GigaX2024B/M

二层网管型交换机

用户手册

C2635
2006 年 9 月
第一版

版权所有・不得翻印 © 2006 华硕电脑

在未获得华硕电脑公司（以下称华硕）书面许可的情况下，本手册中的任何部分，包括所述产品和软件，均不得通过任何手段以任何形式进行复制，转换格式，转译，翻译以及保存于公共资源系统中。本手册仅作为用户购货时附带的说明文档。

若出现以下情况，恕不再提供产品的质保或服务：(1)产品已由未经华硕书面授权的维修商进行维修，改装；或(2)产品序列号无法辨识或已丢失。

华硕提供本手册不代表华硕作出任何隐含或直接的保证，这些保证包括但不限于隐含的质保承诺，产品的畅销性，或针对某种需求的必然适应性。在任何情况下，华硕电脑公司，其领导层，其各级官员和职员，以及其代理商对于本产品造成的任何间接的、特殊的、意外的或后续的损害（包括利润损失、业务损失、资料丢失、业务中断等类似损失）均不承担责任，即使华硕已经事先接到通知提醒，本产品或手册中的错误或缺陷可能导致上述损失。

本手册中的规格和信息仅供参考，并以华硕最新修订版本为准，并且华硕无需对本手册内容的修改进行通知。华硕对本手册中任何错误或不精确的资料均不承担责任，其中包括产品以及所述软件。

本手册中出现的产品和公司名可能是其各自公司的注册商标或版权，华硕在手册中的引用仅作为方便用户进行识别或解释的一种手段，并非对相关公司的侵权行为。

华硕联系信息

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
Email: tsd@asus.com.cn
Netq **论坛**：Netq.asus.com.cn **由华硕工程师提供在线服务**

目录内容

1 产品简介

感谢您购买华硕 GigaX2024B/M 二层网管型交换机！从现在开始，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。

本用户手册将为您提供安装和设置 GigaX2024B/M 交换机所需的相关信息。

1.1 GigaX2024B/M 特性

- 24 个 10/100BSAE-T 以及 2 个 10/100/1000BASE-T 自动侦测 gigabit 以太网交换端口。若使用 all-in-one 模块，GigaX2024M 还可拥有两个额外的 10/100/1000BASE-T 自动侦测 gigabit 以太网交换端口。
- 两个小型 (SFP) Gigabit 端口转换插槽 (GBIC)
- 所有端口支持自动 MDI/MDIX 功能
- 兼容于 802.3z 和 802.3ab 规格
- 802.1D 透明桥接 (transparent bridge)
- STP/RSTP/MSTP
- GigaX2024M 支持 16K (GigaX2024B 支持 8K) MAC 地址缓存及硬件控制的老化时间
- 802.3x 流量控制
- 基于 802.1Q 标记的虚拟局域网（VLAN），GigaX2024B 最多支持 255 组虚拟局域网，GigaX2024M 最多支持 3000 组虚拟局域网
- 802.1p 服务等级， GigaX2024B 每个端口支持 4 个队列，GigaX2024M 每个端口支持 8 个队列。
- 支持 IGMP 侦听
- 802.3ad 链路汇聚（中继），GigaX2024B 最多可支持 6 个中继群组，GigaX2024M 最多可支持 8 个中继群组
- LACP
- GVRP
- 访问控制列表
- 速率限制，GigaX2024B 以 1Mbps 为间隔，GigaX2024M 以 64Kbps 为间隔
- 端口镜像（Port Mirroring）功能
- 802.1x 认证
- 端口安全（Port Security）功能
- 支持 DHCP 侦听

- SNMP v1, v2, v3 简单网络管理协议
- 支持 MIB-II 管理数据库
- 企业级电源供应器、风扇和系统温度、电压管理数据库（MIB）
- Telnet/SSH 远程登录
- TFTP 固件升级和备份设置
- 如 Cisco 操作的 CLI 命令界面
- 网页图形用户界面（GUI）
- LED 指示灯，用于显示端口连接状态

1.2 关于本用户手册

1.2.1 注意事项

- 本手册将在缩写词第一次出现时解释其含义，并将其含义解释收入术语表中。
- 为了方便起见，在本手册中，GigaX2024B/M 交换机将简称为“本交换机”。
- 术语“LAN（局域网）”和“网络”在本手册中将交替使用，表示某个区域内由以太网连接的一组电脑。

1.2.2 印刷提示

粗体字 表示该文字是您从菜单或下拉菜单中选择的项目，或是需要您输入的内容。

1.2.3 提示符号

在本用户手册中会出现以下的图示及说明文字，请您特别注意这些重点事项，这些图示所代表的含义如下：

注意：提供对当前所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，包括涉及人身安全和系统完整性的信息。

2 了解 GigaX2024B/M 交换机

2.1 产品包装内容

GigaX2024B/M 交换机的产品包装中包含以下物品：

- GigaX 2024B/M 二层网管型交换机
- AC 电源线
- 终端管理界面连接线 (DB9)
- 机架安装套件 (包括两个托架与六颗 #6-32 螺丝)
- 连接终端管理界面的 USB 线缆
- 安装光盘
- 快速安装指南

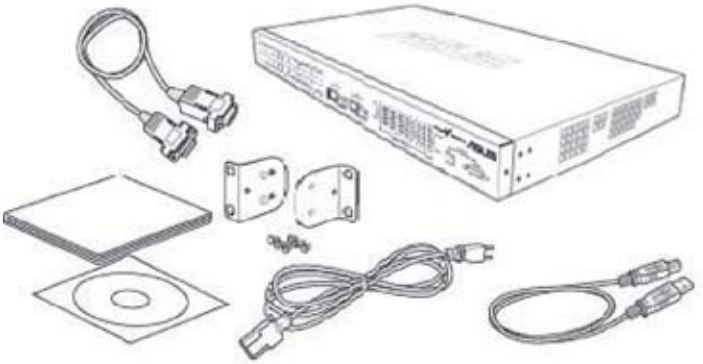


图 1. GigaX 二层网管型交换机产品包装内容

2.2 前面板

前面板包括了 24 个 RJ-45 10/100Base-T 端口，2 个 10/100/1000Base-T 端口，2 个 SPF GBIC 端口和一组 LED 指示灯，用于显示系统、冗余电源(RPS)、风扇与端口的状态。

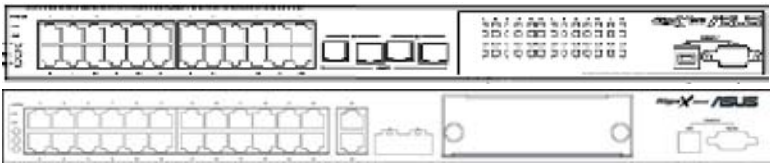


图 2. 前面板（上：GigaX2024B 下：GigaX2024M）

表 1. 前面板标示和 LED 指示灯

标示	颜色	描述
SYSTEM	绿色	设备电源开启
		自检，初始化或下载中
	琥珀色	温度或电压不正常
	熄灭	无电源供应
RPS	绿色	设备的电源供应器 (PSU) 工作正常，且交换机的冗余电源正常
	琥珀色	设备的电源供应器 (PSU) 工作异常，交换机正由冗余电源供电
	熄灭	无电源供应(system LED 亦熄灭)；冗余电源异常或尚未安装(system LED 亮起)
FAN	绿色	两个风扇均工作正常
	琥珀色	两个风扇全部或有一个停止运转
10/100 ports	绿色	以太网连接已建立
		正在传送或接收数据
	熄灭	无以太网连接
10/100/1000 port status	绿色	已建立 RJ-45 或 SFP 连接；端口已启用
		正在传送或接收数据
	琥珀色	已建立连接，但端口已被手动或生成树关闭
		端口处于生成树协议阻塞、侦听和学习状态
	熄灭	无以太网连接
10/100/1000 port speed	绿色	1000Mbps
	琥珀色	100Mbps
	熄灭	10Mbps

2.3 后面板

本交换机的后面板包含有风扇模块、电源线插孔与一个冗余电源供应器(RPS)连接插座。

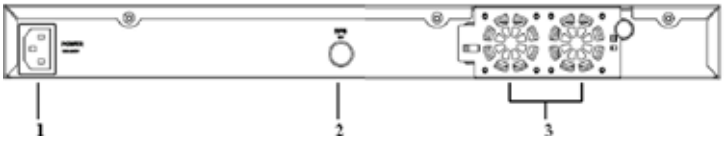


图 3. 后面板

表 2. 后面板标示

序号	标示	描述
1	Power Connector	连接电源线
2	RPS	冗余电源供应器
3	FAN1-FAN2	可替换式风扇

2.4 技术规格

表 3. 技术规格

物理尺寸	43.5mm(H) x 444 mm(W) x 322mm(D)		
电源	输入	耗电量	
	100-240V AC/2.5A 50-60Hz	< 50 瓦	
冗余电源供应器 (RPS)	输入	输出	
	100-240V AC/1.8A 50-60Hz	12V DC/12.5A	
环境需求		操作	存放
	温度	0 ~ 40° C (32 ~ 104° F)	-25 ~ 70° C (-13 ~ 158° F)
	湿度	15 ~ 90%	0 ~ 95%
	高度	最高 10,000ft (3,000m)	最高 40,000 ft (12,000m)
可替换式风扇	尺寸	电压和电流	转速
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

3 快速安装指南

本章节将介绍如何设置交换机的工作环境。您也可以参考 GigaX2024B/M 的安装指南。

第一部分介绍如何将 GigaX2024B/M 交换机安装在水平表面或机架上。

第二部分介绍硬件设置的步骤。

第三部分介绍 GigaX2024B/M 交换机的基本设置。

在您开始安装和设置之前，请先向网络系统管理员取得以下相关信息：

交换机的 IP 地址

默认的网关地址

您所处网络的网络掩码

3.1 第一部分 — 硬件安装

3.1.1 将交换机安装于平坦表面

本交换机必须安装在水平的，且能承受交换机及其附件重量的表面上。请将四个塑胶垫粘贴于交换机底部所标示的位置。

3.1.2 将交换机安装于机架

1. 请将托架分别对准交换机两侧的对应螺丝孔。
2. 用三个螺丝来将托架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托架。
4. 用四个机架螺丝将交换机固定于机架上（本产品包装中不含机架螺丝）。

3.2 第二部分 — 安装交换机

3.2.1 连接控制终端接口（Console port）

在使用控制终端对交换机进行管理之前，请使用 RS232 (DB9) 或 USB 线缆（需要安装随机光盘中的 USB 驱动程序）来连接交换机。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 连接到电脑或局域网

您可以使用以太网线将电脑、集线器(hub)或其他交换机连接到本交换机的端口。您可以使用直通型或交叉型以太网线来连接这些设备。

请使用第 5 类以太网双绞线来连接 1000BASE-T 端口。否则，传输速率无法达到 1Gbps。

3.2.3 连接冗余电源模块（RPS）

将冗余电源(RPS)模块（选购）连接到交换机后面板的 RPS 插孔，并确认 RPS 的另一端连接了电源线。将电源线插到具备接地回路的电源插座上。

3.2.4 连接电源线

1. 将 AC 电源线的一端连接到交换机后面板的电源插孔，然后将电源线的另一端连接到电源插座。
2. 依照表 4 的描述检查前面板的 LED 指示灯状态。若 LED 指示灯亮起，如表中所述，则代表交换机的硬件已正常运行。

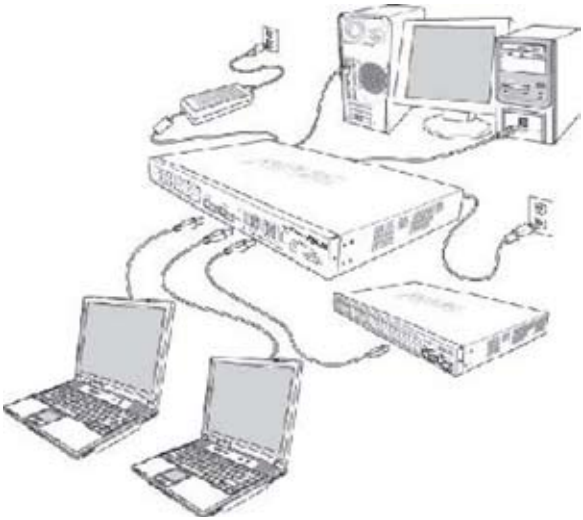


图 4. 硬件连接示意图

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，请检查交换机电源线是否正确连接并已连接到电源插座。
2	Switch ports [1] to [26]	稳定的绿色代表交换机和其他设备的连接已经建立。闪烁代表交换机正在传送或接收数据。
3	RPS	稳定的绿色代表冗余电源（RPS）模块已成功安装。
4	Fan	稳定的绿色代表所有的风扇都运行正常

3.3 第三部分 — 交换机基本管理设置

当您完成硬件的安装和连接后，还需要对交换机进行基本管理设置。您可以用下面的方法进行设置：

- **网页界面：** 本交换机提供网页管理界面，您可以使用带 Java® 功能的 IE5.0 或更高版本的浏览器进行设置。
- **命令行界面**：通过控制终端界面来设置交换机。

3.3.1 通过控制终端界面进行设置

1. 请使用产品包装中附带的交叉型 RS-232 线缆来连接交换机前面右侧的控制终端接口。此接口为 DB-9 公接头，专门用于数据终端设备(DTE) 的连接。将线缆接头上的紧固螺丝固定在控制终端接头上，将线缆的另一头连接到具有终端模拟软件，如 Hyper Terminal 的电脑上。
2. 用产品包装中附带的 USB 线缆将交换机连接到电脑。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/2000/XP 操作系统中模拟一个额外的 COM 端口。
3. 请确认控制终端的模拟软件的设置如下：

   a)选择合适的串口号

   b)将数据波特率设置为 9600

   c)设置数据格式为为无同奇偶校验（no parity），8 个数据位（Data bit）及一个停止位(Stop bit)。

   d)无流量控制

4. 控制终端设置完毕后，您可以在终端画面上看到“ASUS login”。
5. 缺省的用户名称为“admin”，且无需输入密码，直接按下 <Enter> 即可。

您可以随时通过 CLI 命令行界面来修改密码（请参考用户手册 5.3.1 节）。为避免您的交换机被未经许可的人士使用，建议您尽快修改密码。

6.请依照以下步骤来指定交换机的 IP 地址：

a)输入 “enable”。

b)输入 “configure terminal”，新的提示为 “ASUS(config)#”。

c)输入 “interface vlan 1”，新的提示为 “ASUS (config-if)#”。

d)输入 “ip address <您的 IP 地址><您的网络掩码>”。例如，若您的交换机 IP 为 192.168.1.1，网络掩码为 255.255.255.0，则您需要键入 “ip address 192.168.1.1/24”。

e)输入 “end”，此时将回到先前的提示 “ASUS#” 层级。

f)输入 “write”，将会应用变更并将变更写入设置文件中。

g)输入 “reboot”。

如果交换机必须通过网络进行管理，则需要一个默认的网关或静态路由，请按照以下的步骤来指定一个默认的网关或静态路由：

a)输入 “ASUS#”。

b)输入 “show running-configuration” 来查看当前设置。若您输入了不正确的路由，您需要键入 “no ip route 0.0.0.0/0 192.168.1.254” 来删除它。

c)输入 “configure terminal”，新的提示为 “ASUS(config)#”。

d)输入 “no ip route 0.0.0.0/0 192.168.1.254” 来清除默认路由。

e)输入 “ip route 0.0.0.0/0 192.168.1.2” 来设置您的默认路由。

f)输入 “end”。

g)输入 “write”。

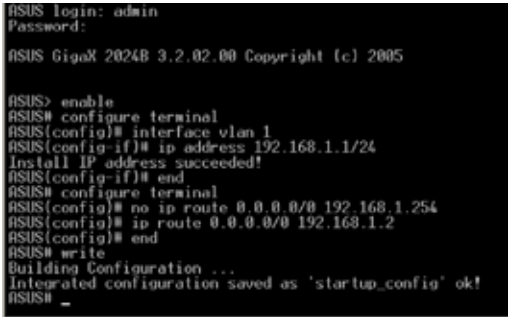


图 5. 控制终端设置

3.3.2 通过网页界面进行设置

若想将您的个人电脑连接到交换机，您的个人电脑必须在网络中取得合法的 IP 地址。请联系您的网络管理人员来取得交换机的合法 IP 地址。若您想要更改交换机的缺省 IP 地址，请参考 3.3.1 节的说明。

1. 若您的电脑中没有安装 Java Runtime Environment，您的电脑将会自动进行下载与安装。这时，您的个人电脑需要能连上 Internet。若您的个人电脑不能连接到 Internet，您必须从光盘或磁盘中安装这个软件。

Java Runtime Environment 安装到您的电脑后，您才可以通过网页进行交换机的管理与设置。您可以从应用程序光盘中找到安装程序。

2. 在交换机可以访问的网络中任何一台电脑上，开启您的网页浏览器(Internet Explorer)，在网址栏内键入以下 URL，并按下 <Enter>:

http://192.168.1.1

这是交换机出厂的缺省 IP 地址值。

此时会出现登录画面，如图 6 所示。

图 6. 登录画面

输入您的用户名称和密码，并按下 OK 以进入设置管理界面。当您第一次登录此画面时，请输入如下所示的缺省值：

缺省用户名 : admin

缺省密码 : (无密码)

您可以随时更改密码（参考 6.3.1 节系统命令部分的说明）。
浏览器将会通过交换机来下载 java 应用程序，这可能需要花费几秒钟的时间。

3. 要设置新的 IP 地址，请点击 System，并选择 IP Setup。 然后请填写 IP 地址、子网掩码与默认网关，完成后点击 OK。

4. 当交换机应用了新的 IP 地址后，浏览器不会自动更新交换机的状态窗口或是退回之前的设置页面。您需要在网址栏内重新输入新的 IP 地址，并按下 <Enter>，重新进入网页设置界面。

图 7. IP 设置

4 用网页界面进行管理

本交换机提供网页管理界面，您可以通过网页浏览器进行交换机的管理工作。本功能推荐使用支持 Java® 的微软 Internet Explorer® 6.0 或更高版本。

4.1 登录网页管理用户界面

1. 在您的电脑上开启网页浏览器(IE)，在网址栏内输入以下内容，并按下<Enter>:

http://192.168.1.1

这是本交换机出厂时缺省的 IP 地址。 输入完成后将会出现登录窗口，如图 8 所示。

图 8. 设置管理界面登录画面

2. 输入您的用户名称和密码，并按下 OK。

   在首次登录时，请使用下面的缺省值。 您可以通过命令行界面随时更改密码（参考 5.3.1 节的说明）。

   缺省用户名：admin

   缺省密码：〈无密码〉

每次当您登录网页管理界面时，您都会看到如图 9 所示的主画面。

图 9. 网页管理界面主画面

4.2 功能结构

网页设置页面包含三个独立的栏位。顶部栏包含了交换机图示和前面板图，如图 10 所示。这个栏位将一直位于浏览器窗口上方 同步显示交换机前面板的 LED 灯。请参考表 4 以认识各指示灯的含义。关于各指示灯颜色的含义，请参考表 5 。

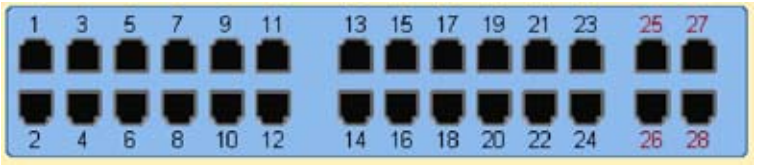
GigaX2024B

GigaX2024M 不带 module 卡

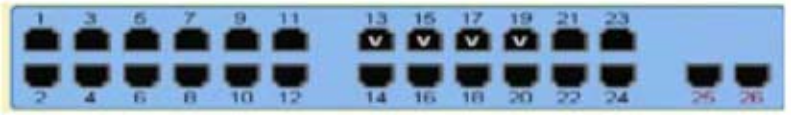
GigaX2024M 带 all-in-one 卡

GigaX2024M 带 stack 卡

图 10. 顶部栏



GigaX2024M 带 all-in-one 卡



GigaX2024B, GigaX2024M 不带 module 卡和 stack 卡

图 11. 端口选择面板

表 5. 端口颜色描述

端口颜色	描述
绿色	以太网连接已建立
琥珀色	连接已存在但端口被手动或被生成树禁用
熄灭	无以太网连接

点击交换机端口图标即可在画面右下方栏位中显示该端口的设置。

菜单项目，如图 12 所示，包含了交换机所有的功能设置选项。这些功能会按照群组划分，例如系统(System)、桥接(Bridge)等功能。您可以点击任何一个项目来开启对应的功能。

图 12. 菜单项目

4.2.1 浏览菜单的技巧

若要开启特定的设置页面，请在菜单中点击您所要开启的选项。

4.2.2 常用按钮与图示

下表介绍了本管理界面中所有按钮与图示的功能。

表 6. 常用按钮与图示

按钮 / 图标	描述
OK	保存您对当前页面做的任何变更。
Reload	重新显示当前页面，更新状态和设置。
Edit	在系统中修改既有设置，如静态路由或过滤的 ACL 规则。
New	在系统中创建一个新的设置。
Add	在系统中新增一个既有的设置，如静态 MAC 地址或过滤的 ACL 规则。
Modify	修改一个既有项目。
Remove	删除已选择的项目，如静态路由或过滤的 ACL 规则。
Query	查找一个指定项目的状态。
Detach All	从所有端口删除此设置值。
Attach All	新增此设置值至所有端口。

4.3 系统页面

系统页面包含有 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 管理（Management）页面

管理（Management）页面包含下列信息：

Model Name: 产品名称。

MAC Address: 交换机的 MAC 地址。

System Name: 用户指定的用来辨识系统的名称（可编辑）。

System Contact（可编辑）。

System Location（可编辑）。

点击 OK 可保存变更并使其立即生效。点击 Reload 将更新设置到当前值。如图 13 所示。

图 13. 管理页面

4.3.2 IP 设置（IP setup）页面

IP 设置（IP Setup）页面包含以下可编辑的信息：

DHCP Client: 启用或禁用 DHCP。

IP Address: 为交换机指定一个静态 IP 地址。

Network Mask（网络掩码）

Default Gateway（默认网关）

点击 OK 可保存变更并使其立即生效。点击 Reload 将更新设置到当前值。

图 14. IP 设置页面

4.3.3 重新启动（Reboot）页面

Reboot 页面包含了一个 Reboot 按钮。点击此按钮可以重新启动系统。

重新启动系统将暂时中断网络连接及网页管理界面的连接。

4.3.4 固件升级（Firmware Upgrade）

Firmware Upgrade and Auto-config 页面包含下列信息：

Hardware Version: 显示硬件版本号。

Boot ROM Version: 显示 boot code 版本。

Firmware Version: 显示当前所运行的固件版本。本编号会随着固件的升级而改变。

输入 TFTP 服务器的 IP 地址与固件名称。点击 Upgrade 来升级交换机的固件。请参考图 15。

例如：TFTP 服务器：192.168.1.155　文件名称：gx2024b-3.2.02.0a.img

点击 Upload 按钮将指定的固件载入到交换机中。升级完成后请重新启动交换机。您需要重新登录网页设置界面。

图 15. 固件升级页面

4.4 物理端口

物理端口会即时显示以太网端口的状态。您可以设置以下项目：

Port: 选择需要设置的端口

Admin: 启用／禁用端口

Mode: 设置速度与双工模式

Flow Control: 启用／禁用 802.3x 流量控制机制。

Switchport Mode: 设置此端口为中继（trunk）模式或访问（access）模式

Admin port VLAN: 将选择的端口指定到特定的 PVID

DHCP-Snoop: 完整启用／禁用 DHCP 侦听功能。要将此功能应用至指定的 VLAN，您需要在 VLAN 设置（VLAN Configuration）中为不同的 VLAN 开启 VLAN-Snooping 功能。

DHCP-Snooping: 指定所选择的端口为不可信任或可信任的端口。

选择对应的端口号并对其进行设置，然后点击 Modify 按钮。您所更改的项目将会在窗口中更新。然而，只有点击了 Save Configuration 按钮之后，您所做的更新才会生效。

Runtime Status Window: 显示每个端口的下列相关信息。

Ethernet Link: 已连接或未连接状态。

STP Status: STP(生成树) 状态。

Duplex: 双工模式。

Speed: 连接速度。

Flow Control: 启用或禁用 802.3x 流量控制机制。

图 16. 物理端口 - 设置页面

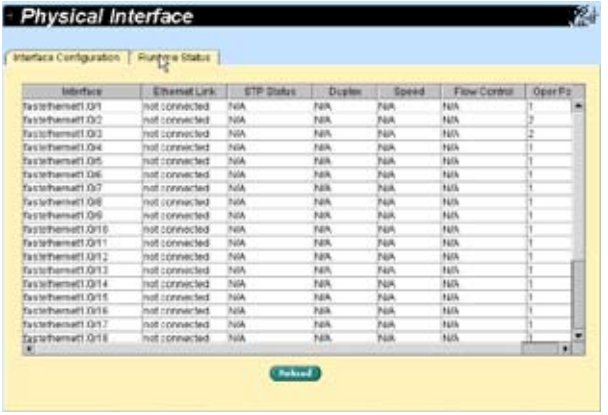


图 17. 物理端口 - runtime status 页面

4.5 桥接（Bridge）页面

桥接（Bridge）页面群组中包含了交换机的二层设置，如链路汇聚（Link Aggreration），STP 等项目。

4.5.1 生成树（Spanning tree）

本页面可设置三种不同类型的生成树协议。

4.5.1.1 STP 状态（STP Status）

第一页“STP Status”可以启用或禁用 STP。您可以启用 STP、RSTP 与 MSTP 三种模式。若启用了 MSTP，则以下的四种属性也同时启用：

Region Name: 由字母和数字组成的名称。

Revision: 设置版本编号。

Instance ID: STP 实例（instance），您可以在交换机上设置 MSTP 来将多个 VLAN 映射到一个单一的 STP 实例（instance）。

VLAN Group: 此群组能联结可被建立的 3000 个 VLAN 里的每一个 VLAN 到给定的实例（instanace）。

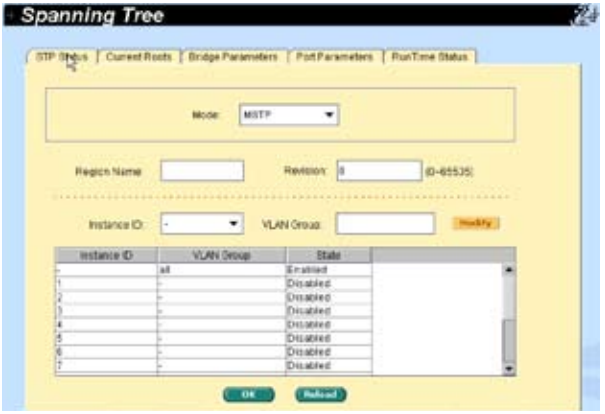


图 18. 生成树 - status 页面

4.5.1.2 当前根（Current roots）

本页显示了当前根的相关信息，包括：

- 实例（Instance）ID
- VLAN 群组属于哪个实例（Instance）ID
- 根桥的 MAC 地址
- 根桥的优先顺序
- 根桥的最长存在时间
- 根桥的 Hello timer
- 根桥的转发延迟计时器
- 根桥的路径开销（Cost）
- 桥接器的根端口

图 19. 生成树 - current roots 页面

4.5.1.3 桥接器参数（Bridge parameters）

在这个页面中可以设置 BPDU 传输的生成树参数（Spanning-tree parameters）：

Hello Time: BPDU 生成设置的间隔。

Max Age: 局域网中所有桥接设备使用的超时设置值。

Forward Delay: 转发延迟。

Bridge Priority: 交换机在局域网中的优先顺序。

Transmission Limit: 根交换机总是传送一个 BPDU（或 M-record）信息，开销（Cost）为 0，transmission limit 设置为最大值。

图 20. 生成树 - bridge parameters 页面

4.5.1.4 端口参数（Port parameters）

本页面包含了一个显示窗口，用来显示每个端口的当前设置。您可以选择一个端口然后对其进行编辑。点击 Modify 按钮将更改端口的生成树设置。您可以设置以下栏位：

Instance ID(仅 MSTP): 一个生成树实例（instance），您可以在交换机上设置 MSTP 来将多个 VLAN 映射到一个单一的 STP 实例（instance）。

Priority: 设置交换机端口的优先顺序。越小的数字代表越高的优先顺序。当侦测到网络回路的状况下，拥有较低优先顺序的端口较可能被 STP 阻塞。有效的设置值为 0 至 240。

Path Cost: 有效的设置值为 1 至 65535(RSTP:200000000)。当侦测到网络回路的状况下，具有较高开销（Cost）的端口较可能被 STP 阻塞。

Link Type: 缺省情况下，连接类型（Link Type）由端口的双工模式决定：全双工模式的端口被判定为点对点连接；半双工模式的端口被判定为共享连接。

Edge Port: 边缘端口与 Port Fast-enabled 端口相同，只有在连接了一个单独的终端设备时您才可以启用它。

点击 OK 使设置生效。点击 Reload 更新设置到当前值。

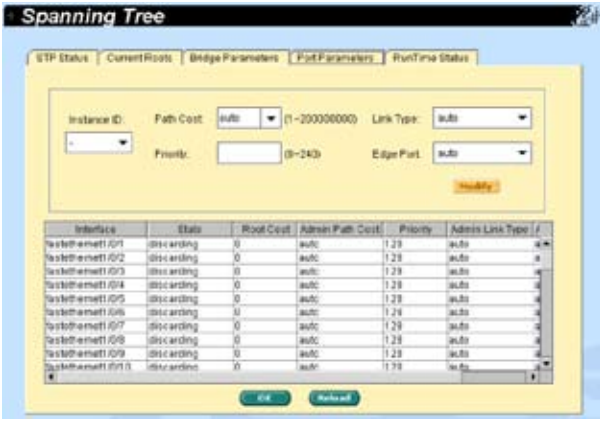


图 21. 生成树 - port parameters 页面

4.5.1.5 运行状态（Runtime status）

本页面包含了一个显示窗口，用来显示每个端口的当前状态。

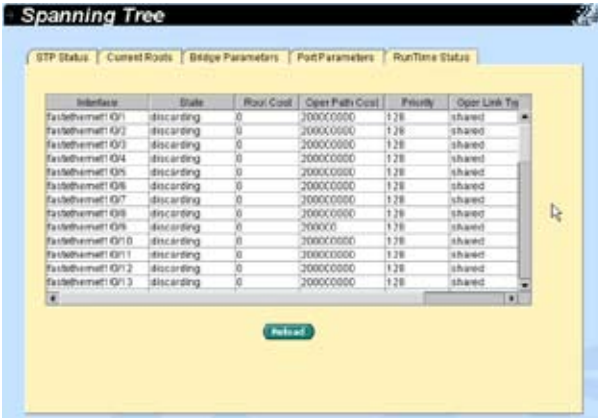


图 22. 生成树 - runtime status 页面

4.5.2 链路汇聚（Link aggregation static）

本页面用来设置链路汇聚群组。GigaX2024B 最多可提供 6 个链路汇聚群组，而 GX2024M 最多可提供 8 个链路汇聚群组。

Port Selection Criterion: 依照封包的来源 MAC 地址、目的地 MAC 地址、来源与目的地 MAC 地址、来源 IP 地址、目的地 IP 地址、来源与目的地 IP 地址在链路汇聚群组的各端口之间分配封包的一种算法。

Trunk ID: 除了群组名称外，用来区分不同汇聚群组的号码。

Port: 这些端口的图示按照交换机前面板上的位置列出。点击图示可以选择群组成员。再次点击选中的图示可将这个端口从群组中删除。

点击 OK 来将设置传送到交换机。点击 Reload 来更新设置到当前值。要使设置生效，请至 Save Configuration 页面并点击 Save。

您需要检查连接速度和双工模式来确认链路汇聚群组实体处于正常运行状态。请至 Physical Interface 页面的 Runtime status 窗口检查汇聚端口的连接模式。如果所有的汇聚群组成员都具有相同的速度和全双工模式，则汇聚群组已正确建立。如果有一个端口具有不一致的速度和双工模式，则汇聚群组的设置不正确。 请检查您的设置，使汇聚群组中的所有成员都具有相同的速度和全双工模式。

链路汇聚群组中所有的端口必须全部在全双工模式下运行且具有相同的速度。

链路汇聚群组中所有的端口必须设置为自动协商（auto-negotiation）模式或全双工模式。这样设置才可能使用全双工模式连接。若您将端口设置为强制全双工模式，则其他端口也必须具有相同的设置，否则链路汇聚可能发生运行异常的状况出现。

链路汇聚群组中所有的端口必须具有相同的 VLAN 设置。

链路汇聚群组中所有的端口都被视为一个逻辑连接，也就是说，如果任何一个群组成员属性改变，其他成员的属性也随之改变。例如，某链路汇聚群组包括端口 1 和端口 2。若端口 1 的 VLAN 改变，则端口 2 的 VLAN 也随之改变。

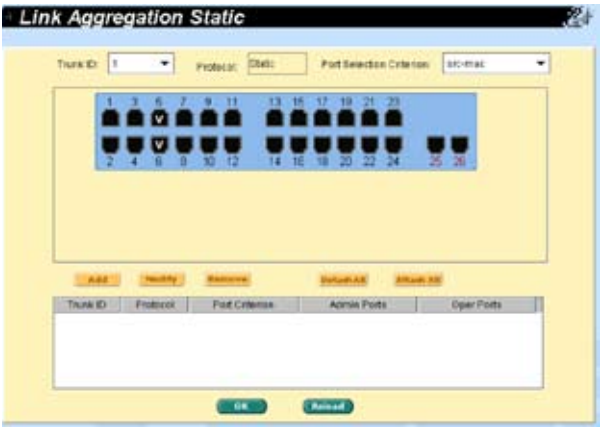


图 23. 链路汇聚页面

4.5.3 LACP

本页面用来设置 LACP 群组(端口汇聚)。GX2024B 提供了最多 6 组(GX2024M 提供最多 32 组)链路汇聚群组，每个群组最多可支持 8 个端口。

Port Selection Criterion: 依照封包的来源 MAC 地址、目的地 MAC 地址、来源与目的地 MAC 地址、来源 IP 地址、目的地 IP 地址、来源与目的地 IP 地址在链路汇聚群组的各端口之间分配封包的一种算法。

Trunk ID: 除了群组名称外，用来区分不同汇聚群组的号码。

Port: 这些端口的图示按照交换机前面板上的位置列出。点击图示可以选择群组成员。再次点击选中的图示可将这个端口从群组中删除。

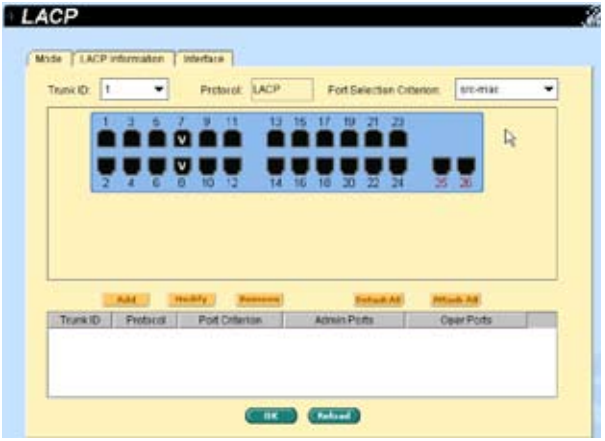


图 24. LACP 页面

4.5.4 镜像（Mirroring）

镜像，配合网络流量分析，可以帮助您监控网络流量。您可以监控所选定之端口的传出与传入封包。

Mirror: 从选择面板上选择镜像群组。您可以对选定端口的传入、传出流量或同时对这两种流量进行镜像。

Mirror Mode: 启用或禁用选定群组的镜像功能。

Monitor Port: 接收选定的镜像端口的所有流量的备份数据。

监控端口不能属于任何链路汇聚群组。

监控端口不能属于任何私有 VLAN。

监控端口不能像一般交换机端口一样运行。它不能进行封包交换或地址学习。

点击 OK 将设置发送至交换机（HTTP 服务器）。点击 Reload 更新设置至当前值。

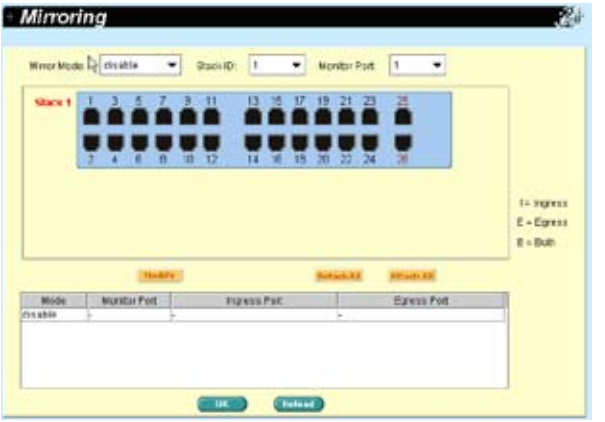


图 25. 镜像页面

4.5.5 静态组播（Static multicast）

在这个页面中，您可以将组播地址添加至组播列表。本交换机可以容纳 256 个组播地址。群组中所有端口将把特定的组播封包转发至这个群组的其他端口。

Port: 从选择面板上选择端口，或者从显示列表中选择一个既有的群组地址。

VLAN: 选择 VLAN 群组，这是一个基于 VLAN 的功能。

MAC Address: 指定组播地址。

CoS: 指定服务等级（CoS）的优先顺序。

点击 OK 来使设置生效。点击 Reload 将设置更新至当前值。

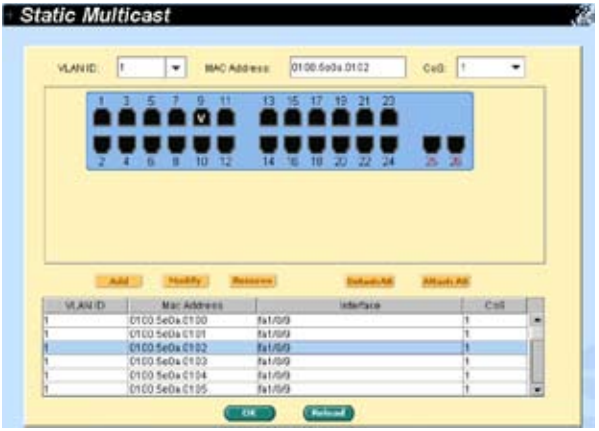


图 26. 静态组播页面

4.5.6 IGMP 侦听（IGMP snooping）

通过开启或关闭 IGMP 侦听功能，可以帮助减少网络中的组播流量。

第一部分提供以下功能设置：

Enable IGMP Snooping: 完整开启所有 VLAN 端口的 IGMP 侦听功能。在缺省值中，交换机的 IGMP 侦听功能已经开启。当完整开启后，所有 VLAN 端口的 IGMP 侦听都被开启。

若完整侦听功能没有开启，您无法开启 VLAN 侦听功能。若完整侦听功能开启，您可以开启或关闭 VLAN 侦听功能。

Last Member Query Interval: 没有即时离线（Immediate-Leave）功能的情况下，当交换机的接收端口从一个用户处收到一个 IGMP 离线信息时，不会立即离线。它会传送一个 IGMP 询问到该端口，并等待 IGMP 群组所有成员回复。如果在设置的时间内，没有收到回复，该接收端口将从多重组播的群组成员中删除。

第二部分提供以下功能设置：

Status: 如果完整的侦听功能已开启，您可以开启或关闭 VLAN 侦听功能。

Immediate leave: 当您开启 IGMP 即时离线（Immediate-Leave）功能后，当交换机在某端口检测到一个 IGMP 版本 2 离线信息时，交换机会立即将该端口删除。只有当 VLAN 中每个端口只有一个主机的情况下才可以使用即时离线（Immediate Leave）功能。仅 IGMP 版本 2 的主机才可支持即时离线（Immediate Leave）功能。

然而，如果静态地址占用了全部的 256 个地址空间，IGMP 侦听将无法正常运行。本交换机只允许 256 个二层组播群组。

图 27. IGMP 侦听页面

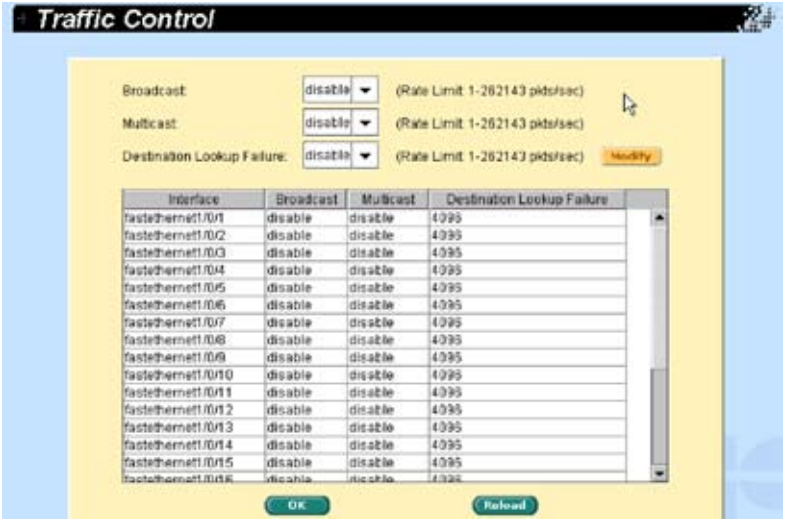
4.5.7 流量控制（Traffic control）

流量控制（Traffic control）可防止涌入过多的泛洪（flooding）封包，如广播封包、组播封包与目的地地址搜寻失败的单一播送封包等，避免系统带宽异常负荷。本页面中所输入的限制数字为所有已开启类型之封包的数目总和。例如，若开启了广播与组播，则这两种封包的总和不能超过已设置的限制数值。

选择一个端口并进行需要的设置，然后点击 Modify。

点击 OK 来保存新设置。要使设置生效，请至“Save Configuration”页面，然后点击 Reload。

GigaX2024B 流量控制



GigaX2024M 流量控制

图 28. 流量控制页面

4.5.8 动态地址（Dynamic addresses）

本页面显示了依据端口、VLAN ID 或指定的 MAC 地址来搜寻动态 MAC 地址的结果。动态 MAC 地址是交换机自动学习的 MAC 地址，若该地址在其存在时间内，没有被交换机再次学习，该地址就会从地址表中老化（age out）。用户可以输入一个 10~1,000,000 范围内的值（单位为秒），即可设置地址的老化时间。点击 OK 可保存新的老化时间值。要使设置生效，请至“Save Configuration”页面，然后点击 Reload。

您可以通过端口、VLAN ID 与／或 MAC 地址来搜寻 MAC 地址，然后点击 Query。地址窗口将显示搜寻结果。

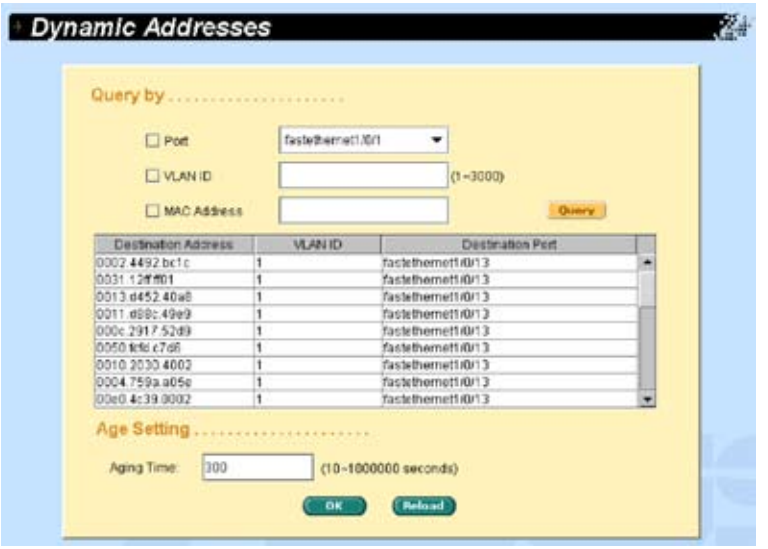


图 29. 动态地址页面

4.5.9 静态地址（Static addresses）

您可以将 MAC 地址添加到交换机的地址表中。通过这种方式添加的 MAC 地址将不会老化（age out），我们称其为静态地址。本交换机允许使用 1024 个静态地址。

MAC Address: 输入 MAC 地址

VLAN ID: 输入此 MAC 地址所归属的 VLAN ID

Port Selection: 选择此 MAC 地址所归属的端口

当您依据上述信息创建了一个新的静态 MAC 地址时，请点击 Add。然后您将在地址窗口中看到这个新增的地址。

您可以用鼠标选定一个既有的地址，然后点击 Remove，即可删除这个地址。Modify 按钮可更新既有的 MAC 地址。您也可以输入 MAC 地址与 VLAN ID，然后按下 Query 来搜寻某个静态地址。点击 OK 将设置传送至交换机（HTTP 服务器）。点击 Reload 更新设置至当前值。要使设置生效，请至 Save Configuration 页面，然后点击 Save。

图 30. 静态地址页面

4.5.10 VLAN 设置（VLAN configuration）

在这个页面中，您可以设置并显示最多 254 个（2024M 为 3000 个）VLAN 群组。VLAN1 是预设的 VLAN，是由系统建立的，无法被删除。本功能可避免交换机的不正常运行。除了预设的 VLAN1 以外，您可以删除其他任何一组既有的 VLAN。

您可以按端口按钮来指定该端口为已标记（tagged）或未标记（Untagged）端口。在端口选择面板上有三种类型的按钮：

“U” type: 未标记的端口，从该端口传送出去的封包会被删除 VLAN 标记（tag）。

“T” type: 自本端口传送的封包都会被标记。

“blank” type: 本端口并非 VLAN 群组的成员。

如果一个未标记的连接端口同时属于两个或更多的 VLAN 群组，将有可能造成交换机的混乱并导致流量拥塞状况。要避免这类状况，交换机只能允许某个未标记端口在同一时间内只属于一个 VLAN。

若您想要将一个未标记的端口从一个 VLAN 配置到另一个 VLAN，您需要首先将其从原有的 VLAN 中删除，或在原有 VLAN 中将其设为已标记状态。

VLAN ID: 当建立一组新的 VLAN 时，这个栏位要求用户输入 VLAN ID。

Name: 本栏位要求用户输入 VLAN 的名称。

DHCP-Snooping: 开启／关闭 VLAN 的 DHCP 侦听功能。

点击 OK 保存设置。要使设置生效，请至 Save Configuration 页面，然后点击 Save。

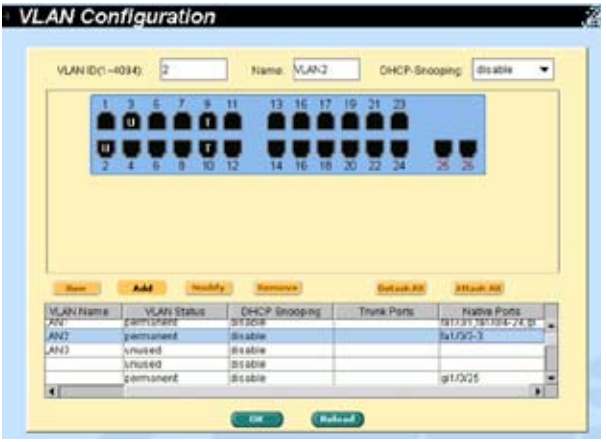


图 31. 标记 VLAN 页面

建立 60 组 VLAN（包括端口 fa1/0/1~fa8/0/26)，大约需要 3 分钟。

建立 256 组 VLAN（包括端口 fa1/0/1~fa8/0/26)，大约需要 5 分钟。

建立 1024 组 VLAN（包括端口 fa1/0/1~fa8/0/26)，大约需要 14 分钟。

建立 2000 组 VLAN（包括端口 fa1/0/1~fa8/0/26)，大约需要 26 分钟。

建立 3000 组 VLAN（包括端口 fa1/0/1~fa8/0/26)，需要超过 30 分钟。

4.5.11 GVRP

GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) 是 IEEE 802.1Q 标准定义的应用程序，提供 VLAN 相关控制。

GVRP 仅能在 802.1Q 中继端口下执行，主要用来在 VLAN 中去除那些不需要在中继交换机之间传递的流量。以下是 GVRP 设置参数：

GVRP Enable: 在缺省状况下，交换机的 GVRP 没有开启。您必须首先在交换机上开启 GVRP 功能，才能设置 802.1Q 端口进行 GVRP 操作。

Port Mode: 在单独的 802.1Q 中继端口上开启／关闭 GVRP。GVRP 必须在中继的两端都进行设置，才能使中继正常运行。

Registration: 在缺省状况下，GVRP 端口为正常（Normal）注册模式。这些端口使用从邻近的交换机上获得的 GVRP 加入信息修整在 802.1Q 中继连接上运行的 VLAN。若设备的另一端无法传送 GVRP 信息，或者您不想让交换机修整任何 VLAN，请使用固定（Fixed）模式。Fixed 模式端口将转发所有存在于交换机数据库中的 VLAN。而禁止（Forbidden）模式下的端口只转发 VLAN 1。

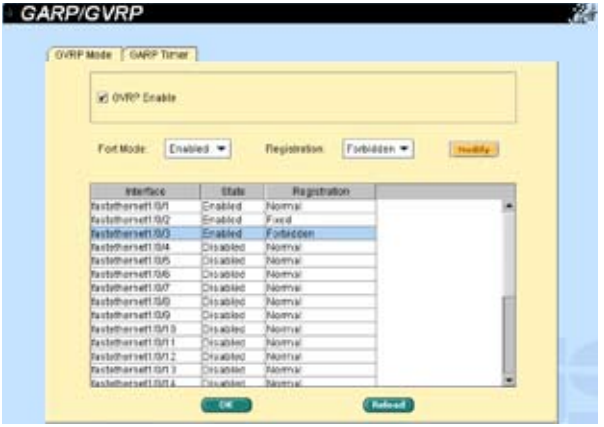


图 32. GVRP 页面

如果需要，您可以编辑以下属性：

Joint Timer: 以百分之一秒为单位设置数值。

Leave Timer: 以百分之一秒为单位设置数值。

LeaveAll Timer: 以百分之一秒为单位设置数值。

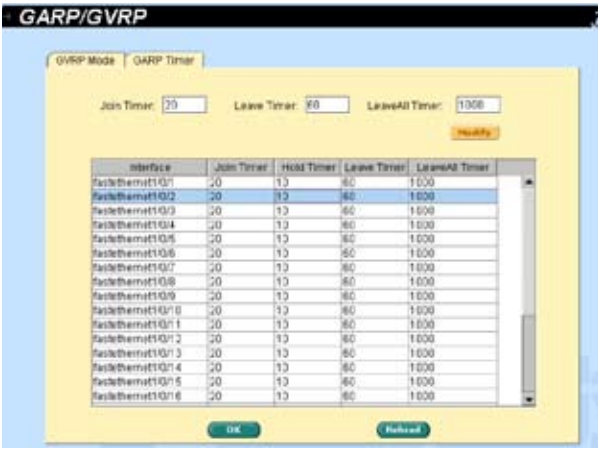


图 33. GARP timer 页面

4.5.12 QoS 与 CoS

4.5.12.1 802.1p 优先级

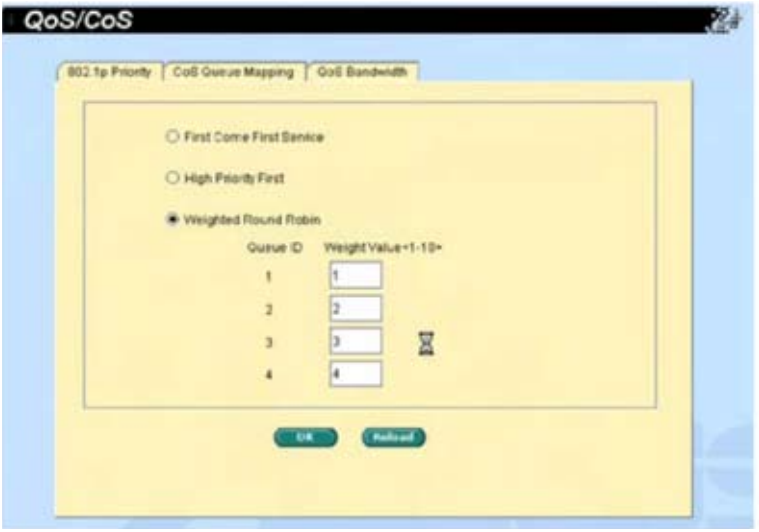
本交换机的每个端口支持四个(GigaX2024B)/ 八个(GigaX2024M) 传出队列。这些队列可以设置为先到先服务（First Come First Service)，最高优先级排序（High Priority First）或加权循环排序（Weight Round Robin，WRR)。绝对优先队列（strict priority queue）在其他队列得到服务之前必须为空。您可以使用绝对优先队列来传送那些关键的或是有很强时效性的流量。以下有三个选项：

First Come First Service: 第一个来到的帧具有最高的优先级。

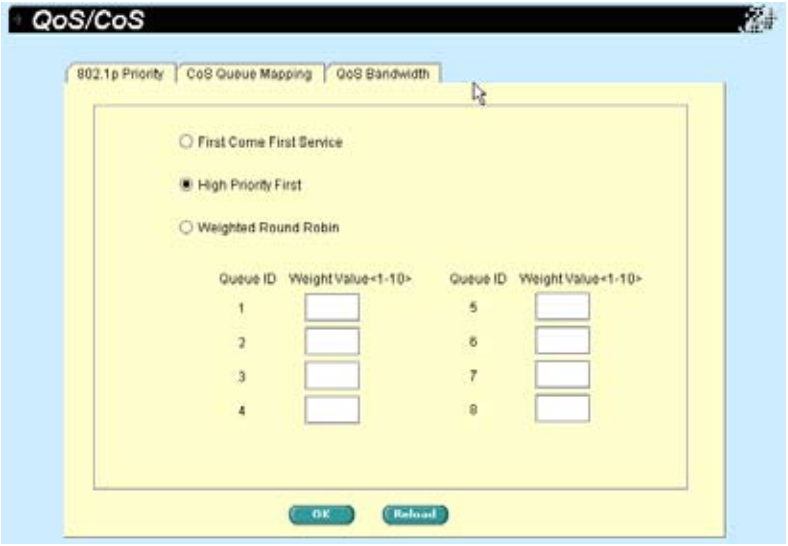
High Priority First: 封包的优先级取决于其 CoS 数值。

Weighted Round Robin (WRR): 若启用了 WRR 算法，加权比率即为每个队列中 WRR 算法的封包被传送频率的比率。

点击 OK 保存设置。要使设置生效，请至 Save Configuration 页面，然后点击 Save。



GigX2024B QoS/CoS



GigaX2024M QoS/CoS

图 34. QoS/CoS 页面

4.5.12.2 CoS 队列映射

GigaX2024B 每个端口支持四个传出队列 (GigaX2024M 支持八个传出队列)，这些队列都可以采用绝对优先级排序。也就是说，每一个 CoS 数值都可以映射至这四／八个队列之一。对于绝对优先级， 队列四／八具有最高的优先级来传送封包。点击 OK 保存设置。要使设置生效，请至 Save Configuration 页面，然后点击 Save。

对于 GigaX2024B，CoS 数值范围从 1 至 4，其中，1 代表最低优先级，4 代表最高优先级。对于 GigaX2024M，CoS 数值范围从 1 至 8，其中，1 代表最低优先级，8 代表最高优先级。

图 35. CoS 队列映射

4.5.12.3 QoS 带宽（QoS bandwidth）

本页面为每个端口提供了一些与 VLAN 标记相关的设置，包括：

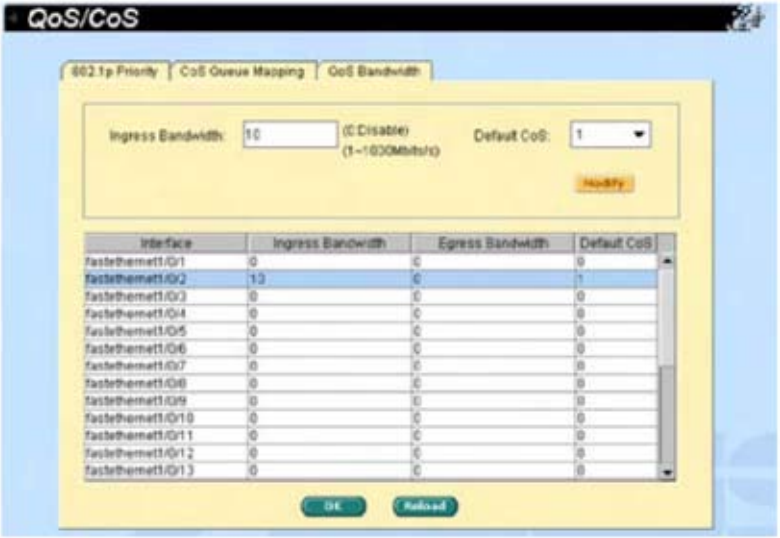
Port: 从列表窗口中选择一个端口进行设置

Ingress Bandwidth: 选定端口的最大传入带宽。

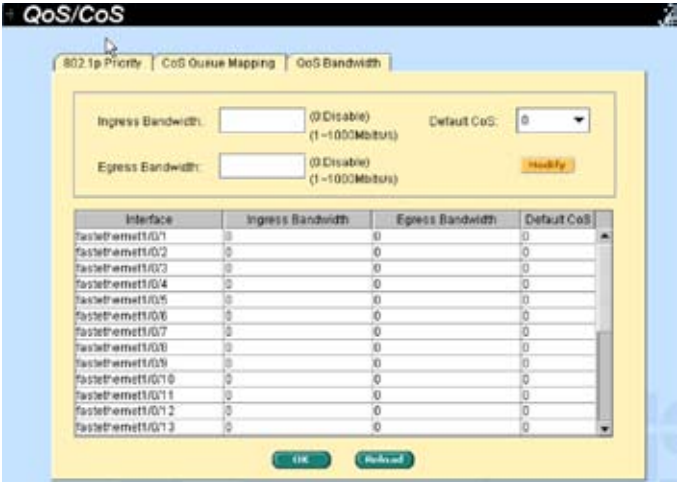
Egress Bandwidth: 选定端口的最大传出带宽（仅 GigaX2024M 适用）

Default CoS: 从这个端口接收到的未标记封包在标记 VLAN 中都会被指定为此 CoS 数值

点击 Modify 更改端口列表窗口中的内容。点击 OK 保存设置。要使设置生效，请至 Save Configuration 页面，然后点击 Save。



GigaX2024B QoS 带宽



GX2024M QoS 带宽

图 36 QoS 带宽页面

4.6 简单网络管理协议（SNMP）

本群组提供包括群组列表（Community Table）、主机列表（Host Table）与 Trap 设置（Trap Setting）在内的 SNMP 设置。

4.6.1 群组列表（Community Host Table）

本页面将主机 IP 地址与群组名称联系起来。输入一个 IP 地址，输入群组名称并从下拉菜单中选择群组类型。“ro” 代表只读，“rw” 代表读／写。点击 OK 永久保存设置，或点击 Reload 更新页面。

图 37. 群组主机列表页面

4.6.2 Trap 设置（Trap setting）

通过设置 Trap 目的地 IP 地址与群组名称，您可以开启 SNMP Trap 功能来传送不同版本的 Trap 封包(v1 或 v2c)。点击 OK 永久保存设置，或点击 Reload 更新页面。

图 38. Trap 设置页面

4.6.3 SNMPv3 VGU 列表

这里有两项 SNMPv3 定义的新安全功能。一为 USM（User-based Security Model，基于用户的模型），可提供 SNMPv3 封包的认证、加密与解密。二为 VACM（View-based Access Control Model，基于检视的访问控制模型），可提供访问控制。以下为相关的三个页面。 点击 OK 永久保存设置，点击 Reload 更新页面。

4.6.3.1 VACM 检视（VACM view）

VACM 检视用来查看 SNMPV3 VACM 群组信息。

View Name: 输入安全群组名称。

View Type: 输入检视所属的检视类型（View Type）。当检视子树（View Subtree）与 SNMPv3 信息中的 Oid 相符合时，选择包含（Included）或排除（Excluded）。

View Subtree: 输入检视（View）所属的检视子树（View Subtree）名称。子树(Subtree)是一个 Oid，它与 SNMPv3 信息中的 Oid 相符合。当子树短于 SNMPv3 信息中的 Oid 时，为良好的符合状态。

当您通过上述信息建立一组新的 VACM 检视项目后，点击 Add。然后您将看到新增的项目显示在检视窗口中。您可以用鼠标选定一个既有项目，并点击 Remove 将其删除。点击 Modify 按钮可更新既有 VACM 检视项目。点击 OK 保存设置。点击 Reload 更新设置到当前值。要使设置生效，请至 Save Configuration 页面，然后点击 Save。

图 39. SNMPv3 VGU 列表 1

4.6.3.2 VACM 群组（VACM group）

VACM 群组用来设置 SNMPV3 VACM 群组。

Group Name: 输入安全群组名称。

Read View Name: 输入群组所属的读取检视名称。相关的 SNMP 信息有：Get，GetNext，GetBulk。

Write View Name: 输入群组所属的写入检视名称。相关的 SNMP 信息为 Set。

Notify View Name: 输入群组所属的通知检视名称（Notify View Name）。 相关的 SNMP 信息为 Trap，Report。

Security Model: 输入群组所属的安全模型名称（Security Model Name）。Any 适用于 v1,v2,v3。USM 则与 SNMPv3 相关。

Security level: 输入群组所属的安全等级名称（Security level Name）。可选的项目有 NoAuth，AuthNopriv 与 AuthPriv。

当您通过上述信息建立一个新的 VACM 群组后，请点击 Add。然后您将看到新增的项目显示在群组窗口中。您可以用鼠标选定一个既有群组，并点击 Remove 将其删除。点击 Modify 按钮可更新既有 VACM 群组项目。点击 OK 保存设置。点击 Reload 更新设置到当前值。要使设置生效，请至 Save Configuration 页面，然后点击 Save。

图 40. SNMPv3 VGU 列表 2

4.6.3.3 USM 用户（USM User）

USM 用户（USM User）功能用来设置 SNMPv3 USM 用户信息。

User Name: 指定安全群组的用户名称

Group Name: 输入安全群组的名称

Auth Algorithm: 输入 SNMP 用户和安全群组所属的认证协议（Auth Protocol），可选的项目有 NoAuth，MD5 与 SHA1。若选择了 NoAuth，则不需要输入密码。

Auth Password: 输入认证算法（Auth Algorithm）的密码。此密码至少为 8 位数的数字或字符。

Priv Algorithm: 输入 SNMP 用户和安全群组所属的 Priv Protocol。可选的项目有 NoPriv 与 DES。若选择了 NoPriv，则不需要输入密码。

Priv Password: 输入 Priv Protocol 的密码。此密码至少为 8 位数的数字或字符。

Security level: 输入群组所属的安全性等级名称（Security level Name）。 可选的项目有 NoAuth，AuthNopriv 与 AuthPriv。

当您通过上述信息建立一组新的 VACM 群组项目后，点击 Add。然后您将看到新增的项目显示在群组窗口中。您可以用鼠标选定一个既有群组，并点击 Remove 将其删除。点击 Modify 按钮可更新既有 VACM 群组项目。点击 OK 保存设置。点击 Reload 更新设置到当前值。要使设置生效，请至 Save Configuration 页面，然后点击 Save。

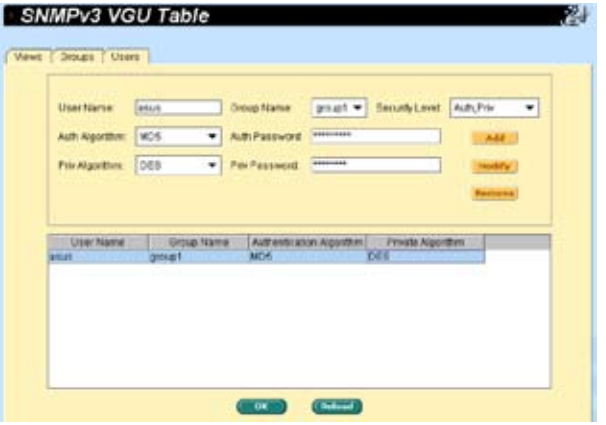


图 41. SNMPv3 VGU 列表 3

4.7 过滤功能页面（Filter pages）

本交换机可根据第二层至第四层封包的头信息来过滤某些封包类型。每个过滤设置都包含多个规则。您需要将过滤设置应用至某些端口才能使过滤功能生效。

4.7.1 过滤组合（Filter set）

本交换机定义了两种规则模式，一种为 MAC 模式，另一种为 IP 模式。只有相同的规则模式可以相互组合形成一组过滤设置。 每种模式具有不同的过滤选项。例如，您可以使用 IP 模式来过滤 FTP 封包。

您可以选择 MAC Filter 并命名，然后点击 Add 来新增一组 MAC 过滤规则。 您也可以选择 IP Filter 并指定其 ID/ 名称， 然后点击 Add 来新增一组 IP 过滤规则。点击 OK 永久保存设置，点击 Reload 更新页面。在编辑前请点击 OK 按钮。

点击您需要编辑或删除的过滤设置。然后点击 Edit 进入规则页面。或点击 Remove 删除该过滤设置。您必须遵照以下规则来建立一组有效的过滤设置。

一个过滤设置组合由一种类型的规则构成。在相同范围内过滤封包的规则属于同一类型。例如，两个规则都是用目的地 IP 地址过滤封包，则它们属于同一类型。但是用来源 IP 地址过滤封包的规则就不属于同一类型。

一个端口可以同时应用四种类型的规则。 若超过了四种，系统会自动禁用这些规则。

图 42. 过滤组合页面

过滤规则（Filter Rule）页面提供了规则模式的选项，一种为 MAC 规则，另一种为 IP 规则。若您没有在空白栏位输入 MAC 地址，则代表此规则对所有的 IP 地址有效。在 IP 规则设置中，您可以输入以下五种类型中的任一种：source IP（来源 IP 地址），destination IP（目的地 IP 地址），protocol（协议），source application port（来源应用端口）与 destination application port（目的地应用端口）。在 Action 栏位，您可以选择要转发或丢弃符合规则的封包。若一个封包符合两种规则，且这两种规则对应不同的动作，封包将依据规则列表中显示的第一个规则来执行。

图 43. MAC 模式下的过滤规则

图 44. IP 模式下的过滤规则

以下两种方式告诉您如何提供 IP：

1. 指定一个专用 IP， Type = subnet，IP = 10.10.1.2，Wildcard = 0.0.0.0
2. 指定一个子网（一组 IP），Type = subnet，IP = 10.10.1.0，Wildcard = 0.0.0.255

4.7.2 附加过滤规则（Filter attach）

一组过滤规则若是没有附加到任何端口，那么这组规则并不能运行。请使用 Filter Attach 页面来将过滤规则附加到交换机的传入端口。

点击 OK 保存设置。要使设置生效，请至 Save Configuration 页面，然后点击 Save，或者点击 Reload 更新页面。

您可以用下列方法将过滤规则附加到端口：

Attach to all ports: 应用过滤规则至系统中所有的端口。

Attach to certain ports: 应用过滤规则至指定的端口。

Detach from all ports: 将原有已应用过滤规则的端口取消应用规则。

使用"Attach All"命令过后，您将无法删除指定的端口的过滤规则。若您需要删除规则，请使用"Detach All"命令。

当过滤规则应用到传入端口，该规则会根据传入端口和规则中的封包范围来过滤封包。例如，某过滤规则附加于传入端口 3，仅过滤目的地 MAC 地址为 00:10:20:30:40:50 的封包。则来自端口 3 且目的地 MAC 地址为 00:10:20:30:40:50 的封包将不会被传送。

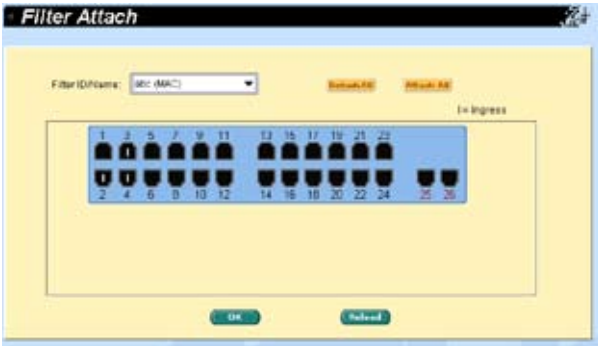


图 45. 附加过滤规则

4.8 安全（Security）

本交换机支持 802.1x 以端口为基础的安全功能。只有经认证的主机才可以访问本交换机的端口。来自未经认证之主机的流量将被阻塞。认证服务可由 RADIUS 服务器或交换机的本地数据库提供。

本交换机亦支持通过 802.1x 认证的动态 VLAN 分配。关于用户／端口的信息必须在开启本功能之前，在认证服务器上进行设置。

4.8.1 端口访问控制（Port access control）

端口访问控制（Port Access Control）可用来设置 802.1x 参数。802.1x 使用 RADIUS 服务器或本地数据库来认证端口的用户。

第一部分是桥接(Global)设置：

Sys-Auth-Control: 选择本项目开启认证

Authentication Method: RADIUS 或本地数据库可用来认证端口的用户。

第二部分为端口设置。当您完成修改后，请点击 Modify：

Port: 从端口列表窗口中选择需要设置的端口。

Host Mode (Single-host/Multi-host): 若开启了本项目，连接到选定端口的所有主机中，只要有一部主机通过了认证，则所有主机都允许使用这个端口。若关闭本项目，则只有通过认证的那部主机可以使用这个端口。

Authentication Control: 若选择了“ForceAuthorized”，选定的端口被认为已强制通过认证。因此，来自所有主机的流量都被允许通过。否则，若选择了“ForceUnauthorized”，选定的端口是阻塞的，不允许任何流量通过。 若选择了“Auto”，选定端口的动作由 802.1x 协议来控制。在正常情况下，所有的端口都应该设置为“Auto”。

Reauthentication: 开启本项目后，交换机会在重新认证时间(ReAuthentication Time）到时，试图重新认证端口的用户。

ReAuthentication Time: 若“Reauthentication” 项目已开启，ReAuthentication Time（重新认证时间）指的是交换机重新发送认证请求到端口用户的时间间隔。

Quiet Period: 若认证失败，交换机再次发送认证请求到端口用户前需要等待的时间。

Guest Vlan: 指定一个访客（Guest）VLAN 给不兼容于 802.1x 的客户端。

点击 OK 永久保存设置。点击 Reload 更新设置至当前值。

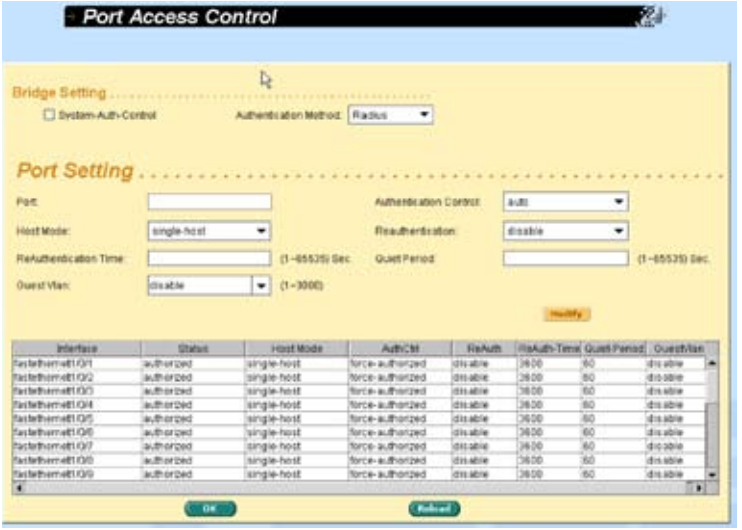

Port Access Control
Bridge Setting
System-Auth-Control
Authentication Method:
Radius
Port Setting
Port:
Authentication Control:
auto
Host Mode:
single-host
Reauthentication:
disable
ReAuthentication Time:
(1~65535) Sec.
Quiet Period:
(1~65535) Sec.
Guest Vlan:
disable
(1~3000)
Interface
Status
Host Mode
AuthCtl
ReAuth
ReAuth-Time
Quiet Period
GuestVlan
OK
Reload

图 46. 端口访问控制

4.8.2 拨入用户（Dial-in user）

拨入用户（Dial-in User）选项用来定义交换机本地数据库中的用户。

User Name: 新的用户名称。

Password: 新用户的密码。

Confirm Password: 再次输入密码。

Vlan ID: 为 802.1x 认证的用户端指定 VLAN ID。

请点击 Add 来新增用户。当您完成修改后，点击 Modify。若您想要删除选定的用户，请点击 Remove 。点击 OK 永久保存设置。点击 Reload 更新设置至当前值。

图 47. 拨入用户

4.8.3 RADIUS

若要使用外部 RADIUS 服务器，您需要设置以下参数：

Authentication Primary-Server IP: RADIUS 服务器的 IP 地址。

Authentication Primary-Server Port: RADIUS 服务器侦听的端口端口号。

Authentication Primary-Server Key: 用于在 GigaX 与 RADIUS 服务器之间进行通讯的密钥。

Confirm Authentication Key: 再次输入上述密码。

连接至交换机之 RADIUS 服务器必须与系统管理端口位于同一个 VLAN 内。

点击 OK 永久保存设置。点击 Reload 更新设置至当前值。

图 48. RADIUS

4.8.4 端口安全（Port security）

本交换机也支持端口安全（Port security）功能。它允许系统管理员来控制哪些用户可以连接到他们的网络。您可以使用端口安全功能来限制和指定可访问该端口的站点的 MAC 地址，从而限制端口的输入量。当您指定了一个安全端口的安全 MAC 地址后，该端口将不会转发除了已定义的来源地址群组之外的任何封包。这样就降低了未经认证的设备使用我们的网络进行恶意行为的可能性。

4.8.4.1 端口设置（Port configuration）

本页面用来进行端口安全设置。

首先，您必须从显示列表中点击一个端口。然后，开始进行端口设置。修改完成后点击 Modify：

a) Admin: 开启或关闭端口安全功能。

b) Violation Mode: 本项用来设置当违反安全设置时端口的动作。若选择“Shutdown”，端口将变成阻塞状态，系统将记录信息，Violation 计数器的数值会增加。若选择“Restrict”，系统将会记录信息，Violation 计数器的数值会增加。若选择“Protect ,当有违反安全设置的事件发生时 ,您将不会被通知。

c) Max MAC Address: 在这个端口上安全 MAC 地址的最大数量。有效设置数值是由 1 至 132，系统中的总数为 1024。

d) Aging Time: 端口上安全 MAC 地址的老化时间。超过了这段时间后，相应的动态安全 MAC 地址就从安全 MAC 地址表中删除。有效的设置范围是由 0 至 1440(mins)。若设置的时间为 0，则该端口的老化时间机制没有开启。

e) Aging Type: 老化类型决定了当安全 MAC 地址老化后的动作。若选择“Absolute”,端口的安全地址在老化时间到后会被删除。若选择“Inactivity”，若在指定的时间内没有来自该安全 MAC 地址的流量，则该地址才会被删除。

点击 OK 永久保存设置。点击 Reload 更新设置至当前值。

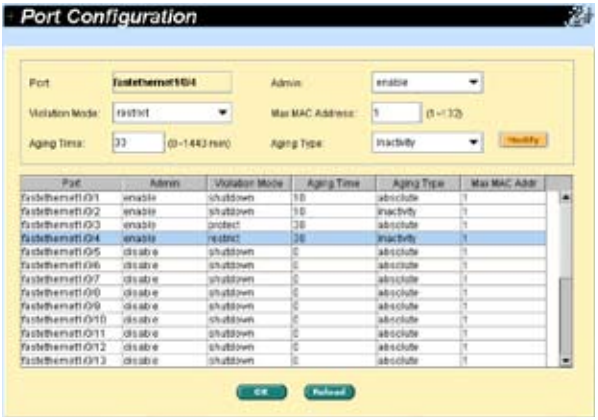


图 49. 端口安全设置

4.8.4.2 端口状态（Port status）

本页面显示了当前的端口状态，MAC 地址数量，静态 MAC 地址数量，以及违反安全设置的事件数量。

端口有五种状态：

a) NoOper: 表示端口的安全功能没有开启。

b) SecureUp: 表示端口安全功能运行中。

c) SecureDown: 表示端口的安全功能无法运行。这种状况一般为开启了端口安全功能，但由于某些原因（如与其他功能冲突）而无法正常运行。

d) Restrict: 表示在 Violatioon mode 设置为"restrict”时，端口出现了违反安全设置的状况。

e) Shutdown: 表示在 Violatioon mode 设置为"Shutdown”时，端口出现了违反安全设置的状况。

若某些端口状态为“Shutdown”，您可以点击它并选择“Re-Start”为“Yes”。这将重新启用端口并将其状态改为“SecureUp”。当您修改完成后，请点击 Modify。

点击 OK 永久保存设置。点击 Reload 更新设置至当前值。

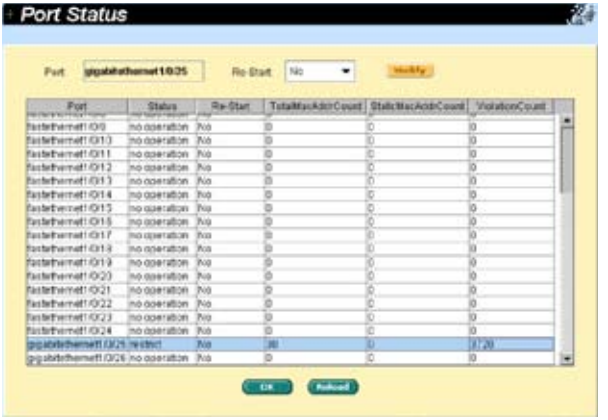


图 50. 端口状态

4.8.4.3 安全 MAC 地址（Secure MAC address）

安全 MAC 地址（Secure MAC Address）提供了三种管理功能：

a) Query: 您可以在“Port Selection”栏位选择一个端口。点击 Query 按钮后，将显示该端口的所有 MAC 地址。

b) Add: 用户可以在“Port Selection”栏位选择一个端口，然后在“MAC Address”栏位输入一个 MAC 地址，并点击 Add 按钮，即可将该地址添加至端口。新增的地址为静态 MAC 地址。

c) Remove: 您可以使用“Query”功能来显示某联接端口上的所有 MAC 地址。从列表中选择一个 MAC 地址并按下 Remove 按钮，即可立刻删除该地址。

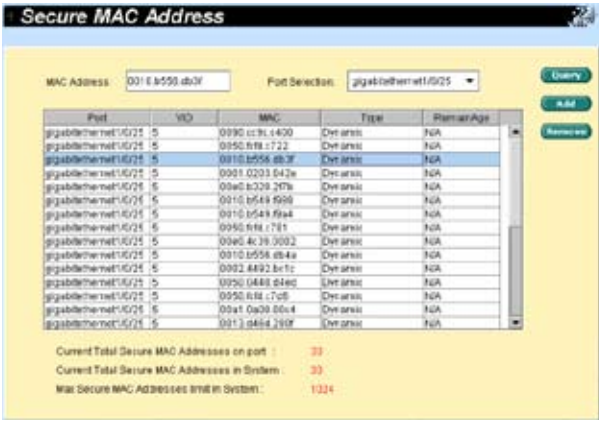


图 51. 安全 MAC 地址

4.9 流量统计图表（Traffic chart）

流量统计图表（Traffic Chart）页面可以在不同的图表中显示网络流量。您可以指定更新统计图表的时间间隔。在这些页面中，您可以利用不同图表来监控网络流量。大多数 MIB-II 计数器都被显示在这些图表中。

点击 Auto Refresh 或 Refresh Rate 来设置从交换机更新数据的时间间隔。您可以选择不同的颜色（Color）来区分不同的端口或统计值。最后，点击 Draw 使浏览器产生统计图表。每次点击 Draw 都会重置统计结果的显示。

4.9.1 流量比较（Traffic comparison）

本页面可将所有端口的某一个统计值显示在同一张图表中。指定一个统计项目，并按下 Draw，浏览器将显示更新的数据，并每隔一段时间更新一次。

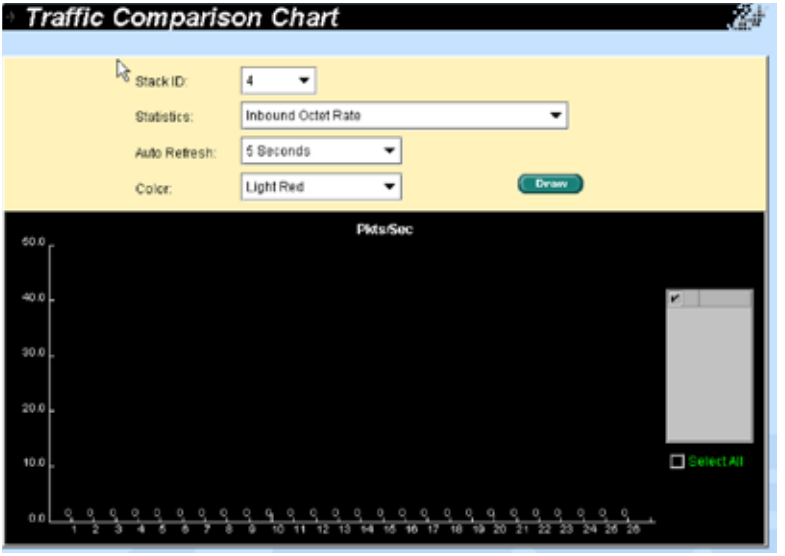


图 52. 流量比较

4.9.2 错误群组（Error group chart）

选择端口和显示颜色（Color），然后点击 Draw，统计窗口将显示指定端口所有丢弃或错误的数量。这个数据每隔一段时间会自动更新。

图 53. 错误群组

4.9.3 历史状态（Historical status）

您可以在这个图表中显示不同的端口和统计项目。由于这里显示的是统计信息的历史状态，因此，即使数据已更新，统计线条图仍然会保留旧的统计数据。

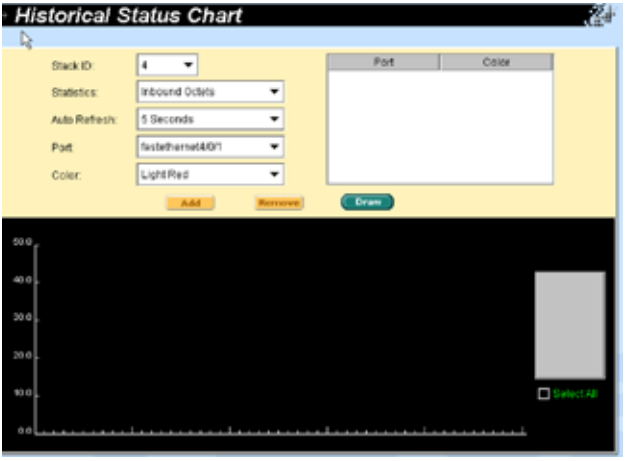


图 54. 历史状态

4.10 线缆诊断（Cable diagnosis）

本功能可以用来分析一般的线缆问题，如开路、短路和阻抗不匹配。

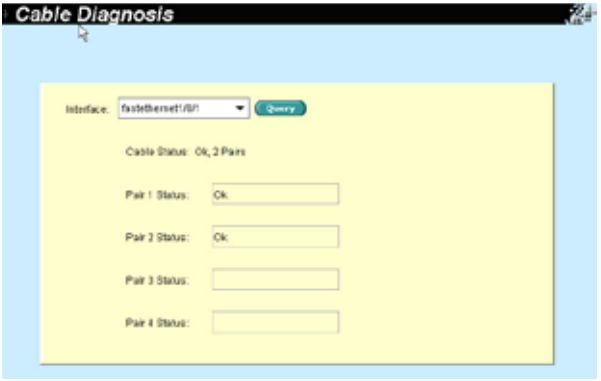


图 55. 线缆诊断

4.11 管理交换机的堆叠

本章节仅适用于带有 Stack 卡的 GigaX2024M 交换机。

交换机堆叠指的是一组（最多8部）GigaX2024M 交换机通过它们的堆叠（Stacking） 端口连接到一起。其中一部交换机控制这组堆叠交换机的运行，称为主机(Master)。卡上的 LED 面板将显示“A.x”，这里的 x 代表堆叠（Stack）ID。堆叠中其他的交换机被称为从机（Slave），卡上的 LED 面板将显示“P.x”。堆叠的成员协同运行，组成一个统一的系统。

所有的堆叠成员都可以成为主机（Master）。若堆叠主机变为不可用，其他的堆叠成员会从它们中间选出一个新的堆叠主机。拥有最高优先级（1为最高优先级）的交换机将成为新的主机。若优先级相同，则具有较低桥接 ID 的交换机将成为主机。要建立一个堆叠系统，请先将它们连接起来并一起开启电源。

点击 Reload 更新堆叠系统。

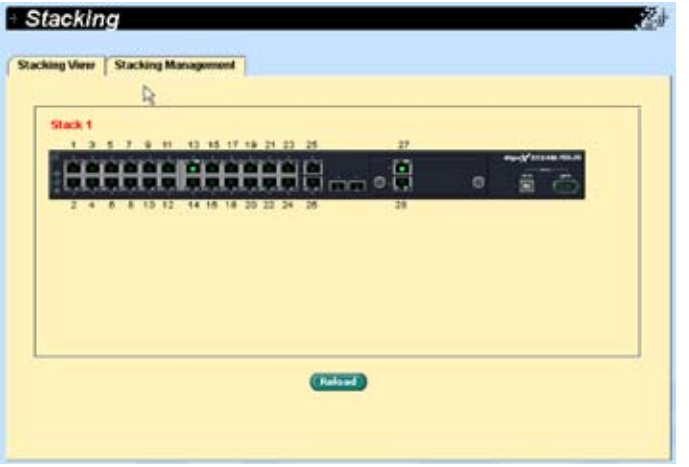


图 60. 堆叠管理

您可以通过堆叠管理（Stacking Management）页面设置堆叠（Stack）ID与优先级。但您不可以在堆叠系统建立后再设置堆叠（Stack）ID与优先级。您必须在建立系统前进行这些设置。

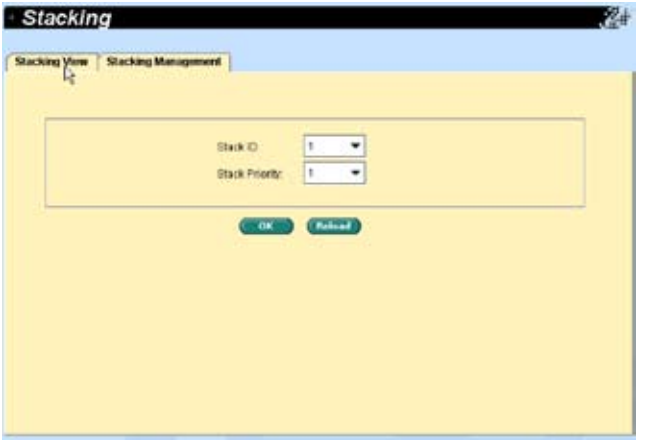


图 61. 堆叠

1. *若您没有指定交换机的堆叠 ID，那此交换机必须最后一个加入堆叠系统。*
2. *当系统自动选择主机失败或无法执行，请重新启动所有交换机。*
3. *我们强烈建议您为交换机指定堆叠 ID。虽然系统将自动指定一个堆叠 ID 给交换机，但仍然会存在一些潜在的问题。*
4. *当您删除然后又增加一个堆叠成员（非主机）时，若新加入的交换机与删除的那部具有相同的堆叠 ID，堆叠系统将自动按照旧的那部交换机的设置来设置新交换机。*

4.12 保存配置（Save configuration）

要永久保存设置，您需要点击 Save 按钮。在成功地保存设置后，此设置即开始生效。

若您希望重置交换机的设置，可以点击 Restore 按钮将设置恢复至出厂默认值。当然，重置设置后，系统将会重新启动。

恢复出厂默认值后，您做的所有设置都将丢失。

图 56. 保存配置

5 控制终端界面（Console interface）

本章节将会介绍如何使用控制终端界面来设置交换机。本交换机提供 RS232 与 USB 端口来与您的 PC 相连接。您的 PC 需要运行终端模拟软件，如 HyperTerminal，以及命令翻译器来对交换机进行设置。您必须将终端模拟软件的波特率设为 9600，8 个数据位，无奇偶校验，1 个停止位，无流量控制。

当您进入 CLI 模式后，输入“?”将显示所有可用的命令帮助信息。若您对于 CLI 命令不熟悉，这将是非常有用的信息。所有的 CLI 命令都区分大小写。

5.1 开机自检（Power-on self test）

POST（开机自检）是在系统启动时进行的。它测试系统内存、LED 指示灯与交换机主板上的硬件芯片。系统测试和初始化完成之后会显示系统信息。您可以忽略这些信息直到出现“ASUS>:”提示符。

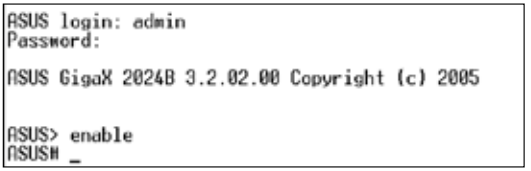


图 57. CLI 界面

5.1.1 Boot ROM 命令模式

在 POST 过程中，您可以按下 <ENTER> 键来进入“Boot ROM Command”模式。输入“?”可显示所有可用命令的帮助信息。

尽管这些命令在有些情况下相当有用，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它们。

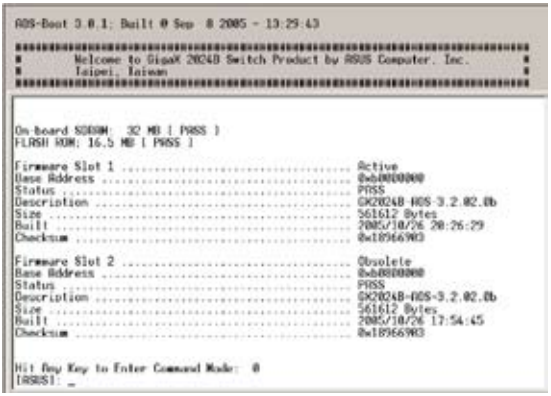


图 58. Boot ROM 命令模式

5.1.2 Boot ROM 命令

以下为 Boot ROM 命令的两种类型：

- command: 显示当前设置。
- command with new setting: 用指定的新设置代替当前设置。

命令	参数	参数举例	说明
baudrate	Baud rate	9600, 38400, 57600, 115200	您需要将终端模拟软件设为相同的波特率。
ethaddr	none	none	取得 MAC 地址
gatewayip	IP address	xxx.xxx.xxx.xxx	设置网关的 IP 地址
go	none	none	启动固件映像
? or help	none	none	显示在线帮助
ipaddr	IP address	xxx.xxx.xxx.xxx	设置 TFTP 客户端的 IP 地址
xload	none	none	载入二进制文件 load binary file over serial line (X modem)
netmask	mask	xxx.xxx.xxx.xxx	设置网络掩码
ping	host	xxx.xxx.xxx.xxx	传送 ICMP echo_request 至主机
pwd	none	none	重置交换机密码
serverip	IP address	xxx.xxx.xxx.xxx	设置 TFTP 服务器 IP 地址
slot	slot	1, 2, auto	选择启动槽区
tftpboot	filename	xxx.img	搭配 TFTP 通过网络载入固件映像
version	none	none	显示版本号

5.2 登录与登出

要进入 CLI 模式，您需要输入一个有效的用户名与密码。首次登录时，您可以输入“admin”作为用户名（无需输入密码）。为了安全考虑，请在登录后修改用户名与密码。若您忘记了用户名和密码，您可以联系华硕技术支持部门，或使用 Boot ROM 命令模式中的“pwd”命令来将用户帐号恢复至缺省值。若您选择第二种方法，用户名将恢复为“admin”。

输入“exit”可安全地离开 CLI 模式。这个动作可在您离开的同时确保系统的安全。下一个用户需要输入经认证的用户名与密码才能登录。

5.3 CLI 命令

本交换机提供了一系列 CLI 命令，用于所有的管理功能。这样，您可以根据提示，如同使用网页界面一样方便正确地进行交换机的设置。

使用“?”或“list”来取得可用的命令与帮助。

使用“end”可返回根目录（enable 模式）。

5.3.1 用户帐号（User account）

5.3.1.1 新增用户（add user）

新增用户或修改既有用户的密码。

CLI **命令：**add user user-name password

举例：ASUS# user add admin 123

5.3.1.2 删除用户（delete user）

删除一个既有的用户。

CLI **命令：**user delete user-name

举例：ASUS# user delete admin

5.3.2 备份与恢复（Backup and Restore）

5.3.2.1 备份启动配置文件（Backup start-up configuration file）

备份交换机的启动配置文件“startup_config”至 TFTP 服务器。

CLI 命令：copy startup-config tftp: URL

举例：ASUS# copy startup-config tftp: 192.168.8.56/gx2024b.cfg

5.3.2.2 恢复启动配置文件（Restore start-up configuration file）

从 TFTP 服务器上恢复交换机的启动配置文件“startup_config”。

CLI 命令：copy tftp: URL startup-config

举例：ASUS# copy tftp: 192.168.1.2/gx2024b.cfg startup-config

5.3.3 系统管理设置（System management configuration）

5.3.3.1 固件升级（Firmware upgrade）

升级新的固件至交换机。

CLI 命令：archive download-sw/overwrite tftp: ImageFile

举例：ASUS# archive download-sw/overwrite tftp: 192.168.1.3/GX2024B-3.2.02.00-release.img

5.3.3.2 配置终端（configure terminal）

进入设置模式来配置终端。

CLI 命令：configure terminal

举例：ASUS# configure terminal

5.3.3.3 启用（enable）

进入启用（enable）模式并开启特权模式命令。

CLI 命令：enable

举例：ASUS# enable

5.3.3.4 禁用（disable）

关闭特权模式并返回用户模式。

CLI 命令：disable

举例：ASUS# disable

5.3.3.5 结束（end）

本命令可让用户结束当前模式并进入启用（enable）模式。

CLI **命令：**end

举例：ASUS# end

5.3.3.6 离开（exit）

本命令可让用户离开当前模式而进入前入一个模式。

CLI **命令：**exit

举例：ASUS# exit

5.3.3.7 列出（list）

本命令行出了操作模式下所有的命令。

CLI **命令：**list

举例：ASUS# list

举例：ASUS# ?

5.3.3.8 主机名称（host name）

显示交换机的名称。这是 RFC-1213 定义的系统群组（System Group）中的 MIB 项目，在管理节点上提供管理信息。

CLI **命令：**hostname WORD

举例：(config)# hostname Switch

若您在名称描述栏位内输入了名称，则交换机系统名称将改为新设的名称。

5.3.3.9 系统联系信息（System contact）

显示交换机的详细联系信息。这是 RFC-1213 定义的系统群组（System Group）中的 MIB 项目，在管理节点上提供联系信息。

CLI **命令：**snmp-server contact DWORD

举例：(config)# snmp-server contact fae@loop.com.tw

若您在若联系信息描述栏位内输入了联系信息，则交换机的联系信息将改为新设的内容。

5.3.3.10 系统位置（System Location）

显示交换机的物理位置。这是 RFC-1213 定义的系统群组（System Group）中的 MIB 项目，在管理节点上提供位置信息。

CLI 命令：snmp-server location DWORD

举例：(config)# snmp-server location Loop-Taipei

在位置描述栏位内输入位置描述信息即可修改位置信息。

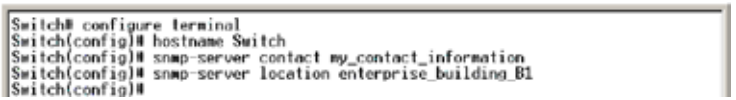


图 59. 系统命令

5.3.3.11 IP 地址与网络掩码（IP address and network mask）

显示交换机的 IP 地址。这个地址用于管理用途，如交换机的 http 服务器、SNMP 服务器、TFTP 服务器、SSH 与 Telnet 服务器等网络应用在 VLAN1 界面中都使用这个 IP 地址。

CLI 命令：ip address A.B.C.D/M

举例：(config)# interface vlan 1

(config-if)# ip address 192.168.20.121/24

5.3.3.12 默认网关（Default gateway）

显示默认网关的 IP 地址。若交换机所在的网络包含一个或多个路由器，则本项目必须设置。

CLI 命令：ip route A.B.C.D/M (A.B.C.D|INTERFACE)

举例：(config)# ip route 0.0.0.0/0 192.168.1.2

5.3.3.13 重新启动（reboot）

使用本命令来重新启动系统。

CLI 命令：reboot

举例：reboot

5.3.3.14 载入预设文件（reload default-config file）

这个命令用预设的配置文件来取代当前配置文件。

CLI 命令：reload default-config file

举例：ASUS# reload default-config file

5.3.3.15 显示运行配置（show running-config）

显示运行配置。

CLI 命令：show running-config

举例：ASUS# show running-config

5.3.3.16 写入（write）

在堆叠或单一的交换机上用写入文件设置命令来将设置写入到交换机设置文件。

CLI 命令：write

举例：ASUS# write

5.3.3.17 指定一个新的用户帐号（Assign a new user account）

如：新增一个用户，名称为 tony，密码为 tony123456。

CLI 命令：user add WORD WORD

举例： user add tony tony123456

5.3.3.18 删除一个用户帐号（Delete a new user account）

如：删除一个名称为 tony 的帐号。

CLI 命令：user delete WORD

举例： user delete tony

5.3.4 物理界面命令（Physical interface commands）

5.3.4.1 端口模式（Interface mode）

在交换机上使用自动协商（auto-negotiation）设置命令来设置端口的自动协商状态。

CLI 命令: auto-negotiation

举例：(config)# interface fa1/0/2

(config-if)# auto-negotiation

这个例子说明了如何使用交换机的自动协商设置命令来开启自动协商模式。

5.3.4.2 端口双工模式（Interface duplex）

使用交换机的双工设置命令来设置连接端口的双工状态。

CLI 命令：duplex (full| half)

举例：(config)# interface fa1/0/2

(config-if)# duplex full

这个例子说明了如何使用交换机的双工设置命令来设置端口的全双工模式。

5.3.4.3 端口流量控制（Interface flow control）

使用交换机的流量控制设置命令来设置端口的流量控制状态。

CLI 命令：flowcontrol (rx| tx | both)

举例：(config)# interface fa1/0/2

(config-if)# flowcontrol both

这个例子说明了如何使用交换机的流量控制设置命令来设置端口的流量控制。

5.3.4.4 显示二层界面（Show L2 interface）

使用交换机的显示端口命令来显示界面状态。

CLI 命令：show interfaces IFNAME

举例：ASUS# show interface fa1/0/2

5.3.5 IP 界面（IP interface）

5.3.5.1 显示 VLAN 名称字符串（show vlan name string）

用显示 VLAN 用户 EXEC 命令来显示交换机上已设置的所有 VLAN 或一个 VLAN（若 VLAN ID 或名称已指定）的参数。

CLI 命令：show vlan name string

举例： ASUS# show vlan name VLAN1

VLAN 1 是用于系统用途，例如，用于固件升级，管理，等等。

5.3.5.2 建立一个 VLAN 项目（Create a vlan entry）

使用 vlan vid 命令在交换机上建立 VLAN 项目。使用名称字符串（name string）命令来建立一个带名称的 VLAN 项目。

CLI 命令：vlan id

举例：（config)# vlan 3

（config-vlan)# name vlan3

5.3.5.3 VLAN 界面命令模式（interface vlan VLAN-ID）

本命令用来将操作更改为 VLAN 界面命令模式。

CLI 命令：interface vlan VLAN-ID

举例： interface vlan 1

5.3.5.4 IP 地址（ip address）

本命令用来设置指定端口的 IP 地址。

CLI 命令：ip address A.B.C.D/M

举例：（config-if)# ip address 192.168.20.121/24

端口的名称在设置过程中不会被显示。请在设置过程中记住您要设置的内容。

5.3.5.5 DHCP 客户端模式（ip dhcp client）

本命令用来设置系统端口通过 DHCP 服务器取得 IP 地址。

CLI 命令：ip dhcp client

举例：(config-if)#ip dhcp client

5.3.5.6 IP 路由（ip route）

本命令用来在系统中设置 IP 路由。

CLI 命令：ip route A.B.C.D A.B.C.D (A.B.C.D|INTERFACE)

举例：(config)# ip route 192.168.20.0 255.255.255.0 192.168.20.1

5.3.6 生成树（Spanning Tree）

5.3.6.1 显示生成树摘要（show spanning-tree summary）

显示目前的生成树。

GigaX2024B:

CLI 命令：aggregation-link group <1-6> IFLIST

举例：ASUS(config)#aggregation-link group 1 fa1/0/1-3

GigaX2024M:

CLI 命令：aggregation-link group <1-8> IFLIST

举例：ASUS(config)#aggregation-link group 1 fa1/0/1-3

5.3.6.2 生成树的启用与禁用（spanning-tree enable and disable）

启用／禁用生成树。

CLI 命令：spanning-tree (enable|disable)

举例： ASUS# spanning-tree disable

5.3.7 链路汇聚（Link aggregation）

5.3.7.1 中继汇聚群组（trunk aggregation group）

使用交换机的链路汇聚中继群组设置命令来设置中继汇聚群组。

CLI 命令：aggregation-link group <1-6> IFLIST

举例：ASUS(config)#aggregation-link group 1 fa1/0/1-3

5.3.7.2 中继负载均衡（trunk load balancing）

使用交换机的链路汇聚中继群组命令，用基于来源地址或基于目的地地址的转发方式来设置中继负载均衡。

GigaX2024B:

CLI 命令：aggregation-link group <1-6> load-balance (src-mac |dst-mac |src-dst-mac |src-ip |dst-ip |src-dst-ip)

举例：ASUS(config)#aggregation-link group 1 load-balance src-mac

GigaX2024M:

CLI 命令：aggregation-link group <1-8> load-balance (src-mac |dst-mac |src-dst-mac |src-ip |dst-ip |src-dst-ip)

举例：ASUS(config)#aggregation-link group 1 load-balance src-mac

5.3.7.3 显示链路汇聚中继（show aggregation-link trunk）

显示链路汇聚中继状态。

CLI 命令：show aggregation-link group [GROUPID]

举例： ASUS# show aggregation-link group 1

5.3.8 LACP

5.3.8.1 LACP 链路汇聚中继（lacp aggregation-link trunk）

本命令用来进行链路汇聚控制协议(LACP)新增／设置交换机上的中继群组端口的操作。

GigaX2024B:

CLI 命令：lacp aggregation-link group <1-6> (add|set) IFLIST

举例：ASUS(config)# lacp aggregation-link group1 add fa1/0/1-3

GigaX2024M:

CLI 命令：lacp aggregation-link group <1-8> (add|set) IFLIST

举例：ASUS(config)# lacp aggregation-link group1 add fa1/0/1-3

5.3.8.2 禁用 LACP 链路汇聚中继（disable lacp aggregation-link trunk）

本命令用来进行链路汇聚控制协议(LACP)新增／设置或禁用交换机上的中继群组端口的操作。

GigaX2024B:

CLI 命令：no lacp aggregation-link group <1-6>

举例：ASUS(config)# no lacp aggregation-link group 1

GigaX2024M:

CLI 命令：no lacp aggregation-link group <1-8>

举例：ASUS(config)# no lacp aggregation-link group 1

5.3.8.3 LACP 系统优先级（lacp system-priority）

本命令为交换机上的链路汇聚控制协议(LACP)设置系统优先级。

CLI 命令：lacp system-priority <1-65535>

举例：(config)# lacp system-priority 20000

5.3.9 镜像（Mirroring）

5.3.9.1 镜像设置（Mirror setting）

使用 "Mirror Session" 命令，您可以将来源端口列表中的流量镜像至目的端口。镜像类型支持接收流量、传送流量或两者兼有。

CLI **命令：** mirror session 1 source IFLIST (both/ rx/ tx)

mirror session 1 destination IFNAME

举例： (config)# mirror session 1 source fa1/0/1-4 both

(config)# mirror session 1 destination fa1/0/5

5.3.9.2 显示镜像（show mirror）

显示当前的镜像功能。

CLI **命令：** Show mirror session

举例： ASUS# show mirror session

5.3.9.3 无镜像（no mirror）

本命令用来关闭镜像功能。

CLI **命令：** no mirror session 1

举例： (config)# no mirror session 1

5.3.9.4 无镜像（no mirror）

本命令用来重置来源端口接收或传送的流量或两者至目的端口。

CLI **命令：** no mirror session 1 source IFLIST

举例： (config)# no mirror session 1 source fa1/01/1-2

5.3.10 静态组播（Static Multicast）

5.3.10.1 MAC 地址表组播（mac-address-table multicast）

使用交换机的 MAC 地址表组播（mac-address-table multicast）设置命令来将组播地址新增至 MAC 地址表。

CLI **命令：** mac-address-table multicast MACADDR VLANID IFLIST

举例： (config)# mac-address-table multicast 0100.5e11.1111 2 fa1/0/1-3

5.3.10.2 无 MAC 地址表组播（no mac-address-table multicast）

使用无 MAC 地址表组播（no mac-address-table multicast） 设置命令来删除 MAC 地址表中的组播静态地址。

CLI 命令：no mac-address-table multicast MACADDR VLANID IFLIST

举 例：（config)# no mac-address-table multicast 0100.5e11.1111 2 fa1/0/1-3

5.3.10.3 显示 MAC 地址表组播（show mac-address-table multicast）

使用显示 MAC 地址表组播（show mac-address-table multicast）用户 EXEC 命令来显示所有 VLAN 的二层组播项目。在特权 EXEC 模式下用这个命令可显示指定的组播项目。

CLI 命令：show mac-address-table multicast

举例：ASUS# show mac-address-table multicast

5.3.11 IGMP 侦听（IGMP snooping）

5.3.11.1 IP IGMP 侦听（ip igmp snooping）

本命令用来完整开启 IGMP 侦听功能。

CLI 命令：ip igmp snooping

举例：（config)# ip igmp snooping

5.3.11.2 间隔时间（interval time）

本命令用来设置交换机传送 IGMP 询问的间隔时间。

CLI 命令：ip igmp snooping last-member-query-interval TIMEVALUE

举例：（config)# ip igmp snooping last-member-query-interval 100

5.3.12 流量控制（Traffic control）

5.3.12.1 风暴控制（storm-control）

在使用交换机的风暴控制（storm-control）设置命令来限制端口用于广播／ dlf ／组播的总带宽的传输速率。GX2024B 风暴控制功能位于 Configure Terminal 模式。它是一个全局的功能，应用于整部交换机。GX2024M 的风暴控制功能位于 Interface 模式。其功能设置是针对每个端口的。以下是 GigaX2024B 的命令举例：

CLI 命令：storm-control (broadcast|dlf|multicast) LIMIT_RATE

举例：（config)# storm-control broadcast 25

5.3.12.2 无风暴控制（no storm-control）

使用交换机的无风暴控制（no storm-control）设置命令来关闭对端口用于广播／dlf ／组播的总带宽的速率限制。

CLI 命令：no storm-control (broadcast|dlf|multicast)

举例：(config-if)# no storm-control broadcast

5.3.12.3 显示风暴控制（show storm-control）

使用交换机的显示风暴控制（show storm-control）设置命令来显示对端口用于广播／ dlf ／组播的总带宽的速率限制。

CLI 命令：show storm-control (broadcast|dlf|multicast)

举例： ASUS# show storm-control broadcast

5.3.13 动态地址（Dynamic addresses）

5.3.13.1 清除动态 MAC 地址（clear dynamic mac-address）

使用交换机的以下命令在数据库中清除动态二层 MAC 地址。

CLI 命令：clear mac-address-table dynamic mac MAC_ADDR

举例：(config)# clear mac-address-table dynamic mac 0000.1111.2222

5.3.13.2 老化时间（aging time）

在一组堆叠或单独的交换机上使用 MAC 地址表老化时间（mac-address-table aging-time）设置命令可设置动态地址在使用或更新后仍然存在于 MAC 地址表中的时间。真正的老化时间是您设置数字的三倍。

CLI 命令：mac-address-table aging-time <10-1000000>

举例：(config)# mac-address-table aging-time 100

这个例子说明了如何将 MAC 地址表的老化时间设置为 300 秒。

5.3.13.3 无老化时间（no aging time）

关闭 MAC 地址表的老化功能。

CLI 命令：no mac-address-table aging-time

举例：(config)# no mac-address-table aging-time

5.3.13.4 显示 MAC 地址表老化时间

(show mac-address-table aging-time)

CLI 命令：show mac-address-table aging-time

举例： ASUS# show mac-address-table aging-time

5.3.14 静态地址（Static addresses）

5.3.14.1 新增静态 MAC 地址（add static mac-address）

您可以新增 MAC 地址到交换机的 MAC 地址表中。通过这种方式新增的 MAC 地址将不会从地址表中老化。我们称之为静态地址。

CLI 命令：mac-address-table static MAC_ADDR VLANID IFNAME

举例：(config)# mac-address-table static 0000.1111.2222 1 fa1/0/2

5.3.14.2 显示 MAC 地址表（show mac-address-table）

显示静态与动态 MAC 地址。

CLI 命令：show mac-address-table

举例： ASUS# show mac-address-table

5.3.15 VLAN

5.3.15.1 显示 VLAN 名称字符串（show vlan name string）

使用交换机的显示 VLAN 用户 EXEC 命令来显示所有设置的 VLAN 或单一 VLAN（若指定 VLAN ID 或名称）的参数。

CLI 命令：show vlan name string

举例： ASUS# show vlan name VLAN1

5.3.15.2 建立 VLAN（vlan vid）

使用 vlan vid 命令在交换机上建立 VLAN 项目。

CLI 命令：vlan vid

举例：(config)# vlan 2

5.3.15.3 名称字符串（name string）

使用名称字符串（name string）命令在交换机上建立带名称的 VLAN 项目。

CLI 命令：name string

举例：(config-vlan)# name VLAN2

5.3.15.4 访问 VLAN（access vlan）

设置所有端口的访问模式特征及设置虚拟局域网。

CLI 命令：switchport access vlan <1-3000>

举例：(config)# interface fa1/0/2

(config-if)# switchport access vlan 1

5.3.15.5 许可的 VLAN（allowed VLANs）

使用交换机端口的中继许可 VLAN（allowed vlan）设置命令来新增或删除许可 VLAN，许可 VLAN 在中继模式下可在此端口以标记形式接收和传送流量。

CLI 命令：switchport trunk allowed vlan (add|remove) VLANLIST

举例：(config)# interface fa1/0/2

(config-if)# switchport trunk allowed vlan add 1-10

5.3.16 GVRP

5.3.16.1 清除 GVRP 统计数据（clear gvrp statistics）

使用交换机的清除 GVRP 统计数据（clear gvrp statistics）设置命令来清除一个或多个端口的所有 GVRP 统计数据。

CLI 命令：clear gvrp statistics [IFNAME]

举例：ASUS# clear gvrp statistics fa1/0/2

5.3.16.2 GVRP 模式（gvrp mode）

本命令可完整开启或关闭交换机的 GVRP 功能。

CLI 命令：gvrp (enable|disable)

举例：ASUS# gvrp enable

5.3.16.3 显示 GVRP 配置（show gvrp configuration）

显示 GVRP 设置状态。

CLI 命令：show gvrp interface IFNAME

举例：ASUS# show gvrp interface fa1/0/1

5.3.16.4 显示 GVRP 统计数据（show gvrp statistics）

显示 GVRP 统计数据的状态。

CLI 命令：show gvrp statistics [IFNAME]

举例：ASUS# show gvrp statistics fa1/0/1

5.3.17 CoS/QoS

5.3.17.1 排列 CoS 映射（queue cos-map）

使用交换机的排列 CoS 映射（queue cos-map）设置命令来设置 CoS 队列的优先级顺序。

CLI 命令：cos cos-map PRIORITY QUEUE

举例：ASUS# cos cos-map 3 3

5.3.17.2 显示排列 CoS 映射（show queue cos-map）

本命令用来将 GVRP 设置恢复为缺省值。

CLI 命令：show cos cos-map

举例：(config)# show cos cos-map

5.3.17.3 QoS 模式（qos mode）

本命令用来设置 QoS 模式。

CLI 命令：cos policy (fifo/ strict/ wrr-queue)

舉例：(config)# cos policy fifo

5.3.17.4 显示 CoS 策略（show cos policy）

本命令显示 CoS 策略。

CLI 命令：show cos policy

举例：(config)# show cos policy

5.3.17.5 QoS 传入带宽（qos ingress bandwidth）

本命令用来设置传入封包的 QoS 带宽信息参数。

CLI 命令：qos ingress bandwidth LIMIT_RATE BURST_RATE

举例：(config)# interface fa1/0/2

(config-if)# qos ingress bandwidth 10

5.3.18 SNMP

5.3.18.1 显示 RMON 统计数据（show rmon statistics）

显示 RMON 统计数据状态。

CLI 命令：show rmon statistics [IFNAME]

举例：ASUS# show rmon statistics fa1/0/1

5.3.18.2 显示 SNMP 服务器群组（show snmp-server community）

显示 SNMP 服务器群组。

CLI 命令：show snmp-server community

举例：ASUS# show snmp-server community

5.3.18.3 SNMP 服务器主机（snmp-server host）

本命令用来设置 SNMP 主机信息。

CLI 命令：snmp-server host A.B.C.D

举例：(config)# snmp-server host 192.168.8.31

5.3.19 过滤（Filter）

5.3.19.1 拒绝任何主机（deny any host）

使用交换机的拒绝 MAC 访问列表（deny MAC access list）设置命令来防止符合条件的非 IP 流量被传送。使用此命令的否定(no)形式来从命名的 MAC 访问列表中删除一个拒绝的条件。

CLI 命令：deny any host MACADDR [IFNAME]

举例：(config-acl)# deny any host c2f3.220a.12f4 [fa1/0/2]

5.3.19.2 过滤组合（filter set）

本命令用名称定义了一个延伸的 MAC 访问列表，并进入访问列表设置模式。

CLI 命令：mac access-list extended WORD

举例：(config)# mac access-list extended mac_acl_1

5.3.19.3 过滤条件（filter conditions）

本命令指定了一个或多个拒绝或允许条件来决定封包应被转发或丢弃。

CLI 命令：(permit|deny) any any

举例：(config-acl)# permit any any

5.3.19.4 附加过滤规则（filter attach）

本命令用名称定义了一个延伸的 MAC 访问列表，并进入访问列表设置模式。

CLI 命令：mac access-group WORD in

举例：(config-if)# mac access-group mac_acl_1 in

5.3.20 端口访问控制（Port access control）

5.3.20.1 dot1x 访客 VLAN（dot1x guest-vlan）

使用交换机的 dot1x guest-vlan 端口命令来指定一组活动的 VLAN 为 802.1x 访客 VLAN。用本命令的否定（no）形式来将设置恢复为缺省值。

CLI 命令：dot1x guest-vlan <1-3000>

举例：(config)# interface fa1/0/1

(config-if)# dot1x guest-vlan 3

5.3.20.2 dot1x 端口控制（dot1x port-control）

使用交换机的 dot1x 端口控制（dot1x port-control）界面设置命令来开启端口认证状态的手动控制。用本命令的否定（no）形式将设置恢复为缺省值。

CLI 命令：dot1x port-control (auto|force-authorized| force-unauthorized)

举例：(config)# interface fa1/0/1

(config-if)# dot1x port-control force-authorized

5.3.21 拨入用户（Dial-in user）

5.3.21.1 dot1x 用户名称和密码（dot1x username password）

新增用户至本地 RADIUS 数据库。

CLI 命令：dot1x user WORD WORD VLAN-ID

举例：(config)# dot1x user test 12345 3

5.3.21.2 显示 dot1x 用户（show dot1x user）

显示 dot1x 拨入用户。

CLI 命令：show dot1x user

举例：ASUS# show dot1x user

5.3.22 RADIUS

5.3.22.1 RADIUS 设置（RADIUS settings）

本命令用来设置 802.1x 的 RADIUS 服务器 IP、RADIUS 密钥及 RADIUS 端口。

CLI 命令：dot1x radius server A.B.C.D RADIUS_KEY [PORT]

举例：(config)# dot1x radius server 192.168.1.38 123456 1812

5.3.22.2 显示 dot1x RADIUS（show dot1x radius）

显示 802.1x 设置的 dot1x RADIUS 服务器 IP、RADIUS 密钥及 RADIUS 端口。

CLI 命令：show dot1x radius

举例：ASUS# show dot1x radius

5.3.23 端口安全（Port security）

5.3.23.1 显示端口安全（show port security）

本命令用来显示端口的安全设置、状态与 MAC 地址信息。

CLI 命令：show port-security [address] [interface IFNAME]

举例：ASUS# show port-security

ASUS# show port-security interface gi1/0/25

ASUS# show port-security address

ASUS# show port-security address gi1/0/25

5.3.23.2 清除端口安全设置（clear port security）

本命令用来清除端口安全动态 MAC 地址。

CLI 命令：clear port-security dynamic [address MAC] | [interface IFNAME]

举例：ASUS# clear port-security dynamic

ASUS# clear port-security dynamic 0023.1313.2313

ASUS# clear port-security dynamic interface gi1/0/25

5.3.23.3 交换端口的端口安全（switchport port-security）

本命令用来设置端口的安全设置及 MAC 地址。

CLI 命令：switchport port-security [mac-address MACADDR] | [maximum VALUE] | [violation {protect | restrict | shutdown}] | [reup]

举例：(config)# interface gi1/0/25

(config-if)# switchport port-security

(config-if)# switchport port-security mac-address 0023.1313.2313

(config-if)# switchport port-security maximum 20

(config-if)# switchport port-security violation protect

(config-if)# switchport port-security reup

5.3.23.4 交换端口的端口安全老化(switchport port-security aging)

本命令用来进行端口安全的老化设置。

CLI 命令：switchport port-security aging {time TIME | type {absolute | inactivity}}

举例：(config)# interface gi1/0/1

(config-if)# switchport port-security aging-time 20

(config-if)# switchport port-security aging-type absolute

5.4 其他命令（Miscellaneous commands）

show private health: 显示环境变量，如温度、风扇转速与电压。

show private led : 显示三个系统 LED 指示灯 - SYSTEM，RPS 与 FAN。

show private model : 显示交换机的型号名称。

show version : 显示硬件、Boot ROM 及固件版本号。

ping : ping 远程主机。

show ip route : 显示路由表中的项目。

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。

本章节设置您已经了解了二进制，比特，字节等基础知识。您可以在第 8 章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（电脑或网络设备）。每个 IP 地址包含 4 组号码，每个号码的范围都是 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位数字，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
在网络中确认电脑或设备身份。

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 8 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

下列是有效的 IP 地址范例：

A 类：10.30.6.125（网络 = 10，主机 = 30.6.125）

B 类：129.88.16.49（网络 = 129.88，主机 = 16.49）

C 类：192.60.201.11（网络 = 192.60.201，主机 = 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络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 位。

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

将其转换为二进制更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 ID，但是请注意 field 4 中第一个位同样也被包括到了网络 ID 中。由于额外的位只有两种值（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 是用于检测您的电脑是否能够识别网络上其他电脑的命令。Ping 命令向您指定的电脑送出一条信息，如果该电脑收到这条信息，它就会发送回应。要使用 ping 命令，您需要知道进行联系的电脑的 IP 地址。

在 Windows® 操作系统的电脑上，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 **“确定”**。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。

如果目标电脑收到了这个信息，就会出现如图 62 所示的提示。

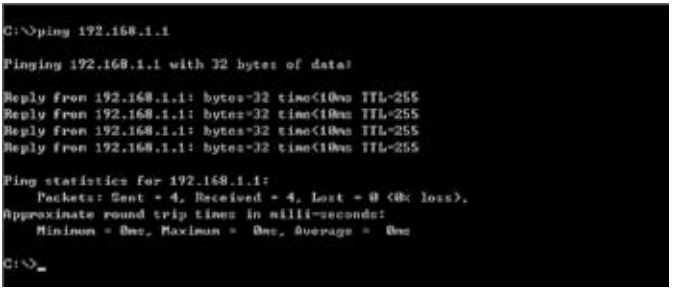


图 62. 使用 ping 工具

如果无法定位目标电脑，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（使用缺省的局域网 IP 地址 192.168.1.1）或其他为交换机指定的地址。

您也可以通过输入一个外部地址，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，地址请求就会传送到上级服务器，以此类推，直到找到地址为止。此时服务器就会将相对应的 IP 地址传送到您的电脑。

对于使用 Windows® 操作系统的电脑，您可以打开 **开始** 菜单，点击 **“运行”**，然后在文本窗口输入以下内容：

nslookup

点击 **“确定”**。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 63 所示。

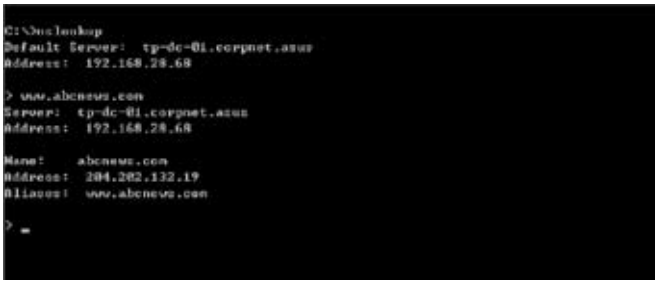


图 63. 使用 nslookup 工具

事实上，一个 Internet 名称可能对应很多个 IP 地址，尤其对网络流量大的站点。这些站点可能使用多个备用服务器来保存相同的信息。

要退出 nslookup，在提示符处键入 exit 并按 <Enter>。

7.2 更换损坏的风扇

在您卸下交换机背面的风扇模块前，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。

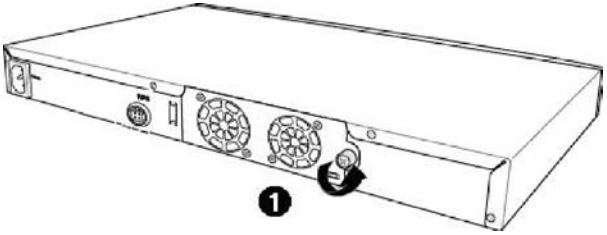


图 64. 拧开螺丝

2. 如图所示拉出风扇模块。

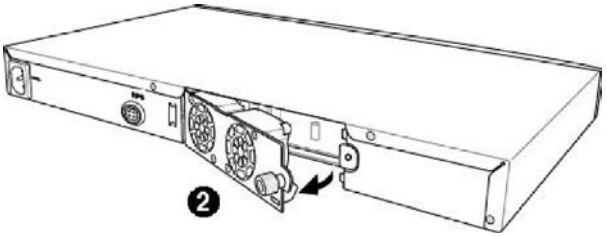


图 65. 卸下风扇

3. 小心地将两条电源线从风扇电源插座上删除。

4. 松开将风扇固定于风扇模块上的螺丝，并删除损坏的风扇。

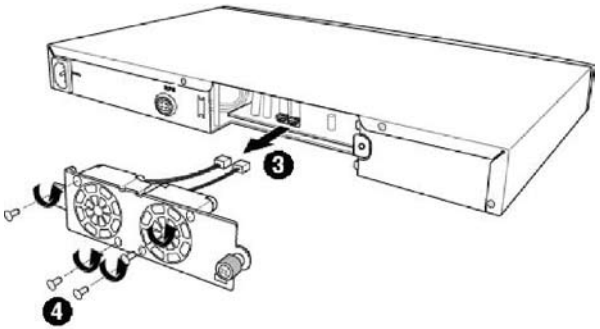


图 66. 卸下损坏的风扇

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块底部。

按照同样的步骤替换另一个风扇。

6. 将风扇电源线连接到电路板上，确认风扇电源线连接到正确的端口。当您面对交换机背部面板时，左边的风扇是风扇 1。

7. 将风扇模块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块和外壳之间。

8. 用螺丝固定风扇模块。检查风扇模块四周确认没有电线卡在风扇模块和外壳之间。

风扇规格

尺寸 : 40 x 40 x 20 mm

电压与电流 : 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 指示灯	
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。
连接后备电源后，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 模块是否符合 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 节的说明替换风扇。
当连接网络线时，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 / 电脑。确认电脑 / 集线器交换机已经打开。 2. 确认线缆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 的线缆。 10Mbit/sec 线缆可能支持较低品质的线缆。
网络访问	
电脑不能访问同一网络中的另一个主机	1. 检查以太网线是否完好，LED 指示灯是否呈绿色。 2. 如果端口的 LED 指示灯呈琥珀色，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。

问题	建议方案
电脑无法显示网页设置界面	1. 交换机已打开并且端口也已经启用。交换机的出厂缺省 IP 为 192.168.1.1. 2. 在您的电脑上确认您的网络设置。如果您的电脑没有设置一个有效的路由来连接到交换机，请将交换机 IP 改成您的电脑可以访问的 IP 地址。 3. 从电脑 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。
网页设置界面	
丢失 / 忘记网页设置端口的用户名称或密码	1. 如果您还没有修改用户名称和密码，请尝试用户名“admin”，密码为空。 2. 通过 RS232 或 USB 登录控制终端，在 Boot ROM 模式下用“psw”命令重置密码。
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 封包丢失，检查您的网络设置，确认设置有效。
对设置的修改无法保存	确认点击了 Save Configuration 页面的 Save 按钮。
控制终端界面	
不能显示终端模拟器上的文字	1. 出厂设置的波特率为 9600，无流量控制，8 位数据，无分奇偶校验，1 位停止位。 2. 将您的终端模拟器设置如上，如果您使用的是 USB 端口，请先安装 USB 驱动程序。 3. 检查连接线是否良好。

8 术语表

10BASE-T　用于以太网的有线线缆，数据传输率为 10Mbps。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 100Mbps。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 1000Mbps。

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，十进位数字 1 写作 1，十进位数字 2 写作 10，十进位数字 3 写作 11，十进位数字 4 写作 100，依次类推。虽然 IP 地址为方便起见表示为十进位数字，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电脑。

download　以下行的方向传输数据，例如，从 Internet 到用户。

Ethernet　以太网。最常见的电脑网络技术，通常使用双绞线。以太网的数据传输速率为 10Mbps 和 100Mbps。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(传入或传出)，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)端口操作的，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 的电脑之间的文件互传。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（通常指电脑）。
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	互联网群组管理协议 一种互联网协议，允许电脑与其网络成员通过组播群组共用信息。一个电脑组播群组就是群组的成员都设置成从成员处接收特定的内容信息。向 IGMP 群组传送组播的应用可随时更新群组的地址簿或将公司的通告传送到收信人列表。
IGMP Snooping	在每个端口侦听 IGMP 封包并将端口与二层组播群组相关联。
Internet	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（电脑）在互联网上的地址，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	网络服务提供商 向顾客提供互联网访问服务的公司，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。交换机前面的指示灯就是 LED。
MAC address	媒体访问控制地址，简称 MAC 地址 由制造商分配的设备的永久性硬件地址。MAC 地址由六对字

	符组成。
mask	掩码。参见 network mask。
Multicast	组播。将数据传送到一组网络设备上。
Mbps	百万比特每秒的缩写。网络数据传输率常表示为 Mbps。
Monitor	监控。亦称“Roving Analysis”，允许将一个网络分析器连接至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，允许相互通信和共用资源（如软件、文件等）的一组电脑。网络可以是小型的，例如局域网(LAN)，也可以是大型的，例如互联网。
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 表示此位有效，0 表示忽略此比特。举例说明，如果网络掩码 255.255.255.0 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 插入电脑，提供网络线缆的物理接口 RJ-45 的适配器。参见 Ethernet，RJ-45。
packet	封包，在网络上传输数据的单位。每个封包都包含数据、添加的信息，如它从哪里来（来源地址）及将到哪里去（目的地地址）。
ping	封包探测 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。物理的网络设备接入点，如电脑，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。为了使数据能够成功传输，数据传输来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	注册端口标准 45 这种 8-pin 的插头是用于在电话在线传输数据的。以太网线通常也会使用这种插头。
RMON	远程监控 SNMP 的延伸，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， 根据来源 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回路的桥接协议。
subnet	子网。子网是网络的一部分，子网通过将网络中的电脑归分为小组而使这些电脑与其他网络上的电脑分隔开来。子网中的电脑仍然在物理上与其他上层网络相连，但是他们被认为是一个独立的网络。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 负责将这些封包传送到目的地址。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，以字符为基础的，用于访问远程电脑的程序。HTTP（网络协议）和 FTP 只允许从远程电脑下载文件，而 Telnet/ SSH 允许从远程登录并使用电脑。
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 封包的一个栏位，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，使用的是一种高端的，用于 10BASE-T 网络的三类线(CAT 3)，以及更高端的 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　广域网络

所有的分布于广大的地理位置的网络统称广域网络，如一个国家或一个洲。对于交换机来说，广域网络指的就是互联网。

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，声音或视讯。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。当用户访问一个网站时，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电脑。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。全球范围内可通过互联网访问的所有网站的总和。