KN-S10-5024GM
全千兆安全管理型
以太网交换机
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
光盘
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 **KN-S10-5024GM** 全千兆安全管理型交换机交换机。本交换机是一款高性能、多用途、高安全性的二四层网管型交换机，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 **KN-S10-5024GM** 全千兆安全管理型以太网交换机。在您准备使用本产品之前，请仔细阅读本手册，以方便、快捷的使用本产品的所有功能。

1．2　约定

在本手册以下部分，均以 **KN-S10-5024GM** 交换机为例，并且所提到的交换机系指 **KN-S10-5024GM** 全千兆安全管理型以太网交换机。

在阅读本手册时，敬请注意下列事项：

 **温馨提示：**在使用交换机需要注意的一些事项

 **重要提示：**在使用交换机需要特别注意的事项

 **友情提示：**在使用交换机过程中必要的解释信息

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（指导您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连接进行交换机管理）
附录 A：　RJ-45 插座/连接器引脚详细说明。
附录 B　　售后技术支持联系方式

第二章　产　品　概　述

2．1　产品简介

KN-S10-5024GM 全千兆安全管理型以太网交换机完全符合 IEEE802.3ab Giga Ethernet 标准，智能配置管理，可为建立小型、中型、大型网络提供理想的组网解决方案。

KN-S10-5024GM 全千兆安全管理型以太网交换机提供多方面的管理功能，可对系统、端口、网络、VLAN、Trunk、优先级、安全等进行管理。包括支持不同病毒防御和二层到四层的安全过滤。

您可以通过 WEB 浏览器对 **KN-S10-5024GM** 全千兆安全管理型以太网交换机进行管理。并且可以通过 RS232 串口查看系统配置信息、修改 IP 网络参数、修改登录密码等。

2．2　产品特性

2．2．1　　主要特性

- 符合 IEEE 802.3、IEEE 802.3u、IEEE 802.3ab 标准
- 全双工采用 IEEE 802.3x 标准，半双工采用 Backpressure 标准
- 24 个 10/100M/1000M 自适应 RJ-45 端口
- 支持端口自动翻转（Auto MDI/MDIX）
- 提供一个终端（DTE）设备配置串口
- 支持 24 个 Port VLAN，512 个 IEEE 802.1Q Tag VLAN
- 支持 MTU VLAN
- 支持静态 MAC 地址表
- 提供端口安全控制功能，支持静态安全地址表的管理，最多可设置 480 组 MAC 地址
- 支持端口汇聚（Port Trunk）功能，最多可设置 8 个 Trunk 组，每组最多 8 个端口
- 支持端口镜像（Port Mirror）功能，能现实数据流的 Rx、Tx 和 ALL 监控
- 支持端口优先级、TOS 优先级、IEEE 802.1p 优先级协议模式，支持 8 个优先级队列
- 支持广播风暴控制，可减少广播风暴和分割广播风暴
- 支持基于端口的带宽限制
- 支持 ARP 攻击报警提示
- 支持应用程序优先级设计模板，管理员可以决定哪些应用程序需要获得高的转发优先级
- 支持病毒防御模板，管理员可以定义病毒的类型并阻止病毒传播
- 全中文 Web 管理界面，支持本地升级（支持 TFTP 远程升级）
- 支持通过 TFTP 的配置文件导入和导出
- 支持静态 IP 地址设置和动态从 DHCP 服务器获取交换机 IP 地址
- 动态 LED 指示灯，提供简单的工作状态提示及故障排除
- 支持带外管理
- 内置优质电源，稳定可靠
- 1U 全钢外壳，优良散热
- 支持标准 19 英寸机架安装

2．2．2　规格说明

产品型号		全千兆安全管理型以太网交换机
符合标准		IEEE 802.3、802.3u、802.3x、802.1Q、802.1p、和 802.3ab
端口数		支持 24 个 1000Base-T
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：超 5 类或六类 UTP 或 STP
MAC 地址表		8K
缓存		6M bit
背板带宽		48G
过滤和转发速率		10Mbps：14880pps；100Mbps：148810pps； 1000Mbps：1488095pps
LED 指示	Link/Act	连接常亮，有数据转发闪烁
	1000Mbps	工作在千兆
外形尺寸（L×W×H）单位（mm）		440×285×44
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

第三章　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。

3．1．1　　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。

3．1．2　　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）

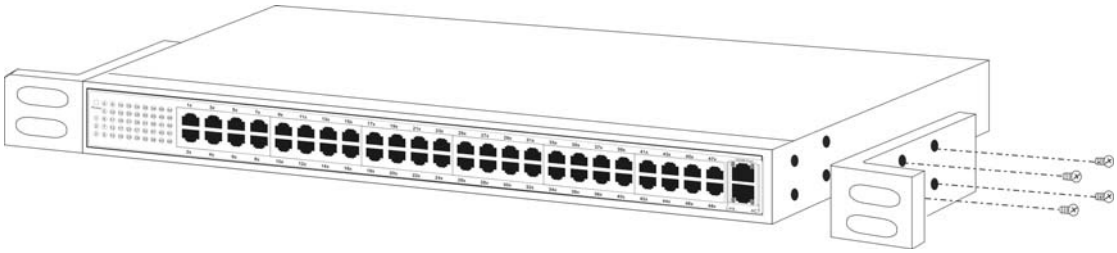


图 3-1　　安装 L 型支架示意图

3．1．3　　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大电流损坏，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。

3．2．1　　前面板

KN-S10-5024GM 交换机前面板由 24 个 10／100/1000Mbps 端口，一个 Console 端口（RS232 串口）和相关的 LED 灯组成，如下图所示：

图 3-2　KN-S10-5024GM 交换机的前面板示意图

- 串口

  串口（Console 端口或者是 RS232 口）位于前面板的最右侧，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。

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

  它们支持 10Mbps、100Mbps、1000Mbps 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。每个端口对应两个 LED 灯，表示 Link/Act、1000M 指示灯。

- 指示灯

指示灯位于面板的最左侧

- 系统指示灯

1. Power 指示灯（电源指示灯）阿

   它的位置在面板的最左边，交换机接上电源后，此指示灯为绿色常亮。如果指示灯不亮，检查电源是否连接好。

- 端口指示灯

1. Link/Act（连接指示灯）

   当一个端口与设备连通时，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为闪烁。

2. 1000M 指示灯（速率指示灯）

   当一个端口与 1000Mbps 设备连通时，相对应的 LED 指示灯为绿色常亮。

3．2．2　后面板

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

图 3-3　KN-S10-5024GM 交换机后面板示意图

- 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　交换机基本概念

本章主要介绍配置和管理交换机时将涉及到的一些基本概念。

4．1　系统配置

交换机系统配置主要是设置交换机的系统信息、交换机参数、更新交换机的系统和配置文件、对交换机重启以及对交换机恢复出厂设置等。

4．1．1　系统信息

包括软硬件版本、系统名称和位置、IP 地址、网页最大闲置时间、串口速率、CPU VLAN ID 等系统的基本信息。

4．1．2　系统密码设置

更改
密码和管理密码

4．1．3　IP 地址参数

如果想要把交换机放在网络里，为了定位交换机，它也应该有属于自己的 IP 地址。**KN-S10-5024GM** 交换机可以通过手动设置 IP 地址、子网掩码和缺省网关，也可以启用 DHCP 功能自动从网络上获取 IP 地址、子网掩码和缺省网关。出厂时我们对交换机的 IP 地址参数进行了设置（出厂默认 IP 地址为 192.168.1.254/255.255.255.0），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。

动态主机配置协议（Dynamic HOST Configuration Protocol，DHCP）是在 TCP／IP 网络上使客户机获得配置信息的协议。配置信息主要是客户机的 IP 地址、子网掩码、默认网关等。DHCP 向网络主机提供配置参数，它由两个基本部分组成：一部分是向网络主机传送专用的配置信息，另一部分是给主机分配网络地址。DHCP 是基于客户机／服务器模式的，这种模式下，专门指定的主机分配网络地址，传送网络配置参数给需要的网络主机，被指定的主机称为 DHCP 服务器。

如果网络中只有一台 DHCP 服务器，并且要从这个 DHCP 服务器上自动获取交换机的 IP 参数配置，此时只需要简单的将 DHCP 功能打开，交换机将从网络上的 DHCP 服务器上自动获取交换机的 IP 地址、缺省网关与子网掩码。如果网络中有多台 DHCP 服务器，交换机的 DHCP 功能打开时，它将从其中一台 DHCP 服务器获得 IP 参数配置，可以在给交换机分配 IP 参数的 DHCP 服务器上了解到交换机的配置信息。

注　意：

当网络中没有 DHCP 服务器而启动了交换机 DHCP 功能时，则需要在交换机启动 5 分钟后通过带外管理为交换机设置 IP 地址、子网掩码及缺省网关。

4．1．4　文件传输

KN-S10-5024GM 交换机提供交换机配置信息、在线更新和备份功能，以及系统文件在线更新升级功能。

该功能是通过标准的 TFTP 协议完成。所谓 TFTP（Trivial File Transfer Protocol）就是简单文件传输协议，它是为了解决网络中两台工作站之间的文件传输而设计的，它是基于 UDP 协议的，相对简单。

在配置时，网络中需要一个 TFTP 文件服务器，在交换机端需要填写这个 TFTP 文件服务器的 IP 地址，如果是更新系统文件或者配置文件，那么一定要给出正确的文件名，如果是备份配置文件，必须指定配置文件保存在这台文件服务器上的文件名。

4．1．5　保存与复位

这一部分的内容主要是重新启动交换机、将交换机设置为出厂设置、退出交换机 WEB 管理系统。

4．2　端口管理

KN-S10-5024GM 交换机有 24 个 10Base-T、100Base-TX、1000Base-T RJ-45 端口。交换机通过端口管理，可以设置端口参数、对端口进行监控和描述、获得端口统计信息和端口状态、对端口的带宽和广播风暴进行控制。

4．2．1　　端口参数

主要包括是否使能端口，是否使用流量控制，设置工作模式，设置端口的缺省 VID，对没有 Tag 标记帧的处理方式，后两项仅在基于 IEEE802.1Q Tag VLAN 模式下可设。

4．2．1．1 端口的工作模式

KN-S10-5024GM 交换机千兆端口有六种工作模式：

- Auto：自协商模式
- 10Mbps／HD：10M 半双工
- 10Mbps／FD：10M 全双工
- 100Mbps／HD：100M 半双工
- 100Mbps／FD：100M 全双工
- 1000Mbps／FD：1000M 全双工

前边的数字表示的是传输速率（Speed），后边表示的是双工模式（Duplex）。所谓半双工（Half Duplex）就是传输的两边既可以发送，也可以接收，但是在某一时刻只能有一个设备使用网络传输介质；所谓全双工（Full Duplex）是传输的两边可以同时的发送和接收，互不影响。

4．2．1．2 端口的 N—Way 自动协商功能

交换机提供 N-Way 自动协商功能。该功能使交换机的端口可根据另一端设备的连接速度和双工模式，自动调节速度和双工模式到双方都可以达到的最高水平。自协商的设备可以交换关于各自功能的信息，这样就可以使设备进行自动配置，实现自动调整传输方式（全双工或半双工）和传输速度（10Mbps，100Mbps，1000Mbps）的功能。

4．2．1．3　端口的自动学习功能

交换机的各端口具有自动学习地址的功能，端口将接收到帧的源地址（MAC 地址）存储到地址表中，**KN-S10-5024GM 交换机**是将 MAC+VID 存储到地址表中。端口的地址学习空间（动态地址表）是有限的，为节省宝贵的动态地址表空间，对于一定时间内没有使用的地址应删除即所谓地址老化，使动态地址表不断的得以更新。这“一定时间”即称之为最大老化时间。最大老化时间是可设定的。“没有使用”是指一个地址记录加入地址表以后，在最大老化时间内端口未收到源地址为该 MAC 地址的帧。

4．2．1．4　流量控制

流量控制（Flow Control）是为了同步接收方和发送方的速度而进行的控制。当接收方接收能力比发送方的发送能力小的时候，如果没有流量控制就会丢失数据。流量控制主要分两种情况，一种在半双工下，一种在全双工下。半双工流量控制是采用 Backpressure 标准，全双工流控使用的是基于 PAUSE 帧的流量控制，即 IEEE802.3x 标准。

半双工方式下，当接收方设备的资源不足时就会启动流量控制，发送一组载波信号脉冲串（假冲突信号），发送方设备检测到网络上的载波信号和自己发送的信号不同，就会停止一段时间（随机）后再发送数据，接收方就可以在这个时间处理数据，从而达到流量控制。采用假冲突信号进行流量控制，就是半双工情况下的 Backpressure 标准。

全双工方式下，当接收方设备的资源不足时就会启动流量控制，由于发送方发送时接收方可以发送数据给发送方（全双工的特征），接收方通过发送一个 PAUSE 帧告诉发送方停止一段时间再发送数据。这就是全双工下的流量控制 IEEE802.3x 标准。

4．2．1．5 端口安全

某个端口的端口安全（Port Security）启动时，该端口将不学习新的 MAC 地址，并且只转发符合条件的源地址发出的帧，其他的帧将被丢弃。判断条件为：该端口收到的帧的源地址为该端口的静态 MAC 地址表成员。

当某个端口的端口安全关闭时，该端口将开始自动学习新的 MAC 地址。

注意：

当某个端口的端口安全（Port Security）启动时，不可以使用这个端口构成 Trunk。

4．2．2　端口监控

端口监控主要是使用一个监控端口对一个或多个被监控端口进行输入监控（Ingress），输出监控（Egress）和输入输出监控（Ingress＆Egress）。

4．2．3　端口描述

端口描述是使用一个字符串描述一个端口，以便网络管理员分清楚各个端口的用途。字符串最多使用 15 个纯汉字或者是 30 个英文字符或数字。

4．2．4　端口统计与端口状态

端口统计将针对每一个端口，统计它收发多少数据字节、多少数据帧、多少个广播帧、

多少个多播帧、多少个错误帧等等；端口状态标识端口上是否接有设备，如果接有设备，那么它的工作速率是多少，它是工作在全双工模式还是半双工模式，它是否启用了流控等等。

注　意：

以太网中的数据帧总长必须在 64 到 1518 字节之间，超出这个范围的帧：都是错误的帧。

4．2．5　　端口带宽

每一个端口的入口带宽可以进行设置，设置的值有以下几种选项：流入带宽限制支持从 100K 到 1000M 之间任意配置

注意：在 KN-S10-5024GM 中，若在 802.1Q　VLAN 和 PORT VLAN 的模式下，交换机计算带宽是假设所有的数据流均带上 4 个字节的 VLAN　TAG。也就是如果流入交换机的数据流如果不带上 VLAN TAG 的话，交换机会自动加上 4 个字节的 VLAN TAG 来进行带宽计算。

在 KN-S10-5024GM 中，则只有 802.1Q VLAN 的模式下会假设所有数据流均带上 4 个字节的 VLAN TAG 这种方式来进行带宽计算。

4．2．6　　端口广播风暴

交换机端口收到的广播分为三类：普通广播、组播、未学习到地址的广播。每一端口可以对各种广播风暴分别选择是否进行控制、广播包转发速率等。

交换机判定端口风暴已经产生后，可以对广播包转发速率进行控制，转发速率限制为 100K-1000M 之间可以任意设定，超过该带宽的广播包将被丢弃。

友情提示：

该端口广播风暴只限制入口带宽

4．3　网络配置

网络配置允许对交换机的最大老化时间、静态地址表、Ping　检测见大网络故障排除工具进行配置。

4．3．1　　最大老化时间

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。

可以设置交换机的最大老化时间，设置的范围是 0 到 630 秒，设置为 0 表示不老化，缺省状态下它的值是 300 秒。

4．3．2　　静态地址表

静态地址表记录了端口的静态地址。静态地址表中一个 MAC 地址对应一个端口，如果设置，则所有发给这个地址的数据只会转发给该端口。

静态地址是不会老化的 MAC 地址，它区别于一般的由端口学习得到的动态地址。静态地址一旦被加入，这个地址表项在被删除之前将一直有效，而不受最大老化时间的限制。

假设在静态地址表中设置了端口 1 对应的 MAC 地址为 00EA0578652E，那么，传给这

个 MAC 地址的所有数据帧（目的地址是 00EA0578652E 的数据帧）只传递给这个端口。这对于某些相对固定的连接来说，由于减少了地址学习步骤，可以提高交换机的效率。同时也限制这个地址只能通过端口 1 连接到交换机上，达到易于管理的目的。

静态 MAC 地址表的大小为 480，也就是说最多可以设置 480 个静态地址表记录。

友情提示：所有端口的静态 MAC 地址表为 480 个，每个端口的不固定。

4．3．3　Ping 检测

网络中通常使用 Ping 来探测网络节点之间是否正常连接，使用交换机时经常需要知道交换机是否和网络中某个节点正常连接。Ping 检测就实现这种网络探测。

4．4　虚拟局域网管理

虚拟局域网（Virtual Local Area Network，VLAN）可以把数据交换限制在各个虚拟网的范围内，从而减少整个网络范围内广播包的传输，提高网络的传输效率；同时各虚拟网之间不能直接进行通讯，而必须通过路由器转发，起到了隔离端口的作用，为高级安全控制提供了可能，增强了网络的安全性。VLAN 功能的适用性很广，在数据交换比较频繁或对网络安全性有要求的环境均可适用，如：1、在智能小区、校园、企业等应用环境，使用 VLAN 功能可使不同 VLAN 间的工作站不能互相访问，可为网络安全控制提供良好保障；2、在大型网吧、大中型企业等环境中，使用 VLAN 可大大减少网络中不必要的数据交换的数量，杜绝广播风暴，提升网络传输性能。并且，通过网络分段的方法，各个网段可共用一套网络设备，这样不仅减少了网络硬件的开销，还有利于设备迁移，降低连网成本。

4．4．1　VLAN 模式配置

KN-S10-5024GM 交换机可以选择基于端口的 VLAN 模式、IEEE802.1Q Tag VLAN 模式和禁止 VLAN 模式。

4．4．1．1　基于端口的 VLAN

在基于端口的 VLAN（Port-Based VLAN）模式下，处于同一 VLAN 的端口之间才能相互通信，可有效的屏蔽广播风暴，隔离不必要的访问，并提高网络安全。

4．4．1．2　IEEE802.1Q Tag VLAN

在 VLAN 最初被应用时，各厂商的交换机由于缺乏统一标准而互不识别，不能兼容。IEEE802.1Q 新的虚拟局域网标准被制订出来后，使不同厂商的设备可同时在同一网络中使用。符合 IEEE802.1Q 标准的交换机之间就可以相互交换 VLAN 信息，并且能够通信。

IEEE802.1Q 标准定义了一种新的帧格式，它在标准的以太网帧的源地址后面加入了一个 Tag Header，如图所示：

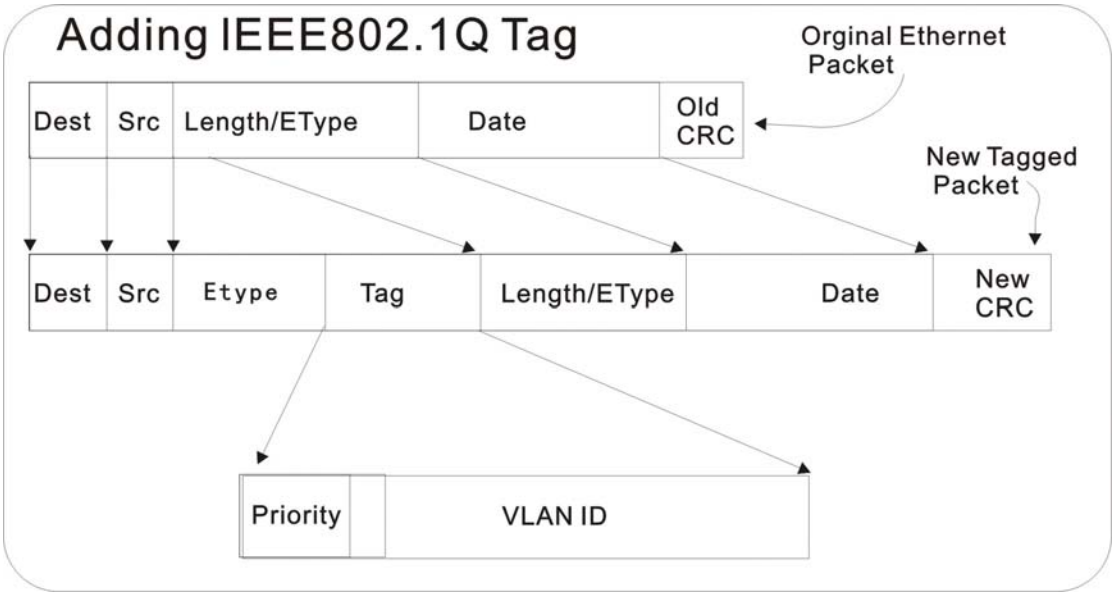


图 4-1 IEEE802.1Q 帧格式

基于 IEEE802.1Q Tag VLAN 用 VID 来划分不同的 VLAN，当数据帧通过交换机的时候，交换机根据帧中 Tag 头的 VID 信息来识别它们所在的 VLAN（但是若帧中无 Tag 头，我们称这种帧为 Untag 帧，并使用帧所通过端口的缺省 VID 信息来识别它们所在的 VLAN。还可以通过设置，对 Untag 帧进行不同的处理），这使得所有属于该 VLAN 的数据帧，不管是单址帧、多址帧还是广播帧，都将限制在该逻辑 VLAN 中传播。组中主机之间能够相互彼此通信，而不受其它主机的影响，就像它们存在于单独的局域网当中一样。

本交换机支持 IEEE802.1Q 的 Tag VLAN，在配置 VLAN 时，有几项配置需要考虑：

- VLAN ID：设置 VLAN 的标识符，用于标识某个 VLAN。
- VLAN 广播域：用于界定该 VLAN 帧的转发范围，不在 VLAN 广播域内的端口将不能收到任何来自该 VLAN 的帧。
- 端口的缺省 VID：当交换机不能从一个帧的 Tag header 中获得该帧属于哪一个 VLAN 时（我们称这种帧是 Untag 帧），则通过帧进入交换机时所通过端口的缺省 VID 来判断该帧在哪个 VLAN 中。

注　意：

普通端口和 Trunk 成员端口的缺省 VID，分别在端口参数和 Trunk 配置中进行设置。

4．4．1．3　禁止 VLAN

在禁止 VLAN（VLAN Disable）模式下，交换机无任何 VLAN，任何数据包都可以在交换机上任意端口之间转发。

4．4．2　VID 配置

4.4.1.2 节中提到，IEEE802.11Q Tag VLAN 模式下，每一个 VLAN 都有一个特定的 VLAN 标识符，我们称之为 VLAN ID（VID）。一般，VLAN ID 可以使用的范围是 1—4094（二进制表示为 12 位其中 0 和 4095 保留）。KN-S10-5024GM 交换机支持用户最多设 512 个 VLAN。

4．4．3　VLAN 配置

两种 VLAN 模式下，VLAN 配置规则不同，具体如下：

- 基于端口的 VLAN 配置规则：

1: 默认所有端口均在 PORT VLAN 1 中。

- （PORT VLAN 我们没有做下面的规则，删掉）

1. 新建立的或修改的 VLAN 不能是已存在的 VLAN 的父集或子集。
2. 不能设置一个空的 VLAN。

- 基于 IEEE802.1Q 的 Tag VLAN 配置规则：

1. VLAN 的 VID 必须是唯一的。
2. VLAN 的合法 VID 必须在 1-4094 的范围内。
3. 不能设置一个空的 VLAN。（我们没有设置此规则）
4. 如果某端口连接的是不支持 IEEE802.1Q 协议的设备（如 HUB、普通交换机或其它不支持 IEEE802.1Q 协议的网络适配器时），则只能将该端口规则设置为 Untag。
5. 默认所有端口均属于 VLAN 1，VLAN 1 不可以被删除和修改。

4．4．4　MTU VLAN 组

在这里用户可以简单快速的设置一对多的 VLAN。

MTU VLAN（Multi-Tenant Unit VLAN）是将每个用户所占用的端口与上行端口划分为一个单独的 VLAN。使不同端口的用户之间不能直接通信，以保障了网络的安全。（在划分了 MTU VLAN 后，只能通过上行端口用 WEB 方式对交换机进行对进行管理，用户端口将无法访问通过 Web 方式访问交换机），这种情况很适合使用在智能小区中，用户之间不可以直接访问，从而保证住户的网络安全。

4．5　Trunk 配置

Trunk 就是一种端口聚合（Port Aggregation）的机制。

端口聚合通常被用于将多个端口聚合在一起，从而形成一个高带宽的数据传输通道。交换机把聚合在一起的所有端口看作一个逻辑端口。

KN-S10-5024GM 交换机最多可以创建 8 组 Trunk，创建 Trunk 时遵循以下规则：

1、 Trunk 必须是 2 个到 8 个端口，不可以使用 8 个以上的端口进行端口汇聚或者仅使用一个端口组成一个 Trunk。

此外，Trunk 还具有 Link Fail Over 功能，即当 Trunk 的某条成员链路断开时，交换机自动将此链路上的数据分配到 Trunk 的其它链路上，以维持该 Trunk 数据传输。当断开的链路重新连接上时将恢复原先的负载分配。

2: KN-S10-5024GM 的 Trunk 为基于 MAC 作为选路策略的 Trunk，就是说如果流过 Trunk 成员端口的数据流选择所走的具体那条 Trunk 成员端口是根据该数据流的目的 MAC 地址和源 MAC 地址来选择。如果所有数据流在选路时均选中同一条 Trunk 成员端口的话, 则无法达到负载分配的效果，此时，Trunk 链路将无法达到该 Trunk 链路理论上的传输最大值。

注意：

Trunk 与 VLAN 之间的影响：

在设置 Trunk 的时候，不管是创建 Trunk 或者是将一个端口加入到 Trunk 中，加入 Trunk 的成员端口都将从所有的 VLAN 中删除。如果是从 Trunk 中删除成员端口或者是删除整个 Trunk 时，原 Trunk 的成员端口不会恢复到任何 VLAN 中。初期创建一个 Trunk，此 Trunk 将不属于任何 VLAN，用户应根据需要将它配置到需要的 VLAN 中。

Trunk 与端口安全、端口带宽、端口监控之间的影响：

设置成 Trunk 成员的端口不能再启用端口安全和端口带宽控制，并且不能设置为监控端口，反之一样。

温馨提示：

Trunk 带宽的计算：

当使用四个全双工 1000Mbps 端口构成 Trunk 时，由于每一个端口上行和下行各是1000Mbps，所以每一个端口的带宽为 2000Mbps。它们使用 Trunk 技术汇聚在一起形成的总带宽为 8000Mbps（2000Mbps ×4）。

4．6 优先级管理

该交换机提供了对不同优先级（priority）帧的传输处理机制，交换机根据传输等级表将收到帧的优先级映射到传输等级，传输等级高的帧将得到优先处理。优先级的分类可以基于端口优先级、DSCP 优先级、802.1p 优先级进行设置。用户可以选择当前优先级的分类标准，该交换机支持 8 个优先级队列。

- **流：**流即业务流traffic 指所有通过交换机的报文。
- **流分类：**流分类traffic classification是指采用一定的规则识别出符合某类特征的报文。分类规则classification rule指配置管理员根据管理需求配置的规则。分类规则很简单，一般的分类依据都局限在封装报文的头部信息。
- **优先级标记：**以太网交换机可为特定报文提供优先级标记的服务，标记内容包括DSCP 802.1p等这些优先级标记分别适用于不同的QoS模型在不同的模型中被定义。
- **队列调度：**当网络拥塞时，必须解决多个报文同时竞争使用资源的问题。通常采用队列调度加以解决。这里介绍3种各具特色的队列调度算法：严格优先级SP（Strict-Priority）加权平均优先级（WRR：Weighted Round Robin）调度算法。

4．6．1 优先级配置

- 优先级模式：共有 Disable、Port-Based Priority、DSCP Priority 及 802.1p Priority 四种模式。其中 802.1p Priority 只在 802.1Q Tag VLAN 模式下生效。
- 优先级控制法则：有 SDWRR 和 Strict-Priority 两种选择。当优先级控制法则为 WRR 时，交换机根据数据帧的优先级（优先级一、优先级二、优先级三、优先级四、优先级五、优先级六、优先级七、优先级八）按比例转发数据帧；当优先级控制法则为 Strict-Priority 时，交换机优先转发优先级最高的数据帧，然后再按一定比例转发其余优先级的数据帧。
- 802.1p 优先级映射模式：只有在 802.1p Priority 模式下才能启用该功能。

4．6．2 端口优先级表

端口优先级有 8 种选择，分别是优先级一、优先级二、优先级三、优先级四、优先级五、优先级六、优先级七和优先级八。当优先级模式为 Port-Based Priority 时，从该端口接收到的所有帧都将指定为该 8 种优先级。

端口优先级表中同时可以设置该端口的默认优先级 Tag，此时从该端口接收到的所有 Untagged 帧都将被赋予此默认优先级 Tag，此功能只在 802.1p Priority 模式下生效。

4．6．3　DSCP 优先级

DSCP（ Difference Service of Class Priority）服务类型是IP首部的TOS一个8bit字段中的前6bit。用来代表不用的优先级，本系列交换机提供依据DSCP优先级进行队列的划分功能。6bit的DSCP值为0～64，可以映射到不同的8个优先级队列。

4．6．4　802.1p 优先级

当 802.1p 优先级生效时，我们可以设置不同优先级 Tag（0-7）所对应的 8 个传输等级。如果端口收到的是 Untagged 帧，它将会把该端口所设置的默认优先级 Tag 赋予该帧以进一步处理。

注　意：

802.1p 优先级只在 802.1Q Tag　VLAN 模式下生效。

4．6．5　802.1p 优先级映射表

原优先级 Tag 到新优先级 Tag 的映射表。可以设置不同的原优先级 Tag（0-7）与新优先级 Tag（1-8）之间的映射关系，交换机依据映射表将收到的不同原优先级 Tag 的帧映射到用户所设置的新优先级 Tag 上。

注　意：

1、该映射表在优先级配置中的 802.1p 优先级映射模式为 Enable 时有效。

2、该映射表对使用了端口默认优先级 Tag 的数据帧无效。

4．6．6 应用程序优先级

根据设置的所需应用，来决定其处理级别的高低。

例：一般来说，如果遇到内网有人下载 BT，那是肯定会很快的把带宽给占满的，这样，就有可能影响内网的其他用户上网。甚至连 QQ 发送消息或者 QQ 语音都无法正常使用。那为了满足大部分用户的 QQ 使用，您就可以把它的优先级设置为高优先级，既转发数据的时候，优先转发关于 QQ 的。做到了就算有人使用 BT，对 QQ 一些简单的操作也不会受影响。

重要提示：

基于应用程序 QoS 和安全防御总的支持 96 条，其只要给设置了基于某个 TCP 或者 UDP 端口的 QoS 优先级之后，安全防御将不可以对 TCP 或者 UDP 端口该进行防御

4．7　交换机安全配置

KN-S10-5024GM 交换机作为一个网络设备，除了承当数据转发的功能外，在病毒多的环境里，还承担着对病毒的过滤功能。这样该交换机所在的局域网可以做到基于端口的病毒隔离。这些功能主要利用绑定的方法和 ACL 工具来实现。

4．7．1　ARP 病毒防护

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，过滤受防护端口广播或回应非绑定主机的 ARP 报文。ip + mac 绑定和 mac 地址邦定户为独立模块，互不影响。

重要提示：

1） 每个端口允许设置的绑定 arp 防护的主机数不固定，总的支持 480 条。

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。

4．7．2 病毒防御模块

可以针对一些病毒如蠕虫、振荡波等等或者用户自定义 TCP 或者 UDP 端口，对设置了病毒防御的端口号的数据进行丢弃处理。

第五章　WEB　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 管理的连接

5．2．1　　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。

首先，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 lE 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，对于已经使用较长时间的 PC 可以不按此设置。

5．2．1　连接

假设需要配置的交换机的 IP 地址是 192.168.1.254，要连接交换机只要在浏览器的地址栏中正确输入 http://192.168.1.254，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（交换机的缺省密码为 admin），点击“登录”按钮，就进入 WEB 管理交换机主页了。其中浏览方式的密码是：user

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，只保留缺省密码。

5．3　　WEB 管理界面及操作方法

在页面左侧，本公司商标的下方，是功能菜单界面，它呈树状目录结构。商标右面是交换机的外观，最右面是端口面板的端口状态界面。端口状态界面以下的大块区域是用于功能配置的主窗口。

KN-S10-5024GM 交换机有 24 个千兆端口，端口面板状态界面指示了它们的工作状态。呈现绿色表明该端口处于连接状态，没有连接的端口图标呈现灰色。端口图标上呈现黑斜杠表明该端口被禁用。在端口图标的右侧有各种状态的图例说明。

图 5-7　KN-S10-5024GM WEB 主页

左侧的功能菜单呈树状目录结构，整个目录分成两层，如果点击某一主项，就会展开这一主项下的所有子项，同时主窗口会显示这一主项第一个子项的配置页。如果想要设置其它子项，只需要点击相应子选项，主窗口就会切换到被点击子项的设置页。

在一个主项被展开的情况下，如果点击其它主项，以前展开的主项会闭合，被点击的主项将展开，此时主窗口会显示被展开的主项的第一个子项的设置页。如果点击已打开的主项，

此主项会闭合，此时没有打开的主项，主窗口又会回到图 5-7 的状态。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。

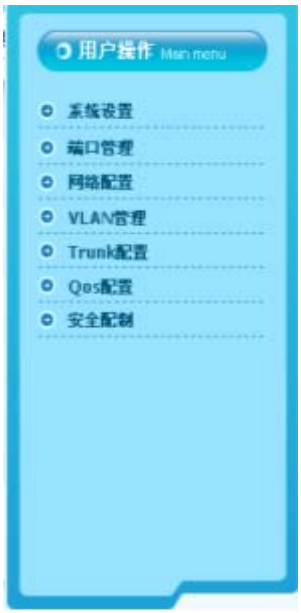


图 5-8 功能菜单

以下列出了功能菜单的主项以及主项下的子项：

- 系统配置：系统信息、系统密码设置、IP 地址参数、文件传输、保存与复位
- 端口管理：端口参数、端口镜像、端口描述、端口统计、端口状态、端口带宽
- 网络配置：最大老化时间、MAC 地址绑定、Ping 检测
- VLAN 管理：VLAN 模式配置、VLAN 配置、MTU VLAN 组
- Trunk 配置：Trunk 配置
- QoS 配置：优先级配置、端口优先级配置、DSCP 优先级、802.1p 优先级、应用程序优先级
- 安全配置：主机安全保护静态配置、主机安全保护动态配置、安全防御模块配置

注意：对交换机设置所做的所有的修改只有在点击“提交”按钮后才会生效。

系统配置

系统配置包括：系统信息（如软硬件版本、串口波特率等）、系统密码设置（设置交换机的管理密码）、IP 地址参数（配置 IP 地址，子网掩码等）、文件传输、保存与复位。

系统信息

主要包括以下设置（如下图）：

图 5-9 系统信息

- 系统名称：使用一个名字来标识交换机。
- 系统位置和联系方法：标识交换机的管理人员和位置。
- 网页最大闲置时间：Web 网页的最大停滞时间，就是如果用户如果在这段时间内没有通过网页对交换机做任何操作，交换机将会重新退出到登陆界面。
- WEB 管理端口号：可以指定访问交换机网页的 TCP 端口号。
- CPU VLAN ID：只有在此 VLAN 内的主机才能管理到交换机。

系统密码设置

主要包括以下设置（如下图）：

图 5-10 系统密码设置

- 管理权限：管理员可以选择是管理用户还是浏览用户
- 当前密码：用户正在使用的密码。
- 新密码：用户将要使用的密码。
- 新密码确认：重新输入一次新密码。

温馨提示：密码最多支持 12 位可以是数字、字母区分大小写

IP 地址参数

主要包括以下设置（如下图）：

图 5-11 IP 地址参数

- 物理地址：交换机在出厂时会被赋予一个唯一的 MAC 地址。
- DHCP 状态：指示 DHCP 功能是否打开，如果该功能打开的话（选择“Enable”），交换机自动根据 DHCP 服务器配置交换机的 IP 地址，子网掩码和缺省网关。若关闭（选择“Disable”）需要手动对交换机的 IP 地址，子网掩码和缺省网关进行设置。
- 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，本交换机的出厂默认 IP 地址为 192.168.1.254/255.255.255.0。
- 默认网关：当数据包的目的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。

注意：

DHCP 功能开启时，交换机将从网络中的 DHCP 服务器自动获取各项 IP 地址参数，所以此时“IP 地址”、“子网掩码”和“默认网关”均不需配置。在 DHCP 方式下，用户必须在带外管理中用显示 IP 地址的命令得知交换机动态所获取的 IP 地址后方可进一步对交换机进行 Web 方式的管理操作。用户在修改了交换机的静态 IP 之后，网页将会停滞不动，无法进一步操作，用户必须在浏览器地址栏中重新输入新更改的 IP 地址来重新访问交换机。

文件传输

主要包括以下设置（如下图）：

图 5-12 文件传输

文件传输说明：

- 传输选项：有三种传输选项，下面会详细介绍。
- 文件名：所传输的文件名，命名规则须符合 DOS 的 8＋3 文件格式。
- TFTP 服务器 IP：使用 TFTP 协议更新或下载文件时的 TFTP 服务器 IP 地址。

传输选项：

- 更新系统文件：从 TFTP 服务器下载并更新系统文件。
- 备份配置文件：将交换机的配置参数备份到 TFTP 服务器上。
- 载入配置文件：从 TFTP 服务器下载配置文件到交换机上进行配置参数更新。

重要提示： （文件更新设置）

1. 进行 TFTP 下载时，TFTP 服务器应包含更新所需的文件。
2. 应保证指定机器上 TFTP 服务器处于运行状态。
3. 在 TFTP 下载过程中不允许中断下载操作，否则交换机有可能出现异常现象。

保存与复位

主要包括以下设置（如下图）：

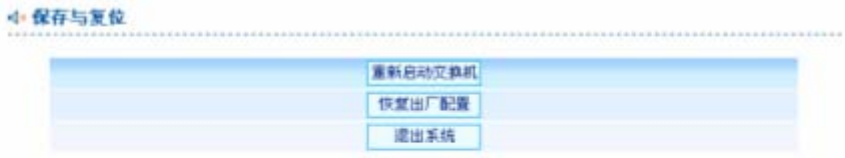


图 5-13 复位

点击其中的按钮会出现提示框请求确定，例如点击“恢复出厂配置”确认提示框如下图：

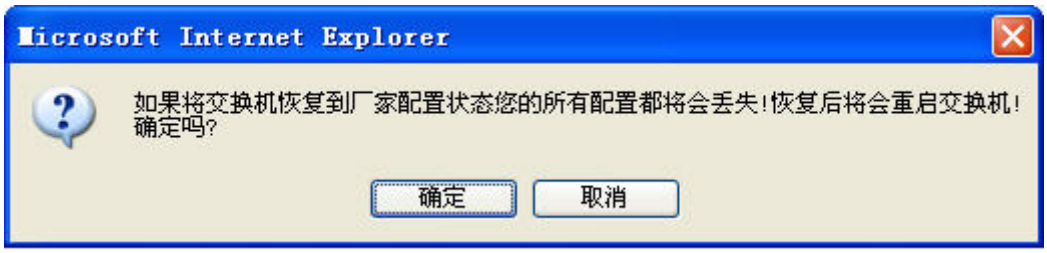


图 5-14 确认提示框

此时可以点击“确定”执行相应操作，或者点击“取消”放弃相应操作。

友情提示注 ：

恢复为出厂状态时，交换机的 IP 地址参数也将被设置为出厂设置。（恢复出厂设置后交换机的默认设置请参考本说明书背后的出厂设置参数表）

恢复出厂默认和重启交换机需要大约两分钟的时间，请耐心等待!!!

端口管理

端口管理主项包括端口参数（设定流量控制、端口安全和选择协商方式等）、端口镜像（设定镜像端口等）、端口描述、端口统计 （统计发送帧、接收帧、碰撞帧等）、端口状态（显示连接状态、端口速率、端口模式等信息）、端口带宽、广播风暴抑制。

端口参数

主要包括以下设置（如下图）：

图 5-15 端口参数（IEEE802.1Q Tag VLAN 模式）

- 端口状态：“Enable”表示端口处于可用状态（默认），“Disable”，表示端口处于禁用状态。端口被禁用时交换机将丢弃来自这个端口的数据包。
- 流量控制：“Enable”表示端口启用流量控制功能，“Disable”，表示不使用这项功能。
- 协商方式：可选择：“Auto”、“10M／HD”、“10M／FD”、“100M／HD”、“100M／FD”、“1000M/FD”。分别表示自动协商、十兆半双工、十兆全双工、百兆半双工、百兆全双工、千兆全双工。
- 缺省 VLAN ID：缺省的 VID 号，只有在 IEEE802.1Q Tag VLAN 模式下可以设置。交换机上端口的缺省 VID 是当端口收到一个 Untag 帧时，指定给这个帧的 VID。

说明：

- 通过改变第一行的端口号，页面会自动切换到你所选择的端口上。
- 当交换机工作在基于端口的 VLAN 模式或者 VLAN 功能不启用时，上图中的 “缺省 VLAN ID”项将不能用。
- 本页面不能修改 Trunk 组的成员端口的参数，如要更改请进入 Trunk 配置页面操作。

端口镜像

本页面配置监控方式的端口、工作模式和数据流向。主要包括以下设置（如下图）：

图 5-16 监控配置

- 监控模式：有“Tx”、“Rx”、“ALL”3 种状态。当监控模式为“Tx”时，监控端口只接收被监控端口的发送数据包；当监控模式为“Rx”时，监控端口只接收被监控端口的接收数据包；当监控模式为“ALL”时，监控端口接收被监控

端口的发送和接收的数据包；

- 监控端口：用于获取监控信息的端口。
- 被监控端口：选择要被监控的端口，它可以是一个或几个端口。

说明：

- Trunk 组的成员端口不能作为监控端口，但可以作为被监控端口。
- 监控端口与被监控端口需处于同一 VLAN 中。
- 一个端口不可以既作为监控端口又作为被监控端口，否则会返回出错信息。

图 5-17 出错信息

5．3．2．3　　端口描述

本页面设置交换机所有端口的描述信息，以便网络管理员分清楚各个端口的用途。主要包括以下设置（如下图）：

图 5-18 端口描述

- 端口：端口的端口号。
- 描述信息：此处填写描述文字，您最多可以存入 15 个纯汉字或 30 个英文字符或数字。

5.3.2.4　端口统计

本页面中显示针对端口的统计信息。

端口统计

端口：	13	刷 新	清 零
Rx (Bytes) :	4289080	Rx Pkts :	4334
Rx Bcast :	1789	Rx Mcast :	94
Rx UnderSz :	0	Rx OversSize :	0
Rx Fragmt :	0	Rx Jobber :	0
Tx (Bytes) :	25516030	TxBcastPkt :	1
TxMcastPkt:	0	Tx DeferPkt :	0
Collisions:	0		

图 5-19 端口数据统计

各项条目的含义如下：

- Rx（Bytes）：接收到的字节数
- Rx Pkts：接收到的包数目
- Rx Bcast：接收到的广播包数目
- Rx Mcast：接收到的组播包数目
- Rx UnderSz：接收到小于 64 字节（总长）的超短帧数目
- Rx OverSz：接收到超过 1518 字节（总长）的超长帧数目
- Rx Fragmt：接收到的非完整的（帧校验错误的）长度小于 64 字节的帧的数目
- Rx Jobber：接收到的非完整的（帧校验错误的） 长度超过 1518 字节的帧的数目
- Tx（Bytes）：转发出的字节数
- TxBcastPkt: 转发的广播包数。
- TxMcastPkt: 转发的广播包数。
- Tx DeferPkt：延迟转发出的包的数目
- Collisions：碰撞次数

5．3．2．5　　端口状态

本页面中显示已建立物理连接的端口状态信息。包括以下设置（如下图）：

端口状态

端口	端口状态	连接速率(Mbps)	双工模式	流量控制
1	Down	--	--	--
2	Up	100M	Full	Disabled
3	Down	--	--	--
4	Down	--	--	--
5	Down	--	--	--
6	Down	--	--	--
7	Down	--	--	--
8	Down	--	--	--
9	Down	--	--	--
10	Up	100M	Full	Disabled
11	Down	--	--	--
12	Down	--	--	--
13	Down	--	--	--
14	Down	--	--	--

图 5-20 端口状态（部分端口）

- 端口状态：“Up”表示当前端口建立了物理连接，“Down”表示当前端口未建立连接。
- 连接速度：显示“10”、“100”或“1000”，单位是 Mbps。如果端口没有连接，显示“--”

- 协商模式：显示“Full”（全双工）或者“Half”（半双工）。
- 流量控制：“Enable”表示启用了流量控制功能，“Disable”表示没有启用流量控制功能。

注意：如果交换机中设置了该端口流控“Enable”，但是如果和该端口连接的对端端口流控为“Disable”或者不支持流控的话，本状态显示栏中显示的流控状态依然为“Disable”。

端口带宽

主要包括以下设置（如下图）：

图 5-21 端口带宽（部分端口）

- 入口带宽控制：“Enable”表示对当前端口的输入方向进行带宽控制，“Disable”表示不对当前端口的输入方向进行带宽控制。

  入口带宽：选择范围是从 100K 到 1G 之间任意数。如果入口带宽控制为“Enable”才可以设置。
- 此页面包含了便于用户设定的快速更改功能。修改“所有端口”一行的某个下拉选框然后点击下拉选框下面的“更改”按钮，所有可设定端口的对应项都会更改。“入口带宽”的快速更改功能只适用于启用带宽控制的端口。
- 快速更改只是做了 WEB 页面上的修改以便于您的操作，更改的内容并没有设入交换机。只有当您点击了“提交”后所做的修改才会生效。
- Trunk 组的成员端口不可以配置端口带宽控制。

网络配置

网络配置主项包括最大老化时间（设定动态地址的老化时间）、动态地址表（显示动态 MAC 地址）、MAC 地址绑定、Ping 检测。

5．3．3．1　最大老化时间

包括以下设置（如下图）：

图 5-22 最大老化时间

- 最大老化时间（10—630）：设定动态地址的老化时间，单位是秒。如果设置为 0 表示地址不会被老化。

说明：

1. 最大老化时间是一个影响交换机学习的参数。如果动态地址表中某个地址在最大老化时间内未被使用，那么该地址将被删除。
2. 最大老化时间的数值范围从 10~630 秒。过长的最大老化时间会导致交换机内的动态 MAC 地址表中地址超期，从而导致交换机进行不正确的过滤 / 转发。如果最大老化时间过短，又会造成地址表刷新过快，大量接收到的数据包的目的地址在动态 MAC 地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这将降低交换机的性能。
3. 静态地址表不受最大老化时间的影响。

5．3．3．2　MAC 地址绑定

MAC 地址绑定的地址是不会老化的 MAC 地址，不同于静态地址，它实现针对数据源的过滤。同时它也是静态的，在被删除之前始终有效，不受最大老化时间的限制。当 MAC 地址绑定后，进入某端口的帧的源地址只有存在于该端口的 MAC 地址绑定的地址表中，才能被转发，否则将被丢弃。

本页面可以对 MAC 地址绑定的地址表中的地址进行添加和删除操作。MAC 地址绑定的地址可以设置在所有的端口中，且不限制每个端口绑定的 MAC 地址数目，只限制交换机的支持绑定 MAC 地址的总容量。

本页面的 MAC 地址绑定的地址按照端口进行分组，所以首先要选择端口号。在“端口号”右侧的下拉选择框中选择您要配置的端口，页面将显示该端口已绑定的地址。在 VID 栏中选中该端口要绑定的 VLAN ID。在 MAC 地址栏中填入需要添加或删除的 MAC 地址然后点击“添加”，“删除”按钮可以进行地址添加和地址状态更改操作。

图 5-23　MAC 地址绑定

“序号”一项显示的值是该地址在整个 MAC 地址绑定表中的位置。您可以进行“Delete”操作，删除该静态安全地址表项。

MAC 地址绑定遵从以下规则：

1、如果该端口没有绑定任何 MAC 地址，则该端口可以正常进行地址学习和转发。但是只要该端口绑定了一条以上的 MAC 地址。该端口的动态学习转发功能将会被关闭。只有符合绑定的地址条件的数据流才可以正常在该端口进行转发。

2、在进行 MAC+VLAN ID+端口绑定之后，所有流经该端口的数据帧只有源 MAC 地址，VLAN ID（如果该数据流不带有 VLAN TAG， 此时该 VLAN ID 则为该端口的默认 VLAN ID 值）和绑定中的值一一对应时方可以正常转发。否则交换机将会把该数据帧丢弃。

温馨提示：

KN-S10-5024GM 交换机不限制每个端口绑定 MAC 地址数目，其支持的 MAC 地址绑定总容量为 480 条。

5．3．3．3　Ping 检测

使用交换机时经常需要知道交换机是否和网络中某个节点正常连接。Ping 检测就实现这种网络探测。本页面可以设定 Ping 的参数如下：

图 5-24　Ping 检测

目标 IP 地址：远程主机 IP 地址。

发送次数：发送 Ping 数据包的次数。

发送报文长度：Ping 数据包内携带的数据部分大小。

5．3．4　VLAN 管理

VLAN 管理主项包括 VLAN 模式配置、VLAN 配置（配置 VID，成员端口，状态等）、MTU VLAN 组（设置 Uplink 端口）。关于 VLAN 的基本知识请参考 4．4 节。

5．3．4．1　VLAN 模式配置

VLAN 模式有三种选项：基于 IEEE802.1Q 的 Tag VLAN、基于端口的 VLAN 和禁止 VLAN 功能。其设置如下图：

图 5-25　VLAN 模式配置

- 802.1Q Tag VLAN：基于 IEEE802.1Q Tag 的 VLAN 模式。
- Port-Based VLAN：基于端口的 VLAN 模式。
- VLAN Disable：禁止 VLAN 功能。

说明：

交换机的默认设置为 IEEE802.1Q Tag VLAN 模式。此时，交换机中存在一个包含所有端口的 VLAN（VID 为 1）。

注　意：

只有改变了原有的 VLAN 模式才可以提交成功，而且这个操作将会重新启动交换机。

5．3．4．2　VLAN 配置

交换机在不同的工作模式下设置是不同的。在 IEEE802.1Q Tag VLAN 模式下，主要包括以下设置（如下图）：

图 5-26　VLAN 配置（IEEE802.1Q VLAN 模式）

- Tag VLAN No.：VLAN 的编号，不能重复，用于管理人员标识 VLAN。
- Tag VLAN ID：VLAN 的标识，不能重复。
- 状态：可以选择“Enable”、“Disable”或“Delete”，表示当前 VLAN 的状态。
- 端口规则：对数据帧的处理方式。“Untag”表示此端口属于该 VLAN，且从该端口发出的数据帧不带 Tag 字段。“Tag”表示此端口属于该 VLAN，且从该端口发出的数据帧包含 Tag 字段。空白表示此端口不属于该 VLAN。
- Clear Up：使所有的端口不在指定的 VLAN 中。
- AII Untag：使所有的端口输出规则为 Untag。
- All Tag：使所有的端口输出规则为 Tag。

当交换机工作在基于端口的 VLAN 模式时，主要包括以下设置（如下图）：

图 5-27　VLAN 配置（Port-Based VLAN 模式）

- VLAN No.：VLAN 的编号，不能重复，用于标识 VLAN。
- VLAN 成员：VLAN 中的端口成员，端口号前的复选框表示该端口是否包含在这个 VLAN 中。

注　意：

如果 VLAN 的模式是 VLAN Disable，“VLAN 配置”页面将会从功能菜单删除，当 VLAN 的模式是在 IEEE802.1Q Tag VLAN 模式或基于 Port VLAN 模式下时，“VLAN 配置”页面又将在功能菜单出现。

5．3．4．3　MTU VLAN 组

本页面设置 MTU VLAN 的 Uplink 口的端口号（如下图）：

图 5-28 MTU VLAN

说　明：

Uplink 端口（1-24）上行端口。当设置某个端口为上行端口时，它将依次和其它 23 个的端口分别组成一个 VLAN，结果将为交换机生成 23 个 VLAN，每个 VLAN 包含两个端口：

一个为刚才设置的上行端口，另一个依次为这个上行端口之外的其他 23 个端口。 在基于 IEEE802.1Q Tag VLAN 模式下，还会再增加一个包含所有端口 VLAN。可以在设置完上行端口后进入 VLAN 管理菜单查看 VLAN 配置情况。

注　意：

当设置了 MTU VLAN 组并生效后，原来设置的所有 VLAN 和所有 Trunk 均将被撤销。

5．3．5　Trunk 配置

关于 Trunk 的配置只有一页。KN-S10-5024GM 交换机最多可以创建 7 组 Trunk。有关 Trunk 配置的说明请参考 4．5 节内容。主要包括以下设置（如下图）：

图 5-29 Trunk 配置

- Trunk 号：KN-S10-5024GM 交换机最多可以创建 8 组 Trunk
- 状态：“Enable”、“Disable”和“Delete”三个状态分别对设置的 Trunk 进行 Enable（允许），Disable（禁止）和 Delete（删除）操作。
- 协商模式：对 Trunk 成员端口的工作模式进行控制。
- 缺省 VID：表示在 Untag 模式下 Trunk 逻辑端口的缺省 VID，此项在 VLAN 模式为 802.1Q Tag VLAN 模式时可以配置。
- Trunk 成员：选择加入 Trunk 的端口。

Trunk 配置规则：

1. KN-S10-5024GM 交换机支持最多 8 组 Trunk，组成 Trunk 的成员端口可以是 2-8 个。
2. 已经成为一个 Trunk 的成员端口不能再设置作为另一个 Trunk 的成员端口。
3. 当设置一个 Trunk 后，Trunk 中的所有成员端口将在整体上被交换机作为一个逻辑端口来看待。

5．3．6　优先级管理

优先级设置包括优先级配置、端口优先级表、DSCP 优先级、802.1p 优先级。优先级配置页面选择一种优先级的模式，后面的四张页面分别对三种类型的优先级进行参数配置，没

有生效的优先级模式其页面也是可以设置的。

各种优先级概念的说明可以参看 4．6 节。

5．3．6．1　优先级配置

包括以下设置（如下图）：

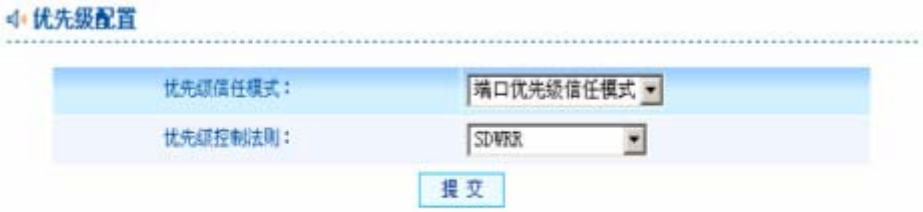


图 5-30 优先级配置

- 优先级模式：共有端口优先级信任模式、DSCP Priority 及 802.1p Priority 四种模式。其中 802.1p Priority 只在 802.1Q Tag VLAN 模式下生效。
- 优先级控制法则：有 SDWRR 和 Preempt+SDWRR 两种选择。当优先级控制法则为 SDWRR 时，交换机根据数据帧的 8 个优先级按比例转发数据帧；当优先级控制法则为 Preempt+WRR 时，交换机优先转发优先级为优先级八的数据帧，然后再按一定比例转发其余优先级的数据帧。
- 802.1p 优先级映射模式：只有在 802.1p Priority 模式下才能启用该功能。交换机会将收到的数据帧的 Tag 优先级映射到用户所设置的新优先级上，从而实现在不改变数据帧中优先级字段的前提下自由改变本地转发的优先级。

5．3．6．2　端口优先级表

本页面的设置对应于优先级配置页面中设置的端口优先级模式。包括以下设置（如下图）：

图 5-31 端口优先级表

- 端口：表项对应的端口号。
- 优先级：用户可以选择 8 个优先级的一个，从该端口接收到的所有帧都将指定为该优先级。其中优先级八是最高的优先级
- 默认优先级 Tag：如果交换机工作在 802.1Q Tag VLAN 模式下，并且优先级模式设为 802.1p Priority 模式，从该端口收到的所有 untagged 帧都将被赋予默认优先级 Tag 值。

5．3．6．3　DSCP 优先级

本页面的设置对应于优先级配置页面中设置的 DSCP 优先级模式，建立 DSCP 字段与本地优先级的映射关系，端口接收的数据按本地优先级规则发送。包括以下设置（如下图）：

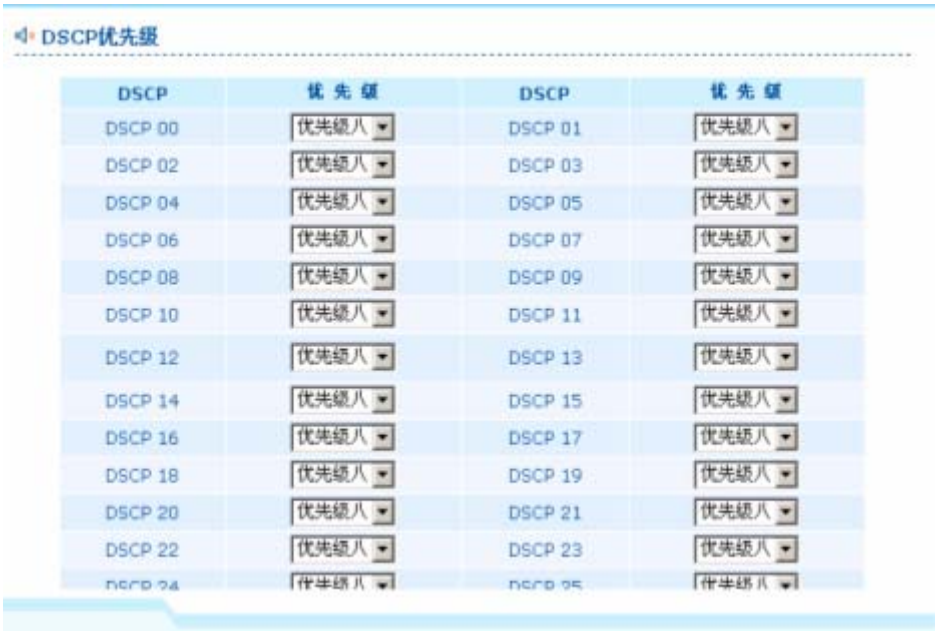


图 5-32 DSCP 优先级

- DSCP：DSCP（Difference Service of Class Priority）服务类型是 IP 首部的 TOS 一个 8bit 字段中的前 6bit,用来代表不用的优先级。值为 0~63。
- 优先级：传输等级，可以选择 8 个优先级中的一项。它们的发送权比为 1：2：4：8：16。端口发送时按权比分配带宽。

5．3．6．4　802.1p 优先级

本页面的设置对应于优先级配置页面中设置的 802.1p Priority （802.1p 优先级）模式。包括以下设置（如下图）：

图 5-33　802.1p 优先级

- 优先级 Tag：数据帧的 Tag 优先级。如果开启了 802.1p 优先级映射功能，则表示映射后的新 Tag 优先级。
- 优先级：传输等级，可以选择 8 个优先级选项中的一项。它们的发送权比为 1：2：4：8：16。端口发送时按权比分配带宽。

说明：如果端口收到的是 untagged 帧，即未添加 Tag 字段，那么交换机将会把该端口所设置的默认优先级 Tag（即端口优先级表页面中设定的值）赋予该帧以进一步处理。

5．3．6．5　应用程序优先级模板设置

本页面的设置主要用于对不同的应用程序给予不同的转发优先级。对一些特殊的应用程序，对转发延迟比较敏感，需要高的转发优先级。比如网络内的游戏就需要高的优先级，而下载可以给予低的优先级。该模板除了设置一些常用程序外，用户还可以自己制定应用程序的类型。如下图：

图 5-34 应用程序优先级设置（固定程序）

图 5-35 应用程序优先级设置（用户自定制）

- 设置选择：用户可以选择是选择已经设定的模板还是用户自定义。
- 应用程序模板：用户可以选择已经定义的应用程序和给该程序赋予的优先级，当用户选择确定后，该设置就生效了。
- 名称：用户定义的优先级程序名称。
- 协议：用户可以选择 TCP 或 UDP，说明用户通过哪个协议来确认应用程序，当用户选定 TCP 后，就会有选项让用户输入 TCP 的端口号；UDP 也一样。
- 优先级：用户给定义的应用程序赋予的优先级。

说明：

当用户选择的应用程序赋予优先级后，在查看程序优先级应用的列表中可以看到。要是想要取消某一条，可以定义该项目后面的删除按钮。

5．3．7　安全配置

安全配置包括主机安全保护静态配置、主机安全保护动态配置、安全防御模块设置。各种交换机的安全概念的说明可以看 4．7 节。

5．3．7．1　主机安全保护静态配置

图 5-36 主机安全保护静态配置

- 手动输入 IP 和 MAC 地址进行防护。
- 当输入完成后，点击添加，则在下面的列表中列出添加的信息。
- 注：列表中列出的是所有的绑定信息（静态配置和动态配置）

5．3．7．2主机安全保护动态配置

图 5-37 主机安全防护动态配置

- 搜寻范围：选择一段 ip 地址范围进行搜索。
- 点击搜索后在下面的列表中列出搜索到的信息条目。
- 注：
  - 当已存在绑定的条目时，显示绑定的条目信息（静态或动态配置的）。
  - 当已存在绑定的条目时，不能进行一键绑定，可以进行一键删除所有的绑定配置。
  - 在未配置绑定信息时，显示动态搜索的信息，可以进行一键绑定，或一键清除（删除动态搜索的所有信息）。
  - 当条目显示为红色时，表示存在一个 mac 对应多个 ip 等错误，不能进行一键绑定。

5．3．7．3 病毒防御模块

本页面的设置主要用于防御利用 TCP/UDP 端口进行入侵的病毒。对用户根据当前应用的环境，防止一些病毒入侵，维护网络安全。该模板除了设置一些常见病毒外，用户还可以自己制定防护病毒的类型。如下图：

图 5-38 安全防御（已定义病毒）

图 5-39 安全防御（用户自定义病毒）

- 设置选择：用户可以选择是选择已经设定的模板还是用户自定义。
- 应用程序模板：用户可以选择已经定义的病毒，当用户选择确定后，该设置就生效了。
- 名称：用户定义的优先级程序名称。
- 协议：用户可以选择 TCP 或 UDP，说明用户通过哪个协议来确认应用程序，当用户选
- 定 TCP 后，就会有选项让用户输入 TCP 的端口号，UDP 也一样。

说明：

当用户选择的防御病毒，在查看安全防御的列表中可以看到。要是想要取消某一条，可以定义该项目后面的删除按钮。

第六章　　带　外　管　理

7．1　概　述

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

注　意：

由于通过 WEB 方式管理更为直观、方便，因此 **KN-S10-5024GM 交换机**提供了详细的 WEB 管理界面，而 Console 界面只提供了网络配置、文件传输、保存与复位及 Ping 等几项配置。

6．2　带外（out—of-band）的连接方法

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（在交换机的后面板最左边）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 38400 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 38400、“数据位”为 8 位、无“奇偶校验”、“停

止位”为 1、无“数据流控制”。

6．3　带外管理的界面及操作方法

```
                                KN-S10-5024GM SWITCH

                                                ShenZhen Kingnet Electronics Co., Ltd
                                                Copyright 2007, All Rights Reserved.

password:
```

友情提示：该处密码输入没有回显

使用正确的密码成功地登录系统以后，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：

```
switch# ?
[Command List]
?.............. Help commands
backup......... Backup configuration file
cls............ Clear the screen
del............ Del commands
help........... Help commands
logout......... Logout
ping........... Ping a specified host with IP address
reset.......... Reset system or reset factory default setting
set............ Set commands
show........... Show commands
upgrade........ Upgrade configuration file
switch# _
```

图 6-2 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。

【举例】

Switch#set ip

在输入“set ip”之后键入“?”，显示下面的内容：

[Syntax]：set ip [IP ADDRESS] [NETMASK]

提示完整的命令为在ip后输入IP地址和子网掩码。

命令帮助使用说明

在下面所有的命令行帮助信息中，对命令和参数进行了区分，在键入的例子中，用粗体字来表示命令，用一般字体表示参数。

系统对于输入的大小写进行区分，因此对于输入的命令和参数的大小写要严格一致，否则系统会提示错误。

常用命令

help 命令

用户使用help 命令显示系统帮助信息。

【使用指南】 **KN-S10-5024GM** 配置提供随时随地的在线帮助，用户也可以随时键入“？”获取在线帮助。

【举例】

Switch#**help**

[Command List]

?..... Help commands

backup..... Backup configuration file

cls..... Clear the screen

del..... Del commands

help..... Help commands

logout..... Logout

Ping..... Ping a specified host with IP address

reset..... Reset system or reset factory default setting

set..... Set commands

show..... Show commands

upgrade..... Upgrade configuration file

switch#

通过Tftp升级和下载配置文件

用户在当前配置的提示符下键入“**upgrade**”或者“**backup**”，该命令用于配置tftp server 的IP地址，建立和TFTP服务器的连接。

【命令格式】1. upgrade <A.B.C.D> <filename>

2. backup <A.B.C.D> <filename>

【使用指南】1. 通过tftp下载配置文件，下载完后交换机将会自动重启，根据新下载的配置文件的内容重新配置交换机各种功能参数。

2. 通过tftp上传配置文件。

【参数说明】<A.B.C.D>为tftp server 的IP 地址，以点分十进制表示。Filename为所要上传或下载的配置文件名。

【举例】

Switch（config）#**backup** 192.168.1.133　config_1008.dat

（此处显示错误，要做修改）Successfully set TFTP address.

Switch（config）#

cls 命令

用户执行该命令用于清除屏幕显示。

【命令格式】**cls**

【举例】

Switch# **cls**

Switch#

del 命令

用户执行该命令用于清除交换机 flash中的配置文件内容。

【命令格式】**del config**

【举例】

Switch# **del config**

Delete the config file successfully，　Reboot the switch now!

switch#

退出命令***logout***

直接退出当前会话。

【命令格式】logout

【举例】

Switch#**logout**

password：

Ping 命令

该命令等同于DOS下的Ping 命令。

【命令格式】Ping <A.B.C.D>

【参数说明】<A.B.C.D>为点分十进制方式表示的目的IP 地址。

【举例】

Switch#**Ping** 192.168.1.198

Reply from 192.168.1.198：　bytes=32 time<5ms TTL=64

Reply from 192.168.1.198：　bytes=32 time<5ms TTL=64

Reply from 192.168.1.198： bytes=32 time<5ms TTL=64
Switch#

reset 命令

用户执行该命令用于重新启动交换机和恢复交换机出厂设置。

- 【命令格式】reset configuration
  【使用指南】恢复交换机的出厂设置并重启交换机。
  【举例】Switch#**reset configuration**
  Load default factory setting....
  Restore factory successfully， Reboot the switch now!
- 【命令格式】reset system
  【使用指南】重启交换机。
  【举例】Switch#reset system
  Reset system.....

set 命令

用户执行该命令用于设置用户的登录密码、交换机的IP地址、掩码和网关。

- 【命令格式】set pswd
  【使用指南】设置用户的登录密码。
  【举例】Switch#**set pswd**
  old password：
  new password：
  Retype new password：
  Switch#
- 【命令格式】1. set ip <A.B.C.D> <mask>
  2. set gw <A.B.C.D>
  【使用指南】1.设置交换机的IP地址。
  2. 设置交换机的网关。
  【举例】Switch#**set ip** 192.168.1.254 255.255.255.0
  Switch#**set gw** 192.168.1.1
  Switch#show net
  [Network Configuration]
  MAC address ： 00：11：22：33：44：55
  IP address ： 192.168.1.254
  Subnet Mask ： 255.255.255.0

show 命令

用户执行该命令用于显示交换机的系统信息。

- 【命令格式】show version
  【使用指南】显示交换机的生产厂家、交换机的标识、硬件和软件的版本号、。
  【举例】switch# **show version**
  [System Configuration]

Company Name ： KingNet Networks CO. LTD
Switch Name ： KN-S10-5024GM Switch
SoftWare version ： 1.00
Hardware version ： 1.00
Create Date ： 2007-7-30
Switch#

- 【命令格式】show net

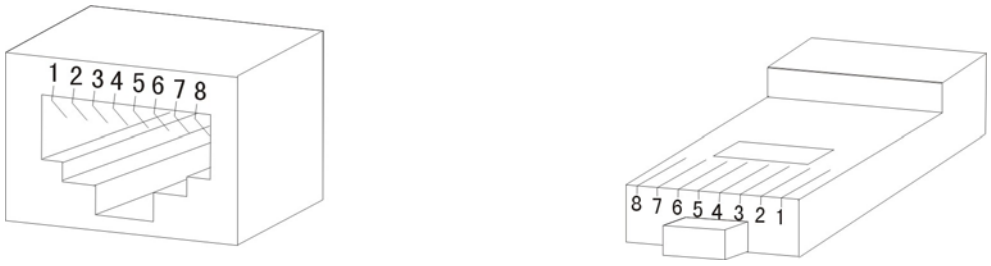
【使用指南】显示交换机的网络信息。

【举例】Switch#show net
[Network Configuration]
MAC address ： 00：11：22：33：44：55
IP address ： 192.168.1.254
Subnet Mask ： 255.255.255.0

附录A RJ-45插座/连接器引脚详细说明

当无自校准功能交换机连接其它的交换机、网桥、集线器时，更改双绞线是必需的。请参照产品手册选择适当的线缆。

下面的图片，就是标准的RJ-45插座/连接器。



图附1 RJ-45插座

2003年6月17日，TIA/EIA委员会正式发布综合布线六类标准（标准号：ANSI/TIA/EIA-568-B.2-1），TIA568B从此真正成为一个能够全面满足目前的网络发展状况，解决网络建设的基础标准集。

5 类线（100M）的制作：

a: 绿白（3）、绿（6）、橙白（1）、蓝（4）、蓝白（5）、橙（2）、棕白（7）、棕（8）

b：橙白（1）、橙（2）、绿白（3）、蓝（4）、蓝白（5）、绿（6）、棕白（7）、棕（8）

常见普通线为：b—b 常见对拷线：a—b（1-3、2-6 交叉）

6 类线的制作（千兆线）：
a：
橙白（1）、橙（2）、绿白（3）、蓝（4）、蓝白（5）、绿（6）、棕白（7）、棕（8）
b:
绿白（3）、绿（6）、橙白（1）、棕白（7）、棕（8）、橙（2）、蓝（4）、蓝白（5）、

常见普通线为：b—b 常见对拷线：a—b（1-3、2-6、4-7、5-8 交叉）—（与 100m 的不同）

附录B 售后技术支持联系方式：

技术支持

支持中心电话：010-62584216
网址：http://www.kingnet.com.cn
E-mail： jinlang@kingnet.com.cn