

# 全千兆管理型交换机

## 使用说明书

## 物 品 清 单

小心打开包装盒，检查包装盒里应有的配件：

一台交换机

一根交流电源线

一根串口线

一本用户手册

两个 L 型支架如果发现包装盒内产品有所损坏或者任何配件短缺的情况，请及时和当地经销商联系。

# 第一章 用户手册简介

---

感谢您购买 24 口全千兆管理型系列交换机。本系列交换机提供多方面的管理功能，整体性能优越，使用简单，是您提升工作组性能的理想选择！

## 1.1 用途

本手册的用途是帮助您熟悉和快捷的使用 24 口全千兆管理型系列交换机。

## 1.2 约定

在本手册以下部分，均以 **24 口全千兆管理型**交换机为例。

## 1.3 用户手册概述

第一章：用户手册简介。

第二章：产品概述。描述交换机的构造和基本特性。

第三章：安装指南。指导你进行交换机的基本安装步骤。

第四章：交换机基本概念。

第五章：**WEB** 管理。讲述如何使用 **WEB** 连接进行交换机管理。

第六章：带外管理。讲述如何使用带外管理来管理交换机。

## 第二章 产品介绍

---

### 2.1 产品简介

24 口全千兆管理型系列交换机是一低端安全交换机，提供 web 配置交换机，提供 24 个 10/100/1000MB 自适应端口或 22 个 10/100/1000MB 自适应端口+2 个 1000M 光电复用端口。该系列交换机硬件支持二层的线速交换，内嵌 ARP 防御系统，百分百有效防御 ARP 攻击，若有机器感染病毒，交换机网页会提示。可以指定上联端口，实现其他端口的隔离。将 IP、MAC、端口三者结合而成的 ARP 欺骗防御体系，百分百防御 ARP 病毒报警系统：随时监控网络异常，ARP 攻击报警提示。

### 2.2 主要特性

- 符合符合 IEEE802.3、IEEE802.3u、IEEE 802.3ab 标准；
- 主机背板带宽可达 48G
- 存储--转发体系结构
- 24 个 10/100/1000M 自适应端口或 22 个 10/100/1000MB 自适应端口+2 个 1000M 光电复用端口
- 8K 的 MAC 地址
- 每一个端口都支持地址学习功能
- 支持自动线序交叉功能（Auto-MDIX）
- 支持广播和多播数据包的控制
- 支持 IP+MAC+PORT 绑定，防御 ARP 攻击。
- 支持上联端口配置，其他端口自动隔离
- 支持广播风暴控制，可有效控制各种广播数据包的转发数率，避免广播风暴。
- 支持 ARP 防护端口 ARP 攻击报警提示
- 支持网关 ARP 攻击检测。
- 支持 WEB、带外 RS232 管理
- 支持 DHCP 客户端协议。
- 可通过 HTTP、XMODEM 进行系统软件升级，。
- 内置优质开关电源，稳定可靠
- 1U 全钢外壳，支持标准 19 英寸机架安装

## 2.3 技术指标

产品名称		24 口全千兆管理型交换机	22+2 光电复用 全千兆管理型交换机
符合标准		IEEE 802.3 Ethernet、802.3x、802.1p 和 802.3ab	
端口数	1000M	24	
	串口	1 个 Console 端口(RS232)	
扩展槽		无	2 个 1000M SFP
网络介质		10BASE-T: 3 类或 3 类以上 UTP 或 STP 100BASE-TX: 5 类 UTP 或 STP 1000BASE-T: 5 类 UTP 或 STP	
			1000Base-LX: 单模光纤传输距离 0~40 公里 1000Base-SX: 多模光纤不大于 2 公里
MAC 地址表		8K	
背板带宽		48G	
过滤和转发速率		10Mbps: 14880pps; 100Mbps: 148800pps; 1000Mbps: 1488000pps	
LED 指示	10/100M	Link/Act(连接/工作)	
	其它	Power(电源)	
外形尺寸(L×W×H) 单位(mm)		440×285×44	440×205×44
使用环境		工作温度: 0℃~40℃; 工作湿度 10%~90%不凝结 存储温度: -40℃~70℃; 存储湿度 5%~90%不凝结	
输入电源		输入: 180-260VAC, 50-60Hz;	

2-1 技术指标列表

## 2.4 包装内容

请参见装箱清单

## 第三章 交换机安装指南

### 3.1 安 装

首先，请按照下述步骤妥当地安置好交换机：

- 必须放在至少能承重 5kg 的表面上。
- 供电的电源插座距离交换机须在 1.5 米之内。
- 确保电源线已可靠地连接在交换机后面板上的电源接口和供电的电源插座间。
- 保证交换机有良好的通风散热环境，并且请勿将重物放置在交换机上。

#### ▣ 安装在桌面上的方法

- 1) 将交换机底部朝上放在足够大且稳定的桌面上。
- 2) 逐个揭去 4 个脚垫的胶面保护纸，分别粘贴在机壳底部 4 个角上圆形凹槽中。
- 3) 再将交换机翻转过来，平稳的放在桌面上。

#### ▣ 安装在机架上的方法

交换机尺寸是符合 EIA(Electronic Industries Association)电子工业协会的标准 19 英寸支架。

- 1) 将配件中的两个 L 型支架分别安装在交换机面板的两侧(配件提供螺钉)
- 2) 再将交换机安放在机架内
- 3) 然后将交换机固定好(螺钉用户自备)

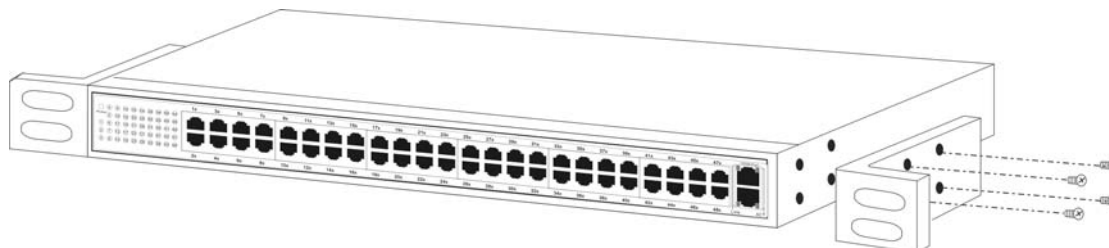


图 3-1 安装 L 型支架示意图

#### ▣ 加 电

交换机的供电输入电压范围是 180-260 伏(50-60Hz)的交流电，交换机的内置电源系统可以根据实际输入的电压自动调整其工作电压。当交换机正常加电后，交换机前面板上的电源(Power)指示灯亮。

注意：

当供电系统出现掉电故障或临时停电时，为了确保交换机不被突发性的电流损坏，请务必将交换机的电源线从供电的插座上拔下来。当供电恢复正常后，再将交换机的电源线插上。

### 3.2 交换机的外观

对交换机的前面板、后面板进行详细说明。

## 前面板

交换机前面板由 24 个 10/100/1000Mbps 端口和相关的 LED 灯组成，如下图所示：



### 24 个 10Base-T/100Base-TX /1000Base-TX RJ-45 端口

LED 指示灯的右侧是 24 个 10/100/1000M 端口，它们支持 10Mbps、100Mbps 或 1000M 带宽的连接设备，均具有自协商能力。通过 WEB 管理对各端口的速率、双工模式、流量控制、广播风暴控制与安全控制等项进行配置。每个端口对应一组 LED 灯，表示 1000M Link/Act、100M Link/Act、Duplex 指示灯。

说明：

22+2 光电复用 全千兆管理型交换机的 23、24 端口还有一光口指示灯，当光口启用时指示灯会常亮。

### 2 个 SFP 扩展槽

2 个 SFP 模块插槽位于串口的左侧，允许插入 1000M 光纤模块。

### 串口

串口(Console 端口或者是 RS232 口)位于后面板的最右侧，它是带外管理时和计算机连接的接口，通过提供的串口线，可对系统信息、网络参数、安全管理等进行配置。

### 指示灯

指示灯位于面板的最左侧

#### 1) 1000M Link/Act 指示灯

当一个普通端口与 1000Mbps 设备连通时，相对应的 LED 指示灯为绿色常亮。当端口有数据传输时指示灯闪烁。

#### 2) 100M Link/Act 指示灯

当一个普通端口与 100Mbps 设备连通时，相对应的 LED 指示灯为绿色常亮；当端口有数据传输时指示灯闪烁。

#### 3) Duplex

当端口工作在 100M 或 1000M 全双工状态时，相对应的 LED 指示灯为绿色常亮。

#### 4) Power 指示灯(电源指示灯)

它的位置在面板的最左边，交换机接上电源后，此指示灯为红色常亮。如果指示灯不亮，检查是否连接好了电源。

## 后面板

交换机后面板有一个电源接口。电源工作范围：180-260V~50Hz-60Hz。



图 3-3 交换机的后面板示意图

#### 1) 电源插座

这是一个二线三相电源插座，把电源线阴性插头接到这个插座上，阳性插头接到交流电源上。

### 3.3 注意事项

- 在放置交换机时请注意稳定性，跌落将造成严重后果。
- 应在正确的电源供电下才能正常工作，请在使用前确认电源供电与交换机所标示的供电要求相符。
- 为减少受电击的危险，在交换机工作时不要打开外壳，即使在不带电的情况下，也不要自行打开。
- 当交换机和工作站、服务器、HUB 或其它的交换机相连时，若所用的网线是 UTP(非屏蔽双绞线)时，其长度不能大于 100 米。
- 对于 10Base-T 的以太网，则所用的网线应是 3 类或 3 类以上的 UTP 线。
- 对于 100Bas-TX 的以太网，则必需使用 5 类或 5 类以上 UTP 线。
- 对于 1000Bas-TX 的以太网，则必需使用超 5 类或 6 类及以上 UTP 线。
- 在交换机工作时网线可以随意插入或拔出端口，而不会中断交换机的工作。
- 在清洁交换机前，应先将交换机电源插头拔出，用湿润的面料擦拭，不可用液体清洗。
- 不要将交换机放在水边或潮湿的地方，并防止水和湿气进入交换机机壳。

在放置交换机时，请避开多尘及电磁干扰强的地区。



## 第四章 交换机的配置与使用

---

### 4.1 系统全局配置

交换机系统全局配置主要是设置交换机的网络参数（IP 地址、子网掩码、网关）、密码、Console 和 Web 控制台的最大闲置时间，ARP 防护保护配置模式等。

#### ❑ 系统信息

包括交换机系统版本的基本信息。

#### ❑ 密码设置

为了保护交换机的设置安全，只有拥有正确密码的用户才能登录到交换机的管理界面对交换机进行管理配置。管理员可以设置交换机的密码，缺省密码为 admin。

#### ❑ 交换机 IP 地址

该交换机可以通过手动设置 IP 地址、子网掩码和缺省网关。若 DHCP 功能打开获得 IP 地址后，手动设置的值就不起作用了。出厂时交换机缺省的 IP 地址为 192.168.1.254，掩码为 255.255.255.0，网关为 192.168.1.1，使用时应根据自己网络的实际情况对这些参数进行重新设置。

#### ❑ DHCP 功能

提供了还提供了通过 DHCP 自动获取交换机 IP 地址的功能。DHCP 功能的缺省状态是关闭，在关闭状态下可以手动配置交换机的 IP 地址、缺省网关与子网掩码。打开交换机的 DHCP 功能，交换机将从网络上的 DHCP 服务器（Server）获取交换机的 IP 地址、缺省网关与子网掩码。

=====

使用 DHCP 功能时应注意：

- 1) 改变 DHCP 状态（打开或关闭）后，新的状态在交换机重新启动后生效；
  - 2) 交换机通过 DHCP 获得的地址信息租用期是无限的，即使 DHCP 服务器配置了有限的租用期，交换机仍将其视为无限期租用；
- =====

#### ❑ 动态地址表

交换机内部总是维护了一张动态 MAC 地址表(Dynamic MAC Address Table)。MAC 地址又称为物理地址，是网络节点的唯一地址，这个地址是 6 个字节，它标识着一个局域网中的一个网络设备。动态 MAC 地址表有两项内容：MAC 地址及其对应的端口号。动态地址表是动态更新的，每一个动态地址的记录都是有寿命限制的，其寿命的长短受最大老化时间控制。如果该记录在寿命限定内没有被重新学习，那么它将会被删除，这个处理叫做老化。这个时间我们就称之为“最大老化时间”。

## 4.2 端口

端口使用的类型和工作模式的配置有着直接的关系，下面对端口的类型及支持的属性做介绍。

### ▣ 端口类型与工作模式

端口的类型不同工作模式也不同，具体的模块与端口说明如下：

#### ✦ 10/100/1000M 自适应 RJ45 端口

端口若工作在电口模式下，这些端口支持 6 种工作模式：

- |                 |                |
|-----------------|----------------|
| 1) 10Mbps-半双工   | 2) 10Mbps-全双工  |
| 3) 100Mbps-半双工  | 4) 100Mbps-全双工 |
| 5) 1000Mbps-全双工 | 6) 端口自协商       |

交换机提供端口提供自动协商能力，使设备可以在一个链路段上交换关于各自功能的信息，自动调整传输方式（全双工或半双工）和传输速度（10Mbps、100Mbps 或 1000Mbps）的功能，将端口最优化处理。

#### A. 1000BASE-TX 口的协商能力：

- |                 |                 |
|-----------------|-----------------|
| 1) 自协商-10M/HD   | 2) 自协商-10M/FD   |
| 3) 自协商-100M/HD  | 4) 自协商-100M/FD  |
| 5) 自协商-1000M/HD | 6) 自协商-1000M/FD |

## 4.3 ARP 攻击防护。

ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。这个目标 MAC 地址是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

每个主机都用一个 ARP 高速缓存存放最近 IP 地址到 MAC 硬件地址之间的映射记录，并通过 arp 请求回应包动态更新映射表。

ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞或者实现“man in the middle”进行 ARP 重定向和嗅探攻击。

本交换机提供 ARP 攻击防护功能。通过设定端口 ip + mac 绑定，过滤 ARP 包，禁止防护端口广播或回应非绑定主机的 ARP 报文。

=====

设置静态地址绑定应注意：

- 1) 每个端口允许设置的绑定 ARP 防护的主机数为 1。
  - 2) 某端口一旦绑定 arp 防护主机后，该端口不能再学习新的动态地址，以非该端口的动态地址或静态地址作为源地址的帧不能进入该端口
  - 3) 某端口设定防护后，从此端口进入的非绑定源主机的 arp 数据包将作为 ARP 病毒处理。
- =====

## 4.4 网关 ARP 病毒监控。

当局域网中存在网关 ARP 病毒时，ARP 广播或回应包将更新局域网内的主机的 ARP 表，

造成网内无法正常连接外部网络。该交换机支持监视网关 ARP 攻击，当受到网关 ARP 攻击时，提示警告信息。

## 4.5 广播风暴的控制

广播风暴是指网络上的广播帧（由于被转发）数量急剧增加而影响正常的网络通讯的反常现象。广播控制允许端口对网络上出现的广播帧达到一定数量时进行控制，以防止广播风暴。该交换机端口支持各种类型的广播包的转发速率，广播包的转发速率率，DLF 包的转发速率。同时还支持包括 ICMP 包的转发速率，学习帧的转发速率，多播包的转发速率，防止一些网络中一些恶意的攻击，也可以关闭这些控制。各种数据保的控制范围为 1Kpbs、2Kpbs、4Kpbs、8Kpbs、16Kpbs、32Kpbs、64Kpbs、128Kpbs、256Kpbs。

## 4.6 交换机文件更新

该交换机提供了文件更新功能，能够方便地实现交换机软件的升级更新。

### 文件传输

Web 界面提供了通过 HTTP 协议实现交换机软件的更新。

在串口上提供了 xmodem 协议实现交换机软件的升级。

=====

进行文件传输时应注意：

通过 xmodem 协议下载交换机软件后系统需要重新启动才能生效。

## 第五章 Web 的管理

### 5.1 概述

本交换机采用 WEB 方式进行管理。用户可以使用 WEB 浏览器登录交换机，友好、直观的管理界面将让您觉得配置交换机是一件轻松的事。

### 5.2 Web Server 连接

#### ■ 准备工作

首先，必须确保管理电脑安装了网页浏览器软件(比如 Microsoft Internet Explorer，简称 IE)，而且浏览器必须支持 Javascript 脚本功能。由于不同的浏览器对网页代码的解释不尽相同，为保证配置操作的准确无误，建议您使用微软的 Internet Explorer 浏览器，如果您使用 Netscape 浏览器，请确保其为最新版本。如果您使用 Internet Explorer 浏览器，请确保其版本在 5.0 以上，建议使用 6.0 版本。为了达到良好的浏览效果，建议您将显示分辨率设为 1024×768 或者更高。

为了使 WEB 方式的管理能正常进行，我们需要对所使用的网页浏览器软件进行配置，下面以 Windows XP 下 IE 5.0 为例说明。

第一步在 IE 菜单中选择“工具”→“Internet 选项”，会弹出 Internet 选项对话框：



图 5-1 Internet 选项设置

第二步：点击“设置”按钮，进入设置对话框，如下图所示：

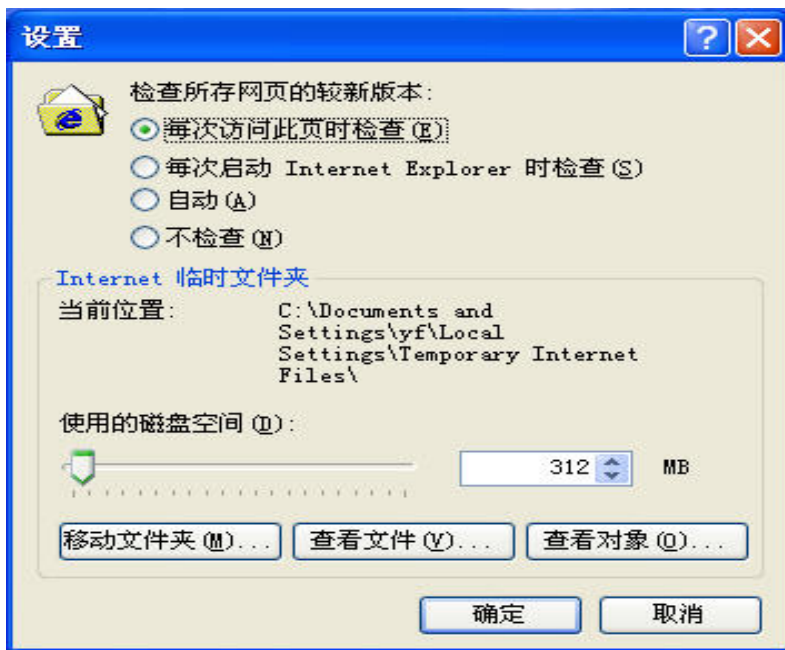


图 5-2 设置对话框

如果您使用 Internet Explorer 5.0 版本的浏览器，请您务必选择“每次访问此页时检查”一项。否则将可能导致某些页面显示的交换机配置信息错误。如果您使用 Internet Explorer 6.0 版本的浏览器，可以选择“每次访问此页时检查”项或“自动”项，建议选择后者。选择完成后点击“确定”按钮即可。

注 意：

选择“每次访问此页时检查”项将使 Internet Explorer 浏览器在每次刷新时都会从交换机读取完整的页面文件，而不是读取磁盘中的临时文件。这将保证配置信息的正确无误，但同时也可能导致页面的显示速度变慢。如果您选择了此项，可以在完成对交换机的 WEB 配置后，将其改为“自动”一项，否则您访问其它网页时显示速度将可能受到较大影响。Internet Explorer 6.0 对此问题处理较好，可以放心使用“自动”项(默认选项)。

第三步：请选择 Internet 选项对话框的“安全”标签，然后点击“自定义级别”按钮，如下图所示：



图 5-3 Internet 选项设置

第四步如果上述操作正确无误，就会弹出以下的对话框：

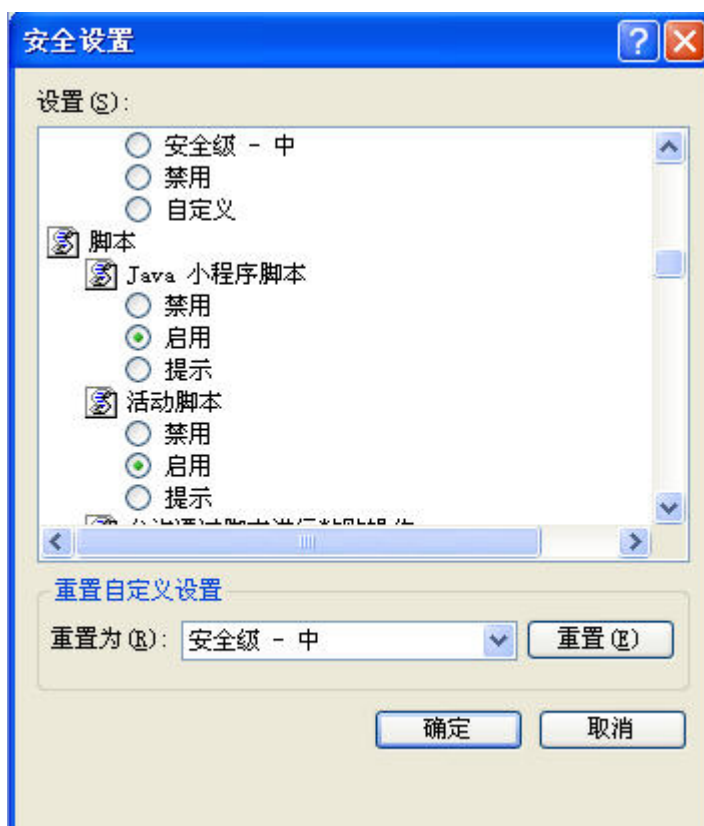


图 5-4 安全设置

请选择活动脚本中的“启用”或者将“重置”下拉文本框设置成“安全级-中”，点击“重置”按钮，最后点击“确定”按钮。

第五步：在桌面上单击鼠标右键，选择弹出菜单中“属性”选项，将弹出显示属性对话框，如下图

所示：



图 5-5 分辨率设置

请选择“设置”标签，将屏幕区域设置为 1024×768，并单击“应用”按钮。如果修改分辨率后感觉屏幕较为闪烁，请单击上图的“高级”按钮，在弹出窗口的“监视器”页面中调高显示刷新率，具体细节此处略过。

经过了以上设置，您就可以畅通无阻地通过 WEB 对交换机进行配置了。

注意：

将屏幕的分辨率设为 1024×768 是对 PC 硬件设备有一定要求的，对于配置较低的 PC 可以不按此设置。

**连接**

首先启动交换机，并确保本机（客户机）与交换机连接上。假设需要配置的交换机的 IP 地址是 192.168.1.1，要连接交换机只要在浏览器的地址栏中正确输入 http: //192.168.1.1，然后敲击回车，就会看见如下对话框：



图 5-6 进入对话框图

在指定的密码输入框中输入密码(交换机的缺省密码是“admin”)，点击“提交”按钮，就进入 WEB 管理交换机主页了。

注 意：

交换机的缺省密码是出厂时设置的。您也可以在交换机的系统密码设置页面中修改密码。如果将交换机恢复为出厂设置，用户自己设置的密码将被删除，只保留密码“admin”。

将让您觉得配置交换机是一件轻松的事。



### 5.3 WEB 管理界面及操作方法

如图 5-7 所示，在页面左侧，是功能菜单界面；页面右侧的大块区域是用于功能配置的主窗口。



图 5-7 24 口千兆远程管理型交换机 WEB 主页左侧的功能菜单

如上图 5-7 所示，左侧的功能菜单呈列表状态，只需要点击相应选项，主窗口就会切换到被点击项的设置页。由于受到网络速度和交换机工作负荷影响，可能菜单会将两次间隔时间较短的点击作一次点击来响应，此时只要注意适当延长点击时间间隔即可。

以下列出了功能菜单项：

- 系统设置：显示和设置系统信息，退出系统，恢复出厂设置。
- 防止 ARP 病毒设置：分静态和动态设置相应端口的 ARP 病毒防护。
- 广播风暴控制：配置系统的数据包的转发率，防止和控制广播风暴。
- VLAN 配置：设置上联端口，隔离其他端口，使其他端口只能和上联端口通信。
- 网关攻击监控：开启网关 ARP 攻击监控，监视网关 ARP 攻击。
- 系统维护：系统升级：



5.3.1 系统配置

系统设置

系统版本	CV1.0.0
是否启动 DHCP	<input type="checkbox"/>
动态 IP 地址	192.168.1.100
动态掩码	255.255.255.0
动态网关	192.168.1.1
DHCP 服务器	0.0.0.0
IP地址	<input type="text" value="192.168.1.100"/>
子网掩码	<input type="text" value="255.255.255.0"/>
默认网关	<input type="text" value="192.168.1.1"/>
密码	<input type="password" value="•••••"/>
Console 最大闲置时间 (秒)	<input type="text" value="0"/> (60-10000)
Web 最大闲置时间 (秒)	<input type="text" value="0"/> (60-10000)

ARP 防护模式

动态绑定模式

保存

刷新

重启

恢复出厂设置

帮助

图 5-8 高级设置

- 系统版本：交换机运行的系统版本。
- 是否开启 DHCP：是否开启 DHCP 客户端自动获得 IP 地址
- IP 地址：每台交换机都应具有其唯一的 IP 地址，用于与主机的网络程序(如 TFTP)进行通信。可以改变交换机 IP 地址，以便与具体的网络相匹配。
- 默认网关：当数据包的目的地地址不属于本子网内工作站地址时，数据包将被转发到缺省网关。
- 密码：登录密码。
- Console 最大闲置时间：设定带外管理的自动刷新时间，单位是秒。如果设置为“0”表示带外管理的不会自动刷新。
- Web 最大闲置时间：设定 Web 管理的自动刷新时间，单位是秒。
- ARP 防护模式设置： 显示 交换机选择 ARP 防护的模式，有两种模式：动态和静态模式。“无”代表未选择防护。
- 保存：保存生效配置修改
- 重启：重启交换机。
- 恢复出厂设置： 将交换机的配置恢复到出厂的默认配置。
- 帮助：显示帮助信息。

5.3.2 防止 ARP 病毒配置。

❏ 防止 ARP 病毒配置向导一  
主要包括以下设置(如下图):

防止ARP病毒设置

防止ARP病毒配置向导第一步

ARP绑定模式选择：

动态绑定模式

---无---

静态绑定模式

动态绑定模式

下一步

帮助

图 5-9 防止 ARP 病毒设置第一步

- ---无---：不设置绑定。
- 静态绑定模式：点击“下一步”，开启静态绑定模式，进入下一页面，见图：5-10。
- 动态绑定模式：点击“下一步”，开启动态绑定模式，进入下一页面，见图 5-11。
- 帮助：显示帮助信息。

❏ 防止 ARP 病毒静态配置：  
配置端口支持的主机。

防止ARP病毒静态配置

IP地址(格式: 192.168.1.111):

MAC地址(格式: 00-E0-4C-63-2B-BD):

00-00-00-00-00-00

绑定

端口选择:

端口 1

序号	IP地址	MAC地址	VLAN ID	是否删除
1	192.168.1.111	00-00-00-00-00-22	1	删除?1

刷新

全部删除

离开

帮助

图 5-10 防止 ARP 病毒设置第一步

- 端口选择：选择要做静态绑定的端口。
  - IP 地址：输入要防护的 IP 地址；
  - MAC 地址：输入要防护的 MAC 地址；
  - 绑定：绑定输入的 ip 和 mac 组。
  - 是否删除：删除所在行的绑定信息。
  - 刷新：刷新本网页。
  - 全部删除：删除本端口的所有绑定信息。
  - 离开：离开此端口。
  - 帮助：显示帮助信息。
- 注：每个端口支持一组 IP 和 MAC 绑定，配置后，此端口支持配置主机的数据转发。

❏ 防止 ARP 病毒动态配置向导第二步：

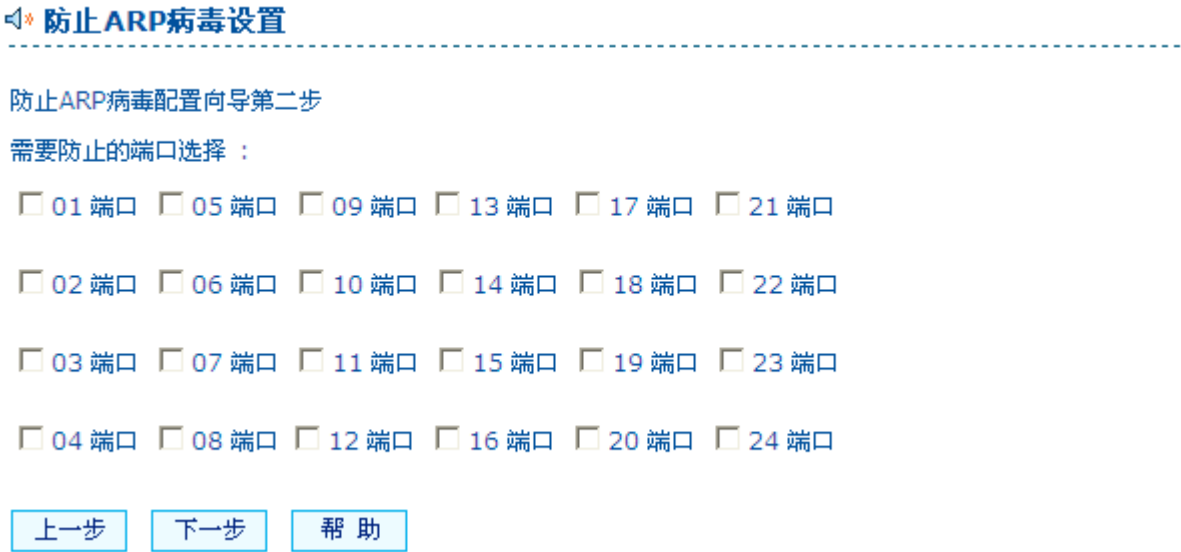


图 5-11 防止 ARP 病毒设置第二步

- 点击选择要防止的端口
  - 上一步： 返回 图 5-9 所示的图的网页。
  - 下一步： 选择端口后，点击下一步进行配置，进入下一个网页，如图 5-12 所示。
- 注：若已经动态绑定有要防护的端口，则不显示此页，直接进入下一个网页（图 5-12 所示）。

❏ 防止 ARP 病毒动态配置向导第三步：



图 5-12 动态绑定向导第三步。

若在选择防护端口连有 PC，着在网页中会显示相应的 ip ， mac ， port 对应信息。

- 上一步： 返回 图 5-11 所示的图的网页。
- 一键绑定： 点击绑定所有状态为“未绑定”信息的对应 pc。
- 一键解绑定： 点击解除所有显示为绑定的信息的主机。
- 更新： 若一个端口显示有多条信息，点击更新此端口。
- 帮助： 显示帮助信息。
- 注： 一个端口支持绑定一组 ip, mac 组，若一个端口连有多个主机，则不能进行动态绑定。  
绑定后，显示有绑定信息的端口只支持绑定主机的数据转发。

5.3.3 广播风暴控制

广播风暴控制

广播风暴控制 每秒钟内最大帧数	
ICMP 包转发率	No Limit
学习帧转发率	No Limit
广播包转发率	No Limit
多播包转发率	No Limit
DLF 包转发率	No Limit

提交

刷新

帮助

图 5-13 广播风暴控制

- 用户可以通过本页面对广播风暴进行控制。设置 ICMP 所转发率、学习帧发率、广播包转发率、多播包转发率、DLF 包转发率每秒钟内最大帧数；可为 1K、2K、4K、8K、16K、32K、64K、128K、256K 等；“No Limit”表示没有限制。

5.3.4 VLAN 配置

配置上联端口，隔离其他非上联端口之间通信。

VLAN配置

MTU Port VLAN配置：

MTU 端口设置  端口（上行端口( 0 ~ 24 )。注意： 0 表示不设上行端口）

确定

帮助

图 5-14mtu vlan 配置

- 设置 MTU 端口（上联端口），可以使交换机的其他端口只支持和上联端口之间通信，端口和端口之间不能互访，增加网络的安全性。
- 确定： 生效上联端口设置。
- 帮助： 显示帮助信息。

5.3.5 网关监控

## 🔊 网关监测

### 网关ARP攻击监测设置

开启检测 ☐

网关IP地址：192.168.1.1

网关MAC地址(格式: 00-E0-4C-63-2B-BD): 00-00-00-00-00-00

确定

帮助

图 5-15 网关 ARP 攻击检视

- 本网页可以开启网关 arp 攻击监视，当处于开启时，当受到网关 arp 攻击时，交换机提示警告信息。
- 网关 MAC 地址：输入现有网关的 mac 地址。
- 确定：生效上联端口设置。
- 帮助：显示帮助信息。

## 5.3.6 系统升级

### 🔊 系统升级

浏览...

升级

图 5-16 软件升级网页内容

升级功能使您可以保持最新版本的系统软件。当您使用升级功能时，您必须到网站下载本交换机的系统软件，保存到您的计算机的某个文件夹下面。

单击“浏览”按钮选择那个文件，然后单击“升级”按钮，文件将被上载到设备上，上载完成后，将重新启动。

## 5.3.7 指示灯显示

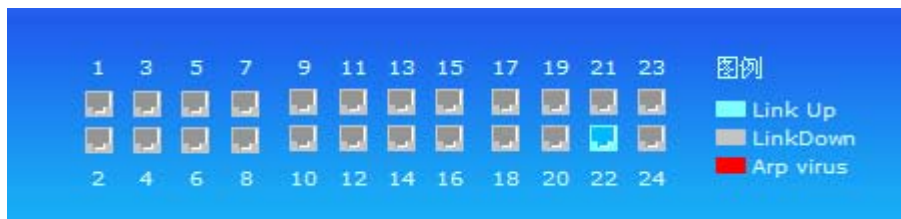


图 5-17 网页头指示灯内容

当显示为红色时，表示端口存在 arp 攻击。点击端口，可得到攻击的 pc 的 ip 和 mac 地址。

## 第六章 带外管理使用说明

### 6.1 概述

**Out-of-Band(带外)**是通过串口在本地对交换机进行管理，它不占用网络带宽。

### 6.2 带外连接方法

带外管理需要一台终端或者是一台终端仿真程序，Windows 上就有一个仿真程序“超级终端” (HyperTerminal)。

首先，使用交换机配套的串口线将交换机的串口(在交换机后面板的最右边)和电脑的串口相连，然后，运行超级终端。如何配置超级终端？请看下图：



图 6-1 超级终端的配置

可以看到，串口的速率是 115200 bps，数据位是 8 位，没有奇偶校验和数据流控制，停止位为 1。如果系统没有超级终端，可以使用系统安装盘重新将超级终端软件安装上去或者在网上下载一个超级终端软件(比如 HyperTerminal Private Edition)。其配置方式基本和 Windows 自带的差不多，注意：“每秒中的位数”为 115200 “数据位”为 8 位、无“奇偶校验”、“停止位”为 1、无“数据流控制”。

注意：

如果超级终端界面出现乱码或者没有反应，请检查串口属性设置，并请检查串口连接是否正确或者交换机的电源是否打开。

## 6.3 带外管理的界面及操作方法



图 6-2 超级终端显示登陆界面

使用正确的密码成功地登录系统以后（密码是：admin），就进入带外管理的界面。

管理界面为命令行驱动。登录以后，首先进入管理界面的根目录，输入“?”可以显示所有命令集如下图：

```
Commands at top level:
System      - System commands
IP          - IP commands
Debug      - Debug commands
>
```

图 6-3 顶层菜单

## 6.4 CLI 命令使用说明

### 6.4.1 语法帮助

命令行接口中内置有语法帮助。如果对某个命令的语法不太确定，请输入该命令中已知道的前面的部分，然后键入“?”或“空格加?”。命令行会提示已经输入的部分命令剩余部分的可能的命令清单。这样就可以根据提示的命令继续输入命令，根据提示命令输入完毕，按回车就可以执行所键入的命令。

命令行接口支持12个模式，包括System、IP、Debug。用户可以在具体的模式下的子命令。比如在根目录下输入system,则进入system模式，可以执行system模式下的命令。可以使用/port在system模式下进入port模式。

### 6.4.2 各配置命令的解释

#### 6.4.2.1 System 系统设置命令

在输入“System”之后键入“?”，显示下面的内容：

```

System>?
Commands at System level:
System Configuration [all]
System Restore Default [keepIP]
System Name [<name>]
System Reboot
System Xmodem
System Webtimeout[<timeout>]
-----
Up
System>_

```

命令格式: configuration [all]

参数说明: [all]为交换机所处的全部状态信息。

功能说明: 显示交换机系统信息。

命令格式: System Restore Default [keepIP]

参数说明: [keepip]在恢复交换机出厂默认值时保持交换机的IP不改变。

功能说明: 恢复交换机的出厂设置。

命令格式: System Reboot

功能说明: 重启交换机。

命令格式: System Name

功能说明: 对交换机的名称进行改变。

命令格式: System xmodem

功能说明: 利用xmodem协议实现机系统软件的升级

输入xmodem命令行后,在串口上点右键,选择发送文件,出现发送文件窗口,在该窗口中选择xmodem协议,然后选择要传输的系统文件即可。如下图所示:

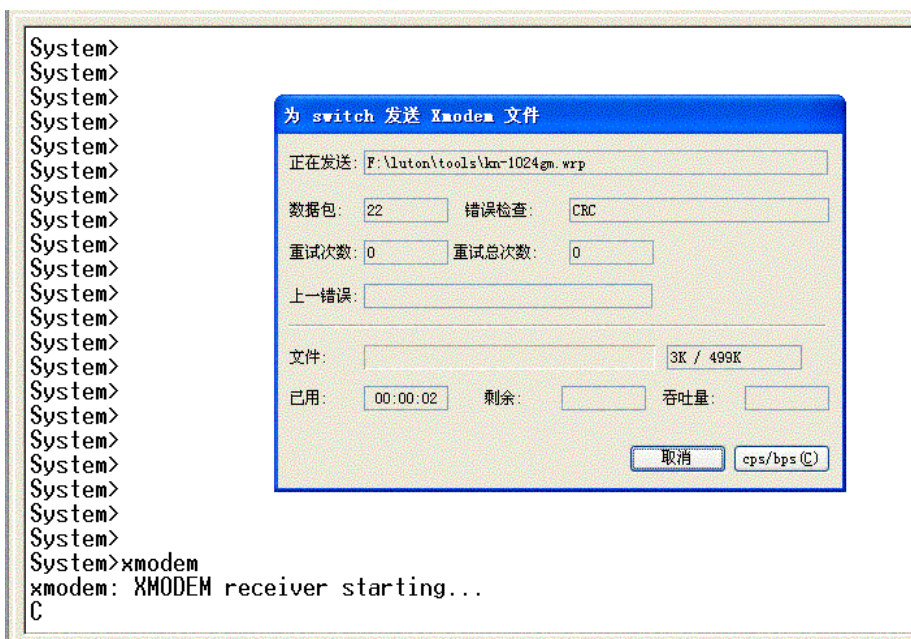


图 6-4 xmodem 传输界面



命令格式: webtimeout [<timeout>]

参数说明: [<timeout>]为交换机网页闲置时间。以秒为单位其取值为: 60-10000。

功能说明: 显示或更改交换机WEB页面的闲置时间。

#### 6.4.2.2 交换机 IP 地址设置命令

Commands at IP level:

IP Configuration

IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]

IP Ping [-n <count>] [-w <timeout>] <ipaddress>

IP Arp

IP Dhcp [enable|disable]

-----

Up  
IP>

命令格式: IP Configuration

功能说明: 显示交换机的IP地址。

命令格式: IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]

参数说明: <ipaddress>十进制方式表示的IP地址, <ipmask>所设IP地址的子网掩码, <ipgateway>交换机的网关, <vid>VLAN的ID号。

功能说明: 设置交换机的IP地址、掩码、网关、管理VLANID。

命令格式: IP Ping [-n <count>] [-w <timeout>] <ipaddress>

参数说明: -n <count>连接计算机ping的次数。-w <timeout>连接计算机ping的时间; <ipaddress>所设交换机的IP地址。

功能说明: 通过ping命令检测交换机与计算机是否连接。

命令格式: IP Arp

功能说明: 显示交换机的ARP表。

命令格式: IP Dhcp [enable|disable]

参数说明: enable为开启状态disable为关闭状态

功能说明: 开启/关闭DHCP客户端功能, 开启后, 交换机从dhcp服务器取得IP地址。