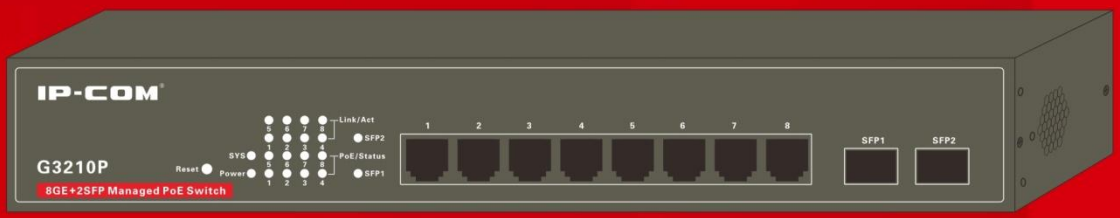
IP-COM®

使用说明书



G3210P

8GE+2SFP 网管型PoE交换机

声明

前言

感谢您购买 IP-COM 产品！阅读此说明书将有助于您配置、管理、维护本产品。

目标读者

本说明书的目标读者为熟悉网络基础知识，了解网络术语的技术人员。

本书约定

本说明书中，所提到的“本交换机”,“本设备”，“交换机”，“设备”，“产品”等名词，如无特别说明，均指 IP-COM 8GE+2SFP 网管型 PoE 交换机 G3210P。

本说明书中的符号格式约定如下：

文字描述	代替符号	举例
按钮	边框+底纹	点击“确定”按钮可简化为点击 确定 。
菜单项	『』	菜单项“系统管理”可简化为『系统管理』。
连续菜单选择	→	进入『PoE 管理』→『端口设置』页面。

本说明书使用的标识和含义如下：

标识	含义
注意	提醒您在操作设备过程中需要注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。
提示	对操作内容的描述进行必要的补充和说明。

内容简介

本说明书各章节内容安排如下：

章节	内容
第 I 部分 产品介绍	介绍交换机的外观、包装及功能特性。
第 II 部分 设备安装	介绍交换机安装注意事项及安装步骤。
第III部分 设备管理入门	介绍如何通过Web网管管理交换机及Web网管的基础操作。
第IV部分 设备管理	介绍通过Web网管设置交换机各功能的具体方法。

章节	内容
第Ⅴ部分 附录	介绍交换机常见问题处理、技术规格、产品有毒有害物质。

相关资料获取方式

您可以登录到 IP-COM 官方网站 www.ip-com.com.cn 获取最新的产品资料。点击『技术支持』→『相关下载』，找到对应的产品即可。

技术支持

网址：http://www.ip-com.com.cn

技术支持邮箱：ip-com@ip-com.com.cn

技术支持热线电话：400-665-0066

目录

第 I 部分

产品介绍

简介

IP-COM 8GE+2SFP 网管型 PoE 交换机 G3210P，提供 8 个 10/100/1000Mbps 自适应 RJ45 端口和 2 个 1000Mbps 独立 SFP 光纤端口。支持 PoE 供电，通过网线连接即可实现数据通信及给受电设备供电，最多可同时接入 8 个 IEEE 802.3af 标准（15.4W）或 4 个 IEEE 802.3at 标准（30W）的受电设备。支持 VLAN、QoS、DHCP 侦听、IGMP snooping、STP/RSTP、端口镜像、链路汇聚等功能，可以通过 Telnet、Web 界面、SNMP 三种方式进行管理。

本交换机针对目前局域网中出现的安全问题，提供了用户分级管理、管理 VLAN 设置、MAC 过滤、802.1x 端口认证等一系列安全特性，通过可视化的 Web 界面简便操作，即可有效防御各种网络攻击。

本交换机广泛应用于酒店、企业等细分行业，为用户提供高性能、低成本、可网管的全千兆安全解决方案。

包装

请小心打开产品包装盒，检查包装盒内应有以下物品：

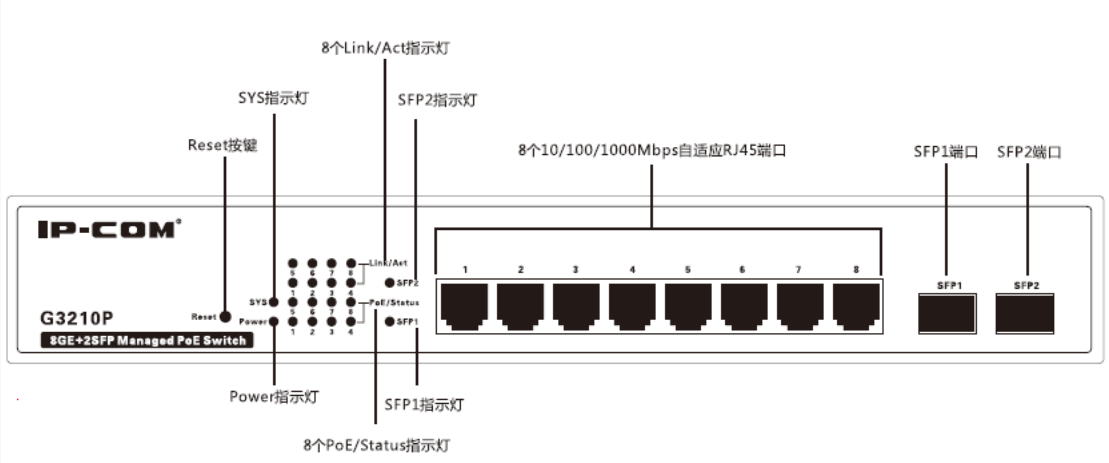
- 交换机*1
- 螺钉*6
- L 型支架*2
- 电源线*1
- 脚垫*4
- 安装手册*1

如果发现有损坏或配件短缺，请持原包装及配件与经销商联系更换。

外观

1 前面板

前面板包括：Reset 按键，指示灯，RJ45 端口，SFP 端口。如下图所示。



➘ Reset 按键

交换机运行正常时，持续按下 Reset 按键至少 5 秒后放开，可将交换机恢复出厂设置。恢复出厂设置后，交换机将自动重启，请等待重启完成（约 45 秒）即可。

重启时，交换机指示灯依次会出现下列现象：所有指示灯亮→SYS 熄灭→Power 保持亮，其它指示灯全熄灭→SYS 亮并闪烁。

➘ 指示灯

各指示灯说明参见下表。

指示灯名称	状态	说明
Power	常亮	交换机供电正常。
	不亮	交换机未通电或出现故障。
SYS	闪烁	系统运行正常。
	常亮	系统运行异常。
	不亮	系统还未启动完成。
Link/Act	常亮	对应的 RJ45 口连接正常。
	闪烁	对应的 RJ45 口正在传输数据。
	不亮	对应的 RJ45 口未连接或连接异常。
PoE/Status	常亮	有受电设备与对应的 RJ45 口连通，并供电正常。
	不亮	无受电设备与对应的 RJ45 口连通或无供电。
SFP1&SFP2	常亮	对应的 SFP 口连接正常或正在传输数据。
	不亮	对应的 SFP 口未连接或连接异常。

➘ RJ45 端口

交换机提供 8 个 10/100/1000Mbps 自适应 RJ45 端口，每个 RJ45 端口对应一个 Link/Act 灯。RJ45 端口各速率和对应的工作模式参见下表。

速率	工作模式
10Mbps（自适应）	半/全双工自动协商
100Mbps（自适应）	半/全双工自动协商
1000Mbps（自适应）	全双工自动协商

所有 RJ45 端口都支持 PoE 供电，兼容 IEEE 802.3af（15.4W）和 IEEE 802.3at（30W），最多可同时接入 8 个 IEEE 802.3af 或 4 个 IEEE 802.3at 标准的受电设备。

提示

PoE 供电采用网线的 1、2，3、6 数据线对供电，网线建议采用 5 类或 5 类以上 UTP/STP，最长供电距离为 100 米。

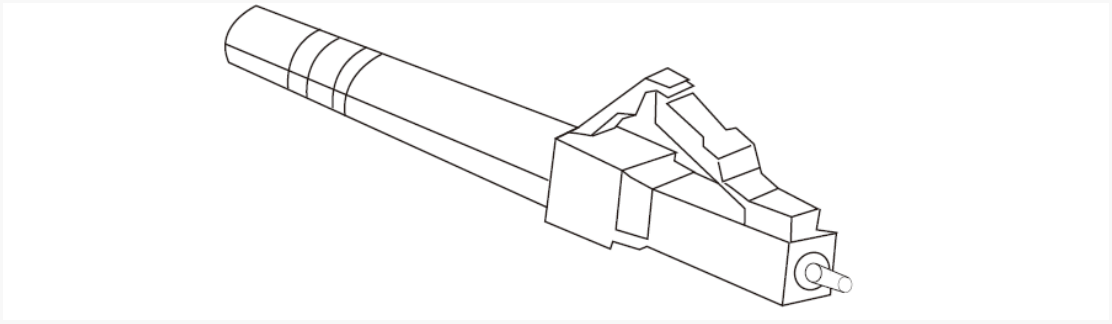
➘ SFP 端口

交换机提供 2 个 1000Mbps SFP 光纤端口，支持千兆 SFP 光模块。

SFP（Small Form-factor Pluggable，小型封装可热插拔）光模块，用于光信号的传输，主要功能是实现光电/电光变换，包括光功率控制、调制发送、信号探测、IV 转换以及限幅放大判决再生功能。

光纤通过光纤连接器连接到 SFP 光模块。光纤连接器（俗称活接头）是光纤通信系统中不可缺少的无源器件，主要用于光通道间的可拆式连接。使用光纤连接器不仅方便了光系统的调测与维护，还使光系统的转接调度更加灵活。

本交换机只支持 LC 型光纤连接器，其外观如下图所示。

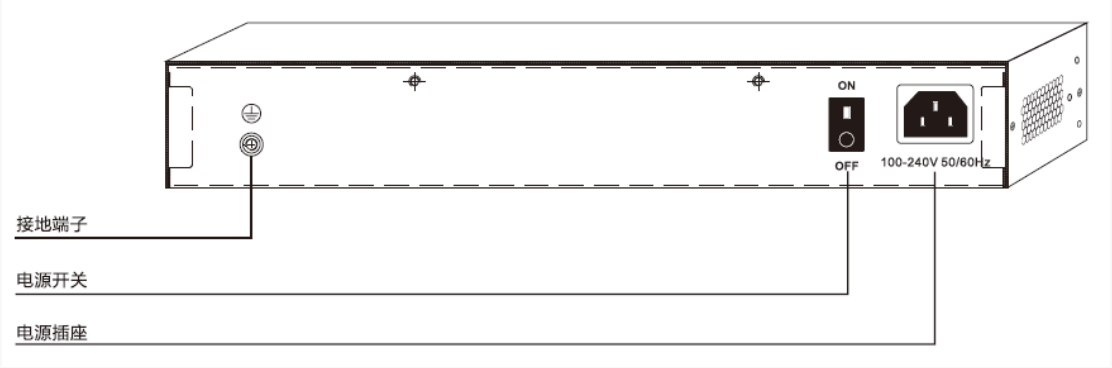


提示

光模块需要用户单独选配，购买本交换机时不随机提供。

2 后面板

后面板有 1 个接地端子，1 个电源开关，1 个电源插座。



➘ 电源开关

用于开启、关闭交换机电源。

➘ 接地端子

用于连接保护地线，以防雷击。连接保护地线的方法请参考连接保护地线。

➘ 电源插座

用于连接电源，给交换机供电。请使用产品包装盒内的配套电源线进行连接。

第 II 部分

设备安装

1 安装注意事项

为避免使用不当造成交换机损坏及人身伤害，请遵从以下注意事项。

➘ 安全措施

- 安装过程中，需佩戴防静电手套，且交换机电源应保持为关闭状态；
- 使用产品包装盒内的电源线给交换机供电；
- 确保输入电压范围与交换机上标明的输入电压范围相符；
- 确保交换机散热孔通风良好；
- 不要打开或拆卸交换机机壳；
- 清洁交换机时，请切断电源。请勿使用任何液体擦洗交换机；
- 交换机远离电力线、电灯、电网附近或任何有可能接触强电电网的地方。

⚠ 注意

交换机机壳的一个安装螺钉上封有 IP-COM 公司的防拆封条，代理商对交换机进行维护时，要求所维护交换机的封条保持完好。如果用户需要打开交换机机壳，请先与本地代理商联系，获得允许；否则，由于擅自操作导致交换机无法维护，将由用户本人负责。

➘ 安装环境要求

1．温/湿度要求

交换机对温度和湿度的要求见下表。

环境描述	温度	湿度
工作环境	-10° C ~ 45° C	10% ~ 90%RH（无凝结）
存储环境	-40℃ ~ 70℃	5% ~ 90% RH（无凝结）

2．洁净度要求

为避免静电影响设备正常工作，请注意：

- 保持室内空气清洁，交换机需要定期除尘；
- 交换机接地良好，确保静电顺利转移。

3．防雷要求

为避免雷电产生的强大瞬间电流破坏交换机，请采取以下防雷措施：

- 确认电源插座、机架、工作台和交换机接地端子均与大地接触良好；
- 合理布线，避免内部感应雷；需要室外布线时，建议使用信号防雷器。

4．安装台要求

无论交换机安装在机架内或其他工作台上，请注意以下事项：

- 确认机架或工作台够平稳、牢固；
- 保持良好的通风，交换机四周留出 10 厘米的散热空间；
- 不要在交换机上放置重物；
- 需要叠放使用时，设备之间的垂直距离不能小于 1.5 厘米。

2 准备安装工具

安装交换机过程中，会用到以下安装工具，请自备。

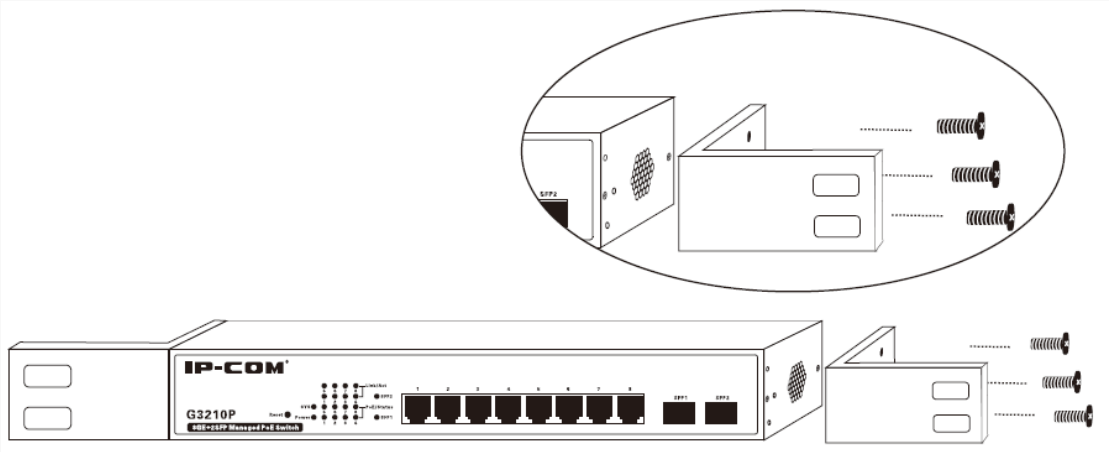
3 安装设备主机

请根据您的安装环境，选择最适合的设备安装方式。

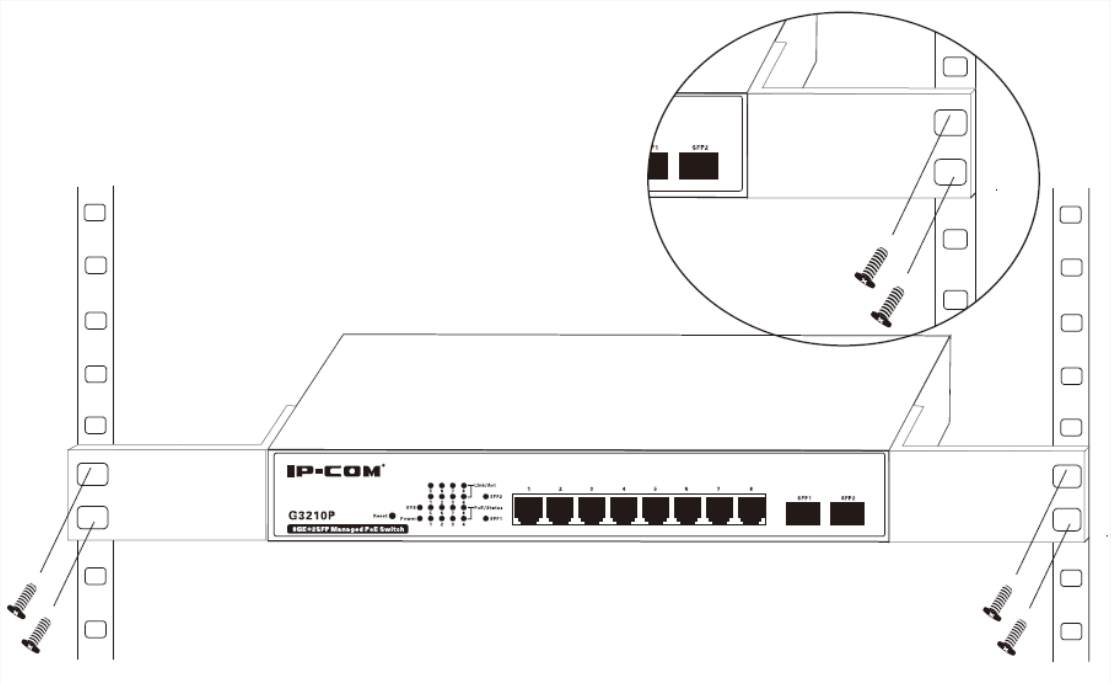
➘ 机架安装方式

交换机配备了 L 型支架和螺钉，可支持标准 19 英寸机架安装。

1. 检查机架的接地与平稳性；
2. 使用配件中提供的螺钉将两个 L 型支架分别固定安装在交换机的两侧；



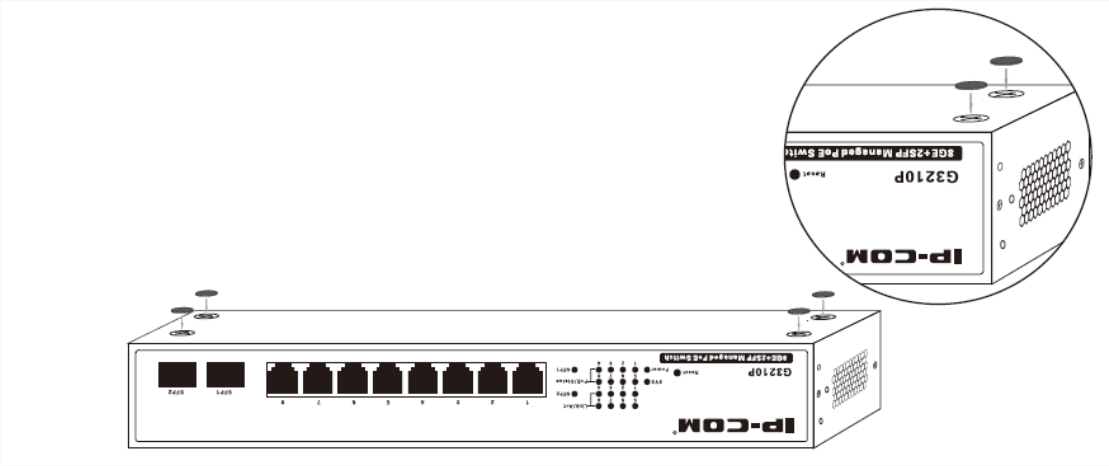
3. 使用螺钉（需用户自备）将安装好 L 型支架的交换机安装在机架上。



➘ 桌面安装方式

如果用户不具备 19 英寸标准机柜，可采用桌面安装方式。

1. 将交换机底部朝上放置于足够大且平稳的桌面上；
2. 将 4 个脚垫粘贴在机壳底部四角对应的圆形凹槽中；



3. 翻转交换机，让其正面朝上放置于桌面即可。

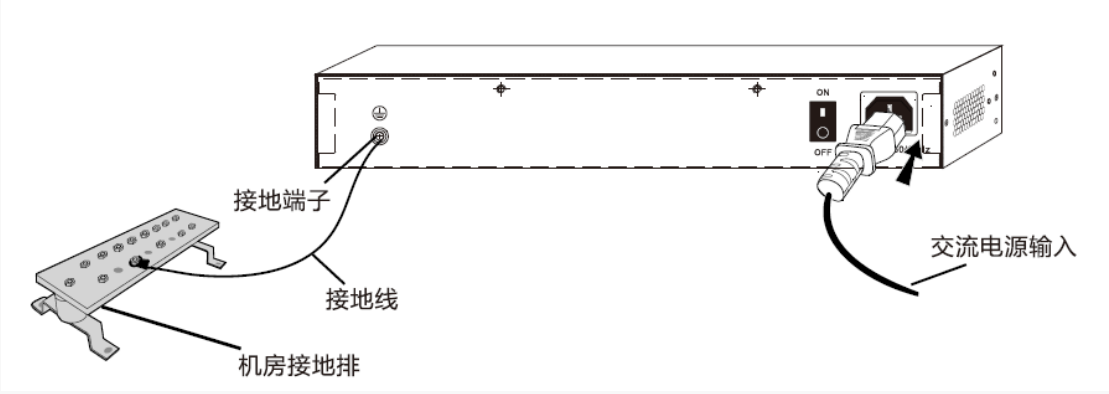
4 连接保护地线

连接保护地线不仅是为了尽快释放掉交换机因雷击而感应的过电压和过电流，也是保障人身安全的必要措施。请根据您的安装环境，选择最适合的连接保护地线的方式。

➘ 安装环境中有接地排

1. 将接地线的一端接到机房工程接地排的接线柱；

2 将接地线的另一端接到交换机接地端子，拧紧固定螺母。



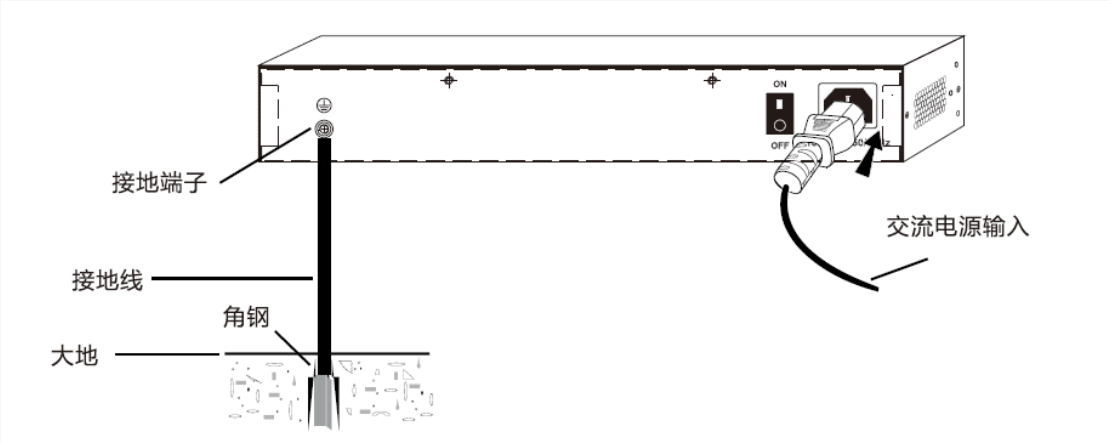
➘ 安装环境中无接地排

如果附近有泥地并且允许埋设接地体，可按以下步骤进行接地安装：

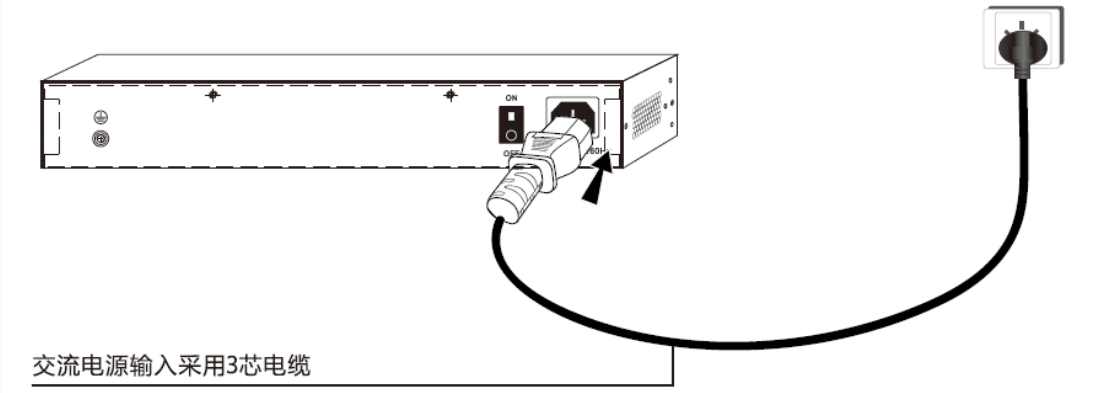
1 将长度不小于0.5米的角钢（或钢管）打入地下；

2 采用电焊连接接地线的一端和角钢(或钢管)，并将焊接点做防腐处理；

3 将接地线另外一端接到交换机的接地端子。

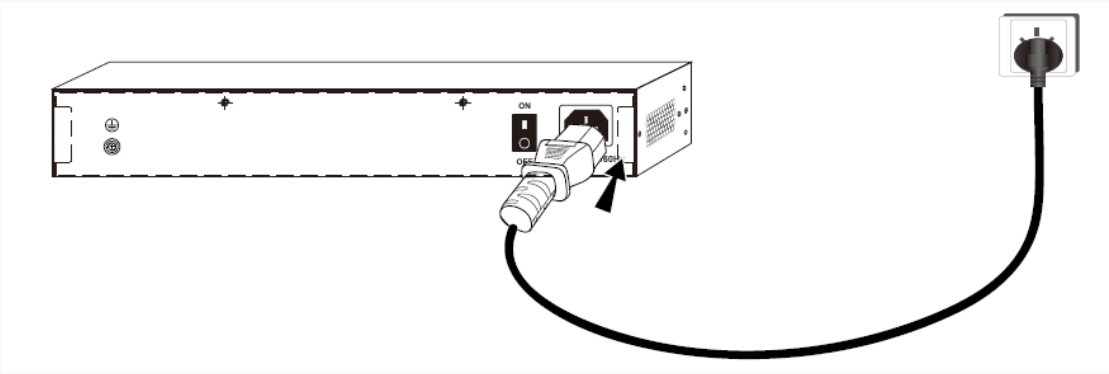


如果不允许埋设接地体，可直接通过电源线进行接地。但前提是：交换机的电源线采用带保护地线的三芯电缆，且交流电源的保护地线已在配电室或交流供电变压器侧良好接地。



5 连接设备电源

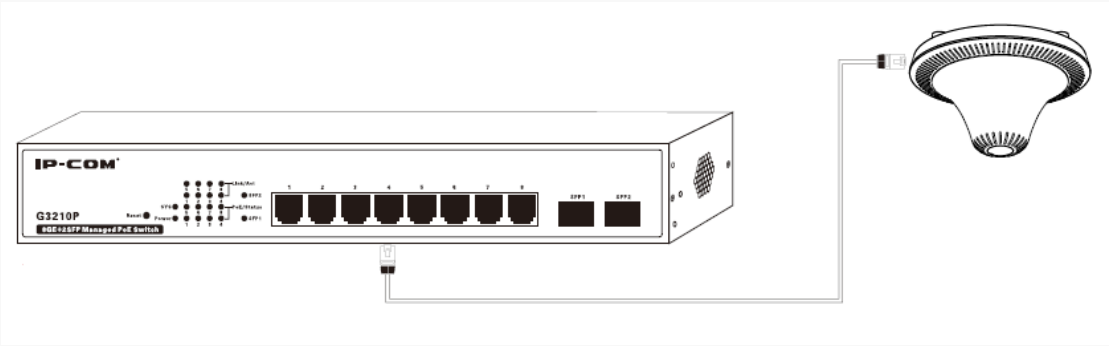
使用产品包装盒内配套的电源线连接交换机和电源插座。



6 连接接口线缆

➘ 连接自适应 RJ45 端口

用网线连接交换机和对端网络设备的 RJ45 端口。

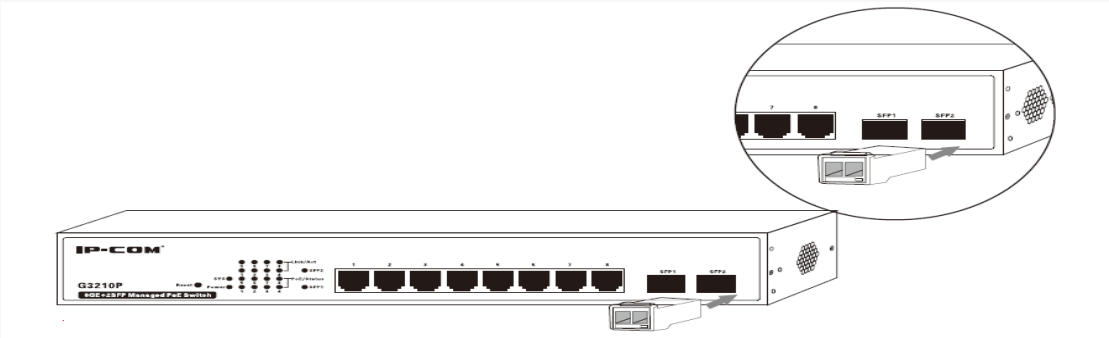


提示

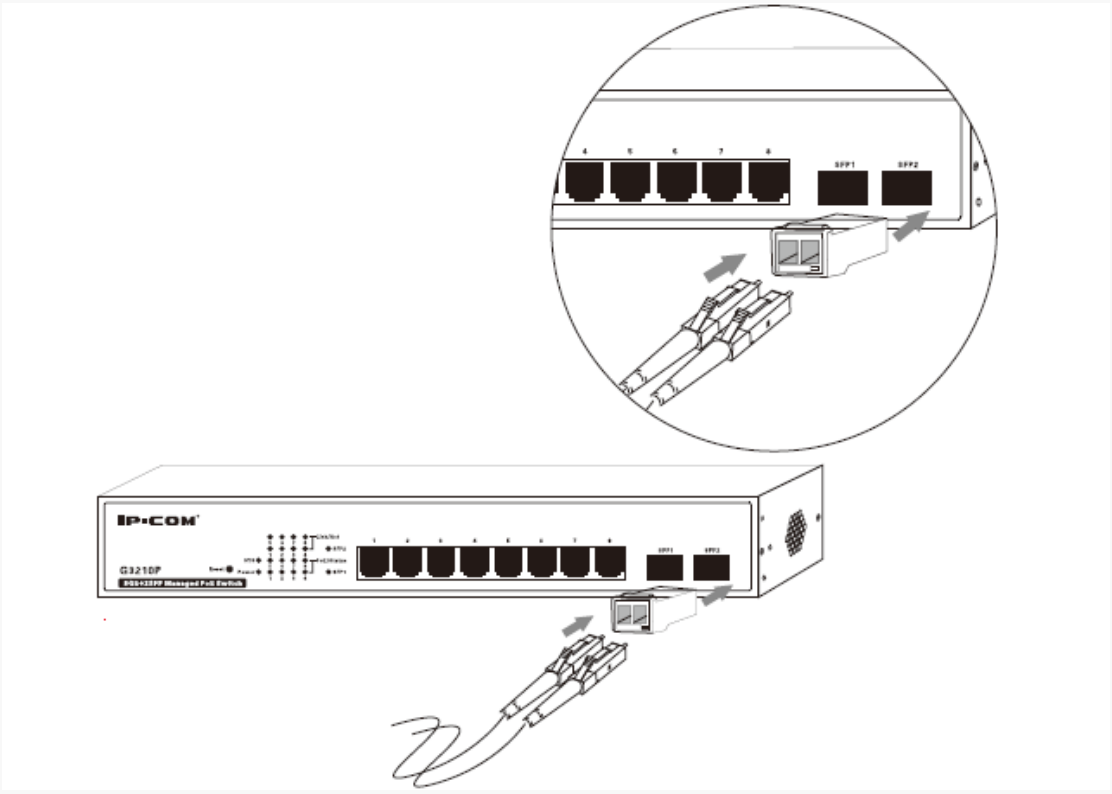
建议采用 5 类或 5 类以上双绞线连接到对端网络设备。因交换机的每个 RJ45 端口均支持 MDI/MDIX 自适应，故双绞线无需区分平行线或交叉线。

➘ 连接 SFP 光纤端口

1. 将 SFP 光模块不带拉手的那一头对准交换机的 SFP 端口，确认好光模块插入时的上下方位后，再将光模块插入 SFP 端口；

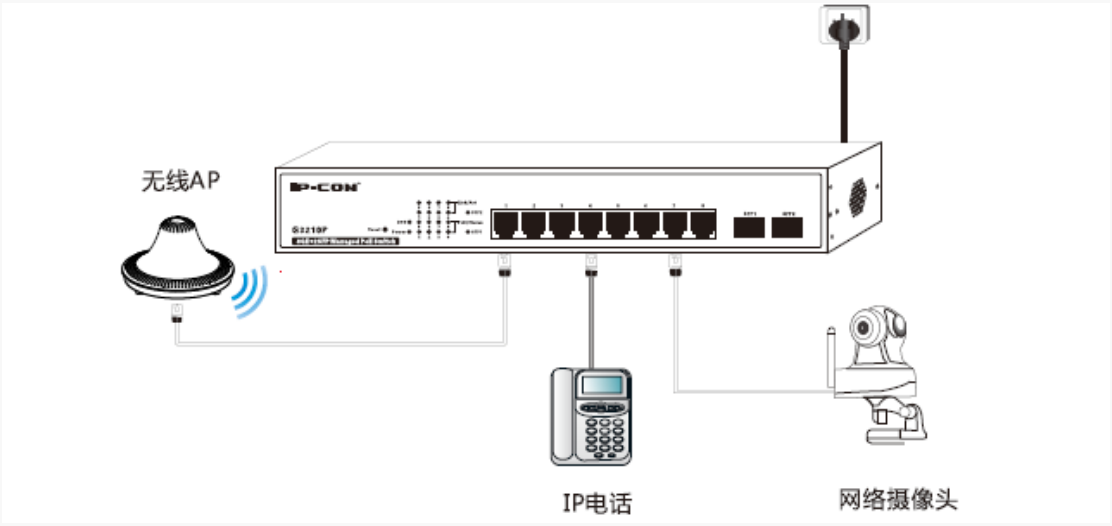


2 将光纤一端的 LC 型光纤连接器插入 SFP 光模块。



➘ 连接受电设备

默认情况下，交换机所有 RJ45 端口均已开启 PoE 供电功能，可对符合 IEEE 802.3at、IEEE 802.3af 标准的 AP、IP 电话和网络摄像头等受电设备进行供电。



提示

交换机 PoE 供电模式为动态供电。即，交换机自动给受电设备提供所需功率的 PoE 电源。

7 设备上电启动

请完成上电前检查后，再给设备上电。

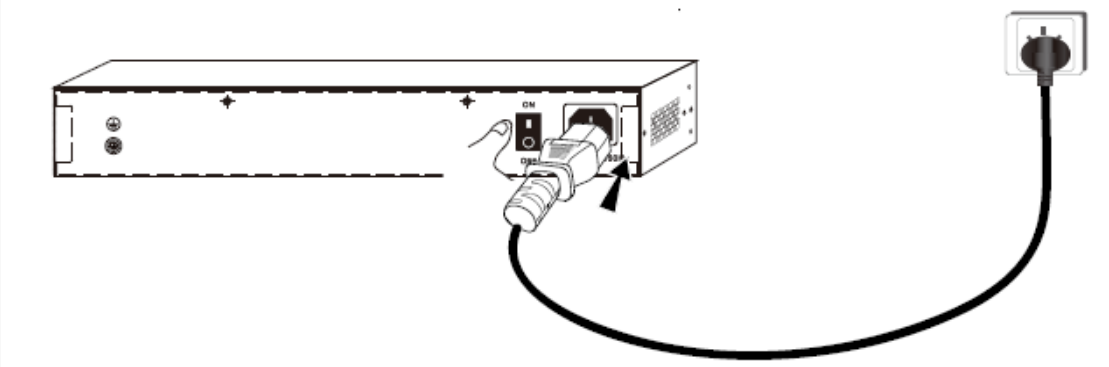
➘ 上电前检查

以上安装完成后，在上电之前，请对交换机进行如下检查：

- 供电电源电压是否与交换机要求一致；
- 电源线和地线连接是否正确；
- 各接口（RJ45 口、SFP 口）连线是否准确；
- 接口线缆是否都在室内走线，若有户外走线情况，请检查是否进行了网口防雷器和交流电源避雷器的连接。

➘ 给设备上电

1. 按下交换机后面板上的电源开关，给交换机上电。



2. 上电后，交换机将自动进行初始化，检查指示灯，应依次出现下列现象：

- 指示灯（Power、SYS、PoE/Status、Link/Act、SFP1、SFP2）全亮进行自检；
- SYS 熄灭；
- Power 保持亮，其它指示灯全部熄灭；

启动完成后，Power 灯亮，SYS 灯闪烁，对应已连接的接口指示灯（Link/Act、SFP1、SFP2）亮或闪烁，对应已连接受电设备的 RJ45 口 PoE/Status 灯亮。

第Ⅲ部分

设备管理入门

1 Web 网管概述

为了方便网络管理员对交换机进行操作和维护，本交换机提供了 Web 网管功能。管理员可以使用 Web 页面直观地管理和维护交换机。Web 网管的运行环境如下图所示。

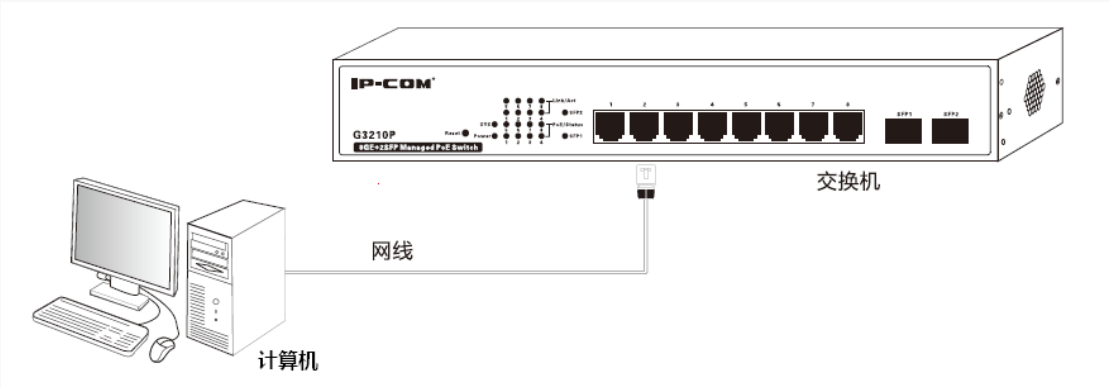
2 登录 Web 网管

首次使用交换机时，您可以直接使用默认登录信息通过浏览器登录到交换机的 Web 网管页面。交换机默认的 Web 登录信息包括：

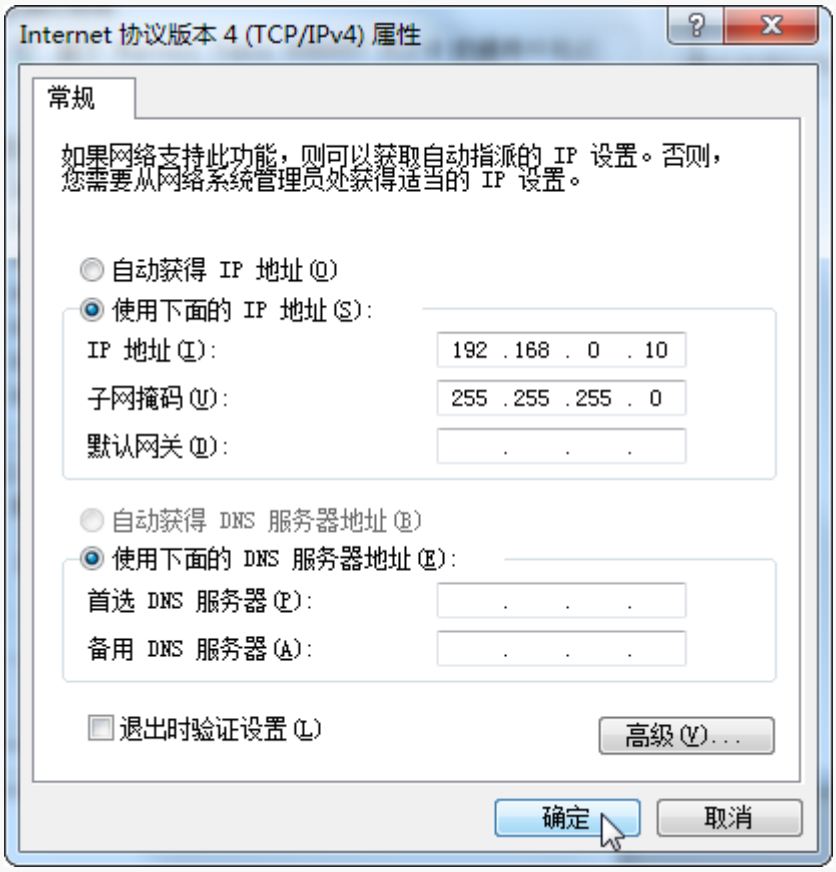
登录信息	默认设置
用户名	admin
密码	admin
IP 地址	192.168.0.1

登录 Web 网管：

1. 用网线连接计算机和交换机的 RJ45 端口；



2. 将计算机的 IP 地址设置为和交换机的 IP 在同一网段的不同 IP 地址。交换机的默认 IP 为 192.168.0.1，所以计算机的 IP 设置为 192.168.0.X（X 为 2~254），子网掩码为 255.255.255.0；



3 打开计算机上的浏览器，在地址栏输入交换机的 IP（192.168.0.1）后，敲回车；

4 进入交换机的 Web 网管登录页面，用户名和密码均输入 admin 后，点击 登录 ；

5 进入交换机的 Web 网管页面。

登录到 Web 网管后，您可查看、更改交换机配置信息。具体功能设置请参考第Ⅳ部分 设备管理的具体章节。

3 退出 Web 网管

直接关闭浏览器窗口或点击浏览器左侧菜单栏的 退出 ，即可退出 Web 网管。退出 Web 网管时，系统不会自动保存当前配置。因此，建议用户在退出 Web 网管前先保存当前配置。

注意

仅关闭浏览器选项卡时，已登录到交换机上的用户并不能自动退出登录。

4 Web 网管页面布局介绍

Web 网管页面共分为：一级&二级导航栏、三级导航栏和配置区三部分，如下图所示。

注意

- 交换机不支持的 Web 网管功能不会显示在 Web 网管导航区，请以交换机软件的实际情况为准。
- Web 网管页面上显示为灰色的功能或参数，表示交换机不支持或在当前配置下不可修改。

序号	名称	说明
1	一&二级导航栏	导航栏以导航树的形式组织交换机的 Web 网管功能菜单。用户在导航栏中可以方便地选择功能菜单，选择结果显示在配置区。
2	三级导航栏	
3	配置区	用户进行配置和查看的区域。

5 Web 网管页面常用元素

端口图示状态介绍：

常用元素	说明
	表示该端口为 RJ45 口。
	表示该端口为 SFP 口。
	表示该端口已连接。
	表示该端口可以被选中并进行配置。
	表示该端口已被选中。
	表示该端口不可被选中和配置。

常用按钮功能介绍：

常用元素	说明
刷新	用于刷新当前页面显示内容。
添加	用于添加一条新的规则。
新建	用于添加一条新的规则。
配置	用于批量修改某一功能设置。
返回	用于取消当前页面配置内容并返回到上一页面。
全部删除	用于删除页面所有规则。
批量删除	用于删除页面部分选定规则。
查询	用于查找匹配搜索条件的规则。
清零	用于清空当前页面统计信息。
下载	用于导出交换机日志文件。
清除日志	用于清除交换机记录的日志信息。
恢复...	用于将交换机的配置信息恢复到出厂默认值。
重启动...	用于将交换机进行重新启动。
帮助	可点击展开详细的帮助信息。
确定	用于保存当前页面配置内容。交换机重启后，会丢失仅点击 确定 保存的配置。
保存...	用于保存交换机当前所有配置内容。交换机重启后，不会丢失已经点击了 保存... 保存的配置。
备份...	用于导出交换机当前配置文件并将其保存到本地计算机。
恢复...	用于将之前导出的配置文件还原到交换机中。
升级	用于升级交换机软件版本。
浏览...	用于交换机软件升级或配置还原时，选择要加载的文件。

第Ⅳ部分

设备管理

系统管理

本节内容可帮助您查看、配置交换机基本信息，了解交换机系统维护工具的用法。包含以下两部分内容：

系统配置：查看、设置交换机系统信息/时间，将交换机重启/重置/软件升级。

系统安全：保障交换机管理安全，防止配置信息被非管理员修改。

1 系统配置

系统配置包括系统信息、系统时间、恢复缺省配置、重启动、软件升级五个页面。

1.1 系统信息

帮助您了解交换机当前端口连接状态及系统信息，点击『系统管理』进入页面。

以下是对页面各参数的说明：

标题项	说明
端口状态	显示交换机当前各端口的连接状态。 填充为绿色表示该端口已连接；无填充色表示该端口未连接。
软件版本	显示交换机的软件版本以及发布时间。
硬件版本	显示交换机的硬件版本。

MAC 地址	显示交换机的物理地址。
管理 VLAN	交换机的管理 802.1Q VLAN ID，默认值为 1。 更改管理 VLAN（需要先到『VLAN 管理』→『VLAN 配置』页面创建其它的管理 VLAN）后，您需要重新连接计算机到新的管理 VLAN 中的某个成员端口（注意：该端口的 PVID 还必须等于管理 VLAN），才可访问交换机。 **提示** 仅交换机的 VLAN 模式为 802.1Q VLAN 时，才可设置此参数。
系统名称	交换机的名称，默认为 G3210P。 建议您为交换机设置一个特别的名称，方便在通过网络对交换机进行管理时，快速定位该交换机。
DHCP	开启/关闭交换机的 DHCP 客户端功能。 **开启：**交换机将从 DHCP 服务器自动获取(管理)IP 地址、子网掩码和网关，您可查看 DHCP 服务器的客户端列表获得交换机的 IP 地址，并使用该 IP 通过 Http 或 Telnet 方式登录到交换机。 **关闭：**由管理员手动设置交换机的 IP 地址、子网掩码和网关。
IP 地址	查看、修改（关闭 DHCP 时）交换机的 IP 地址。默认值为 192.168.0.1。 该 IP 也是交换机的管理 IP 地址，可使用该 IP 通过 Http 或 Telnet 方式登录到交换机。
子网掩码	查看、修改（关闭 DHCP 时）交换机 IP 地址的子网掩码，默认值为 255.255.255.0。
网关	查看、设置（关闭 DHCP 时）交换机的默认网关地址。
MAC 地址表项老化时间	交换机动态 MAC 地址的老化时间，取值范围<10~1000000>，单位为秒，默认值为 300。为 0 时，表示 MAC 地址不老化。 **提示** 本交换机为每个 VLAN 维护一个独立的 MAC 地址（转发）表。

1.2 系统时间

显示、设置交换机的系统时间。本交换机支持两种时间设置方法：

➘ 通过 SNTP 服务器获取系统时间

SNTP，简单网络时间协议，是一种用来同步因特网中计算机时钟的协议。SNTP 采用客户端/

服务器工作方式，客户机通过定期访问服务器提供的时间服务获得准确的时间信息，并调整自己的系统时钟，达到与网络时间同步的目的。

注意

使用 SNTP 服务器获取系统时间时，您首先需要保证交换机已联网成功。方法：进入『系统管理』→『系统配置』→『系统信息』页面正确设置交换机的 IP 地址、子网掩码、网关。

手动设置系统时间

由管理员手动设置的交换机的系统时间。

系统时间设置步骤：

点击『系统管理』→『系统配置』→『系统时间』进入页面。

通过 SNTP 服务器获取时间设置步骤：

1. 在“时区”下拉列表中选择交换机所在的时区；
2. 选择“服务器设置”；
3. 在“首选/备用 SNTP 服务器”输入正确的 SNTP 服务器 IP 地址；
4. 输入自动更新间隔时间，设置后交换机将每隔相应时间跟 SNTP 服务器进行同步，范围可设置为 30~99999 秒，默认 30 秒；
5. 点击 确定 。

手动设置系统时间步骤：

1. 在“时区”下拉列表中选择交换机所在的时区；
2. 选择“手动配置日期和时间”；
3. 手动设置正确的日期和时间；
4. 点击 确定 。

时间设置完成后，可查看页面上的“当前时间”，判断时间设置是否成功。

1.3 恢复缺省配置

如果您需要进入交换机 Web 页面，但却忘记了登录信息（用户名/密码、IP、管理 VLAN 等）；或您上网遇到问题，却找不到问题所在。此时，建议您将交换机恢复出厂设置后重新设置。

本交换机支持硬件和软件两种恢复出厂设置的方法。

硬件恢复出厂设置步骤：

1. 交换机正常运行的情况下，持续按住交换机机身上的 Reset 按键至少 5 秒后放开；
2. 等待约 45 秒钟即可。

软件恢复出厂设置步骤：

1. 登录到交换机 Web 网管；
2. 进入『系统管理』→『系统配置』→『恢复缺省配置』页面；
3. 点击 恢复... ，之后按页面提示操作即可。

提示

恢复出厂设置后，交换机的管理 VLAN 为“1”，登录 IP 地址为“192.168.0.1”，登录用户名和登录密码均为“admin”。

1.4 重启动

重启交换机可释放交换机的部分缓存，为交换机始终保持高性能运行提供保障。某些时候，重启还能解决一些如死锁、登录不了交换机 Web 网管等问题。点击『系统管理』→『系统配置』→『重启动』进入页面。

注意

- 重启后，将丢失仅点击 确定 保存的配置。如果您希望重启后不丢失当前配置（即重启前后所有配置保持一致），请在重启前，首先进入『保存配置』页面，点击 保存... 。
- 断电后重新上电、恢复出厂设置、软件升级等操作都会使交换机重启。

1.5 软件升级

您可登陆到 IP-COM 官方网站 www.ip-com.com.cn，下载本交换机更高版本的软件进行升级，

以获得更多增值功能及更加稳定的性能。

注意

升级过程中，请勿断开交换机电源，否则可能造成交换机损坏！若是突发断电，请重新进行升级；若突发断电后无法进入 Web 网管页面，请联系售后维修。

升级步骤：

1. 登陆到 www.ip-com.com.cn，下载本交换机更高版本的升级文件到本地计算机；
2. 点击『系统管理』→『系统配置』→『软件升级』进入软件升级页面；

3. 点击 浏览 ，从本地计算机选择要加载的升级文件；
4. 点击 升级 后，确认页面提示信息；
5. 等待（约 1.5~2 分钟）出现以下页面后，交换机升级成功。

2 系统安全

管理用户对交换机的访问，点击『系统管理』→『系统安全』进入页面。

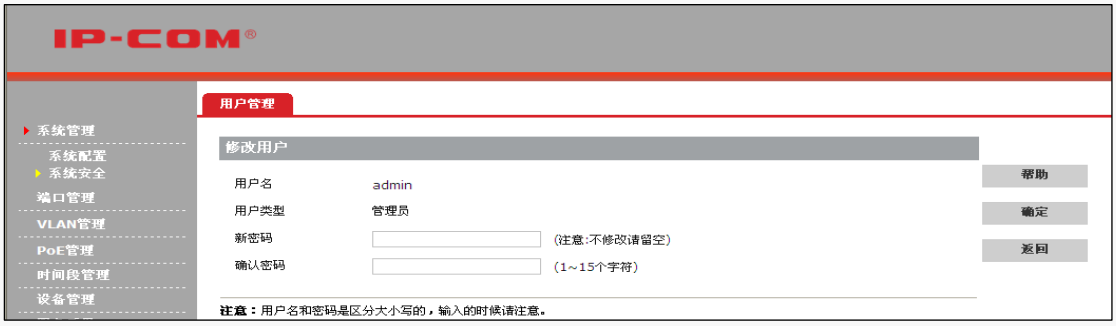
以下是对页面各参数的说明：

标题项	说明
登录超时时间	用户登录到交换机 Web 网管后，如果闲置超过登录超时所设置的时间，将自动退出登录。 登录超时时间取值范围<30~3600>，单位秒。默认值为 300 秒。
用户名	使用 http（Web 网管）、telnet 登录到交换机的用户名。
用户类别	定义用户操作交换机管理系统的权限。 **管理员：**拥有完全管理交换机的权限，用户数量上限为 1 个。默认已存在管理员用户 admin，不可添加、删除管理员用户，也不能修改管理员用户的用户名，但可修改其登录密码。 **操作员：**除“软件升级”，“用户管理”，“恢复出厂设置”和“重启”功能以外，操作员拥有与管理员同样的管理权限，用户数量上限为 5 个。 **普通用户：**可以查看交换机的当前配置，但没有管理的权限，用户数量上限为 10 个。
Telnet	开启/关闭 Telnet 管理功能。 开启后，用户可通过 Telnet 命令登录到交换机管理系统。默认为开启。

修改 admin 用户密码步骤：

1. 点击用户名“admin”；

2. 按页面提示规则输入新密码；
3. 再次输入新密码；
4. 点击 确定 。

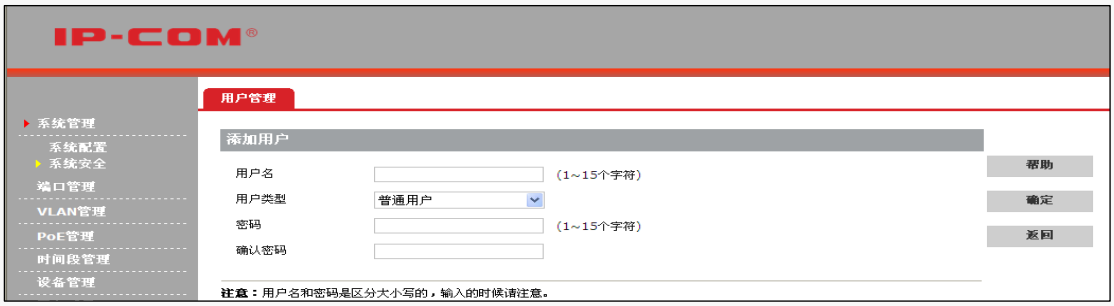


密码修改后，再次登录交换机管理系统时，请使用新的密码。若忘记密码，可持续按住交换机机身上的 Reset 按键 5 秒以上后放开，将密码恢复到出厂设置（admin）。

添加非管理员权限的用户步骤：

1. 点击 添加 ；

2. 按页面提示规则输入用户名；
3. 选择用户类型为“操作员”或“普通用户”；
4. 按页面提示规则输入该用户的密码；
5. 再次输入密码；
6. 点击 确定 。



端口管理

本节内容可帮助您管理交换机的各个端口，了解各端口数据转发情况。包含以下两部分内容：

端口配置：配置交换机端口的基本属性、端口镜像，查看端口数据转发统计信息。

链路汇聚：增加交换机链路带宽，实现链路传输弹性和备份。

1 端口配置

端口配置包括端口设置、端口镜像、端口统计三个页面。

1.1 端口设置

设置交换机各个端口的属性，点击『端口管理』→『端口配置』→『端口设置』进入页面。

以下是对页面各参数的说明：

标题项	说明
链接状态	显示端口的实际工作速率和模式，若未连接或链接失败显示为“--”。
速率/双工	RJ45 端口支持 10M、100M、1000M 三种速率，10M、100M 支持半双工（HDX）和全双工（FDX）；1000M 时，仅支持全双工。SFP 端口仅支持 1000M 全双工。 您可根据以下说明选择端口的双工模式： • 如果您希望端口可同时发送和接收报文，请将端口设置为全双工。 • 如果您希望端口同一时刻只能发送或接收报文，请将端口设置为半双工。 • 如果您希望端口的双工状态由本端口和对端端口自动协商而定，请将端口设置为自协商。 默认情况下，端口的速率和双工模式均为自协商。

流控	端口链路协商为全双工模式，且本交换机与对端设备都开启流控功能后，如果本交换机某端口发生拥塞，该端口将向对端发送流控（Pause）帧，对端收到流控帧后，将暂停对本交换机发送数据；同时，当本交换机的某端口接收到 Pause 帧后，也会暂停该端口对外发送数据。 默认情况下，端口流控处于关闭状态。 **注意** • 本交换机不支持半双工流控； • 开启全双工流控可以避免数据丢失，但同时也会影响数据源端口与其他设备的通信速率，连接 Internet 的端口请慎用此功能。
开启/关闭	开启/关闭端口。默认情况下，端口处于开启状态。如果关闭某端口，则该端口将 Link Down，不转发任何数据。
隔离	开启/关闭端口隔离。 只有在 802.1Q VLAN 模式下才可设置该项。您可以将需要进行控制的端口加入到一个隔离组中，实现隔离组中端口之间的数据隔离。 端口隔离既增强了网络的安全性，也为用户提供了灵活的组网方案。默认情况下，端口关闭隔离。 **注意** • 只有隔离组内各个端口之间的数据不能互通，隔离组内端口与隔离组外端口的通信不会受到影响。 • 当汇聚组中的某个端口加入或离开隔离组时，该汇聚组中的其它端口均会自动加入或离开该隔离组。 • 当汇聚组中的某个端口离开汇聚组时，该汇聚组中的其它端口仍将处于隔离组中，即该汇聚组中端口的隔离属性不受影响。 • 当未隔离端口加入到已隔离的汇聚组时，该端口会自动加入隔离组。
Jumbo 帧	设置交换机接收到 Jumbo 帧大小，取值范围<1518~9216>。默认情况下，帧大小为 1518，为 IEEE 802.3 和以太网标准规定的最大帧长。 设置了 Jumbo 帧长后，当端口收到该长度以内的数据，系统会继续处理。

设置某一个端口的属性：请点击页面上该端口对应的表项，进入页面设置即可。

批量设置端口的属性：请点击页面上的 配置 ，进入页面设置即可。

1.2 端口镜像

端口镜像：将镜像源端口的报文复制一份到镜像目的端口。镜像目的端口连接了数据监测设备，用户利用数据监测设备来分析复制到镜像目的端口的报文，进行网络监控和故障排除。

本交换机支持本地端口镜像功能，即，镜像源端口和镜像目的端口在同一台设备上。点击『端口管理』→『端口配置』→『端口镜像』进入设置页面。

以下是对各页面参数的说明：

字段	含义
镜像端口	选择镜像目的端口，不镜像表示禁用端口镜像功能。 **注意** • 某端口被设为镜像目的端口后，不能再设置为镜像源端口。 • 仅当您设置了镜像目的端口后，才能设置镜像源端口。 • 已加入某个汇聚组的端口不允许设置为镜像目的端口。 • 开启 802.1X 认证、生成树的端口不可设置为镜像目的端口。
镜像方向	选择镜像源端口，不镜像表示该端口不被镜像。 **镜像入端口**：只有该端口接收的数据才被镜像到镜像目的端口。 **镜像出端口**：只有该端口发送的数据才被镜像到镜像目的端口。 **镜像出和入端口**：该端口发送和接收的数据均被镜像到镜像目的端口。 **注意** 当镜像源端口带宽总和大于镜像（目的）端口时将会出现丢包情况。

提示

- 镜像目的端口速率应大于所有源端口速率之和。建议镜像源端口设置为路由端口（即接入 Internet 的端口），实现所有报文的监控。
- 对于同一条数据流，交换机只进行一次复制。例如端口 5 镜像端口 1 的入方向和端口 2 的出方向，对于端口 1 转发到端口 2 的报文，端口 5 只镜像一次。

1.3 端口统计

查看、清零端口统计信息，点击『端口管理』→『端口配置』→『端口统计』进入页面。

如果要查看某一端口的更详细统计信息，点击该端口项，进入页面查看即可。

2 链路汇聚

链路汇聚是将交换机的多个物理端口汇聚在一起形成一个逻辑上的汇聚组，使用链路汇聚服务的上层实体把同一汇聚组内的多条物理链路视为一条逻辑链路。链路汇聚可以实现流量在汇聚组中各个成员端口之间分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。

在同一个汇聚组中，各成员端口必须有一致的配置，这些配置包括 STP、端口优先级、VLAN 配置、端口管理。具体说明如下：

- 加入汇聚组的端口的 STP 配置（包括：STP 状态、P2P 端口、边缘端口、端口优先级、路径开销）、端口优先级配置、端口 VLAN 配置（包括：端口类型、PVID、允许 VLAN、Untag/Tag VLAN）、端口配置（包括：Jumbo 帧、流控、隔离设置）需一致。
- 对于已加入汇聚组的端口，不可进行以下功能设置：添加静态 MAC 地址、设置为镜像目的端口、开启语音 VLAN、开启 802.1X 认证。
- 开启 802.1X 认证、端口镜像（作为镜像目的端口）的端口不能加入汇聚组。

按链路汇聚方式的不同，端口汇聚可分为两类：静态汇聚和 LACP 汇聚。

➘ 静态汇聚

静态汇聚由用户手工配置，不允许系统自动添加或删除汇聚组中的端口。静态汇聚端口的

LACP 协议为关闭状态。

静态汇聚组中的端口状态均为转发状态，建议组中端口速率配置尽量一致。当汇聚组中存在端口速率不一致时，此端口会按照端口实际连接速率转发数据包，此时端口带宽为汇聚端口带宽总和。

➘ LACP 汇聚

基于 IEEE 802.3ad 标准的 LACP 是一种实现链路动态汇聚的协议。LACP 汇聚组中的端口通过 LACPDU 报文自动协商是否成为汇聚端口。LACP 汇聚端口的 LACP 协议为开启状态。

LACP 汇聚组中端口状态分为转发与阻塞状态。已经形成 LACP 汇聚的端口将处于转发状态，否则将处于阻塞状态。如果汇聚组中的端口都未形成汇聚，则只有第一个端口处于转发状态。处于转发状态的端口能收发业务报文和 LACP 协议报文，处于阻塞状态的端口不能收发业务报文，只能收发 LACP 协议报文。

2.1 链路汇聚

点击『端口管理』→『链路汇聚』，进入链路汇聚主页面。

链路汇聚一般有四种物理链路的分配算法。默认情况下，本交换机汇聚组中各成员端口根据源 MAC 地址+目的 MAC 地址进行负荷分担。如图。

以下是对页面各参数的说明：

算法	含义
SA（源 MAC 地址）	汇聚组中各成员端口根据源 MAC 地址进行负荷分担。
DA（目的 MAC 地址）	汇聚组中各成员端口根据目的 MAC 地址进行负荷分担。

源 MAC 地址+目的 MAC 地址	汇聚组中各成员端口根据源 MAC 地址+目的 MAC 地址进行负荷分担。
源 IP 地址+目的 IP 地址	汇聚组中各成员端口根据源 IP 地址+目的 IP 地址进行负荷分担。

添加静态汇聚组步骤：

1. 点击页面的 新建 ；

2. 进入添加链路汇聚组页面，输入有效的汇聚组号（1-2）；
3. 选择“静态”；
4. 选择您要加入汇聚组的端口，最少 2 个端口，最多 8 个端口；
5. 点击 确定 。

提示

在静态汇聚组中的端口，只要链接成功，即可形成汇聚，不受端口速率的影响。

LACP 组添加步骤：

1. 在『端口管理』→『链路汇聚』页面，点击 新建 ；
2. 进入添加链路汇聚组页面，输入有效的汇聚组号（1-2）；
3. 选择“LACP”；

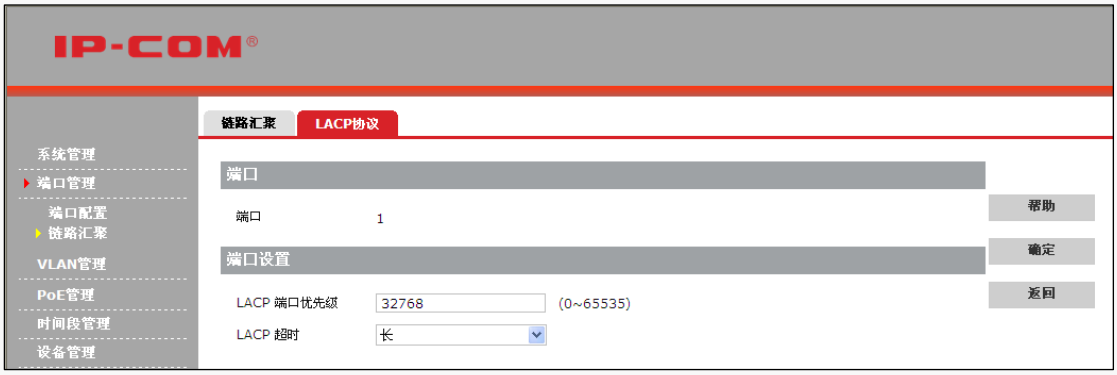
4 选择您要加入汇聚组的端口，最少 2 个端口，最多 8 个端口；

5 点击 确定 。

2.2 LACP 协议

设置系统 LACP 优先级以及端口 LACP 优先级，点击『端口管理』→『链路汇聚』→『LACP 协议』进入页面。

单端口 LACP 参数设置：点击对应端口号，进入页面设置即可。



批量端口 LACP 参数设置：请点击 配置 ，进入页面设置即可。

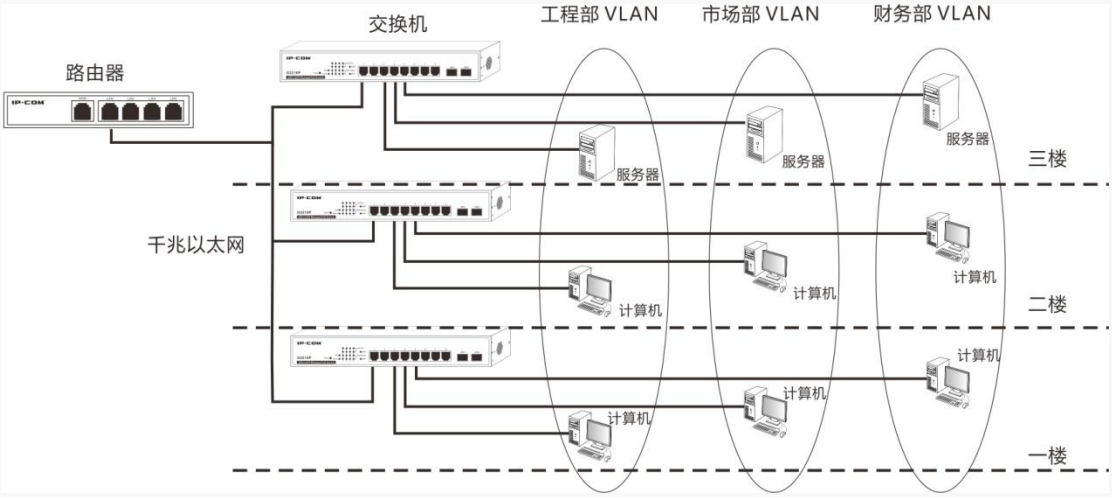
以下是对页面各参数的说明：

标题项	说明
系统优先级	设置交换机系统的优先级，值越小，系统的优先级就越高。 不同系统之间交换信息时，具有较高的优先级的系统可以决定一条链路到底属于哪个汇聚链路，而具有较低优先级的系统则根据对方的选择加入合适的汇聚链路。 系统优先级默认为 32768。取值范围为<0~65535>。
LACP 状态	显示端口是否加入 LACP 汇聚组的状态。 **开启：**端口已加入 LACP 汇聚组。 **关闭：**端口已加入静态汇聚组或者没加入 LACP 汇聚组。
LACP 端口优先级	LACP 端口优先级用于 LACP 汇聚组中的端口选择。 端口优先级值小的端口会被选择为动态汇聚组成员。若端口优先级相同，则端口号小的会被选择为动态汇聚组成员。默认为 32768。
LACP 超时	设置 LACP 超时时间，当 LACP 汇聚组汇聚失败后，将在相应时间内再次发送 LACPDU 报文进行汇聚协商。默认超时设置为“长”。
汇聚组	显示已经形成 LACP 汇聚后的汇聚组号。

VLAN 管理

传统的共享介质以太网和交换式以太网中，所有的用户都在一个广播域。随着网络内计算机数量的增多，广播包的数量也急剧增加，这大大增加了网络中所有设备之间的数据流量，进而影响了网络性能。随着网络的不断扩充，还很可能出现广播风暴，导致整个网络无法使用。

VLAN(Virtual Local Area Network)，是一种将局域网内的设备在逻辑上而不是在物理上划分成一个个网段，从而实现虚拟工作组的数据交换技术。它将一个局域网划分成多个逻辑的局域网-VLAN，VLAN 组内主机位于同一个广播域，它们在任何地理位置都可以像连接在同一个网段上一样正常通信；组间隔绝广播，不同 VLAN 内的主机不能直接通信，必须通过路由器或其它三层包转发设备转发。VLAN 使用示意图如下：



VLAN 有如下优点：

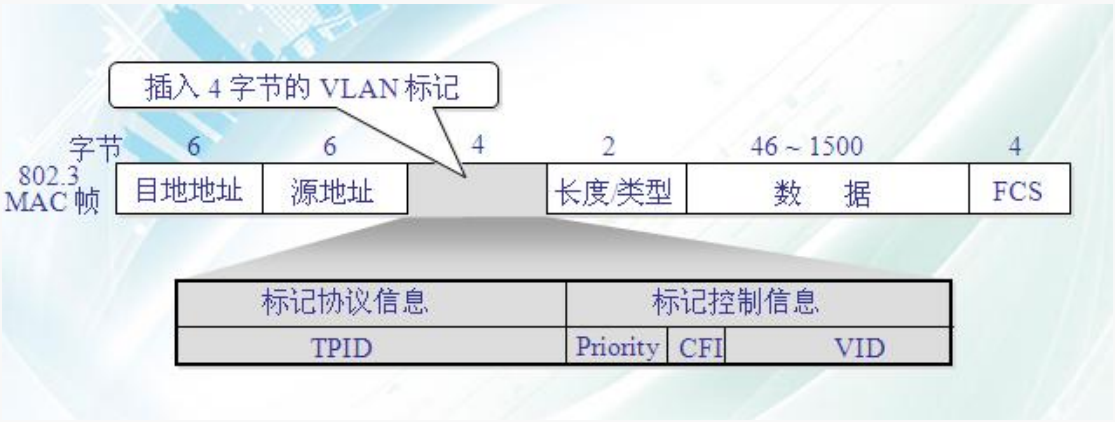
- 提高网络性能。将局域网内的广播包限制在一个 VLAN 内，节省了网络带宽，提高了网络处理能力。
- 减少设备投资。传统通过路由器来隔离广播风暴的方法加大了网络管理成本，VLAN 技术使成本控制成为可能。
- 简化网络管理。使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟局域网范围内移动时，不需要更改网络配置即可正常访问网络。
- 确保网络安全。不同 VLAN 的主机不能直接相互通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发，这加强了企业网络中不同部门之间的安全性。

本交换机支持两种基于端口的 VLAN（802.1Q VLAN，Port VLAN）和一种基于数据流的 VLAN（Voice VLAN），下面将分别对这几种 VLAN 进行详细说明。

1 802.1Q VLAN

IEEE 于 1999 年正式签发了 802.1Q 标准，用于规定 VLAN 的国际标准实现，使得不同厂商设备之间 VLAN 互通成为可能。802.1Q 协议规定在以太网帧的源 MAC 地址之后增加一个 4 字节

的 802.1Q VLAN 标记，用以标识 VLAN 的相关信息。如图所示：



802.1Q 标记中信息解释如下：

字段	说明
TPID	用来标识该数据帧是带有 802.1Q VLAN Tag 的数据帧。该字段长度为两字节，即 16bit，IEEE 802.1Q 协议定义该值为 0x8100。
Priority	用来标识该数据帧的优先级，主要用于当交换机阻塞时，优先发送优先级高的数据包。 该字段长度为 3bit，取值范围为<0~7>，7 为最高优先级，0 为最低优先级。
CFI	用来标识 MAC 地址是否以标准格式进行封装，该字段长度为 1bit。 0 表示 MAC 地址以标准格式进行封装，1 表示以非标准格式封装。对于以太网交换机，默认为 0。
VID	VLAN ID，用来标识报文所属 802.1Q VLAN，该字段长度为 12bit，取值范围为<0~4095>，0 和 4095 通常不使用，所以 VID 取值范围一般为<1~4094>。

➘ 端口的三种链路类型

创建 802.1Q VLAN 时，需要根据端口连接的设备设置该端口链路类型。本交换机支持以下三种端口链路类型：

- Access：端口只能属于 1 个 VLAN，一般用于连接用户终端设备（如计算机）的端口。
- Trunk：端口允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，常用于交换机之间级联的端口。
- Hybrid：端口允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于交换机之间级联，也可以用于连接用户终端设备。

➘ PVID 与 VLAN 数据包处理关系

PVID(Port VLAN ID)，就是端口默认所属 VLAN ID。Access 端口的 PVID 为端口所属 VLAN ID，Trunk 与 Hybrid 端口默认的 PVID 为 1，您也可自定义其 PVID 值。

本交换机不支持进入过滤。只配置了 802.1Q VLAN 时，对于进入端口的 Tag 数据，按数据中

的 VID 转发到相应 VLAN 的其他端口；对于进入端口的 Untag 数据，按该端口的 PVID 转发到相应 VLAN 的其他端口。

各链路类型端口对数据的接收和发送处理方式详见下表：

端口链路类型	接收数据处理		发送数据处理
	接收 Tag 数据	接收 Untag 数据	
Access	按 Tag 中的 VID 转发到相应 VLAN 的其他端口。	按该端口的 PVID 转发到相应 VLAN 的其他端口。	去掉报文的 Tag 再发送。
Trunk			VID = 端口 PVID，去掉 Tag 发送； VID≠ 端口 PVID，保留 Tag 发送。
Hybrid			报文的 VID 值属于 Tagged VLAN，则带 Tag 发送； 报文的 VID 值属于 Untagged VLAN，则去掉 Tag 发送。

➘ 802.1Q VLAN 配置页面说明

本交换机中，IEEE 802.1Q VLAN 配置页面包括 VLAN 切换，802.1Q VLAN，Trunk 端口，Hybrid 端口四个页面：

VLAN 切换：用于 802.1Q VLAN 和端口 VALN 模式切换，两者只能同时存其一。

802.1Q VLAN：用于设置、显示 802.1Q VLAN。

Trunk 端口：用于设置 Trunk 端口。

Hybrid 端口：用于设置 Hybrid 端口。

1.1 VLAN 切换

点击『VLAN 管理』→『VLAN 配置』→『VLAN 切换』进入页面，设置 VLAN 模式为 802.1Q VLAN。

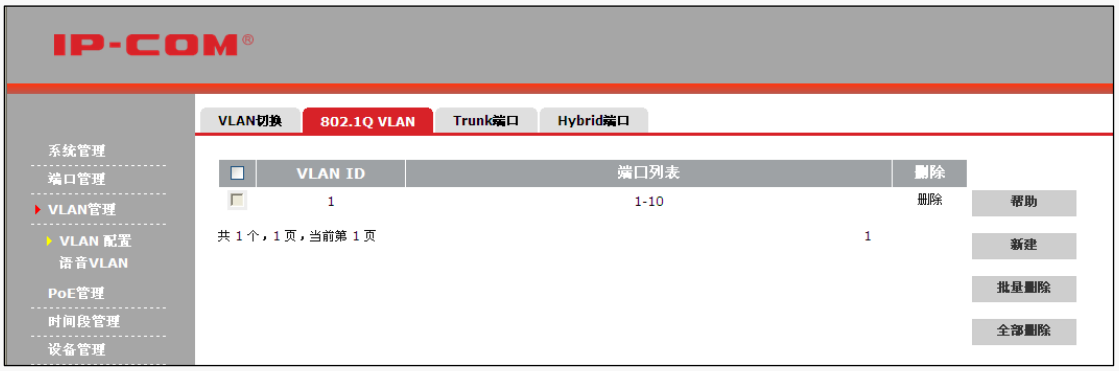
注意

- VLAN 模式由 802.1Q VLAN 切换为端口 VLAN 时，与 802.1Q VLAN 相关的配置都将清空，包括：MAC 过滤、静态 MAC 地址和端口隔离。

- 802.1Q VLAN 切换为端口 VLAN 时，若语音 VLAN 已开启，需先关闭语音 VLAN。

1.2 802.1Q VLAN

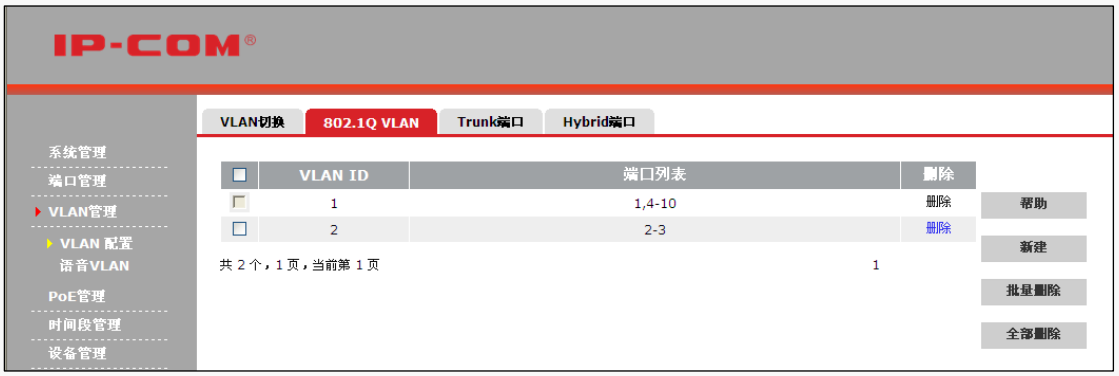
创建 802.1Q VLAN，点击『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』进入页面。



添加 802.1Q VLAN：

1. 点击 新建 ，进入 VLAN 设置页面；
2. 输入 VLAN ID；
3. 选择属于该 VLAN ID 的端口；

4. 点击 确定 ，自动返回到 802.1Q VLAN 显示页面。



提示

- VLAN ID 最大输入(英文)字符长度为 20，输入多个数值时，端口不可选择，点击 确定 后将创建多个空 VLAN。例如输入“2-10”可配置 9 组空 QVLAN，如输入“2，10”，可配置 2 组空 QVLAN。
- 默认全部端口都属于 802.1Q VLAN1，删除 VLAN ID 后该 VLAN ID 包含的端口将自动属于 802.1Q VLAN1。
- 802.1Q VLAN 最多可添加 128 组。

1.3 Trunk 端口

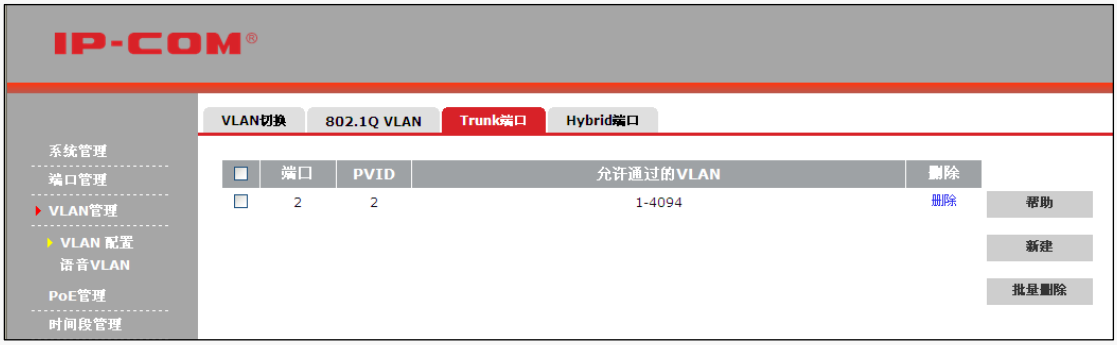
在『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』页面配置的 VLAN 的端口的链路类型默认均为 Access。您可以根据需要修改端口链路类型为 Trunk 或 Hybrid。

点击『VLAN 管理』→『VLAN 配置』→『Trunk 端口』进入 Trunk 端口设置页面。

添加 Trunk 端口：

1. 点击 新建，进入 Trunk 端口配置页面；
2. 输入要设置为 Trunk 端口的端口号；
3. 输入该 Trunk 端口的 PVID，需要对应的 VLAN 已存在；
4. 设置该端口所属的 VLAN，您可以选择“VLAN ALL”或在“VLAN”输入栏输入具体的 VLAN 号；

5. 点击 确定，自动返回到 Trunk 端口显示页面。

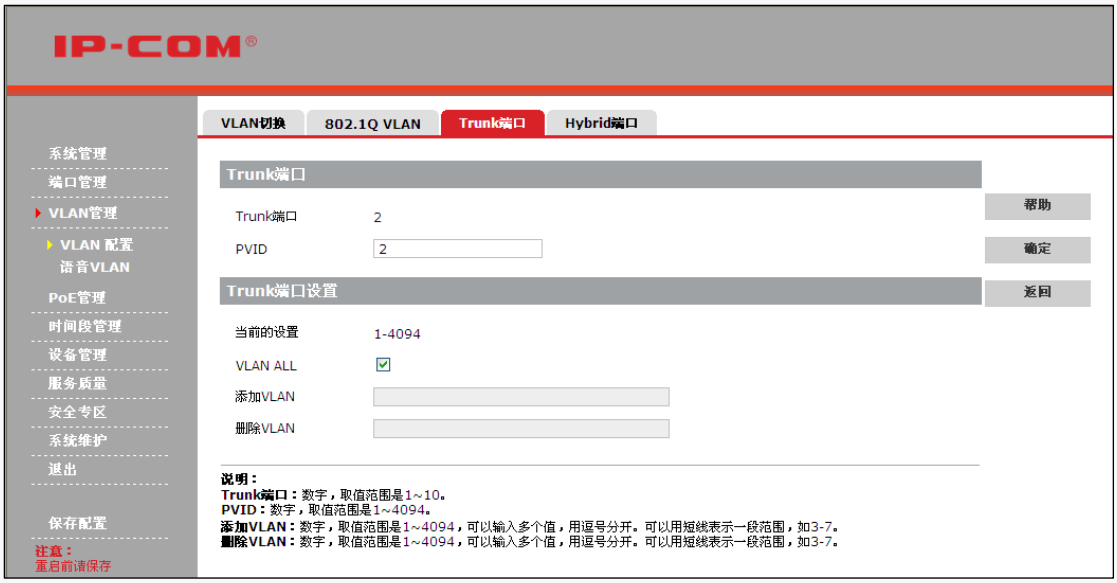


编辑 Trunk 端口：

Trunk 端口添加完成后，如果您还想修改已添加的 Trunk 端口的某些参数值，如 PVID，所属 VLAN 等，请参考如下步骤：

1 在 Trunk 端口显示页面点击相应的 Trunk 端口项；

2 进入页面修改该 Trunk 端口的各项值。



删除 Trunk 端口：

首先，请进入点击『VLAN 管理』→『VLAN 配置』→『Trunk 端口』进入 Trunk 端口显示页面。

删除某个 Trunk 端口：点击对应 Trunk 端口项后的 删除 。

批量删除 Trunk 端口：请勾选您想删除的 Trunk 端口前的“☐”后，点击 批量删除 。

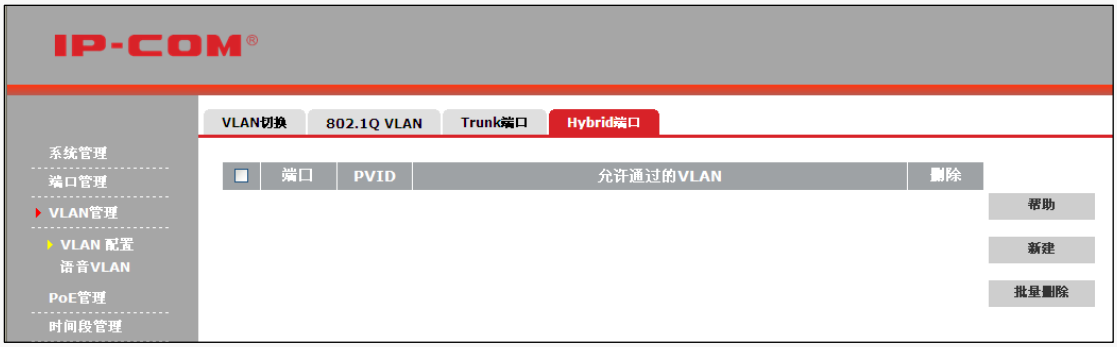
提示

- Hybrid 端口不能再被配置为 Trunk 端口，如需将 Hybrid 端口设置为 Trunk 端口，请先将 Hybrid 端口删除，再配置 Trunk 端口。
- 被删除的 Trunk 端口，将被自动划到 VLAN1 中，端口链路类型改为 Access 端口。

1.4 Hybrid 端口

在『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』页面配置的 VLAN 的端口的链路类型默认均为 Access。您可以根据需要修改端口链路类型为 Trunk 或 Hybrid。

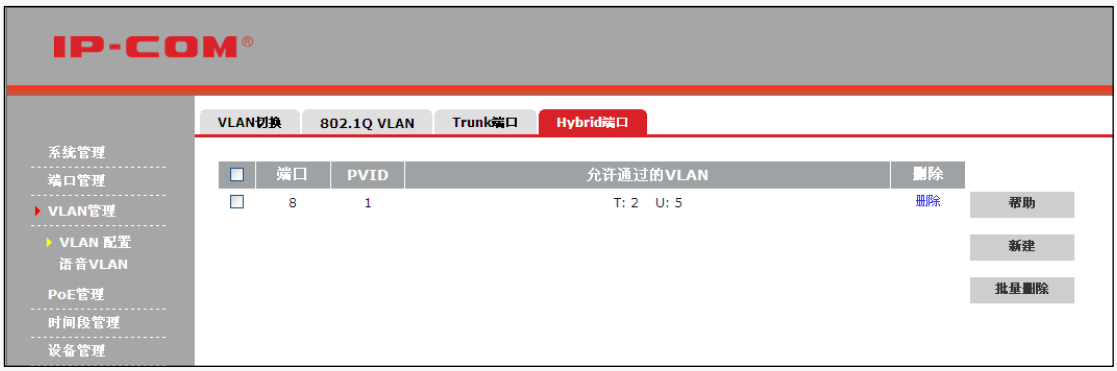
点击『VLAN 管理』→『VLAN 配置』→『Hybrid 端口』进入 Hybrid 端口设置页面。



添加 Hybrid 端口：

1. 点击 新建 ，进入 Hybrid 端口配置页面；
2. 输入要设置为 Hybrid 端口的端口号，范围为 1~10；
3. 输入该 Hybrid 端口的 PVID，前提是对应的 VLAN 已存在；
4. 设置 Tagged VLAN，即发送报文时需要带 Tag 信息的 VLAN，取值为 1~4094 或空；
5. 设置 Untagged VLAN，即发送报文时不需要带 Tag 信息的 VLAN，取值范围为 1~4094 或空；

6 点击 确定 ，自动返回到 Hybrid 端口显示页面。



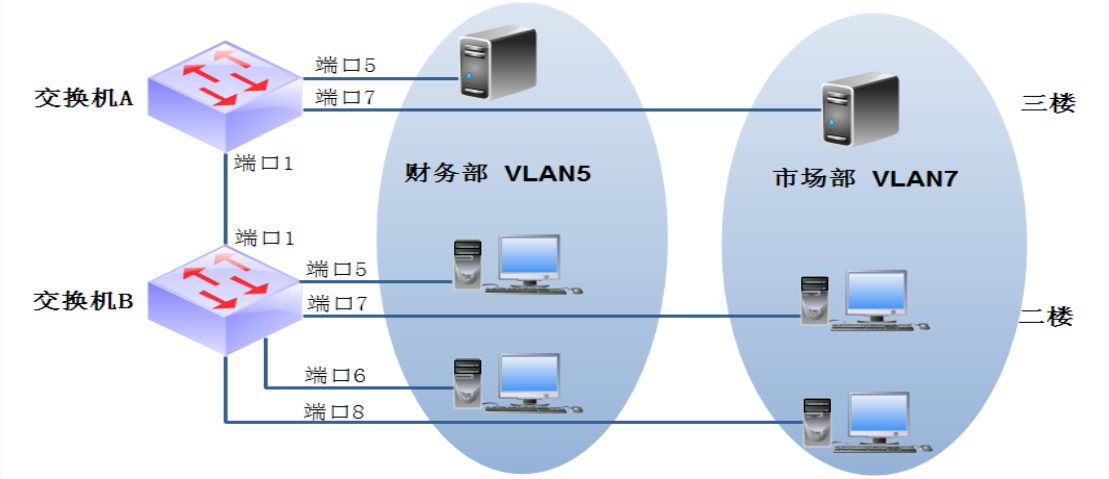
1.5 802.1Q VLAN 组网应用举例

组网需求：

某公司财务部和市场部的工作人员在二楼办公，但财务部和市场部的服务器在三楼。现要实现各部门内部能互相通信并访问其服务器，部门之间不能互相通信。

组网分析：

使用两个交换机，在交换机上设置 802.1Q VLAN 实现。财务部属于 VLAN5，市场部属于 VLAN7。如图。



设置步骤：

交换机 A 设置：

步骤	操作	说明
1	创建 VLAN5	进入『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』页面，设置端口 5 为 VLAN5。
2	创建 VLAN7	进入『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』页面，设置端口 7 为 VLAN7。
3	设置 Trunk 端口	进入『VLAN 管理』→『VLAN 配置』→『Trunk 端口』页面，设置端口 1 为 Trunk 端口，PVID 为 1，属于 VLAN5 和 7。

交换机 B 设置：

步骤	操作	说明
1	创建 VLAN5	进入『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』页面，设置端口 5 和端口 6 为 VLAN5。
2	创建 VLAN7	进入『VLAN 管理』→『VLAN 配置』→『802.1Q VLAN』页面，设置端口 7 和端口 8 为 VLAN7。
3	设置 Trunk 端口	进入『VLAN 管理→『VLAN 配置』→『Trunk 端口』页面，设置端口 1 为 Trunk 端口，PVID 为 1，属于 VLAN5 和 7。

2 端口 VLAN

如果各 VLAN 成员均需要与上级网络设备通信，但上级网络设备不支持 802.1Q VLAN 时，可采用端口 VLAN 实现。

提示

- 端口 VLAN 与 802.1Q VLAN 可以任意切换，但由 802.1Q VLAN 切换至端口 VLAN 时，VLAN 相关的配置(如：MAC 过滤、静态 MAC 地址和端口隔离)将会清空。
- 端口 VLAN 不可跨交换机。只有在同一交换机上且划分在同一 VLAN 的端口才能相互通信。

本交换机中，端口 VLAN 配置页面包括 VLAN 切换，端口 VLAN 两个页面：

VLAN 切换：用于 802.1Q VLAN 和端口 VALN 模式切换，两者只能同时存其一。

端口 VLAN：用于设置、显示端口 VLAN。

2.1 VLAN 切换

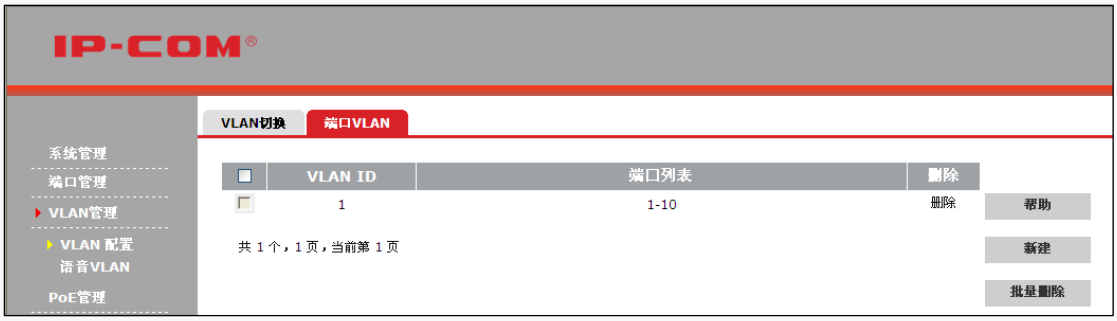
点击『VLAN 管理』→『VLAN 配置』→『VLAN 切换』进入页面，设置 VLAN 模式为端口 VLAN。

2.2 端口 VLAN

创建端口 VLAN，点击『VLAN 管理』→『VLAN 配置』→『端口 VLAN』进入页面。

提示

端口 VLAN 最多可创建 10 个。



添加端口 VLAN：

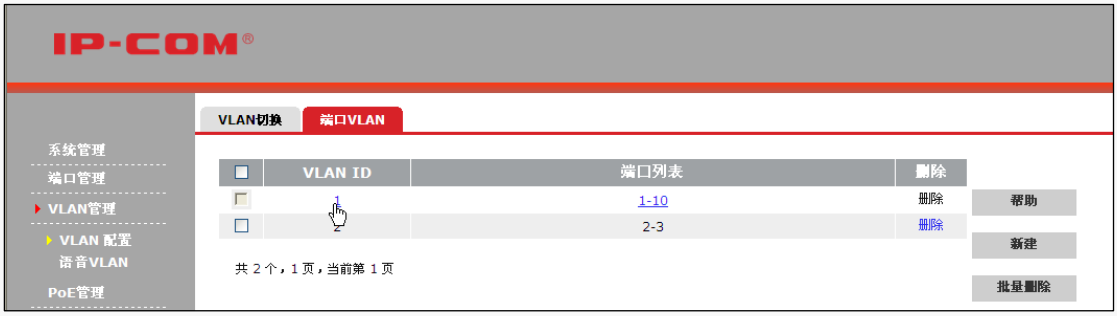
1. 点击 新建，进入端口 VLAN 规则添加页面；
2. 按页面提示规则输入 VLAN ID；
3. 从“可选端口”栏选择端口后，点击 》添加到“VLAN 包含端口”；

4. 点击 确定；

编辑端口 VLAN：

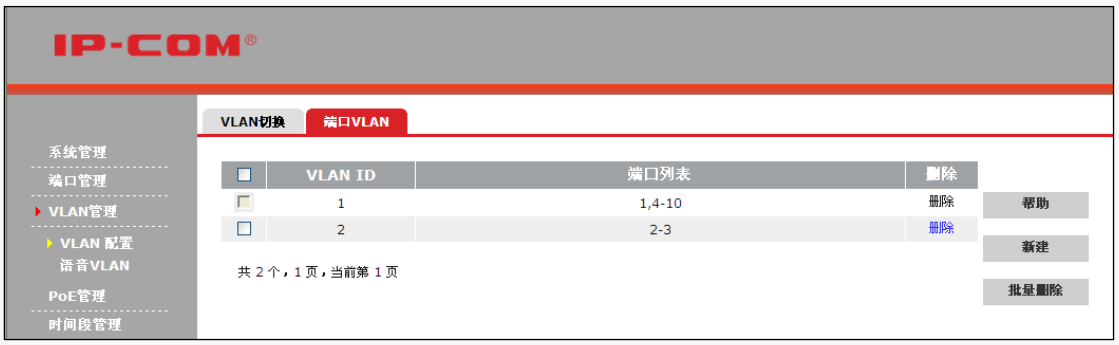
请点击对应的端口 VLAN 项后，进入页面修改即可。如上文中，端口 2，3 其实还在 VLAN1 内，如果想将这两个端口与其他端口隔离，需将 2，3 从 VLAN1 中删除，步骤如下：

1 点击『VLAN 管理』→『VLAN 配置』→『端口 VLAN』页面的 VLAN1；



2 从“VLAN 包含端口”栏选择需要删除的端口后，点击 《 添加到“可选端口”；

3 点击 确定 。



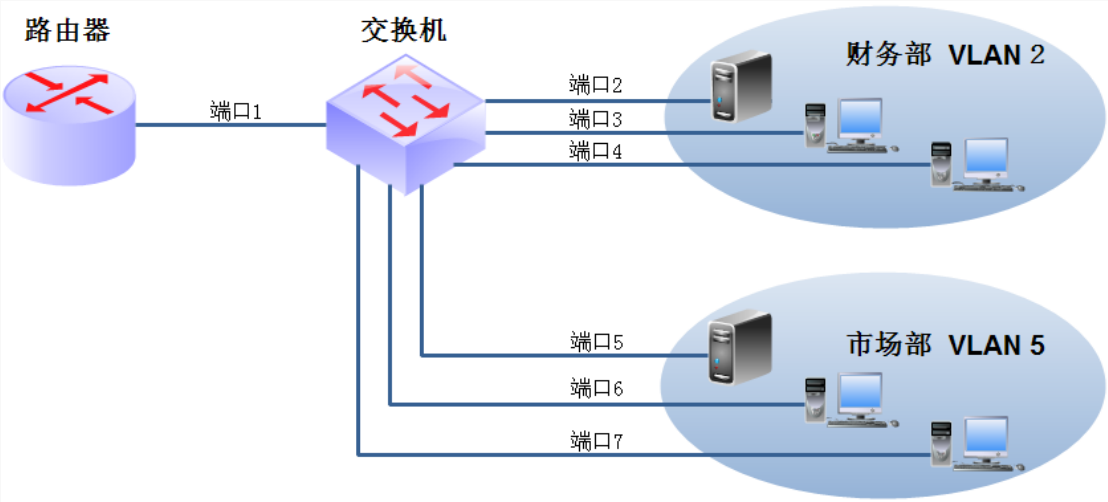
2.3 端口 VLAN 组网应用举例

组网需求：

某公司有财务部、市场部。现要实现如下需求：各部门内部能互相通信，部门之间不能互相通信，各部门人员均要访问外网。

组网分析：

使用两个交换机，在交换机上设置 Port VLAN 实现。财务部属于 VLAN2，市场部属于 VLAN5。如图。



交换机设置步骤：

步骤	操作	说明
1	设置 VLAN 模式	进入『VLAN 管理』→『VLAN 配置』→『VLAN 切换』页面，设置交换机 VLAN 模式为端口 VLAN。
2	创建 VLAN2	进入『VLAN 管理』→『VLAN 配置』→『端口 VLAN』页面，设置端口 1、2、3、4 为 VLAN2。
3	创建 VLAN3	进入『VLAN 管理』→『VLAN 配置』→『端口 VLAN』页面，设置端口 1、5、6、7 为 VLAN5。

3	编辑 VLAN1	进入『VLAN 管理』→『VLAN 配置』→『端口 VLAN』页面，设置端口 2、3、4、5、6、7 不属于 VLAN1。

3 语音 VLAN

随着语音技术的日益发展，语音设备应用越来越广泛，尤其在宽带小区，网络中经常同时存在语音数据和业务数据两种流量。通常，语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。

语音 VLAN 是为语音数据流专门划分的 VLAN。通过将连接语音设备的端口加入到划分的语音 VLAN，使语音数据集中在语音 VLAN 中进行传输，便于对语音流进行有针对性的 QoS(Quality of Service，服务质量）配置，提高语音数据的传输优先级，保证通话质量。

➘ 语音流的识别

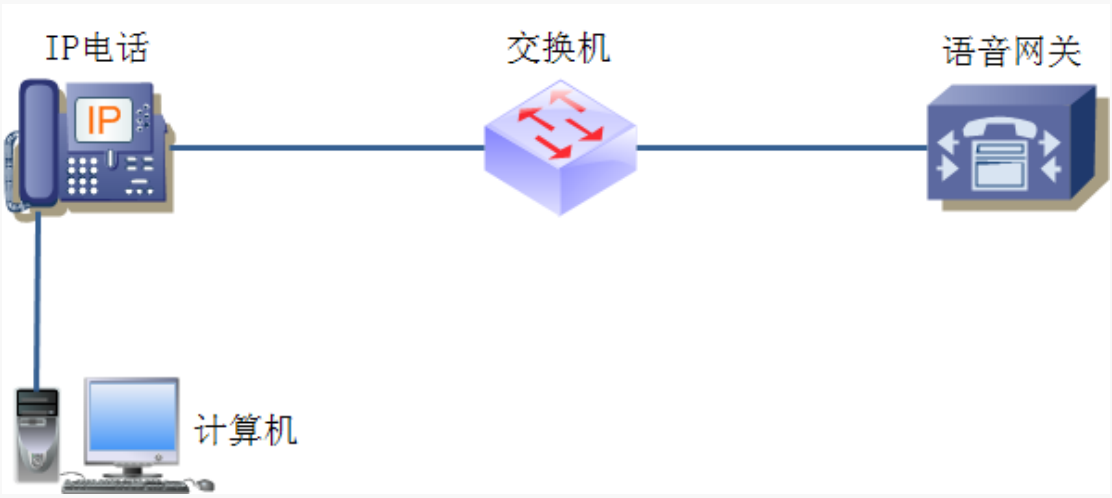
本交换机可以根据接收报文中的源 MAC 地址字段来判断该数据流是否为语音数据流，源 MAC 地址符合系统设置的语音设备 OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流。

用户可以预先设置 OUI 地址，也可以使用缺省的 OUI 地址作为判断标准。OUI 地址通常为 MAC 地址的前 24 位，是 IEEE 为不同设备供应商分配的一个全球唯一的标识符，从 OUI 地址可以判断出该设备是哪一个厂商的产品。本交换机支持配置 OUI 地址的掩码，用户可以通过设定不同的掩码来调节交换机对 MAC 地址匹配的深度。

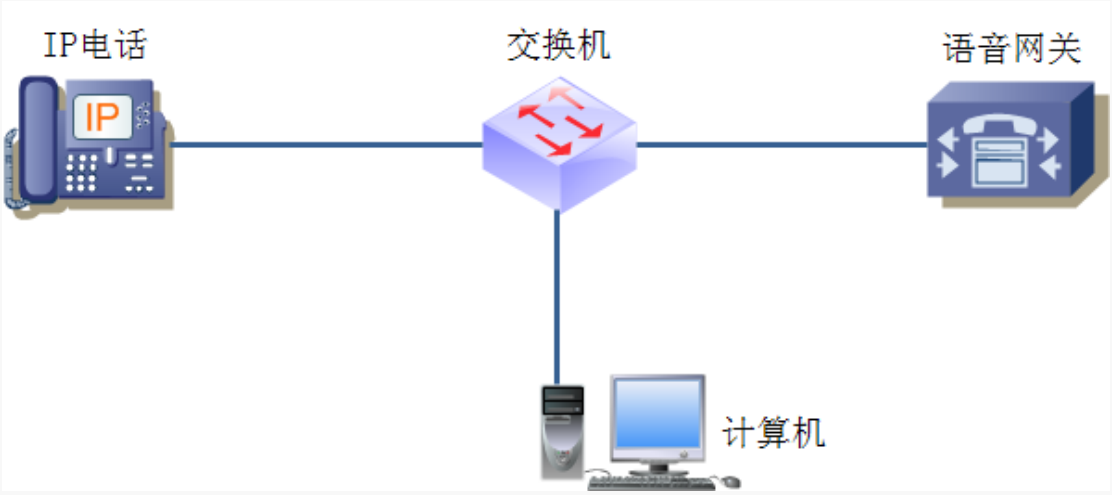
➘ 端口的语音 VLAN 模式

本交换机支持自动和手动语音 VLAN 模式，自动和手动指的是端口加入语音 VLAN 的方式。

自动模式：系统利用 IP 电话上电时发出的协议报文（untagged 报文），通过识别报文的源 MAC，匹配 OUI 地址。匹配成功后，系统自动把语音报文的输入端口加入语音 VLAN，配置报文的优先级。管理员可以在交换机上设置语音 VLAN 的老化时间，如果在老化时间内，系统没有从输入端口收到任何语音报文，系统将把该端口从语音 VLAN 中删除。端口的添加/删除到语音 VLAN 的过程由系统自动实现。自动模式适用于 PC-IP 电话串联接入（端口同时传输语音数据和普通业务数据）的组网方式。如下图。



手动模式：需要管理员手动把 IP 电话接入端口加入到语音 VLAN 中。再通过识别报文的源 MAC，匹配 OUI 地址。匹配成功后，系统将下发 ACL 规则、配置报文的优先级。端口的添加/删除到语音 VLAN 的过程由管理员手动实现。手动模式适用于 IP 电话单独接入（端口仅传输语音报文）的组网方式，如下图。该组网方式可以使该端口专用于传输语音数据，最大限度避免业务数据对语音数据传输的影响。



➘ 各链路类型端口对语音 VLAN 的支持情况

语音 VLAN 功能支持使用 Access、Trunk 和 Hybrid 端口传输语音数据，交换机上原属于其它 VLAN 的 Trunk 和 Hybrid 端口可以通过开启语音 VLAN 功能，同时传输语音和数据业务。根据 IP 电话种类的不同，各种链路类型的端口需要满足不同的条件才能够支持。

对于自动获取 IP 地址及语音 VLAN 编号的电话，端口的支持条件如下表：

语音 VLAN 模式	语音流类型	端口的链路类型
自动模式	tagged 语音流	Access：不支持。
		Trunk：支持，但接入端口的缺省 VLAN 必须存在，且不能是语音 VLAN，同时接入端口允许缺省 VLAN 通过。
		Hybrid：支持，但接入端口的缺省 VLAN 必须存在，且不能是语音 VLAN，同时缺省 VLAN 应在接入端口允许通过的 tagged VLAN 列表中。
	untagged 语音流	Access、Trunk、Hybrid：不支持。
手动模式	tagged 语音流	Access：不支持。
		Trunk：支持，但接入端口的缺省 VLAN 必须存在，且不能是语音 VLAN，同时接入端口允许该缺省 VLAN 通过。
		Hybrid：支持，但接入端口的缺省 VLAN 必须存在，且不能是语音 VLAN，同时语音 VLAN 应在接入端口允许通

		过的 tagged VLAN 列表中。
	untagged 语音流	Access：支持，但接入端口的缺省 VLAN 必须是语音 VLAN。
		Trunk:支持,但接入端口的缺省 VLAN 必须是语音 VLAN,且接入端口允许语音 VLAN 通过。
		Hybrid：支持，但接入端口的缺省 VLAN 必须是语音 VLAN,且在接入端口允许通过的 untagged VLAN 列表中。

对于手动设置 IP 地址及语音 VLAN 编号的电话，由于其只能发送 tagged 语音流，匹配关系较为简单，如下表：

语音 VLAN 模式	端口链路类型	支持条件
自动模式	Access	不支持。
	Trunk	支持，但接入端口的缺省VLAN必须存在且不能是语音VLAN，同时接入端口允许缺省VLAN通过。
	Hybrid	支持，但接入端口的缺省VLAN必须存在且不能是语音VLAN，同时缺省VLAN应在接入端口允许通过的tagged VLAN列表中。
手动模式	Access	不支持。
	Trunk	支持，但接入端口的缺省VLAN必须存在，且不能是语音VLAN，同时接入端口允许该缺省VLAN通过。
	Hybrid	支持，但接入端口的缺省VLAN必须存在且不能是语音VLAN，同时语音VLAN应在接入端口允许通过的tagged VLAN列表中。

➘ 语音 VLAN 安全模式

当端口开启语音 VLAN 功能后，通过配置端口的安全模式还可以过滤数据流。若开启安全模式，则端口只转发语音数据包，对于其他源 MAC 地址不匹配 OUI 地址的数据包，端口将直接丢弃。若关闭安全模式，则端口转发所有数据包。具体请参考下表。

安全模式	报文类型	处理方式
关闭	untagged 报文	不对报文的源 MAC 地址进行检查，所有报文都可以在语音 VLAN 内传输。
	带有语音 VLAN tag 的报文	

	带有其他 VLAN tag 的报文	根据数据的 VID 进行转发，不受语音 VLAN 安全模式的影响。
开启	untagged报文	当该报文源MAC地址是可识别的OUI地址时，允许该报文在语音VLAN内传输，否则将该报文丢弃。
	带有语音VLAN tag的报文	
	带有其他VLAN tag的报文	根据数据的VID进行转发，不受语音VLAN安全模式的影响。

强烈建议用户尽量不要在语音 VLAN 中同时传输语音和业务数据。如确有此需要，请确认语音 VLAN 安全模式为禁用。

3.1 全局设置

设置是否开启交换机语音 VLAN 功能及语音 VLAN 老化时间，点击『VLAN 管理』→『语音 VLAN』→『全局设置』进入页面。

注意

只有在 802.1Q VLAN 模式下，才可开启语音 VLAN。

以下是对页面各参数的说明：

标题项	说明
语音 VLAN 安全模式	设置端口转发数据包的模式。 **关闭**：端口转发所有数据。**开启**：端口只转发语音数据。
语音 VLAN 老化时间	对于在自动模式下加入到语音 VLAN 的端口，在老化时间过后，系统还没有从入端口收到任何语音报文时，系统将把该端口从语音 VLAN 中删除。 对于在手动模式下加入到语音 VLAN 的端口，端口从语音 VLAN 内删除需要手动操作。

3.2 端口设置

点击『VLAN 管理』→『语音 VLAN』→『端口设置』进入语音 VLAN 端口设置页面。

单端口语音 VLAN 设置：点击对应端口号，进入页面设置即可。

批量端口语音 VLAN 设置：点击 配置 ，进入页面设置即可。

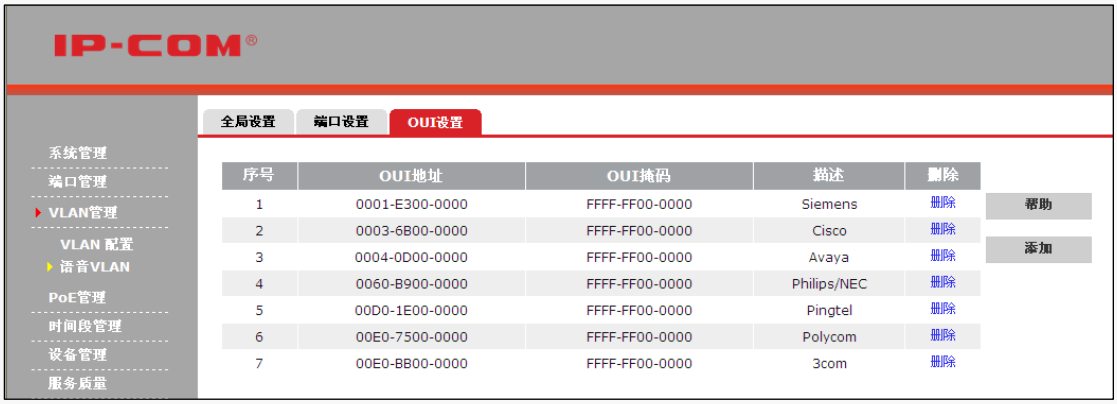
以下是对页面各参数的说明：

标题项	说明
端口	端口号。
语音 VLAN 端口模式	选择语音 VLAN 的工作模式，“手动”或“自动”。 手动模式时，不受语音 VLAN 老化时间限制。

语音 VLAN 端口状态	开启/关闭端口语音 VLAN 功能。
语音 VLAN ID	设置端口语音 VLAN ID。

3.3 OUI 设置

点击『VLAN 管理』→『语音 VLAN』→『OUI 设置』进入页面。



默认情况下，本交换机可识别的 OUI 地址如下表：

序号	OUI 地址	OUI 掩码	描述
1	0001-E300-0000	FFFF-FF00-0000	Siemens
2	0003-6B00-0000	FFFF-FF00-0000	Cisco
3	0004-0D00-0000	FFFF-FF00-0000	Avaya
4	0060-B900-0000	FFFF-FF00-0000	Philips/NEC
5	00D0-1E00-0000	FFFF-FF00-0000	Pingtel
6	00E0-7500-0000	FFFF-FF00-0000	Polycom
7	00E0-BB00-0000	FFFF-FF00-0000	3com

您还可以自定义添加 OUI 地址。方法：点击 添加 ，进入页面添加即可。

以下是对页面各参数的说明：

标题项	说明
OUI 地址	用于识别语音流设备的源 MAC 地址。
掩码	输入 OUI 地址的掩码。 默认为 FFFF-FF00-0000。表示 MAC 地址的前 24 位必须和 OUI 地址一样才能被识别为语音流，MAC 地址后 24 位任意均可。
描述	可以描述某个 OUI 地址所对应的厂商或者其他信息。

PoE 管理

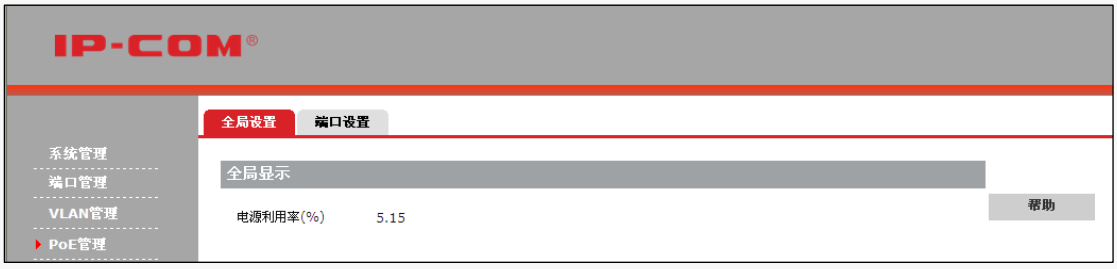
传统的网络建设中，所有的终端设备都采用电力网络直接供电，导致成本高昂，线缆部署安装复杂，走线也很杂乱。

PoE（Power Over Ethernet），在现有以太网网线基础架构不作任何改动的情况下，为一些基于 IP 的终端（如 IP 电话、无线 AP、网络摄像机等）传输数据信号的同时，还能为此类设备提供直流供电的技术。通过 PoE 技术，在确保现有结构化布线安全的同时保证现有网络的正常运作，最大限度地降低了成本。

本交换机的 8 个 10/100/1000M 自适应 RJ45 端口均支持 IEEE 802.3af、IEEE 802.3at 标准 PoE 供电，最多可以同时接入 8 个 IEEE 802.3af 标准或者 4 个 IEEE 802.3at 标准的受电设备。本交换机 PoE 供电的电源管理为动态分配，即，根据端口实际使用功率分配。在供电时，使用网线 1、2，3、6 数据线对供电，最大供电距离为 100 米。

1 全局显示

如果您想要了解当前交换机 PoE 电源的使用情况，请点击『PoE 管理』→『全局设置』进入页面查看。



2 端口设置

默认情况下，交换机的每个 RJ45 口均已开启了 PoE 供电功能。您可点击『PoE 管理』→『端口设置』，进入页面查看当前交换机各 RJ45 口的 PoE 供电情况或修改端口 PoE 属性。

以下是对页面各参数的说明：

标题项	说明
启用 PoE	启用/禁用端口 PoE 供电功能。只有在端口 PoE 启用时，才可对接入该端口的受电设备进行 PoE 供电。
输送功率	实时显示端口的 PoE 供电功率，单位为瓦（W）。 提示 显示结果可能存在误差，该值仅供参考。
时间段	为端口指定的时间段 ID（需要首先在『时间段管理』页面设置时间段），不指定表示不对端口进行任何时间限制。

时间段管理

时间段，用于描述一个特殊的时间范围。通过配置时间段，您可智能定义交换机 PoE 供电时间段，实现智能供电管理，绿色节能。

点击『时间段管理』进入时间段管理页面。

以下是对页面各参数的说明：

标题项	说明
时间段 ID	对应的时间段的 ID 号。
时间片段数	统计本时间段中所包含的时间片段总数，最多可设置四片。
周期时间	显示本时间段 ID 的周期时间，范围：<周一~周日>。若该时间段为绝对时间，则本项显示为“--”。
绝对时间	显示本时间段的绝对时间，范围：<2000 年 1 月 1 日~2035 年 12 月 31 日>。若该时间段为周期时间，则本项显示为“--”。

新建时间段：

1. 点击 新建 ；
2. 进入时间段设置页面，输入一个时间段 ID；
3. 选择“绝对时间”或“周期时间”后，设置对应的时间日期；
4. 选择时间片的“起始—结束”时间；
5. 点击 添加 ，将设置的时间片添加到时间片列表；

6 点击 确定 保存即可。

编辑时间段：

如果您需要修改已添加的时间段，请点击对应的时间段 ID 后，进入页面修改即可。

设备管理

本节内容可帮助您提高交换机的数据转发性能，并提供给您高效管理交换机的方法。包含以下五部分内容：

MAC 配置：管理交换机的 MAC 地址转发表。

STP 配置：消除局域网中数据链路层物理环路，避免广播风暴并提供链路备份冗余。

IGSP 配置：管理和控制组播组，以节约网络带宽，增强组播信息安全，方便每台主机单独计费。

SNMP 配置：高效管理交换机。

DHCP 侦听：保护局域网中 DHCP 服务器安全，避免 DHCP 服务器欺骗和 DHCP 地址耗尽。

1 MAC 配置

交换机在数据链路层对报文进行转发，在转发过程中，交换机通过学习报文的源 MAC 地址等信息，创建包含有 MAC 地址、VLAN ID（如果有）、端口号信息的 MAC 地址转发表。之后，交换机在转发报文时，根据 MAC 地址表项信息，采取对应的转发方式：

- 单播：当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文转发到该表项中的转发出端口。
- 广播：当交换机收到目的 MAC 地址第二字节最低位为 1 的报文，或 MAC 地址转发表中没有包含对应报文目的 MAC 地址的表项时，交换机将采取广播方式将报文向除接收端口外的所有端口转发。即，广播报文、组播报文、未知单播报文都将广播转发。

➘ MAC 地址转发表的老化机制

交换机的 MAC 地址转发表是有容量限制的，为了最大限度利用地址转发表资源，交换机利用老化机制更新 MAC 地址转发表。

系统在动态创建某条表项的同时，开启老化定时器（在『系统管理』→『系统配置』→『系统信息』页面设置的“MAC 地址表项老化时间”），如果在老化时间到期时没有再次收到源地址与表项中的源 MAC 地址一致的报文，交换机就会自动把该 MAC 地址表项删除。

➘ MAC 地址表项的分类与特点

根据配置方式和自身特点的不同，MAC 地址表项可以分为以下二类：

- 静态 MAC 地址表项：也称为“永久地址”，由用户手动添加和删除，不会随着时间老化。对于一个设备变动较小的网络，手动添加静态地址表项可以减少网络中的广播流量。
- 动态 MAC 地址表项：交换机通过 MAC 地址学习机制自动添加的 MAC 地址表项，它会随着用户配置的老化时间的到期而被删除。

1.1 MAC 地址表显示

查看交换机的动态 MAC 地址表项，点击『设备管理』→『MAC 配置』→『MAC 地址显示』进入页面。

提示

- MAC 地址长度为 6 字节。在本交换机中，MAC 地址显示和设置格式为：XXXX-XXXX-XXXX。其中，“X”为 16 进制字符。
- 如果 VLAN 类型为端口 VLAN，则 VLAN 栏显示为“--”。

如果您想了解某个端口 MAC 地址表，请点击具体的端口编号查看即可。

绑定

如果您想要使某条 MAC 地址表项不被老化，可将该条 MAC 地址表项进行绑定，使该条 MAC 地址表项转为静态 MAC 地址表项。

点击 MAC 地址表项后的 绑定 ，即可绑定该条 MAC 地址表项。绑定后页面将显示该 MAC 处于“已绑定”状态。“绑定”的 MAC 表项将在静态 MAC 地址页面显示。

➘ 查询 MAC 表项

点击 查询 ，通过 MAC 和 VLAN 条件组合进行查询，即可查询具体的 MAC 地址表项。

MAC 地址表项查询中，MAC 地址为必填项，VLAN ID 为选填项。端口 VLAN 时，查询 MAC 地址表项只须输入 MAC 地址。

1.2 静态 MAC 地址

查看、设置静态 MAC 地址表，点击『设备管理』→『MAC 配置』→『静态 MAC 地址』进入页面。

提示

- MAC 地址和 VLAN ID 为一个表项，同一表项不可添加到不同的端口。
- 添加为静态 MAC 地址的表项，不可设置 MAC 过滤。
- 切换 802.1Q VLAN 模式将清空 MAC 地址表。
- 添加为静态 MAC 地址的表项，源 MAC 地址与 VLAN ID 匹配的报文只可由该端口接收；目的 MAC 地址与 VID 匹配的报文只会转发到该端口。

2 STP 配置

对以太网来说，两个设备间只能有一条活动的通路，否则就会产生广播风暴。但是为了加强网络的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态。当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路，并提供链路冗余备份的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择地对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备发生由于重复接收相同报文导致的报文处理能力下降问题。

➘ STP 协议报文

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息，BPDU 中包含了足够的信息来保证交换机完成生成树的计算过程。

STP 通过在设备之间传递 BPDU 来确定网络的拓扑结构。STP 协议中的 BPDU 分为两类：

- 配置 BPDU（Configuration BPDU）：用来进行生成树计算和维护生成树拓扑的报文。
- TCN BPDU（Topology Change Notification BPDU）：当拓扑结构发生变化时，用来通知相关设备网络拓扑结构发生变化的报文。

➘ STP 的基本概念

1. 桥 ID

桥 ID 是桥的优先级和 MAC 地址的综合数值，其中桥优先级是一个可以设定的参数。桥 ID 越低，则桥的优先级越高。桥 ID 最小的桥为根桥。

2. 根桥

树形的网络结构必须有树根，于是 STP 引入了根桥（Root Bridge）的概念。根桥在全网中有且只有一个，且根据网络拓扑的变化而改变，因此根桥并不是固定的。

在网络初始化过程中，所有设备都视自己为根桥，生成各自的配置 BPDU 并周期性地向外发送；当网络拓扑稳定后，只有根桥设备才会向外发送配置 BPDU，其它设备只对其进行转发。

3. 根端口

根端口，指一个非根桥设备上离根桥最近的端口，负责与根桥进行通信。非根桥设备上有且

只有一个根端口，根桥上没有根端口。

4．指定桥与指定端口

指定桥：对于一台设备而言，指与本机直接相连并负责向本机转发 BPDU 的设备；对于一个局域网而言，指负责向本网段转发 BPDU 的设备。

指定端口：对于一台设备而言，为指定桥向本机转发 BPDU 的端口；对于一个局域网而言，为指定桥向本网段转发 BPDU 的端口。

5．路径开销

STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

➘ BPDU 的优先级比较原则

根桥 ID 较小的 BPDU 优先级更高；若根桥 ID 相同，则比较根路径开销，比较方法为：用 BPDU 中的根路径开销加上本端口对应的路径开销，假设两者之和为 S，则 S 较小的 BPDU 优先级较高。

若根路径开销也相同，则依次比较指定桥 ID、指定端口 ID、接收该 BPDU 的端口 ID 等，上述值较小的 BPDU 优先级较高。

➘ STP 的计算过程

- 初始状态

各台设备的各个端口在初始时会生成以自己为根桥的配置消息，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

- 最优 BPDU 的选择

各台设备都向外发送自己的 BPDU，同时也会收到其它设备发送的 BPDU。最优 BPDU 的选择过程如下：

步骤	内容
1	当端口收到的 BPDU 比本端口 BPDU 的优先级低时，设备会将接收到的 BPDU 丢弃，对该端口的 BPDU 不作任何处理。 当端口收到的 BPDU 比本端口 BPDU 的优先级高时，设备就用接收到的 BPDU 中的内容替换该端口的 BPDU 中的内容。
2	设备将所有端口的 BPDU 进行比较，选出最优的 BPDU。

- 根桥的选择

通过交换 BPDU，设备之间比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。

- 根端口、指定端口的选择

根端口、指定端口的选择过程如下：

步骤	内容

1	非根桥设备将接收最优 BPDU 的那个端口定为根端口。
2	设备根据根端口的 BPDU 和根端口的路径开销，为每个端口计算一个指定端口 BPDU： • 根桥 ID 替换为根端口的配置消息的根桥 ID； • 根路径开销替换为根端口配置消息的根路径开销加上根端口对应的路径开销； • 指定桥 ID 替换为自身设备的 ID； • 指定端口 ID 替换为自身端口 ID。
3	设备使用计算出来的配置消息和需要确定端口角色的端口上的配置消息进行比较，并根据比较结果进行不同的处理： • 如果计算出来的配置消息优，则设备就将该端口定为指定端口，端口上的配置消息被计算出来的配置消息替换，并周期性向外发送； • 如果端口上的配置消息优，则设备不更新该端口的配置消息并将此端口阻塞，此端口将不再转发数据，只接收但不发送配置消息。

提示

在拓扑稳定状态，只有根端口和指定端口转发流量，其它端口都处于阻塞状态，它们只接收 STP 协议报文（BPDU）而不转发用户流量。

➘ STP 定时器

1. 联络时间（Hello Time）

交换机每隔一段时间会向周围的交换机发送 BPDU，以确认链路是否存在故障。Hello Time 即为交换机发送 BPDU 的间隔，取值范围 1~10 秒。

2. 老化时间（Max Age）

如果在超出老化时间之后，还没有收到根桥发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。取值范围 6~40 秒。

3. 传输时延（Forward Delay）

为交换机状态迁移的延迟时间。取值范围 4~30 秒。

链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新 BPDU 无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。为此，STP 采用了一种状态迁移的机制，新选出的根端口和指定端口要经过 2 倍的 Forward Delay 延时后才能进入转发状态，这个延时保证了新的配置消息已经传遍整个网络。

➘ RSTP

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）在 STP 上做了改进，实现了网络拓扑的快速收敛。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发

状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间（传统的 STP 需要大约 50 秒，RSTP 只需要 1 秒左右）。

RSTP 中，实现根端口和指定端口的状态快速迁移的前提条件分别如下：

- 根端口：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。
- 指定端口：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

➘ RSTP 的基本概念

1．边缘端口

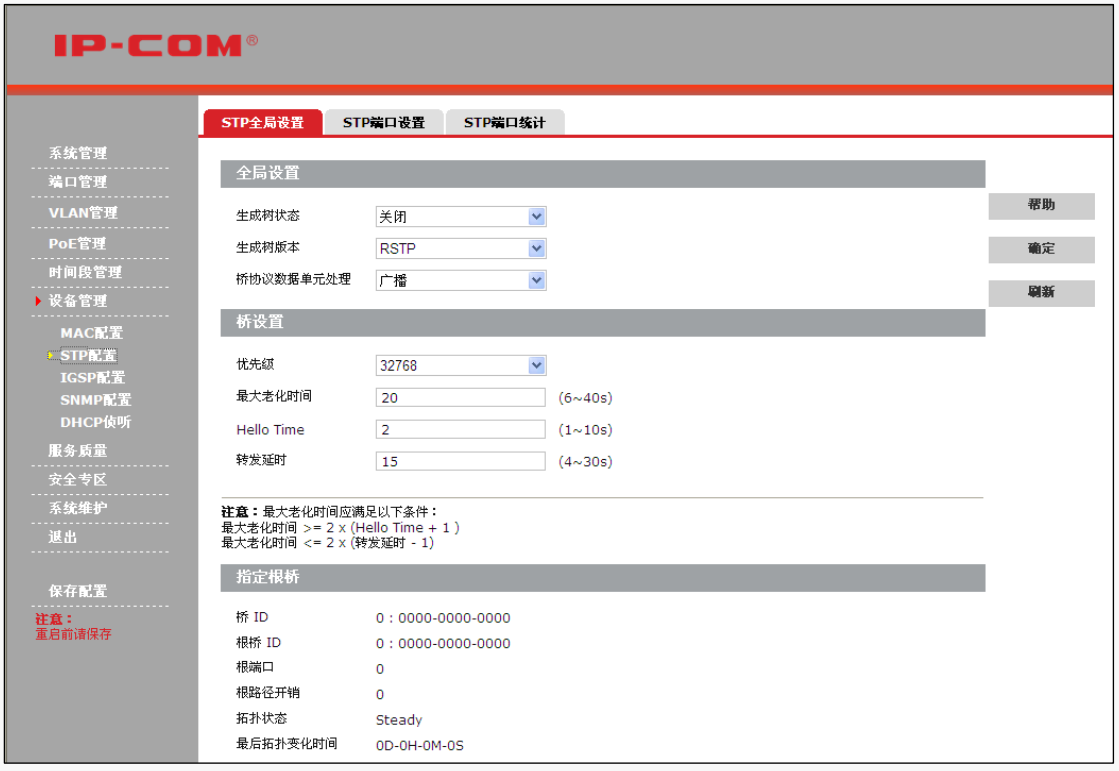
边缘端口是一个可以被设置的指定端口，可直接连接到无环路的网络端口。通常该类直接连接终端设备（用户端）。指定为边缘端口可快速迁移到转发状态，而不需要经历监听和学习的状态。若边缘端口接收到 BPDU 报文，将变为非边缘端口，变成一个普通的生成树端口，参与生成树的计算。

2．点对点端口

点对点端口可以进行快速的迁移。在 RSTP 下，所有在全双工模式下的端口被认为点对点端口，除非手动设置点对点端口关闭。

2.1 STP 全局设置

STP 全局设置用于配置和查看交换机生成树功能的全局属性，点击『设备管理』→『STP 配置』→『STP 全局设置』进入页面。

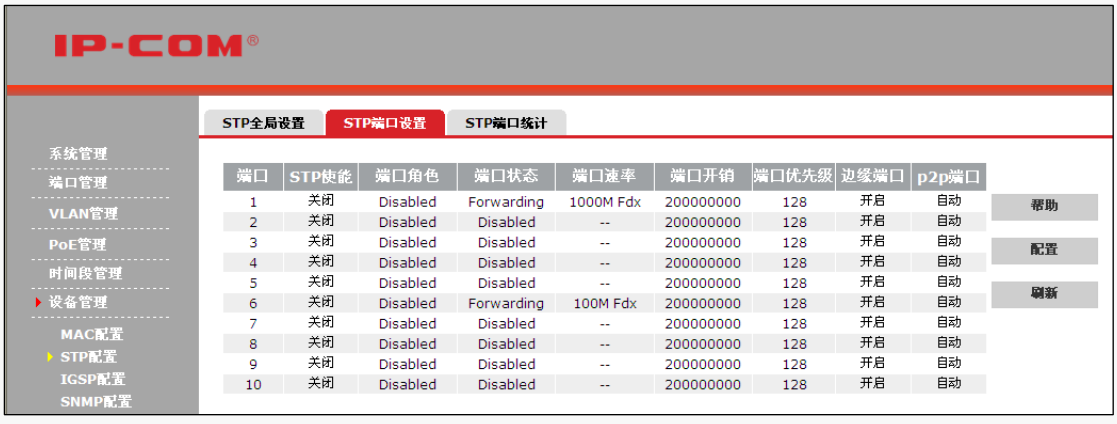


以下是对各页面参数的说明：

标题项	说明
生成树状态	开启/关闭交换机生成树功能。默认情况下，生成树功能处于关闭状态。
生成树版本	选择交换机的生成树模式。 **STP**：生成树兼容模式。 **RSTP**：快速生成树兼容模式。交换机默认为 RSTP 模式。
桥协议数据单元处理	选择交换机禁用生成树功能时，BPDU 报文处理的方式。 **广播**：广播 BPDU 报文。默认情况下，BPDU 报文处理方式为广播。 **过滤**：过滤 BPDU 报文。
优先级	设置交换机的优先级。优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。 值越小，优先级越高。优先级默认为 32768，且必须是 4096 的倍数。
最大老化时间	设置 BPDU 在交换机中能够保存的最大生存期。默认为 20 秒。最大老化时间应满足以下条件： 最大老化时间 >= 2 * (Hello Time + 1) 最大老化时间 <= 2 * (转发延时 - 1)
Hello time	设置交换机发送 BPDU 的时间间隔。默认为 2 秒。
转发延时	设置在网络拓扑改变后，交换机的端口状态迁移的延时时间。默认为 15 秒。
指定根桥	显示交换机生成树功能的相关信息。

2.2 STP 端口设置

STP 端口设置，用于设置交换机各端口的 STP 参数，点击『设备管理』→『STP 配置』→『STP 端口设置』进入页面。



单个端口 STP 参数设置：点击对应端口号，进入页面设置即可。

批量端口 STP 参数设置：点击 配置 ，进入页面设置即可。

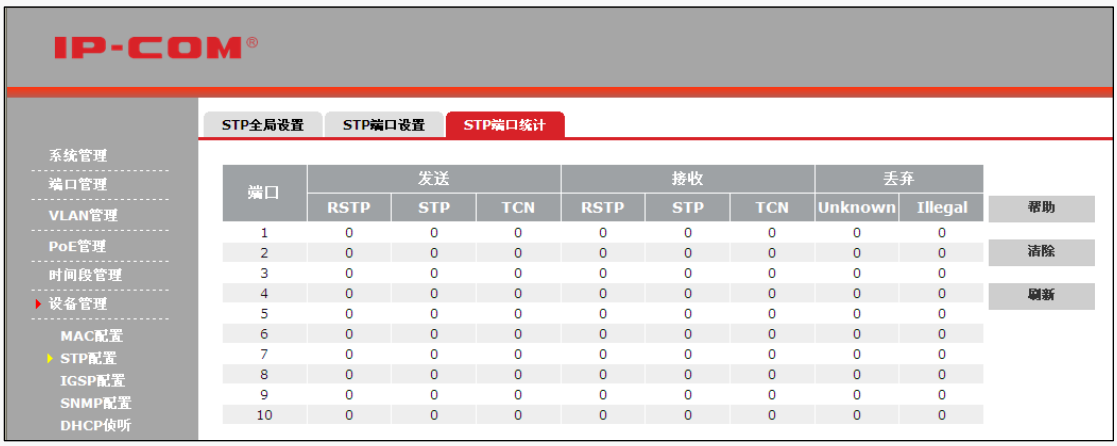
以下是对页面各参数的说明：

标题项	说明
STP 状态	开启/关闭端口的 STP 功能。 默认情况下，端口 STP 功能处于关闭状态；同时开启全局和端口的 STP 功能后，端口 STP 功能才生效。
优先级	确定与该端口连接的端口是否会被选为根端口的重要依据。同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。 默认优先级为 128，取值范围为<0~240>。

默认路径开销	开启/关闭端口默认路径开销。 禁用时可手动设置“端口路径开销”，范围为<1~200000000>；开启时端口根据端口速率和其他设置自动进行计算，支持 802.1t 标准。
路径开销	默认情况下，端口路径开销为 200,000,000。 **提示** 仅当端口默认路径开销处于禁用状态时，才可设置端口路径开销。
边缘端口	选择是否开启边缘端口。默认所有端口都为边缘端口。 边缘端口是指直接与终端设备相连的端口。边缘端口可由阻塞状态快速向转发状态迁移，而无需等待延迟时间。但是当边缘端口接收到 BPDU 报文后将变为非边缘端口。
P2P 端口	选择端口的点对点链路状态。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。 在 RSTP 下，所有在全双工模式下的端口被认为点对点端口。默认端口自动识别链路。

2.3 STP 端口统计

点击『设备管理』→『STP 配置』→『STP 端口统计』进入页面。在这里，您可对端口接收和发送的 BPDU 报文进行刷新和清除。



3 IGSP 配置

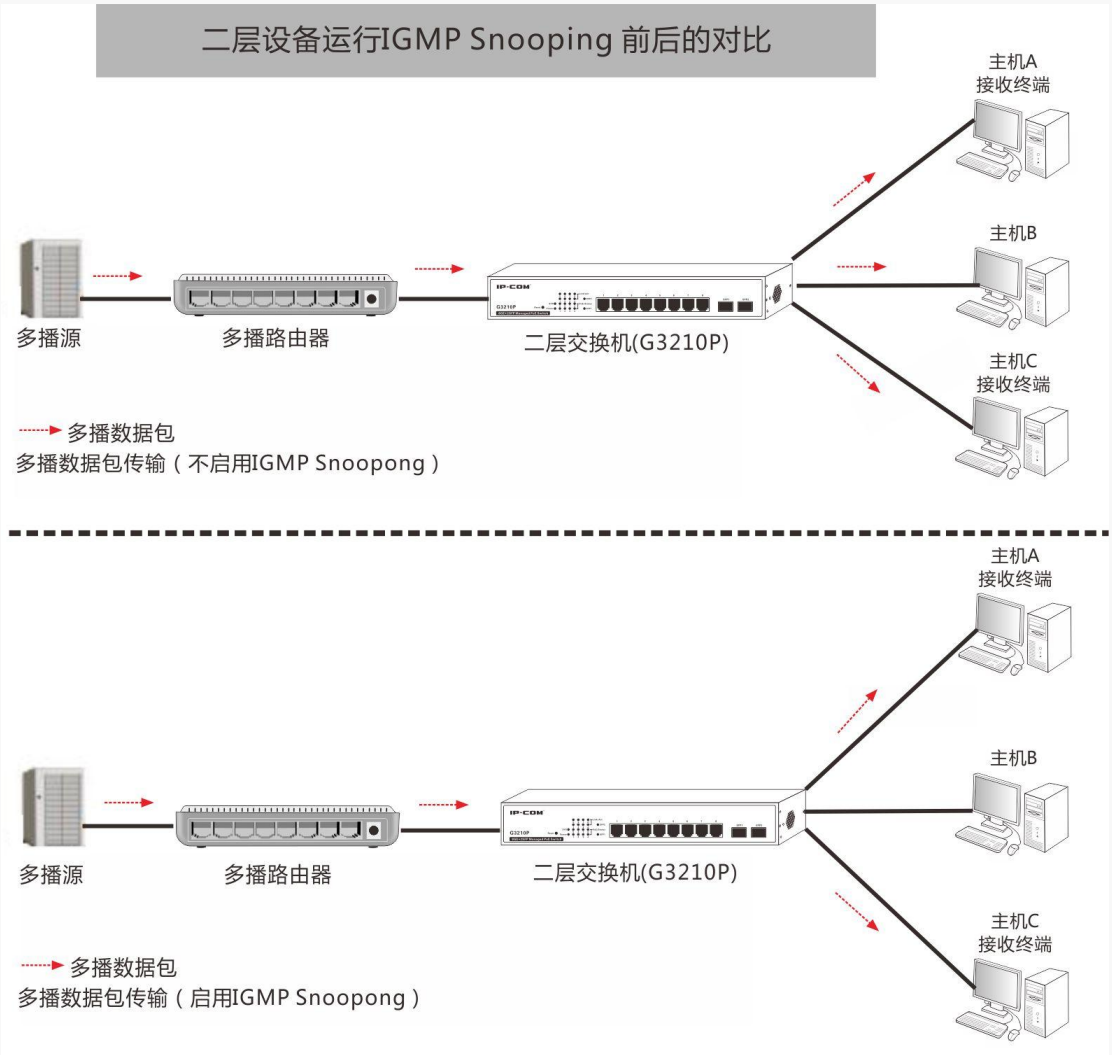
IGMP Snooping（Internet Group Management Protocol Snooping，IGMP 侦听）是运行在二层以太网交换机上的组播约束机制，用于管理和控制组播组。

➘ 原理

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和组播 MAC 地址建立起映射关系，并根据这样的映射关系转发组播数据。

- 二层设备没有运行 IGMP Snooping，组播数据在二层被广播。
- 二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者，但是未知组播数据仍然会在二层广播。

本交换机开启 IGMP Snooping 前后的对比：



➘ 工作机制

运行了 IGMP Snooping 的交换机对不同 IGMP 动作，具体处理方式如下面的描述：

1. 组查询

IGMP 查询器定期向本地网段内的所有主机与网络设备（例如：路由器）发送 IGMP 通用查询报文，以查询该网段有哪些组播组的成员。在收到 IGMP 通用查询报文时，交换机将其通过 VLAN 内除接收端口以外的其它所有端口转发出去，并对该报文的接收端口做处理（主要是端口老化定时器的重置和启动）。

2. 报告成员关系

当组播组的成员主机收到 IGMP 查询报文后，会回复 IGMP 成员关系报告报文。如果主机要加入某个组播组，它会主动向组播路由器发送 IGMP 成员关系报告报文以声明加入该组播组。在收到 IGMP 成员关系报告报文时，交换机将其通过 VLAN 内的所有路由器端口转发出去，从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做如下处理（主要是端口老化定时器的重置和启动）。交换机不会将 IGMP 成员关系报告报文通过非路由器端口转发出去。

➘ 离开组播组

运行 IGMPv1 的主机离开组播组时不会发送 IGMP 离开组报文，因此当其对应的成员端口的老化定时器超时后，交换机就会将该端口对应的转发表项从转发表中删除。

运行 IGMPv2 或 IGMPv3 的主机离开组播组时，会通过发送 IGMP 离开组报文，以通知组播路由器自己离开了某个组播组。

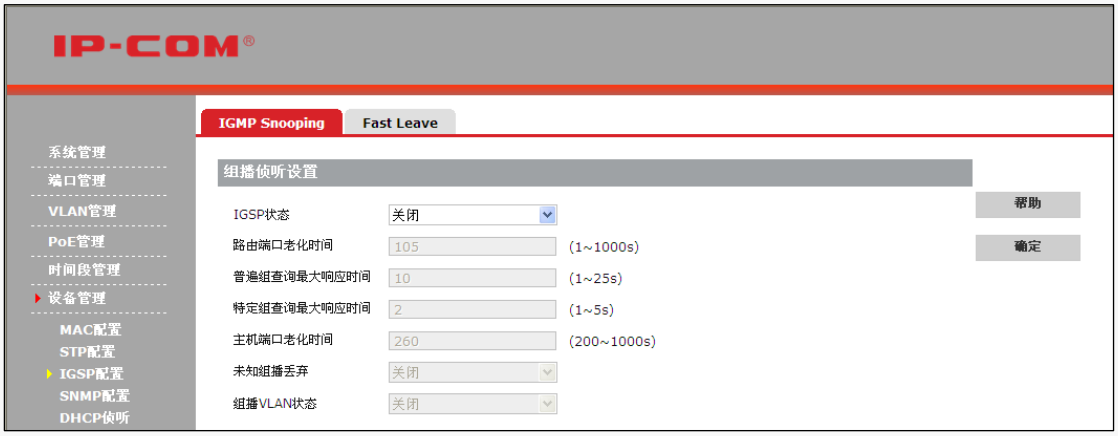
当从最后一个成员端口上收到 IGMP 离开组报文时，交换机会将该报文通过 VLAN 内的所有路由器端口转发出去，同时由于并不知道该报文的接收端口下是否还有该组播组的其它成员，所以交换机不会立刻把该端口对应的转发表项从转发表中删除，而是重置该成员端口的老化定时器。

当 IGMP 查询器收到 IGMP 离开组报文后，从中解析出主机要离开的组播组的地址，并通过接收端口向该组播组发送 IGMP 特定组查询报文。交换机在收到 IGMP 特定组查询报文后，将其通过 VLAN 内的所有路由器端口和该组播组的所有成员端口转发出去。

对于 IGMP 离开组报文的接收端口，交换机在该成员端口的老化时间内：如果从该端口收到了主机发送的响应该组播组的 IGMP 成员关系报告报文，则表示该端口下还有该组播组的成员，于是重置该成员端口的老化定时器；如果没有从该端口收到主机发送的响应该组播组的 IGMP 成员关系报告报文，则表示该端口下已没有该组播组的成员，则在该成员端口老化时间超时后，将转发表中该端口对应该组播组的转发表项删除。

3.1 IGMP Snooping

点击『设备给管理』→『IGSP 配置』→『IGMP Snooping』进入 IGMP Snooping 全局配置页面。

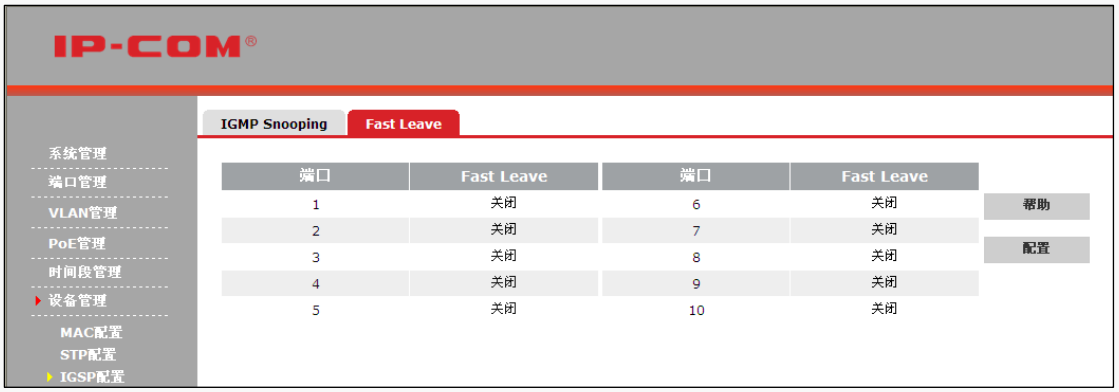


以下是对页面各参数的说明：

标题项	说明
IGSP 状态	开启/关闭 IGMP Snooping 功能。
路由端口老化时间	在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。取值范围为<1~1000>，默认为 105 秒。
普遍组查询最大响应时间	对于 IGMP 普遍组查询报文来说，通过配置 IGMP 普遍组查询的最大响应时间来填充其最大响应时间字段。 对于 IGMP 特定组查询报文来说，所配置的发送 IGMP 特定组查询报文的时间间隔将被填充到其最大响应时间字段。也就是说，IGMP 特定组查询的最大响应时间从数值上与发送 IGMP 特定组查询报文的时间间隔相同。 缺省情况下，普遍组查询最大响应时间为 10s；特定组查询最大响应时间为 2s。
特定组查询最大响应时间	
主机端口老化时间	在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。取值范围<200~1000>秒，默认为 260 秒。
未知组播丢弃	开启/关闭未知组播丢弃功能。开启时，交换机将丢弃收到的未知组播报文；关闭时，交换机将广播收到的未知组播报文。 **提示** 未知组播丢弃功能在 IGMP Snooping 功能禁用时也生效。
组播 VLAN 状态	开启/关闭 VLAN IGMP Snooping 功能。
组播 VLAN ID	开启 VLAN IGMP Snooping 功能后，填写开启 IGMP Snooping 功能的 VLAN ID，使组播报文只在该 VLAN 下进行转发。

3.2 Fast Leave

点击『设备管理』→『IGSP 配置』→『Fast Leave』进入页面。设置端口快速离开，在 IGSP/V2 版本下生效。



单端口配置：点击您想要配置的端口，进入以下页面设置即可。

批量端口配置：点击 配置 ，进入以下页面设置即可。

4 SNMP 配置

SNMP（Simple Network Management Protocol）是目前 TCP/IP 网络中应用最为广泛的网络管理协议。利用 SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

SNMP 能够屏蔽不同设备的物理差异，实现对不同厂商设备的自动化管理，特别适合在小型、快速和低成本的环境中使用。

➘ SNMP 的管理框架

SNMP 管理框架包含三个组成部分：SNMP 管理者，SNMP 代理，MIB 库（Management Information Base）。

- SNMP 管理者：一个利用 SNMP 协议对网络节点进行控制和监视的系统。其中网络环境中最常见的 SNMP 管理者被称为网络管理系统（NMS，Network Management System）。网络管理系统既可以指一台专门用来进行网络管理的服务器，也可以指某个网络设备中执行管理功能的一个应用程序。
- SNMP 代理：被管理设备中的一个软件模块，用来维护被管理设备的管理信息数据并可在需要时把管理数据汇报给一个 SNMP 管理系统。
- MIB 库：被管理对象的集合。它定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个 SNMP 代理都有自己的 MIB。SNMP 管理者根据权限可以对 MIB 中的对象进行读/写操作。

SNMP 管理者是 SNMP 网络的管理者，SNMP 代理是 SNMP 网络的被管理者，它们之间通过 SNMP 协议来交互管理信息。

SNMP 基本操作

本交换机中，SNMP 提供以下三种基本操作来实现 SNMP 管理者和 SNMP 代理的交互：

- Get 操作：SNMP 管理者使用该操作查询 SNMP 代理的一个或多个对象的值。
- Set 操作：SNMP 管理者使用该操作重新设置 MIB 库（Management Information Base）中的一个或多个对象的值。
- Trap 操作：SNMP 代理使用该操作主动向 SNMP 管理者发送报警信息（如被管理设备重新启动等）。

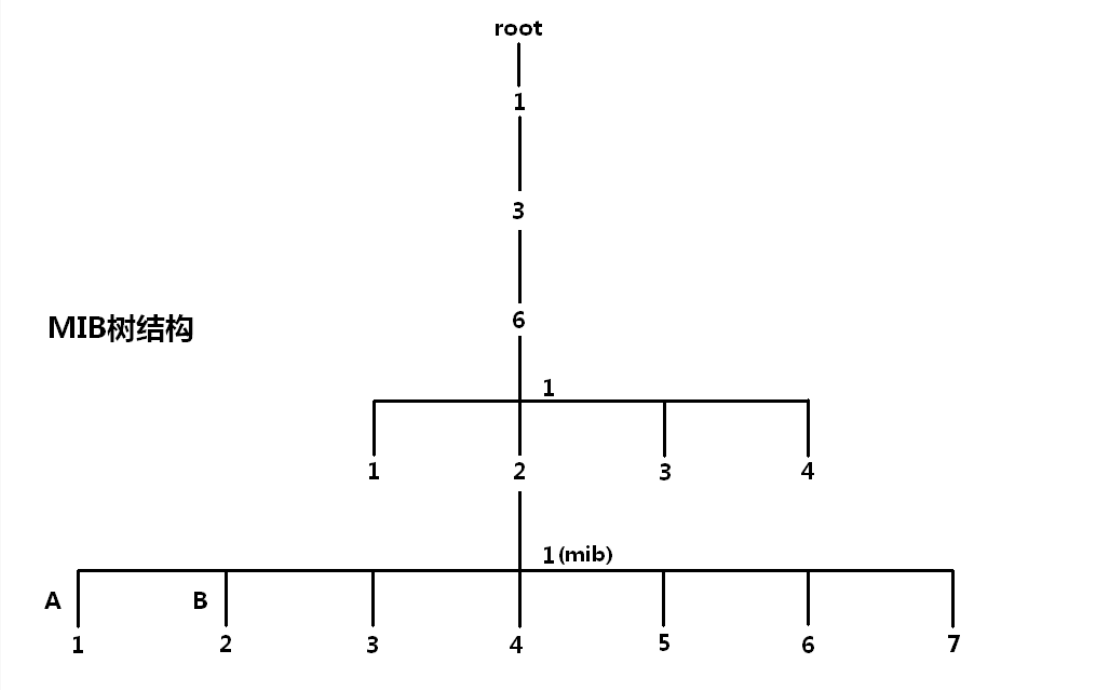
SNMP 协议版本

SNMP 管理者和 SNMP 代理上的 SNMP 版本配置必须相同，才能成功互访。目前，交换机中的 SNMP Agent 支持 SNMPv3 版本，兼容 SNMPv1 版本、SNMPv2c 版本。

- SNMPv1：采用团体名（Community Name）认证。团体名用来定义 SNMP 管理者和 SNMP 代理的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP 管理者对 SNMP 代理的访问。
- SNMPv2c：也采用团体名认证。它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：提供了更多的操作类型（GetBulk 和 InformRequest）；支持更多的数据类型（Counter64 等）；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3：提供了基于用户的安全模型（USM，User-Based Security Model）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 SNMP 管理者和 SNMP 代理之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP 管理者和 SNMP 代理之间的通信提供更高的安全性。

MIB 库简介

MIB 是以树状结构进行组织的。树的节点表示被管理对象，它可以用从根开始的一串表示路径的数字唯一地识别，这串数字称为 OID（Object Identifier，对象标识符）。MIB 的结构如图所示。图中，A 的 OID 为（1.3.6.1.2.1.1），B 的 OID 为（1.3.6.1.2.1.2）。



➘ SNMP 配置任务简介

SNMPv3 建议配置任务及步骤如下：

顺序	配置任务	说明	详细配置
1	开启 SNMP 代理	必选	在『设备管理』→『SNMP 配置』→『代理设置』页面，开启交换机的 SNMP 功能。
2	创建 MIB 视图	必选	在『设备管理』→『SNMP 配置』→『视图管理』页面，创建管理对象的视图。
3	创建 SNMP 组	必选	在『设备管理』→『SNMP 配置』→『组管理』页面创建 SNMPv3 类型的组，并为组添加不同访问权限的视图。
4	创建 SNMP 用户	必选	在『设备管理』→『SNMP 配置』→『用户管理』页面，创建 SNMPv3 组内的用户，并配置用户的认证/加密模式及密码。
5	配置 SNMP Trap	可选	在『设备管理』→『SNMP 配置』→『Trap 开启』页面开启 Trap 功能，之后，在『设备管理』→『SNMP 配置』→『Trap 设置』页面设置 Trap 类型及目标主机。

SNMPv2 或 SNMPv2c 建议配置任务及步骤如下：

顺序	配置任务	说明	详细配置
1	开启 SNMP 代理	必选	在『设备管理』→『SNMP 配置』→『代理设置』页面，开启交换机的 SNMP 功能。
2	创建 MIB 视图	必选	在『设备管理』→『SNMP 配置』→『视图管理』页面，创建管理对象的视图。
3	创建 SNMP 团体	必选	在『设备管理』→『SNMP 配置』→『代理设置』页面，以 SNMPv1 和 v2c 版本的团体名进行设置。
4	配置 SNMP Trap	可选	在『设备管理』→『SNMP 配置』→『Trap 开启』页面开启 Trap 功能，之后，在『设备管理』→『SNMP 配置』→『Trap 设置』页面设置 Trap 类型及目标主机。

4.1 代理设置

点击『设备管理』→『SNMP 配置』→『代理设置』进入 SNMP 代理设置页面。

以下是对页面各参数的说明：

标题项	说明
SNMP 状态	开启/关闭交换机的 SNMP 代理功能。
本地引擎 ID	显示本地 SNMP 实体的引擎 ID。开启 SNMP 代理功能后显示，不可更改。
最大包长	设置 SNMP 代理能接受/发送的 SNMP 的最大包长，默认为 1500。
联系信息	设置交换机的联系信息，便于 SNMP 管理者快速定位本交换机。一般为交换机的域名和 IP 地址。默认为 www.ip-com.com.cn。

物理位置信息	设置交换机的物理位置信息，便于 SNMP 管理者快速定位本交换机。默认为 A16J, Xiandai of Window Building, Huaqiang North Road, Futian District, ShenZhen, P.R.China
SNMP 版本	设置 SNMP 代理使用的 SNMP 版本，可同时支持 SNMP v1、v2c、v3。

点击 增加团体 ，进入创建访问团体名页面。注意：必须先创建视图才能创建团体。

以下是对页面各参数的说明：

标题项	说明
团体名	设置团体名，您可以选择使用标准团体名或自定义团体名。 **标准：** 选择“public”或“private”。 **用户自定义：** 自定义团体名，长度不能大于 31 个字符。
访问模式	选择该团体对视图的访问权限。 **只读：** 团体对相应视图具有只读权限。 **读写：** 团体对相应视图具有读写权限。
视图	选择团体可访问的视图。在『设备管理』→『SNMP 配置』→『视图管理』页面创建视图。

团体创建完成后，用户可在 SNMP 管理者端，使用 v1、v2c 版本添加的团体名，查看或设置交换机 MIB 节点信息。

4.2 用户管理

SNMP 管理者可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。

点击『设备管理』→『SNMP 配置』→『用户管理』进入用户查看、设置页面。

点击 添加 ，进入用户设置页面。注意：必须先创建组才能创建用户。

以下是对页面各参数的说明：

标题项	说明
用户名	输入用户名。
组名	选择组名。需要先在『设备管理』→『SNMP 配置』→『组管理』页面设置。 通过“组名”、“安全级别”来确定用户所属的组。
安全级别	选择安全级别。
认证模式	选择 SNMP v3 用户的认证模式，只有安全级别为 auth/priv 或 auth/nopriv 时才可设置。 none：不认证。MD5：消息摘要算法第五版。SHA：安全散列算法。
密码	输入认证密码。
确认密码	再次输入认证密码。
加密模式	选择 SNMP v3 用户的加密模式，只有安全级别为 auth/priv 时才可设

	置。 None：不加密。DES：数据加密标准。
加密模式密码	输入加密密码。
确认加密模式密码	再次输入加密密码。

4.3 组管理

配置 SNMP 的组，组内的用户通过只读、读&写、通知视图来达到访问控制的目的。点击『设备管理』→『SNMP 配置』→『组管理』进入组查看、设置页面。

点击 添加 ，进入组添加页面。注意：必须先创建视图才能创建组。

以下是对页面各参数的说明：

标题项	说明
组名	填写组名。与“安全级别”共同组成该组的标识，两项项均相同才被认为是同一组。
安全级别	选择 SNMP v3 的组的安全级别。 noauth/nopriv：不认证，也不加密。auth/nopriv：认证但不加密。 auth/priv：认证，同时加密。
只读视图	选择只读视图，对所选的视图只能被查看不能被编辑。

读写视图	选择读写视图，对所选的视图能查看和编辑。
通知视图	选择通知视图，SNMP 管理者可以接收到所选视图发送的异常警报信息。

4.4 视图管理

在 SNMP 报文中使用管理变量(OID)来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。

点击『设备管理』→『SNMP 配置』→『视图管理』进入 SNMP 视图设置页面。

点击 添加 ，进入 SNMP 视图添加页面。

以下是对页面各参数的说明：

标题项	说明
视图名称	填写视图条目的名称。
MIB 子树 OID	填写该视图条目的管理变量（OID）。
规则	选择 OID 的规则。 包括：该 OID 可以被 SNMP 管理者管理。 排除：该 OID 不能被 SNMP 管理者管理。

4.5 Trap 开启

Trap 功能用于交换机主动向 SNMP 管理者发送信息，报告一些紧急的重要的事件。点击『设备管理』→『SNMP 配置』→『Trap 开启』进入 Trap 功能全局设置页面。

默认情况下，交换机已开启所有端口的 SNMP Trap 功能，您可根据具体需要修改。

以下是对页面各参数的说明：

标题项	说明
Snmp Trap	开启/关闭 Snmp Trap 功能。
State	选择发送 Trap 消息的类型。
Coldstart-Trap	当交换机冷启动（交换机断电或重启）时，发送冷启动 Trap 信息。
Warmstart-Trap	当交换机关闭 SNMP 功能时，发送热启动 Trap 信息。
Linkdown-Trap	当端口由 up 状态变为 down 状态时，发送链路 down 的 Trap 信息。
Linkup-Trap	当端口由 down 状态变为 up 状态时，发送链路 up 的 Trap 信息。
Authentication-Trap	当 SNMP 模块认证失败时，发送认证失败的 Trap 信息。

本页面只是启用 SNMP Trap 功能，您还需要配置接收以上所述 Trap 消息的目标主机。

4.6 Trap 设置

设置接收 Trap 消息的目标主机，点击『设备管理』→『SNMP 配置』→『Trap 设置』进入页面。

点击 添加 ，进入 SNMP 目标主机设置页面。

以下是对页面各参数的说明：

标题项	说明
目标主机 IP 地址	输入目标管理主机的 IP 地址。需要与交换机管理 IP 同网段。
端口号	输入管理主机上启用供 Trap 使用的 UDP 端口，一般为 162。
团体名	输入 SNMP 管理者的团体名。对于 SNMP v3，输入 SNMP 管理者的用户名。
Trap 版本	选择交换机与 SNMP 管理者交互所使用的 SNMP 版本号，默认为 v1 版本。

5 DHCP 侦听

为了提高局域网 IP 地址管理效率，网络管理员通常会在局域网架设一台 DHCP 服务器，为网络中的客户端系统自动分配 IP 地址信息。此时，如果网络中存在多台 DHCP 服务器（用户不小心配置的或黑客冒充的），不仅会给网络造成混乱，也对网络安全造成很大威胁。

➘ DHCP 侦听的作用

DHCP 侦听（DHCP Snooping）是一种保护 DHCP 服务器的安全机制，它可以过滤来自网络中的主机或其他设备的非信任 DHCP 报文，以保证客户端能从正确的 DHCP 服务器获得 IP 地址，避免 DHCP 服务器欺骗和 DHCP 地址耗尽。

DHCP 侦听将交换机端口分为非信任端口和信任端口两种。

- 非信任端口：连接终端设备的端口，该端口客户端只能发送 DHCP 请求报文，丢弃来自该端口的其他 DHCP 报文。
- 信任端口：连接合法的 DHCP 服务器的端口或汇聚端口。

使用 DHCP 侦听会建立一个用户绑定表。一旦一个链接在非信任端口的客户端获得一个合法的 IP 地址，交换机会在用户绑定表中自动显示一个条目，包括客户端 IP/MAC 地址、交换机端口号/端口所属 VLAN、租约时间等信息，为进一步部署 MAC 源防护和 Ping 检测做基础。

➘ DHCP Option 82

Option 82 记录了 DHCP 客户端的位置信息，管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。

本交换机的 DHCP Snooping 支持 Option 82 选项，并支持两个子选项：电路 ID 子选项和远程 ID 子选项。默认情况下，本交换机中，电路 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址。

当交换机接收到 DHCP 请求报文后，将根据报文中是否包含 Option 82 以及用户配置的处理策略及用户自定义选项状态对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器。具体的处理方式如下表。

收到的 DHCP 请求报文是否带有 Option 82 选项	处理策略	用户自定义选项的状态	DHCP Snooping 对报文的处理
是	替换	启用	采用用户自定义的电路 ID 子选项和远程 ID 子选项内容填充 Option 82，替换报文中原有的 Option 82 选项信息并进行转发。
		禁用	采用本交换机默认的电路 ID 子选项和远程 ID 子选项内容填充 Option 82，替换报文中原有的 Option 82 选项信息并进行转发。
	保留	任意	保留报文中原有的 Option 82 选项信息并进行转发。
	丢弃	任意	丢弃报文。
否	任意	启用	采用用户自定义的电路 ID 子选项和远程 ID 子选项内容填充 Option 82 并进行转发。
		禁用	采用本交换机默认的电路 ID 子选项和远程 ID 子选项内容填充 Option 82 并进行转

			发。

当交换机接收到 DHCP 服务器的响应报文时，如果报文中含有 Option 82，则删除 Option 82，并转发给 DHCP 客户端；如果报文中不含有 Option 82，则直接转发。

5.1 全局设置

点击『设备管理』→『DHCP 侦听』→『全局设置』进入 DHCP 侦听全局设置页面。

以下是对页面各参数的说明：

标题项	说明
DHCP 侦听	全局开启/关闭 DHCP 侦听功能。默认情况下，DHCP 侦听功能为关闭。
源 MAC 地址检查	开启/关闭源 MAC 地址检查功能。 DHCP 消息中有两个字段储存着客户端的 MAC 地址，开启源 MAC 地址检查后，交换机将对这两个字段进行比较，如果不同，则将该消息丢弃。

5.2 端口设置

DHCP 监听全局设置完成后，您还需要进行端口设置。点击『设备管理』→『DHCP 侦听』→『端口设置』进入页面。

点击某个端口号，进入对应端口设置页面。

点击 配置 ，可批量进行端口设置。

以下是对页面各参数的说明：

标题项	说明
端口	显示对应端口的端口号。
端口属性	设置所选择端口的 DHCP 侦听属性，信任或非信任。
Option 82 选项状态	启用/禁用 DHCP 选项 82。开启了 Option82 选项，Option 82 选项策略才会生效。
Option 82 选项策略	当客户端的 DHCP 请求报文已经有 Option 82 字段时，选择对此字段的操作。 **替换：**替换数据包中的 Option 82 字段信息，替换为交换机默认的或用户自定义的选项内容。 **保留：**保留数据包中的 Option 82 字段信息。 **丢弃：**丢弃包含 Option 82 字段的数据包。
用户自定义选项	启用/禁用自定义电路、远程 ID 子选项内容功能。

电路 ID 子选项	输入用户自定义的 Option 82 选项中电路 ID 子选项的内容。
远程 ID 子选项	输入用户自定义的 Option 82 选项中远程 ID 子选项的内容。

5.3 用户绑定

点击『设备管理』→『DHCP 侦听』→『用户绑定』进入用户绑定显示页面。

以下是对页面各显示参数的说明：

标题项	说明
序号	显示本条用户绑定在列表中的数位。
IP 地址	显示本条用户绑定的 IP 地址。
MAC 地址	显示本条用户绑定的 MAC 地址。
VLAN	显示本条用户绑定的 VLAN ID。
端口	显示本条用户绑定的端口号。
租约剩余时间	显示本条用户绑定的租约剩余时间。

服务质量

本节内容可帮助您对带宽资源进行最优配置，从而提供更高质量的网络服务体验。包括以下两部分内容：

QoS 配置：针对各种网络应用的不同需求，为其提供不同的服务质量。

流量控制：限制交换机端口的带宽和广播流量，保证网络正常有效的运行。

1 QoS 配置

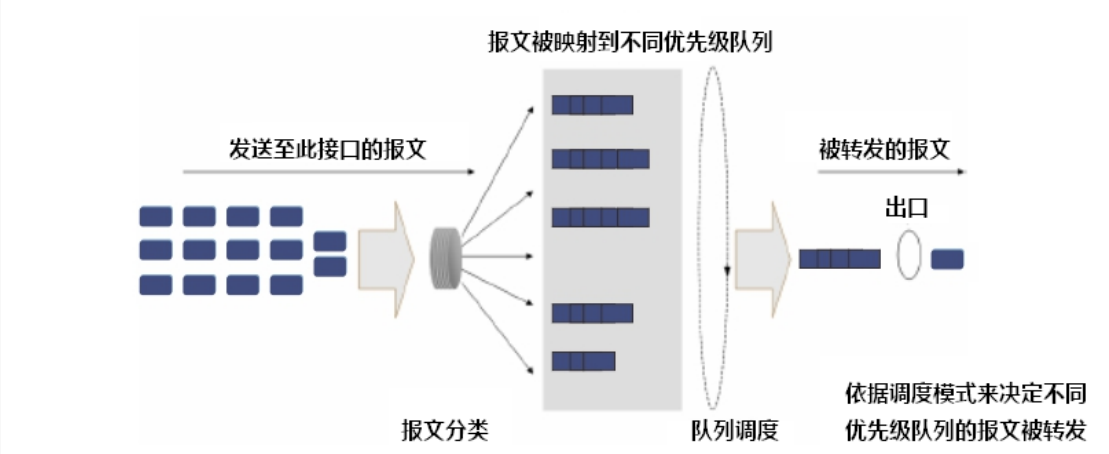
传统的 IP 网络主要承载 www、FTP、E-mail 等数据业务，网络尽最大的努力将报文送到目的地，对分组转发的延时、抖动、丢包率和可靠性等不提供任何保证。

随着 IP 技术的高速发展，以及各种新业务如远程教学、电视会议、视频点播的出现，IP 网络由一个单纯的数据网络转变为多业务承载网，它必须为其所承载的每一类业务提供相应的服务质量（QoS）。

QoS，简单的说，就是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽、减少报文传输的时延和抖动、降低报文丢包率等。

➘ QoS 工作原理

本交换机采用 DiffServ（Differentiated Service）QoS 实现模型。在入端口方向对数据流进行分类，在出端口方向将不同类型的数据流映射到不同优先级的队列，最后根据调度模式决定不同优先级队列的数据包被转发的方式。如图。



- 报文分类：采用一定的规则识别出符合某类特征的对象。
- 映射：用户根据优先级模式，将进入交换机的报文映射到不同的优先级队列中。
- 队列调度：当网络拥塞时，必须解决多种数据流同时竞争使用资源的问题，通常采用队列调度加以解决。

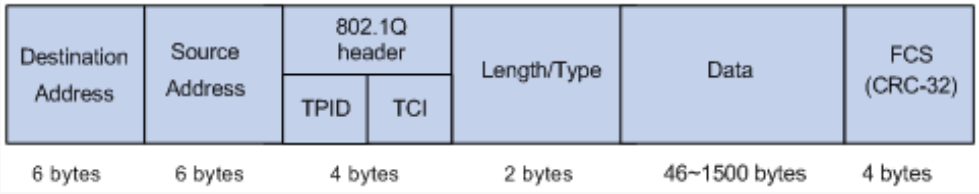
➘ 优先级模式

本交换机支持三种优先级模式：802.1P 优先级、DSCP 优先级和基于端口的优先级。

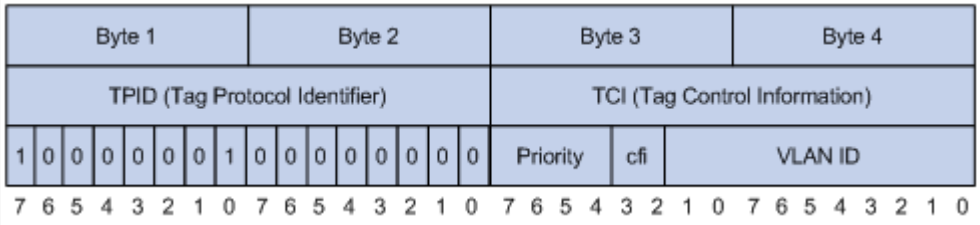
DSCP 优先级开启时，对于同时带有 COS 优先级和 DSCP 优先级的报文，将放入对应的 DSCP 优先级输出队列。如果报文仅带有 COS 优先级，将被放入对应的 COS 优先级输出队列，如果报文既不带 COS 也不带有 DSCP 优先级，将被放入端口优先级队列。

1. 802.1p 优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。带有 802.1Q 标签的数据包才带有 802.1p 优先级，如下图所示，4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID（Tag Protocol Identifier，标签协议标识，取值为 0x8100）和 2 个字节的 TCI（Tag Control Information，标签控制信息）。



下图显示了 802.1Q 标签头的详细内容，TCI 中 Priority 字段就是 802.1p 优先级，也称为 COS 优先级。它由 3 个 bit 组成，取值范围为 0~7。

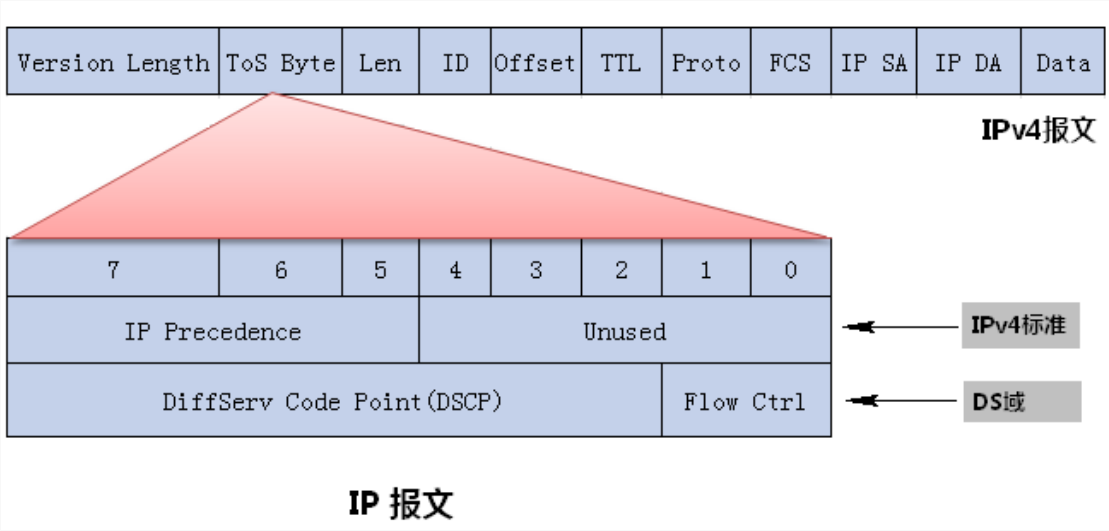


在交换机的配置页面上，可配置不同的 COS 优先级对应不同的队列。交换机发送数据帧时，会根据数据帧的 Tag（COS 优先级）对应的队列进行归队；对于 Untagged 帧，交换机则按照该入口端口的默认 COS 优先级（在『服务质量』→『QoS 配置』→『端口优先级』页面配置）对数据帧进行 QoS 处理。

本交换机默认的 802.1p 优先级与队列映射关系如下表所示。

802.1p 优先级	队列
1、2	1
0、3	2
4、5	3
6、7	4

2. DSCP 优先级



如图所示，IP 报文头部的 ToS 字段有 8 个 bit，其中：前 3 个 bit 表示 IP 优先级，取值范围为 0~7。RFC2474 重新定义了 ToS 域，称之为 DS 域，其中 DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前 6 个 bit 表示，取值范围为 0~63，后 2 个 bit 是保留位。

通过交换机的配置页面，可以配置不同的 DS 字段对应不同的 COS 优先级，交换机发送 IP 包时，会根据 IP 包的 DS 域决定发送的优先级。对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

本交换机默认 DSCP 优先级与 COS 优先级映射关系如下表所示。

DSCP 优先级	COS 优先级
0~15	1
16~31	3
32~47	5
48~63	7

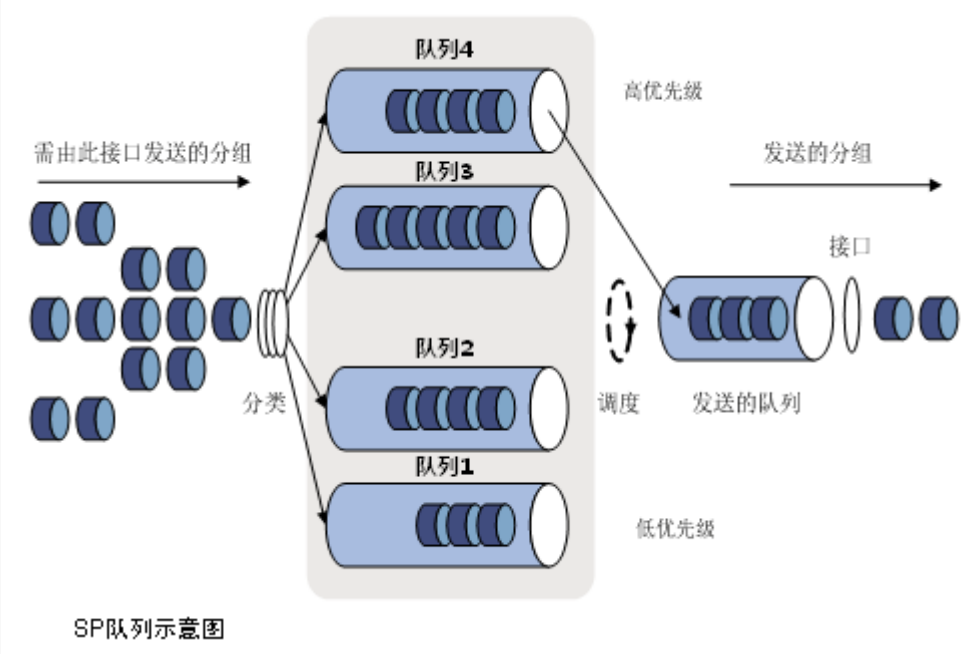
3．端口优先级

端口优先级由交换机物理端口所确定，优先级取值范围 0~7。用于数据包报文不带优先级时决定报文的转发次序。

➘ 调度方式简介

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。本交换机支持二种调度模式：严格优先级模式（SP）、加权轮询优先级模式（WRR）。

1．严格优先级队列（SP）



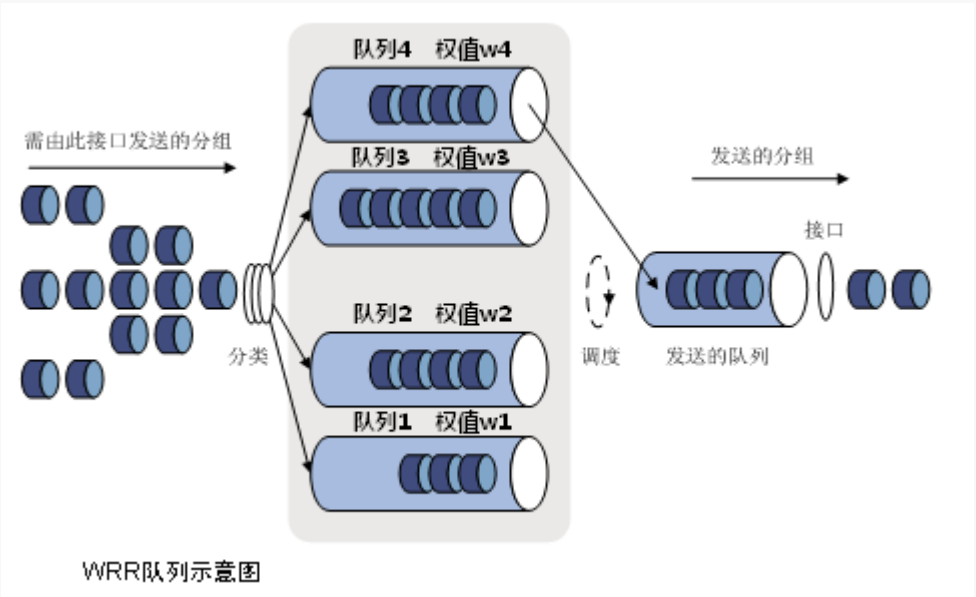
SP队列示意图

SP 队列调度算法是针对关键业务型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有 4 个输出队列为例，优先队列将端口的 4 个输出队列分成 4 类，依次为 3，2，1，0 队列，它们的优先级依次降低。

在队列调度时，SP 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如 E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

2．加权轮询优先级队列（WRR）



WRR队列示意图

WRR 队列调度算法是在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 4 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w4、w3、w2、w1），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 25、15、5、5（依次对应 w4、w3、w2、w1），这样可以保证最低优先级队列至少获得 10Mbps 带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

WRR 队列还有一个优点：虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，使带宽资源可以得到充分的利用。

1.1 调度模式

调度模式，进行交换机调度模式的选择。在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。

点击『服务质量』→『QoS 配置』→『调度模式』进入设置页面。

以下是页面各参数的说明：

标题项	说明
调度模式	选择队列调度模式：“SP”或“WRR”。 **SP**：严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。 **WRR**：加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。
队列设置	设置 WRR 队列调度模式时，各队列的权值。取值范围是 1~31。

1.2 802.1P

802.1P 优先级，交换机根据数据包是否带有 802.1Q tag 来确定所使用的优先级模式。对于带 tag 的数据包，直接应用数据包的 802.1P 优先级将数据包进行归队；对于不带 tag 的数据包，先根据端口优先级映射数据包的 COS 优先级，再将数据包进行归队。

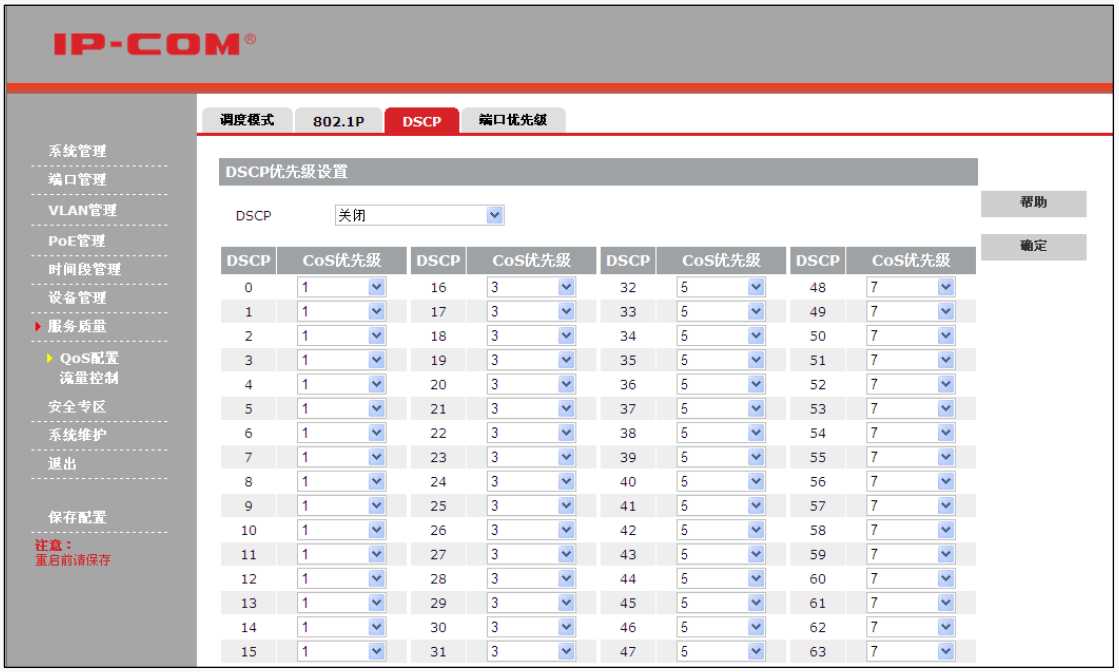
点击『服务质量』→『QoS 配置』→『802.1P』进入 802.1P 优先级设置页面。

您可根据需要修改各 COS 优先级对应的队列。之后，当端口出现拥塞时，交换机将按照所设置的映射关系，将带有 COS 优先级的数据包分配到对应的队列中。

1.3 DSCP

DSCP(DiffServ Code Point，区分服务编码点)是 IEEE 对 IP ToS 字段的重定义，利用该字段可以将 IP 报文划分为 64 个优先级。开启 DSCP 优先级后，如果转发的数据包是 IP 报文，则交换机直接应用数据包 DSCP 优先级所对应的 COS 优先级对该数据包进行归队；对于非 IP 报文，但带有 802.1Q tag 的数据包，直接应用数据包的 802.1P 优先级将数据包进行归队；对于非 IP 报文，也不带有 802.1Q tag 的数据包，先根据端口优先级映射数据包的 COS 优先级，再将数据包进行归队。

点击『服务质量』→『QoS 配置』→『DSCP』进入 DSCP 优先级设置页面。



以下是页面各参数的说明：

标题项	说明
DSCP 优先级设置	开启/关闭 DSCP 优先级。
DSCP	根据 IP 包的 DS 域（0~63）对应 COS 优先级后，再根据『服务质量』→『QoS 配置』→『802.1P』页面配置的对应关系进行归队。

1.4 端口优先级

点击『服务质量』→『QoS 配置』→『端口优先级』进入设置页面。

默认情况下，所有端口的 COS 优先级均为 0，您可根据需要修改。如图。

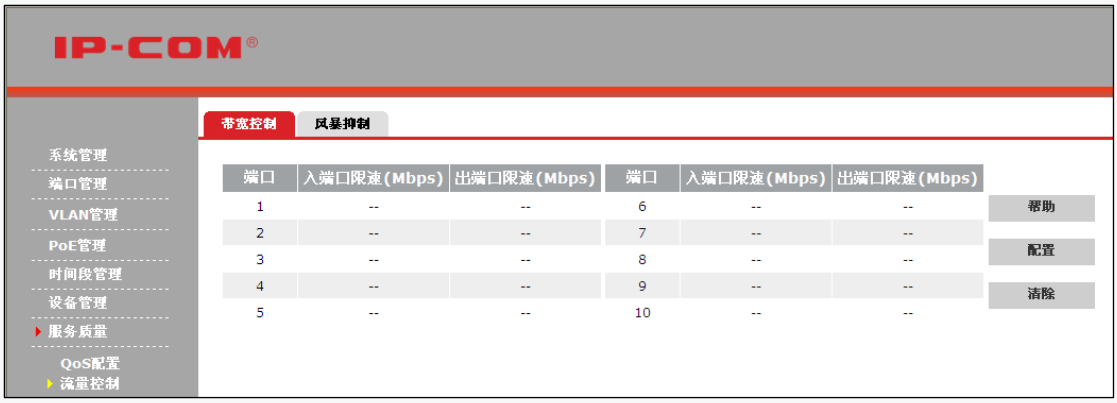
2 流量控制

流量管理用于限制交换机端口的带宽和广播流量，保证网络正常有效的运行。包括带宽控制、风暴抑制两个页面。

2.1 带宽控制

本交换机的带宽控制采用令牌桶进行流量控制。如果在交换机的某个端口上配置了带宽控制，所有经由该端口接收或发送的报文首先要经过令牌桶进行处理。如果令牌桶中有足够的令牌，则报文可以被接收或发送；否则，报文将被丢弃。

点击『服务质量』→『流量控制』→『带宽控制』，进入带宽控制主页面。



默认情况下，所有端口没有进行带宽限制，您可根据需要，点击对应端口项或 配置 后，进入页面设置端口带宽限制。

以下是对页面各参数的说明：

标题项	说明
入端口限速（Mbps）	配置端口接收数据时的带宽，取值范围<1~1000>，默认为 1000（即不限速）。
出端口限速（Mbps）	配置端口转发数据时的带宽，取值范围<1~1000>，默认为 1000（即不限速）。

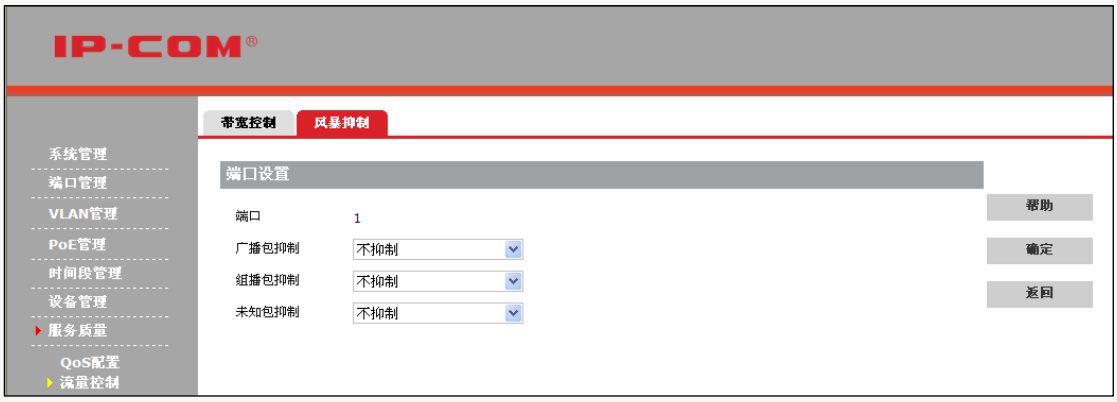
2.2 风暴抑制

作为发现未知设备的主要手段，广播在网络中起着非常重要的作用。随着网络中计算机数量的增多，广播包的数量会急剧增加，网络长时间被大量的广播数据包所占用，当广播数据包的数量达到 30%时，网络的传输速率将会明显下降，使正常的点对点通信无法正常进行，导致网络性能下降，甚至网络瘫痪，造成广播风暴。

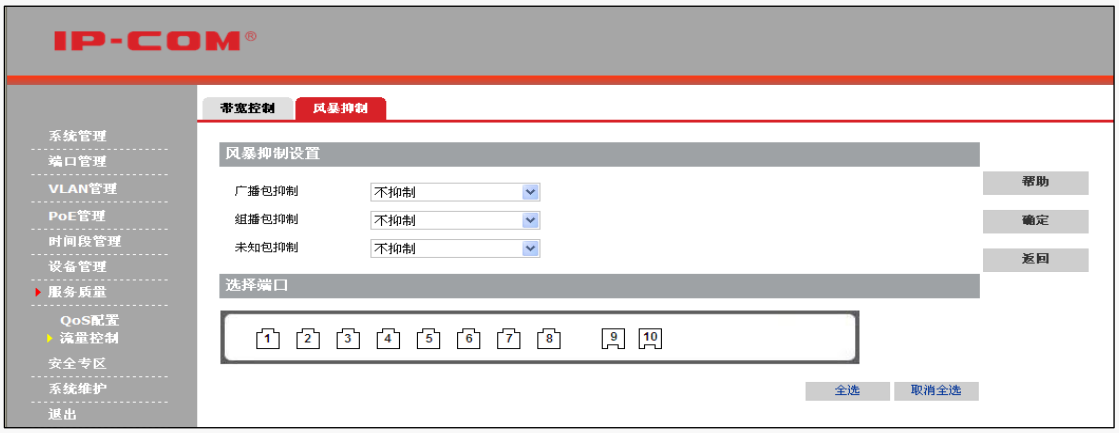
本交换机支持风暴抑制功能，当端口上的广播/组播/未知单播流量超出您设定的值后，交换机将丢弃超出广播/组播/未知单播流量限制的报文，从而使端口广播/组播/未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

点击『服务质量』→『流量控制』→『风暴抑制』进入设置页面。

单端口风暴抑制设置：点击对应端口项，进入页面设置即可。



批量端口风暴抑制功能设置：点击 配置 ，进入页面设置即可。



以下是对页面各参数的说明：

标题项	说明
广播包抑制	启用/禁用相应端口的广播包（目的 MAC 为 FF:FF:FF:FF:FF:FF 的数据包）抑制功能。 启用时，您需要输入对应的广播包抑制带宽速率，取值范围〈128~50000〉，单位 Kbps。
组播包抑制	启用/禁用相应端口的组播包（目的 MAC 的第 8 位为 1 的数据包）抑制功能。 启用时，您需要输入对应的组播包抑制带宽速率，取值范围〈128~50000〉，单位 Kbps。
未知包抑制	启用/禁用相应端口的未知单播包（交换机 MAC 表中没有该单播包的目的 MAC 条目）抑制功能。 启用时，您需要输入对应的未知单播包抑制带宽速率，取值范围〈128~50000〉，单位 Kbps。

安全专区

本节内容可帮助您为局域网安全提供保障。包括以下两部分内容：

MAC 过滤：控制局域网计算机访问网络。

802.1X：在局域网设备的端口级对接入用户进行认证控制，保障局域网设备和资源安全。

1 MAC 过滤

设置 MAC 地址过滤后，交换机将会对进入端口的数据包的源 MAC 和目的 MAC 进行检查，如果该数据包的源 MAC 或目的 MAC 在 MAC 过滤表中存在，将丢弃该数据包。

点击『安全专区』→『MAC 过滤』，进入 MAC 地址过滤设置页面。

添加需要过滤的 MAC 地址：

1. 点击 添加，进入添加过滤 MAC 地址页面；
2. 在 VLAN 栏输入 MAC 地址对应的 VLAN（前提：该 VLAN 已存在）；

提示

端口 VLAN 模式下无需 2 步骤。

3. 按页面提示格式在 MAC 地址栏输入要过滤的 MAC 地址；

4. 点击 确定，自动返回到过滤 MAC 地址显示页面。

提示

- 静态 MAC 地址表项中的 MAC 地址不能添加为过滤 MAC 地址。
- 如果任意端口开启了 802.1X 认证功能，MAC 地址过滤功能将不生效。

2 802.1X

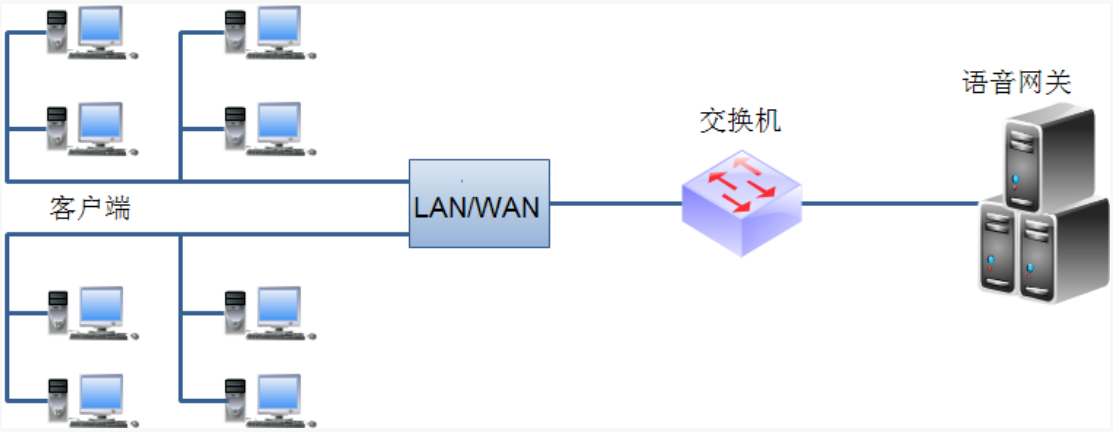
IEEE 802 LAN 协议定义的局域网不提供认证，只要用户接入了局域网设备（如传统的局域网交换机），就可以访问局域网中的设备和资源，这是一个安全隐患。

802.1X 是 IEEE 提出的基于端口的网络接入控制技术，它可以在局域网设备的端口级对接入用户进行认证控制。

本交换机可以对网络中的计算机进行 802.1X 认证，连接在交换机端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，就不能访问局域网中的资源。

802.1X 体系结构

802.1X 系统采用典型的 Client/Server 体系结构，包括客户端（Client）、设备端（Device）和认证服务器（Server）三个实体。如图所示。



- 客户端：局域网中的一个实体，多为普通计算机，用户通过客户端软件发起 802.1X 认证，由设备端对其进行认证。客户端必须支持 EAPOL（Extensible Authentication Protocol over LAN）。

- 设备端：局域网中的另一个实体，如本交换机，它为客户端提供接入局域网的物理/逻辑端口，并对客户端进行认证。
- 认证服务器：为设备端提供认证服务的实体，实现对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service）服务器。

➘ 802.1X 重认证功能

802.1X 重认证是通过定时器或报文触发，对已经认证成功的用户进行一次重新认证，检测用户当前的连接状况。如果接入用户在一定时间内未响应重认证报文，则切断与该用户的连接。若用户希望再次连接，则必须通过客户端软件重新发起 802.1X 认证。

➘ 802.1X 接入认证方式

本交换机支持协议所规定的基于端口的接入认证方式。只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源；但是当第一个用户下线后，其它用户也会被拒绝使用网络。

802.1X 包括全局设置、端口设置、端口统计三个页面。

2.1 全局设置

点击『安全撞去』→『802.1X』→『全局设置』，进入 802.1X 全局设置页面。

以下是对页面各参数的说明：

标题项	说明
全局模式	开启/关闭全局 802.1X 功能。默认情况下，全局 802.1X 功能为关闭。 **提示** 必须同时开启全局和端口的 802.1X 功能后，端口 802.1X 配置才能生效。
认证服务器 IP 地址	设置 Radius 认证服务器的 IP 地址，需要与交换机管理地址同网段。

授权共享密钥	设置 Radius 认证/授权报文的共享密钥，此密钥需要与本交换机对接的 Radius 认证/授权服务器侧设置的密钥一致。
重认证	设置所有端口的重认证状态：开启或关闭。
重认证超时定时器	如果端口开启了重认证功能，交换机端以此定时器设置的时间间隔为周期对该端口在线用户发起重认证。
客户端超时定时器	当交换机向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到客户端的响应，交换机将重发该报文。

2.2 端口设置

801.1X 全局设置完成后，您还需要进行 802.1X 端口设置。点击『安全专区』→『802.1X』→『端口设置』进入页面。

单个端口 802.1X 功能设置：点击对应端口项，进入页面设置即可。

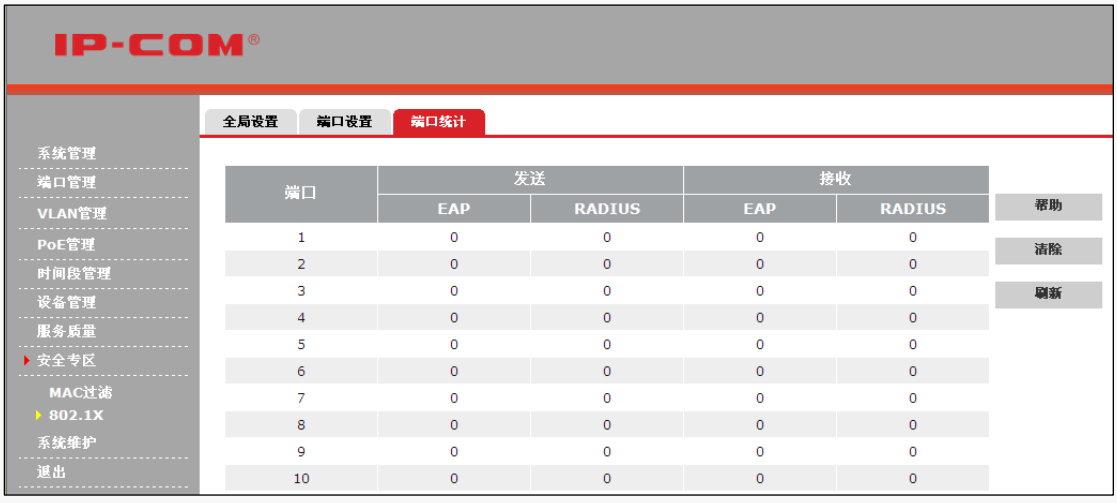
批量端口 802.1X 功能设置：点击 配置 ，进入页面设置即可。

以下是对页面各参数的说明：

标题项	说明
模式	开启/关闭端口 802.1X 认证功能。
端口控制方式	选择 802.1X 端口控制方式。 **自动：**端口初始状态为非授权状态，仅允许 EAPoL 报文收发，不允许用户访问网络资源；如果认证通过，则端口切换到授权状态，允许用户访问网络资源。 **强制授权：**端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。 **强制非授权：**端口始终处于非授权状态，不允许用户访问网络资源。默认情况下，端口控制方式为强制受权。

2.3 端口统计

查看、清空 802.1X 端口统计信息，点击『安全专区』→『802.1X』→『端口统计』进入页面。



系统维护

本节内容可帮助您了解交换机运行状态，并提供网络故障诊断的方法：

系统日志：查看系统日志，监控网络运行情况，必要时，依据该信息进行网络故障诊断。

网络诊断：故障发生时，通过线缆/Ping/Tracert 检测定位故障点。

1 系统日志

本交换机提供的日志系统能够对所有的系统信息进行记录、分类和管理，为网络管理员监控网络运行情况和诊断网络故障提供了强有力的支持。

本交换机的系统日志信息按重要性划分为八种等级，您可按等级进行信息过滤。系统信息的信息级别值越小，紧急程度越高。具体如下：

信息级别	数值	描述
Emergency	1	系统不可用信息。
Alert	2	需要立刻做出反应的信息。
Critical	3	严重信息。
Error	4	错误信息。
Warning	5	警告信息。
Notice	6	正常出现但是重要的信息。
informational	7	需要记录的通知信息。
debug	8	调试过程产生的信息。

1.1 日志信息

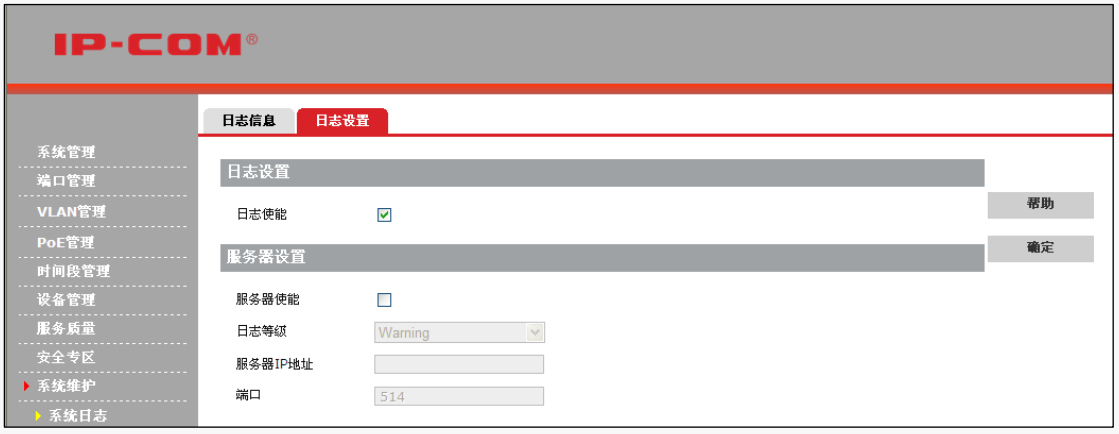
查看、下载交换机系统日志，点击『系统维护』→『系统日志』→『日志信息』进入页面。

为了方便您实时监控网络运行情况及诊断网络故障，建议您到『系统管理』→『系统配置』→『系统时间』页面设置交换机的系统时间，使得系统日志能获取到正确的时间。

1.2 日志设置

启用/禁用系统日志，设置远程日志功能。远程日志功能可以将本交换机的系统日志发送到指定 IP 地址的日志服务器上，方便网络管理员对交换机产生的日志信息进行集中监控和管理。

点击『系统维护』→『系统日志』→『日志设置』进入页面。



以下是对页面各参数的说明：

标题项	说明
日志使能	启用/禁用系统日志功能。默认为启用。
服务器使能	启用/禁用远程日志功能。默认为禁用。
日志等级	设置发送到日志服务器的日志的级别，只有高于此指定级别的日志信息

	才会发送到日志服务器。
服务器 IP 地址	输入日志服务器的 IP 地址。
端口	显示发送/接收系统日志时所用到的 UDP 端口号，默认为 514，不能修改。

提示

为了保证系统日志能发送到远程日志服务器，您需要在『系统管理』→『系统配置』→『系统信息』设置本交换机的 IP 地址、子网掩码和网关，使交换机和远程日志服务器路由可达。

2 网络诊断

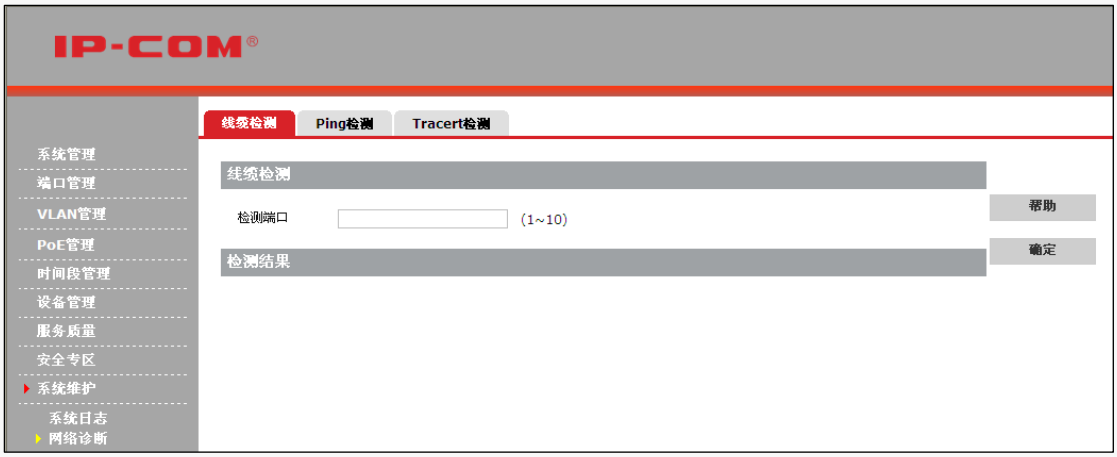
网络诊断用于定位网络故障点，包括线缆检测、Ping 检测、Tracert 检测三个页面。

2.1 线缆检测

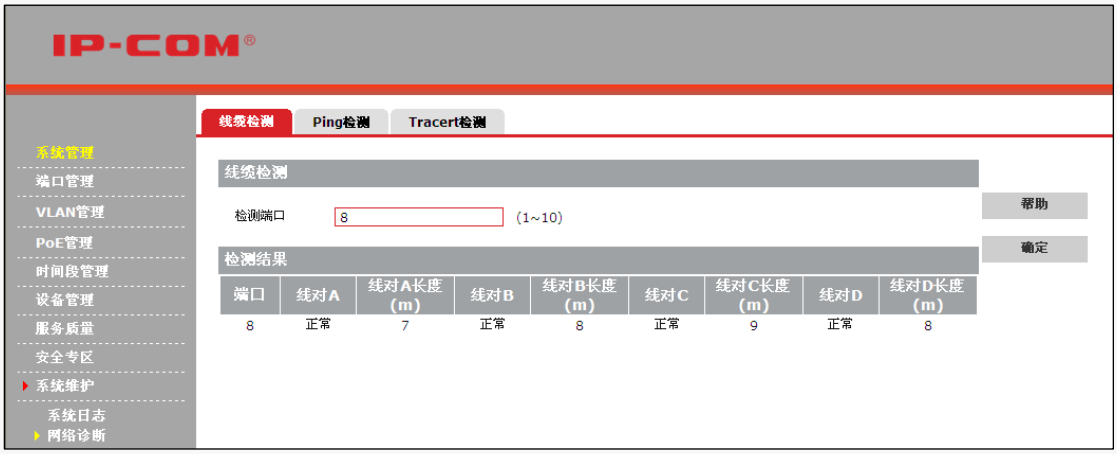
本交换机可以检测出各个以太网端口的当前线缆连接状况，检测内容包括线缆中 A，B，C，D 线对的状态及长度。点击『系统维护』→『网络诊断』→『线缆检测』，进入线缆检测页面。

提示

- 线对的长度是指线缆绕对的长度，不是线缆表皮的长度，检测长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。



您只需要在“检测端口”栏输入需要检测的端口号，再点击 确定 ，检测信息即可显示在“检测结果”栏。



2.2 Ping 检测

Ping 检测功能可以检测本交换机与指定地址的设备是否可达，方便网络管理员检查网络的连通性，定位网络故障。

Ping 检测过程及原理：

1. 交换机向目标设备发送 ICMP 请求（ECHO-REQUEST）报文；
2. 根据是否收到目标设备返回的 ICMP 回显应答(ECHO-REPLY)报文来判断网络是否正常。

如果网络正常，则目标设备在接收到 ICMP 请求报文后，向交换机返回 ICMP 应答报文，并显示相关统计信息；如果网络工作异常，交换机将显示目的地址不可达或超时等提示信息。

进行 Ping 检测：

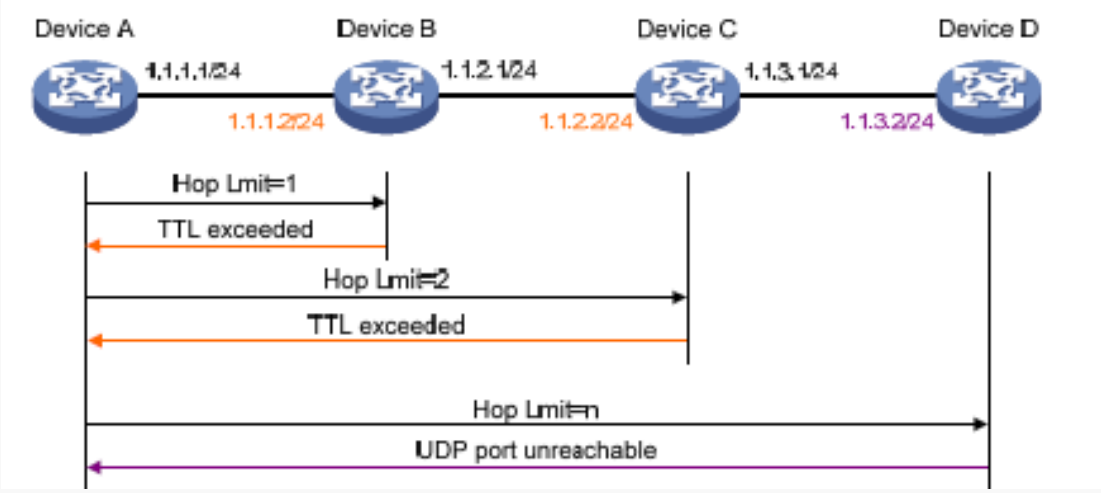
1. 进入『系统维护』→『网络诊断』→『Ping 检测』页面；
2. 输入各项参数后，点击 确定 。

以下是对页面各参数的说明：

标题项	说明
目标 IP 地址	设置 Ping 测试的目标设备的 IP 地址。
发送次数	设置交换机发送 ICMP 请求报文的个数，范围<1~10>，默认为 4 个。
发送报文长度	设置交换机发送 ICMP 请求报文的数据长度，单位为字节。范围<18~512>，默认为 56 字节。
时间间隔	设置交换机发送 ICMP 请求报文的时间间隔，单位为毫秒。范围<100~1000>，默认为 100 毫秒。
Ping 结果	显示 Ping 测试结果。

2.3 Tracert 检测

Tracert 检测可以查看交换机到目标设备之间所经过的路由器。当网络出现故障时，可以使用该命令分析出现网络故障的节点。Tracert 原理如下图所示：



Tracert 检测过程：

1. 交换机（Device A）发送一个 TTL 为 1 的报文给目标设备（Device D）；
2. 第一跳（Device B，即该报文所到达的第一个路由器）回应一个 TTL 超时的 ICMP 报文（该报文中含有第一跳的 IP 地址 1.1.1.2），这样交换机就得到了第一个路由器的地址（1.1.1.2）；
3. 交换机重新发送一个 TTL 为 2 的报文给目标设备；
4. 第二跳（Device C）回应一个 TTL 超时的 ICMP 报文，这样交换机就得到了第二个路由器的地址（1.1.2.2）；
5. 重复以上过程直到该报文到达目标设备，交换机就得到了从它到目标设备所经过的所有路由器的地址。

进行 Tracert 检测：

1. 进入『系统维护』→『网络诊断』→『Tracert 检测』页面；

❷ 输入各项参数后，点击 确定 。

以下是对页面各参数的说明：

标题项	说明
目标 IP 地址	Tracert 检测的目标设备的 IP 地址。
最大跳数	Tracert 检测所能经过的最多路由器的个数，范围<1~30>。默认为 3 个。
Tracert 结果	显示 Tracert 检测结果： • 当设备之间路由可达时，显示经过的路由器的 IP 地址。 • 当设备之间路由不可达时，将会显示如以下信息： 1 * * * request timed out 2 * * * request timed out 3 * * * request timed out

退出

如果您想要安全退出交换机 Web 网管，请点击页面左侧导航栏的“退出”。

您也可以直接关闭浏览器窗口，安全退出交换机 Web 网管。

注意

仅关闭浏览器选项卡时，已登录到交换机上的用户并不能自动退出登录。

保存配置

管理交换机的配置信息，点击『保存配置』进入页面。

保存当前配置

如果您想要交换机重启后，不丢失当前配置信息，请点击页面的 保存... ，保存当前配置。

注意

断电后重新上电、恢复出厂设置、软件升级等操作都会使交换机重启。

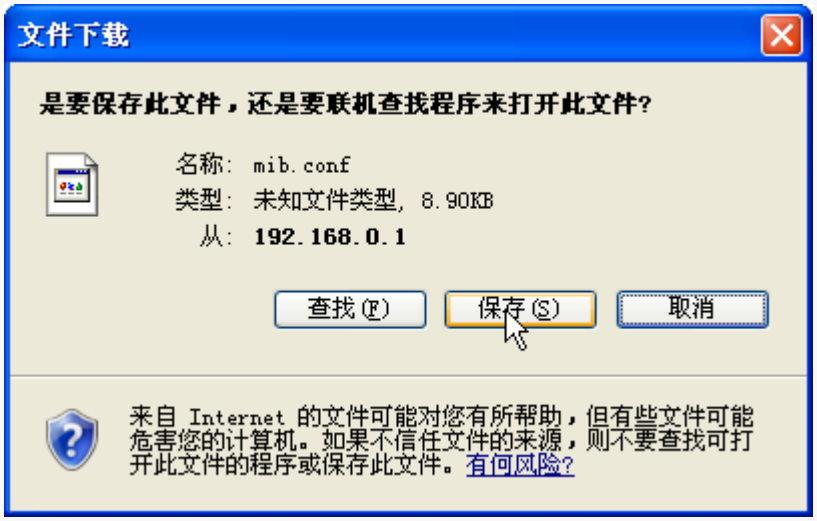
备份当前配置

如果您对交换机进行了大量的配置，使得交换机在运行时拥有更佳的状态、性能或更符合对应场景的需求，建议您对现有配置进行备份，方便故障后问题排查并节省下次配置时间。

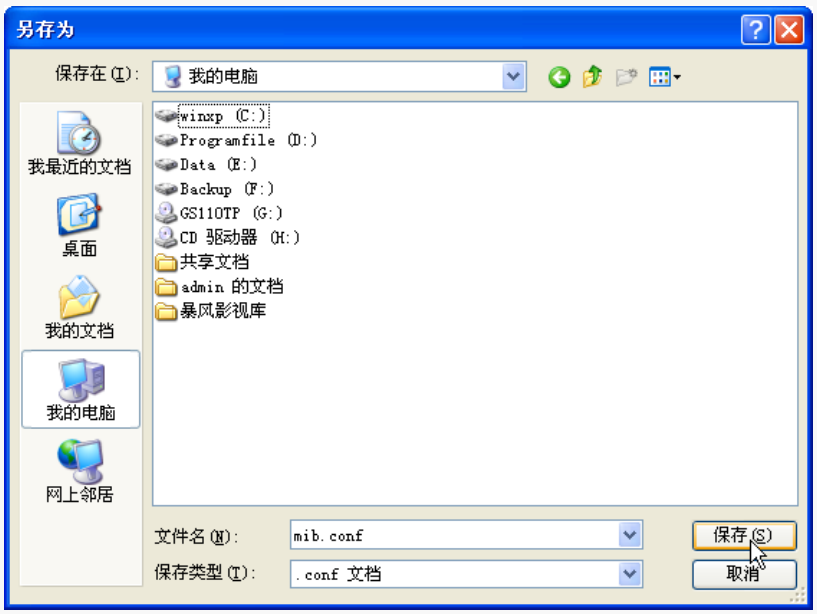
备份当前配置步骤：

1. 点击 备份... ；

2. 弹出【文件下载】对话框，点击 保存 ；



3 选择文件保存在本地计算机的路径后，点击 保存 。



提示

配置文件的默认文件名为“mib.conf”，便于记忆，您可以修改文件名（mib），但为防止恢复配置出现问题，请不要修改文件后缀（.conf）。

恢复配置

如果您需要对多台交换机进行相同的配置，或您不注意进行了某些操作，导致交换机性能下降，此时，您可以使用恢复配置功能，将交换机配置还原到之前备份的配置。

恢复设置步骤：

点击 浏览... ，选择加载您之前备份的配置文件后，点击 恢复... ，之后按页面提示操作即可。

第 V 部分

附录

常见问题处理

1. 电源系统故障处理

您可以根据前面板上的 Power 指示灯来判断交换机电源系统是否故障。电源系统工作正常时，Power 指示灯应保持常亮；如果 Power 指示灯不亮，请进行如下检查：

- 交换机电源线是否连接正确，电源开关是否为开启状态；
- 输入电压是否与交换机所要求的输入电压一致。

2. Link/Act 指示灯不亮时，可能出现的故障及排除方法：

- 交换机与远端设备未连接好，请用网线连接好两端设备；
- 网线长度超过标准距离，请设法减少设备间的网线长度到标准距离以内（≤100 米）。

3. PoE/Status 指示灯不亮时，可能出现的故障及排除方法：

- 交换机与远端设备未连接好，请用网线连接好两端设备；
- 网线长度超过标准距离，请设法减少设备间的网线长度到标准距离以内（≤100 米）；
- 登录到交换机 Web 网管后，进入『PoE 管理』→『端口设置』页面查看是否已禁用该端口的 PoE 供电功能。

技术规格参数

➘ 硬件规格

项目	规格
输入电压	100-240V AC，50/60Hz
功耗	空载时，整机功耗约17W
	PoE满负荷时，整机功耗约128W
PoE	8个10/100/1000Mbps自适应RJ45端口，支持PoE供电，单端口最大可输出40W； 支持动态分配功耗，最多可同时支持8个IEEE 802.3af标准（15.4W）或4个IEEE 802.3at标准（30W）的受电设备；
业务端口描述	8个10/100/1000Mbps自适应RJ45端口，2个1000Mbps SFP端口
工作|存储温度	-10℃ ~ 45℃	-40℃ ~ 70℃
工作|存储湿度	10% ~ 90% RH（无凝结）	5% ~ 90% RH（无凝结）
安全规范	UL 60950-1 CAN/CSAC22.2 No 60950-1 IEC 60950-1 EN 60950-1/A11 AS/NZS 60950-1
EMC	EN 55024;1998+A1:2001+A2:2003 EN 55022:2006 EN 61000-3-2:2000+A1:2001+A2:2005 EN 61000-3-3:1995+A1:2001+A2:2005 AS/NZS CISPR 22:2004 FCC PART 15:2005
MTBF	> 100,000小时
外形尺寸	294mm*178mm*44mm
重量	< 2千克

➘ 软件规格

项目	规格
交换容量(全双工)	20Gbps
包转发率(整机)	14.88Mpps
MAC 地址表	8K
VLAN	1. 支持基于端口的 VLAN 划分，最大可设置 10 组 2. 支持 IEEE 802.1Q VLAN，最大可设置 64 组 3. 支持 Voice VLAN
DHCP	1. 支持 DHCP Snooping 3. 支持 DHCP Client
组播	1. 支持 IGMP Snooping V1/V2 2. 支持最多 200 个组播组 3. 支持端口快速离开模式设置
广播风暴抑制	1. 支持基于端口的广播风暴抑制 2. 支持基于端口的组播风暴抑制 3. 支持基于端口的未知单播风暴抑制
STP(生成树)	1. 支持 IEEE 802.1d 生成树 2. 支持 IEEE 802.1w 快速生成树 3. 支持边缘端口 4. 支持 P2P 端口 5. 支持生成树 BPDU 报文统计
MAC 过滤	1. 支持单播 MAC 地址过滤 2. MAC 过滤最大可以配置 64 条
QoS	1. 支持 802.1P 端口信任模式 2. 支持 IP DSCP 端口信任模式 3. 支持带宽限制 4. 最大可以支持 4 个队列服务质量映射
认证	支持基于端口的 IEEE 802.1X 认证
加载与升级	支持 HTTP 升级
管理	1. 支持 SNMP（Simple Network Management Protocol）

	2. 支持 Web 管理
端口管理	端口设置：包括端口速率设置和显示、流控设置、隔离设置、Jumbo 帧设置（1518-9216） 端口镜像：实现端口入方向、出方向、出和入方向的镜像 端口统计：显示端口接收和发送数据个数 端口汇聚：实现静态汇聚和 LACP，最多支持 2 个汇聚组，每个汇聚组的端口数范围为 2-8
PoE	1. 支持 IEEE 802.3at 标准 PoE 供电 2. 支持 IEEE 802.3af 标准 PoE 供电 3. 最大供电功耗支持 115W
时间段管理	支持绝对时间、周期时间、片段时间叠加，可应用于 PoE 供电。最多可支持 16 个时间段，每个时间段最多可添加 4 个时间片段
维护	支持 Ping\Tracert\线缆检查

电子信息产品有毒有害物质申明

电子信息产品有毒有害物质申明

部件名称	有毒有害物质或元素					
	铅（pb）	汞（Hg）	镉（Cd）	六价铬（Cr6+）	多溴联苯（PBB）	多溴二苯醚（PBDE）
结构件	×	○	○	○	○	○
单板/电路模块	×	○	○	○	○	○
电源适配器	×	○	○	○	○	○
线缆	×	○	○	○	○	○
连接器	×	○	○	○	○	○
附件	×	○	○	○	○	○

1. “○”表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006标准规定的限量要求以下。
2. “X”表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006标准规定的限量要求。
3. 由于中国限量标准中没有豁免条例，故标识为“X”并不一定表示为对人体有害。
4. 对生产制造的产品，可能包含这些欧洲豁免的物质。
5. 在所售产品中可能包含所有部件也可能不包含所有部件。

免责声明：

此为工业级产品，非用户端设备。在生活环境中，该设备可能会造成无线电干扰。在这种情况下，可能需要用户对干扰采取切实可行的措施。