主机 ID 比特。

举例说明，设想将一个 C 网地址 192.168.1. 分为两个子网，您就需要用到下面的子网掩码:

255.255.255.128

将其转换为二进制容易看出它的真实面目:

11111111. 11111111. 11111111.10000000

就像 C 类地址一样，field1 到 field 3 都是网络，但是请注意 field 4 中第一个比特同样也被包括到了网络 ID 中。由于额外的比特只有两种值 (0 和 1)，就表示网络有两个子网，每个子网使用剩余的 7 位比特作为其主机 ID，范围是 0 到 127（而不是原来的 0 到 255 的 C 类地址）。

相似的，要将一个 C 类网络分为 4 个子网，掩码就是:

255.255.255.192 或 11111111. 11111111. 11111111.11000000

Field 4 中额外的两个字节可以有 4 个值 (00, 01, 10, 11)，因此产生了 4 个子网。每个子网使用剩余的 6 位比特作为其主机 ID，范围是 0 到 63。

一些子网掩码并不表示额外的网络 ID 比特，因此也没有子网产生。这样的掩码称为默认子网掩码，这些掩码是:

A 类: 255.0.0.0
B 类: 255.255.0.0
C 类: 255.255.255.0

这些称做默认掩码是因为网络在没有子网存在的时候已经设置完毕。

7 疑难排解

本章节列举出几种可用于诊断问题的 IP 工具。同时还列出一些可能出现的问题并附上建议解决方案。

所有已知的 bug 已经列在出货说明中。请在设置交换机前仔细阅读该说明。如果本手册中的解决方式仍无法解决问题，请与我们的客服部门联系。

7.1 使用 IP 工具诊断问题

7.1.1 ping

Ping 是用于检测您的计算机是否能够识别网络上其他计算机的命令。ping 命令想您指定的计算机送出一条信息，如果该计算机收到这条信息，它就会发送回应。要使用 ping 命令，您需要知道进行联络的计算机的 IP 地址。

在基于 Windows® 的计算机上，您可以打开开始菜单，然后点击“运行”，在提示符下键入命令如下:

ping 192.168.1.1

点击 OK。 您可以用已知局域网的私有地址或公共网络上的 IP 地址来替换。

如果目标计算机收到了这个信息，就会出现如图 70 所示的提示。

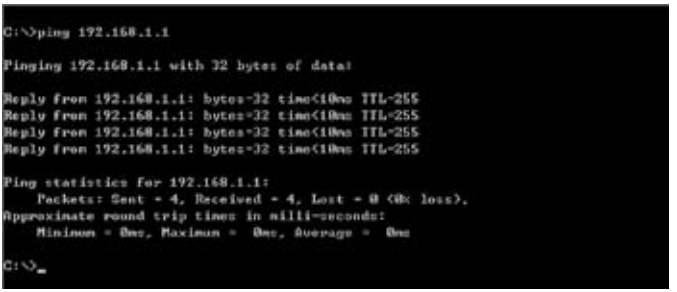

图 70. 使用 ping 工具

如果无法定位目标计算机，就会显示信息“Request timed out”。

ping 命令还可用于测试连接交换机的路径是否通行无阻 (使用默认的局域网 IP 地址) 或其他为交换机分配的地址。

您也可以通过键入一个外部地址，如 www.yahoo.com (216.115.108.243) 来检测通往 Internet 的路径是否畅通。如果您不知道某个 Internet 位置的 IP 地址，您可以使用 nslookup 命令，这个命令将在下节进行描述。

对于其他使用 IP 协议的操作系统，您可以在提示符下使用同样的命令，或通过系统管理工具来实现这个命令。

7.1.2 nslookup

您可以使用 nslookup 命令来决定与 Internet 站点相对应的 IP 地址。您可以指定一个普通名称，nslookup 将在您的 DNS 服务器中寻找 IP 地址（DNS 服务器一般位于您的 ISP）。如果该名称不在您的 ISP 的 DNS 服务器的记录中，地址请求就会发送到上级服务器，以此类推，直到找到地址为止。此时服务器就会将相对应的地址发送到您的计算机。

对于使用 Windows® 操作系统的计算机，您可以打开开始菜单点击“运行”，然后在文本窗口键入以下内容:

nslookup

点击 OK。 提示符后就会出现一个括号提示符 (>)。在这个括号提示符后键入 Internet 地址，如 www.absnews.com。

窗口就会显示相对应的 IP 地址，如图 71 所示。

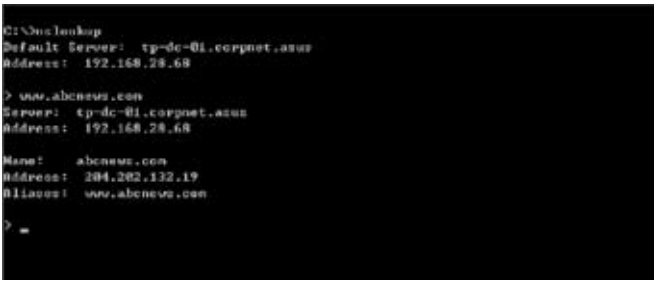

图 71. 使用 nslookup 工具

事实上，一个 Internet 域名可能对应很多个 IP 地址，尤其对网络流量大的站点。这些站点可能使用多个冗余服务器来储存相同的信息。

要退出 nslookup，在提示符处键入 exit 并按 <Enter> 。

7.2　更换故障风扇

当您卸下交换机背面的风扇模组时，请关闭交换机电源。

当交换机背面任何一个风扇出现故障时，您可以按照下列步骤进行替换。

1. 拧开将风扇固定在背部的螺丝。

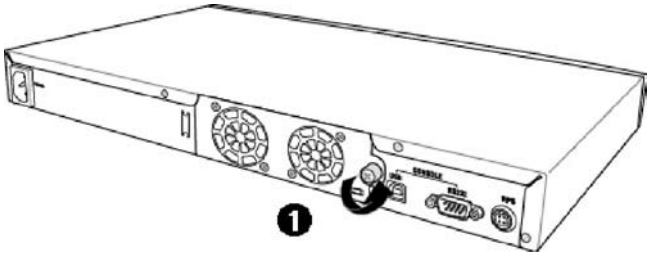

图 72. 拧开螺丝

2. 如图所示拉出风扇模组。

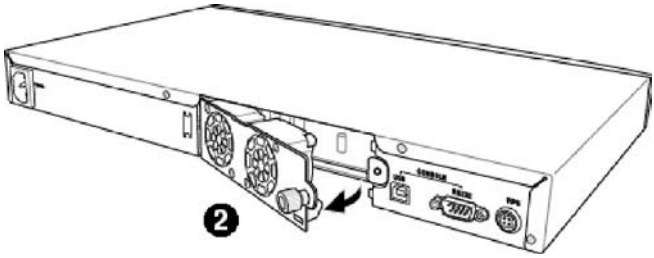

图 73. 拉出风扇模组

3. 从风扇上小心地拔下两条电源线。
4. 旋下将风扇固定在模组上的螺丝，卸下故障风扇。

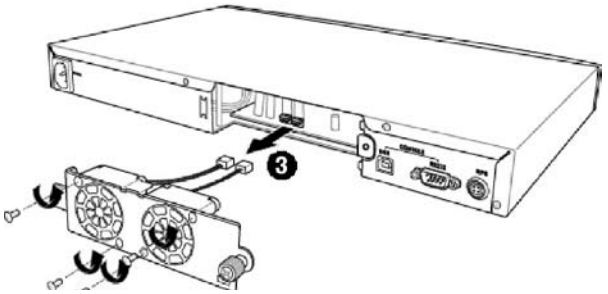

图 74. 卸下风扇

5. 将新的风扇装在原来风扇的位置，确保风扇电源线靠近模组底部。

   按照同样的步骤替换另一个风扇。

6. 将风扇电源线连接到 PCB 上，确认风扇电源线连接到正确的接口。当您面对交换机背部面板时，左边的风扇是风扇 1。

7. 将风扇模组置入交换机直至其卡入位置。确认风扇电源线没有卡在风扇模组和机箱之间。

8. 用螺丝固定风扇模组。检查风扇模组四周确认没有电线卡在风扇模组和机箱之间。

风扇规格

体积 : 40 x 40 x 20 mm

电压和电流 : 12VDC, 0.13A

转速 : 8200RPM

7.3　简易维修

下表内列出了一些交换机的常见问题，您可能在安装或使用交换机的过程中遇到这样的问题，同时该表也列出了一些建议的解决方案。

表 9. 疑难排解

问题	建议方案
LED	
系统打开后 SYSTEM LED 不亮	确认电源线是否连接到交换机或电源插座。
连接冗余电源后 RPS LED 不亮	1. 确认 RPS 电源线是否连接到电源插座。 2. 确认安装的 RPS 模组是否符合 RPS 标准
FAN LED 呈琥珀色闪烁	检查交换机背部的风扇，如果其中任一个风扇有故障，参见 7.2 替换风扇。
当连接千兆网口时，千兆以太网 Link LED 不亮	1. 确认以太网线是否正确地将交换机连接到您的局域网交换机 / 集线器 / 计算机。确认计算机 / 集线器交换机已经打开。 2. 确认缆线长度是否符合您的网络的要求。1000 Mbps 网络 (1000BaseTx) 须使用标有 Cat 5 的缆线。 10Mbit/sec 缆线可能支持低档缆线。
网络访问	
计算机不能访问同一网络中的另一个主机	1. 检查以太网网线是否完好，LED 是否呈绿色。 2. 如果端口的 LED 呈琥珀色，检查该端口是否被禁用。如果刚刚启用 STP，可能会出现短时间的网络中断。
计算机无法显示网页设置界面	1. 交换机以及打开并且连接端口也已经启用。交换机的出厂默认 IP 为 192.168.1.1. 2. 在您的计算机上确认您的网络设置。如果您的计算机没有设置一个有效的路由来连接到交换机，请将交换机 IP 改成您的计算机可以访问的 IP。 3. 从计算机 Ping 您的交换机 IP, 如果失败, 请重复第二步。 4. 如果 ping 成功，但是网页设置界面仍不能使用，请通过 RS232 或 USB 连接控制终端。检查是否有过滤规则或静态 MAC 地址将 WEB 流量堵塞。

（续下页）

问题	建议方案
网页设置界面	
丢失 / 忘记网页设置界面的用户名或密码	1. 如果您还没有修改用户名和密码，请尝试用户名 “admin”，密码为空。 2. 通过 RS232 或 USB 登录控制终端，使用 “sys user show” 显示丢失信息。
某些页面无法完全显示	1. 确认您使用的是 Internet Explorer® v5.5 或以后版本的浏览器。不支持 Netscape。您的浏览器必须启用 Javascript®， 也必须支持 Java®。 2.Ping 交换机的 IP 地址检查连接是否稳定。如果一些 ping 包丢失，检查您的网络设置确认设置有效。
设置修改无法保存	确认点击了 Save Configuration 页面的 Save 按钮。
终端界面	
不能显示终端仿真器上的文字	1. 出厂设置的波特率为 9600，无流量控制，8 位数据，无分集检测，停止位为 1 。 2. 将您的终端仿真器设置如上，如果您使用的是 USB 接口，请先安装 USB 驱动。 3. 检查连接线性能。

8 术语表

10BASE-T	用于以太网的有线线缆，数据传输率为 10 Mbps。亦称 3 类线 (CAT 3) 。参见 data rate, Ethernet。
100BASE-T	用于以太网的有线线缆，数据传输率为 100 Mbps。亦称 5 类线 (CAT 5) 。参见 data rate, Ethernet。
1000BASE-T	用于以太网的有线线缆，数据传输率为 1000 Mbps。
binary	二进制。“基于 2 ”的数字系统，只使用 0 和 1 两个数字来表示所有的数字。在二进制中，十进制数字 1 写作 1 , 十进制 2 写作 10，十进制 3 写作 11，十进制 4 写作 100, 依次类推。虽然 IP 地址为方便起见表示为十进制数字，实际上它使用的是二进制数字。比如 IP 地址 209.191.4.240 转换为二进制是 11010001.10111111.00000100.11110000。比特，IP 地址，网络掩码同样也是二进制。
bit	比特。“二进制数字”的缩写，一个比特就是一个只有 0, 1 两种数值的数字。参见 binary.
bps	比特每秒
CoS	服务级别。在 802.1Q 中规定，值的范围为 0 到 7。
DSCP	差分服务代码点 IP 报头中差分服务部分最重要的六位被称为 DSCP。GigaX 系列中可用的 DSCP 值有 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 和 56。
broadcast	广播。将数据发送到网络上所有的计算机。
download	以下行的方向传输数据，例如，从 Internet 到用户。
Ethernet	以太网。最常见的计算机网络技术 , 通常使用双绞线。以太网的数据传输速率为 10 Mbps 和 100 Mbps。参见 10BASE-T, 100BASE-T, twisted pair。
filtering	根据过滤规则，筛选出符合条件的数据类型。过滤可以是单向 (进入或外出)，也可以是双向的。
filtering rule	判断路由设备应该接受还是拒绝某种类型数据的规则。过滤规则是用于单个 (或多个) 界面操作的, 并且有特定的方向性 (上行、下行或双向)。
FTP	文件传输协议 用于连接到 Internet 的计算机之间的文件互传。常见的用途包括上传或更新网页服务器上的文件 , 从网络服务器下载文件。

host	主机。连接到网络的设备（通常指计算机）。
HTTP	超文本传输协议 HTTP 是用来进行网络数据传输的最主要的协议，可以通过网页浏览器显示。参见 web browser, web site。
ICMP	互联网控制信息协议 一种互联网协议，用于报告错误与其他网络相关信息。ping 命令就是基于这种协议。
IGMP	互联网组管理协议 一种互联网协议，允许计算机与其网络组员通过组播群组共享信息。一个计算机组播群组就是群组的组员都设置成从成员处接收特定的内容信息。向 IGMP 群组发送组播的应用有随时更新群组的地址簿或将公司的通告发送到收信人列表。
IGMP Snooping	在每个端口侦测 IGMP 封包并将端口与二层组播群组相关联。
Internet	国际互联网，用于私人或商业通信。
intranet	私有的公司内部网络，看起来像国际互联网 (Internet) 的一部分（用户使用网页浏览器来访问信息），但是只能被本公司员工所使用。
IP	参见 TCP/IP。
IP address	Internet 协议地址 主机（计算机）在 Internet 上的地址，它包含四个数字，每个数字的范围是 0 ~ 255, 用小数点分隔。如，209.191.4.240。一个 IP 地址包含了网络 ID 和主机 ID，网络 ID 表示主机属于哪个特定的网络，主机 ID 则是网络中确定该主机的唯一标志。网络掩码用来定义网络 ID 和主机 ID。由于 IP 地址比较难记，它们通常都对应一个域名（domain name）。参见 domain name, network mask。
ISP	Internet 服务提供者 向顾客提供 Inernet 访问服务的公司，通常是收费的。
LAN	局域网 存在于一个较小地理范围内的网络，例如家里，办公室或大楼。
LED	发光二极管 一种电子发光设备。SL-1000 前面的指示灯就是 LED。
MAC address	介质访问控制地址，简称 MAC 地址 由制造商分配的设备永久性硬件地址。 MAC 地址由六对字符

	组成。
mask	掩码。参见 network mask。
Multicast	组播。将数据发送到一组网络设备上。
Mbps	兆比特每秒的缩写。网络数据传输率常表示为 Mbps。
Monitor	监视。亦称“Roving Analysis”，允许将一个网络分析器连接到端口上并使之监测交换机的其他端口。
network	网络。指连接在一起，允许相互通信和共享资源（如软件、文件等）的一组计算机。网络可以是小型的，例如局域网 (LAN)，也可以是大型的，例如 Internet。
network mask	网络掩码。网络掩码就是一系列的比特字串用于 IP 地址，以决定网络 ID 和主机 ID 的位数。 1 表示此比特有效，0 表示忽略此比特。举例说明，如果网络掩码 255.255.255.0 应用到 IP 地址 100.10.50.1，网络 ID 为 100.10.50，主机 ID 为 1。参见 binary, IP address, subnet, “IP Addresses Explained” 部分。
NIC	网络接口卡
	插入计算机，提供网络线缆的物理接口 RJ-45 的适配器。参见 Ethernet。
packet	封包。在网络上传输的数据单位。每个封包都包含一个有效载荷（数据），以及包头信息如来源地址和目的地址等。
ping	分组互联网探测器
	用于确认 IP 地址对应的主机是否能够到达。它亦可用于寻找与域名相对应的 IP 地址。
port	端口。实体的网络设备接入点，如计算机，路由器，数据通过该接入点流入流出。
protocol	协议。一系列用于控制数据传输的规则。为了是数据能够成功传输，数据传输源和目标都必须遵守相同协议的规则。
PVLAN	私有虚拟局域网
QoS	服务质量（Quality of Service）
	在 802.1Q 中定义。对于数据通信网络性能，QoS 特性有带宽、延迟和可靠性。
remote	远程。即物理上处于不同地点。比如说，一名职员出差在外时登录公司的 intranet，他就是远程用户。
RJ-45	注册接口标准 45
	这种 8-pin 的插头是用于在电话线上传输数据的。以太网线通

常也会使用这种插头。

RMON 远程监测

SNMP 的扩展，提供综合性的网络监视功能。

routing 路由。在您的网络和互联网之间，根据源 IP 地址和网络情况，选择最有效的路径转发封包。执行路由选择的设备称为路由器。

SNMP 简单网络管理协议

用于管理网络的 TCP/IP 协议

STP 生成树协议 防止封包在复杂网络中造成环路的桥接协议。

subnet 子网。子网是网络的一部分，子网通过将网络中的计算机归分为小组而使这些计算机与其他网络上的计算机分隔开来。子网中的计算机仍然在物理上与其他上层网络相连，但是他们被认作是一个独立的网络。参见 network mask。

subnet mask 子网掩码。将子网之间加以区分的掩码。参见 network mask。

TCP 参见 TCP/IP。

TCP/IP 传输控制协议 / 互联网协议

这是互联网上基本的协议组。TCP 负责将数据分为可以在互联网上传输的封包，IP 负责将这些封包发送到目的地址。当 TCP 和 IP 与一些 上层应用进行捆绑如 HTTP, FTP, Telnet 等，TCP/IP 指的确是整套协议组。

Telnet/SSH 一种互动的，给予字符的，用于访问远程计算机的程序。HTTP（网络协议）和 FTP 只允许从远程计算机下载文件，而 Telnet / SSH 允许从远程进行登录并使用计算机。

TFTP 小型文件传输协议

一种传输文件的协议。TFTP 比 FTP 更加容易使用，但是性能和安全性不如 FTP。

Trunk 两个或两个以上的端口合而为一成为一个虚拟端口，也称为链路汇聚。

TTL 存活时间

IP 封包的一个字段，决定了该封包的寿命。TTL 原本表示的是持续时间，现在则通常用于表示最大计跳数，每经过一跳都消耗一个计跳数，当 TTL 为零时，该封包就被丢弃。

twisted pair 双绞线。即普通的铜制电话线。它包含一对或多对互相缠绕的电线，以消除干扰和杂音。每根电话线使用一对线，在家用情况下，通常都安装两对。对于以太网局域网，使用的是一

	种更高级的 , 用于 10BASE-T 网络的三类线 (CAT 3) , 以及更高级的 100BASE-T 网络的五类线 (CAT 5)。参见 10BASE-T, 100BASE-T, Ethernet。
upstream	上行。数据从用户流向互联网的方向。
VLAN	虚拟局域网
WAN	广域网
	所有的分布于广大的地理位置的网络统称广域网 , 如一个国家或一个洲。当涉及 SL-1000 时 , 广域网指的既是互联网。
Web browser	网页浏览器。一种使用超文本传输协议 (HTTP) 的 , 用于从网站下载 / 上传信息的软件。这些信息包括文本 , 图像 , 声音或视频。网页浏览器使用了超文本传输协议 (HTTP)。常用的网页浏览器包括 Netscape Navigator 和 Microsoft Internet Explorer。参见 HTTP, web site, WWW。
Web page	网页。一个网站的文件通常包括文本 , 图像 , 和连接到其他页面的超链接。当拥护访问一个网站时 , 显示的第一页成为主页。参见 hyperlink, web site。
Web site	网站。互联网上通过网页浏览器为远程用户的提供信息的计算机。网站常由包含文本 , 图像 , 超链接的网页构成。参见 hyperlink, web page。
WWW	万维网
	也称 Web。全球范围内可通过 Internet 访问的所有网站的总和。

9 索引