TP-LINK®

主要功能配置实例

3/5/6/7/8系列企业级交换机

声明

目录

第1章 前言

本手册旨在帮助您正确使用 TP-LINK 企业级交换机。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。

1.2 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 >> 标签页，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字或图形，表示 Web 界面的按钮名称，如<确定>或<新增>。
- 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“ARP 绑定”界面。

本手册中使用的特殊图标说明如下：

图标	含义
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。

1.3 适用机型

本手册适用于 TP-LINK 3/5/6/7/8 系列企业级交换机，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 三层网管交换机管理方法介绍

2.1.1 通过业务接口管理交换机

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

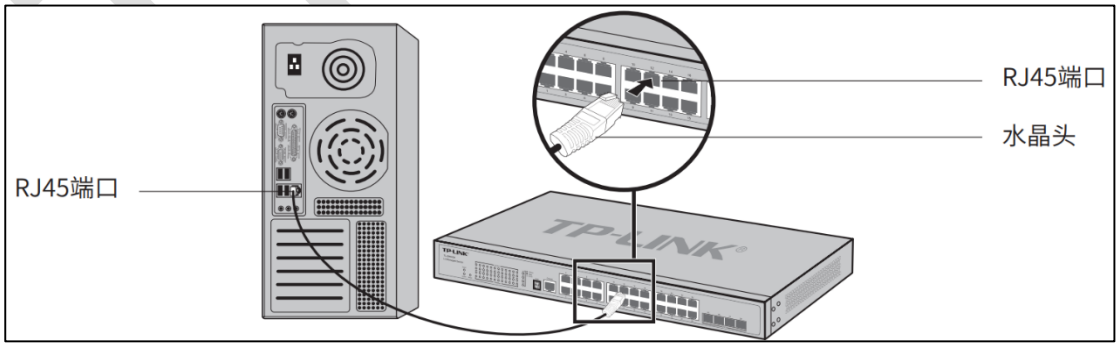
业务口默认管理用户名：admin

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：



第一、HTTP、HTTPS 管理

1、在电脑上打开浏览器，输入 http://192.168.0.1 或者 https://192.168.0.1 （浏览器建议使用 Chrome、Firefox、Edge 或 IE9 以上的浏览器）。

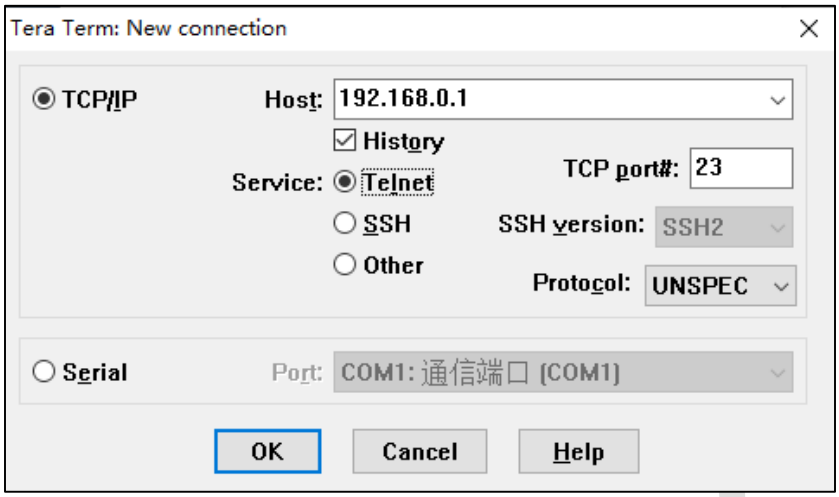
2、输入正确的用户名和密码。

注意：

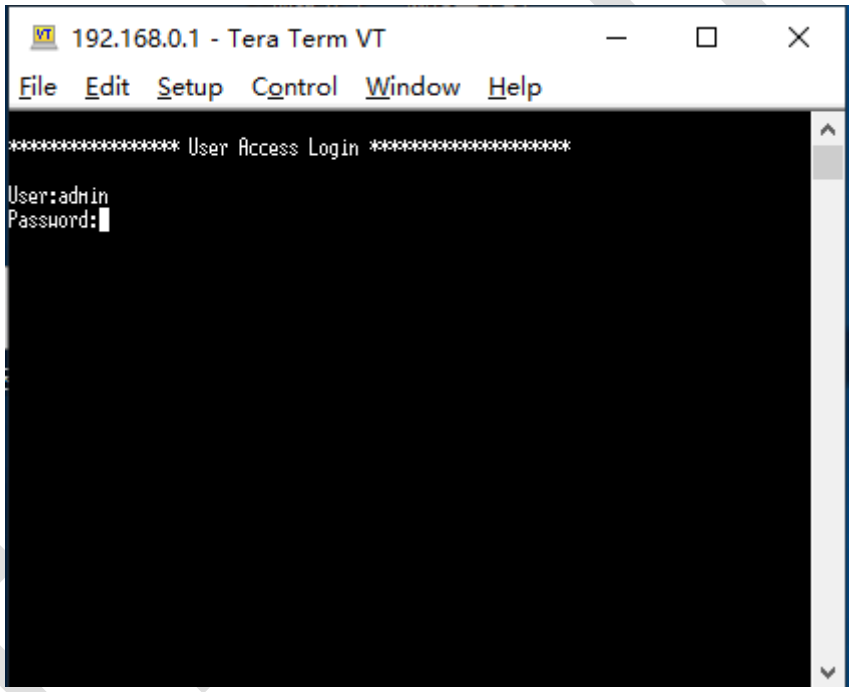
- 如果使用 HTTPS 管理，浏览器会提示安全风险，在浏览器中点击“详细信息”—”继续转到网页”即可。（不同浏览器提示可能会略有不同）
- 如果输入正确用户名和密码之后，管理页面显示不全，可能是由于浏览器缓存原因造成，此时按 Ctrl+F5 刷新页面即可。

第二、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。

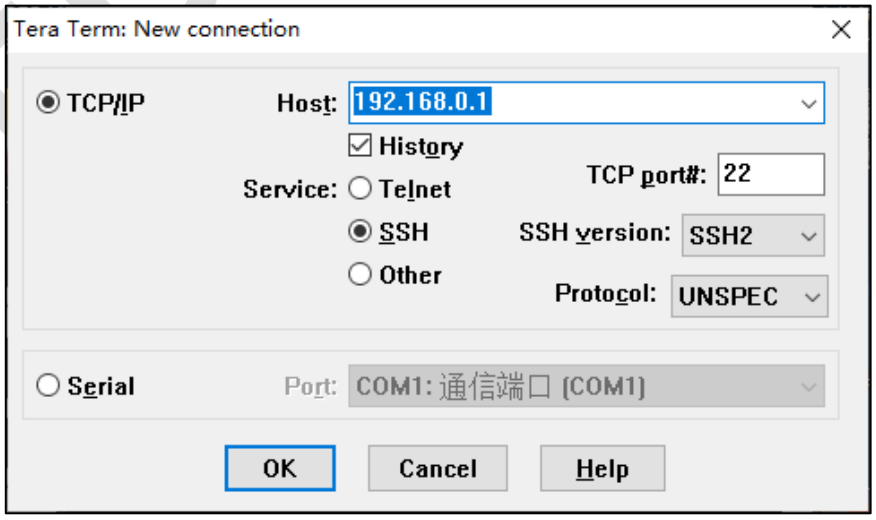


第三、SSH 管理

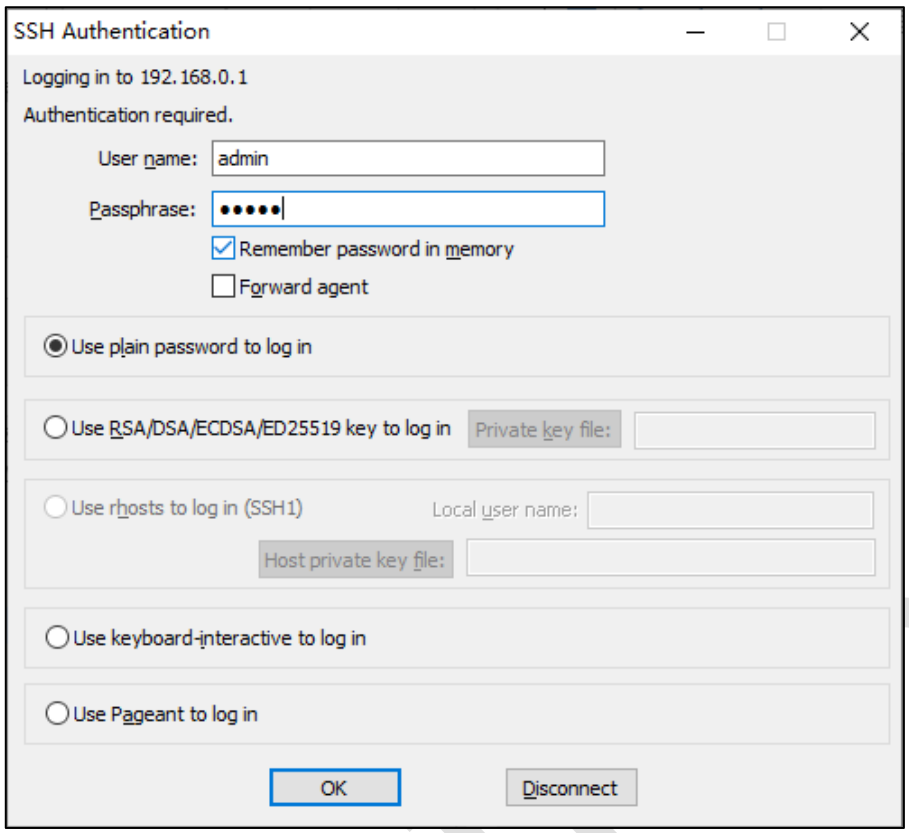
SSH 管理功能在交换机上默认情况下是禁用的，需要先使用其他管理方式进入交换机开启该功能才可以进行 SSH 管理。

1、电脑登录交换机的 Web 页面，“系统管理”-“安全管理”-“SSH 配置”，启用 SSH 功能。

2、电脑上安装 SSH 客户端软件（比如：Tera Term、SecureCRT 等，本章节以 Tera Term 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。



第四、SNMP 管理

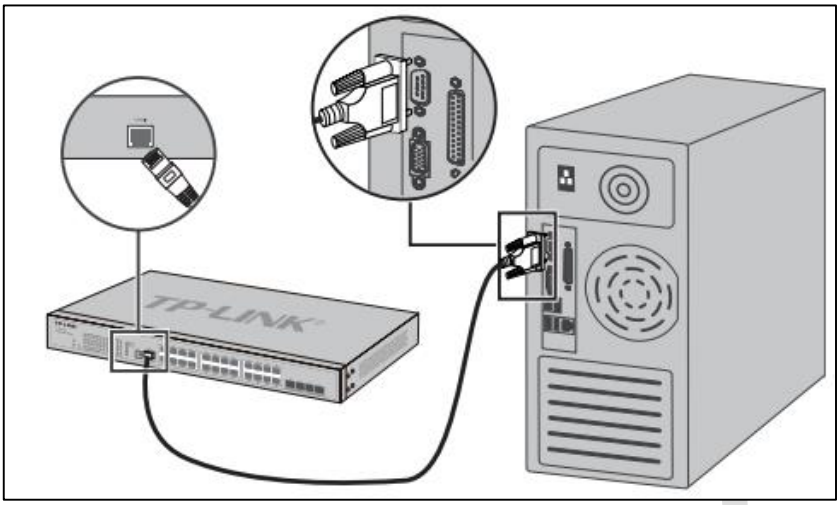
可以参考《SNMP 基础设置方法介绍》。

2.1.2 通过 Console 接口管理交换机

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。

电脑连接方式

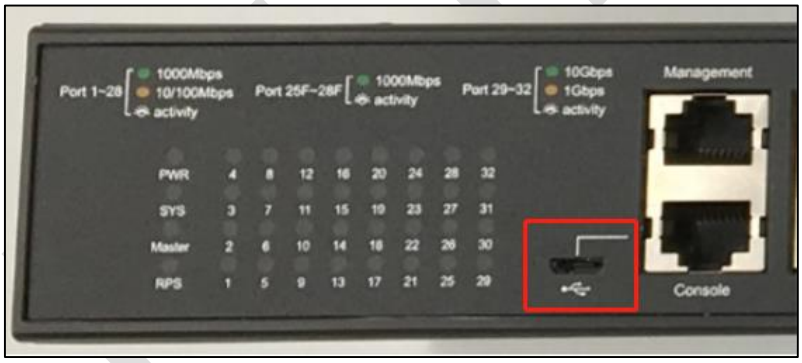
方式一：使用串口线进行连接（所有三层网管交换机均支持这种方式）,串口接电脑，RJ45 接口接交换机的 Console 接口。



注意：

- 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。

方式二：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。



Console 接口管理

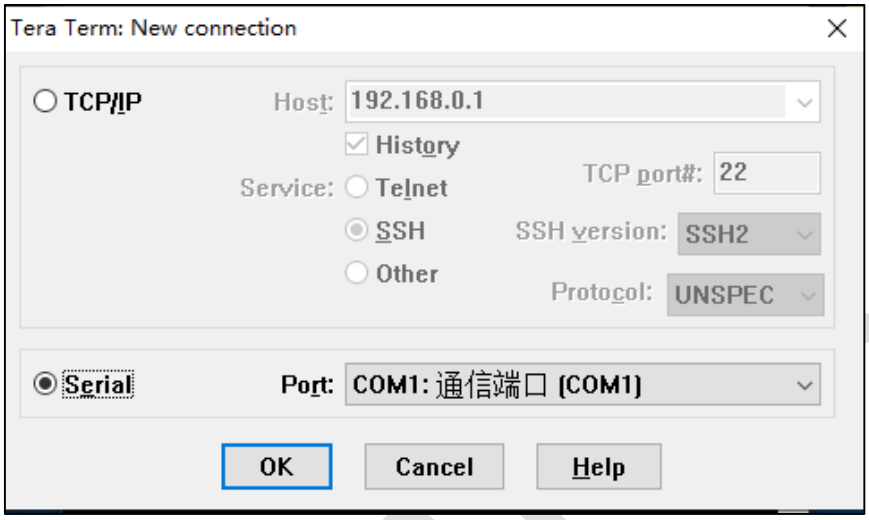
1、安装驱动

1） 如果电脑自带串口接口，不需要安装驱动；

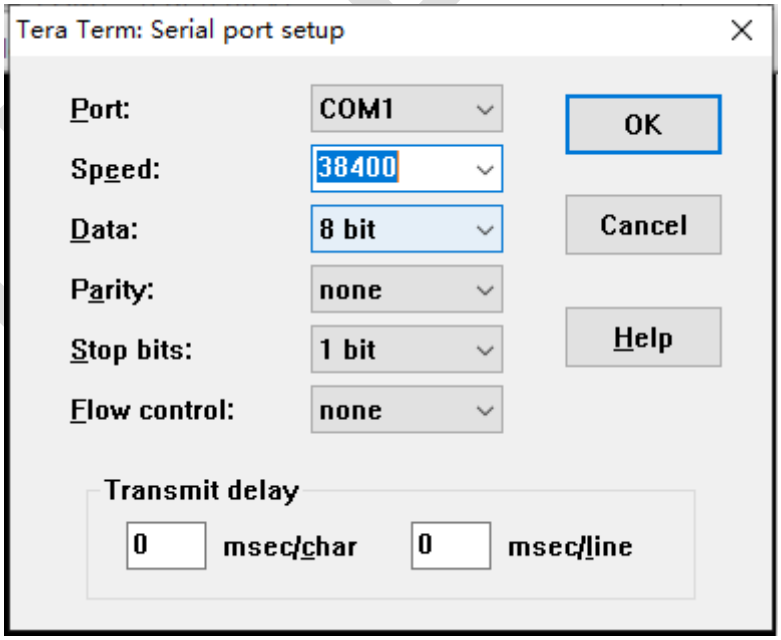
2） 如果使用 USB 转串口线，电脑上需要安装 USB 转串口线的驱动；

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”。

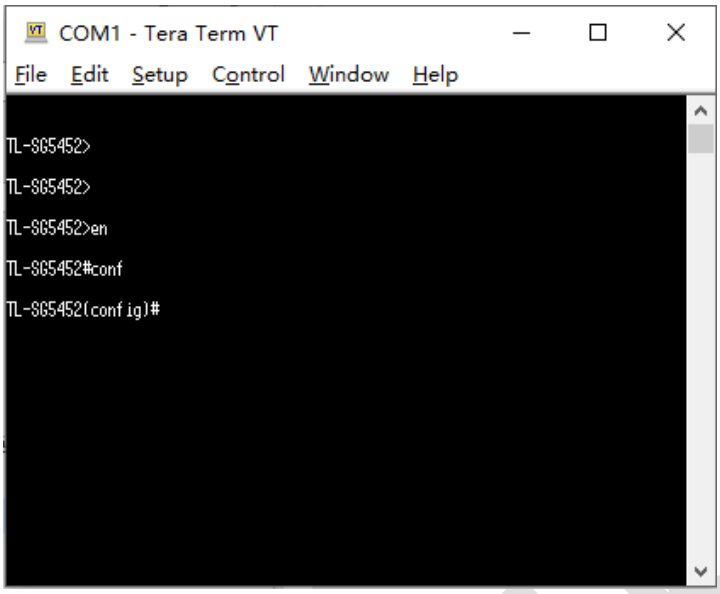
2、电脑上安装串口通信客户端软件 (比如：Tera Term、SerureCRT 等，本章节以 Tera Term 为例)，在串口通信客户端软件上新建连接，选择 Serial，以及对应的通信端口（不同电脑的通信端口会不一样)。



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



4、登录成功之后，直接在窗口中输入管理 CLI 命令即可。



2.1.3 通过 Management 接口管理交换机

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）

电脑连接方式

将电脑的网线连接到交换机的 Management 接口上。

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“系统管理”-“系统设置”-“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）

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

2.1.4 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：仅可以查看交换机各个功能的配置情况。

1、 web 配置举例

在交换机的“系统管理-用户管理-用户配置”界面，设置不同权限的管理员账号。

2、 CLI 配置

需求：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：如果忘记用户名和密码，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。

3、 创建特权模式密码

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。

CLI 配置举例：

需求：交换机中创建特权密码 test1234567

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#enable password test1234567

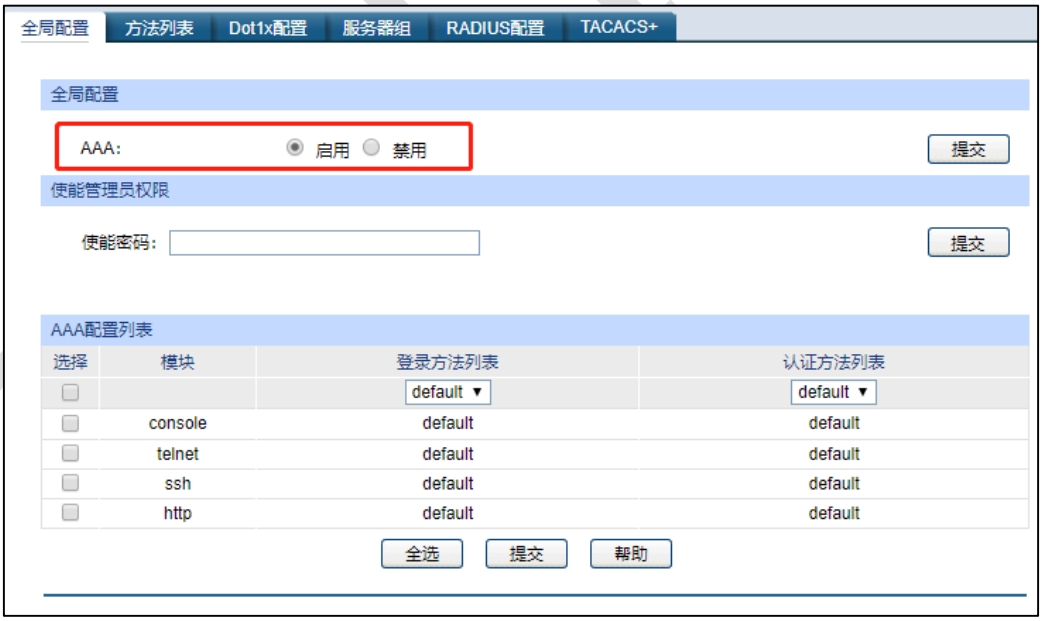
注意：如果忘记了特权密码，希望进入特权模式，交换机就只能复位了。

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：

步骤一：网络安全-AAA-全局配置，启用 AAA 功能。



步骤二：网络安全-AAA-方法列表，查看“登录方法”，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：如果启用了 AAA 认证，又忘记了密码，交换机就只能复位了。

5、终端权限管理

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：限制只有 192.168.0.0/24 网段的用户才能管理交换机。

系统管理-安全管理-安全配置 选择限制类型、接入方式，以及允许访问交换机用户的 IP 地址。

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

2.2 二层网管交换机管理方法介绍

2.2.1 通过业务接口管理交换机

二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

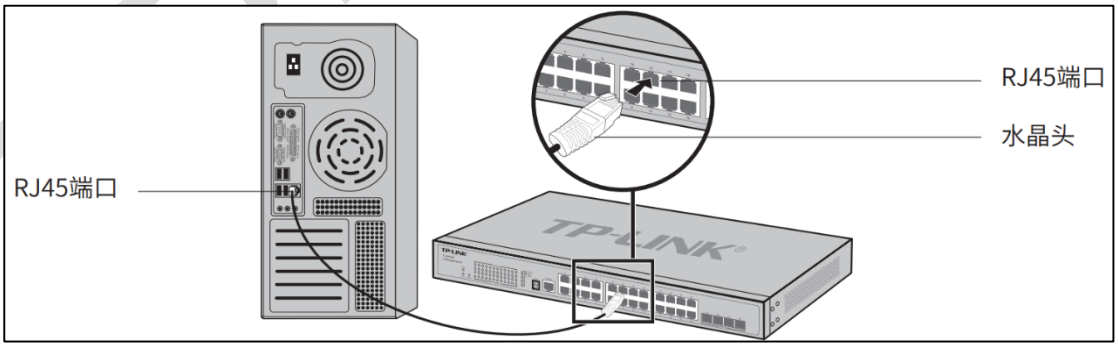
业务口默认管理用户名：admin

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：



第一、HTTP、HTTPS 管理

1、在电脑上打开浏览器，输入 http://192.168.0.1 或者 https://192.168.0.1 （浏览器建议使用 Chrome、Firefox、Edge 或 IE9 以上的浏览器）。

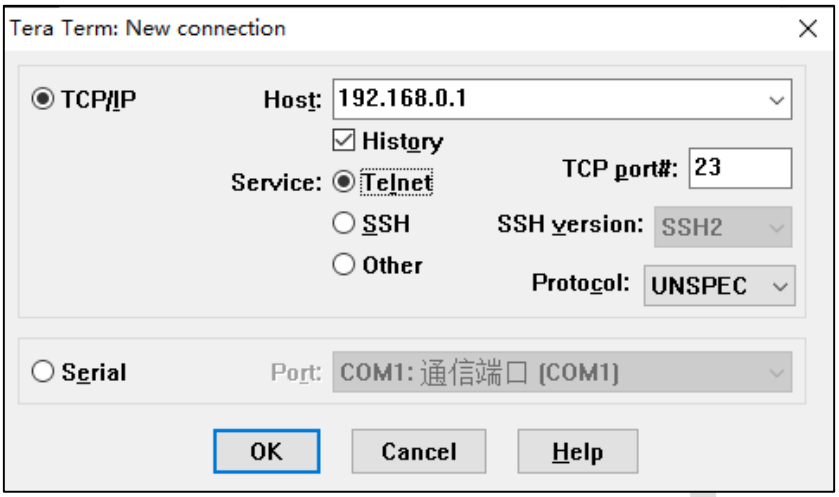
1、输入正确的用户名和密码。

注意：

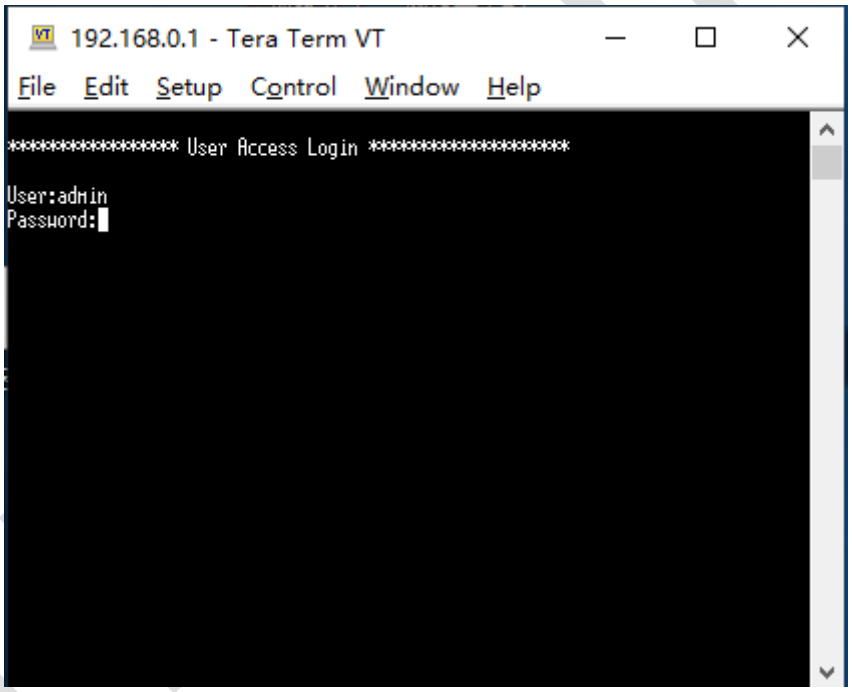
- 如果使用 HTTPS 管理，浏览器会提示安全风险，在浏览器中点击“详细信息”—”继续转到网页”即可。（不同浏览器提示可能会略有不同）
- 如果输入正确用户名和密码之后，管理页面显示不全，可能是由于浏览器缓存原因造成，此时按 Ctrl+F5 刷新页面即可。

第二、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。

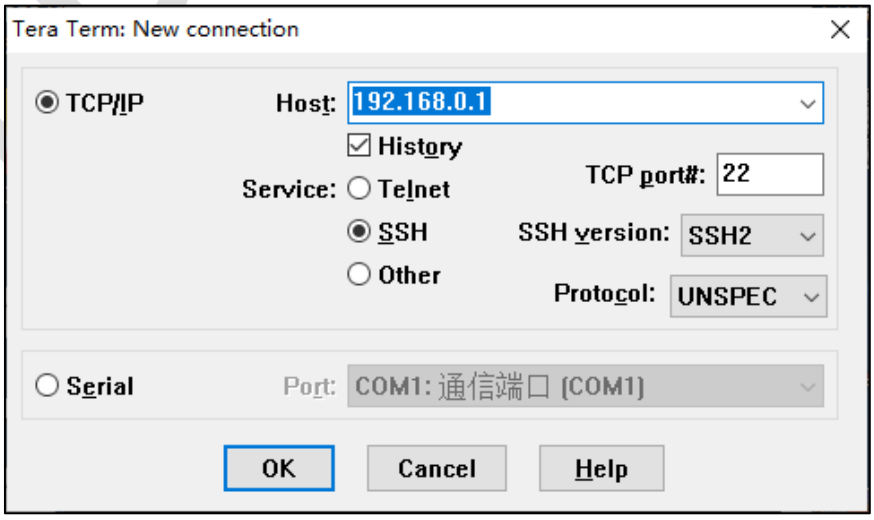


第三、SSH 管理

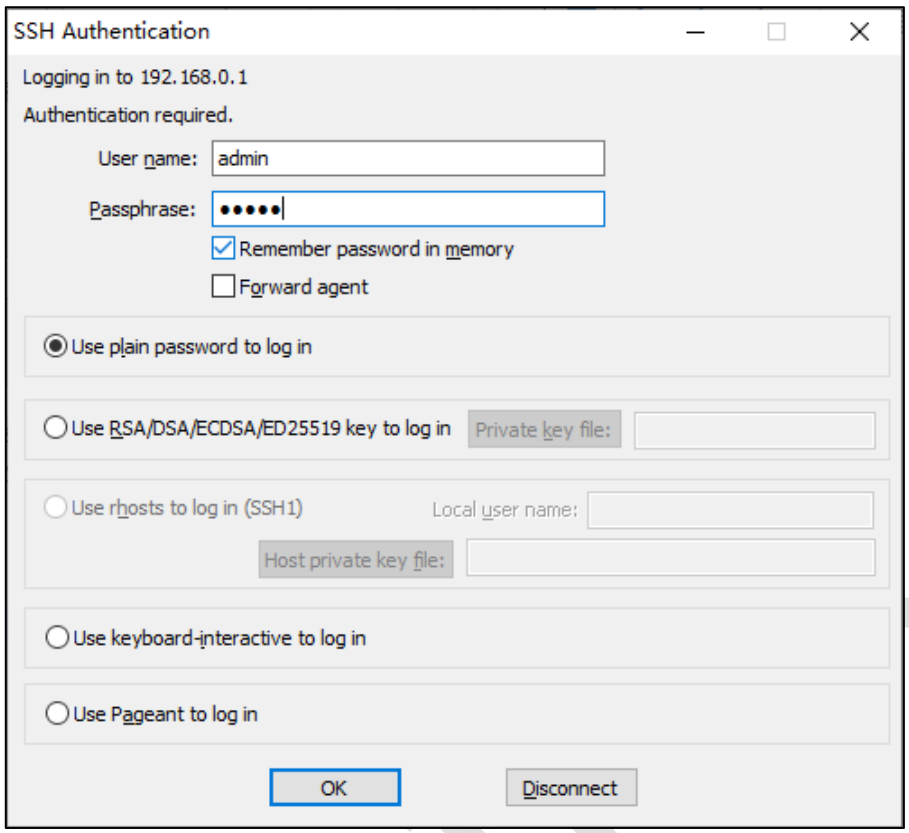
SSH 管理功能在交换机上默认情况下是禁用的，需要先使用其他管理方式进入交换机开启该功能才可以进行 SSH 管理。

1、电脑登录交换机的 Web 页面，“系统管理”-“安全管理”-“SSH 配置”，启用 SSH 功能。

2、电脑上安装 SSH 客户端软件（比如：Tera Term、SecureCRT 等，本章节以 Tera Term 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。



第四、SNMP 管理

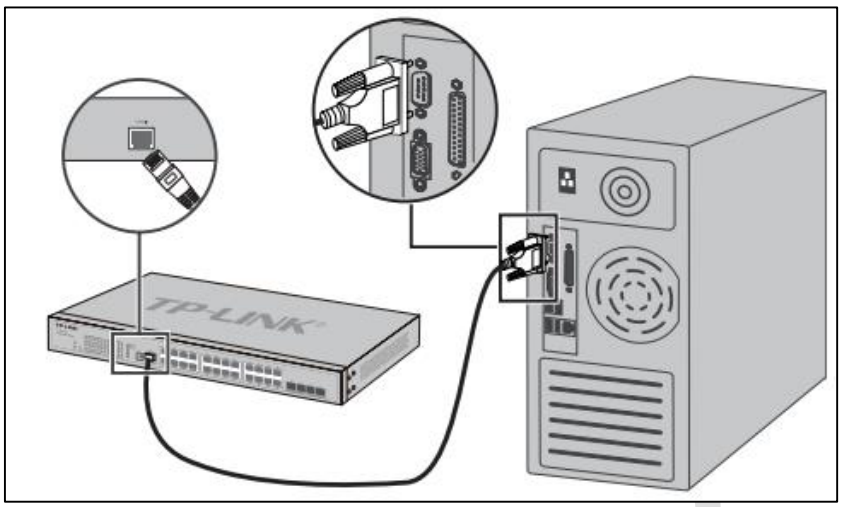
可以参考《SNMP 基础设置方法介绍-。

2.2.2 通过 Console 接口管理交换机

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。

电脑连接方式

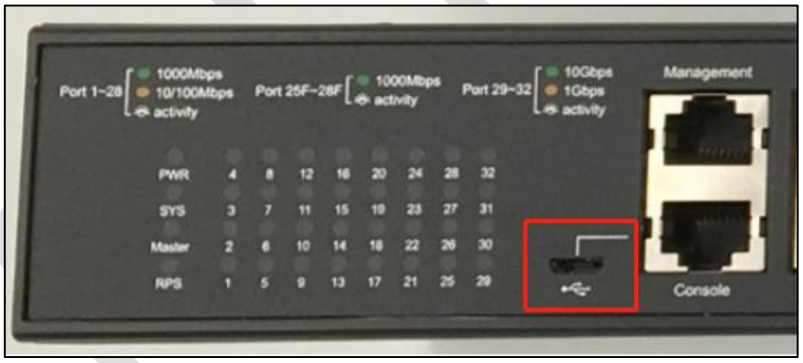
方式一：使用串口线进行连接（所有三层网管交换机均支持这种方式）,串口接电脑，RJ45 接口接交换机的 Console 接口。



注意：

- 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。

方式二：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。



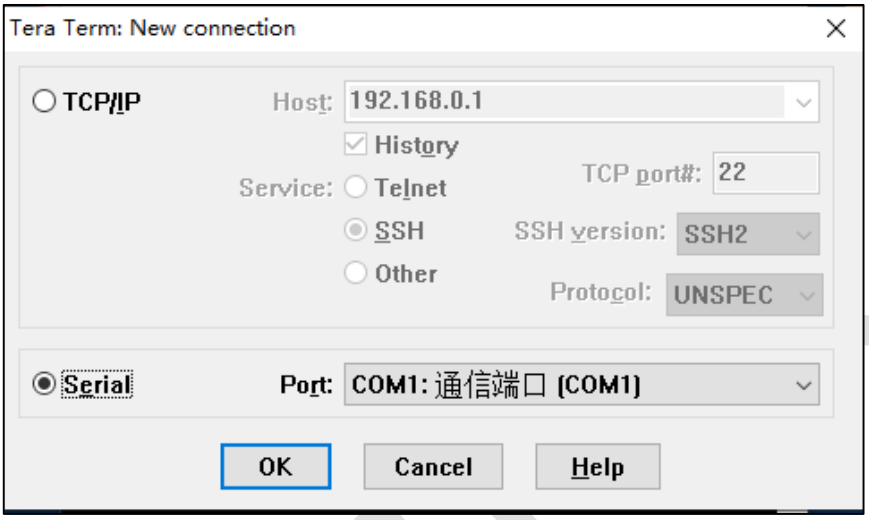
Console 接口管理

1、安装驱动

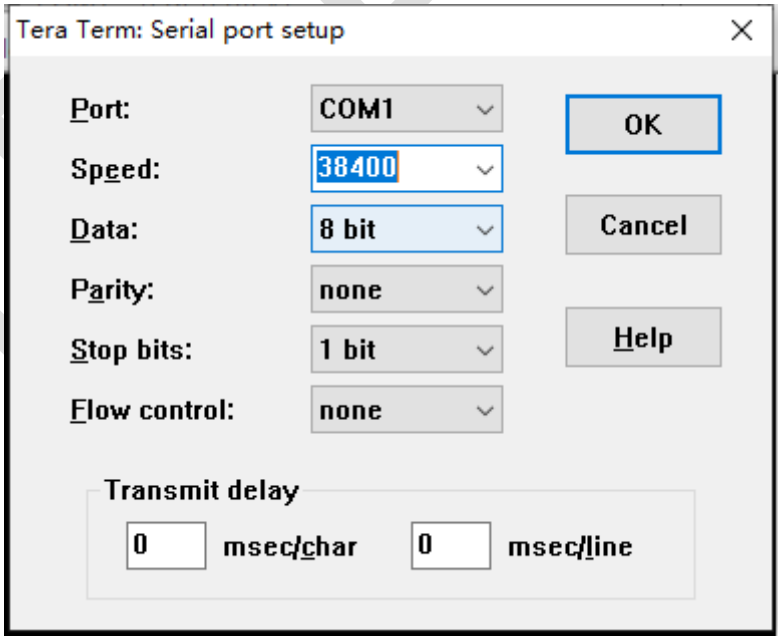
1） 如果电脑自带串口接口，不需要安装驱动；

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；

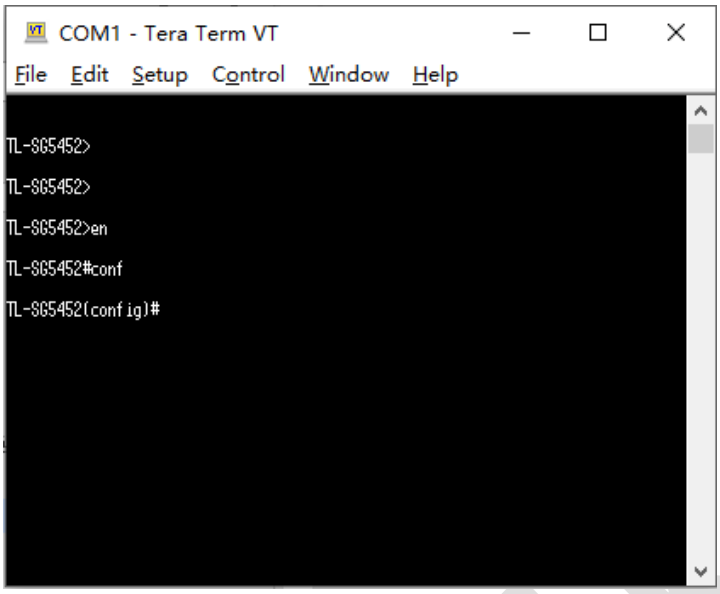
2、电脑上安装串口通信客户端软件 (比如：Tera Term、SerureCRT 等，本章节以 Tera Term 为例)，在串口通信客户端软件上新建连接，选择 Serial，以及对应的通信端口（不同电脑的通信端口会不一样)。



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



4、登录成功之后，直接在窗口中输入管理 CLI 命令即可。



2.2.3 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：仅可以查看交换机各个功能的配置情况。

1、web 配置举例

在交换机的“系统管理-用户管理-用户配置”界面，设置不同权限的管理员账号。

2、CLI 配置

需求：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：如果忘记用户名和密码，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。

3、创建特权模式密码

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。

CLI 配置举例：

需求：交换机中创建特权密码 test1234567

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#enable password test1234567

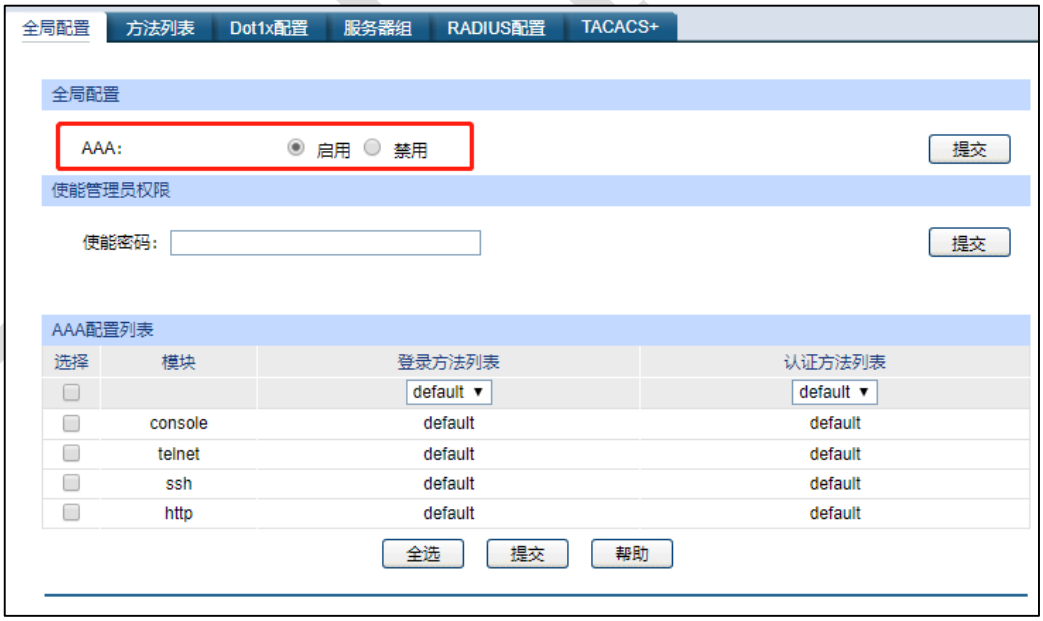
注意：如果忘记了特权密码，希望进入特权模式，交换机就只能复位了。

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：

步骤一：网络安全-AAA-全局配置，启用 AAA 功能。



步骤二：网络安全-AAA-方法列表，查看“登录方法”，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：

1、如果启用了 AAA 认证，又忘记了密码，交换机就只能复位了。

2、早期软件版本的交换机不支持 AAA 认证，需要通过在 Console 接口中使用 line 命令配置 Console 接口的登录密码，具体配置过程如下：

TL-SG3210>enable

TL-SG3210#configure

TL-SG3210(config)#line console 0

TL-SG3210(config-line)#login local

5、终端权限管理

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：限制只有 192.168.0.0/24 网段的用户才能管理交换机。

系统管理-安全管理-安全配置 选择限制类型、接入方式，以及允许访问交换机用户的 IP 地址。

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

2.3 简单 WEB 网管交换机管理方法介绍

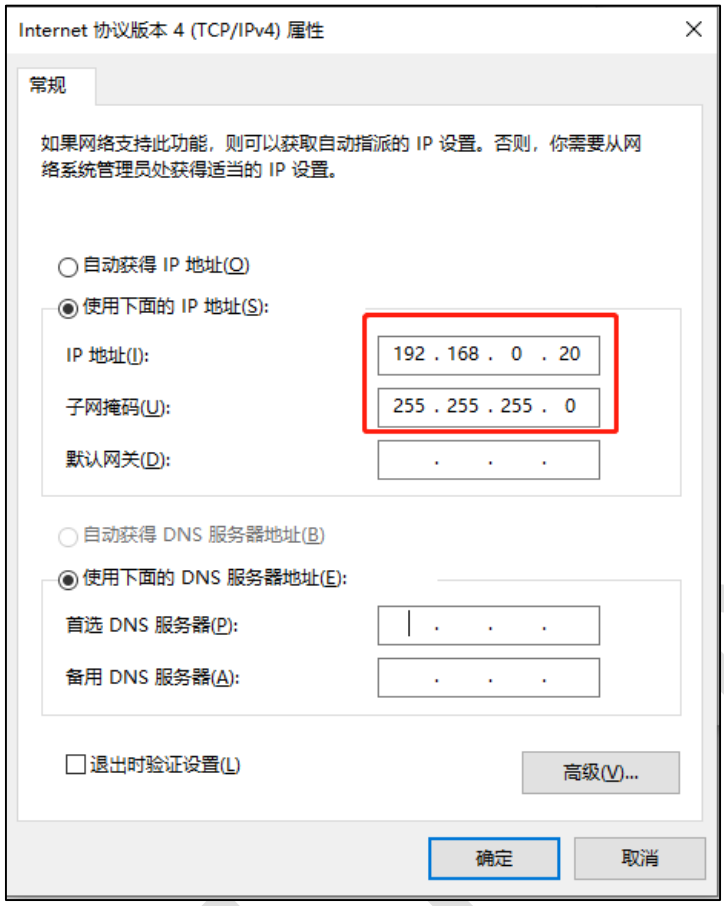
2.3.1 简单 WEB 管理交换机介绍

简单 Web 网管交换机是 TP-LINK2 系列简单网管交换机，目前已经全系升级成云交换系列，本篇文章针对以前老机型的设备管理方式进行介绍，老版本的 2 系列简单 WEB 网管交换机可以通过 Web 界面和 TP-LINK Web 网管交换机客户端进行管理。

2.3.2 WEB 管理

1、 将交换机的模式开关拨动到"Web 管理"模式，使用网线将电脑网口与交换机的任意接口相连。

2、 将电脑的IP地址设置成与交换机同一网段，出厂状态下，交换机默认IP是192.168.0.1。



3、在电脑上打开浏览器，输入 192.168.0.1，即可正常管理交换机。

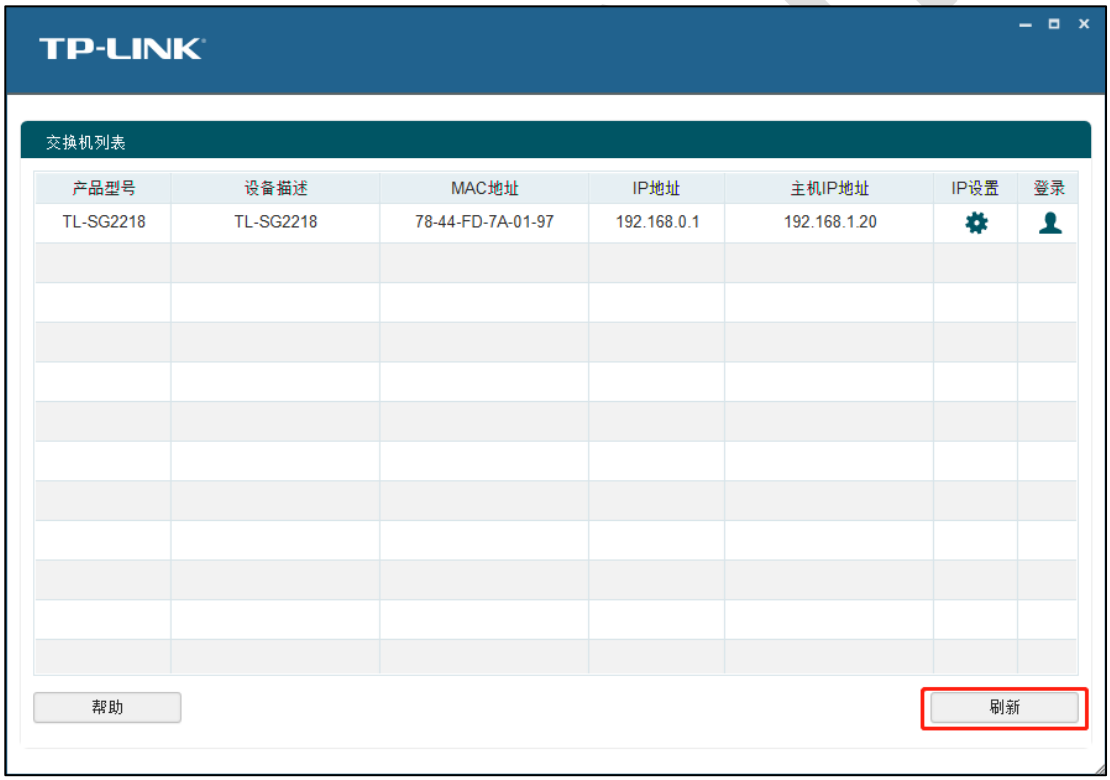
注意：如果输入正确用户名和密码之后，管理页面显示不全，可能是由于浏览器缓存原因造成，此时按 Ctrl+F5 刷新页面即可。

2.3.3 TP-LINK Web 网管交换机客户端应用程序管理

1、设置电脑上安装“TP-LINK Web 网管交换机客户端应用程序”（下载地址：https://service.tp-link.com.cn/detail_download_5553.html）。

2、设置电脑网口与交换机的任意接口相连。

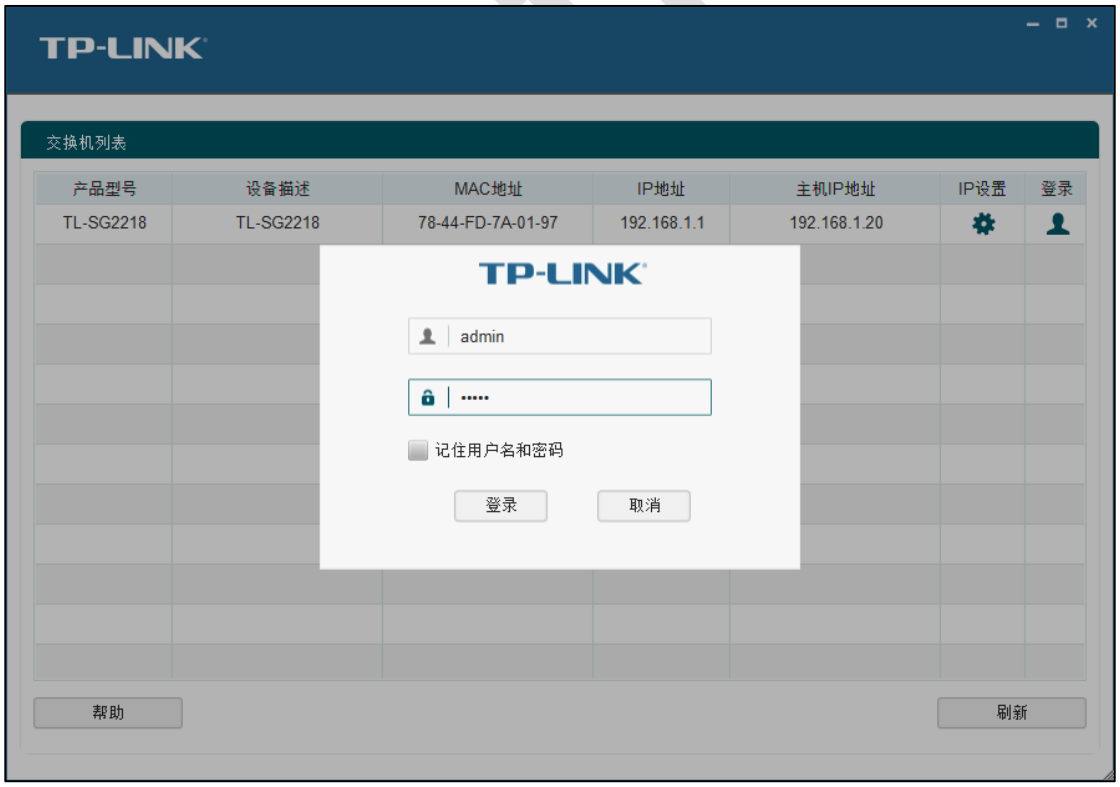
3、运行“TP-LINK Web 网管交换机客户端应用程序”，点击“刷新”按钮。



4、如果交换机 IP 与主机 IP 不在同一个网段，点击 IP 设置，将交换机 IP 修改为与主机 IP 在同一网段。(需要知道交换机正确的用户名和密码才能修改)

5、点击“登录”，输入正确的用户名和密码，即可管理交换机。


TP-LINK
交换机列表
产品型号
设备描述
MAC地址
IP地址
主机IP地址
IP设置
登录
TL-SG2218
TL-SG2218
78-44-FD-7A-01-97
192.168.1.1
192.168.1.20
帮助
刷新


TP-LINK
交换机列表
产品型号
设备描述
MAC地址
IP地址
主机IP地址
IP设置
登录
TL-SG2218
TL-SG2218
78-44-FD-7A-01-97
192.168.1.1
192.168.1.20
TP-LINK
admin
记住用户名和密码
登录
取消
帮助
刷新

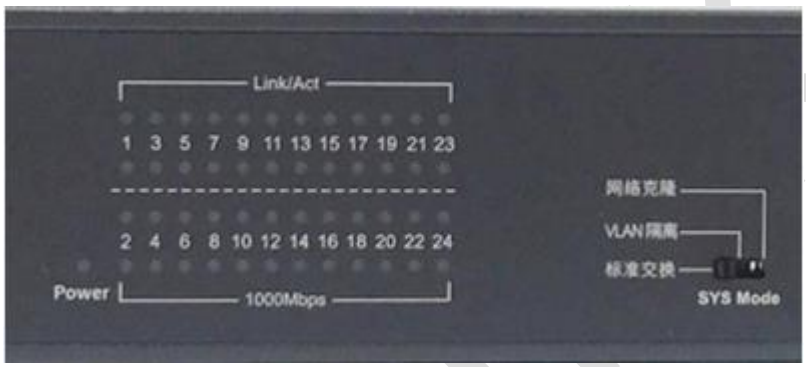

TP-LINK
TL-SG2218 1.0
系统管理
二层交换
监控
VLAN
服务质量
帮助
保存
返回
系统信息
IP设置
用户设置
备份与还原
系统重启
系统恢复
系统升级
系统信息
设备描述：
TL-SG2218
MAC地址：
78-44-FD-7A-01-97
IP地址：
192.168.1.1
子网掩码：
255.255.255.0
默认网关：
0.0.0.0
软件版本：
1.0.0 Build 20180522 Rel.57913
硬件版本：
TL-SG2218 1.0
设备描述：
TL-SG2218
应用
注意：
设备描述长度不能超过32个字符。

2.4 各种交换机硬件拨码开关介绍

2.4.1 硬件拨码开关介绍

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交换机的硬件拨码开关及一些使用说明。

2.4.2 1 系列交换机



标准交换：所有端口自由通信，适用于普通数据传输环境；

VLAN 隔离：端口与端口之间相互隔离，只能与上联口通信，适用于连接无线 AP 的使用场景，抑制网络风暴，提升网络性能。适合用在一些酒店、宿舍、无线覆盖，这种终端只需要上网不需要相互访问的场景中；

网络克隆：所有端口的 IEEE802.3x 流控功能关闭，适合用在一些使用广播或组播传输数据的环境中，如：学校视频教学、网吧网络克隆等。

2.4.3 1 系列 POE 交换机

模式组合 1

VLAN 隔离：端口与端口之间相互隔离，只能与上联口通信，适用于连接无线 AP 的使用场景，抑制网络风暴，提升网络性能。适合用在一些酒店、宿舍、无线覆盖，这种终端只需要上网不需要相互访问的场景中；

视频监控：通过调整交换机中的缓存资源，优化视频传输效率，减少监控网络中卡顿和马赛克现象，适合用在一些视频监控应用场景；

标准交换：所有端口自由通信，适用于普通数据传输环境；

模式组合 2

标准交换：所有端口自由通信，适用于普通数据传输环境；

1~4 延长 (10Mbps)：1～4 号 PoE 端口通过降低协商速率，实现更远距离 (200~300m) 的数据传输，适合用在一些网线较长的视频监控应用场景。

2.4.4 2 系列非云管理机型

VLAN 隔离：端口与端口之间相互隔离，只能与上联口通信，适用于连接无线 AP 的使用场景，抑制网络风暴，提升网络性能。适合用在一些酒店、宿舍、无线覆盖，这种终端只需要上网不需要相互访问的场景中；

Web 管理：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；

标准交换：所有端口自由通信，适用于普通数据传输环境。

2.4.5 2 系列云管理机型

VLAN 隔离：端口与端口之间相互隔离，只能与上联口通信，适用于连接无线 AP 的使用场景，抑制网络风暴，提升网络性能。适合用在一些酒店、宿舍、无线覆盖，这种终端只需要上网不需要相互访问的场景中；

云管理：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；同时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。

标准交换：所有端口自由通信，适用于普通数据传输环境；

2.4.6 工业级交换机

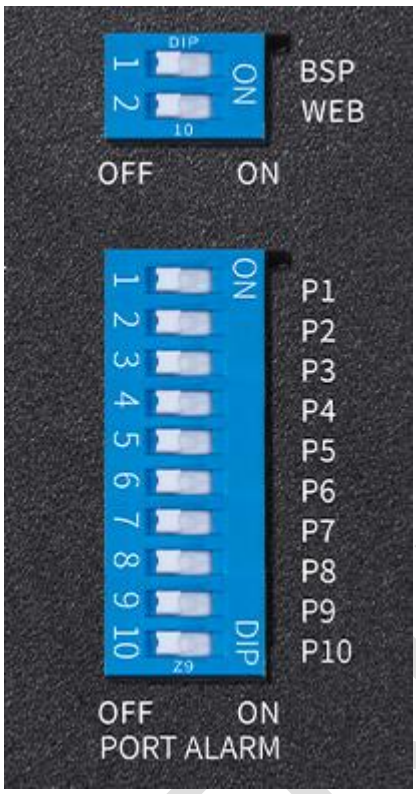
类型 1

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

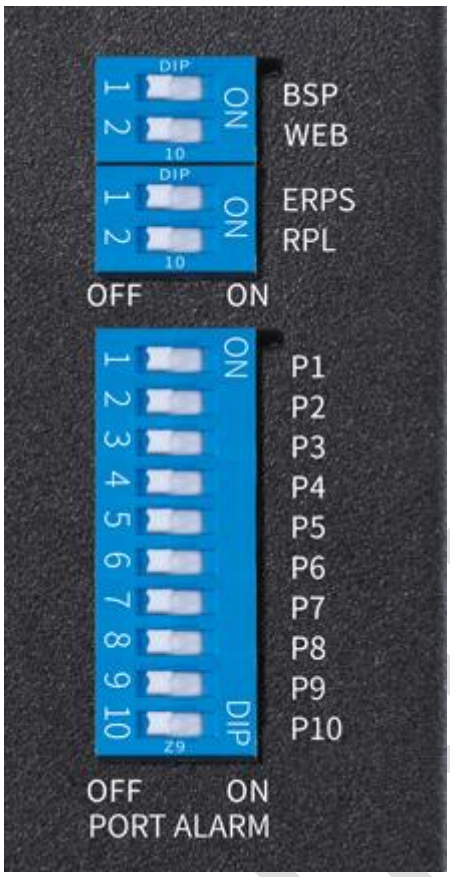


WEB：交换机支持本地 Web 管理，支持配置端口参数，支持设置端口速率，支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置；部分最新硬件版本（3.0 及以上）的工业级交换机也支持云管理功能，可以通过商云 APP 或者商用网络云平台进程远程管理。

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；

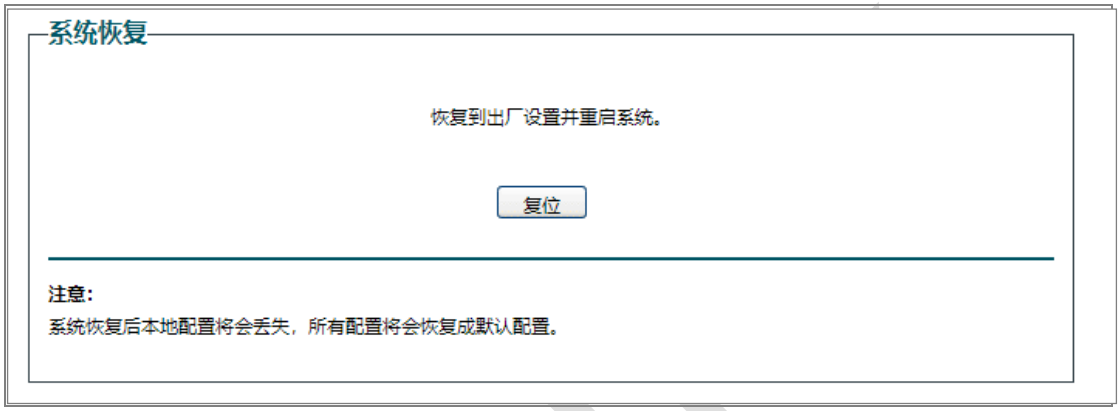
RPL：默认关闭，开启后，配置端口 1 为 RPL 口。

2.5 各种交换机复位方法介绍

2.5.1 2 系列交换机

1、Web 管理界面复位方法

登录交换机管理页面“系统管理”-“系统工具”-“系统恢复”,点击“复位”按钮即可。



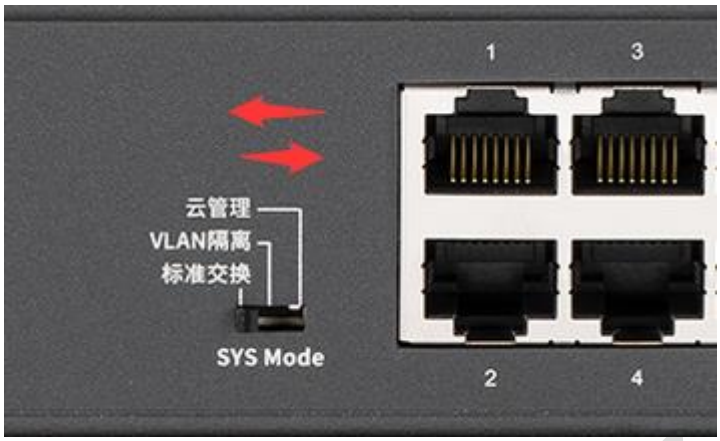
2、硬件复位方法

2.1、非云管理交换机

模式开关由 **Web 管理**拨至**标准交换**，再快速（2s 内）拨回 **Web 管理。**

2.2、云管理交换机

模式开关由**云管理**拨至**标准交换**，再快速（2s 内）拨回**云管理。**



2.5.2 3/5/6/7/8 系列交换机

1、Web 管理界面复位方法

登录交换机管理页面“系统管理”-“系统工具”-“软件复位”,点击“复位”按钮即可。

2、Console 接口复位方法

2.1、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“二层网管交换机的管理方法”或“三层网管交换机的管理方法”。

2、使用 reset 命令对交换机进行复位.

复位命令举例：

TL-SH7428>enable

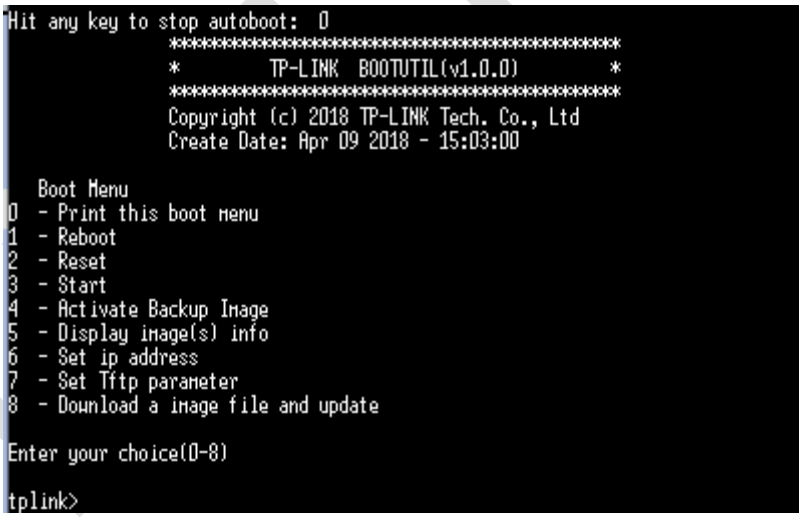
TL-SH7428#reset

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

2.2、Console 接口设置了登录密码

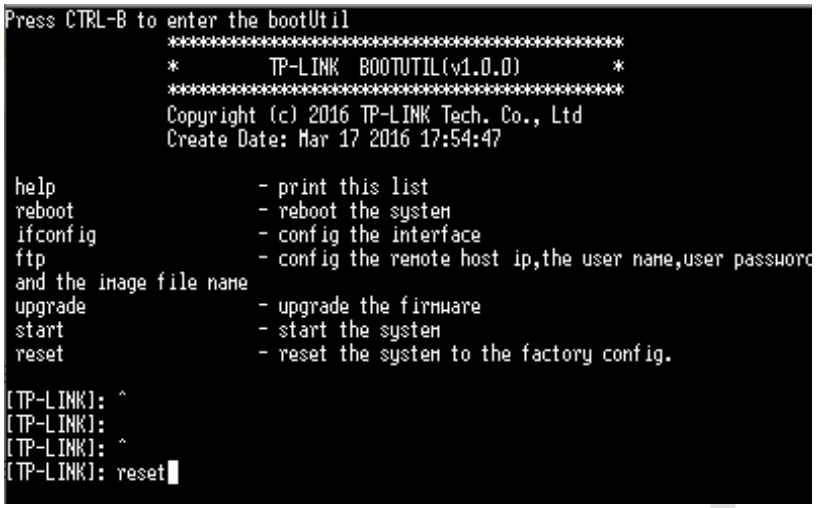
1、电脑连接交换机的 Console 接口，具体连接和设置方法参见“二层网管交换机的管理方法”或“三层网管交换机的管理方法”。

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。


Press CTRL-B to enter the bootUtil
****
* TP-LINK BOOTUTIL(v1.0.0) *
****
Copyright (c) 2016 TP-LINK Tech. Co., Ltd
Create Date: Mar 17 2016 17:54:47
help - print this list
reboot - reboot the system
ifconfig - config the interface
ftp - config the remote host ip,the user name,user passwor
and the image file name
upgrade - upgrade the firmware
start - start the system
reset - reset the system to the factory config.
[TP-LINK]: ^
[TP-LINK]:
[TP-LINK]: ^
[TP-LINK]: reset

第3章 交换设置

3.1 交换机端口监控配置指南

3.1.1 应用介绍

端口监控是一种数据包获取技术，可以实现将一个或几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），通过对收集到的数据包进行分析，可以达到网络监控或排除网络故障的目的。

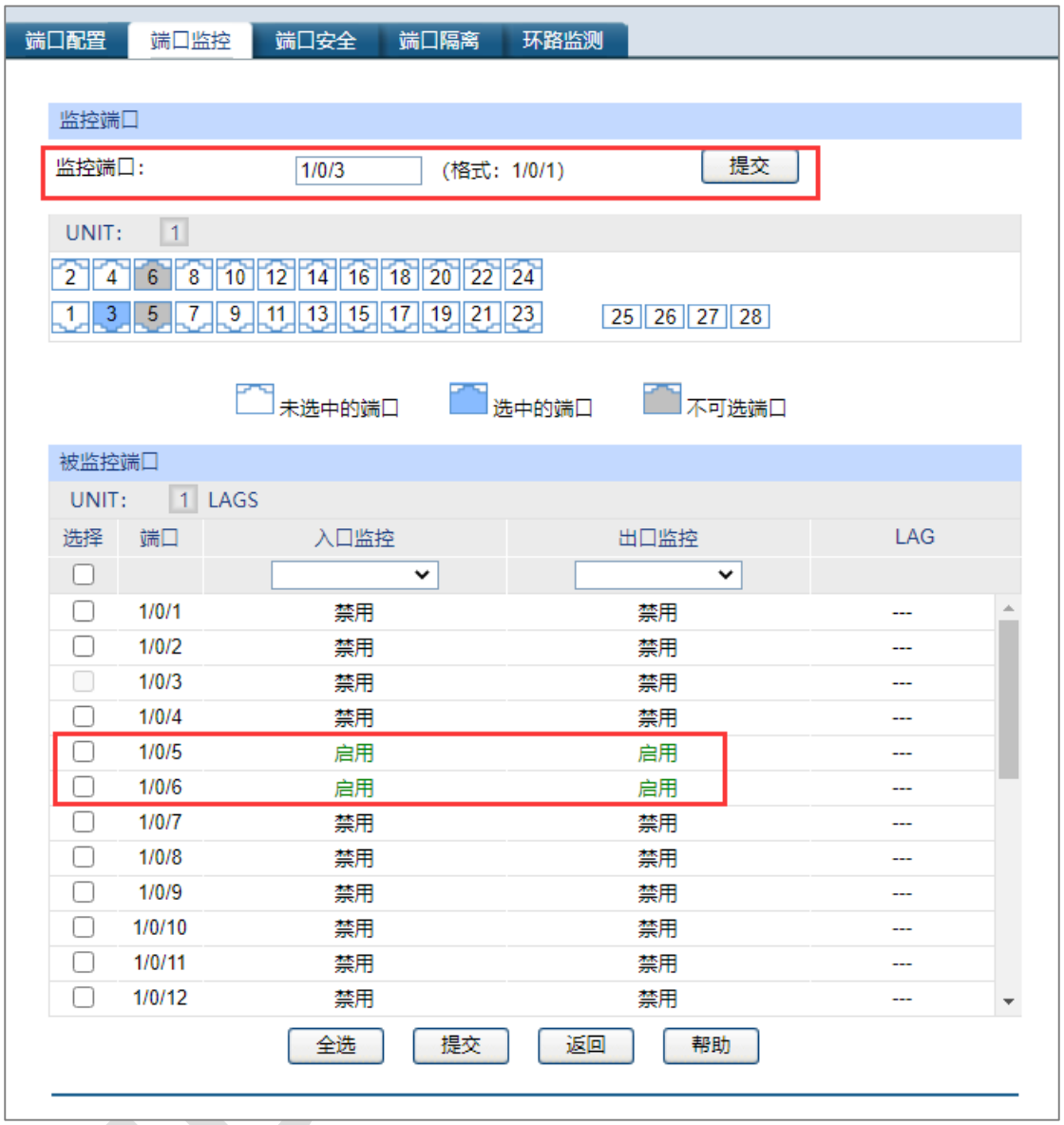
3.1.2 需求介绍

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：

3.1.3 设置方法

1、在“二层交换->端口管理->端口监控”中，点击编辑，如下如所示。

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 5.6 口，入口出口均选择启用，点击提交，如下图所示。



2、提交后可以看到被监控端口状态列表：

至此已完成设置，注意保存配置以免掉电导致配置丢失。

3.1.4 配置注意事项

- 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。

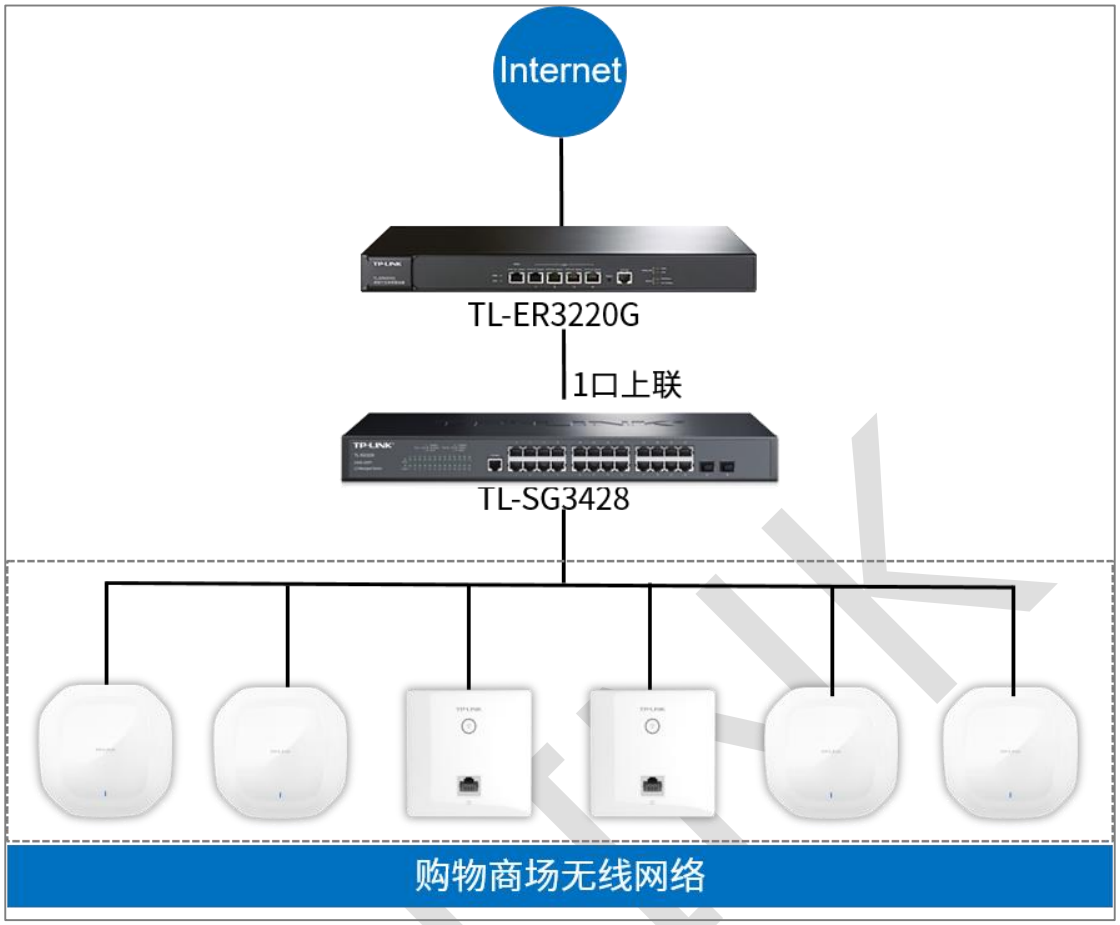
3.2 交换机端口隔离配置指南

3.2.1 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。

3.2.2 需求介绍

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：

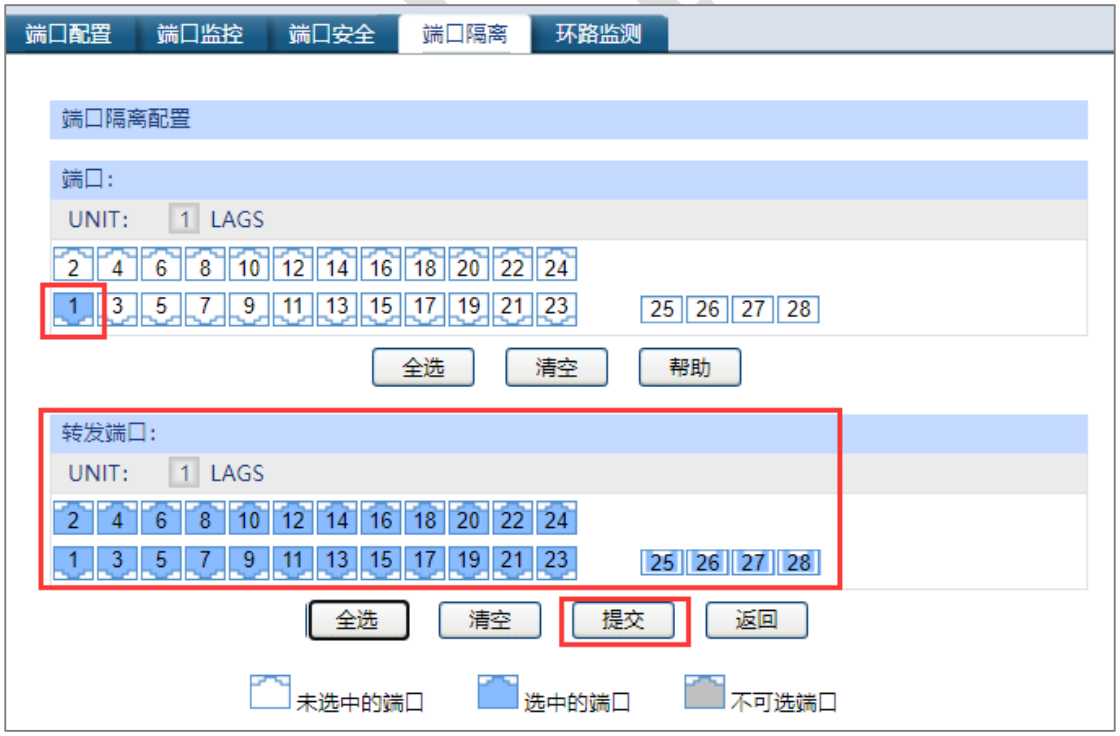


3.2.3 设置方法

在“二层交换->端口管理->端口隔离”中，点击编辑，选择对应端口的转发端口，本次举例设置 2-28 端口的转发端口为 1 端口；因为 1 口是上联口，1 端口的转发端口为所有端口，如下如所示。

1、设置 2-28 端口只转发到 1 端口：

2、设置 1 端口可以转发 1-28 端口：



设置完端口和转发端口的关系，点击提交，可以看到如下的端口转发列表：

至此已完成设置，2-28 口上的 AP 只能和 1 口接的 AC 设备通讯，AP 相互之间不能通讯。另外请注意保存配置以免掉电导致配置丢失。

3.3 交换机端口安全配置指南

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 需求介绍

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。

3.3.3 设置方法

1、在交换机 web 界面“二层交换 -> 端口管理 -> 端口安全”，设置端口安全，端口 1 最大学习地址数为 0：

2、针对端口 1 做静态地址绑定，绑定允许上网的设备。

进行如上设置后，则只有 MAC 为 80-EA-07-0D-0B-CC 的设备接在端口 1 的 VLAN1 下能上网，其他设备接到端口 1 则无法上网。

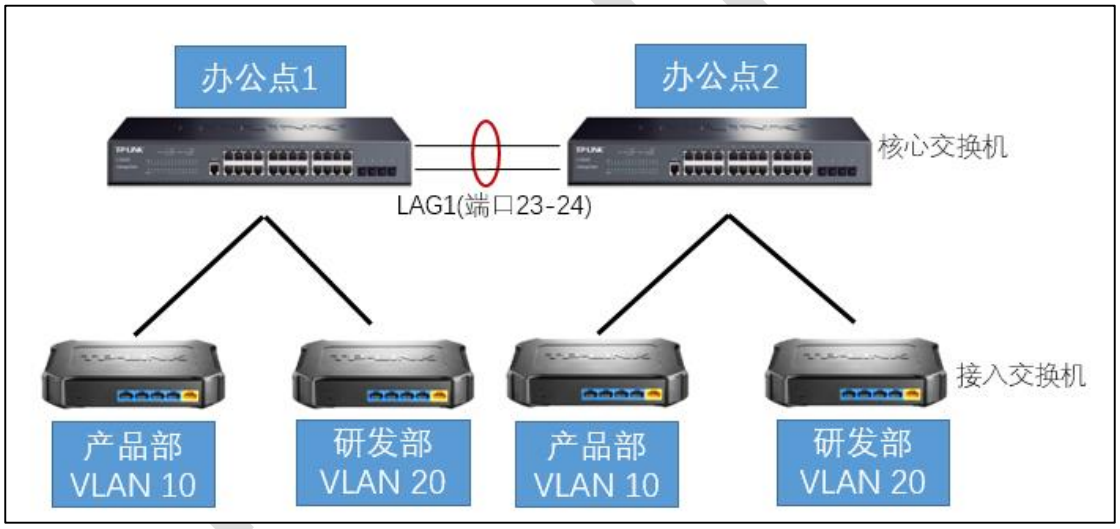
3.4 交换机端口汇聚配置指南

3.4.1 应用介绍

端口汇聚功能是将交换机的多个物理端口汇聚在一起形成一个逻辑上的物理端口，同一汇聚组内的多条链路则可视为一条逻辑链路。端口汇聚主要有两个作用：带宽叠加、链路备份。

3.4.2 需求介绍

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。本文以 TL-SG5428PE 为例介绍如何在（3/5/6/7/8）系列交换机设置端口汇聚以及在 VLAN 设置时如何使用该功能。网络拓扑如下：



3.4.3 设置方法

1、静态聚合设置方法

在“二层交换->汇聚管理->手动配置”中，下拉选择 LAG 组号如 LAG1，选择需要进行汇聚的端口如 23-24 号端口，点击提交。

2、动态聚合设置方法

在"二层交换->汇聚管理->LACP 配置"中，选择需要进行汇聚的端口，输入管理 Key（即 LAG 组号 1-8），状态下拉选择开启，点击提交。

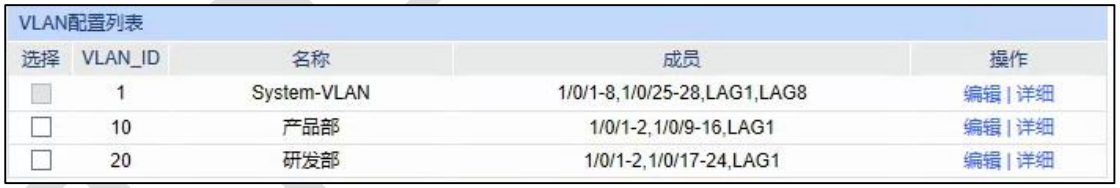
3、 VLAN 设置时如何使用汇聚端口

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、 设置端口类型为 TRUNK。在“VLAN->802.1Q VLAN->端口配置”中，在 VLAN 端口配置的 UNIT 列表中选中 LAGS，将端口 LAG1 的端口类型配置为 TRUNK，点击提交。

2、划分 VLAN：在“VLAN->802.1Q VLAN->VLAN 配置”中，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，再选择对应的汇聚端口，点击提交。如下图 LAG1 口为 Tagged，9-16 口为 Untagged。

3、VLAN20 的设置重复第 2 步即可。添加完成后，VLAN 列表如下：



VLAN配置列表

选择	VLAN_ID	名称	成员	操作
	1	System-VLAN	1/0/1-8,1/0/25-28,LAG1,LAG8	编辑 | 详细
	10	产品部	1/0/1-2,1/0/9-16,LAG1	编辑 | 详细
	20	研发部	1/0/1-2,1/0/17-24,LAG1	编辑 | 详细

至此已完成设置，注意保存配置以免掉电导致配置丢失。

3.4.4 配置注意事项

- 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。

3.5 交换机地址表管理功能使用指南

3.5.1 交换机地址表介绍

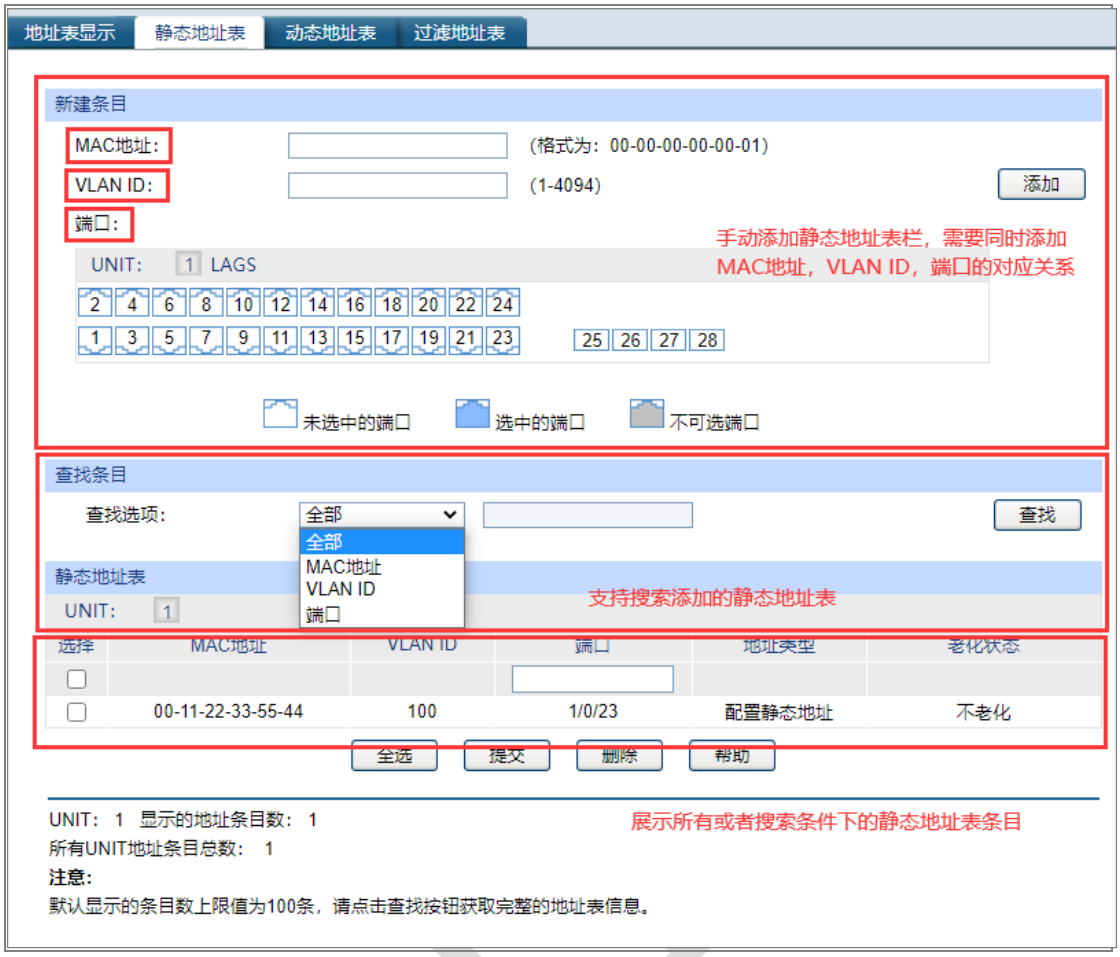
TP-LINK 3/5/6/7/8 系列交换机都带有地址表管理功能，交换机的地址表管理功能是管理交换机所学习到 MAC 的集中展示的地方，通过交换机的地址表管理功能，可以优化网络流量或者保障络安全。交换机的地址表管理功能主要分以下几个功能模块，现分别简介下各个模块的功能和应用场景。

3.5.2 地址表显示

该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。

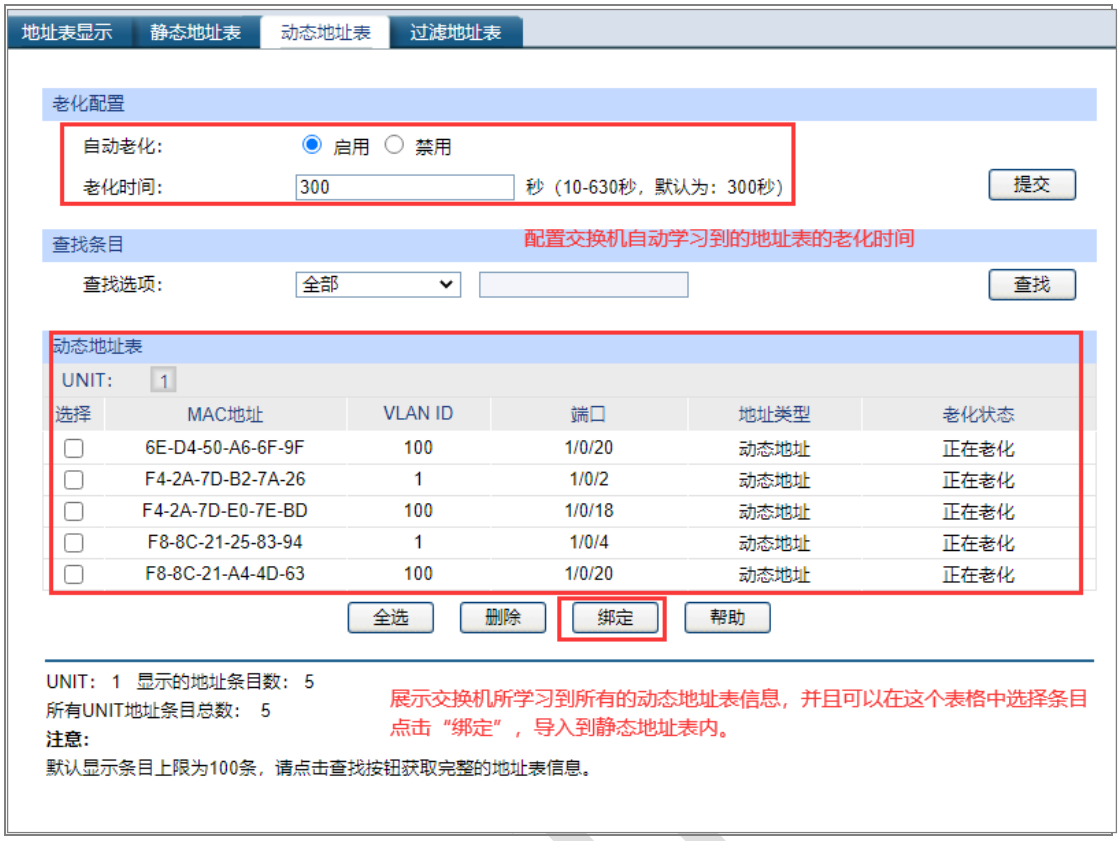
3.5.3 静态地址表

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。



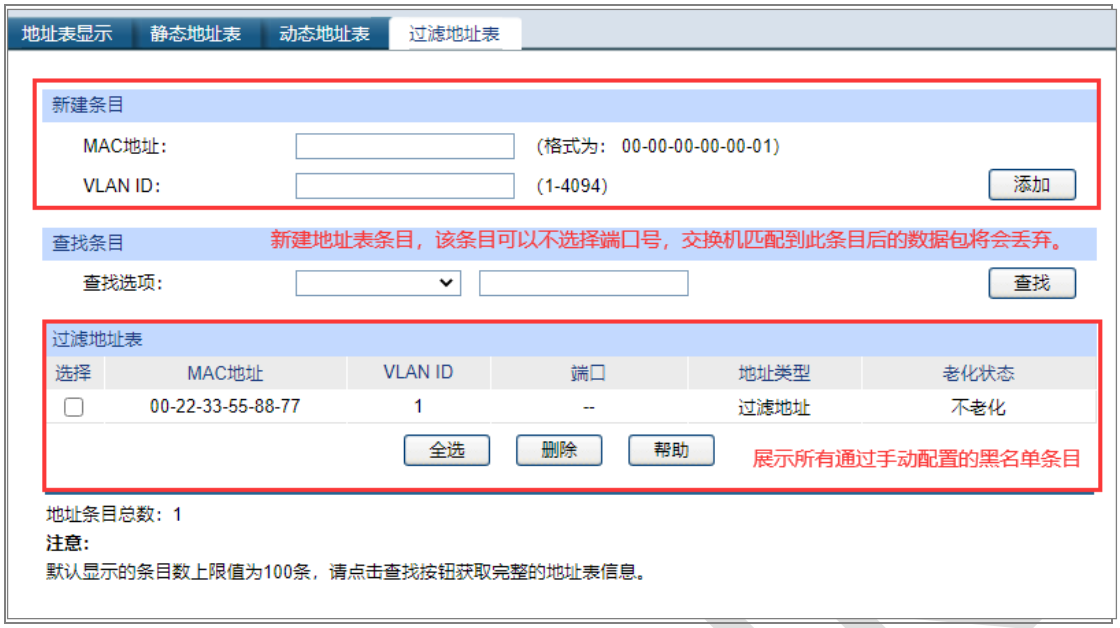
3.5.4 动态地址表

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。



3.5.5 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。


地址表显示
静态地址表
动态地址表
过滤地址表
新建条目
MAC地址：
（格式为： 00-00-00-00-00-01）
VLAN ID：
（1-4094）
添加
查找条目
新建地址表条目，该条目可以不选择端口号，交换机匹配到此条目后的数据包将会丢弃。
查找选项：
查找
过滤地址表
选择
MAC地址
VLAN ID
端口
地址类型
老化状态
00-22-33-55-88-77
1
--
过滤地址
不老化
全选
删除
帮助
展示所有通过手动配置的黑名单条目
地址条目总数：1
注意：
默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

第4章 堆叠功能

4.1 交换机堆叠配置指导

4.1.1 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。

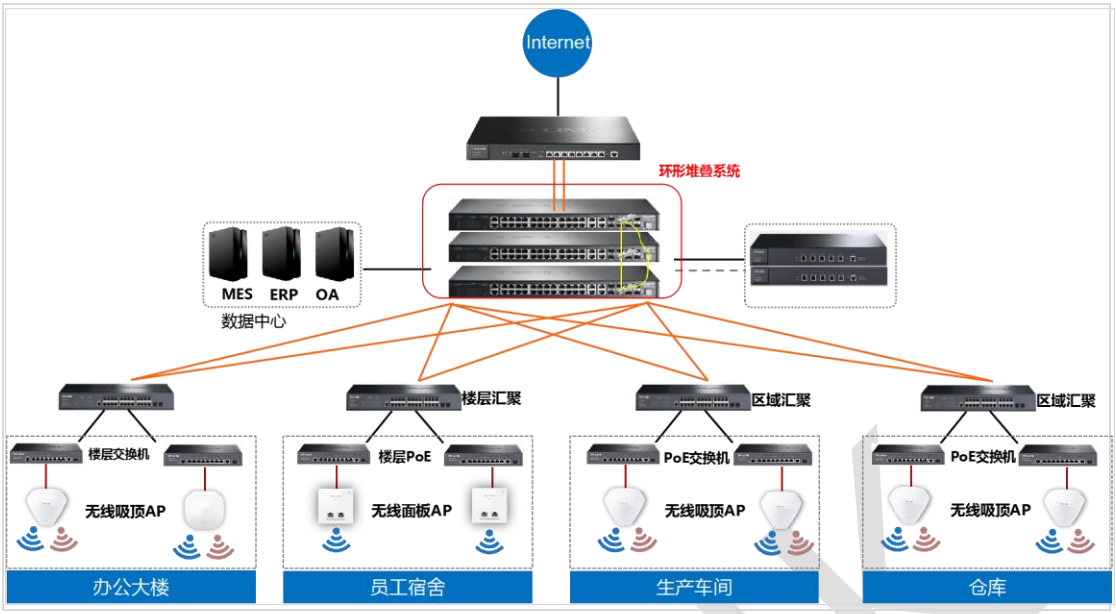
4.1.2 需求介绍

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-SH8434 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。



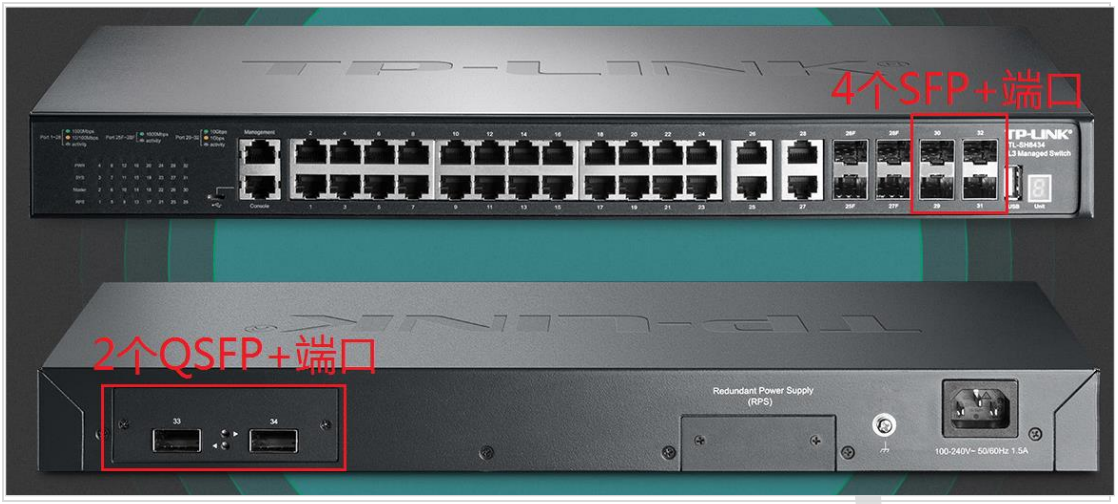
4.1.3 设置方法

第一步、堆叠前准备

准备三台出厂状态下的 TL-SH8434 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。

第二步、堆叠口的配置

TL-SH8434 有 6 个端口可以配置成堆叠端口，其中 4 个万兆 SFP+和 2 个 QSFP+端口，如图：



1、分别登录 3 台设备的 web 界面，在“堆叠功能—堆叠管理—堆叠配置”界面设置堆叠口，将选中的堆叠口状态设置成启用，本次选择将交换机的 29.30 口设置成堆叠口。

2、在进行物理连线之前分别配置三台交换机：

(1) 设置堆叠名称：在“堆叠功能—堆叠管理—堆叠配置”页面设置堆叠名称（可选操作）；

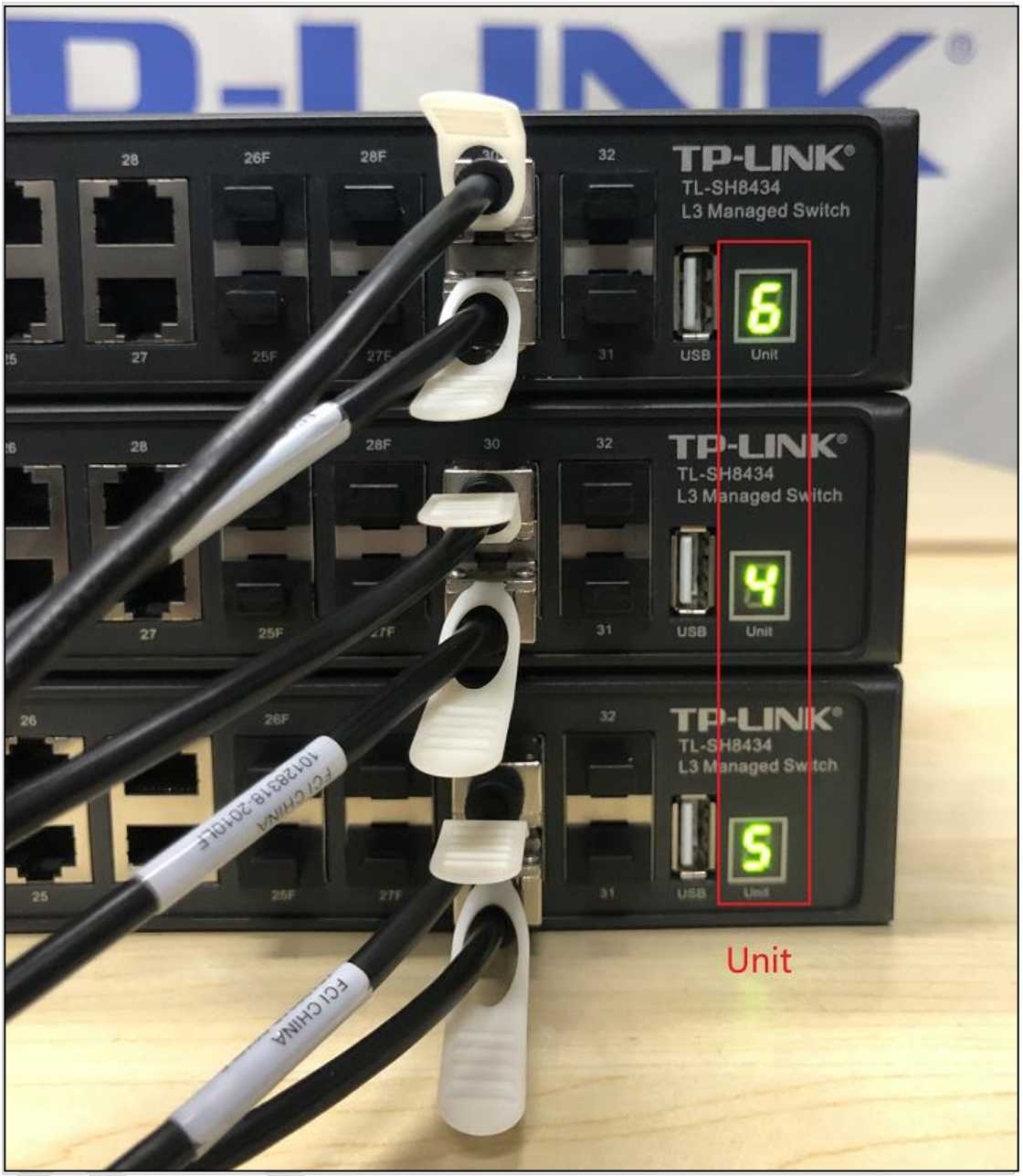
(2) 设置堆叠口：在“堆叠功能—堆叠管理—堆叠配置”页面中将堆叠口状态设置为启用（必选操作）；

(3) 配置堆叠编号：在“堆叠功能—堆叠管理—堆叠成员配置”页面中分别设置三台交换机的堆叠编号为 4、5、6。(可选操作)

备注：每台设备独立配置，配置之后请记得保存配置。

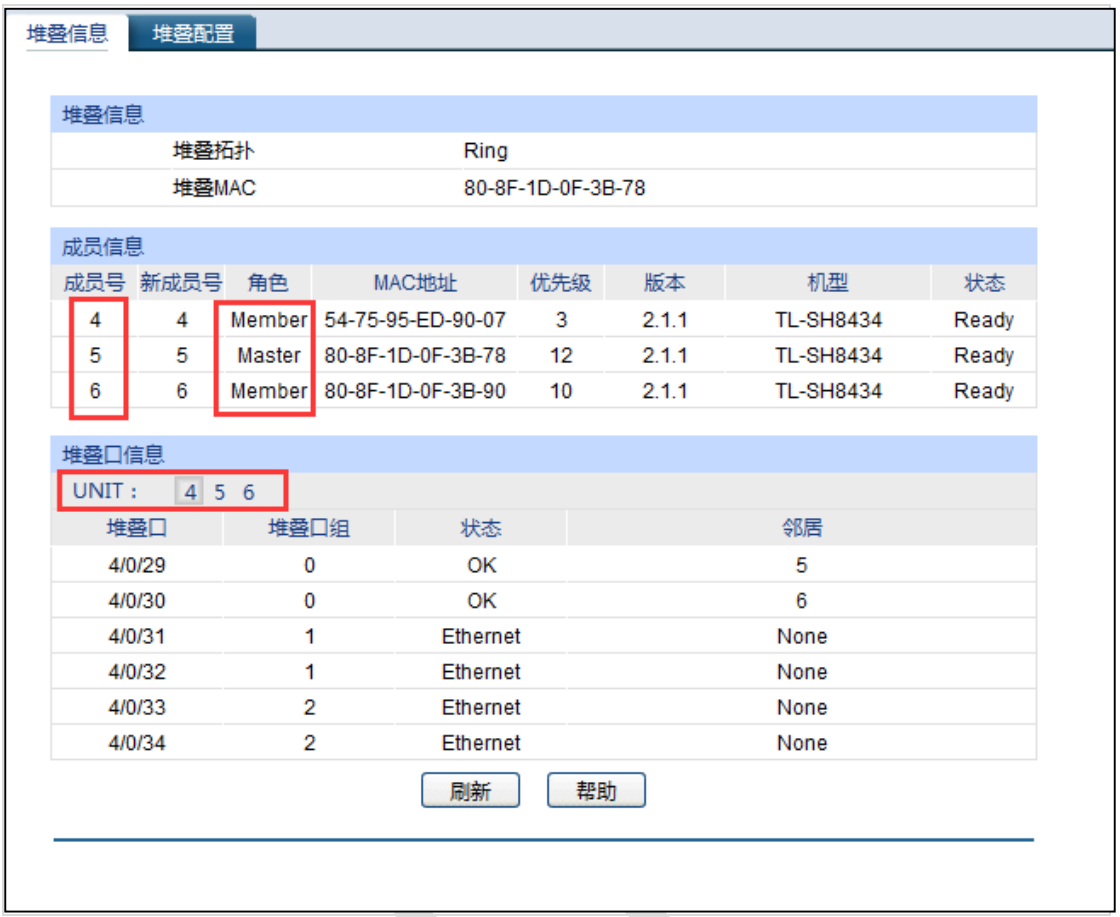
3、将三台交换机分别设置后保存配置后断电，然后按照链式或者环式的连接方式进行物理接线。

4、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。


TP-LINK
TL-SH8434
L3 Managed Switch
USB
Unit
6
4
5
Unit

堆叠系统形成后，用户可以通过任意成员设备的端口登陆堆叠系统。堆叠后的配置分为全局配置和端口配置，涉及到端口相关的配置会在相应的界面显示不同 Unit，通过选择不同 Unit 来配置不同交换机的端口。

堆叠信息展示：



4.1.4 配置注意事项

- 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。

第5章 VLAN

5.1 交换机 802.1Q VLAN 配置指南

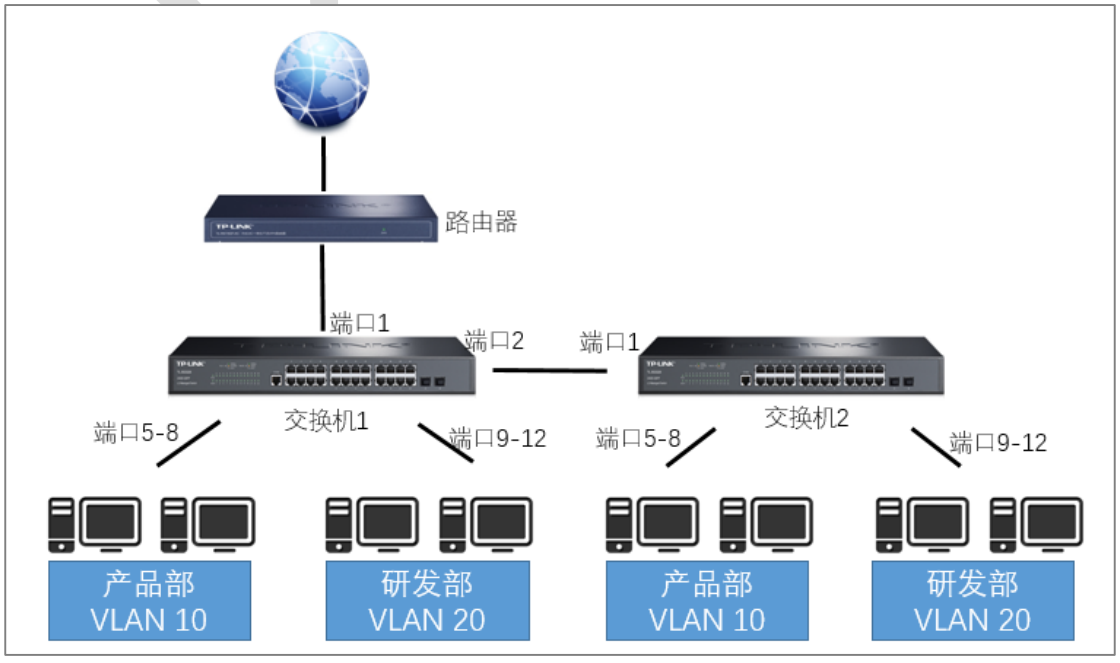
5.1.1 应用介绍

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。

5.1.2 需求介绍

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，本文以 TL-SG5428PE 为例介绍（5/6/7/8）系列交换机设置 IEEE 802.1Q VLAN 的方法。

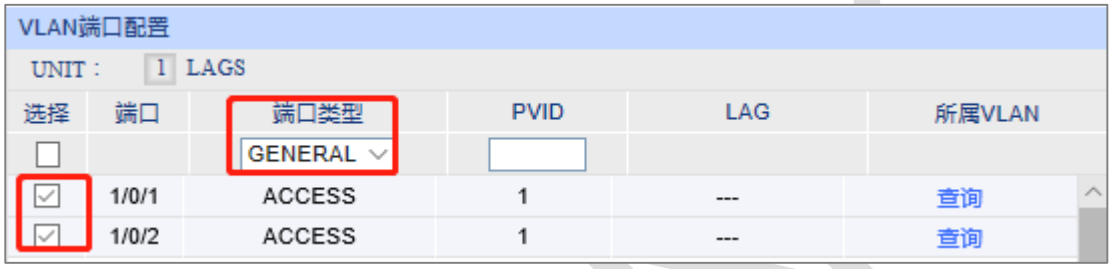
实例：同一个公司的同一个部门有多个不同的办公地点（比如在不同的楼层），各办公点有各自的交换机，级联形成同一个局域网，要求不同部门划分 VLAN。网络拓扑如下：

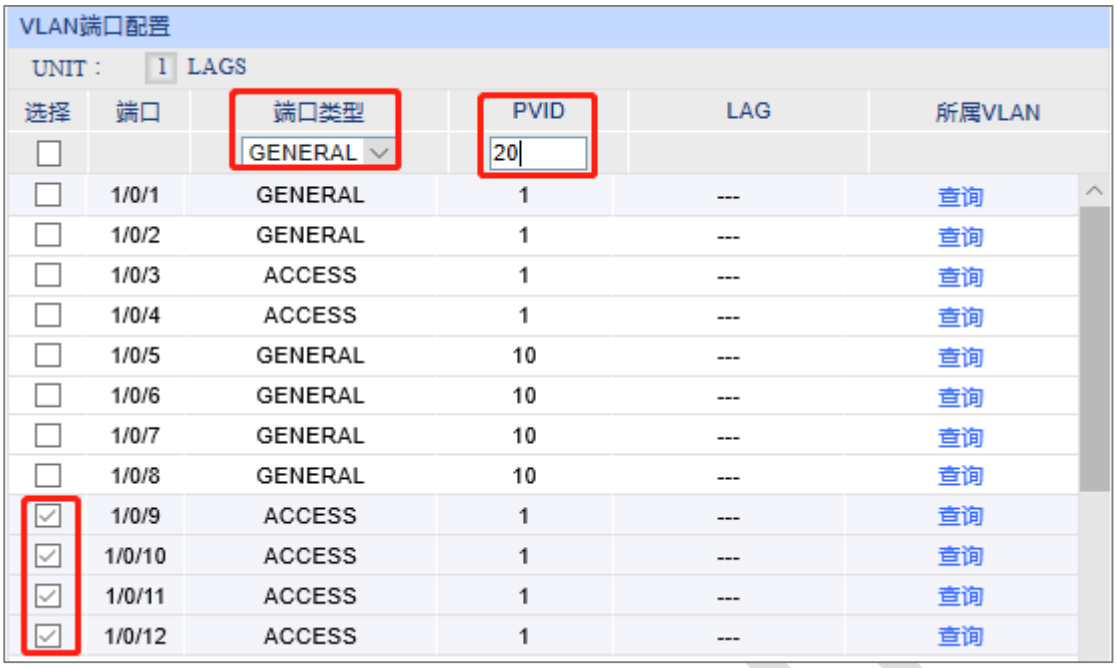


5.1.3 设置方法

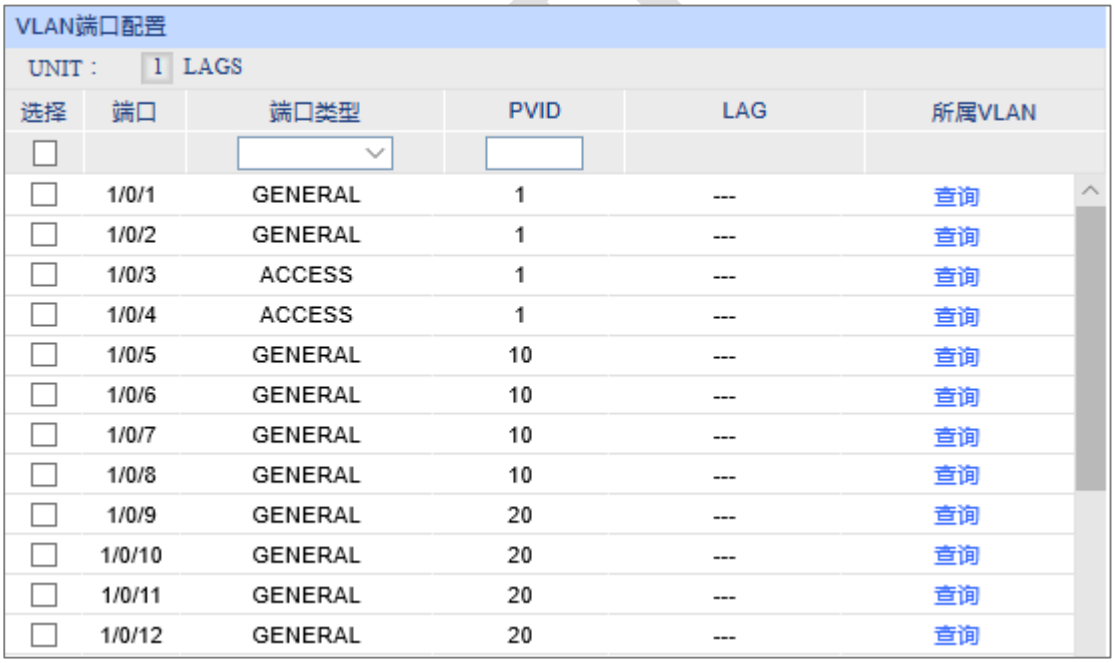
以交换机一为例，端口 1 接路由器，端口 2 接交换机二端口 1。

1、确定端口类型：将端口 1-2，5-12 设置为 GENERAL。在“VLAN->802.1Q VLAN->端口配置”中，勾选对应端口进行设置，注意 5-8 需将 PVID 设置为 10，9-12 需将 PVID 设置为 20。



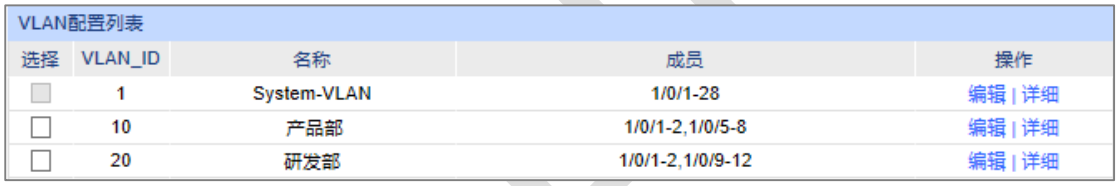


设置完后的端口配置列表：



2、 VLAN 的划分：在“VLAN->802.1Q VLAN->VLAN 配置”中，分别创建 VLAN10、VLAN20 将产品部划分为 VLAN 10，选择对应的端口，注意需将级联口包含进去，如下图端口 2 为 Tagged，端口 1 和端口 5-8 为 Untagged。VLAN20 重复上述步骤即可。

添加完成后，VLAN 列表如下：



交换机二设置是一样的，只是级联口此时只有一个端口 1，与交换机一的端口 2 配置相同。

至此已完成交换机中 802.1Q VLAN 的设置，注意保存配置以免掉电导致配置丢失。

5.2 MAC VLAN 配置指南

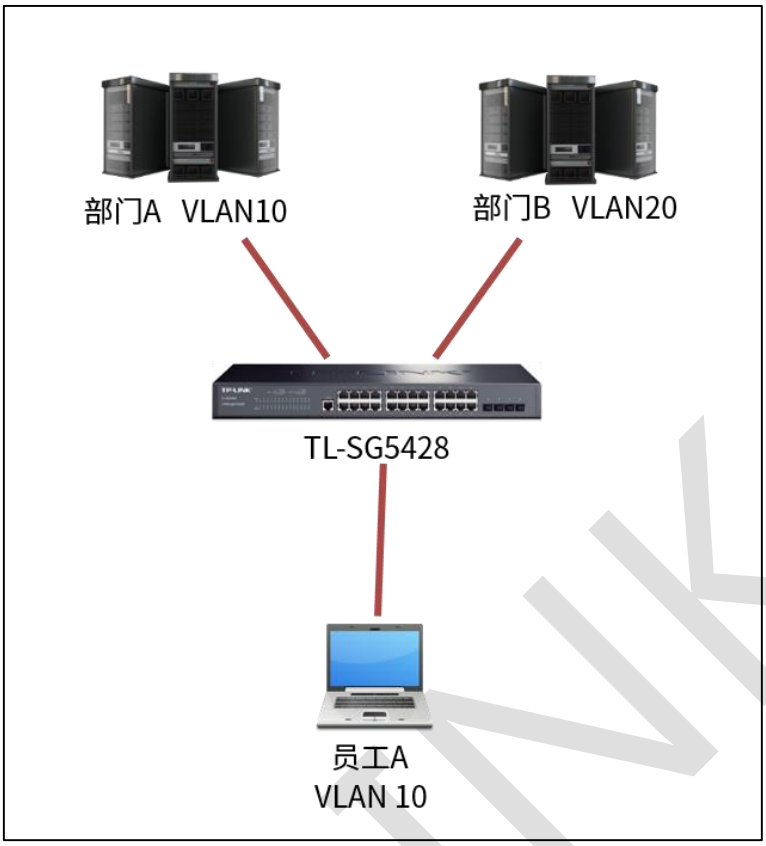
5.2.1 应用介绍

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 VL AN 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 VL AN 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。

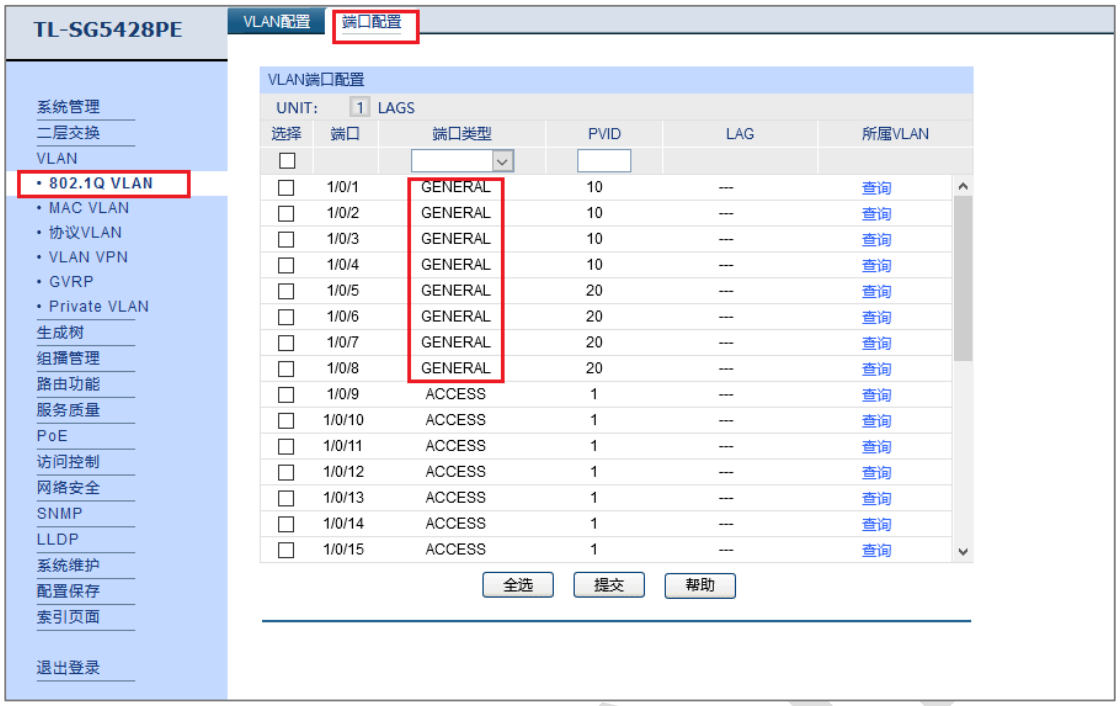
5.2.2 需求介绍

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：



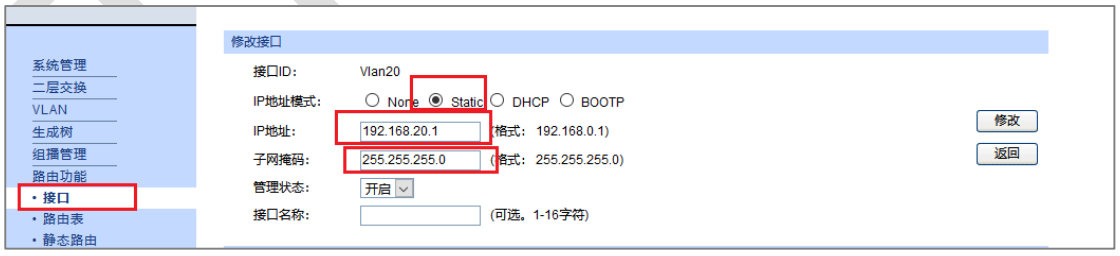
5.2.3 设置方法

1、在“VLAN 管理”—“802.1QVLAN”—“端口配置”，将需求端口均设置为“GENERAL”，点击提交，这里我们示例设置 1-8 口，并修改 1-4 的 PVID 为 10，5-8 的 PVID 为 20，如下图所示：



2、在“VLAN 管理”—“802.1QVLAN”—“VLAN 配置”，设置部门所在的 VLAN，将 1-8 口均设置在 vlan10 和 vlan20 里面，出口规则皆为 untag 如下图所示：

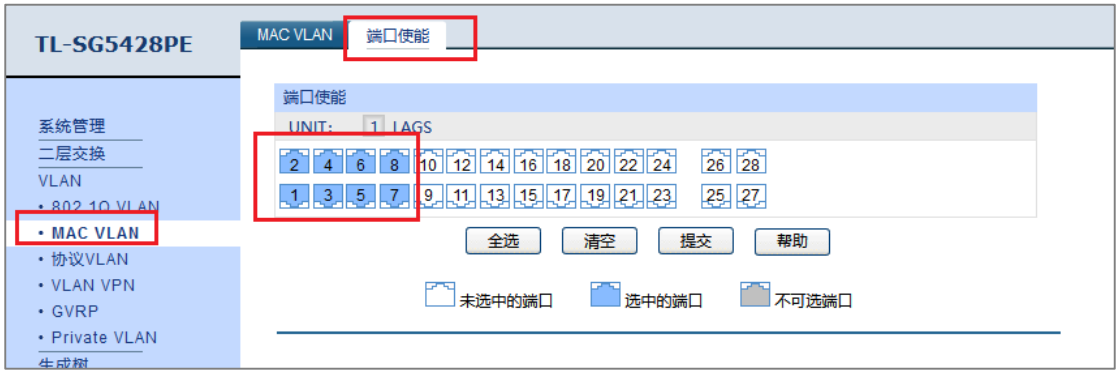
3、在“路由设置”—“接口”配置里面给不同的 VLAN 绑定 IP，如下图所示：



4、在“路由设置”—“DHCP 服务器”里面开启 DHCP 功能，启用即可，并添加地址池，注意网关和 DNS 也添加，如下图所示：

5、在“VLAN”—“MAC VLAN”里面，设置 MAC VLAN，如下图所示：

6、设置端口使能，我们这里设置了 1-8 口，所以开启 1-8 口的端口使能，如下图所示：



以上，MAC VLAN 配置完成！该终端接入任意的 1-8 口都属于 VLAN10。

5.2.4 配置注意事项

- 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 语音 VLAN 典型配置指导

5.3.1 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源 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。

5.3.2 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：

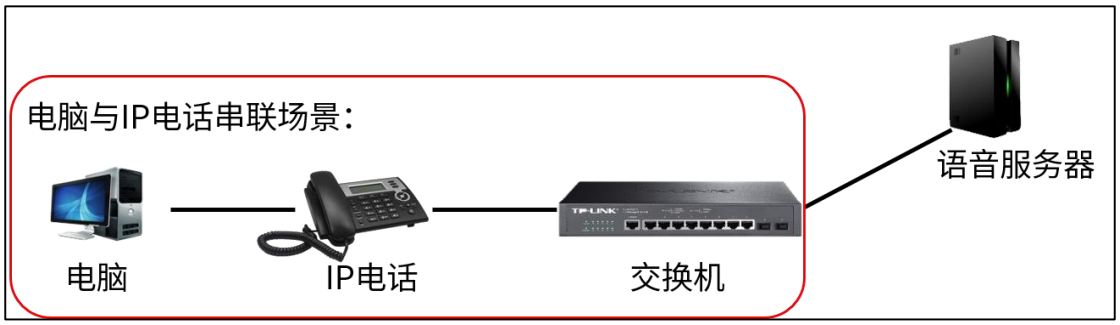
需求 1：

(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 0011-2233-0000、掩码是 ffff-ffff-0000 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。

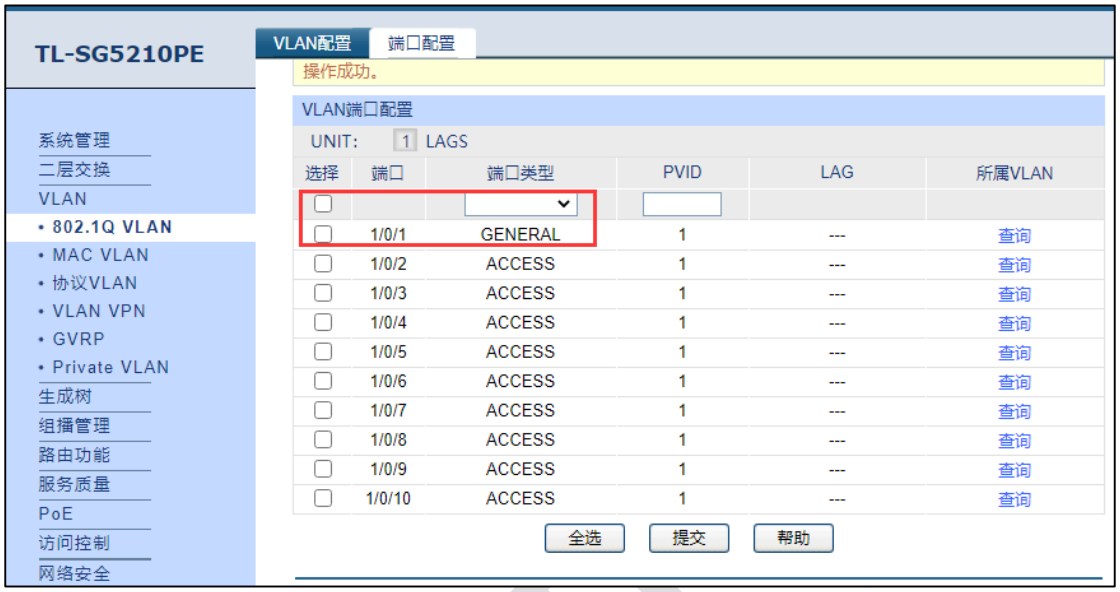
(4) 端口 1 允许 OUI 地址是 0011-2233-0000、掩码是 ffff-ffff-0000 的语音报文通过，描述字符为 test。

5.3.3 设置方法

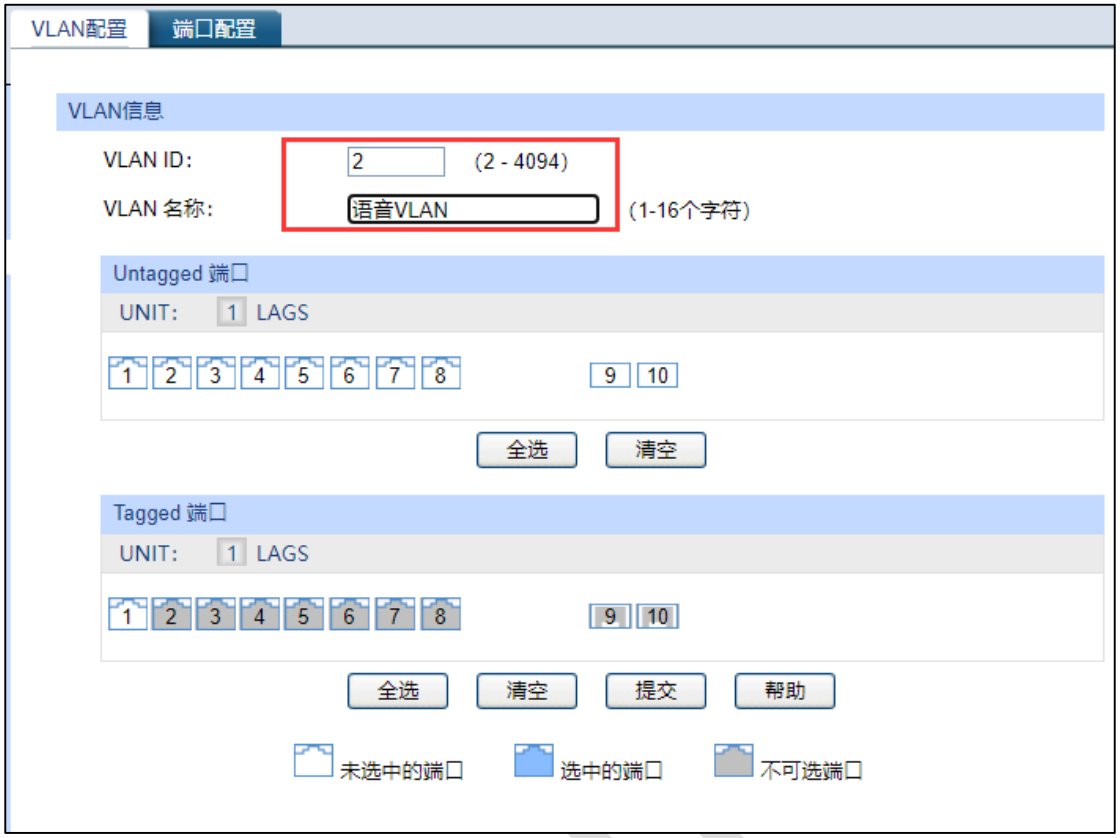
针对需求 1—使用自动模式

第一步、配置接语音电话的口为 general 口，并创建 VLAN 2

1、“VLAN”-“802.1Q　VLAN”-“端口配置”，设置接语音电话的口为 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）：

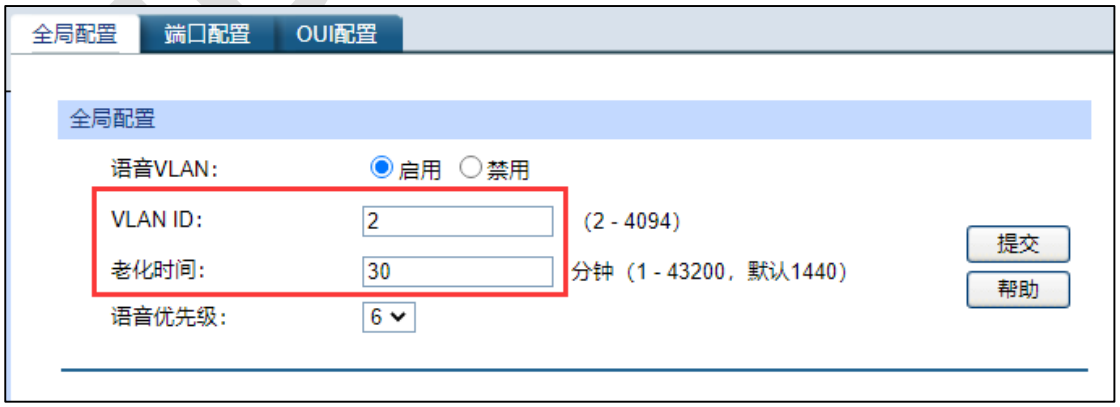


2、新建 VLAN 2 为语音 VLAN，可以不包含端口（自动模式下交换机根据端口是否收到语音数据自动维护端口加入或退出语音 VLAN）：



第二步、配置全局语音 VLAN 功能。

在“服务质量”-“语音 VLAN”，全局配置中启用全局语音 VLAN 功能，配置语音 VLAN 为 VLAN 2，老化时间为 30min：



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。

第三步、配置端口 1 的语音 VLAN 功能。

配置端口 1 的语音 VLAN 功能，设置端口 1 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。

第四步、配置语音 VLAN 能识别的 OUI 地址。

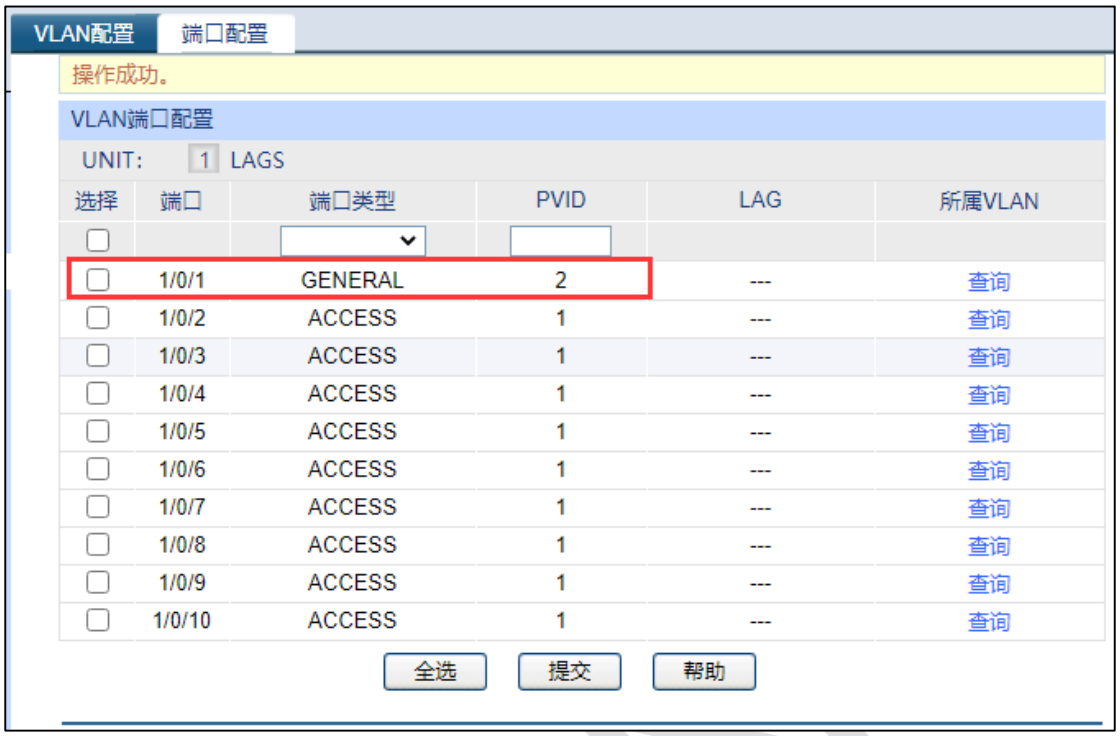
系统已经预设了一些常见厂商的 OUI 地址，如果没有自己厂商的则可以通过掩码与运算将设备的地址添加进去。

至此，自动模式下的语音 VLAN 配置成功，1 口下符合 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。

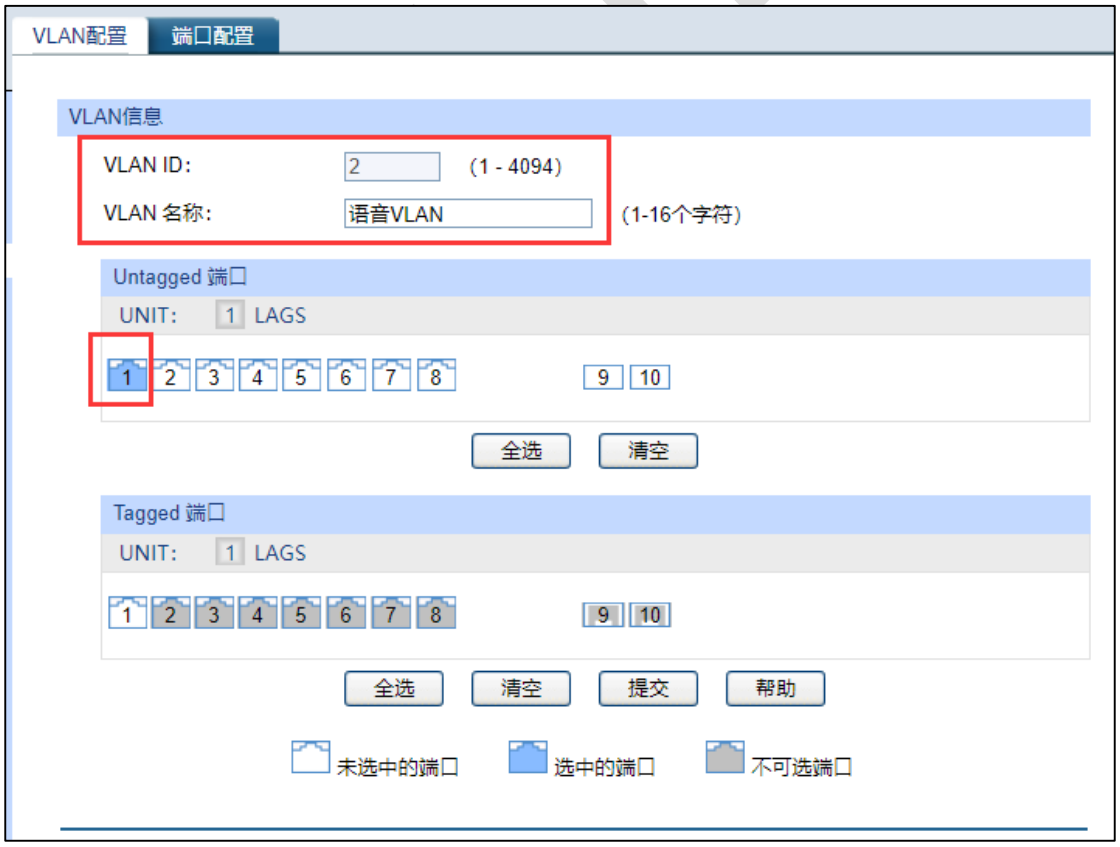
针对需求 2—使用手动模式

第一步、配置接语音电话的口为 general 口，并创建 VLAN 2

1、“VLAN”-“802.1Q　VLAN”-“端口配置”，设置接语音电话的口为 general 口，PVID 设置为 2：

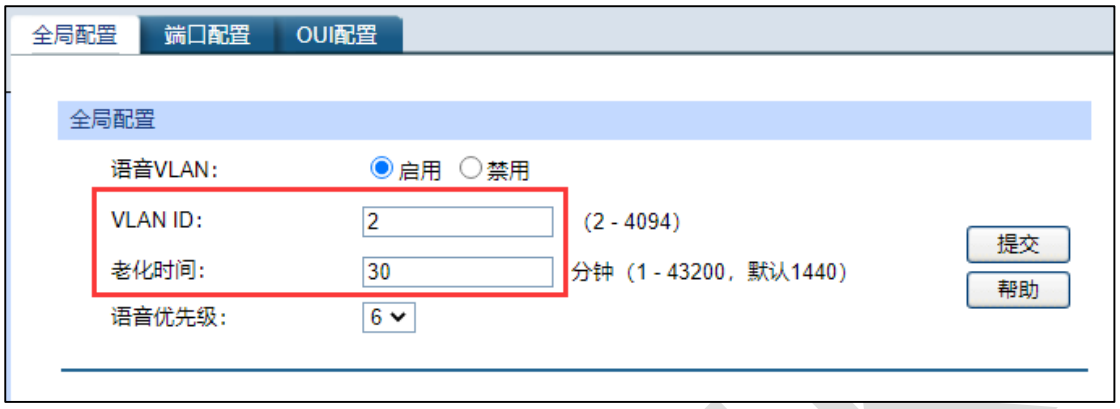


2、新建 VLAN 2 为语音 VLAN，包含端口 1，出口规则为 untag：



第二步、配置全局语音 VLAN 功能。

在“服务质量”-“语音 VLAN”，全局配置中启用全局语音 VLAN 功能，配置语音 VLAN 为 VLAN 2，老化时间为可以保持默认：

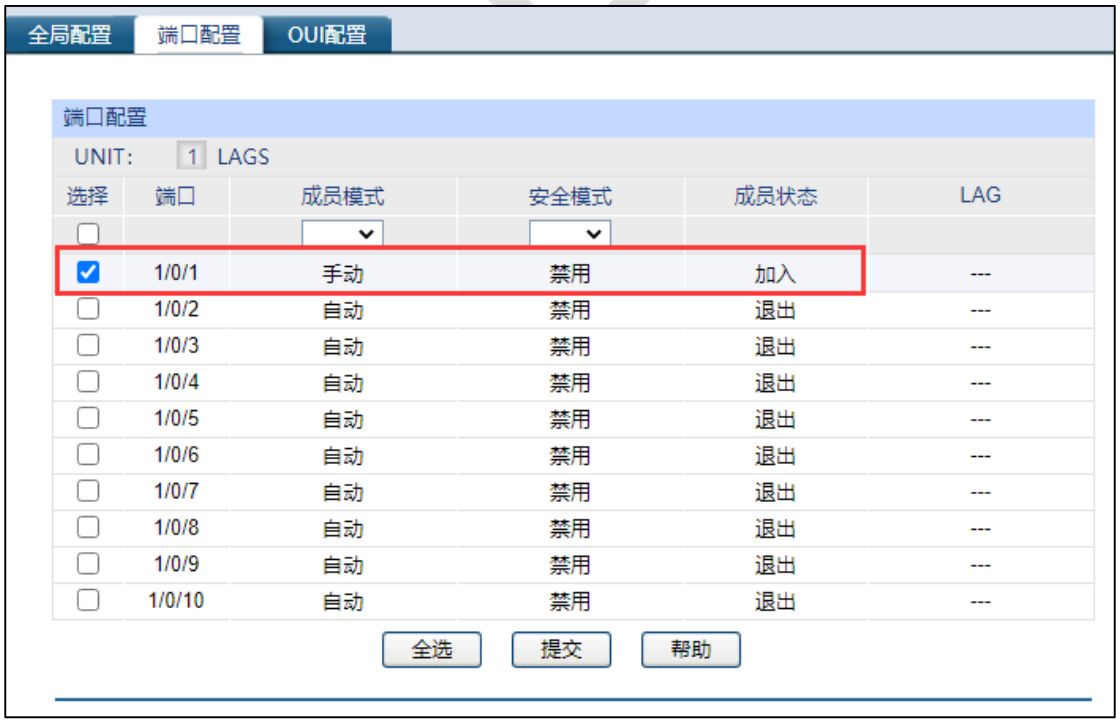


说明：

- 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。

第三步、配置端口 1 语音 VLAN 功能。

配置端口 1 的语音 VLAN 功能，设置端口 1 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。

第四步、配置语音 VLAN 的 OUI 地址。

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以通过掩码与运算将设备地址添加进去。

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。

5.3.4 配置注意事项

- 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。

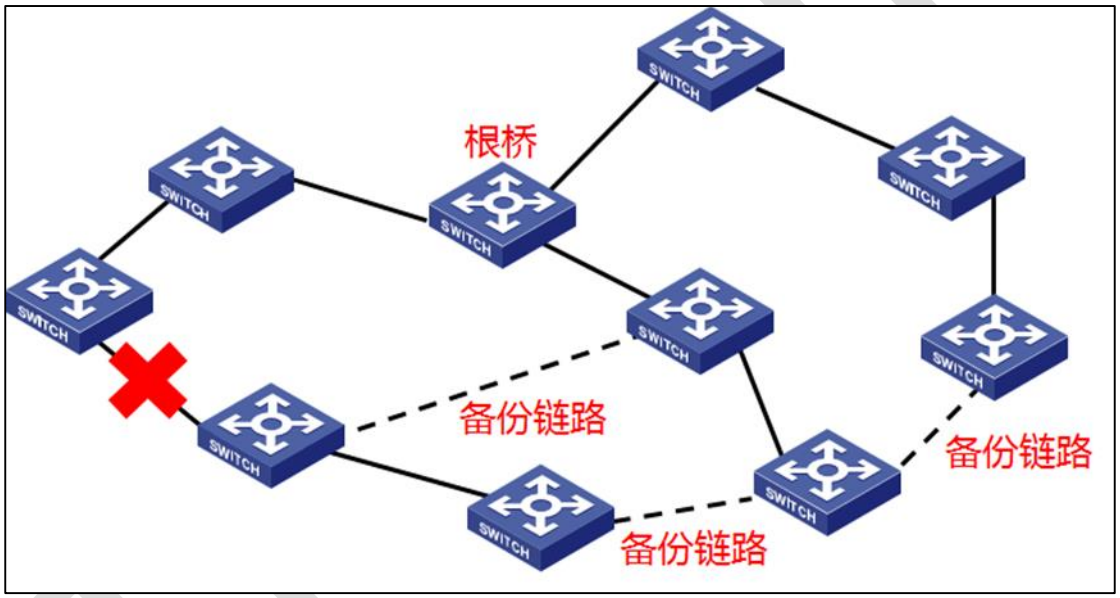
- 语音 VLAN 中的端口可工作在语音 VLAN 的自动模式或手动模式，在不同的工作模式下端口加入语音 VLAN 的方式不同。
- 自动模式：当用户 IP 电话启动时，所发出的报文经支持语音 VLAN 的设备时，设备通过识别该报文的源 MAC 地址，匹配设备上所配置的 OUI 地址，OUI 地址匹配成功后，设备自动将该语音报文的输入端口添加到语音 VLAN，并下发策略，将语音报文的优先级修改为设备上所配置的语音 VLAN 中语音流的优先级，并使用老化机制对语音 VLAN 内的端口进行维护。在老化时间内，系统没有从输入端口收到任何语音报文时，系统将把该端口从语音 VLAN 中删除。
- 手动模式：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。

第6章 生成树

6.1 交换机生成树功能配置指南

6.1.1 应用介绍

生成树 STP（ Spanning Tree Protocal）主要用于在局域网中消除链路层物理环路，并在链路故障时自动激活备份链路恢复网络。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的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。



(1) 通过阻断冗余链路消除网络中存在的路径回环；

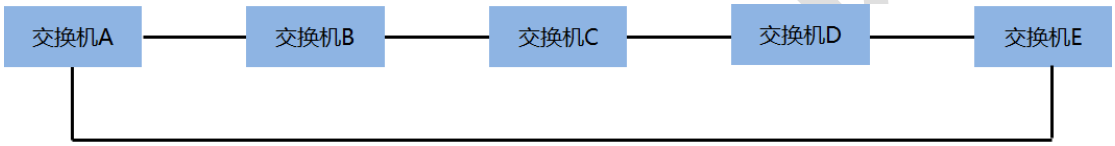
(2) 当前路径发生故障时，激活冗余备份链路，恢复网络连通性。

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。下面介绍 TP-LINK 交换机生成树功能的设置方法。

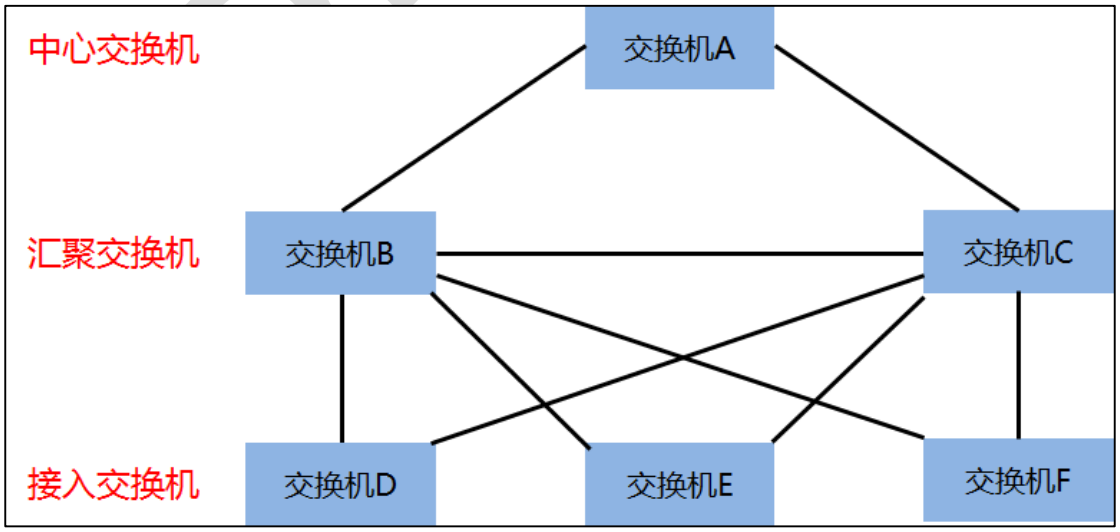
STP 和 RSTP 功能的设置方法是相同的。RSTP 相比于 STP 来说收敛速度更快，且兼容 STP 协议，所以一般推荐使用 RSTP 协议。

6.1.2 需求介绍

1、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。如下图所示：



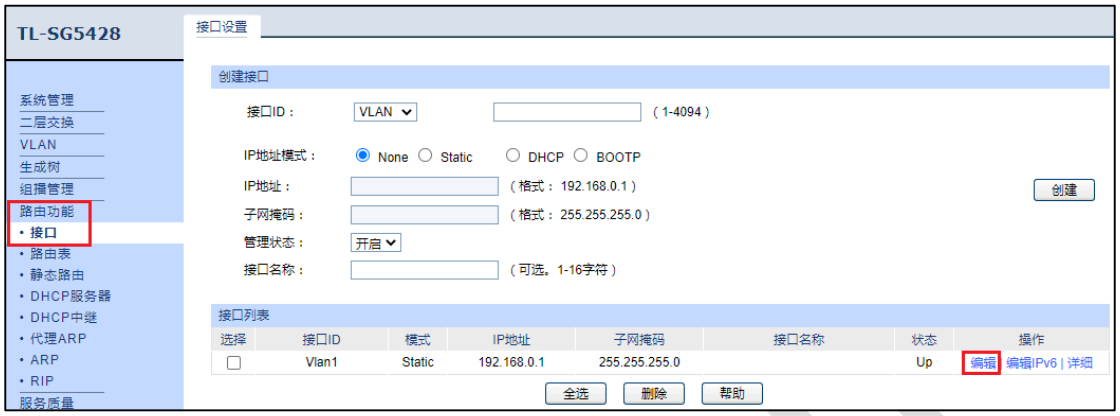
2、客户公司内部网络，如下图所示拓扑结构，整个网络中设置了 6 个 VLAN 101-106，需要实现 VLAN101、103 和 105 的数据流量以 B 为根桥，VLAN102、104 和 106 的数据流量以 C 为根桥。采用 MSTP 阻断网络中的环路，并能达到数据转发过程中 VLAN 数据的冗余备份以及负载分担效果。



6.1.3 设置方法

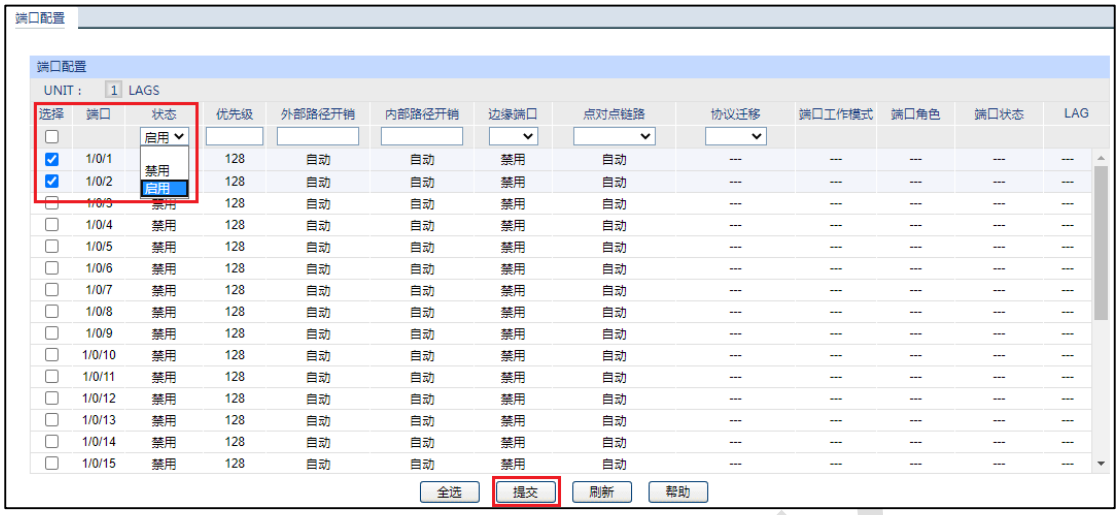
STP/RSTP 设置方法

1、修改交换机的 IP 地址不冲突：TP-LINK 的交换机默认管理 IP 地址均是 192.168.0.1，为了防止地址冲突，首先建议修改为不冲突的 IP 地址。以 TL-SG5428 为例，打开“路由功能”—“接口”页面，点击“编辑”修改。



2、交换机开启 STP 或者 RSTP 全局配置开关：打开菜单“生成树”—“基本配置”页面，生成树功能选择“启用”，生成树模式选择“STP 或者 RSTP”，点击“提交”。

3、交换机级联端口启用生成树功能：打开菜单“生成树”—“端口配置”页面，选择交换机级联的端口（本例中是端口 1 和 2），状态选择“启用”，点击“提交”。



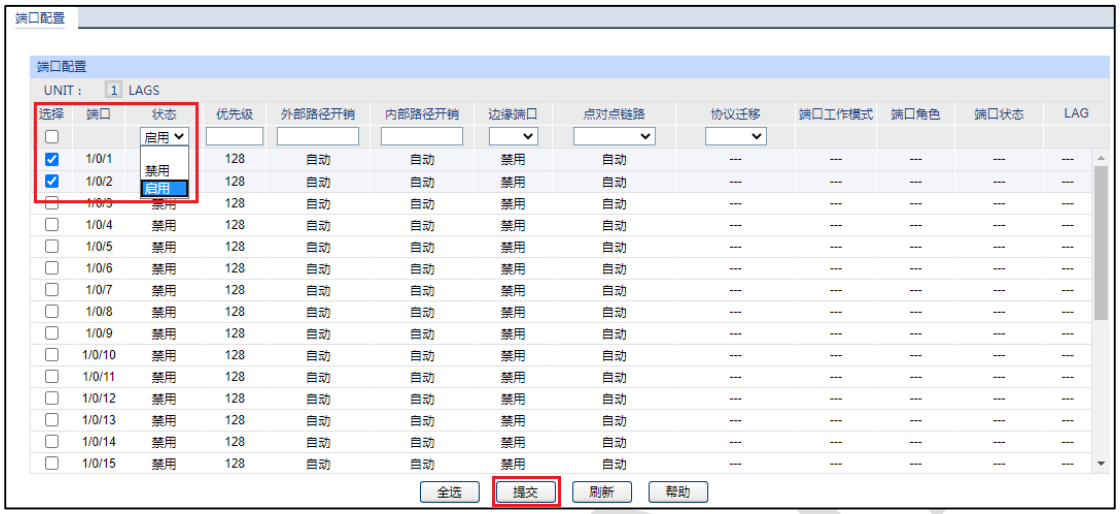
一台交换机设置完成，相同的方法，依次设置其他的交换机。完成 STP/RSTP 功能的设置之后，进行线路连接即可。

MSTP 设置方法

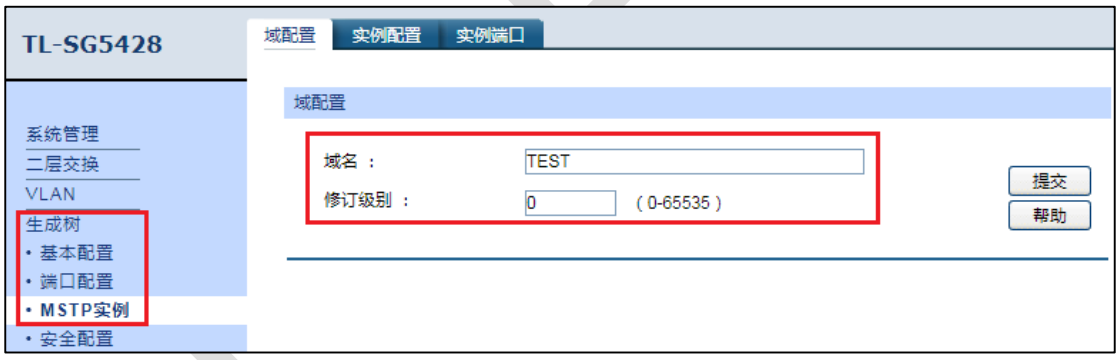
本例中假定 IP、VLAN 等相关的设置已经完成，仅关注生成树的设置。

1、所有交换机开启 MSTP 全局配置开关：打开菜单“生成树”—“基本配置”页面，生成树功能选择“启用”，生成树模式选择“MSTP”，点击“提交”。

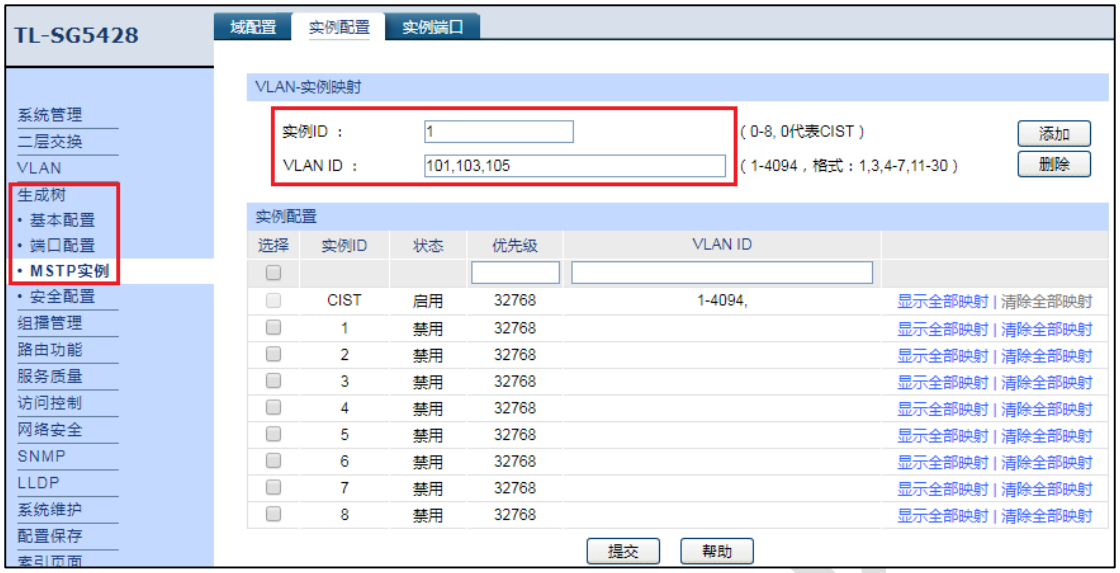
2、所有交换机级联端口启用生成树功能：打开菜单“生成树”—“端口配置”页面，选择交换机之间级联的端口编号。状态选择“启用”，点击“提交”。



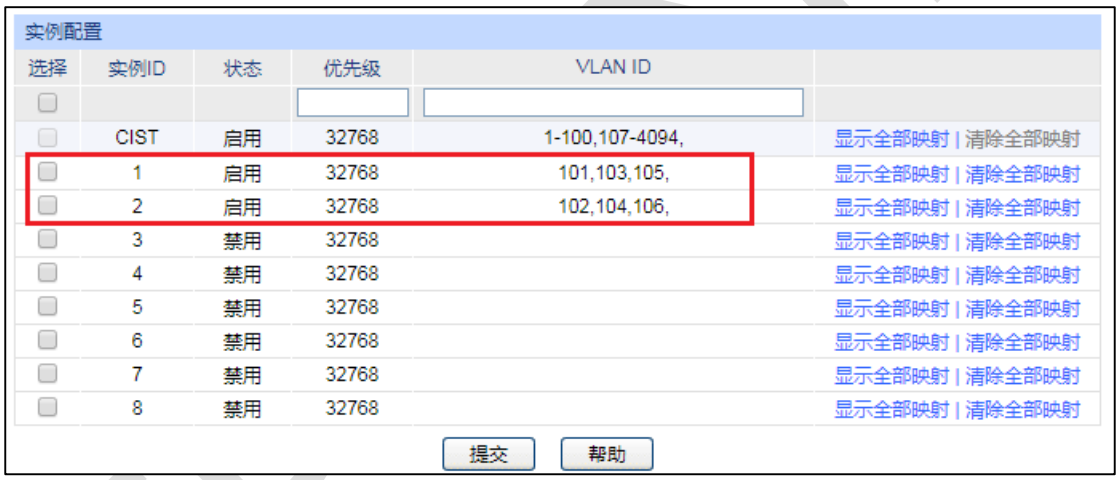
3、所有交换机配置相同的 MST 域的域名（任意域名）和修订级别（默认即可）：打开菜单“生成树”—“MSTP 实例”—“域配置”页面，所有交换机设置相同的域名（本例中为“TEST”）和修订级别（本例中为默认的“0”），点击“提交”。



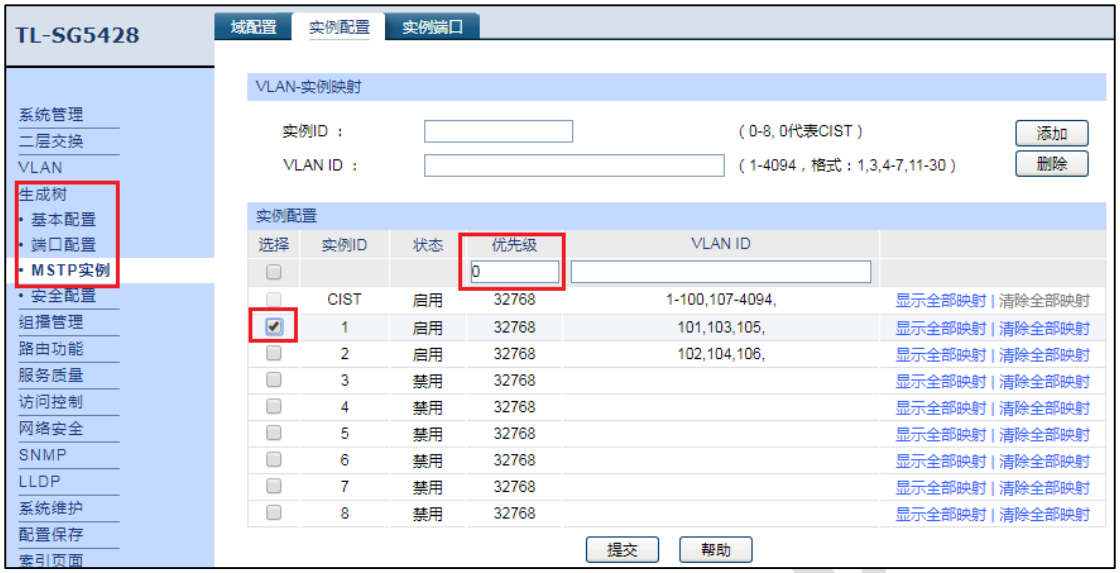
4、所有交换机配置 MST 域的 VLAN-实例映射，将 VLAN 101、103、105 映射到实例 1，将 VLAN 102、104、106 映射到实例 2：打开菜单“生成树”—“MSTP 实例”—“实例配置”页面，实例 ID 设置“1”，VLAN ID 设置“101,103,105”，点击 “添加”，将 VLAN 101、103、105 映射到实例 1。相同设置方法将 VLAN 102、104、106 映射到实例 2。所有交换机相同的设置。



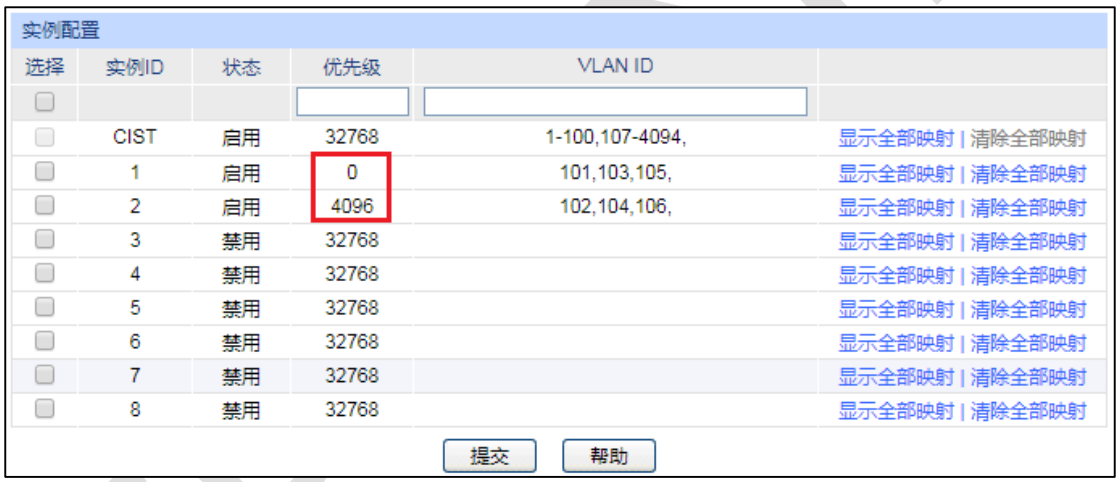
5、添加完毕如下图所示。



6、将交换机 B 配置为实例 1 的根桥，且是实例 2 的指定桥：打开交换机 B 的配置页面，打开菜单“生成树”—“MSTP 实例”—“实例配置”页面，选择实例“1”，并将优先级设置为“0”，点击“提交”。



7、然后选择实例“2”，并将优先级设置为“4096”，点击“提交”。设置完毕如下图所示。



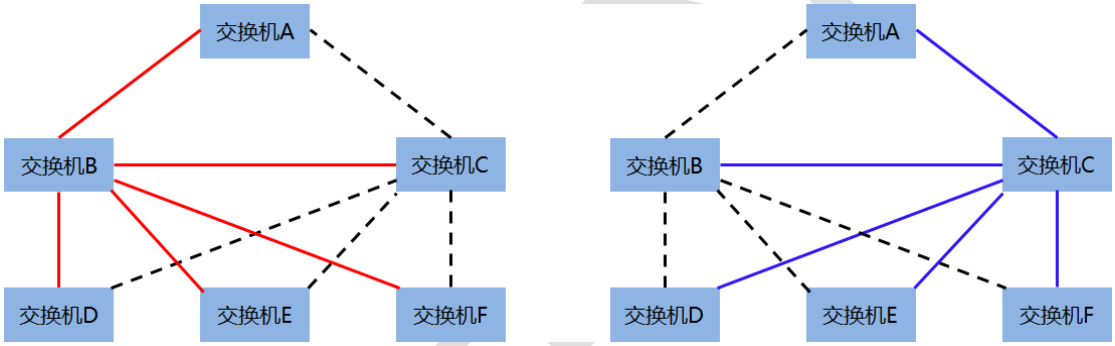
8、将交换机 C 配置为实例 2 的根桥，且是实例 1 的指定桥：打开交换机 C 的配置页面，打开菜单“生成树”—“MSTP 实例”—“实例配置”页面，选择实例“1”，并将优先级设置为“4096”，点击“提交”。然后选择实例“2”，并将优先级设置为“0”，点击“提交”。设置完毕如下图所示。

实例配置

选择	实例ID	状态	优先级	VLAN ID	
	CIST	启用	32768	1-100,107-4094,	显示全部映射 | 清除全部映射
	1	启用	4096	101,103,105,	显示全部映射 | 清除全部映射
	2	启用	0	102,104,106,	显示全部映射 | 清除全部映射
	3	禁用	32768		显示全部映射 | 清除全部映射
	4	禁用	32768		显示全部映射 | 清除全部映射
	5	禁用	32768		显示全部映射 | 清除全部映射
	6	禁用	32768		显示全部映射 | 清除全部映射
	7	禁用	32768		显示全部映射 | 清除全部映射
	8	禁用	32768		显示全部映射 | 清除全部映射

提交 帮助

9、MSTP 的所有设置完成，实现的效果：实例 1（VLAN101、103、105），连通的链路如左边红色所示，实例 2（VLAN102、104、106），连通的链路如右边蓝色所示。



至此，生成树功能的基本设置方法就介绍完了。

6.1.4 配置注意事项

- 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。部和分部路由器都处于联网状态，且至少有一端出口是公网 IP 地址

第7章 组播管理

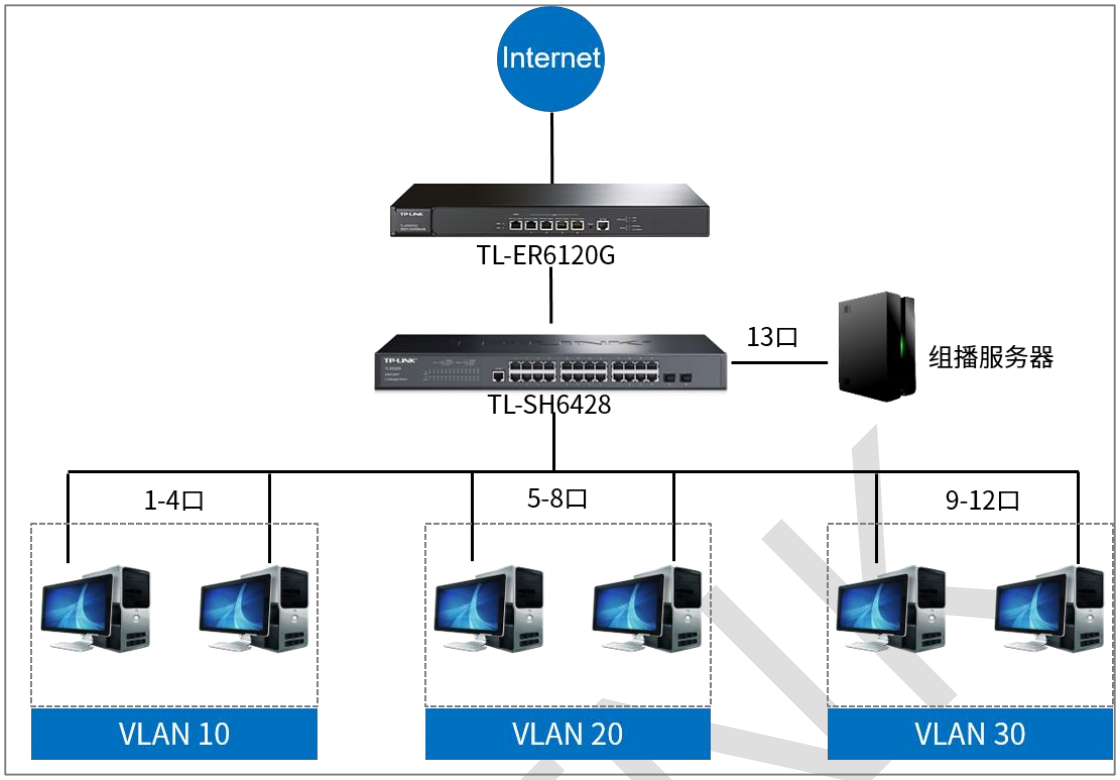
7.1 交换机多网段 IGMP 侦听配置指南

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。

7.1.2 需求介绍

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：

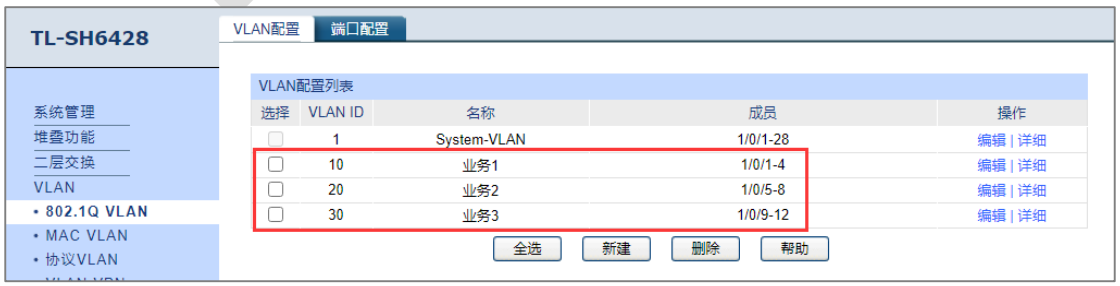


7.1.3 设置方法

第一步、划分业务 VLAN 10.20.30，组播数据使用的 VLAN 40。

划分 VLAN 时需要将需要组播业务的端口设置为 general 口，便于之后的 VLAN 设置，同时保证该端口既可以运行普通业务也可以转发组播数据。

在“VLAN-802.1Q VLAN-VLAN 配置”界面，划分对应端口到对应业务 VLAN 下，本拓扑下出口规则为 untag：

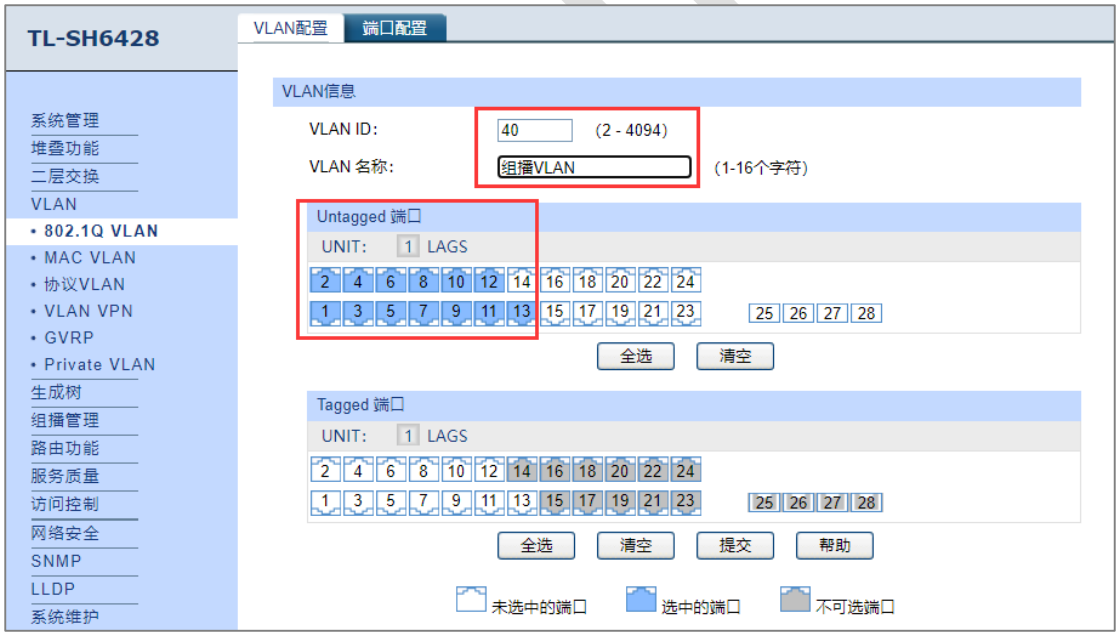


其余的接口，DHCP，以及静态路由配置可以参考：【配置实例】三层交换机企业应用配置实例。

第二步、新建组播服务器和需要用到组播数据端口所在的 VLAN 。

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。

在“VLAN-802.1Q VLAN-VLAN 配置”界面，将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 ：



第三步、设置端口的 PVID

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。 在“VLAN-802.1Q VLAN-端口配置界面”，配置 1-13 口为 general 口，并设置对应端口的的 PVID 为对应的 VLAN ID，如下：

第四步、开启 IGMP 侦听

在组播管理中，启用全局 IGMP 侦听，在 IGMP 全局配置中，选择丢弃未知组播报文，其余选项默认。

注：IGMP 侦听和 MLD 侦听需要同时启用。

第五步、设置 IGMP 侦听的端口和组播 VLAN

在“组播管理-IGMP 侦听-端口配置”中，需要用到组播功能的端口 1-12 口启用 IGMP 侦听，同时启用快速离开功能（在有多个组播组的环境下使用），之后点击提交。

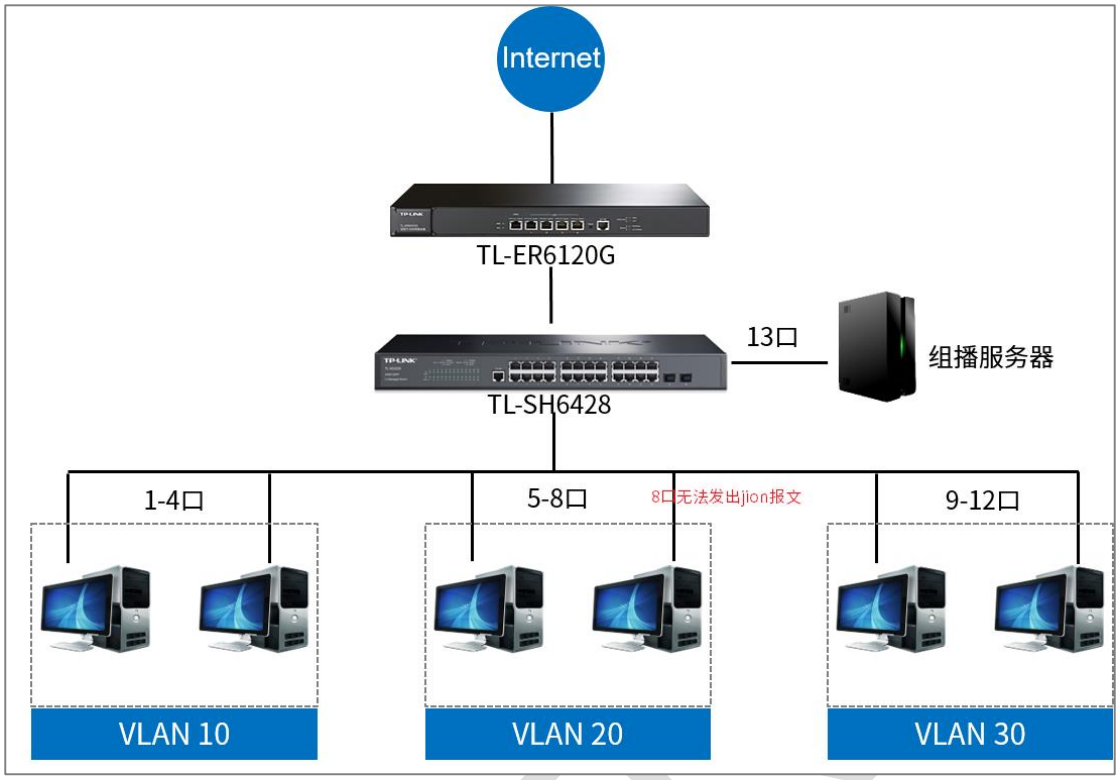
然后在“组播管理-IGMP 侦听-组播 VLAN”一栏中，启用组播 VLAN40，路由器端口时间和成员端口时间根据需要填写，一般选择推荐值。静态路由器端口也就是发送组播数据的端口，选中端口 13，之后点提交。

第六步、组播 VLAN 测试

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。

第七步、组播静态地址表的设置

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。



在“组播管理-组播地址表-IPv4 静态组播地址表”中，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，之后点击添加。

这时在组播地址表中便会生成一条静态的地址表，默认将组播地址为 224.1.1.1 的组播报文转发到 8 端口。

此时，不需要接收端发送组播通告报文，一样可以接收到组播数据。

以上即可完成组播 VLAN 和 IGMP 侦听的设置满足用户的使用需求，配置完成后记得保存配置。

第8章 路由功能

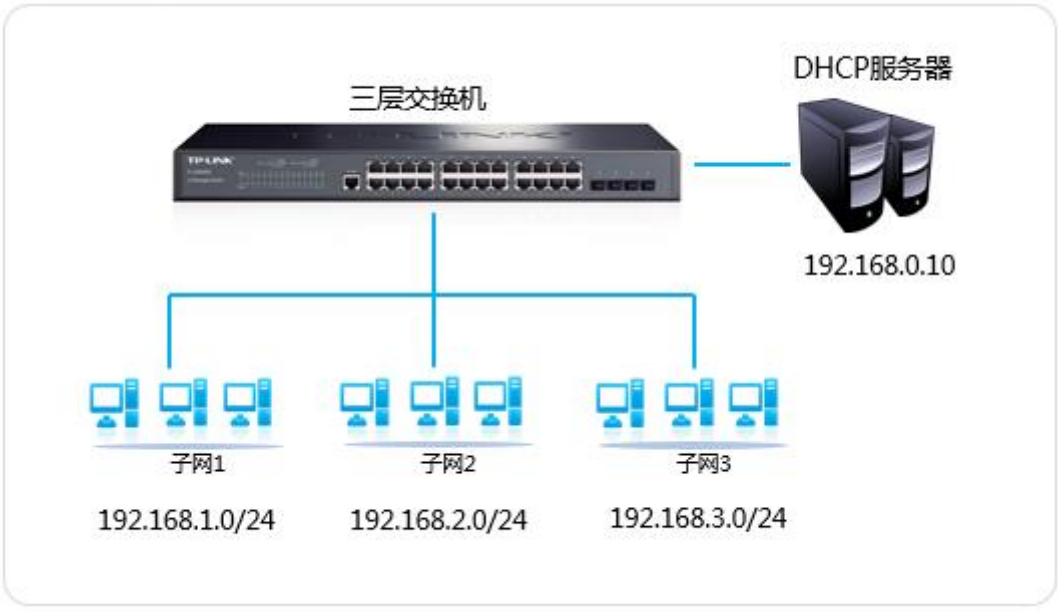
8.1 交换机 DHCP 中继配置指南

8.1.1 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。

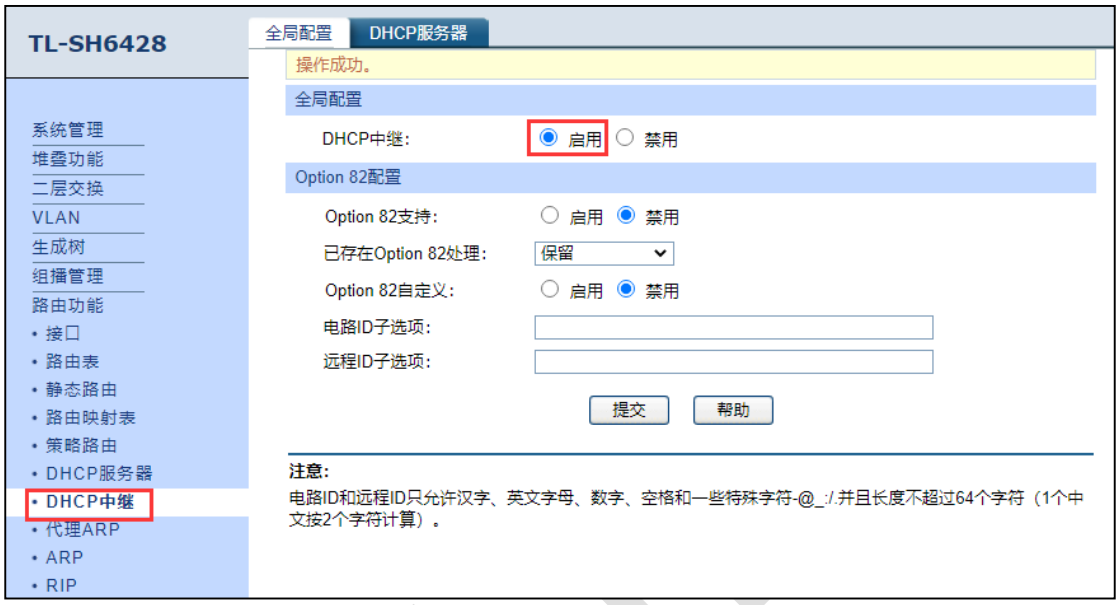
8.1.2 需求介绍

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。



8.1.3 设置方法

登录到三层交换机的管理界面，点击“路由功能-DHCP 中继-全局配置”，启用交换机的 DHCP 中继功能，如下图：



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。

点击“路由功能>DHCP 中继>DHCP 服务器”，添加 DHCP 服务器地址，如下图：

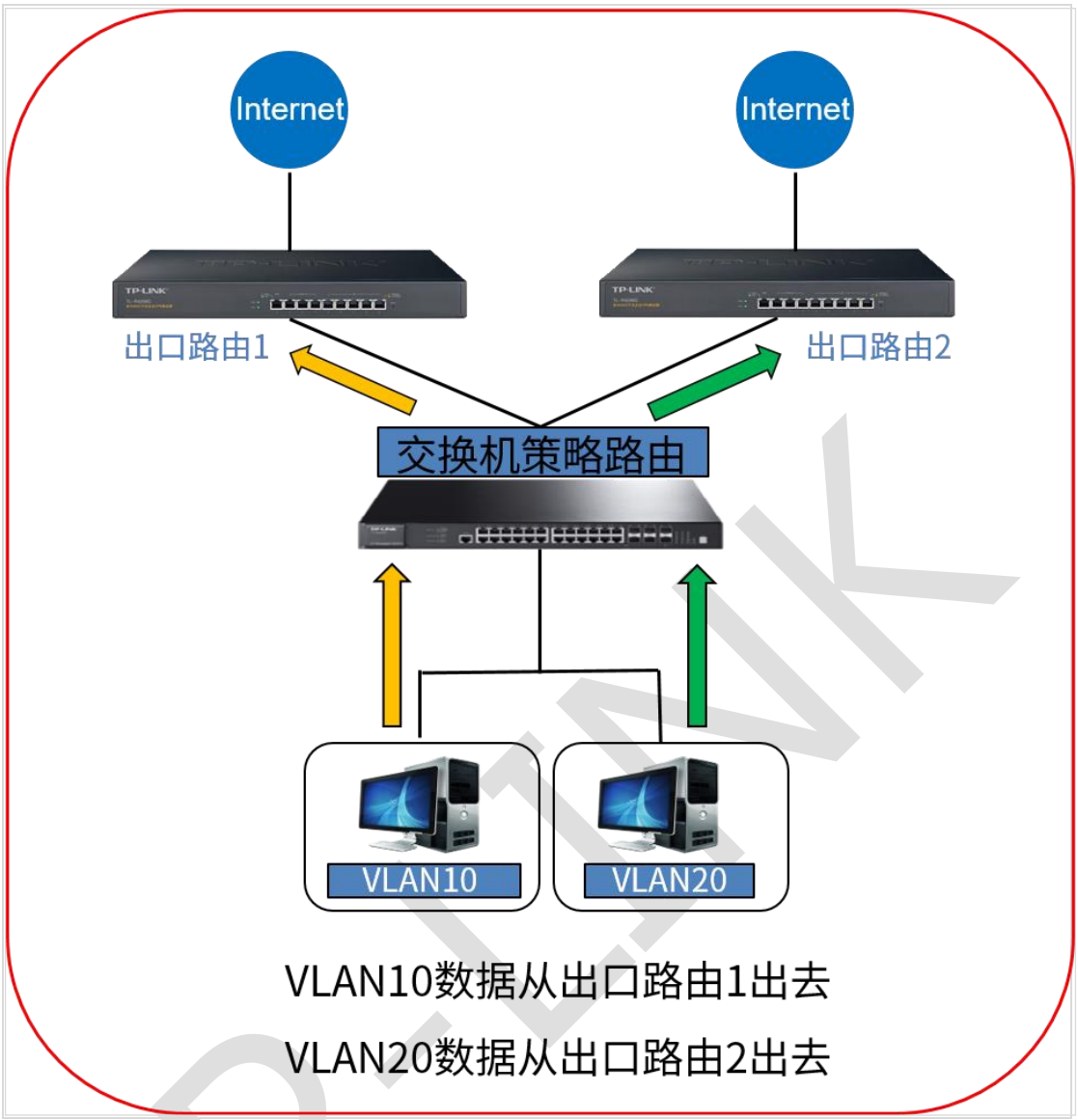
这样，就可以实现三层交换机的不同子网都通过专用的 DHCP 服务器分配 IP 地址。

8.2 三层网管交换机策略路由配置指导

8.2.1 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。



8.2.2 需求介绍

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。

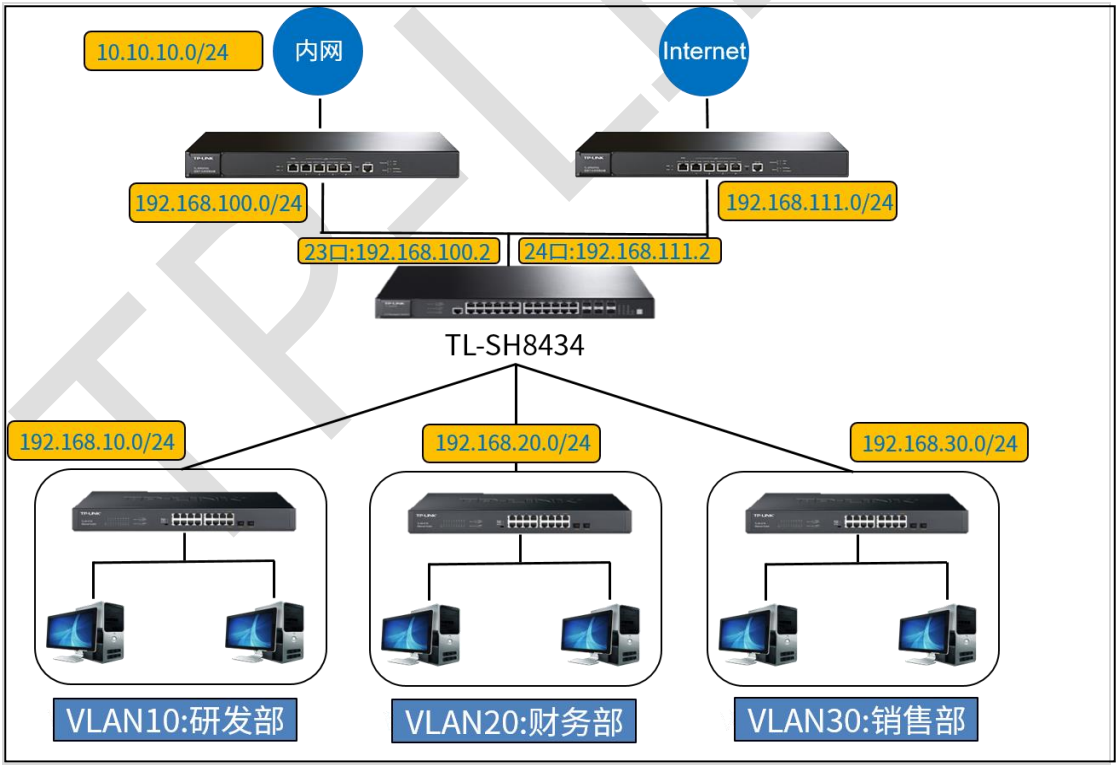
需求分析：

(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) 不同部门不能够互访可以通过设置 ACL 规则来实现；

(3) 针对这种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。

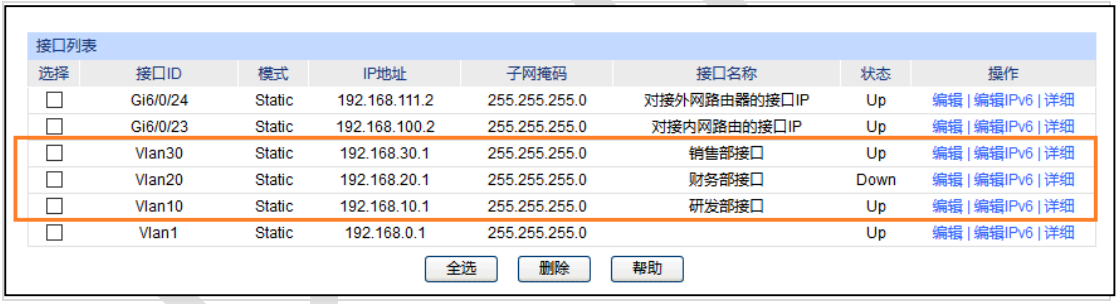
拓扑如下：



8.2.3 设置方法

第一步、研发部、财务部、销售部分别划分为不同网段

交换机按照常规给三个部门规划好 VLAN，接口地址，DHCP 地址池，这里就不再详细描述，具体配置结果如图：



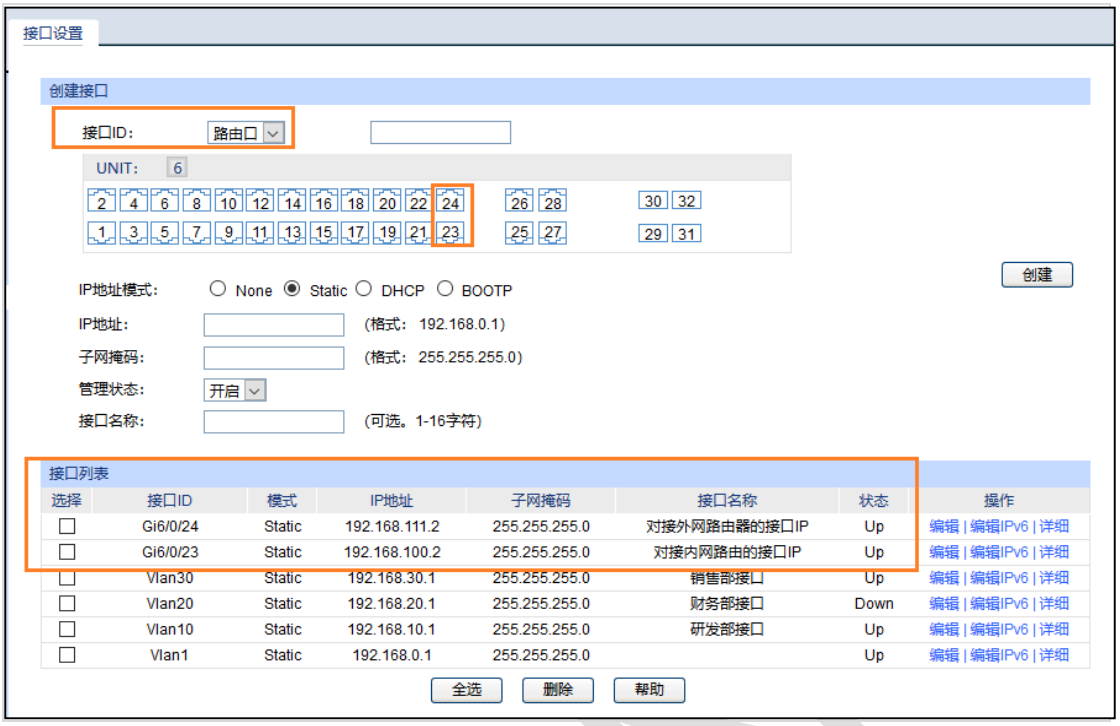
第二步、研发部门、财务部和销售部门之间不能互访

通过 ACL 实现双向禁止访问，配置 ACL 并绑定对应接口后如图：

第三步、设置策略路由控制不同部门的外网权限

1、配置路由接口

配置交换机的路由口地址，对接不同出口路由器，在交换机 Web 界面：“路由功能”—“接口”—“接口 ID”--“路由口”，配置 23 端口对接内网路由的接口 IP 和 24 端口对接外网路由器的接口 IP：



2、配置标准 IP ACL

配置标准 IP ACL 列表，指定数据流量，在交换机 Web 界面："访问控制"—"ACL 配置"—"新建 ACL"--"标准 IP ACL"，创建标准 IP ACL 条目（此条目的目的是指定策略路由的源目的 IP）：

本次举例研发部访问公司内网的数据流创建方法。

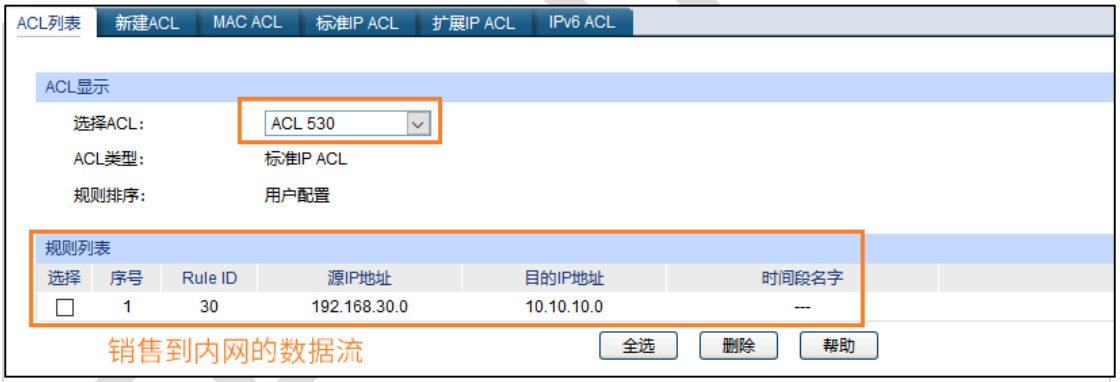
最终创建的几条数据流条目如图：


ACL列表
新建ACL
MAC ACL
标准IP ACL
扩展IP ACL
IPv6 ACL
ACL显示
选择ACL：
ACL 510
ACL类型：
标准IP ACL
规则排序：
用户配置
规则列表
选择
序号
Rule ID
源IP地址
目的IP地址
时间段名字
1
10
192.168.10.0
10.10.10.0

研发访问内网的数据流
全选
删除
帮助


ACL列表
新建ACL
MAC ACL
标准IP ACL
扩展IP ACL
IPv6 ACL
ACL显示
选择ACL：
ACL 520
ACL类型：
标准IP ACL
规则排序：
用户配置
规则列表
选择
序号
Rule ID
源IP地址
目的IP地址
时间段名字
1
20
192.168.20.0
10.10.10.0

财务访问内网的数据流
全选
删除
帮助


ACL列表
新建ACL
MAC ACL
标准IP ACL
扩展IP ACL
IPv6 ACL
ACL显示
选择ACL：
ACL 530
ACL类型：
标准IP ACL
规则排序：
用户配置
规则列表
选择
序号
Rule ID
源IP地址
目的IP地址
时间段名字
1
30
192.168.30.0
10.10.10.0

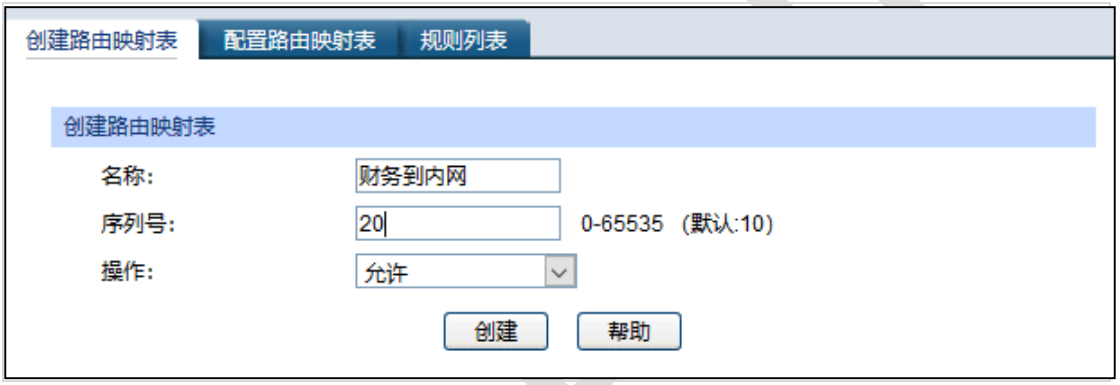
销售到内网的数据流
全选
删除
帮助

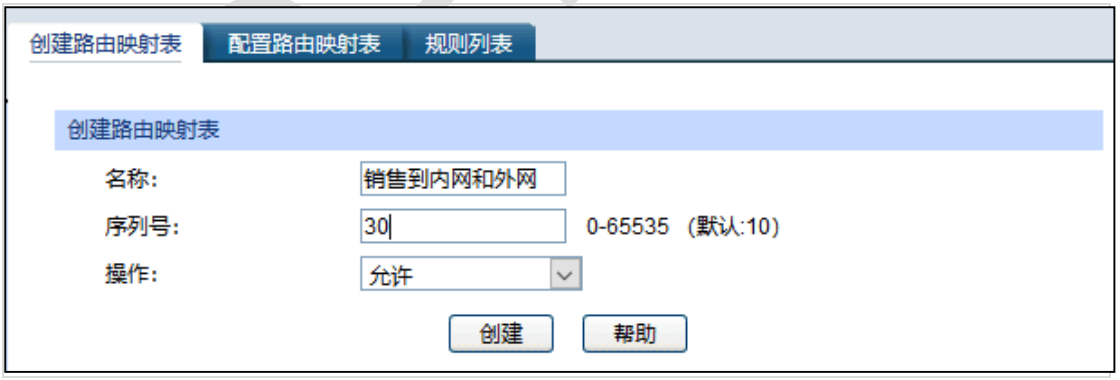

ACL列表
新建ACL
MAC ACL
标准IP ACL
扩展IP ACL
IPv6 ACL
ACL显示
选择ACL：
ACL 531
ACL类型：
标准IP ACL
规则排序：
用户配置
规则列表
选择
序号
Rule ID
源IP地址
目的IP地址
时间段名字
1
31
192.168.30.0
0.0.0.0

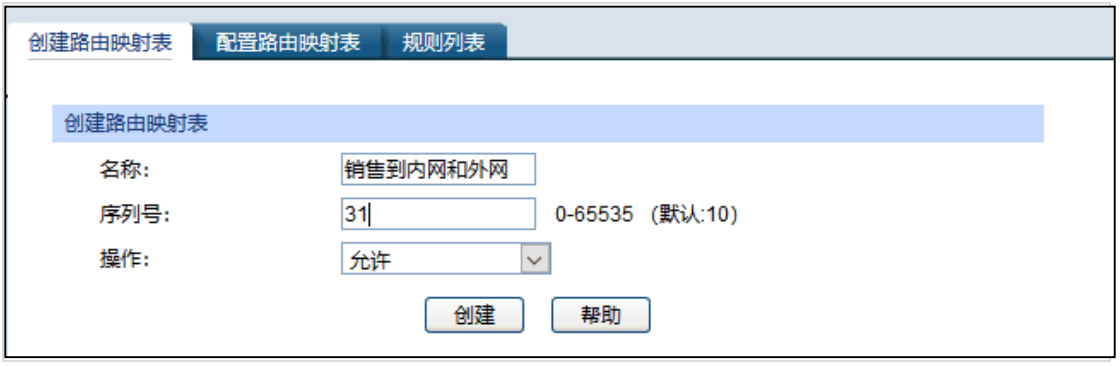
销售到外网的数据流
全选
删除
帮助

3、创建路由器映射表

指定策略路由的条目名称，后续用此条目绑定对应的 VLAN 接口，使能接口，在交换机 Web 界面：“路由功能”—“路由映射表”—“创建路由映射表”，此处创建三条路由映射表分别为：研发到内网，财务到内网和销售到内网和外网三条条目：



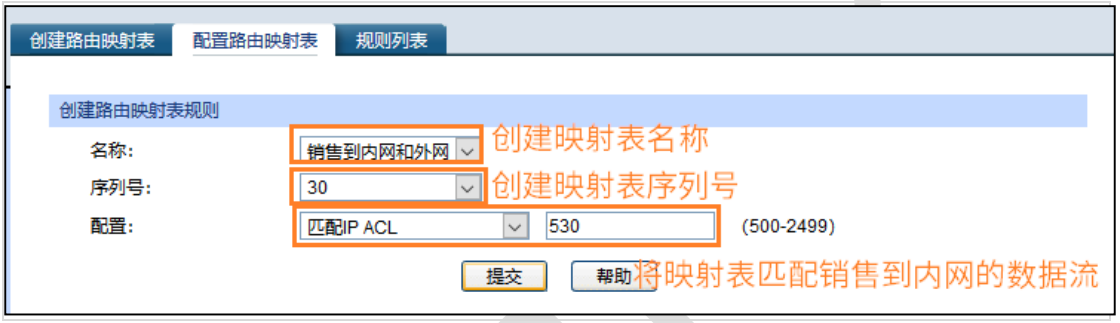




4、配置路由映射表，针对数据流配置交换机的转发操作，在交换机 Web 界面："路由功能"—"路由映射表"—"创建路由映射表，配置路由映射表"，创建路由映射表名称 --路由映射表匹配数据流 --针对匹配的数据流执行的转发操作：

本次列举销售部访问内网和外网数据流匹配操作。

内网：



说明：

- 交换机"设置下一跳"代表这条条目的优先级比系统直连路由高，即：VLAN 间互访数据也会匹配策略路由条目而不是匹配直连路由条目。
- 交换机"设置缺省下一跳"代表这条条目的优先级比系统直连路由低，即：VLAN 间互访数据会匹优先匹配直连路由。

外网：

说明：

- 交换机“设置下一跳”代表这条条目的优先级比系统直连路由高，即：VLAN 间互访数据也会匹配策略路由条目而不是匹配直连路由条目。
- 交换机“设置缺省下一跳”代表这条条目的优先级比系统直连路由低，即：VLAN 间互访数据会匹优先匹配直连路由。
- 在做数据流匹配的时候，一个路由映射表名称可以匹配多个数据流，通过序列号区分，且序列号越小优先级越高。

最终创建的几条路由映射表规则条目如下：


创建路由映射表
配置路由映射表
规则列表
路由映射表
名称:
研发到内网
删除
语句
序列号:
10
删除
操作类型:
允许
修改
规则列表
指定研发访问内网的数据下一跳为内网路由器的地址
选择
序号
匹配/设置
数值
0
匹配IP ACL
510
1
设置下一跳
192.168.100.1
全选
删除
帮助


创建路由映射表
配置路由映射表
规则列表
路由映射表
名称:
财务到内网
删除
语句
序列号:
20
删除
操作类型:
允许
修改
财务访问内网的数据流下一跳地址为内网路由器地址
规则列表
选择
序号
匹配/设置
数值
0
匹配IP ACL
520
1
设置下一跳
192.168.100.1
全选
删除
帮助


创建路由映射表
配置路由映射表
规则列表
路由映射表
名称:
销售到内网和外网
删除
语句
序列号:
30
序列号：30
删除
操作类型:
允许
修改
销售访问内网的数据下一跳为内网路由器
规则列表
选择
序号
匹配/设置
数值
0
匹配IP ACL
530
1
设置下一跳
192.168.100.1
全选
删除
帮助

5、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，在交换机 Web 界面：“路由功能”—“策略路由”—“策略路由配置”：

说明：

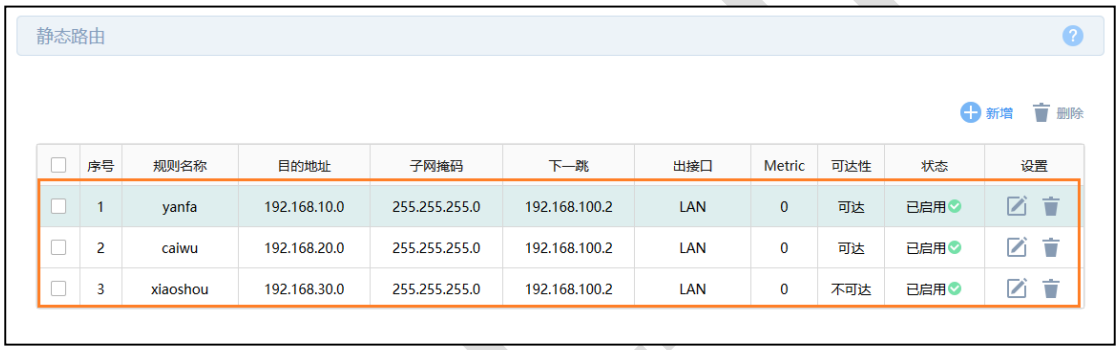
- 一个接口只能绑定一条路由映射表名称，但可以通过一个路由映射表中的序列号区分不同的数据流和动作。

6、配置内网和外网路由器

配置内网路由的 NAPT 条目和静态路由条目，保证数据正常转发。

内网路由器 NAPT 规则：

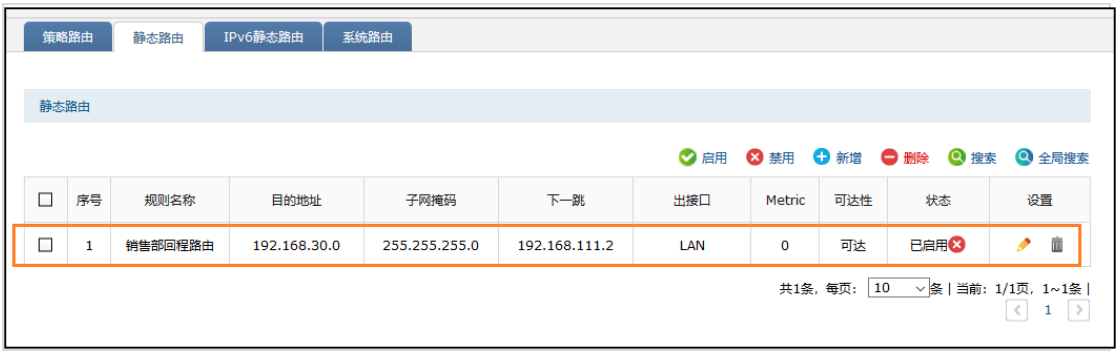
内网路由器回程路由规则：



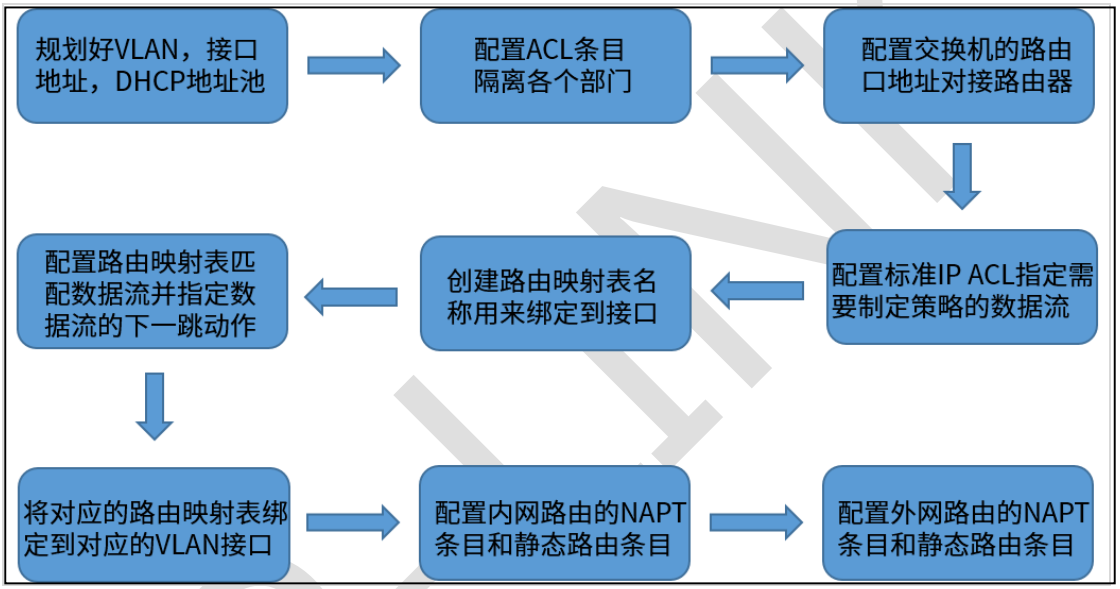
配置外网路由的 NAPT 条目和静态路由条目，保证数据正常转发。

外网路由器 NAPT 规则：

外网路由器回程路由规则：



配置大致流程如下：



至此，以上需求便可以通过配置交换机的策略路由功能全部实现。

第9章 服务质量

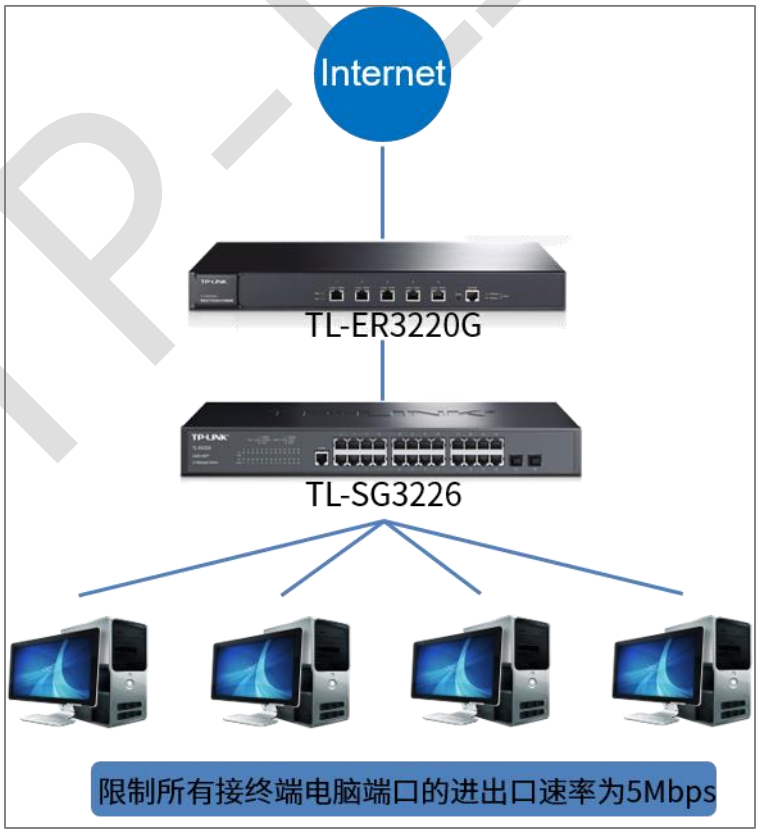
9.1 交换机带宽控制配置指南

9.1.1 应用介绍

交换机的带宽控制功能可以控制每个端口的出入口速率，在使用有限带宽的情况下，保证每个终端都能正常使用应用，不会因为某个端口流量过大导致其他终端无法上网的情况。

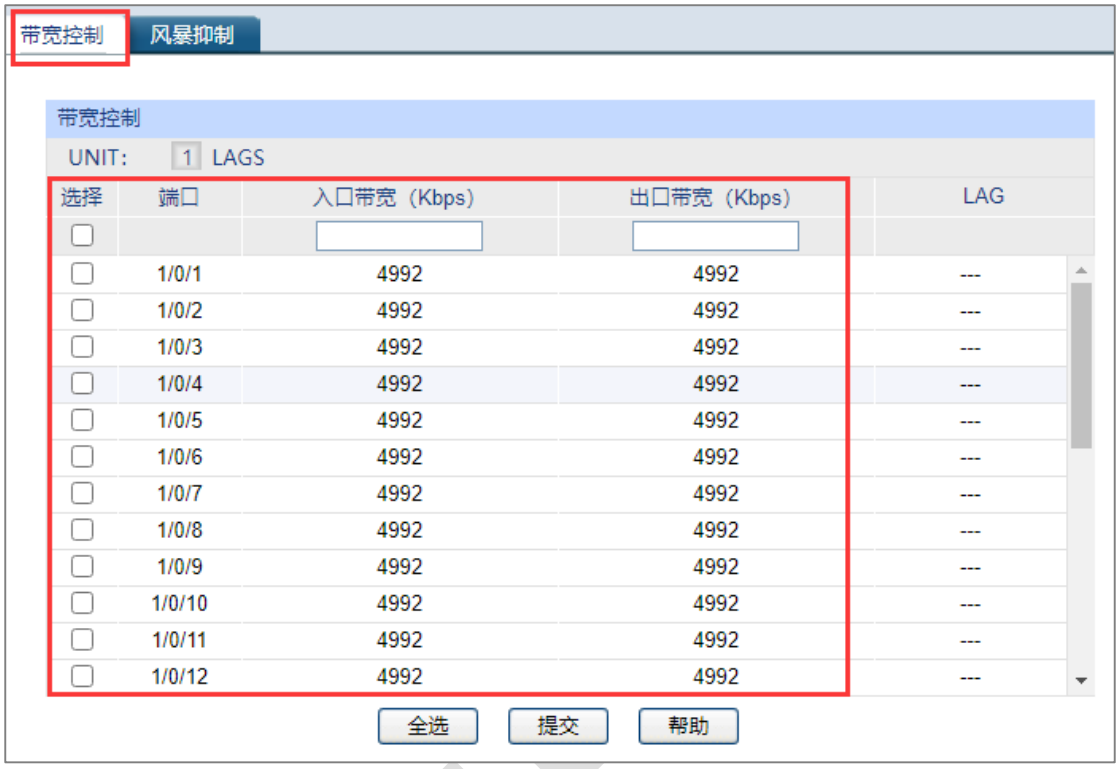
9.1.2 需求介绍

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：



9.1.3 设置方法

在“服务质量->流量管理->带宽控制”中，设置所有下联终端端口的出入口速率为 5Mbps，上联口 24 口不限制，注意单位为 Kbps，如下如所示。



说明：

- 同一个端口的入口带宽限制和风暴抑制不能同时开启；且端口限制数值必须为 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。

这样就可以限制除上联端口外的其他端口的进出口速率约为 5Mbps，保障了整个网络中终端都可以正常使用网络。

9.2 交换机风暴抑制配置指南

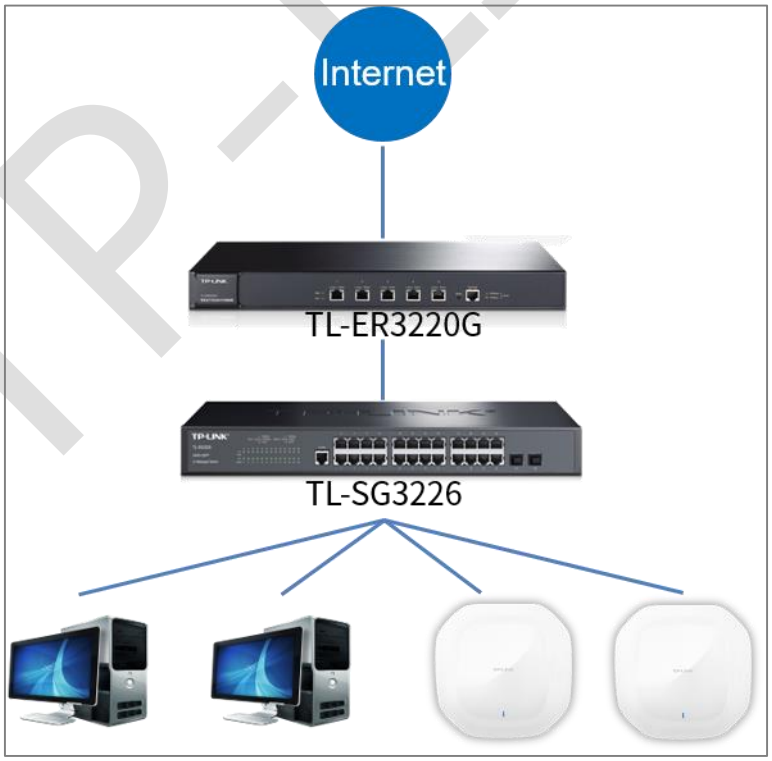
9.2.1 应用介绍

交换机的风暴抑制功能允许交换机在网络中过滤广播、多播和 UL 包。如果三种数据包的传输速率超过了设置的带宽，则会自动丢弃数据包以避免网络广播风暴，保障网络的运行稳定性，这种应用一般在无线网络的场景较多。

9.2.2 需求介绍

某企业使用一台 3 系列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，需要对真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：



9.2.3 设置方法

在“服务质量->流量管理->风暴抑制”中，设置所有终端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），如下如所示：

说明：

- 同一个端口的入口带宽限制和风暴抑制不能同时开启；且端口限制数值必须为 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。
- PPS 模式：交换机统计数据包不按照字节统计，而是按照每秒多少个广播包数量统计；默认情况下 PPS 模式是禁用的状态，启用后，单位只能为 PPS,不能为 kbps 或 ratio。
- 交换机界面还有一个统计单位为 ratio，单位含义为比率，使用此单位时取值范围只能在 0-100 范围内，含义为广播包占比端口总数据包的比例。

这样就可以限制端口的最高广播接受速率，保障了整个网络运行稳定性。

第10章 访问控制

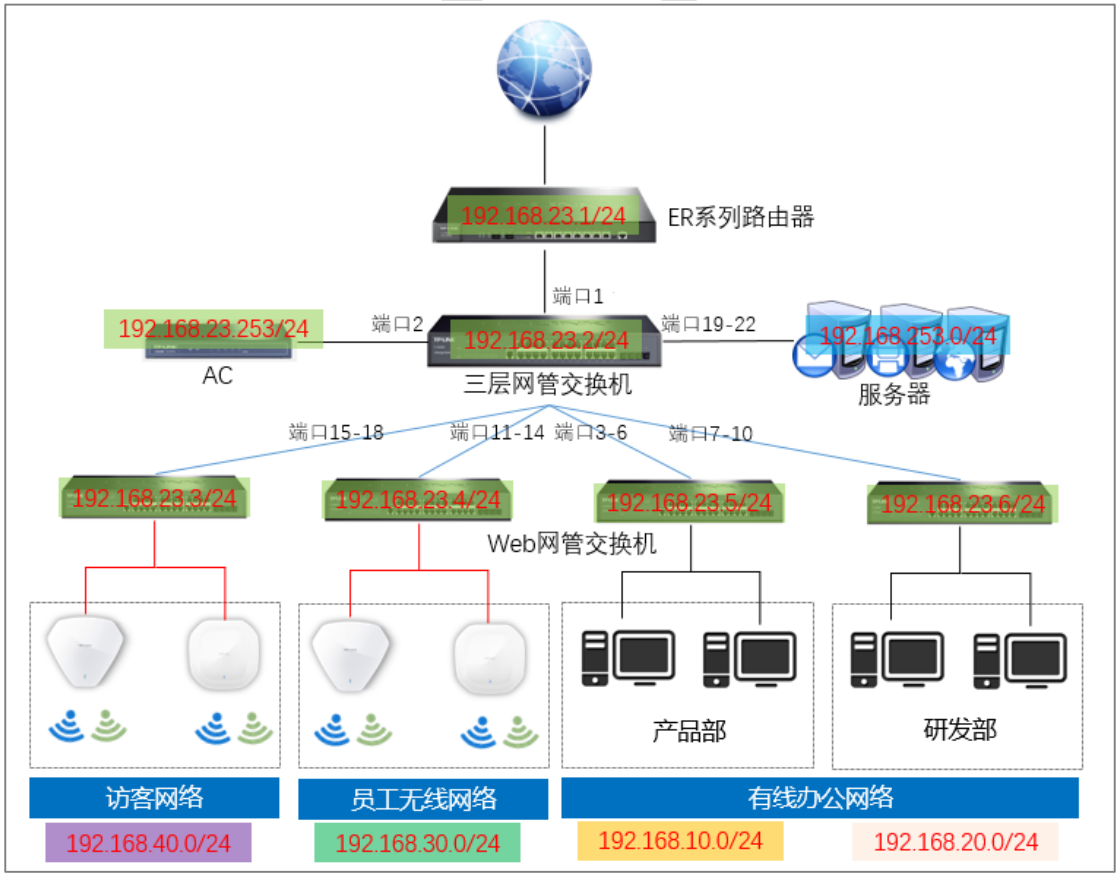
10.1 交换机访问控制设置指南

10.1.1 应用介绍

在交换机中主要通过 ACL 来控制访问权限，由于交换机默认规则是转发所有数据，ACL 控制是逐条匹配的，通过访问控制可以根据需求限制什么可以访问，什么不可以访问，交换机支持 MAC ACL ,标准 IP ACL ，扩展 IP ACL，控制非常灵活多变。

10.1.2 需求介绍

某企业划分了多网段，需要设置访问权限保障网络的安全性，本例使用其中的标准 IP ACL 进行配置，其余的 MAC ACL 等原理类似。示意网络拓扑如下：



需求

产品部：禁止访问研发部网络。

研发部：只允许访问服务器，禁止访问其余网络。

员工无线网络：禁止访问产品部、研发部、服务器网络。

访客网络：禁止访问产品部、研发部、员工无线网络、服务器网络。

10.1.3 设置方法

以研发部为例，具体设置如下：

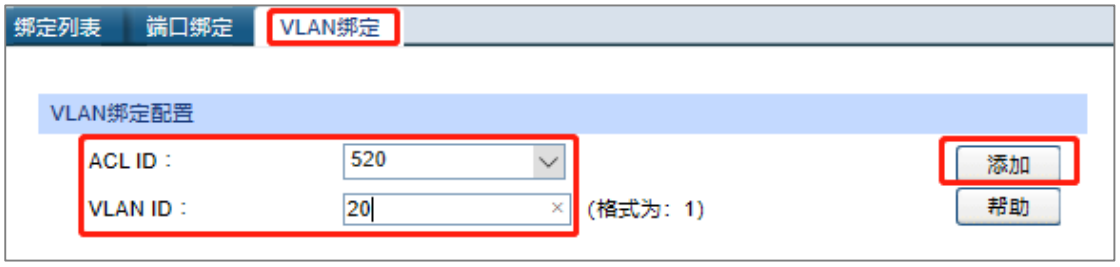
首先需要新建一个 ACL ID，标准 IP ACL 的 ID 号范围是 500-1499，本例使用 520。在“访问控制->ACL 配置->新建 ACL”中，输入 520，点击创建即可。

再根据需求创建 ACL 规则。在“访问控制->ACL 配置->标准 IP ACL”中，下拉选择创建的 ACL 520，输入规则 ID 21，安全操作选择允许，源 IP 为研发部 IP，目的 IP 为服务器 IP。如下图所示，完成后点击提交。

禁止访问其余网络的规则如下所示：

完成后 ACL 520 列表如下图所示：

最后绑定至相应 VLAN 中。在"访问控制->ACL 绑定配置->VLAN 绑定"中，下拉选择 ACL 520，输入 VLAN ID 号 20，点击添加。如下图所示：



其余网络重复上述三个步骤即可，注意每个网络都需要创建一个 ACL ID 号以进行 VLAN 的绑定。

其余网络创建后的 ACL 列表如下：

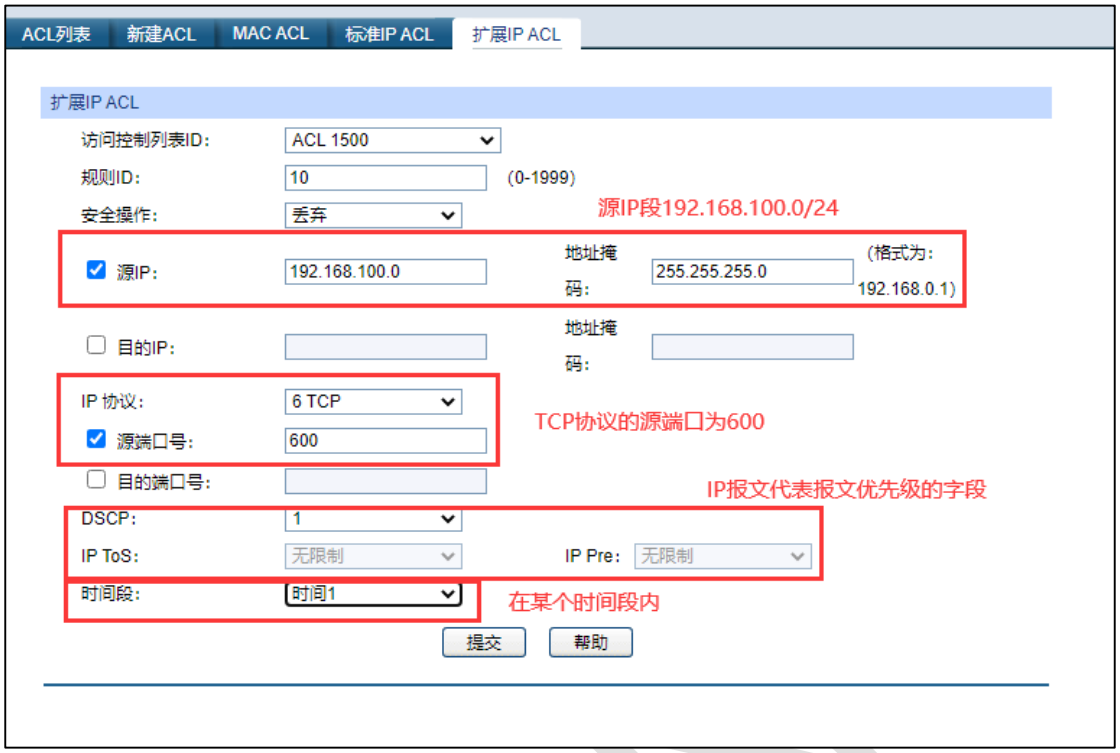
以上通过设置交换机的访问控制功能实现了企业各部门的访问控制需求，如需要更具体的需求可以通过设置 MAC ACL 或者扩展 IP ACL 进行控制。其中 MAC ACL 根据数据包的源 MAC 地址、目的 MAC 地址、二层协议类型等二层信息制定匹配规则，对数据包进行相应的分析处理。

扩展 IP ACL 可以根据报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性等信息来制定匹配规则，对数据包进行相应的分析处理。

例:

1、新建 ACL ID，ID 范围 1500-2499。

2、新建一条扩展 IP 条目:在时间 1 时间段丢弃源 IP 为 192.168.100.0/24,源端口为 600,IP 优先级 DSCP 字段字段为 1 的 TCP 数据包。



可以根据需要填写更具体的源目的 IP，源目的端口，以及对应的协议（ICMP,UDP,TCP 等）

2、条目创建成功后，将对应 ID=1500 的条目绑定到端口或者 VLAN 接口上即可生效，此处同标准 IP ACL 设置。

第11章 网络安全

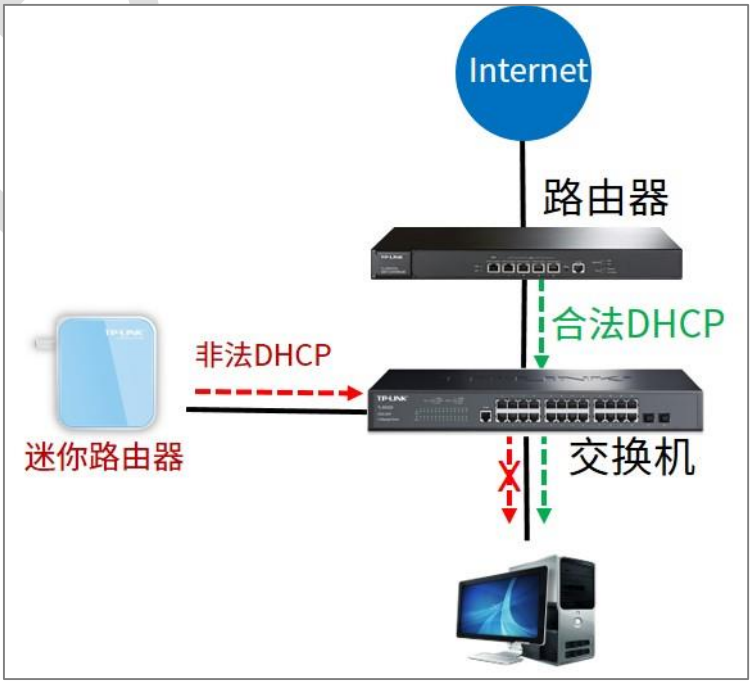
11.1 交换机 DHCP 侦听配置设置指南

11.1.1 应用介绍

DHCP 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。

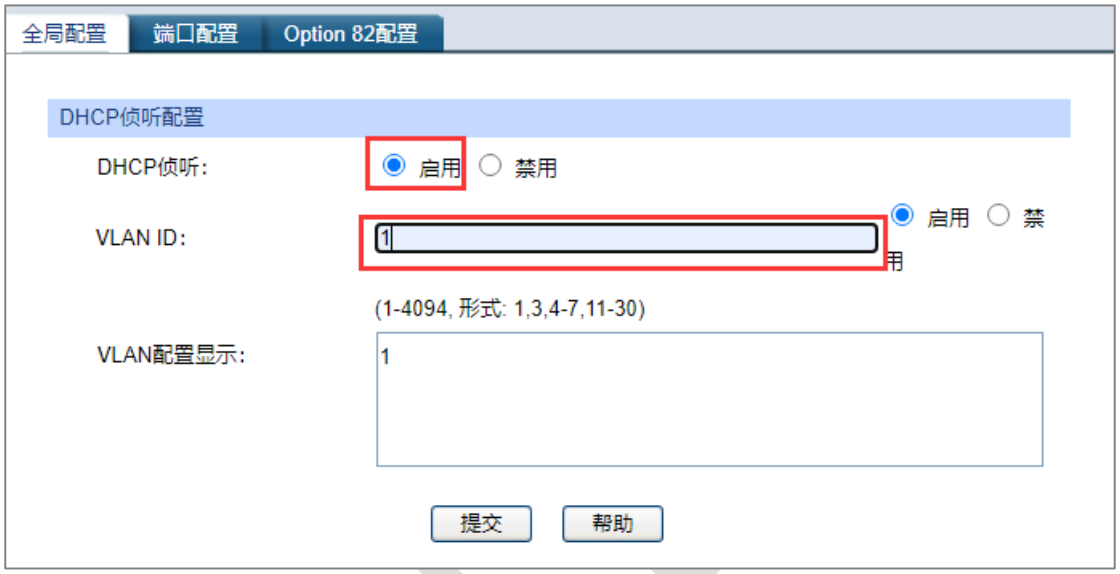
11.1.2 需求介绍

某企业通过 3 系列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 服务器获取 IP 地址，不能从非法的 DHCP 获取地址，示意网络拓扑如下：

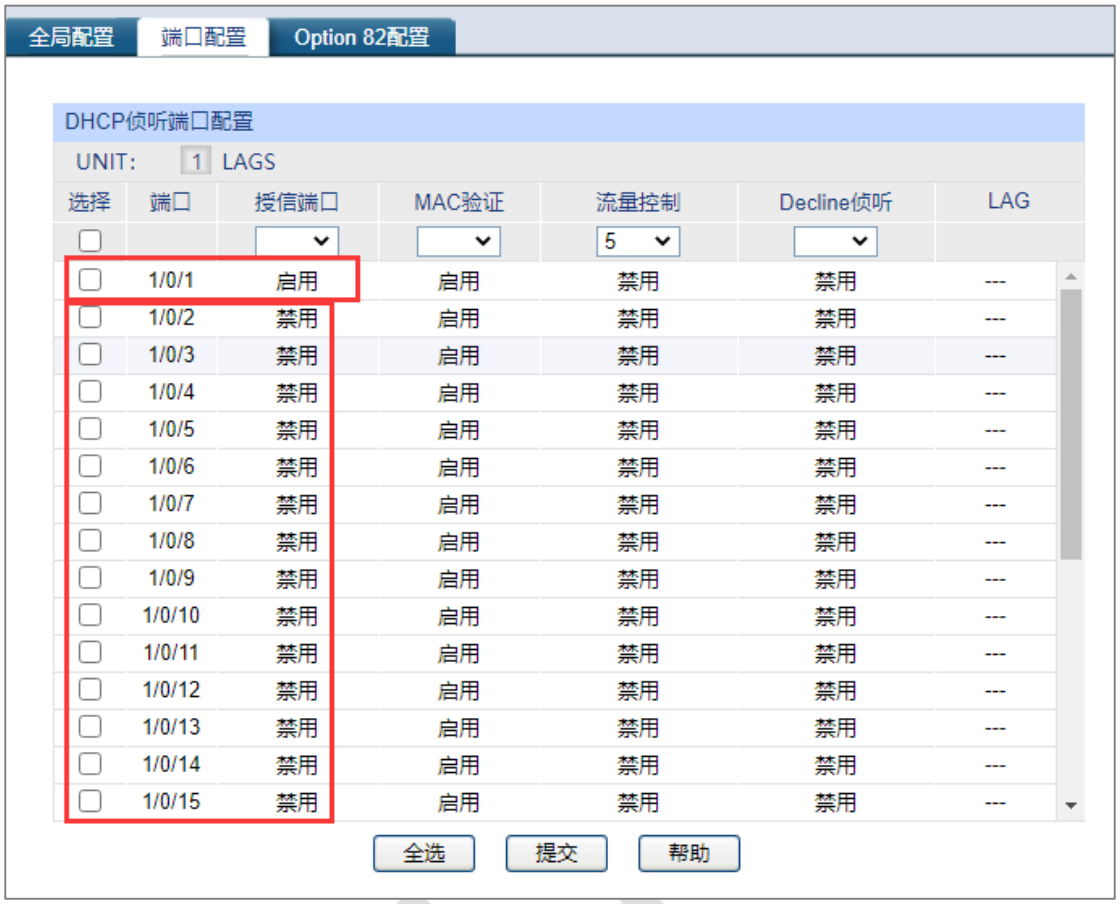


11.1.3 设置方法

在“网络安全->DHCP 侦听->全局配置”中，启用 DHCP 侦听功能，并选择生效的 VLAN，本例只有 VLAN 1 因此选择 VLAN 1，如果有其他 VLAN 需要开启侦听功能，也需要输入对应的 VLAN ID,如下如所示。



在“网络安全->DHCP 侦听->端口配置”中设置连接合法路由器的端口为信任端口，本例设置连接路由器的上联口 1 口为信任端口，其余为非信任端口，其余设置本例选择默认。



这样交换机上所接入的终端就只能从 1 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。

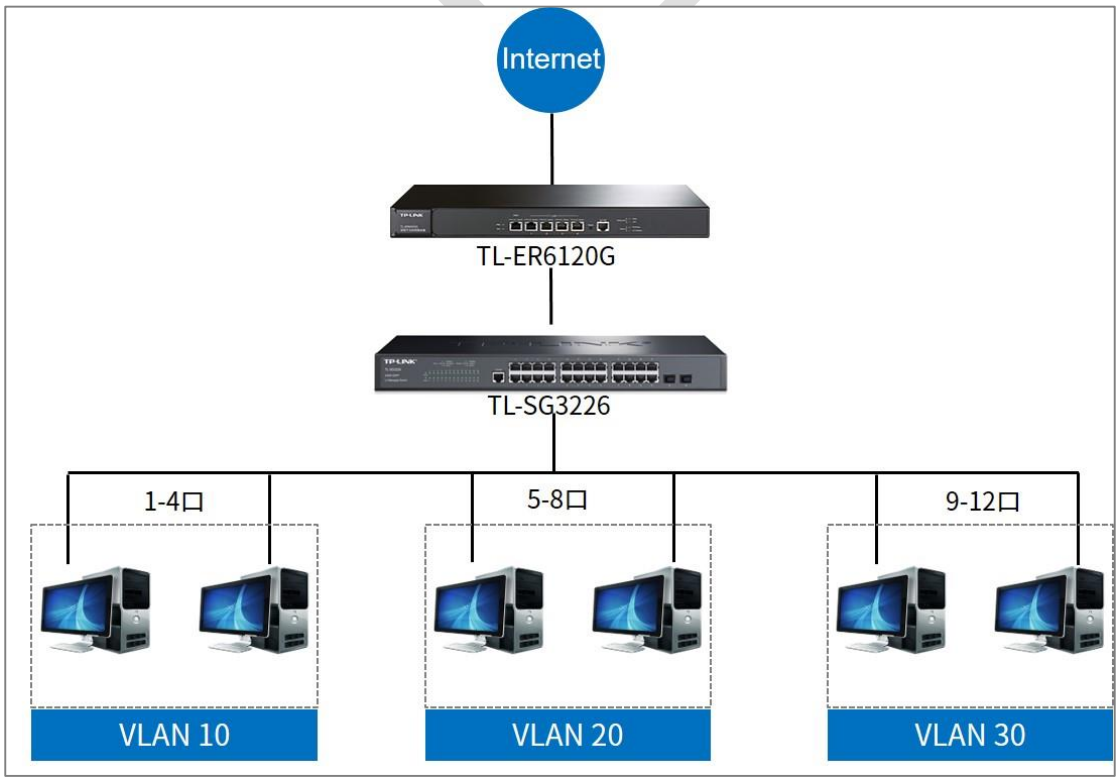
11.2 交换机四元绑定、ARP 防护、IP 源防护设置指南

11.2.1 应用介绍

四元绑定功能可以将局域网中计算机的 IP 地址、MAC 地址、VLAN 和端口进行绑定，ARP 防护功能以及 IP 源防护功能将使用四元绑定条目对数据包进行过滤，在使用了四元绑定条目后可以启用 ARP 防护，IP 源防护来进行网络保护，使只能是绑定条目中的设备才能通过交换机。

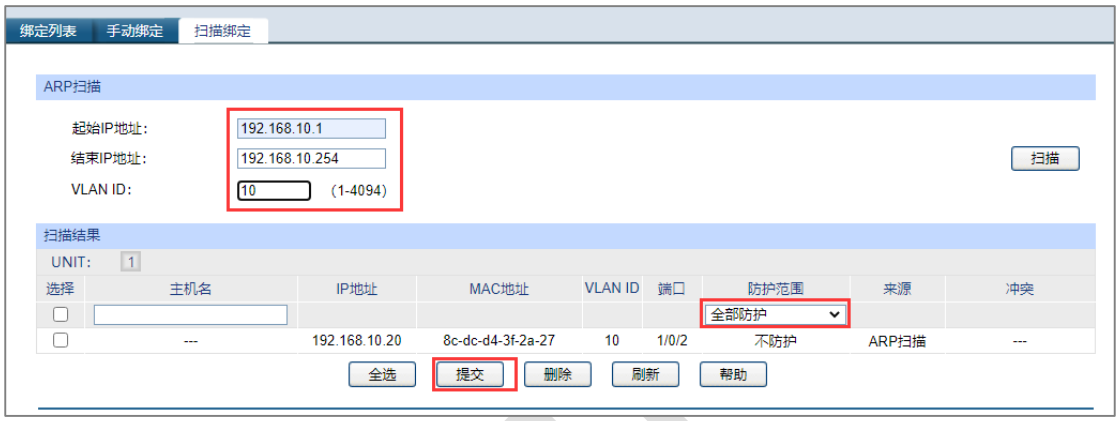
11.2.2 需求介绍

某企业通过 3 系列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：

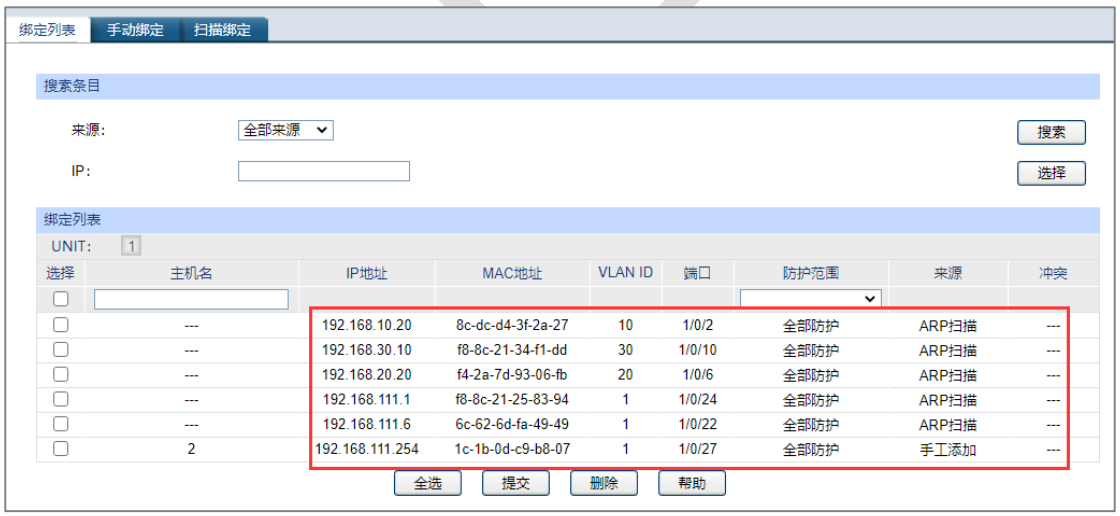


11.2.3 设置方法

在“网络安全->四元绑定->扫描绑定”中，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，并点击提交提交到绑定列表,如下如所示:



最终通过扫描出来的四元绑定列表如下:

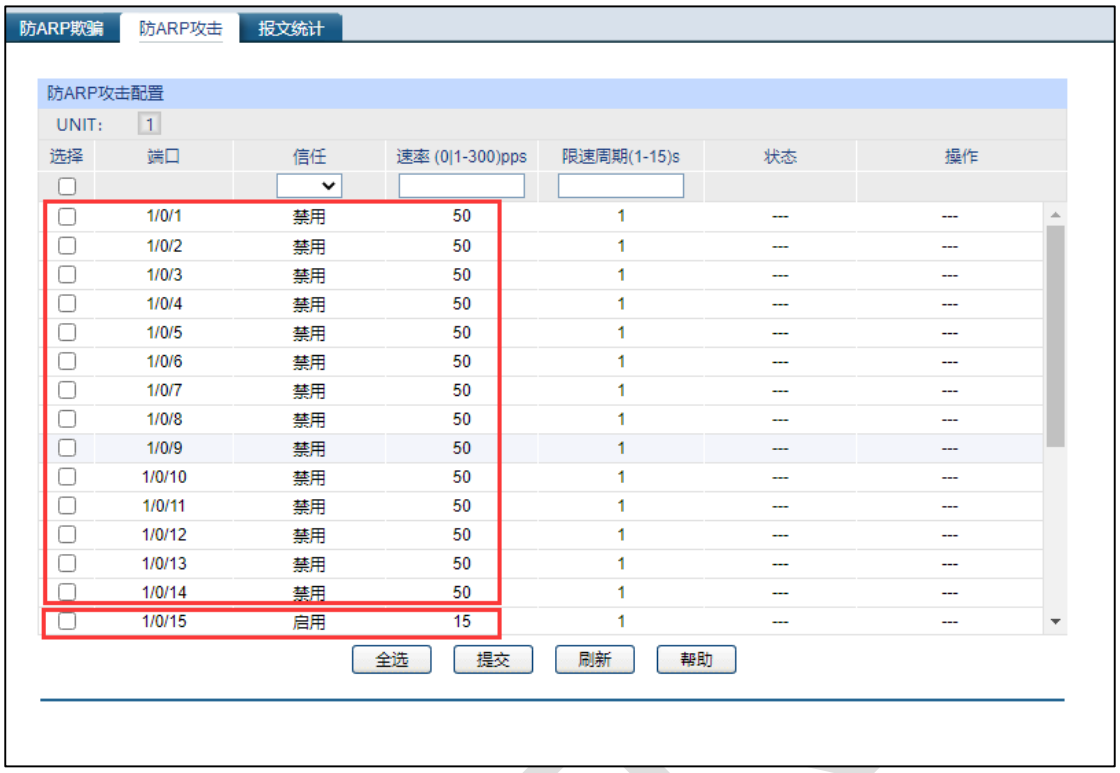


此时光有绑定列表还不能实现需求，需要在“网络安全->ARP 防护->防 ARP 欺骗”中启用源 MAC 验证，目的 MAC 验证，IP 验证，并使能对应的 VLAN，然后点击提交:

说明：

- 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，本处的发送 MAC 是四元绑定条目中对应端口的所对应的 MAC。
- 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,本处目标 MAC 是指这个端口所对应四元绑定条目中的 MAC。
- 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。
- 交换机会根据四元绑定条目来匹配对应端口的 ARP 报文中的源 MAC 或者目的 MAC 是否是端口已经绑定的 MAC，如果不是则选择丢弃。

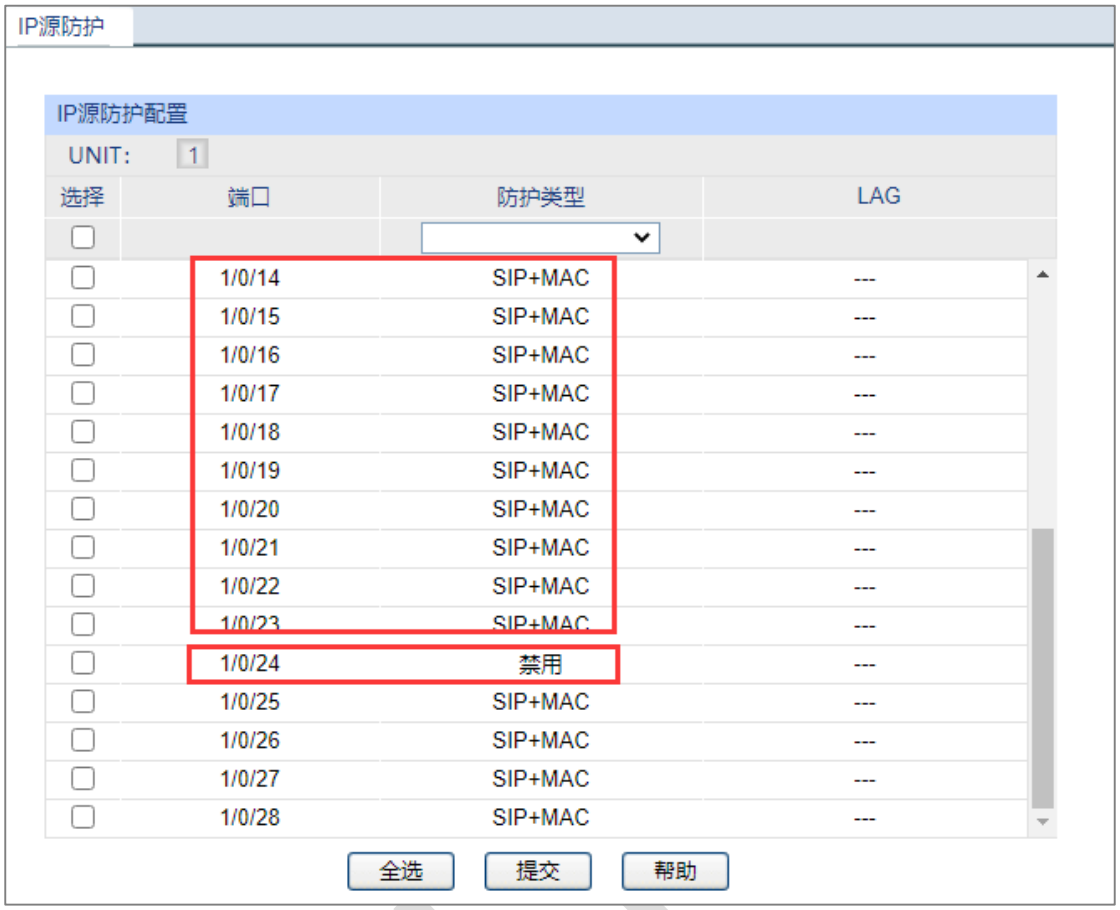
如果用户对网络中的 ARP 报文的数量也需要控制，可以在“网络安全->ARP 防护->防 ARP 攻击”中设置端口的 ARP 报文的速率，单位 PPS，当端口收到的 ARP 报文速率高于设定值后，该端口将会断开，需要手动在界面恢复，因此设置值需要根据实际网络中有用 ARP 的数量来定。



注意：

- 交换机上联口可以启用信任，这个口将放行所有的 ARP 报文，不会对数量有限制。
- 防 ARP 攻击功能需要启用对应 VLAN 才能生效，因此也需要根据四元绑定条目来匹配，如果和对应端口的四元绑定条目不匹配，交换机将会丢弃报文。

同时在“网络安全->ARP 防护->IP 源防护”中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：



说明：

- 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。

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。

第12章 802.1X

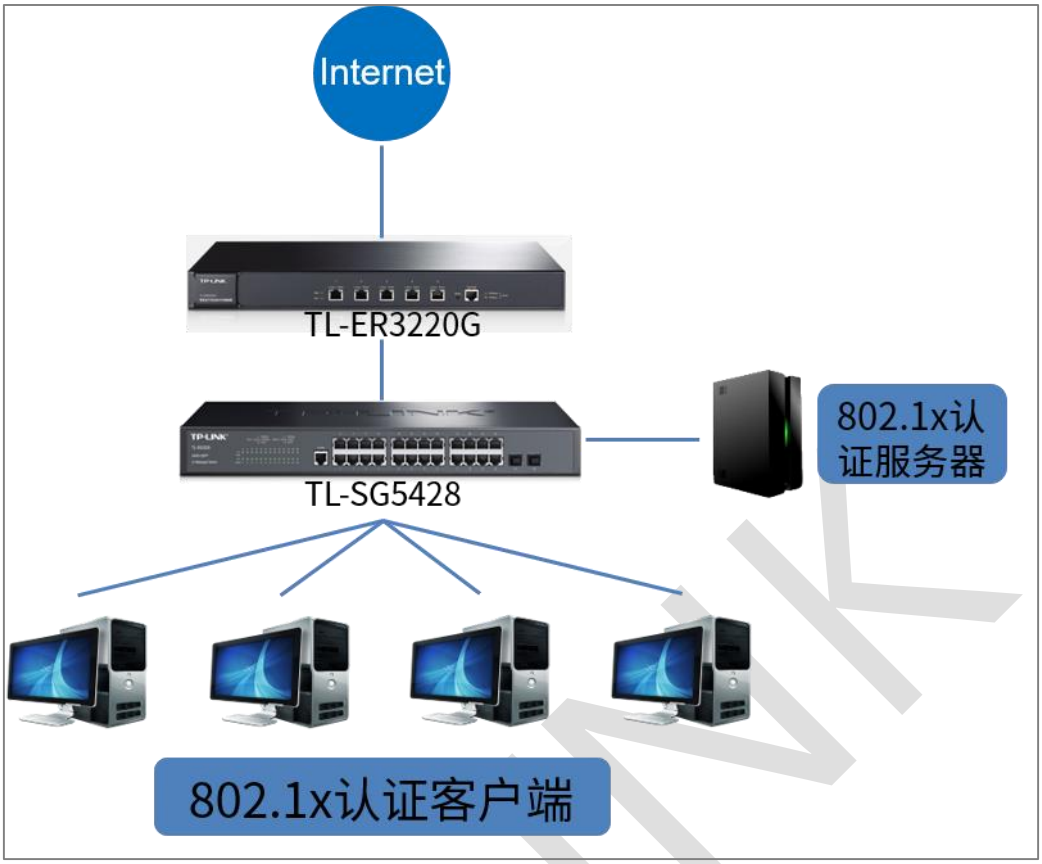
12.1 交换机 802.1X 认证功能配置指南

12.1.1 应用介绍

802.1X 协议作为局域网端口的接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。 802.1X 协议是一种基于端口的网络接入控制协议，“基于端口的网络接入控制”是指在局域网接入设备的端口这一级，对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

12.1.2 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，只有通过登陆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，拓扑结构如下：



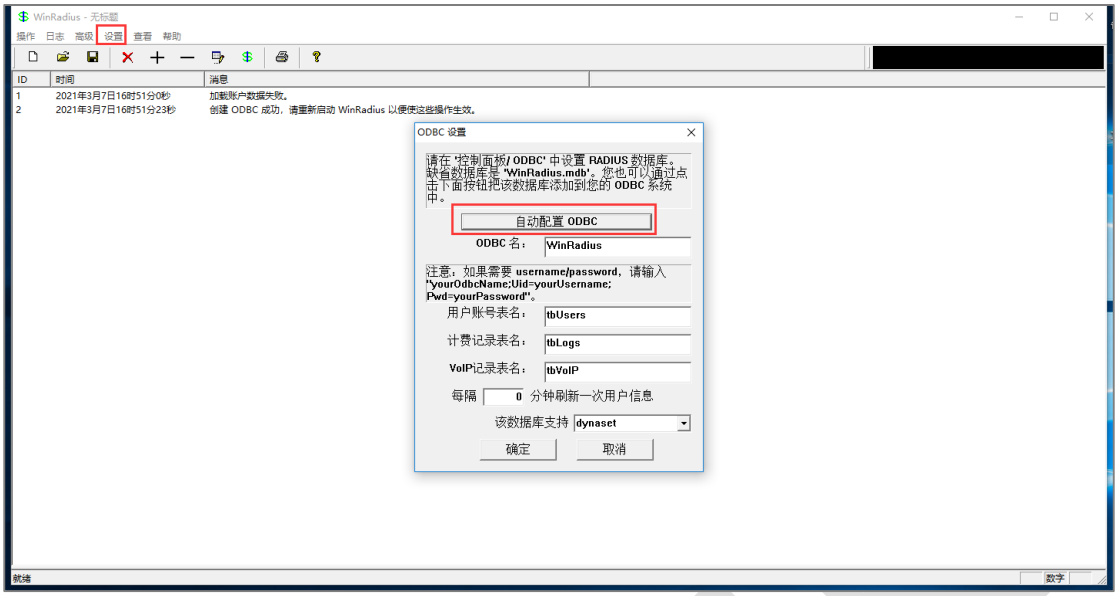
图中以 TL-SG5428 做为中心交换机， 802.1X 认证服务器接在 TL-SG5428 上。所有终端都需要通过认证之后才能访问服务器资源或者网络资源。下面将介绍实现局域网中每台设备通过交换机的 802.1X 功能搭配 Radius 服务器实现认证接入的配置过程。

12.1.3 设置方法

第一步、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)。

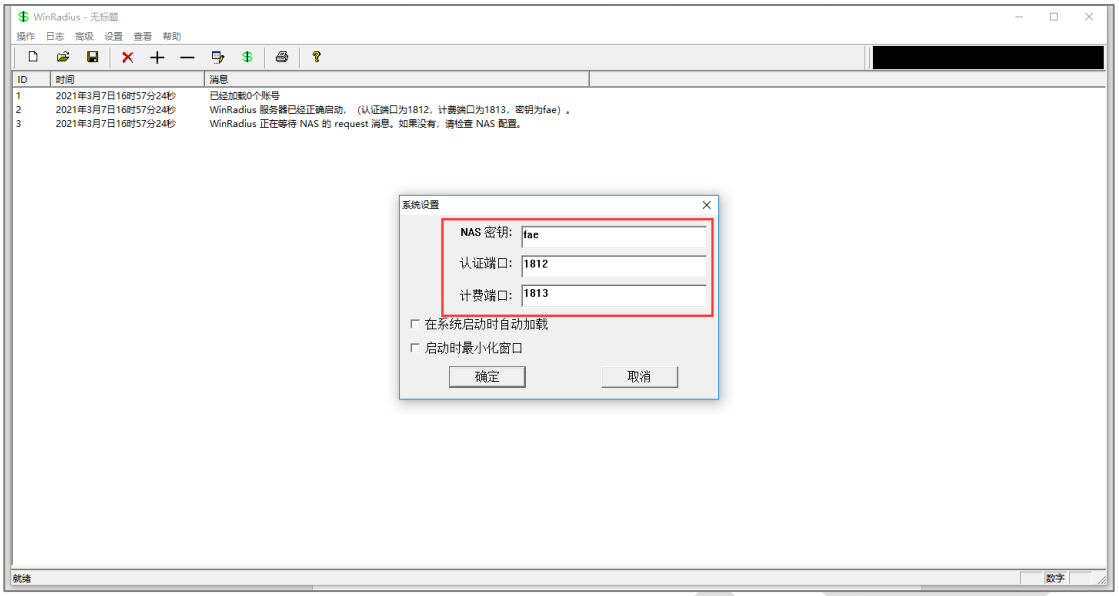
1、启用 Winradius，用管理员身份运行，并在“设置—数据库—自动配置 ODBC”，配置数据库，数据库配置成功后再重启软件。

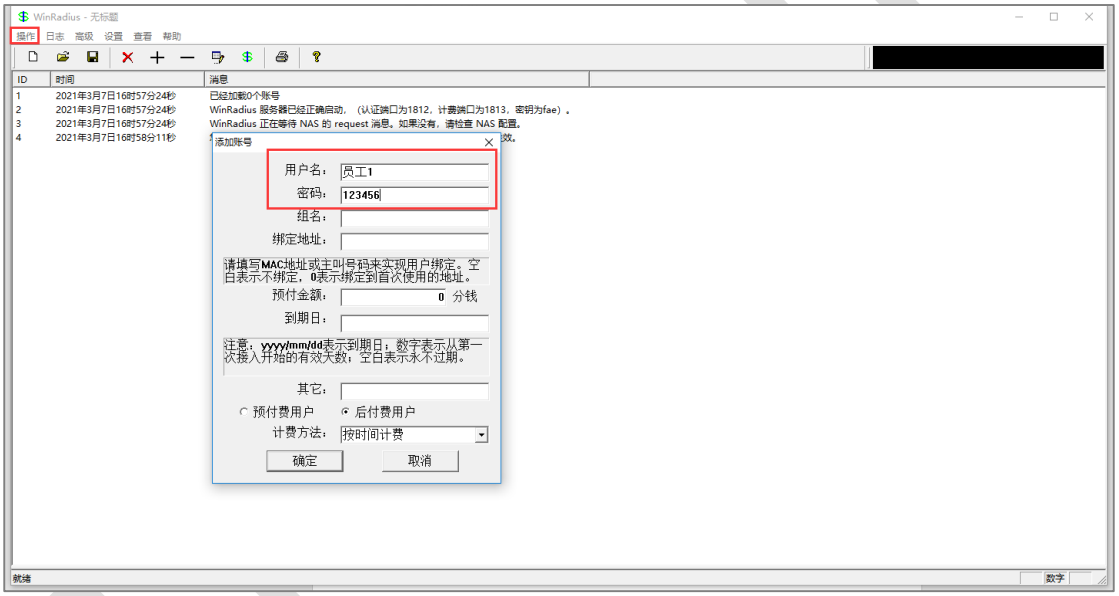


2、软件重启成功后，配置服务器参数

认证服务器上的配置：

- 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

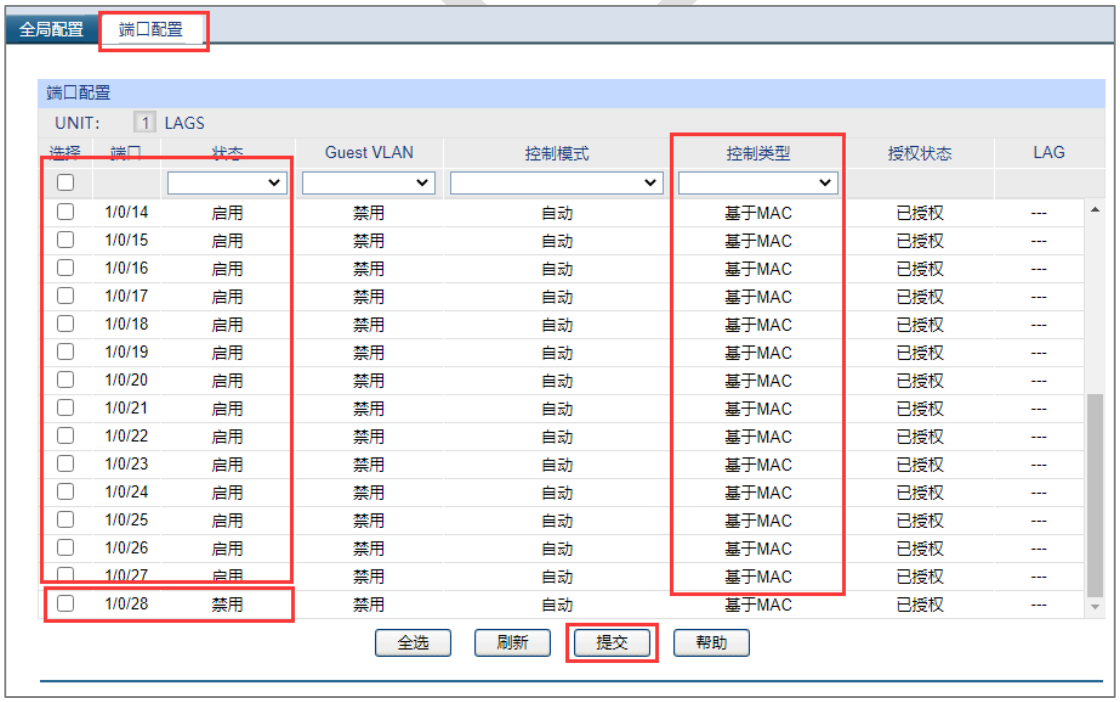




第二步、配置 TL-SG5428 的 802.1X 功能

1、802.1X 配置。在交换机的"网络安全—802.1X 认证—全局配置"界面，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。

2、在交换机的“网络安全—802.1X 认证—端口配置”界面，配置对应端口的 802.1X 功能。

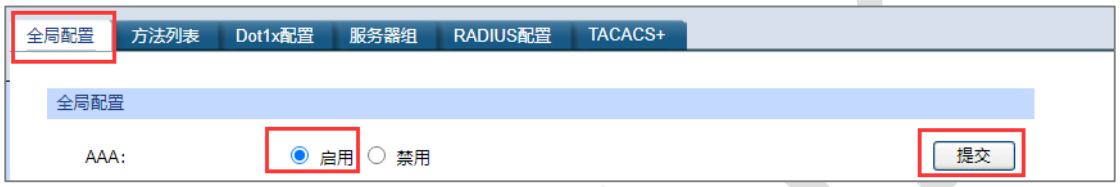


说明：

- 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。

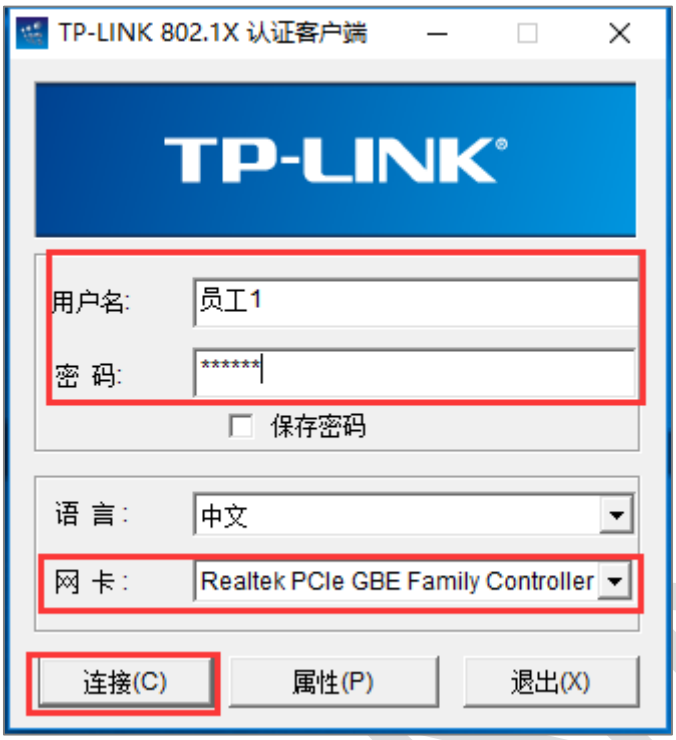
- 配置其它需要认证的端口。(TL-SG5428 可同时支持基于 MAC 和 Port 的认证，这里均采用基于 MAC 的认证方式)。
- 如果端口的"状态"处于禁用，则该端口下的设备不需要进行认证，始终处于接入网络的状态。
- 控制类型中，"基于 MAC"意为着该端口下的所有设备必需单独进行认证，认证通过后才能接入网络；"基于 Port"意味着该端口下只要有一台设备认证通过，其它设备不再需要认证也能接入网络。

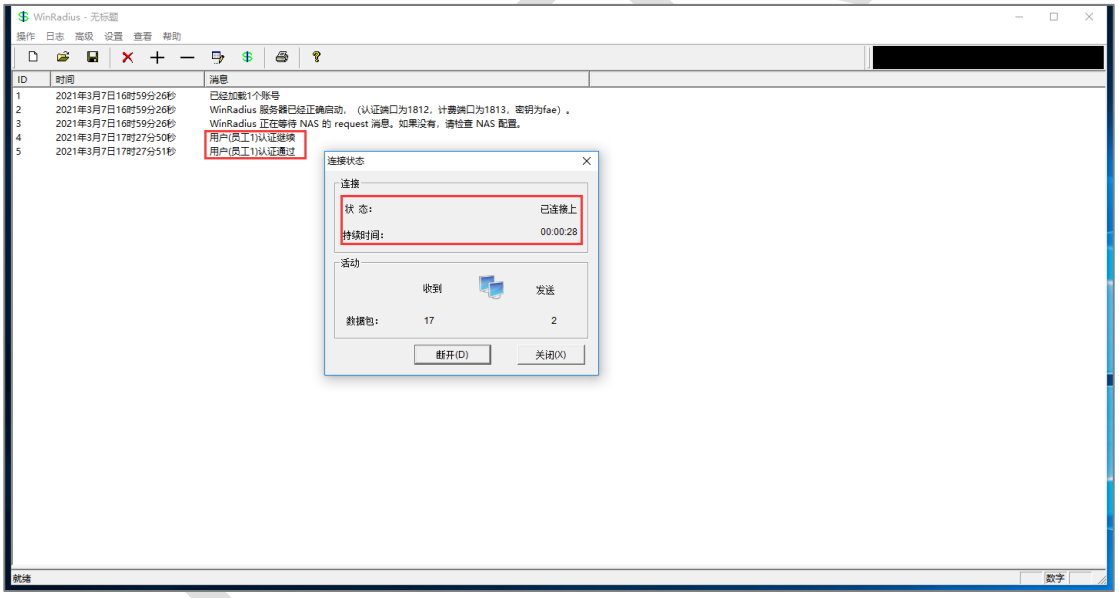
2、AAA 配置。在交换机的"网络安全—AAA—全局配置"界面，配置交换机的 AAA 认证功能，全局配置 AAA 功能启用，以便对接 Radius 服务器。



在交换机的"网络安全—AAA—RADIUS 配置"界面，配置交换机所对接的 Radius 服务器信息。

3、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。

第13章 工业级特性

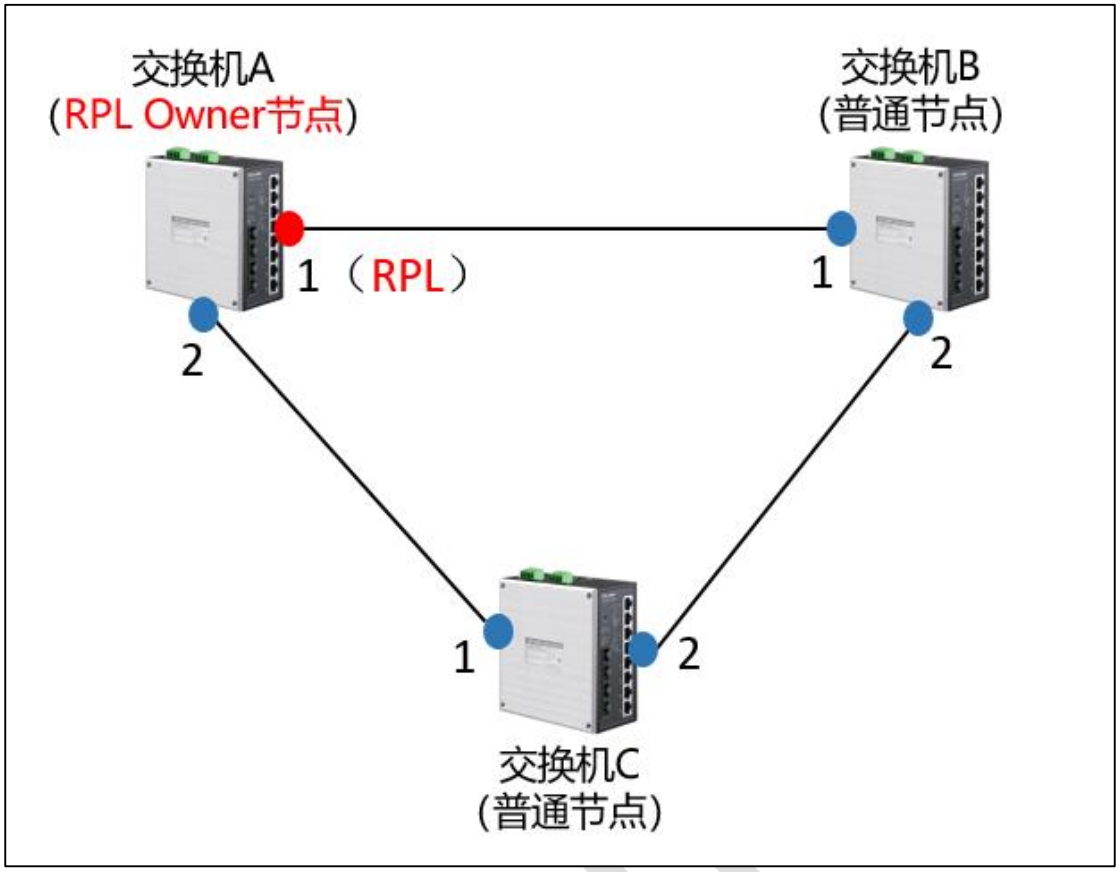
13.1 ERPS 单环环网配置指南

13.1.1 应用介绍

工业环境的交换机需要保证运行的稳定性，即便出现一台设备故障 可以通过其它设备替代运转，而且要求切换快速无延迟。工业级的 ERPS 环网即可满足这种使用场景，比一般的生成树协议切换更快速，能做到业务的无中断切换。ERPS 环网正常工作时，RPL 端口阻塞所在链路，防止网络环路；当环网中某条链路出现异常断开时，异常节点会发包通知 RPL Owner 节点，于是 RPL 端口放开，使所在链路恢复正常通信，保障整个网络通信不中断。一个环网中，有且仅有一个 RPL Owner 节点。

13.1.2 需求介绍

某工业环境使用交换机组环网，保障任何一台交换机故障都不会影响业务的转发，使用 ERPS 组环网拓扑如下：



13.1.3 设置方法

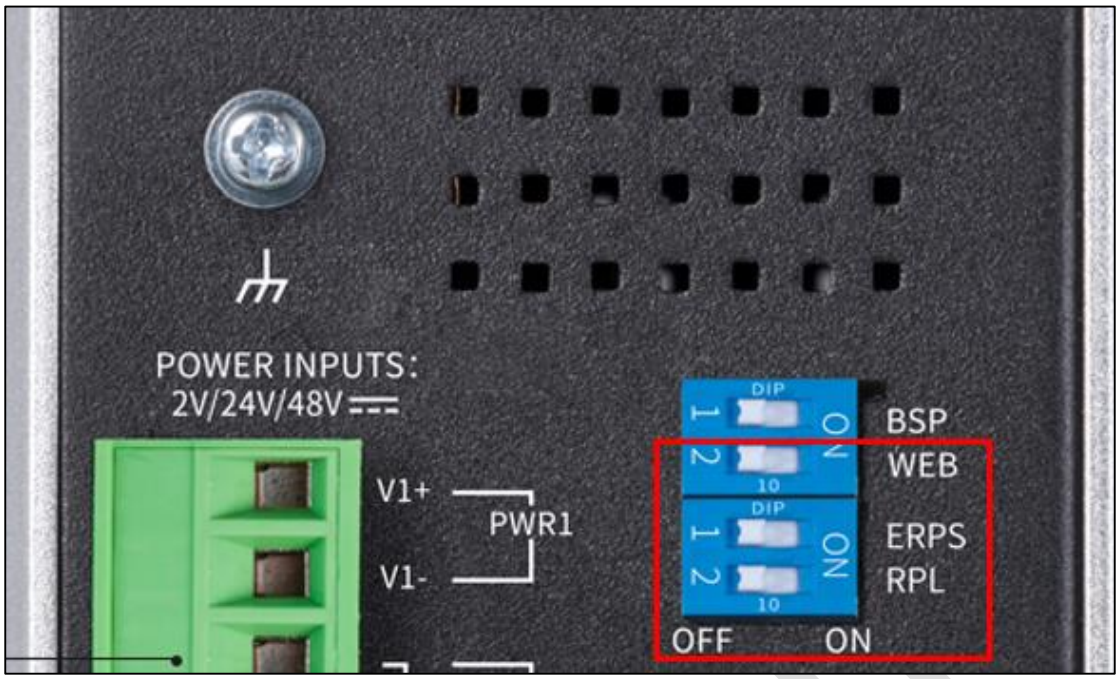
1、通过拨码开关快速配置（以 TL-SG2210R 工业级为例）

TL-SG2210R 工业级交换机机身有 DIP 拨码开关，涉及到 ERPS 环网配置的有以下三个开关：

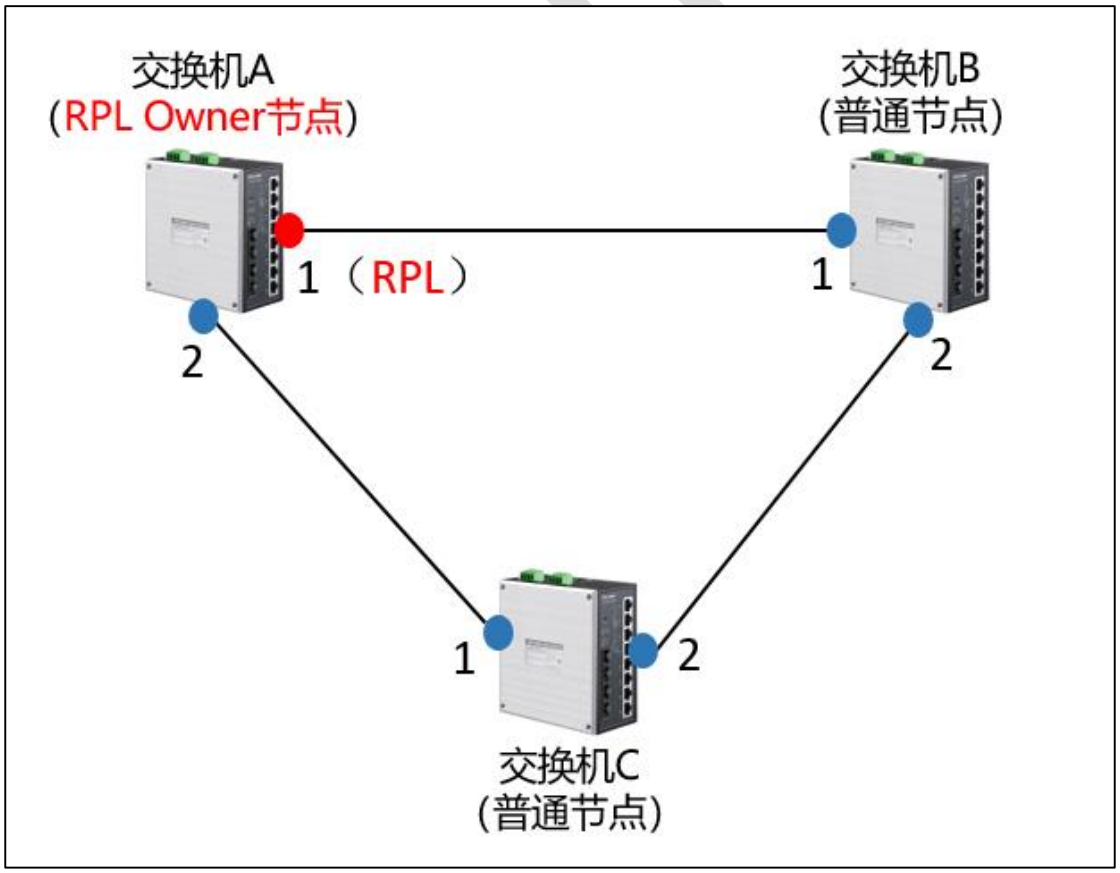
WEB：默认关闭，开启后，交换机开启 WEB 管理功能，只有开启 WEB 管理开关，才能使用 ERPS 环网功能。

ERPS：默认关闭，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 端口。



那么对于这样一个环网拓扑：



只需做如下操作：

(1) 交换机 A 将 WEB 开关、ERPS 开关和 RPL 开关都拨到 ON；

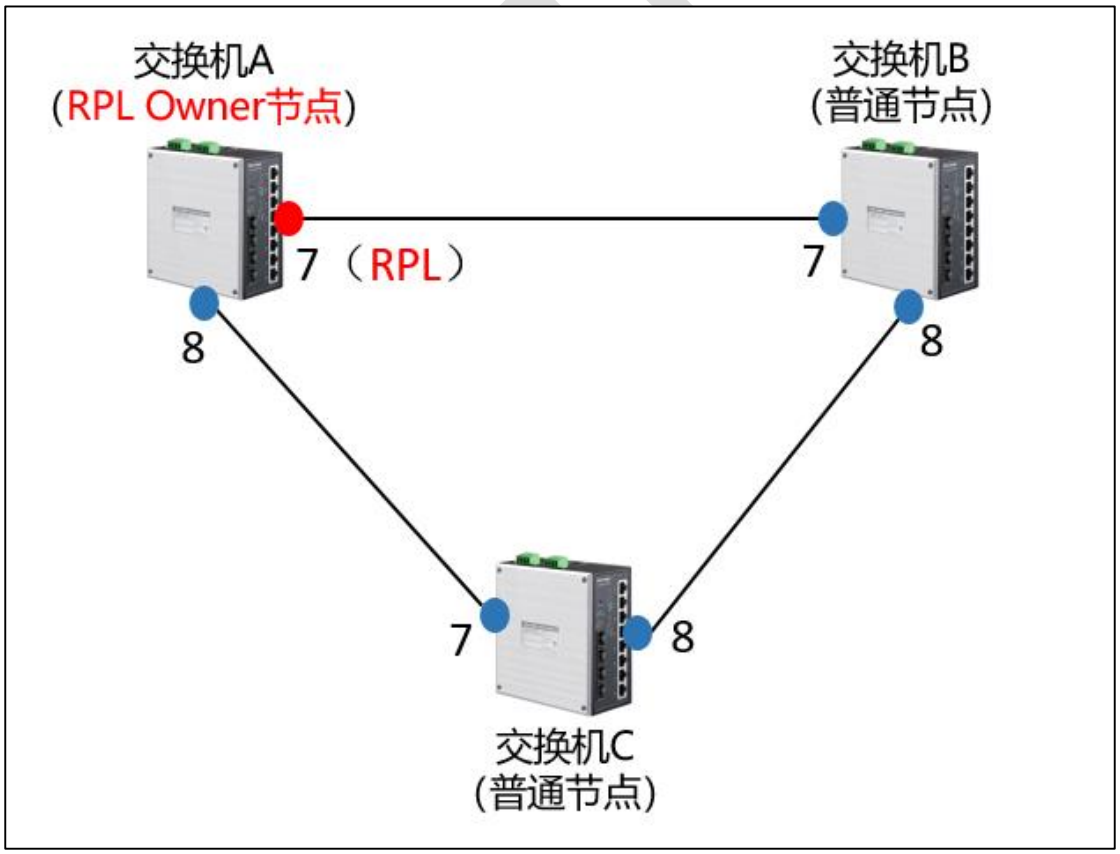
(2) 交换机 B、C 将 WEB 开关和 ERPS 开关拨到 ON。

(3) 将三台交换机的端口 1、2 按照拓扑连接起来。

需要注意的是，使用拨码开关来配置环网时，只能使用端口 1、2 来组建环网，且只能配置端口 1 为 RPL Owner 端口。如果需要使用其他的端口来组建环网，比如使用光口来组建光纤环网，那么就必须采用 WEB 页面配置的方法。

2、WEB 页面配置

使用 WEB 页面配置时，可以任意指定所用端口，拓扑示意如下：



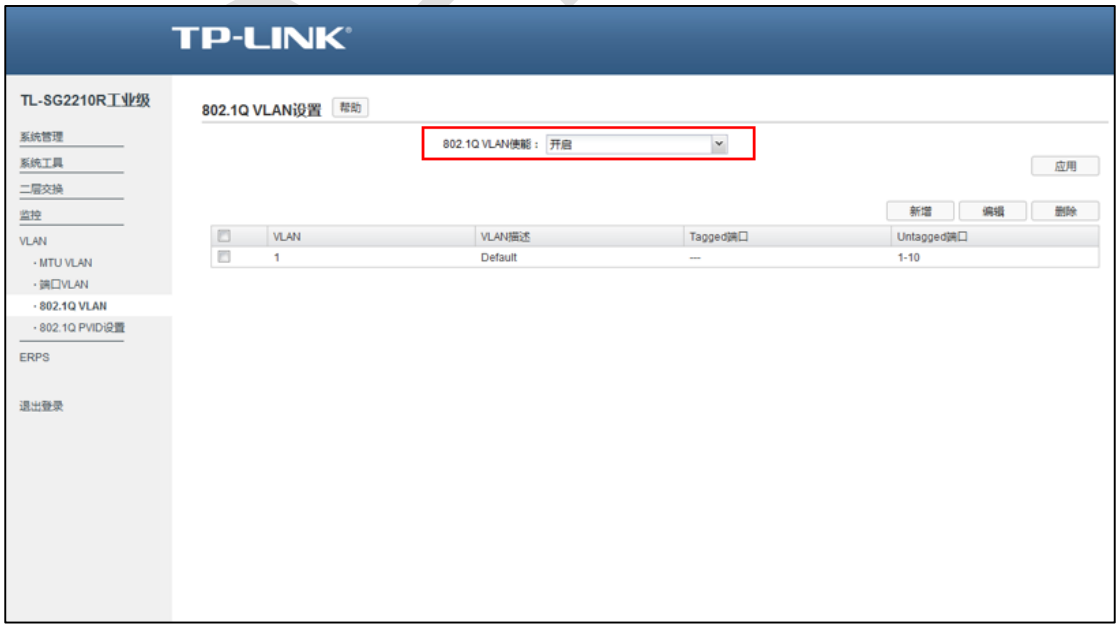
角色分类：交换机 A 为 RPL Owner 节点，交换机 B、C 为普通节点。

交换机 A 配置

（1）启用交换机的 802.1Q VLAN 功能

依次点击<VLAN>→<802.1Q VLAN>，将“802.1Q VLAN 使能”选择为开启，如下图所示：

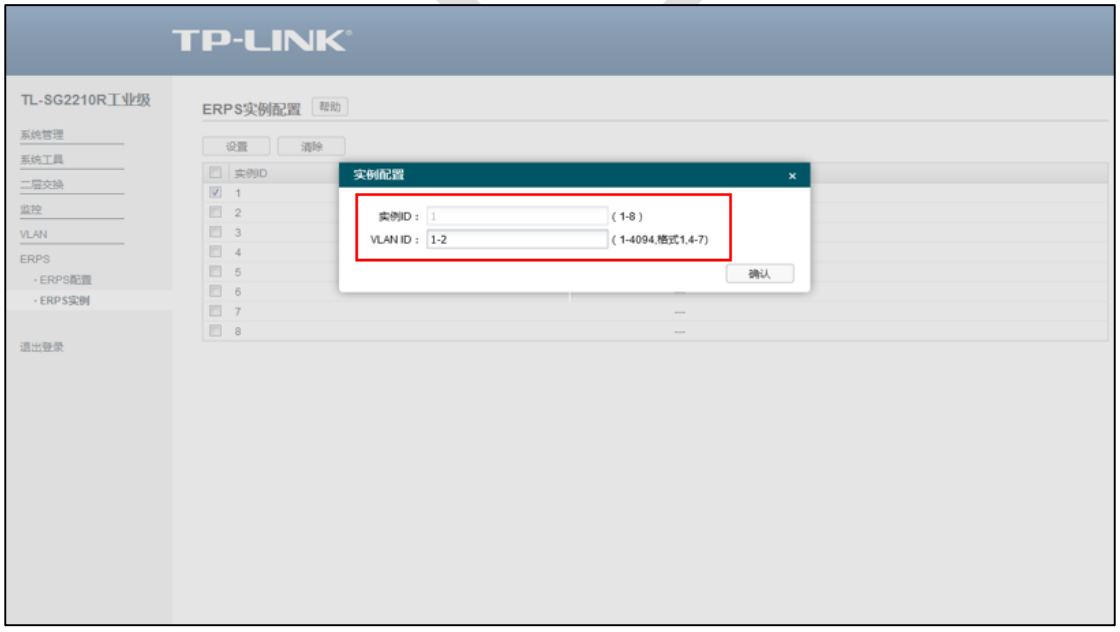
点击<应用>后，页面显示如下图所示：



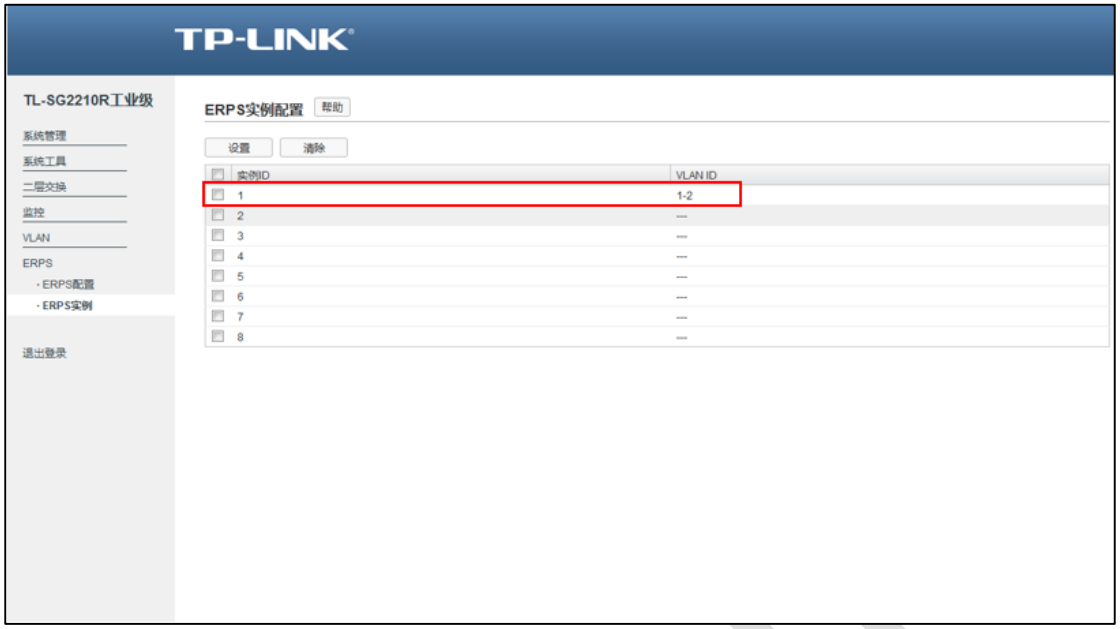
（2）配置环网保护实例

依次点击<ERPS>→<ERPS 实例>，勾选一个实例，然后点击<设置>，如下图所示：

点击<设置>后，填写需要保护的 VLAN，要同时包含数据 VLAN 和协议 VLAN，此处数据 VLAN 为 1，预设协议 VLAN 为 2，如下图所示：



点击<确认>后，页面显示如下图所示：



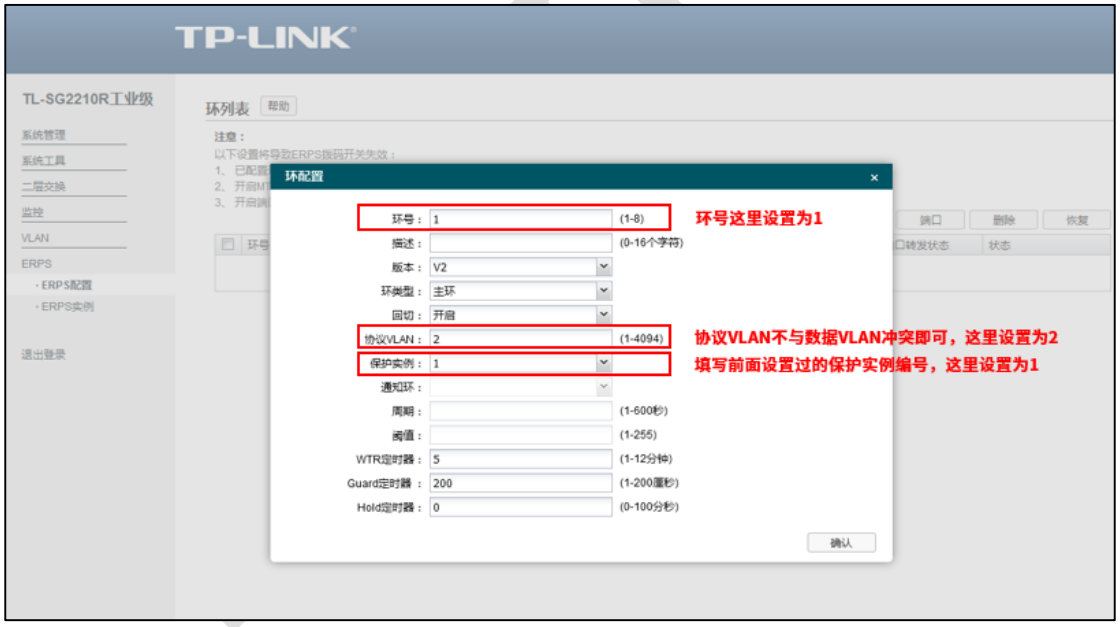
这里，就完成了保护实例的配置，需要注意的是，设置的 VLAN ID 范围，需要包含所有数据 VLAN 和协议 VLAN，比如数据通信用到了 VLAN 1-5，TP 环的协议 VLAN 设置为 10，那么这里 VLAN ID 范围可以设置为 1-10。协议 VLAN 在 ERPS 环配置中会用到。

（3）配置 ERPS 环

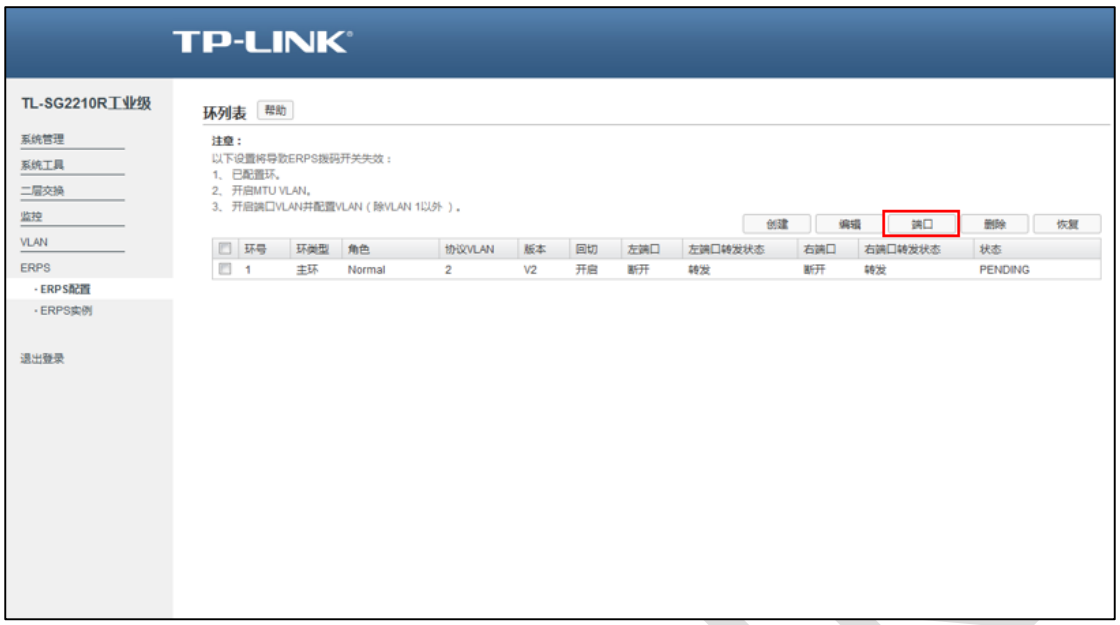
环配置：

依次点击<ERPS>→<ERPS 配置>，然后点击<创建>，如下图所示：

点击<创建>后，配置“环号”、“协议 VLAN”、“保护实例”，如下图所示：

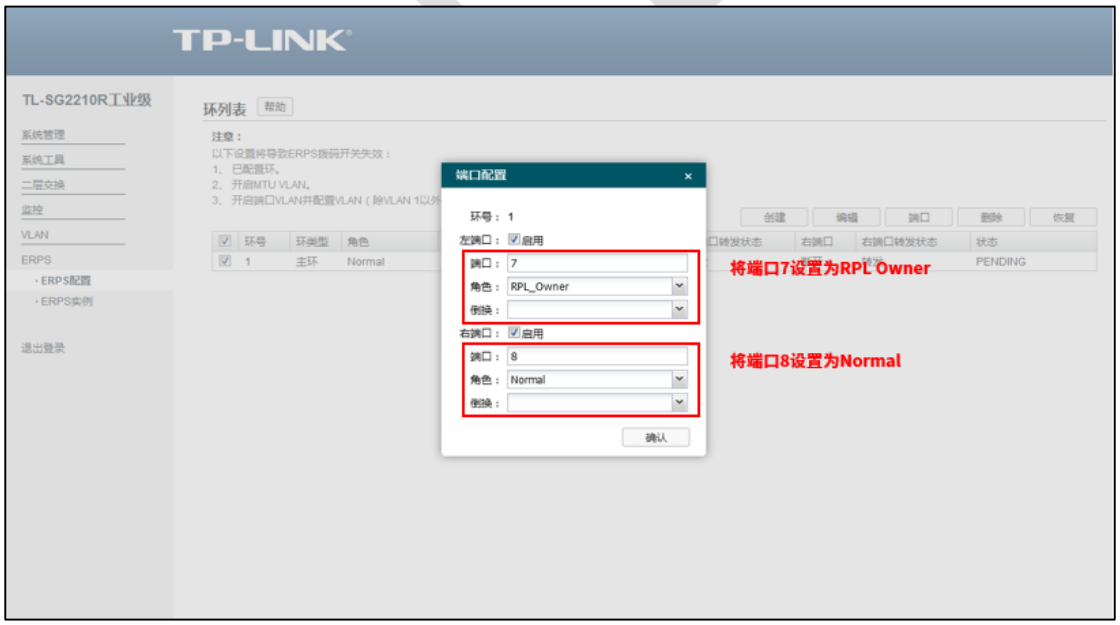


点击<确认>后，页面显示如下图所示：



左右端口配置：

点击上图中红框标出的<端口>，进入左右端口配置，将端口 7 设置为 RPL Owner，将端口 8 设置为 Normal，如下图所示：



点击<确认>，则完成了左右端口配置。

到这里，就完成了对交换机 A 的配置。

交换机 B.C 配置

交换机 B、C 与交换机 A 的唯一区别就是，B 和 C 不需要设置 RPL Owner。也就是说，除了最后的左右端口配置，A、B、C 的其他所有配置都相同。

那么同样的，交换机 B、C 也需要做如下配置：

A. 启用交换机的 802.1Q VLAN 功能

同交换机 A

B. 配置环网保护实例

同交换机 A

C. 配置 ERPS 环

环配置：

同交换机 A

左右端口配置：

左右端口的角色均选择为 Normal 即可，如下图所示：

到这里就完成了对交换机 B、C 的配置。

配置完成后，将三台交换机按照设定的端口两两连接起来，就组建好了一个环网。这种单环网络在实际应用中最为常见，配置起来也比较简单，对于具有 N 个节点的单环网络，只需配置 1 个 RPL Owner 节点和 N-1 个普通节点即可。

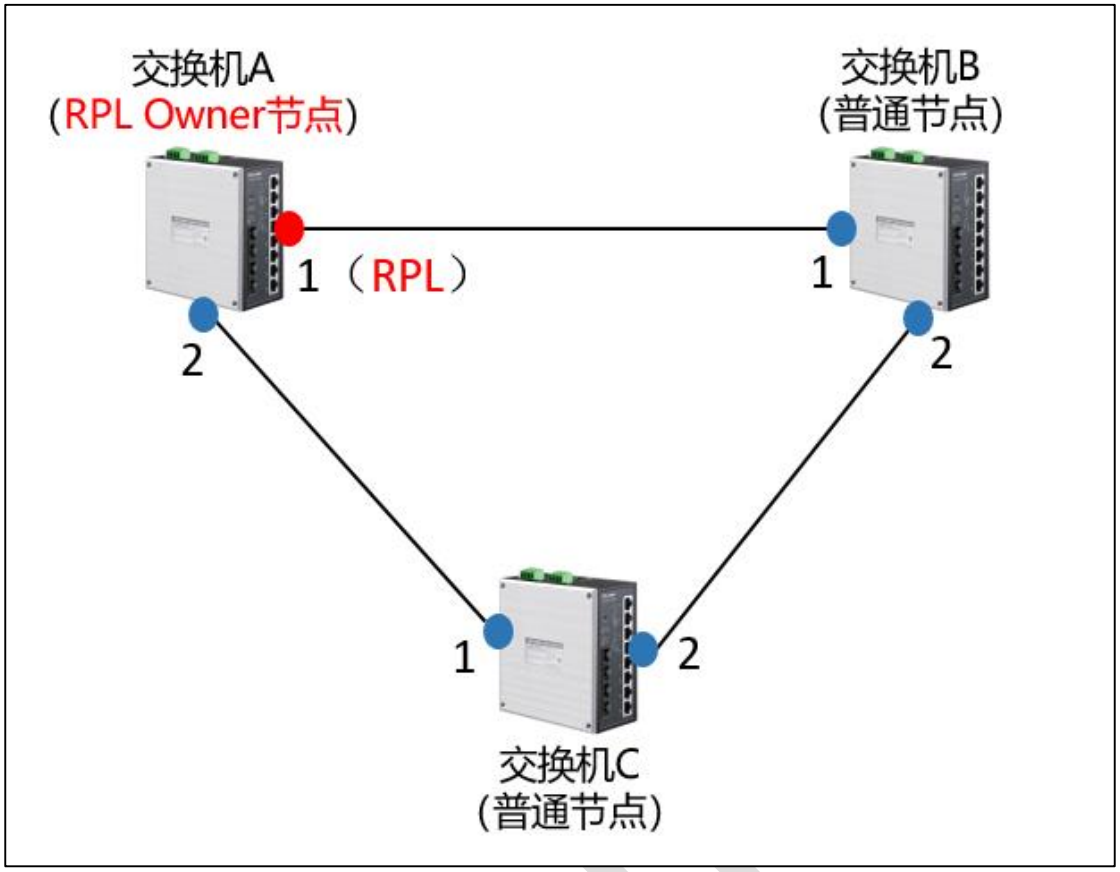
13.2 TP-RING 单环环网配置指南

13.2.1 应用介绍

TL-SG5412 工业级新增了 TP-RING 功能，受到客户的广泛关注。TP-RING 是 TP-LINK 研发的环网协议，支持单环、多环组网，支持快速环网（故障自愈时间<20ms），在实现链路冗余备份的同时，有效避免网络环路、广播风暴等现象，保护工作数据，提高网络可靠性。正常工作时，RPL 端口阻塞所在链路，防止网络环路；当环网中某条链路出现异常断开时，异常节点会发包通知 RPL Owner 节点，于是 RPL 端口放开，使所在链路恢复正常通信，保障整个网络通信不中断。一个环网中，有且仅有一个 RPL Owner 节点

13.2.2 需求介绍

某工业环境使用交换机组环网，保障任何一台交换机故障都不会影响业务的转发，使用 ERPS 组环网拓扑如下：



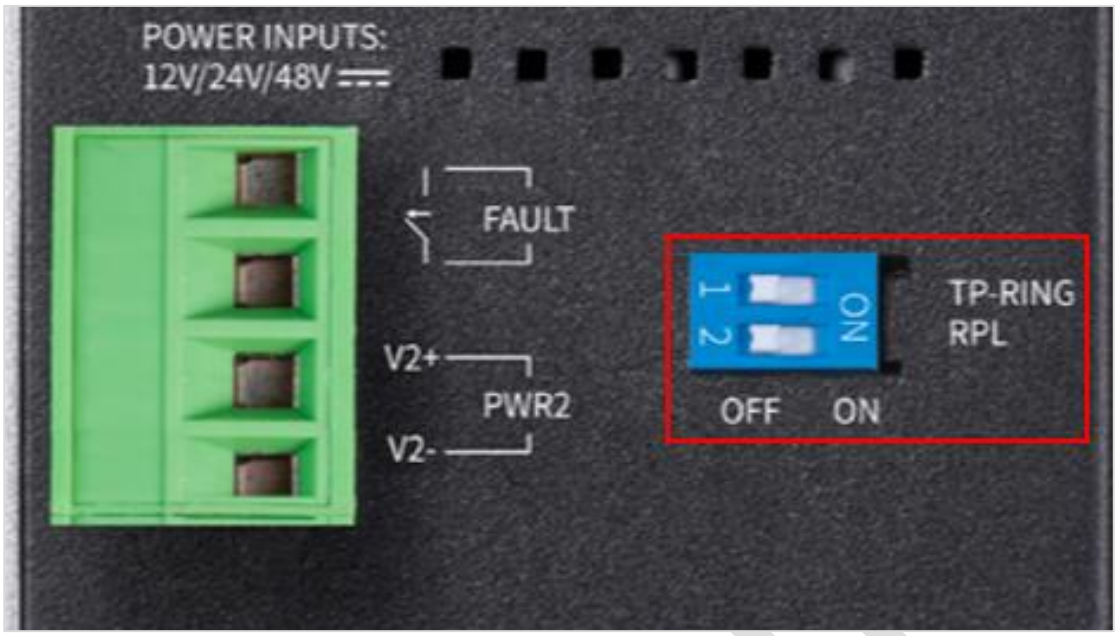
13.2.3 设置方法

1、通过拨码开关快速配置（以 TL-SG5412 工业级为例）

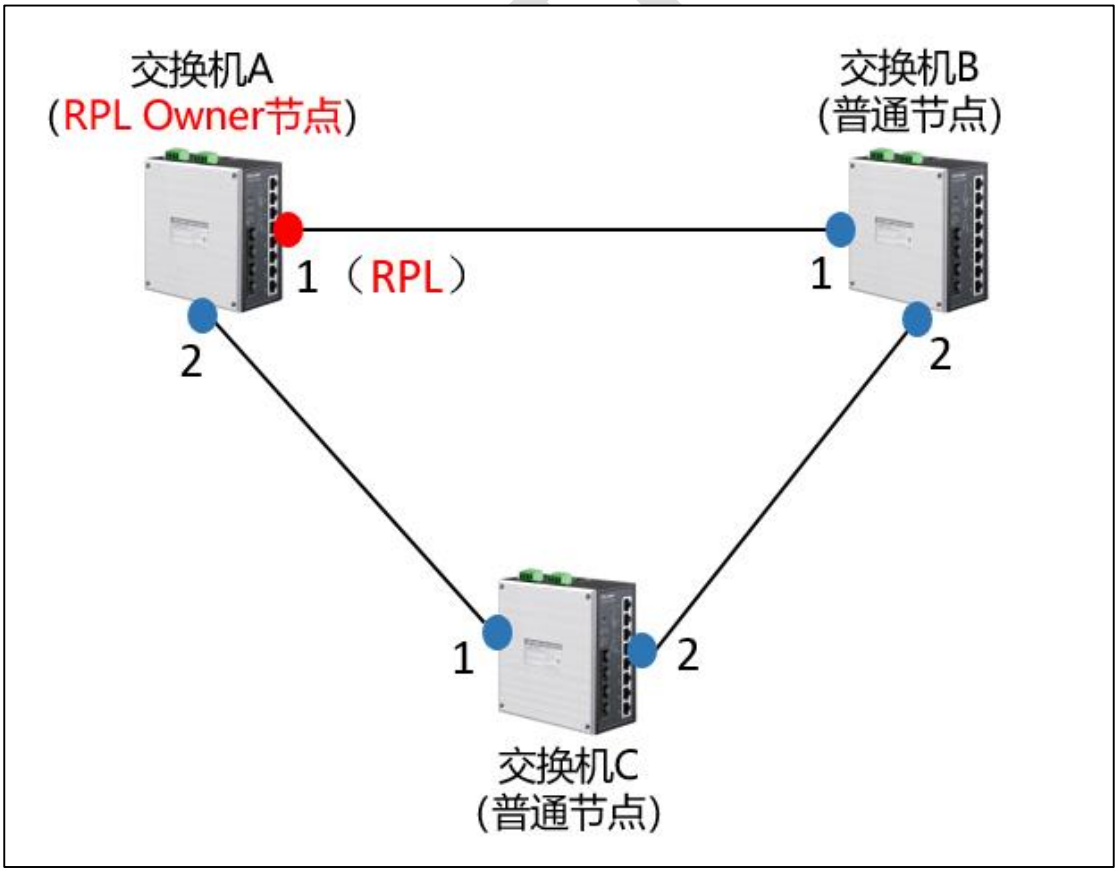
TL-SG5412 工业级交换机有两个拨码开关：

TP-RING：默认关闭，开启后，交换机开启 TP-RING 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 端口。



那么对于这样一个环网拓扑：



只需做如下操作：

(1) 交换机 A 将 TP-RING 开关和 RPL 开关都拨到 ON；

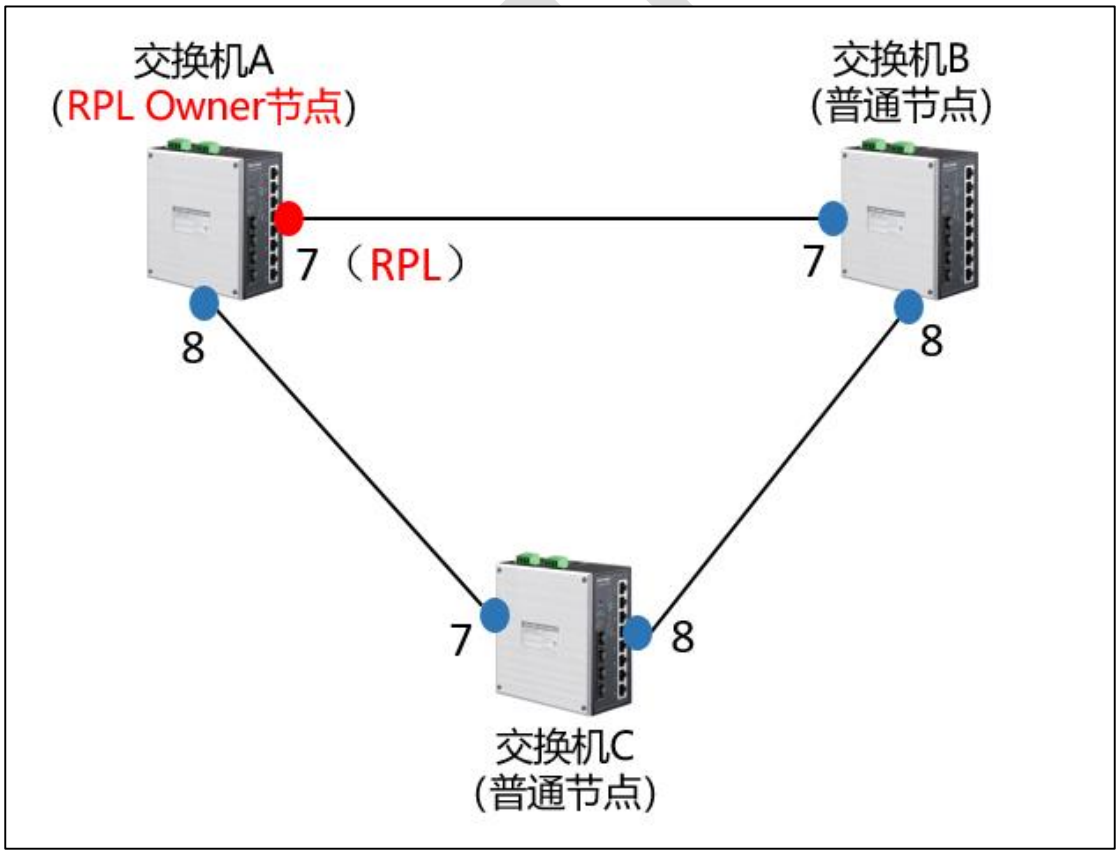
(2) 交换机 B、C 将 TP-RING 开关拨到 ON。

(3) 将三台交换机的端口 1、2 按照拓扑连接起来。

需要注意的是，使用拨码开关来配置环网时，只能使用端口 1、2 来组建环网，且只能配置端口 1 为 RPL Owner 端口。如果需要使用其他的端口来组建环网，比如使用光口来组建光纤环网，那么就必须采用 WEB 页面配置的方法。

2、WEB 页面配置

使用 WEB 页面配置时，可以任意指定所用端口，拓扑示意如下：

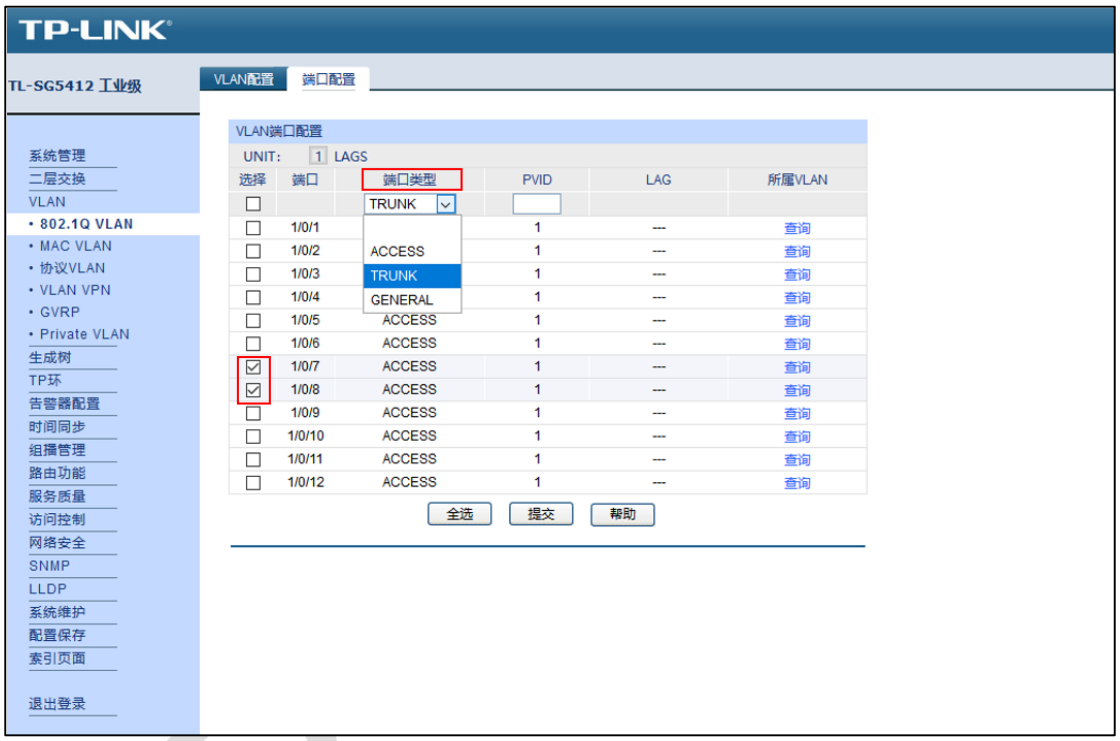


角色分类：交换机 A 为 RPL Owner 节点，交换机 B、C 为普通节点。

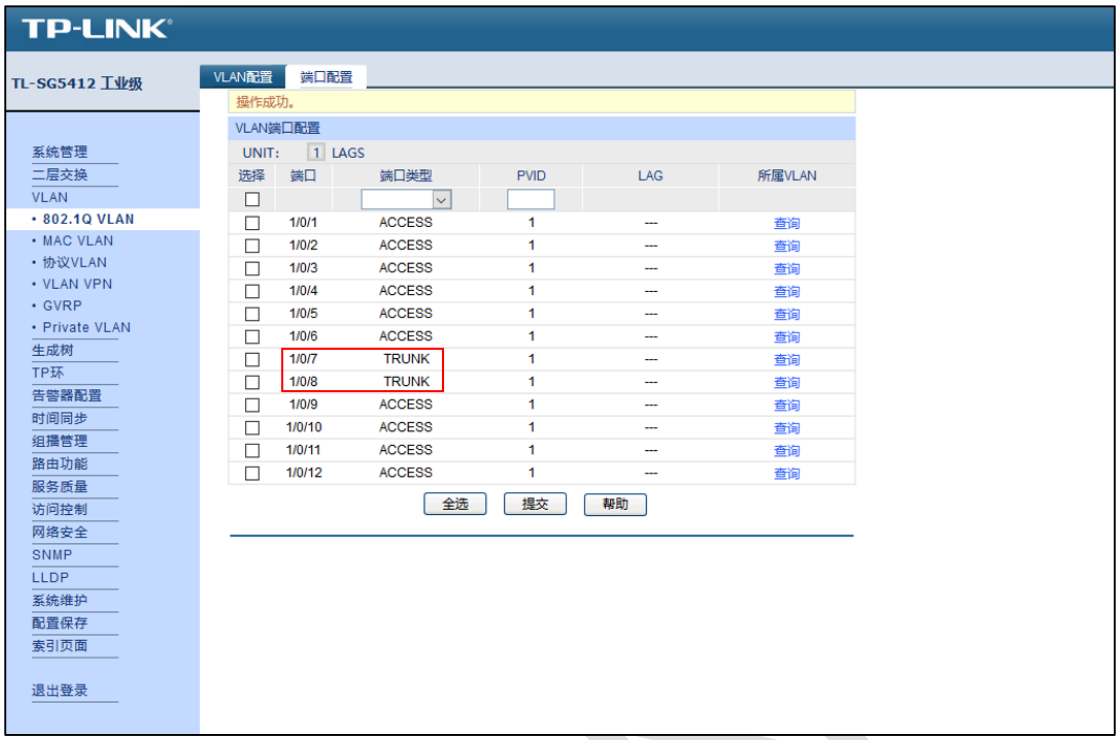
交换机 A 配置

（1）配置相应端口类型为 TRUNK

依次点击<VLAN>→<802.1Q VLAN>→<端口配置>，选中 7、8 两个端口，选择端口类型为 TRUNK，如下图所示：

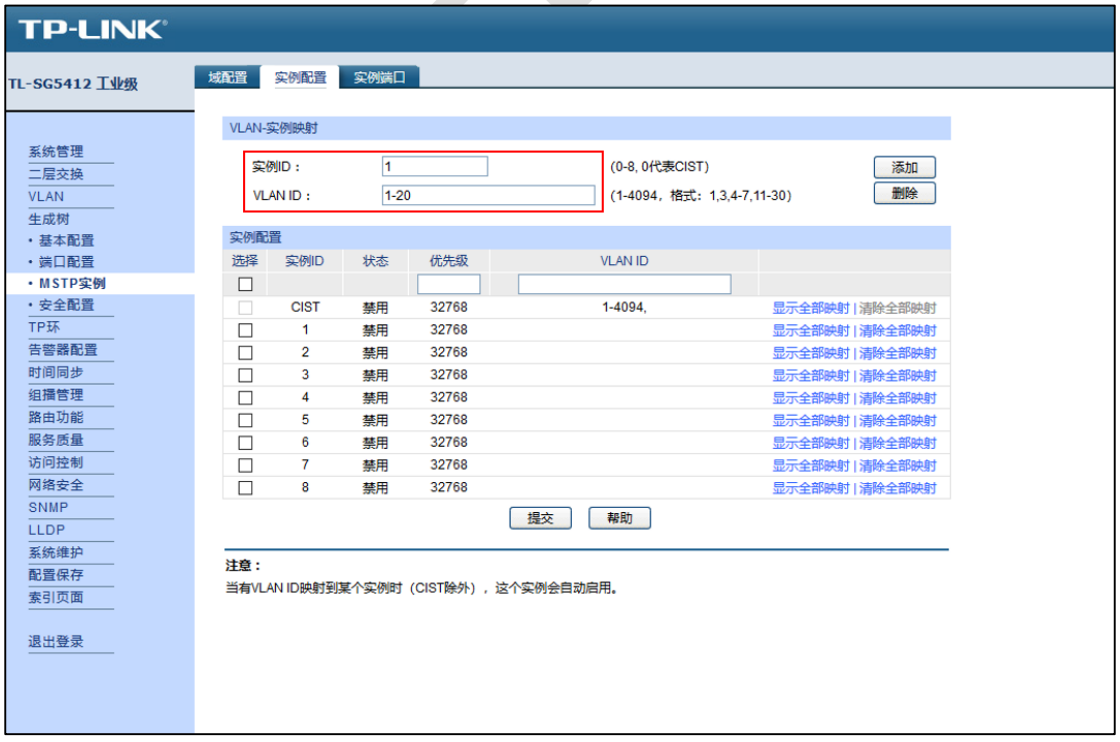


点击<提交>后，页面显示如下图所示：

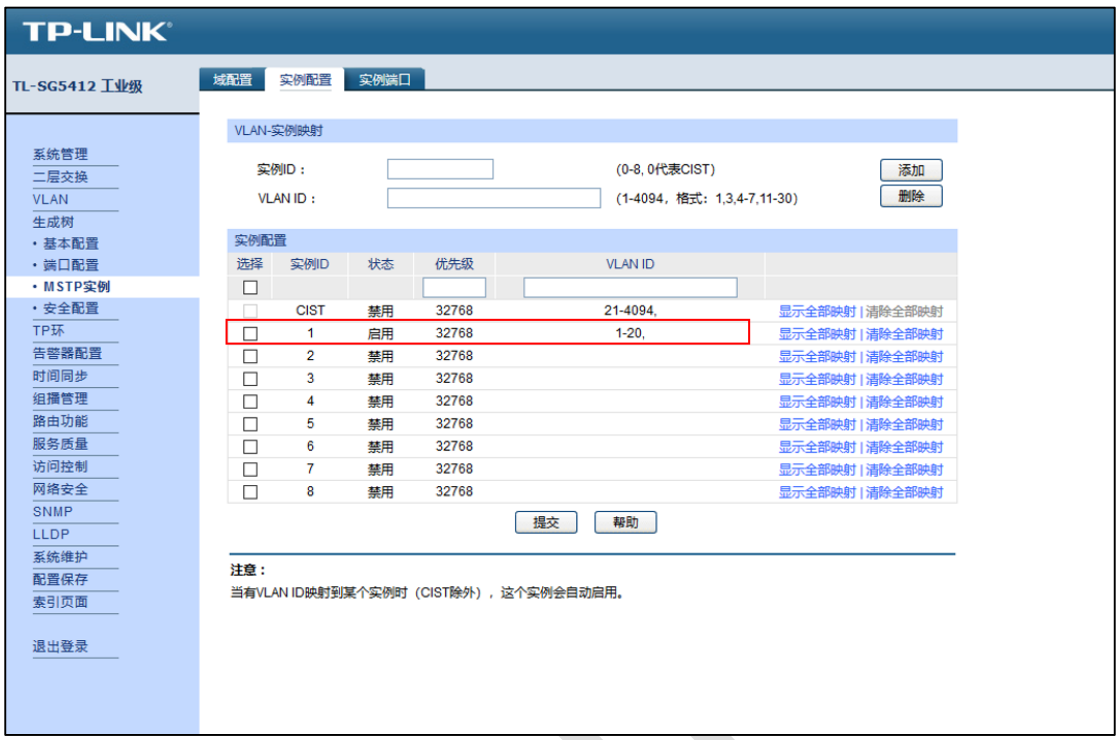


（2）配置环网保护实例

依次点击<生成树>→<MSTP 实例>→<实例配置>，设置实例 ID，本例设置为 1，设置需要保护的 VLAN 范围，本例设置为 1-20，如下图所示：



点击<添加>后，页面显示如下图所示：



这里，就完成了保护实例的配置，需要注意的是，设置的 VLAN ID 范围，需要包含所有数据 VLAN 和协议 VLAN，比如数据通信用到了 VLAN 1-5，TP 环的协议 VLAN 设置为 10，那么这里 VLAN ID 范围可以设置为 1-10。协议 VLAN 在 TP 环配置中会讲到。

（3）配置 ERPS 环

环配置：

依次点击<TP 环>→<环配置>→<全局配置>，如下图所示：

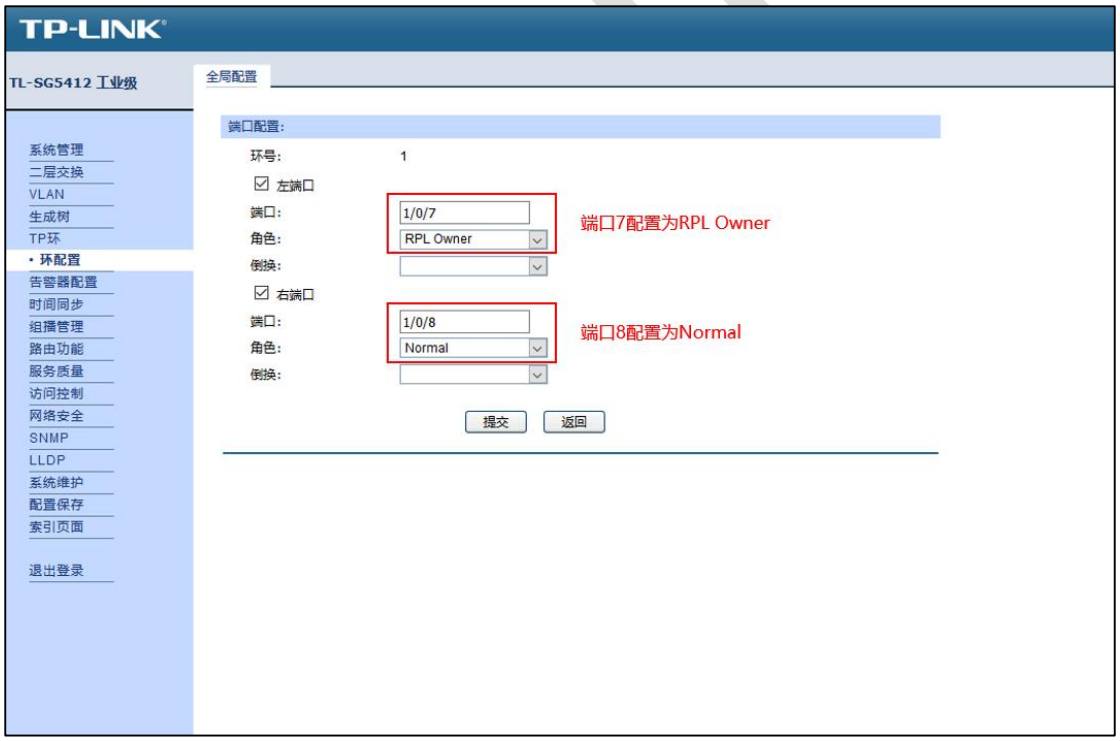
配置好红框标出的项目，其他参数留空或者保持默认即可。

点击<创建>后，如下图所示：

左右端口配置：

点击下图中红框标出的<端口>：

进入左右端口配置，将端口 7 配置为 RPL Owner，如下图所示：



点击<提交>，则完成了左右端口配置。

到这里，就完成了对交换机 A 的配置，别忘了点击<配置保存>。

交换机 B.C 配置

交换机 B、C 与交换机 A 的唯一区别就是，B 和 C 不需要设置 RPL Owner。也就是说，除了最后的左右端口配置，A、B、C 的其他所有配置都相同。

那么同样的，交换机 B、C 也需要做如下配置：

（1）配置相应端口为 TRUNK

同交换机 A

（2）配置环网保护实例

同交换机 A

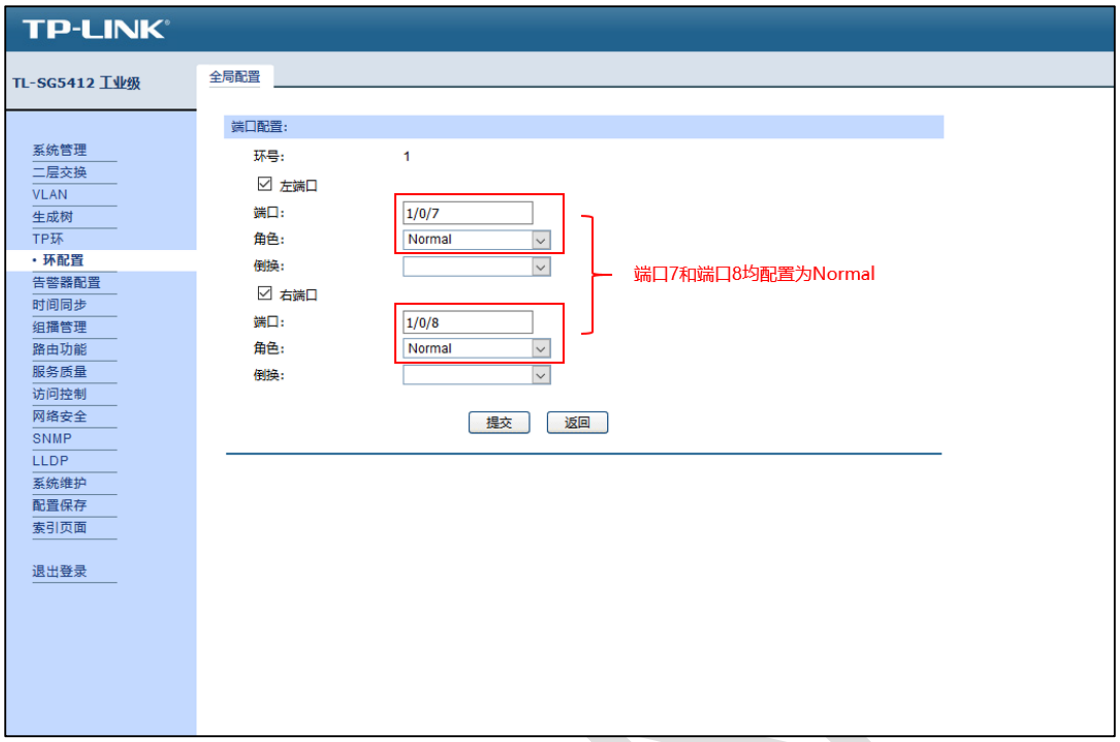
（3）配置 TP 环

1） 环配置：

同交换机 A

2） 左右端口配置：

左右端口的角色均选择为 Normal 即可。



到这里就完成了对交换机 B、C 的配置。

配置完成后，将三台交换机按照设定的端口两两连接起来，就组建好了一个环网。这种单环网络在实际应用中最为常见，配置起来也比较简单，对于具有 N 个节点的单环网络，只需配置 1 个 RPL Owner 节点和 N-1 个普通节点即可。

第14章 其它功能

14.1 三层网管交换机连云配置指南

14.1.1 应用介绍

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：https://www.tp-link.com.cn/act-smbcloud-devices2

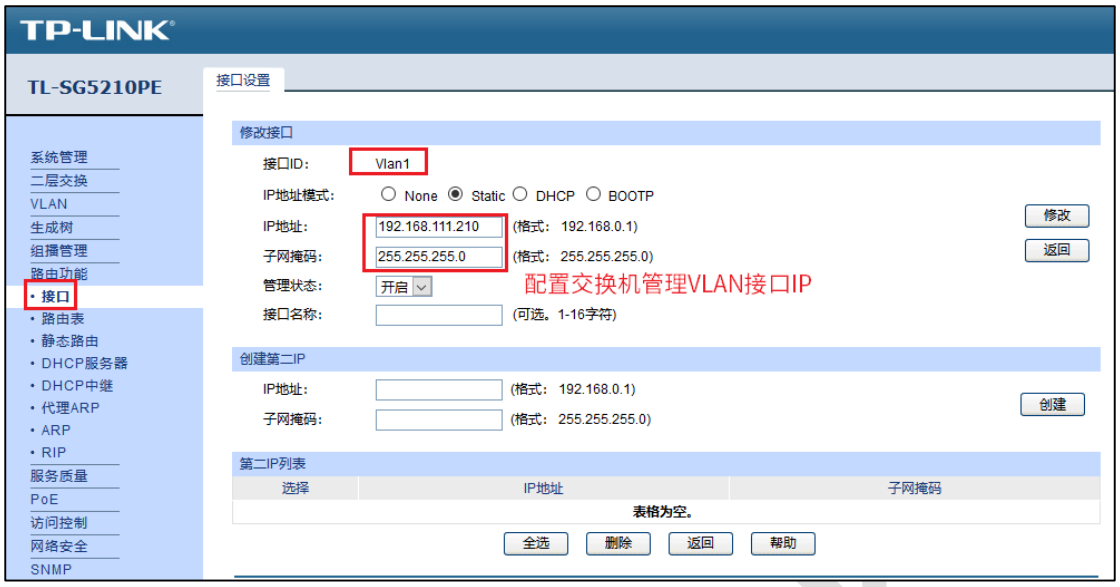
本文介绍三层网管交换机连接商云的配置方法。

14.1.2 需求介绍

某公司三层网管交换机需要连接商用网络云平台，通过云平台管理。

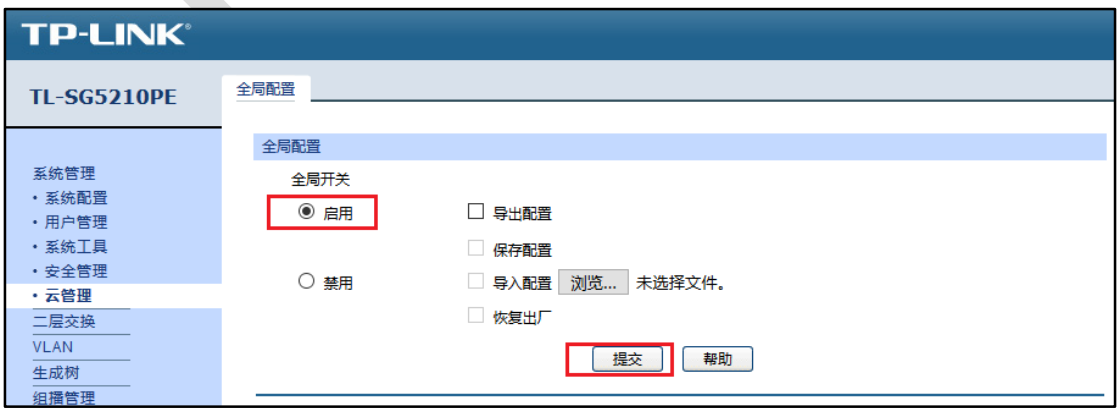
14.1.3 设置方法

在交换机界面，点击“路由功能”-“接口”，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：



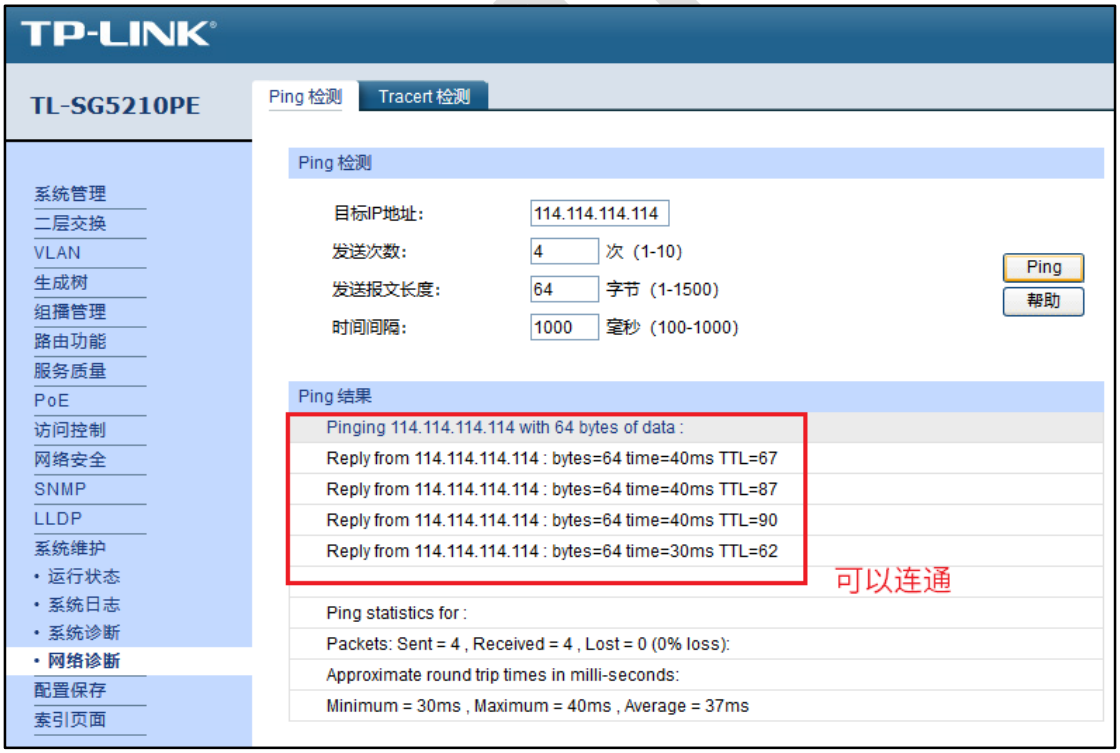
点击“系统配置”-“DNS 配置”，确认设备的 DNS 服务器地址填写正确，交换机默认填写了两条 DNS 地址：

点击“系统管理”-“云管理”，启用交换机的云管理功能，并选择 TP-LINK 商云管理：

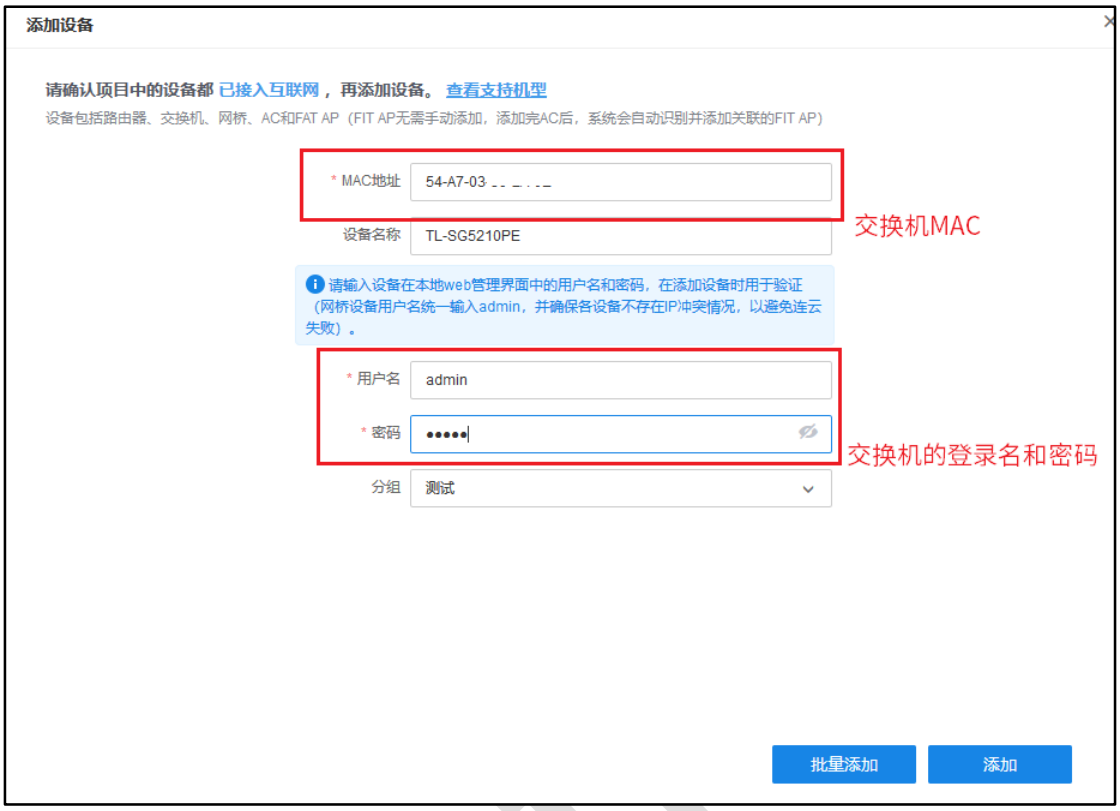


点击“路由功能”-”静态路由”，配置一条全 0 的静态路由下一跳指向前端路由器 LAN 接口：

点击“系统维护”-“网络诊断”-“Ping 检测”，检查设备是否可以正常联网，一般 Ping DNS 服务器：



登陆 TP-LINK 商用网络云平台：https://smbcloud.tp-link.com.cn/,登陆 TP-LINK ID 账号，点击“设备列表”-“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：



至此，设备已经可以正常上云，点击远程管理即可管理设备。

14.2 二层 Web 网管交换机连云配置指南

14.2.1 应用介绍

TP-LINK 新出的 3 系列交换机都支持连接 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：https://www.tp-link.com.cn/act-smbcloud-devices2

本文介绍 3 系列交换机连接商云的配置方法。

14.2.2 需求介绍

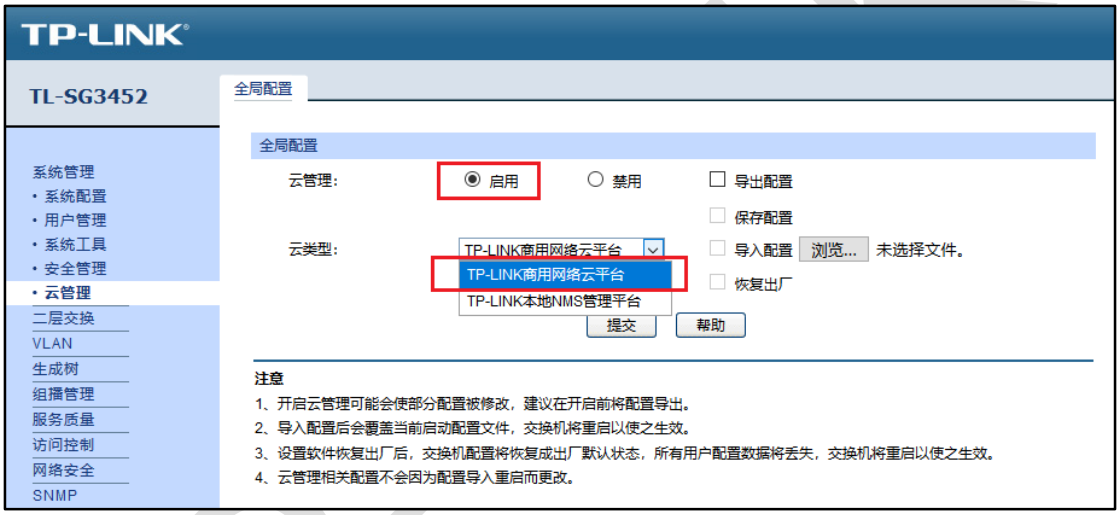
某公司二层网管交换机需要连接商用网络云平台，通过云平台管理。

14.2.3 设置方法

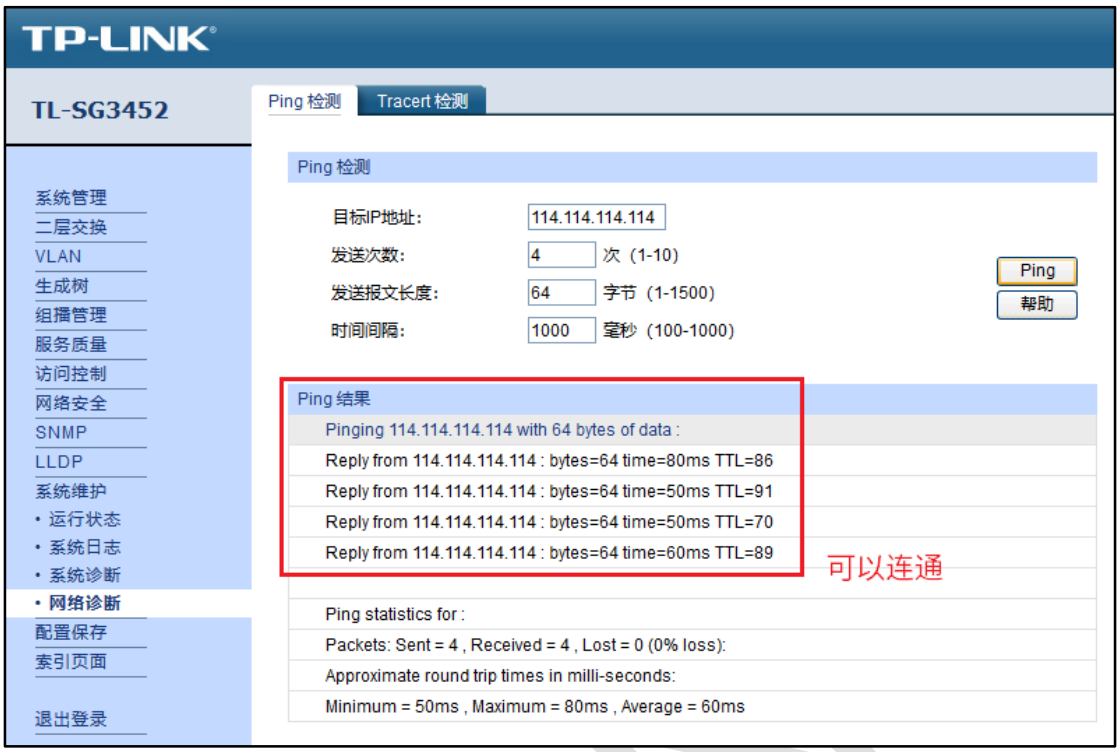
在交换机界面，点击“系统配置”-“管理 IP”，配置交换机设备的 IP 地址和默认网关：

点击“系统配置”-“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：

点击“系统管理”-“云管理”，启用交换机的云管理功能，并选择 TP-LINK 商云管理：



点击“系统维护”-“网络诊断”-“Ping 检测”，检查设备是否可以正常联网，一般 Ping DNS 服务器：



登陆 TP-LINK 商用网络云平台：https://smbcloud.tp-link.com.cn/,登陆 TP-LINK ID 账号，点击“设备列表”-“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：

至此，设备已经可以正常上云，点击远程管理即可管理设备。