SICOM3024P 工业以太网交换机

Web 操作手册

出版日期：2021 年 07 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

http://www.kyland.com

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 SICOM3024P 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 ➢ 产品型号介绍 ➢ 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、设备管理	➢ 重启 ➢ 登出
4、设备状态	➢ 基本信息 ➢ 端口状态 ➢ 端口流量 ➢ 系统运行信息
5、设备基本配置	➢ IP 地址 ➢ 设备基本信息配置 ➢ 端口配置 ➢ 修改密码 ➢ 软件升级(FTP 升级) ➢ 软件版本查询 ➢ 配置上传/下载
6、设备高级配置	➢ 端口流量配置 ➢ VLAN 配置

	➢ PVLAN 配置 ➢ 端口镜像配置 ➢ 端口聚合配置 ➢ 链路状态检测 ➢ 静态组播地址表 ➢ IGMP Snooping ➢ ACL 配置 ➢ ARP 配置 ➢ SNMP 配置 ➢ DT-Ring 配置 ➢ RSTP/STP 配置 ➢ RSTP/STP 透传 ➢ DRP ➢ QoS 配置 ➢ MAC 老化时间 ➢ LLDP 信息 ➢ SNTP ➢ 端口隔离配置 ➢ 告警 ➢ 端口流量告警 ➢ GMRP 配置与查询 ➢ RMON ➢ 日志查询功能 ➢ 单播地址配置与查询 ➢ DHCP

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

SICOM3024P 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

SICOM3024P 工业以太网交换机硬件安装手册	详细了解 SICOM3024P 外型结构、硬件规格以及安装拆卸方法
SICOM3024P 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

用户可以从以下两种途径及时获得产品的相关资料和文档：

- 通过随机光盘、随机印刷手册获取；
- 通过本公司网站获取；

1 产品介绍

1.1 概述

该系列交换机主要应用在电力、轨道交通、煤炭等多个行业，能够适应严酷而危险的环境；支持 RSTP、DT-Ring 和 IEC62439-6 冗余协议族，为系统的可靠运行提供多重保证；灵活的模组化设计，扩展方便；符合 IEC61850-3 和 IEEE1613 标准。

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：RSTP/STP、DT-Ring 和 IEC62439-6；
- 组播协议：IGMP Snooping、GMRP 和静态组播；
- 交换属性：VLAN、PVLAN、QoS、ARP；
- 带宽管理：端口聚合、端口流量配置；
- 安全管理：ACL、端口隔离；
- 同步协议：SNTP；
- 设备管理：FTP 软件升级，配置上传/下载；
- 设备诊断：端口镜像、LLDP、链路状态检测；
- 告警功能：端口告警、电源告警、环告警、IP/MAC 地址冲突告警、温度告警和端口流量告警；
- 网络管理：支持 CLI、Telnet、Web、Kyvision 网管软件管理和 SNMP 网络监控；
- ……

2 交换机的访问方式

支持以下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 登录到 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>	一般用户配置模式	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	“**enable**”进入特权用户配置模式
SWITCH #	特权用户配置模式	上传/下载配置文件； 恢复默认配置； 发送 ping 测试数据包查看响应信息； 重启设备； 保存当前配置； 查看交换机配置信息； 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；<H.H.H.H>指 IP 地址配置格式；<H:H:H:H:H:H>指 MAC 地址配置格式；word<1，31>指字符串范围。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。

1、用 DB9-RJ45 电缆线连接 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；

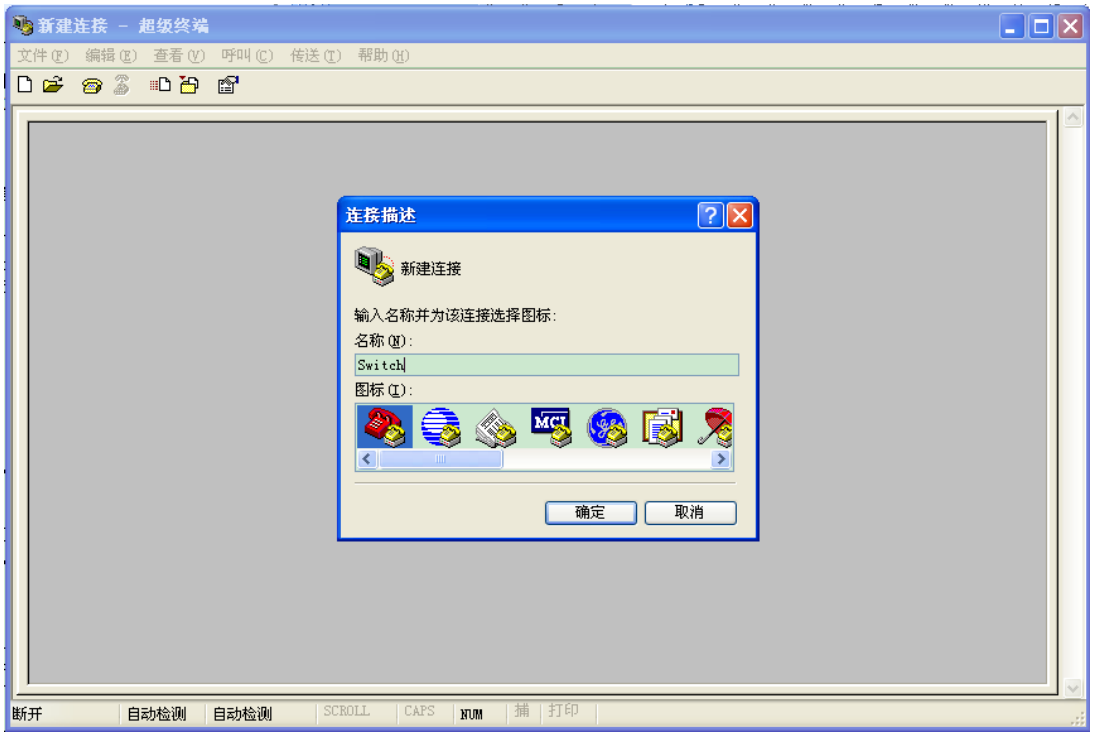

图 2 新建连接

4、 选择正确的通信端口进行连接，如图 3 所示；

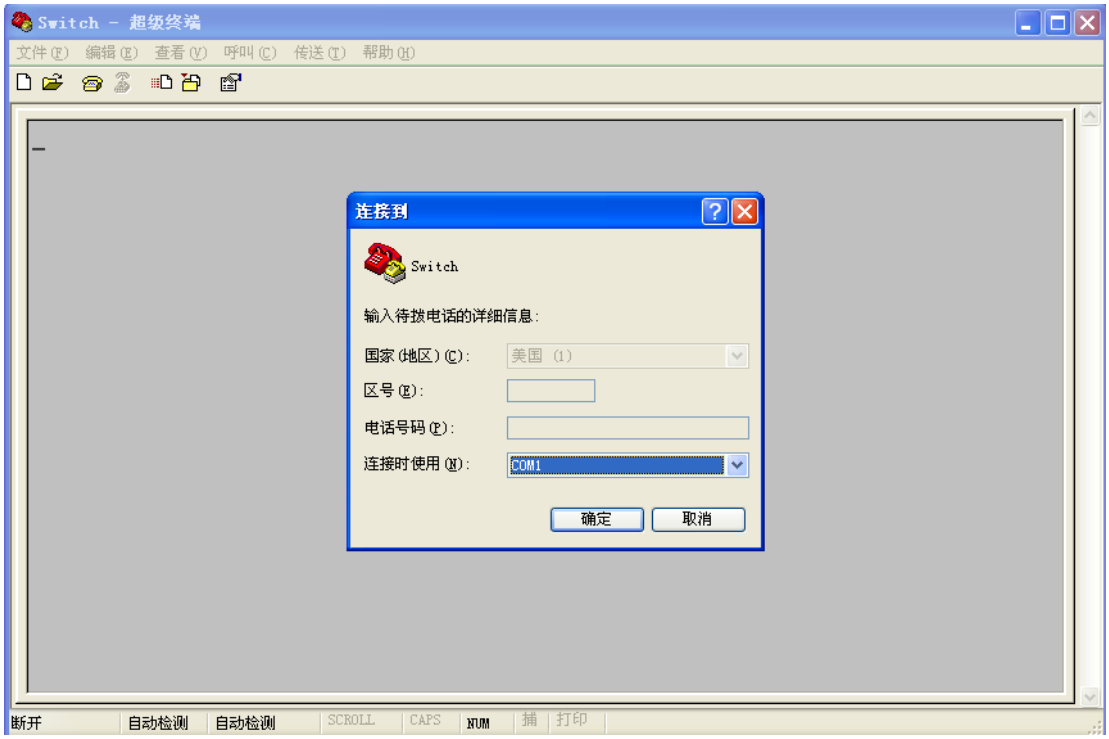

图 3 选择正确的通信端口

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)：9600；数据位：8；奇偶校验：无；停止位：1；数据流控制：无；

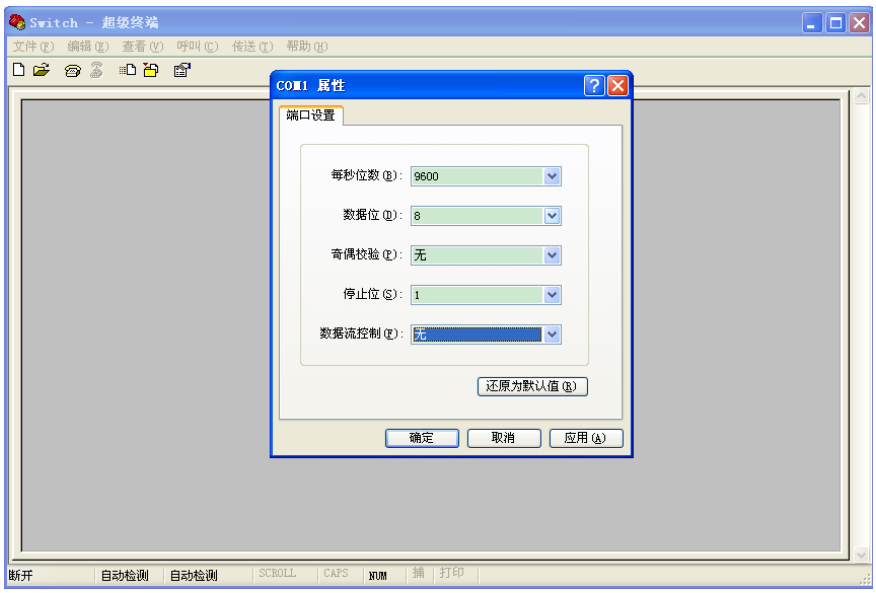

图 4 属性配置

6、点击<确定>按钮，可以成功进入交换机的命令行界面，按<回车>键进入一般用户配置模式，如图 5 所示；

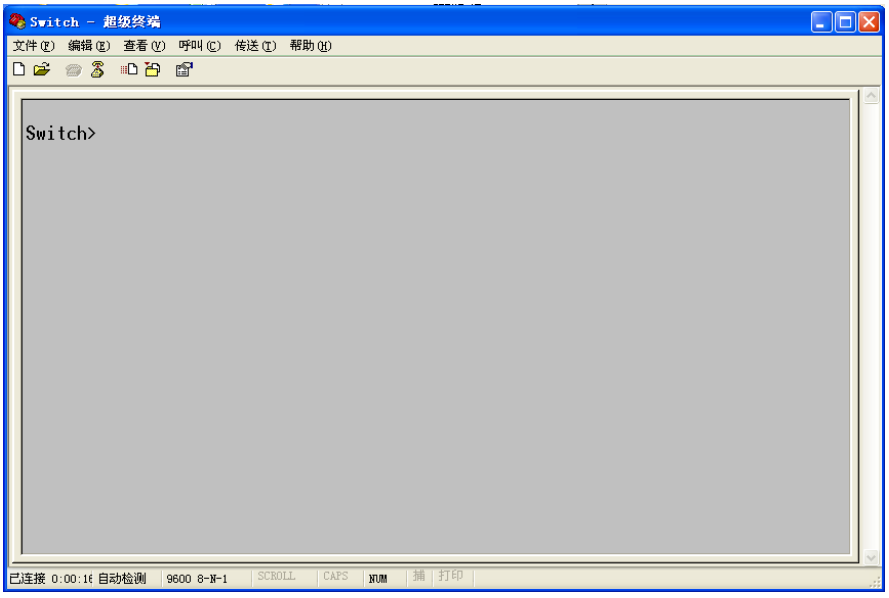

图 5 CLI 界面

2.3 Telnet 访问

Telnet 登录要求 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*”，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“5.1 IP 地址”章节获取 IP 地址。

2、登录到 Telnet 界面，回车即可进入交换机命令行界面，如图 7 所示；

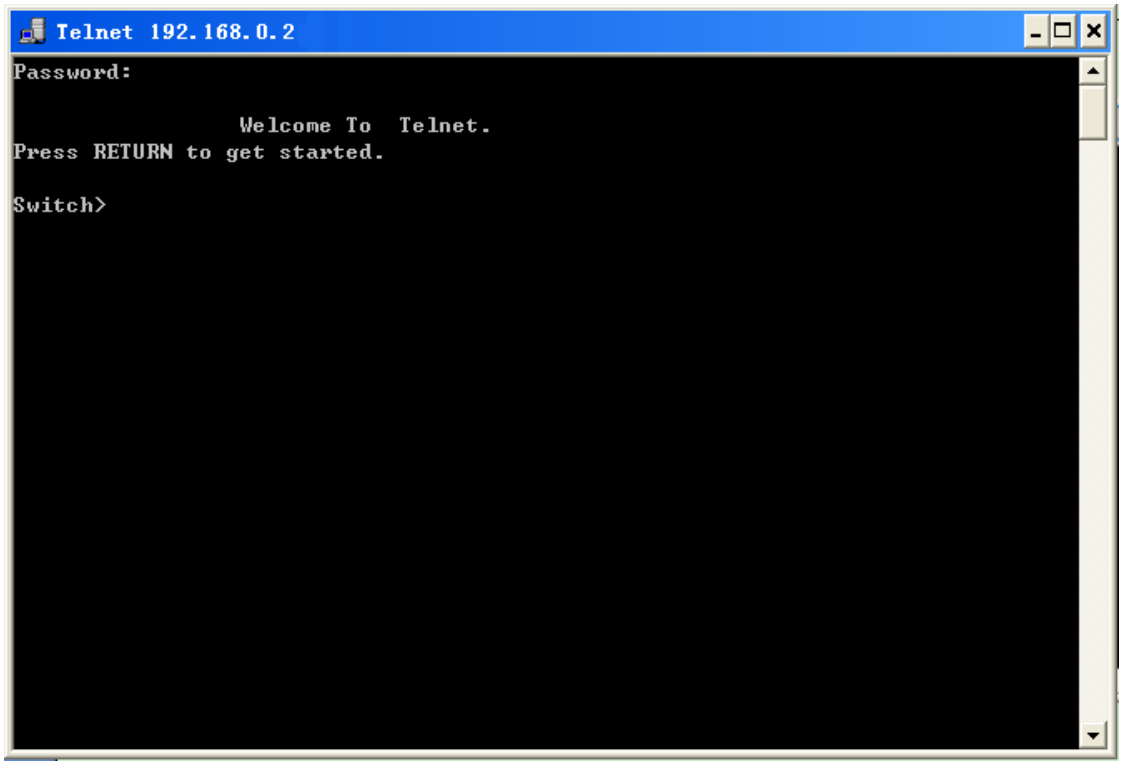

图 7 Telnet 界面

2.4 Web 访问

Web 登录要求 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*”，出现登录对话框如图 8 所示，输入用户名为“admin”，初始密码“123”，点击<登录>按钮；

图 8 Web 登录

点击<English>按钮可以切换到英文登录界面，出厂默认配置为英文登录界面，点击<中文>按钮便可以切换到中文登录界面。

说明：

如果不清楚当前交换机的 IP 地址，请参考“5.1 IP 地址”章节获取 IP 地址。

2、此时成功登录到交换机页面，左边是配置导航树，如图 9 所示；

图 9 Web 界面

点击导航树顶端的<闭合>、<展开>按钮，可以使所有导航树闭合、展开；点击导航树中[保存所有修改]、[恢复默认配置]菜单可以进行相应的操作。点击右上角的<English>按钮可以切换到英文界面。

注意：

恢复默认配置后必须重启设备，才能使该操作生效。

3 设备管理

点击[设备管理]→[重启]/[登出]菜单可以进行重启设备/退出 Web 配置页面操作。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最新保存的配置信息，如果没有保存过配置信息，则重启后交换机配置恢复为出厂默认配置。

4 设备状态

4.1 基本信息

基本信息包括 MAC 地址、设备序列号、IP 地址、子网掩码地址、网关地址、系统名称、设备类型以及版本信息，如图 10 所示。

项目名称	信息
MAC地址	00-1E-CD-00-00-20
设备序列号	S3MOT12030189
IP 地址	192.168.0.112
子网掩码地址	255.255.255.0
网关地址	192.168.0.1
系统名称	SWITCH
设备类型	24T_4G
软件版本号	ID:2 R1005.P05 (2018-6-5 17:28)
BootRom版本号	V4.0.2 (2014-7-11 23:33)
硬件版本信息	V4.0

图 10 设备基本信息

4.2 端口状态

端口状态信息可以自动显示端口号、管理状态、操作状态、连接状态、速率、双工、流控如图 11 所示。

端口	管理状态	操作状态	连接状态	速率	双工	流控	接收方向	发送方向
S1/FE1	使能	使能	断开	---	---	---	---	---
S1/FE2	使能	使能	连接	100M	全双工	关闭	使能	使能
S1/FE3	使能	使能	断开	---	---	---	---	---
S1/FE4	使能	使能	断开	---	---	---	---	---
S1/FE5	使能	使能	断开	---	---	---	---	---
S1/FE6	使能	使能	断开	---	---	---	---	---
S1/FE7	使能	使能	断开	---	---	---	---	---
S1/FE8	使能	使能	断开	---	---	---	---	---
S2/FE1	使能	使能	断开	---	---	---	---	---
S2/FE2	使能	使能	断开	---	---	---	---	---
S2/FE3	使能	使能	断开	---	---	---	---	---
S2/FE4	使能	使能	断开	---	---	---	---	---
S2/FE5	使能	使能	断开	---	---	---	---	---
S2/FE6	使能	使能	断开	---	---	---	---	---
S2/FE7	使能	使能	断开	---	---	---	---	---
S2/FE8	使能	使能	断开	---	---	---	---	---
S3/FE1	使能	使能	断开	---	---	---	---	---
S3/FE2	使能	使能	断开	---	---	---	---	---
S3/FE3	使能	使能	断开	---	---	---	---	---
S3/FE4	使能	使能	断开	---	---	---	---	---
S3/FE5	使能	使能	断开	---	---	---	---	---
S3/FE6	使能	使能	断开	---	---	---	---	---
S3/FE7	使能	使能	断开	---	---	---	---	---
S3/FE8	使能	使能	断开	---	---	---	---	---
S4/GX1	使能	使能	断开	---	---	---	---	---
S4/GX2	使能	使能	断开	---	---	---	---	---
S4/GX3	使能	使能	断开	---	---	---	---	---
S4/GX4	使能	使能	断开	---	---	---	---	---

图 11 端口状态信息

端口

显示端口类型及端口号。

端口采用 Sα/β 格式。

α 表示端口所在板卡的插槽号。

β 表示端口类型+端口所在面板/板卡上的标号。FE/FX/GE/GX 表示端口类型，FE 代表端口为百兆 RJ45 电口，FX 代表端口为百兆光口，GE 代表端口为千兆 RJ45 电口，GX 代表端口为千兆 SFP 接口。

管理状态

显示当前端口管理状态。

使能表示打开端口允许数据传输；

不使能表示关闭端口不传输数据。

操作状态

显示当前端口操作状态。

连接状态

显示当前端口的连接状态。

连接表示端口处于 LinkUp 状态可以正常通信；

断开表示端口处于 LinkDown 状态不能正常通信。

速率

显示当前 LinkUp 状态端口的通信速率。

双工

显示当前 LinkUp 状态端口的双工模式。

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。

流控

显示当前 LinkUp 端口的流控状态。

接收方向

选项：使能/不使能

使能说明该端口可以接收数据；

不使能说明该端口不能接收数据。

发送方向

选项：使能/不使能

使能说明该端口可以发送数据；

不使能说明该端口不能发送数据。

说明：

端口详细介绍和配置参考“5.3 端口配置”章节。

4.3 端口流量

端口流量信息统计发送字节数/数据包、接收字节数/数据包、CRC 错误、小于 64 字节的数据包，如图 12 所示；

端口	状态	连接	发送字节数	发送数据包	接收字节数	接收数据包	CRC错误	小于64Bytes
S1/FE1	使能	断开	0	0	0	0	0	0
S1/FE2	使能	连接	13910246	24707	2052001	17336	0	0
S1/FE3	使能	断开	0	0	0	0	0	0
S1/FE4	使能	断开	0	0	0	0	0	0
S1/FE5	使能	断开	0	0	0	0	0	0
S1/FE6	使能	断开	0	0	0	0	0	0
S1/FE7	使能	断开	0	0	0	0	0	0
S1/FE8	使能	断开	0	0	0	0	0	0
S2/FE1	使能	断开	0	0	0	0	0	0
S2/FE2	使能	断开	0	0	0	0	0	0
S2/FE2	使能	断开	0	0	0	0	0	0
S2/FE3	使能	断开	0	0	0	0	0	0
S2/FE4	使能	断开	0	0	0	0	0	0
S2/FE5	使能	断开	0	0	0	0	0	0
S2/FE6	使能	断开	0	0	0	0	0	0
S2/FE7	使能	断开	0	0	0	0	0	0
S2/FE8	使能	断开	0	0	0	0	0	0
S3/FE1	使能	断开	0	0	0	0	0	0
S3/FE2	使能	断开	0	0	0	0	0	0
S3/FE3	使能	断开	0	0	0	0	0	0
S3/FE4	使能	断开	0	0	0	0	0	0
S3/FE5	使能	断开	0	0	0	0	0	0
S3/FE6	使能	断开	0	0	0	0	0	0
S3/FE7	使能	断开	0	0	0	0	0	0
S3/FE8	使能	断开	0	0	0	0	0	0
S4/GX1	使能	断开	0	0	0	0	0	0
S4/GX2	使能	断开	0	0	0	0	0	0
S4/GX3	使能	断开	0	0	0	0	0	0
S4/GX4	使能	断开	0	0	0	0	0	0

清零

图 12 端口流量信息

点击<清零>按钮清除端口流量信息重新开始统计。

4.4 系统运行信息

系统运行信息统计设备运行时间、CPU 使用率、内存使用率、设备温度和系统时间（本地时间），如图 13 所示；

系统运行信息	
设备运行时间:	0Days,1H:25M:41S
CPU使用率:	1%(30 seconds), 10%(5 minutes)
内存利用率:	68%
设备温度:	+35℃
系统时间:	2015.01.19 23:16:46 星期一

图 13 系统运行信息

5 设备基本配置

5.1 IP 地址

1、 通过 Console 口查看交换机 IP 地址

Console 口访问交换机登录到命令行界面时，在特权用户配置模式下输入命令”**show interface**”可以查看交换机的 IP 地址，如图 14 红色区域部分所示；

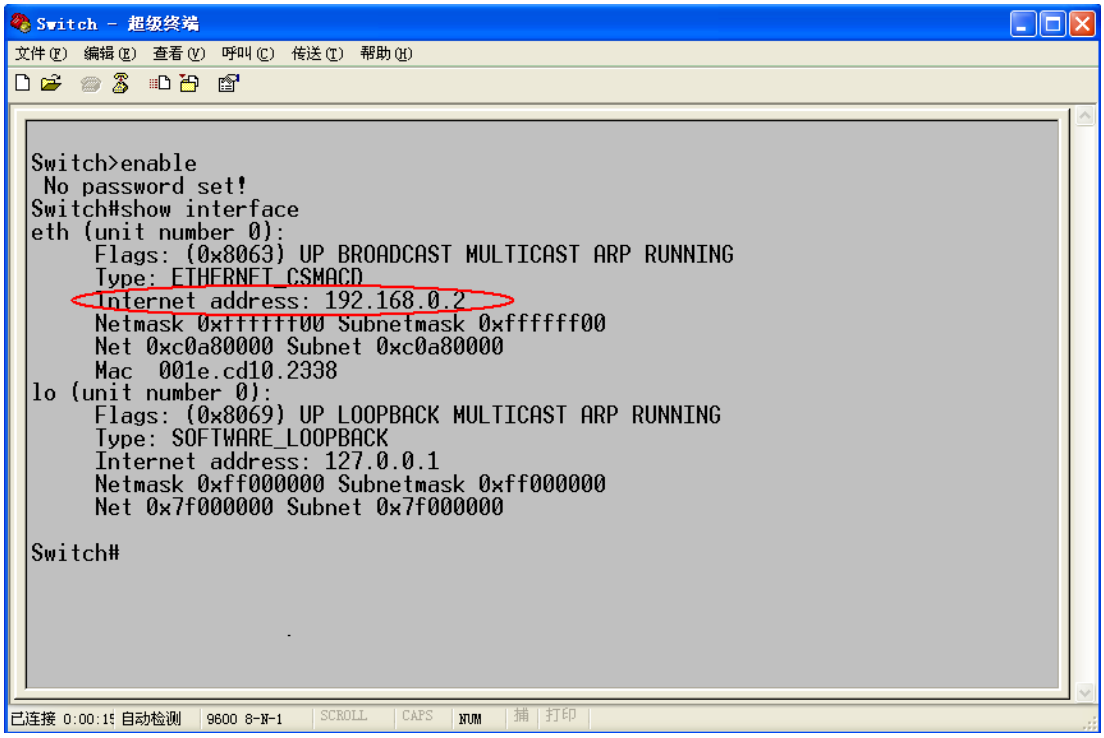

图 14 查看 IP 地址

2、IP 地址配置

交换机的 IP 地址和网关可以通过手动配置如图 15 所示。

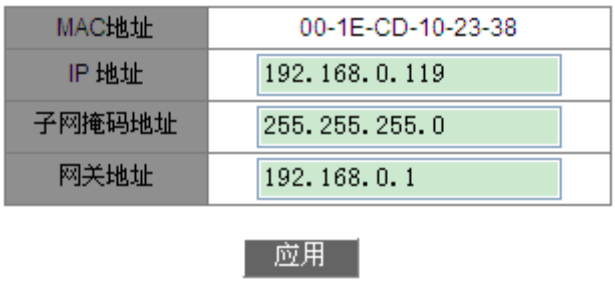

图 15 IP 地址

注意：

- IP 地址和网关必须在同一网段中，否则无法修改 IP 地址；
- IP 地址修改后立即生效，不需要重启设备。

5.2 设备基本信息配置

设备基本信息配置页面可以对设备的维护信息进行配置，包括项目名称、系统名称、时区、地址、联系方式和系统时间，如图 16 所示。

图 16 设备信息

项目名称

配置范围：1~64 个字符

系统名称

配置范围：1~32 个字符

时区

配置选项：0，+1，+2，+3，+4，+5，+6，+7，+8，+9，+10，+11，+12，+13， -1，-2，-3，-4，-5，-6，-7，-8，-9，-10，-11，-12 时

0~59 分

默认配置：0 时 0 分

功能：选择本地时区。

地址

配置选项：字符/汉字

配置范围：1~255 个字符(一个汉字占用两个字符)

联系方式

配置选项：字符/汉字

配置范围：1~32 个字符(一个汉字占用两个字符)

系统时间设置

组合配置：{ 年、月、日、时、分、秒}

配置范围：年取值范围为 2000~2099，月取值范围为 1~12，日取值范围为 1~31 时取值范围为 0~23，分和秒取值范围为 0~59

功能：配置系统日期和时间，使交换机在断电后可以继续计时。

5.3 端口配置

端口配置可以控制端口状态、端口速率、流控等信息，如图 17 所示；

端口	管理状态	操作状态	自动协商	速度	双工	流控制	接收方向	发送方向	复位
S1/FE1	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE2	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE3	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE4	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE5	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE6	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE7	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S1/FE8	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE1	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE2	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE3	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE4	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE5	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE6	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE7	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S2/FE8	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE1	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE2	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE3	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE4	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE5	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE6	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE7	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S3/FE8	使能	使能	使能	100M	全双工	关闭	使能	使能	不复位
S4/GX1	使能	使能	使能	1000M	全双工	关闭	使能	使能	不复位
S4/GX2	使能	使能	使能	1000M	全双工	关闭	使能	使能	不复位
S4/GX3	使能	使能	使能	1000M	全双工	关闭	使能	使能	不复位
S4/GX4	使能	使能	使能	1000M	全双工	关闭	使能	使能	不复位

应用

图 17 端口配置

管理状态

配置选项：使能/不使能

默认配置：使能

功能：配置端口管理状态。

描述：使能表示打开端口允许数据传输；不使能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。

操作状态

描述：管理状态使能时，操作状态强制为使能；管理状态不使能时，操作状态强制为不使能。

自动协商

配置选项：使能/不使能

功能：配置端口自动协商状态。

描述：自动协商配置使能时，端口速率和双工模式会根据端口连接状态自动协商；自动协商配置禁止时，端口速率和双工模式可由用户自行配置。

注意：

- 千兆电口自动协商强制为使能；
- 百兆光口自动协商强制为禁止。

速度

配置选项：10M/100M/1000M

功能：强制配置端口速度。

描述：自动协商不使能时，端口速度由用户自行配置。

双工

配置选项：全双工/半双工

功能：配置端口的双工模式

描述：自动协商不使能时，端口双工模式由用户自行配置。

注意：

- 百兆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；
- 百兆光口强制为 100M 全双工；

- 千兆电口强制为自动协商；
- 千兆光口可以配置为自动协商、1000M 全双工。

建议用户使能每个端口的自动协商，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配置一致。

流控制

配置选项：打开/关闭

默认配置：关闭

功能：打开/关闭指定端口的流控功能。

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。

接收方向

配置选项：使能/不使能

默认配置：使能

功能：是否允许端口接收数据。

描述：使能表示该端口可以接收数据；不使能表示该端口不能接收数据。

发送方向

配置选项：使能/不使能

默认配置：使能

功能：是否允许端口发送数据。

描述：使能表示该端口可以发送数据；不使能表示该端口不能送数据。

复位

配置选项：复位/不复位

默认配置：不复位

功能：是否对指定端口进行一次复位操作。

5.4 修改密码

用户可以修改“admin”用户的对应密码，操作如图 18 所示。

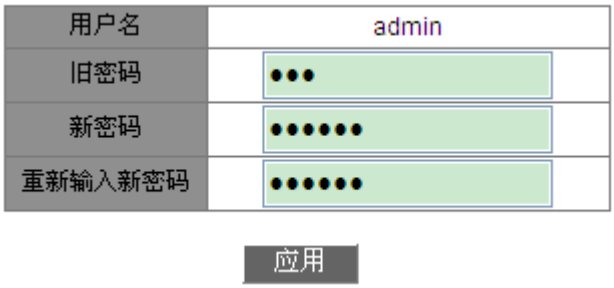

图 18 修改密码

5.5 软件升级

交换机通过升级软件版本可以获得更完美性能。该系列交换机升级包括 Bootrom 软件版本升级和系统软件版本升级，升级时应先升级 Bootrom 软件版本。再升级系统软件版本，在 Bootrom 版本不变的情况下可以只升级系统软件版本。

软件版本升级过程需要借助 FTP 服务器进行。

FTP 升级

安装 FTP 服务器以 WFTPD 软件为例介绍 FTP 服务器的配置及软件升级过程；

1、打开[Security]→[users/rights]对话框点击<new user>按钮来添加 FTP 新用户，如图 19 所示，输入用户名和密码，例如：用户名 admin，密码 123，点击<OK>按钮；

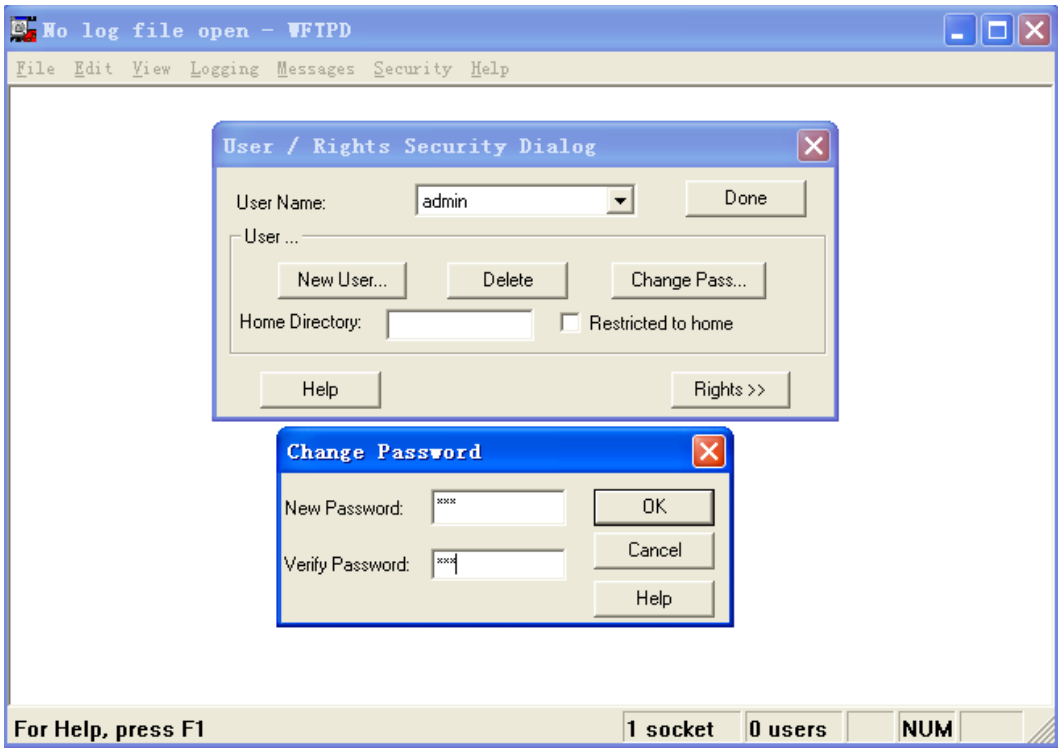

图 19 添加 FTP 新用户

2、在 Home Directory 栏中输入服务器中软件版本文件的存放路径，如图 20 所示，点击<Done>按钮；

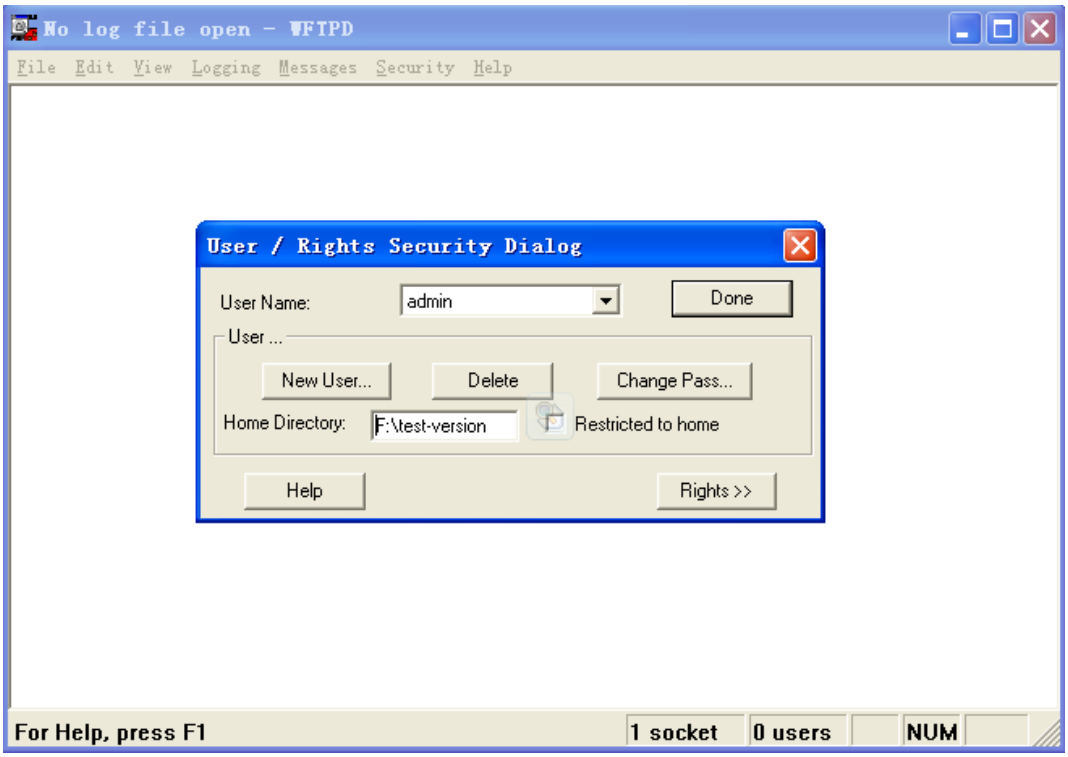

图 20 文件路径修改

3、Bootrom 软件升级需要在特权用户配置模式下输入以下指令完成：

Switch#**update bootrom** *File_name Ftp_server_ip_address User_name Password*

参数说明如表 2 所示；

表 2 FTP 模式下 Bootrom 升级参数说明

参数	说明
File_name	Bootrom 软件版本名称
Ftp_server_ip_address	FTP 服务器 IP 地址
User_name	创建的 FTP 用户名
Password	创建的 FTP 用户密码

4、系统软件升级如图 21 所示，输入 FTP 服务器 IP 地址、文件名(服务器上文件名)、建立的 FTP 用户名、用户密码，点击<应用>按钮；

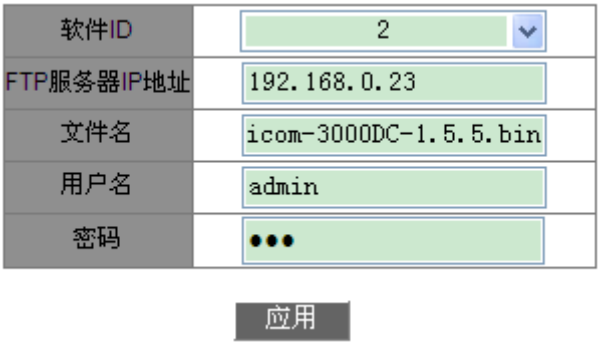

图 21 FTP 模式下升级软件

警告：

文件名必须带有后缀，否则会导致升级失败。

5、确保 FTP 服务器和交换机通信正常，如图 22 所示；

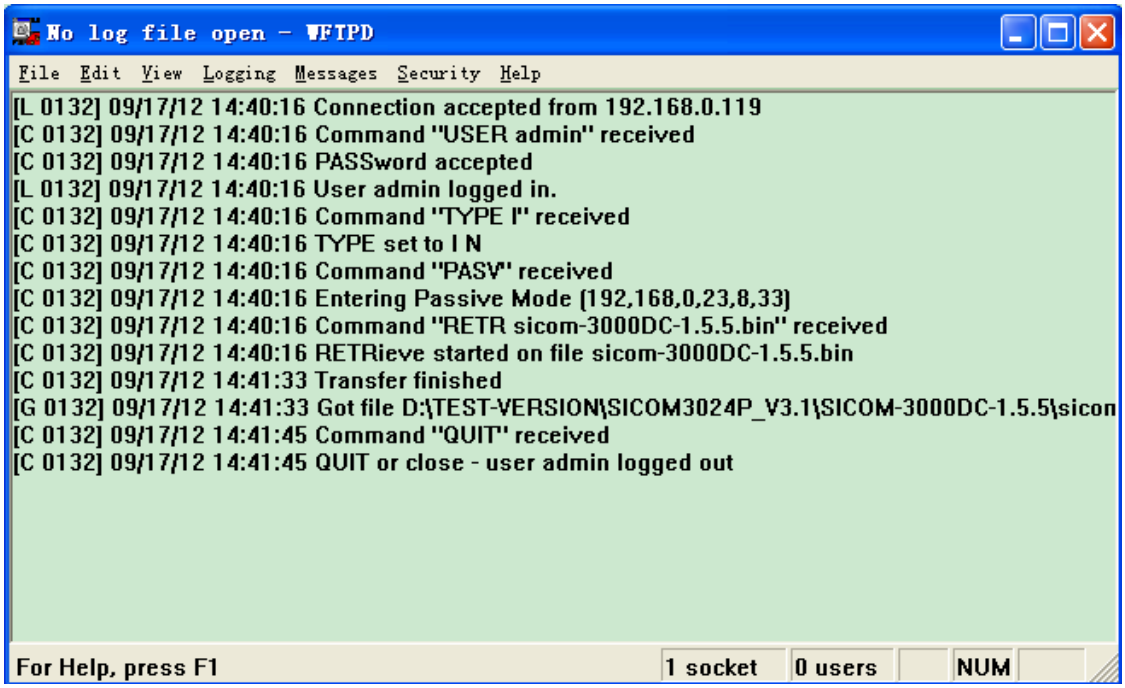

图 22 FTP 服务器和交换机通信正常

注意：

如需显示如图 22 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。

6、待 Web 页面中提示升级成功如图 23 所示，重启设备并在基本信息中检查软件版本是否为升级后的软件版本。

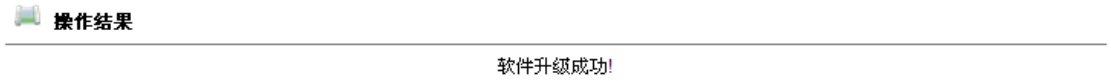

图 23 FTP 软件升级成功

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，必须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。

5.6 软件版本查询

该系列交换机可以下载两个不同的系统软件版本，但只有一个版本处于启动状态。

软件版本查询可以详细了解两个软件版本号、发布日期以及活动状态，如图 24 所示；

图 24 软件版本查询

5.7 配置上传/下载

配置备份功能可以把交换机的当前配置文件保存在服务器中，当交换机配置信息改变后，可以通过 FTP 协议从服务器下载配置文件到交换机中来获取希望得到的配置信息。

文件上传指把交换机的配置信息文件上传到服务器中，一般多保存为*.doc 和*.txt 文件类型。文件下载指从服务器上下载已保存的配置文件到交换机中，如图 25、图 26 所示。

注意：

下载配置文件到交换机中，需要重启交换机，配置信息才能生效。

图 25 FTP 模式上传配置文件

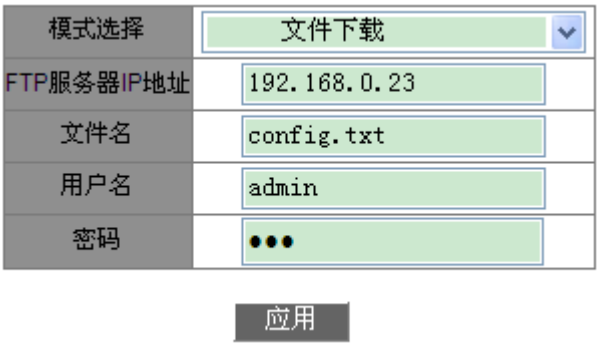

图 26 FTP 模式下载配置文件

6 设备高级配置

6.1 端口流量配置

介绍

端口流量配置指对端口接收或者发送的报文数据量进行限制，并将超过限定值的数据量丢弃。入口对所选择的报文进行限速，出口对所有报文进行限速。

入口限速的报文包括以下七种：

- 单播报文：静态添加或者通过源 MAC 地址已经学习的单播报文；
- 多播报文：静态添加或者通过 IGMP Snooping、GMRP 学习的报文；
- 保留多播：MAC 地址在 0x0180c2000000~0x0180c200002f 范围之间的报文；
- 广播报文：目的 MAC 地址是 FF:FF:FF:FF:FF:FF 的报文；
- 未知多播报文：未静态添加并未通过 IGMP Snooping、GMRP 学习的报文；
- 未知单播报文：未静态添加并未经过源 MAC 地址学习的报文；
- 未知源报文：未知源 MAC 地址的报文。

Web 页面配置

1、抑制报文分类如图 27 所示；

当限制速率配置为0时为限速不使能。

抑制报文分类

限速类型	业务限速	广播限速	注释
单播报文	☑	☐	静态添加或源MAC地址已经学习的单播报文.
多播报文	☑	☐	静态添加或通过IGMP Snooping学习的报文.
保留多播	☐	☑	mac范围在0x0180c2000000~0x0180c200002f的报文.
广播报文	☐	☑	广播地址报文.
未知多播	☐	☑	未静态添加并且未通过IGMP Snooping学习的报文.
未知单播	☐	☑	未静态添加并未经过源MAC地址学习的报文.
未知源报文	☐	☑	未知源mac地址的报文.

图 27 报文抑制分类

接收方把限速报文分成两大类：业务限速和广播限速。每种报文只能加入一种限速类型。

2、端口限速配置如图 28 所示；

端口	业务限速	广播限速	发送速率
S1/FE1	0 Kbps	0 Kbps	0 Kbps
S1/FE2	0 Kbps	0 Kbps	0 Kbps
S1/FE3	0 Kbps	0 Kbps	0 Kbps
S1/FE4	0 Kbps	0 Kbps	0 Kbps
S1/FE5	0 Kbps	0 Kbps	0 Kbps
S1/FE6	0 Kbps	0 Kbps	0 Kbps
S1/FE7	0 Kbps	0 Kbps	0 Kbps
S1/FE8	0 Kbps	0 Kbps	0 Kbps
S2/FE1	0 Kbps	0 Kbps	0 Kbps
S2/FE2	0 Kbps	0 Kbps	0 Kbps
S2/FE3	0 Kbps	0 Kbps	0 Kbps
S2/FE4	0 Kbps	0 Kbps	0 Kbps
S2/FE5	0 Kbps	0 Kbps	0 Kbps
S2/FE6	0 Kbps	0 Kbps	0 Kbps
S2/FE7	0 Kbps	0 Kbps	0 Kbps
S2/FE8	0 Kbps	0 Kbps	0 Kbps
S3/FE1	0 Kbps	0 Kbps	0 Kbps
S3/FE2	0 Kbps	0 Kbps	0 Kbps
S3/FE3	0 Kbps	0 Kbps	0 Kbps
S3/FE4	0 Kbps	0 Kbps	0 Kbps
S3/FE5	0 Kbps	0 Kbps	0 Kbps
S3/FE6	0 Kbps	0 Kbps	0 Kbps
S3/FE7	0 Kbps	0 Kbps	0 Kbps
S3/FE8	0 Kbps	0 Kbps	0 Kbps
S4/GX1	0 Kbps	0 Kbps	0 Kbps
S4/GX2	0 Kbps	0 Kbps	0 Kbps
S4/GX3	0 Kbps	0 Kbps	0 Kbps
S4/GX4	0 Kbps	0 Kbps	0 Kbps

应用

图 28 端口限速配置

业务限速/广播限速

配置范围：64~1000000Kbps

功能：对端口接收报文进行限速，超过限定值的报文数据将被丢失。

描述：百兆口的入口限速值配置范围为 64~100000Kbps；

千兆口的入口限速值配置范围为 64~1000000Kbps。

发送速率

配置范围：64~1000000Kbps

功能：对端口转发报文进行限速。

描述：百兆口的出口限速值配置范围为 64~100000Kbps；

千兆口的出口限速值配置范围为 64~1000000Kbps。

注意：

限速值为 0 意味着没有使能端口限速功能。

典型配置举例

限制端口 2 接收单播报文和多播报文的入口速率为 70Kbps，接收广播报文的入口速率为 80Kbps，出口速率为 90Kbps。

配置过程：

1、业务限速选择单播报文和多播报文，广播限速选择广播报文，见图 27 所示；

2、配置 2 端口业务限速值为 70Kbps；广播限速值为 80Kbps；发送速率值为 90Kbps，见图 28 所示。

6.2 VLAN 配置

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，不同 VLAN 中的主机传输数据包必须通过路由器或三层设备。

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
		Type	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：

Type：16 位，标识本数据帧是带有 VLAN Tag 的数据，取值为 0x8100；

PRI：3 位，标记报文的 802.1p 优先级；

CFI：1 位，值为 0 表示以太网；值为 1 表示令牌环网；

VID：12 位，VLAN 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。

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，将指定端口加入到指定 VLAN 中，该端口就能转发指定 VLAN 标记的报文。

1、端口类型

根据端口在转发报文时对 Tag 标签的处理方式，可将端口类型分为两种：

- Untag端口：端口转发的报文不带tag标记，Untag端口一般用于和不支持802.1Q协议的终端设备相连，默认情况下交换机的所有端口都以Untag类型存在于VLAN1中；
- Tag端口：端口转发的报文都带tag标记。Tag端口通常用于网络传输设备之间的互连。

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。

端口的PVID是端口属性为Untag的VLAN ID，在默认情况下，所有端口的PVID 均为VLAN 1。

配置了端口类型和PVID后，端口对报文接收和转发情况，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		对转发报文的处理	
接收到的报文为 Untag	接收到的报文为 Tag	端口类型	报文处理
为报文添加 PVID 的 Tag 标记	➢ 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，去掉该报文	Untag 端口	去掉 Tag 标记后转发该报文
		Tag 端口	保持报文中原有的 Tag 标记，转发该报文

Web 页面配置

1、 配置 VLAN 透传模式，见图 29 所示；

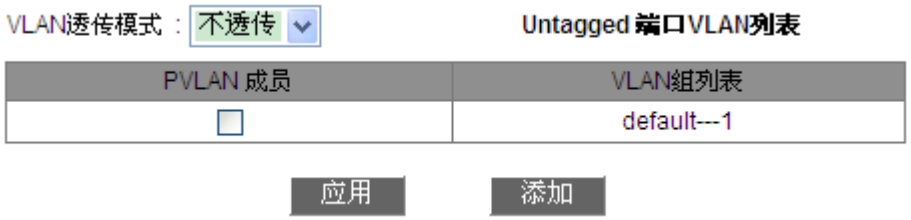

图 29 配置 VLAN 透传模式

VLAN 透传模式

配置选项：不透传/透传

默认配置：不透传

功能：配置 VLAN 透传模式。

描述：透传模式指入端口对报文的检查，如果选择不透传，则报文携带的 VLAN 标记与端口的 VLAN 不一致时，丢弃该报文；如果选择透传时，报文携带的 VLAN 标记与此交换机上其他已连接端口的 VLAN 一致时，接收该报文，否则丢弃。

2、 创建一个 VLAN

点击图 29 中的<添加>按钮，可以创建一个 VLAN 如图 30 所示，选择希望添加到该 VLAN 的端口号，并进行相应的端口配置；

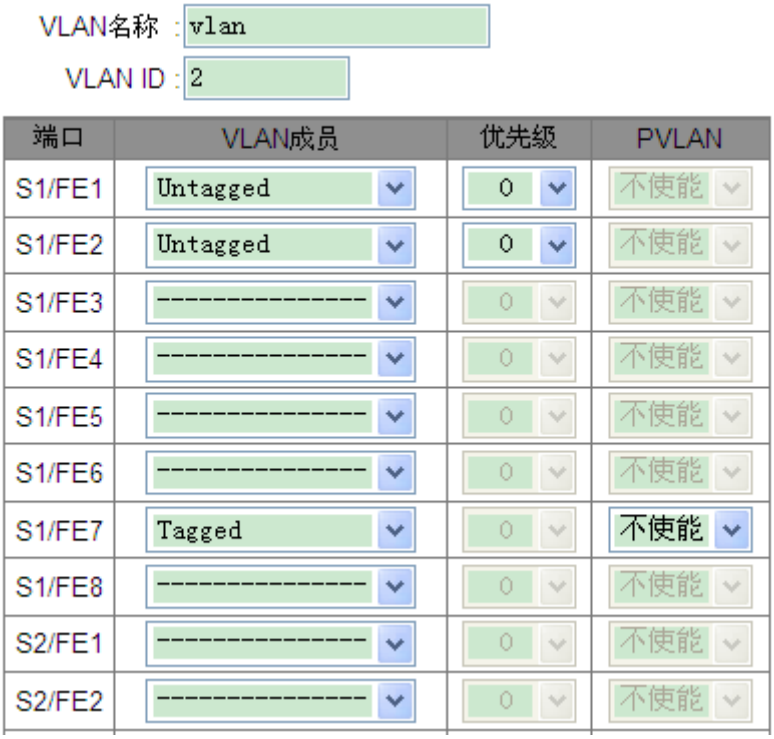

图 30 VLAN 配置表

VLAN 名称

配置范围：1~31 个字符

功能：配置 VLAN 名称。

VLAN ID

配置范围：2~4093 之间的数字

功能：配置 VLAN ID。

描述：VLAN ID 用来区分不同的 VLAN，该系列交换机最多可以同时支持 256 个 VLAN。

VLAN 成员

配置选项：Tagged/Untagged

功能：选择端口以什么方式添加到 VLAN 中。

优先级

配置范围：0~7

默认配置：0

功能：配置端口默认优先级，给 Untag 报文添加 802.1Q 标记时，PRI 字段的值为该优先级值。

PVLAN

配置选项：使能/不使能

默认配置：不使能

功能：端口以 Tag 方式添加到 VLAN 中时，选择是否添加到 PVLAN 中，PVLAN 将在稍后一节中详细介绍。

注意：

一个端口以 Untag 方式只能添加到一个 VLAN 中，即该 VLAN ID 是该端口的 PVID，默认为 VLAN 1；以 tag 方式可以添加到多个 VLAN 中。

3、查看所创建的 VLAN 列表，如图 31 所示；

图 31 查看 VLAN 列表

PVLAN 成员

配置选项：选择/不选择

功能：选择是否应用 PVLAN 功能。这部分内容将在“PVLAN”章节中详细讨论。

4、显示端口的 PVID

点击图 31 中<Untagged 端口 VLAN 列表>显示 Untagged 端口的 VLAN 列表，如图 32 所示；

端口	VLAN ID
S1/FE1	2
S1/FE2	2
S1/FE3	100
S1/FE4	100
S1/FE5	200
S1/FE6	200
S1/FE7	1
S1/FE8	1
S2/FE1	1
S2/FE2	1

图 32 端口 PVID 列表

注意：

每个端口必须有一个 Untag 属性，如果没有配置，则端口的 Untag 默认在 VLAN 1 中。

5、修改/删除 VLAN

点击图 31 中相应的 VLAN 列表便可以修改/删除已创建的 VLAN；点击下方的<删除>按钮可以直接删除当前 VLAN，如图 33 所示；

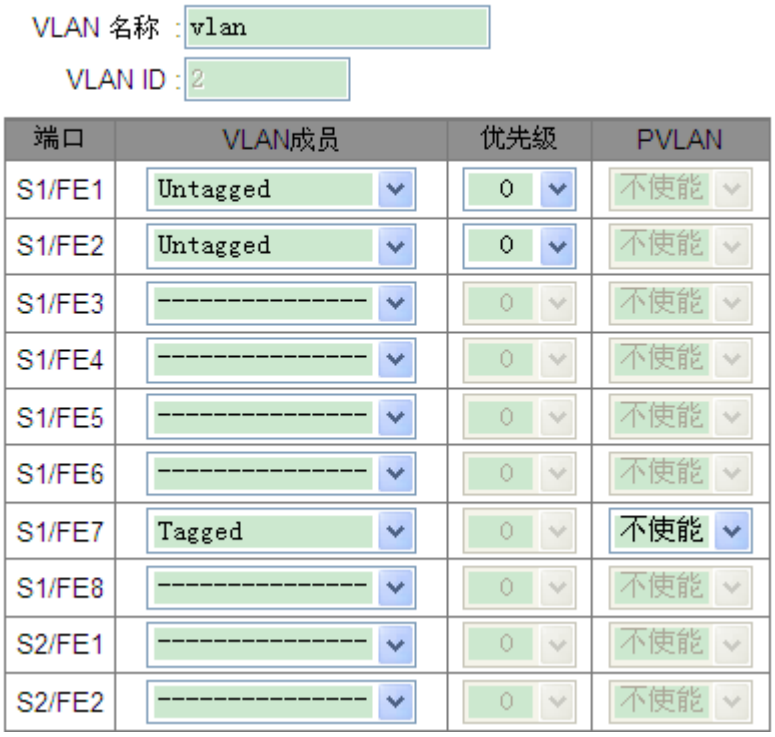

图 33 修改/删除已创建的 VLAN

典型配置举例

如图 34 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 Untag 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 Tag 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(Untag)；端口 7(tag)
VLAN100	A 地、B 地交换机 3、4 端口(Untag)；端口 7(tag)
VLAN200	A 地、B 地交换机 5、6 端口(Untag)；端口 7(tag)

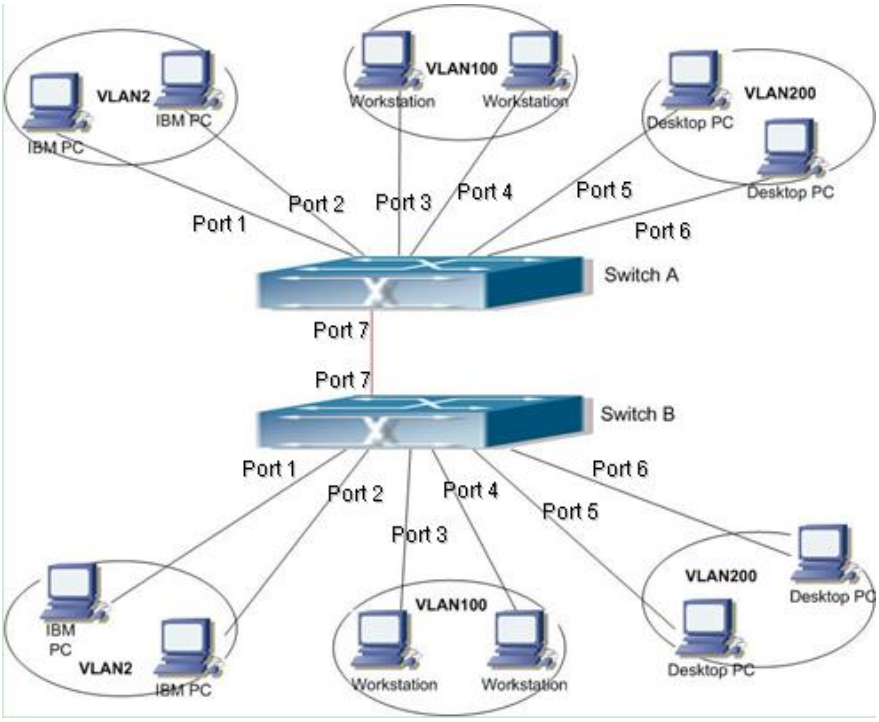

图 34 VLAN 应用

SwitchA、B的配置如下：

1、创建VLAN 2，端口1、2以Untag方式添加进来，端口7以Tag方式添加进来，见图30；

2、创建VLAN 100，端口3、4以Untag方式添加进来，端口7以Tag方式添加进来，见图30；

3、创建VLAN 200，端口5、6以Untag方式添加进来，端口7以Tag方式添加进来，见图30；

6.3 PVLAN 配置

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。

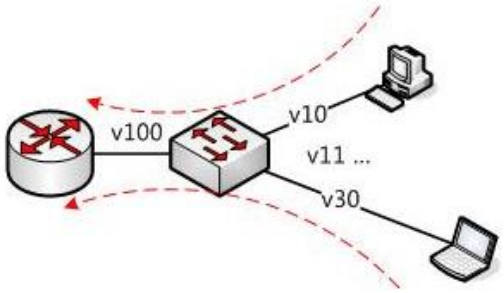

图 35 PVLAN 应用

如图 35 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。

说明：

当 Tag 端口使能 PVLAN 功能加入 PVLAN 应用后，该端口转发 tag 报文时，丢弃 VLAN 标记。

Web 页面配置

1、使能端口的 PVLAN 功能，如图 36 所示；

VLAN名称 : vlan

VLAN ID : 300

端口	VLAN成员	优先级	PVLAN
S1/FE1	Untagged	0	不使能
S1/FE2	Untagged	0	不使能
S1/FE3	Tagged	0	使能
S1/FE4	Tagged	0	使能
S1/FE5	Tagged	0	使能
S1/FE6	Tagged	0	使能
S1/FE7	----------	0	不使能
S1/FE8	----------	0	不使能
S4/GE1	----------	0	不使能
S4/GE2	----------	0	不使能
S4/GE3	----------	0	不使能
S4/GE4	----------	0	不使能

应用 取消

图 36 使能 PVLAN 功能

应用 PVLAN 功能时，在 VLAN 配置中应当使能 tagged 端口的 PVLAN 功能。

当前 VLAN 是共享域，则上联端口以 untag 属性，下联端口以 tagged 属性添加到该 VLAN

中；

当前 VLAN 是隔离域，则下联端口以 untag 属性，上联端口以 tagged 属性添加到该 VLAN 中；

2、选择 PVLAN 的成员 VLAN，如图 37 所示；

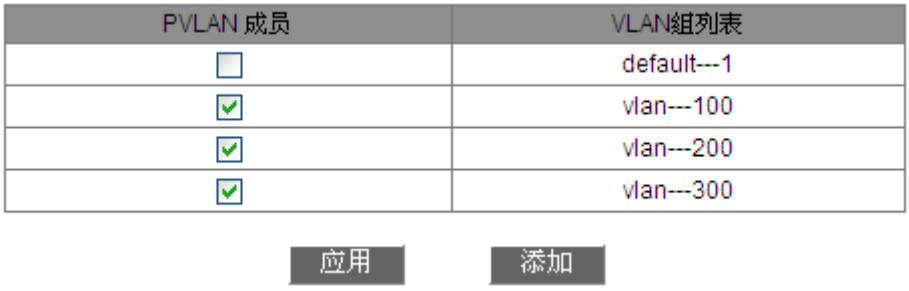

图 37 PVLAN 成员配置

PVLAN 成员

配置选项：选择/不选择

默认配置：不选择

功能：选择 PVLAN 成员。

说明：

共享域 VLAN 和隔离域 VLAN 都属于 PVLAN 的成员 VLAN。

典型配置举例

图 38 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。

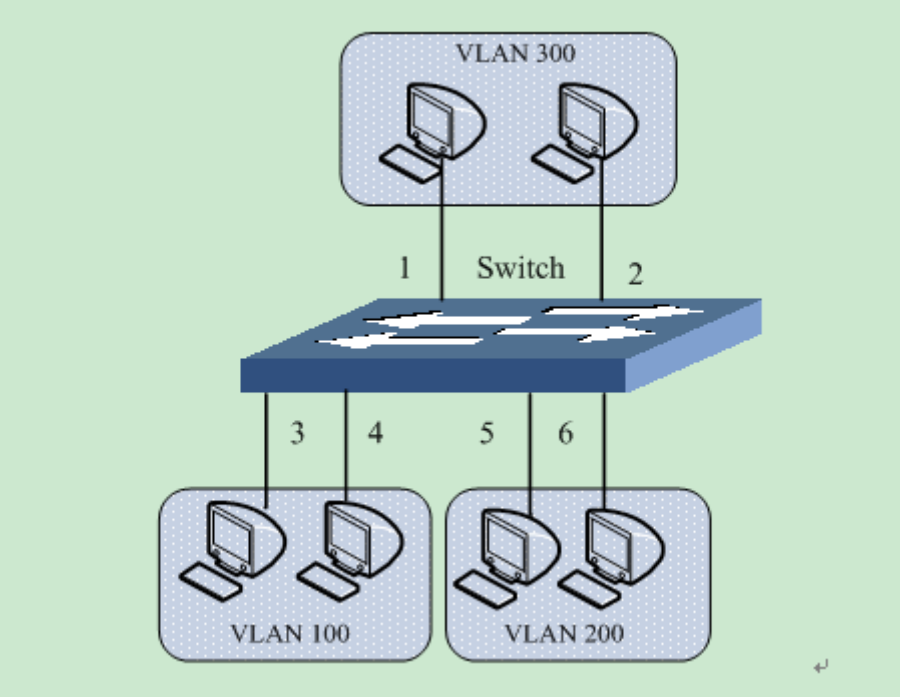

图 38 PVLAN 配置举例

交换机配置如下：

1、配置共享域 VLAN300，见图 36；

端口 1 和 2 以 Untag 方式添加到共享域 VLAN 300 中；

端口 3 和 4 以 tag 方式添加到共享域 VLAN 300 中，并且使能 PVLAN 功能；端口 5 和 6 以 tag 方式添加到共享域 VLAN 300 中，并且使能 PVLAN 功能；

2、配置隔离域 VLAN100，见图 36；

端口 1 和 2 以 tag 方式添加到隔离域 VLAN 100 中，并且使能 PVLAN 功能；

端口 3 和 4 以 Untag 方式添加到隔离域 VLAN 100 中；

3、配置隔离域 VLAN200，见图 36；

端口 1 和 2 以 tag 方式添加到隔离域 VLAN 200 中，并且使能 PVLAN 功能；

端口 5 和 6 以 Untag 方式添加到隔离域 VLAN 200 中；

4、选择共享域 VLAN300、隔离域 VLAN100 和 VLAN200 都为 PVLAN 成员，见图 37。

6.4 端口镜像配置

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。

说明

交换机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：

- 端口镜像与端口聚合互斥，加入聚合组的端口不可以配置为镜像源端口和镜像目的端口，配置为镜像源端口和镜像目的端口后不能加入聚合组；
- 端口镜像与端口冗余协议配置互斥，配置为镜像源端口和镜像目的端口后不可以配置为冗余端口，配置为冗余端口的端口不能配置为镜像源端口和镜像目的端口。

Web 页面配置

1、选择镜像目的端口（镜像端口），如图 39 所示；

图 39 选择镜像端口

镜像端口

配置选项：不使能/交换机上的某一个端口

默认配置：不使能

功能：选择一个端口做为镜像目的端口，只能有一个镜像目的端口。

2、选择镜像源端口（被镜像端口）以及端口镜像模式如图 40 所示；

被镜像端口	端口镜像模式
☑ S1/FE1	TX
☐ S1/FE2	RX
☐ S1/FE3	RX
☐ S1/FE4	RX
☑ S1/FE5	RX & TX
☑ S1/FE6	RX
☐ S1/FE7	RX
☐ S1/FE8	RX
☐ S2/FE1	RX
☐ S2/FE2	RX
☐ S2/FE3	RX
☐ S2/FE4	RX
☐ S2/FE5	RX
☐ S2/FE6	RX
☐ S2/FE7	RX
☐ S2/FE8	RX
☐ S3/FE1	RX
☐ S3/FE2	RX
☐ S3/FE3	RX
☐ S3/FE4	RX
☐ S3/FE5	RX
☐ S3/FE6	RX
☐ S3/FE7	RX
☐ S3/FE8	RX
☐ S4/GX1	RX
☐ S4/GX2	RX
☐ S4/GX3	RX
☐ S4/GX4	RX

应用

图 40 被镜像端口的配置

端口镜像模式

配置选项：RX/TX/RX&TX

功能：选择源端口被镜像的方向。

RX：仅对源端口接收的报文进行镜像；

TX：仅对源端口发送的报文进行镜像；

RX&TX：对源端口接收和发送的报文进行镜像。

典型配置举例

如图 41 所示，镜像端口为 2，被镜像端口为 1，1 端口接收和发送的所有报文都镜像到 2 端口。

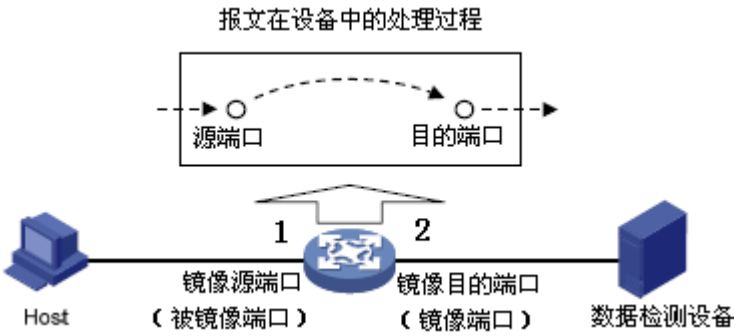

图 41 端口镜像举例

配置过程：

1、选择 2 端口作为镜像端口，见图 39；

2、选择 1 端口作为被镜像端口，端口镜像模式选择 RX&TX，见图 40。

6.5 端口聚合配置

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。

实现

如图 42 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。

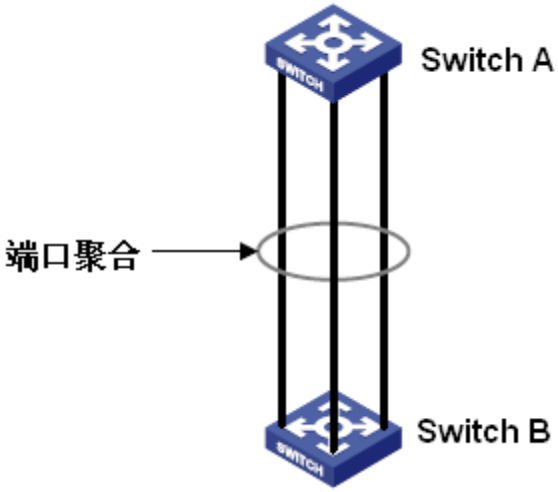

图 42 端口聚合示意图

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。

说明

端口聚合与以下端口操作相互排斥：

- 端口聚合与端口冗余协议配置互斥，加入聚合组的端口不能配置为冗余端口，冗余端口不能加入聚合组；
- 端口聚合与端口镜像互斥，加入聚合组的端口不可以配置为镜像端口和被镜像端口，配置为镜像和被镜像的端口不能加入聚合组；
- 端口聚合与 DHCP Snooping 信任端口配置互斥，加入聚合组的端口不能配置为信任端口，配置为信任端口则不能加入聚合组。

聚合端口不建议进行以下操作：

- 聚合端口使能 GMRP 协议；
- 使能 GMRP 协议的端口加入聚合组；
- 聚合端口加入某静态组播/单播表项；
- 加入某静态组播/单播表项的端口加入聚合组。

注意：

- 千兆口不支持端口聚合；

- 一个端口只能加入一个聚合组。

Web 页面配置

1、添加聚合组

点击<添加>按钮添加聚合组如图 43 所示；

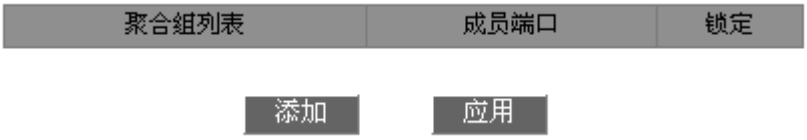

图 43 添加聚合组

2、聚合组配置，如图 44 所示；

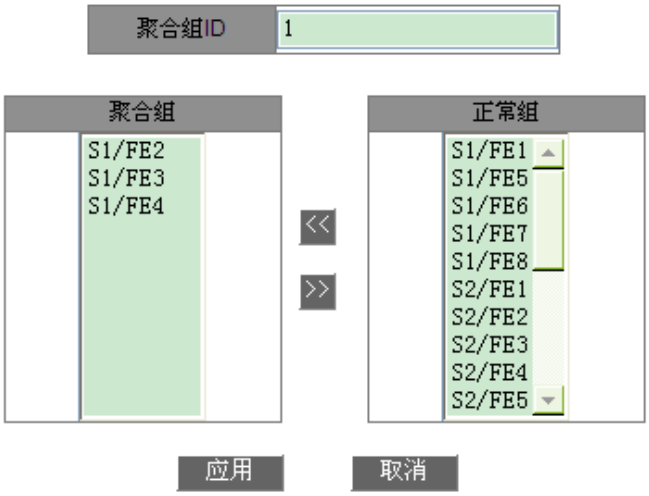

图 44 聚合组配置

聚合组 ID

配置范围：1~14

功能：配置聚合组号。

描述：该系列交换机最多支持 14 个聚合组，每个聚合组最多可以选择 4 个端口。

3、查看聚合组列表，如图 45 所示；

图 45 查看聚合组列表

锁定

用于锁定聚合组中的成员端口，使成员端口处于 Lock 状态。锁定的成员端口从聚合组中删除后，要解除该端口的 Lock 状态，必须在端口配置中手动使能。

点击图 45 中某一聚合组，可以修改聚合组配置以及删除聚合组，如图 46 所示；

图 46 修改/删除聚合组

修改聚合组的端口成员配置（添加新端口到该聚合组或者从该聚合组中删除已有端口成员），点击<应用>按钮后修改生效；点击<删除>按钮便可成功删除该聚合组。

典型配置举例

如图 42 所示，SwitchA 的 3 个端口(端口 2、3、4)分别接入设备 SwitchB 的 3 个端口(端口 2、3、4)形成聚合组 1，从而实现流量在各端口间的分担；

交换机配置过程如下：

1、SwitchA 中添加聚合组 1，并选择端口 2、3、4，见图 44；

2、SwitchB 中添加聚合组 1，并选择端口 2、3、4，见图 44；

6.6 链路状态检测

介绍

链路状态检测利用协议报文的周期性交互，判断链路的连通性，显示使能冗余协议端口的通信状态，如有故障出现可以及时发现问题并进行处理。

使能链路状态检测的端口周期性(1s)发送 link-check 报文检测链路状态。如果在接收超时周期(5s)内，没有收到对端的 link-check 报文，则认为链路有问题，进入接收故障状态；如果接收到对端的 link-check 报文，且报文中显示接收超时周期(5s)内已接收到 link-check 报文，则进入正常状态；如果接收到对端的 link-check 报文，且报文中显示接收超时周期(5s)内未接收到 link-check 报文，则进入发送故障状态。

没有使能链路状态检测的端口，工作在被动模式下。不会主动发送 link-check 报文，但接收到对端的 link-check 报文后，会立即回应一个 link-check 报文告知对端已接收到 link-check 报文。

说明：

- 该功能只针对使能冗余协议的端口有效；
- 使能链路状态检测的 DRP 环端口/备份端口、DT-Ring 环端口/备份端口、RSTP 端口出现异常状态（接收故障/发送故障）时，冗余协议将该端口 block 掉。

Web 页面配置

链路状态检测配置如图 47 所示；

图 47 链路状态配置

管理状态

配置选项：使能/不使能

默认配置：不使能

描述：是否使能端口的链路状态检测功能。

注意：

对端连接设备不支持链路状态检测功能的端口不应使能链路状态检测功能。

运行状态

显示选项：正常/不使能/接收故障/发送故障

描述：如果端口使能了链路状态检测功能，并且该端口收发数据正常，则显示正常；若对端没有收到该设备发送的检测报文则显示发送故障；若该设备没有收到对端发送的检测报文则显示接收故障。如果没有开启端口链路检测功能，则显示不使能。

6.7 静态组播地址表

介绍

可以静态配置组播地址表，按照<组播 MAC 地址、VLAN 号、组播成员端口>格式配置一个表项添加到组播地址表中。组播报文通过查找此表项相应的成员端口进行转发。

该设备最多支持 256 个组播表项。

Web 页面配置

1、使能静态组播，如图 48 所示；

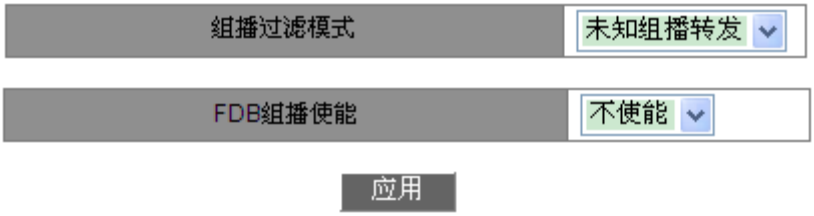

图 48 使能静态组播

组播过滤模式

配置选项：未知组播转发/未知组播丢弃

默认配置：未知组播转发

功能：配置未知组播的处理方式。

描述：未知组播报文指未静态添加并未通过 IGMP Snooping、GMRP 学习的报文。未知组播转发指在该报文的 VLAN 中广播该未知组播报文；未知组播丢弃指丢弃未知组播报文。

FDB 组播使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能静态组播，IGMP Snooping 与静态组播不能同时使能。

2、添加静态组播表项，如图 49 所示；

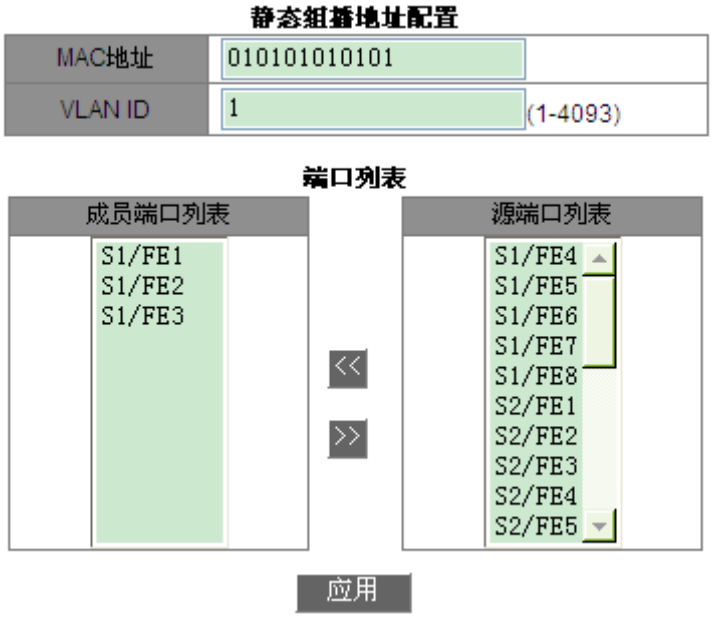

图 49 添加静态组播地址表项

MAC 地址

配置格式：HHHHHHHHHHHH (H 为一个十六进制数)

功能：配置组播组地址，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：配置该静态组播表项的 VLAN ID，属于该 VLAN 的成员端口可以转发该组播报文，否则无法转发该组播报文。

成员端口列表

选择该组播地址的成员端口，如果某端口所连接的主机需要固定接收某个组播组数据，可以配置该端口静态加入组播组成为静态成员端口。

3、查看、修改以及删除静态组播表项，如图 50 所示。

静态组播地址列表

序号	MAC地址	VLAN ID	成员端口
○	03-01-01-01-01-01	2	S1/FE1 S1/FE4
○	01-01-01-01-01-01	1	S1/FE1 S1/FE2 S1/FE3

添加 删除 修改

图 50 静态组播表项操作

静态组播地址列表显示 MAC 地址、VLAN ID 以及成员端口。选择其中任意表项点击<删除>按钮便成功删除该表项；点击<修改>按钮便可以修改该表项的成员端口。

6.8 IGMP Snooping

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。

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。

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)。

Web 页面配置

1、使能 IGMP Snooping 协议，如图 51 所示；

图 51 使能 IGMP Snooping

IGMP 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 IGMP Snooping 功能，IGMP Snooping 与静态组播/GMRP 不能同时使能。

自动查询使能

配置选项：使能/不使能

默认配置：不使能

功能：交换机是否参与查询器的选举。

描述：只有使能了 IGMP Snooping 协议，才能选择使能自动查询功能。

注意：

最好至少一台交换机使能自动查询功能。

IGMP Cross 状态

配置选项：使能/不使能

默认配置：不使能

功能：使能可以实现 report 报文和 leave 报文在 DT-Ring 环端口的转发。

2、查看组播成员列表，如图 52 所示；

组播成员列表

MAC地址	VLAN ID	成员端口
01-00-5E-7F-FF-FA	1	S1/FE1
01-00-5E-0A-18-03	1	S1/FE1
01-00-5E-51-09-08	1	S1/FE1

图 52 IGMP Snooping 成员列表

组播成员列表

组合显示：{ MAC 地址，VLAN ID，成员端口 }

通过 IGMP Snooping 动态学习到的 FDB 组播表，其中 VLAN ID 是指成员端口所在的 VLAN ID。

典型应用举例

如图 53 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；

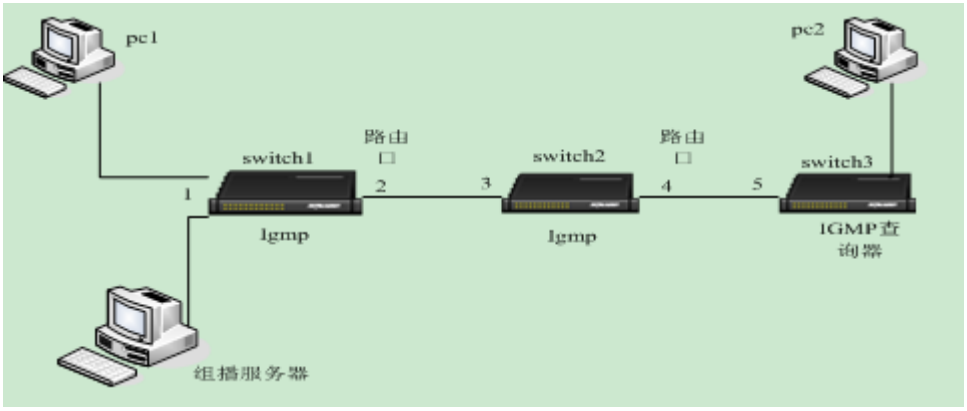

图 53 IGMP Snooping 应用举例

- 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。

6.9 ACL 配置

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。

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，各条 ACL 配置表项之间无任何依赖关系。

在多条 ACL 配置表项内，设备将按照表项序号从小到大的顺序将数据与逐条 ACL 配置表项对比，一旦数据遇到满足条件的第一条 ACL，将立即执行相应的动作，不再受之后的 ACL 表项影响，如图 54 所示。

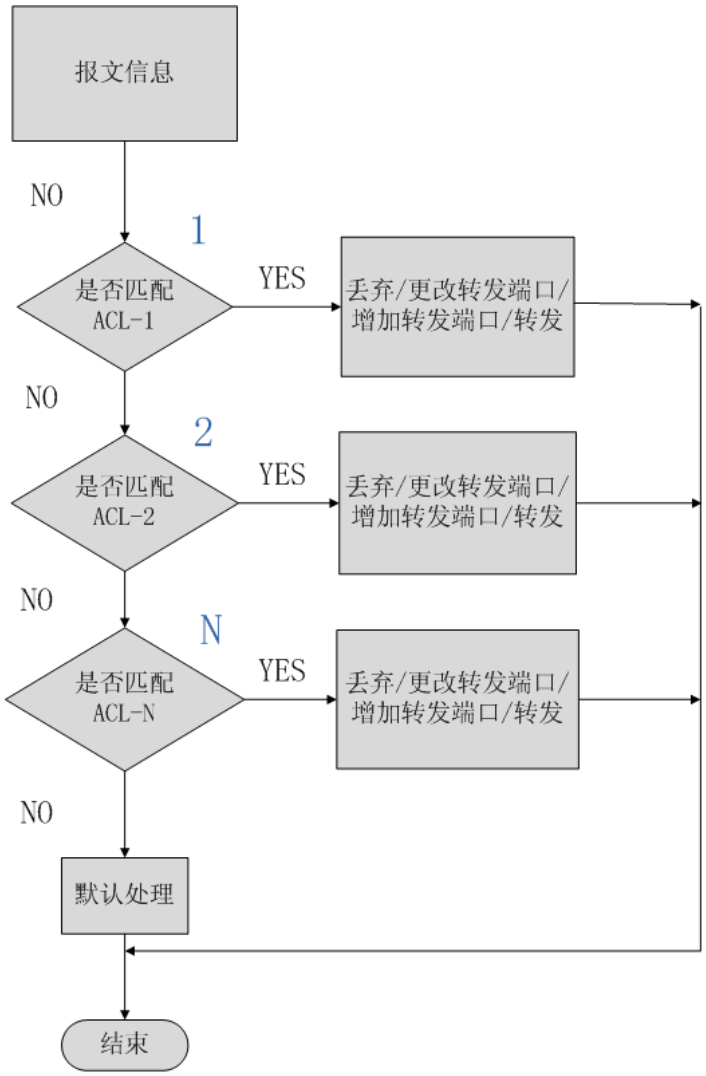

图 54 ACL 匹配流程图

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。

Web 页面配置

1、添加 ACL 配置表项

点击<添加表项>按钮添加 ACL 配置表项，如图 55 所示；

图 55 添加 ACL 配置表项

2、配置 ACL 表项参数，如图 56 所示；

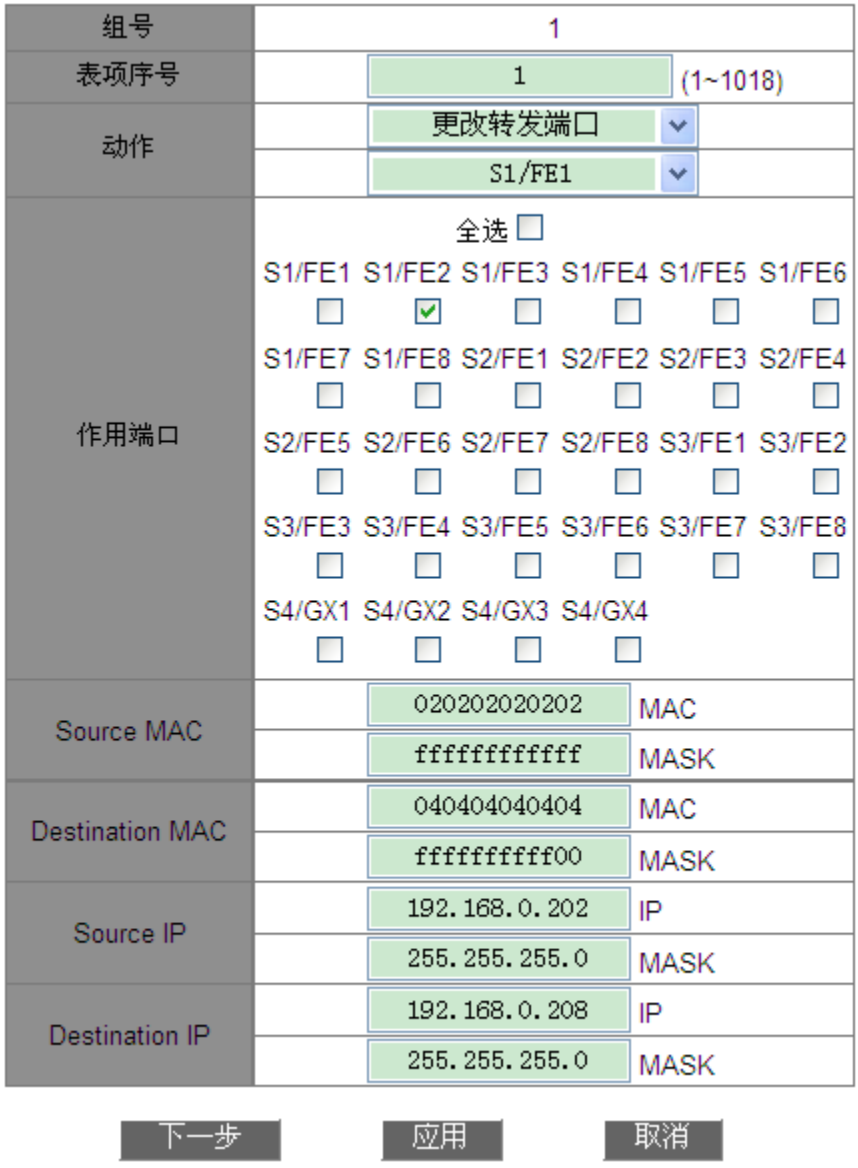

图 56 配置 ACL 表项参数 1

ACL 表项参数众多，不断点击按钮<下一步>将出现 ACL 表项其余参数，如图 57、图 58 和图 59 所示；

表项参数配置

Ethernet Type	1537	(1537~65535)
TOS/DSCP	7	(0~255)
IP Protocol	6	(0~255)
IP TTL	2	(0~3)
Max ICMP	1000	(0~1023)
TCP Flag	60	(0~63)
ICMP Type Code	5000	(0~65535)
Vlan ID		(1~4093)
Vlan ID Range 0	5 ~ 16	(1~4093)
Vlan ID Range 1	~	(1~4093)
Vlan ID Range 2	~	(1~4093)
Vlan ID Range 3	~	(1~4093)

上一步 下一步 应用 取消

图 57 配置 ACL 表项参数 2

表项参数配置

Source L4 Port	65000	(1~65535)
Src Port Range 0	~	(1~65535)
Src Port Range 1	~	(1~65535)
Src Port Range 2	~	(1~65535)
Src Port Range 3	~	(1~65535)
Destination L4 Port	21	(1~65535)
Dst Port Range 0	~	(1~65535)
Dst Port Range 1	~	(1~65535)
Dst Port Range 2	~	(1~65535)
Dst Port Range 3	~	(1~65535)
L2 Format	None	
L3 Format	None	
L4 Format	None	
Same IP	Disable	
Same L4 Port	Disable	
TCP Sequence Zero	Disable	

上一步 下一步 应用 取消

图 58 配置 ACL 表项参数 3

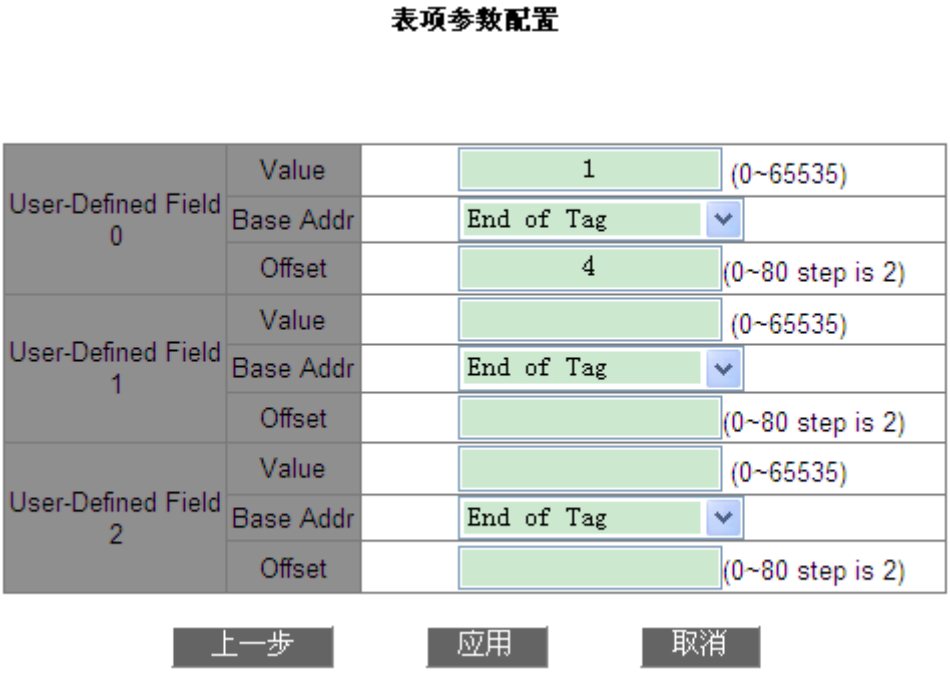

图 59 配置 ACL 表项参数 4

组号

强制配置：1

表项序号

配置范围：1~1018

功能：配置 ACL 表项的序列号，最多可配置 1023 条 ACL 表项。设备中有多条 ACL 表项时，会按照表项序号从小到大的顺序将数据与逐条 ACL 表项匹配。

动作

配置选项：丢弃/更改转发端口/增加转发端口/转发

默认配置：丢弃

功能：端口对匹配该条 ACL 表项成功的报文的处理方式。丢弃：匹配该条 ACL 表项成功的报文将被丢弃。更改转发端口：匹配该条 ACL 表项成功的报文将被转发到更改后的端口，更改后的端口在下面的下拉表中选择。增加转发端口：匹配该条 ACL 表项成功的报文除可正常转发至目的端口外，还可以增加转发至下面的下拉表中选择的端口中。转发：匹配该条 ACL 表项成功的报文将被转发至目的端口。

作用端口

配置选项：全部端口/任意一个或多个指定端口

功能：本条 ACL 表项所作用的端口。

Source MAC

组合配置：{ MAC 地址，MAC 掩码 }

配置格式：{HHHHHHHHHHHH，HHHHHHHHHHHH } (H 为一个十六进制数)功能：配置 ACL 条件参数-源 MAC 地址和源 MAC 掩码，当端口收到的报文中的源 MAC 满足此条件时，该条件匹配成功。

Destination MAC

组合配置：{ MAC 地址，MAC 掩码 }

配置格式：{HHHHHHHHHHHH，HHHHHHHHHHHH } (H 为一个十六进制数)

功能：配置 ACL 条件参数-目的 MAC 地址和目的 MAC 掩码，当端口收到的报文中的目的 MAC 满足此条件时，该条件匹配成功。

Source IP

组合配置：{IP 地址，IP 掩码}

配置格式：{A.B.C.D，A.B.C.D }

功能：配置 ACL 条件参数-源 IP 地址和源 IP 掩码，当端口收到的报文中的源 IP 满足此条件时，该条件匹配成功。

Destination IP

组合配置：{IP 地址，IP 掩码}

配置格式：{A.B.C.D，A.B.C.D}

功能：配置 ACL 条件参数-目的 IP 地址和目的 IP 掩码，当端口收到的报文中的目的 IP 满足此条件时，该条件匹配成功。

Ethernet Type

配置范围：1537~65535

功能：配置 ACL 条件参数-以太网类型值，当端口收到的报文中的对应字段值与此条件一致时，该条件匹配成功。

TOS/DSCP

配置范围：0~255

功能：配置 ACL 条件参数-服务类型值，当端口收到的报文中的对应字段值与此条件一致时，该条件匹配成功。

IP Protocol

配置范围：0~255

功能：配置ACL 条件参数-IP 报文的协议值，当端口收到的报文中的对应字段值与条件一致时，该条件匹配成功。

IP TTL

配置范围：0~3

功能：配置 ACL 条件参数-IP 报文的 TTL 字段，其中 0~3 与 TTL 值对应关系为：0 对应 TTL 值 0；1 对应 TTL 值 1；2 对应 TTL 值 2~254；3 对应 TTL 值 255；当端口收到的报文中对应字段值满足此条件时，该条件匹配成功。

Max ICMP

配置范围：0~1023

功能：配置 ACL 条件参数-Max ICMP 值，此字段为 ICMP 报文数据部分长度值，当收到的 ICMP 报文的数据部分长度大于此条件参数值时，该条件匹配成功。

TCP Flag

配置范围：0~63

功能：配置 ACL 条件参数-TCP 标识值，当端口收到的报文对应字段值与此条件一致时，该条件匹配成功。

ICMP Type Code

配置范围：0~65535

功能：配置 ACL 条件参数-ICMP 报文类型值，当端口收到的报文对应字段值与此条件一致时，该条件匹配成功。

Vlan ID

配置范围：1~4093

功能：配置 ACL 条件参数-报文的 Vlan ID 字段值，当端口收到的报文对应字段值与此条件一致时，该条件匹配成功。

Vlan ID Range (0~3)

组合配置：{X~Y}（X，Y 取值范围为 1~4093 且 X≤Y，X、Y 分别表示 ACL 条件中报文的 Vlan ID 的上下限值）

功能：配置 ACL 条件参数-报文的 Vlan ID 的范围值，当端口收到的报文的 Vlan ID 属于此配置范围时，该条件匹配成功。

Source L4 Port

配置范围：1~65535

功能：配置 ACL 条件参数-4 层协议报文的源端口号，当端口收到的报文的 L4 源端口号与此条件一致时，该条件匹配成功。

Src Port Range (0~3)

组合配置：{X~Y}（X，Y 取值范围为 1~65535 且 X≤Y，X、Y 分别表示 ACL 条件中 L4 源端口号的上下限值）

功能：配置 ACL 条件参数-4 层协议报文的源端口号的范围，当端口收到的报文的 L4 源端口号属于此配置范围时，该条件匹配成功。

Destination L4 Port

配置范围：1~65535

功能：配置 ACL 条件参数-4 层协议报文的目的端口号，当端口收到的报文的 L4 目的端口号与此条件一致时，该条件匹配成功。

Dst Port Range (0~3)

组合配置：{X~Y}（X，Y 取值范围为 1~65535 且 X≤Y，X、Y 分别表示 ACL 条件中 L4 目的端口号的上下限值）

功能：配置 ACL 条件参数-4 层协议报文的目的端口号的范围，当端口收到的报文的 L4 目的端口号属于此配置范围时，该条件匹配成功。

L2 Format

配置选项：None/L2_Others/Ethernet_Ⅱ/IEEE_802_2_SNAP

默认配置：None

功能：配置 ACL 条件-二层以太网帧格式。None 表示不匹配此条件；L2_ Others 表示除 Ethernet_Ⅱ和 IEEE_802_2_SNAP 以外的其它以太网帧格式。当端口收到的报文与此条件定义的以太网帧格式一致时，该条件匹配成功。

L3 Format

配置选项：None/L3_Others/IPV4_without_frag/IPV6_without_exten

默认配置：None

功能：配置 ACL 条件-三层互联网协议。None 表示不匹配此条件；L3_ Others 表示除 IPV4_without_frag 和 IPV6_without_exten 以外的其它三层互联网协议。当端口收到的报文与此条件定义的三层互联网协议一致时，该条件匹配成功。

L4 Format

配置选项：None/L4_Others/TCP/UDP/ (ICMP/IGMP)

默认配置：None

功能：配置 ACL 条件-四层协议类型。None 表示不匹配此条件；L4_ Others 表示除 TCP、UDP、ICMP 和 IGMP 以外的其它协议类型。当端口收到的报文与此条件定义的四层协议类型一致时，该条件匹配成功。

Same IP

配置选项：Disable /True/False

默认配置：Disable

功能：配置 ACL 条件-检查收到的报文源 IP 地址和目的 IP 地址是否相同。Disable 表示不检查收到的报文源 IP 地址和目的 IP 地址是否相同，即不匹配此条件。True 表示收到的报文源 IP 地址和目的 IP 地址相同，即当端口收到的报文中源 IP 地址与目的 IP 地址相同时，此条件匹配成功。False 表示收到的报文源 IP 地址和目的 IP 地址不相同，即当端口收到的报文中源 IP 地址与目的 IP 地址不同时，此条件匹配成功。

Same L4 Port

配置选项：Disable/True/False

默认配置：Disable

功能：配置 ACL 条件-检查收到的报文源 L4 端口号和目的 L4 端口号是否相同。Disable 表示不检查收到的报文源 L4 端口号和目的 L4 端口号是否相同，即不匹配此条件。True 表示收到的报文源 L4 端口号和目的 L4 端口号相同，即当端口接收到的报文中源 L4 端口号与目的 L4 端口号相同时，此条件匹配成功。False 表示收到的报文源 L4 端口号和目的 L4 端口号不相同，即当端口接收到的报文中源 L4 端口号与目的 L4 端口号不同时，此条件匹配成功。

TCP Sequence Zero

配置选项：Disable/True/False

默认配置：Disable

功能：配置 ACL 条件-检查收到的报文 TCP Sequence 字段是否为 0。Disable 表示不检查收到的报文 TCP Sequence 字段是否为 0，即不匹配此条件。True 表示收到的报文 TCP Sequence 字段为 0，即当端口接收到的报文中 TCP Sequence 字段为 0 时，此条件匹配成功。False 表示收到的报文 TCP Sequence 字段不为 0，即当端口接收到的报文中 TCP Sequence 字段不为 0 时，此条件匹配成功。

User-Defined Field (0-2)

组合配置：{Value，Base Addr，Offset }

配置范围、选项：

Value ：1~65535

Base Addr：End of Tag(默认配置)/End of EthType/End of IP Header

Offset：0~80 步长为 2

功能：用户自定义 ACL 条件中的字段。Vlaue 表示要匹配的值；Base Addr 表示报文的基准位置，End of Tag 表示以报文中 Tag 标签字段尾部为基准，End of EthType 表示以报文中 EthType 字段尾部为基准，End of IP Header 表示以报文中 IP 头字段尾部为基准；Offset 表示 Value 相对于基准位置 Base Addr 的偏移值。当端口收到报文中相对于 *Base Addr* 偏移 *Offset* 的值为 *Value* 时，此条件匹配成功。

说明：

上述中 ACL 表项条件至少需配置一条，但并不需全部配置，如果只想要匹配其中的某项条件，其他条件配置可以为空。

3、查看 ACL 表项列表

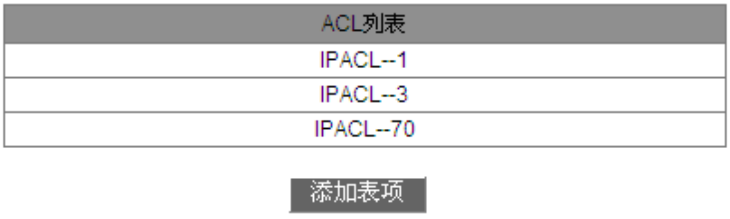

图 60 ACL 表项列表

点击图 60 中某一 ACL 列表，可以修改 ACL 表项配置或删除该 ACL 表项，如图 61 所示；

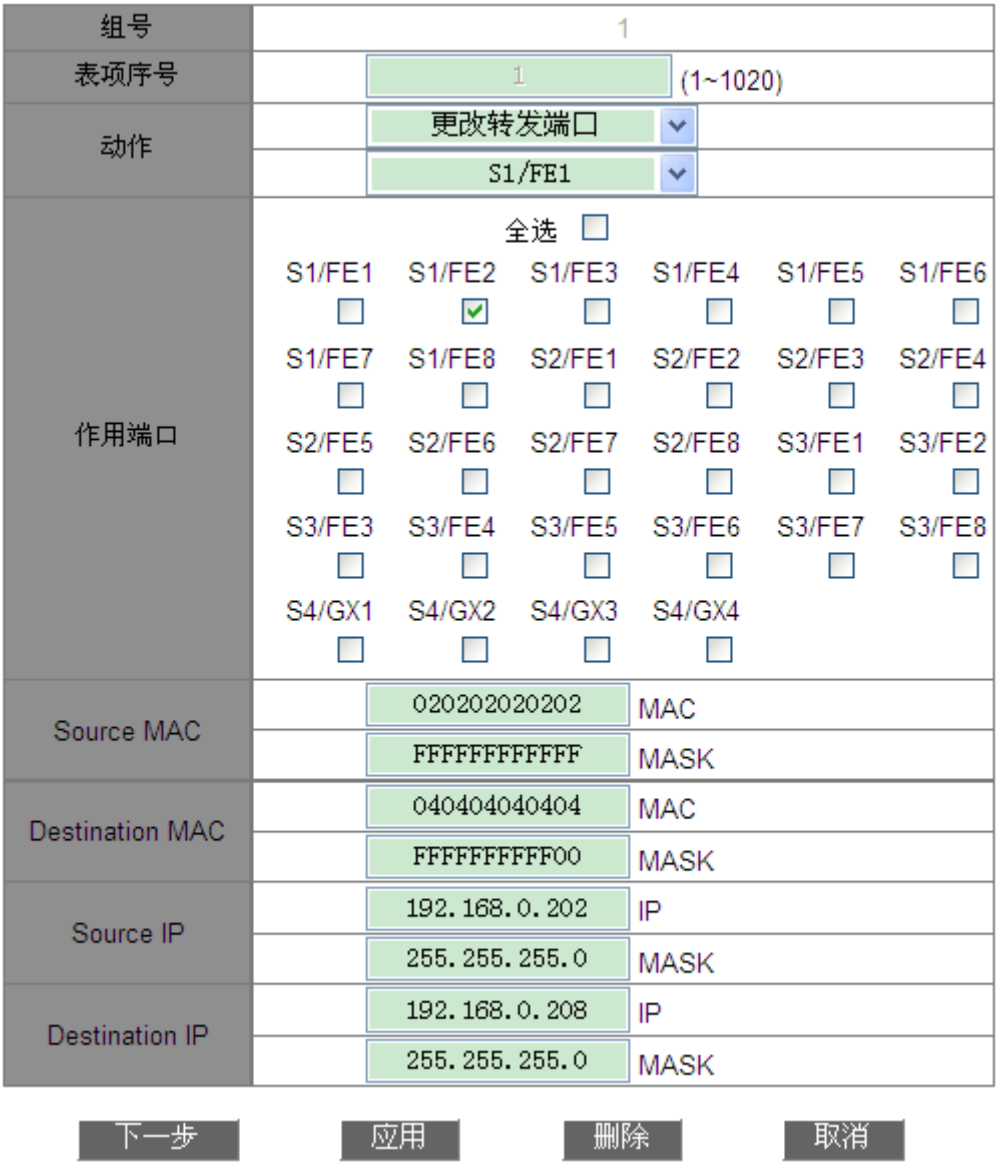

图 61 修改/删除 ACL 表项

修改 ACL 表项参数配置，点击<应用>按钮后修改生效；点击<删除>按钮便可成功删除该 ACL 表项。

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，并将此报文在端口 1 转发。

配置如下：

1、配置端口动作为更改转发端口，并选择端口 1 为转发端口，如图 56 所示；

2、配置作用端口为端口 2，如图 56 所示；

3、配置 ACL 表项的源 MAC 地址为 020202020202，MAC 掩码为 FFFFFFFFFFFF，如图 56 所示；

4、其余参数为默认配置或空。

6.10 ARP 配置

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。

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。

ARP 表项最多支持 512 条，其中静态表项最多可以配置 256 条。当 ARP 表项超过 512 条时，新表项将覆盖旧动态表项。

Web 页面配置

1、配置 ARP 老化时间，如图 62 所示；

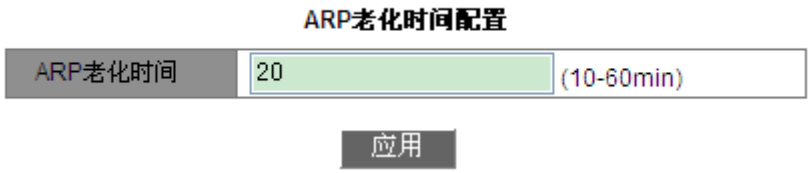

图 62 配置老化时间

ARP 老化时间

配置范围：10 ~ 60min

默认配置：20min

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。

2、静态配置 ARP 地址表项，如图 63 所示；

图 63 静态配置 ARP 表项

ARP 地址配置

组合配置：{ IP 地址，MAC 地址 }

配置格式：{ A.B.C.D，HHHHHHHHHHHH } (H 为一个十六进制数)

功能：静态配置 ARP 地址解析表项。

注意：

- 配置的静态地址表项中 IP 地址必须和交换机 IP 地址在同一网段中；
- 配置的静态表项中 IP 地址为交换机本身 IP 地址时，系统会自动对应该交换机的 MAC 地址；
- 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。

3、查看或删除 ARP 地址表项，如图 64 所示；

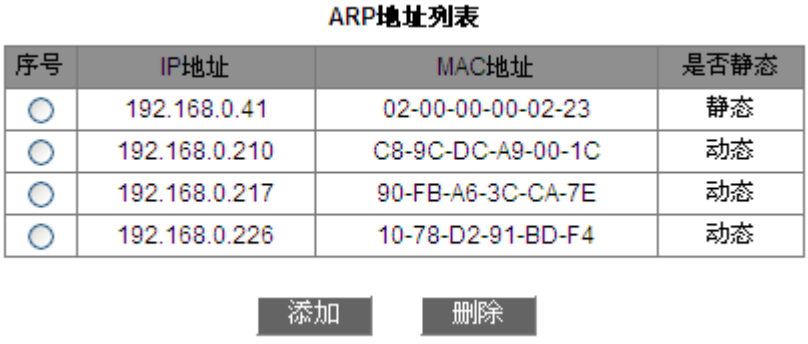

图 64 ARP 地址映射表

ARP 地址列表

组合显示：{ IP 地址，MAC 地址，状态 }

功能：显示 ARP 表项，包括静态表项和动态表项。

用法：通过序号选中一个静态表项，点击<删除>按钮即可成功删除此表项。

注意：

不能删除动态学习的 ARP 表项。

6.11 SNMP 配置

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。

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。

说明

该系列设备SNMP Agent支持SNMP v2版本，SNMP v2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 v2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。

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65所示：

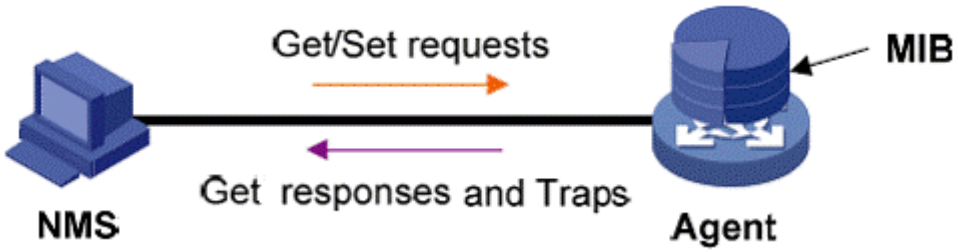

图 65 NMS、Agent 和 MIB 关系图

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 66 所示，被管理对象 A 的 OID 为 1.2.1.1。

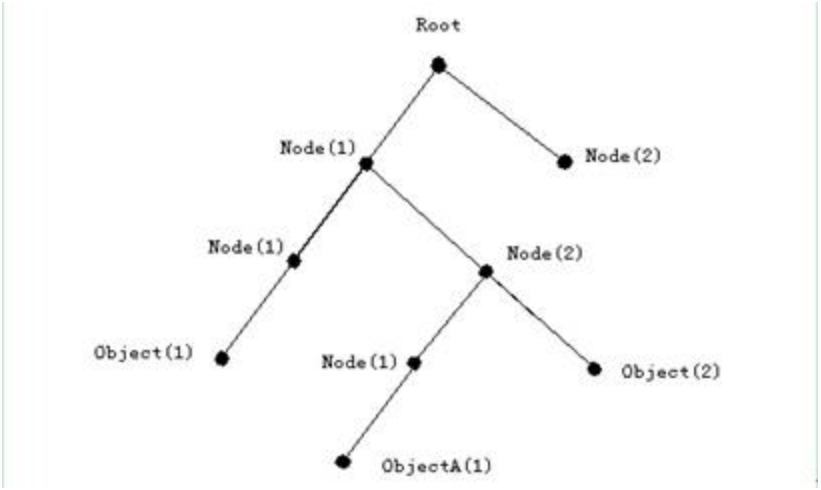

图 66 MIB 树结构

Web 页面配置

1、使能 SNMP 协议，如图 67 所示；

图 67 使能 SNMP 协议

SNMP 使能

配置选项：使能/不使能

默认配置：使能

功能：是否使能 SNMP 协议。

2、配置访问权限，如图 68 所示；

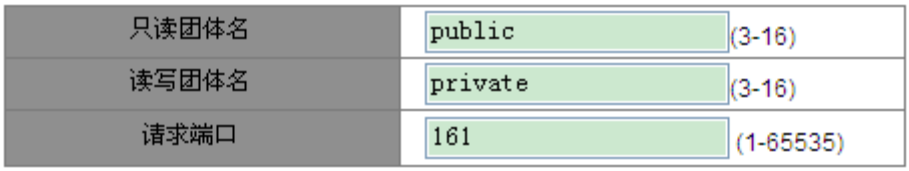

图 68 访问权限配置

只读团体名

配置范围：3~16 个字符

默认配置：public

功能：配置只读权限的团体名称。

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 库信息进行读取操作。

读写团体名

配置范围：3~16 个字符

默认配置：private

功能：配置可读写的团体名称。

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 库信息进行读写操作。

请求端口

配置范围：1~65535

默认配置：161

功能：配置接收 SNMP 请求的端口号。

3、Trap 配置，如图 69 所示；

图 69 Trap 配置

Trap 开关

配置选项：使能/不使能

默认配置：使能

功能：是否允许交换机发送 trap 消息。

Trap 端口号

配置选项：1~65535

默认配置：162

功能：配置发送 trap 报文消息的端口号。

服务器 IP 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，最多支持 5 个 Trap 服务器地址。

4、查看管理服务器 IP 地址，如图 70 所示；

管理服务器

服务器IP地址1	192.168.0.23	(IP 地址)
服务器IP地址2		(IP 地址)
服务器IP地址3		(IP 地址)

图 70 管理服务器 IP 地址

服务器 IP 地址不需要手动配置，只要在服务器上运行网管软件，并对该设备的 MIB 节点信息进行读写操作，服务器的 IP 地址便会自动显示出来。

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 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 71 所示；

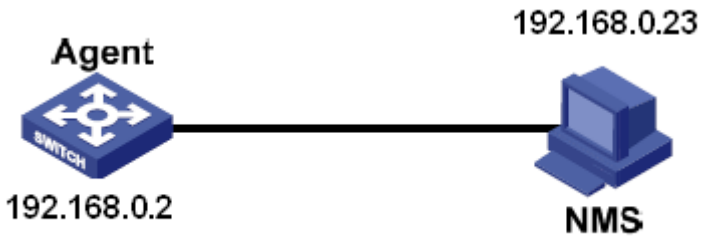

图 71 SNMP 配置举例

Agent 配置如下：

1、使能 SNMP 协议，见图 67；

2、配置访问权限，只读团体名为 public，读写团体名为 private，请求端口为 161，见图 68；

3、使能 Trap 开关，Trap 端口号为 162，服务器地址为 192.168.0.23，见图 69；

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”。

6.12 DT-Ring 配置

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。

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)。

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

说明：

若主站中未配置主端口，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。

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。

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 72 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。

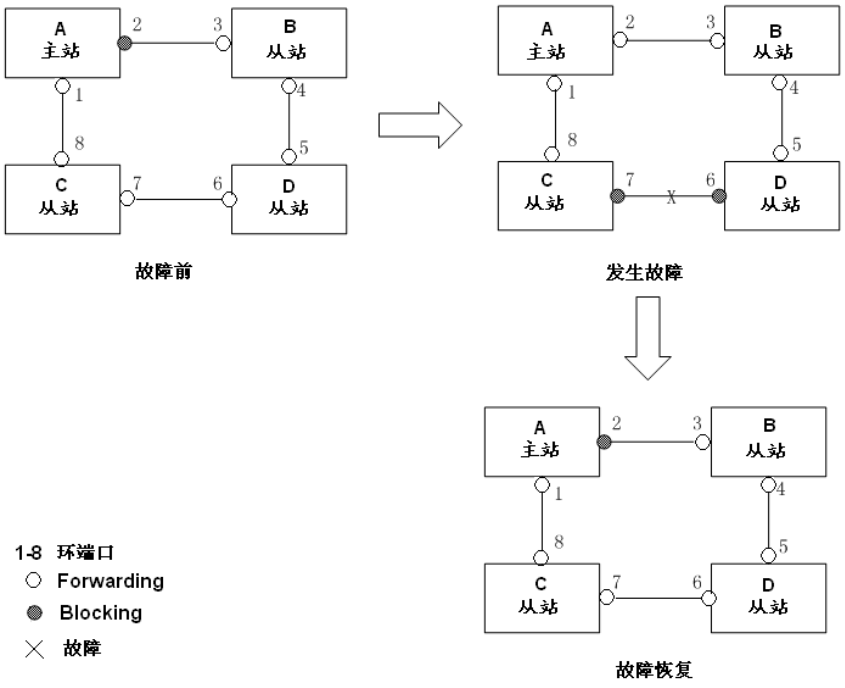

图 72 CD 链路发生故障

说明：

若配置主站 A 的端口 1 为主端口，发生故障和故障恢复过程与以上过程一致。

4、若 AC 链路发生故障，如图 73 所示；

a) 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；

b) AC 链路故障恢复之后：

- 若主站 A 未配置主端口，则仍保持端口 1 为 Blocking 状态，端口 8 为 Forwarding 状态，链路不进行倒换。
- 若主站 A 配置端口 1 为主端口，在环闭状态时，主端口必为 Forwarding 状态，则端口 1 切换为 Forwarding 状态，端口 8 为 Forwarding 状态，端口 2 切换为 Blocking 状态，链路发生倒换。

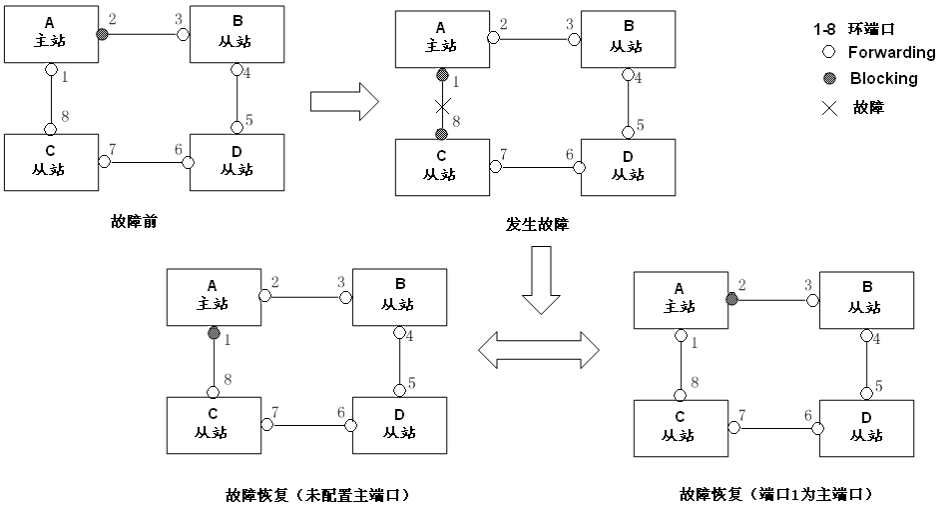

图 73 DT-Ring 链路故障

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 74 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。

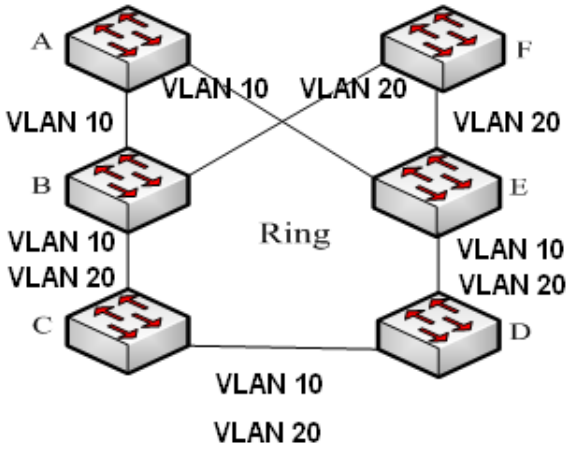

图 74 DT-Ring-VLAN

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 75 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。

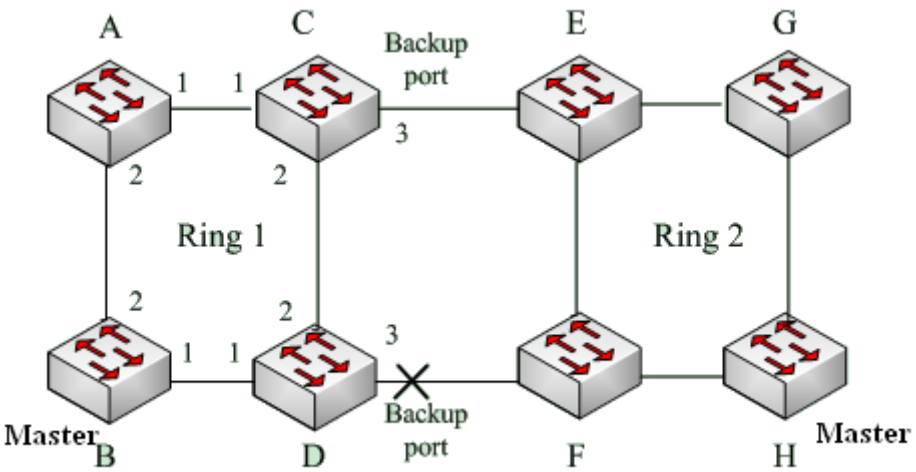

图 75 DT-Ring+拓扑

注意：

链路状态的改变影响备份端口的状态。

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。

Web 页面配置

1、配置冗余环模式，如图 76 所示；

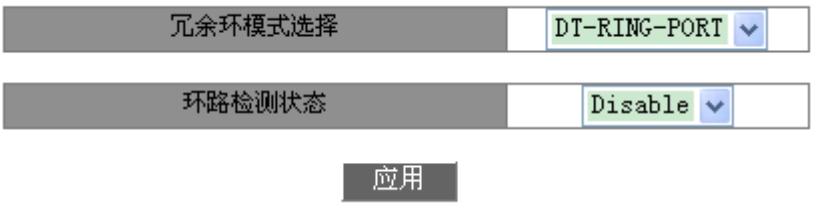

图 76 冗余环模式配置

冗余环模式选择

配置选项：DT-RING-PORT/DT-RING-VLAN

默认配置：DT-RING-PORT

功能：选择冗余环的模式。

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 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。

环路检测状态

配置选项：Enable/Disable

默认配置：Disable

功能：是否使能环路检测状态。

描述：使能环路检测状态后，环路将自动检测。当非环端口收到环协议报文时端口将被 Lock 掉，用户请慎用此功能。

2、创建 DT-Ring 环，如图 77 所示；

图 77 创建 DT-Ring 环

点击<增加>按钮创建 DT-Ring 并对其进行配置。

3、配置 DT-Ring-Port 和 DT-Ring -VLAN，如图 78、图 79 所示；

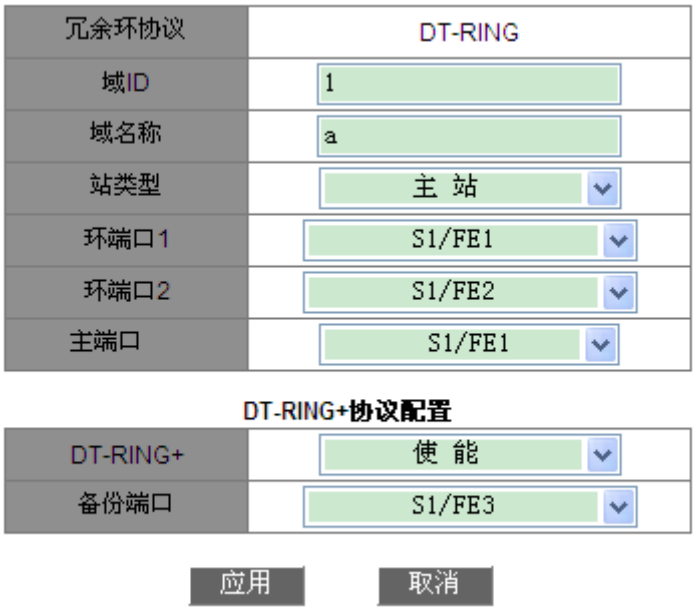

图 78 DT-Ring-Port 配置

图 79 DT-Ring-VLAN 配置

冗余环协议

强制配置：DT-Ring

域 ID

配置范围：1~32

功能：域号用来区分不同的环，一台交换机上最多可以配置 16 个基于端口的环或 8 个基于 VLAN 的环。

域名称

配置范围：1~31 个字符

功能：配置域名称。

站类型

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、备份端口配置与端口聚合互斥，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；
- DT-Ring 环端口、备份端口与端口镜像配置互斥，DT-Ring 环端口和备份端口不能配置为镜像端口和被镜像端口，镜像端口和被镜像端口也不能配置为 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。

主端口

配置选项：不使能/交换机中所有端口

默认配置：不使能

功能：配置主站的主端口。

说明：主端口在环闭时强制为 Forwarding 状态。

注意：

- 只有在环闭状态时，主端口才生效；
- 只有主站可以配置主端口，且主端口必须是两个环端口之一。

DT-Ring+

配置选项：使能/不使能

默认配置：不使能

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。

添加 VLAN 列表

配置选项：已创建的 VLAN 列表

功能：选择当前 DT-Ring-VLAN 环管理的 VLAN。

配置完成后，“DT-Ring 列表”中显示已创建的环列表，如图 80 所示；

图 80 DT-Ring 列表

4、查看、修改 DT-Ring 环配置

点击图 80 中相应 DT-Ring 选项，可以查看该环配置，并对其进行修改如图 81 所示；

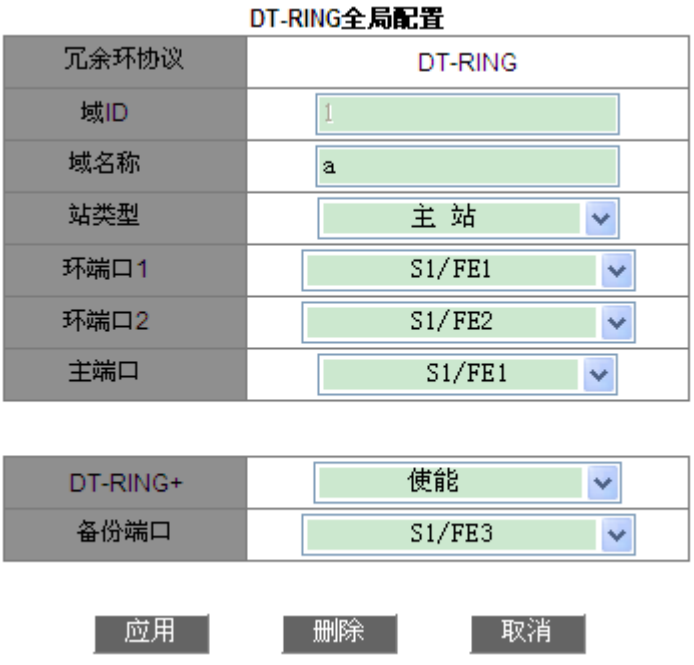

图 81 查看并修改 DT-Ring 配置

修改后点击<应用>按钮即可成功修改；点击<删除>按钮即可删除该 DT-Ring 配置表项。

4、显示 DT-Ring 环状态和各端口状态，如图 82 所示；

环状态列表

冗余环协议	DT-RING
环端口1	阻塞
环端口2	转发
环状态	环闭
环倒换次数清零	清 除

冗余环协议	DT-RING+
设备IP	192.168.0.119
设备MAC地址	00-1E-CD-10-23-38
备份端口状态	阻塞
设备IP	192.168.0.109
设备MAC地址	00-00-EE-EE-02-05
备份端口状态	阻塞

图 82 DT-Ring 状态查看

典型配置举例

如图 75 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：Ring；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 78；

交换机 B 配置过程：

2、域 ID：1；域名称：Ring；环端口选择 1 和 2，不配置主端口；站类型：主站；DT-Ring+不使能，不需配置备份端口，见图 78；

交换机 C、D 配置过程：

3、域 ID：1；域名称：Ring；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 78；

交换机 E、F、G 配置过程：

4、域 ID：2；域名称：Ring；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 78；

交换机 H 配置过程：

5、域 ID：2；域名称：Ring；环端口选择 1 和 2，不配置主端口；站类型：主站；DT-Ring+不使能，不需配置备份端口，见图 78；

6.13 RSTP/STP 配置

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。

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；

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。

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 6 所示；

表 6 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--forwarding 状态转换延时；

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。配置消息比较级原则：

- 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。

Web 配置

1、全局使能 STP/RSTP 协议，如图 83 所示；

图 83 RSTP/STP 协议使能

协议类型

配置选项：不使能/RSTP/STP

默认配置：不使能

功能：是否使能生成树协议并选择协议类型。

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 DT-Ring-VLAN 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。

2、配置该网桥的时间参数，如图 84 所示；

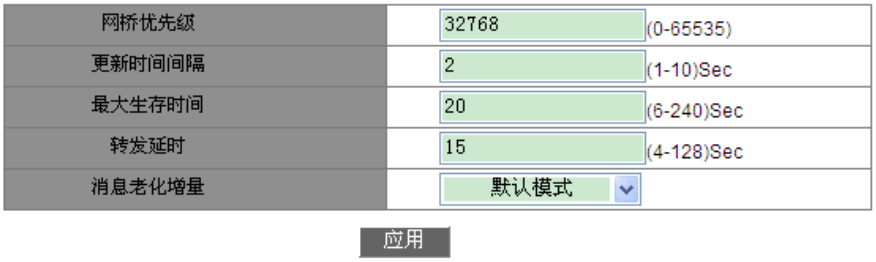

图 84 配置网桥时间参数

网桥优先级

配置范围：0~65535，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。

更新时间间隔

配置范围：1~10s

默认配置：2s

功能：配置 Hello Time 值，即发送 BPDU 消息的时间间隔。

最大生存时间

配置范围：6~240s

默认配置：20s

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。

转发延时

配置范围：4~128s

默认配置：15s

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

消息老化增量

配置选项：强制模式/默认模式

默认配置：默认模式

功能：配置 BPDU 消息经过一个网桥时如何修改 message age 参数。

描述：强制模式时，该参数加 1；

默认模式时，该参数加 max (max age time/16, 1)

Forward Delay Time，Max Age Time，Hello Time 应满足以下关系：

2 x (Forward Delay Time – 1.0 seconds) >= Max Age Time；

Max Age Time >= 2 x (Hello Time + 1.0 seconds)。

3、使能 RSTP 协议端口的信息配置，如图 85 所示；

端口信息配置

端口	协议状态	优先级(0~255)	路径成本(1~200000000)	成本自动计算
S1/FE1	使能	128	2000000	是
S1/FE2	不使能	128	2000000	是
S1/FE3	使能	128	2000000	是
S1/FE4	使能	128	2000000	是
S1/FE5	使能	128	2000000	是
S1/FE6	不使能	128	2000000	是
S1/FE7	不使能	128	2000000	是
S1/FE8	不使能	128	2000000	是
S2/FE1	不使能	128	2000000	是
S2/FE2	不使能	128	2000000	是
S2/FE3	不使能	128	2000000	是
S2/FE4	不使能	128	2000000	是
S2/FE5	不使能	128	2000000	是
S2/FE6	不使能	128	2000000	是
S2/FE7	不使能	128	2000000	是
S2/FE8	不使能	128	2000000	是
S3/FE1	不使能	128	2000000	是
S3/FE2	不使能	128	2000000	是
S3/FE3	不使能	128	2000000	是
S3/FE4	不使能	128	2000000	是
S3/FE5	不使能	128	2000000	是
S3/FE6	不使能	128	2000000	是
S3/FE7	不使能	128	2000000	是
S3/FE8	不使能	128	2000000	是
S4/GX1	不使能	128	20000	是
S4/GX2	不使能	128	20000	是
S4/GX3	不使能	128	20000	是
S4/GX4	不使能	128	20000	是

应用

图 85 端口信息配置

协议状态

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 端口与端口镜像配置互斥，RSTP 端口不能配置为镜像端口和被镜像端口，镜像端口和被镜像的端口也不能配置为 RSTP 端口；
- RSTP 端口与端口聚合互斥，RSTP 端口不能加入聚合组，加入聚合组的端口不能配置为 RSTP 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 RSTP 端口不能配置为 DT-Ring-Port/DRP-Port 环端口、DT-Ring-Port/DRP-Port 备份端口；DT-Ring-Port/DRP-Port 环端口、DT-Ring-Port/DRP-Port 备份端口也不能配置为 RSTP 端口；
- 建议不要将隔离组中的端口同时配置为 RSTP 端口；RSTP 端口不要同时加入隔离组。

优先级

配置范围：0~255，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。

路径成本

配置范围：1~200000000

默认配置：2000000(十兆端口)，200000(百兆端口)，20000(千兆端口)

描述：端口路径成本是端口连接的路径开销，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。手动配置该值时，请把成本自动计算配置为否。

成本自动计算

配置范围：是/否

默认配置：是

描述：是表示端口路径成本采用默认值；否表示用户可以配置端口路径成本。

4、查看 RSTP 状态信息，如图 86 所示；

根桥信息

根桥MAC	00:2f:ab:00:00:10
根桥优先级	0x8000
根桥路径开销	0
根端口	None
最大生存时间(s)	20
Hello间隔(s)	2
转发延迟(s)	15

本桥信息

本桥MAC	00:2f:ab:00:00:10
本桥优先级	0x8000
本桥版本	2
最大生存时间(s)	20
Hello间隔(s)	2
转发延迟(s)	15

端口信息

端口	优先级	路径开销	角色	状态	链路状态
S1/FE1	0x80	2000000	Disabled	Discarding	Down
S1/FE3	0x80	2000000	Disabled	Discarding	Down
S1/FE4	0x80	2000000	Disabled	Discarding	Down
S1/FE5	0x80	2000000	Disabled	Discarding	Down

图 86 RSTP 状态信息

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 87 所示；

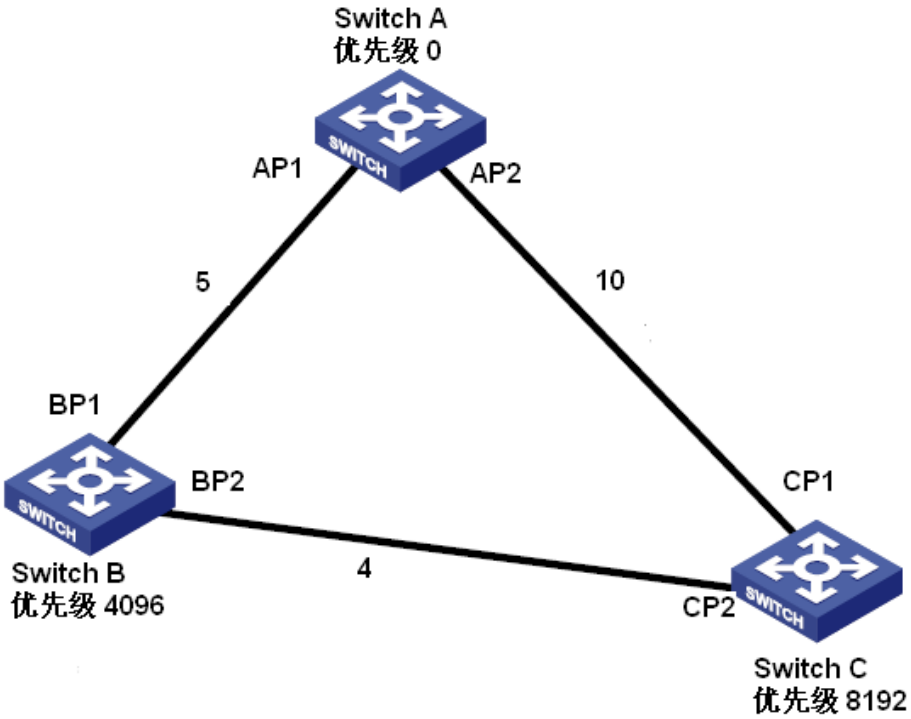

图 87 RSTP 举例

交换机 A 的配置：

1、优先级为 0，时间参数设为默认值，见图 84；

2、端口 1 的路径成本 5，端口 2 的路径成本 10，见图 85；

交换机 B 的配置：

1、优先级为 4096，时间参数设为默认值，见图 84；

2、端口 1 的路径成本 5，端口 2 的路径成本 4，见图 85；

交换机 C 的配置：

1、 优先级为 8192，时间参数设为默认值，见图 84；

2、 端口 1 的路径成本 10，端口 2 的路径成本 4，见图 85；

- 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；

6.14 RSTP/STP 透传

介绍

RSTP 协议遵循 IEEE 标准；DT-Ring/DRP 是本公司私有的冗余保护协议，与 RSTP 协议不能并存于一个网络中。为解决该问题，本公司提出了 RSTP/STP 透传功能。RSTP 透传使交换机保留其他冗余协议的同时能够透传 RSTP 协议报文，来保证链路配置满足工业网需求。

运行其他冗余协议的交换机通过使能端口的 RSTP 透传功能，便可接收并转发 RSTP 协议报文，可以将使能端口透传功能的交换机视为透明链路。

在图 88 中，交换机 A、B、C、D 组成一个 DT-Ring 环网，使能交换机 A、B、C、D 的端口透传功能保证交换机 E 和 F 可以相互接收到对方的 RSTP 协议报文，检测环路并计算生成树。

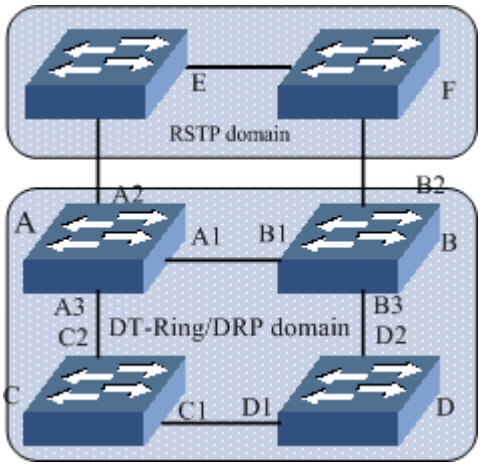

图 88 RSTP 透传应用

Web 页面配置

配置端口的 RSTP 透传，如图 89 所示；

端口	RSTP 透传
S1/FE1	不使能
S1/FE2	使能
S1/FE3	不使能
S1/FE4	不使能
S1/FE5	不使能
S1/FE6	使能
S1/FE7	使能
S1/FE8	不使能
S2/FE1	不使能
S2/FE2	不使能
S2/FE3	不使能
S2/FE4	不使能
S2/FE5	不使能
S2/FE6	不使能
S2/FE7	不使能
S2/FE8	不使能
S3/FE1	不使能
S3/FE2	不使能
S3/FE3	不使能
S3/FE4	不使能
S3/FE5	不使能
S3/FE6	不使能
S3/FE7	不使能
S3/FE8	不使能
S4/GX1	不使能
S4/GX2	不使能
S4/GX3	不使能
S4/GX4	不使能

应用

图 89 RSTP 透传配置表

RSTP 透传

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口 RSTP 透传功能。

注意：

使能 RSTP 协议的端口不可以使能 RSTP 透传功能。

典型配置举例

如图 88 所示组网情况，交换机 A、B、C、D 形成 DT-Ring 环，E、F 形成 RSTP 环，在 RSTP 环中整个 DT-Ring 环作为透传链路转发交换机 E 或 F 发送的 RSTP 协议报文。

- 交换机 A、B、C、D 配置为 DT-Ring 冗余环，配置过程详见“DT-Ring 配置”章节；
- 使能交换机 E、F 对应端口的 RSTP 协议，见图 83 和图 85；
- 使能交换机 A、B、C、D 中的 A1、A2、A3、B1、B2、B3、C1、C2、D1、D2 端口的 RSTP 透传功能，见图 89。

6.15 DRP

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。

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。

注意：

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：15 分钟内 CRC 报文数超过门限值。

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 7 所示：

表 7 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：15 分钟内 CRC 报文数与门限值的比值；

设备角色优先级：可在 Web 页面配置中具体配置。

将表 7 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下：

1、A、B、C 和 D 初始拓扑如图 90 所示，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；

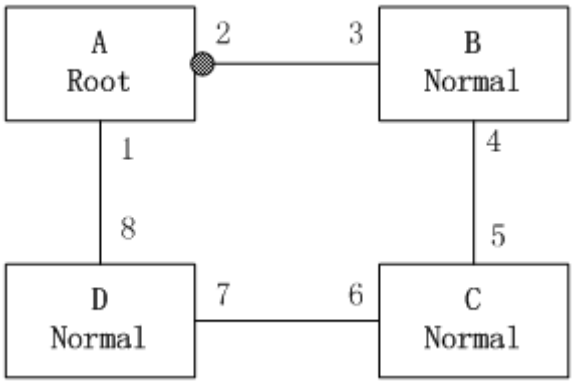

图 90 DRP 拓扑

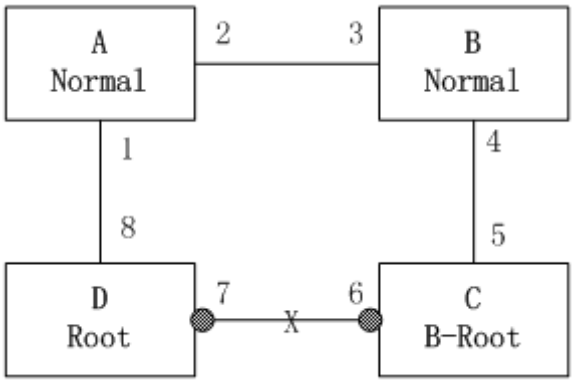

图 91 链路 CD 发生故障

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，如图 91 所示。

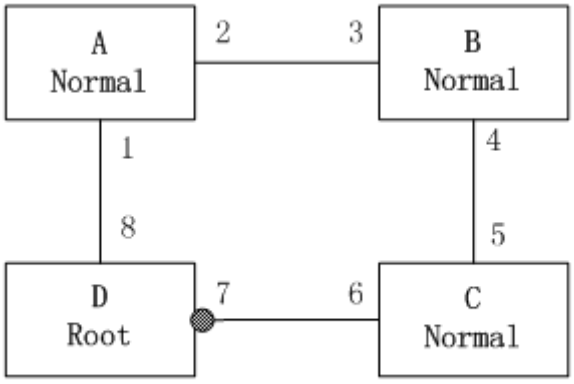

图 92 链路 CD 恢复

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，环端口 7 仍为 blocking；交换机 C 的环端口 6 此时为 Link up，故置端口 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。

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 93 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。

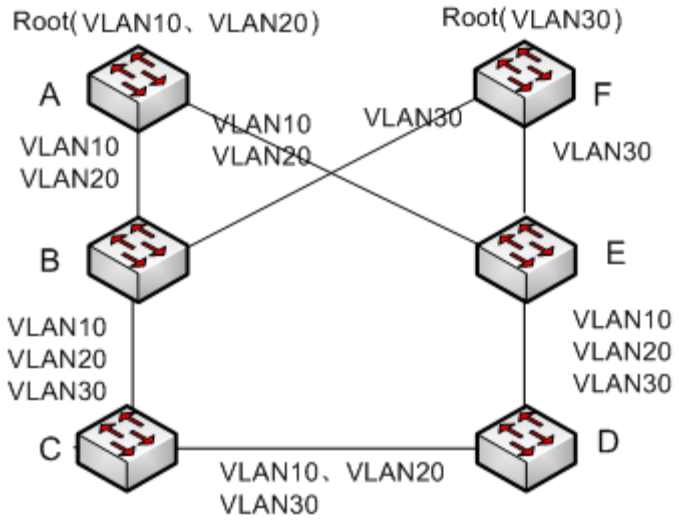

图 93 DRP-VLAN-Based

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 94 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。

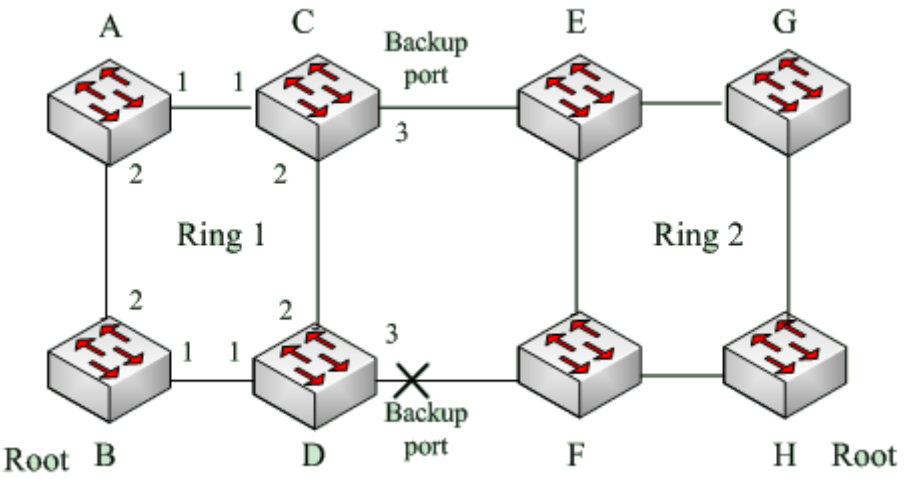

图 94 DRP 备份

注意：

链路状态的改变会影响备份端口的状态。

6.16 DHP

介绍

DHP(Dual Homing Protocol)：即双归链路协议，如图 95 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。

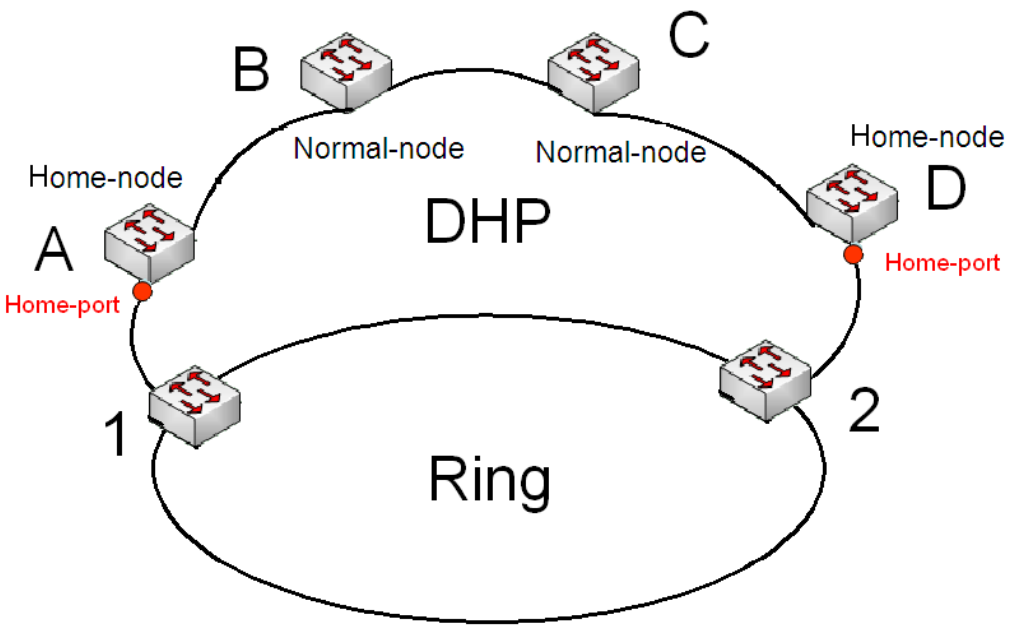

图 95 DHP 协议运用

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。

实现

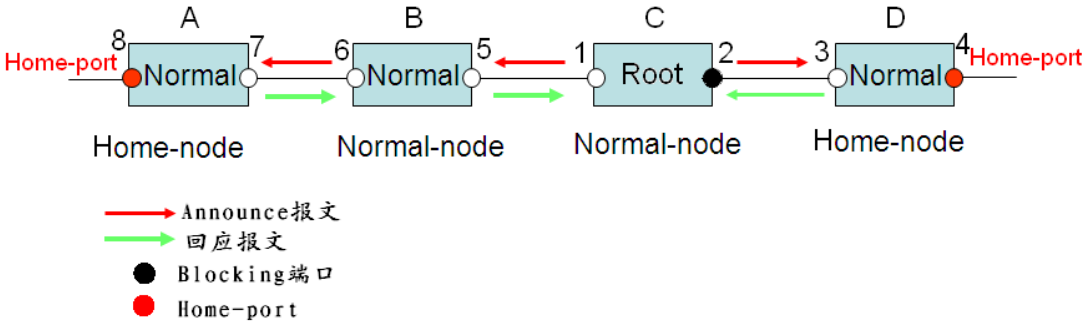

图 96 DHP 配置说明

图 95 中 A、B、C 和 D 的配置如图 96 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 97 所示。

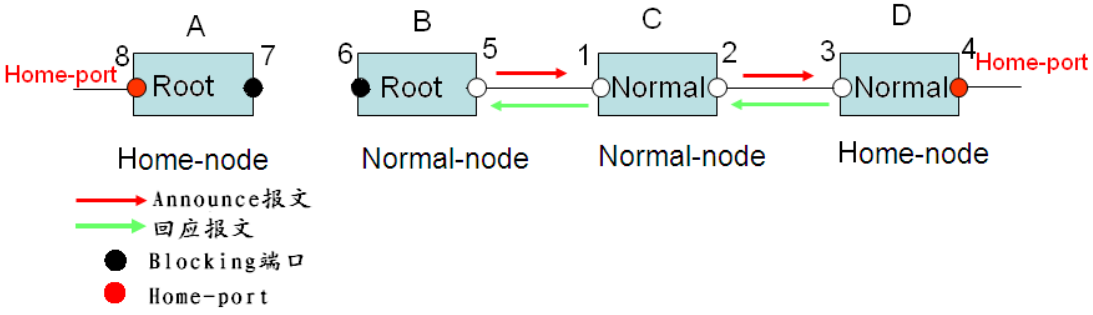

图 97 DHP 故障恢复

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。

Web 页面配置

1、配置 DRP 模式，如图 98 所示；

图 98 DRP 模式配置

DRP 模式

配置选项：PORT MODE/VLAN MODE

默认配置：PORT MODE

功能：配置 DRP 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 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 DRP-Port-Based 环，如图 99 所示；

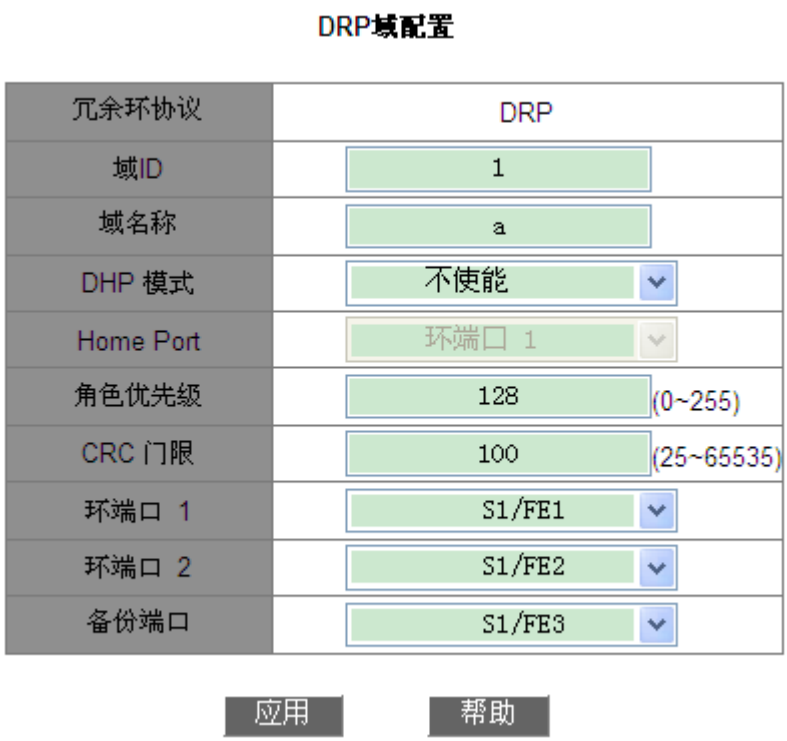

图 99 DRP-Port-Based 配置

冗余环协议

强制配置：DRP

域 ID

配置范围：1~32

功能：域号用来区分不同的环，一台交换机上最多可以配置 16 个 DRP-Port-Based 环。

域名称

配置范围：1~31 个字符

功能：配置域名称。

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。

注意：

DHP 目前只支持在 DRP-Port-Based 模式下进行配置。

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。

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。

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 15 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。

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。

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。

配置完成后，“DRP 列表”中显示已创建的环列表，如图 100 所示；

DRP列表

域ID	站角色	环端口(1,2)	备份端口	环状态
1-a	ROOT	S1/FE1,S1/FE2	S1/FE3	Ring-Close

图 100 DRP-Port-Based 列表

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；
- DRP 环端口、备份端口与端口镜像配置互斥，DRP 环端口和备份端口不能配置为镜像端口和被镜像端口，镜像端口和被镜像端口也不能配置为 DRP 环端口和备份端口；
- 基于端口的环协议 RSTP、DT-Ring-Port 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、DT-Ring-Port 环端口、DT-Ring-Port 备份端口；RSTP 端口、DT-Ring-Port 环端口、DT-Ring-Port 备份端口也不能配置为 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中。

- 查看 DRP-Port-Based 配置

点击图 100 中相应 DRP 选项，可以查看该环配置，并对其进行修改，如下图所示；

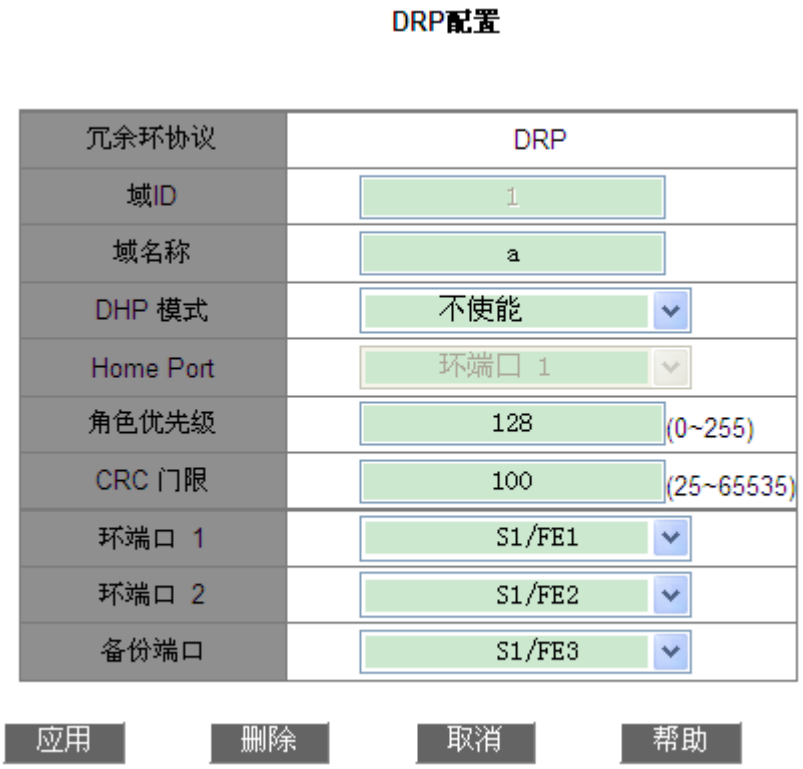

图 101 查看并修改 DRP-Port-Based 配置

修改完后点击<应用>按钮即可成功修改；点击<删除>按钮即可删除该 DRP 配置表项。

- 显示 DRP 协议环中交换机的角色和各端口状态，如下图所示；

DRP状态

站角色	ROOT
环端口 1	FORWARD
环端口 2	BLOCK
备份端口	BLOCK
环状态	Ring-Close
IP 地址	192.168.0.222
MAC地址	08-00-3E-32-53-22

图 102 DRP-Port-Based 状态查看

3、配置 DRP-VLAN-Based 环，如图 103 所示；

DRP域配置

冗余环协议	DRP
域ID	1
域名称	a
DHP 模式	不使能
Home Port	环端口 1
角色优先级	128 (0~255)
CRC 门限	100 (25~65535)
环端口 1	S1/FE1
环端口 2	S1/FE2
备份端口	S1/FE3
协议Vlan	2 (1~4093)
业务Vlan	2-4 (e.g. 1,2,3,6-8)

应用 帮助

图 103 DRP-VLAN-Based 配置

冗余环协议

强制配置：DRP

域 ID

配置范围：1~32

功能：域号用来区分不同的环，一台交换机上最多可以配置 8 个 DRP-VLAN-Based 环。

域名称

配置范围：1~31 个字符

功能：配置域名称。

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。

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 15 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。

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：

- 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；
- DRP 环端口、备份端口与端口镜像配置互斥，DRP 环端口和备份端口不能配置为镜像端口和被镜像端口，镜像端口和被镜像端口也不能配置为 DRP 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中

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。

协议 VLAN

配置范围：1~4093

说明：该 VLAN ID 应从业务 VLAN 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。

业务 VLAN

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。

配置完成后，“DRP 列表”中显示已创建的环列表，如图 104 所示；

DRP列表

域ID	站角色	环端口(1,2)	备份端口	环状态	协议Vlan	业务Vlan
1-a	ROOT	S1/FE1,S1/FE2	S1/FE3	Ring-Close	2	2-4

图 104 DRP-VLAN-Based 列表

- 查看 DRP-VLAN-Based 配置

点击图 104 中相应 DRP 选项，可以查看该环配置，并对其进行修改，如下图所示；

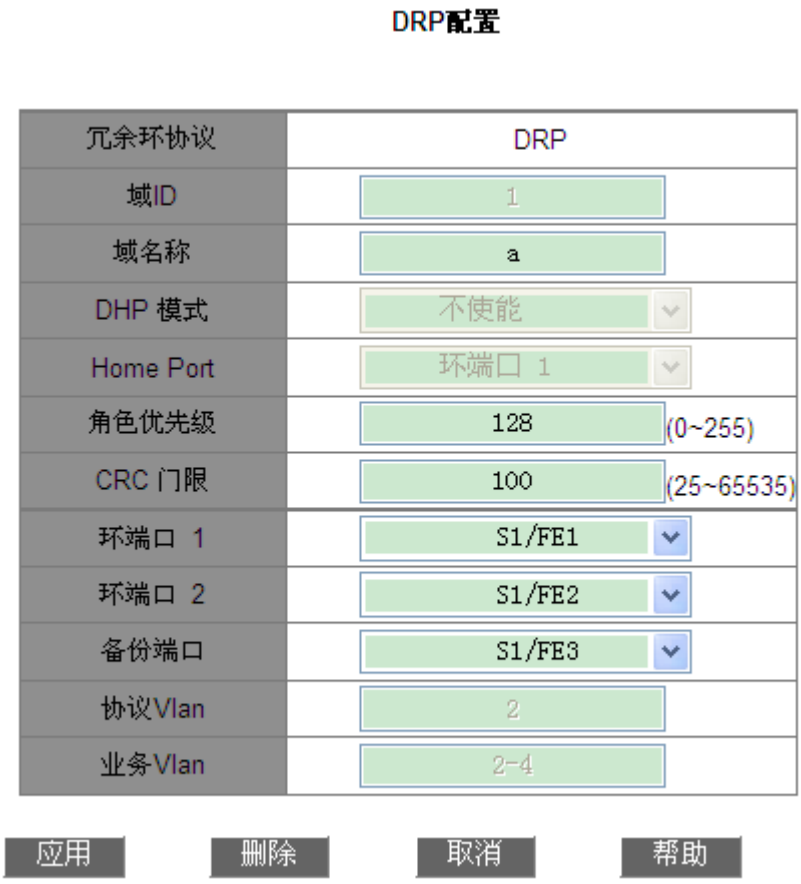

图 105 查看并修改 DRP-VLAN-Based 配置

修改完后点击<应用>按钮即可成功修改；点击<删除>按钮即可删除该 DRP 配置表项。

显示 DRP 协议环中交换机的角色和各端口状态，如图 106 所示；

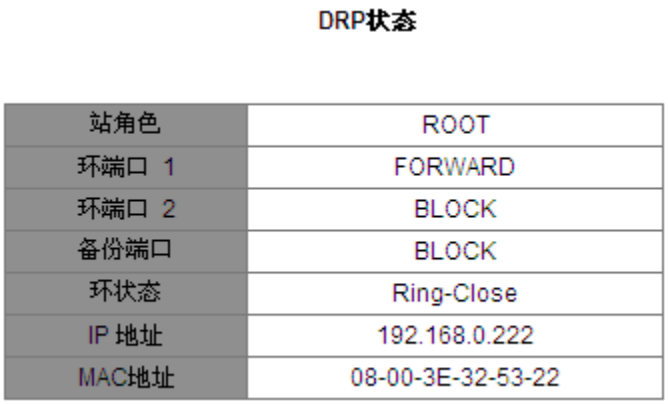

图 106 DRP-VLAN-Based 状态查看

典型配置举例

如图 94 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：Ring；端口优先级采用默认值；环端口选择 1 和 2，备份端口可以不选择，见图 99；

交换机 C、D 的配置：

2、域 ID：1；域名称：Ring；端口优先级采用默认值；环端口选择 1 和 2，备份端口选择 3，见图 99；

交换机 E、F、G、H 的配置：

3、域 ID：2；域名称：Ring；端口优先级采用默认值；环端口选择 1 和 2，备份端口可以不选择，见图 99；

6.17 QoS 配置

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。

业务识别、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：

业务识别：依据一定的匹配规则识别出对象，可以是报文中自带的优先级标志、也可以是根据端口和 VLAN 重新映射的优先级、还可以是根据报文五元组等标识会话的信息来映射的优先级信息。业务识别是 QoS 的前提。

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。

原理

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

通过配置优先级值和队列的映射关系，当一帧数据到达一个端口时，根据其优先级值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业务的优先级识别：最高优先级、基于端口、DIFF、TOS/DIFF、802.1p 优先级。

如果一个端口配置为最高优先级，则该端口转发的报文存放在队列 3 中；

如果一个端口配置为基于端口，则该端口的默认优先级决定报文的存放队列，端口默认优先级与队列的映射关系和 802.1p 优先级与队列的映射关系保持一致；

DIFF 值取决于报文中的 DSCP 部分，TOS/DIFF 值取决于报文中的 TOS/DSCP 部分，该优先级值与队列的映射关系可以配置；

当报文为 Tag 类型时，802.1p 值取决于报文中 802.1Q 的优先级部分；当报文为 Untag 类型时，802.1p 值取决于端口默认优先级，802.1p 优先级与队列的映射关系可以配置；

端口转发数据时，通过调度模式决定如何调度 4 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几种 QoS 队列调度模式：权重式 WRR(Weighted Round Robin，加权轮询调度)、抢占式和严格优先级。

WRR 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。

抢占式能够严格保证最高优先级报文的转发，如果一帧数据进入最高优先级队列，将停止低优先级队列的调度来处理最高优先级队列的数据。当最高优先级队列为空时，按照权重比调度其他 3 个队列中数据。

严格优先级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。

Web 页面配置

1、QoS 模式选择，如图 107 所示；

图 107 QoS 模式选择

QoS 模式

配置选项：Disable/权重式 WRR/严格优先级

默认配置：严格优先级

功能：配置端口调度模式。

2、配置队列权重比，如图 108 所示；

权重比

3--HIGHEST	2--SECHIGH	1--SECLOW	0--LOWEST
8	4	2	1

图 108 配置队列权重比

{3-HIGHEST, 2-SECHIGH, 1-SECLOW, 0-LOWEST}

配置范围：{1~55，1~55，1~55，1~55}

默认配置：{8, 4, 2, 1}

功能：配置队列权重比，配置时应遵循以下规则：

队列 3 权重>=2×队列 2 权重； 队列 2 权重>=2×队列 1 权重；

队列 1 权重>=2×队列 0 权重

3、配置 QoS 端口优先级队列映射模式，如图 109 所示；

端口优先级配置

端口	基于端口	DIFF	802.1P优先级
S1/FE1	☑	☐	☐
S1/FE2	☐	☐	☑
S1/FE3	☐	☑	☐
S1/FE4	☐	☐	☑
S1/FE5	☐	☐	☑
S1/FE6	☐	☐	☑
S1/FE7	☐	☐	☑
S1/FE8	☐	☐	☑
S2/FE1	☐	☐	☑
S2/FE2	☐	☐	☑
S2/FE3	☐	☐	☑
S2/FE4	☐	☐	☑
S2/FE5	☐	☐	☑
S2/FE6	☐	☐	☑
S2/FE7	☐	☐	☑
S2/FE8	☐	☐	☑
S3/FE1	☐	☐	☑
S3/FE2	☐	☐	☑
S3/FE3	☐	☐	☑
S3/FE4	☐	☐	☑
S3/FE5	☐	☐	☑
S3/FE6	☐	☐	☑
S3/FE7	☐	☐	☑
S3/FE8	☐	☐	☑
S4/GX1	☐	☐	☑
S4/GX2	☐	☐	☑
S4/GX3	☐	☐	☑
S4/GX4	☐	☐	☑

应用

图 109 配置 QoS 端口优先级队列映射模式

端口优先级配置

配置选项：基于端口/DIFF/802.1p 优先级

默认配置：802.1p 优先级

功能：配置端口的优先级队列映射模式。

说明：每个端口只能选择一种优先级队列映射模式。

4、配置基于端口/802.1p 优先级到队列的映射关系

当端口优先级配置中选择基于端口或 802.1p 优先级模式时，这两种模式的优先级队列映射关系一致，均在 802.1p 优先级队列映射表中配置，如图 110 所示；

点击图 107 右边的<802.1p 优先级>按钮，出现 802.1p 优先级队列映射表：

图 110 802.1p 优先级队列映射表

802.1p 优先级配置

组合配置：{ 优先级，队列 }

配置范围：{ 0~7，0~3 }

默认配置：优先级 0、1 映射到队列 0；优先级 2、3 映射到队列 1；

优先级 4、5 映射到队列 2；优先级 6、7 映射到队列 3；

功能：配置 802.1p 优先级到队列的映射关系。

5、配置 DSCP 优先级到队列的映射关系

点击图 107 右边的<DSCP 优先级>按钮配置 DSCP 优先级到队列的映射关系，如图 111 所示；

图 111 DSCP 优先级队列映射表

DSCP 优先级配置

组合配置：{ DSCP，QoS 队列 }

配置范围：{ 0~63，0~3 }

默认配置：优先级 0~63 映射到队列 0；

功能：配置 DSCP 优先级到队列的映射关系。

典型配置举例

如图 112 所示，port1~port4 向 port5 转发报文，其中 port1 采用基于端口模式，port1 的默认优先级为 6，进入 port1 的报文映射到队列 3 中，进入 port2 的报文携带 802.1p 优先级为 2，映射到队列 1 中；进入 port3 的报文携带 802.1p 优先级是 4，映射到队列 2 中；进入 port4 的 IP 报文携带的 DSCP 优先级是 6，映射到队列 3 中；port5 采用 WRR 调度模式。

配置过程如下：

1、QoS 模式选择权重式 WRR， WRR 队列权重比采用默认配置，如图 107 和图 108 所示。

2、端口 1 优先级配置为基于端口，端口 2 和端口 3 优先级配置为 802.1p，端口 4 优先级配置为 DIFF，如图 109 所示。

3、配置 802.1p 优先级 6、2 和 4 分别映射到队列 3、1 和 2 中，如图 110 所示。

4、配置 DSCP 优先级 6 映射到队列 3 中，如图 111 所示。

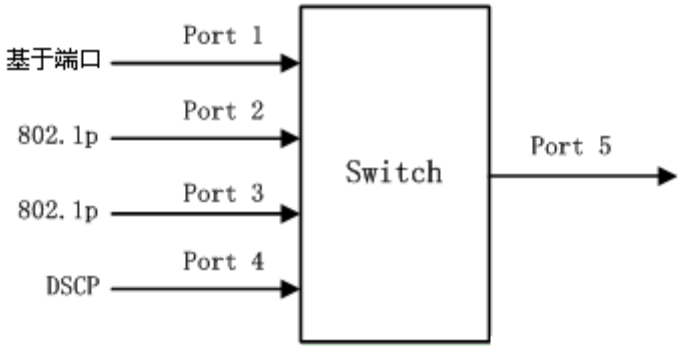

图 112 QoS 配置举例

port1 和 port4 的报文都入队列 3，port2 的报文入队列 1，port3 的报文入队列 2，再根据队列和权重的对应关系知道，队列 1 的权重＝2，队列 2 的权重＝4，队列 3 的权重＝8，那么入队列 1 的报文分配的带宽比例为：2/(2+4+8)，入队列 2 报文分配的带宽比例为：4/(2+4+8)，入队列 3 报文分配的带宽比例为：8/(2+4+8)。其中 port1 和 port4 的报文都入队列 3，所以只能按照先进先出的方式转发，但肯定的是 port1 和 port4 的总带宽比例一定是 8/(2+4+8)。

6.18 MAC 老化时间

介绍

交换机中各端口具有自动学习地址的功能，将端口接收帧的源地址(源 MAC 地址、交换机端口号)存储到地址表中。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。

Web 页面配置

MAC 地址老化时间配置如图 113 所示；

图 113 MAC 地址老化时间表

MAC 老化时间

配置范围：15~3600s

默认配置：300 s

描述：用户可根据具体情况调整老化时间有效的实现 MAC 地址老化功能。

6.19 LLDP 信息

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。

Web 页面配置

1、使能 LLDP 协议，如图 114 所示；

图 114 使能 LLDP 协议

LLDP

配置选项：使能/不使能

默认配置：使能

功能：是否使能 LLDP 协议。

描述：使能 LLDP 协议后，该设备会向相邻设备发送 LLDP 报文，同时也会接收并处理相邻设备发送的 LLDP 报文；禁止 LLDP 协议后，该设备既不发送 LLDP 报文也不处理 LLDP 报文。

2、查看 LLDP 连接信息，如图 115 所示；

LLDP 连接信息

本机端口	邻端口	邻IP	邻MAC
1/1	0/1	192.168.0.109	00:00:ee:ee:02:05

图 115 LLDP 连接信息

LLDP 连接信息列表中可以查看相邻设备的信息，包括相邻设备与该交换机连接的端口号、相邻设备的 IP 地址和 MAC 地址；

注意：

显示 LLDP 信息的前提是相连接的设备必须都使能 LLDP 协议，该协议是链路层发现协议，系统默认是开启 LLDP 协议的。

6.20 SNTP

介绍

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，可以支持 4 个 SNTP 服务器，但同一时间只能有一个处于活动状态。交换机也可以作为 SNTP Server 同步其他客户端时间。

SNTP 客户端的请求以单播形式逐次发送给各个服务器，最先作出回应的服务器处于活动状态，其他服务器处于非活动状态。

注意：

- 交换机使用 SNTP 对时，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。

Web 页面配置

1、使能 SNTP 协议，并且选择服务器进行相关配置，如图 116 所示；

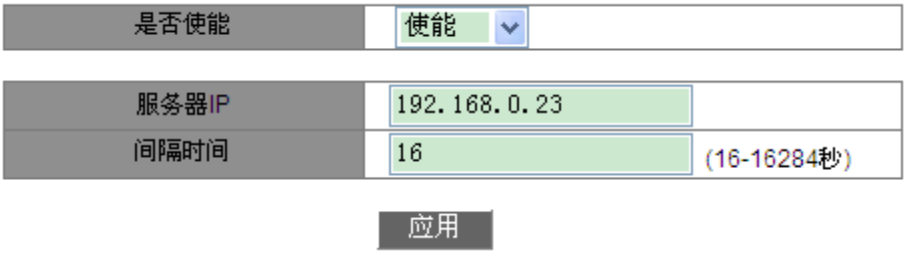

图 116 SNTP 配置

是否使能

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 IP

配置格式：A.B.C.D

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

间隔时间

配置选项：16~16284s

功能：配置 SNTP 客户端向 SNTP 服务器发送同步请求的时间间隔。

2、选择客户端与服务器同步时间的方式，如图 117 所示；

图 117 时间同步方式

服务器时间

功能：显示设备从服务器获得的上次同步时间。

本地时间

功能：显示设备的本地时间。

更新方式

配置选项：自动/手动

默认配置：自动

功能：选择设备和服务器同步时间的方式。

3、查看 SNTP 配置信息，在序号框中选中要删除 SNTP 服务器，点击<删除>按钮即可删除，如图 118 所示；

图 118 SNTP 配置信息

服务器状态

显示选项：活动/静止

描述：活动状态的服务器为客户端提供 SNTP 时间，同一时间只能有一个服务器处于活动状态，其他的都为静止状态。

手动同步

手动同步时点击<同步>按钮。

4、配置交换机作为 SNTP Server，如图 119 所示；

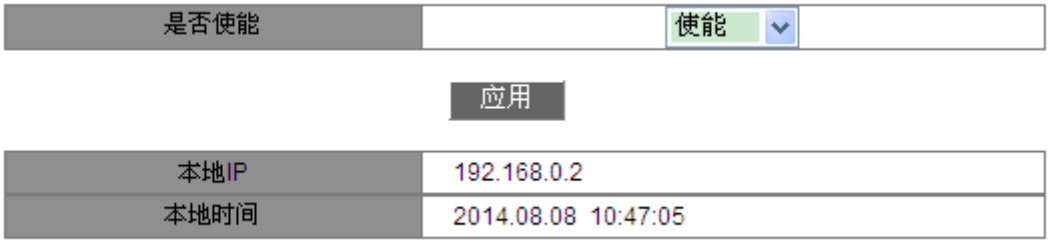

图 119 交换机作为 SNTP Server

是否使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能交换机作为 SNTP Server。

6.21 端口隔离

介绍

为了实现报文之间的二层隔离，可以将不同的端口加入不同的VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一VLAN 内端口之间的隔离。用户只需要将端

口加入到隔离组中，由于隔离组中的端口不会向隔离组内的其它端口转发报文，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

说明：

- 加入隔离组的端口只能是同一台交换机的端口；
- 配置隔离组后，只有隔离组内各端口之间的报文不能互通，隔离组内端口与隔离组外端口之间的通信不受影响。

Web 页面配置

使能端口隔离功能，如图 120 所示；

端口	隔离使能
S1/FE1	☑
S1/FE2	☑
S1/FE3	☑
S1/FE4	☐
S1/FE5	☐
S1/FE6	☐
S1/FE7	☐
S1/FE8	☐
S2/FE1	☐
S2/FE2	☐

图 120 端口隔离配置

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。

说明：

该设备只支持一个隔离组，即使能端口隔离的端口之间相互隔离所有流量；使能端口隔离的端口和未使能端口隔离的端口之间通信不受影响。

典型配置举例

组网需求：

PC1、PC2、PC3 分别与交换机的以太网端口1、2、3 相连， 4 端口与外部网络相连，PC1、PC2 和PC3 之间两两不能互通，但都可访问外部网络，如图 121所示；

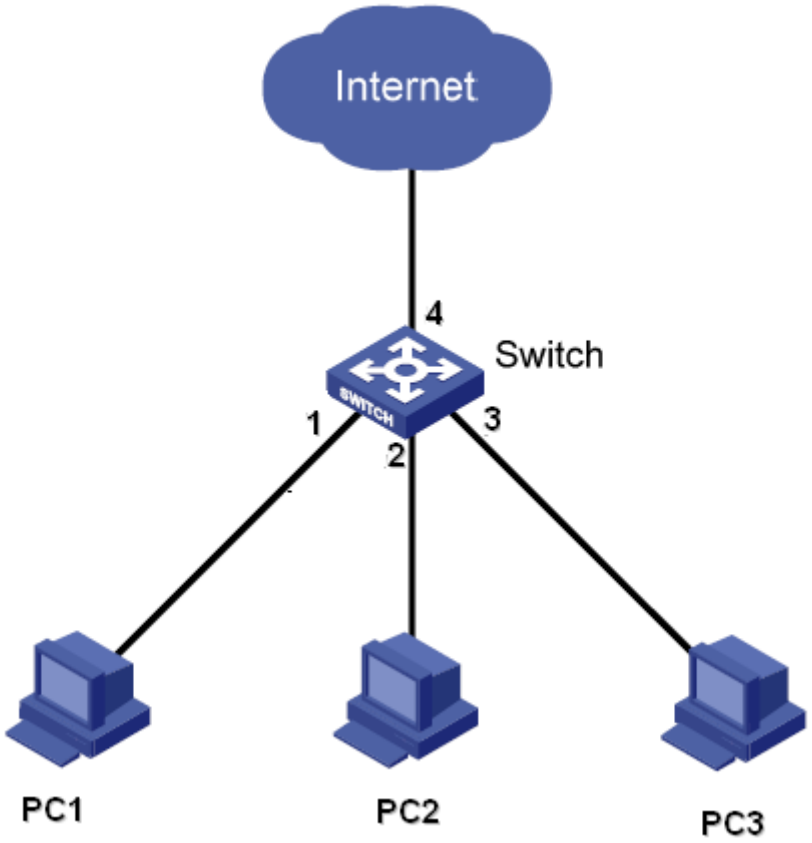

图 121 端口隔离配置举例

具体配置：

将端口1，2，3加入隔离组，如图 120所示，即可实现PC1、PC2和PC3之间隔离。

6.22 告警

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，单电源输入时会产生告警；

温度告警：使能情况下，交换机温度低于等于下阈值或高于等于上阈值时会发生告警；

IP/MAC 冲突告警：使能情况下，IP/MAC 地址冲突时会产生告警；

端口告警：使能情况下，端口 Link down 时会产生告警；

环告警：使能情况下，环开时会产生告警。

注意：

只有 DT-Ring 环的主站、DRP 环的 Root 支持环告警功能。

Web 页面配置

1、告警配置，如图 122 所示；

IP、MAC冲突告警

告警名称	告警使能	检测时间
IP、MAC冲突	☑	300 (180~600秒)

电源告警

告警名称	告警使能
电源告警	☑

温度告警

告警名称	告警使能	温度告警阀值范围
温度告警	使能	上阀值 + 80 ～ 下阀值 - 30

端口告警配置

端口	告警使能	端口	告警使能	端口	告警使能	端口	告警使能
S1/FE1	☑	S1/FE2	☑	S1/FE3	☑	S1/FE4	☐
S1/FE5	☐	S1/FE6	☐	S1/FE7	☐	S1/FE8	☐
S2/FE1	☐	S2/FE2	☐	S2/FE3	☐	S2/FE4	☐
S2/FE5	☐	S2/FE6	☐	S2/FE7	☐	S2/FE8	☐
S3/FE1	☐	S3/FE2	☐	S3/FE3	☐	S3/FE4	☐
S3/FE5	☐	S3/FE6	☐	S3/FE7	☐	S3/FE8	☐
S4/GX1	☐	S4/GX2	☐	S4/GX3	☐	S4/GX4	☐

环告警配置

DT-RING 域ID	告警使能
1	☑
2	☑

DRP告警配置

DRP 域ID	告警使能
1	☑
2	☑

应用

图 122 告警配置

IP、MAC 冲突告警

配置选项：使能/不使能

默认配置：使能

功能：是否使能地址冲突告警。

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。

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。

温度告警 {告警使能，上阈值~下阈值}

配置范围：{使能/不使能，+150℃~-55℃}

默认配置：{不使能，+80℃~-30℃}

功能：是否使能温度告警，并配置温度上、下阈值。

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。

环告警/DRP 告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能环告警。

2、使能告警功能后，告警显示如图 123 所示；

基本告警

告警名称	告警状态
电源告警	有告警
温度告警	正常
IP冲突告警	正常
MAC冲突告警	正常

端口告警

端口	告警状态	端口	告警状态	端口	告警状态	端口	告警状态
S1/FE1	Link Up	S1/FE2	Link Up	S1/FE3	Link Down	S1/FE4	-
S1/FE5	-	S1/FE6	-	S1/FE7	-	S1/FE8	-
S2/FE1	-	S2/FE2	-	S2/FE3	-	S2/FE4	-
S2/FE5	-	S2/FE6	-	S2/FE7	-	S2/FE8	-
S3/FE1	-	S3/FE2	-	S3/FE3	-	S3/FE4	-
S3/FE5	-	S3/FE6	-	S3/FE7	-	S3/FE8	-
S4/GX1	-	S4/GX2	-	S4/GX3	-	S4/GX4	-

DT-RING告警

DT-RING 域ID	告警状态
2	Ring Open
1	Ring Close

DRP告警

DRP 域ID	告警状态
1	正常
2	告警

图 123 告警显示

电源告警

显示选项：正常/有告警

描述：使能电源告警后，双电源输入时显示正常，单电源输入时显示有告警。

温度告警

显示选项：正常/上限告警/下限告警

描述：交换机温度高于或等于上阈值时，显示上限告警；当交换机温度低于或等于下阈值时，显示下限告警；否则，显示正常。

IP/MAC 冲突告警

显示选项：正常/有告警

描述：有地址冲突时显示有告警，否则显示正常。

端口告警

显示选项：Link Up/Link Down

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

环告警

DT-Ring 显示选项：Ring Open/Ring Close

DRP 显示选项：告警/正常

描述：使能环告警后，环开时显示 Ring Open 或告警，环闭时显示 Ring Close 或正常。

6.23 端口流量告警

介绍

端口流量告警指某个端口的指定流量超过预先设定的阈值，或发生 CRC 错误时产生的告警。

注意：

- 流量告警是针对端口的，只有对某个端口进行配置后才可能产生告警；
- 流量告警是有方向的，入流量和出流量分别对应不同的告警；
- 流量发生 CRC 校验错误时产生 CRC 错误告警。

Web 页面配置

1、端口流量告警配置，如图 124 所示；

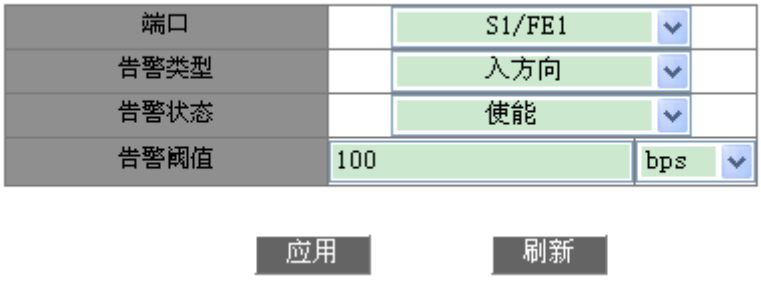

图 124 端口流量告警配置

端口

配置选项：所有端口

功能：选择配置流量告警的端口。

告警类型

配置选项：入方向/出方向/CRC 错误

功能：配置端口流量告警类型。

告警状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口相应的告警类型。

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。

2、查看端口流量异常告警信息，如图 125 所示；

端口	入方向		告警状态	出方向		告警状态	CRC错误	告警状态
S1/FE1	使能	100bps	告警	使能	1000bps	告警	使能	告警
S1/FE2	使能	100kbps	正常	使能	100bps	正常	使能	正常
S1/FE3	不使能	-	-	不使能	-	-	不使能	-
S1/FE4	不使能	-	-	不使能	-	-	不使能	-
S1/FE5	不使能	-	-	不使能	-	-	不使能	-
S1/FE6	不使能	-	-	不使能	-	-	不使能	-
S1/FE7	不使能	-	-	不使能	-	-	不使能	-
S1/FE8	不使能	-	-	不使能	-	-	不使能	-
S4/GE1	不使能	-	-	不使能	-	-	不使能	-
S4/GE2	不使能	-	-	不使能	-	-	不使能	-
S4/GE3	不使能	-	-	不使能	-	-	不使能	-
S4/GE4	不使能	-	-	不使能	-	-	不使能	-

图 125 端口流量异常告警信息

6.24 GMRP 配置与查询

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。

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。

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。

Web 页面配置

1、使能全局 GMRP 协议，如图 126 所示；

图 126 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：是否使能全局 GMRP 功能，该功能与 IGMP-Snooping 功能不能同时使能。

LeaveAll timer

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。

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。

2、配置每个端口的 GMRP 功能，如图 127 所示；

端口配置

端口	GMRP使能	代理使能	Hold Timer	Join Timer	Leave Timer
S1/FE1	使能	使能	100 ms	500 ms	3000 ms
S1/FE2	使能	不使能	100 ms	500 ms	3000 ms
S1/FE3	使能	不使能	100 ms	500 ms	3000 ms
S1/FE4	使能	不使能	100 ms	500 ms	3000 ms
S1/FE5	不使能	不使能	100 ms	500 ms	3000 ms
S1/FE6	不使能	不使能	100 ms	500 ms	3000 ms
S1/FE7	不使能	不使能	100 ms	500 ms	3000 ms
S1/FE8	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE1	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE2	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE3	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE4	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE5	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE6	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE7	不使能	不使能	100 ms	500 ms	3000 ms
S2/FE8	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX1	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX2	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX3	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX4	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX5	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX6	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX7	不使能	不使能	100 ms	500 ms	3000 ms
S3/FX8	不使能	不使能	100 ms	500 ms	3000 ms
S4/GE1	不使能	不使能	100 ms	500 ms	3000 ms
S4/GE2	不使能	不使能	100 ms	500 ms	3000 ms
S4/GE3	不使能	不使能	100 ms	500 ms	3000 ms
S4/GE4	不使能	不使能	100 ms	500 ms	3000 ms

应用

图 127 端口 GMRP 配置

GMRP 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 GMRP 功能。

代理使能

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 GMRP 代理功能。

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。

Hold timer

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 timer

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 timer

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。

3、添加一个 GMRP 代理表项，配置如图 128 所示；

图 128 GMRP 代理表项配置

MAC 地址

配置格式：HHHHHHHHHHHH (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。

成员端口列表

选择代理表项的成员端口，只能从代理端口中选择。

源端口列表

配置选项：使能 GMRP 代理功能的端口。

4、查看、修改以及删除 GMRP 代理表项，如图 129 所示。

图 129 GMRP 代理表项操作

GMRP 代理表项显示代理 MAC 地址、VLAN ID 以及代理成员端口。选择其中任意表项点击<删除>按钮便成功删除该代理表项；点击<修改>按钮便可以修改该代理表项的成员端口。

5、在连接的相邻设备上查看该代理表项的组播成员，如图 130 所示；

查看该表项应满足以下条件：

- 相连设备都使能 GMRP 功能；
- 两台设备相连的两个端口都是扩散端口，并且本端设备扩散端口的 VLAN ID 应与代理表项的 VLAN ID 一致。

图 130 GMRP 动态组播表

GMRP 动态组播表

组合显示：{ 序号，组播地址，VLAN 号，成员端口 }

功能：显示 GMRP 动态组播表项。

典型配置举例

如图 131 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。

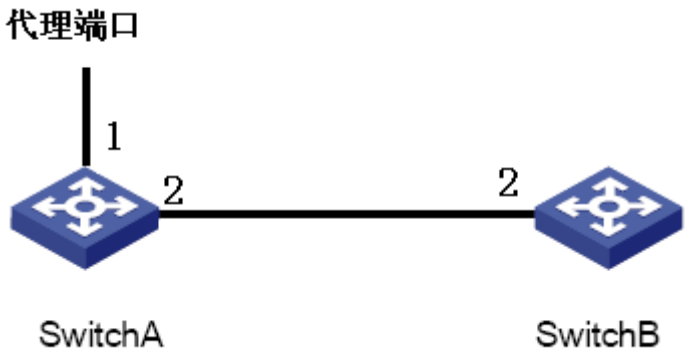

图 131 GMRP 组网图

交换机 A 的配置过程：

1、使能交换机 A 的全局 GMRP 功能，LeaveAll 定时器采用默认值，见图 126；

2、使能端口 1 的 GMRP 功能和代理功能；只使能端口 2 的 GMRP 功能，定时器的值都采用默认值，见图 127；

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 128；

交换机 B 的配置过程：

1、使能交换机 B 的全局 GMRP 功能，LeaveAll 定时器采用默认值，见图 126；

2、使能端口 2 的 GMRP 功能，定时器的值都采用默认值，见图 127；

交换机 B 上动态学习到的 GMRP 组播表项如表 8 所示；

表 8 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**
Untag1	Untag1	MAC：01-00-00-00-00-01 VLAN ID：1

		成员端口：2
Untag2	Untag2	MAC：01-00-00-00-00-02 VLAN ID：2 成员端口：2
Untag1	Untag2	MAC：01-00-00-00-00-01 VLAN ID：2 成员端口：2

6.25 RMON

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。

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，每个组最多支持32个表项。

- 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。

Web 页面配置

1、统计表配置如图 132 所示；

图 132 RMON 统计配置表

索引

配置范围：1~65535

功能：配置统计信息表项的编号。

Owner

配置范围：1~32 个字符

功能：配置统计信息表项的名称。

Data source

功能：选择统计哪个端口的信息。

2、历史表配置如图 133 所示；

图 133 RMON 历史配置表

索引

配置范围：1~65535

功能：配置历史控制表项的编号

Data source

功能：选择对哪个端口信息进行采样。

Owner

配置范围：1~32 个字符

功能：配置历史控制表项的名称。

采样数目

配置范围：1~65535

功能：配置端口信息的采样次数。

采样间隔

配置范围：1~3600s

功能：配置端口信息的采样周期。

3、事件控制配置如图 134 所示；

图 134 RMON 事件控制配置表

索引

配置范围：1~65535

功能：配置事件控制表项的索引号。

Owner

配置范围：1~32 个字符

功能：配置事件控制表项的名称。

事件类型

配置选项：NONE/LOG/Snmp-Trap/Log and Trap

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。

事件描述

配置范围：1~127 个字符

功能：对事件的描述。

事件团体

配置范围：1~127 个字符

功能：配置发送 trap 事件的团体名称，与 SNMP 中团体名保持一致。

4、告警控制配置如图 135 所示；

图 135 RMON 告警配置表

索引

配置范围：1~65535

功能：配置告警控制表项的编号。

OID

当前 MIB 节点的 OID 号。

Owner

配置范围：1~32 个字符

功能：配置告警控制表项的名称。

Data source

功能：选择对哪个端口的信息进行监测。

采样类型

配置选项：Absolute/Delta

默认配置：Absolute

功能：Absolute 为绝对值采样，即采样时间到达时直接提取变量的值。delta 为变化值采样，即采样时间到达时提取的是变量在采样间隔内的变化值。

报警类型

配置选项：RisingAlarm/FallingAlarm/RisOrFallAlarm

默认配置：RisingAlarm

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。

采样间隔

配置范围：1~65535

功能：配置端口信息的采样周期，该值最好与历史表中的采样间隔配置保持一致。

上升阈值

配置范围：0~65535

功能：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 RisOrFallAlarm 时，将会报警并激活上升事件索引。

下降阈值

配置范围：0~65535

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 FallingAlarm 或者

RisOrFallAlarm 时，将会报警并激活下降事件索引。

上升事件索引

配置范围：0~65535

功能：配置上升事件的索引，即对上升沿告警的处理方式。

下降事件索引

配置范围：0~65535

功能：配置下降事件的索引，即对下降沿告警的处理方式。

6.26 日志查询功能

介绍

交换机中的运行日志功能主要记录交换机的运行信息，便于管理员对日志报文的读取和管理，查找故障。

运行日志记录的消息包括：

- 电源告警、温度告警、IP/MAC 地址冲突告警、端口告警、环告警以及端口流量告警
- 广播风暴
- 软件系统重启

说明

运行日志中最多支持 1024 条表项，当表项超过 1024 条时，新的日志表项将会覆盖旧的日志表项。

Web 页面配置

1、使能日志功能，如图 136 所示；

图 136 日志状态配置

运行日志使能

配置选项：使能/不使能

默认配置：使能

功能：是否使能运行日志，使能后，日志中会记录运行日志。

2、运行日志上传，如图 137 所示；

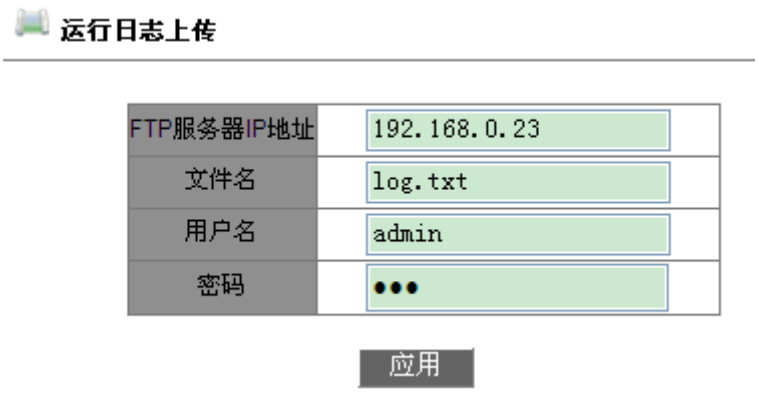

图 137 运行日志上传

FTP 服务器 IP 地址

配置格式：A.B.C.D

功能：配置 FTP 服务器 IP 地址。

文件名

配置范围：1~20 个字符

功能：配置服务器中保存的日志信息文件名。

用户名

配置范围：1~20 个字符

功能：配置 FTP 用户名。

密码

配置范围：1~20 个字符

功能：配置 FTP 密码。

注意：

上传日志过程中，FTP 服务器软件应保持运行状态。

3、查看运行日志，如图 138 所示；

运行日志查询

序号	日志类型	产生时间	日志描述
10	环开闭告警	THU SEP 13 15:24:42 2012	Ring alarm: entity id:1 state:Ring open
9	端口LINK告警	THU SEP 13 15:24:42 2012	Port alarm: entity id:1/2 port:1/2 state:Link down
8	环开闭告警	THU SEP 13 15:24:07 2012	Ring alarm: entity id:1 state:Ring close
7	端口LINK告警	THU SEP 13 15:24:07 2012	Port alarm: entity id:1/2 port:1/2 state:Link up
6	出口速率	THU SEP 13 15:23:44 2012	Output alarm: entity id:1 state:Alarm
5	入口速率	THU SEP 13 15:23:43 2012	Input alarm: entity id:1 state:Alarm
4	端口LINK告警	THU SEP 13 15:23:39 2012	Port alarm: entity id:1/1 port:1/1 state:Link up
3	出口速率	THU SEP 13 15:22:58 2012	Output alarm: entity id:2 state:Normal
2	端口LINK告警	THU SEP 13 15:22:55 2012	Port alarm: entity id:1/2 port:1/2 state:Link down
1	电源告警	THU SEP 13 15:21:49 2012	Power alarm: entity id:2 state:Power down
0	出口速率	THU SEP 13 15:21:28 2012	Output alarm: entity id:2 state:Alarm

图 138 运行日志查询

运行日志

显示组合{序号，日志类型，产生时间，日志描述}

功能：显示当前记录的运行日志。

6.27 单播地址配置与查询

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。

该系列交换机最多可以配置 256 个静态单播表项。

Web 页面配置

1、添加静态 MAC 地址表项，如图 139 所示；

图 139 添加静态单播 FDB 表

MAC 地址

配置格式：HHHHHHHHHHHH (H 为一个十六进制数)

功能：配置单播 MAC 地址，最高字节的最低位为 0。

VLAN ID

配置选项：端口所属的 VLAN 号。

成员端口

配置选项：交换机上所有端口

功能：选择转发该目的 MAC 地址报文的端口，所选端口应存在于上述指定 VLAN 中。

2、查看静态单播地址列表，如图 140 所示；

图 140 查看静态 FDB 表

选中一个表项，点击<删除>按钮可以删除该静态单播地址表项；点击<修改>按钮可以修改该静态单播地址表项的成员端口。

3、查看动态单播地址表项，如图 141 所示；

动态单播地址列表

序号	MAC地址	VLAN ID	成员端口
1	00:1e:cd:17:c6:3e	2	S1/FE2
2	44:87:fc:45:60:0b	2	S1/FE2
3	e0:69:95:03:a0:bf	2	S1/FE2
4	80:c1:6e:e0:5c:c3	2	S1/FE2
5	90:fb:a6:3c:ca:7e	2	S1/FE2
6	00:1f:d0:0d:fd:01	2	S1/FE2
7	e0:69:95:03:91:f4	2	S1/FE2
8	d4:be:d9:b9:50:08	2	S1/FE2
9	00:25:11:86:c3:f3	2	S1/FE2
10	d0:67:e5:19:b7:1d	2	S1/FE2
11	00:00:ff:ff:aa:96	2	S1/FE2
12	00:24:8c:9e:56:26	2	S1/FE2
13	44:87:fc:45:62:18	2	S1/FE2
14	e0:69:95:03:92:b6	2	S1/FE2
15	d0:27:88:46:0a:e8	2	S1/FE2
16	00:23:cd:8f:7e:aa	2	S1/FE2

清除

图 141 动态单播 FDB 表

6.28 DHCP

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 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 142 所示；

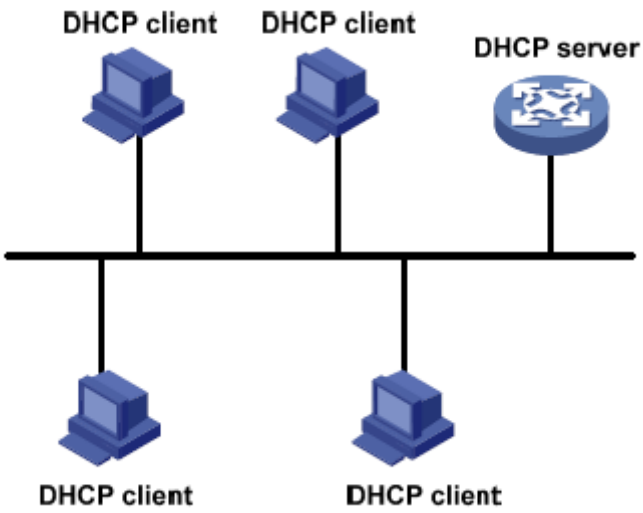

图 142 DHCP 典型应用结构

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。本系列设备不支持 DHCP 中继，所以要求客户机和服务器位于同一网段中。

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，该分配策略包括端口 IP 地址绑定和 MAC 地址绑定两种；

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。

DHCP 服务器配置

6.28.1.1 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。

6.28.1.2 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 地址或者客户端连接服务器端口号静态绑定的 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。

6.28.1.3 Web 页面配置

1、使能 DHCP 服务器，如图 143 所示；

图 143 DHCP 服务器状态

DHCP 服务器状态

配置选项：使能/不使能

默认配置：不使能

功能：是否选择当前交换机做为 DHCP 服务器为客户端分配 IP 地址。使能时如果选择 VLAN 号，则 DHCP 服务器只给该 VLAN 中的提出申请的客户端分配 IP 地址；如果选择所有 VLAN，则给所有提出申请的客户端分配 IP 地址。

说明：选择 VLAN 号时，只能选择一个 VLAN ID。

2、选择 DHCP 服务器模式，如图 144 所示；

图 144 DHCP 服务器模式

DHCP 服务器模式

配置选项：普通模式/端口模式

默认配置：端口模式

描述：普通模式包括动态分配 IP 地址和静态 MAC 地址绑定；端口模式指端口 IP 设定。

3、端口模式配置；

DHCP 服务器模式选择端口模式时，分配端口静态绑定的 IP 地址，配置如图 145 所示；

端口	设定IP
S1/FE1	
S1/FE2	
S1/FE3	192.168.0.6
S1/FE4	
S1/FE5	
S1/FE6	
S1/FE7	
S1/FE8	

图 145 端口 IP 设定

端口 IP 绑定是在端口处静态配置 IP 地址。当该端口收到客户端请求报文时，将分配该端口绑定的 IP 地址给客户端，这种分配模式具有最高优先级，租期为 1000 天 23 小时 59 分。

CAUTION

注意：

端口绑定的 IP 地址必须和 DHCP 服务器在同一网段。

端口模式分配 IP 地址时，需要配置 DHCP 服务器的 IP 地址池名称、IP 地址池域名和子网掩码，如图 146 所示；

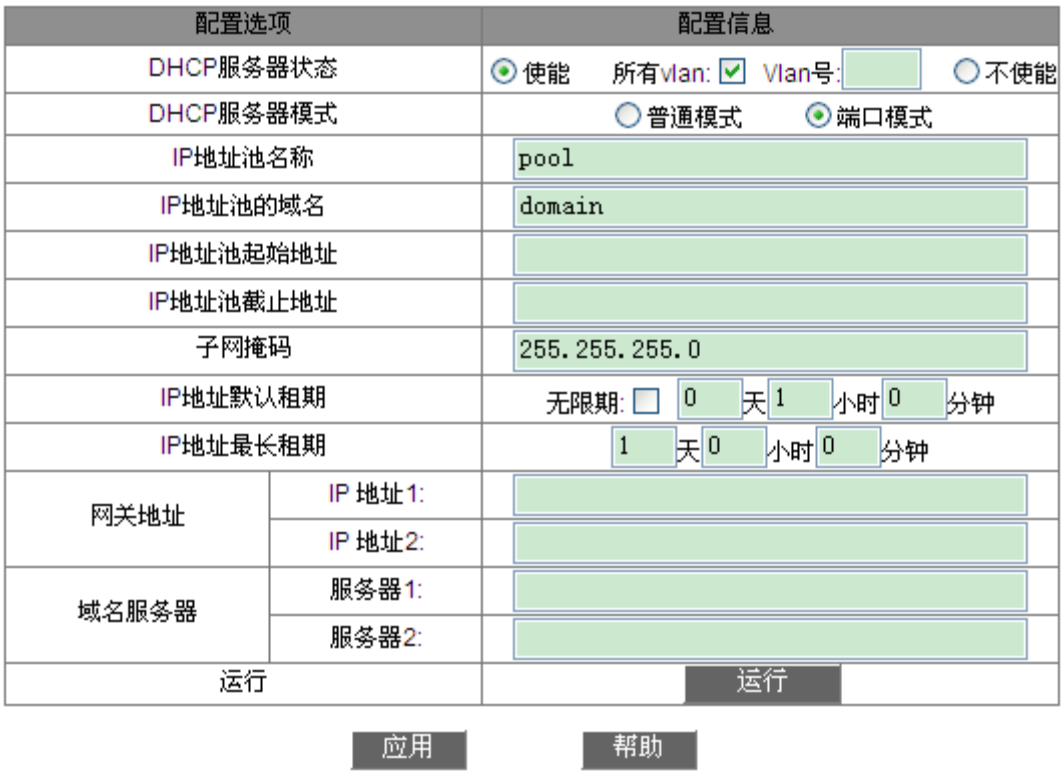

图 146 端口模式服务器配置

IP 地址池名称

配置范围：1~15 个字符

功能：配置 IP 地址池名称。

IP 地址池的域名

配置范围：1~60 个字符

功能：配置 IP 地址池的域名。

子网掩码

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。一般配置成255.255.255.0

注意：

- 配置完成后，需要点击页面中的<运行>按钮，才能给客户端分配正确的 IP 地址；
- 配置修改后，再次点击页面中的<运行>按钮，才能给客户端分配正确的 IP 地址。

4、普通模式配置

DHCP 服务器模式选择普通模式时，包括静态 MAC 地址绑定和动态分配 IP 地址，当配

置有静态 MAC 地址绑定时，优先分配 MAC 地址绑定的 IP 地址，否则将从地址池中动态分配 IP 地址；静态 MAC 地址绑定配置如图 147、图 148 所示；动态分配 IP 地址配置如图 149 所示；

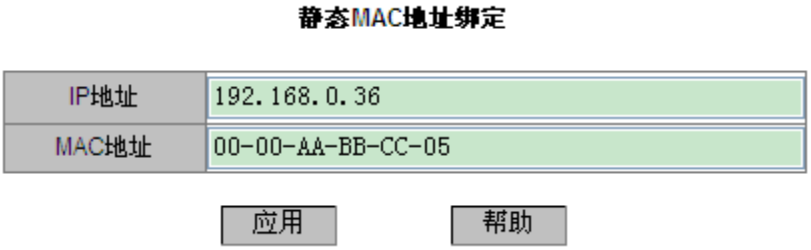

图 147 静态 MAC 地址绑定

静态 MAC 地址绑定是将客户端的 MAC 地址与 IP 地址绑定，当收到的请求报文中源 MAC 地址为指定 MAC 地址时，将分配该 MAC 地址绑定的 IP 地址给客户端，这种分配模式优先级高于动态分配 IP 地址，租期为 1000 天 23 小时 59 分。此分配模式时，需要对服务器进行图 149 所示配置。

配置完成后“静态 MAC 地址绑定列表”显示了静态配置的 MAC 地址和 IP 地址的绑定关系，选中相应的序号，可以删除某一绑定表项。

图 148 静态 MAC 地址绑定列表

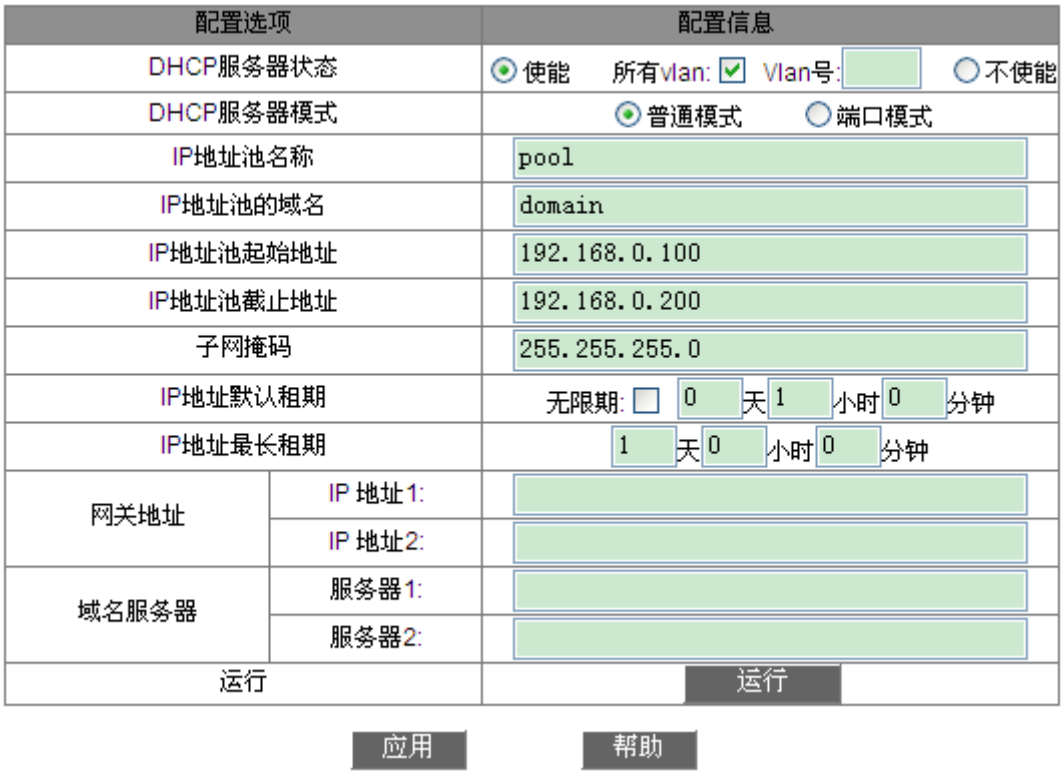

图 149 普通模式服务器配置

IP 地址池名称

配置范围：1~15 个字符

功能：配置 IP 地址池名称。

IP 地址池的域名

配置范围：1~60 个字符

功能：配置 IP 地址池的域名。

IP 地址池起始地址/IP 地址池截止地址

配置格式：A.B.C.D (起始地址和截止地址必须在同一网段)

子网掩码

子网掩码是长度为 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。采用动态地址分配方式时，需要配置地址池的地址范围，地址范围的大小通过子网掩码来设定。

IP 地址默认租期

配置范围：0 天 0 小时 1 分~1000 天 23 小时 59 分/无限期

默认配置：0 天 1 小时 0 分

描述：如果客户端发送申请 IP 地址请求报文时，报文中没有包含有效租期值时，服务器按照此默认值给客户端分配 IP 地址。

IP 地址最长租期

配置范围：0 天 0 小时 1 分~1000 天 23 小时 59 分

默认配置：1 天 0 小时 0 分

描述：客户端发送申请 IP 地址请求报文时，报文中包含的有效租期值不能超过配置的 IP 地址最长租期值。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。

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两个 2 个网关地址。

域名服务器

通过域名访问网络上的主机时，需要将域名解析为 IP 地址，这是通过域名系统(DNS)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域名服务器 IP 地址。DHCP 地址池可以配置 2 个域名服务器地址。

注意：

- 根据客户端所在网络拓扑结构配置正确的网关地址；
- 配置完成后，需要点击页面上的<运行>按钮，才能给客户端分配正确的 IP 地址；
- 配置修改后，再次点击页面中的<运行>按钮，才能给客户端分配正确的 IP 地址。

6.28.1.4 典型配置举例

如图 150 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，服务器可以通过三种方式为客户端分配 IP 地址。

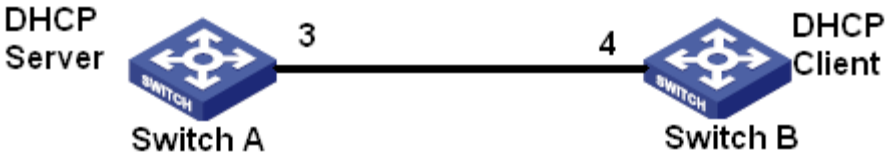

图 150 DHCP 典型配置举例

端口 IP 绑定方式

➢ 交换机 A 的配置：

1、使能 DHCP 服务器状态，见图 143；

2、选择 DHCP 服务器模式为端口模式，见图 144；

3、IP 地址池名称配置为 pool，地址池域名配置为 domain，子网掩码配置为 255.255.255.0，见图 146；

4、端口 3 绑定 IP 地址为 192.168.0.6，见图 145；

5、点击服务器配置中的<运行>按钮，开始运行服务器。

➢ 交换机 B 的配置：

1、交换机 B 作为 DHCP 客户端自动获取 IP 地址；

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 151 所示；

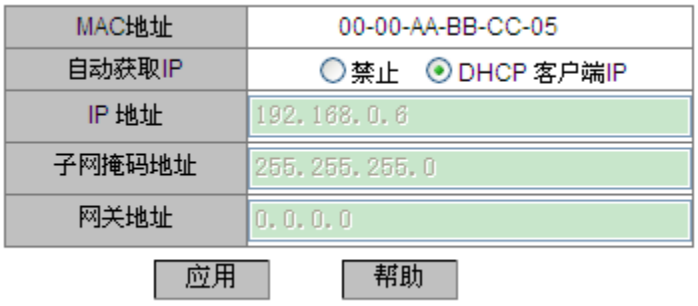

图 151 DHCP 客户端获取 IP 地址-1

静态 MAC 地址绑定方式

➢ 交换机 A 的配置：

1、使能 DHCP 服务器状态，见图 143；

2、选择 DHCP 服务器模式为普通模式，见图 144；

3、IP 地址池名称配置为 pool，地址池域名配置为 domain，地址池的起始地址和截止地址分别为 192.168.0.3 和 192.168.0.201；子网掩码配置 255.255.255.0；租期采用默认值，见图 149；

4、绑定交换机 B 的 MAC：00-00-AA-BB-CC-05 与 IP 地址：192.168.0.36，见图 147；

5、点击服务器配置中的<运行>按钮，开始运行服务器。

➢ 交换机 B 的配置：

1、交换机 B 作为 DHCP 客户端自动获取 IP 地址；

2、交换机 B 从 DHCP 服务器上获取 IP 地址：192.168.0.36，子网掩码：255.255.255.0，如图 152 所示；

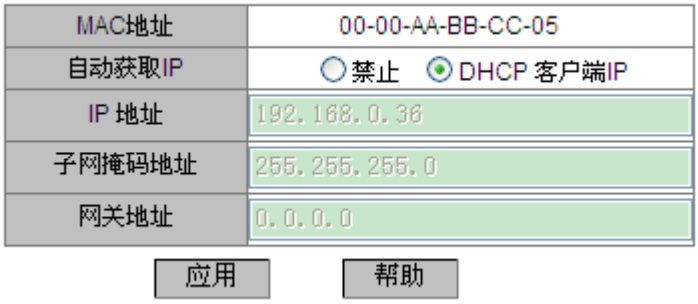

图 152 DHCP 客户端获取 IP 地址-2

地址池中动态获取方式

➢ 交换机 A 的配置：

1、使能 DHCP 服务器状态，见图 143；

2、选择 DHCP 服务器模式为普通模式，见图 144；

3、IP 地址池名称配置为 pool，地址池域名配置为 domain，地址池的起始地址和截止地址分别为 192.168.0.3 和 192.168.0.201，子网掩码配置 255.255.255.0；租期采用默认值，见图 149；

4、点击服务器配置中的<运行>按钮，开始运行服务器。

➢ 交换机 B 的配置：

1、交换机 B 作为 DHCP 客户端自动获取 IP 地址；

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 地址及其他网络参数分配给交换机 B，子网掩码：255.255.255.0，如图 153 所示；

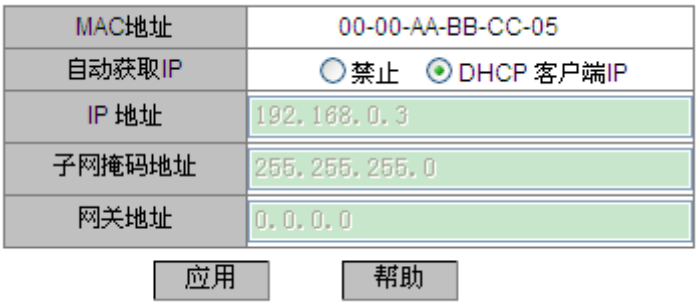

图 153 DHCP 客户端获取 IP 地址-3

DHCP Snooping

6.28.2.1 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。

6.28.2.2 Web 页面配置

1、使能 DHCP Snooping 功能，如图 154 所示；

图 154 DHCP Snooping 状态

DHCP Snooping 状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能交换机的 DHCP Snooping 功能。

注意：

做为 DHCP 服务器和客户端的交换机不能使能 DHCP Snooping 功能。

2、配置信任端口，如图 155 所示；

端口	端口状态
S1/FE1	◉ 信任 ○ 非信任
S1/FE2	○ 信任 ◉ 非信任
S1/FE3	○ 信任 ◉ 非信任
S1/FE4	○ 信任 ◉ 非信任
S1/FE5	○ 信任 ◉ 非信任
S1/FE6	○ 信任 ◉ 非信任
S1/FE7	○ 信任 ◉ 非信任
S1/FE8	○ 信任 ◉ 非信任

图 155 信任端口配置

端口状态

配置选项：信任/非信任

默认配置：非信任

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。

注意：

信任端口配置与端口聚合互斥，加入聚合组的端口不能配置为信任端口；信任端口不能加入聚合组。

6.28.2.3 典型配置举例

如图 156 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。

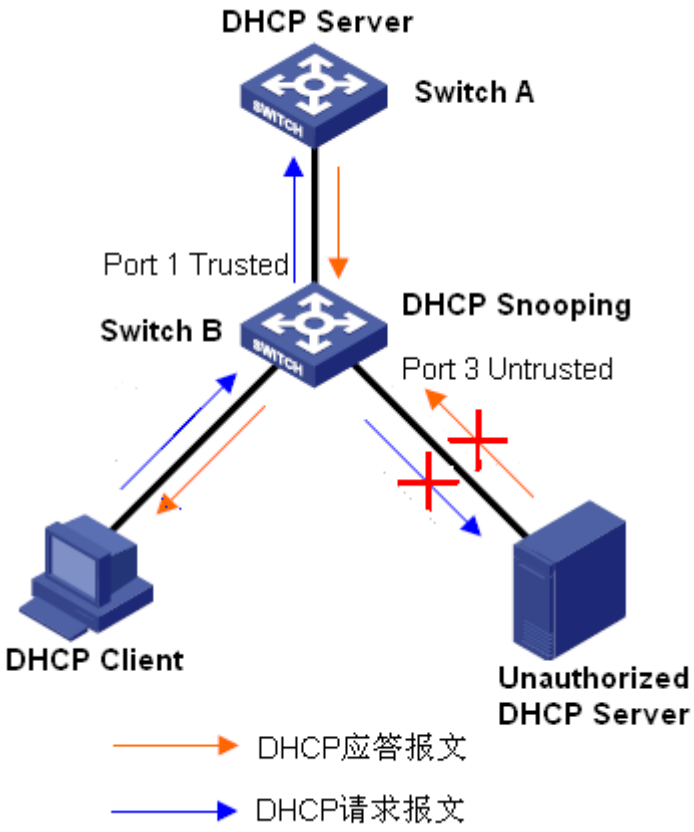

图 156 DHCP Snooping 典型配置举例

交换机 B 配置过程：

- 使能 DHCP Snooping 功能，见图 154；
- 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 155。

Option 82 配置

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 Snooping 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，报文中需要添加 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，如表 9 所示；

表 9 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 Snooping 设备接收到客户端请求报文的端口的 VLAN ID；

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

- Sub-option2 内容可以是接收 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址如表 10 所示；也可以是用户自己配置的字符串如表 11 所示；

表 10 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

表 11 sub-option2 字段格式-字符串

Sub-option type (0x02)	Length (0x10)	字符串
1 个字节	1 个字节	16 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，字符串占用 16 个字节；

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

字符串：Sub-option2 内容是用户自己配置的 1~16 个字符(字符用 ASCⅡ码表示，每个字符占用一个字节)，此时 Length 为固定值 16。如果配置的字符串长度小于 16 字节，后面自动用 0 补齐。

6.28.3.1 DHCP Snooping 支持 Option 82 功能

1 介绍

如果 DHCP Snooping 支持 Option82 功能，则当 DHCP Snooping 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。具体的处理方式如表 12 所示；

表 12 DHCP Snooping 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 Snooping 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 Snooping 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 Snooping 设备的 Option82 字段并进行转发

当 DHCP Snooping 接收到 DHCP 服务器的响应报文时，如果报文中含有 Option 82，则删除 Option82 字段并转发给客户端，如果报文中不带有 Option82，则根据服务器策略对响应报文进行相应的处理，如表 13 所示；

表 13 DHCP Snooping 对响应报文的处理方式

收到 DHCP 服务器响应报文	服务器策略	DHCP Snooping 对响应报文的处理
响应报文中带有 Option 82	丢弃/保留	删除该响应报文中的 Option82 字段并进行转发
响应报文中不带有 Option 82	丢弃	丢弃该响应报文
	保留	保持该报文格式不变并进行转发

2 Web 页面配置

DHCP Snooping option82 配置如图 157 所示；

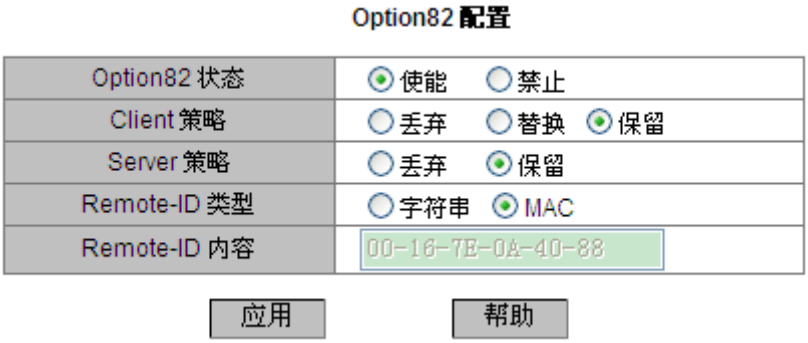

图 157 DHCP Snooping option82 配置

Option82 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 DHCP Snooping 设备的 Option82 功能。

Client 策略

配置选项：丢弃/替换/保留

默认配置：保留

功能：配置客户端策略，DHCP Snooping 根据客户端策略对 Client 发送的请求报文的处理情况如表 12 所示。

Server 策略

配置选项：丢弃/保留

默认配置：保留

功能：配置服务器端策略，DHCP Snooping 根据服务器端策略对 Server 发送的响应报文的处理情况如表 13 所示。

Remote-ID 类型

配置选项：字符串/MAC

默认配置：MAC

功能：配置 sub-option2 的内容。

描述：选择 MAC 指 sub-option2 的内容是接收到客户端请求报文的 DHCP Snooping 设备的 MAC 地址；选择字符串时 sub-option2 的内容是由用户自己定义的字符串。

Remote-ID 内容

配置选项：MAC 地址/1~16 个字符

默认配置：MAC 地址

描述：当 Remote-ID 类型配置为 MAC 时，Remote-ID 内容强制为当前 Snooping 设备的 MAC 地址；当 Remote-ID 类型为字符串时，Remote-ID 内容由用户自己配置，配置内容为 1~16 个字符(每个字符占用一个字节)。

6.28.3.2 DHCP Server 支持 Option 82 功能

1 介绍

如果配置 DHCP Server 支持 Option82 功能，则当 DHCP 服务器接收到 DHCP 请求报文后，将根据报文中是否包含 Option82 以及服务器用户的配置提供不同的地址分配方案。

DHCP 服务器端的配置变量包括：

类：每个 DHCP 服务器可以配置 32 个类，每个类中包含起止 IP 地址范围、无条件匹配和样本信息三个变量；

样本信息变量和 Option82 字段进行匹配，该变量值和 Option82 字段相同时认为匹配，否则认为不匹配。

无条件匹配开启认为样本信息和 Option82 字段永远匹配，不需要判断；无条件匹配关闭则需要判断样本信息和 Option82 字段是否匹配。

根据以上变量的配置，服务器对请求报文的具体处理方案如

表 14 所示；

表 14 DHCP Server 支持 Option82 功能时对请求报文的处理

<table>
<tr><th>收到 DHCP 客户端请求报文</th><th colspan="2">变量配置</th><th>DHCP Server 对请求报文的处理</th></tr>
<tr><td rowspan="3">请求报文中带有 Option 82</td><td colspan="2">无条件匹配开启</td><td>响应报文中携带 Option82，并为客户端分配 IP 地址等信息</td></tr>
<tr><td rowspan="2">无条件匹配关闭</td><td>配置有样本信息值</td><td>➢ 样本信息值与 Option82 字段匹配：响应报文中携带 Option82，并为客户端分配 IP 地址等信息
➢ 样本信息值与 Option82 字段不匹配：服务器不给客户端分配 IP 地址</td></tr>
<tr><td>没有配置样本信息值</td><td>服务器不给客户端分配 IP 地址</td></tr>
<tr><td rowspan="2">请求报文中不带有 Option 82</td><td colspan="2">无条件匹配开启</td><td>响应报文中不带 Option82，为客户端分配 IP 地址等信息</td></tr>
<tr><td colspan="2">无条件匹配关闭</td><td>服务器不给客户端分配 IP 地址</td></tr>
</table>

如果配置 DHCP Server 不支持 Option82 功能，则当 DHCP 服务器收到带有 Option82 的报文后，响应报文中不携带 Option82，可以为客户端分配 IP 地址等信息。该情况下服务器对请求报文的具体处理方案如表 15 所示；

表 15 DHCP Server 不支持 Option82 功能时对请求报文的处理

收到 DHCP 客户端请求报文	DHCP Server 对请求报文的处理
请求报文中带有 Option 82	响应报文中不带 Option82 字段，为客户端分配 IP 地址等信息
请求报文中不带有 Option 82	

2 Web 页面配置

- 使能 DHCP server 的 Option82 功能，如图 158 所示；

图 158 使能 DHCP server 的 Option82 功能

DHCP 服务器 Option82 使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 DHCP server 的 Option82 功能。

- DHCP server Option82 配置如图 159 所示；

图 159 DHCP server option82 配置

操作

配置选项：添加/删除

默认配置：添加

功能：添加/删除指定类。

操作对象

配置选项：类/样本信息/起止 IP/无条件匹配

默认配置：类

描述：添加类时，可以对下面的参数进行配置。删除类时，指定类名即可删除。添加样本信息向已创建的指定类中添加样本信息，一个类中可以添加多个样本信息。添加起止 IP/无条件匹配时，修改已创建的指定类中的相关参数配置。删除样本信息可以删除当前类中指定的样本信息。

类名

配置范围：1~15 个字符

功能：配置该类的类名。

样本信息

配置范围：12~60 个十六进制数

功能：配置该类的样本信息值。

起始 IP/终止 IP

配置格式：A.B.C.D

说明：配置该类中的起止 IP 地址范围，此范围应该从 DHCP Server 的地址池内选取。

无条件匹配

配置选项：开启/关闭

功能：是否打开无条件匹配。开启时认为样本信息和 Option82 字段永远匹配，不需要判断；关闭时需要判断样本信息和 Option82 字段是否匹配。

注意：

创建多个类时，DHCP server 按照样本信息匹配的类信息给 client 分配 IP 地址；如果有多个类样本信息都匹配时，则按照最先创建的类信息给 client 分配 IP 地址。

- DHCP server Option82 查询如图 160 所示；

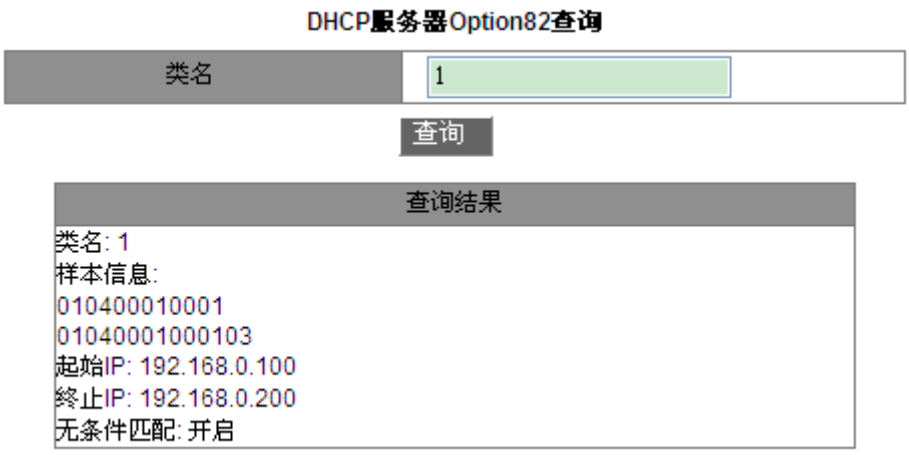

图 160 DHCP server option82 查询

附录 缩略语表

缩略语	英文全称	中文
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
CLI	Command Line Interface	命令行接口
CRC	Cyclic Redundancy Check	循环冗余校验
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHP	Dual Homing Protocol	双归链路协议
DRP	Distributed Redundancy Protocol	分布式冗余协议
DSCP	Differentiated Services CodePoint	差分服务编码点
FTP	File Transfer Protocol	文件传输协议
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
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
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
MAC	Media Access Control	媒体访问控制
MIB	Management Information Base	管理信息库
NMS	Network Management Station	网络管理站
OID	Object Identifier	对象标识符
PVLAN	Private VLAN	私有 VLAN
QoS	Quality of Service	服务质量
RMON	Remote Network Monitoring	远程网络监控
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
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
STP	Spanning Tree Protocol	生成树协议

TCP	Transmission Control Protocol	传输控制协议
ToS	Type of Service	服务类型
VLAN	Virtual Local Area Network	虚拟局域网
WRR	Weighted Round Robin	加权轮询调度