GigaX 系列

二层可网管交换机

用户手册

C1757 2004 年 12 月

华硕联络信息

华捷联合信息（上海）有限公司（莘庄）
电话：021-54421515/1616/4949/2424
传真：021-54420088/0099/0066
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：020-85572366/70/71
传真：020-85572352/2355
地址：广州中山大道西高新技工业园建工路 12 号 1-3 楼
邮编：510665

华捷联合信息（上海）有限公司成都办事处
电话：028-82916655/56/58
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
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：北京市海淀路 52 号太平洋科技大厦 13 层
邮编：100080

华硕技术支持：
免费咨询电话：800-8206655
Email：tsd@asus.com.cn
NetQ 论坛：Netq.asus.com.cn

华硕工程师提供在线技术支持

目录表

图表目录

表格目录

1 简介

再次感谢您购买华硕 GigaX 系列二层可网管交换机。从现在开始您可以通过友好、功能强大的用户界面来管理您的局域网（LAN：local area net）。此用户手册将为您提供安装及设置 GigaX L2 可网管交换机所需的相关信息。

1.1 L2 二层交换机 规格

- (GigaX 2048) 48 个 10/100BASE-TX 自适应高速以太网接口
- (GigaX 2024) 24 个 10/100BASE-TX 自适应高速以太网接口
- 2 个 10/100/1000BASE-T 自适应千兆以太网接口
- 2 组 SFP、GBIC 插槽
- 10/100BASE-TX 及 10/100/1000 BASE-T 端口自适应 MDI/MDIX
- 兼容 IEEE 802.3u、802.3z 及 802.3ab 规格
- 802.1D 透明桥接/生成树协议
- 802.1w RSTP (快速生成树协议)
- 硬件支持 8K MAC 地址缓存
- 支持 802.3x 流量控制
- 基于 802.1Q 帧标记虚拟局域网（VLAN）,最多可支持 255 个 VLAN
- 支持 802.1p 服务级别（class of service）,每个端口 4 组队列
- 支持 IGMP snooping
- 支持 802.3ad 链路汇聚（link aggregation）中继（trunking），最多可支持 6 组中继
- 支持 LACP (链路汇聚控制协议 Link Aggregation Control Protocol)
- 支持端口镜像
- 支持访问控制列表
- 支持 RMON 远程网络监控：支持 4 个群组 (1, 2, 3, 9)
- 支持 SNMP（简易网络管理通信协议） v1, v2, v3
- 支持 MIB-II（管理信息数据库-II）
- 针对 PSU、风扇、系统温度和电压的企业级 MIS 管理

- 支持 Telnet 或 SSH 远程登录
- 可通过 FTP 更新固件及备份配置文件
- IEEE 802.1x 验证 (动态 VLAN 指派)
- 支持 DHCP 侦测
- 支持 Syslog 系统日志记录
- 支持终端控制端口、Telnet 及 SSH 命令行命令功能
- Web 图形用户界面
- LED 链路状态指示灯
- LED 系统、冗余电源 (RPS)及风扇状态指示灯

1.2 关于本用户手册

1.2.1 注意事项

- 本手册对文中及术语表第一次出现的首字母缩写词做解释。
- 为方便起见，GigaX 可网管交换机简称为“本交换机”。
- 本手册中局域网（*LAN*）与网络（*network*）交替使用，是指在一定范围内通过以太网连接的一组计算机的集合。
- 除非另有说明，本手册中的图标及网络界面均适用于 GigaX 2048 及 GigaX 2024 交换机。

1.2.2 排版字体

- *斜体*字代表命令行解释程序的参数。
- **黑体字**表示从菜单及下拉列表中选择的项目，以及程序提示的文本信息。

1.2.3 提示符号

本用户手册中会出现以下图表及说明文字，请特别注意：

提供进一步的信息说明

解释文中出现的术语或名词。这些术语也可包含在术语表中。

提示需高度注意的信息，请您在进行某一项操作时注意安全

2 开始使用 GigaX 系列交换机

2.1 产品包装信息

您的产品包装包含以下信息：

- GigaX 2048 (48 个端口)或 GigaX 2024 (24 个端口) L2 二层交换机
- 交流电源线
- 仿真调制解调器排线 (DB9)
- 机架安装配件组 (两个固定托架及六颗 #6-32 螺钉)
- USB 规格的终端线
- 安装光盘
- 快速安装指南

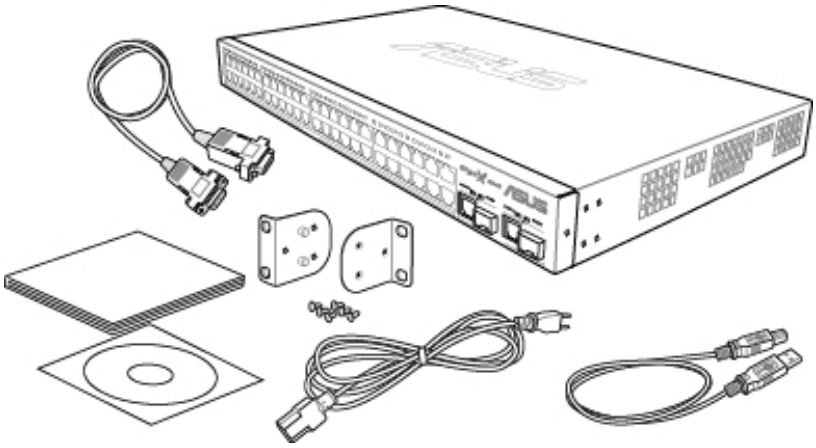

图 1. GigaX L2 交换机包装内容

前面板

前面板包括 LED 指示灯，可显示系统、冗余电源、风扇及端口的状态。

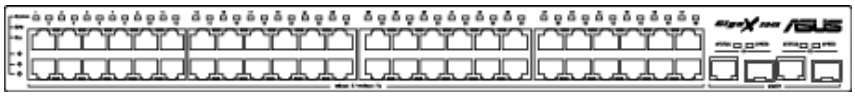

图 2. 前面板 (GigaX 2048)

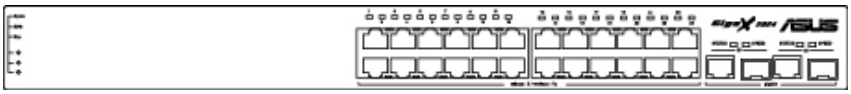

图 3. 前面板 (GigaX 2024)

表 1. 前面板标示及 LED 指示灯说明

标示	颜色	状态	说明
SYSTEM（系统）	绿色	亮灯	系统电源开启
		闪烁	自动检测、INIT 或程序下载中
	琥珀色	亮灯	温度或电压异常
	熄灭		无电源供应
RPS（冗余电源）	绿色	亮灯	电源装置（PSU ）工作正常，冗余电源充足
	琥珀色	亮灯	PSU 工作异常，系统目前由冗余电源供电
	熄灭		无电源供应（系统指示灯熄灭）, 冗余电源工作异常或未安装（系统 LED 指示灯亮）
FAN	绿色	亮灯	所有风扇运转正常
	琥珀色	亮灯	一个或两个风扇都停止运转
10/100 ports	绿色	亮灯	已建立网络连接
		闪烁	数据传送/接收中
	熄灭		无网络连接
	琥珀色	亮灯	已建立连接，但端口被手动或生成树协议屏蔽
		闪烁	端口处于 STP 阻塞（ blocking）或侦听（ listening）/ 学习（learning）状态
10/100/1000 port status	绿色	亮灯	已建立连接(RJ-45 或 SFP)，端口启用
		闪烁	数据传送/接收中
	熄灭		无网络连接
	琥珀色	亮灯	已建立连接，但端口被手动或生成树协议屏蔽
		闪烁	端口处于 STP 阻塞 （ blocking）或侦听（ listening）/ 学习（learning）状态
10/100/1000 port speed	绿色	亮灯	1000Mbps
	琥珀色	亮灯	100Mbps
	熄灭		10Mbps

2.2 后面板

本交换机后面板包括数据端口与电源插座。

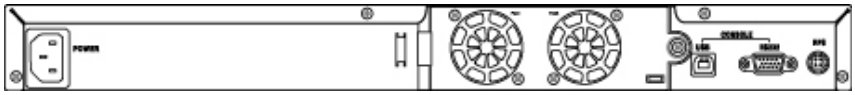

图 4. 后面板

表 2.后面板标示说明

No.	标示	说明
1	Power Connector	连接电源线
2	FAN1 – FAN2	可更换式系统风扇
3	Console USB	终端控制管理 USB 接口
4	Console RS232	终端控制管理 RS-232 串行接口
5	RPS	冗余电源插口

2.3 技术规格

表 3. 技术规格

尺寸	43.5mm(H) X 444 mm(W) X 265mm(D)		
电源	输入	耗电量	
	100-240V AC/2.5A 50-60Hz	< 90 watts	
冗余电源 (RPS)	输入	输出	
	100-240V AC/1.8A 50-60Hz	12V DC/12.5A	
环境需求		操作中	储存
	温度	-10 -50℃ (14 to 122℉)	-40 - 70℃ (-40 - 158℉)
	湿度	15-90%	0-95%
	海拔	最高达 10,000 英尺 (3,000m)	40,000 英尺 (12,000m)
可更换风扇	尺寸	电压与电流	速度
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

3 快速安装指南

本章节主要介绍 GigaX 的基本环境设置。您可参考 GigaX 的快速安装指南。

第 1 部分 如何将 GigaX 安装在一个水平表面或机架上

第 2 部分 提供基本的硬件设置方式

第 3 部分 如何设置 GigaX

在您开始设置之前，请先向您的网络管理员获得以下信息：

本交换机的 IP 地址

本交换机的默认网关

本交换机的子网掩码

3.1 第 1 部分 —硬件安装

将本交换机连接至电源插座、计算机或网络。

图 5 显示了本交换机的硬件连接。

3.1.1 将交换机安装至水平表面

本交换机应被安装在水平表面，且该表面能支撑本机及其配件的重量。在本机底部的标示区域贴上四块橡皮垫。

3.1.2 将交换机安装至机架

1. 将固定托架锁在本机两侧，并将机体置入机架。
2. 用螺钉将托架锁在机架上。

3.2 第 2 部分 —设置交换机

将本机连上电源，并连接至计算机与网络。见图。

3.2.1 连接终端口

欲进行终端控制管理，可使用一条 RS232 (DB9) 或 USB 线缆连接至交换机。若您欲使用 WEB 界面，请用一条以太网线将您的 PC 连接至交换机上。

3.2.2 连接计算机或局域网

请使用以太网线将计算机连接至交换机的连接端口。或者连接集线器/交换机至本交换机端口。您可以使用交叉式（crossover）或直连式（straight）以太网线连接您的计算机、集线器或交换机。

请使用第五类以太网双绞线连接 1000B SE-T 以太网端口。否则，链路速度将无法达到 1Gbps。

3.2.3 连接 RPS 模块

将您的 RPS 模块连接至 RPS 插孔，并确认其另一端已连接至电源线。将电源线连接至接地的插座上。

3.2.4 连接电源适配器

1. 将交流电源线连接至本机后面板的电源插座，并将另一端连接至墙上的电源插座或延长线上。
2. 根据表 4 的内容，检查前面板的 LED 指示灯。若 LED 指示灯符合该表内容，则表明本交换机工作正常。

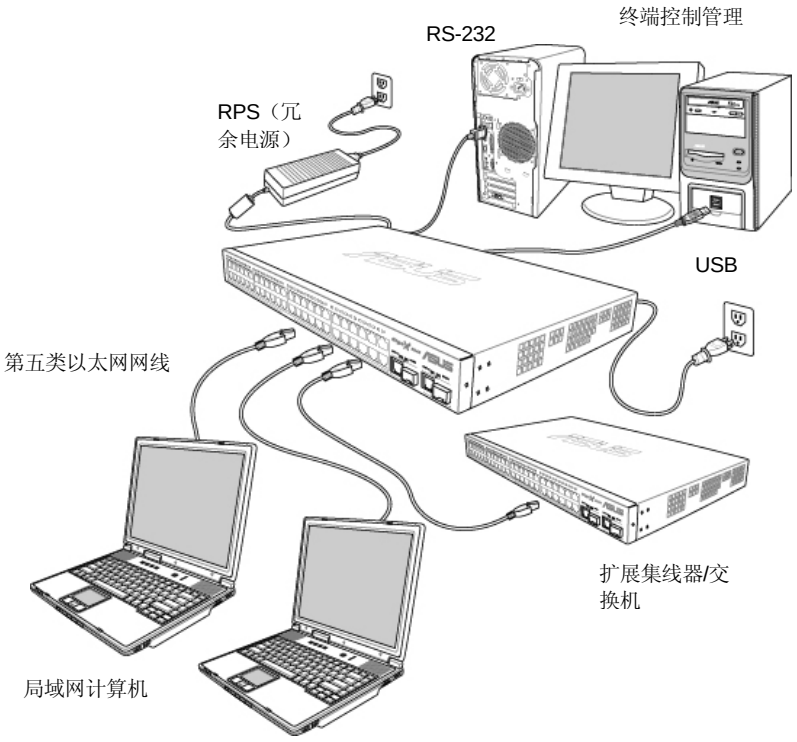

图 5. 硬件连接示意图

表 4. LED 指示灯

No.	LED	说明
1	System	绿灯恒亮表明装置启用。若灯不亮，请检查电源适配器是否连接至本交换机并且通电。
2	Switch ports [1] - [50] (2048) [1] - [26] (2024)	绿灯恒亮表明交换机的网络功能正常。闪烁表示正在接收或传送数据至网络上的其它计算机。
3	RPS	绿灯恒亮表示已成功安装 RPS 模块。
4	Fan	绿灯恒亮表明所有风扇运转正常。

3.3 第 3 部分 — 交换机网络管理基本设置

硬件安装完成以后，您的交换机还需要做一些基本设置。您可以利用以下方法设置本交换机：

- Web 管理接口：您可使用具备 Java®功能的浏览器如 IE5.5 或更新版本的浏览器来管理交换机。
- 终端机命令行界面：使用超级终端接口管理交换机。

3.3.1 通过终端控制端口设置

1. 使用本机所附的交叉式 RS-232 线缆连接本交换机后端的终端控制端口。此端口为 DB-9 的公接头，提供数据终端设备(DTE)的连接。将排线上的螺钉锁好固定，然后将排线上的另一端连接至运行终端机仿真软件如 Hyper Terminal 的 PC 上。
2. 您也可使用本机所附的 USB 排线连接到 PC 上。但在使用 USB 之前，您必须安装本机随机光盘内的 USB 驱动程序，该驱动程序支持 Windows ME/2K/XP 操作系统，该驱动程序会在操作系统中建立一个模拟 COM 端口。

3. 请按照以下步骤设置您的终端机仿真软件：
   a) 选择适当的串行端口号码
   b) 设置数据波特率（data baud rate）为 115200bps (某些型号上为 9600bps)
   c) 设置数据格式为无同位检查（no parity），8 个数据位（data bit）及 1 个停止位（stop bit）。
   d) 设置流量控制为无
   e) 设置仿真模式（emulation mode）为 VT1000
4. 设置好终端机后，您将在终端机上看到“(ASUS)%”的字样。
5. 输入“login”可进入接口的命令列。默认的用户名是“admin”。密码无需输入，按下**<Enter>**键即可。

您可随时通过 CLI 来更改密码 (参考5. 1系统命令)。为避免您的交换机被未经许可的人士使用，建议您及早更改密码。

6. 欲指定 IP 地址给本交换机，请参考以下步骤：
   a) 输入“net interface ip sw0 <your ip address> <your network mask>”。例如，您的交换机 IP 是 192.168.10.1，子网掩码是 255.255.255.0。那么，您应该输入“net interface ip sw0 192.168.10.1 255.255.255.0”。
   b) 若本交换机必须通过网络来管理，就必须要默认网关或一个静态路由。输入“net route static add 0.0.0.0 <your network gateway IP> 0.0.0.0 1”为您的默认路由。如图 6

b)

```
(Asus)% login
user name: admin
password: ****

user 'admin' logged in

(Asus)% net interface ip sw0 192.168.10.1 255.255.255.0
IP address set successfully

(Asus)% net route static add 0.0.0.0 192.168.10.254 0.0.0.0 1
Route added successfully

Specific route is added successfully

(Asus)% _
```

图 6. 登录及 IP 设置界面

3.3.2 通过 Web 界面设置

欲成功地连接 PC 至交换机，您的 PC 必须具有可以访问该交换机的有效 IP 网络。请联系您的网络管理员以获得交换机的合法 IP 地址。若您欲更改默认 IP， 请参考 3.3.1 章节相关方法操作。由于本机并不支持 DHCP 功能，您必须指定合法的固定 IP 地址来使用网络接口。

1. 第一次使用网络接口时无需用户名称及登录密码，因为网络存取验证功能是关闭的。为确保系统设置的安全性，请启用“System”单元下“Administration”页面的验证功能。若验证功能关闭，可略过第 2 步。
2. 本交换机可连接至任何本网络内的计算机，请打开网页浏览器 (Internet Explorer)并在地址栏输入以下地址，按**<Enter>**键：

   http://192.168.1.1

   此为本交换机的出厂默认 IP 地址。

   一个登录画面将会出现，如图 7 所示：.

图 7. 登录界面

输入您的用户名称及密码，点击 OK 进入设置管理页面。第一次登录时请使用以下缺省值：

默认用户名称：	Admin
默认密码：	(无密码)

您可以随时更改密码（见 5.3.1 系统 令).

3. 欲建立新的 IP 地址，请点击“**System**”，然后点击“**IP Setup**” (见图)。输入 IP 地址，子网掩码与默认网关，然后点击 OK。
4. 若新地址与缺省值不同，浏览器将无法更新交换机状态窗口或重新取得任何页面，这是正常情况。请在地址栏重新输入新的 IP 地址，并按**<Enter>**键，网络随即恢复正常。
5. 欲激活 Web 访问验证功能，点击菜单中的“**Administration**”，然后选择“**Enabled**”以激活保护功能。

   在您点击 OK 后将会出现登录画面。见下页图示。

请注意 GigaX 2048 与 2024 型号具 相同的网络接口，只是画面上方的前面板图示有所不同 见下页图示)。

在以下章节中，当两种型号的画面 容相同时，将只显示其中一个画面（GigaX 2048）。若 面内容不同，则两种型号均会列出。

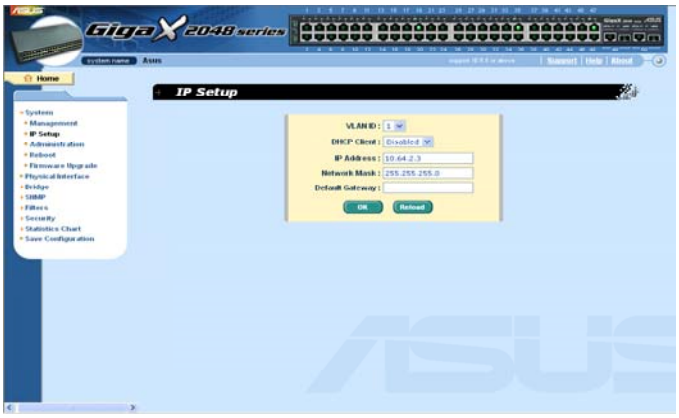

图 8. IP 设置(GigaX 2048)

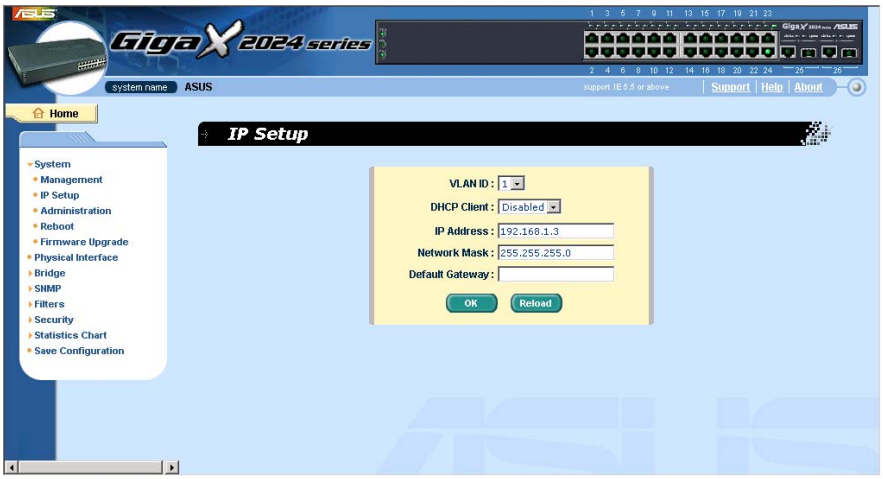

图 9.IP 设置(GigaX 2024)

4 通过 Web 界面管理

本交换机提供一个 Web 管理界面，可让您通过 Internet 来管理交换机。支持此管理界面的最佳工作平台是 Microsoft Internet Explorer® 5.5 或更新版本。
注意：不支持 Netscape。

4.1 登录 Web 用户界面

1. 请打开 PC 上的网页浏览器，在地址栏中输入以下地址，并按**<Enter>**键：

   http://192.168.1.1

   此为交换机的出厂默认地址，接下来会出现一个登录画面，如图 10：.

图 10. 登录界面

注意：若您未开启网络存取验证功能，则无需在此画面登录。（见 3.3.2).

2. 输入您的用户名称及密码，然后点击 OK 。

当您第一次登录时，请使用以下缺省值。您可以随时通过 CLI 更改登录密码（参考 5.3.1系统命令)。

默认用户名称：	admin
默认密码：	<无密码>

您每次登录时都会出现此主页画面。(如图)

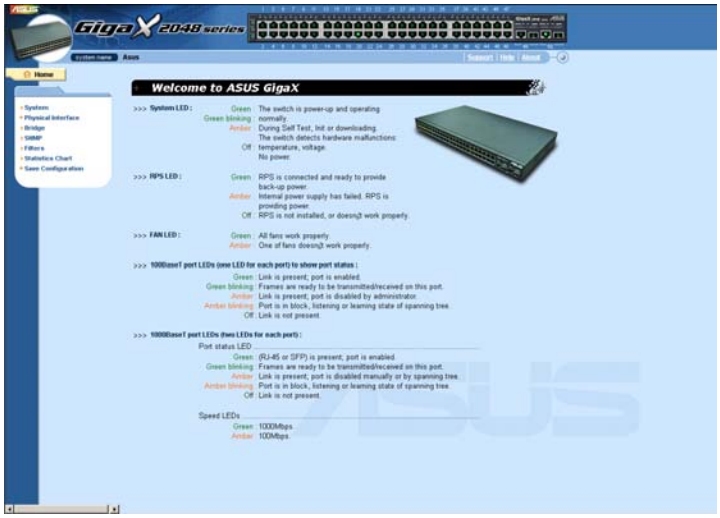

图 11. 主页 (GigaX 2048)

图 12. 主页 (GigaX 2024)

4.2 功能布局（Functional layout）

一个典型的网页通常包括三个主要的页框。上页框包含交换机 logo 与前面板图示，如图 13、14。此页框会一直出现在窗口画面的最上方，且 LED 指示灯会定期更换。LED 指示灯的意义请参考表 4。表 5 为端口颜色说明。

图 13. 上页框 (GigaX 2048)

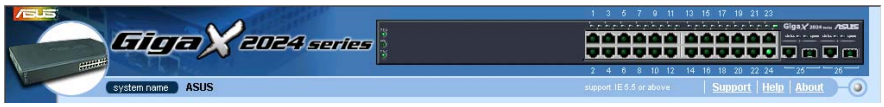

图 14. 上页框 (GigaX 2024)

表 5. 端口颜色说明

端口颜色	说明
绿色	以太网连接正常
黑色	以太网未连接
琥珀色	已联机，但连接端口被手动关闭或生成树屏蔽

点击交换机端口图标，右下方页框会出现端口设置菜单。

左页框菜单如图 15，包含了所有交换机设置的功能。这些功能包含在几个主要的项目中，例如 System、Bridge 等。您可以点击各项功能来进行相关的设置。


System
Management
IP Setup
Administration
Reboot
Firmware Upgrade
Physical Interface
Bridge
Spanning Tree
Link Aggregation
Mirroring
Static Multicast
IGMP Snooping
Traffic Control
Dynamic Addresses
Static Addresses
Tagged VLAN
Default Port VLAN & CoS
CoS Queue Mapping
DHCP Snooping
SNMP
Community Table
Host Table
Trap Setting
VACM Group
VACM View
USM User
Filters
Filter Set
Filter Attach
Security
Port Access Control
Dial-in User
RADIUS
Statistics Chart
Traffic Comparison
Error Group
Historical Status
Save Configuration

图 15. 扩展菜单列表

右框架显示设置页面或统计图表。详见章节4.3。

4.2.1 菜单浏览技巧

- 欲展开群组功能菜单， 请点击该群组名称。展开后符号▸将变成▾。
- 欲关闭群组功能菜单，请点击该群组名称。▸符号会出现在该群组功能名称的后面。
- 欲开启特定的设置页面，请直接点击所需的菜单项目。

4.2.3 常用按纽及图标

下表说明各个按纽及图标的功能。

表 6. 常用按纽及图标

按纽/图标	功能
OK	储存该页面上的任何更改设置
Add	在目前的系统增加新的设置，如一个静态 MAC 地址或一个防火墙 ACL 规则等
Modify	修改目前状态
Edit	修改系统目前设置，如一个静态路由或一个过滤器 ACL 规则等
Remove	删除选定项目，如一个静态路由或一个过滤器 ACL 规则等
Reload	重新显示目前页面，且已加载统计或设置

4.3 系统设置页面（System Pages）

系统页面包括网管设置(management)、IP 设置、管理员设置(administration)、重新启动（reboot）及固件更新（firmware update）等功能。

4.3.1 网管设置（Management）

Management 页面包含了以下信息：

Model Name: 产品名称

MAC Address: 交换机 MAC 地址

System Name: 用户指定的系统名称 (可修改)

System Contact (可修改)

System Location (可修改)

点击 OK 按钮可储存变更并使其立即生效。点击 Reload 按钮可刷新设置，如图 16：

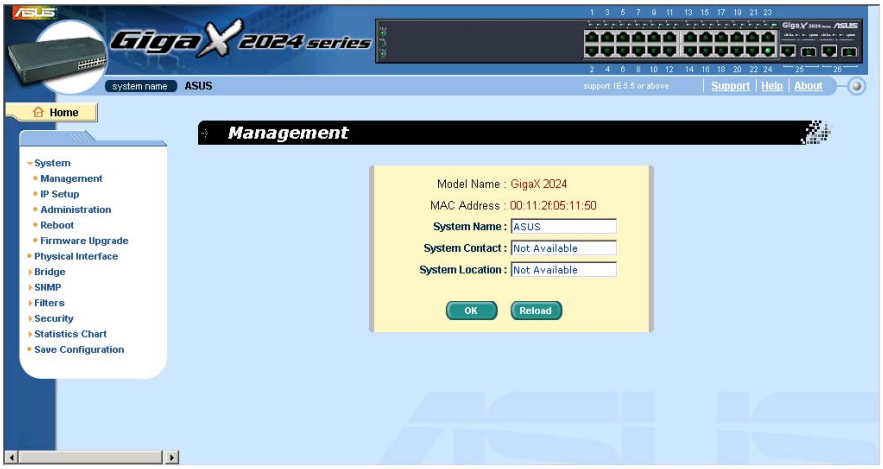

图 16. 网管设置页面

4.3.2 IP 设置

本交换机支持动态 IP 与静态 IP。动态 IP 来自同一 VLAN 内的 DHCP 服务器。**IP 设置**页面包括以下可修改信息：

VLAN ID: 指定一个 VLAN ID 到系统管理接口。要求在同一 VLAN 内。

DHCP Client: 启用 DHCP 以获得动态 IP 地址，或关闭 DHCP 以指定静态 IP 地址。DHCP 服务器必须在网管设置 VLAN 内。

IP Address: 指定静态 IP 地址到交换机网管设置接口。

Network Mask（子网掩码）

Default Gateway（默认网关）

点击 OK 按钮可储存变更并使其立即生效。点击 Reload 按钮可刷新设置，如图 17：

图 17. IP 设置

4.3.3　管理员设置（Administration）

Administration 页面利用*密码保护*功能来启用或关闭 Web 访问验证功能。缺省值为关闭网络存取验证功能。

点击 OK 按钮可存储变更并使其立即生效。点击 Reload 按钮可刷新设置，如图 18 所示。当您启用密码保护功能时，您必须立即重新登录。

您可以随时通过 CLI 更改密码。

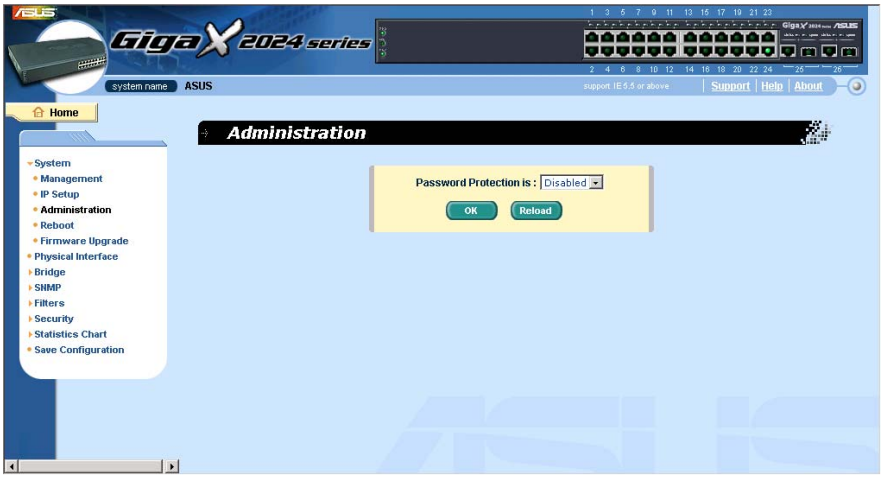

图 18. 管理员设置页面

4.3.4 重新启动（Reboot）

Reboot 页面包含一个 Reboot 按钮。点击此按钮可重新启动系统。

当您重新启动系统时，将会停止网络传输并中断 Web 界面访问。

固件升级（**Firmware Upgrade**）

Firmware 页面包含以下信息：

Hardware Version: 显示硬件版本号

Boot ROM Version: 显示 Boot ROM 版本

Firmware Version: 显示当前运行的固件版本。当您更新固件时，此版本号也会随之更新。

在 firmware 字段中直接输入固件所在的位置，或点击 Browse... 从窗口中选择一个固件文件名称。点击 Upload 可更新交换机的固件。请参考图 19。

请您在点击 upload 按钮并成功更新固件后，重新启动系统，然后重新登录。

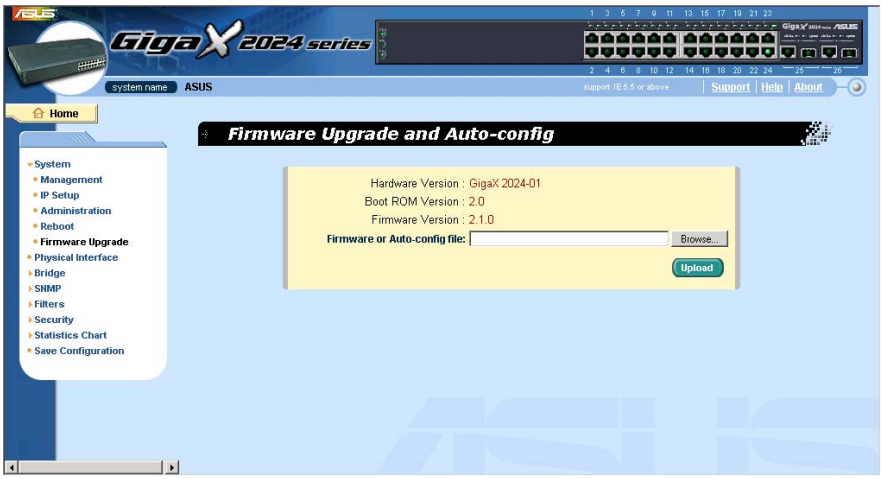
GigaX 2024 series
system name
ASUS
Support
Help
About
Home
Firmware Upgrade and Auto-config
System
Management
IP Setup
Administration
Reboot
Firmware Upgrade
Physical Interface
Bridge
SNMP
Filters
Security
Statistics Chart
Save Configuration
Hardware Version : GigaX 2024-01
Boot ROM Version : 2.0
Firmware Version : 2.1.0
Firmware or Auto-config file:
Browse...
Upload

图 19. 固件升级

4.4 物理接口（Physical Interface）

物理接口（Physical Interface）可显示网络端口的实时状态。您可进行以下设置：

Port（端口）: 选择端口进行设置

Admin（管理）: 关闭/启用端口

Mode（模式）: 设置速率及双工模式

Flow Control（流量控制）: 启用/关闭 802.3x 流量控制

Port Status Window（端口状态窗口）: 显示各个连接端口的以下信息：

a) Link status（连接状态）: 显示既有连接的速率及双工模式，或连接中断
b) State（状态）: STP 状态
c) Admin（管理）：设置不同的值启用或关闭端口
d) Mode（模式）：设置不同的值调节连接速度及双工模式
e) Flow Control（流量控制）：设置不同的值启用或关闭 802.3x 流量控制

选择所需的连接端口号码，并进行相关的设置，然后点击 

按钮，显示画面将会显示更新后的内容。然而，新的设置值在您选择 “*Save Configuration*” 之前并不会生效。

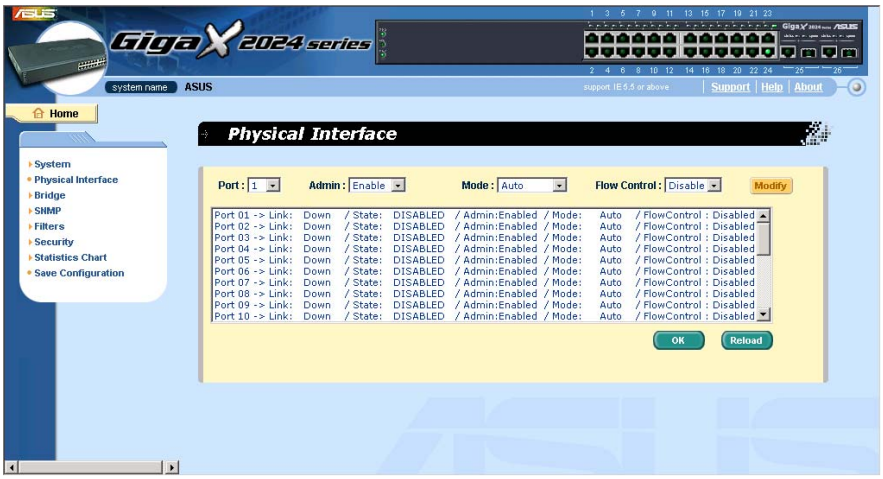
GigaX 2024 series
system name
ASUS
support IE 5.5 or above
Support
Help
About
Home
System
Physical Interface
Bridge
SNMP
Filters
Security
Statistics Chart
Save Configuration
Physical Interface
Port : 1
Admin : Enable
Mode : Auto
Flow Control : Disable
Modify
Port 01 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 02 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 03 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 04 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 05 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 06 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 07 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 08 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 09 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
Port 10 -> Link: Down / State: DISABLED / Admin:Enabled / Mode: Auto / FlowControl : Disabled
OK
Reload

图 20. 物理接口

4.5 桥接设置（Bridge）

Bridge 页面包含大部分二层设置，如链路汇聚（link aggregation）、STP 等。

4.5.1 生成树（Spanning Tree）

生成树通信协议的设置页面可以实时关闭或启用此功能。此页面包含三个部分：

第一部分显示 root 信息：描述根交换机的 STP 设置

第二部分为 STP 设置，包含以下几个选项：

Disable/STP Enable/RSTP Enabled: 启用或关闭 STP/RSTP。当您启用 STP/RSTP 时，若交换机为 root 交换机，STP/RSTP 将使用以下设置：

Hello Time（问候间隔）：BPDU 数据包生成间隔

Max Age（最长存在时间）：所有交换机等待 BPDU 数据包的最长时间

Forward Delay（转发延迟）：交换机转发延迟时间

Bridge Priority（优先级）：设置相对于生成树中其它交换机的优先级

第三部分为端口设置：包含一个显示窗口以显示各个端口目前的设置值。点击 Modify 可改变 STP/RSTP 的端口设置。包含以下项目：

Port（端口）：选择所需的端口进行设置

Priority（优先级）：设置交换机中端口的优先级。数值越低，表明优先级越高。若 STP 检测到网络回路，则端口的优先级越低，被阻塞的可能性越大。设置的有效值是 0-255。

Path Cost（Path 成本）：有效值为 1-65535。若 STP 检测到网络回路，则连接成本越高，被阻塞的可能性越大。

Edge Port（边缘端口）: 所有端口均预设为 edge ports。接收到 BPDU 时，Edge port 即变为 STP 端口。edge port 进入转发状态只需很短的时间。

点对点（Point to Point）：自动/是/否。全双工链接被视为点对点的链接。否则，就成为共享链接。点对点的链接所需的集中时间更少。多数情况下，建议选择“自动”。

点击 OK 可使设置生效。点击 Reload 可刷新设置值至当前值。

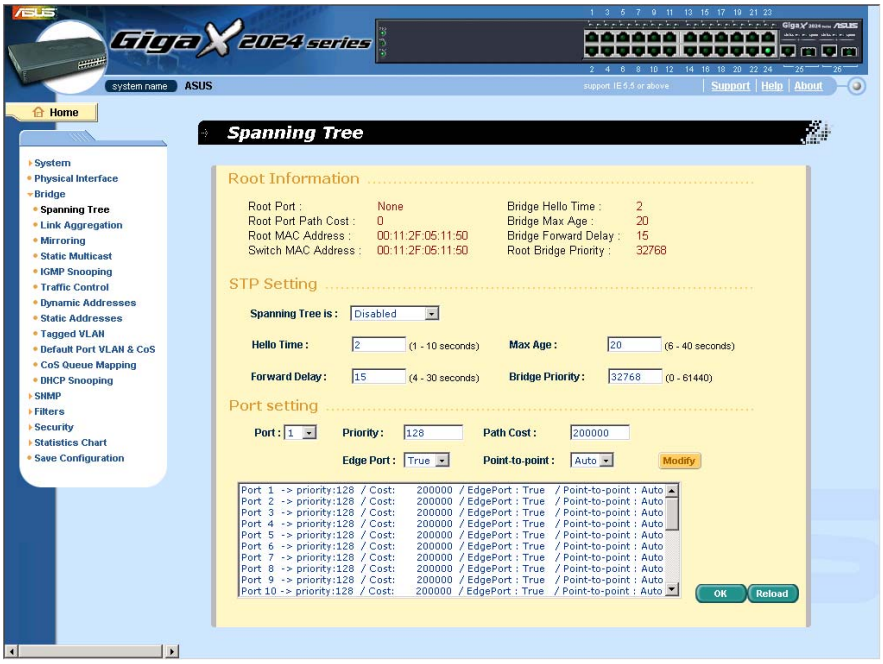

图 21. 生成树

4.5.2　链路汇聚（Link Aggregation）

此页面设置链路汇聚组（端口中继）。本交换机可建立 6 组链路汇聚组。

Show Trunk: 选择“Add a new Trunk” 以建立新的中继线。或选择一个既有中继线，显示以下内容项目及连接端口图标。

Port Selection Criterion: 在链路汇聚的端口之间分配数据包，决定于源 MAC 地址，目的 MAC 地址，源及目的 MAC 地址，源 IP 地址，目的 IP 地址，或源及目的 IP 地址。

Name: 组名

Trunk ID: 名称之外用以识别中继群组的代码

LACP: 在选定的中继线上启用/关闭 LACP。LACP 模式设置为“活动”

Remove Trunk: 删除选定的中继线

Port Icons: 端口图标排列成如前面板的方式。点击图标可选择群组成员，若再次点击该图标，则可从该群组删除该端口。

点击 OK 按钮可将设置值发送到交换机（HTTP 服务器）。点击 Reload 可刷新到当前设置值。欲使设置生效，请至“*Save Configuration*”页面，点击 Save 按钮。

您需要检查运行链路速率及双工模式，以确保该中继线处于实体运作状态。进入物理接口界面，检查中继端口运行状态窗口的链路模式。若所有中继成员均具有相同的速率且都运行于全双工模式，则中继干线设置成功。若其中一个成员速率不同或未运行于全双工模式，则设置不成功。检查连接的端口并更改设置，以使所有中继干线成员具有相同的速率且都运行于全双工模式。

- 群组成员**必须**属于同一个 8 端口簇。千兆端口可在同一个群组中。
  GigaX 2048 的簇是端口 1-8，端口 16，端口 17-24，端口 25-32，端口 41-48。
  GigaX 2024 的簇是端口 1-8，端口 16，端口 17-24。
- 链路汇聚群组中的所有端口**必须**在全双工模式、相同速率下运行。
- 链路汇聚群组中的所有端口**必须**在自动或全双工模式下设置，否则全双工链路无法生效。若在强制全双工模式下设置，则其它端口也必须有相同的设置，否则此链路汇聚无法正常工作。
- 链路汇聚中的所有端口**必须**具有相同的 VLAN 设置。
- 链路汇聚中的所有端口视为单一的逻辑连接。也就是说，

若其中任何一个改变了属性，其它的也会随之改变。例如，一个干线由端口 1 和端口 2 组成，若端口 1 的 VLAN 改变，则端口 2 的 VLAN 也会随着端口 1 改变。

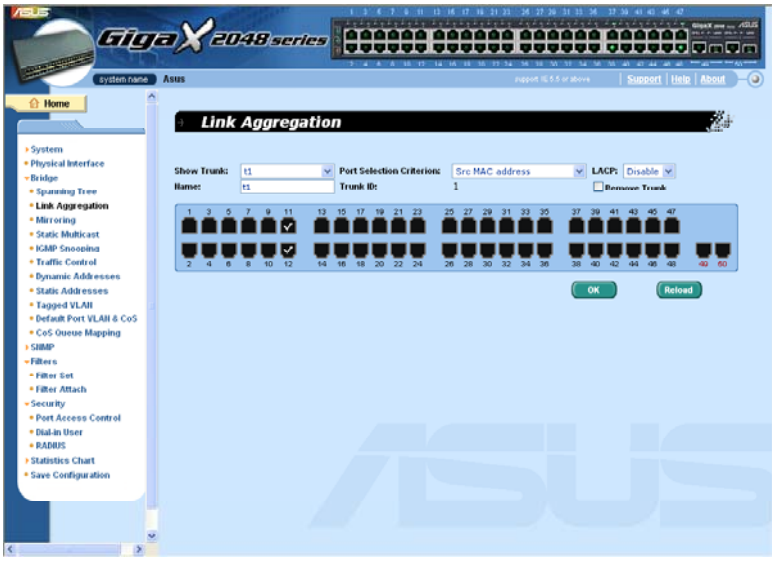

图 22. 链路汇聚 (GigaX 2048)

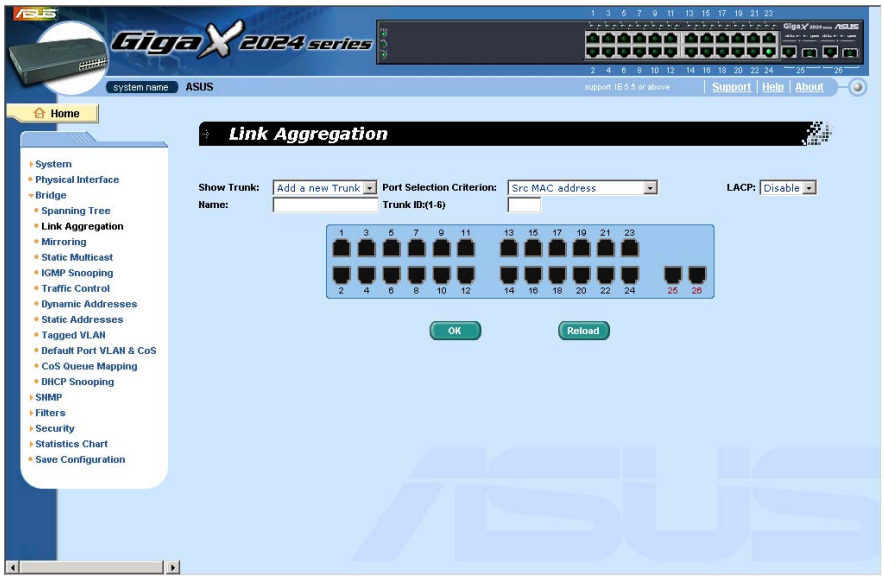

图 23. 链路汇聚 (GigaX 2024)

4.5.3 端口镜像（Mirroring）

通过端口镜像与网络传送分析仪（network traffic analyzer），可监控网络流量。您可监控特定端口上的数据包传送或接收。

Mirror: 选择镜像群集。每一个群集可以包含 24 个 Fast Ethernet 端口与 1 个 Gigabit 端口。(仅 GigaX 2048 交换机)

Mirror Mode: 启用或关闭所选群集的端口镜像功能。

Monitor Port: 接收所有被端口镜像的端口发出的传输信息备份。

GigaX 2048 有两个端口镜像端口。每个端口可监控 24 个 Fast Ethernet 端口与 1 个 Gigabit 端口。

GigaX 2024 仅有 1 个监控端口。此端口可监控 24 个 Fast Ethernet 端口与 2 个 Gigabit 端口。

监控端口不能属于任一链路汇聚。

监控端口不能作为一般的交换机端口来使用　它无法交换数据包或做地址识别。

点击 OK 按钮可将设置发送到交换机 (HTTP 服务器)。点击 Reload 按钮可将设置值刷新到当前值。

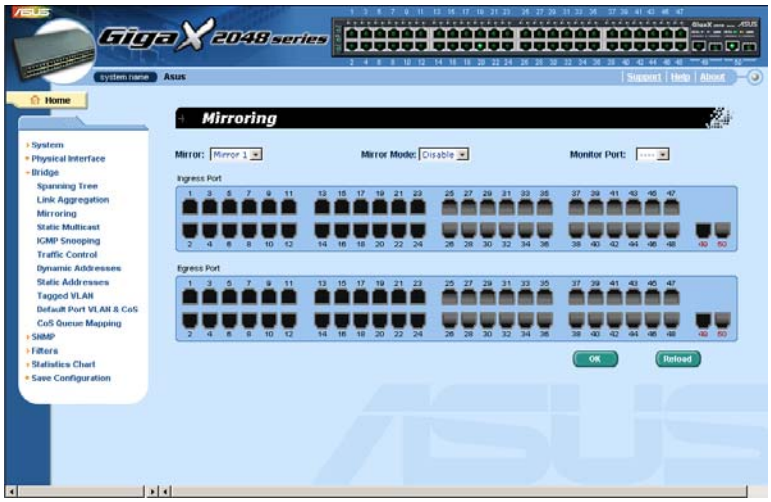

图 24. 端口镜像设置页面 (GigaX 2048)

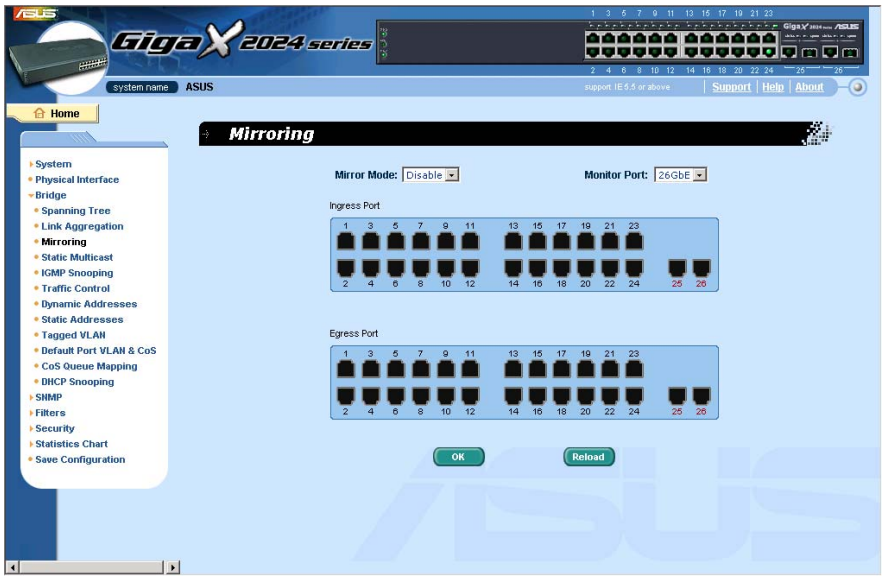

图 25. 端口镜像设置页面 (GigaX 2024)

4.5.4　静态组播（Static Multicast）

此页面可新增多重组播地址至组播表。本交换机最多可支持 256 个组播条目。群组中的所有端口均可转发特定的组播数据包至群组中的其它端口。

Show Group: 选择“Add a new Group”可增加新的群组。也可选择既有的群组以显示以下信息

MAC Address: 选择组播地址

VLAN: 选择 VLAN 群组

CoS: 给服务级别分配优先级

点击 OK 按钮可使设置生效。点击 Reload 按钮可刷新设置为当前值。

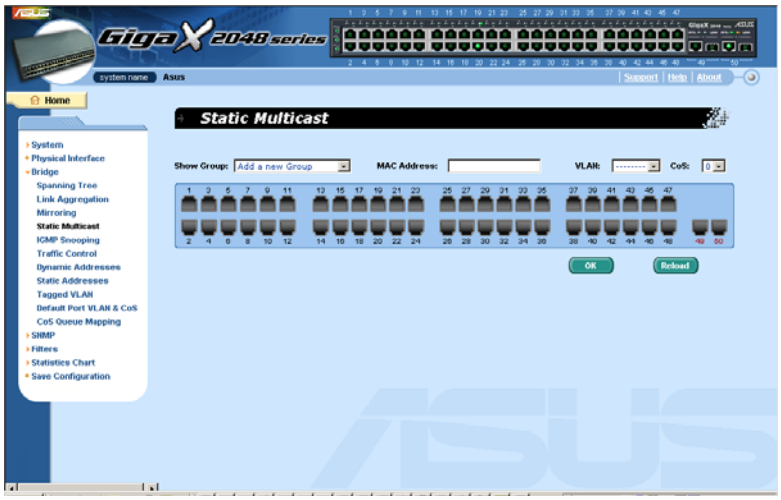

图 26. 静态组播 (GigaX 2048)

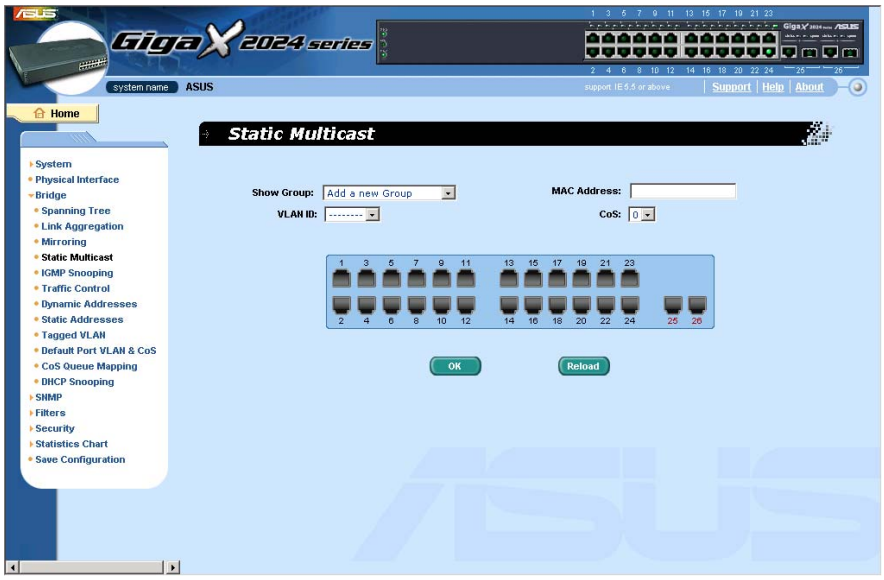

图 27. 静态组播 (GigaX 2024)

4.5.5 IGMP 侦测（IGMP Snooping）

使用 IGMP 协议侦测，可减少网络的组播传送。启用本功能时，交换机会侦测 IGMP 数据包并将新的群组列入组播表。然而，若静态组播占据所有的 256 个表项，IGMP 侦测将无法正常工作。本交换机仅支持 256 个二层组播群组。

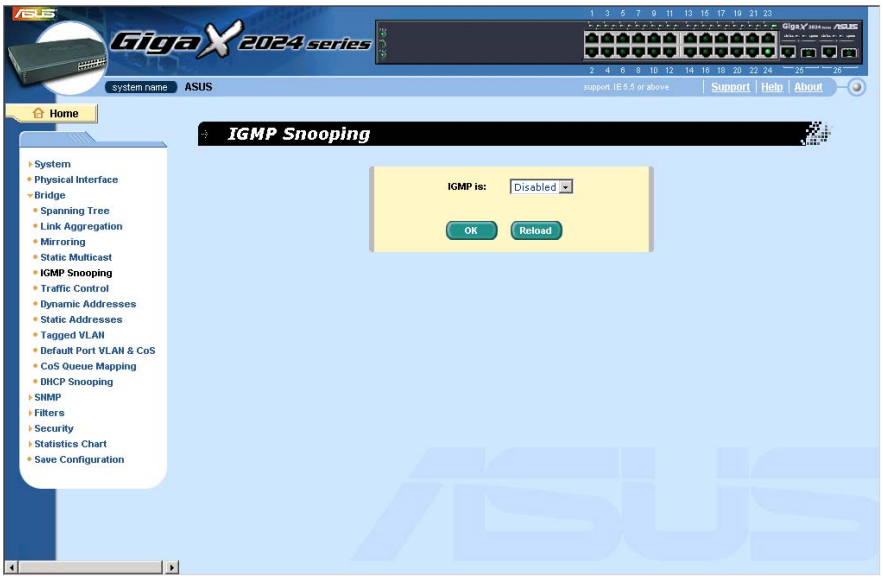

图 28. IGMP 侦测

4.5.6　流量控制（Traffic Control）

流量控制可防止因广播数据包、组播数据包及目的地址错误造成的单播数据包流量过大，导致交换机带宽泛洪。Limit 字段用来限制该形态数据包的整体传输量。例如，当启用组播与广播功能时，则此两种形态数据包的整体传输量将不会超过限制的传输量。点击 OK 按钮可保存新的设置。欲使设置值生效，请至 “*Save Configuration*”页面，点击 Save 即可。

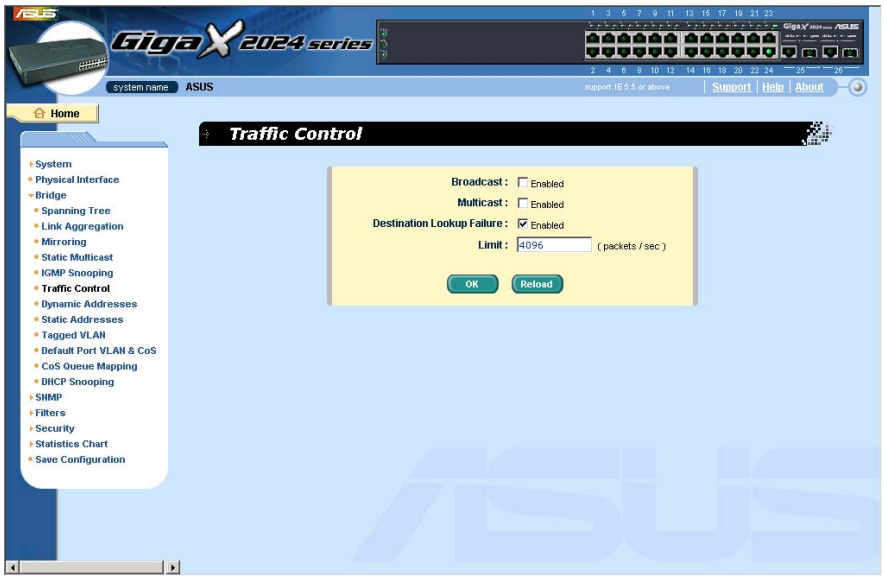

图 29. 流量控制

4.5.7 动态地址（Dynamic Addresses）

本页面显示经由端口、VLAN ID 或特定 MAC 地址查询到的动态 MAC 地址结果。动态地址是指交换机交换机识别的 MAC 地址，若超过存在时间将会从地址表中删除。用户可以设置 10-1,000,000 秒的存在时间。点击 OK 按钮保存新的时间值，为使设置值生效，请进入 “*Save Configuration*”页面，点击 Save 按钮。

您可通过选择端口、VLAN ID 或/和 MAC 地址并点击 Query 来查询。地址窗口将会显示查询结果。


GigaX 2024 series
system name
ASUS
support IE 5.5 or above
Support
Help
About
Home
System
Physical Interface
Bridge
Spanning Tree
Link Aggregation
Mirroring
Static Multicast
IGMP Snooping
Traffic Control
Dynamic Addresses
Static Addresses
Tagged VLAN
Default Port VLAN & CoS
CoS Queue Mapping
DHCP Snooping
SNMP
Filters
Security
Statistics Chart
Save Configuration
Dynamic Addresses
Query by
Port
Port 1
VLAN ID
(1 ~ 4094)
Query
MAC Address
Age Setting
Aging Time :
300
(10 - 1000000 seconds)
OK
Reload

图 30. 动态地址

4.5.8 静态地址（Static Addresses）

您可增加一个 MAC 地址至交换机地址表。以此种方式新增的 MAC 地址，不会有存在时间限制而被从地址表中删除，此即成为静态地址。

MAC Address: 输入 MAC 地址

VLAN ID: 输入此 MAC 的 VLAN ID

Port Selection: 选择此 MAC 地址所属的端口

Discard: 当 MAC 地址以目的地址、源地址或两者兼之的形式存在于数据包之中时，您可运行数据包过滤功能。

通过以上信息，点击 Add 按钮可建立新的静态 MAC 地址 。接下来您将在显示窗口看到此新增条目。欲删除既有地址时，您可先用鼠标点选，然后点击 Remove 按钮。Modify 按钮可更新既有的 MAC 地址，OK 按钮可储存设置。点击 Reload 按钮可刷新设置至当前值。欲使设置值生效，请至“save configuration”页面，点击 Save 。

图 31. 静态地址

4.5.9 VLAN 标记（Tagged VLAN）

您最多可设置 255 个 VLAN 群组，并在本页显示所有的 VLAN。本交换机已建立一个默认的 VLAN，且无法删除，可防止交换机发生故障。除此 VLAN 外，您可删除任何既有的 VLAN。

您可通过点击端口按纽来指定连接端口为标记或未标记。共有三种类型的按纽：

“U” 型：端口未标记，将从传送数据包中删除 VLAN 标记

“T” 型：此连接端口传送的所有数据包均加标记

“空白”型：此端口非 VLAN 群组成员

若一个未标记端口同时属于两个或多个 VLAN 群组，会使交换机发生混乱，从而引起流量泛洪。为防止这种情况发生，本交换机仅允许一个未标记成员在同一时间属于一个 VLAN。即：未标记端口属于一个称为“PVID”的 VLAN 群组，可在 “Default Port VLAN & CoS” 页面设置。若您想将一个未标记端口从一个 VLAN 配置到另一个 VLAN， 您必须先将其从原来的 VLAN 删除，或在原来的 VLAN 中先将其改为标记成员。

Show VLAN： 选择一个既有的 VLAN 显示其内容或选择 “Add a new VLAN”新增一个 VLAN 群组

Name：VLAN 名称

DHCP Snoop：启用或关闭此 VLAN 的 DHCP 侦测功能

VLAN ID：当您新增一个 VLAN 时，请输入 VLAN ID

Remove VLAN：删除一个既有的 VLAN。此项在新增 VLAN 页面中不会出现。

点击 

按纽保存设置。欲使设置生效，请至 “*Save Configuration*” 页面点击 

按纽。

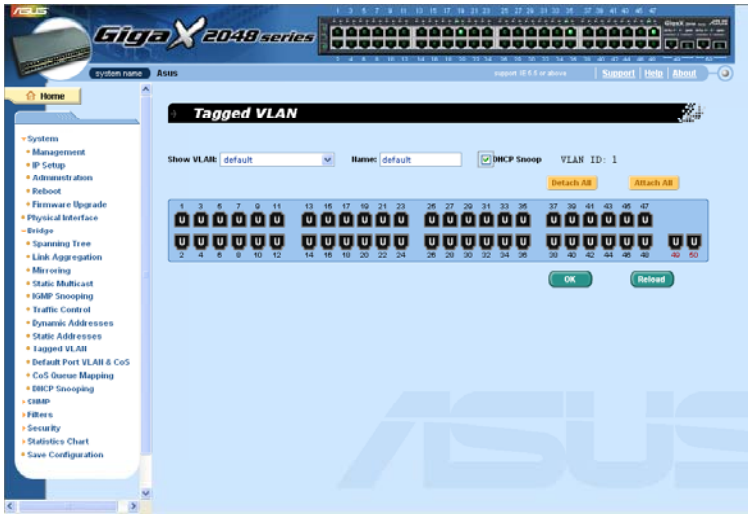

图 32. VLAN 标记 (GigaX 2048)

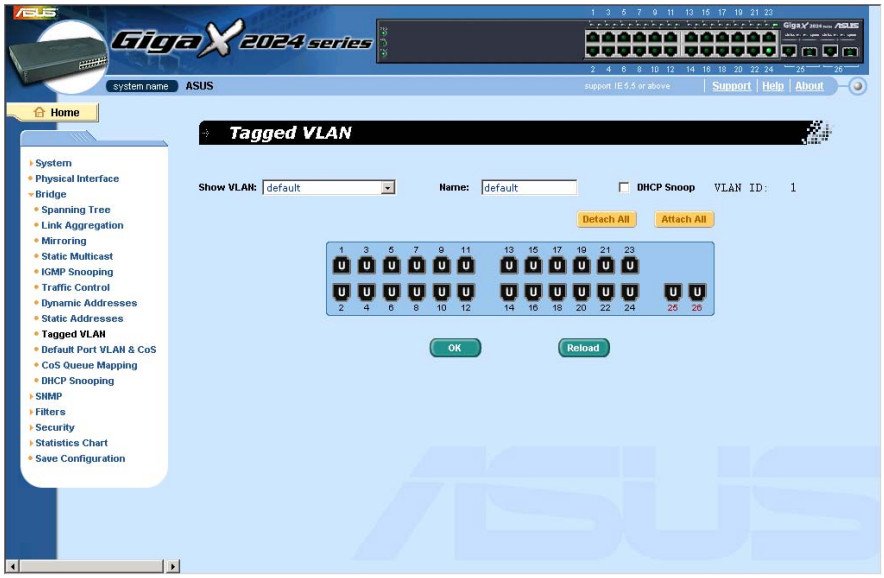

图 33. VLAN 标记 (GigaX 2024)

4.5.10　默认端口 VLAN 及服务级别（CoS）

本页面包含每个端口里部分与 VLAN 标记相关的设置。具体包括：

Port: 选择欲设置的端口

PVID: 基于端口的 VLAN ID。进入此端口的所有未标记数据包均使用此 VLAN ID 标记。

CoS (服务级别)值：进入此端口的所有未标记数据包均使用此指定的 VLAN 标记的 CoS。

点击 Modify 按钮可改变端口列表窗口里的内容。点击 OK 按钮可保存设置。欲使设置生效，请至 “*Save Configuration*”页面，点击 Save 按钮。

图 34. 默认端口 VLAN 及 CoS

4.5.11 CoS 优先级缓冲队列

本交换机的每一个端口均支持 4 个缓冲优先级等级，亦即每个 CoS 顺序值都可对应到这 4 个等级的其中之一。Queue 4 具有最高的数据包传送优先级。点击 OK 按钮可保存设置。欲使设置生效，请至 “*Save Configuration*”页面，点击 Save 按钮。

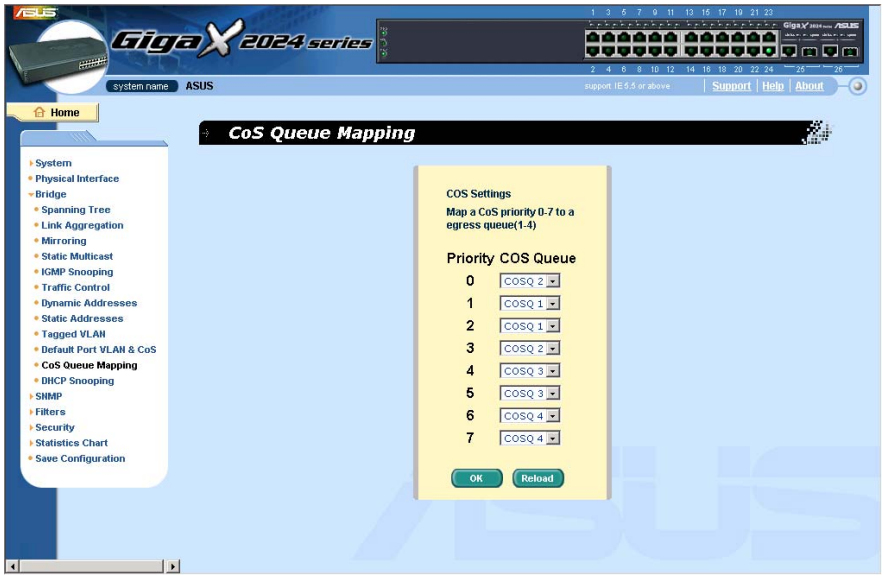

图 35. CoS 优先级队列

4.5.12 DHCP 侦测

DHCP 侦测是一项 DHCP 安全特性，可通过过滤不可靠 DHCP 信息及建立、维护 DHCP 绑定表（binding table）提供安全功能。您可指定一些端口为可靠端口。选定的端口（可靠）将作为正常端口转发 DHCP 数据包， 但当未选定（不可靠）的端口接收到这些数据包时，DHCP ACK 数据包将会被丢弃。

DHCP Snooping：启用或关闭 DHCP 侦测

点击 OK 按钮可发送设置值至交换机。点击 Reload 按钮可刷新设置为当前值。

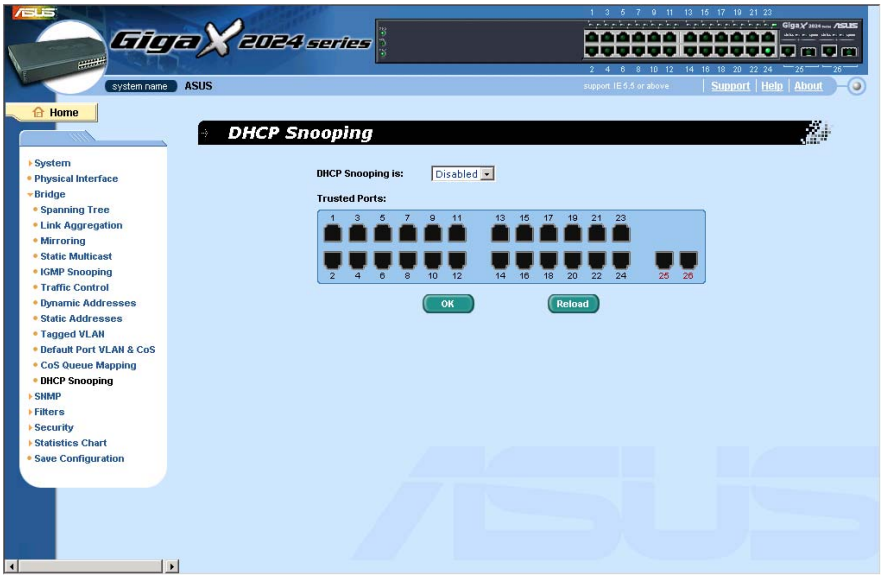

图 36. DHCP 侦测

4.6 SNMP

此页面提供 SNMP 设置，包括团体表（**Community Table**）、主机表（**Host Table**）及 ***Trap*** **设置（*Trap* Setting）。SNMPv3 可提供更多的安全管理与访问控制功能。**

4.6.1 团体表（Community Table）

您可以输入不同的团体名称、并定义其是否具有设置（写入存取）的权利。点击 OK 按钮可永久保存设置，点击 Reload 可加载目前的设置。

图 37. 团体表

4.6.2　主机表（Host Table）

此页面连接主机 IP 地址至 **Community Table** 页面里的团体名称。输入 IP 地址并在下拉菜单中选择团体名称，点击 OK 可永久保存设置，点击 Reload 按钮可加载设置。

图 38. 主机表

4.6.3 Trap 设置（Trap Setting）

通过设置 trap 目的 IP 地址及团体名称，您可启用 SNMP 的 trap 功能传送不同版本的 trap 数据包（v1 或 v2c）。点击 OK 按钮可永久保存设置，点击 Reload 可加载目前的设置。

图 39. Trap 设置

4.6.4 VACM 群组

VACM(View-based Access Control Model)群组用于设置 SNMPV3 VACM 群组的信息。

Group Name：输入安全群组名称

Read View Name: 输入此群组所属的 Read View 名称。相关的 SNMP 信息为 Get、GetNext、GetBulk。

Write View Name：输入此群组所属的 Write View 名称。相关的 SNMP 信息为 Set。

Notify View Name：输入此群组所属的 Notify View 名称。相关 SNMP 信息为 Trap、Report。

Security Model：输入此群组所属的安全模式名称。任何适合 USM 的 v1、v2、v3 均为 SNMPv3 相关信息。

Security level：输入此群组所属的安全等级名称。仅可选 NoAuth、AuthNopriv、AuthPriv。

欲通过以上信息建立新的 VACM 群组，点击 Add 按钮。然后即可在群组窗口中看到新增条目。欲删除既有群组，可先用鼠标点选，然后点击 Remove 按纽。 Modify 按纽可更新既有的 VACM 群组。点击 OK 可保存设置。点击 Reload 可加载当前设置。欲使设置值生效，请至 Save Configuration" 页面点击 Save 。

图 40. ***VACM 群组***

4.6.5 VACM View 模式

VACM(View-based Access Control Model) View 用于浏览 SNMPV3 VACM 群组的信息。

View Name: 输入安全群组名称

View Type: 输入 View 所属的 View 类型。当 View Subtree 与 SNMPv3 中的 Oid 匹配时，被包括或排除在外。

View Subtree: 输入 View 所属的 View Subtree。Subtree 是与 SNMPv3 中 Oid 匹配的 Oid。若 subtree 比 SNMPv3 中的 Oid 短时，则匹配成功。

View Mask: 输入 View 所属的 View Mask。掩码中的每个比特代表 View Subtree 中从左至右圆点之间的数字。

欲通过以上信息创建新的 VACM VIEW，请点击Add，然后您将会在显示窗口中看到新增条目。欲删除既有 VIEW，可点选该项，然后点击Remove。Modify按钮可更新既有的 VACM View 条目。点击OK可保存设置，点击Reload可刷新设置到当前值。欲使设置生效，请至"Save Configuration"页面点击Save。

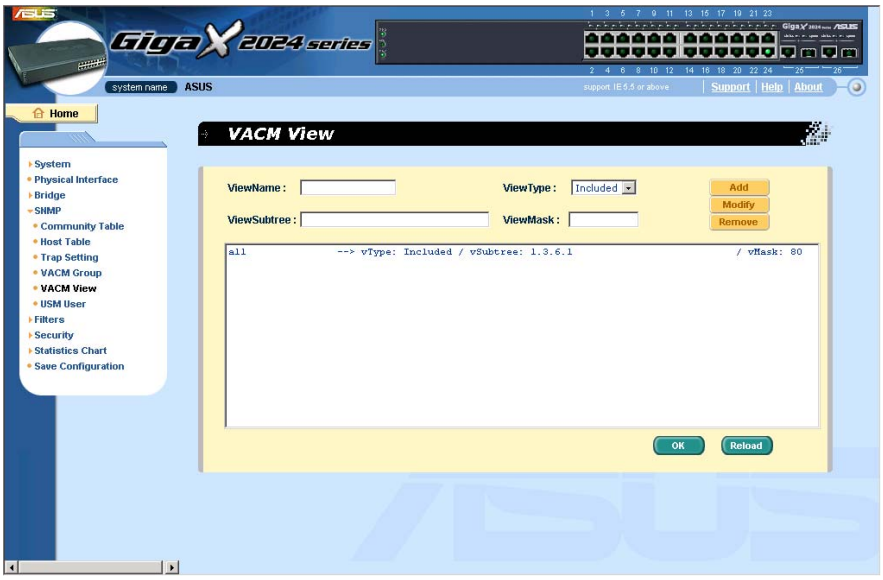

图 41. VACM View 页面

4.6.6 USM 模式

USM(用户安全模式)用于设置 SNMPV3 USM 用户的信息。

Engine Id: 输入应与管理器中的 ID 匹配的 Engine Id。

Name: 输入应与管理器中的名称与 Engine ID 匹配的名称与 Engine ID。

Auth Protocol: 输入 Engine ID 与名称所属的 Auth Protocol。仅可选择 NoAuth、MD5 与 SHA1。若选择 NoAuth 无需输入密码。

Auth Password: 输入 Auth Password 的密码。密码需至少 8 位数字或字符。

Priv Protocol: 输入 Engine ID 与名称的 Priv Protocol。仅可选择 NoPriv 与 DES。若选择 NoPriv，无需输入密码。

Priv Password: 输入 Priv Protocol 的密码。密码需至少 8 位数或字符。

欲通过以上信息建立新的 USM 用户，请点击 Add，然后您将在用户窗口看到显示的新增条目。若要删除既有的用户，可用鼠标点选，然后点击 Remove。 Modify 按钮可更新现有的 USM 用户条目。点击 OK 可保存设置。点击 Reload 刷新设置到当前值。欲使设置生效，，请至"Save Configuration"页面点击 Save。

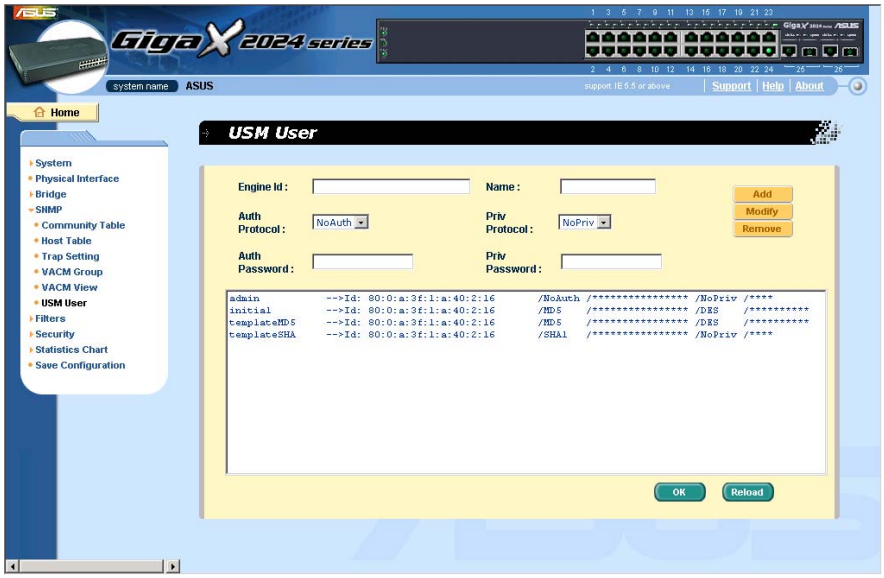

图 42.***USM User 页面***

4.7　过滤器（Filters）

本交换机可按照 2、3、4 层协议数据包的头信息来过滤流量类型。每个过滤器设置包含许多规则，您必须附加过滤设置至某个端口，以使其正常工作。

4.7.1　过滤设置（Filter Set）

您可以通过输入名称、ID 及规则模式来建立过滤组合。本交换机有两种模式的设置规则：一种为 MAC 模式，另一种是 IP 模式。只有相同的模式才能一起组合成一个过滤组合。每种模式的设置项目都不同，例如，您可以使用 IP 模式规则来过滤 FTP 数据包。

当您点击 **Filter Set** 时会出现 Filter Set 页面（如图）。首先，请输入名称与 ID 以建立过滤组合，然后点击 

；其次，点击  按钮选择编辑或删除设置；第三，点击 

进入规则页面（如图），或点击 

删除过滤组合。您必须依照以下规则来设置有效的过滤组合：

- 一个组合有一种类型的规则。每一规则有相同的过滤数据包选项。例如，两个过滤数据包规则有两个目的 IP 地址，具有相同的类型。但一个过滤规则的源 IP 地址与上两个不属于相同的类型。
- 一个端口可同时运用四种类型的规则。若超过四种，系统会自动取消这个规则。

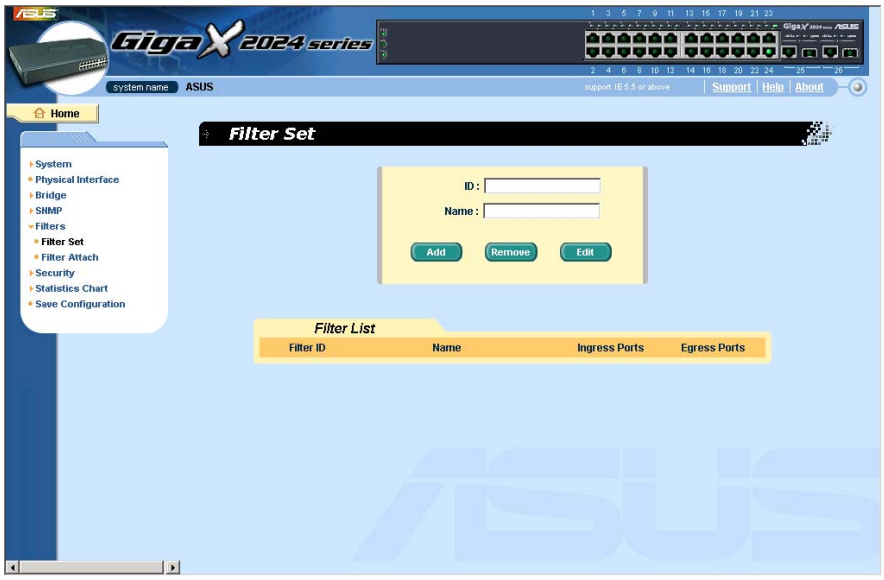

图 43. 过滤设置

过滤规则页面提供规则模式的选项，一为 MAC 规则（如图），一为 IP 规则（如图）。若空白字段中不输入 MAC 地址，表示此规则不需考虑 MAC 值。而在 IP 规则设置中，您可输入以下任一信息：源 IP、目的 IP、协议、源端口协议及目的端口协议。当数据包符合此一规则时，**Action** 字段会决定此数据包应被丢弃或转发出去。若数据包符合两种不同的运行规则，此数据包将会按照规则表中最先显示的规则运行。

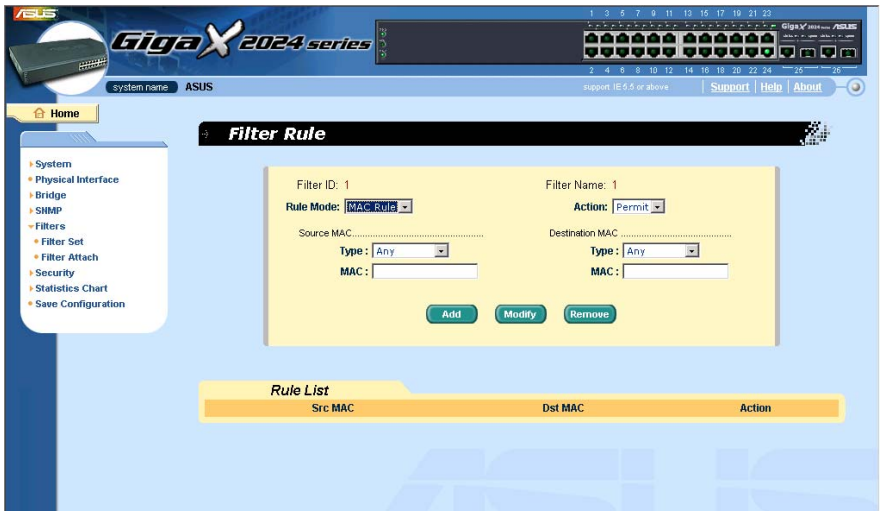

图 44. MAC 模式过滤规则

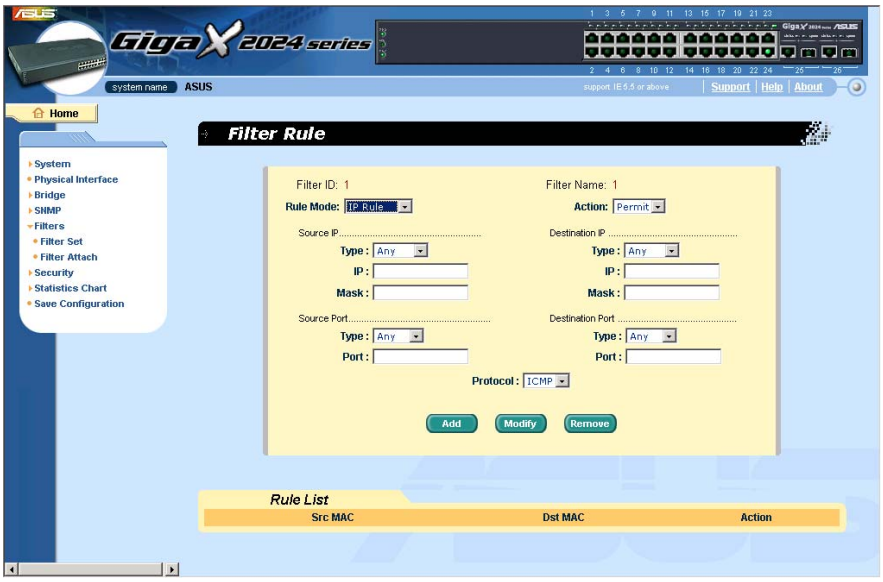

图 45. IP 模式过滤规则

4.7.2 添加过滤规则（Filter Attach）

若您没有将过滤组合附加到传送或接收端口，此过滤组合将无法发挥作用。请使用 Filter Attach 页面将过滤组合附加至接收或传送端口。

点击 OK 可保存设置。欲使设置生效，请至 “Save Configuration”页面，点击 Save，或点击 Reload 加载设置。

附加过滤组合至连接端口：

- 附加至所有端口：此过滤组合适用系统所有连接端口。
- 附加至特定端口：您可自行指定欲传送和接收的端口。GigaX 2048 的传送或接受端口必须为 1-24 及 49，或 25 – 48 及 50。
- 从所有端口删除：从附加连接端口删除所有的过滤组合。

选择"Attach All"命令后，您将无法从特定连接端口删除过滤组合。若您欲删除端口，请选择"Detach All"命令。

当过滤组合附加至接收及传送端口后，会视接收、传送端口及数据包项目规则来过滤数据包。例如，过滤规则为当接收端口接收到目的 MAC 地址为 00:10:20:30:40:50 的数据包时，不可传送至端口 2，则当端口 1 接收到目的 MAC 地址为 00:10:20:30:40:50 的数据包时，绝对不可传送至端口 2，但在流量较大的情况下，会传送到端口 2 以外的其它端口。

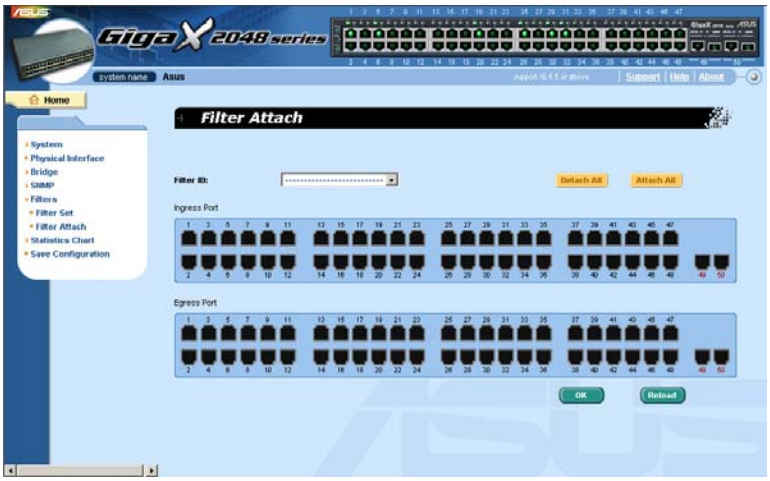

图 46. 添加过滤规则 (GigaX 2048)

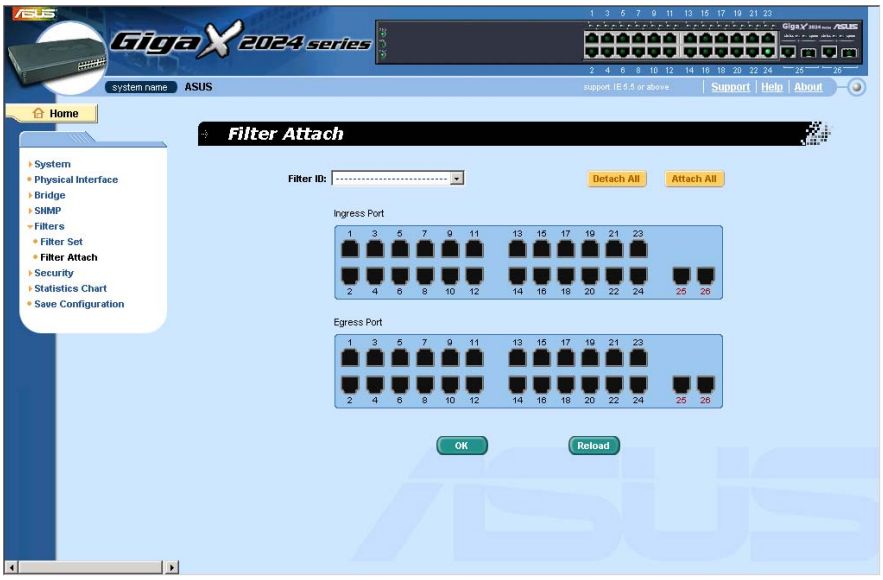

图 47. 添加过滤规则 (GigaX 2024)

4.8 安全性能（Security）

本交换机具有基于端口的 802.1X 安全特性。仅经过验证的主机可进入本交换机端口。未经验证的主机将被阻塞数据传输。RADIUS 服务器或交换机中的本地数据库可提供验证服务。

本交换机也可通过 802.1x 验证程序支持指定动态 VLAN。用户/端口的 VLAN 信息应在启用此功能前在验证服务器上正确设置。

4.8.1 端口访问控制（Port Access Control）

端口访问控制用于设置不同的 802.1x 参数。802.1x 可使用 RADIUS 服务器或本地数据库验证端口用户。

第一部分为桥接（Global)设置：

- Reauthentication: 启用此功能后，交换机将会在重新验证时间到达时重新验证端口用户。
- Reauthentication Time: 若启用“Reauthentication”，则此项为交换机向端口用户重新发送验证请求的时间间隔（见上）。
- Authentication Method: 可使用 RADIUS 或本地数据库验证端口用户。
- Quiet Period: 若 RADIUS 或本地数据库验证失败，交换机再次向端口用户发送新的验证请求的等待时间。
- Retransmission Time: 若端口用户没有对交换机的验证请求做出回应，交换机再次向端口用户发送验证请求的等待时间。
- Max Reauthentication Attempts: 若端口用户未对交换机的验证请求做出回应，交换机的最大发送请求次数。

第二部分为端口设置。修改完毕后请点击 Modify 按钮。

- Port: 指定欲设置的端口。
- Multi-host: 若启用此功能，在所有连接到选定端口的主机中，一个主机通过验证，则全部都可使用此端口。若关闭此功能，则只有一个主机可使用此端口。

- Authentication Control: 若选择“force_authorized”，则选定的端口将强制通过验证。这样，所有主机的数据都可通过。否则，若选择“force_unauthorized”，则选定的端口会被阻塞，不能通过数据。若选择“Auto”，选定的端口将由 802.1x 协议控制。正常情况下，所有端口都应被设置为“Auto”。
- Guest VLAN: 为无法使用 802.1x 的用户指定访问 VLAN。

点击 OK 可使设置永久生效。点击 Reload 可加载当前设置。

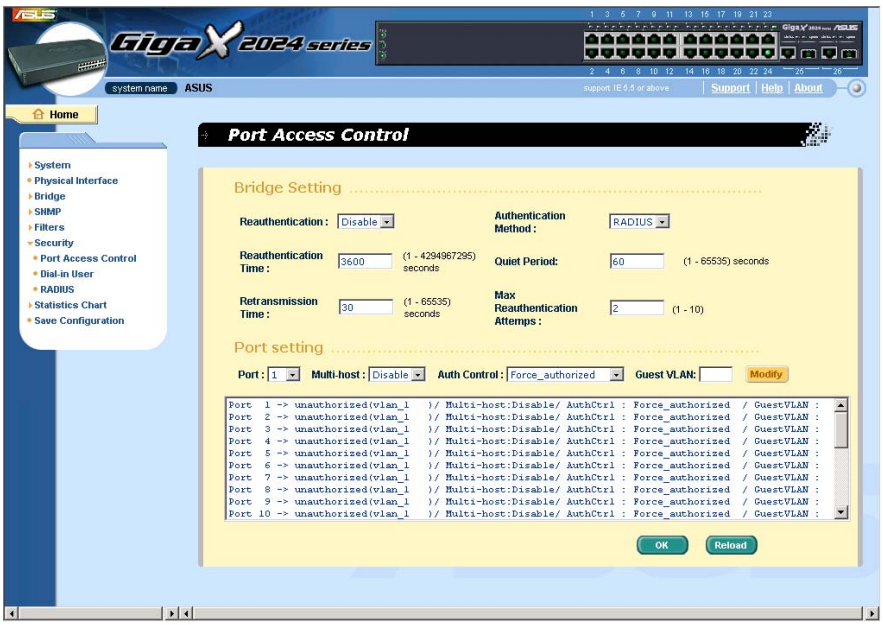

图 48. 端口访问控制

4.8.2　拨号用户（Dial-In User）

拨号用户用于指定交换机本地数据库的用户。

- User Name: 新的用户名称
- Password: 新用户的密码

- Confirm Password: 重新输入密码
- Dynamic VLAN: 指派经 802.1x 验证用户的 VLAN ID。

点击 Add 可增加新的用户。设置完后点击 Modify 按纽。点击 Remove 可删除选定的用户。点击 OK 可使设置永久生效。点击 Reload 可加载当前设置。

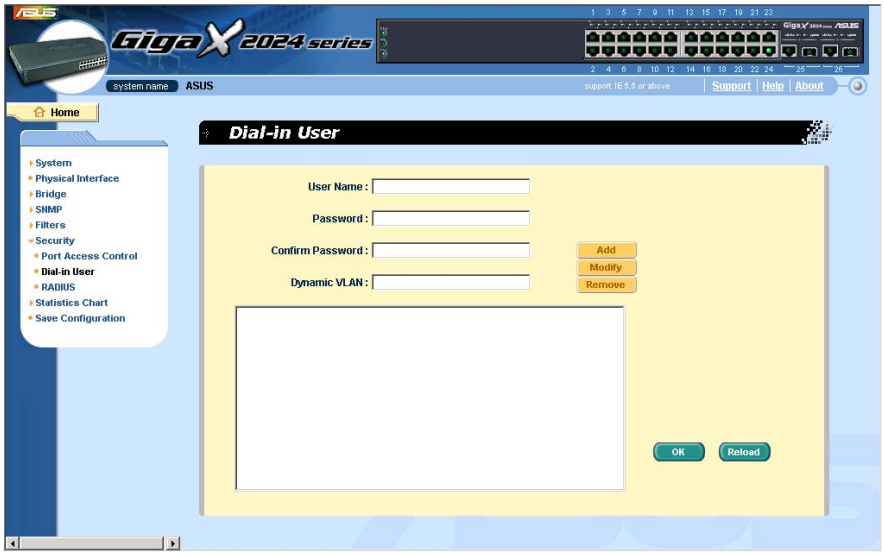

图 49. 拨号用户

4.8.3 RADIUS

欲使用外部 RADIUS 服务器，请对以下参数进行设置：

- Authentication Server IP: RADIUS 服务器的 IP 地址
- Authentication Server Port: RADIUS 服务器侦听（listening）的端口数
- Authentication Server Key: GigaX 与 RADIUS 服务器之间的通信密钥。

- Confirm Authentication Key: 重新输入上一项的密钥
-

连接到交换机的 RADIUS 服务器的 VLAN 必 须和系统管理界面的 VLAN 一致。

点击 OK 可使设置永久保存。点击 Reload 可加载当前设置值。

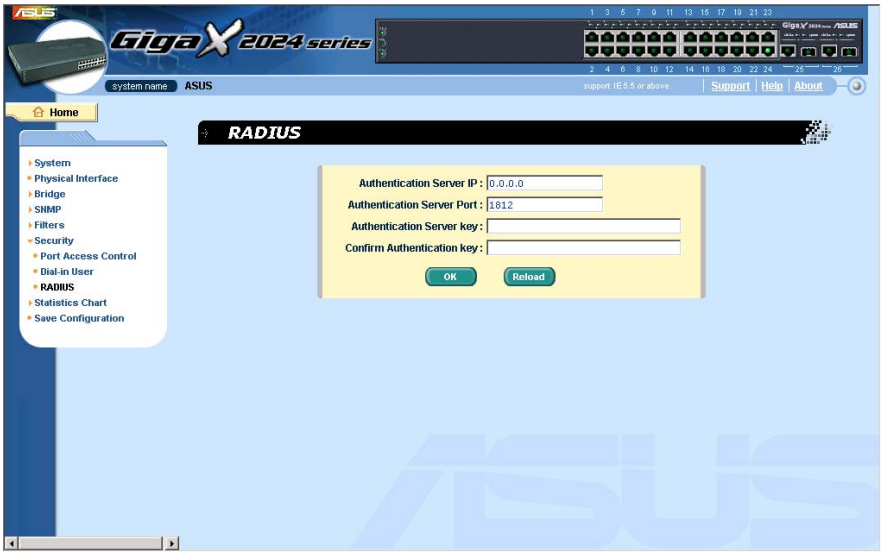

图 50. RADIUS

4.9 统计表（Statistics Chart）

Statistics Chart 页面提供各种不同的网络流量统计图表。您可设置所需的时间间隔来刷新图表。利用这些不同的系统统计图表可控制网络的流量。大部分的 MIB-II 计数器会显示在这些图表上。

点击 **Refresh Rate** 可设置自交换机取得最新数据的时间间隔。您可以通过选择**颜色**来区分统计结果或端口。最后，点击 **Draw** 开始绘制图表。，每一个新的图表都会重新显示最新的统计结果。

4.9.1 流量比较（Traffic Comparison）

此页面可在同一图表中比较所有端口的同一种统计项目。在这里设置要显示的统计项目并点击 **Draw**，即会定期更新数据及统计图表。

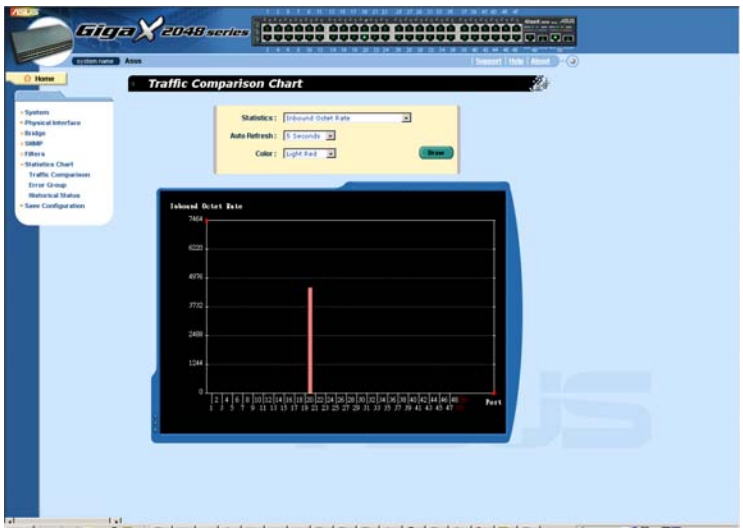

图 51. 流量比较 (GigaX 2048)

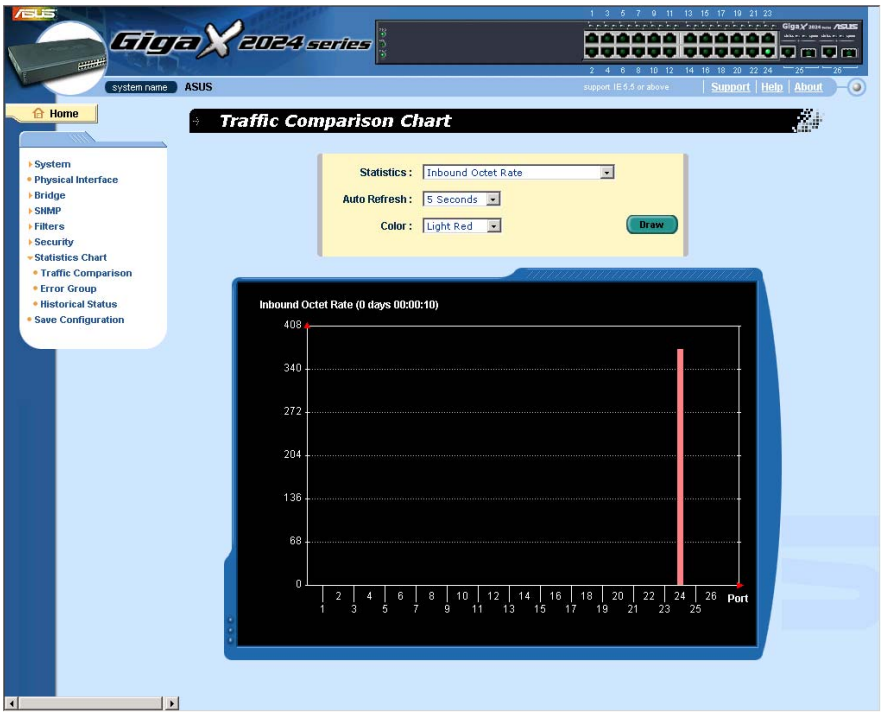

图 52. 流量比较 (GigaX 2024)

4.9.2　错误群组（Error Group ）

选择端口及显示颜色，然后点击 **Draw**，统计窗口会显示该端口所有要丢弃及错误的计数数据，该数据会定期更新。

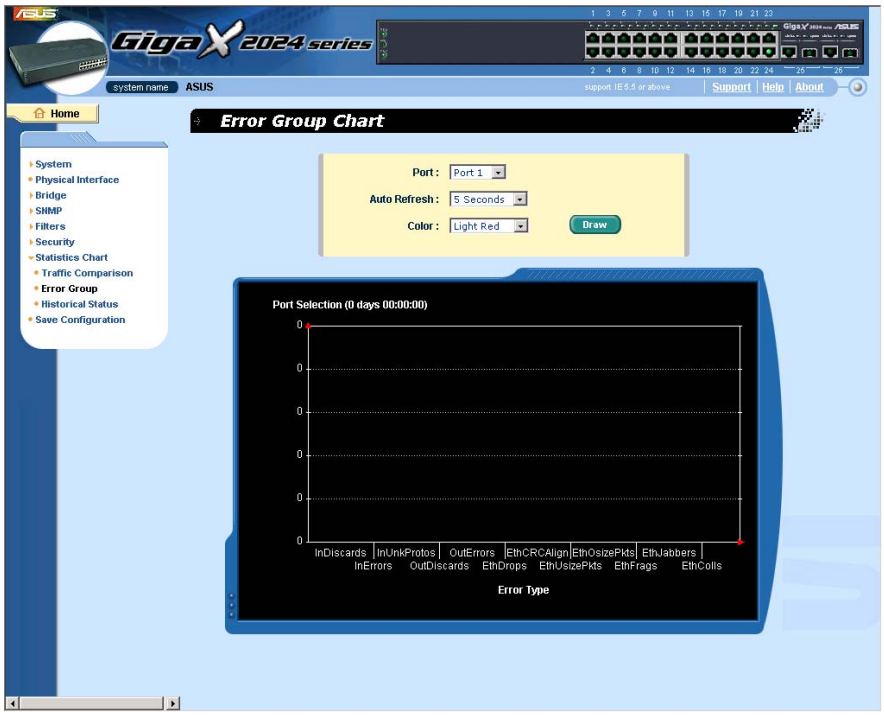

图 53. 错误群组

4.9.3 历史记录表（Historical Status）

此图表可显示不同端口的统计项目信息。由于这个图表是显示所有的历史记录，即使您重新加载数据时，旧的数据也不会被删除。

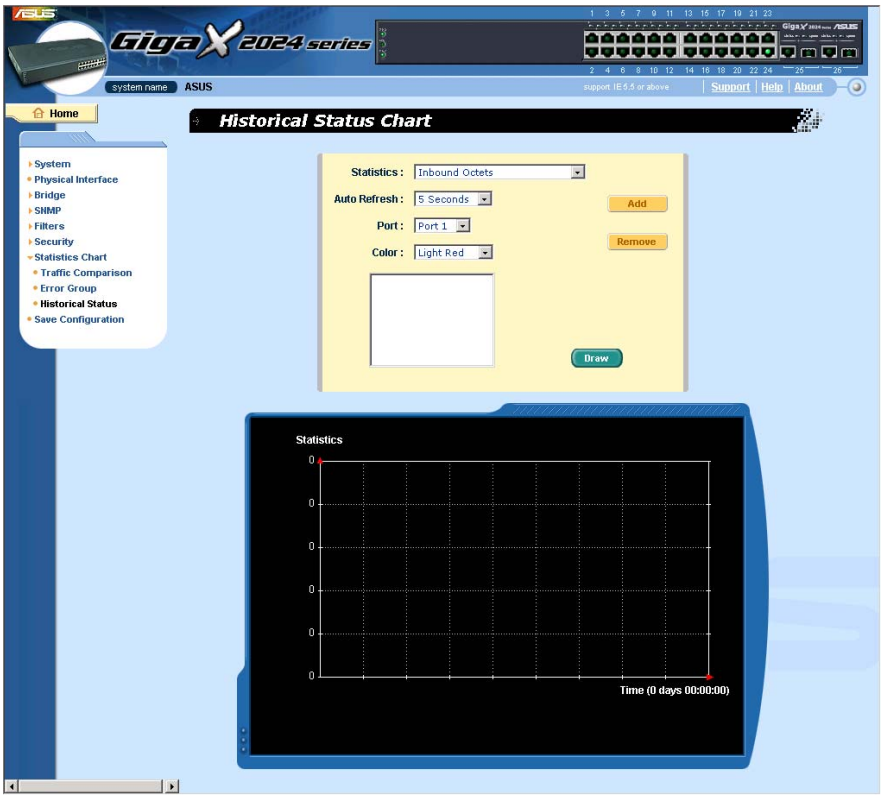
GigaX 2024 series
system name
ASUS
Support
Help
About
Home
Historical Status Chart
System
Physical Interface
Bridge
SNMP
Filters
Security
Statistics Chart
Traffic Comparison
Error Group
Historical Status
Save Configuration
Statistics :
Inbound Octets
Auto Refresh :
5 Seconds
Port :
Port 1
Color :
Light Red
Add
Remove
Draw
Statistics
0
0
0
0
0
0
Time (0 days 00:00:00)

图 54. 历史记录图表

4.10 保存设置（Save Configuration ）

欲永久保存设置，需点击Save。储存成功之后，新的设置立即生效。

有时您可能需要重新加载交换机设置，此时请点击Restore还原出厂设置值。当然，系统将随之重新启动。

当您恢复出厂设置值时，您将会永久丢失所有设置值。

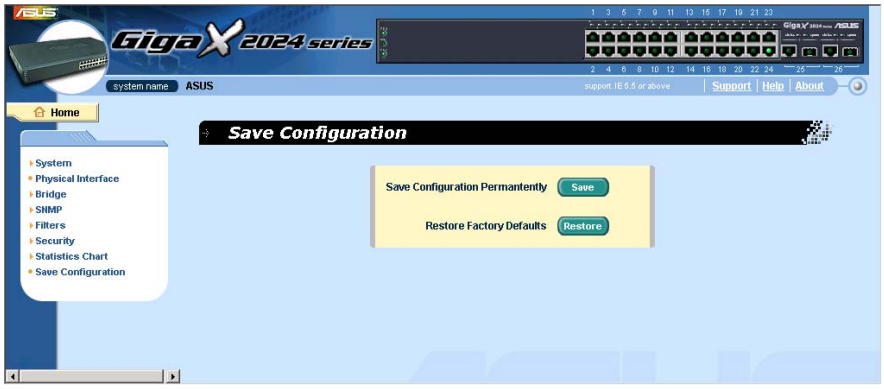

图 55. 保存设置

5 终端控制接口（Console Interface）

本章介绍怎样使用终端控制接口来设置交换机。本交换机提供了 RS232 及 USB 规格接口来连接 PC。您可以使用 PC 机上诸如 Hyper Terminal 超级终端仿真软件通过命令行对本交换机进行设置。在使用终端仿真软件之前，设置参数如下：每秒位数=9600，数据位=8、奇偶校验=无、停止位=1、数据流控制=无。

进入 CLI 模式后，输入“？”会显示所有可用的命令说明信息，这对不熟悉 CLI 命令的用户将非常有用。当系统闲置超过 10 分钟时，CLI 模式会关闭，您必须重新登录。

为了使用户操作更加简便，所有的 CLI 命令都设计的非常灵活。您可以输入不同类型的根命令全称进入不同的操作模式。这样，您就不必在子命令之前输入“sys”根命令了。例如，“sys”根命令包含许多子命令，在输入“sys”进入 sys 工作模式后，就不需要在子命令之前输入“sys”前缀。一旦进入“sys”工作模式，系统会自动显示“(*system name)sys%*”。

5.1 开机自检（Power On Self Test）

系统在开机时会进行自我检测（POST），用以检测系统内存、LED 及交换机主板上的芯片。系统检测结果及初始化信息将会显示出来。您可以忽略这些信息直至出现“(*ASUS)%*”字样。(见图).

```
Flash Driver Initialization ..................... [ DONE ]


Step 2
>>>>>> FLASH File System Initialization Start

[File System]: Major File System Summary
*** scanFlash: b04  used = 0 dirty = 0 bad = 0
*** scanFlash: b05  used = 12996 dirty = 4196 bad = 0
*** scanFlash: b06  used = 0 dirty = 0 bad = 0
*** scanFlash: b07  used = 0 dirty = 0 bad = 0

[File System]: Mirror File System Summary
*** scanFlash: b00  used = 0 dirty = 0 bad = 0
*** scanFlash: b01  used = 13068 dirty = 4336 bad = 0
*** scanFlash: b02  used = 0 dirty = 0 bad = 0
*** scanFlash: b03  used = 0 dirty = 0 bad = 0

[File System]: Perform File System Integrity Validation Check
*** Both file system image is OK!


System Log Restoring ............................ [ DONE ]
Network Library Initialization .................. [ DONE ]
Thread System Initialization .................... [ DONE ]
SSHd Host Key Initialization..................... [ DONE ]
WatchDog System Initialization .................. [ DONE ]
CLI Initialization .............................. [ DONE ]


Step 3
>>>>>> Switching Fabrics Initialization Start

Switching Fabrics Driver Initialization ......... [ DONE ]
System Network Initialization ................... [ DONE ]


Step 4
>>>>>> Asus OS Initialization Start(Phase 2)

System Parameters Reloading ..................... [ DONE ]
CLI Command Tree Initialization ................. [ DONE ]
In-ROM File System Initialization ............... [ DONE ]
FTPd Initialization ............................. [ DONE ]
Telnetd Initialization .......................... [ DONE ]
HTTPd Initialization ............................ [ DONE ]
SNMPd Initialization ............................ [ DONE ]

Asus OS Initialization Success.


Step 5
>>>>>> Entering CCM(CLI Command Mode) ...


Login is required!
(ASUS)%
```

图 56. CLI 界面

5.1.1 Boot ROM 模式

在开机自检过程中，您可以按下<ENTER>键进入“**Boot ROM Command**”模式，如图 57。

图 57 显示交换机的两个镜像固件，一个镜像固件位于 Slot 0，另一个镜像固件位于 Slot 1。系统会自动选择较新固件的版本来启动。

输入 “?”可以显示所有命令的帮助信息。

虽然特殊情况下，使用这些命令很有帮助，但我们强烈建议您：若您不清楚这些命令的功能，请勿任意使用。

```
################################################################################
#           Welcome to GigaX 2024 Switch Product by Asus Computer, inc.        #
#           Taipei, Taiwan                                                     #
################################################################################
FLASH ROM: 8M bytes

FLASH ROM Test ... done

                  >>>> SDRAM Test Starts <<<<

Phase 1: Fill in Test Pattern ... done
Phase 2: Perform SDRAM Test: 16384K
SDRAM Test Completed

               >>>> Boot Module Processing <<<<

Loading(Decompressing) Boot Module Image ... done
Destination Address: 0x80700000
Image Size: 188941 bytes
Starting Address: 0x80700000


             >>>> Switch Software Information <<<<

Boot ROM Version: 2.0, Build Date: 04/05/2004 14:57:25

[Firmware Information on Slot 0]
Firmware Address: 0xa4200000
Version: 2.0.0
Firmware Created at: 4/6/2004 10:12:22
Firmware Size: 1618926 bytes
Checksum: 0x7e80
Starting Address: 0x80010020
Web Files Size: 484782 bytes

[Firmware Information on Slot 1]
Firmware Address: 0xa4500000
Version: 2.1.0
Firmware Created at: 7/6/2004 21:30:22
Firmware Size: 1845510 bytes
Checksum: 0x8999
Starting Address: 0x80010020
Web Files Size: 309382 bytes

Hit Any Key to Enter Command Mode in 2 Second(s)

[Asus OS Boot]: _
```

图 57. Boot ROM 模式

5.1.2 Boot ROM 命令

在交换机重启过程中输入“?”可显示所有 Boot ROM 命令列表。

表 7. Boot ROM 命令

命令	参数	用法	说明
d	Address [,length]	提供地址及长度以调出并显示内存内容	
p	NONE	显示目前 Boot ROM 参数	
g	NONE	运行固件，进入 CLI 模式	
a	NONE	显示 MAC 地址	
b	0 or 1 or a	支持双重镜像文件。您可提供 Slot ID 来选择要执行的固件，或使用“a”自动选择。自动选择时，将会执行最新的固件。以上都是缺省设置	固件更新失败时，可使用此命令以旧的固件启动交换机。成功更新固件后再改为自动选择模式。
S	0, 1, 2, 3	设置控制台波特率 0: 9600bps 1:38400bps 2:57600bps 3:115200bps	必须为终端机仿真软件的波特率参数设置与此相同的数值
X	NONE	更新固件至交换机	使用终端口更新固件较慢。但若您中断网络连接，仍可使用此方式更新固件。
R	NONE	安全模式	若配置文件损毁或您忘记密码，请使用安全模式进入 CLI 模式 。在此模式中您的配置文件将会遗失，必须重新加载或设置。
W	NONE	管理员密码设置	重置用户 ID 与密码为缺省值。其它设置不会更改。

5.2 登录及注销（Login and Logout）

输入“**login**”进入 CLI 模式，您必须输入正确的用户名与密码。第一次登录时，请输入 “**admin**”作为用户名，不需要输入密码。为安全起见，请登录后修改用户名及密码。若您忘记用户名称及密码，请与华硕技术支持部门联系，或删除所有储存在 **Boot ROM Command** 模式里的设置。您选择后者时，系统设置将全部遗失，也就是说，您必须重新设置交换机。

输入“*logout*”可安全离开 CLI 模式。此操作可以有效保护 CLI 模式，下一位用户再次登录时必须验证用户名称及密码。

5.3 CLI 命令

本交换机提供所有管理功能的 CLI 命令。这些命令使用说明同 WEB 管理界面一样分类别列出。这样，您可以根据指示，方便、准确地设置本交换机。

使用“?”可取得可用命令列表及帮助信息

使用“/”可回到根目录。

使用“**..**”可回到上一级目录。

输入命令仅用于获得该命令的帮助信息

5.3.1 系统命令（System Commands）

[System Name]

显示交换机的名称。这是一个 RFC-1213 规范的系统群组的 MIB 对象，提供管理端的管理信息。

CLI 命令: sys name <*system name description*>

若您在系统名称描述栏中输入新的名称，则交换机的名称会更新为名称。

[System Contact]

显示交换机的详细联系信息。这是一个 RFC-1213 规范的系统群组的 MIB 对象，提供管理端的联系信息。

CLI 命令: sys contact <*system contact description*>

若您在系统联系描述栏中输入新的联系信息，则本交换机的联系信息会更新至此内容。

[System Location]

显示交换机的物理位置。这是一个 RFC-1213 规范的系统群组的 MIB 对象，提供管理端的位置信息。

CLI 命令: sys location <*system location description*>

在系统位置描述栏中输入位置信息，可更新交换机的物理位置。

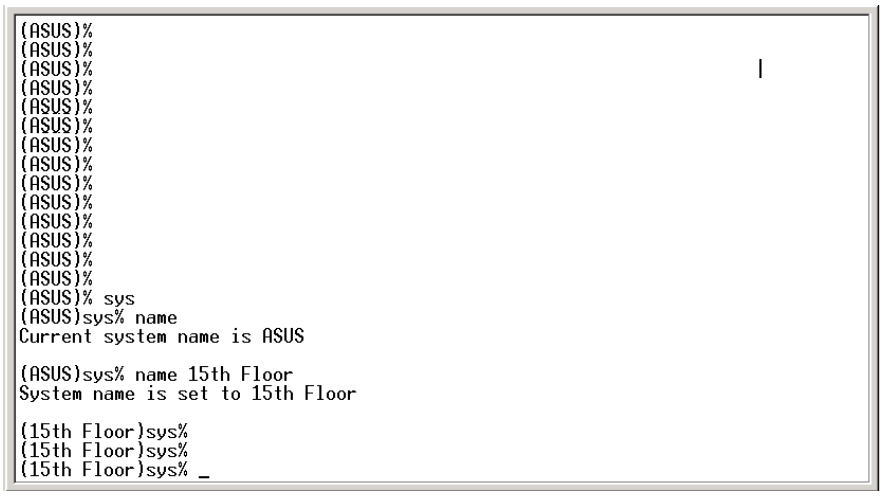

图 58. 系统命令

[VLAN ID]

显示交换机的 VLAN ID。这对 VLAN 内部管理是非常必要的

CLI 命令: net interface vlan sw0 <*VLAN ID*>

[DHCP Client]

启用 DHCP 获取一个动态 IP 地址，或关闭 DHCP 指定一个静态 IP 地址。若启用 DHCP， 您可更新或删除交换机的 IP 地址，并可使用显示命令显示动态 IP 地址。

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

[IP Address]

显示交换机的静态 IP 地址。此 IP 地址可用于管理功能，例如，交换机的网络工具如： http server、SNMP 服务器、ftp 服务器、 telnet 服务器及 SSH 服务器均使用此 IP 地址。

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

[Network Mask]

显示交换机的子网掩码。

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

[Default Gateway]

显示默认网关的 IP 地址。若交换机网络含一个或多个路由时，必须有此字段。

CLI 命令: net route static add <*destination subnet/IP*> <*gateway*> <*netmask*> <*metric*>

[Password Protection is] *[Enabled/Disabled*]

若启用密码保护，当用户通过浏览器进入交换机时，网络界面将要求验证用户名称及密码。

CLI 命令: sys weblogin set <*enable/disable*>

[New Password]
[Verify Password]

默认用户名为 **admin**，不需要输入密码。您可以通过以下命令参数设置密码：

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

user name (*old user name, 'admin' by default*)**:** <*新用户名称*>

password (old password, 'asus' by default): <*新密码*>

[Reboot]

用户可通过重新启动命令来重启交换机。

CLI 命令: sys reboot

[Upload]

此功能无 CLI 命令。请参考 Boot ROM commands。

5.3.2 物理接口命令（Physical Interface Commands）

[Admin] [Enable/Disable]

显示端口状态，用户可启用或关闭此连接端口功能。

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

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

显示连接端口当前的速度及双工模式。当您开启连接端口的自动功能时，会自动协商速率及双工模式。

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

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

CLI 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。注意此流量控制只能在全双工模式下运行。

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

[Reload]
从配置文件中恢复此端口原先的设置值。

CLI 命令: sys l2 port retrieve

5.3.3 桥接命令（Bridge Commands）

[Spanning Tree is] [*STP Enabled/ RSTP Enabled/ Disabled*]
用户可指定交换机是否参与生成树协议 (STP/ RSTP)。

CLI 命令: l2 stp *start <stp / rstp>*

CLI 命令: l2 stp *stop*

[Hello Time]
[Forward Delay]
[Max Age]
[Bridge Priority]
显示当前的 STP/RSTP 生成树网桥参数设置。

CLI 命令: l2 stp bridge set

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

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

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

Bridge Priority (0..65535):[*old Bridge Priority*] *<new Bridge Priority>*

[Priority]
[Path Cost]
[Edge Port]
[Point-to-point]
显示当前的 STP/RSTP 端口参数设置。

CLI 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..255):[old port Priority] <*new port Priority*>

Port <port number> Path Cost (1..65535):[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]

从配置文件中恢复原先的设置值。

CLI 命令: l2 stp retrieve

CLI 命令： l2 stp bridge retrieve

CLI 命令: l2 stp port retrieve

[Show Trunk]

显示特定的中继线设置。用户可自行设定中继线 ID、中继线名称描述、端口选择标准 (rtag)、LACP 模式(启用或关闭)及中继组成员端口来创建新的干线.

CLI 命令: l2 trunk show <*trunk id*>

[Create Trunk]

通过指定中继线 ID、rtag、名称、LACP 模式与端口代码创建新的干线。"rtag" 是对中继组内数据包分布传输的计算法。

Rtag 值及对应意义：

1: 通过源 MAC 选择端口

2: 通过目的 MAC 选择端口

3. 通过源 MAC 及目的 MAC 选择端口

4. 通过源 IP 选择端口

2: 通过目的 IP 选择端口

3. 通过源 IP 及目的 IP 选择端口

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

[Add/Remove Trunk]
从既有中继组中增加或删除群组端口成员。

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

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

[LACP Action]
用户可在特定中继线启用或关闭 LACP。

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

[LACP System Priority]
用户可指定运行 LACP 的优先级。

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

[LACP Port Priority]
用户可指定运行 LACP 的端口优先级。

CLI 命令: **l2 port lacppri *<priority> <port list / * for all ports>***

[Reload]
自备份文件中恢复先前储存的设置。

CLI 命令: l2 trunk retrieve

***适用 GigaX 2048**

[Mirror] [Mirror 1/*Mirror 2*]

[Mirror Mode] [*Enable/Disable*]

[Monitor Port] [*port number*]
显示交换机端口的端口镜像设置。用户可创立最多两个端口镜像端口。其一与 SoC 关联，即镜像端口 1 用于 SoC0，另一镜像端口 2 用于 SoC1。这样，仅有 1-24 的端口能指定到镜像 1 作为镜像端口，输入端口或输出端口。仅 25-48 可指定到镜像 2 作为镜像端口。

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

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

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

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

***适用 GigaX 2024**

[Mirror Mode] [*Enable/Disable*]

[Monitor Port] [*port number*]
显示交换机的镜像映射设置。

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

CLI 命令: l2 mirror ingress *<port list>*

CLI 命令: l2 mirror egress *<port list>*

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

[Reload]
自备份文件中恢复先前储存的设置。

CLI 命令: l2 mirror retrieve

[Show Multicast Group]

显示组播表中的静态组播群组。

CLI 命令: l2 mcast show

[Set Multicast Group]

用户可通过指定 MAC 地址、VLAN ID、服务级别（CoS）、VLAN 端口成员及未标记端口成员来增加或修改静态组播群组。注意，在组播表中，MAC 地址及 VLAN ID 之间的绑定不可有重复。

CLI 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]

用户可通过指定 MAC 地址及 VLAN ID，从组播表中删除静态组播群组。

CLI 命令: l2 mcast delete

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

vlan id: <*vlan id*>

[Reload]

从备份文件中恢复先前储存的设置。

CLI 命令: l2 mcast retrieve

[IGMP is] [Enabled/Disabled]
若有需要，用户可开始或终止第二层 IGMP 侦测。

CLI 命令: l2 igmp <*start/stop*>

[Reload]
从备份文件中恢复先前储存的设置。

CLI 命令: l2 igmp retrieve

[Broadcast] [Enabled/Disabled]

[Multicast] [Enabled/Disabled]

[Destination Lookup Failure] [Enabled/Disabled]
用户可启用流量控制功能以显示广播、组播及因传送目标的错误而导致的流量泛洪

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

[Limit]
显示交换机的目前速率限制。用户可更改此限制速率。此限制值适用所有前述的流量控制内容。

CLI 命令: l2 rate limit <*limit rate*>

[Reload]
从备份文件中恢复先前储存的设置。

CLI 命令: l2 rate retrieve

[Aging Time]
设置 ARL（Address Resolution Logic）项的存在时间。

CLI 命令: l2 arl age *[aging time value]*

[Query by Port]
按照端口连接号查询 ARL 表中各项。

CLI 命令: l2 arl port <*port number*>

[Query by VLAN ID]
按照 VLAN ID 查询 ARL 表中各项。

CLI 命令: l2 arl vlan <*vlan id*>

[Query by MAC Address]
按照 MAC 地址查询 ARL 表中各项。

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

[MAC Address]

[VLAN ID]

[Port Selection]

[Discard] [none/source/destination/source & destination]
用户可通过指定 MAC 地址、VLAN ID、连接端口号码、中继线 ID 及过滤标准来增加或修改静态 ARL 表项。

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

[Remove]

静态 ARL 表项可通过 MAC 地址与 VLAN ID 来删除。上两项组合在 ARL 表中被视为一个特定的表项。

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

[Reload]
从备份文件中恢复先前储存的设置。

CLI 命令: l2 arl retrieve

[Show VLAN]
显示交换机目前的 VLAN 信息。

CLI 命令: l2 vlan show <*vlan id*>

[Name]

[VLAN ID]
用户可进行 VLAN 设置。通过指定特定的 VLAN ID、VLAN 描述名称及其端口成员列表建立新的 VLAN。注意这里的端口成员是指已标记的端口。若要将 VLAN 连接端口成员设置为未标记端口，可利用 CLI 命令的 utportadd 来完成。用户可利用 CLI 命令来增加或删除 VLAN 中的某些端口成员。

CLI 命令: l2 vlan create <vlan id> <vlan name> <port list>

CLI 命令: l2 vlan add <*vlan id*> <*port list*>

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

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

[DHCP Snoop]
在此 VLAN 上启用或关闭 DHCP Snooping 功能。

CLI 命令: l2 dhcpsnoop enable <*vlan id list*>

CLI 命令: l2 dhcpsnoop disable <*vlan id list*>

[Remove VLAN]
用户可完整地删除现有的 VLAN。

CLI 命令: l2 vlan delete <*vlan id*>

[Reload]
从备份文件中恢复先前储存的设置。

CLI 命令: l2 vlan retrieve

[PVID]

通过指定 VLAN ID 及其关联的端口成员列表为某端口设置缺省 VLAN。

CLI 命令: l2 port vlan <vlan id, 4095 to disable the port-based vlan> <port list> **[CoS Value]**

通过指定优先级（0-7）标准值设置端口的服务级别。

CLI 命令: l2 port priority <*CoS*> <*port list*>

[Reload]

从备份文件中恢复先前储存的设置值。

CLI 命令: l2 port retrieve

[Priority] [CoS Queue]

用户可设置缓冲（共 4 个优先级等级，Queue1-4）服务级别顺序值（0-7）。

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

[Reload]

从备份文件中恢复先前的设置值。

CLI 命令: l2 cos retrieve

[DHCP Snooping is]

在特定的 VLAN 上启用或关闭 DHCP。

CLI 命令: l2 dhcpsnoop enable <*vlan id list*>

CLI 命令: l2 dhcpsnoop disable <*vlan id list*>

[Add/Remove Trusted Port]

用户可增加或删除 DHCP 侦测的端口。

CLI 命令: l2 dhcpsnoop add <*port list*>

CLI 命令: l2 dhcpsnoop remove <*port list*>

[Reload]
从备份文件中恢复先前的设置。

CLI 命令: l2 dhcpsnoop retrieve

5.3.4 SNMP

[Community Name] [Set]
团体项目包含团体名称及一组优先顺序。Get 优先权默认是开启的，建立新的条目时，用户可自行定义是否赋予 Set 优先权。

CLI 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'*>

CLI 命令: snmp community set

修改团体表内容及其权限。

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

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

修改所有主机所属的团体名称。将团体名称从'*old community*'修改为'*new community*'。

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'>

CLI command: snmp community delete

删除团体表中的用户。

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

'*delete community*'将会删除某团体中所有主机。

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

[Reload]

从备份文件中恢复先前储存的设置。

CLI 命令: snmp community retrieve

[Host IP Address] [Community]

主机内容包含了主机 IP 地址子网掩码及其所属团体。

CLI 命令: snmp host add

Host IP/Subnet: <*IP address*>

Netmask: <*netmask*>

Community: <*community string*>

CLI 命令: snmp host set

用户可通过重新输入 IP 地址、子网掩码及其所属团体，在此表中修改主机内容。

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>

CLI 命令: snmp host delete

用户可从主机表中删除主机内容。

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

[Reload]

从备份文件中恢复先前设置。

CLI 命令: snmp host retrieve

[Trap Version] [v1/v2c]

[Destination]

[Community for Trap]

Trap 项目中包含 SNMP 版本（目前支持版本 1 及 2c）、目的 IP 地址及远端团体名。

CLI 命令 : snmp trap add

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

Destination IP: <*IP address*>

Community: <*community string*>

CLI 命令: snmp trap set

用户可通过修改 SNMP 版本、目的 IP 地址及团体名称来修改 Trap 表。

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>

CLI 命令: snmp trap delete

用户可以从 Trap 表中删除某一项目。

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

[Reload]

丛备份文件中恢复先前储存 的设置。

CLI 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) 包括 group 名称、read view 名称、write view 名称、notify view 名称、security model、security level 与 context match 等。

CLI 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*>

CLI 命令: snmp snmpv3 access set

用户可通过重新指定 group 名称、read view 名称、write view 名称、notify view 名称、security model、security level 及 context match 修改群组中的 VACM 内容。

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>*

CLI 命令: snmp snmpv3 access delete

用户可从 VACM 群组中删除 VACM 内容。

Access entry: <entry id to delete>

[Reload]

从备份文件中恢复先前储存的设置。

CLI 命令 : snmp snmpv3 access retrieve

[View Name]

[View Type]

[View Subtree]

[View Mask]

VACM(View-based Access Control Model) View 用于监控 SNMPV3 VACM 群组信息。VACM View 内容包括 view name、view type、view subtree 及 view mask。

CLI 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*>

CLI 命令: snmp snmpv3 view set

用户可通过重新指定 view name、view type、view subtree 及 view mask 修改 VACM View 内容。

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* >

CLI 命令: snmp snmpv3 view delete

用户可删除 VACM View 内容。

View entry: <entry id to delete>

[Reload]
从备份文件中恢复先前储存的设备。

CLI 命令: snmp snmpv3 view retrieve

[Engine Id]

[Name]

[Auth Protocol]

[Auth Password]

[Priv Protocol]

[Priv Password]

USM(User-based Security Model) User 用于设置 SNMPV3 USM User 信息。USM User 内容包括 engine Id、名称、auth protocol、auth password、priv protocol 及 priv password。

CLI 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* >

CLI 命令: snmp snmpv3 usmuser set

用户可通过重新指定 engine Id、name、auth protocol、auth password、priv protocol 及 priv password 修改 USM User 内容。

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* >

CLI 命令： snmp snmpv3 view delete

用户可删除 USM User 内容。

USM user entry: <entry id to delete>

[Reload]

从备份文件中恢复先前储存的设置。

CLI 命令: snmp snmpv3 usmuser retrieve

5.3.5 过滤规则命令（Filters Commands）

[New]
指定一个特定的 ACL ID 及名称来新建一个过滤规则。

CLI 指定: filter set new <*acl id*> <*acl name*>

[Remove]
用户可指定 ACL ID 来删除过滤规则。

CLI 命令: filter set delete <*acl id*>

[Edit]

[Rule Mode] [MAC Rule]

[Action] [Permit/Deny]

[Source MAC]

[Destination MAC]

[Add]
用户可为过滤规则增加一个新的 MAC 地址规则。此一过滤规则和 ICMP、TCP 或 UDP 协议及其允许或拒绝的操作相关。用户也可使用 CLI 命令 dstmac 及 srcmac 来指定过滤规则的 MAC 地址。

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

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

CLI 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]
用户可为过滤设置增加一个新的 IP 地址规则。此一过滤规则和 ICMP、TCP 或 UDP 协议及其允许或拒绝的选项共同作用。用户也可分别使用 CLI 命令 dstip/scrip 及 dstport/scrport 来指定过滤规则的 IP 地址（源或目的地址）。

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

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

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

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

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

[Rule Mode] [MAC Rule]

[Action] [Permit/Deny]

[Source MAC]

[Destination MAC]

[Modify]
用户可修改 MAC 过滤规则。

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

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

CLI 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]
用户可修改 IP 过滤规则。Allows user to modify the IP filter rule.

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

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

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

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

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

[Rule Mode] [MAC Rule]

[Action] [Permit/Deny]

[Source MAC]

[Destination MAC]

[Delete]
用户可删除 MAC 过滤规则。

CLI 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]
用户可删除 MAC 过滤规则。

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

[Rule List]
显示过滤设置及过滤规则设置。

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

Attach

附加过滤规则至输入/输出端口以启用过滤功能。

[Filter ID]
显示过滤设置。

CLI 命令: filter show

[Ingress Port]
将某一输入端口加至此过滤规则。

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

[Egress Port]
将某一连接端口加至此过滤规则。

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

[Reload]
从备份文件中恢复先前储存的设置。

CLI 命令: filter retrieve

5.3.6 安全命令（Security Commands）

[Reauthentication]
可启用或关闭定期重新验证。

CLI 命令: security dot1x bridge reauth <*enable* / *disable*>

[Reauthentication Time]
用户可设置重新验证时间。

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

[Authentication Method]
用户可设置验证方法 (RADIUS 或本地数据库）。

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

[Quiet Period]
用户可设置间隔时间。

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

[Retransmission Time]
用户可设置重新传输时间。

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

[Max Reauthentication Attempts]
设置重新验证的最大请求次数。

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

[Multi-host]
用户可启用或关闭某些特定端口的多宿主机。

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

[Authentication Control]
用户可建立对某些端口的验证控制。

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

[Guest VLAN]

用户可建立某些特定端口的访客 VLAN ID。

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

[Reload]

从备份文件中恢复先前储存的设置。

CLI 命令: security dot1x retrieve

[User Name]

[Password]

[Confirm Password]

[Dynamic VLAN]

在交换机的本地数据库建立 802.1X 验证用户。用户内容包括用户名称、密码与动态 VLAN。

CLI 命令: security dialinuser create

User Name: <user name string>

Password: <password string>

Confirm Password: <confirm password string>

Dynamic VLAN: <dynamic VLAN>

CLI 命令: security dialinuser remove <*user name/**>

从本地数据库中删除用户项。

CLI 命令 : security dialinuser modify <*user name/**>

从本地数据库中修改用户内容。包括用户名称、密码与动态 VLAN。

User Name: <new user name string>

Password: <new password string>

Confirm Password: <new confirm password string>

Dynamic VLAN: <new dynamic VLAN>

[Reload]
从备份文件中恢复先前储存的设置。

CLI 命令: security dialinuser retrieve

[Authentication Server IP]

[Authentication Server Port]

[Authentication Server Key]

[Confirm Authentication Key]

用户可配置 RADIUS 服务器、服务器 IP、服务器端口及服务器密钥。

CLI 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]
从备份文件中恢复先前储存的设置。

CLI 命令: security radius retrieve

[Generate SSH key]
用户可生成 SSH 密钥。SSH（Secure Shell）是通过 shell 远程登录的协议。功能上与 telnet 非常相似，但不同的是，所有客户端与服务器之间的数据都是加密的。加密功能可为各种网络安全问题提供保护。目前，此交换机支持第二版 SSH 协议，一次只能允许一名用户登录。两种 SSH 密钥可在系统闪存中创建，分别是 RSA 和 DSA 公钥/个人密钥。

CLI 命令: security sshkey start

[Reset SSH key]

重置 SSH 密钥为缺省值。

CLI 命令: security radius default

[Show Generating Status]

显示 SSH 密钥生成状态。将会显示： “success”或“SSH keys generated fail” 或 “system is generating keys ...”.

CLI 命令: security sshkey show

5．4 其它命令

sys uptime: 显示系统启动时间

sys date: 显示当前时间与日期

sys settime: 设置当前时间

net ping: ping 远程主机

net route show: 显示路由表内容

6 IP 地址、子网掩码与子网

6.1 IP 地址

此部分仅适用 IPv4 (Internet Protocol version 4)的 IP 地址。不含 IPv6 地址。

此部分将会讲述二进制数、比特与字节的基本知识。详情见附录 6。

IP 地址是 Internet 世界的电话号码，用于识别 Internet 上独立的节点（计算机等网络设备）。每个 IP 地址含 4 个数位，每个数位从 0-255，由圆点（句点）分开，例如：20.56.0.211，这些数字从左至右称为 field1（第一个 8 位组）、field2（第二个 8 位组）、field3（第三个 8 位组）及 field4（第四个 8 位组）。

这种由小数点分隔的十进制 IP 地址书写方法称为*十进制点标记法*。IP 地址 20.56.0.211 读作 "二零点五六点零点二一一。"

6.1.1 IP 地址结构

IP 地址结构如电话号码结构的等级设计。例如，一个 7 位的电话号码的前 3 位用于识别一组含数千条的电话线，后四位则用于识别该组中特定的某条线。

同样，IP 地址也包含了两种信息：

Network ID
识别 Internet 或 Intranet 上的一个特定网络。

Host ID
识别此网络上一个特定的计算机或设备。

每一个 IP 地址的前一部分包括网络号信息，其它部分则包含了主机号信息。网络号的长度依其类别而定（见下部分）。表 7 列出了 IP 地址的结构。

表 8. IP 地址结构

	Field1	Field2	Field3	Field4
A 类	网络号	主机号		
B 类	网络号		主机号	
C 类	网络号			主机号

以下示例为有效 IP 地址：

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 分类网址（Network classes）

三种常用的分类网址为 A、B、C 类（D 类由于另有特殊功能，不包含在此范围之内）。这些分类网址有不同的功能与特性：

A 类网络是 Internet 中最大的网络，每个均有 1600 万台主机空间。最多可有 126 个这样大的网络存在，主机总数达 20 多亿台。由于有这样的空间，这些网络广泛应用于广域网及 Internet 上的基本组织，如您的 ISP 即属此例。

B 类网络相对较小，但空间仍然很大，每个均可容纳 65，000 多台主机。最多可有 16，384 个 B 类网络存在。B 类网络适用于大型组织机构，如商业、政府部门等。

C 类网络最小，最多可容纳 254 台主机，但总数可超过 2 百万台（具体为 2,097,152）。连接到 Internet 的网络通常都是 C 类。

有关 IP 地址的一些重要事项：

自 field 1 可以方便的确定网络类别：

field1 = 1-126: A 类
field1 = 128-191: B 类
field1 = 192-223: C 类

(未显示 field1 的值表示另有其它用途)

主机号可以是任意值，若所有 field 的值均设为 0 或 255，则表示设置值另有用途。

6.2 子网掩码（Subnet masks）

*掩码*看起来就 如同一个规则的 IP 地址，但它通过一种数据位模式，可区分 IP 地址哪部分是网络号，哪部分是主机号；比特值设为 1 表示“此比特是网络号的一部分”，比特值设为 0 表示“此比特是主机号的一部分”。

*子网掩码*用于定义子网（即将网络分割成更小的网络）。子网的网络号是通过从主机号“借用”一个或多个位来创建的。子网掩码可识别这些主机号的位。

例如，一个 C 类往址 192.168.1，要将其分为两个子网，您要使用以下子网掩码：

255.255.255.128

若写成二进制则很容易识别：

11111111. 11111111. 11111111.10000000

所有 C 类网址的地址中，从 field1 到 field 3 都是网络号的部分，但请注意掩码定义的时候，field 4 的第一位也包含在内。既然此位只有两个值可选（0 和 1），这说明只有两个子网。每个子网将使用 field 4 其余的 7 位作为其主机号，设置值可为 0-127（不是 C 类网址常用的 0-255）。

同样地，要将 C 类网址分成 4 个子网，其掩码是：

255.255.255.192 或 11111111. 11111111. 11111111.11000000

Field 4 中的两个位值可有 4 个选项值（00、01、10、11），所以有 4 个子网。每个子网使用 field 4 中其余的 6 位作为其主机号，范围是 0-63。

有时子网掩码不会定义任何附加的网 各号位，这样就没有子网。这样的掩码称为*缺省子网掩码* 这些掩码是：

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

称为缺省是因为网络初始设置时即在 使用，这时没有子网。

7 故障排除

此部分将介绍几种使用 IP 工具进行问题诊断的方法。同时也提供一些常见的问题及解决方案，供您参考。

所有需要注意的部分也在注意事项中列出，请在安装交换机之前仔细阅读。若仍无法解决您的问题，请与本公司客服部门联系。

7.1 使用 IP 工具诊断问题

7.1.1 Ping

Ping 命令可检测您的 PC 是否可以识别网络上的其它电脑。Ping 命令可发送消息到您指定的电脑，若对方收到，即会回应。使用本命令时，您必须知道对方计算机的 IP 地址。

在 Windows 环境中，您可以从<开始>菜单执行此命令。点击<运行>，在打开的文本框中输入信息，如:

ping 192.168.1.1

点击 OK ，您可以输入所知道的任何 IP 地址。

若对方收到信息，则会出现如图所示的提示窗口：

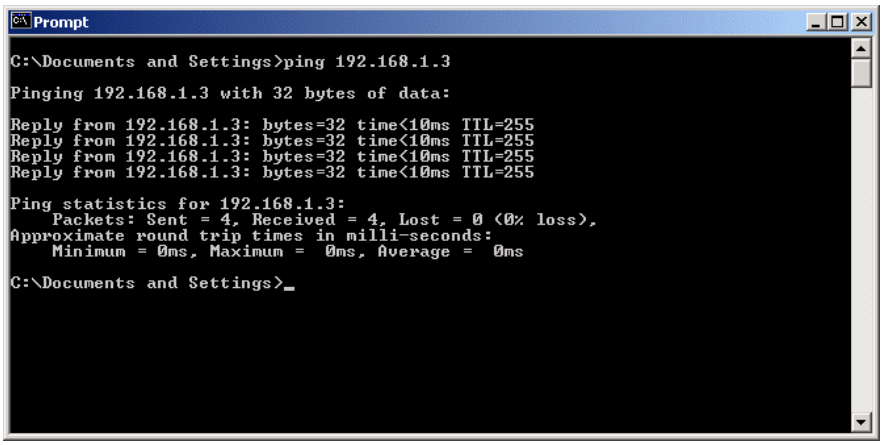

图 59. 使用 ping 工具

若无法找到对方计算机，您将会收到“Request timed out（请求超时）”的信息。

使用 ping 命令，您还可确定与交换机 (使用预设 IP 地址 192.168.1.1)或其它指定地址的连接是否正常。

通过输入一个外部地址，如 www.yahoo.com (216.115.108.243)，您可以检测与 Internet 的连接是否正常。若不知道某个 Internet 的 IP 地址，可使用 nslookup 命令，将在下一章节说明。

与其它具有 IP 功能的操作系统不同，您可通过命令提示或系统管理工具执行相同的命令。

7.1.2　Nslookup

使用 nslookup 命令可确定 Internet 网址的 IP 地址。只要指定网络上的通用名称， nslookup 就可在 DNS 服务器（通常在 ISP 上）上查找 IP 地址。若此名称不在 ISP 的 DNS 表之列，此请求将会被传送至高一级的服务器，依次类推，直至找到此地址，服务器然后会发回此地址信息。

在 Windows 环境中，您可以从<开始>菜单执行此命令。点击<运行>，在打开的文本框中输入：nslookup

点击 OK 。命令提示框会出现提示符，在提示符后输入您欲查找的 Internet 地址，如www.absnews.com。

此窗口会显示相关的 IP 地址，如图：

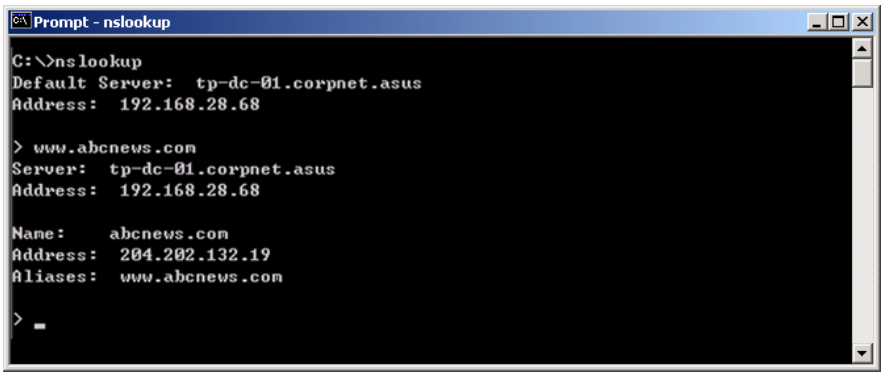

图 60. 使用 ***nslookup 工具***

一个 Internet 名称可能同时有几个 IP 地址，这对流量大的网站来说是正常情况；这些网址可以使用多个服务器来传递同样的信息。

要从 nslookup 工具中退出，可在命令框中输入 **exit**，然后按 **<Enter>** 键。

7.2 更换故障风扇

要拆下交换机后端的故障风扇，请先关闭电源。

若交换机的任何一个风扇（位于后端面板）出现故障，您可以依照以下几个步骤轻松地更换：

1. 用螺丝刀松开后端面板上用于固定风扇模块的螺钉。

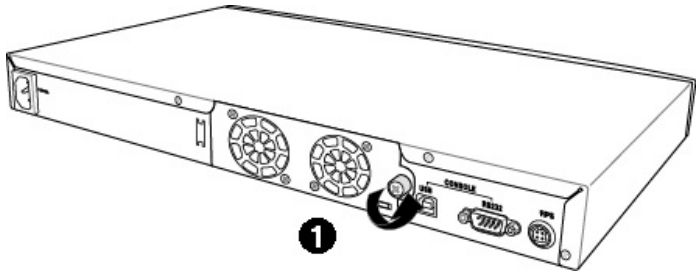

图 61. 松开螺钉

2. 小心地取出风扇模块。

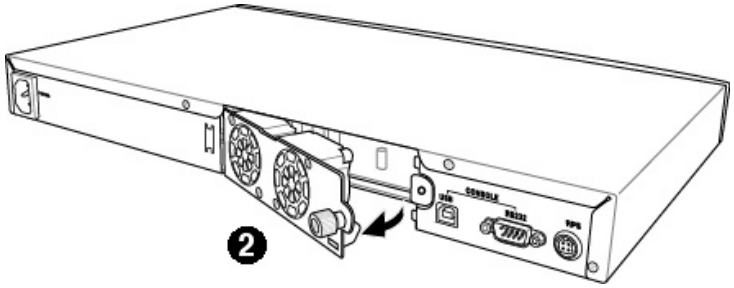

图 62. 取出风扇模块

3. 小心地从风扇插头上拔下两根电源线。
4. 松开模块上固定风扇的螺钉，取出故障风扇。

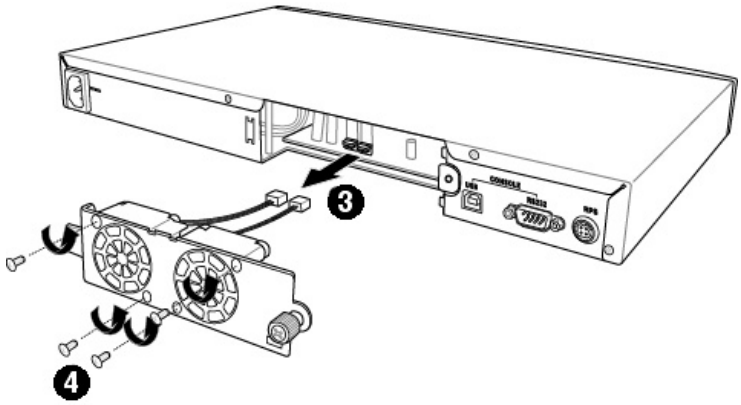

图 63. 将风扇从模块中取出

5. 将新的风扇固定在风扇模块上，请注意风扇电源线应在模块底部。
   按照同样的方式装好另一个风扇。
6. 将电源线连接至电路板上正确的插头。当您面对后端面板时，FAN 1 应该在左边。
7. 将风扇模块装入交换机机箱，并注意风扇的电源线没有夹在模块与机箱之间。
8. 用螺钉将模块固定在机箱上，并再次检查电源线没有被模块与机箱夹住。

风扇规格

尺寸: 40 x 40 x 20 mm

电压与电流: 12VDC, 0.13A

速度: 8200RPM

7.3 简易故障排除

下表列出了您在安装或使用本交换机的过程中可能会碰到的问题及相应的解决方案。

表 9.故障排除

问题	建议方法
LED 指示灯	
开启交换机电源后系统 LED 不亮	确认电源线是否正确连接在交换机上及墙上/延长线的电源插座上。
安装好冗余电源后，RPS LED 指示灯不亮	1. 确认 RPS 电源线是否正确连接在交换机上及墙上/延长线的电源插座上。 2. 确认 RPS 电源符合其所提供的标准。 3. 若您忘记更改后的用户名与密码，进入 BootROM 模式使用“w”启用管理员密码设置（用户名也重置）。然后输入“g”按 Enter 键执行固件。注意用户名与密码只可重设一次。
风扇 LED 指示灯的琥珀色闪烁	检查交换机后端的风扇。若有风扇问题，请参照 7.2 章节更换风扇。
连接好网线之后，网络 LED 不亮	1. 检查网络线是否已正确连接在 LAN 交换机/集线器/PC 及该交换机上。确认 PC 和/或 Hub/交换机电源均开启。 2. 检查您的网络线是否符号要求。如 100 Mbps 的网络（100BaseTx）需使用第 5 类或 6 类网线。10Mbps 的网络可使用级别较低的网线。
网络访问问题	
PC 无法访问同一网络其它	1. 检查网络线是否正常，网络 LED 是否为绿色。 2. 若端口 LED 为琥珀色，请检查此端口是否无 用。若您启用 STP 协议，网络可能会中断一小段时间（约 1 分钟）。

问题	建议方法
PC 无法显示网络设置页面	1. 确认您的交换机电源已开启且连接端口正常。本交换机的默认 IP 地址为 192.168.1.1。 2. 请检查 PC 上的网络安装。若您的 PC 无法正常访问本交换机，可将此交换机的 IP 改为您可访问的 IP 地址。 3. 在您的 PC 上 Ping 交换机 IP 地址，若还是无法联机，请重复第二步。 4. 若 ping 到交换机 IP 地址，但仍无法显示网络设置，请连接 RS232 或 USB 进入终端管理口，并检查过滤规则或静态 MAC 地址是否阻碍 WEB 数据传输。
Web 界面配置	
忘记/遗失登录 WEB 管理接口的用户名称或密码	1. 若您还未更改缺省用户名及密码，请在用户名一栏输入“admin”，无需输入密码 2. 使用 RS232 或 USB 登录终端机模式，通过“sys user show”显示遗失信息
部分页面无法完整显示	1. 确认您使用的是 Internet Explorer v5.5 或更新版本。不支持 Netscape。此外必须在浏览器上选择支持 Javascript®功能及 Java®功能。 2. Ping 交换机的 IP 地址以确定联机是否正常。若联机不正常，请重新检查您的网络设置。
无法保存更改的设置	确认在 **Save Configuration** 页面点击 Save 按钮以保存任何设置更改。
终端控制口	
终端仿真机上无法显示文本	1. 出厂预设数据波特率为 9600bps、无流量控制、8 个数据位（8 bit data）、无同位检查（no parity）及 1 个停止位。 2. 请更改您的终端仿真机设置值为上述数据，若您使用 USB 接口连接交换机，请先安装 USB 驱动程序。 3. 检查网络线是否正常。

8 术语表

10BASE-T 一种用于以太网、数据传输率为 10 Mbps 的线缆，也称为三类(CAT 3)电缆。*见 data rate*、*Ethernet*。

100BASE-T 一种用于以太网、数据传输率为 100Mbps 的线缆，也称为五类(CAT 5)电缆。*见 data rate*、*Ethernet*。

1000BASE-T 一种用于以太网、数据传输率为 1000Mbps 的电缆。

Binary（二进制） 二进制数字系统，即只使用数字“0”和“1”来代表所有的数字。在二进制中，数字“1”写作 1，“2”写作 10，“3”写作 11，“4”写作 100，依此类推。尽管为了方便，IP 地址都写成十进制数字，但它们实际上都是二进制，如：IP 地址 209.191.4.240 在二进制里 1010001.10111111.00000100.11110000，见 *bit*、*IP address*、*network mask*。

Bit（位、比特） "binary digit"的缩写，一个比特是一个具有两个值可选的数，即 0 或 1。*见 binary*。

bps bit/秒

CoS 服务级别（Class of Service）。在 802.1Q 中使用，有效值为 0-7。

Broadcast（广播） 将数据分组发送到网络上的所有计算机。

Download（下载） 从主机上传送数据到远程设备的操作，如从 Internet 到用户。

Ethernet（以太网） 最常用的计算机网络技术，通常使用双绞线。以太网数据传输率为 10 Mbps 和 100 Mbps。见 *10BASE-T*、*100BASE-T*、*twisted pair*。

Filtering（过滤） 依据过滤规则筛选出选定的数据类型。过滤可单向（输入或输出）进行，或双向同时进行。

filtering rule（过滤规则） 决定路由设备接收和/或拒绝何种类型数据的规则。过滤规则常用在接口（或多个接口）及某个特定方向（上游、下行游或两者）中。

FTP 文本传输协议（ File Transfer Protocol）
用于在网络节点之间传输文件的应用协议。通常用于上传文件至服务器或自服务器中下载文件。

Host（主机） 连接至网络的设备（通常为计算机）。

HTTP 超文本传输协议（ Hyper-Text Transfer Protocol）
HTTP 是 Web 浏览器和 Web 服务器用来传输文件的主要协议。见 *web browser*、*web site*。

ICMP Internet 消息控制协议（ Internet Control Message Protocol）
是网络层 Internet 协议，它报告故障并提供与 IP 分组处理相关的其它信息。Ping 命令即使用 ICMP。

IGMP Internet 组管理协议（ Internet Group Management Protocol）
是 IP 主机用来向邻近的组播路由器报告其组播成员的协议。计算机组播群组是指其群组成员已指定接收某一特定内容。IGMP 组播可用来同时更新有一组用户的地址簿。

IGMP Snooping 在每个端口侦测 IGMP 数据包，并连接端口与第二层组播。

Internet 全球最大的互连网，用于个人或商业联络。

intranet 个人、公司内部网络——形同 Internet 的一部分（用户使用网页浏览器访问），但只有内部成员才可进入访问。

IP *见 TCP/IP*.

IP address（IP 地址） Internet 协议地址（ Internet Protocol address）
分配给使用 TCP/IP 的主机（计算机）地址，由 4 个数位组成，每个从 0-255，由句点分开，如： 209.191.4.240。IP 地址由网络号与主机号组成，网络号可识别特定的网络，而主机号则可识别此主机在网络中的地址。子网掩码用于识别网络号与主机号。由于 IP 地址不方便记忆，通常它们用域名来识别。见 *domain name*、*network mask*。

ISP Internet 服务提供商（Internet Service Provider）
为其它公司或个人提供 Internet 接入服务的公司。常需付费。

LAN 局域网（Local Area Network）
所覆盖的地理区域相对较小的网络，如家庭、办公室或一座建筑物。

LED 发光二极管（Light Emitting Diode）
电子发光设备。SL-1000 前端的指示灯即为 LED。

MAC address 媒体访问控制地址（Media Access Control address）
每一个连接到局域网的端口或设备的永久硬件地址，由厂商指定。MAC 地址长度为 6 个字节。

Mask（掩码） 见 *network mask*.

Multicast（组播） 网络对单个分组进行复制并发送到某个网络地址子集。

Mbps Megabits per second 或 one million bits per second 的缩写。网络数据传输率通常用 Mbps 表示。

Monitor（监控器） 也称为"*Roving Analysis*"，用户可将网络分析仪连接在一个端口，以监视交换机上其它端口的流量。

Network（网络） 通过某种传输媒体连接在一起可相互通信的计算机，可共享资源，如软件、文件等。网络可大可小，大如 *Internet*，小如*局域网*。

network mask（网络掩码） 在 IP 中用来指示子网地址所使用的 IP 地址比特，可识别网络号，不识别主机号。比特值设为“1”表示选择此比特，而设为“0”表示忽视此比特。例如，若子网掩码 255.255.255.0 用于 IP 地址 100.10.50.1，则网络号是 100.10.50，而主机号是 1。*见 binary*、*IP address*、*subnet*、*"IP Addresses Explained" 部分*。

NIC 网络接口卡（Network Interface Card）
可插入计算机的适配卡，为网络线缆提供物理接口，以太网的典型的 NIC 是 RJ-45 接口。见 *Ethernet*、*RJ-45*。

Packet（数据包） 网络层的数据单元。每个数据包包括数据和报头如自哪来（源地址）、到哪去（目的地址）。

ping 分组互连网探测器（Packet Internet (or Inter-Network) Groper）
ICMP 回送信息及其应答，经常在 IP 网络中被用来测试网络设备的可达性。

port（端口） 网络互连设备如计算机或路由上的接口，经此接口可传输数据。

Protocol（协议） 一套管理网络中的设备如何交换信息的规则和协定的正式描述。连接双方均需遵循才可成功传输。

Remote（远程） 实质上分开的不同地址。例如，一个在外地旅游的职员登录企业内部互连网络即为远程用户。

RJ-45 注册接口标准（Registered Jack Standard-45）
用于电话线路连接的 8 针脚插座。以太网线缆连接中经常使用此种类型接口。

RMON 远程监控（Remote Monitoring）
SNMP 的延伸，提供综合的网络监控能力。

Routing（路由选择） 根据数据的目的 IP 地址及当前的网络状况，找到最有效的路径的过程。进行路由选择的设备称为路由器。

SNMP 简易网络管理协议（Simple Network Management Protocol）
用于网络管理的 TCP/IP 协议。

STP 生成树协议（Spanning Tree Protocol）
避免数据包在复杂网络中的环路的网桥协议。

Subnet（子网） 子网是网络的一部分。以子网掩码区分，子网掩码可选择网络中的部分计算机而摒弃其它计算机。连接子网的计算机实质上仍连接到母网，但被当作一个单独的网络。见 *network mask*。

subnet mask（子网掩码） 定义子网的掩码。见 *network mask*。

TCP *见 TCP/IP*.

TCP/IP 传输控制协议/IP 协议（Transmission Control Protocol/Internet Protocol）
用于 Internet 的基本协议。TCP 负责将数据分组并在目的地址重组，而 IP 负责将分组的数据包发送到目的地址。若 TCP、IP 与高一级的应用程序捆绑，如 HTTP、FTP、Telnet 等，则 TCP/IP 就指这一整套的协议。

Telnet/SSH（远程登录/SSH） 远程访问计算机的互动的、基于字符的程序。HTTP（网络协议）与 FTP 仅支持远程下载，而 Telnet/SSH 可让用户远程登录并使用计算机。

TFTP 简易文件传输协议（Trivial File Transfer Protocol）
传输文件的协议，TFTP 比 FTP 易于使用，但容量与安全性不如后者。

Trunk（中继线） 两个交换系统之间的连接线路，也称链路汇聚（Link Aggregation）

TTL 存活期（Time To Live）
在数据包传输的过程中，TTL 域指示数据包由于无法处理而被丢弃前还能存活多久。原指时间长度，TTL 通常以跳数为单位。每当路由器接收到一个数据包，该值减去 1（以跳数为单位）。当 TTL 值为 0 时，数据包未到达目的地址，则会被丢弃。

twisted pair（双绞线）电话线路中通常使用的铜线，由一条或多条线绞在一起以降低感应系数与噪音。家用电话中通常是双绞线。以太网线缆中，一种高一级的 3 类线缆(CAT 3)用于 10BASE-T 网络，更高一级的 5 类(CAT 5)线缆用于 100BASE-T 网络。见 *10BASE-T*、*100BASE-T*、 *Ethernet*。

upstream（上行） 从用户至 Internet 的数据传输方向。

VLAN 虚拟局域网（Virtual Local Area Network）

WAN 广域网（Wide Area Network）
在较大地理范围内为用户提供服务的网络，如在一个国家或洲之内。在 SL-1000 中，WAN 指 Internet。

Web browser（Web 浏览器） 超文本客户应用程序，可下载/上传信息，并显示，包括文本、图形、音频或视频等。Web 浏览器应用超文本传输协议。常用 Web 浏览器包括 Netscape Navigator 与 Microsoft Internet Explorer。见 *HTTP*、*web site*、*WWW*。

Web page（网页） 一个典型的网址文件包括文本、图形及该网址与其它网页、其它网址的网页之间的超链接。当用户进入一个网址时，所显示的第一页称为主页。见 *home page*、*hyperlink*、*web site*。

Web site（网址） 连接在 Internet 上的计算机通过 Web 浏览器向远程用户发送(接收）信息。一个典型的网址包括网页，含文本、图形及超链接。见 *hyperlink*、 *web page*。

WWW 万维网（World Wide Web）
是链接超文本文件的网络。全球所有可通过 Internet 登录的网址的集合名词。