敬告：

请做好静电保护！干燥的空气或者线路从地毯下通过导致静电聚集，严重的会损坏设备芯片。

保护设备，请注意：

- 在安装设备前，把所有设备做好接地工作。
- 尽量把网线固定在墙壁的某一边缘。

Electronic Emission Notices

Federal Communications Commission (FCC) 声明：

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which is designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromag -netic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:

EN55022(1988)/CISPR-22(1985)	class A
EN60555-2(1995)	class A
EN60555-3	
IEC1000-4-2(1995)	4K V CD\8KV\AD
IEC1000-4-3(1995)	3V\m
IEC1000-4-4(1995)	1KV – (power line) 0.5KV – (signal line)

目　录

一、安装前注意事项

为避免使用不当造成设备损坏及人身伤害，请遵从以下注意事项：

- 在清洁交换机前，应先将交换机电源插头拔出。请用干净干燥抹布擦拭交换机，不可用液体清洗交换机。
- 请不要将交换机放在水边或潮湿的地方，以防止水或湿气进入交换机内部。
- 请不要将交换机放在不稳固的地方，以防跌落对交换机造成严重损害。
- 应保持室内通风良好，并保持交换机通气孔处畅通。
- 交换机要在额定的电压范围内才能正常工作，请确认工作电压同交换机所标示的电压相符。

检查安装场所

交换机必须在室内使用，无论您将交换机安装在机柜内还是直接放在工作台上，都需要保证以下条件：

- 确认交换机的出入风口有足够空间，以利于交换机机箱的散热。
- 确认机柜和工作台自身有良好的通风散热系统。
- 确认机柜和工作台足够牢固，能够支撑交换机的重量。
- 确认机柜和工作台有良好接地。

为保证交换机正常工作和延长使用寿命，安装场所还应该满足下列要求：

A、温/湿度要求

为保证交换机正常工作和延长使用寿命，机房内需保持工作温度：0℃~40℃，工作湿度 5%~90%RH。若机房内长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件锈蚀等现象。若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，同时在干燥气候环境下易产生静电，危害交换机电路。温度过高危害更大，长期高温将加速绝缘材料的老化，使交换机可靠性大大降低，严重的影响工作寿命。

B、洁净度要求

灰尘对交换机运行安全会造成很大的危害。室内灰尘落在机体上，可以造成静电吸附，使金属接插件或金属接点接触不良。尤其在室内相对湿度偏低的情况下，更易造成静电吸附，不但会影响设备寿命，而且容易造成通信故障。除灰尘外，交换机机房对空气中所含盐、酸、硫化物也有严格要求。这些有害气体会加速金属腐蚀和某些部件的老化过程。机房内应防止有害气体如 SO_2、H_2S、NH_3、CL_2 等入侵。

C、抗干扰要求

交换机在使用中可能受到来自系统外部干扰，这些干扰通过电容耦合、电感耦合、电磁波辐射、公共阻抗（包括接地系统）耦合和导线（电源线、信号线和输出线等）传导方式对设备产生影响。

为此应注意：

交流供电系统为 TN 系统，交流电源插座应采用有保护地线（PE）的单相三线电源插座，使设备上滤波电路能有效滤出电网干扰。交换机工作地点应远离强功率无线电发射台、雷达发射台、高频率大电流设备。必要时采取电磁屏蔽方法，如接口电缆采用屏蔽电缆。接口电缆要求在室内走线，禁止户外走线，以防止因雷电产生过电压、过电流将设备信号口损坏。

二、安装指导

一、产品配置表

在开始安装交换机前，请检查产品包装中有以下配件：

- 一台交换机
- 托架附件 （19” 机架）
- 一本中文用户指南
- AC 电源线

二、设置交换机

1. 安装好交换机与架置辅助部件
2. 接通电源
3. 连接交换机与终端 PC
4. 出厂默认设置如下：

设置 IP 地址：192.168.1.3

子 网 掩 码：255.255.0.0

默 认 网 关：192.168.1.1

初 始 用 户：admin

初 始 密 码：无

注：在终端 PC 连接交换机设置时，要保证 PC 机的 IP 地址属于 192.168.1 网段，即设 IP 地址为 192.168.1.2～192.168.1.254 之间的任意 IP，这样才能正常访问本交换机设置页面。

5. 恢复出厂设置：

在交换机断电情况下，按住交换机前面板左上角的复位开关，并通电，一直等看到 SYS 指示灯猛闪（时间大约 5-10 秒），即表示恢复出厂设置。

三、安装交换机

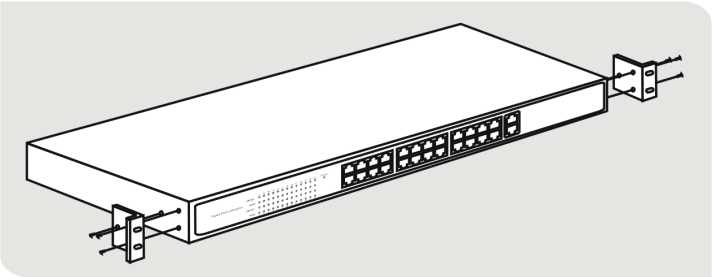
1、准备工作

交换机需要安装在通风良好的环境下。请确认有良好的通风，同时交换机四周要留出 100 毫米（4 英寸）的空间。

将交换机安装在 19 英寸标准机架

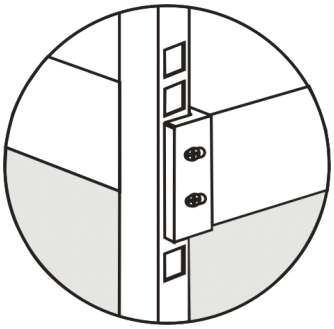
每个交换机都提供了一套耳片，用来将交换机安装在 19 英寸机架上。每套耳片包括两片耳片和六个螺丝。

第一步。 按照下图指示方向，将耳片用螺丝固定在交换机上。



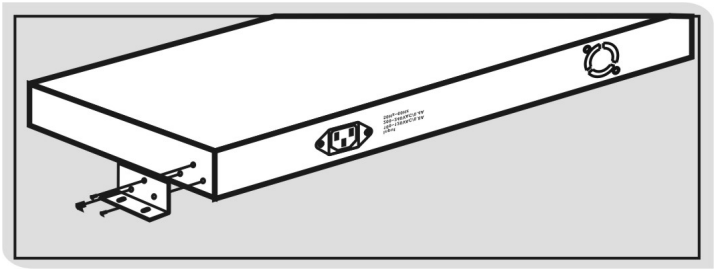
第二步：将交换机放入 19 英寸机架，并确认留有足够的通风距离。

第三步：按照下图的指示，用螺丝将耳片锁定在机架上。

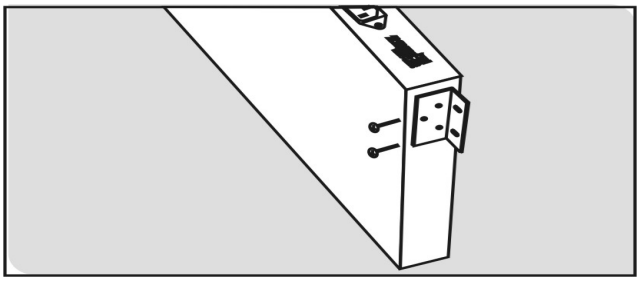


2、将交换机安装在墙壁

第一步：按照下图指示方向，将耳片用螺丝固定在交换机上。



第二步：按照下图指示，使用 5/8 英寸 12 号木螺丝（未提供）将耳片固定在墙壁。

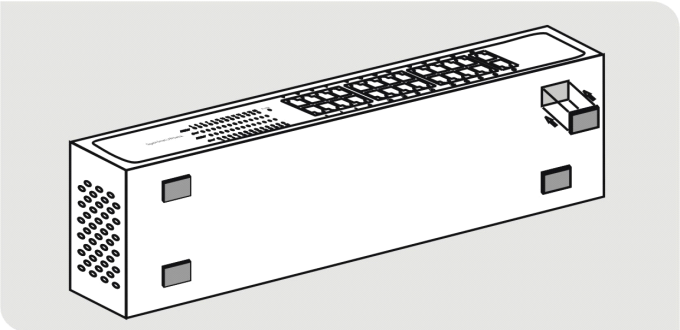


3、将交换机安装到桌面

在交换机的包装中提供了四个橡胶垫。这些橡胶垫可以防止交换机在桌面滑动。

第一步：将橡胶垫背面的贴纸揭开。

第二步：如下图，将橡胶垫牢固的粘贴在交换机底部。



第三步：将交换机摆放在平坦的位置。

4、将交换机连接交流电源

在交换机的包装内，有一条符合您国家电源插座规范的电源线。如果您发现电源线的规格不正确请联系当地的经销商更换。

第一步：将电源线母头一端插入位于交换机后面板的主电源插座。然后将另一端接入交流电源。

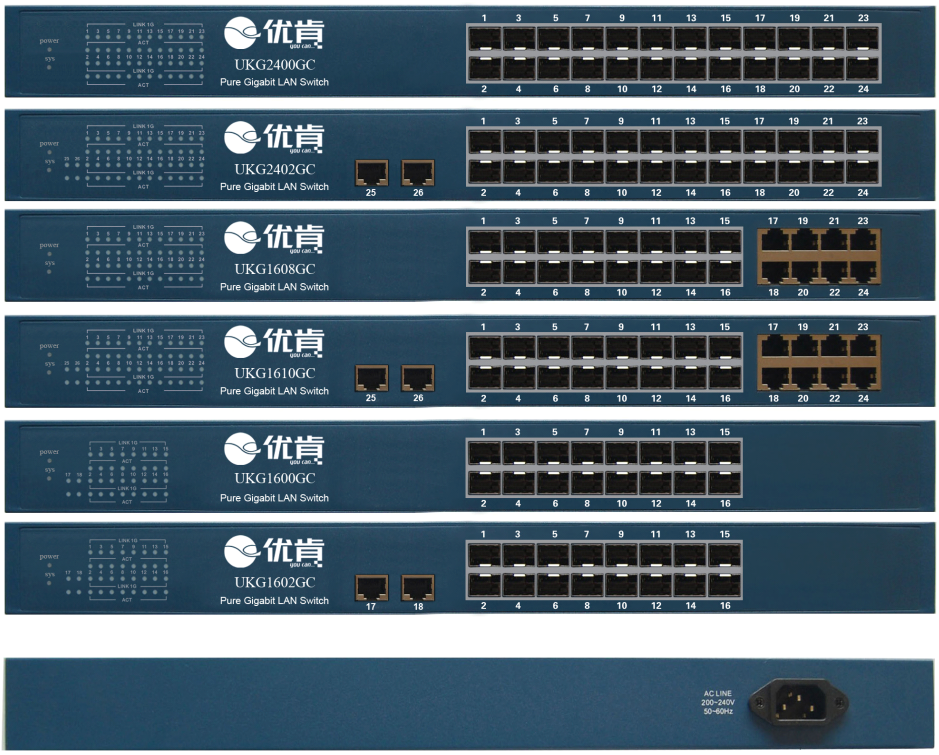
第二步：一旦交换机接入交流电源，交换机将立即开始工作。

三、产品简介

● 1-1.产品概述

Broadcom 系列交换机具备二、四层千兆管理型功能。硬件支持二层全线速交换。用户可以通过以太网端口以 WEB 形式对交换机的各项功能进行设置。内置 ARP 和 DOS 防御系统，可以有效的防御 ARP、DOS 以及各种变种病毒的攻击，另外还配备了许多非常强大的功能：全面 QoS、Spanning Tree、各种风暴抑制、Bandwidth Control、IGMP Snooping、ACL 访问控制、DHCP Snooping 等。非常适合中小企业、校园网和城域网的汇接应用。

● 1-2.产品外观



● 1-3.产品关键特征

- ARP 防御：MAC 地址与端口绑定功能与 MAC 地址安全过滤功能可以有效的防御 ARP 攻击；DHCP Snooping 可以给动态获取 MAC 地址的用户提供 ARP 保护。
- QoS:支持多种 QOS 策略，基于 802.1p 的优先级设置每个端口提供了 8 个优先级队列；IP-DSCP 可以根据不同的 IP 报头划分服务等级，实现全面的 QOS；AUTO VOIP 功能可将端口设置语音信号最高优先级，大大提高网络 IP 电话的语音质量。
- voice vlan:支持语音 vlan 功能，使语音等多媒体信息有更高的优先级；在 QOS 设置里面也具有语音优先级设置，保障多媒体通信的流畅。
- AUTO DOS:可以对下面七种不同方式的 DOS 攻击进行防御

  （1）Land 攻击：攻击者发送具有相同 IP 源地址、IP 目标地址的伪造 TCP SYN 数据包信息流，受害系统试图向自己发送响应信息，结果是系统受到干扰并会瘫痪或重启。

  （2）Blat 攻击：攻击者发送具有相同源端口号和目的端口号的伪造数据包，受害系统试图向自己发送响应信息，结果是系统瘫痪或重启。

  （3）Smurf 攻击：攻击者使用攻击目标的伪装源地址向一个广播地址执行 ping 操作，然后所有活动主机都会向该目标应答，从而导致网络拥塞甚至中断。

（4）Ping 淹没：利用 Ping 广播风暴,淹没整个目标系统,以至于该系统不能响应合法的通信。

（5）SYN/SYN-ACK 淹没：利用 SYN 或者 SYN/ACK 报文淹没整个目标系统。

（6）防护无效 TCP 攻击 ：防止带有无效的 TCP 数据包造成的数据洪流。

（7）Ping of Death 攻击：发送出一个非常大的 ICMP 请求数据包（一次“Ping”），其用意在于引起目标计算机输入缓存溢出，从而使之瘫痪。

- 风暴抑制：可以对广播、组播、DLF 的流量进行设置。
- ACL 访问控制:用于控制端口进出数据包,保证内网的某些站点不会被没有经过授权的用户访问,同时间接的起到了防御 ARP 攻击的功能。
- IGMP Snooping: 支持 IGMP 版本 2 (RFC 2236): IGMP Snooping 是用来当多播数据包溢出网络时，建立多播组对多播数据包进行转发，避免浪费带宽。
- 支持 802.1x 认证，为用户提供接入认证。
- 支持自动线序交叉功能（AUTO MDIX/MDI）和自适应 RJ45 端口。
- 线速过滤-存储-转发模式，提供真正的非阻塞交换结构。
- 支持端口镜像、端口汇聚、端口限速功能。
- 支持基于端口的 VLAN 和基于 IEEE802.1Q 的 VLAN。

1-4.产品技术规格

产品型号	UKG1600GC	UKG1602GC	UKG1608GC
	UKG1610GC	UKG2400GC	UKG2402GC
支持的协议	IEEE802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、IEEE802.1q、IEEE802.1p、IEEE802.1z、IEEE802.1d、IEEE802.1s、IEEE802.1w、IEEE802.1ax、IEEE802.1ak		
最大帧长度	9216B		
端口数	16 个 SFP 光口	16 个 SFP 光口 2 个 RJ45 电口	16 个 SFP 光口 8 个 RJ45 电口
	16 个 SFP 光口 10 个 RJ45 电口	24 个 SFP 光口	24 个 SFP 光口 2 个 RJ45 电口
网络介质	1000Base-LX：使用长波长激光（1310nm）越过多模式和单模式光纤，多模式光纤的最大距离是 550m，单模式是 10-24km（现在本公司已有支持 70km 单模模块）。		
	1000Base-SX：62.5μm 多模光纤的最大传输距离为 275m，使用 50μm 多模光纤的最大传输距离为 550 米。		
	10Base-T：3 类或 3 类以上 UTP；（支持最大传输距离 200m）		
	100Base-TX：5 类 UTP；（支持最大传输距离 100m）		
	1000Base-T：CAT-5E UTP 或 6 类 UTP（支持最大传输距离 100m）		
VLAN 地址表	4K		
MAC 地址表	8K		
缓存	4Mbits		
背板带宽	52Gbit		
过滤和转发速率	10Mbps：14880pps 100Mbps：148800pps		
	1000Mbps：1488000pps		
外形尺寸	440x280x44mm(1U19 寸标准机壳)		
使用环境	存储温度：-20℃～70℃；存储湿度 5%～90%不凝结		
	工作温度： 0℃～40℃；工作湿度 10%～90%不凝结		
电源	输入：90-264VAC，50-60HZ；输出：5V/12A		
功 耗	功耗：最大 60W		

四、Web 网络管理

本章将教导使用者如何透过网络浏览器接口来管理交换机。智能型交换机提供 24 个固定千兆以太网络端口；使用者可以透过交换机上的任何一个连接口来连接及监管本交换机的状况，包括统计信息、端口流量、端口汇聚、端口镜像、虚拟局域网络、优先级等等。由于本软件为英文版，本章主要介绍该软件的操作。

交换机出厂默认值如表 2-1 所列：

IP 地址	192.168.1.3
子网掩吗	255.255.0.0
默认网关	192.168.1.1
管理帐户	Admin
管理密码	无

表 2-1

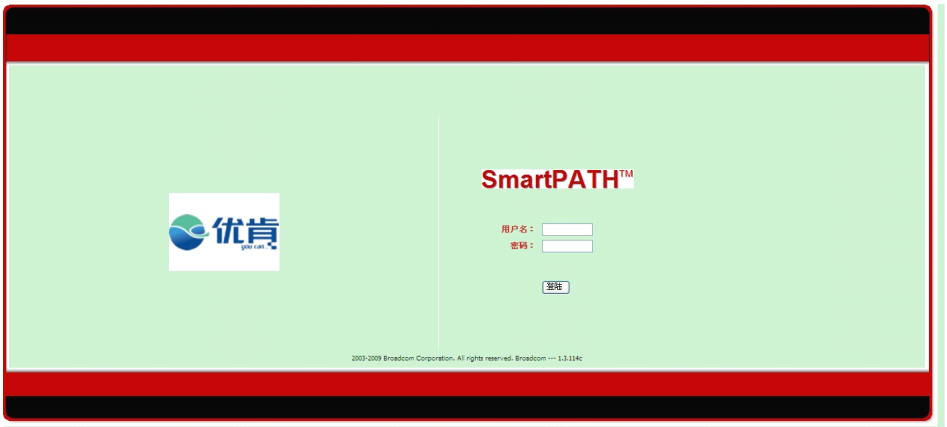


图 2-1

在浏览器的地址栏键入 http://192.168.1.3，进入后将出现图 2-1 的登录界面，分别在“用户名”和“密码”处输入表 2-1 的管理帐户和管理密码，点击“登录”完成登录程序。

图 2-2

管理界面分为 3 个部分(如图 2-2)，上边部分是标签栏，登录后可以通过标签栏切换需要操作的项目；左边部分是导航栏，当选择导航栏的某一项目时，主界面将弹出对应的内容；右边部分是主界面。

为求最佳显示效果，建议使用微软Microsoft 网络浏览器（IE）。

2-1. 系统描述

系统描述页面主要显示系统基本信息例如：软件版本、系统升级时间等。“系统名”“系统定位”“系统联系”主要填写身份信息，交换机出厂时已经配置好，建议不要修改。图 2-3 为系统描述界面。

注：当配置好相应信息或功能后，点击“apply”，然后在标签栏中选择“tools”选项，导航栏中选择“save configuration”，进入保存界面，在主界面中点击“save configuration”保存成功。如果不进行此步骤操作，相应的修改将会在交换机重启后丢失。

图 2-3

2-2. 网络连接

详细设置=>系统=>网络 进入网络连接，可以配置 IP 信息，选择协议类型。“static”为静态 IP 设置，此时需要手动设置 IP 地址、子网掩码、网关地址；如果交换机所在的网络使用“DHCP”协议，请选择“DHCP”。

“最大会话时间”设置交换机 web 界面允许最大不活动时间，超过设置时间交换机将自动退出 WEB 界面（默认为 5 分钟）。

“管理型 VLAN 设置”设置管理型 vlan 时用到的选项，“管理型 VLAN ID”选择管理型 vlan ID，“管理型 VLAN 端口”选择管理型 vlan 的端口号。

配置完成后，点击“apply”，选择“save configuration”保存配置。

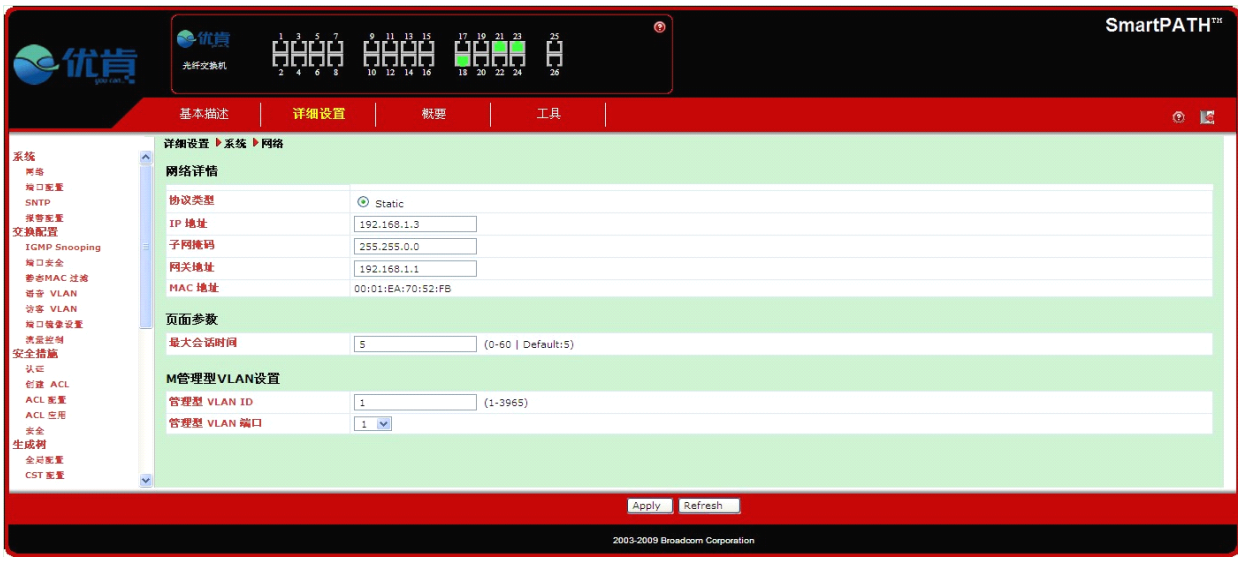


图 2-4

2-3. 端口配置

详细设置=>系统=>端口配置 进入端口配置，可以对交换机的任意一个端口进行配置，“端口号”选择所要配置的端口，“物理介质”、“连接状态”分别为该端口的物理介质和连接状态，“up”显示该端口为已经连接上，“down”显示该端口为断开。

“启动该端口管理功能”选择是否可以通过该端口来管理交换机。

“自动协商功能”选择该端口是否启动自动协商功能，如果不勾选此项，需要根据实际的网络环境手动配置该端口的工作模式和传输速度。

“最大帧长度”设置该端口最大支持的帧长度，其中包括帧头、CRC、有效帧信息，默认设置为 1518（非专业人士建议不要修改此项）。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-5

2-4. SNTP 配置

详细设置=>系统=>SNTP 进入 SNTP 配置，此配置使交换机具有与指定服务器同步时间的功能，勾选“激活 SNTP”启动 SNTP 服务功能。

“SNTP/NTP 服务器 IP 地址”设置 SNTP 服务器的 IP 地址，“服务器端口”设置的 UDP 端口，默认为（123）；

“当前 时间/日期”当地时间和日期；

“与服务器核对次数”交换机启动后与 SNTP 服务器核对时间的次数；

“最后一次连接到服务器状态”最后一次连接到 SNTP 服务器的状态；

“与服务器连接失败次数”交换机启动后连接到 SNTP 服务器失败的次数。

配置完成后，点击“apply”，选择“save configuration”保存配置。

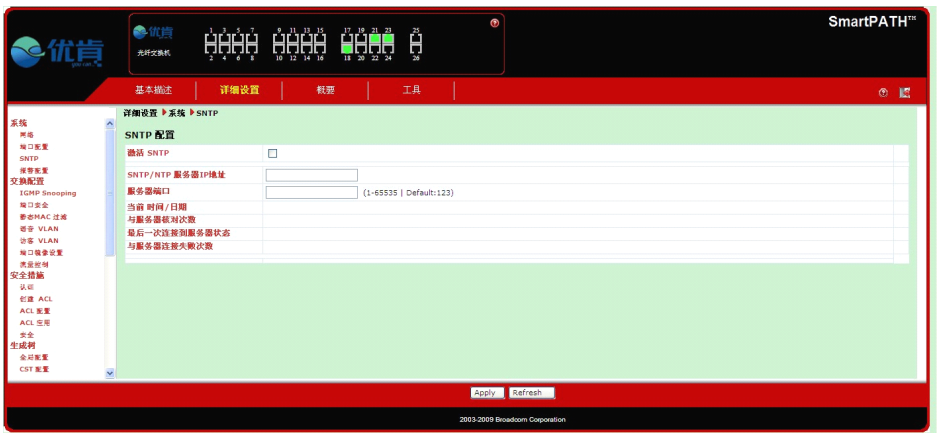


图 2-6

2-5. 警报配置

详细设置=>系统=>警报配置 进入警报配置界面。

勾选“激活系统报错”激活系统报错功能；

“警报级别”可以选择从 emergency-debug（由高到低）八个不同等级的报警；

“将警报发送到指定服务器”启动将报警文本信息发送到指定服务器的功能；

“接受警报信息服务器 IP 地址”设置需要接受报警信息的服务器 IP 地址。

配置完成后，点击“apply”，选择“save configuration”保存配置。

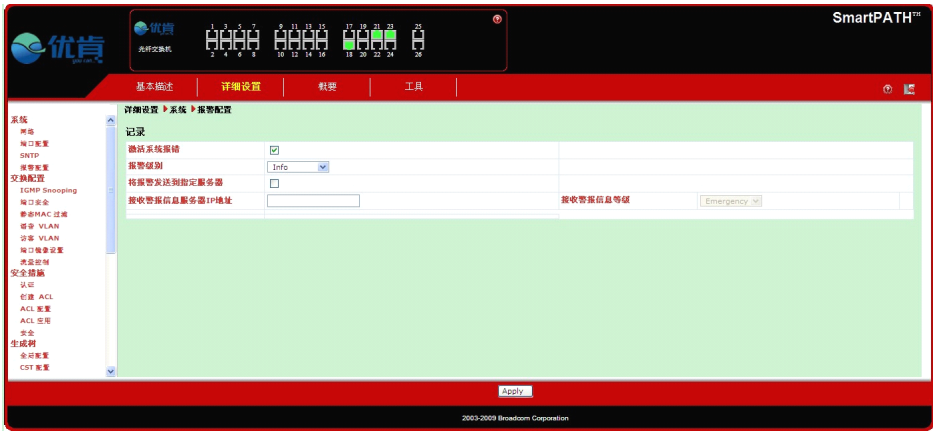


图 2-7

2-6. IGMP snooping 配置

详细设置=>交换配置=>IGMP snooping 进入 IGMP 设置。

勾选“激活 IGMP snooping”启动 IGMP 功能后，该主界面的其它设置才是有效的。

“IGMP snooping 接口”显示交换机的每个端口；

“激活 snooping”启动相应端口的 IGMP 功能；

“组播信息老化时间”设置相应端口组播信息的老化时间；

“最大相应时间”设置最大应答时间；

“立即移除组播信息”激活后交换机可以立即移除组播信息。

“连接多组播路由设备”启动该项后，对应的端口可以连接一个多组播的路由器设备；

“更新接口列表时间”设置更新接口列表所需要的时间。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-8

2-7. 端口安全设置

详细设置=>交换配置=>端口安全 进入端口安全设置，此设置可以将端口、MAC 地址、VLAN ID 三者绑定，大大提高网络的安全，并能有效的防御 ARP 等各种攻击。

“启动”启动 port security 功能；

“端口号”对应交换机的各个端口；

“启动”启动对应端口的 port security 功能；

“操作”中有三个选项“none、add、remove”，选择“add”可以在“mac 地址”和“vlan ID”处添加一个 MAC 地址和 VLAN ID 与该端口绑定；选择“remove”可以在“mac 地址”和“vlan ID”处输入想要删除的 MAC 地址和 VLAN ID；

“最大动态入口”设置最大动态地址进入该端口的数量；

“最大静态入口”设置最大静态地址允许进入该端口的数量。

配置完成后，点击“apply”，选择“save configuration”保存配置。

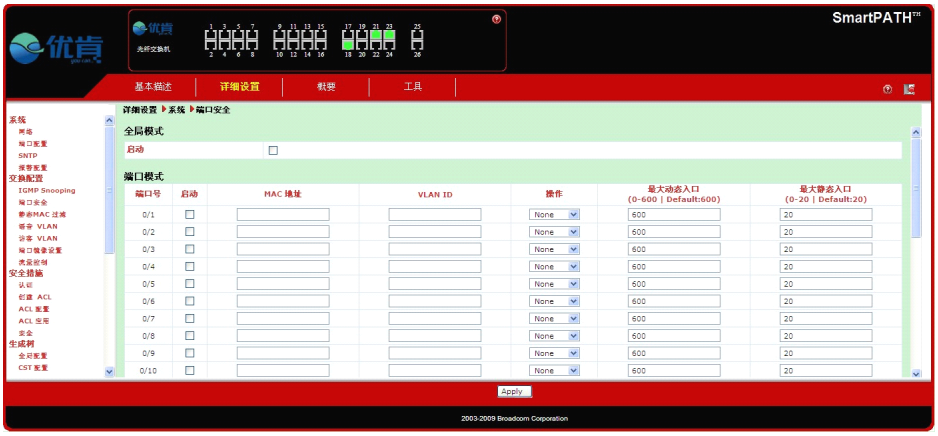


图 2-9

2-8. 静态 MAC 过滤

详细=>交换配置=>静态 MAC 过滤 进入静态 MAC 过滤设置。

“MAC 过滤操作”设置可以进行产生和删除操作，选中“create”在“mac address”和“VLAN ID”处输入相应的 MAC 地址和 VLAN ID 建立一个新规则；选中“delete”后，在“mac address”和“VLAN ID”处输入想要删除的规则。

“生成的 MAC VLAN ID”选择你所生成的“VID MAC”，在“过滤对象”选择“source”（源地址）或者“destination”（目的地址），在“接口”选择相应的端口即可以建立一个新规则。

配置完成后，点击“apply”，选择“save configuration”保存配置。

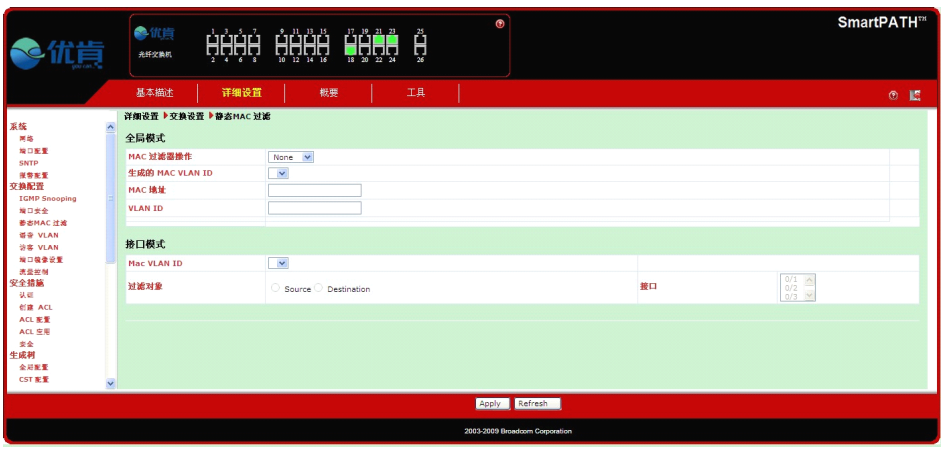


图 2-10

2-9. 语音 VALN

详细设置=>交换配置=>语音 vlan 进入语音 VLAN 设置界面。

勾选“语音 VLAN”启动该功能；

“模式”选择对应端口需要划入的 VLAN 类型，在“模式”中选择“voice vlan ID”可将该端口划入语音 vlan；

“是否启动 cos override”是否启动 COS OVERRIDE 功能。

“可操作状态”该端口语音 VLAN 处在的工作状态。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-11

2-10. 访客 VALN

详细设置=>交换配置=>访客 vlan 进入访客 VLAN 设置界面。该设置允许一个未经授权的访客进入 VLAN，但权限受到限制。

“访客 VLAN 操作”中选择“add”让相应端口添加到访客 vlan 中；“访客 vlan ID”设置 vlan ID；“分配所需时间”设置当端口未被认证后分配到访客 vlan 所需要的时间。

配置完成后，点击“apply”，选择“save configuration”保存配置。

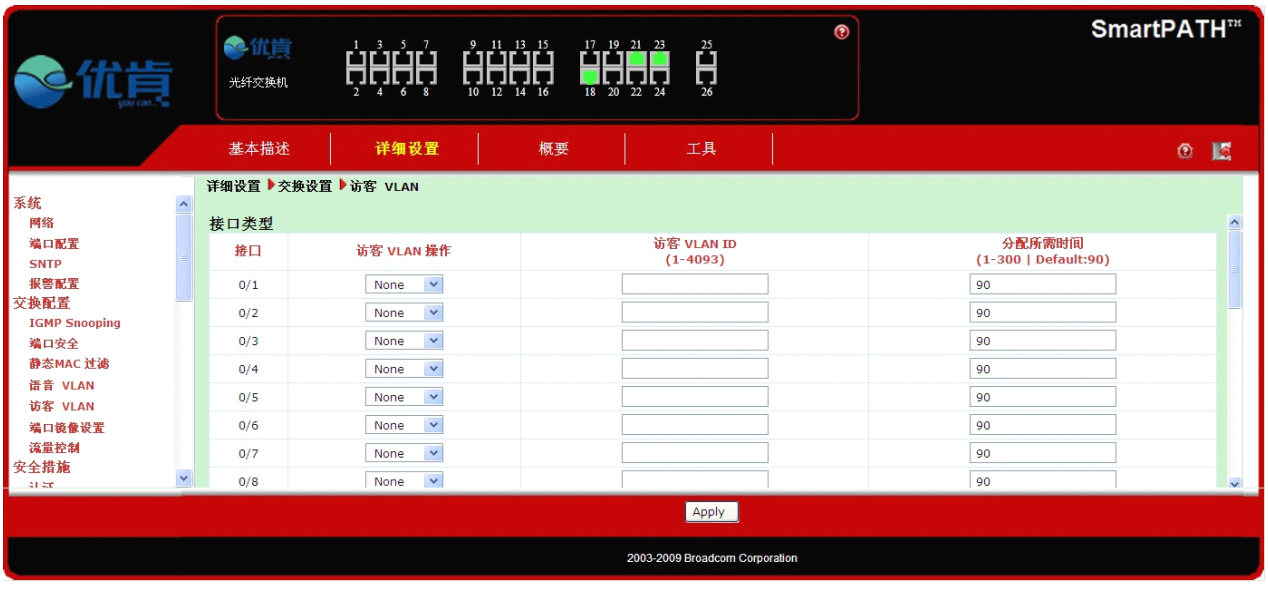


图 2-12

2-11. 端口镜像设置

详细设置=>交换配置=>端口镜像设置 进入基本配置，该设置包括 MAC 地址的老化时间和端口镜像。

“MAC 地址老化期”该项设置 mac 地址老化时间默认为 300 秒；

勾选“激活镜像”启动端口镜像功能；

“目的端口”设置目的端口；

“源端口”和“流向”设置源端口的数据传输方向。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-13

2-12. 流量控制

详细设置=>交换配置=>流量控制 进入流量控制界面。

勾选“激活流量控制”启动流量控制功能。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-14

2-13. 802.1x 设置

详细设置=>安全措施=>认证 进入 802.1X 设置。

勾选“激活端口认证”启动交换机认证功能；

“认证方法”有三个选项，“RADIUS,reject”：通过远程 RADIUS 服务器认证；“reject”：拒绝所有认证请求；“load”：用 802.1x 认证管理员账户。

“控制模式”有三个选项，“auto”：对应端口的工作状态由认证服务器决定；“force authentication”：强制认证，无论该端口是否被认证，它所连接的工作站都处于被认证状态；“force unauthentication”：强制未认证，无论该端口是否被认证，它所连接的工作站都处于未被认证状态。

勾选“启动重新认证”启动对应端口按周期性重新认证。

“静态周期”设置该端口在未被认证后，到下次认证所需要的时间（默认 60 秒）。

“转换周期”设置认证服务器向请求者发送帧的间隔时间（默认 30 秒）。

“重新认证周期”设置周期重新认证之间的时间间隔（默认 3600 秒）。

“最大相应时间”设置请求重新发送的时间间隔；勾选“RADIUS attribute 4（NAS-IP）”启动 NAS 认证服务器；“NAS IP 地址”设置 NAS 服务器的 IP 地址。

“RADIUS 操作”和“RADIUS server IP”对 RADIUS IP 地址进行添加和移除操作；“密钥”设置服务器的密码。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-15

图 2-16

2-14. ACL 设置

ACL 的全称是访问控制列表，它可以建立一种访问控制机制，有效的保护网络的安全，使网络的机密资源得到保护。下面我们有列表 2-2 说明 ACL 设置。

创建 ACL	
ACL 名	建立一个 ACL 名字，可以是字母或数字
类型	选择 ACL 类型，IP ACL 基于 IP 地址的访问顺序，MAC ACL 基于 MAC 地址的访问顺序。
创建的 ACL 数量	当前 ACL 数量
最大 ACL 数量	最大 ACL 规则的数量为 50 个
ACL 配置	
效应	选择当前 ACL 规则处在激活（permit）状态还是屏蔽（deny）状态
级别	设置当前 ACL 规则所处的优先等级
匹配任意包	选择该项使当前 ACL 规则应用与所有数据包
源 IP/IP 掩码/port	设置源 IP 地址/子网掩码/端口（目的 IP 地址/IP 子网掩码/端口）
源 MAC 地址	设置源 MAC 地址（目的 MAC 地址）
删除 ACL	删除当前 ACL 规则
应用 ACL	
接口	选择一个端口
应用 ACL	将选择的端口应用当前 ACL 规则
删除接口	将选择端口的当前 ACL 规则移除

表 2-2

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-17

图 2-18

图 2-19

2-15. 防御 DOS 攻击

详细设置=>安全措施=>安全 进入 DOS 攻击和风暴控制界面。

交换机主要可以对下面七种 DOS 攻击进行防御。用户可以根据自己的需要勾选相应的选项来激活功能。

（1）Land 攻击：攻击者发送具有相同 IP 源地址、IP 目标地址的伪造 TCP SYN 数据包信息流，受害系统试图向自己发送响应信息，结果是系统受到干扰并会瘫痪或重启。

（2）Blat 攻击：攻击者发送具有相同源端口号和目的端口号的伪造数据包，受害系统试图向自己发送响应信息，结果是系统瘫痪或重启。

（3）Smurf 攻击：攻击者使用攻击目标的伪装源地址向一个广播地址执行 ping 操作，然后所有活动主机都会向该目标应答，从而导致网络拥塞甚至中断。

（4）Ping 淹没：利用 Ping 广播风暴，淹没整个目标系统，以至于该系统不能响应合法的通信。

（5）SYN/SYN-ACK 淹没：利用 SYN 或者 SYN/ACK 报文淹没整个目标系统。

（6）防护无效 TCP 攻击 ：防止带有无效的 TCP 数据包造成的数据洪流。

（7）Ping of Death 攻击：发送出一个非常大的 ICMP 请求数据包（一次“Ping”），其用意在于引起目标计算机输入缓存溢出，从而使之瘫痪。

风暴控制可以对广播、组播、DLF 的流量进行抑制。勾选相应选项就会激活功能。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-20

2-16. 生成树设置

本交换机支持快速生成树和多生成树协议，用户在使用时请根据自己的需要选择使用。表 2-3 说明生成树设置的各项功能。

全局设置	
激活生成树	勾选此项激活生成树协议
使用协议	用户根据自己需要选择协议“IEEE802.1D”：生成树协议；“IEEE802.1W” 快速生成树协议；“IEEE802.1S”多生成树协议
区域名	设置此项可使当前生成树的网络地址区域被识别
修订数量	该项用户自定义当前设置版本的修订等级
MST 实例操作	对一个多生成树进行操作，“create”产生一个多生成树；“delete”删除一个多生成树
创建/删除 MST 端口	输入要创建的多生成树的 ID/选择需要删除多生成树的 ID
快速生成树设置	
生成树	勾选激活对应端口的生成树功能
设备端口	勾选此项当交换机连接电脑或者没有生成树功能的网络设备时使用
外不值	设置对应端口的路径消耗
多生成树设置	
选择一个多生成树 ID	选择一个多生成树 ID
桥优先级	设置该多生成树的桥优先级别
端口消耗	设置对应端口的路径消耗
端口优先级	设置端口的优先级别

表 2-3

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-21

图 2-22

图 2-23

2-17. QOS 设置

用户可以通过该项设置灵活的优先级，例如可以通过“Auto VOIP”设置使需要连续传播的帧得到更高的优先级，“IP-DSCP”用户可根据报文自带的 DSCP 值来控制其转发的优先级，DSCP 字段的取值范围是 0-63

表 2-4 说明 QOS 的各项功能。

端口队列设置	
端口	选择要设置的端口
Queue ID	选择对应端口所加入的队列
端口占用对应队列的带宽百分比	设置该端口占用对应队列的带宽百分比。
队列优先级算法类型	设置对应队列优先级算法类型，“strict”严格按照优先等级策略，“weight”按照加权算法决定优先级别。
端口的优先等级设置	
端口	选择要设置的端口
端口信任帧模式	设置端口信任帧的模式，“untrusted”不信任任何包的优先设置，“trust dot1p”信任 802.1p 的优先级设置，“trust IP-DCSP”信任 IP-DCSP 的优先级设置
数字占用带宽比	通过此项可以设置对应端口的流量限制，输入数字占用带宽的百分比(输入 0 说明对该端口带宽无限制)
设置报文 DSCP 的优先级	
队列	设置对应 DSCP 值的优先等级
802.1p 优先级设置	
端口	选择需要设置优先级的端口
802.1p 映射	此项有 8 个优先级，4 个优先队列，用户根据实际情况设置 4 个队列的优先级

表 2-4

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-24

图 2-25

图 2-26

图 2-27

2-18. VLAN 设置

VLAN 设置包括三个步骤：生成一个 VLAN、添加 VLAN 端口、设置 VLAN 类型。表 2-5 详细介绍 VLAN 设置操作。

VLAN 配置	
创建 VLAN	勾选此项将建立一个新 VLAN
创建 VLAN ID	在 1-4093 之间任意选一个数字做为新 VLAN 的 ID 号。（配置玩以上两项后点击“apply”主界面刷新处刚生成的 VLAN 如图 2-8）
VLAN 名/删除 VLAN/设置名字	填写 VLAN 名字（允许字母或数字）/勾选为删除该 VLAN/勾选使设置的 VLAN 名字生效
VLAN 的端口	
端口号	选择需要进行 VLAN 配置的端口
PVID	这个设置将提高 VLAN 的灵活度，下文将介绍 PVID 的用法。
进行过滤	激活此项交换机将会丢弃不带当前 VLAN 标签头的帧，屏蔽此项交换机会转发与 802.1a 相匹配的带标签的帧
可接受的帧类型	“admit all”不带标签或带优先级标签的帧允许通过并且被分配到 PVID 中；“admit tagged only”交换机丢弃不带标签或只带优先级标签的帧
端口优先级	设置当前端口的优先级
标签	
Tag/untag/exclude all	点击端口下面的小方格，出现“T”的字样则该 VLAN 的帧带标签，再点击出现“U”的字样则该 VLAN 的帧都不带标签，再点击出现空白说明该端口不在当前 VLAN

表 2-5

下面将列举一个应用实例来说明 PVID 的作用。

有四台 PC 机（PC1,PC2,PC3,PC4），要求 PC1 与 PC3 能互访，PC2 与 PC4 能互访，但 PC1 与 PC4 不能互访，PC2 与 PC3 不能互访。

第一步：创建 VLAN2，将 PC1 对应端口（假设为端口 6）加入 VLAN2，打开 VLAN 端口配置，将端口 6 的 PVID 选择 2，点击“应用”。

第二步：创建 VLAN3，将 PC2 对应端口（假设为端口 7）加入 VLAN3，打开 VALN 端口配置，将端口 7 的 PVID 选择 3，点击“应用”。

同样将 PC3,PC4 也分别加入到 VLAN2 和 VLAN3 中。

第三步：配置两台交换机相连的两个端口为 TRUNK：分别将这两个端口都加入到 VLAN2、3 中，同时在端口配置界面中将此两端口的报文类型选中“ALL”即可。

配置完成后，点击“apply”，选择“save configuration”保存配置。

图 2-28

图 2-29

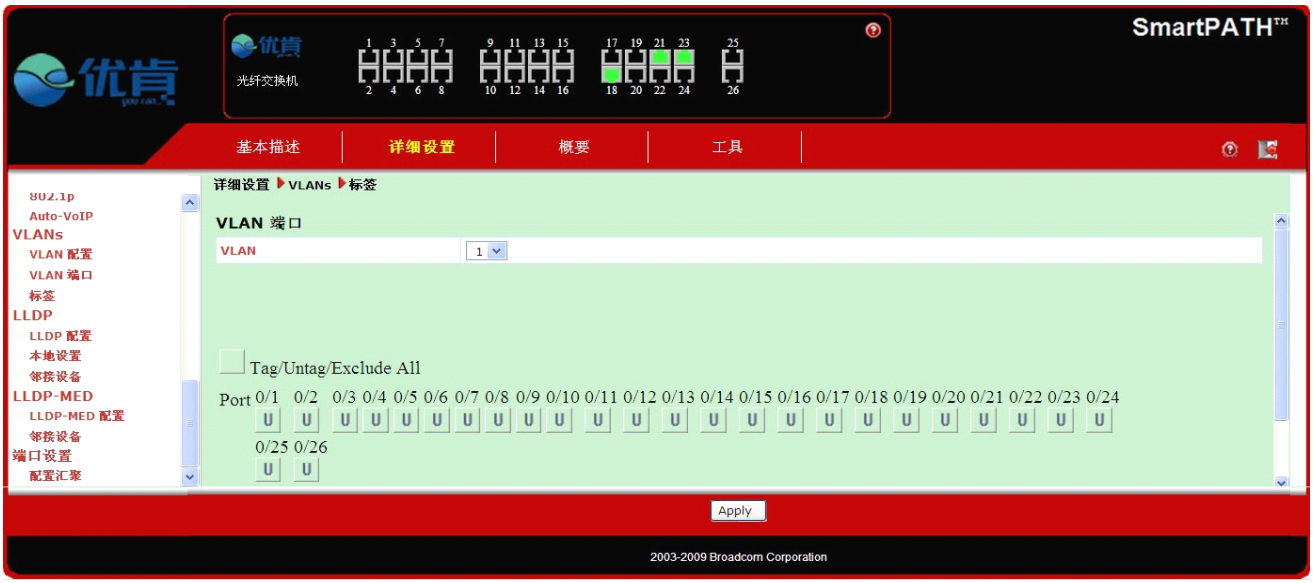


图 2-30

2-19. 端口聚合设置

表 2-31 点击详细设置-端口设置-配置汇聚，进入端口配置汇聚界面。

图 2-31

如图 2-31 配置（注：图 2-32 中 1 和 2 是要配置的端口，中间用空格或“,”分开）

图 2-32

配置完成后，点击“apply”，选择“save configuration”保存配置。

2-20. 备份当前管理软件及设置

工具=>备份管理 进入备份管理界面可以对当前的管理软件和配置信息进行备份。

需要说明的是本交换机支持两种传输模式 HTTP 和 TFTP，“HTTP”通过网络浏览器将信息下载到本地计算机；“TFTP”通过网络将信息保存到 TFTP 服务器上。

“备份方法”选择“HTTP”和“TFTP”中的一种进行备份操作；

“备份类型”中“code”将交换机管理软件全部备份；“configuration”只将管理软件的配置信息备份；“ACL XML”仅仅把 ALC 规则配置备份。

图 2-33

2-21. 升级管理软件及设置

工具=>更新管理 进入升级管理软件设置界面，该界面也包括“HTTP”和“TFTP”两种传输模式，用户选择适用自己的方式进行升级。

图 2-34

2-22. 其它设置

点击“工具”标签栏，“用户管理”修改管理员账号密码；“重启”重启交换机；“出厂默认设置”恢复出厂设置。

图 2-35

附录 1——Broadcom（光交换机）系列产品目录

➢ **UKG1600GC**	网管型 16 个 SFP 口全千兆光纤交换机
➢ **UKG1602GC**	网管型 16 个 SFP 口、2 个 RJ45 口全千兆光纤交换机
➢ **UKG1608GC**	网管型 16 个 SFP 口、8 个 RJ45 口全千兆光纤交换机
➢ **UKG1610GC**	网管型 16 个 SFP 口、10 个 RJ45 口全千兆光纤交换机
➢ **UKG2400GC**	网管型 24 个 SFP 口全千兆光纤交换机
➢ **UKG2402GC**	网管型 24 个 SFP 口、2 个 RJ45 口全千兆光纤交换机

附录 2——常见故障诊断

故障现象	可能的故障原因	解决方法
加电时所有指示灯均不亮	电源连接错误或供电不正常	检查电源线和插座
LINK 指示灯不亮	1. 网线损坏或连接不牢。 2. 网线类型错误或网线过长，超出允许范围。	更换网线
LINK 指示灯闪烁	1. 网线接线不标准。 2. 网线过长，超出允许范围。	更换或重做网线。
网络能通，但传输速度变慢，有丢包现象	交换机与网格终端以太网口工作模式不匹配。	设置以太网口工作模式使其匹配或将其设为自适应工作模式。
在某一口可通，将网线换到其他口时则不通	将网线换到其他网口时，如果此端口所连接的设备没有发送数据，交换机将学不到新地址，因此此端口会暂时不通。	150 秒后交换机的地址会自动更新，此现象会自动消失。或者从此网口发送数据也会使交换机立即更新其地址表。
所有 ACT 指示灯闪烁，网络速率变慢	广播风暴	1. 检查网络连接是否成环路，合理配置网络。 2. 检查是否有站点发送大量的广播包。
正常工作一段时间后停止工作	1. 电源不正常。2. 过热。	1. 检查电源是否有接触不良，电压过低或过高。 2. 检查周围环境，通风孔是否畅通，交换机风扇是否工作正常。