

# GigaX2024B

二层网管型交换机

用户手册

C2403

2006.3 V1

#### 版权所有 © 2006 华硕电脑

在未获得华硕电脑公司（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，翻译以及存储于公共资源系统中。本手册仅作为用户购货时附带的说明文件。

若出现以下情况，恕不再提供产品的保修或服务：(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) 产品序列号无法辨认或已丢失。

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保修承诺，产品的畅销性，或针对于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（包括损失利润，损失业务，数据丢失，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有可能会導致上述损失。

本手册中的规格和信息仅作参考，并以华硕最新修订版本为准，并且华硕毋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数据均不承担责任，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。

## 华硕联络信息

### 华捷联合信息（上海）有限公司（莘庄）

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

### 华捷联合科技(广州)有限公司

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

### 华捷联合信息(上海)有限公司成都办事处

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

### 华捷联合信息(上海)有限公司沈阳办事处

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

### 华捷联合信息(上海)有限公司北京海淀分公司

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

### 华硕技术支持:

免费咨询电话: 800-8206655 (7\*24小时人工接听)

Email: [tsd@asus.com.cn](mailto:tsd@asus.com.cn)

Netq论坛: [Netq.asus.com.cn](http://Netq.asus.com.cn)由华硕工程师提供在线服务



# 目录

<b>1</b>	<b>简介</b>	<b>1</b>
1.1	GigaX2024B 特性	1
1.2	手册使用说明	2
1.2.1	表示意义	2
1.2.2	排版字体	2
1.2.3	符号说明	2
<b>2</b>	<b>认识 GigaX2024B</b>	<b>3</b>
2.1	包装内容	3
2.2	前面板	4
2.3	后面板	5
2.4	技术规格	5
<b>3</b>	<b>快速设置指南</b>	<b>6</b>
3.1	第一部分 — 安装硬件	6
3.1.1	将交换机安装在水平表面上	6
3.1.2	将交换机安装在机架上	6
3.2	第二部分 — 安装交换机	6
3.2.1	连接控制终端接口	6
3.2.2	连接计算机或局域网 (LAN)	7
3.2.3	连接冗余电源 (RPS) 模块	7
3.2.4	连接电源适配器	7
3.3	第三部分 — 基本管理设置	8
3.3.1	通过控制终端进行设置	8
3.3.2	通过网页界面进行设置	10
<b>4</b>	<b>网页界面下的设置</b>	<b>12</b>
4.1	登录到网页设置界面	12
4.2	功能结构图	13
4.2.1	菜单导航技巧	14

4.2.2	常用的按钮和图标.....	14
4.3	System (系统).....	15
4.3.1	Management (管理).....	15
4.3.2	IP setup (IP 设置).....	15
4.3.3	Reboot (重新启动).....	16
4.4	Physical interface (物理端口) .....	17
4.5	Bridge (桥接).....	19
4.5.1	Spanning tree (生成树).....	19
4.5.1.1	STP status (STP 状态).....	19
4.5.1.2	Current roots (当前根).....	20
4.5.1.3	Bridge parameters (桥接参数).....	21
4.5.1.4	Port parameters (端口参数).....	22
4.5.1.5	Runtime status (运行状态).....	23
4.5.2	Link aggregation static (静态链路汇聚).....	23
4.5.3	LACP.....	25
4.5.4	Mirroring (镜像).....	26
4.5.5	Static multicast (静态组播).....	27
4.5.6	IGMP snooping (IGMP 侦测).....	28
4.5.7	Traffic control (流量控制).....	29
4.5.8	Dynamic addresses (动态地址).....	29
4.5.9	Static addresses (静态地址).....	30
4.5.10	VLAN configuration (VLAN 设置).....	31
4.5.11	GVRP .....	32
4.5.12	QoS 和 CoS.....	33
4.5.12.1	802.1p priority (802.1p 优先级).....	33
4.5.12.2	CoS queue mapping (CoS 队列映射).....	34
4.5.12.3	QoS bandwidth (QoS 带宽).....	35
4.6	SNMP .....	36
4.6.1	Community table (团体列表).....	36

4.6.2	Host table (主机列表).....	37
4.6.3	Trap setting (Trap 设置).....	37
4.6.4	SNMPv3 VGU table (SNMPv3 VGU 列表).....	38
4.6.4.1	VACM view (VACM 视图).....	38
4.6.4.2	VACM group (VACM 群组).....	39
4.6.4.3	USM user (USM 用户).....	40
4.7	Filter 页面.....	41
4.7.1	Filter set (过滤集).....	41
4.7.2	Filter attach (过滤规则分配).....	43
4.8	安全.....	44
4.8.1	Port access control (端口访问控制).....	44
4.8.2	Dial-in user (拨入用户).....	46
4.8.3	RADIUS.....	47
4.8.4	端口安全.....	48
4.8.4.1	Port configuration (端口配置).....	48
4.8.4.2	Port status (端口状态).....	49
4.8.4.3	Secure MAC address (安全 MAC 地址).....	50
4.9	Traffic chart (流量图表).....	51
4.9.1	Traffic comparison (流量比较).....	51
4.9.2	Error group chart (错误分组).....	52
4.9.2	Historical status (历史状态).....	52
4.10	Cable diagnosis (缆线诊断).....	53
4.11	Save configuration (保存设置).....	53
5	控制终端画面.....	54
5.1	开机自检.....	54
5.1.1	Boot ROM 命令模式.....	54
5.1.2	Boot ROM 命令.....	55
5.2	登录和注销.....	56
5.3	CLI 命令.....	56

5.3.1	用户帐户 .....	56
5.3.1.1	新增用户 .....	56
5.3.1.2	删除用户 .....	56
5.3.2	备份和恢复 .....	56
5.3.2.1	备份启动设置文件 .....	56
5.3.2.2	恢复启动设置文件 .....	57
5.3.3	系统管理设置 .....	57
5.3.3.1	固件升级 .....	57
5.3.3.2	configure terminal .....	57
5.3.3.3	enable .....	57
5.3.3.4	disable .....	57
5.3.3.5	end .....	58
5.3.3.6	exit .....	58
5.3.3.7	help .....	58
5.3.3.8	host name (主机名) .....	58
5.3.3.9	System contact (系统联系信息) .....	58
5.3.3.10	System Location (系统位置) .....	59
5.3.3.11	IP 地址和网络掩码 .....	59
5.3.3.12	Default gateway (默认网关) .....	59
5.3.3.13	reboot (重新启动) .....	59
5.3.3.14	reload default-config file .....	60
5.3.3.15	show running-config .....	60
5.3.3.16	write .....	60
5.3.3.17	分配一个新的用户帐户 .....	60
5.3.3.18	删除一个用户帐户 .....	60
5.3.4	物理端口命令 .....	60
5.3.4.1	端口模式 .....	61
5.3.4.2	端口双工模式 .....	61
5.3.4.3	端口流量控制 .....	61



5.3.4.4	Show L2 interface .....	61
5.3.5	IP 界面 .....	62
5.3.5.1	show vlan name string .....	62
5.3.5.2	创建一个 VLAN .....	62
5.3.5.3	interface vlan VLAN-ID .....	62
5.3.5.4	ip address .....	62
5.3.5.5	ip dhcp client .....	63
5.3.5.6	ip route .....	63
5.3.6	生成树 .....	63
5.3.6.1	show spanning-tree summary .....	63
5.3.6.2	spanning-tree enable/disable .....	63
5.3.7	链路汇聚 .....	63
5.3.7.1	干线群组 .....	63
5.3.7.2	干线负载平衡 .....	64
5.3.7.3	show aggregation-link trunk .....	64
5.3.8	LACP .....	64
5.3.8.1	lacp 汇聚链路 .....	64
5.3.8.2	禁用 lacp 汇聚链路 .....	64
5.3.8.3	lacp system-priority .....	64
5.3.9	镜像 .....	65
5.3.9.1	镜像设置 .....	65
5.3.9.2	Show mirror .....	65
5.3.9.3	No mirror .....	65
5.3.9.4	No mirror .....	65
5.3.10	静态组播 .....	65
5.3.10.1	mac-address-table multicast .....	65
5.3.10.2	no mac-address-table multicast .....	66
5.3.10.3	show mac-address-table multicast .....	66
5.3.11	IGMP 侦测 .....	66

5.3.11.1	ip igmp snooping.....	66
5.3.11.2	间隔时间.....	66
5.3.12	流量控制 .....	66
5.3.12.1	storm-control .....	66
5.3.12.2	no storm-control .....	67
5.3.12.3	show storm-control .....	67
5.3.13	动态地址 .....	67
5.3.13.1	clear dynamic mac-address.....	67
5.3.13.2	aging time .....	67
5.3.13.3	no aging time .....	67
5.3.13.4	show mac-address-table aging-time .....	68
5.3.14	静态地址 .....	68
5.3.14.1	新增静态 MAC 地址.....	68
5.3.14.2	show mac-address-table .....	68
5.3.15	VLAN .....	68
5.3.15.1	show vlan name string.....	68
5.3.15.2	vlan vid .....	68
5.3.15.3	name string .....	69
5.3.15.4	access vlan .....	69
5.3.15.5	allowed VLANs .....	69
5.3.16	GVRP .....	69
5.3.16.1	clear gvrp statistics.....	69
5.3.16.2	gvrp 模式 .....	69
5.3.16.3	显示 gvrp 设置 .....	70
5.3.16.4	show gvrp statistics .....	70
5.3.17	CoS/QoS .....	70
5.3.17.1	queue cos-map .....	70
5.3.17.2	show queue cos-map.....	70
5.3.17.3	qos 模式.....	70

---

5.3.17.4	show cos policy .....	70
5.3.17.5	qos ingress bandwidth.....	71
5.3.18	SNMP .....	71
5.3.18.1	show rmon statistics .....	71
5.3.18.2	show snmp-server community.....	71
5.3.18.3	snmp-server host.....	71
5.3.19	过滤 .....	71
5.3.19.1	deny any host.....	71
5.3.19.2	过滤集 .....	72
5.3.19.3	过滤条件.....	72
5.3.19.4	过滤规则分配 .....	72
5.3.20	端口访问控制 .....	72
5.3.20.1	dot1x guest-vlan.....	72
5.3.20.2	dot1x max-req .....	73
5.3.20.3	dot1x port-control .....	73
5.3.21	拨入用户 .....	73
5.3.21.1	dot1x username password.....	73
5.3.21.2	show dot1x user .....	73
5.3.22	RADIUS .....	74
5.3.22.1	RADIUS 设置 .....	74
5.3.22.2	show dot1x radius .....	74
5.3.23	端口安全 .....	74
5.3.23.1	show port security .....	74
5.3.23.2	clear port security .....	74
5.3.23.3	switchport port-security .....	75
5.3.23.4	switchport port-security aging.....	75
5.4	其他命令 .....	75
6	IP 地址, 网络掩码和子网.....	76
6.1	IP 地址.....	76

6.1.1	IP 地址的结构 .....	76
6.1.2	网络类型 .....	77
6.2	子网掩码 .....	77
<b>7</b>	<b>疑难排解 .....</b>	<b>79</b>
7.1	使用 IP 工具诊断问题 .....	79
7.1.1	ping .....	79
7.1.2	nslookup .....	80
7.2	更换故障风扇 .....	81
7.3	简易维修 .....	83
<b>8</b>	<b>术语表 .....</b>	<b>85</b>

# 1 简介

感谢您购买华硕 GigaX 2024B 二层网管型交换机！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 Network）。

本用户手册将为您提供安装及设置 GigaX 2024B 二层网管型交换机所需的相关信息。

## 1.1 GigaX 2024B 特性

---

- 共计 24 个 10/100BSAE-T 和 2 个 10/100/1000BASE-T 自适应千兆以太网交换端口
- 1 个小型 (SFP) 千兆端口转换插槽 (GBIC)
- 所有端口支持自适应 MDI/MDIX 功能
- 兼容 802.3z 和 802.3ab 规格
- 802.1D 透明桥接
- STP/RSTP/MSTP
- 16K MAC 地址存储，基于硬件的地址老化时间
- 802.3x 流量控制
- 基于 802.1Q 标记的 VLAN, 最多支持 255 组 VLAN
- 802.1p 服务级别，每端口支持 4 个队列
- IGMP 侦测
- 802.3ad 链路汇聚（干线），最多支持 6 个干线群组
- LACP
- GVRP
- 访问控制列表 (ACL)
- 速度限制，粒度 1Mbps
- 端口镜像
- 802.1x
- 端口安全
- DHCP 侦测
- SNMP v1, v2, v3
- MIB-II
- 企业 MIB: 电源、风扇、系统及电压

- Telnet/SSH 远程登录
- 通过 TFTP 进行固件升级和设置备份
- 命令行界面
- 网页图形界面
- 端口链路状态 LED 指示灯
- 系统、冗余电源 (RPS) 和风扇 LED 指示灯

## 1.2 手册使用说明

---

### 1.2.1 表示意义

- 缩写意义将在首次出现以及术语表中列出。
- 为简洁起见，GigaX 交换机简称 “交换机”。
- 术语 “LAN（局域网）” 和 “网络” 将交替使用，表示某个区域内通过以太网连接的一组计算机。

### 1.2.2 排版字体

- **粗体字**表示该文字是您从菜单或下拉菜单中选择的项目，或是程序提示字符串。

### 1.2.3 符号说明

本用户手册使用以下图标表示特殊信息，以此引起用户的注意。



**注意：** 提供对当前叙述内容的说明或额外信息。



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



**警告：** 高重要性的信息，包括涉及人身安全或系统完整性的信息。

## 2 认识 GigaX 2024B

### 2.1 包装内容

GigaX 2024B 交换机包装内包含以下内容：

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

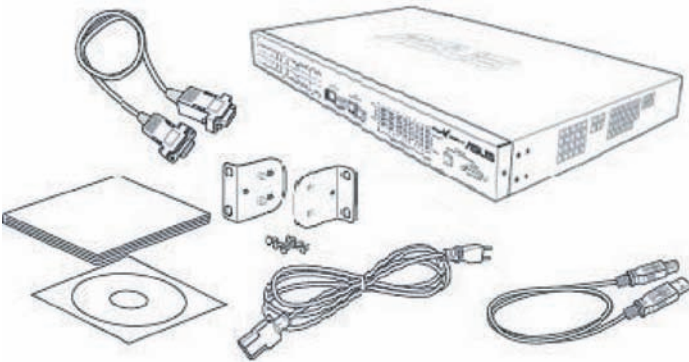


图 1. GigaX 2024B 二层网管型交换机包装内容

## 2.2 前面板

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



图 2. 前面板

表 1. 前面板标识和 LED 指示灯

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



## 2.3 后面板

交换机的后面板包含了风扇模组、一个电源接口和一个冗余电源 (RPS) 接口。

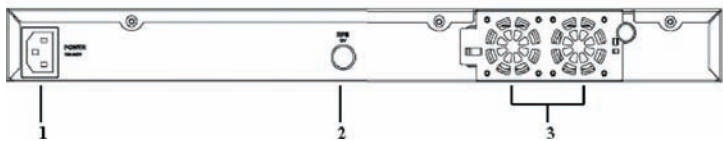


图 3. 后面板

表 2. 后面板标识

No.	项目	描述
1	电源接口	连接电源线
2	RPS	冗余电源接口
3	FAN1-FAN2	可置换的系统风扇

## 2.4 技术规格

表 3. 技术规格

物理尺寸	43.5mm( 高 ) x 444 mm( 宽 ) x 322mm( 深 )		
电源	输入	功耗	
	100-240V AC/ 2.5A 50-60Hz	< 50 瓦	
冗余电源 (RPS)	输入	输出	
	100-240V AC/ 1.8A 50-60Hz	12V DC/12.5A	
环境		操作	存储
	温度	0 ~ 40 °C ( 32 ~ 122 °F)	-25 ~ 70 °C ( -40 ~1 58 °F)
	湿度	15 ~ 90%	0 ~ 95%
	海拔	最高 3,000 米	最高 12,000 米
可置换式风扇	尺寸	电压和电流	速率
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

## 3 快速设置指南

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

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

第二部分阐述设置硬件的步骤。

第三部分阐述 GigaX 2024B 交换机的基本设置步骤。

在开始进行安装和设置之前，请先向网络管理员获取如下信息：

交换机的 IP 地址

网络的默认网关

网络的子网掩码

### 3.1 第一部分 — 安装硬件

---

#### 3.1.1 将交换机安装在水平表面上

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

#### 3.1.2 将交换机安装在机架上

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

### 3.2 第二部分 — 安装交换机

---

#### 3.2.1 连接控制终端接口

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

### 3.2.2 连接计算机或局域网 (LAN)

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



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

### 3.2.3 连接冗余电源 (RPS) 模块

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

### 3.2.4 连接电源适配器

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

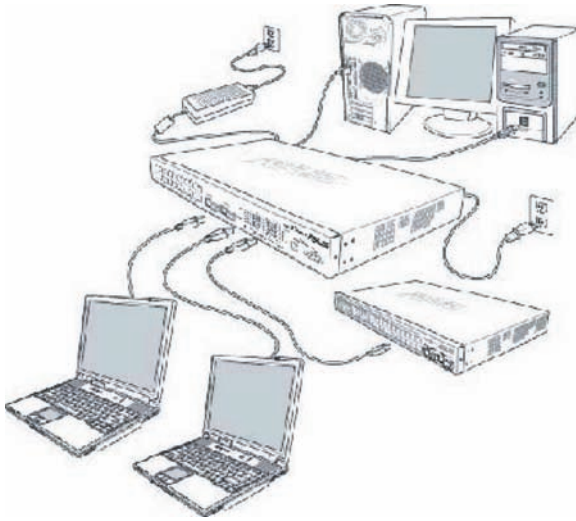


图 4. 硬件连接图

表 4. LED 指示灯

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

### 3.3 第三部分 — 基本管理设置

完成硬件连接后, 您需要为交换机进行基础设置。您可以选择以下方法进行设置:

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

#### 3.3.1 通过控制终端进行设置

1. 请使用附带的 RS-232 交叉线连接交换机后面板的控制终端接口。这个接口为 DB-9 公接口, 专门用于数据终端设备 (DTE) 的连接。将缆线接头上的紧固螺丝固定在控制终端接头上, 将缆线的另一头连接到具备终端仿真软件, 如 Hyper Terminal 的计算机上。
2. 使用 USB 线将交换机连接到 PC。在连接前您必须首先安装随机光盘中的 USB 驱动程序。USB 驱动可以在 Windows Me/2K/XP 系统下模拟额外的一个 COM 口。
3. 请确认控制终端的仿真软件的设置如下:
  - a) 选择合适的串列端口号
  - b) 将数据传输波特率设为 9600
  - c) 将数据格式设为无配类, 8 位数据, 1 位停止
  - d) 无流量控制
  - e) 将仿真模式设为 VT1000
4. 控制终端设置完毕后, 您可以看到终端显示 “(ASUS)%” 提示符。
5. 键入 “login” 进入命令行界面。默认的用户名为 “admin”。按 <Enter> 跳过密码。



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

6. 请按照下列步骤为交换机配置 IP 地址：

- a) 键入 “enable” 。
- b) 键入 “configure terminal”，出现新的提示符 “ASUS(config)#” 。
- c) 键入 “interface vlan 1”，出现提示符 “ASUS (config-if)#” 。
- d) 键入 “ip address <您的 IP 地址> <您的网络掩码>”。例如，您的交换机的 IP 为 192.168.1.1，网络掩码为 255.255.255.0。那么您需要键入 “ip address 192.168.1.1/24” 。
- e) 键入 “end”，将返回上一级的提示符 “ASUS#” 。
- f) 键入 “write”，您所做的变更将写入配置文件中。
- g) 键入 “reboot” 。

如果交换机需要跨网络进行管理，您还需要输入默认网关或静态路由。请按照下列步骤为交换机分配一个默认网关或静态路由：

- a) 输入 “ASUS#” 。
- b) 键入 “show running-configuration” 以查看当前配置。若路由地址设置错误，您需要键入 “no ip route 0.0.0.0/0 192.168.1.254” 来将它移除。
- c) 键入 “configure terminal”，出现新的提示符 “ASUS(config)#” 。
- d) 键入 “no ip route 0.0.0.0/0 192.168.1.254” 来清除默认路由。
- e) 键入 “ip route 0.0.0.0/0 192.168.1.2” 来设置您的默认路由。
- f) 键入 “end” 。
- g) 键入 “write” 。

```
ASUS login: admin
Password:
ASUS GigaX 2024B 3.2.02.00 Copyright (c) 2005

ASUS> enable
ASUS# configure terminal
ASUS(config)# interface vlan 1
ASUS(config-if)# ip address 192.168.1.1/24
Install IP address succeeded!
ASUS(config-if)# end
ASUS# configure terminal
ASUS(config)# no ip route 0.0.0.0/0 192.168.1.254
ASUS(config)# ip route 0.0.0.0/0 192.168.1.2
ASUS(config)# end
ASUS# write
Building Configuration ...
Integrated configuration saved as 'startup_config' ok!
ASUS# _
```

图 5. 控制终端设置

### 3.3.2 通过网页界面进行设置

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

1. 若您的 PC 没有安装 Java Runtime Environment，PC 会自动从网络下载和安装这个环境。这就意味着您的 PC 必须可以访问网络。如果您的 PC 不能访问 Internet，您需要将程序保存在磁盘，然后进行安装。



若您想通过网页形式进行管理，您的 PC 必须安装了 Java Runtime Environment。您可以从随机光盘中安装这个程序。

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

http://192.168.1.1

这是交换机出厂时的默认 IP 地址。

如图 6 的登录窗口将出现。



图 6. 登录

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



默认用户名：admin

默认密码：（无）

您可在任何时间对密码进行修改（见 5.3.1 系统命令）

浏览器将会从交换机上下载 java 平台，这个过程需要几秒钟时间。

3. 设置新的 IP 地址时, 点击 **System**, 然后点击 **IP Setup** 页面。填入 IP 地址、网络掩码和默认网关, 然后按 **OK**。
4. 如果交换机采用了新的 IP 地址, 浏览器不能自动更新交换机的状态窗口, 也不能退回之前的设置页面。您需要重新在网页地址栏中键入新的 IP 地址, 然后按 <Enter>, 重新进入网页设置界面。



图 7. IP 设置

## 4 网页界面下的设置

GigaX 2024B 交换机提供网页设置界面，这样您就可以通过网络对交换机进行设置。这个功能推荐配合带有 Java® 的 Microsoft Internet Explorer 6.0 及以后版本使用。

### 4.1 登录到网页设置界面

---

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

http://192.168.1.1

这是交换机出厂时默认的 IP 地址。图 8 显示的是登录窗口。



图 8. 设置界面登录窗口

2. 输入用户名和密码，然后按 OK。

当您第一次登录到网页界面时，请使用下列默认参数。您可在命令行界面下随时更改密码。（请参考 56 页 5.3.1 的内容）

默认用户名: admin

默认密码: <无>

每当您登录到网页设置界面时，您都会看到设置主页。



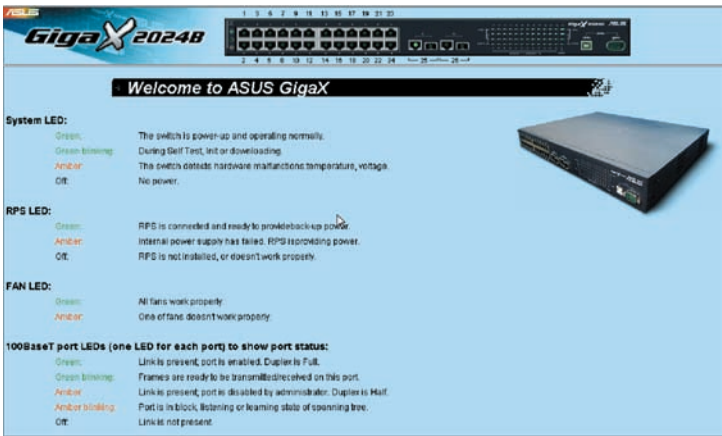


图 9. 主页

## 4.2 功能结构图

GigaX 2024B 交换机的网页设置界面分为三个部分。顶部栏包括了交换机的 logo 和前面板，如图 10 和图 11 所示。顶部栏将一直出现在设置过程中，并且每隔一段时间更新 LED 状态，见表 4 中 LED 的表示意义以及表 5 的 LED 颜色意义。



图 10. 顶部栏



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，但端口被手动或生成树禁用。
黑色	没有以太网连接

点击交换机图片上端口的图标，端口的设置情况将显示在窗口的右下部位。

菜单中的项目，如图 12 所示，包含了交换机可设置的所有特性。这些特性都已经进行了分类，例如 System, Bridge。您可以点击其中的每一项以显示不同的设置页面。



图 12. 菜单项目

4.2.1 菜单导航技巧

要打开某个设置页面，点击对应的菜单项目。

4.2.2 常用的按钮和图标

下表显示的是网页界面中的按钮和图标的功能。

表 6. 常用按钮和图标

按钮 / 图标	描述
	将当前页面中的设置进行保存。
	重新显示当前页，更新状态或设置。
	修改系统中已有的设置，例如静态路由或滤波器 ACL 规则和其他。
	将设置添加到系统，例如，静态 MAC 地址或防火墙 ACL 规则等。
	添加系统设置，例如静态 MAC 地址或防火墙 ACL 规则及其他。
	修改已存在的设置。
	删除选中的项目，例如静态路由或过滤 ACL 规则及其他。
	查找某个项目的状态。
	让面板上的所有端口禁止这个功能
	让面板上所有端口具有这个功能

## 4.3 System( 系统 )

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

### 4.3.1 Management ( 管理 )

Management ( 管理 ) 页面包括以下信息:

Model Name ( 型号 ) : 产品名称


MAC Address ( MAC 地址 ) : 交换机的 MAC 地址

System Name ( 系统名称 ) : 用户定义的用于区分系统的名称 ( 可编辑 )

System Contact ( 系统联系信息 ) : ( 可编辑 )

System Location ( 系统方位 ) : ( 可编辑 )

若要保存并立即应用设置, 请点击 OK。点 Reload 刷新设置, 如图 13 所示。



The screenshot shows a web interface titled "Management" with a light blue background. A yellow rectangular box contains the configuration fields. The fields are: Model Name (GigaX 2024B), MAC Address (0020.24b0.320a), System Name (ASUS), System Contact (support@asus.com.tw), and System Location (rd@asustek). At the bottom of the yellow box are two green buttons: "OK" and "Reload".

图 13. 管理

### 4.3.2 IP setup ( IP 设置 )

IP 设置页面包含以下可编辑的信息:

DHCP Client ( DHCP 客户端 ) : 允许或禁用 DHCP。

IP Address ( IP 地址 ) : 为交换机管理界面分配一个静态 IP 地址。

Network Mask ( 网络掩码 )

Default Gateway ( 默认网关 )

要保存设置并使之立刻生效, 请点击 OK 然后点击 Reload 更新设置。



图 14. IP 设置

### 4.3.3 Reboot ( 重新启动 )

Reboot 页面中包括一个 Reboot 按钮。点击该按钮重新启动系统。



重新启动系统将中断网络并中止网页界面的连接。

### 4.3.4 Firmware upgrade ( 固件升级 )

固件升级页面包括以下信息：

Hardware Version( 硬件版本 )：显示硬件版本号

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

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

输入 TFTP 服务器的 IP 地址和固件名称。点击 Upgrade 更新交换机的固件。参见图 15。

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



点击 upload 按钮将指定的固件刷新到交换机，固件升级完成后将重新启动系统。您需要在重新启动后再次登录网页界面。



图 15. 固件升级

## 4.4 Physical interface (物理端口)

物理端口页面显示端口即时状态。您可以在下列栏目内对端口进行设置：

- Port (端口)：选择要进行设置的端口
- Admin (管理)：禁用 / 启用端口
- Mode (模式)：选择速度和双工模式
- Flow Control (流量控制)：启用 / 禁用 802.3x 流量控制机制
- Switchport Mode (交换端口模式)：将端口设置成链路汇聚模式或访问模式
- Admin port VLAN (管理端口 VLAN)：为选中的端口分配 PVID
- DHCP-Snoop: 启用 / 禁用 DHCP 侦测功能。
- DHCP-Snooping: 将选中的端口设置为 untrusted 或 trusted 端口

选择相关的端口号码进行设置，然后点击 Modify 按钮。修改的栏目将更新端口状态窗口中的信息，但是新的设置直到进行 Save Configuration 之后才会生效。

- Runtime Status (运行状态)：显示每个端口的下列信息：
- Ethernet Link (以太网连接)：已连接或未连接
- STP Status: STP 状态
- Duplex: 双工模式
- Speed: 连接速率
- Flow Control: 启用 / 禁用 802.3x 流量控制机制

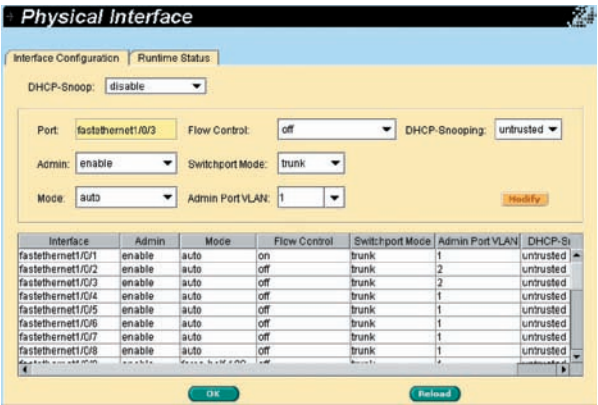


图 16. 物理端口 - 设置

Physical Interface						
Interface Configuration   Runtime Status						
Interface	Ethernet Link	STP Status	Duplex	Speed	Flow Control	Oper Po
fastethernet1/0/1	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/2	not connected	N/A	N/A	N/A	N/A	2
fastethernet1/0/3	not connected	N/A	N/A	N/A	N/A	2
fastethernet1/0/4	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/5	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/6	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/7	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/8	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/9	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/10	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/11	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/12	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/13	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/14	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/15	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/16	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/17	not connected	N/A	N/A	N/A	N/A	1
fastethernet1/0/18	not connected	N/A	N/A	N/A	N/A	1

图 17. 物理端口 - 运行状态

## 4.5 Bridge（桥接）

桥接页面包括了大部分的二层设置内容，如链路汇聚、STP 等。

### 4.5.1 Spanning Tree（生成树）

您可以在这个页面设置三种类型的生成树协议。

#### 4.5.1.1 STP Status（STP 状态）

第一个“STP Status”页面可以让您禁止或启用 STP。这里有三种模式可选，分别是 STP, RSTP 和 MSTP。如果启用了 MSTP，下列四项也同时启用：

Region Name: 由字母和数字组成的配置名称

Revision: 配置的修订号

Instance ID: STP 实例，您可以设置您交换机的 MSTP，将多组 VLAN 映射到一个 STP 实例中。

VLAN Group: 将 4094 组可能存在的 VLAN 的每一个联合到已给实例(instance)的一个群组。

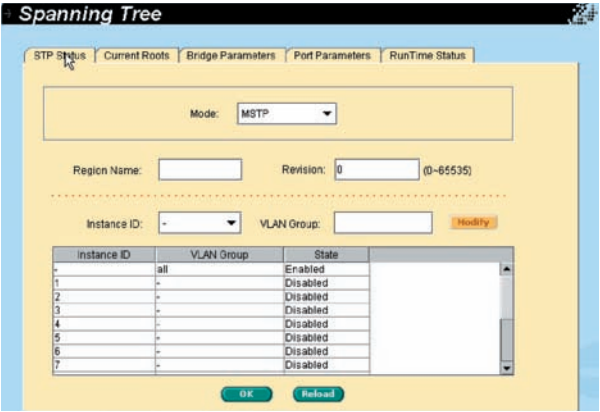


图 18. 生成树 - 状态

#### 4.5.1.2 Current roots (当前根)

这个页面显示了当前的根桥信息，包括：

- Instance ID
- VLAN 群组属于哪个 instance ID
- 根桥的 MAC 地址
- 根桥的优先级
- 根桥存在的最长时间
- 根桥的 hello time
- 根桥的转发延迟时间
- 根桥的路径代价 (Path cost)
- 网桥的根端口

# Spanning Tree

STP Status | **Current Roots** | Bridge Parameters | Port Parameters | RunTime Status

Instance ID	VLAN Group	MAC Address	Priority	Max Age	Hello Time	
-	-	0020.24b0.320a	32768	20	2	15

Refresh

图 19. 生成树 - 当前根



### 4.5.1.3 Bridge parameters( 桥接参数 )

BPDU 传输的生成树参数可以在这个面板上设置:

Hello Time: 生成 BPDU 配置之间的间隔

Max Age: 局域网中所有网桥使用的老化时间

Forward Delay: 转发延迟

Bridge Priority: 局域网中的交换优先级

Transmission Limit: 实例的根交换机通常发出一个代价为 0 的 BPDU( 或 M-record), 传送界限设为最大值。

Instance ID	VLAN Group	Priority	Max Age	Hello Time	Forward Delay	Tr
-	-	32768	20	2	15	3

图 20. 生成树 - 桥接参数

4.5.1.4 Port parameters ( 端口参数 )

这个页面包含了一个显示窗口，用来显示当前每个端口的配置情况。您可以选择一个端口，然后对它进行编辑。点击 Modify 为生成树修改端口设置。下列是可编辑的区域：

Instance ID ( 只在 MSTP 模式下可用 )：生成树实例，您可以在交换机上设置 MSTP 模式，将多个 VLAN 映射到一个 STP 实例。

Priority：设置交换机端口的优先级。越小的数字代表越高的优先级。如果检测到网络循环，较低优先级的端口更有可能被 STP 阻塞。可以设置的值为 0~240。

Path Cost：可设置的值为 1~65535(RSTP:200000000)。如果检测到网络循环，较高代价 ( cost ) 的端口更有可能被 STP 阻塞。

Link Type：在默认情况下，连接类型由端口的双工类型决定：全双工端口采用点对点的连接；而半双工端口采用的是共享连接。

Edge Port：边缘端口 ( edge port )。与 Port Fast-enabled 端口相同，您只能在连接了一个单独末端站点的端口上启用它。

点击 OK 使设置生效。点击 Reload 刷新当前设置。

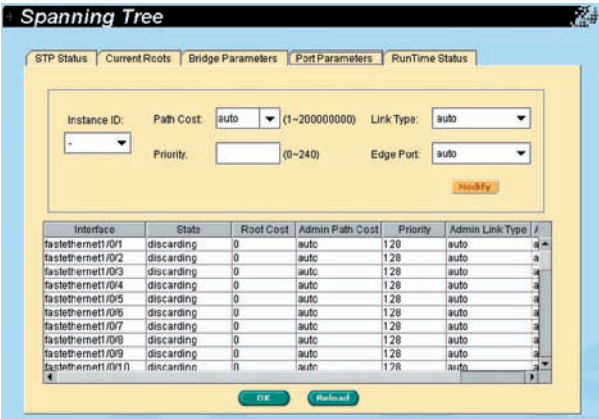


图 21. 生成树 - 端口参数

#### 4.5.1.5 Runtime status (运行状态)

这个页面包含了一个显示窗口用来每个端口的当前状态。

Interface	State	Root Cost	Oper Path Cost	Priority	Oper Link Typ
fastethernet1/0/1	discarding	0	200000000	128	shared
fastethernet1/0/2	discarding	0	200000000	128	shared
fastethernet1/0/3	discarding	0	200000000	128	shared
fastethernet1/0/4	discarding	0	200000000	128	shared
fastethernet1/0/5	discarding	0	200000000	128	shared
fastethernet1/0/6	discarding	0	200000000	128	shared
fastethernet1/0/7	discarding	0	200000000	128	shared
fastethernet1/0/8	discarding	0	200000000	128	shared
fastethernet1/0/9	discarding	0	200000000	128	shared
fastethernet1/0/10	discarding	0	200000000	128	shared
fastethernet1/0/11	discarding	0	200000000	128	shared
fastethernet1/0/12	discarding	0	200000000	128	shared
fastethernet1/0/13	discarding	0	200000000	128	shared

图 22. 生成树 - 运行状态

#### 4.5.2 Link aggregation static (静态链路汇聚)

本页面用于设置链路汇聚群组（端口群组）。本交换机可以提供最多 32 个链路汇聚群组。这个最大值可以通过堆栈设置来实现。

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

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

**Port:** 这些端口图标按照交换机前面板上的位置列出。您需要点击这些图标来选取群组成员。再次点击选中的端口可将这个端口从群组中删除。

点击 OK 将这些设置送到交换机。点击 Reload 刷新当前设置。要使这些设置生效，请进入“Save Configuration”页面，然后点击 Save。

您需要检查连接速度和双工模式，以确保干线群组是激活的。进入 Physical Interface(物理端口)界面并在 Runtime Status 窗口中检查群组端口的连接模式。如果所有的群组成员都具有相同的速度和全双工模式，那么干线群组就设置成功了。如果有一个成员不具备相同的速度和全双工模式，则群组的设置不正确。检查连接的对象和设置，使群组中的所有成员都具有相同的速度，并工作于全双工模式。



链路汇聚群组中的所有端口**必须**工作于全双工模式，并具有相同的速度。

链路汇聚群组中的所有端口**必须**设置为自动协商模式或全双工模式。这样才有可能建立全双工连接。如果您将端口设置为全双工模式，那么与之连接的对象也**必须**具有相同设置。否则链路汇聚的运作可能出现不正常。

链路汇聚群组中的所有端口**必须**具有相同的 VLAN 设置。

链路汇聚群组中的所有端口被视作一个逻辑连接。也就是说，如果任何成员的属性发生变更，其他成员也会随之变更。例如，一个群组包含端口 1 和端口 2，若端口 1 的 VLAN 发生改变，端口 2 的 VLAN 也会随端口 1 一起改变。

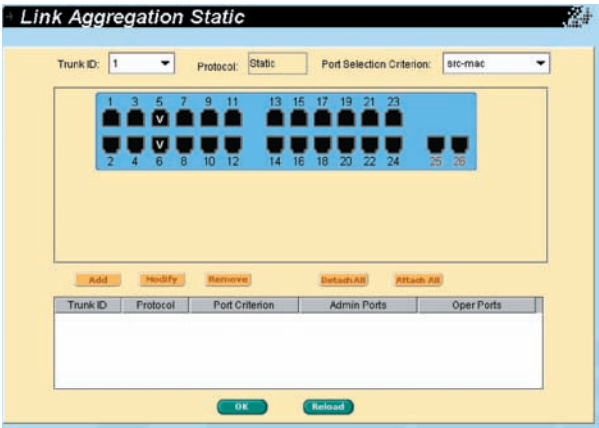


图 23. 链路汇聚

4.5.3 LACP

这个页面用来设置 LACP 群组（端口群组）。本交换机提供了最多 32 组链路汇聚，每个群组最多可包含 8 个端口。这个最大值可以通过堆栈设置来实现。这项功能提供了五个统计量。

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

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

**Port:** 这些端口图标按照交换机前面板上的位置列出。您需要点击这些图标来选取群组成员。再次点击选中的端口可将这个端口从群组中删除。

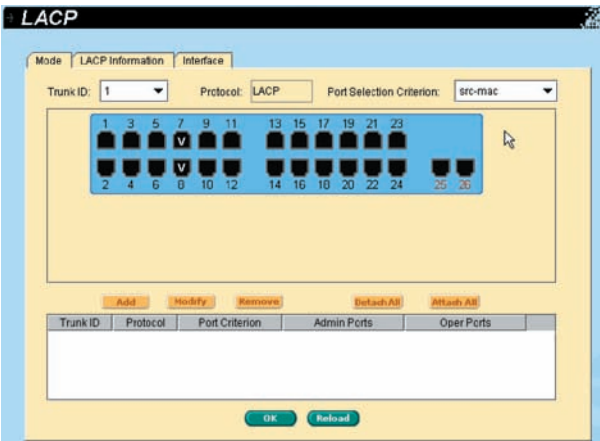


图 24. LACP

4.5.4 Mirroring（镜像）

镜像和网络流量分析，能帮助您监控网络流量。您可以监控所选端口的发送或接收的封包。

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

Mirror Mode（镜像模式）：启用或禁用所选群组的镜像功能。

Monitor Port（监视端口）：接收所有已选的镜像端口流量的拷贝。



监视端口不能属于任何一个链路汇聚群组。

监视端口不能属于任何一个私有 VLAN。

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

点击 OK 将设置送至交换机（HTTP 服务器）。点击 Reload 将设置刷新到当前值。

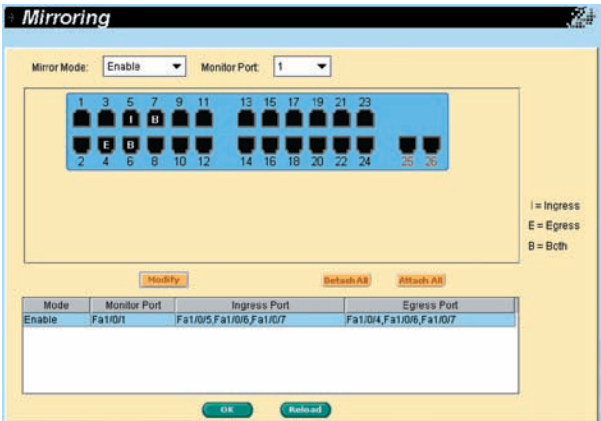


图 25. 镜像页面

4.5.5 Static multicast (静态组播)

通过这个页面您可以将组播地址添加到组播表中。本交换机可以保存最多 256 个组播地址。群组中的所有端口都会把特定的组播封包转发到群组中的其他端口。

Port: 在选择面板上选择端口。或从列表选择一个存在的群组地址，从而显示对应端口。

VLAN: 选择 VLAN 群组，这是基于 VLAN 的功能

MAC Address: 分配组播地址

CoS: 为服务等级分配优先级

点击 OK 将设置激活。点击 Reload 将设置刷新到当前值。

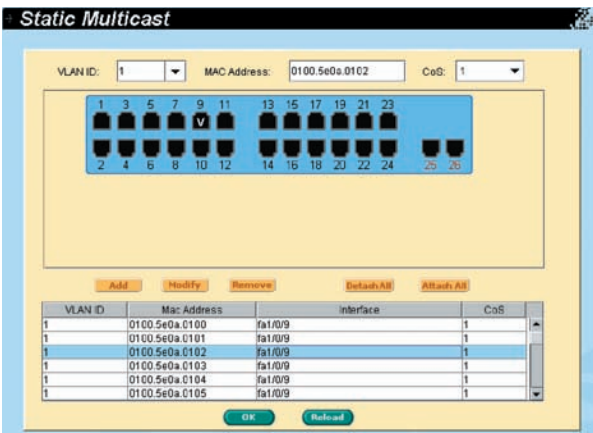


图 26. 静态组播

### 4.5.6 IGMP Snooping (IGMP 侦测)

IGMP Snooping 帮助您减少网络中的组播流量，您只需简单地开启或关闭 IGMP Snooping 功能。

第一部分您可以进行以下设置：

**Enable IGMP Snooping:** 从总体上开启所有已存在的 VLAN 界面的 IGMP Snooping 功能。在默认情况下，如果总体 IGMP Snooping 功能是开启或关闭的，则所有已存在的 VLAN 界面的这个功能也是对应开启或关闭的。

如果总体的 Snooping 功能没有开启，您无法启用 VLAN snooping。如果总体 snooping 已开启，您可以开启或关闭 VLAN snooping 功能。

**Last Member Query Interval:** 当交换机从一个接收端口成员处接收到一个 IGMP leave 信息，它会在该端口发出一个 IGMP 询问，并等待群组中其他成员回复。如果在设定的时间内没有收到回复，这个接收端口将从组播群组中移除。

第二部分您可以进行以下设置：

**Status:** 如果总体的 snooping 功能已开启，您可以开启或关闭 VLAN snooping 功能。

**Immediate leave:** 当您开启了 IGMP Immediate-Leave 功能后，交换机在接收到某端口的 IGMP version 2 leave 信息后，会立即将该端口从组播群组中移除。只有当 VLAN 中每个端口只有一个主机存在的情况下，您才能使用 Immediate-Leave 功能。只有 IGMP version 2 主机才支持 Immediate Leave 功能。

但是，如果静态地址占据了所有的 256 个地址，IGMP snoop 功能就不能正常工作。本交换机只允许 256 个二层组播群组。

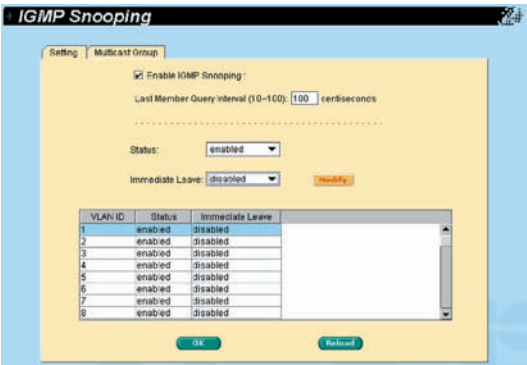


图 27. IGMP 侦测



4.5.7 Traffic control ( 流量控制 )

流量控制确保交换机的带宽不被泛洪封包，如广播封包、组播封包，以及无法找到目的地址的封包阻塞。Limit 的数值代表了封包总数的上限值。例如，如果您允许了广播和组播，这两种类型的封包流量不能超过设置的上限值。

选择一个界面进行需要的设置，然后点击 Modify。

点击 OK 保存新设置。若要让设置生效，请进入 Save Configuration 页面，然后点击 Reload。

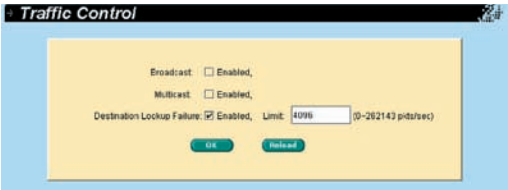


图 28. 流量控制

4.5.8 Dynamic addresses ( 动态地址 )

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

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

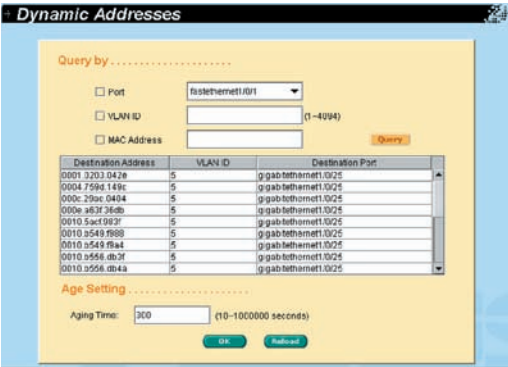


图 29. 动态地址

### 4.5.9 Static addresses (静态地址)

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

MAC Address (MAC 地址): 输入 MAC 地址

VLAN ID: 输入 MAC 地址所属的 VLAN ID

Port Selection( 端口选择 ): 选择 MAC 地址所属的端口号

点击 Add 添加新的 MAC 地址。然后您就可以看到新记录已经添加到地址窗口中。您也可以鼠标选择 MAC 地址记录, 点击 Remove 删除该条地址。Modify 按钮用于更新现存的 MAC 地址。您可以通过输入 MAC 地址和 VLAN ID, 点击 Query 来查找静态地址。点击 OK 将设置送至交换机(HTTP 服务器)。点击 Reload 刷新设置。要激活设置, 请进入 save configuration 页面按 Save。

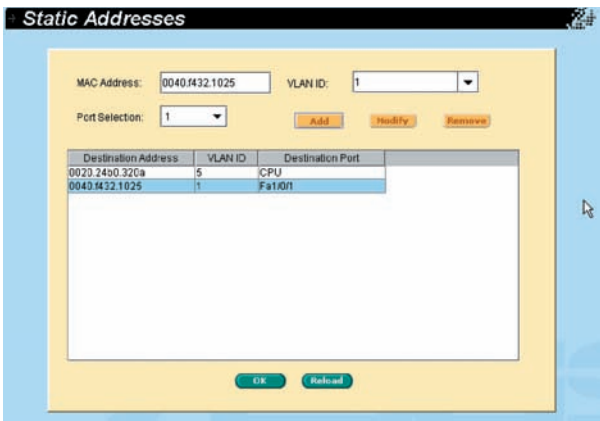


图 30. 静态地址

4.5.10 VLAN configuration (VLAN 设置 )

您可以设置 256 个 VLAN 群组并在本页中显示 VLAN 群组。VLAN1 是默认的 VLAN, 是由系统创建的, 不能被删除。这项功能可以防止交换机出错。除了默认的 VLAN1 外, 您可以删除任何其余的 VLAN。

您可以通过鼠标点击来为端口进行属性分配: 标记或不标记。一共有三种按钮显示:

“U” 型: 未标记的端口 , 将把传输的封包上的 VLAN 标记删除。

“T” 型: 从该端口传输的端口都会进行标记。

“Blank” 型: 该端口不属于 VLAN 群组。

如果一个未标记的端口同时属于两个或更多 VLAN, 就会使交换机产生混淆从而造成流量泛洪。为了防止这种情况的发生, 交换机只允许一个未标记端口只属于一个 VLAN。

如果您希望将一个未标记的端口从一个 VLAN 分配到另一个 VLAN, 您就必须将其从原来的 VLAN 中删除, 或先将其变为标记端口。

VLAN ID: 当用户创建新的 VLAN 时, 需要在这里输入 VLAN ID。

Name: 设定 VLAN 名称

DHCP-Snooping: 启用 / 禁用 VLAN 的 DHCP-Snooping 功能

点击 OK 保存设置。若要激活设置, 请进入 Save Configuration 页面点击 Save。

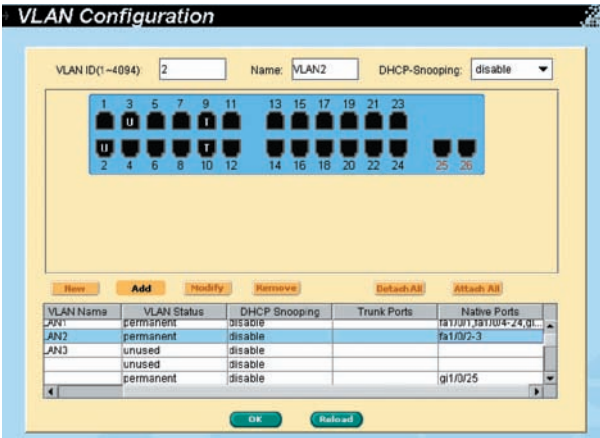


图 31. 标记 VLAN

4.5.11 GVRP

通用属性注册协议 (GARP) 中的 VLAN 注册协议 (GVRP) 是在 IEEE 802.1Q 标准中定义的一种应用，允许您对 VLAN 进行控制。

GVRP 只能在 802.1Q 链路汇聚端口使用，主要用来在 VLAN 中去除那些不需要在链路汇聚交换机之间传递的流量。GVRP 设置参数有：

**GVRP Enable:** 在默认情况下，交换机没有启用 GVRP。您必须首先启用交换机的 GVRP，然后才能设置 802.1Q 端口用于 GVRP 操作。

**Port Mode:** 在单独的 802.1Q 端口启用 / 禁用 GVRP。GVRP 需要在链路汇聚的两端进行设置，以确保其工作正常。

**Registration:** 默认情况下，GVRP 端口处于一般注册 (Normal Registration) 模式。这些端口使用 GVRP 协议，在 802.1Q 链路中修剪从邻近的的交换机上获得的 VLAN 信息。如果另一端的设备不能发送 GVRP 信息，或您不想让交换机修剪任何 VLAN 信息，请使用 fixed 模式。Fixed 模式端口将转发所有存在于交换机数据库内的 VLAN。Forbidden 模式下的端口只转发 VLAN 1。

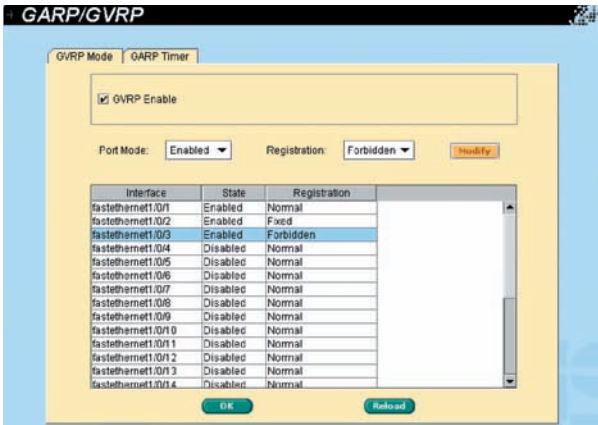


图 32. GVRP

根据需要修改下列属性:

**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。

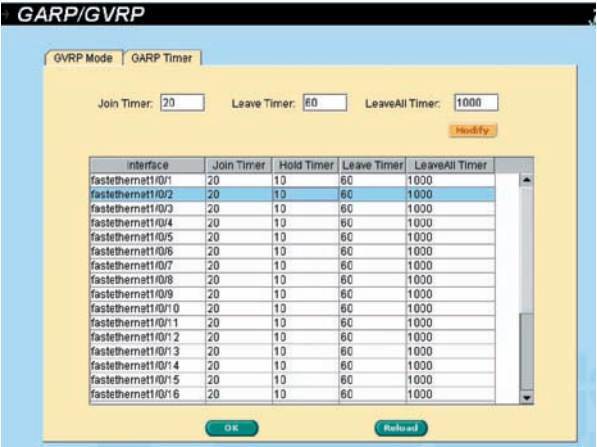


图 33. GARP 定时器

4.5.12 QoS 和 CoS

4.5.12.1 802.1p priority (802.1p 优先级 )

交换机的所有端口有八个出口队列。这些队列可以通过加权轮转 (WRR) 调度算法进行设置或将一个队列设为 Strict priority queue (绝对优先队列)，其他队列按照 WRR 算法进行设置。绝对优先队列在其他队列得到服务之前必须为空。您可以用绝对优先队列传输关键的或有很强时效性的信息流量。这里有三个选项:

- First Come First Service: 最先到达的帧具有最高的优先级
- High Priority First: 封包的优先级取决于她的 CoS 值
- Weighted Round Robin (WRR): 如果启用了 WRR 调度算法，权重的比例就是每个队列中 WRR 调度的封包被传送频率的比例。

点击 OK 保存设置。若要激活设置，进入 Save Configuration 页面后然后点击 Save。

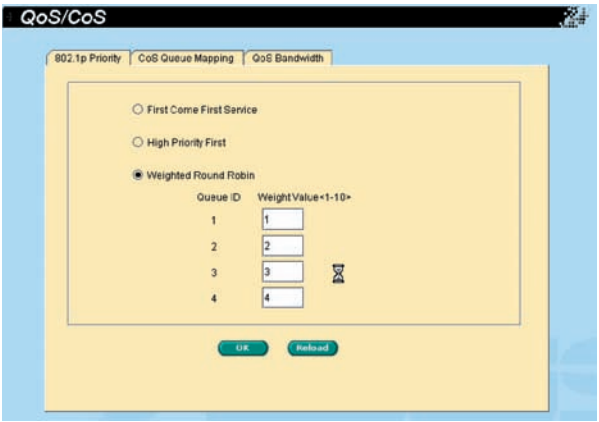


图 34. 802.1p 优先级

#### 4.5.12.2 CoS queue mapping (CoS 队列映射)

本交换机支持每端口四个 Strict priority (绝对优先) 算法的出口队列。也就是说, 每一个 CoS 值都可以映射到四个队列之一。对于 strict priority 调度来说, 队列四在传输封包时具有最高的优先级。点击 OK 保存设置。若要激活设置, 进入 Save Configuration 页面后然后点击 Save。

CoS 值从 0 到 4, 0 代表最低优先级, 而 4 代表最高优先级。

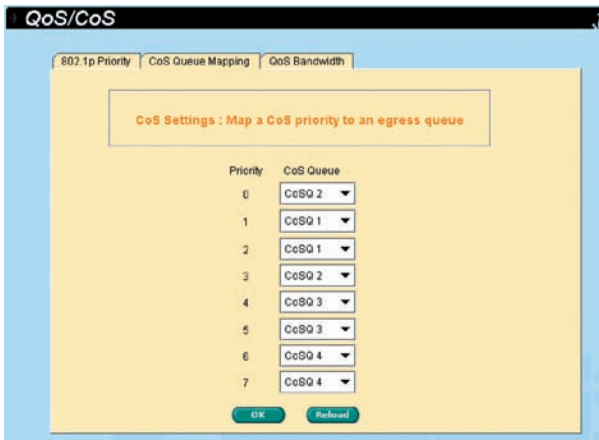


图 35. CoS 队列

### 4.5.12.3 QoS bandwidth (QoS 带宽)

这个页面包含了每个端口与标记 VLAN 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:** 所选端口的最大入口带宽

**Default CoS:** 从这个端口接收的所有未标记封包都将在标记 VLAN 中被分配这个 CoS 值

点击 **Modify** 更改端口列表窗口中的内容。点击 **OK** 保存设置。若要激活设置，进入 **Save Configuration** 页面后然后点击 **Save**。

**QoS/CoS**

802.1p Priority | CoS Queue Mapping | **QoS Bandwidth**

Ingress Bandwidth: 10 (0-1000Mbps) Default CoS: 1 Modify

Interface	Ingress Bandwidth	Egress Bandwidth	Default CoS
FastEthernet1/0/1	0	0	0
FastEthernet1/0/2	10	0	1
FastEthernet1/0/3	0	0	0
FastEthernet1/0/4	0	0	0
FastEthernet1/0/5	0	0	0
FastEthernet1/0/6	0	0	0
FastEthernet1/0/7	0	0	0
FastEthernet1/0/8	0	0	0
FastEthernet1/0/9	0	0	0
FastEthernet1/0/10	0	0	0
FastEthernet1/0/11	0	0	0
FastEthernet1/0/12	0	0	0
FastEthernet1/0/13	0	0	0

OK Reload

图 36. QoS 带宽

## 4.6 SNMP

本群组提供 SNMP(简单网络管理协议)设置,内容包括 Community Table(团体列表), Host Table(主机列表),以及 Trap Setting(Trap 设置)。

### 4.6.1 Community table (团体列表)

您可以键入不同的团体名并指定该团体是否具有设置(写操作)的权限。点击 OK 永久保存设置,点击 Reload 刷新页面。



The image shows a web-based configuration interface titled "Community Table". It features a table with two columns: "Community Names" and "Set". The "Community Names" column contains text input fields, with "public" and "private" already entered. The "Set" column contains checkboxes. The checkbox for "private" is checked, while the others are unchecked. At the bottom of the table, there are two green buttons: "OK" and "Reload".

Community Names	Set
public	<input type="checkbox"/>
private	<input checked="" type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

OK Reload

图 37. 团体列表



### 4.6.2 Host table (主机列表)

本页面将主机 IP 地址与 Community Table 页面中设置的团体名称联系在一起。键入一个 IP 地址并从下拉菜单中选择团体名称。点击 OK 永久保存设置，或点击 Reload 刷新页面。



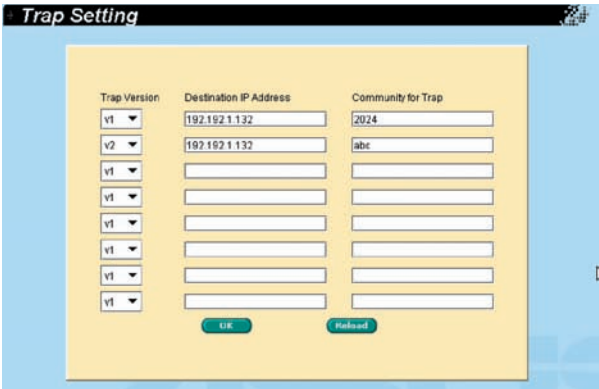
The 'Host Table' configuration window shows a table with two columns: 'Host IP Address' and 'Community'. The first row has '0.0.0.0' and 'public'. The second row has '127.0.0.1' and 'private'. There are four more rows with empty IP fields and 'public' in the community dropdown. At the bottom are 'OK' and 'Reload' buttons.

Host IP Address	Community
0.0.0.0	public
127.0.0.1	private
	public
	public
	public
	public
	public
	public

图 38. 主机列表

### 4.6.3 Trap setting (Trap 设置)

通过设置 trap 目的 IP 地址和团体名称，您可以启用 SNMP trap 功能来发送不同版本的 trap 封包 (v1 or v2c)。点击 OK 保存设置；点击 Reload 刷新页面。



The 'Trap Setting' configuration window shows a table with three columns: 'Trap Version', 'Destination IP Address', and 'Community for Trap'. The first row has 'v1', '192.162.1.132', and '2024'. The second row has 'v2', '192.162.1.132', and 'abc'. There are five more rows with empty fields. At the bottom are 'OK' and 'Reload' buttons.

Trap Version	Destination IP Address	Community for Trap
v1	192.162.1.132	2024
v2	192.162.1.132	abc
v1		
v1		
v1		
v1		
v1		
v1		

图 39. Trap 设置

### 4.6.4 SNMPv3 VGU table (SNMPv3 VGU 列表 )

有两篇论文介绍了 SNMPv3 定义的这种新的安全特色。基于用户的安全模型 (USM), 提供了 SNMPv3 封包的身份验证、加密和解密。基于视图的访问控制模型 (VACM), 提供了访问控制。以下是相关的三个页面。点击 OK 保存设置; 点击 Reload 刷新页面。

#### 4.6.4.1 VACM view (VACM 视图 )

VACM 视图用来查看 SNMPV3 VACM 群组的信息。

View Name: 输入安全群组的名称

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

View Subtree: 输入 View 子树。子树就是用于配对 SNMPv3 信息的 Oid 的 Oid。当子树长度小于 SNMPv3 信息中的 Oid, 配对即成功。

点击 Add 添加一条新的 VACM View 记录, 随后您就会在视图窗口看到这条记录。您可以用鼠标选中一条记录, 点击 Remove 删除该记录。Modify 按钮则用于更新既存的 VACM View 记录。点击 OK 保存设置; 点击 Reload 刷新设置到当前值。要激活设置, 请进入 Save Configuration 页面并点击 Save。

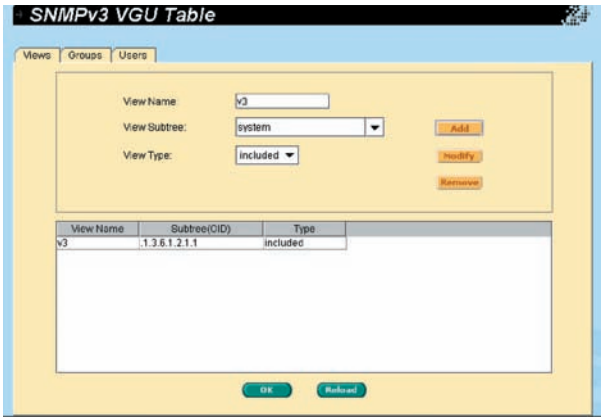


图 40. SNMPv3 VGU 表 1

4.6.4.2 VACM group (VACM 群组 )

VACM 群组用来设置 SNMPV3 VACM 群组信息。

- Group Name ( 群组名称 ) : 输入安全群组名称。
- Read View Name ( 读取视图名 ) : 输入群组隶属的读取视图名称 , 与其相关的 SNMP 消息为 Get,GetNext,GetBulk。
- Write View Name ( 写入视图名 ) : 输入群组隶属的写入视图名称 , 与其相关的 SNMP 消息为 Set。
- Notify View Name ( 通知视图名 ) : 输入群组隶属的通知视图名称 , 与其相关的 SNMP 消息为 Trap,Report..
- Security Model ( 安全模型 ) : 输入群组隶属的安全模型 , Any 适用于 v1,v2,v3。 USM 与 SNMPv3 相关。
- Security level ( 安全等级 ) : 输入群组隶属的安全等级 , 选项只有 NoAuth, AuthNopriv, AuthPriv。

输入上述信息后, 点击 Add 新增一个新的 VACM 群组。然后您就可以在群组窗口中看到新增的记录。您可以通过鼠标选中记录, 点击 Remove 删除一条记录。Modify 按钮用更新现有的 VACM 群组。点击 OK 进行保存; 点击 Reload 刷新页面; 若要激活设置, 请进入 Save Configuration 页面并点击 Save。

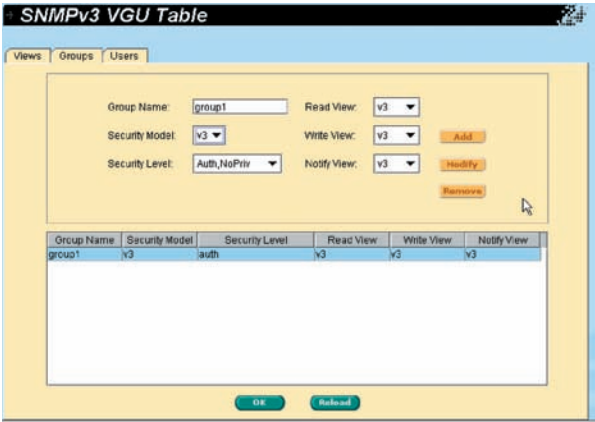


图 41. SNMPv3 VGU 表 2

4.6.4.3 USM user (USM 用户)

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

User Name: 特定的安全群组的用户名

Group Name: 输入安全群组的名称

Auth Protocol: 输入 SNMP 用户和安全群组隶属的认证协议 (Auth Protocol)。选项只有 NoAuth ,MD5, SHA1。如果选择 NoAuth 就不必输入密码。

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

Priv Protocol: 输入 SNMP 用户和安全群组隶属的 Priv 协议。选项只有 NoPriv 和 DES。如果选择 NoPriv, 就无须输入密码。

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

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

输入上述信息后, 点击 Add 添加一条新的 USM 用户记录, 随后您就会在视图窗口看到这条记录。您可以选中一条用户记录, 点 Remove 删除该记录。Modify 按钮则用于更新既存的 VACM 视图记录。点击 OK 保存设置; 点击 Reload 刷新设置到当前值。要激活设置, 请进入 Save Configuration 页面并点击 Save。

SNMPv3 VGU Table

ViewsGroupsUsers

User Name:asusGroup Name:group1Security Level:AuthPrivAuth Algorithm:MD5Auth Password:\*\*\*\*\*Priv Algorithm:DESPriv Password:\*\*\*\*\*AddModifyRemove

User Name	Group Name	Authentication Algorithm	Private Algorithm
asus	group1	MD5	DES

OKReload

图 42. SNMPv3 VGU 表 3

## 4.7 Filter 页面

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

### 4.7.1 Filter set (过滤集)

本交换机定义了两种模式的规则，一种是 MAC 模式，另一种是 IP 模式。只有相同模式的规则才能在一起构成一个过滤集。每种模式都有不同的项目需要设置。例如，您可以使用 IP 模式规则来过滤 FTP 封包。

您可以选择 **MAC Filter** 并命名，然后点击 **Add** 进行添加。您也可以选择 **IP Filter**，填入 ID/Name，然后点击 **Add**。点击 **OK** 永久保存设置，或点击 **Reload** 刷新页面。在编辑之前请先点击 **OK**。

点击您要编辑或删除的过滤集。然后点击 **Edit** 进入规则页面，或点击 **Remove** 删除过滤集。您必须按照规则设置有效的过滤集。

一个集由一个类型的规则组成。这些在相同范围内过滤封包的规则都属于一个类型。例如，两个规则都通过目的地 IP 地址过滤封包，则它们输入同一类型。但是通过源 IP 地址过滤封包的规则就不属于同一个类型。

一个端口可以同时应用四种类型的规则。如果为端口分配了四种以上的规则，系统会自动禁用这些规则。

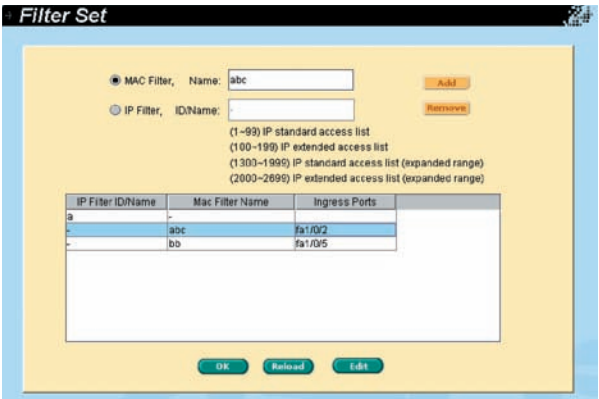


图 43. 过滤集

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

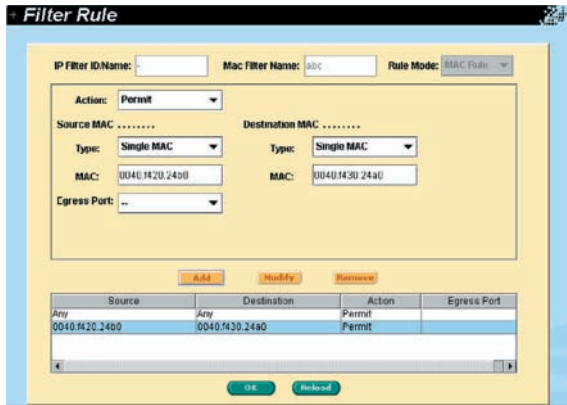


图 44. MAC 模式下的过滤规则

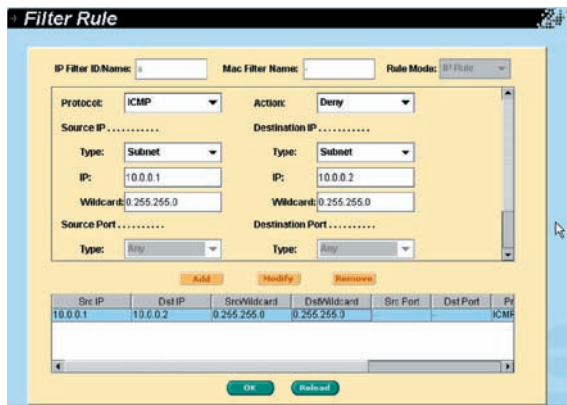


图 45. IP 模式下的过滤规则

以下是两个例子：

1. 指定一个专用的 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 Filter attach (过滤规则分配)

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

点击 OK 保存设置。要激活设置，请进入 Save Configuration 页面并点击 Save，或点击 Reload 刷新页面。

请按照以下说明将过滤设置分配到端口：

Attach to all ports (分配给所有端口)：这个过滤规则将应用到系统中的所有端口。

Attach to certain ports (分配给指定的端口)：您可以将规则分配给指定的端口。

Detach from all ports (从端口删除)：将规则从已分配的端口上删除。



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

当过滤规则分配到入口端口之后，它将根据入口端口和规则中的封包范围进行封包过滤。例如，一个过滤设置是一个单一规则，即过滤进入端口 3 的所有目的地 MAC 地址为 00:10:20:30:40:50 的封包。那么从端口 3 进入的目的地的 MAC 地址为 00:10:20:30:40:50 的封包就会被禁止。

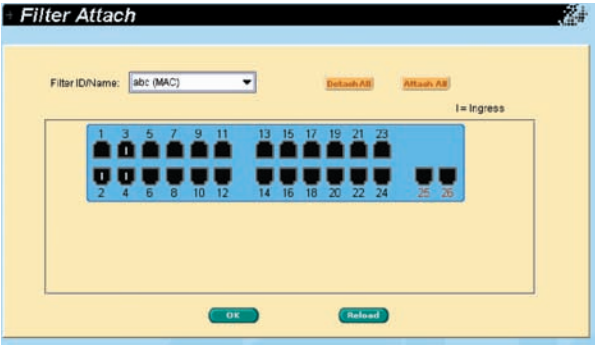


图 46. 过滤规则分配

## 4.8 安全

---

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

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

### 4.8.1 Port access control ( 端口访问控制 )

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

第一部分为桥接 (Global) 设置：

**Sys-Auth-Control:** 勾选这项以允许认证。

**Authentication Method ( 认证方式 ):** 可以使用 RADIUS 或本地数据库进行端口用户认证。

第二部分为端口设置。当您修改完设置后，请点击 **Modify**：

**Port ( 端口 ):** 从端口列表窗口中指定需要设置哪个端口。

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

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

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

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

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

**Retransmission Time ( 重传时间 ):** 如果端口用户没有响应交换机的认证请求，交换机将在再次发送请求前等待一端时间。



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

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

点击 OK 永久保存设置。点击 Reload 刷新设置。

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

Retransmission Time:  (1-65535) Sec

Max Reauthenth Attempt:  (1-10)

Guest Vlan: disable (1-4094)

Apply

Interface	Status	Host Mode	AuthCtrl	ReAuth	ReAuth-Time	Tx-Tim
fastEthernet1/0/1	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/2	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/3	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/4	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/5	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/6	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/7	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/8	authorized	single-host	force-authorized	disable	3600	30
fastEthernet1/0/9	authorized	single-host	force-authorized	disable	3600	30

OK

Reload

图 47. 端口访问控制

## 4.8.2 Dial-in user ( 拨入用户 )

Dial-in User 用于定义处于交换机本地的用户。

User Name: 新的用户名。

Password: 新用户的密码。

Confirm Password: 再次输入密码。

Vlan ID: 指定分配给 802.1x 认证用户的 VLAN ID。

点击 Add 添加新的用户，修改完毕后点击 Modify。要删除用户时，选中该用户后点击 Remove。点击 OK 永久使用该设置。点击 Reload 刷新设置到当前值。

**Dial-in User**

User Name:

Password:

Confirm Password:

Vlan ID:  (1-4094)

UserName	Password	Vlan ID
asus	*****	1

图 48. 拨入用户

### 4.8.3 RADIUS

为了使用外部 RADIUS 服务器，下列参数须进行设置：

Authentication Server IP: RADIUS 服务器 IP 地址。

Authentication Server Port: RADIUS 侦听的端口号。

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

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



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

点击 OK 永久使用该设置。点击 Reload 刷新设置到当前值。

**RADIUS**

Authentication Primary-Server IP: 192.192.1.132

Authentication Primary-Server Port: 1812

Authentication Primary-Server Key: \*\*\*\*\*

Confirm Authentication Key: \*\*\*\*\*

Authentication Secondary-Server IP: 192.192.1.131

Authentication Secondary-Server Port: 1812

Authentication Secondary-Server Key: \*\*\*\*\*

Confirm Authentication Key: \*\*\*\*\*

OK Reload

图 49. RADIUS

## 4.8.4 端口安全

本交换机还支持端口安全功能。这一功能允许系统管理员控制谁可以连接到他们的网络。使用端口安全功能，您可以通过禁止或指定可访问该端口的基站的 MAC 地址来限制一个界面的输入量。当您为一个安全端口分配了一个安全 MAC 地址后，这个端口不会转发除了已定义的源地址群组之外的其他封包。这样就降低了未经过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 Port configuration ( 端口配置 )

这个页面用来进行端口安全配置。

首先，从下面的列表中点击需要设置的端口，将其选中。然后开始进行端口配置。更改完成后请点击 **Modify**。

- a) **Admin:** 启用或禁用安全功能。
- b) **Violation Mode:** 当与安全规则相违背时决定端口行为。若选择“Shutdown”，端口将变为阻塞状态，同时系统将记录日志信息，并相应增加 Violation 计数器的数值。若选择“Restrict”，系统将会记录日志信息，并相应增加 Violation 计数器的数值。若选择“Protect”，系统将不会通知您发生了违背规则的事件。
- c) **Max MAC Address:** 这个端口允许的安全 MAC 地址数量的最大值。这个值的范围为 1 ~ 132，系统中的总数为 1024。
- d) **Aging Time:** 端口的老化时间。当超过了一定时间后，相应的动态安全 MAC 地址将会从安全 MAC 地址表中删除。这个值的有效范围是 0 ~ 1440( 分钟 )。如果时间值为 0，则代表端口禁用老化机制。
- e) **Aging Type:** 老化类型决定了当安全 MAC 地址过期时的对应动作。若选择“Absolute”，在指定的老化时间结束后，端口的安全地址会被删除。若选择“Inactivity”，只有在指定时间内安全源 MAC 地址没有数据流量的情况下才将该地址删除。

点击 **OK** 永久保存设置。点击 **Reload** 刷新设置到当前值。

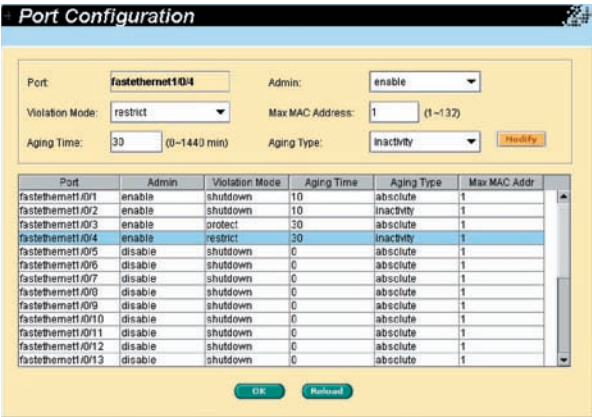


图 50. 端口安全

4.8.4.2 Port status ( 端口状态 )

这个页面显示了当前的端口状态，MAC 地址数和 violation（违背规则的事件）数目。

端口具有五种状态：

- a) NoOper: 表示本端口的端口安全设置为禁用。
- b) SecureUp: 表示端口安全正在运行。
- c) SecureDown: 表示端口安全没有运行。此时端口安全设置为启用，但是因为某些原因（如与其他功能冲突）而未能启用。
- d) Restrict: 表示当 violation mode 为 “restrict” 时，端口出现端口安全违背事件。
- e) Shutdown: 表示当 violation mode 为 “shutdown” 时，端口因为端口安全违背事件而阻塞。

当某些端口状态为 “Shutdown” 时，您可以点击这个端口然后将 “Re-Start” 设为 “Yes”。这个操作会将重新启动端口并将端口装载设置为 “SecureUp”。当您完成修改后，请点击 Modify。

点击 OK 永久保存设置。点击 Reload 刷新设置到当前值。

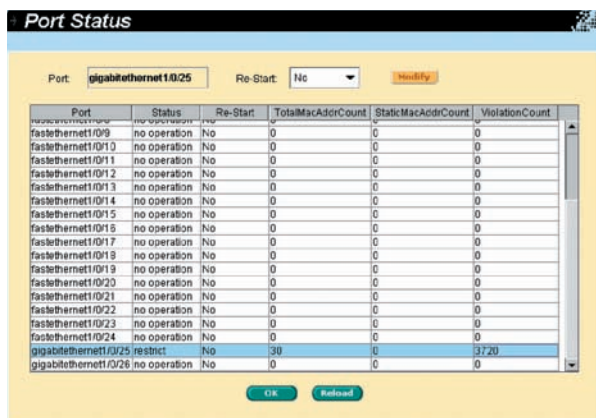


图 51. 端口状态

#### 4.8.4.3 Secure MAC Address (安全 MAC 地址)

安全 MAC 地址为用户的管理提供了三种功能:

- Query:** 您可以在“Port Selection”区域选择某个端口。点击“Query”按钮，将显示该端口上的所有 MAC 地址。
- Add:** 用户可以在“Port Selection”区域选择某个端口，然后在“MAC Address”区域内输入一个 MAC 地址。点击“Add”按钮后，这个 MAC 地址将添加到选定的端口，且 MAC 地址的类型为静态地址。
- Remove:** 您可以使用“Query”功能来显示某个端口上的所有 MAC 地址。从列表总选择一个 MAC 地址，然后点击“Remove”按钮，这个地址将立刻被删除。

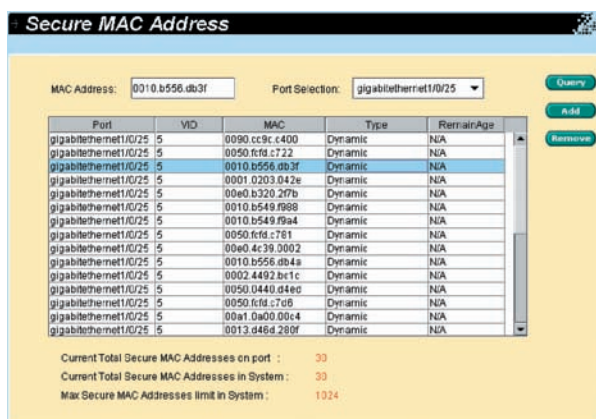


图 52. 安全 MAC 地址

## 4.9 Traffic chart ( 流量图表 )

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

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

### 4.9.1 Traffic comparison ( 流量比较 )

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

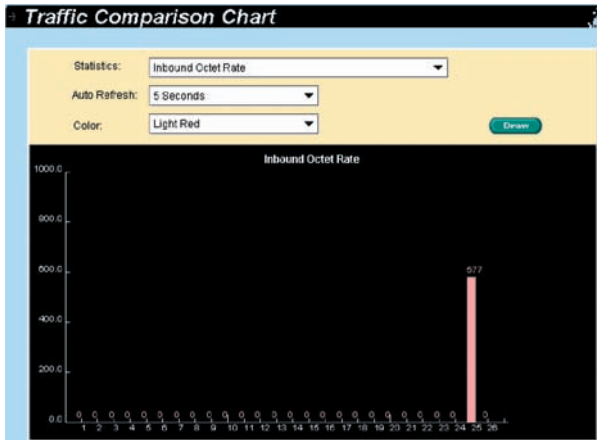


图 53. 流量比较

#### 4.9.2 Error group chart ( 错误分组 )

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

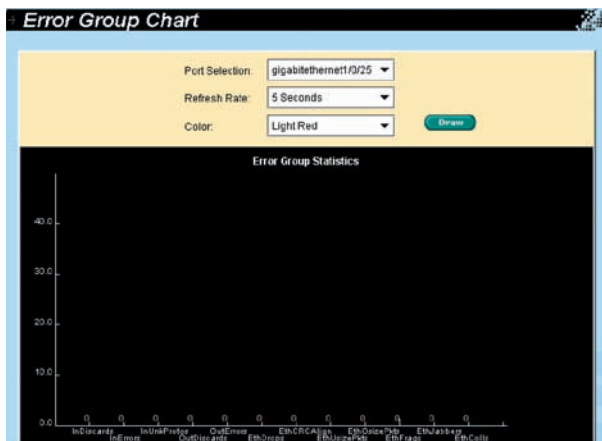


图 54. 错误分组

### 4.9.3 Historical status (历史状态)

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

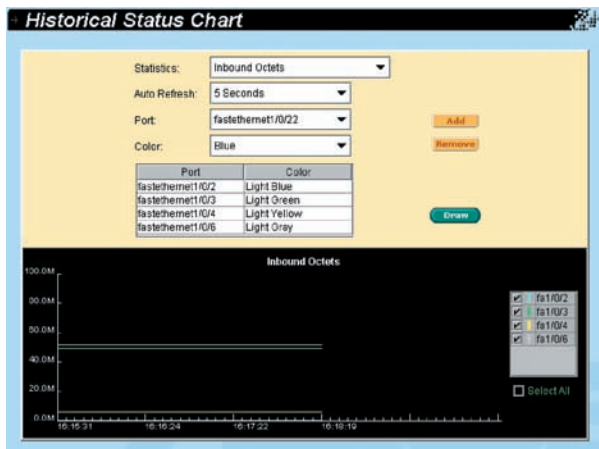


图 55. 历史状态



## 4.10 Cable diagnosis ( 缆线诊断 )

本页面用来分析缆线设备故障，例如开路、短路和阻抗不匹配。



图 56. 缆线诊断

## 4.11 Save configuration ( 保存设置 )

要永久保存设置，您需要点击 Save。

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



当恢复出厂设置时，所有的设置均会丢失。



图 57. 保存设置

## 5 控制终端界面

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

当您进入命令行模式, 键入 “?”, 屏幕将显示所有可以使用的命令的帮助信息。如果您对命令行不熟悉, 这将是一个相当有用的帮手。所有的命令行命令都区分大小写。

### 5.1 开机自检

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

```
ASUS login: admin
Password:
ASUS GigaX 2024B 3.2.02.00 Copyright (c) 2005

ASUS> enable
ASUS# _
```

图 58. 命令行界面

#### 5.1.1 Boot ROM 命令模式

在开机自检的过程中, 按下 <ENTER> 可以进入 “Boot ROM Command” 模式, 键入 “?” 显示所有可以使用命令的帮助信息。



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

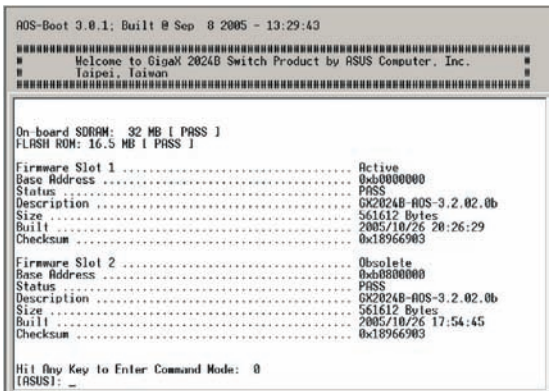


图 59. Boot ROM 命令模式

5.1.2 Boot ROM 命令

以下是两种类型的 boot ROM 命令:

- 命令: 将显示当前设置。
- 带有新设置的命令: 指定的新设置将取代当前设置。

表 7. Boot ROM 命令

命令	参数	参数举例	用途
baudrate	Baud rate	9600, 38400, 57600, 115200	您需要将终端仿真器设置为相同的波特率。
ethaddr	none	none	获得 MAC address
gatewayip	IP address	xxx.xxx.xxx.xxx	设置网关的 IP 地址
go	none	none	启动固件 image
? or help	none	none	显示线上帮助
ipaddr	IP address	xxx.xxx.xxx.xxx	设置 TFTP 客户端 IP 地址
xload	none	none	通过串行线载入二进制文件 (X modem)
netmask	mask	xxx.xxx.xxx.xxx	设置网络掩码
ping	host	xxx.xxx.xxx.xxx	将 ICMP echo 请求发送到主机
pwd	none	none	重设交换机密码
serverip	IP address	xxx.xxx.xxx.xxx	设置 TFTP 服务器 IP 地址
slot	slot	1, 2, auto	选择启动方式
tftpboot	filename	xxx.img	通过网络上的 TFTP 协议下载固件
version	none	none	显示版本号

## 5.2 登录和注销

---

要进入命令行模式，你必须输入一个有效的用户名和密码。当您第一次登录时，用户名为“admin”，密码为空。为了安全考虑，请在登录后立刻修改密码。如果您忘记了用户名和密码，请与华硕技术支持人员联系，或在 Boot ROM 命令模式中使用“pwd”命令恢复初始用户帐号。如果您选择第二种方式，那么用户名将恢复到默认值“admin”。

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

## 5.3 CLI 命令

---

GigaX 2024B 交换机提供 CLI 命令来设置所有的网管功能。这样，您就能根据提示像使用网页界面一样正确而轻松地设置交换机。



请使用“?”或“list”来获取可使用命令列表和帮助信息。

请使用“end”来返回根目录（enable 模式）。

### 5.3.1 用户帐户

#### 5.3.1.1 新增用户

用来新增用户或修改已存在用户的密码。

命令：add user user-name password

例：ASUS# user add admin 123

#### 5.3.1.2 删除用户

删除一个存在的用户。

命令：delete user user-name

例：ASUS# user delete admin

### 5.3.2 备份和恢复

#### 5.3.2.1 备份启动设置文件

将交换机的启动设置文件“startup\_config”备份到 TFTP 服务器。

命令: copy startup-config tftp: URL

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

### 5.3.2.2 恢复启动设置文件

从 TFTP 服务器恢复交换机的启动设置文件 “startup\_config”。

命令: copy tftp: URL startup-config

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

## 5.3.3 系统管理设置

### 5.3.3.1 固件升级

升级交换机的固件。

命令: archive download-sw /overwrite tftp: ImageFile

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

### 5.3.3.2 configure terminal

使用交换机的 write 设置命令进行设置。

命令: configure terminal

例: ASUS# configure terminal

### 5.3.3.3 enable

进入 enable 模式，开启特权模式命令。

命令: enable

例: ASUS# enable

### 5.3.3.4 disable

关闭特权模式，返回用户模式。

命令: disable

例: ASUS# disable

#### 5.3.3.5 end

这条命令让用户结束当前模式进入 enable 模式。

命令：end

例：ASUS# end

#### 5.3.3.6 exit

这条命令让用户退出当前模式，进入上一个模式。

命令：exit

例：ASUS# exit

#### 5.3.3.7 help

显示运行模式下的所有命令。

命令：list

例：ASUS# list

例：ASUS# ?

#### 5.3.3.8 host name (主机名)

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

命令：hostname WORD

例：(config)# hostname Switch

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

#### 5.3.3.9 System contact (系统联系信息)

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

命令：snmp-server contact DWORD

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

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


### 5.3.3.10 System Location (系统位置)

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

命令：snmp-server location DWORD

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

在 system location description 键入地点描述即更新地点信息。



```
Switch# configure terminal
Switch(config)# hostname Switch
Switch(config)# snmp-server contact my_contact_information
Switch(config)# snmp-server location enterprise_building_B1
Switch(config)#
```

图 60. 系统命令

### 5.3.3.11 IP 地址和网络掩码

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

命令：ip address A.B.C.D/M

例：(config)# interface vlan 1

(config-if)# ip address 192.168.20.121/24

### 5.3.3.12 Default gateway (默认网关)

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

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

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

### 5.3.3.13 reboot (重新启动)

使用这条命令重新启动系统。

命令：reboot

例：reboot

#### 5.3.3.14 reload default-config file

这条命令用来复制默认的设置文件来取代现有文件。

命令 : reload default-config file

例 : ASUS# reload default-config file

#### 5.3.3.15 show running-config

显示 running-config 文件。

命令 : show running-config

例 : ASUS# show running-config

#### 5.3.3.16 write

使用文件设置命令 write 将设置写入单个或一组交换机中的文件。

命令 : write

例 : ASUS# write

#### 5.3.3.17 分配一个新的用户帐户

新增一个用户，用户名为 tony，密码为 tony123456

命令 : user add WORD WORD

例 : user add tony tony123456

#### 5.3.3.18 删除一个用户帐户

删除一个名称为 tony 的帐户。

命令 : user delete WORD

例 : user delete tony



### 5.3.4 物理端口命令

#### 5.3.4.1 端口模式

使用交换机的 `auto-negotiation` 命令来设置端口的自动协商状态。

命令：`auto-negotiation`

例：(config)# interface fa1/0/2  
(config-if)# auto-negotiation

这个例子说明了如何使用 `auto-negotiation` 设置命令来启用自动协商模式。

#### 5.3.4.2 端口双工模式

使用 `duplex` 命令设置端口的双工状态。

命令：`duplex (full | half)`

例：(config)# interface fa1/0/2  
(config-if)# duplex full

这个例子说明了如何使用 `duplex` 设置命令将端口设置为全双工模式。

#### 5.3.4.3 界面流量控制

使用 `flowcontrol` 命令来设置端口的流量控制状态。

命令：`flowcontrol (rx | tx | both)`

例：(config)# interface fa1/0/2  
(config-if)# flowcontrol both

这个例子说明了如何使用 `flow control` 设置命令同时开启端口的发送和接收流量控制。

#### 5.3.4.4 show L2 interface

使用 `show interface` 命令显示界面状态。

命令：`show interfaces IFNAME`

例：ASUS# show interface fa1/0/2

### 5.3.5 IP 界面

#### 5.3.5.1 show vlan name string

使用 show vlan user EXEC 命令显示所有已设置的 VLAN 或一组 VLAN（如果指定了 VLAN ID 或名称）的参数。

命令：show vlan name string

例：ASUS# show vlan name VLAN1



*vlan1 用于系统用途，例如，固件升级、管理等。*

#### 5.3.5.2 创建一个 vlan

使用 vlan vid 命令创建一个新的 vlan。Use the name string command to create vlan entry with string on the switch.

命令：vlan id

例：(config)# vlan 3

(config-vlan)# name vlan3

#### 5.3.5.3 interface vlan VLAN-ID

这条命令将操作改为 vlan interface 命令模式。

命令：interface vlan VLAN-ID

例：interface vlan 1

#### 5.3.5.4 ip address

这条命令为指定界面设置 IP 地址。

命令：ip address A.B.C.D/M

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



*界面的名称在设置过程中不会显示。请记住您设置的内容。*

### 5.3.5.5 ip dhcp client

这条命令用来设置系统界面，以通过 DHCP 服务器获得 IP 地址。

命令：ip dhcp client

例：(config-if)#ip dhcp client

### 5.3.5.6 ip route

这条命令用来设置系统中的 IP 路由。

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

例：(config)# ip route 192.168.20.0 255.255.255.0 192.168.20.1

## 5.3.6 生成树

### 5.3.6.1 show spanning-tree summary

显示生成树。

命令：show spanning-tree summary

例：ASUS# show spanning-tree summary

### 5.3.6.2 spanning-tree enable/disable

允许 / 禁止生成树。

命令：spanning-tree (enable|disable)

例：ASUS# spanning-tree disable

## 5.3.7 链路汇聚

### 5.3.7.1 干线群组

使用链路汇聚干线群组设置命令来设置干线群组。

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

例：ASUS#aggregation-link group 1 fa1/0/1-3

### 5.3.7.2 干线负载均衡

使用链路汇聚群组设置命令，通过采用基于源地址或目的地址的转发方式来实现干线负载均衡。

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

**例：**ASUS#aggregation-link group 1 load-balance src-mac

### 5.3.7.3 show aggregation-link trunk

显示链路汇聚干线状态。

**命令：**show aggregation-link group [GROUPID]

**例：**ASUS# show aggregation-link group 1

## 5.3.8 LACP

### 5.3.8.1 lacp 汇聚链路

这条命令用来进行链路汇聚控制协议（LACP）新增 / 设置端口的干线群组的操作。

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

**例：**ASUS# lacp aggregation-link group1 add fa1/0/1-3

### 5.3.8.2 禁用 lacp 汇聚链路

这条命令用来进行链路汇聚控制协议（LACP）新增 / 设置或禁止端口的干线群组的操作。

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

**例：**ASUS# no lacp aggregation-link group 1

### 5.3.8.3 lacp system-priority

这条命令用来为链路汇聚控制协议（LACP）设置系统优先级。

**命令：**lacp system-priority <1-65535>

**例：**(config)# lacp system-priority 20000

## 5.3.9 镜像

### 5.3.9.1 镜像设置

这个命令将源界面列表流量镜像到目的界面。支持的镜像类型有接收流量、发送流量或两者。

命令：mirror session 1 source IFLIST (both/ rx/ tx)  
mirror session 1 destination IFNAME

例：(config)# mirror session 1 source fa1/0/1-4 both  
(config)# mirror session 1 destination fa1/0/5

### 5.3.9.2 Show mirror

显示当前的镜像功能。

命令：Show mirror session  
例：ASUS# show mirror session

### 5.3.9.3 No mirror

这条命令用来禁止镜像功能。

命令：no mirror session 1  
例：(config)# no mirror session 1

### 5.3.9.4 No mirror

这条命令用来重置源界面的接收或发送流量或两者的目的界面。

命令：no mirror session 1 source IFLIST  
例：(config)# no mirror session 1 source fa1/0/1-2

## 5.3.10 静态组播

### 5.3.10.1 mac-address-table multicast

使用 mac-address-table multicast 设置命令，在 MAC 地址表中添加组播静态地址。

命令：mac-address-table multicast MACADDR VLANID IFLIST  
例：(config)# mac-address-table multicast 0100.5e11.1111 2 fa1/0/1-3

### 5.3.10.2 no mac-address-table multicast

使用 no mac-address-table multicast 设置命令来删除 MAC 地址表中的组播静态端口。

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

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

### 5.3.10.3 show mac-address-table multicast

使用 show mac-address-table multicast 用户 EXEC 命令可以显示所有 VLAN 的二层组播项目。在特权模式中使用这条命令可以显示指定的组播项目。

命令：show mac-address-table multicast

例：ASUS# show mac-address-table multicast

## 5.3.11 IGMP 侦测

### 5.3.11.1 ip igmp snooping

这条命令从总体上启用 IGMP 侦测功能。

命令：ip igmp snooping

例：(config)# ip igmp snooping

### 5.3.11.2 间隔时间

这条命令用来设置交换机发出的 IGMP 询问的间隔时间。

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

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

## 5.3.12 流量控制

### 5.3.12.1 storm-control

使用 storm-control 设置命令可以设置交换机总的带宽中用于广播 /dlf/ 组播的速度上限值。

命令：storm-control (broadcast|dlf|multicast) LIMIT\_RATE

例：(config)# storm-control broadcast 25

### 5.3.12.2 no storm-control

使用 no storm-control 设置命令可以取消交换机总带宽中用于广播 /dlf/ 组播的速度限制。

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

**例：**(config-if)# no storm-control broadcast

### 5.3.12.3 show storm-control

使用 show storm-control 设置命令来显示交换机总带宽中用于广播 /dlf/ 组播的速度上限值。

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

**例：**ASUS# show storm-control broadcast

## 5.3.13 动态地址

### 5.3.13.1 clear dynamic mac-address

使用这条命令可以清除数据库中的动态二层 MAC 地址。

**命令：**clear mac-address-table dynamic mac MAC\_ADDR

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

### 5.3.13.2 aging time

使用 mac-address-table aging-time 设置命令可以在单独的或一组交换机上设置动态地址在使用或更新后，存在于 MAC 地址表中的最长时间。

真正的 aging-time（老化时间）是命令中输入数值的三倍。

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

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

这个例子显示了如何将 mac-address-table aging-time（MAC 地址表老化时间）设置为 300 秒。

### 5.3.13.3 no aging time

禁止使用 mac-address-table（MAC 地址表）老化计时器。

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

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

#### 5.3.13.4 show mac-address-table aging-time

命令 : show mac-address-table aging-time

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

### 5.3.14 静态地址

#### 5.3.14.1 新增静态 MAC 地址

您可以新增 MAC 地址到交换机的地址表。通过这种方式新增的地址不会老化。我们称其为静态地址。

命令 : mac-address-table static MAC\_ADDR VLANID IFNAME

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

#### 5.3.14.2 show mac-address-table

显示静态和动态 MAC 地址。

命令 : show mac-address-table

例 : ASUS# show mac-address-table

### 5.3.15 VLAN

#### 5.3.15.1 show vlan name string

使用 show vlan 命令来现实所有已设置 VLAN 或一组 VLAN (若指定了 VLAN ID) 的参数。

命令 : show vlan name string

例 : ASUS# show vlan name VLAN1

#### 5.3.15.2 vlan vid

使用 vlan vid 命令来创建一组 VLAN。

命令 : vlan vid

例 : (config)# vlan 2



### 5.3.15.3 name string

使用 name string 命令来创建带有 string 的 VLAN。

命令：name string

例：(config-vlan)# name VLAN2

### 5.3.15.4 access vlan

设置所有界面的访问节点特性和 VLAN。

命令：switchport access vlan <1-4094>

例：(config)# interface fa1/0/2

(config-if)# switchport access vlan 1

### 5.3.15.5 allowed VLANs

使用 switchport trunk allowed vlan 设置命令可以在汇聚模式下新增或删除该界面中以标记形式接收和发送流量的 VLAN。

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

例：(config)# interface fa1/0/2

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

## 5.3.16 GVRP

### 5.3.16.1 clear gvrp statistics

使用 clear gvrp statistics 命令可以清除一个或所有界面中的全部 GVRP 统计信息。

命令：clear gvrp statistics [IFNAME]

例：ASUS# clear gvrp statistics fa1/0/2

### 5.3.16.2 gvrp 模式

这条命令可以启用或禁用交换机的 GVRP 功能。

命令：gvrp (enable|disable)

例：ASUS# gvrp enable

### 5.3.16.3 显示 gvrp 设置

显示 gvrp 设置的状态。

命令：show gvrp interface IFNAME

例：ASUS# show gvrp interface fa1/0/1

### 5.3.16.4 show gvrp statistics

显示 gvrp 统计数据的状态。

命令：show gvrp statistics [IFNAME]

例：ASUS# show gvrp statistics fa1/0/1

## 5.3.17 CoS/QoS

### 5.3.17.1 queue cos-map

使用 queue cos-map 命令可以设置 CoS 队列的优先级顺序。

命令：cos cos-map PRIORITY QUEUE

例：ASUS# cos cos-map 3 3

### 5.3.17.2 show queue cos-map

这条命令将 GVRP 恢复为默认值。

命令：show cos cos-map

例：(config)# show cos cos-map

### 5.3.17.3 qos 模式

这条命令将 qos 模式设置为 highfirst。

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

例：(config)# cos policy fifo

### 5.3.17.4 show cos policy

这条命令用来显示 cos 模式。

命令：show cos policy

例：(config)# show cos policy

### 5.3.17.5 qos ingress bandwidth

这条命令用来设置进入交换机的封包的 QoS 带宽参数。

**命令：** qos ingress bandwidth LIMIT\_RATE BURST\_RATE

**例：** (config)# interface fa1/0/2  
(config-if)# qos ingress bandwidth 10

## 5.3.18 SNMP

### 5.3.18.1 show rmon statistics

显示 rmon statistics IFNAME 状态。

**命令：** show rmon statistics [IFNAME]

**例：** ASUS# show rmon statistics fa1/0/1

### 5.3.18.2 show snmp-server community

显示 snmp 服务器团体。

**命令：** show snmp-server community

**例：** ASUS# show snmp-server community

### 5.3.18.3 snmp-server host

这条命令用来设置 SNMP host 信息。

**命令：** snmp-server host A.B.C.D

**例：** (config)# snmp-server host 192.168.8.31

## 5.3.19 过滤

### 5.3.19.1 deny any host

使用 deny MAC access list 命令来阻止符合条件的非 IP 流量的转发。使用这条命令的否定 (no) 形式可以从已命名的 MAC 访问列表中删除一种拒绝访问的情况。

**命令：** deny any host MACADDR [IFNAME]

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

### 5.3.19.2 过滤集

这条命令用名称定义了一组扩展的 MAC 访问列表，并进入 access-list 设置模式。

命令：mac access-list extended WORD

例：(config)# mac access-list extended mac\_acl\_1

### 5.3.19.3 过滤条件

这条命令指定了一种或几种拒绝或允许条件，用来决定封包是转发还是丢弃。

命令：(permit|deny) any any

例：(config-acl)# permit any any

### 5.3.19.4 过滤规则分配

这条命令用名称定义了一组扩展的 MAC 访问列表，并进入 access-list 设置模式。

命令：mac access-group WORD in

例：(config-if)# mac access-group mac\_acl\_1 in

## 5.3.20 端口访问控制

### 5.3.20.1 dot1x guest-vlan

使用 dot1x guest-vlan 界面设置命令来指定一个活动的 VLAN 作为 802.1X guest VLAN。使用这条命令的否定 (no) 形式来恢复默认设置。

命令：dot1x guest-vlan <1-4094>

例：(config)# interface fa1/0/1

(config-if)# dot1x guest-vlan 3

### 5.3.20.2 dot1x max-req

使用 dot1x max-req 界面设置命令来设置交换机在发送扩展认证协议 (EAP)- 请求 / 身份帧 (假设没有收到答复) 到客户端的最大次数, 超过这个最大次数后交换机将重新开始认证过程。

**命令:** dot1x max-req <1-10>

**例:** (config)# interface fa1/0/1  
(config-if)# dot1x max-req 2

### 5.3.20.3 dot1x port-control

使用 dot1x port-control 命令来启用端口认证状态的手动控制。使用这个命令的否定 (no) 形式可恢复到默认设置。

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

**例:** (config)# interface fa1/0/1  
(config-if)# dot1x port-control force-authorized

## 5.3.21 拨入用户

### 5.3.21.1 dot1x username password

在本地 radius 数据库中新增用户。

**命令:** dot1x user WORD WORD VLAN-ID

**例:** (config)# dot1x user test 12345 3

### 5.3.21.2 show dot1x user

显示 dot1x 拨入用户。

**命令:** show dot1x user

**例:** ASUS# show dot1x user

## 5.3.22 RADIUS

### 5.3.22.1 RADIUS 设置

这条命令用来设置 radius 服务器 IP, Radius 密钥和 Radius 端口, 用于 802.1X 设置。

命令: dot1x radius server A.B.C.D RADIUS\_KEY [PORT]

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

### 5.3.22.2 show dot1x radius

显示用于 802.1X 设置的 dot1x radius 服务器 IP, Radius 密钥和 Radius 端口。

命令: show dot1x radius

例: ASUS# show dot1x radius

## 5.3.23 端口安全

### 5.3.23.1 show port security

这条命令用来显示端口安全设置、状态和 MAC 地址信息。

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

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 clear port security

这条命令用来清除端口安全动态 MAC 地址。

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

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 switchport port-security

这条命令用来设置端口安全和 MAC 地址。

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

**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 switchport port-security aging

这条命令用来进行端口安全老化设置。

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

**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

---

show private health: 显示环境变量，例如温度、风扇转速和电压等。

show private led: 显示系统的三个 LED 指示灯 - SYSTEM, RPS 和 FAN。

show private model: 显示交换机的型号。

show version: 显示硬件、boot rom 和固件的版本号。

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。

本章节设定您已经了解了二进制，比特，字节等基础知识。您可以在第 8 章中找到这些内容的详细信息。

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

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

#### 6.1.1 IP 地址的结构

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

类似地，IP 地址包含两种信息。

##### 网络 ID

在 Internet 或 Intranet 确认网络身份。

##### 主机 ID

在网络中确认计算机或设备身份。

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



下面是有效的 IP 地址范例：

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

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

C 类：192.60.201.11 (网络号 = 192.60.201, 主机号 = 11)

### 6.1.2 网络类型

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

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

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

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

一些与 IP 地址相关的重要信息：

从 field1 可以轻松识别地址类型：

field1 = 1-126:           A 类

field1 = 128-191:       B 类

field1 = 192-223:       C 类

(field1 值中缺少的部分留作特殊用途)

主机 ID 可以是范围除 0 和 255 的任何值,这些值已留作专用。

## 6.2 子网掩码



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

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

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

255.255.255.128

将其转换为二进制容易看出它的真实面目:

11111111. 11111111. 11111111.10000000

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

相似的,要将一个 C 类网络分为 4 个子网,掩码就是:

255.255.255.192 或 11111111. 11111111. 11111111.11000000

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



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

A 类: 255.0.0.0

B 类: 255.255.0.0

C 类: 255.255.255.0

这些称做默认掩码是因为网络在没有子网存在的时候已经设置完毕。

## 7 疑难排解

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

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

### 7.1 使用 IP 工具诊断问题

#### 7.1.1 ping

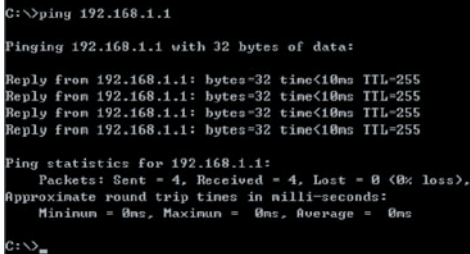
Ping 是用于检测您的计算机是否能够识别网络上其他计算机的命令。ping 命令向您指定的计算机送出一条信息，如果该计算机收到这条信息，它就会发送回应。要使用 ping 命令，您需要知道进行联络的计算机的 IP 地址。

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

```
ping 192.168.1.1
```

点击 **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。

如果目标计算机收到了这个信息，就会出现如图 61 所示的提示。



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

图 61. 使用 ping 工具

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

ping 命令还可用于测试连接交换机的路径是否通行无阻（使用默认的局域网 IP 地址 192.168.1.1）或其他为交换机分配的地址。

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

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

### 7.1.2 nslookup

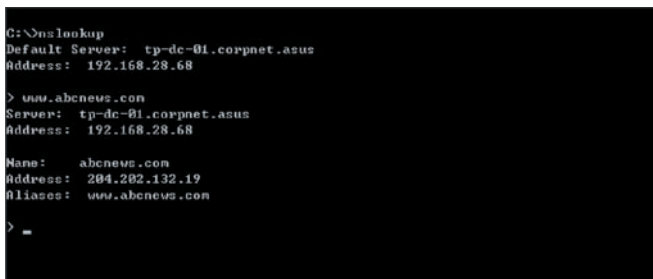
您可以使用 nslookup 命令来决定与 Internet 站点相对应的 IP 地址。您可以指定一个普通名称，nslookup 将在您的 DNS 服务器中寻找 IP 地址 (DNS 服务器一般位于您的 ISP)。如果该名称不在您的 ISP 的 DNS 服务器的记录中，地址请求就会发送到上级服务器，以此类推，直到找到地址为止。此时服务器就会将相对应的地址发送到您的计算机。

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

nslookup

点击 **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 62 所示。



```
C:\>nslookup
Default Server:  tp-dc-01.corpnet.asus
Address:  192.168.28.68

> www.absnews.com
Server:  tp-dc-01.corpnet.asus
Address:  192.168.28.68

Name:    absnews.com
Address:  204.202.132.19
Aliases:  www.absnews.com

> =
```

图 62. 使用 nslookup 工具

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

要退出 nslookup，在提示符处键入 exit 并按 <Enter>。

## 7.2 更换故障风扇



在您卸下交换机背面的风扇模组前，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。

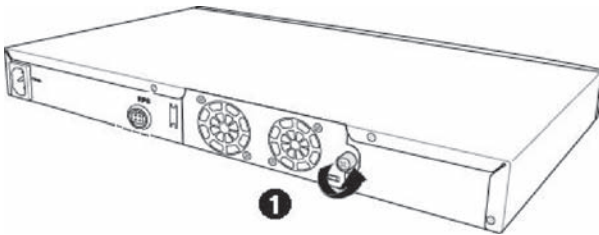


图 63. 拧开螺丝

2. 如图所示拉出风扇模组。

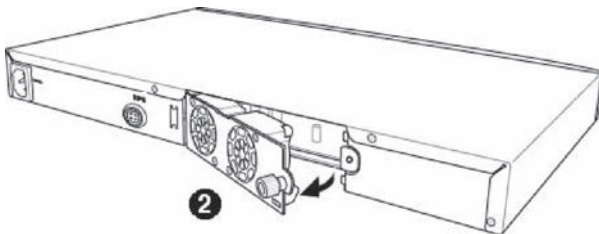


图 64. 拉出风扇模组

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

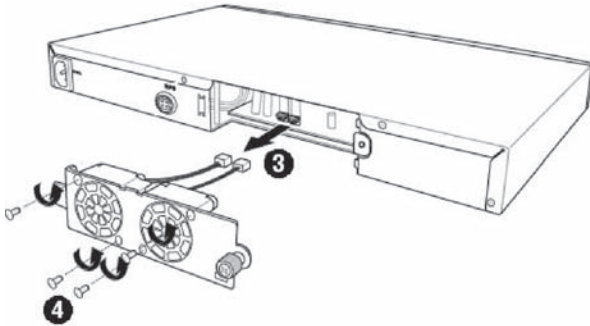


图 65. 卸下风扇

5. 将新的风扇装在原来风扇的位置，确保风扇电源线靠近模组底部。
- 按照同样的步骤替换另一个风扇。
6. 将风扇电源线连接到 PCB 上，确认风扇电源线连接到正确的接口。当您面对交换机背部面板时，左边的风扇是风扇 1。
  7. 将风扇模组置入交换机直至其卡入位置。确认风扇电源线没有卡在风扇模组和机箱之间。
  8. 用螺丝固定风扇模组。检查风扇模组四周确认没有电线卡在风扇模组和机箱之间。

#### 风扇规格

体积：40 x 40 x 20 mm

电压和电流：12VDC, 0.13A

转速：8200RPM

### 7.3 简易维修

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

表 9. 疑难排解

问题	建议方案
LED	
系统打开后，SYSTEM LED 不亮	确认电源线是否连接到交换机或电源插座。
连接冗余电源后，RPS LED 不亮	1. 确认 RPS 电源线是否连接到电源插座。 2. 确认安装的 RPS 模組是否符合 RPS 标准。
FAN LED 呈琥珀色闪烁	检查交换机背部的风扇，如果其中任一个风扇有故障，参见 7.2 替换风扇。
当连接网线时，以太网 Link LED 不亮	1. 确认以太网线是否正地将交换机连接到您的局域网交换机 / 集线器 / 计算机。确认计算机 / 集线器交换机已经打开。  2. 确认缆线长度是否符合您的网络的要求。1000 Mbps 网络 (1000BaseTx) 须使用标有 Cat 5 的缆线。10Mbit/sec 缆线可能支持低档缆线。
网络访问	
计算机不能访问同一网络中的另一个主机	1. 检查以太网网线是否完好，LED 是否呈绿色。  2. 如果端口的 LED 呈琥珀色，检查该端口是否被禁用。如果刚刚启用 STP，可能会出现短时间的网络中断。

问题	建议方案
计算机无法显示网页设置界面	<div>1. 交换机已打开并且连接端口也已经启用。交换机的出厂默认 IP 为 192.168.1.1.</div> <div>2. 在您的计算机上确认您的网络设置。如果您的计算机没有设置一个有效的路由来连接到交换机, 请将交换机 IP 改成您的计算机可以访问的 IP。</div> <div>3. 从计算机 Ping 您的交换机 IP, 如果失败, 请重复第二步。</div> <div>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。</div>
网页设置界面	
丢失 / 忘记网页设置界面的用户名或密码	<div>1. 如果您还没有修改用户名和密码, 请尝试用户名“admin”, 密码为空。</div> <div>2. 通过 RS232 或 USB 登录控制终端, 使用 “sys user show” 显示丢失信息。</div>
某些页面无法完全显示	<div>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®。</div> <div>2. Ping 交换机的 IP 地址检查连接是否稳定。如果一些 ping 包丢失, 检查您的网络设置确认设置有效。</div>
设置修改无法保存	确认点击了 <b>Save Configuration</b> 页面的 <b>Save</b> 按钮。
控制终端界面	
不能显示终端仿真器上的文字	<div>1. 出厂设置的波特率为 9600, 无流量控制, 8 位数据, 无分集检测, 停止位为 1。</div> <div>2. 将您的终端仿真器设置如上, 如果您使用的是 USB 接口, 请先安装 USB 驱动。</div> <div>3. 检查连接线性能。</div>



## 8 术语表

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

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

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

RMON	远程监测  SNMP 的扩展, 提供综合性的网络监视功能。
routing	路由。在您的网络和互联网之间, 根据源 IP 地址和网络情况, 选择最有效的路径转发封包。执行路由选择的设备称为路由器。
SNMP	简单网络管理协议  用于管理网络的 TCP/IP 协议
STP	生成树协议 防止封包在复杂网络中造成环路的桥接协议。
subnet	子网。子网是网络的一部分, 子网通过将网络中的计算机归分为小组而使这些计算机与其他网络上的计算机分隔开来。子网中的计算机仍然在物理上与其他上层网络相连, 但是他们被认作是一个独立的网络。参见 network mask。
subnet mask	子网掩码。将子网之间加以区分的掩码。参见 network mask。
TCP	参见 TCP/IP。
TCP/IP	传输控制协议 / 互联网协议  这是互联网上基本的协议组。TCP 负责将数据分为可以在互联网上传输的封包, IP 负责将这些封包发送到目的地址。当 TCP 和 IP 与一些 上层应用进行捆绑如 HTTP, FTP, Telnet 等, TCP/IP 指的确是整套协议组。
Telnet/SSH	一种互动的, 给予字符的, 用于访问远程计算机的程序。HTTP (网络协议) 和 FTP 只允许从远程计算机下载文件, 而 Telnet / SSH 允许从远程进行登录并使用计算机。
TFTP	小型文件传输协议  一种传输文件的协议。TFTP 比 FTP 更加容易使用, 但是性能和安全性不如 FTP。
Trunk	两个或两个以上的端口合而为一成为一个虚拟端口, 也称为链路汇聚。
TTL	存活时间  IP 封包的一个字段, 决定了该封包的寿命。TTL 原本表示的是持续时间, 现在则通常用于表示最大计跳数, 每经过一跳都消耗一个计跳数, 当 TTL 为零时, 该封包就被丢弃。
twisted pair	双绞线。即普通的铜制电话线。它包含一对或多对互相缠绕的电线, 以消除干扰和杂音。每根电话线使用一对线, 在家用情况下, 通常都安装两对。对于以太网局域网, 使用的是一种更高级的, 用于 10BASE-T 网络的三类线 (CAT 3), 以及更高级的 100BASE-T 网络的五类线 (CAT 5)。参见 10BASE-T,

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

