www.ip-com.com.cn

Web 配置指南

智能型 PoE 供电交换机

IP-COM

无线网络解决方案专家

声明

版权所有©2020 深圳市和为顺网络技术有限公司。保留一切权利。

未经本公司书面许可，任何单位或个人不得擅自复制、摘抄及翻译本文档部分或全部内容，且不得以任何形式传播。

IP-COM 是深圳市和为顺网络技术有限公司在中国和（或）其它国家与地区的注册商标。其它品牌和产品名称均为其相应持有人的商标或注册商标。

由于产品版本升级或其它原因，本文档内容会不定期更新。除非另有约定，本文档仅作为使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

前言

感谢选择 IP-COM 产品。开始使用本产品前，请先阅读本手册。

适用型号

本手册适用于 IP-COM 以下型号的交换机，具体产品图和软件截图以实物为准。文中如无特别说明，均以 F1218P-16-250W 为例。

型号	产品名称
F1218P-16-250W	16 口百兆+2GE/1SFP 智能型 PoE 交换机
F1226P-24-410W	24 口百兆+2GE/1SFP 智能型 PoE 交换机

约定

本文用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
按钮	边框+底纹	点击 确定 。

本文用到的标识说明如下。

标识	含义
注意	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
提示	表示有助于节省时间或资源的方法。

相关资料获取方式

访问 IP-COM 官方网站 http://www.ip-com.com.cn，搜索对应产品型号，可获取最新的产品资料。

产品资料一览表

文档名称	概述
Web 配置指南	帮助您了解交换机的更多功能配置。包括交换机管理页面上的所有功能介绍。
产品彩页	帮助您了解交换机的基本参数。包括产品概述、产品特性、产品规格等。
快速安装指南（或安装手册）	帮助您快速设置交换机联网。包括交换机的安装、上网设置指导、指示灯/接口/按钮说明、常见问题解答、保修条款等。

技术支持

如需了解更多信息，请通过以下方式与我们联系。

40066-50066	ip-com@ip-com.com.cn	http://www.ip-com.com.cn

目录

1 设备登录 1

1.1 登录 Web 管理页面 1

1.2 退出登录 3

1.3 Web 管理页面介绍 4

2 系统管理 5

2.1 系统信息 5

2.2 用户管理 7

2.3 恢复缺省配置 8

2.4 重启动 9

2.5 软件升级 10

3 端口管理 13

3.1 端口设置 13

3.2 端口镜像 16

3.2.1 概述 16

3.2.2 配置端口镜像 16

3.2.3 端口镜像配置举例 18

3.3 端口统计 20

3.4 端口限速 21

4 链路汇聚 22

5 网络延长 24

6 PoE 管理 26

7 VLAN 管理 28

7.1 概述 28

7.2 端口 VLAN 31

7.2.1 配置向导 31

7.2.2 配置端口 VLAN 31

7.2.3 端口 VLAN 配置举例 36

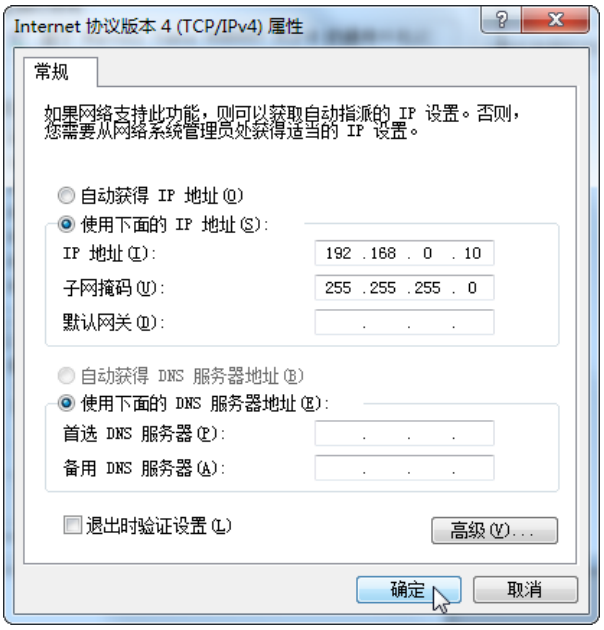
7.3 一键 VLAN 39

7.3.1 配置向导 39
7.3.2 配置一键 VLAN 39
7.4 802.1Q VLAN 41
7.4.1 配置向导 41
7.4.2 配置 802.1Q VLAN 41
7.4.3 802.1Q VLAN 配置举例 46
8 设备管理 49
8.1 MAC 绑定 49
8.1.1 概述 49
8.1.2 配置 MAC 绑定 50
8.1.3 MAC 绑定配置示例 51
8.2 QoS 配置 53
8.2.1 概述 53
8.2.2 配置 QoS 54
8.3 STP 配置 56
8.3.1 概述 56
8.3.2 STP 全局设置 59
8.3.3 端口设置 62
8.4 IGSP 配置 65
8.5 SNMP 配置 67
8.5.1 概述 67
8.5.2 配置 SNMP 68
8.5.3 SNMP 配置举例 70
9 退出 73
10 配置管理 74
10.1 备份系统配置信息 74
10.2 从文件中恢复配置信息 75

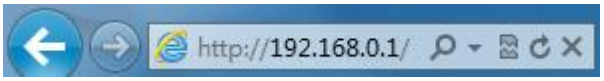
1 设备登录

1.1 登录 Web 管理页面

1. 用网线连接电脑和交换机的下联端口；
2. 将电脑的本地连接 IP 地址设置为和交换机的 IP 在同一网段的不同 IP 地址“192.168.0.X”（X 为 2~254，且未被其他设备占用），子网掩码为 255.255.255.0；



3. 打开电脑上的浏览器(以 IE 为例)，在地址栏输入交换机的 IP 地址“192.168.0.1”，然后按“Enter”键；



4. 进入交换机的 Web 登录页面，输入用户名和密码（默认均为 **admin**），然后点击 登录 。

---完成

成功登录到交换机的 Web 管理页面，可以在此查看或者修改交换机的配置信息。

1.2 退出登录

点击管理页面左边导航栏的「退出」，即可安全地退出交换机的 Web 管理页面。

1.3 Web 管理页面介绍

Web 管理页面共分为：一&二级导航栏、三级导航栏和配置区三部分，如下图所示。

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 管理页面功能菜单。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。

提示

点击页面右上角的 帮助 ，可以查看页面设置的简单介绍。

2 系统管理

2.1 系统信息

在这里，可以查看交换机的基本信息，设置交换机的 IP 地址信息及 MAC 老化时间。

点击「系统管理」进入页面。

参数说明

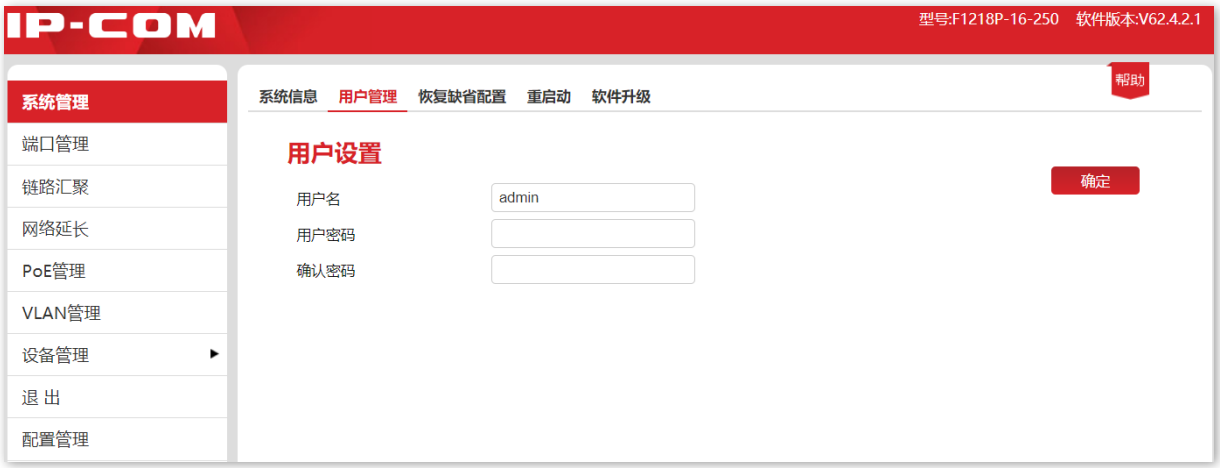
标题项	说明
软件版本	显示交换机软件的版本信息以及发布时间。
硬件版本	显示交换机的硬件版本。
MAC 地址	显示交换机的物理地址。

标题项	说明
管理 VLAN	显示交换机的管理 VLAN 为 1，不支持修改。此参数只在交换机 VLAN 模式为 802.1Q VLAN 时有效。 注意 只有连接到管理 VLAN 成员端口（且端口的 PVID 为 1）的电脑，才可以访问交换机。
设备名称	显示交换机的产品型号，如 24+2G 智能型 PoE 交换机的设备名称为“TEF1226P-24-410”。
DHCP 客户端	开启/关闭交换机的 DHCP 客户端功能。 – 开启：此时，交换机自动从网络中的 DHCP 服务器获得 IP 地址、子网掩码和网关。 – 关闭：此时，需手动设置交换机的 IP 地址、子网掩码和网关，用于设备管理和联网。 注意 开启 DHCP 客户端后，下次登录交换机 Web 管理页面前，您必须到 DHCP 服务器查看交换机获得的 IP 地址，再用该 IP 地址进行登录。
IP 地址	交换机的 IP 地址。默认值为 192.168.0.1，关闭 DHCP 客户端时，可以修改此值。 该 IP 地址也是交换机的管理 IP 地址，可通过该 IP 地址登录到交换机的 Web 管理页面。 注意 修改 IP 地址后，需要更改管理电脑的 IP 地址，使其和新的 IP 在相同网段，并使用新的 IP 地址才能重新登录到交换机的 Web 管理页面。
子网掩码	交换机的子网掩码。默认值为 255.255.255.0，关闭 DHCP 客户端时，可以修改此值。
网关	交换机的默认网关地址。关闭 DHCP 客户端时，可以修改此值。
MAC 老化时间	交换机动态 MAC 地址的老化时间，建议使用默认值“300 秒”。 提示 老化时间过短会造成动态 MAC 地址表刷新过快，大量接收到的数据包的目的地址在地址表中找不到，导致交换机只能广播这些数据包到所有端口而降低交换机的性能； 老化时间过长会造成动态 MAC 地址表中保存太多过时的地址表项，会耗尽地址表资源，导致交换机无法根据网络的变化更新地址表。

2.2 用户管理

在这里，可以修改 Web 管理页面的登录用户名和登录密码，防止非授权用户进入交换机的 Web 管理页面更改设置，影响网络正常使用。

点击「系统管理」>「用户管理」进入页面。



操作步骤：

1. 用户名：输入 1~15 个字符，只能包含英文字母、数字和下划线，且以字母开头；
2. 用户密码：输入 1~15 个字符，由字母、数字、下划线及连字符组成；
3. 确认密码：再次输入用户密码；
4. 点击 确定 。

   ---完成

设置完成之后，交换机将自动重新启动。下次登录交换机的 Web 管理页面时，需要使用新的用户名和密码才能登录。

2.3 恢复缺省配置

如果您忘记了交换机的登录 IP 地址或登录用户名/密码或者交换机出现了无法定位的问题时，可以将交换机恢复缺省配置，然后再配置。

提示

- 恢复缺省配置后，交换机的登录 IP 地址为“192.168.0.1”，登录用户名、密码均为“admin”。
- 恢复缺省配置后，交换机的所有配置恢复至出厂状态，您需要重新进行设置，请谨慎使用恢复出厂设置操作。

操作方法一：

在「系统管理」>「恢复缺省配置」页面中，点击 恢复 。

当 SYS 指示灯重新闪烁时，恢复缺省配置成功。

操作方法二：

交换机 SYS 指示灯呈闪烁状态时，使用持续按住机身前面板上的 RESET 按钮约 8 秒，待 SYS 指示灯熄灭时松开。当 SYS 指示灯重新闪烁时，交换机恢复缺省配置成功。

2.4 重启动

重启交换机可释放交换机部分缓存、清除无用报文，为交换机保持高性能运转提供保障。某些时候，重启交换机还能解决一些如死锁、无法登录交换机 Web 管理页面等问题。

点击「系统管理」>「重启动」进入页面。

注意

在交换机重启动期间，请勿关闭交换机电源，以免损坏交换机。

2.5 软件升级

您可以访问 IP-COM 官方网站 www.ip-com.com.cn，下载对应型号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。

交换机进行软件升级前，需要先验证用户密码（登录交换机 Web 管理页面时使用的密码，默认为“admin”）。

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 管理页面，请联系售后维修。

点击「系统管理」>「软件升级」进入软件升级验证页面。

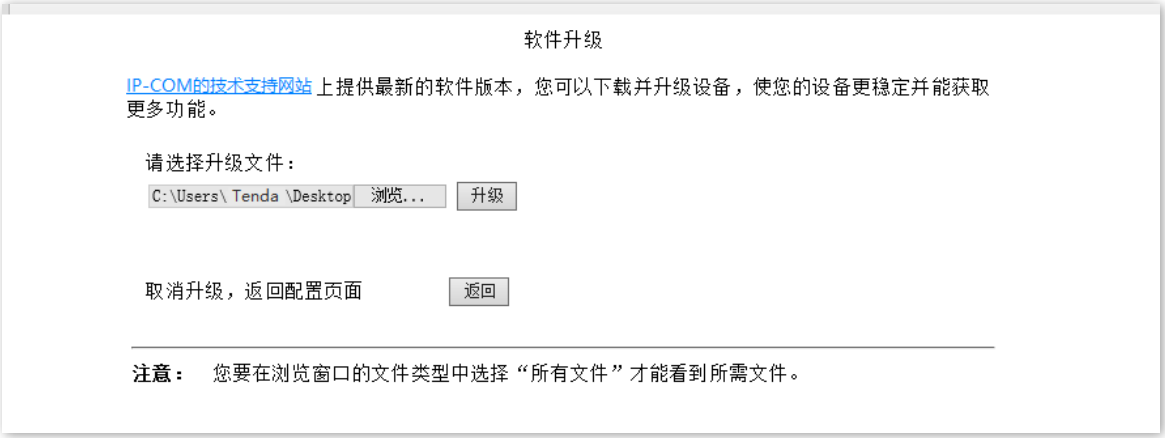
操作步骤：

1. 访问 www.ip-com.com.cn，下载对应型号交换机更高版本的升级文件到本地电脑并解压；
2. 登录交换机 Web 管理页面，然后点击「系统管理」>「软件升级」进入软件升级验证页面；
3. 在“用户密码”后的输入框输入交换机 Web 管理页面的登录密码，然后点击 确定 ；

4. 确认弹出框的提示信息后，点击 确定 ；

5. 进入软件升级页面，点击 浏览... ，从本地电脑选择并加载交换机的升级软件；

6. 点击 升级 ；



7. 弹出提示框，点击 确定 。

注意

请勿中断升级过程，必须等待页面出现 确定 按钮，并且该按钮高亮时，点击 确定 才能完成升级操作！否则需重新升级软件。

---完成

升级进度条走完后，出现以下页面，且 确定 按钮为高亮时，点击 确定 ，完成软件升级。

http://192.168.0.1/
Firmware Update
升级完成!
确 定

3 端口管理

3.1 端口设置

在这里，您可以查看和设置交换机各端口的基本参数。点击「端口管理」进入页面。

设置项参数说明

标题项	说明
☐	勾选对应端口号前面的复选框，可选中该端口。勾选最上面的复选框，可选中全部端口。
开启/关闭	开启/关闭端口。 – 开启：开启选中端口的数据包转发功能。 – 关闭：关闭选中端口的数据包转发功能。 – 不改变：不改变端口该参数的值。 注意 只有开启端口，该端口才能正常转发数据。建议关闭交换机长时间不使用的端口，需要使用时再开启，有效减小交换机的功耗。

标题项	说明
速率/双工	选择端口的传输速率和传输模式。 FDX 指全双工，表示端口可同时接收和发送报文；HDX 指半双工，表示端口在同一时刻只能接收或发送报文。 端口 G1、G2/SFP2 支持 1000M/FDX 和自协商；其他端口支持 10M/FDX、10M/HDX、100M/FDX、100M/HDX 和自协商。 注意 交换机与对端网络设备连接时，必须保持两者端口的速率/双工模式一致，才能保证通信正常。 一般情况下，建议保持默认设置**自协商**，此时传输速率和传输模式将由本端口和对端端口自动协商来决定。
优先级	用于进行 QoS 配置时，选择端口的优先级。
流控	开启/关闭选中端口的流控功能。默认情况下，端口流控处于开启状态。 交换机与对端设备都开启流控时，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，对端设备收到流控帧后，将暂停对本交换机该端口发送数据；同样，当本交换机的某端口接收到流控帧后，也会暂停该端口对外发送数据。 注意 开启流控可以避免因发送和接收速率不一致导致的数据包丢失，但同时也会影响数据源端口与其他设备的通信速率，连接互联网的端口请慎用此功能。
广播抑制	开启/关闭选中端口的广播风暴抑制功能。默认情况下，广播抑制处于关闭状态。 广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通信、降低交换机的性能，甚至导致网络瘫痪。 开启广播抑制后，当端口上的广播流量超过限定值（2000pps）时，交换机将丢弃超出部分的广播报文，进而使端口的广播流量所占的比例降低到限定范围。
地址学习	开启/关闭选中端口的地址学习功能。 开启地址学习后，当交换机收到数据包时，如果其 MAC 地址表中没有这个 MAC 地址的对应关系，则向所有的端口广播该数据包。当目的主机从某个端口返回信息时，交换机便把该 MAC 对应的端口记录到 MAC 表中。 交换机的 MAC 地址表维护着交换机端口与连接到该端口的主机的 MAC 地址的对应关系。 提示 端口开启 MAC 绑定功能时，该端口的 MAC 地址学习功能将自动关闭。

列表参数说明

标题项	说明
端口	显示端口号。
链接状态	显示端口实际的速率和双工模式，若未连接或链接失败显示为“---”。
速率/双工	显示端口当前设置的速率和双工模式。
优先级	显示端口的优先级。
流控	显示端口流控功能的开启/关闭状态。
开启/关闭	显示端口的启用状态。
广播抑制	显示端口是否开启广播抑制功能。
地址学习	显示端口是否开启地址学习功能。

3.2 端口镜像

3.2.1 概述

交换机提供了端口镜像功能，可将一个或多个端口（镜像源端口）的数据复制到指定的端口（镜像目的端口），在镜像目的端口一般接有数据监测设备，以便网络管理员实时进行流量监控、性能分析和故障诊断。

- **端口镜像的基本概念**
  - 源端口

    源端口是被监控的端口，用户可以对通过该端口的报文进行监控、分析。镜像源端口设置为路由端口（即接入互联网的端口）时，可以实现所有报文的监控。
  - 镜像目的端口

    镜像目的端口也可称为监控端口，该端口将接收到的报文转发到数据监测设备，以便对报文进行监控和分析。
    镜像目的端口的带宽应大于或等于所有源端口的带宽之和。
  - 镜像方向

    端口镜像的方向分为以下三种。
    - 入方向：仅对源端口接收的报文进行镜像。
    - 出方向：仅对源端口发送的报文进行镜像。
    - 入和出方向：对源端口接收和发送的报文都进行镜像。

提示

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。

- **交换机支持的端口镜像类型**

  交换机支持的端口镜像类型为本地端口镜像，即，镜像源端口和镜像目的端口在同一台交换机上。

3.2.2 配置端口镜像

1. 点击「端口管理」>「端口镜像」；
2. 镜像目的端口：选择一个端口作为镜像目的端口；

3. 镜像状态：选择作为镜像源端口的端口并勾选对应的镜像状态复选框；

4. 镜像方向：选择镜像方向；

5. 点击 确定 。

---完成

参数说明

标题项	说明
镜像目的端口	选择交换机的镜像目的端口，留空表示关闭镜像功能。 镜像目的端口只能设置一个，且镜像目的端口的带宽应大于或等于镜像源端口的总带宽。 注意 – 端口设置为镜像目的端口后，不能再设置为镜像源端口。 – 只有设置了镜像目的端口后，才能设置镜像源端口。 – 镜像目的端口不能作为任何汇聚组的成员。 – 开启生成树功能后，端口不可设置为镜像目的端口。
镜像方向	选择镜像方向。 – 不镜像：该端口禁用端口镜像功能。 – 镜像入方向：将镜像源端口接收的数据复制到镜像目的端口。 – 镜像出方向：将镜像源端口发送的数据复制到镜像目的端口。 – 镜像入和出方向：将镜像源端口发送和接收的数据都复制到镜像目的端口。 注意 如果镜像源端口的带宽总和大于镜像目的端口的带宽，将会出现丢包情况。

标题项	说明
源端口	显示交换机的端口。 提示 端口被选中为镜像目的端口后，不可再将其设置为镜像源端口。
镜像状态	选择交换机的镜像源端口。

3.2.3 端口镜像配置举例

组网需求

某企业网络环境如下：

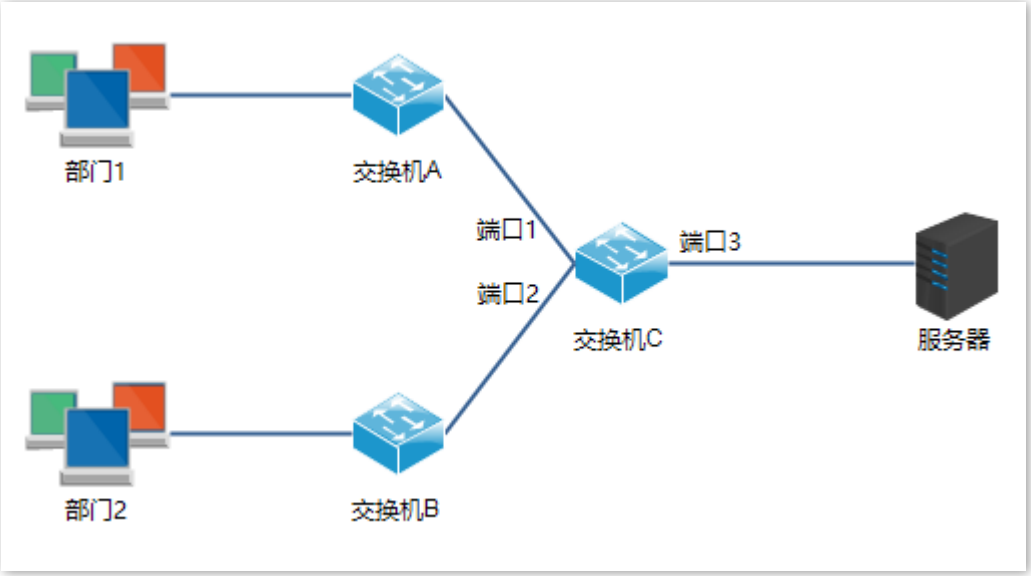
- 部门 1 通过端口 1 接入交换机。
- 部门 2 通过端口 2 接入交换机。
- 服务器接在交换机的 3 端口上。

网络管理员希望通过服务器对部门 1 和部门 2 收发的报文进行监控。

方案设计

使用端口镜像功能实现该需求，具体如下：

- 设置端口 1 和 2 为镜像源端口，镜像方向为“镜像出和入方向”。
- 设置连接服务器的端口 3 为镜像目的端口。



配置步骤

1. 登录到交换机 C 的 Web 管理页面，然后点击「端口管理」>「端口镜像」进入设置页面；
2. 镜像目的端口：选择“3”；
3. 镜像状态：勾选源端口 1 和 2；
4. 镜像方向：选择“镜像出和入方向”；
5. 点击 确定 。

---完成

3.3 端口统计

在这里，您可以查看、清零交换机所有端口的流量统计信息。点击「端口管理」>「端口统计」进入页面。

操作按钮说明

清零：清除当前页面的统计数据，进行重新统计。

刷新：刷新页面的统计数据。

参数说明

标题项	说明
统计模式	选择统计的数据类型。 – 发送与接收：显示端口发送和接收的数据包数量。 – 冲突与发送：显示端口冲突数据包数量和发送的数据包数量。 – 丢弃与接收：显示端口丢弃的数据包数量和接收到的数据包的数量。 – CRC 错误与接收：显示端口 CRC 检验错误的数据包数量和接收到的数据包数量。

3.4 端口限速

在这里，您可以设置交换机下联端口的发送和接收速率。点击「端口管理」>「端口限速」进入页面。

操作按钮说明

复位：清除所有的限速设置，全部端口以实际链接速率收、发数据帧。

设置参数说明

标题项	说明
发送速率（bps）	设置选中端口的发送数据速率。
接收速率（bps）	设置选中端口的接收数据速率。
☐	勾选端口号前面的复选框，可选中该端口。勾选最上面的复选框，可选中全部端口。

列表参数说明

标题项	说明
端口	交换机的各个端口，勾选端口号前的复选框，可对其进行限速设置。 只能对交换机下联口进行限速设置，上联端口（G1、G2/SFP2）不提供端口限速功能。
发送速率（kbps）	显示该端口的发送速率限定值。“--”表示端口将以实际链接速率发送数据。
接收速率（kbps）	显示该端口的接收速率限定值。“--”表示端口将以实际链接速率接收数据。
链接速率	显示该端口协商到的连接速率。“---”表示端口未连接或者协商失败。

4 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，同一汇聚组内的多条物理链路可视为一条逻辑链路。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 配置、VLAN 配置、地址学习、端口管理。具体说明如下：

- 加入汇聚组的端口的 STP 配置（包括：端口状态、端口优先级、路径开销）、VLAN 配置（包括：PVID、Tag 处理策略）、端口配置（包括：开启/关闭状态、速率/双工、优先级、流控、广播抑制、地址学习）等需一致。
- 对于已加入汇聚组的端口，不可进行以下功能设置：端口静态 MAC 地址绑定、设置为镜像目的端口。
- 已设置为“镜像目的端口”的端口不能加入汇聚组。

点击「链路汇聚」，进入端口静态汇聚设置页面。

参数说明

标题项	说明
汇聚算法	选择汇聚算法。 – 基于端口 ID：汇聚组中各成员端口按接收数据中的端口 ID 进行负荷分担。 – 基于源 MAC 地址：汇聚组中各成员端口按接收数据中的源 MAC 地址进行负荷分担。 – 基于目的 MAC 地址：汇聚组中各成员端口按接收数据中的目的 MAC 地址进行负荷分担。 – 基于源与目的 MAC 地址：汇聚组中各成员端口按接收数据中的源 MAC 地址+目的 MAC 地址进行负荷分担。
汇聚组号	显示汇聚组的序号。
汇聚配置端口	显示本交换机中，可配置为汇聚组成员的端口。勾选端口后的复选框，可选中该端口。
启用	启用/禁用该汇聚组。

5 网络延长

交换机提供了网络延长功能，可以延长交换机**下联端口**的数据传输和 PoE 供电距离，为网络部署带来极大的便利。

端口开启端口延长功能后，其链接速率将自动协商为 10Mbps，此时，使用超五类及以上网线，该端口的数据传输和 PoE 供电距离最远可达 250 米。

注意

使用端口延长时，为了避免链路协商失败，请确保对端设备端口的速率与双工模式为“自协商”。

点击「网络延长」进入页面。

操作步骤

1. 勾选端口号前面的复选框，选中要设置的端口；
2. 端口延长：点击下拉菜单，选择“开启”；
3. 点击 确定 。

---完成

参数说明：

标题项	说明
端口延长	开启/关闭选定端口的网络延长功能。
☐	勾选端口号前面的复选框，可选中该端口。勾选最上面的复选框，可选中全部端口。 提示 开启了端口延长功能的端口，仅支持 10Mbps 全/半双工通信。
PoE 端口	显示可以提供 PoE 供电的端口号。
PoE 供电延长	显示端口的 PoE 供电延长功能的启用状态。
链接状态	显示端口的工作速率和双工模式。“---”表示端口未连接或者协商失败。

6 PoE 管理

交换机的**下联端口**均支持 PoE 供电，并符合 IEEE 802.3af、IEEE 802.3at 标准。受电设备连接到交换机的 PoE 端口时，交换机将自动给受电设备提供所需功率的 PoE 电源。

点击「PoE 管理」进入页面。在这里，您可以查看当前交换机 PoE 电源的使用情况，还可开启/关闭下联端口的 PoE 供电功能。

提示

默认情况下，交换机已开启所有下联端口的 PoE 供电功能。

设置参数说明

标题项	说明
PoE 状态	开启/关闭选中端口的 PoE 供电功能。
☐	勾选端口号前面的复选框，可选中该端口。勾选最上面的复选框，可选中全部端口。

显示参数说明

标题项	说明
PoE 消耗功率	显示交换机当前 PoE 供电已输出的总功率。

标题项	说明
PoE 剩余功率	显示交换机当前 PoE 供电还能输出的功率。
端口	显示交换机各个下联端口的序号。
PoE 状态	显示交换机各个下联端口的 PoE 供电状态（开启或关闭）。
输送功率[W]	显示交换机各个下联端口的 PoE 供电输出功率。

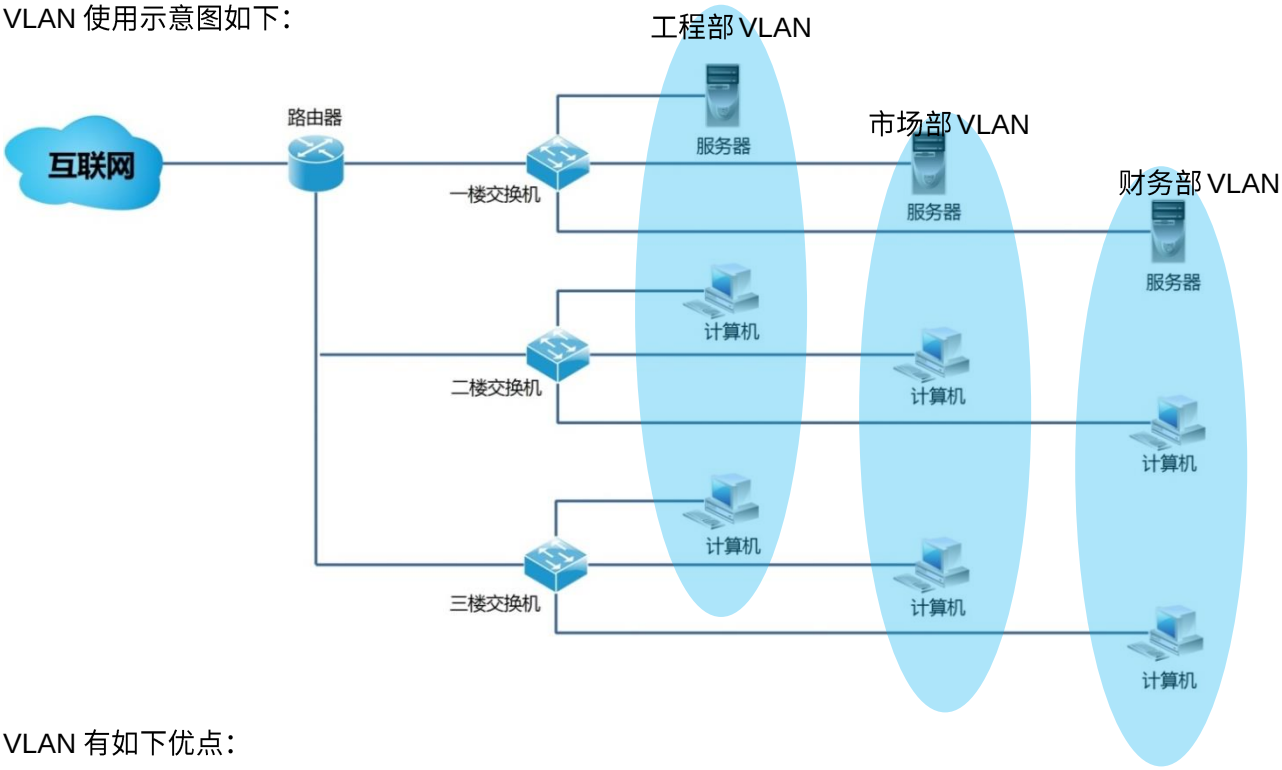
7 VLAN 管理

7.1 概述

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。随着网络不断扩充，还可能出现广播风暴，导致整个网络无法使用。

VLAN（Virtual Local Area Network，虚拟局域网），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不同网段，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。

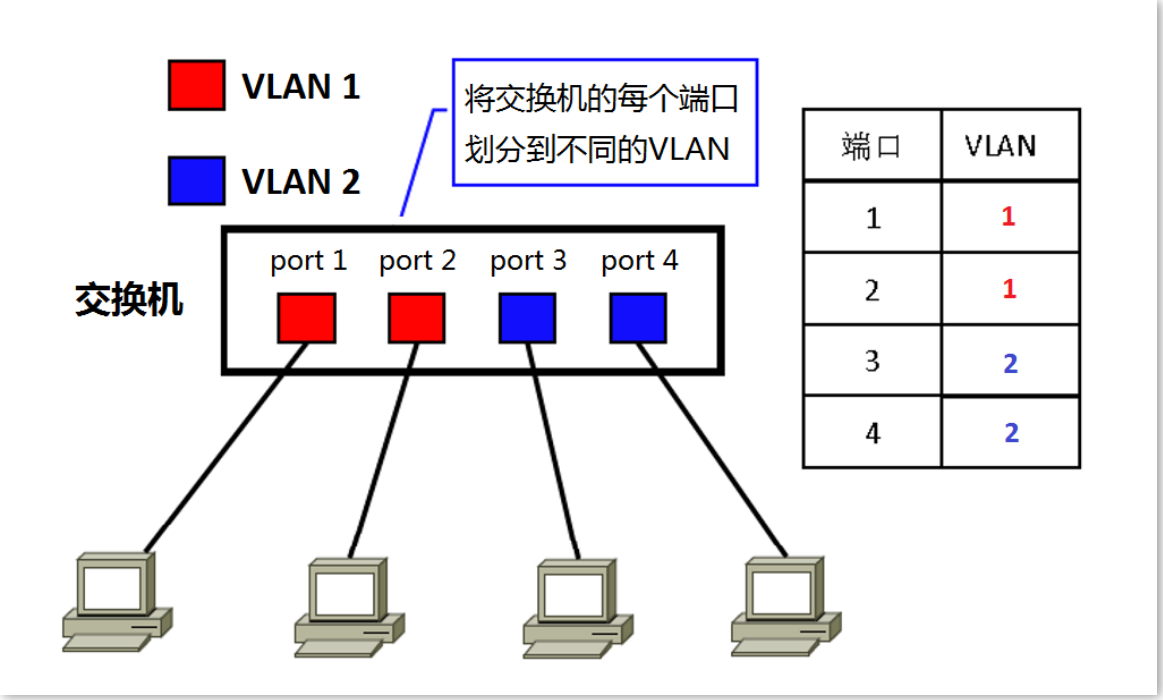
- 简化网络管理。使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟局域网范围内移动时，不需要更改网络配置即可正常访问网络。
- 确保网络安全。不同 VLAN 的主机不能直接相互通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发，这加强了企业网络中不同部门之间的安全性。

本交换机支持三种 VLAN 模式：端口 VLAN、一键 VLAN 和 802.1Q VLAN。

- **端口 VLAN**

端口 VLAN 是基于物理端口来划分 VLAN 的方法。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 内的端口才能相互通信。

如下图所示，某个 4 口交换机进行端口 VLAN 划分，将 4 个端口分别划分到 2 个不同的 VLAN 中：端口 1、端口 2 划分到 VLAN 1；端口 3、端口 4 划分到 VLAN 2。



进行端口 VLAN 划分后，只有在同一个 VLAN 中的端口才能进行通信，不在同一个 VLAN 的端口之间不能进行通信。上例中的端口 1 只能和端口 2 通信，和端口 3、端口 4 不能相互通信。

- **一键 VLAN**

一键 VLAN 本质上仍是基于端口的 VLAN 划分。

启用一键 VLAN 后，系统自动将交换机的每个下联端口分别与上联端口（G1 和 G2/SFP2）划分为一个单独的 VLAN。下联端口之间不能直接通信，只能和上联端口通信，有效保障网络安全。

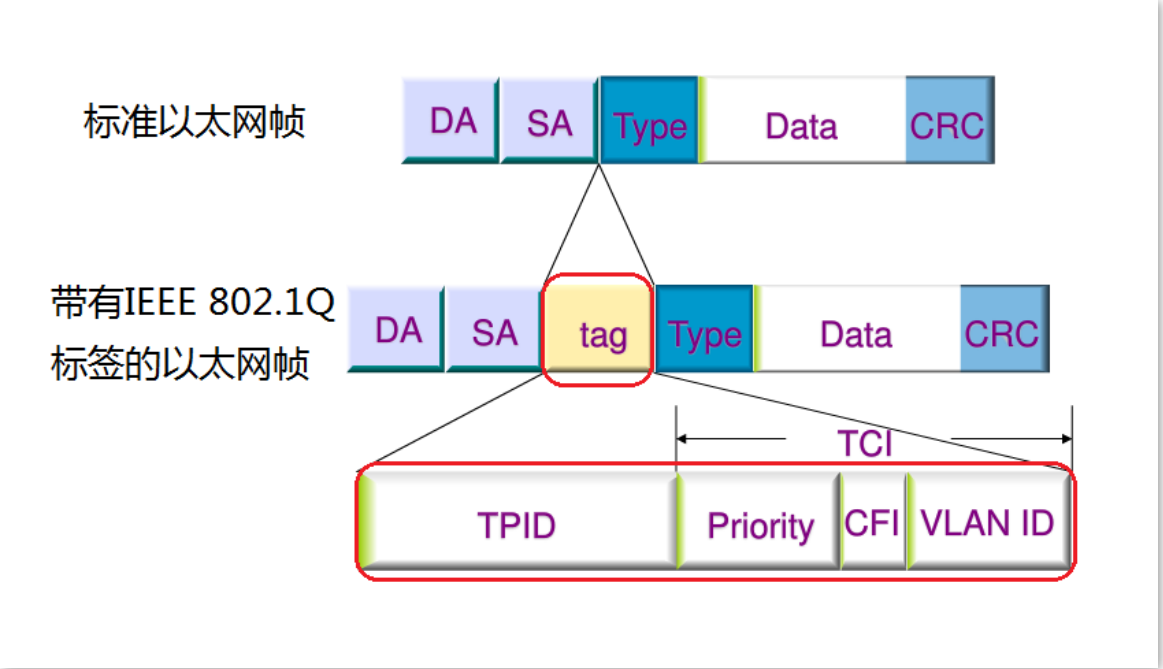
注意

启用“一键 VLAN”后，请将端口 G1、G2/SFP2 连接到中心交换设备。当交换机下可能存在私接无线路由器，导致 DHCP 冲突时，建议启用本模式。

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目的 MAC 地址和源 MAC 地址之后封装一个 4 字节的 802.1Q VLAN 标记，用以标识 VLAN 的相关信息。如下图所示，标准以太网帧在目的 MAC 地址（DA）和源 MAC 地址（SA）后加入一个 802.1Q VLAN 标签（tag）就变成了带有 802.1Q 标签的以太网帧。



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>。

7.2 端口 VLAN

7.2.1 配置向导

本交换机的端口 VLAN 配置步骤及任务说明如下：

步骤	配置任务	说明
1	切换 VLAN 模式	可选。 默认情况下，交换机的 VLAN 模式为端口 VLAN。
2	划分 VLAN	必选。 默认情况下，交换机没有划分 VLAN。

7.2.2 配置端口 VLAN

请先切换 VLAN 模式，再划分 VLAN。

切换 VLAN 模式

将交换机的 VLAN 模式切换为端口 VLAN。

操作步骤：

1. 登录到交换机的 Web 管理页面，然后转到「VLAN 管理」页面；
2. VLAN 模式：点击“VLAN 模式”下拉菜单，选择“端口 VLAN”；
3. 点击 确定 。

---完成

划分 VLAN

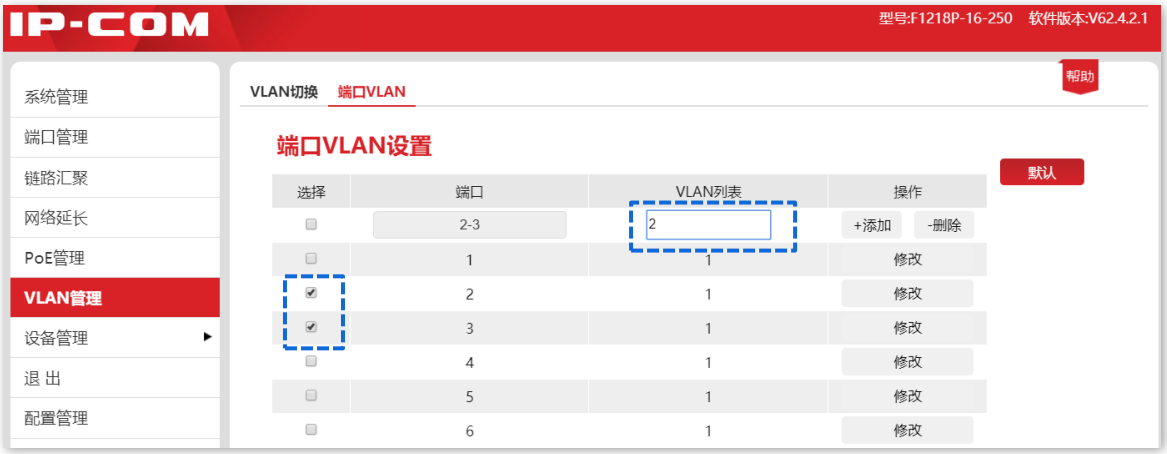
本节以示例的形式说明添加、删除、修改端口 VLAN 以及将端口 VLAN 配置恢复到出厂状态的方法步骤。

添加端口 VLAN

假设需要将端口 2、3 添加到 VLAN2。

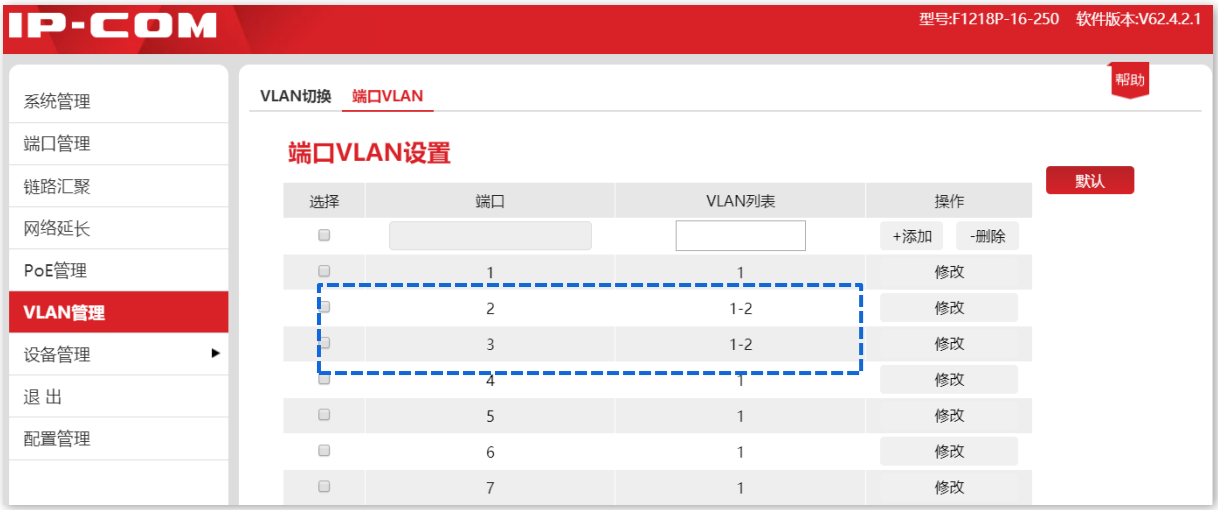
操作步骤：

1. 点击「VLAN 管理」>「端口 VLAN」；
2. 选择：勾选端口号 2 和 3 前的复选框☐；
3. VLAN 列表：在 VLAN 列表的输入框中输入 2；
4. 操作：点击 +添加 。



---完成

设置完成效果图如下。

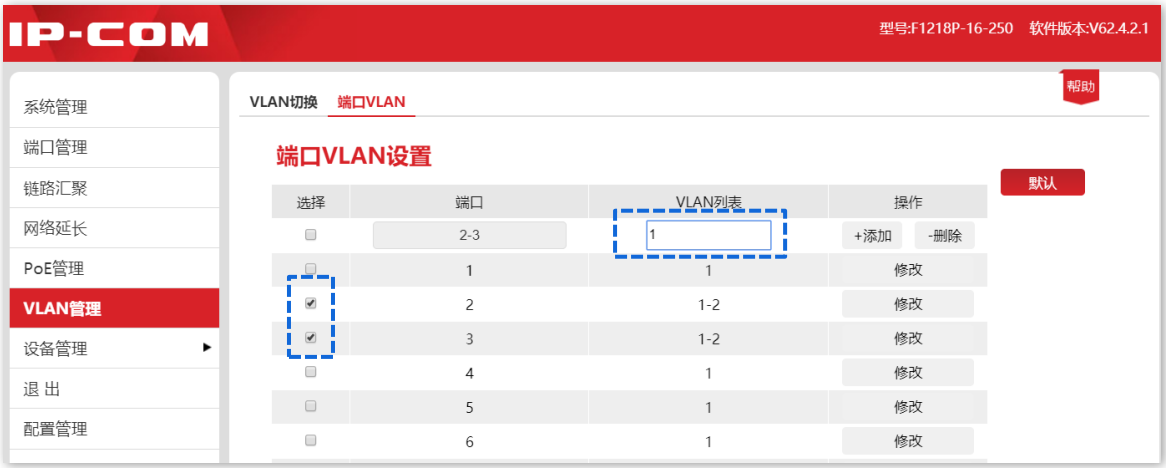


删除端口 VLAN

如上文添加端口 VLAN 的示例中，端口 2、3 其实还在 VLAN1 内，如果想让 2、3 端口只能与上联端口 G1、G2/SFP2 通信，与其他非上联端口隔离，需将 2、3 从 VLAN1 中删除。

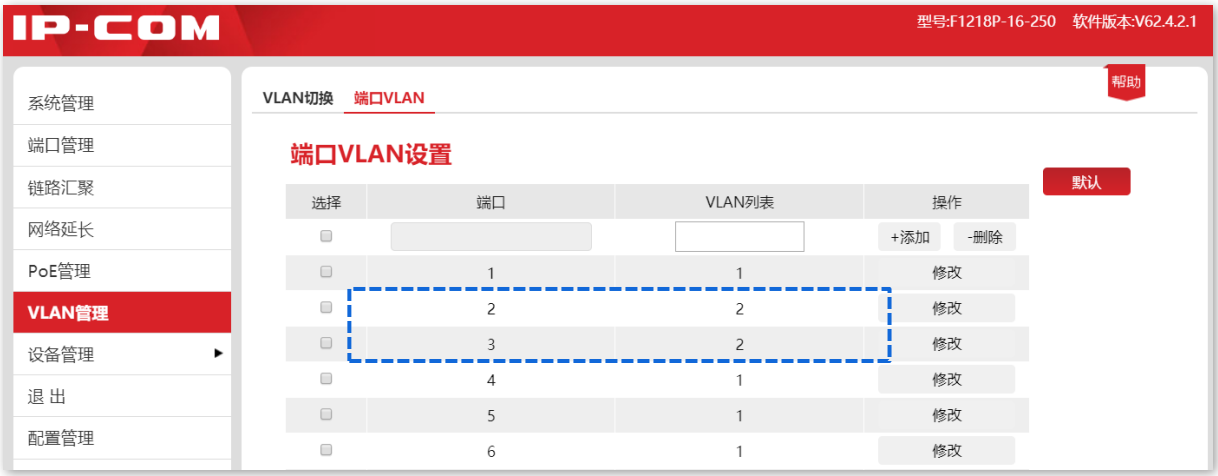
操作步骤：

1. 点击「VLAN 管理」>「端口 VLAN」；
2. 选择：勾选端口号 2 和 3 前的复选框；
3. VLAN 列表：在 VLAN 列表输入框中输入 1；
4. 操作：点击 -删除 。



---完成

设置完成效果图如下。

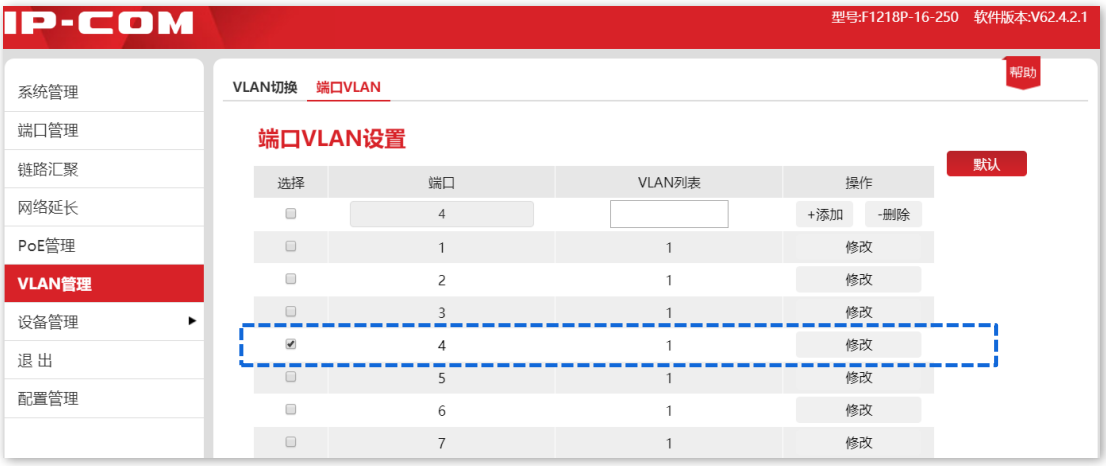


修改端口 VLAN

假设需要将端口 4 的 VLAN 由 1 改为 2。

操作步骤：

1. 点击「VLAN 管理」>「端口 VLAN」；
2. 操作：点击端口号 4 后的 修改 ；



3. 进入修改 VLAN 页面，修改 VLAN；
   (1) 从“端口包含 VLAN”栏选择需要删除的 VLAN1，然后点击 << 。
   (2) 从“可选 VLAN”栏选择需要添加的 VLAN2，然后点击 >> 。

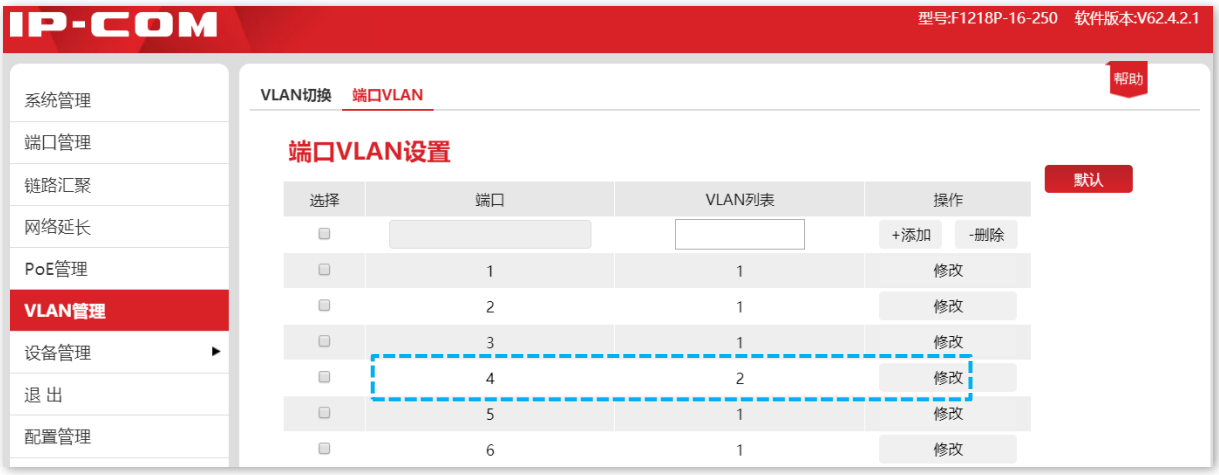
提示

删除的 VLAN 将重新显示在“可选 VLAN”栏，添加的 VLAN 将显示在“端口包含 VLAN”栏。

4. 点击 确定 。

---完成

设置完成效果图如下。



将端口 VLAN 配置恢复到出厂状态（缺省配置）

如果需要将端口 VLAN 恢复到出厂状态，但又不改变交换机的其他配置，可执行以下操作。

操作步骤：

1. 点击「VLAN 管理」>「端口 VLAN」；
2. 点击 默认 。

---完成

设置完成后，交换机的端口 VLAN 配置将恢复到出厂状态，即所有端口都在 VLAN1 中。

7.2.3 端口 VLAN 配置举例

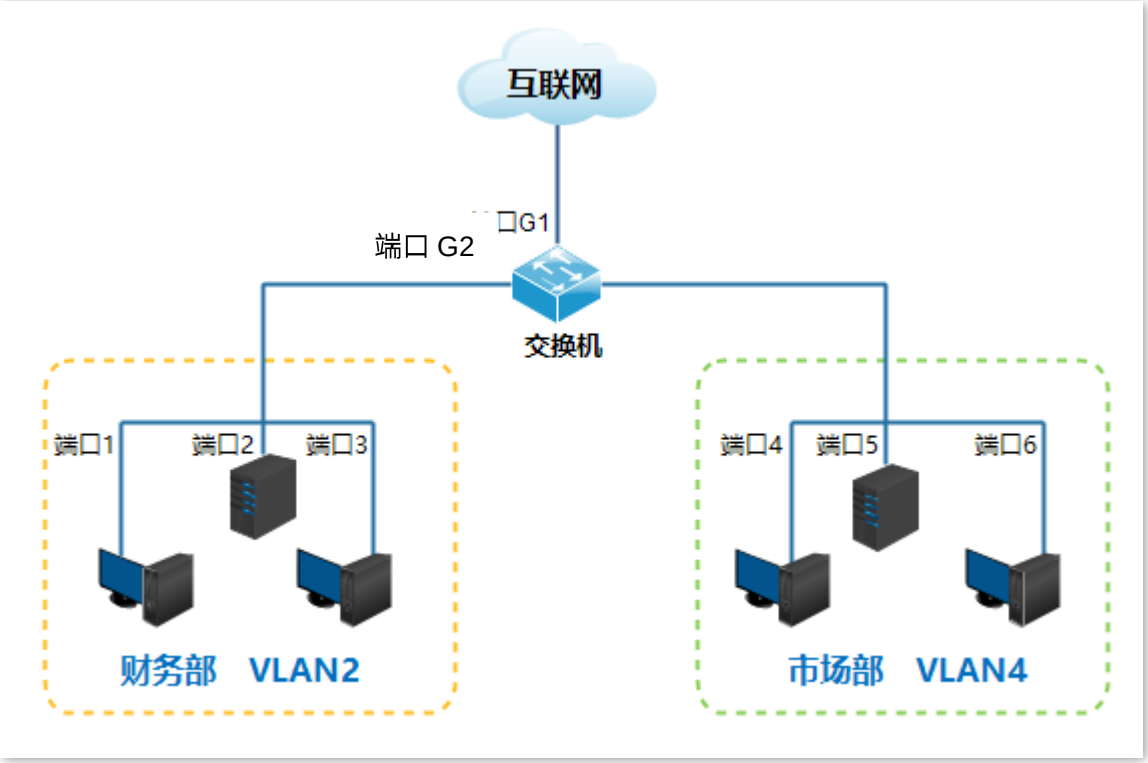
组网需求

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互联网。

方案设计

在交换机上设置端口 VLAN：

- 财务部属于 VLAN2，市场部属于 VLAN4。
- 连接互联网的端口同时属于 VLAN2 和 VLAN4。

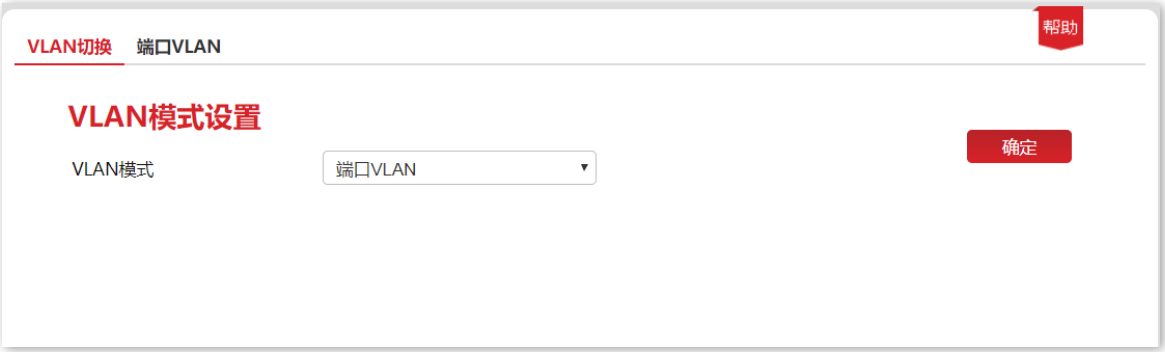


配置步骤

一、切换 VLAN 模式为端口 VLAN

1. 点击「VLAN 管理」；
2. VLAN 模式：点击“VLAN 模式”下拉菜单，选择“端口 VLAN”；

3. 点击 确定 。



二、划分 VLAN

1. 点击「VLAN 管理」>「端口 VLAN」；
2. 选择端口 1、2、3、G2/SFP2，在 VLAN 列表栏下的输入框填入 2，然后点击 +添加 ；
3. 选择端口 4、5、6、G2/SFP2，在 VLAN 列表栏下的输入框填入 4，然后点击 +添加 ；
4. 选择端口 1、2、3、4、5、6、G2/SFP2，在 VLAN 列表栏下的输入框填入 1，然后点击 –删除 。

---完成

设置完成效果图如下。

验证配置

各部门内部能相互通信，部门之间不能相互通信，各部门人员都能访问互联网。

7.3 一键 VLAN

注意

- 启用“一键 VLAN”时，请将端口 G1、G2/SFP2 连接到中心交换设备。
- 当交换机下可能存在私接无线路由器，导致 DHCP 冲突时，建议启用本模式。

7.3.1 配置向导

本交换机的一键 VLAN 配置步骤及任务说明如下：

步骤	配置任务	说明
1	切换 VLAN 模式	必选。 默认情况下，交换机的 VLAN 模式为端口 VLAN。
2	查看 VLAN 划分结果	可选。

7.3.2 配置一键 VLAN

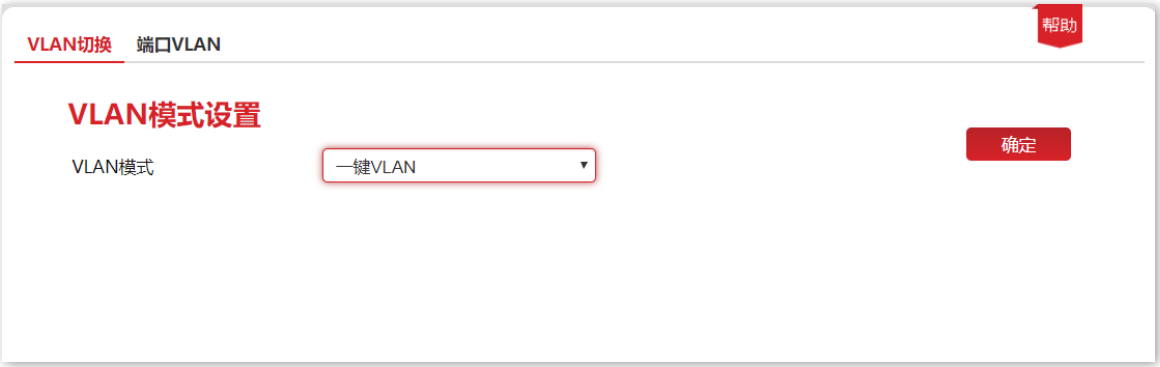
请先切换 VLAN 模式，再查看 VLAN 划分结果。

切换 VLAN 模式

将 VLAN 模式切换为一键 VLAN 后，系统会自动将交换机的每个下联端口分别与上联端口（端口 G1 和端口 G2/SFP2）划分为一个单独的 VLAN。

操作步骤：

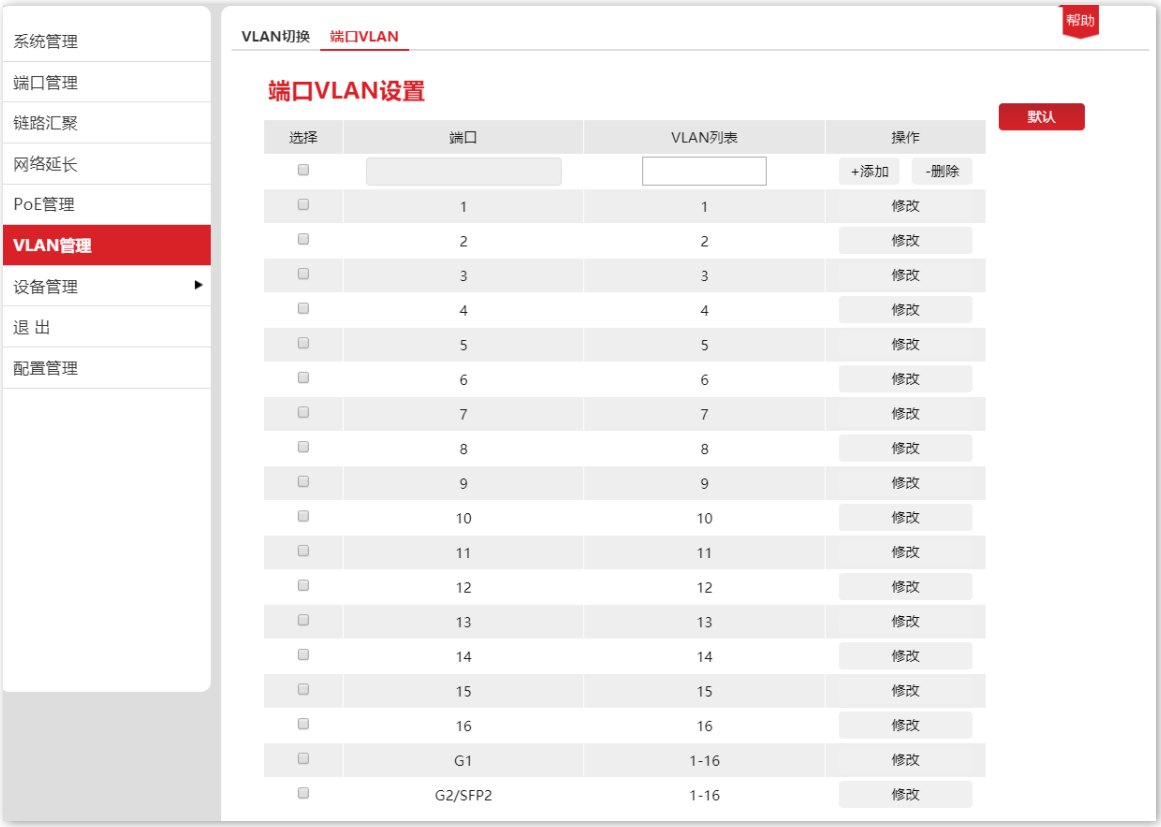
1. 点击「VLAN 管理」；
2. VLAN 模式：点击“VLAN 模式”下拉菜单，选择“一键 VLAN”；
3. 点击 确定 。



---完成

查看 VLAN 划分结果

点击「VLAN 管理」>「端口 VLAN」进入页面，即可查看 VLAN 划分结果。



7.4 802.1Q VLAN

7.4.1 配置向导

本交换机的 802.1Q VLAN 配置步骤及任务说明如下：

步骤	配置任务	说明
1	切换 VLAN 模式	必选。 默认情况下，交换机的 VLAN 模式为端口 VLAN。
2	划分 VLAN	必选。 默认情况下，交换机的所有端口都在 VLAN 1 中。
3	设置端口属性	必选。 默认情况下，交换机的 所有端口的 PVID 都为 1，Tag 处理策略为不处理。

7.4.2 配置 802.1Q VLAN

请先切换交换机的 VLAN 模式为 802.1Q VLAN 后，再进行本节其他设置。

提示

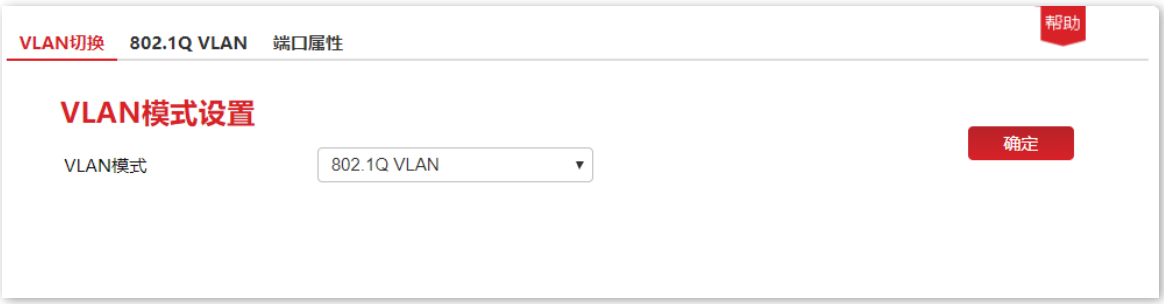
- 802.1Q VLAN 最多可创建 31 组。
- 802.1Q VLAN 可以跨交换机实现 VLAN 隔离效果。
- 所有端口都始终会属于 VLAN1 内，可以配合 802.1Q VLAN 端口属性来实现 VLAN 隔离效果。

切换 VLAN 模式

将交换机的 VLAN 模式切换为 802.1Q VLAN。

配置步骤：

1. 点击「VLAN 管理」；
2. VLAN 模式：点击“VLAN 模式”下拉菜单，选择“802.1Q VLAN”；
3. 点击 确定 。



---完成

划分 VLAN

本节以示例的形式说明添加、删除、修改 802.1Q VLAN 的方法。

添加 802.1Q VLAN

假设需要将端口 2、3 加入 VLAN2。

操作步骤

1. 点击「VLAN 管理」>「802.1Q VLAN」；
2. 选择：勾选端口 2 和 3 前的复选框；
3. VLAN 列表：在 VLAN 列表输入框中输入 2；

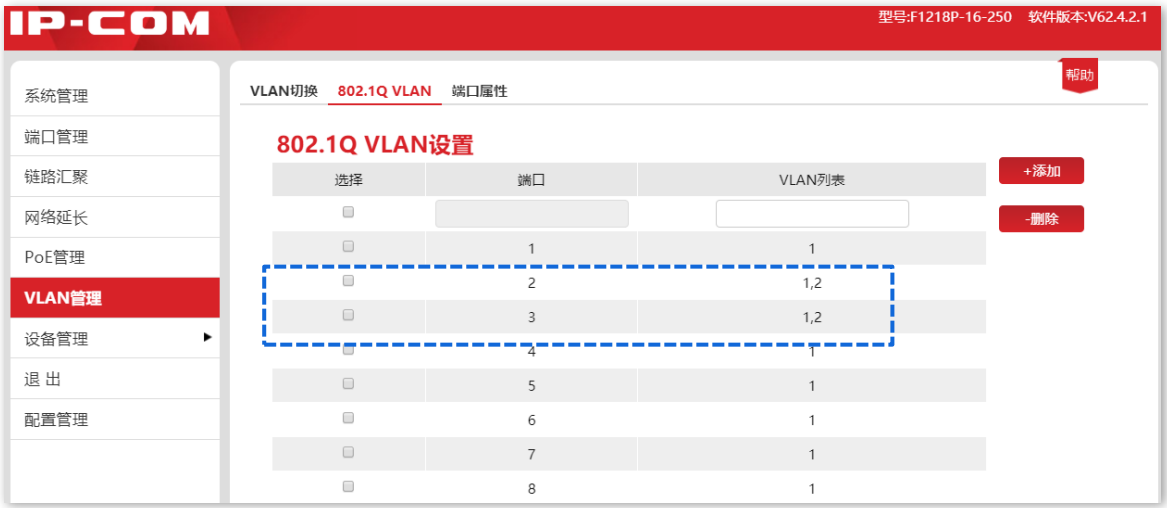
提示

- 勾选最上面的复选框，可选择全部端口。
- 端口可以同时属于多个 VLAN，但每次只能添加 1 个 VLAN。

4. 点击 +添加 。

---完成

设置完成效果图如下。



删除 802.1Q VLAN

假设需要将上述添加 802.1Q VLAN 示例中的端口 3 从 VLAN2 中删除。

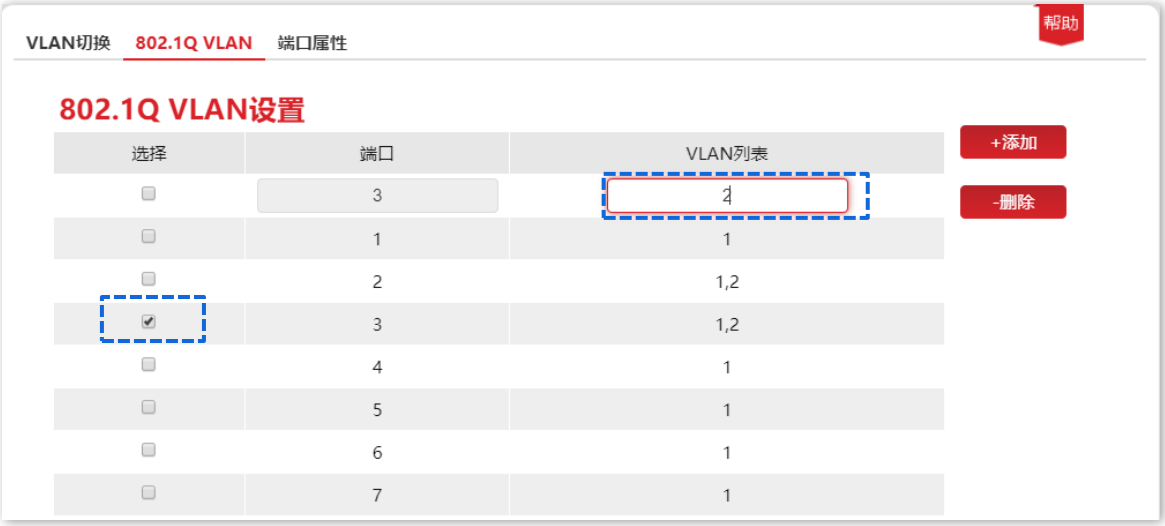
操作步骤

1. 点击「VLAN 管理」>「802.1Q VLAN」；
2. 选择：勾选端口 3 前的复选框☐；
3. VLAN 列表：在 VLAN 列表的输入框中输入 2；

提示

VLAN 1 为端口的默认 VLAN ID，不能删除。

4. 点击 -删除 。

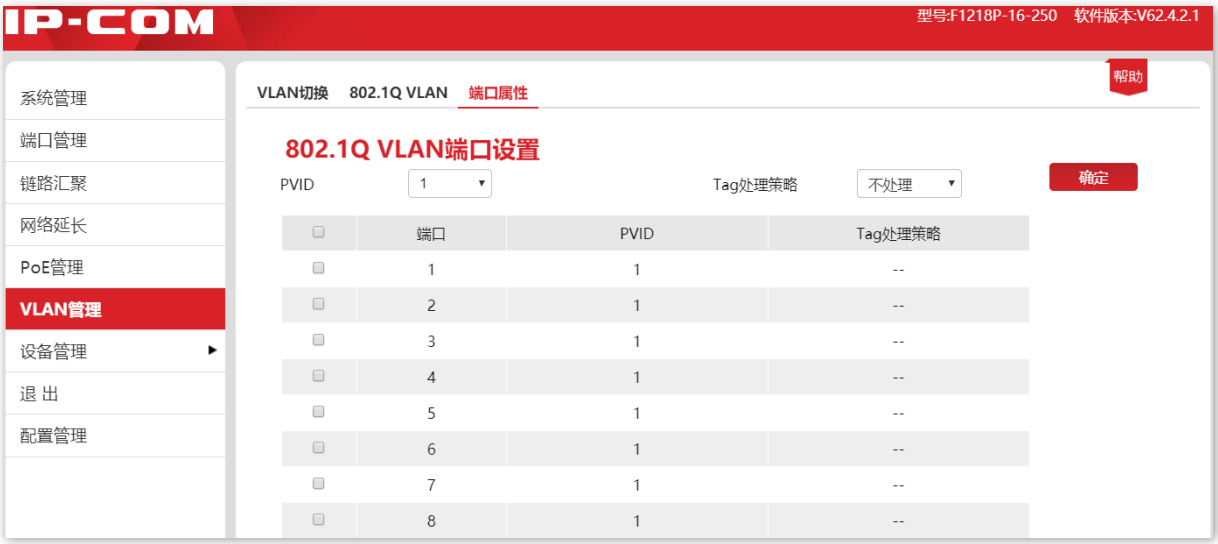


---完成

设置完成效果图如下。

设置端口属性

要使用 802.1Q VLAN 实现 VLAN 隔离效果，需通过设置 802.1Q VLAN 端口的 PVID 和 Tag 处理策略来实现。



设置参数说明

标题项	说明
	通过勾选 ☐，选择需要设置 802.1Q VLAN 端口属性的端口。 勾选最上面的 ☐，可选择全部端口；勾选端口号前的端口，可选择对应端口。
PVID	设置端口默认所属的 VLAN ID，用于给不带 VLAN Tag 标签的数据包一个默认 VLAN 归属。 每个端口的 PVID 可以不同，但 PVID 只能选择为已存在的 VLAN。默认各端口的 PVID 均为 1。
Tag 处理策略	设置端口对数据的发送处理策略。 – 不处理：若接收到的数据包不带 Tag，则发出去的数据包也不带 Tag；若接收到的数据包带 Tag，则发出去的数据包保留该 Tag。 – 添加 Tag：若接收到的数据包不带 Tag，则发出去的数据包打上接收端口的 PVID；若接收到的数据包带 Tag，则发出去的数据包保留该 Tag。 – 移除 Tag：若接收到的数据包不带 Tag，则发出去的数据包也不带 Tag；若接收到的数据包带 Tag，则发出去的数据包去掉该 Tag。

交换机各端口对数据的接收处理模式见下表：

接收数据包类型	处理模式
接收 Tag 数据	按 Tag 中的 VID 转发到相应 VLAN 的其他端口。
接收 Untag 数据	按该端口的 PVID 转发到相应 VLAN 的其他端口。

提示

– 交换机在 802.1Q VLAN 下的 MAC 表是共享学习方式，即在不同 VLAN 内学习到的 MAC 地址，在 MAC 表中是同一个条目。

- 端口的 PVID 可以不属于该端口的 VLAN ID 集合，但当端口 PVID 对应的 VLAN ID 被删除时，PVID 会自动变为默认值 1。

7.4.3 802.1Q VLAN 配置举例

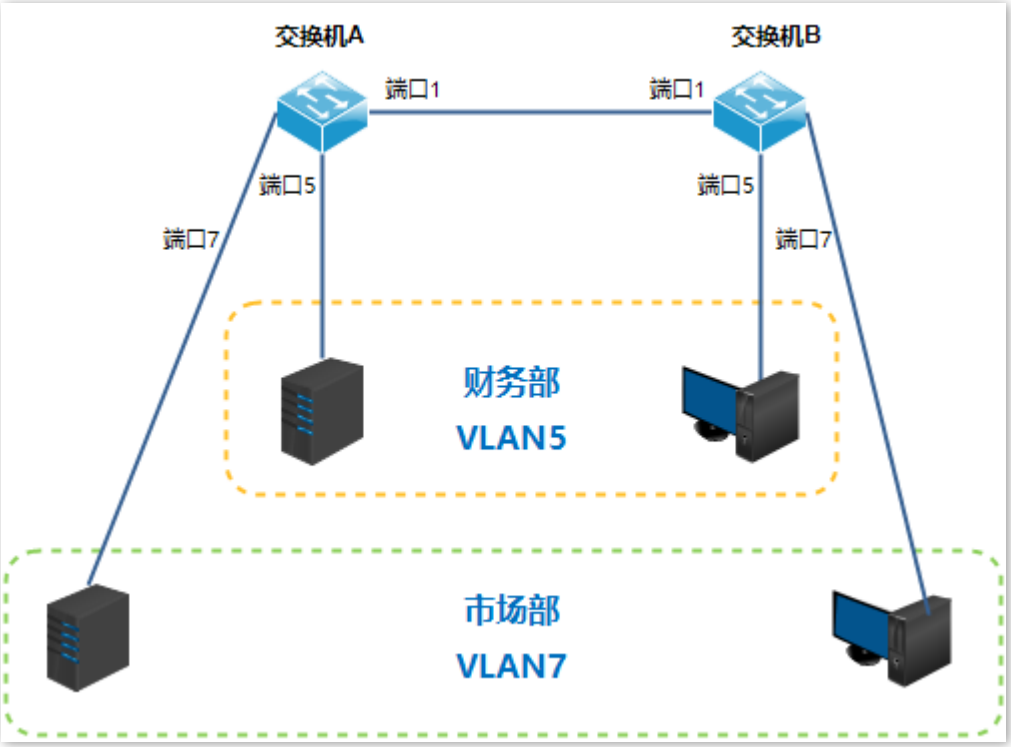
组网需求

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。

方案设计

在交换机上设置 802.1Q VLAN：

- 在交换机上添加两个 VLAN，将连接财务部设备的端口添加到 VLAN5，连接到市场部设备的端口添加到 VLAN7。
- 连接两个交换机的端口同时添加到 VLAN5 和 VLAN7。



配置步骤

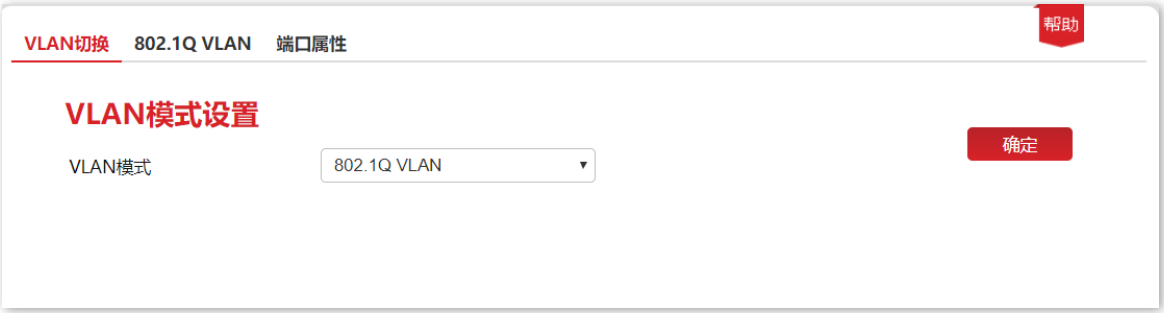
一、设置交换机 A

1. 切换 VLAN 模式为 802.1Q VLAN；

(1) 点击「VLAN 管理」。

(2) VLAN 模式：点击“VLAN 模式”下拉菜单，选择“802.1Q VLAN”。

(3) 点击 确定 。



2. 划分 VLAN；

(1) 点击「VLAN 管理」>「802.1Q VLAN」。

(2) 选择端口 1 和 5，之后在 VLAN 列表下的输入框输入 5，然后点击 +添加 。

(3) 选择端口 1 和 7，之后在 VLAN 列表下的输入框输入 7，然后点击 +添加 。

3. 设置端口属性；

(1) 点击「VLAN 管理」>「端口属性」。

(2) 选择端口 5，设置 PVID 为 5、Tag 处理策略为移除 Tag，点击 确定 。

(3) 选择端口 7，设置 PVID 为 7、Tag 处理策略为移除 Tag，点击 确定 。

(4) 选择端口 1，设置 PVID 为 1、Tag 处理策略为添加 Tag，点击 确定 。

二、设置交换机 B

交换机 B 的设置步骤与交换机 A 的设置步骤相同，这里就不再进行赘述。

---完成

验证配置

员工能访问本部门服务器，不能访问其他部门服务器。

8 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 绑定：进行交换机端口静态 MAC 地址绑定。

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。

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：用于高效管理交换机。

8.1 MAC 绑定

8.1.1 概述

MAC 绑定实现了静态 MAC 地址表和 MAC 过滤的功能：

- 静态 MAC 地址表：端口绑定 MAC 地址后，匹配指定 MAC 地址的设备只能通过该端口访问网络，不能通过其他端口访问网络。
- MAC 过滤：端口绑定 MAC 地址后，该端口仅允许指定 MAC 地址的设备访问网络，禁止其他设备访问网络。

通过 MAC 绑定功能，实现了单端口只允许设置的用户使用网络资源，保证网络安全和用户权限，有效防止假冒身份的非法用户骗取数据以及蹭网。

提示

- 开启了 MAC 绑定的端口，自动关闭地址学习功能。
- 绑定的 MAC 地址由用户手动添加和删除，不会随着时间自动删除。

8.1.2 配置 MAC 绑定

在「设备管理」页面，您可以进行端口静态 MAC 地址绑定操作。

设置参数说明

标题项	说明
选择端口	选择要设置静态 MAC 地址绑定功能的端口。
静态 MAC 地址 1 静态 MAC 地址 2 静态 MAC 地址 3	输入绑定到该端口的设备的 MAC 地址，最多支持绑定 3 个。 注意 广播或组播地址不允许绑定。
绑定	开启/关闭该端口的 MAC 绑定功能。 提示 – 启用 MAC 绑定的端口将关闭地址学习功能。 – 启用 MAC 绑定后，交换机仅允许指定的设备通过该端口访问网络。

设置完成后，点击 确定 ，系统会自动将设置信息显示在下方列表中，您可以查看列表检查设置信息是否有误。

列表参数说明

标题项	说明
端口	显示交换机各个端口的序号。

标题项	说明
状态	显示该端口静态 MAC 地址绑定功能的启用状态。
绑定 MAC1/2/3	显示绑定到该端口的接入设备的 MAC 地址。

8.1.3 MAC 绑定配置示例

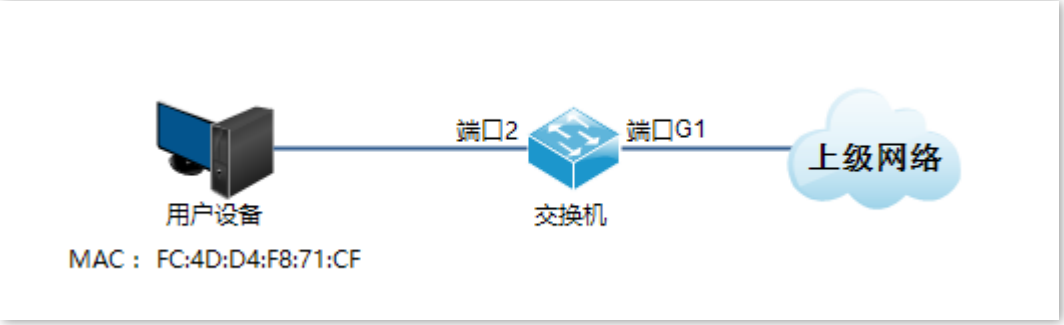
添加 MAC 绑定配置示例

组网需求

用户设备 MAC 地址为 FC:4D:D4:F8:71:CF，连接到交换机的 2 端口。为防止其他非法用户蹭网以及伪装成合法用户的 MAC 地址从交换机其他端口进入来骗取数据。

方案设计

在交换机的 2 端口绑定该用户设备的 MAC 地址。



配置步骤

1. 点击「设备管理」>「MAC 绑定」；
2. 点击“选择端口”下拉菜单，选择“2”；
3. 将用户设备的 MAC 地址“FC4DD4F871CF”填写在静态 MAC 地址 1 栏中；
4. 点击“绑定”下拉菜单，选择“开启”；
5. 点击 确定 。

---完成

设置完成效果图如下。

验证配置

设置完成后，接入到端口 2 的所有用户设备中，只有 MAC 地址为 FC:4D:D4:F8:71:CF 的设备才能顺利访问上级网络；将 MAC 地址为 FC:4D:D4:F8:71:CF 的设备接入到交换机的其他端口，不能访问上级网络。

8.2 QoS 配置

8.2.1 概述

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**

  本交换机实现了简单的 QoS 功能，通过设置端口的优先级，发生网络拥塞时，系统首先丢弃低优先级端口上的数据包，从而保证高优先级端口数据包的传送。交换机共有两个优先级队列，队列 low 为低优先级，队列 High 为高优先级。交换机支持的调度算法为：先进先出（FIFO）、严格优先级（SP）、加权优先级（WRR）。默认情况下为先进先出（FIFO）。

- **队列调度算法**

  - 先进先出（FIFO）

    FIFO 是对先收到的数据包先进行转发，它适用于绝大多数网络应用，如 E-Mail 和 FTP 等。

  - 严格优先级（SP）

    SP 队列调度算法是针对关键业务型应用设计的。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”。

  - 加权优先级（WRR）

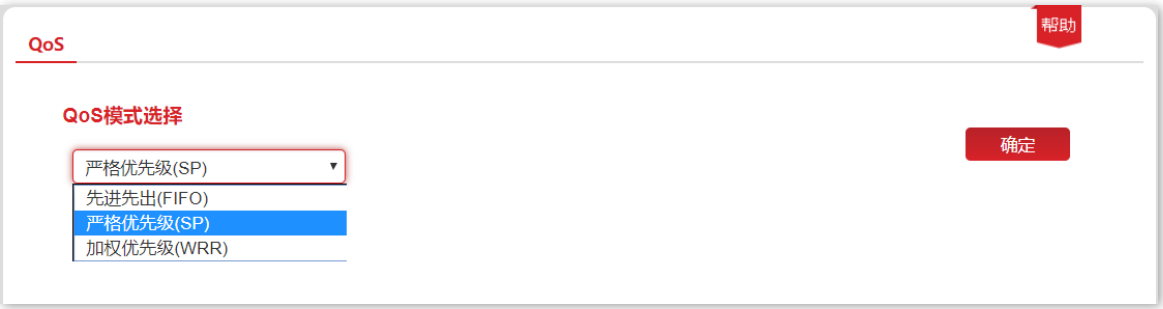
    WRR 队列调度算法是在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 2 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w2、w1），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 7、3（依次对应 w2、w1），这样可以保证最低优先级队列至少获得 30Mbps 带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

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。

8.2.2 配置 QoS

1. 点击「设备管理」>「QoS 配置」；

2. QoS 模式选择：选择 QoS 模式，如果选择加权优先级（WRR），还需设置 Low weight 和 High weight，注意 High 的比例一定要高于 Low 的比例，本系列交换机支持 1-7 比例；



3. 点击 确定 ；

4. 设置端口优先级。

   (1) 点击「端口管理」>「端口设置」。

   (2) 选择相应端口，设置其端口优先级，本例为 1 和 2 号端口。

   (3) 点击 确定 。

---完成

Qos 配置说明

如果选择 QoS 模式为严格优先级（SP），在端口优先级中配置 1 号端口为高，2 号端口为低。当两个端口同时向同一个端口发送数据时，那么该端口将会优先保证 1 号口的数据包通过，然后才允许 2 号口的数据包通过。

如果是选择了加权优先级（WRR），设置权值分别为 High=7、Low=1，当两个端口同时向同一个端口发送数据时，该端口会按照 7:1 的流量比例发送数据。

8.3 STP 配置

8.3.1 概述

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的问题。

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

- **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。

- **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。

- **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。

- **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。

    在每个网段，到根桥的路径开销最小的设备会成为指定桥，当所有交换机具有相同的根路径开销时，网桥 ID 最低的设备会被选为指定桥。
  - 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。

- **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 优先级比较

根桥 ID 越小的 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

1. 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。

2. 选择最优 BPDU

   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。

3. 选举根桥

网络中所有的设备通过交换 BPDU，设备之间比较桥 ID，网络中桥 ID 最小的设备被选为根桥。

4. 选举根端口、指定端口

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

- **联络时间（Hello Time）**

  根桥交换机向周围的交换机发送 BPDU 报文的时间间隔，用来检测链路是否存在故障，取值范围 1~10 秒。

- **老化时间（Max Age）**

  如果在超出老化时间后，还没有收到根桥交换机发出的 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。

- **传输时延（Forward Delay）**

  指交换机端口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开始转发数据，可能会产生暂时性的环路。因此，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 倍的传输时延后才能进入转发状态，这个传输时延可确保新的 BPDU 已经传遍整个网络。

- **RSTP（快速生成树协议）**

  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。若指定端口是边缘端口，则指定端口可以直接进入转发状态；若指定端口连接着点对点链路，则设备可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

- **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。

- **点对点链路**

  点对点链路是两台交换机之间直接连接的链路。

8.3.2 STP 全局设置

点击「设备管理」>「STP 配置」进入页面。

全局设置

用于配置、查看交换机生成树功能的全局属性。

参数说明

标题项	说明
协议版本	关闭/开启交换机的 STP 功能，启用时直接选择交换机的生成树模式： – 关闭：关闭生成树功能。 – STP：启用生成树兼容模式。 – RSTP：启用快速生成树兼容模式。

标题项	说明
系统优先级	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。数值越小，优先级越高。优先级默认为 32768。
Hello Time	设置交换机发送 BPDU 的时间间隔，默认为 2 秒。
最大老化时间	设置 BPDU 报文在交换机中保存的最大生存时间。默认为 20 秒。 最大老化时间必须满足以下要求： – 最大老化时间 ≥ 2 * (Hello Time + 1) – 最大老化时间 ≤ 2 * (转发延时 – 1)
转发延迟	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。

端口下游设备检测

用于查看、配置端口下游环路检测机制。

注意

– 当生成树功能关闭时，环路检测功能、自动唤醒和唤醒时间间隔不可设置。
– 当生成树功能开启、环路检测功能关闭时，自动唤醒功能无效。只有在 STP 功能和环路检测功能同时开启，自动唤醒功能才生效。

参数说明

标题项	说明
环路检测功能	开启/关闭环路检测功能。 开启该功能后，若端口接收到由该端口转发出去的 BPDU 报文，则判定下游设备有环路产生，并且将该端口设为 Discard 状态。

标题项	说明
自动唤醒	开启/关闭自动唤醒功能。 – 开启：Discard 端口在经历了唤醒时间间隔后，将转变为 Forwarding 状态并重新检测。 – 关闭：当端口转变为 Discard 状态时，需要手动开启端口。
唤醒时间间隔	设置唤醒时间间隔。 开启自动唤醒时，Discard 端口在经历唤醒时间间隔后，将转变为 Forwarding 状态并重新检测。

根桥状态

查看当前根桥状态。

参数说明

标题项	说明
桥 ID	显示当前交换机的网桥 ID，由交换机的系统优先级和 MAC 地址组成。
根桥 ID	在整个网络生成树中，被选举为根桥的设备的网桥 ID。
Hello Time	显示根桥设置的 Hello Time 时间值。
最大老化时间	显示根桥设置的最大老化时间值。
转发延时	显示根桥设置的转发延时时间值。

8.3.3 端口设置

在这里，可以设置端口的优先级和路径开销，也可以查询交换机各端口的端口角色、端口状态等信息。

点击「设备管理」>「STP 配置」>「端口设置」进入页面。

设置参数说明

标题项	说明
选择端口	选择要进行设置的端口。
优先级	设置端口的优先级，有效值是 16 的整数倍，数值越小，优先级越高。 端口优先级是确定与该端口相连接的端口是否会被选为根端口的重要依据。同等条件下，与优先级高的端口相连接的下游设备的端口将被选为根端口。
路径开销(0=AUTO)	设置端口的路径开销。

列表参数说明

标题项	说明
端口	显示交换机各端口的序号。
端口角色	显示该端口的端口角色：Root、Designated、Alternate、Backup 和--。其中“--”表示该端口未连接或交换机关闭了 STP 功能。
端口状态	显示该端口的端口状态：Forwarding、Learning、Listening、Blocking、Discard、Disable。
链接状态	显示该端口的速率和双工模式。其中“--”，表明该端口未连接或协商失败。
路径开销	显示该端口的路径开销。
优先级	显示该端口的优先级。

标题项	说明
下游自环状态	显示该端口的下游设备是否发生环路，若端口下游发生环路，则显示“Active”；反之，则显示“--”。

8.4 IGSP 配置

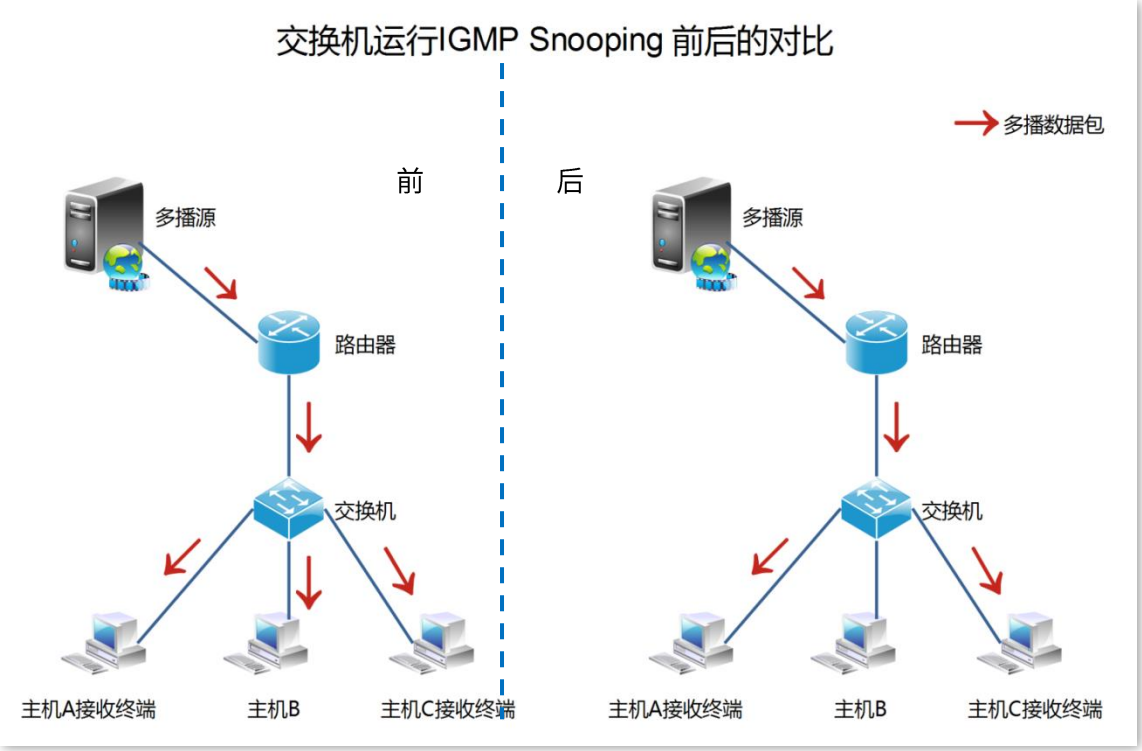
IGSP（Internet Group Management Protocol Snooping，IGMP 侦听）是运行在二层设备上的组播约束机制，用于管理和控制组播组。

运行 IGMP 侦听的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播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。

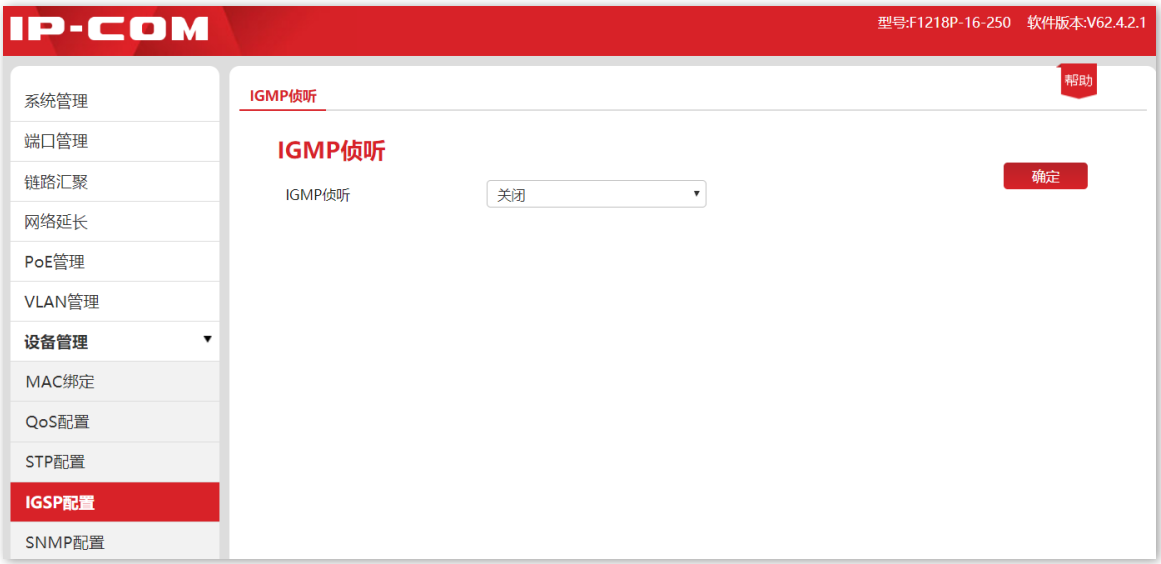
二层设备没有运行 IGMP 侦听时，组播数据在二层被广播；二层设备运行了 IGMP 侦听后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者，但是未知组播数据仍会在二层广播。

IGMP 侦听的主要作用是在交换机上完成二层组播的动态注册。通过开启 IGMP 侦听实现二层组播时，需要在主机和路由器上都实现 IGMP，交换机只是通过侦听主机和路由器传送的不同类型的 IGMP 报文来动态维护二层组播组，并且在本交换机上的组播注册一般不会传播到其它交换机上。只有加入了组播组的端口才可以接收组播数据流，这样可减少网络流量，节省网络带宽。

以下是交换机开启 IGMP 侦听前后的对比图。



点击「设备管理」>「IGSP 配置」页面，您可以在此处开启/关闭交换机的 IGMP 侦听功能。



8.5 SNMP 配置

8.5.1 概述

SNMP（Simple Network Management Protocol，简单网络管理协议）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）。

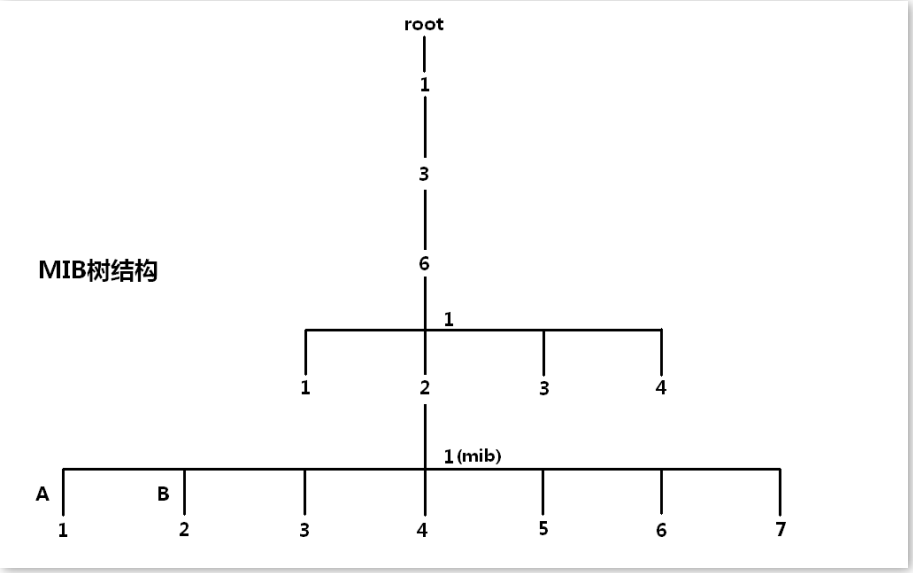
- **SNMP 协议版本**

  本交换机兼容 SNMP v1、SNMP v2c 版本，采用团体名认证。SNMP 团体名用来定义 SNMP NMS 和 SNMP 管理者的关系。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。

SNMP v2c 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。

- **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）。



8.5.2 配置 SNMP

配置向导

本交换机的 SNMP 配置任务如下：

步骤	配置任务	说明
1	开启 SNMP 功能	必选。 默认情况下，交换机的 SNMP 代理功能处于关闭状态。
2	设置 SNMP 团体名	可选。 默认情况下，交换机的只读团体名为“public”，读/写团体名为“private”。
3	设置 SNMP Trap	可选。 默认情况下，交换机的 SNMP Trap 功能处于关闭状态。 如果交换机不用在故障或者出错时向 SNMP 管理者主动上报情况，则无需进行此步骤。

配置任务

设置 SNMP 团体名

假设需要将只读团体名修改为“zhangsan”，读/写团体名修改为“zhangsan123”。

1. 点击「设备管理」>「SNMP 配置」；
2. SNMP 功能：点击下拉框，选择“开启”；
3. 团体名：点击团体名栏下的输入框，可以修改只读访问模式和读/写访问模式的团体名；
4. 点击 确定 。

---完成

参数说明

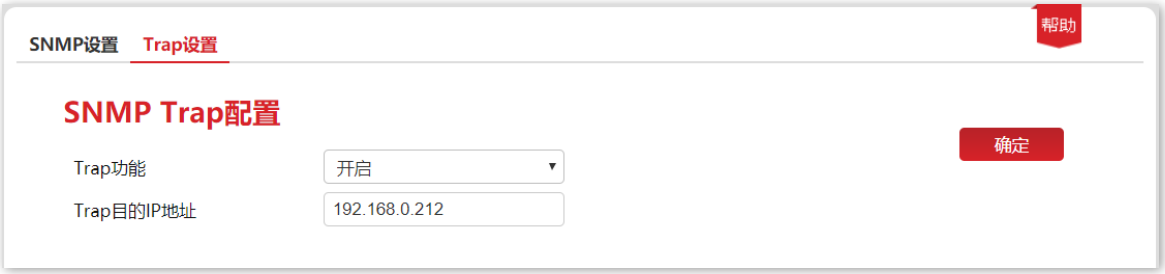
标题项	说明
SNMP 功能	开启/关闭交换机的 SNMP 代理功能。
团体名	设置团体名。“只读”访问模式的团体名默认为“public”，“读/写”访问模式的团体名默认为“private”。 团体名长度为 1~15 个字符，不允许包含中文字符、空格、引号和以下引号内的特殊字符：“/”、“<”、“>”、“|”、“? ”。
访问模式	选择该团体对 MIB 视图的访问权限，有“只读”和“读/写”两种。 – 只读：团体对 MIB 视图具有只读权限。 – 读写：团体对 MIB 视图具有读和写的权限。

设置 SNMP Trap

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。假设 SNMP 管理者的 IP 地址为 192.168.0.212。

1. 点击「设备管理」>「SNMP 配置」>「Trap 设置」；

2. Trap 功能：点击下拉框，选择“开启”；
3. Trap 目的 IP 地址：输入 SNMP 管理者的 IP 地址，本例为 192.168.0.212；
4. 点击 确定 。



---完成

参数说明

标题项	说明
Trap 功能	开启/关闭交换机的 SNMP Trap 功能。默认为关闭。
Trap 目的 IP 地址	开启了 Trap 功能后，需设置 Trap 目的 IP 地址。 当交换机发生紧急的重要事件时，将发送 Trap 信息到 Trap 目的 IP 地址所在主机的 SNMP 管理者。 提示 Trap 目的 IP 地址只能设置为与交换机同网段的合法单机地址，否则无法启动 Trap 功能。

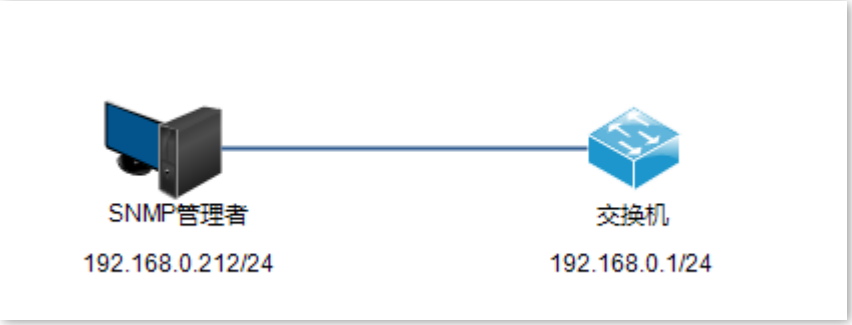
8.5.3 SNMP 配置举例

组网需求

- 交换机与 SNMP 管理者通过以太网相连，交换机的 IP 地址为 192.168.0.1/24，SNMP 管理者的 IP 地址为 192.168.0.212/24。
- SNMP 管理者通过 SNMP v1 或者 SNMP v2c 对交换机进行监控管理，交换机在故障或者出错的时候能够主动向 SNMP 管理者报告情况。

方案设计

只读密钥为“zhangsan”，读/写密钥为“zhangsan123”。



配置步骤

一、配置交换机

1. 开启交换机的 SNMP 功能，并配置 SNMP 团体名；

(1) 点击「设备管理」>「SNMP 配置」页面。

(2) SNMP 功能：点击下拉框，选择“开启”。

(3) 团体名：将只读团体名修改为“zhangsan”，读/写团体名修改为“zhangsan123”。

(4) 点击 确定 。

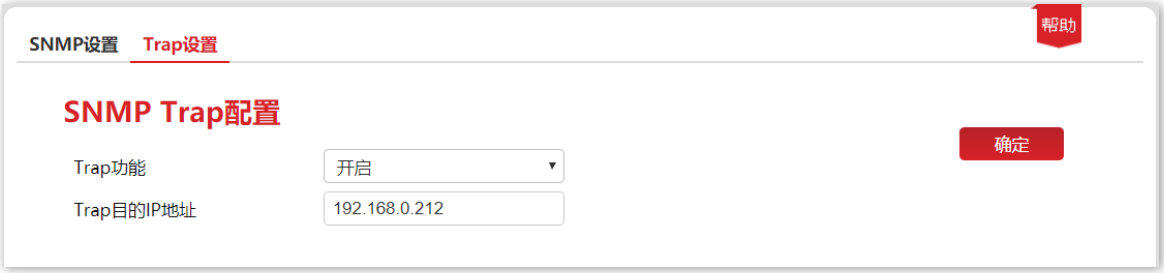
2. 允许交换机向 SNMP 管理者主动报告故障或出错信息；

(1) 点击「Trap 设置」页面。

(2) Trap 功能：点击下拉框，选择“开启”。

(3) Trap 目的 IP 地址：输入 SNMP 管理者的 IP 地址“192.168.0.212”。

(4) 点击 确定 。



二、配置 SNMP 管理者

在使用 SNMP v1/v2c 版本的 SNMP 管理软件上，设置“只读团体名”和“读/写团体名”，注意需要与交换机配置保持一致。具体设置方法请参考 SNMP 管理软件的配套手册。

---完成

验证配置

完成上述设置后，SNMP 管理者和交换机上的 SNMP 代理建立 SNMP 连接，能够通过 MIB 节点查询、设置 SNMP 代理上某些参数的值。

交换机若故障或出错事件，SNMP 管理者可以看到相应的告警信息。

9 退出

点击 Web 管理页面左侧导航栏的「退出」，可以安全地退出交换机的 Web 管理页面。

10 配置管理

在这里，可以备份/恢复配置，点击「配置管理」进入页面。

10.1 备份系统配置信息

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或更符合对应场景的需求，建议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。

操作步骤：点击 备份 ，之后按 Web 管理页面提示操作即可。

10.2 从文件中恢复配置信息

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。

操作步骤：点击 选择文件 ，在弹出的窗口中，找到并双击之前备份的配置文件，然后点击 恢复 ，交换机将导入配置文件，重新启动后生效。