主要功能配置实例

三层网管交换机

1910041116 REV2.0.0

声明

目录

第1章　用户手册简介

本手册旨在帮助您正确使用 TP-LINK 35678 系列三层网管交换机。内容包含配置交换机各种功能的的实例和详细说明。请在操作前仔细阅读本手册。

1.1　目标读者

本手册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

在本手册中，

- 用 **>>** 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 三级菜单**，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字，表示 Web 界面的按钮名称，如<确定>。
- 正文中出现的“”双引号标记文字，表示 Web 界面出现的除按钮外名词，如“系统升级”界面。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.2　适用机型

本手册适用于 TP-LINK 3/5/6/7/8 系列交换机，部分功能仅特定型号支持，以产品实际页面为准。。

第2章　设备管理

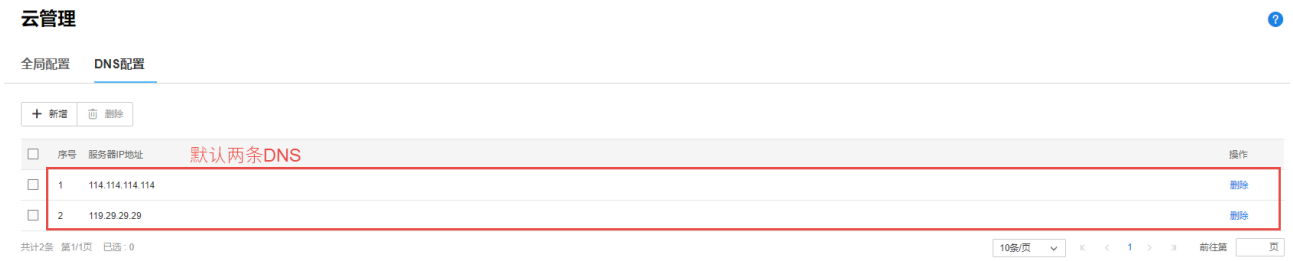
2.1　云管理

TP-LINK 全新推出的三层网管交换机都支持连接 TP-LINK 商用网络云平台，通过将设备上云，用户可以在云平台上针对交换机做一些远程操作，减少运维成本，非常方便。目前具体支持的机型可见链接：TL-LINK 智能开局功能支持机型。

本文介绍三层网管交换机连接商云的配置方法。

1. 进入页面：网络管理 >> 接口配置，配置交换机设备 VLAN1（管理 VLAN，即对接前端路由器的 VLAN）的接口 IP 地址，使接口 IP 地址和前端路由器地址在同一个网段。

2. 进入页面：系统运维 >> 系统管理 >> 云管理 >> DNS 配置，确认设备的 DNS 服务器地址填写正确，交换机默认填写了两条 DNS 地址。



3. 进入页面：系统运维 >> 系统管理 >> 云管理 >> 全局配置，启用交换机的云管理功能，并选择 TP-LINK 商用云平台，点击<保存>。

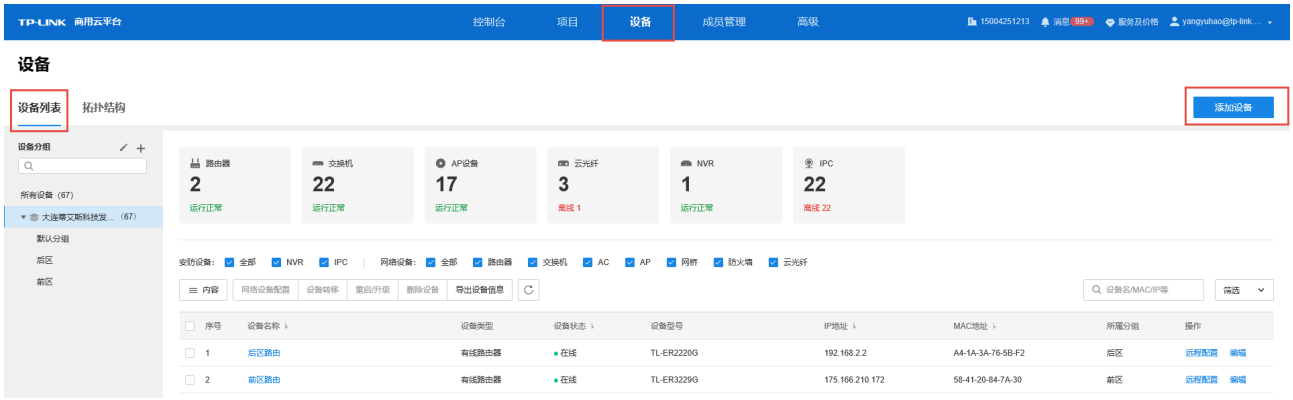
4. 进入页面：网络管理 >> 路由配置 >> 静态路由 >>IPv4 静态路由条目，点击<新增>，配置一条全 0 的静态路由下一跳指向前端路由器 LAN 接口。

进入页面：系统运维 >> 系统维护 >> 测试工具 >> Ping 检测，检查设备是否可以正常联网，一般 Ping

DNS 服务器。

5. 登录 TP-LINK 商用网络云平台：https://smbcloud.tp-link.com.cn/，登录 TP-LINK ID 账号。

6. 进入页面“项目集中管理 >> 设备 >> 设备列表”，点击<添加设备>，设备上云后即可在列表中看到并且可以远程管理。



7. 可选择“设备 ID 添加”，设备 ID 可在路由器底部标贴上查找。

8. 点击添加完成后在设备信息中找到对应路由器设备，点击条目后方 远程配置 ，即可实现通过 TP-LINK 商用云平台远程管理设备。

2.2 通过业务接口管理

三层网管交换机可以通过业务口直接管理交换机，通过业务口可以使用 HTTP、HTTPS、 Telnet、SSH、SNMP 管理交换机。

业务口默认管理 IP：192.168.0.1

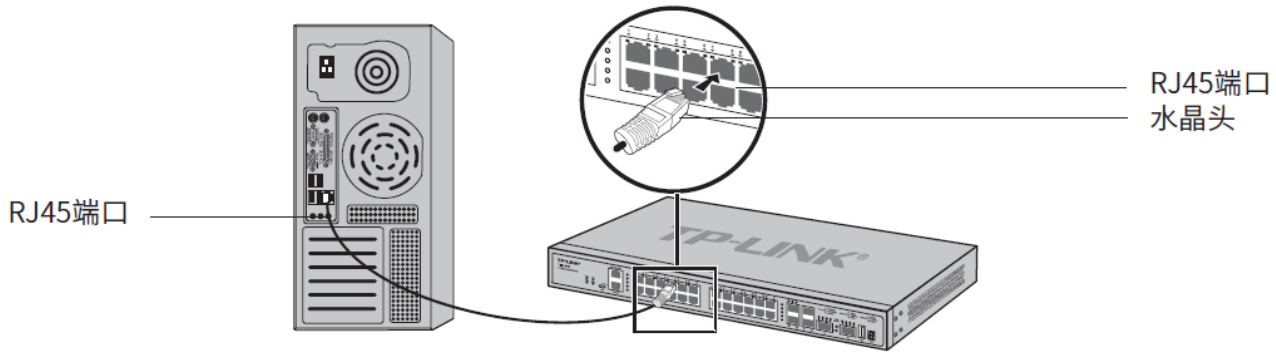
业务口默认管理用户名：admin

业务口默认管理密码：admin

本章介绍交换机在出厂情况下，电脑如何通过业务口使用 HTTP、HTTPS、Telnet、SSH 管理交换机。

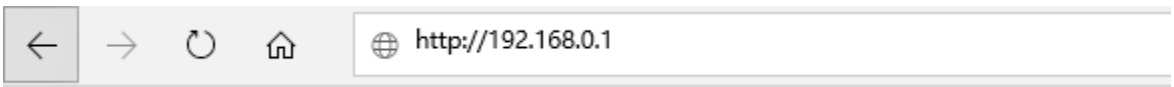
电脑连接方式。

将电脑的网线连接到交换机的业务接口上，如下图所示：



2.2.1 HTTP/HTTPS 管理

1. 打开 IE 浏览器，在地址栏中输入交换机默认管理地址 http://192.168.0.1 或 https://192.168.0.1 登录交换机的 Web 管理界面。建议使用 Chrome、Firefox、Edge 或 IE9 以上的浏览器.



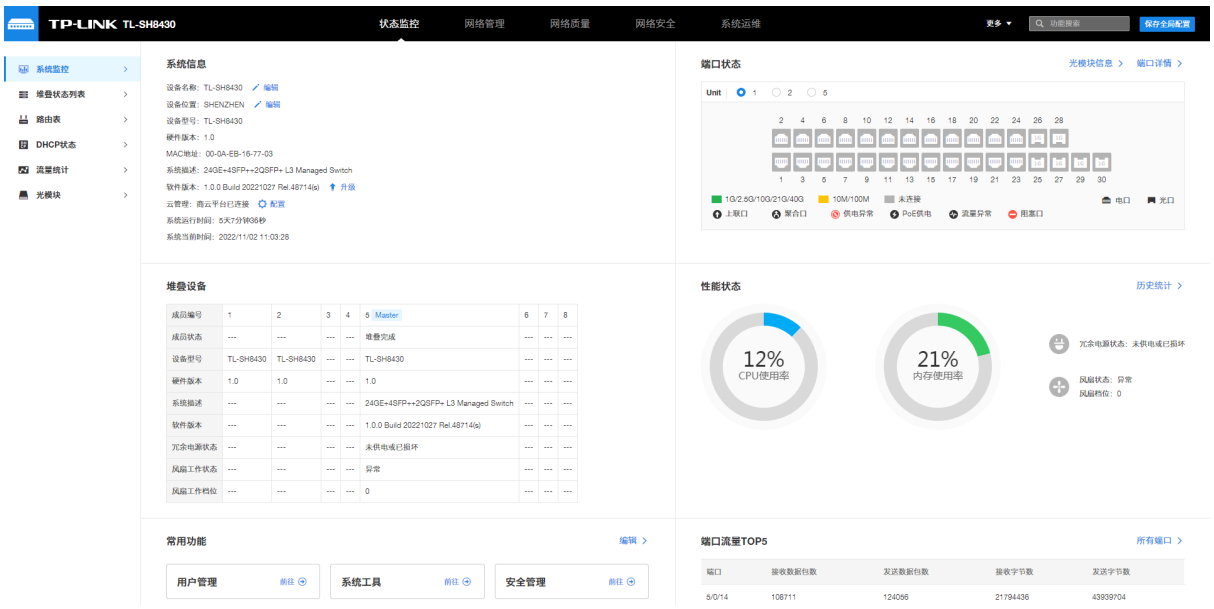
说明：

- 如果使用 HTTPS 管理，浏览器会提示安全风险，在浏览器中点击“详细信息”—”继续转到网页”即可。（不同浏览器提示可能会略有不同）。

2. 首次登录，设置用户名和密码，点击确认。

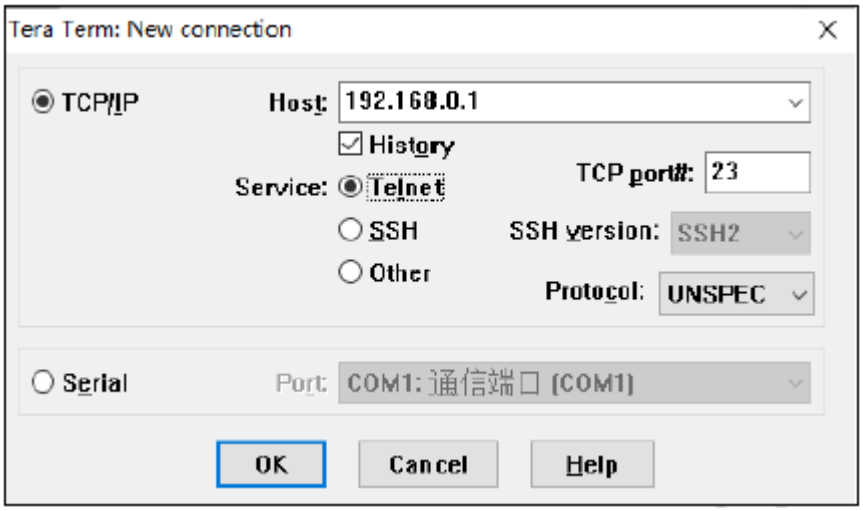
3. 再次输入已设置的交换机管理帐号的用户名和密码，点击登录。

4. 成功登录后将看到交换机的 Web 界面首页，如下图所示。

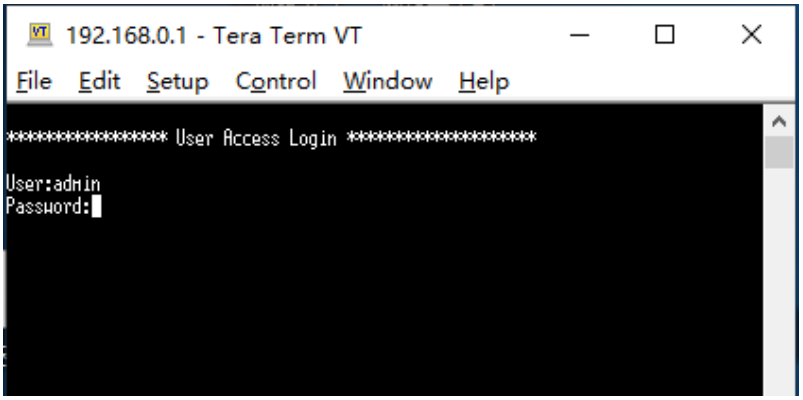


2.2.2 Telnet 管理

1. 电脑上安装 Telnet 客户端软件（比如：Tera Term、SecureCRT 等，本章节以 Tera Term 为例），在 Telnet 客户端软件上新建连接，选择 Telnet 协议，主机 IP 192.168.0.1，端口号 23。



2. 输入正确的用户名和密码。

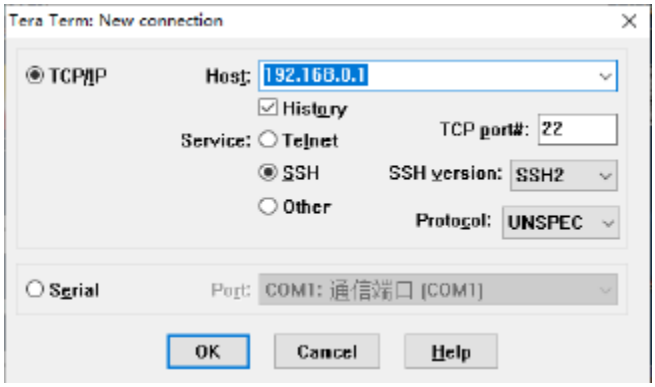


2.2.3 SSH 管理

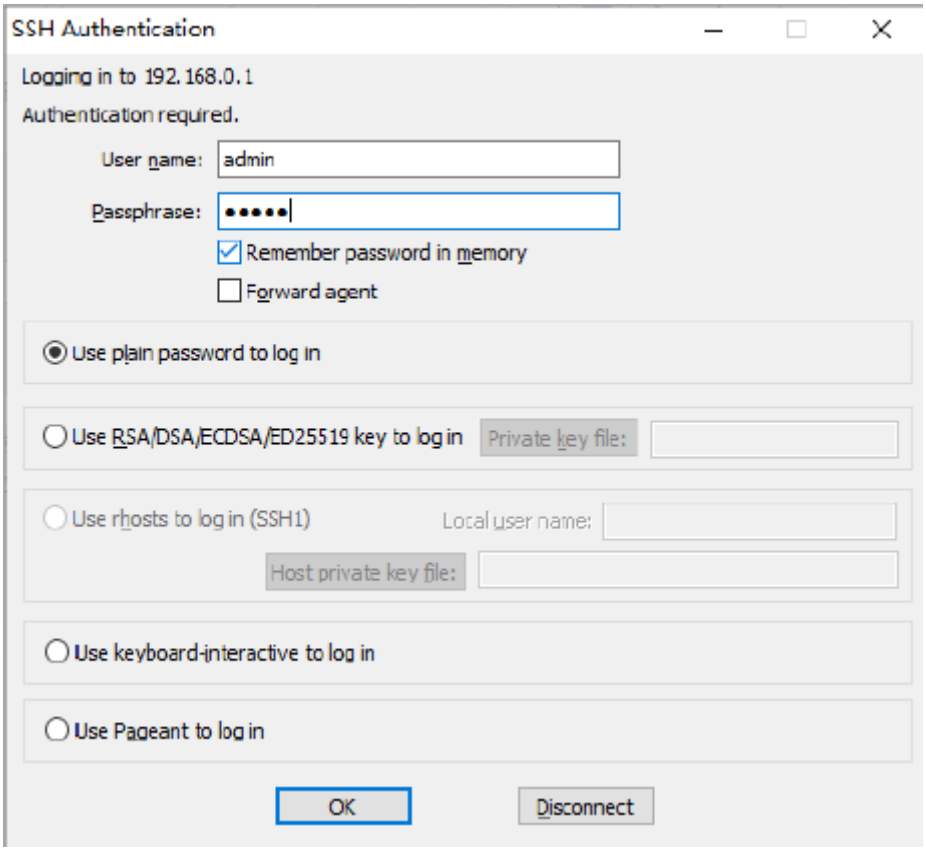
SSH 管理功能在交换机上默认情况下是禁用的，需要先使用其他管理方式进入交换机开启该功能才可以进行 SSH 管理。

1. 电脑登录交换机的 Web 页面，进入“系统运维 >> 系统管理 >> 安全管理 >> SSH 配置”，启用 SSH 配置功能。

2. 电脑上安装 SSH 客户端软件（比如：Tera Term、SecureCRT 等，本章节以 TeraTerm 为例），在 SSH 客户端软件上新建连接，选择 SSH 协议，主机 IP 192.168.0.1，端口号 22。



3. 输入正确的用户名和密码。



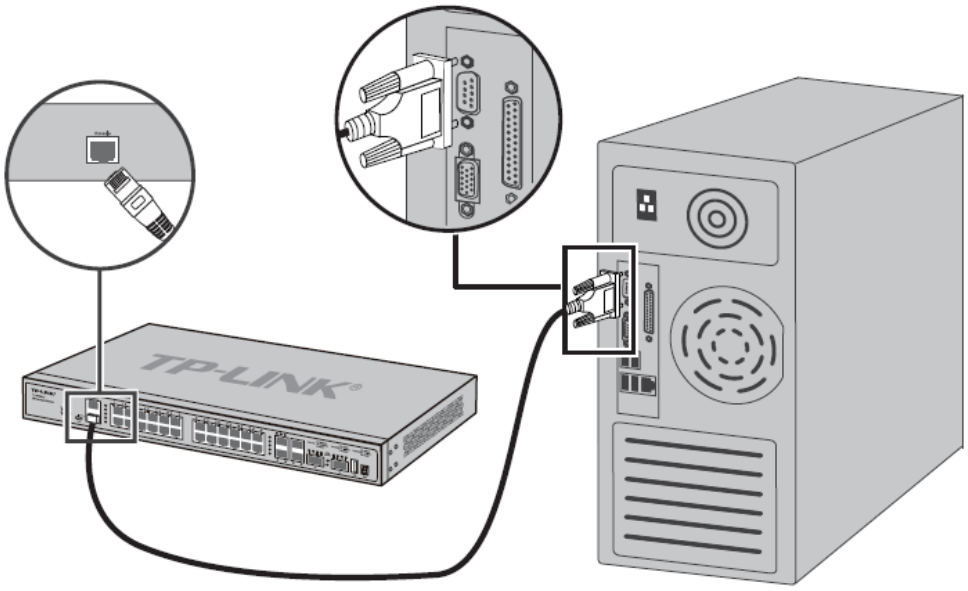
2.3 通过 Console 接口管理

三层网管交换机可以通过 Console 接口进行管理，交换机出厂配置下，使用 Console 管理交换机不需要用户名和密码。

2.3.1 接口连接方式

- **使用串口线连接**

所有三层网管交换机均支持这种方式，串口接电脑，RJ45 接口接交换机的 Console 接口。

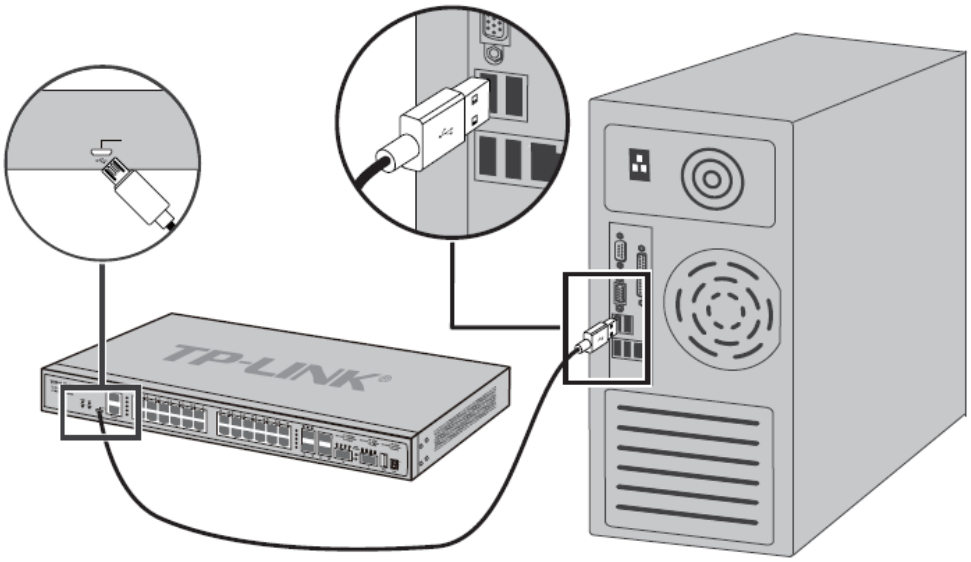


说明：

- 采用这种方式连接电脑必须支持串口，如果电脑没有串口需要自行购买 USB 转串口线。

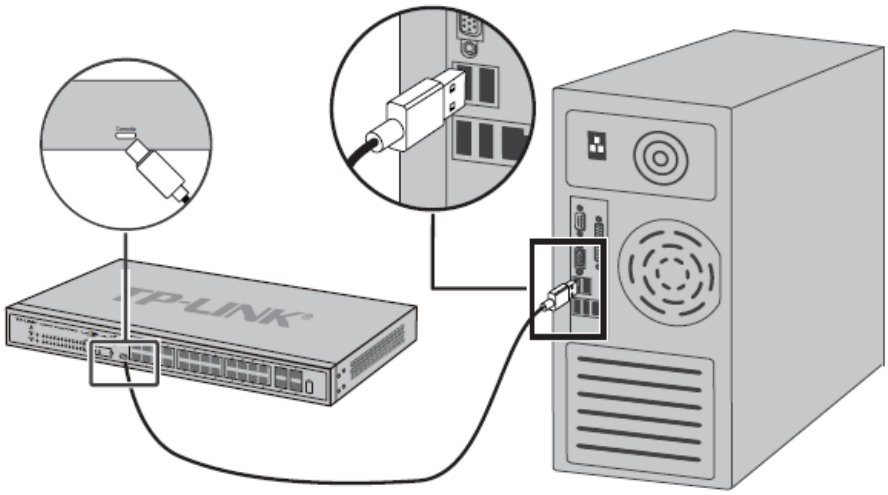
➢ **使用标准 USB 转 Micro USB 线连接**

部分交换机支持这种方式，标准 USB 接电脑，Micro USB 接交换机。



➢ **Type-C Console 端口连接**

部分交换机支持这种方式。



2.3.2 Console 接口管理

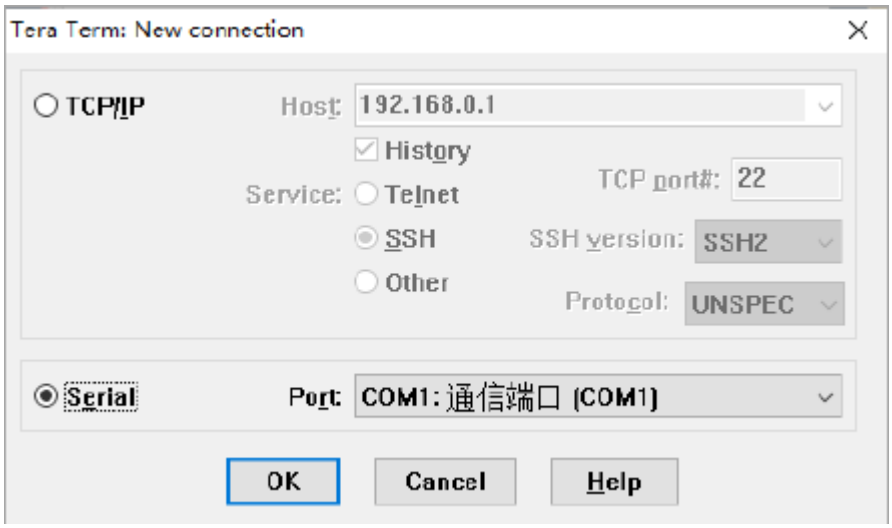
1. 安装驱动。

1） 如果电脑自带串口接口，不需要安装驱动；

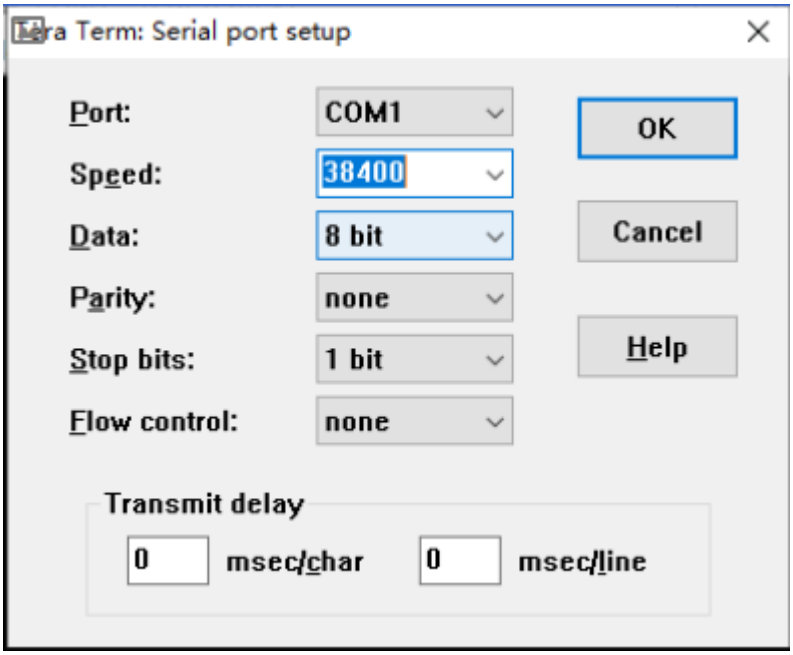
2） 如果使用 USB 转串口线，电脑上需要安装 USB 转串口线的驱动；

3） 如果使用 USB 转 Micro USB 线连接，需要安装“TP-LINK Micro USB 串口驱动程序”。

2. 电脑上安装串口通信客户端软件（比如：Tera Term、SerureCRT 等，本章节以 TeraTerm 为例），在串口通信客户端软件上新建连接，选择 Serial，以及对应的通信端口（不同电脑的通信端口会不一样）。



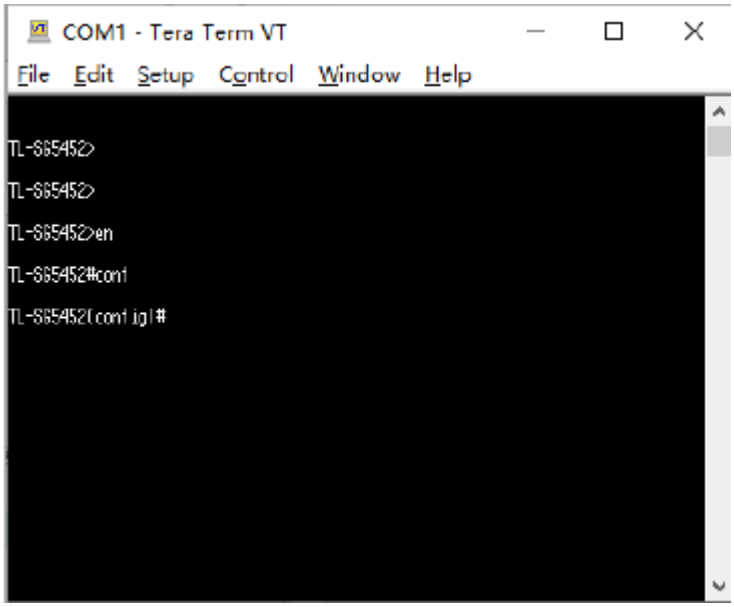
3. Serial Port 相关设置中设置波特率：38400/115200bps、数据位：8bit、奇偶校验：none、停止位：1bit、数据流控制：none。



说明：

- 一般情况下，3/5 系列交换机波特率需设为 38400，6/7/8 系列交换机波特率需设为 115200。
- 如选择某一波特率无法连接时，请尝试更换波特率进行连接。
- 如无法连接，请致电 TP-LINK 技术支持热线 400-8863-400，或发送邮件到 fae@tp-link.com.cn 寻求技术支持。

4. 登录成功之后，直接在窗口中输入管理 CLI 命令即可。

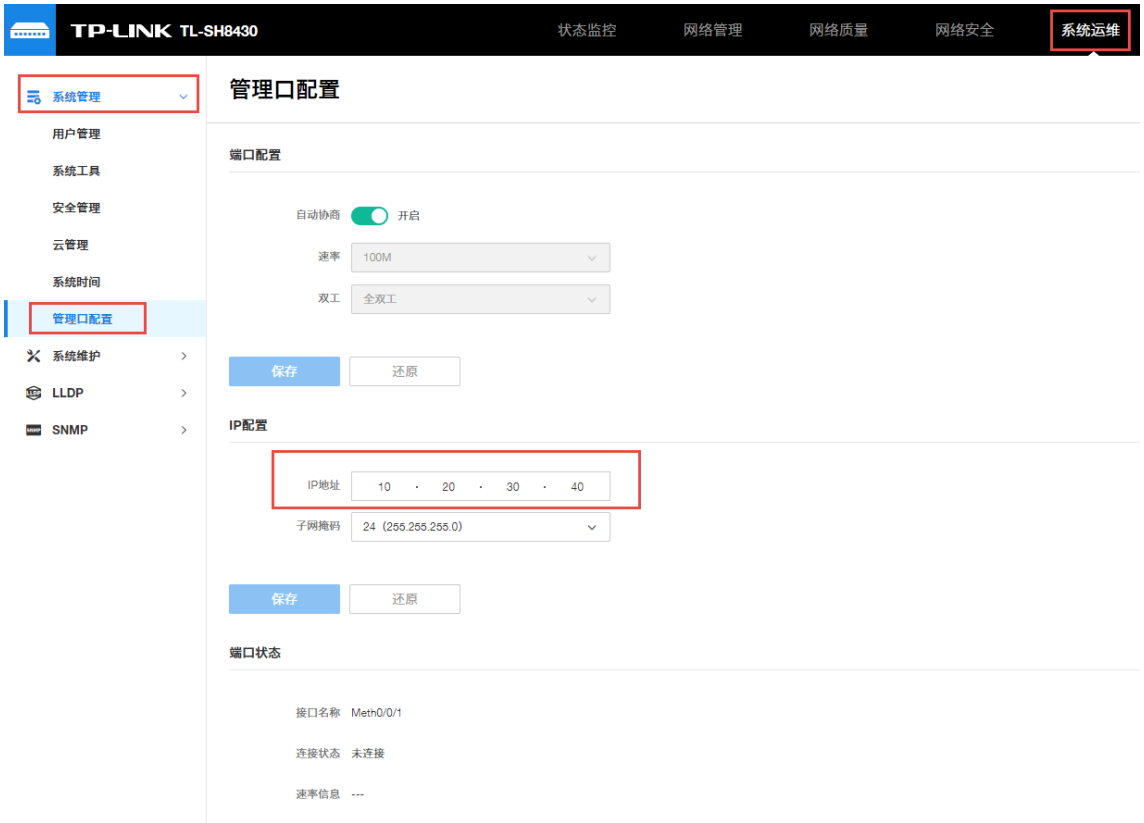


2.4 通过 Management 接口管理

三层网管交换机可以通过 Management 接口管理。（部分交换机不支持该接口）

将电脑的网线连接到交换机的 Management 接（或 MGMT）上。

1. 通过其他管理方式，设置 Management 接口的 IP 地址，以 Web 管理为例在“系统运维 >> 系统管理 >> 管理口设置”中设置 Management 接口的 IP 地址。部分交换机该管理口默认 IP 为 192.168.1.1，部分交换机该管理口默认 IP 为 10.20.30.40。



2. 通过 Management 接口，可以使用 HTTP、HTTPS、Telnet、SSH 等方式管理交换机，具体操作方法与通过业务口连接交换机操作方法一致。

2.5 管理安全

交换机中用户分为 4 个级别，在实际应用过程中根据需求创建用户：

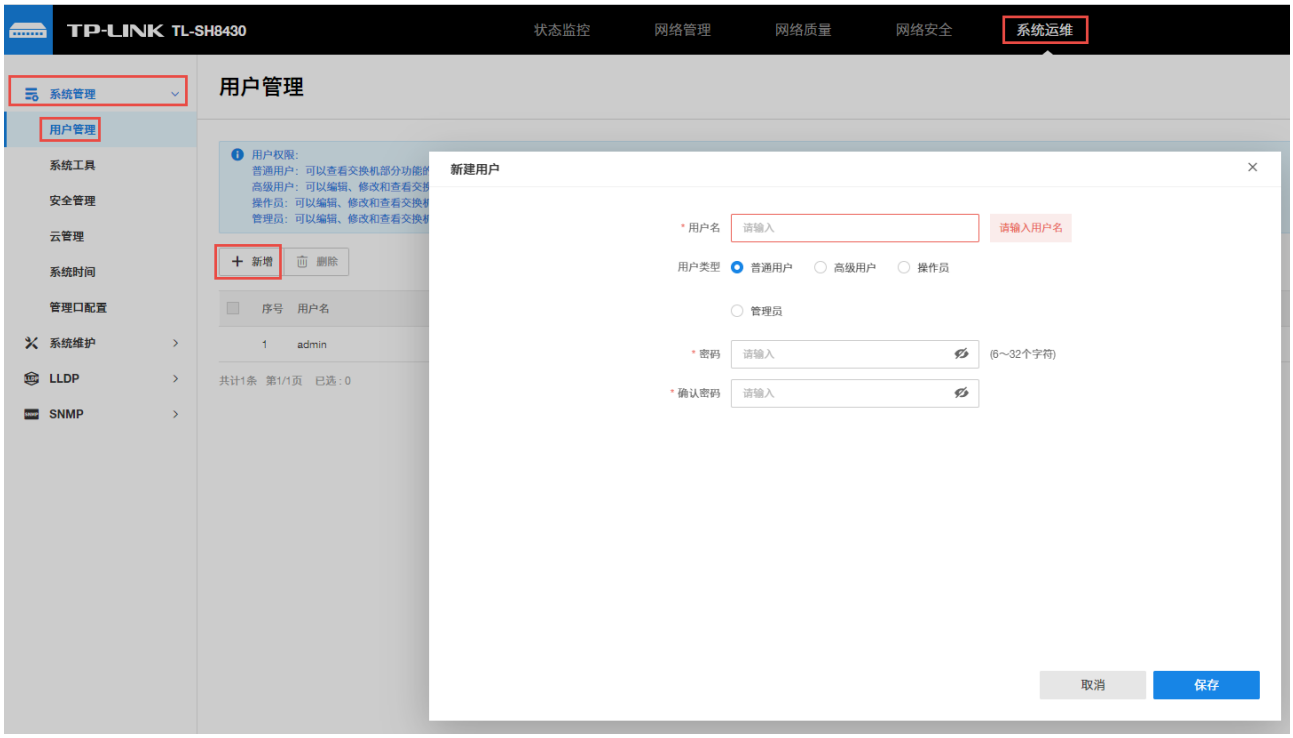
- 管理员：可以设置和修改所有功能，包括创建和修改用户。
- 操作员：可以设置和修改大部分功能，但不能创建和修改用户。(具体不可设置的功能参见用户手册和

命令行手册）

- 高级用户：不可备份和导入配置、不可创建和修改用户，可以设置和修改交换机大部分功能。（具体不可设置的功能参见用户手册和命令行手册）
- 普通用户：仅可以查看交换机部分功能的配置情况。

2.5.1 Web 用户管理

在 Web 管理页面中，进入“系统运维 >> 系统管理 >> 用户管理”，点击<新增>，设置用户名，用户类型和账号密码，点击<保存>即创建完成新用户。



在所创建的用户，点击<编辑>，可以更改用户类型和密码。

如需修改密码，点击<修改密码>，需要输入原始密码，才能设置新密码。

2.5.2 CLI 用户配置实例

需求介绍：交换机中创建一个管理员，用户名 test 密码 test1234567。

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)# user name test privilege admin password test1234567

注意：

如忘记用户名和密码，可以通过 Console 口管理交换机，通过 CLI 创建一个管理员账户，重新管理交换机。

2.5.3 创建特权模式密码配置实例

通过 CLI 管理，在特权模式下，用户可以设置交换机的所有功能，网络管理员可以根据网络安全需要启用 CLI 特权模式密码。

需求介绍：交换机中创建特权密码 test1234567。

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#enable password test1234567

注意：

如忘记特权密码，只能通过复位交换机进入特权模式。

2.5.4 设置 Console 口登录用户名密码认证

如果希望增强交换机 Console 接口管理的安全性，则需要启用交换机的 AAA 认证，通过 AAA 功能给 Console 接口增加用户名和密码。

- **Web 配置举例**

1. 在 Web 管理页面中，进入“网络安全 >> AAA >> 全局配置”，启用 AAA 功能，点击<保存>。

2. 在 Web 管理页面中，进入“网络安全 >> AAA >> 方法列表”，查看“登录方法列表”，默认已经添加了 local 的认证方式，无需额外设置。

➢ **CLI 配置举例**

“登录方法列表”出厂设置默认已经设置好了，CLI 中只要启用 AAA 认证即可。

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#aaa enable

注意：

启用 AAA 认证后，如忘记密码，只能将交换机复位。

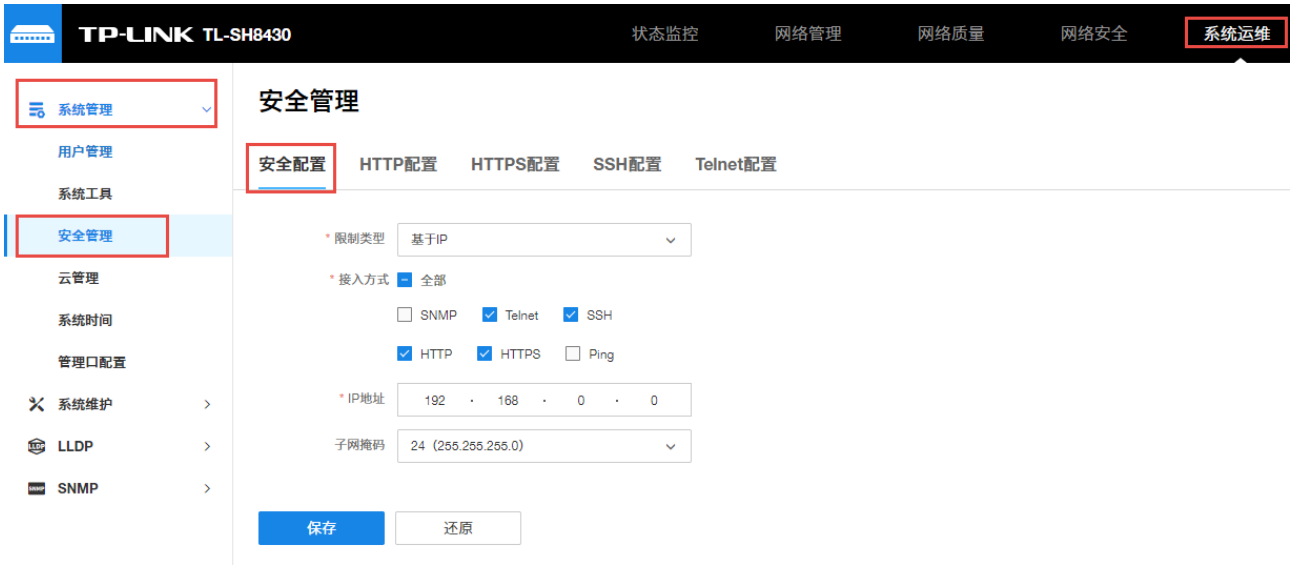
2.5.5 终端权限管理配置实例

交换机可以针对 IP、MAC 和端口来限制管理交换机的用户属性。

➢ **Web 配置举例**

需求介绍：限制只有 192.168.0.0/24 网段的用户才能管理交换机。

在 Web 管理页面中，进入“系统运维 >> 系统管理 >> 安全管理 >> 安全配置”，选择基于 IP 的限制类型，设置接入方式，输入 IP 网段，点击<保存>。



- **CLI 配置举例**

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#user access-control ip-based 192.168.0.0 255.255.255.0 telnet ssh http

2.6 工业交换机拨码开关介绍

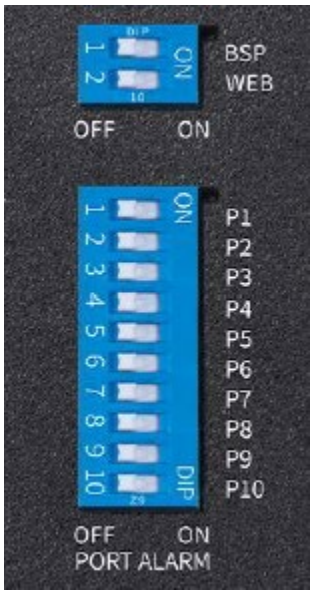
TP-LINK 不同型号的交换机拥有不同的拨码开关，因此可选择的工作模式不一样，适用的场景也不一样，这篇文章主要介绍目前所有的工业交换机的硬件拨码开关及一些使用说明。

- **类型 1**

- VLAN：开启/关闭端口与端口之间相互隔离，只能与上联口通信；
- BSP：开启/关闭广播风暴保护功能；

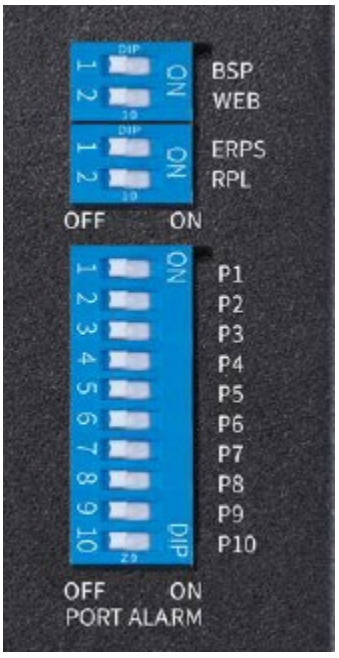
以上两种功能都是用在工业场景，使用者根据实际需求决定是否开启。

➢ **类型 2**



- WEB：交换机支持本地 Web 管理，支持配置端口参数，支持设置端口速率，支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置；部分最新硬件版本（3.0 及以上）的工业级交换机也支持云管理功能，可以通过商云 APP 或者商用网络云平台进程远程管理。
- BSP：开启/关闭广播风暴保护功能；
- DIP 拨码开关（P1-P10）：开启/关闭对应端口中断报警功能，开启后端口如果断开且也通过 FAULT 接线端子接入了报警器的情况下，设备会输出报警信息给报警器产生报警；

➢ **类型 3**



- WEB：交换机支持本地 Web 管理，支持配置端口参数，支持设置端口速率，支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置；部分最新硬件版本（3.0 及以上）的工业级交换机也支持云管理功

能，可以通过商云 APP 或者商用网络云平台进程远程管理。

- BSP：开启/关闭广播风暴保护功能；
- DIP 拨码开关（P1-P10）：开启/关闭对应端口中断报警功能，开启后端口如果断开且也通过 FAULT 接线端子接入了报警器的情况下，设备会输出报警信息给报警器产生报警；
- ERPS：环网开关，默认关闭，需要在 WEB 模式下才能开启，开启后，交换机开启 ERPS 的主环功能，并使能 RPL 开关；
- RPL：默认关闭，开启后，配置端口 1 为 RPL 口。

2.7 交换机复位方法介绍

2.7.1 Web 管理界面复位方法

登录交换机 Web 管理界面，进入页面“系统运维 >> 系统管理 >> 系统工具 >> 恢复出厂”，点击<恢复出厂>，交换机配置将恢复成出厂默认状态，用户配置数据将丢失。

2.7.2 Console 接口复位方法

➢ **Console 接口未设置登录密码**

1. 电脑连接交换机的 Console 接口，具体连接和设置方法参见 2.3 通过 Console 接口管理。
2. 使用 reset 命令对交换机进行复位。

复位命令举例：

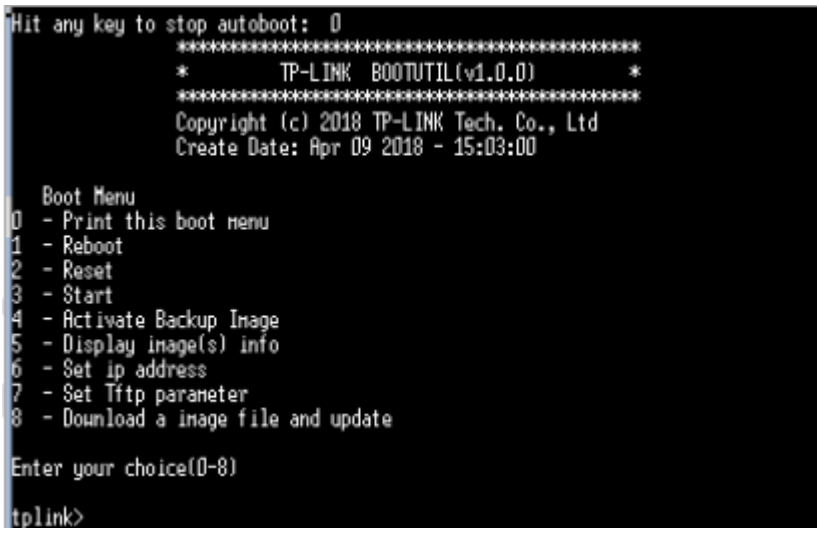
TL-SH7428>enable

TL-SH7428#reset

System software reset, are you sure? (Y/N):y

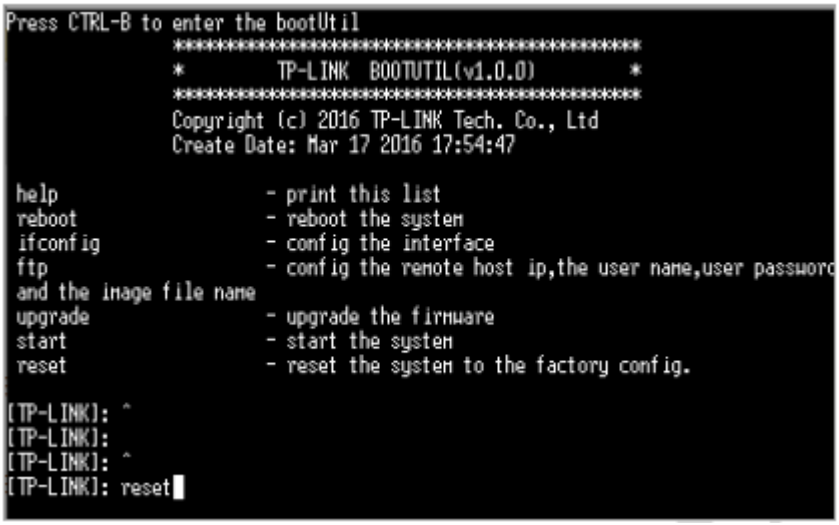
- **Console 接口设置了登录密码**

1. 电脑连接交换机的 Console 接口，具体连接和设置方法参见 2.3 通过 Console 接口管理。
2. 对设备重新上电的过程中，当串口界面中出现“Hit any key to stop autoboot”提示的时候，按任意键，出现如下界面：



3. 选择 2，选择复位交换机。

4. 如果交换机使用的比较早期的软件版本，在启动时，当串口界面中出现“Press CTRL-B to enter the bootUtil”及时按下 Ctrl+B，在出现的界面中选择 reset。

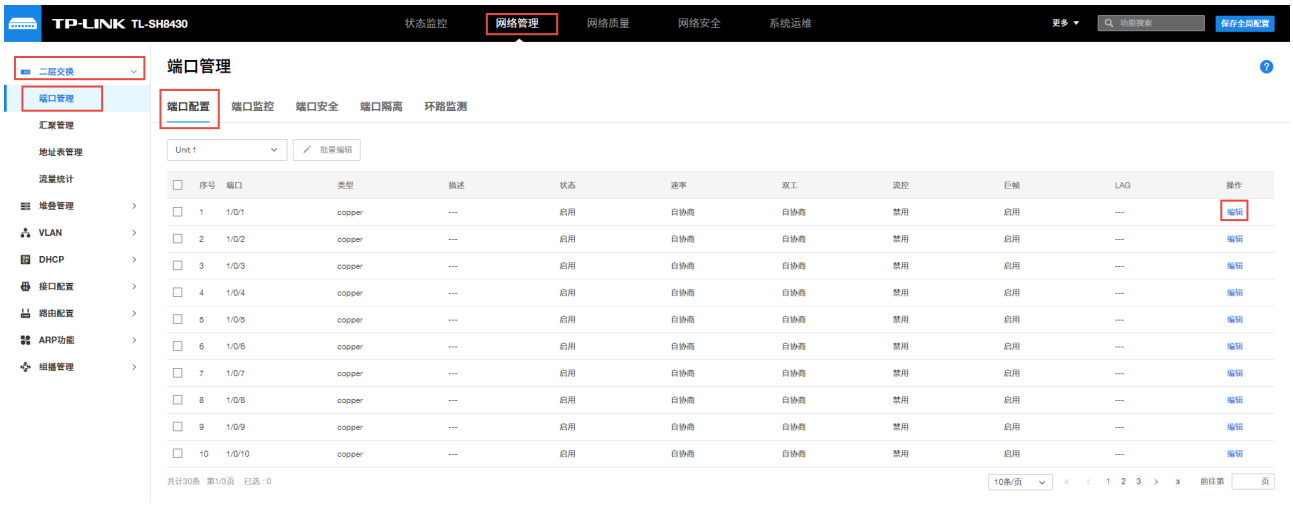


回目录

第3章　交换机设置

3.1　端口通用配置

进入页面：网络管理 >> 二层交换 >> 端口管理 >> 端口配置，选中交换机端口，点击<编辑>，可启用/禁用端口，设置端口速率，配置双工速率，启用流控或巨帧。



- **启用/禁用端口**

交换机允许启用或禁用端口。端口选择“启用”时，可以正常转发报文。端口状态选择“禁用”时，交换机将丢弃来自这个端口的数据包。当交换机端口长时间不使用时，可以将该端口设为禁用，可有效减小交换机的功耗，待使用时再将该端口设为启用。

- **配置端口速率/双工模式**

与交换机相连的设备端口必须与交换机端口的传输速率及双工状态保持一致。当选择“自动”选项时，该端口的速率和双工模式由自动协商决定。默认为自动。

- **配置端口流量控制功能**

启用端口流量控制功能能防止交换机因阻塞而丢包。当交换机某端口在短时间内收到较多报文，而交换机没有能力处理这些报文时，为了防止报文因拥塞被丢弃。交换机通知该端口报文的发送者暂时停止发送报文。

- **配置巨帧控制功能**

巨帧指有效负载超过 IEEE 802.3 标准所限制的 1500 字节的以太网帧。

3.2 端口监控功能

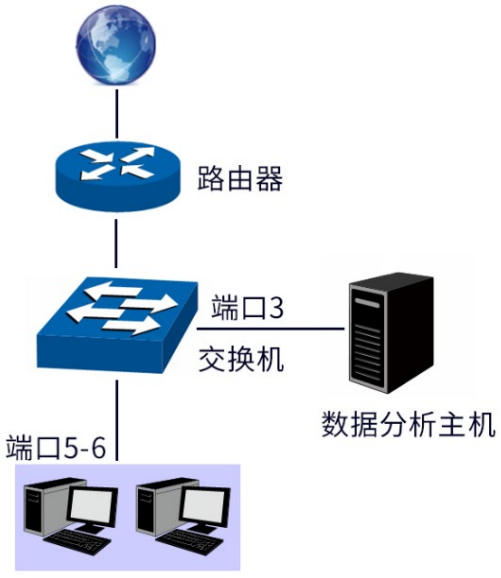
3.2.1 端口监控介绍

端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

3.2.2 端口监控配置实例

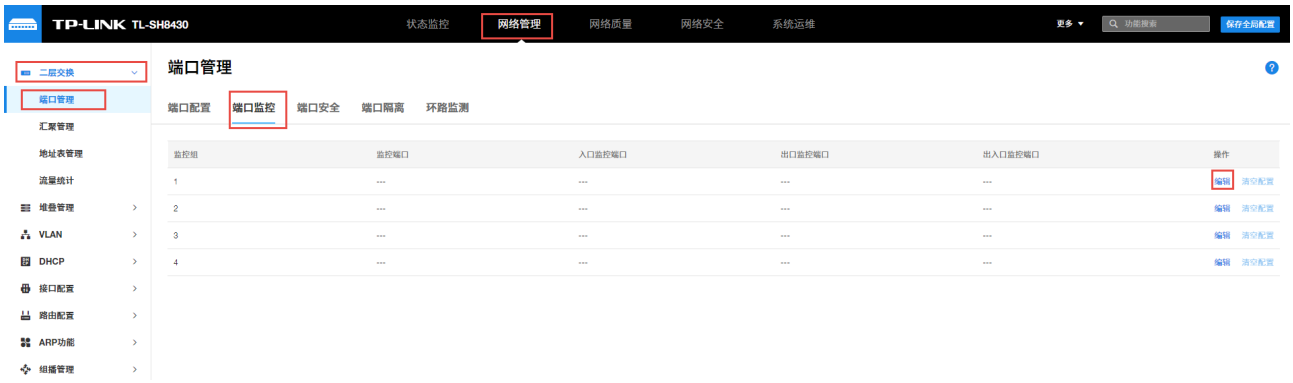
组网介绍：

网络中有一台安装了数据包分析软件的主机连接在交换机的 3 号端口，需要对网络中电脑的上网行为进行监控。示意网络拓扑如下：



配置步骤：

1. 进入页面：网络管理 >> 二层交换 >> 端口管理 >> 端口监控，选中监控组，点击<编辑>。



2. 选择监控端口 3 的，并点击提交；在被监控端口中选择需要被监控的端口 5 和端口 6，入口出口均选择启用，配置完成后，点击<保存>。

注意：

设置过多被监控端口可能造成网络不稳定，网络中流量较大时不建议一次性设置过多被监控端口。

3.3 端口安全功能

3.3.1 应用介绍

一些网络场景下需要通过限制端口的最大学习 MAC 数目，来防范 MAC 地址攻击和控制端口的网络流量。如果端口启用端口安全功能，将动态学习接入的 MAC 地址，当学习地址数达到最大值时停止学习。此后，MAC 地址未被学习的网络设备将不能再通过该端口接入网络，保证安全性，通常将静态地址表+端口安全结合起来使用。

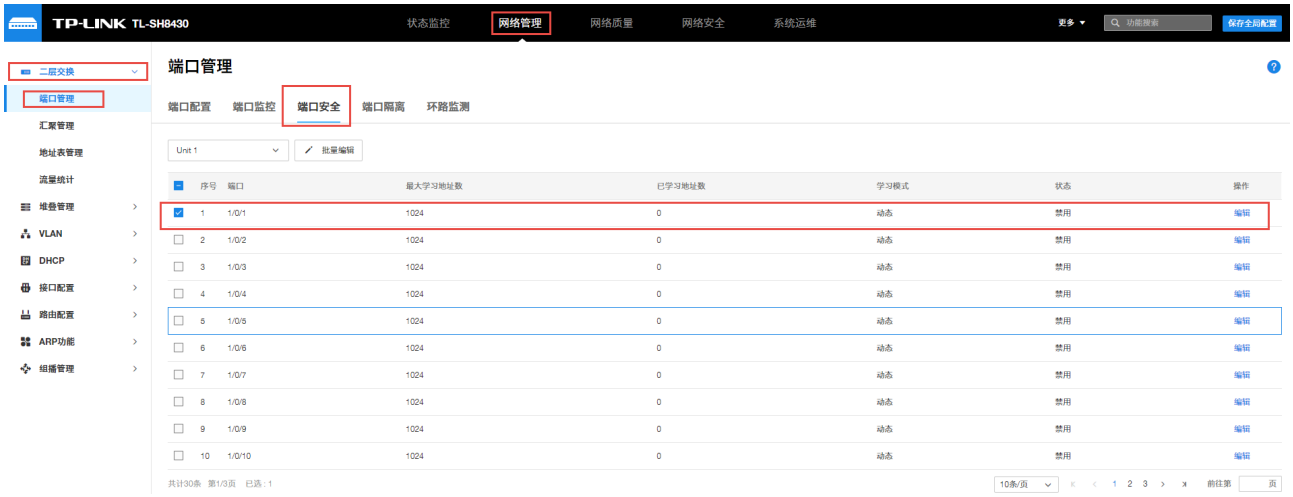
3.3.2 端口安全配置实例

组网介绍：

某公司管理员要求交换机的端口 1 只能是静态地址表中 1 个 MAC 对应的设备可以上网，不在静态地址表中的设备则无法上网，那么设置端口安全功能针对端口 1 设置最大学习地址数为 0.，并且在静态地址表中添加允许上网的这个设备的 MAC。

配置步骤：

1. 进入页面：网络管理 >> 二层交换 >> 端口管理 >> 端口安全，勾选端口号 1，点击<编辑>。



2. 设置端口最大学习地址数为 0，学习模式为永久，端口状态为启用。设置完成后，点击<保存>。

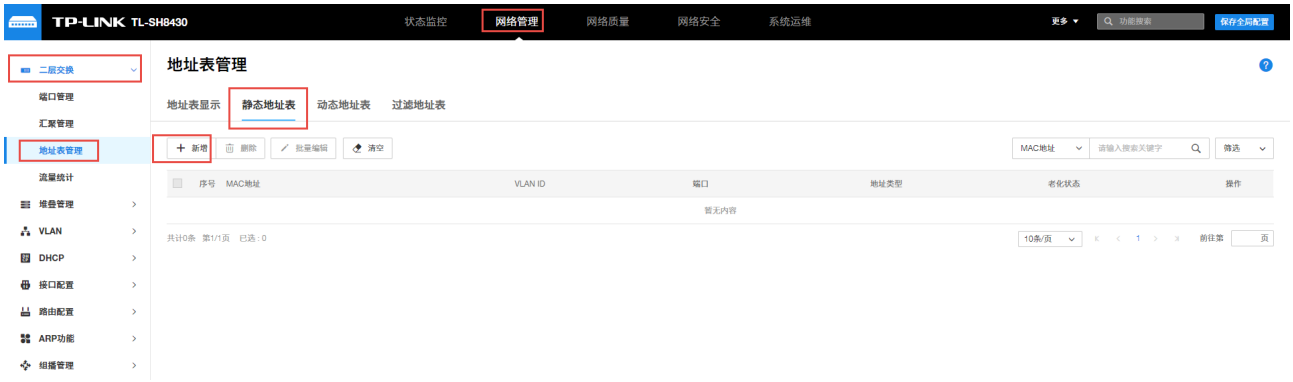
学习模式 动态：MAC 地址学习受老化时间的限制，老化时间过后，所学的 MAC 地址将被删除。

静态：MAC 地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目清空。

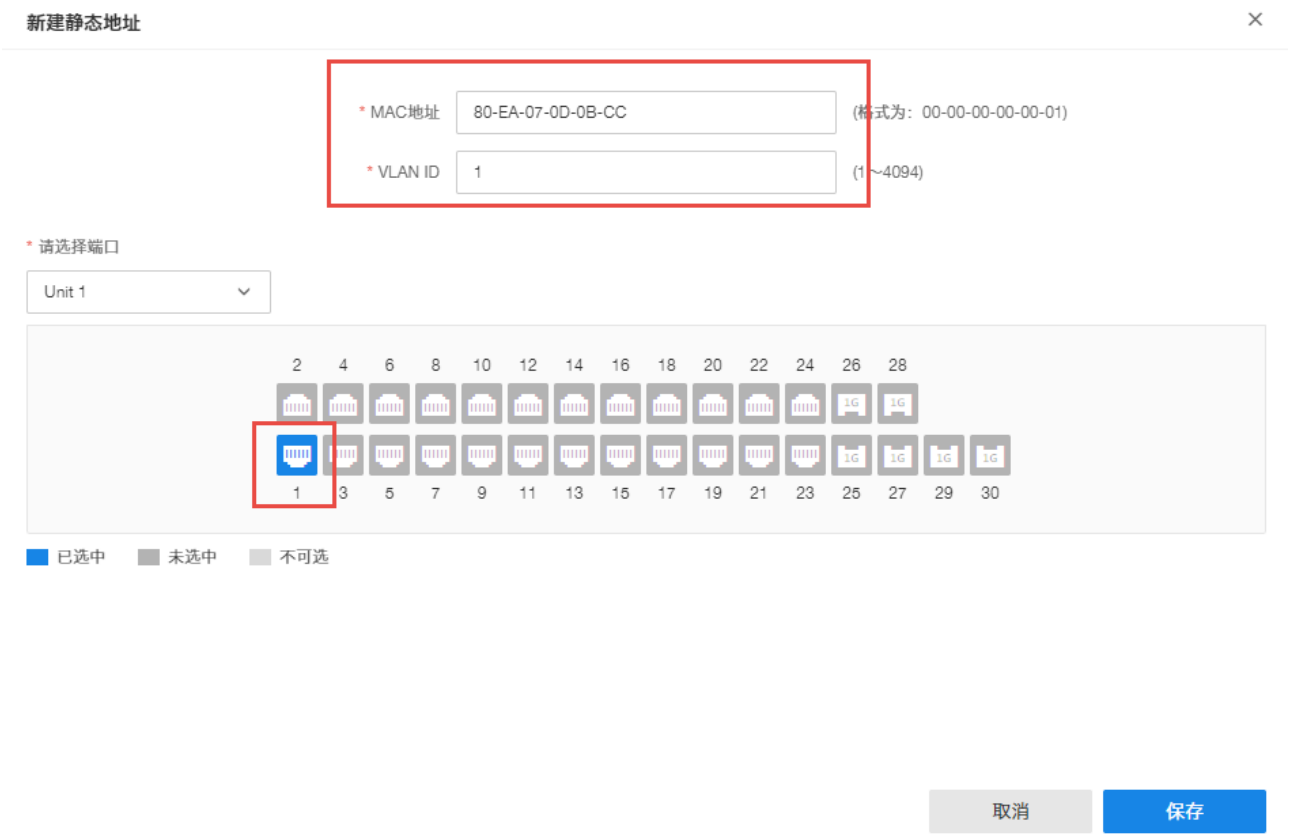
永久：MAC 地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目保持不变。

状态 设置当前端口安全功能是否启用。

3. 针对端口 1 做静态地址绑定，绑定允许上网的设备。进入页面：网络管理 >> 二层交换 >> 地址表管理 >> 静态地址表，点击<新增>。



4. 将 MAC 地址 80-EA-07-0D-0B-CC 的设备绑定在端口 1 下，则该设备接在端口 1 的 VLAN1 下能上网，其他设备接到端口 1 则无法上网。



3.4 端口隔离

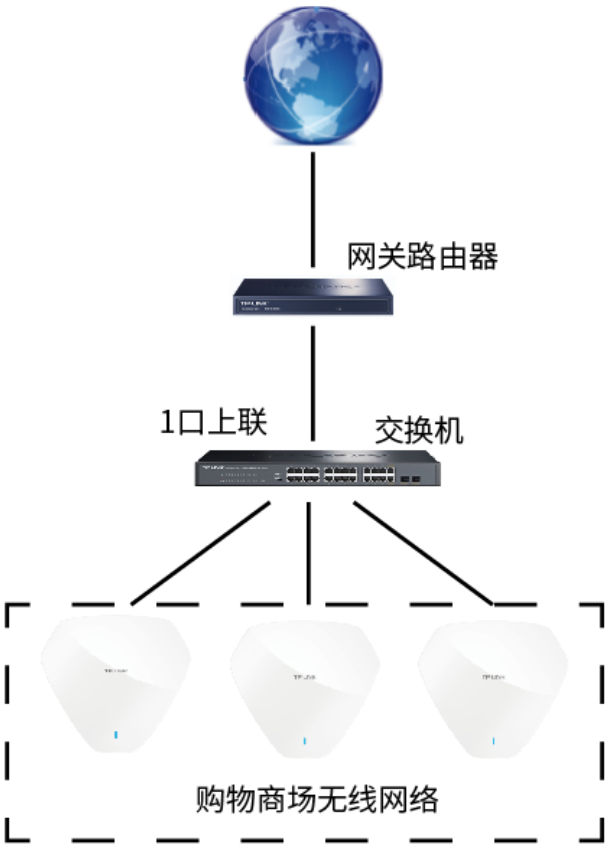
3.4.1 应用介绍

端口隔离功能可以限制一个端口到另外一组端口的数据转发。这种限制数据转发的方式和通过 VLAN 进行限制的方式很相似，但是限制性更强。通过设置端口隔离可以在物理上隔绝开两个端口通讯，一般适用于一些对广播流量比较敏感的场所，通过设置端口隔离来隔绝广播域。

3.4.2 端口隔离配置实例

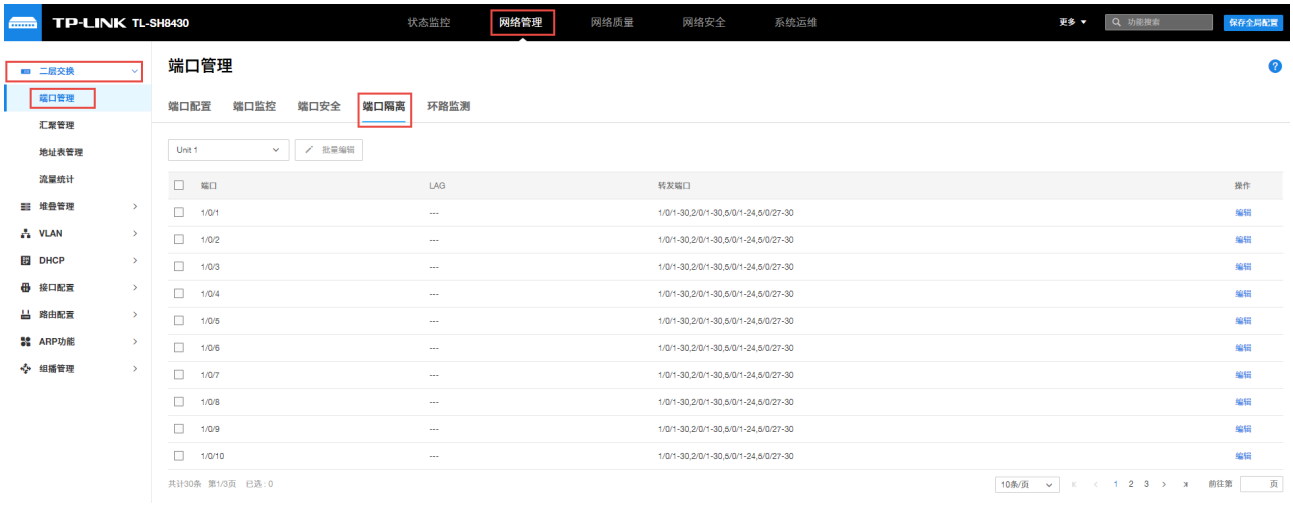
组网介绍：

某购物商场进行无线覆盖组网，使用双频 AP 搭配 AC 的组网方案，为了隔离 AP 和 AP 之间的通讯，减少广播流量的干扰，增强无线的运行稳定性，采用在接入交换机上进行端口隔离的设置，使 AP 只能和上联的 AC 通讯，相互之前不能通讯，网络拓扑如下：

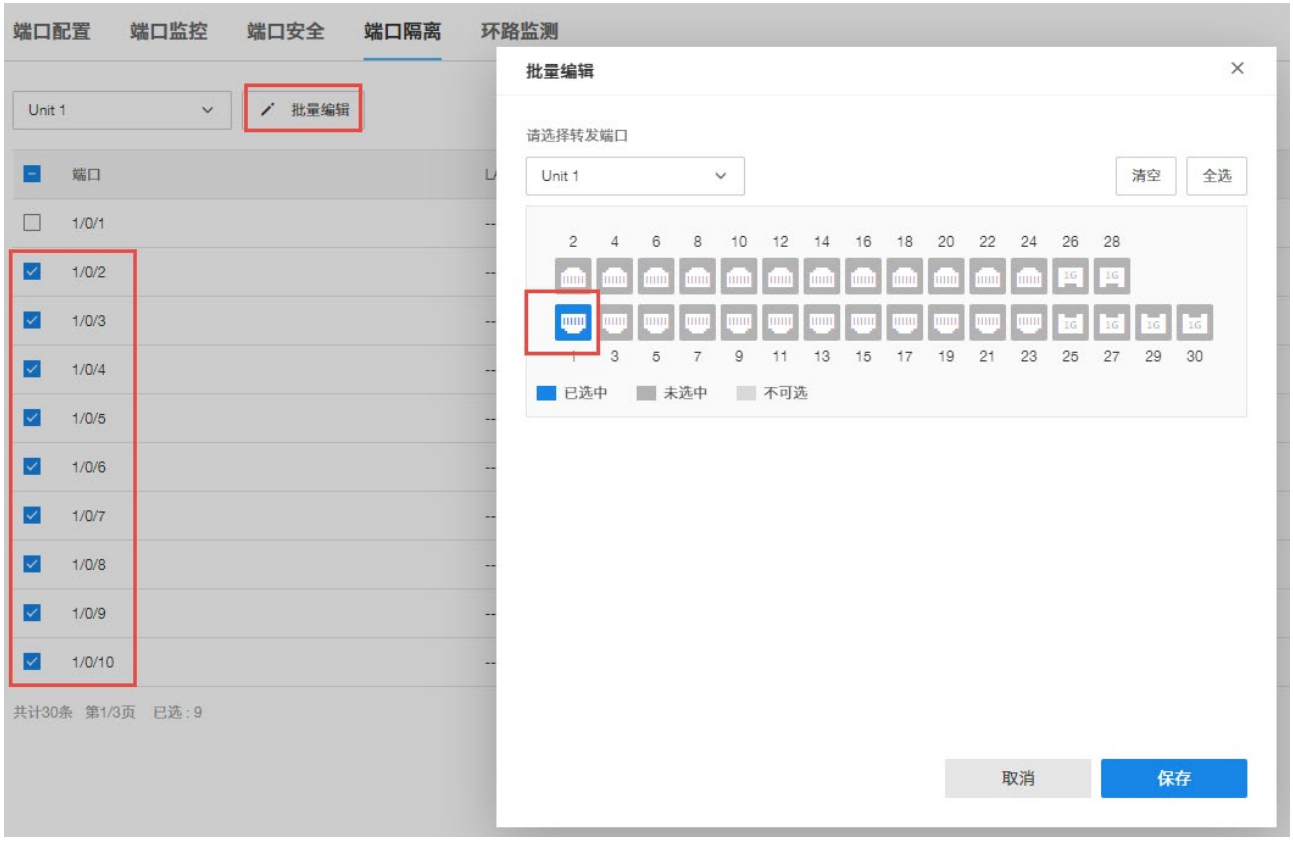


配置步骤：

1. 进入页面：网络管理 >> 二层交换 >> 端口管理 >> 端口隔离。



2. 端口的转发端口为 1 端口，勾选端口 2-30，点击<批量编辑>，设置转发端口为端口 1。



3. 端口 1 可向端口 1-30 转发数据，在端口 1 条目中，点击<编辑>，端口 1 可向端口 1-30 转发。

3.5 环路检测

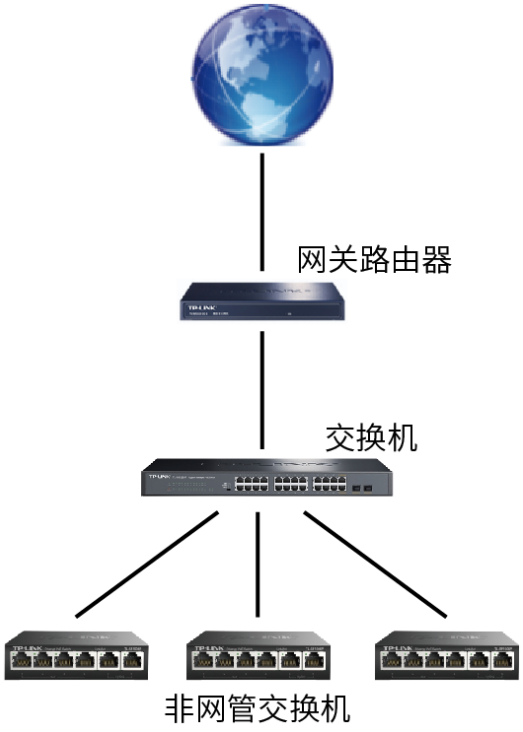
3.5.1 应用介绍

环路即交换机网络形成了环状的拓扑结构，环路会造成内网广播风暴，消耗交换机大量的 CPU 和线路带宽，严重时甚至可能造成设备死机、网络瘫痪。开启环回保护功能，当某个端口检测到环路后，当检测出环路时根据用户设定处理相应的端口。若处理方式为阻塞端口，则通过被阻塞的端口对下接网络进行排查以便彻底消除环路。

3.5.2 环回监测配置实例

组网介绍：

很多企业使用三层管理型交换机作为主交换机，下接多台非管理型交换机，由于网络比较庞大，容易形成环路，仅靠管理员维护检测难以实现，需要开启环回保护以消除环路。此处介绍交换机设置环回监测的方法，示意网络拓扑如下：

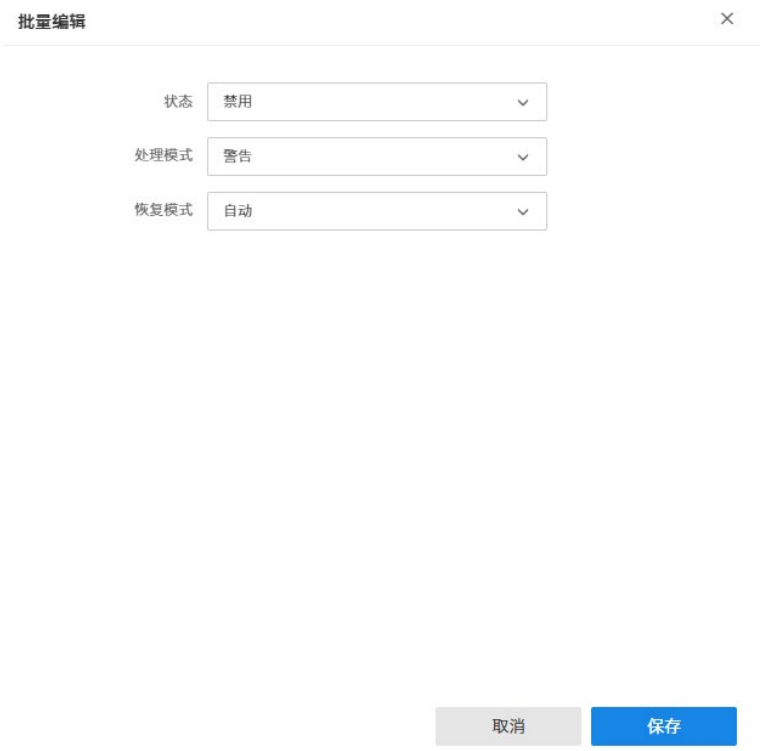


配置步骤：

1. 进入页面：网络管理 >> 二层交换 >> 端口管理 >> 环路监测，在全局配置中，开启环路监测功能，设置监测间隔和自动恢复时间，点击<保存>保存配置。

环路监测间隔	交换机按照该时间间隔为周期进行环路监测。
自动恢复时间	设置被阻塞环路端口的自动恢复时间，设置值为环路监测间隔的整倍数。

2. 在端口配置中，选中对应端口，点击<编辑>，或同时勾选多个端口，点击<批量编辑>。开启所选端口的环路监测功能，设置环路发生时的处理模式和恢复模式。



状态	开启/禁用端口的环路监测功能。
处理模式	选择端口发现环路时的处理模式 • 警告：端口上发现环路时只发出报警信息。 • 阻塞端口：端口上发现环路时发出报警信息，同时阻塞端口。

恢复模式	选择端口被阻塞后的恢复模式。 • 自动：端口被阻塞后经过自动恢复时间后会自动解除阻塞。 • 手动：端口被阻塞后只能手动解除阻塞状态。

注意保存配置以免掉电导致配置丢失。

3.6 配置端口汇聚功能

3.6.1 端口汇聚介绍

端口汇聚是一种增加端口最大带宽的技术，将交换机的多个物理端口汇聚在一起形成一个逻辑端口，多端口形成的多条链路可视为一条逻辑链路。普通千兆的端口最大传输速率为 1000Mbps，在某些服务器或者交换机对接的场景下要求端口速率叠加，增加内网的传输速率，因此就可以利用交换机的端口汇聚功能来做到端口速率的叠加，增加内网的传输速率。

LAG（Link Aggregation Group，端口汇聚组）可以实现流量在汇聚组中各个成员端口之间进行分担，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。属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 QoS、VLAN、端口属性等。具体说明如下：开启 802.1Q VLAN、QoS 配置及端口配置（速率、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。

如果需要配置汇聚组，建议在本功能处优先配置汇聚组后，再去其它功能处配置汇聚组的其它功能。

进入页面：二层交换 >> 汇聚管理。选择汇聚组，选择汇聚端口作为汇聚组成员。点击<应用>使配置生效。

说明：

- LAG 带宽的计算：当使用四个全双工 1000Mbps 端口构成 LAG 时，由于每一个端口上行和下行各是 1000Mbps，所以每一个端口的带宽为 2000Mbps。它们使用 LAG 技术汇聚在一起可以形成的最大总带宽为 8000Mbps。
- LAG 的流量会根据选路算法均衡分配到各个成员端口中去。当 LAG 中的一个或几个端口连接断开的时候，这些端口的流量会转移到 LAG 中其它链接正常的端口中去，即具备链路冗余备份功能。
- 最多可创建 8 个汇聚组，每个汇聚组最多可以有 4 个成员端口。
- 监控端口不能被加入到汇聚组。

注意：

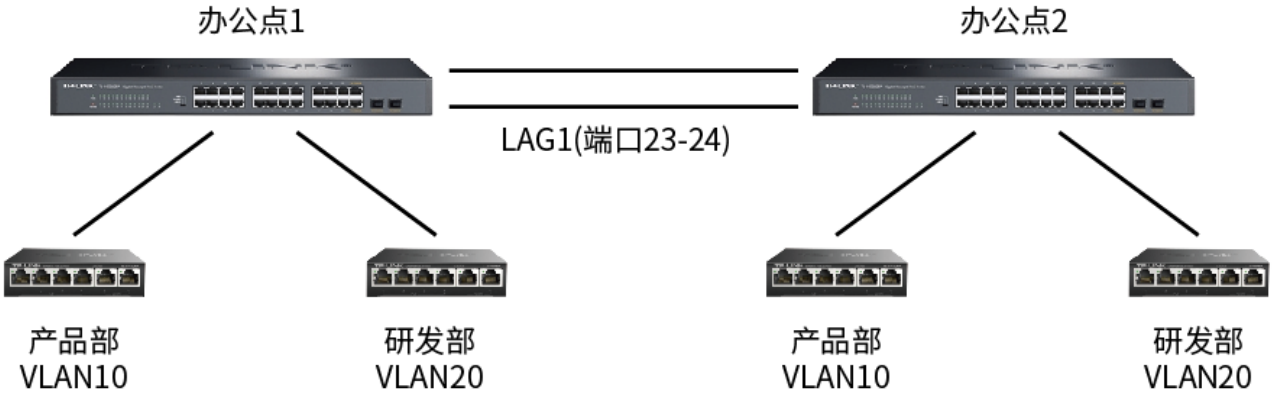
- 属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、 VLAN、端口属性、MAC 地址学习等。如果需要配置汇聚组，建议在优先配置汇聚组后，再配置汇聚组的其它功能。如果两台设备之间做端口汇聚，两者必须都支持端口汇聚，否则可能会导致环路。

- 开启 802.1Q VLAN、语音 VLAN、生成树、QoS 配置、DHCP 侦听及端口配置（速率、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。
- 开启端口安全、端口监控、MAC 地址过滤、静态 MAC 地址绑定、半双工及 802.1X 认证功能的端口，不能加入汇聚组。
- 开启 ARP 防护、DoS 防护功能的端口，建议不要将其加入汇聚组。
- 链路聚合分为静态聚合和动态聚合，实际应用中使用其中一种即可，我司产品推荐使用静态聚合的方式。

3.6.2 端口汇聚配置实例

组网介绍：

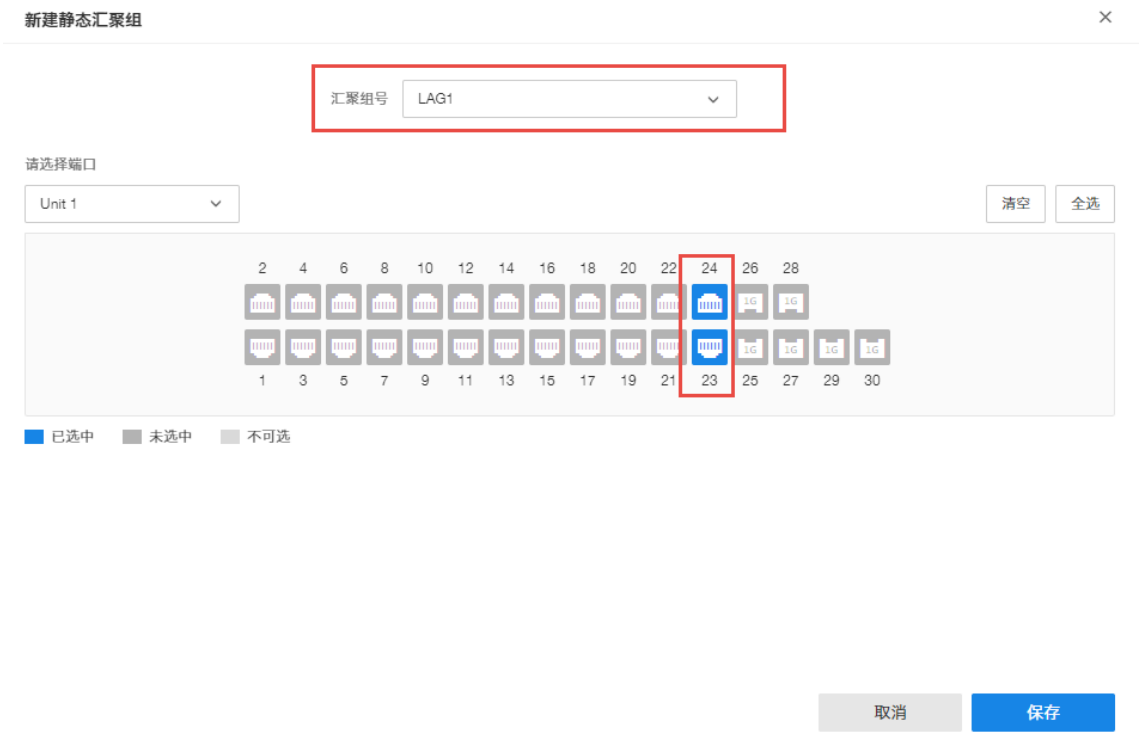
某企业中有两个部门，每个部门有两个办公点，每个办公点的两个部门各有一个接入交换机，不同办公点之间通过核心交换机进行连接，现在需要核心交换机之间的链路进行汇聚，同时不同部门需设置不同VLAN。网络拓扑如下：



➢ **静态聚合配置方法**

配置步骤：

1. 进入页面：网络管理 >> 二层交换 >> 汇聚管理 >> 汇聚列表，点击<新增静态汇聚>，设置汇聚组号如 LAG1，选择需要进行汇聚的端口如 23-24 号端口，点击<保存>。



2. 在另一台交换机上设置端口 23-24 为汇聚口，并连接两台交换机的端口 23-24。完成交换机的端口汇聚功能配置。注意保存配置以免掉电导致配置丢失。

- **动态聚合配置方法**

配置步骤：

进入页面：网络管理 >> 二层交换 >> 汇聚管理 >> 配置 LACP，选择需汇聚的端口 23 和 24，点击<编辑>，或者同时勾选端口 23 和 24，点击<批量修改>。

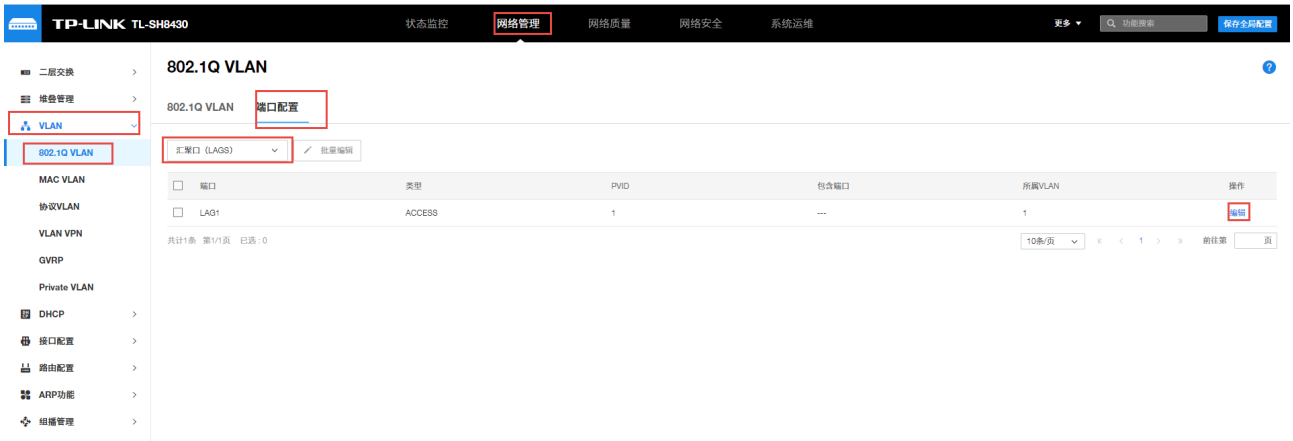
开启 LACP 功能，设置管理 KEY 即汇聚组号如 LAG 1。

管理 KEY	处于同一汇聚组的成员，需配置相同的管理 Key，并且 Key 值和已有的 LAG 值不能相同，此处 Key 等同于 LAG 号。
端口优先级	决定了成为汇聚组成员的端口的优先级。在本端系统优先级较高的情况下，端口优先级值小的端口会优先被选择为动态汇聚组成员。若端口优先级相同，则端口号小的会优先被选择为动态汇聚组成员。
模式	选择相应端口的 LACP 模式。

- **VLAN 设置时如何使用汇聚端口**

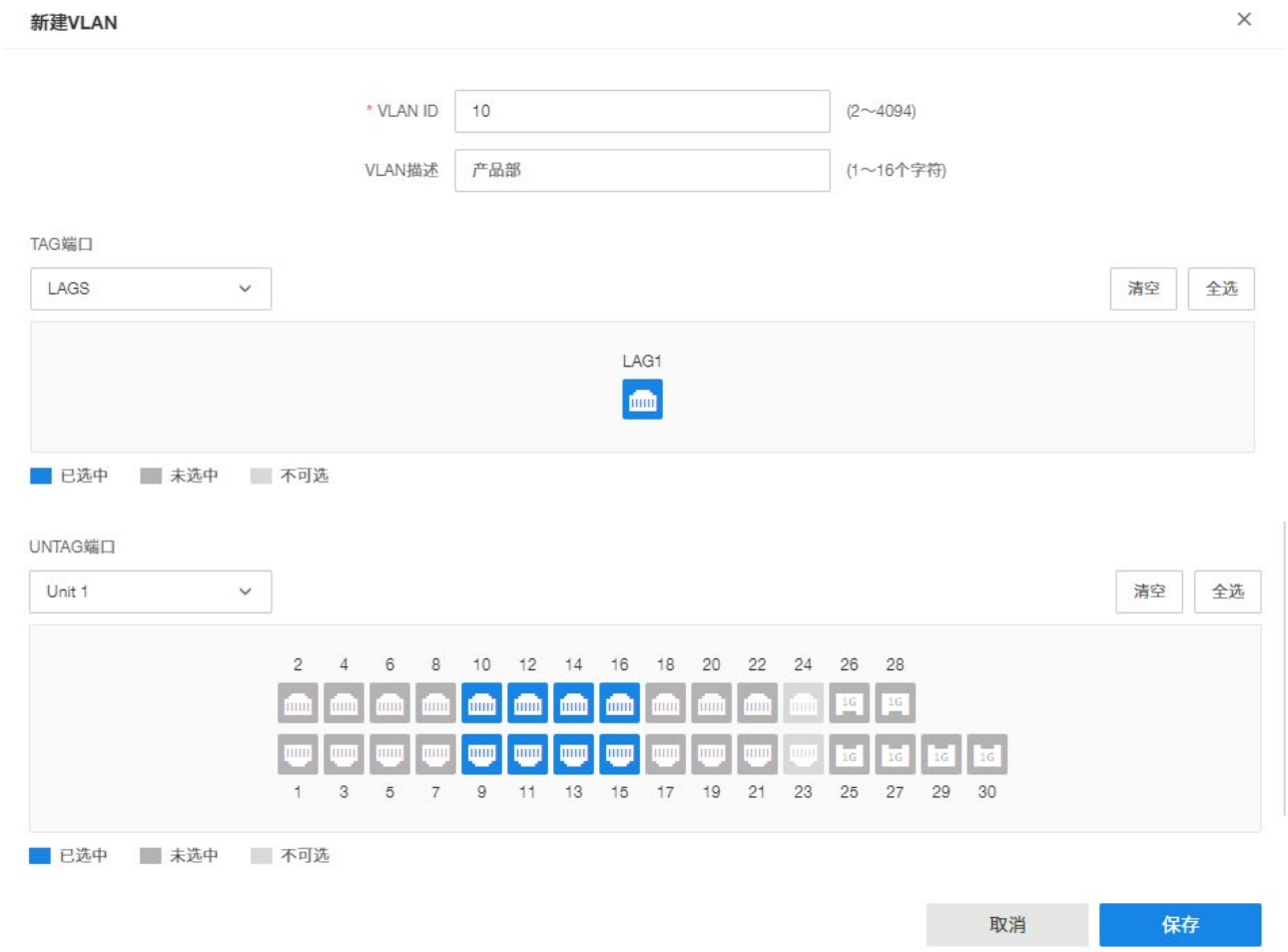
多个端口进行汇聚后在逻辑上是一个端口，进行 VLAN 设置时与普通端口类似，只是需要注意手动选择 LAGS 列表。具体设置方法如下：

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择汇聚口（LAGS），对汇聚端口点击<编辑>。



2. 将汇聚口端口类型配置为 TRUNK，属于默认 VLAN 1

3. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，分别创建 VLAN10、VLAN20 选择对应的端口，注意汇聚端口需设置为 Tagged，在 Tagged 端口的 UNIT 列表中选择 LAGS，Untagged 端口选择 9-16，点击<保存>。



4. VLAN20 的设置步骤同 VLAN10.

至此已完成设置，注意保存配置以免掉电导致配置丢失。

3.7 地址表管理

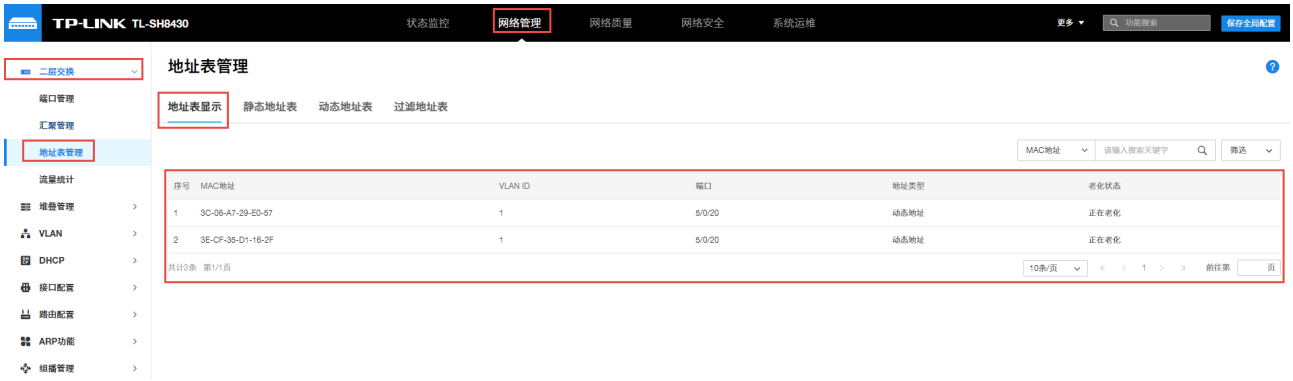
3.7.1 MAC 搜索介绍

TP-LINK 三层网管交换机都带有地址表管理功能，交换机的地址表管理功能是管理交换机所学习到 MAC 的集中展示的地方，通过交换机的地址表管理功能，可以优化网络流量或者保障络安全。交换机的地址表管理功能主要分以下几个功能模块，现分别简介下各个模块的功能和应用场景。

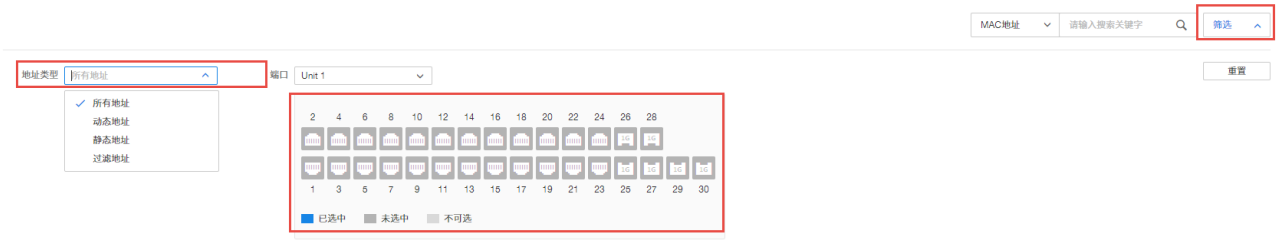
3.7.2 地址表显示

地址表包含了端口间报文转发的地址信息，是交换机实现二层报文快速转发的基础。可以在本页查看到交换机地址表的全部信息。

进入页面：网络管理 >> 二层交换 >> 地址表管理 >> 地址表显示，可查看到交换机地址表的全部信息，包括动态地址、手动配置的静态地址和过滤地址表。



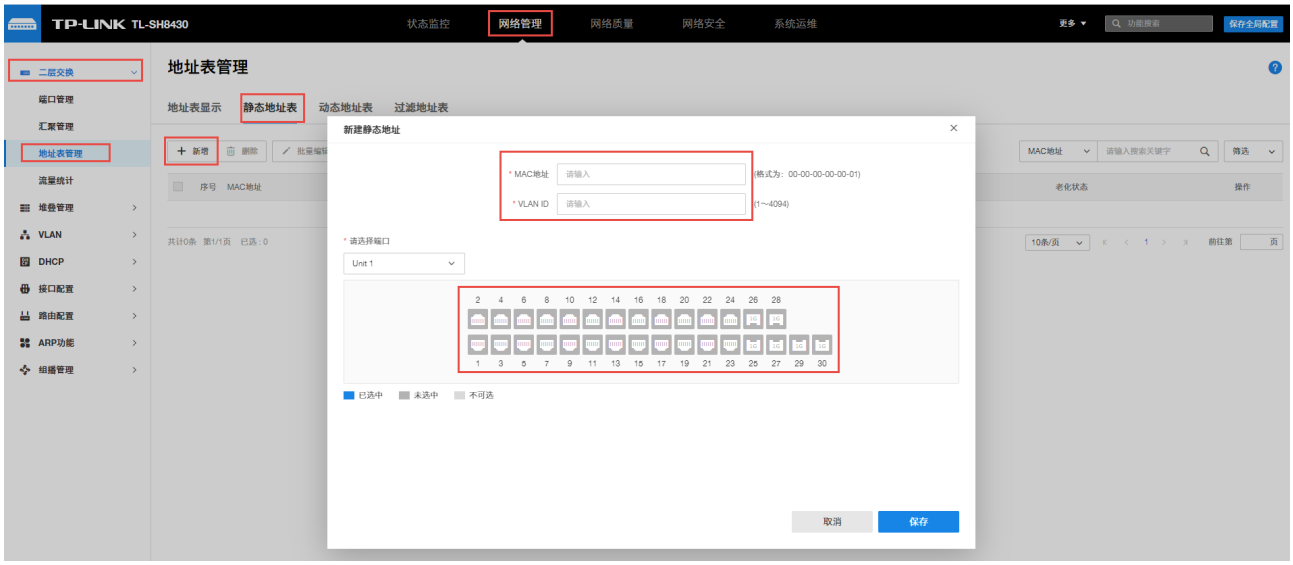
点击页面上<筛选>，可根据地址类型和具体端口来筛选地址表。



3.7.3 静态地址表

静态地址由用户手工添加和删除，不受最大老化时间的限制。对于网络拓扑相对固定的使用环境来说，使用静态地址绑定可以提高交换机的转发效率，减少网络中的广播流量。

进入页面：网络管理 >> 二层交换 >> 地址表管理 >> 静态地址表，点击<新增>，输入 MAC 地址、VLAN ID 选择对应端口，点击<保存>，新的静态地址表添加完成。

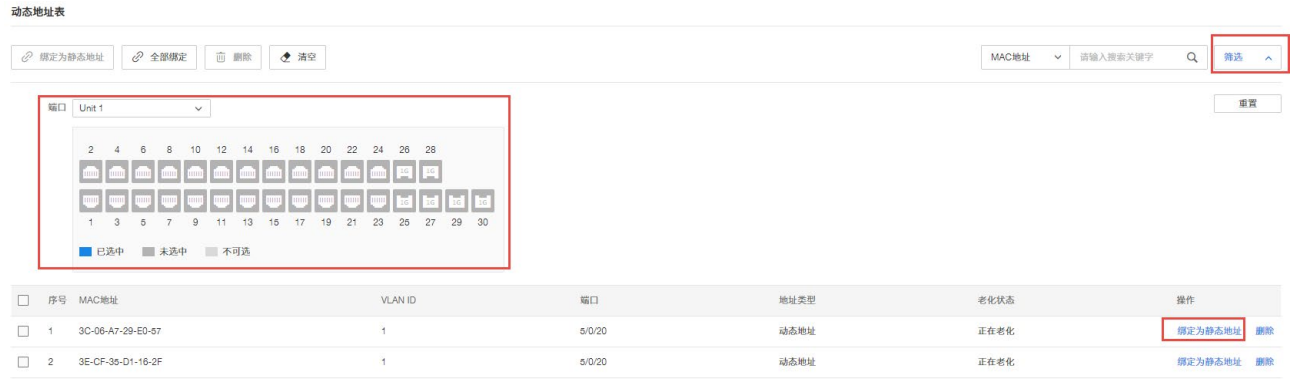


3.7.4 动态地址表

动态地址是交换机通过自动学习获取的 MAC 地址。交换机通过自动学习新的地址和自动老化掉不再使用的地址来不断更新其动态地址表。

进入页面：网络管理 >> 二层交换 >> 地址表管理 >> 动态地址表，配置交换机自动学习到的地址表老化时间，超过老化时间的地址表项将被自动删除，点击<保存>存储配置。也可查看交换机已学习到的动态地址表。

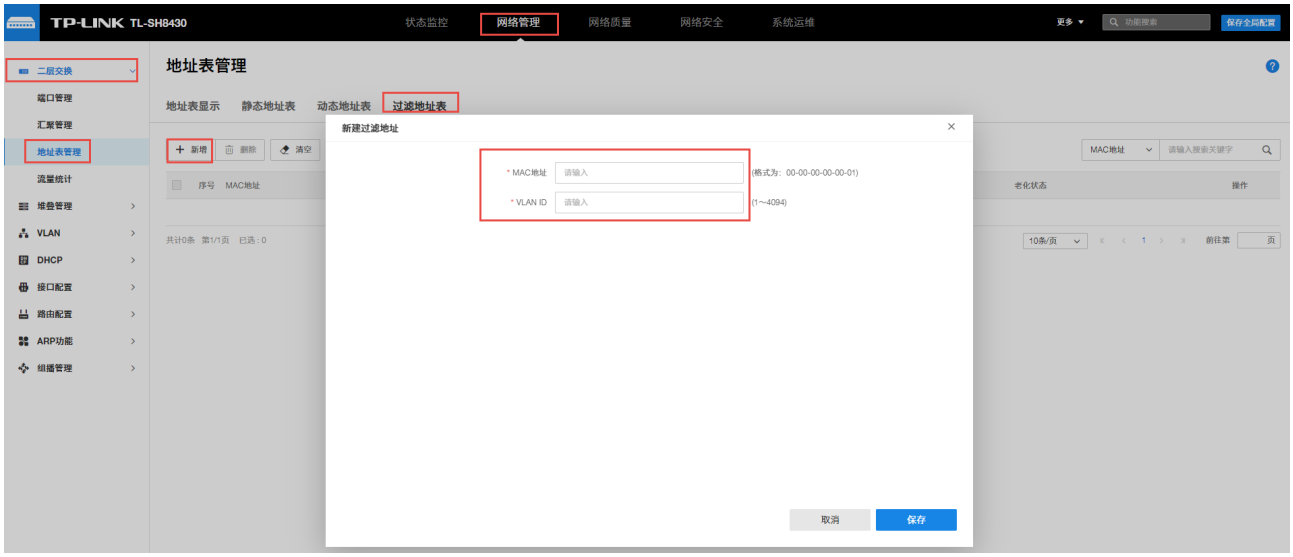
在动态地址表中，点击<绑定为静态地址表>，可将该动态地址转换为静态地址；点击<筛选>，可根据端口查看相关动态地址表。



3.7.5 过滤地址表

通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤，即此处是配置交换机的 MAC 地址转发黑名单，此列表中的 MAC 数据包到了交换机，交换机会选择丢弃。过滤地址不会被老化，只能手工进行配置和删除。

进入页面：网络管理 >> 二层交换 >> 地址表管理 >> 过滤地址表，点击<新增>，输入 MAC 地址和对应 VLAN ID，点击<保存>。交换机根据 MAC 地址匹配到的数据包将会直接丢弃。



3.8 流量统计

可查看交换机的端口的流量统计信息，同时也可以查看详细统计信息用来统计各端口传输数据包的详细信息，便于您定位网络问题。

进入页面：网络管理 >> 二层交换 >> 流量统计，或者进入页面：状态监控 >> 流量统计，可查看各端口接收/发送数据包或者接收/发送字节数的统计结果，点击<详情>，可查看更详细的统计结果。

回目录

第4章　堆叠功能

4.1　应用介绍

堆叠（Stack）是指将多台设备通过专用的堆叠口连接起来，堆叠系统由多台成员设备组成，主交换机（Master）设备负责堆叠系统的运行、管理和维护，其他成员设备在处理业务的同时可作为主交换机的备份。一旦主交换机设备故障，系统会迅速自动选举新的主交换机，以保证业务不中断，从而实现了设备的1：N 备份。进行必要的配置后，所有设备虚拟化成一台“ 分布式设备”。使用堆叠技术可以实现多台设备的协同工作和统一管理，对外表现就像一台设备一样。

4.2　堆叠配置实例

4.2.1 需求介绍

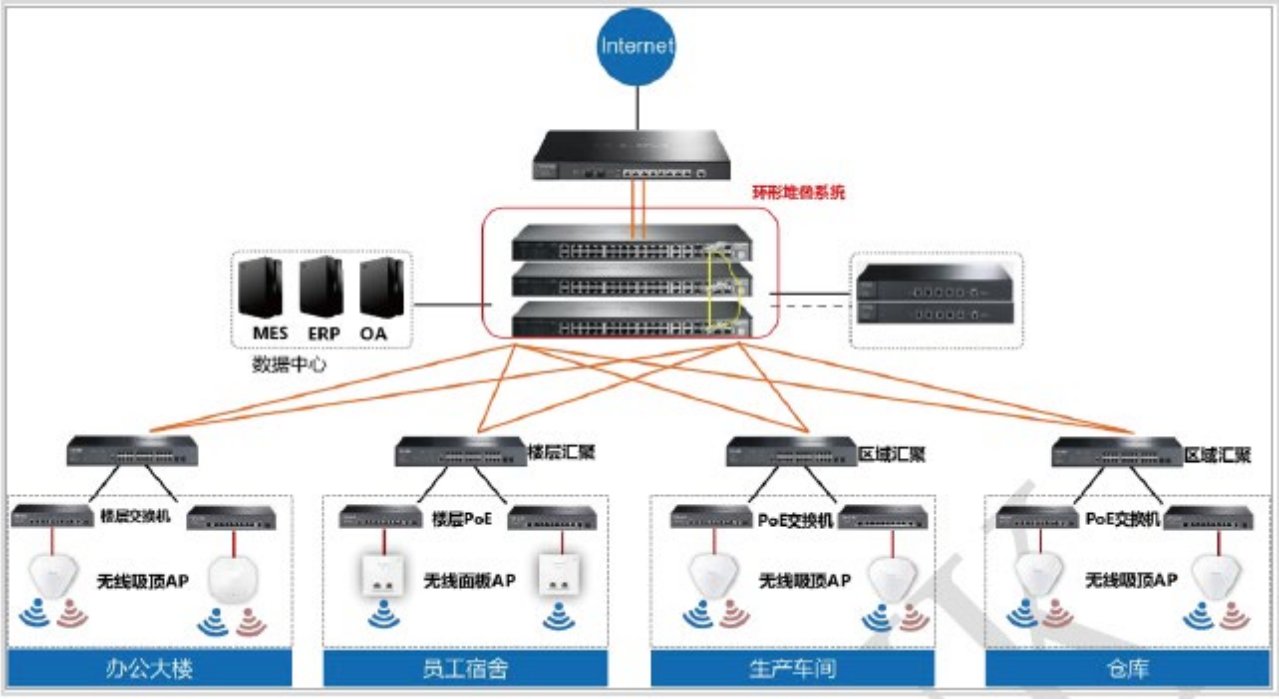
某大型网络为了保障网络运行的稳定性，并且增加转发带宽使用三台 TL-SH8430 交换机进行堆叠组网，设备堆叠后要求达到以下网络需求：

1、强大的网络扩展能力，堆叠增加交换机的背板带宽，增加端口数量；

2、堆叠后设备统一成一台设备，统一配置；

3、增加设备的冗余备份能力，保障网络的稳定性。

组网如下：



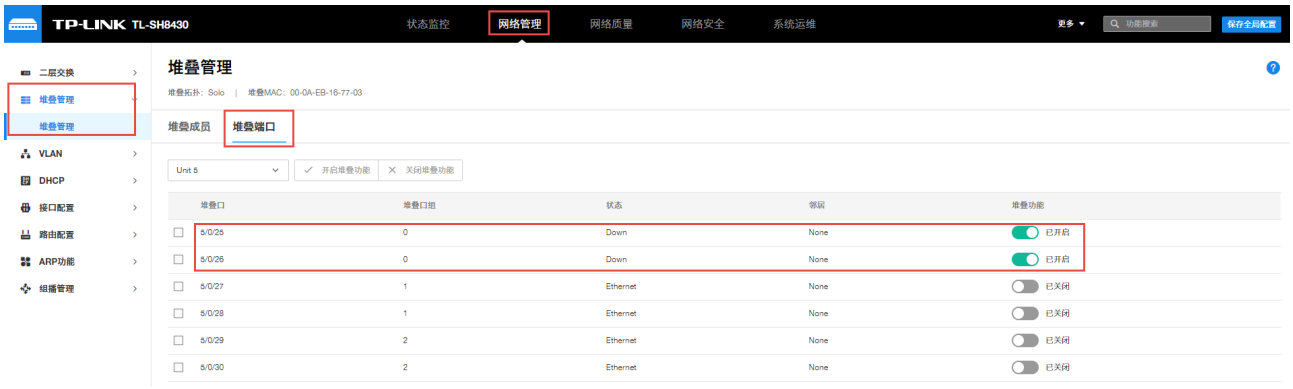
4.2.2 配置方法

➢ **配置前准备**

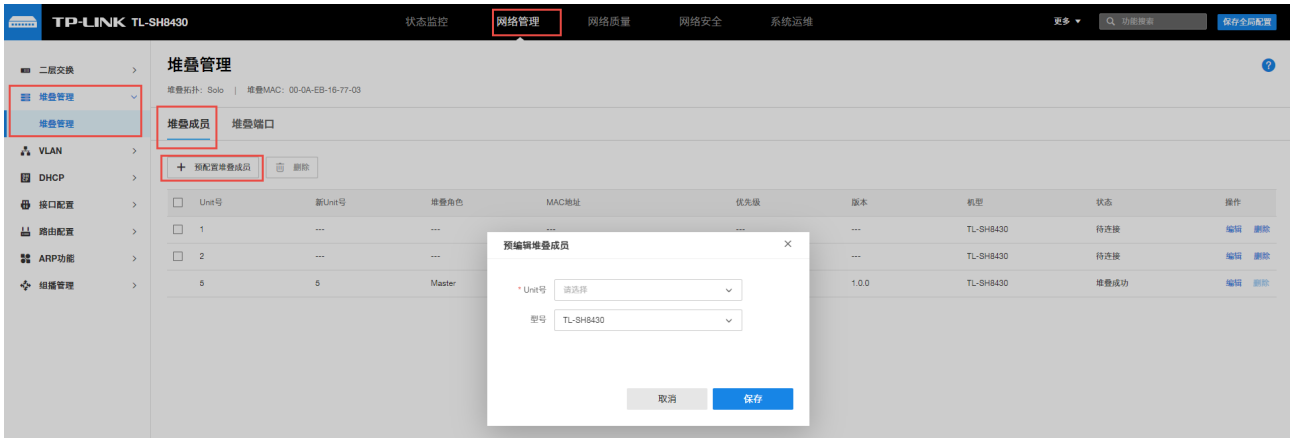
准备三台出厂状态下的 TL-SH8430 交换机，三根 1 米万兆 SFP+电缆 TL-TC532-1 用于连接交换机的堆叠口。

➢ **配置步骤**

1. 分别登录 3 台设备的 web 界面，进入页面“网络管理 >> 堆叠管理 >> 堆叠端口”或“状态监控 >> 堆叠状态列表 >> 堆叠端口”界面设置堆叠口，将选中的堆叠口状态设置成启用，本次选择将 3 台交换机的 25、26 口设置成堆叠口。



2. 分别登录 3 台设备的 web 界面，进入页面“网络管理 >> 堆叠管理 >> 堆叠成员”或“状态监控 >> 堆叠状态列表 >> 堆叠成员”，点击<预配置堆叠成员>，分别将三台交换机的堆叠编号为 Unit4、Unit5、Unit6。



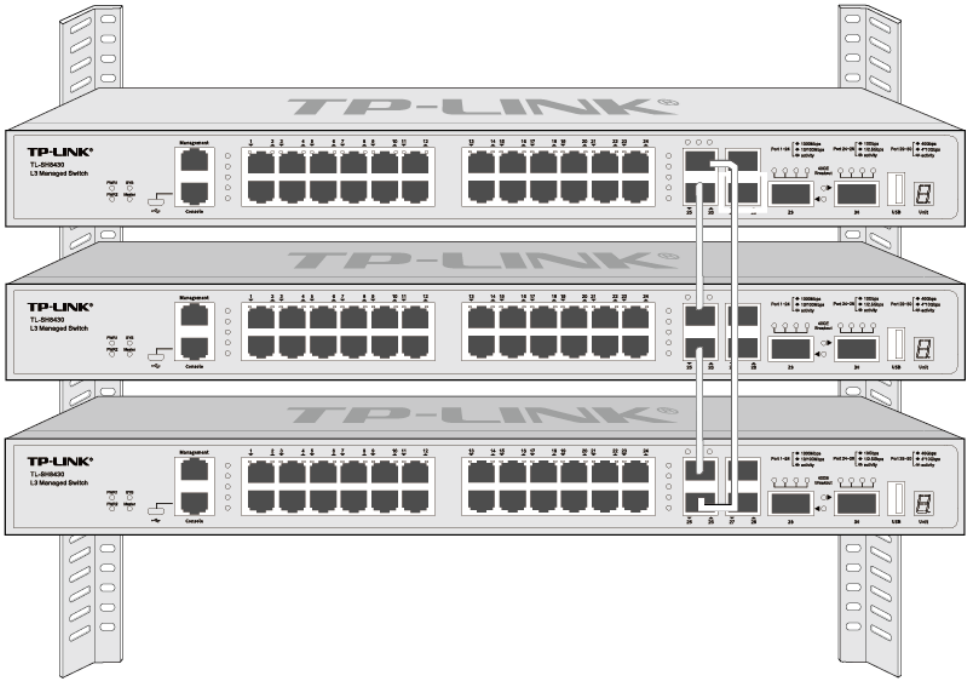
说明：

- 如需在加入堆叠之前提前配置交换机，可点击<预配置堆叠成员>令配置交换机的 unit 号和机型。可以手动创建预配置成员信息，或当交换机加入堆叠时，自动创建/更新其成员信息。当堆叠成员离开时，预配置信息会保留在堆叠中。
- 如无需在加入堆叠之前提前配置交换机，可省略步骤 2，交换机可自行分配堆叠角色和 Unit 号。

- **网络连线**

TL-SH8430 支持将 25 和 26 号 SFP+端口、27 和 28 号 SFP+端口、29 和 30 号 QSFP+端口分别配置为一组堆叠端口。TL-SH8430 可利用 SFP+或 QSFP+端口将最多 8 台设备互联形成一个堆叠系统。建立堆叠系统时，建议连接成环形拓扑结构以实现链路的冗余备份、提高网络可靠性。

此处连接 25 和 26 SFP+端口形成环状堆叠结构为例进行说明。



物理连接后，给设备上电，堆叠开始形成，堆叠后只有作为主交换机的“Master”指示灯会亮。

- **堆叠信息展示**

堆叠系统形成后，用户可以通过任意成员设备的端口登录堆叠系统。

进入页面“状态监控 >> 系统监控 >> 堆叠设备”，查看堆叠的各成员信息。

堆叠设备

成员编号	1	2	3	4	5 Master	6	7	8
成员状态	---	---	---	---	堆叠完成	---	---	---
设备型号	TL-SH8430	TL-SH8430	---	---	TL-SH8430	---	---	---
硬件版本	1.0	1.0	---	---	1.0	---	---	---
系统描述	---	---	---	---	24GE+4SFP++2QSFP+ L3 Managed Switch	---	---	---
软件版本	---	---	---	---	1.0.0 Build 20221027 Rel.48714(s)	---	---	---
冗余电源状态	---	---	---	---	未供电或已损坏	---	---	---
风扇工作状态	---	---	---	---	异常	---	---	---
风扇工作档位	---	---	---	---	0	---	---	---

注意：

- 堆叠的设备型号和软件版本要求一样；堆叠后全局配置会沿用 Master 设备的配置。
- 如果设备不是在出厂状态下配置，堆叠形成后哪个设备是 Master，就会沿用这个设备的所有配置。
- 堆叠配置是无法通过复位交换机消除的，需要手动关闭堆叠口和其它堆叠功能。
- 设备对应端口启用了堆叠功能后无法再用作业务口配置。

回目录

第5章　VLAN

VLAN（Virtual Local Area Network，虚拟局域网）是一种将局域网设备从逻辑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，这种技术通过在局域网数据帧上定义扩展字段，来对物理网络进行逻辑上的分割，从而限定局域网数据帧的转发范围，缩小广播域。VLAN 技术主要应用于交换机、路由器和交换机等网络设备中。

5.1　配置 802.1Q VLAN

5.1.1 802.1Q VLAN 介绍

802.1Q VLAN 可以实现局域网内二层网络的隔离以及跨交换机的 VLAN 互访，在中大型网络中为了隔离广播域，设置 802.1Q VLAN 是一个非常有效且方便的办法，这样既能保证用户带宽，也能降低设备因为处理局域网广播所带来的性能损耗。

IEEE 802.1Q 协议标准化了 VLAN 实现方案，对数据包统一规定增加 VLAN Tag，交换机利用 VLAN Tag 中的 VLAN ID 来识别报文所属的 VLAN。

2 系列云管理交换机可设置端口是否带有 tag：

Untagged 端口：在发送数据包之前，交换机会丢弃 tag 头；

Tagged 端口：在发送数据包之前，交换机会添加 tag 头，常用在网络设备的级联之间。

- **PVID 与 VLAN 数据包处理关系**

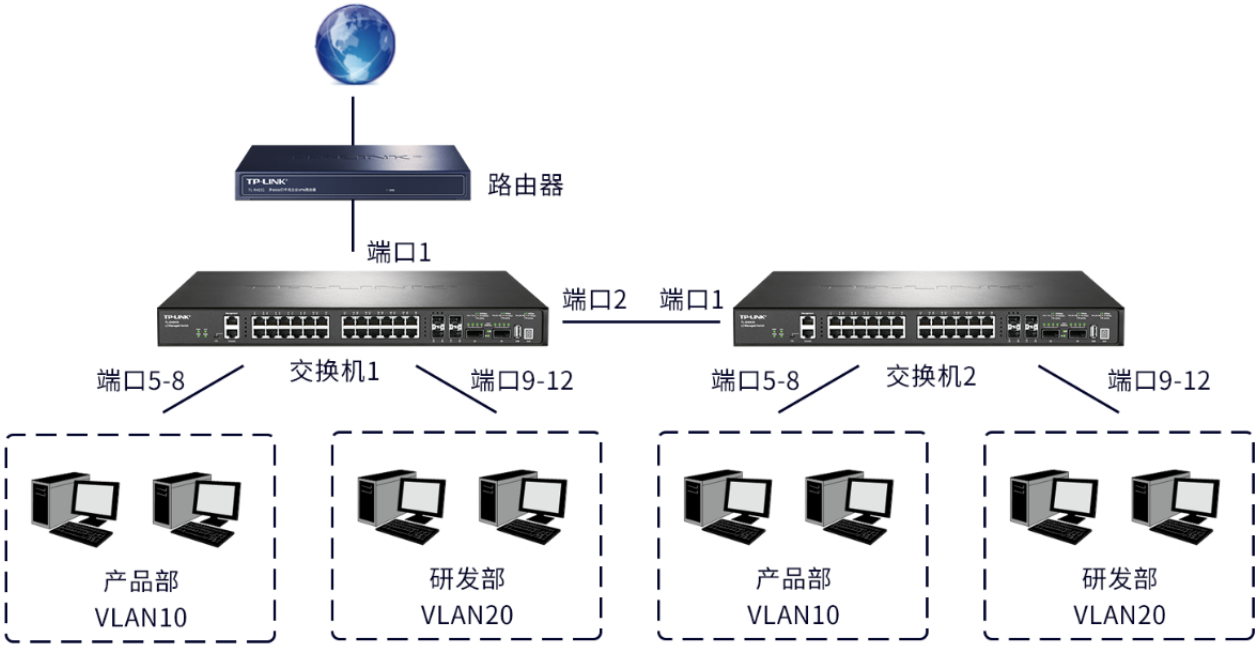
PVID（Port Vlan ID），端口的缺省 VID，当在局域网中划分 VLAN 时，PVID 是每个端口的一个重要参数，表示端口默认所属的 VLAN。当交换机的端口接收到的报文不带 VLAN Tag 时，交换机会根据接收端口的 PVID 值为该报文插入 VLAN Tag，并进行转发。

端口的链路类型本质上是交换机对出入端口的 VLAN Tag 的处理方式。

5.1.2 802.1Q VLAN 配置实例

组网介绍：

同一个公司的同一个部门有多个不同的办公地点，各办公点有各自的交换机，级联形成同一个局域网。要求不同部门之间相互隔离，不能互访；不同交换机下的相同部门的成员能进行互访。网络拓扑如下：



配置步骤：

- **首先设置交换机 1：**

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1 和端口 2，点击<编辑>，将端口类型更改为 TRUNK，PVID 为 1。设置完成，点击<保存>。

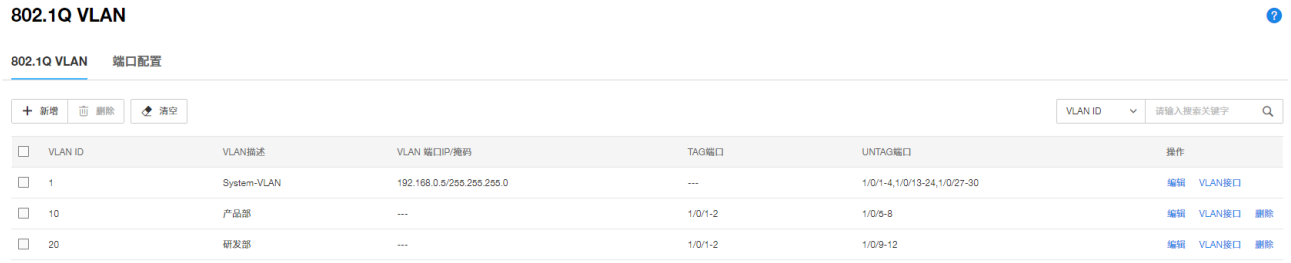
注意：

所属 VLAN 的编号需要用英文字符“,”隔开。

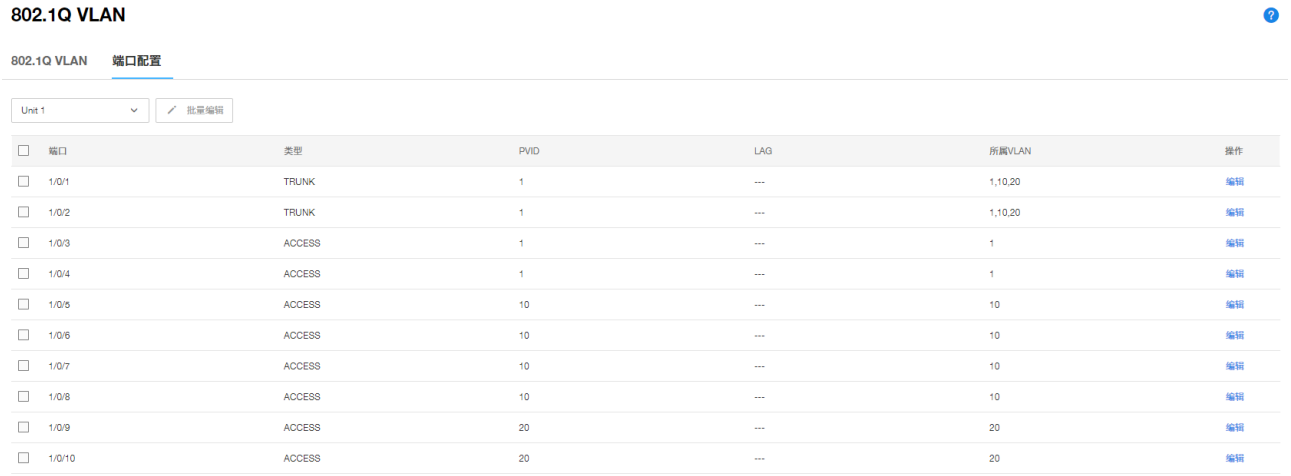
2. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，添加 VLAN 10，备注“产品部 “，该 VLAN 包含 tagged 端口 1 和端口 2，untagged 端口 5~8。设置完成后，点击<保存>。

3. 再次点击<新增>，添加 VLAN 20，备注“研发部”，该 VLAN 包含 tagged 端口 1 和端口 2，untagged 端口 9~12。设置完成后，点击<保存>。

配置完成的 VLAN 如下：



配置完成 VLAN10 和 VLAN20 后，进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，可查看到端口 5-8 的 PVID 已自动更改为 10，端口 9-12 的 PVID 已自动更改为 20。



- **其次设置交换机 2：**

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1，点击<编辑>，将端口类型更改为 TRUNK，PVID 为 1。设置完成，点击<保存>。

注意：

所属 VLAN 的编号需要用英文字符“,”隔开。

2. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，添加 VLAN 10，备注“产品部“，该 VLAN 包含 tagged 端口 1，untagged 端口 5~8。设置完成后，点击<保存>。

3. 再次点击<新增>，添加 VLAN 20，备注“研发部”，该 VLAN 包含 tagged 端口 1，untagged 端口 9~12。设置完成后，点击<保存>。

5.2 配置 MAC VLAN

5.2.1 应用介绍

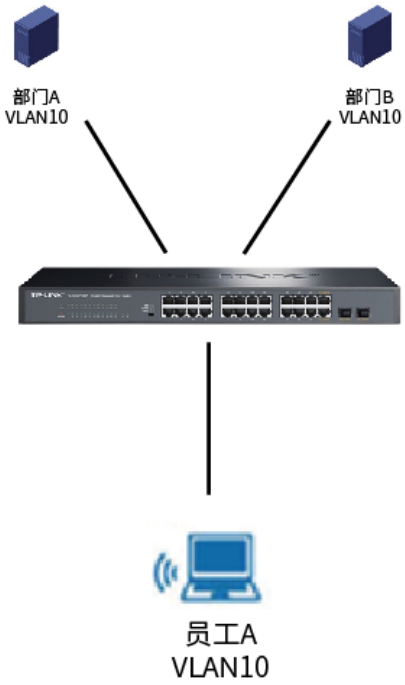
MAC VLAN 根据每个主机的 MAC 地址来划分 VLAN,即对每个主机的 MAC 地址均划分到 VLAN 中。MAC VLAN 的优点在于，将 MAC 地址与 VLAN 绑定后，该 MAC 地址对应的设备可以随意切换端口，只要连接到相应 VLAN 的成员端口即可，而不必改变 VLAN 成员的配置。

MAC VLAN 能够实现灵活的接入控制，同一终端通过不同端口接入设备时，设备会给终端分配相同的 VLAN；而不同终端通过同一端口接入设备时，设备可以给不同终端分配不同的 VLAN。

5.2.2 MAC VLAN 配置实例

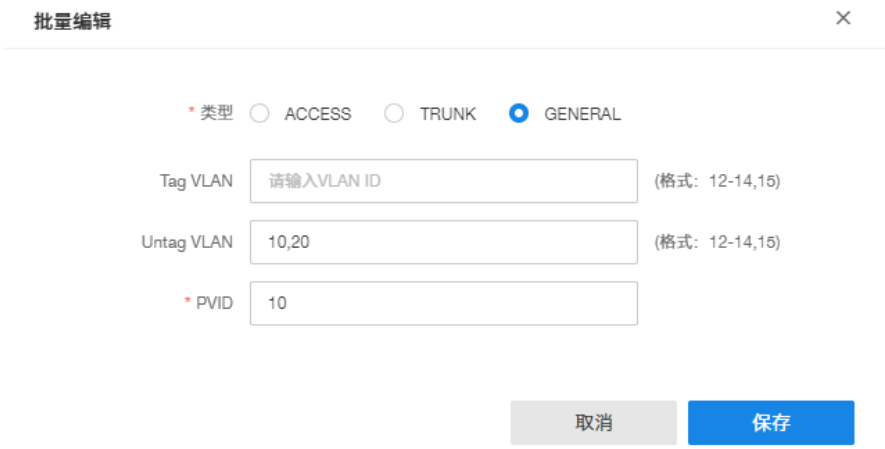
需求介绍：

某公司有两个部门，为了通信安全设置了 VLAN 隔离。由于人员流动较大，公司在会议室提供了临时的办公场所，即员工可以通过临时办公场所接入公司网络，但要求接入后只能划分到自己部门所在的 VLAN，拓扑如下：

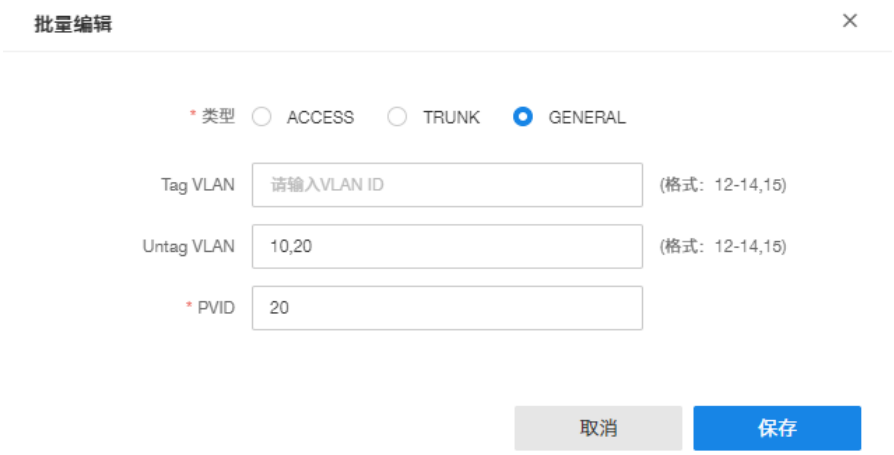


配置步骤：

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，同时勾选端口 1-4，点击<批量编辑>，将端口类型更改为 GENERAL，UNTAG VLAN 为 VLAN 10，PVID 为 10。设置完成，点击<保存>。



同时再勾选 5-8，点击<批量编辑>，将端口类型更改为 GENERAL，UNTAG VLAN 为 VLAN 20，PVID 为 20。



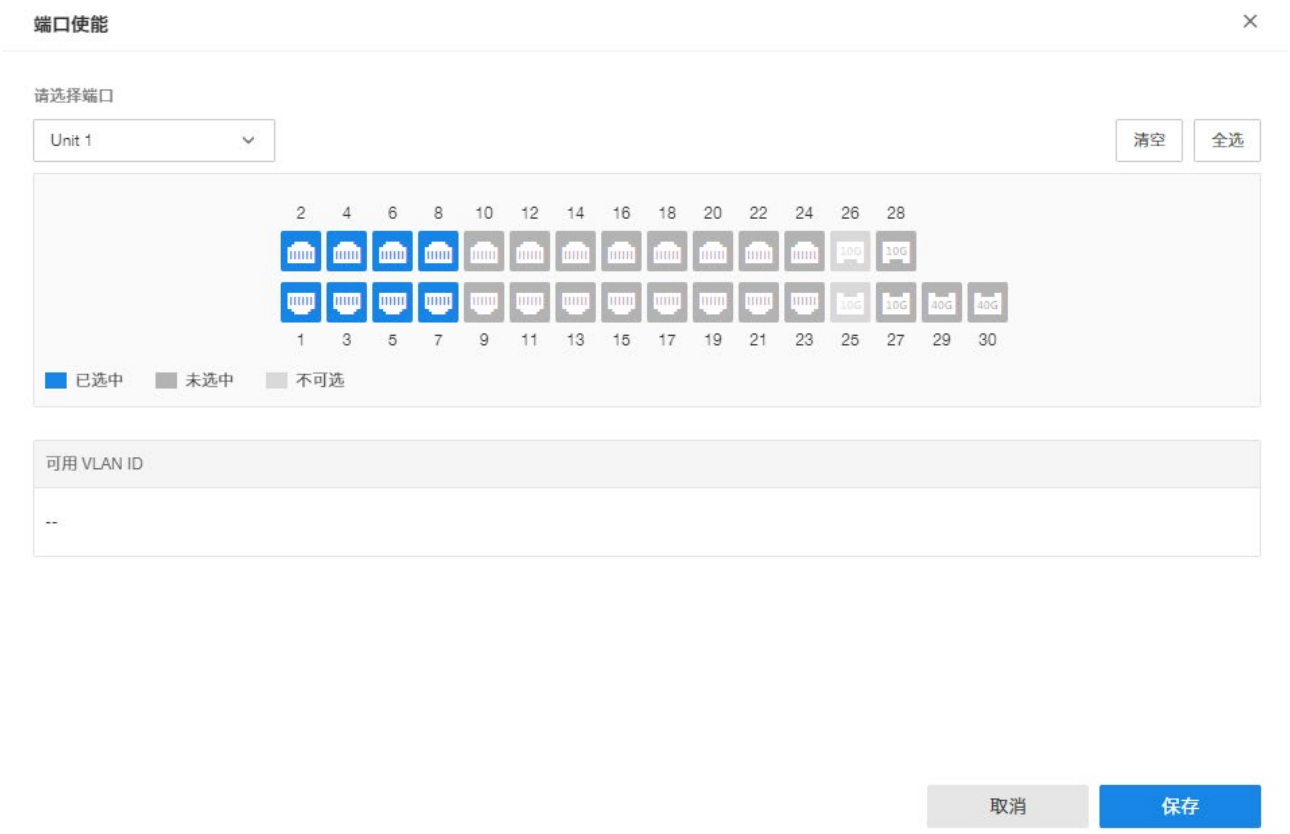
如此配置完成后，端口 1-8 均属于 VLAN10 和 VLAN20。

2. 进入页面：网络管理 >> 接口配置，点击<新增>，给 VLAN10 和 VALN 20 绑定 IP。

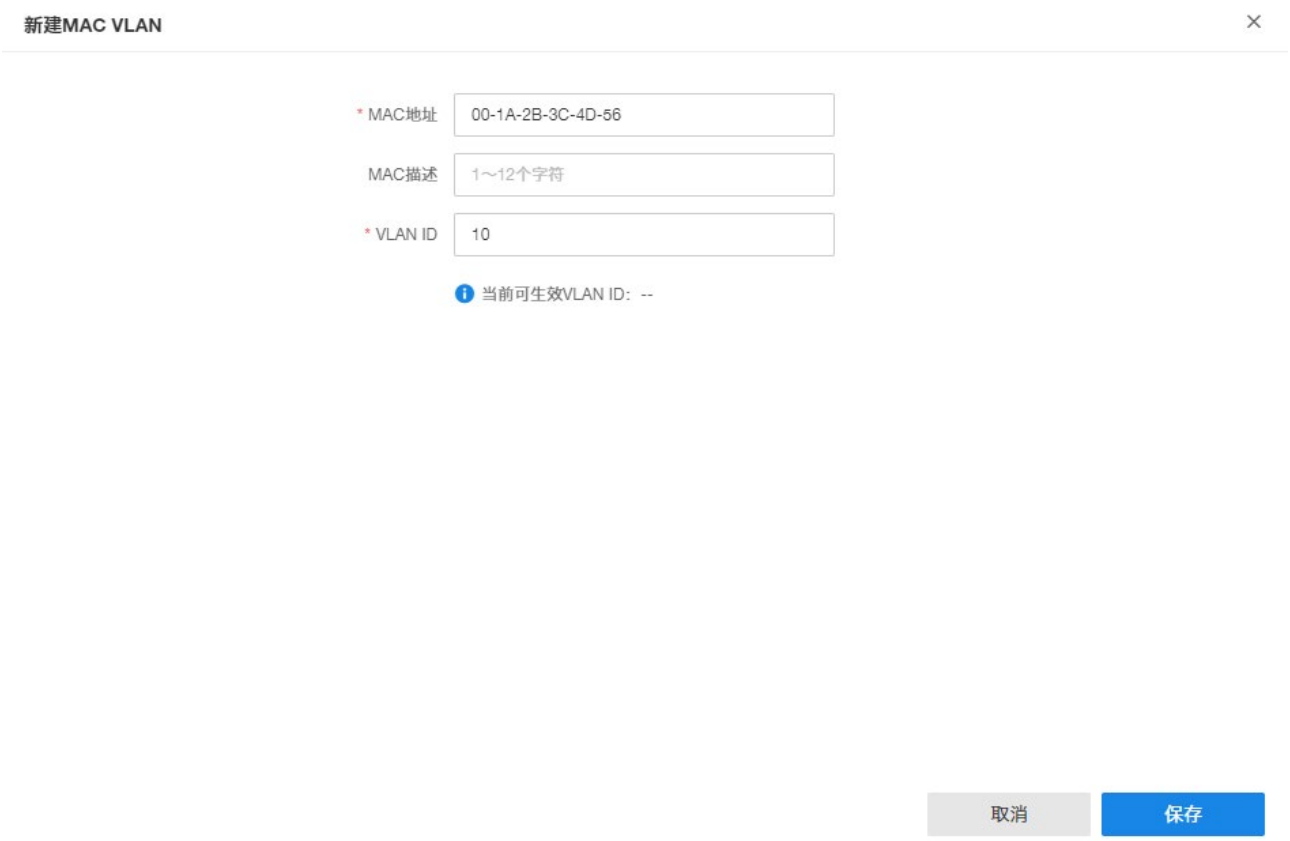
3. 进入页面：网络管理 >> DHCP >> DHCP 服务器，开启 DHCP 服务器。

4. 进入页面：网络管理 >> DHCP >> DHCP 服务器 >> 地址池设置，点击<新增>，添加地址池。

5. 进入页面：网络管理 >> VLAN >> MAC VLAN，点击<端口使能>，选择端口 1-8，点击保存。



6. 进入页面：网络管理 >>VLAN>>MAC VLAN，点击<新增>，输入该员工的 MAC 地址和所属 VLAN ID，点击<保存>。



以上，该终端接入任意的 1-8 口都属于 VLAN 10。

说明：

- 输入该 MAC VLAN 对应的 VLAN ID 时，此 VLAN 必须是输入端口所在的 802.1Q VLAN。

5.3 配置协议 VLAN

5.3.1 应用介绍

协议 VLAN 是按照网络层协议来划分 VLAN，可分为 IP、IPX、DECnet、AppleTalk、Banyan 等 VLAN 网络。每个协议对应一个 VLAN ID，交换机给端口收到的无 tag 帧和优先级 tag 帧分配此 VLAN ID。这种按网络层协议来组成的 VLAN，可使广播域跨越多个交换机，同时用户在网络内部可以自由移动且无须改变其 VLAN 成员身份。对于希望针对具体应用和服务来管理用户的网络管理员，可通过划分协议 VLAN 来进行管理。

由于协议 VLAN 本身是基于 802.1Q VLAN，在创建协议 VLAN 的时候，需要提前建立对应端口所属的 802.1Q VLAN，在使能端口时才能选中对应的 VLAN ID。

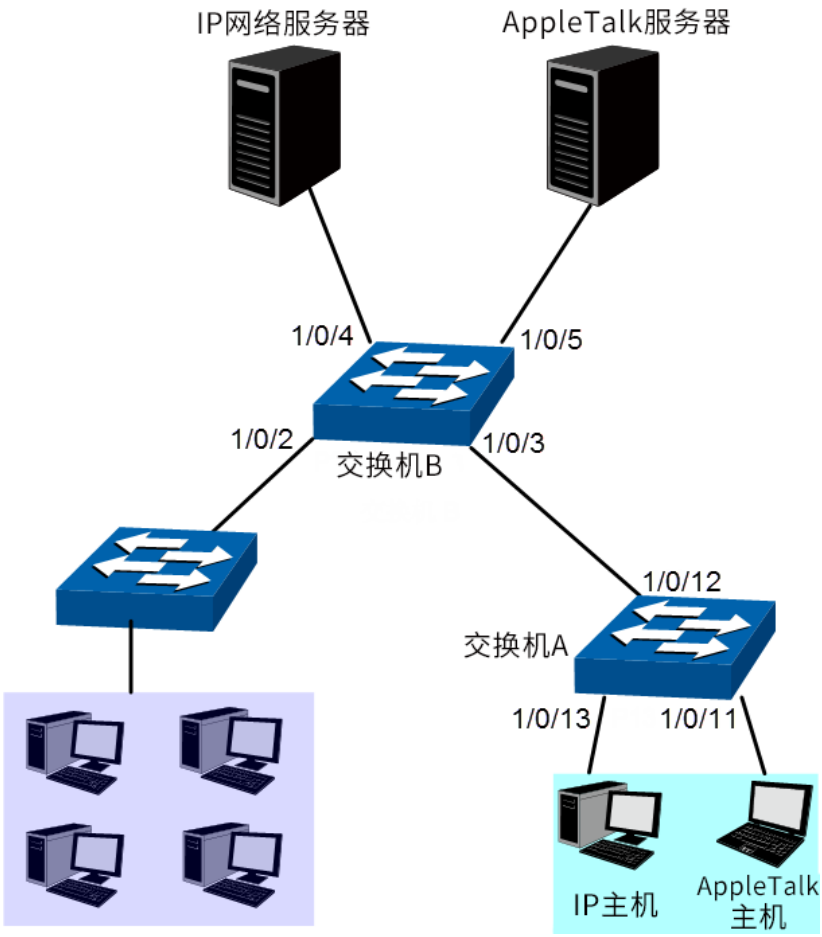
5.3.2 协议 VLAN 配置实例

需求介绍：

平面部门通过内部交换机 A 的端口 1/0/12 连入公司局域网；

平面部门中分别有 IP 主机和 AppleTalk 主机；

IP 主机需要 IP 网络服务器提供服务，属于 VLAN10；AppleTalk 主机需要 AppleTalk 服务器提供服务，属于 VLAN20；交换机 B 分别连接了 IP 网络服务器和 AppleTalk 网络服务器。网络拓扑如下：

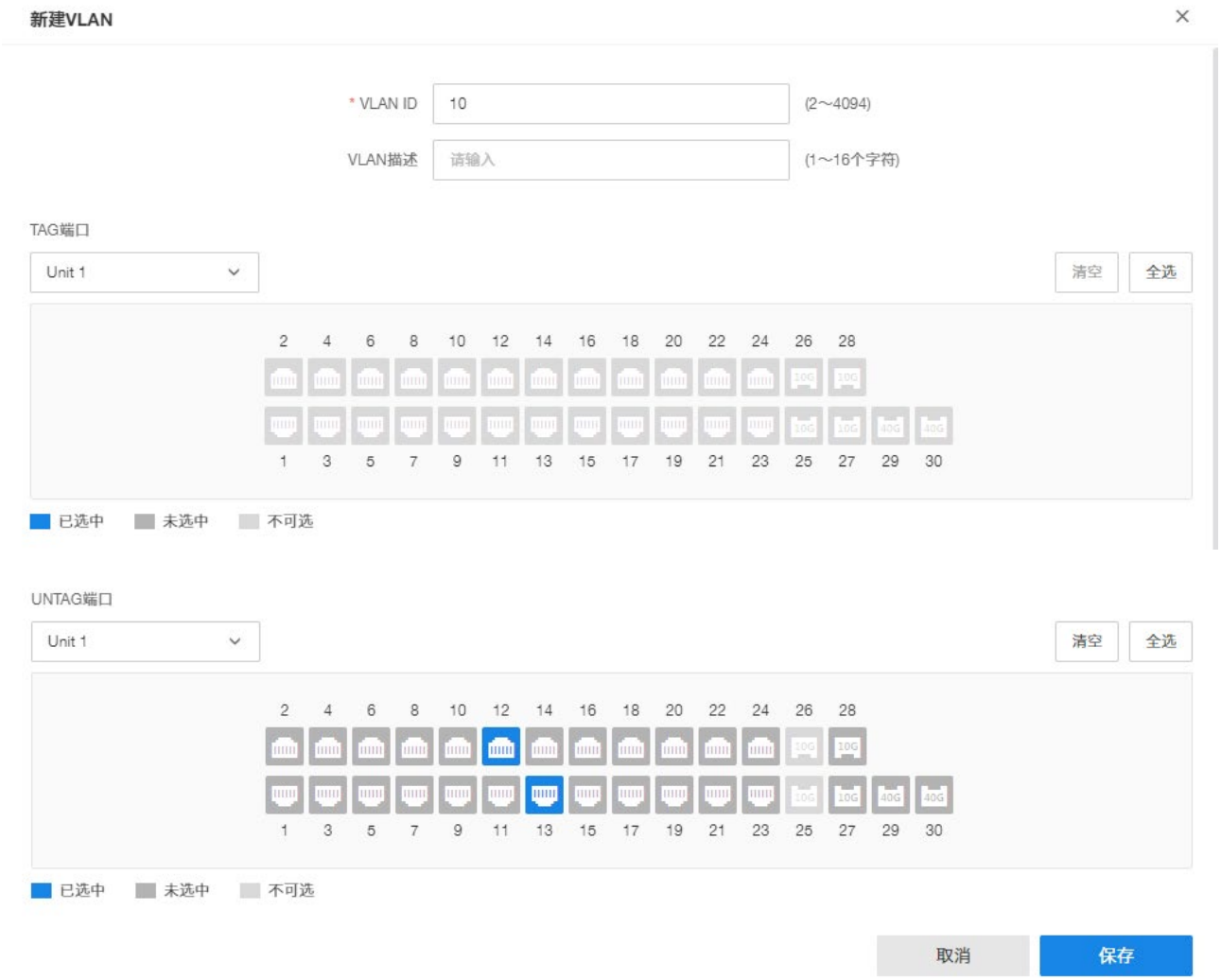


配置步骤：

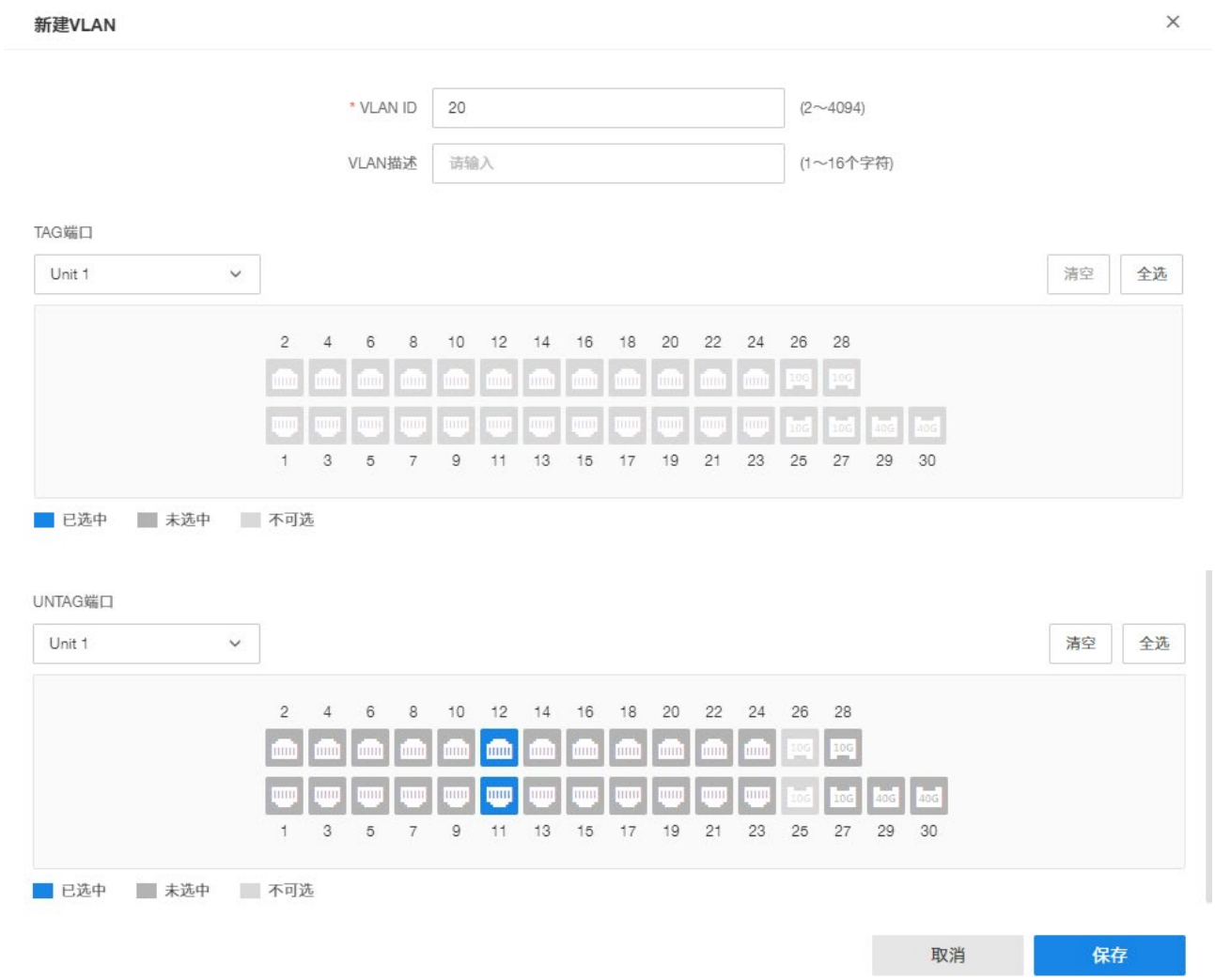
- **首先配置交换机 A**

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，对端口 12 点击<编辑>，模式选择为 GENERAL，点击<保存>。端口 11 和端口 13 默认为 ACCESS 端口，无需更改。

2. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，配置 VLAN 10，输入 VLAN 为 10，UNTAG 端口选中端口 12 和端口 13，点击<保存>。



3. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，配置 VLAN 20，输入 VLAN 为 20，UNTAG 端口选中端口 12 和端口 11，点击<保存>。

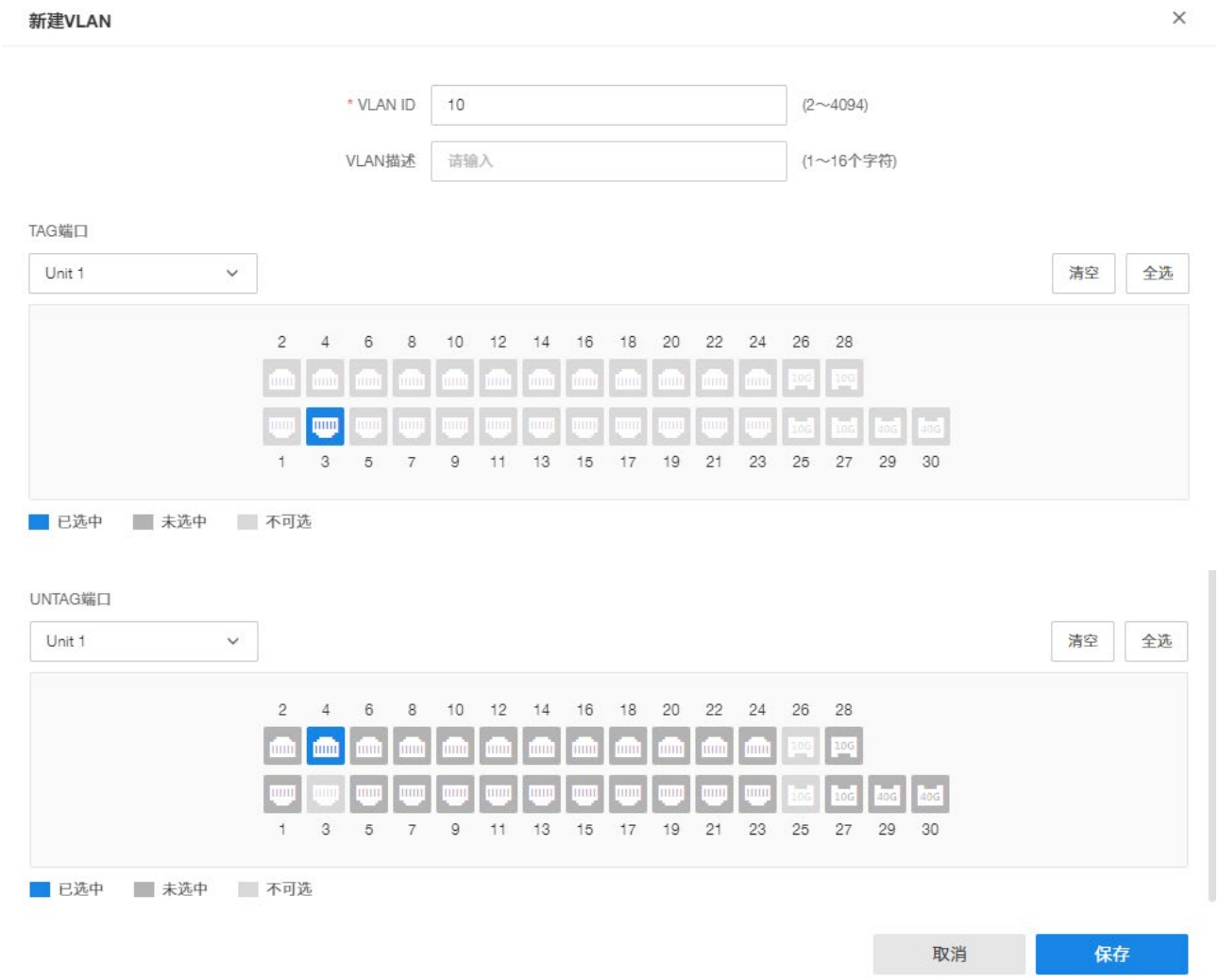


此时配置完成后，进入页面网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，可看到此时端口 12 处于 VLAN10 和 VLAN20，端口 11 属于 VLAN 20，PVID 为 20，端口 13 属于 VLAN 10，PVID 为 10。

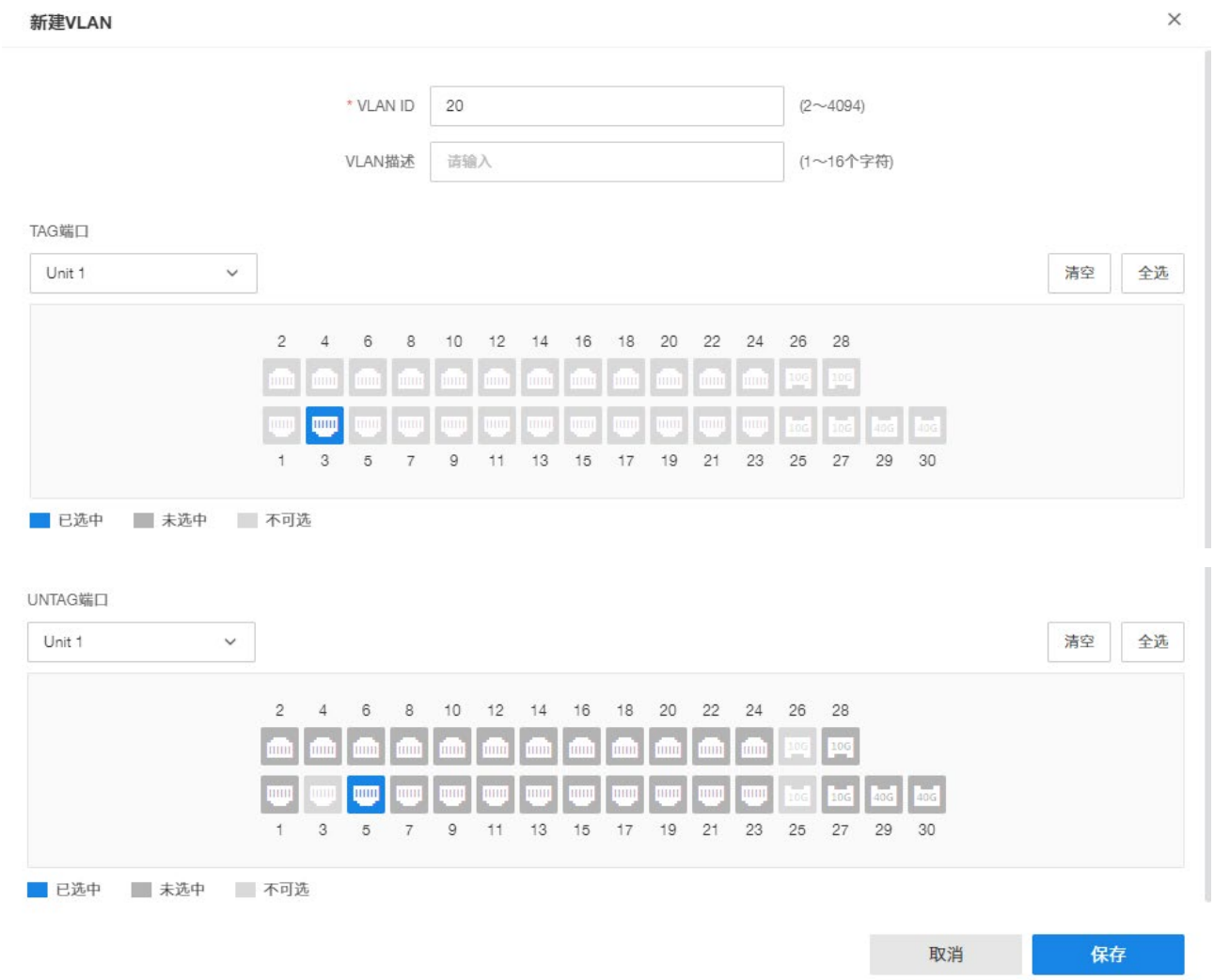
- **其次配置交换机 B**

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，对端口 3 点击<编辑>，模式选择为 GENERAL，点击<保存>。端口 4 和端口 5 默认为 ACCESS 端口，无需更改。

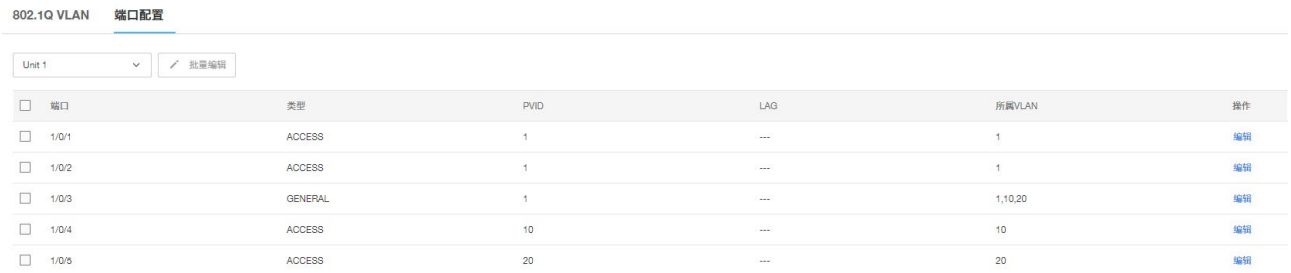
2. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，配置 VLAN 10，输入 VLAN 为 10，TAG 端口选中端口 3，UNTAG 端口选中端口 4，点击<保存>。



3. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，配置 VLAN 20，输入 VLAN 为 20，TAG 端口选中端口 3，UNTAG 端口选中端口 5，点击<保存>。



此时配置完成后，进入页面网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，可看到此时端口 3 处于 VLAN10 和 VLAN20，端口 5 属于 VLAN 20，PVID 为 20，端口 4 属于 VLAN 10，PVID 为 10。



4. 交换机默认配置有 IP 协议 VLAN 模板，进入页面：网络管理 >> VLAN >> 协议 VLAN，在 IP 协议中点击<编辑>，选中端口 3，关联 VLAN 10。设置完成，点击<保存>。

5. 交换机默认配置有 AppleTalk 协议 VLAN 模板，进入页面：网络管理 >>VLAN>> 协议 VLAN，在 AT 协议中点击<编辑>，选中端口 3，关联 VLAN 20。设置完成，点击<保存>。

说明：

- 若需要创建交换机默认含有的协议 VLAN 模板，进入页面：网络管理 >>VLAN>> 协议 VLAN，点击<新增>，请根据实际情况配置协议模板。

5.4 配置 VLAN VPN

5.4.1 应用介绍

VPN（Virtual Private Network，虚拟私有网络）是随着Internet的广泛应用而迅速发展起来的一种新技术，用来实现在骨干网络上构建私人专用网络。通过在客户端或运营商接入端对指定报文进行处理，使骨干网络中的设备可以为其建立专用的传输隧道，保证数据的安全。

VLAN-VPN(Virtual Private Network)是一种简单、灵活的二层VPN技术，它通过在运营商接入端为用户的私网报文封装外层VLAN Tag，使报文携带两层VLAN Tag穿越运营商网络（骨干网）。在骨干网中，报文只根据外层VLAN Tag进行传输，用户的私网VLAN Tag则当作报文中的数据部分来进行传输。

VLAN-VPN主要可以解决如下几个问题：

（1） 为小型城域网或企业网提供一种较为简单的二层VPN解决方案。

（2） 缓解日益紧缺的公网VLAN ID资源问题。

（3） 用户可以规划自己的私网VLAN ID，不会导致和骨干网VLAN ID冲突。

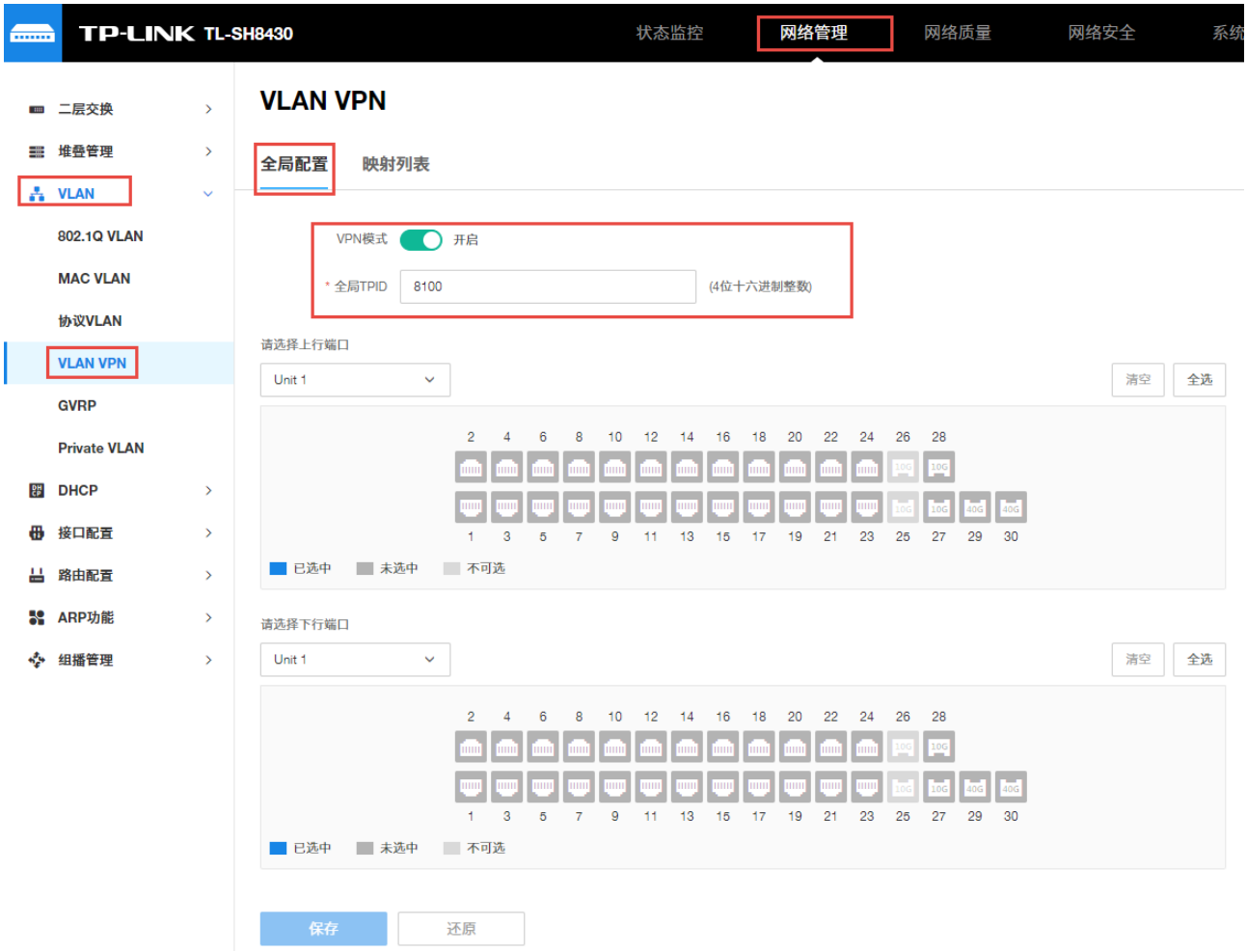
（4） 当运营商升级网络时，用户网络不必更改原有配置，使用户网络具有了较强的独立性。

在本交换机中，将用户的原始VLAN称作C VLAN；而骨干网络中，运营商通常使用公网VLAN为不同的C VLAN提供服务，本交换机中将公网VLAN称为SP VLAN。在本交换机上，需要在入口端配置端口PVID为运营商的公网VLAN，以及将连接公网的端口设置为上联端口，使报文顺利穿越骨干网络到达目的地。

启用VLAN-VPN功能后，不管端口收到tagged或者untagged报文，交换机都会根据PVID给报文封装外层VLAN Tag，然后通过上联端口在骨干网络中传输双Tag报文。

5.4.2 VLAN VPN 配置步骤

1. 进入页面：网络管理 >> VLAN >> VLAN VPN >> 全局配置，开启 VPN 模式，根据对端设备属性设置全局 TPID 值。选择连接到运营商网络的上行端口，选择与下行网络设备相连的下行端口。



2. 进入页面：网络管理 >> VLAN >> VLAN VPN >> 映射列表，开启映射功能，点击<新增>，配置局域网原始 VLAN（C VLAN）和公网 VLAN（SP VLAN）的映射关系。

5.5 GVRP

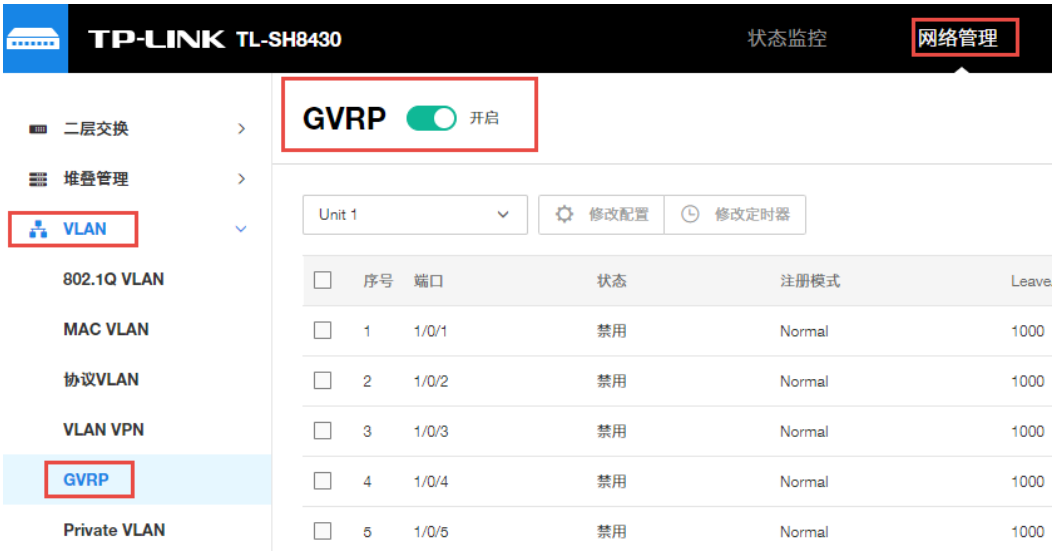
5.5.1 应用介绍

GVRP（GARP VLAN Registration Protocol，GARP VLAN注册协议）是GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用。它通过在端口动态注册和注销VLAN信息来达到创建或删除VLAN的目的，并传播VLAN信息到其它交换机中，减少配置VLAN时烦琐的手动操作。

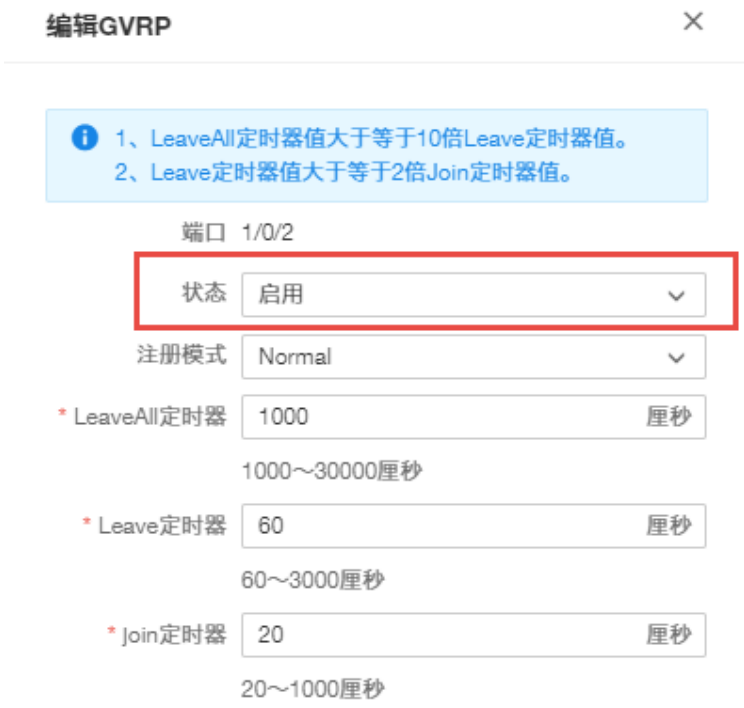
GARP（Generic Attribute Registration Protocol，通用属性注册协议）提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息。GVRP 是 GARP 的一种应用。它基于 GARP 的工作机制，维护设备中的 VLAN 动态注册信息，并传播 VLAN 信息到其它设备中。

5.5.2 GVRP 配置步骤

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，将需开启 GVRP 的端口设置为 TRUNK。
2. 进入页面：网络管理 >> VLAN >> GVRP，开启 GVRP 功能。



3. 进入页面：网络管理 >> VLAN >> GVRP，选择相应端口，点击<编辑>，状态选择为启用，据实际应用情况设置端口的其他参数。



5.6 Private VPN

5.6.1 应用介绍

Private VLAN功能采用了分层结构，将多个Secondary VLAN与一个Primary VLAN组成VLAN对，下层用户通过Secondary VLAN相互之间进行二层报文隔离，上层设备仅需识别Primary VLAN从而节约了VLAN资源，解决了上层设备VLAN资源短缺以及传统VLAN中的广播问题。

Private VLAN 功能基于 802.1Q VLAN 建立 Primary VLAN 和 Secondary VLAN 的包含关系，通过这种包含关系，上联设备只需识别 Primary VLAN 信息，下联设备只需识别 Secondary VLAN 信息。

Primary VLAN：上行设备感知的用户 VLAN，不是用户真正所属的 VLAN，一个 Primary VLAN 可以和多个 Secondary VLAN 建立包含关系，用于转发上层设备和 Secondary VLAN 之间的通信数据。

Secondary VLAN：用户真正属于的 VLAN，将用户划分到不同的 Secondary VLAN 中，Secondary VLAN 之间相互隔离。

Secondary VLAN 有两种类型，Community VLAN 和 Isolated VLAN。Community VLAN 中的成员相互之间可以直接通信，Isolated VLAN 中的成员相互隔离。

5.6.2 Private VPN 配置实例

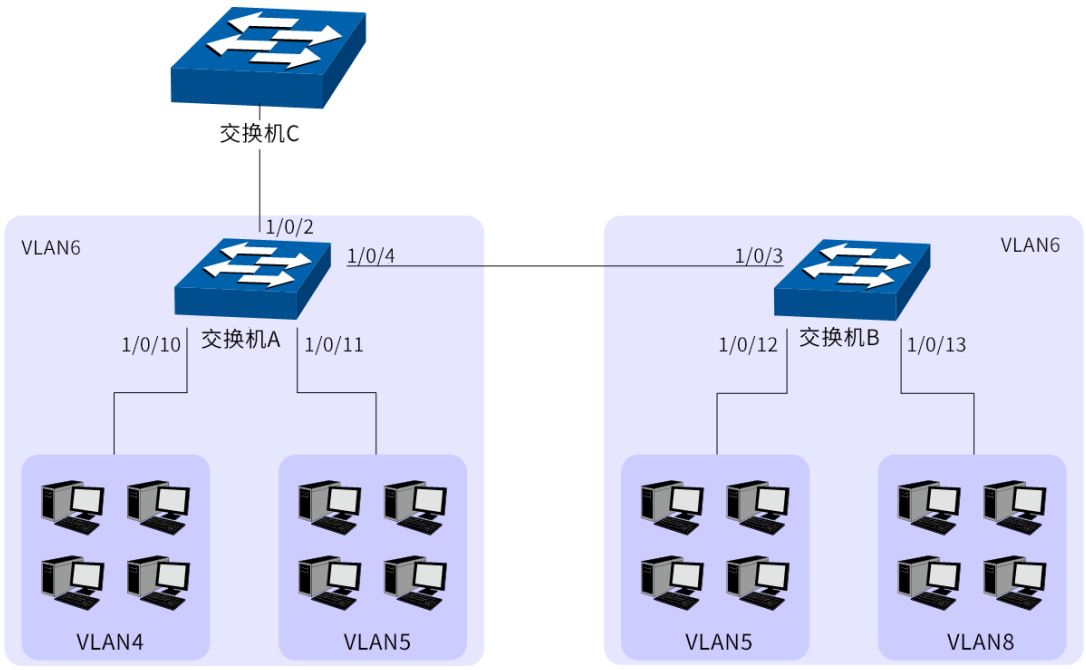
需求如下：

ISP 向某公司提供了网络接入服务，连接到 ISP 机房的接入交换机 A 上，并通过 VLAN6 向企业提供网络服务；

企业中心交换机上连接了许多用户，各用户之间要求通过 VLAN 功能进行二层隔离；

中心交换机向下级联了另外一台汇聚层交换机，汇聚层交换机上配置了 VLAN 功能，部分 VLAN 要求和中心交换机上的 VLAN 进行连通，且所连接的用户均能够访问网络。

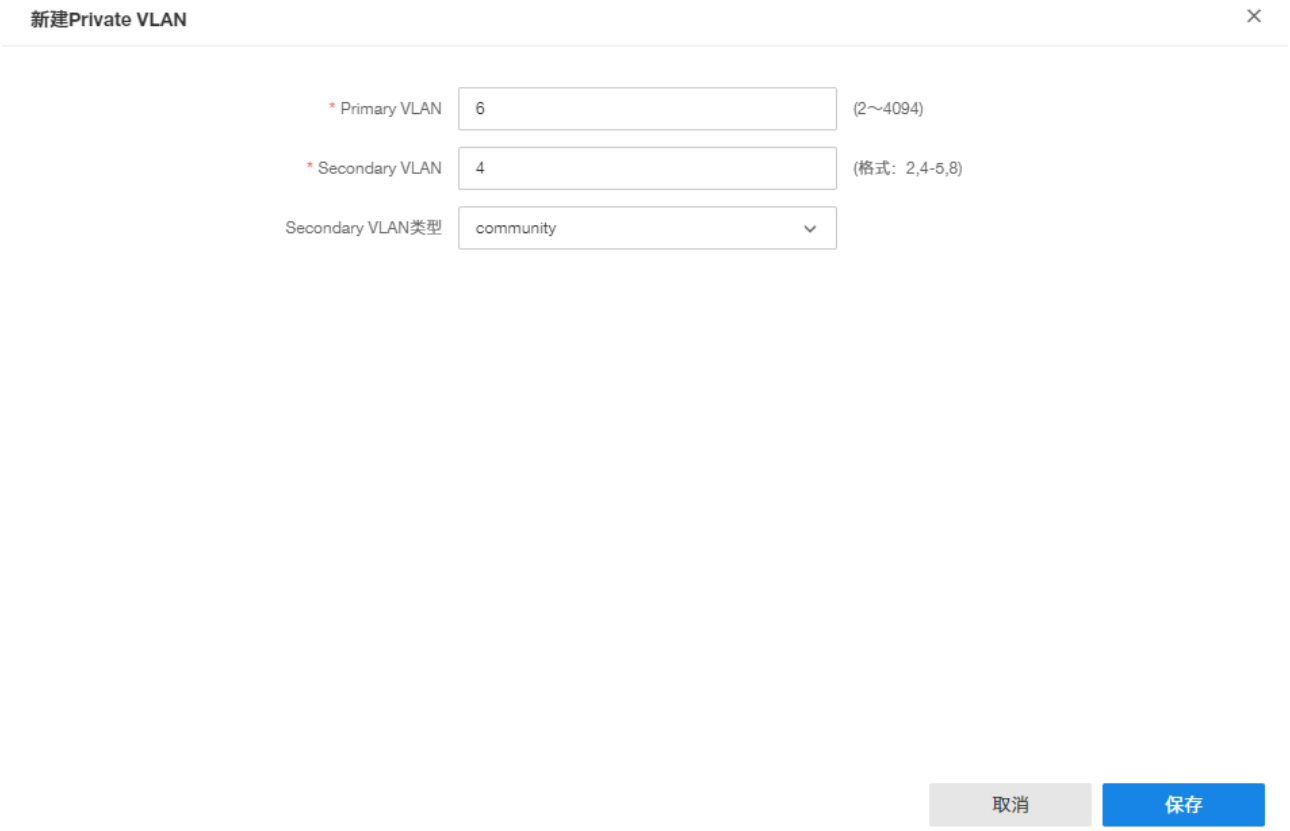
拓扑如下：



- **首先配置交换机 A**

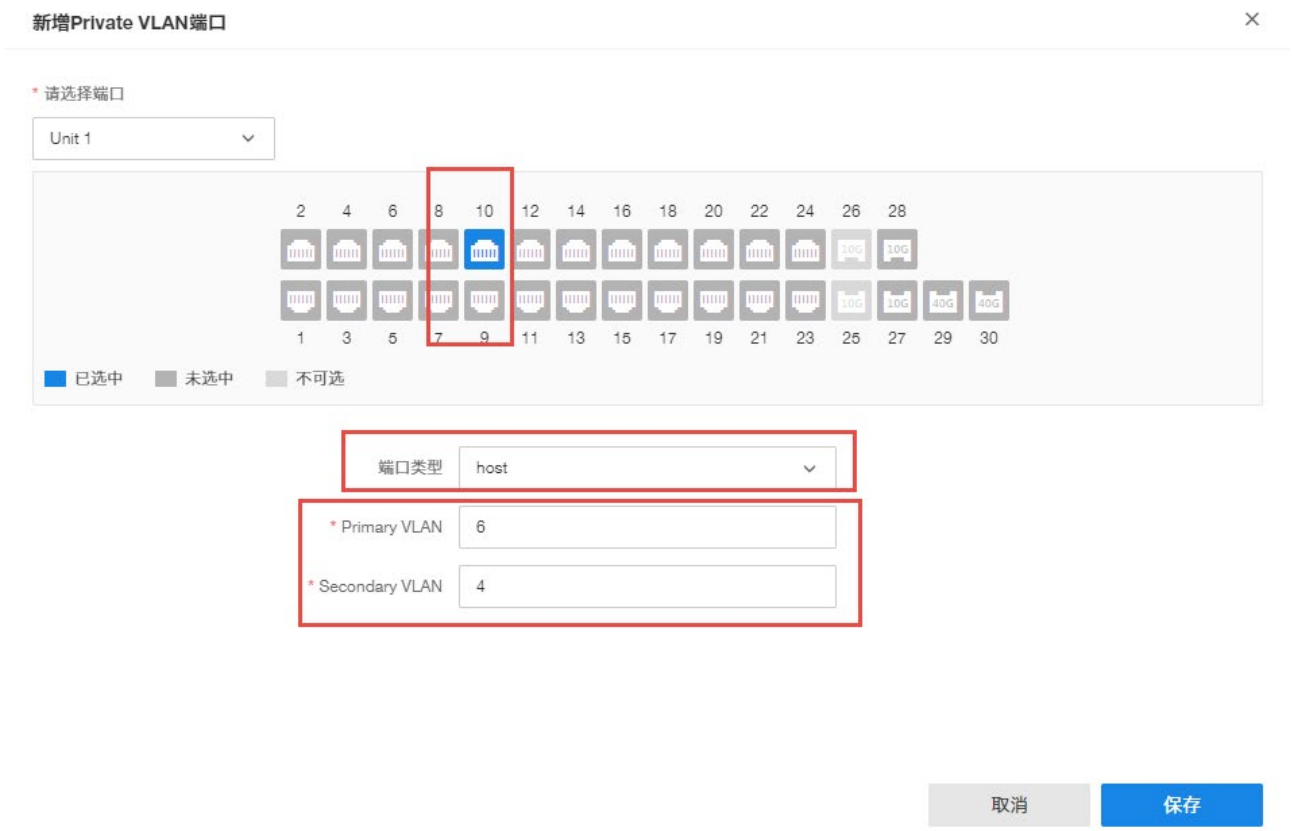
1. 进入页面：网络管理 >> VLAN >> Private VLAN >> PVLAN 配置，点击<新增>，创建 Private VLAN 6/4 和 Private VLAN 6/5。Private VLAN 6/4 中 Primary VLAN 为 6，Secondary VLAN 为 4，Secondary VLAN 类型选择 Community。Private VLAN 6/5 中 Primary VLAN 为 6，Secondary VLAN 为 5，

Secondary VLAN 类型选择 Community。Community VLAN 中的成员相互之间可以直接通信，Isolated VLAN 中的成员相互隔离。设置完成后，点击<保存>。



Private VLAN 配置完成后如下：

2. 进入页面：网络管理 >> VLAN >> Private VLAN >> 端口配置，点击<新增>，选中端口 10，设置端口类型为 Host 并添加到 Private VLAN 6/4 中；选中端口 11，设置端口类型为 Host 并添加到 Private VLAN 6/5 中；选中端口 2 和端口 4，设置端口类型为 Promiscuous 并添加到 Private VLAN 6/4 中。设置完成，点击<保存>。



端口配置完成后如下：

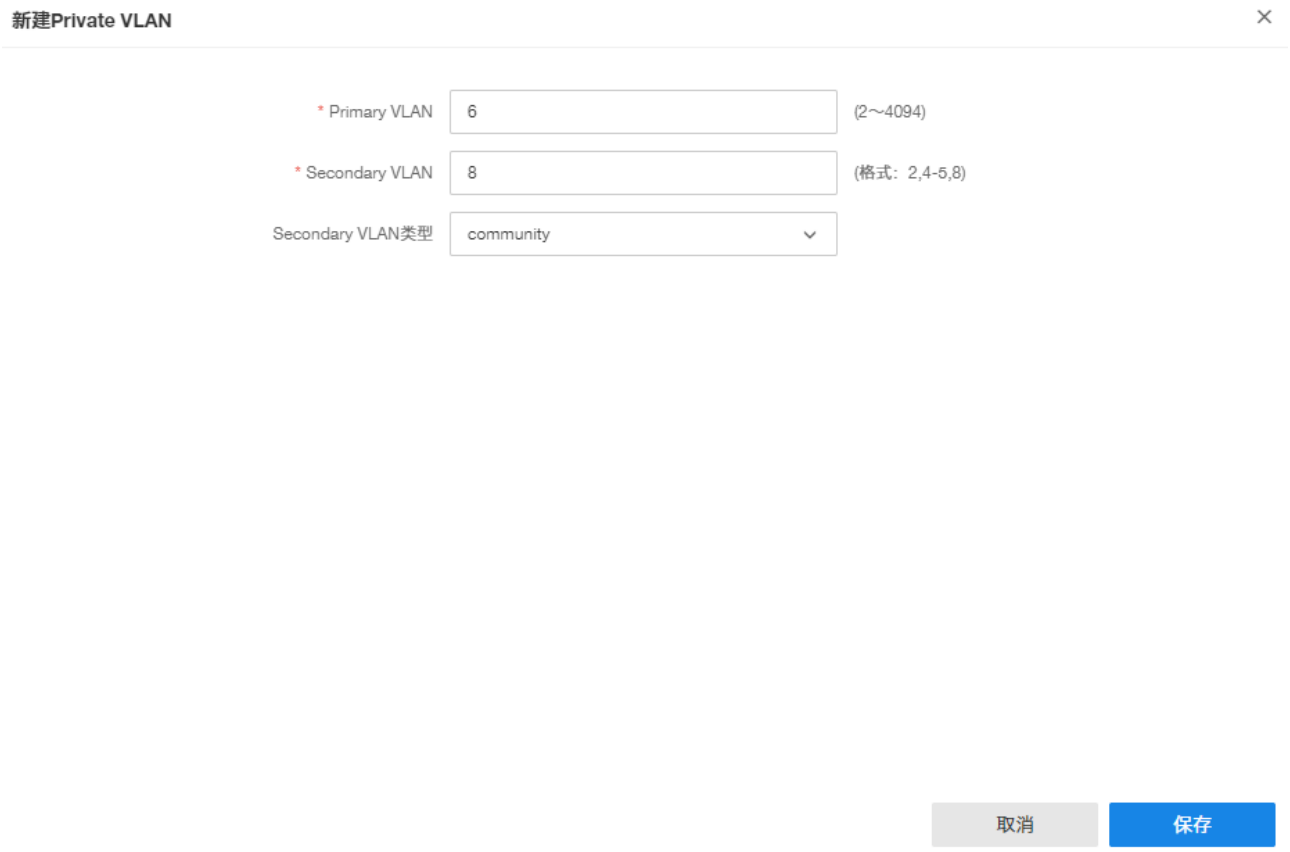
说明：

- 一个 Host 端口只能加入一个 Private VLAN。
- 一个 Promiscuous 只能加入一个 Primary VLAN。
- 如果需要把 Promiscuous 端口加入多个 Private VLAN 中且 Primary VLAN 相同时，只需把 Promiscuous 端口加入任意一个 Private VLAN 即可，端口将自动同步到其它 Private VLAN。
- Promiscuous：和上行设备相连，负责和上行设备通信；Host：和下行设备相连，负责和下行设备通信。

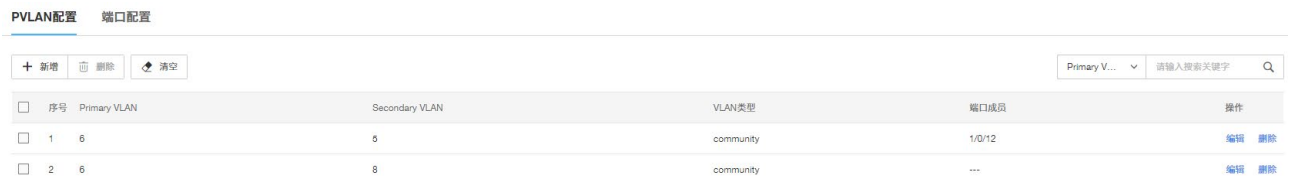
➢ **其次配置交换机 B**

1. 进入页面：网络管理 >> VLAN >> Private VLAN >> PVLAN 配置，点击<新增>，创建 Private VLAN 6/8 和 Private VLAN 6/5。Private VLAN 6/8 中 Primary VLAN 为 6，Secondary VLAN 为 8，Secondary

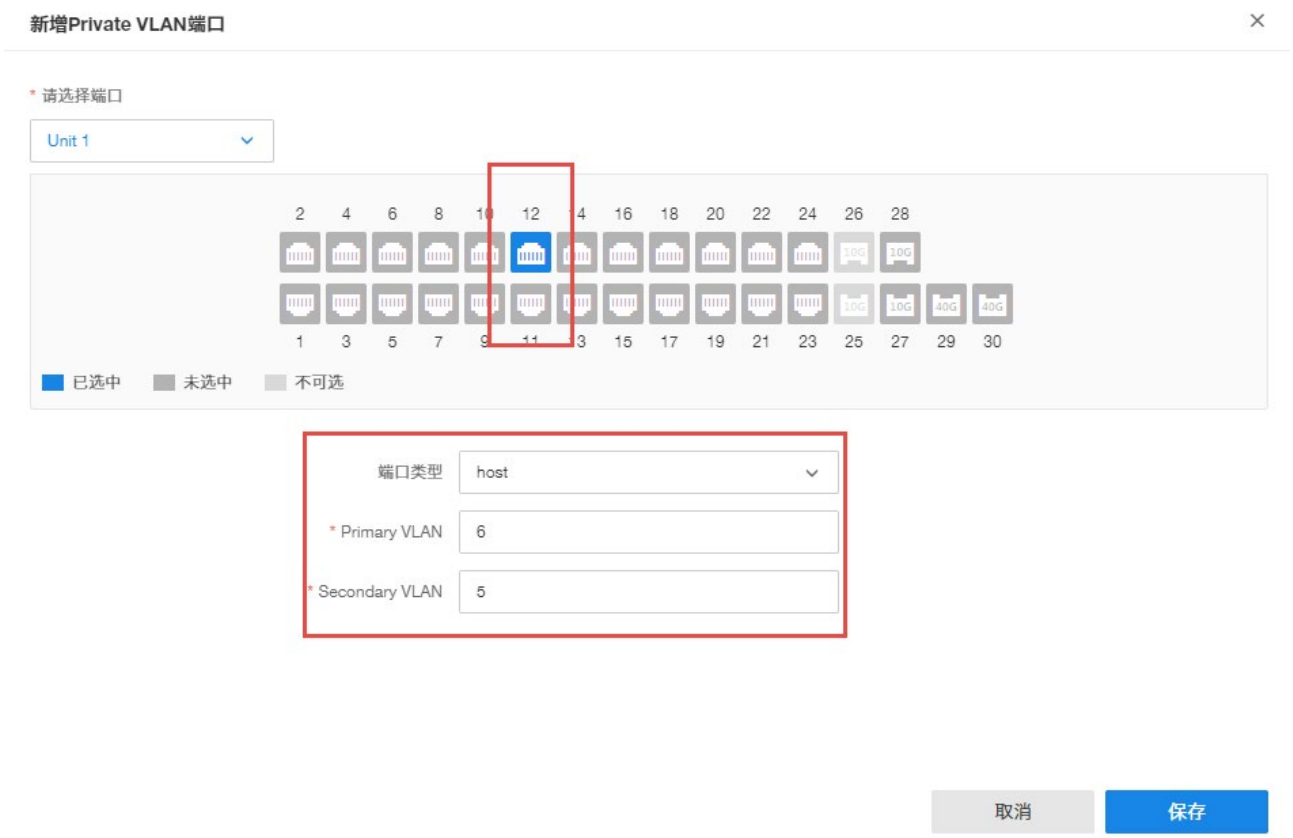
VLAN 类型选择 Community。Private VLAN 6/5 中 Primary VLAN 为 6，Secondary VLAN 为 5，Secondary VLAN 类型选择 Community。Community VLAN 中的成员相互之间可以直接通信，Isolated VLAN 中的成员相互隔离。设置完成后，点击<保存>。



Private VLAN 配置完成后如下：



2. 进入页面：网络管理 >> VLAN >> Private VLAN >> 端口配置，点击<新增>，选中端口 13，设置端口类型为 Host 并添加到 Private VLAN 6/8 中；选中端口 12，设置端口类型为 Host 并添加到 Private VLAN 6/5 中；选中端口 3，设置端口类型为 Promiscuous 并添加到 Private VLAN 6/5 中。设置完成，点击<保存>。



端口配置完成后如下：

5.7 语音 VLAN

5.7.1 应用介绍

具有语音 VLAN 功能的设备将通过 OUI 地址来匹配进入端口的报文中的 MAC 地址字段，源 MAC 地址符合系统设置（预先在交换机上面配置了这个 OUI 地址表）的语音设备 OUI 地址（提供语音 IP 电话的厂商的 OUI 标识是唯一的，可以事先查询到）的报文被认为是语音数据流，被划分到语音 VLAN 中传输，并自动下发优先级规则，提高语音流的优先级，保证通话质量。

5.7.2 语音 VLAN 配置实例

需求介绍：

某公司需要实现语音电话和网络混合组网的需求，且语音电话需要专门在一个 VLAN 中传输。需求如下：

需求 1：

(1) 配置 VLAN 2 为语音 VLAN，只允许语音报文通过。

(2) IP Phone 类型为 Untagged，接入端口是 General 类型端口 1。

(3) 电脑和 IP 电话串联接入交换机，端口 1 工作在自动模式，如果它们在 30 分钟内没有收到语音流，就将相应的语音 VLAN 老化。

(4) 端口 1 允许 OUI 地址是 00-11-22-33-00-00、掩码是 ff-ff-ff-ff-00-00 的语音报文通过，描述字符为 test。

需求 2：

(1) 配置 VLAN 2 为语音 VLAN，只允许语音报文通过。

(2) IP Phone 类型为 Untagged，接入端口是 General 类型端口 1。

(3) 端口 1 只接入了语音电话，工作在手动模式。

(4) 端口 1 允许 OUI 地址是 00-11-22-33-00-00、掩码是 ff-ff-ff-ff-00-00 的语音报文通过，描述字符为 test。

配置步骤：

- **针对需求 1—使用自动模式**

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，对接语音电话的端口 1 点击<编辑>，设置为 GENERAL 口，PVID 保持之前的业务设置不改变（不影响端口 1 的其他业务数据）。

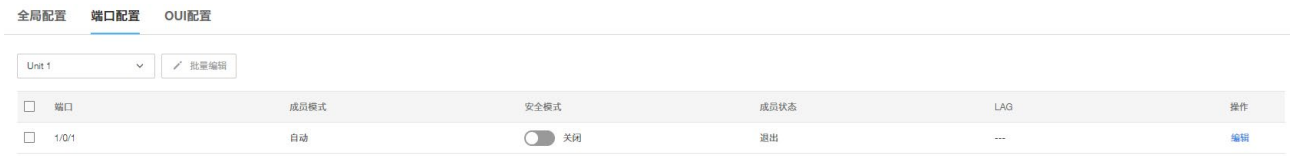
2. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，设置语音 VLAN 2，可以不包含端口（自动模式下交换机根据端口是否收到语音数据自动维护端口加入或退出语音 VLAN）。

3. 进入页面：网络质量 >> 服务质量 >> 语音 VLAN >> 全局配置，启用全局语音 VLAN 功能，配置语音 VLAN 为 VLAN 2，老化时间为 30min，点击<保存>。

说明：

- 语音优先级分为 0~7 共 8 档，默认优先级为 6，且数字越大，优先级越高。

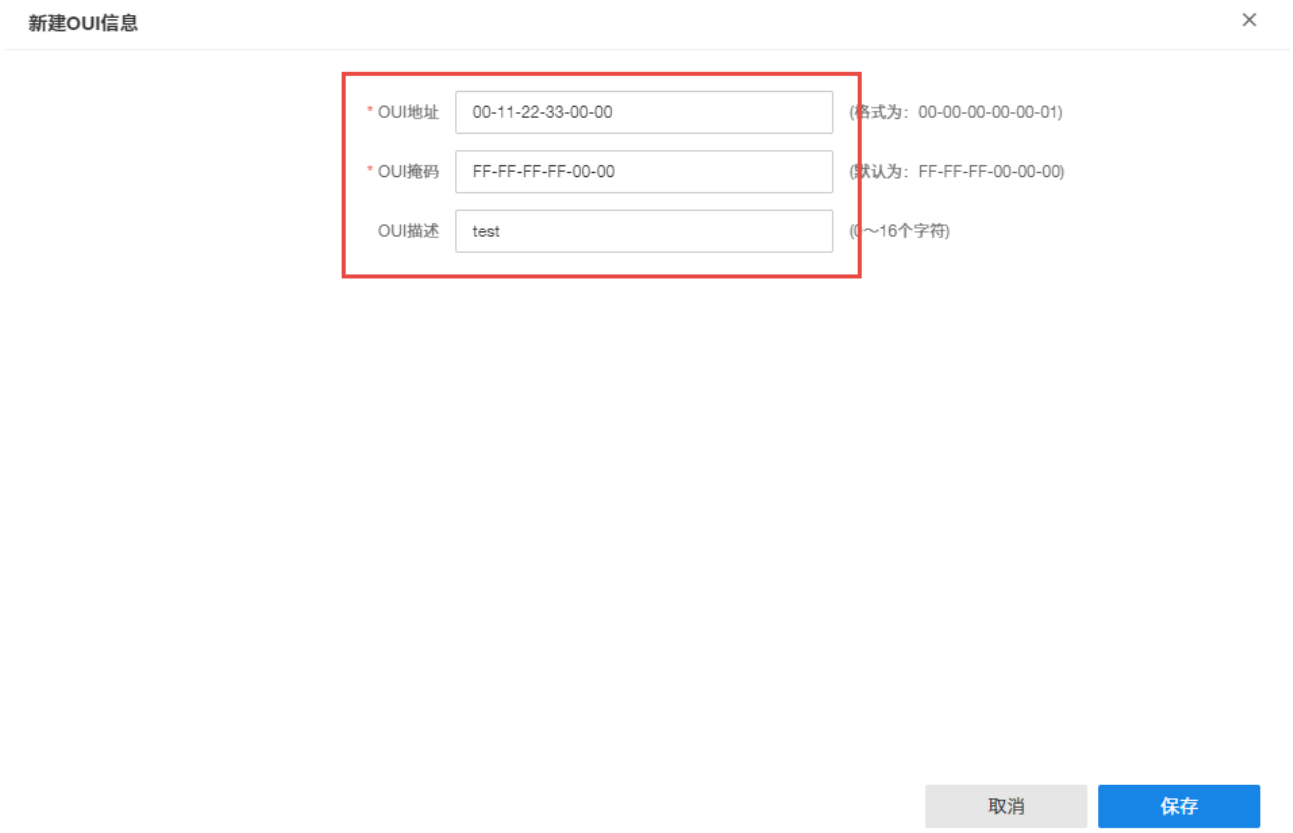
4. 进入页面：网络质量 >> 服务质量 >> 语音 VLAN >> 端口配置，端口 1 默认为自动模式，安全模式禁用。



说明：

- 安全模式代表设置端口转发数据包的模式，其中禁用代表端口转发所有数据包，启用代表端口只转发语音数据包。

5. 进入页面：网络质量 >> 服务质量 >> 语音 VLAN >> OUI 配置，系统已经预设了一些常见厂商的 OUI 地址，如果没有自己厂商的则可点击<新增>通过掩码与运算将设备的地址添加进去。配置完成，点击<保存>。



至此，自动模式下的语音 VLAN 配置成功，端口 1 下符合 OUI 配置的语音设备接入后交换机自动将语音电话数据在 VLAN 2 中传输。

- **针对需求 2—使用手动模式**

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，对接语音电话的端口 1 点击<编辑>，设置为 GENERAL 口，Unta VLAN 为 1 和 2，PVID 设置为 2。

2. 进入页面：网络质量 >> 服务质量 >> 语音 VLAN >> 全局配置，启用全局语音 VLAN 功能，配置语音 VLAN 为 VLAN 2，老化时间为 30min，点击<保存>。

说明：

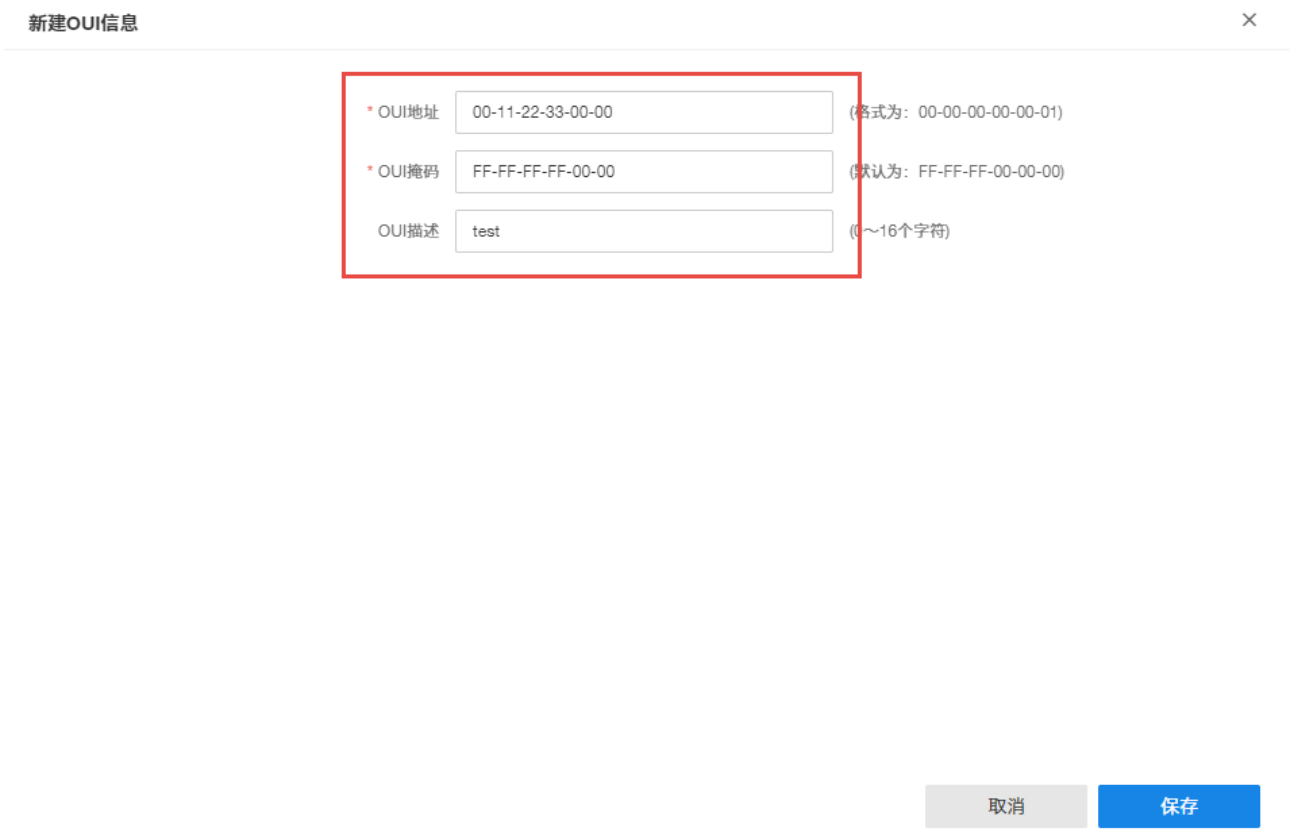
- 语音优先级分为 0~7 共 8 档，默认优先级为 6，且数字越大，优先级越高。

3. 进入页面：网络质量 >> 服务质量 >> 语音 VLAN >> 端口配置，在端口 1 点击<编辑>，设置成员模式为手动模式，安全模式根据自己需求选择。

说明：

- 安全模式代表设置端口转发数据包的模式，其中禁用代表端口转发所有数据包，启用代表端口只转发语音数据包。

4. 进入页面：网络质量 >> 服务质量 >> 语音 VLAN >> OUI 配置，系统已经预设了一些常见厂商的 OUI 地址，如果没有自己厂商的则可点击<新增>通过掩码与运算将设备的地址添加进去。配置完成，点击<保存>。



至此，手动模式下的语音 VLAN 配置成功，手动将 1 口加入在语音 VLAN 2 中。。

注意：

- IP 电话的工作原理：与其他网络设备一样，IP 电话也需要 IP 地址才能在网络中正常通信。IP 电话获取 IP 地址的方式有两种:通过 DHCP 自动获取和通过用户手工配置,可以参考 IP 电话的使用说明书。
- 一般情况下：IP 电话在自动获取 IP 地址时，IP 电话还可以向 DHCP 服务器同时请求 Voice VLAN 信息，如果 DHCP 服务器返回了 Voice VLAN 信息，IP 电话就可以直接发送携带有 Voice VLAN Tag 的语音流（简称 tagged 语音流）；如果 DHCP 服务器没有返回 Voice VLAN 信息，IP 电话就只能发送不带 VLAN Tag 的语音流（简称 untagged 语音流）。同样，在用户在 IP 电话上手工设置 IP 地址时，也可以设置或不设置 Voice VLAN 信息，IP 电话会根据用户的配置发出 tagged/untagged 语音流。
- 语音 VLAN 中的端口可工作在语音 VLAN 的自动模式或手动模式，在不同的工作模式下端口加入语音 VLAN 的方式不同。
- 自动模式：当用户 IP 电话启动时，所发出的报文经支持语音 VLAN 的设备时，设备通过识别该报文的源 MAC 地址，匹配设备上所配置的 OUI 地址，OUI 地址匹配成功后，设备自动将该语音报文的输入端口添加到语音 VLAN，并下发策略，将语音报文的优先级修改为设备上所配置的语音 VLAN 中语音流的优先级，并使用老化机制对语音 VLAN 内的端口进行维护。在老化时间内，系统没有从输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。

- 手动模式：手动模式下，端口加入语音 VLAN 或从语音 VLAN 中删除的过程由管理员手动进行配置。用户 IP 电话通讯过程中，设备通过识别报文的源 MAC 地址，匹配设备上所配置的 OUI 地址，OUI 地址匹配成功后，下发策略，将语音报文的优先级修改为设备上所配置的语音 VLAN 中语音流的优先级。
- 自动模式适用于 PC--IP 电话串联接入端口，可以同时传输语音数据和普通业务数据的组网方式。
- 手工模式适用于 IP 电话单独接入交换机，端口仅传输语音报文的组网方式，这种组网的方式可以使该端口专用于传输语音数据，避免业务数据对语音数据传输的影响。

回目录

第6章　路由功能

说明：

本章节提及的路由器是指传统意义上的路由器或者运行了路由协议的以太网交换机。

在网络中通常由传统路由器或者运行了路由协议的以太网交换机实现不同网络间的数据转发。路由是指路由器根据收到的数据包的目的地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程，而此路径上的最后一个路由节点则将数据转发给目标主机。

在一次路由过程中选择最优路径是路由器需要完成的最重要的工作。路由器通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。常用的路由选择协议有 RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。路由表中的每一个路由条目基本都包含如下基本属性：

- 目的网络地址：用于标识该条路由条目所指向的目标网络。
- 子网掩码：用于标识目标网络的子网掩码。
- 下一跳地址：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。
- 下一跳接口：用于标识数据从本地发出的出接口。

路由条目的来源有三种，分别为直连路由、静态路由和动态路由。

1) 直连路由：通过数据链路层协议发现的，通常为与路由器直接连接的网络的路由。

2) 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

3) 动态路由：通过相互连接的路由器之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。

本交换机的路由模块主要支持直连路由和静态路由两种，也支持动态路由协议 RIP。直连路由即为本地直连网络的路由，如本地配置的 VLAN 进行工作组划分时，同时提供代理 ARP 功能来满足特定网络需求。

6.1　创建接口

网络接口是一种三层模式下的虚拟接口，主要用于实现 VLAN、路由端口之间的三层互通。每个 VLAN 接

口对应一个 VLAN，路由端口对应一个物理端口，环回接口是纯软件接口的。网络接口通过地址与子网掩码参数确定了一个 IP 网段（或称为 IP 子网），并作为该网段的网关对需要跨网段的报文进行基于 IP 地址的三层转发。

进入页面：网络管理 >> 接口配置，点击<新增>，添加新的接口。

接口类型 选择需要配置 IP 地址的接口类型，如 VLAN ID、交换机端口号、环回接口。

接口 ID 选择对应的接口类型后指定 VLAN ID、环回接口 ID、路由端口号或者汇聚口号。

IP 地址模式 设置 IP 地址申请模式。

- None：无 IP。
- 静态 IP：手动设置。
- DHCP：通过 DHCP 申请。
- BOOTP：通过 BOOTP 申请。

IP 地址 选择静态 IP 地址模式时，设置网络接口的 IP 地址。

子网掩码 选择静态 IP 地址模式时，设置网络接口 IP 地址的子网掩码。

三层转发功能 默认开启三层路由转发功能。若此功能后，设备对应接口的三层转发功能关闭，同时无法使用该接口管理设备。默认情况建议开启，关闭后会带来转发异常。

6.2 设置静态路由

静态路由是由网络管理员手动设置的路由，在组网结构比较简单的网络中，网络管理员只需手工配置静态路由即可实现网络互通。静态路由一般在规模不大、拓扑结构固定的网络中配置。在网络中使用合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。当网络发生改变时则需要网络管理员再次修改配置参数以保证网络正常通信。

6.2.1 添加 IPv4 静态路由

进入页面：进入页面：网络管理 >> 路由配置 >> IPv4 静态路由条目，点击<新增>，添加 IPv4 静态路由条目。

目的地址	设置路由条目需要到达的目标网络地址。
子网掩码	设置路由条目需要到达的目标网络的子网掩码。
下一跳地址	设置通往目标网络的路由路径上下一个节点的 IP 地址。
管理距离	指定路由条目的管理距离。管理距离越小，优先级越高。

6.2.2 添加 IPv6 静态路由条目

进入页面：网络管理 >> 路由配置 >> IPv6 静态路由条目，点击<新增>，添加 IPv6 静态路由条目。

目的地址	设置路由条目需要到达的目标网络地址。
前缀长度	设置路由条目需要到达的目标网络的前缀长度。
下一跳地址	设置通往目标网络的路由路径上下一个节点的 IP 地址。
管理距离	指定路由条目的管理距离。管理距离越小，优先级越高。

6.3 路由映射表

路由映射表是交换机策略路由的一个基准表，交换机根据路由映射表来匹配数据流并对数据执行对应的策略转发动作。简单来说是确定指定的数据流，然后对数据流执行操作的一个数据匹配动作表。

6.3.1 创建路由映射表

1. 进入页面：网络管理 >> 路由配置 >> 路由映射表，点击页面上“+”，设置路由映射表名称，点击<保存>。策略路由绑定生效接口时需要指定该名称。

2. 点击页面上<新增>，新建路由映射规则。设置路由映射表规则的序列号和操作类型。

序列号 一条路由映射表中对应不同数据流的序列号，一条路由映射表可以有多个序列表表征多条数据流，序列号默认为 10。

操作类型 对数据包的操作类型有两种，一种是允许，即交换机收到这个数据包会执行下一步动作；一种是拒绝，交换机对收到的数据包不执行下一步动作；默认情况下是允许。

匹配条件 支持设置匹配 ACL，此处 ACL 需要在 ACL 设置指定的数据流条目包括 IP ACL 或 MAC ACL 来指定数据流；支持匹配长度，匹配报文的三层部分长度，最小长度大于等于 68，最大长度小于等于 12270。

设置动作 针对匹配到的数据流执行下一步的转发动作。

设置下一跳：指定下一跳 IP 地址，该动作优先级很高，高于系统直连路由，直连网段数据也会交由下一跳处理。

设置缺省下一跳：指定缺省下一跳 IP 地址，该动作优先级低于系统直连路由。

设置 IP 优先级：在 IP 报文头中配置 IP 优先级。

设置出接口为 null0：将目标接口配置为空接口即丢弃这类数据报文。

6.4 策略路由

6.4.1 应用介绍

交换机的策略路由（PBR：Policy-Based Routing）提供了一种比基于目的地址进行路由转发更加灵活的数据包路由转发机制。策略路由可以根据 IP/IPv6 报文源地址、目的地址、端口、报文长度等内容灵活地进行路由选择，优先级比普通的路由高，这样就可以按照管理员的意志针对部分感兴趣的流量重新定义报文的转发路径，满足一些特殊场景下的需求。

6.4.2 策略路由配置实例

某公网络出口分为外网和专网，需要通过交换机的策略路由实现不同部门访问不同网络。

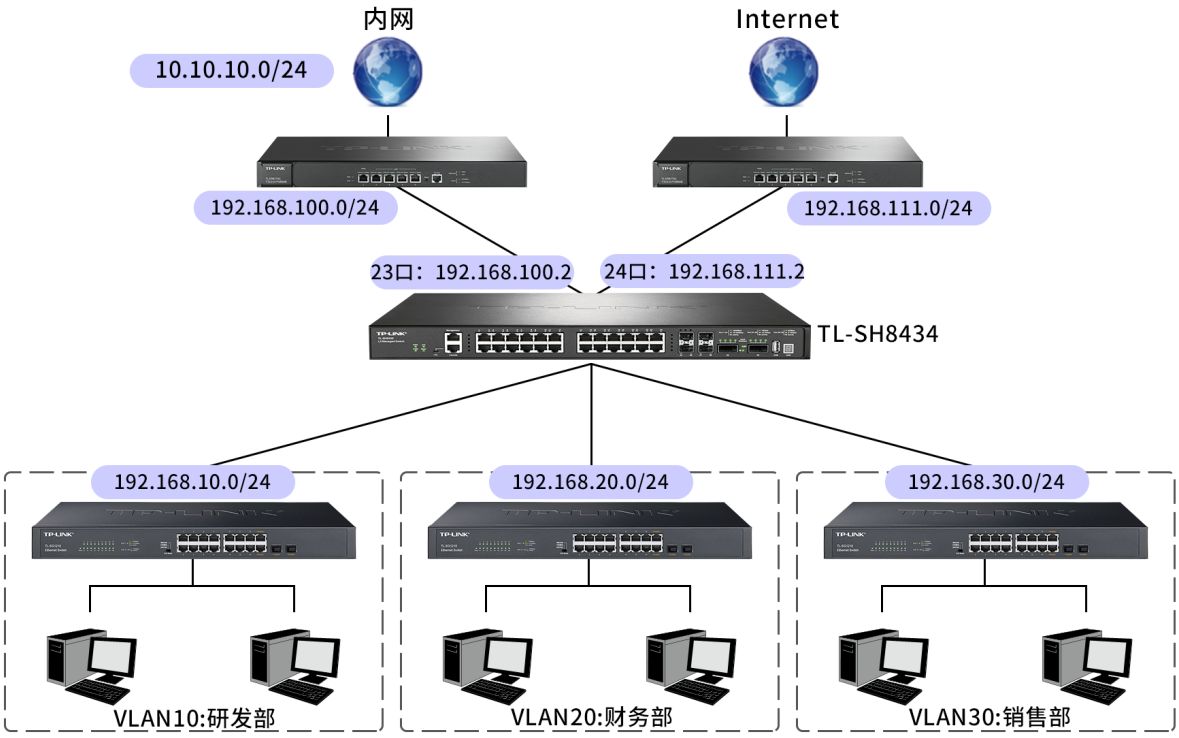
需求介绍：

1. 研发部、财务部、销售部分别划分成不同网段；
2. 研发部门、财务部和销售部门之间不能互访；
3. 研发和财务部门不能访问外网，但可以访问公司内网；销售部门既可以访问外网，也可以访问公司内网。

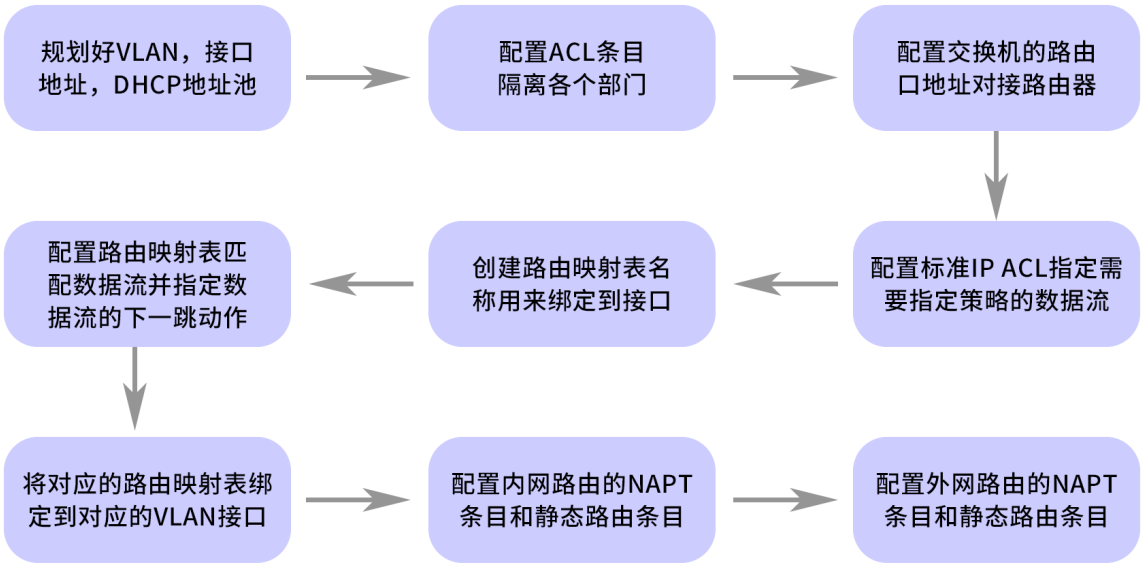
需求分析:

1. 交换机对接两台路由可以通过设置交换机路由口对接不同的出口路由；
2. 不同部门不能互访可以通过设置 ACL 规则来实现；
3. 针对不同网段访问不同资源需要从不同出口路由转发的情况，可以使用核心三层交换机的策略路由功能，通过 ACL 条目匹配交换机中的数据流，针对数据流指定路由下一跳的 IP 地址，从而实现不同数据流从不同出口转发。

拓扑如下：



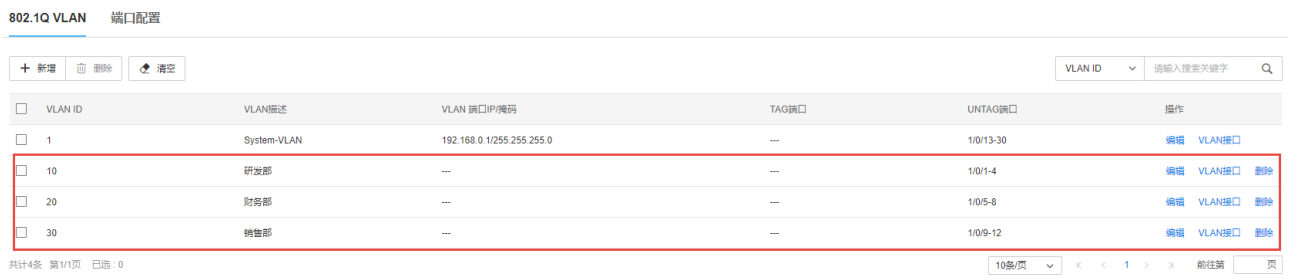
配置流程大致如下：



配置步骤如下：

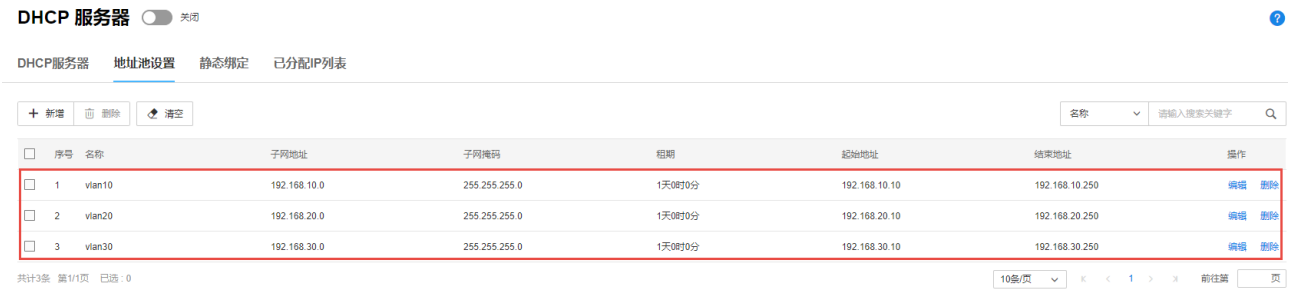
首先，为研发部、财务部和销售部分别划分不同网段。

1. 进入页面：网络管理 >> VLAN >>802.1Q VLAN >> 802.1Q VLAN，点击<新增>，为研发部、财务部、销售部创建 VLAN。创建完成后如下：



2. 进入页面：网络管理 >> 接口配置，点击<新增>，为研发部、财务部、销售部创建接口。创建完成后如下：

3. 进入页面：网络管理 >> DHCP >> DHCP 服务器 >> 地址池设置，点击<新增>，为研发部、财务部、销售部创建 DHCP 地址池。创建完成后如下：



其次，设置研发部、财务部和销售部之间不能互访。

4. 设置研发部不能访问财务部和销售部。进入页面：网络安全 >> 访问控制 >>ACL 配置 >> 标准 IP 访问控制，点击 ACL 列表处的“+”号，创建 ACL ID。创建好之后，点击<新增>，创建 ACL 规则。

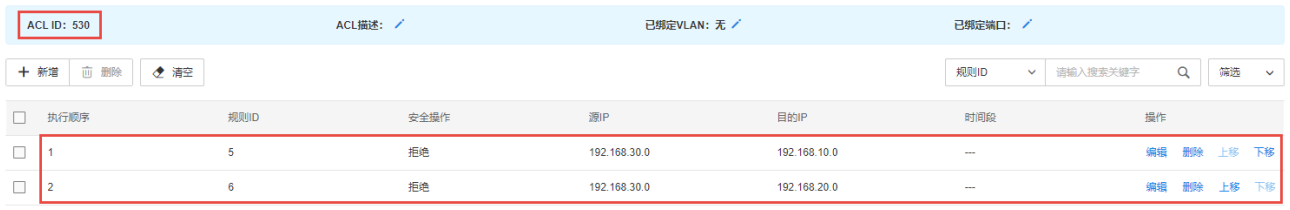
设置完成后，如下：

5. 设置财务部不能访问研发部和销售部。进入页面：网络安全 >> 访问控制 >>ACL 配置 >> 标准 IP 访问控制，点击 ACL 列表处的“+”号，创建 ACL ID。创建好之后，点击<新增>，创建 ACL 规则。

设置完成后，如下：

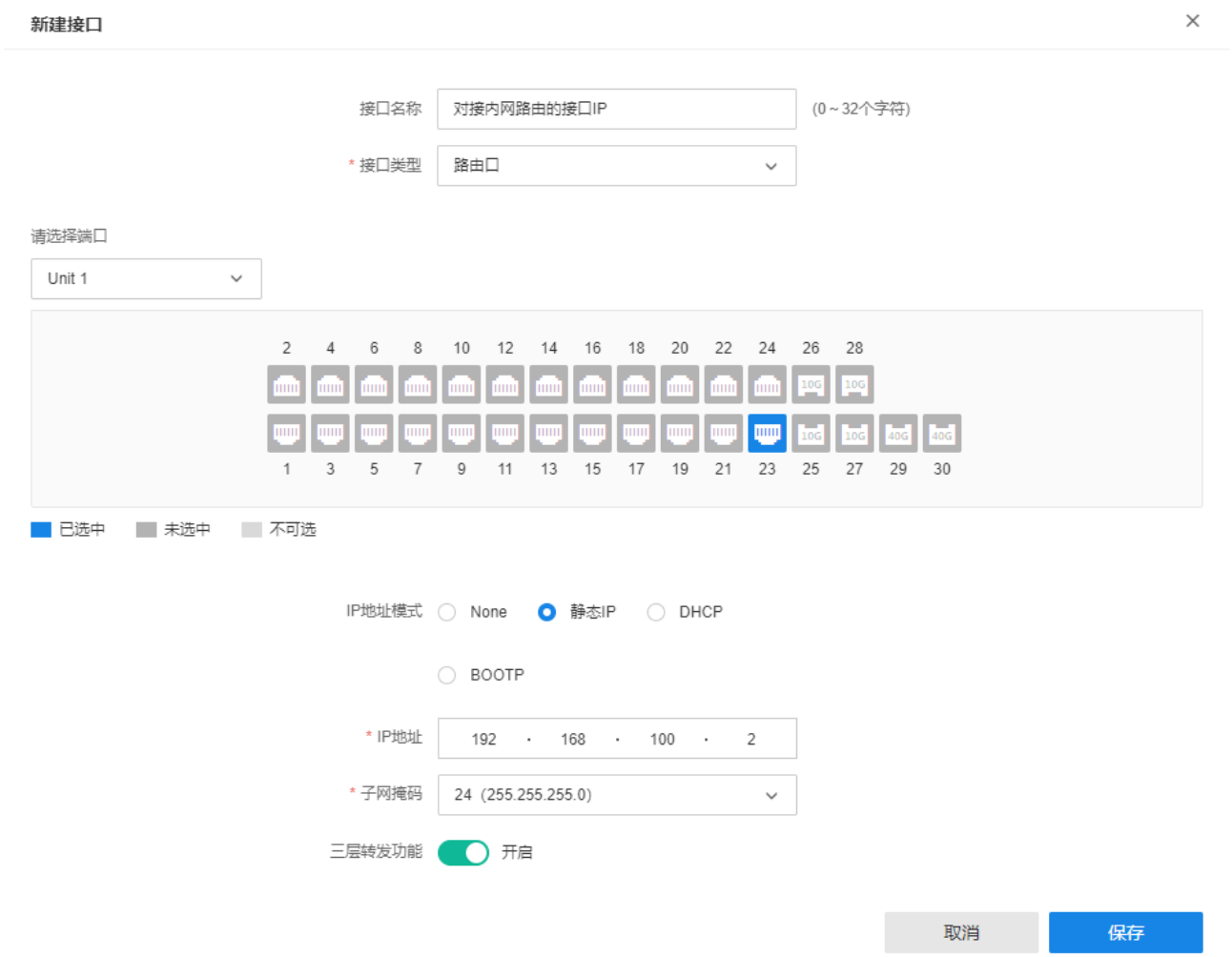
6. 设置销售部不能访问研发部和财务部。进入页面：网络安全 >> 访问控制 >>ACL 配置 >> 标准 IP 访问控制，点击 ACL 列表处的“+”号，创建 ACL ID。创建好之后，点击<新增>，创建 ACL 规则。

设置完成后，如下：

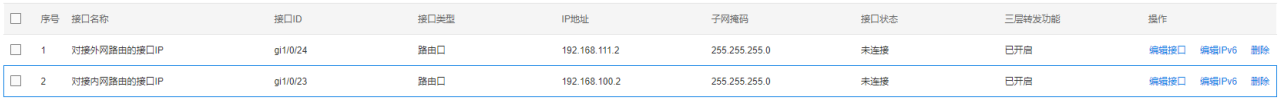


接着，设置策略路由控制不同部门的外网权限。

7. 配置交换机的路由口地址，对接不同的出口路由器。进入页面：网络管理 >> 接口配置，点击<新增>，添加路由口，配置端口 23 对接内网路由器的接口 IP，配置端口 24 对接外网路由器的接口 IP。



配置完成后如下：

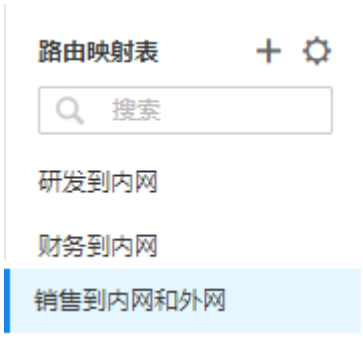


8. 配置研发部、财务部和销售部可以访问公司内网的数据流。进入页面：网络安全 >> 访问控制 >>ACL 配置 >> 标准 IP 访问控制，点击 ACL 列表处的“+”号，创建 ACL ID，点击<新增>，创建 ACL 规则，允许研发部访问公司内网数据流。

同理，创建财务部访问内网数据流和销售部访问内网数据流。

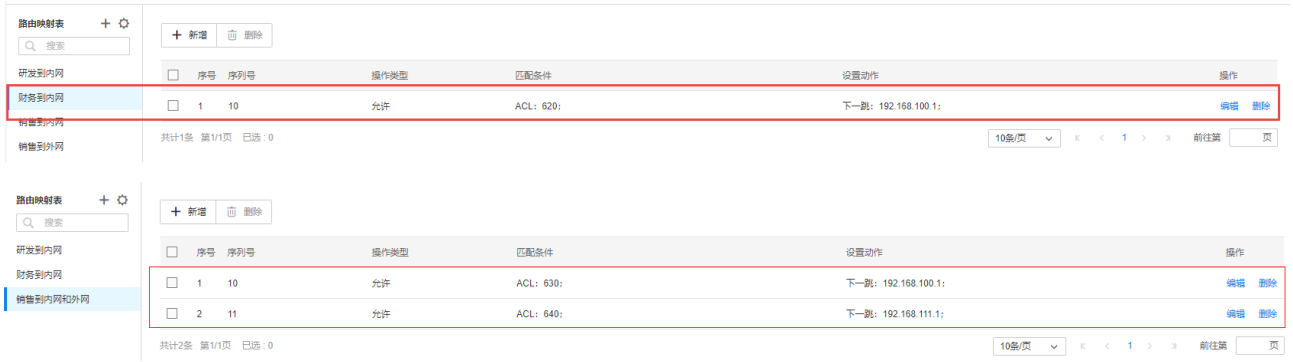
9. 配置销售部访问外网的数据流。进入页面：网络安全 >> 访问控制 >> ACL 配置 >> 标准 IP 访问控制，点击 ACL 列表处的“+”号，创建 ACL ID，创建 ACL 规则，允许销售部访问外网的数据流。

10. 创建路由器映射表，制定策略路由的条目名称，后续用此条目绑定对应的 VLAN 接口、路由接口。进入页面：网络管理 >> 路由配置 >> 路由映射表，点击路由映射表的“+”，设置路由器映射表名称，创建完成如下。



11. 配置路由映射表，针对数据流配置交换机的转发操作。进入页面：网络管理 >> 路由配置 >> 路由映射表，选择研发到内网路由映射表，点击<新增>，将映射表匹配研发到内网的数据流，同时将匹配的数据流执行下一跳到内网路由。

同理，配置财务到内网路由映射表，销售到内网和外网路由映射表。配置完成如下：



12. 配置策略路由，将配置好的路由映射表规则绑定到对应的 VLAN 接口。进入页面：网络管理 >> 路由配置 >> 策略路由，选择 VLAN10，点击<编辑>，路由映射表选择“研发到内网”，完成绑定。

同理绑定 VLAN20 和财务到内网，绑定 VLAN30 和销售到内网、销售到外网。配置完成如下：

说明：

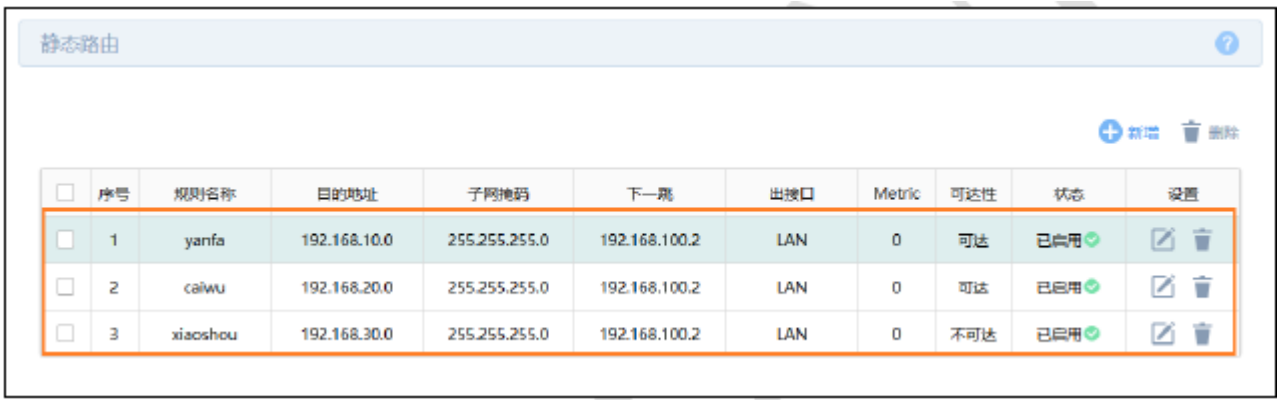
- 一个接口只能绑定一条路由映射表名称，但可以通过一个路由映射表中的序列号区分不同的数据流和动作。

最后配置 NAPT 和静态路由条目，保证数据正常转发。

13. 在内网路由器上配置内网 NAPT 规则和静态路由。具体配置方法可参见对应路由器的用户手册。

内网 NAPT 规则：

内网路由器回程路由规则：



14. 在外网路由器上配置外网 NAPT 规则和静态路由。具体配置方法可参见对应路由器的用户手册。

外网路由器 NATP 规则：

外网路由器回程路由规则：

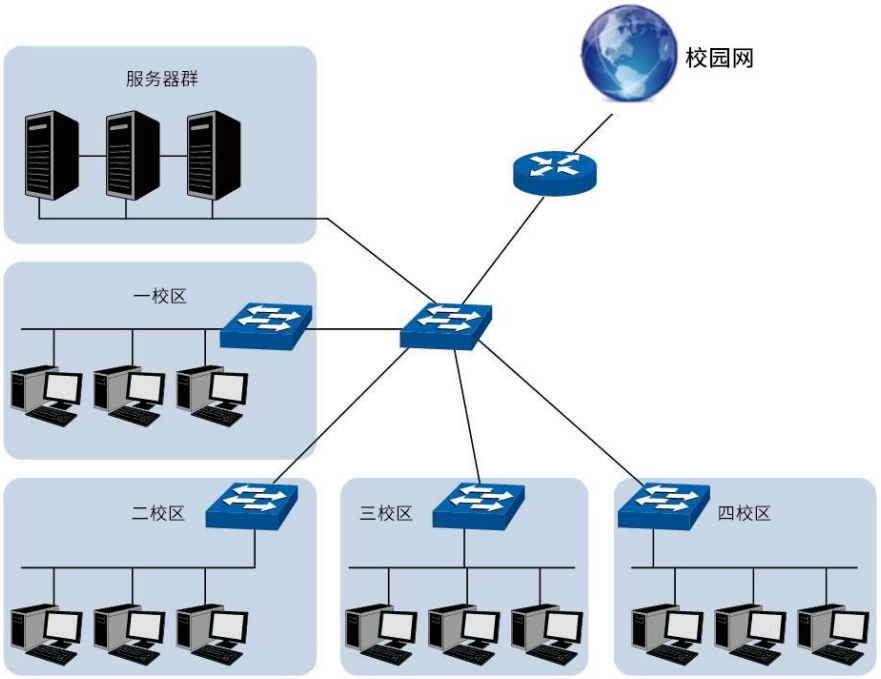
15. 点击页面右上角<保存全局配置>，至此，配置完成。

6.5 RIP

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的动态路由协议，主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP 协议。RIP 作为最早的内部网关协议（Interior Gateway Protocol，IGP）之一，由于实现比较简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，至今仍被广泛使用。RIP 当前有 RIPv1 和 RIPv2 两个版本。

- **RIP 应用场景**

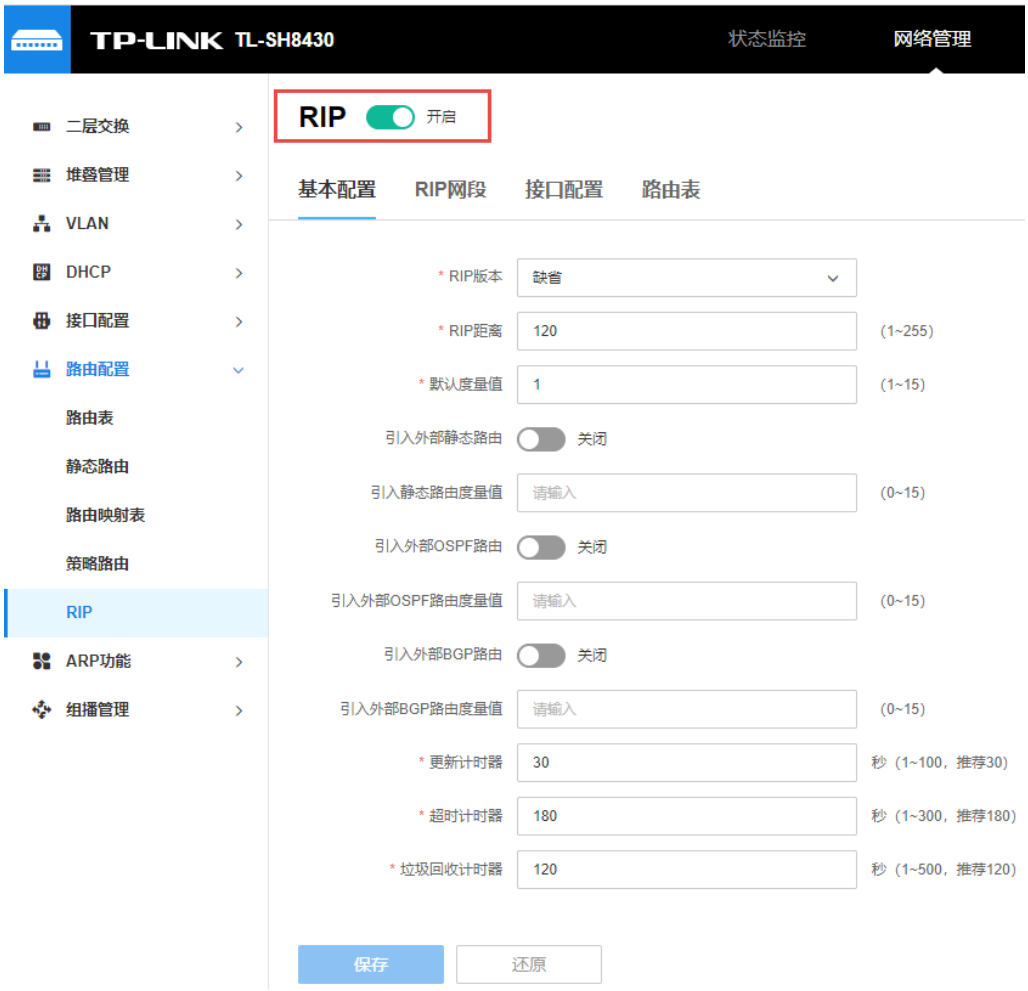
RIP 允许的最大跳数为 15，因此 RIP 适用于规模较小的网络，比如校园网以及结构较简单的地区性网络，如下图所示：



6.5.1 RIP 全局配置

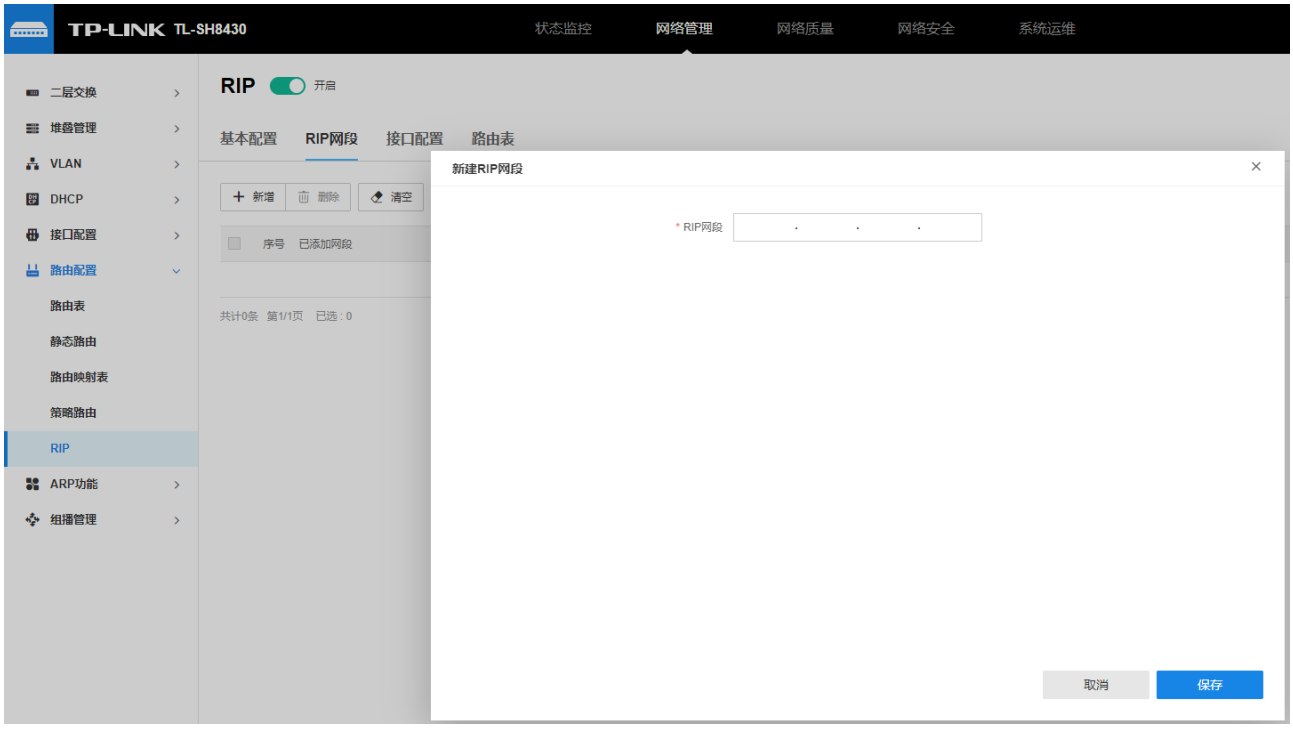
首先启用 RIP 协议，其次添加网段并开启该网段的 RIP 协议。

1. 进入页面：网络管理 >> 路由配置 >> RIP >> 基本配置，开启 RIP 功能，配置基本参数。



RIP 版本	选择使用的 RIP 协议版本，可选版本有 RIPv1 和 RIPv2。 ● 缺省：发送数据包按照 RIP 协议版本 2 格式，接收 RIP 协议版本 1 和 2 的数据包。 ● RIPv1：仅发送和接收 RIPv1 报文。发送报文时采用广播方式。 ● RIPv2：仅发送和接收 RIPv2 报文。发送报文时采用组播方式。
RIP 距离	配置 RIP 协议的管理距离。取值范围为 1-255。管理距离被看作是一个可信度测度，管理距离数值越小，协议的可信度越高。其中 255 表示任何来自不可信源端的路由。默认为“120”。
默认度量值	设置 RIP 协议在引入外部路由时的默认度量值，取值范围为 1-15，默认值为“1”。
引入外部静态路由	选择使能或者禁用引入外部静态路由到 RIP 协议中，默认为“禁用”。
引入静态路由度量值	设置 RIP 协议在引入外部静态路由时的默认度量值，取值范围为 0-15。默认值为“0”。
引入外部 OSPF 路由	选择启用或者禁用引入外部 OSPF 路由到 RIP 协议中，默认为 “禁用”。
引入 OSPF 路由的度量值	设置 RIP 协议在引入外部 OSPF 路由时的默认度量值，取值范围为 0-15。
引入外部 BGP 路由	选择启用或者禁用引入外部 BGP 路由到 RIP 协议中，默认为禁用。
引入 BGP 路由的度量值	设置 RIP 协议在引入外部 BGP 路由时的默认度量值，取值范围为 0-15。
更新计时器	填写 RIP 任务发送更新报文的间隔。取值范围为 1-100 秒，推荐设置为“30 秒”。
超时计时器	填写路由条目的有效期，如果在此段时间内该条目未被更新，那么该条目所表达的路径将被自动设置为不可达。取值范围为 1-300 秒，推荐设置为“180 秒”（即 6 个更新周期）。
垃圾回收计时器	垃圾回收计时器决定了路由条目从变为不可达到被彻底删除的时间间隔，如果一条路由条目变为不可达以后，并且在该段时间内仍未被更新，那么该条目将会被自动删除。取值范围为 1-500 秒，推荐设置为“120 秒”。

2. 进入页面：网络管理 >> 路由配置 >> RIP >> RIP 网段，点击<新增>，添加新的 RIP 协议生效的网段。在该网段中的交换机接口将启动 RIP 协议。



6.5.2 RIP 接口配置

进入页面：网络管理 >> 路由配置 >> RIP >> 接口配置，对当前已有接口点击<编辑>。

接口 ID 显示该接口的 ID。

接口状态 显示接口的 RIP 运行状态，由 RIP 使能的网段决定。

RIP 发送版本　选择接口所支持的发送报文的 RIP 版本号。

- RIPv1：发送报文使用 RIPv1 格式。
- RIPv2：发送报文使用 RIPv2 格式。

RIP 接收版本　接口所支持的接收报文的 RIP 版本号。

- RIPv1：支持接收 RIPv1 格式的报文。
- RIPv2：支持接收 RIPv2 格式的报文。
- Both：同时支持接收 RIPv1 和 RIPv2 格式的报文。

被动接口　抑制接口发送路由更新报文。

认证类型　设置接口所接收和发送的报文是否使用认证功能，默认为“无”。只有使用相同认证类型和认证密码的设备能交换 RIP 报文。仅 RIPv2 支持报文认证功能。

- 无：不使用认证功能。
- 简单认证：使用简单密码进行认证。选择“简单认证”后，需要在“密钥”一栏输入认证时使用的密钥。该密钥将被添加在 RIP 报文首部，只有使用相同认证类型和密钥的设备能相互通信。
- MD5：使用 MD5 进行认证。选择“MD5”后，需要在“密钥 ID”和“密钥”栏中输入认证时使用的密钥 ID 和密钥。

密钥 ID　设置 MD5 密钥时必须同时输入密钥 ID，该 ID 为 1-255 之间的一个整数。

密钥　设置接口认证时使用的密匙。该密钥为一个字符串。

水平分割　选择是否启用水平分割功能。启用以后，本设备不会把从某个接口学到的路由信息再从该接口发送回去。默认为“启用”。

毒性逆转　选择是否启用毒性逆转功能。启用以后，RIP 从某个接口学到路由条目后，会将该路由条目的度量值设为 16，再从原来的接口发送回去。当同时启用水平分割和毒性逆转时，只有毒性逆转功能生效。该功能默认为“禁用”。


说明：

- 当 RIP 接收版本和发送版本的全局配置与接口配置不一致时，将以接口配置为准。
- RIPv1 不支持报文认证，因此当 RIP 版本号选择为 RIPv1，配置的认证信息（认证类型，密钥 ID 和密钥）不生效。当 RIP 的版本为 RIPv1 时，虽然在接口视图下仍然可以配置验证方式，但由于 RIPv1 不支持认证，因此该配置不会生效。

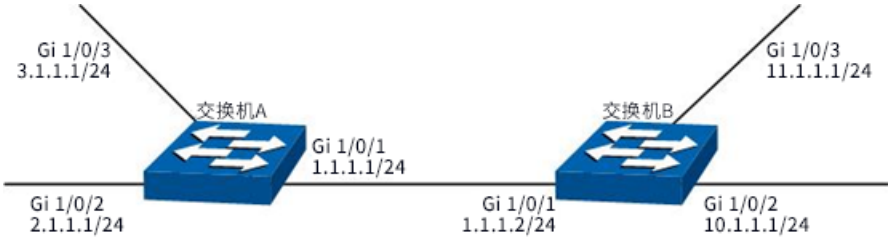
6.5.3 RIP 配置实例

- **组网需求**

交换机 A 三个接口的 IP 地址分别为 1.1.1.1/24，2.1.1.1/24，3.1.1.1/24。交换机 B 三个接口的 IP 地址分别为 1.1.1.2/24，10.1.1.1/24，11.1.1.1/24。

要求在交换机 A，B 的所有接口上使能 RIP，并使用 RIPv2 协议进行网络互连。

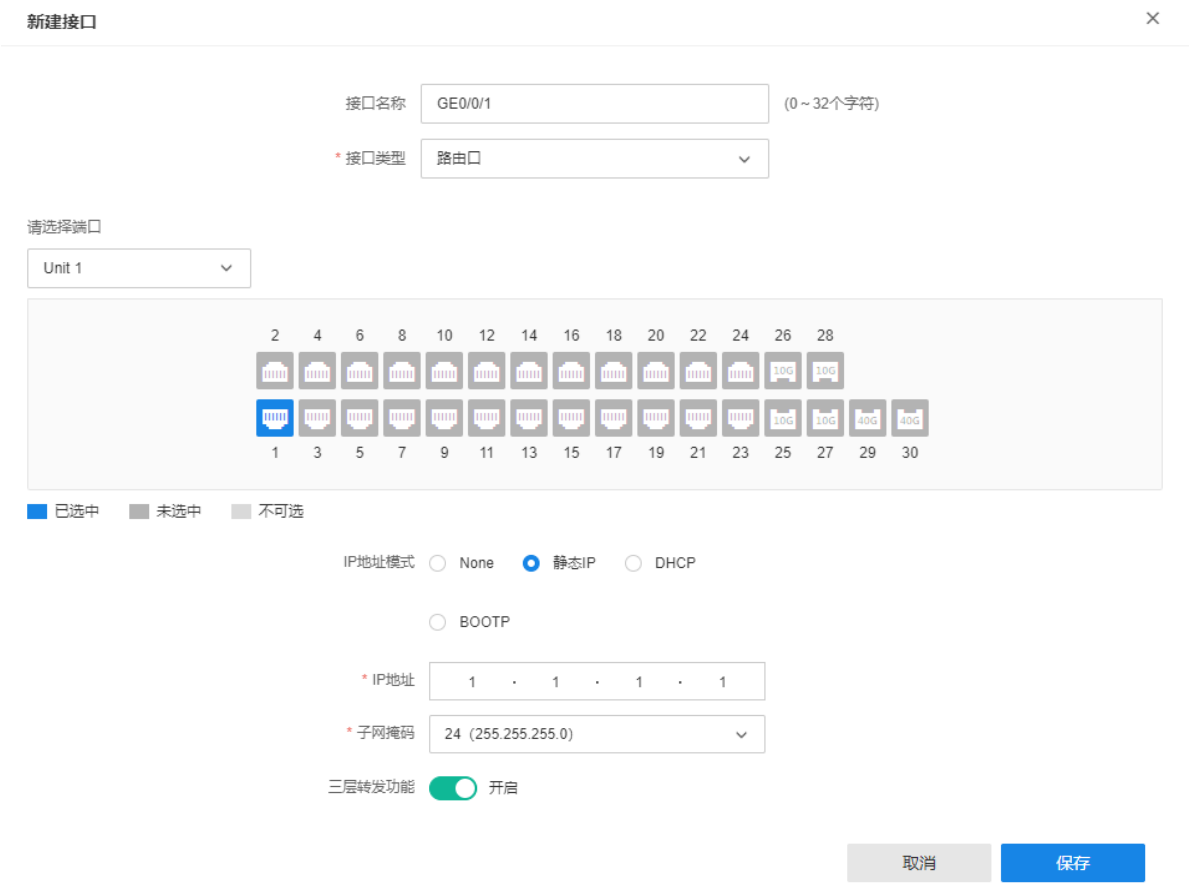
- **组网拓扑**



配置步骤：

- **配置交换机 A**

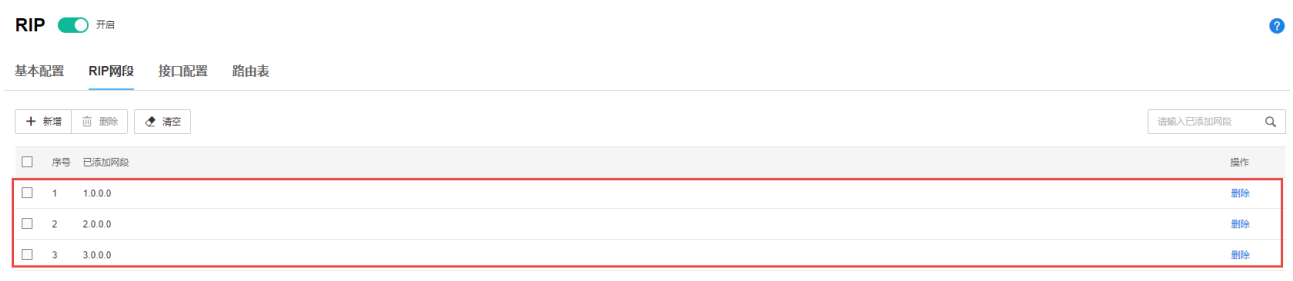
1. 进入页面：网络管理 >> 接口配置，点击<新增>，创建三个接口，分别配置静态 IP 地址 1.1.1.2/24，2.1.1.1/24，3.1.1.1/24.



创建完成后如下：

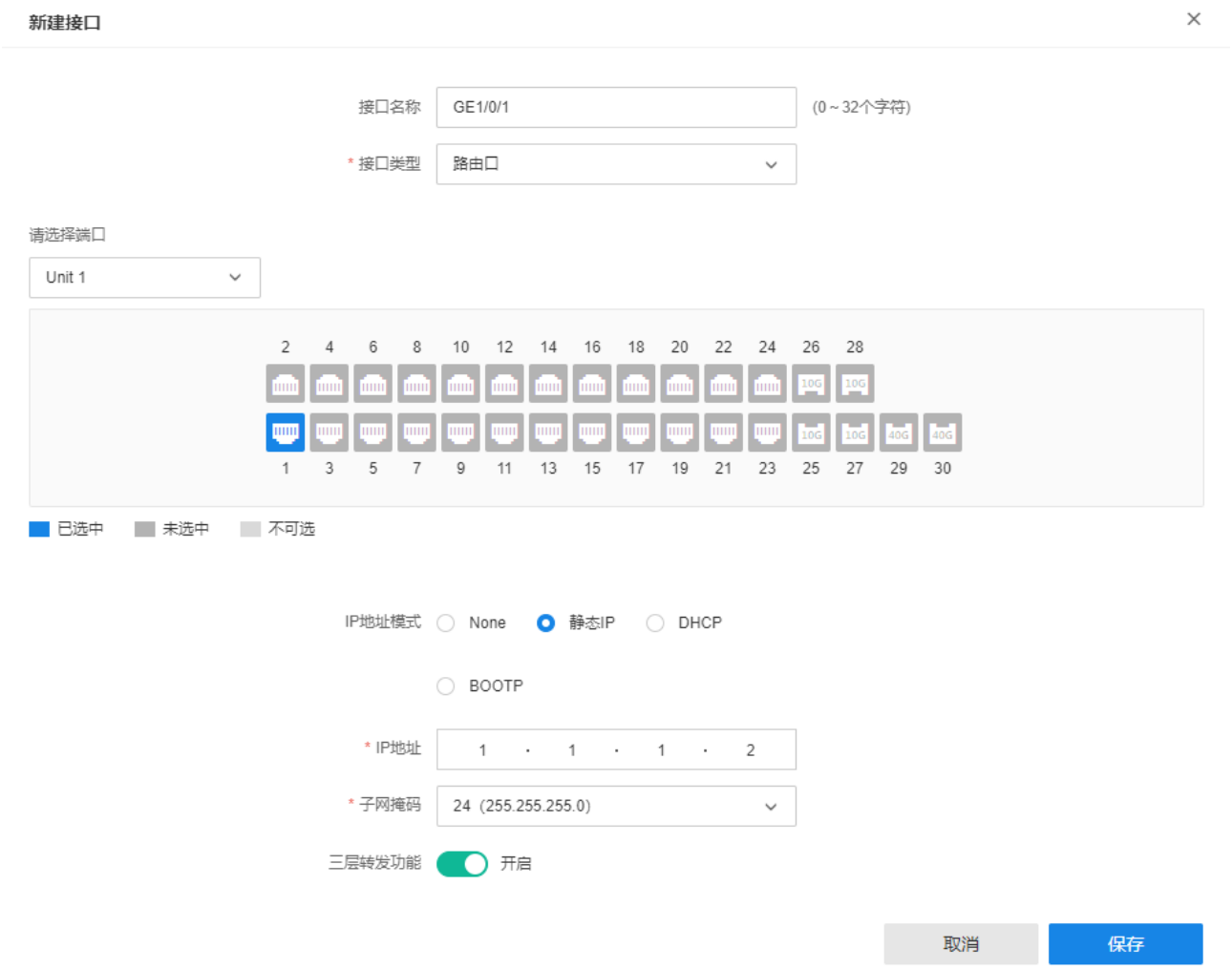
2. 进入页面：网络管理 >> 路由配置 >>RIP>> 基本配置，开启 RIP 协议，选择 RIP 版本为 RIPv2，点击<保存>。

3. 进入页面：网络管理 >> 路由配置 >>RIP>>RIP 网段，点击<新增>，添加 RIP 网段 1.0.0.0，2.0.0.0，3.0.0.0。设置完成如下：

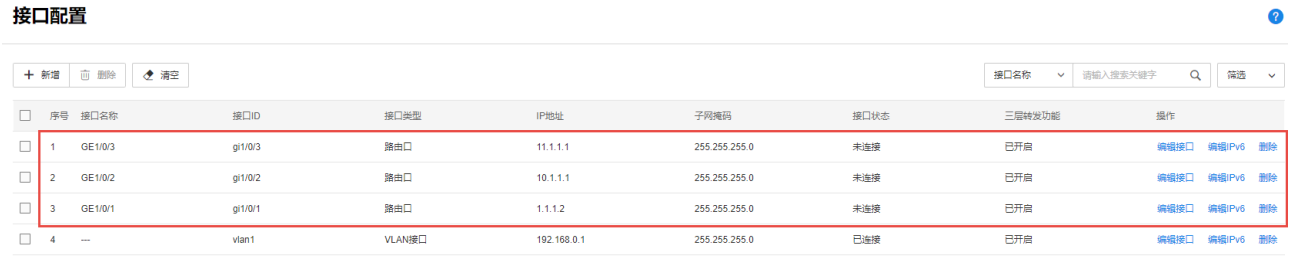


➢ **配置交换机 B**

1. 进入页面：网络管理 >> 接口配置，点击<新增>，创建三个接口，分别配置静态 IP 地址 1.1.1.1/24，10.1.1.1/24，11.1.1.1/24.

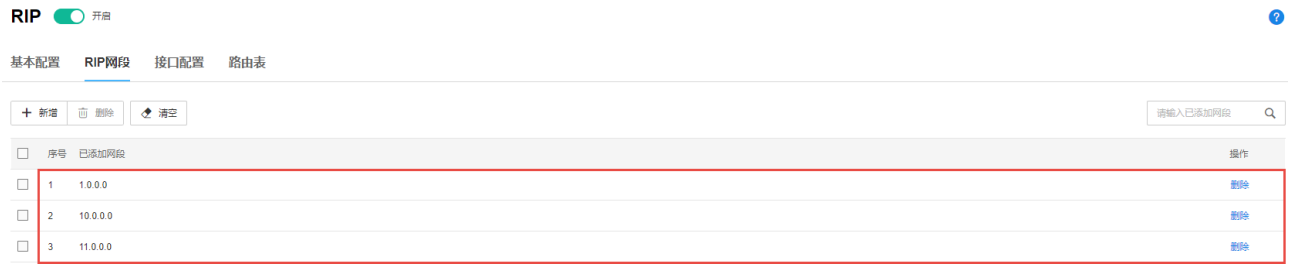


创建完成后如下：



2. 进入页面：网络管理 >> 路由配置 >>RIP>> 基本配置，开启 RIP 协议，选择 RIP 版本为 RIPv2，点击<保存>。

3. 进入页面：网络管理 >> 路由配置 >> RIP >> RIP 网段，点击<新增>，添加 RIP 网段 1.0.0.0，2.0.0.0，3.0.0.0。设置完成如下：



6.6 DHCP 服务器

6.6.1 应用介绍

DHCP 服务器的应用环境

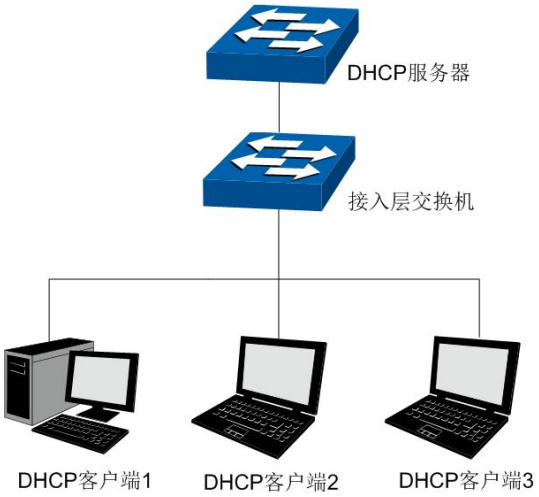
DHCP 服务器可以在下列场景中高效完成网络设备的 IP 地址配置工作：

1) 网络规模大，为每台网络设备手工配置网络参数的工作量较大，且不便于对网络进行集中管理。

2) 网络中设备数目大于该网络支持的设备数量，相应的 IP 资源不足。例如，ISP 限制同时接入网络的用户数目，而网络中的设备并不需要同时访问网络，则用户可以动态按需获得网络 IP。

3) 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

下图为本交换机配置为 DHCP 服务器时的网络拓扑图示范，具体的网络环境可能根据实际需求有所调整。



为了使网络中的设备能够安全顺利的获得 IP 地址，保证网络的稳定性，本交换机的 DHCP 服务器功能可以完成如下所示任务：

- 本交换机为网络中的多个 VLAN 指定特定的地址池，实现不同 VLAN 的设备获得不同网段的 IP 地址。
- 当客户端向本交换机申请 IP 地址时，交换机判断接收请求报文的端口所属的默认 VLAN，从该 VLAN 接口 IP 所属的地址池中选取合适的地址分配给客户端。
- 如果服务器和客户端之间搭建了 DHCP 中继设备，DHCP 请求报文经过 DHCP 中继设备时报文中的 giaddr 字段将被填入中继设备上客户端连接的接口 IP 地址，服务器将在此 IP 网段地址池中选择合适的 IP 地址分配给客户端。如果 DHCP 服务器上没有创建中继设备 IP 地址段的地址池，客户端将无法获得 IP 地址。
- IP 地址重复分配检测功能，避免因同一地址重复分配而造成的网络中 IP 冲突。

➢ **IP 地址重复分配检测**

当交换机配置了 DHCP 服务器功能为网络中的设备分配 IP 地址时，为防止 IP 地址重复分配导致 IP 地址冲突，交换机将对该地址进行 Ping 探测。地址检测方式如下：

DHCP 服务器发送目的 IP 地址为待分配地址的 ICMP 回显请求报文，如果在等待时间内收到响应报文，DHCP 服务器从地址池中选择新的 IP 地址，并重复上述探测操作；如果在指定时间内没有收到回显响应报

文，则将地址分配给客户端，从而确保客户端被分得的 IP 地址唯一。

- **分配 IP 地址的优先次序**

交换机的 DHCP 服务器功能为客户端分配 IP 地址时，其分配规则如下：

1) DHCP 服务器中与客户端 MAC 地址手动绑定的 IP 地址。

2) DHCP 服务器曾经分配给客户端的 IP 地址。

3) 客户端发送的 DHCP-DISCOVER 报文中指定的 IP 地址。

4) 选择合适的地址池，从中顺序查找可供分配的第一个 IP 地址。

- **DHCP 服务器在本交换机上的配置要点**

1) 为每个网段保留特定的 IP 地址不做分配，如网关地址、网段广播地址、服务器地址等。

2) 为特殊用户群手动绑定静态 IP，当收到特殊用户群的 IP 申请时，交换机将为客户端分配租期为无限长的固定的 IP 地址。

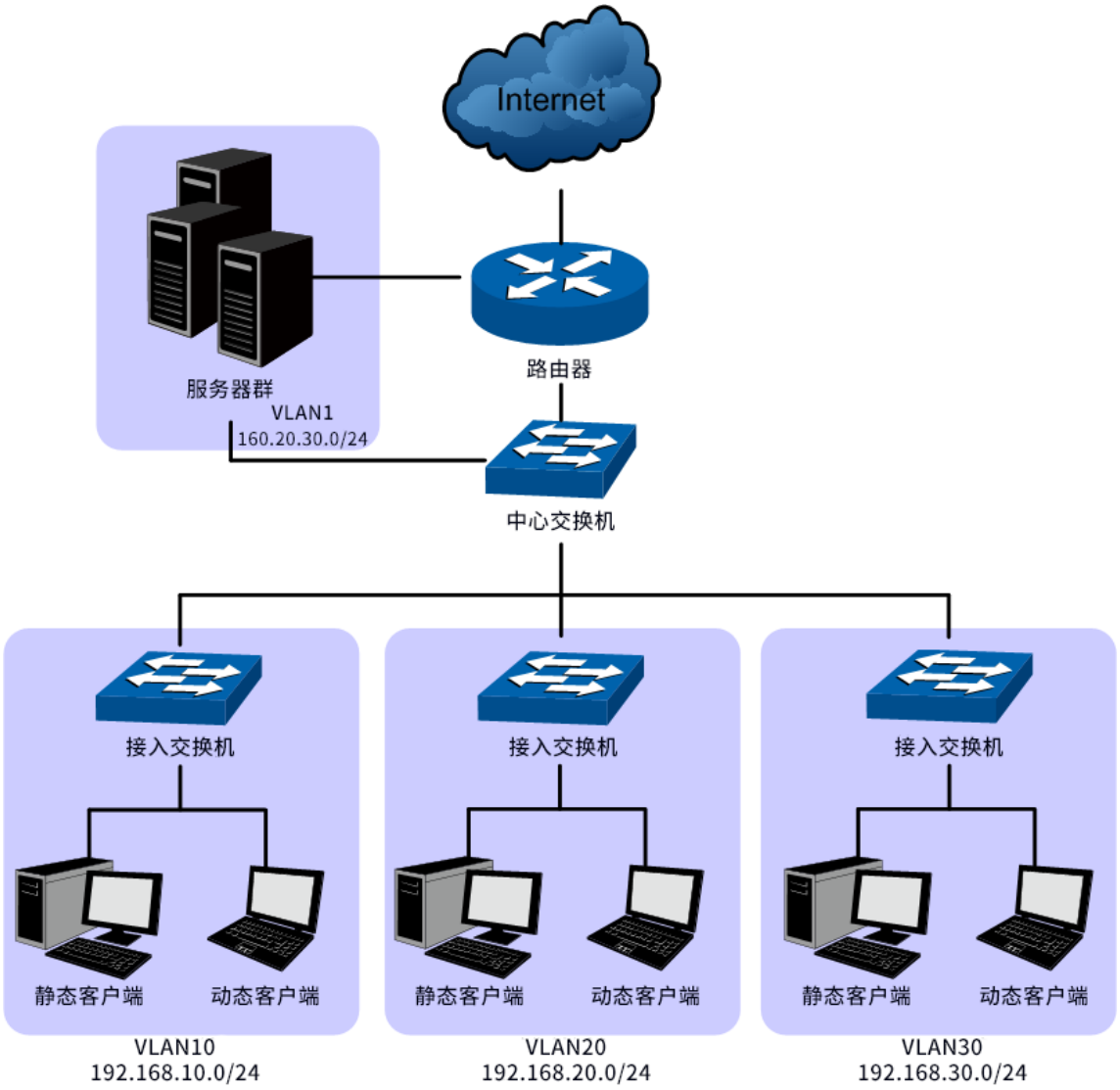
3) 创建动态分配地址池，网络中的设备申请 IP 地址时，可以获得相应接口地址池中的空闲地址。

6.6.2 DHCP 服务器配置实例

网络需求：

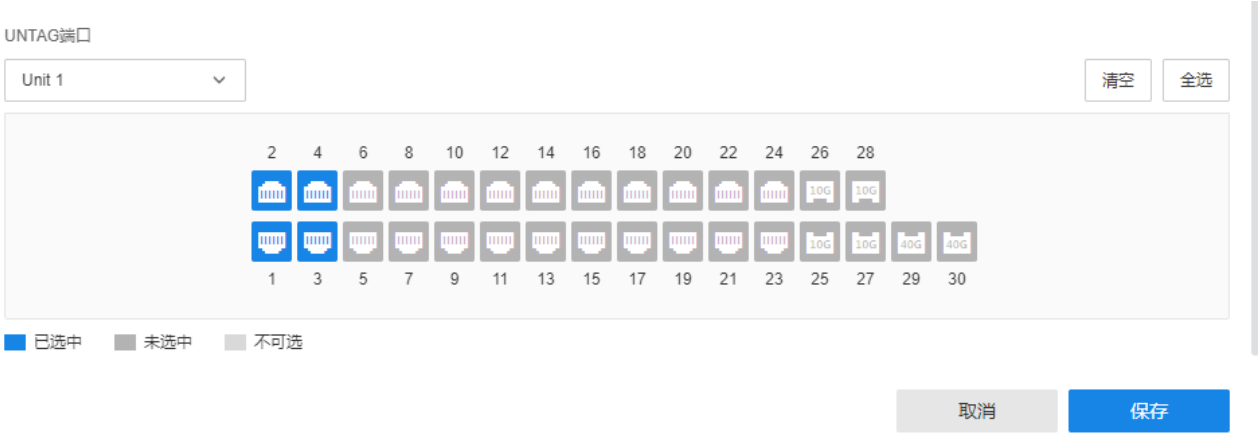
- 将校园中每一栋楼划分独立的 VLAN，并属于不同的 IP 网段；
- 每一栋楼中的接入点分成两部分，一部分是办公室，配有固定计算机，采用静态 IP 地址；另一部分是教室，多为笔记本电脑接入，采用动态 IP 地址，需要从网络中的 DHCP 服务器上获取 IP 地址；
- DNS 服务器位于 VLAN 1 中，IP 为 160.20.30.2，连接中心交换机的接口 13。

组网拓扑：



中心交换机采用本设备，并启用 DHCP 服务器为网络中的设备分配 IP 地址，配置步骤如下：

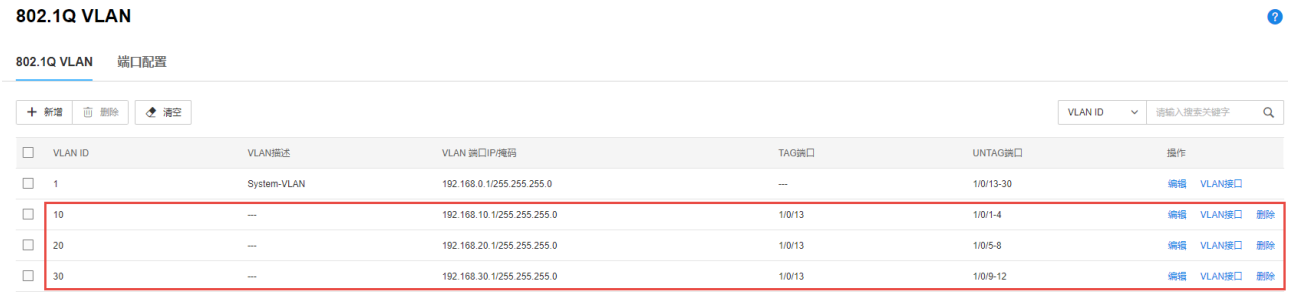
1. 创建 VLAN10、VLAN20、VLAN30，进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，点击<新增>，创建 VLAN10，配置 UNTAG 端口 1-4。



同理，创建 VLAN20，配置 UNTAG 端口 5-8，创建 VLAN30，配置 UNTAG 端口 9-12。

进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1/0/13，点击编辑，选择端口类型为 GENERAL，设置 Tag VLAN 为 10，20，30，点击<保存>。

VLAN 配置完成后如下：



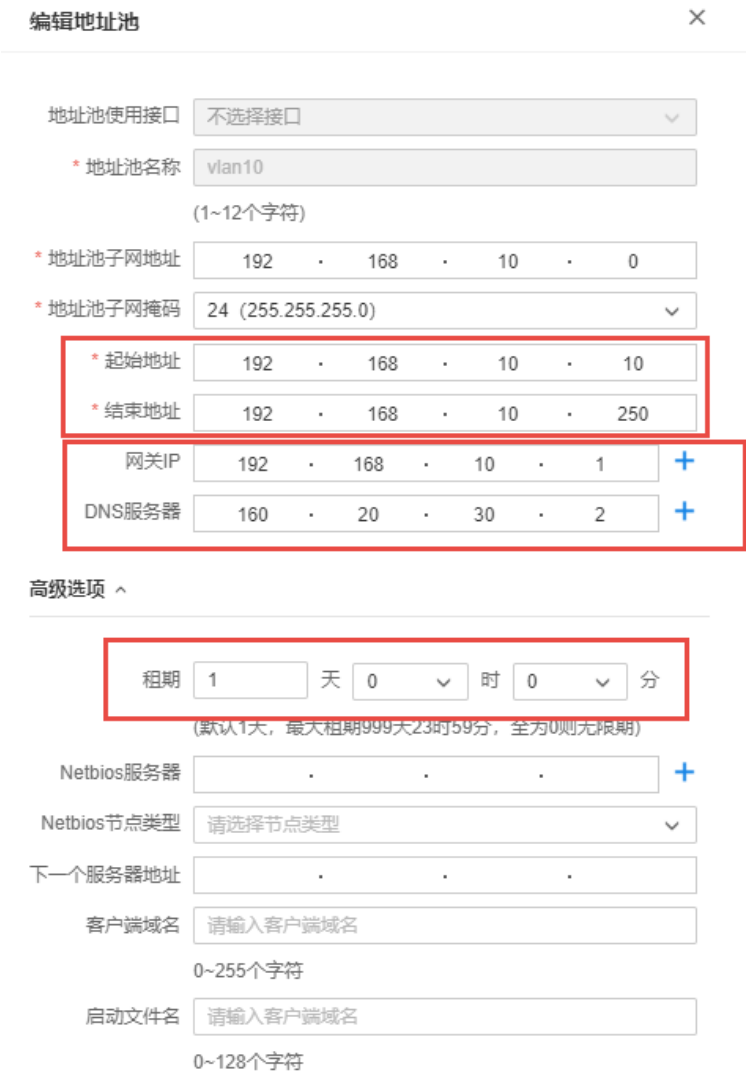
2. 创建 VLAN 接口，进入页面：网络管理 >> 接口配置，点击<新增>，选择 VLAN 接口，设置接口 ID 为 10，设置静态 IP：192.168.10.1/24.

同理，创建接口 VLAN20，配置静态 IP192.168.20.1/24，创建接口 VLAN30，配置静态 IP192.168.30.1/24，配置完成如下：

3. 启用 DHCP 服务器功能，进入页面：网络管理 >> DHCP >> DHCP 服务器，全局开启 DHCP 服务器功能。

4. 为各 VLAN 接口配置 IP 地址池，进入页面：网络管理 >> DHCP >> DHCP 服务器 >> 地址池设置，选择 VLAN10 接口，点击<编辑>。

配置 VLAN10 的地址池参数，设置地址池开始地址和结束地址，设置网关为 192.168.10.1，设置 DNS 服务器为 160.20.30.2，并设置租约，设置完成后，点击<保存>。



同理，为 VLAN20 和 VLAN30 配置地址池。

6.7 DHCP 中继

6.7.1 应用介绍

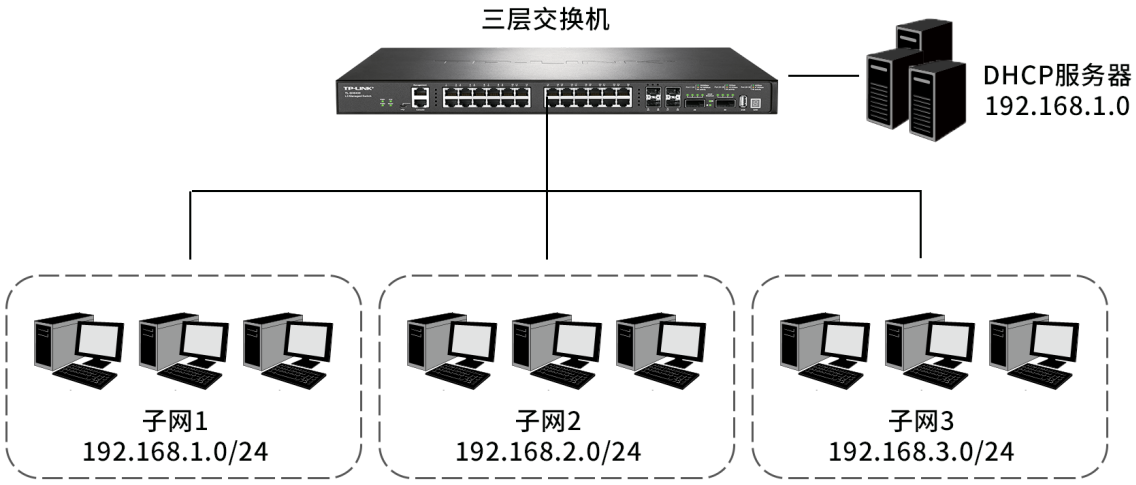
在大型的网络中，可能会存在多个子网。DHCP 客户端通过网络广播消息获得 DHCP 服务器的响应后得到 IP 地址。但广播消息是不能跨越子网的。因此，如果 DHCP 客户端和服务器在不同的子网内，客户端

还能不能向服务器申请 IP 地址呢？这就需要用到 DHCP 中继功能。DHCP 中继功能，承担不同子网间 DHCP 客户端和服务器的通信任务。

6.7.2 DHCP 中继配置实例

需求介绍：

某企业使用三层交换机划分多个子网，同时装有一台专用的 DHCP 服务器。三层交换机上不配置 DHCP 服务器，各个子网都由专用的 DHCP 服务器分配 IP 地址。



配置步骤：

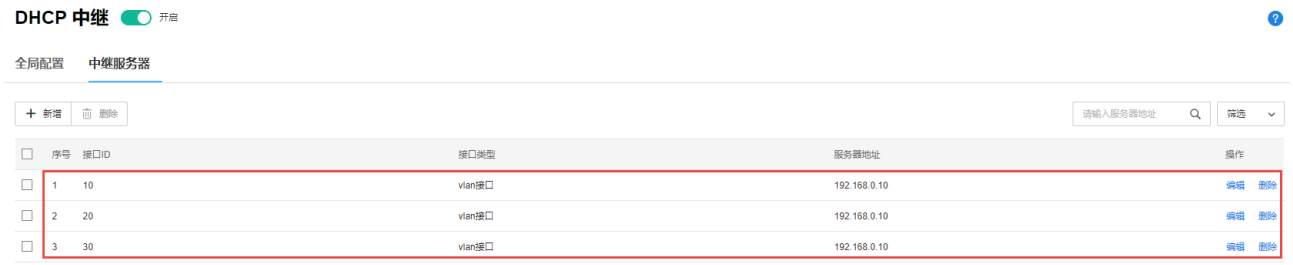
1. 启用 DHCP 中继功能，进入页面：网络管理 >> DHCP >> DHCP 中继，开启 DHCP 中继功能。

说明：

Option 82 配置需要根据实际需求确认是否开启。Option 82 一般在 802.1X 认证等应用中会使用到。

2. 添加 DHCP 中继服务器地址，进入页面：网络管理 >> DHCP >> DHCP 中继 >> 中继服务器，点击<新增>，添加通过服务器分配地址的 VLAN 信息。

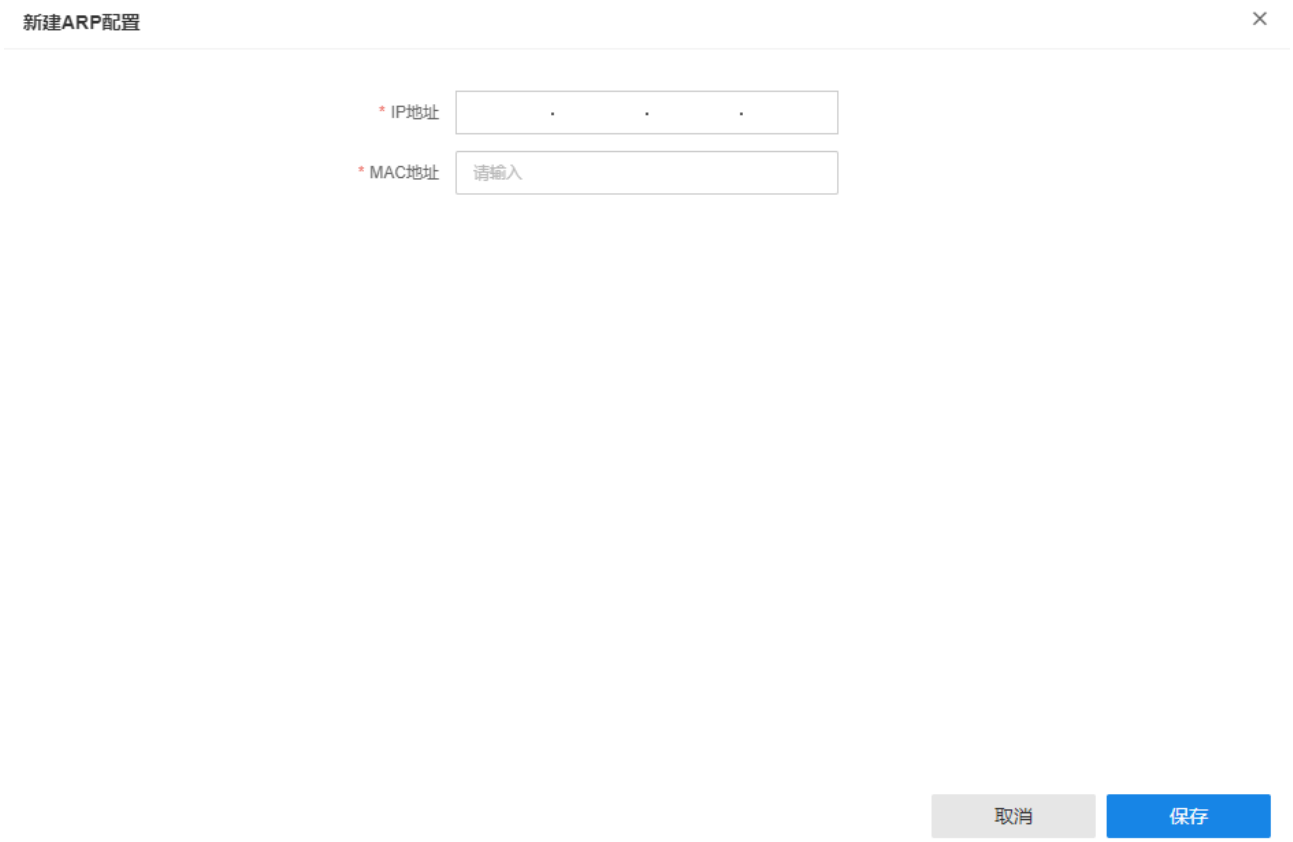
VLAN10\VLAN20\VLAN30 添加 DHCP 中继服务器后如下：



6.8 ARP 功能

6.8.1 添加静态 ARP

进入页面：网络管理 >> ARP 功能 >>ARP>> 静态 ARP，点击<新增>，输入 IP 地址和 MAC 地址，点击<保存>即可。



进入页面：网络管理 >> ARP 功能 >> ARP >> ARP 列表，可查看当前已有的 ARP 列表。

6.8.2 代理 ARP 配置实例

代理 ARP 是 ARP 协议的一种应用。通常应用于网关在连接不同网络时，为不同网络中的计算机提供 ARP 代理服务。网关收到源计算机向目标网络计算机发送的 ARP 请求时，使用自己的 MAC 地址与目标计算机的 IP 地址对源计算机进行 ARP 应答，使得不同网络中的计算机能够正常通信而不必关心网络的划分。

代理 ARP 多应用于下列两种环境：

1) 当不同网络中没有配置缺省网关的计算机要和其他网络中的计算机实现通信，其通过发送的 ARP 请求报文来试图通信，而网关在收到该 ARP 请求报文时，其代理 ARP 机制将代替目标计算机进行 ARP 应答，并为两个网络转发通信报文。

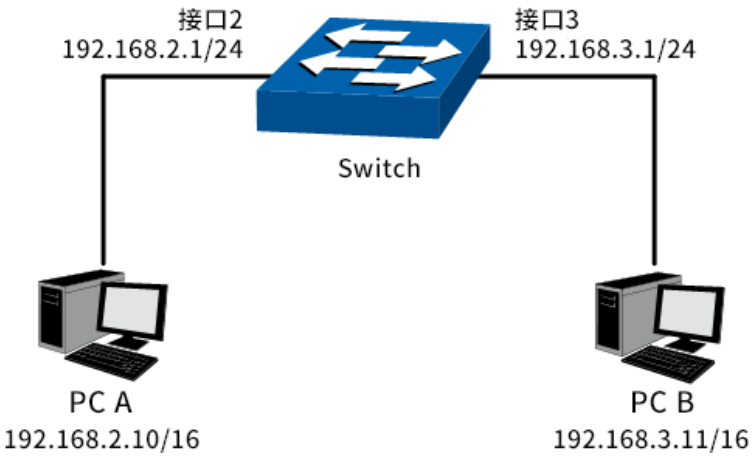
2) 当对网络进行 VLSM 子网划分时，可通过在网关上配置 ARP 代理，使得网络中计算机原有网络参数配置不做相应变更也可以进行通信。

组网需求：

1. PC A 和 PC B 在同一网段，PC A 的 IP 地址为 192.168.2.10/16，PC B 的 IP 地址为 192.168.3.11/16。
2. PC A 和 PC B 分别属于不同的子网 VLAN2 和 VLAN3。
3. 通过开启接口 2（192.168.2.1/24）和接口 3（192.168.3.1/24）的代理 ARP 功能实现 A、B 之间的通

信。

拓扑如下：

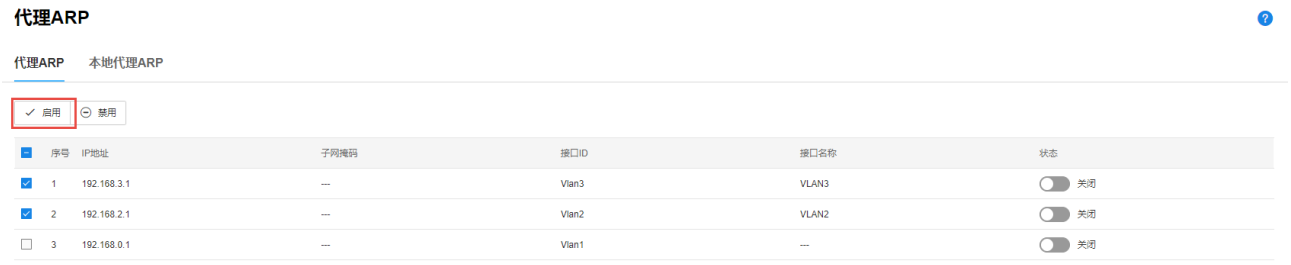


配置步骤：

1. 创建 VLAN，进入页面：网络管理 >> VLAN >>802.1Q VLAN >> 802.1Q VLAN，点击<新增>，创建 VLAN 2 和 VLAN 3。
2. 创建接口，进入页面：网络管理 >> 接口配置，点击<新增>，创建 VLAN 接口 2，接口 ID 为 2，配置 IP 地址 192.168.2.1。

同理，创建 VLAN 接口 3，接口 ID 为 3，配置静态 IP 地址 192.168.3.1。

3. 开启代理 ARP 功能，进入页面：网络管理 >> ARP 功能 >> ARP >> 代理 ARP，启用接口 2 和接口 3 的代理 ARP 功能。



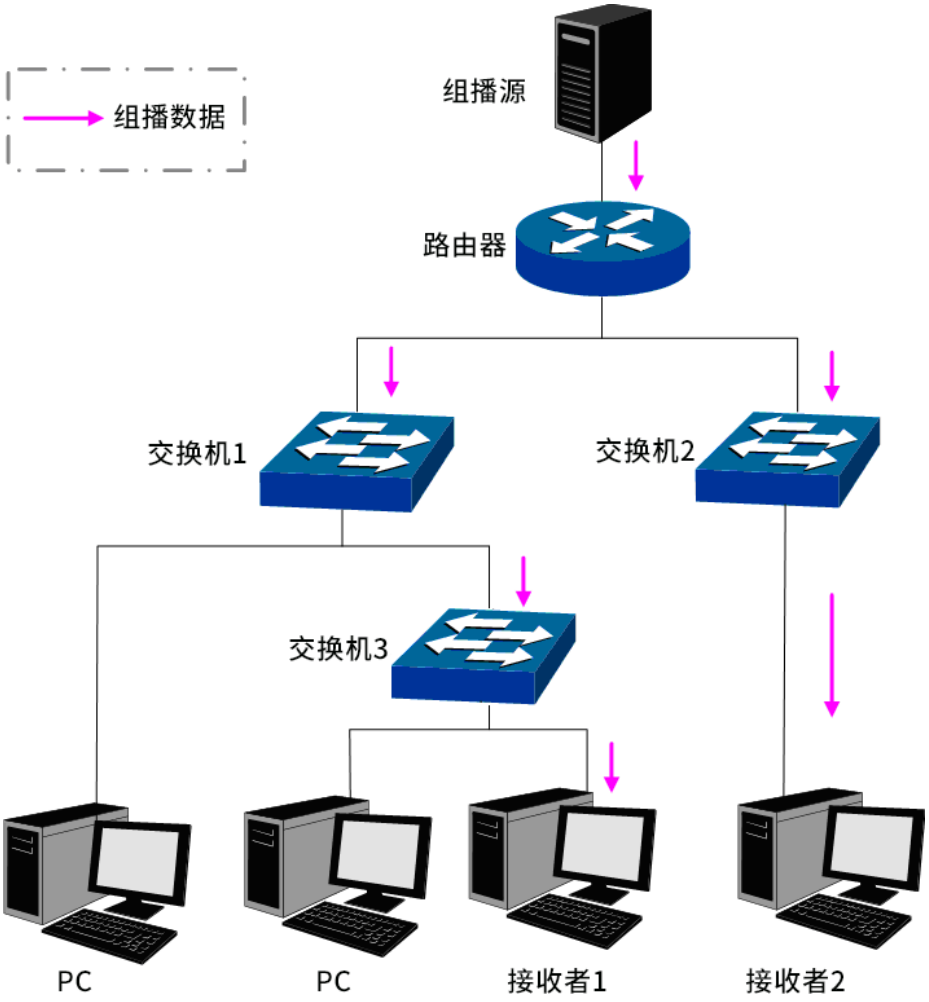
回目录

第7章　组播管理

➢ 组播概述

在网络中，存在着三种发送报文的方式：单播、广播、组播。数据采用单播（Unicast）方式传输时，服务器会为每一个接收者单独传输一份信息，如果有多个接收者存在，网络上就会重复地传输多份相同内容的信息，这样将会大量占用网络资源。数据采用广播（Broadcast）方式传输时，系统会把信息一次性的传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。

当前，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（multicast）应运而生，它实现了网络中单点到多点的高效数据传送，能够节约大量网络带宽，降低网络负载。组播传输信息的方式如下图所示。



7.1 IGMP 侦听

7.1.1 应用介绍

在很多网络环境中需要用到组播来传递数据，由于交换机默认转发本 VLAN 中的组播报文，所以不加以限制的话，会造成交换机被占用过多资源、端口几乎全部用来转发组播数据，带宽浪费严重。为了合理的转发组播数据，节省资源，提高终端的上网体验，可以通过设置 IGMP 侦听并选择丢弃未知组播报文来解决。设置之后该端口只有加入到这个组播组中，才会收到组播数据，不加入的话该组播组的组播报文被该端口认定为未知组播报文，并进行丢弃，这样这个端口是不会收到组播数据的。这样设置能有效节约带宽和交换机的性能，同时也方便对组播成员进行管理，合理的设置组播业务。

网络中的主机通过发送 IGMP（Internet Group Management Protocol，互联网组管理协议）报文向临近的路由器申请加入（或离开）组播组，当上层路由设备将组播数据转发下来后，交换机负责将组播数据转发给主机。IGMP 侦听（IGMP Snooping）是组播约束机制，运行 IGMP 侦听的交换机通过侦听和分析主机与组播路由器之间交互的 IGMP 报文来管理和控制组播组，从而可以有效抑制组播数据在网络中扩散。

- **IGMP 侦听的工作过程**

交换机侦听用户主机与路由器之间的交互 IGMP 报文，跟踪组播信息及其申请的端口。当交换机侦听到主机向路由器发出报告报文（IGMP Report）时，交换机便把该端口加入组播地址表中；当交换机侦听到主机发送的离开报文（IGMP Leave）时，路由器会发送该端口的特定组查询报文（Group-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若路由器收不到任何主机的回应，交换机便把该端口从组播地址表中删除。路由器会定时发查询报文（IGMP Query），交换机收到查询报文后，如果在一定的时间段内没有收到主机的报告报文，便把该端口从组播表中删除。

- **IGMP 报文**

运行了 IGMP 侦听的交换机对不同类型的 IGMP 报文的处理方法如下。

1. 查询报文（IGMP Query）

由路由器发出，又可分为通用查询报文和特定组查询报文。路由器定时发出通用查询报文，以查询该网段有哪些组播组的成员。当路由器收到 IGMP 离开报文后，会通过接收端口向该组播组发送 IGMP 特定组查询报文，交换机会将此报文转发，以确定该端口中是否还有组播组的其它组成员。

对于通用查询报文，交换机会将此报文通过 VLAN 内除接收端口以外的其它端口转发，并对接收端口做出相应的处理：如果接收端口不是已有路由器端口，则将其加入路由器端口列表，并启用路由器端口时间；如果是已有路由器端口，则直接重置路由器端口时间。

对于特定组查询报文，交换机要向被查询的组播组的成员转发 IGMP 特定组查询报文。

2. 报告报文（IGMP Report）

由主机发出，当主机想主动加入某一组播组或对路由器查询报文给予响应时产生此种报文。

在收到 IGMP 报告报文时，交换机将此报文通过 VLAN 内的路由器端口转发出去，同时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相应的处理：如果接收端口是新成员端口，则将其加入到组播地址表中，并启用该端口的成员端口时间；如果接收端口是旧成员端口，则直接重置成员端口时间。

3. 离开报文（IGMP Leave）

运行 IGMPv1 的主机离开组播组时不会发送 IGMP 离开报文，因此交换机无法立即获知主机离开的信息。但是，由于主机离开组播组后不会再发送 IGMP 报告报文，因此当其对应的成员端口时间超时后，交换机就会将该端口从相应的组播地址表中删除。运行 IGMPv2 或 IGMPv3 的主机离开组播组时，会通过发送 IGMP 离开报文，以通知组播路由器自己离开了某个组播组。

当交换机从某一端口收到 IGMP 离开报文时，为了确认此端口下是否还有其它组成员存在，交换机向此端口转发特定组查询报文，然后重置成员端口时间为离开滞后时间，离开滞后时间超时后，交换机将此端口从相应的组播地址表中删除。如果删除离开端口后组播组中没有其它组成员存在，则将整个组播组删除。

- **IGMP 侦听的基本概念**

1. 相关端口

路由器端口（Router Port）：交换机上连接路由组播设备的端口。

成员端口（Member Port）：交换机上连接组播组成员的端口。

2. 相关定时器

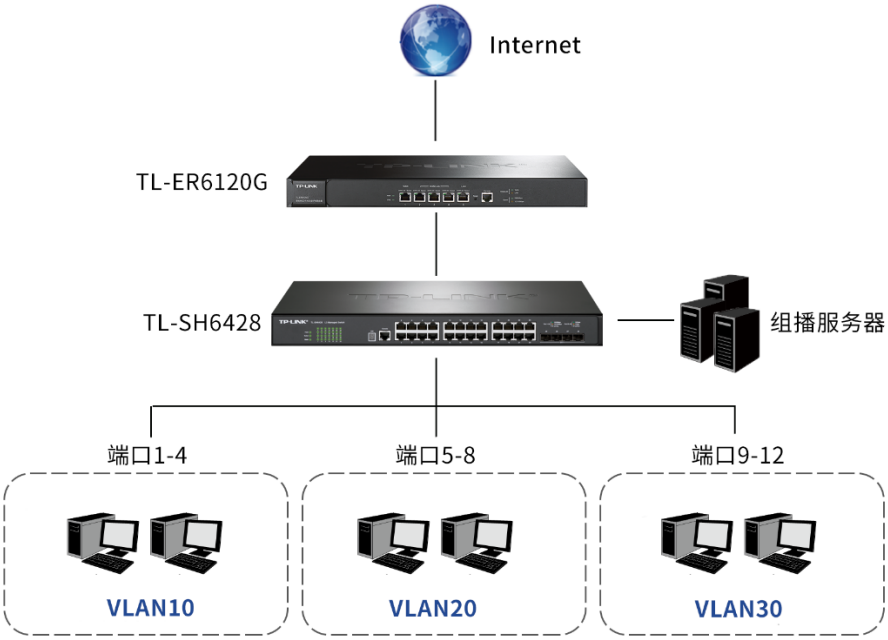
路由器端口时间：这段时间内，如果交换机没从路由器端口接收到查询报文，就认为该路由器端口失效。默认是 300 秒。

成员端口时间：这段时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口不再有主机属于多播组。默认是 260 秒。

离开滞后时间：从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。默认是 1 秒。

7.1.2 IGMP 侦听配置实例

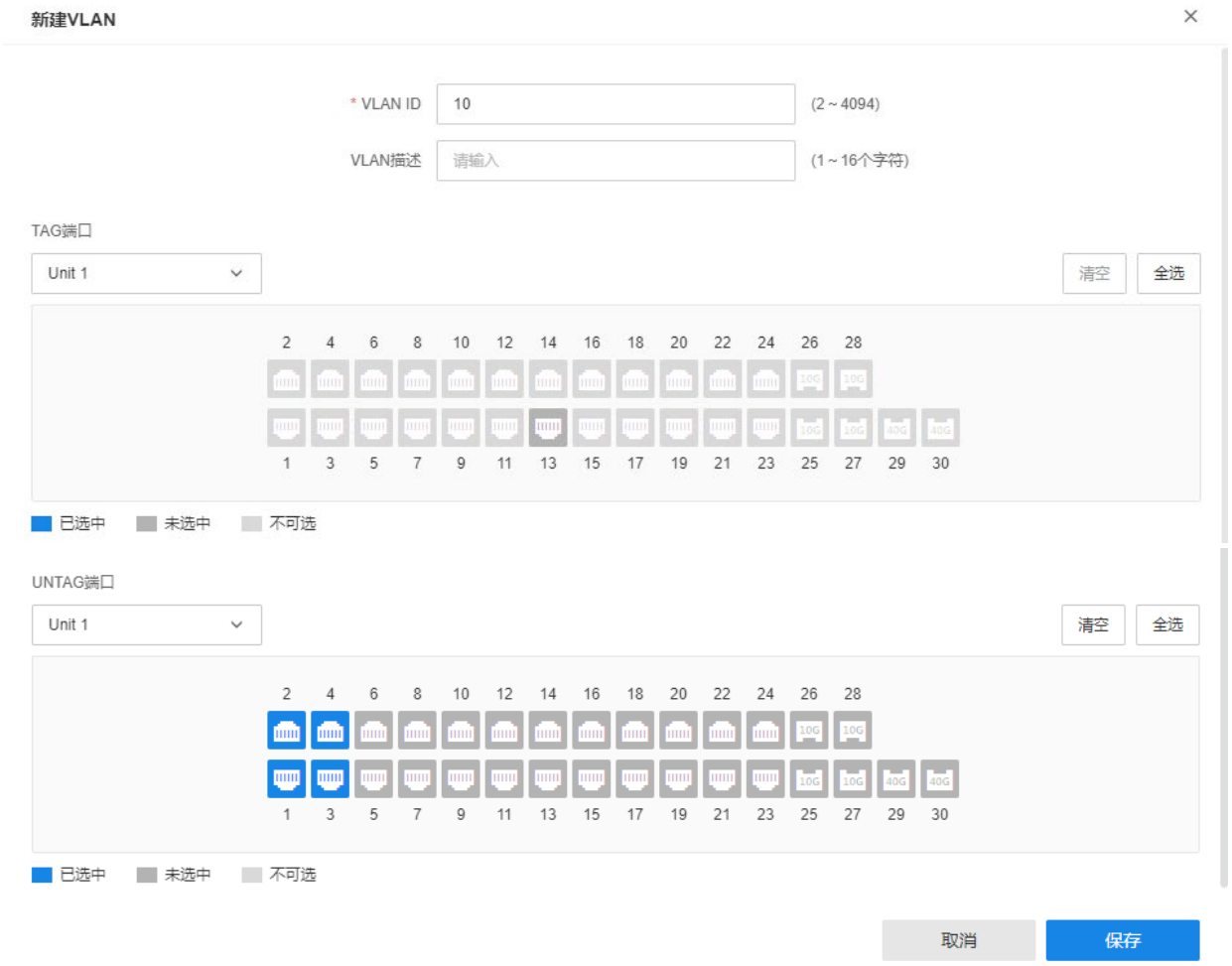
某企业通过三层交换机划分了 3 个业务 VLAN，分别是 VLAN 10、20、30,这三个业务部门都需要收到来自公司组播服务器的组播业务数据，但是为了节约交换机资源需要设置 IGMP 侦听来控制哪些需要端口需要转发这份数据，网络拓扑如下：



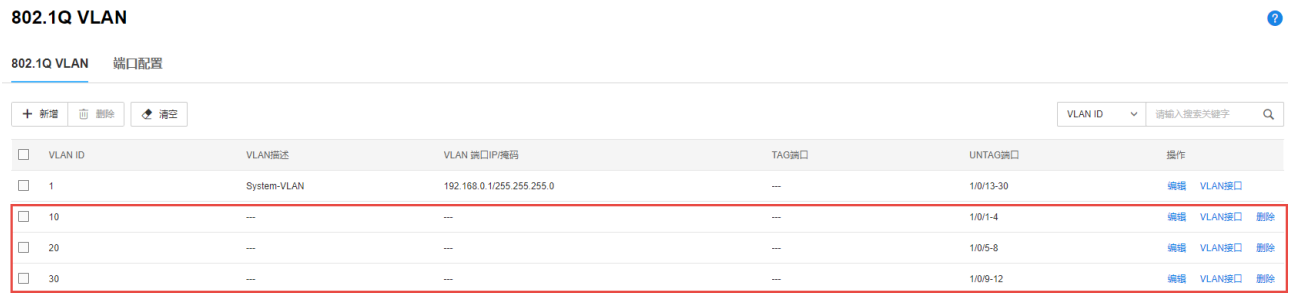
配置步骤：

首先设置 VLAN10\20\30，组播数据使用 VLAN40。

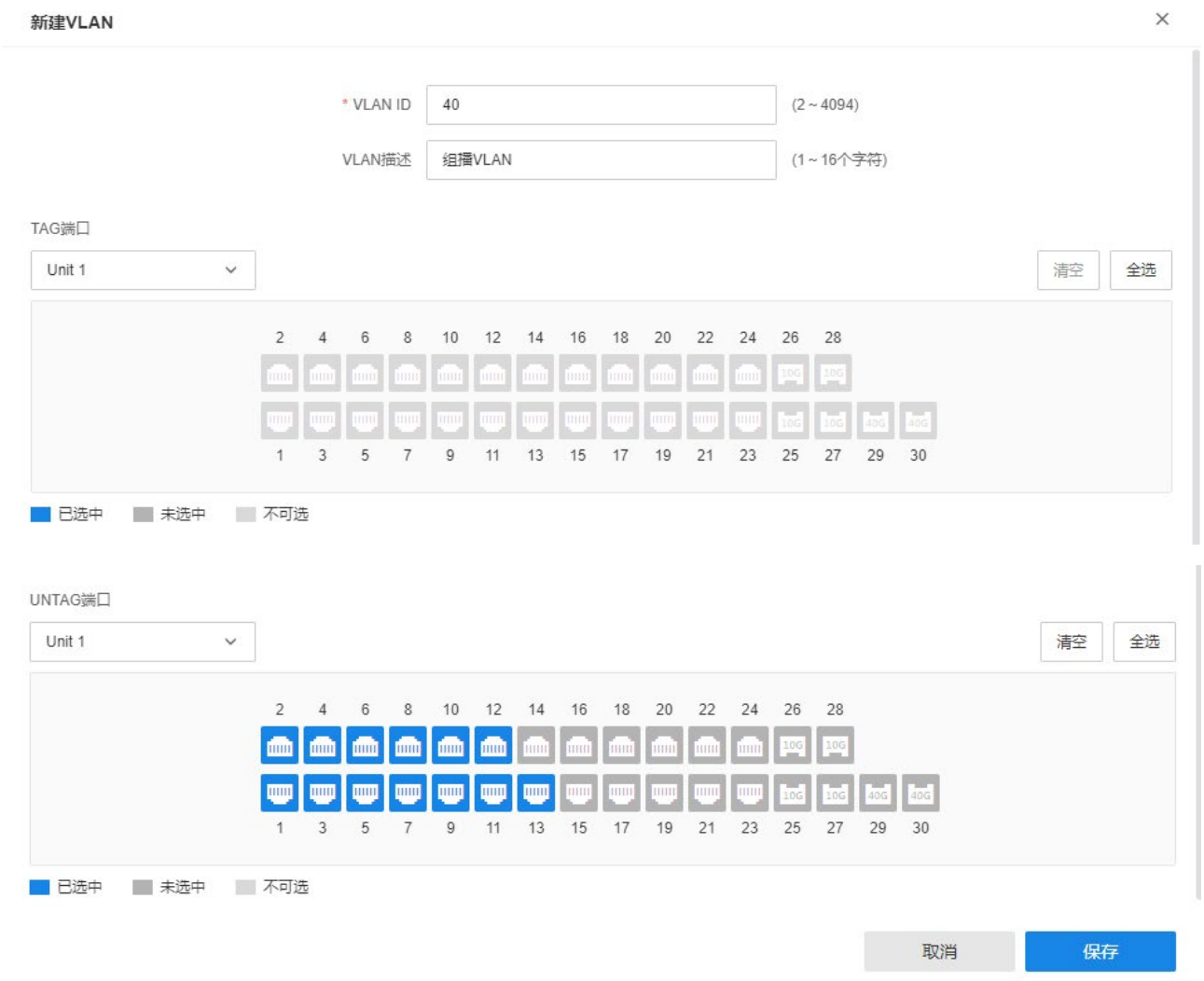
1. 进入页面：网络管理 >> VLAN >>802.1Q VLAN >> 802.1Q VLAN，点击<新增>，创建 VLAN10，包含 untag 端口 1-4。



同理，创建 VLAN20，包含 untag 端口 5-8；创建 VLAN30，包含 untag 端口 9-12。创建完成如下：

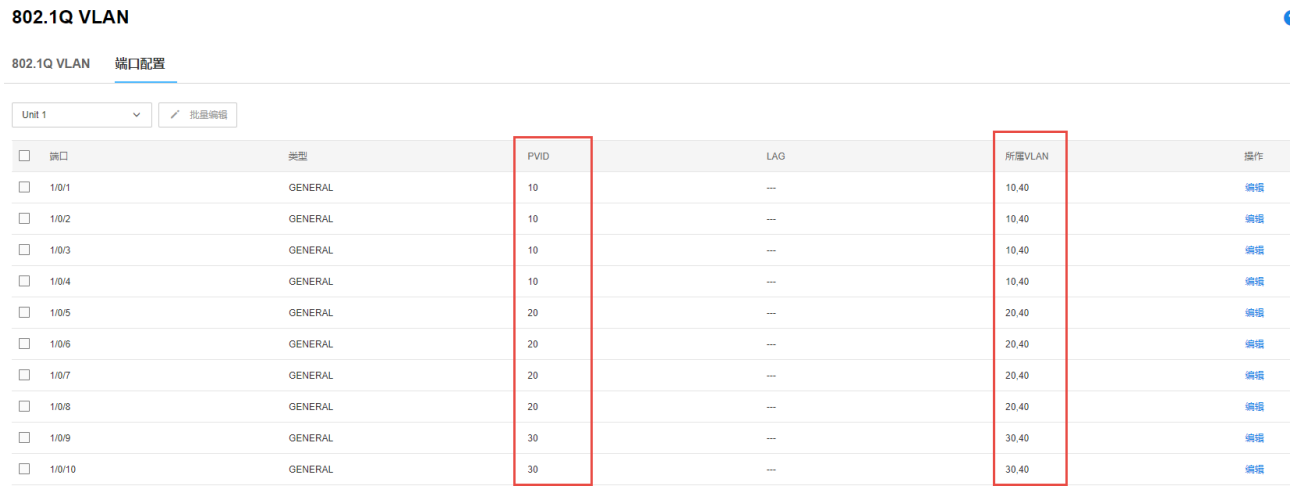


2. 新建一个 VLAN40 用于在该 VLAN 传输组播数据，保证组播数据只会在该 VLAN 中转发，不会影响的其他的 VLAN 和端口，节约交换机的资源，提高带宽利用率。进入页面：网络管理 >> VLAN >>802.1Q VLAN >> 802.1Q VLAN，点击<新增>，创建 VLAN40，需要用到组播业务的端口添加到该 VLAN 中，端口带不带 tag 视具体网络环境而定，成员端口的类型不会影响到正常的组播转发，本次设置选择 untagged 接口，新建组播 VLAN 40 包含 1-13 端口，且皆为 untag，13 端口接组播服务器，PVID 设置为 40。



3. 对于组播 VLAN 所在的端口，组播源端口（本例是 13 号端口）即发送组播数据的端口，其 PVID 要设置成组播 VLAN 的 ID（本例是 VLAN40），保证组播数据进来的时候是在组播 VLAN 中的； 而其他成员端口 1-12 端口，即需要接收组播数据的端口，PVID 仍为之前所在 VLAN 的 ID，也就是说这些端口原有的配置和业务不会受到影响。进入页面：网络管理 >>VLAN>>802.1Q VLAN>> 端口配置，端口 1-13 为 general 端口，设置端口 1-4 的 PVID 为 10，端口 5-8 的 PVID 为 20，端口 9-12 的 PVID 为 30，端口 13 的 PVID 设置为 40。

配置完成如下：

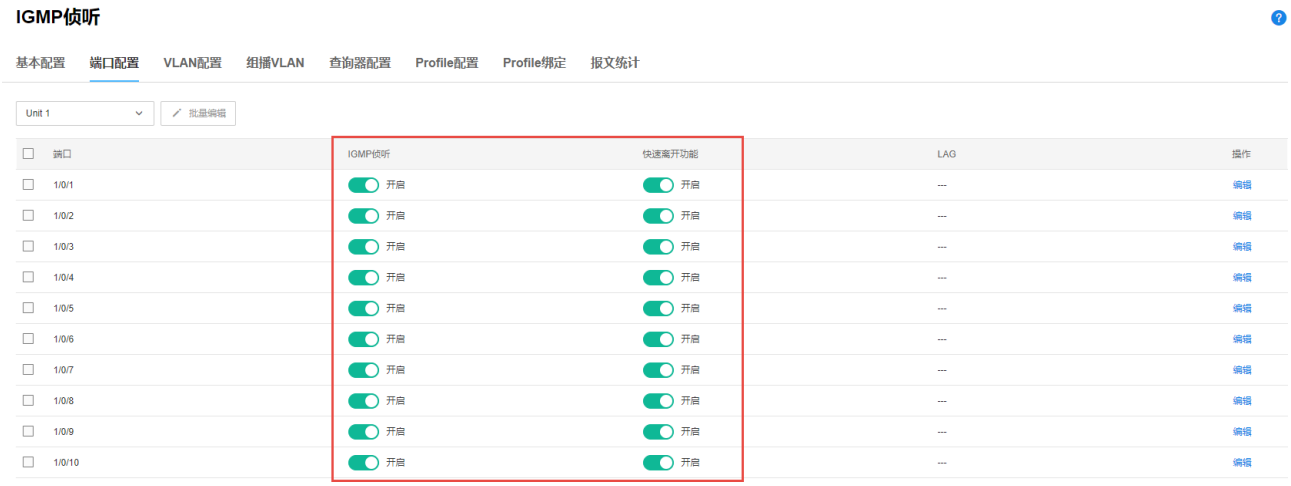


其次，开启 IGMP 侦听和 MLB 侦听。

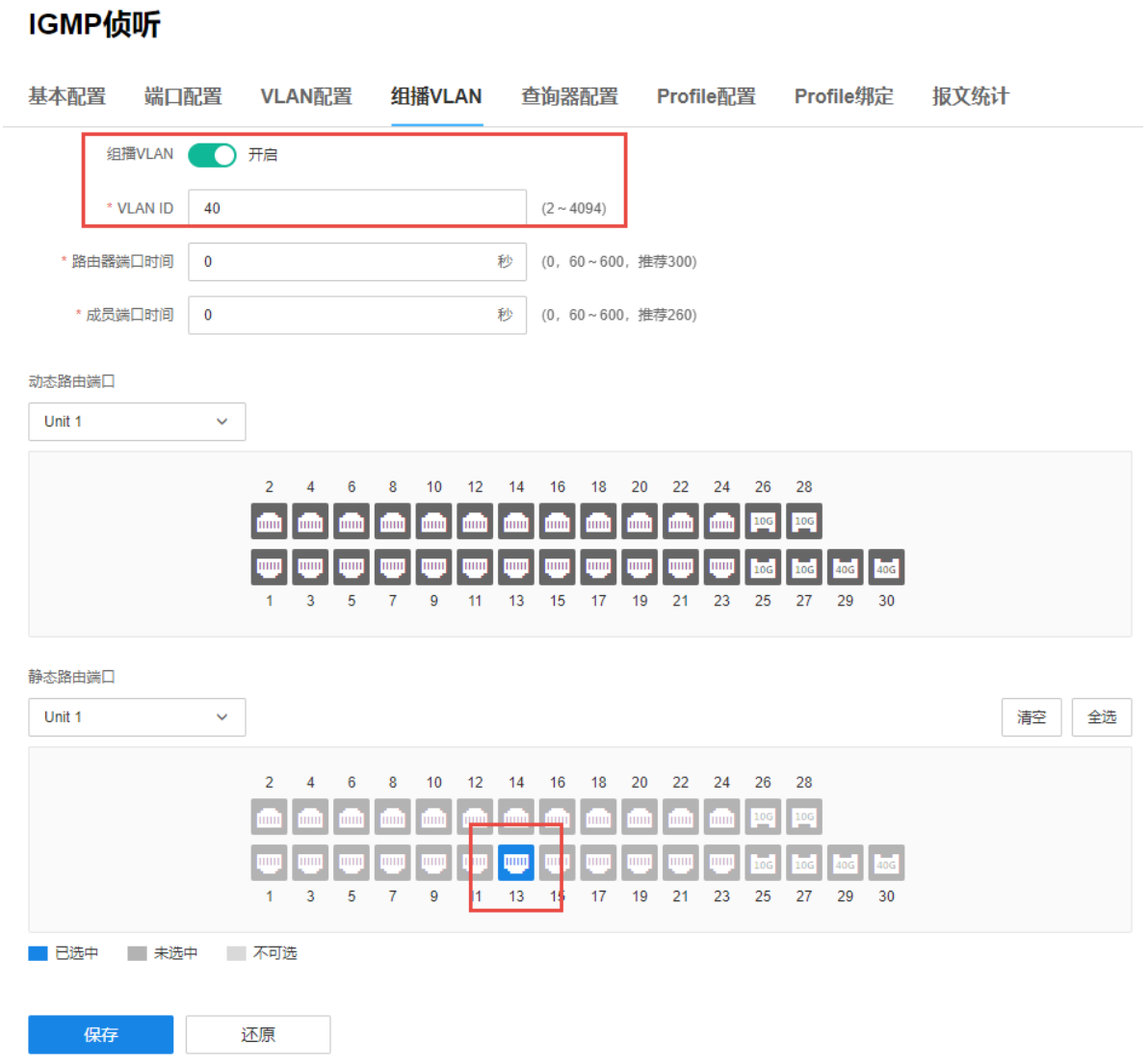
4. 进入页面：网络管理 >> 组播管理 >> IGMP 侦听 >> 基本配置，开启 IGMP 侦听功能，选择丢弃未知组播报文，其余保持默认。

同理，进入页面：网络管理 >> 组播管理 >> MLD 侦听 >> 基本配置，开启 MLD 侦听功能，选择丢弃未知组播报文，其余保持默认。

5. 进入页面：网络管理 >> 组播管理 >> IGMP 侦听 >> 端口配置，开启端口 1-12 的 IGMP 侦听功能，时启用快速离开功能（在有多个组播组的环境下使用）。



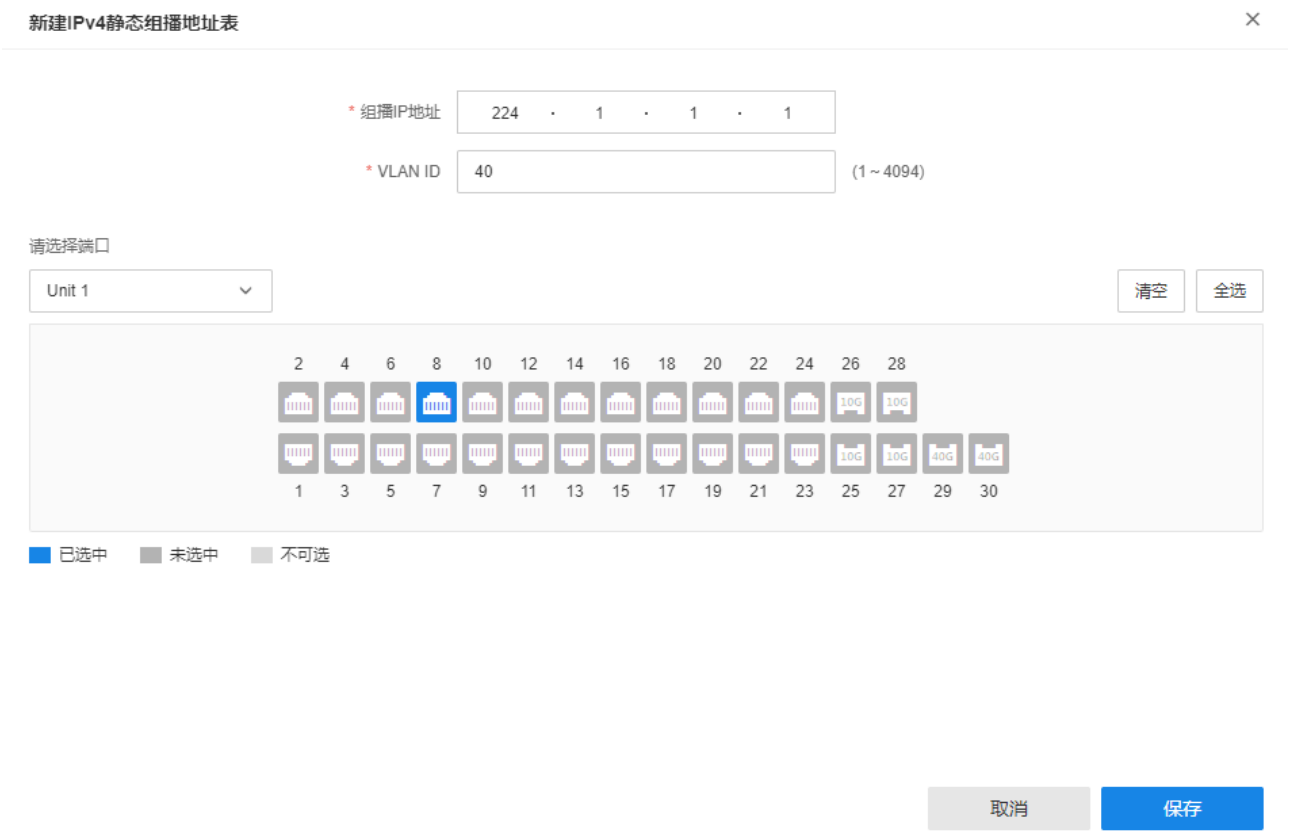
6. 进入页面：网络管理 >> 组播管理 >>IGMP 侦听 >> 组播 VLAN，启用组播 VLAN40，路由器端口时间和成员端口时间根据需要填写，一般选择推荐值。静态路由器端口也就是发送组播数据的端口，选中端口 13，配置完成后点击<保存>。



7. 设置好组播 VLAN 和 IGMP 侦听后，服务器通过交换机的 13 端口开始发送组播数据，接收端电脑连接交换机的 1-12 端口，由于未知组播报文丢弃，此时是收不到组播报文的。 当接收端电脑发送加入该组播组的声明之后，该 13 口的组播源发送的组播组数据不再被认为是未知组播报文，故可以被接收端电脑收到。

8. 对于某些特定的场所来说，接收端即组播成员端口下终端不支持标准的组播协议，是不会发出加入这个组播的通告的。由于设置了未知组播报文丢弃，所以该成员端口是不会收到未通告过的组播报文的。此时，为了保证该成员端口也能接收到组播数据，可以设置静态组播地址表。

9. 进入页面：网络管理 >> 组播管理 >> 组播地址表 >> IPv4 静态组播地址表，点击<新增>，填写需要加入的组播 IP 和组播 VLAN，转发端口选择无法发送通告报文的端口 8。



7.2 MLD 侦听

7.2.1 应用介绍

MLD Snooping（Multicast Listener Discovery Snooping，MLD 侦听）是运行在交换机上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组。启用 MLD 侦听功能可以有效地避免组播数据在网络中广播。

MLD 侦听所建立的组播组是基于 VLAN 广播域的，不同 VLAN 可以设置不同的 MLD 参数。当交换机运行了组播 VLAN，上有组播设备无需向交换机的每个 VLAN 分别发送一组组播数据，而只需向交换机的组播 VLAN 发送一份组播数据即可，这样既避免了带宽的浪费，也减轻了上游组播设备的负担。

7.2.2 MLD 侦听配置实例

组网介绍：

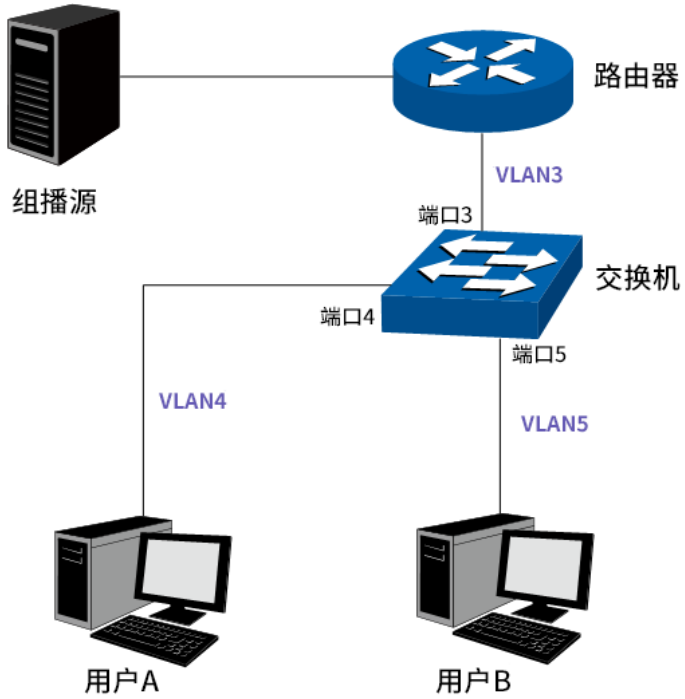
组播源通过路由器转发组播数据，组播数据流通过交换机被转发到接收端用户 A 和用户 B。

路由器 WAN 口与组播源相连；LAN 口与交换机相连，且通过 VLAN3 转发数据。

交换机端口 3 与路由器相连，且通过 VLAN3 转发数据；端口 4 与用户 A 相连，且通过 VLAN4 转发数据；端口 5 与用户 B 相连，且通过 VLAN5 转发数据。

用户 A 与交换机的端口 4 相连，用户 5 与交换机的端口 5 相连。

配置组播 VLAN 使用户 A 和用户 B 通过组播 VLAN 接收组播数据，网络拓扑图如下：



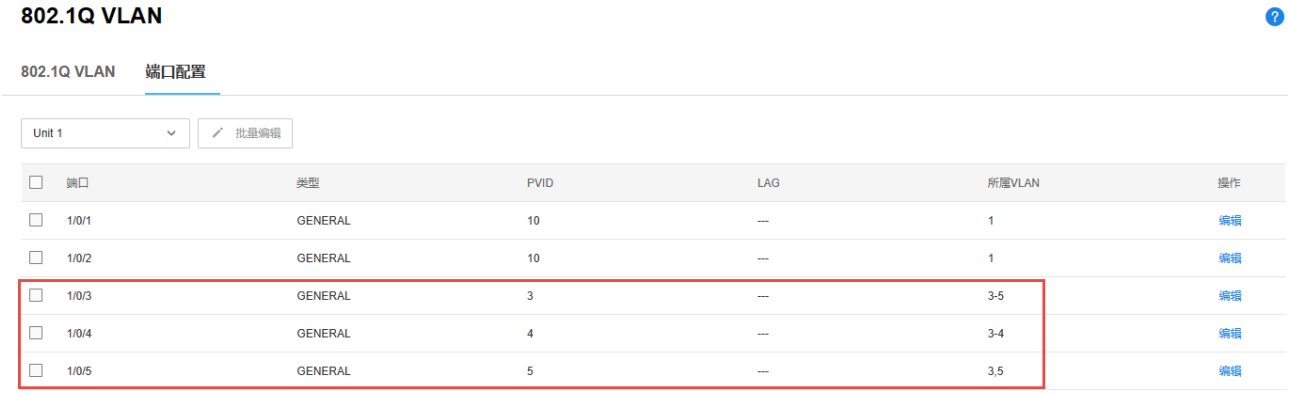
1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 802.1Q VLAN，创建 VLAN3，包含 TAG 端口 3，UNTAG 端口 4、5；创建 VLAN4，包含 UNTAG 端口 4、TAG 端口 3；创建 VLAN5，包含 UNTAG 端口 5、TAG 端口 3。

2. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，配置端口属性。

设置端口 3 的端口类型为 GENERAL，将端口 3 加入 VLAN3，4，5。

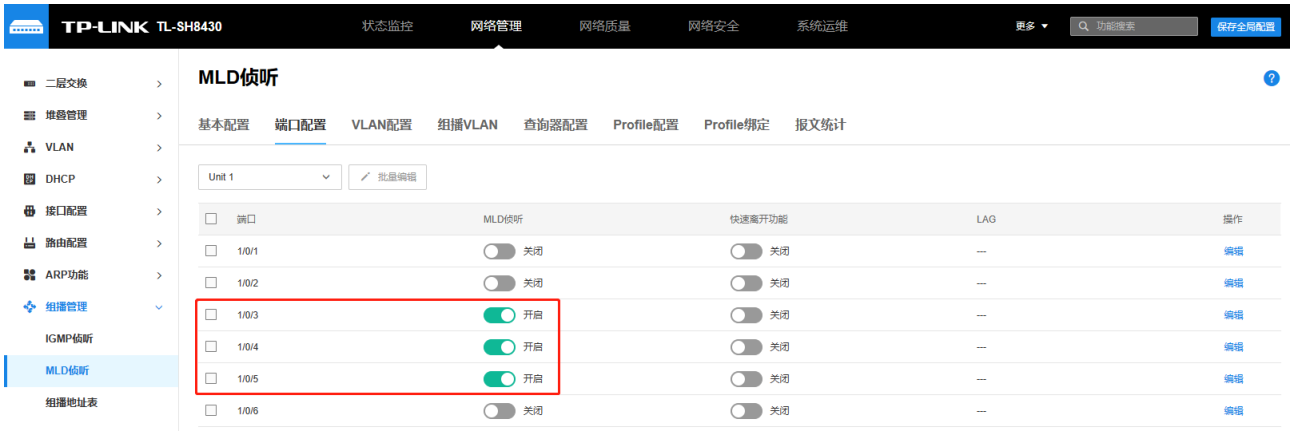
设置端口 4 的端口类型为 GENERAL，将端口 4 加入 VLAN3,4。

设置端口 5 的端口类型为 GENERAL，将端口 5 加入 VLAN3,5。

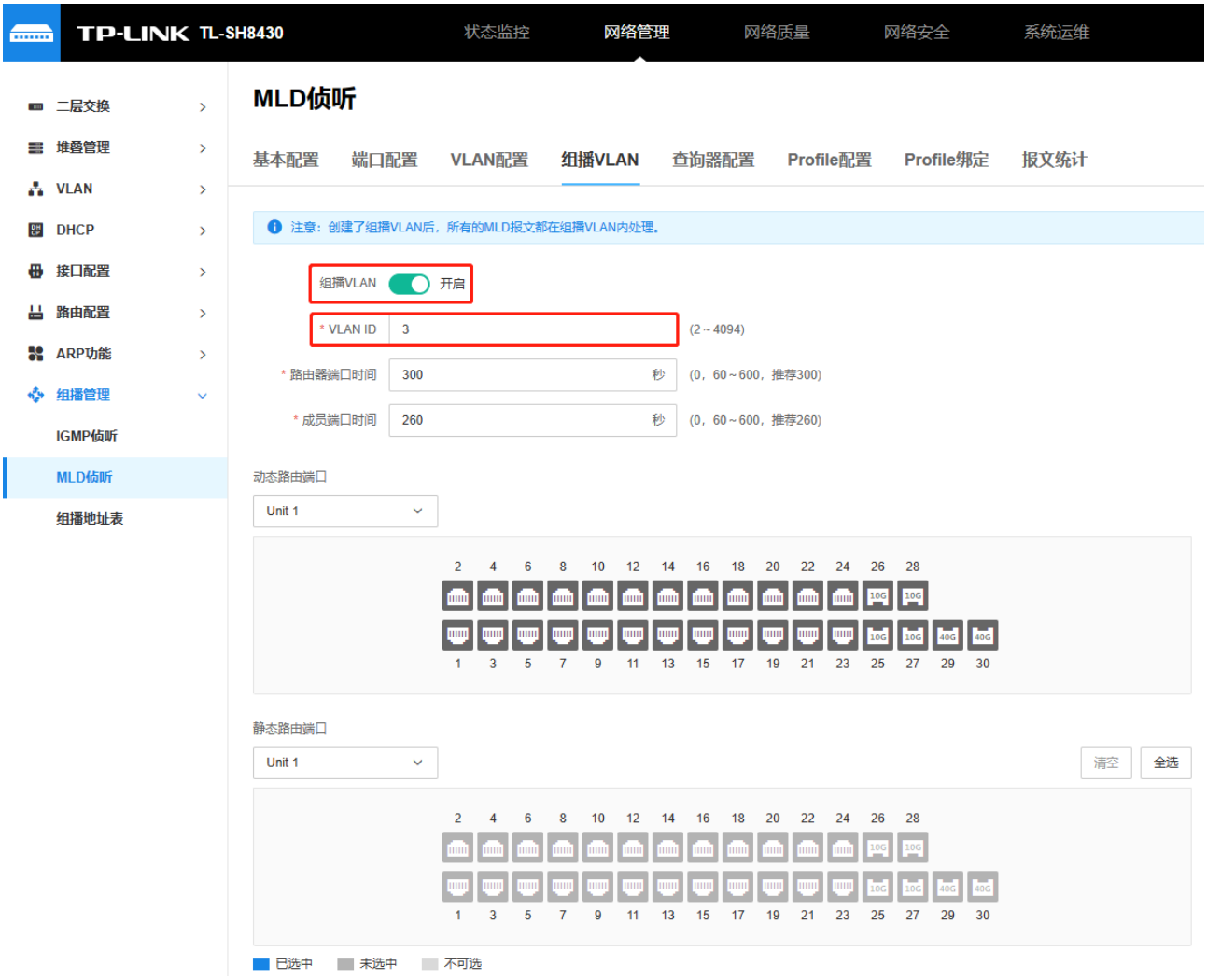


3. 进入页面：组播管理 >> MLD 侦听 >> 基本配置，启用 MLD 侦听功能。

4. 进入页面：组播管理 >> MLD 侦听 >> 端口配置，启用端口 3，4，5 的 MLD 侦听功能。



5. 进入页面：组播管理 >> MLD 侦听 >> 组播 VLAN，启用组播 VLAN，配置组播 VLAN 的 VLAN ID 为 3，其他参数建议使用默认值。



6. 检查组播 VLAN，组播管理 >> MLD 侦听 >> 基本配置，MLD 侦听信息处，已启用的端口显示为 3-5，已启用的 VLAN 显示为 3。

MLD侦听信息

刷新

描述	成员
已启用端口	1/0/3-5
已启用VLAN	3

回目录

第8章　服务质量

服务质量模块主要用于优先级配置和流量控制管理，流量控制主要是带宽流量控制和广播流量控制。针对各种网络应用的不同需求，为其提供不同的服务质量，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 QoS 配置、带宽控制和风暴抑制。

8.1　配置 QoS 优先级模式

8.1.1 QoS 三种优先级介绍

QoS(Quality of Service 即服务质量)功能用以提高网络传输的可靠性，提供高质量的网络服务体验。在传统的网络中，所有的报文都被无区别的等同对待，网络尽最大的努力（Best-Effort）发送报文，但对时延、可靠性等性能不能提供任何保证。伴随着网络技术、多媒体技术的飞速发展，IP 网在现有的 www, FTP, E-mail 等服务的基础上，越来越多承载交互式多媒体通信业务如电视会议、远程教学、视频点播、可视电话等，而每种业务要求的传输时延、可变迟延、吞吐量和丢包率都不同。因此，为用户各种业务提供不同的服务质量（QoS)成为 Internet 发展的重要挑战。

通常所说的 QoS，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，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。

云管理交换机提供基于端口的优先级、IEEE 802.1P 优先级和 DSCP 优先级三种模式。其中基于端口的优先级是默认被启用的，其它两种优先级模式可供选择。

- **基于端口的优先级**

将进入端口的数据包映射到不同的优先级。云管理交换机的端口优先级分为 4 个等级：

队列编号	优先级等级
1	最低
2	正常
3	中等
4	最高

配置方法：

进入页面：服务质量 >> QoS 配置，选择<基于端口>，勾选对应端口，选择“优先级队列“，点击<应用>。

- **基于 802.1P 的优先级**

每一个 802.1Q Tag 中都有一个 Pri 域，该域由三个 bit 为组成，取值范围是 0~7。802.1P 优先级就是根据 Pri 值来决定数据帧的优先级。

Pri 值	优先级等级
1，2	最低
0，3	正常
4，5	中等
6，7	最高

配置方法：

进入页面：服务质量 >> QoS 配置，选择<基于 802.1P>，点击<应用>。

- **基于 DSCP 优先级**

IP 报文的 DS 域包含 8bit，DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前 6 个 bit（0～5bit）表示，取值范围为 0～63，后 2 个 bit（6、7bit）是保留位。交换机发送 IP 包时，将 IP 包的 DS 域值映射到不同的优先级等级。

Pri 值	优先级等级
0-15	最低
16-31	正常
32-47	中等
48-63	最高

配置方法：

进入页面：服务质量 >> QoS 配置，选择<基于 DSCP>，点击<应用>。

注意：

当没有启用 DSCP 优先级时，交换机根据数据包是否带有 802.1Q Tag 确定使用哪种优先级模式。对于带有 Tag 的数据包，应用 802.1P 优先级；否则应用端口优先级。当启用 DSCP 优先级时，如果接收的数据包是 IP 包，则应用 DSCP 优先级；对于非 IP 包，如果数据帧带有 Tag 则应用 802.1P 优先级，否则应用端口优先级。

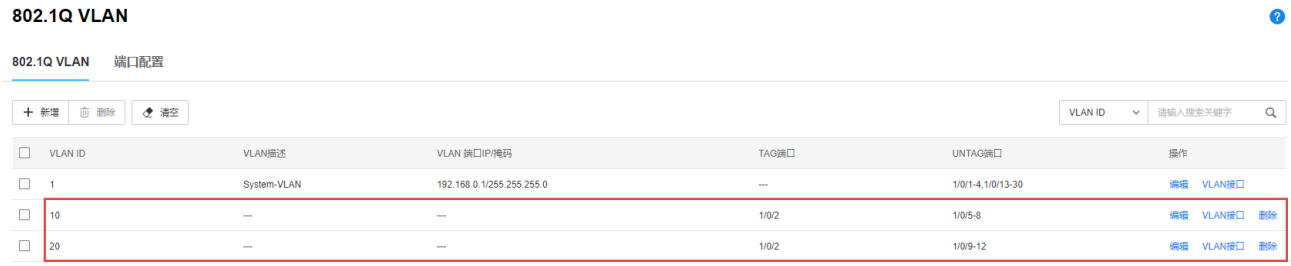
8.1.2 QoS 优先级配置实例

组网介绍：

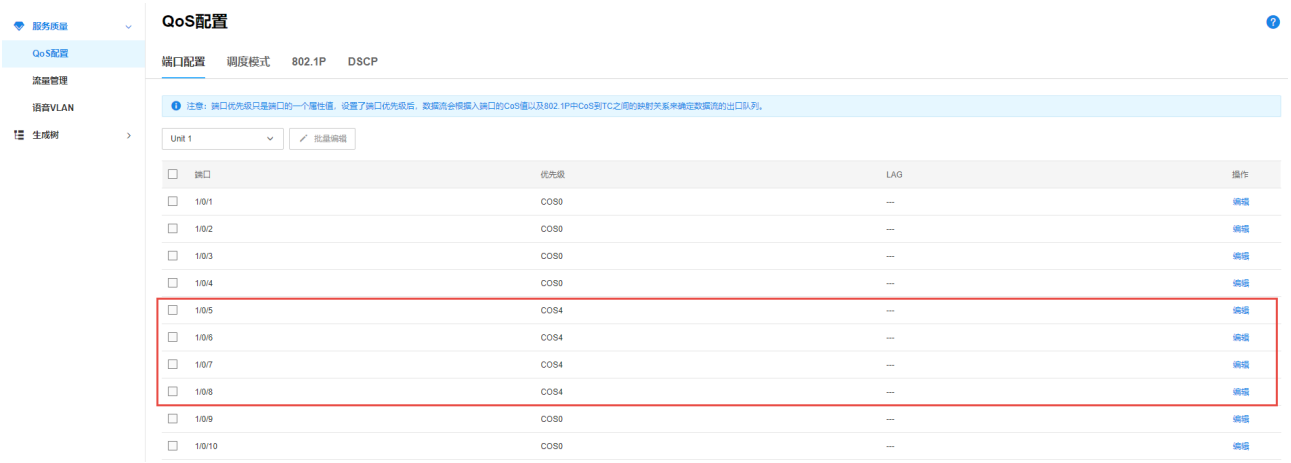
某公司的内网服务器上存在公司较多事务数据，要求管理部和研发部对内网服务器的访问优先级不同，当管理部和研发部同时访问内网服务器时，管理部数据优先研发部传输。网络拓扑如下：

配置步骤：

1. 进入页面：网络管理 >> VLAN >>802.1Q VLAN >> 802.1Q VLAN，点击<新增>，创建 VLAN10，包含 untag 端口 5-8，tag 端口 2，创建 VLAN20，包含端口 9-12，tag 端口 2。



2. 进入页面：网络质量 >> 服务质量 >>QoS 配置 >> 端口配置，设置端口优先级，端口 5-8 优先级队列值为 4，端口 9-12 优先级队列值为 2。



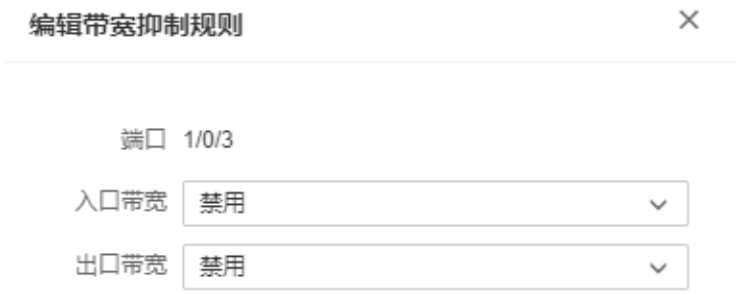
8.2 配置带宽控制功能

8.2.1 带宽控制介绍

带宽控制是通过设定端口可用带宽，来控制端口的输入/输出数据传输速率，从而合理地分配和利用网络带宽。

配置方法：

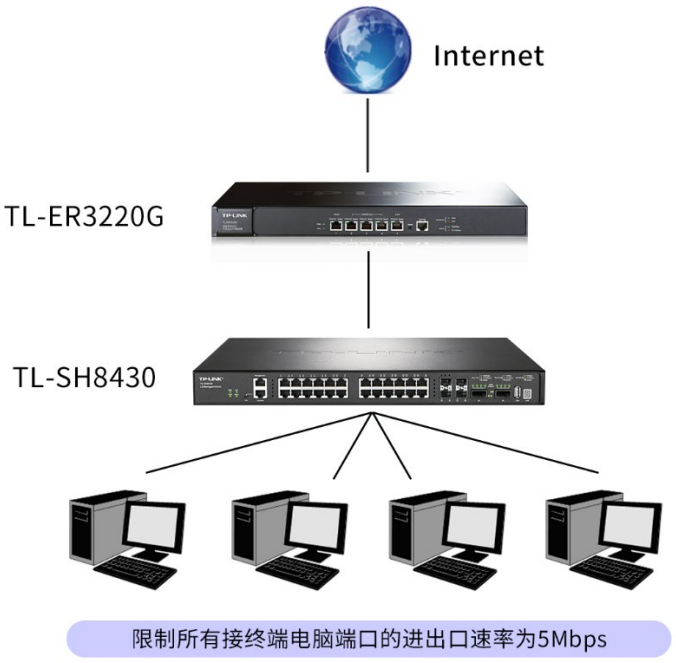
进入页面：网络质量 >> 服务质量 >> 流量管理 >> 带宽抑制，勾选对应端口，点击<编辑>，输入入口/出口限速值，点击<保存>。



8.2.2 带宽控制配置实例

组网介绍：

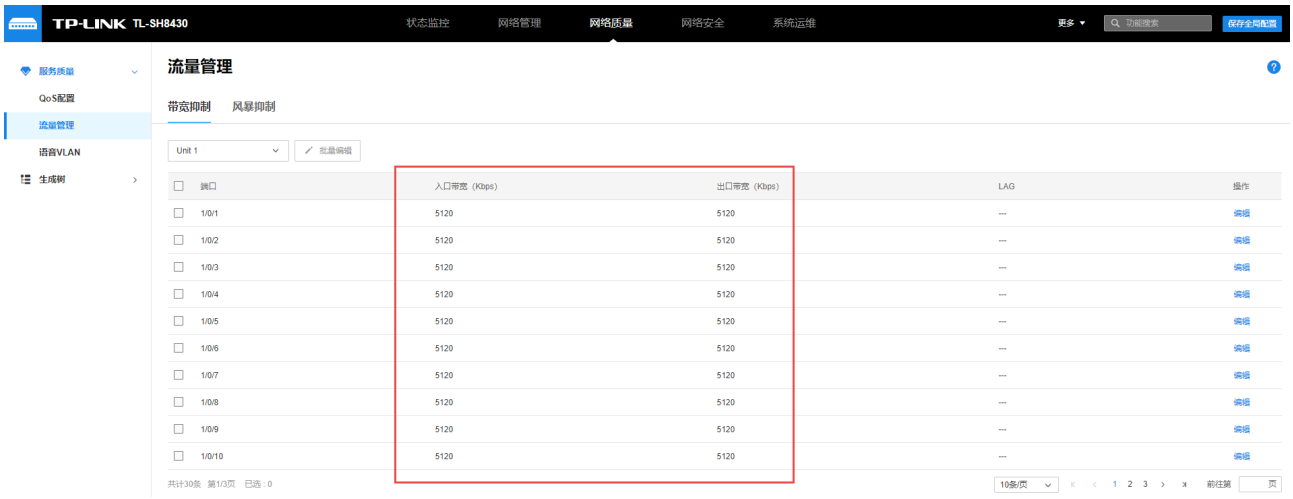
某出租屋的管理人员发现经常有租户在使用电脑下载大量视频数据，在下载数据时导致其他用户无法使用网络，因此管理人员通过设置接入交换机的端口带宽控制功能控制每个端口的出入口速率，保障所有用户的上网使用，示意网络拓扑如下：



配置步骤：

进入页面：网络质量 >> 服务质量 >> 流量管理 >> 带宽抑制，设置所有下联终端端口的出入口速率为 5120Kbps 即 5Mbps，上联口不限制。

设置完成后如下：



注意：

- 端口限制数值单位为 kpbs 且必须为 64 的整数倍，输入其他数值后设备会自动匹配最近的一个值。
- 同一个端口的入口带宽限制和风暴抑制不能同时开启。

8.3 配置风暴抑制功能

8.3.1 风暴抑制介绍

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讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

本交换机可以对三种常见的广播帧（广播包、组播包、UL 包）进行限制。

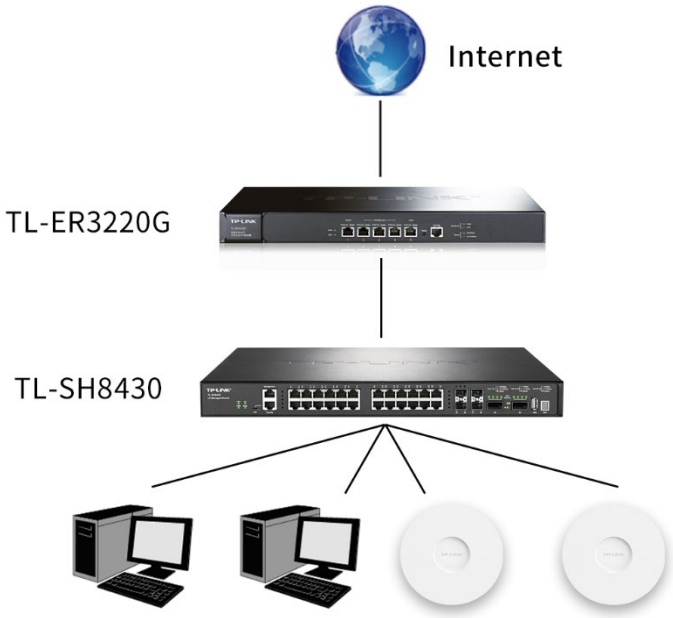
配置方法：

进入页面：网络质量 >> 服务质量 >> 流量管理 >> 风暴抑制，选择对应端口，点击<编辑>，设置广播包、组播包和 UL 包限速值，点击<保存>。

8.3.2 风暴抑制配置实例

组网介绍：

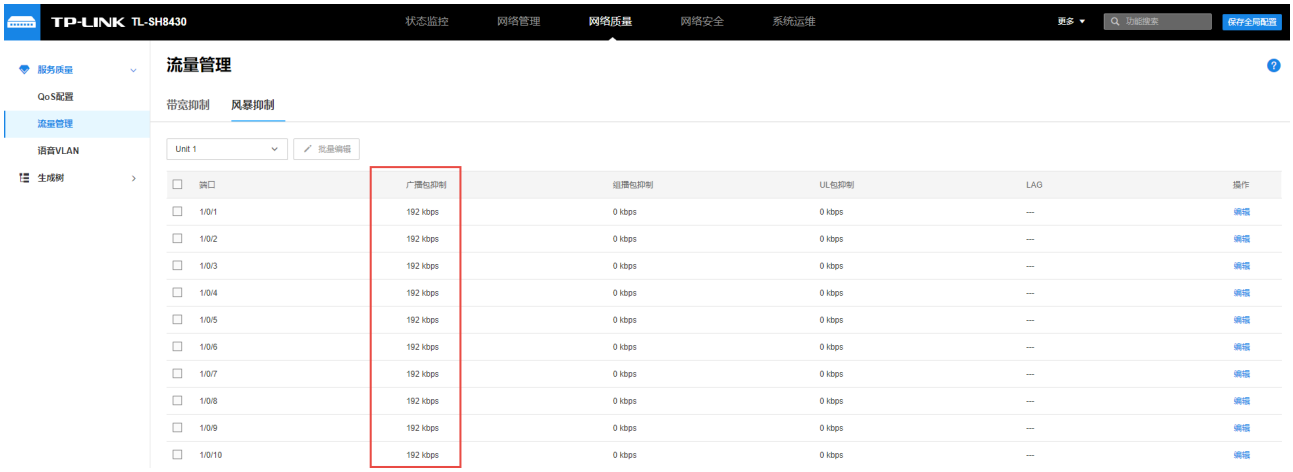
某企业使用一台三层交换机作为接入层设备，为了保障网络（尤其是无线网络）运行的稳定性，需要对整个网络拓扑中的广播包流量有所控制，因此需要在交换机上设置端口的最大接受广播速率，如果端口的接受广播速率超过此值，则丢弃多余广播包，保障网络稳定性。示意网络拓扑如下：



配置步骤：

进入页面：网络质量 >> 服务质量 >> 流量管理 >> 风暴抑制，设置所有终端口的广播接受速率为200Kbps（一般情况下无线场景接 AP 的千兆端口建议值），注意单位为 Kbps，勾选所有终端端口，点击<批量编辑>，设置广播包抑制速率 200Kbps，如下如所示：

配置完成如下：



注意：

- 端口限制数值单位为 kpbs 且必须为 64 的整数倍，输入其他数值后设备会自动匹配最近的一个值。
- 同一个端口的入口带宽限制和风暴抑制不能同时开启。

回目录

第9章　生成树

9.1　生成树介绍

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，避免设备由于重复接收相同的报文所造成的报文处理能力下降的问题发生。

生成树协议分为三种，普通生成树 STP（Spanning Tree Protocal）、快速生成树 RSTP（Rapid Spanning Tree Protocal）以及多生成树 MSTP（Multiple Spanning Tree Protocal），可以根据需要选用，满足多种使用环境需求。

STP 和 RSTP 功能的设置方法是相同的。RSTP 相比于 STP 来说收敛速度更快，且兼容 STP 协议，所以一般推荐使用 RSTP 协议。

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在 STP 和 RSTP 的基础上，根据 IEEE 协会制定的 802.1S 标准建立的，它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发， 从而为冗余链路提供了更好的负载分担机制。

配置方法：

进入页面：网络质量 >> 生成树，启用生成树功能，选择生成树模式，点击<保存>。

说明：

- RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是优化版的 STP，它大大缩短了端口进入转发状态的延时，从而缩短了网络最终达到拓扑稳定所需要的时间。
- MSTP 将整个网络划分为多个 MST 域，各个域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。

配置参数：

进入页面：网络质量 >> 生成树，进行生成树的参数配置，点击<保存>。

说明：

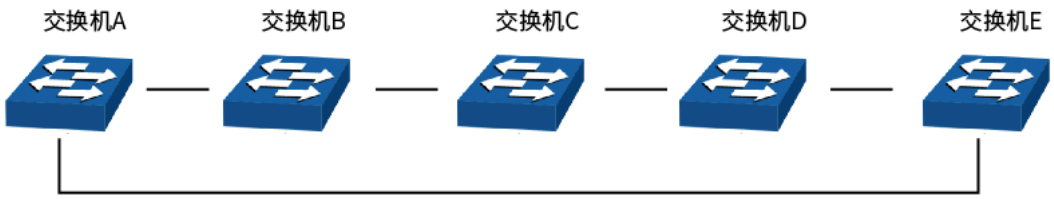
- CIST 优先级：是一个用户可以设定的参数，数值范围从 0 到 61440。设定的值越小， 优先级越高。交换机的桥优先级越高，才越有可能成为根桥。

9.2 STP/RSTP 配置实例

组网介绍：

客户公司内部网络，5 台 TP-LINK 管理型交换机搭建 STP 或者 RSTP 环形网络，实现链路故障备份的功能。5 台交换机环形连接，所有交换机之间的连接用端口为 1、2 号端口 。

示意网络拓扑如下：



配置步骤：

- 设置交换机 A

1. TP-LINK 交换机的默认管理 IP 均为 192.168.0.1，为了防止地址冲突，建议首先将各交换机设置为不冲突的 IP 地址。进入页面：进入页面：网络管理 >> 接口配置，点击<编辑接口>，进行修改。

2. 进入页面：网络质量 >> 生成树 >> 基本配置，启用生成树功能，选择“STP”或者“RSTP”生成树模式，点击 <保存>。

3. 进入页面：网络质量 >> 生成树 >> 端口配置，开启端口（本实例中是端口 1 和端口 2）的生成树功能。

一台交换机设置完成，相同的方法，依次设置其他的交换机。完成 STP/RSTP 功能的设置之后，进行线路连接即可。

9.3 MSTP 配置实例

组网介绍：

客户公司内部网络，如下图所示拓扑结构， 交换机 A、B、C、D、E 均支持 MSTP 功能；

A 为中心交换机；

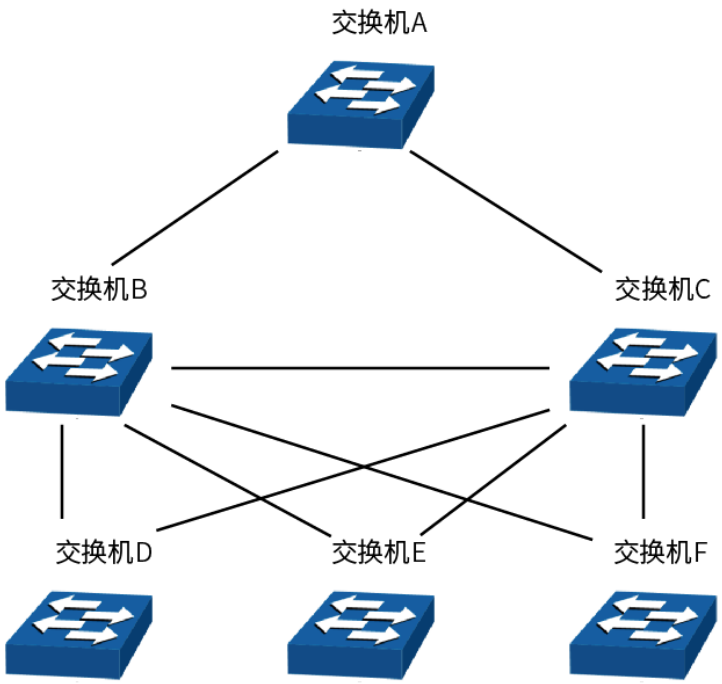
B、C 为汇聚层交换机，D、E、F 为接入层交换机；

整个网络中共有 6 个 VLAN，为 VLAN101-VLAN106；

所有设备运行 MSTP，并且所有设备均属于同一个 MST 域；

VLAN101、103 和 105 的数据流量以 B 为根桥，VLAN102、104 和 106 的数据流量以 C 为根桥。阻断网络中的环路，并能达到数据转发过程中 VLAN 数据的冗余备份以及负载分担效果。

示意网络拓扑如下：



配置步骤：

- 配置交换机 A

1. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1，点击<编辑>，将端口类型更改为 TRUNK，并将端口加入 VLAN 101 到 VLAN 106，PVID 为 1。设置完成，点击<保存>。

2. 进入页面：网络质量 >> 生成树 >> 基本配置，启用生成树功能，选择“MSTP”生成树模式，点击<保存>。

3. 进入页面：网络质量 >> 生成树 >> 端口配置，开启端口的生成树功能。

4. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 域配置，配置域名为“TP-LINK”，修订级别默认，点击<保存>。

5. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 实例配置，配置 VLAN-实例映射表，将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。

- 配置交换机 B

6. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1，点击<编辑>，将端口类型更改为 TRUNK，并将端口加入 VLAN 101 到 VLAN 106，PVID 为 1。设置完成，点击<保存>。

7. 进入页面：网络质量 >> 生成树 >> 基本配置，启用生成树功能，选择“MSTP”生成树模式，点击<保存>。

8. 进入页面：网络质量 >> 生成树 >> 端口配置，开启端口的生成树功能。

9. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 域配置，配置域名为“TP-LINK”，修订级别默认，点击<保存>。

10. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 实例配置，配置 VLAN-实例映射表，将 VLAN101、103 和 105 映射到实例 1，**实例 1 的优先级设置为 0**；将 VLAN102、104 和 106 映射到实例 2，**实例 2 的优先级设置为 4096**。

- 配置交换机 C

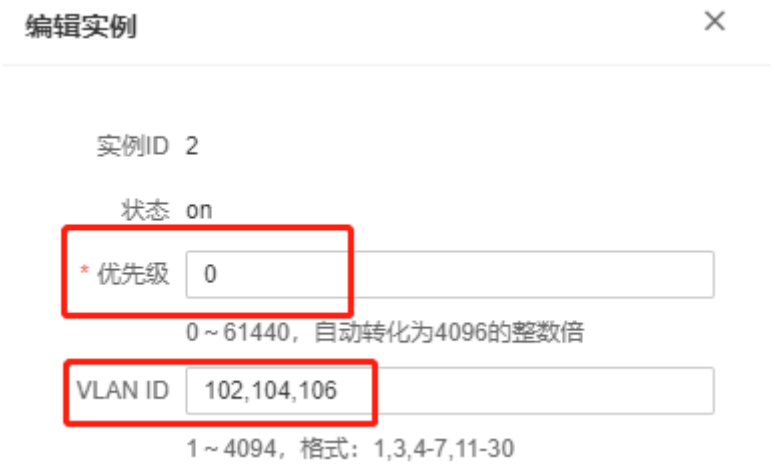
11. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1，点击<编辑>，将端口类型更改为 TRUNK，并将端口加入 VLAN 101 到 VLAN 106，PVID 为 1。设置完成，点击<保存>。

12. 进入页面：网络质量 >> 生成树 >> 基本配置，启用生成树功能，选择“MSTP”生成树模式，点击<保存>。

13. 进入页面：网络质量 >> 生成树 >> 端口配置，开启端口的生成树功能。

14. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 域配置，配置域名为“TP-LINK”，修订级别默认，点击<保存>。

15. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 实例配置，配置 VLAN-实例映射表，将 VLAN101、103 和 105 映射到实例 1，**实例 1 的优先级设置为 4096**；将 VLAN102、104 和 106 映射到实例 2，**实例 2 的优先级设置为 0**。



- 配置交换机 D

16. 进入页面：网络管理 >> VLAN >> 802.1Q VLAN >> 端口配置，选择端口 1，点击<编辑>，将端口类型更改为 TRUNK，并将端口加入 VLAN 101 到 VLAN 106，PVID 为 1。设置完成，点击<保存>。

17. 进入页面：网络质量 >> 生成树 >> 基本配置，启用生成树功能，选择“MSTP”生成树模式，点击<保存>。

18. 进入页面：网络质量 >> 生成树 >> 端口配置，开启端口的生成树功能。

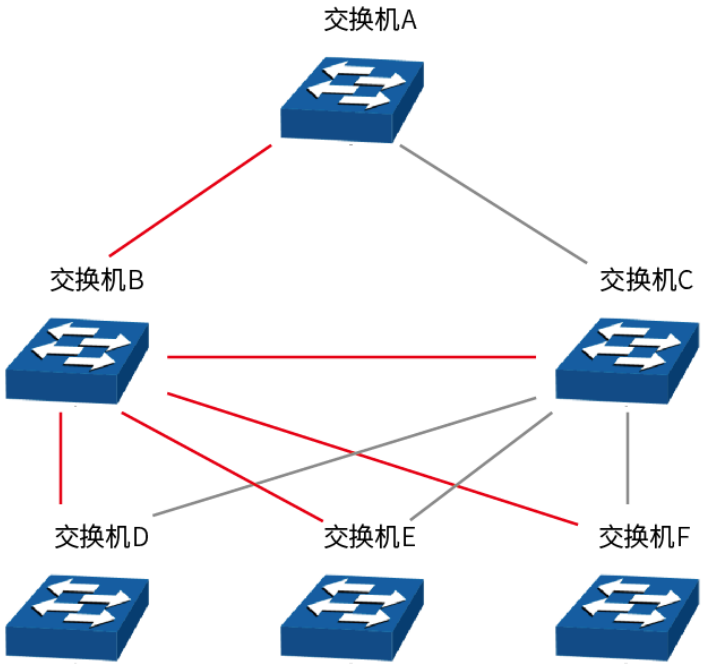
19. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 域配置，配置域名为“TP-LINK”，修订级别默认，点击<保存>。

20. 进入页面：网络质量 >> 生成树 >> MSTP 实例 >> 实例配置，配置 VLAN-实例映射表，将 VLAN101、103 和 105 映射到实例 1；将 VLAN102、104 和 106 映射到实例 2。

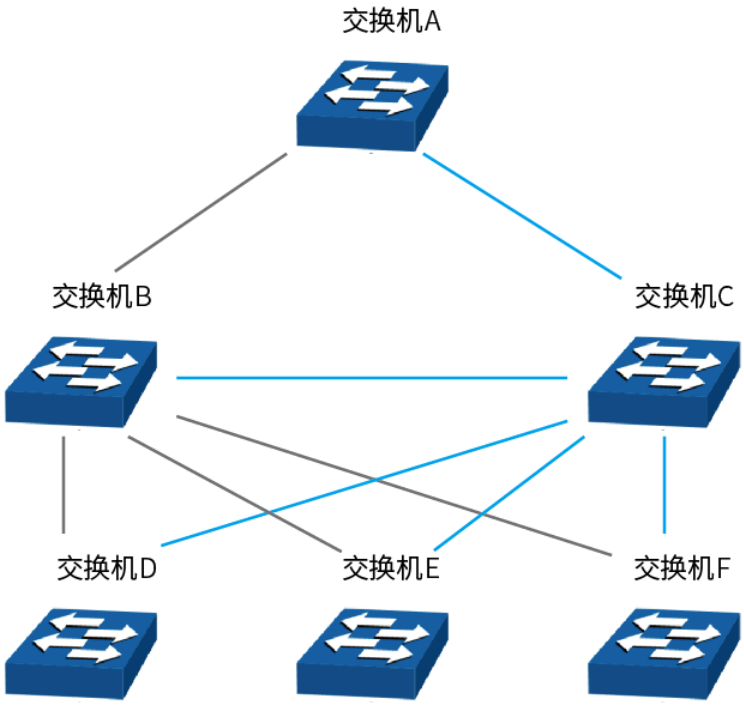
- 交换机 E 和交换机 F 的配置方法同交换机 D。

➢ 拓扑稳定以后两个实例所生成的动态拓扑结构

- 对于实例 1（VLAN 101 103 105）而言，连通的链路为下图中红色的路径，灰色的路径断开。



- 对于实例 2（VLAN 102 104 106）而言，连通的链路为下图中蓝色的路径，灰色的路径断开。



➢ 配置建议

- 所有交换机的端口均建议启用“TC 保护”功能。
- 根桥交换机的所有端口建议启用“根桥保护”功能。
- 非边缘端口建议启用“环路保护”功能。
- 连接 PC 与服务器的边缘端口，建议启用“BPDU 保护”或“BPDU 过滤”功能。

设置时每台交换机单独连接设置，每次设置一台交换机。设置完成后再进行线路连接。

回目录

第10章 网络安全

10.1 四元绑定

四元绑定，是将计算机的 MAC 地址、IP 地址、所属 VLAN 以及与之相连的交换机的端口号四者绑定，以下这四个参数信息简称四元信息。该功能可以启用 ARP 防护，只有符合绑定关系的计算机才能访问网络。

本交换机支持如下三种四元绑定方式：

1) 手动绑定，通过手动方式绑定局域网用户的四元信息。当可以全面获取正确的局域网用户的四元信息时，可通过此方式进行绑定。

2) 扫描绑定：通过 ARP 扫描获取局域网用户的四元信息，并根据实际需要选择扫描结果进行绑定。此绑定方式只需在相应的功能页面输入 IP 地址段进行扫描。

3) DHCP 侦听：通过 DHCP 侦听功能侦听 DHCP 广播包，记录数据包中的 IP、MAC 和 VLAN ID 等信息。当局域网中搭建了 DHCP 服务器给局域网用户分配 IP 地址时，DHCP 侦听功能可以很方便地记录局域网用户的四元信息。

此三种方式也称为四元绑定条目的三个来源。三种来源的四元绑定条目信息必须完全不一致，以避免冲突。如果四元绑定条目发生冲突，只有“来源”优先级最高的条目生效。此三种来源方式中，手动绑定优先级最高，其次是扫描绑定，DHCP 侦听优先级最低。

- **手动绑定**

进入页面：网络安全 >> 四元绑定 >> 手动绑定，选择当前局域网已有的条目，点击<手动绑定>即可。

- **扫描绑定**

进入页面：网络安全 >> 四元绑定 >> 扫描绑定，输入 ARP 扫描的 IP 范围和所属 VLAN，点击<搜索>，在扫描结果列表中，选中需要绑定的条目，点击<批量绑定>即可。

10.2 ARP 防护

10.2.1 防 ARP 欺骗

防 ARP 欺骗功能，通过四元绑定表对交换机收到的 ARP 报文进行检查，过滤非法的 ARP 报文，以此防御局域网中的 ARP 攻击。

进入页面：网络安全 >> ARP 防护 >> 防 ARP 欺骗。

源 MAC 验证　　当此功能开启后，ARP 防护功能会检查 ARP 报文的源 MAC 是否等于发送 MAC，如果不等则将报文丢弃。

目的 MAC 验证　　当此功能开启后，ARP 防护功能会检查 ARP 回复报文的目的 MAC 是否等于目标 MAC，如果不等则将报文丢弃。

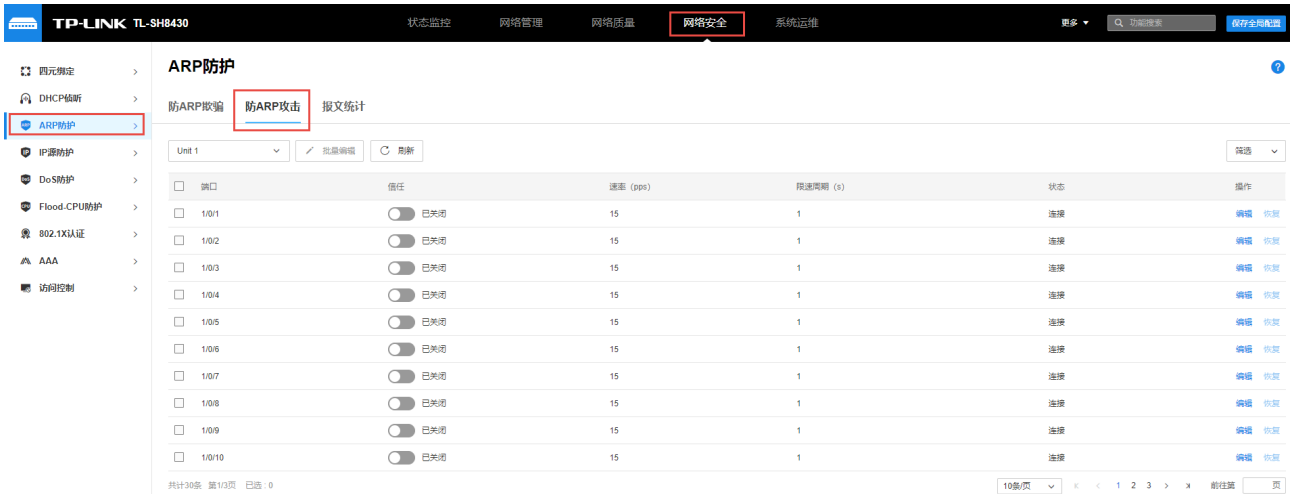
IP 验证　　当此功能开启后，ARP 防护功能会检查报文的 IP 合法性，如果 IP 字段不合法则将报文丢弃。

使能 VLAN　　使能对应 VLAN 的防 ARP 欺骗功能和防 ARP 攻击功能，如果不使能 VLAN，则对应 VLAN 的防 ARP 欺骗功能和防 ARP 攻击功能都不生效。

10.2.2　防 ARP 攻击

防 ARP 攻击功能对交换机的各端口处理的合法 ARP 数据包设定阀值，在单位时间内不可超过设定值。超过设定值时，交换机将停止处理 ARP 数据包 300 秒，能够有效的避免 ARP 泛洪攻击。

进入页面：网络安全 >> ARP 防护 >> 防 ARP 攻击。

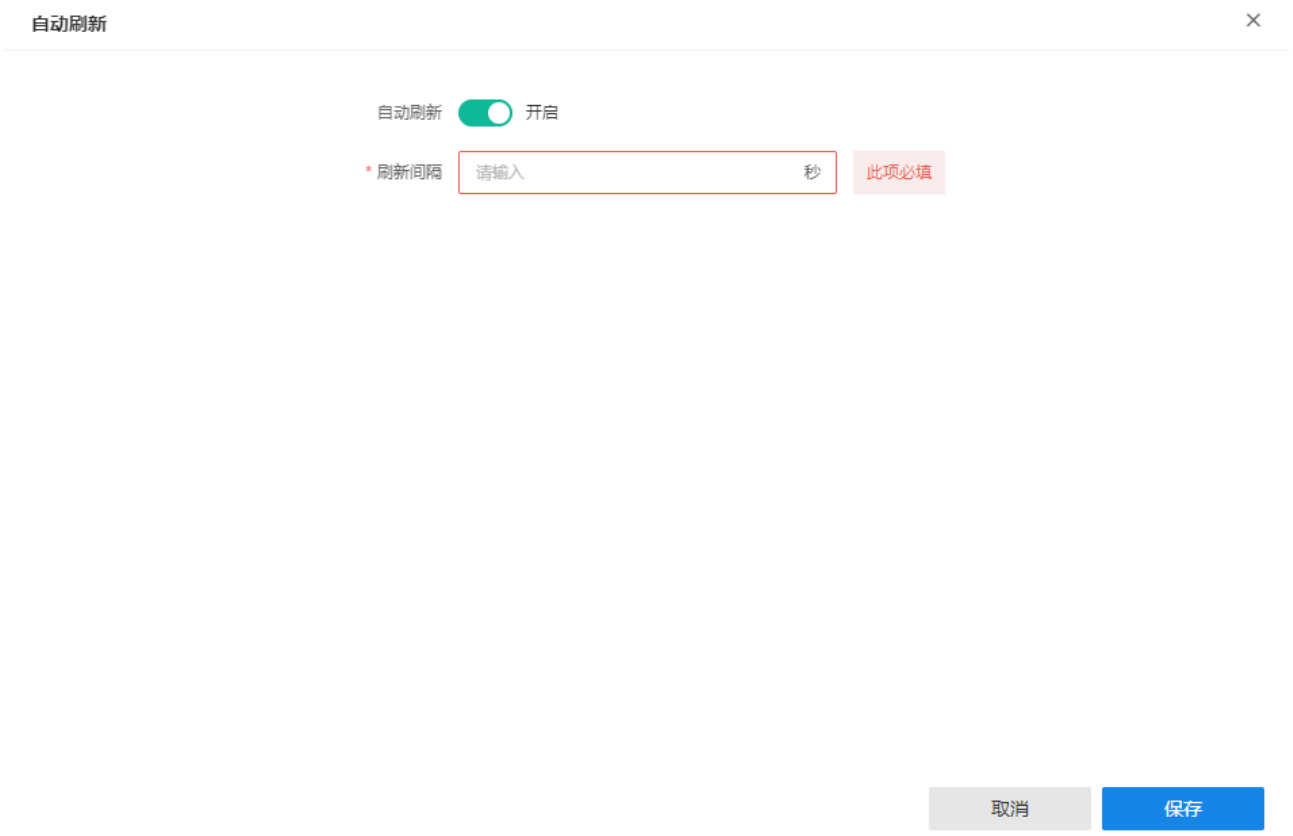


10.2.3 报文统计

通过报文统计功能，可以直观地查看各个端口收到的非法 ARP 数据包个数，并以此定位网络问题，并采取相应的防护措施。

进入页面：网络安全 >> ARP 防护 >> 报文统计。

自动刷新默认关闭，点击<自动刷新已关闭>，可开启自动刷新功能，输入刷新间隔，点击<保存>。



10.3 IP 源防护

IP 源防护功能是交换机根据四元绑定条目对接收的 IP 包进行过滤，只处理数据包相关字段与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

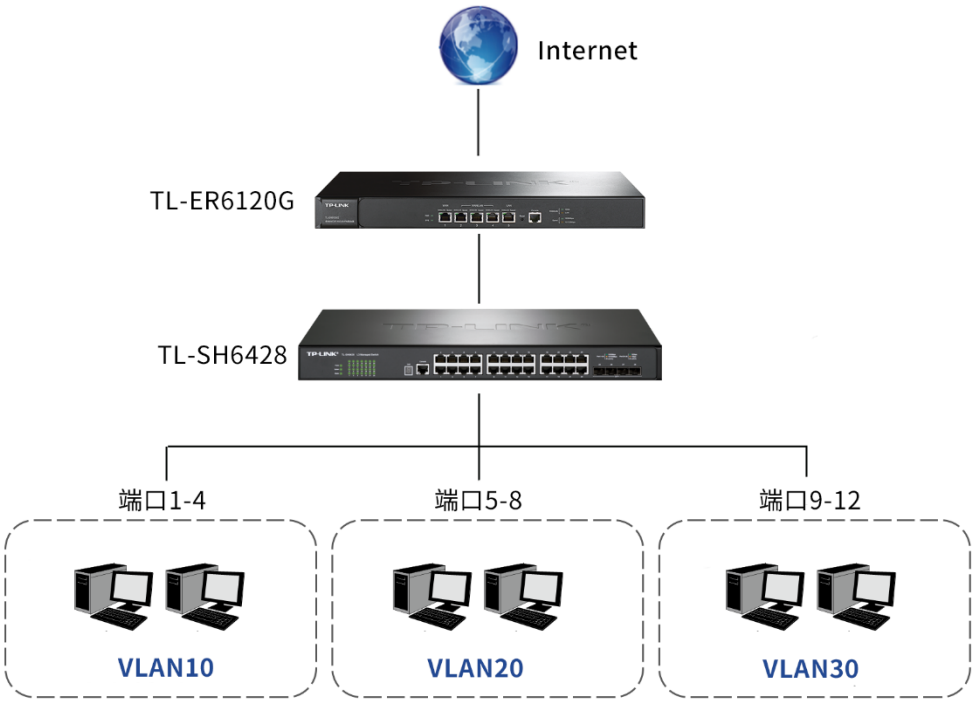
进入页面：网络安全 >> ARP 防护 >> IP 源防护。选择需开启 IP 源防护的端口，点击<编辑>，选择防护类型未 SIP+MAC，SIP+MAC 机制是只处理源 IP 地址、源 MAC 地址和端口均符合四元绑定信息的数据包，

点击<保存>。

10.4 四元绑定/ARP 防护/IP 源防护配置实例

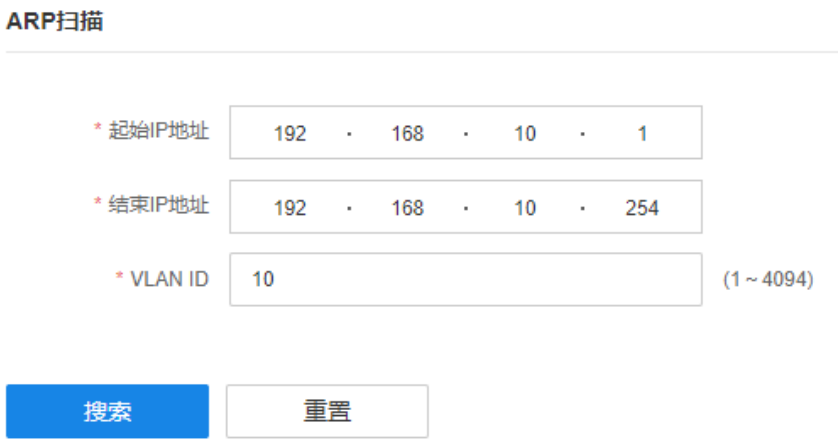
需求介绍：

某企业通过交换机作为接入层使用，为了保证网络的运行稳定性和安全性，需要开启每个业务 VLAN 下的 ARP 防护和 IP 源防护功能，保证只有固定终端在固定端口才能正常通过交换机转发数据，避免了非法的 ARP 攻击，示意网络拓扑如下：

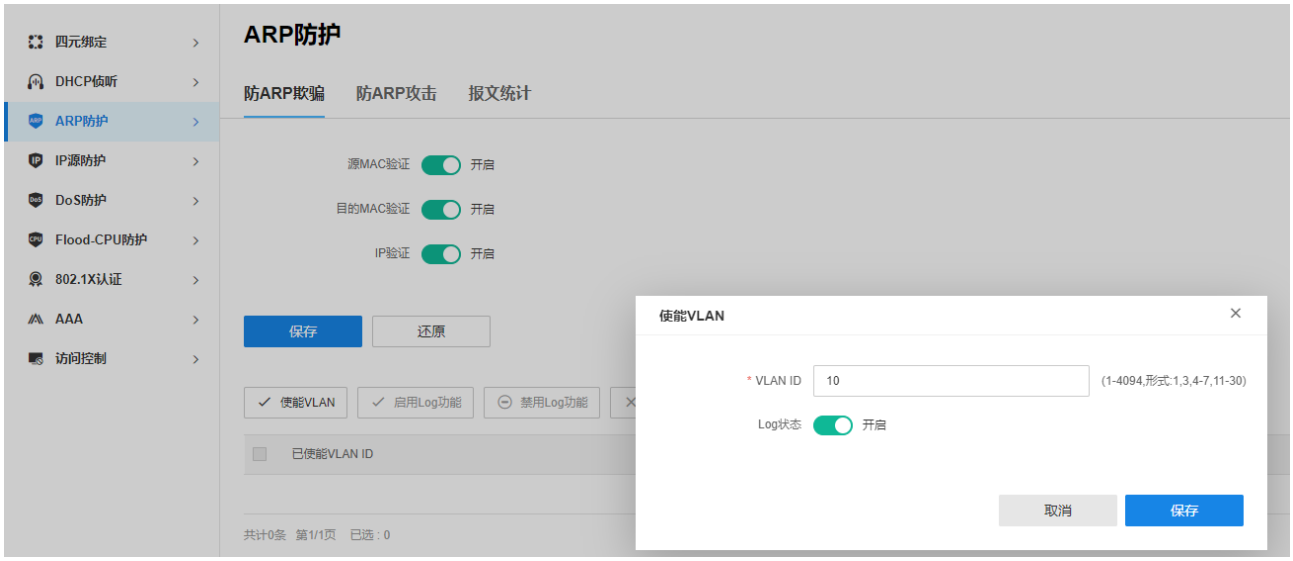


配置步骤：

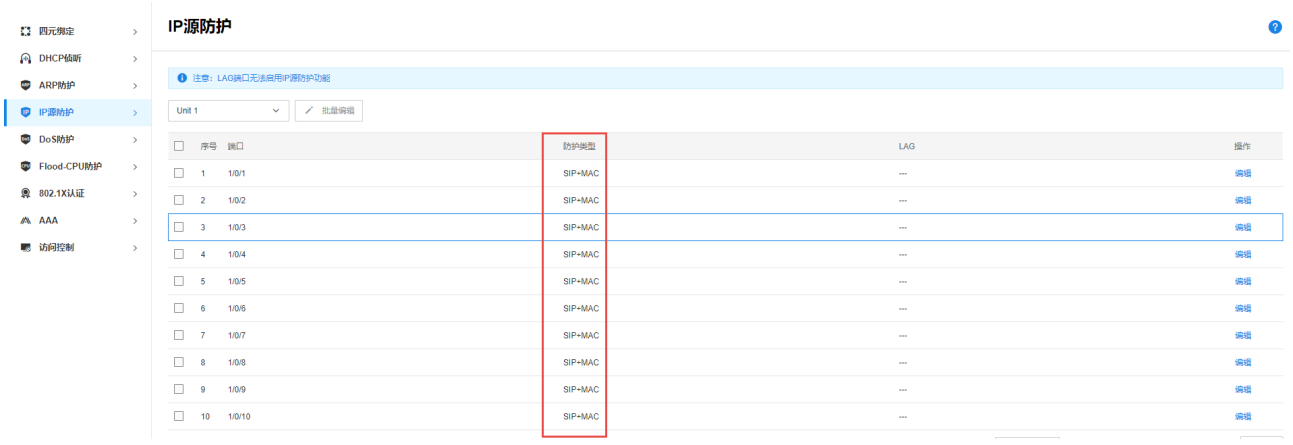
1. 进入页面：网络安全 >> 四元绑定 >> 扫描绑定，通过 ARP 扫描扫描当前所有正常接入交换机的终端设备，三个 VLAN 需要扫描三次，每次扫描出的结果选择防护范围为全部防护，并勾选所有结果，点击<批量绑定>。



2. 进入页面：网络安全 >> ARP 防护 >> 防 ARP 欺骗，启用源 MAC 验证，目的 MAC 验证，IP 验证，并使能对应的 VLAN，点击<保存>。



3. 进入页面：网络安全 >> IP 源防护，启用需要设置的端口 IP 源防护功能，防护类型选择 SIP+MAC 的方式，上联端口 24 口一般不要启用，因为外网回复的数据包源 IP 可能没在四元绑定条目内导致无法上网。



以上即可完成只有对应终端接入到对应端口且使用对应 IP 才能上网，保证了企业网络的安全性。

10.5 DoS 防护

DoS（Denial of Service，拒绝服务）攻击是指攻击者利用网络协议实现的缺陷，耗尽被攻击对象的资源，使目标计算机或网络无法提供正常的服务或资源访问甚至崩溃。

DoS 攻击的具体的影响如下：

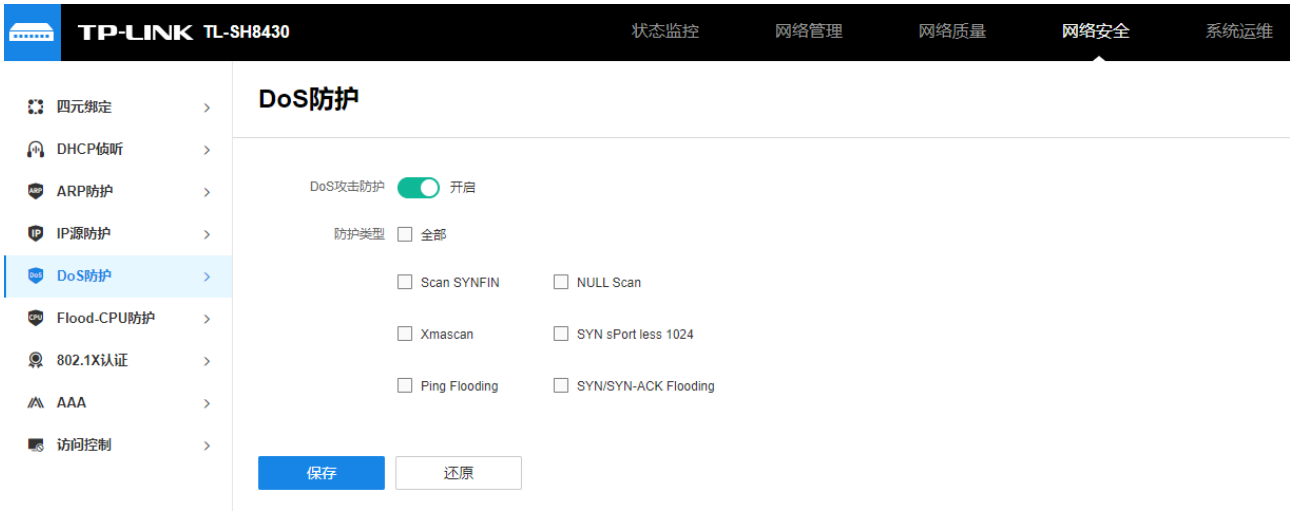
1) 耗尽服务器的资源，包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。使服务器疲于响应此类报文，导致网络瘫痪。

2) 由于交换机接收到此类报文需经过 CPU 处理，因此若请求报文数量过多，会导致交换机 CPU 利用率持续上升，无法正常工作。

本交换机通过解析 IP 数据包，分析数据包中的特定字段，并判断是否符合 DoS 攻击数据包的特征。对于非法的数据包，交换机将直接丢弃；而对于某些正常的数据包，由于流量过大可能导致受害主机瘫痪时，交换机可以对此类数据包进行限速。本交换机能够防护的 DoS 攻击种类如下表。

DoS攻击类型	攻击特征
Scan SYNFIN	TCP标志位SYN、FIN位被置1的数据包。由于SYN标志用来初始化连接的，FIN标志用来表示发端已完成发送任务请求关闭连接，所以SYN/FIN肯定是非法的数据包，本交换机能够识别此类攻击。
Xmascan	TCP序号置为0，FIN、URG、PSH位置为1的数据包。
NULL Scan	TCP序号置为0，所有控制位置为0的数据包。在正常的TCP连接以及数据传输过程中，不会出现所有控制位置0的情况，此类数据包为非法的数据包。
SYN sPort less 1024	TCP SYN标志位置1，源端口小于1024的数据包。
Ping Flooding	利用Ping广播风暴，淹没整个目标系统，以至于该系统不能响应合法的通信。
SYN/SYN-ACK Flooding	每当我们进行一次标准的TCP连接，都会有一个三次握手的过程，而TCP-SYN Flood只进行前两个步骤，服务方在一定时间内等待请求方ASK消息。由于一台服务器可用的TCP连接是有限的，如果攻击方发送大量此类连接请求，则服务方TCP连接队列将会很快阻塞，系统资源和可用带宽急剧下降，无法提供正常的网络服务，从而造成拒绝服务。

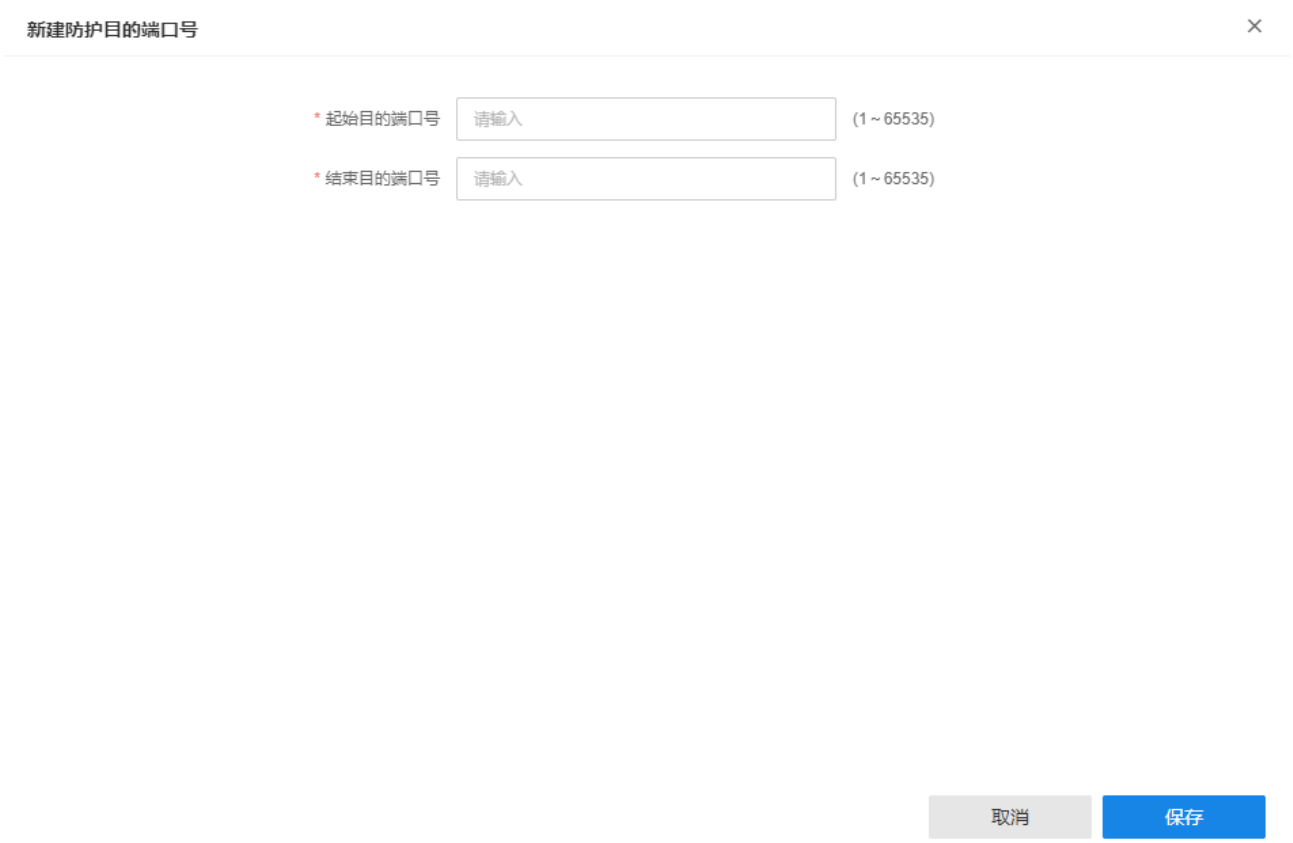
进入页面：网络安全 >> DoS 防护。开启<DoS 攻击防护>功能，选择防护类型，点击<保持>。



10.6 Flood-CPU 防护

TCP/UDP 泛洪的 CPU 防护功能用于避免交换机消耗大量的资源用于处理无意义的 IP 报文，同时可减少网络上因处理该类 IP 报文带来的大量 ARP 查询报文。

进入页面：网络安全 >> Flood-CPU 防护，点击<新增>，输入起始目的端口号和结束目的端口号，点击<保存>。



10.7 DHCP 侦听

10.7.1 DHCP 侦听介绍

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）主要作用是集中分配和管理 IP 地址，通常我们是通过路由器或三层网管交换机充当 DHCP 服务器的角色，但如果网络中有其他能够分配 DHCP 的非法服务器，也会给客户端分配不正确的 IP，导致终端无法上网，网络结构紊乱。而开启“DHCP 侦听”功能，添加授信端口，可以让终端和服务器只能从授信端口接收发送 DHCP Offer 报文，从而能正确的进行网络通信。

DHCP 侦听是运行在交换机上的一种 DHCP 安全特性。

通过 DHCP 侦听功能，交换机可以侦听用户动态申请 IP 地址的过程，阻止局域网中非法 DHCP 服务器给终端分配地址，并记录局域网中计算机的 IP 地址、MAC 地址、VLAN 以及连接端口等信息，自动进行四元绑定。交换机还可以利用 Option82 字段传递控制信息和网络配置参数，为客户端提供更加丰富的网络配置信息。

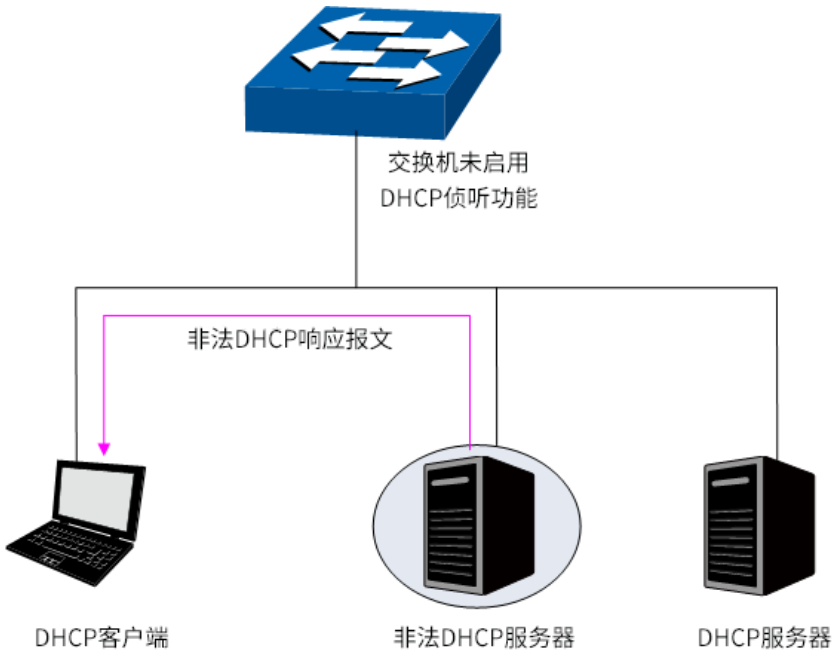
通过设置 DHCP 服务器的连接端口为授信端口，只处理授信端口发来的 DHCP 响应报文；通过监听 DHCP 报文，记录用户从 DHCP 服务器获取局域网用户的四元信息，进行绑定后与 ARP 攻击防护配合使用；同时也可以过滤不可信任的 DHCP 信息，防止局域网中发生 DHCP 服务欺骗攻击，提高网络的安全性。

DHCP 服务欺骗攻击：

在 DHCP 工作过程中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，不仅会给网络造成混乱，也对网络安全造成很大威胁。这种网络中出现非法的 DHCP 服务器，通常分为两种情况：

1) 用户不小心配置的 DHCP 服务器，由此引起的网络混乱非常常见。

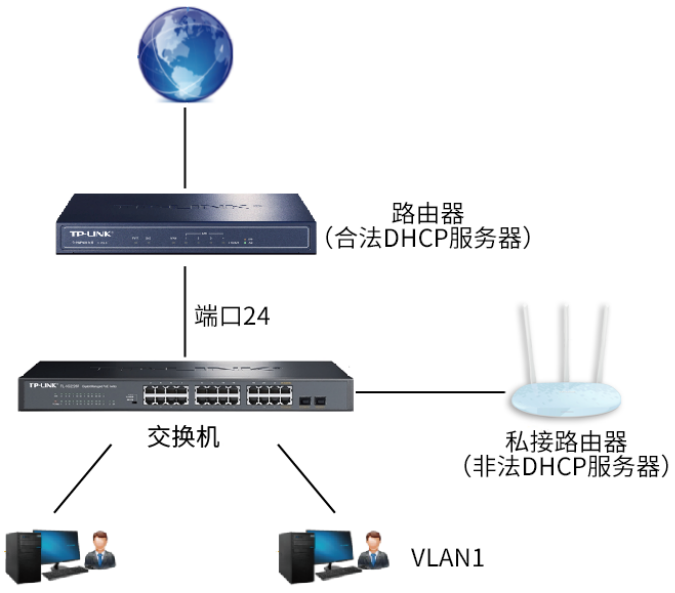
2) 黑客将正常的 DHCP 服务器中的 IP 地址耗尽，然后冒充合法的 DHCP 服务器，为客户端分配 IP 地址等配置参数。例如黑客利用冒充的 DHCP 服务器，为用户分配一个经过修改的 DNS 服务器地址，在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站，骗取用户的帐户和密码，如下图所示。



10.7.2 DHCP 侦听配置实例

组网介绍：

某酒店通过交换机作为接入层使用，为了保证网络的运行稳定性，使终端只能从规定的 DHCP 服务器（路由器）获取 IP 地址，不能从非法的 DHCP 服务器处获取地址，示意网络拓扑如下：

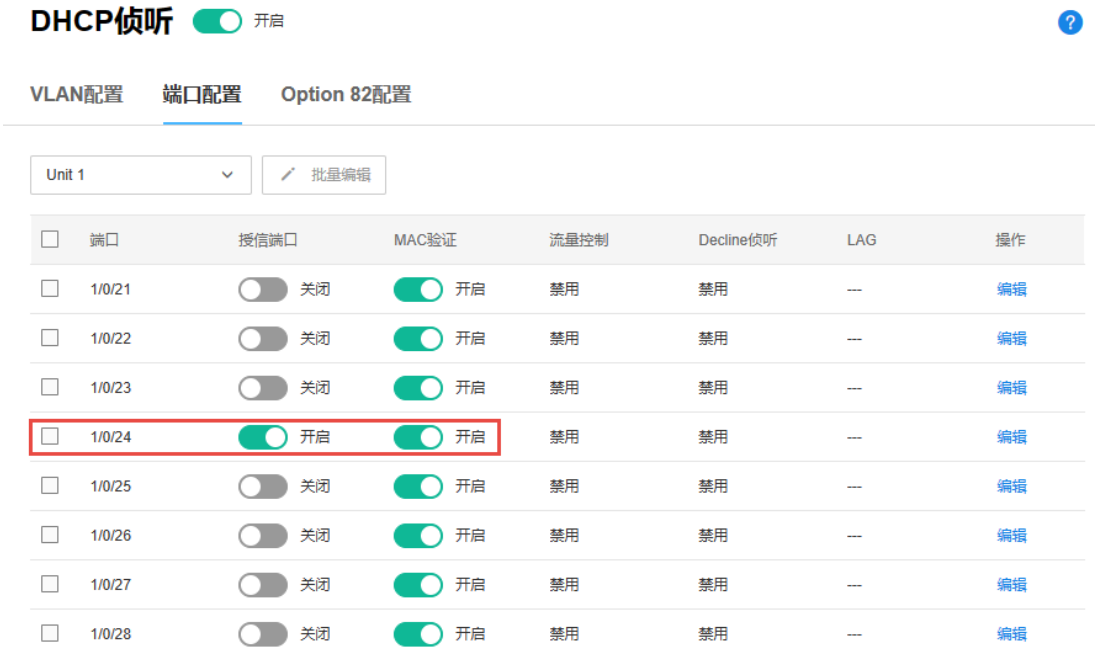


配置步骤：

1. 进入页面：网络交换 >> DHCP 侦听，开启 DHCP 侦听功能。

2. 进入页面：网络安全 >> DHCP 侦听 >> 全局配置，启用 DHCP 侦听功能，并选择生效的 VLAN，在本例中只有 VLAN1，因此选择 VLAN1。如果有其他 VLAN 需要开启侦听功能，也需要输入对应的 VLAN ID，如下图所示。

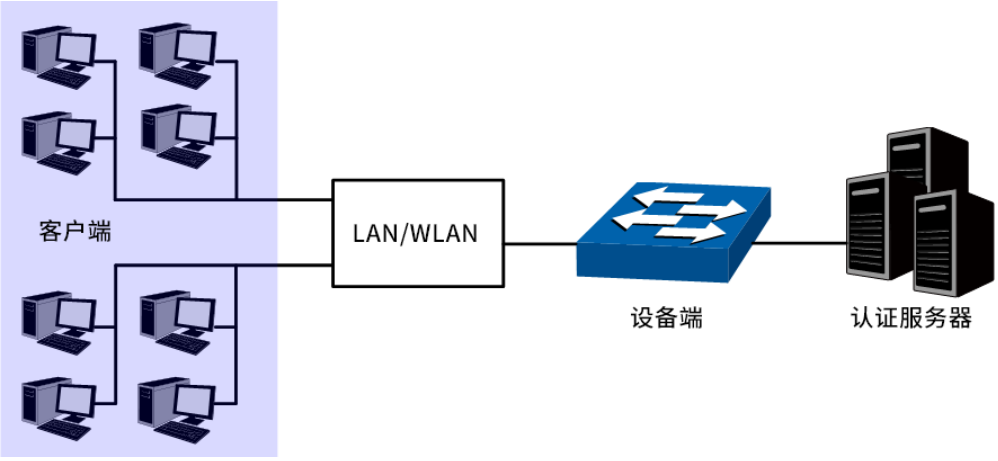
3. 进入页面：网络安全 >> DHCP 侦听 >> 端口配置，设置连接合法路由器的端口为信任端口，本例中设置路由器的上联口 24 为受信端口，其余为非信任端口。交换机上所接入的终端就只能从 24 口上联的设备获取地址，不会从其余端口的非法 DHCP 服务器获取地址，保障了网络的安全性。



10.8 802.1X 认证

- **802.1X 体系结构**

802.1X 的系统是采用典型的 Client/Server 体系结构，包括三个实体，如下图所示。



1) 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，并由设备端对其进行认证。客户端软件必须为支持 802.1X 认证的用户终端设备。

2) 设备端：通常为支持 802.1X 协议的网络设备，如本交换机，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。

3) 认证服务器：为设备端提供认证服务的实体，例如可以使用 RADIUS 服务器来实现认证服务器的认证和授权功能。该服务器可以存储客户端的相关信息，并实现对客户端的认证和授权。为了保证认证系统的稳定，可以为网络设置一个备份认证服务器。当主认证服务器出现故障时，备份认证服务器可以接替认证服务器的工作，保证认证系统的稳定。

- **802.1X 认证工作机制**

IEEE 802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交换。

1) 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

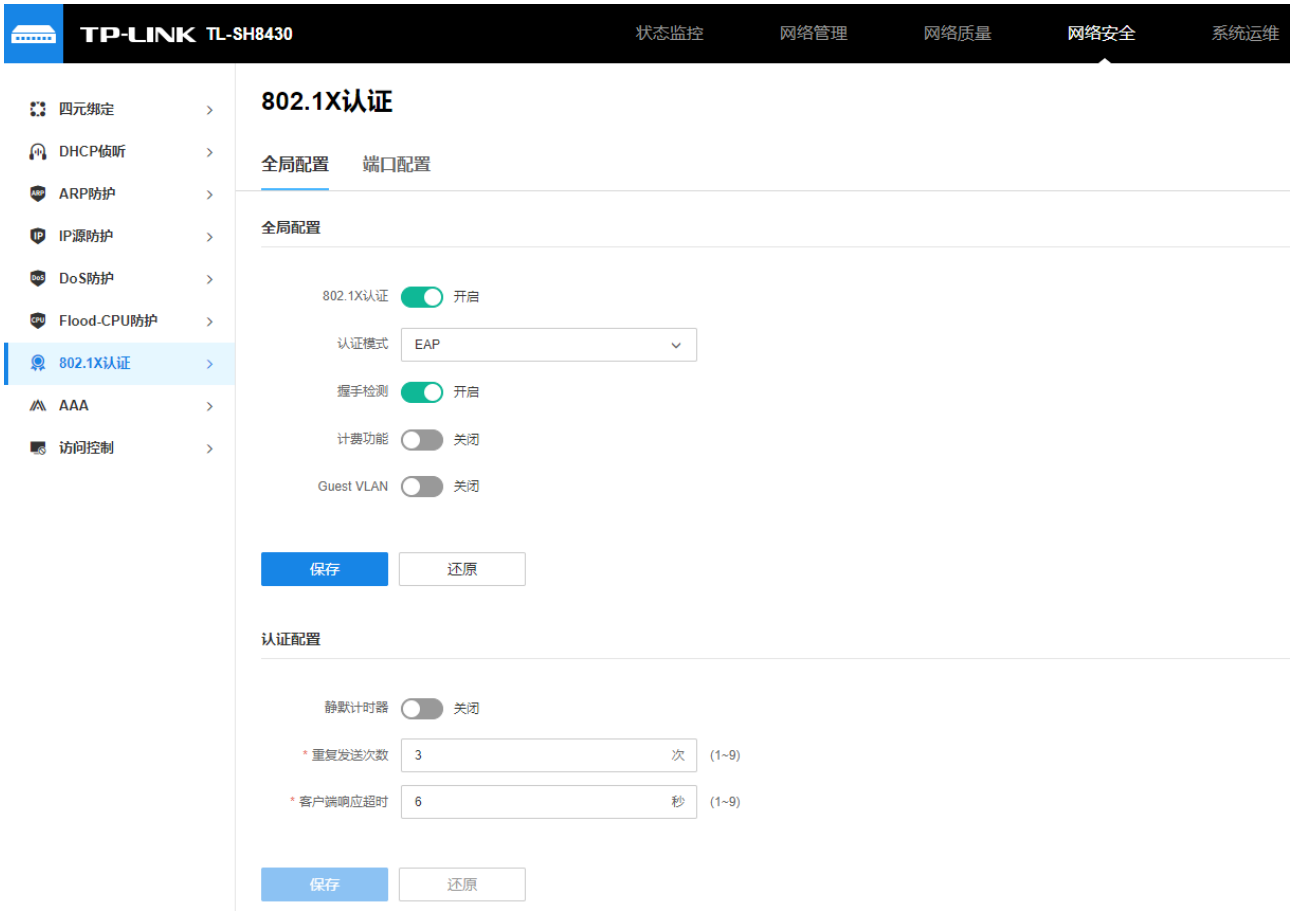
2) 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是设备端终结 EAP 协议报文，采用包含 PAP （Password Authentication Protocol，密码验证协议）或 CHAP （Challenge Handshake Authentication Protocol，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证。

3) 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端根据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

10.8.1 全局配置

在全局配置功能页面，可以开启全局 802.1X 认证功能。

进入页面：网络安全 >>802.1X 认证 >> 全局配置，开启 802.1X 认证功能，配置其他认证参数，点击<保存>。



802.1X 功能： 选择是否启用 802.1X 认证功能。

认证模式： 选择 802.1X 认证方法。

- EAP：用户端与交换机之间运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其它高层次协议中(如 RADIUS)，以便穿越复杂的网络到达认证服务器。
- PAP：用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议(如 RADIUS)，传递用户认证信息给认证服务器系统。

握手检测： 选择是否启用握手检测功能。握手检测功能用于检测客户端与交换机的连接状态。如果使用其他客户端软件进行连接，请关闭握手检测功能。

Guest VLAN： 选择是否启用 Guest VLAN 功能。

Guest VLAN ID： 填写启用 Guest VLAN 的 VLAN ID。Guest VLAN 中的用户可以访问指定的网络资源。

计费功能： 选择是否启用计费功能。

静默： 选择是否启用静默计时器。

静默时长： 填写静默时长。用户认证失败后，在静默时间内不再处理同一用户的 802.1X 认证请求。

重复发送次数： 填写认证报文的最大重传次数。

客户端响应超时： 填写交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。

10.8.2 端口配置

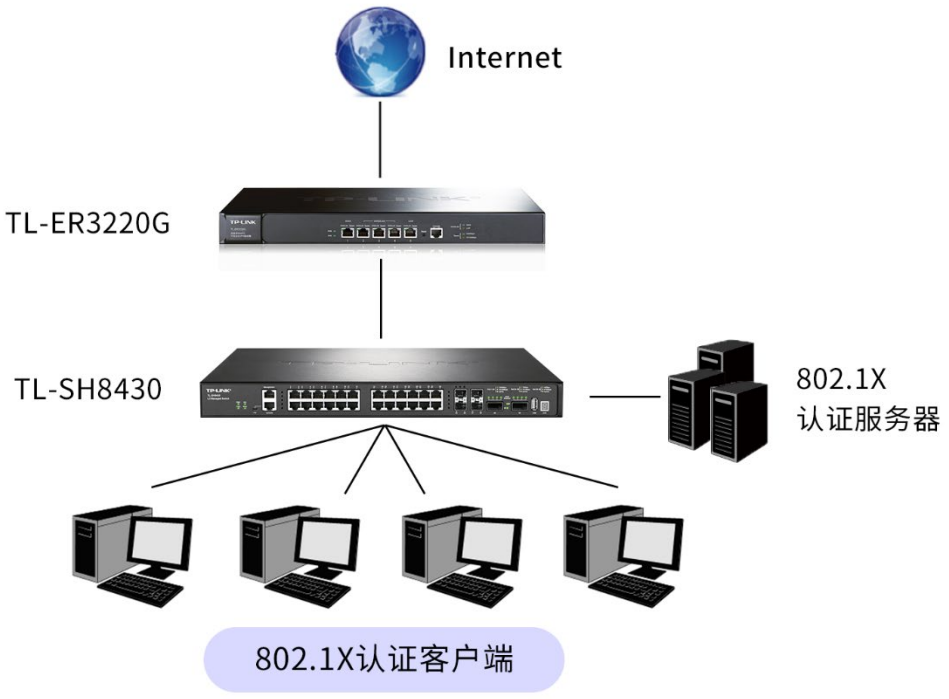
在端口配置功能页面，可以根据实际的网络情况设置端口的 802.1X 功能特性。

进入页面：网络安全 >> 802.1X 认证 >> 端口配置，选中特定端口，点击<编辑>。

10.8.3 802.1X 认证配置实例

需求介绍：

某公司为了保证数据接入的安全性，使用交换机做 802.1X 认证，只有通过登录网络管理员分配的员工账号才有权接入网络使用网络资源，拓扑如下：



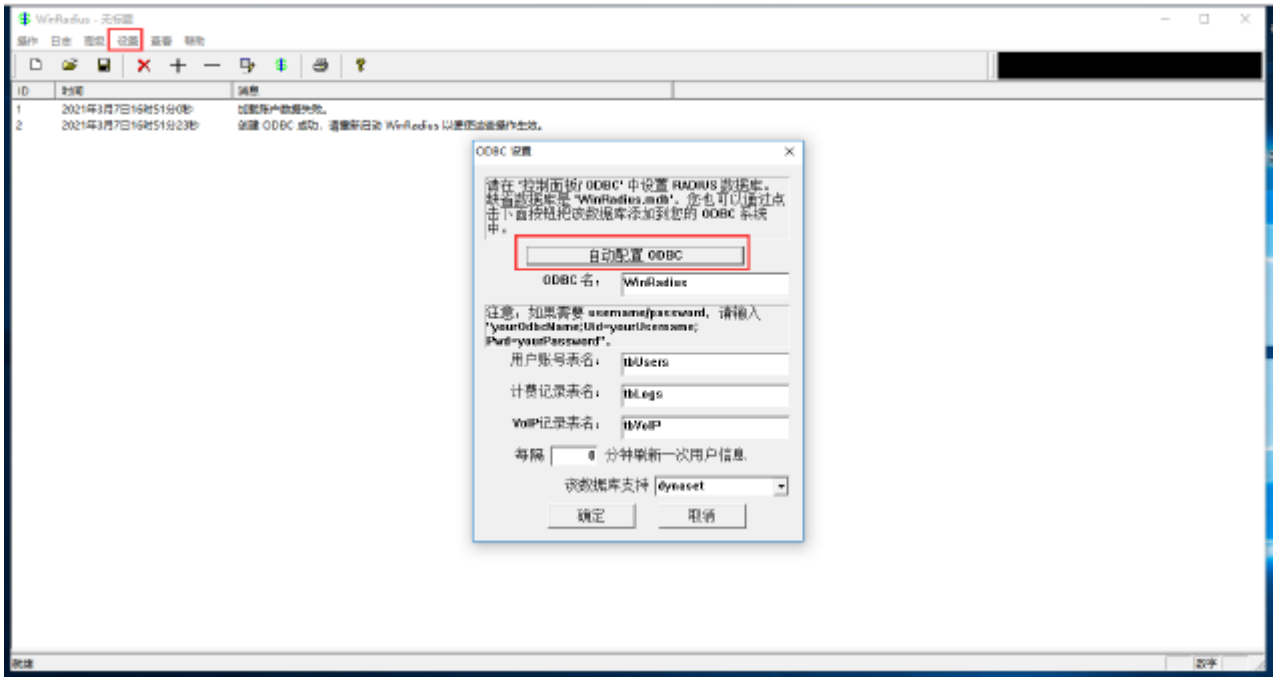
图中以 TL-SH8430 做中心交换机，802.1X 认证服务器接在 TL-SH8430 上。所有终端都需要通过认证之后才能访问服务器资源或者网络资源。

配置方法：

首先搭建 Radius 认证服务器。

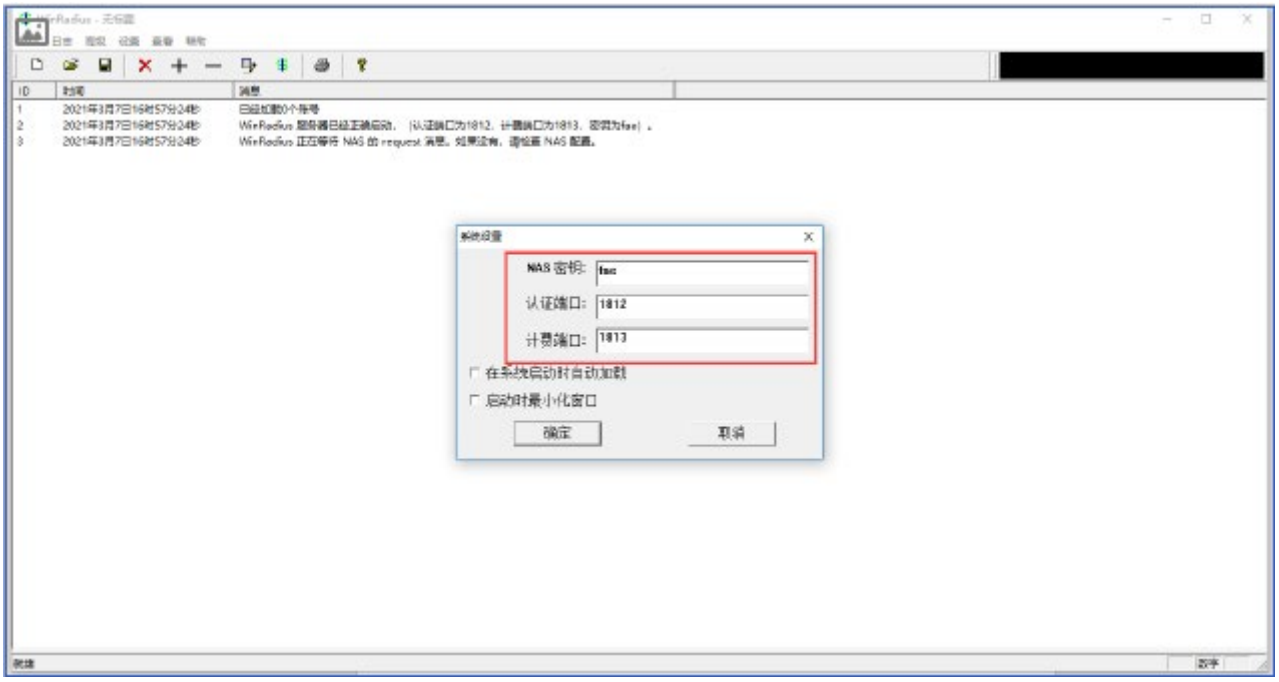
本文以试用版的 WinRadius 做为认证服务端。（也可以在 Windows Server 上搭建 Radius 认证服务器。有关服务器的搭建方法请在网上参考相关资料）。

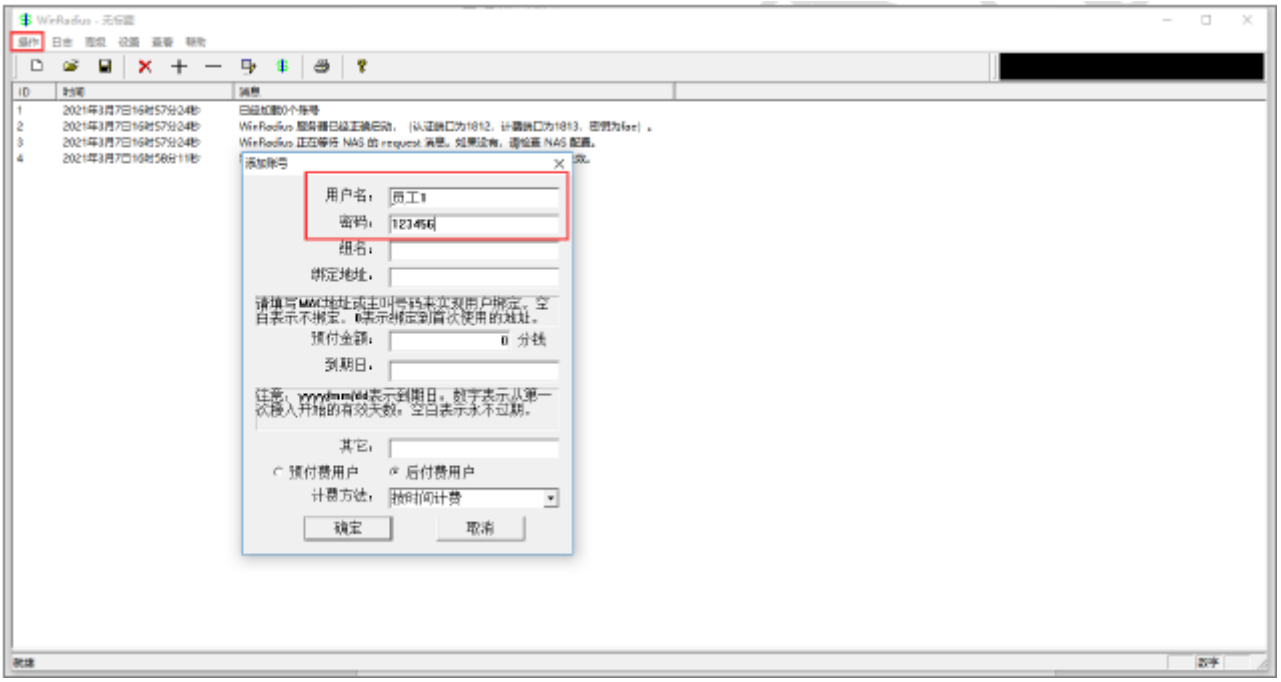
1. 启用 Winradius，用管理员身份运行，并在“设置—数据库—自动配置 ODBC”，配置数据库，数据库配置成功后再重启软件。



2. 软件重启成功后，配置服务器参数;

- 服务器 IP 地址：192.168.111.250 （服务器 IP 需要保证与交换机 VLAN1 的接口 IP 是可以相互通讯的，本例按照和 VLAN 1 同网段 IP 举例）。
- 认证端口：1812
- 计费端口：1813
- 密钥：fae
- 服务器上设置用户账号密码：员工 1/123456

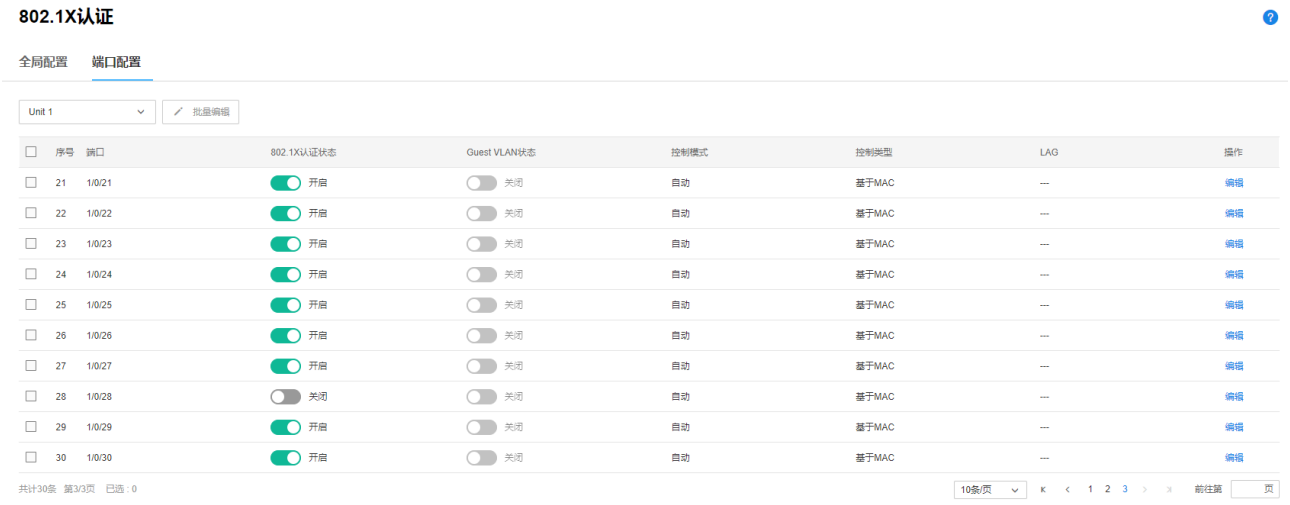




其次，配置 TL-SH8430 的 802.1X 功能

3. 进入页面：网络安全 >> 802.1X 认证 >> 全局配置，启用 802.1X 全局配置功能，认证模式选择 EAP，其余参数本次配置选择默认。

4. 进入页面：网络安全 >> 802.1X 认证 >> 端口配置，配置应端口的 802.1X 功能。



注意：

- 不启用 TL-SG5428 级联端口(28 端口)的 802.1X 认证，使认证服务器在任何时候都能通过该端口接入网络以便认证客户端。
- 配置其他需要认证的端口。（TL-SH8430 可同时支持基于 MAC 和 Port 的认证，这里均采用基于 MAC

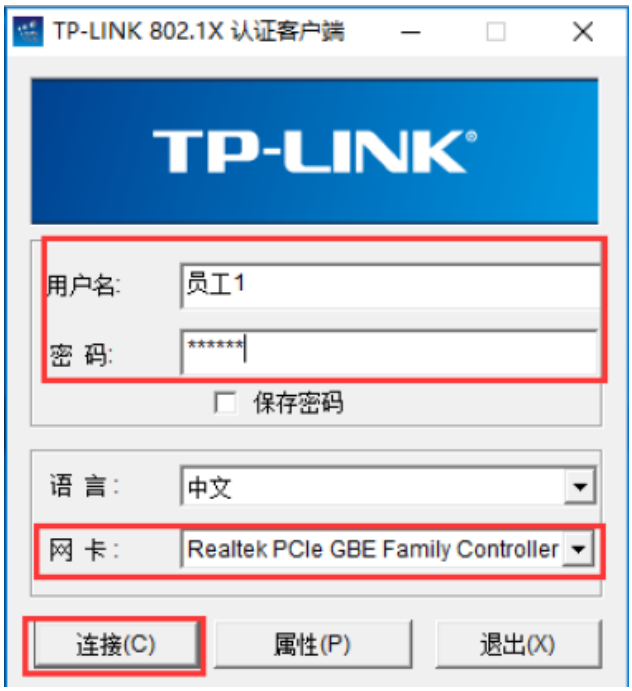
的认证方式)。

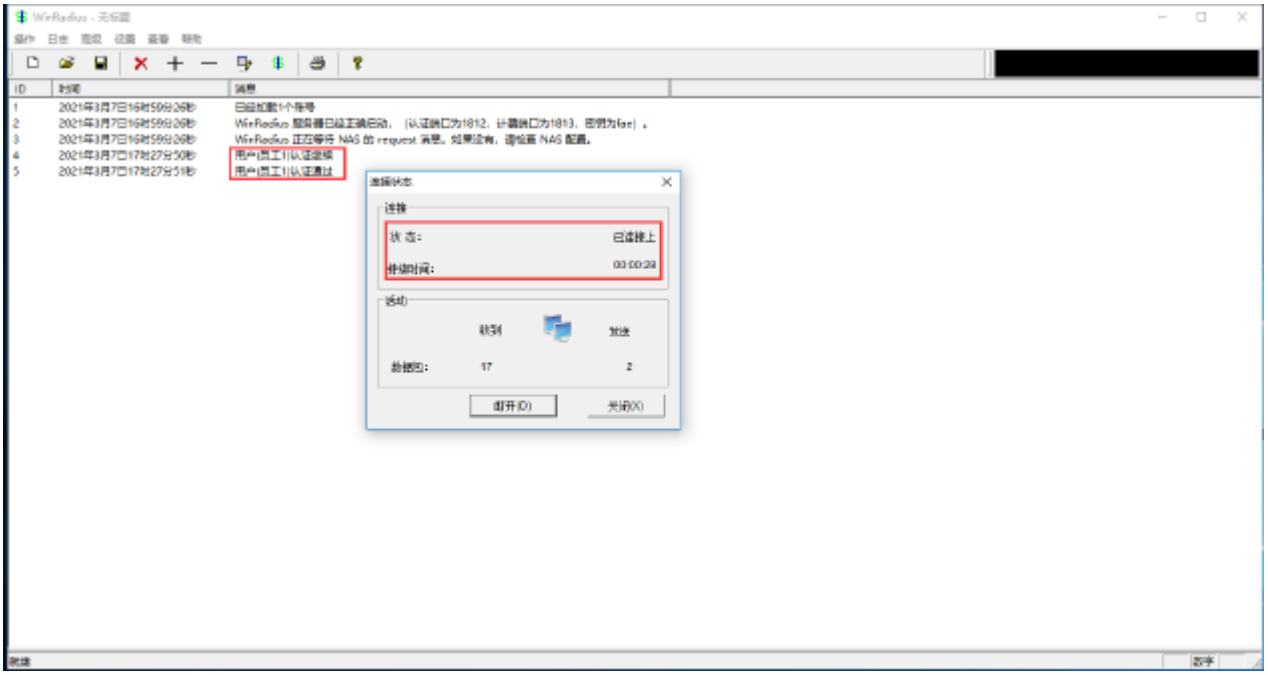
- 如果端口的“状态”处于禁用，则该端口下的设备不需要进行认证，始终处于接入网络的状态。
- 控制类型中，“基于 MAC”意味着该端口下的所有设备必须单独进行认证，认证通过后才能接入网络，“基于 Port”意味着该端口下只要有一台设备认证通过，其他设备不再需要认证也能接入网络。

5. 进入页面：网络安全 >> AAA >> 全局配置，开启 AAA 全局功能，便对接 Radius 服务器。

6. 进入页面：网络安全 >> AAA >> RADIUS 配置，配置”界面，配置交换机所对接的 Radius 服务器信息。点击<新增>，输入 RADIUS 服务器的 IP 地址、共享密钥、认证端口等信息。

7. 802.1X 认证客户端配置。本次以 WIN 10 电脑为例，在电脑上安装 TP-LINK 802.1X_V2.1 版客户端应用程序，配置参数默认，电脑接入交换机的端口客户端软件输入用户名账号和密码：员工 1/123456，选择对应连接交换机的网卡，电脑通过认证即可使用网络资源。





说明：

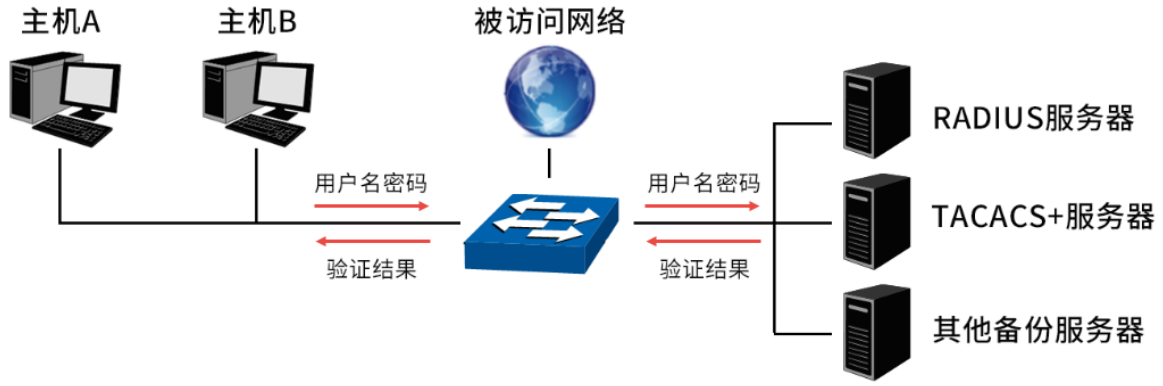
- 802.1X 客户端软件下载链接：https://service.tp-link.com.cn/detail_download_1266.html。

至此 802.1X 认证接入实现完成，局域网中所有电脑需要通过认证后才能访问局域网，从而实现了网络的安全接入。

10.9 AAA

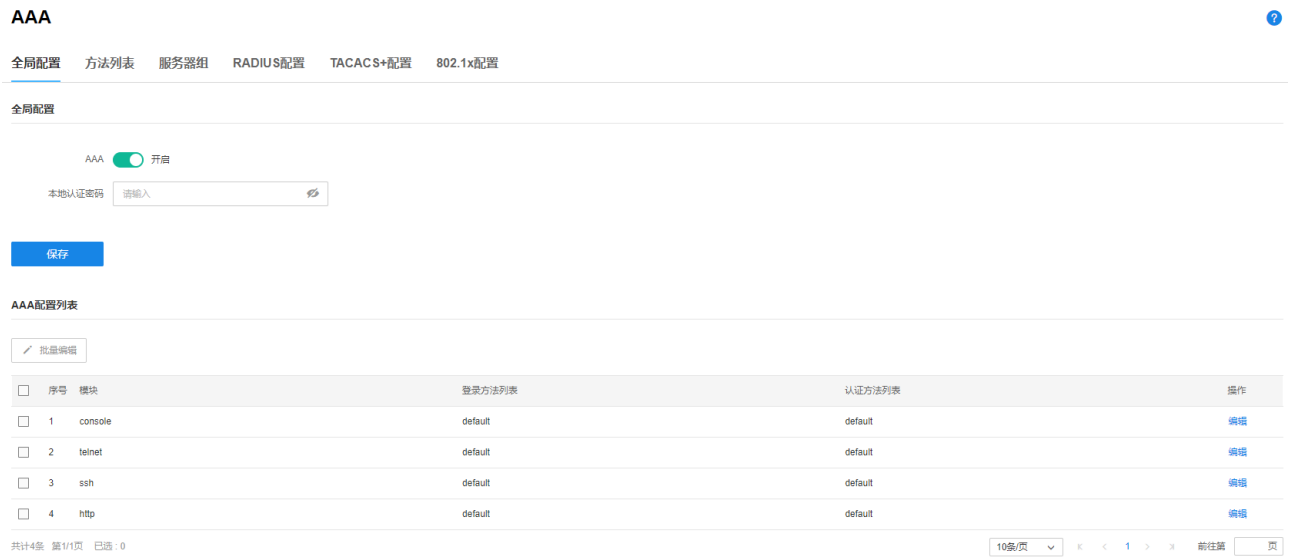
AAA 是认证、授权和计费（Authentication、Authorization、Accounting）三个英文单词的简称。主要用于对试图访问交换机或者获得访问权限的用户进行认证，管理具有访问权的用户可以获得哪些服务，如何对正在使用网络资源的用户进行计费。具体功能表现为：

1. 认证(Authentication)：验证用户是否可以获得访问权限；
2. 授权(Authorization)：授权用户可以使用哪些服务；
3. 计费(Accounting)：记录用户使用网络资源的情况。



10.9.1 全局配置

进入页面：网络安全 >> AAA >> 全局配置，开启 AAA 全局认证功能，输入正确的密码，才能通过认证，获得管理员权限，点击<保存>。



10.9.2 方法列表

这里允许配置一个用户自定义的或者系统默认的方法列表，使用户经过认证后可以登录交换机或者提升为管理员权限。登录方法列表指可以配置一个方法列表对登录交换机的用户进行认证。如果认证通过，采用远程认证的用户将获得一个 guest 用户权限。可以在使能管理员权限中提升用户的权限为管理员权限。认证方法列表指配置一个方法列表使经过认证的用户可以获得管理员权限。

进入页面：网络安全 >> AAA >> 方法列表，在登录方法列表或认证方法列表中点击<新增>，新建登录方法或认证方法。

方法列表名	输入方法列表的名字。
列表类型	选择一个方法列表类型。
方法一	首选方法。None 表示不需要认证；local 表示使用本地认证；radius 表示使用所有配置好的 RADIUS 服务器进行验证；tacacs 表示使用所有配置好的 TACACS+服务器进行认证。
方法二/方法三/方法四	备选方法。

10.9.3 服务器组

服务器组可以添加多个服务器 IP 作为一个认证集，交换机有两个默认的服务器组（radius 和 tacacs），它

们不可被修改，所有配置的服务器 IP 都会自动加入到对应的默认组。

进入页面：网络安全 >> AAA >> 服务器组，点击<新增>，输入服务器组和选择服务器组类型，点击<保存>。

10.9.4 RADIUS 配置

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）认证服务器为交换机提供认证服务，其存储有关用户的信息，包括用户名、密码以及其它参数，用于实现对用户进行认证、授权和计费。RADIUS 配置功能页面用来设置网络中认证服务器的参数，保证认证过程通畅有序的进行。

进入页面：网络安全 >> AAA >> RADIUS 配置，点击<新增>，输入 RADIUS 服务器信息，点击<保存>。

10.9.5 TACACS+配置

本页面可以配置 TACACS+（增强的终端接入控制系统）。

进入页面：网络安全 >> AAA >> TACACS+配置，点击<新增>，输入服务器信息，点击<保存>。

10.9.6 802.1X 配置

本页面可以配置用于 802.1X 认证的默认方法列表，默认方法支持 RAIDUS 服务组。

进入页面：网络安全 >> AAA >> 802.1X 配置。

10.10访问控制

10.10.1 应用介绍

随着网络规模的扩大以及流量的增加，如何有效地控制网络安全和分配带宽已成为网络管理的重要内容。ACL（Access Control List，访问控制列表）功能，通过配置报文的匹配规则和处理方式来实现对数据包的

过滤功能，从而有效防止非法用户对网络的访问。另外 ACL 功能也可以控制流量，节约网络资源。ACL 功能提供灵活的安全访问控制策略，对网络安全的控制提供了方便。

在交换机中，ACL 功能可以对数据包的 L2-L4 层的协议字段进行匹配。通过定义时间段可以设置 ACL 规则的生效时间；配置 policy 可以将 ACL 和动作组合起来，组成一个访问控制策略，对符合相应 ACL 规则的数据包进行控制，可添加的操作包括流镜像、流监控、QoS 重标记和端口重定向。

在 ACL 功能中，一个 ACL 可以包括多个规则，而每个规则可以针对数据包中特定字段内容进行匹配。在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，交换机将对该报文执行第一次匹配的规则指定的动作，以此来提高交换机的效率。

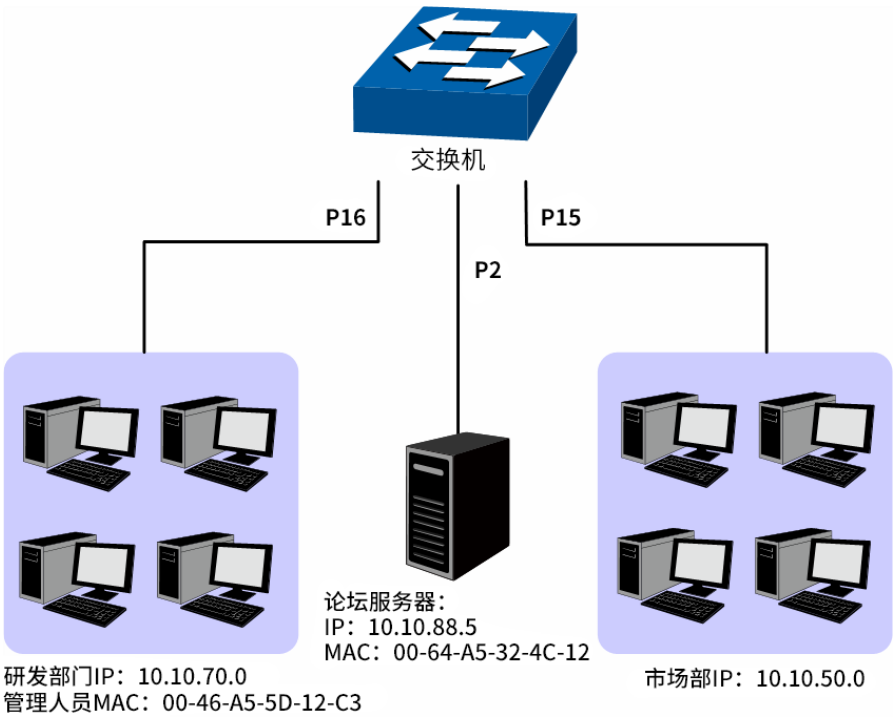
10.10.2 访问控制配置实例

组网需求：

某企业办公网络环境中，需要对内部办公电脑进行网络权限差异化设置，从而提升办公效率和网络安全，具体需求如下：

1. 研发部门的管理人员自由访问公司论坛，管理人员 MAC 地址为 00-64-A5-5D-12-C3。
2. 研发部门工作人员在工作时间可以访问公司论坛。
3. 市场部人员在工作时间不能访问公司论坛。
4. 市场部和研发部门之间互相不能访问。

拓扑图如下：



配置步骤：

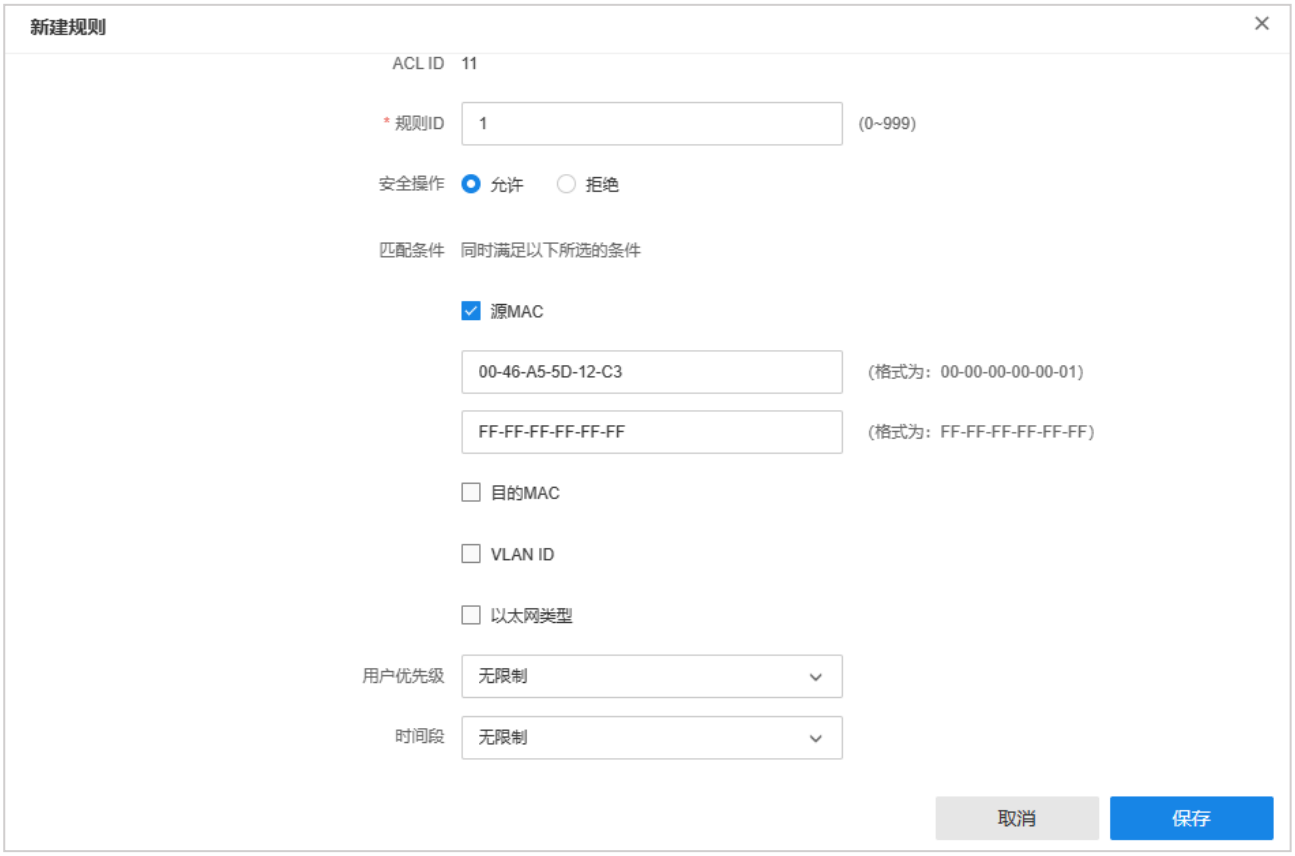
1. 配置时间段。进入页面：网络安全 >> 访问控制 >> 时间段配置，新建时间段，描述为 work_time。

时间段采用周期时间，周期时间选择工作日周一到周五，时间片段添加 08:00~18:00。

2. 配置需求 1。

进入页面：网络安全 >> 访问控制 >> ACL 配置 >> MAC 访问配置，创建 ACL 11。

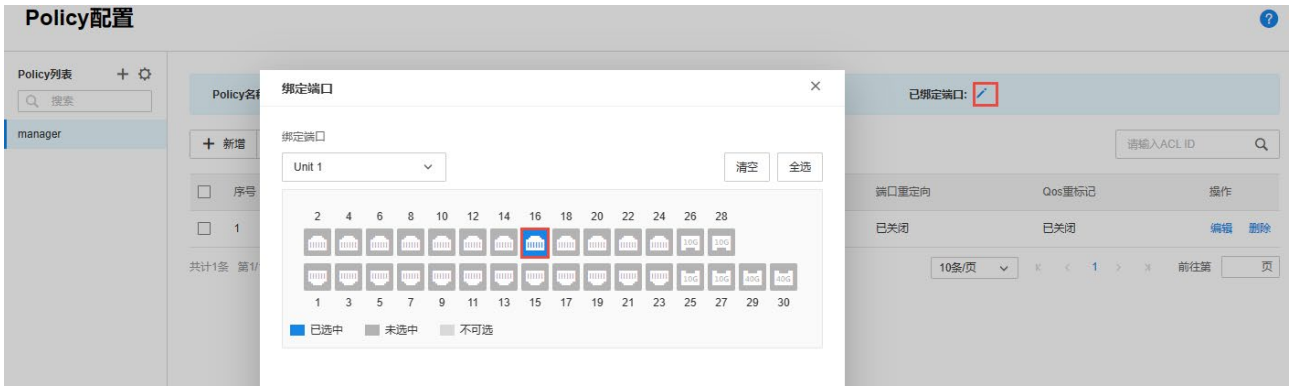
选择 ACL 11，创建规则 1，安全操作设置为允许；勾选源 MAC 设置为 00-46-A5-5D-12-C3，掩码为 FF-FF-FF-FF-FF-FF；时间段选择无限制。



进入页面：网络安全 >> 访问控制 >> Policy 配置，在 Policy 列表创建 Policy，名称定为 manager。

将 ACL 11 应用到 Policy manager。

将 Policy manager 与端口 16 绑定。



3. 需求 2、4 配置。

进入页面：网络安全 >> 访问控制 >> ACL 配置 >> 标准 IP 访问控制，创建 ACL 500。

选择 ACL 500，创建规则 1，安全操作设置为允许；设置源 IP 为 10.10.70.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.88.5，掩码为 255.255.255.255；时间段选择 work_time。

选择 ACL 500，创建规则 2，安全操作设置为丢弃；设置源 IP 为 10.10.70.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.50.0，掩码为 255.255.255.0；时间段选择无限制。

选择 ACL 500，创建规则 3，安全操作设置为丢弃；设置源 IP 为 10.10.70.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.88.5，掩码为 255.255.255.255；时间段选择无限制。

进入页面：网络安全 >> 访问控制 >> Policy 配置，在 Policy 列表中创建 Policy，名称设为 limit1。

将 ACL 500 应用到 Policy limit1，将 Policy limit1 与端口 16 绑定。

4. 需求 3、4 配置

进入页面：网络安全 >> 访问控制 >> ACL 配置 >> 标准 IP 访问控制，创建 ACL 501。

选择 ACL 501，创建规则 4，安全操作设置为丢弃；设置源 IP 为 10.10.50.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.70.0，掩码为 255.255.255.0；时间段选择无限制。

选择 ACL 501，创建规则 5，安全操作设置为丢弃；设置源 IP 为 10.10.50.0，掩码为 255.255.255.0；设置目的 IP 为 10.10.88.5，掩码为 255.255.255.255；时间段选择 work_time。

进入页面：网络安全 >> 访问控制 >> Policy 配置，创建 Policy，名称定为 limit2，将 ACL 501 应用到 Policy limit2，将 Policy limit2 与端口 15 绑定。


Policy配置
Policy列表
搜索
manager
limit1
limit2
Policy名称: limit2
已绑定VLAN: 无
已绑定端口: 1/0/15
新增
删除
清空
请输入ACL ID
序号
ACL ID
流镜像端口
流监管
端口重定向
Qos重标记
操作
1
501
已关闭
已关闭
已关闭
已关闭
编辑
删除

回目录

第11章 系统运维

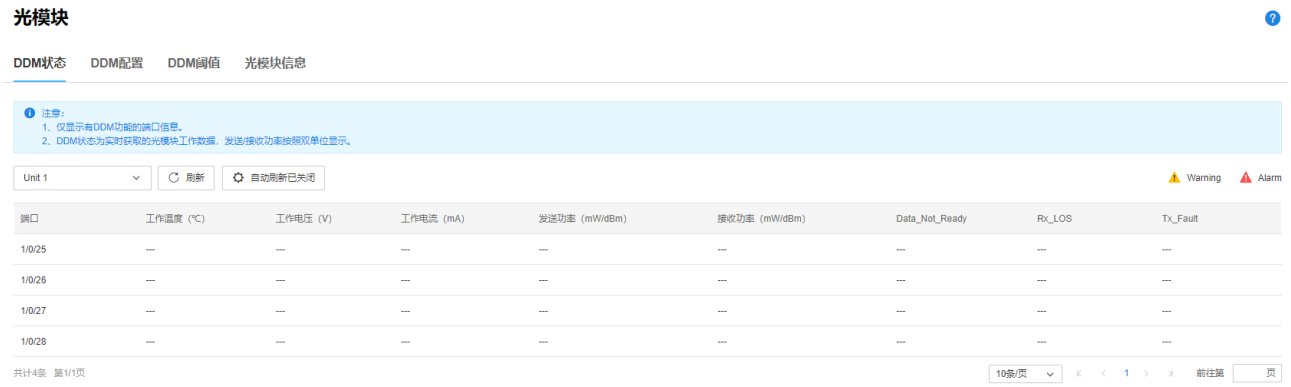
11.1 光模块管理

11.1.1 DDM 管理

DDM(Digital Diagnostic Monitoring)：数字诊断监控，通过读取光模块内部信息获取光模块的工作状态，从而确保光模块在正常工作。

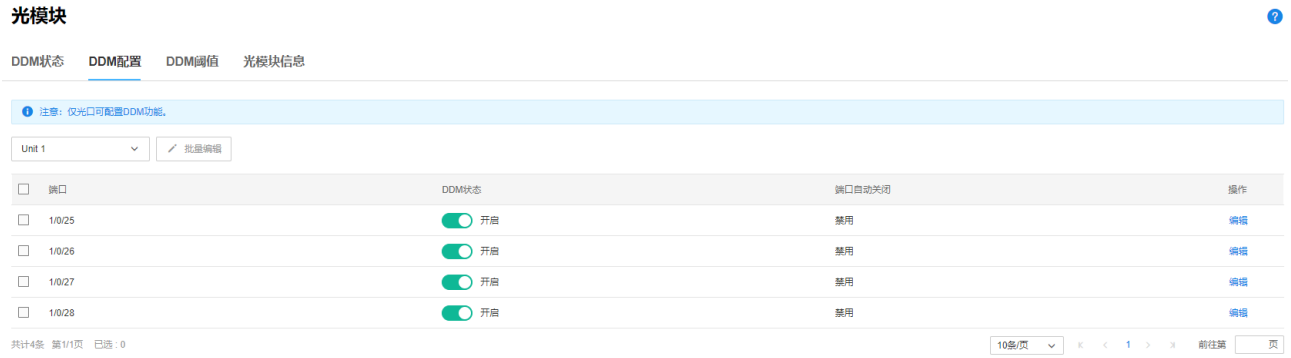
- **DDM 状态**

进入页面：状态监控 >> 光模块 >> DDM 状态，查看光模块的工作温度、工作电压、工作电流、发送功率，接受功率等。



- **DDM 配置**

进入页面：状态监控 >> 光模块 >> DDM 配置，选择端口是否开启 DDM 功能。



DDM 状态　选择端口是否开启 DDM 功能。选择“禁用”选项，将关闭该端口的 DDM 功能。选择“启用”选项，将打开该端口的 DDM 功能。

端口自动关闭	选择端口强制关闭的阈值条件。选择“Alarm 关闭”选项，该端口将在超过 Alarm 阈值时强制关闭。选择“Warning 关闭”选项，该端口将在超过 Warning 阈值时强制关闭。

- **DDM 阈值**

DDM 阙值为光模块厂商提供，发送/接收功率按照双单位显示。

进入页面的方法：状态监控 >> 光模块 >> DDM 阈值

11.1.2 光模块信息

通过读取光模块内部信息获取参数，从而获取光模块的基本信息。

进入页面的方法：状态监控 >> 光模块 >> 光模块信息

11.2 系统管理

11.2.1 用户管理

用户管理可以设置不同权限的账号来登录设备，不同的账号可以操作和查看的内容不一样，以达到保护交换机配置的目的。通过新增来创建普通用户/高级用户/操作员/管理员账号。

普通用户	可以查看交换机部分功能的配置情况；

高级用户	可以编辑、修改和查看交换机部分功能的配置；
操作员	可以编辑、修改和查看交换机大部分功能的配置；
管理员	可以编辑、修改和查看交换机各个功能的配置。

进入页面的方法：系统运维 >> 系统管理 >> 用户管理。

- **添加新用户**

点击<新增>，输入新用户名，输入旧密码，设置新密码。点击<保存>。

- **更改用户类别**

在已有的用户条目下，点击<编辑>，可更改用户类别。

- **修改用户密码**

点击<修改密码>，输入原始密码和新密码，点击<保存>。

11.2.2 启动配置

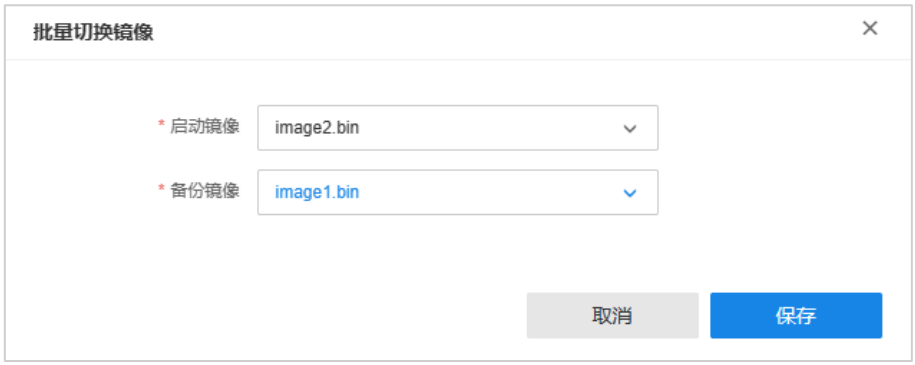
进入页面：系统运维 >> 系统管理 >> 系统工具 >> 启动配置，可以查看和修改交换机的启动配置参数。

交换机上电后用启动镜像启动，如果失败则尝试使用备份镜像启动。

交换机启动后会尝试读取启动配置，如果失败则读取备份配置。

点击<切换配置>，可修改对应的启动镜像及备份镜像，修改完成后，点击<保存>使配置生效。

点击<批量切换镜像>，选择启动镜像及备份镜像，点击<保存>，可批量修改镜像。



11.2.3 配置系统备份

通过配置系统备份，可以将交换机当前的启动配置保存到 PC 中，方便日后通过该文件恢复配置。

进入页面：系统运维 >> 系统管理 >> 系统工具 >> 导入/导出配置。点击<导出配置>，将系统配置文件保存到本地电脑。

11.2.4 还原系统配置

将以前备份的配置文件导入至交换机中，覆盖现在的系统配置。

进入页面：系统运维 >> 系统管理 >> 系统工具 >> 导入/导出配置。点击<选择文件>，从本地选择一个备份配置文件（后缀为 cfg），点击<导入>按钮，恢复交换机配置。

注意：

- 恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。
- 导入配置文件后，交换机将重启以使之生效。
- 如果您导入的配置文件有误，可能会导致交换机无法被管理。

11.2.5 重启系统

通过软件界面进行设备重启操作。

进入页面：系统运维 >>系统管理 >> 系统工具 >> 系统重启，选择成员，点击<重启>。

重启前请注意保存配置。

11.2.6 恢复出厂设置

进入页面：系统运维 >> 系统管理 >> 系统工具 >> 恢复出厂，点击<恢复出厂>。

恢复出厂配置后需重新配置交换机。

注意：

软件复位后，交换机配置将恢复成出厂默认状态，用户配置数据将丢失。

11.2.7 软件升级

进入页面：系统运维 >> 系统管理 >> 系统工具 >> 软件升级，可查看设备当前硬件及软件版本，并对设备进行本地或在线升级。

在线升级

在交换机能够连接互联网的情况下， 可通过在线监测给设备升级。点击<检测新版本>，如检测到更新软件，点击<升级>按钮对设备进行升级。升级完成后，设备将自动重新启动。

本地升级

通过导入升级文件，给主镜像或备份镜像升级。

请前往 TP-LINK 资料中心，输入设备型号及硬件版本，下载最新版本的系统文件。

选择需要升级的镜像，点击<选择文件>从本地选择升级软件，点击<升级>。

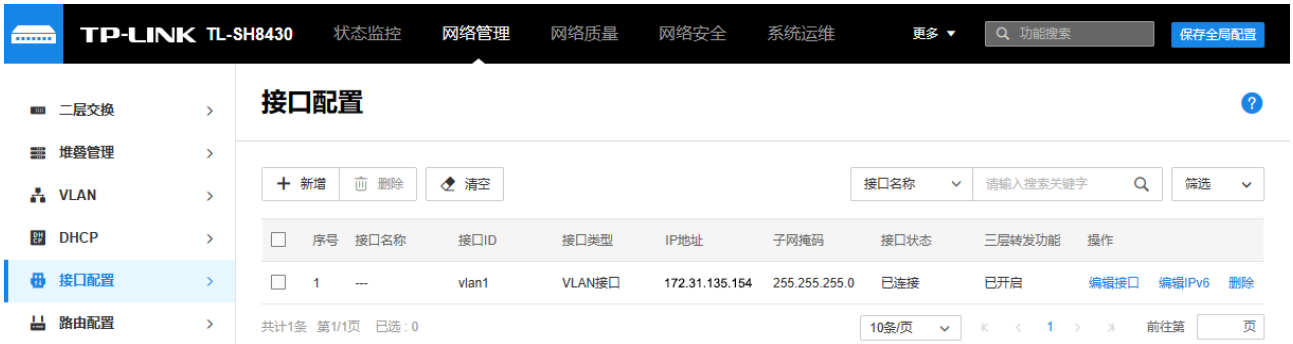
升级完成后，设备将自动以新镜像重新启动。

11.2.8　云管理

TP-LINK 全新推出的三层网管交换机都支持云管理，开启云管理之后设备可以实现远程统一管理和部署。本小节将介绍三层网管交换机连接 TP-LINK 商用云平台及商用管理系统的配置方法。

设备联网

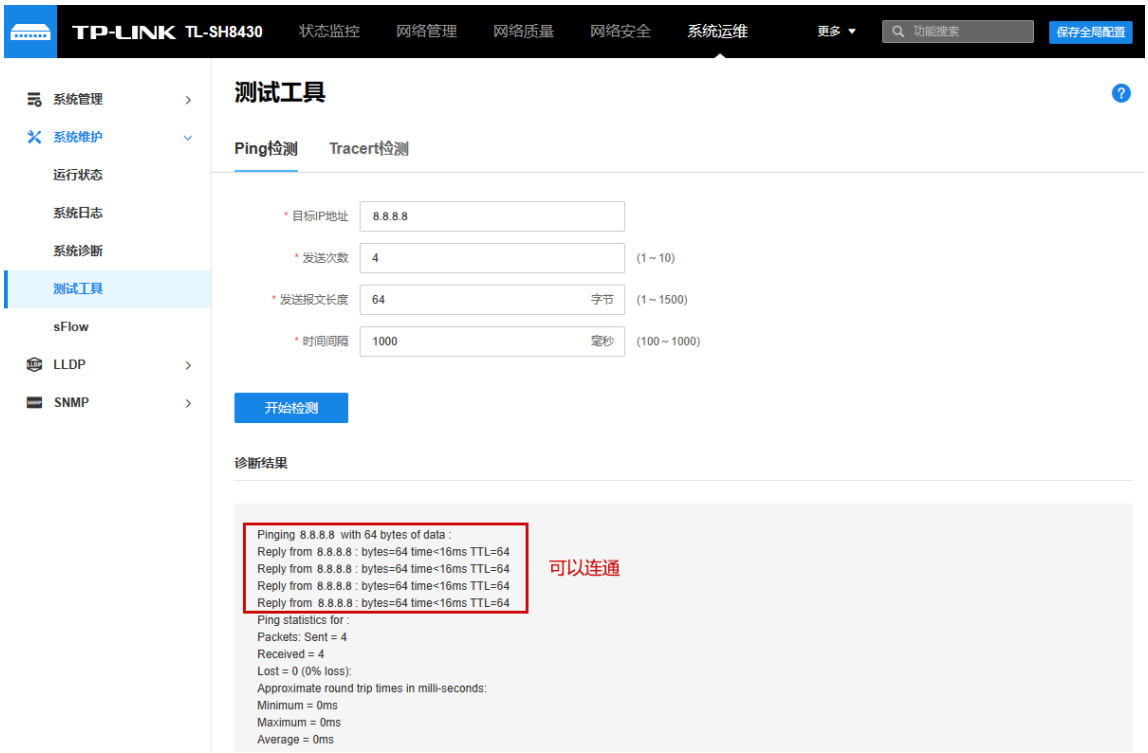
进入交换机管理页面：网络管理 >> 接口配置，配置交换机设备 VLAN1（管理 VLAN，即对接前端路由器的 VLAN）的接口 IP 地址，使接口 IP 地址和前端路由器地址在同一个网段：



进入页面：系统运维 >> 云管理 >> DNS 配置，确认设备的 DNS 服务器地址填写正确，交换机默认填写了两条 DNS 地址：

进入页面：网络管理 >> 路由配置 >> 静态路由 >>IPv4 静态路由条目，配置一条全 0 的静态路由，下一跳指向前端路由器 LAN 接口：

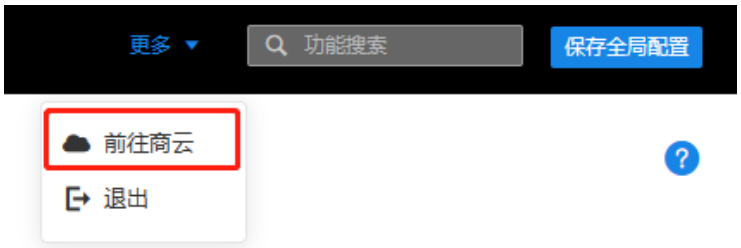
进入页面：系统运维 >> 系统维护 >> 测试工具 >> Ping 检测，检查设备是否可以正常联网，一般 Ping DNS 服务器：



TP-LINK 商用云平台

1. 进入页面：系统运维 >> 云管理 >> 全局配置，启用交换机的云管理功能，并选择 TP-LINK 商用云平台。

2. 点击页面右上角<更多>，选择前往商云，进入 TP-LINK 商用云平台，登录 TP-LINK ID 账号，进入“设备”页面，选择<添加网络设备>，使用设备 ID 或 MAC 地址将交换机添加到商用云平台。



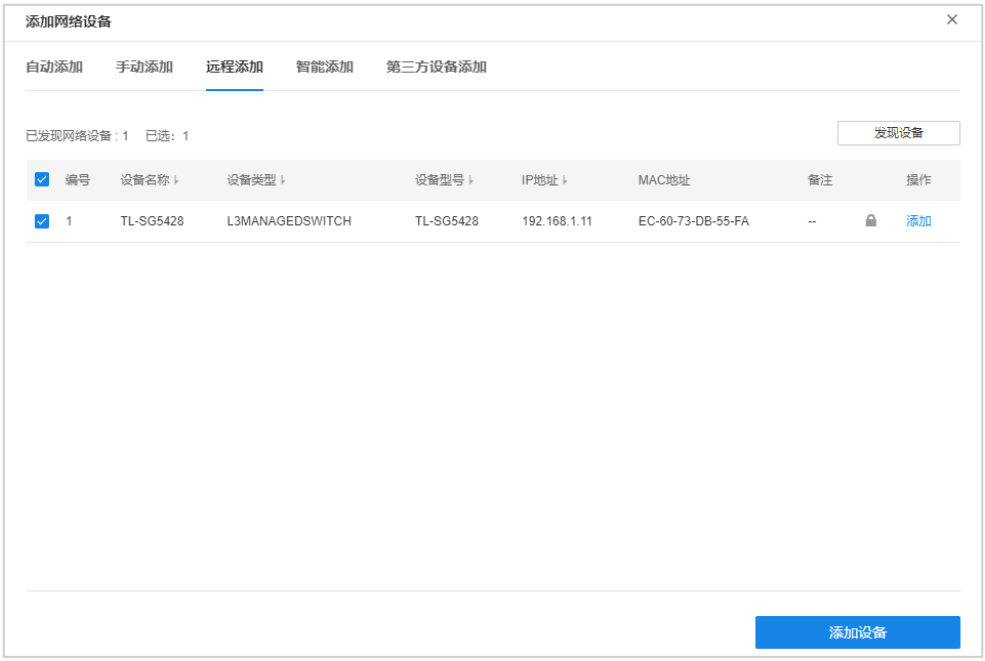
3. 设备上云后即可在列表中查看，点击<远程管理>即可管理设备。

TP-LINK 商用管理系统（TUMS）

1. 在 TUMS 服务器管理页面设置服务器广域网地址，在路由器设置端口映射。

2. 进入交换机管理页面：系统运维 >> 云管理 >> 全局配置，开启云管理功能，选择 TP-LINK 商用管理系统（TUMS），填写 TUMS 服务器地址（公网 IP 或域名）及设备接入端口号。

3. 在 TUMS 服务器远程添加页面，点击<发现设备>，TUMS 服务器会自动发现可以连接的设备。在已发现设备列表中点击<添加>，按照弹框提示输入交换机的用户名及密码，即可完成设备添加。



4. 在 TUMS 服务器端，进入页面：设备 >> 设备列表，点击<远程配置>即可进入对应设备的远程配置界面。

11.2.9 系统时间

本页面用来配置交换机的系统时间。系统时间是交换机工作时使用的时间，其它功能（如访问控制）中的时间信息以此处为准。可以选择手动设置时间或者连接到一个 NTP（网络时间协议）服务器获取 UTC 时间，也可以获取当前管理 PC 的时间作为交换机的系统时间。

进入页面的方法：系统运维 >>系统管理 >>系统时间

条目介绍：

- **时间信息**

当前时间	显示交换机当前的日期、时间。

- **校时方式**

手动校时	勾选后，手动配置日期、时间。 同步计算机时间：点击即可获取管理主机的时间配置，再进行提交即可。
NTP 自动校时	勾选后，配置时区和 NTP 服务器的 IP 地址，交换机将自动获取 UTC 时间。此时交换机必须连接至 NTP 服务器。 ● 时区：选择所在的时区。 ● 首选/备选 NTP 服务器：填写 NTP 服务器的 IP 地址。 ● 时间获取周期：设定从 NTP 服务器获取时间的周期。有效范围为 1~24。

注意：

- 如果向指定的时间服务器请求时间不成功，交换机会选择向上一次成功获取时间的服务器地址和网络上默认的公用时间服务器地址来获取时间。

11.2.10 管理口配置

管理端口是一个专门的以太网端口，用于设备的带外管理。这个端口的流量是与运行于交换机端口的流量隔离，不能被交换或路由到工作网络，该页面用来配置管理口的端口、IP 信息，以及显示管理口的工作状

态。

进入页面的方法：系统运维 >>系统管理>>管理口配置

条目介绍：

- **端口配置**

  自动协商： 选择是否开启自动协商。

  速率： 当“自动协商”关闭时，在此设置管理口的工作速率。

  双工： 当“自动协商”关闭时，在此设置管理口的双工模式。

- **IP 配置**

  IP 地址： 设置管理口的 IP 地址。

  子网掩码： 设置管理口的子网掩码。

- **管理口状态**

  接口名称： 显示管理口的接口名称。

连接状态： 显示管理口的连接状态。

速率信息： 显示管理口的速率与双工状态。

11.3 安全管理

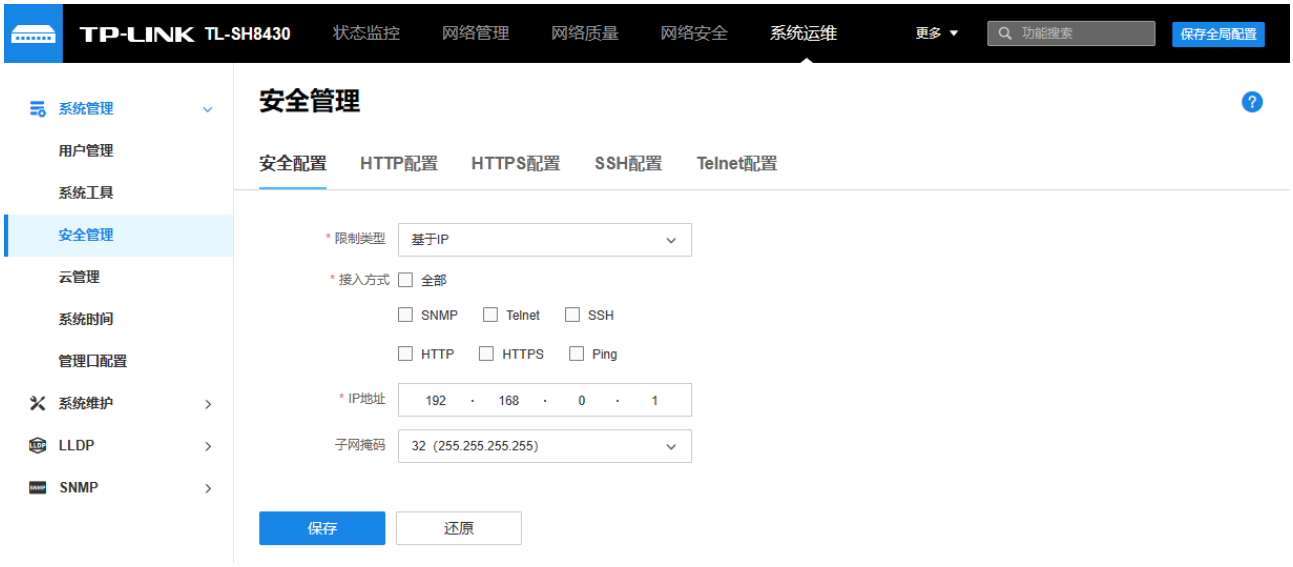
安全管理功能是针对不同的远程登录方式，采取相应的安全措施，以增强用户管理交换机的安全性。其中，管理员、操作员、高级用户及普通用户的定义请参考 **12.2.1 用户管理**。

本功能包括**安全配置**、**HTTP 配置**、**HTTPS 配置**、**SSH 配置**和 **Telnet 配置**五个配置界面。

11.3.1 安全配置

安全配置用来限制管理交换机的用户属性，配置白名单用户，只有在白名单内的用户才可以以固定的方式访问设备，以达到保护交换机配置的目的。

进入页面：系统运维 >> 系统管理 >> 安全管理 >> 安全配置，选择限制类型及接入方式，设置完成后点击<保存>使配置生效。



限制类型 支持基于 IP/MAC/端口三种白名单方式限制用户访问设备，选择了对应的限制类型后只有这个类型的对应 IP/MAC/端口才能访问设备。

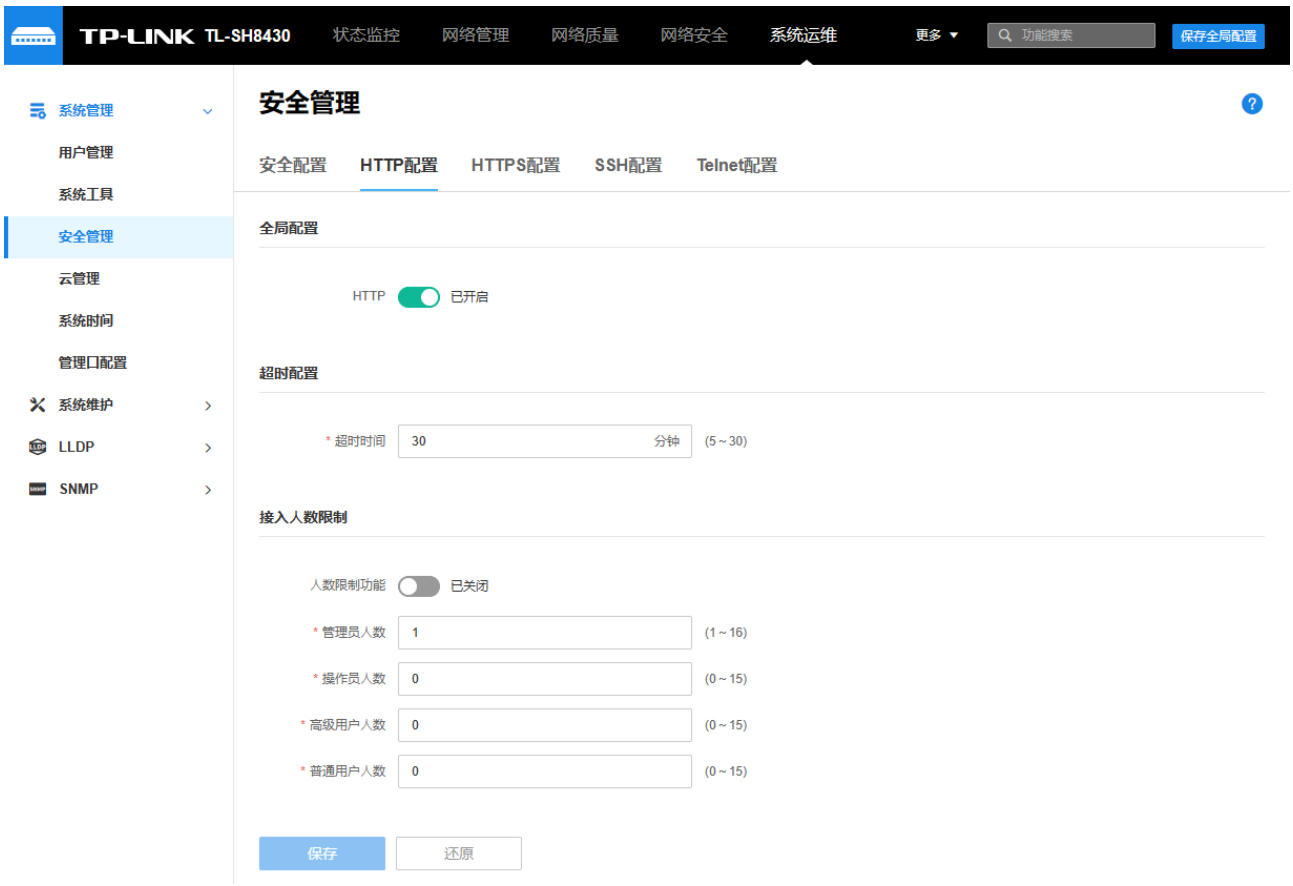
接入方式 针对对应限制类型的终端指定访问交换机的方式，勾选了对应方式后，限制类型的终端只能以这个方式访问设备。

11.3.2 HTTP 配置

通过 HTTP（HyperText Transfer Protocol，超文本传输协议），可以使用户在浏览器上管理交换机。 HTTP 标准是由互联网工程任务组（Internet Engineering Task Force）和万维网联盟（World Wide Web

Consortium）共同合作研究的成果。本页可以配置 HTTP 功能。

进入页面的方法：系统运维 >> 系统管理 >> 安全管理 >> HTTP 配置



条目介绍：

- **全局配置**

HTTP 功能	选择是否开启交换机的 HTTP 功能。

- **超时配置**

超时时间	如果在超时时间之内没有对交换机管理页面进行操作，系统会自动退出管理页面，若要再次进行管理请重新登录。

- **接入人数限制**

人数限制功能	选择是否启用人数限制功能。
管理员人数	填写可同时登录交换机 Web 页面的管理员总数。
操作员人数	填写可同时登录交换机 Web 页面的操作员总数。
高级用户人数	填写可同时登录交换机 Web 页面的高级用户总数。
普通用户人数	填写可同时登录交换机 Web 页面的普通用户总数。

11.3.3 HTTPS 配置

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，它为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 采用非对称加密技术，用密钥对进行信息的加密/解密，密钥对由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名证书）和对应私钥，用户也可以通过证书/密钥导入功能替换默认的密钥对。

SSL 协议广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输，多使用在电子商务、网上银行等领域，为网络上数据通讯提供安全性保证。

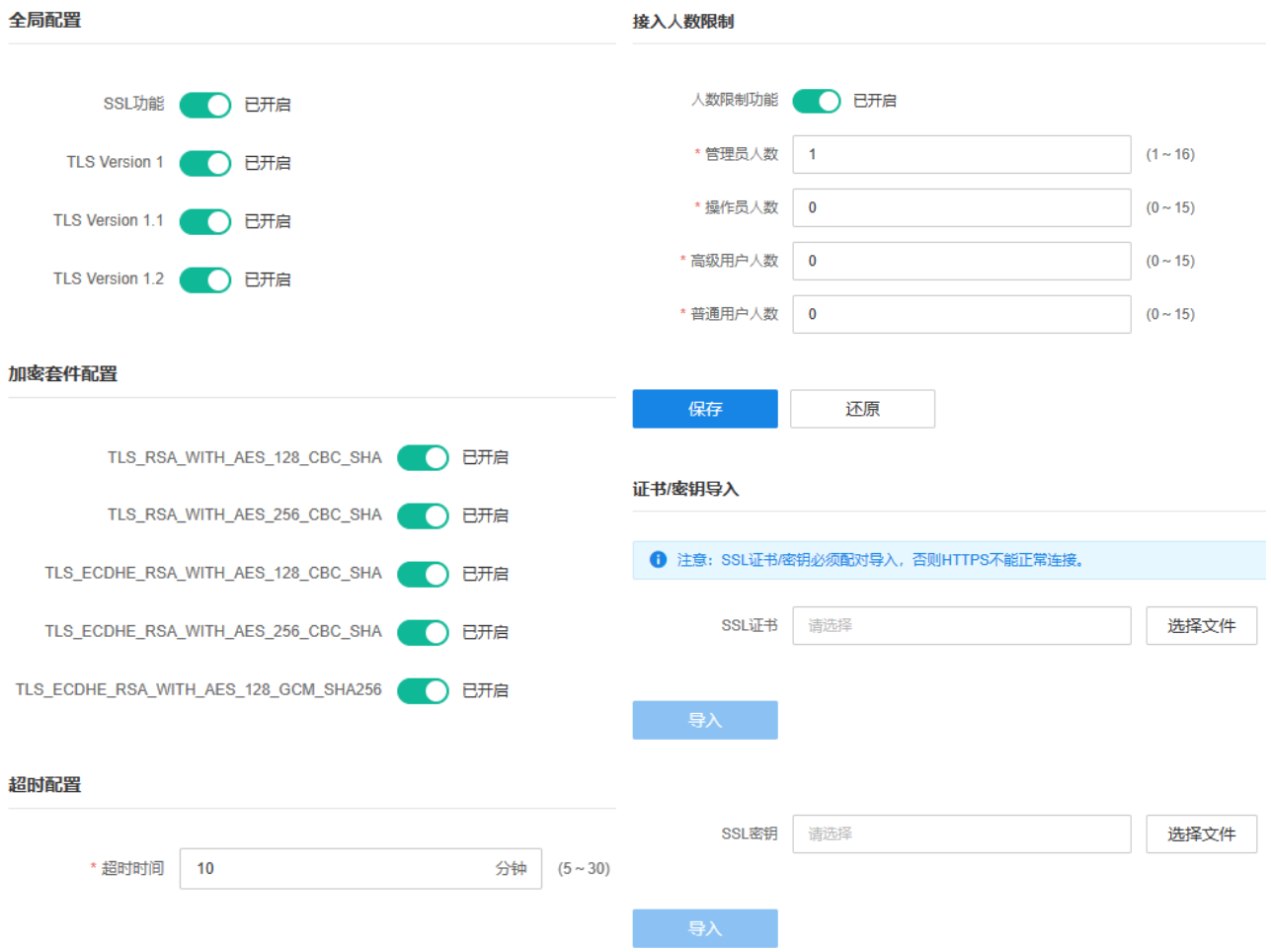
SSL 协议提供的服务主要有：

1. 对用户和服务器进行基于证书的身份认证，确保数据发送到正确的用户和服务器；
2. 对传输数据进行加密，以防止数据中途被窃取；
3. 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 采用非对称加密技术，使用“密钥对”进行数据的加密/解密，“密钥对”由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名）和对应私钥，也可以通过证书/密钥导入功能替换默认的密钥对，但 SSL 证书/密钥必须配对导入，否则 HTTPS 不能正常连接。

本功能生效后，即可通过 https://192.168.0.1 登录交换机的 Web 页面。初次使用交换机默认的证书通过 HTTPS 登录交换机时，浏览器可能会提示“该证书是自签名的而不被信任”或“证书错误”，此时请将此证书添加为信任证书，或者继续浏览此网站即可。

进入页面的方法：系统运维 >> 系统管理 >> 安全管理 >> HTTPS 配置。



条目介绍：

- **全局配置**

HTTPS	选择是否开启交换机的 HTTPS 功能。
SSL Version 3	可以在此选择是否开启 SSL 3.0。默认开启
TLS Version 1	可以在此选择是否开启 TLS1.0。默认开启。
TLS Version 1.1	可以在此选择是否开启 TLS1.1。默认开启。
TLS Version 1.2	可以在此选择是否开启 TLS1.2。默认开启。

- **加密套件配置**

RSA_WITH_RC4_128_MD5	通过 RC4 128-bit 加密进行密钥交换，消息摘要采用 MD5。默认开启。
RSA_WITH_RC4_128_SHA	通过 RC4 128-bit 加密进行密钥交换，消息摘要采用 SHA。默认开启。
RSA_WITH_DES_CBC_SHA	通过 DES_CBC 加密进行密钥交换，消息摘要采用 SHA。默认开启。
RSA_WITH_3DES_EDE_CBC_SHA	通过 3DES_EDE_CBC 加密进行密钥交换，消息摘要采用 SHA。默认开启。

- **超时配置**

超时时间	如果在超时时间之内没有对交换机管理页面进行操作，系统会自动退出管理页面，若要再次进行管理请重新登录。

- **接入人数限制**

人数限制功能	选择是否启用人数限制功能。
管理员人数	填写可同时登录交换机 Web 页面的管理员总数。
操作员人数	填写可同时登录交换机 Web 页面的操作员总数。
高级用户人数	填写可同时登录交换机 Web 页面的高级用户总数。
普通用户人数	填写可同时登录交换机 Web 页面的普通用户总数。

- **证书导入**

SSL 证书	选择要导入的 SSL 证书。证书必须为 BASE64 编码格式。

- **密钥导入**

SSL 密钥	选择要导入的 SSL 密钥。密钥必须为 BASE64 编码格式。

注意：

- SSL 证书/密钥必须配对导入，否则 HTTPS 不能正常连接。
- 要使用 HTTPS 建立安全连接，必须在浏览器的地址栏指定“https://提示符”。
- HTTPS 连接涉及身份认证、加密、解密等过程，故响应速度可能会比普通的 HTTP 连接稍慢。

11.3.4 SSH 配置

SSH（Secure Shell，安全外壳）是由 IETF（Internet Engineering Task Force，因特网工程任务组）所制定，建立在应用层和传输层基础上的安全协议。SSH 加密连接所提供的功能类似于一个 telnet 连接，但是传统的 telnet 远程管理方式在本质上是不安全的，因为它在网络上是使用明文传送口令和数据的，别有用心的人可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境远程登录到设备时，SSH 功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

SSH 是由服务器端和客户端组成的，并且有 V1 和 V2 两个不兼容的版本。在通讯过程中，SSH 服务器与客户端会自动互相协商 SSH 版本号和加密算法，协商一致后，由客户端向服务器端发起请求登录的认证请

求，认证通过后双方即可进行信息的交互。本交换机支持 SSH 服务器功能，可以使用 SSH 客户端软件通过 SSH 连接方式登录交换机。

SSH 密钥导入是将 SSH 的公钥文件导入至交换机中。如果密钥导入成功，交换机会优先选用密钥认证的方式接受 SSH 登入。

进入页面的方法：系统运维 >> 系统管理 >> 安全管理 >> SSH 配置。

条目介绍：

- **全局配置**

SSH 功能	选择是否启用 SSH 功能。
Protocol V1	选择是否启用对 SSH V1 的支持。
Protocol V2	选择是否启用对 SSH V2 的支持。
静默时长	填写静默时长。该时间内客户端无任何操作时，连接会自动断开。
最大连接数	填写 SSH 同时可允许的最大连接数，连接数若满，将无法再建立新的连接。

- **加密算法**

  勾选复选框，启用相应的加密算法。

- **数据完整性算法**

  勾选复选框，启用相应的数据完整性算法。

- **密钥导入**

密钥类型	选择所要导入的密钥类型。支持 SSH-1 RSA,SSH-2 RSA 和 SSH-2 DSA 三种类型的密钥。
密钥文件	选择要导入的密钥文件。
导入密钥	点击此按键，将所选的 SSH 密钥导入交换机。

注意：

- 请确保导入的文件是密钥长度为 512 至 3072 比特的 SSH 公钥。
- 导入密钥文件后，交换机中此用户原有的同类型密钥将会被覆盖。如果导入的密钥文件有误，SSH 会转用密码认证的方式登录。

11.3.5 Telnet 配置

进入页面：系统运维 >> 系统管理 >> 安全管理 >> Telnet 配置，可选择启用/禁用交换机的 Telnet 功能。

11.4 系统维护

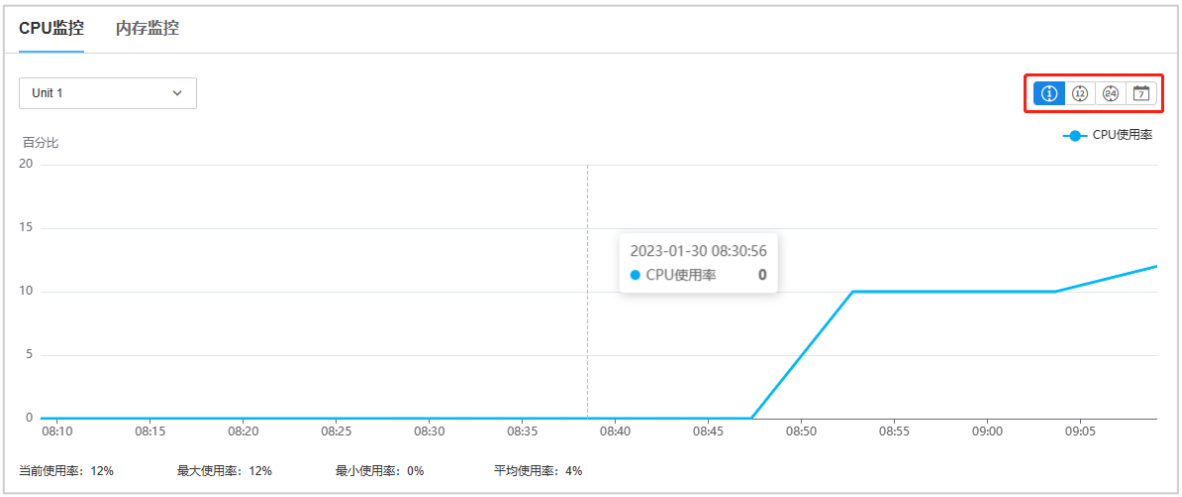
11.4.1 运行状态

在本功能中可以通过曲线数据监控交换机 CPU 和内存的使用情况，CPU 和内存使用率应该在一定数值上下波动。当 CPU 和内存使用率波动较大且明显增大时，请检查网络是否受到攻击。

本功能包括 CPU 监控和内存监控两个配置页面。

CPU 监控

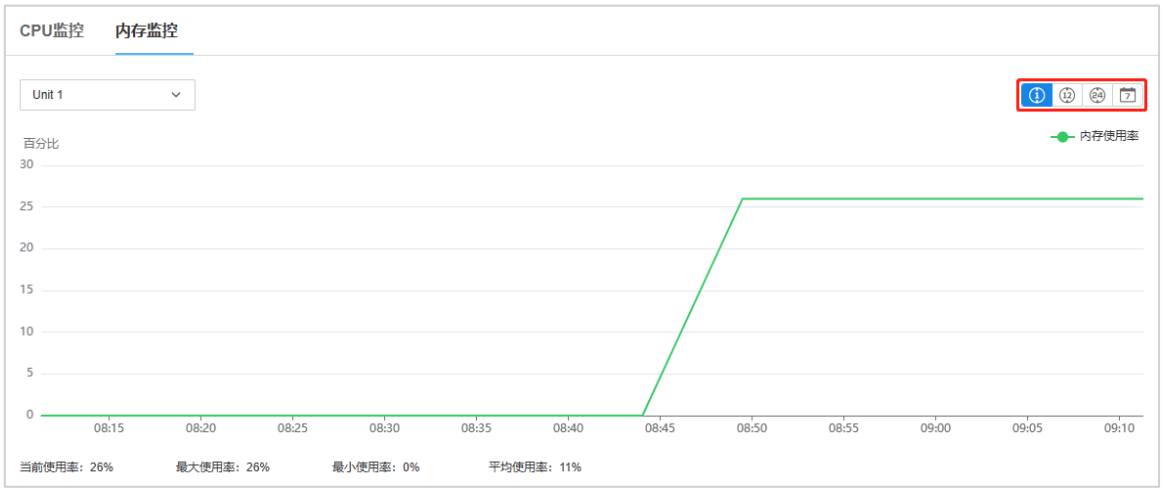
进入页面的方法：系统运维 >> 系统维护 >> 运行状态 >> CPU 监控



点击右上角可查看近 1H/12H/24H/7 天的 CPU 运行状态信息。

内存监控

进入页面的方法：系统运维 >> 系统维护 >> 运行状态 >> 内存监控



点击右上角可查看近 1H/12H/24H/7 天的内存状态信息。

11.4.2 系统日志

交换机提供的日志系统能够对所有的系统信息进行记载、分类、管理，为网络管理员监控设备运行情况和诊断设备故障提供强有力的支持。

本交换机的系统日志分为八个等级，如下表所示。

级别名称	严重等级	描述
emergencies	0	系统不可用信息
alerts	1	需要立刻做出反应的信息
critical	2	严重信息
errors	3	错误信息
warnings	4	警告信息
notifications	5	正常出现但是重要的信息
informational	6	需要记录的通知信息
debugging	7	调试过程产生的信息

本功能包括**日志列表**、**本地日志配置**和**远程日志配置**三个配置页面。

日志列表

系统日志可以保存到两个不同的地方：日志缓冲区和日志文件。日志缓冲区的日志信息在交换机重启后将会丢失，日志文件里的日志信息在交换机重启后仍然有效。日志列表显示了日志缓冲区中的系统日志信息。

进入页面的方法：系统运维 >> 系统维护 >> 系统日志 >> 日志列表

条目介绍：

- **系统日志列表**

序号	显示该日志信息的序号。
时间	显示该日志信息的发生时间。需先在**系统管理>>系统配置>>系统时间页面**进行配置后，系统日志才能获取到正确的时间。
功能模块	显示该日志信息所属功能模块，从下拉列表可选择显示某一模块的日志信息。
严重级别	显示该日志信息的严重级别，从下拉列表选择某一级别，可显示小于或等于该级别值的日志信息。
日志信息	显示该日志信息的内容。
导出日志	将日志文件手动导出。将系统日志信息以文件的形式导出，可供设备诊断和统计分析使用。

注意：

- 严重级别划分为 0-7 共八个等级，级别值越小，紧急程度越高。
- 本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为 1024 条。
- 导出日志文件可能需要较长时间，此期间请耐心等待，不要对设备进行其他操作。

本地日志配置

本地日志是指保存在本设备上的系统日志信息。本地日志有两个输出方向，即可以保存到两个不同地方：日志缓冲区和日志文件。

进入页面的方法：系统运维 >> 系统维护 >> 系统日志 >> 本地日志配置

条目介绍：

- **系统日志列表**

  输出方向　显示日志输出方向。

  - 日志缓冲区：日志缓冲区是用于保存系统日志的一块内存区域。缓冲区中的信息在“日志列表”页面上进行显示，在断电重启后这些信息将会丢失。
  - 日志文件：日志文件是 Flash 里的一块存储区域。日志文件的信息在断电重启后不会丢失，可通过导出日志文件来查看。

  严重等级　限定各个输出方向上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会进行输出。

  启用状态　选择启用或禁用该输出方向。

  同步频率　日志信息写入日志文件的时间间隔。

远程日志配置

远程日志功能可以将本交换机的系统日志发送到日志服务器上。日志服务器相当于一个可维护的共用消息区，它可以对网络中各设备产生的日志信息进行集中的监控和管理。

进入页面的方法：系统运维 >> 系统维护 >> 系统日志 >> 远程日志配置

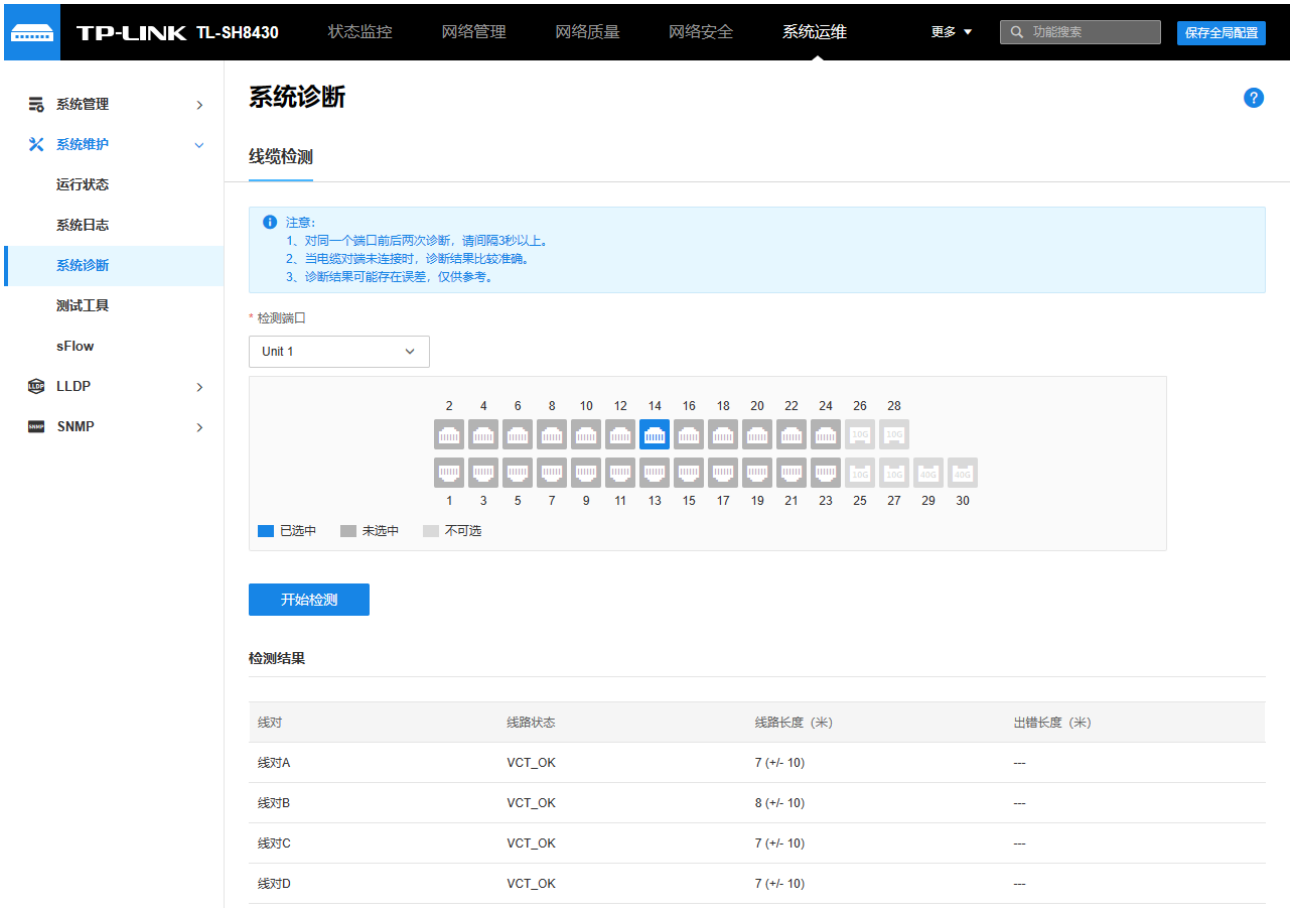
条目介绍：

- **日志服务器**

序号	日志服务器序号。本交换机共支持 4 个日志服务器。
服务器 IP	配置日志服务器的 IP 地址。
UDP 端口号	发送/接收系统日志时所用到的 UDP 端口号，这里使用标准的 514 端口。
严重级别	限定发往各个服务器上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会发送到相应的服务器。
状态	启用/禁用该服务器。

11.4.3 线缆诊断

当交换机端口与线缆连接时，线缆检测功能可以检测出该线缆连接状态、长度范围或出错长度，便于对网络故障进行定位。



条目介绍：

- **检测端口**

  选择要进行线缆检测的端口，点击<开始检测>。

- **检测结果**

线对	显示线对序号。
线路状态	检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。 • 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。 • 短路：线路金属内芯互相接触，导致短路。 • 阻抗失配：网线质量问题。
线路长度	若线路为正常状态，显示该线缆的长度范围。
出错长度	若线路为短路、开路或阻抗失配状态，则显示该线缆的出错长度。

注意：

- 对同一个端口前后两次诊断，请间隔 3 秒以上。
- 当电缆对端未连接时，诊断结果会较为准确。
- 这里的长度是指线缆绕对的长度，不是线缆表皮的长度，线缆检测的长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

11.4.4 测试工具

交换机提供了 Ping 检测和 Tracert 检测功能。

Ping 检测

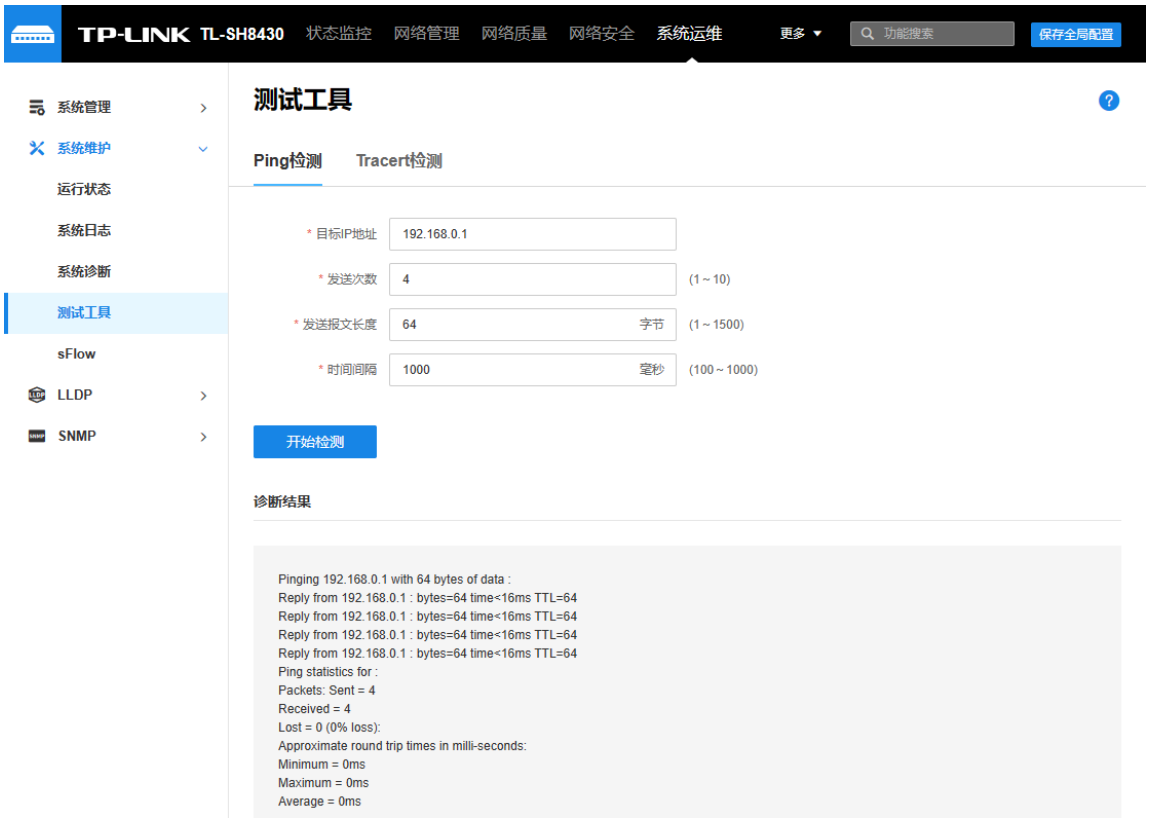
Ping 检测功能可以检测交换机与某网络设备是否可达，方便网络管理员检查网络的连通性，定位网络故障。

Ping 检测过程如下：

1) 交换机向目标设备发送 ICMP 请求报文；

2) 如果网络工作正常，则目标设备在接收到该报文后，向交换机返回 ICMP 应答报文；显示相关统计信息；

3) 如果网络工作异常，源设备将显示目的地址不可达或超时等提示信息。



条目介绍：

- **Ping 检测**

目标 IP 地址	填写需要测试的目标节点的 IP 地址。支持 IPv4 地址。
发送次数	填写 Ping 检测时发送的检测包次数。建议使用缺省值。
发送报文长度	填写 Ping 检测时发送的检测包长度。建议使用缺省值。
时间间隔	交换机发送检测包后，在此时间间隔内如果没有收到回复，则重新发送检测包，直到所发送的检测包达到所设置的发送次数。建议使用缺省值。

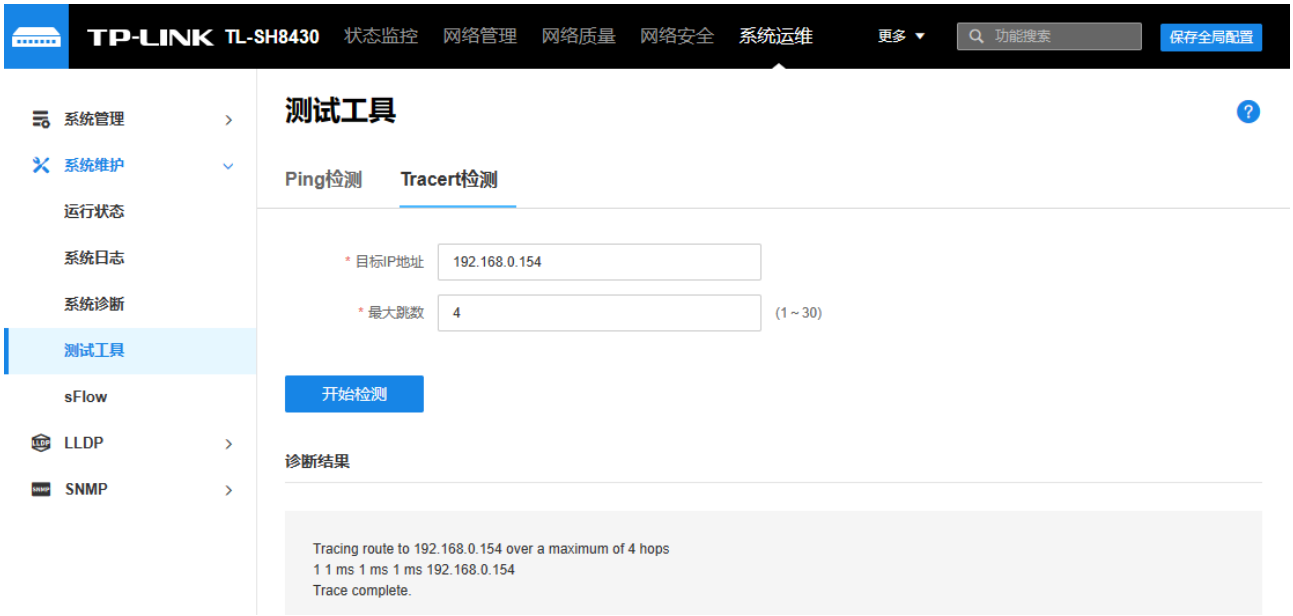
Tracert 检测

Tracert 检测可以查看交换机到目标节点所经过的路由器。当网络出现故障时，使用该命令可以分析出现故障的网络节点。

在 IP 数据包首部中包含一个 TTL 字段，当数据包在网络中转发时，每经过一个路由 TTL 字段的值减 1。当接收的 IP 数据包的 TTL 字段为 0 或 1 时，路由器将此数据包丢弃，并给发送源回复一个 ICMP 超时报文。这样能有效防止数据包在网络发生故障时，无休止地在网络中流动。

Tracert 检测过程如下：

1) 交换机发送一个 TTL 为 1 的报文给目的设备；
2) 第一跳（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），这样交换机就得到了第一个路由器的地址；
3) 交换机重新发送一个 TTL 为 2 的报文给目的设备；
4) 第二跳回应一个 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；
5) 重复以上过程直到最终到达目的设备，交换机就得到了从它到目的设备所经过的所有路由器的地址。



条目介绍：

- **Tracert 检测**

目标 IP	填写目的设备的 IP 地址。支持 IPv4 地址。
最大跳数	填写测试报文发送的最大跳数。

11.4.5 sFlow

采样流 sFlow（Sampled Flow）是一种基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。sFlow 系统包含一个嵌入在设备中的 sFlow 代理和远处的 sFlow 接收端。

本功能包括**全局配置**、**sFlow 接收端**和 **sFlow 采样端**三个功能页面。

全局配置

选择是否启用 sFlow 功能，并配置 sFlow 代理 IP 地址，sFlow 代理 IP 用于指定 sFlow 报文的源 IP。

进入页面的方法：系统运维 >> 系统维护 >> sFlow >> 全局配置

条目介绍

sFlow	选择是否启用交换机上的 sFlow 功能。
代理 IP 地址	sFlow 代理的 IPv4 地址。
sFlow 版本	显示 sFlow 版本信息。

sFlow 接收端

可配置 sFlow 接收端参数，指定接收端 IP，端口，描述，报文长度等

进入页面的方法：系统运维 >> 系统维护 >> sFlow >> 全局配置

接收端列表

批量编辑	对已选择的接收端进行批量编辑。
恢复默认	当用户想要恢复自己当前操作修改前的配置，可点击该按钮。
接收端 ID	显示接收端 ID，不可编辑。

描述	对接收端进行描述。
接收端 IP	指定接收端的 IP 地址，用于构造 sFlow 报文的目的 IP。
接收端端口	指定接收单接收 sFlow 报文的端口号。
最大报文长度	这里可以配置单个 sFlow 报文的最大报文长度。
超时(s)	当超时时间到了接收端信息会失效，接收端不再收到 sFlow 报文。
生存时间(s)	生存时间会基于超时时间倒计时。

注意：

- 超时时间设置为 0 时接收端的生命周期无限。
- 代理 IP 地址需要在 sFlow 使能之前分配。

sFlow 采样端

可以在此界面配置 sFlow 采样端。

进入页面的方法：系统维护>>sFlow>>sFlow 采样端

条目介绍：

➢ **采样端列表**

批量编辑	对已选择的接收端进行批量操作。
接收端 ID	一个接收端可以从多个 sFlow 采样端口接收采样报文。
入口采样速率	入口采样速率指在数据源处观察到的入口包与生成的样本的比率。

出口采样速率	出口采样速率指在数据源处观察到的出口包与生成的样本的比率。
最大截取长度	使用报文最大截取长度来指定从采样数据包复制的最大字节数。

注意：

- 一个端口只能分配给一个接收端。
- 当接收端 ID 为 0 时表示没有一个接收端口指定。

11.5 LLDP

11.5.1 LLDP 介绍

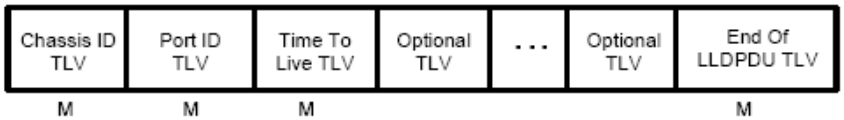
链路层发现协议 LLDP（Link Layer Discovery Protocol）是一个二层协议，在符合 IEEE802 标准的局域网络中，允许网络设备周期性地向邻居设备通告自己的设备信息。LLDP 根据 IEEE802.1AB 标准把设备的标识、性能和配置等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给邻居设备，邻居设备收到这些信息后将其以标准的 MIB（Management Information Base，管理信息库）形式保存起来。网络管理系统可以通过管理协议 SNMP（Simple Network Management Protocol，简单网络管理协议）获取到这些信息，以查询及判断链路的通信状况。

为了描述网络的物理拓扑和拓扑中的相关系统，IETF（Internet Engineering Task Force，互联网工程任务组）组织提出了标准 MIB，一些公司也提出了私有 MIB。但是，IEEE 802 局域网站点并没有统一的标准来传输 MIB 信息。LLDP 解决了这一问题。LLDP 协议允许不同厂商的网络设备协同工作，运行 LLDP 协议的设备能够自动检测并学习邻居设备的信息。LLDP 还可以使运行不同网络层协议的系统互相学习对方的设备信息。

SNMP 应用可以利用 LLDP 获取的信息，进行网络故障排除，从而提高网络的稳定性，维持正确的网络拓扑。

➢ **LLDPDU**

每一个 LLDPDU 携带四个必须的 TLV 以及一个或者多个可选的 TLV。如下图所示，Chassis ID TLV, Port ID TLV, TTL TLV 和 End TLV 是每个 LLDPDU 所必须携带的四个 TLV。可选的 TLV 是由网络管理系统决定的，它们提供了关于本地 LLDP 设备的详细信息。



M - mandatory TLV - required for all LLDPDUs

LLDPDU 的最大长度由特定的传输速率和协议所允许的最大报文长度决定。就 IEEE 802.3 MAC 协议来说，LLDPDU 的最大长度是不带 TAG 的基本 MAC 帧的最大长度，即 1500 字节。

➢ LLDP 工作机制

1) LLDP 的工作模式

每个端口都可以分别配置 LLDPDU 的接收和发送功能，这样端口可以配置四种工作模式：

- 发送接收：既发送也接收 LLDPDU。
- 只接收：只对接收到的 LLDPDU 进行处理，而不向外发送 LLDPDU。
- 只发送：只向外发送 LLDPDU，而不对接收到的 LLDPDU 进行处理。
- 禁用：既不向外发送 LLDPDU，也不对接收到的 LLDPDU 进行处理。

2) LLDPDU 的传输机制

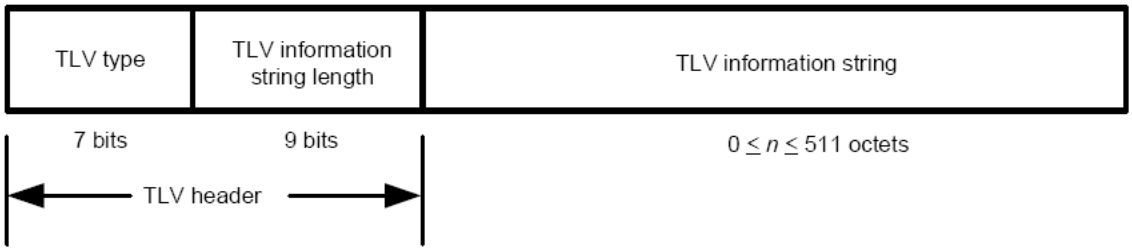
- 当端口工作在发送接收模式或者只发送模式时，设备会周期性地向邻居设备发送 LLDPDU 以通告自己的信息。
- 当本地设备发生变化时，设备会发送变化通告。当本地设备在短时间内频繁变化时，为避免设备连续地发送 LLDPDU 而导致网络阻塞，NMS（Network Management System，网络管理系统）将会设定一个报文发送时延，以确保 LLDPDU 的发送有一个固定的最小时间差。
- 当端口的工作模式由禁用或者只接收模式切换为发送接收模式或者只发送模式时，该设备的快速启动机制将被激活，报文的发送间隔变为 1s，快速发出一些 LLDPDU 之后，设备恢复正常的发送周期。

3) LLDPDU 的接收机制

当端口工作在发送接收模式或只接收模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 TTL（Time To Live，生存时间） TLV 中 TTL 的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

➢ TLV

TLV 是 LLDPDU 的基本组成单位，是 Type/Length/Value 的简称，即类型/长度/值。基本 TLV 的格式如下图所示：



每个 TLV 的类型都是不一样的，根据 TLV 的类型可以判断 TLV 中的信息类型。

下表是目前定义的各种 TLV 的详细信息。

TLV 类型	TLV 名称	说明	是否必须携带
0	End of LLDPDU	标识 LLDPDU 结束。任何在 End Of LLDPDU TLV 之后的信息将被丢弃。	是
1	Chassis ID	标识连接设备的 Chassis ID	是
2	端口 ID	标识发送端口的 ID 信息	是
3	Time To Live	本地设备信息在邻居设备上的老化时间	是
4	端口描述	用以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述	否
5	系统名称	用以向邻居发布本地设备的系统名称	否
6	系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述	否
7	系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息	否
8	管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理	否
127	组织定义	允许不同的组织、软件和设备生产商定义向邻居设备发送信息的 TLV	否

TLV 一般分为两类，基本 TLV 和组织定义的 TLV。

1) 基本 TLV

基本 TLV 是实现 LLDP 协议必不可少的，它们包含网络管理的基本信息。

2) 组织定义的 TLV

不同的组织定义了许多不同的 TLV。端口 VLAN ID、协议 VLAN ID、VLAN 名称以及协议标识 TLV 都是 IEEE 802.1 定义的，MAC/PHY 配置/状态、供电能力、链路聚合以及最大帧长度 TLV 则是由 IEEE 802.3 定义的。

注意:

要获取更多关于 TLV 的详细信息，请参考 IEEE 802.1AB 标准。

TP-LINK 交换机中所支持的可携带 TLV 如下表所示：

端口描述	用以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述。
系统	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息。
系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述。
系统名称	用以向邻居发布本地设备的系统名称。
管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理。
端口 VLAN ID	用以向邻居发布本端口所处 802.1Q VLAN 的 ID。
协议 VLAN ID	用以向邻居发布本端口所处协议 VLAN 的 ID。
VLAN 名称	用以向邻居发布本端口所处 VLAN 被指派的名称。
链路聚合	用以向邻居发布本端口当前的链路聚合信息，包括本端口是否具有链路聚合能力、是否处于聚合状态以及处于链路聚合状态时的端口 ID。
端口状态	用以向邻居发布本端口的端口属性，包括端口支持的速率双工、当前工作的速率双工以及是手工设置还是自动协商而得到的速率双工。
最大帧长	用以向邻居发布本端口的 MAC 和 PHY 支持的最大帧长度。
电源属性	用以向邻居发布本端口的基本供电信息。

LLDP 模块主要用来配置交换机的 LLDP 功能，包括**全局配置**、**端口配置**、**设备信息**、**设备统计**四个部分。

11.5.2 LLDP-MED

LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery，用以媒体终端发现的链路层发现协议）是 LLDP 协议的一个扩展，仅适用于 LLDP-MED 规定的网络连接设备和终端设备之间的交互。

LLDP-MED 规定了两种设备类型，分别是网络连接设备（Network Connectivity）和终端设备（Endpoint Device），比如交换机和 IP 电话，其中终端设备又可以分为 I 、 II 和III型共三种。

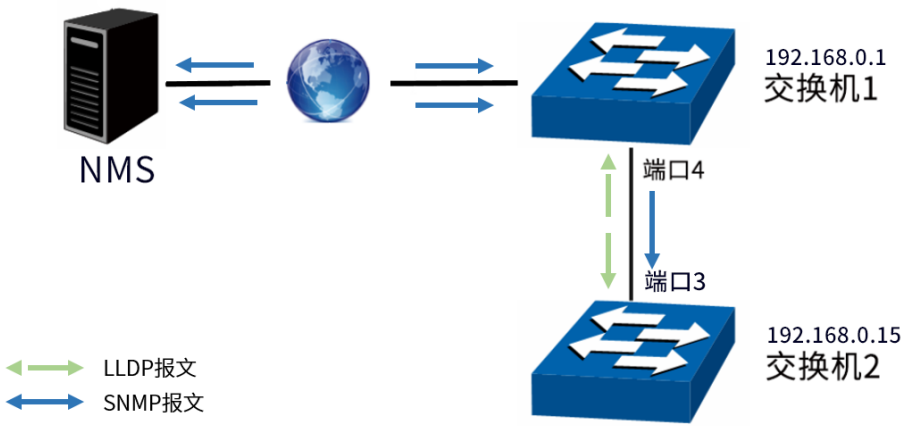
LLDP-MED 可应用于 VoIP（Voice over IP）。TP-LINK 交换机中所支持的可携带 LLDP-MED TLV 如下表所示：

网络策略	网络设备或终端设备上端口的 VLAN 类型、VLAN ID、应用优先级以及使用策略等。
设备地址	网络设备的位置标识信息。
扩展供电能力	设备供电能力。
资产信息	终端设备的资产标识符。

LLDP-MED 模块包括**全局配置**、**端口配置**、**设备信息**三个部分。

11.5.3 LLDP 配置实例

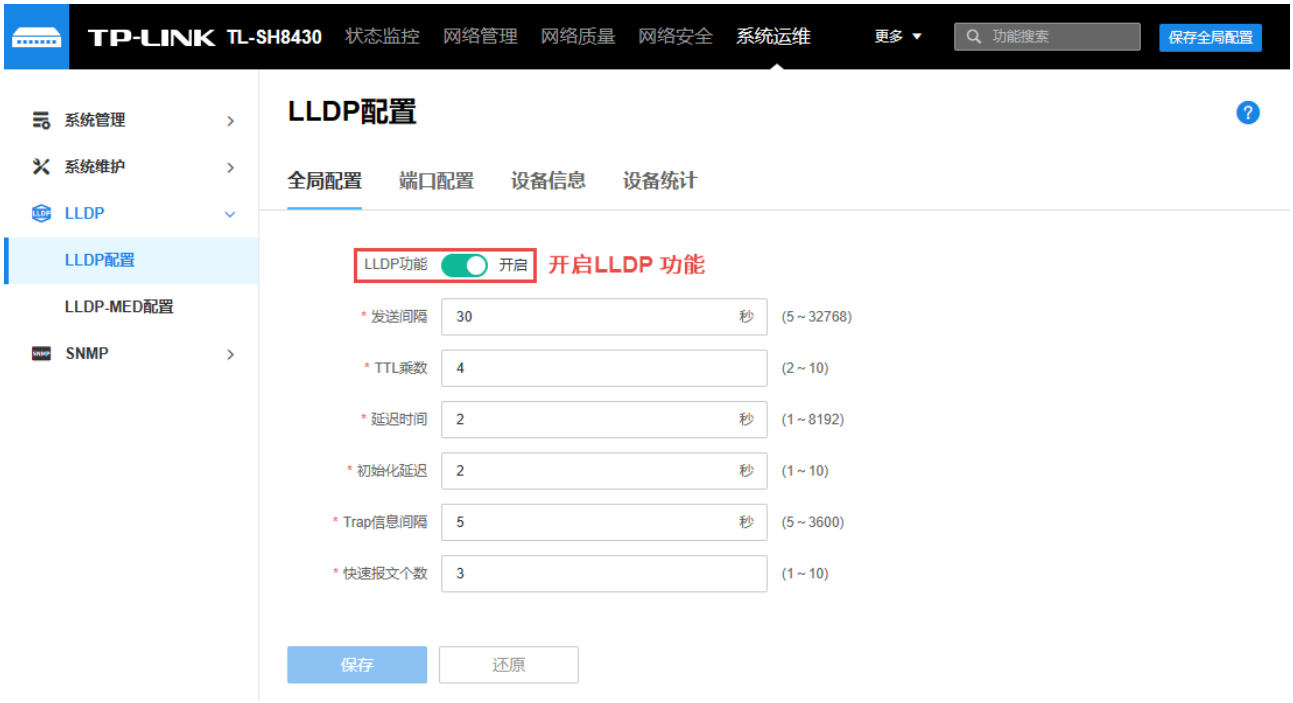
网络管理员希望通过 NMS 网络管理系统可以获取到交换机 1 和交换机 2 之间链路的通信情况、邻居设备变化的 trap 信息。示意网络拓扑图如下：



交换机配置如下：

1. 启用交换机 1 和交换机 2 的 LLDP 功能。

   进入页面：系统运维 >> LLDP >> LLDP 配置 >> 全局配置，开启 LLDP 功能。



2. 启用交换机 1 和交换机 2 的 SNMP 通知功能，配置 Trap 信息间隔，使告警信息可以及时传送到 NMS。

   Trap 信息间隔即为本地设备向网管系统发送 Trap 信息的发送时间间隔。通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致 Trap 信息的频繁发送。

   进入页面：系统运维 >> LLDP >> LLDP 配置 >> 全局配置，配置 Trap 信息间隔。

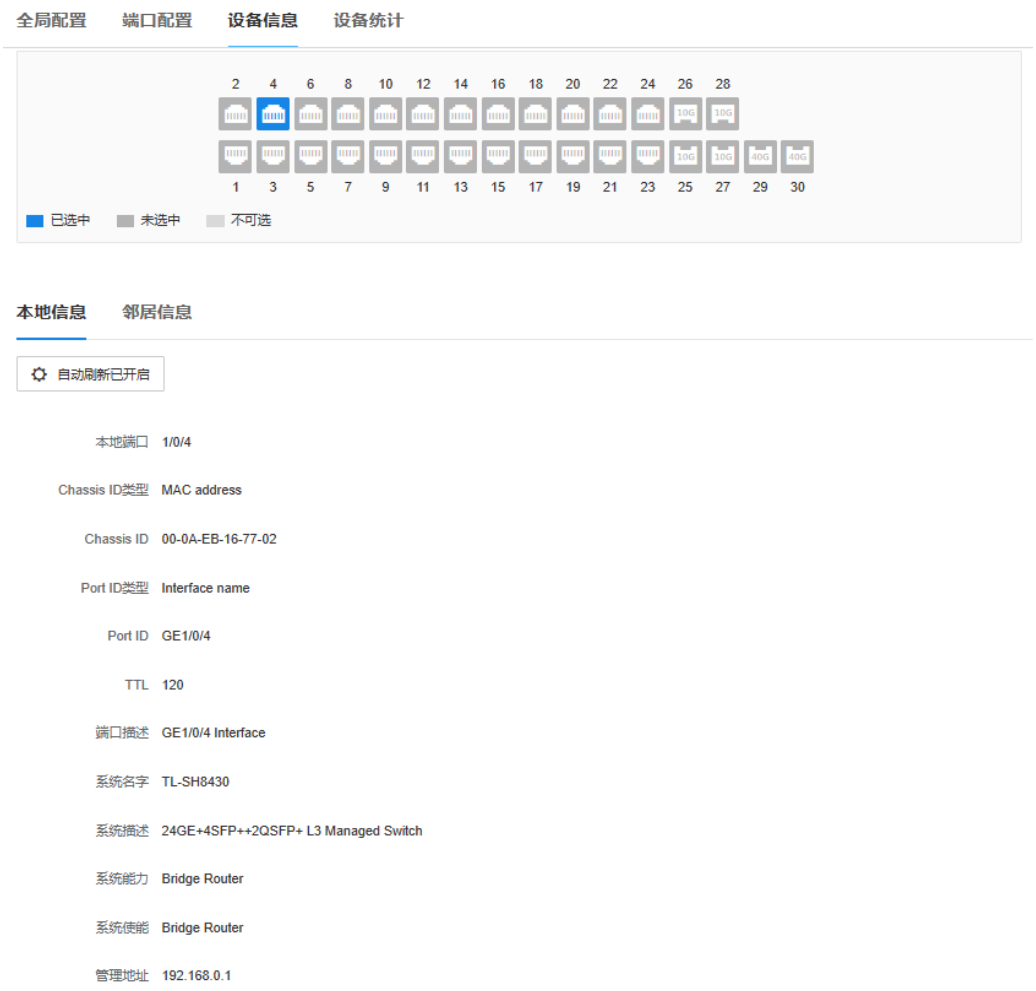
   进入页面：系统运维 >> LLDP >> LLDP 配置 >> 端口配置，开启 SNMP 通知功能。

交换机 1：

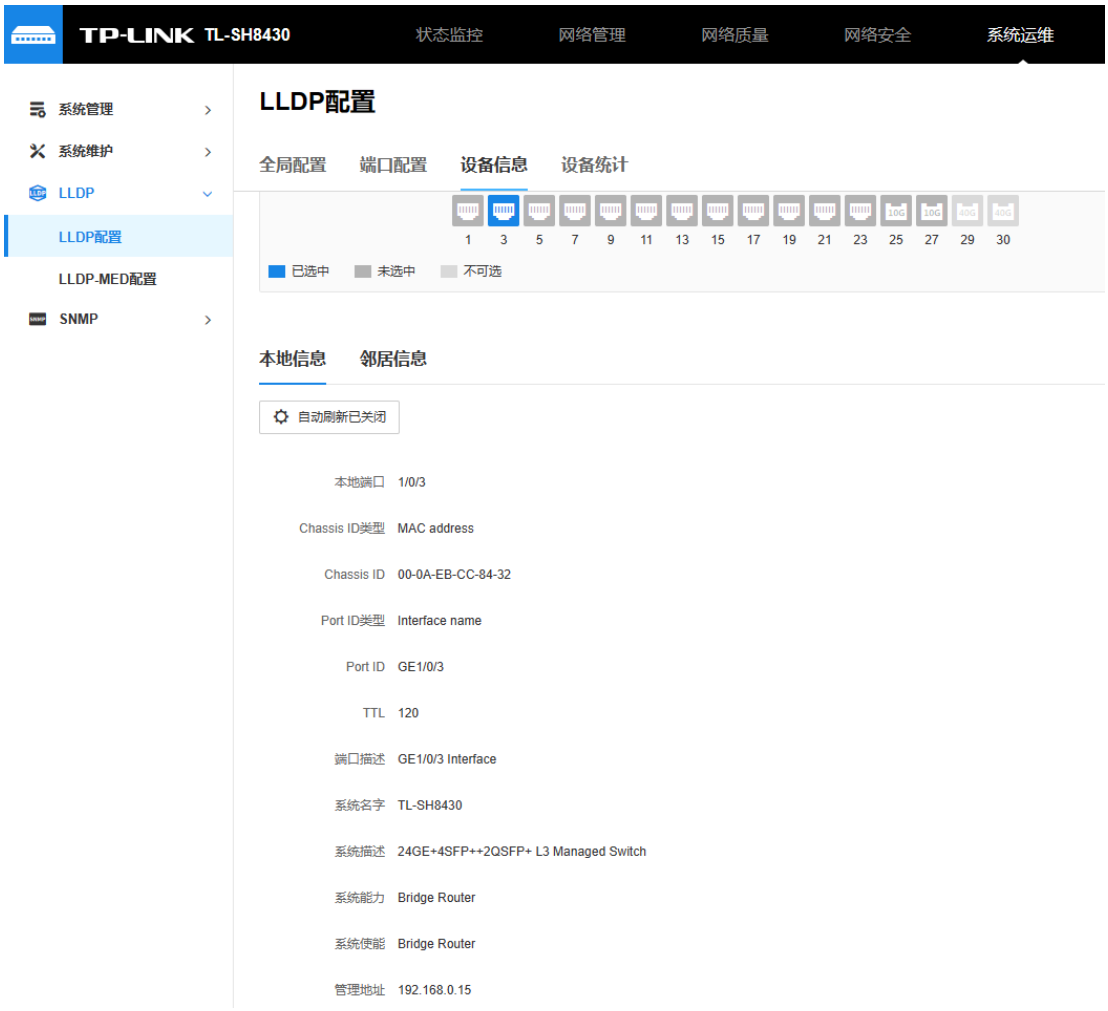
交换机 2：

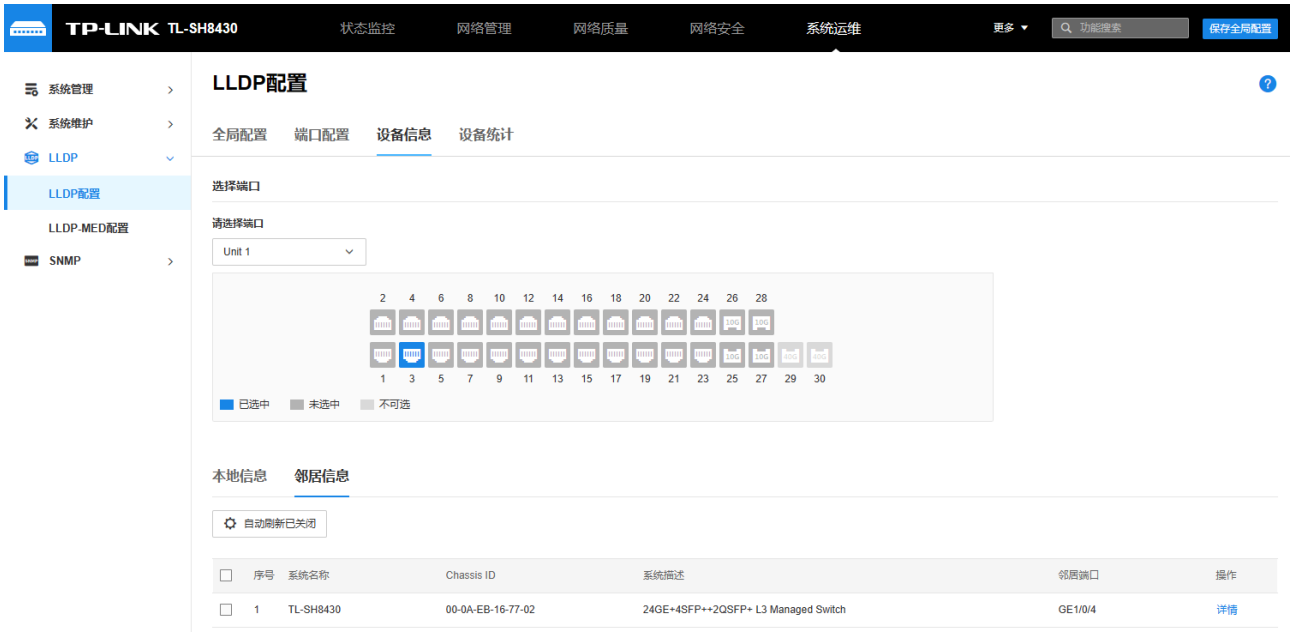
3. 验证配置结果：

进入交换机 1 管理页面：系统运维 >> LLDP >> LLDP 配置 >> 设备信息，查看端口 4 的本地信息及邻居信息。



进入交换机 2 管理页面：系统运维 >> LLDP >> LLDP 配置 >> 设备信息，可查看端口 3 的本地信息及邻居信息。





点击<详情>可查看该邻居设备的具体信息：

11.6 SNMP 管理

11.6.1 SNMP 介绍

- **SNMP 概述**

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前 UDP/IP 网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。SNMP 结构简单，使用方便，并且能够屏蔽不同设备的物理差异，实现对不同设备的自动化管理，所以得到了广泛的支持和应用，目前大多数网络管理系统和平台都是基于 SNMP 的。

SNMP 的最大优势就是设计简单，他既不需要复杂的实现过程，也不会占用太多的网络资源，便于使用。SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时，SNMP 可实现统计、配置和测试等功能；当网络出故障时，可实现各种错误检测和恢复功能。

- **SNMP 的管理框架**

SNMP 包括三个网络元素：SNMP 管理者(SNMP Manager)，SNMP 代理(SNMP Agent)，MIB 库（Management Information Base，管理信息库）。

SNMP 管理者：运行在 SNMP 客户端程序的工作站，提供了非常友好的人机交互页面，方便网络管理员完成绝大多数的网络设备管理工作。

SNMP 代理：驻留在被管理设备上的一个进程，负责接受、处理来自 SNMP 管理者的请求报文。在一些紧急情况下，SNMP 代理也会通知 SNMP 管理者事件的变化。

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，他们之间通过 SNMP 协议来交互管理信息。SNMP 管理者、SNMP 代理、MIB 库三者的关系如下图所示。

- **SNMP 的协议版本**

我司交换机提供了 SNMPv3 的管理功能，同时兼容 SNMPv1 和 SNMPv2c，SNMP 管理者和 SNMP 代理的 SNMP 版本需要一致，它们之间才能相互通信，可以根据自己的应用需求，选择不同安全级别的管理模式。

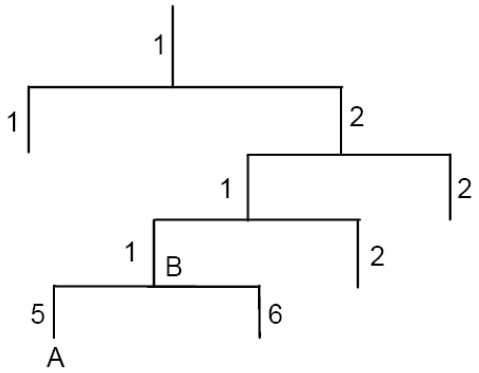
SNMPv1：采用团体名（Community Name）认证。团体名用来定义 SNMP 管理者和 SNMP 代理的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP 管理者对 SNMP 代理的访问。

SNMPv2c：也采用团体名认证。它在兼容 SNMPv1 的同时又扩充了 SNMPv1 的功能。

SNMPv3：SNMPv3 在前两个版本 v1、v2c 的基础上大大加强了安全性和用户可控制性，他采用了 VACM（View-based Access Control Model，基于视图的访问控制模型）及 USM（User-Based Security Model，基于用户的安全模型）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 是以树状结构进行存储的。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别，被管理对象可以用一串数字唯一确定，这串数字是被管理对象的 OID（Object Identifier，对象标识符）。MIB 的结构如下图所示。图中，B 的 OID 为{1.2.1.1}，A 的 OID 为{1.2.1.1.5}。



- **SNMP 配置概要**

- 创建视图

MIB 视图是全部 MIB 管理对象的一个子集。管理对象以 OID（Object Identifier，对象标识符）来表示，通过配置管理对象的视图类型（包括/排除），来达到控制该管理对象能否被管理的目的。各管理对象的 OID 可以在 SNMP 管理软件上找到。

- 创建 SNMP 组

创建完视图之后，需要创建 SNMP 组，只有“组名”、“安全模式”、“安全级别”三项均相同的组，才被认为是同一个组。同时可以为各个 SNMP 组添加只读/只写/通知视图，从而满足了处于不同组内的用户对交换机功能的访问权限不同的需求。

- 创建用户

用户创建于 SNMP 组中，SNMP 管理端使用此处创建的用户及其认证/加密密码来登录 SNMP 代理端。

SNMP 模块主要用于配置交换机的 SNMP 功能，包括 **SNMP 配置**、**通知管理**和 **RMON** 三个部分。

11.6.2 SNMP 管理配置实例

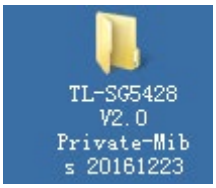
SNMP 管理协议目前有三种：SNMPv1、SNMPv2C 和 SNMPv3，本小节中将分别讲解如何使用三种协议实现对我司交换机的 SNMP 管理。

安装 SNMP 管理软件

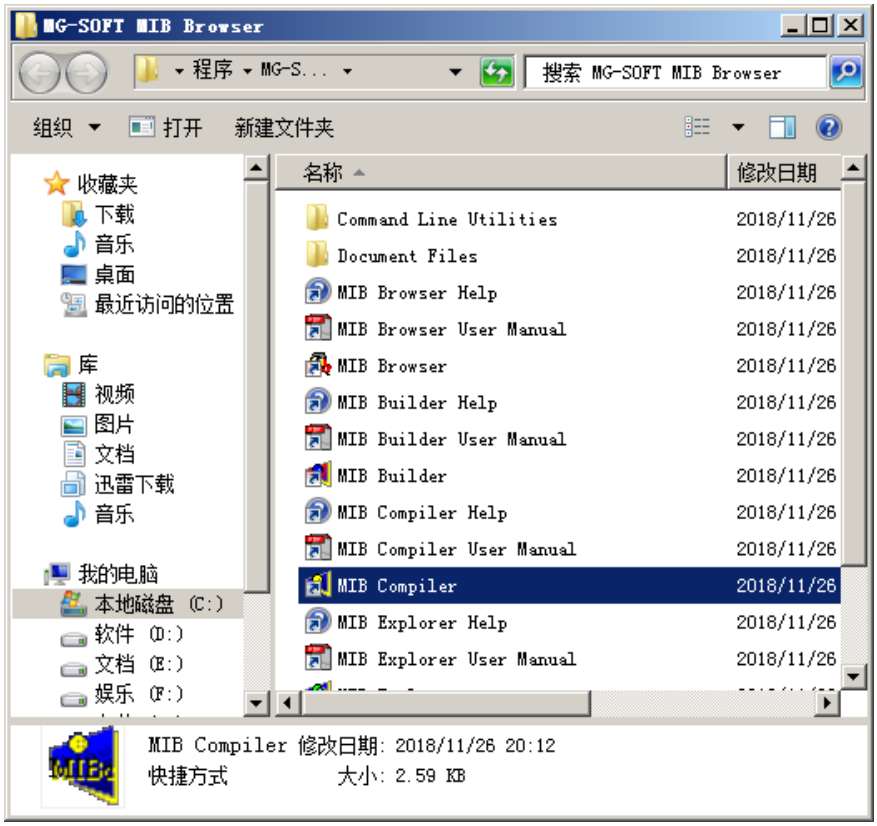
首先需要安装 SNMP 管理软件，加载交换机私有 MIB 库。配置步骤如下：

1. 安装 SNMP 管理软件（SNMP 管理需要在电脑上安装专用的管理软件，此处以 MG-SOFT MIB Browse 为例进行说明）。
2. 将设备的 MIB 文件下载或拷贝到电脑，此处以 TL-SG5428 V2.0 的 MIB 库 TL-SG5428 V2.0 Private-Mibs20161223 为例。

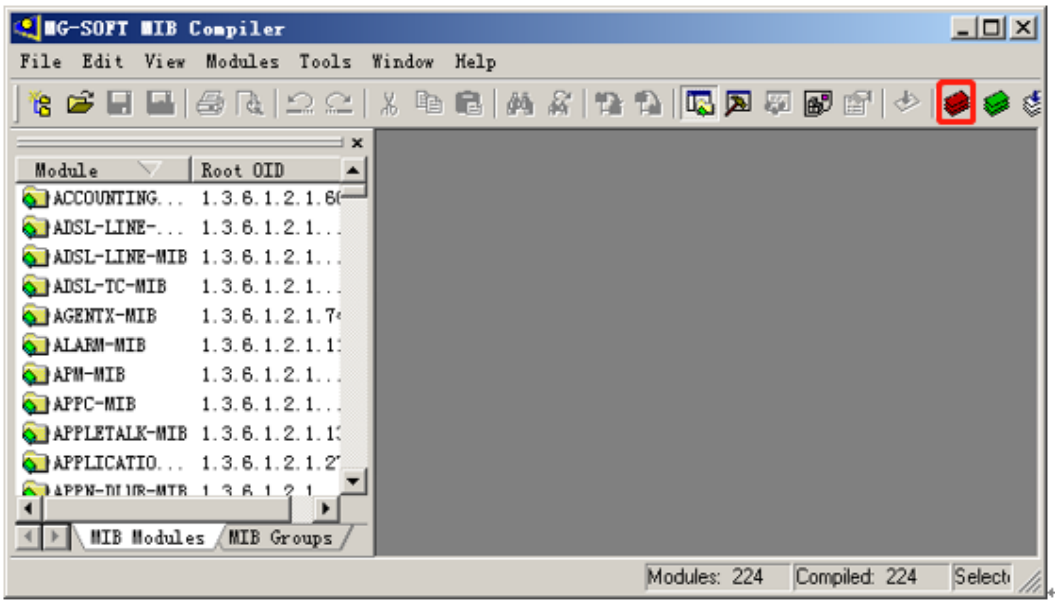
   不同的交换机的 MIB 库有所区别，具体文件可前往 TP-LINK 资料中心获取。

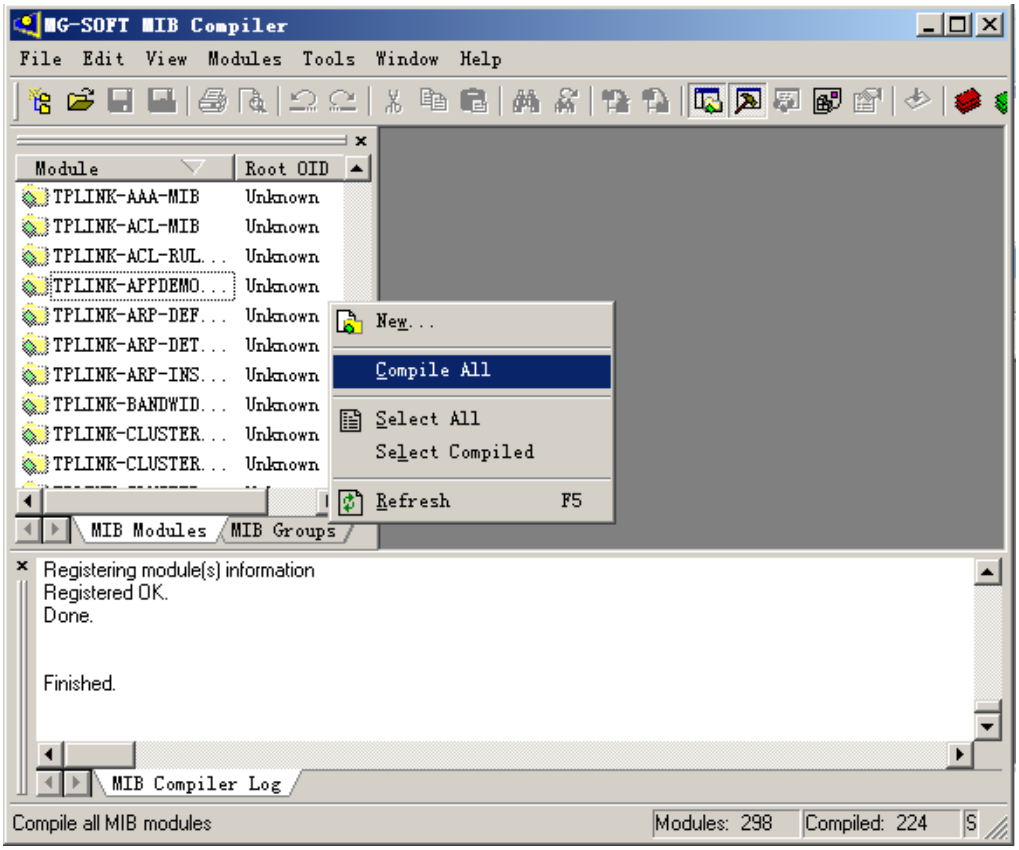
3. 在电脑中打开 MIB Compiler（MG-SOFT MIB Browse 安装完成后，在应用程序对应的文件夹中可以看到此程序）。



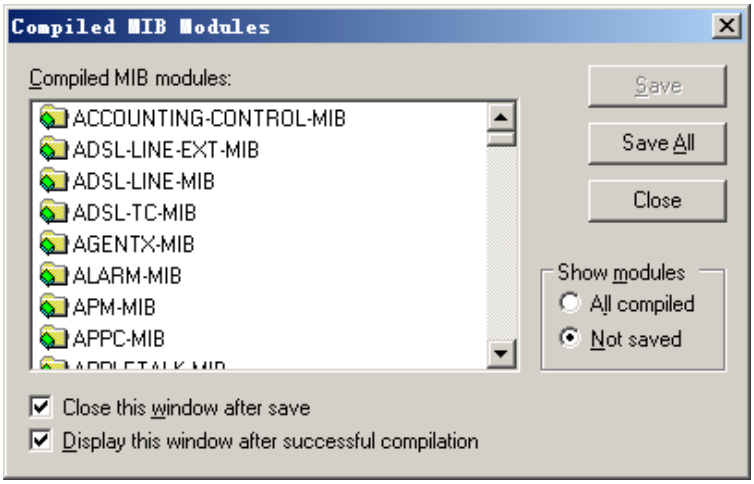
4. 导入交换机的 MIB 文件。



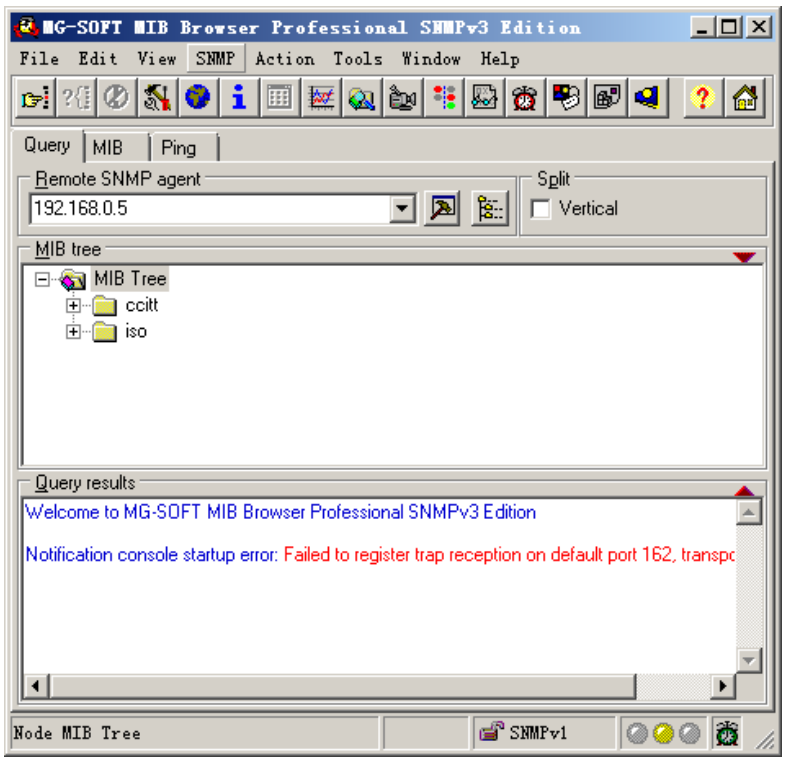
5. 右键点击左边 MIB 文件的空白处，选择<Complie ALL>。



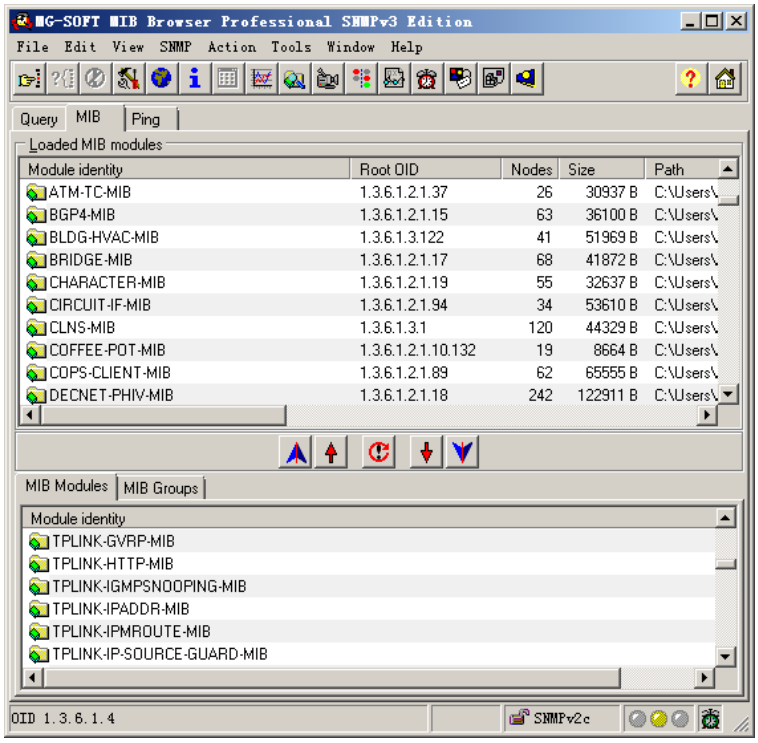
6. 点击<Save ALL>，将 TL-SG5428 C2.0 的 MIB 库文件保存在计算机指定路径下。



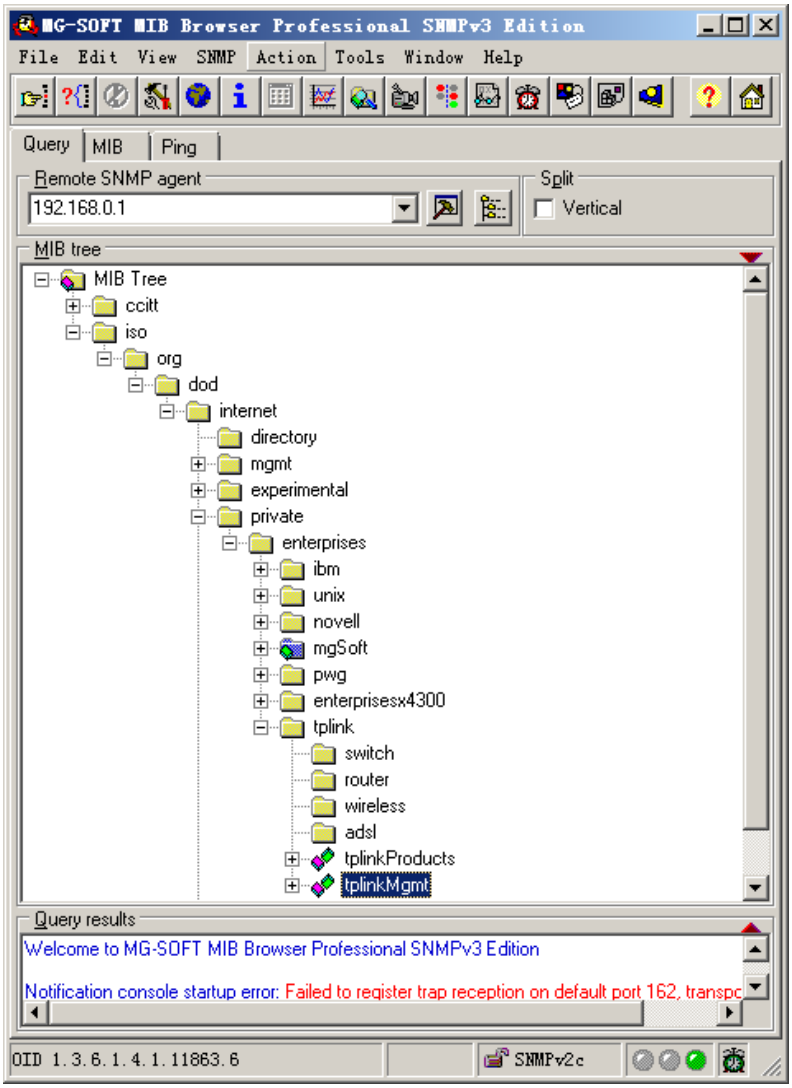
7. 打开软件 MIB Browser。



8. 点击<MIB>窗口，将 TP-LINK 的 MIB 库添加到软件中，选中所有 TP-LINK 开头的 MIB 文件，然后点击图标<  >，加载选中的 MIB 文件。



9. 加载成功，回到<Query>窗口，依次展开，可以看到“tplinkMgmt”。



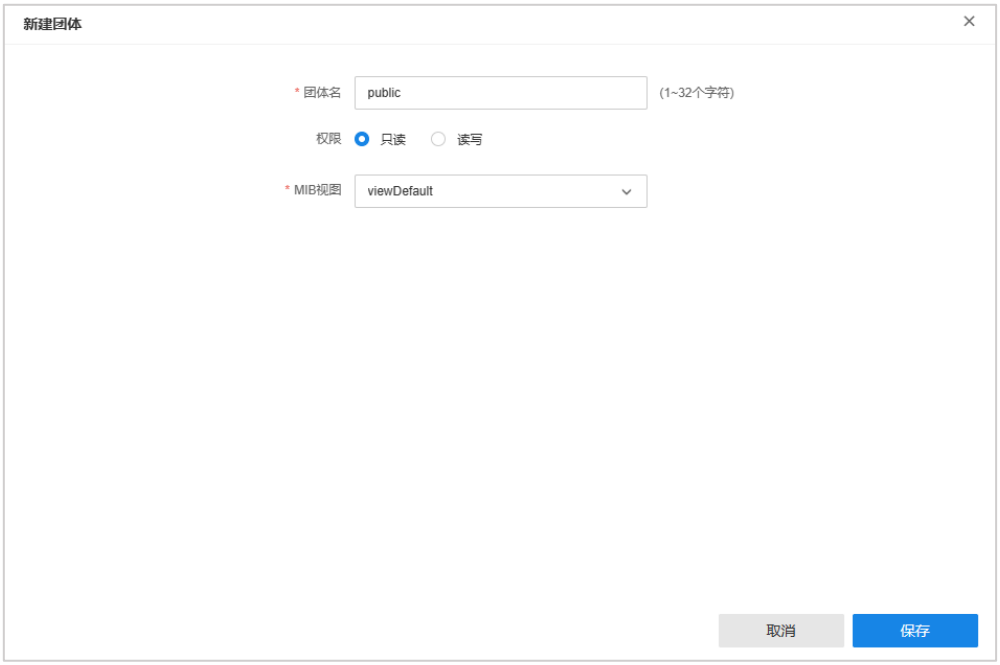
SNMP v1 和 SNMP v2C

➢ **交换机设置**

1. 登录交换机管理界面，**进入页面：系统运维 >> SNMP >> 全局配置**，启用 SNMP 功能，并点击<保存>。

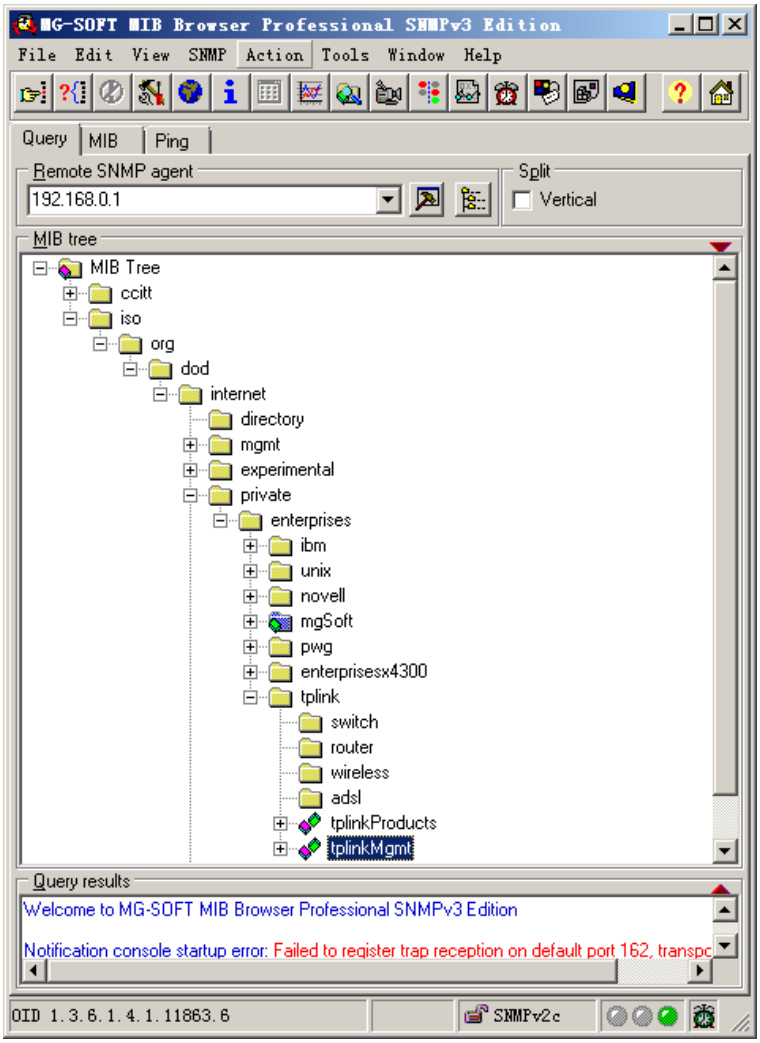
2. **进入页面：系统运维 >> SNMP >> 团体管理**，点击<新增>新建团体。

设置团体名，如“public”，并选择管理权限，MIB 视图默认即可，点击<保存>。

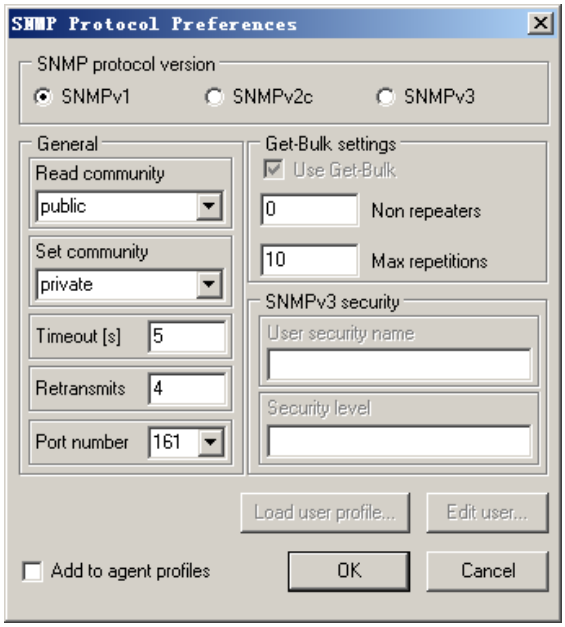


➢ SNMP 软件设置

1. 打开 MIB Browser 软件。



2. 设置交换机的 IP 地址（本例中为 192.168.0.1），并点击<  >设置 SNMP 管理相关参数。

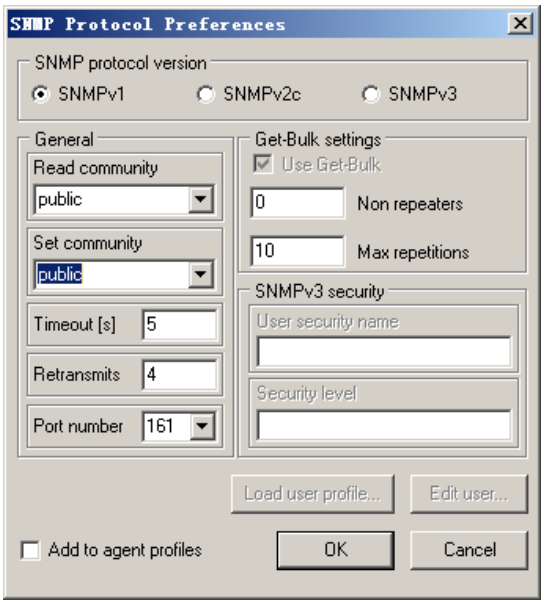


3. 设置参数如下：

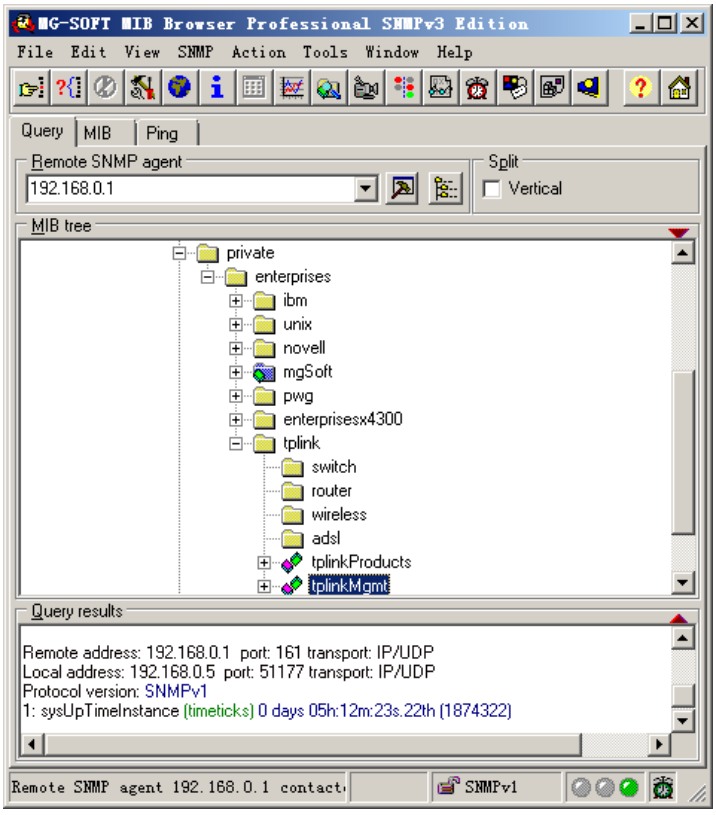
SNMP protocol version（SNMP 版本） 选择 v1

Read community	设置为 public
Set community	设置为 public

public 即为刚刚在交换机中添加读写权限的团体名，如下图所示：

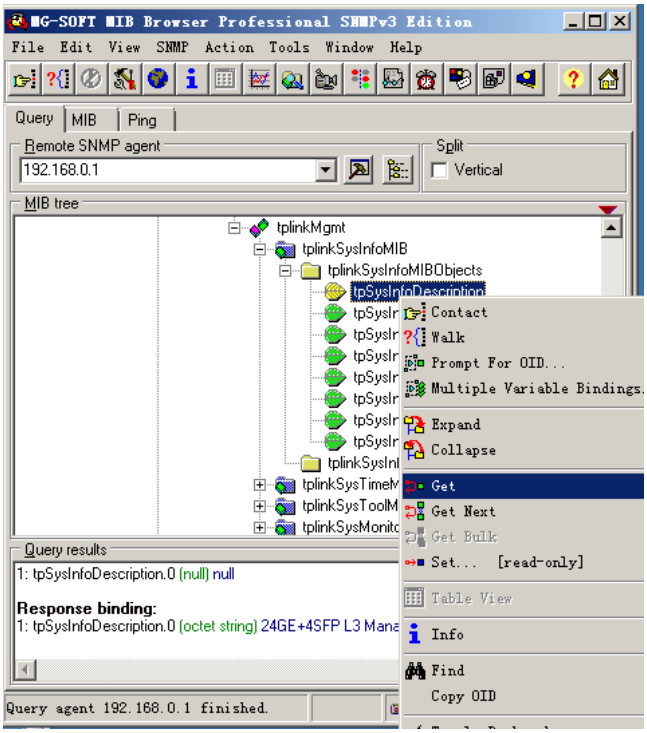


4. 点击<OK>，下方窗口中可以看到已经连接成功。

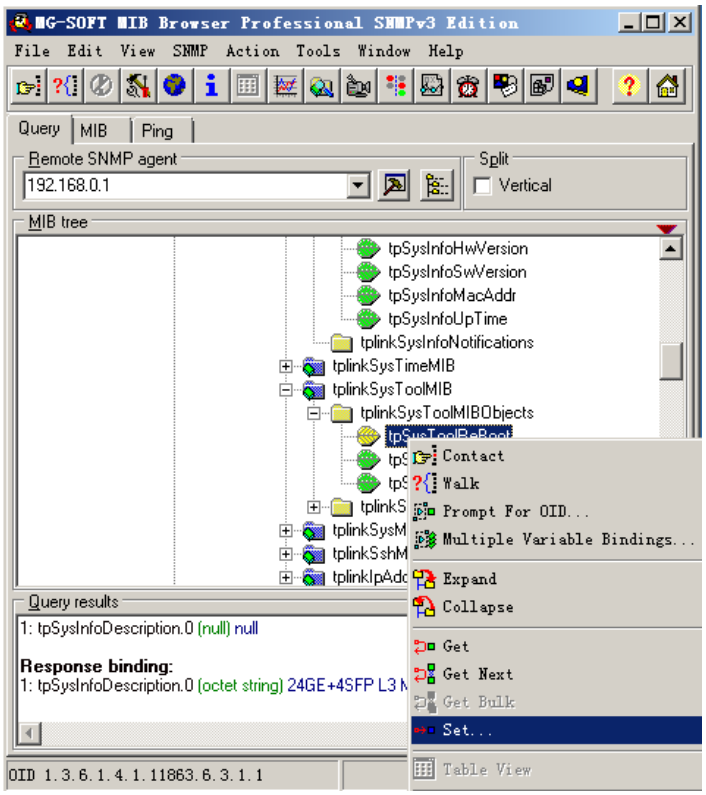


5. 此时即可对交换机的参数进行查看和设置了。

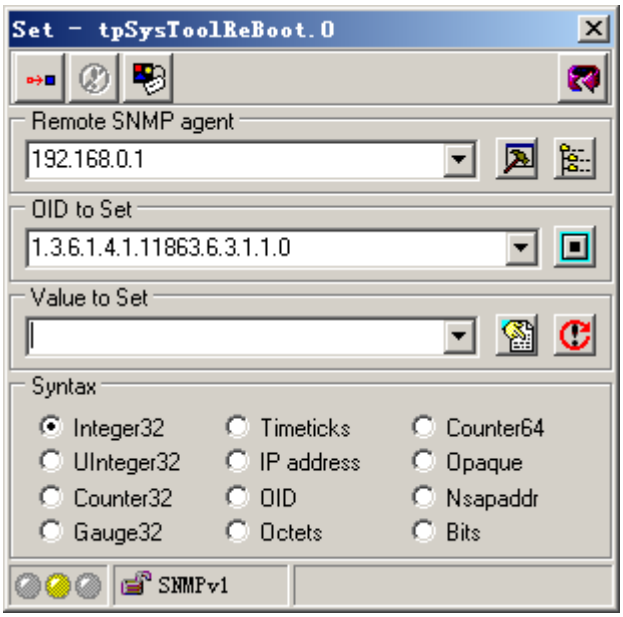
如读取交换机的系统描述信息，选择相应项，右键点击<GET>即可。



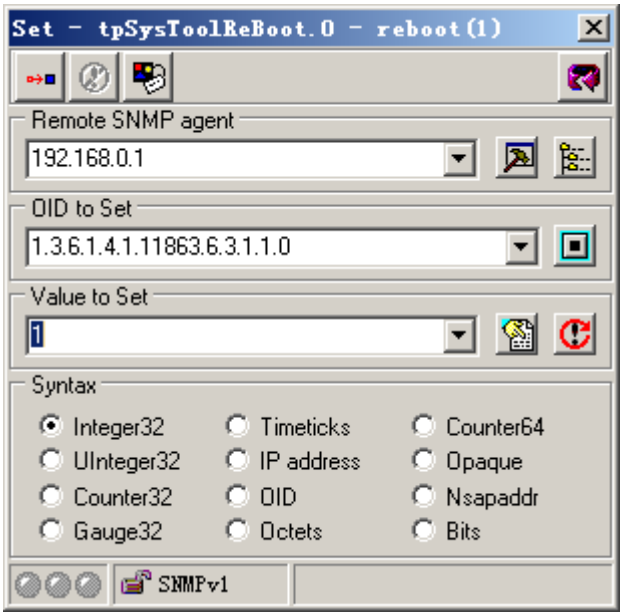
也可以对交换机进行设置。如对交换机进行重启，选择<tpSysToolReBoot>项，右键点击<Set>，如下图所示：



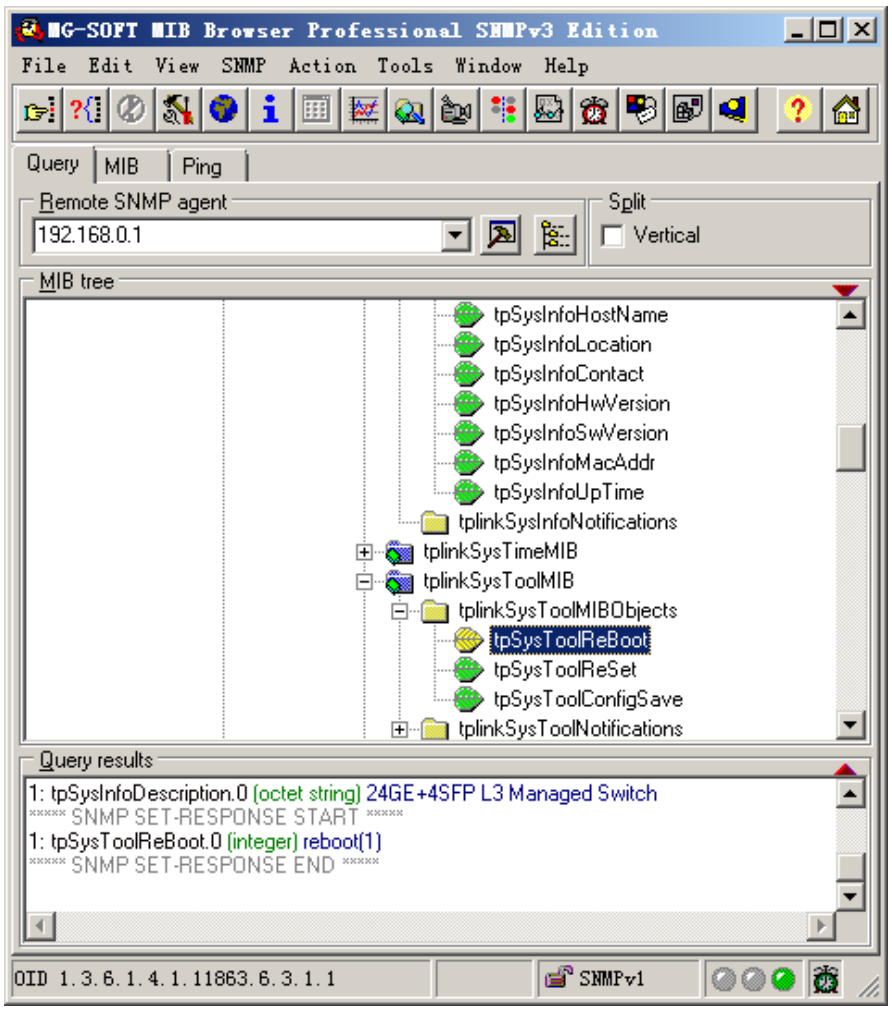
点击<Set>后打开如下窗口。



将值设置为 1，表示重启。可点击旁边图标<  >进行下拉选择。



点击左上角<  >执行操作，此时交换机将会重启。



SNMP v3

➢ **交换机设置**

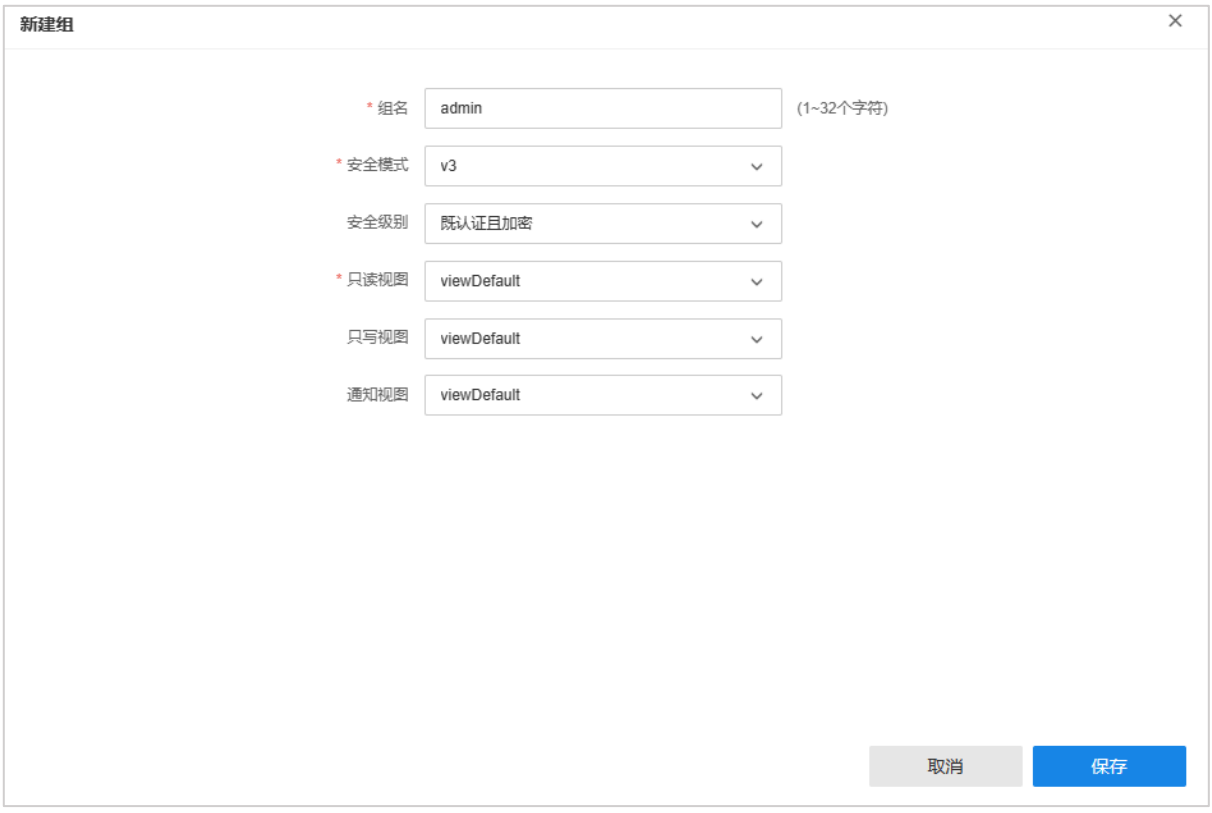
1. 登录交换机管理界面，**进入页面：系统运维 >> SNMP >> 全局配置**，启用 SNMP 功能并点击<保存>。

2. **进入页面：系统运维 >> SNMP >> 组管理**，点击<新增>，添加用户信息。

设置如下参数：

添加组用户名	本例为 admin
安全模式	选择 v3
安全级别	选择“既认证且加密”
只读视图	选择默认视图 viewDefault
只写视图	选择默认视图 viewDefault
通知视图	选择默认视图 viewDefault

参数设置完成后，点击<保存>。

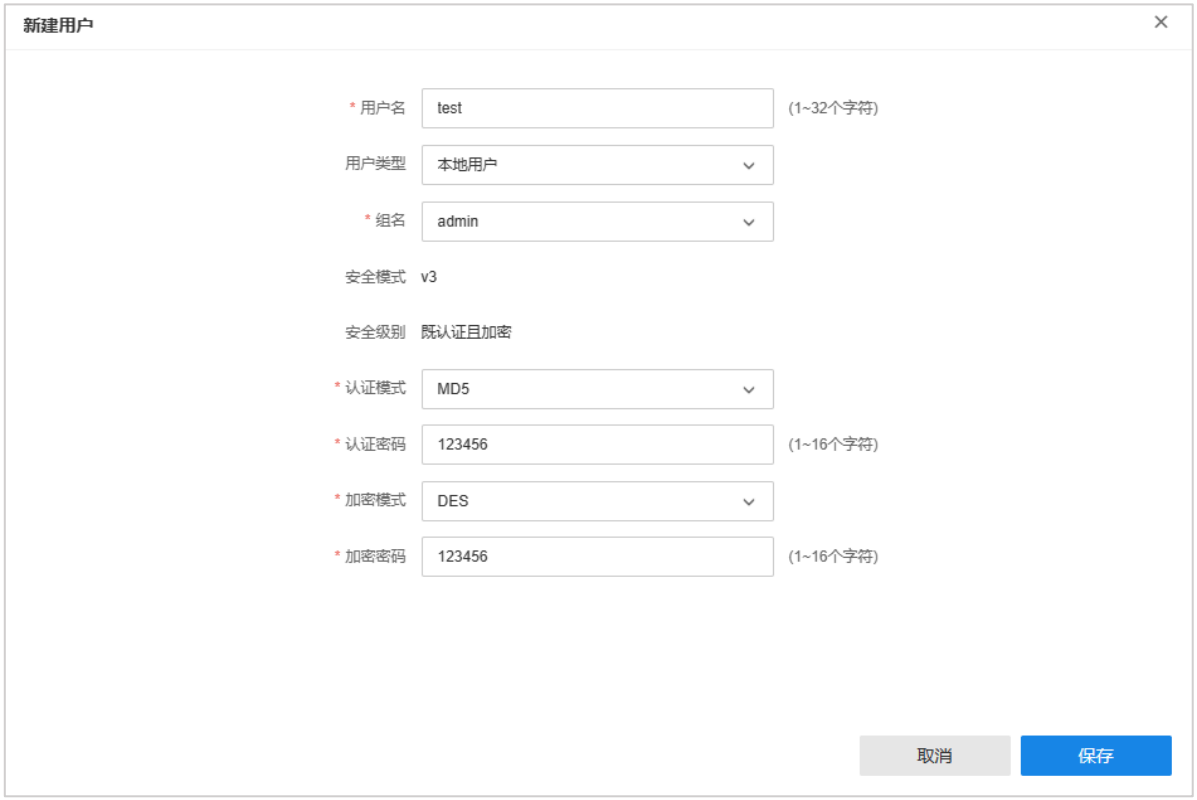


3. **进入页面：系统运维 >> SNMP >> 用户管理**，点击<新增>，设置如下参数：

用户名	本例中为“test”
用户类型	选择“本地用户”
组名	选择上一步中新建的组名“admin”

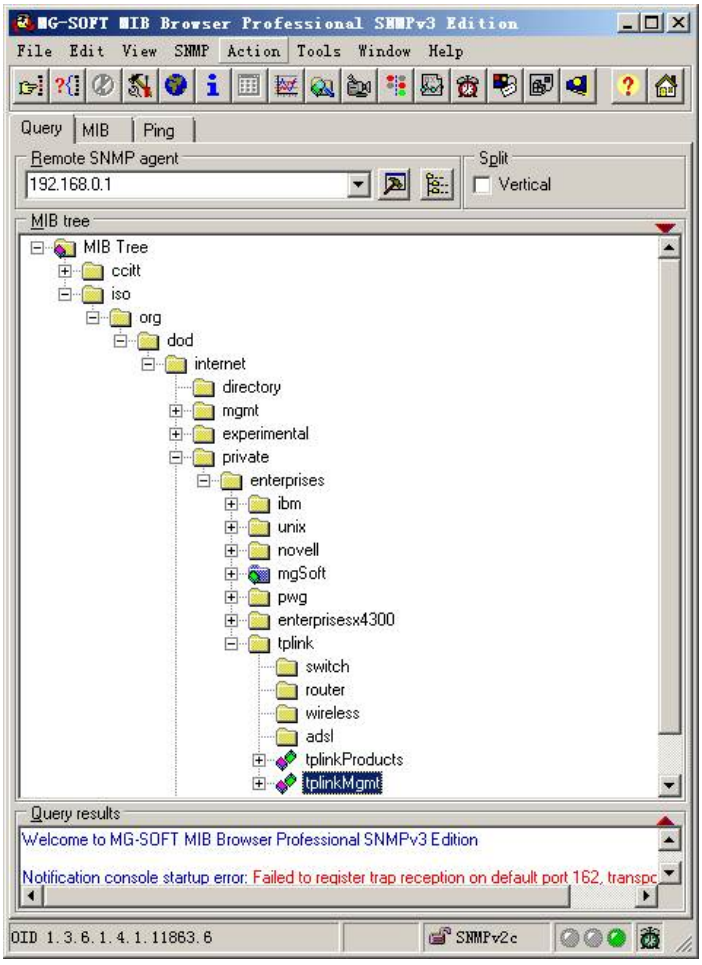
安全模式	选择“v3”
认证模式	选择“MD5”，设置相应密码，本例中为 123456
加密模式	选择“DES”，设置相应密码，本例中为 123456

参数设置完成后，点击<保存>。

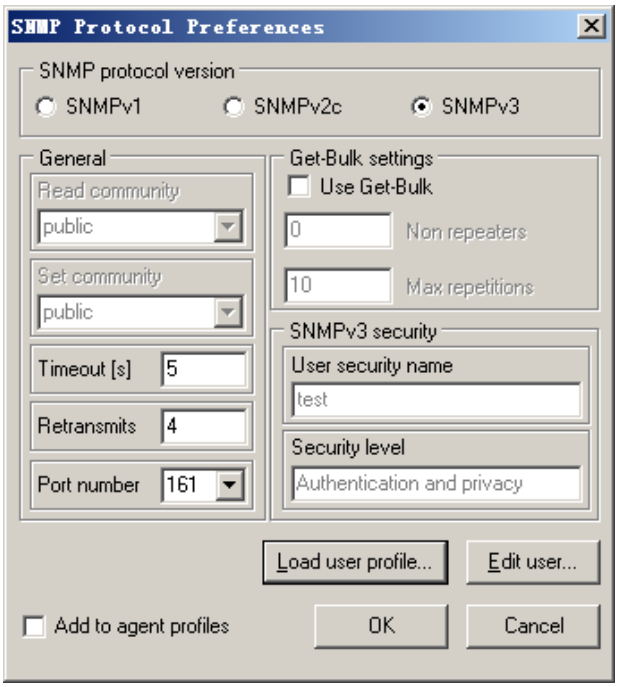


➢ SNMP 软件设置

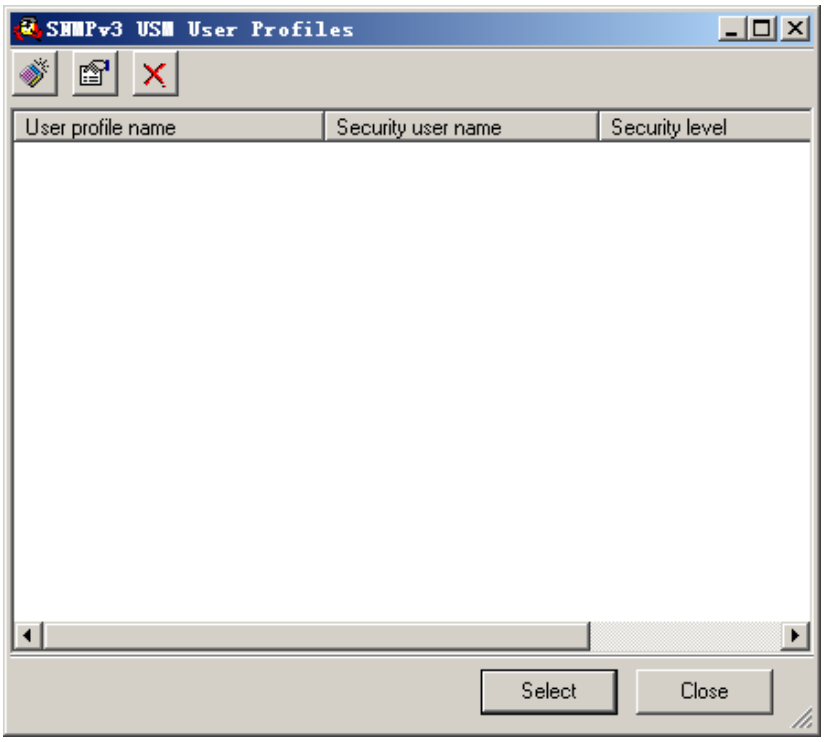
1. 打开 MIB Browser 软件。



2. 设置交换机的IP地址(本例中为192.168.0.1),并点击<>设置SNMP管理相关参数,选择SNMPv3。



3. 初次设置时，选择<Load user profile>，打开如下窗口。



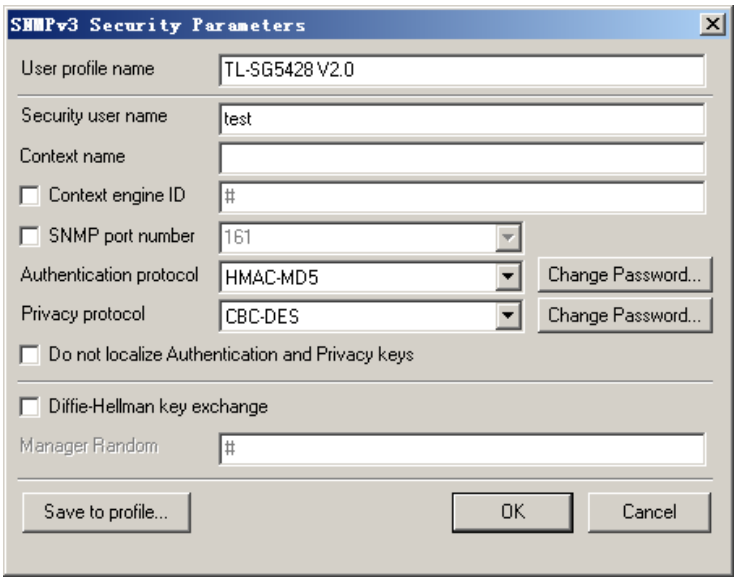
4. 点击  >添加用户配置文件，设置如下参数：

User profile name 配置文件名称。可以任意填写，本例中为“TL-SG5248 V2.0”。

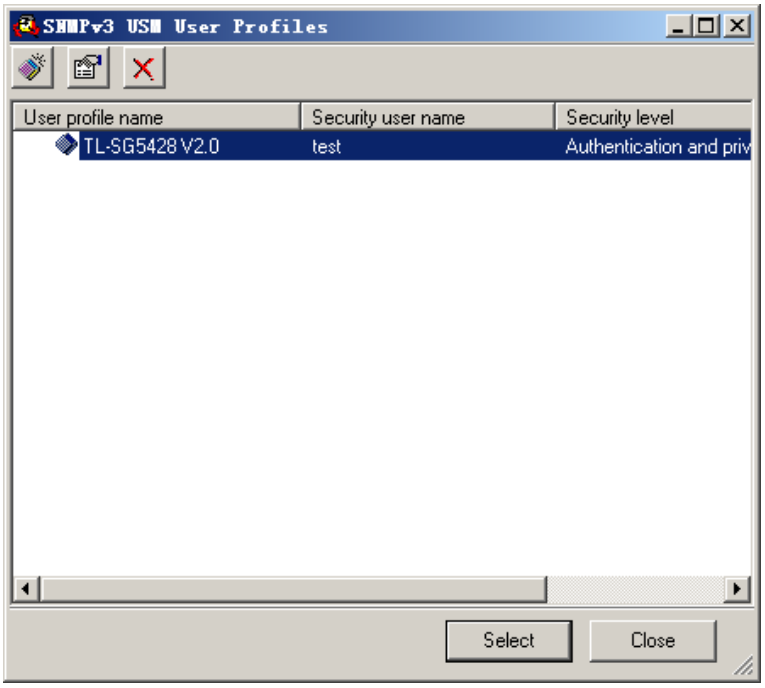
Security user name SNMP 用户名。和交换机设置对应，本例中为“test”。

Authentication protocol 认证协议。和交换机设置对应，本例中为“MD5”，并设置密码“123456”。

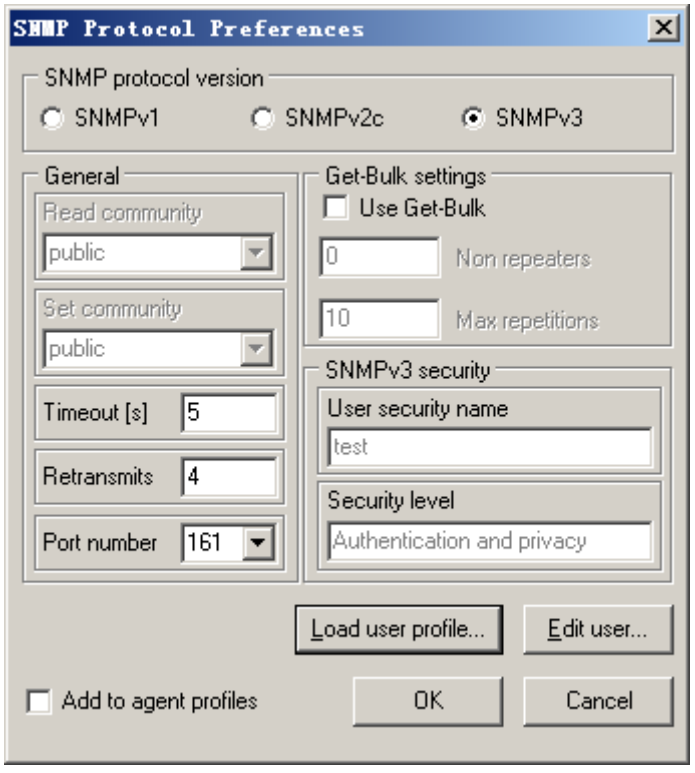
Privacy protocol 加密协议。和交换机设置对应，本例中为“DES”，并设置密码“123456”。



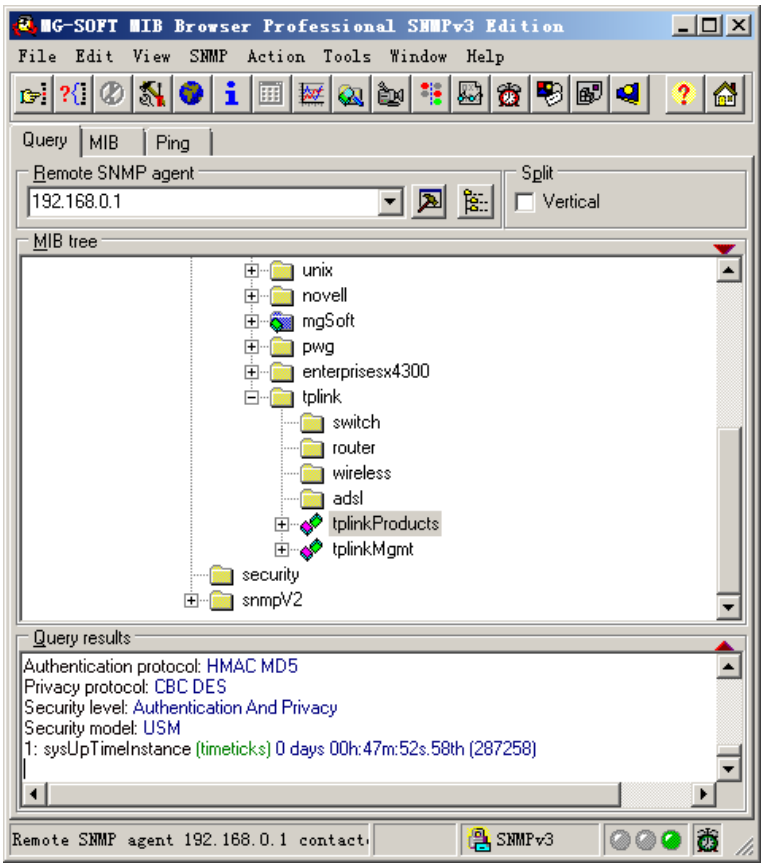
设置完成后点击<OK>。



5. 选中该配置文件，点击<Select>，加载该配置文件参数。



6. 点击<OK>，可以看到下方窗口已经连接成功。



7. 接下来即可对交换机的参数进行查看和设置，读取和设置的操作与 SNMP v1 和 SNMP v2C 相同。

回目录