GigaX 系列

第二层网管型交换机

使用手册

C2211

第一版 07.2005

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with manufacturer's instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING! The use of shielded cables for connection of the monitor to the graphics card is required to assure compliance with FCC regulations. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Canadian Department of Communications Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This class B digital apparatus complies with Canadian ICES-003.

华捷联合信息（上海）有限公司（莘庄）

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

华捷联合科技(广州)有限公司

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

华捷联合信息(上海)有限公司成都办事处

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

华捷联合信息(上海)有限公司沈阳办事处

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

华捷联合信息(上海)有限公司北京海淀分公司

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

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

目录

图片目录

表格目录

1 简介

感谢您购买华硕 GigaX 二层网管型交换机！现在您就可以通过功能强大且使用方便的管理界面对交换机进行设置。

本使用手册将指导您如何对 GigaX 二层网管型交换机进行设置，以及如何根据您的个性需要进行设置以获取最大的效益。

1.1 二层网管特色

- 24 个 10/100 BASE-TX 自感应高速以太网端口
- 2 个小型 (SFP) 千兆端口转换端口 (GBIC)
- 802.1D/802.1w 透明桥接 / 生成树协议 / 快速生成树协议
- 8K MAC 地址存储，并具备基于硬件的地址存在时间
- 802.3x 流量控制
- 基于 802.1Q 的标记 VLAN，最高支持 256 组
- 802.1p 服务级别，每个端口支持 4 个队列
- 支持 IGMP 侦测
- 802.3ad 链路汇聚 (手动和 LACP)，最高支持 15 个干线群组
- 端口镜像
- 802.1X 基于端口的网络网络访问控制
- RADIUS 远程拨号服务认证
- RMON: 支持 4 组 (1, 2, 3, 9)
- SNMP v1, v2, v3
- MIB-II
- 企业 MIB: PSU，风扇，系统温度，电压
- Telnet 或 SSH 远程登录
- 通过 FTP 服务器进行固件升级和设置备份
- 系统日志
- 控制终端，Telnet，和 SSH 命令行界面

- 基于网页的图形设置界面
- LED 指示灯表示连接状态
- 系统，冗余电源适配器 (RPS) 和风扇状态 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 版面设计意义

- 斜体字表示命令行界面中表示的参数
- 粗体字表示该文字是您从菜单或下拉菜单中选择的项目，或是程序提示字串。

1.2.3 特殊符号意义

本使用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 了解 GigaX 2024X

2.1 包装内容

GigaX 2024X 交换机销售包装内含以下内容:

- GigaX 2024X (26 端口) 二层网管型交换机
- AC 电源线
- Null modem cable for console interface (DB9)
- 机架安装部件 (两个挂钩和六个 #6-32 螺丝)
- 用于连接控制终端的 USB 连接线
- 安装 CD
- 使用手册
- 快速安装指南

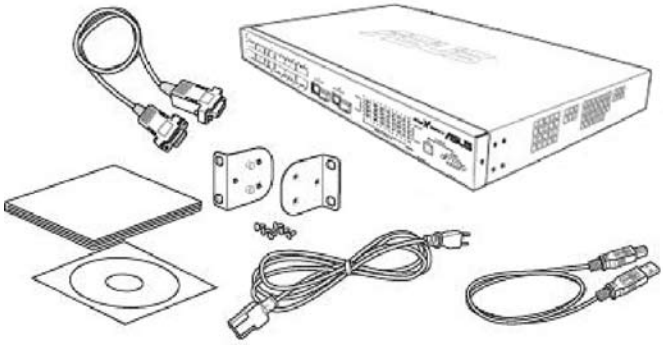

图 1. GigaX 二层网管型交换机包装内容

2.2 前面板

前面板包括 LED 指示灯，显示系统，冗余电源，风扇以及端口的状态。

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	系统已通电
		闪烁	自检，初始化，或下载中
	琥珀色	亮灯	温度或电压不正常
	熄灭		无电源输入
RPS	绿色	亮灯	主机电源工作正常，并且具备冗余电源
	琥珀色	亮灯	主机电源不正常，系统由冗余电源供电
	熄灭		无电源输入（当系统LED 也熄灭时），冗余电源工作不正常或没有安装冗余电源（当系统 LED 亮灯时）
FAN	绿色	亮灯	主风扇和冗余风扇均正常工作
	琥珀色	亮灯	主风扇和冗余风扇其中之一停止工作
10/100/1000 port status	绿色	亮灯	RJ45 或 SFP 已连接，端口已启用
		闪烁	数据传输 / 接收中
	熄灭		无以太网连接
	琥珀色	亮灯	端口已连接，但端口因手动设置或生成树协议而禁用
		闪烁	端口处于生成树堵塞，侦听，和学习状态中
10/100/1000 port speed	绿色	亮灯	千兆端口速度为 1000Mbps，百兆端口速度为 100Mbps
	琥珀色	亮灯	千兆端口速度为 100Mbps
	熄灭		连接速度为 10Mbps 或连接不存在

2.3 后面板

交换机的后面板包括电源和数据接口。

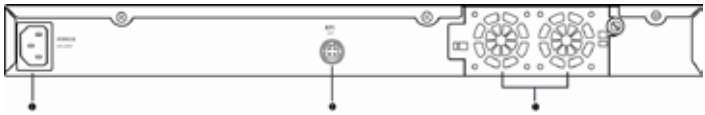

图 3. 后面板

No.	标识	描述
1	Power Connector	用于连接附带的电源线
2	RPS	冗余电源接口
3	FAN1-FAN2	可置换系统风扇

2.4 技术规格

表 2. 技术规格

实体体积	43.5mm(高) x 444mm(宽) x 265mm(深)		
电源	输入	功耗	
	100-240V AC/2.5A 50-60Hz	<90 瓦	
冗余电源 (RPS)	输入	输出	
	100-240V AC/1.8A 50-60Hz	12V DC/12.5A	
环境要求		工作	储存
	温度	-10 ~ 50℃ (14 ~122 ℉)	-40 ~ 70℃ (-40 ~158 ℉)
	湿度	15 ~ 90%	0 ~ 95%
	海拔高度	最高 10,000 英尺 (3,000 米)	40,000 英尺 (12,000 米)
可置换风扇	体积	电源和电压	转速
	40 x 40 x 20 mm	12V DC/0.13A	8200RPM

3 快速设置指南

本章节将阐述设置 GigaX 交换机工作环境的基本步骤。

第一部分阐述如何将 GigaX 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 系列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

将交换机接上电源，并与网络或计算机进行连接。

图 4 显示的是各种硬件的连接方式。

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. 用螺丝将销售包装中附带的挂钩固定在交换机的两侧。
2. 将交换机上的挂钩固定在机架的两侧，并用螺丝加固。

3.2 第二部分 — 设置交换机

将交换机与电源，计算机／网络进行连接。参见图 4。

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时，请使用 RS232 (DB9) 或 USB 线连接交换机。如果您希望使用网页界面的设置方式，请用以太网线将交换机与计算机相连。

3.2.2 将交换机与计算机或局域网进行连接

您可以使用以太网线将计算机直接连接到交换机的以太网端口。您也可将交换机与集线器或其他交换机相连。直连线可交叉线均可用于连接计算机，集线器或交换机。

请使用 5 类以太网双绞线连接交换机的 1000BASE-T 端口，否则，连接的速度就不能达到 1Gbps。

3.2.3 连接 RPS 模组

将 RPS 模组连接到 RPS 接口并确认 RPS 的另外一端连接到接地的电源插座上。

3.2.4 连接电源适配器

1. 将交流电源线连接到交换机背部的 POWER 接口，并将电源线的另一头连接到墙面插座或接线板上。
2. 请参考表 4 观察前面板处的 LED 指示灯。如果 LED 指示灯的显示状况同表 4 描述，说明交换机硬件正常工作。

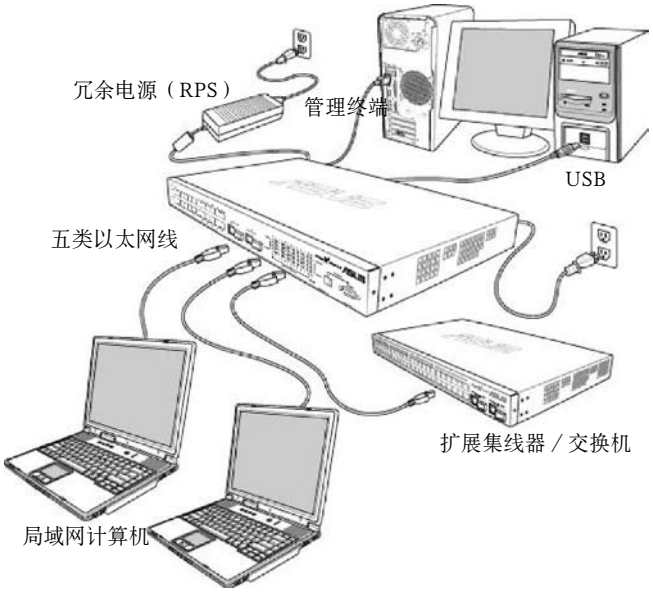

图 4. 硬件连接图示

表 3. LED 指示灯

No.	LED	描述
1	系统	绿色表示交换机已经开启。如果 LED 熄灭，请检查电源适配器是否连接完好。
2	交换端口 1~26	绿色表示交换机能够与局域网进行通信，闪烁表示交换机正在传送或接受数据。
3	冗余电源 (RPS)	绿色表示交换机已经安装冗余电源。
4	风扇	绿色表示风扇正常工作

3.3 第三部分 — 基本管理设置

完成硬件连接之后，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: GX2024X 交换机提供网页设置界面，您可以使用启用 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。这个端口为 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模拟终端软件，如 Hyper Terminal 的计算机上。
2. 用附带的 USB 线连接到计算机。您需要首先从附带的 CD 光盘中安装驱动程序以确保 USB 正常工作。驱动程序将使 USB 在 Windows ME/2K/XP 操作系统下模拟 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) 将模拟模式设为 VT1000
4. 在设置完控制终端后，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) 输入“net interface ip sw0 <your ip address> <your network mask>”. 例如，您的交换机 IP 地址为 192.168.10.1，网络掩码为 255.255.255.0，您就须键入“net interface ip sw0 192.168.10.1 255.255.255.0”。

   b) 如果您希望通过网络来进行交换机设置，您就需要设置默认网关或静态路由。键入“net route static add 0.0.0.0 <your network gateway IP> 0.0.0.0 1”作为默认路由，如图 5 所示 .

图 5. 登录和 IP 设置窗口

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。由于交换机支持 DHCP 客户端功能，交换机需要获取一个有效的静态 IP 地址，或通过网页设置界面从 DHCP 获取动态地址。

1. 首次使用网页界面时无须登录，因为此时默认下通过网页进行的设置将无效。为了保存网页界面下的设置，请先进入 System 目录下的 Administration 页面进行认证。如果认证被禁用，请跳过第二步。

2. 在交换机连接的网络上打开任意一台计算机，打开网页浏览器（如 Internet Explorer®），在此地址栏内键入下面的 URL 并按 <Enter>:

   http://192.168.1.1

这是出厂默认下的交换机 IP 地址。

然后，如图 6 的登录屏幕将会出现。

图 6. 登录窗口

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

默认用户名 : admin
默认密码 : （无）
您可在任何时间对密码进行修改（见 5.3.1 系统命令）。

3. 设置新的 IP 地址时，点击 System，然后点击 IP Setup **页面**（见图 8）。添入 IP 抵制，网络掩码和默认网关，然后按 OK。
4. 如果新地址与默认地址不同，浏览器就不能自动更新交换机的状态窗口，也不能退回之前的设定页面。这是正常的现象。您需要重新在网页的地址栏中键入新的 IP 地址，然后按 <Enter>。您就重新进入了网页设置界面。
5. 为了启用网页设置界面的认证功能，请按菜单列表中的 Administration，然后按下 Enabled 开始对网页设置进行保护。

按下 OK 后登录页面即出现。

图 7. IP 设置

4 网页界面下的设置

GigaX 2024X 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 Microsoft Internet Explorer® 5.5 及以后版本使用。注意：不支持 Netscape®。

4.1 登录到网页设置界面

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

   http://192.168.1.1

   这是交换机出厂默认 IP 地址。图 8 显示的是登录窗口。

图 8. 设置界面登录窗口

如果您未启用网页设置认证功能 (见 3.3.2)，登录窗口将不会出现。

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。(见 5.3.1)

   默认用户名: admin

   默认密码: < 无 >

每当您登录到网页设置界面时，您都会看到设置主页 (见图 9)。

图 9. 主页

4.2 功能结构图

GigaX 2024 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. 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

表 4. 端口颜色描述

端口颜色	描述
绿色	以太网连接已建立
黑色	无以太网连接
琥珀色	以太网连接已建立，但端口被生成树手动禁用。

点击交换机图片上端口的图标，端口的设置情况将显示在窗口的右下部位。

左边拦是菜单栏（见图 11），它包括了交换机设置的各种可用设置特色。这些设置内容被分为若干组, 如 System（系统）, Bridge（桥接）, 等等。您可以点击这些条目来打开相应的设置页面。

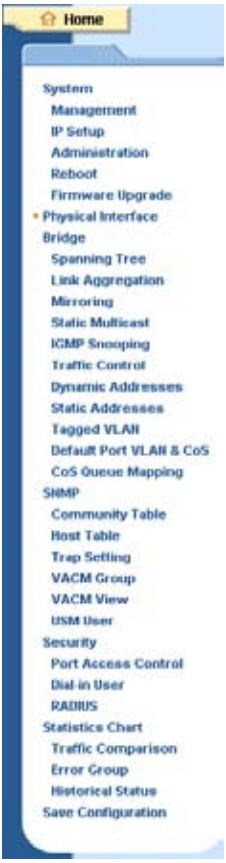

图 11. 完整的菜单列表

右边栏现实的是设置页面或统计的图表。参见 4.3 。

4.2.1 导航菜单

- 打开一组相关菜单，请点击相对应的分组条目。菜单打开后，菜单前部向右的箭头将指向下。
- 收拢一组相关菜单，请点击相对应的分组条目。
- 打开一个设置页面，请点击您需要设定的页面条目。

4.2.2 常用按钮和图标

下表显示的是网页界面中的按钮和图标的功能。

表 5. 常用按钮和图标

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

4.3 System （系统）

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

4.3.1 Management（管理）

Management（管理）页面包括以下信息:

Model Name（型号）: 设备名

MAC Address（MAC 地址）: 交换机的 MAC 地址

System Name(系统名): 用户定义的用于区分系统的名称(可编辑)

System Contact（系统联络）：（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 12. 所示。

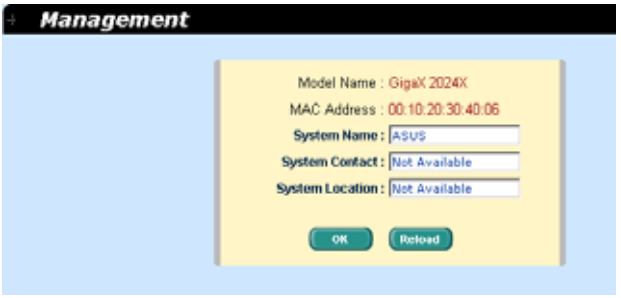

图 12. 管理

4.3.2 IP Setup（IP 设置）

GigaX 2024X 交换机支持动态和静态 IP 分配方式。动态 IP 地址是从同一个 VLAN 下的 DHCP 服务器获得。IP 设置页面包括以下几项可编辑的内容:

VLAN ID: 在系统管理界面中设置一个 VLAN ID。管理的规则将应用于该 VLAN。

DHCP 客户端: 启用 DHCP 获得动态 IP 地址; 或禁用 DHCP 手动分配静态地址。DHCP 服务器必须在 VLAN 的范围内。

IP 地址: 为交换机管理界面分配一个静态 IP 地址。

Network Mask（网络掩玛）

Default Gateway（默认网关）

需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，如图 13. 所示。

图 13. IP 设置

4.3.3 Administration（管理权限）

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

按 OK 保存设置并按 Reload 刷新设置，如图 14 所示。若要启用密码保护，您需要立刻重新登录。

您可以在命令行界面下随时更改密码。

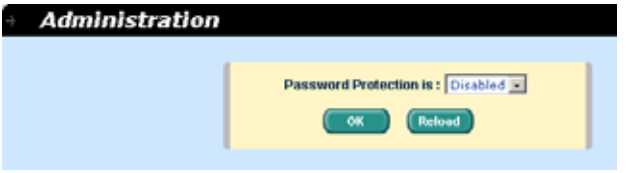

图 14. 管理权限

4.3.4 Reboot （重新启动）

重新启动页面中包括一个 Reboot 按钮。点击该按钮重新启动系统。

重新启动系统将中断网络并中止网页界面的连接。

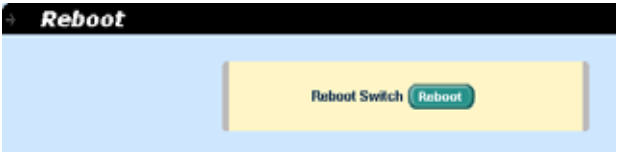

图 15. 重新启动

4.3.5 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): 显示启动编码的版本

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。

在固件路径栏输入固件文件位置，或点击 Browse... 后从弹出窗口中选择文件。点击 Upload 更新交换机的固件，参见图 16。

点击 upload 按钮将指定的固件刷新到交换机，固件升级成功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。

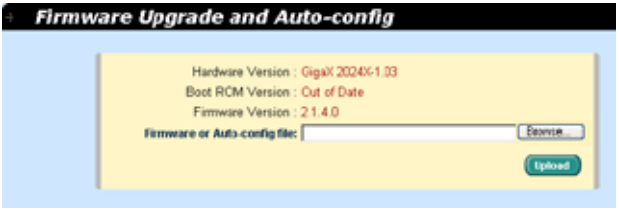

图 16. 固件升级

4.4 Physical Interface（实体端口）

实体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

Port Status Window（端口状态窗口）：显示每个端口的以下信息:

a) 连接状态：存在连接的连接速度，双工模式，或显示无连接

b) 状态：生成树状态

c) 管理：启用／禁用端口的设置值

d) 模式：连接速度和双工模式的设置值

e) 流量控制：启用／禁用 802.3x 流量控制机制的设置值

选择相应的端口号来设置端口，然后按 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。

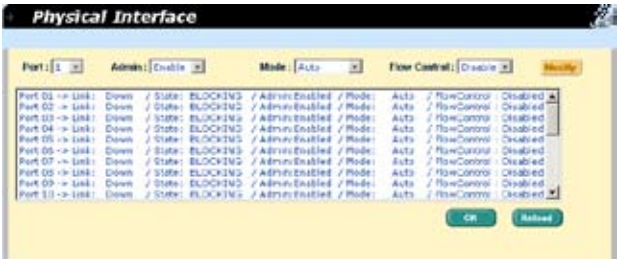

图 17. 实体端口

4.5 Bridge（桥接）

桥接页面包括了大部分的二层设置内容，如链路汇聚， STP 等。

4.5.1 Spanning Tree 生成树

生成树协议的设置页面能够在交换机运行时启用或禁用其设置。该页面包括三个部分。

第一部分显示根信息，告知用户根交换机的生成树设置。

第二部分是生成树设置。您可以对以下内容进行设置:

Disable/STP Enable/RSTP Enabled（禁用／启用生成树协议／启用快速生成树协议）: 启用／禁用生成树协议／快速生成树协议。当启用生成树协议／快速生成树协议时，且交换机为根交换机时，协议将使用下列设置:

Hello Time（Hello 时间）: 生成 BPDU 的时间间隔

Max Age（最大寿命）: 局域网内所有网桥使用的超时值

Forward Delay（转发延迟）: 局域网内所有网桥使用的超时值

Bridge Priority（桥接优先）: 局域网内交换机的优先级

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

Port（端口）: 选择需要进行设置的端口号。

Priority(优先级) 交换机端口的优先级。数字越小表示优先级越高。当侦测到环路时，优先级较低的端口号相比其他端口更容易被生

成树堵塞有效的优先范围是 0 到 240。

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

FastLink（快速连接）：连接时，端口处于转发状态，随后端口将采用生成树规则。

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

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

点击 OK 激活设置，按 Reload 将设置进行刷新。

图 18. 生成树

4.5.2 Link Aggregation 链路汇聚

本页面用于设置链路汇聚群组（端口群组）。GigaX 2024X 交换机可以支持 15 个链路汇聚群组。

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

Name（名称）：链路汇聚群组名称。

Trunk ID（群组 ID）：群组名称之外另一个用于区分链路汇聚的数字。

LACP: 在选择的群组上启用／禁用 LCAP。LACP 模式一直为活动。

Remove Trunk(取消群组): 取消选中的群组。

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

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

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

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

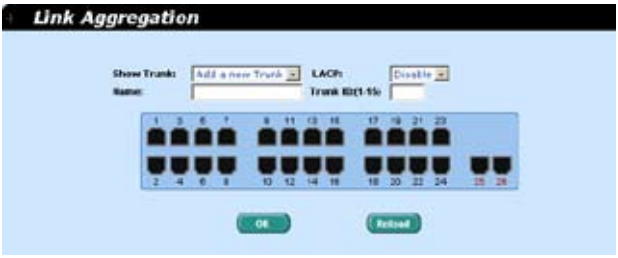

图 19. 链路汇聚

4.5.3 Mirroring（镜像）

镜像和网络流量分析器帮助您监测网络的流量。您可以检测选中端口的出入封包。

Mirror Mode（镜像模式）：对选定端口组启用或禁用镜像功能。

Monitor Port（镜像端口）：获取选中端口的封包之副本。

监视端口不能属于链路汇聚群组。

监视端口的功能与普通交换端口不同，不能对封包进行交换，也不能进行地址学习。

点击 OK 将设置发送到交换机(HTTP 服务器)。点 Reload 刷新设置。

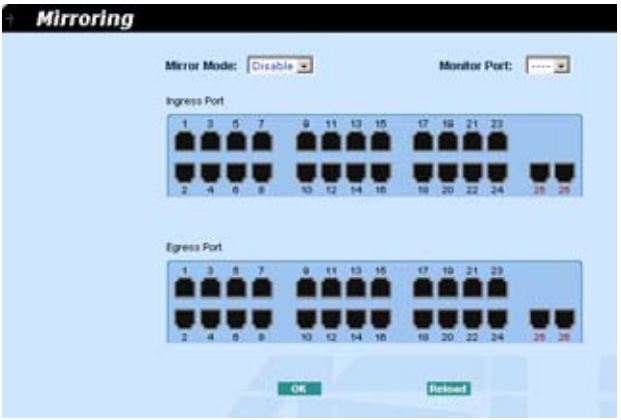

图 20. 镜像页面

4.5.4 Static Multicast（静态组播）

本页面用于将组播地质添加到组播表中。交换机可以容纳 256 条组播条目。群组中所有端口就将把特定的组播包转发到群组中其他的端口。

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

MAC Address（MAC 地址）：选择组播地址

VLAN：选择 VLAN 群组

点击 OK 激活设置。点 Reload 刷新设置。

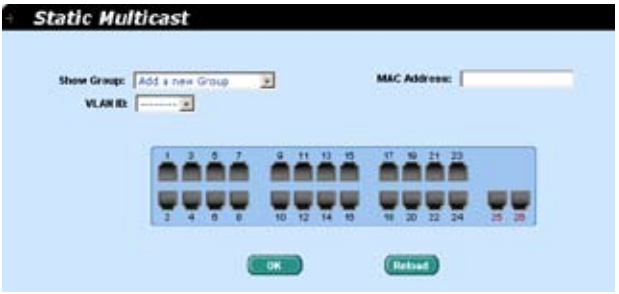

图 21. 静态组播

4.5.5 IGMP 侦测

IGMP 侦测通过开启或关闭 IGMP 侦测功能，有效的减少了网络上的组播流量。当 IGMP 侦测功能开启时，交换机就会侦测 IGMP 封包并将新的群组添加到组播表中。然而，当静态组播表的条目超过 256 条时，IGMP 侦测就不能正常工作了。交换机只允许 256 个二层组播群组。

图 22. IGMP 侦测

4.5.6 Traffic Control（流量控制）

流量控制确保交换机的带宽不被泛洪封包，如广播封包，组播封包所堵塞。限制数值是用来现实某种风暴总数量的上限值。如果广播／组播功能启用，他们各自的流量不会超过上限值。点击 OK 保存设置，进入 Save Configuration 页面点 Save 激活设置。

图 23. 流量控制

4.5.7 Dynamic Addresses（动态地址）

本页面显示基于端口，VLAN ID，或指定的 MAC 地址查找动态 MAC 地址的结果。动态地址指的是交换机自动学习的 MAC 地址，当地址在老化时间内不再学习，该地址就会过期。用户可以根据需要在 15 到 3825 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，按 Query 观察 MAC 地址状态。地址窗口将显示查找结果。

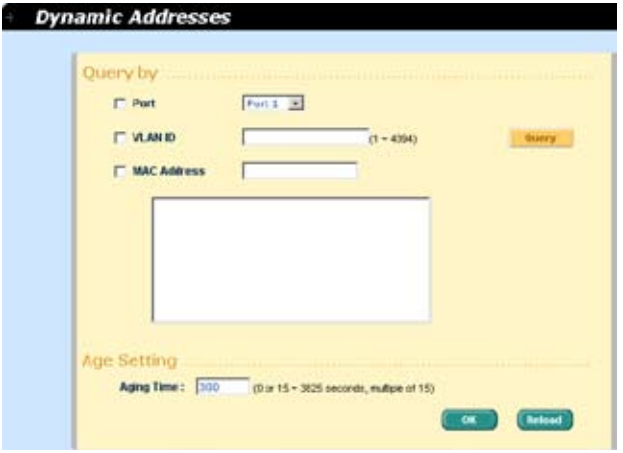

图 24. 动态地址

4.5.8 Static Addresses（静态地址）

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

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。窗口一页显示 15 条记录。当地址数超过 15 后，新的地址将出现在下一页中。 您可以按 First, Previous, Next, 或 Last 来浏览 MAC 地址表；或者输入页数，按 Go 进行浏览。您也可以用鼠标选择 MAC 地址记录，按 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，按 Query 来查找静态地址。地址窗口将现实查找结果。按 OK 保存设置。按 Reload 刷新设置。要激活设置，请进入 save configuration 页面按 Save。

图 25. 静态地址

4.5.9 Tagged VLAN（标记 VLAN）

您可以设置 256 个 VLAN 群组并在本页中显示 VLAN 群组。交换机默认设置下有一个 VLAN，它是不能删除的。这项功能可以防止交换机出错。除了默认 VLAN 外，您可以删除任何其余的 VLAN。

您可以通过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：从该端口传输的所有封包都会进行标记。

“Blank” 型：该端口不属于 VLAN 群组。

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

Show VLAN（显示 VLAN）：选择既存的 VLAN 显示其状态或选择 Add a new VLAN 来新建一个 VLAN 群组。

Name（名称）：VLAN 名称

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

删除 VLAN 删除既存的 VLAN。在新建VLAN时本栏目不会出现。

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

图 26. 标记 VLAN

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

本页面包括了一些与 VLAN 标记相关的设置，包括:

端口: 选择需要进行设置的端口。

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

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

点击 Modify 更改端口列表中的内容，按 OK 保存设置。若要激活设置，请进入 Save Configuration 页面按 Save。

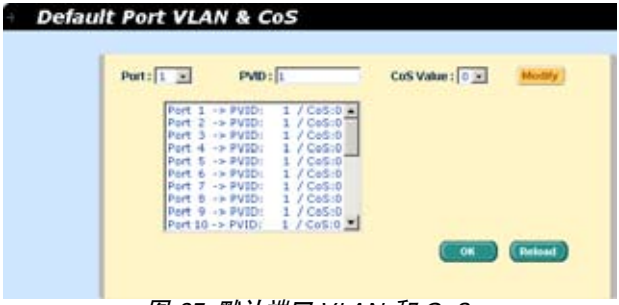

图 27. 默认端口 VLAN 和 CoS

4.5.11 CoS Queue Mapping（CoS 队列）

GigaX 2024X 交换机支持每个端口 4 个出口队列。您可对每个队列进行调度选择:

- Strict priority 调度: 每个 CoS 值可以规划到四个队列中的任何一个。队列 4 具有最高的传输数据包的优先级。低优先级的队列要等到优先级高的队列传完才开始传输。在 Strict priority 调度中，加权设置总是为零。
- Weighted round-robin （加权轮转）调度 (WRR): WRR 调度要求您定义一个数值用于规定当前队列与其他 CoS 队列的相对重要性（weight）。WRR 调度防止低优先级的队列在高优先级队列传输时被完全忽略。 WRR 调度对各个队列实行轮流发送机制。封包的号码与队列的重要性相对应。举例说明，如果队列 1 的 weight 为 1，队列 2 的 weight 为 2，那么队列 1 在队列 2 每次发送完 2 个封包后发送 1 个封包。通过调度功能，即使高优先级的队列为非空，低优先级的队列也能获得机会发送封包。固定的 weight 值为 1,2,4,8。

点击 OK 保存设置，点击 Reload 刷新设置到当前值 若要激活设置，进入 Save Configuration 页面后然后按 Save.

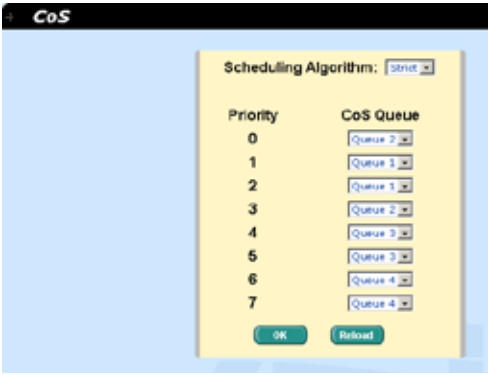

图 28. Cos 队列

4.6 SNMP

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

4.6.1 Community Table（团体列表）

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

图 29. 团体列表

4.6.2 Host Table（主机列表）

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

图 30. 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；按 Reload 刷新页面。

图 31. Trap 设置

4.6.4 VACM Group（VACM 群组）

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

Group Name（群组名）: 输入安全群组名称。

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 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 Reload 刷新页面；若要激活设置，请进入 Save Configuration 页面并按 Save。

图 32. VACM 群组

4.6.5 VACM View

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

View Name（View 名）：输入安全群组名称。

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

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

View Mask（View 掩码）：输入 View 的掩码。掩码中的每一位表示的是 View 掩码自左向右数字。数位 ‘0’ 表示 ‘无关’。

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

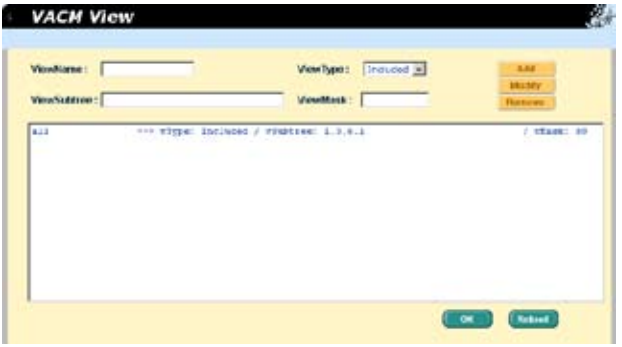

图 33. VACM View

4.6.6 USM User（USM 使用者）

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

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

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

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

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

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

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

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

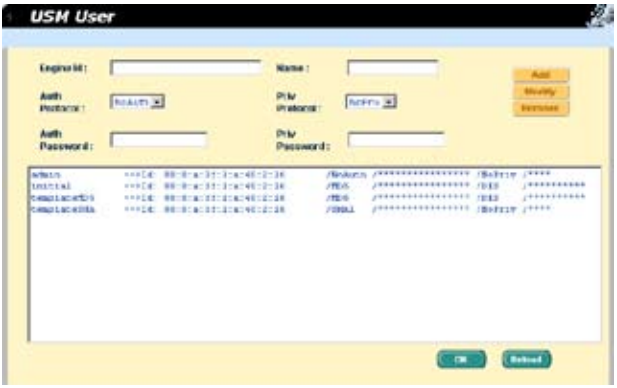

图 34. USM 使用者

4.7 Security（安全）

本交换机采用了 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。

4.7.1 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:

- Reauthentication（重新认证）: 一旦启用，交换机就会在重新认证时间期满时要求重新认证端口的使用者。
- Reauthentication Time（重新认证时间）: 如果重新认证启用，这里定义的就是交换机发送认证信息到端口用户的时间间隔。
- Authentication Method（认证方式）: RADIUS 或本地数据库可用于认证端口使用者。
- Quiet Period: 如果 RADIUS 或本地数据库认证失败，交换机将在再次发送认证要求前等待的一端时间。
- Retransmission Time（重传时间）: 如果端口用户没有响应交换

机的认证请求，交换机将在再次发送请求前等待一端时间

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

第二部分是端口设置。当更改完成时请点击 Modify。

- Port（端口）：指定要进行设置的端口。
- Multi-host（多主机）：如果启用该功能，连接到选定端口的所有主机在其中一个主机通过验证后均可使用端口。如果禁用，只有通过验证的主机才能访问该端口。
- Authentication Control（认证控制）：如果选择 'force authorized'，选定的端口都强制通过了认证。这样，所有主机的流量都可以通过该端口；如果选择 'force unauthorized'，选定的端口就被堵塞，任何流量也不能通过。如果选择 'Auto' 选定端口的性质由 802.1x 协议进行控制。在一般情况下，所有的端口都被设为 'Auto'。
- Guest VLAN: 为访客指定一个无 802.1x 的 guest VLAN。

点击 OK 永久保存设置。点击 Reload 刷新设置到当前值。

图 35. 端口访问控制

4.7.2 Dial-In User

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（确认密码）: 再次输入密码
- Dynamic VLAN（动态 VLAN）: 指定分配给 802.1x 认证用户的 VLAN ID

点击 Add 添加新的使用者，修改完毕后点击 Modify。 要删除使用者时，选中该使用者后点 Remove 。点击 OK 永久使用该设置。点 Reload 刷新设置到当前值。

图 36. Dial-In user

4.7.3 RADIUS

为了使用外部 RADIUS 服务器，下列参数须进行设置:

- Authentication Server IP: 认证服务器 IP 地址
- Authentication Server Port: RADIUS 侦听的端口号
- Authentication Server Key: GigaX 和 RADIUS 服务器通信密码
- Confirm Authentication Key: 重新输入一遍上面的密码

The VLAN of the RADIUS server connected to the switch must be the same as the VLAN of the system management interface.

Please click OK to make the settings permanent. Click Relaod to refresh the settings to current value.

图 37. RADIUS

4.8 Statistics Chart（统计表）

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

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

4.8.1 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 38. 流量比较

4.8.2 Error Group（错误分组）

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

图 39. 错误分组

4.8.3 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。

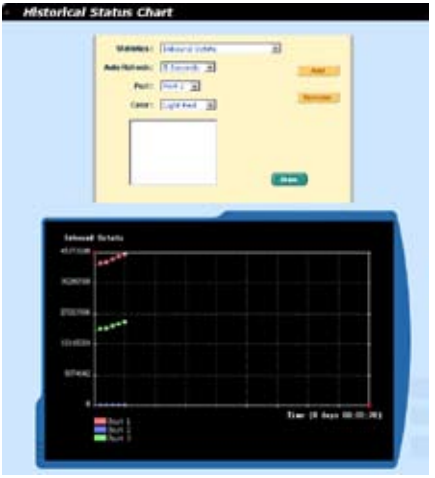

图 40. 历史状态

4.9 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。

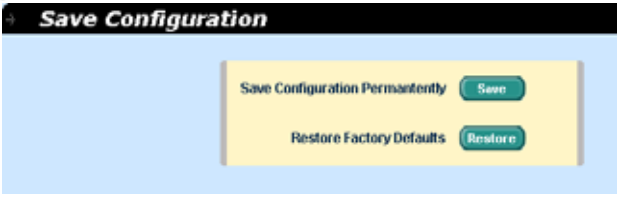

图 41. 保存设置

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 2024X 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模拟软件如 HyperTerminal，以及用于设置交换机的命令行翻译器。您需要将终端模拟器的波特率设置为 9600, 8 位数据，无配类， 1 个停止位，无流量控制。

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

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

5.1 开机自检

POST（开机自检）是在系统启动时间进行的。它测试交换机主板上的系统内存，LED，以及硬件芯片等。检测完毕时，它就会现实系统测试和初始化的结果。当提示符 “(ASUS) %” 出现时，（如图 43），您即可忽略这些自检信息。

图 42. 命令行界面。

5.1.1 Boot ROM 命令模式

在开机自检的过程中，按下 <ENTER> 可以进入 “Boot ROM Command” 模式，如图 43 所示。

图 43 显示交换机的双镜像备份。

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 43. Boot ROM 命令模式

5.1.2 Boot ROM 命令

键入 “?” 显示所有可以使用命令的列表。

表 6. Boot ROM 命令

命令	参数	用途
c	IP address	设置 TFTP 用户端的 IP 地址
g	NONE	载入并执行固件
h	NONE	显示线上帮助
m	mask	设置网络掩码
p	NONE	显示当前设置
r	NONE	系统重启
s	IP address	设置 TFTP 服务器 IP 地址
t	NONE	Toggle 安全模式
u	File name	通过网络上的 TFTP 协议上传启动模块／固件
v	NONE	显示 boot rom 的版本号
w	NONE	重设 Toggle 管理员密码

5.2 登录和登出

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

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

5.3 CLI 命令

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

请使用 “?” 获取可使用命令列表和帮助信息

请使用 “/” 回到根目录

请使用 “..” 回到上级目录

键入命令获取命令的帮助信息

5.3.1 系统命令

[System Name]

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

命令: sys info name <system name description>

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

[System Contact]

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

命令: sys info contact <system contact description>

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

[System Location]

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

命令: sys info location <system location description>

在 location description 键入地点描述即更新地点信息。

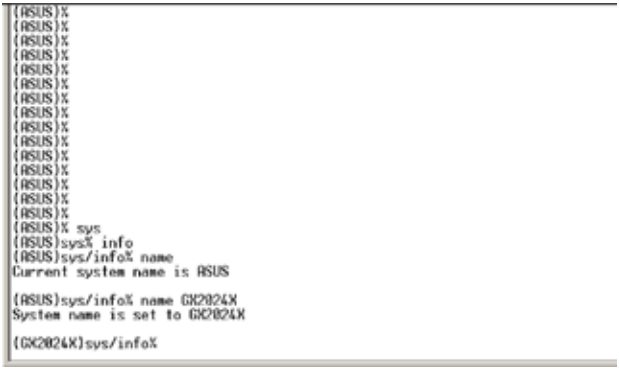

图 44. SYS 命令

[VLAN ID]

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

命令: net interface vlan sw0 <VLAN ID>

[DHCP Client]

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

命令: net interface dhcp sw0 <enable/ disable/ renew/ release/ show>[IP Address]

显示交换机的静态 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，ftp 服务器，telnet 服务器和 SSH 服务器都使用这个地址。

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

[Network Mask]

显示交换机的子网掩码。

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

[Default Gateway]

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

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

[Password Protection is] [Enabled/Disabled]

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

命令: sys web set <enable/disable>

[New Password] / [Verify Password]

默认用户名为 admin, 密码为空。您可以通过设置以下内容设置密码。

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

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

password (old password,): <new password>

[Reboot]

用户可以发出重启命令来重启交换机。

命令: sys reboot

[Upload]

命令行界面没有这个命令，请参见 Boot ROM 命令组的相关命令。

5.3.2 实体端口命令

[Admin] [Enable/Disable]

显示端口的管理状态，并允许用户启用或关闭该端口。

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

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

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

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

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

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

[Flow Control] [Enable/Disable]

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

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

[Reload]

从设置文件中恢复之前的端口设置。

命令: l2 port retrieve

5.3.3 桥接命令

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

允许用户指定交换机是否使用生成树协议 (STP/ RSTP)。

命令: l2 stp start <stp / rstp>

命令: l2 stp stop

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

显示当前的 STP/RSTP 桥接设置参数。

命令: l2 stp bridge set

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

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

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

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

[Priority]

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

显示当前端口的 STP/RSTP 参数设置。

命令: l2 stp port set

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

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

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

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

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

[Reload]

从设置文件恢复之前的设置。

命令: l2 stp retrieve

命令: l2 stp bridge retrieve

命令: l2 stp port retrieve

[Show Trunk]

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

命令: l2 trunk show <trunk id>

[Create Trunk]

通过指定干线 ID, rtag, 名称, LACP 模式和端口号码来新建一个新的干线群组。

命令: l2 trunk create <trunk id> <trunk name> <lacp (enable/disable)> <port list>

[Add/Remove Trunk]

可以在干线群组中增加或删除端口。

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

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

[LACP Action]

用户可以在干线群组中启用或禁用 LACP。

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

[LACP System Priority]

用户可以为运行中的 LACP 设置系统优先级。

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

[LACP Port Priority]

用户可以为运行中的 LACP 分配端口优先级。

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

[Reload]

从设置文件中恢复之前的设置。

命令: l2 trunk retrieve

[Mirror Mode] [Enable/Disable]

[Monitor Port] [port number]

显示交换机镜像设置。

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

命令: l2 mirror ingress <port list>

命令: l2 mirror egress <port list>

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

[Reload]

从设置文件中恢复之前的设置。

命令: l2 mirror retrieve

[Show Multicast Group]

显示静态组播群组列表中的群组。

命令: l2 mcast show

[Set Multicast Group]

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

命令: l2 mcast set

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

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

port list [format: 1 2 3 4- 26/* for all ports]: <port list>

[Remove Multicast Group]

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

命令: l2 mcast delete

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

vlan id: <vlan id>

[Reload]

从设置文件中恢复之前的设置。

命令: l2 mcast retrieve

[IGMP is] [Enabled/Disabled]

Layer 2 IGMP 侦测功能可根据实际需要决定是否启用。

命令: l2 igmp <start/stop>

[Reload]

从设置文件中恢复之前的设置。

命令: l2 igmp retrieve

[Action] [Enable/Disable]

[Mode] [Broadcast] or [Broadcast/Multicast] or [Broadcast/Multicast/

Unknown unicast]

[Limit Rate]

用户可以通过开启流量控制功能来限制广播，组播和泛洪（封包无法找到目的地）。

命令: l2 rate set <enable/disable> [<mode (1:broadcast only, 2: broadcast and multicast, 3:broadcast, multicast and unknown unicast)> <limit rate (70~250000 Kbps/sec)>]

[Reload]

从设置文件中恢复之前的设置。

命令: l2 rate retrieve

[Aging Time]

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

命令: l2 arl age [aging time value]

[Query by Port]

ARL 表中的记录可以根据端口号进行搜索排序。

命令: l2 arl port <port number>

[Query by VLAN ID]

ARL 表中的记录可以根据 VLAN ID 进行搜索排序。

命令: l2 arl vlan <vlan id>

[Query by MAC Address]

ARL 表中的记录可以根据 MAC 地址进行搜索排序。

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

[MAC Address]

[VLAN ID]

[Port Selection]

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

命令: l2 arl static <mac> <vlan id> <port no> <trunk id>

[Remove]

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

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

[Reload]

从设置文件中恢复之前的设置。

命令: l2 arl retrieve

[Show VLAN]

显示交换机中现有的 VLAN 信息。

命令: l2 vlan show <vlan id>

[Name]

[VLAN ID]

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

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

命令: l2 vlan add <vlan id> <port list>

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

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

[Remove VLAN]

允许用户完全删除整个 VLAN。

命令: l2 vlan delete <vlan id>

[Reload]

从设置文件中恢复之前的设置。

命令: l2 vlan retrieve

[Show Port]

显示端口设置。

命令: l2 port show <port id or * for all ports>

[PVID]

通过指定 VLAN ID 和其下的端口号列表为一个端口设置默认 VLAN。

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

[CoS Value]

通过分配优先级 (0-7) 为端口设置未标记封包服务级别。

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

[Reload]

从设置文件中恢复之前的设置。

命令: l2 port retrieve

[CoS] [Map]

允许用户为缓冲队列 (总共 4 个,队列 ID 1-4)设置 CoS 优先级 (0-7)。

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

[Scheduling Algorithm] [Strict/WRR]

允许用户设置基于 strict priority 或 weight priority 的调度。

命令: l2 cos sched <mode (1: strict 2: weighted round robin)>

[Reload]

从设置文件中恢复之前的设置。

命令: l2 cos retrieve

5.3.4 SNMP

[Community Name] [Set]

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

命令: snmp community add

New community string: <new community string>

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

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

用户可以通过重新分配团体字串和特权来修改团体记录。

命令: snmp community set

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

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

这项操作将修改所有主机的团体字串。

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

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

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

允许用户从团体表中删除团体记录。

命令: snmp community delete

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

这项操作将删除所有具有指定团体字串的主机。

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

[Reload]

从设置文件中恢复之前的设置。

命令: snmp community retrieve

[Host IP Address] [Community]

每条主机记录包括一个主机 IP 地址，网络掩码，以及其团体字串。

命令: snmp host add

Host IP/Subnet: <IP address>

Netmask: <netmask>

Community: <community string>

用户可以通过重新分配允许范围内的 IP 地址，网络掩码和团体字串

对主机记录进行修改。

命令: snmp host set

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

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

Netmask (old netmask): <new netmask>

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

允许用户从主机表中删除一个主机记录。

命令: snmp host delete

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

[Reload]

从设置文件中恢复之前的设置。

命令: snmp host retrieve

[Trap Version] [v1/v2c]

[Destination]

[Community for Trap]

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

命令: snmp trap add

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

Destination IP: <IP address>

Community: <community string>

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

命令: snmp trap set

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

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

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

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

允许用户从 trap 表中删除记录。

命令: snmp trap delete

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

[Reload]

从设置文件中恢复之前的设置。

命令: snmp trap retrieve

[Group Name]

[Read View Name]

[Write View Name]

[Notify View Name]

[Security Model]

[Security level]

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

命令: snmp snmpv3 access add

Gruop Name: <group name string>

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

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

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

Read View Name: <read view name string>

Write View Name: <write view name string>

Notify View Name: <notify view name string>

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

命令: snmp snmpv3 access set

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

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

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

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

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

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

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

允许用户删除 VACM 记录。

命令: snmp snmpv3 access delete

Access entry: <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令: snmp snmpv3 access retrieve

[View Name]

[View Type]

[View Subtree]

[View Mask]

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

命令: snmp snmpv3 view add

View Name: <view name string>

View Subtree [oid]: <view subtree>

View Mask: <view mask>

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

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

命令: snmp snmpv3 view set

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

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

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

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

允许用户删除 VACM view 记录。

命令: snmp snmpv3 view delete

View entry: <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令: snmp snmpv3 view retrieve

[Engine Id]

[Name]

[Auth Protocol]

[Auth Password]

[Priv Protocol]

[Priv Password]

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

命令: snmp snmpv3 usmuser add

EngineId: <engine id string >

Name: <user name string >

AuthProtocol [oid]: <auth protocol oid string >

AuthPassword: <auth password string>

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

Priv Password: <priv password string >

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

命令: snmp snmpv3 usmuser set

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

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

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

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

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

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

允许用户删除 USM User 记录。

命令: snmp snmpv3 usmuser delete

USM user entry: <entry id to delete>

[Reload]

从设置文件中恢复之前的设置。

命令: snmp snmpv3 usmuser retrieve

5.3.5 安全命令

[Reauthentication]

允许用户启用或禁用周期重新认证功能。

命令: security dot1x bridge reauth <enable / disable>

[Reauthentication Time]

允许用户设置重新认证时间。

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

[Authentication Method]

允许用户设置认证模式 (RADIUS 或本地数据库)。

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

[Quiet Period]

允许用户设置安静时间。

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

[Retransmission Time]

允许用户设置重传时间。

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

[Max Reauthentication Attempts]

允许用户设置重新认证尝试最大次数。

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

[Multi-host]

允许用户对指定端口启用或禁用多主机功能。

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

[Authentication Control]

允许用户对指定端口设置认证控制。

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

[Guest VLAN]

允许用户为指定端口设置 guest VLAN ID。

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

[Reload]

从设置文件中恢复之前的设置。

命令: security dot1x retrieve

[User Name]

[Password]

[Confirm Password]

[Dynamic VLAN]

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

命令: security dialinuser create

User Name: <user name string>

Password: <password string>

Confirm Password: <confirm password string>

Dynamic VLAN: <dynamic VLAN>

命令: security dialinuser remove <user name/*>

允许用户从数据库删除用户记录。

命令: security dialinuser modify <user name/*>

允许用户从本地数据库中修改用户记录。记录包含用户名，密码和动态 VLAN。

User Name: <new user name string>

Password: <new password string>

Confirm Password: <new confirm password string>

Dynamic VLAN: <new dynamic VLAN>

[Reload]

从设置文件中恢复之前的设置。

命令: security dialinuser retrieve

[Authentication Server IP]

[Authentication Server Port]

[Authentication Server Key]

[Confirm Authentication Key]

允许用户设置 RADIUS 服务器 IP，服务器端口和服务器密码。

命令: security radius set

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

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

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

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

[Reload]

从设置文件中恢复之前的设置。

命令: security radius retrieve

[Generate SSH key]

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

命令: security sshkey start

[Reset SSH key]

将 SSH 密码重设为默认值。

命令: security radius default

[Show Generating Status]

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

命令: security sshkey show

5.4 其他命令

sys time uptime: 显示从系统启动以来经过的时间

sys time date: 显示当前日期和时间

sys time settime: 设置当前时间

sys files config backup: 备份设置文件

sys files config default: 恢复出厂默认值

sys monitor auto: 启用或禁用风扇自动检测

sys monitor set: 风扇设置命令 (1~255)

sys monitor show: 显示系统环境的状态

net ping: 对远程主机使用 ping 命令

net route show: 显示路由表中的记录

6 IP 地址，网络掩码和子网

6.1 IP 地址

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

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

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

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

6.1.1 IP 地址的结构

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

类似地， IP 地址包含两种信息。

网络 ID

在 Internet 或 Intranet 确认网络身份。

主机 ID

在网络中确认主机身份。

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

表 7. IP 地址结构

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

下面是有效的 IP 地址范例:

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

6.1.2 网络类型

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

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

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

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

一些与 IP 地址相关的重要信息:

从 field1 可以轻松识别地址类型:

field1 = 1-126: A 类

field1 = 128-191: B 类

field1 = 192-223: C 类

(field1 值中缺少的部分留作特殊用途)

主机 ID 可以是范围内除 0 和 255 的任何值，这些值已留作专用。

6.2 网络掩码

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

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

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

255.255.255.128

将其转换为二进制容易看出它的真实面目:

11111111. 11111111. 11111111.10000000

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

相似的，要将一个 C 类网络分为 4 个子网，掩码就是:

255.255.255.192　或　11111111. 11111111. 11111111.11000000

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

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

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

这些称做默认掩码是因为网络在没有子网存在的时候已经设置完毕。

7 问题排除

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

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

7.1 使用 IP 工具诊断问题

7.1.1 ping

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

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

ping 192.168.1.1

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

如果目标计算机收到了这个信息，就会出现如图 45 所示的提示。

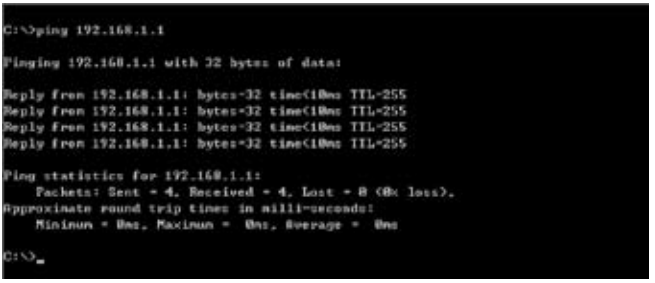

图 45. 使用 ping 工具

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

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

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

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

7.1.2 nslookup

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

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

nslookup

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

窗口就会显示相对应的 IP 地址，如图 46 所示。

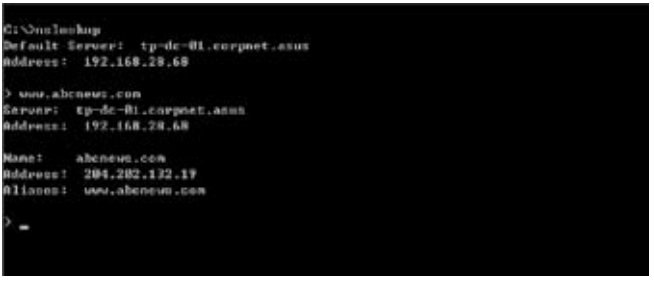

图 46. 使用 nslookup 工具

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

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

7.2 更换故障风扇

当您卸下交换机背面的风扇模组时，请关闭交换机电源。

当交换机背面任何一个风扇出现故障时，您可以按照下列步骤进行替换。

1. 拧开将风扇固定在背部的螺丝。

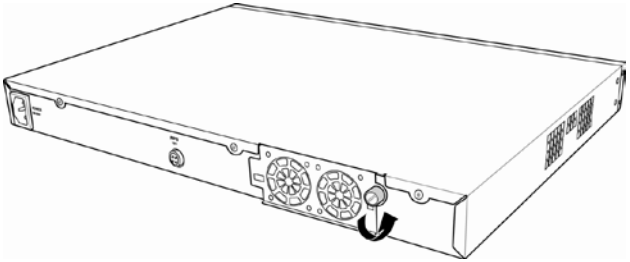

图 47. 拧开螺丝

2. 如图所示拉出风扇模组。

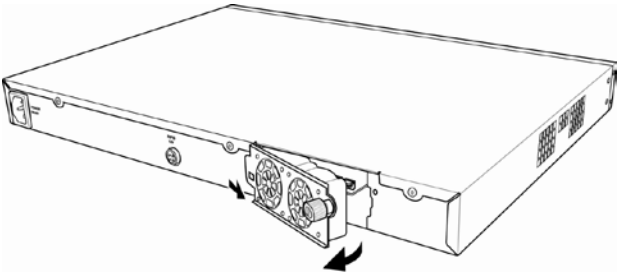

图 48. 拉出风扇模组

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。

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。

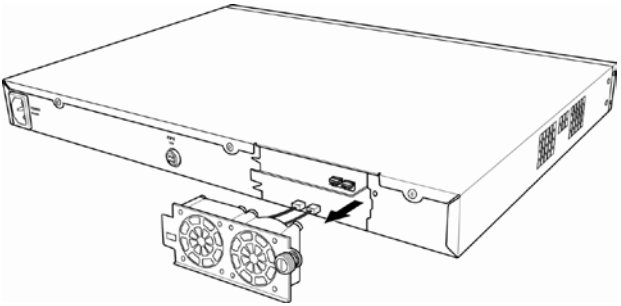

图 49. 卸下风扇

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 8. 问题排除

问题	建议方案
LEDs	
系统打开后 SYSTEM LED 不亮	确认电源线是否连接到交换机或电源插座。
连接冗余电源后 RPS LED 不亮	1. 确认 RPS 电源线是否连接到电源插座。 2. 确认安装的 RPS 模组是否符合 RPS 标准
FAN LED 呈琥珀色闪烁	检查交换机背部的风扇，如果其中任一个风扇有故障，参见 7.2 替换风扇。

问题	建议方案
当连接千兆网口时，千兆以太网 Link LED 不亮	1. 确认以太网线是否正确地将交换机连接到您的局域网交换机 / 集线器 / 计算机。确认计算机 / 集线器交换机已经打开。 2. 确认缆线长度是否符合您的网络的要求。1000 Mbps 网络 (1000BaseTx) 须使用标有 Cat 5 的缆线。10Mbit/sec 缆线可能支持低档缆线。
网络访问	
计算机不能访问同一网络中的另一个主机	1. 检查以太网网线是否完好，LED 是否呈绿色。 2. 如果端口的 LED 呈琥珀色，检查该端口是否被禁用。如果刚刚启用 STP，可能会出现短时间的网络中断。
计算机无法显示网页设置界面	1. 交换机以及打开并且连接端口也已经启用。交换机的出厂默认 IP 为 192.168.1.1. 2. 在您的计算机上确认您的网络设置。如果您的计算机没有设置一个有效的路由来连接到交换机，请将交换机 IP 改成您的计算机可以访问的 IP。 3. 从计算机 Ping 您的交换机 IP，如果失败，请重复第二步。 4. 如果 ping 成功，但是网页设置界面仍不能使用，请通过 RS232 或 USB 连接控制终端。检查是否有过滤规则或静态 MAC 地址将 WEB 流量堵塞。
网页设置界面	
丢失 / 忘记网页设置界面的用户名或密码	1. 如果您还没有修改用户名和密码，请尝试用户名“admin”，密码为空。 2. 通过 RS232 或 USB 登录控制终端，使用“sys user show” 显示丢失信息。
某些页面无法完全显示	1. 确认您使用的是 Internet Explorer® v5.5 或以后版本的浏览器。不支持 Netscape。您的浏览器必须启用 Javascript® ， 也必须支持 Java®。 2.Ping 交换机的 IP 地址检查连接是否稳定。如果一些 ping 包丢失，检查您的网络设置确认设置有效。
设置修改无法保存	确认点击了 Save Configuration 页面的 Save 按钮。
终端界面	

问题	建议方案
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, 无分集检测, 停止位为 1 。 2. 将您的终端模拟器设置如上, 如果您使用的是 USB 接口, 请先安装 USB 驱动。 3. 检查连接线性能。

8 术语表

10BASE-T	用于以太网的有线线缆，数据传输率为 10 Mbps。亦称 3 类线 (CAT 3) 。参见 data rate, Ethernet。
100BASE-T	用于以太网的有线线缆，数据传输率为 100 Mbps。亦称 5 类线 (CAT 5) 。参见 data rate, Ethernet。
1000BASE-T	用于以太网的有线线缆，数据传输率为 1000 Mbps。
binary	二进制。“基于 2 ”的数字系统，只使用 0 和 1 两个数字来表示所有的数字。在二进制中，十进制数字 1 写作 1 , 十进制 2 写作 10，十进制 3 写作 11，十进制 4 写作 100, 依次类推。虽然 IP 地址为方便起见表示为十进制数字，实际上它使用的是二进制数字。比如 IP 地址 209.191.4.240 转换为二进制是 11010001.10111111.00000100.11110000。比特，IP 地址，网络掩码同样也是二进制。
bit	比特。“二进制数字”的缩写，一个比特就是一个只有 0, 1 两种数值的数字。参见 binary.
bps	比特每秒
CoS	服务级别。在 802.1Q 中规定, 值的范围为 0 到 7。
broadcast	广播。将数据发送到网络上所有的计算机。
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。
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）。
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。
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 mask	网络掩码。网络掩码就是一系列的比特字串用于 IP 地址，以决定网络 ID 和主机 ID 的位数。1 表示此比特有效，0 表示忽略此比特。举例说明，如果网络掩码 255.255.255.0 应用到 IP 地址 100.10.50.1, 网络 ID 为 100.10.50, 主机 ID 为 1。参见 binary, IP address, subnet, “IP Addresses Explained” 部分。
NIC	网络接口卡
	插入计算机，提供网络线缆的物理接口 RJ-45 的适配器。参见 Ethernet。
packet	封包。在网络上传输的数据单位。每个封包都包含一个有效载荷（数据），以及包头信息如来源地址和目的地址等。
ping	分组互联网探测器
	用于确认 IP 地址对应的主机是否能够到达。它亦可用于寻找与域名相对应的 IP 地址。
port	端口。实体的网络设备接入点，如计算机，路由器，数据通过该接入点流入流出。
protocol	协议。一系列用于控制数据传输的规则。为了是数据能够成功传输，数据传输源和目标都必须遵守相同协议的规则。
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	远程检测

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　上连。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。