AQUAM8124TSN/AQUAM8624TSN

工业以太网交换机 Web 操作手册

出版日期：2022 年 8 月

版　　本：V1.0

KYLAND

免责声明

北京东土科技股份有限公司竭力使本手册中的信息尽可能准确、最新。然而本公司不能保证本手册完全没有任何技术错误或笔误，并保留在未通知用户的情况下对其修改的权利。

出版：北京东土科技股份有限公司

网址：http://www.kyland.com.cn

客户服务热线：010-88796676

传真：010-88796678

邮箱：services@kyland.com.cn

目录

前言

本手册主要介绍了 Aquam8124TSN/Aquam8624TSN 系列工业以太网交换机的访问方式和软件特性，并通过 Web 界面详细介绍了该系列交换机的配置使用方法。

内容组织

本手册主要从以下内容进行介绍：

模块	特性说明
1、产品介绍	➢ 概述 ➢ 软件特性
2、交换机访问方式	➢ 视图类型简介 ➢ Console 口访问 ➢ Telnet 访问 ➢ Web 访问
3、用户	➢ 用户管理 ➢ 认证方式
4、系统	➢ 基本信息 ➢ 配置管理 ➢ 时间管理 ➢ PTP ➢ 软件升级（本地升级、FTP、TFTP 升级） ➢ 软件版本激活 ➢ 语言包升级 ➢ 重启 ➢ 关于
5、服务	➢ SSL 配置 ➢ SNMP v1/v2c/v3 ➢ SSH 配置 ➢ TACACS+配置 ➢ RADIUS 配置

	➢ DNS ➢ RMON
6、告警	
7、功能管理	➢ 端口配置 ➢ VLAN ➢ IP 配置 ➢ 端口聚合 ➢ 冗余 ➢ ARP 配置 ➢ ACL 配置 ➢ MAC 表配置 ➢ POE ➢ IGMP snooping ➢ DHCP 配置 ➢ IEEE802.1X 配置 ➢ GMRP ➢ 静态路由 ➢ QoS 配置
8、环路保护	➢ 环路保护
9、TSN	➢ TSN
10、NETCONF	➢ NETCONF
11、诊断	➢ 日志 ➢ 端口镜像 ➢ LLDP 信息 ➢ 跟踪路由 ➢ Ping ➢ IP Source Guard

本手册约定

1、文本格式约定

格式	说明
< >	“< >”中内容表示按钮名，如“单击<应用>按钮”。
[ ]	“[ ]”中内容表示窗口名、菜单名，如点击“[文件]”菜单项。
{ }	“{ }”中内容表示一个组合，如“{IP 地址，MAC 地址 }”表示 IP 地址和 MAC 地址是一个组合，可以一起配置、显示。
→	多级菜单用“→”隔开，如“开始→程序→附件”表示[开始]菜单下的[程序]子菜单下的[附件]菜单项。
/	从两个或者多个中间选一个用“/”隔开，如“加/减”表示加或者减。
~	表示范围，如“1~255”表示从 1 到 255 的范围。

2、命令行格式约定

格式	说明
粗体	命令行关键字，在 CLI 配置中照输的部分，如“**show version**”显示交换机的软件版本。
斜体	命令行参数，必须由实际值进行代替的部分，如“**show vlan** *vlan id*”显示 VLAN 号为 vlan id 的 VLAN 信息。

3、标志约定

标志	说明
 注意	提醒操作、配置中应注意的事项，对操作内容描述的补充。
 说明	对操作内容进行必要的说明。
 警告	需格外注意的地方，不正确的操作可能会导致数据丢失或者设备损坏。

产品配套资料

Aquam8124TSN/Aquam8624TSN 系列工业以太网交换机的配套资料包括以下内容：

资料名称	内容介绍
Aquam8124TSN/Aquam8624TSN 系列工业以太网交换机硬件安装手册	详细了解 Aquam8124TSN/Aquam8624TSN 外型结构、硬件规格以及安装拆卸方法
Aquam8124TSN/Aquam8624TSN 工业以太网交换机 Web 操作手册	了解交换机软件功能并掌握各功能模块的 Web 配置方法及配置步骤

资料的获取方式

用户可以从以下途径及时获得产品的相关资料和文档：

- 通过本公司网站获取。
- 通过扫设备二维码获取。

1 产品介绍

1.1 概述

Aquam8124TSN/ Aquam8624TSN 是本公司专为轨道交通行业开发的高性能以太网交换机。满足 EN50155、EN50121 等轨道交通行业标准的要求。该系列交换机支持时间敏感网络（TSN）特性，支持 Bypass 掉电直通功能、环网冗余协议，为系统的可靠运行提供了多重保障。

1.2 软件特性

该系列交换机具有丰富的软件特性，可以满足客户的不同需求。

- 冗余协议：DT-Ring、DRP、RSTP/STP、和 MSTP；
- 组播协议：IGMP Snooping、GMRP；
- 交换属性：VLAN、GVRP、QoS、ARP；
- 带宽管理：端口静态聚合、LACP、端口流量配置和广播风暴抑制；
- 安全管理： 用户管理、访问管理、SSH、SSL、TACACS+、RADIUS、IEEE802.1X、ACL、IP Source Guard 和端口隔离；
- 同步协议：SNTP、NTP；
- 设备管理：软件升级，配置文件上传/下载、日志记录与上传；
- 设备诊断：端口镜像、LLDP；
- 告警功能：电源告警、端口告警、环告警、高温告警、低温告警、端口流量告警’和 IP/MAC 地址冲突告警；
- 网络管理：支持 CLI、Telnet、Web、Kyvision 网管软件管理、DHCP 和 SNMPv1/v2c/v3 网络监控；
- ……

2 交换机的访问方式

支持几种方式访问交换机：

- Console 口访问；
- Telnet/SSH 访问；
- Web 浏览器访问；
- Kyvision 管理软件访问；

Kyvision 是东土公司自己开发的网络管理软件，使用方法请参阅相关用户手册。

2.1 视图类型简介

Console 口和 Telnet 登陆到 CLI（command line interface）时，通过不同命令可以进入不同视图或在不同视图下进行切换，如表 1 所示；

表 1 各种视图转换

视图显示	视图类型	视图功能	视图切换
SWITCH #	特权用户配置模式	查看最近使用的历史指令； 查看软件版本； 发送 ping 测试数据包查看响应信息； 上传/下载配置文件； 恢复默认配置； 重启设备； 保存当前配置； 显示设备当前的配置信息； 软件升级	“**configure terminal**”从特权用户配置模式进入全局配置模式； “**exit**”返回到上级视图即一般用户配置模式
SWITCH（config）#	全局配置模式	对交换机进行各个功能模块配置	“**exit**”或者“**end**”返回特权用户配置模式

使用命令行配置交换机时，可以用“?”来获取指令帮助，在帮助信息的提示列表中有不同格式的参数描述：例如<1-255>指数值范围；<xx:xx:xx:xx:xx:xx>指 MAC 地址配置格式；<word31>指字符串范围为 1~31。除此之外也可以使用↑和↓调用最近使用过的指令。

2.2 Console 口访问

可以使用 Windows 系统的超级终端或者其他支持串口连接的软件如：HTT3.3，通过 Console 口访问交换机。下面以超级终端为例介绍怎样通过 Console 口访问到交换机。

可以使用 Windows 系统的超级终端或者其他支持串口连接的软件如：HTT3.3，通过 Console 口访问交换机。下面以超级终端为例介绍怎样通过 Console 口访问到交换机。

1、用 M12-A-4P-M 串口线连接 PC 机的串行通信口和交换机的 Console 口；

2、从 Windows 桌面打开超级终端，[开始]→[程序]→[附件]→[通讯]→[超级终端]，如图 1 所示；

图 1 超级终端

3、建立一个新连接“Switch”，如图 2；

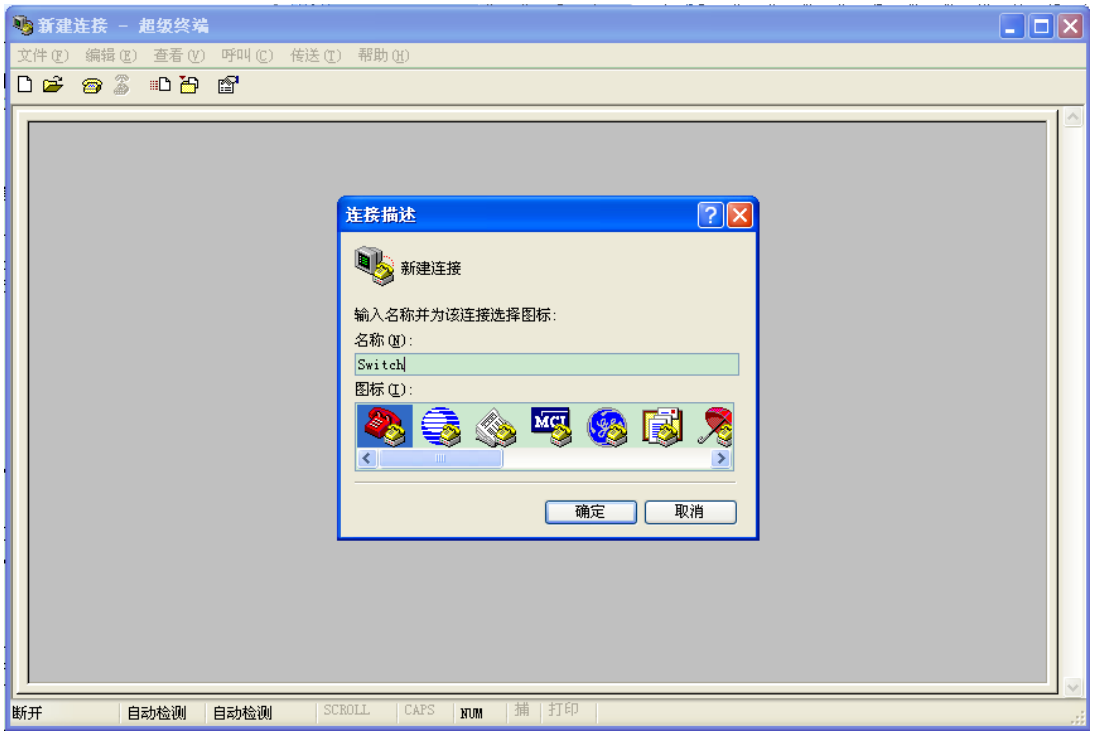


图 2 新建连接

4、选择正确的通信端口进行连接，如图 3 所示；

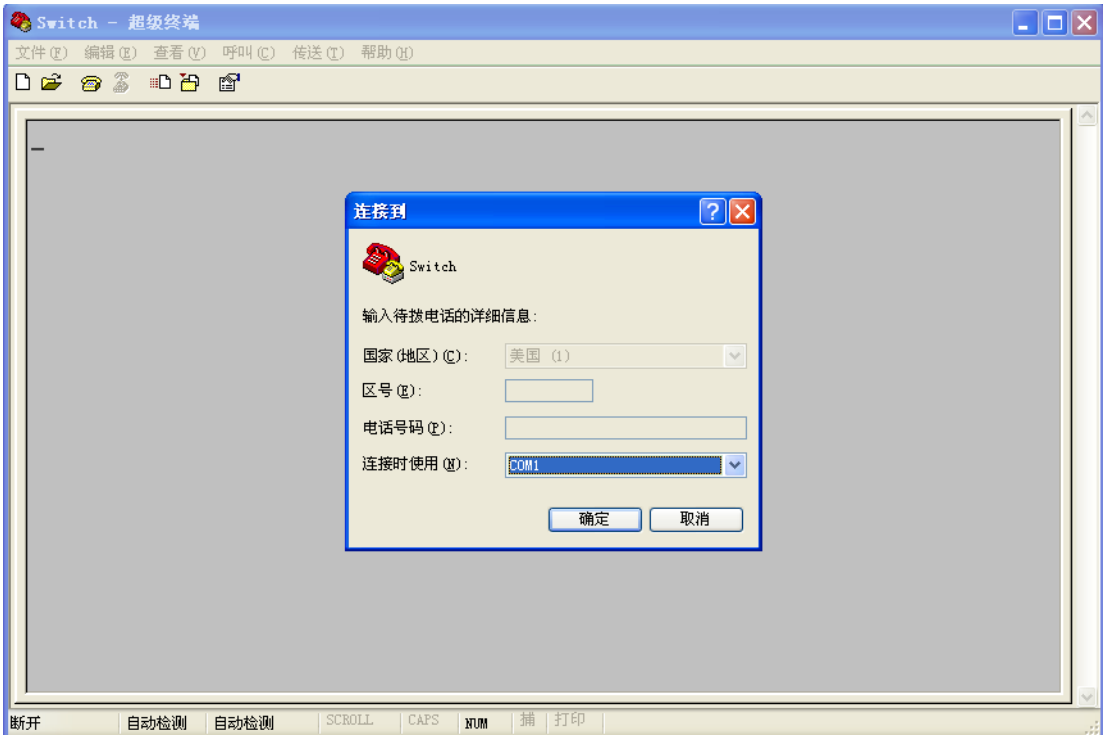


图 3 选择正确的通信端口

说明：

如果不清楚当前设备的通信端口，可以右击[我的电脑]→[属性]→[硬件]→[设备管理器]→[端口]查

看 Console 口使用的通信端口。

5、串口参数配置如图 4 所示，每秒位数（波特率）：115200；数据位：8；奇偶校验：无；停止位：1；数据流控制：无；

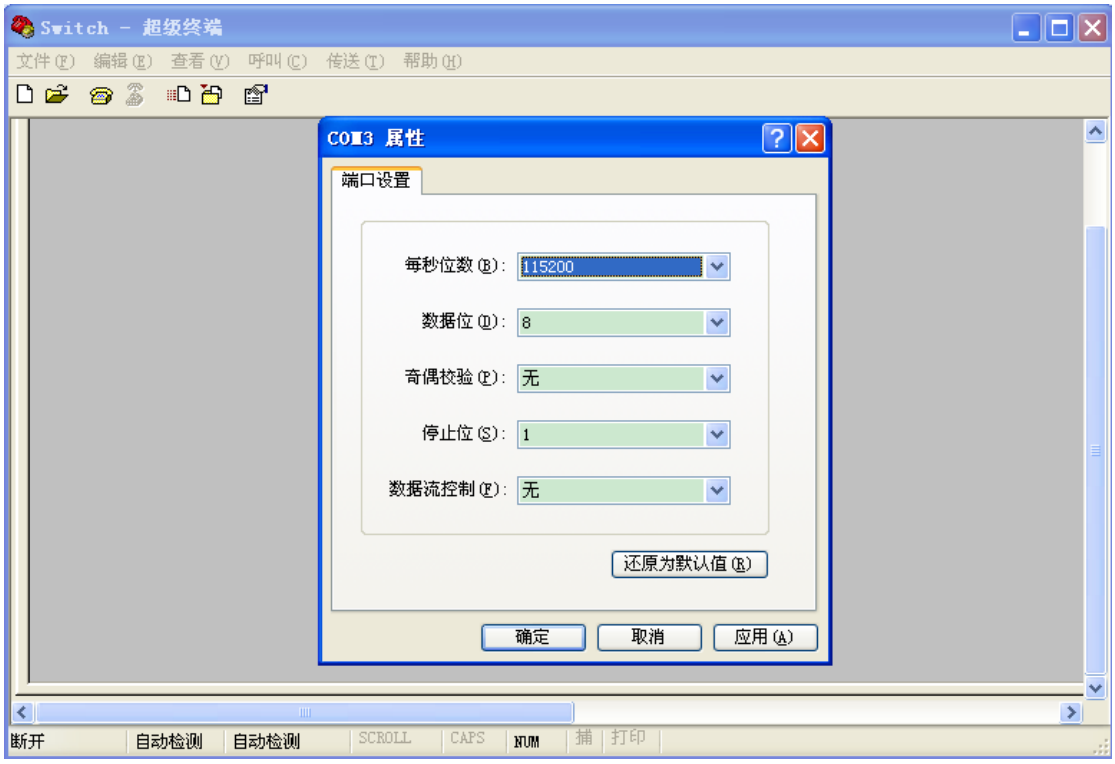


图 4 属性配置

6、点击<确定>按钮，可以成功进入交换机的命令行界面，输入默认用户名“admin”和密码“123”；也可输入其他已创建的用户名和密码，进入特权用户配置模式，如图 5 所示；

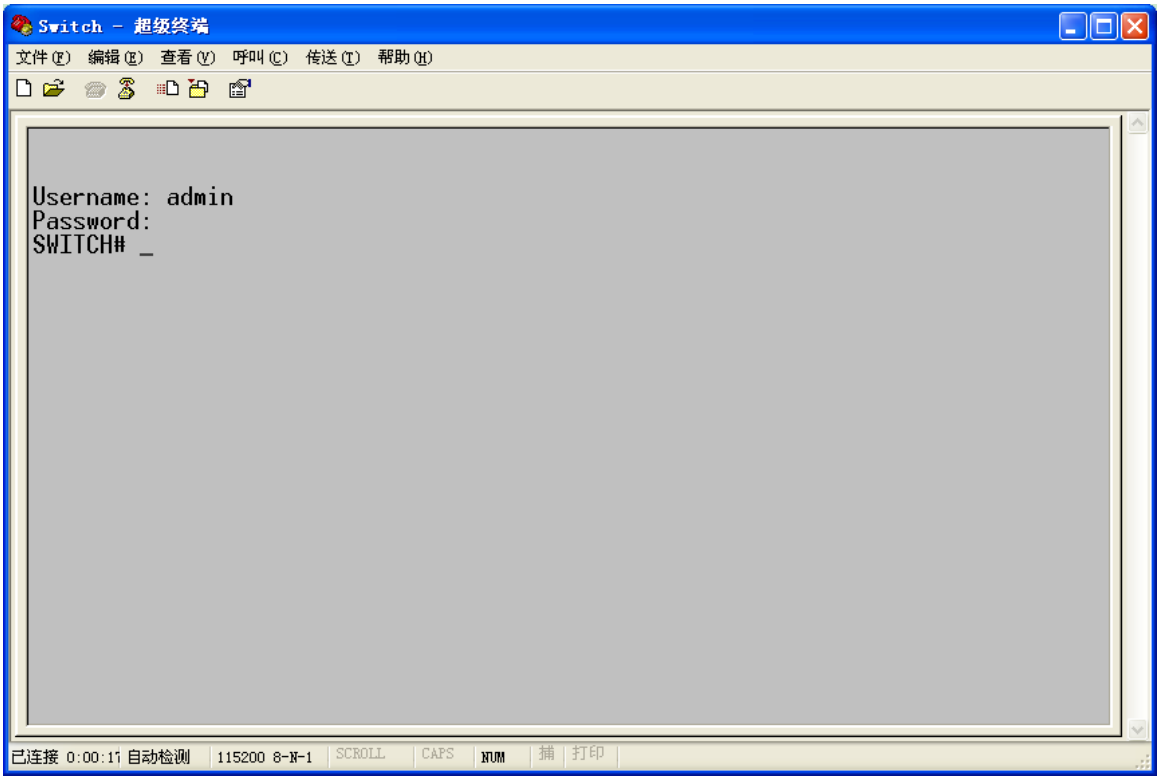


图 5 CLI 界面

2.3 Telnet 访问

Telnet 登陆要求 PC 机和交换机能够正常通信。

1、在运行对话框中输入“**telnet** *IP 地址*”，东土公司交换机的默认 IP 地址为“192.168.0.2”，如图 6 所示；

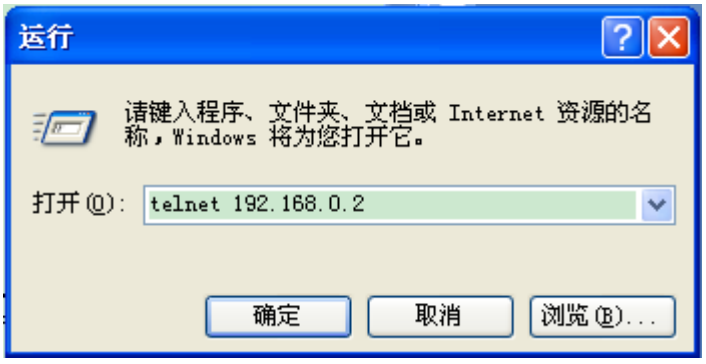


图 6 Telnet 访问

说明：

如果不清楚当前交换机的 IP 地址，请参考“7.3 IP 配置”章节获取 IP 地址。

2、Telnet 界面中输入默认用户名”admin”和密码”123”；也可输入其他已创建的用户名和

密码，进入交换机命令行界面，如图 7 所示；

图 7 Telnet 界面

2.4 Web 访问

Web 登陆要求 PC 机和交换机能够正常通信。

说明：

推荐使用 IE8.0 或以上版本浏览器，使 Web 管理界面更加友好。

1、在浏览器地址栏中输入“*IP 地址*”，出现登陆对话框如图 8 所示，输入默认用户名”admin”和密码”123”，也可输入其他已创建的用户名和密码，点击<确定>按钮；

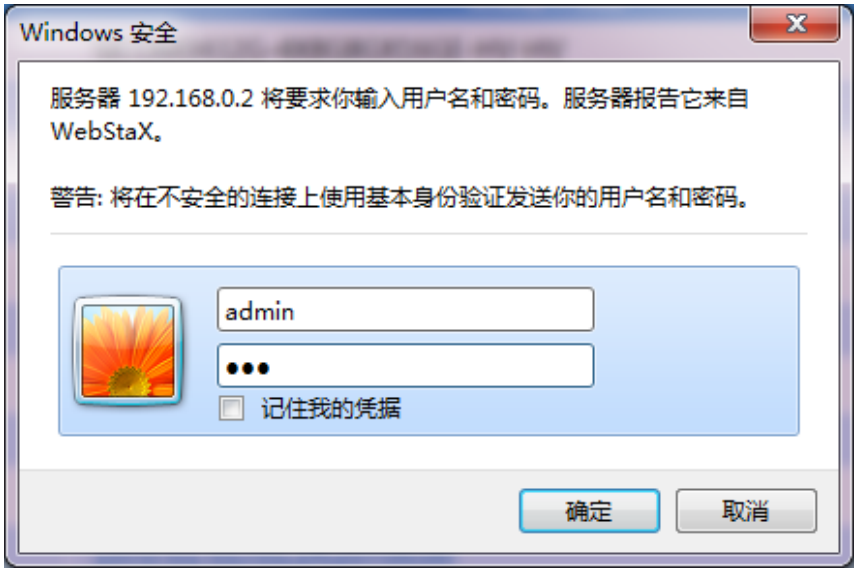


图 8 Web 登陆

进入主界面，在右上角可以切换到英文或中文 Web 操作界面，出厂配置默认为中文界面。

说明：

如果不清楚当前交换机的 IP 地址，请参考“7.3 IP 配置”章节获取 IP 地址。

2、此时成功登陆到交换机页面，左边是配置导航树，如图 9 所示；

图 9 Web 界面

点击导航树中的菜单，可以展开/闭合该菜单项。点击 主页 可以链接到图 9 所示的 Web 首界面，即任何情况下点击该图标可以切换到 Web 首界面；点击  退出 Web 操作界面。

3 用户

3.1 用户管理

3.1.1 介绍

为了解决非法用户访问交换机造成的安全隐患，本交换机提供了用户分级管理功能，基于不同的用户身份，制定不同的权限，满足用户权限控制的多样化需求。

3.1.2 Web 页面配置

1、创建新用户，如下图所示：

图 10 创建新用户

在用户名编辑栏添加新用户，配置不同的用户等级，最多可以创建 20 个用户。

用户名

配置范围：1~31 字符

功能：配置用户名。

权限等级

配置范围：0~15

功能：配置该用户的权限等级。不同权限等级的用户具有不同的访问权限。

密码

配置范围：0~31 字符

功能：配置用户登陆密码。

2、修改用户配置，如图 11 所示；

图 11 修改用户配置

勾选需要编辑的用户，点击<编辑>按钮可以修改该用户的密码和权限等级。

点击<删除>按钮可删除当前用户。

说明：

- 不能删除默认用户 admin。

3、配置组权限等级，如下图所示：

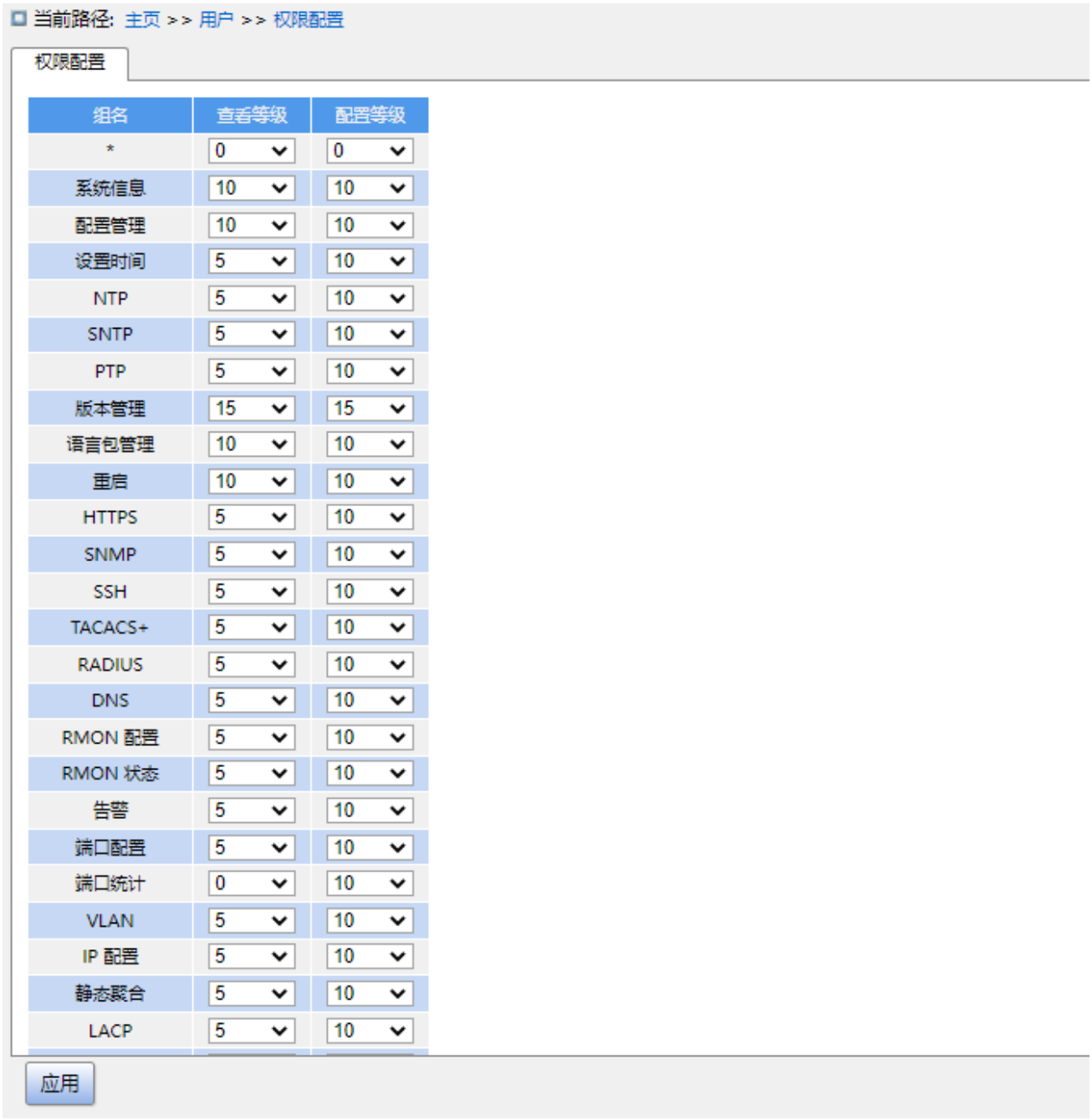


图 12 配置组权限等级

组名

配置选项：所有功能组

功能：选择操作交换机的功能组。

查看等级

配置选项：0-15

默认配置：5

功能：配置当前功能组可被用户查看的级别，不同等级的功能组对用户查看有不同的权限等级要求。

配置等级

配置选项：0-15

默认配置：10

功能：配置当前功能组可被用户操作的级别，不同等级的功能组对用户操作有不同的权限等级要求。

说明：

用户权限等级等于或高于组权限等级时，该用户具有对该组相应的读写权限。

3.2 认证方式

配置访问交换机的登陆方式采用的认证方式和认证顺序，如图 13所示；

图 13 登陆认证配置

服务类型

配置选项：Web/console/telnet/ssh

功能：选择访问交换机的登陆方式。

认证方式 1/认证方式 2/认证方式 3

配置选项：--/Local/RADIUS/TACACS+

默认配置：Local

功能：从左到右依次为**认证方式** 1、**认证方式** 2 和**认证方式** 3。选择登陆认证的顺序，先采用认证方式 1 进行认证；如果认证不通过，再采用认证方式 2 进行认证；如果前两种认证都不通过，则采用认证方式 3 进行认证。

描述：--表示不允许通过该登陆方式访问交换机；Local 表示采用本地创建的用户名和密码进行认证；TACACS+认证表示采用 tacacs 服务器上创建的用户名和密码进行认证；RADIUS 表示采用 radius 服务器上创建的用户名和密码进行认证。

注意：

认证方式 1 和认证方式 2 选择 TACACS+/RADIUS 认证时，建议将方式 3 配置为 Local 认证，确保远端服务器故障时，可以通过本地认证成功访问交换机。

3.3 使能密码权限配置

配置密码权限，如下图所示；

图 14 使能密码权限配置

勾选需要编辑的用户，点击<编辑>按钮可以修改该用户的密码和权限等级。

点击<删除>按钮可删除当前用户。

4 系统

4.1 基本信息

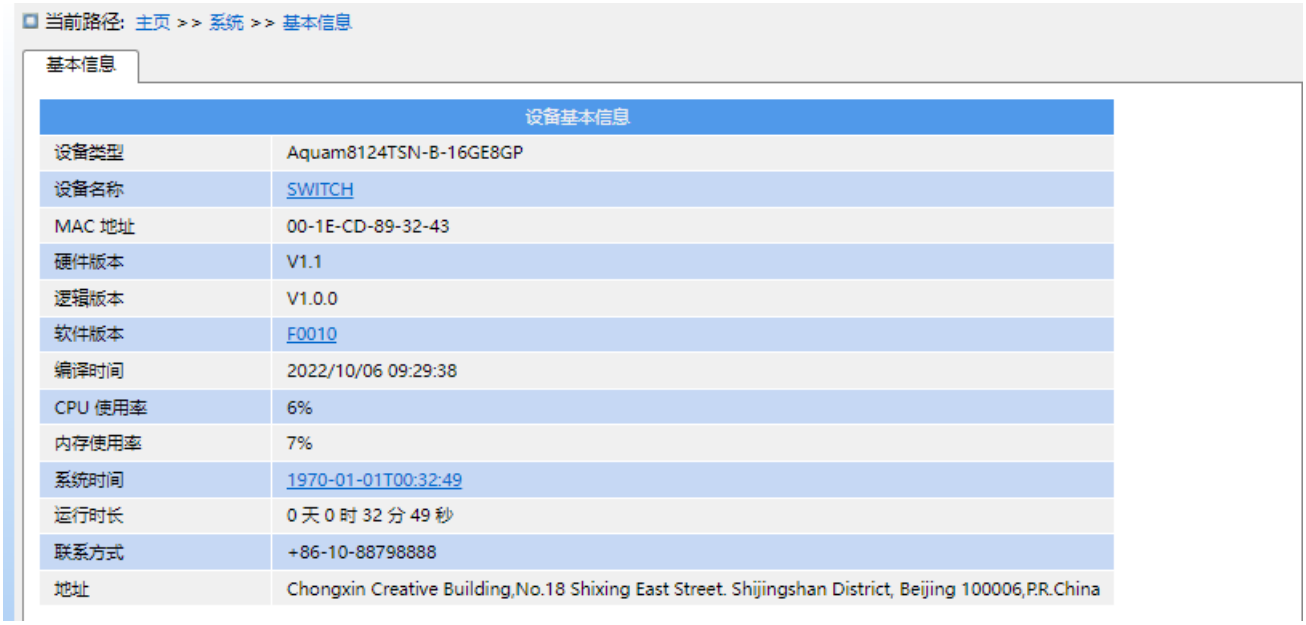


图 15 基本信息

4.2 配置管理

1、保存当前运行配置信息，如下图所示；

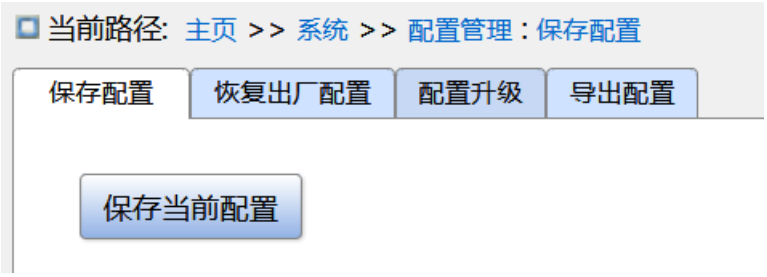


图 16 保存配置

2、恢复出厂配置，如下图所示；

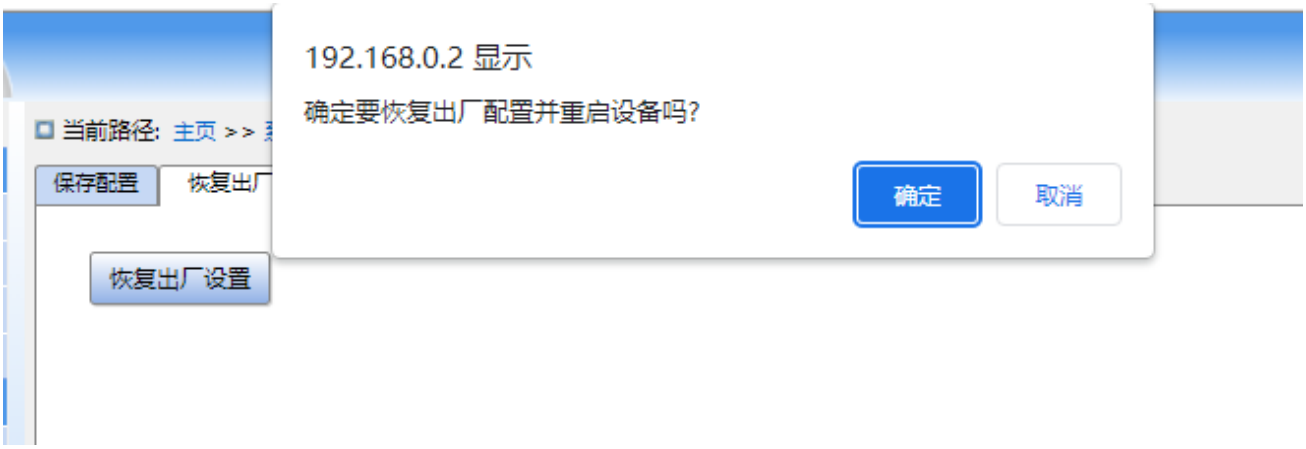


图 17 恢复出厂默认配置

3、导出配置，上传交换机中的文件到本地/服务器，如图 18-图 20 所示；

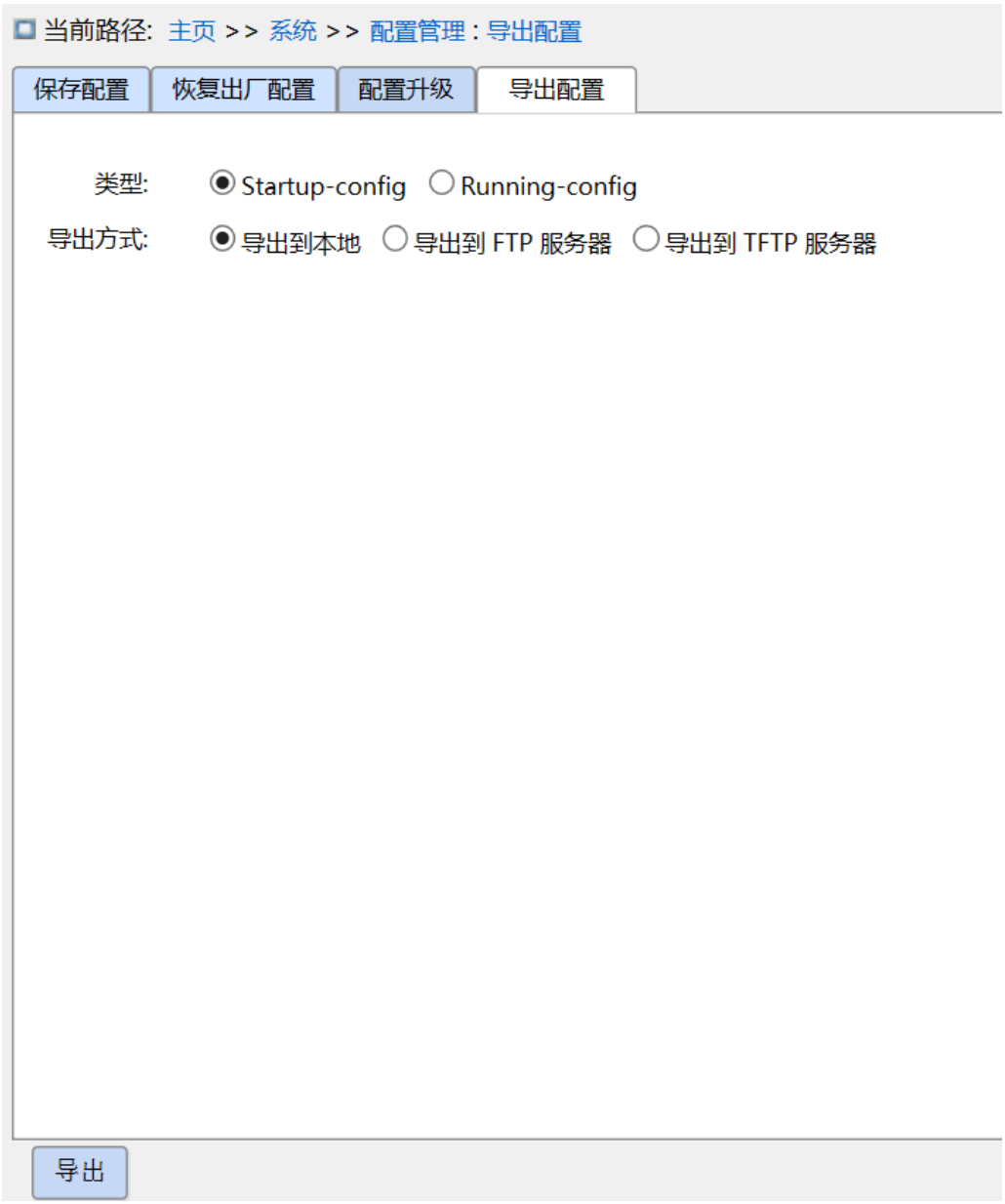


图 18 导出文件-HTTP

图 19 导出文件-FTP

服务器 IP 地址

配置格式：A.B.C.D

描述：输入 FTP 服务器的 IP 地址。

{用户名，用户密码 }

配置范围：{ 1~63 个字符，1~63 个字符}

描述： FTP 服务器创建的用户名和密码。

注意：

- 使用 FTP 传输文件时，需要配置 FTP 用户名、密码和 FTP 服务器 IP 地址；
- 文件传输过程中，FTP 服务器软件应保持运行状态。

图 20 导出文件-TFTP

从设备导出是把交换机中的文件保存到本地/服务器。running-config 文件是交换机当前运行配置文件； startup-config 文件是交换机启动文件。选中一个文件，点击<导出>可以将该文件保存到本地/服务器。

4、配置升级，下载本地/服务器配置文件到交换机中，作为交换机的启动文件，如图 21 -图 23 所示；

图 21 下载配置文件-HTTP

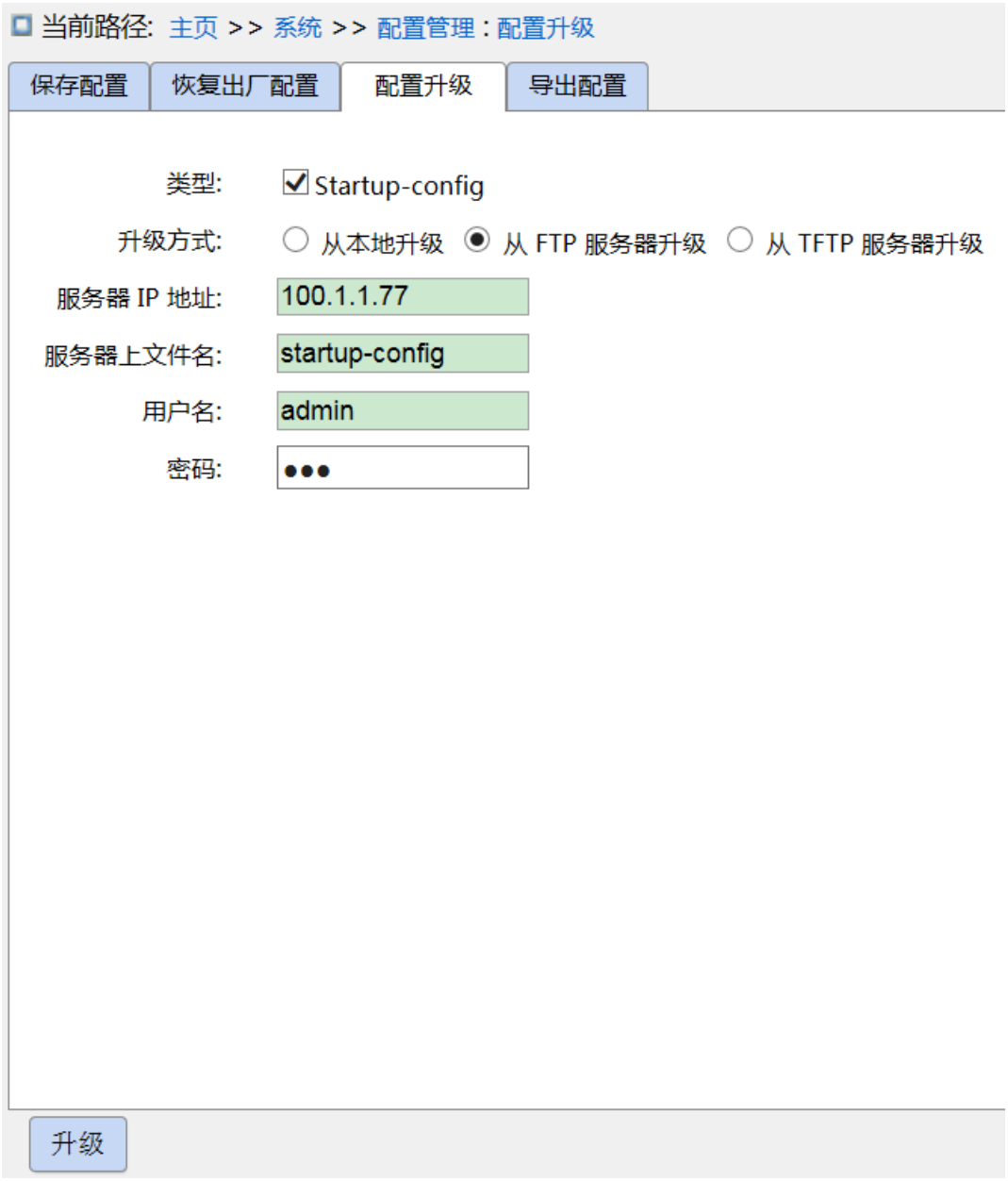


图 22 下载配置文件-FTP

服务器 IP 地址

配置格式：A.B.C.D

描述：输入 FTP 服务器的 IP 地址。

服务器上文件名

配置范围：1~63 个字符

描述：FTP 服务器中配置文件名。

{用户名，用户密码 }

配置范围：{ 1~63 个字符，1~63 个字符}

描述：FTP 服务器创建的用户名和密码。

注意：

- 使用 FTP 传输文件时，需要配置 FTP 用户名、密码和 FTP 服务器 IP 地址、文件名；
- 文件传输过程中， FTP 服务器软件应保持运行状态。

图 23 下载配置文件-TFTP

配置升级是把本地/服务器的配置文件下载到交换机中，作为交换机新的启动文件，将覆盖原有 startup-config 文件。点击<升级>可以将本地/服务器的该配置文件下载到交换机中。

4.3 时间管理

1、配置夏时制，如下图所示；

夏季为了充分利用日光，节约能源，可以采用夏时制（DST: Daylight Saving Time）时间，即将夏季作息时间人为提前的经济时制。夏时制配置分循环式配置和非循环式配置。

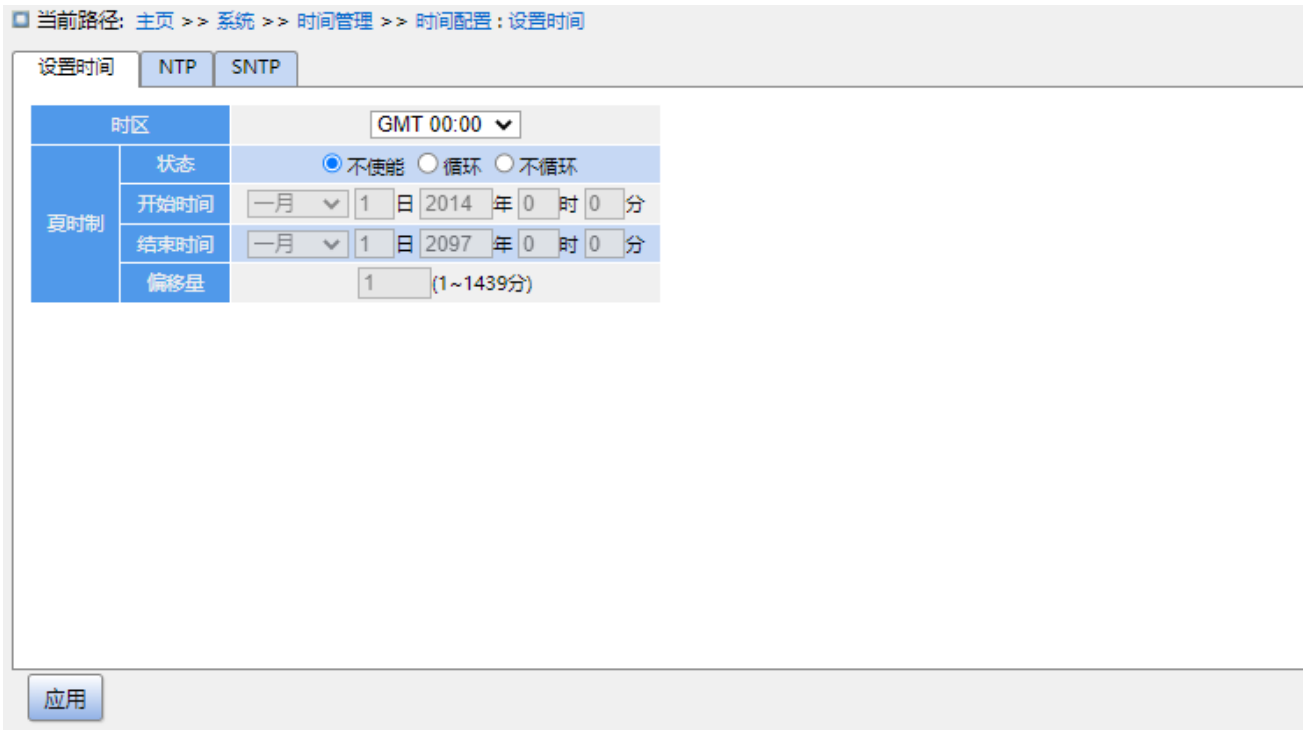


图 24 循环配置时间

图 25 不循环配置时间

时区

功能：选择本地时区。

夏时制状态

配置选项：不使能/循环/不循环

默认配置：不使能

功能：是否使能夏时制时间，使能后，选择夏时制时间执行模式，循环模式按年循环。

开始时间/结束时间

功能：使能夏时制后，配置执行夏时制的时间范围。不循环模式配置年、月、日、时、分指定夏时制时间的执行范围，如图 25 中配置 2014 年 1 月 1 日 00:00 ~ 2097 年 7 月 1 日 23:59 期间执行夏时制时间。循环模式配置月、周、日、时、分指定每年夏时制时间的执行范围，如图 24 中配置每年 1 月第一个星期一 00:00 ~ 7 月第一个星期一 23:59 期间执行夏时制时间。

偏移量

配置范围：1~1439 分

默认配置：1 分

功能：配置夏时制时钟偏移量，即执行夏时制时间，时钟被提前的时间量。

注意：

- 结束时间和起始时间应不同；
- 起始时间指非夏时制时间，结束时间指夏时制时间。

例：从 4 月 1 日 10:00:00 开始执行夏时制时间，到 10 月 1 日 9:00:00 结束，夏时制时间偏移量为 60min。

非夏时制时间运行至 4 月 1 日 10:00:00，直接跳至夏时制时间 11:00:00，开始执行夏时制时间，当夏时制时间运行至 10 月 1 日 9:00:00，再返回至非夏时制时间 8:00:00，开始执行非夏时制时间。

2、NTP 配置

NTP(Network Time Protocol，网络时间协议)用来在分布式时间服务器和客户端之间进行时间同步。NTP 可以对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于同一时间的多种应用。对于运行 NTP 的本地系统，既可以接收来自其他时钟源的同步，又可以作为时钟源同步其他时钟。

注：本设备仅支持做 NTP 客户端，无法作为时钟源同步其他时钟。

图 26 NTP 配置

NTP 状态

配置选项：使能/不使能

默认配置：不使能

功能：是否开启全局 NTP 服务功能。

注意：

- NTP 和 SNTP 协议互斥。由于 NTP 和 SNTP 使用相同的 UDP 端口号，因此两者不能同时使能；
- 未开启 NTP 服务时，可以对 NTP 服务进行配置并保存，即 NTP 服务的开启与否不影响 NTP 服务的配置。

服务器地址 1/服务器地址 2/服务器地址 3/服务器地址 4/服务器地址 5

配置格式：A.B.C.D

功能：配置 NTP 服务器 IP 地址，客户端将根据该服务器的消息来校准时间。

3、SNTP 配置

SNTP（Simple Network Time Protocol，简单网络时间协议）协议通过服务器和客户端之间请求、响应来校准时间。交换机做为客户端根据服务器的消息来校准时间。

注意：

- 交换机使用 SNTP 对时，需要有 SNTP Server 处于活动状态；
- SNTP 协议中携带的时间信息均为 0 时区的标准时间信息。

图 27 SNTP 配置

SNTP 状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 SNTP 协议。

服务器地址

配置格式：A.B.C.D

功能：配置 SNTP 服务器 IP 地址，客户端将根据该服务器的消息来校准时间。

4、查看交换机时间是否与服务器时间同步

点击导航树[系统] →[基本信息]，查看系统时间信息，如图 28 所示；

图 28 查看时钟信息

根据服务器时间，结合时区选择和夏时制配置，查看交换机时间信息。

4.4 PTP

1、PTP 外部时钟模式，如下图所示；

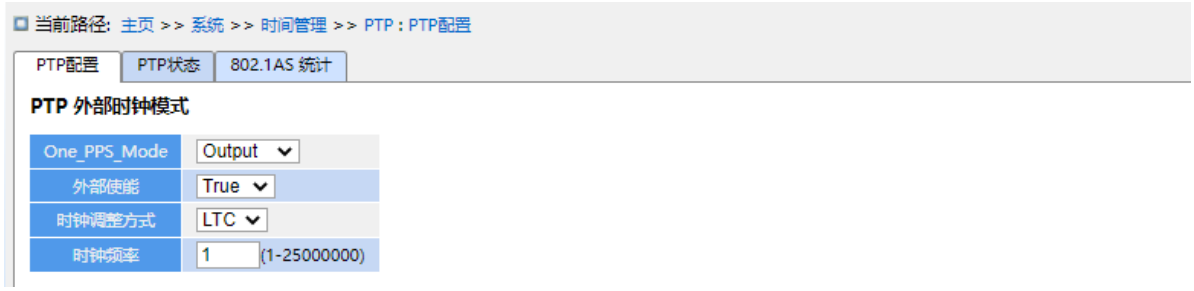


图 29 PTP 外部时钟模式

PTP 外部时钟模式

One_PPS_Mode

配置选项：Disable、Output、Input、OutInput

功能：Output：启用 pps 时钟输出。Input：启用 pps 时钟输入。OutInput：启动 pps 时钟输入/输出。

外部使用

配置选项：True、False

功能：True：启用外部时钟输出。False：禁用外部时钟输出。

时钟调整方式

配置选项：LTC、Auto

功能：LTC ： 选择本地时间计数器 （LTC） 频率控制。Auto：自动选择时钟控制，基于 PTP 配置文件和可用的硬件资源。

时钟频率

配置范围：1 - 25000000 （1 - 25MHz）

2、PTP 时钟配置，如下图所示；

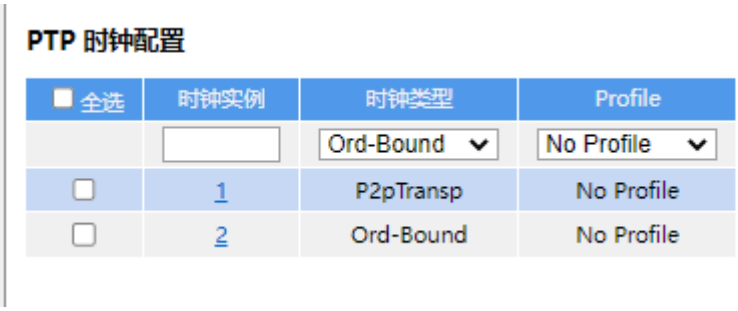


图 30 PTP 时钟配置

时钟实例

配置范围：0-3

描述：时钟实例。

配置范围：Ord-Bound、P2pTransp、E2eTransp、Mastronly、Slaveonly

功能：指示时钟实例的类型。有五种设备类型。Ord-Bound - 时钟的设备类型为普通边界时钟。P2p Transp - 时钟的设备类型是点对点透明时钟。E2e Transp - 时钟的设备类型是端到端透明时钟。Mastronly - 时钟的设备类型为“仅主设备”。Slaveonly - 时钟的设备类型为“仅从属”。

Profile

配置选项：No Profile、1588、802.1AS

功能：指示时钟使用的配置文件。

3、时钟类型与配置文件，如下图所示；

图 31 时钟类型与配置文件

时钟实例

功能：指示特定时钟实例 [0..3] 的实例编号。

时钟域

功能：指示时钟使用的硬件时钟域。

设备类型

描述：时钟实例的类型。

Profile

描述:指示时钟使用的配置文件。

过滤器类型

描述：确定的 PTP 筛选器类型应与网络的运行条件和 PTP 配置文件匹配。

过滤器类型

表 2 过滤类型信息

PTP 配置文件	过滤器类型	描述
1588	ACI_BASIC_PHASE	需要 PTP 同步和 Delay_req 帧速率为 16 fps 或更高。
1588	ACI_BASIC_PHASE_SYNCE	需要 PTP 同步和 Delay_req 帧速率为 16 fps 或更高。
1588	ACI_BASIC_PHASE_LOW	当 PTP 同步和 Delay_req 帧速率介于 1 fps 到 16 fps 之间时使用。
1588	ACI_BASIC_PHASE_LOW_SYNCE	当 PTP 同步和 Delay_req 帧速率介于 1 fps 到 16 fps 之间时使用。
没有	ACI_DEFAULT	未使用
G.8265.1	ACI_FREQ_XO	PTP 不知道频率。本地操作系统类型 XO。帧速率为 64 帧/秒。
没有	ACI_PHASE_XO	未使用
G.8265.1	ACI_FREQ_TCXO	PTP 不知道频率。本地断续器。帧速率为 64 帧/秒。
没有	ACI_PHASE_TCXO	未使用
G.8265.1	ACI_FREQ_OCXO_S3E	PTP 不知道频率。局部超氧体地层 3E。帧速率为 64 帧/秒。
没有	ACI_PHASE_OCXO_S3E	适用于包含符合 3E 层标准的振荡器的系统。
没有	ACI_BC_PARTIAL_ON_PATH_FREQ	未使用

没有	ACI_BC_PARTIAL_ON_PATH_PHASE	相位和频率由 PTP 恢复。帧速率为 16 帧/秒。
没有	ACI_BC_PARTIAL_ON_PATH_PHASE_SYNCE	由同步恢复的频率。帧速率为 16 帧/秒。
没有	ACI_BC_FULL_ON_PATH_FREQ	用于带基本滤波器的合成 TC。
G.8275.1	ACI_BC_FULL_ON_PATH_PHASE	符合 G.8273.2 标准的过滤器。低通滤波器，带宽为 0.1Hz。帧速率为 16 帧/秒。
G.8275.1	ACI_BC_FULL_ON_PATH_PHASE_SYNCE	符合 G.8273.2 标准的过滤器。由同步恢复的频率。帧速率为 16 帧/秒。
G.8265.1	ACI_FREQ_ACCURACY_FDD	符合 G.8263 标准的过滤器。PTP 不知道频率。帧速率为 64 帧/秒。
没有	ACI_FREQ_ACCURACY_XDSL	未使用
没有	ACI_ELEC_FREQ	未使用
没有	ACI_ELEC_PHASE	未使用
没有	ACI_PHASE_RELAXED_C60W	未使用
没有	ACI_PHASE_RELAXED_C150	未使用
没有	ACI_PHASE_RELAXED_C180	未使用
没有	ACI_PHASE_RELAXED_C240	未使用
没有	basic	基本低通滤波器舵机仅用于 802.1AS 型材

4、端口使能与配置，如下图所示；

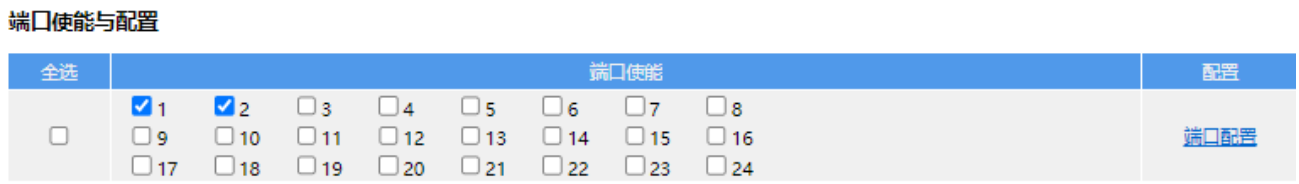


图 32 端口使能与配置

5、PTP 时钟端口配置，如下图所示；

图 33 PTP 时钟端口配置

端口

功能：端口号。

状态

描述：端口的当前状态。

MDR

功能：log 最小延迟请求间隔：主服务器宣布的延迟请求间隔。

Peer Mean Path Del

功能：端口在 P2P 模式下测量的路径延迟。在 E2E 模式下，此值为 0。

Anv

功能：发出处于主状态的通知消息的时间间隔。

ATo

功能：在端口上接收公告消息的超时。

Syv

功能：在主服务器中发出同步消息的时间间隔。

延时测量机制

功能：延迟机制：用于端口的延迟机制：e2e 端到端延迟测量 p2p 点对点延迟测量。

MPR

功能：在 E2e 模式下为端口发出 Delay_Req 消息的时间间隔。此值在公告消息中从主站到从站宣布。该值反映在从属服务器的 MDR 字段中在 P2P 模式下为端口发 Pdelay_Req 消息的时间间隔。

注： 此参数的解释已从 2.40 版更改。在早期版本中，该值是相对于同步间隔解释的，这违反了标准，因此现在该值被解释为间隔。即 MPR = 0 = > 1 Delay_Req pr 秒，与同步速率无关。

不对称延时

功能：链路的传输延时不对称。

入方向延时补偿

功能：以 ns 为单位测量的入口延迟。

出方向延时补偿

功能：以 ns 为单位测量的出口延迟。

版本

描述：当前实现仅支持 PTP 版本 2。

6、802.1AS 端口数据配置，如下图所示；

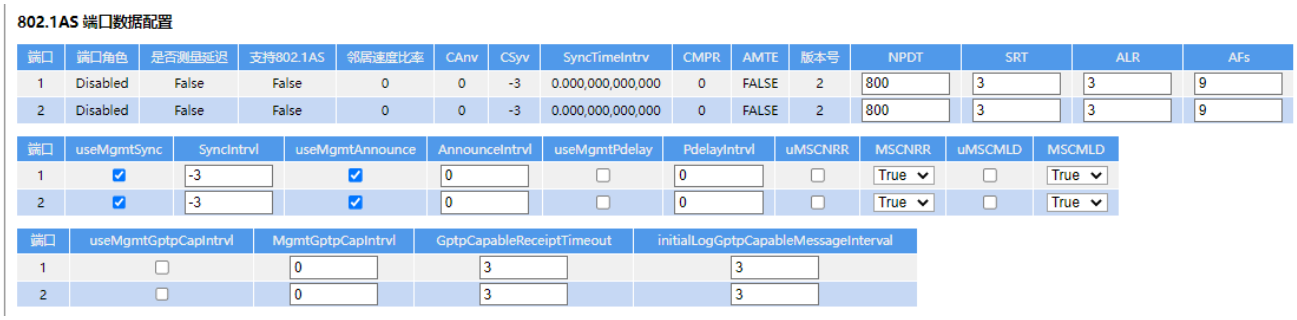


图 34 802.1AS 端口数据配置

端口使能

配置范围：交换机上的所有端口。

功能：使能交换机上的端口。

配置

功能：单击“端口配置”以编辑分配给此时钟实例的端口的端口数据集。

端口角色

功能：此端口的端口角色。

是否测量延迟

功能：如果端口正在测量链路传播延迟，则为 TRUE

支持 802.1AS

功能：如果链路另一端的时间感知系统支持 802.1AS，则为 TRUE

邻居速度比率

功能：计算出的相邻速率比表示为分数频率偏移乘以 2**41。

CAnv

功能：当前日志通告间隔-当前通告间隔的 log2，它是配置的初始 logAnnounceInterval 或消息间隔请求中接收的值

CSyv

功能：当前日志同步间隔-当前同步间隔的 log2，它是配置的初始 logSyncInterval 或消息间隔请求中接收的值

SyncTimeIntrv

功能：Sync Receipt Time Interval（同步接收时间间隔）—如果在该时间间隔内未接收到

时间同步信息，则会发生同步接收超时的时间间隔。

CMPR

功能：Current Log PDelay Req Interval-当前 PDelay_Req 间隔的 log2，它是配置的初始 logMinPdelayReqInterval 或消息间隔请求中接收的值。

AMTE

功能：可接受主表已启用-始终为 FALSE。

版本号

功能：IEEE 1588 PTP 版本号（始终为 2）。

NPDT

功能：邻居属性延迟阈值-允许的最大平均链路延迟。

SRT

功能：Sync Receive Timeout（同步接收超时）—从端口在未接收同步信息的情况下等待的时间同步传输间隔数。

ALR

功能：Allowed Lost response（允许的丢失响应）—未收到有效响应的 Pdelay_Req 消息的数量，超过该数量的端口被视为未与其邻居交换对等延迟消息。

AFs

功能：允许的故障—计算的平均传播延迟超过阈值 meanLinkDelayThresh 和/或相邻 RateRatio 计算无效的允许实例数。

useMgmtSync

功能：用于决定用于同步间隔的值的标志。

SyncIntrvl

功能：如果设置了 useMgmtSync，则端口使用此值来决定同步数据包间隔，否则使用默认值。范围为-7 至 4。

useMgmtAnnounce

功能：用于决定用于通告数据包间隔的值的标志。

AnnounceIntrvl

功能：如果设置了 useMgmtAnnouncement，则端口使用此值来决定 Announcer 数据包间隔，否则使用默认值。范围为-3 到 4。

useMgmt**Pdelay**

功能：用于决定用于通告数据包间隔的值的标志。

PdelayIntrvl

功能：如果设置了 useMgmtPdelay，则端口使用该值来决定对等延迟请求数据包间隔，否则使用默认值。范围为-7 至 5。

uMSCNRR

功能：useMgtSttableComputeNeighborRateRatio-此值确定 computeNeighRateRatio 值的来源。'True”表示源为“mgtSettiablecomputeNeighborRateRatio”“false”表示源为初始值或由“LinkDelayIntervalSetting 状态机”设置的值。

MSCNRR

功能：mgtSettiableComputeNeighborRateRatio-此值指示通过管理接口输入是否计算邻居比率。

uMSCMLD

功能：useMgtSttableComputeMeanLinkDelay-此值确定 computeMeanLink 延迟值的来源。'True”表示源为“mgtSettiableComputeMeanLinkDelay”。否则，将使用初始值或 LinkDelayInterval 状态机设置的值。

MSCMLD

功能：mgtSettiableComputeMeanLinkDelay-此值指示通过管理接口输入是否计算 Mean Link Delay//802.1AS 的公共链路延迟服务参数*/

useMgmtGptpCapIntrvl

功能：用于决定用于支持 gptp 的 tlv 信令数据包间隔的值的标志。

MgmtGptpCapIntrvl

功能：如果设置了 useMgmtGptpCapIntrvl，则端口使用该值来决定支持 gptp 的 tlv 信令数据包间隔，否则使用默认值。范围为-24 至 24。

GptpCableReceiveTimeout

功能：在确定其邻居不再调用 gPTP 协议之前，在没有从其邻居接收到包含 gPTP 能力 TLV 的信令消息的情况下等待的 gPTP 功能消息间隔的数量。

initialLogGptpCableMessageInterval

功能：initialLogGptpCableMessageInterval 指定端口初始化时支持 gPTP 的消息间隔，并且当接收到支持 gPTP 的 TLV 且 logGptpCable MessageInterval 字段设置为 126。

7、802.1AS 通用链路延迟服务特定端口数据配置，如下图所示；

802.1AS 通用链路延迟服务特定端口数据配置

端口	MLDT	DA	iLPDRv	uMSLPDRv	MSLPDRv	iCNRR	cm_uMSCNRR	cm_MSCNRR	iCMLD	cm_uMSCMLD	cm_MSCMLD	cm_ALR	cm_AFs
1	800	0	0	☐	0	True	☐	True	True	☐	True	3	9
2	800	0	0	☐	0	True	☐	True	True	☐	True	3	9

图 35 802.1AS 通用链路延迟服务特定端口数据配置

MLDT

功能：meanLinkDelayThresh-传播时间阈值，超过该阈值，端口不能参与 IEEE 802.1AS 协议。

DA

功能：delay 对称性-连接到该端口的链路上传播延迟相对于特级大师时基的不对称性，如 8.3 所定义。如果传播延迟不对称性未建模，则延迟对称性为零。

iLPDRv

功能：initialLogPdelayReqInterval-该值是所用 Pdelay_Req 消息传输间隔的以 2 为底的对数。

uMSLPDRv

功能：useMgtSttableLogPdelayReqInterval-此值确定“currentLogPdelayNeqInterval”的来源 True”表示源为“mgtSettiableLogPdelayReqInterval”。否则，初始值或 L 设置的值。

MSLPDRv

功能：mgtSttableLogPdelayReqInterval-如果 useMgtSttablelogPdelayreqInterval 为 true，则使用此值。

iCNRR

功能：initialComputeNeighborRateRatio-指示此端口是否要计算 neighborRateRatio 的初始值。

cm_uMSCNRR

功能：useMgtSttableComputeNeighborRateRatio-此值确定 computeNeighRateRatio 值的来源。'True”表示源为“mgtSettiablecomputeNeighborRateRatio”。否则，将使用初始值或 LinkDelayInterval 状态机设置的值。

cm_MSCNRR

功能：mgtSettiableComputeNeighborRateRatio-此值指示通过管理接口输入是否计算邻居比率。

iCMLD

功能：initialComputeMeanLinkDelay-初始值，指示此端口是否计算平均链路延迟。

cm_uMSCML D

功能：useMgtSttableComputeMeanLinkDelay-此值确定 computeMeanLink 延迟值的来源。'True”表示源为“mgtSettiableComputeMeanLinkDelay”。否则，将使用初始值或 LinkDelayInterval 状态机设置的值。

cm_MSCMLD

功能：mgtSettiableComputeMeanLinkDelay-此值指示通过管理接口输入是否计算 Mean Link Delay。

cm_ALR

功能：allowedLostResponses-它是未收到有效响应的 Pdelay_Req 消息的数量，超过该数量，链路端口被视为未交换对等延迟消息。

cm_AFs

功能：allowedFaults-它是错误的数量，超过此值时，asCapableAcrossDomains 设置为 FALSE。

8、当前时钟数据集，如下图所示；

当前时钟数据集

PTP时间	时钟调整方式	系统时钟同步到PTP时间	PTP时间同步到系统时钟
1970-01-01T05:21:58 164,126,960	Internal Timer	False	False

图 36 当前时钟数据集

PTP 时间

功能：以纳秒分辨率显示实际的 PTP 时间。

时钟调整方式

功能：显示实际的时钟调整方法。该方法取决于可用的硬件。

系统时钟同步到 PTP 时间

配置选项：False、True

PTP 时间同步到系统时钟

配置选项：False、True

功能：激活此按钮可将系统时钟与 PTP 时间同步。

9、时钟默认数据集，如下图所示；

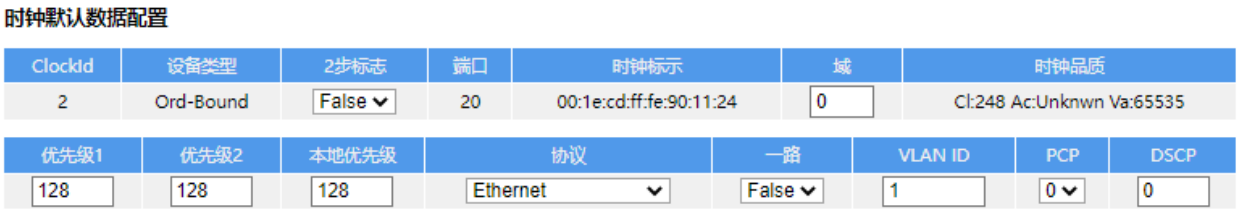


图 37 时钟默认数据集

设备类型

功能：指示时钟实例的类型。有五种设备类型。Ord-Bound - 时钟的设备类型为普通边界时钟。P2p Transp - 时钟的设备类型是点对点透明时钟。E2e Transp - 时钟的设备类型是端到端透明时钟。Mastronly - 时钟的设备类型为“仅主设备”。Slaveonly - 时钟的设备类型为“仅从属”。

2 步标志

功能：如果使用两步同步事件和 Pdelay_Resp 事件，则为 true。

端口

功能：节点中物理端口的总数。

时钟标识

功能：它显示唯一的时钟标识符。

域

功能：时钟域 [0..127]。

时钟品质

功能：时钟质量由系统决定，包含 3 个部分：IEEE1588 中定义的时钟等级、时钟精度和偏移缩放日志方差。

优先级 1

配置范围：0-255

功能：BMC 主选择算法使用的时钟优先级 1 [0..255]。

优先级 2

配置范围：0-255

功能：BMC 主选择算法使用的时钟优先级 2 [0..255]。

本地优先级

配置范围：0-255

功能：G8275.1 BMC 算法的本地优先级（1 是最高优先级）

协议

配置范围：Ethernet、EthernetMixed、IP4vmulti 、IPv4Mixed、OnePPS、IPv6Mixed、EthIPv4IPv6Combo

功能：PTP 协议引擎使用的传输协议。

VLAN ID

功能：用于标记 PTP 帧的 VLAN 标识符。

注： 如果为配置的 VID 配置了 vlan 标记的端口，则会标记数据包。

PCP

描述：用于 PTP 帧的优先级代码点值。

DSCP

描述：传输 IPv4 封装数据包时使用的 DSCP 值。

10、时钟电流数据集，如下图所示；

时钟电流数据集在 IEEE 1588 标准中定义。当前数据集是动态的。

时钟当前数据配置

stpRm	与主钟偏差	平均链路延时
0	0.000,000,000,000	0.000,000,000,000

图 38 时钟电流数据集

stpRm

描述：删除的步骤：它是从特级时钟到本地从时钟的 PTP 时钟的遍历数。

与主钟偏差

功能：主时钟和本地从时钟之间的时间差，以 ns 为单位测量。

平均链路延时

功能：主站和本地从站之间链路的平均传播时间。

11、主钟数据据集，如下图所示；

主钟数据集

主钟端口ID	端口	PStat	Var	改变速率	GrandMaster钟ID	GrandMaster钟质量	优先级1	优先级2
00:1e:cd:ff:fe:90:11:24	0	False	0	0	00:1e:cd:ff:fe:90:11:24	Cl:248 Ac:Unknwn Va:65535	128	128

图 39 主钟数据据集

主钟端口 ID

描述：主时钟的时钟标识，如果本地时钟不是从时钟，则该值为时钟自己的 id。

端口

功能：主端口的端口 ID

PStat

功能：家长统计数据（总是假的）。

Var

功能：观察到父偏移缩放对数方差。

改变速率

功能：观察到的母时钟相位变化率。即从时钟与主时钟相比的速率偏移。（单位 = ns 每秒）。

GrandMaster 钟 ID

功能：时钟标识为特级主时钟，如果本地时钟不是从时钟，则该值为时钟自己的 ID。

GrandMaster 钟质量

功能：特级大师宣布的时钟质量（请参阅时钟默认数据集：时钟质量的描述）。

优先级 1

功能：时钟优先级 1 由特级大师宣布。

优先级 2

功能：时钟优先级 2 由特级大师宣布。

12、时钟时间特性数据配置，如下图所示；

时钟时间特性数据配置

与UTC时间差	是否有效	负闰秒	正闰秒	时间可追溯	频率可追溯	PTP时间测量	时间源
0	False	False	False	False	False	True	111

图 40 时钟时间特性数据配置

功能：时钟时间特性数据在 IEEE 1588 标准中定义。数据集既是可配置的，也是动态的，即参数可以为特级大师配置。在从时钟中，参数被特级时钟的时序属性覆盖。这些参数未在当

前 PTP 实现中使用。

时间源参数的有效值为：

16 （0x10） ATOMIC_CLOCK

32 （0x20） 全球定位系统

48 （0x30） TERRESTRIAL_RADIO

64 （0x40） 太平洋标准杆

80 （0x50） 新能源计划

96 （0x60） HAND_SET

144 （0x90） 其他

160 （0xA0） INTERNAL_OSCILLATOR

与 UTC 时间差

功能：在时代为 UTC 的系统中，它是 TAI 和 UTC 之间的偏移量。

是否有效

功能：如果为 true，则当前偏移量的值有效。

负润秒

如果为 true，则此字段指示当前 UTC 日的最后一分钟只有 59 秒。

正润秒

如果为 true，则此字段指示当前 UTC 日的最后一分钟有 61 秒。

时间可追踪

如果时间刻度和当前 UtcOffset 的值可追溯到主参考，则为真。

频率可追溯

功能：如果确定时间刻度的频率可追溯到主基准电压源，则为 True。

PTP 时间测量

功能：如果特级大师时钟的时钟时间刻度为真，否则为假。

时间源

配置范围：0-255

功能：特级大师时钟使用的时间来源。

13、基本的过滤参数配置，如下图所示；

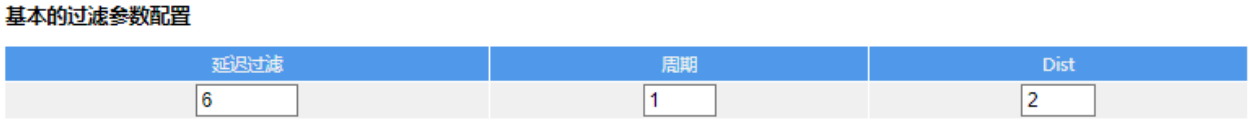


图 41 基本的过滤参数配置

功能：默认延迟滤波器是低通滤波器，时间常数为 2**DelayFilter*DelayRequestRate。如果 DelayFilter 参数设置为 0 或 Dist 参数为 0，则延迟滤波器使用与偏移滤波器相同的算法。默认偏移过滤器使用最小偏移或平均值过滤器方法 i、 e.计算中使用周期样本期间的最小测量偏差。两次计算之间的距离为 Dist 周期。

注意：在启用时间戳的 PHY 的配置中，如果（period*dist<SyncPackets pr sec/4），即每秒最多进行 4 次调整，则周期会自动增加。

如果 Dist 为 0，则对偏移进行低通滤波，滤波器 BW 为 0.1Hz，如果 Dist 为 1，则在周期上对偏移进行平均，如果 Dist 大于 1，则使用“最小”偏移量计算偏移量。

14、基本的伺服参数配置，如下图所示；

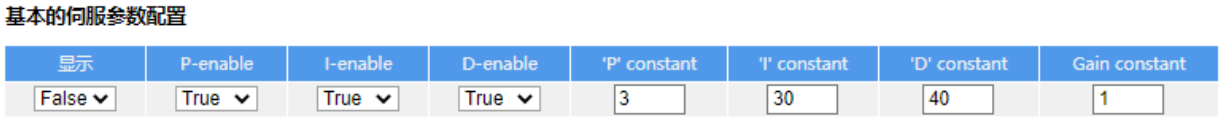


图 42 基本的伺服参数配置

显示

功能：如果为 true，则在调试终端上记录从主设备偏移、MeanPathDelay 和 clockAdjustment。

P-enable

功能：如果为真，则包含算法的 P 部分。

I-Enable

功能：如果为真，则包含算法的 I 部分。

D-enable

功能：如果为真，则包含算法的 D 部分。

'P' constant

功能：如果为真，则包含算法的 P 部分。

'I' constant

功能：如果为真，则包含算法的 I 部分。

'D' constant

功能：如果为真，则包含算法的 D 部分。

15、PTP 状态，如下图所示；

图 43 PTP 状态

时钟实例

描述：指示特定时钟实例 [0..3] 的实例。

功能：单击时钟实例编号以监视时钟详细信息。

设备类型

描述：指示时钟实例的类型。有五种设备类型。1. Ord-Bound - 时钟的设备类型是普通边界时钟。2. P2p Transp - 时钟的设备类型是点对点透明时钟。3. E2e Transp - 时钟的设备类型是端到端透明时钟。4. Master Only - 时钟的设备类型为仅主设备。5. Slave Only - 时钟的设备类型为仅从属。

16、802.1AS 统计，如下图所示；

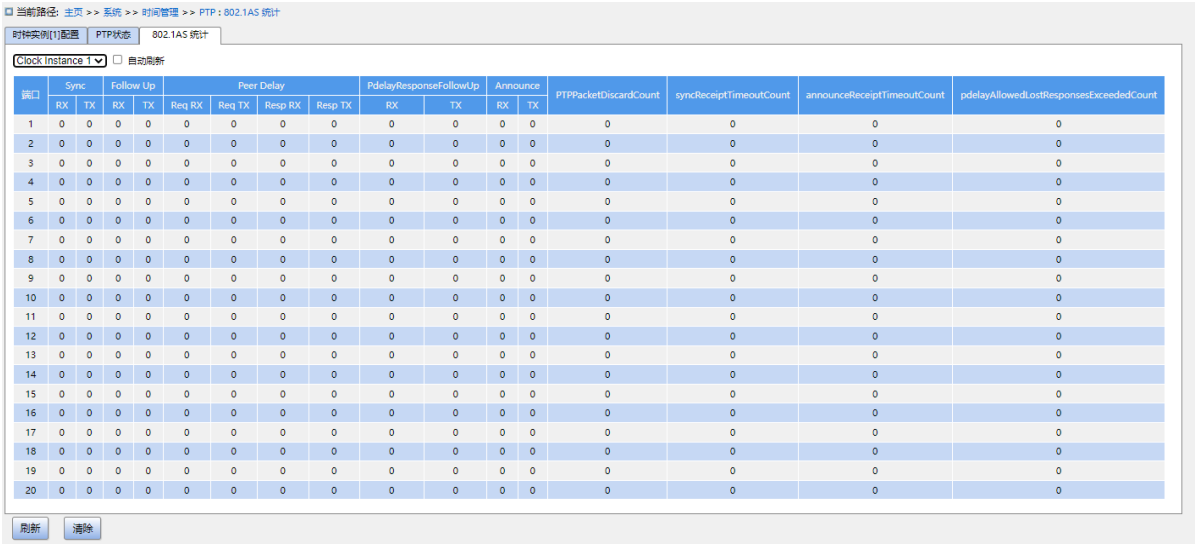


图 44 802.1AS 统计信息

Sync

功能：RX:每次收到同步信息时递增的计数器。TX: 每次传输同步信息时递增的计数器。

PdelayResponseFollowUp

功能：RX:每次收到后续消息时递增的计数器。TX: 每次传输 Follow_Up 消息时递增的计数器。

Peer Delay Req

功能：Req RX：每次收到 Peer Delay_ Req 消息时递增的计数器。Req TX：每次传输 Peer Delay_Req 消息时递增的计数器。

Peer Delay Resp

功能：Resp RX:每次收到 Pdelay_Resp 消息时递增的计数器。Resp TX: 每次传输 Pdelay_Resp 消息时递增的计数器。

PdelayResponseFollowUp

功能：RX:每次收到 Pdelay_Resp_Follow_Up 消息时递增的计数器。TX: 每次传输 Pdelay_Resp_Follow_Up 消息时递增的计数器。

Announce

功能：RX:每次收到“宣布”消息时递增的计数器。TX: 一个计数器，每次传输“播报”消息时都会递增。

PTPPacketDiscardCount

功能：每次收到“宣布”消息时递增的计数器。

syncReceiptTimeoutCount

功能：每次发生同步接收超时时递增的计数器。

announceReceiptTimeoutCount

功能：每次发生通知接收超时时递增的计数器。

pdelayAllowedLostResponsesExceededCount

功能：一个计数器，每次变量丢失的值超过变量允许的值丢失响应时，该计数器都会递增。

4.5 软件升级

交换机通过升级软件版本可以获得更完善性能。该系列交换机升级包括 Boot 版本升级和软件版本升级，升级时应先升级 Boot 版本，再升级软件版本，在 Boot 版本不变的情况下可

以只升级软件版本。可以通过本地升级/FTP/TFTP 协议升级软件版本。

4.5.1 本地升级

1、本地升级软件，如图 45 所示；

图 45 升级软件-本地升级

升级方式

配置选项：从本地升级/从 FTP 服务器升级/从 TFTP 服务器升级

说明：选择升级方式。

升级对象

配置选项：软件版本/Boot 版本

功能：选择升级对象。

升级模式

配置选项：主分区/备份分区

说明：该交换机可以下载两个软件版本，两个版本可以相同也可以不同。

2、待 Web 页面提示升级成功，如图 46 所示，激活软件版本并重启设备，在系统信息中检查软件版本是否为升级后的版本。

图 46 升级成功

警告：

- 软件升级成功后，必须激活软件版本并重启设备，软件版本才能生效；
- 升级失败后不能重启交换机，避免版本文件丢失设备无法正常启动。

4.5.2 FTP 升级

安装 FTP 服务器，以 WFTPD 软件为例介绍 FTP 服务器配置及软件升级过程；

1、打开[Security]→[users/rights]对话框点击<New User>按钮添加 FTP 新用户，如图 47 所示，输入用户名和密码，例如：用户名 admin，密码 123，点击<OK>按钮；

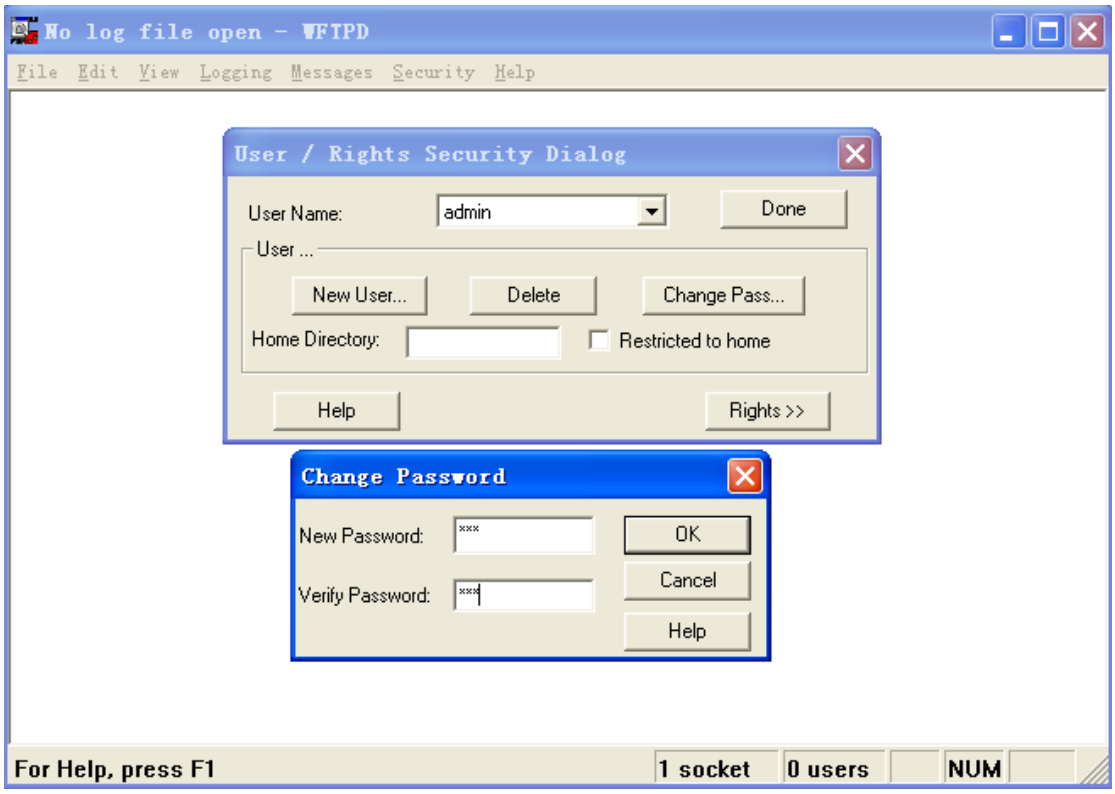


图 47 添加 FTP 新用户

2、Home Directory 栏中输入服务器中软件版本文件的存放路径，如图 48 所示，点击<Done>按钮；

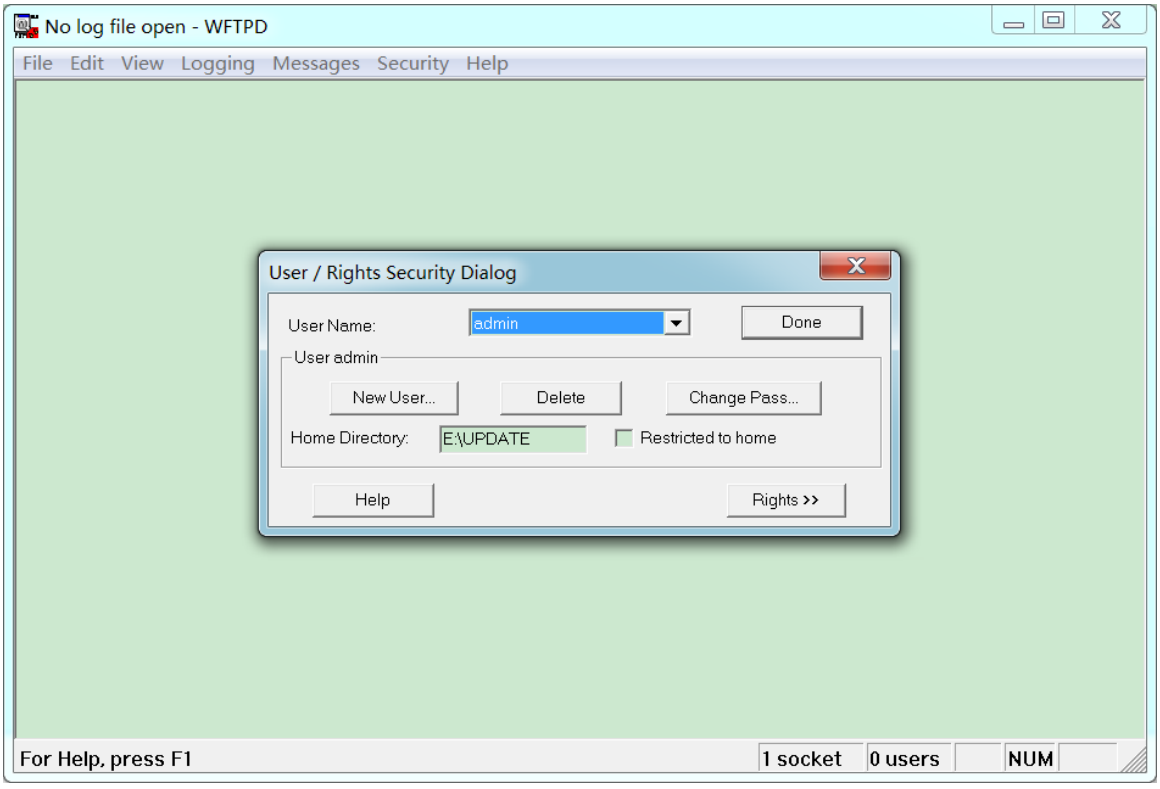


图 48 文件路径修改

3、点击导航树[系统]→[软件升级]菜单进入升级软件界面如图 49 所示，输入 FTP 服务器 IP 地址、建立的 FTP 用户名、用户密码、服务器上文件名，点击<升级>按钮；

图 49 FTP 服务器升级软件

升级方式

配置选项：从本地升级/从 FTP 服务器升级/从 TFTP 服务器升级

说明：选择升级方式。

升级对象

配置选项：软件版本/Boot 版本

功能：选择升级对象。

升级模式

配置选项：主分区/备份分区

说明：该交换机可以下载两个软件版本，两个版本可以相同也可以不同。

警告：

- 文件名应带有后缀，否则会导致升级失败。

4、确保 FTP 服务器和交换机通信正常，如图 50 所示；

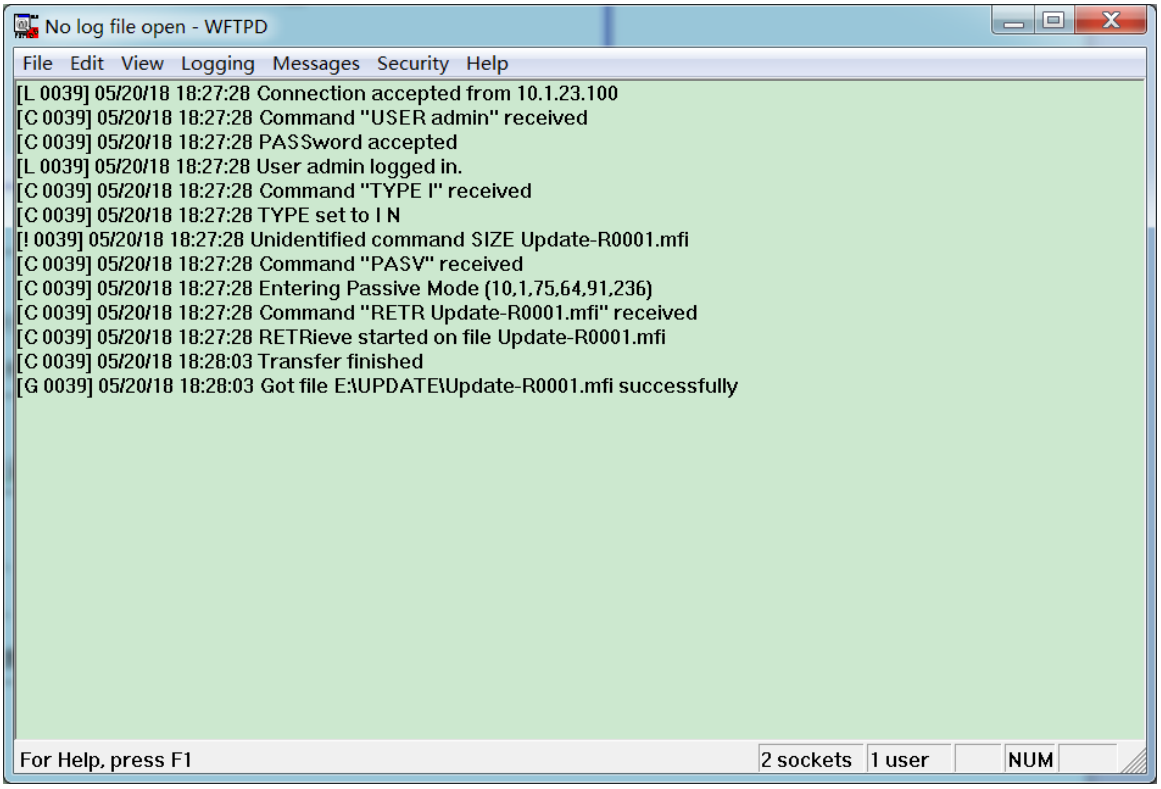


图 50 FTP 服务器和交换机通信正常

注意：

如需显示如图 50 所示的升级日志信息，须在 WFTPD 软件中点击[Logging]→[Log Options]，选择 Enable Logging 和需要显示的日志信息。

5、交换机等待升级过程，如图 51 所示；

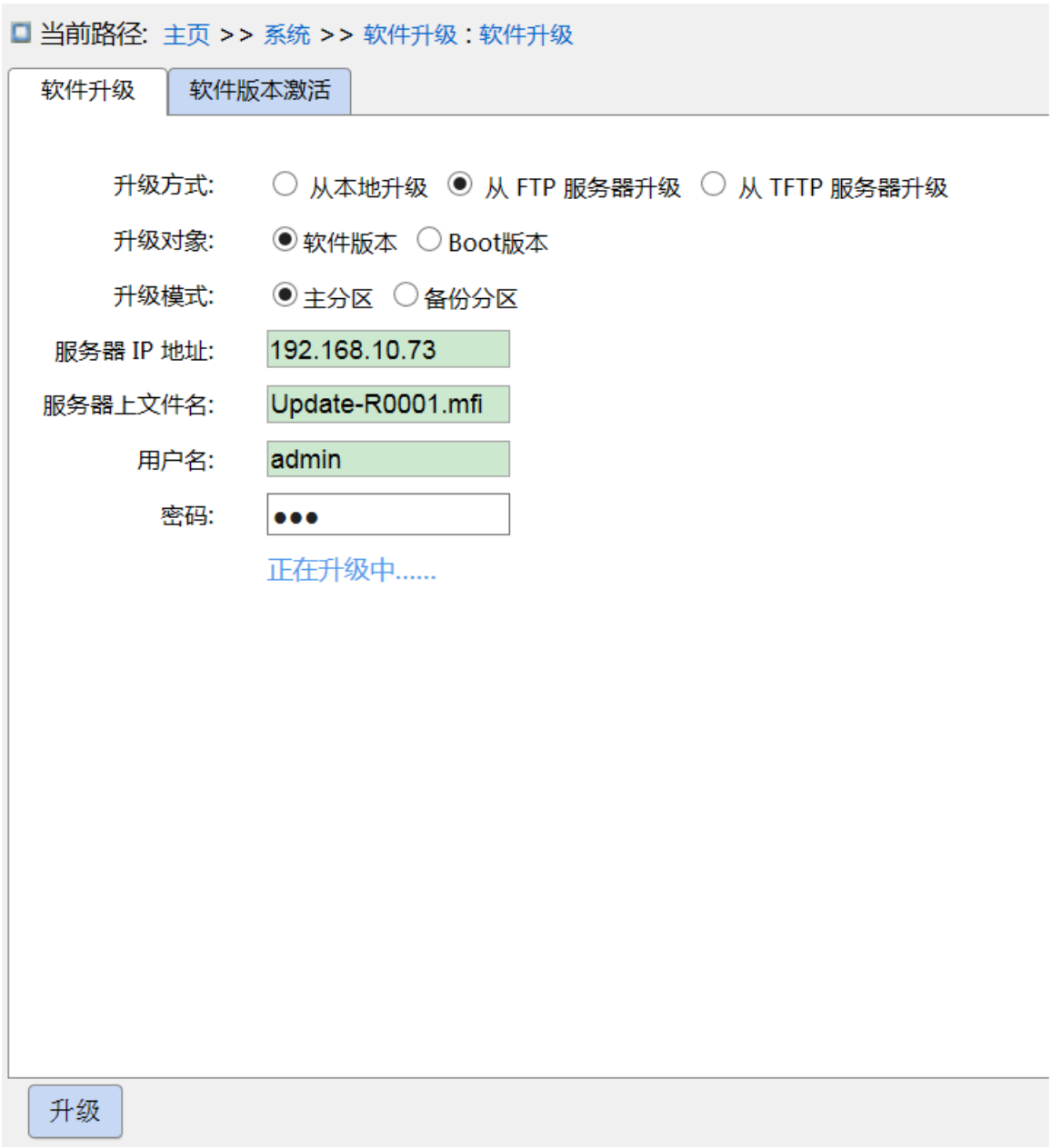


图 51 升级等待

6、升级成功后，重启设备并在交换机主要信息中检查软件版本是否为升级后的软件版本。

警告：

- 软件升级过程中，FTP 服务器软件应保持运行状态；
- 软件升级成功后，需要重启设备新的软件版本才能生效；
- 升级失败后不能重启交换机，避免版本文件丢失设备无法正常启动。

4.5.3 TFTP 升级

安装 TFTP 服务器，以 TFTPD 软件为例介绍 TFTP 服务器配置及软件升级过程，如下图所示：

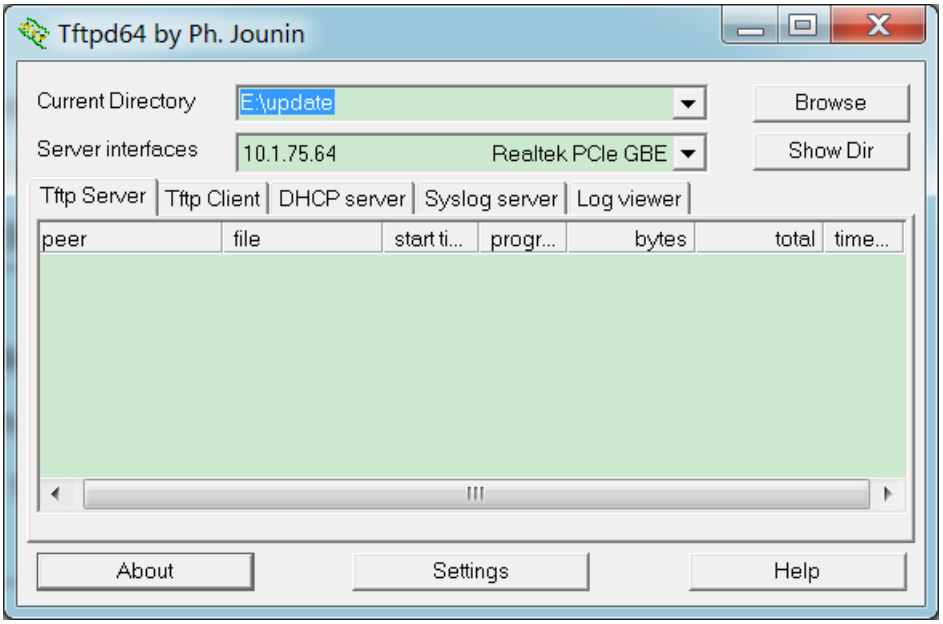


图 52 TFTP 服务器端配置

1、Current Directory 栏中选择服务器中软件版本文件的存放路径；Server interface 栏中选择服务器 IP 地址。

2、点击导航树[系统]→[软件升级]菜单进入升级软件界面如下图所示，输入 TFTP 服务器 IP 地址、服务器上文件名，点击<升级>按钮；

图 53 TFTP 模式下升级软件

3、确保 TFTP 服务器和交换机通信正常，如下图所示；

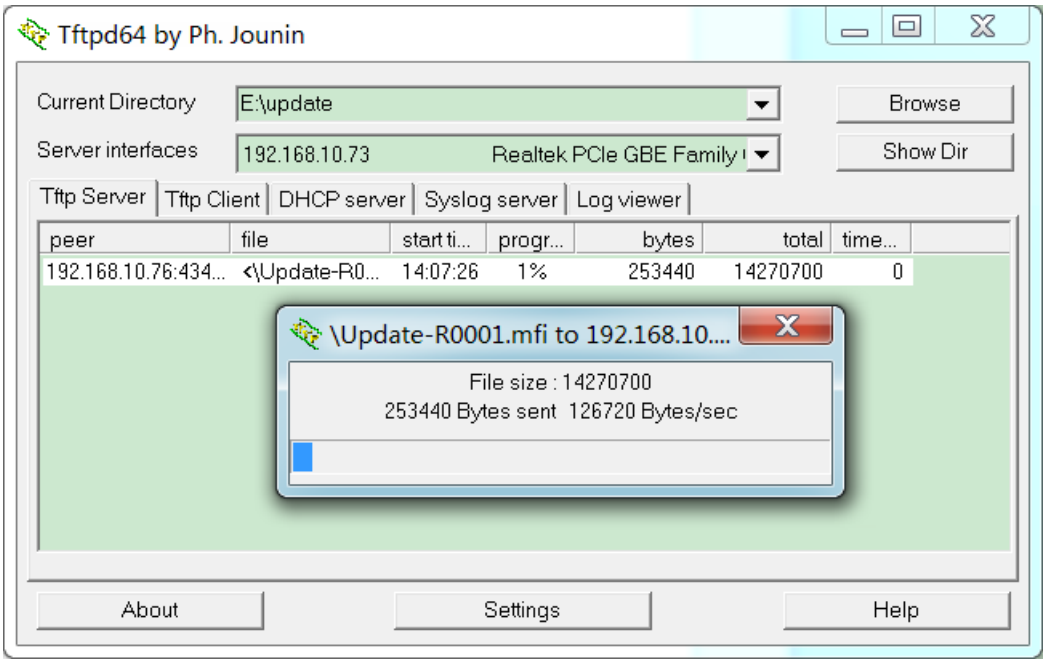


图 54 TFTP 服务器和交换机通信正常

4、交换机等待升级过程，如下图所示；

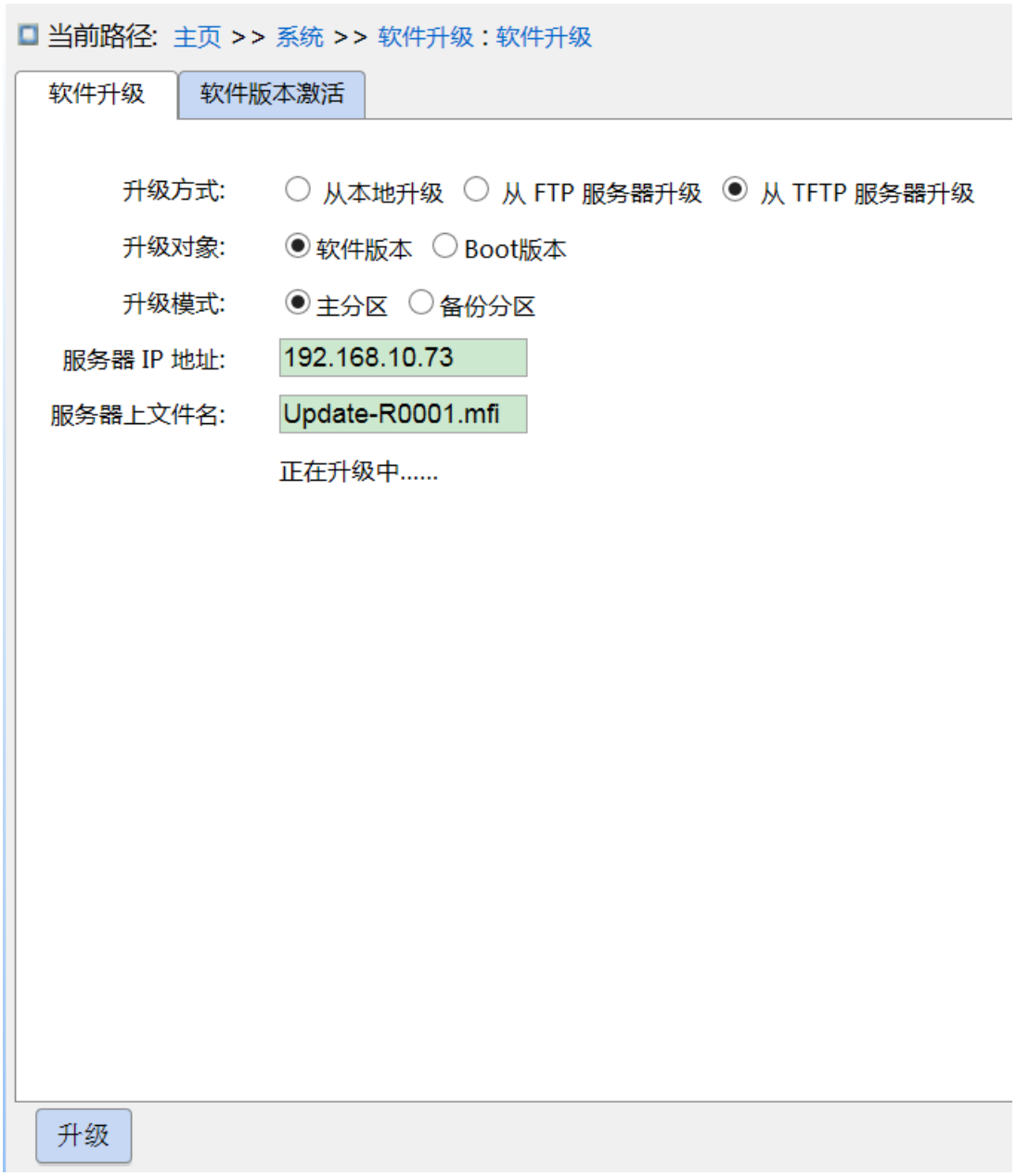


图 55 升级等待

5、升级成功后，重启设备并在交换机主要信息中检查软件版本是否为升级后的软件版本。

警告：

- 软件升级过程中，TFTP 服务器软件应保持运行状态；
- 软件升级成功后，需要重启设备新的软件版本才能生效；
- 升级失败后不能重启交换机，避免版本文件丢失设备无法正常启动。

4.6 软件版本激活

激活软件版本，如图 56 所示；

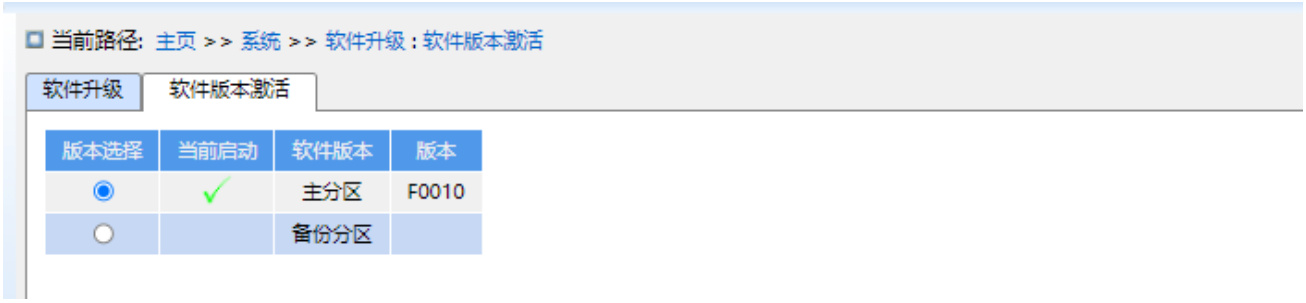


图 56 激活软件版本

选中一个版本，点击<应用>按钮，激活该版本使其成为下次启动时的启动版本，只能有一个版本处于激活状态。

当前启动版本表示此版本为当前运行版本。

4.7 语言包升级

图 57 升级语言包

升级方式

配置选项：从本地升级

功能：下载语言包到设备，设备可支持多种语言访问。

4.8 重启

重启设备，如下图所示；

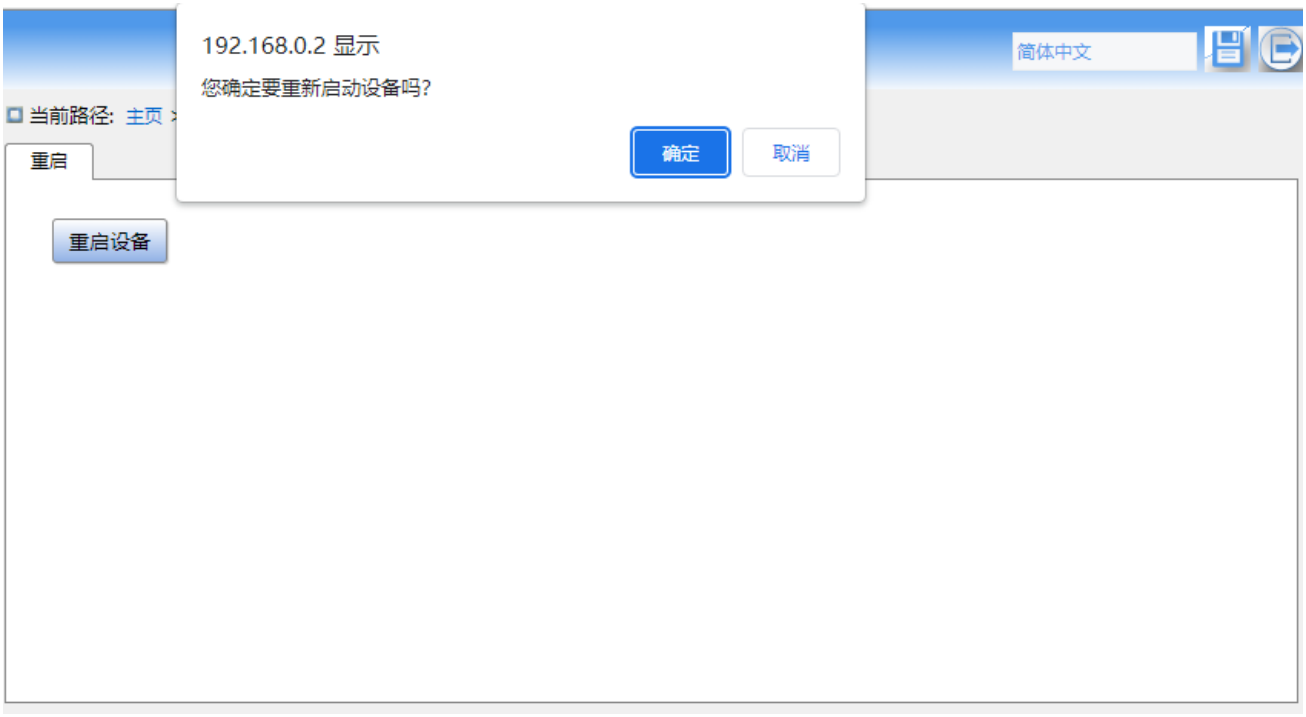


图 58 重启设备

重启设备之前应确认是否需要保存当前配置，重启后交换机配置为保存的最新配置信息，如果没有保存过配置信息，重启后交换机配置恢复为出厂默认配置。

4.9 关于

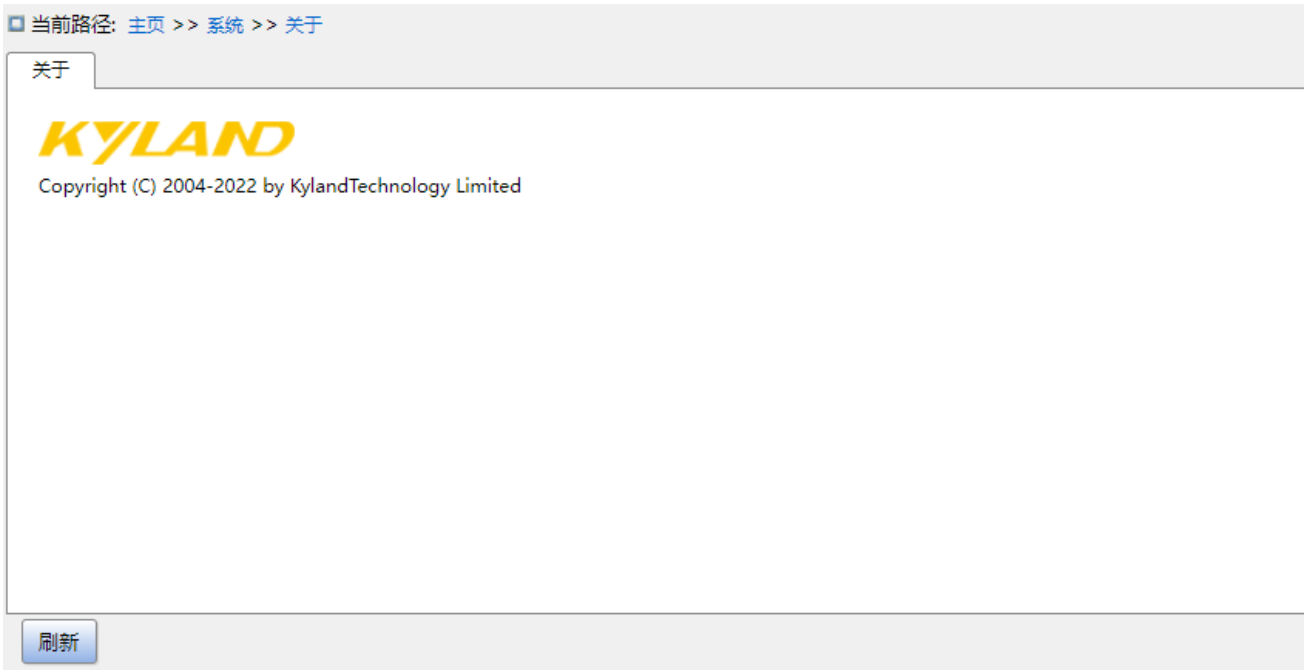


图 59 系统相关信息

5 服务

5.1 SSL 配置

5.1.1 介绍

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，为基于 TCP 的应用层协议提供安全链接，如 HTTPS。SSL 传输层对网络连接进行加密，使用加密算法保证数据的保密性，使用密钥鉴别码保证信息的可靠性。该协议广泛应用于 Web 浏览，收发电子邮件，网络传真，实时通讯等，为网络提供安全传输的加密协议。

5.1.2 Web 页面配置

1、使能 HTTPS 协议，如图 60 所示；

图 60 使能 HTTPS 协议

HTTPS 状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 HTTPS 协议，使能后，可以使用 http://*ip address* 和安全链接 https://*ip address* 登陆交换机 Web 页面。

自动重定向

配置选项：使能/去使能

默认配置：去使能

功能：使能时，只允许使用安全链接 https://*ip address* 登陆交换机 Web 页面。不使能时，可以通过 HTTP 和 HTTPS 登陆交换机 Web 页面。只有“HTTPS 状态”使能时，才可配置“自动重定向”参数。

2、证书管理，如图 61 所示；

图 61 生成证书

管理

配置选项：自动生成/从 URL 获取/从本地上传/删除

功能：选择证书的上传方式

从 URL 获取证书

URL

功能：配置 web 路径，例如：https://10.10.10.10:80/new_image_path/new_image.dat

从本地上传

选择文件

功能：选择本地 HTTPS 证书文件

5.2 SNMP v1/SNMP v2c

5.2.1 介绍

SNMP（Simple Network Management Protocol，简单网络管理协议）是使用TCP/IP协议族对网络中设备进行管理的一个框架。管理员利用SNMP功能可以查询设备信息、修改设备参数值、监控设备状态、发现网络故障等。

5.2.2 实现

SNMP协议采用管理站/代理模式，因此SNMP网络元素分为NMS和Agent 两部分。

NMS（Network Management Station，网络管理站）是运行支持SNMP协议的网管软件客户端程序的工作站，在SNMP网络管理中起核心作用。

Agent是驻留在被管理网络设备的一个进程，负责接收、处理来自NMS的请求报文。有告警发生时，Agent也会主动通知NMS。

NMS是SNMP网络的管理者，Agent是SNMP网络的被管理者。NMS和Agent之间通过SNMP协议来交互管理信息。SNMP提供五种基本操作：

Get-Request

Get-Response

Get-Next-Request

Set-Request

Trap

NMS通过Get-Request、Get-Next-Request和Set-Request消息来对Agent发出查询和配置管理变量的请求，Agent收到请求后，用Get-Response消息对请求进行回复。有告警发生时，Agent会主动的向NMS发送Trap消息通知NMS发生了异常事件。

5.2.3 说明

该系列设备SNMP Agent支持SNMP v2c版本，SNMP v2c兼容SNMP v1版本。

SNMP v1采用团体名（Community Name）认证，团体名起到了类似于密码的作用，用来限制SNMP NMS对SNMP Agent的访问。如果SNMP报文携带的团体名没有得到设备认可，该报文将被丢弃。

SNMP v2c也采用团体名认证。它在兼容SNMP v1 的同时又扩充了SNMP v1 的功能。

NMS和Agent的SNMP版本匹配是它们之间成功互访的前提条件。Agent可以同时配置多个版本，与不同的NMS通信采用不同的版本。

5.2.4 MIB 介绍

任何一个被管理资源都表示成一个对象，称为被管理的对象。MIB（Management Information Base，管理信息库）是被管理对象的集合。定义了被管理对象之间的层次关系以及对象的一系列属性，比如对象的名字、访问权限和数据类型等。每个Agent都有自己的MIB库。NMS根据权限可以对MIB中的对象进行读/写操作。NMS、Agent和MIB之间的关系如图 62 所示：

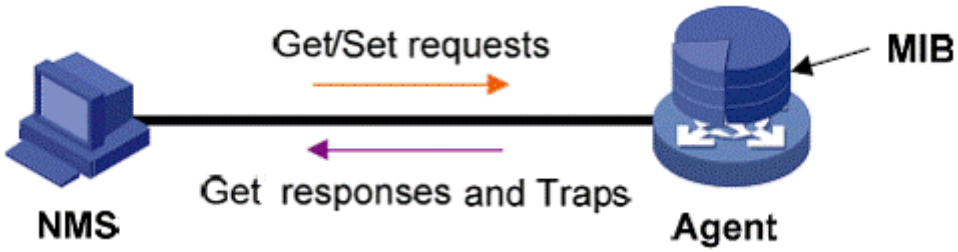


图 62 NMS、Agent 和 MIB 关系图

MIB 定义了一个树型结构，树的节点表示被管理对象，每个节点都包含一个唯一的 OID（Object Identifier，对象标识符），OID 指示该节点在 MIB 树型结构中的位置，如图 63 所示，被管理对象 A 的 OID 为 1.2.1.1。

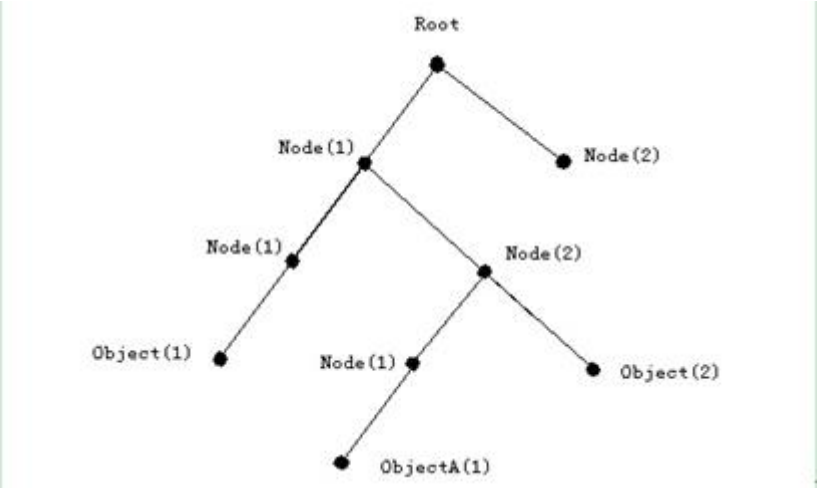


图 63 MIB 树结构

5.2.5 Web 页面配置

1、使能 SNMP 协议，如下图所示；

图 64 使能 SNMP 协议

模式

配置选项：使能/不使能

默认配置：使能

功能：是否使能 SNMP 协议。

引擎 ID

配置范围：偶数个十六进制数，不能为全 0 或全 F，偶数的取值范围 10~64。

功能：配置 SNMP v3 系统引擎 ID，修改引擎 ID 时，会清除用户表中相应设备 ID 对应的

用户。

2、配置团体名，如下图所示；

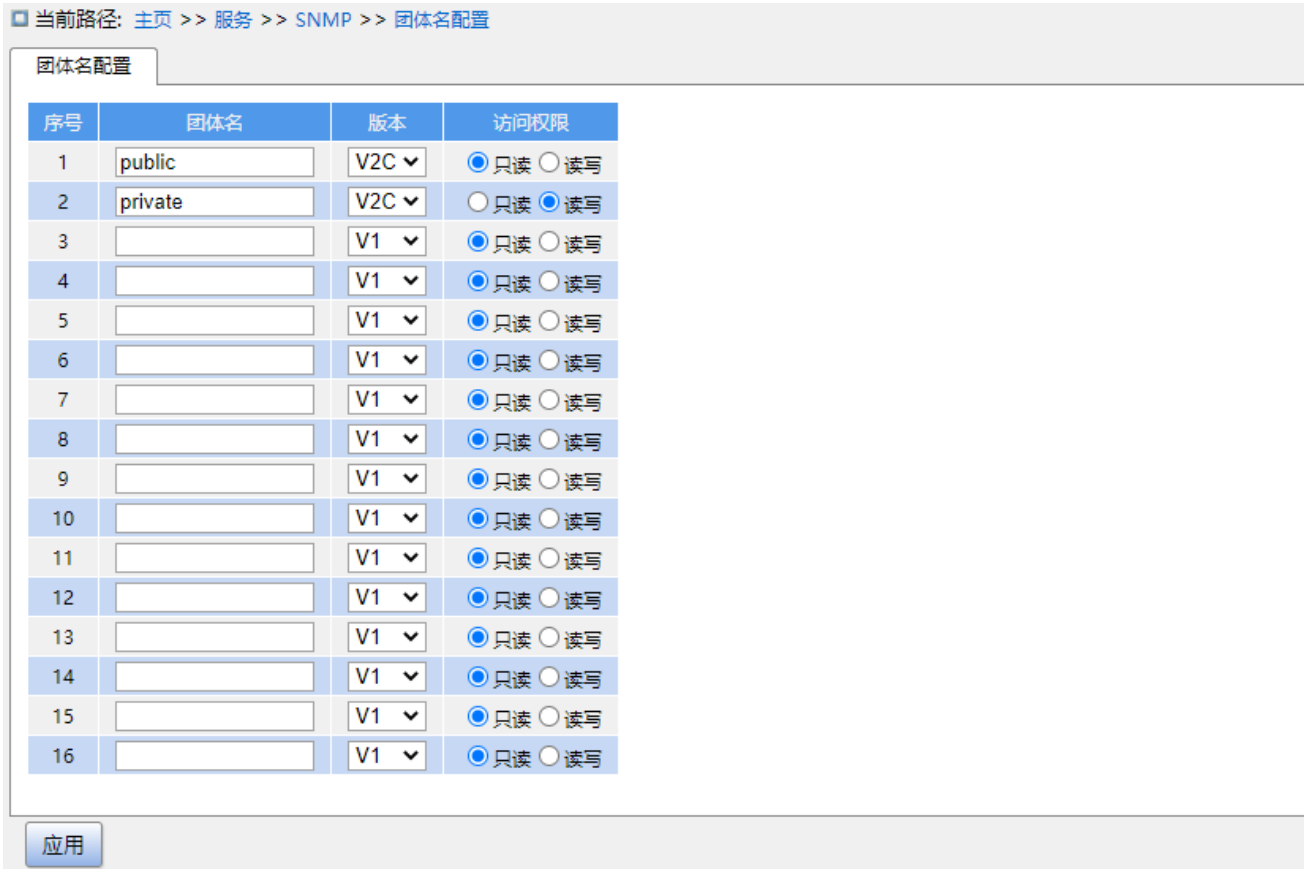


图 65 配置团体名

团体名

配置范围：1~32 个字符

功能：配置交换机的团体名。

描述：只有 SNMP 报文中携带的团体名与该团体字符串一致时才能对交换机的 MIB 库信息进行访问。

说明：最多可以配置 16 个团体字符串。

访问权限

配置选项：只读/读写

默认配置：只读

功能：配置 MIB 库的访问方式。

描述：只读权限只能读取 MIB 库信息；读写权限可以对 MIB 库信息进行读写操作。

3、配置 trap，如下图所示；

图 66 配置 trap 表项

Trap 名称

配置范围：1~32 个字符

功能：配置 trap 表项名称。

状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能该 trap 表项，使能后交换机向服务器发送相应的 trap 报文。

版本

配置选项：v1/ v2c/ v3

默认配置：v1

功能：配置交换机向服务器发送的 trap 报文版本号。

目的 IP

配置格式：A.B.C.D

功能：配置接收 Trap 消息的服务器地址。

目的端口

配置范围：1~65535 功能：配置发送 trap 报文的端口号。

4、点击 trap 配置项详细信息可以看到 trap 配置详细信息，如下图所示；

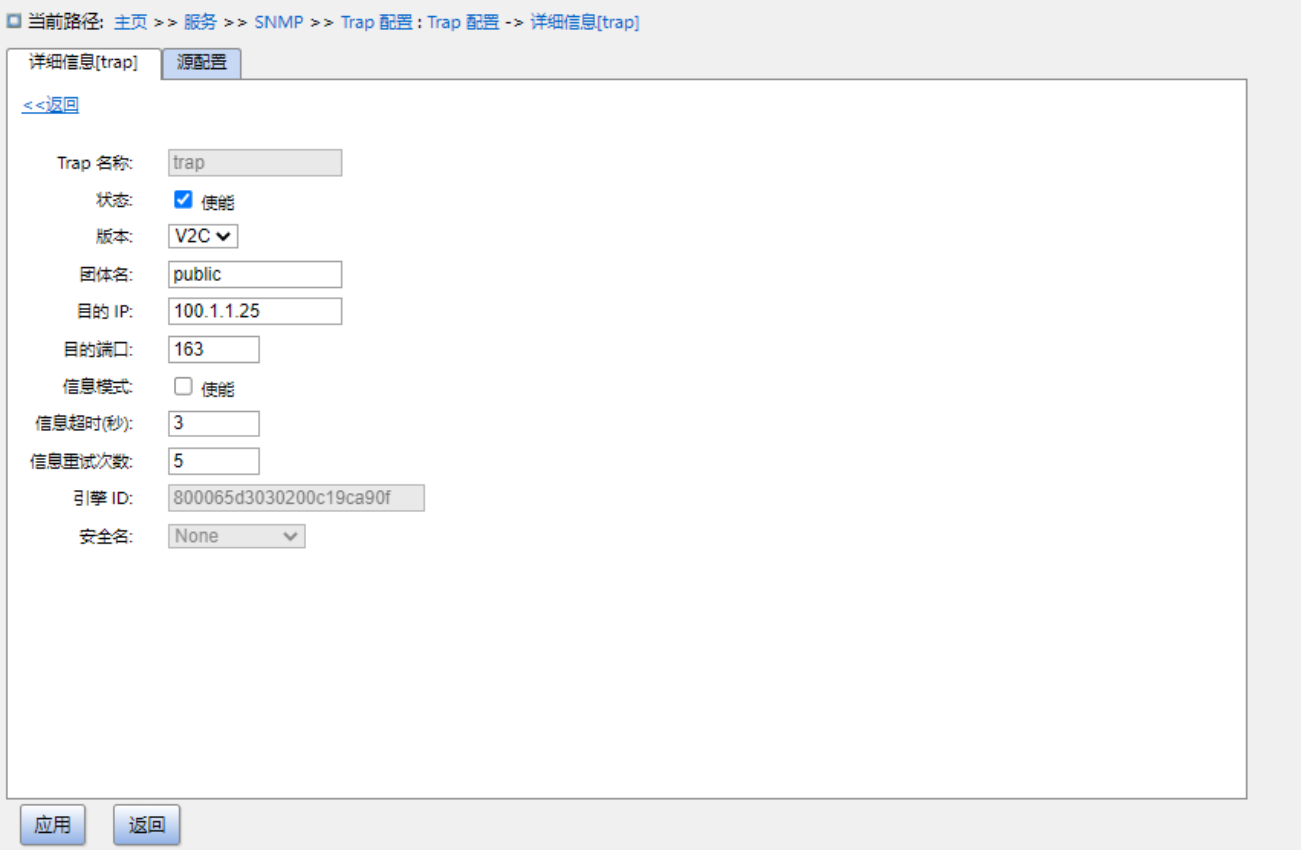


图 67 trap 详细信息

Trap 团体名

配置范围：0~255 个字符

默认配置：public

功能：配置发送 trap 报文中携带的团体名。

信息模式

配置选项：使能/不使能

默认配置：不使能

功能：服务器接收到 trap 消息后，是否向交换机发送回复信息。

信息超时

配置范围：0~2147 秒

默认配置：3 秒

功能：配置 trap 信息发送超时时间；交换机发送 trap 报文后，如果该时间段内，未收到服务器的回复，则重新发送 trap 报文。

信息重试次数

配置范围：0~255

默认配置：5

功能：配置 trap 报文超时重发的次数，如果累计的发送次数超过该配置值，服务器仍旧没有回复，则认为 trap 信息发送失败。

5、配置 trap 事件，如下图所示；

图 68 trap 源配置

系统热启动/冷启动

配置选项：使能/不使能

默认配置：不使能

功能：系统热启动/冷启动时，是否发送 trap 报文。

RMON 下降/上升告警

配置选项：使能/不使能

默认配置：不使能

功能：RMON 产生下降/上升告警时，是否发送 trap 报文。

STP 新的根桥/拓扑改变

配置选项： 使能/不使能

默认配置：不使能

功能：STP 状态变化时，是否发送 trap 报文。

端口链路 up/链路 down

配置选项：使能/不使能

默认配置：不使能

功能：端口状态变化时，是否发送端口 up/down 的 trap 报文。

告警

配置选项：使能/不使能

默认配置：不使能

功能：有告警信息时，是否发送 trap 报文。

SNMP 认证失败

配置选项：使能/不使能

默认配置：不使能

功能：SNMP 认证失败时，是否发送 trap 报文。

LLDP

配置选项：使能/不使能

默认配置：不使能

功能：邻居状态变化时，是否发送 LLDP 的 trap 报文。

5.2.6 典型配置举例

SNMP 管理站与交换机通过以太网相连，管理站 IP 地址为 192.168.0.23，交换机 IP 地址为 192.168.0.2。NMS 通过 SNMP v2c 对 Agent 进行监控管理，对 Agent 的 MIB 节点信息进行读写操作，并在 Agent 出现故障或错误时主动向 NMS 发送 Trap 报文报告情况，如图 69 所示；

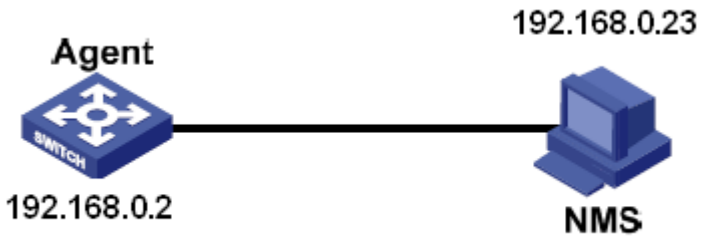


图 69 SNMPv2c 配置举例

Agent 配置如下：

1、使能 SNMP 协议和 v2c 版本状态，配置访问权限，只读团体名为 public，读写团体名为 private，见图 64、图 65；

2、使能全局 trap 模式，见图 66；

3、创建 trap 表项 111，并使能 trap 模式，版本选择 SNMP v2c，目的地址为 192.168.0.23，trap 事件选择系统、接口、认证和交换全部事件，其他采用默认配置，见图 67、图 68；

如果要对 Agent 设备的状态进行监控和管理，需要在 NMS 端运行相应的管理软件，如东土公司的 Kyvision 网管软件。NMS 端 Kyvision 软件的具体操作请参考“Kyvision 网管软件操作手册”。

5.3 SNMPv3

5.3.1 介绍

SNMP v3 提供了基于用户的安全模型（USM，User-Based Security Model）的认证机制，同时也兼容 SNMP v1 和 SNMP v2c 。用户可以配置认证和加密功能，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 NMS 和 Agent 之间的传输报文进行加密，以免窃听。通过有无认证和有无加密等功能组合，可以为 SNMP NMS 和 SNMP Agent 之间的通信提供更高的安全性。

NMS 和 Agent 的 SNMP 版本匹配是它们之间成功互访的前提条件。Agent 可以同时配置多个版本，与不同的 NMS 通信采用不同的版本。

5.3.2 实现

SNMPv3 中有 4 个配置表，每个表中可以配置 16 条表项，这些表共同决定了一个组中的用户是否可以访问 MIB 信息。

用户表创建多个用户，每个用户使用不同的安全策略实现用户认证和加密等安全功能。

组表是指多个用户的集合，访问权限是针对一个用户组的，组具有的访问权限适用于组中所有的用户。

视图表指 MIB 视图信息，以指定用户可以访问的 MIB 信息。MIB 视图可以包含某个 MIB 子树的所有节点（即允许访问 MIB 子树的所有节点），也可以不包含某个 MIB 子树的所有节点（即禁止访问 MIB 子树的所有节点）。

访问表通过匹配组名，通过相应的安全模式和安全等级来访问 MIB 节点信息。

5.3.3 Web 页面配置

1、使能 SNMP 协议，如下图所示；

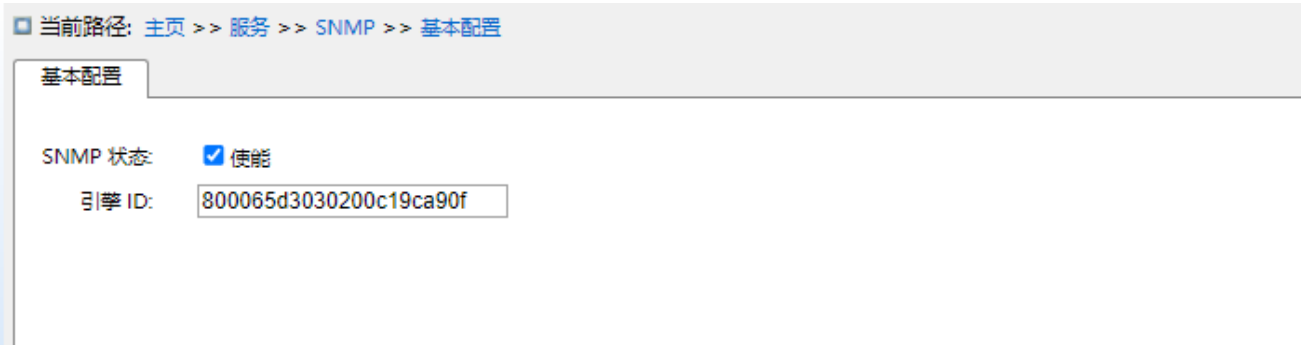


图 70 使能 SNMP 协议

模式

配置选项：使能/不使能

默认配置：使能

功能：是否使能 SNMP 协议。

引擎 ID

配置范围：偶数个十六进制数，不能为全 0 或全 F，偶数的取值范围 10~64。

功能：配置 SNMP v3 系统引擎 ID，修改引擎 ID 时，会清除用户表中相应设备 ID 对应的用户。

2、配置 trap 表项，如下图所示；

图 71 配置 trap 表项

Trap 名称

配置范围：1~32 个字符

功能：配置 trap 表项名称。

状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能该 trap 表项，使能后交换机向服务器发送相应的 trap 报文。

版本

配置选项：v1/ v2c/ v3

默认配置：v1

功能：配置交换机向服务器发送的 trap 报文版本号。

目的地址

配置格式：A.B.C.D

功能：配置接收 Trap 消息的服务器地址。

目的端口

配置选项：1~65535

功能：配置发送 trap 报文的端口号。

3、点击 trap 配置项详细信息可以看到 trap 配置详细信息，如下图所示；

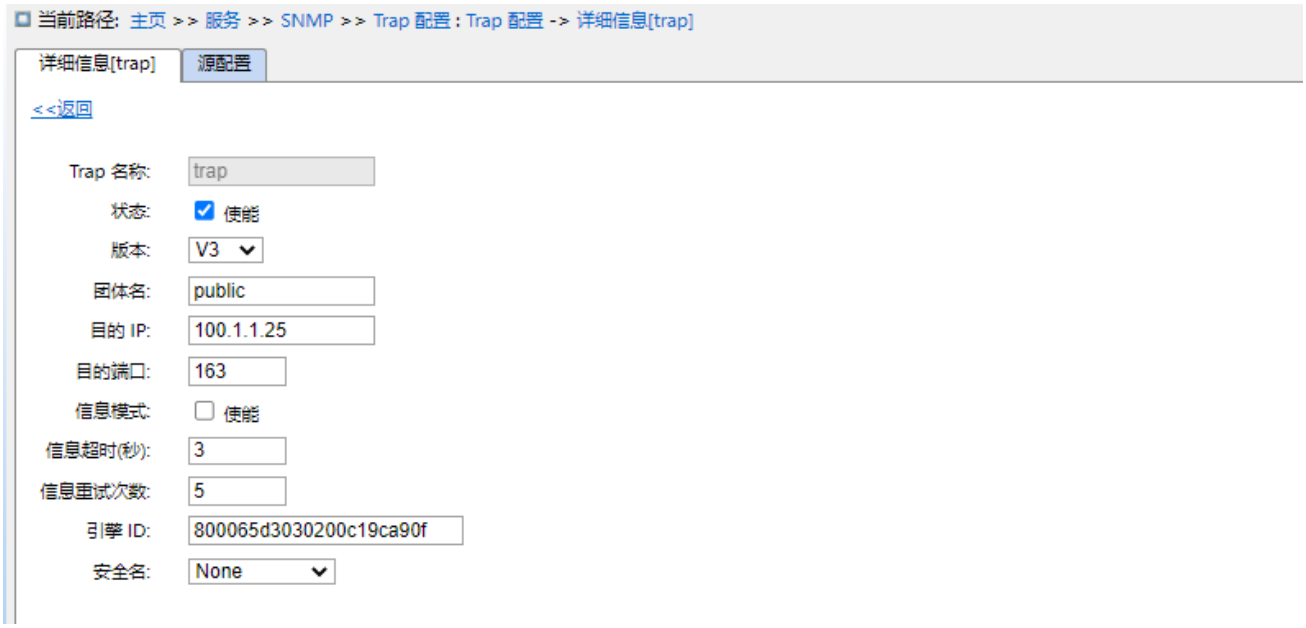


图 72 trap 详细信息

Trap 团体名

配置范围：0~255 个字符

默认配置：public

功能：配置发送 trap 报文中携带的团体名。

信息模式

配置选项：使能/不使能

默认配置：不使能

功能：服务器接收到 trap 消息后，是否向交换机发送回复信息。

信息超时

配置范围：0~2147 秒

默认配置：3 秒

功能：配置 trap 信息发送超时时间；交换机发送 trap 报文后，如果该时间段内，未收到服务器的回复，则重新发送 trap 报文。

信息重试次数

配置范围：0~255

默认配置：5

功能：配置 trap 报文超时重发的次数，如果累计的发送次数超过该配置值，服务器仍旧没有回复，则认为 trap 信息发送失败。

引擎 ID

配置范围：偶数个十六进制数，不能为全 0 或全 F，偶数的取值范围 10~64。

功能：配置 SNMP v3 trap 报文中携带安全引擎 ID 值。

4、配置 trap 事件，如下图所示；

图 73 trap 源配置

系统热启动/冷启动

配置选项：使能/不使能

默认配置：不使能

功能：系统热启动/冷启动时，是否发送 trap 报文。

RMON 下降/上升告警

配置选项：使能/不使能

默认配置：不使能

功能：RMON 产生下降/上升告警时，是否发送 trap 报文。

STP 新的根桥/拓扑改变

配置选项： 使能/不使能

默认配置：不使能

功能：STP 状态变化时，是否发送 trap 报文。

端口链路 up/链路 down

配置选项：使能/不使能

默认配置：不使能

功能：端口状态变化时，是否发送端口 up/down 的 trap 报文。

端口链路 up/链路 down

配置选项：使能/不使能

默认配置：不使能

功能：端口状态变化时，是否发送端口 up/down 的 trap 报文。

告警

配置选项：使能/不使能

默认配置：不使能

功能：有告警信息时，是否发送 trap 报文。

SNMP 认证失败

配置选项：使能/不使能

默认配置：不使能

功能：SNMP 认证失败时，是否发送 trap 报文。

LLDP

配置选项：使能/不使能

默认配置：不使能

功能：邻居状态变化时，是否发送 LLDP 的 trap 报文。

5、配置用户表，如下图所示；

图 74 配置 SNMPv3 用户表

安全名

配置范围：1~32 个字符

功能：创建用户名。

引擎 ID

配置范围：偶数个十六进制数，不能为全 0 或全 F，偶数的取值范围 10~64。

功能：配置 SNMP v3 trap 报文中携带安全引擎 ID 值。

安全等级

配置选项：NoAuthNoPriv/AuthNoPriv/AuthPriv

功能：配置当前用户的安全级别。

描述：NoAuthNoPriv 既不需要认证也不需要加密；AuthNoPriv 需要认证但不需要加密；AuthPriv 既需要认证也需要加密。

认证加密协议

配置选项：MD5/SHA

功能：选择一种认证协议。安全级别选择 AuthNoPriv/AuthPriv 时，需要配置认证协议和认证密码。

认证加密密码

配置范围：8~40 个字符（MD5 协议）8~32 个字符（SHA 协议）

功能：创建认证密码。

报文加密协议

配置选项：DES/AES

功能：选择一种加密协议。安全级别选择 Auth,Priv 时，需要配置加密协议和加密密码。

报文加密密码

配置范围：8~32 个字符

功能：创建加密密码。

最多可配置 16 个用户。

6、配置组表，如下图所示；

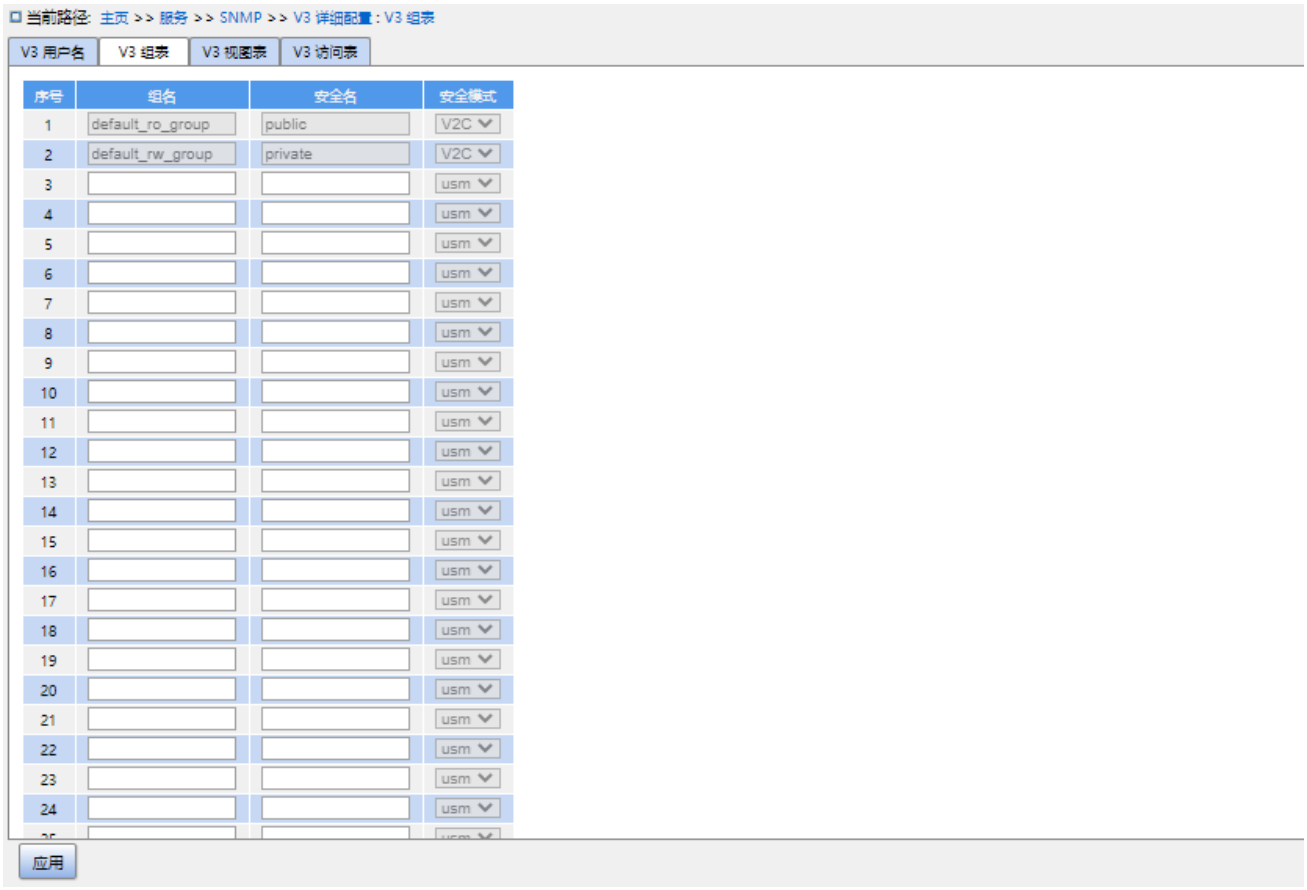


图 75 配置 SNMPv3 组表

组名

配置范围：1~32 个字符

功能：配置组表的名称，组名相同的用户属于同一个组。

安全模式

默认配置：usm

功能：选择当前组的 usm（基于用户的安全模型）技术，目前该选项强制为 usm 模式。

安全名

配置范围：已创建的用户名，1~32 个字符

功能：配置安全名，安全名应和用户表中的用户名配置一致。组名相同的用户属于同一个组。

最多可配置 32 个组表。

7、配置视图表，如下图所示；

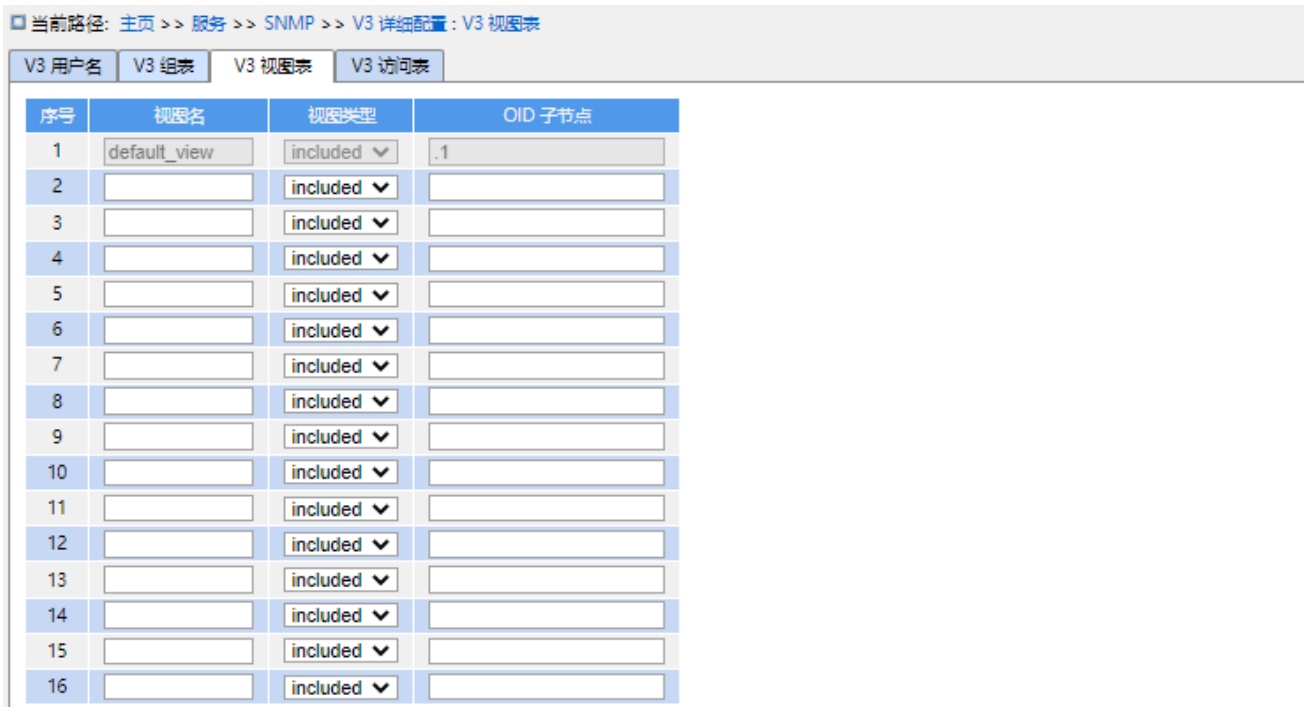


图 76 配置 SNMPv3 视图表

视图名

配置范围：1~32 个字符

功能：配置视图名。

视图类型

配置选项：included/excluded

功能：included 表示当前视图包括该 MIB 子树的所有节点；excluded 表示当前视图不包括该 MIB 子树的任何节点。

OID 子节点

功能：配置 MIB 子树，用子树根节点的 OID 表示。

最多可配置 16 个视图表。

说明：

交换机中缺省存在视图表 default_view 包含 1 子树的所有节点。

8、配置访问表，如下图所示；

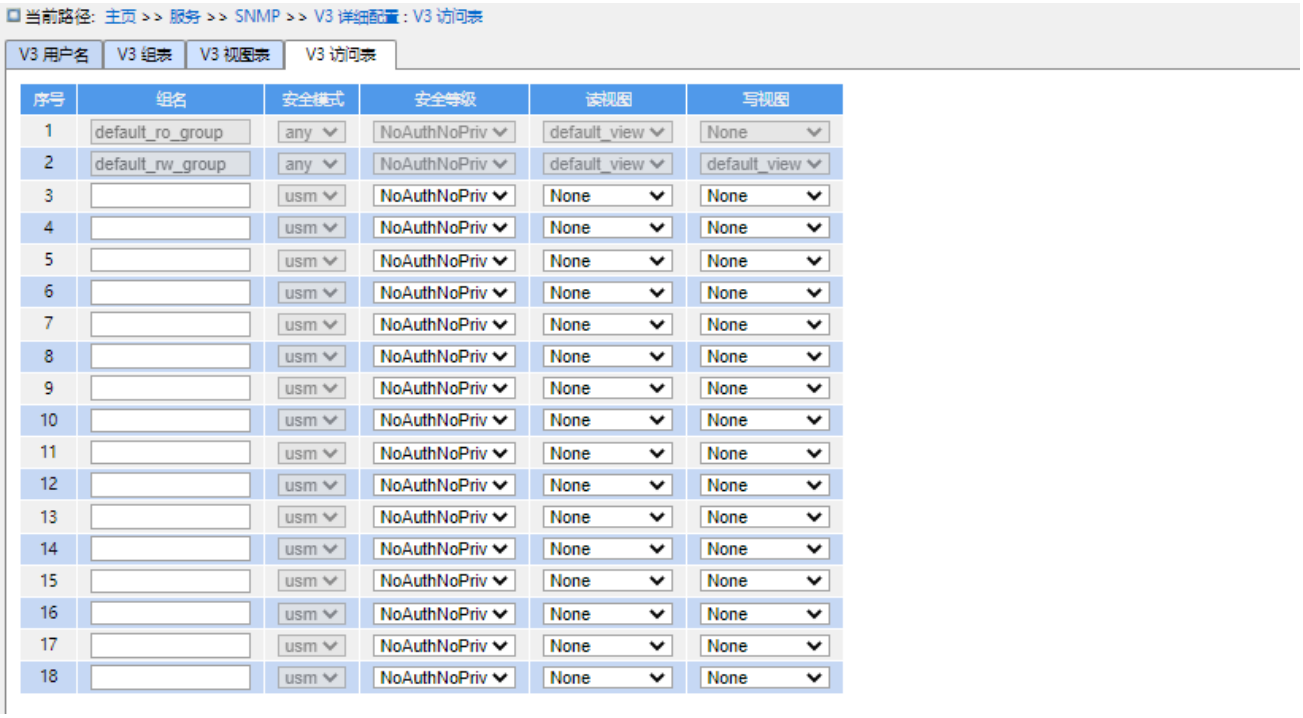


图 77 配置 SNMPv3 访问表

组名

配置范围：已创建的组名，1~32 个字符

描述：一个组中的所有用户具有相同的访问权限。

安全模式

默认配置：any/v1/v2/usm

功能：选择当前组访问交换机时采用 USM（基于用户的安全模型）技术，any 指可以采用任何一种安全模式。组名称、安全模式的配置应和组表中的组名、安全模式配置一致。

安全等级

配置选项：NoAuthNoPriv/AuthNoPriv/AuthPriv

功能：配置当前组的安全级别。

描述：NoAuthNoPriv 既不需要认证也不需要加密；AuthNoPriv 需要认证但不需要加密；AuthPriv 既需要认证也需要加密。需要加密时，NMS 侧的认证/加密协议、认证/加密密码应与用户表中的配置保持一致，才能成功访问交换机相应节点信息。

NoAuthNoPriv、AuthNoPriv、AuthPriv 安全级别依次递增，低级别的安全级别允许高级别的安全级别访问。如配置一个组的安全级别为 AuthNoPriv，则该组中安全级别为 AuthNoPriv 和 AuthPriv 的用户在认证/加密协议和认证/加密密码都正确的情况下都可以成功访问交换机；

但安全级别为 NoAuth,NoPriv 的用户无法访问。

读视图

配置选项：default_view/None/已创建的视图名

功能：选择只读视图名。

写视图

配置选项：default_view/None/已创建的视图名

功能：选择读写视图名。

最多可配置 16 个访问表项（不包括缺省的 2 个表项）。

说明：

交换机中缺省存在访问表{default_ro_group, any, NoAuth,NoPriv, default_view, None}、{default_rw_group, any, NoAuth,NoPriv, default_view, default_view}。

5.3.4 典型配置举例

SNMP 管理站与交换机通过以太网相连，管理站 IP 地址为 192.168.0.23，交换机 IP 地址为 192.168.0.2。用户名 1111 和用户 2222 通过 SNMPv3 对 Agent 进行监控管理，安全等级采用 AuthNoPriv，可以对 Agent 中所有节点信息进行只读操作；agent 有告警时主动向 NMS 发送 trap v3 报文，如图 78 所示；

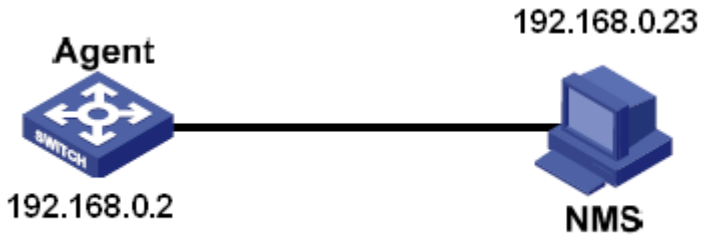


图 78 SNMPv3 配置举例

Agent 配置如下：

1、使能 SNMP 协议，见图 70；

2、配置 SNMP v3 用户表

用户名：1111，安全级别：Auth,Priv，认证协议：MD5，认证密码：aaaaaaaa，加密协议：DES，加密密码：xxxxxxxx；

用户名：2222，安全级别：Auth,Priv，认证协议：SHA，认证密码：bbbbbbbb，加密协

议：AES，加密密码：yyyyyyyy；见图 74；

3、创建 group 组，安全模式 usm，包含用户 1111 和 2222，见图 75；

4、配置 SNMP v3 访问表

组名称：group，安全模式：usm，安全等级：Auth,NoPriv，读视图名：default_view，写视图名：None，见图 77；

5、使能 trap 模式，见图 71；

6、创建 trap 表项 222，并使能 trap 模式，版本选择 SNMP v3，目的地址为 192.168.0.23，trap 事件选择系统、接口、认证和交换全部事件，其他采用默认配置；

如果要对 Agent 设备的状态进行监控和管理，需要在 NMS 端运行相应的管理软件。

5.4 SSH 配置

5.4.1 介绍

SSH（Secure Shell，安全外壳）是进行安全远程登陆的网络协议，SSH 对所传输的数据进行加密防止信息泄露，在这种加密情况下用户使用命令行对交换机进行配置。

该系列设备支持 SSH 服务器功能，同一时间允许多个 SSH 用户连接，从而通过 SSH 登陆到远程设备上。

5.4.2 实现

在通信过程中为实现 SSH 的安全连接，服务器与客户端之间要经历五个阶段：

版本号协商阶段：SSH 目前包括 SSH1 和 SSH2 两个版本，双方通过版本协商确定使用的版本；

密钥和算法协商阶段：SSH 支持多种加密算法，双方根据所支持的算法协商出最终使用的算法；

认证阶段：SSH 客户端向服务器端发起认证请求，服务器端对客户端进行认证；

会话请求阶段：认证通过后，客户端向服务器端发送会话请求；

会话阶段：会话请求通过后，服务器端和客户端进行信息交互。

5.4.3 Web 页面配置

1、使能 SSH 协议，如图 79 所示；

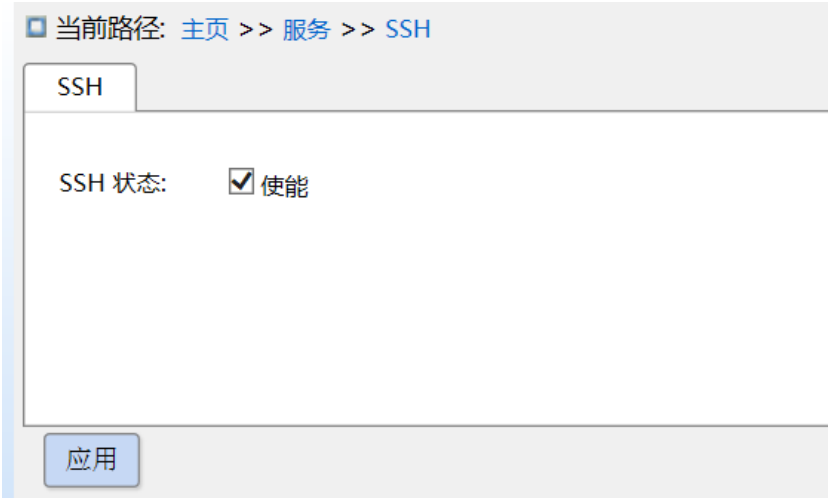


图 79 使能 SSH 协议

SSH 状态

配置选项：使能/不使能

默认配置：使能

功能：是否使能 SSH 协议，使能时，设备作为 SSH 服务器。

5.4.4 典型配置举例

Host 做为 SSH 客户端与 Switch 建立本地连接，如图 80 所示；

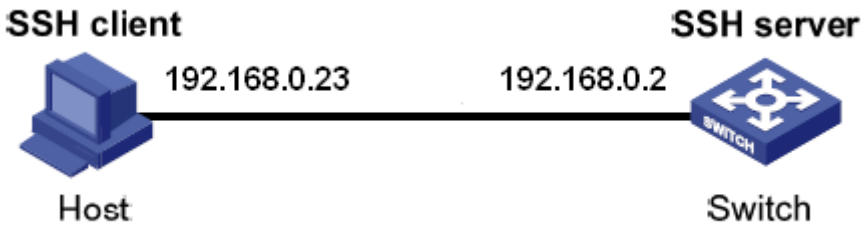


图 80 SSH 配置举例

1、使能 SSH 协议，见图 79；

2、建立与 SSH 服务器端的连接，打开 PuTTY.exe 软件如图 81 所示，在 Host Name（ or IP address）中输入 SSH 服务器 IP 地址：192.168.0.2；

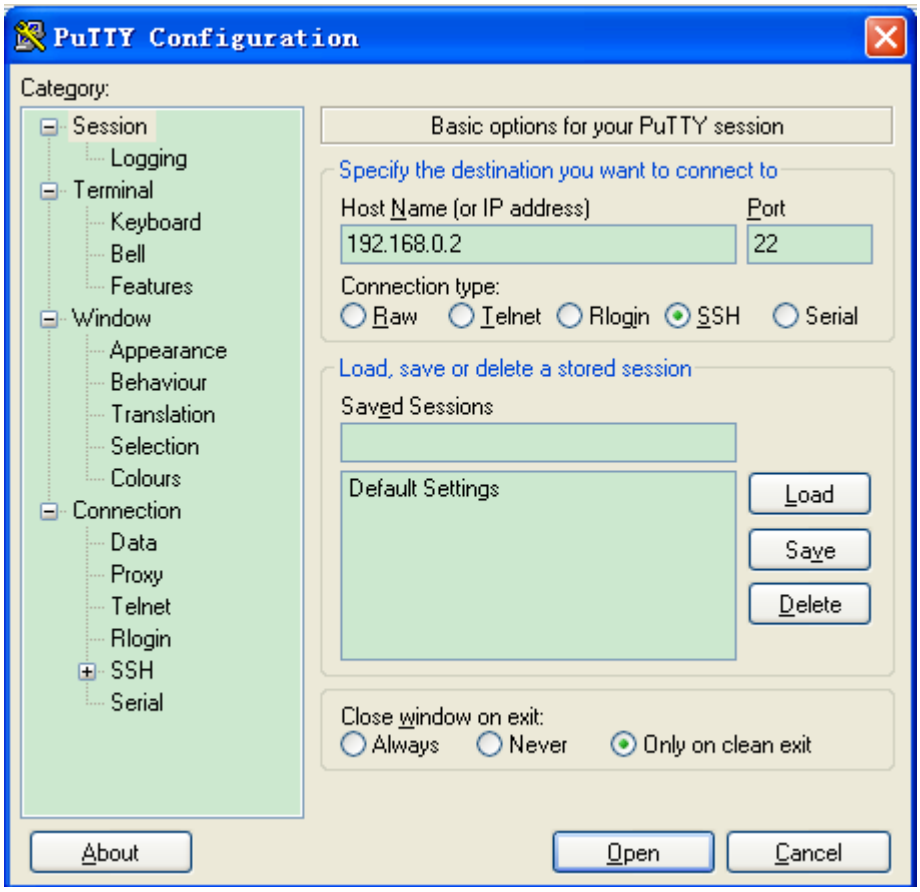


图 81 SSH 客户端配置

4、点击<Open>按钮，出现如图 82 所示警告信息时，点击<是（Y）>按钮；

图 82 警告信息

5、按提示输入用户名：admin 和密码为”123”，便可以进入交换机配置页面，如图 83 所

示。

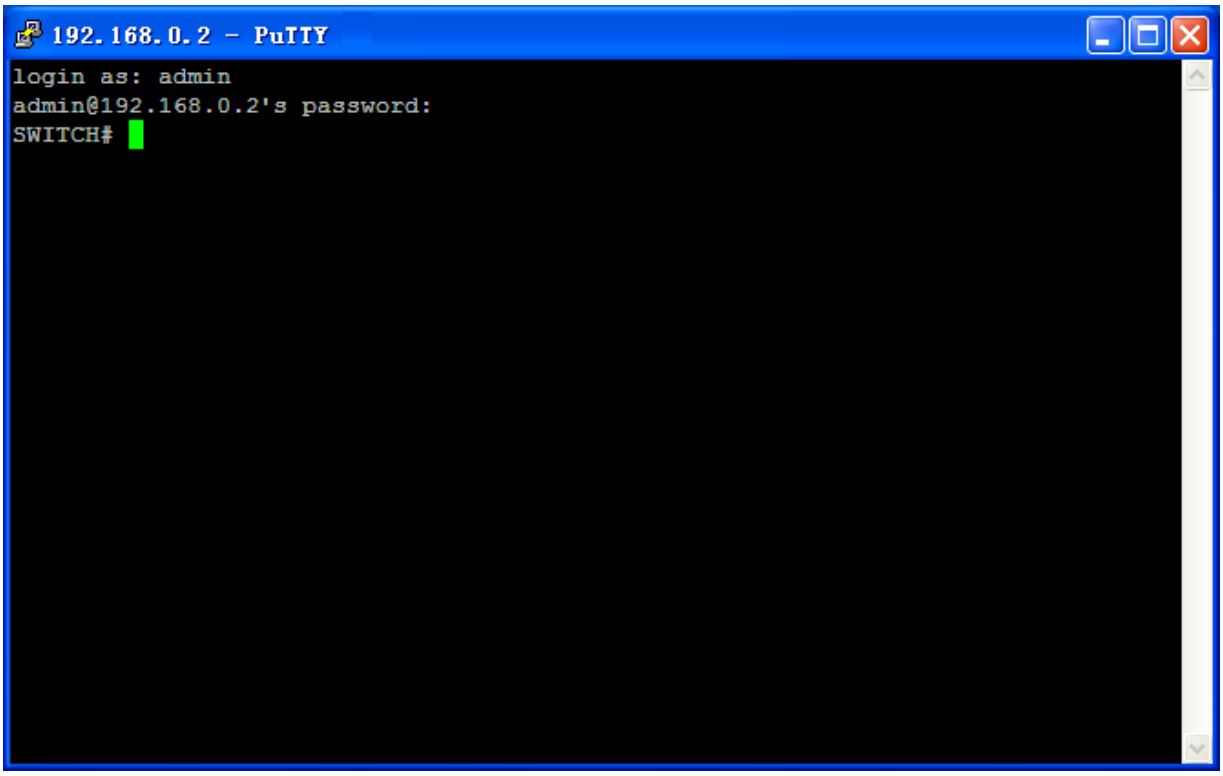


图 83 SSH 密码认证方式登陆界面

5.5 TACACS+配置

5.5.1 介绍

TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）是一种基于 TCP 传输协议的应用，采用客户端/服务器模式实现 NAS（Network Access Server，网络接入服务器）与 TACACS+服务器之间的通信，客户端运行于 NAS 上，服务器上集中管理用户信息。NAS 对于用户来说是服务器端，对于服务器来说是客户端，结构示意图如图 84 所示。

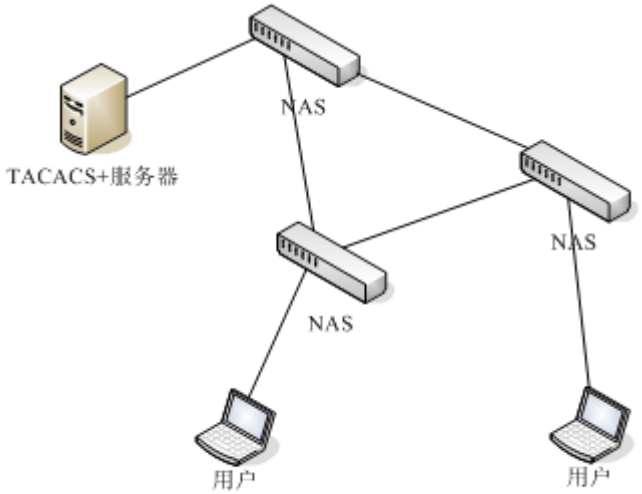


图 84 TACACS+结构示意图

该协议对需要登陆到设备上进行操作的终端用户进行认证、授权、计费。设备作为 TACACS+的客户端，将用户名和密码发给 TACACS+服务器进行验证，服务器接受客户的 TCP 连接，并对认证请求进行响应，验证用户是否属于合法用户，用户验证通过并得到授权后可以登陆到设备上进行操作。

5.5.2 Web 页面配置

1、TACACS+服务器配置，如下图所示；

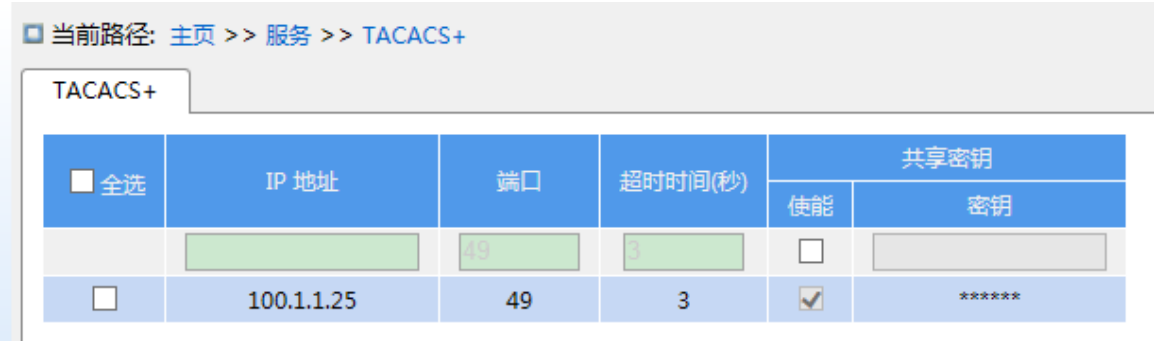


图 85 TACACS+服务器配置

IP 地址

功能：配置 TACACS+服务器的 IP 地址，最多支持 5 个 TACACS+服务器。

端口

配置范围：1~65535

默认配置：49

功能：配置 TACACS+服务器的 TCP 认证端口号。

超时时间

配置范围：1~1000s

功能：配置 TACACS+服务器应答超时时间；设备发送 TACACS+请求报文后，如果该时间段内，未收到 TACACS+服务器的响应，则本次认证失败，设备认为该服务器处于失效状态。

共享密钥

配置范围：0~63 个字符

功能：配置设备和 TACACS+服务器的共享密钥，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，彼此才能接受对方发来的报文并作出响应，因此必须保证设备上配置的共享密钥与 TACACS+服务器上的密钥值完全一样。

5.5.3 典型配置举例

图 86 所示，通过 Switch 实现 TACACS+服务器对用户进行认证、授权。服务器 IP 地址为 192.168.0.23，交换机与服务器交互报文时的共享密钥为 aaa。

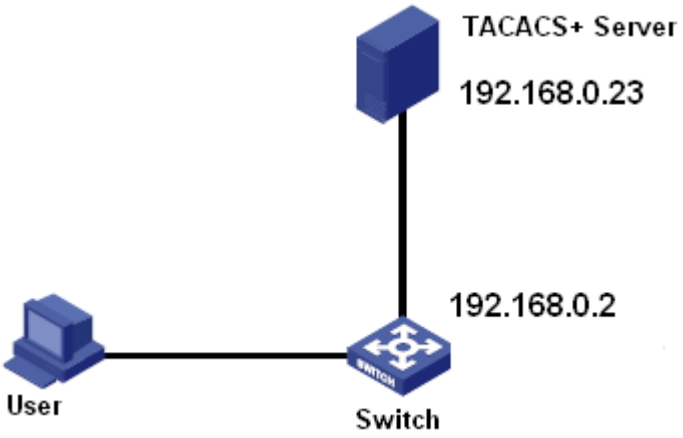


图 86 TACACS+认证举例

1、服务器信息配置，IP 地址为 192.168.0.23，共享密钥为 aaa，见图 85；

2、Web 登陆时采用本地认证；Telnet 登陆时采用 TACACS+认证，见图 13；

3、TACACS+服务器上配置用户名和密码 bbb，密钥值 aaa；

4、Web 登陆交换机时输入用户名 admin，密码 123 便可通过本地认证成功访问交换机；

5、Telnet 登陆交换机时输入用户名和密码 bbb 便可通过 TACACS+认证成功访问交换机。

5.6 RADIUS 配置

5.6.1 介绍

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的信息交互协议，该协议定义了基于UDP的RADIUS帧格式及其消息传输机制，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

该协议采用客户端/服务器模式实现NAS（Network Access Server，网络接入服务器）与RADIUS服务器之间的通信，RADIUS客户端运行于NAS上，RADIUS服务器上集中管理用户信息。NAS对于用户来说是服务器端，对于RADIUS服务器来说是客户端，结构示意图如图 87 所示；

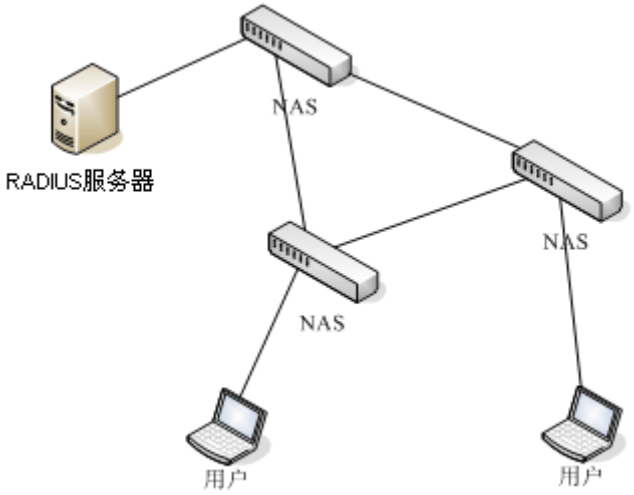


图 87 RADIUS 结构示意图

该协议对需要登陆到设备上进行操作的终端用户进行登陆认证。设备作为 RADIUS 的客户端，将用户发送过来的认证信息发给 RADIUS 服务器进行认证，并根据 RADIUS 服务器的认证结果允许/拒绝用户登陆设备。

5.6.2 Web 页面配置

1、RADIUS 服务器配置，如下图所示；

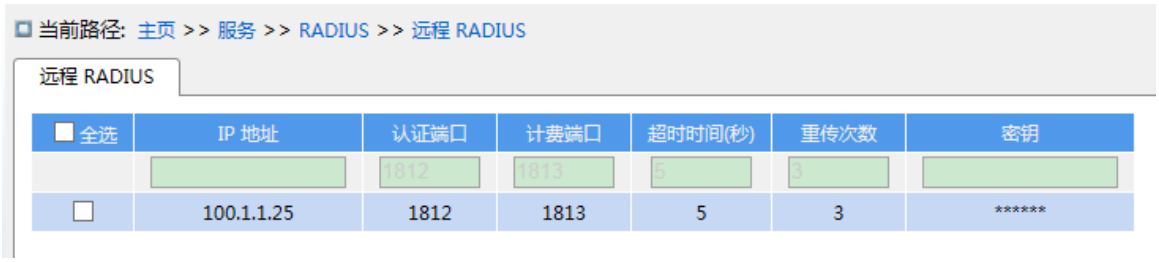


图 88 RADIUS 服务器配置

IP 地址

功能：配置 RADIUS 服务器的 IP 地址，最多支持 5 个 RADIUS 服务器。

认证端口

配置范围：0~65535

默认配置：1812

功能：配置 RADIUS 服务器的 UDP 认证端口号。

计费端口

配置范围：0~65535

默认配置：1813

功能：配置 RADIUS 服务器的 UDP 计费端口号。由于 RADIUS 协议采用不同的 UDP 端口来收发认证和计费报文，因为必须将认证和计费端口号配置得不同。

超时时间

配置范围：1~1000s

默认配置：5s

功能：配置 RADIUS 服务器应答超时时间；设备发送 RADIUS 请求报文后，如果该时间段内，未收到 RADIUS 服务器的响应，则重新发送 RADIUS 请求报文。

重传次数

配置范围：1~1000

默认配置：3

功能：配置 RADIUS 请求报文超时重传的次数，如果累计的传送次数超过该配置值，RADIUS 服务器仍旧没有响应，则本次认证失败，设备认为该服务器处于失效状态。

密钥

配置范围：0~63 个字符

功能：配置设备和 RADIUS 服务器的共享密钥，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，彼此才能接受对方发来的报文并作出响应，因此必须保证设备上配置的共享密钥与 RADIUS 服务器上的密钥值完全一样。

2、RADIUS 客户端全局配置，如下图所示；

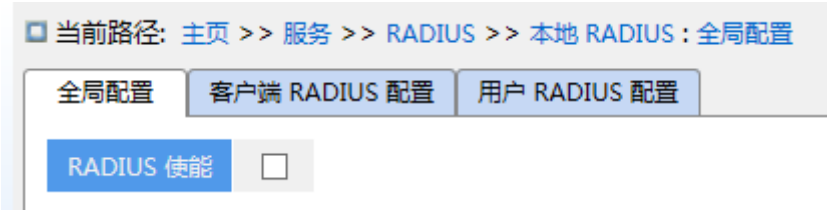


图 89 RADIUS 客户端全局配置

RADIUS 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能本地 RADIUS 为其他设备作为 RADIUS 服务器使用。

3、RADIUS 客户端配置，如下图所示；

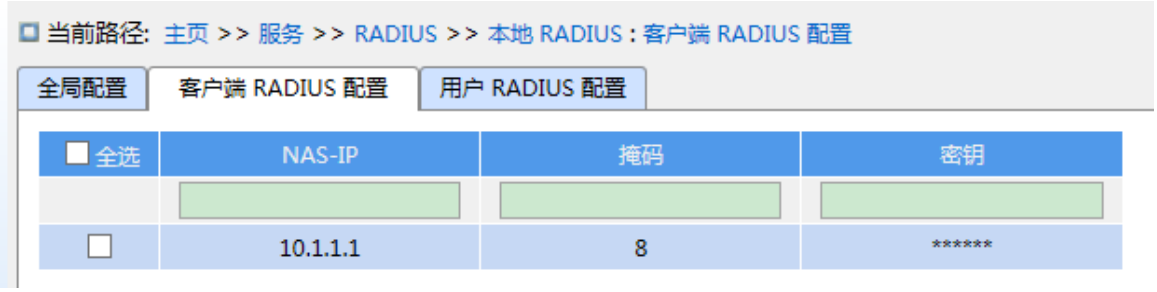


图 90 RADIUS 客户端配置

NAS-IP

功能：配置 RADIUS 客户端的 IP 地址或 IP 地址段。

掩码

配置范围：1-32

功能：配置 RADIUS 客户端地址网段，同一网段的 IP 地址只需配置一个网段即可。

密钥

配置范围：1~63 个字符

功能：配置设备和 RADIUS 客户端的共享密钥，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，彼此才能接受对方发来的报文并作出响应，因此必须保证设备上配置的共享密钥与 RADIUS 客户端上的密钥值完全一样。

4、RADIUS 用户配置，如下图所示；

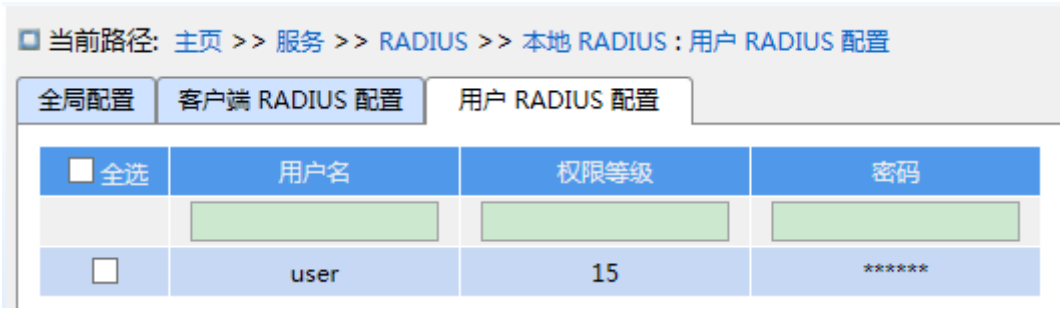


图 91 RADIUS 用户配置

用户名

配置范围：1~31 字符

功能：配置 RADIUS 用户名。

权限等级

配置范围：1~15

功能：配置该用户的权限等级。不同权限等级的用户具有不同的访问权限。

密码

配置范围：1~31 字符

功能：配置该用户登陆密码。

5.6.3 典型配置举例

如图 92 所示，Switch 的端口 1 使能 IEEE802.1X 协议，用户需通过 RADIUS 服务器进行认证打开端口 1 登陆到 Switch 上。服务器 IP 地址为 192.168.0.23，Switch 与服务器交互报文时的共享密钥为 aaa。

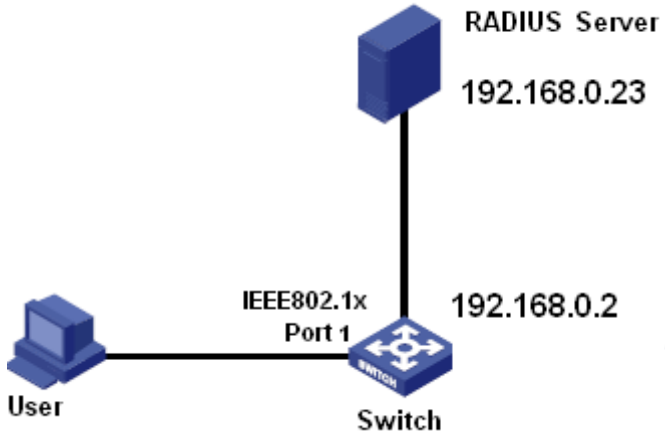


图 92 RADIUS 认证举例

1、配置认证服务器 IP 地址为 192.168.0.23，密码为 aaa，见图 88。

2、IEEE802.1X 功能配置：全局使能 IEEE802.1X 功能，认证方式选择 Radius，配置端口 1 的管理状态为基于端口的 802.1X，其它配置保持默认。

3、在 RADIUS Server 上配置用户名和密码为 ccc，密钥为 aaa；

4、在 PC 上安装运行 802.1X 认证客户端软件，输入用户名和密码 ccc，用户可通过认证访问交换机。

5.7 DNS

5.7.1 介绍

域名系统（DNS，Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的域名解析服务器将域名解析为正确的 IP 地址。

域名解析分为静态域名解析和动态域名解析，二者可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。

静态域名解析就是手工建立域名和IP地址之间的对应关系。当用户使用域名进行某些应用（如telnet应用）时，系统查找静态域名解析表，从中获取指定域名对应的IP地址。

5.7.2 Web 页面配置

1、使能 DNS 代理、配置网域名称

图 93 DNS 配置

DNS 代理

配置选项：不使能/使能

默认配置：不使能

功能：是否使能 DNS 代理功能。

网域名称

配置范围：域名的格式为***.***.com，并且***的长度不能超过 63 字符，其总长度不超过 251 字符

默认配置：空

功能：设备使用客户端请求域名直接向服务器进行地址解析失败后，添加此域名后缀再次向 DNS 服务器解析。

2、DNS 服务器配置

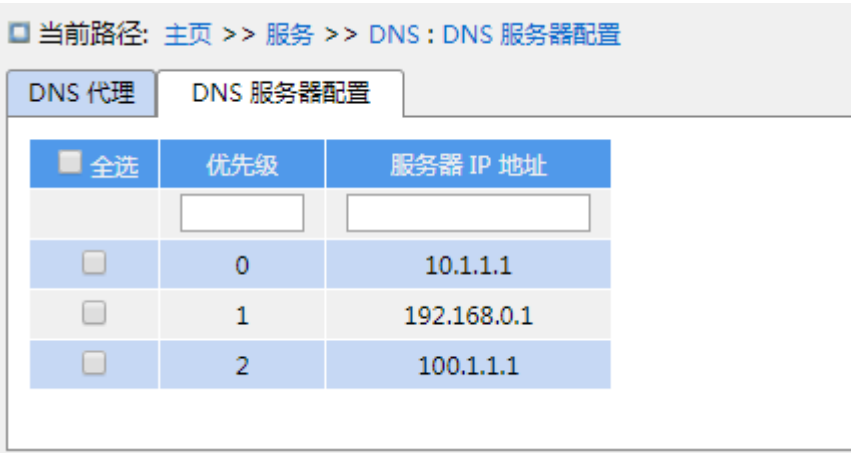


图 94 DNS 服务器配置

优先级

配置范围：0、1、2

默认配置：无

功能：代理设备按照优先级先后顺序，以此向指定的 DNS 服务器进行地址解析，直到解析成功。

服务器 IP 地址

配置格式：A.B.C.D

功能：手动配置 DNS 服务器 IP 地址。

5.7.3 典型配置举例

如下图所示，DNS 客户端有时候不能或者不必须直接配置成 DNS 服务器地址，这时就可以通过在交换机上设置 DNS 代理后直接把客户端的 DNS 地址设置成 DNS 代理的地址即可。在配置域名后缀列表后，DNS 代理在一次请求失败后，再次发送 DNS 解析请求时会自动把域名加上所配置的后缀。

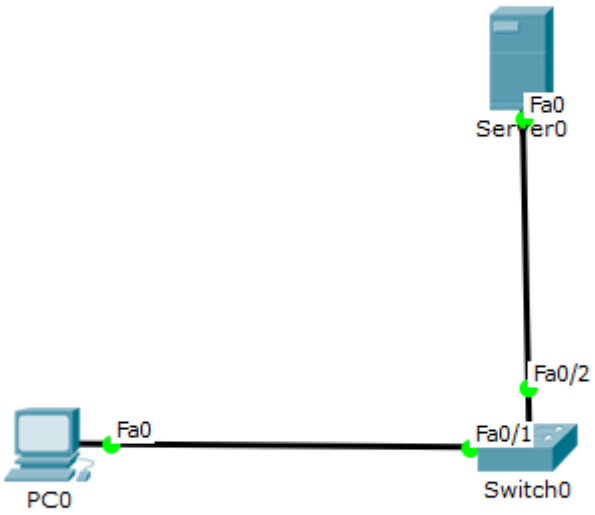


图 95 DNS 代理配置配置示例

1、配置 DNS 服务器 IP 地址为 192.168.0.254/24。

2、配置 PC 的 IP 地址为 192.168.1.2/24，DNS 服务器为 192.168.1.1；

3、配置 Switch0 接口 Fa1/1 以 access 模式加入 VLAN 1，配置三层接口 IP 为 192.168.1.1/24，接口 Fa1/2 以 access 模式加入 VLAN 2，配置三层接口 IP 为 192.168.0.1/24；

4、Switch0 上开启 DNS 代理，配置 DNS服务器地址为 192.168.0.254，配置域名后缀为 abc.com，从而可以实现交换机代理 DNS 服务器进行 DNS 域名解析。

5.8 RMON

5.8.1 介绍

RMON（Remote Network Monitoring，远程网络监视）基于SNMP体系结构使网络中管理设备能够积极主动的对被管理设备进行监控和管理。RMON包括网络管理站和网络上的Agent，管理站对网络中的Agent进行管理；Agent可以统计端口上的各种流量信息。

RMON主要实现统计和告警功能，统计功能指Agent可以按周期统计端口的各种流量信息，比如某段时间内某网段上收到的报文总数等。告警功能指Agent能监控指定MIB变量的值，当该值达到告警阈值时（比如报文总数达到指定值），能自动记录告警事件到RMON日志或者向管理设备发送Trap消息。

5.8.2 RMON 组

RMON规范（RFC2819）中定义了多个RMON 组，该系列设备实现了公有MIB 中支持的统计组、历史组、事件组和告警组。

- 统计组

统计组指系统对端口的各种流量信息进行统计，并将统计结果存储在以太网统计表中以便管理设备随时查看。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。

- 历史组

历史组规定系统定期对端口各种流量信息进行采样，并将采样值存储在历史记录表中以便管理设备随时查看。历史组统计的是采样间隔内各种数据的统计值。

- 事件组

事件组用来定义事件索引号及事件处理方式。事件组定义的事件用于告警组配置项中，当监控对象达到告警条件时，就会触发事件，事件有如下几种处理方式：

Log：将事件相关信息记录在本设备RMON日志表中。

Trap：向网管站发送Trap消息告知该事件的发生。

Log-Trap：既在本设备上记录RMON日志，又向网管站发送Trap消息。

None：不做任何处理。

- 告警组

RMON 告警管理可对指定的告警变量进行监视。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

注意：

当告警变量的采样值在同一方向连续多次超过阈值时，只在第一次产生告警事件，后面几次不会产生告警事件，即上限告警和下限告警是交替产生的，出现了一次上限告警，则下一次一定下限告警。

5.8.3 Web 页面配置

1、配置统计组，如下图所示；

图 96 配置 RMON 统计组

ID

配置范围：1~65535

功能：配置统计信息表项的编号，最多支持 128 条统计表项。

数据源

配置选项：1000001-1000024

功能：选择统计哪个端口的信息。

2、查看统计组状态，如下图所示；

图 97 查看 RMON 统计组状态

丢弃：该端口丢弃的报文数；

字节：该端口接收的所有字节数；

报文：该端口接收的所有报文数；

广播：该端口接收的广播报文数；

组播：该端口接收的组播报文数；

CRC 错误：指端口接收到字节数为 64~9600 字节的 CRC 错误报文；

过小：指端口接收到字节数小于 64 字节的报文；

过大：指端口接收到字节数大于 9600 字节的报文；

Frag.：指端口接收到字节数小于 64 字节的 CRC 错误报文；

Jabb.：指端口接收到字节数大于 9600 字节的 CRC 错误报文；

Coll.：指端口接收到半双工模式下的冲突帧；

64 字节：指端口接收到字节数为 64 字节的报文；

65~127：指端口接收到字节数为 65~127 字节的报文；

128~255：指端口接收到字节数为 128~255 字节的报文；

256~511：指端口接收到字节数为 256~511 字节的报文；

512~1023：指端口接收到字节数为 512~1023 字节的报文；

1024~1588：指端口接收到字节数为 1024~1588 字节的报文。

说明：

过大报文字节数由端口配置中“最大报文大小”参数而定，见 7.1 端口配置。本实例中以最大报文大小为 9600 字节进行说明。

3、配置历史组，如下图所示；

图 98 配置 RMON 历史组

ID

配置范围：1~65535

功能：配置历史控制表项的编号，最多支持 256 条历史控制表项。

数据源

配置选项：10000portid

功能：选择对哪个端口信息进行采样。

间隔

配置范围：1~3600s

默认配置：1800s

功能：配置端口信息的采样周期。

Buckets

配置范围：1~65535

默认配置：50

功能：配置 RMON 中保存的端口信息最新采样值的个数。

4、查看历史组状态，如下图所示；

历史索引	样本索引	样本开始	丢弃	字节	报文	广播	组播	CRC错误	过小	过大	Frag.	Jabb.	Coll.	利用率
2	104	595858	0	117942	487	54	11	0	0	0	0	0	0	0
2	105	595918	0	118133	461	3	24	0	0	0	0	0	0	0
2	106	595978	0	116802	453	3	21	0	0	0	0	0	0	0
2	107	596038	0	119633	476	10	32	0	0	0	0	0	0	0
2	108	596098	0	119283	474	20	20	0	0	0	0	0	0	0
2	109	596158	0	120150	494	39	33	0	0	0	0	0	0	0
2	110	596218	0	118550	463	12	17	0	0	0	0	0	0	0
2	111	596278	0	116002	454	11	19	0	0	0	0	0	0	0
2	112	596338	0	118200	462	11	17	0	0	0	0	0	0	0
2	113	596398	0	116531	453	1	26	0	0	0	0	0	0	0

图 99 查看 RMON 历史组状态

5、配置事件控制组，如下图所示；

图 100 配置 RMON 事件控制组

ID

配置范围：1~65535

功能：配置事件控制表项的索引号，最多支持 128 条统计表项。

描述

配置范围：0~127 个字符

功能：对事件的描述。

类型

配置选项：none/log/snmptrap/logandtrap

默认配置：none

功能：配置当告警发生时所采用的事件类型，即对告警的处理方式。

上次事件

功能：显示该事件上次被采用的 sysUpTime 值。

6、查看事件组状态，如下图所示；

图 101 查看 RMON 事件组状态

7、配置告警控制组，如下图所示；

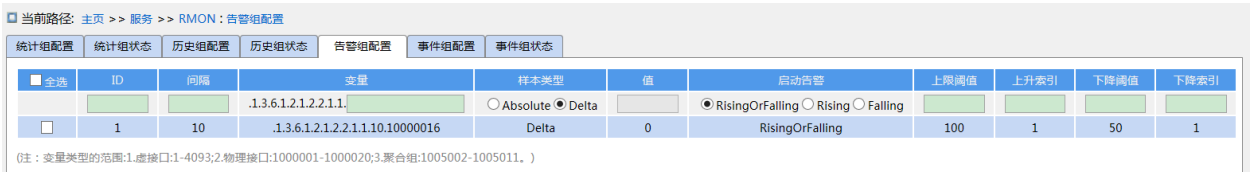


图 102 配置 RMON 告警控制组

ID

配置范围：1~65535

功能：配置告警控制表项的编号，最多支持 256 条告警控制表项。

间隔

配置范围：1~2147483647s

默认配置：30s

功能：配置端口信息的采样周期。

变量

配置格式：A.10000portid/A.vlanid

配置范围：A：10~21

功能：选择需要监测的端口 MIB 信息。

InOctets: A=10，该端口接收的所有字节数。

InUcastPkts: A=11，该端口接收的单播报文数。

InNUcastPkts: A=12，该端口接收的组播和广播报文数。

InDiscards: A=13，该端口丢弃的报文数。

InErrors: A=14，指端口接收的错误报文数。

InUnknownProtos: A=15，指端口接收的未知报文数。

OutOctets: A=16，该端口发送的所有字节数。

OutUcastPkts: A=17，该端口发送的单播报文数。

OutNUcastPkts: A=18，该端口发送的组播和广播报文数。

OutDiscards: A=19，该端口发送的被丢弃报文数。

OutErrors: A=20，该端口发送的错误报文数。

OutQLen: A=21，该端口出队列的报文长度。

样本类型

配置选项：Absolute/Delta

默认配置：Delta

功能：配置采样值与阈值的比较方式。

描述：Absolute 直接方式将每次采样值直接与阈值进行比较；Delta 差值方式将本次采样值减去上一次的采样值，将差值再与阈值进行比较。

启动告警

配置选项：Rising/Falling/RisingOrFalling

默认配置：RisingOrFalling

功能：选择报警的类型，包括上升沿告警、下降沿告警、上升沿和下降沿都告警。

上升阈值

配置范围：1~2147483647

功能：配置配置上升沿阈值，当采样值超过该上升沿阈值并且报警类型为 RisingAlarm 或者 RisingOrFalling 时，将会报警并激活上升事件索引。

上升索引

配置范围：1~65535

功能：配置上升事件的索引，即对上升沿告警的处理方式。

下降阈值

配置范围：1~2147483647

功能：配置下降沿阈值，当采样值低于该下降沿阈值并且报警类型为 Falling 或者 RisingOrFalling 时，将会报警并激活下降事件索引。

下降索引

配置范围：1~65535

功能：配置下降事件的索引，即对下降沿告警的处理方式。

6 告警

6.1 介绍

该系列设备支持以下几种类型的告警：

- 电源告警：使能情况下，电源模块掉电或异常时会产生告警；
- IP/MAC 冲突：使能情况下，IP/MAC 地址冲突时会产生告警；
- 内存及 CPU 利用率告警：使能情况下，内存及 CPU 利用率超过设定阈值时产生告警；
- 端口告警：使能情况下，端口 Link down 时会产生告警；
- 端口流量告警：使能情况下，端口的入方向/出方向流量超过设定阈值时产生告警；
- CRC 错误及丢包率告警：使能情况下，端口 CRC 错误及丢包率超过设定阈值时产生告警；
- 环告警：使能情况下，环开时会产生告警。
- DDM 告警：使能情况下，光模块传输功率低于阈值时会产生告警。

6.2 Web 页面配置

1、基本告警配置与显示，如下图所示；

图 103 基本告警

电源告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能电源告警。

电源告警状态

显示选项：正常/告警

功能：显示电源工作状态。告警表示双电源模块中一个电源模块掉电或异常，产生告警；正常表示单电源模块工作或者双电源模块中两个电源均正常供电。

IP、MAC 冲突告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能地址冲突告警。

状态

显示选项：IP 冲突/MAC 冲突/正常

描述：使能冲突告警后，有冲突时显示冲突提示，否则显示正常。

检测时间

配置范围：180~600s

默认：300s

功能：配置检测地址冲突的时间间隔。

CPU/内存利用率告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 CPU/内存利用率。

阈值（%）

配置范围：50~100

默认配置：85

功能：配置交换机 CPU/内存利用率阈值，该交换机的 CPU/内存利用率大于该值时，产生 CPU/内存利用率超阈值告警。

浮动值（%）

配置范围：1~20

默认配置：5

功能：配置交换机 CPU/内存利用率浮动值。

说明：当产生 CPU/内存利用率超阈值告警时，为防止 CPU/内存利用率在阈值附近波动

造成频繁的告警和告警解除，可配置一浮动值(默认为 5%)，只有当 CPU/内存利用率比阈值低一个浮动值时，告警才会解除。例如：设置交换机内存利用率阈值为 60%，浮动值为 5%，当交换机的实际内存利用率≤60%时，无告警发生；当交换机的实际内存利用率≥61%时，产生内存利用率超阈值告警；此时，只有当交换机的实际内存利用率≤55%时，内存利用率超阈值告警才会解除。

高温告警 /低温告警

配置选项：使能不使能

默认配置：不使能

功能：显示交换机工作的温度状态。告警表示交换机温度突破高温/低温门限值，产生告警；正常表示交换机温度正常。

阈值（℃）

配置范围：-40~+80

功能：配置高温/低温的温度。

2、端口告警配置与显示，如下图所示；

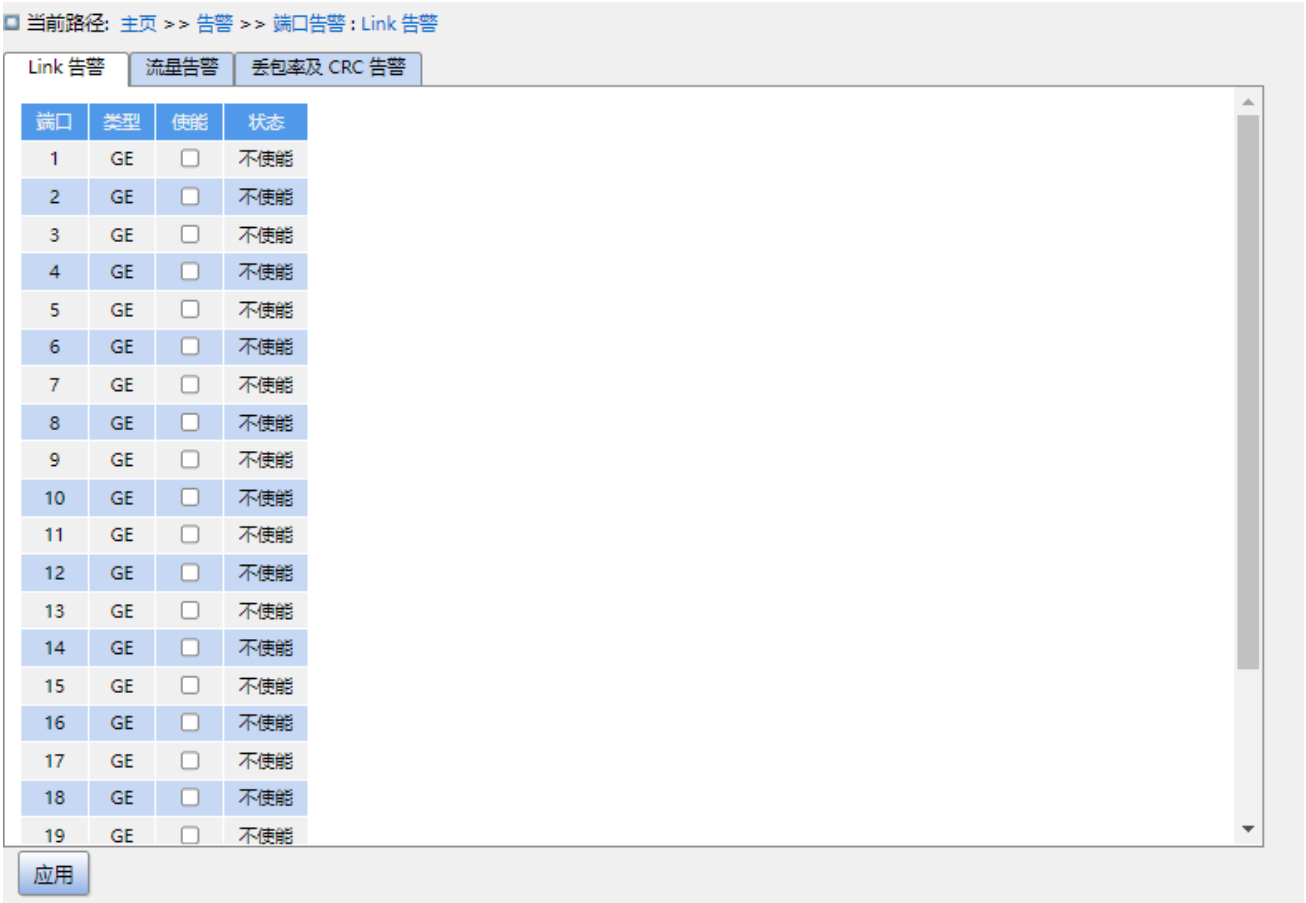


图 104 端口告警

端口告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口告警。

状态

显示选项：不使能/Up/Down

描述：使能端口告警后，端口连接正常时显示 Up，端口断开或者连接异常时显示 Down。

3、端口流量告警配置与显示，如下图所示；

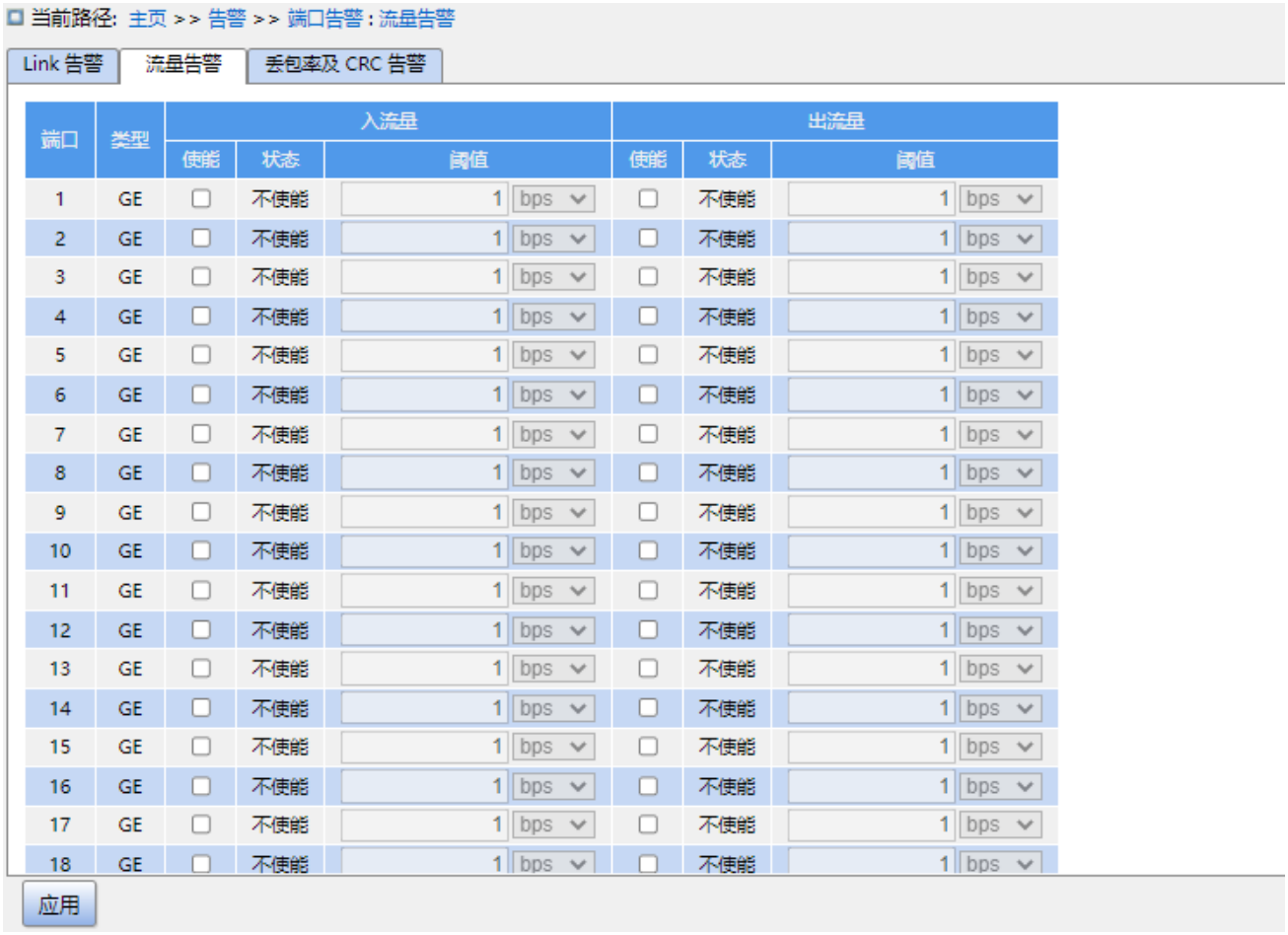


图 105 端口流量告警

入方向流量告警/出方向流量告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口流量告警。

阈值

配置范围：1~1000000000bps 或 1~1000000kbps

功能：配置端口流量告警阈值。

状态

显示选项：不使能/告警/正常

功能：显示端口流量状态。告警表示端口的入方向/出方向流量超过设定阈值，产生告警。

4、丢包率及 CRC 告警配置与显示，如下图所示；

图 106 丢包率及 CRC 告警

丢包率/CRC 告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口 CRC/丢包率告警。

阈值

配置范围：1~1000000pps

功能：配置端口 CRC/丢包率告警阈值。

状态

显示选项：不使能/正常/告警

功能：显示端口 CRC/丢包率状态，告警表示端口 CRC/丢包率超过设定阈值，产生告警。

5、环告警配置与显示，如下图所示；

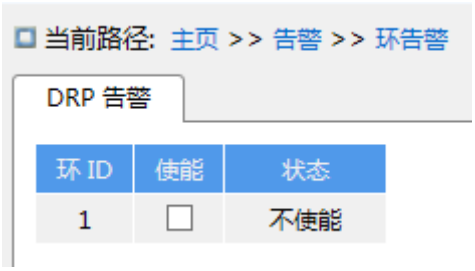


图 107 环告警

DRP 告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 DRP 环告警。

状态

显示选项：不使能/环闭 / 环开

描述：使能 DRP 环告警后，环开时显示环开，环闭时显示环闭。

7 功能管理

7.1 端口配置

1、配置端口状态、速率、流控等信息，如下图所示；

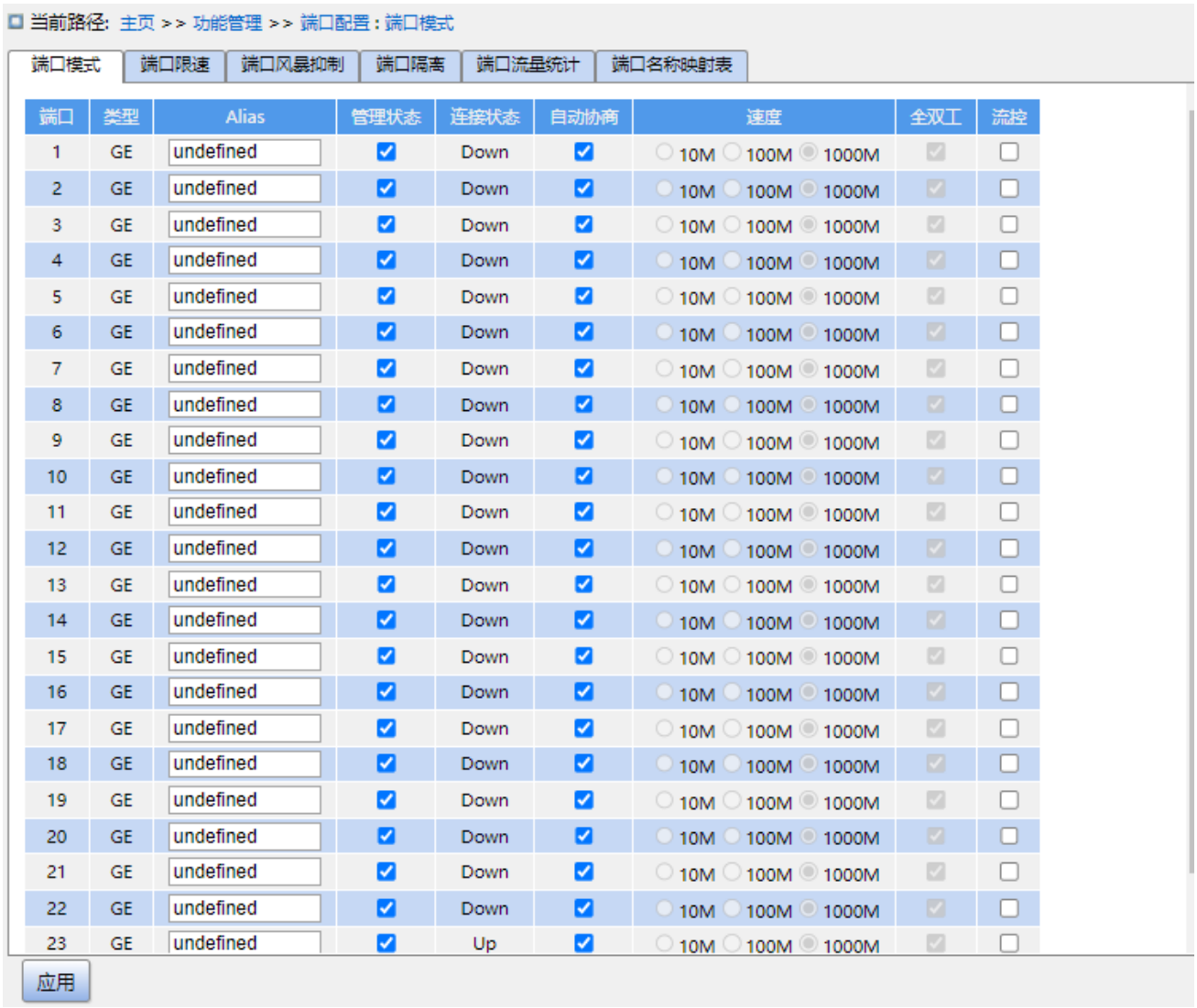


图 108 配置端口模式

管理状态

配置选项：使能/不使能

默认配置：使能

功能：是否允许端口传输数据。

描述：使能时表示打开端口允许数据传输；不使能时表示关闭端口不传输数据。本选项能够直接影响端口的硬件状态并触发端口告警信息。

连接状态

显示当前端口的连接状态。

up 表示端口处于 LinkUp 状态可以正常通信；

down 表示端口处于 LinkDown 状态不能正常通信。

自动协商

配置选项：使能/不使能

默认配置：使能

功能：配置端口速率和双工模式。描述：端口速率和双工模式可自动协商也可强制配置。配置为自动协商模式时端口速率和双工模式会根据双方端口连接状态自动协商。建议用户将端口的速率和双工模式配置为自动协商，这样可以尽可能避免由于端口配置不匹配带来的连接问题。如果用户将端口配置为强制速率/双工模式，请确认连接双方速率/双工模式配置一致。

注意：

➢千兆电口可以配置为自动协商、10M 全双工、10M 半双工、100M 全双工、100M 半双工、1000M 全双工。

速度

配置选项：10M/100M/1000M

功能：配置端口自协商速率。

描述：配置端口模式为自动协商时，默认情况下端口速率是通过和对端自协商决定的，协商得到的速率可以是端口速率能力范围内的任一个。通过配置速率能力可以让端口只协商部分速率，从而控制速率的协商。

注意：

双工能力和速率能力配置只在自动协商模式关闭时才能配置。

全双工

配置选项：使能/不使能

功能：配置端口自协商双工模式。

描述：全双工指端口在发送数据的同时可以接收数据；半双工指端口同一时刻只能发送数据或接收数据。配置端口模式为自动协商时，默认情况下端口双工模式是通过和对端自协商决

定的，协商得到的双工模式可以是全双工和半双工中的任一个。通过配置双工能力可以让端口只协商某一双工模式，从而控制双工模式的协商。

流控

配置选项：使能/不使能

默认配置：不使能

功能：是否打开端口的流控功能。

描述：打开端口流控功能后，当端口接收的流量大于端口缓存所能容纳的最大值时，端口将通过算法或者协议通知发送端减慢发送速度以防止丢包。对于半双工模式和全双工模式，流控通过不同的方式来实现。全双工模式时，接收端通过发送一种特殊的数据帧（Pause 帧）来通知发送端停止发送报文，发送端收到 Pause 帧后会根据该帧中的等待时间停止发送报文，等待时间超时后继续发送报文；半双工模式支持背压流控，接收端可以有意制造一次冲突或载波信号，发送端检测到冲突或载波后采取 Backoff 来延缓数据的发送。

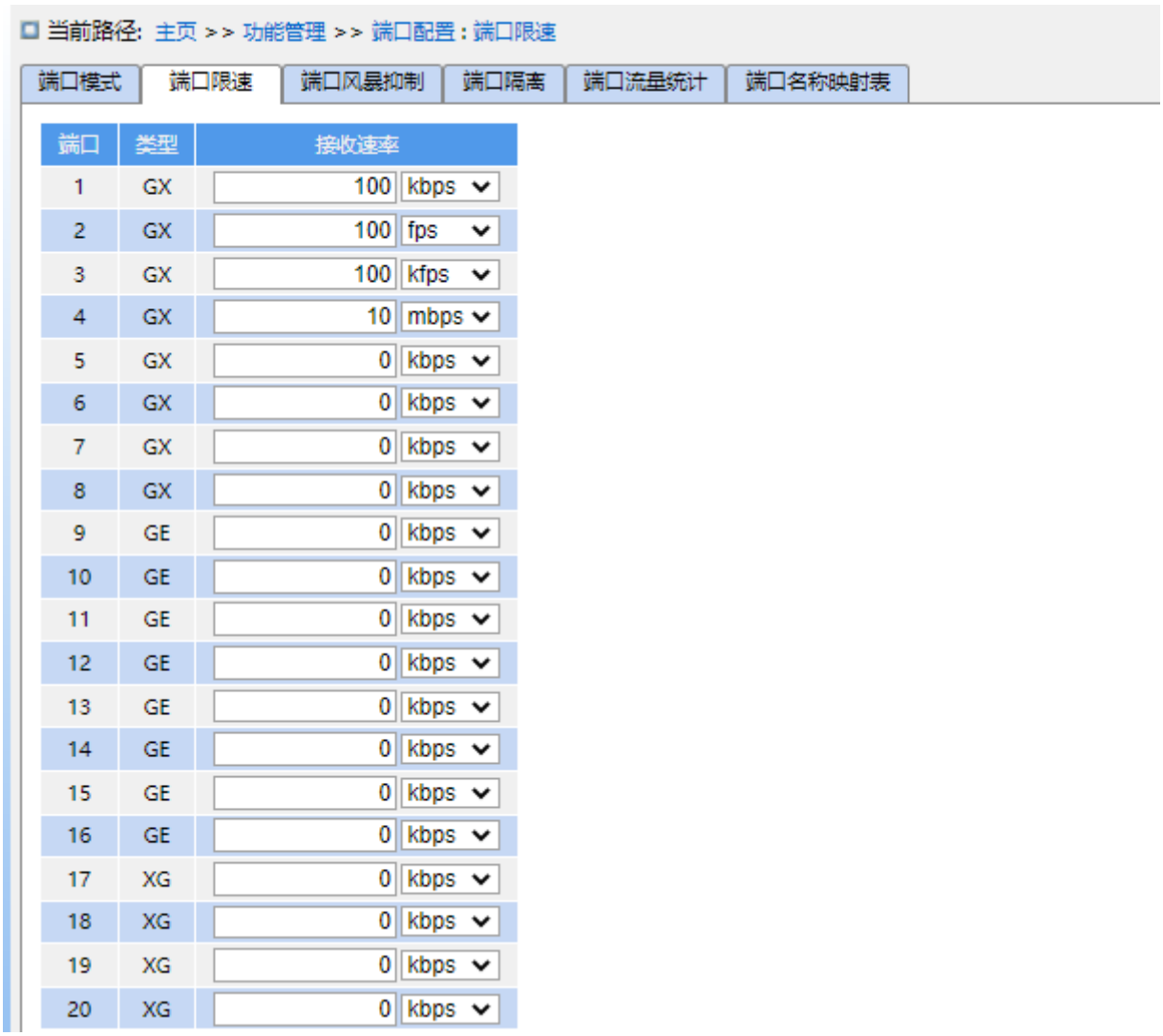
最大报文大小

配置范围：1518~10240 字节

默认：10240 字节

功能：配置端口允许通过的最大报文大小，超过该大小的报文将被丢弃。

2、端口限速配置及显示，如下图所示；



端口	类型	接收速率
1	GX	100 kbps
2	GX	100 fps
3	GX	100 kfps
4	GX	10 mbps
5	GX	0 kbps
6	GX	0 kbps
7	GX	0 kbps
8	GX	0 kbps
9	GE	0 kbps
10	GE	0 kbps
11	GE	0 kbps
12	GE	0 kbps
13	GE	0 kbps
14	GE	0 kbps
15	GE	0 kbps
16	GE	0 kbps
17	XG	0 kbps
18	XG	0 kbps
19	XG	0 kbps
20	XG	0 kbps

图 109 端口限速

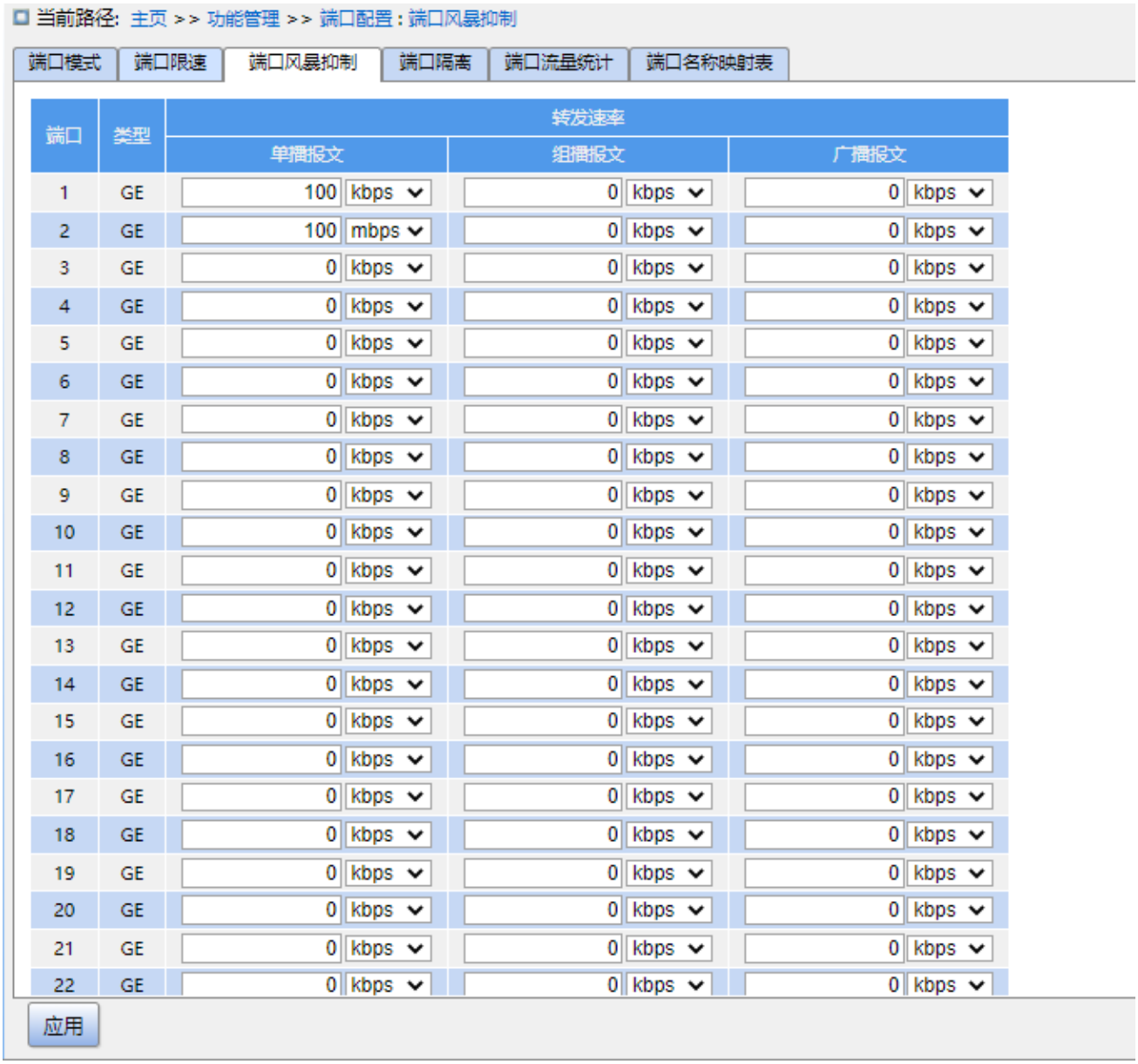
接收速率

配置范围：0/10~13128147kbps/1~13128mbps

默认配置：0，值为 0 表示限速不使能。

功能：配置端口限速阈值，超过阈值的报文数据将被丢失。

3、端口风暴抑制配置及显示，如下图所示；



端口	类型	转发速率		
		单播报文	组播报文	广播报文
1	GE	100 kbps	0 kbps	0 kbps
2	GE	100 mbps	0 kbps	0 kbps
3	GE	0 kbps	0 kbps	0 kbps
4	GE	0 kbps	0 kbps	0 kbps
5	GE	0 kbps	0 kbps	0 kbps
6	GE	0 kbps	0 kbps	0 kbps
7	GE	0 kbps	0 kbps	0 kbps
8	GE	0 kbps	0 kbps	0 kbps
9	GE	0 kbps	0 kbps	0 kbps
10	GE	0 kbps	0 kbps	0 kbps
11	GE	0 kbps	0 kbps	0 kbps
12	GE	0 kbps	0 kbps	0 kbps
13	GE	0 kbps	0 kbps	0 kbps
14	GE	0 kbps	0 kbps	0 kbps
15	GE	0 kbps	0 kbps	0 kbps
16	GE	0 kbps	0 kbps	0 kbps
17	GE	0 kbps	0 kbps	0 kbps
18	GE	0 kbps	0 kbps	0 kbps
19	GE	0 kbps	0 kbps	0 kbps
20	GE	0 kbps	0 kbps	0 kbps
21	GE	0 kbps	0 kbps	0 kbps
22	GE	0 kbps	0 kbps	0 kbps

图 110 端口风暴抑制

转发速率

显示选项：单播报文抑制/组播报文抑制/广播报文抑制

配置范围：0/10~13128147kbps/1~13128mbps

默认配置：0，值为 0 表示风暴抑制不使能。

功能：配置端口转发速率阈值，超过阈值的该类型报文数据将被丢失。

4、端口隔离配置及显示，如下图所示；

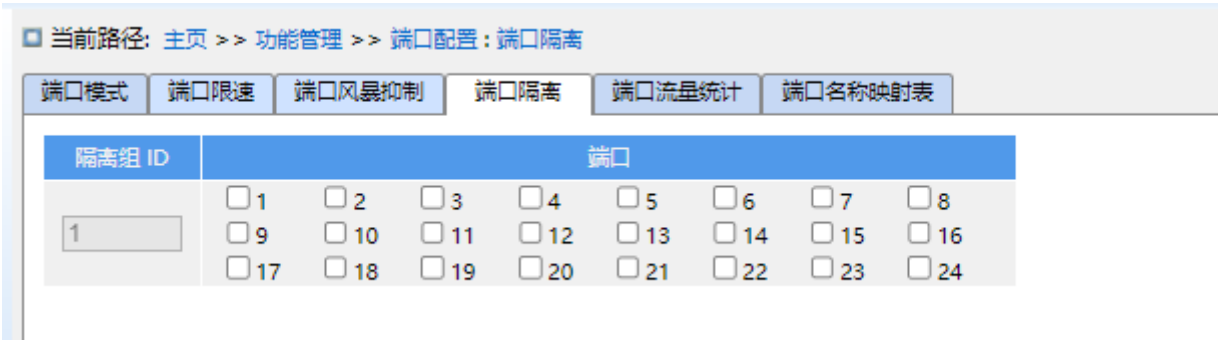


图 111 端口隔离

端口隔离使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的隔离功能。

注：只有一个端口隔离组。

5、统计端口流量，如下图所示；

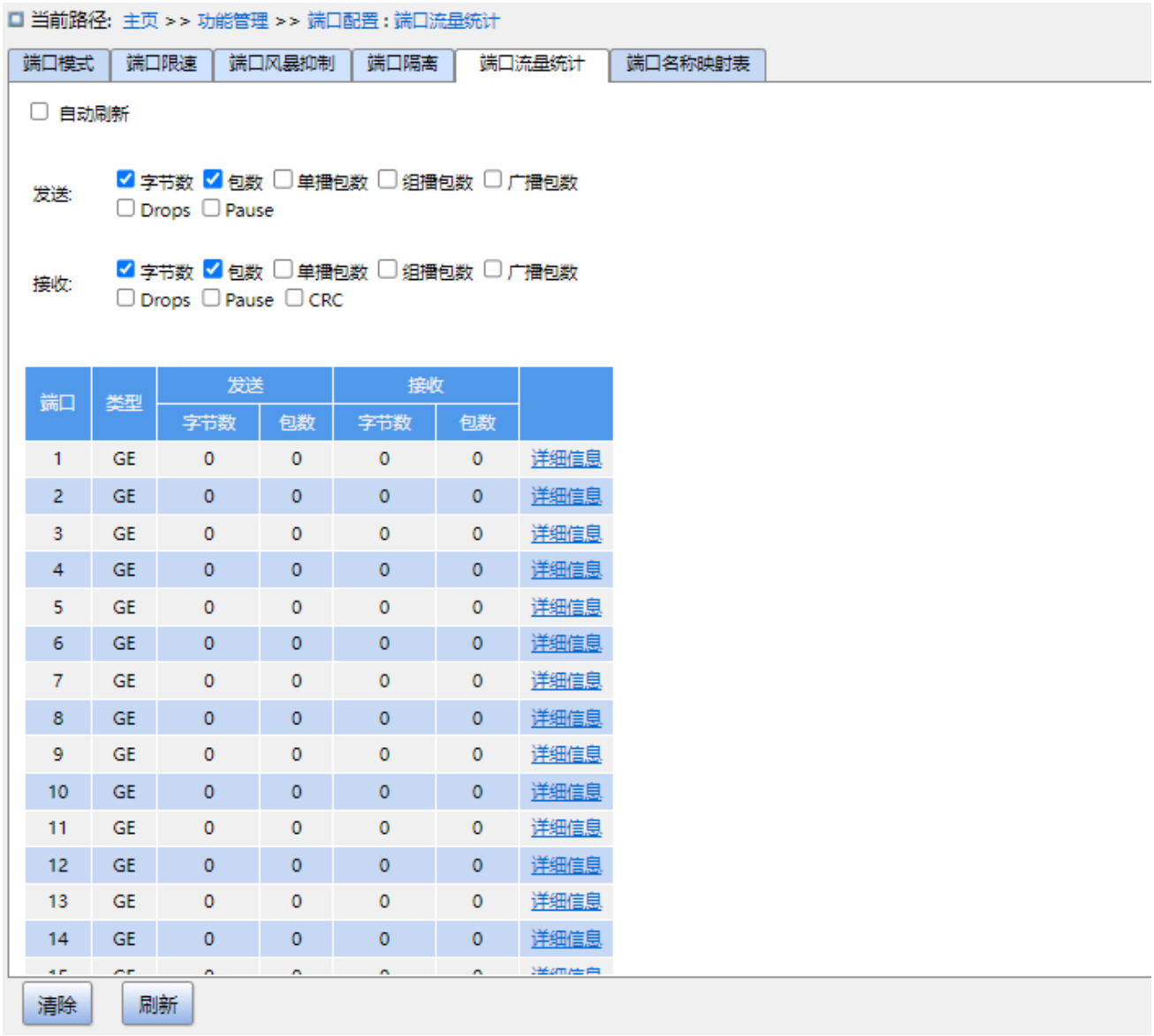


图 112 统计端口流量

字节数

统计端口接收/发送字节数。

包数

统计端口接收/发送包数。

单播包数

统计端口接收/发送单播包数。

组播包数

统计端口接收/发送组播包数。

广播包数

统计端口接收/发送广播包数。

Drops

统计由于接收/发送冲突而丢弃的报文数。

Pause

统计端口接收/发送 Pause 帧数。

CRC

统计端口接收 CRC 错误报文数

点击端口号对应详细信息进入相应端口的详细信息统计界面。

6、统计端口详细信息，如下图所示；

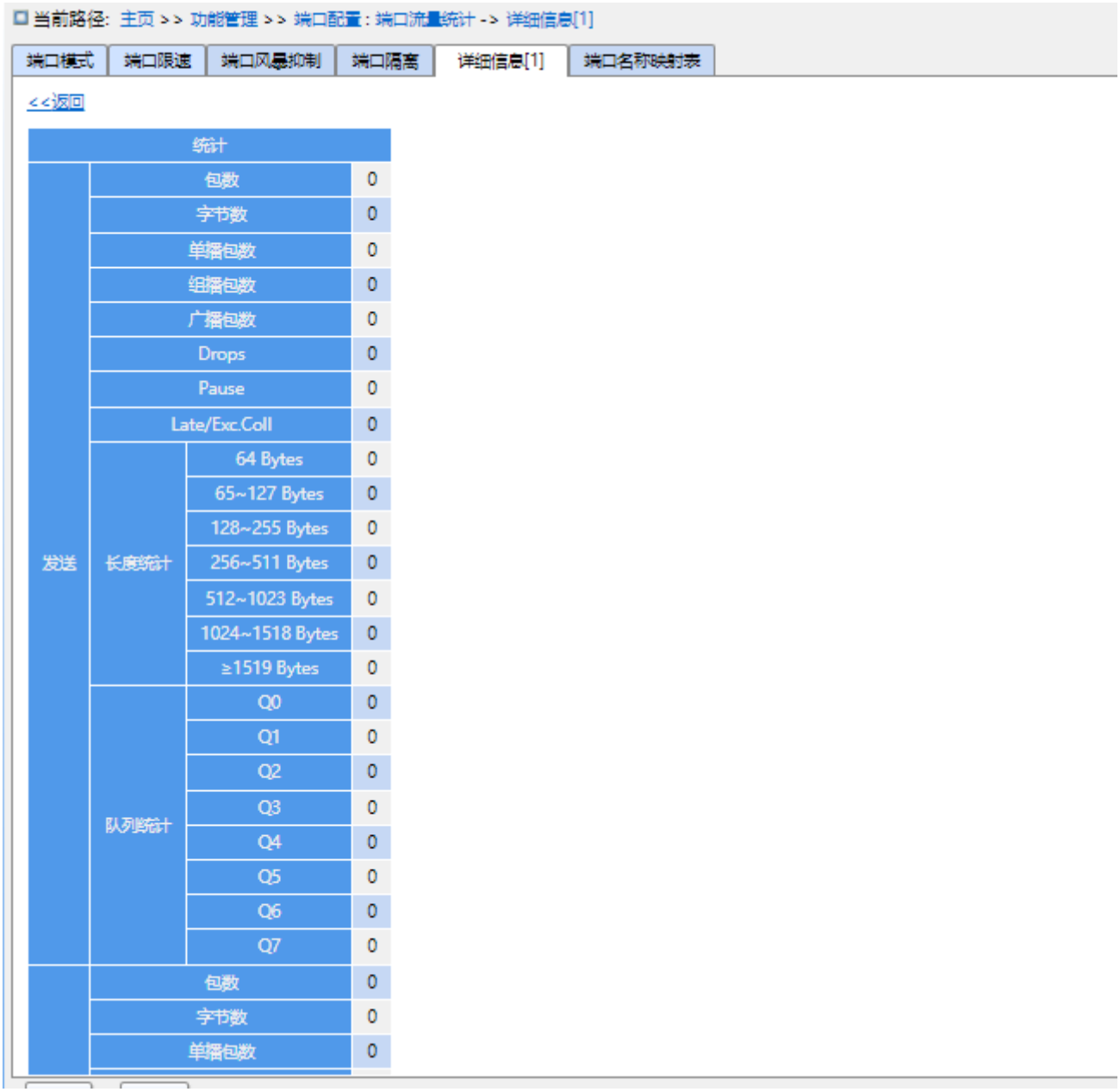


图 113 统计端口详细信息

7、端口名称映射表，如下图所示；

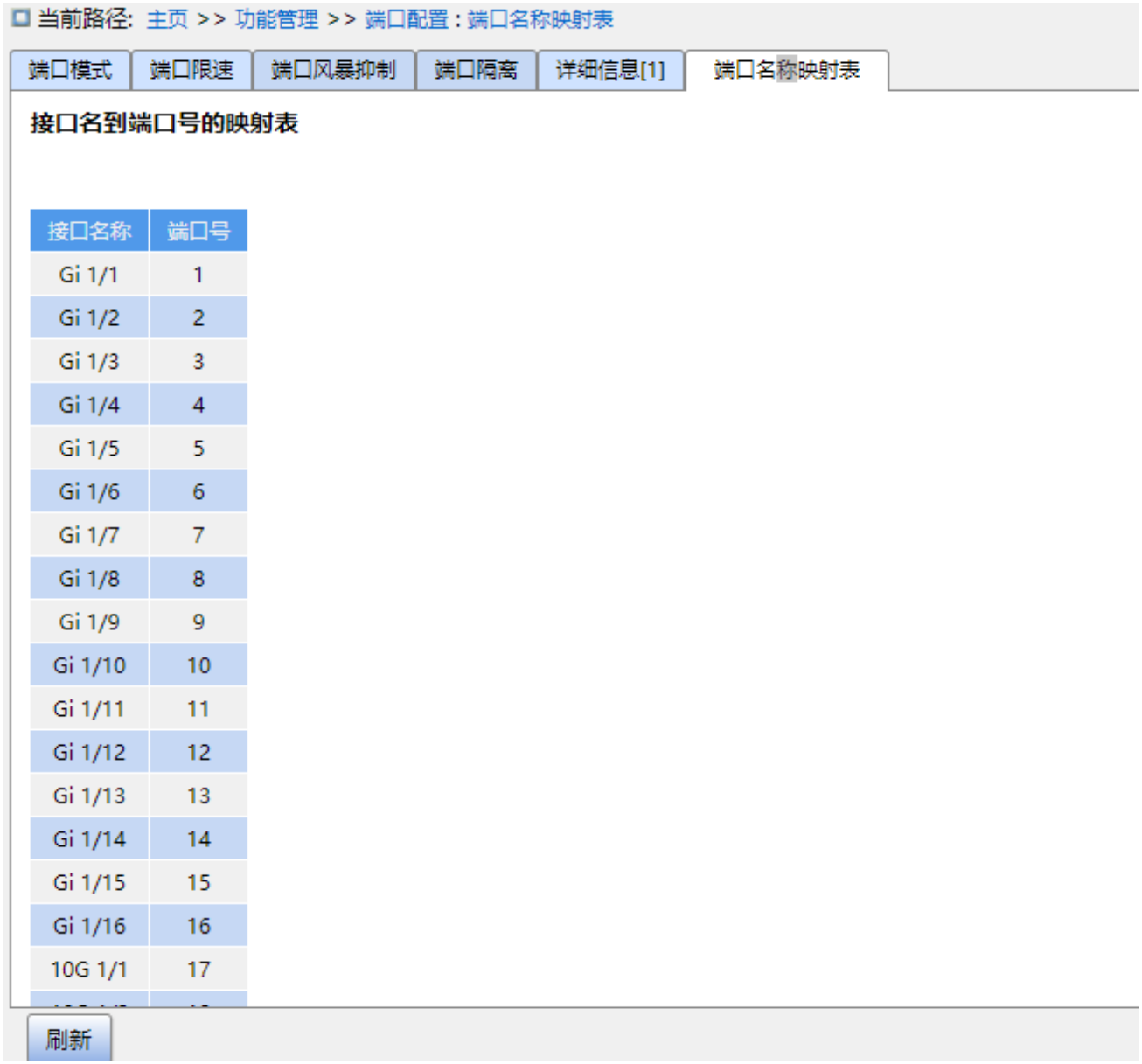


图 114 接口名到端口好的映射表

7.2 VLAN

7.2.1 VLAN 配置

7.2.1.1 介绍

VLAN（Virtual Local Area Network，虚拟局域网）指把一个局域网划分为多个逻辑 VLAN，同一个 VLAN 中的设备之间可以相互通信，不同 VLAN 中的设备无法通信，这样广播报文被限制在一个 VLAN 中，大大提高了局域网的安全性。

VLAN 的划分不受物理位置的限制，每个 VLAN 被认为是一个逻辑网络。

7.2.1.2 原理

为使网络设备能够分辨不同 VLAN 报文，需要在报文中添加标识 VLAN 的字段，目前标识 VLAN 最通用的协议是 IEEE802.1Q 协议，802.1Q 帧结构如表 3 所示：

表 3 802.1Q 帧结构

DA	SA	802.1Q header				Length/type	Data	FCS
		TPID	PRI	CFI	VID			

传统的以太网数据帧结构中插入一个 4 字节的 802.1Q 头信息指明一帧的 VLAN 标记：

TPID：16 位，标识本数据帧是带有 VLAN Tag 的数据，802.1Q 协议中规定的取值为 0x8100；

PRI：3 位，标记报文的 802.1p 优先级；

CFI：1 位，标识 MAC 地址在不同的传输介质中是否以标准格式进行封装，值为 0 表示 MAC 地址以标准格式进行封装；值为 1 标识以非标准格式封装；

VID：12 位，标识该报文所属 VLAN 的编号，取值范围是 1~4093，0、4094、4095 为协议保留取值。

说明：

- VLAN 1 为系统缺省 VLAN，用户不能手动创建和删除；
- 保留 VLAN 是系统为实现特定功能预留的 VLAN，用户也不能手动创建和删除。

带有 802.1Q 头信息的报文为标记（Tag）报文，否则为无标记（Untag）报文，所有报文在交换机内都带有 802.1Q 标记。

7.2.1.3 基于端口的 VLAN 介绍

VLAN 划分可以有多种方式，例如：基于端口、基于 MAC 地址等。该系列交换机支持基于端口的 VLAN 划分，根据交换机端口来定义 VLAN 成员，将端口加入到指定 VLAN 中，该端口就能转发指定 VLAN 标记的报文。

1、端口模式

根据端口在发送报文时对 Tag 标签的处理方式，可将端口分为三种模式：

Access：端口只能属于一个VLAN，默认情况下交换机所有端口都以Access模式存在于

VLAN1中。Access端口发送的报文均不带tag标记；一般用于连接用户设备。

Trunk：端口允许多个VLAN通过。Trunk端口只接收tagged报文，发送PVID报文时可以选择是否携带tag标记，发送其他报文时均带tag标记；一般用于网络设备之间连接。

Hybrid：端口允许多个VLAN通过。Hybrid端口可以选择接收报文的类型，发送报文时也可以选择是否携带tag标记；可以用于网络设备之间连接，也可以用于连接用户设备。

Hybrid端口和Trunk端口的区别在于：Hybrid端口允许多个VLAN的报文发送时不带tag标记；Trunk端口只允许PVID的报文发送时不带tag标记。

2、PVID

每个端口都有一个PVID属性，当端口收到Untag报文时，根据PVID为报文添加Tag标记。默认所有端口的PVID 均为1。

注意：

- 端口 PVID 应从该端口允许通过的 VLAN ID 中选择，否则该端口无法转发报文；
- 为 Untag 报文添加 PVID 的 tag 标记时，端口缺省 PRI 和 CFI 值见图 240 中参数 PCP 和 DEI 配置。

配置了端口模式和PVID后，端口对报文接收和发送情况，如表 4所示；

表 4 不同端口类型收发报文的区别

对接收报文的处理		对发送报文的处理	
接收到的报文为 Untag	**接收到的报文为 Tag**	**端口模式**	**报文处理**
为报文添加 PVID 的 Tag 标记： ➢ 当 PVID 在端口允许通过的 VLAN 列表中，接收该报文 ➢ 当 PVID 不在端口允许通过的VLAN列表中，丢弃该报文	➢ 当 VLAN ID 在端口允许通过的VLAN列表中时，接收该报文 ➢ 当 VLAN ID 不在端口允许通过的 VLAN 列表中时，丢弃该报文	Access 端口	去掉 Tag 标记后发送该报文
		Trunk 端口	根据“出口标签”配置发送报文： ➢ Untag Port VLAN：当 VLAN ID 与 PVID 相同且在该端口允许通过的 VLAN 列表时，去掉 Tag 标记，发送该报文；当 VLAN ID 与 PVID 不同，且在该端口允许通过的 VLAN 列表时，保持报文中原有的 Tag 标记，发送该报文 ➢ Tag All：当 VLAN ID 在该端口允许

			通过的 VLAN 列表时，保持报文中原有的 Tag 标记，发送该报文
		Hybrid 端口	根据“出口标签”配置发送报文： ➢ Untag Port VLAN：同上 ➢ Tag All：同上 ➢ Untag All：当 VLAN ID 在该端口允许通过的 VLAN 列表时，去掉 Tag 标记，发送该报文

7.2.1.4 Web 页面配置

1、配置端口链路模式，如下图所示；

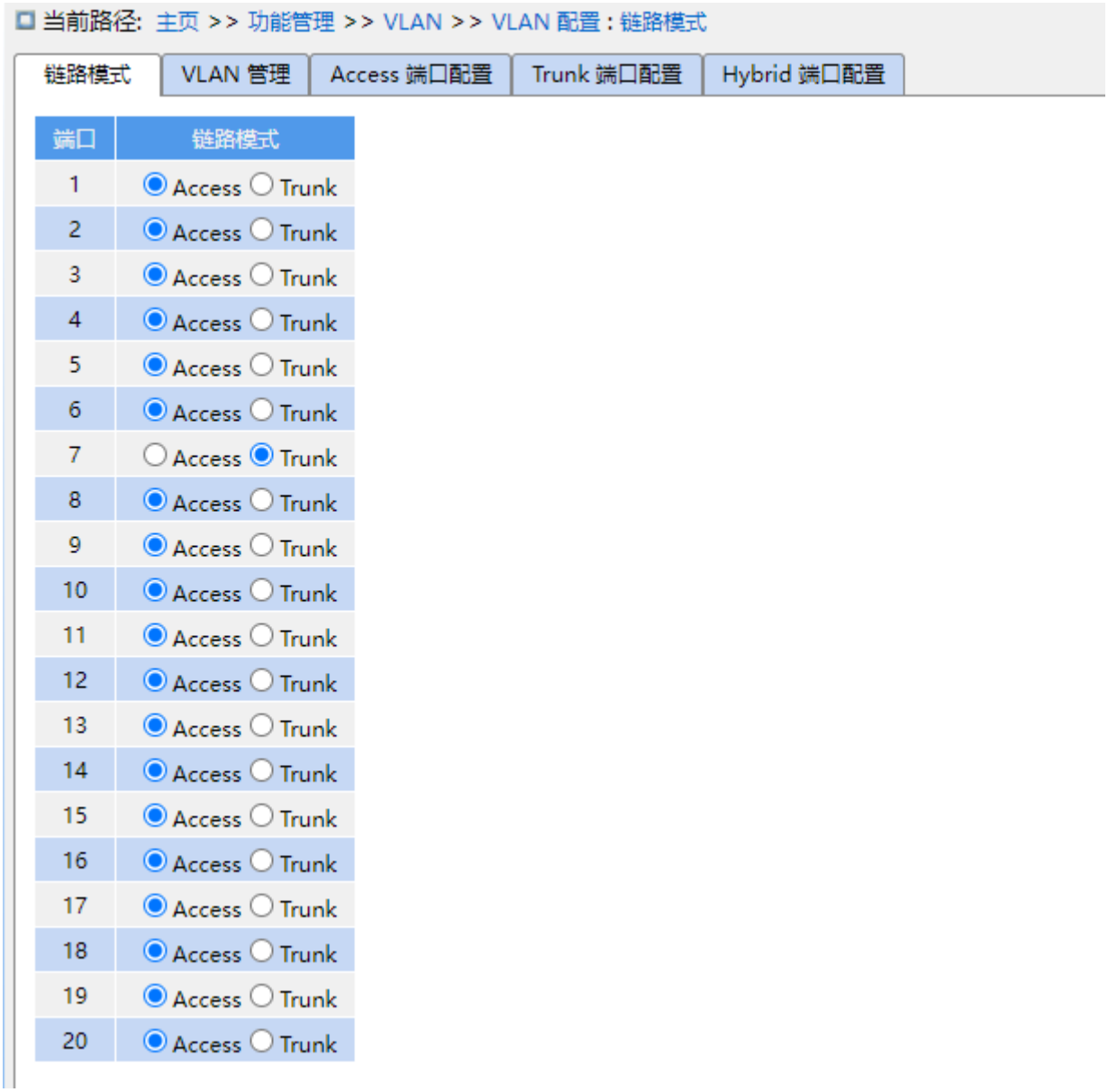


图 115 配置端口链路模式

链路模式

配置选项：Access、Trunk

默认配置：Access

功能：配置指定端口链路模式。

2、VLAN 管理，如下图所示；

图 116 VLAN 管理配置

VLAN ID

配置范围：1-4093

默认配置：1

功能：创建 VLAN。

VLAN 名称

配置范围：1-32 个字符，可包含大小写字母、数字及下划线

功能：配置 VLAN 的名称。

3、Access 端口配置，如下图所示：

图 117 Access 端口配置

PVID

配置范围：1-4093

默认配置：1

功能：配置 Access 端口的默认 VLAN。

注意：

➢ 配置 Access 端口 VLAN ID 时需先创建此 VLAN，Trunk 模式端口类似。

4、Trunk 端口配置，如下图所示：

图 118 Trunk 端口配置

PVID

配置范围：1-4093

默认配置：1

功能：配置 Trunk 端口的默认 VLAN。

允许的 VLAN

配置范围：1-4093，使用半角逗号','和连字符'-'分隔（M-N，M 必须小于 N），例如：2,33,34-77。

默认配置：1

功能：配置 Trunk 端口允许的 VLAN。

7.2.1.5 典型配置举例

如图 119 所示，将整个局域网划分为 3 个 VLAN：VLAN2、VLAN100 和 VLAN200，要求同一 VLAN 中的设备可以相互通信，不同 VLAN 之间相互隔离。终端 PC 设备不识别带 tag 标记的报文，所以将 Switch A、B 和 PC 相连的端口配置为 Access 端口。Switch A 和 Switch B 之间需要传输 VLAN 2、VLAN 100 和 VLAN200 的报文，所以将 Switch A、 B 相连的端口配置为 Trunk 端口，并允许 VLAN 2、VLAN 100 和 VLAN200 通过。具体配置如表 5 所示。

表 5 VLAN 配置

配置项目	配置说明
VLAN2	A 地、B 地交换机 1、2 端口（Access）；端口 7（Trunk）

VLAN100	A 地、B 地交换机 3、4 端口（Access）；端口 7（Trunk）
VLAN200	A 地、B 地交换机 5、6 端口（Access）；端口 7（Trunk）

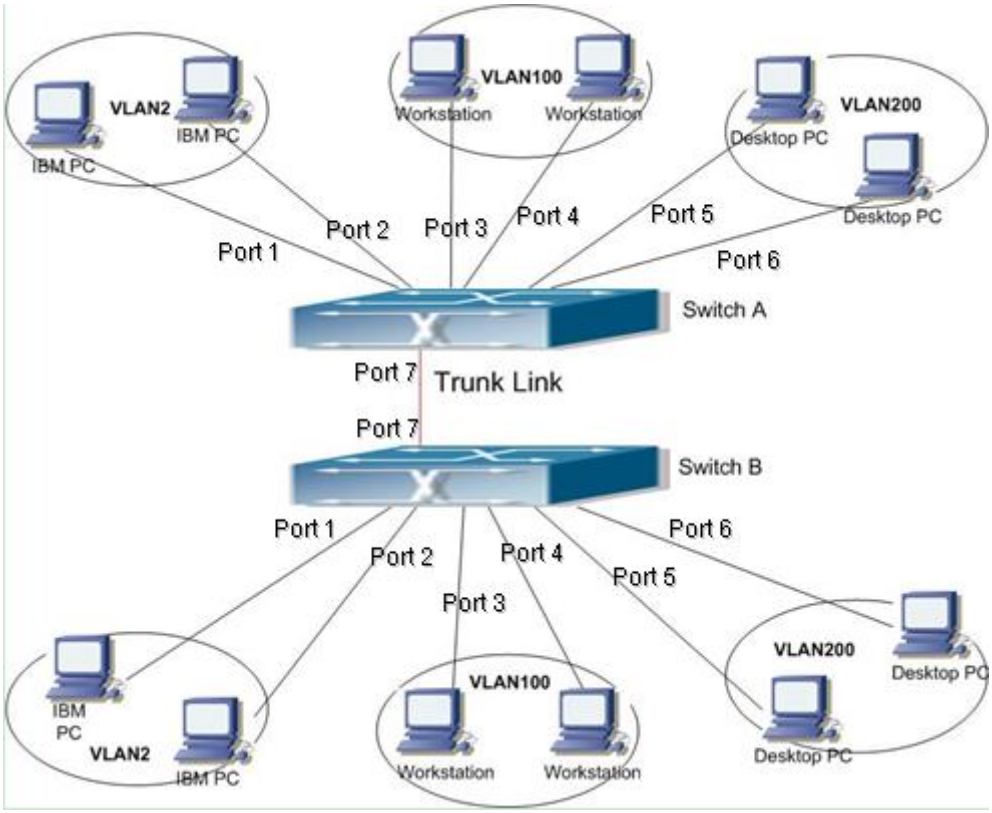


图 119 VLAN 应用

SwitchA、B的配置如下：

1、配置Access端口允许通过的VLAN：1,2,100,200，见图 117；

2、配置端口1~2为Access模式，端口VLAN为2；端口3~4为Access模式，端口VLAN为100；端口5~6为Access模式，端口VLAN为200；端口7为Trunk模式，端口VLAN为1，允许VLAN为1,2,100,200，见图 118；

3、其余为默认配置。

7.2.2 GVRP

7.2.2.1 GARP 介绍

GARP（Generic Attribute Registration Protocol，通用属性注册协议）用于同一网络内交换机之间传播、注册和注销某种信息（VLAN、组播地址等）。GARP 应用分为 GVRP 和 GMRP。

通过 GARP 机制，一个 GARP 成员的配置信息会迅速传播到整个交换网。GARP 成员通过 join/leave 消息通知其它 GARP 成员注册或注销自己的属性信息，并根据其他成员的

join/leave 消息注册或注销对方的属性信息。

GARP 中起作用的消息有三类：Join、Leave、LeaveAll。

当一个 GARP 应用实体希望其它交换机注册自己的某种属性信息时，将 对外发送 Join 消息。Join 消息分为 JoinEmpty 和 JoinIn 两种，发送 JoinIn 消息用来声明一个该应用实体已经注册的属性；发送 JoinEmpty 消息用来声明一个该应用实体没有注册的属性；

当一个 GARP 应用实体希望其它交换机注销自己的某种属性信息时，将对外发送 Leave 消息；

每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GARP 应用实体将对外发送 LeaveAll 消息。

说明：

应用实体指使能该注册协议的端口。

GARP 的定时器包括 Hold 定时器、Join 定时器、Leave 定时器和 LeaveAll 定时器：

Hold 定时器：当 GARP 应用实体接收到某注册信息时，不立即对外发送 Join 消息，而是启动 Hold 定时器，当该定时器超时后，将此时段内收到的所有注册信息放在一个 Join 消息中向外发送，从而减少报文的发送量有利于网络稳定。

Join 定时器：为保证 Join 消息能够可靠地传输到其它应用实体，GARP 应用实体发送第一个 Join 消息后将等待一个 Join 定时器时间间隔，如果在该时间段内没有收到 JoinIn 消息，则再发送一个 Join 消息，否则不发送第二个 Jion 消息。

Leave 定时器：当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息，接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有再次收到 Join 消息，则注销该属性信息。

LeaveAll 定时器：每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体的所有属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

7.2.2.2 GVRP 介绍

GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）是 GARP 的一种应用，基于 GARP 工作机制维护设备中的 VLAN 动态注册信息，并传播该信息到其他设备中。

设备启动 GVRP 特性后，能够接收来自其它设备的 VLAN 注册信息，并动态更新本地的

VLAN 注册信息。而且设备能够将本地的 VLAN 注册信息向其它设备传播，以便使同一局域网内所有设备的 VLAN 信息达成一致。GVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

注意：

GVRP 端口和聚合端口互斥，即使能 GVRP 功能的端口不应加入聚合组；加入聚合组的端口不应使能 GVRP 功能。

7.2.2.3 Web 页面配置

1、全局使能 GVRP 协议，并配置相应定时器，如下图所示；

图 120 GVRP 全局配置

GVRP 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 GVRP 协议。

Join 定时器

配置范围：1-20（厘秒）

默认配置：20（厘秒）

功能：配置 Join 定时器值。

Leave 定时器

配置范围：60-300（厘秒）

默认配置：60（厘秒）

功能：配置 Leave 定时器值。

LeaveAll 定时器

配置范围：1000-5000（厘秒）

默认配置：1000（厘秒）

功能：配置 leave all 定时器值。

描述：如果不同设备的 LeaveAll 定时器同时超时，就会同时发送多个 LeaveAll 消息增加不必要的报文数量，为了避免不同设备同时发生 LeaveAll 定时器超时，Leave all 定时器实际运行的值是大于 leave all 定时器值，小于 1.5 倍 leave all 定时器值的一个随机值。

最大 VLAN 数

配置范围：1~4093

默认配置：20

功能：配置 GVRP 端口动态注册的最大 VLAN 数。

注意：

➢配置 GVRP 定时器和最大 VLAN 参数时需要先关闭 GVRP 功能。

2、配置 GVRP 端口，如下图所示；

图 121 GVRP 端口配置

端口

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的 GVRP 功能。

注意：

- GVRP 端口应配置为 Trunk 端口；
- GVRP 端口扩散其他处于 Up 状态的 GVRP 端口的 VLAN 属性。

7.2.2.4 典型配置举例

如图 122 所示，为了实现 Device A 和 Device B 之间 VLAN 信息的动态注册和更新，需要在设备上启动 GVRP。

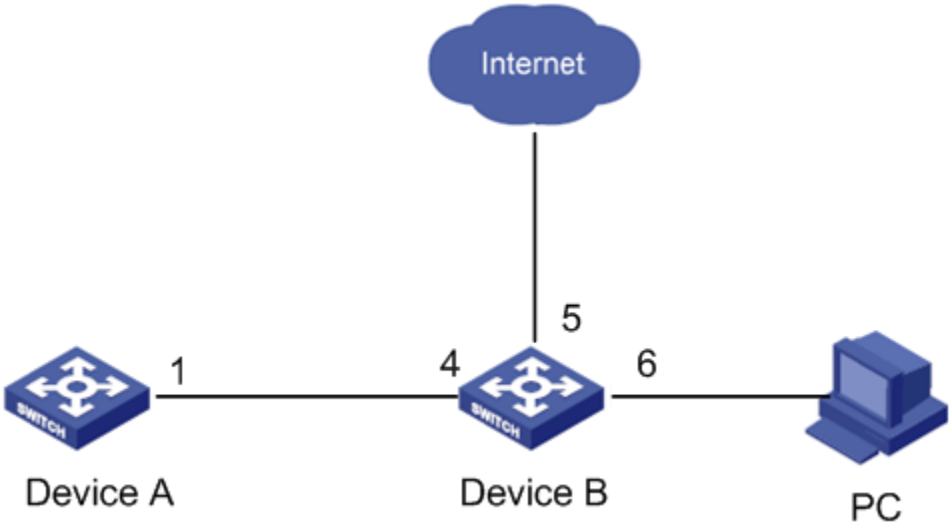


图 122 GVRP 配置举例

Device A 配置如下：

1、配置端口 1 为 Trunk 模式；

2、全局使能 GVRP 功能，见图 120；

3、使能端口 1 的 GVRP 功能，见图 121；

Device B 配置如下：

1、配置端口 4 为 Trunk 模式；端口 6 为 Trunk 模式，允许通过的 VLAN 为 1、6;

2、全局使能 GVRP 功能，见图 120；

3、使能端口 4、5、6 的 GVRP 功能，见图 121；

交换机 A 中端口 1 注册到和交换机 B 中端口 5 和 6 相同的 VLAN 信息。

7.2.3 PVLAN 配置

7.2.3.1 介绍

PVLAN（Private VLAN，私有 VLAN）采用两层隔离技术实现复杂端口业务隔离功能，可以实现网络安全，广播域隔离功能。

位于上层的 VLAN 为共享域 VLAN，位于共享域 VLAN 中的端口为上联端口；下层 VLAN 为隔离域 VLAN，位于隔离域 VLAN 中的端口为下联端口。可以把下联端口配置到不同的隔离域中，可以同时和上联端口通信，不同的隔离域间不能通信。

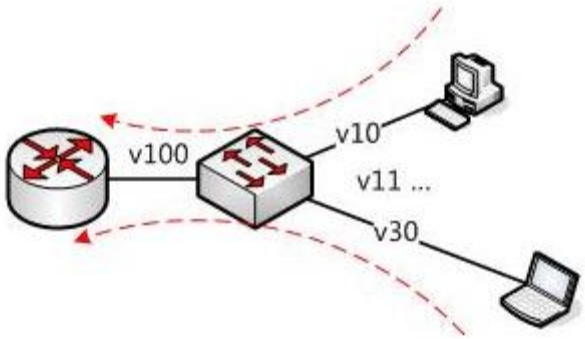


图 123 PVLAN 应用

如图 123 所示，共享域为 VLAN 100；隔离域为 VLAN 10 和 VLAN 30；隔离域的设备可以和共享域的设备通信，如 VLAN 10 可以和 VLAN 100 通信，VLAN 30 可以和 VLAN 100 通信；但是隔离域中的设备之间不能通信，如：VLAN 10 和 VLAN 30 之间不能通信。

7.2.3.2 说明

通过对端口进行特殊配置便可以实现 PVLAN 功能。

- 上联端口的 PVID 与共享域 VLAN 一致，下联端口的 PVID 与各自隔离域一致；
- 上联端口以 Hybrid 类型添加到共享域 VLAN 和所有隔离域 VLAN 中，下联端口以 Hybrid 类型添加到共享域 VLAN 和各自的隔离域 VLAN 中；
- PVLAN 成员端口发送报文均为 Untag 报文。

7.2.3.3 Web 页面配置

1、上联端口配置，如下图所示；

图 124 配置上联端口

端口

配置选项：使能/不使能

默认配置：不使能

功能：配置端口为上联端口。

2、PVLAN 配置，如下图所示；

图 125 PVLAN 配置

PVLAN ID

配置选项：1-N（N 为端口数）

默认配置：1

功能：配置端口 PVLAN ID。

端口

配置选项：使能/不使能

默认配置：1-N（N 为端口数）

功能：指定 PVLAN 端口。

7.2.3.4 典型配置举例

图 126 中为 PVLAN 应用，VLAN300 为共享域，端口 1 和 2 为上联端口；VLAN100 和 VLAN200 都属于隔离域，端口 3、4、5、6 是下联端口。

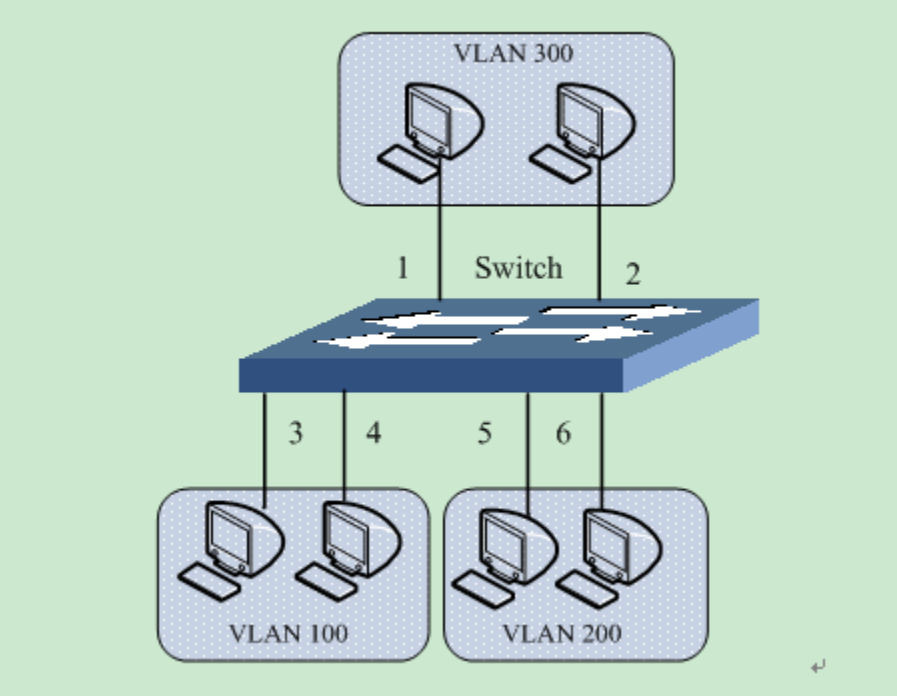


图 126 PVLAN 配置举例

交换机配置如下：

1、配置端口 1、2 为 Trunk/Hybrid 模式，PVID 为 300，允许 VLAN 为 100,200,300；

2、配置端口 3、4 为 Trunk/Hybrid 模式，PVID 为 100，允许 VLAN 为 100,300；

3、配置端口 5、6 为 Trunk/Hybrid 模式，PVID 为 200，允许 VLAN 为 200,300；

4、其余采用默认配置。

7.2.4 VLAN 状态

查看端口 VLAN 状态，如下图所示；

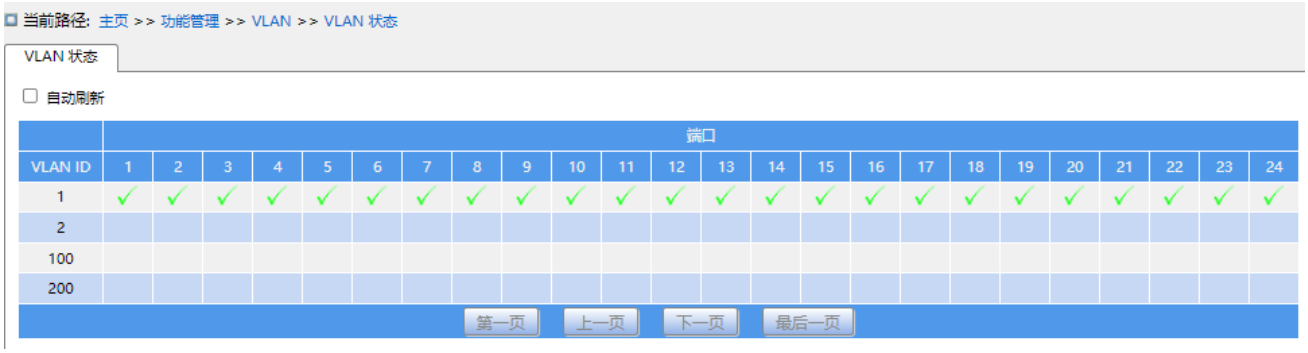


图 127 端口 VLAN 状态

7.3 IP 配置

7.3.1 IP 地址配置

1、通过 Console 口查看交换机 IP 地址

Console 口访问交换机登陆到命令行界面时，在特权用户配置模式下输入命令”**show interface vlan 1**”可以查看交换机的 IP 地址，如图 128 红色区域部分所示；

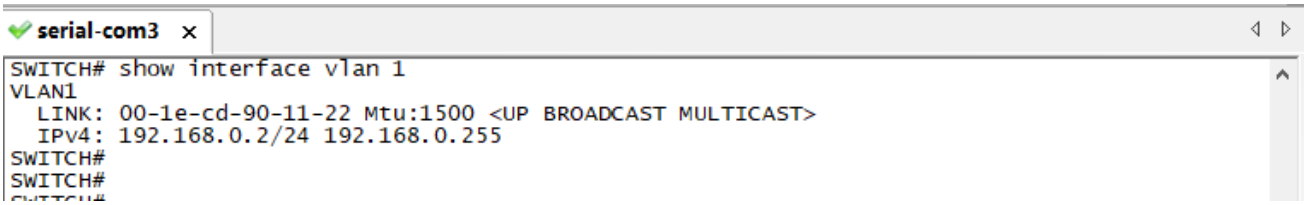


图 128 查看 IP 地址

2、创建 IP 接口

不同 VLAN 的主机之间不能直接通信，需要通过路由器或三层交换机等网络层设备进行转发，三层转发需要通过 IP 接口实现。该系列交换机提供 IP 接口，IP 接口是一种三层模式下的虚拟接口，主要用于实现 VLAN 间的三层互通，不作为物理实体存在于设备上。每个 VLAN 都可以创建一个 IP 接口，该接口可以为本 VLAN 内端口收到的报文进行网络层转发。

3、配置主 IP 地址

交换机的主 IP 地址可以通过手动配置和自动获取两种方式来获得，如图 130 所示。

图 129 Vlan 接口配置

VLAN ID

功能：配置 IP 接口的 VLAN 属性，只有该 VLAN 成员端口可以访问当前 IP 接口。

地址

功能：Vlan 接口获取的 IP 地址和掩码。

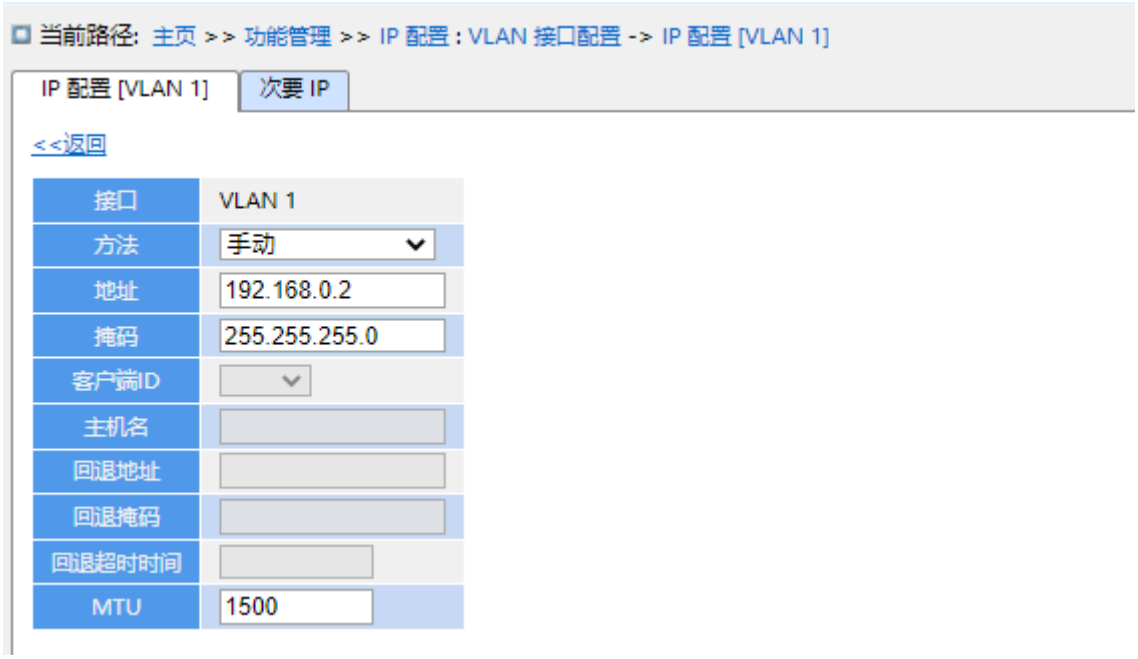


图 130 配置 IP 地址

方法

配置选项：None/DHCP/手动

默认配置：None

功能：选择手动，需要手动配置 IP 地址和子网掩码；DHCP 使能时，交换机作为 DHCP client 通过 DHCP 协议自动获取 IP 地址，此时网络中应存在 DHCP Server 为客户端分配 IP 地址、子网掩码。

地址

配置格式：A.B.C.D

功能：Vlan 接口的 IP 地址。

掩码长度

功能：子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。掩码长度指掩码中 1 的个数。

客户端 ID

配置选项：名称/Hex/端口

功能：指定 IP 接口发送 DHCP 请求时，携带 option61 字段具体填充信息。Hex 指以类型 01+mac 地址形式填充 option61；名称指以类型 00+字符串形式填充 option61；端口指以对应接口 mac 填充 option61。

主机名

配置范围：0~63 个字符

功能：配置交换机的主机名。

回退地址

配置格式：A.B.C.D

功能：Vlan 接口通过 DHCP 协议获得 IP 地址超时后，将地址设为回退 IP 地址。

回退掩码长度

功能：回退子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。掩码长度指掩码中 1 的个数。

回退超时时间

配置范围：0~4294967295s

功能：值为非 0 时，交换机通过 DHCP 协议获得 IP 地址的尝试时间，此时需要手动配置 IP 地址，尝试时间超时后，手动配置的 IP 地址生效。值为 0 时，交换机将反复尝试直到通过 DHCP 协议获得 IP 地址，此时不需要手动配置 IP 地址。

MTU

配置范围：68-9600

默认配置：1500

功能：配置在 IP 层上能通过的最大报文长度。

4、配置次要 IP 可以手动配置交换机 IP 接口的次要 IP 地址，如下图所示。

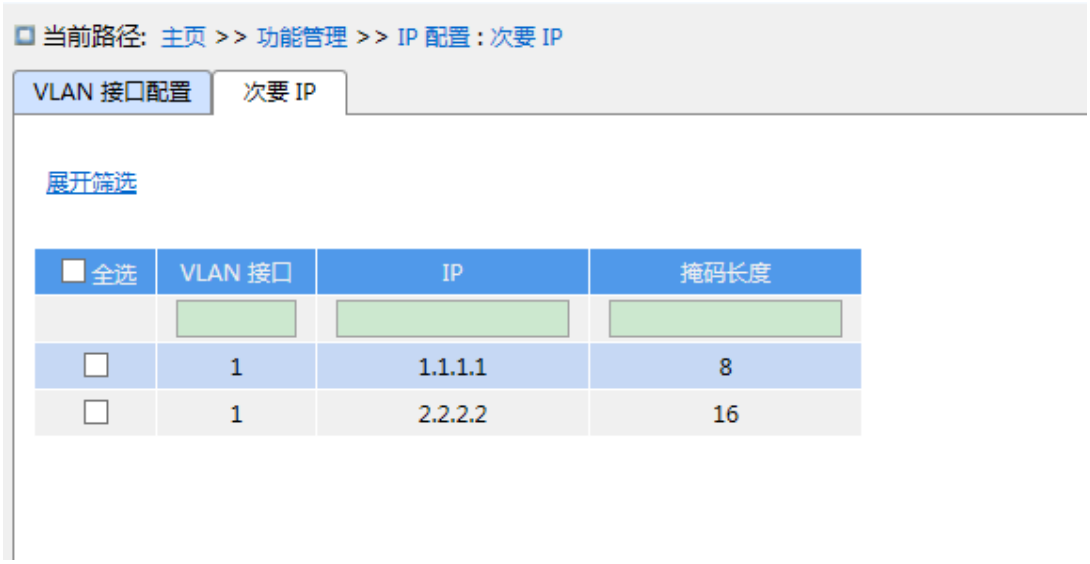


图 131 配置次要 IP

VLAN 接口

功能：配置 IP 接口的 VLAN 属性，只有该 VLAN 成员端口可以访问当前 IP 接口。

IP

配置格式：A.B.C.D

功能：手动配置 IP 地址。

掩码长度

功能：子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。掩码长度指掩码中 1 的个数。

注意：

- 每个 IP 接口对应一个主 IP 地址，可对应多个次要 IP 地址；
- 不同 IP 接口应配置不同网段的主/次 IP 地址。

7.4 端口聚合

7.4.1 静态聚合

7.4.1.1 介绍

端口聚合是将有相同属性配置的一组端口抽象成一个逻辑端口来增加带宽、提高传输速率。同一聚合组中各成员端口实现流量分担，并且彼此之间动态备份，提高连接的可靠性。

聚合组是配置层面的一个物理端口组，配置到聚合组中的物理端口才能参加链路聚合，成为聚合组中的成员端口。加入聚合组中的物理端口满足某种条件时进行端口汇聚，形成一个聚合组独立的逻辑端口。对于用户来讲完全可以将这个聚合组当做一个端口使用，因此不仅能增加网络带宽，还可以提供链路备份功能。

7.4.1.2 实现

如图 132 所示 SwitchA 的 3 个端口汇聚成一个聚合组，该聚合组的带宽为 3 个端口带宽总和。

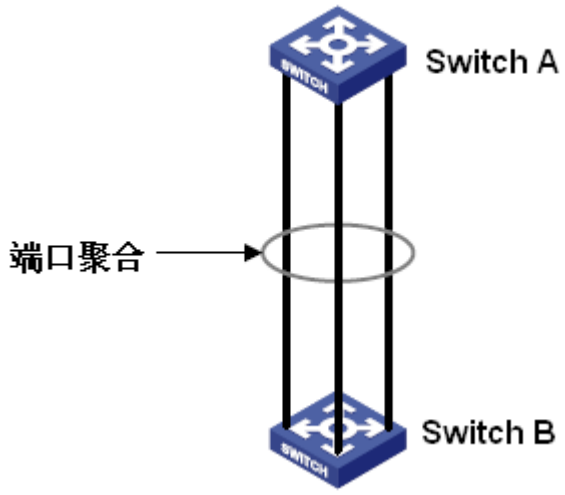


图 132 端口聚合示意图

SwitchA 如果有流量要经过链路聚合传输到 SwitchB，SwitchA 的聚合组将根据流量分担方式进行流量分配运算，根据运算结果决定由聚合组中的某一成员端口承担该流量。当聚合组中的一个端口连接失败，则原该由该端口承担的流量将再次通过流量分配算法分配给其他连接正常的端口分担。

注意：

➢一个端口只能加入一个聚合组；

➢使能 LACP 协议的端口不能加入静态聚合组，加入静态聚合组的端口不能使能 LACP 协议；

➢ 端口聚合与冗余端口互斥，加入聚合组的端口不可以配置为冗余端口，配置为冗余端口的端口不能加入聚合组；

➢ 本文中提到的冗余端口指 DRP 环端口、DRP 备份端口、STP、RSTP 端口和 MSTP 端口。

7.4.1.3 Web 页面配置

1、静态聚合配置如下图所示；

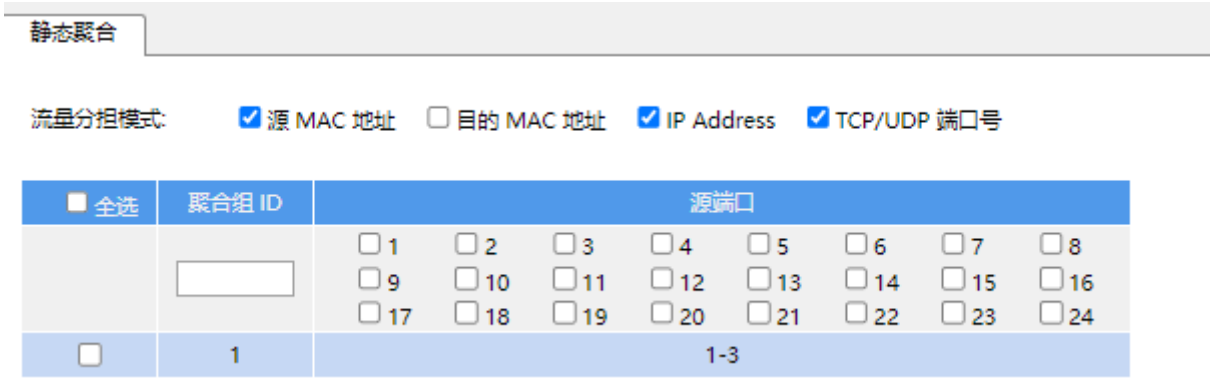


图 133 配置静态聚合

流量分担模式

配置选项：源 MAC 地址/目的 MAC 地址/IP 地址/ TCP/UDP 端口号

默认配置：源 MAC 地址/IP 地址/ TCP/UDP 端口号

功能：配置聚合组的负载分担方式。

描述：源 MAC 地址根据源 MAC 地址进行流量分担；目的 MAC 地址根据目的 MAC 地址进行流量分担；IP 地址根据 IP 地址进行流量分担；TCP/UDP 端口号根据 TCP/UDP 端口号进行流量分担。

聚合组 ID

配置范围：1-N (N 为端口数/2)

功能：配置聚合组 ID 号。

描述：同一聚合组的成员端口具有相同的端口属性。聚合组的数量取决于设备端口，每个聚合组最多支持 8 个成员端口。

源端口

配置选项：使能/不使能

功能：选择加入指定聚合组的端口。

7.4.1.4 典型配置举例

如图 132 所示，SwitchA 的 3 个端口（端口 1、2、3）分别接入 SwitchB 的 3 个端口（端口 1、2、3）形成聚合组 1，从而实现流量在各端口间的分担（假设交换机的 3 个聚合端口有相同的属性）。

交换机配置过程：

1、SwitchA 中选择成员端口 1、2、3 加入聚合组 1，见图 133；

2、SwitchB 中选择成员端口 1、2、3 加入聚合组 1，见图 133。

7.4.2 LACP

7.4.2.1 介绍

LACP（Link Aggregation Control Protocol，链路聚合控制协议）是基于 IEEE802.3ad 标准的协议，通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元）与对端端口交互信息，已选择动态聚合组中的成员端口。

7.4.2.2 实现

使能 LACP 协议的端口通过发送 LACPDU 报文向对端告知本端的设备 LACP 优先级、设备 MAC、端口 LACP 优先级、端口号和 key 值。对端接收到 LACPDU 报文后和本端进行协商：

1、比较两端的设备 ID（设备 ID = 设备 LACP 优先级+设备 MAC），首先比较设备 LACP 优先级，如果相同则比较设备 MAC 地址，选择设备 ID 小的一端为主设备。

2、比较主设备的端口 ID（端口 ID = 端口 LACP 优先级+端口号），首先比较端口 LACP 优先级，如果相同则比较端口号，选择端口 ID 小的端口为参考端口。

3、如果端口与参考端口的 key 值、端口属性配置都相同且处于 up 状态，并且该端口的对端端口与参考端口的对端端口的 key 值、端口属性配置也相同时，该端口才可能成为动态聚合组的成员端口。

7.4.2.3 Web 页面配置

1、配置 LACP 优先级，如下图所示；

图 134 配置 LACP 优先级

LACP

配置范围：1-65535

默认配置：32768

功能：配置设备 LACP 优先级，用于在进行 LACP 协商时选择主设备。

2、LACP 端口配置，如图 154 所示：

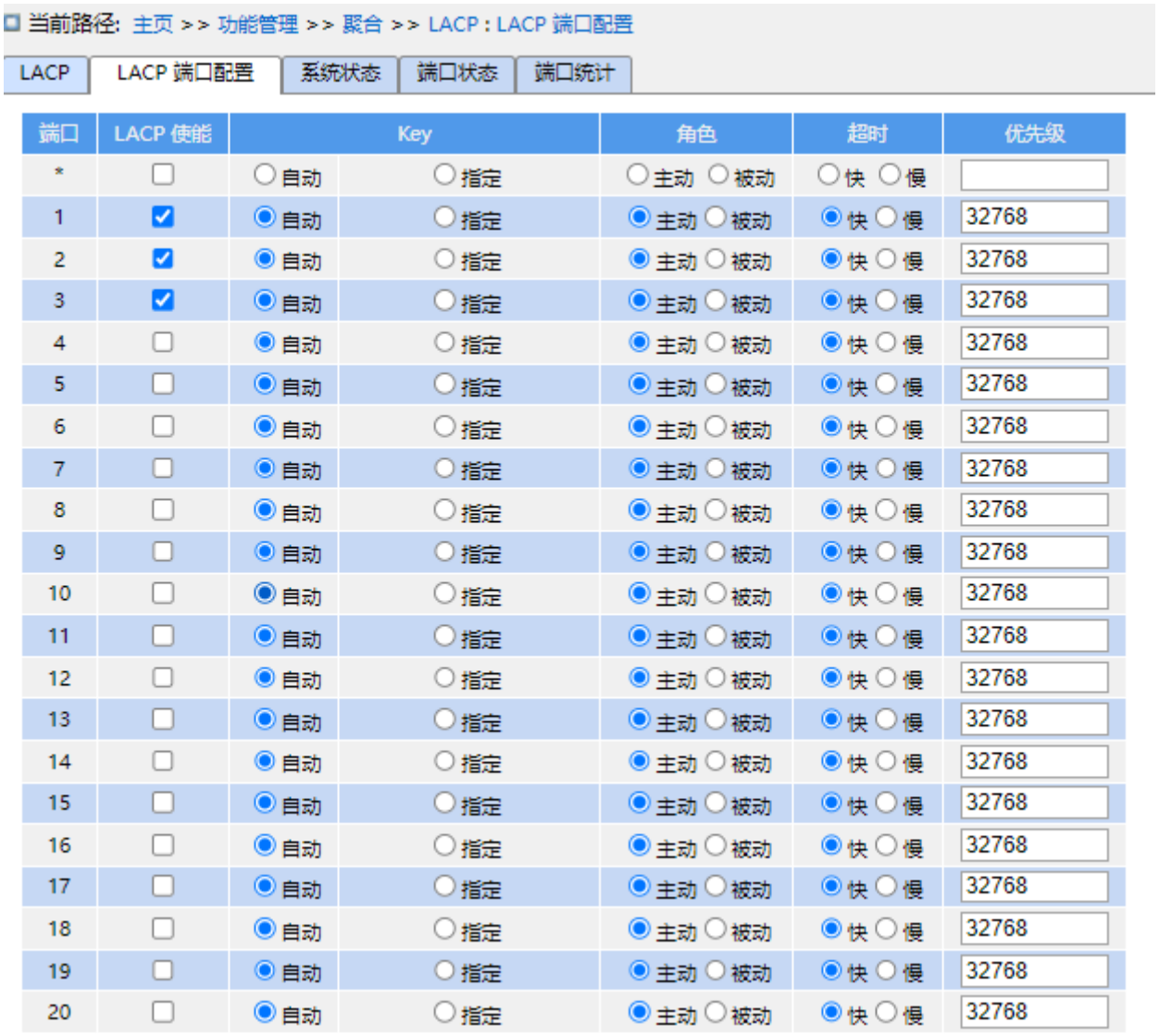


图 135 配置 LACP 端口

LACP 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的 LACP 协议。

Key

配置选项：自动/指定（1~65535）

默认配置：自动

功能：配置端口 key 值。选择自动时，key 值由端口速率决定，key=1（10Mb）；key=2（100Mb）；key=3（1000Mb），key 值不同的端口不能加入动态聚合组中。

角色

配置选项：主动/被动

默认配置：主动

功能：选择 LACP 的角色状态。主动的端口将主动发送 LACPDU 报文给对端端口；被动的端口接收到对端的 LACPDU 报文后才发送 LACPDU 报文给对端端口。

注意：

相连的两端端口至少有一个端口角色为主动，否则双方将无法交互信息。

超时

配置选项：快/慢

默认配置：快

功能：配置主动端口发送 LACPDU 报文的时间间隔。快指间隔时间为 1s；慢指间隔时间为 30s。

优先级

配置范围：1~65535

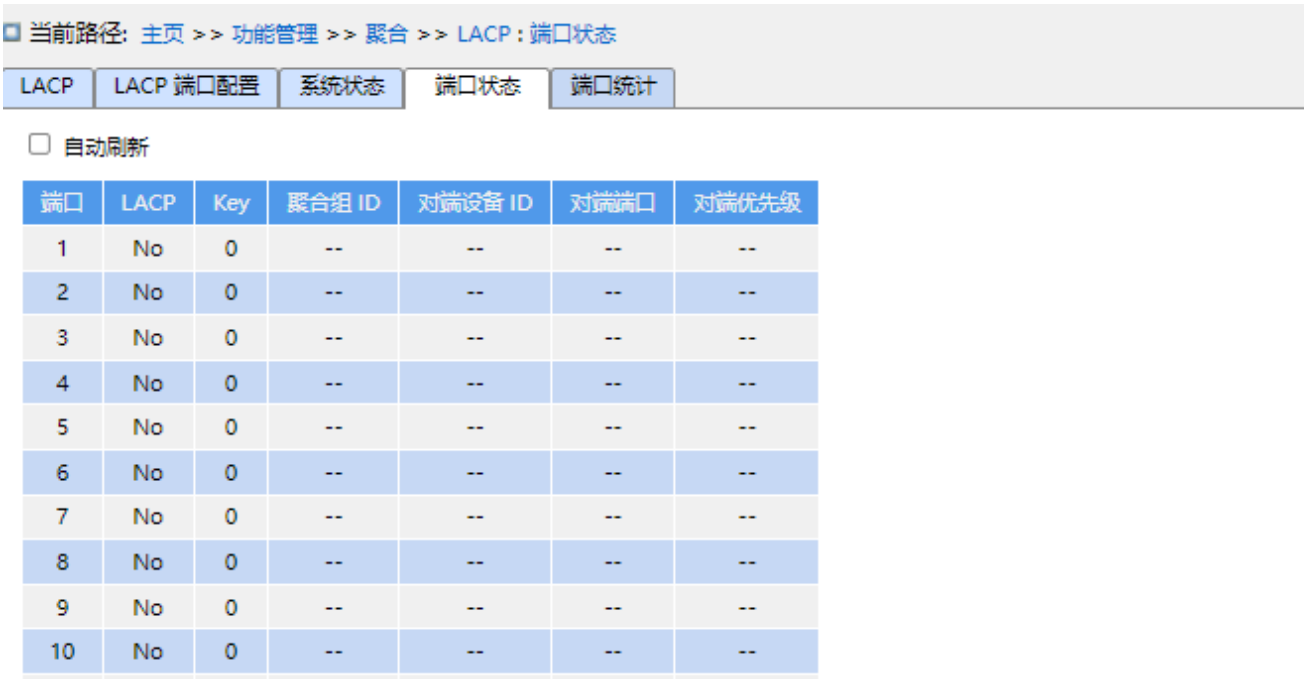
默认配置：32768

功能：配置端口 LACP 优先级，用于选择参考端口时使用。主设备中优先级小的端口被选择为参考端口。

3、查看 LACP 系统状态，如下图所示；

图 136 查看 LACP 系统状态

4、查看端口 LACP 状态，如下图所示；



端口	LACP	Key	聚合组 ID	对端设备 ID	对端端口	对端优先级
1	No	0	--	--	--	--
2	No	0	--	--	--	--
3	No	0	--	--	--	--
4	No	0	--	--	--	--
5	No	0	--	--	--	--
6	No	0	--	--	--	--
7	No	0	--	--	--	--
8	No	0	--	--	--	--
9	No	0	--	--	--	--
10	No	0	--	--	--	--

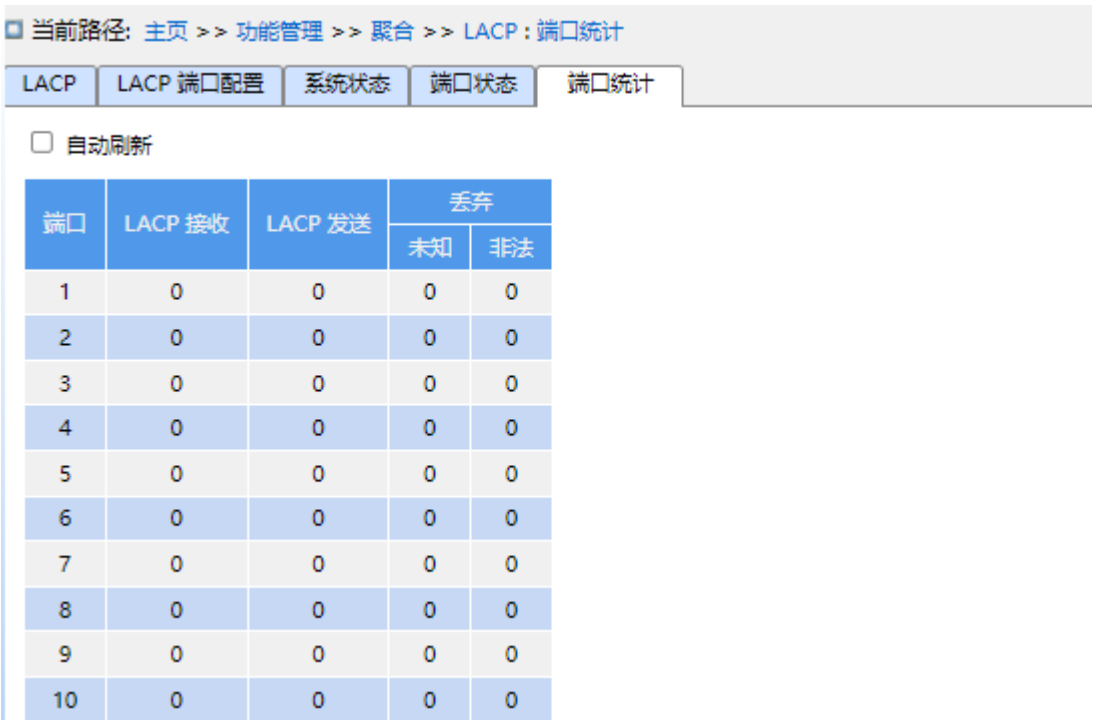
图 137 查看 LACP 端口状态

LACP 状态

显示选项：Yes/No

功能：显示端口的 LACP 状态。Yes 指端口使能 LACP 协议且端口处于 up 状态；No 指端口不使能 LACP 协议或端口处于 down 状态。

5、查看 LACP 端口统计，如下图所示；



端口	LACP 接收	LACP 发送	丢弃	
			未知	非法
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

图 138 查看 LACP 端口统计

7.4.2.4 典型配置举例

如图 132 所示，SwitchA 的 3 个端口（端口 1、2、3）分别接入 SwitchB 的 3 个端口（端口 1、2、3）形成动态聚合组 1，从而实现流量在各端口间的分担（假设交换机的 3 个聚合端口有相同的属性）。

交换机配置过程：

1、使能 SwitchA 中端口 1、2、3 的 LACP 协议，见图 135；

2、使能 SwitchB 中端口 1、2、3 的 LACP 协议，见图 135。

7.5 冗余

7.5.1.1 介绍

DT-Ring 和 DT-Ring+是本公司专有的冗余保护协议族，链路发生故障时能够在 50ms 之内快速倒换使网络恢复正常，保证稳定可靠的通信。

DT-Ring 环类型分为基于端口的环（DT-Ring-Port）和基于 VLAN 的环（DT-Ring-VLAN）：

DT-Ring-Port：针对某个具体的端口转发或阻塞报文；

DT-Ring-VLAN：某个端口针对具体的 VLAN 报文进行转发和阻塞，因此 DT-Ring-VLAN 允许相切的环端口可以有多个 VLAN 配置，即同一端口根据不同 VLAN 属性存在于不同的冗余环中。

DT-Ring-Port 和 DT-Ring-VLAN 不能混合使用。

7.5.1.2 概念

主站（Master）：一个环网中只有一个主站，主站发送 DT-Ring 环协议报文并检测当前环状态；环闭时主站的两个环端口分别处于转发状态（Forwarding）和阻塞状态（Blocking）。

说明：

环闭时首先 Link Up 的环端口处于 Forwarding 状态，后 Link Up 的环端口处于 Blocking 状态。

从站（Slave）：环网中可以有多个从站，从站监听和转发 DT-Ring 环协议报文并向主机

报告故障信息。

备份端口：DT-Ring 环与环之间的通信端口。

主备份端口：一个环中有多个备份端口时，对应设备 MAC 地址大的备份端口为主备份端口，处于转发状态（Forwarding）。

从备份端口：一个环中有多个备份端口时，除主备份端口以外的其余备份端口均为从备份端口，处于阻塞状态（Blocking）。

Forwarding 状态：端口可以接收、发送数据。

Blocking 状态：端口可以接收转发 DT-Ring 环协议报文，不能接收转发其他数据报文。

7.5.1.3 实现

DT-Ring-Port 实现

主站的 Forwarding 环端口周期性发送环协议报文检测环状态，如果主站的 Blocking 环端口收到该报文表示当前环闭合，否则处于环开状态。

A、B、C、D 交换机的工作过程：

1、配置交换机 A 为主站，其余交换机均为从站；

2、主站环端口 1 是 Forwarding 状态，环端口 2 是 Blocking 状态；从站两个环端口均为 Forwarding 状态；

3、若 CD 链路发生故障，如图 139 所示；

a) CD 链路发生故障，从站端口 6 和端口 7 为 Blocking 状态，主站端口 2 切换为 Forwarding 状态，仍能保持链路正常通信；

b) CD 链路故障恢复后，从站端口 6 和端口 7 为 Forwarding 状态，主站端口 2 切换为 Blocking 状态，链路发生倒换，恢复到故障前的状态。

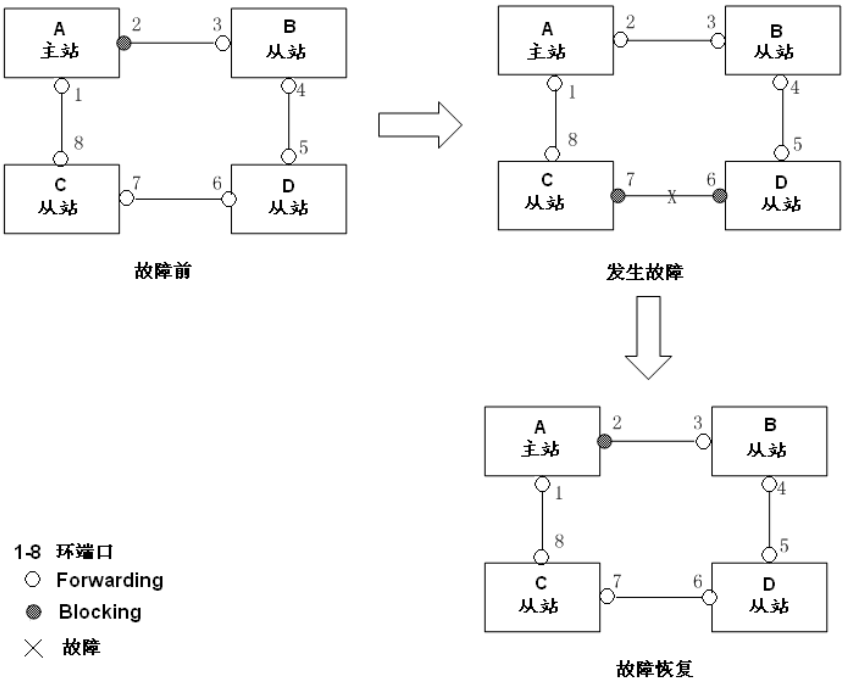


图 139 CD 链路发生故障

4、若 AC 链路发生故障，如图 140 所示；

- AC 链路发生故障时，端口 1 为 Blocking 状态，端口 2 切换为 Forwarding 状态，仍能保持链路正常通信；
- AC 链路故障恢复之后，仍保持端口 1 为 Blocking 状态，端口 8 为 Forwarding 状态，链路不进行倒换。

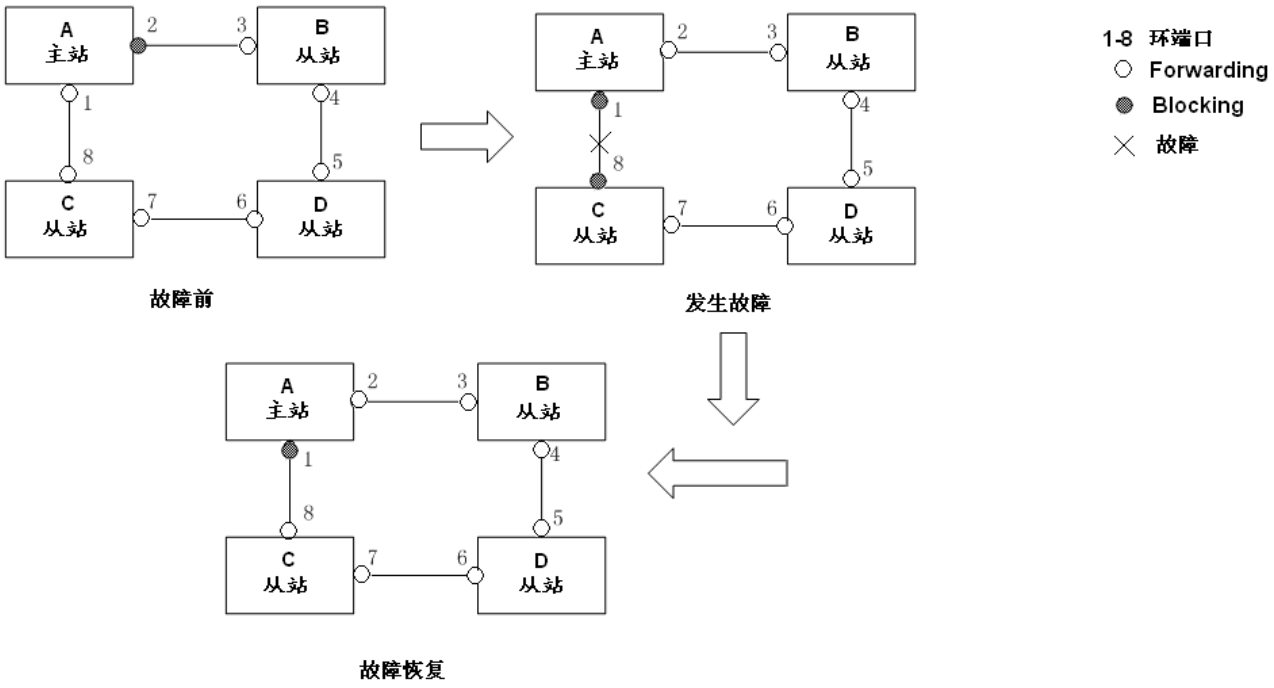


图 140 DT-Ring 链路故障

注意：

链路状态的改变影响环端口的状态。

DT-Ring-VLAN 实现

DT-Ring-VLAN 允许不同 VLAN 报文沿着不同路径进行转发，每个 VLAN 的转发路径形成一个 DT-Ring-VLAN，不同环中主站可以不同。如图 141 中有两条 DT-Ring-VLAN：

DT-Ring-VLAN 10 的环链路：AB-BC-CD-DE-EA；

DT-Ring-VLAN 20 的环链路：FB-BC-CD-DE-EF；

两个环在链路 BC、CD、DE 上相切，交换机 C 和 D 在两个环中有相同的环端口，但是通过 VLAN 隔离使用不同的逻辑链路。

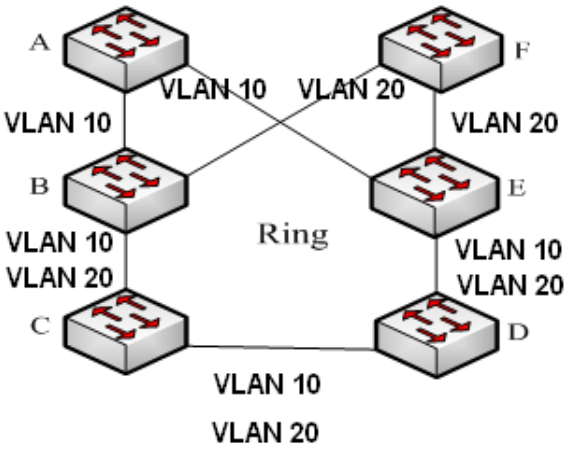


图 141 DT-Ring-VLAN

说明：

在每条 DT-Ring-VLAN 逻辑环链路中，环开环闭实现过程与 DT-Ring-Port 一致。

DT-Ring+实现

DT-Ring+可以为两个 DT-Ring 环之间提供备份，如图 142 所示，交换机 C 和 D 各配置一个备份端口，根据交换机 C 和 D 的 MAC 地址决定主备份端口。如果主备份端口或者链路出现故障，会选择从备份端口转发报文，保证冗余环间能够不成环正常通信。

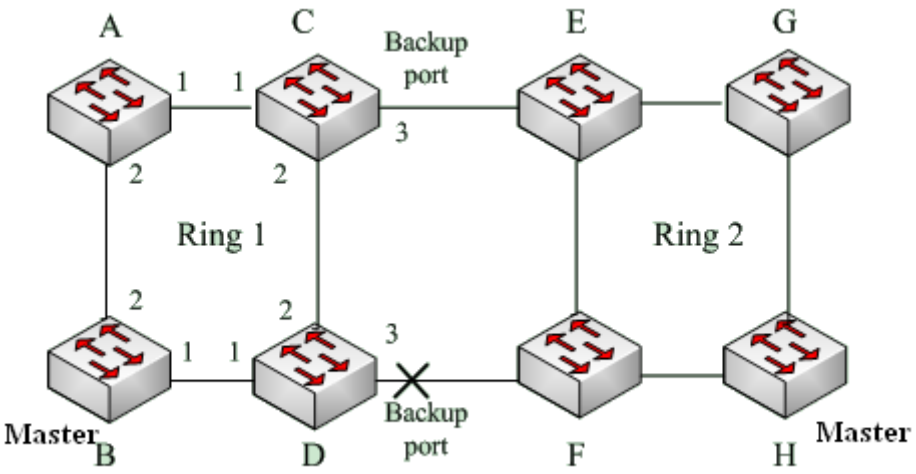


图 142 DT-Ring+拓扑

注意：

链路状态的改变影响备份端口的状态。

7.5.1.4 说明

DT-Ring 配置应满足以下条件：

- 同一环中所有交换机必须配置相同的域号；
- 每个环中只能配置一个主站，可以配置多个从站；
- 一个环中每台交换机只允许配置两个环端口；
- 针对相连的两个环，备份端口只能在其中一个环中配置；
- 一个环中最多允许配置两个备份端口；
- 一台交换机在一个环中只能配置一个备份端口；
- 一台交换机不能同时配置 DT-Ring-Port 和 DT-Ring-VLAN。

7.5.1.5 Web 页面配置

1、配置 DT-Ring 冗余模式，如图 143 所示；

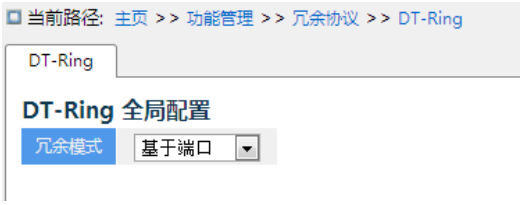


图 143 配置冗余模式

冗余模式

配置选项：基于端口/基于 VLAN

默认配置：基于端口

功能：选择 DT-Ring 冗余模式。

注意：

- 基于端口的环协议包括 RSTP、DT-Ring-Port 和 DRP-Port，基于 VLAN 的环协议包括 MSTP、DT-Ring-VLAN 和 DRP-VLAN；
- 基于 VLAN 的环协议之间互斥，一台设备只能配置一种基于 VLAN 的环协议；
- 基于端口的环协议和基于 VLAN 的环协议互斥，一台设备只能选择一种环协议模式。

2、配置 DT-Ring-Port 和 DT-Ring-VLAN，如图 144、图 145 所示；

图 144 DT-Ring-Port 配置

图 145 DT-Ring-VLAN 配置

域 ID

配置范围：1~32

功能：域号用来区分不同的环，该系列交换机最多支持 16 个基于 VLAN 的环，基于端口的环数量取决于设备端口。

域名称

配置范围：1~31 个字符

功能：配置域名称。

站点类型

配置选项：主站/从站

默认：主站

功能：选择当前环中交换机的角色。

环端口 1/环端口 2

配置选项：交换机中所有端口

功能：选择两个环端口。

注意：

- DT-Ring 环端口、备份端口与端口聚合互斥，DT-Ring 环端口和备份端口不能加入聚合组；加入聚合组的端口也不可以配置为 DT-Ring 环端口和备份端口；
- 基于端口的环协议 RSTP、DT-Ring-Port 和 DRP-Port 之间环端口互斥，即 DT-Ring-Port 环端口和备份端口不能配置为 RSTP 端口、DRP-Port 环端口、DRP-Port 备份端口；RSTP 端口、DRP-Port 环端口、DRP-Port 备份端口也不能配置为 DT-Ring-Port 环端口和备份端口；
- 建议不要将隔离组中的端口同时配置为 DT-Ring 环端口、备份端口；DT-Ring 环端口、备份端口不要同时加入隔离组。

DT-Ring+

配置选项：使能/去使能

默认配置：去使能

功能：是否使能 DT-Ring+功能。

备份端口

配置选项：交换机中所有端口

功能：选择一个端口作为备份端口。

说明：只有使能 DT-Ring+功能之后才需配置备份端口。

注意：

备份端口选择除环端口外的其他端口。

VLAN ID

配置选项：已创建的 VLAN 列表

功能：选择当前环端口允许通过的 VLAN 列表。包含多个 VLAN 时，可以用“，”和“-”特殊字符连接，“-”连接连续的 VLAN 号，“，”连接不连续的 VLAN 号。

3、查看、修改 DT-Ring 配置，如图 146 所示；

图 146 查看并修改 DT-Ring 配置

选中其中一条 DT-Ring 表项，点击<修改>按钮修改该 DT-Ring 表项配置；点击<删除>按钮即删除该 DT-Ring 表项。

4、点击 DT-Ring 表项，显示 DT-Ring 环状态和各端口状态，如图 147 所示；

图 147 查看 DT-Ring 状态

7.5.1.6 典型配置举例

如图 142 所示组网情况，A、B、C、D 形成 Ring1；E、F、G、H 形成 Ring2；CE 和 DF 为 Ring1 和 Ring2 的备份链路。

交换机 A 配置过程：

1、域 ID：1；域名称：a；环端口选择 1 和 2；站类型：从站；DT-Ring+不使能，不需配置备份端口，见图 144；

交换机 B 配置过程：

2、域 ID：1；域名称：a；环端口选择 1 和 2；站类型：主站；DT-Ring+不使能，不需配置备份端口，见图 144；

交换机 C、D 配置过程：

3、域 ID：1；域名称：a；环端口选择 1 和 2；站类型：从站；DT-Ring+使能，备份端口选择 3，见图 144；

交换机 E、F、G 配置过程：

4、域 ID：2；域名称：b；环端口选择 1 和 2；站类型：从站；DT-Ring+不使能，不需配置备份端口，见图 144；

交换机 H 配置过程：

5、域 ID：2；域名称：b；环端口选择 1 和 2；站类型：主站；DT-Ring+不使能，不需配置备份端口，见图 144；

7.5.2 DRP

7.5.2.1 介绍

DRP（Distributed Redundancy Protocol）是本公司针对环形拓扑提出的数据传输冗余保护协议，当以太网环闭时，该协议能够防止数据环路引起的广播风暴，而在环网出现链路故障或节点故障时能够实时切换到备用链路上来保证数据报文的正常传输。

DRP 协议符合 IEC-62439-6 标准，并采用无固定主站的主站选举机制。该协议具有以下优势：

- 与网络规模无关的故障恢复时间

通过对环网检测报文数据转发机制的优化，DRP 协议能够实现与网络规模无关的故障恢复时间，通过实时中断上报等机制的引入，DRP 的故障恢复时间能够达到 20ms 以内，从而

大大提高实时报文传输时的可靠性，对电力、轨道交通等要求实时控制的应用领域提供更可靠的数据承载。

- 支持丰富的链路检测功能

为了提高网络稳定性，DRP 协议针对网络应用中的典型故障进行分析，在进行故障检测时除了对链路断开进行快速检测外，还提供了光纤单通检测、链路质量检测、设备健康性检测等机制，并根据以上来确保环网承载报文的最优承载。

- 支持多种网络拓扑

DRP 除支持简单环网快速自愈功能外，还能够支持相交环、相切环等复杂组网，并能够支持基于 VLAN 的冗余环多实例，提供灵活的组网模式满足多种网络应用需求。

- 提供丰富的诊断维护功能

DRP 协议提供了丰富的状态查询和告警机制来帮助对网络进行维护和诊断，并且提供机制来防止由于误操作或配置错误导致的环网风暴等问题。

7.5.2.2 概念

1、DRP 模式

DRP 分为基于端口的环（DRP-Port-Based）和基于 VLAN 的环（DRP-VLAN-Based）两种模式。

DRP-Port-Based：是针对某个具体的物理端口转发或阻塞报文；

DRP-VLAN-Based：是针对某个端口的 VLAN 属性进行转发和阻塞报文，阻塞端口只阻塞相应 VLAN 内的数据报文，不影响其它 VLAN 报文的转发，因此 VLAN-Based 允许相切的环端口可以有多个 VLAN 配置，即同一端口根据不同 VLAN 属性存在于不同的冗余环中。

2、DRP 端口状态

Forwarding 状态：即转发状态，端口可以接收、转发数据报文；

Blocking 状态：即阻塞状态，端口可以接收转发 DRP 协议报文，不能接收转发其他数据报文。

主端口：环闭时 Root 中强制处于 Forwarding 状态的环端口，该端口须由用户自行配置。

注意：

- 若 Root 中未配置主端口，环闭时首先 Link Up 的环端口处于 Forwarding 状态，后 Link Up 的环端口处于 Blocking 状态。

- Root 设备的 Blocking 端口可以主动发送 DRP 协议报文。

3、DRP 设备角色

DRP 协议通过转发 Announce 报文选举交换机角色，从而保证冗余网络不成环。

INIT：设备 DRP 协议使能但两个环端口都为 Link down 状态。

Root：设备 DRP 协议使能且至少有一个环端口为 Link up 状态，环网中 Root 由交换机加入后自主学习、判定来选举，会根据网络拓扑的变化而变化，并不是固定不变的。Root 周期性向外发送本设备的 Announce 报文。环端口状态：两个环端口分别处于 forwarding 和 blocking 状态。当 Root 收到非本设备的 Announce 报文时，如果该报文携带的比较向量大于本设备的，则根据端口的连接状态和 CRC 劣化状态切换角色为 Normal 或 B-Root。

B-Root：设备 DRP 协议使能并至少满足下列一个条件：一个环端口为 Link up，另一个环端口为 Link down；CRC 劣化；优先级大于等于 200。B-Root 设备比较并转发 Announce 报文，当收到 Announce 的比较向量比自己更低时，会切换到 Root，否则则只转发该报文，设备角色不变。环端口状态：必有一个端口处于 forwarding 状态。

Normal：设备 DRP 协议使能，两个环端口都为 Link up、无 CRC 劣化且优先级小于 200。Normal 只负责转发 Announce 报文，而不检测报文的具体内容。环端口状态：两个端口都处于 forwarding 状态。

说明：

CRC 劣化：30 分钟内 CRC 报文数超过门限值。

7.5.2.3 实现

每台交换机各自维护一个 Announce 报文比较向量，在选举交换机角色时，会将 Announce 报文比较向量大的一台交换机选举为 Root。

Announce 报文携带的比较向量中包含了足够的信息来保证交换机角色的选举，其中包含的几个重要信息如表 6 所示：

表 6 Announce 报文比较向量示意图

链路 Link 状态	CRC 劣化		设备角色优先级	设备 IP 地址	设备 MAC 地址
	CRC 劣化状态	CRC 劣化速率			

链路 Link 状态：当设备中有一个端口 Link down 时，则置为 1；两个端口都为 Link up 时置 0；

CRC 劣化状态：当设备中有一个端口 CRC 劣化，则置为 1；CRC 正常则置 0；

CRC 劣化速率：30 分钟内 crc 报文数与总报文数的比值*10000，即每接收 10000 个报文中出现 CRC 错误个数；

设备角色优先级：可在 Web 页面配置中具体配置。

将表 6 中的比较信息从左到右依次比较，具体如下：

1、首先比较链路 Link 状态，链路断开的设备比较向量较大；

2、若链路 Link 状态相同，则需比较 CRC 劣化状态，CRC 劣化的设备比较向量较大；若 CRC 劣化状态都为 1 时，CRC 劣化速率大的设备比较向量大；

3、若链路 Link 状态、CRC 劣化状态都相同，则依次比较设备角色优先级，设备 IP 地址，设备 MAC 地址，上述值大的比较向量更大；

4、最终将比较向量大的那台交换机选举为 Root。

说明：

只有 CRC 劣化状态为 1 时，CRC 劣化速率才参与设备向量比较；CRC 劣化状态为 0 时，CRC 劣化速率不参与设备向量比较。

- DRP-Port-Based 实现

交换机角色选择过程如下：

1、初始状态时，所有交换机全部处于 INIT 状态，当一个端口 Link up 后，角色切换为 Root，Root 收发 Announce 报文进行选举，通过 Announce 报文比较向量来选举端口角色；

2、将加入环网连接且 Announce 报文比较向量最大的交换机选举为 Root，Root 首先 Link up 的环端口是 forwarding 状态，另外一个环端口则是 blocking 状态；在其余的交换机中，如果交换机有一个环端口处于 Link down 或者 CRC 劣化，则该设备角色为 B-Root，如果交换机两个环端口都为 Link up 且无 CRC 劣化，则该设备角色为 Normal。

交换机故障恢复过程如图 148 所示：

1、A、B、C 和 D 初始拓扑，A 为 Root，环端口 1 为 forwarding，环端口 2 为 blocking；B、C、D 为 Normal，环端口都为 forwarding 状态；

2、当链路 CD 断开时，通过 DRP 协议，将交换机 C 和 D 的环端口 6，7 置为 blocking 状态，C、D 角色切换为 Root；Root A、Root C 和 Root D 都向外发送各自 Announce 报文，由于 Root C 和 Root D 链路断开，比较向量必然大于此时 Root A 的比较向量，假设 D 的比较向量大于 C，故 D 被选举为 Root， C 角色切换为 B-Root，A 收到 D 的 Announce 报文后，发现比自己的比较向量大，且自己的环端口都为 Link up，故切换角色为 Normal，并将环端口 2 置于 forwarding 状态；

3、当链路 CD 恢复后，Root D 的比较向量仍大于 B-Root C，交换机 D 角色仍保持为 Root，

- 若交换机 D 未配置主端口，则仍保持环端口 7 仍为 blocking，8 为 forwarding 状态；
- 若交换机 D 配置端口 7 为主端口，则端口 7 切换为 Forwarding 状态，端口 8 切换为 Blocking 状态。

交换机 C 的环端口 6 为 forwarding，切换 C 角色为 Normal，所以在链路恢复时，网络不产生倒换。

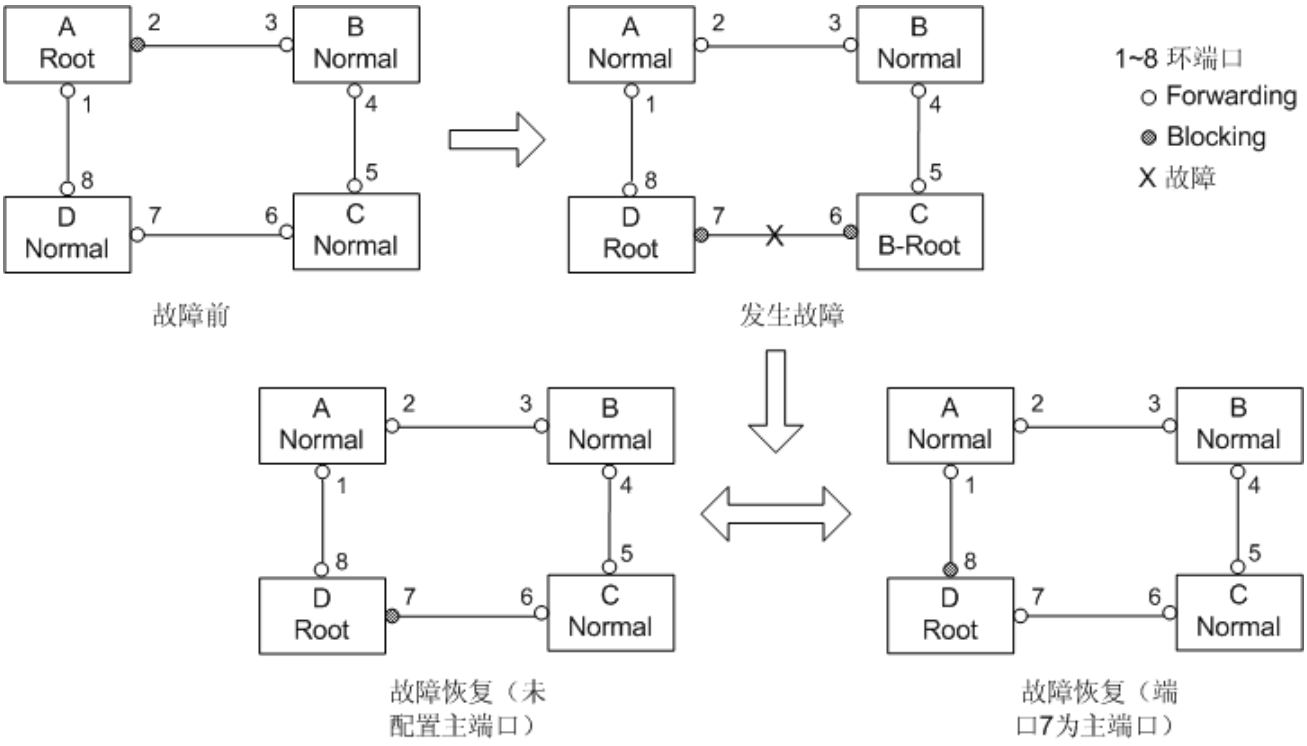


图 148 DRP 链路故障

说明：

DRP 协议环网中，网络故障时，发生一次环倒换，网络恢复时，环网不再产生倒换，提高了网络的安全性和数据传输的可靠性。

➢ DRP-VLAN-Based 实现

DRP-VLAN-Based 允许不同 VLAN 报文沿着不同路径进行转发，每个 VLAN 的转发路径形成相应的一个 DRP-VLAN-Based 环，不同环中 Root 可以不同。

如图 149 中有两个 DRP-VLAN-Based 环：

DRP-VLAN10/20-Based 的环链路：AB-BC-CD-DE-EA；

DRP-VLAN30-Based 的环链路：FB-BC-CD-DE-EF；

两个环在链路 BC、CD、DE 上相切，交换机 C 和 D 在两个环中有相同的环端口，但是通过 VLAN 隔离使用不同的逻辑链路。

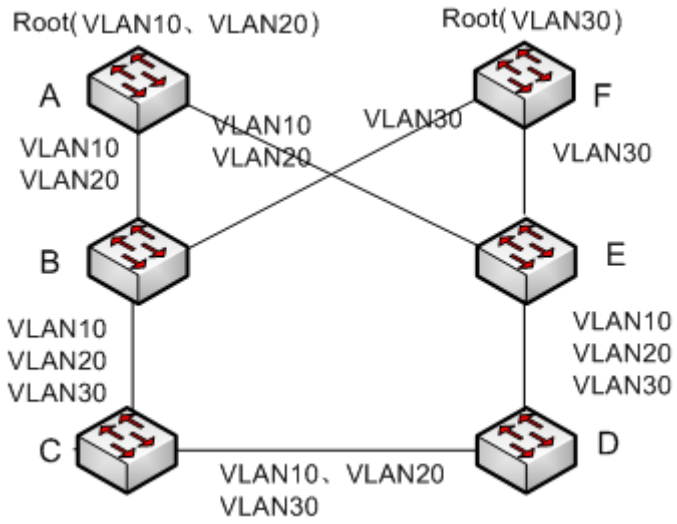


图 149 DRP-VLAN-Based

说明：

在每个 DRP-VLAN-Based 环中，设备端口状态以及角色的选择与 DRP-Port-Based 一致。

➢ DRP 备份

DRP 协议还可以为两个 DRP 环之间提供备份，保证 DRP 环间能够不成环正常通信。

备份端口：DRP 环与环之间的通信端口，可以配置多个备份端口，所有备份端口必须存在于同一个 DRP 环中，首先 Link up 的备份端口为主备份端口，主备份端口处于 forwarding 状态；其余备份端口为从备份端口，从备份端口处于 blocking 状态。

如图 150 所示，每台交换机都可以配置一个备份端口，主备份端口处于 forwording 状态，其余备份端口都处于 blocking 状态。如果主备份端口或者链路出现故障，会重新选择一个从备份端口转发数据。

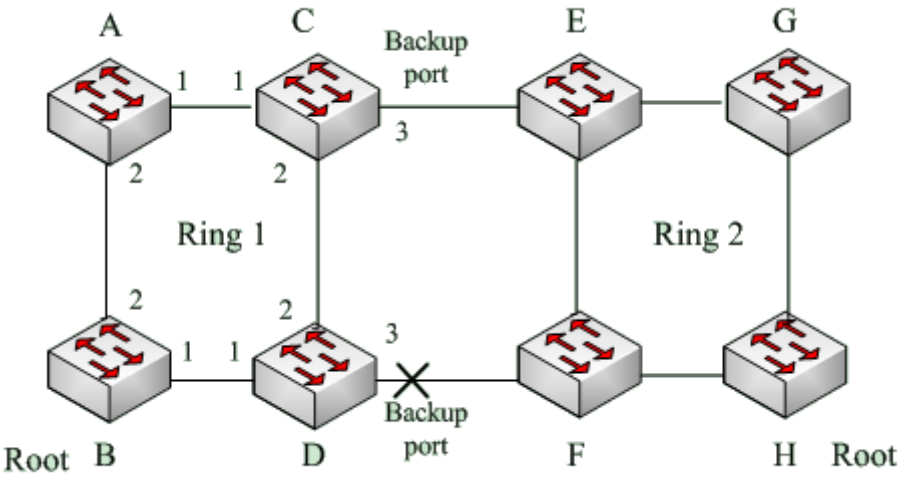


图 150 DRP 备份

注意：

链路状态的改变会影响备份端口的状态。

7.5.3 DHP

7.5.3.1 介绍

DHP（Dual Homing Protocol）：即双归链路协议，如图 151 所示，设备 A 、B、 C、 D 挂接在一个环网 Ring 中，在 A、B、C 和 D 上运行 DHP 协议，可实现如下功能：

- A、B、C、D 彼此可相互通信且不影响环网 Ring 中设备的正常运行；
- 当链路设备 AB 之间线路发生断路时，设备 A 依然可以通过环网中的 1 和 2 之间的链路实现同 B、C、D 之间正常的数据通信，实现对 A、B、C 和 D 链路的备份功能。

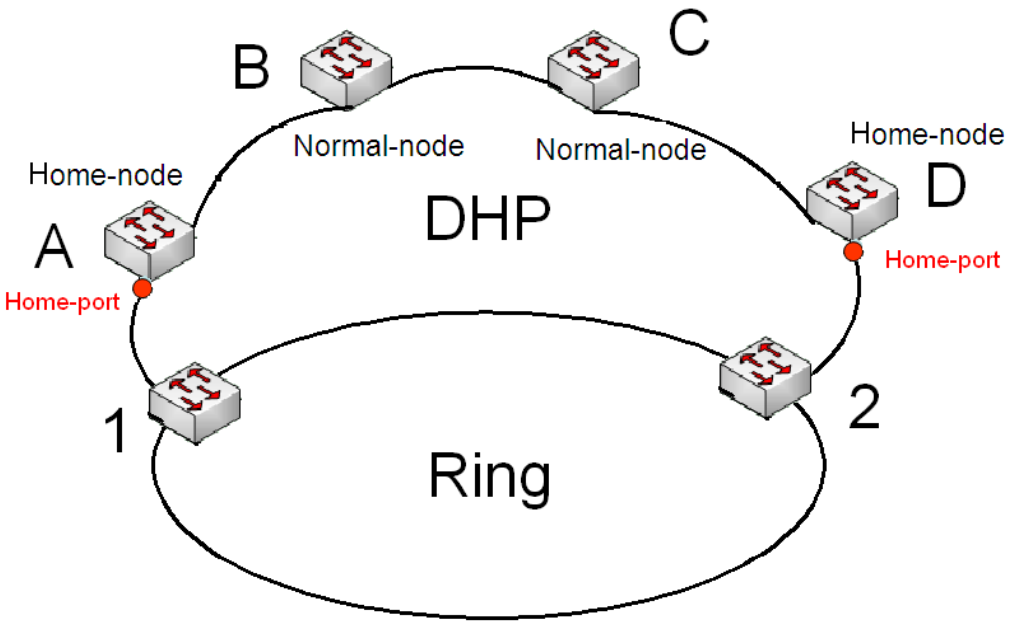


图 151 DHP 协议运用

7.5.3.2 概念

DHP 协议实现是基于 DRP 协议，链路中设备 Root 选举、设备角色切换等原理跟 DRP 实现方式一样，通过配置 Home-node，Norml-node 以及 Home-node 上的 Home-port 实现 DHP 链路备份功能。

Home-node：双归链路两端边界设备，终结 DRP 协议报文。

Home-port：在 Home Node 上，同不是双归链路中的外部设备相连的端口被称为 Home-port，通过配置 Home-port 可以实现：

- 当收到 Root 设备发出的 announce 报文时，会返回回应报文给 Root，Root 根据回应报文的接收情况指示当前链路的闭合状态；
- 阻止外部链路中的环协议报文进入本链，实现 DHP 链路和外部链路的隔离；
- 当本链路拓扑发送变化时，向外部链路发送清表报文。

Normal-node：双归链路中间设备，用于传递 Home-node 的回应报文。

7.5.3.3 实现

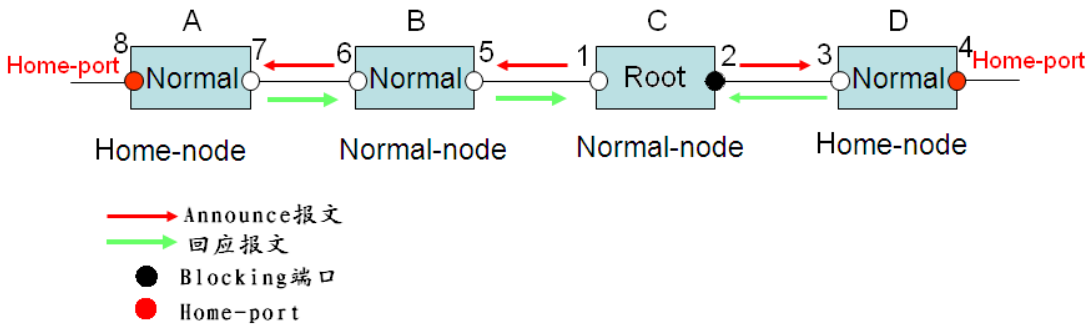


图 152 DHP 配置说明

图 151 中 A、B、C 和 D 的配置如图 152 所示；

- DRP 配置：其中 C 为 Root，环端口 2 为 blocking，A、B 和 D 为 Normal，环端口都处于 forwarding 状态；
- DHP 配置：A 和 D 为 Home-node，A 的环端口 8 和 D 的环端口 4 配置为 Home-port，B 和 C 为 Normal-node。

实现过程：

1、RootC 从两个环端口向外发送 Announce 报文，Home-port 8 和 Home-port 4 收到报文后终结 Announce 报文，并且返回回应报文给 RootC，此时链路为环闭状态， Root 环端口 2 处于 blocking 状态。

2、当链路 AB 出现故障时，该链路拓扑为 2 条链路：A 和 B-C-D

- 选举 A 为 Root，环端口 7 为 blocking 状态；
- 在 B-C-D 链路中，选举 B 为 Root，置环端口 6 为 blocking 状态，C 状态切换为 Normal，并置环端口 2 为 forwarding 状态，A 即可通过设备 1,2 与 B、C、D 进行通信，如图 153 所示。

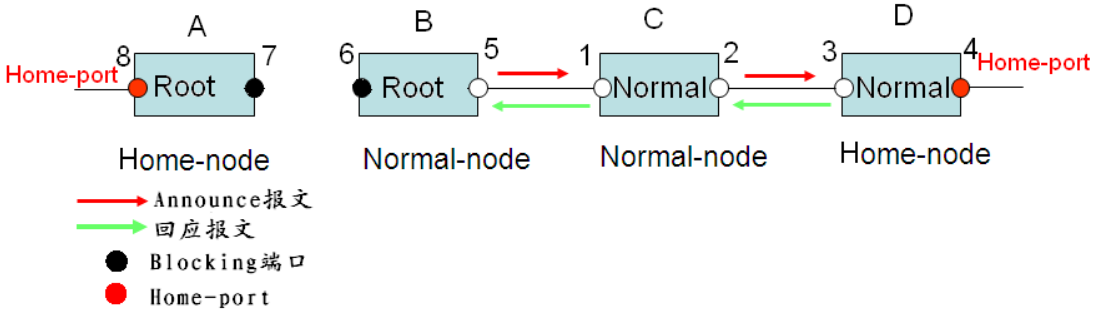


图 153 DHP 故障恢复

7.5.3.4 说明

DRP 配置满足以下条件：

- 同一环中所有交换机必须配置相同的域号；
- 一个环中只有一个 Root，可以有多个 B-Root 或 Normal；
- 交换机在一个环中只允许配置两个环端口；
- 针对相连的两个环，备份端口只能在其中一个环中配置；
- 一个环中允许配置多个备份端口；
- 一台交换机在一个环中只能配置一个备份端口。

7.5.3.5 Web 页面配置

1、配置 DRP 冗余模式，如图 154 所示；

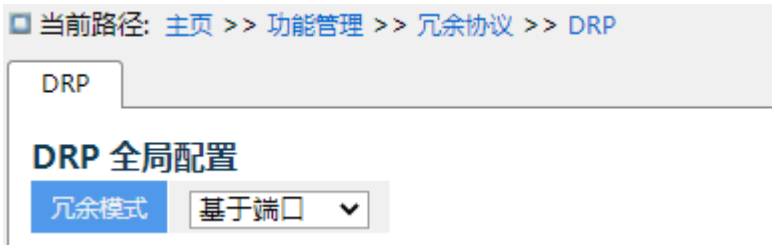


图 154 配置 DRP 冗余模式

冗余模式

配置选项：基于端口/基于 VLAN

默认配置：基于端口

功能：配置 DRP 冗余模式。

注意：

- 基于端口的环协议包括 RSTP、DRP-Port，基于 VLAN 的环协议包括 MSTP、DRP-VLAN；
- 基于 VLAN 的环协议之间互斥，一台设备只能配置一种基于 VLAN 的环协议；
- 基于端口的环协议和基于 VLAN 的环协议互斥，一台设备只能选择一种环协议模式。

2、配置 DRP-Port-Based 和 DRP-VLAN-Based，如图 155、图 156 所示；

图 155 DRP-Port-Based 配置

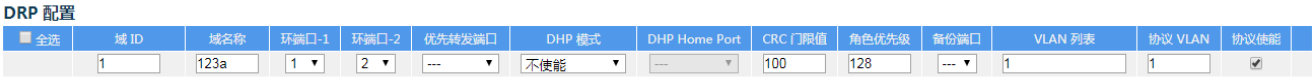


图 156 DRP-VLAN-Based 配置

域 ID

配置范围：1~32

功能：域号用来区分不同的环，该系列交换机最多支持 8 个基于 VLAN 的环，基于端口的环数量取决于设备端口。

域名称

配置范围：1~31 个字符

功能：配置域名称。

环端口 1/环端口 2

配置选项：交换机中所有端口

功能：选择两个不同的端口作为环端口。

注意：

- DRP 环端口、备份端口配置与端口聚合互斥，DRP 环端口和备份端口不能加入聚合组，加入聚合组的端口也不能配置为 DRP 环端口和备份端口；
- 基于端口的环协议 RSTP 和 DRP-Port 之间环端口互斥，即 DRP-Port 环端口和备份端口不能配置为 RSTP 端口；RSTP 端口也不能配置为 DRP-Port 环端口和备份端口；
- 建议不要将隔离组中的端口同时配置为 DRP 环端口、备份端口；DRP 环端口、备份端口不要同时加入隔离组。

优先转发端口

配置选项：--/环端口-1/环端口-2

默认配置：--

功能：配置主端口，环闭时 Root 中的主端口强制为 forwarding 状态。

DHP 模式

配置选项：Disable/Normal-Node/Home-Node

默认配置：Disable

功能：是否使能 DHP 模式以及配置 DHP 模式。

DHP Home Port

配置选项：环端口-1/环端口-2/环端口-1-2

功能：配置 DHP Home-node 上的 Home-port。

说明：如果 DHP 链路为单节点链路时，应将两个环端口都配置为 Home-port。

CRC 门限值

配置范围：25~65535

默认配置：100

功能：配置 CRC 门限值。

说明：此配置在选举 root 的时起作用，系统每隔 30 分钟检测环端口在这段时间内收到的 CRC 个数，只要有一个环端口 CRC 个数越过此门限值，认为该端口劣化，就置 Announce 报文比较向量中 CRC 劣化状态为 1。

角色优先级

配置范围：0~255

默认配置：128

功能：配置交换机优先级。

备份端口

配置选项：交换机中所有端口

功能：配置备份端口。

注意：

备份端口选择除环端口外的其他端口。

VLAN 列表

配置选项：已创建的 VLAN 列表

功能：选择当前 DRP-VLAN-Based 环管理的 VLAN，VLAN 列表需要在端口加入的 VLAN 中选择。

协议 VLAN

配置范围：1~4093

说明：该 VLAN ID 应从上面的 VLAN 列表中选择。

功能：根据携带此 VLAN ID 的 DRP 协议报文诊断和维护本 DRP-VLAN-Based 环。

协议使能

配置选项：使能/不使能

功能：使能指定域的 DRP 协议。

3、查看、修改 DRP 配置，如图 157 所示；

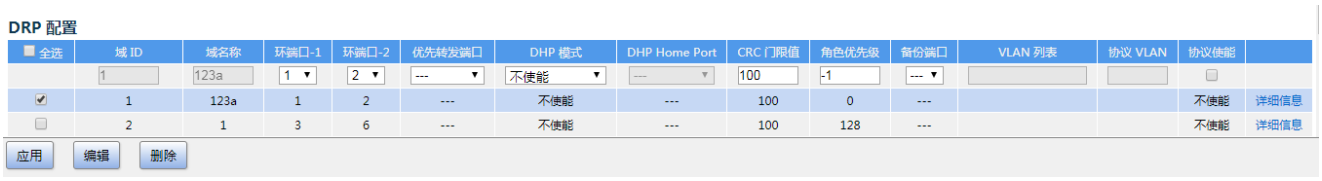


图 157 查看并修改 DRP 配置

选中其中一条 DRP 表项，点击<编辑>按钮修改该 DRP 表项配置；点击<删除>按钮即删除该 DRP 表项。在修改 DRP 参数或删除 DRP 环时，应先去使能 DRP 环协议。

4、点击图 157 中 DRP 表项后“详细信息”，显示 DRP 环中交换机的角色和各端口状态，如图 158 所示；

图 158 查看 DRP 状态

7.5.3.6 典型配置举例

如图 150 所示组网情况，A、B、C、D 形成 Ring1；E、F、G、H 形成 Ring2；CE 和

DF 为 Ring1 和 Ring2 的备份链路。

交换机 A、B 配置过程：

1、域 ID：1；域名称：a；CRC 门限值 100；角色优先级 128；环端口选择 1 和 2，备份端口可以不选择，见图 155；

交换机 C、D 的配置：

2、域 ID：1；域名称：a；CRC 门限值 100；角色优先级 128；环端口选择 1 和 2，备份端口选择 3，见图 155；

交换机 E、F、G、H 的配置：

3、域 ID：2；域名称：b；CRC 门限值 100；角色优先级 128；环端口选择 1 和 2，备份端口可以不选择，见图 155；

7.5.4 RSTP/STP 配置

7.5.4.1 介绍

STP（Spanning Tree Protocol，生成树协议 ）是根据 IEEE 协议制定的 802.1D 标准建立的，用在局域网中避免链路环路产生广播风暴并提供链路备份的协议。运行该协议的设备通过彼此交互信息，有选择的阻塞某些端口将环路网络修剪成无环路的树形网络，从而避免报文在环路网络中的增生和无限循环。STP 的不足就是不能快速迁移，必须等待 2 倍 Forward Delay 时间延迟，端口才能迁移到转发状态。

为解决 STP 协议的这个缺陷，IEEE 推出了 802.1w 标准，作为对 802.1D 标准的补充。在 IEEE 802.1w 标准里定义了快速生成树协议 RSTP（Rapid Spanning Tree Protocol）。RSTP 协议在 STP 协议基础上做了以下改进使得收敛速度快得多：为根端口和指定端口分别配置了快速切换的替换端口（Alternate Port）和备份端口（Backup Port），当根端口失效时，替换端口便无时延地进入转发状态。

7.5.4.2 基本概念

根桥：在树形网络结构中类似于树根的作用，根桥在全网中只有一个，而且根桥会根据网络拓扑的变化而变化，并不是固定不变的。根桥周期性发送 BPDU 配置消息，其他设备对该配置消息进行转发来保证拓扑稳定。

根端口：从非根桥到根桥传输的最佳端口，即到根桥开销最小的端口。根端口负责与根桥

进行通信，非根桥设备有且只有一个根端口，根桥设备没有根端口。

指定端口：向其他设备或者局域网转发配置消息的端口，根桥的所有端口都是指定端口。

替换端口：根端口的备份端口，根端口发生故障后，替换端口将成为新的根端口。

备份端口：指定端口的备份端口，指定端口发生故障后，备份端口将转换为新的指定端口转发数据。

7.5.4.3 BPDU 配置消息

为使通信链路不成环，局域网中所有网桥共同计算出一棵生成树。这个过程通过在设备之间传递 BPDU 报文来确定网络的拓扑结构，BPDU 报文的数据结构如表 7 所示；

表 7 BPDU 数据

…	根桥 ID	根路径开销	指定桥 ID	指定端口 ID	Message age	Max age	Hello time	Forward delay	…
…	8 字节	4 字节	8 字节	2 字节	2 字节	2 字节	2 字节	2 字节	…

根桥 ID：2 字节根桥优先级+6 字节根桥 MAC 地址；

根路径开销：到根桥路径中所有端口成本之和；

指定桥 ID：2 字节指定桥优先级+6 字节指定桥 MAC 地址；

指定端口 ID：端口优先级+端口号；

Message age：BPDU 配置消息在网络中传播的生存期；

Max age：BPDU 配置消息在设备中能够保存的最大生存期，当 Message age > Max age 时，丢弃 BPDU 消息；

Hello time：发送 BPDU 配置消息的时间间隔；

Forward delay：discarding—learning 或 learning --forwarding 状态转换延时。

7.5.4.4 实现过程

各网桥使用 BPDU 报文计算生成树的具体过程：

1、初始状态，各设备的各个端口会生成以自己为根桥的配置消息，根桥 ID 为自身设备 ID，根路径开销为 0，指定桥 ID 为自身设备的 ID，指定端口为本端口。

2、最优配置消息选择，各设备都向外发送自己的配置消息，同时也收到其他设备发送的

配置消息。每个端口收到配置消息后跟本端口的配置消息比较：

- 如果本端口的配置消息优先级高，则不作任何处理；
- 如果本端口的配置消息优先级低，就用接收到的配置消息的内容替换该端口的配置消息的内容。

设备将所有端口的配置消息进行比较，选出最优的配置消息。配置消息优先级比较原则：

- 根桥 ID 较小的配置消息优先级高；
- 若根桥 ID 相同则比较根路径开销，比较方法：用配置消息中的根路径开销加上本端口对应的路径开销，该值较小的配置消息优先级较高；
- 若根路径开销也相同，则依次比较指定桥 ID、指定端口 ID、接收该配置消息的端口 ID 等，上述值较小的配置消息优先级较高。

3、根桥的选择，生成树的根桥是具有最小桥 ID 的网桥。

4、根端口的选择，非根桥设备将接收最优配置消息的端口定为根端口。

5、 指定端口配置消息的计算，根据根端口的配置消息和根端口的路径开销，为每个端口计算一个指定端口配置消息：

- 根桥 ID 替换为根端口的配置消息的根桥 ID；
- 根路径开销替换为根端口配置消息的根路径开销加上根端口对应的路径开销；
- 指定桥 ID 替换为自身设备的 ID；
- 指定端口 ID 替换为自身端口 ID。

6、指定端口的选择，如果上述计算的配置消息优，则设备就将该端口定为指定端口，端口的配置消息被计算出来的配置消息替换并向外转发；如果端口的配置消息优，则设备不更新该端口的配置消息并将此端口阻塞，阻塞端口只能接收转发 RSTP 协议报文，不能接收转发其他数据报文。

7.5.4.5 Web 页面配置

配置 STP/RSTP 桥参数，如下图所示；

图 159 配置 RSTP/STP 桥参数

全局使能

配置选项：不使能/使能

默认配置：不使能

功能：是否使能生成树协议。

注意：

- 基于端口的环协议包括 RSTP 和 DRP-Port，基于 VLAN 的环协议包括 MSTP 和 DRP-VLAN；
- 基于端口的环协议和基于 VLAN 的环协议互斥，一台设备只能选择一种环协议模式。

协议版本

配置选项：MSTP/RSTP/STP

默认配置：MSTP

功能：选择生成树协议

桥优先级

配置范围：0~61440，步长为 4096

默认配置：32768

功能：配置网桥优先级。

描述：网桥优先级用来选择根桥，该值越小表示优先级越高。

Hello 间隔

配置范围：1~10 秒

默认配置：2 秒

功能：配置 Hello Time 值，即发送 BPDU 消息的时间间隔。

转发延时

配置范围：4~30 秒

默认配置：15 秒

功能：配置 Forward Delay 值，即状态转换时间，Discarding--Learning 或 Learning--Forwarding。

最长生存时间

配置范围：6~40 秒

默认配置：20 秒

功能：配置 Max Age 值，即 BPDU 配置消息在设备中能够保存的最大生存期。

描述：BPDU 中 message age 超过该参数值时，丢弃 BPDU 配置消息。

注意：

- 转发延时（Forward Delay Time）、Hello 间隔（Hello Time）、最长生存时间（Max Age Time）三个时间参数取值之间应满足如下关系：2*（Forward Delay Time – 1.0 seconds）>= Max Age Time；Max Age Time >= 2*（Hello Time + 1.0 seconds）；
- 建议用户采用默认值。

最大跳数

配置范围：6~40

默认配置：20

功能：配置 MST 域的最大跳数，MST 域的最大跳数限制了 MST 域的规模，域根配置的最大跳数作为 MST 域的最大跳数。

描述：从 MST 域内生成树的根桥开始，域内配置消息每经过一台设备转发，跳数被减 1，设备将丢弃收到跳数为 0 的配置消息。

注意：

- 只有 MST 域中根桥设备的最大跳数配置才有效，非根桥设备采用根桥设备的最大跳数配置；
- 建议用户采用默认值配置。

传输保持数

配置范围：1~10

默认配置：6

功能：每 Hello Time 时间内端口最多能够发送的 BPDU 报文个数。

边缘端口 BPDU 过滤

配置选项：使能/不使能

默认配置：不使能

功能：控制边缘端口是否接收和转发 BPDU 报文。

端口错误恢复

配置选项：使能/不使能

默认配置：不使能

功能：控制端口是否能从错误状态自动恢复到正常状态。

端口错误恢复超时时间

配置范围：30~86400s

功能：控制端口从错误状态恢复到正常状态的时间。

2、配置 RSTP 端口，如下图所示；

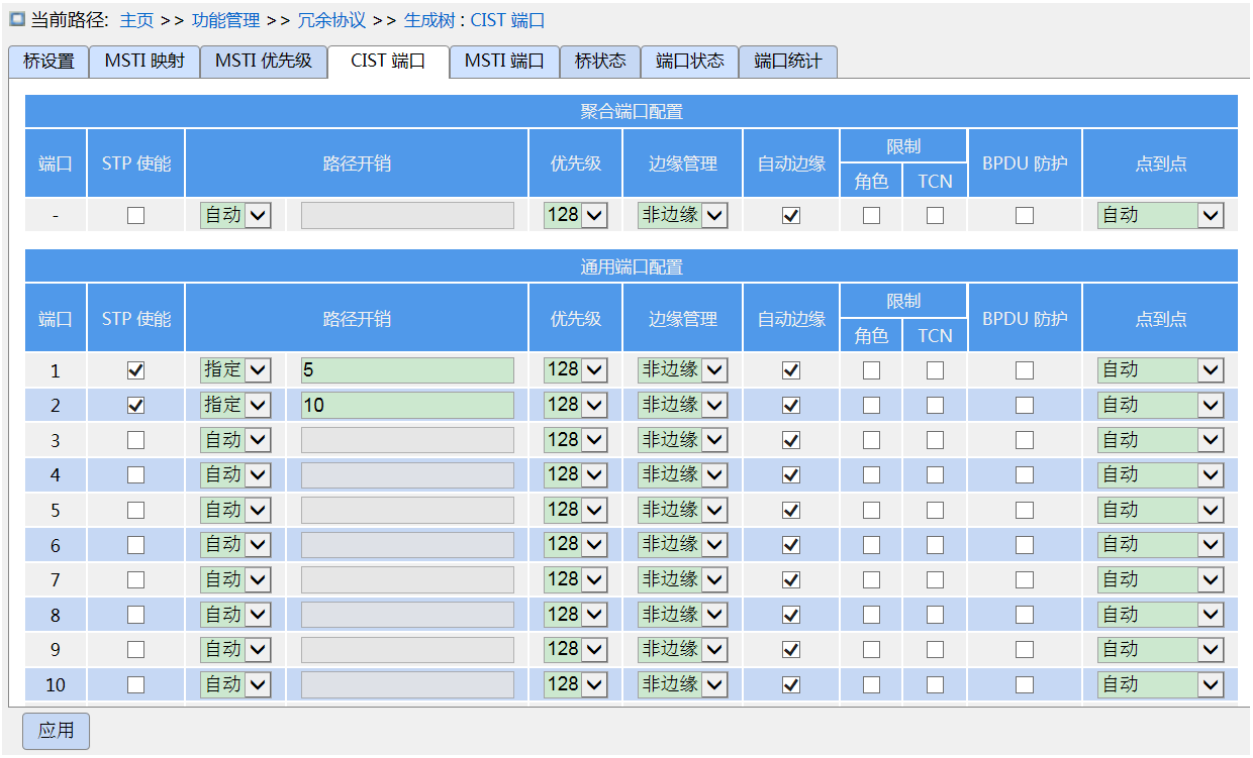


图 160 配置 RSTP 端口

CIST 聚合端口配置

功能：将聚合组作为一个 CIST 端口，并配置其在指定实例中的路径开销和优先级。

STP 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的生成树协议。

注意：

- RSTP 端口与端口聚合互斥，RSTP 端口不能加入聚合组；加入聚合组的端口也不可以配置为 RSTP 端口；
- 基于端口的环协议 RSTP 和 DRP-Port 之间环端口互斥，即 RSTP 端口不能配置为 DRP-Port；DRP-Port 也不能配置为 RSTP 端口。
- 建议不要将同一隔离组中的端口同时配置为 RSTP 端口；RSTP 端口不要加入同一隔离组中。

路径开销

配置选项：自动/指定（1~200000000）

默认配置：自动

功能：配置端口的路径开销

描述：端口路径开销用来计算最优路径，该参数取决于带宽，带宽越大开销越低。通过改变端口路径开销可以改变从当前设备到根桥的传输路径，从而改变端口角色。

优先级

配置范围：0~240，步长 16

默认配置：128

功能：配置端口优先级，用来选择端口角色。

边缘管理

配置选项：非边缘/边缘

默认配置：非边缘

功能：配置当前端口是否为边缘端口

描述：当端口直接与终端相连没有连接到其他设备或共享网段上时，该端口被认为是边缘端口，边缘端口从堵塞状态向转发状态迁移时，可以实现快速转换无需等待延时。一旦边缘端口收到 BPDU 报文后，该端口会重新变为非边缘端口。

自动边缘

配置选项：使能/不使能

默认配置：使能

功能：是否使能边缘端口自动检测功能。

限制角色

配置选项：使能/不使能

默认配置：不使能

功能：如果限制端口，会导致这个端口永远不会被选为的根节点（即使其优先级最高）。

限制 TCN

配置选项：使能/不使能

默认配置：不使能

功能：如果限制 TCN，那么这个端口不会主动发出 TCN 消息

BPDU 防护

配置选项：使能/不使能

默认配置：不使能

功能：控制边缘端口在接收到 BPDU 报文时是否进入 Error-Disable 的状态，关闭该端口。

点到点

配置选项：自动/强制点对点/强制共享

默认配置：自动

功能：配置该端口的连接类型，如果端口和点对点链路相连，则端口的状态可以快速迁移。

描述：自动指交换机会根据端口的双工状态自动检测链路类型，当端口工作在全双工模式下，认为与该端口相连的链路类型为点对点类型，当端口工作在半双工模式下，认为与该端口相连的链路类型为共享型；强制点对点指与本端口相连的链路是点对点链路；强制共享指与本端口相连的链路是共享链路。

7.5.4.6 典型配置举例

交换机 A、B、C 的优先级分别为 0、4096、8192，各个链路的路径开销分别是 4、5、10，如图 161 所示；

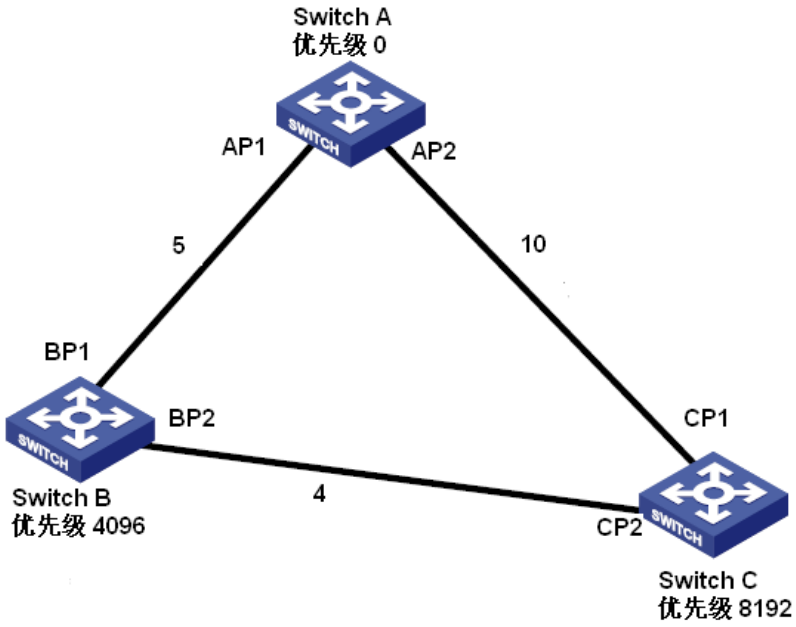


图 161 RSTP 举例

交换机 A 的配置：

1、优先级为 0，时间参数设为默认值，见图 159；

2、端口 1 的路径成本 5，端口 2 的路径成本 10，见图 160；

交换机 B 的配置：

1、优先级为 4096，时间参数设为默认值，见图 159；

2、端口 1 的路径成本 5，端口 2 的路径成本 4，见图 160；

交换机 C 的配置：

1、优先级为 8192，时间参数设为默认值，见图 159；

2、端口 1 的路径成本 10，端口 2 的路径成本 4，见图 160；

- 交换机 A 的优先级为 0，桥 ID 最小，选为根桥；
- AP1 到 BP1 的路径开销为 5，AP2 到 BP2 的路径开销为 14，所以选 BP1 为根端口；
- AP1 到 CP2 的路径开销为 9，AP2 到 CP1 的路径开销为 10，所以选 CP2 为根端口，BP2 为指定端口。

7.5.5 MSTP 配置

7.5.5.1 介绍

虽然 RSTP 可以快速收敛，但是和 STP 一样存在以下缺陷：局域网中所有网桥共享一颗生成树，所有 VLAN 的报文都沿着一颗生成树进行转发。如图 162 所示，在某种配置情况下，会把交换机 A 和 C 之间的链路 Block 掉，由于交换机 B 和 D 不包含 VLAN 1，无法转发 VLAN 1 的报文，这样交换机 A 的 VLAN 1 就无法与交换机 C 的 VLAN 1 通信。

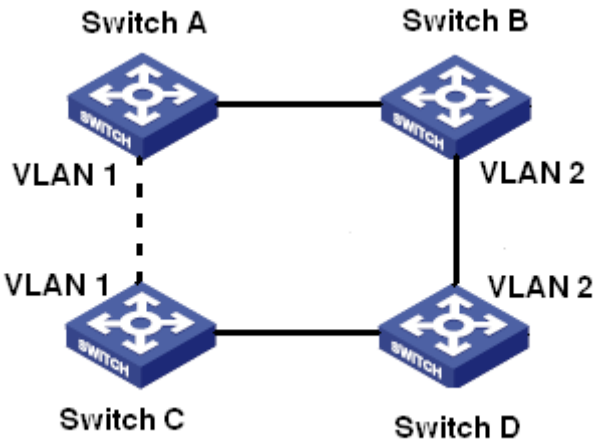


图 162 RSTP 缺陷

针对上述问题产生了 MSTP（Multiple Spanning Tree Protocol，多生成树协议），它既可以快速收敛，也可以使不同 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。

MSTP 把一个或多个 VLAN 映射到一个实例中，有着相同配置的交换机组成一个域，每个域中形成多棵生成树，生成树之间彼此独立，该域相当于一个交换机节点，与其他域再进行生成树算法运算，得出一个整体的生成树。按照这种算法，图 162 所示网络便形成图 163 所示拓扑，交换机 A 和 C 都在 Region1 中，该域中没有产生环路，所以没有链路 Block 掉；同理 Region2 中类似。Region1 和 Region2 相当于交换机节点。这两台“交换机”之间有环路，因此应该 Block 掉一条链路。

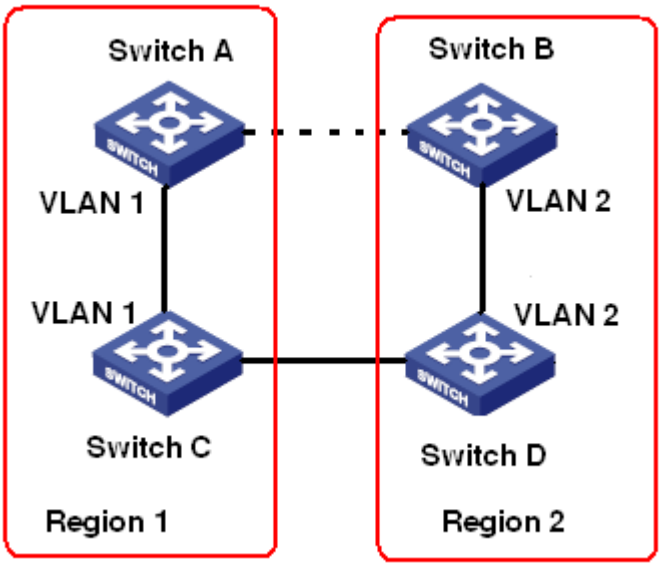


图 163 MSTP 拓扑

7.5.5.2 基本概念

结合图 164~图 167 了解 MSTP 的相关概念：

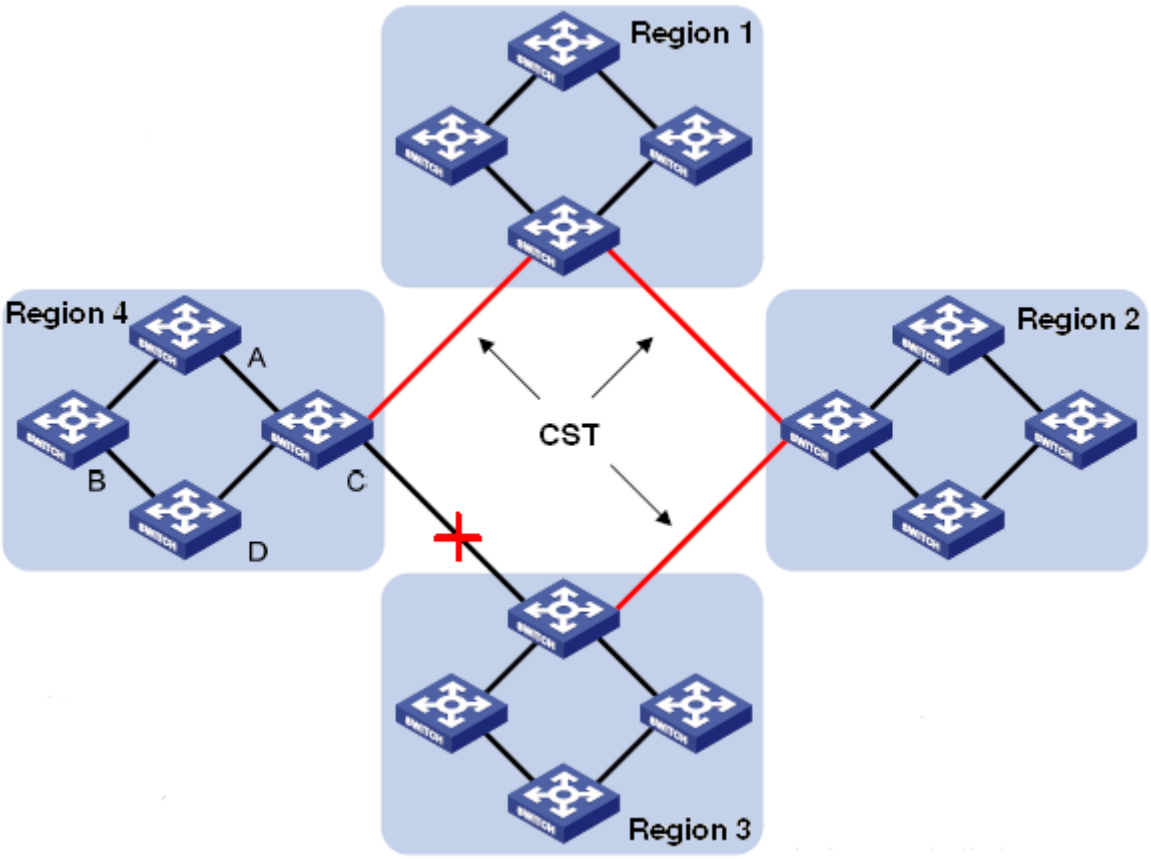


图 164 MSTP 概念解释示意图

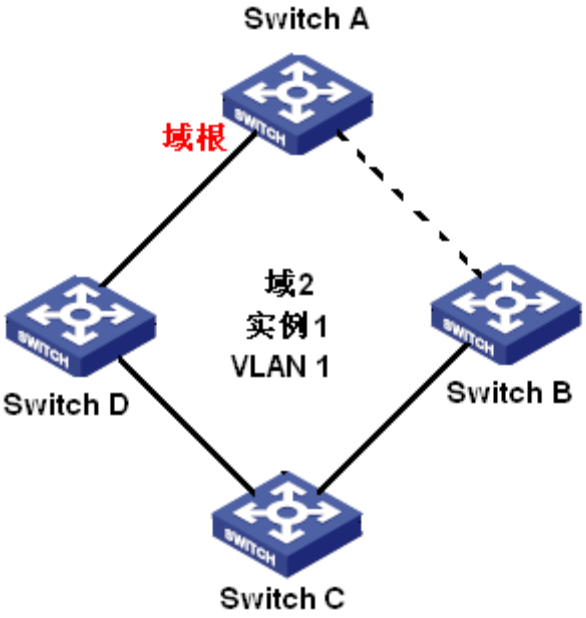


图 165 VLAN 1 映射到实例 1

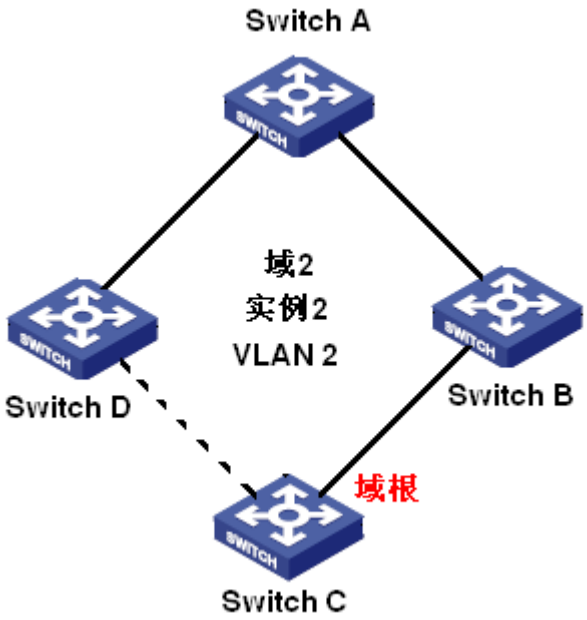


图 166 VLAN 2 映射到实例 2

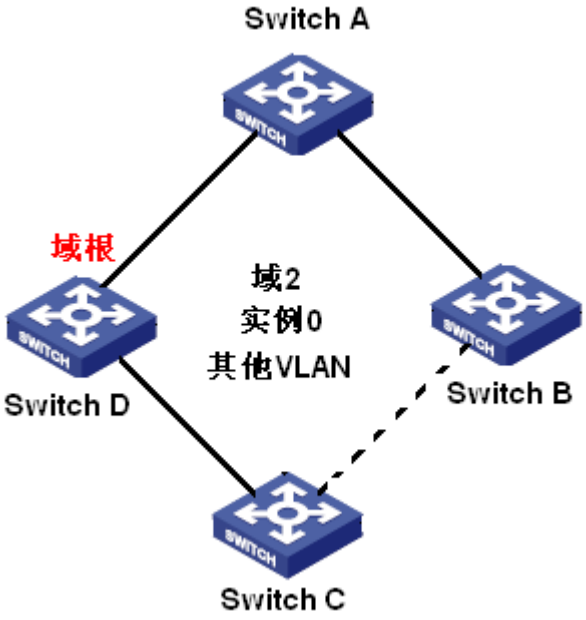


图 167 其他 VLAN 映射到实例 0

实例（Instance）：多个 VLAN 的一个集合。可以一个 VLAN 映射到一个实例（一个 VLAN 形成一棵生成树），如图 165、图 166 所示；也可以多个有相同拓扑结构的 VLAN 映射到一个实例（多个 VLAN 共享一棵生成树），如图 167 所示。不同的实例对应不同的生成树，实例 0 是针对所有域中设备的生成树，其他实例是针对当前域中设备的生成树。

MST 域（Multiple Spanning Tree Regions，多生成树域）：MSTP 域名、修订级别、VLAN 到生成树实例映射配置都相同且相互连接的交换机在同一个域中，如图 164 中 Region1、

Region2、Region3、Region4 为 4 个不同的 MST 域。

VLAN 映射表：描述 VLAN 和生成树实例之间的映射关系。图 164 中，域 2 的 VLAN 映射表是：VLAN 1 映射到生成树实例 1，如图 165 所示；VLAN 2 映射到生成树实例 2，如图 166 所示；其余 VLAN 映射到生成树实例 0，如图 167 所示。

CIST（Common and Internal Spanning Tree，公共和内部生成树）：即生成树实例 0，指连接一个交换网络内所有设备的单生成树，如图 164 中，由 IST 和 CST 共同组成。

IST（Internal Spanning Tree，内部生成树）：CIST 在 MST 域内的片段，即每个域中的实例 0，如图 167 所示；

CST（Common Spanning Tree，公共生成树）：连接交换网络内所有 MST 域的单生成树。如果把每个 MST 域看作是一个“设备节点”，CST 就是这些节点通过 STP/RSTP 协议计算的一个生成树，如图 164 中红色线条组成的生成树。

MSTI（Multiple Spanning Tree Instance，多生成树实例）：一个 MST 域中可以生成多棵生成树，每棵生成树之间彼此独立，每棵生成树都是一个 MSTI，如图 165、图 166 所示；IST 也是一个特殊的 MSTI。

总根：CIST 的根桥，网络中根桥 ID 最小的交换机被选为总根。

域根：MST 域内 IST 或 MSTI 的根桥就是域根。MST 域内每棵生成树拓扑不同，域根也可能不同，如图 165、图 166 和图 167 三个实例中域根不同。MSTI 的根桥是在当前 MST 域中通过 STP/RSTP 协议计算得到的。IST 的根桥是从与其他 MST 域连接的设备中，根据端口收到的优先级向量信息来选取。

域边界端口：位于 MST 域的边缘，连接不同 MST 域、MST 域和运行 STP 区域、MST 域和运行 RSTP 区域的端口。

端口状态：根据端口是否学习 MAC 地址和是否转发用户流量，可将端口状态划分为以下三种：

Forwarding 状态：学习 MAC 地址，转发用户流量；

Learning 状态：学习 MAC 地址，不转发用户流量；

Discarding 状态：不学习 MAC 地址，不转发用户流量。

根端口：从非根桥到根桥传输的最佳端口，即到根桥开销最小的端口，根端口负责与根桥进行通信；非根桥设备上有且只有一个根端口，根桥上没有根端口。根端口能够具有的端口状态：Forwarding、Learning、Discarding 状态。

指定端口：向其他设备或者局域网转发配置消息的端口，根桥上的所有端口都是指定端口。指定端口可以具有的端口状态：Forwarding、Learning、Discarding 状态。

Master 端口：连接 MST 域到总根的端口，位于整个域到总根的最短路径上。从 CST 上看，Master 端口是域的“根端口”（把域看成一个节点）。Master 端口是特殊的域边界端口，Master 端口在 CIST 中是根端口，在其他实例中是 Master 端口。Master 端口可以具有的端口状态：Forwarding、Learning、Discarding 状态。

Alternate 端口：根端口和 Master 端口的备份端口。当根端口或 Master 端口发生故障后，Alternate 端口将成为新的根端口或 Master 端口。Alternate 端口可以具有的端口状态：Discarding 状态。

Backup 端口：指定端口的备份端口，当指定端口发生故障后，Backup 端口便快速转换为新的指定端口，并无延时的转发数据；Backup 端口可以具有的端口状态： Discarding 状态。

7.5.5.3 MSTP 的实现

MSTP 将网络划分为多个 MST 域，各个域之间计算生成 CST；域内计算生成多棵生成树，每棵生成树是一个多生成树实例。其中实例 0 被称为 IST，其他实例为 MSTI。

1、CIST 的计算

- 设备发送接收 BPDU 报文，通过比较 MSTP 配置消息，在整个网络中选择一个优先级最高的设备作为 CIST 的总根；
- 在每个 MST 域内计算生成 IST；
- 将每个 MST 域作为单台设备对待，通过计算在域间生成 CST；
- CST 和 IST 共同构成了整个网络的 CIST。

2、MSTI 的计算

在 MST 域内，MSTP 根据 VLAN 和生成树实例的映射关系，针对不同的 VLAN 生成不同的生成树实例。每个生成树独立计算，计算过程与 STP 过程类似。

在 MST 域内，VLAN 报文沿着其对应的 MSTI 转发；在 MST 域间，VLAN 报文沿着 CST 转发。

7.5.5.4 Web 页面配置

配置 MSTP 桥参数，如下图所示；

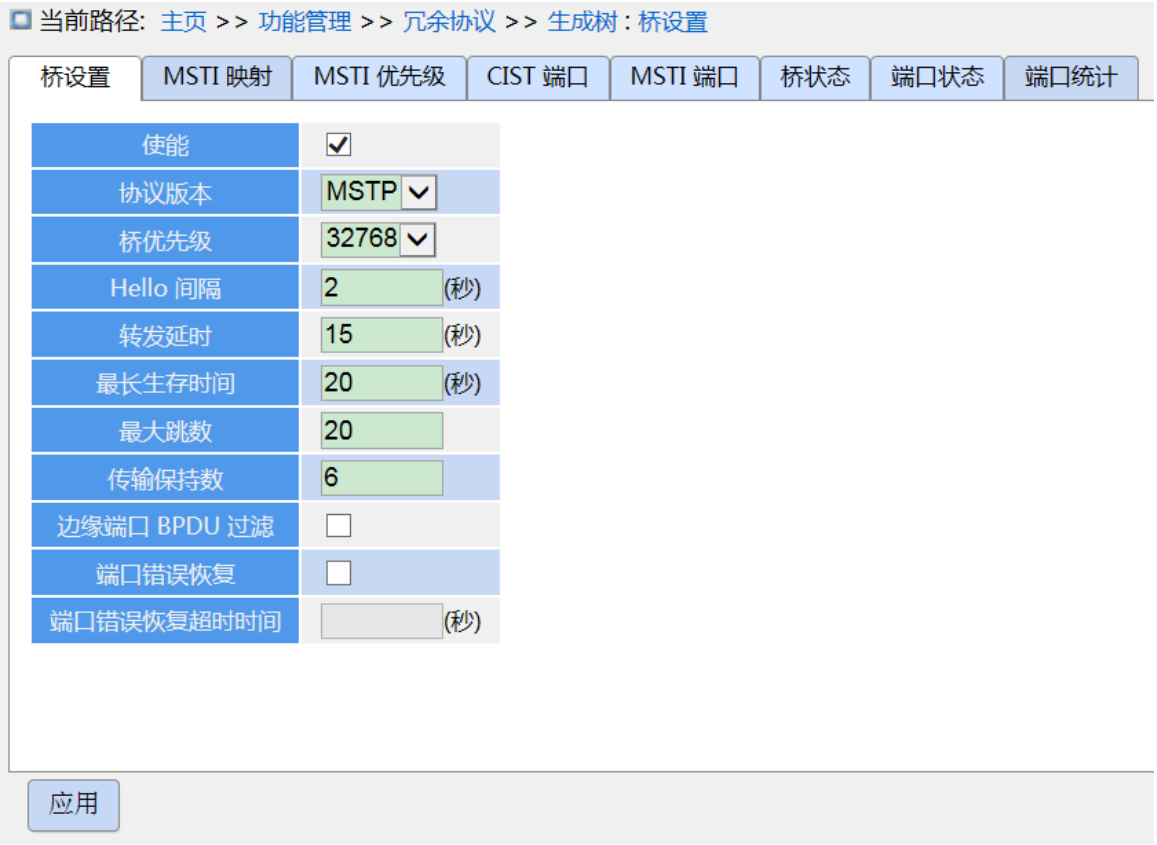


图 168 配置 MSTP 桥参数

全局使能

配置选项：不使能/使能

默认配置：不使能

功能：是否使能生成树协议。

注意：

- 基于端口的环协议包括 RSTP 和 DRP-Port，基于 VLAN 的环协议包括 MSTP 和 DRP-VLAN；
- 基于 VLAN 的环协议之间互斥，一台设备只能配置一种基于 VLAN 的环协议；
- 基于端口的环协议和基于 VLAN 的环协议互斥，一台设备只能选择一种环协议模式。

协议版本

配置选项：MSTP/RSTP/STP

默认配置：MSTP

功能：选择生成树协议

桥优先级

配置范围：0~61440，步长为 4096

默认配置：32768

功能：配置网桥优先级。

描述：网桥优先级用来选择根桥，该值越小表示优先级越高。

Hello 间隔

配置范围：1~10 秒

默认配置：2 秒

功能：配置 Hello Time 值，即发送 BPDU 消息的时间间隔。

转发延时

配置范围：4~30 秒

默认配置：15 秒

功能：配置 Forward Delay 值，即状态转换时间，Discarding--Learning 或 Learning--Forwarding。

最长生存时间

配置范围：6~40 秒

默认配置：20 秒

功能：配置 Max Age 值，即 BPDU 配置消息在设备中能够保存的最大生存期。

描述：BPDU 中 message age 超过该参数值时，丢弃 BPDU 配置消息。

注意：

- 转发延时（Forward Delay Time）、Hello 间隔（Hello Time）、最长生存时间（Max Age Time）三个时间参数取值之间应满足如下关系：2*（Forward Delay Time – 1.0 seconds）>= Max Age Time；Max Age Time >= 2*（Hello Time + 1.0 seconds）；
- 建议用户采用默认值。

最大跳数

配置范围：6~40

默认配置：20

功能：配置 MST 域的最大跳数，MST 域的最大跳数限制了 MST 域的规模，域根配置的最大跳数作为 MST 域的最大跳数。

描述：从 MST 域内生成树的根桥开始，域内配置消息每经过一台设备转发，跳数被减 1，设备将丢弃收到跳数为 0 的配置消息。

注意：

- 只有 MST 域中根桥设备的最大跳数配置才有效，非根桥设备采用根桥设备的最大跳数配置；
- 建议用户采用默认值配置。

传输保持数

配置范围：1~10

默认配置：6

功能：每 Hello Time 时间内端口最多能够发送的 BPDU 报文个数。

边缘端口 BPDU 过滤

配置选项：使能/不使能

默认配置：不使能

功能：控制边缘端口是否接收和转发 BPDU 报文。

端口错误恢复

配置选项：使能/不使能

默认配置：不使能

功能：控制端口是否能从错误状态自动恢复到正常状态。

端口错误恢复超时时间

配置范围：30~86400s

功能：控制端口从错误状态恢复到正常状态的时间。

2、配置 MSTI 映射，如下图所示；

图 169 配置 MSTI 映射

配置名称

配置范围：1~32 个字符

默认配置：当前设备的 MAC 地址

功能：配置 MST 域的名称。

配置修订号

配置范围：0~65535

默认配置：0

功能：配置 MST 域的修订号。

描述：修订号和名称、VLAN 映射表共同决定设备所属的 MST 域。只有以上配置均相同时，设备才认为彼此在同一个 MST 域中。

VLAN 映射

配置范围：1~4093

功能：配置当前 MST 域中 VLAN 的映射表。包含多个 VLAN 时，可以用“，”和“-”特殊字符连接，“-”连接连续的 VLAN 号，“，”连接不连续的 VLAN 号。

描述：默认情况下，所有的 VLAN 都映射到实例 0。一个 VLAN 只能映射到一个生成树实例。如果删除指定 VLAN 与生成树实例之间的映射关系，这些 VLAN 将重新映射到实例 0。

3、配置交换机在指定实例中的网桥优先级，如下图所示；

图 170 配置指定实例中的网桥优先级

优先级

配置范围：0~61440，步长为 4096

默认配置：32768

功能：配置交换机在指定实例中的网桥优先级。

描述：网桥优先级大小决定了该设备能否被选为生成树实例中的域根，数值越小表示优先级越高，通过配置较小的优先级，可以指定某台设备成为生成树的根桥。使能 MSTP 协议的设备在不同的生成树实例中可以配置不同的优先级。

点击<应用>按钮使当前配置生效。

4、配置 CIST 端口，如下图所示；

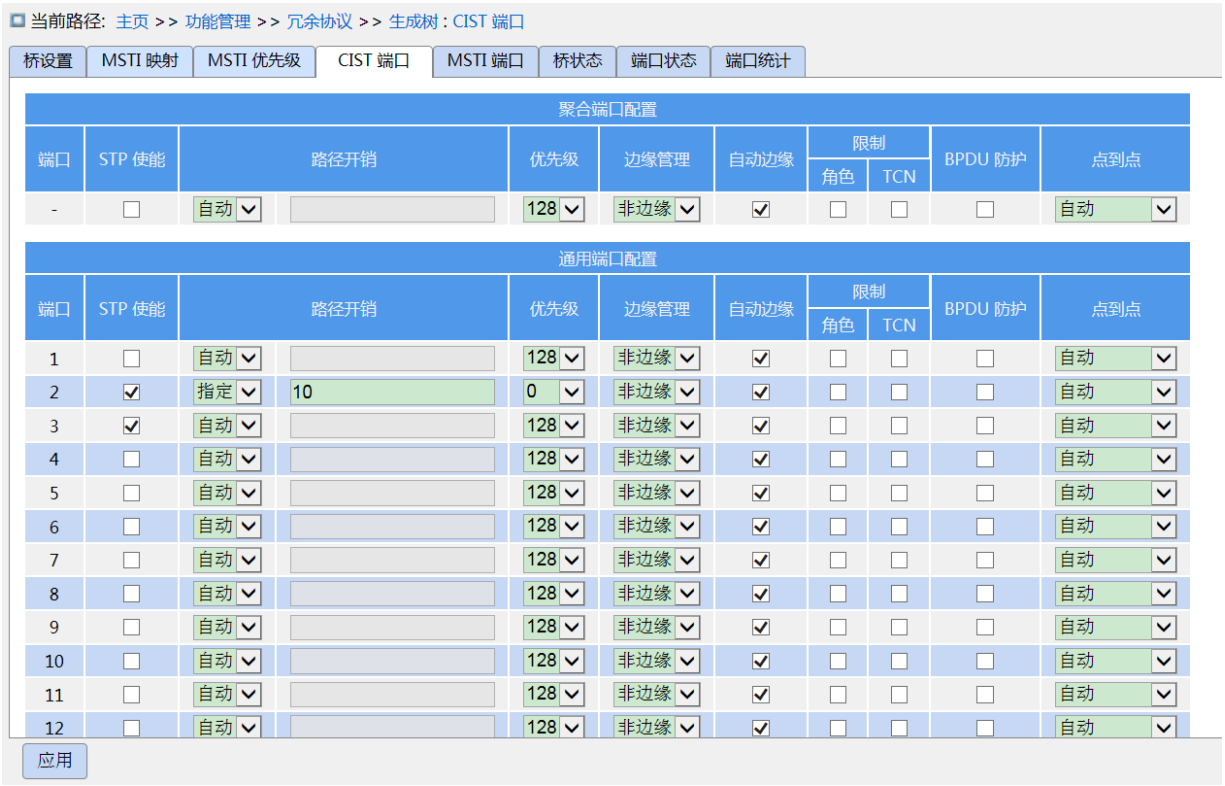


图 171 配置 CIST 端口

CIST 聚合端口配置

功能：将聚合组作为一个 CIST 端口，并配置其在指定实例中的路径开销和优先级。

STP 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的生成树协议。

注意：

- MSTP 端口与端口聚合互斥，MSTP 端口不能加入聚合组；加入聚合组的端口也不可以配置为 MSTP 端口；
- 建议不要将同一隔离组中的端口同时配置为 MSTP 端口；MSTP 端口不要加入同一隔离组中。

路径开销

配置选项：自动/指定（1~200000000）

默认配置：自动

功能：配置端口的路径开销

描述：端口路径开销用来计算最优路径，该参数取决于带宽，带宽越大开销越低。通过改

变端口路径开销可以改变从当前设备到根桥的传输路径，从而改变端口角色。

优先级

配置范围：0~240，步长 16

默认配置：128

功能：配置端口优先级，用来选择端口角色。

边缘管理

配置选项：非边缘/边缘

默认配置：非边缘

功能：配置当前端口是否为边缘端口

描述：当端口直接与终端相连没有连接到其他设备或共享网段上时，该端口被认为是边缘端口，边缘端口从堵塞状态向转发状态迁移时，可以实现快速转换无需等待延时。一旦边缘端口收到 BPDU 报文后，该端口会重新变为非边缘端口。

自动边缘

配置选项：使能/不使能

默认配置：使能

功能：是否使能边缘端口自动检测功能。

限制角色

配置选项：使能/不使能

默认配置：不使能

功能：如果限制端口，会导致这个端口永远不会被选为的根节点（即使其优先级最高）。

限制 TCN

配置选项：使能/不使能

默认配置：不使能

功能：如果限制 TCN，那么这个端口不会主动发出 TCN 消息。

BPDU 防护

配置选项：使能/不使能

默认配置：不使能

功能：控制边缘端口在接收到 BPDU 报文时是否进入 Error-Disable 的状态，关闭该端口。

点到点

配置选项：自动/强制点对点/强制共享

默认配置：自动

功能：配置该端口的连接类型，如果端口和点对点链路相连，则端口的状态可以快速迁移。

描述：自动指交换机会根据端口的双工状态自动检测链路类型，当端口工作在全双工模式下，认为与该端口相连的链路类型为点对点类型，当端口工作在半双工模式下，认为与该端口相连的链路类型为共享型；强制点对点指与本端口相连的链路是点对点链路；强制共享指与本端口相连的链路是共享链路。

5、配置 MSTI 端口，如下图所示；

图 172 配置 MSTI 端口

选择 MSTI

配置选项：MST1~MST7

默认配置：MST1

功能：选择一个 MST 实例

MSTI 聚合端口配置

功能：将聚合组作为一个 MSTP 端口，并配置其在指定实例中的路径开销和优先级。

路径开销

配置选项：自动/指定（1~200000000）

默认配置：自动

功能：配置端口在指定实例中的路径开销。

描述：端口路径路径开销用来计算最优路径，该参数取决于带宽，带宽越大成本越低。通过改变端口路径成本可以改变从当前设备到根桥的传输路径，从而改变端口角色。使能 MSTP 协议的端口在不同生成树实例中可以配置不同的路径开销。

优先级

配置范围：0~240，步长 16

默认配置：128

功能：配置端口在指定实例中的优先级。

描述：端口优先级决定端口是否会被选为根端口，同等条件下优先级低的端口被选为根端口。使能 MSTP 协议的端口在不同生成树实例中可以配置不同的优先级，担任不同的端口角色。

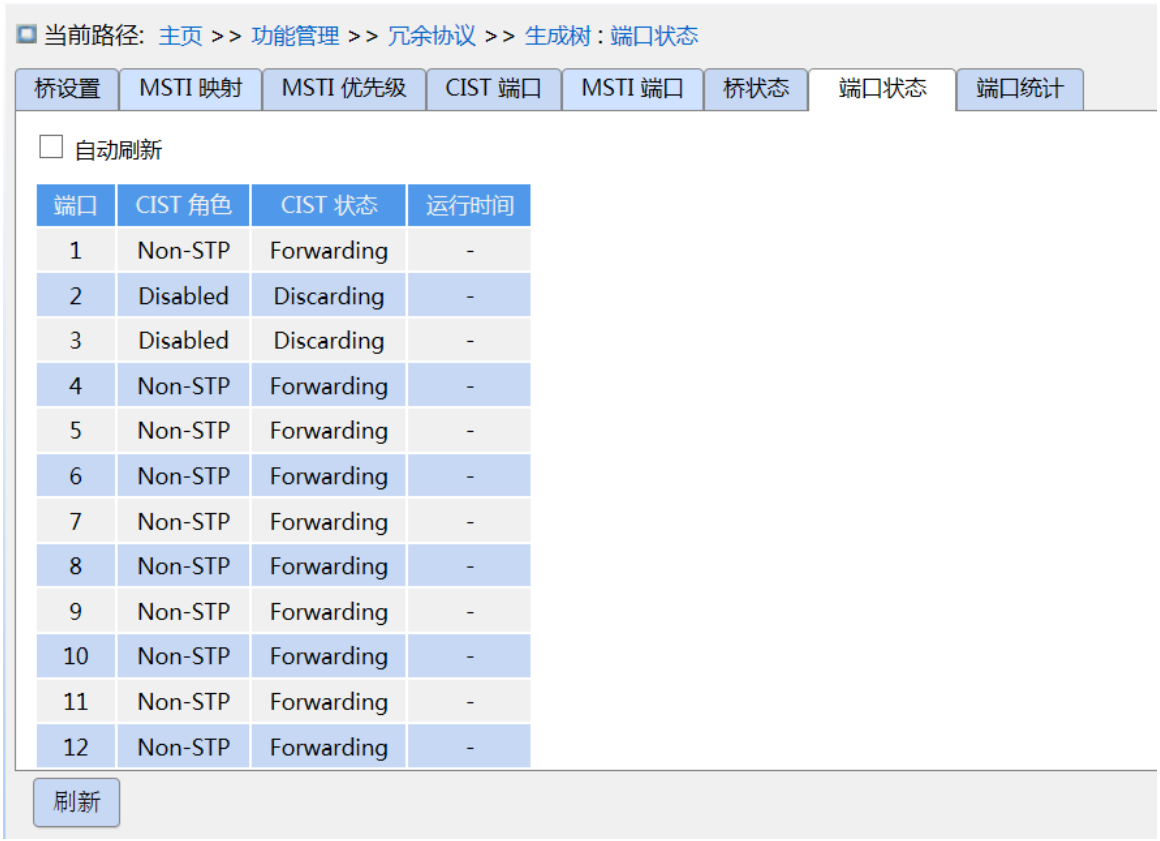
点击<应用>按钮使当前配置生效。

6、查看桥状态，如下图所示；

MSTI	桥 ID	根			拓扑标识	拓扑改变后持续时间
		ID	端口	开销		
CIST	32768.00-22-A2-01-02-12	32768.00-22-A2-01-02-12	-	0	Steady	-
MSTI1	32769.00-22-A2-01-02-12	32769.00-22-A2-01-02-12	-	0	Steady	-
MSTI3	32771.00-22-A2-01-02-12	32771.00-22-A2-01-02-12	-	0	Steady	-
MSTI4	32772.00-22-A2-01-02-12	32772.00-22-A2-01-02-12	-	0	Steady	-

图 173 查看桥状态

7、查看端口状态，如下图所示；



端口	CIST 角色	CIST 状态	运行时间
1	Non-STP	Forwarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-

图 174 查看端口状态

8、查看 STP 端口统计报文，如下图所示；

端口	发送				接收				丢弃	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	未知	非法
4	0	8	0	0	0	0	0	0	0	0
5	0	8	0	0	0	0	0	0	0	0
15	0	8	0	0	0	0	0	0	0	0
16	0	8	0	0	0	0	0	0	0	0

图 175 查看 STP 端口统计报文

7.5.5.5 典型配置举例

图 176 所示网络中交换机 A、B、C、D 属于一个 MST 域，红色标记为该条链路允许通过的 VLAN 报文。通过配置使不同 VLAN 报文沿不同生成树实例转发：VLAN 10 的报文沿实例 1 转发，实例 1 的根桥为 Switch A；VLAN 30 的报文沿实例 3 转发，实例 3 的根桥为 SwitchB；

VLAN 40 的报文沿实例 4 转发，实例 4 的根桥为 Switch C；VLAN 20 的报文沿实例 0 转发，实例 0 的根桥为 Switch B。

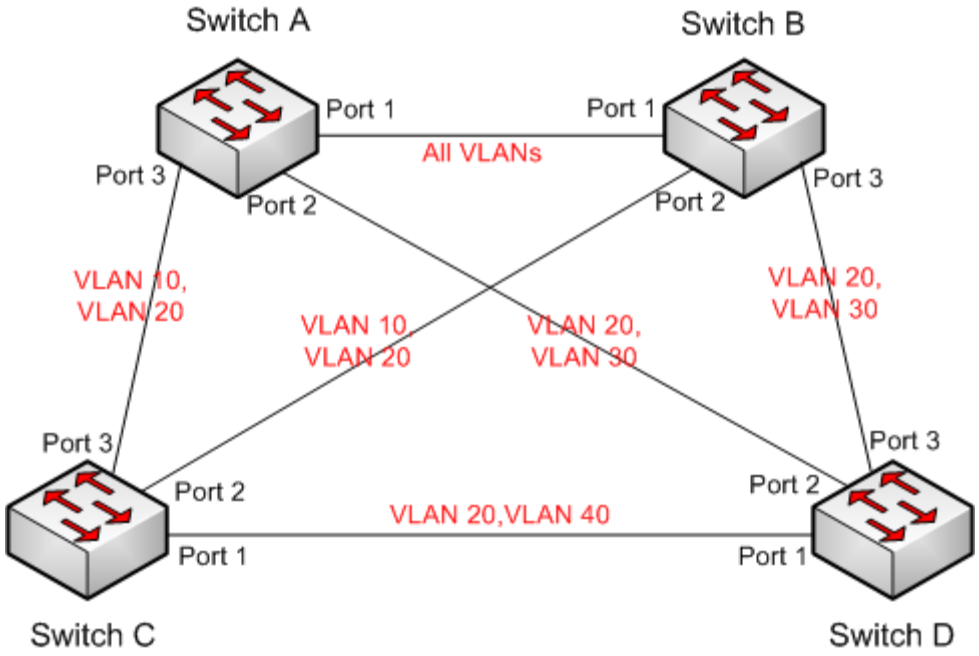


图 176 MSTP 典型配置举例

Switch A 配置过程：

1、在 Switch A 上创建 VLAN 10、20 和 30，配置端口允许相应的 VLAN 通过；

2、全局使能 MSTP 协议，如图 168 所示；

3、配置 MST 域的名称为 Region，修正参数为 0，如图 172 所示；

4、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 172 所示；

5、配置该交换机在实例 1 中的网桥优先级为 4096，其余实例中为默认值，如图 170 所示；

Switch B 配置如下：

6、在 Switch B 上创建 VLAN 10、20、30，配置端口允许相应的 VLAN 通过；

7、全局使能 MSTP 协议，如图 168 所示；

8、配置 MST 域的名称为 Region，修正参数为 0，如图 172 所示；

9、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 172 所示；

10、配置该交换机在实例 3 和实例 0 中的网桥优先级为 4096，其余实例中为默认值，如图 170 所示；

Switch C 配置如下：

11、在 Switch C 上创建 VLAN 10、20、40，配置端口允许相应的 VLAN 通过；

12、全局使能 MSTP 协议，如图 168 所示；

13、配置 MST 域的名称为 Region，修正参数为 0，如图 172 所示；

14、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 172 所示；

15、配置该交换机在实例 4 中的网桥优先级为 4096，其余实例中为默认值，如图 170 所示；

Switch D 配置如下：

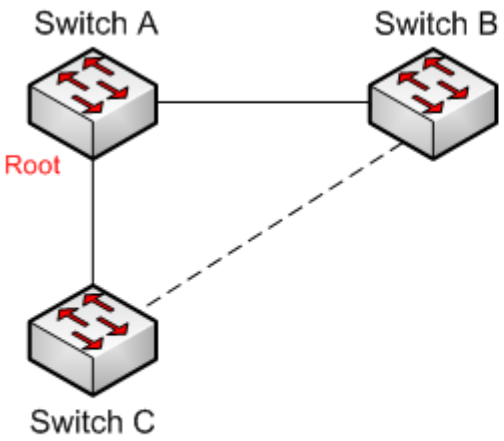
16、在 Switch D 上创建 VLAN 20、30、40，配置端口允许相应的 VLAN 通过；

17、全局使能 MSTP 协议，如图 168 所示；

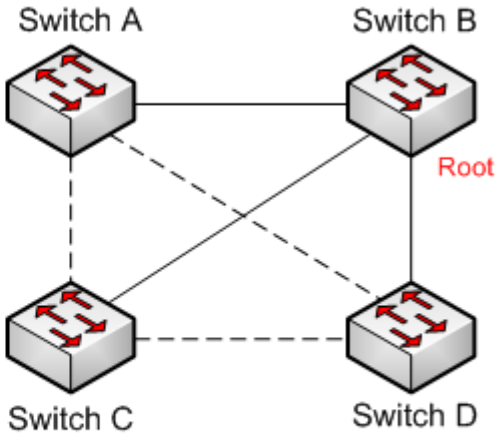
18、配置 MST 域的名称为 Region，修正参数为 0，如图 172 所示；

19、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 172 所示；

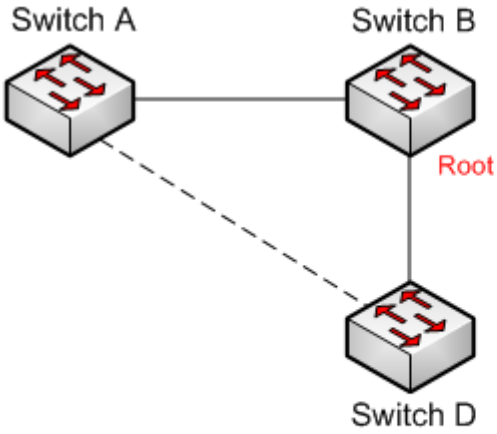
MSTP 计算完成后，各 VLAN 对应的 MSTI 如下图所示；



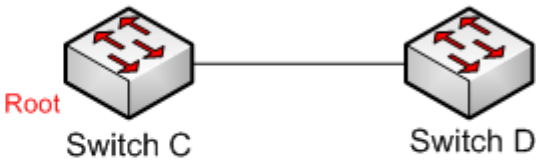
VLAN 10对应的生成树实例1



VLAN 20对应的生成树实例0



VLAN 30对应的生成树实例3



VLAN 40对应的生成树实例4

……表示通过MSTP计算Block掉的链路

图 177 各 VLAN 对应的生成树实例

7.6 ARP 配置

7.6.1 介绍

ARP（Address Resolution Protocol，地址解析协议）通过地址请求和应答机制解析 IP 地址和 MAC 地址之间的映射关系。交换机可以动态学习到本网段其他主机 IP 地址与 MAC 地址的映射关系，也可以配置静态 ARP 表项指定网络中固定的 IP 地址与 MAC 地址映射关系。动态 ARP 表项需要定期进行老化来保证表项与实际应用的一致性。

虽然只提供二层交换功能，该系列交换机也支持 ARP 功能来实现与同网段其他主机的 IP 地址解析，从而实现与网管系统和其他管理主机的互通。

7.6.2 说明

ARP 表项分为动态 ARP 表项和静态 ARP 表项。

动态表项通过 ARP 报文交互自动生成和维护，可以被老化，被新的 ARP 报文更新，被静态 ARP 表项覆盖。

静态表项通过手动配置和维护，不会被老化，不会被动态 ARP 表项覆盖。

7.6.3 代理 ARP

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么和源主机直连的具有代理 ARP 功能的网关就可以回应该请求报文，这个过程称做代理 ARP。

代理 ARP 的过程如下：

1、源主机向另一物理网络的主机发 ARP 请求；

2、与源主机直连的网关已经使能该 VLAN 接口的代理 ARP 功能，如果存在到达目的主机的正常路由，则代替目的主机回复自己接口的 MAC 地址；

3、源主机向目的主机发送的 IP 报文都发给了使能代理 ARP 的设备；

4、网关对报文做正常的 IP 路由转发；

5、发往目的主机的 IP 报文通过网络，最终到达目的主机。

7.6.4 Web 页面配置

1、静态配置 ARP 地址表项，如下图所示：

图 178 静态配置 ARP 表项

VLAN ID

配置内容：已创建的三层 VLAN 接口，范围 1-4093

功能：选择当前 ARP 表项的三层 VLAN 接口。

IP 地址

配置格式：A.B.C.D

功能：配置静态 ARP 表项的 IP 地址。

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH (H 为一个十六进制数)

功能：配置静态 ARP 表项的 MAC 地址。

注意：

一般情况下，交换机自动学习 ARP 表项，不需管理员配置静态表项。

2、代理 ARP 配置，如下图所示：

图 179 代理 ARP 配置

VLAN ID

配置范围：1-4093

功能：选择使能代理 ARP 功能的三层接口。

3、配置 ARP 老化时间，如下图所示：

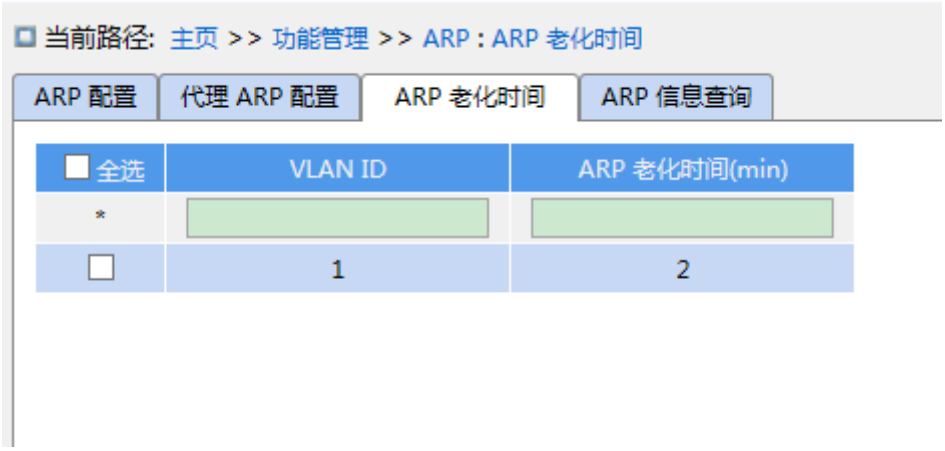


图 180 配置老化时间

VLAN ID

配置范围：1-4093

功能：指定配置 ARP 老化时间的三层接口。

ARP 老化时间

配置范围：1 ~ 60min

默认配置：5min

功能：配置 ARP 老化时间

描述：ARP 老化时间指从一个动态 ARP 表项加入地址表开始计时，老化时间到后该动态地址表项将从 ARP 列表中删除。

4、ARP 信息查询，如下图所示：

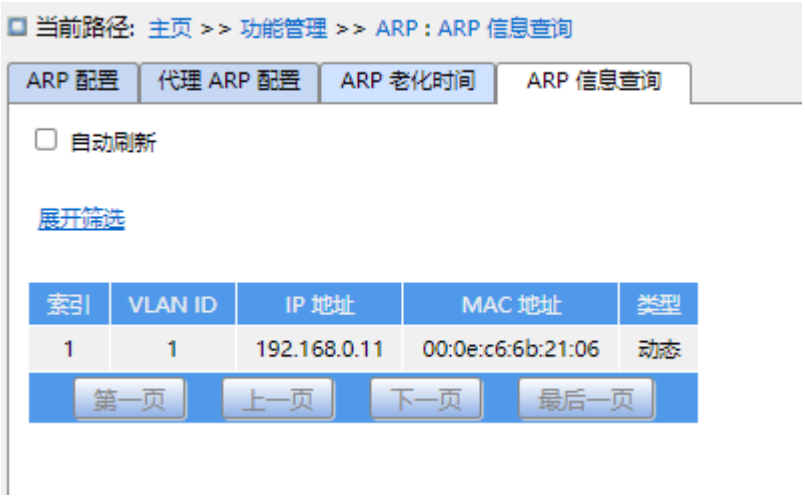


图 181 配置老化时间

ARP 信息查询

组合显示：{序号，VLAN ID，IP 地址，MAC 地址，类型}

功能：显示 ARP 表项

描述：列表中显示 LinkUp 状态端口对应的所有 ARP 表项，包括静态表项和动态表项。

7.7 ACL 配置

7.7.1 介绍

由于随着网络技术的发展，网络功能越来越多样化，网络结构也越来越复杂，网络上的资源越来越丰富。随之而来的网络安全，隐私，用户权限方面的问题也开始突出，这就需要一种可以用于管理对网络资源的访问机制。ACL（Access Control List，访问控制列表）通过匹配交换机入方向的报文中信息与访问表参数实现报文过滤。

7.7.2 实现

通过匹配 ACL 配置表项实现报文过滤，每条 ACL 配置表项由若干 ACL 条件构成，这些条件是“与（&）”的关系，端口接收的报文只有满足所有条件时，才视为匹配该 ACL 表项。各条 ACL 配置表项之间无任何依赖关系。

存在多条 ACL 表项时，设备将报文与 ACL 表项逐条对比，一旦报文遇到匹配的第一条 ACL 表项时，立即执行相应的动作，不再受之后 ACL 表项影响，如图 182 所示。

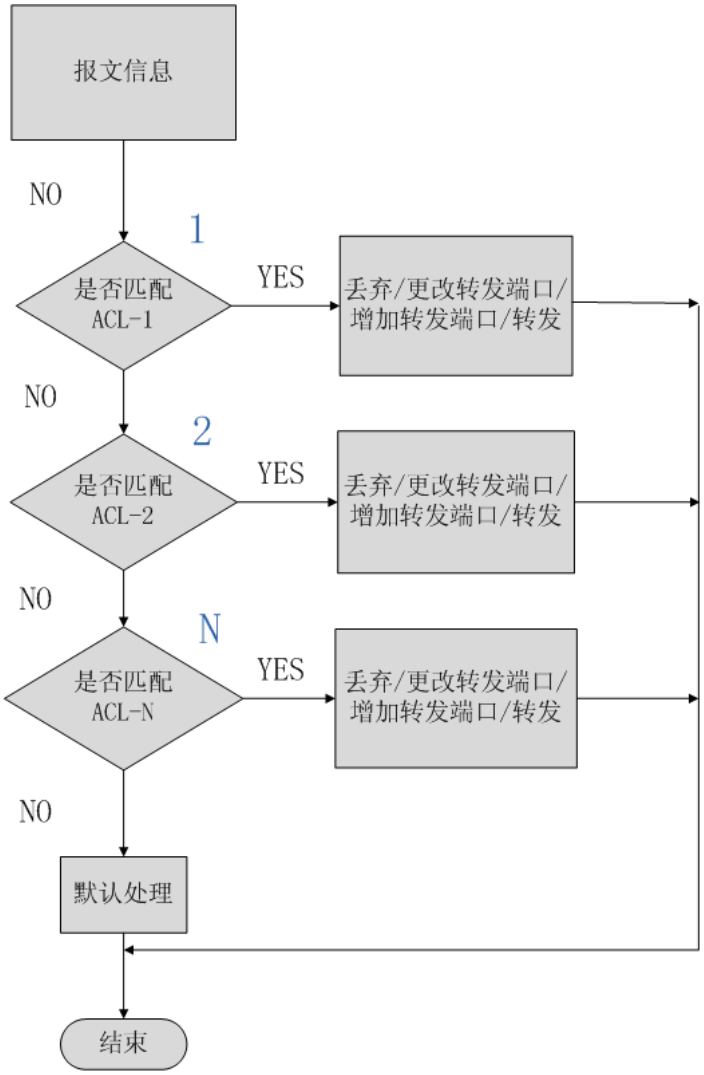


图 182 ACL 匹配流程图

说明：

“默认处理”方式即端口在无配置 ACL 表项的情况下对报文的处理方式。

7.7.3 Web 页面配置

1、配置 ACL 限速，如下图所示；

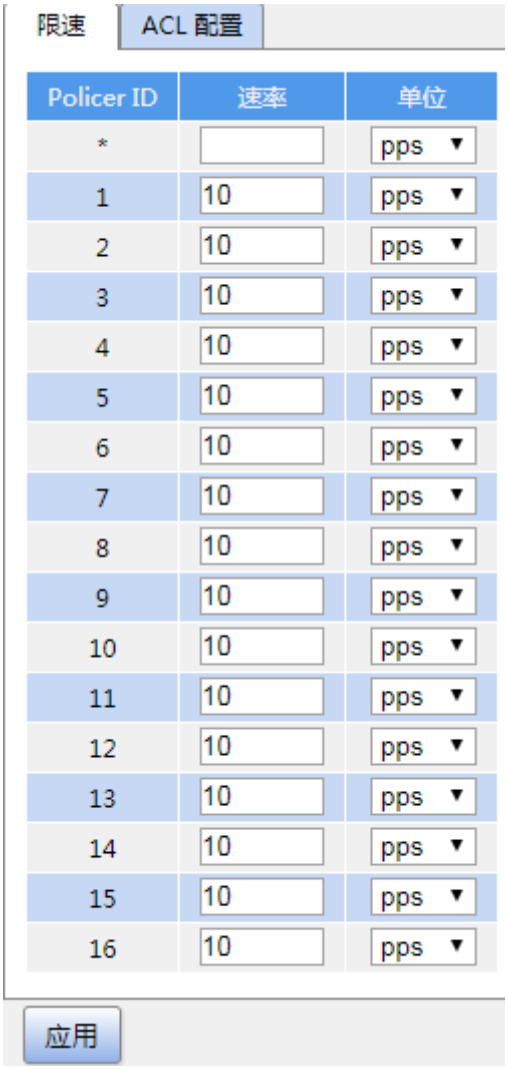


图 183 配置 ACL 限速

速率 单位

配置范围： 0~5000000 pps（步长 10）/ 0~10000000Kbps（步长 25）

默认配置：10 pps

功能：配置对应限速 ID 的限速速率。

2、配置 ACL 表项，如下图所示；

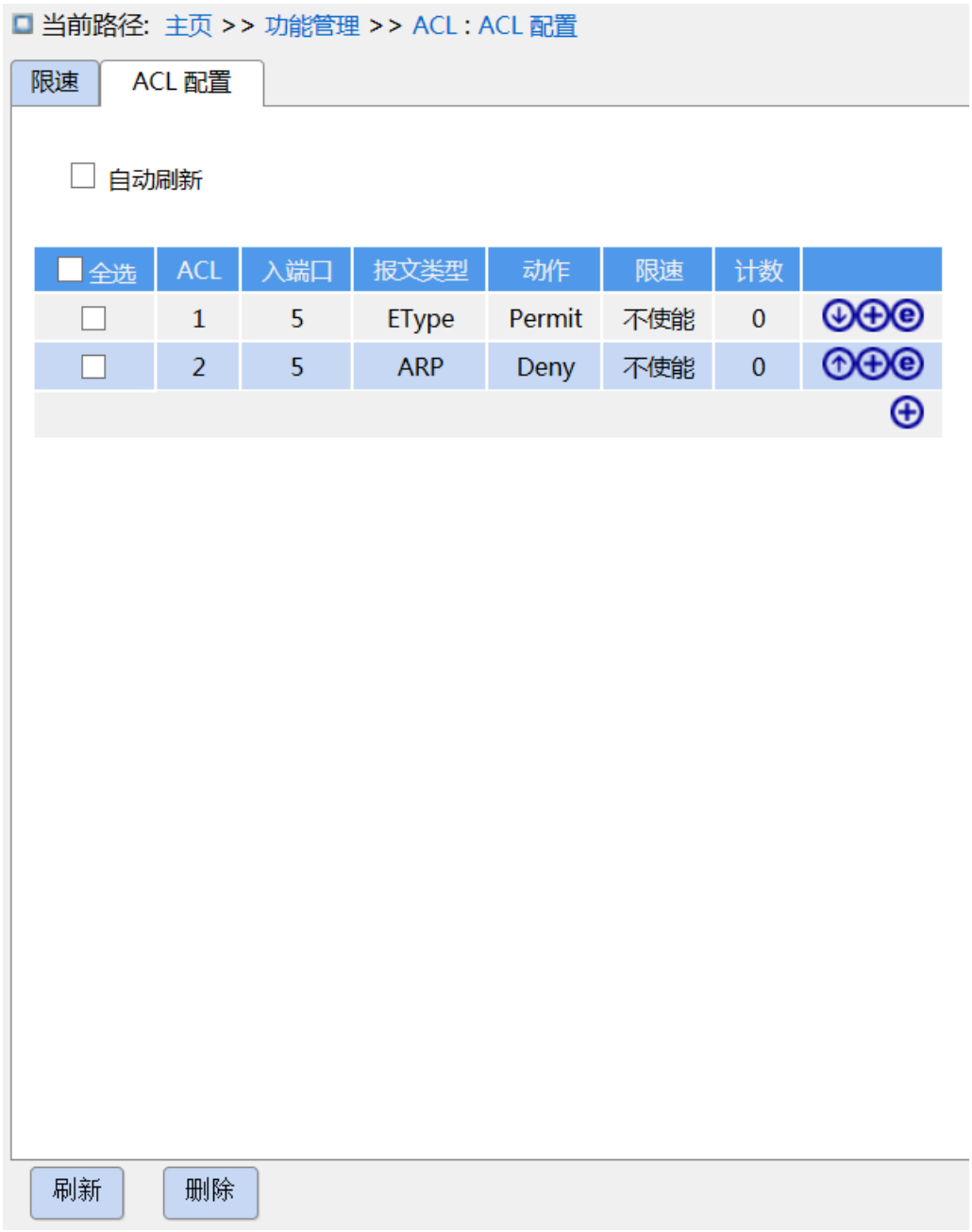


图 184 配置 ACL 表项

存在多条 ACL 表项时，设备将报文与 ACL 表项逐条对比（按照表项从上到下的顺序），一旦报文遇到匹配的第一条 ACL 表项时，立即执行相应的动作。

点击< ⊕ >按钮，新建一条 ACL 表项；点击< ⓔ >按钮，编辑当前表项；点击<⊙>按钮，上移当前表项；点击<⊙>按钮，下移当前表项；勾选<☑>，再点击<删除>按钮，删除当前表项。

3、配置 ACL 表项规则

➢ 配置 ACL 表项参数，如下图所示；

图 185 配置 ACL 表项参数

ACL

配置范围：1-512

功能：配置 ACL 表项 ID。

入端口

配置选项：任意指定端口

功能：选择本条 ACL 的作用端口。

报文类型

配置选项：Any/Ethernet Type/IPv4/ARP

默认配置：Any

功能：配置 ACL 条件参数—报文类型。当入端口接收的报文类型满足该参数配置时，该条件匹配成功。

动作

配置选项：Deny/Permit

默认配置：Permit

功能：端口对匹配 ACL 表项报文的处理方式。Deny：丢弃匹配 ACL 表项的报文。Permit：转发匹配 ACL 表项的报文。

限速

配置范围：不使能/1~16

默认配置：不使能

功能：是否使能端口限速功能，并选择限速 ID。

计数

功能：统计入端口接收的匹配该 ACL 的报文数量。

VLAN ID 过滤

配置选项：Any/ Specific（1~4094）

默认配置：Any

功能：配置条件参数—VID，选择 Specific 时，需要配置 VID 值。当入端口接收的报文中 VID 满足该参数配置时，该条件匹配成功。

➢ 配置 Ethernet Type 报文参数，如下图所示；

图 186 配置 EtherType 报文参数

SMAC 过滤

配置选项：Any/ Specific

默认配置：Any

功能：配置条件参数—源 MAC 地址，选择 Specific 时，需要配置一源 MAC 地址。当入端口接收的报文中源 MAC 地址满足该参数配置时，该条件匹配成功。

DMAC 过滤

配置选项：Any/ Specific

默认配置：Any

功能：配置条件参数--目的 MAC 地址，选择 Specific 时，需要配置一目的 MAC 地址。当入端口接收的报文中目的 MAC 地址满足该参数配置时，该条件匹配成功。

Ether Type 过滤

配置选项：Any/ Specific（0x600~0xFFFF）

默认配置：Any

功能：配置条件参数--以太网类型，选择 Specific 时，需要配置以太网类型值。当入端口接收的以太网报文满足该参数配置时，该条件匹配成功。

➢配置 ARP 报文参数，如下图所示；

图 187 配置 ARP 报文参数

SMAC 过滤

配置选项：Any/ Specific

默认配置：Any

功能：配置条件参数—源 MAC 地址，选择 Specific 时，需要配置一源 MAC 地址。当入端口接收的报文中源 MAC 地址满足该参数配置时，该条件匹配成功。

ARP/RARP

配置选项：Any/ ARP/RARP

默认配置：Any

功能：配置条件参数—报文类型。当入端口接收的报文类型满足该参数配置时，该条件匹配成功。

源 IP 过滤

配置选项：Any/Host/Network

默认配置：Any

功能：配置条件参数-源 IP 地址，选择 Host 时，需要配置一 IP 地址；选择 Network 时，需要配置一 IP 地址和掩码。当入端口接收的报文中源 IP 地址满足该参数配置时，该条件匹配成功。

目的 IP 过滤

配置选项：Any/Host/Network

默认配置：Any

功能：配置条件参数--目的 IP 地址，选择 Host 时，需要配置一 IP 地址；选择 Network 时，需要配置一 IP 地址和掩码。当入端口接收的报文中目的 IP 地址满足该参数配置时，该条件匹配成功。

➢ 配置 IPv4 报文参数，如下图所示；

图 188 配置 IPv4 报文参数

IP 协议过滤

配置选项：Any/ ICMP/ UDP/ TCP/ Other（0~255）

默认配置：Any

功能：配置条件参数--IPv4 报文协议类型，选择 ICMP/ UDP/ TCP 时，需要配置相应参数；选择 Other 时，需要配置协议号。当入端口接收的 IPv4 报文中协议类型满足该参数配置时，该条件匹配成功。

SIP 过滤

配置选项：Any/Host/Network

默认配置：Any

功能：配置条件参数-源 IP 地址，选择 Host 时，需要配置一 IP 地址；选择 Network 时，需要配置一 IP 地址和掩码。当入端口接收的 IPv4 报文中源 IP 地址满足该参数配置时，该条件匹配成功。

DIP 过滤

配置选项：Any/Host/Network

默认配置：Any

功能：配置条件参数--目的 IP 地址，选择 Host 时，需要配置一 IP 地址；选择 Network 时，需要配置一 IP 地址和掩码。当入端口接收的 IPv4 报文中目的 IP 地址满足该参数配置时，该条件匹配成功。

➢ 配置 ICMP 参数，如下图所示；

图 189 配置 ICMP 参数

ICMP 类型过滤

配置选项：Any/Specific（0~255）

默认配置：Any

功能：配置条件参数--ICMP 类型值，选择 Specific 时，需要配置一 ICMP 类型值。当入端口接收的 IPv4 报文中 ICMP 类型值满足该参数配置时，该条件匹配成功。

ICMP 代码过滤

配置选项：Any/Specific（0~255）

默认配置：Any

功能：配置条件参数--ICMP 代码值，选择 Specific 时，需要配置一 ICMP 代码值。当入端口接收的 IPv4 报文中 ICMP 代码值满足该参数配置时，该条件匹配成功。

➢ 配置 UDP 参数，如下图所示；

图 190 配置 UDP 参数

源端口过滤/ 目的端口过滤

配置选项：Any/ Range（0~65535）

默认配置：Any

功能：配置条件参数--UDP 源端口号和目的端口号，选择 Range 时，需要配置端口号范围。当入端口接收的 IPv4 报文中 UDP 端口号满足该参数配置时，该条件匹配成功。

➢ 配置 TCP 参数，如下图所示；

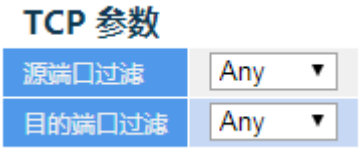


图 191 配置 TCP 参数

源端口过滤/ 目的端口过滤

配置选项：Any/ Range（0~65535）

默认配置：Any

功能：配置条件参数--TCP 源端口号和目的端口号，选择 Range 时，需要配置端口号范

围。当入端口接收的 IPv4 报文中 TCP 端口号满足该参数配置时，该条件匹配成功。

7.7.4 典型配置举例

连接设备的 2 端口，使得该端口只接收源 MAC 地址为 02-02-02-02-02-02 的报文。配置如下：

1、创建 ACL1，配置端口 2 的动作为 Permit，如图 185；

2、配置 ACL1，报文类型为 Ethernet Type，如图 186；

3、配置 ACL1，Ethernet Type 报文参数，SMAC 为 02-02-02-02-02-02，如图 186；

4、创建 ACL，配置端口 2 的动作为 Deny，如图 185；

5、其余参数为默认配置。

7.8 MAC 表

7.8.1 介绍

交换机转发报文时，根据 MAC 地址表查看报文中目的 MAC 地址对应的端口号，并将报文从该端口转发。

MAC 地址分为静态 MAC 地址和动态 MAC 地址。

静态 MAC 地址由用户配置，具有最高优先级（不被动态 MAC 地址覆盖）且永久生效。

动态 MAC 地址由交换机在转发数据帧的过程中学习，且在有限时间内生效，定期的更新 MAC 地址表。当交换机接收到需要转发的数据帧时，首先学习数据帧的源 MAC 地址，与接收端口建立映射关系；然后根据目的 MAC 地址查询 MAC 地址表，如果查到相关表项，交换机将数据帧从相应端口转发；否则，交换机将数据帧在其所属广播域内广播。

老化时间指从一个动态 MAC 地址加入地址表开始计时，如果在 1~2 倍的老化时间内各端口未收到源地址为该 MAC 地址的帧，将从动态转发地址表中删除该表项。静态 MAC 地址表不受老化时间影响。

7.8.2 Web 页面配置

1、配置 MAC 地址老化时间，如图 192 所示；

图 192 MAC 地址老化时间配置

老化时间

配置范围：0 或 10~1000000s

默认配置：300s

功能：配置动态 MAC 地址表项的老化时间。

2、配置静态 MAC 地址表项，如下图所示；

图 193 配置静态 MAC 地址表项

VLAN ID

配置选项：已创建的所有 VLAN ID

功能：配置静态 MAC 表的 VLAN ID。

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH 或 HH:HH:HH:HH:HH:HH（H 为一个十六进制数）

功能：配置 MAC 地址。单播 MAC 地址最高字节的最低位为 0；组播 MAC 地址最高字节的最低位为 1。

端口成员

功能：选择该 MAC 地址的成员端口。

该设备最多支持 64 条静态 MAC 表项。

3、查看 MAC 地址表项，如下图所示；

图 194 查看 MAC 地址表项

VLAN ID

配置选项：*/>=/<=/选择范围

默认配置：*

功能：按照配置的 VLAN ID 显示 MAC 表。

MAC 地址

配置选项：*/>=/<=/选择范围

默认配置：*

功能：按照配置的 MAC 地址显示 MAC 表。

端口

配置选项：*/包含/不包含

默认配置：*

功能：按照配置的端口显示 MAC 表。

类型

配置选项：*/静态/动态

默认配置：*

功能：按照配置的类型显示 MAC 表。

4、配置单播 MAC 过滤表项，如下图所示；

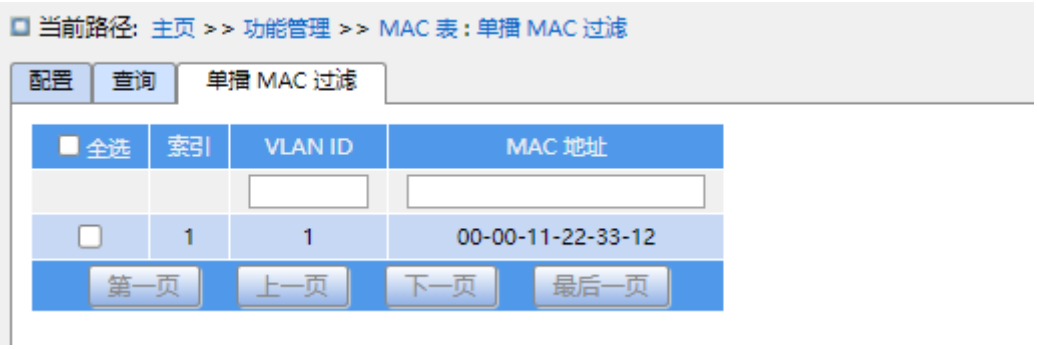


图 195 配置单播 MAC 过滤表项

VLAN ID

配置选项：已创建的所有 VLAN ID

功能：配置静态 MAC 表的 VLAN ID。

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH 或 HH:HH:HH:HH:HH:HH（H 为一个十六进制数）

功能：配置 MAC 地址。单播 MAC 地址最高字节的最低位为 0；组播 MAC 地址最高字节的最低位为 1。

7.9 PoE

7.9.1 介绍

POE（Power Over Ethernet，以太网供电，又称远程供电）是指交换机通过以太网电口，利用双绞线进行远程供电，其可靠供电的距离最长为 100 米，有效地解决 IP 电话、无线 AP、便携设备充电器、刷卡机、摄像头、数据采集等终端的集中式电源供电问题，且无需考虑其室内电源系统布线问题，在接入网络的同时就可以实现对设备的供电。

本系列交换机 POE 供电符合 IEEE 802.3at 统一标准， POE 供电系统包含 PSE 和 PD，PSE（Power Sourcing Equipment，供电设备）是用来给其他设备进行供电的设备，PD（Powered Device，受电设备）是 POE 供电系统中受电的设备，本系列交换机可以作为 PSE 设备。

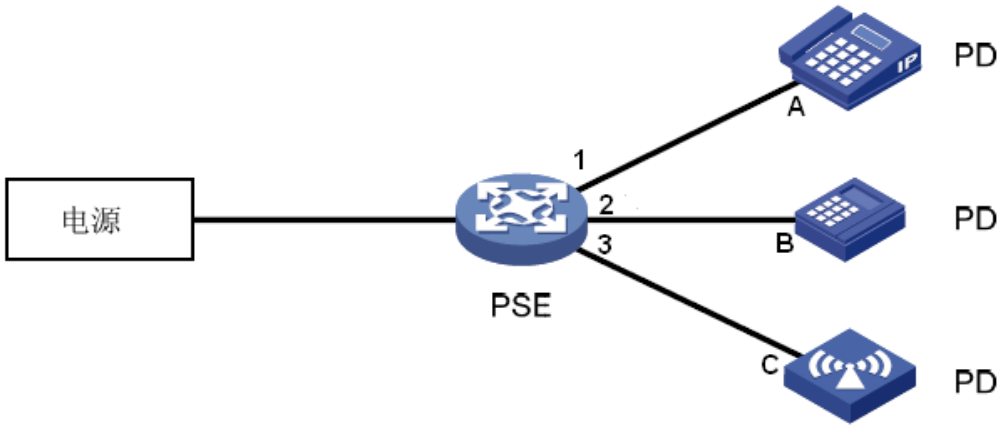


图 196 POE 供电系统

7.9.2 Web 页面配置

1、POE 全局配置，如下图所示；

图 197 POE 全局配置

PoE 端口切断模式

配置选项：自动/手动

默认配置：自动

功能：配置 POE 的供电管理模式。

描述：所有 PD 设备消耗的总功率大于 PSE 能够提供的最大功率时，手动模式下，PSE 按照 PD 设备接入的先后顺序进行供电，即优先对先接入的 PD 设备供电。自动模式下， PSE 按照端口供电优先级对连接的 PD 设备进行供电。

检查负载启动电流

配置选项：检查/跳过

默认配置：检查

功能：检查 PD 设备的启动电流。

负载类型

配置选项：标准/不标准

默认配置：标准

功能：配置可供电的 PD 设备类型。

优先电源供给

配置选项：1-120/1-240

默认配置：120/240

功能：配置该 PSE 整机能够提供的最大功率。设备作为 PSE 时，不接辅助电源，整机最大可提供的最大功率为 120W；增加外置辅助电源，整机最大可提供的最大功率为 240W。如果所有 PD 设备消耗的总功率超过该配置值时，对最后接入的 PD 设备（手动模式）或者优先级最低的 PD 设备（自动模式）进行断电处理。

2、配置端口 PoE 功能，如下图所示；

图 198 端口 PoE 配置

PoE 模式

配置选项：不使能/PoE/PoE+

默认配置：不使能

功能：是否使能端口的 POE 功能。PoE：百兆以太网接口支持符合 IEEE802.3af 的 POE 输出；PoE+：百兆以太网接口支持符合 IEEE802.3at 的 POE 输出。

优先级

配置选项：Low/High/Critical

功能：配置端口供电优先级。Low 为最低优先级，High 为次级优先级，Critical 为最高优先级。

最大功率[W]

配置范围：1~15.4w（PoE）/1~30.0w（PoE+）

功能：配置 POE 端口的最大输出功率。如果端口连接的 PD 设备消耗的功率超过该配置值，则对 PD 设备进行断电处理。用户可根据实际需要，对交换机的各供电端口输出功率限制进行合理配置，有效满足各端口的供电需求。

3、查看供电状态，如下图所示；

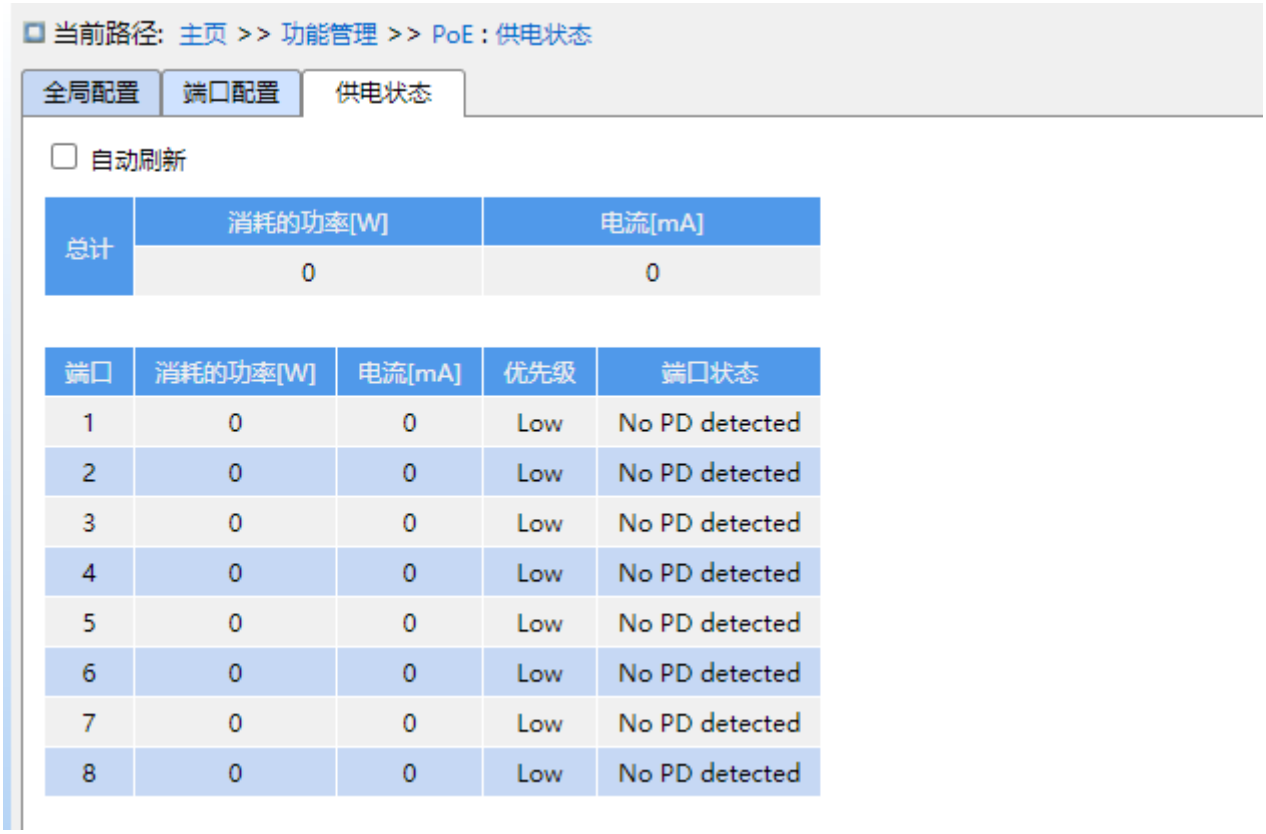


图 199 显示 PoE 供电状态

消耗的功率/电流/优先级

功能：显示使能 POE 功能端口的供电功耗，电流和优先级参数。

端口状态

显示选项：No PD detected/Invalid PD/PoE turned ON/PoE turned OFF-PoE disabled/ PoE turned OFF-Power budget exceeded/PoE turned OFF-PD overload/ PoE turned ON-PD forced ON

功能：显示端口 POE 供电状态。

说明：No PD detected指端口使能POE功能，但未检测到PD设备；

Invalid PD 指端口使能POE功能，检测到PD设备，但供电异常；

PoE turned ON指端口使能POE功能，检测到PD设备，且供电正常；

PoE turned OFF-PoE disabled指端口未使能POE功能；

PoE turned OFF-Power budget exceeded指端口使能POE功能，检测到PD设备，但该PD的接入使得所有PD设备消耗的总功率超过整机提供的最大功耗时，该PD设备断电；

PoE turned OFF-PD overload 指端口使能 POE 功能，检测到 PD 设备，且所有 PD 设备消耗的总功率未超过整机提供的最大功耗，但 PD 设备消耗的功率超过该 POE 端口的最大输出功率，该 PD 设备断电；

PoE turned ON-PD forced ON 指端口使能 POE 功能，强制供电使能。

7.9.3 典型应用举例

如图 196 所示，交换机作为 PSE，所提供的最大功率为 11W，交换机的端口 1 和端口 2 分别于连接设备 A 和设备 B， A 的最大功耗为 5W， B 的最大功耗为 4W，交换机的端口 3 预计会接入设备 C，C 的最大功耗为 5W。

要求：

1、交换机仅连接设备 A 和和设备 B 时，可以正常供电；

2、若在交换机的端口 3 接入 PD 设备 C，此时所有 PD 设备消耗的总功率大于交换机能够提供的最大功率，需保证优先对端口 3 连接设备 C 的供电。

PSE 配置如下：

1、配置切断模式为自动模式，配置优先电源供给为 11W，见图 197；

2、使能交换机端口 1~端口 3 的 POE 功能，配置端口 3 的优先级为 Critical，其它配置为默认配置。

7.10 IGMP Snooping

7.10.1 介绍

IGMP Snooping（Internet Group Management Protocol Snooping ，互联网组管理协议窥探）是运行在数据链路层的组播协议，用于管理和控制组播组。运行 IGMP Snooping 的交换机通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址之间建立起映射关系，并根据此映射关系转发组播报文。

目前 IGMP 共有三个版本，IGMPv1，v2 和 v3。IGMPv1 在 RFC1112 中定义，IGMPv2 在 RFC2236 中定义，IGMPv3 在 RFC3376 中定义。

IGMPv1 版本只有两种报文，report 和 query 报文，定义了基本的组成员查询和报告过程。

IGMPv2 是在 IGMPv1 的基础上增加了组成员快速离开的机制 leave 报文，这种机制的好处是当组播组内的最后一个成员离开组播组时能通知路由器快速收敛。而且和 IGMPv1 相比还有一点不同是 IGMPv2 的查询报文有两种，一种是正常的 query 报文，设备周期性地发送通用组查询消息进行成员关系查询，另外一种是特定组播组查询报文，当主机离开组播组时，设备收到离开消息后，该设备发送特定组播组查询报文，来确定是否组播组内所有的成员都已离开。

IGMPv3 主要是增加了主机源过滤的功能，主机可以指定接收或者指定不接收某些组播组源的报文。

7.10.2 基本概念

查询器：周期性发送 IGMP 通用查询报文来询问已经加入组播组的成员是否还处于活动状态，从而维护组播组信息。网络中存在多个查询器时，会自动选举 IP 地址最小的一台设备作为查询器，只有被选举为查询器的设备会周期性发送 IGMP 查询报文，其他非查询器设备只接收和转发查询报文而不发送查询报文。

路由端口：在开启 IGMP 协议的设备中，接收查询器发送的通用查询报文的端口为路由端口。当一个 IGMP 报告到来时，设备要建立组播表项，将接收 IGMP 报告的端口作为成员端口，另外如果存在路由端口，把路由端口也加入成员端口列表；同时也会将 IGMP 报告报文从路由端口向外转发以便在其他设备上也建立同样的组播表项。

IGMP Snooping 代理：通过在边缘设备上配置 IGMP Snooping Proxying（IGMP Snooping 代理）功能，可以减少其上游设备收到的 IGMP 报告报文和离开报文的数量，有效提高其上

游设备的整体性能。配置了 IGMP Snooping Proxying 功能的设备（称为 IGMP Snooping 代理设备），在其上游设备看来，相当于一台主机；而在其下游主机看来，则相当于一台查询器。

7.10.3 原理

IGMP Snooping 通过 IGMP 设备之间发送相关报文来完成组播组成员的管理和维护。主要有以下几种重要报文：

通用组查询报文：查询器周期性的向外发送通用组查询报文（该报文的目的 IP 固定为 224.0.0.1）来确认组播组中是否还有成员端口存在。非查询器收到通用查询报文后也会向所有连接的端口转发该查询报文。

特定组查询报文：如果有主机想离开一个组播组时会发送 IGMP leave 报文，查询器收到该离开报文后会向外发送 IGMP 特定组查询报文（该报文的目的 IP 为所离开的组播组的 IP 地址），目的是查询该特定组播组内是否还有其他成员端口存在。

成员报告报文：如果主机已经加入组播组，收到 IGMP 查询报文后会发送 IGMP report 报文响应查询报文，目的是报告自己还存在。如果主机想加入某个组播组时，会主动向 IGMP 查询器发送 IGMP report 报文从而加入感兴趣的组播组。IGMP report 报文的目的 IP 为所加入的组播组的 IP 地址。

成员离开报文：主机想离开一个组播组时会发送 IGMP leave 报文（该报文目的 IP 固定为 224.0.0.2）。

7.10.4 Web 页面配置

1、配置 IGMP Snooping 协议，如下图所示；

图 200 配置 IGMP Snooping

Snooping 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能全局 IGMP Snooping 功能。

IGMP SSM 范围

配置格式：A.B.C.D/ 4~32

默认配置：232.0.0.0/8

功能：配置设备对 v1/v2 报文的组地址学习范围，若 v1/v2 报文携带的组地址在该范围中，则设备不学习该地址。

离开代理使能

配置选项：使能/不使能

默认配置：不使能

功能：决定了离开报文是否继续往查询器转发，使能时不转发。

代理使能

配置选项：使能/不使能

默认配置：不使能

功能：决定了离开和成员报告报文是否向查询器转发，使能时不转发。

未知组播丢弃

配置选项：使能/不使能

默认配置：不使能

功能：当交换机收到未知组播报文时是否丢弃。

2、配置 IGMP 端口，如下图所示；

图 201 配置 IGMP 端口

状态

显示选项：--/static/dynamic

功能：显示路由器端口状态。static 指端口被静态配置为路由端口；dynamic 指端口动态学习为路由端口。

路由器端口

配置选项：使能/不使能

默认配置：不使能

功能：配置路由端口。

限流

配置选项：无限制/1~10

默认配置：无限制

功能：是否限制端口学到的组播表项数目。

3、配置 IGMP Snooping VLAN，如下图所示；

图 202 配置 IGMP Snooping VLAN

VLAN 接口

配置选项：已创建的所有 VLAN 接口

Snooping 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能该 VLAN 的 IGMP Snooping 功能。

查询选举

配置选项：使能/不使能

默认配置：使能

功能：是否使能该 VLAN 的 IGMP query 功能。

描述：查询器会从使能自动查询功能的设备中选中 IP 地址最小的一台设备作为查询器，若只有一台设备使能了 IGMP 查询功能，那该设备就是查询器。

查询地址

配置格式：A.B.C.D

功能：配置发送查询报文的源 IP 地址，配置为 0.0.0.0 时，选择该 VLAN 接口的 IP 地址作为查询地址。

兼容性

配置选项：强制 IGMPv1/强制 IGMPv2/强制 IGMPv3

默认配置：强制 IGMPv2

功能：配置 IGMP 协议版本号。

PRI（Priority of Interface）

配置范围：0~7

默认配置：0

功能：配置 IGMP 控制报文的优先级。

RV（Robustness Variable）

配置范围：2~255

默认配置：2

功能：指定该 VLAN 内的 IGMP Query 功能的活力参数。

描述：活力参数越大表示网络环境越糟糕；活力参数越小表示网络环境越好用户可以根据实际网络适当的配置活力参数。

QI（Query Interval）

配置范围：1~31744s

默认配置：125s

功能：配置查询器发送通用查询报文的时间间隔。

QRI（Query Response Interval）

配置范围：0~31744（单位 0.1s）

默认配置：100

功能：配置响应通用查询报文的最大响应时间。

LLQI（Last Member Query Interval）

配置范围：0~31744（单位 0.1s）

默认配置：10

功能：配置响应特定查询报文的最大响应时间。

注意：

QI、QRI、LLQI 参数配置只针对查询器有效。

URI（Unsolicited Report Interval）

配置范围：0~31744s

默认配置：1s

功能：主机发送加入组播组报告报文的时间间隔。

本设备最多支持 32 条 IGMP Snooping VLAN 表项。

4、查看 IGMP Snooping 状态，如下图所示：

图 203 查看 IGMP Snooping 状态

5、查看组播成员列表，如下图所示：

图 204 IGMP Snooping 成员列表

VLAN ID

配置选项：*/>=/<=/选择范围

默认配置：*

功能：按照配置的 VLAN ID 显示组信息。

组

配置选项：*/>=/<=/选择范围

默认配置：*

功能：按照配置的组地址显示组信息。

端口

配置选项：*/包含/不包含

默认配置：*

功能：按照配置的端口显示组信息。

6. 查看 IPv4 SFM 信息，如下图所示。

图 205 IPv4 SFM 信息

7.10.5 典型应用举例

如图 206 所示，Switch1、Switch2、Switch3 设备都使能 IGMP Snooping 功能并且 Switch2、Switch3 使能自动查询。Switch2 的 IP 地址：192.168.1.2；Switch3 的 IP 地址：192.168.0.2。所以 Switch3 被选为查询器。

1、使能 Switch1 的 IGMP Snooping 功能；

2、使能 Switch2 的 IGMP Snooping 和自动查询功能；

3、使能 Switch3 的 IGMP Snooping 和自动查询功能；

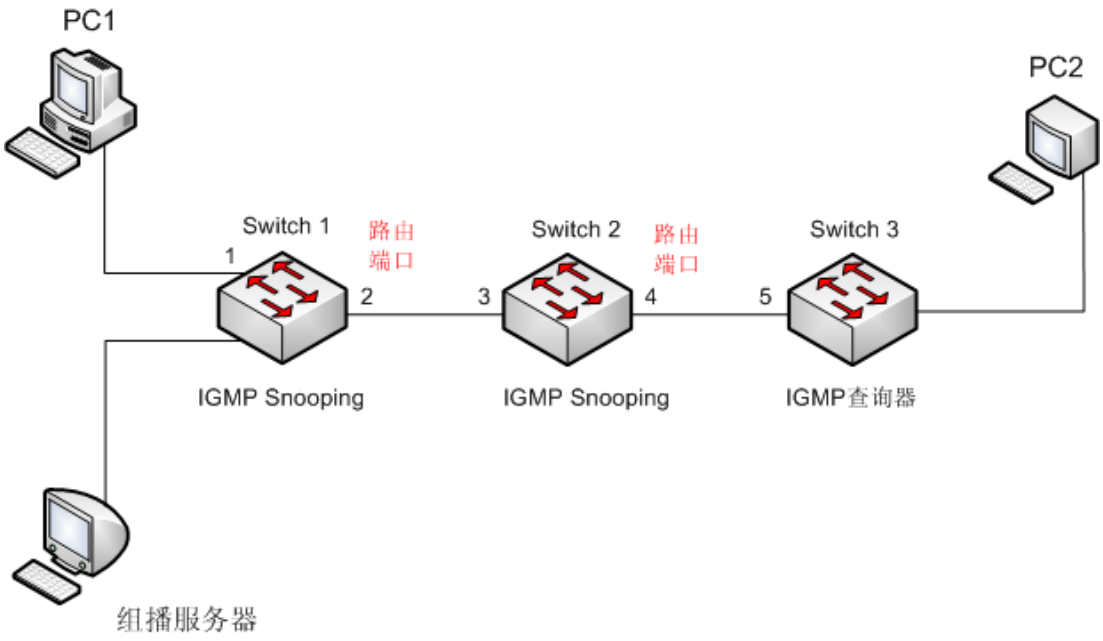


图 206 IGMP Snooping 应用举例

- 由于 Switch3 被选举为查询器，周期性向外发送通用查询报文， Switch2 的 4 端口收到查询报文，所以被选为路由端口，同时 Switch2 也会将查询报文从 3 端口转发出去，Switch1 的 2 端口收到后被选举为路由端口。
- 当 PC1 加入组播组 225.1.1.1 时，向外发送该组的 igmp report 报文，此时，Switch1 的端口 1 和路由端口 2 都会加入组播组 225.1.1.1；同时 igmp report 报文通过路由端口 2 转发到 Switch2 上，Switch2 的端口 3 和 4 也加入 225.1.1.1，同时也会将 igmp report 报文通过路由端口 4 转发到 Switch3，Switch3 的端口 5 也加入 225.1.1.1。
- 当组播服务器的组播数据到 Switch1 上时，会通过端口 1 向外转发给 pc1，同时由于路由端口 2 也是组播组成员，所以组播数据也会通过路由端口向外转发，依次类推，到达 Switch3 的端口 5 上由于没有了接收者而停止转发，但是如果 pc2 也加入了 225.1.1.1，那么组播数据也会转发到 pc2 上。

7.11 DHCP 配置

随着网络规模的不断扩大，网络配置也越来越复杂，在计算机经常移动（如便携机或无线网络）和计算机的数量超过可分配 IP 地址等情况下，原有针对静态主机配置的 BootP（Bootstrap Protocol，自举协议）已经越来越不能满足实际需求。为方便用户快速地接入和退出网络、提高 IP 地址资源的利用率，需要在 BootP 基础上制定一种自动机制来进行 IP 地址的分配。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）就是为解决这些问题而发展起来的。

DHCP 采用客户端/服务器的通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等配置信息，以实现IP地址的动态配置。DHCP的典型应用结构如图 207 所示；

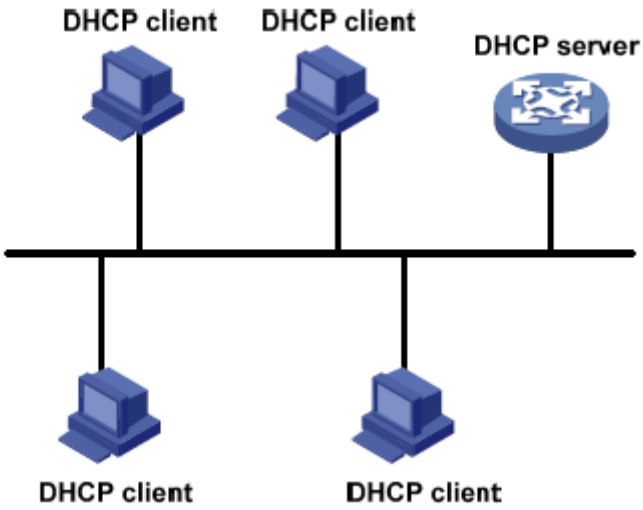


图 207 DHCP 典型应用结构

注意：

由于在 IP 地址动态获取过程中采用广播方式发送报文，因此要求 DHCP 客户端和 DHCP 服务器处于同一网段，如果位于不同网段时，客户端可以通过 DHCP 中继与服务器通信，获取 IP 地址及其他配置信息。

DHCP 提供两种 IP 地址分配策略：

静态分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定 IP 地址，通过 DHCP 将绑定的 IP 地址发给客户端，该策略分配的 IP 地址租期为无限长。

动态分配地址：DHCP 服务器为客户端动态分配 IP 地址，该分配策略包括分配租期无限长的 IP 地址和租期为有效期限的 IP 地址，如果为有效期则到达使用期限后，客户端需要重新申请 IP 地址。

管理员可以选择 DHCP 采用哪种策略响应每个客户机。

7.11.1 DHCP 服务器配置

7.11.1.1 介绍

DHCP 服务器是 DHCP 服务的提供者，通过 DHCP 报文与 DHCP 客户端交互，为客户端分配合适的 IP 地址，并可以根据需要为客户端分配其他网络参数。通常在以下情况下利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大工作量，难以管理整个网络；
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配固定 IP 地址；

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

7.11.1.2 地址池

DHCP 服务器从地址池中为客户端选择并分配 IP 地址及其他相关参数。分配 IP 地址的优先次序如下：

1、与客户端 MAC 地址静态绑定的 IP 地址；

2、DHCP 服务器记录的曾经给客户端分配的 IP 地址；

3、客户端发送的请求报文中指定的 IP 地址；

4、从地址池中顺序查找可供分配的 IP 地址，最先找到的 IP 地址；

5、如果没有找到可用的 IP 地址，则依次查询租约过期、曾经发生过冲突的 IP 地址，如果找到则进行分配，否则不予处理。

7.11.1.3 Web 页面配置

1、使能 DHCP 服务器，如下图所示；

图 208 使能 DHCP 服务器

全局模式

配置选项：去使能/使能

默认配置：去使能

功能：是否选择当前交换机做为 DHCP 服务器为客户端分配 IP 地址。

{VLAN 范围， 模式}

配置范围：{1~4093，使能/去使能}

功能：如果 IP 地址申请的客户端的 VLAN 属性为使能模式时，DHCP 服务器给该客户端

分配 IP 地址；否则，DHCP 服务器不给客户端分配 IP 地址。

2、创建 DHCP 地址池，如下图所示；

图 209 创建地址池

名称

配置范围：1~32 个字符

功能：配置 DHCP 地址池名称。

3、配置地址池，点击图 209 中的<名称>进入地址池配置界面，如图 210 所示；

图 210 配置 IP 地址池

类型

配置选项：None/Network/Host

默认配置：None

功能：配置地址池的类型。Network 用于动态分配 IP 地址，可以服务多个 DHCP 客户端；Host 用于静态分配 IP 地址，为特殊的 DHCP 客户端服务。

{IP，子网掩码}

功能：Type 为 Network 时，配置该地址池可分配的地址范围，地址范围的大小通过掩码来设定。掩码是长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。一般配置成 255.255.255.0。

Type 为 Host 时，配置静态绑定的 IP 地址。静态分配 IP 地址通过将客户端的 MAC 地址与 IP 地址绑定的方式实现，当具有此 MAC 地址的客户端申请 IP 地址时，DHCP 服务器将根据客户端的 MAC 地址查找对应的 IP 地址，并分配给客户端，这种分配方式优先级高于动态分配 IP 地址，租期为永久。

租约时长

配置范围：0 日 0 时 0 分~365 日 23 时 59 分

默认配置：1 日 0 时 0 分

描述：配置动态分配 IP 地址的租用有效期限。对于不同的地址池，DHCP 服务器可以指定不同的地址租用期限，但同一 DHCP 地址池中的地址具有相同的期限。

域名称

配置范围：1~32 个字符

功能：配置 DHCP 地址池的域名后缀，给客户端分配 IP 地址的同时，将域名后缀发送给客户端。

广播地址

配置格式：A.B.C.D

功能：配置 DHCP 服务器为 DHCP 客户端分配的广播地址。

默认路由

配置格式：A.B.C.D

功能：配置 DHCP 服务器为 DHCP 客户端分配的网关地址。

描述：DHCP 客户端访问本网段以外的主机时，数据必须通过网关进行转发，DHCP 服务

器为客户端分配 IP 地址的同时可以指定网关地址。DHCP 地址池最多可以配置 4 个网关地址。

DNS 服务器

配置格式：A.B.C.D

功能：配置 DHCP 服务器为 DHCP 客户端分配的 DNS 服务器地址。

描述：通过域名访问网络上的主机时，需要将域名解析为 IP 地址，这是通过 DNS（Domain Name System，域名系统）实现的。为了使 DHCP 客户端能够通过域名访问网络上的主机，DHCP 服务器为客户端分配 IP 地址的同时可以指定 DNS 服务器地址。DHCP 地址池最多可以配置 4 个 DNS 服务器地址。

NTP 服务器

配置格式：A.B.C.D

功能：配置 DHCP 服务器为 DHCP 客户端分配的 NTP 服务器地址。

NetBIOS 结点类型

配置选项：None/B-node/P-node/M-node/H-node

默认配置：None

功能：配置 DHCP 服务器为客户端分配的 NetBIOS 节点类型。DHCP 客户端在网络上使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。每个节点类型获取映射关系的方式不同。

描述：B-node，此类节点采用广播方式获取映射关系；P-node，此类节点采用发送单播报文与 WINS 服务器通信的方式获取映射关系；M-node，此类节点首先发送广播报文来获取映射关系，如果没有获取到，则再发送单播报文与 WINS 服务器通信来获取映射关系；H-node，此类节点首先发送单播报文与 WINS 服务器通信来获取映射关系，如果没有获取到，再发送广播报文来获取映射关系。

NetBIOS 范围

配置范围：1~32 个字符

功能：配置 NetBIOS 的名称。

NetBIOS 命名服务器

配置格式：A.B.C.D

功能：配置 DHCP 服务器为 DHCP 客户端分配的 WINS 服务器地址。

描述：对于使用 Microsoft Windows 操作系统的客户端，由 WINS（Windows Internet

Naming Service，Windows Internet 名称服务）服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 客户端需要进行 WINS 配置。为了使 DHCP 客户端实现主机名到IP地址的解析，DHCP服务器为客户端分配IP地址的同时可以指定WINS服务器地址。DHCP 地址池最多可以配置 4 个 WINS 服务器地址。

NIS 域名

配置范围：1~32 个字符

功能：配置客户端的 NIS 域名。

NIS 服务器

配置格式：A.B.C.D

功能：配置 DHCP 服务器为 DHCP 客户端分配的 NIS 服务器地址。

客户端标识

配置选项：None/FQDN/MAC

默认配置：None

功能：当地址池的类型为 host 时，配置静态绑定的客户端标识。

硬件地址

配置格式：HH-HH-HH-HH-HH-HH（H 为一个十六进制数）

功能：当地址池的类型为 host 时，配置静态绑定的客户端 MAC 地址。

客户端名称

配置范围：1~32 个字符

功能：当地址池的类型为 host 时，配置客户端用户名。

Vendor i 类标识

配置范围：1~64 个字符

功能：配置 DHCP 服务器为 DHCP 客户端分配的用来标记供应商类型的值。

Vendor i 详细信息

配置范围：1~64 个 16 进制数

功能：配置 DHCP 服务器为 DHCP 客户端分配的用来标记 vendor Class Identifier 的特殊信息。

4、配置外挂 IP 地址，即 DHCP 地址池中不参与动态分配的 IP 地址，如下图所示；

图 211 配置外挂 IP 地址

IP 范围

功能：配置 DHCP 地址池中不参与动态分配的 IP 地址范围。DHCP 服务器分配地址时，需要排除已经被占用的 IP 地址（如网关、DNS 服务器等），否则，同一地址分配给两个客户端会造成 IP 冲突。

5、查看 DHCP 服务器统计信息，如下图所示；

图 212 查看 DHCP 服务器统计信息

6、查看 DHCP 服务器分配 IP 地址情况，如下图所示；

图 213 查看 DHCP 服务器分配 IP 地址信息

7、查看 DHCP 客户端拒绝接收的 IP 地址，如下图所示；

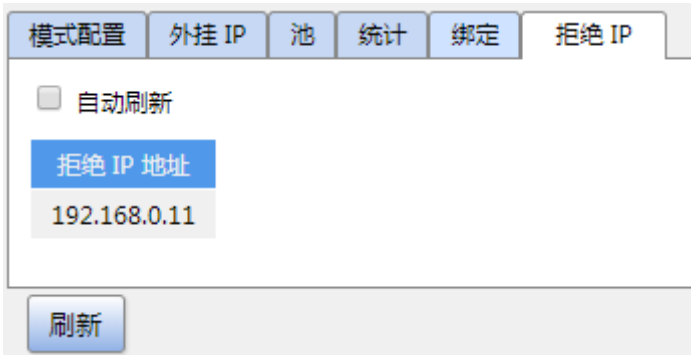


图 214 查看 DHCP 客户端拒绝接收的 IP 地址

客户端检测到服务器分配的 IP 地址和该网段内某个静态 IP 地址有冲突时，会向服务器发送 decline 报文拒绝接收该 IP 地址。服务器端记录客户端拒绝接收的 IP 地址，并在一定时间内不会将该 IP 地址分配给其他的客户端。

7.11.1.4 典型配置举例

如图 215 所示，交换机 A 作为 DHCP 服务器，交换机 B 作为 DHCP 客户端，交换机 A 的 3 端口连接交换机 B 的 4 端口。客户端发出申请 IP 地址请求报文，服务器可以通过两种方式为客户端分配 IP 地址。DHCP 服务器动态分配 IP 地址时，192.168.0.1~192.168.0.10 范围的 IP 地址不参与动态分配。

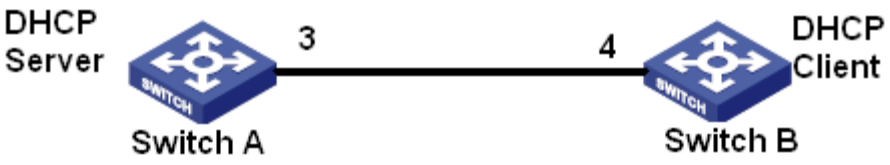


图 215 DHCP 典型配置举例

静态分配 IP 地址方式

➢ 交换机 A 的配置：

1、在相应 VLAN 打开 DHCP 服务器状态，见图 208；

2、创建地址池 pool-1，见图 209；

3、选择地址池类型为 Host；IP 地址：192.168.0.6；掩码：255.255.255.0；绑定交换机 B 的 MAC 地址：00-11-22-33-44-55，见图 210；

➢ 交换机 B 的配置：

1、交换机 B 通过 DHCP 获取 IP；

2、交换机 B 从 DHCP 服务器上获取 IP 地址：192.168.0.6，子网掩码：255.255.255.0，如图 216 所示；

图 216 DHCP 客户端获取 IP 地址-1

动态分配 IP 地址方式

➢ 交换机 A 的配置：

1、在相应 VLAN 打开 DHCP 服务器状态，见图 208；

2、创建地址池 pool-2，见图 209；

3、选择地址池类型为 Network；IP 地址：192.168.0.6；掩码：255.255.255.0；其余为默认配置；

➢ 交换机 B 的配置：

1、交换机 B 通过 DHCP 获取 IP；

2、DHCP 服务器从地址池中顺序查找可供分配的 IP 地址，把最先找到的 IP 地址：192.168.0.11，子网掩码：255.255.255.0 分配给交换机 B，如图 217 所示；

图 217 DHCP 客户端获取 IP 地址-2

7.11.2 DHCP Snooping

7.11.2.1 介绍

DHCP Snooping 即 DHCP 服务的二层监听功能，是 DHCP 的一种安全特性，可以为客户端提供安全保证。DHCP Snooping 安全机制控制 DHCP 客户端发送的请求报文只从信任端口转发至合法服务器，同时也控制 DHCP 服务器应答报文的来源，保证客户端从合法服务器获取 IP 地址，防止网络中可能存在的伪造或非法 DHCP 服务器为其他主机分配 IP 地址等配置信息。

DHCP Snooping 安全机制将端口分为信任端口和非信任端口：

信任端口是与合法 DHCP 服务器直接或间接连接的端口，信任端口正常转发 DHCP 客户端的请求报文和 DHCP 服务器的应答报文，从而保证 DHCP 客户端获取正确的 IP 地址；

非信任端口是与非法 DHCP 服务器连接的端口，非信任端口不转发 DHCP 客户端的请求报文和 DHCP 服务器的响应报文，从而防止 DHCP 客户端获得错误的 IP 地址。

7.11.2.2 Web 页面配置

1、使能 DHCP Snooping 功能，如下图所示；

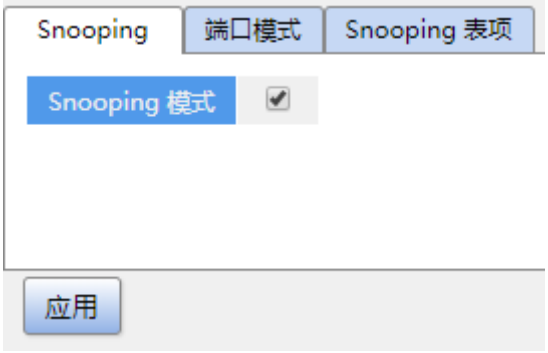


图 218 DHCP Snooping 状态

DHCP Snooping 模式

配置选项：使能/去使能

默认配置：去使能

功能：是否使能交换机的 DHCP Snooping 功能。

2、配置信任端口，如下图所示；

图 219 配置信任端口

端口模式

配置选项：Trusted/Untrusted

默认配置：Trusted

功能：配置端口为信任端口或者非信任端口，与合法 DHCP 服务器直接或间接连接的端口配置为信任端口。

3、查看 snooping 表项，如下图所示；

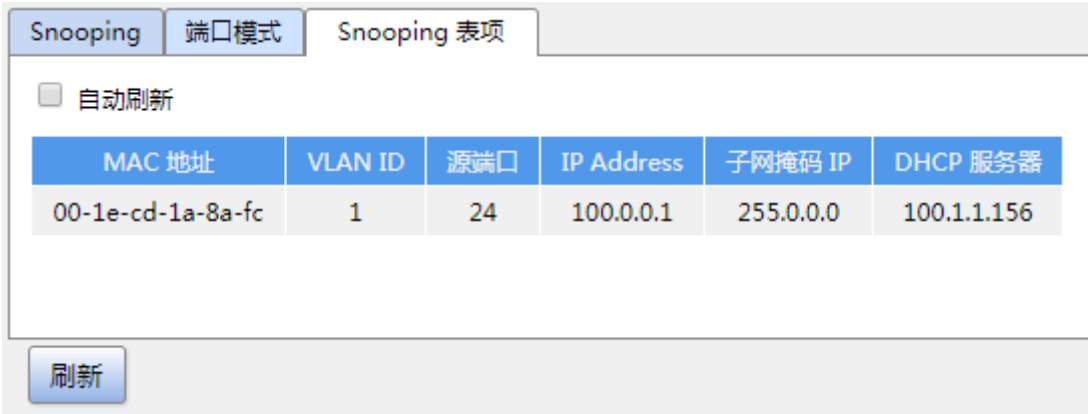


图 220 查看 DHCP Snooping 表项

7.11.2.3 典型配置举例

如图 221 所示，DHCP Client 请求从 DHCP Server 自动获得 IP 地址，网络中存在不合法的 DHCP Server。通过配置 DHCP Snooping 端口 1 为信任端口，把 DHCP Client 的请求报文转发给 DHCP Server，并把 DHCP Server 的应答报文转发给 DHCP Client；配置端口 3 为非信任端口，不转发 DHCP Client 的请求报文和非法 DHCP Server 的应答报文，可以保证客户端从合法 DHCP 服务器上获得合法的 IP 地址。

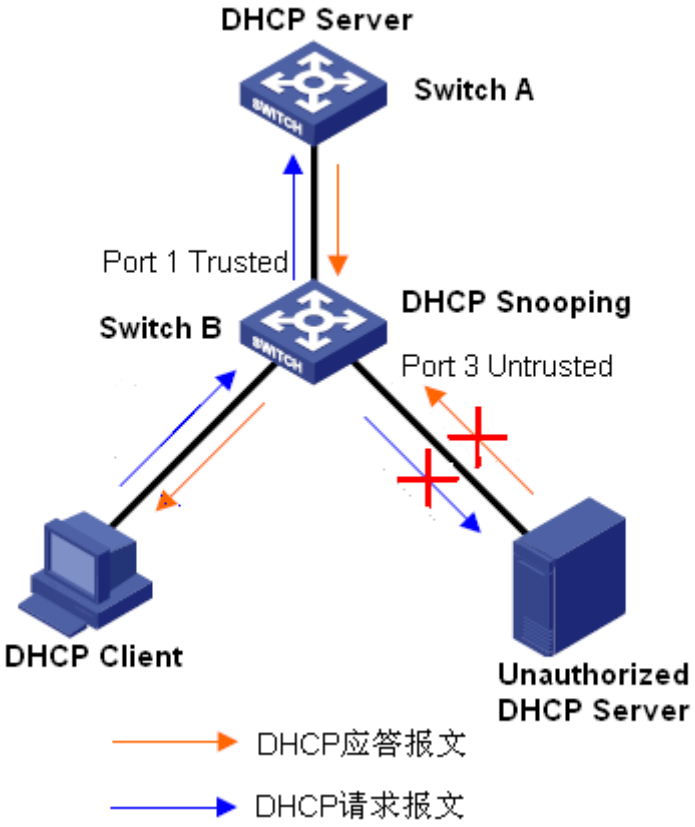


图 221 DHCP Snooping 典型配置举例

交换机 B 配置过程：

- 使能 DHCP Snooping 功能，见图 218；
- 配置交换机 B 的端口 1 为信任端口，端口 3 为非信任端口，见图 219。

7.11.3 中继

7.11.3.1 介绍

1、DHCP 中继

DHCP 中继，就是在DHCP 服务器和客户端之间转发DHCP 数据包。当DHCP 客户端

与服务器不在同一个子网上，就必须有DHCP 中继来转发DHCP 请求和应答消息。DHCP 中继的数据转发，与通常路由转发是不同的，通常的路由转发相对来说是透明传输的，设备一般不会修改IP 包内容。而DHCP 中继接收到DHCP消息后，重新生成一个DHCP 消息，然后转发出去。在 DHCP 客户端看来，DHCP 中继代理就像DHCP 服务器；在DHCP 服务器看来，DHCP 中继代理就像DHCP 客户端。

DHCP中继将收到的DHCP请求报文以单播方式转发给DHCP 服务器，同时将收到的DHCP响应报文转发给DHCP客户端。DHCP中继相当于一个转发站，负责沟通位于不同网段的DHCP客户端和DHCP服务器。实现了只要安装一个DHCP 服务器，就可以对多个网段的动态IP 管理，即Client—Relay—Server 模式的DHCP 动态IP 管理。如下图所示：

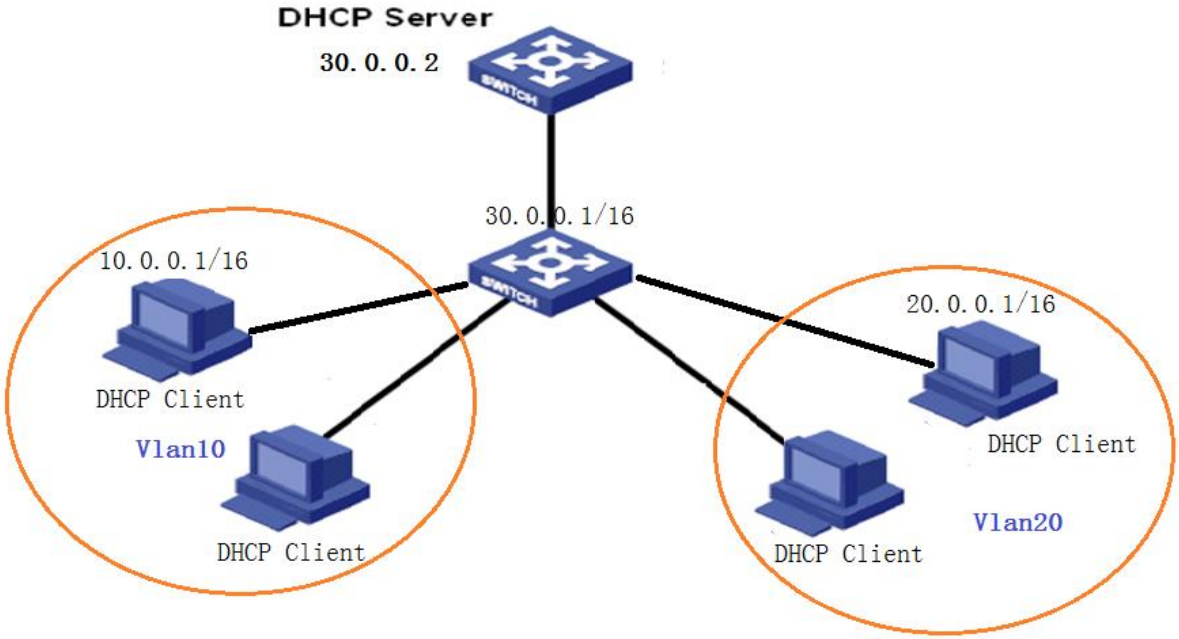


图 222 Client—Relay—Server 模式

2、DHCP Relay Agent Information(option 82)

中继设备进行DHCP relay时，可以通过添加option 的方式来详细的标明DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的IP。根据RFC3046的定义，所使用option 选项的选项号为82，故也被称作option 82。

Options 82（中继代理信息表项）记录了客户端信息，支持 Options 82 功能的 DHCP 中继接收到 DHCP 客户端发送的请求报文后，在报文中添加相应的 Options 82 字段并转发给 DHCP 服务器。支持 Options 82 功能的服务器根据该报文信息能够提供更加灵活的地址分配方案。

如果使能 Options 82 功能，报文中将会添加 Option82 字段，该系列交换机 Option82 字

段包含两个子选项：sub-option1（Circuit ID，电路 ID 子选项）和 sub-option2（Remote ID，远程 ID 子选项）。两个子选项对应的格式如下：

- Sub-option1 内容包含接收 DHCP 客户端请求报文的端口所属的 VLAN ID 以及端口号，如下表所示；

表 8 sub-option1 字段格式

Sub-option type（0x01）	Length（0x04）	VLAN ID	Port number
1 个字节	1 个字节	2 个字节	2 个字节

Sub-option type：Sub-option1 子选项类型为 1；

Length：指 VLAN ID 和 Port number 占用的字节数；

VLAN ID：DHCP Relay 设备接收到客户端请求报文的端口的 VLAN ID；

Port number：DHCP Relay 设备接收到客户端请求报文的端口号。

- Sub-option2 内容是接收 DHCP 客户端请求报文的 DHCP Realy 设备的 MAC 地址如下表所示；

表 9 sub-option2 字段格式-MAC 地址

Sub-option type（0x02）	Length（0x06）	MAC 地址
1 个字节	1 个字节	6 个字节

Sub-option type：Sub-option2 子选项类型为 2；

Length：指 Sub-option2 内容占用的字节数，MAC 地址占用 6 个字节；

MAC 地址：Sub-option2 内容是接收到客户端请求报文的 DHCP Realy 设备的 MAC 地址。

如果 DHCP Relay 支持 Option82 功能，则当 DHCP Relay 接收到 DHCP 请求报文后，将根据报文中是否包含 Option82 及客户端策略对请求报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器。具体的处理方式如下表所示；

表 10 DHCP Relay 对请求报文的处理方式

收到 DHCP 客户端请求报文	**客户端策略**	**DHCP Relay 对请求报文的处理**
请求报文中带有 Option 82	丢弃	丢弃该请求报文
	保留	保持该报文格式不变并进行转发

	替换	将该报文中的 Option 82 字段替换为当前 Relay 设备的 Option82 字段并进行转发
请求报文中不带有 Option 82	丢弃/保留/替换	添加当前 Relay 设备的 Option82 字段并进行转发

当 DHCP Relay 接收到 DHCP 服务器的响应报文时，不处理直接转发给客户端。

7.11.3.2 Web 页面配置

1、DHCP 中继全局配置，如下图所示；

图 223 DHCP 中继全局配置

模式

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 DHCP 中继功能。

服务器地址

功能：配置 DHCP 服务器地址。

Option82 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 DHCP 中继的 Option82 功能。

Client 策略

配置选项：替换/保留/丢弃

默认配置：保留

功能：配置客户端策略，DHCP 中继根据客户端策略对 Client 发送的请求报文进行处理，具体处理方式见表 10。

2、查看 DHCP 安全表项，如下图所示；

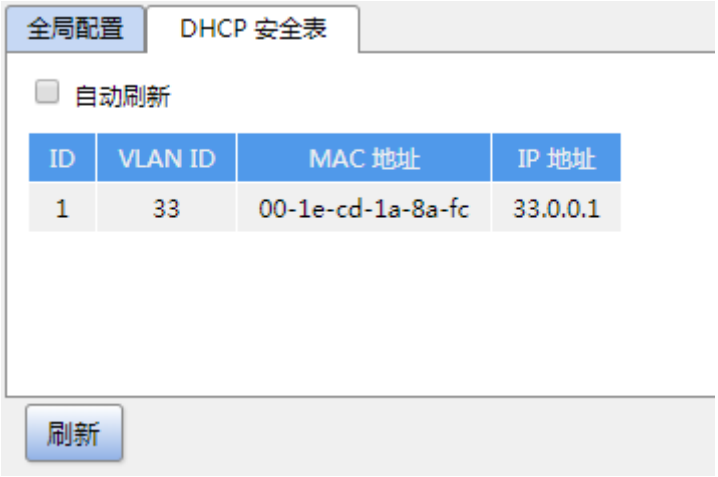


图 224 查看 DHCP 安全表

7.12 IEEE802.1X 配置

7.12.1 介绍

IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。802.1X 协议作为局域网端口的一个普通接入控制机制应用于以太网中，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（Port Based Network Access Control）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。

802.1X 系统使用典型的 Client/Server 体系结构，如下图所示。只有具备了以下三个元素才能够完成基于端口的访问控制的用户认证和授权。

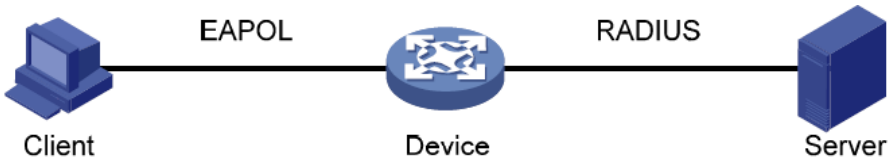


图 225 IEEE802.1X 认证系统的体系结构

客户端：一般为用户终端设备，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。客户端应支持 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）。

设备端：在以太网系统中指认证交换机，主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。

认证服务器：为设备端提供认证服务的实体，通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向设备端发出打开或保持端口关闭的状态。

7.12.2 Web 页面配置

1、IEEE802.1X 任务管理，如下图所示；

图 226 IEEE802.1X 任务管理

操作类型

配置选项：重启认证进程/初始化

功能：端口选择基于 MAC 认证、基于端口的 802.1X 的认证模式时，可以选择<重启认证进程>/<初始化>来重新认证。重认证过程中，端口状态切换为未认证状态。

端口

功能：选择需要重启认证进程/初始化的端口

2、IEEE802.1X 基本配置，如下图所示；

图 227 IEEE802.1X 基本配置

系统认证控制

配置选项：使能/不使能

默认配置：不使能

功能：是否使能全局 IEEE802.1X 安全功能。

Guest-VLAN

配置选项：使能/不使能

默认配置：不使能

功能：使能时，客户端用户在未认证或认证失败的情况下，设备将客户端认证端口加入到客户 VLAN 中，所有该端口下接入的用户被授权访问客户 VLAN 中的资源。

RADIUS-QOS

配置选项：使能/不使能

默认配置：不使能

功能：使能时，客户端认证通过后，服务器会把授权信息传送给设备端。如果服务器上配置了指派流控功能，则授权信息中含有授权指派的 CoS 信息，设备将按照该指派值修改客户

端认证端口的 CoS 值。

RADIUS-VLAN

配置选项：使能/不使能

默认配置：不使能

功能：客户端认证通过后，服务器会把授权信息传送给设备端。如果服务器上配置了指派 VLAN 功能，则授权信息中含有授权指派的 VLAN 信息，设备将客户端认证端口加入到指派 VLAN 中。

重认证

配置选项：使能/不使能

默认配置：不使能

功能：当认证成功后，是否需要周期性的重新认证，以定期检测用户的在线情况。

认证模式

配置选项：Remote/Local

默认配置：Remote

功能：配置 radius 认证模式为远程认证或本地认证。

重认证定时器(秒)

配置范围：1~3600s

默认配置：3600s

功能：认证成功后，重认证的时间间隔。

重认证最大次数

配置范围：1~255

默认配置：2

功能：配置 Identity EAPOL 请求报文超时重传的次数，如果累计的传送次数超过该配置值，客户端仍旧没有响应，则认为本次认证失败。

EAPOL 重传间隔

配置范围：1~65535s

默认配置：30s

功能：配置客户端响应超时时间；设备发送 Identity EAPOL 请求报文后，如果该时间段内，未收到客户端的响应，则重新发送 Identity EAPOL 请求报文。

Inactivity Timer

配置范围：10~1000000s

默认配置：300s

功能：基于 MAC 认证时，认证成功后，若该时间内没有报文通过，则删除对应安全表项。

静默定时器(秒)

配置范围：10~1000000s

默认配置：10s

功能：认证失败后，设备进入静默周期；静默周期内，设备对客户端的认证请求不予响应。

Guest-VLAN

配置选项：1~4093

默认配置：1

功能：配置客户 VLAN ID。

Guest-VLAN Supplicant

配置选项：使能/不使能

默认配置：不使能

功能：使能时，客户端用户在未认证或认证失败的情况下，设备将客户端认证端口加入到客户 VLAN 中；不使能时，只有当该端口无 EAPOL 帧记录时，设备将该端口加入到客户 VLAN 中。

注意：

- “Guest-VLAN 号”、“重认证最大次数”、“Guest-Vlan Supplicant”参数配置的前提是使能 Guest-VLAN；
- 如果客户端认证端口类型为 Trunk 或 Hybrid 类型时，不建议使能 RADIUS-VLAN 和 Guest-VLAN；
- 授权指派的 CoS 并不改变端口的配置，也不影响端口的配置。但授权指派的 CoS 优先级高于用户配置的 CoS，即认证通过后起作用的是授权指派的 CoS；用户认证失败或用户下线后，用户配置的 CoS 生效；
- 授权指派的 VLAN/客户 VLAN 并不改变端口的配置，也不影响端口的配置。但授权指派的 VLAN/客户 VLAN 优先级高于用户配置的 VLAN。

客户端用户发起认证，如果认证成功：

若端口使能 RADIUS-VLAN，则端口加入 RADIUS 服务器指派 VLAN 中；

若端口不使能 RADIUS-VLAN，则端口加入用户配置的 VLAN 中。

如果认证失败或用户下线：

若端口使能 Guest-VLAN 和 Guest-Vlan Supplicant，则端口加入客户 VLAN 中；

若端口使能客户 VLAN，不使能 Guest-Vlan Supplicant，则端口无 EAPOL 帧记录时加入客户 VLAN 中，端口有 EAPOL 帧记录时加入用户配置的 VLAN 中；

若端口不使能客户 VLAN，则端口加入用户配置的 VLAN 中。

3、IEEE802.1X 端口配置，如下图所示；

图 228 配置 IEEE802.1X 端口

端口

配置选项：交换机上所有端口

管理状态

配置选项：强制认证/强制不认证/基于端口/基于 MAC

默认配置：强制认证

功能：选择端口的认证模式。

描述：强制认证表示端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。强制不认证表示端口始终处于非授权状态，不允许用户进行认证，设备端不对通过该端口接入的客户端提供认证服务。基于 MAC 和基于端口表示端口初始状态为未认证通过状态，不允许用户访问网络资源，如果认证通过，则端口切换到认证通过状态，允许用户访问网络资源；如果认证失败，则端口切换到未认证通过状态，不允许用户访问网络资源。

基于 MAC 认证表示该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。基于端口表示只要该端口下的第一个用户认证成功后，该端口即可打开，其他接入用户无须认证就可使用网络资源，但是当第一个用户下线后，该端口关闭，其他用户也会被拒绝使用网络。

RADIUS-QOS

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的 RADIUS 指派流控。

RADIUS-VLAN

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的 RADIUS 指派 VLAN。

Guest-VLAN

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的客户 VLAN。

说明：

RADIUS-QOS、RADIUS-VLAN、Guest-VLAN 必须全局和端口同时使能时，该功能才生效。

4、IEEE802.1X 用户配置，如下图所示；

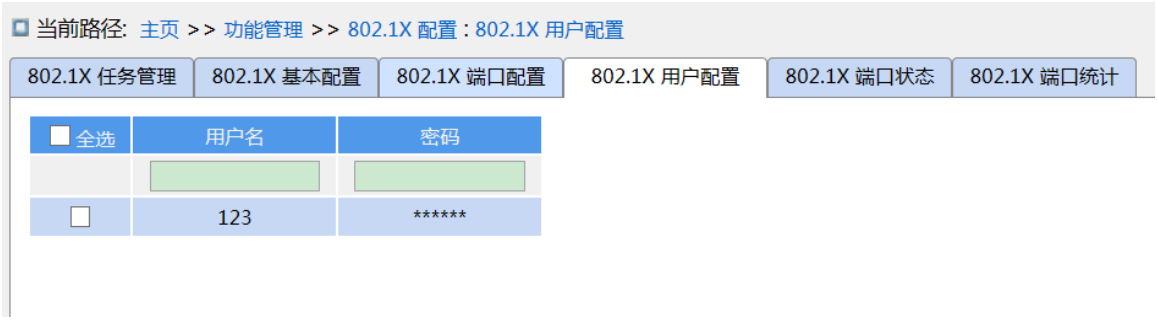


图 229 IEEE802.1X 用户配置

用户名

配置选项：1-16 个字符

默认配置：空

功能：配置本地认证用户名。

密码

配置选项：1-16 个字符

默认配置：空

功能：配置本地认证密码。

5、查看 IEEE802.1X 端口状态，如下图所示；

端口	Admin	端口状态	Last Src	Last ID	QoS	VLAN	Guest
1	Port-based 802.1X	Disable	--	--	--	--	--
2	Force Authorized	Disable	--	--	--	--	--
3	Force Authorized	Disable	--	--	--	--	--
4	Force Authorized	Disable	--	--	--	--	--
5	Force Authorized	Disable	--	--	--	--	--
6	Force Authorized	Disable	--	--	--	--	--
7	Force Authorized	Disable	--	--	--	--	--
8	Force Authorized	Disable	--	--	--	--	--
9	Force Authorized	Disable	--	--	--	--	--
10	Force Authorized	Disable	--	--	--	--	--
11	Force Authorized	Disable	--	--	--	--	--
12	Force Authorized	Disable	--	--	--	--	--
13	Force Authorized	Disable	--	--	--	--	--
14	Force Authorized	Disable	--	--	--	--	--
15	Force Authorized	Disable	--	--	--	--	--
16	Force Authorized	Disable	--	--	--	--	--

图 230 IEEE802.1X 端口状态

端口状态

显示选项：Disable、Auth、UnAuth、down、x A/y UnA

功能：显示端口状态。Disable 指 802.1X 功能全局去使能；Auth 指该端口下用户认证成功；UnAuth 指该端口下用户认证失败；down 指该端口处于 link down 状态；x A/yUnA 指基于 MAC 认证时，该端口下 x 个用户认证成功，y 个用户认证失败。

6、查看 IEEE802.1X 端口统计信息，如下图所示；

图 231 查看 IEEE802.1X 端口统计信息

点击端口详细信息，进入相应端口的 IEEE802.1X 信息统计界面，如下图所示；

<<返回

统计		
Eapol	Rx Total	0
	Tx Total	0
	Rx RespId	0
	Tx ReqId	0
	Rx RespMD5	0
	Tx ReqMD5	0
	Rx Resp	0
	Tx Req	0
	Rx Start	0
	Rx LogOff	0
	Rx Invalid Type	0
	Rx Invalid Len	0
Radius	Rx Access Challenges	0
	Rx Other Requests	0
	Rx Auth Successes	0
	Rx Auth Failures	0
	Tx Responses	0
	Mac Address	--
Local	MD5-Challenge Match	0
	MD5-Challenge Mismatch	0
	Error User	0
	Error Decode	0
	Error InvalidNethod	0

图 232 查看 IEEE802.1X 端口的详细统计信息

7.12.3 典型配置举例

如下图所示，客户端连接交换机端口 1，使能端口 1 的 IEEE802.1X 协议并且采用基于端口的 802.1X 认证模式，远程认证用户名和密码为 ddd，其余配置采用默认值；

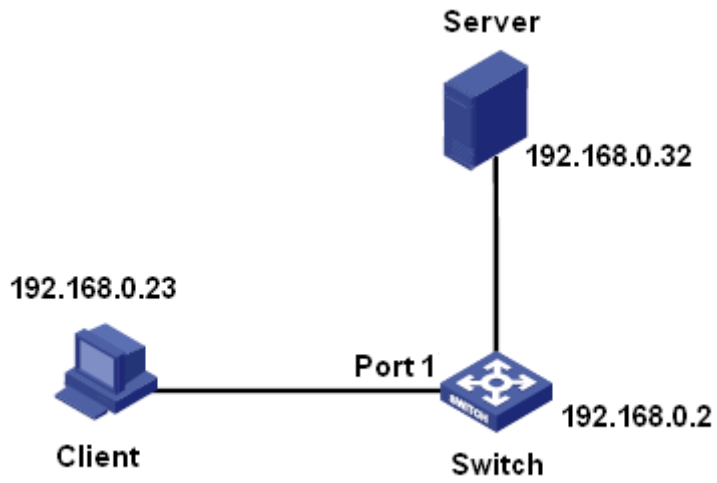


图 233 IEEE802.1X 配置举例

可参考“5.6 RADIUS 配置”章节的配置举例内容。

7.13 GMRP

7.13.1 GARP 介绍

GARP(Generic Attribute Registration Protocol，通用属性注册协议)用于同一网络内交换机之间传播、注册和注销某种信息(VLAN、组播地址等)。GARP 应用分为 GVRP 和 GMRP。

通过 GARP 机制，一个 GARP 成员的配置信息会迅速传播到整个交换网。GARP 成员通过 join/leave 消息通知其它 GARP 成员注册或注销自己的属性信息，并根据其他成员的 join/leave 消息注册或注销对方的属性信息。

GARP 中起作用的消息有三类：Join、Leave、LeaveAll。

- 当一个 GARP 应用实体希望其它交换机注册自己的某种属性信息时，将 对外发送 Join 消息。Join 消息分为 JoinEmpty 和 JoinIn 两种，发送 JoinIn 消息用来声明一个该应用实体已经注册的属性；发送 JoinEmpty 消息用来声明一个该应用实体没有注册的属性。
- 当一个 GARP 应用实体希望其它交换机注销自己的某种属性信息时，将对外发送 Leave 消息。Leave 消息分为 LeaveEmpty 和 LeaveIn 两种，发送 LeaveIn 消息用来注销一个该应用实体已经注册的属性；发送 LeaveEmpty 消息用来注销一个该应用实体没有注册的属性。
- 每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GARP 应用实体将对外发送 LeaveAll 消息。

说明：

应用实体指使能该注册协议的端口。

GARP 定时器包括 Hold 定时器、Join 定时器、Leave 定时器和 LeaveAll 定时器：

Hold 定时器：当 GARP 应用实体接收到某注册信息时，不立即对外发送 Join 消息，而是启动 Hold 定时器，当该定时器超时后，将此时段内收到的所有注册信息放在一个 Join 消息中向外发送，从而减少报文发送量有利于网络稳定。

Join 定时器：为保证 Join 消息能够可靠地传输到其它应用实体，GARP 应用实体发送第一个 Join 消息后将等待一个 Join 定时器时间间隔，如果在该时间段内没有收到 JoinIn 消息，则再发送一个 Join 消息，否则不发送第二个 Join 消息。

Leave 定时器：当一个 GARP 应用实体希望注销某属性信息时，将对外发送 Leave 消息，接收到该消息的 GARP 应用实体启动 Leave 定时器，如果在该定时器超时之前没有再次收到 Join 消息，则注销该属性信息。

LeaveAll 定时器：每个 GARP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后，GARP 应用实体将对外发送 LeaveAll 消息，以使其它 GARP 应用实体重新注册本实体的所有属性信息。随后再启动 LeaveAll 定时器，开始新的一轮循环。

7.13.2 GMRP 协议

GMRP(GARP Multicast Registration Protocol ，GARP 组播注册协议)是基于 GARP 的一个组播注册协议，用于维护交换机中的组播注册信息。所有使能 GMRP 协议的交换机都能接收来自其他交换机的组播注册信息，并动态更新本地的组播注册信息，同时也能将本地的组播注册信息向其他交换机传播。这种信息交换机制，确保了同一网络中所有支持 GMRP 的交换机维护的组播信息的一致性。

一旦交换机或者终端注册或注销某组播组时，通过使能 GMRP 功能的端口将该信息广播给同一 VLAN 中的所有端口。

7.13.3 说明

代理端口：使能 GMRP 功能和代理功能的端口；

扩散端口：只使能 GMRP 功能，没有使能代理功能的端口；

动态学习的 GMRP 组播表项以及代理端口的代理表项将从扩散端口转发至下一级设备的

扩散端口。

同一网络中的所有 GMRP 定时器必须保持一致以防相互之间存在潜在的干扰问题。定时器之间应遵循的规则如下：holdtimer < jointimer，2*jointimer < leavetimer，leavetimer < leavealltimer。

7.13.4 Web 页面配置

1、使能全局 GMRP 协议，配置全局定时器，如下图所示：

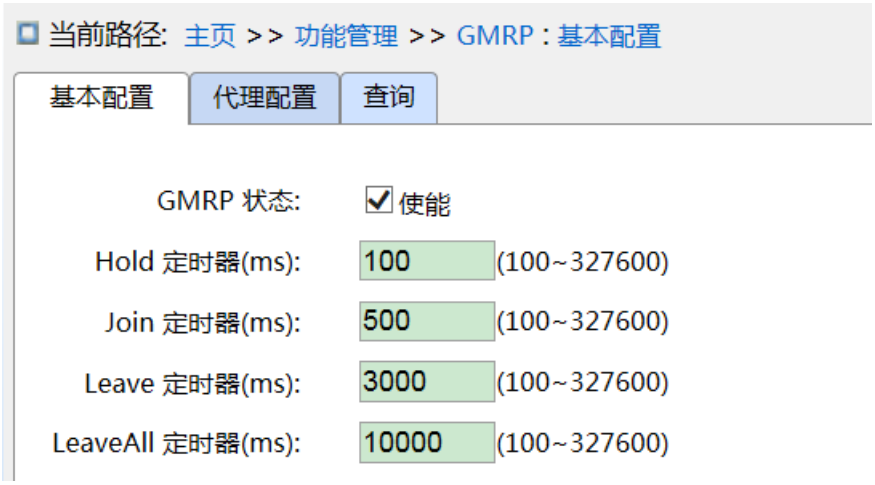


图 234 GMRP 全局配置表

GMRP 状态

配置选项：使能/不使能

默认配置：不使能

功能：是否全局使能 GMRP 功能，该功能与 IGMP-Snooping 功能不能同时使能。

Hold 定时器

配置范围：100ms~327600ms

默认配置：100ms

描述：该值必须是 100 的倍数，所有使能 GMRP 功能端口的 Hold timer 值最好一致。

Join 定时器

配置范围：100ms~327600ms

默认配置：500ms

描述：该值必须是 100 的倍数，所有使能 GMRP 功能端口的 Join timer 值最好一致。

Leave 定时器

配置范围：100ms~327600ms

默认配置：3000ms

描述：该值必须是 100 的倍数，所有使能 GMRP 功能端口的 Leave timer 值最好一致。

LeaveAll 定时器

配置范围：100ms~327600ms

默认配置：10000ms

功能：发送 leave all 信息的时间间隔，必须是 100 的倍数。

说明：如果不同设备的 LeaveAll 定时器同时超时，就会同时发送多个 LeaveAll 消息增加不必要的报文数量，为了避免不同设备同时发生 LeaveAll 定时器超时，Leave all 定时器实际运行的值是大于 leave all 定时器值，小于 1.5 倍 leave all 定时器值的一个随机值。

2、配置每个端口的 GMRP 功能，如下图所示：

端口	GMRP 使能	GMRP 代理使能	最后的PDU源
1	☑	☑	--
2	☑	☐	--
3	☐	☐	--
4	☐	☐	--
5	☐	☐	--
6	☐	☐	--
7	☐	☐	--
8	☐	☐	--
9	☐	☐	--
10	☐	☐	--
11	☐	☐	--
12	☐	☐	--

图 235 端口 GMRP 配置

GMRP 功能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的 GMRP 功能。

GMRP 代理功能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的 GMRP 代理功能。

最后的 PDU 源

功能：此端口最后收到协议报文的源 MAC 地址。

注意：

- 代理端口不可以传播代理表项；
- 使能端口 GMRP 代理功能的前提是使能端口 GMRP 功能。

3、添加一个 GMRP 代理表项，配置如下图：

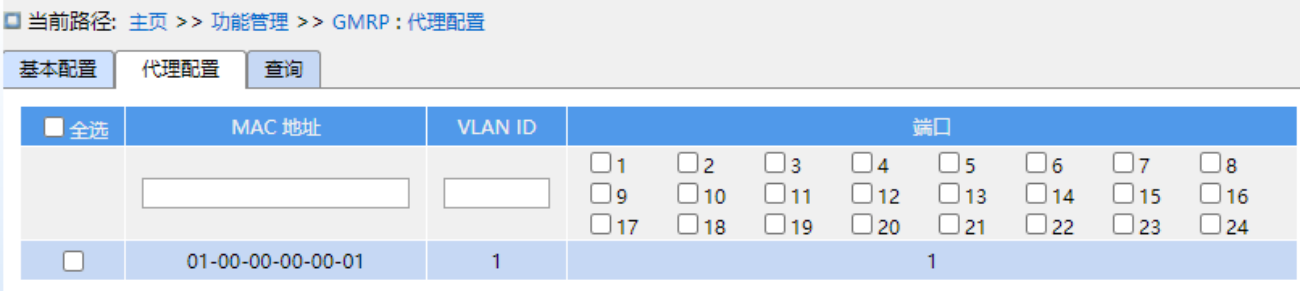


图 236 GMRP 代理表项配置

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH (H 为一个十六进制数)

功能：配置组播组 MAC 地址，最高字节的最低位为 1 即可。

VLAN ID

配置选项：已创建的 VLAN 号

功能：配置 GMRP 代理表项的 VLAN ID。

描述：GMRP 代理表项只从跟该表项 VLAN ID 一致的扩散端口转发。

端口

配置选项：已配置的代理端口

4、查看 GMRP 配置信息，如下图所示：

图 237 查看 GMRP 配置信息

7.13.5 典型配置举例

如下图所示，交换机 A 和 B 通过端口 2 连接，交换机 A 中端口 1 配置为代理端口，并且代理两条组播表项：

MAC 地址：01-00-00-00-00-01 VLAN：1

MAC 地址：01-00-00-00-00-02 VLAN：2

通过配置端口的不同 VLAN 属性观察交换机之间动态注册和更新组播信息的情况。

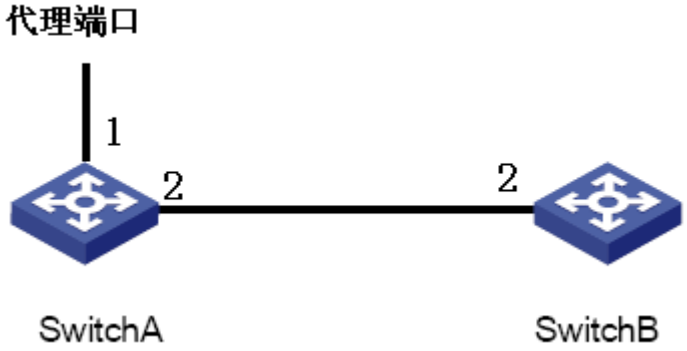


图 238 GMRP 组网图

交换机 A 配置过程：

1、使能交换机 A 的全局 GMRP 功能，定时器采用默认值，见图 234；

2、使能端口 1 的 GMRP 功能和代理功能；使能端口 2 的 GMRP 功能，见图 235；

3、配置代理组播表项，<MAC 地址，VLAN ID，成员端口>配置为<01-00-00-00-00-01，1，1>和<01-00-00-00-00-02，2，1>，见图 236；

交换机 B 的配置过程：

4、使能交换机 B 的全局 GMRP 功能，定时器采用默认值，见图 234；

5、使能端口 2 的 GMRP 功能，定时器的值都采用默认值，见图 235；

交换机 B 上动态学习到的 GMRP 组播表项如下表所示；

表 11 动态组播表项

SwitchA 端口 2 的属性	**SwitchB 端口 2 的属性**	**SwitchB 上收到的组播表项**
Access VID=1	Access VID=1	MAC：01-00-00-00-00-01 VLAN ID：1 成员端口：2
Access VID=2	Access VID= 2	MAC：01-00-00-00-00-02 VLAN ID：2 成员端口：2
Access VID= 1	Access VID= 2	MAC：01-00-00-00-00-01 VLAN ID：2 成员端口：2

7.14 路由表

7.14.1.1 介绍

静态路由是由管理员手工配置。在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。静态路由的优点是简单易配、稳定、限制非法的路由改变，便于实现负载分担和路由备份。静态路由的缺点在于：不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

7.14.1.2 Web 页面配置

静态路由配置

图 239 静态路由配置

IP 模式

配置选项：使能/不使能

功能：是否使能 IP 模式。

目的网络

配置格式：A.B.C.D

功能：配置目的主机或目的网络 IP 地址。

掩码长度

功能：子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。掩码长度指掩码中 1 的个

数。

下一跳

配置格式：A.B.C.D

功能：配置下一跳 IP 地址。

7.15 QoS 配置

7.15.1 介绍

QoS（Quality of Service，服务质量）是 IP 网络中利用流量控制和资源分配思想来解决有限带宽条件下为有不同需求的多业务提供有区别的服 务，尽可能满足不同业务的传输特点减少网络拥塞发生的概率，并将网络拥塞对高优先级业务的影响减到最少的一种机制。

流分类、流量监管、流量整形、拥塞管理和拥塞避免是 QoS 部署的主要思路，它们主要完成如下功能：

流分类：依据一定的匹配规则识别出对象，是 QoS 的基础和前提。

流量监管：对进入设备的特定流量的规格进行监管，当流量超出规格时，可以采取限制或惩罚措施，以保护网络资源不受损害。流量监管分为基于端口和基于队列两种流量监管。

流量整形：主动调整流量输出速率的措施，通常是为了使流量适配下游设备可供给的网络资源，避免不必要的报文丢弃和拥塞。流量整形分为基于端口和基于队列两种流量整形。

拥塞管理：拥塞管理是必须采取的解决资源竞争的措施。通常是将报文放入队列中缓存，并采取某种调度算法安排报文的转发次序，从而实现对关键业务内容的优先转发。

拥塞避免：过度的拥塞会对网络资源造成损害。拥塞避免监督网络资源的使用情况，当发现拥塞有加剧的趋势时采取主动丢弃报文的策略，通过调整流量来解除网络的过载。

流量监管、流量整形、拥塞管理和拥塞避免从不同方面对网络流量及其分配的资源实施控制，是 QoS 思想的具体体现。例如：当报文进入网络时依据承诺速率对它进行监管；流出节点之前进行整形；拥塞时采取队列调度管理；拥塞加剧时采取拥塞避免措施。

7.15.2 原理

该系列交换机每个端口有 8 个缓存队列，依次为 0、1、2、3、4、5、6、7，优先级逐渐递增。

当一帧数据到达一个端口时，根据其报文信息或端口决定报文应存放的队列。该系列交换

机支持以下几种队列映射模式来实现流分类：端口、802.1Q 头信息、DSCP、QCL（QoS Control List，QoS 控制列表），优先级依次递增。

端口转发数据时，通过调度模式决定如何调度 8 个队列中的数据以及每个队列所占用的带宽，该系列交换机支持以下 QoS 队列调度模式：SP（Strict Priority，严格优先级）模式和 6 Queues Weighted 模式。

WRR（Weighted Round Robin，加权轮询调度）模式按照权重比对数据流进行调度，各队列按照权重比来分配所占用的带宽。WRR 调度算法偏重于权重比高的队列，给该队列分配较多的带宽传输数据。

SP 调度模式能够严格保证高优先级报文的转发，主要用于敏感信号的传输。如果一帧数据进入高优先级队列，将停止低优先级队列的调度来处理高优先级队列的数据。当高优先级队列为空时，再依次处理下一优先级队列中的数据。

6 Queues Weighted 调度模式即指 SP 与 WRR 的组合使用，如调度模式指队列 6 和队列 7 使用 Strict Priority 调度模式，队列 0~队列 5 使用 WRR 调度模式。6 Queues Weighted 优先处理队列 7 中的数据，其次为队列 6，当队列 7 和队列 6 为空时，按照权重比调度队列 0~队列 5 中的数据。

7.15.3 Web 页面配置

1、配置基于端口的队列映射模式，如下图所示；

图 240 配置基于端口的队列映射模式

CoS

配置范围：0~7

默认配置：0

功能：配置端口默认 CoS 值。

描述：CoS 值决定报文的存放队列，CoS 值 0~7 依次对应队列 0~7。报文进入交换机后，交换机给报文分配 CoS 值。如果报文为 tag 类型且不使能标签分级，或报文为 untag 类型，则报文的 CoS 值为接收端口的默认 CoS 值。

DPL

配置范围：0~1

默认配置：0

功能：配置端口默认 DPL（Drop Priority Level，丢弃优先级）值

功能：Untag 报文或未使能标签分级的 tag 报文进入交换机后指定的 DPL 值为端口默认 DPL。

PCP

配置范围：0~7

默认配置：0

功能：配置端口默认 PCP（Priority Code Point，优先级代码点）值。

描述：Untag 报文进入交换机后添加的 Tag 标记中优先级值为端口默认 PCP 值。

DEI

配置范围：0~1

默认配置：0

功能：配置端口默认 DEI（Drop Eligible Indicator）值。

描述：Untag 报文进入交换机后添加的 Tag 标记中 CFI 值为端口默认 DEI 值。

2、配置基于 802.1Q 头信息的队列映射模式

“√”选图 240 中端口的<标签分级>选项，并点击（PCP,DEI）到（QOS,DPL）的映射列<详细配置>按钮，进入对应接口的基于 802.1Q 头信息的队列映射模式配置界面，如下图所示。

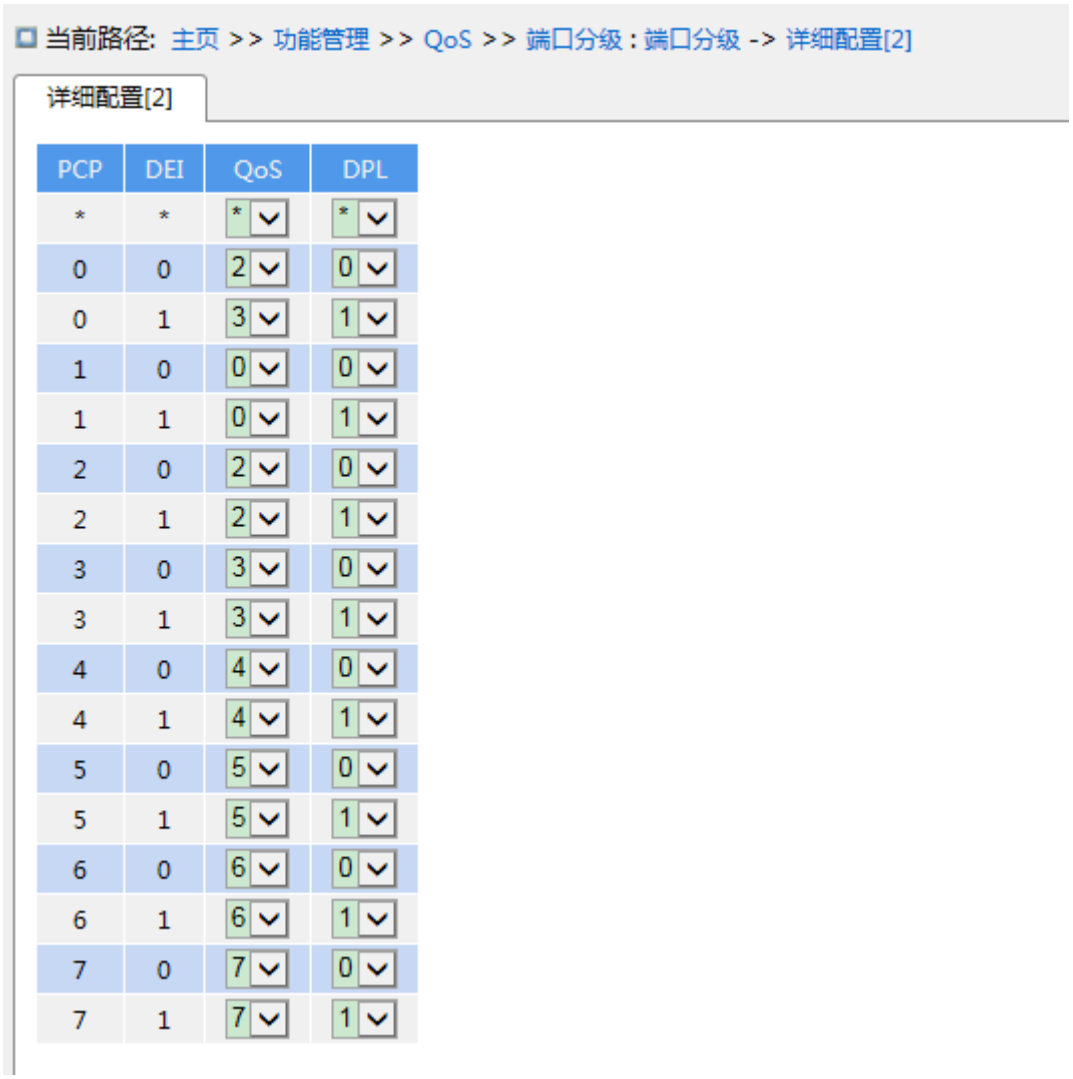


图 241 配置基于 802.1Q 头信息的队列映射模式

注意：

基于 802.1Q 头信息的队列映射模式只适用于端口接收的报文为 Tag 类型。

（PCP, DEI）到（QoS, DP）映射

配置范围：0~7（QoS 类别）0~1（DP 等级）

默认配置：PCP 值 0, 1, 2, 3, 4, 5, 6, 7 分别映射到 QoS 类别 1, 0, 2, 3, 4, 5, 6, 7；DEI 值 0, 1 分别映射到 DP 等级 0, 1。

功能：根据报文中的 PCP 和 DEI 值，配置（PCP, DEI）到（CoS, DPL）映射关系。

描述：QoS 类别等同于 CoS 值，CoS 值决定报文的存放队列，CoS 值 0~7 依次对应队列 0~7。报文进入交换机后，交换机给报文分配 CoS 值和 DPL 值。如果报文类型为 tag，且使能 Tag 分级，则报文的 CoS 值和 DPL 值为（PCP, DEI）映射的（CoS, DPL）。

3、配置端口重标记，如下图所示；

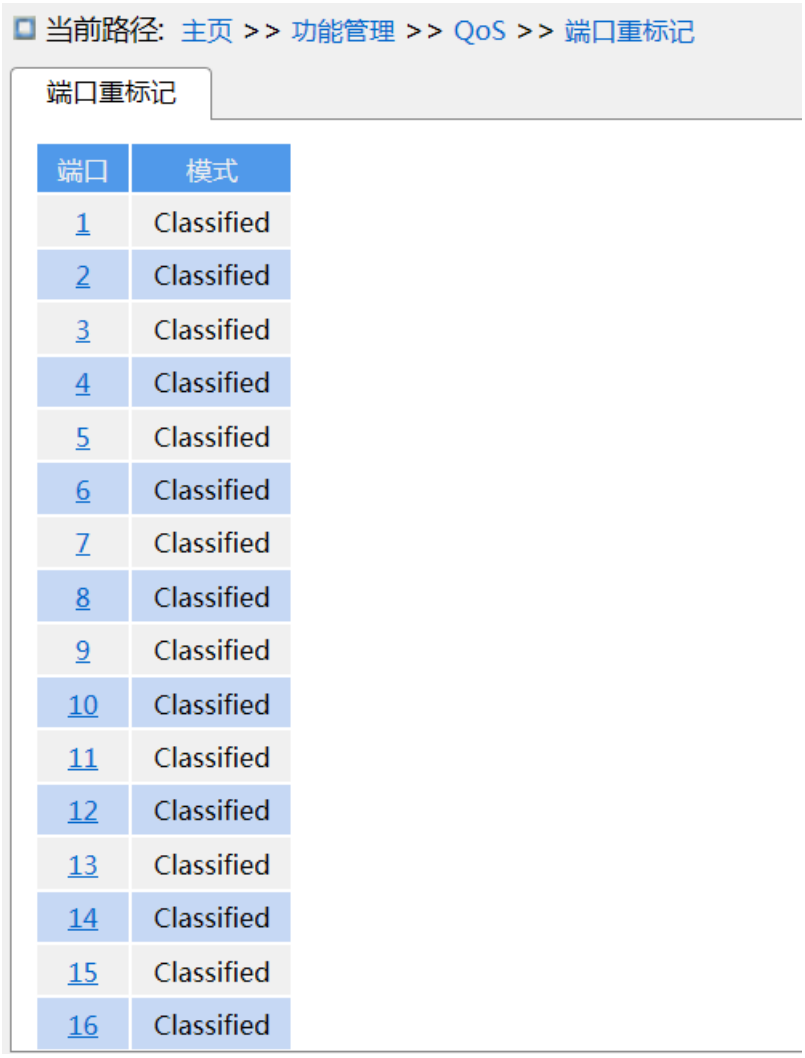


图 242 配置 802.1p 重标记

点击<端口>按钮，进入 802.1p 重标记配置界面，如图 243 所示。该页面显示出端口转发报文时重标记 802.1p 的模式。802.1p 重标记指出端口转发报文时更新报文中的 PCP 和 DEI 值。

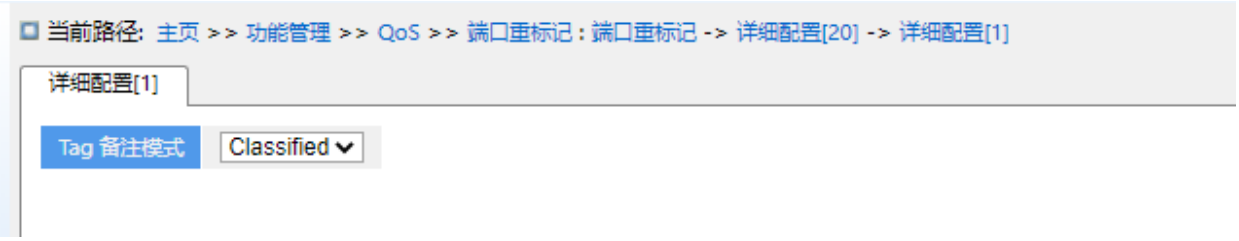


图 243 配置指定端口的 802.1p 重标记模式

注意：

如果出端口转发的报文中不带有 Tag 标记，则 802.1p 重标记功能无效。

➢ 配置 802.1p 重标记模式为 Classified，如图 243 所示。

Tag 备注模式

配置选项：Classified/Mapped/Default

默认配置：Classified

功能：配置 802.1p 重标记模式。Classified 模式：出端口转发报文时，不更新报文中的 PCP 和 DEI 值。

➢ 配置 802.1p 重标记模式为 Default，如下图所示；

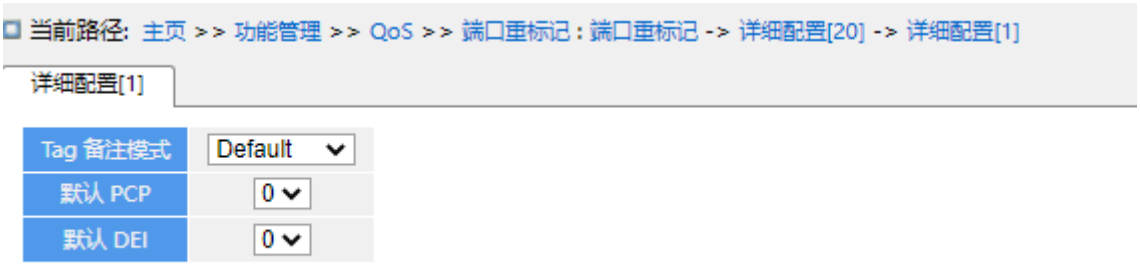


图 244 配置 Default 重标记模式

Tag 备注模式

配置选项：Classified/Mapped/Default

默认配置：Classified

功能：配置 802.1p 重标记模式。Default 模式：出端口转发报文时，更新报文中的 PCP 和 DEI 值为出端口的默认值（下方配置）。

默认 PCP

配置范围：0~7

默认配置：0

功能：配置出端口的默认 PCP 值。

默认 DEI

配置范围：0~1

默认配置：0

功能：配置出端口的默认 DEI 值。

➢ 配置 802.1p 重标记模式为 Mapped，如下图所示；

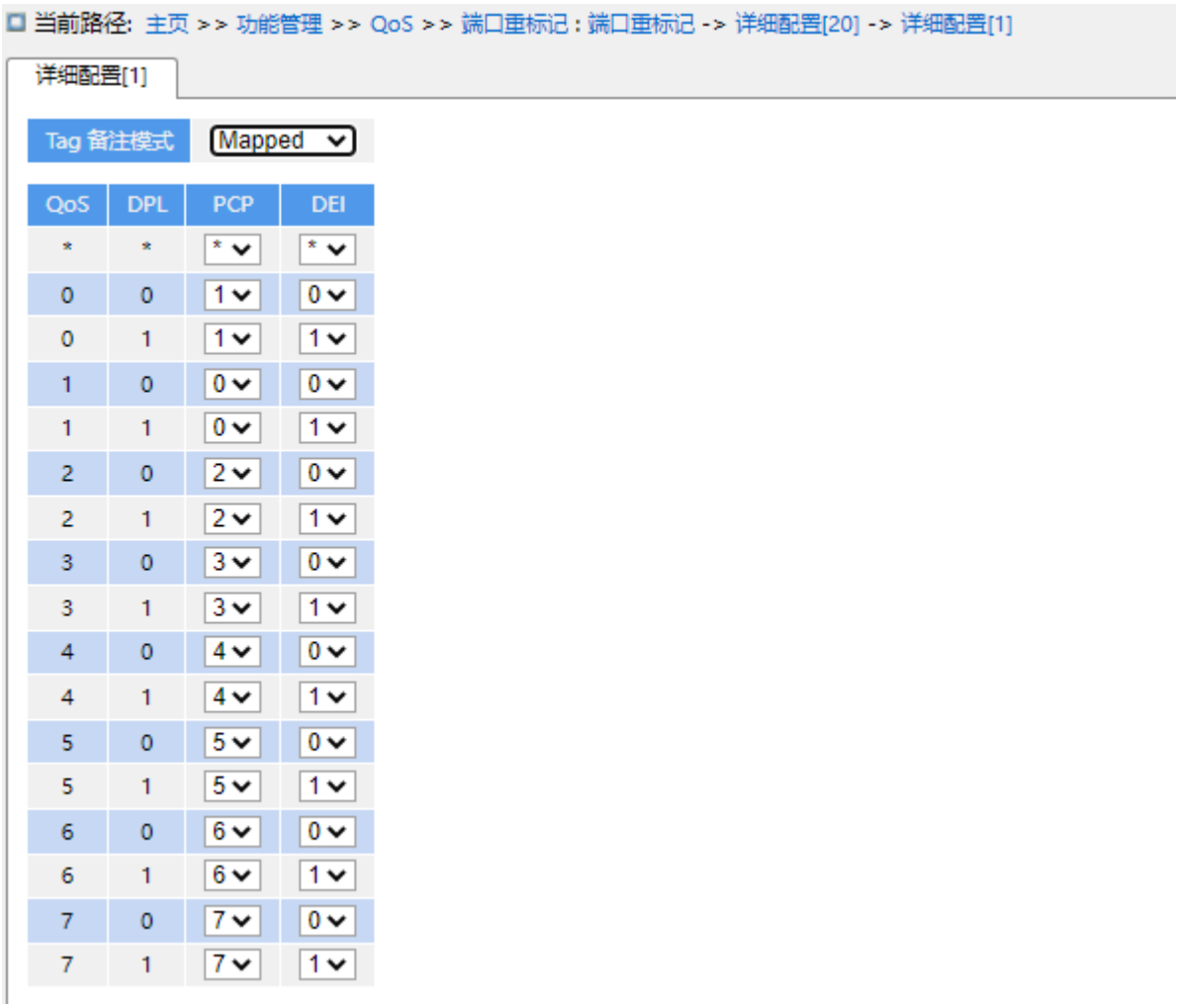


图 245 配置 Mapped 重标记模式

Tag 备注模式

配置选项：Classified/Mapped/Default

默认配置：Classified

功能：配置 802.1p 重标记模式。Mapped 模式：出端口转发报文时，更新报文中的 PCP 和 DEI 值为（CoS, DPL）映射的（PCP, DEI）值（映射关系下方配置）。

（QoS 分级, DP 等级）到（PCP, DEI）映射

配置范围：0~7（PCP）0~1（DEI）

默认配置：QoS 分级 0, 1, 2, 3, 4, 5, 6, 7 分别映射到 PCP 值 1, 0, 2, 3, 4, 5, 6, 7；DP 等级 0, 1 分别映射到 DEI 值 0, 1。

功能：根据报文中的 CoS 和 DPL 值，配置（CoS, DPL）到（PCP, DEI）的映射关系。

4、使能基于 DSCP 的队列映射模式，如下图所示；

图 246 使能基于 DSCP 的队列映射模式

基于 DSCP

配置选项：使能/不使能

默认配置：不使能

功能：是否使能基于 DSCP 的队列映射模式，该队列映射模式优先级高于基于 802.1Q 头信息的队列映射模式。

5、使能入端口 DSCP 转换、出端口 DSCP 重写功能，如下图所示；

图 247 配置端口 DSCP 功能

转换

配置选项：使能/不使能

默认配置：不使能

功能：入端口接收报文后，是否对报文中的 DSCP 值进行转换。若使能，DSCP 值的转换按照 DSCP 转换表（图 249 中“转换”列）进行。

分类

配置选项：不使能/DSCP=0/Selected/All

默认配置：不使能

功能：重写配置为 Enable 时，该参数选择出端口重写的 DSCP 值。

不使能：出端口转发报文时，不重写报文中的 DSCP 值；

DSCP=0：出端口转发报文时，如果报文中的 DSCP=0，则按照图 249 中的分级规则重写报文中的 DSCP 值；

Selected：出端口转发报文时，如果报文中的 DSCP 值为选定值（图 249 中“分类”列），则按照图 250 中的分级规则重写报文中的 DSCP 值；

All：出端口转发报文时，按照图 250 中的分级规则重写报文中的 DSCP 值。

重写

配置选项：不使能/使能/重映射

默认配置：不使能

功能：配置出端口转发报文时，DSCP 值的重写方式。

不使能：出端口转发报文时，不重写报文中的 DSCP 值；

使能：出端口转发报文时，按照分类的配置决定是否重写报文中的 DSCP 值；

重映射：出端口转发报文时，按照（DSCP，DPL）到 DSCP 的映射关系（图 249 中“重映射 DP0、DP1”列）重写报文中的 DSCP 值。

6、配置基于 DSCP 的队列映射模式，如下图所示；

图 248 配置基于 DSCP 的队列映射模式

信任

配置选项：使能/不使能

默认配置：不使能

功能：是否信任该 DSCP 值。

注意：

基于 DSCP 的队列映射模式只适用于端口接收的报文中 DSCP 值为信任值。

COS

配置范围：0~7

默认配置：0

功能：配置 DSCP 到 CoS 映射关系。

描述： CoS 值决定报文的存放队列，CoS 值 0~7 依次对应队列 0~7。DSCP 值为信任值的报文进入交换机后，交换机按照 DSCP 到 CoS 的映射关系给报文分配 CoS 值。

注意：

入端口使能转换时，交换机按照转换后的 DSCP 值分配 CoS 值；否则，按照报文中原有的 DSCP 值分配 CoS 值。

DPL

配置范围：0~1

默认配置：0

功能：配置 DSCP 到 DPL 映射关系

描述：DSCP 值为信任值的报文进入交换机后，交换机按照 DSCP 到 DPL 的映射关系给报文分配 DPL 值。

7、配置 DSCP 转换及重写，如下图所示；

图 249 配置 DSCP 转换与重写

转换

配置范围：0~63

功能：配置 DSCP 值的转换表。

分类

配置选项：使能/不使能

默认配置：不使能

功能：图 247 中“分类”配置为 Selected，该参数配置选中的 DSCP 值。

注意：

入端口使能转换时，选中的 DSCP 值为转换后的 DSCP 值；否则，选中的 DSCP 值为报文中原有的 DSCP 值。

重映射 DP0

配置范围：0~63

功能：配置（DSCP，DPL）到 DSCP 值的映射关系。

8、配置 DSCP 分级规则，如下图所示；

图 250 配置 DSCP 分级

DSCP DP0

配置范围：0~63

功能：配置（CoS，DPL）到 DSCP 值的映射关系。QoS 分级等同于 CoS 值，CoS 值决定报文的存放队列，CoS 值 0~7 依次对应队列 0~7。

9、配置 QCL 表项，如下图所示；

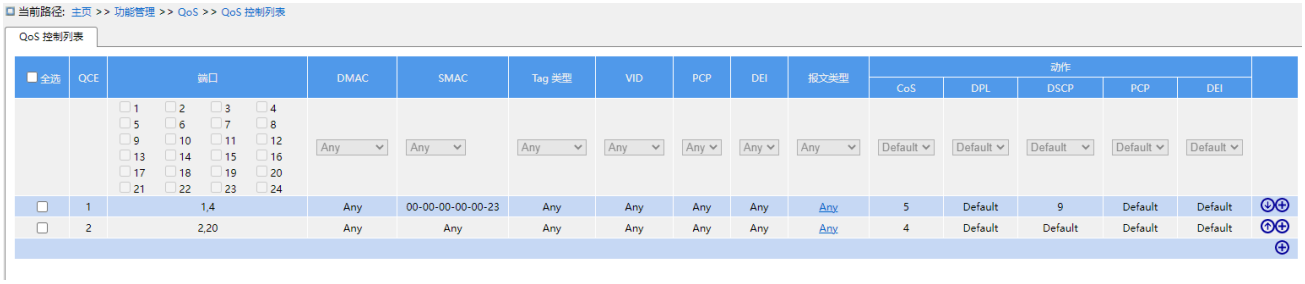


图 251 配置 QCL 表项

通过匹配 QCL 表项实现报文的队列映射，每条 QCL 表项有若干 QCL 条件构成，这些条件之间是“与”的关系，成员端口接收的报文只有满足所有条件时，才视为匹配该 QCL 表项。各条 QCL 表项之间无任何依赖关系。

存在多条 QCL 表项时，设备将报文与 QCL 表项逐条对比（按照表项从上到下的顺序），一旦报文遇到匹配的第一条 QCL 表项时，立即执行相应的动作。

点击<⊕>按钮，新建一条 QCL 表项；选中某条表项，点击<编辑>按钮，编辑当前表项；选中某条表项，点击<删除>按钮，删除当前表项。

QCE 为 QCL 表项 ID 号，按照表项创建先后顺序依次编号。

端口

功能：选择当前 QCL 表项的作用端口。

- 配置 QCL 表项参数，如下图所示；

DMAC

配置选项：Any/ Unicast/ Multicast / Broadcast

默认配置：Any

功能：配置条件参数--目的 MAC 地址，当成员端口接收的报文中目的 MAC 地址满足该参数配置时，该条件匹配成功。

SMAC

配置选项：Any/ Specific

默认配置：Any

功能：配置条件参数—源 MAC 地址，选择 Specific 时，需要配置一 MAC 地址。当成员端口接收的报文中源 MAC 地址满足该参数配置时，该条件匹配成功。

Tag

配置选项：Any/ Untagged/ Tagged

默认配置：Any

功能：配置条件参数--Tag 标记。当成员端口接收的报文满足该参数配置时，该条件匹配成功。

VID

配置选项：Any/ Specific（1~4095）/ Range（1~4093）

默认配置：Any

功能：配置条件参数--VID，选择 Specific 时，需要配置 VID 值；选择 Range 时，需要配置 VID 范围。当成员端口接收的报文中 VID 满足该参数配置时，该条件匹配成功。当 Tag 参数配置为 Untagged 时，该参数不可配置。

PCP

配置选项：Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

默认配置：Any

功能：配置条件参数--PCP。当成员端口接收的报文中 PCP 满足该参数配置时，该条件匹配成功。当 Tag 参数配置为 Untagged 时，该参数不可配置。

DEI

配置选项：Any/0/1

默认配置：Any

功能：配置条件参数--DEI。当成员端口接收的报文中 DEI 满足该参数配置时，该条件匹配成功。当 Tag 参数配置为 Untagged 时，该参数不可配置。

报文类型

配置选项：Any/ EtherType/ LLC/ SNAP/ IPv4

默认配置：Any

功能：选择报文类型。

点击任一 QCL 报文类型字段，可进入报文类型详细配置界面。

- 配置 EtherType 报文参数，下图所示；

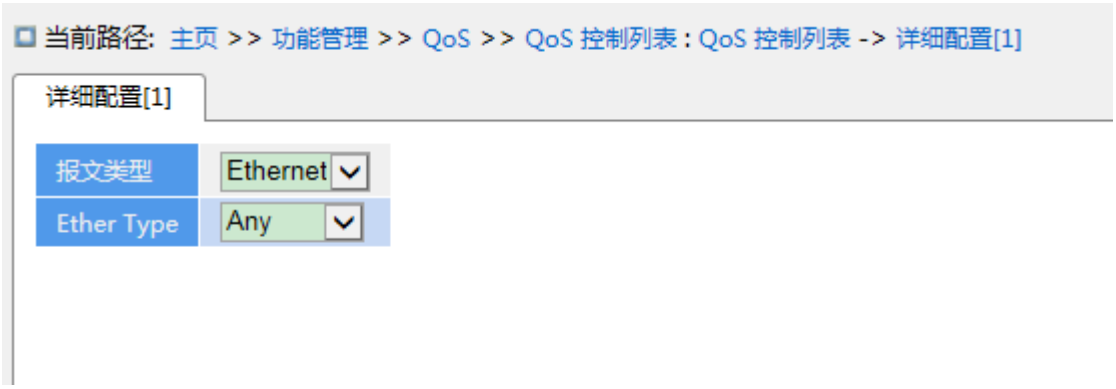


图 252 配置 EtherType 报文参数

Ether Type

配置选项：Any/ Specific（<0x600-0x7FF,0x801-0x86DC,0x86DE-0xFFFF>）

默认配置：Any

功能：配置条件参数--以太网类型，选择 Specific 时，需要配置以太网类型值。当成员端口接收的以太网报文满足该参数配置时，该条件匹配成功。

➢ 配置 LLC 报文参数，如下图所示；

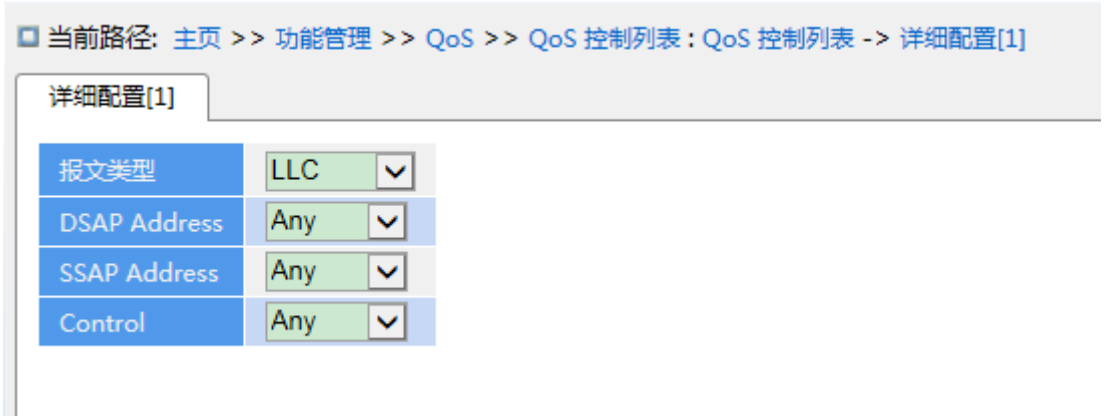


图 253 配置 LLC 报文参数

DSAP Address/SSAP Address/Control

配置选项：Any/Specific（0x00~0xFF）

默认配置：Any

功能：配置条件参数--LLC 报文参数，选择 Specific 时，需要配置具体值。当成员端口接收的 LLC 报文满足该参数配置时，该条件匹配成功。

➢ 配置 SNAP 报文参数，如下图所示；

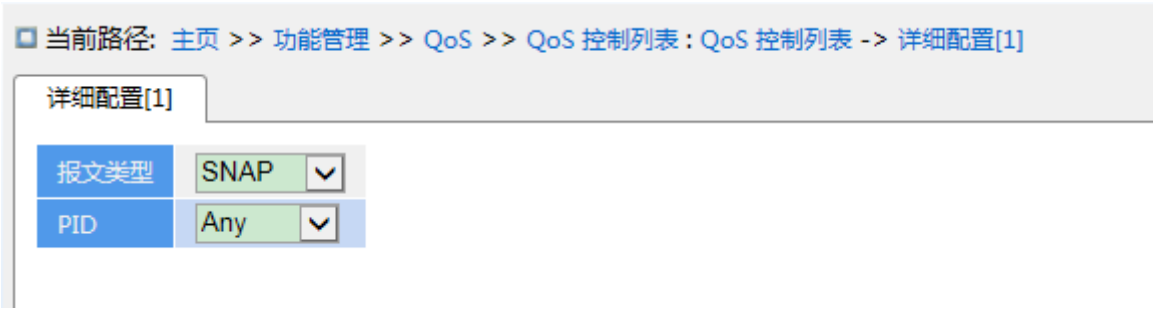


图 254 配置 SNAP 报文参数

PID

配置选项：Any/ Specific（0x0000~0xFFFF）

默认配置：Any

功能：配置条件参数--SNAP 报文参数，选择 Specific 时，需要配置 PID 值。当成员端口接收的 SNAP 报文中 PID 满足该参数配置时，该条件匹配成功。

➢ 配置 IPv4 报文参数，如下图所示；

图 255 配置 IPv4 报文参数

IP 协议

配置选项：Any/ UDP/ TCP/ Other（0~255）

默认配置：Any

功能：配置条件参数--IPv4 报文协议类型。选择 UDP/ TCP 时，需要配置源端口号和目的端口号；选择 Other 时，需要配置协议号。当成员端口接收的 IP 报文中协议类型满足该参数配置时，该条件匹配成功。

Sport/ Dport

配置选项：Any/ Specific（0~65535）/ Range（0~65535）

默认配置：Any

功能：配置条件参数--TCP/ UDP 源端口号和目的端口号，选择 Specific 时，需要配置端口号值；选择 Range 时，需要配置端口号范围。当成员端口接收的 IP 报文中端口号满足该参数配置时，该条件匹配成功。

SIP

配置选项：Any/ Specific

默认配置：Any

功能：配置条件参数--源 IP 地址和源 IP 掩码，选择 Specific 时，需要配置 IP 地址和 IP 掩码。当成员端口接收的 IP 报文中 SIP 满足该参数配置时，该条件匹配成功。

IP 分段

配置选项：Any/ Yes/ No

默认配置：Any

功能：配置条件参数--IP 分片报文。当成员端口接收的 IPv4 报文中 Fragment 满足该参数配置时，该条件匹配成功。

DSCP

配置选项：Any/ Specific（0~63）/ Range（0~63）

默认配置：Any

功能：配置条件参数--DSCP 值，选择 Specific 时，需要配置 DSCP 值；选择 Range 时，需要配置 DSCP 范围。当成员端口接收的 IP 报文中 DSCP 满足该参数配置时，该条件匹配成功。

- 配置 QCL 表项动作，如图 251 所示；

CoS

配置选项：0~7/ Default

默认配置：Default

功能：成员端口接收的报文匹配该 QCL 表项时，修改报文的 CoS 为该配置值。CoS 值决定报文的存放队列，CoS 值 0~7 依次对应队列 0~7，Default 指不修改报文的 Cos 值。

DPL

配置选项：Default/ 0/ 1

默认配置：Default

功能：成员端口接收的报文匹配该 QCL 表项时，修改报文中的 DPL 为该配置值。Default 指不修改报文中 DPL 值。

DSCP

配置选项：Default/ 0~63

默认配置：Default

功能：成员端口接收的报文匹配该 QCL 表项时，修改报文中的 DSCP 为该配置值。Default 指不修改报文中 DSCP 值。

PCP

配置选项：Default/ 0~7

默认配置：Default

功能：成员端口接收的报文匹配该 QCL 表项时，修改报文中的 PCP 为该配置值。Default

指不修改报文中 PCP 值。

DEI

配置选项：Default/ 0/ 1

默认配置：Default

功能：成员端口接收的报文匹配该 QCL 表项时，修改报文中的 DEI 为该配置值。Default 指不修改报文中 DEI 值。

➢ 查看 QCL 表项，如下图所示；

图 256 查看 QCL 表项

冲突

显示选项：No/Yes

功能：显示 QCL 表项的冲突状态。如果创建一条 QCL 表项的资源不足，则该表项冲突状态为 Yes；否则为 No。

点击<解决冲突>按钮，为有冲突的 QCL 表项释放所需资源使冲突消失。

10、配置基于队列的流量监管，如下图所示；

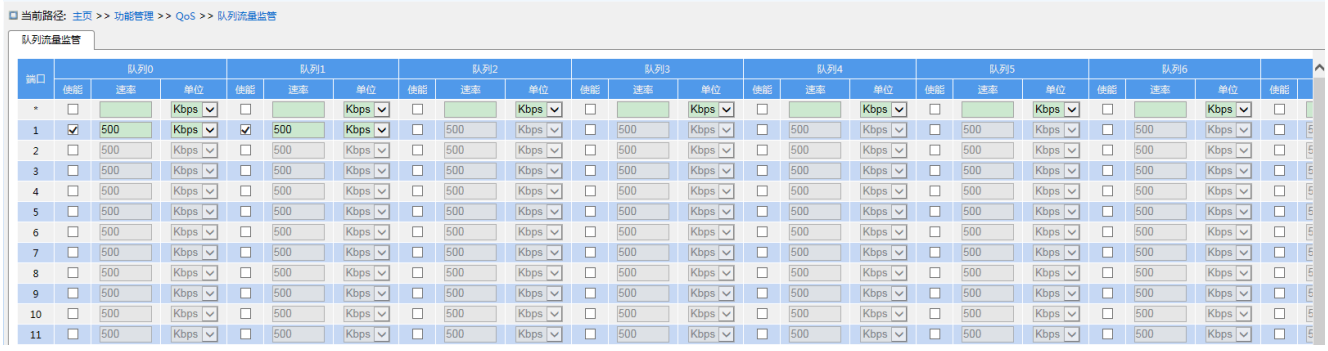


图 257 配置基于队列的流量监管

使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能队列的流量监管。使能队列的流量监管后，需要配置速率和单位参数。

速率、单位

配置范围：25~13128147kbps/ 1~13128Mbps

默认配置：500kbps

功能：对端口上队列接收的报文数据量进行限速，并将超过限定值的数据量丢弃。

11、配置端口队列调度模式及参数，如图 258 图 259 所示；

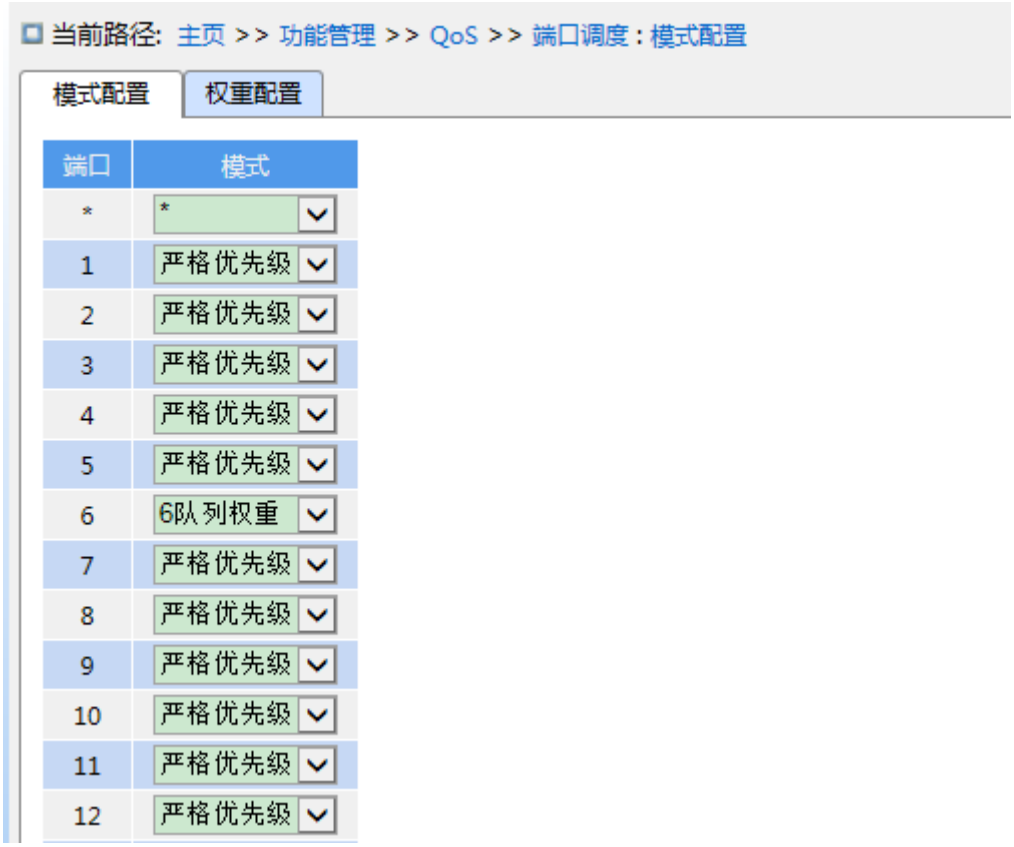


图 258 配置端口队列调度模式

端口	权重							
	队列0	队列1	队列2	队列3	队列4	队列5	队列6	队列7
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	20	40	40	20	20	20	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--

图 259 配置端口 wrr 调度模式权重值

调度模式

配置选项：严格优先级/2-8 队列权重

默认配置：严格优先级

功能：配置端口队列调度模式。

权重

配置范围：1~100

默认配置：17

功能：配置各队列的权重值。

12、配置基于端口的流量整形，如下图所示；

图 260 配置基于端口的流量整形

使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的流量整形。端口流量整形通过端口限速来实现。

速率、单位

配置范围：100~13107100kbps/ 1~13107Mbps

默认配置：500kbps

功能：对端口发送的报文数据量进行限速，并将超过限定值的数据量丢弃。

速率类型

配置选项：Line/Data

默认配置：Line

功能：指定整形限速值生效形式。Line 指对报文总长度限速，Data 指对报文有效长度限速。

13、配置基于队列的流量整形，如下图所示；

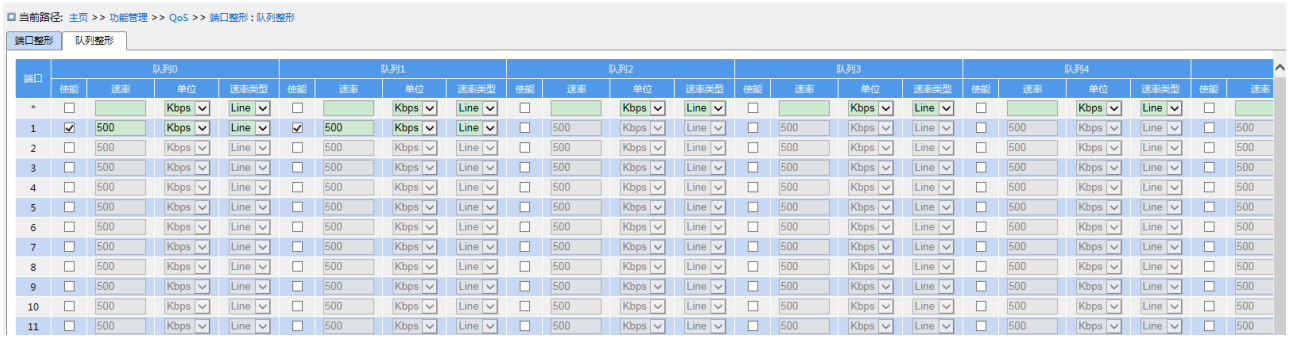


图 261 配置基于队列的流量整形

使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能队列的流量整形。

速率、单位

配置范围：100~13107100kbps/ 1~13107Mbps

默认配置：500kbps

功能：对端口上队列发送的报文数据量进行限速，并将超过限定值的数据量丢弃。

速率类型

配置选项：Line/Data

默认配置：Line

功能：指定整形限速值生效形式。Line 指对报文总长度限速，Data 指对报文有效长度限速。

7.15.4 典型配置举例

如图 262 所示，port1~port4 向 port5 转发报文，其中：

port1 接收的报文为 Untag 报文，进入 port1 的报文映射到队列 2 中；

port2 接收的报文中 PCP 值为 0，DEI 值为 1，进入 port2 的报文映射到队列 3 中；

port3 接收的报文中 DSCP 值为 4，进入 port3 的报文映射到队列 6 中；

port4 接收的所有源 MAC 地址为 00-00-00-00-00-23 的报文映射到队列 5 中，并且将这些报文的 DSCP 值改为 9 进行转发；

port5 接收的报文中 DSCP 值为 5，进入 port5 的报文映射到队列 2 中；

port6 采用 SP+WRR 调度模式。

交换机配置过程：

1、配置端口 1 的 CoS 值为 2，见图 240；

2、使能端口 2 的 Tag 分级，并且配置（PCP=0, DEI=1）映射到 CoS=3，如图 241；

3、使能端口 3 和端口 5 的基于 DSCP，如图 246；

4、选择信任 DSCP 值 4 和 5，并配置 DSCP 值 4 和 5 分别映射到队列 6 和队列 2 中，如图 248 所示；

5、端口 4 配置 QCL 表项，源 MAC 地址 00-00-00-00-00-23，表项动作 CoS 值为 5，DSCP 值为 9，如图 257 所示；

6、配置端口 6 出队列模式为 6 Queues Weighted，Q0~Q5 的权重值为 20、40、40、20、20、20，见图 258 图 259；

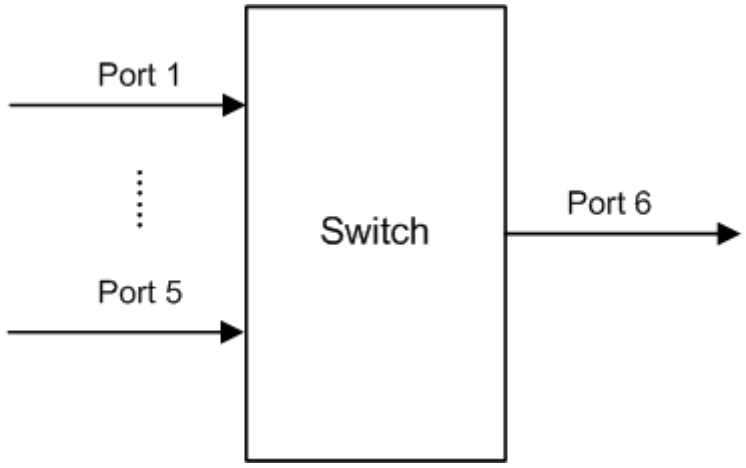


图 262 QoS 配置举例

port1 和 port5 的报文都入队列 2，port2 的报文入队列 3，port3 的报文入队列 6，port4 的报文入队列 5。

队列 6 和队列 7 使用 Strict Priority 调度模式，队列 0~队列 5 使用 WRR 调度模式。优先处理队列 6 中的数据，当队列队列 6 为空时，按照权重比调度队列 0~队列 5 中的数据。

权重值为 20、40、40、20、20、20。队列 2 的报文分配的带宽比例为：40/（20+40+40+20+20+20）=25%，队列 3 报文分配的带宽比例为：20/（20+40+40+20+20+20）=13%，入队列 5 报文分配的带宽比例为：20/（20+40+40+20+20+20）=13%。其中 port1 和 port5 的报文都入队列 2，所以只能按照先进先出的方式转发，但肯定的是 port1 和 port5 的总带宽比例一定是 25%。

8 环路保护配置

8.1 介绍

端口使能环路检测后，通过此端口发送环路检测报文来判断该端口连接的网络中是否存在环路。CPU 周期性向端口发送环路检测报文，如果该设备任意端口接收到环路检测报文，说明网络中有环路存在，此时将发送环路检测报文的端口关闭，一段时间后自动打开该端口继续检测。其中，发送环路检测报文的时间间隔和端口恢复时间均可在软件中配置。

说明：

环路检测与 DT-Ring、DRP、RSTP、MSTP 功能互斥，即使能环路检测的端口不能配置为冗余端口；冗余端口不能使能环路检测功能。

8.2 Web 页面配置

1、配置端口环路检测功能，如图 263 所示；

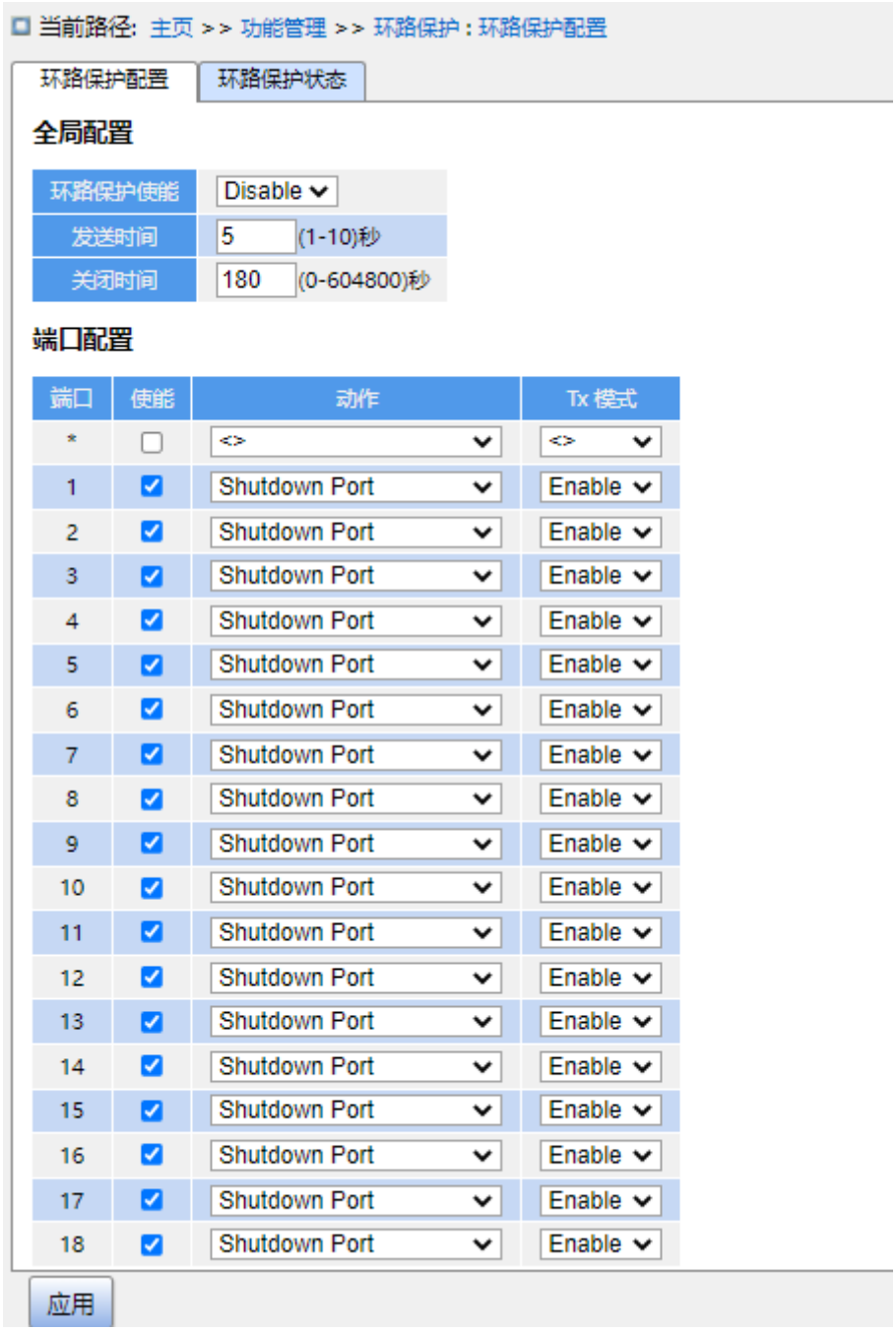


图 263 使能端口环路检测

使能环路保护

配置选项：Disable/Enable

默认配置：Disable

功能：是否使能全局环路保护功能。

发送时间

配置范围：1~10s

默认配置：5s

功能：配置发送环路检测报文的时间间隔。

关闭时间

配置范围：0~604800s

默认配置：180s

功能：配置端口关闭后自动恢复的时间间隔，0 表示端口关闭后将不自动恢复直到设备重启。

使能

配置选项：使能/不使能

默认配置：使能

功能：是否使能端口的环路检测功能。

动作

配置选项：Shutdown Port/ Shutdown Port and Log/Log Only

默认配置：Shutdown Port

功能：端口检测到有环路存在时执行的动作。

Tx 模式

配置选项：Disable/Enable

默认配置：Enable

功能：配置端口是否发送环路检测报文。

注意：

只有全局使能环路保护、端口使能环路保护、端口使能 Tx 模式后，端口才能准确检测环路。

2、环路保护状态，如图 264 所示；

端口	动作	发送	环路次数	状态	环路	最后一次环路时间
1	Shutdown	Enabled	0	Down	--	--
2	Shutdown	Enabled	0	Down	--	--
3	Shutdown	Enabled	0	Down	--	--
4	Shutdown	Enabled	0	Down	--	--
5	Shutdown	Enabled	0	Down	--	--
6	Shutdown	Enabled	0	Down	--	--
7	Shutdown	Enabled	0	Down	--	--
8	Shutdown	Enabled	0	Down	--	--
9	Shutdown	Enabled	0	Down	--	--
10	Shutdown	Enabled	0	Down	--	--
11	Shutdown	Enabled	0	Down	--	--
12	Shutdown	Enabled	0	Down	--	--

图 264 查看环路保护状态

环路

显示选项：--/Loop

功能：显示使能环路检测功能的端口所在网络中是否存在环路。Loop 说明存在环路；--说明不存在环路。

8.3 典型配置举例

组网需求：

交换机端口3与外部网络相连，当网络中有环路存在时，将端口3关闭，如图 265所示。

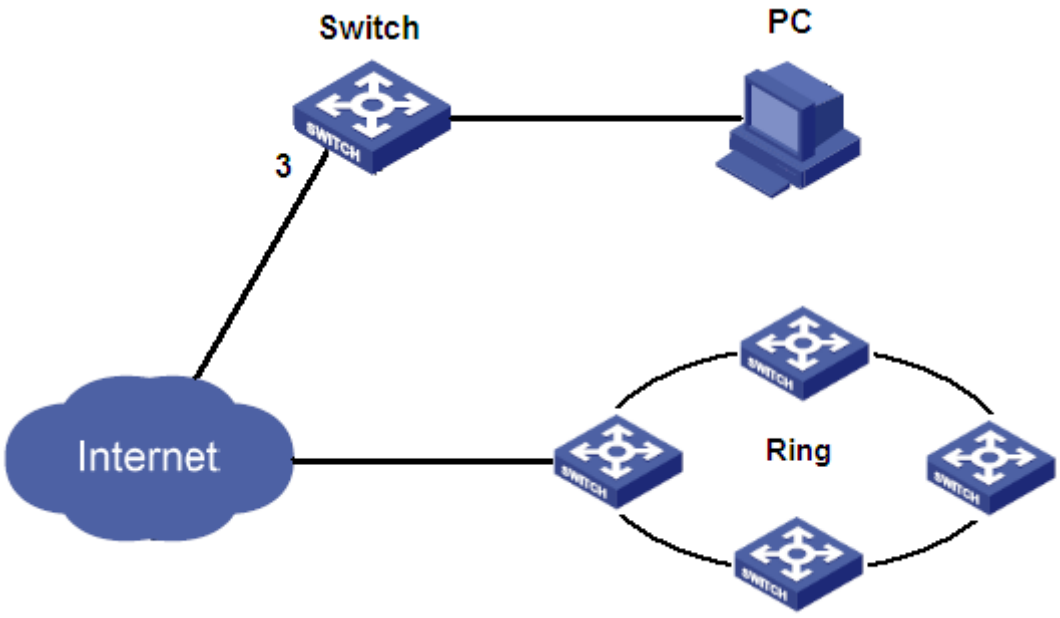


图 265 环路保护配置举例

具体配置：

使能端口 3 的环路检测功能，如图 263 所示。

9 TSN

9.1.1 介绍

TSN（Time Sensitive Networking）指在传统以太网基础上，使用精确的时间同步，通过保障带宽来限制传输延迟，提供高级别服务质量以支持各种工业应用的一种实时性网络。

9.1.2 原理

1）时间同步

时间敏感网络交换机应符合IEEE 1588v2中PTP精确时钟同步协议相关要求，宜符合IEEE 802.1AS 中PTP广义精确时钟同步协议要求。时间敏感网络交换机应支持本地时钟源和TOD时钟源两种时钟源，并且支持针对TOD时钟源配置时间等级与时间精度。

时间敏感网络交换机支持发送、接收并识别Announce报文中的时钟优先级、时钟等级、时钟精度等参数，支持通过BMC算法动态选举最优时钟；通过事件消息报文及通用消息报文进行频率同步、延时测量及时钟同步计算。

同步精度不得大于最小的调度周期和门控周期的精度，并保证同步精度至少在1us之内，宜保证100ns。

2）流量调度

时间敏感网络交换机应符合IEEE802.1Qbv中门控调度机制对下行队列进行流量调度，通过配置同时对每一队列门控进行打开和关闭，当队列处于关闭状态时，进入该队列的报文应存放在缓冲区，不应进入发送端口；当队列处于打开状态时，进入该队列的报文应正常发送。

时间敏感网络交换机宜符合IEEE802.1Qbu以及IEEE802.3br中报文抢占机制的相关规定，将接收到的报文按照优先级标记为可被抢占和抢占帧，实现进入抢占帧MAC（Preemptable MAC）的可被抢占帧的传输过程可被进入快速帧MAC（express MAC）通道的抢占帧打断。

时间敏感网络交换机宜符合 IEEE802.1QCi 中流过滤和监管机制的相关规定，通过 MAC 地址、VLAN、优先级等标识特定的数据流，在队列入口端处进行流过滤和监管，依据端口及时间窗配置流过滤配置模板，保证标记报文在正确的时间片和端口进行传送。

3）管理功能

时间敏感网络交换机应符合IETF RFC6241、RFC6242中规定的NETCONF协议，并必须实现NETCONF所有操作及Yang模型。

9.1.3 Web 页面配置

1、PTP 检查，如下图所示；

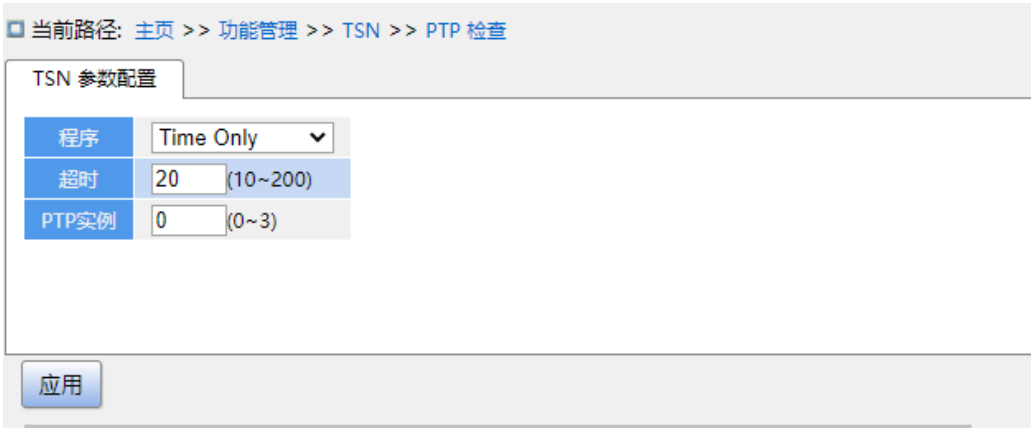


图 266 PTP 检查

程序

配置范围：Tim Only/Time And PTP

功能：选择 PTP 状态。

超时

配置范围：10-200（s）

功能： TSN 功能引用 ptp 时钟前，需要根据配置的程序模式检查是否经过这个配置的超时时间。

PTP 实例

配置范围：0-3

功能：可配置 0-3 个 PTP 实例。

2、帧抢占配置，如下图所示；

图 267 帧抢占配置

端口

功能：同一行中包含的设置的逻辑端口。

帧抢占 TX

功能：端口的 802.3br aMACMergeEnableTx 参数的值。该值确定在传输方向的 MAC 合并子层中是启用 (TRUE) 还是禁用 (FALSE) 帧抢占。

无 LLDP 启动

功能：如果选中此字段，则在选中 Frame Preemption TX 时 Frame Preemption 将被激活。

验证禁用 TX

功能：端口的 802.3br aMACMergeVerifyDisableTx 参数的值。该值确定在发送方向的 MAC 合并子层中验证功能是禁用 (TRUE) 还是启用 (FALSE)。

可抢占队列 TX

功能：该参数是优先级抢占状态的管理值。如果选中，则如果为优先级排队的帧将使用端口的可抢占服务传输，则它具有可抢占值。如果未选中，如果为优先级排队的帧将使用端口的 express 服务传输并且为端口启用抢占，则取值 express。

3、TAS 参数配置，如下图所示；

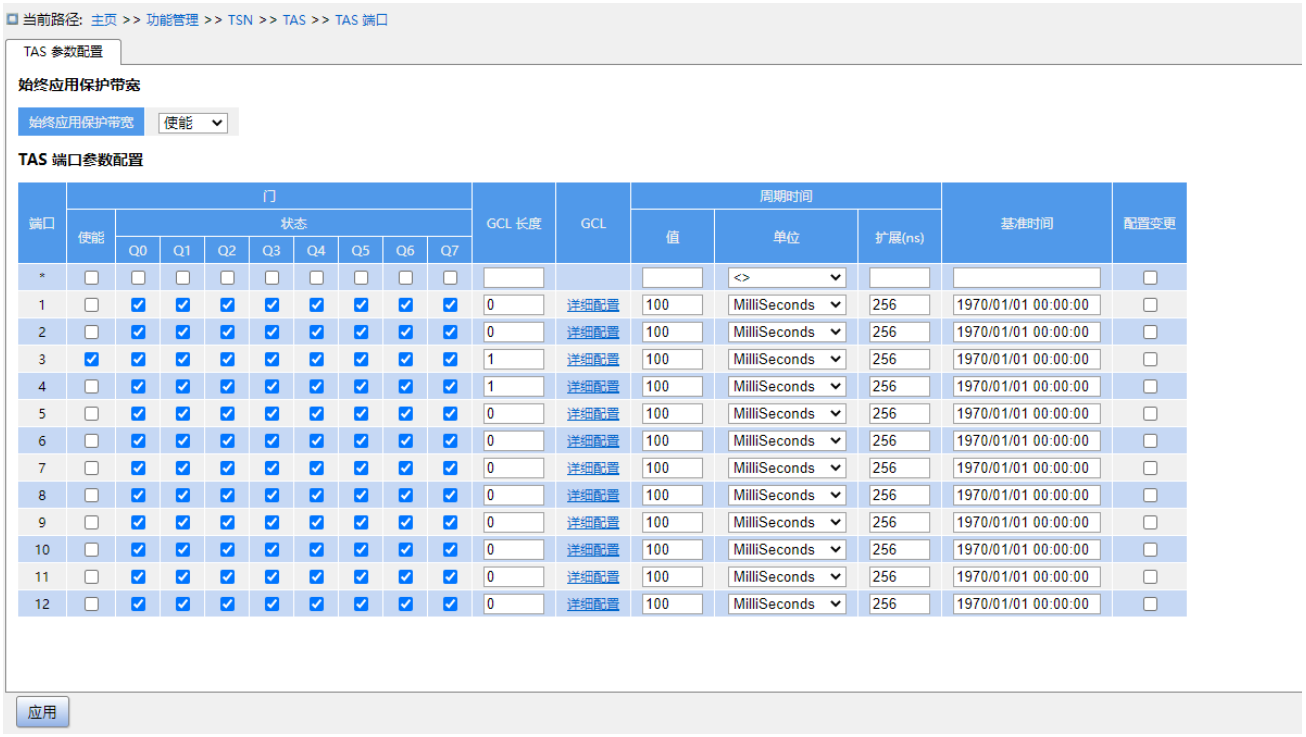


图 268 TAS 参数配置

始终应用保护带宽

功能：是否使能始终应用保护带宽。禁用：为非计划队列到计划队列的转换实施保护带宽。已启用：为任何队列到计划队列的转换实施保护带宽。

端口

功能：交换机的端口号。

门状态

功能：启动参数确定流量调度是活动的 (true) 还是非活动的 (false)。门状态：当端口上没有 GCL 处于活动状态时使用的端口打开状态的初始值。

GCL 长度

配置范围：0- 256

功能：端口的门控列表长度参数的管理值。整数值表示 AdminControlList 中的条目 (TLV) 数。如果您更改该值，请在通过按 GCL 链接配置 GateControlList 之前按保存按钮。

周期

配置范围：0- 999999999

功能：端口门控周期的管理值。Admin Cycle Time 变量是有理数秒，由值和单位定义。周期时间值：AdminCycleTime 由 Unit 字段中定义的单位上的此数字定义。周期时间单位：AdminCycleTime 单位。可以是 milliseconds、microseconds 或 nanoseconds。周期时间扩展：整数纳秒，定义安装新周期配置时允许延长端口门控周期的最长时间。

基准时间

功能：基准时间的 Admin 值，表示为 IEEE 1588 精确时间协议 (PTP) 时间刻度。

配置更改

功能：是否使能配置变更。

4、Gi 1/1 GCL 配置，如下图所示；

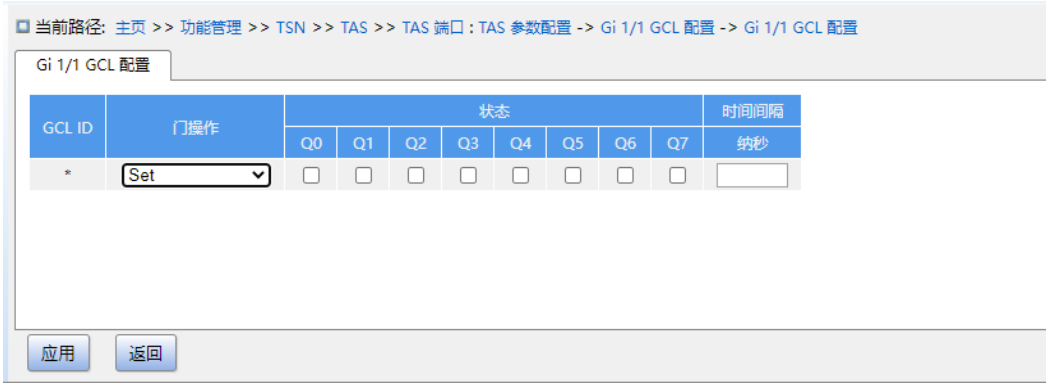


图 269 Gi 1/1 GCL 配置

GCL ID

描述：门控列表索引。

门操作

配置范围：Set、SetAndRelease 或 SetAndHold

功能：操作可以是 Set、SetAndRelease 或 SetAndHold。IEEE802.1Q 表 8.7 详细解释了 SetAndRelease 和 SetAndHold 选项如何影响支持帧抢占时的行为。如果不支持帧抢占，则所有选项都表现为 Set。

门状态

描述：门状态为每个队列配置在给定时间间隔内是打开还是关闭。

时间间隔

配置范围：0-周期时间，所有 GCL ID 对应的时间间隔总和小于周期时间。

描述：时间间隔以纳秒数指定。

5、TAS SDU 配置，如下图所示；

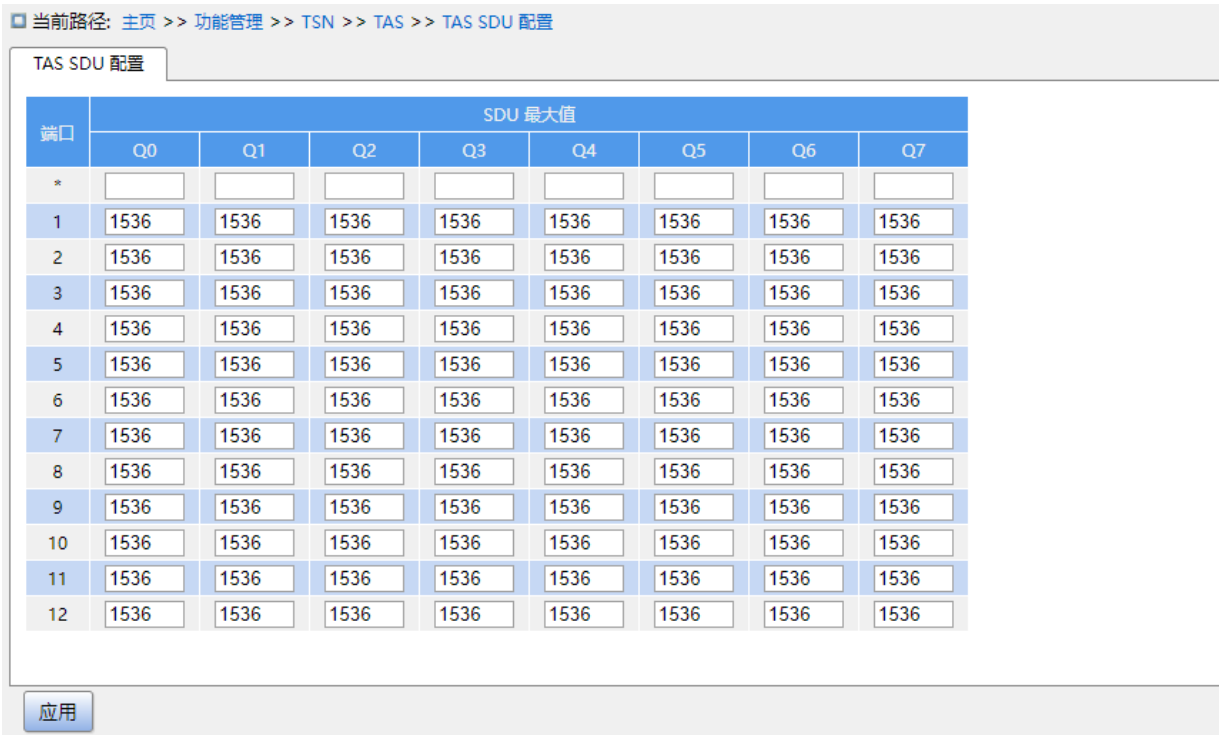


图 270 TAS SDU 配置

端口

功能：交换机的端口号。

SDU 最大值

配置范围：SDU 最大值必须是 64- 10240 范围内的数字,或者 0!

功能：端口支持的流量类别的 SDU 最大值。此值表示为无符号整数。值 0 被解释为底层 MAC 支持的最大 SDU 大小。

6、流量计配置，如下图所示；

图 271 流量计配置

FMI ID

配置范围：0- 1022

功能：参数是流量计表的索引。

CIR

配置范围：0- 4294967295

描述：承诺信息速率，表示向 C 桶（单桶模式中只有一个令牌桶，称为 C 桶）中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率。

CBS

配置范围：0- 4294967295

描述：承诺突发尺寸，表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量。

EIR

配置范围：0- 4294967295

功能：额外信息速率。

EBS

配置范围：0- 4294967295

描述：超额突发尺寸，表示 E 桶的容量，即 E 桶瞬间能够通过的超出突发流量。

CF

配置选项：0/1

描述：耦合标志(CF)的值为 0 或者 1。CF 值的选择会影响到进入网络的黄色业务帧的数量。CF 为 O，允许进入网络的黄色业务帧的长期平均比特率受到 EIR 的限制，CF 为 1，允许进入供应商网络的黄色业务帧的长期平均比特率受到 CIR+EIR 的限制。在这两种情况下，允许进入供应商网络的黄色业务帧的突发尺寸受到 EBS 的限制。

CM

配置选项：ColorBlind/ColorAware

功能：在 ColorBlindUNI 中，该算法会忽略任何用户可能已经在他们的业务帧中标记的颜色指示。例如，用户帧可能会通过 IEEE802．1Q 标记中的用户优先级比特(802．1p)来标记用户帧。在 MEF 中是指 CE—VLANCoS 比特。在 ColorAwareUNI 中，该算法会利用用户在他们的业务帧上标记的颜色来决定对业务帧进行的操作。例如，企业网会利用 IP 的 DiffServ 结构在他们的网络中提供 QoS。通过差分服务代码点(DSCP)对他们的 IP 包进行标记来指示

包的颜色和业务类别(CoS)。CE 设备将 DSCP 指示的颜色和 CoS 映射为业务帧的 CE-VLANCoS(802．1p)值然后传递到供应商的网络，在供应商的网络中，根据网络情况，会对不同的业务帧进行不同的处理，如在遇到网络拥塞的时候，优先丢弃黄色的业务帧。该算法根据这些预先标记的颜色信息来决定速率执行的决定。

标记红色帧

功能：是启用还是禁用。如果报文已被标记为红色，则令牌桶直接将到达报文标记为红色。

丢弃黄色帧

功能：如果报文已被标记为黄色，则令牌桶根据报文长度和令牌数的大小，为符合流量规定的报文标记为黄色，为不符合的报文标记为红色。

7、流过滤器配置，如下图所示，

图 272 流过滤器配置

SFI ID

配置范围：1-1022

功能：SFI 参数是 SFT 的索引。

流 ID

配置范围：0-127

功能：流标识符值。

优先级规格

配置范围：优先级规范值。值 -1 表示通配符值；零或正值表示优先级值。

SGI ID

功能：SGI 条目索引。

SDU 大小

功能：最大 SDU 大小参数指定流的最大允许帧大小。任何超过此值的帧都将被丢弃。值 0 表示对此流禁用了最大 SDU 大小过滤器。

FMI ID

功能：FlowMeterInstanceID 参数包含流量计表中条目的索引。值 -1 表示未分配流量计；零或正值表示流量计 ID。

超大块使能

功能：StreamBlockedDueToOversizeFrameEnable 对象包含一个布尔值，指示 StreamBlockedDueToOversizeFrame 函数是启用 (TRUE) 还是禁用 (FALSE)。

8、流门，如下图所示；

图 273 流门

SGI ID

配置范围：0- 1022

描述：流门实例参数是流门表的索引。

门

使能：参数确定流门是活动的还是非活动的。门状态：open 值表示门是打开的，close 值表示门是关闭的。

周期时间

单位配置选项：ms/us/ns

扩展范围：0- 1022

功能：门的周期时间延长参数的管理值。该值是一个无符号整数纳秒。

基准时间

功能：门的基准时间参数的管理值。该值是 PTP 时间值的表示形式，由 48 位整数秒数和 32 位整数纳秒数组成。当前时间：以 PTP 时间为单位，由本地系统维护。该值是 PTPtime 值的表示形式，由 48 位整数秒数和 32 位整数纳秒数组成。

Admin IPV

配置范围：0-7

功能：门的 IPV 参数的管理值。

GCL 长度

配置范围：0- 1022

功能：门控制列表中的条目数。

使能关门原由

功能：收到无效数据：指示在收到无效数据时是否关闭门。字节：指示如果收到太多八位字节，是否关闭门。

配置变更

功能：在设置为 TRUE 时表示门的配置更改开始。只有当各种管理参数都设置为适当的值时，才应该这样做。

9、GCL 配置，如下图所示；

图 274 GCL 配置

SGI ID

描述：流门实例。

GCL ID

描述：门控列表索引。

GCL 参数-状态

功能：流门指定所需的状态，Open 或 Closed。

GCL 参数-IPV

功能：IPV 被编码为有符号整数。表示内部优先级值。

GCL 参数-时间间隔

描述：时间间隔 以 4 个八位字节编码为 32 位无符号整数，表示纳秒数。

GCL 参数-八位字节最大值

功能：门允许在时间片内能够通过的最大字节数，有效范围是 0-4294967295。

10、流配置，如图所示；

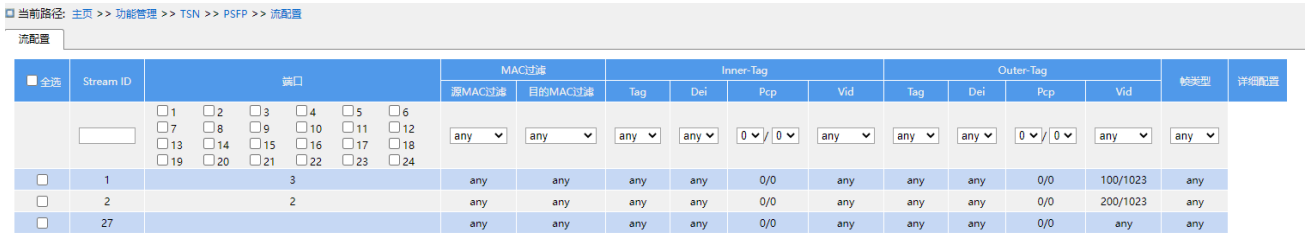


图 275 流配置

Stream ID

配置范围：1-127

功能：可配置的流 ID.

端口

配置范围：交换机上所有端口。

功能：选择流在交换机上的端口。

11、流门状态,如下图所示；

图 276 流门状态

SGI 标识

功能：流门实例参数是流门表的索引。

门

功能：使能：参数确定流门是活动还是非活动的门状态：流门的 open 值表示门是打开的，close 值表示门是关闭的。

周期时间

功能：可以是 milliseconds、microseconds 或 nanoseconds。

周期时间延长

功能：整数纳秒，定义安装新周期配置时允许延长端口门控周期的最长时间。

时间

功能：基准时间：门的基准时间参数的管理值。该值是 PTP 时间值的表示形式，由 48 位整数秒数和 32 位整数纳秒数组成。当前时间：以 PTP 时间为单位，由本地系统维护。该值是 PTPtime 值的表示形式，由 48 位整数秒数和 32 位整数纳秒数组成。

配置变更

功能：配置更改时间：计划发生下一次配置更改的 PTP 时间。该值是 PTP 时间值的表示形式，由 48 位整数秒数和 32 位整数纳秒数组成。

配置更改错误：已请求重新配置交通计划但旧计划仍在运行且所请求的基准时间已过去的次数的计数器。

Tick 间隔

功能：循环时间时钟的粒度，表示为无符号数的十分之一纳秒。

配置待定

功能：状态机变量的值。如果配置更改正在进行但尚未完成，则该值为 TRUE。

RX

功能：收到无效数据。

Octets

功能：八位字节溢出。

12、流过滤器状态，如下图所示；

图 277 流过滤器状态

SFI ID

功能：流过滤器实例的 ID。

由于帧过大而阻塞

功能：如果过滤器由于帧过大而被阻塞，则为 true，否则为 false。

13、流过滤器统计参数，如下图所示；

图 278 流过滤器统计

SFI ID

功能：支持的最大流过滤器 ID。

匹配到帧计数

功能：计数器对匹配此流过滤器的接收帧进行计数。

通过帧计数

功能：计数器对通过与此流过滤器关联的门的接收帧进行计数。

未通过帧计数

功能：计数器对未通过与此流过滤器关联的门的接收帧进行计数。

通过 SDU 计数

功能：计数器对通过与此流过滤器关联的 SDU 大小过滤器规范的接收帧进行计数。

未通过 SDU 计数

功能：计数器对未通过与此流过滤器关联的 SDU 大小过滤器规范的接收帧进行计数。

RED 帧计数

功能：计数器对接收到的与此流过滤器关联的随机早期检测 (RED) 帧进行计数。

14、FRER 配置，如下图所示；

图 279 FRER 配置

Instance(1-127)

配置范围：1-27

描述：

模式

配置范围：Generation/Recovery

功能：决定此 FRER 实例是否应在生成模式或恢复模式下运行。

使能

描述：FRER 实例启用或禁用。

入口流列表

配置范围：1- 127

功能：选择应映射到此 FRER 实例的入口流。在生成器模式下只能指定一个流 ID。

FRER VLAN

配置范围：

功能：入口流分类到的 VLAN ID。

出口端口列表

配置范围：交换机上所有端口

功能：选择此 FRER 实例将命中的出口端口。

算法

配置范围：Vector/Match

功能：IEEE 802.1CB-2017 要求实现提供两种不同的恢复函数算法，匹配和向量。

历史长度

默认配置：2

功能：矢量算法的历史长度。

复位超时

默认配置：1000

功能：复位恢复功能超时。

Take-no-sequence

功能：如果为真，则接受所有帧，无论它们是否带有 R 标记。

Individua

功能：使用个人恢复。单独恢复是指成员流在达到复合恢复功能之前进行恢复。复合恢复功能位于 FRER 实例中的每个出口端口上。单个恢复可以做而复合恢复不能做的唯一一件事是过滤掉由于发送器缺陷而保持呈现相同 R-tag 序列号的成员流。

Terminate

功能：从帧中剥离 R-Tag，然后再将其呈现在出口上。

使能

功能：启用/禁用潜在错误检测。

Error Diff

配置范围：0- 10000000

功能：潜在错误检测误差差异。

周期

配置范围：1000- 86400000

功能：潜在错误检测周期。

路径

默认配置范围：30000

功能：潜在错误检测路径。

重置期

潜在错误检测复位周期。

15、FRER 状态，如下图所示；

图 280 FRER 状态

操作

描述：FRER 实例的运行状态。

警告

描述：FRER 实例的操作警告。

潜在错误

描述：发现的潜在错误。

统计

功能：检查以重置统计计数器。

重置功能

功能：单击清除功能重置。如果此 FRER 实例处于生成模式，则用于重置序列生成器的序列号。如果此 FRER 实例处于恢复模式，则用于重置恢复功能。它重置了可能的单个恢复功能和复合恢复功能。

重置潜在错误

功能：清除潜在错误。

16、FRER 统计，如下图所示；

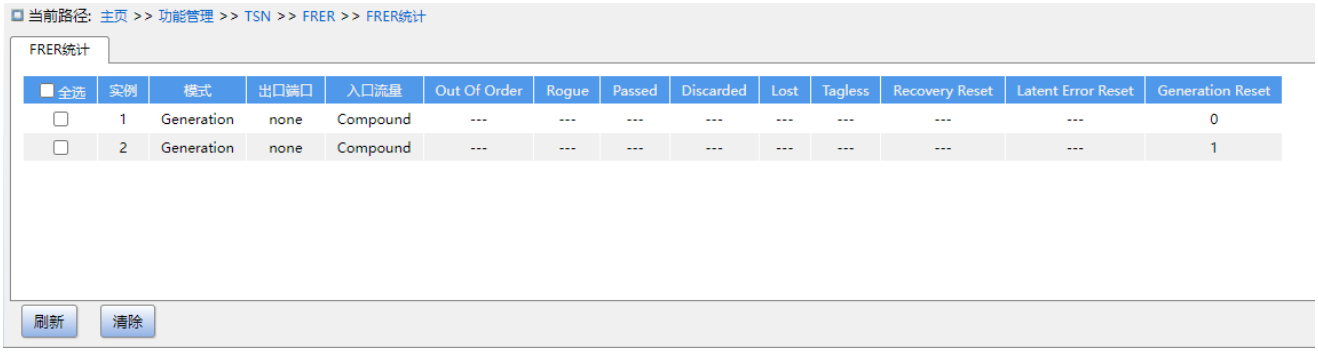


图 281 FRER 统计

实例

功能：FRER 实例 ID。

模式

配置范围：Generation/ Recovery

出口端口

功能：出口端口号列表。

入口流

功能：入口流 ID 列表。

Out of order

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyOutOfOrderPackets。

Rogue

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyRoguePackets。

Passed

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyPassedPackets。

Discarded

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyDiscardedPackets。

Lost

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyLostPackets。

Tagless

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyTaglessPackets。

Recovery resets

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyResets。

Latent error resets

功能：IEEE 802.1CB-2017：frerCpsSeqRcvyLatentErrorResets。

Generation resets

功能：IEEE 802.1CB-2017：frerCpsSeqGenResets。

10 NETCONF 配置

10.1.1 介绍

随着网络规模的增大，复杂性的增加，传统的简单网络管理协议 SNMP 的简单管理模式已经不能适应当前复杂网络的管理，特别是不能满足配置管理需求，为了弥补 SNMP 的缺陷，NETCONF 协议应运而生。

10.1.2 原理

NETCONF（Network Configuration Protocol，网络配置协议）是一种基于 XML 的网络管理协议，并使用简单的基于 RPC（Renote Procedure Call）机制实现客户端和服务器之间的通信， 它提供了一种可编程的、对网络设备进行配置和管理的方法。用户可以通过该协议设置参数、获取 参数值、获取统计信息等。

NETCONF 报文使用 XML 格式，具有强大的过滤能力，而且每一个数据项都有一个固定的元素名 称和位置，这使得同一厂商的不同设备具有相同的访问方式和结果呈现方式，不同厂商之间的设备 也可以经过映射 XML 得到相同的效果，这使得它在第三方软件的开发上非常便利，很容易开发出 在混合不同厂商、不同设备的环境下的特殊定制的网管软件。在这样的网管软件的协助下，使用 NETCONF 功能会使网络设备的配置管理工作，变得更简单更高效

10.1.3 Web 页面配置

1、使能 NETCONF 功能，如下图所示;

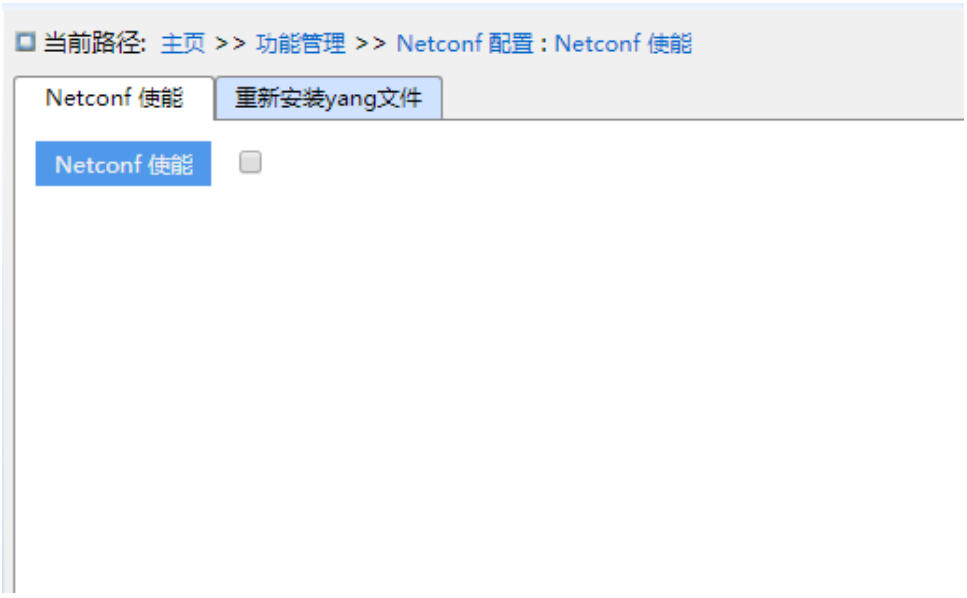


图 282 NETCONF 功能

2、重新加载 yang 文件

如设备上 yang 文件有修改时，需要重新加载 yang 文件，该功能需要在 NETCONF 去使能的情况下使用，如下图所示;

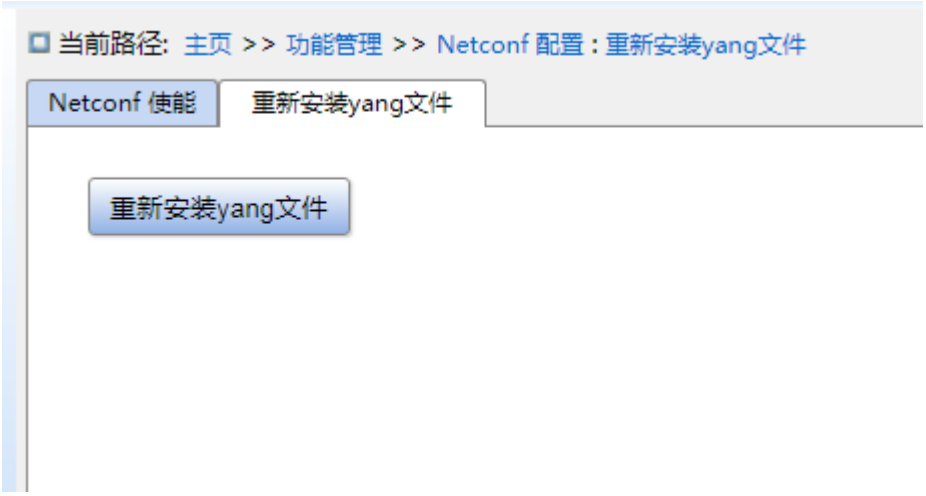


图 283 重新安装 yang 文件

11 诊断

11.1 日志

11.1.1 介绍

交换机的日志功能主要记录交换机系统的状态变化、故障、调试、异常、用户操作等信息，便于查找故障，通过配置可以实时上传日志信息到支持 Syslog 协议的服务器。

日志记录的消息包括：各种告警信息、广播风暴、重启、内存及用户操作信息。

11.1.2 Web 页面配置

1、配置系统日志，如下图所示；

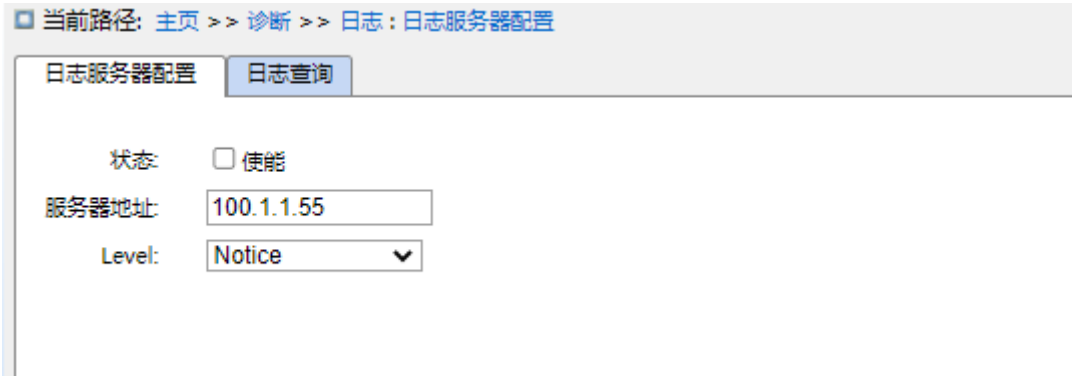


图 284 配置日志服务器

状态

配置选项：使能/ 不使能

默认配置：不使能

功能：是否使能日志服务器。

服务器地址：

配置格式：A.B.C.D

功能：配置日志服务器 IP 地址。

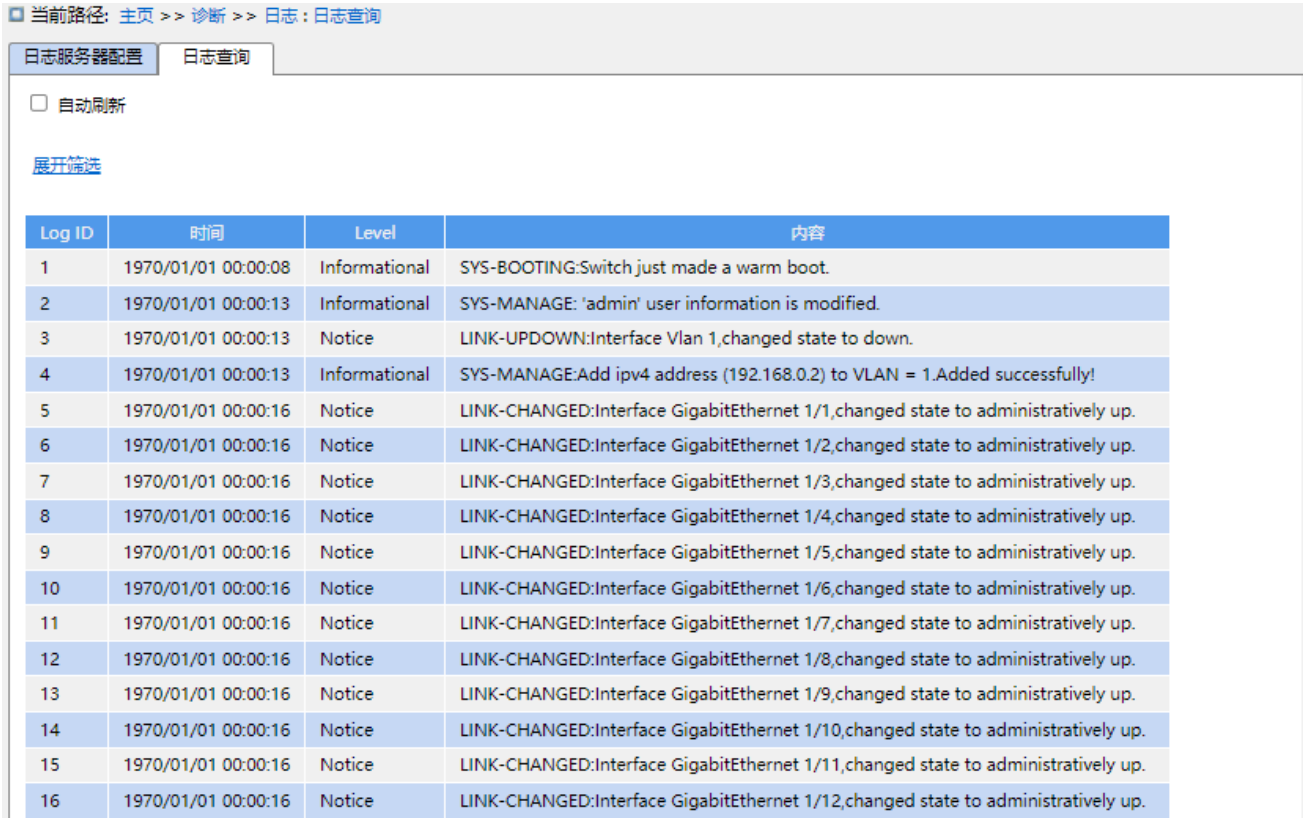
Level

配置选项：Error/Warning/Notice

默认配置：Informational

功能：选择显示的日志信息等级。

2、日志查询，如下图所示；



Log ID	时间	Level	内容
1	1970/01/01 00:00:08	Informational	SYS-BOOTING:Switch just made a warm boot.
2	1970/01/01 00:00:13	Informational	SYS-MANAGE: 'admin' user information is modified.
3	1970/01/01 00:00:13	Notice	LINK-UPDOWN:Interface Vlan 1,changed state to down.
4	1970/01/01 00:00:13	Informational	SYS-MANAGE:Add ipv4 address (192.168.0.2) to VLAN = 1.Added successfully!
5	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/1,changed state to administratively up.
6	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/2,changed state to administratively up.
7	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/3,changed state to administratively up.
8	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/4,changed state to administratively up.
9	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/5,changed state to administratively up.
10	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/6,changed state to administratively up.
11	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/7,changed state to administratively up.
12	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/8,changed state to administratively up.
13	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/9,changed state to administratively up.
14	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/10,changed state to administratively up.
15	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/11,changed state to administratively up.
16	1970/01/01 00:00:16	Notice	LINK-CHANGED:Interface GigabitEthernet 1/12,changed state to administratively up.

图 285 日志查询

自动刷新

配置选项：勾选/不勾选

默认配置：不勾选

功能：是否使能自动刷新功能

Log ID

配置选项：*/>=/<=/选择范围

默认配置：*

功能：选择筛选的 Log ID，“*”为所有 ID 日志，“>=”为筛选大于等于某个 ID 的日志，“<=”为筛选小于等于某个 ID 的日志，“选择范围”可以手动输入某个 ID 范围内日志。

时间

配置选项：*/开始时间/结束时间/选择范围

默认配置：*

功能：选择筛选的时间范围，“*”为全部时间的日志，“开始时间”为日志的起始时间，“结束时间”为日志的结束时间，“选择范围”可以手动输入某个时间范围内日志。

Level

配置选项：*/>=/<=/选择范围

默认配置：*

功能：选择筛选等级范围，“*”为全部等级的日志，“>=”为刷选大于等于某个等级的日志，“<=”为刷选小于等于某个等级的日志，“选择范围”可以手动输入某个等级范围内日志，等级包括 Error，Warning，Notice，Informational。

内容

配置选项：*/包含/不包含

默认配置：*

功能：选择筛选内容，“*”为所有的日志，“包含”包含某些字段的的日志，“不包含”为排除某些字段的日志。

11.2 端口镜像

11.2.1 介绍

端口镜像指交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制端口称为镜像源端口，复制端口称为镜像目的端口，可以在镜像目的端口处连接一个协议分析仪或者 RMON 监测仪来监视和管理网络，并诊断网络故障。

11.2.2 说明

交换机最多支持 3 组镜像，每组镜像只支持一个镜像目的端口，镜像源端口则没有使用上的限制，可以是 1 个也可以是多个。

多个源端口可以在相同 VLAN 中也可以在不同 VLAN 中。目的端口和源端口可以在同一个 VLAN 中也可以在不同 VLAN 中。

源端口和目的端口不能是同一个端口。

注意：

目的端口应关闭动态 MAC 地址学习。

11.2.3 Web 页面配置

1、配置本地镜像，如下图所示；

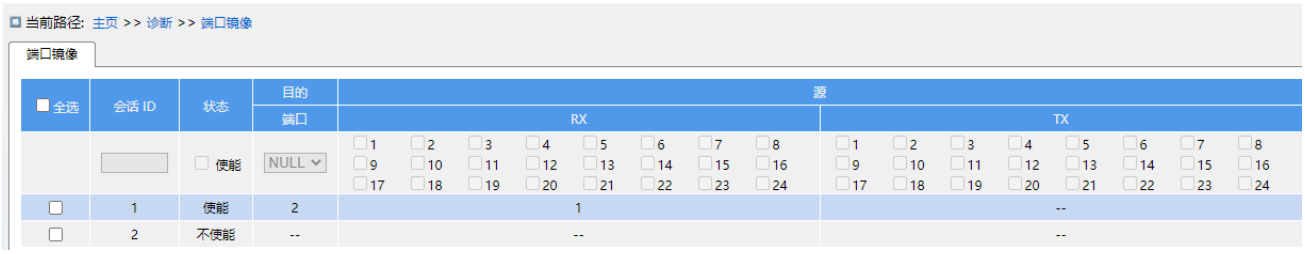


图 286 配置本地镜像功能

全选

配置选项：勾选/不勾选

默认配置：不勾选

功能：选中此镜像组才能进行编辑修改。

状态

配置选项：使能/不使能

功能：是否使能端口镜像功能。

目的端口

配置选项：NULL/设备端口号

默认配置：NULL

功能：选择镜像目的端口，只能有一个镜像目的端口。

Rx 配置选项：使能/不使能

默认配置：不使能

功能：是否对源端口接收的报文进行镜像。

Tx 配置选项：使能/不使能

默认配置：不使能

功能：是否对源端口发送的报文进行镜像。

11.2.4 典型配置举例

如图 287 所示，镜像目的端口为 2，镜像源端口为 1，1 端口接收和发送的所有报文都镜像到 2 端口。

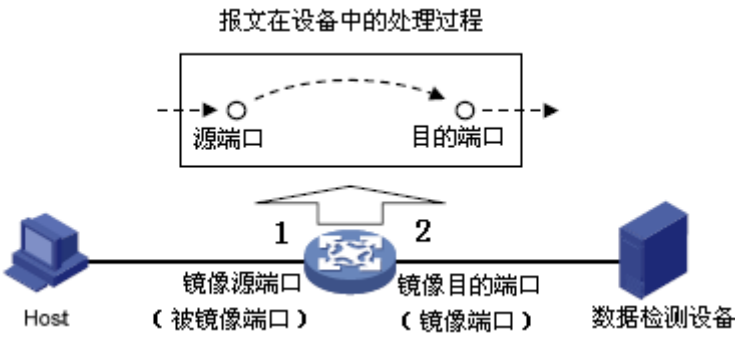


图 287 端口镜像举例

配置过程：

1、使能端口镜像功能，见图 286；

2、选择端口 2 作为镜像目的端口，端口 1 作为镜像源端口，镜像模式选择 Rx 和 Tx，见图 286。

11.3 LLDP 信息

11.3.1 介绍

LLDP（Link Layer Discovery Protocol，链路层发现协议）提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB 形式保存起来，以供网络管理系统查询及判断链路状况。

11.3.2 Web 页面配置

1、配置 LLDP，如下图所示；

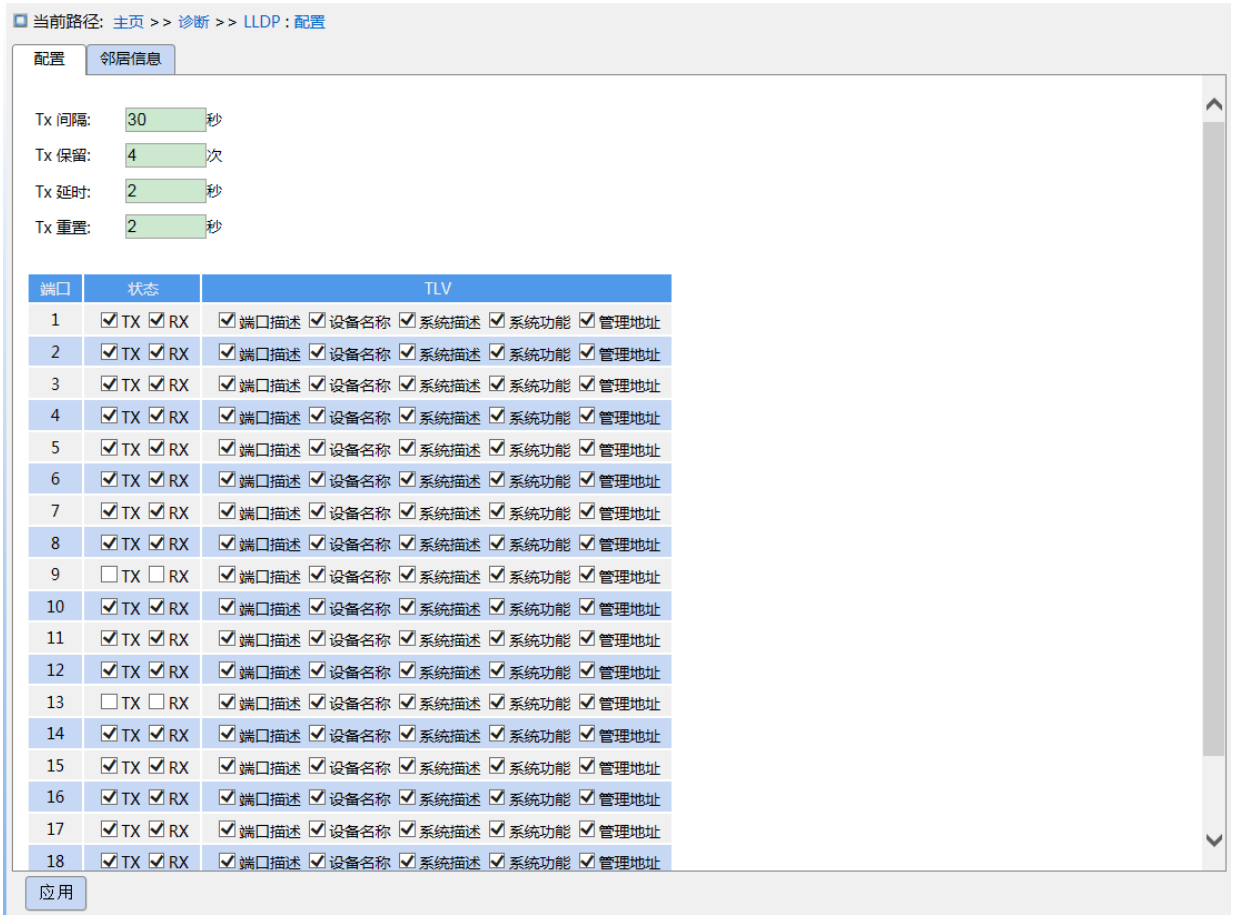


图 288 配置 LLDP 协议

Tx 间隔

配置范围：5~32768 秒

默认配置：30 秒

功能：配置周期性发送 LLDP 报文的时间间隔。

Tx 保留

配置范围：2~10 次

默认配置：4 次

功能：配置 Tx 保留次数。LLDP 报文的有效时间= Tx 间隔×Tx 保留。

Tx 延时

配置范围：1~8192 秒

默认配置：2 秒

功能：配置信息改变后，发送新 LLDP 报文与上次 LLDP 报文发送之间的时间间隔。Tx 延时时间不能超过 Tx 间隔的 1/4。

Tx 重置

配置范围：1~10 秒

默认配置：2 秒

功能：端口去使能 LLDP 或设备重启，会发送 LLDP shutdown 帧给邻居节点，告知之前的 LLDP 信息失效。Tx 重置时间指发送 LLDP shutdown 帧和重新初始化 LLDP 报文之间的时间间隔。

状态

配置选项：不使能/TX/RX/TX&RX

默认配置：TX&RX

功能：配置 LLDP 报文模式。使能 TX&RX 模式指交换机既发送 LLDP 报文，也接收并识别 LLDP 报文；不使能模式指交换机既不发送 LLDP 报文，也不接收 LLDP 报文；仅 Rx 模式指交换机只接收并识别 LLDP 报文，不发送 LLDP 报文；仅 Tx 模式指交换机只发送 LLDP 报文，不接收 LLDP 报文。

端口描述

配置选项：使能/不使能

默认配置：使能

功能：使能时，LLDP 报文会携带端口描述信息。

设备名称

配置选项：使能/不使能

默认配置：使能

功能：使能时，LLDP 报文会携带设备名称。

系统描述

配置选项：使能/不使能

默认配置：使能

功能：使能时，LLDP 报文会携带系统描述。

系统功能

配置选项：使能/不使能

默认配置：使能

功能：使能时，LLDP 报文会携带系统能力。

管理地址

配置选项：使能/不使能

默认配置：使能

功能：使能时，LLDP 报文会携带管理地址。

2、查看 LLDP 信息，如下图所示；

图 289 查看 LLDP 信息

注意：

显示 LLDP 信息的前提是相连接的设备都使能 LLDP 协议。

11.4 跟踪路由

Traceroute 可以让我们看到 IP 数据报从一台主机传到另一台主机所经过的路由。

1、配置 Traceroute 功能，如下图所示；

图 290 配置 Traceroute

目的地址

配置格式：A.B.C.D

功能：配置目的设备的 IP 地址。

超时时间

配置范围：1~10 秒

默认配置：2 秒

功能：配置超时时间，如果该时间值内发送方未收到接收方的响应报文，认为通信失败。

最大跳数

配置范围：1~255

默认配置：30

功能：测试数据包从发送设备到目的设备所经过的网关数目。

2、查看 Traceroute 命令输出信息，如下图所示；

图 291 查看输出

11.5 Ping

日常系统维护中，用户可以使用 ping 命令来检查指定地址的设备是否可达，测试网络连接是否出现故障。

1、配置 Ping 命令，如图 292 所示；

图 292 配置 ping 命令

服务器地址

配置格式：A.B.C.D

功能：配置目的设备的 IP 地址。

Ping 长度

配置范围：2~1452 字节

默认配置：56 字节

功能：指定发送 ICMP 请求报文的长度（不包括 IP 和 ICMP 报文头）。

Ping 数量

配置范围：1~60

默认配置：5

功能：指定发送 ICMP 请求报文的次数。

Ping 间隔

配置范围：0~30 秒

默认配置：0 秒

功能：指定发送 ICMP 请求报文的时间间隔。

2、查看 ping 命令输出信息，如图 293 所示；

图 293 查看 ping 结果

Ping 命令输出信息包括目的设备对每个 ICMP 请求报文的响应以及 ping 过程报文的统计信息。

11.6 IP Source Guard

11.6.1 介绍

通过 IP Source Guard 绑定功能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户IP 接入网络），提高了端口的安全性。

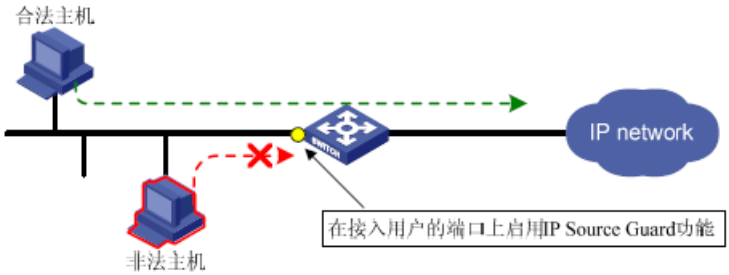


图 294 IP Source Guard 功能示意图

11.6.2 实现原理

配置了该特性的端口接收到报文后查找 IP Source Guard绑定表项，如果报文中的特征项与绑定表项中记录的特征项匹配，则端口转发该报文，否则做丢弃处理。绑定功能是针对端口

的，一个端口被绑定后，仅该端口被限制，其他端口不受该绑定影响。

IP Source Guard用于匹配报文的特征项包括：源IP地址、源MAC地址和VLAN标签。并且，可支持端口与如下特征项的组合（下文简称绑定表项）：

➢IP、MAC、IP＋MAC

➢IP＋VLAN、MAC＋VLAN、IP＋MAC＋VLAN

端口所支持绑定表项的种类与设备的型号有关，请以设备的实际情况为准。

IP Source Guard 按照绑定表项的产生方式分为静态绑定和动态绑定：

➢**静态绑定**：通过手工配置产生绑定表项来完成端口的控制功能，适用于局域网络中主机数较少或者需要为某台主机进行单独的绑定配置的情况；

➢**动态绑定**：通过自动获取 DHCP Snooping或DHCP Relay的绑定表项来完成端口控制功能，适用于局域网络中主机较多，并且采用DHCP进行动态主机配置的情况，可有效防止IP地址冲突、盗用等问题。其原理是每当DHCP为用户分配一条表项时，动态绑定功能就相应地增加一条绑定表项以允许该用户访问网络。如果某个用户私自设置IP地址，会由于没有触发DHCP分配表项，导致动态绑定功能未增加相应的访问允许规则，使得该用户不能访问网络。

8.6.3 Web 页面配置

1、使能 IP Source Guard 功能，如下图所示；

图 295 配置 IP Source Guard

模式

配置选项：使能/不使能

默认配置：不使能

功能：是否使能全局 IP Source Guard 功能。

2、配置端口 IP Source Guard 功能，如下图所示；

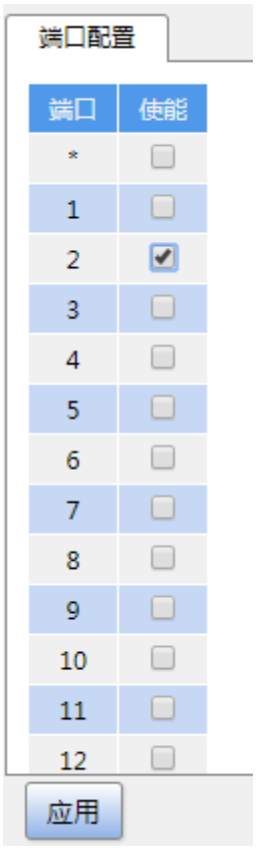


图 296 配置端口 IP Source Guard

使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口 IP Source Guard 功能。

3、配置静态绑定表，如下图所示；

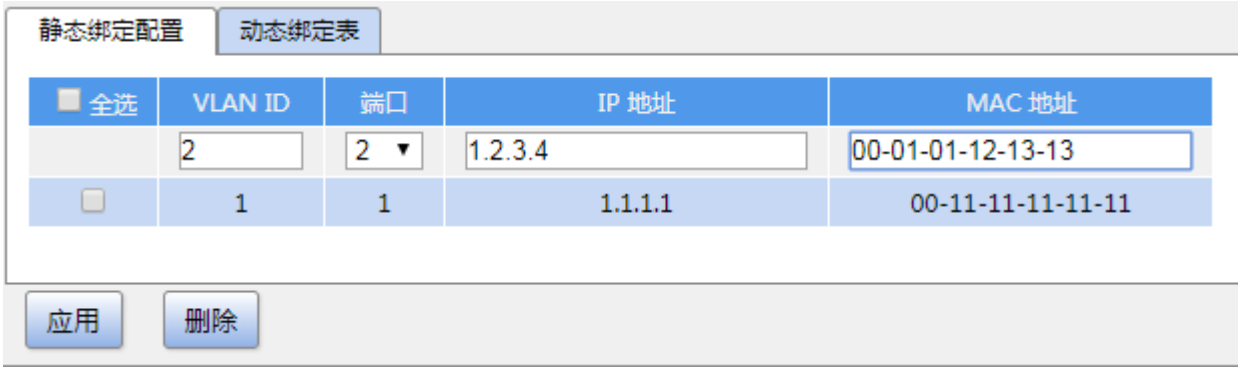


图 297 配置静态绑定表

VLAN ID

配置选项：所有 VLAN ID

功能：配置静态绑定表的 VLAN ID。

端口

功能：选择该静态绑定表的成员端口。

IP 地址

配置格式：A.B.C.D

功能：配置静态绑定表的 IP 地址。

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH 或 HH:HH:HH:HH:HH:HH（H 为一个十六进制数）

功能：配置静态绑定表的 MAC 地址，只能配置为单播 MAC 地址。

4、查看动态绑定表，如下图所示；

图 298 查看动态绑定表

类型

显示选项：Relay/Snooping

说明：动态绑定表由 DHCP Relay 和 DHCP Snooping 设备产生，其中 Relay 类型的表项在全局使能 IP Source Guard 功能后产生，Snooping 类型的表项在全局和连接 DHCP 客户端的端口均使能 IP Source Guard 功能后产生。

8.6.4 典型配置举例

1、Relay 类型 IP Source Guard 表项

如图 299所示，交换机A作为DHCP服务器，交换机B作为DHCP中继，交换机C作为DHCP客户端，交换机A的1端口连接交换机B的1端口，交换机B的2端口连接交换机C的2端口。DHCP服务器与DHCP客户端不在同一个局域网中，中继设备开启IP Source Guard后，客户端通过DHCP中继，以DHCP的方式动态获取IP地址和其他网络参数，中继设备形成IP Source Guard

表项。

图 299 DHCP 典型配置举例

- 交换机 A 的配置：

  1、创建 VLAN1 接口并配置 IP：100.1.1.156；

  2、在 VLAN 1 打开 DHCP 服务器状态，见图 208；

  3、创建地址池 pool-33，见图 209；

  4、选择地址池类型为 Network；IP 地址：33.1.1.6；掩码：255.0.0.0，见图 210;

- 交换机 B 的配置：

  1、创建 VLAN1 接口，并配置 IP：100.1.1.180；

  2、创建 VLAN33 接口，并配置 IP：33.1.1.2；

  3、使能 DHCP 中继，见图 223；

  4、配置服务器地址：100.1.1.156，见图 223；

  5、全局使能 IP Source Guard，见图 295；

- 交换机 C 的配置：

  1、创建 VLAN33 接口，并使能 DHCP Client；

  2、交换机 A 将地址 33.0.0.1 分配给交换机 C；

交换机 C 获取到地址后，交换机 B 上即可查看 IP Source Guard 表项，见图 298。

2、Snooping 类型 IP Source Guard 表项

如下图所示，交换机A作为DHCP服务器，交换机B作为DHCP Snooping，交换机C作为DHCP客户端，交换机A的1端口连接交换机B的1端口，交换机B的2端口连接交换机C的2端口。DHCP服务器与DHCP客户端在同一个局域网中，Snooping设备开启IP Source Guard后，客户端通过DHCP Snooping，以DHCP的方式动态获取IP地址和其他网络参数，中继设备形成IP Source Guard 表项。

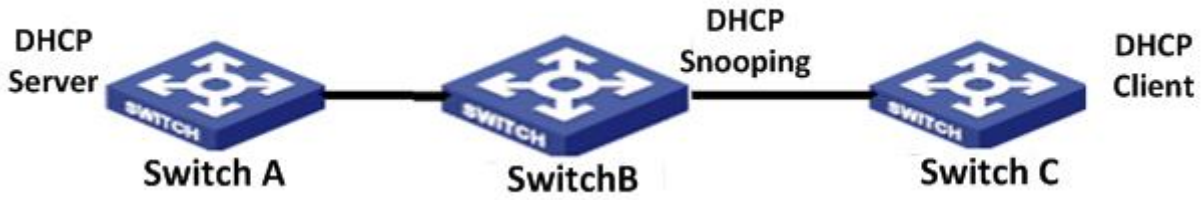


图 300 DHCP 典型配置举例

- 交换机 A 的配置：

  1、创建 VLAN1 接口并配置 IP：100.1.1.156；

  2、在 VLAN 1 打开 DHCP 服务器状态，见图 208；

  3、创建地址池 1；

  4、选择地址池类型为 Network；IP 地址：100.1.1.6；掩码：255.0.0.0;

- 交换机 B 的配置：

  1、创建 VLAN1 接口，并配置 IP：100.1.1.180；

  2、使能 DHCP Snooping；

  3、配置 1 端口为信任端口，见图 219；

  4、全局使能 IP Source Guard，见图 295；

  5、端口 2 使能 IP Source Guard，见图 296；

  交换机 C 的配置：

  1、创建 VLAN1 接口，并使能 DHCP Client；

  2、交换机 A 将地址 100.0.0.1 分配给交换机 C；

交换机 C 获取到地址后，交换机 B 上即可查看 IP Source Guard 表项。

附录 缩略语表

缩略语	英文全称	中文
ACE	Access Control Entry	访问控制表项
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
BootP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
CIST	Common and Internal Spanning Tree	公共和内部生成树
CLI	Command Line Interface	命令行接口
CoS	Class of Service	服务等级
CST	Common Spanning Tree	公共生成树
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHP	Dual Homing Protocol	双归链路协议
DNS	Domain Name System	域名系统
DRP	Distributed Redundancy Protocol	分布式冗余协议
DSCP	Differentiated Services CodePoint	差分服务编码点
DST	Daylight Saving Time	夏时制
EAPOL	Extensible Authentication Protocol over LAN	局域网上的可扩展认证协议
GARP	Generic Attribute Registration Protocol	通用属性注册协议
GMRP	GARP Multicast Registration Protocol	GARP 组播注册协议
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
HTTP	Hyper Text Transfer Protocol	超级文本传送协议
ICMP	Internet Control Message Protocol	因特网控制消息协议
IGMP	Internet Group Management Protocol	因特网组管理协议
IGMP Snooping	Internet Group Management Protocol Snooping	互联网组管理协议窥探
IST	Internal Spanning Tree	内部生成树
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元

LLDP	Link Layer Discovery Protocol	链路层发现协议
LLDPDU	Link Layer Discovery Protocol Data Unit	链路层发现协议数据单元
MIB	Management Information Base	管理信息库
MSTI	Multiple Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议
NAS	Network Access Server	网络接入服务器
NetBIOS	Network Basic Input/Output System	网络基本输入/输出系统
NMS	Network Management Station	网络管理站
NTP	Network Time Protocol	网络时间协议
OID	Object Identifier	对象标识符
PCP	Priority Code Point	优先级代码点
PVLAN	Private VLAN	私有 VLAN
QCL	QoS Control List	QoS 控制列表
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial-In User Service	远程认证拨号用户服务
RMON	Remote Network Monitoring	远程网络监控
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
SFTP	Secure File Transfer Protocol	安全文件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SNTP	Simple Network Time Protocol	简单网络时间协议
SP	Strict Priority	严格优先级
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	安全套接层
SSM	Source Specific Multicast	指定信源组播
STP	Spanning Tree Protocol	生成树协议
TACACS+	Terminal Access Controller Access Control System	终端访问控制器访问控制系统
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
USM	User-Based Security Model	安全模型

VLAN	Virtual Local Area Network	虚拟局域网
WINS	Windows Internet Naming Service	Windows Internet 名称服务
WRR	Weighted Round Robin	加权轮询调度