GigaX 系列

二层网管型交换机

用户手册

C2664/2006年9月

C2664
2006 年 9 月
第一版

华硕联系信息

华捷联合信息（上海）有限公司（莘庄）

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

华捷联合科技（广州）有限公司

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

华捷联合信息（上海）有限公司成都办事处

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

华捷联合信息（上海）有限公司沈阳办事处

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

华捷联合信息（上海）有限公司北京海淀分公司

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

华硕技术支持:
免费咨询电话：800-8206655
Email: tsd@asus.com.cn
Netq **论坛**：Netq.asus.com.cn **由华硕工程师提供在线服务**

目录内容

图片目录

表格目录

1 产品简介

感谢您购买华硕 GigaX2024B/M 二层网管型交换机！

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

1.1 关于本用户手册

1.1.1 注意事项

- 本手册将在缩写词第一次出现时解释其含义，并将其含义解释收入术语表中。
- 为了方便起见，在本手册中，华硕 GigaX 二层网管型交换机将简称为“本交换机”。
- 术语“LAN（局域网）”和“网络”在本手册中将交替使用，表示某个区域内由以太网连接的一组电脑。

1.1.2 印刷提示

- **粗体字** 表示该文字是您从菜单或下拉菜单中选择的项目，或是需要您输入的内容。

1.1.3 提示符号

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

注意：提供对当前所述内容的说明或额外信息。

定义：解释用户可能不了解或不熟悉的术语或缩写。这些术语均可在术语表中查到。

警告：高重要性的信息，包括涉及人身安全和系统完整性的信息。

1.2 产品包装内容

华硕 GigaX 系列交换机的产品包装中包含以下物品：

- ☑ GigaX 2024X (26 端口) 二层网管型交换机 或 GigaX 2016X (18 端口) 二层网管型交换机
- ☑ AC 电源线
- ☑ 支持光盘
- ☑ 终端管理界面连接线 (DB9)
- ☑ 机架安装套件 (包括两个托架与六颗 #6-32 螺丝)
- ☑ 连接终端管理界面的 USB 线
- ☑ 安装光盘
- ☑ 本用户手册

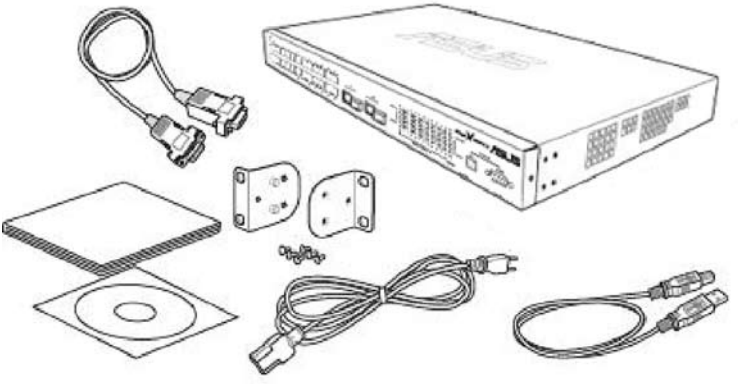


图 1. GigaX 二层网管型交换机包装内容

1.3 特性

华硕 GigaX 系列具备以下特性：

- (GX2024X) 24 个 10/100BASE-TX 自动侦测百兆以太网端口
- (GX2016X) 16 个 10/100BASE-TX 自动侦测百兆以太网端口
- 两个 10/100/1000BASE-T 自动侦测千兆以太网交换端口
- 两个小型 (SFP) Gigabit 端口转换插槽 (GBIC)

- 802.1D/802.1w 透明桥接(transparent bridge)/生成树协议(spanning tree protocol)/快速生成树协议(rapid spanning tree protocol)
- 8K MAC 地址缓存及硬件控制的老化时间
- 802.3x 流量控制
- (GX2024X) 基于 802.1Q 标记的虚拟局域网（VLAN），最多可支持 229 组 VLAN
- (GX2016X) 基于 802.1Q 标记的虚拟局域网（VLAN），最多可支持 237 组 VLAN
- 私有 VLAN，最多支持 4 组私有 VLAN
- (GX2024X) 基于端口的 VLAN，最多可支持 26 个群组
- (GX2016X) 基于端口的 VLAN，最多可支持 18 个群组
- 802.1p 服务等级，每个端口支持 4 个队列
- 支持静态组播，最多可支持 127 个群组
- 支持 IGMP (v1/v2/v3) 侦听
- 802.3ad 链路汇聚 (手动与 LACP)，最多可支持 15 个中继群组
- 端口镜像（Port Mirroring）功能
- 带宽控制
- DHCP 客户端
- 802.1X 基于端口／MAC 地址的网络访问控制
- RADIUS 远程认证拨入用户服务
- TACACS+ 远程认证
- 端口安全（Port Security）功能
- 服务质量（Quality of service）等级：目的地／来源 MAC 优先级，VLAN 优先级，IPv4 ToS/DiffServ，IPv6 流量等级（Traffic Class）
- 以太网线缆诊断
- RMON: 支持 4 个群组(1，2，3，9)
- SNMP v1, v2, v3
- MIB-II
- 企业级电源供应器、风扇和系统温度、电压管理数据库（MIB）
- Telnet 或 SSH 远程登录
- FTP 固件升级和备份配置
- Syslog
- 通过控制终端、Telnet 与 SSH 的命令界面
- 网页图形用户界面（GUI）
- LED 指示灯，用于显示端口连接状态
- LED 指示灯，用于显示系统、冗余电源供应器 (RPS)及风扇状态

1.4 前面板

前面板 LED 指示灯显示了系统、冗余电源供应器（RPS）、 风扇以及端口状态。

图 2. GigaX 2024X 前面板

图 3. GigaX 2016X 前面板

表 1: 前面板标示与 LED 指示灯

标示	颜色	状态	描述
SYSTEM	绿色	恒亮	设备电源开启
		闪烁	自检，初始化或下载中
	琥珀色	恒亮	温度或电压不正常
	熄灭		无电源供应
RPS	绿色	恒亮	设备的电源供应器 (PSU) 工作正常，且交换机的冗余电源正常
	琥珀色	恒亮	设备的电源供应器 (PSU) 工作异常，交换机正由冗余电源供电
	熄灭		无电源供应 (system LED 亦熄灭); 冗余电源异常或尚未安装 (system LED 亮起)
Fan	绿色	恒亮	两个风扇均工作正常
	琥珀色	恒亮	两个风扇全部或有一个停止运转
10/100/1000 port status	绿色	恒亮	已建立 RJ-45 或 SFP 连接；端口已启用
		闪烁	正在传送或接收数据
	熄灭		无以太网连接
10/100/1000 port speed	绿色	恒亮	Giga 端口连接速率为 1000Mbps，或 10/100 端口连接速率为 100Mbps
	琥珀色	恒亮	Giga 端口连接速率为 100Mbps
	熄灭		连接速率为 10Mbps 或连接不存在

1.5 后面板

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

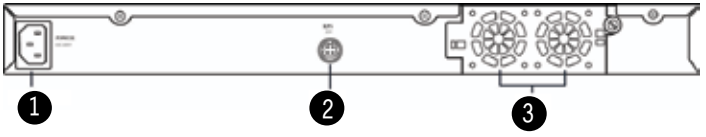


图 4. 后面板

表 2: 后面板标示

No	标示	描述
1	Power	连接电源线
2	RPS	冗余电源供应器
3	FAN1 - FAN2	可抽换式风扇

1.6 技术规格

表 3: 技术规格

物理尺寸	43.5mm (H) X 444 mm (W) X 265mm (D)		
电源	输入 : 100-240V AC/2.5A 50-60Hz		
	耗电量 : < 90 瓦		
冗余电源供应器 (RPS)	输入 : 100-240V AC/1.8A 50-60Hz		
	输出 : 12V DC/12.5A		
环境需求		操作	存放
	温度	-10 to 50°C (14 - 122°C)	-40 - 70°C (-40 - 158°C)
	湿度	15 - 90%	0 - 95%
	高度	最高 10,000 ft (3,000m)	最高 40,000 ft (12,000m)
可抽换式风扇	尺寸 : 40 x 40 x 20 mm		
	电压和电流 : 12VDC, 0.13A		
	转速 : 8200RPM		

2 快速安装指南

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

第一部分介绍如何将 GigaX2024X/2016X 交换机安装在水平表面或机架上。

第二部分介绍硬件设置的步骤。

第三部分介绍 GigaX2024X/2016X 交换机的基本配置。

在您开始安装和设置之前，请先向网络系统管理员取得以下相关信息：

交换机的 IP 地址

默认网关地址

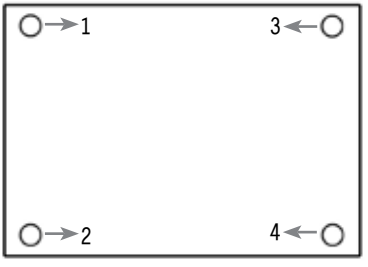
您所处网络的网络掩码

2.1 第一部分 — 硬件安装

本交换机可以安装在平坦的表面或机架上。

2.1.1 将交换机安装于平坦表面

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



请将四个塑胶垫粘贴于交换机底部所标示的位置

2.1.2 将交换机安装于机架

1. 将固定托架锁在本机两侧，并将交换机置入机架。
2. 用螺丝将托架锁在机架上。

2.2 第二部分 — 安装交换机

将本交换机连上电源，并连接至电脑与网络。图 5 为本交换机的硬件连接示意图。

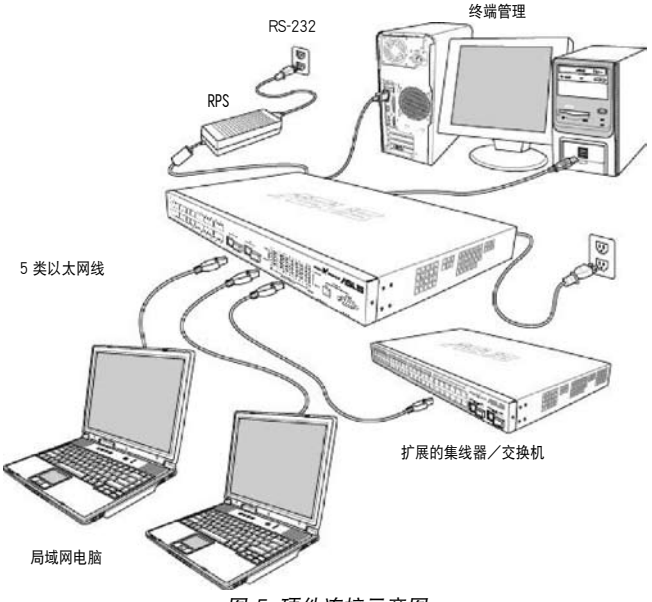


图 5. 硬件连接示意图

2.2.1 连接控制终端接口（Console port）

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

2.2.2 连接到电脑或局域网

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

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

2.2.3 连接冗余电源模块（RPS）

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

2.2.4 连接电源线

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

表 4: LED 指示灯

No	LED	描述
1	System	稳定的绿色代表交换机已经开启。如果 LED 熄灭，请检查交换机电源线是否正确连接并已连接到电源插座。
2	Switch ports [1] to [26] (GX2024X) [1] to [18] (GX2016X)	稳定的绿色代表交换机和其他设备的连接已经建立。闪烁代表交换机正在传送或接收数据。
3	RPS	稳定的绿色代表冗余电源(RPS)模块已成功安装。
4	Fan	稳定的绿色代表所有的风扇都运行正常

2.3 第三部分 — 交换机基本管理配置

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

- **配置管理器**：本交换机提供网页管理界面，您可以使用带 Java® 功能的 IE5.0 或更高版本的浏览器进行配置。 详细说明请参考第 3 章与第 5 章。
- **命令行界面**:通过控制终端接口来配置交换机。详细说明请参考第5 章。

2.3.1 通过控制终端接口进行设置

1. 请使用产品包装中附带的交叉型 RS-232 缆线来连接交换机前面右侧的控制终端接口。此接口为 DB-9 公接头，专门用于数据终端设备(DTE)的连接。将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有终端模拟软件，如 Hyper Terminal 的电脑上。
2. 用产品包装中附带的 USB 缆线将交换机连接到电脑。在连接前您必须首先安装随机光盘中的 USB 驱动程序。USB 驱动可以在 Windows Me/2000/XP 操作系统中模拟一个额外的 COM 端口。
3. 请依照下面的步骤来设置您的模拟软件：
   a) 选择合适的串口号
   b) 将数据波特率设置为 9600
   c) 设置数据格式为无奇偶校验（no parity），8个数据位(Data bit) 及一个停止位(Stop bit)。
   d) 无流量控制
4. 控制终端设置完毕后，您可以在终端画面上看到 “(ASUS)%”。
5. 输入 “login” 来访问命令行界面。默认的用户名称为 “admin”，且无需输入密码，直接按下 <Enter> 即可。

您可以随时通过 CLI 命令行界面来修改密码 (请参考用户手册 5.2 节：登录与登出 部分的说明)。为避免您的交换机被未经许可的人士使用，建议您尽快修改默认密码。

6. 请依照以下步骤来指定交换机的 IP 地址：

a) 输入 “net interface ip sw0 < 您的 ip 地址 > < 您的网络掩码 >”。如，若您的交换机 IP 地址为 192.168.10.1，网络掩码为 255.255.255.0。则您需要输入 “net interface ip sw0 192.168.10.1 255.255.255.0”。

b) 如果交换机必须通过网络进行管理，则需要一个默认网关或静态路由。请输入 “net route static add 0.0.0.0 < 您的网络网关 IP> 0.0.0.0 1” 作为您的默认路由，如图 6 所示。

```
(Asus)% login
user name: admin
password: ****
user 'admin' logged in
(Asus)% net interface ip sw0 192.168.10.1 255.255.255.0
IP Address set successfully

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

(Asus)% _
```

图 6. 登录与 IP 设置画面

2.3.2 通过配置管理器 (Configuration Manager) 进行配置

本交换机提供了一个预先安装的网页界面软件应用程序，称为配置管理器 (Configuration Manager)。

您可以通过与交换机 LAN 端口相连的任意一部电脑上的网页浏览器（如 Microsoft Internet Explorer® 5.0 或更高版本，不支持 Netscape）来访问配置管理器。

1. 在默认情况下，交换机的网页认证是关闭的。您必须开启它以保证系统的安全设置。您可以在 System --> Administration 页面开启交换机的网页认证功能。

图 7. 配置管理器登录画面

2. 在网页浏览器(IE 5.0 或更高版本)中，输入以下 IP 地址：http://192.168.1.1 并按下 <Enter>。这是交换机的默认 IP 地址。

   此时将出现登录画面，如图 7 所示。

3. 输入您的用户名称与密码，然后按下 <OK>。当登录画面首次出现时，请使用下面的默认值：

   用户名称 : admin

   密码 : (无密码)

为避免您的交换机被未经许可的人士使用，建议您尽快修改默认密码。详细说明请参考 5.2 登录与登出 部分的说明。

3 使用配置管理器（Configuration Manager）

本交换机提供了一个预先安装的网页界面软件应用程序，称为配置管理器（Configuration Manager）。它可让您依据网络需要对设备进行设置。您可以通过与交换机 LAN 端口相连的任意一部电脑上的网页浏览器来访问配置管理器。

3.1 登录到 Configuration Manager

配置管理器（Configuration Manager）已预先安装到了交换机。要访问这个应用程序，您需要以下条件：

- 一台连接到交换机 LAN 端口的电脑，如快速安装指南章节所述。
- 您的电脑必须安装了网页浏览器。建议使用 Microsoft Internet Explorer® 5.0 或更高版本，这样可以达到最佳效果。不支持 Netscape。

您可以从任何一台连接到本交换机 LAN 端口的电脑上访问这个应用程序。

3.1.1 设置 Configuration Manager

1. 在默认情况下，交换机的网页认证是关闭的。您必须开启它以保证系统的安全设置。您可以在 System --> Administration 页面开启交换机的网页认证功能。
2. 在网页浏览器（IE 5.0 或更高版本）中，输入以下 IP 地址：http://192.168.1.1 并按下 <Enter>。这是交换机的默认 IP 地址。
3. 输入您的用户名称与密码，然后按下 <OK>。当登录画面首次出现时，请使用下面的默认值：

   用户名称: admin
   密码:（无密码）

3.1.2 设置一个新的 IP 地址

1. 要设置一个新的 IP 地址，请点击 System --> IP Setup。填入新的 IP 地址，网络掩码与默认网关，然后点击 <OK>。
2. 若新的地址与默认的不同，浏览器不会更新交换机的状态窗口或重新取得任何页面，这是正常情况。请在网址栏内输入新的 IP 地址，然后按下 <Enter>，即可更新您的网页显示。
3. 要开启网络访问认证功能，请在菜单中点击 Administration 项，然后选择 Enabled 以开启密码保护功能。

在您点击 <OK> 后，会出现 IP 设置画面，如图 8 与图 9 所示。

图 8. GX2024X IP 设置

图 9. GX2016X IP 设置

GigaX 2024X 与 2016X 机型具有相同的网页界面，只是画面上方的前面板图标有所不同。

在以下章节中，当两种机型的画面内容相同时，将只显示其中一个画面(GigaX 2024X)。若画面内容不同，则两个机型的画面均会列出。

3.2 功能结构

网页设置页面包含三个独立的栏位：顶部栏、左侧菜单栏与右侧栏位。

顶部栏包含了交换机图标和前面板图，如图 10 所示。这个栏位将一直位于浏览器窗口上方，同步显示交换机前面板的 LED 指示灯。以下是关于各指示灯颜色的含义。

- 表 4 为各指示灯的代表含义（见第 8 页）。
- 表 5 为端口颜色说明。

点击端口图标即可在画面右下方显示端口的设置状况。

表 5. 端口颜色说明

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

左侧框位为菜单栏，包含了本交换机的所有可用功能设置选项。这些功能已经进行了分类，如 System, Bridge 等。您可以点击任何项目以显示对应的设置页面。

右侧栏位用来显示设置页面或统计数据图。详细说明请参考第 4.7 章节的说明。

图 10. 完整菜单

3.2.1 浏览菜单的技巧

- 要展开一组相关的功能菜单，请双按菜单项目前的 图标。
- 要关闭一组相关的功能菜单，请双按菜单项目前的 图标。

3.2.2 常用按钮与图标

下表介绍了本管理界面中所有按钮与图标的功能。

表 6: 常用按钮与图标

按钮／图标	功能
	保存您对当前页面做的任何修改。
	在系统中新增一个既有的设置，如静态 MAC 地址或过滤的 ACL 规则。
	修改一个既有项目。
	删除已选择的项目，如静态路由或过滤的 ACL 规则。
	重新显示当前页面，且已加载新的统计数据或设置。

请参考下面的章节以了解通过配置管理器（Configuration Manager）或 CLI 界面来的设置交换机的步骤。

4 配置管理

本章节介绍了您可在配置管理器(Configuration Manager)中使用的功能。此配置管理器软件应用程序已预先安装至交换机。这些功能包括：

- 系统（System）
- 物理端口（Physical Interface）
- 桥接（Bridge）
- 简单网络管理协议（SNMP）
- 安全（Security）
- 线缆诊断（Cable Diagnosis）
- 统计图表（Statistical Chart）
- 保存配置（Save Configuration）

要永久保存对交换机功能（或配置）的修改或新的配置值，您必须至 Save Configuration 页面，然后点击 <Save>。

4.1 系统页面（System）

本章节介绍您在配置管理器（Configuration Manager）中的 System 页面功能可执行的操作：

- 设置系统名称、联系信息、系统位置及其他系统信息；
- 指定 IP 地址；
- 开启／关闭网页认证功能；
- 重新启动交换机；
- 固件升级

4.1.1 管理（Management）

图 11. 管理

管理（Management）页面包含以下信息：

- Model Name: 产品名称。
- MAC Address: 交换机的 MAC 地址。
- System Name: 用户指定的用来辨识系统的名称（可编辑）。
- System Contact: 系统联系信息（可编辑）。
- System Location: 系统位置（可编辑）

System Name, System Contact 及 System Location 栏位不能包含符号 ‘/’。

要保存您所做的修改，请点击 <OK>。请点击 <Reload> 按钮来更新设置。

4.1.2 IP 设置（IP Setup）

图 12. IP 设置

本交换机可支持动态 IP 与静态 IP 地址。动态 IP 地址可从同一 VLAN 内的 DHCP 服务器获取。IP 设置（IP Setup）页面包含以下可设置的参数：

- VLAN ID: 为系统管理界面指定 VLAN ID。若要用于管理，VLAN ID 必须位于同一个 VLAN 内。
- DHCP Client: 开启 DHCP 以获取动态 IP 地址，或关闭 DHCP 来指定静态 IP 地址。DHCP 服务器必须位于所管理的 VLAN 内，且可以访问。
- IP Address: 为交换机的管理界面指定一个静态 IP 地址。
- Network Mask
- Default Gateway

要保存所做的修改，请点击 <OK>。点击 <Reload> 更新设置。

4.1.3 管理权限（Administration）

管理权限（Administration）页面可让您开启或关闭网页用户认证，以及在用户数据库中新增／移除用户。您可以设置最多 8 个用户。默认的网页访问设置不需要任何认证。

图 13. 管理权限

- Password Protection is: 开启或关闭网页认证功能。
- User Name: 新的用户名称。
- Password: 新用户的密码。
- Confirm Password: 再次输入密码。

要保存所做的修改，请点击 <OK>。点击 <Reload> 更新设置。若您开启了密码保护功能，您必须立即重新登录。

4.1.4 重新启动（Reboot）

请依照以下步骤来重新启动交换机：

1. 点击 System --> Reboot。此时将显示 Reboot 页面。
2. 点击 <Reboot> 按钮。

重新启动交换机将停止网络流量并中断 Internet 连接。

4.1.5 固件升级（Firmware Upgrade）

华硕将经常推出更新的固件，为您的 GigaX 二层网管型交换机提供升级。所有的系统软件都包含在一个单一的文件内，称为固件映像（image）。配置管理器（Configuration Manager）提供了一种简单的方法来载入新的固件映像。

图 14. 固件升级

请依照以下步骤来升级固件：

1. 点击 System --> Firmware Upgrade 来开启固件升级页面。

固件升级页面包含下列信息：

- Hardware Version: 显示硬件版本号。
- Boot ROM Version: 显示启动代码的版本。
- Firmware Version: 显示当前执行的固件版本。这个号码会随着固件升级而更新。

2. 在 Firmware or Auto-config file 框中， 输入固件映像文件的位置与名称。您也可以点击 <Browse> 按钮在您的电脑上查找固件映像。
3. 点击 <Upload> 升级固件，升级完成后自动重新启动交换机。

若没有自动重新启动交换机，请参考 4.1.4 重新启动（Reboot）中的描述步骤来重新启动交换机。

自动配置文件的文件名必须为“config.bat”，且文件的第一行必须为“#autoconfig”。

4.1.6 设置备份（Configuration Backup）

本页面可用来备份和恢复系统配置文件。

图 15. 配置备份

备份配置文件

点击 <Backup> 以保存配置文件 (config.bac)。

恢复配置文件

您可以直接在“Restore configuration file”栏位输入配置文件位置，或点击 <Browse> 并从随即出现的窗口中选择配置文件的名称。点击 <Restore> 恢复配置文件。

4.2 物理界面（Physical Interface）

物理端口（Physical Interface）显示了以太网端口的即时状态。

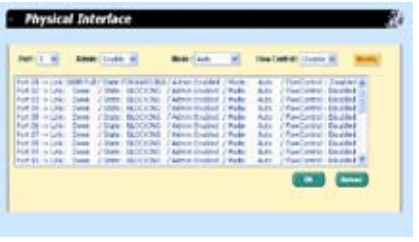


图 16. 物理界面

您可以配置端口的以下栏位：

- Port: 选择需要配置的端口
- Admin: 禁用／启用端口
- Mode: 设置速率和双工模式
- Flow Control: 开启／关闭 802.3x 流量控制机制
- Port Status Window: 显示每个端口的下列信息：

Link Status	既有连接的速率和双工模式，否则此连接为关闭的
State	显示 STP（生成树协议）状态
Admin	显示该端口是开启还是关闭
Mode	显示由用户设置的连接速率和双工模式

要更改这个页面，请选择相应的端口号码，并重新对端口进行配置，然后点击 <Modify> 按钮。您更改的栏位将更新至显示窗口中。然而，您必须执行 Save Configuration 操作后，才能使这些设置生效。参见 4.9 保存配置（Save Configuration）部分的说明。

4.3 桥接（Bridge）

桥接（Bridge）页面群组中包含了交换机的第二层设置，如链路汇聚（Link Aggreration），STP 等项目。

4.3.1 生成树 (Spanning Tree)

生成树协议（STP）设置页面可在运行中开启或关闭生成树协议功能。本页面包含三个部分：

图 17. 生成树

a) 根信息（Root Information）

b) STP 设置(STP Setting)

c) 端口设置(Port Setting)

根信息（Root Information）

第一部分显示了根信息。我们可以从中了解到根交换机的 STP 设置。

STP 设置（STP Setting）

第二部分是 STP 设置。您可以设置以下项目：

- Disable/STP Enable/RSTP Enabled: 开启／关闭 STP/RSTP 功能。当您开启了 STP/RSTP 功能，若本交换机为根交换机，则 STP/RSTP 将使用以下设置。
- Hello Time: BPDU 生成设置的间隔。
- Max Age: 接收到的协议信息存在的最大时间，超过这个时间后，将会被丢弃。
- Forward Delay: 转发延迟。
- Bridge Priority: 交换机在局域网中的优先级

端口设置（Port Setting）

第三部分是端口设置。它包含了一个显示窗口，显示每个端口的当前设置。点击 <Modify> 更改 STP/RSTP 的端口设置。您可以设置以下栏位：

- Port: 选择需要设置的端口
- Priority: 交换机端口的优先级。越小的数字代表越高的优先级。当侦测到网络回路的状况下，拥有较低优先级的端口较可能被 STP 封锁。有效的设置值为 0 至 240。
- Path Cost: 有效的设置值为 1 至 200000000，或设置为 Auto。用户设置的路径开销（Path Cost）将被显示在 AdminCost 中，而运行路径开销（Path Cost）将被显示在 OperCost 中。当侦测到网络回路的状况下，具有较高开销（Cost）的端口较可能被 STP 封锁。
- Edge Port: 默认情况下，所有的端口都被设置为边缘端口（Edge port）。边缘端口接收到 BPDU 后变为 STP 端口。边缘端口只需要很短的时间就可进入转发状态。
- Point to Point: Auto/Yes/No: 全双工模式的端口被判定为点对点连接；其他模式的端口被判定为共享连接。点对点连接具有较少的汇聚时间。在大多数情况下，建议设置为 Auto。

点击 <OK> 保存您所做的更改。点击 <Reload> 更新设置。

4.3.2 链路汇聚（Link Aggregation）

本页面用来设置链路汇聚群组。本交换机最多可提供 15 个链路汇聚群组。您可以设置以下参数：

图 18. GX2024X 链路汇聚

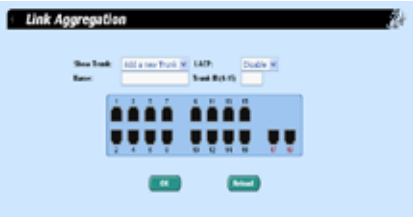


图 19. GX2016X 链路汇聚

- Show Trunk: 选择 Add a new Trunk 来新增一个群组。或选择一个既有群组以显示以下设置栏位与端口图标。
- Name: 群组名称
- Trunk ID: 除了群组名称外，用来区分不同汇聚群组的号码。
- LACP: 开启／关闭选定中继群组的 LCAP 功能。LACP 模式固定为 Active。
- Remove Trunk: 移除选定的中继群组。
- Port Icons: 这些端口的图标按照交换机前面板上的位置列出。点击图标可以选择群组成员。再次点击选中的图标可将这个端口从群组中移除。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

您必须检查连接速率和双工模式，以确保中继群组物理处于活动状态。请至**物理端口**（Physical Interface）的 runtime status 窗口检查中继端口的连接模式。若所有的中继成员都具有相同的速率与全双工模式，则这个中继群组已成功建立。若有一个成员不具备相同的速率或全双工模式，则中继群组没有正确建立。请将中继群组中的所有成员都设置为相同的速率与全双工模式。

链路汇聚群组中所有的端口必须全部在全双工模式下运行且具有相同的速度。

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

链路汇聚群组中所有的端口必须具有相同的 VLAN 设置。

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

4.3.3 镜像（Mirroring）

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

- Mirror Mode: 启用或禁用选定群组的镜像功能。
- Monitor Port: 接收选定的镜像端口的所有流量的备份数据。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。

图 20. GX2024X 镜像页面

图 21. GX2016X 镜像页面

监控端口不能属于任何链路汇聚群组。监控端口不能像一般交换机端口一样运行。它不能进行封包交换或地址学习。本交换机最多可对 8 个端口进行镜像，被镜像的端口都是未标记(untag)的。

4.3.4 静态组播（Static Multicast）

在这个页面中，您可以将组播地址添加至组播列表。本交换机可以容纳 127 个组播地址。群组中所有端口将把特定的组播封包转发至这个群组的其他端口。

- Show Group: 选择 Add a new Group 来建立一个新项目，或选择一个既有的群组地址以显示。
- MAC Address: 选择组播地址。
- VLAN: 选择 VLAN 群组。

点击 <OK> 保存所做的修改。点击 <Reload> 更新设置。

图 22. GX2024X 静态组播

图 23. GX2016X 静态组播

4.3.5 IGMP 侦听（IGMP Snooping）

通过开启或关闭 IGMP 侦听功能，可以帮助减少网络中的组播流量。当本功能开启时，交换机将会侦听 IGMP 封包，并将新群组添加到组播列表。但是，一旦静态地址项目占用了全部 256 个地址空间，IGMP 侦听功能将无法正常运行。本交换机只允许 256 个第二层组播群组。

图 24. IGMP 侦听

4.3.6 带宽控制（Bandwidth Control）

带宽控制（bandwidth control）可限制所选定的帧的传输速率。本交换机以每个端口为基础支持此功能，您需要设置以下栏位：

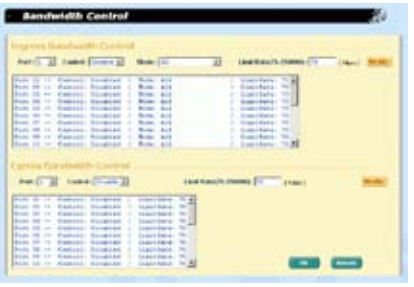


图 25. 带宽控制

传入带宽控制（Ingress bandwidth control）

- Port: 选择需要设置的端口。
- Control: 关闭／开启传入带宽控制功能。
- Mode:
  - Bcast: 限制广播封包。
  - Bcast, Mcast: 限制广播封包与组播封包。
  - Bcast, Mcast, Dlf: 限制广播封包、组播封包与目的地地址搜寻失败的单播封包。
  - All: 限制所有类型的封包。
- Limit Rate: 所有选定类型封包的总数限制值。例如，若开启了广播／组播封包限制功能，则每种类型封包的流量不能超过所设置的限制值。有效的设置值范围为 70 至 250000(Kbps)。

传出带宽控制（Egress bandwidth control）

- Port: 选择需要设置的端口。
- Control: 关闭／开启传出带宽控制功能。
- Limit Rate: 最大传出速率。有效的设置值范围为 70 至 250000(Kbps)。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.3.7 动态地址（Dynamic Addresses）

本页面用来显示通过端口、VLAN ID 或 MAC 地址来查找动态 MAC 地址的结果。在查找中指定的 MAC 地址称为动态地址，它的存在时间由您设置的 Aging Time 所决定。您可以输入一个 15 至 3825（单位为秒）之间的值来设置其存在时间（或称老化时间）。点击 <OK> 可保存您在本页面所做的所有修改。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

图 26. 动态地址

要查找 MAC 地址，您可以勾选 port、VLAN ID 或 MAC address，并输入相应的值，然后点击 <Query>。地址窗口将显示查找结果。

4.3.8 静态地址（Static Addresses）

本页面的 MAC 地址项目不会过期老化。它将一直存在于地址表中，直到您将其从地址表中移除。

静态地址（Static Addresses）页面可设置以下参数：

- MAC Address: 输入 MAC 地址。
- VLAN ID: 输入 MAC 地址所属的 VLAN ID。
- Port Selection: 选择 MAC 地址所属的端口。
- Discard on: 当 MAC 地址作为目的地地址出现在封包时，您可以执行封包过滤。

建立一个新的静态 MAC 地址

点击 <Add>。新的项目将出现在地址窗口中。第一个地址窗口最多可以显示 15 个项目，其他项目将在接下来的页面显示。点击 First, Previous, Next 或 Last 可浏览列表的各个页面。

更改一个 MAC 地址

选择您需要更改的 MAC 地址，然后点击 <Modify>。

移除一个 MAC 地址

选择您需要移除的 MAC 地址，然后点击 <Remove>。

查找一个 MAC 地址

输入 MAC 地址与 VLAN ID，然后点击 <Query>. 查找结果将被显示在地址窗口中。

点击 <OK> 可保存您在本页面所做的所有修改。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.3.9 VLAN

4.3.9.1 VLAN 模式（VLAN Mode）

本交换机有两种 VLAN 模式：(1) 基于端口的 VLAN（Port-Based VLAN），(2) 802.1Q 标记 VLAN（802.1Q Tagged VLAN）。本交换机以每个端口为基础支持这个功能，您需要设置以下栏位：

a) Port: 选择需要设置的端口。

b) VLAN Mode（VLAN 模式）

- 802.1Q Tagged VLAN: 依照 802.1Q Tagged VLAN 的规则来做出转发决定。
- Port-Based VLAN: 若端口是基于端口的 VLAN 模式，则 1）当该端口接收到标记（Tagged）封包时，将依照 802.1Q Tagged VLAN 的规则来做出转发决定； 2）当该端口接收到未标记（Untagged）封包时，将依照 Port-Based VLAN 的规则来做出转发决定。

限制

- 若一个端口为基于端口的 VLAN 模式，它将不能成为一个混杂端口（promiscuous port），也不能执行 802.1x 与 IGMP 侦听。
- 中继（Trunk）成员必须具备相同的 VLAN 模式。

点击 <OK> 可保存您在本页面所做的所有修改。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.3.9.2 标记 VLAN（Tagged VLAN）

图 27. GX2024X 标记 VLAN

图 28. GX2016X 标记 VLAN

您可以设置最多 229(GX2024X)/237(GX2016X)个 VLAN 群组，并在这个页面显示。交换机有一个默认的 VLAN。这一功能可避免交换机的不正常运行。除了默认的 VLAN1 以外，您可以移除其他任何一组既有的 VLAN。

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

- “U” type: 未标记的端口，从该端口传送出去的封包会被移除 VLAN 标记（tag）。
- “T” type: 自本端口传送的封包都会被标记。
- “blank” type: 本端口并非 VLAN 群组的成员。

其他可设置的栏位有：

- Show VLAN: 显示选定的既有 VLAN。
- Add a new VLAN: 选择建立一个新的 VLAN 群组。
- Name: VLAN 名称。
- VLAN ID: 当建立一个新的 VLAN 时，用户需要在这里输入 VLAN ID。
- Remove VLAN: 移除一个既有的 VLAN。这个栏位在建立新 VLAN 时不会出现。
- Private VLAN: 将这个 VLAN 设为私有 VLAN(PVLAN)。PVLAN 通过简易的 VLAN 设置，实现 VLAN 安全。系统管理员可以减少 VLAN 和 IP 资源消耗，却可获得相同的 VLAN 安全。我们不能使用默认的 VLAN (VLAN 1) 作为私有 VLAN(PVLAN)。在我们的系统中，最多可有 4 个 PVLAN。镜像功能中的监控端口不能成为 PVLAN 成员。静态组播群组不能应用于 PVLAN。一个 PVLAN 共有两种端口类型： 1) 混杂端口（Promiscuous Port） 2) 隔离端口（Isolated Port）。

  a) Promiscuous Port: 一个 PVLAN 必须且仅可拥有一个混杂端口。它与 PVLAN 内的所有端口通信。对于混杂端口，有如下限制：

  - 混杂端口必须为未标记端口

- 中继（Trunk）端口不能作为混杂端口（promiscuous）。
- 混杂端口不能运行于基于端口的 VLAN（Port-Based VLAN）模式。

b) Isolated Port: PVLAN 中的非混杂（non-promiscuous）端口。它与同一 VLAN 内的其他端口在第二层是完全隔离的，仅能与该 PVLAN 内的混杂端口通信。PVLAN 将封锁除了混杂端口流量之外的所有传送至隔离端口的流量。从隔离端口传出的流量仅可转发至混杂端口。流量控制对隔离端口无效。对于隔离端口，有如下限制：

- 隔离端口仅处理未标记的封包。若隔离端口接收到标记封包，会将其丢弃。
- 隔离端口仅能属于一个 VLAN，且此 VLAN 必须为私有 VLAN（PVLAN）。
- 隔离端口不能进行 IGMP 侦听。

- Priority Override: 当选择了 priority override(优先级重写)，基于 VLAN ID 的优先级重写（priority override）功能仅适用于本 VLAN 成员。当应用此功能时，带有此 VLAN ID 的任何封包的优先级（priority）栏位将被重写为所设置的新的优先级数值。VLAN 优先级重写（priority override）的优先级比端口默认的优先级及 IP 优先级更高。
- Priority: 若优先级重写（priority override）功能开启，这个值用来重写与此 VLAN ID 相关的任何帧的优先级。

若您想让 VLAN 成员依照 802.1Q Tagged VLAN 的规则来做出转发决定，您必须进入 VLAN Mode 页面并选择 802.1Q Tagged VLAN 模式作为这些端口成员的 VLAN Mode。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.3.9.3 基于端口的 VLAN（Port-Based VLAN）

基于端口的 VLAN（Port-Based VLAN）是依照目的地 MAC 地址及与其相关联的端口来做出封包转发决定的 VLAN。这是最简单和最常见的 VLAN 形式。在一个基于端口的 VLAN 中，系统管理员可指定交换机的端口至特定的 VLAN 群组。在这个页面中，您可以设置最多 26 (GX2024X)/18 (GX2016X) 个基于端口的 VLAN 群组，并将它们显示出来。

- Show Port-Based VLAN: 选择 Add a new VLAN 来建立一个新的群组，或选择一个既有的群组以显示下列栏位和端口图标：

- Name: 群组名称。
- Group ID: 当您建立一个新的基于端口的 VLAN 时，这个栏位需要您输入群组 ID（Group ID）。有效的群组 ID 值从 1 至 26 (GX 2024X)/18 (GX 2016X)。
- Remove Group: 移除一个既有的基于端口的 VLAN 群组。本栏位在建立新的基于端口的 VLAN 页面不会出现。

图 29: GX2024X 基于端口的 VLAN

若您想让新建的基于端口的 VLAN 生效，您必须到 VLAN Mode 页面选择 Port-Based VLAN 模式作为这些端口成员的 VLAN Mode 。

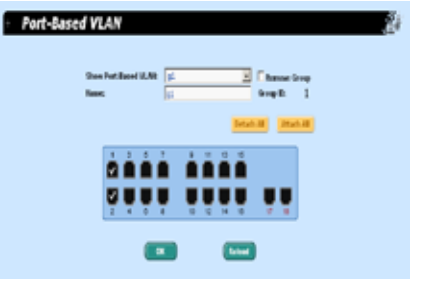


图 30: GX2016X 基于端口的 VLAN

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.3.10 默认端口 VLAN 与 CoS(Default Port VLAN and CoS)

本页面包含了每个端口与 VLAN 标记相关的栏位设置。这些设置项目如下：

- Port: 选择需要设置的端口
- PVID: 基于端口的 VLAN ID。从这个端口接收到的每一个未标记的封包都会标记为这个 VLAN 群组 ID。
- CoS (Class of Service) value: 从这个端口接收到的每一个未标记的封包都会被指定此 CoS 值到标记的 VLAN 中。

点击 <Modify> 将更改端口列表窗口中显示的内容。点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.4 SNMP 设置（SNMP Setup）

简单网络管理协议（SNMP）可用来管理网络。您可以使用 SNMP 设置页面来开启或关闭 SNMP 功能。

SNMPv3 可提供更多的安全管理和访问控制。SNMP 具有下列可设置的参数：

4.4.1 群组列表（Community Table）

您可以输入不同的群组名称并可勾选后面的框来为群组指定写入权限。点击 <OK> 保存设置或点击 <Reload> 更新页面。

图 31. 群组列表

4.4.2 主机列表（Host Table）

本页面将主机 IP 地址与群组列表（Community Table）页面中填入的群组名称连结在一起。输入一个 IP 地址并从下拉菜单中选择群组名称。点击 <OK> 保存设置或点击 <Reload> 更新页面。

图 32. 主机列表

4.4.3 Trap 设置（Trap Setting）

通过设置 trap 目的地 IP 地址与群组名称，您可以开启 SNMP trap 功能，传送不同版本（v1 或 v2c）的 trap 封包。点击 <OK> 保存设置或点击 <Reload> 更新页面。

图 33. Trap 设置

4.4.4 VACM 群组（VACM Group）

图 34. VACM 群组

VACM（View-based Access Control Model，基于检视的访问控制模型）群组可用来设置 SNMPv3 VACM 群组信息。

VACM Group 页面有下列可设置的参数：

- Group Name: 输入安全群组名称。
- Read View Name: 输入群组所属的读取检视名称（Read View Name）。相关的 SNMP 信息为 Get, GetNext, GetBulk。
- Write View Name: 输入群组所属的写入检视名称（Write View Name）。相关的 SNMP 信息为 Set。
- Notify View Name: 输入群组所属的通知检视名称（Notify View Name）。相关的 SNMP 信息为 Trap, Report。
- Security Model: 输入群组所属的安全模型（Security Model）。Any 适用于 v1,v2,v3。USM 则与 SNMPv3 相关。
- Security level: 输入群组所属的安全等级（Security level）。可选的项目有 NoAuth、AuthNopriv 与 AuthPriv。

点击 <Add> 以建立一个新的 VACM 群组。要移除一个既有的 VACM 群组，请选择需要移除的群组并按下 <Remove>。要更新一个项目，请选择需要更新的项目并按下 <Modify>。点击 <OK> 可保存对页面所做的更改。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.4.5 VACM 检视（VACM View）

VACM 检视用来查看 SNMPV3 VACM 群组信息。

图 35. VACM 检视

VACM 检视（VACM View）页面包含下列参数：

- View Name: 输入安全群组名称。
- View Type: 输入检视所属的检视类型（View Type）。当检视子树（View Subtree）与 SNMPv3 信息中的 OID 相符合时，选择包含(Included)或排除(Excluded)。

- View Subtree: 输入检视（View）所属的检视子树（View Subtree）名称。子树(Subtree)是一个 Oid，它与 SNMPv3 信息中的 Oid 相符合。当子树短于 SNMPv3 信息中的 Oid 时，为良好的符合状态。
- View Mask: 输入检视（View）所属的检视掩码（View Mask）。掩码的每个位代表了检视子树（View Subtree）中左侧看过来点与点之间的数字，而 '0' 表示无所谓。

点击 <Add> 可建立一个新的 VACM 检视（View）项目。 要移除一个既有项目，选择需要移除的检视并按下 <Remove>。要更新一个既有的项目，选择需要更新的检视并按下 <Modify>。点击 <OK> 可保存对页面所做的更改。点击 <Reload> 可更新设置。 要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.4.6 USM 用户（USM User）

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

USM 用户（USM User）页面包含下列参数：

图 36. USM 用户

- Engine Id: 输入符合管理员中 ID 的 Engine ID。
- Name: 在管理员中输入符合 Engine ID 名称与 Engine ID 的一个合并名称。
- Auth Protocol: 输入 Engine ID 与名称所属的 Auth Protocol。在这当中只能选择 NoAuth, MD5, SHA1 。若您选择了 NoAuth，则无须输入密码。
- Auth Password: 输入 Auth Protocol 所属的密码。在这里密码必须是至少八位的数字或字母。
- Priv Protocol: 输入 Engine ID 与名称所属的 Priv Protocol。 在这当中只能选择 NoPriv ,DES。若您选择了 NoPriv ，则无须输入密码。
- Priv Password: 输入 Priv Protocol 所属的密码。在这里密码必须是至少八位的数字或字母。

点击 <Add> 以建立一个新的 USM 用户项目。要移除一个既有项目，选择需要移除的检视并按下 <Remove>。要更新一个既有的项目，选择需要更新的检视并按下 <Modify>。点击 <OK> 可保存对页面所做的更改。点击 <Reload> 可更新设置。 要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.5 安全（Security）

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

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

4.5.1 端口访问控制（Port Access Control）

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

端口访问控制有两个设置：桥接设置（Bridge Setting）与端口设置（Port Setting）。

图 37. 端口访问控制

桥接设置（Bridge Setting）

桥接设置页面包含下列设置参数：

- Reauthentication: 开启本项目后，交换机会在重新认证时间（ReAuthentication Time）到时，试图重新认证端口的用户。
- Reauthentication Time: 若“Reauthentication”项目已开启，ReAuthentication Time（重新认证时间）指的是交换机重新发送认证请求到端口用户的时间间隔。
- Authentication Method: 可以使用 RADIUS 或本地数据库认证端口的用户。
- Quiet Period: 若从 RADIUS 或本地数据库认证失败，交换机再次发送认证请求到端口用户前需要等待的时间。
- Retransmission Time: 若端口用户未能响应交换机发出的认证请求，交换机再次发送认证请求到该端口用户前需要等待的时间。
- Max Reauthentication Attempts: 若端口用户未能响应交换机发出的认证请求，交换机重新发送认证请求的次数。

端口设置（Port setting）

端口设置页面包含下列设置参数：

- Port: 指定需要设置的端口。
- AuthMode(Authentication Mode): 若选择了 Port_based，则每个连接埠只需有一台主机（host）通过远程 RADIUS 服务器、远程 TACACS+ 服务器或本地用户数据库的认证。Port_based 支持多主机（Multi-host）及 GuestVID。若选择了 MAC_based，每个主机在访问网络之前都必须经过认证。MAC_based 不支持多主机（Multi-host）及 GuestVID。系统最多可支持 256 个尝试用 MAC_based 方式通过认证的主机。若选择了 MAC_based，建议您开启桥接设置中的 Reauthentication 项目。
- AuthCtrl (Authentication Control): 若选择了 Force_authorized，选定的端口被认为已强制通过认证。因此， 来自所有主机的流量都被允许通过。否则，若选择了 Force_unauthorized，选定的端口是封锁的，不允许任何流量通过。若选择了 Auto，选定端口的动作由 802.1x 协议来控制。
- Multi-host: 开启本项目后，只要连接到选定端口的所有主机中，有一部通过了认证，则所有连接到该连上接端口的主机都可以使用这个端口。若关闭本项目，则仅有通过认证的那部主机可以使用这个端口。若您在 Auth Mode 中选择了 MAC_based，则不支持 Multi-host。
- GuestVID: 访客 VLAN（Guest VLAN）可允许非 802.1x 用户端访客用户拥有受限的网络访问权限。

点击 <OK> 可保存更改。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.5.2 端口访问控制状态（Port Access Control Status）

端口访问控制状态（Port Access Control Status）页面分为两个部分： 所有端口的 802.1x 访问控制信息，以及端口初始化。

802.1x 访问控制信息

这个部分包括：

- Port: 端口号码
- AuthMode: 本栏位显示端口的认证模式 (authentication mode) 设置 (port_based 或 MAC_based)。
- AuthCtrl: 本栏位显示端口的认证控制（authentication control）设置（Force_authorized、Force_unauthorized 或 Auto)。

图 38. 端口访问控制状态

- Status: 本栏位显示每个端口（或请求认证的 MAC 地址）认证的结果，显示为 authorized（已认证）或 unauthorized（未认证）。
- VID: 本栏位显示端口的 VLAN ID。
- MAC: 本栏位显示已通过或未通过认证的 MAC 地址。

端口初始化 (Port Initialize)

这个部分包含下列设置参数：

- Port: 您想要强制此端口进行初始化的端口号码。点击 <OK> 保存设置。用户可以使用初始化功能发现通过集线器连接到某端口的新主机，以及要求新主机通过认证。

点击 <Reload> 可更新状态。

4.5.3 拨入用户（Dial-In User）

拨入用户（Dial-in User）选项用来定义交换机本地数据库中的用户。本项目包含下列设置参数：

- User Name: 新的用户名称。
- Password: 新用户的密码。
- Confirm Password: 再次输入密码以确认。
- Dynamic VLAN: 指定一个分配给 802.1x 认证之用户端的 VLAN ID。

图 39. 拨入用户

点击 <Add> 建立新的用户。若您想要做更改，请点击 <Modify>。若您想要移除一个选定的用户，请点击 <Remove>。点击 <OK> 保存设置，点击 <Reload> 更新设置。

4.5.4 RADIUS

若要使用外部 RADIUS 服务器，您需要设置以下参数：

- Authentication Server IP: RADIUS 服务器的 IP 地址。
- Authentication Server Port: RADIUS 服务器所侦听的端口号码。

图 40. RADIUS

- Authentication Server Key: 这个密钥用来在 GigaX 交换机与 RADIUS 服务器之间进行通信。
- Confirm Authentication Key: 再次输入密钥以确认。

点击 <OK> 保存设置，点击 <Reload> 更新设置。

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

4.5.5 TACACS+

若要使用外部 TACACS+ 服务器，您需要设置以下参数：

- Authentication Server IP: TACACS+ 服务器的 IP 地址。
- Authentication Server Port: 服务器所侦听的端口号码。
- Authentication Server Key: 这个密钥用来在 GigaX 交换机与 TACACS+ 服务器之间进行通信。

图 41. TACACS+

- Confirm Authentication Key: 再次输入密钥以确认。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

连接到交换机的 TACACS+ 服务器必须与系统管理界面位于同一个 VLAN 内。

4.5.6 端口安全（Port Security）

端口安全（Port security）页面包含了端口设置（port configuration），端口状态（port status）以及安全 MAC 地址（secure MAC addresses）功能。

4.5.6.1 端口设置（Port Configuration）

本页面用来设置端口安全（Port Security）功能的多个参数。本交换机最多可支持 1024 个安全 MAC 地址。用户可以设置端口的以下栏位：

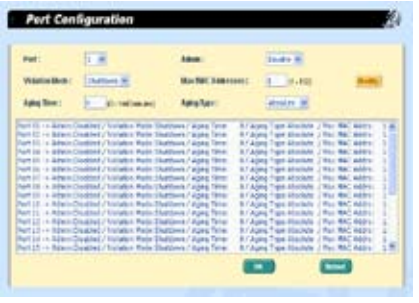


图 42. 端口设置

- Port: 选择需要设置的端口。
- Admin: 关闭／开启某端口的安全功能。
- Violation Mode: 本项用来设置当违反安全设置时端口的动作。下列状况均为违反安全设置：

  1) 地址表中已经添加了最大数量的安全 MAC 地址，而此时有一个 MAC 地址并不存在于地址表中的设备想要访问端口。

  2) 在一个安全界面内学习所得或设置的地址在同一 VLAN 内的另一个安全界面出现。您可以设置界面在违反安全设置时的三种模式：

     a) Protect: 在这个模式下，当有违反安全设置的事件发生时，您将不会被通知。

     b) Restrict: 在这个模式下，当有违反安全设置的事件发生时，您将会被通知。此时，系统将会记录信息，Violation 计数器的数值会增加。

     c) Shutdown: 在这个模式下，端口将立即变成封锁状态，系统将发送一个 SNMP trap 并记录信息，Violation 计数器的数值会增加。

- Max MAC Addresses: 设置安全 MAC 地址的最大数量。有效值范围从 1 至 132。所有端口这个值的总和必须小于或等于交换机允许的安全 MAC 地址的最大数量。
- Aging Time: 设置老化时间 （aging time）。有效值范围从 0 至 1440(分钟)。老化机制仅对动态 MAC 地址有效。若时间设置为 0，则没有开启此端口的老化机制。

- Aging Type: 老化类型决定了当安全 MAC 地址老化后的动作。每个端口支持两种类型的老化类型：

  a) Absolute: 端口的安全地址在老化时间到后会被移除。

  b) Inactivity: 若在指定的时间内没有来自该安全 MAC 地址的流量，则该地址才会被移除。

选择相应的端口号码并进行设置，然后点击 <Modify>。显示窗口的内容将会自动更新为您的新设置。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.5.6.2 端口状态（Port Status）

本页面显示了所有端口的端口安全信息，包括以下项目：

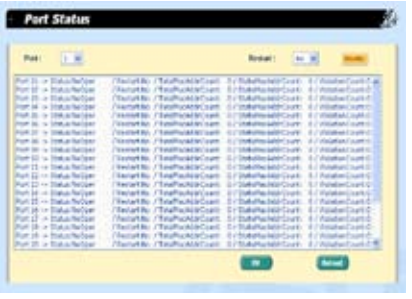


图 43. 端口状态

- Port: 端口号码。
- Status:

  a) NoOper: 表示端口的安全功能没有开启。

  b) SecureUp: 表示端口安全功能运行中。

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

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

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

- Restart: 是否重新开启处于 shutdown 状态下的端口 (Yes/No)。
- TotalMacAddrCount: 当前静态与动态安全 MAC 地址的总和。
- StaticMacAddrCount: 当前静态安全 MAC 地址的总数。
- ViolationCount: 违反安全设置事件的总数。

当下列情况发生时，端口的安全状态为 SecureDown：

- 端口未连接。
- 管理员桥接端口被关闭
- 该端口为中继端口。
- 该端口为端口镜像功能中的监控端口。
- 该端口正在执行 802.1x，且运行于单主机模式下。

若端口的状态为 Shutdown，用户可以选择相应的端口号码并将 Restart 设置为 Yes，然后点击 <Modify>。显示窗口的内容将会自动更新为您的新设置。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.5.6.3 安全 MAC 地址（Secure MAC Addresses）

用户可以新增 MAC 地址至端口的安全 MAC 地址表。通过这种方式新增的 MAC 地址不会从安全 MAC 地址表中老化。我们称其为静态安全 MAC 地址。

- MAC Address: 输入 MAC 地址。
- Port Selection: 选择 MAC 地址归属的端口。

在您新增了一个静态 MAC 地址后，请点击 <Add>。这个新项目将会显示在地址窗口中。

图 44. 安全 MAC 地址

用户可以从 Port Selection 中选择一个端口，然后点击 <Query>。这个端口当前的所有安全 MAC 地址将显示在地址窗口中。

用户可以从列表中选择一个端口，并按下 <Remove>，即可移除这个既有的地址。若您想要选中多个项目，请按住键盘上的 Shift 键，并用鼠标选择多个项目。

点击 <Add> 或 <Remove> 可使设置立即生效。要永久保存这些静态安全 MAC 地址，请至 Save Configuration 页面，然后点击 <Save>。

4.6 QoS

QoS 页面包含信任状态(trust state),映射(mapping)优先级重写(priority override),以及 CoS 功能(CoS function)。

4.6.1 信任状态(Trust State)

传入策略(Ingress Policy)的任务是,为队列控制器(Queue Controller)决定每个帧的优先级。本交换机以每个端口为基础支持这一功能,您只需设置以下栏位:

图 45. 信任状态

- Port: 选择需要设置的端口。
- Trust State: Trust DSCP 或 CoS。
  a) Trust CoS: 使用 IEEE 标记(Tags)。若帧为 IEEE 802.3ac 标记帧,则使用 IEEE 802.1p Traffic Class 栏位的数值作为帧的优先级。否则,使用默认的优先级数值。
  b) Trust DSCP: 使用 IP 作为优先级。若帧的 IP 为 IPv4 模式,则使用 IPv4 TOS 与/或 Diffserv 栏位的数值作为帧的优先级;若帧的 IP 为 IPv6 模式,则使用 IPv6 Traffic Class 栏位的数值作为帧的优先级。否则,使用默认的优先级数值。关于 Trust DSCP,相关的设置位于 Mapping 与 CoS 页面。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置,请至 Save Configuration 页面,然后点击 <Save>。

4.6.2 映射(Mapping)

本页面用来将 DSCP(差分服务代码点)值映射至 CoS(服务等级)优先级。有效的 DSCP 值范围为 0 至 63。对于 IPv6,DSCP 值乘以 4 得到的是流量等级(Traffic Class)的值。例如,DSCP 值 4 代表 IPv6 流量等级(Traffic Class)的值为 16。您只需设置以下栏位,即可开启交换机的这个功

图 46. 映射

能：

• DSCP: 选择 DSCP 值。

• CoS: 选择 CoS 优先级。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.6.3 优先级重写（Priority Override）

优先级重写（Priority Override）页面可让您开启或关闭 QoS 来源 MAC 地址优先级重写和目的地 MAC 地址优先级重写。

图 47. 优先级重写

若开启了来源 MAC 地址重写（priority override）功能，基于来源 MAC 地址的优先级重写功能对所有端口都有效。当一个封包的来源 MAC 地址与已添加至静态 MAC 地址表中并已指定了优先级的 MAC 地址项目相同时，即会执行来源 MAC 地址优先级重写。当发生这种状况时，指定给静态 ARL 表的优先级数值将替代封包先前的优先级数值。来源 MAC 地址优先级重写功能的优先级要高于端口的默认优先级、IP 优先级，及 VLAN 优先级重写功能。

若开启了目的地 MAC 地址优先级重写功能，基于目的地 MAC 地址的优先级重写功能对所有端口都有效。当一个封包的目的地 MAC 地址与已添加至静态 MAC 地址表中并已指定了优先级的 MAC 地址项目相同时，即会执行目的地 MAC 地址优先级重写。当发生这种状况时，指定给静态 ARL 表的优先级数值将替代封包先前的优先级数值。目的地 MAC 地址优先级重写功能的优先级是最高的，它要高于端口的默认优先级、IP 优先级、 VLAN 优先级重写，以及来源 MAC 地址优先级重写功能。

若您想要新增一个静态 MAC 项目并具有 CoS 优先级，请至 Static Addresses 页面。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.6.4 CoS

本交换机每个端口支持 4 个传出队列。也就是说，每个 CoS 值可映射到四个队列之一。队列 4 具有最高的优先级来传输封包。您可以指定以下的排序方式：

图 48. CoS

- Strict priority scheduling: 较低优先级队列中的封包只有在高优先级队列为空时才能被传送。
- Weighted round-robin (WRR) scheduling: WRR（加权循环排序）可防止在传送高优先级队列中的流量时，低优先级队列被完全忽略的状况。WRR 排序将轮流从每个队列中传送一些封包。传送的封包数量取决于相应队列的重要程度。例如，若队列一的权（weight）为 2，队列二的权（weight）为 4，则每次从队列一传送两个封包，从队列二传送四个封包。通过这种排序方式，即使高优先级队列不为空，低优先级队列也有机会来传送封包。在本交换机中，队列 1 的权为 1，队列 2 的权为 2，队列 3 的权为 4，队列 4 的权为 8。

点击 <OK> 可通过 HTTP 服务器将设置传送至交换机。点击 <Reload> 可更新设置。要永久保存新设置，请至 Save Configuration 页面，然后点击 <Save>。

4.7 线缆诊断（Cable Diagnosis）

线缆诊断（Cable Diagnosis）的主要功能是检测线缆错误（开路或短路）并报告预测的错误位置。此外，线缆诊断功能还可以检测 PHY 类型（10M, 100M 或 1000M）以及估测一般缆线的长度。缆线长度估测功能仅支持 Giga 速度模式。

只需选择端口号码，并按下 <Go>，即可显示检测结果。

图 49. 线缆诊断

当您开启端口的线缆诊断功能，则在诊断过程中，端口的网络连接将会中断。

4.8 统计图表（Statistics Chart）

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

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

图 50. GX2024X 流量比较

4.8.1 流量比较 (Traffic Comparison)

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

图 51. GX2016X 流量比较

4.8.2 错误群组（Error Group）

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

图 52. 错误群组

4.8.3 历史状态 (Historical Status)

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

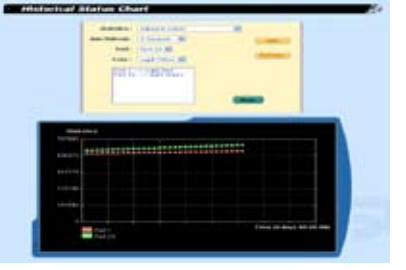


图 53. 历史状态

4.9 保存配置（Save Configuration）

要永久保存配置，您需要点击 <Save> 按钮。点击 <Restore> 可将配置恢复至出厂默认值。恢复出厂默认值后，您做的所有配置都将丢失。

图 54. 保存配置

5 命令行界面 (CLI)

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

当您进入 CLI 模式后，输入“?”将显示所有可用的命令帮助信息。若您对于 CLI 命令不熟悉，这将是非常有用的信息。CLI 模式若闲置 10 分钟即会超时。在超时后，您必须重新登录 CLI 模式。

```
Step 4
>>>>>>      ASUS OS Initialization Start (Phase 2)

System Parameters Reloading.....................[DONE]
Layer 2 Functions Initialization................[DONE]
CLI     Tree Initialization.................[DONE]
In-ROM File System Initialization..............[DONE]
RADIUSd Initialization..........................[DONE]
TACACSd Initialization..........................[DONE]
SNMPd Initialization............................[DONE]
Telnetd Initialization..........................[DONE]
HTTPd Initialization............................[DONE]
FTPd Initialization.............................[DONE]
SSHd Initialization.............................[DONE]

ASUS OS Initialization Success.

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

Login is required!
(ASUS)%
```

图 55. CLI 界面

所有的 CLI 命令都区分大小写。为了使它们更容易使用，您可以输入一个类型命令的全名，这个类型即成为您的工作类型。这样，如果您需要工作于 System 类别，您就不需要在每一条次命令前输入“sys”。例如，“sys”是一个命令类型，它包含了多个次命令。当您更改您的工作命令到“sys”，则您不需要在次命令前输入“sys”。当您进入“sys”工作类型后，系统提示符会变为“(system name) sys%”。

5.1 开机自检（Power On Self Test）

POST（开机自检）是在系统开机时进行的。它测试系统内存、LED 指示灯与交换机主板上的硬件芯片。系统测试和初始化完成之后会显示系统信息。您可以忽略这些信息直到出现“ASUS>:”提示（如图 55）。

5.1.1 Boot ROM 命令模式

```
>>>>>> Firmware slot 1 information

Firmware Starting Address ......................0xff900000
Firmware Age....................................0x24
Firmware Status.................................PASS
Firmware Version................................2.1.6
Firmware Creation Date..........................11/25/2005 17:31:50
Firmware Size...................................2104528 bytes
Firmware Checksum...............................0x1051
Firmware Starting Address.......................0x100000
Firmware Web Files Size ........................281545 bytes

>>>>>> Firmware slot 2 information

Firmware Starting Address ......................0xffc00000
Firmware Age....................................0x25
Firmware Status.................................PASS
Firmware Version................................2.1.6
Firmware Creation Date..........................11/28/2005 11:17:28
Firmware Size...................................2104576 bytes
Firmware Checksum...............................0x0ffc
Firmware Starting Address.......................0x100000
Firmware Web Files Size ........................281588 bytes


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

[Asus OS Boot]:
```

图 56. Boot ROM 命令模式

在 POST 过程中，您可以按下 <Enter> 键，以进入 “Boot ROM Command” 模式，如图 56 所示。

图 56 显示了本交换机的双固件映像。其中一个固件位于 Slot 1，另一个位于 Slot 2。

输入 “?” 可显示所有可用命令的说明信息。

尽管这些命令在有些情况下相当有用，但如果您不了解这些命令的功能，我们强烈建议您不要使用它们。

5.1.2 Boot ROM 命令

在 Boot 模式下输入“?”即可显示所有有效的命令列表。

表 7: Boot ROM 命令

命令	参数	用途	说明
a	NONE	显示 MAC 地址	
b	1 or 2 or a	支持双固件映像（dual image)。您可以指定一个 slot ID 来选择执行哪个固件，或设为“a”让系统自动选择。自动选择功能将会执行最新的固件。这是交换机默认的设置。	若您执行固件升级失败，您可以使用这一命令来用较旧的固件启动交换机。请在固件成功升级后将此项重新设置为自动选择。
c	IP address and mask / None	设置／显示 TFTP 客户端的 IP 地址。	
g	NONE	载入与执行固件	
h	NONE	显示在线说明	
p	NONE	显示当前设置	
r	NONE	系统重新启动	
s	IP address and mask / None	设置／显示 TFTP 服务器的 IP 地址	
t	NONE	进入安全模式	当配置文件损坏或您忘记了密码，请使用安全模式来进入CLI 模式。在这种模式下，您的配置文件会丢失。您需要恢复您的配置，或重新配置系统。
u	File name	通过使用 TFTP 协议的网络上传启动模块／固件	
v	NONE	显示开机 rom 版本	
w	NONE	管理员密码重置	

5.2 登录与登出

输入“login”即可进入 CLI 模式。当您首次登录时，请输入“admin”作为用户名称（无需输入密码）。为了安全考虑，请在登录后修改用户名称与密码。若您忘记了用户名称和密码，您可以联系华硕技术支持部门，或在 Boot ROM 命令模式中擦除所有配置文件。若您选择第二种方法，整个系统的配置将会丢失，您需要重新设置。

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

5.3 CLI 命令

本交换机提供了一系列 CLI 命令，用于所有的管理功能。这些命令的用途都已分类列出，形成一个网页管理界面。这样，您可以根据提示，如同使用网页界面一样方便正确地进行交换机的配置。“save”命令用于保存设置。有些 CLI 命令必须要等到执行了 “save”命令后才能生效。

使用“?”来获取所有可用命令和说明。
使用“/”来返回根目录。
使用“..”来返回上一层目录。
仅输入命令可获取该命令的说明。

5.3.1 系统命令

[System Name]

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

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

在 <*system name description*> 位置输入新的系统名称，即可更改交换机的系统名称。

```
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)%
(ASUS)% sys
(ASUS) sys% info
(ASUS) sys/info% name
Current system name is ASUS

(ASUS) sys/info% name GX2024X
System name is set to GX2024X
(GX2024X) sys/info%
```

图 57. SYS 命令

[System Contact]

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

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

在 <*system contact description*> 位置输入新的联系信息即可更改交换机的系统联系信息。

[System Location]

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

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

在 <*system location description*> 位置输入新的系统位置即可更改系统位置。

[VLAN ID]

显示交换机的 VLAN ID。用于管理时，VLAN ID 必须在同一个 VLAN 内。

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

[DHCP Client]

开启 DHCP 功能可取得动态 IP 地址，或关闭此功能以指定静态 IP 地址。若您开启了 DHCP，您可以更新或释放交换机的 IP 地址，并可使用 show 命令来显示动态 IP 地址。

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

[IP Address]

显示交换机的静态 IP 地址。这个 IP 地址用于管理用途，如网络应用（http 服务器，SNMP 服务器，ftp 服务器，telnet 服务器及 SSH 服务器）。

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

[Network Mask]

显示交换机的子网掩码。

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

[Default Gateway]

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

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

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

若开启了密码保护（password protection）功能，则当您想要使用浏览器访问交换机时，网页界面将会要求您输入用户名称与密码。

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

[Username]
[Password]
[Confirm Password]

默认的用户名称为 admin。在默认状况下，不需要输入密码。您可以通过设置这些栏位来设置密码。

CLI **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]

用户可使用 reboot 命令来重新启动交换机。

CLI **命令：**sys reboot

[Upload]

本功能没有对应的 CLI 命令。请参考 Boot ROM 命令。

[Backup Configuration File]

备份系统配置文件。请参考 7.4.7 通过控制终端（Console）备份系统配置文件 部分的说明。

CLI 命令 : sys files config backup

[Restore Configuration File]

恢复系统配置文件。请参考 7.4.8 通过控制终端（Console）恢复系统配置文件 部分的说明。

CLI 命令 : sys files config restore

5.3.2 物理界面命令

[Admin] [*Enable/Disable*]

显示端口的管理状态并允许用户开启或关闭端口。

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

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

显示端口当前的速率和双工模式。当端口的自动协商功能开启时，系统可自动侦测端口的速率和双工模式。

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

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

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

[Flow Control] [*Enable/Disable*]

显示端口的 IEEE802.3x 流量控制设置。注意：这个流量控制只能在全双工模式下才能运行。

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

[Reload]

从配置文件中恢复先前的端口设置。

CLI 命令 : l2 port retrieve

5.3.3 桥接命令

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

允许用户指定是否让交换机采用生成树协议(STP/ RSTP)。

CLI 命令 : l2 stp start <*stp / rstp*>

CLI 命令 : l2 stp *stop*

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

显示当前的 STP/RSTP 桥接参数设置。

CLI 命令 : l2 stp bridge set

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

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

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

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

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

显示当前的 STP/RSTP 端口参数设置。

CLI 命令 : l2 stp port set

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

Port <port number> Priority (0..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]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 stp retrieve

CLI 命令 : l2 stp bridge retrieve

CLI 命令 : l2 stp port retrieve

[Show Trunk]

显示指定的中继（trunk）群组设置。用户可以指定一个唯一的中继 ID，一个中继名称描述，LACP 模式（开启或关闭），以及其中继群组成员端口来建立一个新的中继群组。

CLI 命令 : l2 trunk show <*trunk id*>

[Create Trunk]

指定中继 ID，中继名称，LACP 模式及中继群组成员端口号码即可建立一个新的中继群组。

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

[Add/Remove Trunk]

您可以在一个既有的中继群组中新增或移除中继群组端口成员。

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

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

[LACP Action]

用户可以在一个指定的中继群组中开启或关闭 LACP 功能。

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

[LACP System Priority]

用户可以指定系统的优先级，用于运行 LACP。

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

[LACP Port Priority]

用户可以指定端口的优先级，用于运行 LACP。

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

[Reload]

从配置文件中恢复先前保存的中继设置。

CLI **命令 :** l2 trunk retrieve

[Mirror Mode] [*Enable/Disable*]
[Monitor Port] [*port number*]

显示交换机的镜像设置。

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

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

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

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI **命令 :** l2 mirror retrieve

[Show Multicast Group]

显示存在于组播群组列表中的静态组播群组。

CLI 命令 : l2 mcast show

[Set Multicast Group]

用户可以通过指定 MAC 地址、VLAN ID、VLAN 端口成员及未标记端口成员来新增或更改一个静态组播群组。注意：MAC 地址与 VLAN ID 的组合作为组播表中的项目。

CLI 命令 : l2 mcast set

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

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

port list [format: 1 2 3 4 - 26/* for all ports]: <port list> (GX2024X)

port list [format: 1 2 3 4 - 18/* for all ports]: <port list> (GX2016X)

[Remove Multicast Group]

用户可通过指定 MAC 地址与 VLAN ID，从组播列表中移除一个静态组播群组项目。

CLI 命令 : l2 mcast delete

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

vlan id: <vlan id>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 mcast retrieve

[IGMP is] [Enabled/Disabled]

如果需要，用户可以启用或终止第二层 IGMP 侦听功能。

CLI 命令 : l2 igmp <start/stop>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 igmp retrieve

[Ingress Bandwidth Control] [Enable/Disable]
[Mode][Bcast] or [Bcast, Mcast] or [Bcast, Mcast, DLF] or [All]
[Limit Rate]

所选定类型封包的总数限制值。

CLI 命令 : l2 rate ingress <port no: * for all ports> <enable/disable> [<mode (1:broadcast only, 2: broadcast and multicast, 3:broadcast, multicast and unknown unicast, 4:all)> <limit rate (70~250000 Kbps)>]

[Ingress Bandwidth Control] [Enable/Disable]
[Limit Rate]

传出流量的最大速率。

CLI 命令: l2 rate egress <port no: * for all ports> <enable/disable> [<limit rate (70~250000 Kbps)>]

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 rate retrieve

[Aging Time]

透挝设置 aging time 的值，用户可以设置 ARL (Address Resolution Logic) 项目的老化时间。

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

[Query by Port]

用户可根据端口号码来查询 ARL 表中的 ARL 项目。

CLI 命令 : l2 arl port <*port number*>

[Query by VLAN ID]

用户可根据 VLAN ID 来查询 ARL 表中的 ARL 项目。

CLI 命令 : l2 arl vlan <*vlan id*>

[Query by MAC Address]

用户可根据 MAC 地址来查询 ARL 表中的 ARL 项目。

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

[MAC Address]
[VLAN ID]
[Port Selection]

用户可以指定 MAC 地址、VLAN ID、端口号码，中继 ID、封包丢弃状况及优先级来新增或更改一个静态 ARL 项目。

CLI 命令 : l2 arl static <mac> <vlan id> <port no> <trunk id (0: not trunk)> <discard (0:No 1:destination)> <priority ('none' or 0-7)>

[Remove]

指出静态 ARL 项目的 MAC 地址和 VLAN ID 即可移除该项目。这两个栏位的组合构成了 ARL 表中的项目。

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

[Reload]

从配置文件恢复先前保存的配置。

CLI 命令 : l2 arl retrieve

[VLAN Mode] [802.1Q Tagged VLAN/Port-Based VLAN]

若端口处于 802.1Q 标记 VLAN 模式，则系统依据 802.1Q Tagged VLAN 的规则来做出转发决定。若端口处于 Port-Based VLAN 模式 : 1) 若端口接收到一个标记封包，将依照 802.1Q Tagged VLAN 的规则做出转发决定；2) 若接收到一个未标记封包，则依照 the Port-Based VLAN 规则做出转发决定。

CLI **命令 :** l2 vlan vlanmode set <VLAN Mode (1: 802.1Q Tagged VLAN, 2: Port-Based VLAN> <port list/*>

[Show VLAN]

显示交换机既有的 VLAN 信息。

CLI **命令 :** l2 vlan show <*vlan id*>

[Name]
[VLAN ID]
[Private VLAN]

允许用户进行 VLAN 设置。用户可以通过指定 VLAN ID、VLAN 名称描述及端口成员列表来新增一个 VLAN。注意：这里的端口成员指的是标记的端口成员。要指定一个 VLAN 端口成员作为未标记端口，可使用 CLI 命令 utportadd。用户可使用 CLI 命令 add 或 remove 来进一步新增端口成员至 VLAN 或将既有的端口从 VLAN 移除。用户可用 CLI 命令来指定 VLAN 类型为 'private' 或用 'create' 命令来建立一个私有 VLAN（private VLAN）。

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

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

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

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

[Remove VLAN]

允许用户完全移除一个既有的 VLAN。

CLI **命令 :** l2 vlan delete <vlan id>

[Promiscuous Port]

为私有 VLAN 设置混杂（promiscuous）端口。

CLI **命令 :** l2 vlan tagged promisport <vlan id> <promiscuous port id>

[Priority Override]
[Priority]

开启／关闭优先级重写功能并指定优先级数值。

CLI 命令 : l2 vlan tagged prioverride <vlan id> <priority override: enable/ disable> <priority>

[Show Port-Based VLAN]

显示交换机既有的 Port-Based VLAN 信息。

CLI 命令 : l2 vlan portbased show <group id: * for all port-based vlan groups>

[Name]
[Group ID]

允许用户进行 Port-Based VLAN 设置。用户可以通过指定一个群组 ID、群组的名称描述及其端口成员列表来新增一个群组。用户可使用 CLI 命令 add 或 remove 来进一步新增端口成员至群组或将既有的端口从群组中移除。

CLI 命令 : l2 vlan portbased create <group id> <group name> [<port list: * for all ports>]

CLI 命令 : l2 vlan portbased add <group id> <port list: * for all ports>

CLI 命令 : l2 vlan portbased remove <group id> <port list: * for all ports>

[Remove Group]

允许用户完全移除一个既有的 Port-Based VLAN 群组。

CLI 命令 : delete <group id: * for all port-based vlan groups>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 vlan retrieve

[Show Port]

显示端口设置。

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

[PVID]

通过指定一个 VLAN ID 及其相关联的端口成员列表即可为端口设置一个默认的 VLAN。

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

[CoS Value]

为未标记封包指定优先级标准数值（范围为 0-7）来设置端口的服务等级（Class of Service）。

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 port retrieve

5.3.4 简单网络管理协议（SNMP）

[Community Name] [Set]

一个群组（community）项目包含一个群组描述字串和一组特权（privilege）。Get Privilege 是默认为开启的，用户可以在新增项目时，指定是否开启 Set Privilege。

CLI 命令 : snmp community add

New community string: <new community string>

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

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

用户可以重新指定群组字串和特权 (privilege) 来更改群组 (community) 项目。

CLI 命令 : snmp community set

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

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

这一操作将会修改所有主机的群组名称，从 ‘*old community*’ 改为 ‘*new community*’。

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

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

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

允许用户从群组列表中删除一个群组项目。

CLI 命令 : snmp community delete

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

这一操作将会删除所有主机的某一群组。

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : snmp community retrieve

[Host IP Address] [Community]

一个主机项目包含主机 IP 地址、网络掩码与它所属群组。

CLI 命令 : snmp host add

Host IP/Subnet: <*IP address*>

Netmask: <*netmask*>

Community: <*community string*>

用户可以重新指定主机的 IP 地址、网络掩码与它所属群组来修改一个主机项目。

CLI 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>

允许用户从主机列表中移除一个主机项目。

CLI 命令 : snmp host delete

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : snmp host retrieve

[Trap Version] [v1/v2c]
[Destination]
[Community for Trap]

Trap 项目包含 SNMP 版本 (目前支持版本 1 与版本 2c) , 目的地 IP 地址与远程群组名称。

CLI 命令 : snmp trap add

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

Destination IP: <*IP address*>

Community: <*community string*>

用户可以重新指定 trap 项目的 SNMP 版本、目的地 IP 地址与群组名称来修改一个 trap 项目。

CLI 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 列表中删除一个 trap 项目。

CLI 命令 : snmp trap delete

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : snmp trap retrieve

[Group Name]
[Read View Name]
[Write View Name]
[Notify View Name]
[Security Model]
[Security level]

VACM (View-based Access Control Model) 群组项目包含群组名称、读取检视名称、写入检视名称，通知检视名称，安全模型、安全性等级与背景比较。

CLI 命令 : snmp snmpv3 access add

Group 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*>

用户可以重新指定 VACM 项目的群组名称、读取检视名称、写入检视名称，通知检视名称，安全模型、安全性等级与背景比较来修改一个 VACM 项目。

CLI 命令 : snmp snmpv3 access set

Group 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>

用户可以从 VACM 群组中删除一个 VACM 项目。

CLI 命令 : snmp snmpv3 access delete

Access entry: <entry id to delete>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : snmp snmpv3 access retrieve

[View Name]
[View Type]
[View Subtree]
[View Mask]

VACM (View-based Access Control Model) 检视 (View) 用来检视 SNMPv3 VACM 群组信息。一个 VACM 检视项目包含检视名称 (view name) 检视类型 (view type) 检视子树 (view subtree) 与检视掩码 (view mask)。

CLI 命令 : snmp snmpv3 view add

View Name: <*view name string*>

View Subtree [oid]: <*view subtree*>

View Mask: <*view mask*>

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

用户可以重新指定检视名称 (view name)、检视类型 (view type)、检视子树 (view subtree) 与检视掩码 (view mask) 来修改一个 VACM 检视项目。

CLI 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*>

用户可以删除一个 VACM 检视项目。

CLI 命令 : snmp snmpv3 view delete

View entry: <entry id to delete>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : snmp snmpv3 view retrieve

[Engine Id]
[Name]
[Auth Protocol]
[Auth Password]
[Priv Protocol]
[Priv Password]

USM (User-based Security Model) 用户用来设置 SNMPv3 USM 用户信息。USM 用户项目包含 engine Id，名称，认证协议，认证密码，隐私协议与隐私密码。

CLI 命令 : snmp snmpv3 usmuser add

EngineId: <engine id string >

Name: <user name string >

AuthProtocol [oid]: <auth protocol oid string >

AuthPassword: <auth password string>

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

Priv Password: <priv password string >

用户可以重新指定 engine Id，名称，认证协议，认证密码，隐私协议与隐私密码来修改 USM 用户项目。

CLI 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*>

用户可以删除一个 USM 用户项目。

CLI 命令 : snmp snmpv3 usmuser delete

USM user entry: <entry id to delete>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : snmp snmpv3 usmuser retrieve

5.3.5 安全命令

[Reauthentication]

用户可开启或关闭每隔一段时间的重新认证功能。

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

[Reauthentication Time]

用户可设置重新认证的时间。

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

[Authentication Method]

用户可设置认证方式(RADIUS 或本地数据库)。

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

[Quiet Period]

用户可设置 quiet period。

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

[Retransmission Time]

用户可设置重新传输时间。

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

[Max Reauthentication Attempts]

用户可设置重新认证的最多次数。

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

[AuthMode]

用户可选择认证模式 (Port_based/Mac_based).

CLI 命令: security dot1x port authmode <type (1: port_based 2:MAC_based)> <port list/*>

[Multi-host]

用户可开启或关闭某些特定端口的多主机功能。

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

[AuthCtrl]

用户可设置某些端口的认证控制功能。

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

[GuestVID]

用户可设置某些特定端口的访客 VLAN ID。

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

[Port Initialize]

用户可以强制这个端口执行初始化。这样可以发现通过集线器连接到这个端口的新主机并要求新主机通过认证。

CLI 命令 : security dot1x port initialize <port no: * for all ports>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : security dot1x retrieve

[User Name]
[Password]
[Confirm Password]
[Dynamic VLAN]

在交换机的本地数据库建立用户作为 802.1x 认证之用。一个用户项目包含用户名称、密码与动态 VLAN。

CLI 命令 : security dialinuser create

User Name: <user name string>

Password: <password string>

Confirm Password: <confirm password string>

VLAN ID: <dynamic VLAN>

CLI 命令 : security dialinuser remove <*user name/**> （用户可以从本地数据库中移除一个用户项目）

CLI 命令 : security dialinuser modify <*user name/**>（用户可以从本地数据库中修改一个用户项目，包括用户名称，密码与动态 VLAN）

User Name: <new user name string>

Password: <new password string>

Confirm Password: <new confirm password string>

VLAN ID: <new dynamic VLAN>

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : security dialinuser retrieve

[Authentication Server IP]
[Authentication Server Port]
[Authentication Server Key]
[Confirm Authentication Key]

用户可以设置 RADIUS 服务器 IP、服务器端口和服务器密钥。

CLI 命令 : security radius set

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

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

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

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : security radius retrieve

[Authentication Server IP]
[Authentication Server Port]
[Authentication Server Key]
[Confirm Authentication Key]

用户可以设置 TACACS+ 服务器 IP、服务器端口和服务器密钥。

CLI 命令 : security tacacs 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]

从配置文件中恢复先前保存的配置。

CLI 命令 : security tacacs retrieve

[Violation Mode] [Protect/Restrict/Shutdown]

用户可以设置某些特定的端口违反安全设置之模式 (Violation mode)。

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

[Max MAC Addresses]

用户可以设置安全 MAC 地址的最大数量。

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

[Aging Time]

用户可以设置某些特定端口的老化时间。

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

[Aging Type] [Absolute/Inactivity]

用户可以设置某些特定端口的老化类型。

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

[Restart]

用户可以重新启动某些特定的处于 ‘shutdown’ 状态下的端口。

CLI 命令 : security portsecu restart <port list/*>

[Port Selection]
[Query]

显示某些特定端口当前的安全 MAC 地址。

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

[MAC Address]
[Port Selection]
[Add]

新增静态安全 MAC 地址至端口。

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

[Remove]

用户可以指定 MAC 地址、VID 及端口号码来移除端口的一个安全 MAC 地址，或清除某些特定端口的所有安全 MAC 地址。

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

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : security portsecu retrieve

[Generate SSH key]

用户可以产生 SSH 密钥。SSH (Secure SHell) 为一种通过 shell 远程登录至一台机器的通信协议。这项协议与 telnet 功能相当类似，然而却又不同于 telnet，所有的客户端与服务器端的数据都是经过加密的。经过加密可以保护数据避免许多来自网络的安全性风险。目前来说，我们的交换机支持 SSH protocol version 2 并可在同一时间内登录一个用户。两对 SSH 密钥将会被建立并保存于交换机的闪存中。这两个密钥分别为 RSA 与 DSA 公共／私有密钥。

CLI 命令 : security sshkey start

[Reset SSH key]

重置 SSH 密钥至默认值。

CLI 命令 : security radius default

[Show Generating Status]

显示 SSH 密钥产生的状态。系统将显示“success”或“SSH keys generated fail”或“system is generating keys ...”。

CLI 命令 : security sshkey show

5.3.6 QoS 命令

[State] [CoS/DSCP]

用户可以设置某些特定端口的信任状态（trust state）。

CLI 命令 : qos trust state <cos/dscp> <port list/*>

[Map DSCP]
[to CoS]

用户可以设置 DSCP 至 CoS 映射。

CLI 命令 : qos map dscpcos <dscp(0-63):input single dscp value or dscp value range(ex:5-12)> <cos priority(0-7)>

[Source MAC Priority Override]

[Destination MAC Priority Override]

用户可以开启或关闭 QoS 来源 MAC 地址优先级重写与目的地 MAC 地址优先级重写功能。

CLI 命令 : qos prioverride set <SA priority override (0:disable 1:enable)> <DA priority override (0:disable 1:enable)>

[Scheduling Algorithm] [Strict/WRR]

可让用户使用强制优先级或基于权 (weight) 的优先级来排序。

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

[Priority]
[CoS Queue]

用户可指定缓冲队列（总共 4 组，使用 1-4 的队列 ID）的 CoS 优先级（范围 0-7）。

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

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : l2 cos retrieve

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : security portsecu retrieve

[Reload]

从配置文件中恢复先前保存的配置。

CLI 命令 : qos retrieve

5.3.7 线缆诊断

[Port]

开启端口的线缆诊断功能。

CLI 命令 : cablediag port <port no>

5.4 其他命令

sys time uptime: 显示系统启动后经历的时间。

sys time date: 显示当前的日期与时间。

sys time settime: 设置当前时间。

sys files config backup: 备份配置文件。

sys files config default: 恢复出厂默认之配置文件。

sys monitor auto: 开启或关闭风扇自动检测功能。

sys monitor set: 设置风扇速度命令。(1~255)

sys monitor show: 显示系统环境状态。

net ping: ping 远程的主机。

net route show: 显示路由表内容。

6. IP 地址、网络掩码与子网

6.1 IP 地址

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

本章节设置您已经了解了二进制，比特，字节等基础知识。

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

书写 IP 地址的习惯一般用十进制数字，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
在网络中确认电脑或设备身份。

每个 IP 地址的第一部分包含网络 ID，其余部分则是主机 ID。网络 ID 的长度取决于网络的级别（见下面的章节）。表 8 显示的是 IP 地址的结构。

表 8: IP 地址结构

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

下列是有效的IP 地址范例：

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

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

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

6.1.2 网络类型

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

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

B 类网络比 A 类网络小，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。

从field1可以轻松识别地址类型:
field1 = 1-126: A 类
field1 = 128-191: B 类
field1 = 192-223: C 类
(field1 值中缺少的部分留作特殊用途)

主机 ID 可以是范围内除0和255的任何值, 这些值已留作专用。

6.2 子网掩码

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

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

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

255.255.255.128

将其转换为二进位更容易看出它的真实面目：

11111111.11111111.11111111.10000000

就像 C 类地址一样，field1 到 field 3都是网络 ID，但是请注意 field 4 中第一个位元同样也被包括到了网络 ID 中。由于额外的位元只有两种值(0 和 1)，就表示网络有两个子网，每个子网使用剩余的 7 位元作为其主机 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 位元作为其主机 ID，范围是 0 到 63。

一些子网掩码并不表示额外的网络ID位元，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

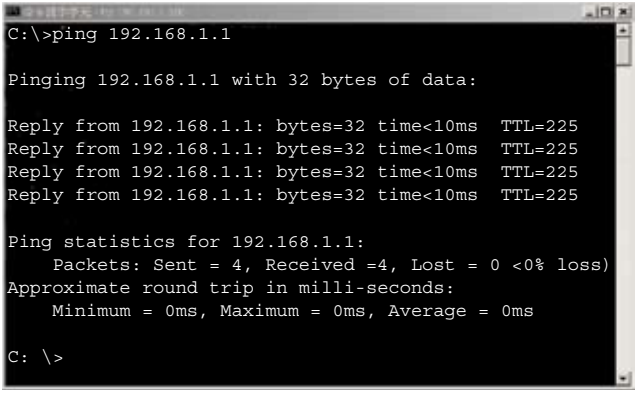


图 58. 使用 ping 工具

Ping 是用于检测您的电脑是否能够识别网络上其他电脑的命令。ping 命令向您指定的电脑送出一条信息，如果该电脑收到这条信息，它就会发送回应。要使用 ping 命令，您需要知道所联系的电脑的 IP 地址。

在 Windows® 操作系统的电脑上，您可以打开 **开始** 菜单，然后点击 **运行**，在提示符下键入命令如下:

ping 192.168.1.1

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

如果目标电脑收到了这个信息，就会出现如图 58 所示的提示。

如果无法定位目标电脑，就会显示信息“Request timed out”。

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

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

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

7.1.2 nslookup

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

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

nslookup

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

窗口就会显示相对应的 IP 地址 , 如图 59 所示。

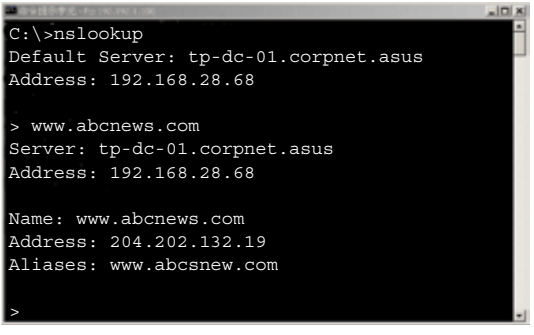


图 59. 使用 nslookup 工具

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

要退出 nslookup，在提示符处键入 exit 并按 <Enter>。

7.2 更换损坏的风扇

在您卸下交换机背面的风扇模块前，请关闭交换机电源。

当交换机背面任何一个风扇出现故障时，您可以按照下列步骤进行替换。

1. 拧开将风扇固定在背部的螺丝。

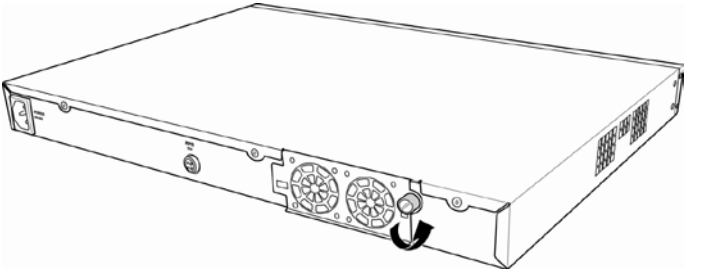


图 60. 拧开螺丝

2. 如图所示拉出风扇模块。

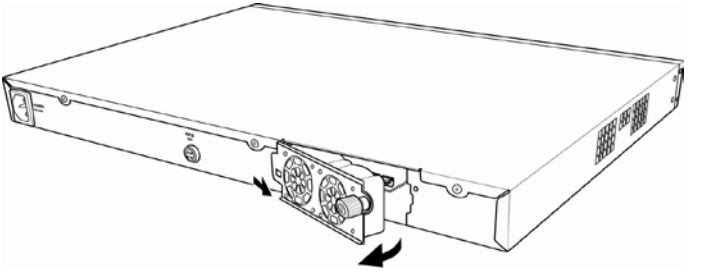


图 61. 拉出风扇模块

3. 小心地将两条电源线从风扇电源插座上移除。

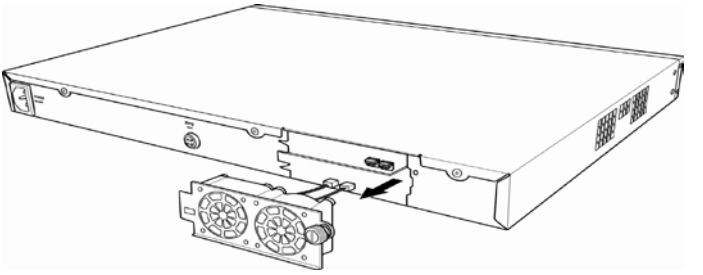


图 62. 卸下损坏的风扇

4. 松开将风扇固定于风扇模块上的螺丝，并移除损坏的风扇。
5. 将新的风扇装在原来风扇的位置，确保风扇电源线靠近模块底部。

按照同样的步骤替换另一个风扇。

6. 将风扇电源线连接到电路板上，确认风扇电源线连接到正确的接口。当您面对交换机背部面板时，左边的风扇是风扇1。
7. 将风扇模块置入交换机直至其卡入位置。确认风扇电源线没有卡在风扇模块和机体外壳之间。
8. 用螺丝固定风扇模块。检查风扇模块四周确认没有电线卡在风扇模块和机体外壳之间。

风扇规格

尺寸: 40 x 40 x 20 mm
电压与电流: 12VDC, 0.13A
转速: 8200RPM

7.3 简易维修

表 9. 疑难排解

问题	建议方案
LED灯号	
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 模块是否符合 RPS 标准。
FAN LED 呈琥珀色闪烁	检查交换机背部的风扇。如果其中任一个风扇有故障，参见 7.2 节的说明更换风扇。
当连接网线时，以太网 Link LED 不亮	1.确认以太网线是否正确地将交换机连接到您的局域网交换机/集线器/电脑。确认电脑/集线器交换机已经打开。 2.确认线缆长度是否符合您的网络的要求。1000 Mbps 网络(1000BaseTx)须使用标有 Cat 5 的缆线。 10Mbit/sec 缆线可能支持较低质量的缆线。
网络访问	
电脑不能访问同一网络中的另一个主机	1.检查以太网线是否完好，LED 灯号是否呈绿色。 2.如果端口的LED灯号呈琥珀色，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。
电脑无法显示网页设置界面	1.交换机已打开并且端口也已经启用。交换机的出厂默认 IP 为 192.168.1.1. 2.在您的电脑上确认您的网络设置。如果您的电脑没有设置一个有效的路由来连接到交换机，请将交换机 IP 改成您的电脑可以访问的 IP 地址。 3.从电脑 Ping 您的交换机 IP，如果失败，请重复第二步。 4.如果ping成功，但是网页设置界面仍不能使用，请通过 RS232 或 USB 连接控制终端。检查是否有过滤规则或静态 MAC 地址将 WEB 流量堵塞。

表 9. 疑難排解

问题	建议方案
网页设置界面	
丢失/忘记网页设置界面的用户名称或密码	1.如果您还没有修改用户名称和密码，请尝试用户名称“admin”，密码为空。 2.通过 RS232 或 USB 登录控制终端界面，在 Boot ROM 模式下用“psw”命令重置密码。
某些页面无法完全显示	1.确认您使用的是 Internet Explorer® v5.5 或以后版本的浏览器。不支持Netscape。您的浏览器必须启用 Javascript®，也必须支持 Java®。 2.Ping 交换机的 IP 地址检查连接是否稳定。如果一些ping封包丢失，检查您的网络设置，确认设置有效。
对设置的修改无法保存	确认点击了 Save Configuration 页面的 Save 按钮。
控制终端界面	
不能显示终端模拟器上的文字	1.出厂设置的波特率为 9600，无流量控制，8个数据位，无奇偶校验，1 个停止位。 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 驱动程序。 3.检查连接线是否良好。

7.4 上传与下载文件的步骤

7.4.1 通过 TFTP 上传启动模块

```
Firmware Starting Address ..........................0x100000
Firmware Web Files Size ............................281242 bytes
..
Hit Any Key to Enter Command Mode in 2 Second(s)

[Asus OS Boot]:
[Asus OS Boot]: c 192.192.1.100  255.255.255.0
IP Address Syntax Check ............................PASS
IP Address .........................................192.192.1.100
```

```
Configuration Save..................................DONE

(Asus) OS Boot: c 192.192.1.121  255.255.255.0
IP Address Syntax Check ............................PASS
Server IP Address...................................192.192.1.121
Configuration Save..................................PASS

(Asus OS Boot): u armboot.img
Please wait, this takes a while ...
TFTP from server....................................192.192.1.121
Our IP address is...................................192.192.1.100
File name...........................................armboot,img
Loading.............................................-
Total bytes transferred.............................2622311(400a7 hex)

Total Bytes Received................................2622311 bytes
Download Image Type.................................Boot ROM Image
Verify New Boot ROM Checksum Value..................PASS
Overriding current boot loader.Are you sure? (Y/N)...Y
Erasing Sectors.....................................DONE
Program Sectors.....................................DONE
---- Please Power Cycle to Activate the new Boot ROM ----
(Asus OS Boot):
```

图 63. 通过 TFTP 上传启动模块

1. 在控制终端（console）里，在系统开机自检时按下任意键，以进入 "Boot ROM Command" 模式。
2. 用命令 "c <IP Address> <Netmask>" 来设置 TFTP 客户端 IP 地址作为交换机的 IP 地址，如“c 192.192.1.100 255.255.255.0”。
3. 用命令 "s <IP Address> <Netmask>" 来设置启动模块所在的 TFTP 服务器的 IP 地址。如：“s 192.192.1.121 255.255.255.0”。
4. 用命令 "u <File Name>" 来上传启动模块。文件名为位于 TFTP 服务器的启动模块的名称，如：“u armboot.img”。
5. 输入 “Y” 来覆盖当前的启动程序。
6. 重新启动以开始启用新的启动模块。

7.4.2 通过 TFTP 上传固件

```
u         - Upload boot module/firmware via network using TFTP protocol
v         - Display boot rom version
w         - Toggle administrator password reset
[Asus OS Boot): u gx2024x_2.1.3.2.051026
Please wait, this takes a while ...
TFTP from server.................................192.192.1.121
Our IP address is................................192.192.1.100
File name........................................gx2024x_2.1.3.2_051026
Loading..........................................|/
Total Bytes transferred..........................2102720 (2015c0 hex)

Total Bytes Received.............................2102720 bytes
Download Image Type..............................Firmware Image
Checking Download Firmware Checksum..............PASS
Slot for New Firmware............................0
Erasing Sectors..................................DONE
Program Sectors..................................DONE
Checking New Firmware Checksum Value.............PASS

(Asus OS Boot):g
Firmware Boot Device.............................ON-BOARD FLASH
Configured Boot Slot.............................AUTO
Real Boot Slot...................................0
Verify Firmware Signature........................PASS
Verify Firmware Checksum.........................PASS
Decompress Firmware..............................DONE
Firmware is Starting at..........................0x100000

Adding 12103 symbols for standalone.

Step 1
>>>>>> ASUS OS Initialization Start (Phase 1)
```

图 64. 通过 TFTP 上传固件

1. 在控制终端（console）里，在系统开机自检时按下任意键，以进入 "Boot ROM Command" 模式。
2. 用命令 "c <IP Address> <Netmask>" 来设置 TFTP 客户端的 IP 地址作为交换机的 IP 地址，如：“c 192.192.1.100 255.255.255.0”。
3. 用命令 "s <IP Address> <Netmask>" 来设置固件所在的 TFTP 服务器的 IP 地址，如 “s 192.192.1.121 255.255.255.0”。
4. 用命令 “u <File Name>” 来上传固件，文件名为位于 TFTP 服务器的固件的名称，如：“u gx2024x_2.1.3.2_051026”。
5. 上传固件后，请使用命令 “g” 来载入与执行固件。

7.4.3 通过 FTP 上传固件

在您使用 ftp 功能及其他远程管理工具时，请确认您的 PC 与交换机位于同一 VLAN 下。交换机的 VLAN 可显示于网页管理界面的 System—>IP setup 页面，或您可使用 CLI 命令“net interface show”来显示 VID。

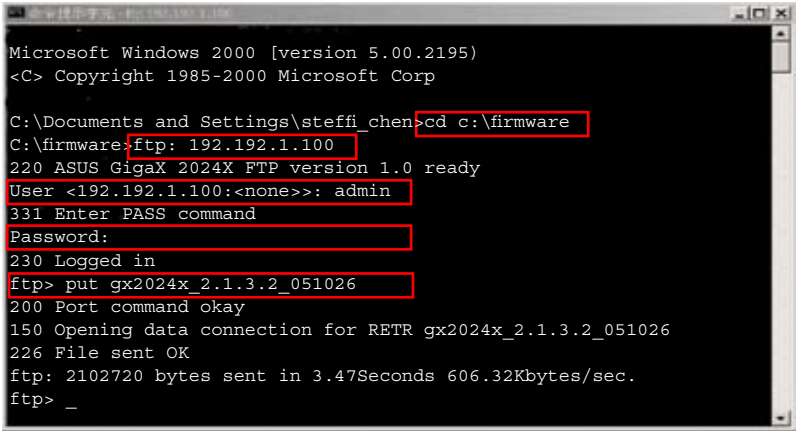


图 65. 通过 FTP 上传固件

1. 开启命令行界面窗口。
2. 将目录更改为固件所在的位置。
3. 用命令“ftp <IP Address>”来连接至交换机内部的 FTP 服务器，所以此 IP 地址为交换机的 IP 地址，如“ftp 192.192.1.100”。
4. 输入系统的用户名称。
5. 输入系统密码。
6. 用命令“put <File Name>”来上传固件。文件名为固件的名称，如“put gx2024x_2.1.3.2_051026”。

7.4.4 通过 FTP 上传自动配置文件（auto-config file）

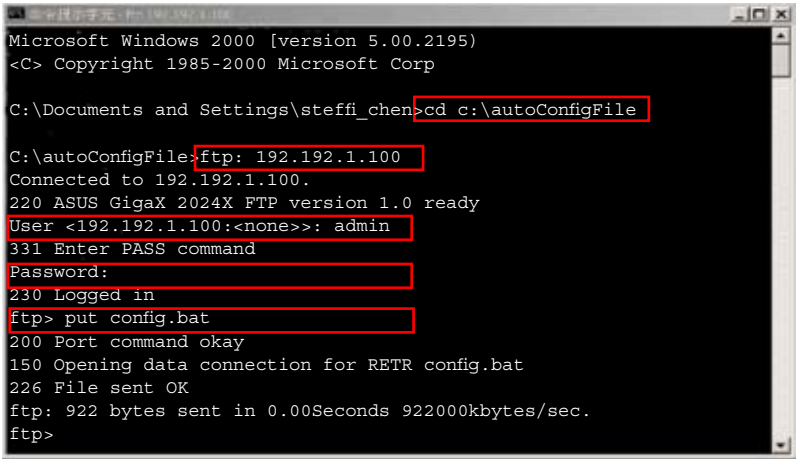


图 66. 通过 FTP 上传自动配置文件

在您使用 ftp 功能及其他远程管理工具时，请确认您的 PC 与交换机位于同一 VLAN 下。交换机的 VLAN 可显示于网页管理界面的 System-->IP setup 页面，或您可使用 CLI 命令“net interface show”来显示 VID。

自动配置文件（auto-config file）是一个由 CLI 命令构成的文字档，当这个文件载入交换机后，交换机将执行这些命令。

1. 开启命令行界面窗口。
2. 将目录更改为自动配置文件所在的位置。
3. 用命令“ftp <IP Address>”来连接至交换机内部的 FTP 服务器，所以此 IP 地址为交换机的 IP 地址，如“ftp 192.192.1.100”。
4. 输入系统的用户名称。
5. 输入系统密码。
6. 用命令“put <File Name>”来上传自动配置文件。文件内容的开头必须为“#autoconfig”，且自动配置文件的名称必须为“config.bat”，如：“put config.bat”。

7.4.5 通过 FTP 备份系统配置

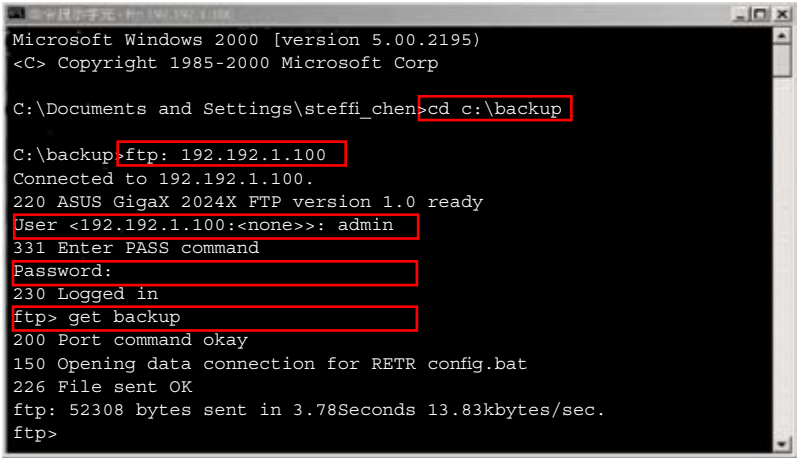


图 67. 通过 FTP 备份系统配置

在您使用 ftp 功能及其他远程管理工具时，请确认您的 PC 与交换机位于同一 VLAN 下。交换机的 VLAN 可显示于网页管理界面的 System-->IP setup 页面，或您可使用 CLI 命令“net interface show”来显示 VID。

1. 开启命令行界面窗口。
2. 将目录更改为系统配置文件所在的位置。
3. 用命令“ftp <IP Address>”来连接至交换机内部的 FTP 服务器，所以此 IP 地址为交换机的 IP 地址，如“ftp 192.192.1.100”。
4. 输入系统的用户名称。
5. 输入系统密码。
6. 系统配置文件的默认名称为“backup”。用户必须使用这一名称来备份系统配置。您可以在下载文件后重新命名文件。

7.4.6 通过 FTP 恢复系统配置

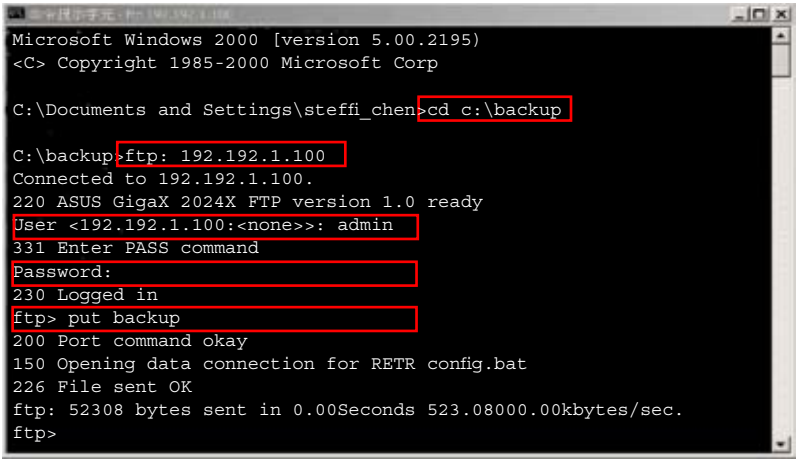


图 68. 通过 FTP 恢复系统配置

在您使用 ftp 功能及其他远程管理工具时，请确认您的 PC 与交换机位于同一 VLAN 下。交换机的 VLAN 可显示于网页管理界面的 System-->IP setup 页面，或您可使用 CLI 命令“net interface show”来显示 VID。

1. 开启命令行界面窗口。
2. 将目录更改为自动配置文件所在的位置。
3. 用命令“ftp <IP Address>”来连接至交换机内部的FTP服务器，所以此 IP 地址为交换机的 IP 地址，如“ftp 192.192.1.100”。
4. 输入系统的用户名称。
5. 输入系统密码。
6. 用命令 “put <File Name>” 来恢复系统配置。此文件必须是同一交换机机型的备份文件如：“put backup”。

7.4.7 通过控制终端（Console）备份系统配置

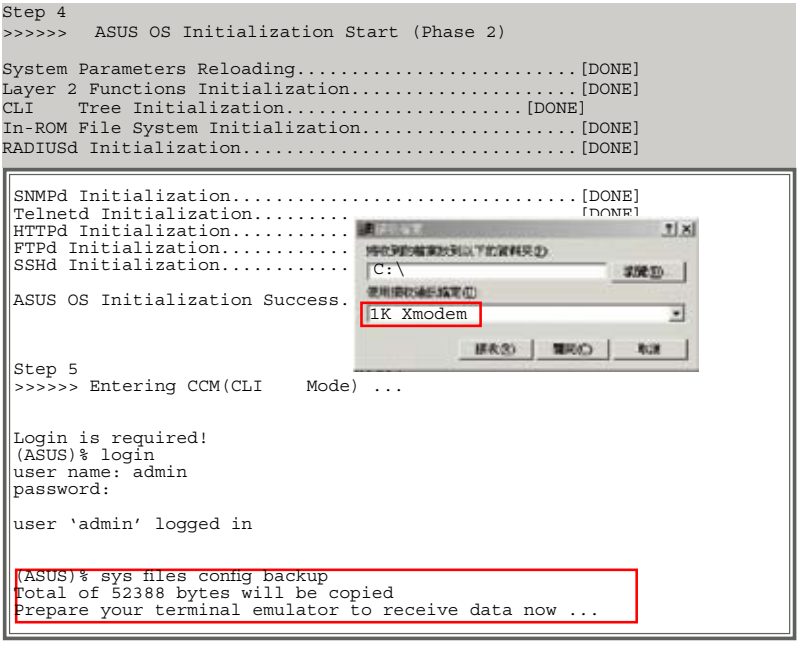


图 69. 通过控制终端备份系统配置

1.将您的控制终端速率设置为 9600bps。

2.执行 CLI 命令 “sys files config backup” 。

3.通过终端用 1K Xmodem 接收系统配置。

7.4.8 通过控制终端（Console）恢复系统配置

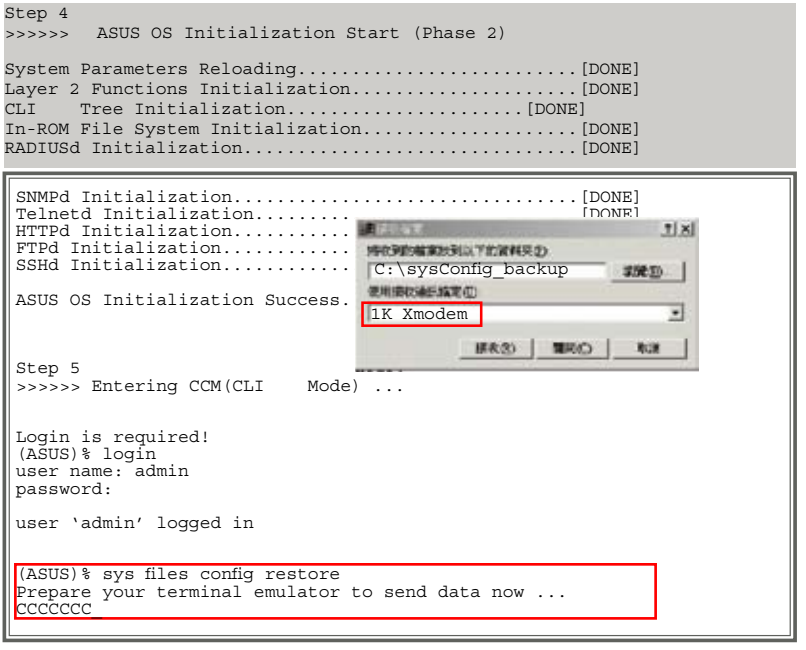


图 70. 通过控制终端备份系统配置

1. 执行 CLI 命令“sys files config restore”。此文件必须是同一交换机机型的备份文件。
2. 通过终端用 1K Xmodem 传送系统配置。

8. 术语表

10BASE-T	用于以太网的有线线缆，数据传输率为 10Mbps。亦称 3 类线 (CAT 3)。参见data rate, Ethernet。
100BASE-T	用于以太网的有线线缆，数据传输率为 100Mbps。亦称 5 类线 (CAT 5)。参见data rate, Ethernet。
1000BASE-T	用于以太网的有线线缆，数据传输率为 1000Mbps。
binary	二进制。“基于2”的数字系统，只使用 0 和 1 两个数字来表示所有的数字。在二进制中，十进位数字 1 写作 1，十进位数字2 写作10，十进位数字 3 写作11，十进位数字 4 写作 100，依次类推。虽然IP地址为方便起见表示为十进位数字， 实际上它使用的是二进制数字。比如 IP 地址 209.191.4.240 转换为二进制是 11010001.10111111.00000100.11110000。比特，IP 地址，网络掩码同样也是二进制。
bit	比特。“二进制数字”的缩写，一个比特就是一个只有0, 1两种数值的数字。参见 binary。
bps	比特每秒
CoS	服务等级。在802.1Q 中规定，值的范围为0到7。
DSCP	差分服务代码点 IP 报头中差分服务部分最重要的六位被称为DSCP。GigaX 系列中可用的DSCP 值有 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46,48 和 56。
broadcast	广播。将数据发送到网络上所有的电脑。
Ethernet	以太网。最常见的电脑网络技术,通常使用双绞线。以太网的数据传输速率为10Mbps和100Mbps。参见 10BASE-T, 100BASE-T, twisted pair。
FTP	文件传输协议 用于连接到 Internet 的电脑之间的文件互传。常见的用途包括上传或更新网页服务器上的文件，从网络服务器下载文件。
host	主机。连接到网络的设备(通常指电脑)。
HTTP	超文本传输协议 HTTP 是用来进行网络数据传输的最主要的协议，可以通过网页浏览器显示。参见web browser, web site。

ICMP	互联网控制信息协议 一种互联网协议，用于报告错误与其他网络相关信息。ping 命令就是基于这种协议。
IGMP	互联网群组管理协议 一种互联网协议，允许电脑与其网络成员通过组播群组共用信息。一个电脑组播群组就是群组的成员都设置成从成员处接收特定的内容信息。向IGMP群组传送组播的应用可随时更新群组的地址簿或将公司的通告传送到收信人列表。
IGMP Snooping	在每个端口侦听IGMP封包并将端口与二层组播群组相关联。
Internet	互联网，用于私人或商业通信。
intranet	私有的公司内部网络，看起来像互联网(Internet) 的一部分(用户使用网页浏览器来访问信息)，但是只能被本公司员工所使用。
IP	参见 TCP/IP。
IP address	Internet 协议地址 主机（电脑）在互联网上的地址，它包含四个数字，每个数字的范围是0~255，用小数点分隔。如，209.191.4.240。一个 IP 地址包含了网络 ID 和主机 ID，网络 ID 表示主机属于哪个特定的网络，主机 ID 则是网络中确定该主机的唯一标志。网络掩码用来定义网络 ID 和主机 ID。由于 IP 地址比较难记，它们通常都对应一个域名（domain name）。参见 domain name, network mask。
ISP	网络服务提供商 向顾客提供互联网访问服务的公司，通常是收费的。
LAN	局域网 存在于一个较小地理范围内的网络，例如家里，办公室或大楼。
LED	发光二极管 一种电子发光设备。交换机前面的指示灯就是LED。
MAC address	媒体访问控制地址，简称MAC 地址 由制造商分配的设备的永久性硬件地址。MAC 地址由六对字符组成。

mask	掩码。参见 network mask。
Multicast	组播。将数据传送到一组网络设备上。
Mbps	百万比特每秒的缩写。网络数据传输率常表示为Mbps。
Monitor	监控。亦称“Roving Analysis”，允许将一个网络分析器连接至端口上并使之监测交换机的其他端口。
network	网络。指连接在一起，允许相互通信和共用资源（如软件、文件等）的一组电脑。网络可以是小型的，例如局域网(LAN)，也可以是大型的，例如互联网。
network mask	网络掩码。网络掩码就是一系列的比特字串用于IP地址，以决定网络ID和主机ID的位数。1 表示此位有效，0表示忽略此比特。举例说明，如果网络掩码 255.255.255.0 用到IP地址100.10.50.1，网络ID为100.10.50，主机 ID 为 1。参见 binary, IP address, subnet,“IP Addresses Explained” 部分。
NIC	网络接口卡 插入电脑，提供网络线缆的物理接口RJ-45 的适配器。参见Ethernet，RJ-45。
packet	封包，在网络上传输数据的单位。每个封包都包含数据、添加的信息，如它从哪里来（来源地址）及将到哪里去（目的地地址）。
ping	封包探测 用于确认IP 地址对应的主机是否能够到达。它亦可用于寻找与域名相对应的 IP 地址。
port	端口。物理的网络设备接入点，如电脑，路由器，数据通过该接入点流入流出。
protocol	协议。一系列用于控制数据传输的规则。为了使数据能够成功传输，数据传输来源和目标都必须遵守相同协议的规则。
PVLAN	私有虚拟局域网
QoS	服务质量（Quality of Service） 在802.1Q 中定义。对于数据通信网络性能， QoS特性有带宽、延迟和可靠性。
remote	远程。即物理上处于不同地点。比如说，一名职员出差在外时登录公司的 intranet, 他就是远程用户。
RJ-45	注册端口标准45

	这种 8-pin 的插头是用于在电话在线传输数据的。以太网线通常也会使用这种插头。
RMON	远程监控
	SNMP 的延伸，提供综合性的网络监视功能。
routing	路由。在您的网络和互联网之间，根据来源IP地址和网络情况，选择最有效的路径转发封包。执行路由选择的设备称为路由器。
SNMP	简单网络管理协议
	用于管理网络的 TCP/IP 协议。
STP	生成树协议
	防止封包在复杂网络中造成回路的桥接协议。
subnet	子网。子网是网络的一部分，子网通过将网络中的电脑归分为小组而使这些电脑与其他网络上的电脑分隔开来。子网中的电脑仍然在物理上与其他上层网络相连，但是他们被认为是一个独立的网络。参见network mask。
subnet mask	子网掩码。将子网之间加以区分的掩码。参见network mask。
TCP	参见 TCP/IP。
TCP/IP	传输控制协议/互联网协议
	这是互联网上基本的协议组。TCP负责将数据分为可以在互联网上传输的封包，IP负责将这些封包传送到目的地址。当 TCP 和 IP 与一些上层应用进行捆绑如 HTTP, FTP, Telnet等，TCP/IP 指的确是整套协议组。
Telnet/SSH	一种互动的，以字符为基础的，用于访问远程电脑的程序。HTTP (网络协议)和 FTP 只允许从远程电脑下载文件，而 Telnet/ SSH 允许从远程登录并使用电脑。
TFTP	小型文件传输协议
	一种传输文件的协议。TFTP 比 FTP 更加容易使用，但是性能和安全性不如 FTP。
Trunk	两个或两个以上的端口合而为一成为一个虚拟端口，也称为链路汇聚。
TTL	存活时间
	IP 封包的一个栏位，决定了该封包的寿命。TTL 原本表示的是持续时间，现在则通常用于表示最大计跳数，每经过一跳都消耗一个计跳数，当 TTL 为零时，该封包就被

丢弃。

twisted pair　双绞线。即普通的铜制电话线。它包含一对或多对互相缠绕的电线，以消除干扰和杂音。每根电话线使用一对线，在家用情况下，通常都安装两对。对于以太网局域网，使用的是一种高端的，用于10BASE-T网络的三类线(CAT 3)，以及更高端的100BASE-T 网络的五类线 (CAT 5)。参见 10BASE-T，100BASE-T，Ethernet。

upstream　上行。数据从用户流向互联网的方向。

VLAN　虚拟局域网

WAN　广域网络

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

Web browser　网页浏览器。一种使用超文本传输协议 (HTTP) 的，用于从网站下载/上传信息的软件。这些信息包括文本，图像，声音或视讯。网页浏览器使用了超文本传输协议(HTTP)。常用的网页浏览器包括 Netscape Navigator 和 Microsoft Internet Explorer。参见HTTP, web site。

Web page　网页。一个网站的文件通常包括文本，图像，和连接到其他页面的超链接。当用户访问一个网站时，显示的第一页成为主页。参见 hyperlink, web site。

Web site　网站。互联网上通过网页浏览器为远程用户的提供信息的电脑。网站常由包含文本，图像，超链接的网页构成。参见hyperlink, web page。