Aquam8012A 系列工业以太网交换机

Web 操作手册

出版日期：2021 年 10 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.cn

客户服务热线：010-88796676

传真：010-88796678

邮箱：services@kyland.com.cn

目录

前言 1

1 产品介绍 5

1.1 概述 5

1.2 软件特性 5

2 交换机的访问方式 6

2.1 视图类型简介 6

2.2 Console 口访问 7

2.3 Telnet 访问 11

2.4 Web 访问 12

3 设备信息 14

3.1 交换机主要信息 14

4 交换机维护 15

4.1 保存当前配置 15

4.2 回复出厂配置 15

4.3 软件升级 15

4.3.1 FTP 升级 15

4.3.2 TFTP 升级 19

4.3.3 SFTP 升级 22

4.4 软件版本选择 24

4.5 重新启动 25

5 设备基本配置 27

5.1 基本配置 27

5.1.1 基本配置 27

5.1.2 时钟配置 28

5.2 用户管理配置 29

5.2.1 Web 页面配置 30

5.3 端口配置 34

5.3.1 物理端口配置 34
5.3.2 端口信息查看 37
5.4 VLAN 配置....38
5.4.1 介绍 38
5.4.2 原理 38
5.4.3 基于端口的 VLAN 介绍....39
5.4.4 Web 页面配置....40
5.4.5 典型配置举例 46
5.5 QinQ 配置....47
5.5.1 介绍 47
5.5.2 设备支持的 QinQ 特性 49
5.5.3 QinQ 外层 VLAN tag 的 TPID 值可配置 49
5.5.4 Web 页面配置....51
5.6 端口镜像....52
5.6.1 介绍 52
5.6.2 说明 52
5.6.3 Web 页面配置....52
5.6.4 典型配置举例 54
5.7 端口风暴抑制....54
5.7.1 介绍 54
5.7.2 Web 页面配置....55
5.7.3 典型配置举例 56
5.8 端口隔离....57
5.8.1 介绍 57
5.8.2 Web 页面配置....57
5.8.3 典型配置举例 58
5.9 Port channel....58
5.9.1 介绍 58

5.9.2 实现 59
5.9.3 说明 59
5.9.4 Web 页面配置 60
5.9.5 典型配置举例 62
5.10 Telnet 服务器配置 62
5.10.1 介绍 62
5.10.2 Web 页面配置 62
5.11 SSH 服务器配置 64
5.11.1 介绍 64
5.11.2 密钥 64
5.11.3 实现 64
5.11.4 Web 页面配置 65
5.11.5 典型配置举例 67
5.12 SSL 配置 75
5.12.1 介绍 75
5.12.2 Web 页面配置 75
5.13 访问管理 76
5.13.1 Web 页面配置 76
5.14 文件传输服务 78
5.14.1 TFTP 服务 78
5.14.2 FTP 服务 82
5.14.3 SFTP 服务 89
5.15 MAC 地址配置 91
5.15.1 介绍 91
5.15.2 Web 页面配置 92
5.16 基本配置维护和调试信息 95
6 设备高级配置 101
6.1 ARP 配置 101

6.1.1 介绍 101
6.1.2 说明 101
6.1.3 代理 ARP 101
6.1.4 Web 页面配置 102
6.1.5 典型配置举例 104
6.2 三层接口配置 105
6.2.1 查看交换机 IP 地址 105
6.2.2 IP 地址配置 106
6.3 SNMPv2c 109
6.3.1 介绍 109
6.3.2 实现 109
6.3.3 说明 110
6.3.4 MIB 介绍 110
6.3.5 Web 页面配置 111
6.3.6 典型配置举例 115
6.4 SNMP v3 116
6.4.1 介绍 116
6.4.2 实现 116
6.4.3 Web 页面配置 117
6.4.4 典型配置举例 125
6.5 DT-Ring 126
6.5.1 介绍 126
6.5.2 概念 126
6.5.3 实现 127
6.5.4 说明 130
6.5.5 Web 页面配置 130
6.5.6 典型配置举例 135
6.6 STP/RSTP 135

6.6.1 介绍 135
6.6.2 基本概念 136
6.6.3 BPDU 配置消息 136
6.6.4 实现过程 137
6.6.5 Web 页面配置 138
6.6.6 典型配置举例 142
6.7 DRP 144
6.7.1 介绍 144
6.7.2 概念 144
6.7.3 实现 146
6.8 DHP 150
6.8.1 介绍 150
6.8.2 概念 151
6.8.3 实现 152
6.8.4 说明 153
6.8.5 Web 页面配置 153
6.8.6 典型配置举例 163
6.9 MSTP 配置 163
6.9.1 介绍 163
6.9.2 基本概念 164
6.9.3 MSTP 的实现 168
6.9.4 Web 页面配置 169
6.9.5 典型配置举例 177
6.10 告警 179
6.10.1 介绍 179
6.10.2 Web 页面配置 180
6.11 日志配置 187
6.11.1 介绍 187

6.11.2 Web 页面配置 187
6.12 DHCP 配置 191
6.12.1 DHCP 服务器配置 192
6.13 ACL 配置 205
6.13.1 介绍 205
6.13.2 ACL 表项与规则 205
6.13.3 Web 页面配置 206
6.13.4 典型配置举例 211
6.14 QoS 配置 211
6.14.1 介绍 211
6.14.2 QoS CAR 212
6.14.3 QoS Remark 212
6.14.4 QoS 212
6.14.5 Web 页面配置 213
6.14.6 典型配置举例 225
6.15 IEC61850 配置 227
6.15.1 介绍 227
6.15.2 Web 页面配置 227
6.16 IGMP Snooping 229
6.16.1 介绍 229
6.16.2 基本概念 229
6.16.3 原理 229
6.16.4 Web 页面配置 230
6.16.5 典型应用举例 234
6.17 GMRP 235
6.17.1 GARP 介绍 235
6.17.2 GMRP 协议 236
6.17.3 说明 236

6.17.4 Web 页面配置 237
6.17.5 典型配置举例 241
6.18 未知组播动作配置 242
6.18.1 介绍 242
6.18.2 Web 页面配置 242
6.19 静态组播配置 244
6.19.1 介绍 244
6.19.2 Web 页面配置 244
6.20 LLDP 245
6.20.1 介绍 245
6.20.2 Web 页面配置 245
6.21 RMON 248
6.21.1 介绍 248
6.21.2 RMON 组 248
6.21.3 Web 页面配置 249
6.22 SNTP 配置 254
6.22.1 介绍 254
6.22.2 Web 页面配置 254
6.23 NTP 配置 255
6.23.1 介绍 255
6.23.2 NTP 工作模式 256
6.23.3 Web 页面配置 256
6.23.4 典型配置举例 261
6.24 TACACS+配置 264
6.24.1 介绍 264
6.24.2 Web 页面配置 265
6.24.3 典型配置举例 266
6.25 RADIUS 配置 267

6.25.1 介绍 267
6.25.2 Web 页面配置 268
6.25.3 典型配置举例 269
6.26 IEEE802.1x 配置 270
6.26.1 介绍 270
6.26.2 Web 页面配置 270
6.26.3 典型配置举例 275
6.27 登录认证配置 276
6.28 诊断功能配置 277
6.28.1 链路状态检测 277
6.28.2 电缆检测配置 279
6.29 环路检测配置 282
6.29.1 介绍 282
6.29.2 Web 页面配置 283
6.29.3 典型配置举例 284
6.30 端口 CRC 保护配置 285
6.30.1 介绍 285
6.30.2 Web 页面配置 285
附录 缩略语表 287

前言

本手册主要介绍本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 口访问交换机 ➢ Telnet 访问交换机 ➢ Web 访问交换机
3、设备信息	交换机主要信息
4、交换机维护	➢保存当前配置 ➢恢复出厂配置 ➢ 重新启动 ➢ 软件升级(FTP、TFTP、SFTP 升级) ➢软件版本选择
5、设备基本配置	➢ 基本配置(基本配置、时钟配置) ➢ 用户管理配置 ➢ 端口配置(物理端口配置、端口信息查看) ➢ VLAN 配置 ➢ QinQ 配置 ➢端口镜像

	➢ 端口风暴抑制 ➢ 端口隔离 ➢ Port channel ➢ Telnet 服务器用户管理 ➢ SSH 服务器配置 ➢ SSL 配置 ➢ 访问管理 ➢ 文件传输(TFTP 服务、FTP 服务、SFTP) ➢ MAC 地址配置 ➢ 基本配置维护和调试信息
6、设备高级配置	➢ ARP 配置 ➢ 三层接口配置 ➢ SNMPv2c、SNMPv3 ➢ DT-Ring ➢ STP/RSTP ➢ DRP ➢ MSTP 配置 ➢ 告警 ➢ 数字诊断功能 ➢ 日志配置 ➢DHCP 服务器配置 ➢ ACL 配置 ➢ QoS 配置 ➢ IEC61850 配置 ➢IGMP Snooping ➢ GMRP ➢ 静态组播配置 ➢LLDP

	➢ RMON ➢SNTP 配置 ➢ NTP 配置 ➢TACACS+配置 ➢ RADIUS 配置 ➢ IEEE802.1x 配置 ➢ 登录认证配置 ➢ 诊断功能配置 ➢ 环路检测配置 ➢ 端口 CRC 保护配置

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、标志约定

标志	说明
CAUTION 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

Aquam8012A 系列工业以太网交换机的配套资料包括以下内容：

资料名称	内容介绍
Aquam8012A 系列工业以太网交换机硬件安装手册	详细了解 **Aquam8012A** 系列产品外型结构、硬件规格以及安装拆卸方法
Aquam8012A 系列工业以太网交换机 Web 操作手册	了解交换机软件功能并掌握各功能模块的 Web 页面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相关手册：

- 通过扫描机身二维码标签获取；
- 通过东土公司网站获取；

1 产品介绍

1.1 概述

该交换机主要应用在轨道交通行业，符合 EN50155、EN50121 行业标准要求。支持 MSTP/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。

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：STP/RSTP、MSTP、DT-Ring 和 IEC62439-6；
- 组播协议：IGMP Snooping、GMRP 和静态组播；
- 交换属性：VLAN、QoS、ARP；
- 带宽管理：端口聚合、端口限速、广播风暴抑制；
- 同步协议：SNTP 和 NTP；
- 安全管理：IEEE802.1x、TACACS+、RADIUS、SSH、SSL、ACL、MAC 地址绑定、端口隔离、用户管理；
- 设备管理：FTP/TFTP/SFTP 软件升级，FTP/TFTP/SFTP 文件传输，日志记录与上传；
- 设备诊断：端口镜像、LLDP、链路状态检测、电缆检测、环路检测、CRC 保护、数字诊断功能；
- 告警功能：CPU/内存利用率告警、端口告警、电源告警、环告警、高温告警、低温告警、端口流量告警、CRC 错误/丢包率告警和光功率告警；
- 网络管理：支持 CLI、Telnet、Web、Kyvision 网管软件管理、DHCP 和 SNMPv1/v2/v3、IEC61850 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，命令行接口)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 各种视图类型

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	查看系统日期和时间； 查看软件版本信息	“**enable**”进入特权用户配置模式
Switch#	特权用户配置模式	配置系统时钟与日期； 传输文件/升级软件； 删除交换机中文件； 配置 CLI 界面语言环境； 查看交换机配置及系统信息； 恢复默认配置； 保存当前配置； 重启交换机	“**config**”从特权用户配置模式进入全局配置模式； “**exit**”返回一般用户配置模式
Switch (config) #	全局配置模式	对交换机进行各个功能模块配置	“**exit**”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；<A.B.C.D>指 IP 地址配置格式；

<FF-FF-FF-FF-FF-FF>指 MAC 地址配置格式； <1-32> character 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 口访问交换机。

1、用 DB9-M12 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]→[所有程序]→[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；

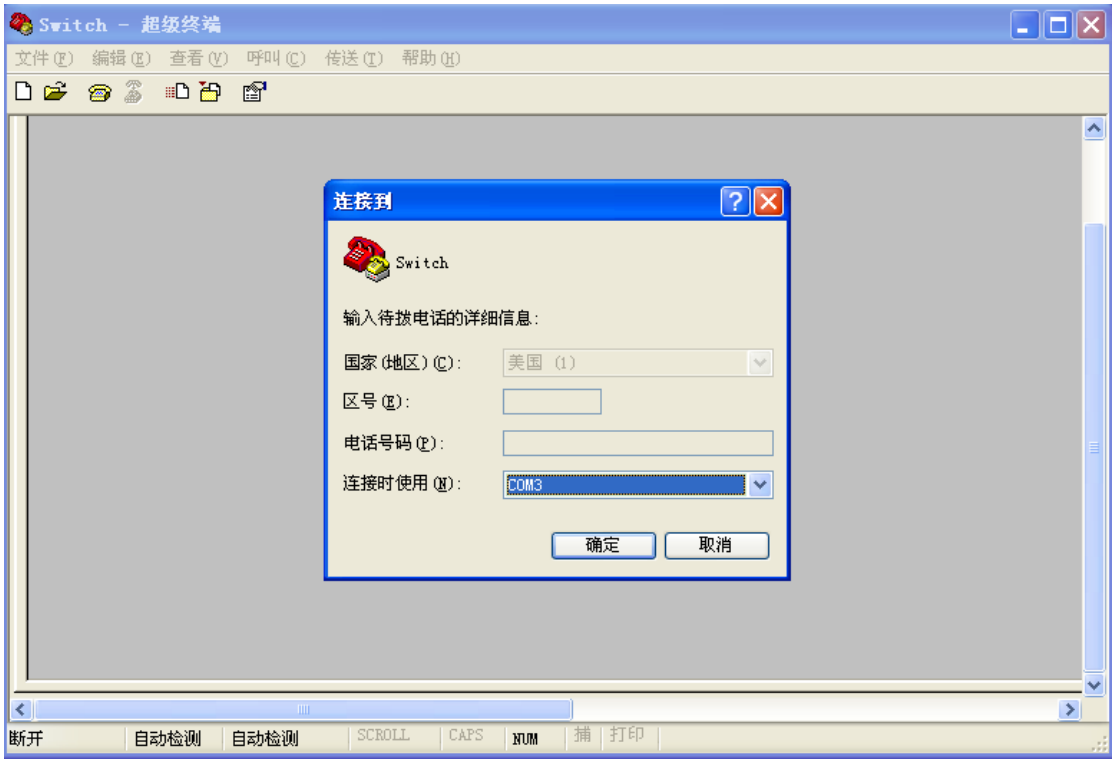


图 3 通信端口选择

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 USB 口使用的通信端口。

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

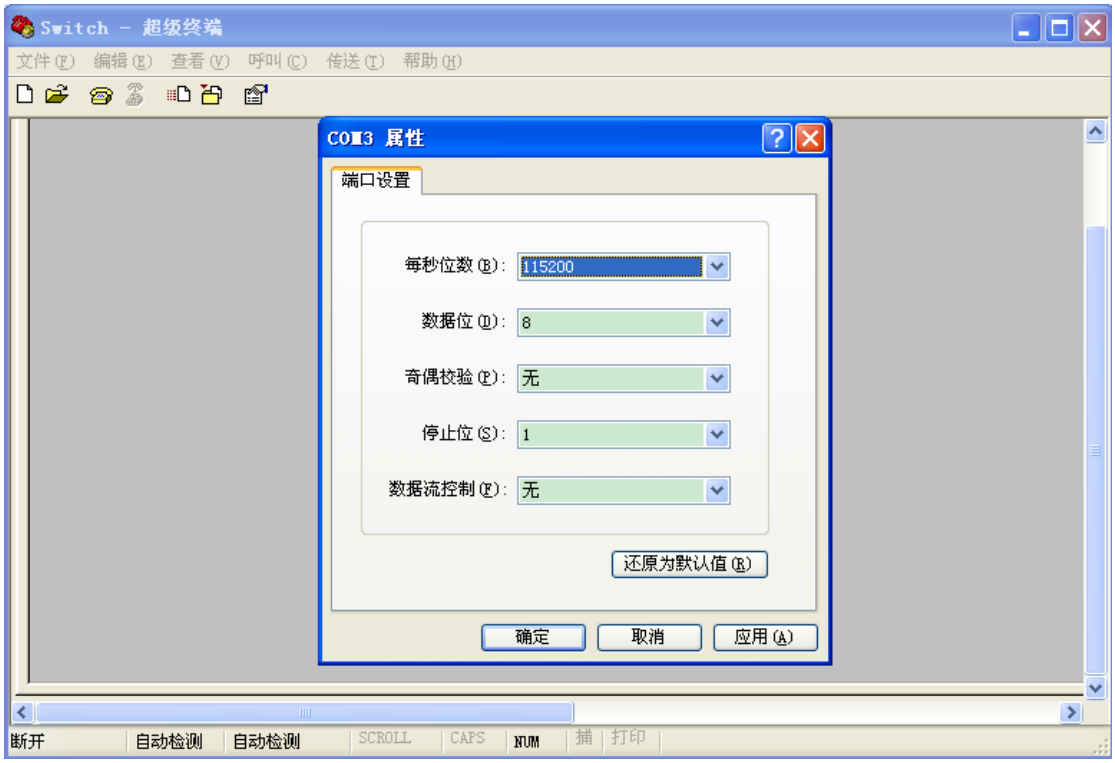


图 4 属性配置

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

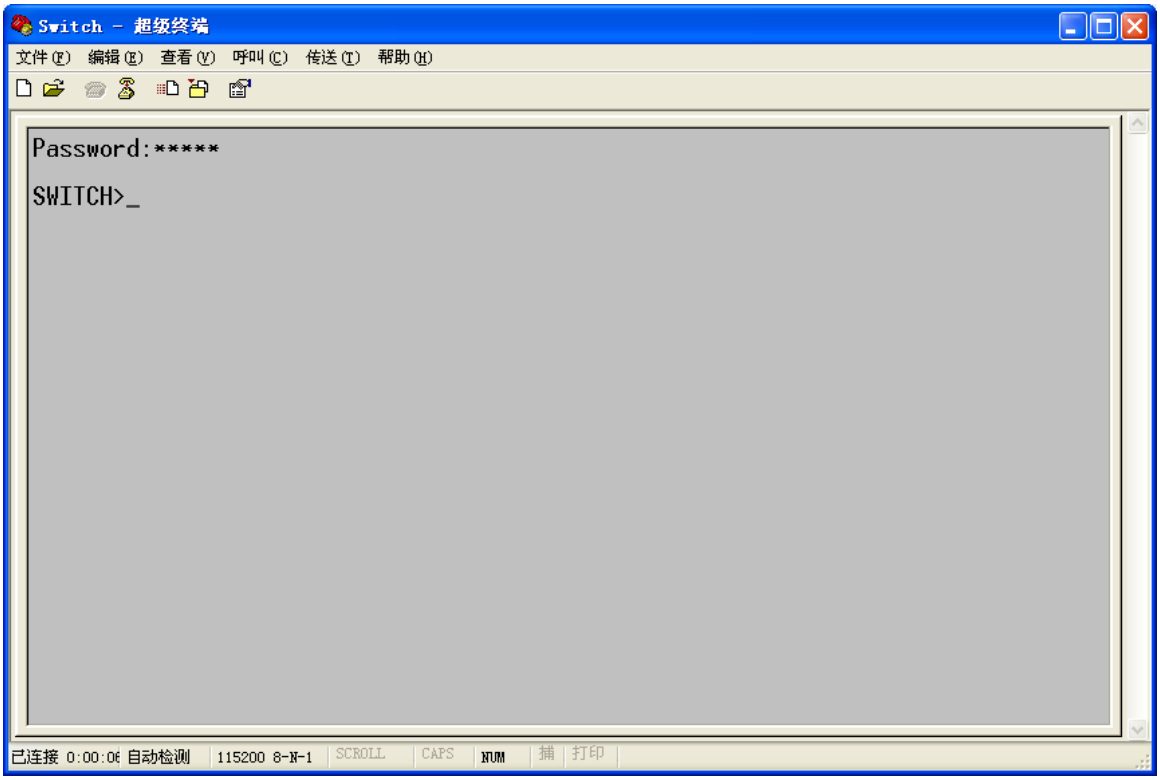


图 5 CLI 界面

7、输入命令”enable”，默认用户名"admin”和密码”123”；也可输入其他已创建的用户名和密码，进入特权用户配置模式，如图 6 所示；

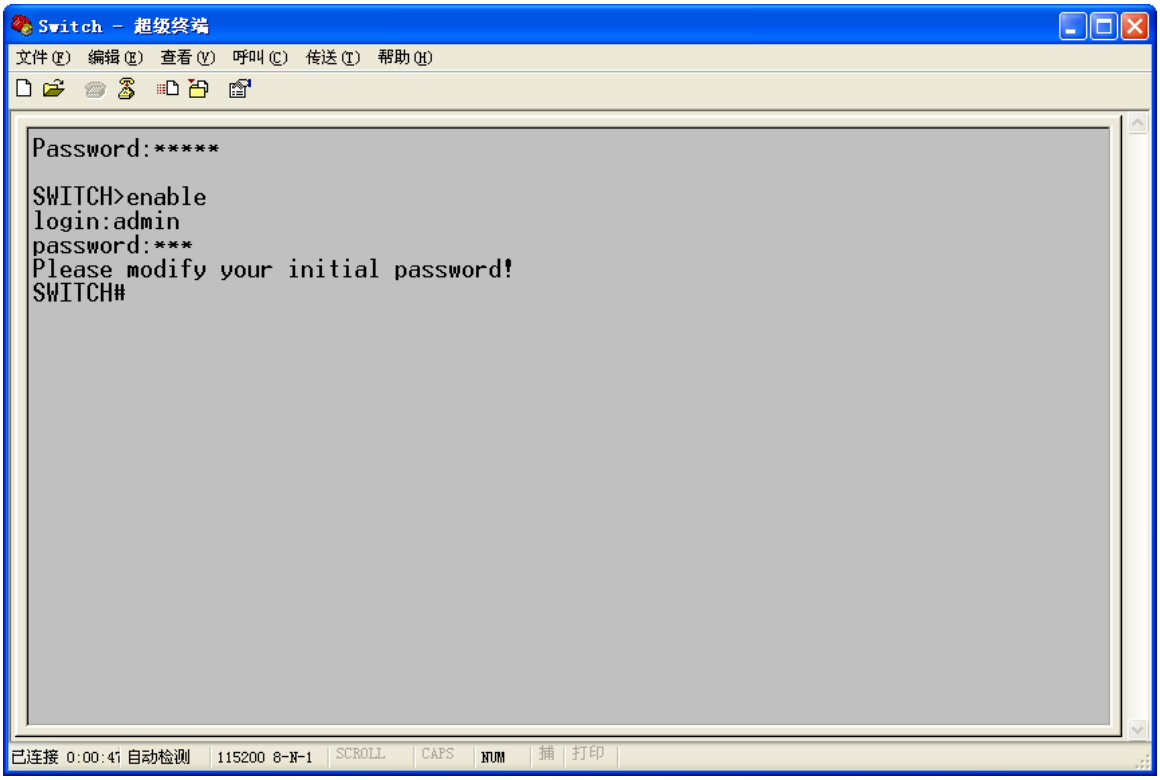


图 6 特权用户配置模式

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”，东土公司交换机的默认 IP 地址为“192.168.0.2”，如图 7 所示；

图 7 Telnet 访问

说明：

如果不清楚当前交换机 IP 地址，请参考“6.2.1 查看交换机 IP 地址”章节获取 IP 地址。

2、Telnet 界面中中输入默认用户名”admin”和密码”123”；也可输入其他已创建的用户名和密码，进入交换机命令行界面，如图 8 所示；

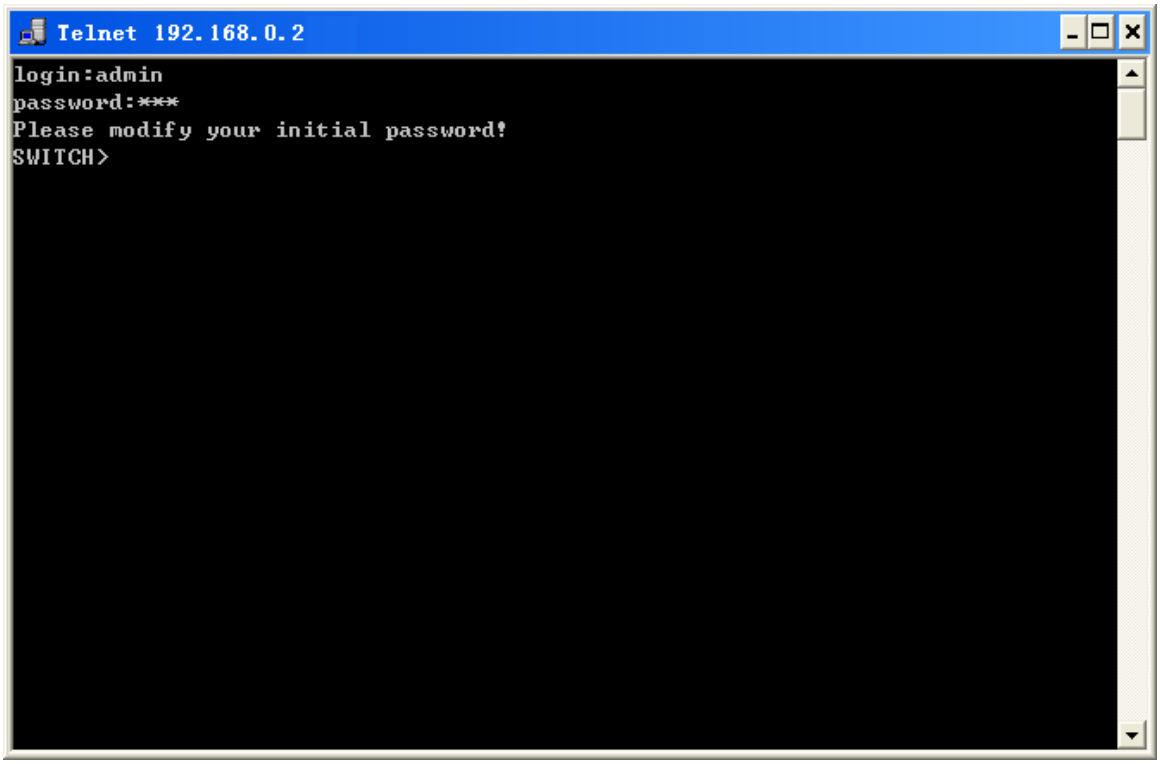


图 8 Telnet 界面

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 9 所示，输入默认用户名”admin”和密码”123”及下方显示的验证码，也可输入其他已创建的用户名和密码，点击<登陆>按钮；

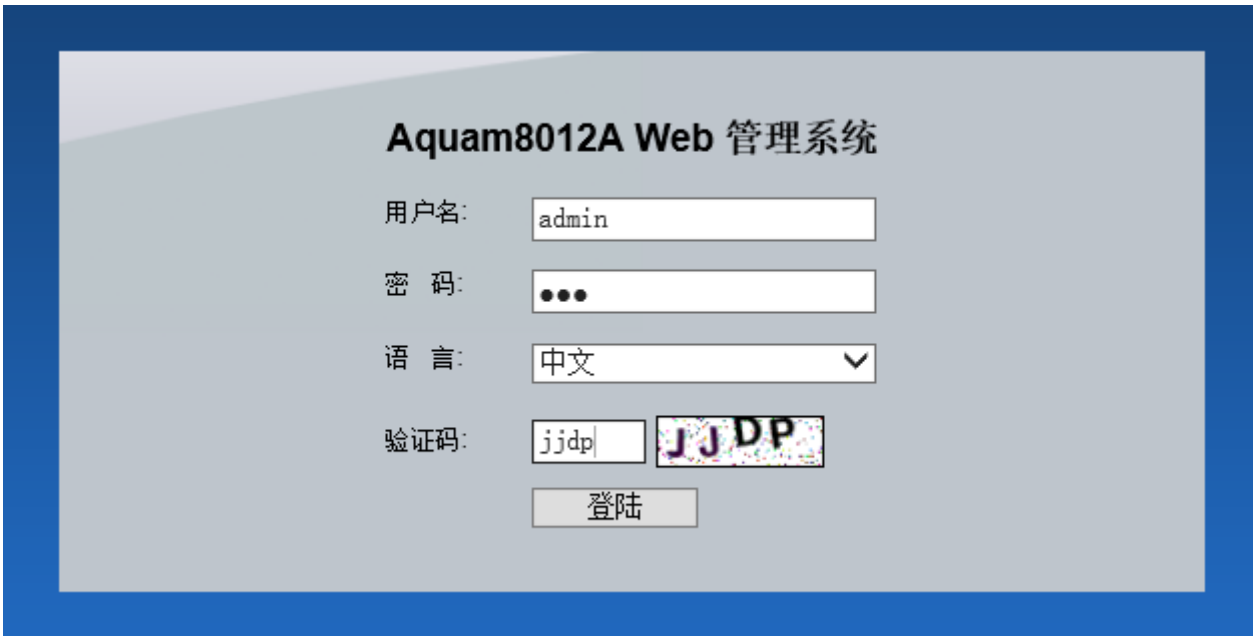


图 9 Web 登录

语言选择 English 可以切换到英文登录界面，出厂配置默认为英文登录界面，选择中文便可以切换到该中文登录界面。

说明：

如果不清楚当前交换机 IP 地址，请参考“6.2.1 查看交换机 IP 地址”章节获取 IP 地址。

2、出现修改密码的提示，点击<确定>按钮；

3、成功登录到交换机 Web 管理页面，左边为配置导航树，如图 10 所示；

图 10 Web 界面

点击右上角<English>按钮可以切换到英文界面；点击<退出系统>按钮便退出 Web 页面配置页面。

3 设备信息

3.1 交换机主要信息

交换机主要信息包括提示符名称、MAC 地址、硬件版本号、软件版本号、bootrom 版本号、设备类型、版本编译时间以及交换机运行时间。

点击导航树[设备信息]→[交换机主要信息]菜单进入交换机主要信息显示界面如图 11 所示。

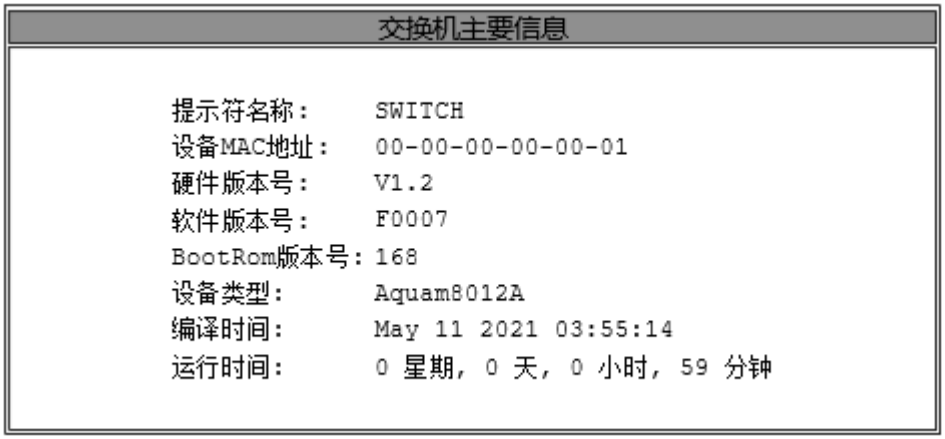


图 11 交换机主要信息

4 交换机维护

4.1 保存当前配置

当设备需要重新启动时，点击导航树[交换机维护]→[保存当前配置]菜单进入保存当前配置界面，如图 12 所示；

图 12 保存配置

4.2 回复出厂配置

当设备需要重新启动时，点击导航树[交换机维护]→[恢复出厂配置]菜单进入恢复出厂配置界面，如图 13 所示；

图 13 恢复出厂默认配置

4.3 软件升级

交换机通过升级软件版本可以获得更完善性能。该系列交换机升级只需升级软件版本文件，该版本文件既携带了系统软件版本，又携带了与该系统软件版本匹配的 bootrom 软件版本。

软件版本升级过程需要借助 FTP/TFTP/SFTP 服务器进行。

4.3.1 FTP 升级

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

1、打开[Security]→[users/rights]对话框点击<New User>按钮添加 FTP 新用户，如图 14 所示，输入用户名和密码，例如：用户名 admin，密码 123，点击<OK>按钮；

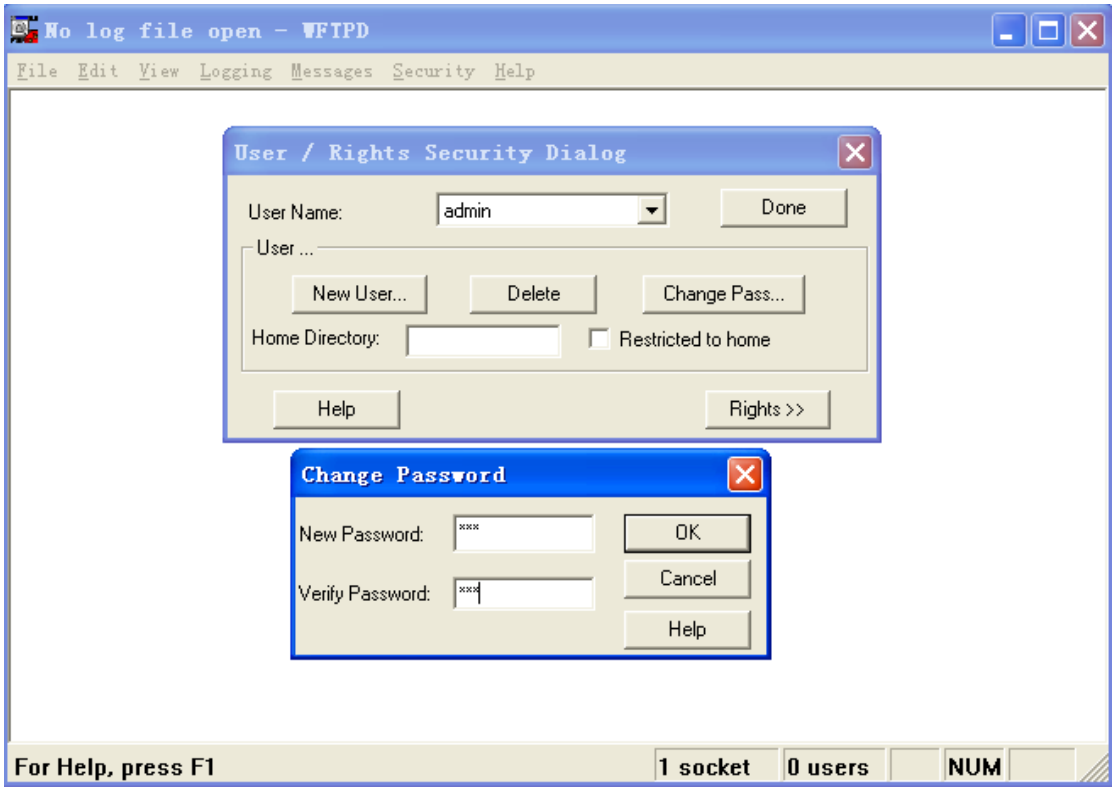


图 14 添加 FTP 新用户

2、Home Directory 栏中输入服务器中软件版本文件的存放路径，如图 15 所示，点击<Done>按钮；

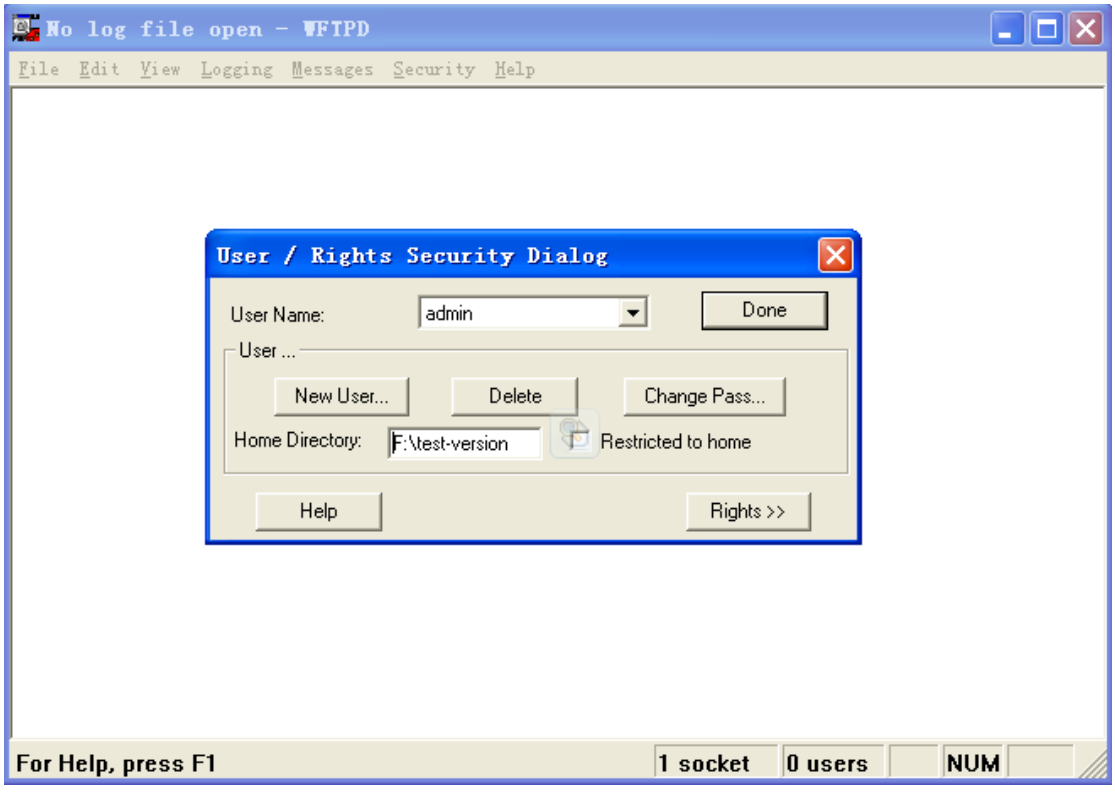


图 15 文件路径修改

3、点击导航树[交换机维护]→[FTP 升级软件]菜单进入 FTP 升级软件界面如图 16 所示，输入 FTP 服务器 IP 地址、建立的 FTP 用户名、用户密码、服务器上文件名，点击<下载>按钮；

图 16 FTP 服务器升级软件

传输类型

配置选项：binary/ascii

默认配置：binary

功能：选择文件传输标准。

说明：ascii 表示采用 ASCII 标准传输文件；binary 表示采用二进制标准传输文件。

强制状态

配置选项：不强制/强制

默认配置：不强制

功能：选择软件版本与交换机硬件不匹配时的处理方式。

描述：不强制表示软硬件不匹配时取消软件升级；强制表示软硬件不匹配时继续升级软件，这种情况可能会导致系统功能异常甚至不能启动。

是否覆盖当前版本

配置选项：覆盖当前版本/不覆盖当前版本

默认配置：覆盖当前版本

功能：是否直接覆盖当前启动使用版本。

描述：若覆盖当前版本，设备重新启动后生效。如果不覆盖当前版本，文件仅上传设备，

作为备用文件使用。

警告：

- 文件名应带有后缀，否则会导致升级失败；
- 软件版本文件属于非文本文件，应采用 binary 二进制标准传输文件；
- 为保证交换机可以正常工作，强制状态选项请选择不强制，即软件与硬件版本不匹配时取消软件升级。

4、确保 FTP 服务器和交换机通信正常，如图 17 所示；

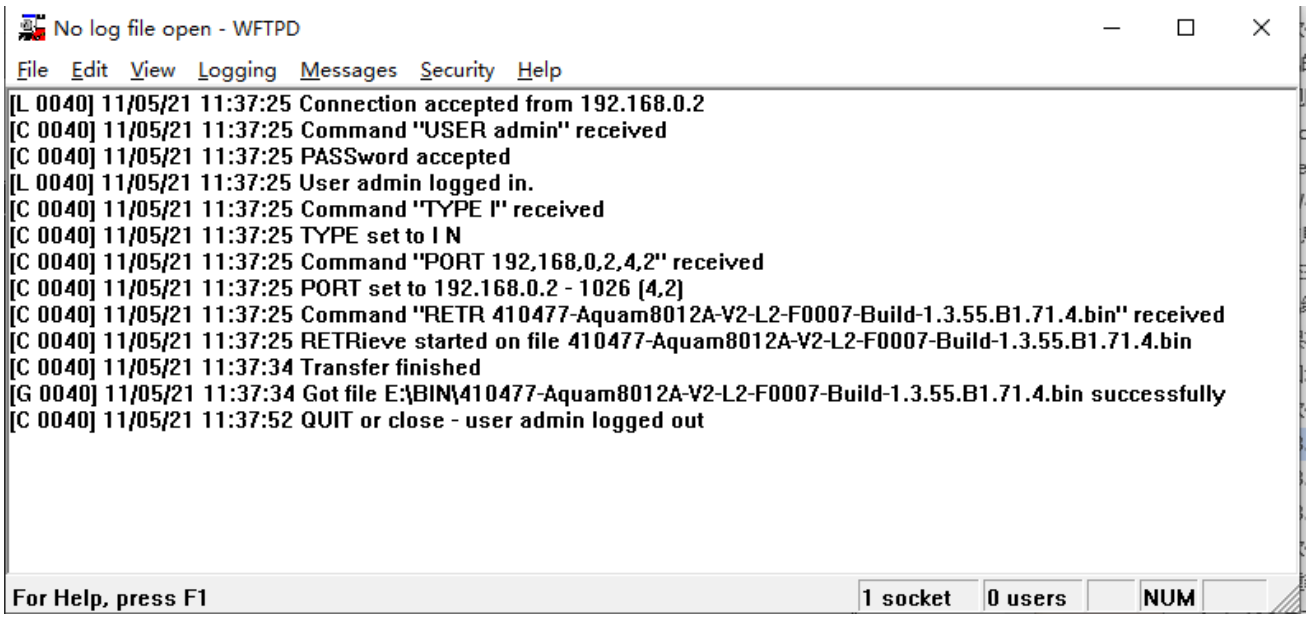


图 17 FTP 服务器和交换机通信正常

注意：

如需显示如图 17 所示的升级日志信息，须在 WFTPD 软件中点击[Logging]→[Log Options]，选择 Enable Logging 和需要显示的日志信息。

5、交换机等待升级过程，如图 18 所示；

图 18 升级等待

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

警告：

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

4.3.2 TFTP 升级

安装 TFTP 服务器，以 TFTPD 软件为例介绍 TFTP 服务器配置及软件升级过程，如图 19 所示；

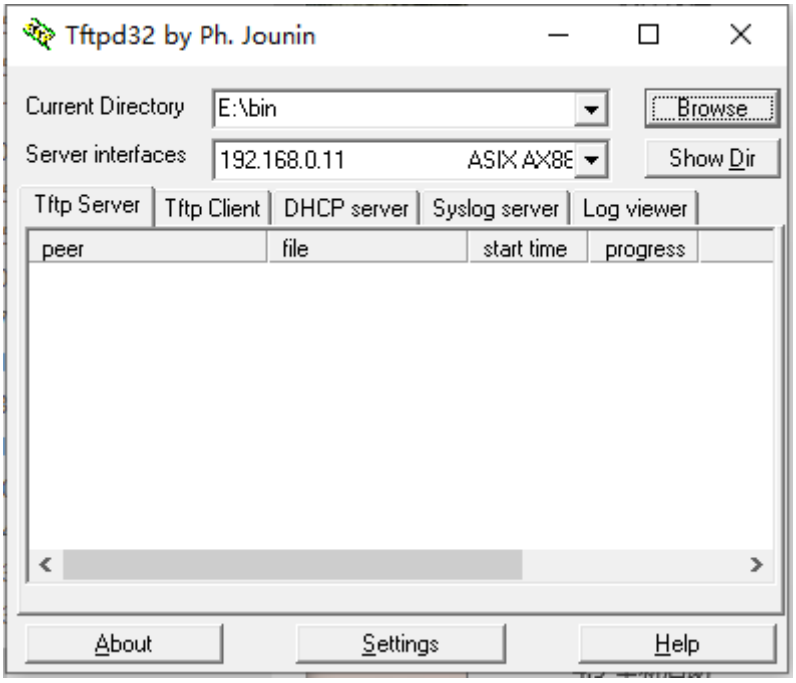


图 19 TFTP 服务器端配置

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

2、点击导航树[交换机维护]→[TFTP 升级软件]菜单进入 TFTP 升级软件界面如图 20 所示，输入 TFTP 服务器 IP 地址、服务器上文件名，点击<下载>按钮；

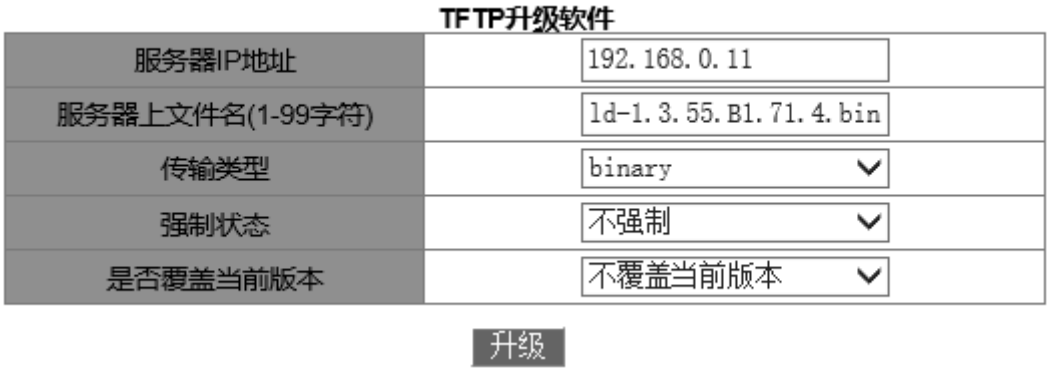


图 20 TFTP 模式下升级软件

传输类型

配置选项：binary/ascii

默认配置：binary

功能：选择文件传输标准。

描述：ascii 表示采用 ASCII 标准传输文件；binary 表示采用二进制标准传输文件。

强制状态

配置选项：不强制/强制

默认配置：不强制

功能：选择软件版本与交换机硬件不匹配时的处理方式。

描述：不强制表示软硬件不匹配时取消软件升级；强制表示软硬件不匹配时继续升级软件，这种情况可能会导致系统功能异常甚至不能启动。

是否覆盖当前版本

配置选项：覆盖当前版本/不覆盖当前版本

默认配置：覆盖当前版本

功能：是否直接覆盖当前启动使用版本。

描述：若覆盖当前版本，设备重新启动后生效，如果不覆盖当前版本，文件仅上传设备，作为备用文件使用。

警告：

- 文件名应带有后缀，否则会导致升级失败；
- 软件版本文件属于非文本文件，应采用 binary 二进制标准传输文件；
- 为保证交换机可以正常工作，强制状态选项请选择不强制，即软件与硬件版本不匹配时取消软件升级。

3、确保 TFTP 服务器和交换机通信正常，如图 21 所示；

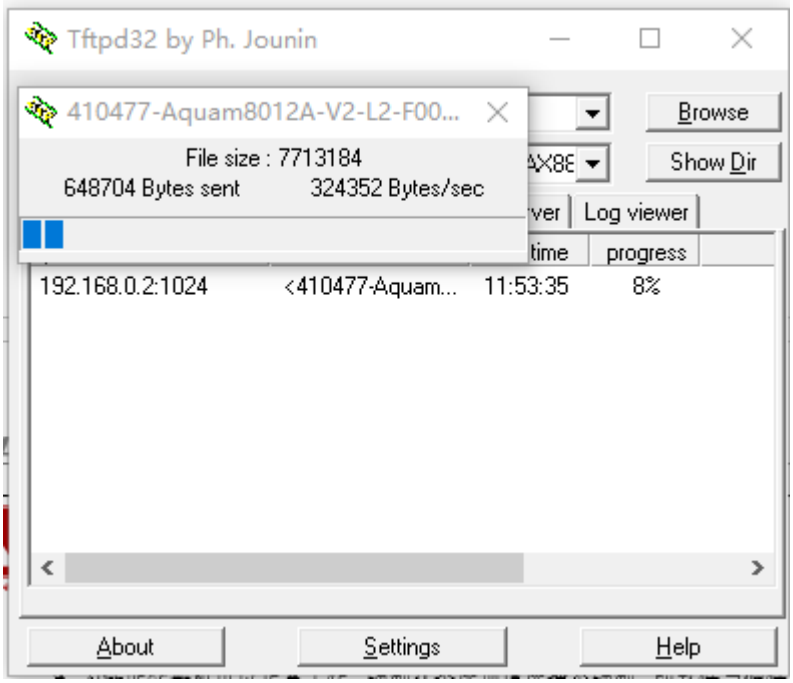


图 21 TFTP 服务器和交换机通信正常

4、交换机等待升级过程，如图 22 所示；

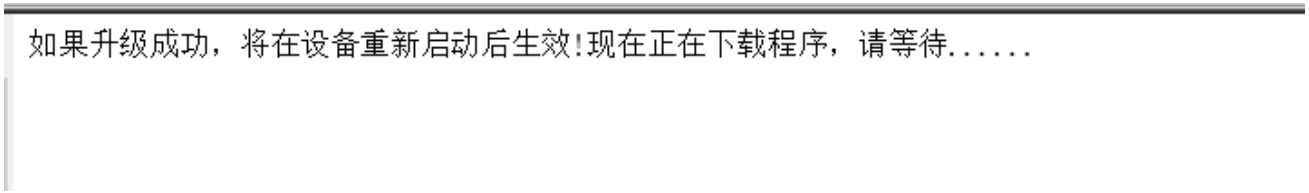


图 22 升级等待

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

警告：

- 软件升级过程中，TFTP 服务器软件应保持运行状态；
- 软件升级成功后，需要重启设备新的软件版本才能生效；

- 升级失败后不能重启交换机，避免版本文件丢失设备无法正常启动。

4.3.3 SFTP 升级

SFTP（Secure File Transfer Protocol，安全文件传输协议）是基于 SSH 的一个文件传输协议，可以进行文件的加密传输，保证传输的安全性。

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

1、添加 SFTP 用户，如图 23 所示，输入 User 和 Password，例如：User: admin, Password: 123；Port 为 SFTP 协议端口号 22；Root path 栏中输入服务器中软件版本文件的存放路径，点击<Start>按钮；

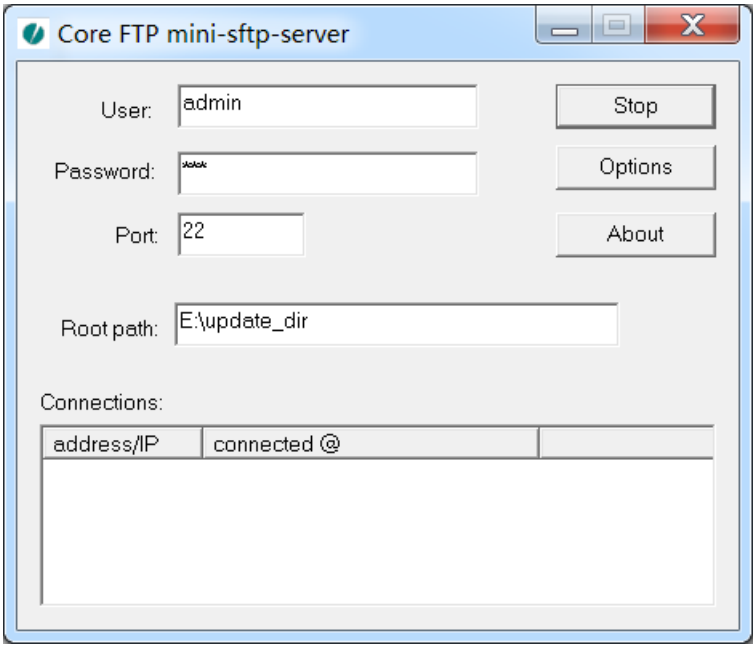


图 23 添加 SFTP 新用户

2、升级软件，如图 24 所示；

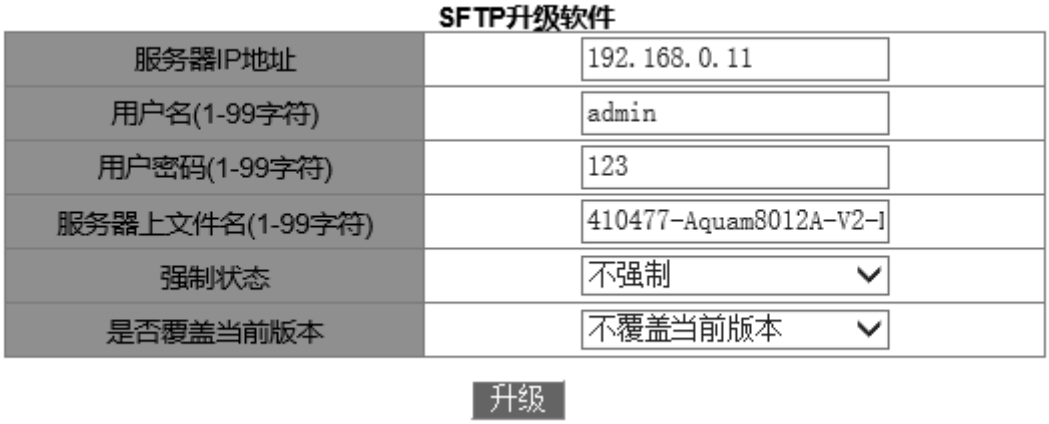


图 24 SFTP 模式下升级软件

服务器 IP 地址

配置格式：A.B.C.D

描述：输入 SFTP 服务器的 IP 地址。

{用户名，用户密码 }

配置范围：{ 1~99 个字符，1~99 个字符}

描述：SFTP 服务器创建的用户名和密码。

服务器上文件名

配置范围：1~99 个字符

描述：SFTP 服务器中版本文件名。

强制状态

配置选项：不强制/强制

默认配置：不强制

功能：选择软件版本与交换机硬件不匹配时的处理方式=-098765432ds ‘’；kjl/.,mn 描述：不强制表示软硬件不匹配时取消软件升级；强制表示软硬件不匹配时继续升级软件，这种情况可能会导致系统功能异常甚至不能启动。

是否覆盖当前版本

配置选项：覆盖当前版本/不覆盖当前版本

默认配置：覆盖当前版本

功能：是否直接覆盖当前启动使用版本。

描述：若覆盖当前版本，设备重新启动后生效，如果不覆盖当前版本，文件仅上传设备，

作为备用文件使用。

警告：

文件名必须带有后缀，否则会导致升级失败。

3、待 Web 页面中提示升级成功，如图 25 所示，激活软件版本并重启设备，在系统信息中检查软件版本是否为升级后的版本。

```
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 70.7 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 72.6 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 74.4 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 76.3 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 78.2 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 80.0 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 82.9 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 83.8 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 85.7 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 87.5 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 91.2 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 93.1 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 95.9 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 96.8 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin” 98.7 %
Write “410477-Aquam8012A-V2-L2-F0007-Build-1.3.55.B1.71.4.bin”100.0 %
Write to flash success
```

图 25 升级成功

警告：

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

4.4 软件版本选择

软件版本选择，如图 26 所示；

图 26 软件版本选择

索引

配置选项：选择/不选择

功能：选择一个软件版本。

描述：选中一个版本，点击<设为启动文件>，选择该版本使其成为下次启动时的启动版本。点击<删除>即删除该选中版本。

强制

配置选项：选择/不选择

功能：选择强制切换版本，将不进行设备校验检查，不选择强制时，将会对文件进行兼容性或合法性校验，校验不通过，设置不成功。

注意：

如果不进行合法性校验，可能会导致设备无法启动。

4.5 重新启动

当设备需要重新启动时，点击导航树[交换机维护]→[重新启动]菜单进入重新启动界面，如图 27 所示；

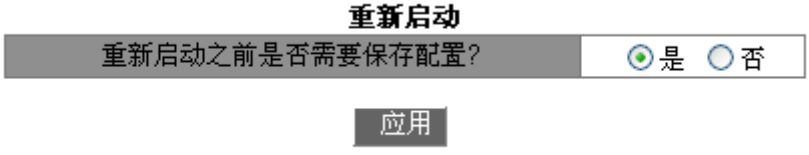


图 27 重新启动

重新启动之前需要确认是否保存当前配置，选择“是”重启后交换机配置为当前配置；选择“否”重启后交换机配置为上一次保存的配置，如果没有保存过配置，则恢复为出厂默认配置。

5 设备基本配置

5.1 基本配置

交换机的基本配置包括配置主机名称、主机与 IP 地址映射关系以及交换机时钟。

5.1.1 基本配置

1、配置主机名称

点击导航树[设备基本配置]→[基本配置]→[基本配置]菜单进入基本配置界面，如图 28 所示；

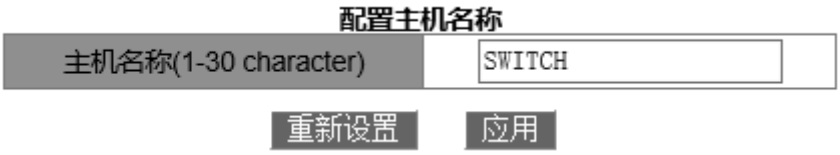


图 28 配置主机名称

主机名称

配置范围：1~30 个字符

默认配置：SWITCH

功能：配置交换机命令行界面提示符。

用法：点击<应用>按钮可以使当前配置的主机名称生效；点击<重新设置>按钮则取消当前配置，使用已经生效的主机名称配置。

2、配置主机与 IP 地址的映射关系，如图 29 所示；

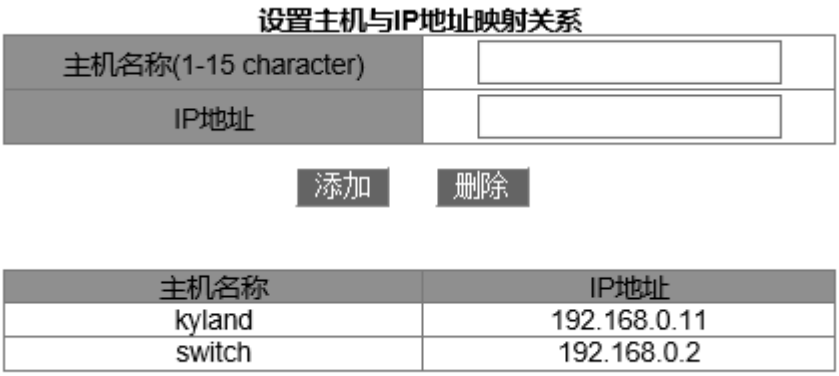


图 29 设置主机与 IP 地址映射关系

{主机名称，IP 地址 }

配置格式：{ 1~15 个字符，A.B.C.D }

功能：根据映射关系用主机名称能够访问对应的设备。

用法：输入有效的主机名称和 IP 地址，点击<添加>按钮成功配置一条主机名称和 IP 地址的映射关系表项；点击<删除>按钮即可成功删除该映射关系表项。

举例：如成功添加主机名称“Switch”与 IP 地址“192.168.0.4”映射关系表项。在交换机命令行中可用“**ping host Switch”**代替“**ping 192.168.0.4**”进行 ping 操作。

5.1.2 时钟配置

配置系统日期和时间，该系列交换机支持 RTC 实时时钟，交换机在断电后可以继续计时。

夏季为了充分利用日光，节约能源，可以采用夏时制(DST: Daylight Saving Time)时间，即将夏季作息时间人为提前一小时的经济时制。

点击导航树[设备基本配置]→[基本配置]→[时钟配置]菜单进入时钟配置界面，如图 30 所示；

图 30 时钟配置

HH:MM:SS

配置范围：HH(时)取值范围为 0~23，MM(分)和 SS(秒)取值范围为 0~59。

YYYY.MM.DD

配置范围：YYYY(年)取值范围为 1970~2099，MM(月)取值范围为 1~12，DD(日)取值范围为 1~31

说明：DD(日)的配置范围每月存在差异，如 3 月从 1 日到 31 日，4 月从 1 日到 30 日。

具体配置请按当月具体情况操作。

时区

功能：选择本地时区。

夏时制状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能夏时制时间，使能后，夏时制时间范围内，时钟将被提前一小时。

夏时制时间

使能夏时制状态后，配置执行夏时制的时间段。

注意：

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

例：从 4 月 1 日 10:00:00 开始执行夏时制时间，到 10 月 1 日 9:00:00 结束。

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

5.2 用户管理配置

为解决非法用户访问交换机造成的安全隐患，该系列交换机对用户进行分级管理，基于不同的用户身份，制定不同的权限，满足用户权限控制的多样化需求。支持 3 个级别的用户，如表 2 所示；

表 2 用户级别说明

用户级别	权限说明
来宾级用户	权限最低，仅可访问交换机中部分功能，但不能对其进行配置修改。 以下功能来宾级用户无法访问：软件升级、用户管理、文件传输服务、重启、保存配置以及恢复出厂配置。
系统级用户	有部分权限限制，可对交换机中部分功能进行访问并配置修改。

	以下功能系统级用户无法访问：软件升级、用户管理、文件传输服务、重启以及恢复出厂配置。 注：系统级用户可以修改当前用户的登录密码。
管理级用户	无权限限制，可访问交换机中所有功能并进行配置修改。

5.2.1 Web 页面配置

1、配置交换机访问用户

点击导航树[设备基本配置]→[用户管理配置]→[用户管理配置]菜单进入用户管理配置界面，如图 31 所示；

图 31 用户管理

用户名

配置范围：1~16 个字符

用户类型

配置选项：console/telnet/ssh/web

功能：选择当前用户访问交换机的方式，可以选择一个或多个访问方式。

用户等级

配置选项：来宾级/系统级/管理级

默认配置：来宾级

功能：选择当前用户的级别，不同等级的用户对交换机有不同的操作权限。

认证方式

配置选项：密码/密钥/密码或密钥

默认配置：密码

功能：选择当前用户访问交换机时的验证方式。选择密码时，需要配置后面的密码选项；选择密钥时需要配置后面的密钥选项。

密码

配置范围：1~32 个字符

功能：配置当前用户访问交换时使用的密码。

密钥

配置范围：1~16 个字符

功能：选择当前用户通过 ssh 访问交换机时使用的密钥名。

注意：

- console/telnet/web 目前暂不支持密钥验证方式，所以服务类型为 console/telnet/web 时，认证类型请勿选择密钥；
- ssh 支持密码和密钥两种验证方式；
- 最多可配置 9 个用户；
- 不能删除默认用户 admin。该用户的默认用户类型（console, telnet, ssh, web）和用户等级（管理级）无法修改；默认密码（123）可以修改。
- console/telnet/web 访问交换机方式请参考“2 交换机的访问方式”章节；
- ssh 访问交换机方式请参考“5.11 SSH 服务器配置”章节。

2、修改、删除用户信息

点击图 31 用户管理列表中的用户名，进入图 32 所示界面，点击<应用>按钮可以修改当前用户信息，点击<删除>按钮可以删除该用户。

图 32 用户信息修改、删除界面

3、配置 SSH 密钥

点击导航树[设备基本配置]→[用户管理配置]→[SSH 密钥配置]菜单进入 SSH 密钥配置界面，如如图 33 所示；

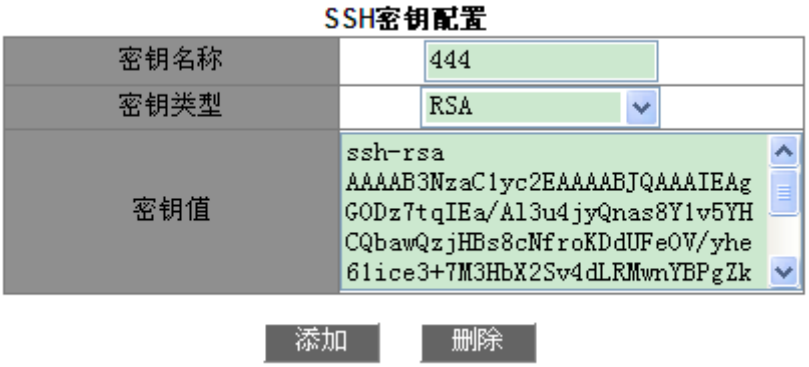


图 33 SSH 密钥配置

密钥名称

配置范围：1~16 字符

密钥类型

强制配置：RSA

该系列产品只支持 RSA 密钥算法。

密钥值

配置格式：{ 算法名，公共密钥，密钥信息 }

算法名：ssh-rsa | ssh-dsa

公共密钥：基于 64 位码，长度小于 2048 字节

密钥信息：密钥的更多信息

功能：配置客户端的公有密钥，通常是由 Puttygen 软件生成并拷贝到服务器的密钥值中，私有密钥保存在客户端。

4、修改当前登录用户的密码

点击导航树[设备基本配置]→[用户管理配置]→[修改密码]菜单进入密码修改界面，如图 34 所示。

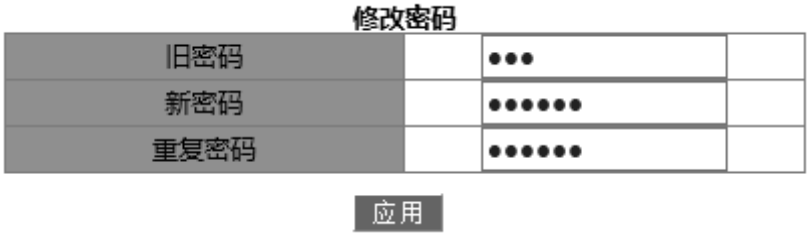


图 34 修改密码

新密码/重复密码

配置范围：1~32 个字符

5、配置登录方式的超时时间

点击导航树[设备基本配置]→[用户管理配置]→[超时设置]菜单进入超时时间配置界面，如图 35 所示。

图 35 配置登录超时时间

超时时间

配置范围：0~44640 min

默认配置：console/ssh/telnet 登录超时时间为 5 min；web 登录超时时间为 10min

功能：配置登录用户超时断开连接的时间。用户完成最后一项操作开始计时，到达配置时间值时，便退出该登录方式。配置超时时间为 0 即关闭超时断开连接功能，说明登录用户不会被服务器判断超时而退出该登录方式。

6、WEB 服务器安全 IP

点击导航树[设备基本配置]→[用户管理配置]→[WEB 服务器安全 IP]菜单进入 WEB 服务器安全 IP 界面，如图 36 所示。

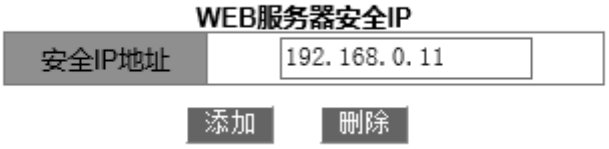


图 36 WEB 服务器 IP

安全 IP 地址

配置格式：A.B.C.D

功能：配置 交换机作为 WEB 服务器时允许登录的 WEB 客户端的 IP 地址。

描述：没有配置安全 IP 地址时，登录交换机的 WEB 客户端 IP 地址 不受限制；配置安全 IP 地址后，只有安全 IP 地址的客户端才能通过 WEB 登录到交换机进行配置 。

交换机最多可以配置 10 个安全 IP 地址，默认情况下没有配置任何安全 IP。

配置完成后，“服务器安全 IP 列表”中显示可以登录到交换机的用户管理 IP 地址。如图 37 所示；

服务器安全IP列表
192.168.0.11
192.168.0.184

图 37 安全 IP 地址列表

5.3 端口配置

5.3.1 物理端口配置

5.3.1.1 介绍

物理端口配置可以控制端口连线类型、管理状态、速率/模式等信息。

5.3.1.2 Web 页面配置

点击导航树[设备基本配置]→[端口配置]→[以太网端口配置] →[物理端口配置]菜单进入物理端口信息配置界面，如图 38 所示；

端口配置

端口	端口别名	类型	连线类型	状态	管理状态	速率/模式	流控	链路up延迟(单位1/60秒)
1/1		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/2		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/3		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/4		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/5		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/6		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/7		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/8		FE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/9		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/10		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/11		GE	auto	up	no shutdown	auto	Invalid	0 (0-600)
1/12		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)

应用

图 38 物理端口配置

端口

配置选项：交换机上所有端口

描述：采用 X/Y 格式表示端口，其中 X 指端口所在板卡的插槽号，Y 指端口在板卡面板上的标号。

端口别名

配置范围：1~64 个字符

功能：配置端口别名对该端口进行描述。

连线类型

配置选项：auto/normal/across

默认配置：auto

功能：配置以太网端口支持的连线类型。

描述：auto 表示自动识别连线类型；across 表示端口只识别交叉线；normal 表示端口只识别直连线。

注意：

建议用户采用自动识别连线类型。

管理状态

配置选项：shutdown/no shutdown

默认配置：no shutdown

功能：是否允许端口传输数据。

描述：no shutdown 表示打开端口允许数据传输； shutdown 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。

速率/模式

配置选项：auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half, 1000M/Full

默认配置：auto

功能：配置端口速率和双工模式。

描述：端口速率和双工模式可自动协商也可强制配置。配置为 auto 模式时端口速率和双工模式会根据端口连接状态自动协商；当端口双工模式从自动协商变为强制全双工/半双工时，端口速率也会变为强制模式。建议用户将每个端口的速率和双工模式配置为自动协商，这样可以尽可能避免由于端口配置不匹配带来的连接问题。如果用户将端口配置为强制速率/双工模式，请确认连接双方速率/双工模式配置一致。

注意：

- 百兆电口的速率/模式可以配置为 auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full；
- 百兆光口的速率/模式可以配置为 100M/Full；
- 千兆电口的速率/模式可以配置为 auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half, 1000M/Full；
- 千兆光口的速率/模式只能配置为 auto, 1000M/Full。

流控

配置选项：无效/有效

默认配置：无效

功能：是否打开端口的流控功能。

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

链路 up 延迟

配置范围：0~600 （单位：1/60 秒）

默认配置：0 （0 秒）

功能：配置端口 link up 延迟时间，连接的双方端口 up 延迟配置应保持一致。

5.3.2 端口信息查看

点击导航树[设备基本配置]→[端口配置]→[端口检测和调试信息] →[端口信息查看]菜单进入端口信息查看界面，可以查看指定端口的连接状态，端口类型，报文接收与转发统计等信息，如图 39 所示；

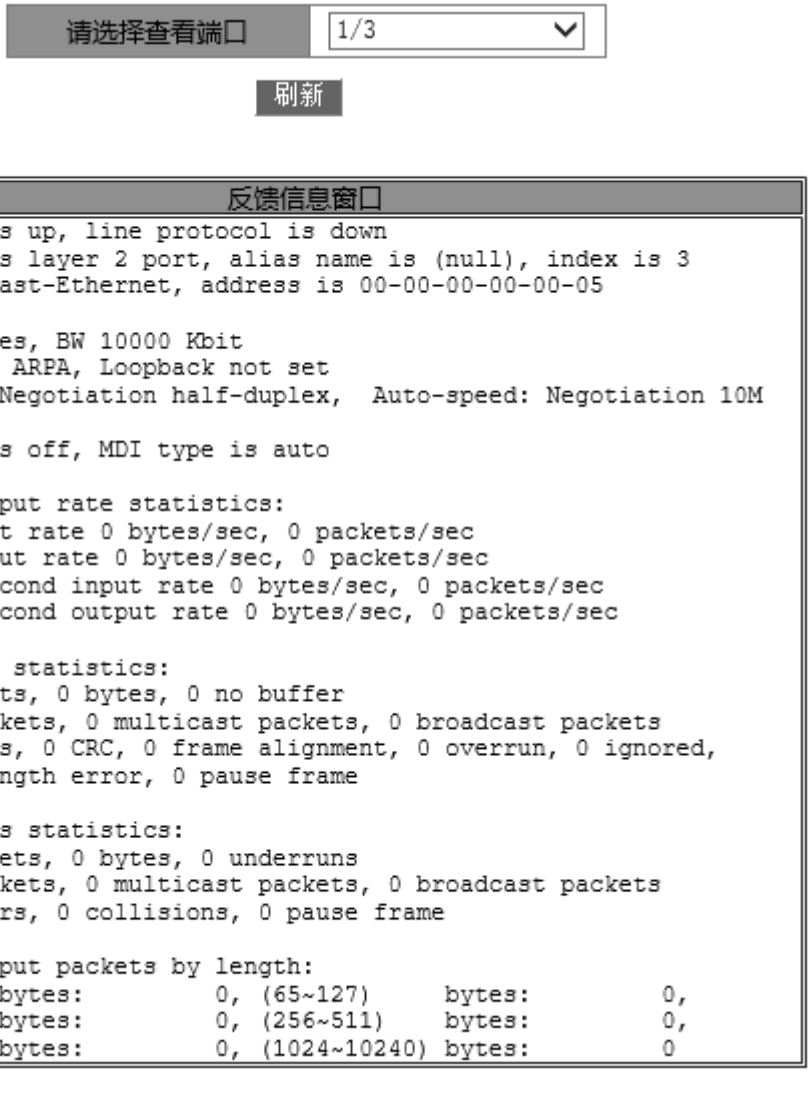


图 39 端口信息

5.4 VLAN 配置

5.4.1 介绍

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

VLAN 的划分不受物理位置的限制，每个 VLAN 被认为是一个逻辑网络，不同 VLAN 中的主机传输数据包需通过路由器或三层设备。

5.4.2 原理

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

表 3 802.1Q 帧结构

DA	SA	802.1Q 头信息				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。

5.4.3 基于端口的 VLAN 介绍

VLAN 划分可以有多种方式，例如：基于端口、基于 MAC 地址等。该系列交换机支持基于端口的 VLAN 划分，根据交换机端口来定义 VLAN 成员，将指定端口加入指定 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、端口模式

Access：该模式端口只能以Untag类型添加到一个VLAN中，不能以Tag类型添加到任何VLAN中。

Trunk：该模式端口以Untag类型添加到PVID VLAN中；以Untag/Tag类型添加到其他任何VLAN中。

3、PVID

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

Access端口的PVID是该端口所在的VLAN ID，不能配置；

Trunk端口的PVID可以配置为该端口允许通过的VLAN ID。

根据端口模式、端口类型和PVID，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

<table>
<tr><th colspan="2">对接收报文的处理</th><th colspan="2">对转发报文的处理</th></tr>
<tr><th>接收到的报文为 Untag</th><th>接收到的报文为 Tag</th><th>端口类型</th><th>报文处理</th></tr>
<tr><td rowspan="2">为报文添加 PVID 的 Tag 标记</td><td rowspan="2">➢ 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</td><td>Untag 端口</td><td>去掉 Tag 标记后转发该报文</td></tr>
<tr><td>Tag 端口</td><td>保持报文中原有的 Tag 标记，转发该报文</td></tr>
</table>

	允许通过的 VLAN 列表中时，丢弃该报文		

5.4.4 Web 页面配置

1、创建或删除 VLAN

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[创建或删除 VLAN] →[VLAN ID 分配管理]菜单进入 VLAN 管理界面，如图 40 所示；

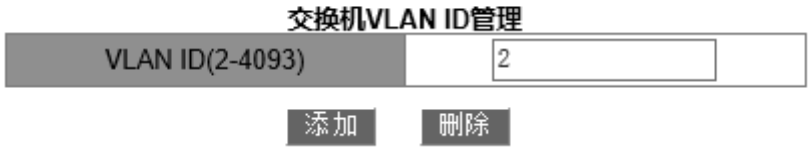


图 40 创建/删除 VLAN

VLAN ID

配置范围：2~4093

功能：VLAN 号用来区分不同的 VLAN。

描述：该系列交换机最多可以同时支持 4093 个 VLAN。

用法：点击<添加>按钮创建该 VLAN；点击<删除>按钮即可删除已创建的指定 VLAN。

2、配置 VLAN 名称

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[创建或删除 VLAN] →[VLAN ID 属性配置]菜单进入 VLAN 名称配置界面，如图 41 所示；

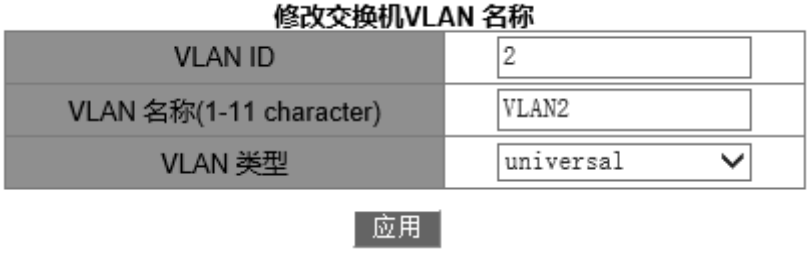


图 41 配置 VLAN 名称

VLAN ID

配置范围：已创建的 VLAN ID

功能：输入需要修改 VLAN 名称的 VLAN ID。

VLAN 名称

配置范围：1~11 个字符

功能：输入指定 VLAN ID 的 VLAN 名称。

VLAN 类型

配置选项：universal

默认配置：universal

配置完成后“交换机 VLAN ID 信息”栏中显示所有已创建 VLAN 的属性信息，如图 42 所示；

交换机VLAN ID 信息

VLAN ID	VLAN 名称	VLAN 类型
1	default	universal
2	VLAN2	universal
100	VLAN100	universal
200	VLAN200	universal

图 42 查看 VLAN 列表

3、给已创建的 VLAN 分配端口

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[为 VLAN 分配以太网端口]→[给 VLAN 分配以太网端口]菜单 VLAN 端口配置界面，如图 43 所示；

图 43 为 VLAN 分配端口

标签类型

配置选项：Tag/Untag

功能：选择端口以什么类型添加到 VLAN 中。

注意：

- Access 端口只能以 Untag 类型添加到一个 VLAN 中；
- Trunk 端口以 Untag 类型添加到 PVID VLAN 中；以 Untag/Tag 类型添加到其他任何 VLAN 中。

4、配置交换机端口模式

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[设置交换机端口类型] →[端口类型 Trunk/Access 分配]菜单进入端口类型配置界面，如图 44 所示；

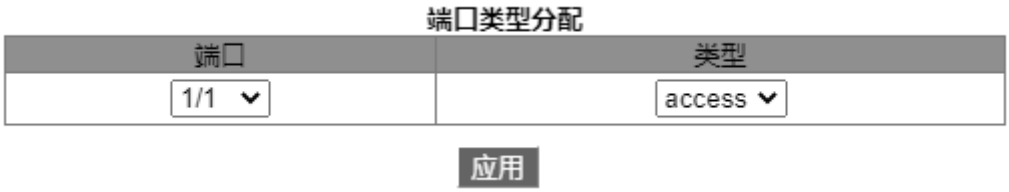


图 44 端口类型配置

端口

配置选项：交换机上所有端口

类型

配置选项：access/trunk

默认配置：access

功能：选择端口模式，每个端口只能选择一种模式。

配置完成后“端口类型分配”列表中显示所有端口类型，如图 45 所示；

端口类型分配

端口	类型
1/1	access
1/2	access
1/3	access
1/4	access
1/5	access
1/6	access
1/7	access
1/8	access
1/9	access
1/10	access
1/11	access
1/12	trunk

图 45 查看端口类型列表

5、配置 Trunk 端口的 PVID

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[设置 Trunk 端口]→[Trunk 端口 VLAN 配置]菜单进入 Trunk 端口 VLAN 配置界面，如图 46 所示；

图 46 配置 Trunk 端口 PVID

Trunk 端口

配置选项：所有的 Trunk 端口

trunk native vlan(pvid)

配置选项：已创建的 VLAN

默认配置：1

功能：配置 Trunk 端口的 PVID。

描述：无论端口是否存在于该 VLAN 中，或以 Untag/Tag 类型存在于该 VLAN 中，指定 PVID 后，该端口都会以 Untag 类型添加到该 VLAN 中。

用法：点击<恢复默认值>按钮则恢复当前 Trunk 端口的 PVID 为 1。

6、配置 Trunk 端口允许通过的 VLAN 列表，如图 47 所示；

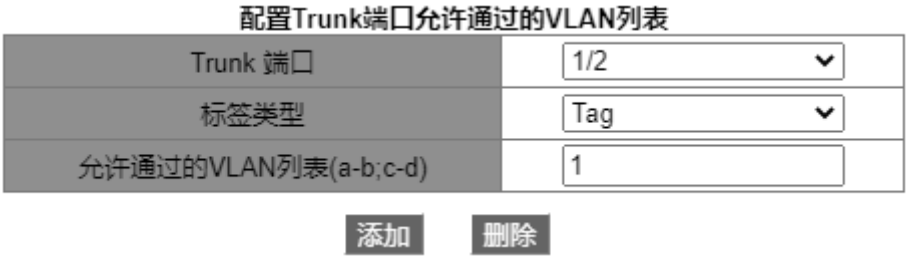


图 47 配置 Trunk 端口允许通过的 VLAN 列表

Trunk 端口

配置选项：所有的 Trunk 端口

标签类型

配置选项：Tag/Untag

功能：选择该 Trunk 端口以什么类型添加到 VLAN 中。

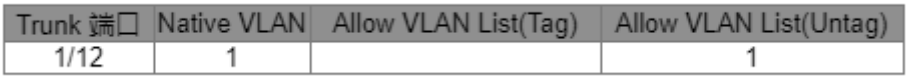
允许通过的 VLAN 列表

配置选项：已创建的 VLAN

默认配置：已创建的全部 VLAN

功能：配置选定 Trunk 端口允许通过的 VLAN 列表。

配置完成后下方列表中显示所有 Trunk 端口的 VLAN 属性信息，如图 48 所示；



Trunk 端口	Native VLAN	Allow VLAN List(Tag)	Allow VLAN List(Untag)
1/12	1		1

图 48 查看 Trunk 端口 VLAN 配置

7、配置端口 VLAN 入口规则

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[使能或禁止 VLAN 的入口规则]→[使能或禁止 VLAN 的入口规则]菜单进入端口的 VLAN 入口规则配置界面，如图 49 所示；

图 49 配置端口 VLAN 入口规则

配置选项：使能/禁止

默认配置：使能

功能：使能/禁止端口的 VLAN 入口规则。

描述：端口 VLAN 入口规则使能时，端口在接收数据时检查 Tag 报文中 VLAN ID 是否属于端口所允许通过的 VLAN 列表，如果存在于列表中端口接收报文数据并转发，否则丢弃该报文。端口 VLAN 入口规则禁止时，端口不检查报文中 Tag 标签与端口允许通过的 VLAN 列表的一致性，接收所有报文并进行转发。

配置完成后下方会显示所有端口的 VLAN 入口规则列表，如图 50 所示；

端口	类型	入口规则
1/1	FE	使能
1/2	FE	使能
1/3	FE	使能
1/4	FE	使能
1/5	FE	使能
1/6	FE	使能
1/7	FE	使能
1/8	FE	使能
1/9	GE	使能
1/10	GE	使能
1/11	GE	使能
1/12	GE	使能

图 50 端口 VLAN 入口规则列表

8、配置 VLAN-aware

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 配置]→[VLAN-aware]→[VLAN-aware]菜单进入 VLAN-aware 配置界面，如图 51 所示；

图 51 配置 VLAN-aware

配置选项：Aware/Unaware

默认配置：Aware

功能：选择 Aware 时，设备按照 IEEE802.1Q 协议识别判断 VLAN，并正常转发报文。选择 Unaware 时，对于未知单播，设备不判断报文的 VLAN ID，将报文转发至任意端口（广

播）；对于已知单播，设备不判断报文的 VLAN ID，按照 MAC 地址表转发至相应端口。

9、显示已创建的 VLAN 信息

点击导航树[设备基本配置]→[VLAN 配置]→[VLAN 检测和调试信息]→[显示 VLAN 信息]菜单进入 VLAN 信息显示界面，如图 52 所示；

VLAN ID	名称	类型	介质	端口
1	default	Static	ENET	1/2(TR) 1/7 1/8 1/9 1/10 1/11 1/12(TR)
2	VLAN0002	Static	ENET	1/1 1/2 1/12(TR|TG)
100	VLAN0100	Static	ENET	1/3 1/4 1/12(TR|TG)
200	VLAN0200	Static	ENET	1/5 1/6 1/12(TR|TG)

图 52 显示 VLAN 信息

5.4.5 典型配置举例

如图 53所示，将整个局域网划分为3个VLAN：VLAN2、VLAN100和VLAN200，要求同一VLAN中的设备可以相互通信，不同VLAN之间相互隔离。终端PC设备不识别带tag标记的报文，所以将Switch A、B和PC相连的端口配置为Access端口。Switch A和Switch B之间需要传输VLAN 2 、VLAN 100和VLAN200的报文，所以将Switch A、 B相连的端口配置为Trunk端口，并允许 VLAN 2、VLAN 100和VLAN200通过。具体配置如表 5所示。

表 5 VLAN 配置

配置项目	**配置说明**
VLAN2	A 地、B 地交换机 1/1、1/2 端口(Untag 类型)；端口 1/12(Tag 类型，PVID=1)
VLAN100	A 地、B 地交换机 1/3、1/4 端口(Untag 类型)；端口 1/12(Tag 类型，PVID=1)
VLAN200	A 地、B 地交换机 1/5、1/6 端口(Untag 类型)；端口 1/12(Tag 类型，PVID=1)

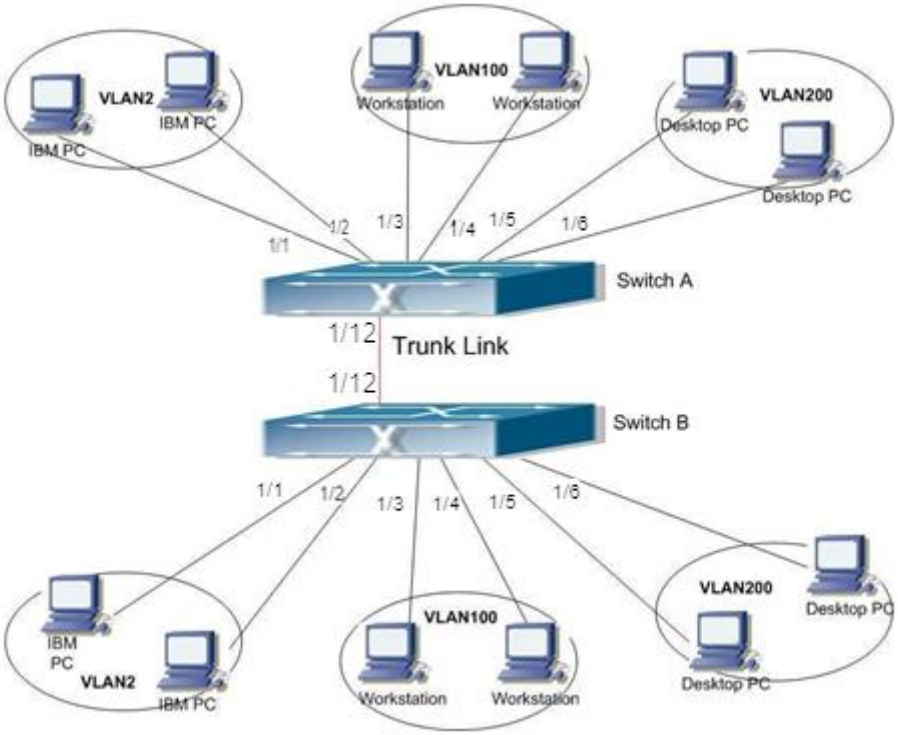


图 53 VLAN 应用

SwitchA、B配置过程：

1、创建VLAN2、VLAN 100、VLAN 200，如图 40所示；

2、配置端口1/1、1/2、1/3、1/4、1/5、1/6为Access类型，端口1/12为Trunk类型，如图 45所示；

3、配置端口1/1、1/2以Untag类型添加到VLAN2，端口1/3、1/4以Untag类型添加到VLAN100，端口1/5、1/6以Untag类型添加到VLAN200。端口1/12以Tag类型添加到VLAN2、VLAN100、VLAN200，如图 43所示；

5.5 QinQ 配置

5.5.1 介绍

QinQ 技术是一项扩展 VLAN 空间的技术，通过在 802.1Q 标签报文的基础上再增加一层 802.1Q 的标签头来达到扩展 VLAN 空间的功能，可以使私网 VLAN 透传公网。

在基于传统的 802.1Q 协议的局域网互联模式中，当两个用户网络需要通过 ISP 互相访问时，ISP 必须为每个接入用户的不同 VLAN 分配不同的 VLAN ID，如图 54 所示。假设用户的网络 1 和网络 2 位于两个不同地点，并分别通过 ISP 的 PE1、PE2 接入骨干网。

如果用户需要将网络 1 的 VLAN100～VLAN200 和网络 2 的 VLAN100～VLAN200 互联起来，那么必须将 CE1、PE1、P 和 PE2、CE2 的相连接口都配置为 Trunk 属性，并允许 VLAN100～VLAN200 通过。

这种配置方法使得用户的 VLAN 在骨干网络上可见，而非透明传输。这不仅耗费服务提供商的 VLAN ID 资源（一般只有 4094 个 VLAN ID），而且还需要服务提供商管理用户的 VLAN 编号。这种情况下，网络结构过于紧密，ISP 或客户网络规划的变化将会影响整个网络，导致网络灵活性差。

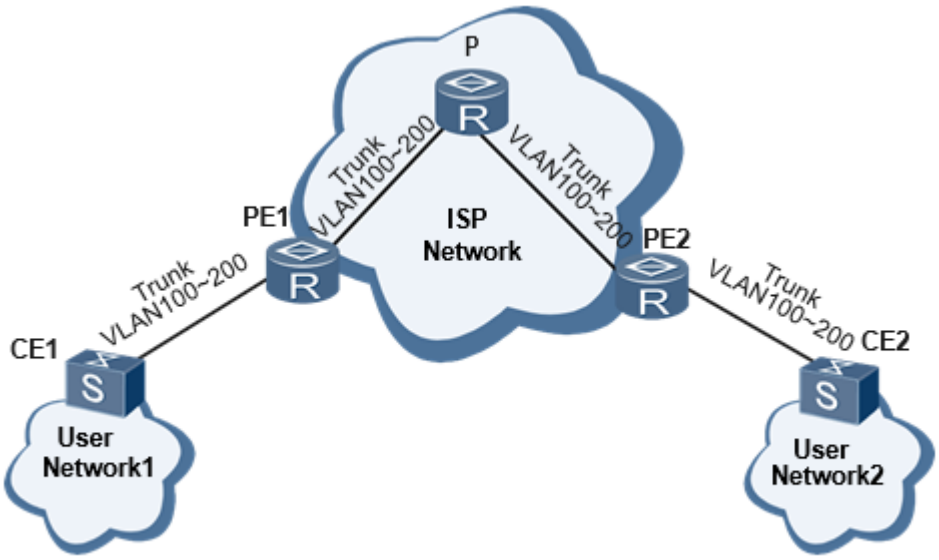


图 54 传统的基于 802.1Q 协议的二层局域网互联模式

QinQ 技术在 802.1Q Tag 报文的基础上又增加了一层 802.1Q Tag。这样，在骨干网中传递的报文就有两层 802.1Q Tag（一层公网 Tag，一层私网 Tag），ISP 网络只需为来自同一用户网络的不同 VLAN 提供一个 VLAN ID，节约了 ISP 的 VLAN ID，解决了 ISP 网络 VLAN ID 资源紧张的问题。同时可以使私网 VLAN 透传公网，也为小型城域网或者局域网提供一种较为简单的二层 VPN 解决方案。

5.5.2 设备支持的 QinQ 特性

QinQ 因为其自身简单灵活的特点，在各解决方案中扮演着重要的角色。

基础 QinQ：基本 QinQ 又称为 QinQ 二层隧道，是基于接口方式实现的。开启接口的基本 QinQ 功能后，当该接口接收到报文，设备会为该报文打上本接口缺省 VLAN 的 VLAN Tag。如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是不带 VLAN Tag 的报文，该报文就成为带有接口缺省 VLAN Tag 的报文。

5.5.3 QinQ 外层 VLAN tag 的 TPID 值可配置

如

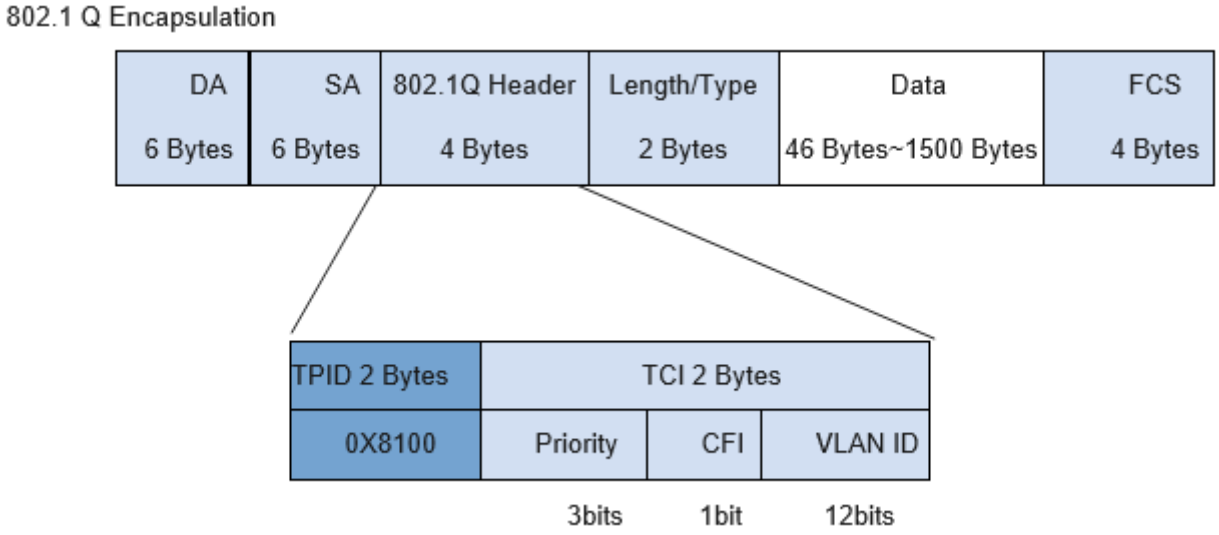


图 55 所示，是 IEEE802.1Q 协议定义的以太网帧的 VLAN Tag 结构。标签协议标识 TPID（Tag Protocol Identifier）是 VLAN Tag 中的一个字段，用于表示 VLAN Tag 的协议类型，IEEE 802.1Q 协议规定该字段的取值为 0x8100。

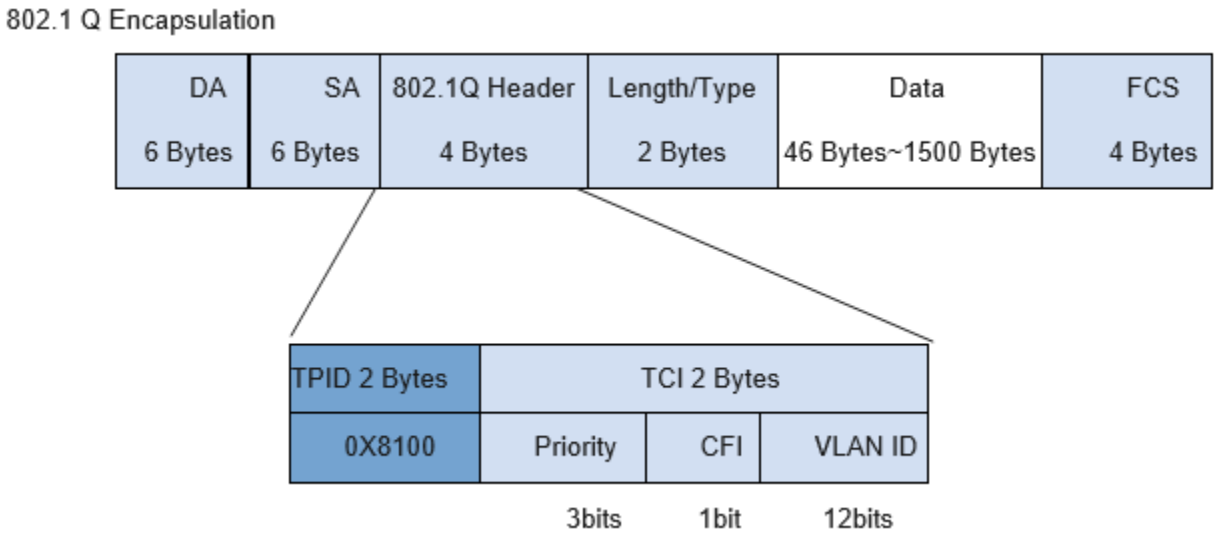


图 55 802.1Q 封装

不同厂商的设备可能将 QinQ 报文外层 VLAN Tag 的 TPID 字段设为不同的值，为了和其他厂商的设备兼容，设备提供了 QinQ 报文外层 VLAN Tag 的 TPID 值可修改功能。用户通过配置 TPID 的值，使得发送到公网中的 QinQ 报文携带的 TPID 值与其他厂商相同，就可以实现与其他厂商的设备互通。

以太网帧的 TPID 与不带 VLAN 标记的帧的协议类型字段位置相同。为避免在网络中转发和处理数据包时出现问题，不可将 TPID 值设置为下表中的任意值：

表 6 协议类型及对应值描述表

协议类型	对应值
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7
设备保留	0xFFFD/0xFFFE/0xFFFF

5.5.4 Web 页面配置

点击导航树[设备基本配置]→[QinQ]→[QinQ 配置]菜单进入 QinQ 配置界面，如图 40 所示；

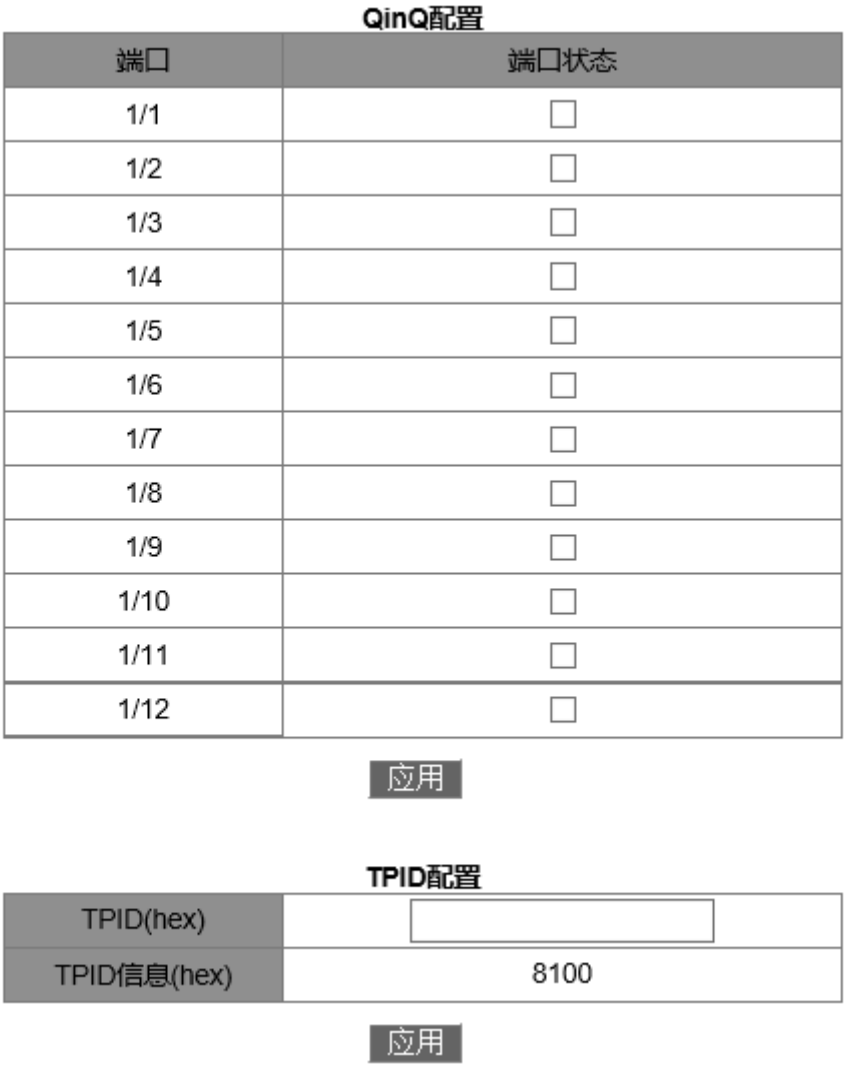


图 56 QinQ 配置

端口

配置范围：交换机上所有端口

端口状态

配置选项：选择/不选择

功能：选择是否应用QinQ 端口。

TPID(hex)

配置范围：5dd-ffff

功能：配置 **TPID(hex)**

描述：当该接口接收到报文，设备会为该报文打上本接口缺省 VLAN 的 VLAN Tag。

5.6 端口镜像

5.6.1 介绍

端口镜像指交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制端口称为镜像源端口，复制端口称为镜像目的端口。可以在镜像目的端口处连接一个协议分析仪或者 RMON 监测仪来监视和管理网络，并诊断网络故障。

5.6.2 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：

镜像目的端口与端口聚合互斥，镜像目的端口不能加入聚合组；加入聚合组的端口也不能配置为镜像目的端口。

5.6.3 Web 页面配置

1、选择镜像源端口以及镜像模式

点击导航树[设备基本配置]→[端口镜像配置]→[镜像配置]菜单进入镜像源端口配置界面，如图 57 所示；

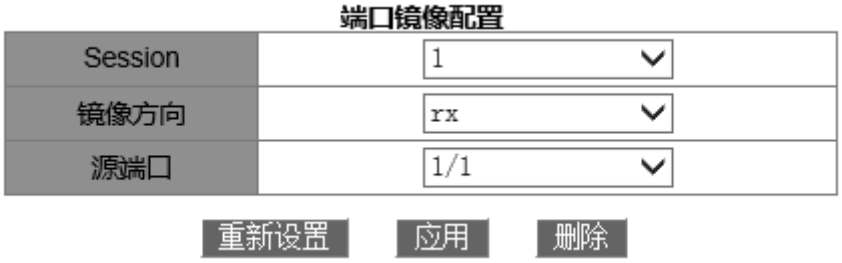


图 57 镜像源端口配置

Session

配置选项：1~7

默认配置：1

功能：选择一个镜像组。

镜像方向

配置选项：rx/tx/both

默认配置：both

功能：选择源端口被镜像的方向。

描述：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；both 对源端口接收和发送的报文进行镜像；

源端口

配置选项：交换机上所有端口

功能：选择镜像源端口，可以配置多个镜像源端口。

2、选择镜像目的端口，如图 58 所示；

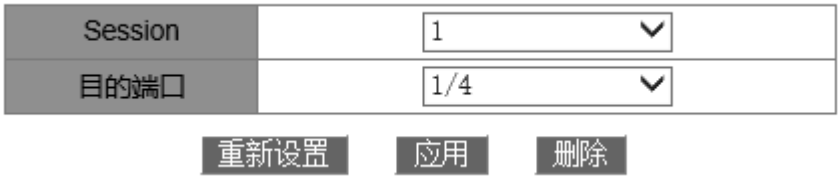


图 58 选择镜像目的端口

Session

配置选项：1~7

默认配置：1

功能：选择一个镜像组。

目的端口

配置选项：源端口之外的其他端口

功能：选择镜像目的端口。

描述：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。镜像目的端口不能是端口聚合组成员，并且端口吞吐量最好大于或等于它所镜像的所有源端口的吞吐量的总和。

5.6.4 典型配置举例

如图 59 所示，镜像目的端口为 2，镜像源端口为 1，1 端口接收和发送的报文都镜像到 2 端口。

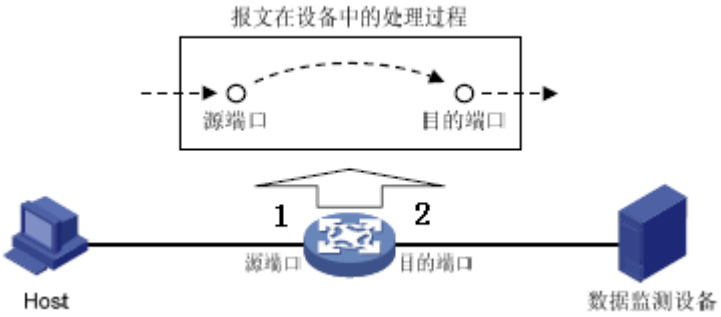


图 59 端口镜像举例

配置过程：

1、选择 2 端口作为镜像目的端口，见图 58；

2、选择 1 端口作为镜像源端口，端口镜像模式选择 both，见图 57。

5.7 端口风暴抑制

5.7.1 介绍

端口风暴抑制指对端口接收到的广播/组播/未知单播报文数据量进行限制，当端口接收的广播/组播/未知单播流量超过用户配置的限定阈值时，系统将丢弃超出流量限制的广播/组播/未知单播报文，从而使端口接收的广播/组播/未知单播报文流量所占的比例降低到限定的范围，保证网络业务的正常运行。

5.7.2 Web 页面配置

1、端口风暴抑制配置

点击导航树[设备基本配置]→[端口风暴抑制配置]→[端口风暴抑制配置]菜单进入端口风暴抑制配置界面，如图 60 所示；

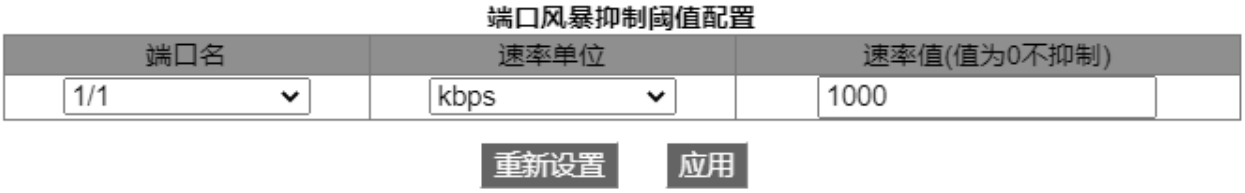


图 60 端口风暴抑制阈值配置

端口号

配置选项：交换机上所有端口

功能：选择需要限制流量的端口。

速率单位

配置选项：bps/kbps/ percent

功能：选择配置限定阈值的单位类型。

速率值

配置范围：1~1000000kbps/1~1000000000bps/1~100 Percent

默认配置：0，值为 0 表示风暴抑制不使能。

功能：配置端口限速阈值，超过阈值的报文数据将被丢失。取值范围视端口实际速率而定见表 7 所示；

描述：百兆口的限速阈值配置范围为 1~100000kbps/1~100000000bps；千兆口的限速阈值配置范围为 1~1000000kbps/1~1000000000bps。百分比值针对端口带宽，例如：100M 端口的限速值为 60%，则端口接收 60M 的数据流量，之后接收的数据将被丢弃。

表 7 端口限速取值范围

端口速率	阈值单位	步长	取值范围
10M	bps	512	512~10000000
	kbps	不建议使用	不建议使用
100M	bps	5120	5120~100000000

	kbps	5	5~100000
1000M	bps	51200	51200~1000000000
	kbps	50	50~1000000

2、选择端口抑制的报文类型，如图 61 所示；

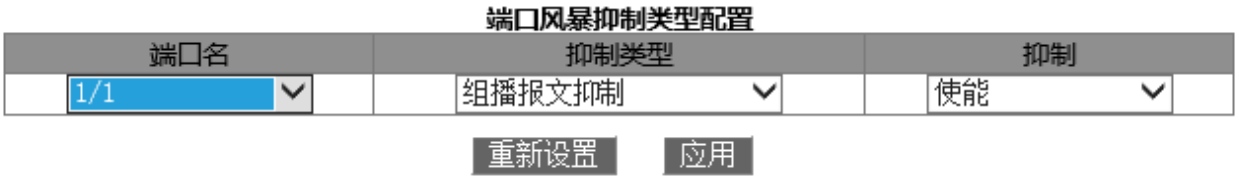


图 61 端口限速报文类型配置

端口名

配置选项：使能端口风暴抑制功能的端口

抑制类型

配置选项：组播报文抑制/广播报文抑制/未知单播报文抑制

功能：选择端口抑制的报文类型。

抑制

配置选项：使能/禁止

默认配置：禁止

功能：是否对所选报文进行抑制。

说明：

一个端口只能配置一个限速阈值，该阈值对使能的报文类型进行限速。

5.7.3 典型配置举例

使能端口 1/1 的未知组播风暴抑制，带宽阈值配置为 1000kbps。

配置过程：

1、选择端口 1/1；限速单位：kbps；速率值：1000kbps，见图 60 所示；

2、选择抑制类型：组播报文抑制，如图 61 所示；

5.8 端口隔离

5.8.1 介绍

为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，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：

- 加入到隔离组中的端口只能是同一台交换机的端口；
- 一台设备可支持 14 个隔离组，组内的以太网端口数量没有限制；
- 配置隔离组后，一个隔离组内各个端口之间的报文不能互通，不同隔离组内端口、隔离组内与隔离组外端口之间的通信正常；
- 隔离端口和聚合端口互斥，加入隔离组的端口不能加入聚合组；加入聚合组的端口也不能加入隔离组。

5.8.2 Web 页面配置

点击导航树[设备基本配置]→[端口隔离配置]→[端口隔离配置]菜单进入端口隔离配置界面，使能端口隔离功能，如图 62 所示；

全选	隔离组ID	1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	1/12
	1	1/8											
	2	1/1,1/2											
	3	1/4,1/5											

应用 编辑 删除

图 62 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。

注意：

一个端口只能加入一个隔离组。

5.8.3 典型配置举例

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，端口1、2、3、4均在VLAN 1中。PC1、PC2 和PC3 之间两两不能互通，但都可访问外部网络，如图 63所示；

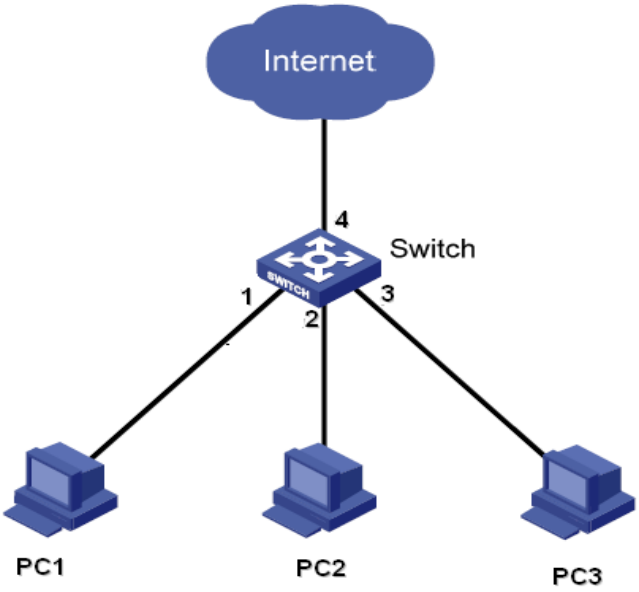


图 63 端口隔离配置举例

将端口 1，2，3 加入隔离组，如图 62 所示，即可实现 PC1、PC2 和 PC3 之间隔离。

5.9 Port channel

5.9.1 介绍

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

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

5.9.2 实现

如图 64 所示 SwitchA 的 3 个端口汇聚成一个 Port Channel，该 Port Channel 的带宽为 3 个端口带宽总和。

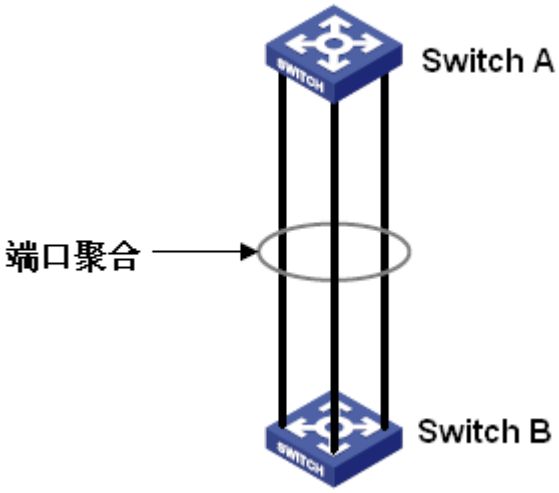


图 64 端口聚合示意图

SwitchA 如果有流量要经过 Port Channel 传输到 SwitchB，SwitchA 的 Port Channel 将根据流量分担方式进行流量分配运算，根据运算结果决定由 Port Channel 中的某一成员端口承担该流量。当 Port Channel 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。

5.9.3 说明

该系列交换机最多支持 8 个聚合组，每个聚合组最多支持 8 个成员端口。

注意：

- 一个端口只能加入一个聚合组。
- 聚合端口和隔离端口互斥，加入聚合组的端口不能加入隔离组；加入隔离组的端口也不能加入聚合组。
- 聚合端口与镜像目的端口互斥，加入聚合组的端口不能配置为镜像目的端口；镜像目的端口也不能加入聚合组。

5.9.4 Web 页面配置

1、配置聚合组的流量分担方式

点击导航树[设备基本配置]→[Port Channel 配置]→[链路聚合配置]菜单进入配置界面，如图 65 所示；

图 65 流量分担模式配置

流量分担方式

配置选项：mac-only/ip-only/mac-ip/ip-l4/mac-ip-l4

默认配置：mac-only

功能：配置聚合组的流量分担方式。

描述：mac-only 根据 MAC 地址进行流量分担；ip-only 根据 IP 地址进行流量分担；mac-ip 根据 MAC 地址和 IP 地址进行流量分担；ip-l4 根据 IP 地址和 TCP/UDP 端口号进行流量分担；mac-ip-l4 根据 MAC 地址、IP 地址和 TCP/UDP 端口号进行流量分担。

2、创建或删除一个 port group，如图 66 所示；

图 66 聚合组配置

链路聚合组号

配置范围：1~8

功能：配置 Port Group 组号，最多支持 8 个聚合组。

操作类型

配置选项：add port group/remove port group

默认配置：add port group

功能：创建/删除 port group 操作。

配置完成后，“组号列表”中显示所创建的 port group 组号及流量分担方式，如图 67 所示；

组号列表

组号	流量分担
3	mac-only
2	mac-only
1	mac-only

图 67 聚合组列表

3、聚合组成员配置

点击导航树[设备基本配置]→[Port Channel 配置]→[链路聚合端口配置]菜单进入聚合组成员配置界面，如图 68 所示；

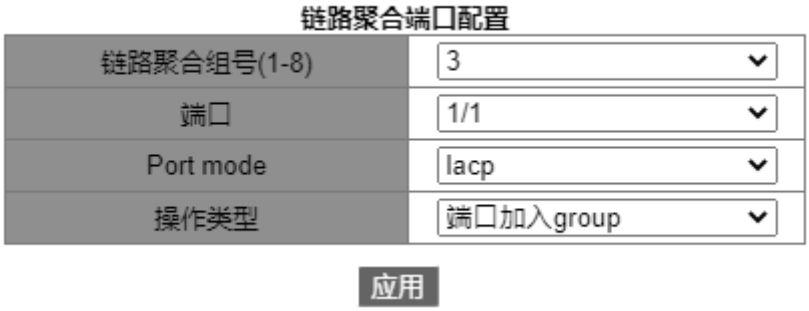


图 68 聚合组成员配置

链路聚合组号

配置选项：已创建的 Port Group 组号

端口

配置选项：交换机上所有端口

功能：选择要加入或离开指定聚合组的端口。

描述：同一聚合组的成员端口具有相同的端口属性，一个组中最多可以添加 8 个端口。

操作类型

配置选项：端口加入 group/端口退出 group

默认配置：端口加入 group

功能：选择指定端口加入/退出 Port Group。

5.9.5 典型配置举例

如图 64 所示，SwitchA 的 3 个端口(端口 1、2、3)加入 Port Group 1； SwitchB 的 3 个端口(端口 1、2、3)加入 Port Group 2；将上述对应端口分别用网线相连形成一个 Port Channel，从而实现流量在各端口间的分担(假设交换机的 3 个聚合端口有相同的属性)。

交换机配置过程：

1、SwitchA 中添加 Port Group 1，见图 66；

2、选择端口 1、2、3 加入 Port Group 1，见图 67；

3、SwitchB 中添加 Port Group 2，见图 66；

4、选择端口 1、2、3 加入 Port Group 2，见图 67。

5.10 Telnet 服务器配置

5.10.1 介绍

Telnet 远程登录是简单的远程终端协议，用户通过 Telnet 可在其所在地登录到远程的另一台主机上(使用 IP 地址或者主机名)。Telnet 能把用户的击键传到远程主机，也能把远程主机的输出信息通过 TCP 连接返回到用户屏幕。

Telnet 使用客户端-服务器模式，本地系统为 Telnet 客户端，远程主机为 Telnet 服务器，该系列交换机既可以作为 Telnet 服务器也可以作为 Telnet 客户端。

当交换机作为 Telnet 服务器时，用户可以通过 Windows 或其他操作系统自带的 Telnet 客户端软件，Telnet 登录到交换机上。交换机作为 Telnet 服务器时最多可以同时与 5 个 Telnet 客户端建立 TCP 连接。

当交换机作为 Telnet 客户端时，在交换机一般用户配置模式下使用 telnet 命令即可登录到其他远程主机。交换机作为 Telnet 客户端时只能与一个远程主机建立 TCP 连接，如果想与另一个远程主机建立连接，则必须先断开与上一个远程主机的 TCP 连接。

5.10.2 Web 页面配置

1、使能交换机 Telnet 服务器功能

点击导航树[设备基本配置]→[Telnet 服务器配置]→[Telnet 服务器端管理]菜单进入 Telnet 服务器端配置界面，如图 69 所示；

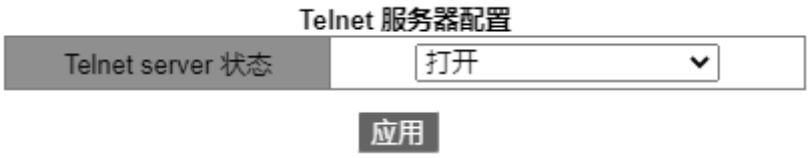


图 69 Telnet 服务器配置

Telnet server 状态

配置选项：打开/关闭

默认配置：打开

功能：打开/关闭交换机的 Telnet 服务器功能。

描述：打开表示 Telnet 客户端可以登录到交换机；关闭表示 Telnet 客户端不能登录到交换机。

说明：

无论该配置打开或关闭，交换机都可以作为 Telnet 客户端，通过 Telnet 命令登录到其他远程主机。

2、配置可以登录到交换机的 Telnet 客户端安全 IP 地址

点击导航树[设备基本配置]→[Telnet 服务器配置]→[Telnet 服务器安全 IP]菜单进入该配置界面，如图 70 所示；

图 70 Telnet server 安全 IP 地址配置

安全 IP 地址

配置格式：A.B.C.D

功能：配置交换机作为 Telnet 服务器时允许登录的 Telnet 客户端的 IP 地址。

描述：没有配置安全 IP 地址时，登录交换机的 Telnet 客户端 IP 地址不受限制；配置安全 IP 地址后，只有安全 IP 地址的客户端才能通过 Telnet 登录到交换机进行配置。

交换机最多可以配置 32 个安全 IP 地址，默认情况下没有配置任何安全 IP 地址。

配置完成后，“Telnet server 安全 IP 列表”中显示可以登录到交换机的 Telnet 客户端 IP 地

址。如图 71 所示；

Telnet server 安全 IP 列表
192.168.1.30
192.168.1.31
192.168.1.32
192.168.1.33
192.168.1.34
192.168.1.35

图 71 安全 IP 地址列表

5.11 SSH 服务器配置

5.11.1 介绍

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

该系列设备支持 SSH 服务器功能，可以配置多个 SSH 用户，但是同一时间最多允许两个 SSH 用户连接，从而通过 SSH 登录到远程设备上。

5.11.2 密钥

未加密的信息称为明文，加密后的信息称为密文，加密和解密都在密钥控制下进行。密钥是一组特定字符串，是控制明文和密文交换的唯一参数，起到“钥匙”的作用。加密操作可以将明文变成密文，解密操作可以将密文恢复为明文。

基于密钥的安全认证需要密钥，也就是通信的每一端都存在一对密钥，即一个私钥和一个公钥。可以用公钥对报文进行加密，然后由拥有私钥的合法者使用私钥对数据进行解密，这样保证数据的机密性。

5.11.3 实现

在通信过程中为实现 SSH 的安全连接，服务器与客户端之间要经历五个阶段：

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

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

认证阶段：SSH 客户端向服务器端发起认证请求，服务器端对客户端进行认证；

会话请求阶段：认证通过后，客户端向服务器端发送会话请求；

会话阶段：会话请求通过后，服务器端和客户端进行信息交互。

5.11.4 Web 页面配置

➢ SSH 服务器的配置过程如下：

点击导航树[设备基本配置]→[SSH 服务器配置]→[SSH 服务器端配置]菜单进入 SSH 服务器配置界面。

1、禁止 SSH 状态；

2、点击<销毁>按钮来销毁旧密钥对，如图 72 所示；

图 72 销毁旧密钥对

3、点击<生成>按钮来生成新密钥对；

4、使能 SSH 协议，并对 SSH 服务器进行配置，如图 73 所示；

图 73 SSH 服务器配置

SSH 状态

配置选项：打开/关闭

默认配置：关闭

功能：是否使能 SSH 协议，如果使能 SSH，则该设备作为 SSH 服务器。

重复认证次数

配置范围：1~10

默认配置：10

功能：尝试登录 SSH 服务器的次数。

本地密钥对

配置选项：生成/销毁

功能：生成或销毁 SSH 服务器的本地密钥对，使能 SSH 服务器前应生成本地密钥对，生成新密钥对之前先销毁旧密钥对。

本地密钥值

显示本地密钥值，点击<生成>按钮后自动生成密钥值。

- SSH 安全 IP 地址配置

点击导航树[设备基本配置]→[SSH 服务器配置]→[SSH 服务器安全 IP]菜单进入 SSH 安全 IP 地址配置界面。如图 74 所示；

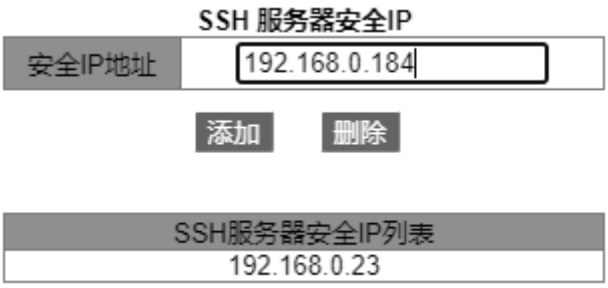


图 74 SSH 安全 IP 地址配置

安全 IP 地址

配置格式：A.B.C.D

功能：配置允许登录交换机的 SSH 客户端 IP 地址；没有配置安全 IP 地址时，登录交换机的 SSH 客户端 IP 地址不受限制；配置安全 IP 地址后，只有安全 IP 地址才可通过 SSH 协议访问交换机。

说明：最多可以配置 6 个 SSH 安全 IP 地址，默认情况下，没有配置任何安全 IP 地址。

5.11.5 典型配置举例

Host 做为 SSH 客户端与 Switch 建立本地连接，如图 75 所示；

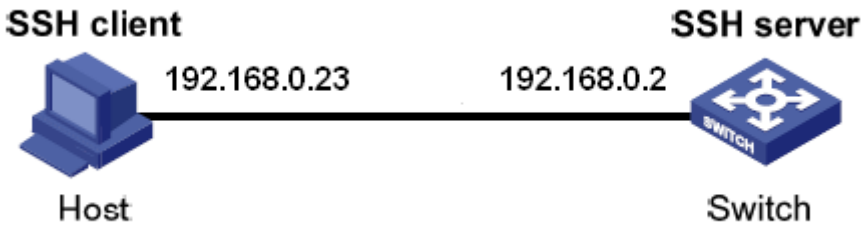


图 75 SSH 配置举例

- SSH 用户采用密码认证方式；

1、销毁服务器旧密钥对，生成新的密钥对并启动 SSH 服务器，见图 72，图 73；

2、配置 SSH 用户名：333，服务类型：ssh，认证类型：密码，密码：333，见图 31；

3、建立与 SSH 服务器端的连接，打开 PuTTY.exe 软件如图 76 所示，在 Host Name(or IP address)中输入 SSH 服务器 IP 地址：192.168.0.2；

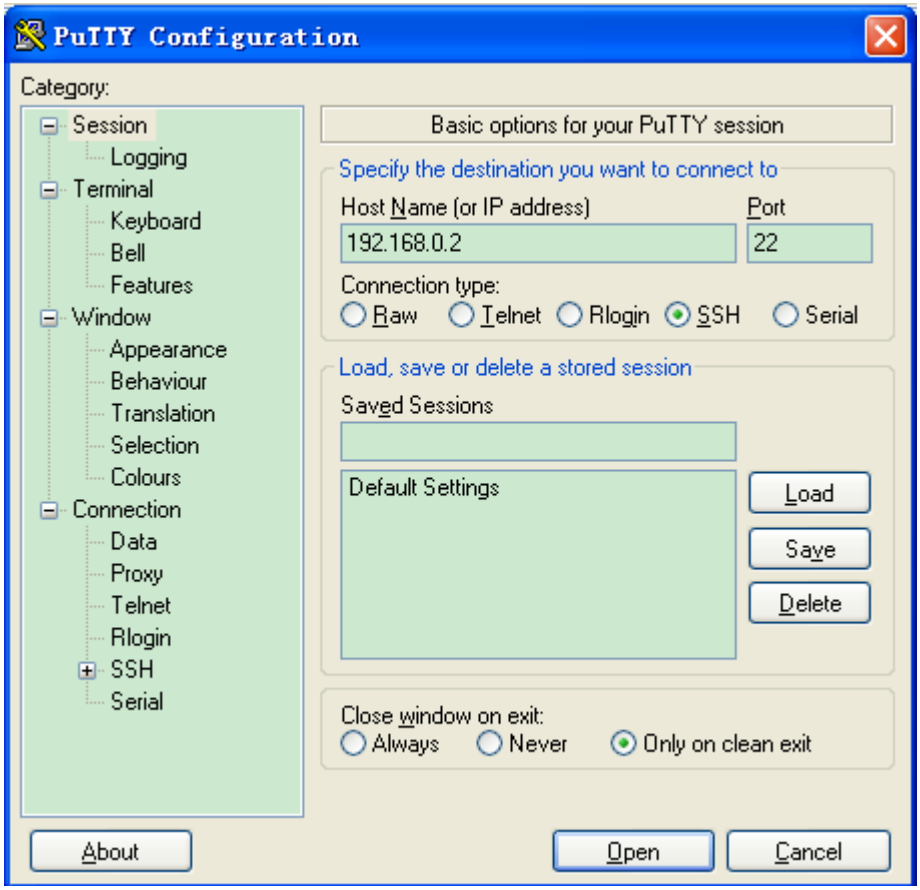


图 76 SSH 客户端配置

4、点击<Open>按钮，出现如图 77 所示警告信息时，点击<是(Y)>按钮；

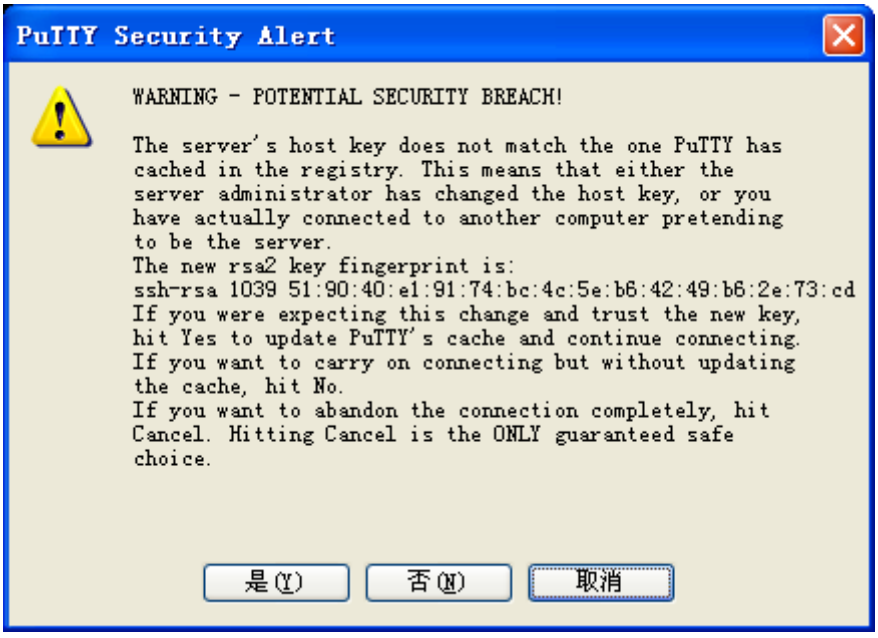


图 77 警告信息

5、按提示输入用户名：333 和密码：333，便可以进入交换机配置页面，如图 78 所示。

图 78 SSH 密码认证方式登录界面

➢ SSH 用户采用密钥认证方式；

1、销毁服务器旧密钥对，生成新的密钥对并启动 SSH 服务器，见图 72，图 73；

2、配置 SSH 客户端，见图 33；在客户端运行 PuTTYGen.exe，点击<Generate>按钮产生客户端密钥对，如图 79 所示；

图 79 生成客户端密钥

3、生成客户端密钥对的过程中将鼠标在窗口中移动，否则进程条不动，密钥停止生成，如图 80 所示；

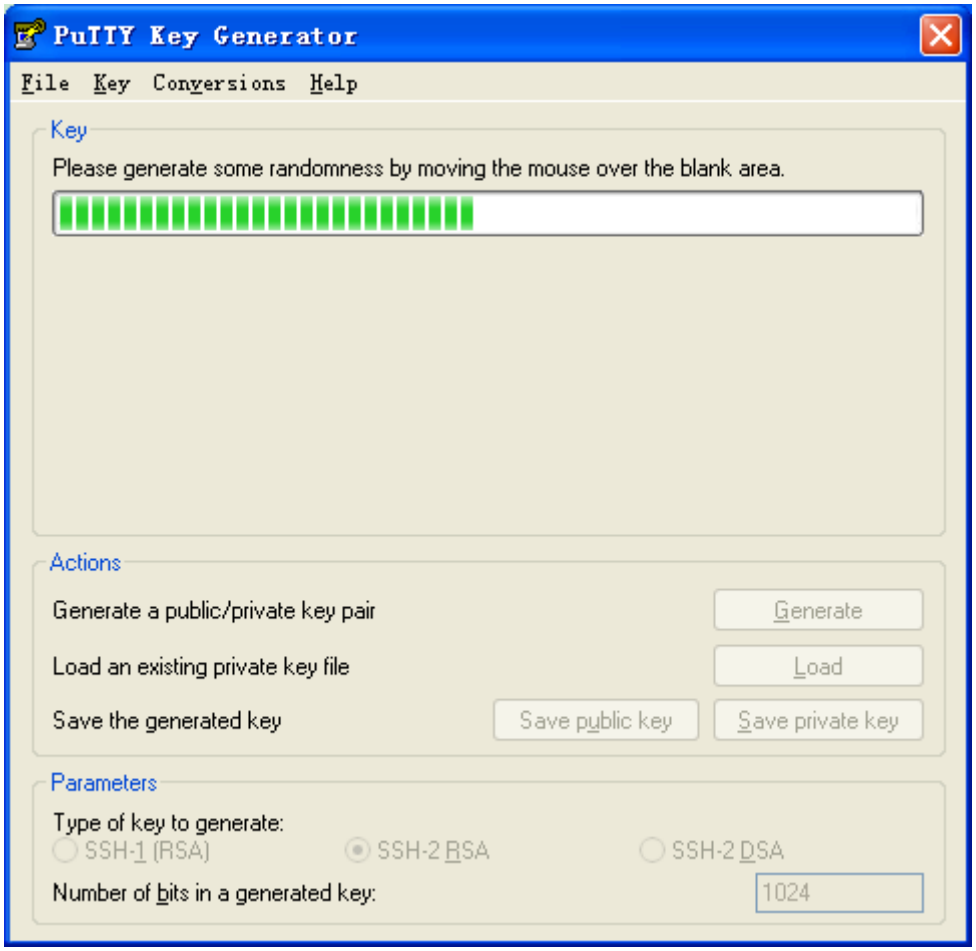


图 80 密钥生成过程

4、图 81 所示生成密钥，点击<Save private key>按钮存储私钥为 444.ppk 文件，并将公有密钥拷贝到 SSH 密钥配置的密钥值中并输入密钥名 444，见图 33。

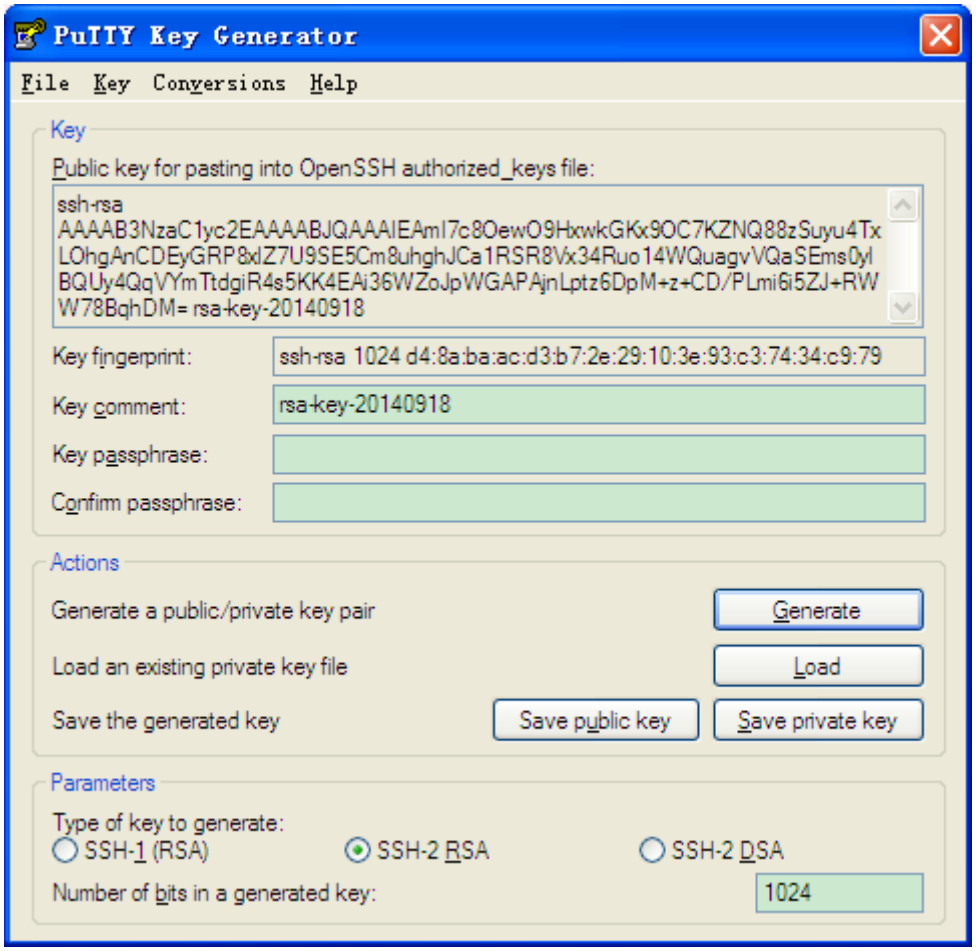


图 81 生成密钥值

5、配置 SSH 用户名：444，服务类型：ssh，认证类型：密钥，密钥：444，见图 31；

6、建立与 SSH 服务器端的连接，打开 PuTTY.exe 软件如图 82 所示，在 Host Name(or IP address)中输入 SSH 服务器 IP 地址：192.168.0.2。

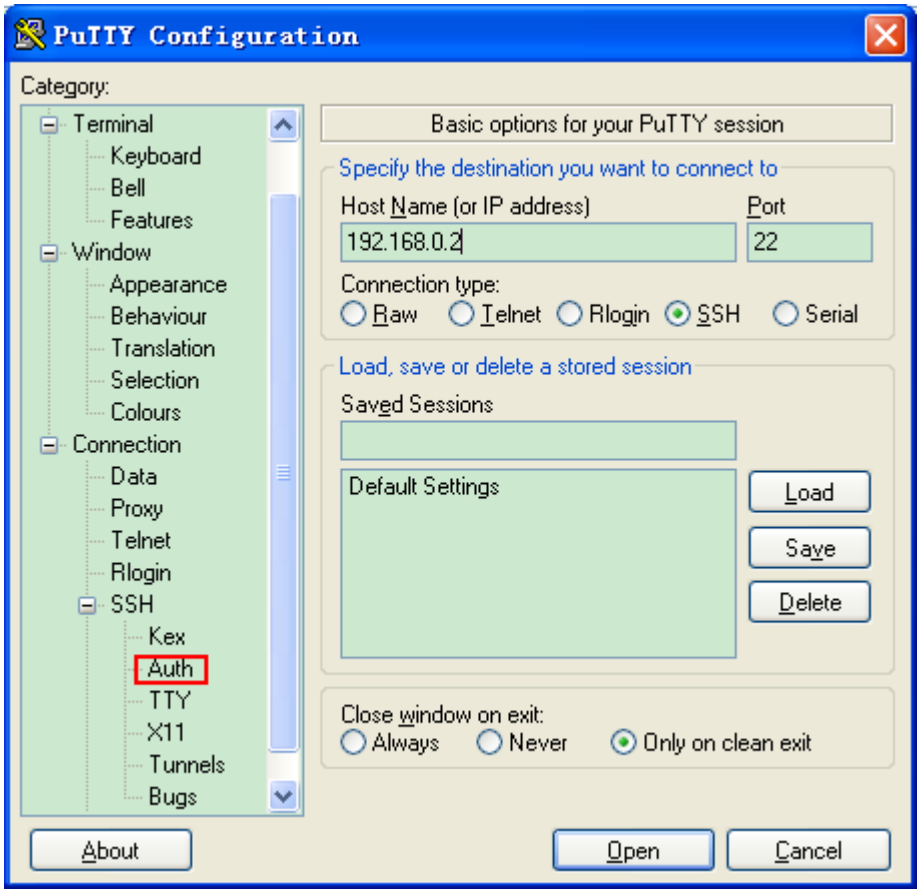


图 82 选择密钥验证方式时 SSH 客户端配置

7、点击图 82 左边[SSH]→[Auth]，出现图 83 所示界面，点击<Browse>按钮，选择第 4 步中存储的私钥文件，

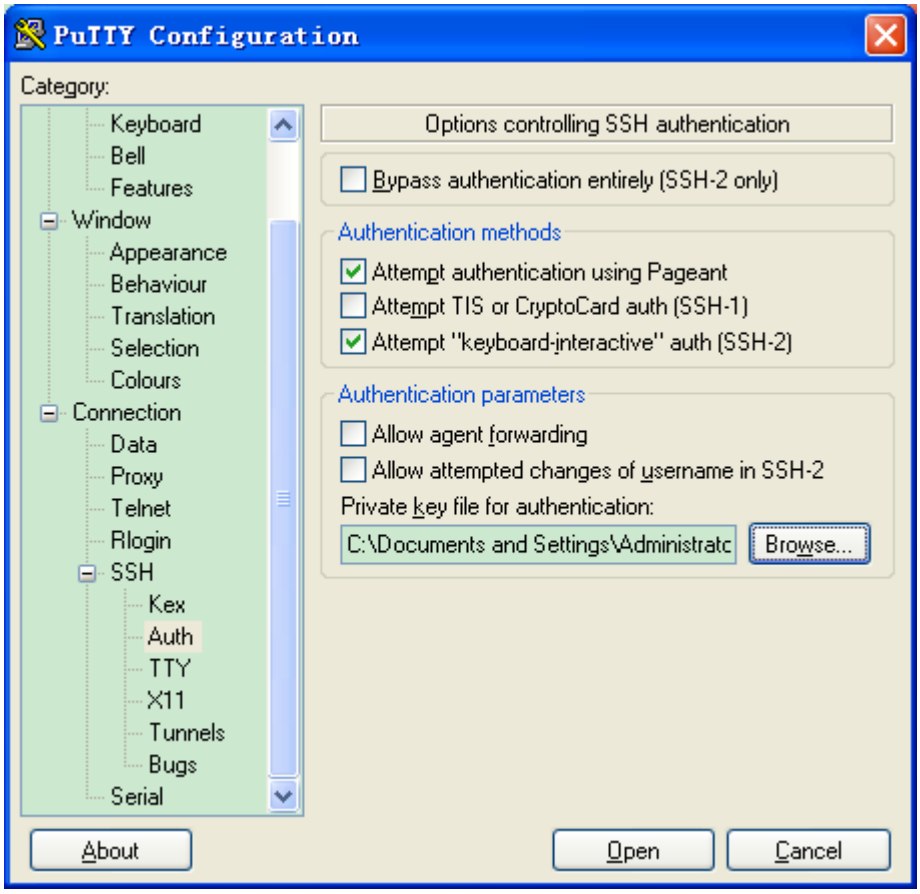


图 83 选择密钥文件

8、点击<Open>按钮，按照提示输入用户名，即可进入交换机的配置界面，如图 84 所示。

图 84 SSH 密钥认证方式登录界面

5.12 SSL 配置

5.12.1 介绍

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

交换机使能 SSL 后，用户必须使用安全链接 https(如：https://192.168.0.2)登录交换机。

5.12.2 Web 页面配置

1、使能 HTTPS 协议

点击导航树[设备基本配置]→[SSL 配置]→[SSL 配置]菜单进入 SSL 配置界面，如图 85 所示；

图 85 使能 HTTPS 协议

服务器状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能 SSL 协议。

描述：使能后，使用安全链接 https://*ip address* 登录交换机 Web 页面。

证书/私钥

功能：输入正确的证书和私钥值，点击<应用>按钮导入交换机中。

注意：

该交换机中已导入本公司提供的缺省证书和私钥，用户可直接使能 SSL 协议，通过 HTTPS 方式访问交换机。

2、登录 Web 页面，输入用户名和密码，通过 HTTPS 成功登录到交换机。

5.13 访问管理

5.13.1 Web 页面配置

访问管理页面，可以配置是否使能访问管理，访问管理 ID，vlan ID，起始 IP 地址，结束

IP 地址，HTTP/HTTPS，SNMP，TELNET/SSH 访问管理方式，如图 86 所示。

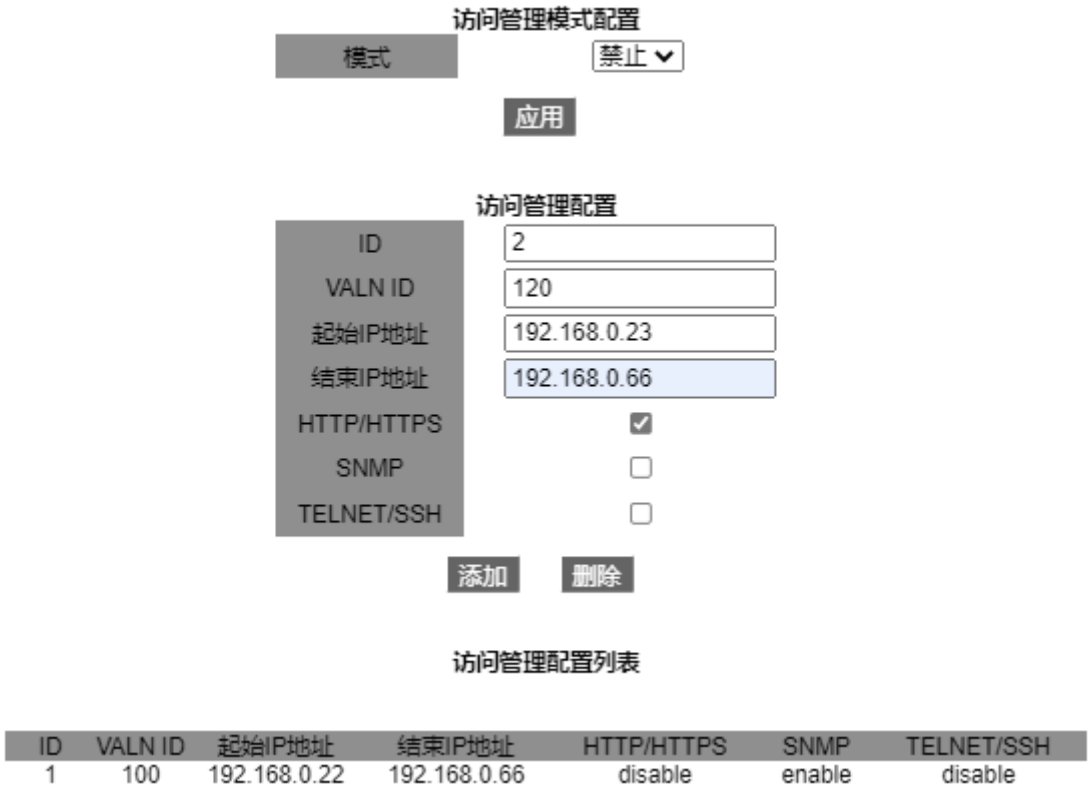


图 86 访问管理配置页面

访问管理模式配置

配置选项：使能/禁止

默认配置：禁止

功能：是否使能访问管理，如果使能访问管理，则该设备将对设备访问进行管理。

访问管理配置

ID

配置范围：1~16

功能：用于标记设备的访问管理条件。

Vlan ID

配置范围：1~4093

功能：配置需要进行访问管理的 VLAN。

起始 IP 地址

配置格式：A.B.C.D

功能：配置允许登录交换机的 IP 地址范围；起始 IP 地址不能为空；配置了起始 IP 地址后，只有起始 IP 地址以后的 IP 地址才可访问对应的 VLAN。

结束 IP 地址

配置格式：A.B.C.D

功能：配置允许登录交换机的 IP 地址范围；配置了终止 IP 地址后，只有起始 IP 地址到终止 IP 地址之间的 IP 地址才可访问对应的 VLAN。

HTTP/HTTPS

功能：选中 HTTP/HTTPS 时，匹配表项中 VLAN ID 以及 IP 地址的主机可以通过 HTTP/HTTPS 访问交换机

SNMP

功能：选中 SNMP 时，匹配表项中 VLAN ID 以及 IP 地址的主机可以通过 SNMP 访问交换机。

TELNET/SSH

功能：选中 TELNET/SSH 时，匹配表项中 VLAN ID 以及 IP 地址的主机可以通过 TELNET/SSH 访问交换机。

5.14 文件传输服务

文件传输服务可以使客户端和服务器中的文件信息相互备份，当客户端(服务器)文件信息改变后可以通过 FTP/TFTP/SFTP 协议从服务器(客户端)通过文件传输获得备份文件。

交换机既可以作为客户端也可以作为服务器通过 FTP/TFTP/SFTP 协议上传、下载文件。

5.14.1 TFTP 服务

1、交换机作为 TFTP 客户端

- 首先安装 TFTP 服务器，如图 87 所示，在 Current Directory 栏选择服务器上文件存放路径；Server interface 中输入服务器 IP 地址；

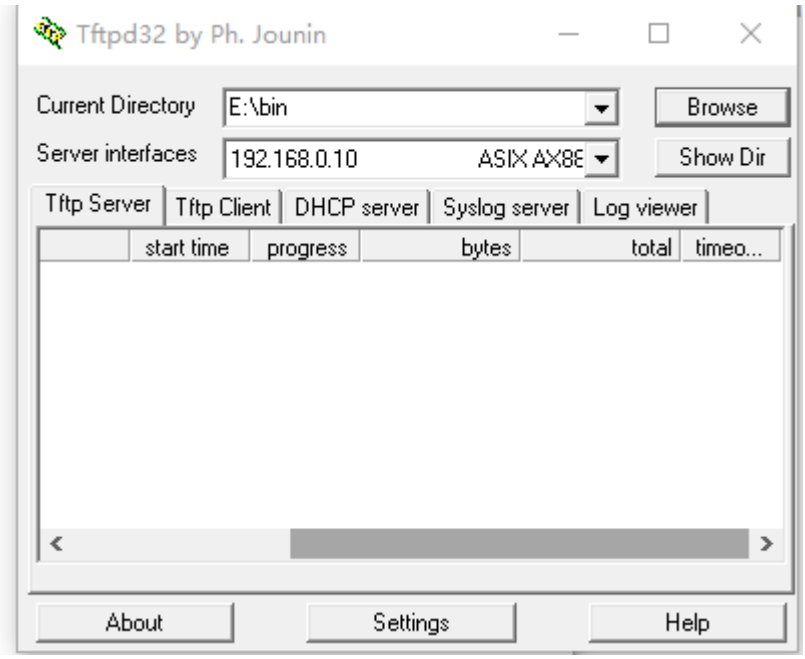


图 87 TFTP 服务器配置

- 点击导航树[设备基本配置]→[文件传输服务]→[TFTP 服务] →[TFTP 客户端服务]菜单进入交换机 TFTP 客户端配置界面，如图 88 所示；

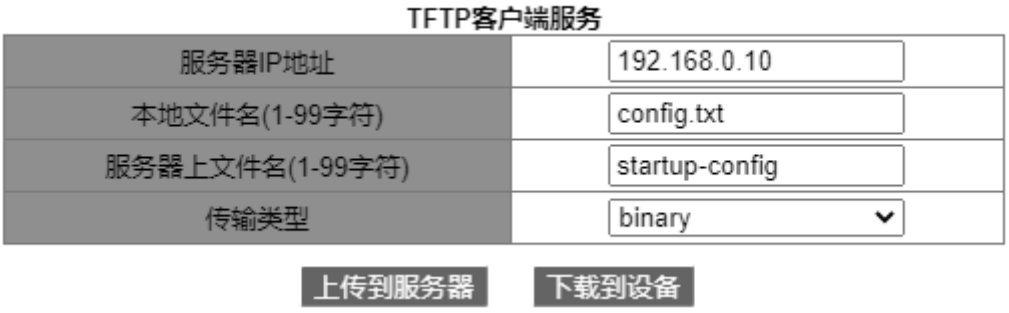


图 88 TFTP 客户端服务

服务器 IP 地址

配置格式：A.B.C.D

描述：输入服务器的 IP 地址。

本地文件名

配置范围：1~99 个字符

描述：交换机中文件名。

服务器上文件名

配置范围：1~99 个字符

描述：服务器中文件名。

传输类型

配置选项：binary/ascii

默认配置：binary

功能：选择文件传输标准。

描述：ascii 表示采用 ASCII 标准传输文件；binary 表示采用二进制标准传输文件。

用法：点击<上传到 PC>按钮把交换机中文件上传到服务器中；点击<下载到设备>按钮把服务器中文件下载到交换机中。

- Web 页面中出现如图 89、图 90 所示信息时表示文件传输成功。

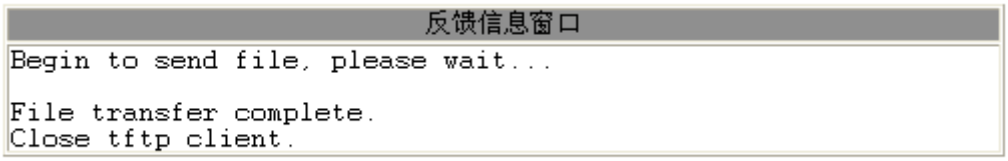


图 89 TFTP 客户端上传文件成功

图 90 TFTP 客户端下载文件成功

注意：

文件传输过程中，TFTP 服务器软件应保持运行状态；

- 软件版本文件属于非文本文件，应采用 binary 二进制标准传输文件。

2、交换机作为 TFTP 服务器

- 点击导航树[设备基本配置]→[文件传输服务]→[TFTP 服务] →[TFTP 服务器端服务]菜单进入交换机 TFTP 服务器配置界面，如图 91 所示；

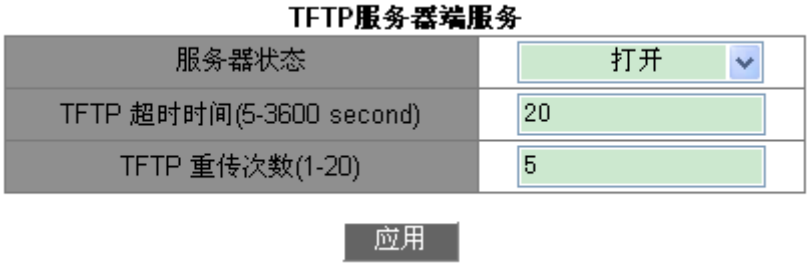


图 91 TFTP 服务器端服务

服务器状态

配置选项：打开/关闭

默认配置：关闭

功能：打开/关闭交换机 TFTP 服务器功能。

TFTP 超时时间

配置范围：5~3600s

默认配置：20s

功能：配置 TFTP 服务器连接超时时间。

TFTP 重传次数

配置范围：1~20

默认配置：5

功能：配置超时时间内 TFTP 服务器重新传输数据的次数。

- 安装 TFTP 客户端软件，如图 92 所示，在 Host 中输入交换机的 IP 地址；Local File 栏选择客户端文件存放路径及文件名称；Remote File 栏输入交换机中文件名。点击<Get>按钮把交换机中文件下载到客户端，点击<Put>按钮把客户端文件上传到交换机中。

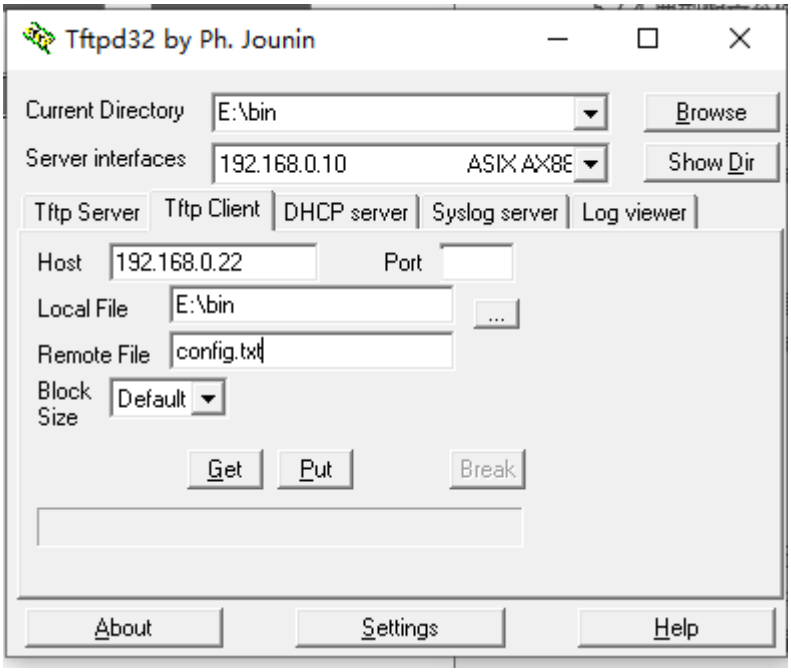


图 92 TFTP 客户端配置

注意：

文件传输过程中，TFTP 客户端软件应保持运行状态。

5.14.2 FTP 服务

1、交换机作为 FTP 客户端

- 首先安装 FTP 服务器，打开[Security]→[users/rights]对话框点击<new user>按钮添加 FTP 新用户，如图 93 所示，输入用户名和密码，例如：用户名 admin，密码 123，点击<OK>按钮；

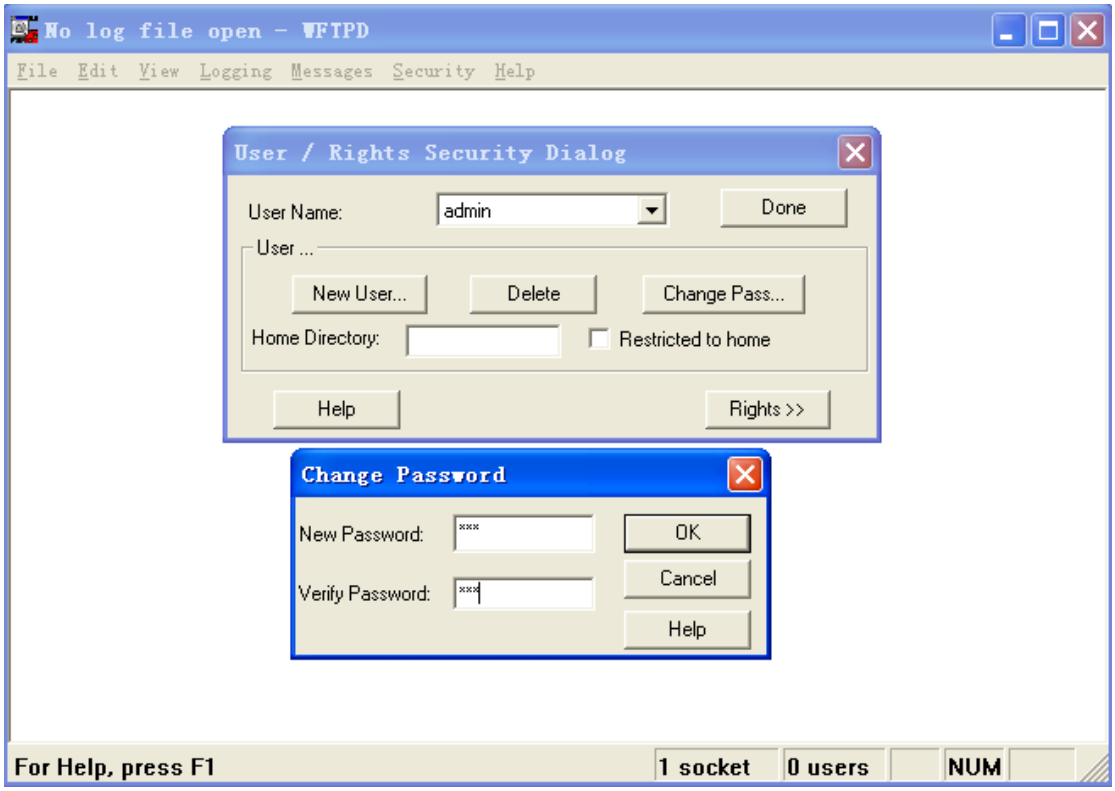


图 93 添加 FTP 新用户

- Home Directory 栏中输入需要服务器中文件的存放路径，如图 94 所示，点击<Done>按钮；

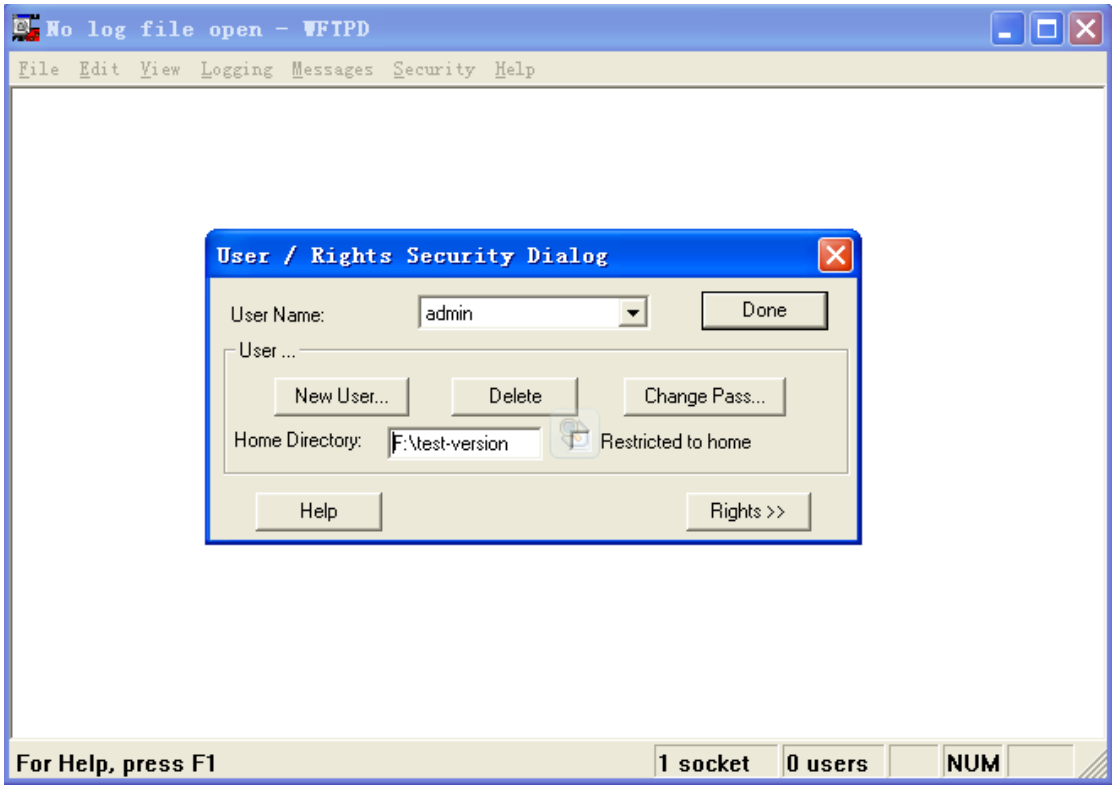


图 94 文件路径修改

- 点击导航树[设备基本配置]→[文件传输服务]→[FTP 服务] →[FTP 客户端服务]菜单进入交换机 FTP 客户端配置界面，如图 95 所示；

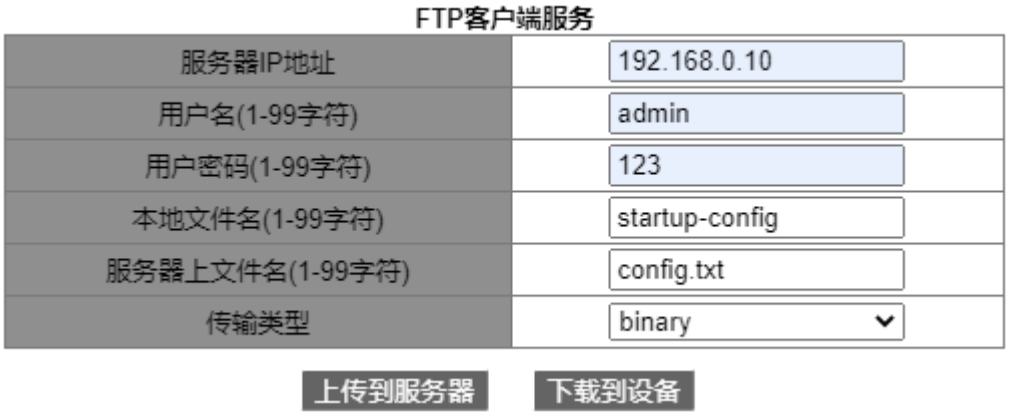


图 95 FTP 客户端服务

服务器 IP 地址

配置格式：A.B.C.D

描述：输入服务器的 IP 地址。

{ 用户名，密码 }

配置范围：{ 1~99 个字符，1~99 个字符}

描述：FTP 服务器创建的用户名和密码。

本地文件名

配置范围：1~99 个字符

描述：交换机中文件名。

服务器上文件名

配置范围：1~99 个字符

描述：服务器中文件名。

传输类型

配置选项：binary/ascii

默认配置：binary

功能：选择文件传输标准。

描述：ascii 表示采用 ASCII 标准传输文件；binary 表示采用二进制标准传输文件。

用法：点击<上传到 PC>按钮把交换机中文件上传到服务器中；点击<下载到设备>按钮把

服务器中文件下载到交换机中。

- Web 页面中出现如图 96、图 97 所示信息时表示文件传输成功。

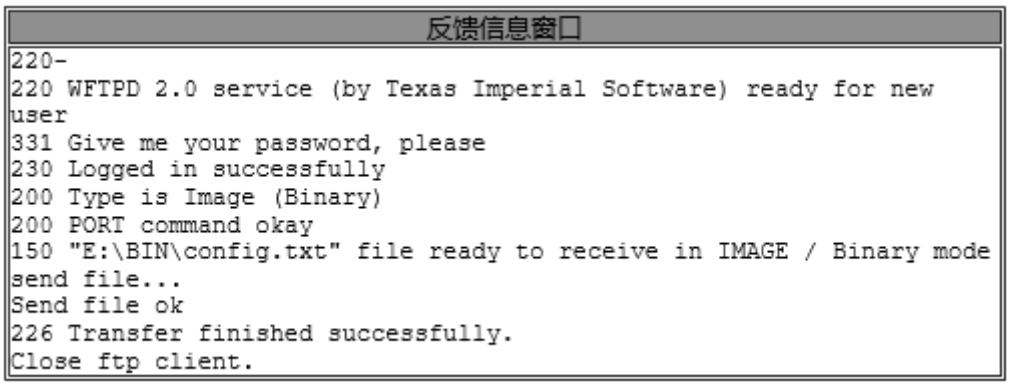


图 96 FTP 客户端上传文件成功

图 97 FTP 客户端下载文件成功

注意：

- 文件传输过程中，FTP 服务器软件应保持运行状态；
- 软件版本文件属于非文本文件，应采用 binary 二进制标准传输文件。

2、交换机作为 FTP 服务器

- 点击导航树[设备基本配置]→[文件传输服务]→[FTP 服务] →[FTP 服务器端服务]菜单进入交换机 FTP 服务器配置界面，如图 98 所示；

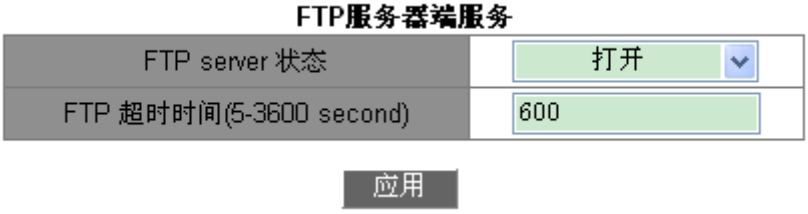


图 98 FTP 服务器端服务

FTP Server 状态

配置选项：打开/关闭

默认配置：关闭

功能：打开/关闭交换机 FTP 服务器功能。

FTP 超时时间

配置范围：5~3600s

默认配置：600s

功能：配置 FTP 服务器连接空闲时间。

描述：如果在该空闲时间内，FTP 服务器和客户端没有消息交互，则断开他们之间的连接。

- 配置登录 FTP 服务器使用的用户名和密码，如图 99 所示；

图 99 FTP 服务器用户名和密码配置

{ 用户名，用户密码 }

配置范围：{ 1~16 个字符，1~16 个字符 }

功能：配置登录 FTP 服务器使用的用户名和密码。

描述：交换机 FTP 服务器可以同时与多个 FTP 客户端建立连接。

状态

配置选项：明文/密文

默认配置：明文

功能：选择密码显示方式。

- 点击 Windows 系统[开始]→[运行]打开运行对话框，输入“**cmd**”打开命令行界面，如图 100 所示；

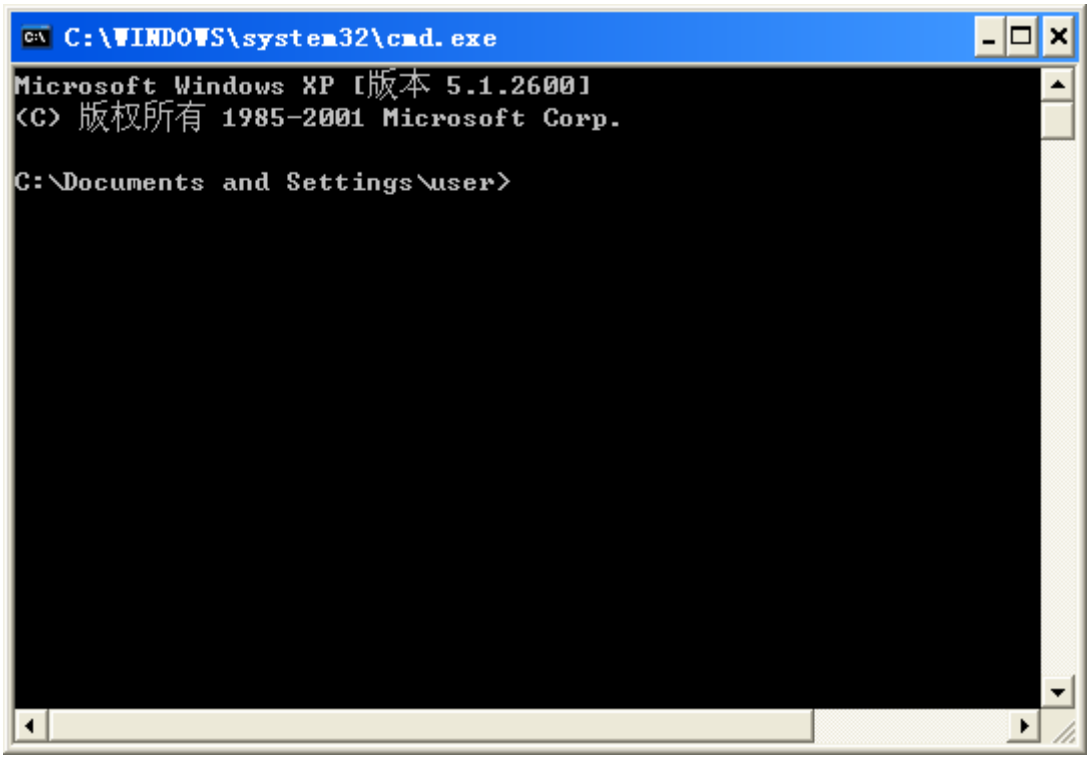


图 100 cmd 命令行界面

- 可以修改文件传输路径，登录 FTP 服务器，如图 101 所示；

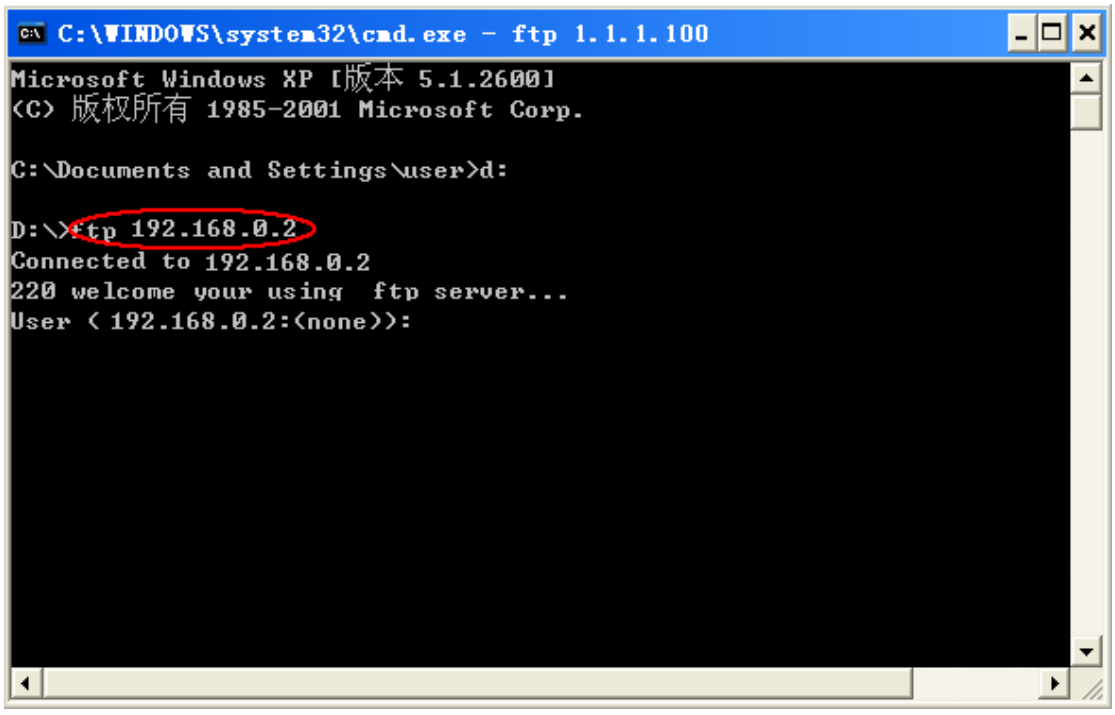


图 101 连接 FTP 服务器

- 用已配置的用户名：admin，密码：123 登录 FTP 服务器，如图 102 所示；

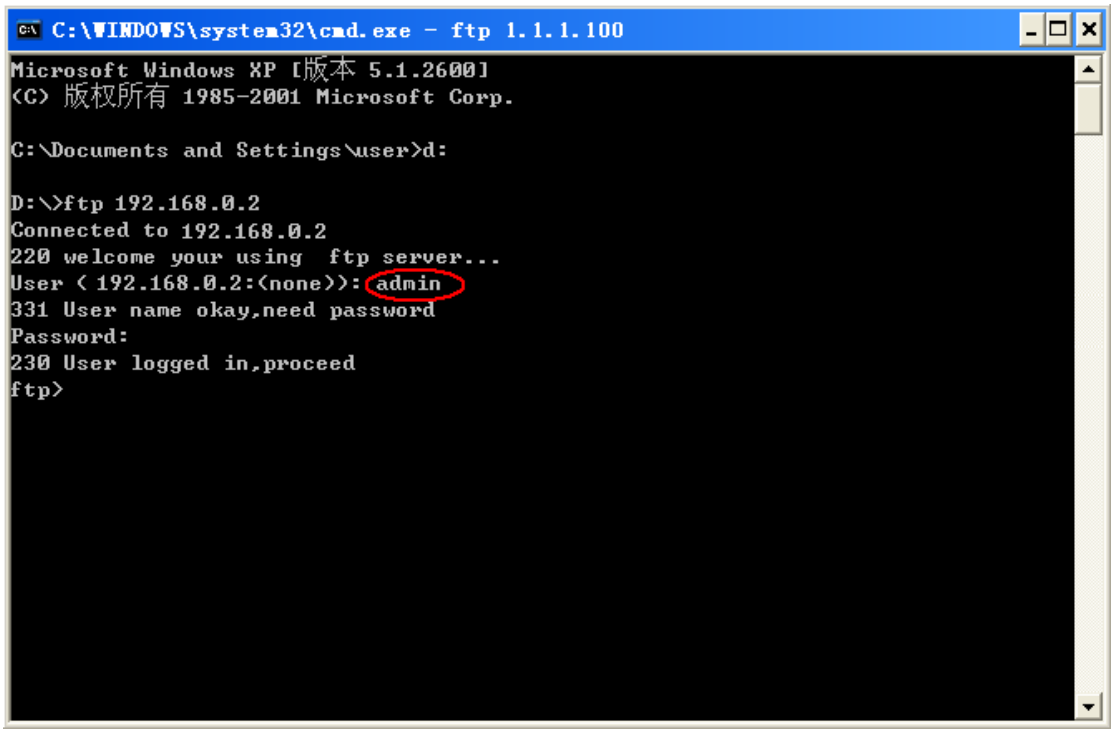


图 102 登录 FTP 服务器

- 通过指令 get 可以把交换机中文件下载到客户端指定路径，如图 103 所示，输入 get 命令按回车，Remote file 输入交换机中需要下载的文件名，Local file 输入客户端中文件名；

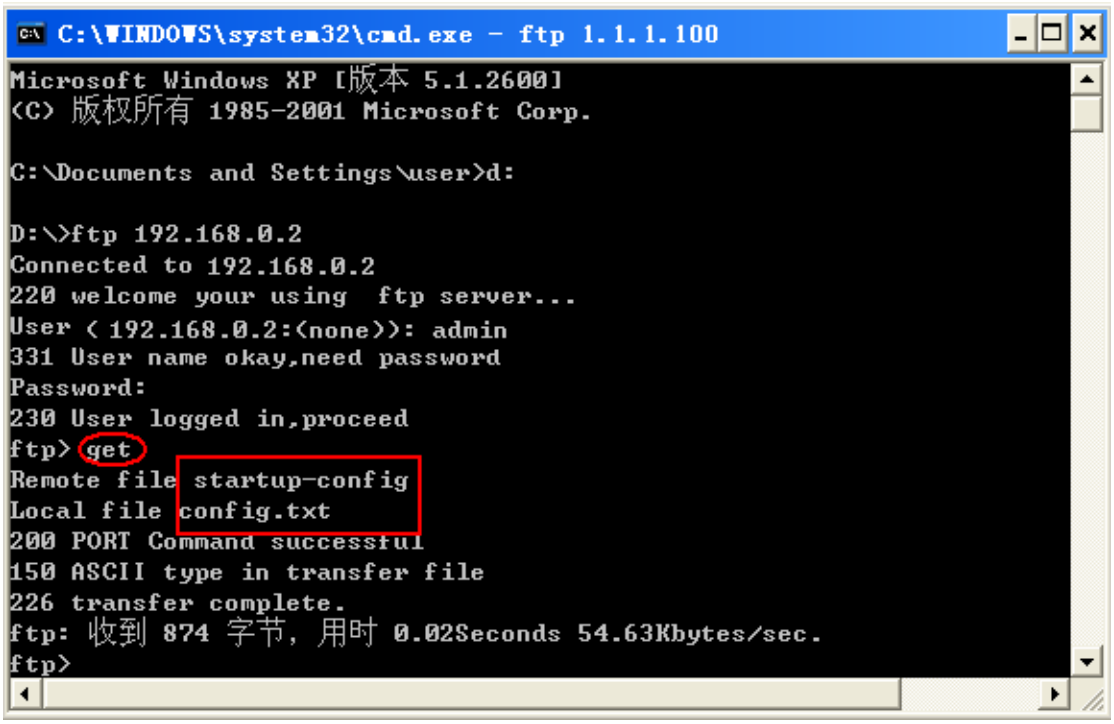


图 103 从交换机下载文件到客户端

- 通过指令 put 可以把客户端指定路径下的文件上传到服务器中，如图 104 所示，输入

put 命令按回车，Remote file 输入交换机中文件名，Local file 输入客户端需要上传的文件名。

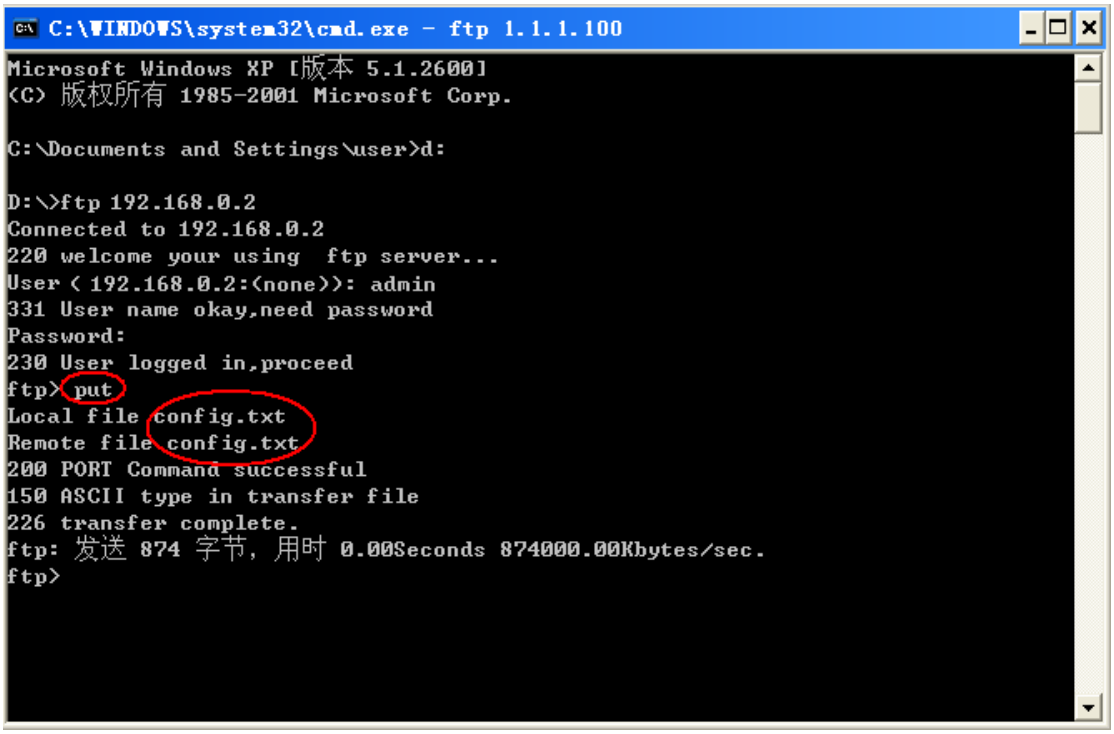


图 104 从客户端上传文件到交换机

5.14.3 SFTP 服务

交换机作为 SFTP 客户端

- 首先安装 SFTP 服务器，打开添加 SFTP 新用户，如图 105 所示，输入 User 和 Password，例如：User: admin, Password: 123；Port 为 SFTP 协议端口号 22；Root path 栏中输入服务器中文件的存放路径，点击<Start>按钮；

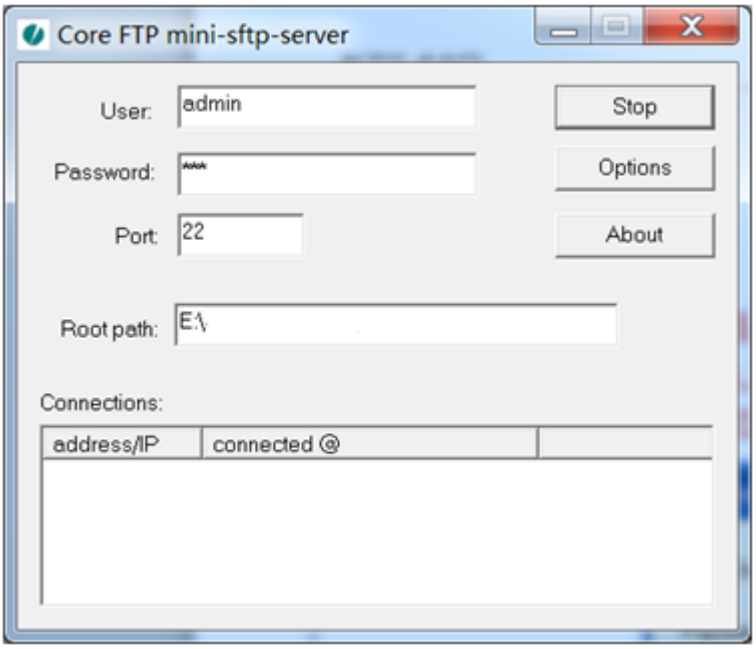


图 105 添加 SFTP 新用户

➢点击导航树[设备基本配置]→[文件传输服务]→[SFTP 服务] →[SFTP 客户端服务]菜单进入交换机 SFTP 客户端配置界面，如图 106 所示；

SFTP客户端服务

服务器IP地址	192.168.0.50
用户名(1-99字符)	admin
用户密码(1-99字符)	123
本地文件名(1-99字符)	running-config
服务器上文件名(1-99字符)	config.txt

上传到服务器　下载到设备

图 106 SFTP 客户端服务

服务器 IP 地址

配置格式：A.B.C.D

描述：输入服务器的 IP 地址。

{ 用户名，密码 }

配置范围：{ 1~99 个字符，1~99 个字符}

描述：SFTP 服务器创建的用户名和密码。

本地文件名

配置范围：1~99 个字符

描述：交换机中文件名。

服务器上文件名

配置范围：1~99 个字符

描述：服务器中文件名。

用法：点击<上传到服务器>按钮把交换机中文件上传到服务器中；点击<下载到设备>按钮把服务器中文件下载到交换机中。

➢Web 页面中出现如图 107、图 108 所示信息时表示文件传输成功。

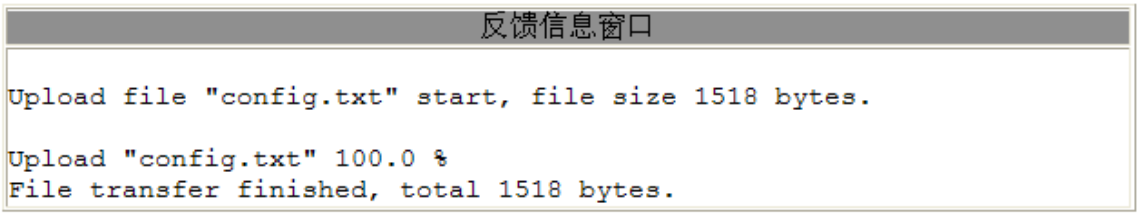


图 107 SFTP 客户端上传文件成功

图 108 SFTP 客户端下载文件成功

5.15 MAC 地址配置

5.15.1 介绍

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

MAC 地址分为静态 MAC 地址和动态 MAC 地址。

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

动态 MAC 地址由交换机在转发数据帧的过程中学习，且在有限时间内生效，定期的更新

MAC 地址表。当交换机接收到需要转发的数据帧时，首先学习数据帧的源 MAC 地址，与接收端口建立映射关系；然后根据目的 MAC 地址查询 MAC 地址表，如果查到相关表项，交换机将数据帧从相应端口转发；否则，交换机将数据帧在其所属广播域内广播。

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

该系列交换机最多可以配置 1024 个静态单播表项。

5.15.2 Web 页面配置

1、配置 MAC 地址绑定

点击导航树[设备基本配置]→[MAC 地址配置]→[MAC 地址绑定配置]菜单进入 MAC 地址绑定配置界面，如图 109 所示；

图 109 MAC 地址绑定配置

MAC 地址绑定配置状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 MAC 地址绑定功能。使能时，报文中的源 MAC 地址、VLAN ID 与静态配置的 MAC 地址表项中的 MAC 地址、VLAN ID 一致时，检查入端口是否与该静态 MAC 地址表项的端口一致，一致时接收该报文并转发，不一致时丢弃该报文。不使能时，不进行上述检查。

2、添加静态单播 MAC 地址表项

点击导航树[设备基本配置]→[MAC 地址配置]→[单播地址配置]菜单进入单播 MAC 地址配置界面，如图 110 所示；

图 110 添加静态 FDB 表

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH (H 为一个十六进制数)

功能：配置单播 MAC 地址，最高字节的最低位为 0。

VLAN 号

配置选项：已创建的所有 VLAN ID

默认配置：VLAN 1

配置类型

配置选项：静态地址/永久过滤

默认配置：静态地址

功能：选择 MAC 地址表项的属性。

描述：静态地址将特定 MAC 地址与端口号、VLAN ID 建立映射关系；永久过滤丢弃源 MAC 地址或目的 MAC 地址为特定 MAC 地址的报文。

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。

3、删除单播地址

点击导航树[设备基本配置]→[MAC 地址配置]→[单播地址删除]菜单进入单播 MAC 地址删除界面，如图 111 所示；

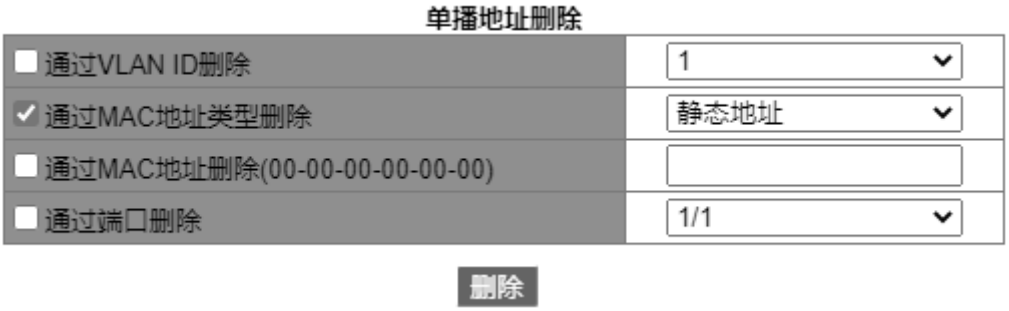


图 111 单播 MAC 地址删除

选择删除单播 MAC 地址的条件，如果选择多个条件时，相互之间是“与”的关系。

4、配置 MAC 地址老化时间

点击导航树[设备基本配置]→[MAC 地址配置]→[MAC 地址老化时间设置]菜单进入老化时间配置界面，如图 112 所示；

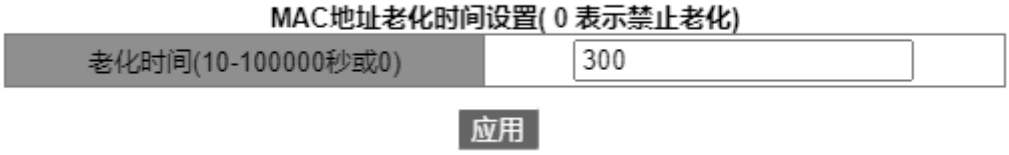


图 112 MAC 地址老化时间配置

老化时间

配置范围：10~100000s

默认配置：300s

功能：配置动态 MAC 地址表项的老化时间。

描述：当老化时间为 0 时禁止老化，即交换机动态学习到的 MAC 地址表项将一直保存在 MAC 地址表中，不会随着时间而老化。

5、单播 MAC 地址查询

点击导航树[设备基本配置]→[MAC 地址配置]→[MAC 地址查询]菜单进入单播 MAC 地址查询界面，如图 113 所示；

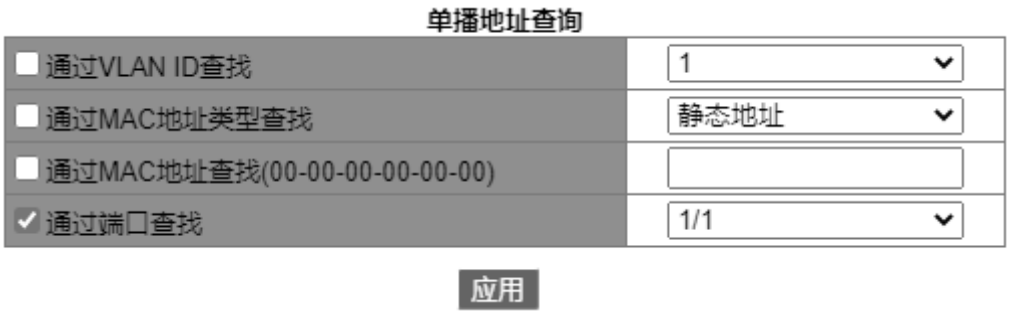


图 113 单播 MAC 地址查询

选择查询单播 MAC 地址的条件，如果选择多个条件时，相互之间是“与”的关系。例如查询端口 1/1 对应的 MAC 地址表，如图 114 所示；

图 114 单播 MAC 地址查询列表

6、查看单播地址表项

点击导航树[设备基本配置]→[MAC 地址配置]→[显示 MAC 地址表]菜单进入单播 MAC 地址查看界面，可以查看所有的动态表项和静态表项。如图 115 所示；

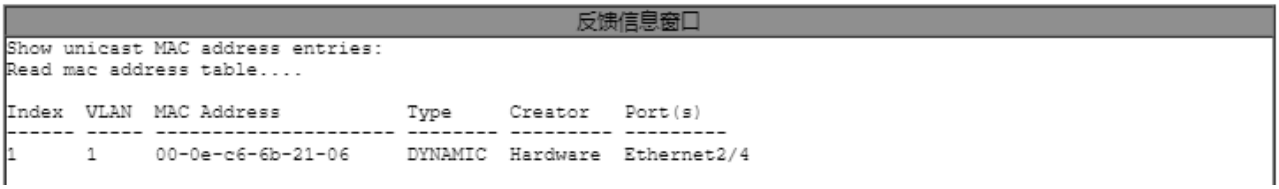


图 115 查看单播地址表项

5.16 基本配置维护和调试信息

当用户配置交换机时，需要查看各项配置是否正确，交换机是否按要求正常工作；或者当网络出现故障时用户需要诊断故障。通过以下操作能够帮助用户查看系统配置、运行状态等信息。

1、ping 操作

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[Ping 和 Traceroute]菜单进入 Ping 操作界面，如图 116 所示；

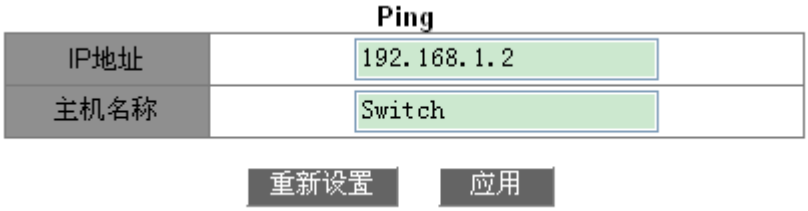


图 116 Ping 操作

IP 地址

配置格式：A.B.C.D

描述：输入远端设备的 IP 地址。

主机名称

配置范围：1~30 个字符

功能：如果已配置远端主机与 IP 地址的映射关系，可以输入远端主机名称进行 Ping 操作。交换机向远端设备发 ICMP 请求包，检测交换机与远端设备之间是否可以正常通信

2、Traceroute 操作配置，如图 117 所示；

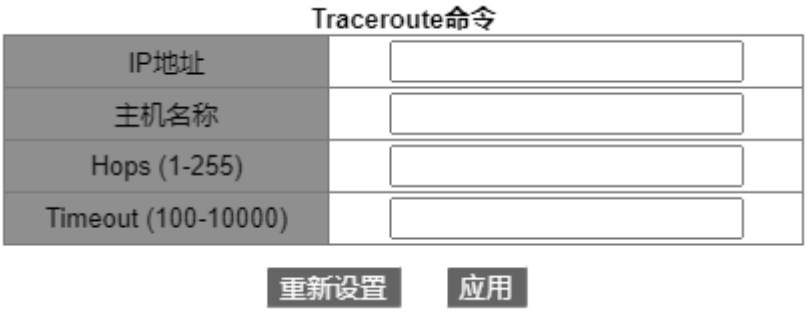


图 117 Traceroute 操作

IP 地址

配置格式：A.B.C.D

描述：输入远端设备的 IP 地址。

主机名称

配置范围：1~30 个字符

功能：如果已配置远端主机与 IP 地址的映射关系，可以输入远端主机名称进行 Ping 操作。

Hops

配置选项：1~255

功能：测试数据包从发送设备到目的设备所经过的网关数目。

Timeout

配置选项：100~10000ms

功能：配置超时时间，如果该时间值内发送方未收到接收方的响应报文，认为通信失败。

3、显示系统日期和时间

该系列交换机支持 RTC 实时时钟，交换机在断电后可以继续计时，点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示时钟]菜单进入时钟显示界面，如图 118 所示；

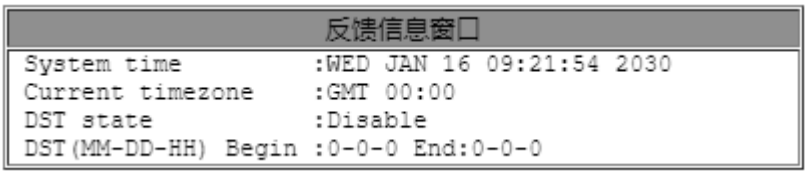


图 118 时钟显示

4、显示 Flash 中文件信息

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示 Flash]菜单进入 Flash 显示界面，如图 119 所示；

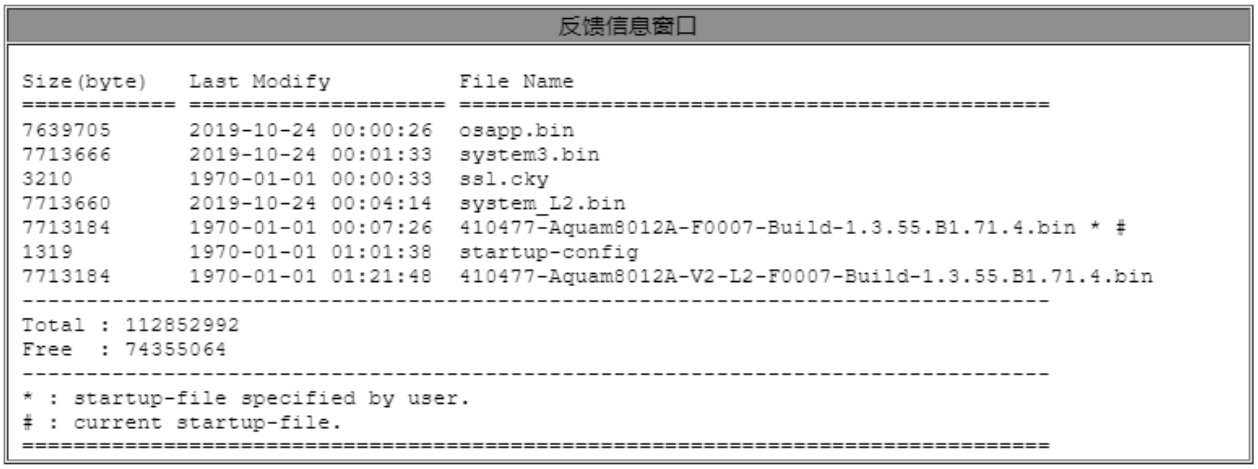


图 119 显示 flash

5、显示运行配置信息，即修改后生效的配置参数

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示运行配置]菜单进入运行配置显示界面，如图 120 所示；

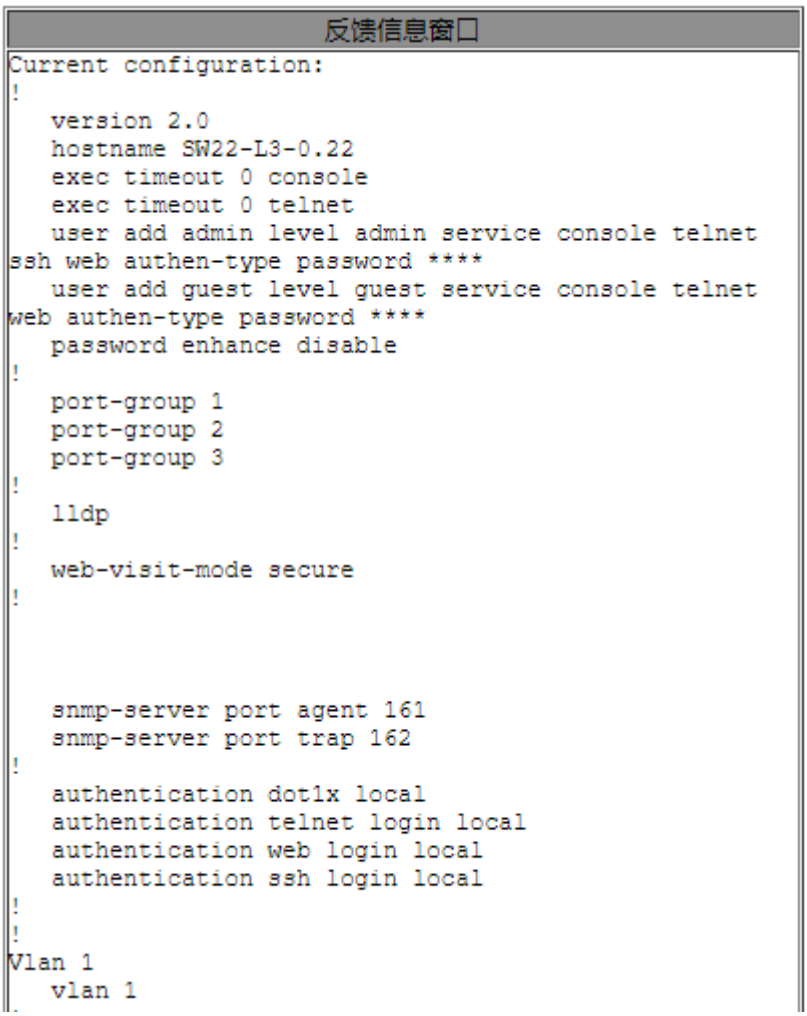


图 120 显示运行配置信息

6、显示端口信息

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示端口信息]菜单进入端口信息显示界面，如图 121 所示；

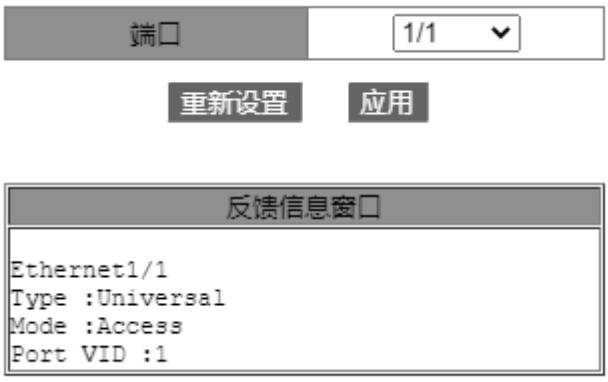


图 121 显示端口信息

Type

描述：VLAN 的类型。

Mode

描述：当前端口的模式。

Port VID

描述：当前端口的 PVID 号。

Trunk allowed Vlan With TAG

描述：当前 Trunk 端口以 Tag 类型允许通过的 VLAN 列表。

Trunk allowed Vlan With TAG

描述：当前 Trunk 端口以 Untag 类型允许通过的 VLAN 列表。

7、显示当前与交换机建立的 TCP 连接情况

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示 TCP 连接信息]菜单进入 TCP 连接信息显示界面，如图 122 所示；

反馈信息窗口

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State sockaddr
192.168.0.2	80	192.168.0.11	61632	ESTABLISH 418f0cc
192.168.0.2	80	192.168.0.11	57577	ESTABLISH 418f0e0
192.168.0.2	80	192.168.0.11	56681	ESTABLISH 418f0f4
192.168.0.2	80	192.168.0.11	56620	TIMEWAIT 418f108
192.168.0.2	80	192.168.0.11	49773	TIMEWAIT 418f11c
192.168.0.2	80	192.168.0.11	61337	TIMEWAIT 418f130
192.168.0.2	80	192.168.0.11	56387	TIMEWAIT 418f144
192.168.0.2	80	192.168.0.11	58584	TIMEWAIT 418f158

图 122 显示 TCP 连接信息

LocalAddress

描述：TCP 连接的本地地址。

LocalPort

描述：TCP 连接的本地端口号。

ForeignAddress

描述：TCP 连接的对端地址。

ForeignPort

描述：TCP 连接的对端端口号。

State

描述：TCP 连接当前状态。

8、显示当前与交换机建立的 UDP 连接情况

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示 UDP 连接信息]菜单进入 UDP 连接信息显示界面，如图 123 所示；

状态信息窗口

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	0	0.0.0.0	0	(null)

图 123 显示 UDP 连接信息

LocalAddress

描述：UDP 连接的本地地址。

LocalPort

描述：UDP 连接的本地端口号。

ForeignAddress

描述：UDP 连接的对端地址。

ForeignPort

描述：UDP 连接的对端端口号。

State

描述：UDP 连接当前状态。

9、显示在线用户

点击导航树[设备基本配置]→[基本配置维护和调试信息]→[显示已登录的用户]菜单进入在线用户显示界面，如图 124 所示；

反馈信息窗口

No.	Name	Level	Login	Authen	IP Address	Time(min)
1	admin	admin	web	local	192.168.0.11	341

图 124 在线用户

6 设备高级配置

6.1 ARP 配置

6.1.1 介绍

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

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

6.1.2 说明

ARP 表项分为动态 ARP 表项和静态 ARP 表项。

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

静态表项通过手动配置和维护，不会被老化，不会被动态 ARP 表项覆盖。

ARP 表项最多支持 8192 条，当 ARP 表项超过 8192 条时，新表项将覆盖旧动态表项。

6.1.3 代理 ARP

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

代理 ARP 的过程如下：

1、源主机向另一物理网络的主机发 ARP 请求；

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

3、源主机向目的主机发送的 IP 报文都发给了使能代理 ARP 的设备；

4、网关对报文做正常的 IP 路由转发；

5、发往目的主机的 IP 报文通过网络，最终到达目的主机。

注意：

匹配缺省路由的 ARP 请求不进行代理。

6.1.4 Web 页面配置

1、添加或删除静态 ARP 表项

点击导航树[设备高级配置]→[ARP 配置]→[ARP 配置]菜单进入 ARP 配置界面，如图 125 所示；

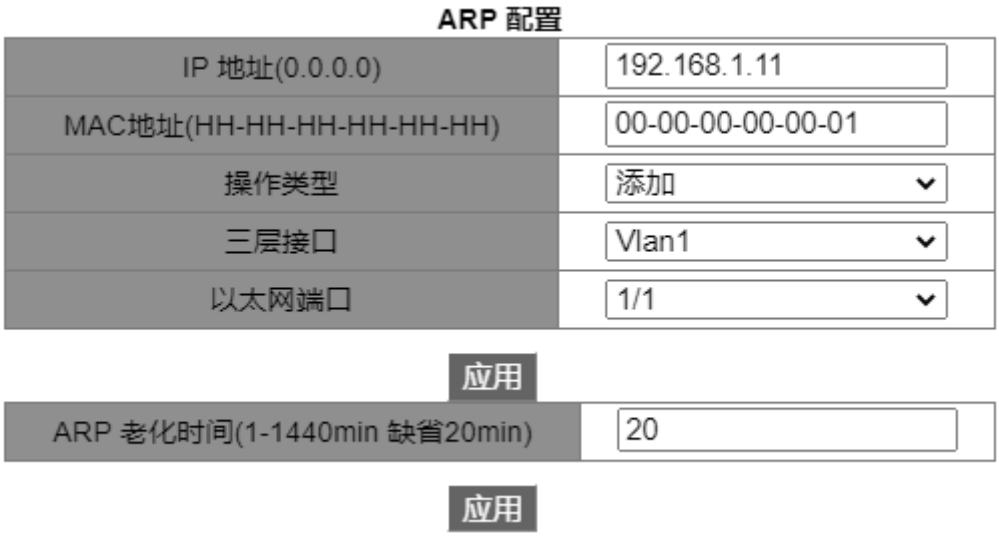


图 125 静态配置 ARP 表项

IP 地址

配置格式：A.B.C.D

功能：配置静态 ARP 表项的 IP 地址。

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH (H 为一个十六进制数)

功能：配置静态 ARP 表项的 MAC 地址。

操作类型

配置选项：添加/删除

默认配置：添加

功能：选择当前 ARP 表项的操作。

三层接口

配置选项：已创建的三层 VLAN 接口

默认配置：VLAN1

功能：选择当前 ARP 表项的三层 VLAN 接口。

以太网端口

配置选项：指定 VLAN 中的所有端口

功能：选择当前 ARP 表项对应的转发端口。

ARP 老化时间

配置范围：1 ~ 1440min

默认配置：20min

功能：配置 ARP 老化时间。

描述：ARP 老化时间从一个动态 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。

注意：

- 静态配置 ARP 表项时，静态绑定 IP 地址不能是交换机本身的 IP 地址；
- 不同的 IP 地址可以绑定相同的 MAC 地址；
- 一条 ARP 表项在某一 VLAN 中只能对应一个转发端口；
- 一般情况下，交换机自动学习 ARP 表项，不需管理员配置静态表项。

2、查看 ARP 地址表项

点击导航树[设备高级配置]→[ARP 配置]→[ARP 显示]菜单进入 ARP 显示界面，如图 126 所示；

ARP列表

IP 地址	MAC地址	三层接口	以太网端口	类型
192.168.0.11	00-0e-c6-6b-21-06	Vlan1	1/11	dynamic

刷新

图 126 ARP 列表

ARP 列表

组合显示：{IP 地址，MAC 地址，三层接口，以太网端口，类型}

功能：显示 ARP 表项。

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

3、清空 ARP 缓存

点击导航树[设备高级配置]→[ARP 配置]→[清空 ARP 缓存]菜单进入 ARP 缓存清空界面，如图 127 所示；

图 127 清空 ARP 缓存

点击<应用>按钮，可清空缓存中的动态 ARP 表项。

4、使能代理 ARP

点击导航树[设备高级配置]→[ARP 配置]→[配置代理 ARP]菜单进入代理 ARP 配置界面，如图 128 所示；

图 128 配置代理 ARP

三层 VLAN 接口

功能：选择使能代理 ARP 功能的三层接口。

6.1.5 典型配置举例

如图 129 所示，PC1、PC2 和 PC3 属于同一网段主机，分别属于 VLAN1、VLAN2、VLAN4 不同的子网。

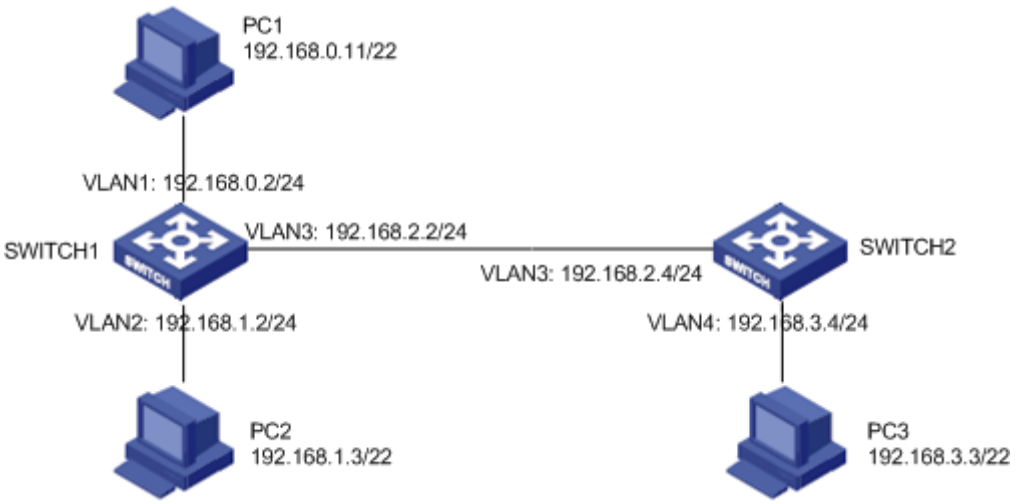


图 129 代理 ARP 配置举例

PC1 以广播方式发 ARP 请求，请求 PC2、PC3 的 MAC 地址。

- 当 SWITCH1 的 VLAN1 接口代理 ARP 功能未使能时，由于他们处于不同的 VLAN，因此 ARP 请求不能到达 PC2、PC3，双方无法通信；
- 当 SWITCH1 的 VLAN1 接口代理 ARP 功能使能时，VLAN1 接口收到 ARP 请求后，通过查找路由表项，发现存在到达 PC2、PC3 的路由，则 SWITCH1 使用 VLAN1 接口的 MAC 地址发送 ARP 应答消息（应答报文中的源 IP 地址是 PC2、PC3 的 IP 地址）。PC1 收到应答报文后建立 ARP 表项，后续 PC1 发往 PC2、PC3 的 IP 报文都发送到 SWITCH1 的 VLAN1 接口，然后由 SWITCH1 进行转发。

6.2 三层接口配置

6.2.1 查看交换机 IP 地址

Console 口访问交换机登录到命令行界面时，输入“enable”从一般用户配置模式切换到特权用户配置模式，输入命令”**show interface vlan 1**”可以查看交换机 IP 地址，如图 130 中红色区域部分所示；

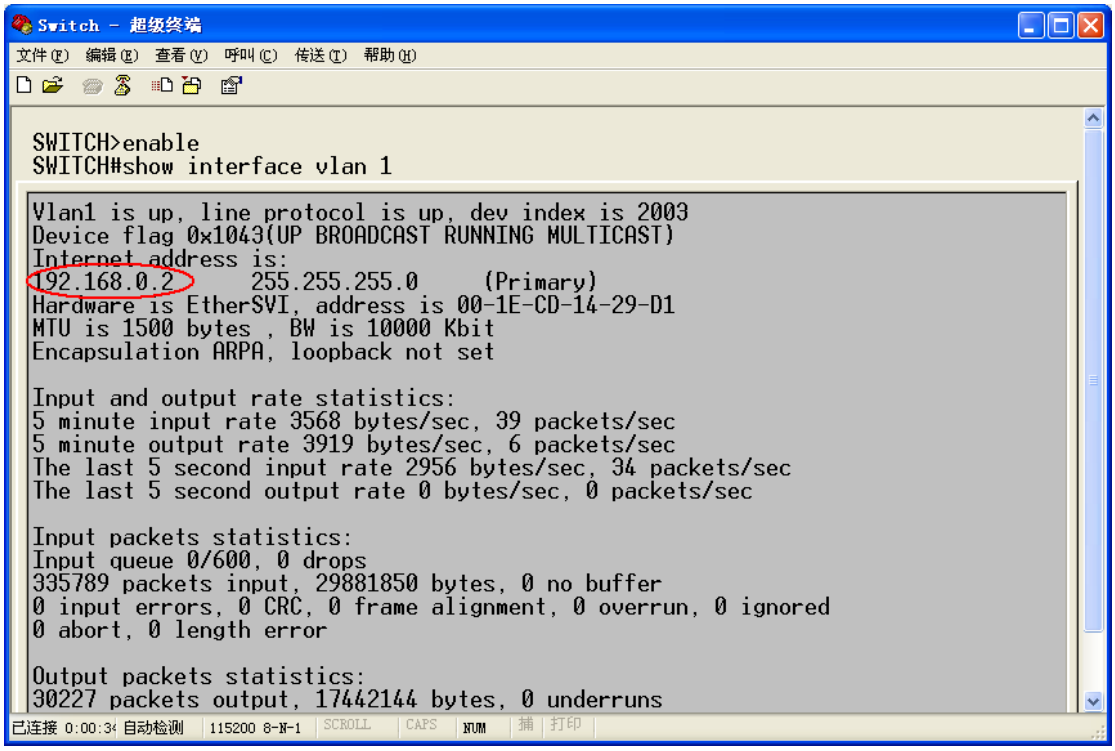


图 130 查看 IP 地址

6.2.2 IP 地址配置

1、创建三层 VLAN 接口

不同 VLAN 的主机之间不能直接通信，需要通过路由器或三层交换机等网络层设备进行转发，三层转发需要通过 VLAN 接口实现。

该系列交换机提供三层 VLAN 接口，VLAN 接口是一种三层模式下的虚拟接口，主要用于实现 VLAN 间的三层互通，不作为物理实体存在于设备上。每个 VLAN 都可以创建一个三层 VLAN 接口，该接口可以为本 VLAN 内端口收到的报文进行网络层转发。

点击导航树[设备高级配置]→[三层接口配置]→[创建一个 VLAN 接口]菜单进入 VLAN 接口创建界面，如图 131 所示；

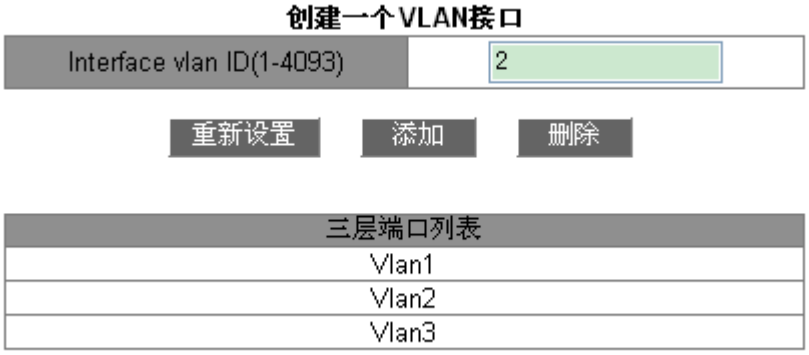


图 131 创建 VLAN 接口

Interface vlan ID

配置选项：已创建的 VLAN 号

默认配置：1

功能：创建三层 VLAN 接口。

说明：

- 最多可以创建 16 个三层 VLAN 接口；
- 在创建 VLAN 接口之前，必须保证对应的 VLAN 已经存在，否则不能创建指定的 VLAN 接口；
- 不能删除当前 Web 访问交换机使用的 IP 地址对应的 VLAN 接口。

2、获取 IP 地址方式

交换机的 IP 地址可以通过手动配置和自动获取两种方式来配置。

点击导航树[设备高级配置]→[三层接口配置]→[三层接口配置 IP 地址方式]菜单进入获取 IP 地址配置界面，如图 132 所示；

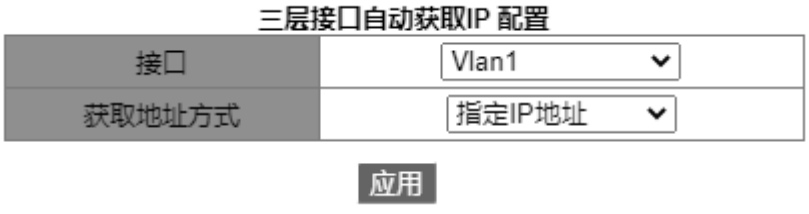


图 132 获取 IP 地址方式

接口

配置选项：已创建的三层 VLAN 接口

默认配置：VLAN 1

获取地址方式

配置选项：bootp-client/dhcp-client/指定 IP 地址

默认配置：指定 IP 配置

功能：选择获取 IP 地址的方式。

描述：指定 IP 地址使用手工配置 IP 地址；bootp-client/dhcp-client 指交换机通过 DHCP/BootP 协议自动获取 IP 地址，此时网络中应存在 DHCP/BootP Server 为客户端分配 IP 地址。DHCP/BootP Server 配置请参考”6.12 DHCP 配置”。

3、手工配置 IP 地址

点击导航树[设备高级配置]→[三层接口配置]→[三层接口指定 IP 地址配置]菜单进入指定 IP 地址配置界面，如图 133 所示；

图 133 指定 IP 地址配置

IP 地址

配置格式：A.B.C.D

功能：配置指定三层接口的 IP 地址。

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。

状态

配置选项：no shutdown/ shutdown

默认配置：no shutdown

功能：配置三层 VLAN 接口状态。

描述：no shutdown 表示打开当前三层 VLAN 接口；shutdown 表示关闭该三层 VLAN 接

口。

类型

配置选项：secondary/primary

默认配置：primary

功能：在同一端口中，可以设置两个以上的不同的网段 IP 地址，这样可以实现连接在同一局域网上不同的网段之间的通讯。一般由于一个网段对于用户来说不够用，可以采用这种方法。

描述：secondary IP 可以解决 RIP v1 中的路由汇总的问题，可以用于 NAT,转换后地址并非路由器直连地址。

点击<添加>配置该 VLAN 接口的 IP 地址；点击<删除>可删除当前 IP 地址，删除 primary IP 地址前，应先删除 secondary IP 地址；

注意：

- 每个三层 VLAN 接口下最多可以配置 32 个 IP 地址；
- 每个 VLAN 接口下可以配置同一网段或不同网段的 IP 地址；
- 不同 VLAN 接口下应配置不同网段的 IP 地址；

6.3 SNMPv2c

6.3.1 介绍

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

6.3.2 实现

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

- NMS(Network Management Station，网络管理站)是运行支持SNMP协议的网管软件客户端程序的工作站，在SNMP网络管理中起核心作用。
- Agent 是驻留在被管理网络设备的一个进程，负责接收、处理来自NMS 的请求报文。

有告警发生时，Agent也会主动通知NMS。

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

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

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

6.3.3 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，则请求失败并返回错误。

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。

6.3.4 MIB 介绍

任何一个被管理资源都表示成一个对象，称为被管理对象。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 134所示：

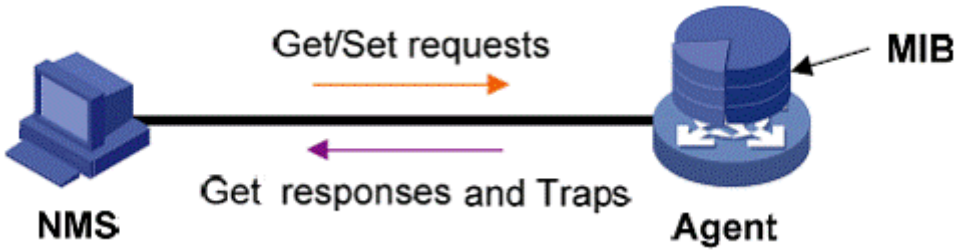


图 134 NMS、Agent 和 MIB 关系图

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 135 所示，被管理对象 A 的 OID 为 1.2.1.1。

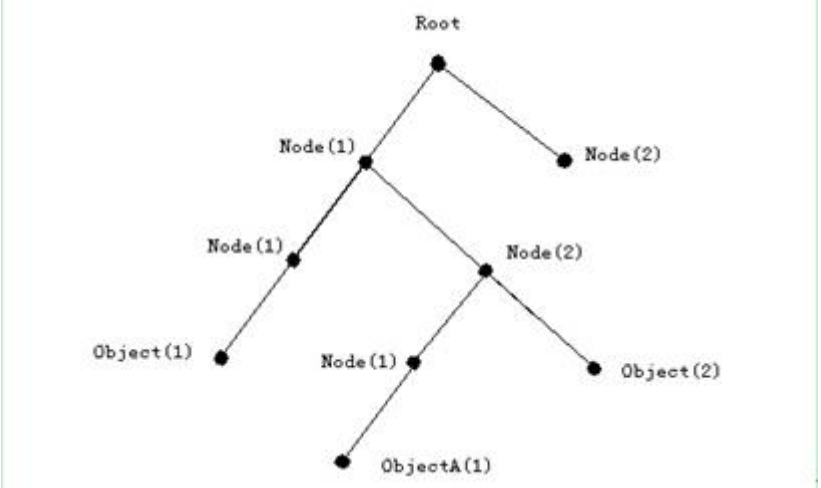


图 135 MIB 树结构

6.3.5 Web 页面配置

1、配置 SNMP v2

点击导航树[设备高级配置]→[SNMP 配置]→[SNMP 基本配置]菜单进入 SNMP v2 配置界面，如图 136 所示；

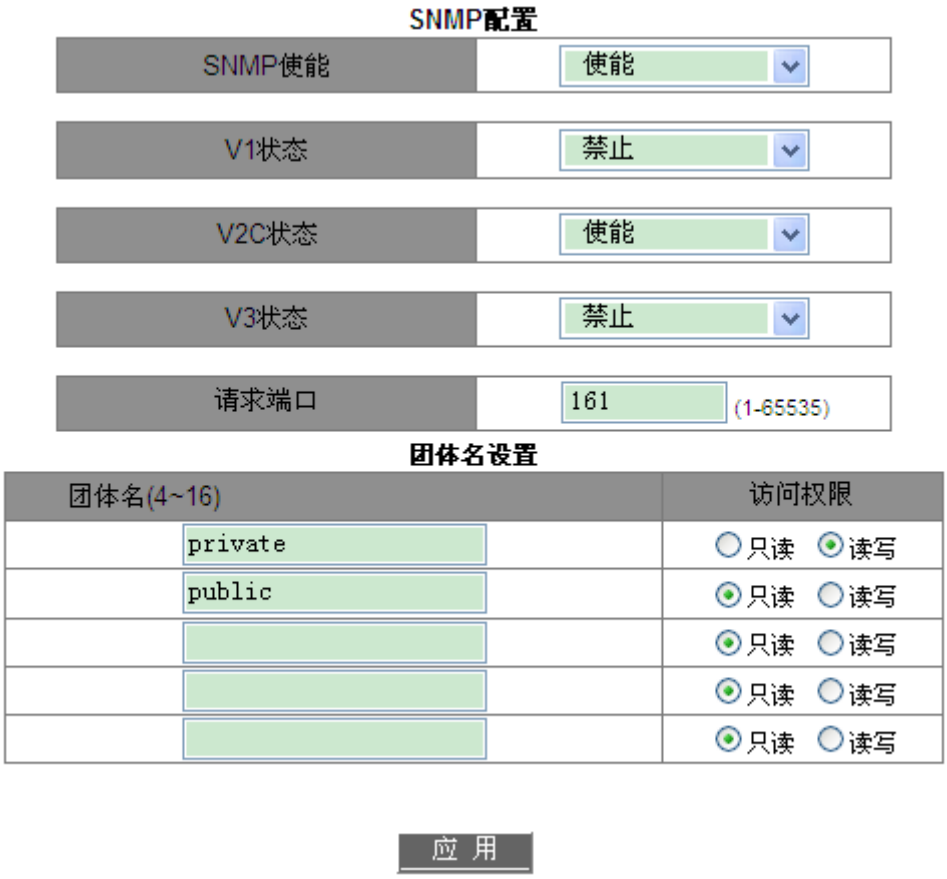


图 136 SNMP v2c 配置

SNMP 使能

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 SNMP 协议。

V1/V2C/V3 状态

配置选项：使能/禁止

功能：选择 SNMP 的版本号。

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。

团体名

配置范围：4~16 个字符

功能：配置交换机的团体名。

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

说明：最多可以配置 5 个团体字符串。

访问权限

配置选项：只读/读写

默认配置：只读

功能：配置 MIB 库的访问方式。

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

2、配置安全 IP 地址

点击导航树[设备高级配置]→[SNMP 配置]→[管理方 IP 地址设置]菜单进入安全 IP 地址配置界面，如图 137 所示；

图 137 安全 IP 地址配置

安全 IP 检查

配置选项：使能/禁止

默认配置：禁止

功能：是否使能安全 IP 地址检查，使能时需要配置下面的 NMS IP 地址，并且只有安全 IP 地址的 NMS 可以访问交换机 MIB 库信息。不使能时，不需要配置下面的 NMS IP 地址，连接成功的 NMS 都可以访问交换机 MIB 库信息。

IP 地址

配置格式：A.B.C.D

功能：配置 NMS 管理站的安全 IP 地址。

描述：只有安全 IP 地址的 NMS 管理站才能访问交换机 MIB 库信息。最多可以配置 6 个安全管理方 IP 地址。

3、配置 Trap

点击导航树[设备高级配置]→[SNMP 配置]→[TRAP 配置]菜单进入 Trap 配置界面，如图 138 所示；

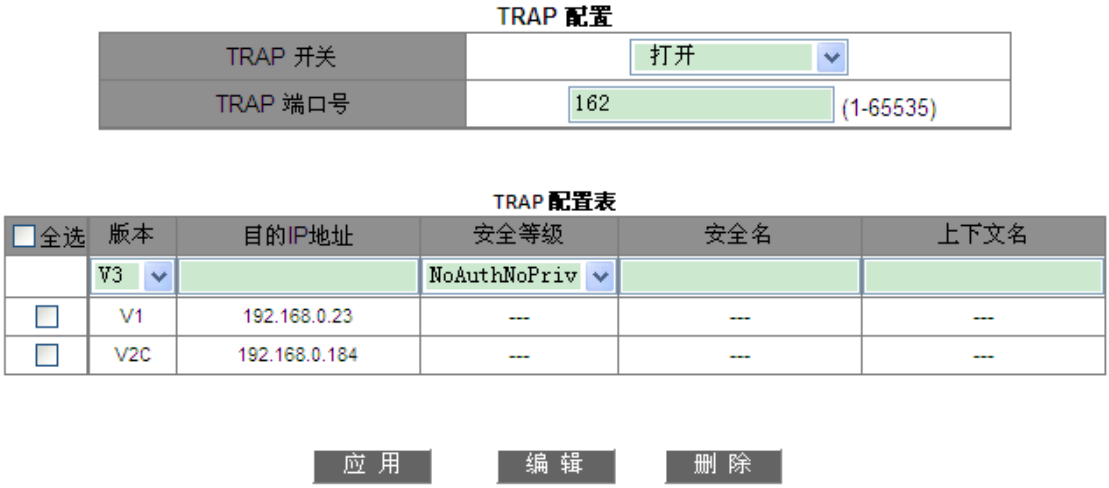


图 138 Trap 使能

TRAP 开关

配置选项：打开/关闭

默认配置：关闭

功能：是否允许交换机发送 Trap 消息。

TRAP 端口号

配置范围：1~65535

默认配置：162

功能：发送 trap 报文消息的端口号。

版本

配置选项：V1/V2C/V3

功能：V1/V2C 表示交换机向服务器发送 V1/V2C 版本的 trap 报文；V3 表示交换机向服

务器发送 V3 版本的 trap 报文。选择 V1、V2C 版本时，只需配置目的 IP 地址即可。

目的 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 8 个 Trap 服务器地址，即最多可配置 8 条 trap 表项。

4、查看 SNMP 统计信息

点击导航树[设备高级配置]→[SNMP 配置]→[SNMP 统计信息]菜单进入 SNMP 统计信息界面，如图 139 所示；

SNMP 统计信息	number
输入的snmp报文	37
版本信息错误的报文数目	0
收到的getnext请求的报文	4
收到的set请求的报文	2
输出的snmp报文	20
收到too_big错误的snmp报文	0
Snmp报文的最大长度	1500
不存在的MIB对象进行请求的报文	0
bad_values错误的snmp报文	0
general_errors错误的snmp报文	0
发送的响应报文	12
发送的trap报文	8
Nms SET 请求包数	2
团体名错误的报文数目	0
团体名对应的权限错误的报文	6
编码错误的snmp报文	0

显示最新统计

图 139 SNMP 统计信息

6.3.6 典型配置举例

SNMP 管理站与交换机通过以太网相连，管理站 IP 地址为 192.168.0.23，交换机 IP 地址为 192.168.0.2。NMS 通过 SNMPv2c 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 140 所示；

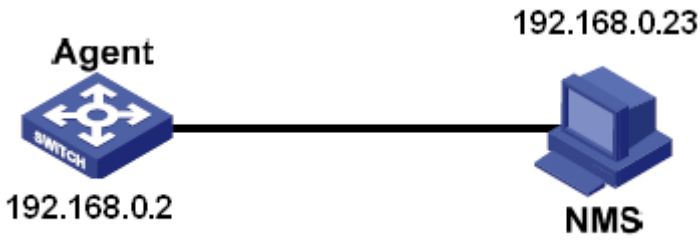


图 140 SNMPv2c 配置举例

Agent 配置过程：

1、使能 SNMP 协议和 V2C 状态；配置访问权限，只读团体名为 public，读写团体名为 private；见图 136；

2、配置安全 IP 地址为 192.168.0.23，见图 137；

3、使能 Trap 状态，版本选择 V2C，服务器地址为 192.168.0.23，见图 138；

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”。

6.4 SNMP v3

6.4.1 介绍

SNMP v3 提供了基于用户的安全模型(USM，User-Based Security Model)的认证机制。用户可以配置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免窃听。通过有无认证和有无加密等功能组合，可以为 SNMP NMS 和 SNMP Agent 之间的通信提供更高的安全性。

6.4.2 实现

SNMPv3 中有 5 个配置表，每个表中可以配置 16 条表项，这些表共同决定了基于上下文组中的特定用户是否可以访问 MIB 信息。

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

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

上下文表是标识用户的可读字符串，与具体的安全模型无关。

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

访问表通过匹配组名和上下文名，通过相应的安全模式和安全等级来访问 MIB 信息。

6.4.3 Web 页面配置

1、配置用户表

点击导航树[设备高级配置]→[SNMP 配置]→[V3 用户表配置]菜单进入 SNMP v3 用户表配置界面，如图 141 所示；

图 141 SNMP v3 用户表配置

用户名

配置范围：4~16 个字符

功能：创建的用户名。

鉴定加密协议

配置选项：NONE/HMAC-MD5/HMAC-SHA

默认配置：NONE

功能：选择一种鉴定加密协议。

鉴定加密密码

配置范围：4~16 个字符

功能：创建鉴定加密密码。

报文加密协议

配置选项：NONE/HMAC-DES

默认配置：NONE

功能：选择一种报文加密协议。

报文加密密码

配置范围：4~16 个字符

功能：创建报文加密密码。

2、配置组表

点击导航树[设备高级配置]→[SNMP 配置]→[V3 组表配置]菜单进入 SNMP v3 组表配置界面，如图 142 所示；

图 142 SNMP v3 组表配置

组名

配置范围：4~16 个字符

功能：配置组表的名称。

安全名

配置范围：已创建的用户名，4~16 个字符

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

安全模式

默认配置：SNMPv3

描述：SNMPv3 表示采用的 USM(基于用户的安全模型)技术，目前该选项强制为 SNMPv3 模式。

3、配置上下文表

点击导航树[设备高级配置]→[SNMP 配置]→[V3 上下文表配置]菜单进入 SNMP v3 上下文表配置界面，如图 143 所示；

图 143 SNMP v3 上下文表配置

上下文名

配置范围：4~16 个字符

功能：配置上下文名。

说明：第一条上下文名强制为空。

4、配置视图表

点击导航树[设备高级配置]→[SNMP 配置]→[V3 视图表配置]菜单进入 SNMP v3 视图表配置界面，如图 144 所示；

V3视图表配置

序号	视图名	类型	oid-tree	子树掩码
1	view1	included	1.3.6.1.2.1.1.1	0xfd,0xff,0xff,0xff
2	view2	excluded	1.3.6.1.2.1.1.1	0xff,0xff,0xff,0xff
3	view-no	excluded	1	0xff,0xff,0xff,0xff
4	view-all	included	1	0xff,0xff,0xff,0xff
5		included		
6		included		
7		included		
8		included		
9		included		
10		included		
11		included		
12		included		
13		included		
14		included		
15		included		
16		included		

应用

图 144 SNMPv3 视图表配置

视图名

配置范围：4~16 个字符

功能：配置视图名。

类型

配置选项：included/excluded

默认配置：included

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

oid-tree

功能：MIB 子树，用子树根节点的 OID 表示。

子树掩码

功能：MIB 子树掩码。Oid-tree 和 mask 共同决定当前视图的 MIB 节点信息。

例如：图 144 中视图名 view1 只能访问 1.3.6.1.2.1.1.1、1.3.6.1.2.1.2.1、1.3.6.1.2.1.3.1、1.3.6.1.2.1.4.1……1.3.6.1.2.1.n.1 节点信息。

5、配置访问表

点击导航树[设备高级配置]→[SNMP 配置]→[V3 访问表]菜单进入 SNMP v3 访问表配置界面，如图 145 所示；

V3访问表

序号	组名	上下文名	上下文匹配方式	安全模式	安全等级	读视图	写视图	通告视图
1			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
2			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
3			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
4			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
5			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
6			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
7			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
8			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
9			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
10			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
11			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
12			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
13			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
14			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
15			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
16			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1

应用

图 145 SNMPv3 访问表配置

组名

配置范围：已创建的组名，4~16 个字符

功能：该组中的所有用户具有相同的访问权限。

上下文名

配置范围：已创建的上下文名，4~16 个字符

功能：配置上下文名，组名和上下文名共同决定一组访问权限。上下文表中第一条上下文名强制为空，所以上下文名可以为空。

上下文匹配方式

配置选项：exact/prefix

默认配置：exact

功能：选择上下文名的匹配方式。Exact 全部匹配，指上下文名应与上下文表中上下文名配置一致；prefix 前缀匹配，指上下文名配置为上下文表中上下文名的前 4~16 个字符，此时前缀相同的上下文名具有相同的访问权限。

安全模式

默认配置：SNMP V3

描述：SNMP V3 表示采用的 USM(基于用户的安全模型)技术，目前该选项强制为 SNMPv3 模式。

安全等级

配置选项：NoAuthNoPriv/AuthNoPriv/AuthPriv

默认配置：NoAuthNoPriv

功能：选择访问 MIB 信息的访问权限。

描述：NoAuthNoPriv 既不需要鉴定加密也不需要报文加密；AuthNoPriv 需要鉴定加密但不需要报文加密；AuthPriv 既需要鉴定加密也需要报文加密。需要加密时，网管软件中的加密算法、加密密码应与用户表中的配置并保持一致，才能成功访问交换机相应节点信息。

读视图

配置选项：view1/view2/view-no/view-all

默认配置：view1

功能：选择只读视图名。

写视图

配置选项：view1/view2/view-no/view-all

view1

功能：选择写视图名。

通告视图

配置选项：view1/view2/view-no/view-all

view1

功能：选择可以发 Trap 消息的视图名。

6、配置安全 IP 地址

点击导航树[设备高级配置]→[SNMP 配置]→[管理方 IP 地址设置]菜单进入安全 IP 地址配置界面，如图 146 所示；

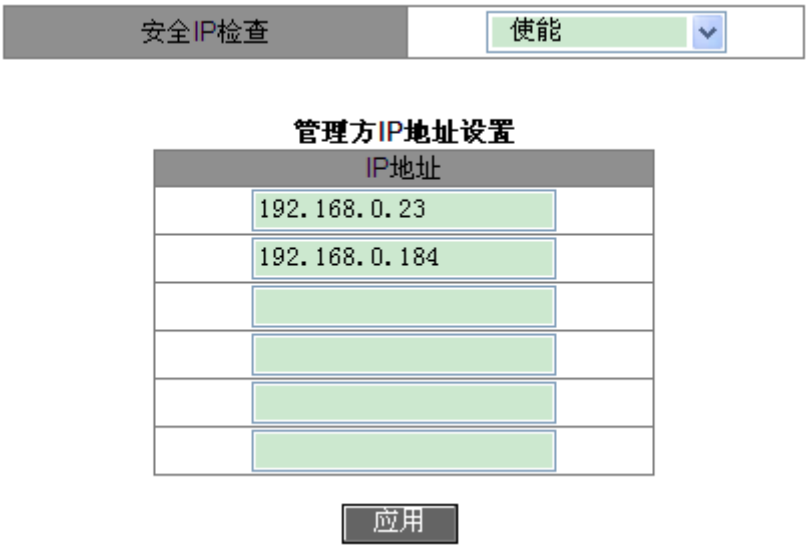


图 146 安全 IP 地址配置

安全 IP 检查

配置选项：使能/禁止

默认配置：禁止

功能：是否使能安全 IP 地址检查，使能时需要配置下面的服务器 IP 地址，并且只有安全 IP 地址的服务器可以访问交换机 MIB 库信息。不使能时，不需要配置下面的服务器 IP 地址，连接成功的服务器都可以访问交换机 MIB 库信息。

IP 地址

配置格式：A.B.C.D

功能：配置 NMS 管理站的安全 IP 地址。

描述：只有安全 IP 地址的 NMS 管理站才能访问交换机 MIB 库信息。最多可以配置 6 个安全管理方 IP 地址。

7、配置 Trap

点击导航树[设备高级配置]→[SNMP 配置]→[TRAP 配置]菜单进入 Trap 配置界面，如图 147 所示；

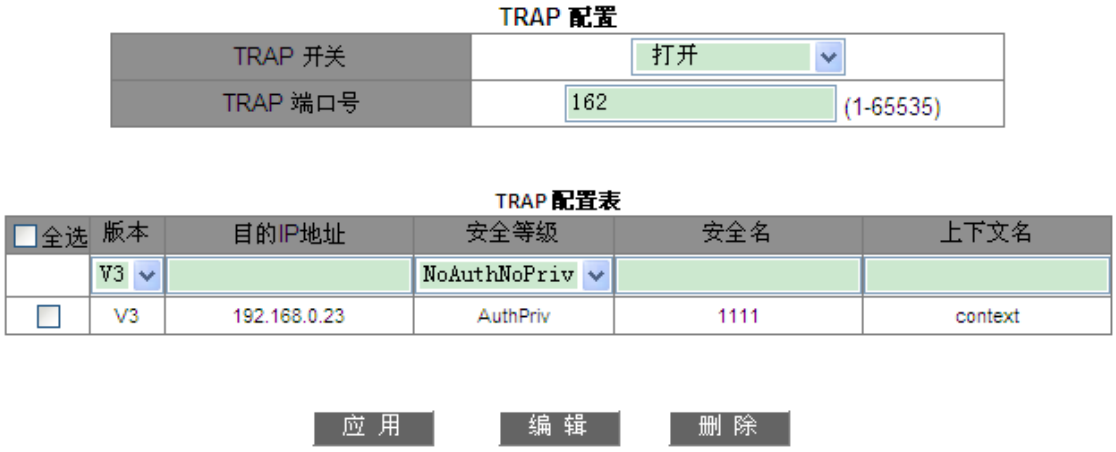


图 147 SNMP v3 Trap 配置

TRAP 开关

配置选项：打开/关闭

默认配置：关闭

功能：是否允许交换机发送 trap 消息。

TRAP 端口号

配置范围：1~65535

默认配置：162

功能：发送 trap 报文消息的端口号。

版本

配置选项：V1/V2C/V3

功能：V1/V2C 表示交换机向服务器发送 V1/V2C 版本的 trap 报文；V3 表示交换机向服务器发送 V3 版本的 trap 报文。

目的 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 8 个 Trap 服务器地址，即最多可配置 8 条 trap 表项。

{安全等级，安全名，上下文名}

配置选项：{NoAuthNoPriv/AuthNoPriv/AuthPriv，4~16 个字符，4~16 个字符}

功能：该三项只有发送 V3 版本 trap 报文时需要配置。该配置应与访问表中的相应配置保持一致，其中安全等级可以等于或高于访问表中的安全等级。例如用户 1111 的访问权限为

AuthNoPriv，则安全名 1111 的安全等级为 AuthNoPriv 或 AuthPriv 时可以向服务器发送 trap 报文。上下文名和访问表中的 Context Prefix 匹配一致即可。

6.4.4 典型配置举例

SNMP 管理站与交换机通过以太网相连，管理站 IP 地址为 192.168.0.23，交换机 IP 地址为 192.168.0.2。用户 1111 和用户 2222 通过 SNMPv3 对 Agent 进行监控管理，安全等级采用 AuthNoPriv，可以对 Agent 中所有节点信息进行只读操作；agent 有告警时主动向 NMS 发送 trap v3 报文，如图 148 所示；

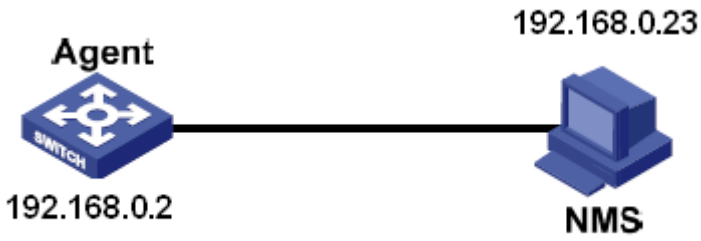


图 148 SNMPv3 配置举例

Agent 配置如下：

1、配置 SNMPv3 用户表，用户名：1111，鉴定加密：HMAC-MD5，鉴定加密密码：aaaa，报文加密协议：HMAC-DES，报文加密密码：xxxx；用户名：2222，鉴定加密：HMAC-SHA，鉴定加密密码：bbbb，报文加密协议：HMAC-DES，报文加密密码：yyyy；见图 141；

2、创建 group 组，包含用户 1111 和 2222，见图 142；

3、创建上下文表，上下文名：context，见图 143；

4、创建视图 view-all 包括所有节点，view-no 不包含任何节点，见图 144；

5、配置 SNMPv3 访问表，组名：group，上下文名：context，上下文匹配方式：全部匹配，安全等级：AuthNoPriv，读视图：view-all，写视图：view-no，通告视图：view-all，见图 145；

6、使能 Trap，端口号为 162。 配置 trap 表项，版本：V3，目的 IP 地址：192.168.0.23，安全等级：AuthPriv，安全名：1111，上下文名：context，见图 147；

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。

6.5 DT-Ring

6.5.1 介绍

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

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

DT-Ring-Port：针对某个具体的端口转发或阻塞报文；

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

DT-Ring-Port 和 DT-Ring-VLAN 不能混合使用。

6.5.2 概念

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

说明：

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

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

备份端口：DT-Ring 环与环之间的通信端口。

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

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

Forwarding 状态：端口可以接收、发送数据。

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

6.5.3 实现

DT-Ring-Port 实现

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

A、B、C、D 交换机的工作过程：

1、配置交换机 A 为主站，其余交换机均为从站；

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

3、若 CD 链路发生故障，如图 149 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。

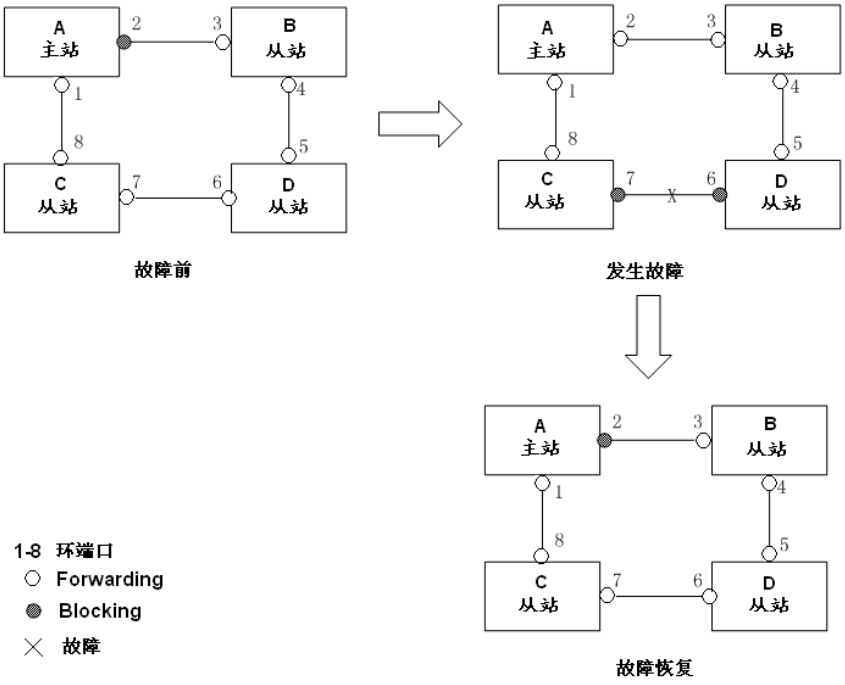


图 149 CD 链路发生故障

4、若 AC 链路发生故障，如图 150 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，仍保持端口 1 为 Blocking 状态，端口 8 为 Forwarding 状态，链路不进行倒换。

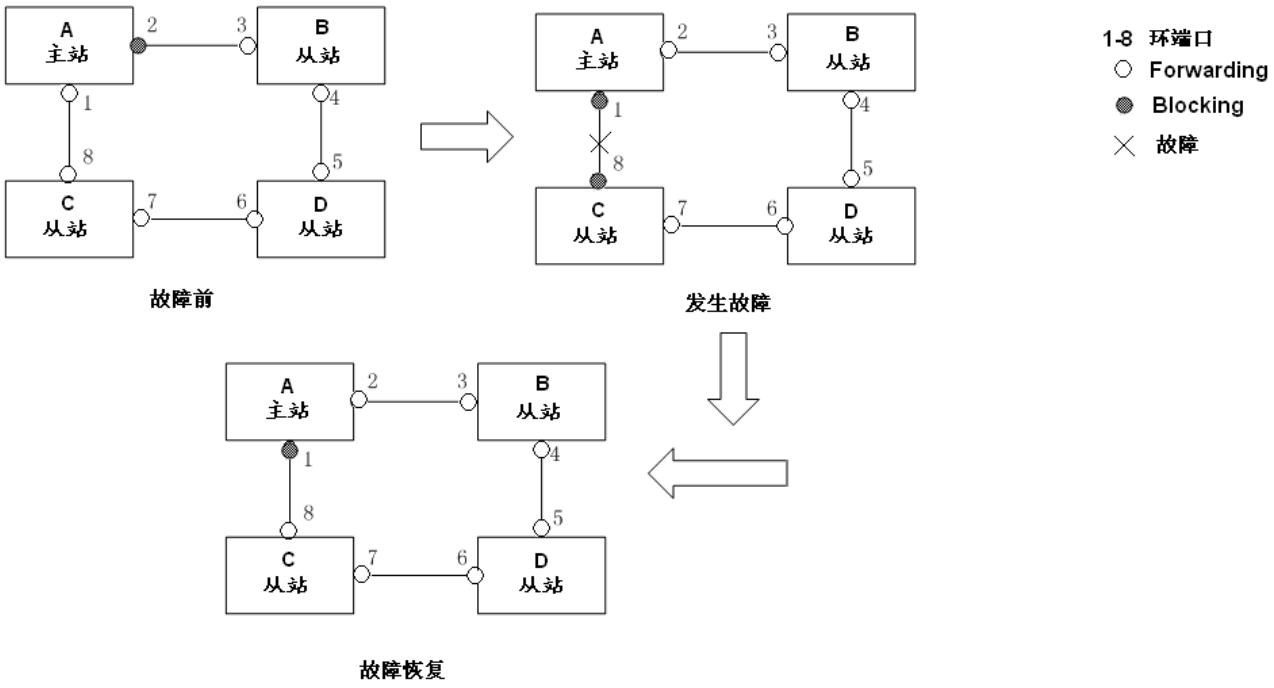


图 150 DT-Ring 链路故障

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 151 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。

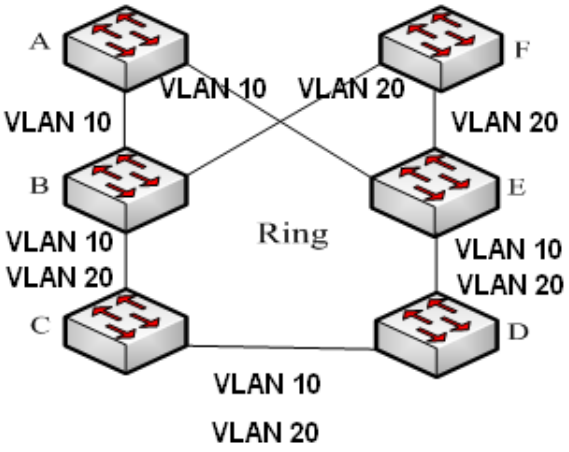


图 151 DT-Ring-VLAN

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 152 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。

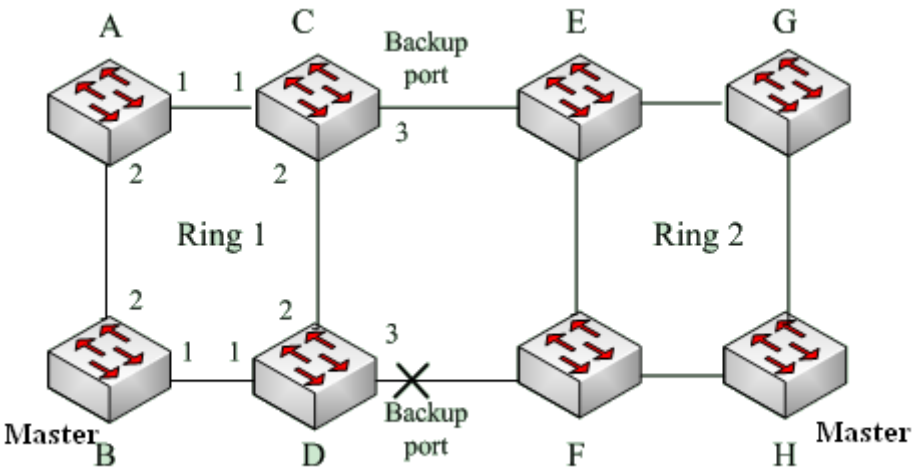


图 152 DT-Ring+拓扑

注意：

链路状态的改变影响备份端口的状态。

6.5.4 说明

DT-Ring 配置应满足以下条件：

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

6.5.5 Web 页面配置

1、配置冗余环模式

点击导航树[设备高级配置]→[DT-Ring 配置]→[DT-Ring 模式]菜单进入环模式配置界面，如图 153 所示；

图 153 冗余环模式配置

冗余环模式配置

配置选项：Disable/DT-PORT/DT-VLAN

默认配置：Disable

功能：是否使能 DT-Ring 协议并选择冗余环的模式。

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

2、创建 DT-Ring 环

点击导航树[设备高级配置]→[DT-Ring 配置]→[DT-Ring 配置]菜单进入环创建界面，如图 154 所示；

图 154 创建 DT-Ring

点击<添加>按钮创建 DT-Ring 并对其进行配置。

3、配置 DT-Ring 和 DT-VLAN-Ring，如图 155、图 156 所示；

图 155 DT-Ring 配置

图 156 DT-VLAN-Ring 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、备份端口与镜像目的端口配置互斥，DT-Ring 环端口和备份端口不能配置为镜像目的端口；镜像目的端口也不能配置为 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；
- 建议不要将同一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、备份端口不要加入同一隔离组中。

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：选择当前环端口允许通过的 VLAN 列表。

配置完成后，“DT-Ring 列表”中显示已创建的环列表，如图 157 所示；

图 157 DT-Ring 列表

4、查看、修改 DT-Ring 环配置

点击图 157 中相应 DT-Ring 选项，可以查看该环配置，并对其进行修改如图 158 所示；

图 158 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。

5、显示 DT-Ring 环状态和各端口状态，如图 159 所示；

图 159 DT-Ring 状态查看

6.5.6 典型配置举例

如图 152 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 155；

交换机 B 配置过程：

2、域 ID：1；域名称：Ring；环端口选择 1 和 2；站类型：主站；DT-Ring+不使能，不需配置备份端口，见图 155；

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 155；

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 155；

交换机 H 配置过程：

5、域 ID：2；域名称：Ring；环端口选择 1 和 2；站类型：主站；DT-Ring+不使能，不需配置备份端口，见图 155；

6.6 STP/RSTP

6.6.1 介绍

STP(Spanning Tree Protocol，生成树协议)是根据 IEEE 协会制定的 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 IEEE802.1w 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。

6.6.2 基本概念

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

根端口：从非根桥到根桥传输的最佳端口，即到根桥开销最小的端口。根端口负责与根桥进行通信，非根桥设备有且只有一个根端口，根桥设备没有根端口；

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

替换端口：根端口的备份端口，根端口发生故障后，替换端口将成为新的根端口；

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

6.6.3 BPDU 配置消息

为使通信链路不成环，局域网中所有网桥共同计算出一棵生成树。这个过程通过在设备之间传递 BPDU 报文来确定网络的拓扑结构，BPDU 报文的数据结构如表 8 所示；

表 8 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。

6.6.4 实现过程

各网桥使用 BPDU 报文计算生成树的具体过程：

1、初始状态

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

2、最优配置消息选择

各设备都向外发送自己的配置消息，同时也收到其他设备发送的配置消息。每个端口收到配置消息后跟本端口的配置消息比较：

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

设备将所有端口的配置消息进行比较，选出最优的配置消息。配置消息比较原则如下：

- 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。

6.6.5 Web 页面配置

1、全局使能 RSTP 协议

点击导航树[设备高级配置]→[RSTP 配置]→[RSTP 配置]菜单进入 RSTP 配置界面，如图 160 所示；

图 160 RSTP/STP 协议使能

协议状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 RSTP 协议。

注意：

- 基于端口的环协议包括 RSTP、DT-Ring-Port 和 DRP-Port，基于 VLAN 的环协议包括 MSTP、DT-Ring-VLAN 和 DRP-VLAN；
- 基于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 161 所示；

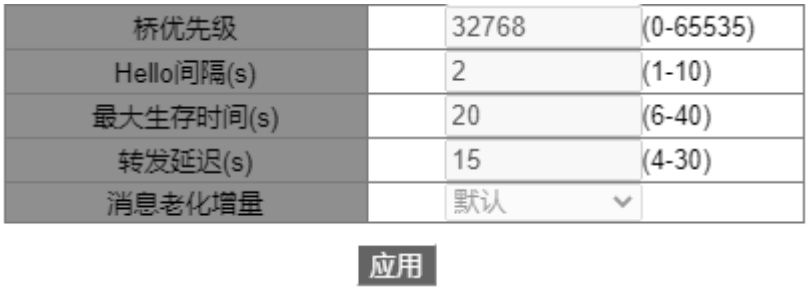


图 161 配置网桥时间参数

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。

Hello 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：6~40s

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：4~30s

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 162 所示；

图 162 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 端口与端口聚合互斥，RSTP 端口不能加入聚合组；加入聚合组的端口也不可以配置为 RSTP 端口；
- RSTP 端口与镜像目的端口配置互斥，RSTP 端口不能配置为镜像目的端口；镜像目的端口也不能配置为 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 DRP-Port/DT-Ring-Port 环端口、DRP-Port/DT-Ring-Port 备份端口；

DRP-Port/DT-Ring-Port 环端口、DRP-Por/DT-Ring-Portt 备份端口也不能配置为 RSTP 端口。

- 建议不要将同一隔离组中的端口同时配置为 RSTP 端口；RSTP 端口不要加入同一隔离组中。

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 163 所示；

根桥信息

根桥MAC	00:00:00:00:00:01
根桥优先级	32768
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	00:00:00:00:00:01
本桥优先级	32768
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
1/1	128	2000000	Disabled	Discarding	Down
1/2	128	2000000	Disabled	Discarding	Down
1/3	128	2000000	Disabled	Discarding	Down
1/4	128	2000000	Disabled	Discarding	Down

图 163 RSTP 状态信息

6.6.6 典型配置举例

交换机 A、B、C 的优先级分别为 0、4096、8192，各个链路的路径开销分别是 4、5、10，如图 164 所示；

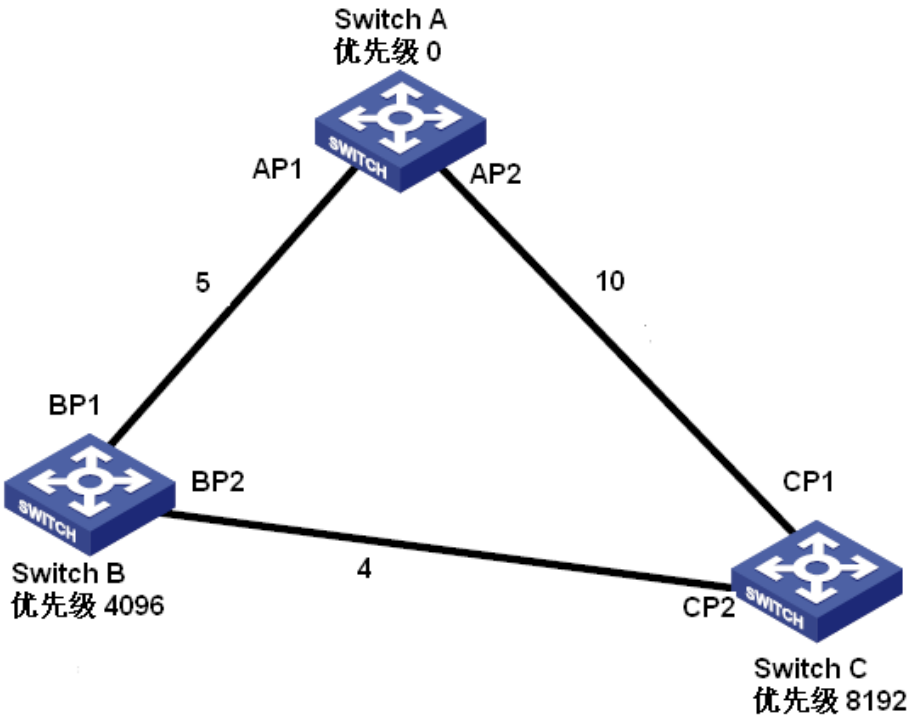


图 164 RSTP 举例

交换机 A 的配置：

1、优先级为 0，时间参数设为默认值，见图 161；

2、端口 1 的路径成本 5，端口 2 的路径成本 10，见图 162；

交换机 B 的配置：

1、优先级为 4096，时间参数设为默认值，见图 161；

2、端口 1 的路径成本 5，端口 2 的路径成本 4，见图 162；

交换机 C 的配置：

1、优先级为 8192，时间参数设为默认值，见图 161；

2、端口 1 的路径成本 10，端口 2 的路径成本 4，见图 162；

- 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；

6.7 DRP

6.7.1 介绍

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

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

- 与网络规模无关的故障恢复时间

通过对环网检测报文数据转发机制的优化，DRP 协议能够实现与网络规模无关的故障恢复时间，通过实时中断上报等机制的引入，DRP 的故障恢复时间能够达到 20ms 以内，从而大大提高实时报文传输时的可靠性，对电力、轨道交通等要求实时控制的应用领域提供更可靠的数据承载。

- 支持丰富的链路检测功能

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

- 支持多种网络拓扑

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

- 提供丰富的诊断维护功能

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

6.7.2 概念

1、DRP 模式

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

DRP-Port-Based：是针对某个具体的物理端口转发或阻塞报文；

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

2、DRP 端口状态

Forwarding 状态：即转发状态，端口可以接收、转发数据报文；

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

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

注意：

- 若 Root 中未配置主端口，环闭时首先 Link Up 的环端口处于 Forwarding 状态，后 Link Up 的环端口处于 Blocking 状态。
- Root 设备的 Blocking 端口可以主动发送 DRP 协议报文。

3、DRP 设备角色

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

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

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

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

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

说明：

CRC 劣化：15 分钟内 CRC 报文数超过门限值。

6.7.3 实现

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

Announce 报文携带的比较向量中包含了足够的信息来保证交换机角色的选举，其中包含的几个重要信息如表 9 所示：

表 9 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 9 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；在其余的交换机中，如果交换机有一个环端口处于 Link down 或者 CRC 劣化，则该设备角色为 B-Root，如果交换机两个环端口都为 Link up 且无 CRC 劣化，则该设备角色为 Normal。

交换机故障恢复过程如图 165 所示：

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

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

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

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

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

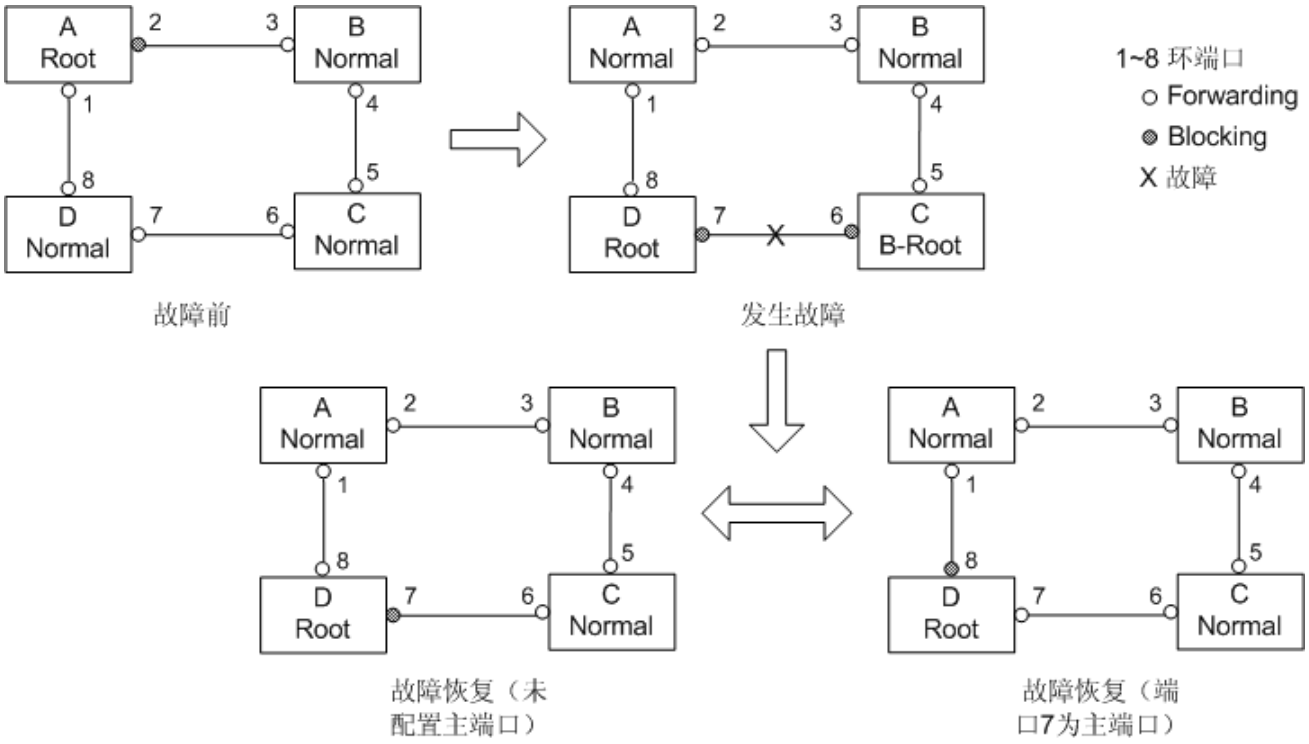


图 165 DRP 链路故障

说明：

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

1. DRP-VLAN-Based 实现

DRP-VLAN-Based 设置 VLAN 和 STG 实例的对应关系，把 VLAN 和 STG 实例联系起来。可以一个 VLAN 映射到一个 STG 实例；也可以多个 VLAN 映射到一个 STG 实例。

STG 实例：每个 STG 实例对应一个 DRP-VLAN-Based 环，通过 DRP 协议，STG 实例记录该环中设备角色及环端口状态。交换机接收到报文后，根据报文所属 VLAN 属性，确定 VLAN 所映射的 STG 实例，根据该实例中设备角色和端口状态对报文进行相应的处理。

通过配置 DRP-VLAN-Based 环可以使不同 VLAN 报文沿着不同路径进行转发。如图 166 所示，假设所有设备上 STG 实例和 VLAN 的映射关系都相同。

基于 STG1 的环链路：AB-BC-CD-DE-EA，VLAN10 和 VLAN20 按照该链路进行报文转发，A 为 Root。

基于 STG2 的环链路：FB-BC-CD-DE-EF，VLAN30 按照该链路进行报文转发，F 为 Root。

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。

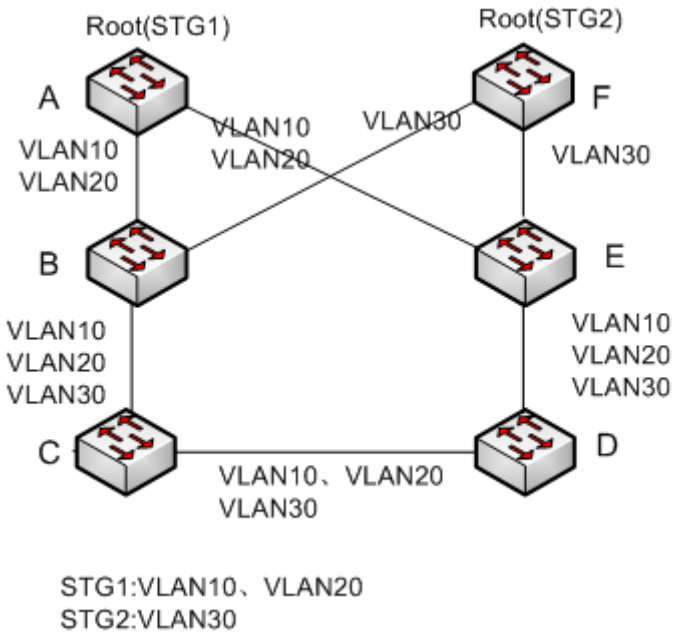


图 166 DRP-VLAN-Based

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。

2. 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 167 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。

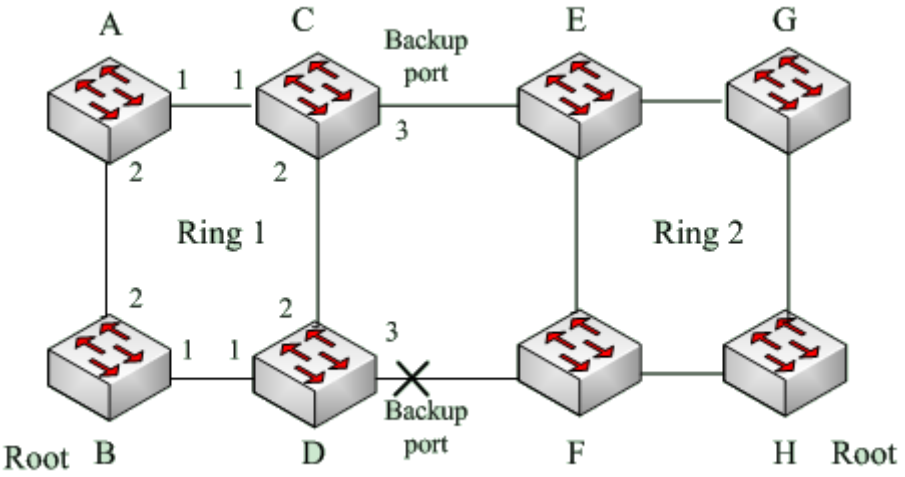


图 167 DRP 备份

注意：

链路状态的改变会影响备份端口的状态。

6.8 DHP

6.8.1 介绍

DHP(Dual Homing Protocol)：即双归链路协议，如图 168 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。

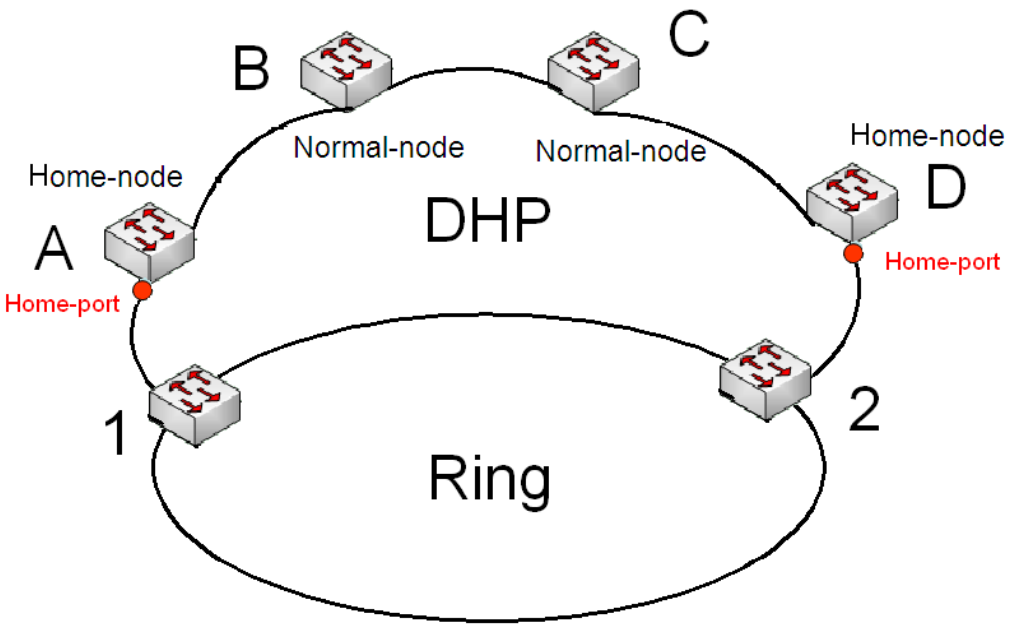


图 168 DHP 协议运用

6.8.2 概念

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

Home-node：双归链路两端边界设备，终结 DRP 协议报文。

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

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

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

6.8.3 实现

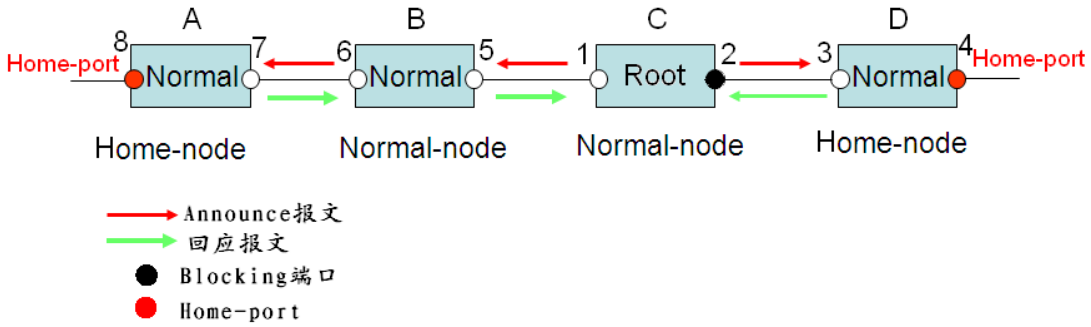


图 169 DHP 配置说明

图 168 中 A、B、C 和 D 的配置如图 169 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 170 所示。

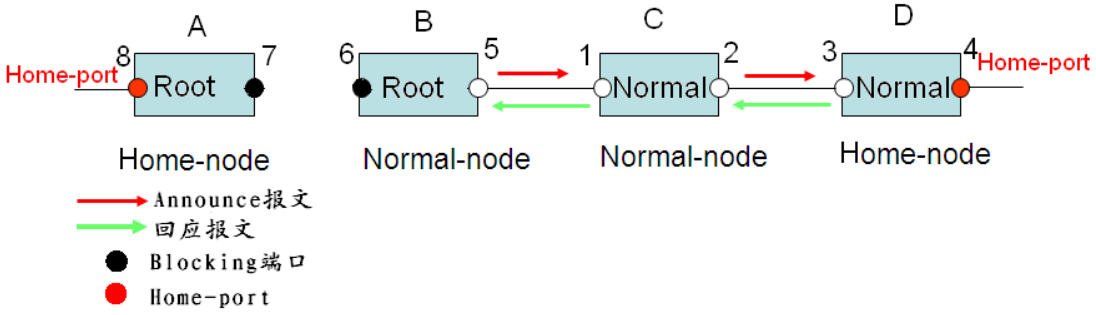


图 170 DHP 故障恢复

6.8.4 说明

DRP 配置满足以下条件：

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

6.8.5 Web 页面配置

1、配置 DRP 模式

点击导航树[设备高级配置]→[DRP 配置]→[DRP 模式]菜单进入 DRP 模式配置界面，如图 171 所示；

图 171 DRP 模式配置

DRP 模式

配置选项：Port Based/VLAN Based

默认配置：Port Based

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

2、创建 DRP-Port-Based

点击导航树[设备高级配置]→[DRP 配置]→[基于端口的 DRP 配置]菜单进入 DRP 创建界面，如图 172 所示；

图 172 创建 DRP

点击<添加>按钮创建 DRP 表项并进行 DRP-Port-Based 配置；

- DRP-Port-Based 配置，如图 173 所示；

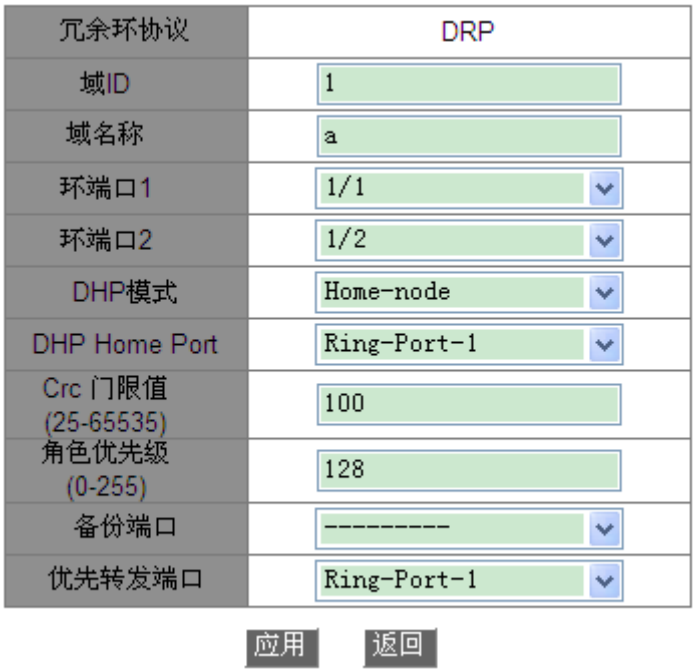


图 173 DRP-Port-Based 配置

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。

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。

DHP 模式

配置选项：Disable/Normal-node/Home-node

默认配置：Disable

功能：是否使能 DHP 模式以及配置 DHP 模式。

DHP Home Port

配置选项：Ring-Port-1/Ring-Port-2/Ring-Port-1-2

功能：配置 DHP Home-node 上的 Home-port。

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

CRC 门限值

配置范围：25~65535

默认配置：100

功能：配置 CRC 门限值。

说明：此配置在选举 root 的时起作用，系统每隔 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。

角色优先级

配置范围：0~255

默认配置：128

功能：配置交换机优先级。

备份端口

配置选项：交换机中所有端口

功能：配置备份端口。

注意：

备份端口选择除环端口外的其他端口。

优先转发端口

配置选项：--/Ring-Port-1/Ring-Port-2

默认配置：--

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

配置完成后，“DRP 列表”中显示已创建的环列表，如图 174 所示；

图 174 DRP-Port-Based 列表

注意：

- DRP 环端口、备份端口与端口聚合互斥，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可以配置为 DRP 环端口和备份端口；
- DRP 环端口、备份端口与镜像目的端口配置互斥，DRP 环端口和备份端口不能配置为镜像目的端口；镜像目的端口也不能配置为 DRP 环端口和备份端口；
- 基于端口的环协议 RSTP、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；
- 建议不要将同一隔离组中的端口同时配置为 DRP 环端口、备份端口；DRP 环端口、备份端口不要加入同一隔离组中。

- 查看 DRP-Port-Based 配置

点击图 174 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；

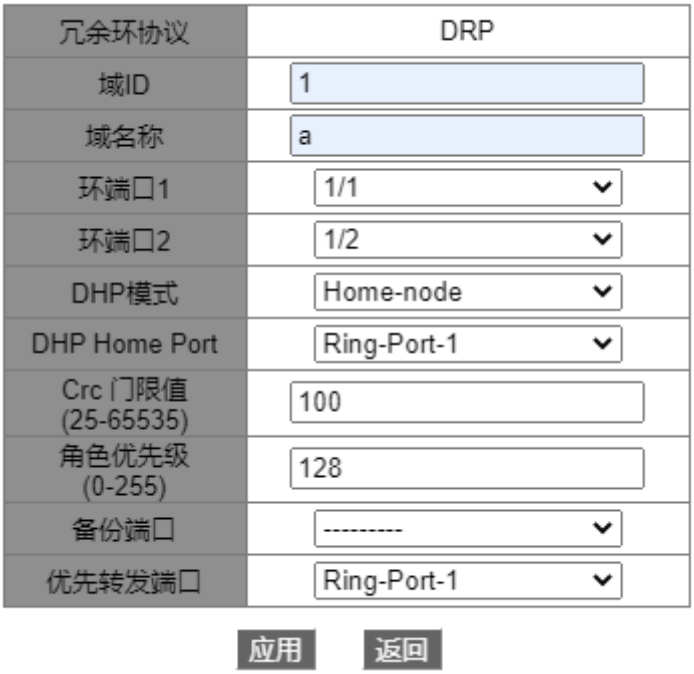


图 175 查看并修改 DRP-Port-Based 配置

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；

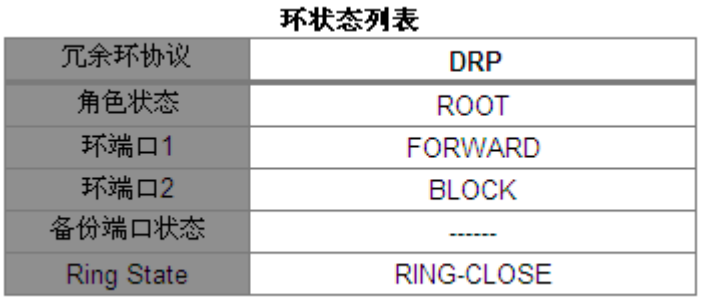


图 176 DRP-Port-Based 状态查看

3、DRP-VLAN-Based 配置

点击导航树[设备高级配置]→[DRP 配置]→[DRP 模式]菜单进入 DRP 模式配置界面，选择 DRP 模式为 VLAN Based。

- DRP 实例配置

点击导航树[设备高级配置]→[DRP 配置]→[基于 VLAN 的 DRP 配置]→[DRP STG 实例]菜单进入 DRP 实例配置界面，如图 177 所示；

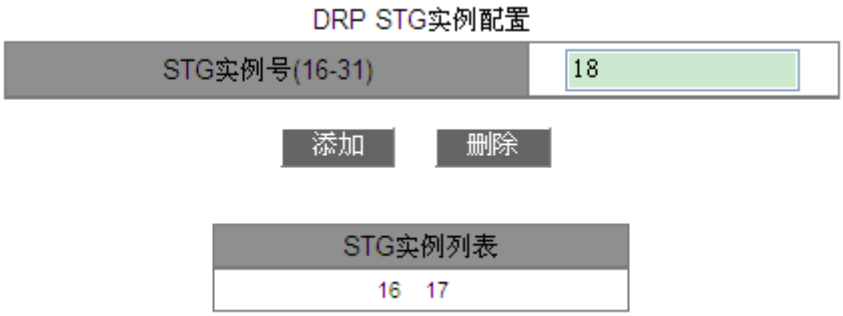


图 177 DRP 实例配置

STG 实例号(16-31)

配置范围：16~31

功能：配置 DRP 实例号。

➢ DRP 实例中的 VLAN 配置

点击导航树[设备高级配置]→[DRP 配置]→[基于 VLAN 的 DRP 配置]→[STG 实例中 VLAN 配置]菜单进入 DRP 实例中 VLAN 配置界面，如图 178 所示；

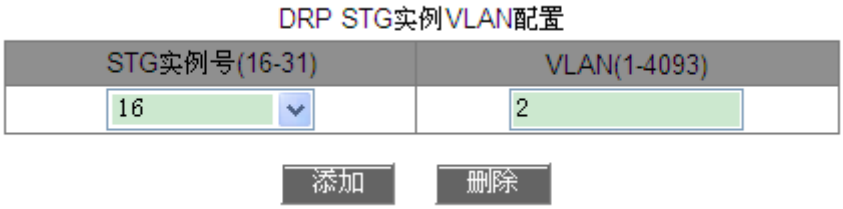


图 178 DRP 实例 VLAN 配置

DRP STG 实例 VLAN 配置

组合配置：{STG 实例号，VLAN ID}

配置范围：{16~31, 1~4093}

功能：配置 DRP 实例中 VLAN ID。

说明：同一实例可以对应多个 VLAN ID，一个 VLAN ID 只能存放于一个实例中。

➢ DRP 实例信息查看

点击导航树[设备高级配置]→[DRP 配置]→[基于 VLAN 的 DRP 配置]→[查看 STG 实例信息]菜单进入 DRP 实例信息查看界面，如图 179 所示；

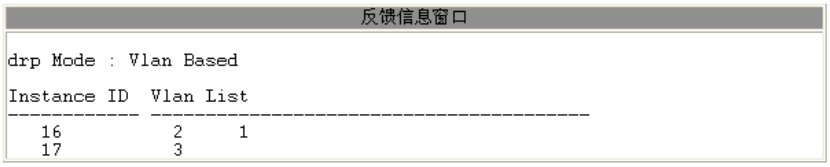


图 179 DRP 实例信息查看

➢ DRP-VLAN-Based 配置

点击导航树[设备高级配置]→[DRP 配置]→[基于 VLAN 的 DRP 配置]→[环配置]菜单进入 DRP-VLAN-Based 创建界面，如图 180 所示；

图 180 创建 DRP-VLAN-Based

点击<添加>按钮创建 DRP 表项并进行 DRP-VLAN-Based 配置，如图 181 所示；

图 181 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。

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。

DHP 模式

配置选项：Disable/Normal-node/Home-node

默认配置：Disable

功能：是否使能 DHP 模式以及配置 DHP 模式。

DHP Home Port

配置选项：Ring-Port-1/Ring-Port-2/Ring-Port-1-2

功能：配置 DHP Home-node 上的 Home-port。

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

CRC 门限值

配置范围：25~65535

默认配置：100

功能：配置 CRC 门限值。

说明：此配置在选举 root 的时起作用，系统每隔 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。

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。

注意：

- DRP 环端口、备份端口与端口聚合互斥，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可以配置为 DRP 环端口和备份端口；
- DRP 环端口、备份端口与镜像目的端口配置互斥，DRP 环端口和备份端口不能配置为镜像目的端口；镜像目的端口也不能配置为 DRP 环端口和备份端口；
- 建议不要将同一隔离组中的端口同时配置为 DRP 环端口、备份端口；DRP 环端口、备份端口不要加入同一隔离组中。

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。

STG Instance

配置选项：已配置的 DRP 实例

功能：配置本环所应用的实例。

说明：本环网的环开环闭以及形成的拓扑是针对本实例的，即环网中的阻塞端口将阻塞所属该实例的所有 VLAN 的数据报文。

Protocol VLAN

配置范围：1~4093

说明：该 VLAN ID 应从已配置的 STG 实例中选择。

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。

优先转发端口

配置选项：--/Ring-Port-1/Ring-Port-2

默认配置：--

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

配置完成后，“DRP 列表”中显示已创建的环列表，如图 182 所示；

图 182 DRP-VLAN-Port 列表

点击相应的 DRP 选项，可以查看该环的配置，并可以对其进行修改，如图 183 所示。

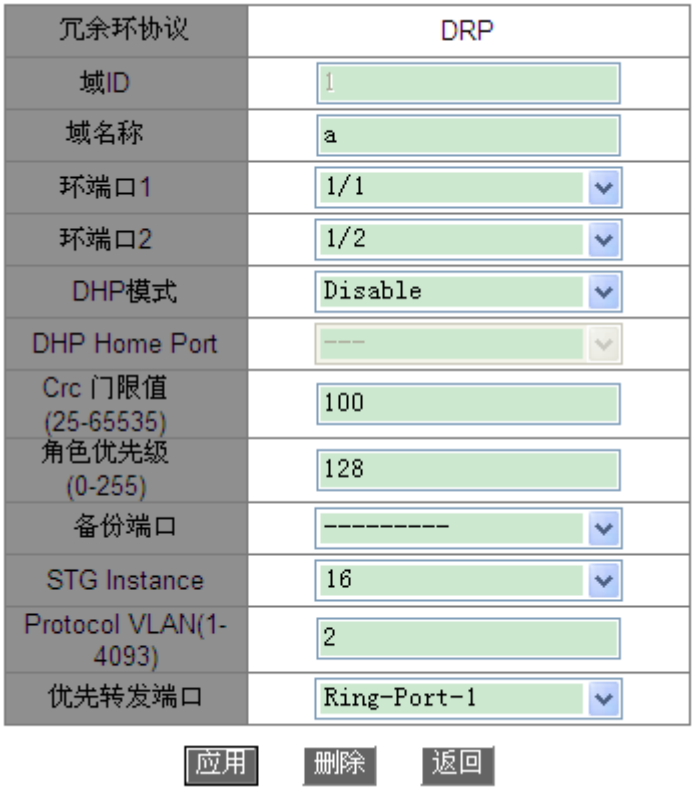


图 183 查看并修改 DRP-VLAN-Based 配置

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 184 所示；

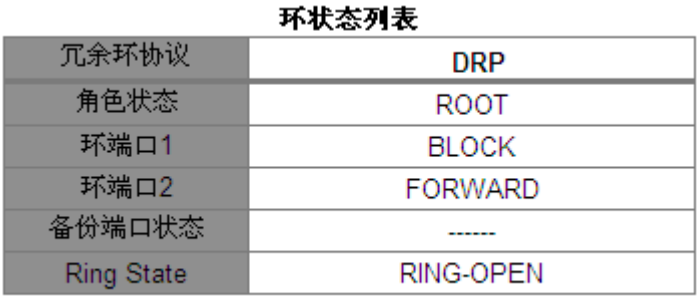


图 184 DRP-VLAN-Based 状态查看

6.8.6 典型配置举例

如图 167 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 173；

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 173；

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 173；

6.9 MSTP 配置

6.9.1 介绍

虽然 RSTP 可以快速收敛，但是和 STP 一样存在以下缺陷：局域网中所有网桥共享一颗生成树，所有 VLAN 的报文都沿着一颗生成树进行转发。如图 185 所示，在某种配置情况下，会把交换机 A 和 C 之间的链路 Block 掉，由于交换机 B 和 D 不包含 VLAN 1，无法转发 VLAN 1 的报文，这样交换机 A 的 VLAN 1 就无法与交换机 C 的 VLAN 1 通信。

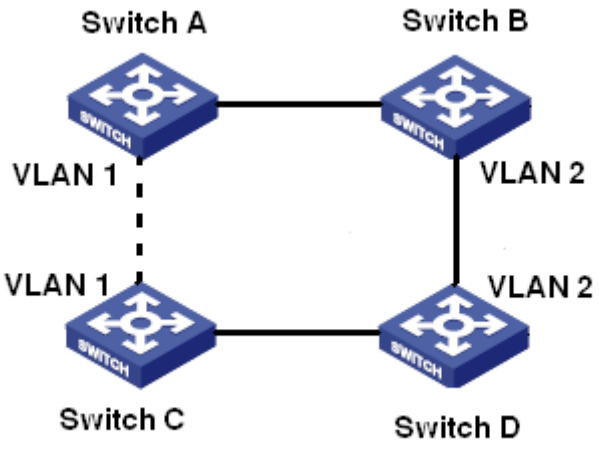


图 185 RSTP 缺陷

针对上述问题产生了 MSTP(Multiple Spanning Tree Protocol，多生成树协议)，它既可以快速收敛，也可以使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

MSTP 把一个或多个 VLAN 映射到一个实例中，有着相同配置的交换机组成一个域，每个域中形成多棵生成树，生成树之间彼此独立，该域相当于一个交换机节点，与其他域再进行生成树算法运算，得出一个整体的生成树。按照这种算法，图 185 所示网络便形成图 186 所示拓扑，交换机 A 和 C 都在 Region1 中，该域中没有产生环路，所以没有链路 Block 掉；同理 Region2 中类似。Region1 和 Region2 相当于交换机节点。这两台“交换机”之间有环路，因此应该 Block 掉一条链路。

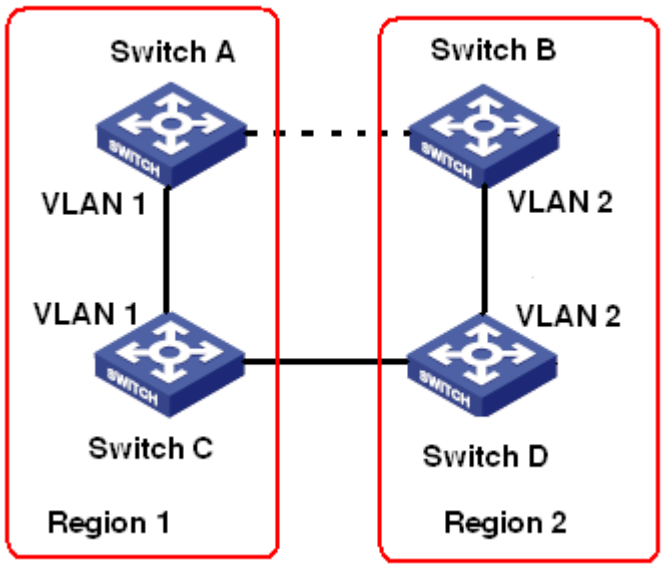


图 186 MSTP 拓扑

6.9.2 基本概念

结合图 187~图 190 了解 MSTP 的相关概念：

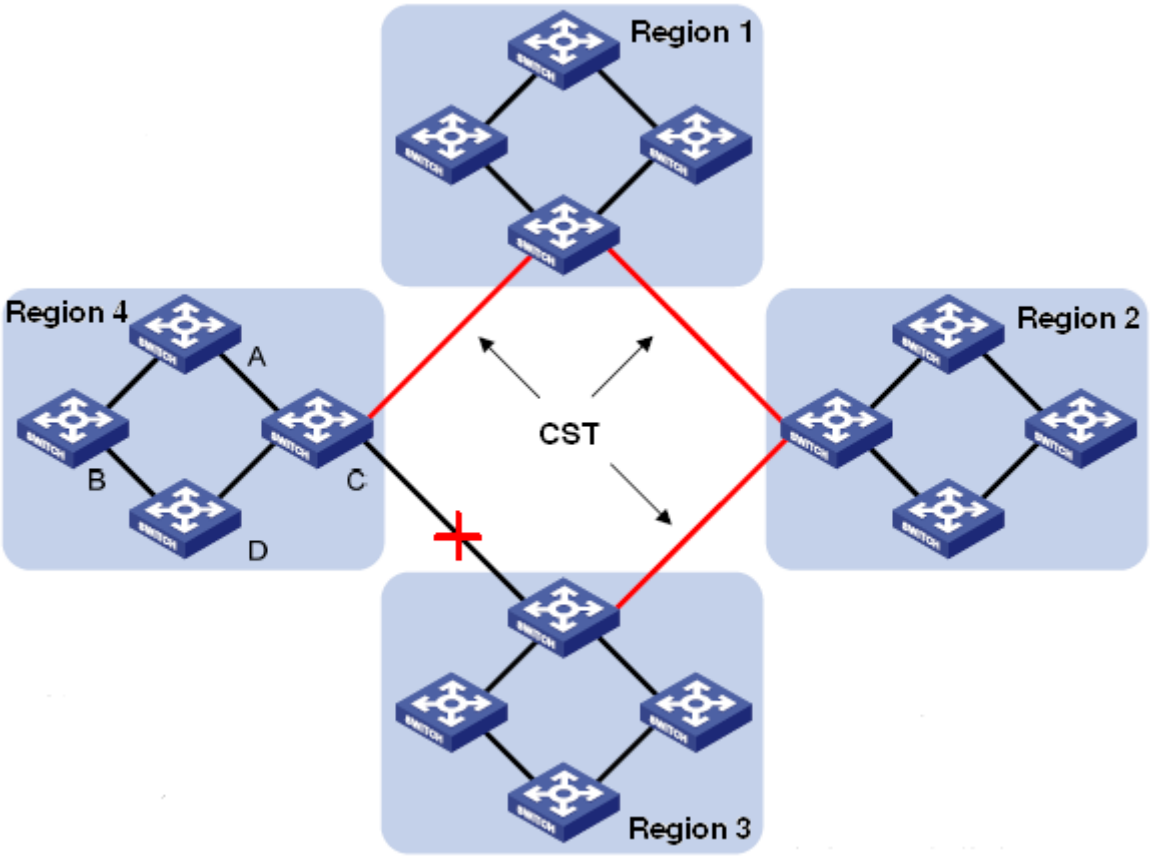


图 187 MSTP 概念解释示意图

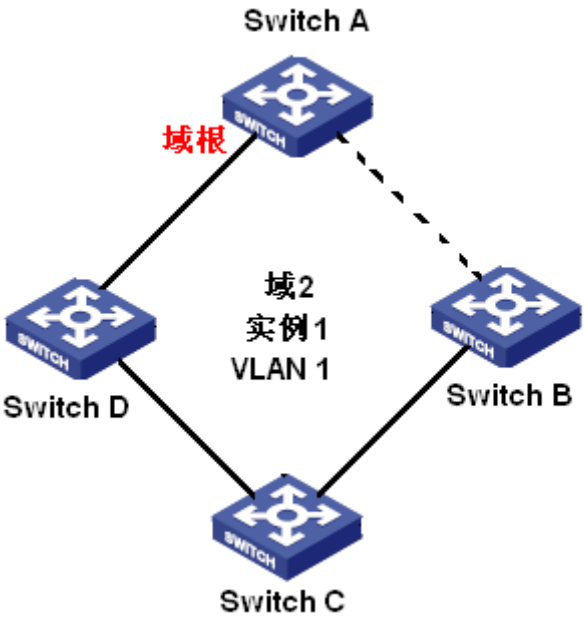


图 188 VLAN 1 映射到实例 1

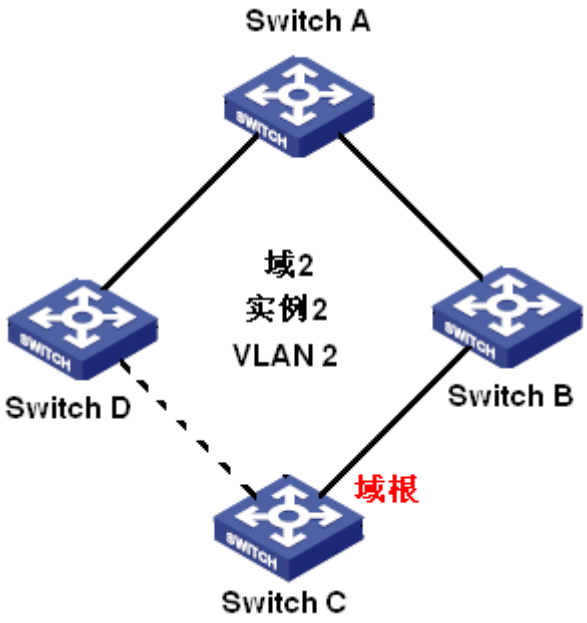


图 189 VLAN 2 映射到实例 2

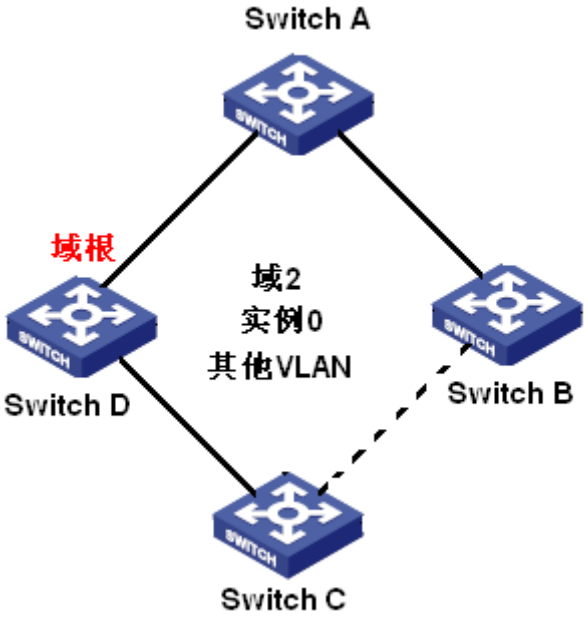


图 190 其他 VLAN 映射到实例 0

实例(Instance)：多个 VLAN 的一个集合。可以一个 VLAN 映射到一个实例(一个 VLAN 形成一棵生成树)，如图 188、图 189 所示；也可以多个有相同拓扑结构的 VLAN 映射到一个实例(多个 VLAN 共享一棵生成树)，如图 190 所示。不同的实例对应不同的生成树，实例 0 是针对所有域中设备的生成树，其他实例是针对当前域中设备的生成树。

MST 域(Multiple Spanning Tree Regions，多生成树域)：MSTP 域名、修订级别、VLAN 到生成树实例映射配置都相同且相互连接的交换机在同一个域中，如图 187 中 Region1、

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

VLAN 映射表：描述 VLAN 和生成树实例之间的映射关系。图 187 中，域 2 的 VLAN 映射表是：VLAN 1 映射到生成树实例 1，如图 188 所示；VLAN 2 映射到生成树实例 2，如图 189 所示；其余 VLAN 映射到生成树实例 0，如图 190 所示。

CIST(Common and Internal Spanning Tree，公共和内部生成树)：即生成树实例 0，指连接一个交换网络内所有设备的单生成树，如图 187 中，由 IST 和 CST 共同组成。

IST(Internal Spanning Tree，内部生成树)：CIST 在 MST 域内的片段，即每个域中的实例 0，如图 190 所示；

CST(Common Spanning Tree，公共生成树)：连接交换网络内所有 MST 域的单生成树。如果把每个 MST 域看作是一个“设备节点”，CST 就是这些节点通过 STP/RSTP 协议计算的一个生成树，如图 187 中红色线条组成的生成树。

MSTI(Multiple Spanning Tree Instance，多生成树实例)：一个 MST 域中可以生成多棵生成树，每棵生成树之间彼此独立，每棵生成树都是一个 MSTI，如图 188、图 189 所示；IST 也是一个特殊的 MSTI。

总根：CIST 的根桥，网络中根桥 ID 最小的交换机被选为总根。

域根：MST 域内 IST 或 MSTI 的根桥就是域根。MST 域内每棵生成树拓扑不同，域根也可能不同，如图 188、图 189 和图 190 三个实例中域根不同。MSTI 的根桥是在当前 MST 域中通过 STP/RSTP 协议计算得到的。IST 的根桥是从与其他 MST 域连接的设备中，根据端口收到的优先级向量信息来选取。

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

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

Forwarding 状态：学习 MAC 地址，转发用户流量；

Learning 状态：学习 MAC 地址，不转发用户流量；

Discarding 状态：不学习 MAC 地址，不转发用户流量。

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

态：Forwarding、Learning、Discarding 状态。

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

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

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

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

6.9.3 MSTP 的实现

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

1、CIST 的计算

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

2、MSTI 的计算

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

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

6.9.4 Web 页面配置

1、全局使能 MSTP 协议

点击导航树[设备高级配置]→[MSTP 配置]→[MSTP 全局使能]菜单进入 MSTP 协议配置界面，如图 191 所示；

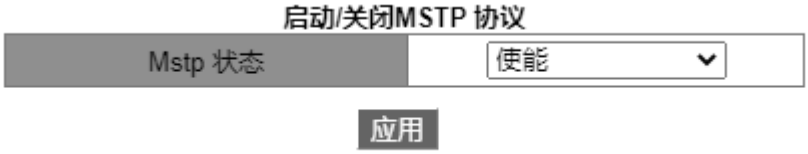


图 191 MSTP 协议使能

Mstp 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 MSTP 协议。

注意：

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

2、强制端口迁移到 MSTP 模式下运行，如图 192 所示；

图 192 强制端口迁移到 MSTP 模式下

端口

配置选项：交换机上所有端口

功能：当运行 MSTP 协议的设备连接运行 STP 协议的设备时，该端口会自动迁移到 STP 模式下工作。如果此时运行 STP 协议的设备被拆离，该端口不会自动迁移到 MSTP 模式下工作，此时通过该配置强制端口迁移到 MSTP 模式下工作。如果再次收到 STP 报文时，会再次

自动迁移到 STP 模式下工作。

注意：

只有交换机运行模式配置为 MSTP 时，该配置才会生效，否则该配置无效。

3、配置端口的 MSTP 状态

点击导航树[设备高级配置]→[MSTP 配置]→[MSTP 端口使能]菜单进入端口 MSTP 配置界面，如图 193 所示；

图 193 配置端口的 MSTP 状态

端口

配置选项：交换机上所有端口

默认配置：全局使能 MSTP 协议的情况下，所有端口的 MSTP 状态全部默认为打开状态

功能：是否使能端口的 MSTP 协议。

注意：

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

4、配置 MST 域参数

点击导航树[设备高级配置]→[MSTP 配置]→[配置 MSTP 域参数]菜单进入 MST 域参数配置界面，如图 194 所示；

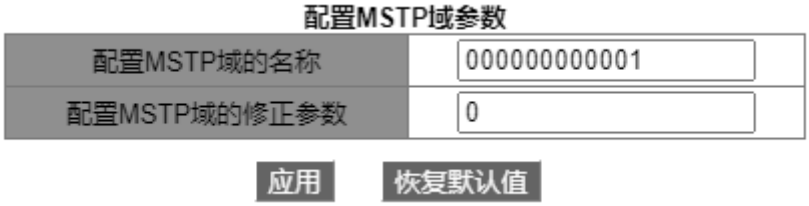


图 194 配置 MST 域参数

配置 MSTP 域的名称

配置范围：1~32 个字符

默认配置：当前设备的 MAC 地址

功能：配置 MST 域的名称。

配置 MSTP 域的修正参数

配置范围：0~65535

默认配置：0

功能：配置 MSTP 域的修正参数。

描述：修正参数和 MST 域名、VLAN 映射表共同决定设备所属的 MST 域。只有以上配置均相同时，设备才认为彼此在同一个 MST 域中。

5、配置 VLAN 映射表，如图 195 所示；

图 195 配置 VLAN 映射表

{实例号，Vlan 列表}

配置范围：{0~16，1~4094}

默认配置：{0，1~4094}

功能：配置当前 MST 域中 VLAN 的映射表。

描述：默认情况下，所有的 VLAN 都映射到实例 0。一个 VLAN 只能映射到一个生成树实例，如果将一个已建立映射关系的 VLAN 重新映射到另外一个实例时，原先的映射关系被取消。如果删除指定 VLAN 与生成树实例之间的映射关系，这些 VLAN 将重新映射到实例 0。

注意：

点击<删除>按钮不能删除实例 0 中的 VLAN 列表。

配置完成后“实例列表”中显示 VLAN 与实例的映射关系。

6、配置交换机在指定实例中的网桥优先级

点击导航树[设备高级配置]→[MSTP 配置]→[配置实例参数]菜单进入 MSTP 实例参数配置界面，如图 196 所示；

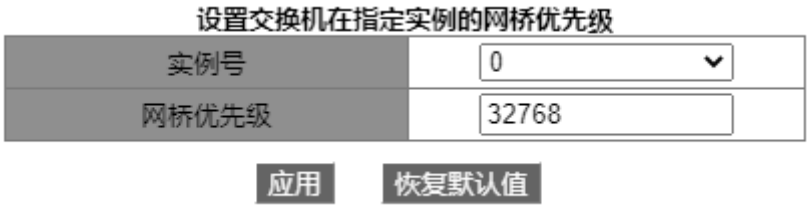


图 196 配置指定实例中的网桥优先级

实例号

配置选项：已创建的实例

网桥优先级

配置范围：0~61440，步长为 4096

默认配置：32768

功能：配置交换机在指定实例中的网桥优先级。

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

7、配置端口在指定实例中的优先级和路径代价，如图 197 所示；

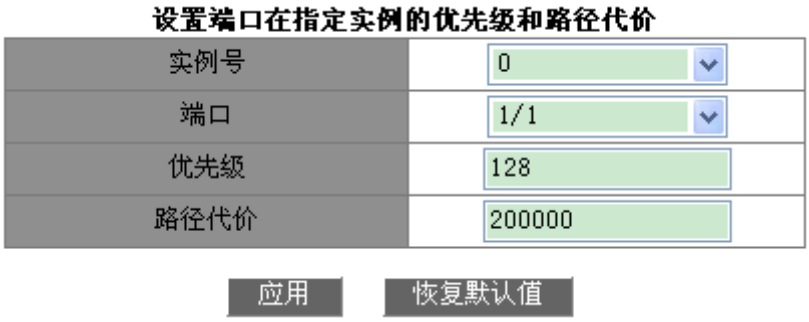


图 197 配置端口在指定实例中的优先级和路径代价

实例号

配置选项：已创建的实例

端口

配置选项：交换机上所有端口

优先级

配置范围：0~240，步长 16

默认配置：128

功能：配置端口在指定实例中的优先级。

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

路径代价

配置范围：1~200000000

默认配置：如表 10、表 11 所示：

表 10 普通端口默认路径代价

端口类型	缺省路径代价	建议配置范围
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000

表 11 汇聚端口默认路径代价

端口类型	汇聚端口个数(在允许汇聚的个数范围内)	建议配置范围

10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N

功能：配置端口在指定实例中的路径代价。

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

8、配置 MSTP 时间参数

点击导航树[设备高级配置]→[MSTP 配置]→[配置 MSTP 时间参数]菜单进入 MSTP 时间参数配置界面，如图 198 所示；

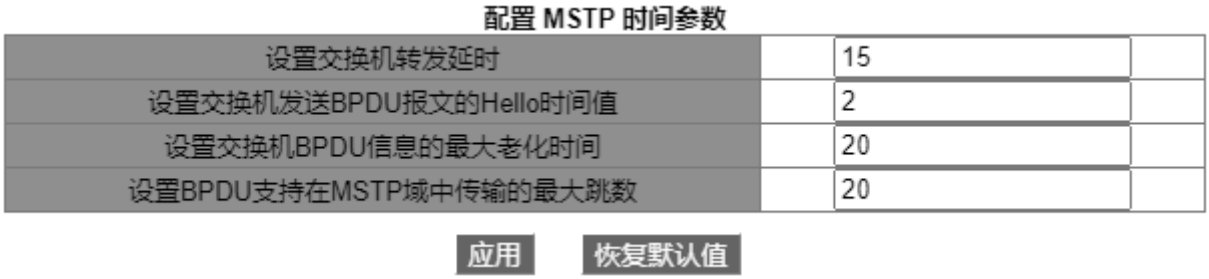


图 198 配置 MSTP 时间参数

设置交换机转发延时

配置范围：4~30s

默认配置：15s

功能：配置端口状态转换的时间间隔，Discarding--Learning 或 Learning--Forwarding。

设置交换机发送 BPDU 报文的 Hello 时间值

配置范围：1~10s

默认配置：2s

功能：配置交换机发送 BPDU 配置消息的时间间隔。

设置交换机 BPDU 信息的最大老化时间

配置范围：6~40s

默认配置：20s

功能：配置 BPDU 报文消息生存的最长时间。

注意：

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

设置 BPDU 支持在 MSTP 域中传输的最大跳数

配置范围：1~40

默认配置：20

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

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

注意：

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

9、配置 MSTP 快速迁移特性

点击导航树[设备高级配置]→[MSTP 配置]→[配置 MSTP 快速迁移特性]菜单进入 MSTP 时间参数配置界面，如图 199 所示；

图 199 配置 MSTP 快速迁移特性

设置端口的链路类型

配置选项：自动检测/点对点/共享

默认配置：自动检测

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

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

设置/取消端口为边缘端口

配置选项：边缘端口/非边缘端口

默认配置：非边缘端口

功能：配置当前端口是否为边缘端口。

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

10、查看 MSTP 配置信息

点击导航树[设备高级配置]→[MSTP 配置]→[MSTP 主要信息]菜单进入 MSTP 信息配置查看界面，如图 200 所示；

状态信息窗口

```
                -- MSTP Bridge Config Info --

Bridge MAC    :  00:00:11:11:11:11
Bridge Times  :  Max Age 20, Hello Time 2, Forward Delay 15
Force Version:  3

############################ Instance 0 ############################
Self Bridge Id    : 32768 -  00:00:11:11:11:11
Root Id           : this switch
Ext.RootPathCost  : 0
Region Root Id    : this switch
Int.RootPathCost  : 0
Root Port ID      : 0
Current port list in Instance 0:
Ethernet3/4 (Total 1)

   PortName      ID      ExtRPC   IntRPC  State Role     DsgBridge      DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
   Ethernet3/4 128.012       &
```

图 200 查看 MSTP 配置信息

6.9.5 典型配置举例

图 201 所示网络中交换机 A、B、C、D 属于一个 MST 域，红色标记为该条链路允许通过的 VLAN 报文。通过配置使不同 VLAN 报文沿不同生成树实例转发：VLAN 10 的报文沿实例 1 转发，实例 1 的根桥为 Switch A；VLAN 30 的报文沿实例 3 转发，实例 3 的根桥为 SwitchB；VLAN 40 的报文沿实例 4 转发，实例 4 的根桥为 Switch C；VLAN 20 的报文沿实例 0 转发，实例 0 的根桥为 Switch B。

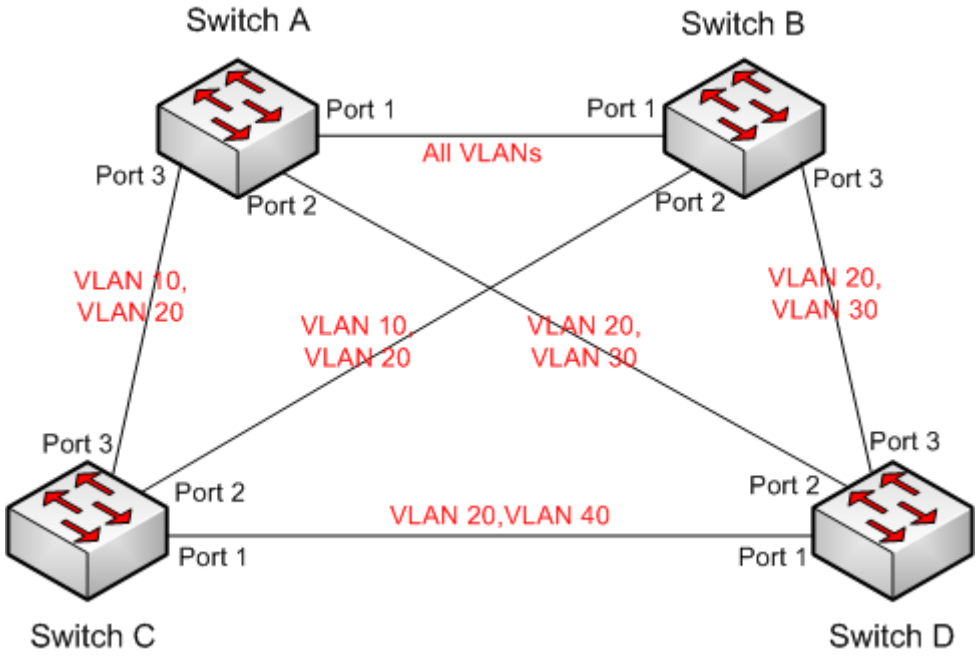


图 201 MSTP 典型配置举例

Switch A 配置过程：

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

2、全局使能 MSTP 协议，如图 191 所示；

3、配置 MST 域的名称为 Region，修正参数为 0，如图 194 所示；

4、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 195 所示；

5、配置该交换机在实例 1 中的网桥优先级为 4096，其余实例中为默认值，如图 196 所示；

Switch B 配置如下：

1、在 Switch B 上创建 VLAN 10、20、30，将对应端口配置为 Trunk 端口并允许相应的

VLAN 通过；

2、全局使能 MSTP 协议，如图 191 所示；

3、配置 MST 域的名称为 Region，修正参数为 0，如图 194 所示；

4、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 195 所示；

5、配置该交换机在实例 3 和实例 0 中的网桥优先级为 4096，其余实例中为默认值，如图 196 所示；

Switch C 配置如下：

1、在 Switch C 上创建 VLAN 10、20、40，将对应端口配置为 Trunk 端口并允许相应的 VLAN 通过；

2、全局使能 MSTP 协议，如图 191 所示；

3、配置 MST 域的名称为 Region，修正参数为 0，如图 194 所示；

4、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 195 所示；

5、配置该交换机在实例 4 中的网桥优先级为 4096，其余实例中为默认值，如图 196 所示；

Switch D 配置如下：

1、在 Switch D 上创建 VLAN 20、30、40，将对应端口配置为 Trunk 端口并允许相应的 VLAN 通过；

2、全局使能 MSTP 协议，如图 191 所示；

3、配置 MST 域的名称为 Region，修正参数为 0，如图 194 所示；

4、创建实例 1、3、4，并将 VLAN 10、30、40 分别映射到实例 1、3、4 上，如图 195 所示；

MSTP 计算完成后，各 VLAN 对应的 MSTI 如图 202 所示；

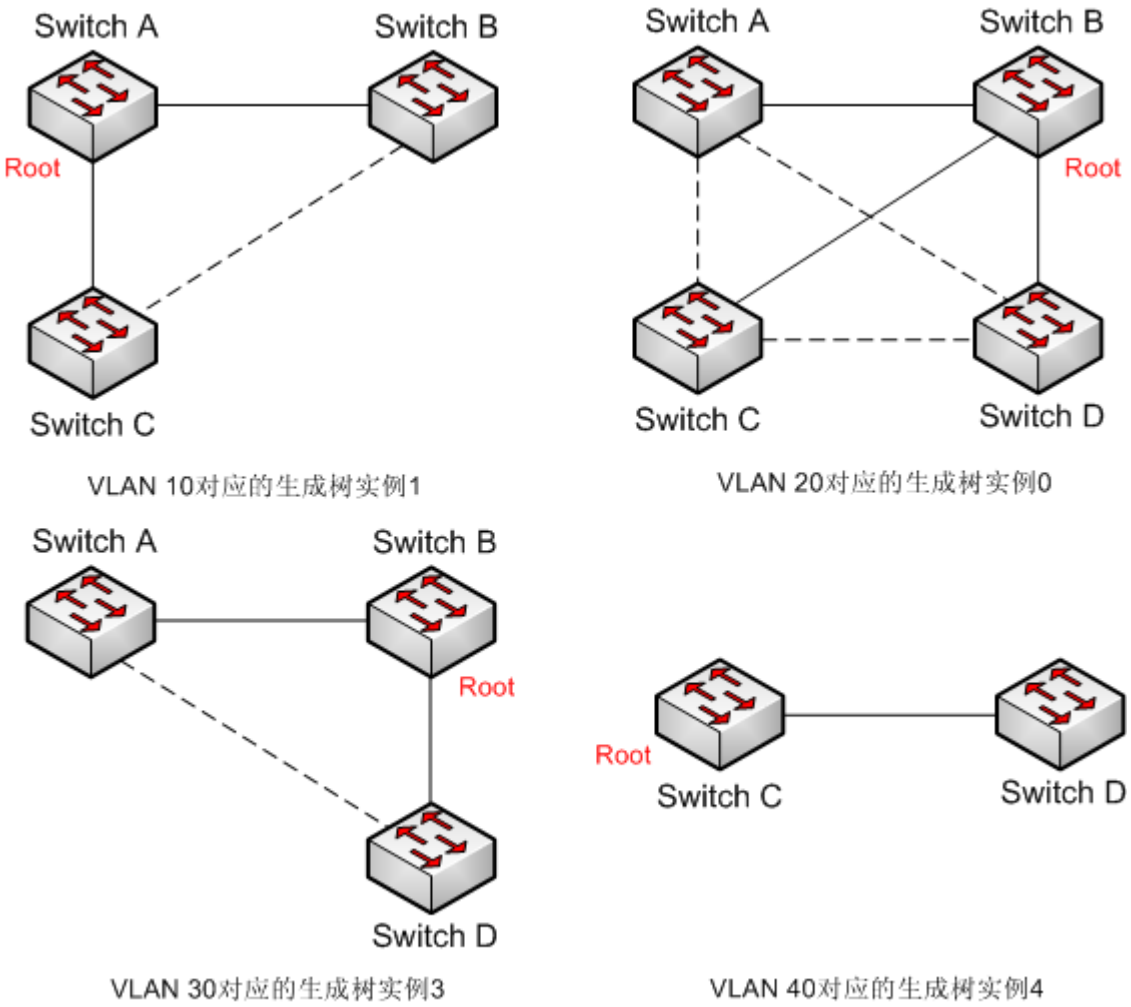


图 202 各 VLAN 对应的生成树实例

6.10 告警

6.10.1 介绍

该系列设备支持以下几种类型告警：

IP/MAC 冲突告警：使能情况下，IP/MAC 地址冲突时会产生告警；

内存/CPU 利用率告警：使能情况下，内存/CPU 利用率超过设定阈值时产生告警；

端口告警：使能情况下，端口 Link down 时会产生告警；

电源告警：双电源模块的设备在电源告警使能情况下，电源模块掉电或异常时会产生告警；

环告警：使能情况下，环开时会产生告警；

高温告警：使能情况下，交换机温度突破高温门限时会产生高温告警；普通高温上限 T-high

的取值范围：85~94℃，默认值为 85℃；危险高温门限 T-max 的取值范围：95~100℃，默认值为 95℃；交换机当前温度 T-high<T-cur<T-max 时触发普通高温告警，交换机当前温度 T-cur>=T-max 时触发危险温度告警；

低温告警：使能情况下，交换机温度突破低温门限时会产生低温告警；低温下限 T-low 的取值范围：-40~-10℃，默认值为-40℃；交换机当前温度 T-cur<T-low 时触发低温告警；

端口流量告警：使能情况下，端口的入方向/出方向流量超过设定阈值时产生告警；

CRC 错误/丢包率告警：使能情况下，端口 CRC 错误/丢包率超过设定阈值时产生告警；

告警使能时，告警方式有日志记录、前面板 Alarm 指示灯闪亮、触发告警端子、发送 SNMP Trap 报文。

注意：

只有 DT-Ring 环的主站、DRP 环的 Root 支持环告警功能。

6.10.2 Web 页面配置

1、内存及 CPU 利用率告警配置与显示

点击导航树[设备高级配置]→[告警]→[基础告警]菜单进入内存及 CPU 利用率告警配置与显示界面，如图 203 所示；

内存及CPU利用率告警

使能	内存利用率告警	CPU利用率告警
阈值	85 (50~100)	85 (50~100)
浮动值	5 (1~20)	5 (1~20)
告警状态	禁止	禁止

应用

图 203 内存/CPU 利用率告警配置

内存利用率告警/CPU 利用率告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能内存/CPU 利用率告警。

阈值（%）

配置范围：50~100

默认配置：85

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

浮动值（%）

配置范围：1~20

默认配置：5

功能：配置交换机内存/CPU 利用率浮动值。

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

告警状态

显示选项：禁止/禁止

功能：显示交换机内存/CPU 利用率状态。告警表示内存/CPU 利用率超阈值，产生告警。

注意：

文中 CPU 利用率均指 5 分种内的 CPU 利用率均值。

2、电源、温度告警配置与显示，如图 204 所示；

图 204 电源、温度告警配置

电源告警/高温告警/低温告警

配置选项：不使能禁止

默认配置：禁止

功能：是否使能电源/高温/低温告警。

电源告警状态

显示选项：正常/告警

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

高温/低温告警状态

显示选项：正常/告警

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

3、IP&MAC 冲突告警配置显示，图 205 所示；

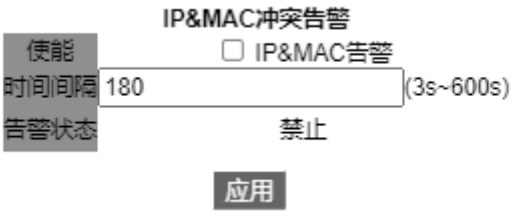


图 205 IP&MAC 冲突告警配置

IP/MAC 冲突告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能地址冲突告警。

时间间隔

配置范围：3s~600s

默认配置：180s

功能：配置检测地址冲突的时间间隔。

4、端口告警配置与显示

点击导航树[设备高级配置]→[告警]→[端口 LinkDown 告警]菜单进入端口告警配置与显示

界面，如图 206 所示；

端口LinkDown告警

使能(端口)	告警状态	使能(端口)	告警状态
☐ 1/1	禁止	☐ 1/2	禁止
☐ 1/3	禁止	☐ 1/4	禁止
☐ 1/5	禁止	☐ 1/6	禁止
☐ 1/7	禁止	☐ 1/8	禁止
☐ 1/9	禁止	☐ 1/10	禁止
☐ 1/11	禁止	☐ 1/12	禁止

应用

图 206 端口告警配置

端口

配置选项：不使能/使能

默认配置：不使能

功能：是否使能端口告警。

告警状态

显示选项：LinkDown/LinkUp

功能：显示端口连接状态。LinkUp 表示端口处于连接状态可以正常通信；LinkDown 表示端口处于断开或者连接异常状态，会产生告警。

5、端口流量告警配置与显示

点击导航树[设备高级配置]→[告警]→[端口流量告警]菜单进入端口流量告警配置与显示界面，如图 207 所示；

端口流量告警

端口	入方向流量告警			出方向流量告警		
	使能	阈值	告警状态	使能	阈值	告警状态
1/1	☐	0 bps	禁止	☐	0 bps	禁止
1/2	☐	0 bps	禁止	☐	0 bps	禁止
1/3	☐	0 bps	禁止	☐	0 bps	禁止
1/4	☐	0 bps	禁止	☐	0 bps	禁止
1/5	☐	0 bps	禁止	☐	0 bps	禁止
1/6	☐	0 bps	禁止	☐	0 bps	禁止
1/7	☐	0 bps	禁止	☐	0 bps	禁止
1/8	☐	0 bps	禁止	☐	0 bps	禁止
1/9	☐	0 bps	禁止	☐	0 bps	禁止
1/10	☐	0 bps	禁止	☐	0 bps	禁止
1/11	☐	0 bps	禁止	☐	0 bps	禁止
1/12	☐	0 bps	禁止	☐	0 bps	禁止

应用

图 207 端口流量告警配置

入方向流量告警/出方向流量告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口流量告警。

阈值

配置范围：1~1000000000bps 或 1~1000000kbps

功能：配置端口流量告警阈值。

告警状态

显示选项：告警/正常

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

6、CRC 错误及丢包率告警配置与显示

点击导航树[设备高级配置]→[告警]→[CRC 及丢包率告警]菜单进入 CRC 错误及丢包率告警配置与显示界面，如图 208 所示；

CRC及丢包率告警

端口	CRC			丢包率告警		
	使能	阈值	告警状态	使能	阈值	告警状态
1/1	☐	0 pps	禁止	☐	100 pps	禁止
1/2	☐	0 pps	禁止	☐	100 pps	禁止
1/3	☐	0 pps	禁止	☐	100 pps	禁止
1/4	☐	0 pps	禁止	☐	100 pps	禁止
1/5	☐	0 pps	禁止	☐	100 pps	禁止
1/6	☐	0 pps	禁止	☐	100 pps	禁止
1/7	☐	0 pps	禁止	☐	100 pps	禁止
1/8	☐	0 pps	禁止	☐	100 pps	禁止
1/9	☐	0 pps	禁止	☐	100 pps	禁止
1/10	☐	0 pps	禁止	☐	100 pps	禁止
1/11	☐	0 pps	禁止	☐	100 pps	禁止
1/12	☐	0 pps	禁止	☐	100 pps	禁止

应用

图 208 CRC 及丢包率告警配置

CRC/丢包率告警

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口 CRC/丢包率告警。

阈值

配置范围：1~1000000pps

功能：配置端口 CRC/丢包率告警阈值。

状态

显示选项：正常/告警

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

7、DT-Ring 环告警配置与显示

点击导航树[设备高级配置]→[告警]→[环告警]菜单进入 DT-Ring 环告警配置与显示界面，如图 209 所示；

图 209 DT-Ring 环告警配置

DT-Ring 告警

配置选项：不使能/使能

默认配置：不使能

功能：是否使能 DT-Ring 环告警。

告警状态

显示选项：告警/正常

功能：显示 DT-Ring 环环状态，正常表示 DT-Ring 环处于环闭状态；告警表示 DT-Ring 环处于环开或者异常状态。

8、DRP 环告警配置与显示，如图 210 所示；

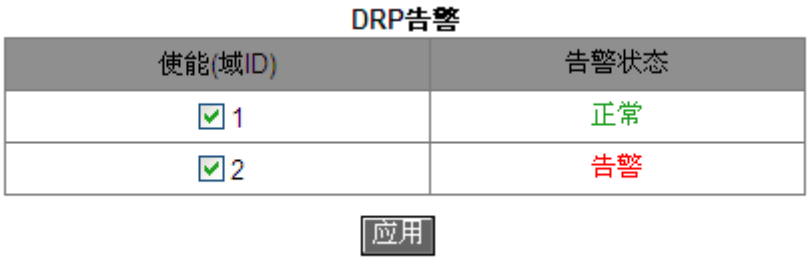


图 210 DRP 环告警配置

DRP 告警

配置选项：不使能/使能

默认配置：不使能

功能：是否使能 DRP 环告警。

告警状态

显示选项：告警/正常

功能：显示 DRP 环环状态，正常表示 DRP 环处于环闭状态；告警表示 DRP 环处于环开或者异常状态。

6.11 日志配置

6.11.1 介绍

交换机的日志功能主要记录交换机系统的状态变化、故障、调试、异常等信息。通过配置可以实时上传日志信息到支持 Syslog 协议的服务器。

日志信息按重要性分为 4 级，由高到低依次为：Critical、Warning、Information、Debugging，数值越小的信息紧急程度越高。

表 12 信息级别列表

信息级别	数值	描述
Critical	2	系统严重问题信息
Warning	4	告警信息
Information	6	需要记录的通知信息
Debugging	7	调试过程中产生的信息

6.11.2 Web 页面配置

1、日志功能配置

点击导航树[设备高级配置]→[日志配置]→[日志配置]菜单进入日志配置界面，如图 211 所示；

图 211 日志配置

保存日志到 fiash 使能

配置选项：使能/ 禁止

默认配置：禁止

功能：保存日志到 flash 使能服务。

保存日志到 flash 间隔(10~14400 分)

配置范围：10~14400 分

默认配置：14400

功能：配置保存日志到 flash 的时间间隔

远程日志服务器 IP

配置上传日志信息的服务器 IP 地址。

Facility

配置选项：Local0~Local7

默认配置：Local0

描述：Facility 用于在日志服务器端标志不同的日志来源。

Level

配置选项：Critical/Warning/Information/Debugging

默认配置：Warning

功能：选择记录的日志信息级别。

描述：可按等级对日志信息进行过滤，过滤采取的规则是：禁止数值大于所选信息级别数值的信息输出，如选择信息级别为 Warning 时，因为 Warning 对应的数值为 4，系统会输出数值为 2 的 Critical 信息和数值为 4 的 Warning 信息

Syslog 协议的服务器可选择在 PC 上安装支持 Syslog Server 的软件，如 Tftp32。通过 Syslog Server 可以实时查看日志信息，如图 212 所示。

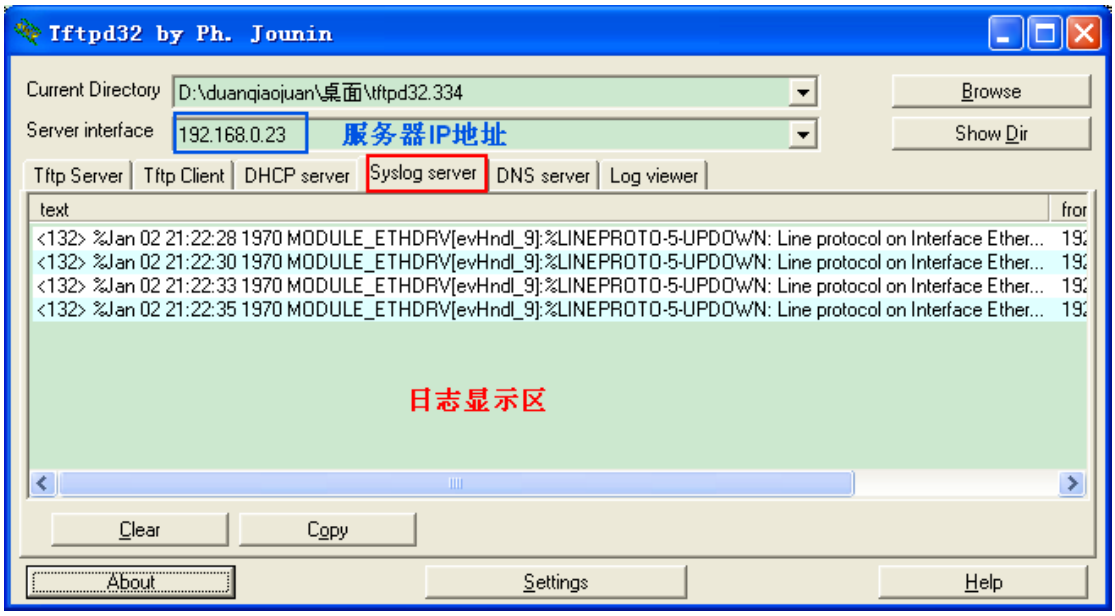


图 212 实时上传日志信息

2、显示日志信息配置

点击导航树[设备高级配置]→[日志配置]→[显示日志]菜单进入日志显示界面如图 213 所示；

图 213 显示日志配置

Level

配置选项：Warning/Critical

默认配置：Warning

功能：选择显示的日志信息的最低等级。

日志显示起始行数/日志显示截止行数

配置范围：1~65535

功能：显示 Buffer 中指定的日志信息，一行即一条日志信息。

下方反馈信息窗口显示 Buffer 中指定的日志信息，如图 214 所示；

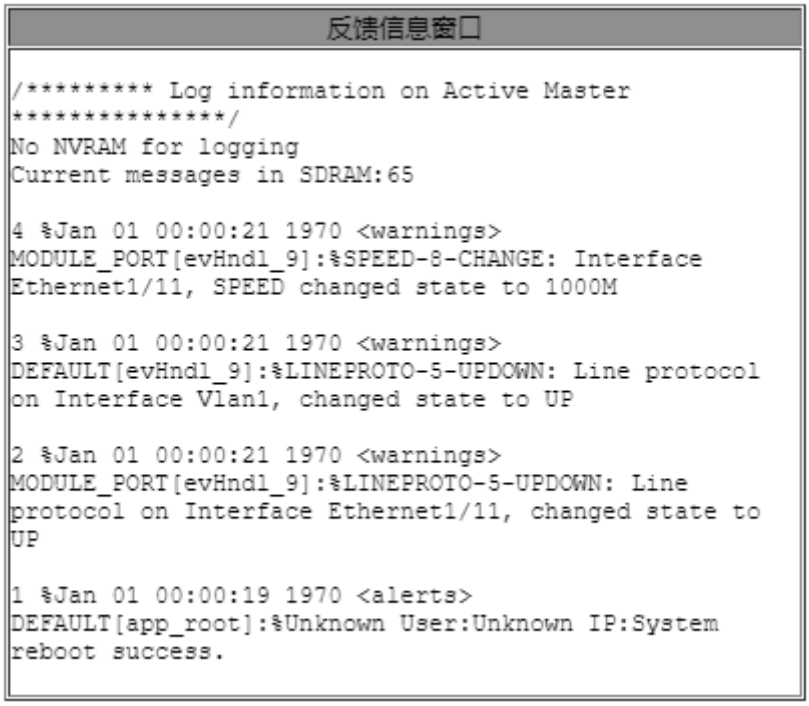


图 214 显示日志信息

注意：

只有 Critical 和 Warning 日志信息保存在 Buffer 中，Information 和 Debugging 日志信息并没有保存在 Buffer 中。

3、借助 FTP 服务器上传日志

点击导航树[设备高级配置]→[日志配置]→[日志上传]菜单进入日志清除界面，如图 215 所示；

图 215 上传日志

FTP 服务器

配置格式：A.B.C.D

功能：配置 FTP 服务器 IP 地址。

用户名

功能：配置 FTP 用户的名称。

密码

功能：配置 FTP 用户的密码。

文件名

配置范围：1~32 字符

功能：配置服务器中保存的日志信息文件名。

注意：

上传日志信息时，FTP 服务器应保持运行状态。

4、清除 Buffer 中的日志信息

点击导航树[设备高级配置]→[日志配置]→[清除日志]菜单进入日志清除界面，如图 216 所示；

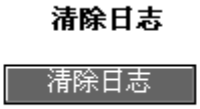


图 216 清除日志信息

6.12 DHCP 配置

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

DHCP 采用客户端/服务器的通信模式，由客户端向服务器提出配置申请，服务器返回为

客户端分配的IP地址等配置信息，以实现IP地址的动态配置。DHCP的典型应用结构如图 217所示；

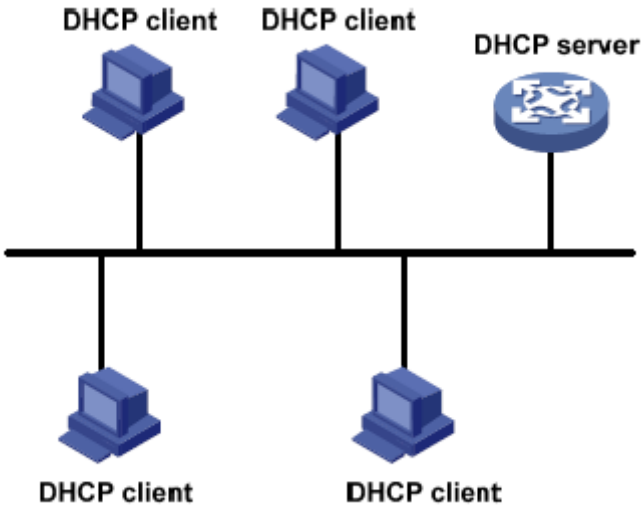


图 217 DHCP 典型应用结构

注意：

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

DHCP 提供两种 IP 地址分配策略：

静态分配地址：由管理员为少数特定客户端(如 WWW 服务器等)静态绑定 IP 地址，通过 DHCP 将绑定的 IP 地址发给客户端。

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。

6.12.1 DHCP 服务器配置

6.12.1.1 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。

6.12.1.2 地址池

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

1、与客户端 MAC 地址静态绑定的 IP 地址；

2、DHCP 服务器记录的曾经给客户端分配的 IP 地址；

3、客户端发送的请求报文中指定的 IP 地址；

4、从地址池中顺序查找可供分配的 IP 地址，最先找到的 IP 地址；

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

6.12.1.3 Web 页面配置

1、使能 DHCP 服务器

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[启动 DHCP 配置]菜单进入 DHCP 服务器启动界面，如图 218 所示；

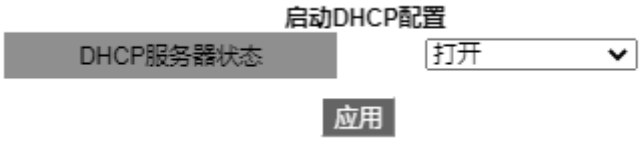


图 218 DHCP 服务器状态

DHCP 服务器状态

配置选项：打开/关闭

默认配置：关闭

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。

2、静态分配 IP 地址

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[地址池管理配置]菜单进入地址池创建界面，如图 219 所示；

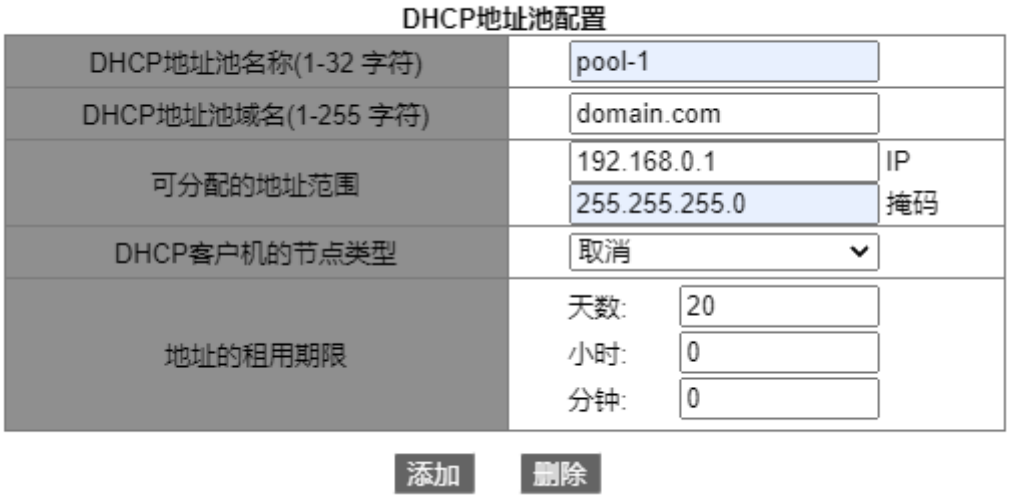


图 219 创建地址池

DHCP 地址池名称

配置范围：1~32 个字符

功能：配置 DHCP 地址池名称。

DHCP 地址池域名

配置范围：1~255 个字符

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

地址的租用期限

配置范围：0 天 0 小时 0 分~365 天 23 小时 59 分

描述：静态分配的 IP 地址无有效期限制，该参数对静态分配 IP 地址无效。

说明：

- 静态分配 IP 地址可以看做是从一个特殊的地址池中获取 IP 地址，该地址池中只包含一个特定的 IP 地址。所以静态分配 IP 地址前应先创建一个 DHCP 地址池；
- 每个 DHCP 地址池只能配置一种 IP 地址分配策略。

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[手动地址池配置]菜单进入静态分配 IP 地址界面，如图 220 所示；

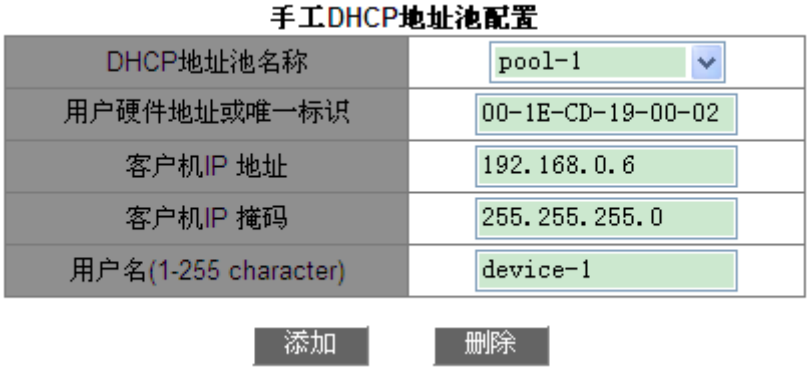


图 220 静态分配 IP 地址

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

用户硬件地址或唯一标识

配置格式：HH-HH-HH-HH-HH-HH（H 为一个十六进制数）

功能：配置静态绑定的客户端 MAC 地址。

客户机 IP 地址

配置格式：A.B.C.D

功能：配置静态绑定的 IP 地址。

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

客户机 IP 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。

用户名

配置范围：1~255 个字符

功能：配置客户端用户名。

3、动态分配 IP 地址

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[地址池管理配置]菜单进入动态分配 IP 地址界面，如图 221 所示；

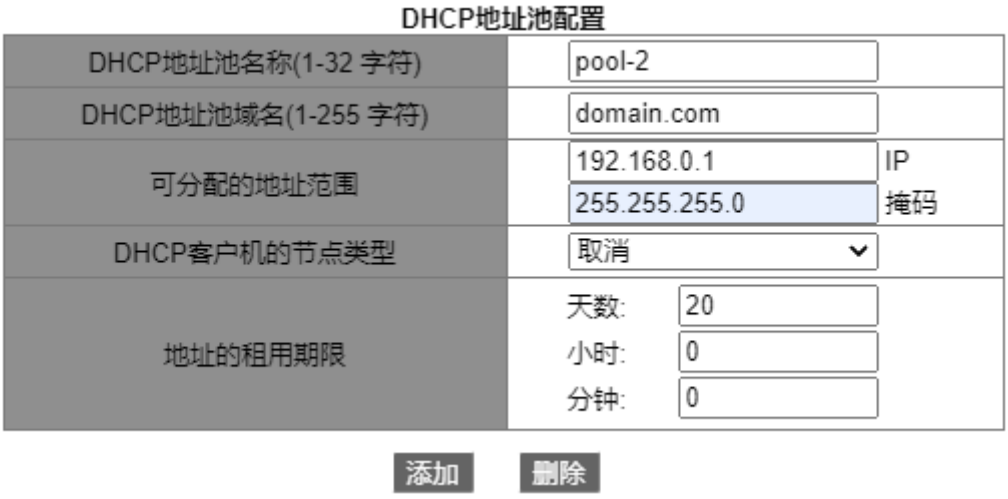


图 221 动态分配 IP 地址

DHCP 地址池名称

配置范围：1~32 个字符

功能：配置 DHCP 地址池名称。

DHCP 地址池域名

配置范围：1~255 个字符

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

可分配的地址范围{IP，MASK}

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

说明：

一个地址池中只能配置一个地址段；

DHCP 客户机的节点类型

配置选项：取消/Broadcast node/Peer-to-peer node/Mixed node/Hybrid node

默认配置：取消

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

关系的方式不同。

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

地址的租用期限

配置范围：0 天 0 小时 0 分~365 天 23 小时 59 分

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

4、配置 DHCP 客户端网关地址

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[默认网关配置]菜单进入 DHCP 客户端网关地址配置界面，如图 222 所示；

图 222 配置 DHCP 客户端网关地址

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

网关 1~网关 8

功能：配置 DHCP 服务器为 DHCP 客户端分配的网关地址。

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

务器为客户端分配 IP 地址的同时可以指定网关地址。DHCP 地址池最多可以配置 8 个网关地址。网关 1 优先级最高，网关 8 优先级最低。

5、配置 DHCP 客户端 DNS 服务器地址

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[DHCP 客户端 DNS 服务器配置]菜单进入 DHCP 客户端 DNS 服务器地址配置界面，如图 223 所示；

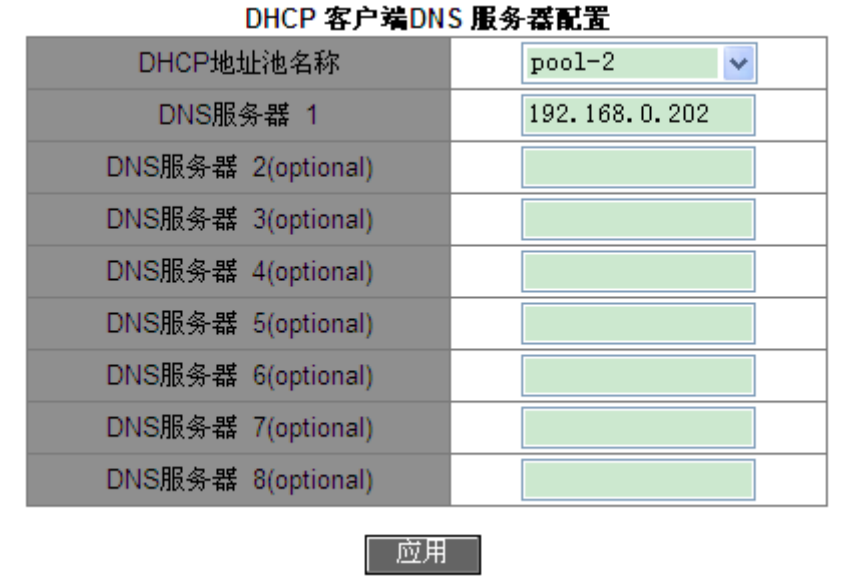


图 223 配置 DHCP 客户端 DNS 服务器地址

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

DNS 服务器 1~DNS 服务器 8

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

描述：通过域名访问网络上的主机时，需要将域名解析为 IP 地址，这是通过 DNS（Domain Name System，域名系统）实现的。为了使 DHCP 客户端能够通过域名访问网络上的主机，DHCP 服务器为客户端分配 IP 地址的同时可以指定 DNS 服务器地址。DHCP 地址池最多可以配置 8 个 DNS 服务器地址。DNS 服务器 1 优先级最高，DNS 服务器 8 优先级最低。

6、配置 DHCP 客户端 WINS 服务器地址

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[DHCP 客户端 WINS 服务器配置]菜单进入 DHCP 客户端 WINS 服务器地址配置界面，如图 224 所示；

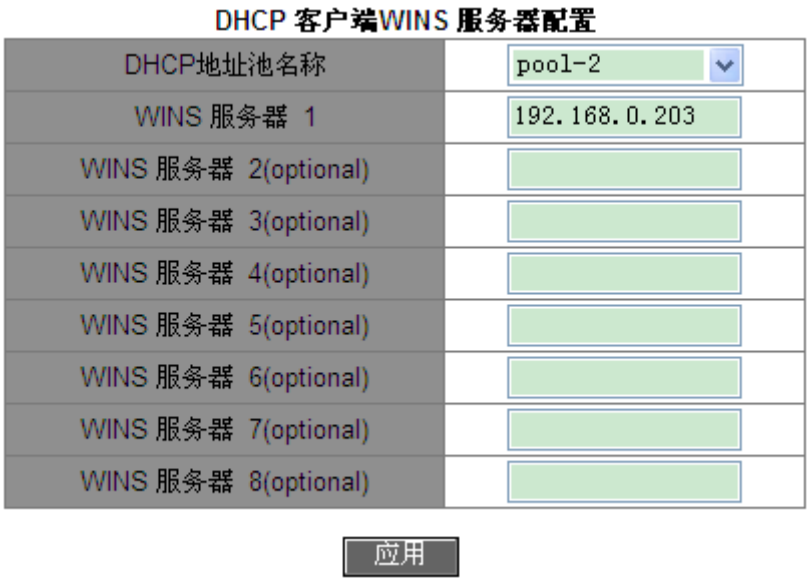


图 224 配置 DHCP 客户端 WINS 服务器地址

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

WINS 服务器 1~WINS 服务器 8

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

描述：对于使用 Microsoft Windows 操作系统的客户端，由 WINS（Windows Internet Naming Service，Windows Internet 名称服务）服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 客户端需要进行 WINS 配置。为了使 DHCP 客户端实现主机名到IP地址的解析，DHCP服务器为客户端分配IP地址的同时可以指定WINS服务器地址。DHCP 地址池最多可以配置 8 个 WINS 服务器地址。WINS 服务器 1 优先级最高，WINS 服务器 8 优先级最低。

7、配置 DHCP 客户端的 TFTP 服务器地址及启动文件

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[客户机导入文件存放地址配置]菜单进入 DHCP 客户端的 TFTP 服务器地址及启动文件配置界面，如图 225 所示；

图 225 配置 DHCP 客户端的 TFTP 服务器地址及启动文件

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

DHCP 客户机启动时的导入文件名

配置范围：1~128 个字符

功能：配置 DHCP 服务器为 DHCP 客户端分配的启动文件名。无盘设备启动时，需要从服务器上下载导入启动文件。

导入文件服务器 1~导入文件服务器 8

功能：配置 DHCP 服务器为 DHCP 客户端分配的 TFTP 服务器地址。DHCP 地址池最多可以配置 8 个导入文件服务器。导入文件服务器 1 优先级最高，导入文件服务器 8 优先级最低。

8、配置 DHCP 地址池网络参数

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[DHCP 网络参数配置]菜单进入 DHCP 地址池网络参数配置界面，如图 226 所示；

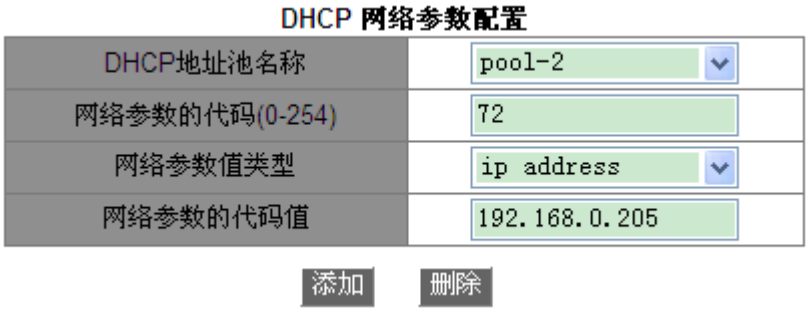


图 226 配置 DHCP 地址池网络参数

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

网络参数的代码

配置范围：0~254

功能：配置 DHCP Option 选项。DHCP 为了与 BootP 兼容，保留了 BootP 的消息格式。比 BootP 新增的功能，通过 Option 字段来实现。DHCP 通过 Option 字段传递控制信息和网络配置参数，实现 IP 地址分配的同时，为客户端提供更加丰富的配置信息。如 Option72 为 WWW 服务器选项，用来指定为客户端分配的 WWW 服务器地址。

说明：

- 更多 DHCP 选项的介绍，请参见 RFC2132；
- Web 界面提供了常用选项的配置（如网关地址、DNS 服务器地址、WINS 服务器地址等），网络参数代码不能配置为这些常用 Option 选项。

网络参数值类型

配置选项：ascii/hex/ip address

功能：配置网络参数值类型。ascii 为 ascii 字符串，配置范围为 1~255 个字符；hex 为十六进制数，配置长度范围为 1~510，且必须为偶数。

网络参数的代码值

功能：按照网络参数值类型，配置相应的网络参数值。

9、查询 DHCP 地址池信息

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[查询 DHCP 地址池信息]菜单进入 DHCP 地址池信息查询界面，如图 227 所示；

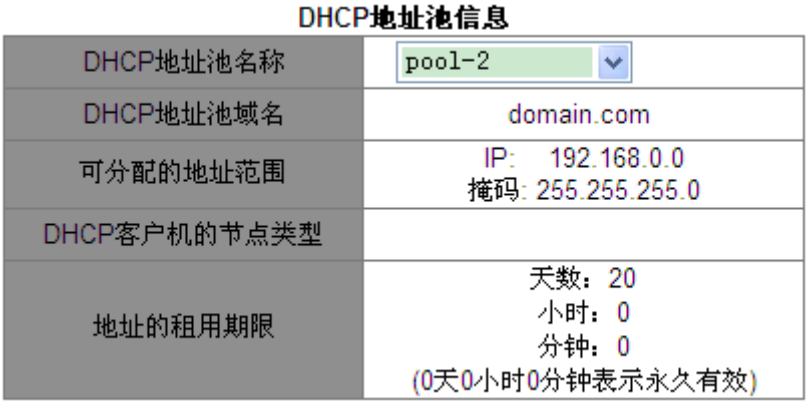


图 227 查询 DHCP 地址池信息

DHCP 地址池名称

功能：选择一个已创建的 DHCP 地址池。

10、配置 DHCP 地址池中不参与动态分配的 IP 地址

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[剔除动态分配地址配置]菜单进入 DHCP 地址池不参与动态分配的 IP 地址配置界面，如图 228 所示；

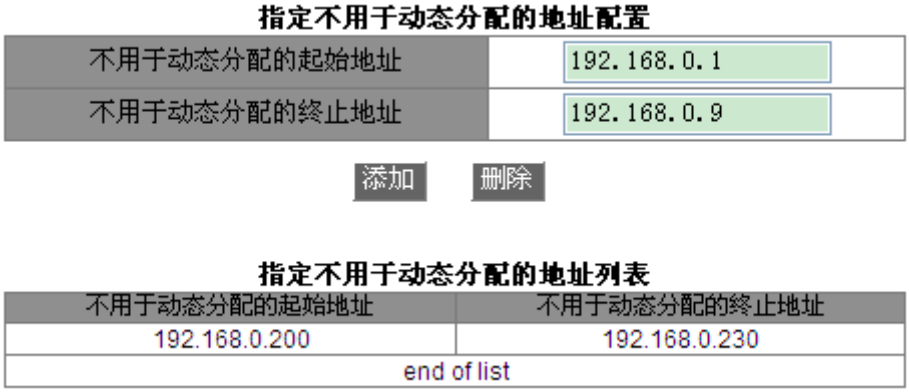


图 228 配置 DHCP 地址池中不参与动态分配的 IP 地址

不用于动态分配的起始地址/不用于动态分配的终止地址

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

11、统计 DHCP 数据包信息

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 服务器配置]→[DHCP 数据包的统计信息]菜单进入 DHCP 数据包信息统计界面，如图 229 所示；

DHCP数据包的统计信息

配置的DHCP地址池个数	2
代理数据库的个数	0
自动分配地址的个数	1
手工绑定地址的个数	-1
有地址冲突的个数	0
绑定超期的个数	2
错误报文	546

接收DHCP数据包的统计

接收的数据包总数	3395
DHCPDISCOVER包个数	1226
DHCPREQUEST包个数	1724
DHCPDECLINE包个数	24
DHCPRELEASE包个数	7
DHCPINFORM包个数	412

发送DHCP数据包的统计

发送的数据包的总数	2580
DHCPOFFER包的个数	1162
DCHPACK包的个数	562
DHCPNAK包的个数	570
DHCPRELAY包的个数	0
DHCPFORWARD包的个数	0

清空统计信息　　刷新统计信息

图 229 统计 DHCP 数据包信息

点击<刷新统计信息>按钮，可以实时更新获取 DHCP 数据包统计信息；点击<清空统计信息>按钮，可以清空接收/发送 DHCP 数据包的统计信息。

12、显示静态绑定信息

点击导航树[设备高级配置]→[DHCP 配置]→[DHCP 排错]→[显示 IP 与 MAC 绑定情况]菜单进入静态绑定信息查看界面，如图 230 所示；

反馈信息窗口

```
IP address              Hardware adress         Lease expiration
Type
192.168.0.23            44-37-E6-88-6E-90       Infinite
Manual
192.168.0.6             00-1E-CD-19-00-02       Infinite
Manual
Total dhcp binding items: 2, the matched: 2
```

图 230 查看静态绑定信息

6.12.1.4 典型配置举例

如图 231 所示，交换机 A 作为 DHCP 服务器，交换机 B 作为 DHCP 客户端，交换机 A 的 3 端口连接交换机 B 的 4 端口。客户端发出申请 IP 地址请求报文，服务器可以通过两种方式为客户端分配 IP 地址。DHCP 服务器动态分配 IP 地址时，192.168.0.1~192.168.0.9 范围的 IP 地址不参与动态分配。

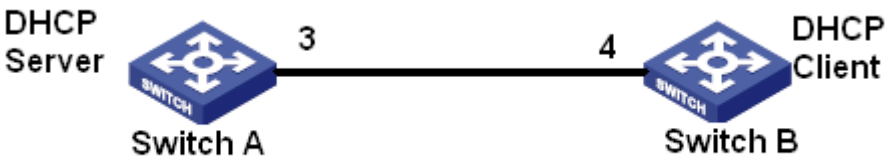


图 231 DHCP 典型配置举例

静态分配 IP 地址方式

➢ 交换机 A 的配置：

1、打开 DHCP 服务器状态，见图 218；

2、创建地址池 pool-1，见图 219；

3、绑定交换机 B 的 MAC 地址：00-1e-cd-19-00-02 与 IP 地址：192.168.0.6，掩码：255.255.255.0，见图 220；

➢ 交换机 B 的配置：

1、交换机 B 获取 IP 地址方式为 bootp-client 或 dhcp-client，见图 132；

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 232 所示；

图 232 DHCP 客户端获取 IP 地址-1

动态分配 IP 地址方式

➢ 交换机 A 的配置：

1、打开 DHCP 服务器状态，见图 218；

2、创建地址池 pool-2，地址池域名配置为 domain.com，可分配的地址范围为 192.168.0.3（IP）和 255.255.255.0（MASK）；租期为 20 天，见图 221；

3、配置不参与动态分配的 IP 地址范围 192.168.0.1~192.168.0.9，见图 228；

➢ 交换机 B 的配置：

1、交换机 B 获取 IP 地址方式为 bootp-client 或 dhcp-client，见图 132；

2、DHCP 服务器从地址池中顺序查找可供分配的 IP 地址，把最先找到的 IP 地址：192.168.0.10，子网掩码：255.255.255.0 分配给交换机 B，如图 233 所示；

三层接口IP配置

接口	IP地址	子网掩码	状态
Vlan1	0.0.0.0	0.0.0.0	no shutdown

添加 删除

Vlan1		
IP地址	子网掩码	类型
192.168.0.10	255.255.255.0	(Primary)

图 233 DHCP 客户端获取 IP 地址-2

6.13 ACL 配置

6.13.1 介绍

ACL(Access Control List，访问控制列表)通过对交换机端口入方向的报文配置匹配规则和处理操作方式可以对报文进行过滤，有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。

6.13.2 ACL 表项与规则

一条 ACL 表项可以包含多个规则，而每个规则都指定不同的报文匹配选项以及对报文的处理动作。在配置规则之前需要先创建 ACL 表项。同一条 ACL 表项的多个规则中，规则号小的优先级高，对报文的动作从第一条规则开始匹配，直到匹配到一条规则，其后的规则将不再进行匹配。

ACL 表项可以应用到端口、VLAN 和全局，当多个表项有冲突时，端口应用优先级最高，全局应用优先级最低。例如，配置 ACL1 表项（丢弃目的 IP 为 192.168.0.3 的报文）应用到

全局；配置 ACL2 表项（接收目的 IP 为 192.168.0.3 的报文）应用到 VLAN1；配置 ACL3 表项（镜像目的 IP 为 192.168.0.3 的报文）应用到端口 2/1，端口 2/1 属于 VLAN1。对于端口 2/1，由于端口应用优先级高于 VLAN 应用优先级，所以端口 2/1 镜像目的 IP 为 192.168.0.3 的报文。对于 VLAN1，由于 VLAN 应用高于全局应用，所以 VLAN1 接收目的 IP 为 192.168.0.3 的报文。其余情况丢弃目的 IP 为 192.168.0.3 的报文。

由于 ACL 表项是一条或多条规则的集合，所以将一条 ACL 表项应用到端口/VLAN/全局后，所有属于该 ACL 的规则都会应用到该端口/VLAN/全局。

同一端口/VLAN/全局下应用的 ACL 优先级默认采用先下发先生效，用户可根据需要调整 ACL 表项的优先级。

6.13.3 Web 页面配置

1、配置 ACL 表项

点击导航树[设备高级配置]→[ACL 配置]→[ACL 基本配置]菜单进入 ACL 表项配置界面，如图 234 所示；

图 234 ACL 表项配置

ACL ID

配置范围：1~1024

功能：配置 ACL 表项 ID。

描述：该产品最多支持 512 条 ACL 表项，如果将表项应用到多个端口，则每个端口下的应用为一条 ACL 表项；同理，如果将表项应用到多个 VLAN，则每个 VLAN 下的应用为一条 ACL 表项。

说明：如果应用到多个连续的端口或 VLAN 时，可使用“-”隔开；如果应用到多个不连续的端口或 VLAN 时，可使用“,”隔开。

注意：

由于设备存在一些系统 ACL 表项，所以用户实际上可配置的 ACL 表项小于 512 条。

描述

配置范围：1~127 个字符

功能：为 ACL 表项添加描述信息。

入方向 VLAN /入方向端口/全局

功能：配置该 ACL 表项的应用范围。

2、编辑 ACL 表项，如图 235 所示；

图 235 修改 ACL 表项

选中一条 ACL 表项，点击<删除>按钮可删除该表项；点击<编辑>按钮可修改该 ACL 表项配置。

3、为 ACL 表项添加规则

点击图 234 中已创建的一条表项，进入图 236 所示界面，点击下方<添加规则>按钮配置 ACL 表项规则。

图 236 ACL 信息显示

4、配置 ACL 表项规则，如图 237 所示；

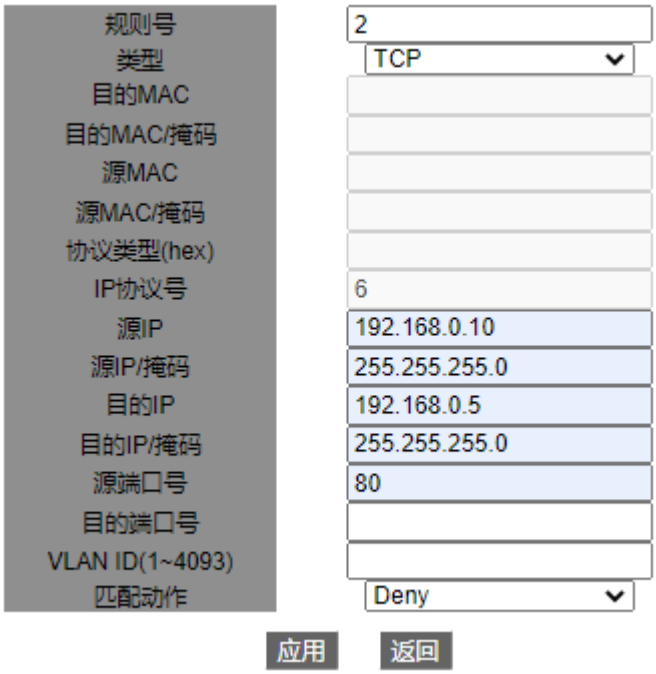


图 237 ACL 规则配置

规则号

配置范围：1~1024

功能：配置 ACL 表项的规则号。

描述：每条 ACL 表项最多支持 512 条规则，并且所有 ACL 下的规则数总和不能超过 512。

类型

配置选项：自定义/IGMP/ICMP/TCP/UDP/MAC

默认配置：自定义

功能：配置 ACL 规则的报文类型。

目的 MAC/目的 MAC 掩码

功能：配置规则的目的 MAC 地址信息。目的 MAC 掩码中为 1 代表关心的目的 MAC 地址位，为 0 的代表忽略的目的 MAC 地址位。

源 MAC/源 MAC 掩码

功能：配置规则的源 MAC 地址信息。源 MAC 掩码中为 1 代表关心的源 MAC 地址位，为 0 代表忽略的源 MAC 地址位。

协议类型（hex）

配置范围：5DD-FFFF

功能：配置规则的协议类型。

IP 协议号

配置范围：0~255

功能：配置规则的 IP 协议号。

源 IP/源 IP 掩码

功能：配置规则的源 IP 地址信息。源 IP 掩码中为 1 代表关心的源 IP 地址位，为 0 代表忽略的源 IP 地址位。

目的 IP/目的 IP 掩码

功能：配置规则的目的 IP 地址信息。目的 IP 掩码中为 1 代表关心的目的 IP 地址位，为 0 的代表忽略的目的 IP 地址位。

源端口号

配置范围：0~65535

功能：配置规则的源端口号。

目的端口号

配置范围：0~65535

功能：配置规则的目的端口号。

VLAN ID

配置选项：1~4093

功能：配置规则的 VLAN ID。

匹配动作

配置选项：Permit/Deny/Mirror to CPU/ Mirror to Port/Redirect to CPU/ Redirect to Port

默认配置：Permit

功能：配置匹配成功的报文的处理方式。

描述：Permit 代表接收匹配成功的报文；Deny 代表丢弃匹配成功的报文；Mirror to CPU 代表接收匹配成功的报文并镜像到 CPU；Mirror to Port 代表接收匹配成功的报文并镜像到指定端口；Redirect to CPU 代表重定向匹配成功的报文到 CPU；Redirect to Port 代表重定向匹配成功的报文到指定端口。

5、查询 ACL 表项

点击导航树[设备高级配置]→[ACL 配置]→[ACL 查询与下发]菜单进入 ACL 表项查询界面，如图 238 所示；

图 238 ACL 查询

应用对象

配置选项：全局/端口/VLAN

功能：选择要查询的 ACL 表项应用范围。

入方向端口

功能：当应用对象选择端口时，选择要查询 ACL 表项的应用端口。

入方向 VLAN

功能：当应用对象选择 VLAN 时，选择要查询 ACL 表项的应用 VLAN。

下方右侧的 ACL 列表中显示查询的 ACL 表项。

6、基于某一应用对象下发 ACL 表项并配置 ACL 表项优先级，如图 239 所示；

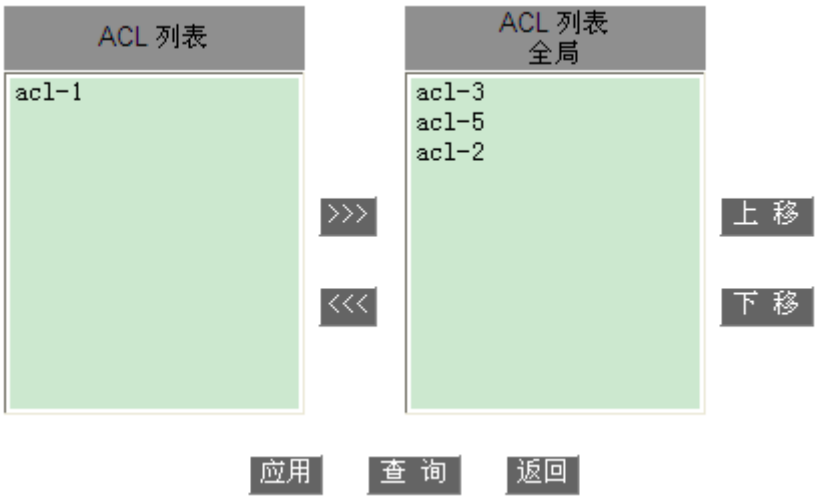


图 239 配置 ACL 表项优先级

移动需要下发到该应用对象的 ACL 表项到右侧列表中，选中表项，点击<上移>/<下移>按钮重新排列该应用对象下的 ACL 表项优先级，列表中从上到下，ACL 表项的优先级依次降低。

6.13.4 典型配置举例

端口 2/1 丢弃 192.168.1.0 网段的主机向 192.168.0.0 网段的主机发送源端口号为 80 的 TCP 报文。

配置如下：

1、配置 ACL 表项 1 应用到端口 2/1，如图 234 所示；

2、配置 ACL 规则，类型选择 TCP；源 IP 为 192.168.1.5，源 IP 掩码为 255.255.255.0；目的 IP 为 192.168.0.5，目的 IP 掩码为 255.255.255.0；源端口号为 80；匹配动作为 deny，如图 237 所示。

6.14 QoS 配置

6.14.1 介绍

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

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。

6.14.2 QoS CAR

QoS CAR（Committed Access Rate，约定访问速率）是一种限速策略，引用 ACL 规则进行流识别，对匹配的报文进行端口限速，丢弃报文中超出 QoS 策略规定范围（带宽和突发值）的流量。

6.14.3 QoS Remark

QoS Remark 引用 ACL 规则进行流识别，为匹配的报文重新指定优先级（DSCP 或 COS 值）。

6.14.4 QoS

该系列交换机每个端口有 8 个缓存队列，依次为队列 0、1、2、3、4、5、6、7，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，根据该帧头信息中的优先级值决定报文应存放的队列。该系列交换机支持两种优先级队列映射模式：CoS 和 DSCP。

- CoS 值取决于报文中 802.1Q 的优先级部分，CoS 值与队列的映射关系可以配置。
- DSCP 值取决于报文中的 TOS/DSCP 部分，DSCP 值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 8 个队列中的数据以及每个队列所占用的带宽。该系列交换机支持两种 QoS 队列调度模式：权重式 WRR(Weighted Round Robin，加权轮询调度)和优先级队列(priority-queue，优先级队列调度)。

- 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。

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

6.14.5 Web 页面配置

1、使能 QoS 功能

点击导航树[设备高级配置]→[QoS 配置]→[启动 QoS 功能]→[QoS 开关配置]菜单进入 QoS 全局使能界面，如图 240 所示；

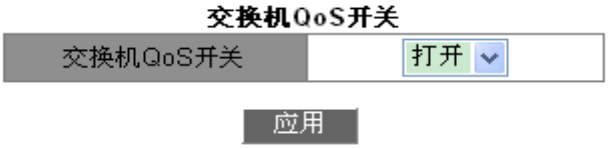


图 240 使能 QoS 功能

交换机 QoS 开关

配置选项：打开/关闭

默认配置：关闭

功能：是否全局使能 QoS 功能。

2、创建/删除分类表

点击导航树[设备高级配置]→[QoS 配置]→[分类表配置]→[添加删除分类表]菜单进入分类表创建/删除界面，如图 241 所示；

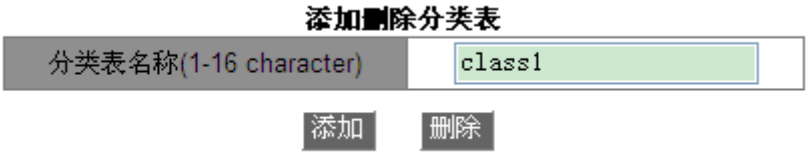


图 241 创建/删除分类表

分类表名称

配置范围：1~16 个字符

功能：配置分类表名称。点击<添加>/<删除>按钮，可创建/删除分类 port 表。

3、配置分类表匹配标准

点击导航树[设备高级配置]→[QoS 配置]→[分类表配置]→[分类表配置]菜单进入分类表匹配标准配置界面，如图 242 所示；

图 242 分类表匹配标准配置

分类表名称

配置选项：已创建的分类表。

匹配标准

默认配置：access-group 1st

功能：配置分类表中的匹配标准。

匹配标准值 1

配置范围：961~1024

功能：匹配指定的 ACL 表项。被匹配的 ACL 表项，动作只能配置为 permit。

操作类型

配置选项：设置/删除

功能：设置/删除分类表的匹配标准。

4、创建/删除策略表

点击导航树[设备高级配置]→[QoS 配置]→[策略表配置]→[添加删除策略表]菜单进入策略表创建/删除界面，如图 243 所示；

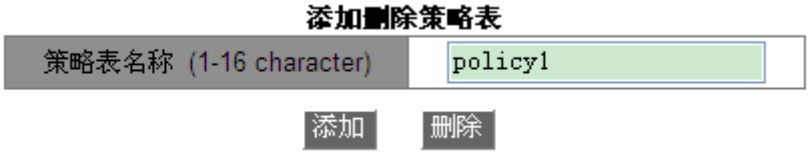


图 243 创建/删除策略表

策略表名称

配置范围：1~16 个字符

功能：配置策略表名称。点击<添加>/<删除>按钮，可创建/删除策略表。

5、配置策略表中限速策略

点击导航树[设备高级配置]→[QoS 配置]→[策略表配置]→[策略表带宽配置]菜单进入策略表限速配置界面，如图 244 所示；

图 244 限速策略配置

策略表名称

配置选项：已创建的策略表。

分类表名称

配置选项：已创建的分类表。

配置带宽

配置选项：1~10000000 kbit/s

功能：配置流量平均速率值。

配置突发值

配置选项：11000-1000000 byte

功能：配置流量突发。

配置超出带宽策略

配置选项：丢包

功能：满足分类表匹配标准的报文中超出限速值的部分，将采取丢包策略。

操作类型

配置选项：设置/删除

功能：配置/删除策略表中当前限速策略。

6、配置策略表中优先级重标记策略

点击导航树[设备高级配置]→[QoS 配置]→[策略表配置]→[策略表优先级配置]菜单进入策略表优先级配置界面，如图 245 所示；

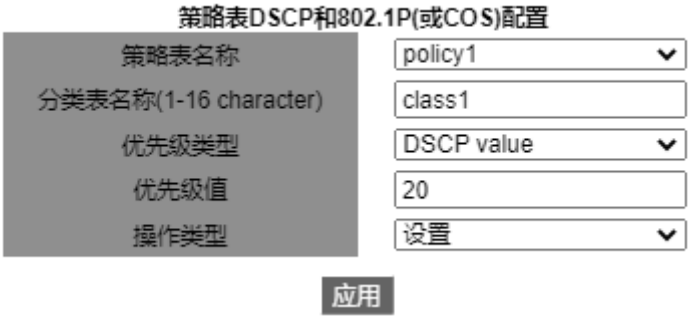


图 245 优先级策略配置

策略表名称

配置选项：已创建的策略表。

分类表名称

配置选项：已创建的分类表。

优先级类型

配置选项：DSCP value/COS value

功能：选择需要重标记的优先级类型。

优先级值

配置选项：0~63（DSCP value）/0~7（COS value）

功能：配置优先级的重标记值。

描述：满足分类表匹配标准的报文中优先级值，将采取重标记策略

操作类型

配置选项：设置/删除

功能：配置/删除策略表中当前重标记策略。

7、应用策略表到交换机端口

点击导航树[设备高级配置]→[QoS 配置]→[将 QoS 应用到端口]→[端口上应用一个策略表]菜单进入端口应用策略表配置界面，如图 246 所示；

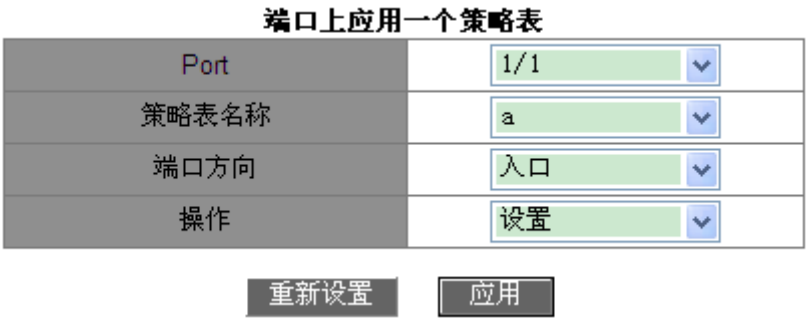


图 246 应用策略表到交换机端口

策略表名称

配置选项：已创建的策略表。

端口方向

配置选项：入口

功能：在端口入方向应用该策略表，从而实现对端口接收的报文进行限速或优先级重标记。

操作类型

配置选项：设置/删除

功能：配置/删除端口应用策略表。

注意：

- 每个端口只能应用一个策略表；
- 端口信任状态和端口应用策略表配置互斥；

8、配置端口信任模式

点击导航树[设备高级配置]→[QoS 配置]→[将 QoS 应用到端口]→[配置端口的信任模式]菜单进入端口信任模式配置界面，如图 247 所示；

图 247 端口信任模式配置

端口

配置选项：交换机上所有端口

端口的信任状态

配置选项：cos/cos and pass through dscp/dscp/dscp and pass through cos/port

默认配置：如果端口接收的报文是 IP 报文，则默认 dscp；否则如果报文为 Tag 类型，则默认 cos；如果报文为 Untag 类型，端口没有默认的信任模式，此时端口接收的报文默认存放到队列 0。

功能：配置交换机端口的信任状态。

描述：cos 和 cos and pass through dscp 都指端口信任 CoS 值，按照 CoS 值和队列的映射关系决定该端口接收的报文应存放的队列，如果报文中没有 CoS 值，则按照 CoS 值等于 0 来进行映射。区别在于：cos 指转发报文时按照 CoS 值到 DSCP 值的映射关系把报文中 DSCP 值修改为该 CoS 值映射的 DSCP 值；cos and pass through dscp 转发报文时不修改报文中的 DSCP 值。

dscp 和 dscp and pass through cos 都指端口信任 DSCP 值，按照 DSCP 值和队列的映射关系决定该端口接收的报文应存放的队列，如果报文中没有 DSCP 值，则按照 DSCP 值等于 0 来进行映射。区别在于：dscp 指转发报文时按照 DSCP 值到 CoS 值的映射关系把报文中的 CoS 值修改为该 DSCP 值映射的 CoS 值；dscp and pass through cos 转发报文时不修改报文中的 CoS 值。

9、配置端口缺省 CoS 值

点击导航树[设备高级配置]→[QoS 配置]→[将 QoS 应用到端口]→[配置端口的缺省 CoS 值]菜单进入端口缺省 CoS 值配置界面，如图 248 所示；

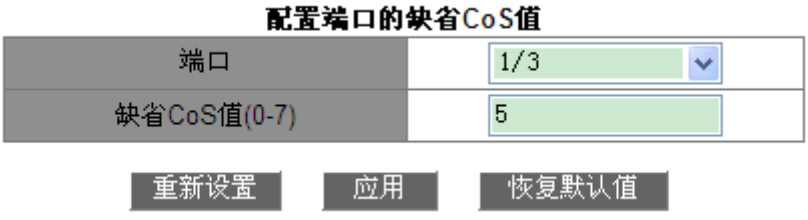


图 248 端口缺省 COS 值配置

端口

配置选项：交换机上所有端口

缺省 CoS 值

配置选项：0~7

默认配置：0

功能：配置端口缺省 CoS 值。

说明：当报文为 Untag 类型时，进入交换机后添加的 Tag 标记中优先级值为端口缺省 CoS 值。

10、配置端口的出队列模式

点击导航树[设备高级配置]→[QoS 配置]→[端口出队列配置]→[设置端口出队模式]菜单进入队列模式配置界面，如图 249 所示；

图 249 端口出队列模式配置

出队列工作模式

配置选项：PQ/WRR

默认配置：PQ

功能：配置指定端口的出队列工作模式。

11、配置端口出队列的权重 WRR

点击导航树[设备高级配置]→[QoS 配置]→[端口出队列配置]→[设置端口出队列的 WRR 权重]菜单进入权重 WRR 配置界面，如图 250 所示；

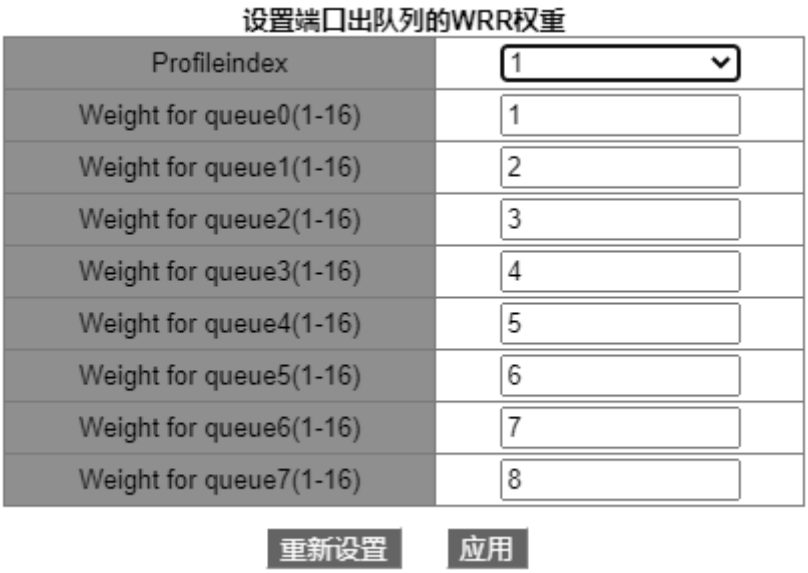


图 250 权重配置

Profileindex

配置选项：1~6

默认配置：1

功能：配置一组权重值。

说明：最多可以配置 6 组权重值。

{Weight for queue0, Weight for queue1, Weight for queue2, Weight for queue3, Weight for queue4, Weight for queue5, Weight for queue6, Weight for queue7}

配置选项：{0~15, 0~15, 0~15, 0~15, 0~15, 0~15, 0~15}

默认配置：{1, 2, 3, 4, 5, 6, 7, 8}

功能：配置该组权重值，绝对权重值是没有意义的，WRR 通过 8 个权重值的比率来分配带宽。

描述：如果有一个队列的权重值为 0，则此队列为最高优先级队列，其中的数据优先转发；如果有多个队列的权重值为 0，优先转发权重值为 0 的高优先级队列中的数据，再转发权重值为 0 的低优先级队列中的数据，当权重值为 0 的队列中数据转发完毕后，再按照权重比转发其他队列中的数据。

12、配置端口的队列调度模式为 WRR，并绑定端口采用的权重值组号，如图 251 所示；

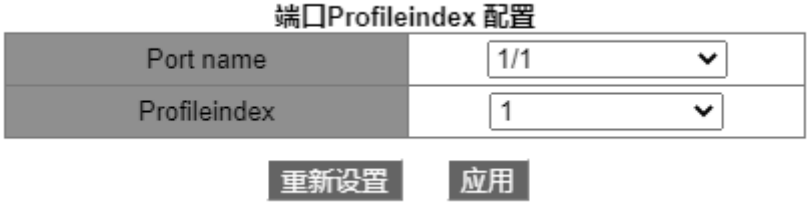


图 251 WRR 调度模式配置

Port name

配置选项：交换机上所有端口

功能：选择配置调度模式为 WRR 的端口。

Profileindex

配置选项：1~6

功能：选择端口采用的 WRR 权重比。

13、配置 CoS 值和队列的映射关系

点击导航树[设备高级配置]→[QoS 配置]→[端口出队列配置]→[设置 CoS 值对应端口出队列的映射]菜单进入 CoS 和队列映射关系配置界面，如图 252 所示；

图 252 配置 COS 值和队列的映射关系

{CoS value，Queue-ID}

配置选项：{0~7，0~7}

默认配置：CoS 值 0 映射到队列 0；CoS 值 1 映射到队列 1；CoS 值 2 映射到队列 2；CoS 值 3 映射到队列 3；CoS 值 4 映射到队列 4；CoS 值 5 映射到队列 5；CoS 值 6 映射到队列 6；CoS 值 7 映射到队列 7；

功能：配置 CoS 值和队列的映射关系。

说明：每个 CoS 值只能映射到一个队列中；可以多个 CoS 值映射到同一队列中。

14、配置 DSCP 值和队列的映射关系

点击导航树[设备高级配置]→[QoS 配置]→[端口出队列配置]→[设置 DSCP 值对应端口出队列的映射]菜单进入 DSCP 和队列映射关系配置界面，如图 253 所示；

图 253 配置 DSCP 值和队列的映射关系

{DSCP，Queue value}

配置选项：{0~63，0~7}

默认配置：DSCP 值 0~7 映射到队列 0；DSCP 值 8~15 映射到队列 1；DSCP 值 16~23 映射到队列 2；DSCP 值 24~31 映射到队列 3；DSCP 值 32~39 映射到队列 4；DSCP 值 40~47 映射到队列 5；DSCP 值 48~55 映射到队列 6；DSCP 值 56~63 映射到队列 7

功能：配置 DSCP 值和队列的映射关系。

说明：每个 DSCP 值只能映射到一个队列中，可以多个 DSCP 值映射到同一队列中。

点击<设置>新建 DSCP 值和队列的映射关系；<删除>则恢复 DSCP 值和队列的默认映射关系。

15、配置 CoS 值到 DSCP 值的映射关系

点击导航树[设备高级配置]→[QoS 配置]→[配置 QOS 映射关系]→[CoS-to-DSCP 映射]菜单进入 COS 值到 DSCP 值的映射关系配置界面，如图 254 所示；

CoS-to-DSCP 映射

CoS value	0	1	2	3	4	5	6	7
DSCP value(0-63)	0	11	22	33	44	55	63	0

设置 删除

图 254 配置 COS 值到 DSCP 值的映射关系

DSCP value

配置选项：0~63

默认配置：CoS 值 0 映射到 DSCP 值 0；CoS 值 1 映射到 DSCP 值 8；CoS 值 2 映射到 DSCP 值 16；CoS 值 3 映射到 DSCP 值 24；CoS 值 4 映射到 DSCP 值 32；CoS 值 5 映射到 DSCP 值 40；CoS 值 6 映射到 DSCP 值 48；CoS 值 7 映射到 DSCP 值 56

功能：配置 CoS 值到 DSCP 值的映射关系。当端口信任模式选择 CoS 时，根据此映射关系来修改报文中的 DSCP 值。

说明：可以多个 CoS 值映射到同一个 DSCP 值。

点击<设置>新建 CoS 值到 DSCP 值的映射关系；<删除>恢复 CoS 值到 DSCP 值的默认映射关系。

16、配置 DSCP 值到 CoS 值的映射关系

点击导航树[设备高级配置]→[QoS 配置]→[配置 QOS 映射关系]→[DSCP-to-CoS 映射]菜单进入 DSCP 值到 CoS 值的映射关系配置界面，如图 255 所示；

DSCP-to-CoS 映射

DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS	DSCP	CoS
0	0	8	1	16	2	24	3	32	4	40	5	48	6	56	7
1	0	9	1	17	2	25	3	33	4	41	5	49	6	57	7
2	0	10	1	18	2	26	3	34	4	42	5	50	6	58	7
3	0	11	1	19	2	27	3	35	4	43	5	51	6	59	7
4	0	12	1	20	2	28	3	36	4	44	5	52	6	60	7
5	0	13	1	21	2	29	3	37	4	45	5	53	6	61	7
6	0	14	1	22	2	30	3	38	4	46	5	54	6	62	7
7	0	15	1	23	2	31	3	39	4	47	5	55	6	63	7

设置 恢复默认值

图 255 配置 DSCP 值到 COS 值的映射关系

{DSCP value,COS value}

配置选项：{0~63，0~7}

默认配置：DSCP 值 0~7 映射到 CoS 值 0；DSCP 值 8~15 映射到 CoS 值 1；DSCP 值

16~23 映射到 CoS 值 2；DSCP 值 24~31 映射到 CoS 值 3；DSCP 值 32~39 映射到 CoS 值 4；DSCP 值 40~47 映射到 CoS 值 5；DSCP 值 48~55 映射到 CoS 值 6；DSCP 值 56~63 映射到 CoS 值 7

功能：配置 DSCP 值到 CoS 值的映射关系。当端口信任模式选择 DSCP 时，根据此映射关系来修改报文中的 CoS 值

说明：最多可以 8 个 DSCP 值映射到同一个 CoS 值。

点击<设置>新建 DSCP 值到 CoS 值的映射关系；<删除>恢复 DSCP 值到 CoS 值的默认映射关系。

17、配置 DSCP 值到 DSCP 值的映射关系

点击导航树[设备高级配置]→[QoS 配置]→[配置 QOS 映射关系]→[DSCP-to-DSCP 转换映射]菜单进入 DSCP 值到 DSCP 值的映射关系配置界面，如图 256 所示；

图 256 DSCP 值到 DSCP 值的映射关系

DSCP 转换表名称（1-16 字符）

配置范围：1~16 个字符

功能：配置 DSCP 转换表名称。

{入方向，出方向 }

配置选项：{0~63，0~63}

功能：配置 DSCP 值到 DSCP 值的映射关系，如果想改变报文中 DSCP 值时，可以通过该映射关系修改出端口转发报文的 DSCP 值。

说明：最多可以 8 个 DSCP 值映射到同一个 DSCP 值。

点击<设置>新建 DSCP 值到 DSCP 值的映射关系；<删除>取消 DSCP 值到 DSCP 值的映射关系。最多可创建 28 个 DSCP 映射关系表。

注意：

报文的存放队列按照报文中原始的 DSCP 值和队列的映射关系来决定。

18、配置端口应用 DSCP 转换映射关系

点击导航树[设备高级配置]→[QoS 配置]→[将 QOS 应用到端口]→[端口上应用 DSCP 转换映射]菜单进入端口应用 DSCP 转换映射关系配置界面，如图 257 所示；

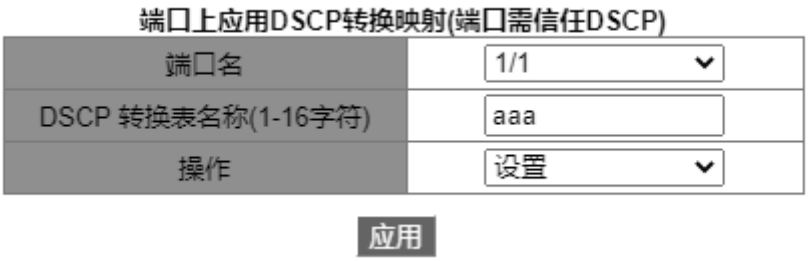


图 257 端口应用 DSCP 转换映射关系

端口名

配置选项：交换机上所有端口

功能：选择应用 DSCP mutation 映射关系的端口。

DSCP 转换表名称

配置选项：已创建的 DSCP 值到 DSCP 值的映射关系表名称

功能：配置该端口采用的 DSCP mutation 映射关系表。

操作

配置选项：设置/删除

功能：添加/删除当前端口应用的 DSCP mutation 映射关系。

6.14.6 典型配置举例

如图 258 所示，port1~port4 向 port5 转发报文，其中：

port1 接收的报文 DSCP 值为 6，信任模式为 DSCP pass CoS，进入 port1 的报文映射到队列 3 中；

port2 接收的报文中 CoS 值为 2，信任模式为 CoS pass DSCP，进入 port2 的报文映射到队列 1 中；

port3 接收的报文中 CoS 值为 2，DSCP 值为 32，信任模式为 DSCP，进入 port3 的报文映射到队列 2 中；

port4 接收的报文中 DSCP 值为 26，CoS 值为 3，信任模式为 CoS，进入 port4 的报文映射到队列 3 中；

port5 采用 WRR 调度模式。

交换机配置过程：

1、启动 QoS 功能，见图 240；

2、配置端口 1 信任模式为 DSCP pass CoS，端口 2 信任模式为 CoS pass DSCP，端口 3 的信任模式为 DSCP，端口 4 的信任模式为 CoS，见图 247；

3、CoS 值到 DSCP 值的映射和 DSCP 值到 CoS 值的映射都采用默认映射关系，即端口 port3 转发报文时，修改 CoS 值为 4，端口 port4 转发报文时，修改 DSCP 值为 24；

4、配置 CoS 值 2 和 3 分别映射到队列 1 和 3 中，见图 252；

5、配置 DSCP 值 6 和 32 分别映射到队列 3 和 2 中，见图 253；

6、配置端口 5 出队列模式为 WRR，见图 249；采用默认队列权重比，见图 251；

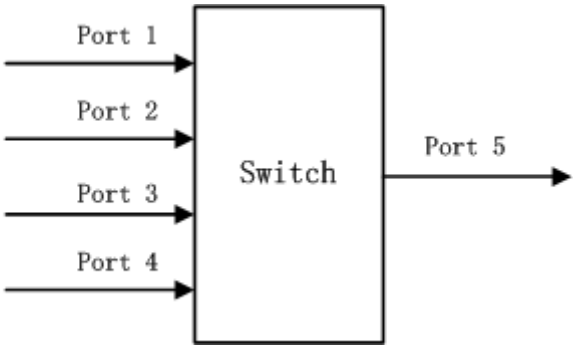


图 258 QoS 配置举例

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＝3，队列 3 的权重＝4，那么入队列 1 的报文分配的带宽比例为：2/(2+3+4)，入队列 2 报文分配的带宽比例为：3/(2+3+4)，入队列 3 报文分配的带宽比例为：4/(2+3+4)。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 4/(2+3+4)。

6.15 IEC61850 配置

6.15.1 介绍

目前交换机在变电站网络中，被变电站功能主体透明化。监控需要使用 IEC61850 之外的工具（协议），如 EMS、WEB、CLI、OPC 等。导致知识点，配置点分散、不统一、不方便。

为解决这些问题，按照 IEC61850 规约进行建模，将交换机作为智能电子设备（IED，Intelligent Electronic Device）纳入到变电站自动化系统中（IEC61850）。统一变电站自动化监控视图，方便用户的集成管理方案规划，节约施工成本，节省维护成本。

注意：

该交换机中已导入本公司提供的缺省建模文件 switch. cid，客户如需导入其他建模文件，请参考“文件传输服务”章节导入文件。

6.15.2 Web 页面配置

1、使能 IEC 61850 功能

点击导航树[设备高级配置]→[IEC 61850 配置]→[IEC 61850 配置]菜单进入 IEC 61850 配置界面，如图 259 所示；

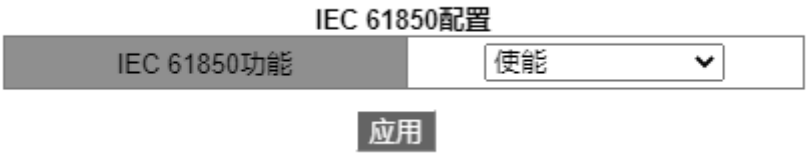


图 259 IEC61850 配置

IEC61850 功能

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 IEC61850 功能。

2、配置 IEC 61850 参数

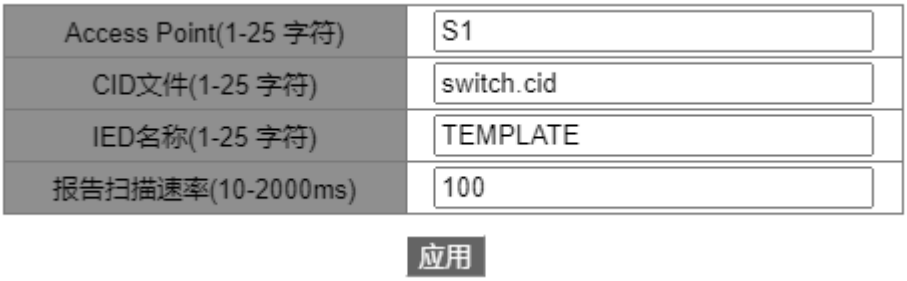


图 260 IEC61850 配置

Access Point

配置范围：1~25 个字符

默认配置：S1

功能：配置建模文件中本 IED 的访问点名称。

CID 文件

配置范围：1~25 个字符

默认配置：switch.cid

功能：指定 IEC61850 功能初始化时生效的建模文件。

IED 名称

配置范围：1~25 个字符

默认配置：TEMPLATE

功能：配置建模文件中本 IED 的逻辑设备名称。

报告扫描速率

配置范围：10~2000ms

默认配置：100ms

功能：配置扫描设备节点信息的时间间隔。

注意：

Access Point 和 IED 名称配置应和指定的建模文件中的 Access Point 和 IED 名称一致，否则导致 IEC61850 功能启动失败。

6.16 IGMP Snooping

6.16.1 介绍

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

6.16.2 基本概念

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

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

6.16.3 原理

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

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

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

成员报告报文：如果主机已经加入组播组，收到 IGMP 查询报文后会发送 IGMP report 报文响应查询报文，目的是报告自己还存在。如果主机想加入某个组播组时，会主动向 IGMP

查询器发送 IGMP report 报文从而加入感兴趣的组播组。IGMP report 报文的目的 IP 为所加入的组播组的 IP 地址。

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

6.16.4 Web 页面配置

1、使能 IGMP Snooping 协议

点击导航树[设备高级配置]→[组播协议配置]→[IGMP Snooping 配置]→[IGMP Snooping 使能]菜单进入 IGMP Snooping 全局配置界面，如图 261 所示；

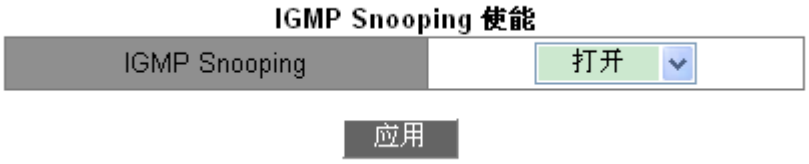


图 261 使能 IGMP Snooping

IGMP Snooping

配置选项：打开/关闭

默认配置：关闭

功能：是否全局使能 IGMP Snooping 协议，IGMP Snooping 与 GMRP 不能同时使能。

2、IGMP Snooping 配置

点击导航树[设备高级配置]→[组播协议配置]→[IGMP Snooping 配置]→[IGMP Snooping 配置]菜单进入 IGMP Snooping 配置界面，如图 262 所示；

图 262 IGMP Snooping 配置

VLAN ID

配置选项：已创建的所有 VLAN ID

Snooping 状态

配置选项：打开/关闭

默认配置：打开

功能：是否打开该 VLAN 的 IGMP Snooping 功能，打开此功能的前提必须打开全局 IGMP Snooping 功能。

静态 IP

配置格式：A.B.C.D

默认配置：192.168.0.2

功能：配置发送报文的源 IP 地址。

3、IGMP query 配置，如图 263 所示；

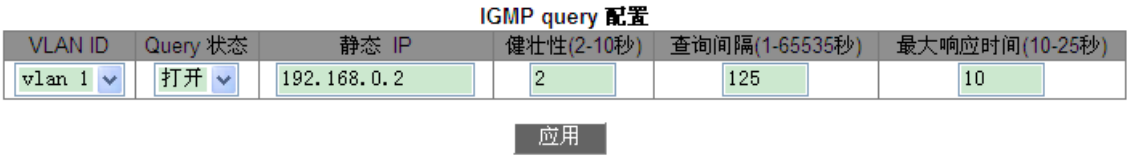


图 263 IGMP query 配置

VLAN ID

配置选项：已创建的所有 VLAN ID

功能：选择要启动 IGMP query 功能的 VLAN ID。

Query 状态

配置选项：打开/关闭

默认配置：关闭

功能：是否打开该 VLAN 的 IGMP query 功能，打开此功能的前提必须打开全局 IGMP Snooping 功能。

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

注意：

同一 VLAN 中 Query 和 Snooping 功能互斥，即一个 VLAN 中打开 Query 必须关闭 Snooping，打开 Snooping 必须关闭 Query。

静态 IP

配置格式：A.B.C.D

默认配置：192.168.0.2

功能：配置发送查询报文的源 IP 地址。

健壮性

配置范围：2~10

默认配置：2

功能：指定该 VLAN 内的 IGMP Query 功能的活力参数。

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

查询间隔

配置范围：1~65535s

默认配置：125s

功能：配置指定 VLAN 内发送查询报文的时间间隔。

最大响应时间

配置范围：10~25s

默认配置：10s

功能：配置指定 VLAN 内响应查询报文的最大响应时间。

配置完成后在下方“IGMP 配置”列表中显示 IGMP 配置信息，如图 264 所示；

IGMP 配置

VLAN ID	Snooping 状态	Query 状态	静态 IP	健壮性(秒)	查询间隔(秒)	最大响应时间(秒)
1	关闭	打开	192.168.0.2	2	125	10
2	打开	关闭	192.168.0.2	0	0	0

图 264 查看 IGMP 配置

4、IGMP Snooping 静态组播配置

点击导航树[设备高级配置]→[组播协议配置]→[IGMP Snooping 配置]→[IGMP Snooping 静态组播配置]菜单进入 IGMP Snooping 静态配置界面，如图 265 所示；

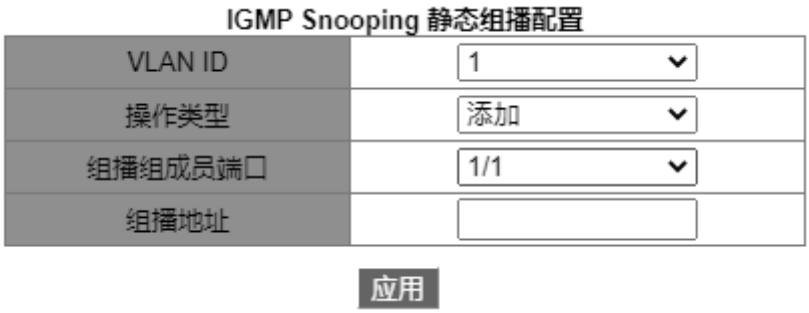


图 265 IGMP Snooping 静态组播配置

VLAN ID

配置选项：已创建的 VLAN ID

操作类型

配置选项：添加/删除

默认配置：添加

功能：添加/删除组播组中成员端口。

组播组成员端口

配置选项：交换机上所有端口

功能：选择要加入/离开组播组的成员端口，如果某端口所连接的主机需要固定接收某个组播组的数据，可以配置该端口静态加入组播组成为静态成员端口。

组播地址

配置范围：224.0.1.0~239.255.255.255

功能：输入组播组地址。

描述：当加入的静态组播地址已经动态学习到，则静态组播地址表项将覆盖动态组播地址表项。

5、查看组播表项

点击导航树[设备高级配置]→[组播协议配置]→[IGMP Snooping 配置]→[IGMP Snooping 查询]菜单进入组播表项查看界面，如图 266 所示；

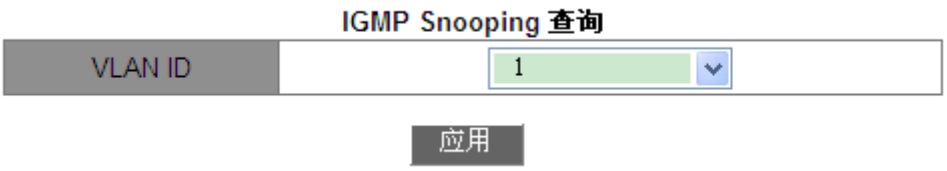


图 266 查看组播成员列表

查看选定 VLAN 中的组播表项。

6.16.5 典型应用举例

如图 267 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；

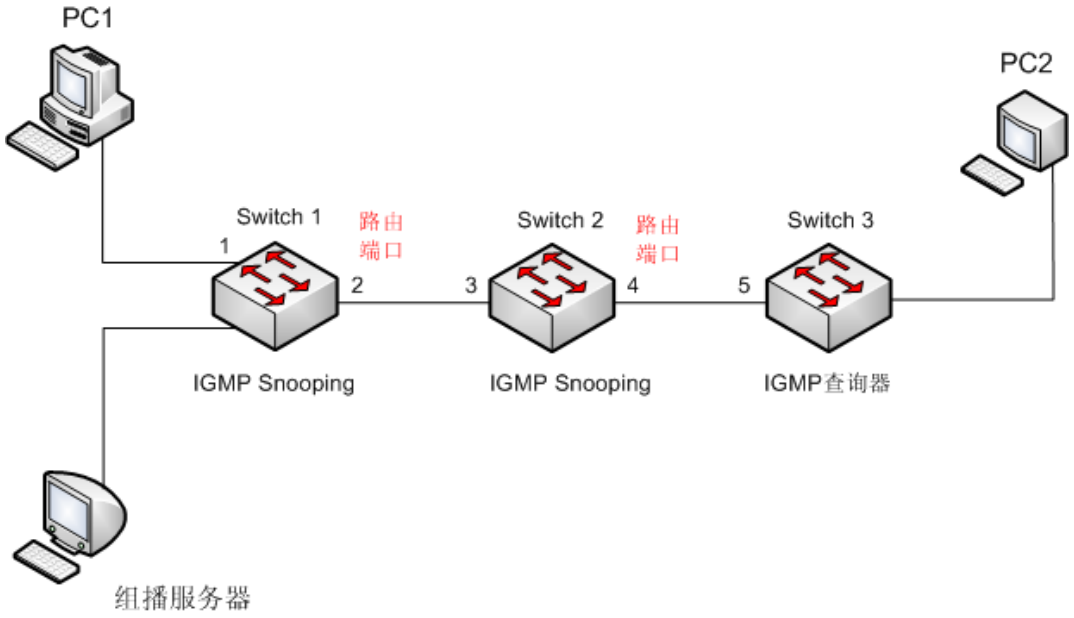


图 267 IGMP Snooping 应用举例

- 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。

6.17 GMRP

6.17.1 GARP 介绍

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

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

GARP 中起作用的消息有三类：Join、Leave、LeaveAll。

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

说明：

应用实体指使能该注册协议的端口。

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

Hold 定时器：当 GARP 应用实体接收到某注册信息时，不立即对外发送 Join 消息，而是启动 Hold 定时器，当该定时器超时后，将此时段内收到的所有注册信息放在一个 Join 消

息中向外发送，从而减少报文发送量有利于网络稳定。

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

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

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

6.17.2 GMRP 协议

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

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

6.17.3 说明

代理端口：使能 GMRP 功能和代理功能的端口；

扩散端口：只使能 GMRP 功能，没有使能代理功能的端口；

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

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

6.17.4 Web 页面配置

1、使能全局 GMRP 协议

点击导航树[设备高级配置]→[组播协议配置]→[GMRP 配置]→[GMRP 配置]菜单进入 GMRP 配置界面，如图 268 所示；

图 268 GMRP 全局配置表

GMRP 功能

配置选项：使能/禁止

默认配置：禁止

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

Leave-All 定时器

配置范围：600-327600ms

默认配置：10000ms

功能：发送 leave all 信息的时间间隔，必须是 100 的倍数。

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

2、配置每个端口的 GMRP 功能，如图 269 所示；

图 269 端口 GMRP 配置

端口名

配置选项：交换机上所有端口

GMRP 功能

配置选项：使能/禁止

默认配置：使能

功能：是否使能端口的 GMRP 功能。

GMRP 代理功能

配置选项：使能/禁止

默认配置：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 定时器

配置范围：100-163600ms

默认配置：100ms

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

Join 定时器

配置范围：200-163700ms

默认配置：500ms

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

Leave 定时器

配置范围：500-327500ms

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

点击导航树[设备高级配置]→[组播协议配置]→[GMRP 配置]→[GMRP 代理配置]菜单进入 GMRP 代理表项配置界面，如图 270 所示；

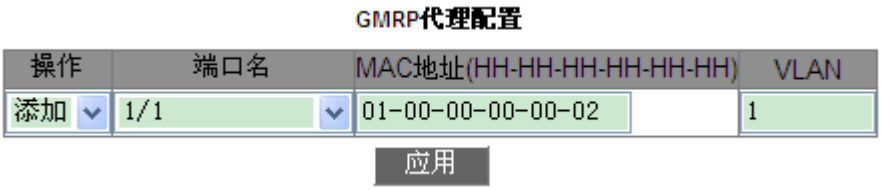


图 270 GMRP 代理表项配置

操作

配置选项：添加/删除

默认配置：添加

功能：选择对当前表项的操作。

端口名

配置选项：已配置的代理端口

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH (H 为一个十六进制数)

功能：配置组播组 MAC 地址，最高字节的最低位为 1 即可。

VLAN

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。

4、查看 GMRP 配置信息

点击导航树[设备高级配置]→[组播协议配置]→[GMRP 配置]→[GMRP 信息]菜单进入 GMRP 配置信息查看界面，如图 271 所示；

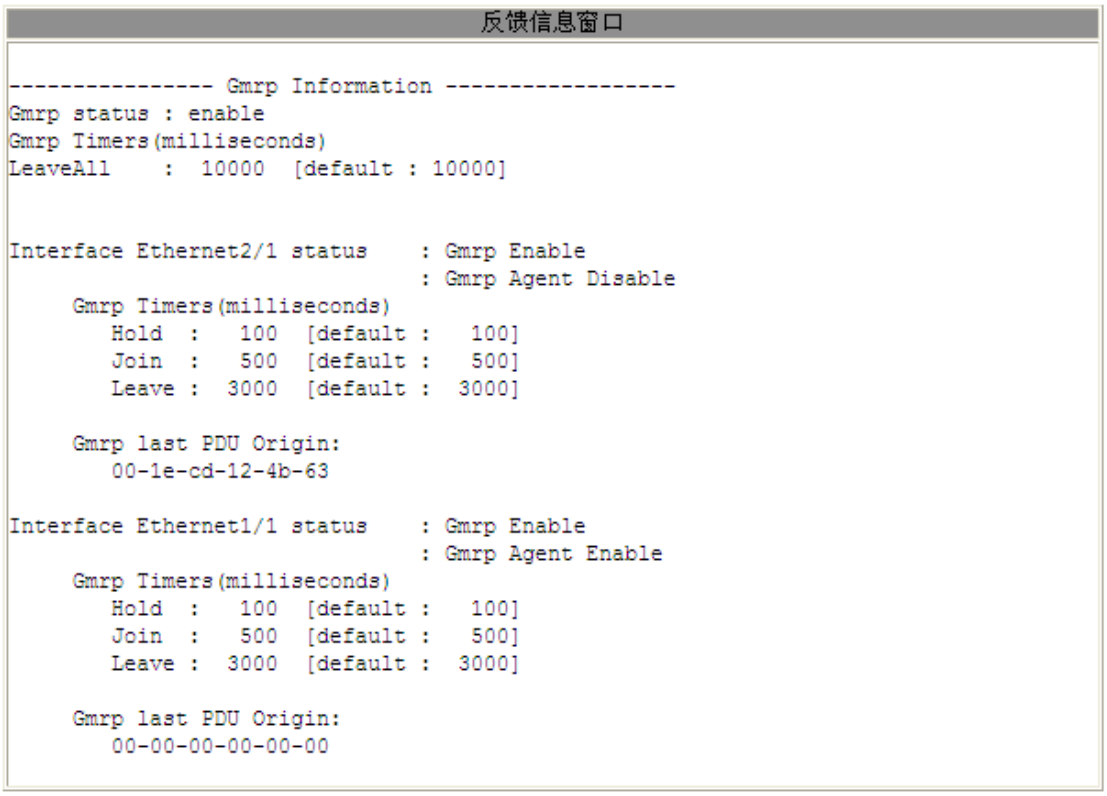


图 271 查看 GMRP 配置信息

5、查看 GMRP 代理表项

点击导航树[设备高级配置]→[组播协议配置]→[GMRP 配置]→[GMRP 代理信息]菜单进入 GMRP 代理表项查看界面，如图 272 所示；

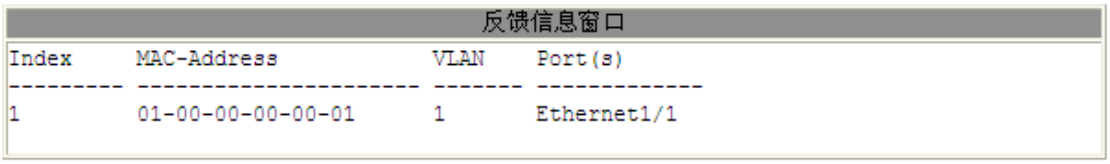


图 272 查看 GMRP 代理表项

6、在连接的相邻设备上查看该代理表项的组播成员，如图 273 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，并且该设备上的扩散端口应存在于代理表项的 VLAN ID 中。

GMRP动态组播表

序号	组播地址	VLAN ID	成员端口
1	01-00-00-00-00-02	1	2

图 273 GMRP 动态组播表

GMRP 动态组播

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。

6.17.5 典型配置举例

如图 274 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。

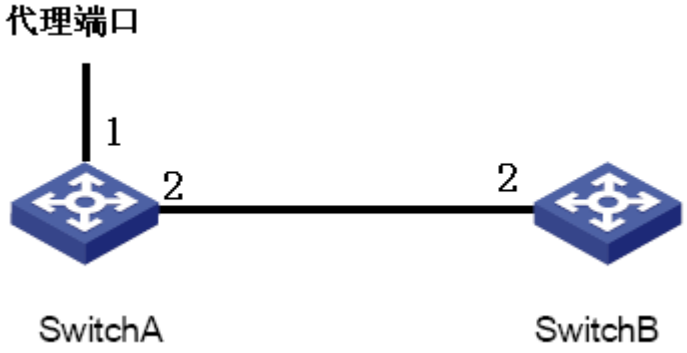


图 274 GMRP 组网图

交换机 A 配置过程：

1、使能交换机 A 的全局 GMRP 功能，LeaveAll 定时器采用默认值，见图 268；

2、使能端口 1 的 GMRP 功能和代理功能；使能端口 2 的 GMRP 功能，定时器的值都采用默认值，见图 269；

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 270；

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 268；

2、使能端口 2 的 GMRP 功能，定时器的值都采用默认值，见图 269；

交换机 B 上动态学习到的 GMRP 组播表项如表 13 所示；

表 13 动态组播表项

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

6.18 未知组播动作配置

6.18.1 介绍

未知组播报文是指交换机中不存在相应转发表项的组播报文，当交换机收到未知组播报文时，会在该 VLAN 内（除入端口外的其他端口）广播，这样会占用大量的网络带宽，影响转发速率。此时可以启动丢弃未知组播报文功能，当交换机收到未知组播报文时会被丢弃，不再转发。

6.18.2 Web 页面配置

1、配置未知组播动作

点击导航树[设备高级配置]→[组播协议配置]→[未知组播动作配置]菜单进入未知组播动

作配置界面，如图 275 所示；

图 275 未知组播处理方式

未知组播动作

配置选项：转发/丢弃

默认配置：转发

功能：配置未知组播报文的处理方式。

2、配置组播流监听端口，如图 276 所示；

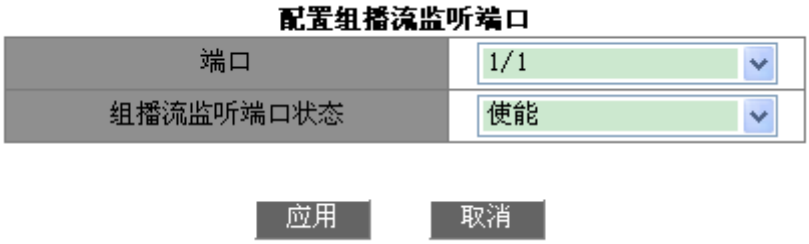


图 276 配置组播流监听端口

组播流监听端口状态

配置选项：禁止/使能

默认配置：禁止

功能：配置组播流监听端口。该监听端口转发相同 VLAN 域中其他端口接收到的组播业务流（包括已知组播业务流和未知组播业务流），该功能主要用于组播监听。

说明：

- 未知组播动作配置为丢弃时，无法配置组播流监听端口；
- 如果存在组播监听端口，则未知组播流仅转发至组播监听端口；如果不存在组播监听端口，则未知组播流转发至该 VLAN 中其他端口；
- 组播监听端口无组播协议能力，因此不可配置为组播成员端口。

6.19 静态组播配置

6.19.1 介绍

可以静态配置组播地址表，按照{VLAN 号、组播 MAC 地址、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。

6.19.2 Web 页面配置

1、添加静态组播表项；

点击导航树[设备高级配置]→[组播协议配置]→[静态组播配置]菜单进入静态组播配置界面，如图 277 所示；

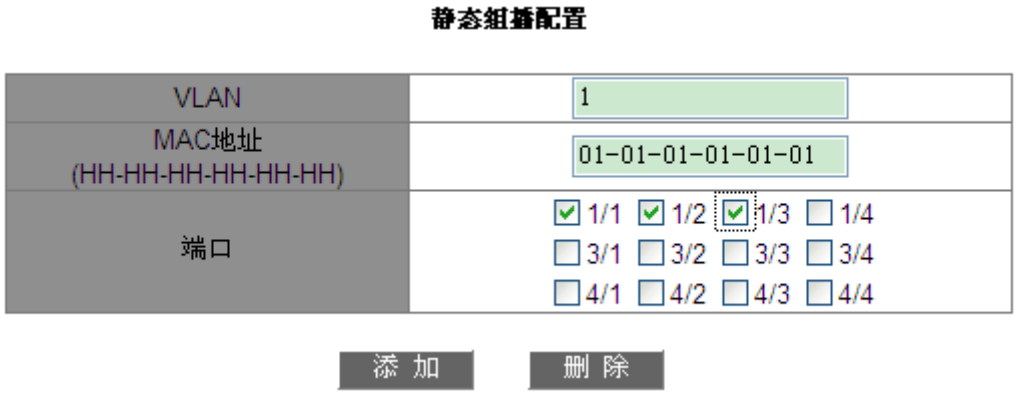


图 277 添加静态组播地址表项

VLAN

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。

MAC 地址

配置格式：HH-HH-HH-HH-HH-HH (H 为一个十六进制数)

功能：配置组播组地址，最高字节的最低位为 1 即可。

端口

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。

点击<添加>按钮，成功添加当前组播表项；点击<删除>按钮，可删除当前组播表项。

2、查看静态组播表项，如图 278 所示。

VLAN	MAC地址	端口
2	03-01-01-01-01-01	1/1 1/4
1	01-01-01-01-01-01	1/1 1/2 1/3
1	01-00-00-00-00-01	1/1 1/2

图 278 查看静态组播表项

6.20 LLDP

6.20.1 介绍

LLDP(Link Layer Discovery Protocol，链路层发现协议)提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息封装在 LLDPDU(Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元)中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB 形式保存起来，以供网络管理系统查询及判断链路状况。

6.20.2 Web 页面配置

1、使能 LLDP 协议

点击导航树[设备高级配置]→[LLDP 配置]→[LLDP 配置]菜单进入 LLDP 配置界面，如图 279 所示；

图 279 使能 LLDP 协议

LLDP 配置

配置选项：使能/禁止

默认配置：禁止

功能：使能 LLDP 协议。

2、使能 TLV 管理地址功能，如图 280 所示；

图 280 使能 TLV 管理地址

TLV 管理地址

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 LLDP 发送管理地址的功能。

描述：该功能关闭时，向相连设备发送接口 IP 地址，即本端口所在第一个 VLAN 虚接口的主 IP 地址；如果本端口所在 VLAN 虚接口没有配置 IP 地址，则不向相连设备发送接口 IP 地址，包括本设备其他端口已配置的所有 IP 地址。该功能打开时，向相连设备发送接口 IP 地址和本设备该端口已配置的所有 IP 地址，最多可以发送 64 个 TLV 管理地址；如果本端口所在 VLAN 虚接口没有配置 IP 地址，则不向相连设备发送接口 IP 地址，包括本设备其他端口已配置的所有 IP 地址。

注意：

本端设备打开 TLV 管理地址功能时，要求对端设备能够解析 TLV 功能，才可以正确显示本端交换机配置的所有 IP 地址。

3、查看 LLDP 显示信息

点击导航树[设备高级配置]→[LLDP 配置]→[查看 LLDP 信息]菜单进入 LLDP 信息显示界面，如图 281 图 284 所示；

➢打开 TLV 管理地址时，LLDP 显示信息包括相邻设备与该交换机连接的端口号、相邻设备的接口 IP 地址、已配置的所有 IP 地址、MAC 地址以及系统信息。

图 281 打开 TLV 管理地址时 LLDP 显示信息 1

上图所示为端口 1/4 所在的第一个 VLAN 虚接口主 IP 地址为 192.168.0.5 的情况。

反馈信息窗口

```
Local Port ID                       : Port_1/5
Remote Port ID<ifAlias>             : Port_1/1
Remote Chassis ID<MacAddr>          : 00:1e:cd:01:5a:88
Remote Management Address<MacAddr>  : 00:1e:cd:01:5a:88
Remote System Capability            : Bridge    Router
Remote System Name                  : Aquam8012A
Remote System Description           : SWITCH
```

图 282 打开 TLV 管理地址时 LLDP 显示信息 2

上图所示为端口 1/1 所在的 VLAN 虚接口没有配置 IP 地址的情况。

➢关闭 TLV 管理地址时，LLDP 显示信息包括相邻设备与该交换机连接的端口号、相邻设备的接口 IP 地址、MAC 地址以及系统信息。

反馈信息窗口

```
Local Port ID                       : Port_1/5
Remote Port ID<ifAlias>             : Port_1/4
Remote Chassis ID<MacAddr>          : 00:1e:cd:01:5a:88
Remote Management Address<IPV4>     : 192.168.0.5
Remote System Capability            : Bridge    Router
Remote System Name                  : Aquam8012A
Remote System Description           : SWITCH
```

图 283 关闭 TLV 管理地址时显示 LLDP 信息 1

上图所示为端口 1/4 所在的第一个 VLAN 虚接口主 IP 地址为 192.168.0.5 的情况。

反馈信息窗口

```
Local Port ID                       : Port_1/5
Remote Port ID<ifAlias>             : Port_1/1
Remote Chassis ID<MacAddr>          : 00:1e:cd:01:5a:88
Remote Management Address<MacAddr>  : 00:1e:cd:01:5a:88
Remote System Capability            : Bridge    Router
Remote System Name                  : Aquam8012A
Remote System Description           : SWITCH
```

图 284 关闭 TLV 管理地址时显示 LLDP 信息 2

上图所示为端口 1/1 所在的 VLAN 虚接口没有配置 IP 地址的情况。

注意：

显示 LLDP 信息的前提是相连接的设备都使能 LLDP 协议。

6.21 RMON

6.21.1 介绍

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

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

6.21.2 RMON 组

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

6.21.3 Web 页面配置

1、点击导航树[设备高级配置]→[RMON 配置]→[RMON 统计信息]菜单进入 RMON 统计信息设置如图 285 所示；

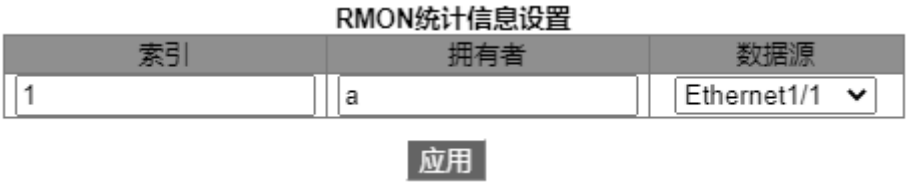


图 285 RMON 统计配置表

索引

配置范围：1~65535

功能：配置统计信息表项的编号。

拥有者

配置范围：1~30 个字符

功能：配置统计信息表项的名称。

数据源

功能：选择统计哪个端口的信息。

2、点击导航树[设备高级配置]→[RMON 配置]→[RMON 历史控制]菜单进入 RMON 历史控制如图 286 所示；

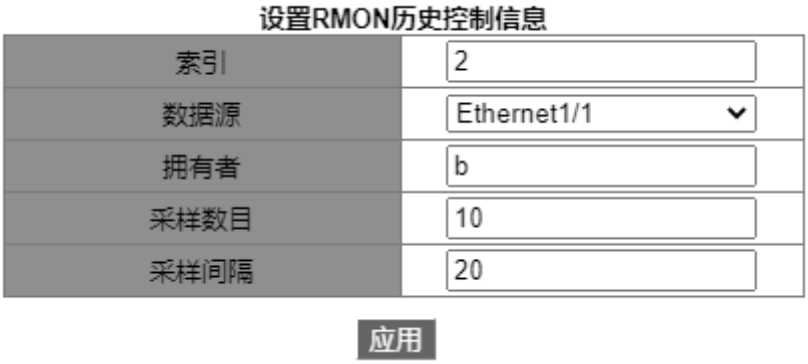


图 286 RMON 历史配置表

索引

配置范围：1~65535

功能：配置历史控制表项的编号

数据源

功能：选择对哪个端口信息进行采样。

拥有者

配置范围：1~31 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、点击导航树[设备高级配置]→[RMON 配置]→[RMON 事件控制]菜单进入 RMON 事件控制配置如图 287 所示；

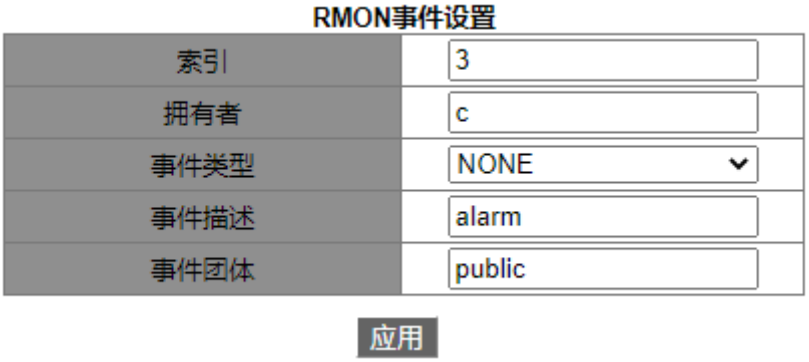


图 287 RMON 事件控制配置表

索引

配置范围：1~65535

功能：配置事件控制表项的索引号。

拥有者

配置范围：1~30 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：1~126 个字符

功能：对事件的描述。

事件团体

配置范围：1~126 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、点击导航树[设备高级配置]→[RMON 配置]→[RMON 告警]菜单进入 RMON 告警如图 288 所示；

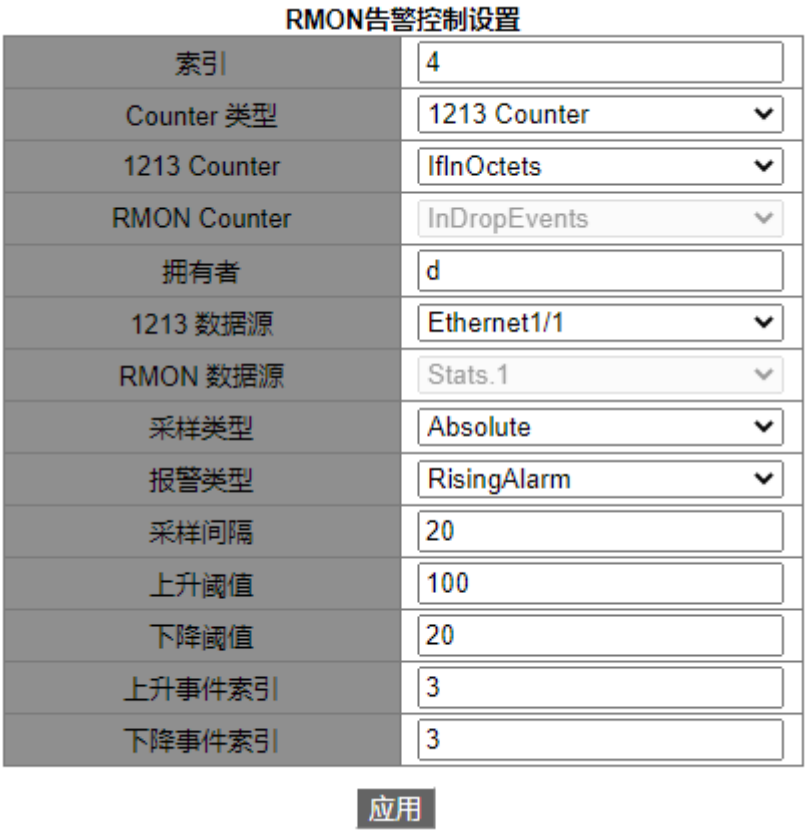


图 288 RMON 告警配置表

索引

配置范围：1~65535

功能：配置告警控制表项的编号。

Counter 类型

配置选项：1213 Counter/ RMON Counter

功能：选择 MIB 节点类型。

1213 Counter/RMON Counter

功能：指定 RMON 告警类型。

拥有者

配置范围：1~31 个字符

功能：配置告警控制表项的名称。

1213 数据源

功能：选择对哪个端口的信息进行监测。

RMON 数据源

配置选项：RMON 统计配置表中统计信息表项的索引号

功能：选择对哪个统计信息表项中的端口进行监测。

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。

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。

6.22 SNTP 配置

6.22.1 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，可以支持多个 SNTP 服务器，但同一时间只能有一个处于活动状态。

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。

6.22.2 Web 页面配置

1、使能 SNTP 协议

点击导航树[设备高级配置]→[SNTP 配置]→[设置 SNTP 服务器]菜单进入 SNTP 配置界面，如图 289 所示；

图 289 使能 SNTP 协议

SNTP 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 SNTP 协议。

注意：

SNTP 和 NTP 协议互斥。由于 NTP 和 SNTP 使用相同的 UDP 端口号，因此两者不能同时使能。

2、查看 SNTP 配置信息

点击导航树[设备高级配置]→[SNTP 配置]→[SNTP 主要信息]菜单进入 SNTP 配置信息查看界面，如图 290 所示；

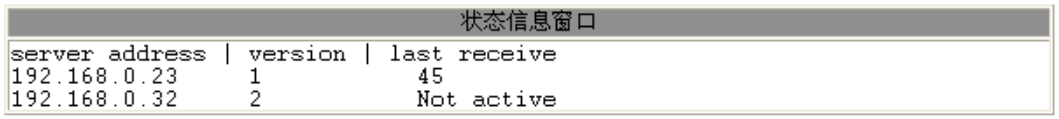


图 290 查看 SNTP 配置信息

Last receive 显示距上次同步时间的间隔。

6.23 NTP 配置

6.23.1 介绍

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

如图 291 所示，通过 NTP 报文交互可以估算报文在网络上的往返延迟 Delay=(T4-T1)-(T3-T2)和设备时钟偏差 Offset=((T2-T1)+(T3-T4))/2，从而实现在网络上的高精度设备对时。

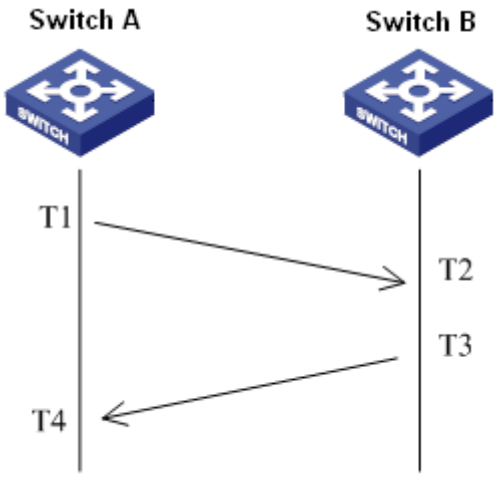


图 291 NTP 原理图

6.23.2 NTP 工作模式

NTP 协议可以采用以下工作模式进行时间同步，用户可以根据需要选择合适的工作模式：

客户端/服务器模式：此模式下，客户端向服务器发送时钟同步报文(客户端模式)；服务器收到报文后自动工作在服务器模式，并发送应答报文(服务器模式)；客户端收到应答报文后，同步到最优服务器时钟。

对等体模式：此模式下，主动对等体向被动对等体发送时钟同步报文(主动对等体模式)，被动对等体收到报文后工作在被动对等体模式，并发送应答报文(被动对等体模式)。经过报文交互，建立起对等体模式，主动对等体和被动对等体可以互相同步，如果都已经同步，则以层数小的时钟为准。

广播模式：此模式下，广播服务器周期性地广播时钟同步报文(广播模式)，广播客户端收到广播报文后，向服务器端发送时钟同步报文(客户端模式)，服务器端收到请求报文后，发送应答报文(服务器模式)。服务器和客户端通过 8 次请求、应答报文的交互完成系统时钟同步。

组播模式：组播客户端向组播服务器周期性发送组播时钟同步请求报文(客户端模式)，服务器收到报文后发送单播应答报文(服务器模式)。之后服务器和客户端交互单播时钟同步请求、应答报文完成时钟同步。

6.23.3 Web 页面配置

1、使能 NTP 协议

点击导航树[设备高级配置]→[NTP 配置]→[NTP 全局配置]菜单进入 NTP 全局配置界面，

如图 292 所示；

图 292 使能 NTP 协议

NTP 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否开启全局 NTP 服务功能。

注意：

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

2、配置 NTP 单播，如图 293 所示；

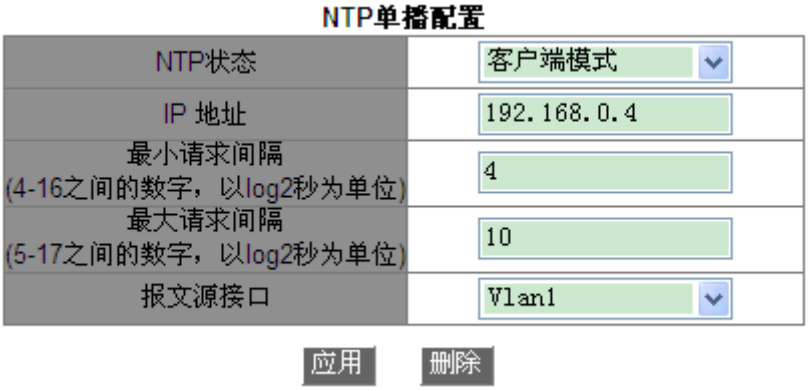


图 293 NTP 单播配置

NTP 状态

配置选项：客户端模式/对等体模式

功能：选择 NTP 工作模式。

描述：客户端模式表示 NTP 工作模式为客户端/服务器模式；对等体模式表示 NTP 工作

模式为对等体模式。

IP 地址

配置格式：A.B.C.D

描述：采用客户端/服务器工作模式时，该地址为 NTP 服务器 IP 地址；采用对等体工作模式时，该地址为被动对等体 IP 地址。

最小请求间隔

配置范围：4~16 间隔时间=2^n s

默认配置：4 即 2^4=16s

功能：配置 NTP 协议与服务器交互的最小请求时间间隔。

最大请求间隔

配置范围：5~17 间隔时间=2^n s

默认配置：10 即 2^{10}=1024s

功能：配置 NTP 协议与服务器交互的最大请求时间间隔。

报文源接口

功能：指定发送 NTP 报文的接口。

描述：采用客户端/服务器工作模式时，本地设备给服务器发送 NTP 报文时，报文中的源 IP 地址为该接口的主 IP 地址；采用对等体工作模式时，本地设备给对端发送 NTP 报文时，报文中的源 IP 地址为该接口的主 IP 地址。

注意：

- 采用客户端/服务器工作模式时，只需在客户端进行上述配置；
- 配置的 NTP 服务器时钟必须被同步，才能同步其他设备；
- 采用对等体工作模式时，只需在主动对等体上进行上述配置；
- 最小请求间隔≤最大请求间隔；
- 互为 NTP 对等体的两台设备最小间隔值应该相等。

3、配置 NTP 组播服务器

点击导航树[设备高级配置]→[NTP 配置]→[组播服务器配置]菜单进入组播服务器配置界面，如图 294 所示；

图 294 组播服务器配置

组播 IP 地址

配置格式：A.B.C.D

功能：配置组播 IP 地址，如果没有指定组播 IP 地址时，默认采用 224.0.1.1 组播 IP 地址。

使能组播接口

功能：指定开启组播模式的接口。

4、配置 NTP 组播客户端

点击导航树[设备高级配置]→[NTP 配置]→[组播客户端配置]菜单进入组播客户端配置界面，如图 295 所示；

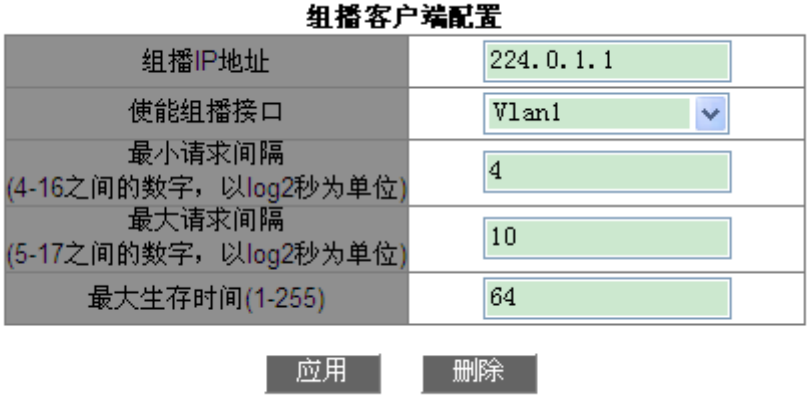


图 295 组播客户端配置

组播 IP 地址

配置格式：A.B.C.D

功能：配置组播模式下使用的组播 IP 地址，如果没有指定组播 IP 地址时，默认采用 224.0.1.1 组播 IP 地址。

使能组播接口

功能：指定开启组播模式的接口。

最小请求间隔

配置范围：4~16 间隔时间=2^n s

默认配置：4 即 2^4=16s

功能：配置 NTP 协议与服务器交互的最小请求时间间隔。

最大请求间隔

配置范围：5~17 间隔时间=2^n s

默认配置：10 即 2^{10}=1024s

功能：配置 NTP 协议与服务器交互的最大请求时间间隔。

最大生存时间

配置范围：1~255

默认配置：64

功能：配置组播客户端发送组播请求的最大 TTL 值。

5、配置 NTP 广播服务器

点击导航树[设备高级配置]→[NTP 配置]→[广播服务器配置]菜单进入广播服务器配置界面，如图 296 所示；

图 296 广播服务器配置

使能广播接口

功能：指定开启广播模式的接口。

6、配置 NTP 广播客户端

点击导航树[设备高级配置]→[NTP 配置]→[广播客户端配置]菜单进入广播客户端配置界面，如图 297 所示；

图 297 广播客户端配置

广播客户端配置

功能：指定开启广播模式的接口。

7、配置参考时钟

点击导航树[设备高级配置]→[NTP 配置]→[参考时钟配置]菜单进入参考时钟配置界面，如图 298 所示；

图 298 参考时钟配置

参考时钟 IP 地址

配置格式：127.127.t.u

默认配置：127.127.0.1

描述：127.127.t.u 中 t 表示参考时钟类型，u 表示实例号。目前只支持 127.127.0.1，即以系统时钟为参考时钟。

参考时钟等级

配置范围：1~15

默认配置：4

功能：配置参考时钟的等级。

描述：时钟等级定义了时钟的准确度，准确度从 1 到 16 依次递减，等级为 16 的时钟未处于同步状态，不能作为参考时钟。

注意：

目前只支持以交换机自己为参考时钟，配置该项时需要谨慎，请确认网络对时系统的需求。

6.23.4 典型配置举例

➢ 对等体模式配置

如图 299 所示，Switch D 配置本地时钟作为参考时钟，层数为 2。Switch A 工作在客户端模式，指定 Switch D 为 NTP 服务器。Switch B 工作在对等体模式，将 Switch A 设为对等

体，其中 Switch B 为主动对等体，Switch A 为被动对等体。

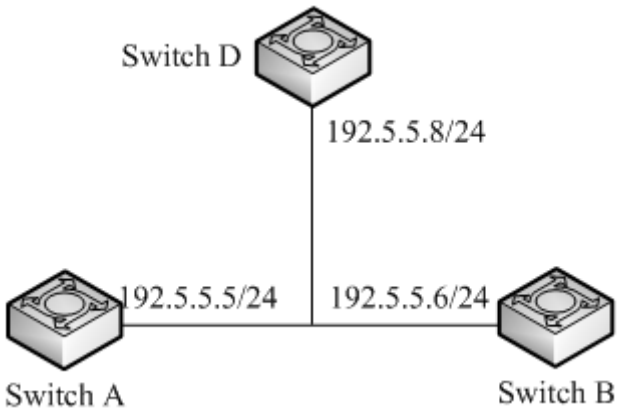


图 299 对等体模式组网图

Switch D 配置过程：

1、使能 NTP 协议，见图 292；

2、配置参考时钟 IP 地址为 127.127.0.1，参考时钟等级为 2，见图 298；

Switch A 配置过程：

1、使能 NTP 协议，见图 292；

2、配置 NTP 服务器 IP 地址为 192.5.5.8，最小间隔间隔为默认值 4，最大请求间隔为默认值 10，报文源接口选择 VLAN 1 ，见图 293；

Switch B 配置过程：

1、使能 NTP 协议，见图 292；

2、配置 NTP 对等体 IP 地址为 192.5.5.5，最小间隔间隔为默认值 4，最大请求间隔为默认值 10，报文源接口选择 VLAN 1 ，见图 293；

- 组播模式配置

如图 300 所示，Switch D 配置本地时钟作为参考时钟，层数为 2，工作在组播服务器模式，在 VLAN 2 接口开启组播服务器模式。Switch A 和 Switch B 工作在组播客户端模式，在 VLAN 2 接口开启组播客户端模式。

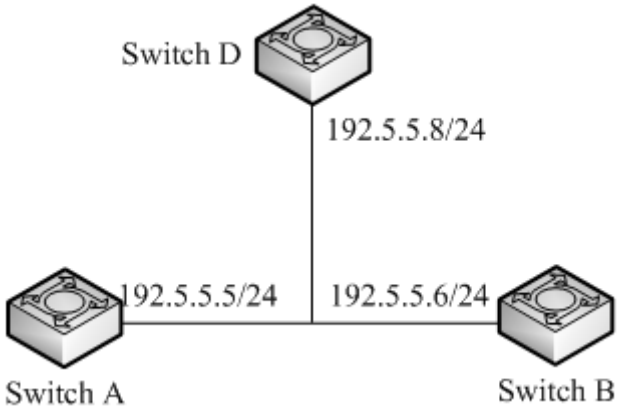


图 300 组播模式组网图

Switch D 配置过程：

1、使能 NTP 协议，见图 292；

2、配置参考时钟 IP 地址为 127.127.0.1，参考时钟等级为 2，见图 298；

3、配置组播服务器：组播 IP 地址为 224.0.1.1，使能 VLAN 接口为 VLAN 2，见图 294；

Switch A、B 配置过程：

1、使能 NTP 协议，见图 292；

2、配置组播客户端：组播 IP 地址为 224.0.1.1，使能组播接口为 VLAN 2 最小间隔间隔为默认值 4，最大请求间隔为默认值 10，最大生存时间为 64，见图 295；

➢ 广播模式配置

如图 301 所示，Switch D 配置本地时钟作为参考时钟，层数为 2，工作在广播服务器模式，在 VLAN 2 接口开启广播服务器模式。Switch A 和 Switch B 工作在广播客户端模式，在 VLAN 2 接口开启广播客户端模式。

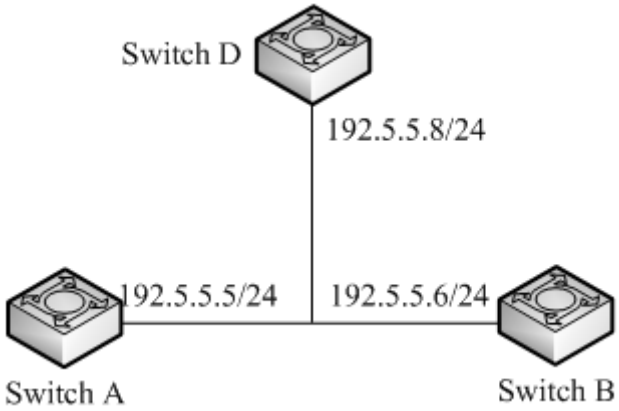


图 301 广播模式组网图

Switch D 配置过程：

1、使能 NTP 协议，见图 292；

2、配置参考时钟 IP 地址为 127.127.0.1，参考时钟等级为 2，见图 298；

3、配置广播服务器：使能广播接口为 VLAN 2，见图 296；

Switch A、B 配置过程：

1、使能 NTP 协议，见图 292；

2、配置广播客户端：使能广播接口为 VLAN 2，见图 297。

6.24 TACACS+配置

6.24.1 介绍

TACACS+(Terminal Access Controller Access Control System，终端访问控制器访问控制系统)是一种基于 TCP 传输协议的应用，采用客户端/服务器模式实现 NAS(Network Access Server，网络接入服务器)与 TACACS+服务器之间的通信，客户端运行于 NAS 上，服务器上集中管理用户信息。NAS 对于用户来说是服务器端，对于服务器来说是客户端，结构示意图如图 302 所示。

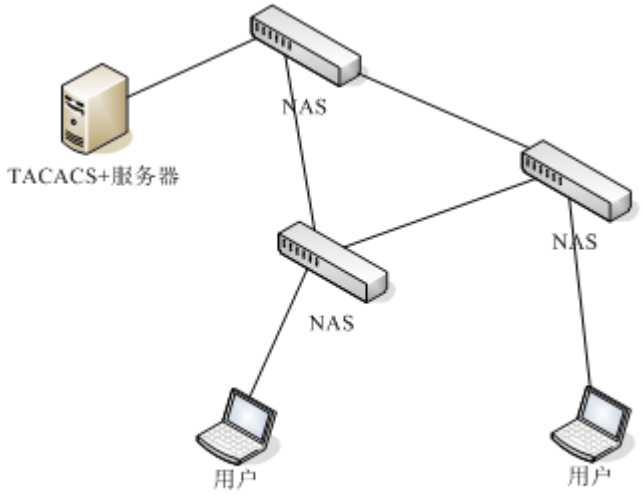


图 302 TACACS+结构示意图

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

登录到设备上进行操作。

6.24.2 Web 页面配置

1、使能 TACACS+协议

点击导航树[设备高级配置]→[TACACS-PLUS 配置]→[TACACS-PLUS 配置]菜单进入TACACS+配置界面，如图 303 所示；

图 303 使能 TACACS+协议

Tacacs-plus 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能 TACACS+协议。

2、TACACS+服务器配置，如图 304 所示；

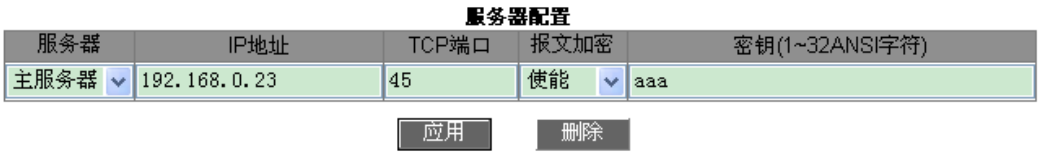


图 304 TACACS+服务器配置

服务器

配置选项：主服务器/备服务器

默认配置：主服务器

功能：选择当前配置的服务器类型。

IP 地址

配置格式：A.B.C.D

功能：输入服务器 IP 地址。

TCP 端口

配置范围：1~65535

默认配置：49

功能：接收 NAS 认证请求的端口号。

报文加密

配置选项：使能/不使能

默认配置：不使能

功能：报文是否需要加密，当加密使能后需要输入加密密钥值。

密钥

配置范围：1~32 个字符

描述：配置密钥值提高客户端与 TACACS+服务器通信的安全性。双方通过设备共享密钥来验证报文的合法性，只有密钥一致时，双方才能彼此接收对方发送的报文并作出响应，因此必须保证设备上配置的共享密钥与 TACACS+服务器上的密钥值完全一样。

配置完成后在下方“服务器列表”中显示服务器配置信息，如图 305 所示；

服务器列表			
主服务器	192.168.0.23	49	加密
备服务器	192.168.0.32	45	不加密

图 305 服务器配置列表

6.24.3 典型配置举例

图 306 所示，通过 Switch 实现 TACACS+服务器对用户进行认证、授权。服务器 IP 地址为 192.168.0.23，交换机与服务器交互报文时的共享密钥为 aaa。

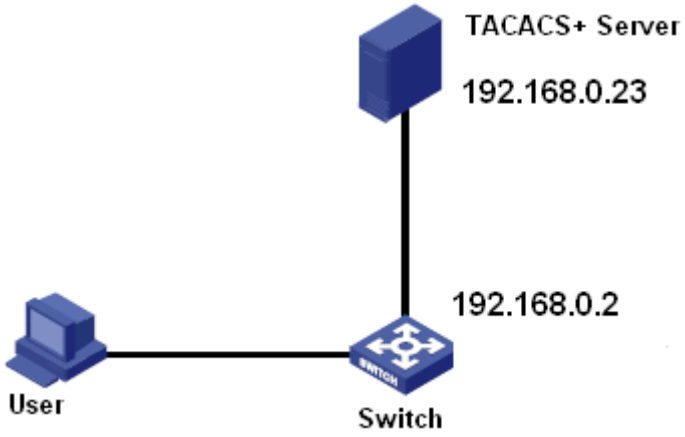


图 306 TACACS+认证举例

1、使能 TACACS+协议，见图 303；

2、服务器信息配置，IP 地址为 192.168.0.23，报文加密，密钥值为 aaa，见图 304；

3、Web 登录时采用本地认证；Telnet 登录时采用 TACACS+认证，见图 318；

4、TACACS+服务器上配置用户名和密码 bbb，密钥值 aaa；

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

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

6.25 RADIUS 配置

6.25.1 介绍

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

该协议采用客户端/服务器模式实现NAS(Network Access Server，网络接入服务器)与RADIUS服务器之间的通信，RADIUS客户端运行于NAS上，RADIUS服务器上集中管理用户信息。NAS对于用户来说是服务器端，对于RADIUS服务器来说是客户端，结构示意图如图 307 所示；

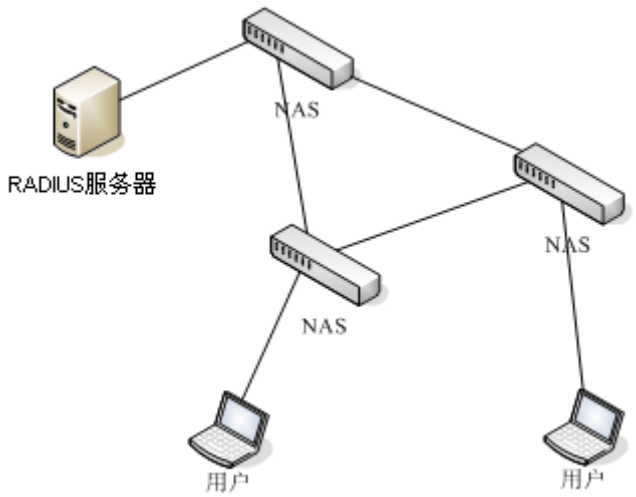


图 307 RADIUS 结构示意图

该协议对需要登录到设备上进行操作的终端用户进行登录认证。设备作为 RADIUS 的客户端，将用户发送过来的认证信息发给 RADIUS 服务器进行认证，并根据 RADIUS 服务器的

认证结果允许/拒绝用户登录设备。

6.25.2 Web 页面配置

1、配置 RADIUS 认证参数

点击导航树[设备高级配置]→[RAIDUS 配置]→[RAIDUS 配置]菜单进入 RAIDUS 配置界面，如图 308 所示；

图 308 RADIUS 认证参数配置

请求次数

配置范围：1~3

默认配置：3

功能：配置 RAIUDS 请求报文超时重传的次数，如果累计的传送次数超过该配置值，RADIUS 服务器仍旧没有响应，则设备将认为本次认证失败。

超时时间

配置范围：1~3s

默认配置：3s

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

2、RADIUS 服务器配置，如图 309 所示；

图 309 RADIUS 服务器配置

服务器类型

配置选项：认证主服务器/认证从服务器

功能：配置 RADIUS 认证主/从服务器。当主服务器不可达时，交换机将使用从服务器进行认证。

服务器 IP

配置格式：A.B.C.D

功能：配置 RADIUS 服务器的 IP 地址。

端口：

配置范围：1~65535

默认配置：1812

功能：配置 RADIUS 服务器的 UDP 端口号。

密码

配置范围：1~32 字符

功能：配置 RADIUS 服务器密码。

6.25.3 典型配置举例

如图 310 所示，Switch 的端口 1 使能 IEEE802.1x 协议，用户需通过 RADIUS 服务器进行认证打开端口 1 登录到 Switch 上。服务器 IP 地址为 192.168.0.23，Switch 与服务器交互报文时的共享密钥为 aaaa。

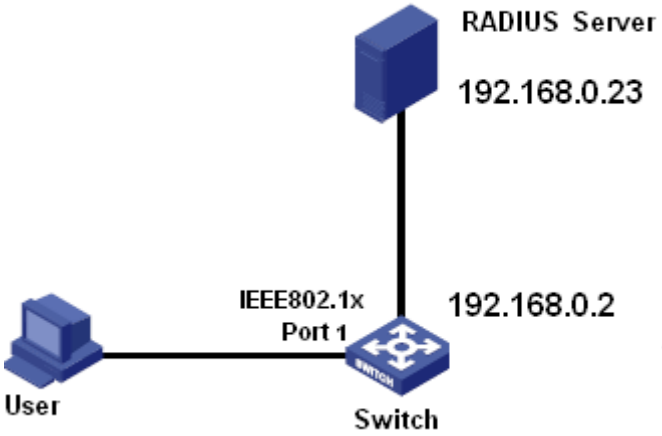


图 310 RADIUS 认证举例

1、配置认证主服务器 IP 地址为 192.168.0.23，密码为 aaaa，见图 309。

2、IEEE802.1x 功能配置：全局使能 IEEE802.1x 功能，使能端口 1 的 IEEE802.1x 功能，

其它配置保持默认，参照“6.26 IEEE802.1x 配置”章节。

3、Dot1x 认证方式选择 Radius 认证，见图 318；

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

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

6.26 IEEE802.1x 配置

6.26.1 介绍

IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。802.1x 协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要解决以太网内认证和安全方面的问题。802.1x 协议是一种基于端口的网络接入控制(Port Based Network Access Control)协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。使用 802.1x 的系统为典型的 Client/Server 体系结构，只有具备了以下三个元素才能够完成基于端口的访问控制的用户认证和授权：

客户端：一般为用户终端设备，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求；

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

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

6.26.2 Web 页面配置

1、使能全局 IEEE802.1x 协议

点击导航树[设备高级配置]→[IEEE802.1x 配置]→[IEEE802.1x 配置]菜单进入 IEEE802.1x 配置界面，如图 311 所示；

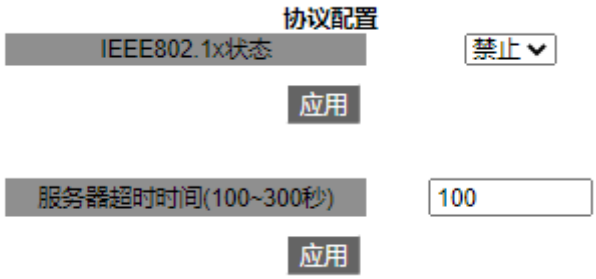


图 311 全局使能 IEEE802.1x

IEEE802.1x 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否开启全局 IEEE802.1x 安全功能。

服务器超时时间

配置范围：100~300 秒

默认配置：100 秒

功能：设备端向认证服务器发送 RADIUS Access-Request 请求报文后，设备端启动该定时器，若在该定时器设置的时长内，设备端没有收到认证服务器响应，设备端将重发认证请求报文。

2、配置使能 IEEE802.1x 协议的端口，如图 312 所示；

图 312 IEEE802.1x 协议端口配置

端口

配置选项：交换机上所有端口

IEEE802.1x 状态

配置选项：使能/禁止

默认配置：禁止

功能：是否使能端口的 IEEE802.1x 协议。

描述：使能后端口通信取决于 IEEE802.1x 控制模式。

控制模式

配置选项：强制未授权/自动识别/强制授权

默认配置：自动识别

功能：选择端口的认证模式。

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

重认证

配置选项：使能/禁止

默认配置：禁止

功能：当认证成功后，是否需要周期性的重新认证。

重认证定时器

配置范围：60~7200s

默认配置：3600s

功能：认证成功后，重认证的时间间隔。

静默定时器

配置范围：10~120s

默认配置：60s

功能：认证失败后进入静默周期，静默周期时间之后服务器才会再接受认证请求；静默周期内，服务器对客户端的认证请求不予响应。

接口接入控制模式

配置选项：基于端口/基于 MAC

默认配置：基于端口

功能：配置 IEEE802.1x 端口的接入控制模式。

描述：基于 MAC 地址对接入用户进行控制，即该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。基于端口对接入用户进行控制，即只要该端口下的第一个用户认证成功后，该端口即可打开，其他接入用户无须认证就可使用网络资源，

但是当第一个用户下线后，该端口关闭，其他用户也会被拒绝使用网络。

最大用户数

配置范围：1~128

默认配置：128

功能：配置使能 IEEE802.1x 功能的端口最大的接入用户数量。

说明：此配置只对基于 MAC 接入控制模式的端口有效，对基于端口接入控制模式的端口无效。

3、查看 IEEE802.1x 配置信息

点击导航树[设备高级配置]→[IEEE802.1x 配置]→[IEEE802.1x 主要信息]菜单进入 IEEE802.1x 配置信息查看界面，如图 313 所示。

状态信息窗口

```
IEEE802.1X status         : enable
IEEE802.1X type           : chap
IEEE802.1X server-timeout : 100(s)

 interface  config    method   running  authentication mode authentication result
---------- ------- ---------- -------- ------------------- ---------------------
1/1         enable  port-based active   auto                authorized
1/2         disable port-based unactive auto                N/A
1/3         disable port-based unactive auto                N/A
1/4         disable port-based unactive auto                N/A
2/1         disable port-based unactive auto                N/A
2/2         disable port-based unactive auto                N/A
2/3         disable port-based unactive auto                N/A
2/4         disable port-based unactive auto                N/A
4/1         disable port-based unactive auto                N/A
4/2         disable port-based unactive auto                N/A
4/3         disable port-based unactive auto                N/A
4/4         disable port-based unactive auto                N/A


********** 1/1 **********
IEEE802.1X config status           : enable
IEEE802.1X running status          : active
IEEE802.1X port method is          : port-based
IEEE802.1X port mode               : auto
IEEE802.1X authentication result   : authorized
IEEE802.1X reauthentication status : enable
IEEE802.1X reauthentication period : 3600(s)
IEEE802.1X quiet period            : 60(s)
IEEE802.1X max user number         : 128

********** 1/2 **********
IEEE802.1X config status           : disable
IEEE802.1X running status          : unactive
IEEE802.1X port method is          : port-based
IEEE802.1X port mode               : auto
IEEE802.1X authentication result   : N/A
IEEE802.1X reauthentication status : disable
IEEE802.1X reauthentication period : 3600(s)
IEEE802.1X quiet period            : 60(s)
IEEE802.1X max user number         : 128
```

图 313 IEEE802.1x 配置信息查看

4、配置 IEEE802.1x 用户认证组

点击导航树[设备高级配置]→[IEEE802.1x 配置]→[IEEE802.1x 组配置]菜单进入

IEEE802.1x 用户认证组配置界面，如图 314 所示；

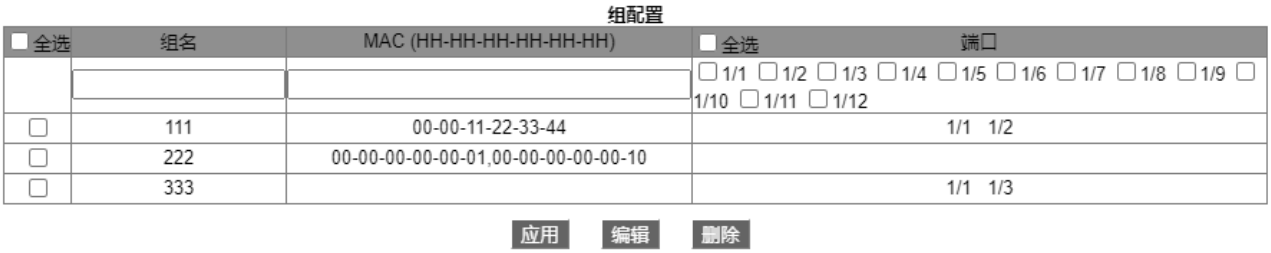


图 314 配置 IEEE802.1x 用户认证组

组名

配置范围：1~16 个字符

功能：配置用户认证组组名。

MAC

配置格式：HH-HH-HH-HH-HH-HH(H 为一个十六进制数)

功能：为当前用户认证组添加 MAC 地址。一个组中可以添加多个 MAC 地址，MAC 地址之间用半角逗号隔开。

端口

功能：为当前用户认证组添加端口。

说明：

用户认证组可以只配置 MAC 地址或端口号。

5、配置 IEEE802.1x 用户信息

点击导航树[设备高级配置]→[IEEE802.1x 配置]→[IEEE802.1x 用户配置]菜单进入 IEEE802.1x 用户配置界面，如图 315 所示；

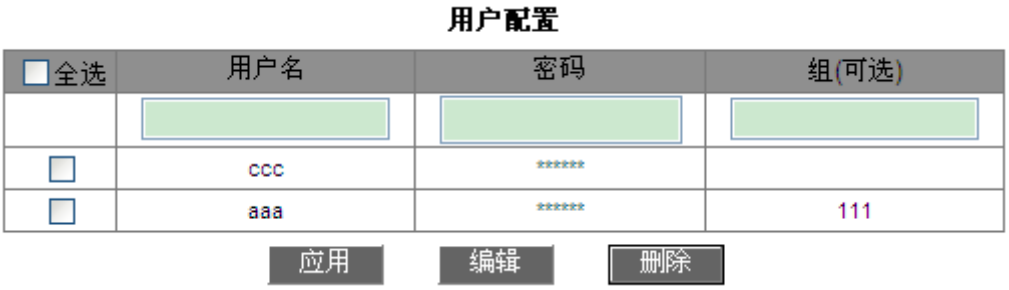


图 315 配置 IEEE802.1x 用户信息

用户名

配置范围：1~16 个字符

功能：配置 IEEE802.1x 用户名。

密码

配置范围：1~16 个字符

功能：配置 IEEE802.1x 密码。

组

功能：给当前用户绑定一个用户认证组。

说明：如果当前用户绑定了用户认证组，此时只有 MAC 地址和访问端口号都与绑定组中匹配的用户才可通过认证成功访问交换机。当前用户也可以不绑定任何用户认证组，此时用户可通过任何 MAC 地址和端口号进行认证。

6、查看 IEEE802.1x 在线用户信息

点击导航树[设备高级配置]→[IEEE802.1x 配置]→[IEEE802.1x 在线用户]菜单进入 IEEE802.1x 在线用户查看界面，如图 316 所示；

图 316 查看 IEEE802.1x 在线用户信息

选中一个或多个用户，点击<断开>按钮，可以断开该用户与交换机的连接。

6.26.3 典型配置举例

如图 317 所示，客户端连接交换机端口 1，使能端口 1 的 IEEE802.1x 协议并且采用 Auto 自动认证模式，本地认证用户名和密码为 ccc，远程认证用户名和密码为 ddd，其余配置采用默认值；

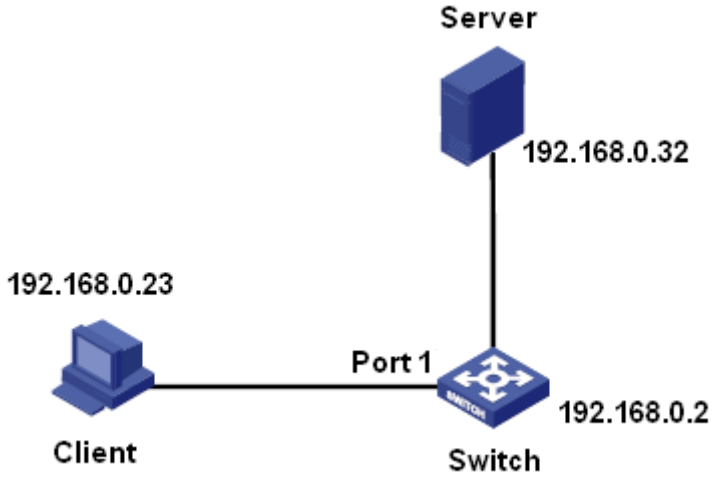


图 317 IEEE802.1x 配置举例

- 本地认证配置：

  1、全局使能 IEEE802.1x 协议，见图 311；

  2、Dot1x 认证方式选择本地认证，见图 318；

  3、配置用户名和密码为 ccc，见图 315；

  4、使能端口 1 的 IEEE802.1x 协议，认证模式选择 Auto 模式，见图 312；

  5、安装 802.1x 认证客户端软件并运行，输入用户名和密码 ccc 进行认证，认证成功后可以成功访问交换机。

- 远程认证配置：

  可参考“6.25 RADIUS 配置”章节的配置举例内容。

6.27 登录认证配置

配置访问交换机的登录方式及登录时采用的认证方式和认证顺序。

点击导航树[设备高级配置]→[登录认证配置]→[登录认证配置]菜单进入登录认证配置界面，如图 318所示；

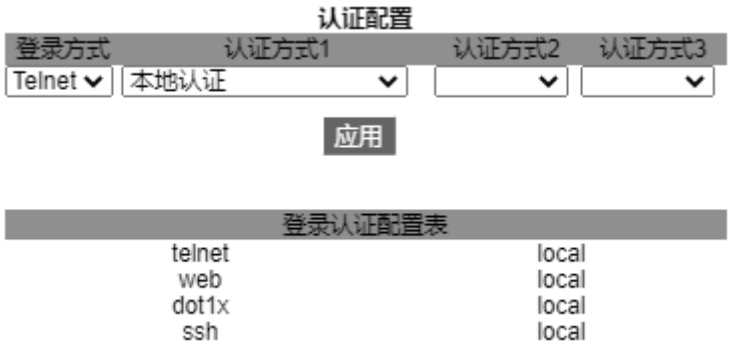


图 318 登录认证配置

登录方式

配置选项：Telnet/Web/dot1x/SSH

功能：选择访问交换机的登录方式。

认证方式 1/认证方式 2/认证方式 3

配置选项：本地认证/Tacacs+认证/Radius 认证/Radius+Local 认证/TacacsPlus+Local 认证

默认配置：本地认证

功能：选择登录认证的顺序，先采用认证方式 1 进行认证；如果认证不通过，再采用认证方式 2 进行认证；如果前两种认证都不通过，则采用认证方式 3 进行认证。

描述：本地认证表示采用本地创建的用户名和密码进行认证；Tacacs+认证表示采用 Tacacs+服务器上创建的用户名和密码进行认证；Radius 表示采用 Radius 服务器上创建的用户名和密码进行认证。

注意：

通过 dot1x 访问交换机时，认证方式只能选择一种。

6.28 诊断功能配置

6.28.1 链路状态检测

6.28.1.1 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，进入接收异常状态；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，则进入发送异常状态；如果端口 link down，则进入断开状态。

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：

使能链路状态检测的 DRP 环端口/备份端口出现异常状态（接收异常/发送异常/断开）时，DRP 环协议将该环端口/备份端口 block 掉。

6.28.1.2 Web 页面配置

1、使能端口的链路状态检测功能；

点击导航树[设备高级配置]→[诊断功能配置]→[链路状态检测]菜单进入链路状态检测配置界面，如图 319 所示；

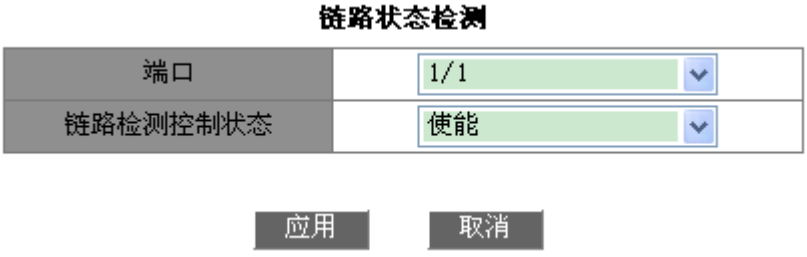


图 319 使能端口链路状态检测

链路检测控制状态

配置选项：使能/不使能

默认配置：不使能

功能：是否使能指定端口的链路检测功能。

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。

2、显示端口链路状态，如图 320 所示；

端口	状态
1/1	断开
1/2	不使能
1/3	不使能
1/4	不使能
1/5	不使能
1/6	不使能
1/7	不使能
1/8	不使能
1/9	不使能
1/10	不使能
1/11	不使能
1/12	不使能

图 320 链路状态显示

状态

显示选项：正常/不使能/接收异常/发送异常/断开

描述：如果使能了端口的链路状态检测功能，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；如果端口 link down，则显示断开。如果没有开启端口链路检测功能，则显示不使能。

6.28.2 电缆检测配置

6.28.2.1 介绍

VCT(virtual cable tester，虚拟线缆检测)利用 TDR(时域反射测试)来检测双绞线状态。通过向导线发射一个脉冲信号并检测此脉冲信号的反射来检测电缆故障。当电缆线有故障时，发送的脉冲信号到达电缆末端或电缆故障点时，部分或全部脉冲能量被反射回原发送源，VCT

技术测量脉冲信号在导线中的传输，到达故障点以及返回发送源的时间，并将时间换算为距离值。

VCT 能够对以太网电口连接电缆进行链路介质检测，并返回检测结果，使用 VCT 可以检测到以下几种线对状态：

Short：表示一个线对短接。

Open：表示开路，说明线对中有断线。

Normal：表示线对状态正常。

Mismatch：表示阻抗不匹配，例如：5 类线的阻抗为 100 欧，为了防止波形反射和数据错误，线缆两端的终止器阻抗也必须是 100 欧。

6.28.2.2 Web 页面配置

检测端口线对状态

点击导航树[设备高级配置]→[诊断功能配置]→[电缆检测]菜单进入电缆检测界面，如下图所示；

电缆检测

全选/端口	端口类型	端口状态	线对	状态	长度(m)
1/1	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/2	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/3	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/4	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/5	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/6	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/7	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/8	FE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
1/9	GE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
			(4,5)	未检测	未检测
			(7,8)	未检测	未检测
1/10	GE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
			(4,5)	未检测	未检测
			(7,8)	未检测	未检测
1/11	GE	up	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
			(4,5)	未检测	未检测
			(7,8)	未检测	未检测
1/12	GE	down	(1,2)	未检测	未检测
			(3,6)	未检测	未检测
			(4,5)	未检测	未检测
			(7,8)	未检测	未检测

检测 检测LinkDown端口 检测LinkUp端口

图 321 电缆检测显示状态

全选/端口

配置选项：交换机上的所有电口

选择需要检测线对状态的端口，点击<检测>按钮，检测出当前端口线对状态。

端口类型

显示当前端口类型。

线对

百兆电口只检测(1,2)和(3,6)两个线对；千兆电口需要检测(1,2)、(3,6)、(4,5)和(7,8)四个线对。

状态

显示选项：开路/短路/正常/失配

显示当前端口的线对状态。

长度

显示从线缆的端口连接处到故障点之间的长度，该测量技术存在少量的误差。Normal 状态的线对不显示长度。

点击<检测>按钮检测所选中端口的线对状态并显示检测结果；点击<测试 Link down 端口>按钮检测所有 Link down 端口的线对状态并显示检测结果；点击<测试 Link Up 端口>按钮检测所有 Link up 端口的线对状态并显示检测结果。

说明：

- 检测端口在检测过程中处于 Link down 状态；
- 检测完成后，端口会恢复 Link up 状态；
- 检测检测 Link Down 端口><检测 Link Up 端口>时，页面不会只显示 Link Down(或 Link Up)的端口，而是显示所有端口的状态。即保留上一次检测的结果的基础上刷新页面中此次检测的端口的状态。

6.29 环路检测配置

6.29.1 介绍

端口使能环路检测后，通过此端口发送环路检测报文来判断该端口连接的网络中是否存在环路。CPU 周期性向端口发送环路检测报文，如果该设备任意端口接收到环路检测报文，说

明网络中有环路存在，此时将发送环路检测报文的端口关闭，一段时间后自动打开该端口继续检测。其中，发送环路检测报文的时间间隔和端口恢复时间均可在软件中配置。

说明：

环路检测与 DT-Ring、DRP、RSTP、MSTP 功能互斥，即使能环路检测的端口不能配置为冗余端口；冗余端口不能使能环路检测功能。

6.29.2 Web 页面配置

配置端口环路检测功能，如图 322 所示；

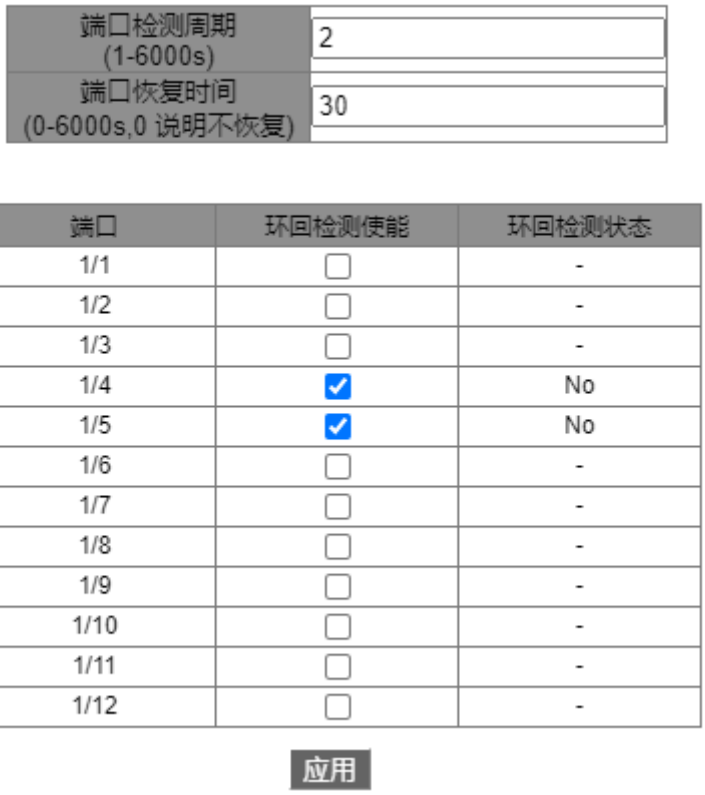


图 322 使能端口环路检测

端口检测周期

配置范围：1~6000s

默认配置：2s

功能：配置发送环路检测报文的时间间隔。

端口恢复时间

配置范围：0~6000s

默认配置：30s

功能：配置端口关闭后自动恢复的时间间隔，0 表示端口关闭后将不自动恢复直到设备重启。

环回检测使能

配置选项：使能/不使能

默认配置：不使能

功能：是否使能端口的环回检测功能。

环回检测状态

显示选项：Yes/No

功能：显示使能环回检测功能的端口所在网络中是否存在环路。Yes 说明存在环路；No 说明不存在环路。

6.29.3 典型配置举例

组网需求：

交换机端口3与外部网络相连，当网络中有环路存在时，将端口3关闭，如图 323所示。

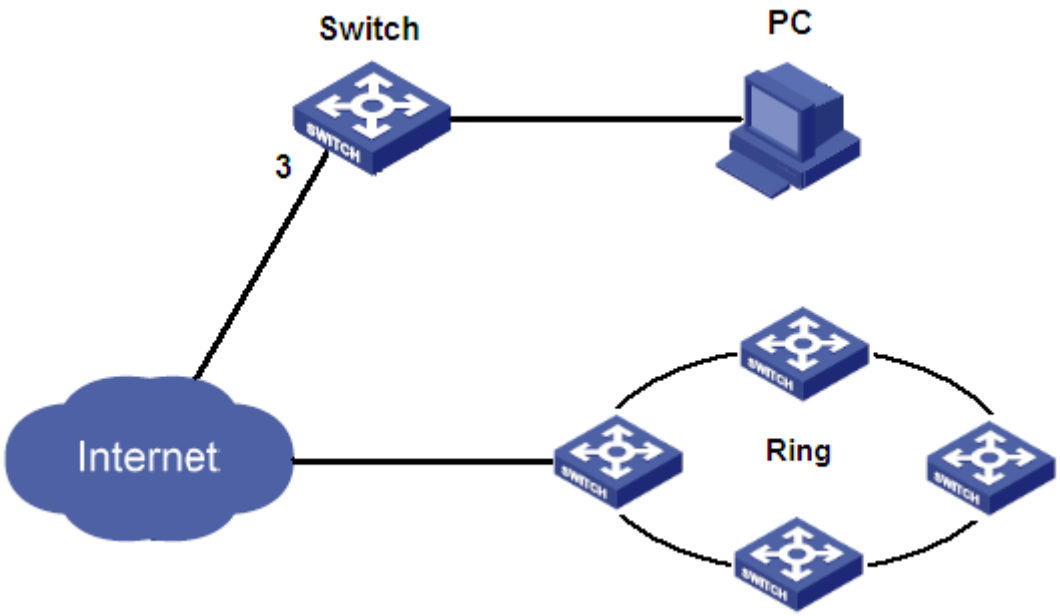


图 323 环路检测配置举例

具体配置：

使能端口 3 的环回检测功能，如图 322 所示。

6.30 端口 CRC 保护配置

6.30.1 介绍

端口使能 CRC 保护后，可以周期性检测 CRC 错误报文的数量。如果在检测时间内，CRC 错误报文的数量超过预设的阈值，则将该端口关闭，一段时间后打开端口继续检测。其中，检测 CRC 错误报文的时间和端口恢复时间均可在软件中配置。

6.30.2 Web 页面配置

配置端口 CRC 保护功能，如图 324 所示；

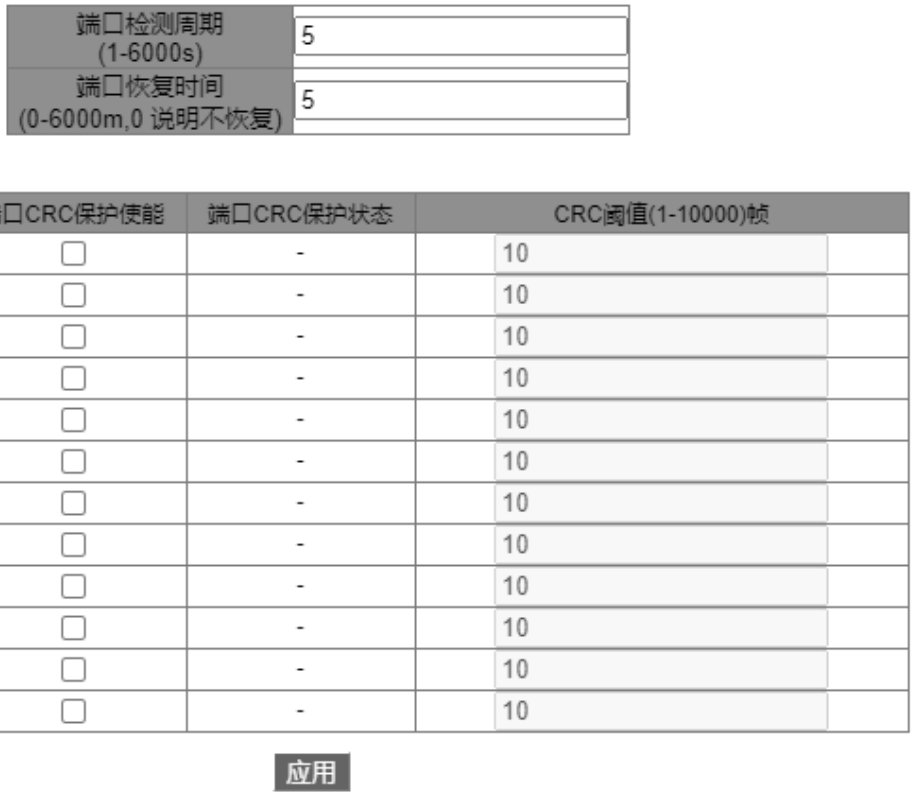


图 324 使能端口 CRC 保护功能

端口检测周期

配置范围：1~6000s

默认配置：5s

功能：配置检测 CRC 错误报文的时间，在该检测时间内，如果 CRC 错误报文数量超出阈值，则将该端口关闭。

端口恢复时间

配置范围：0~6000 m

默认配置：5m

功能：配置端口关闭后自动恢复的时间间隔，0 表示端口关闭后将不自动恢复直到设备重启。

端口 CRC 保护使能

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 CRC 保护功能。该检测机制只针对使能 CRC 保护功能的端口有效。

端口 CRC 保护状态

显示选项：-- / Yes / No

描述：Yes：端口使能 CRC 保护功能，因发生 CRC 错误而处于 linkdown 状态；No：端口使能 CRC 保护功能，并且处于 linkup 状态；--：端口没有使能 CRC 保护功能。

CRC 阈值

配置范围：1~10000 帧

默认配置：10 帧

功能：配置 CRC 错误阈值。

附录 缩略语表

缩略语	英文全称	中文
ABR	Area Border Router	区域边界路由器
ACL	Access Control List	访问控制列表
AS	Autonomous System	自治系统
ASBR	Autonomous System Boundary Router	自治系统边界路由器
ARP	Address Resolution Protocol	地址解析协议
BC	Boundary Clock	边界时钟
BDR	Backup Designated Router	备份指定路由器
BootP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
CAR	Committed Access Rate	约定访问速率
CIST	Common and Internal Spanning Tree	公共和内部生成树
CLI	Command Line Interface	命令行接口
CoS	Class of Service	服务等级
CST	Common Spanning Tree	公共生成树
DD	Database Description	数据库描述
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHP	Dual Homing Protocol	双归链路协议
DNS	Domain Name System	域名系统
DR	Designated Router	指定路由器
DSCP	Differentiated Services CodePoint	差分服务编码点
DST	Daylight Saving Time	夏时制
E2ETC	End-to-End Transparent Clock	端到端透传时钟
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

GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
HTTP	Hyper Text Transfer Protocol	超级文本传送协议
ICMP	Internet Control Message Protocol	因特网控制消息协议
IED	Intelligent Electronic Device	智能电子设备
IGMP	Internet Group Management Protocol	因特网组管理协议
IGMP Snooping	Internet Group Management Protocol Snooping	互联网组管理协议窥探
IST	Internal Spanning Tree	内部生成树
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
LSA	Link State Advertisement	链路状态通告
LSAck	Link State Acknowledgment	链路状态确认
LSDB	Link State Database	链路状态数据库
LSR	Link State Request	链路状态请求
LSU	Link State Update	链路状态更新
MIB	Management Information Base	管理信息库
MSTI	Multiple Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议
NAS	Network Access Server	网络接入服务器
NetBIOS	Network Basic Input/Output System	网络基本输入/输出系统
NMS	Network Management Station	网络管理站
NTP	Network Time Protocol	网络时间协议
OC	Ordinary Clock	普通时钟
OID	Object Identifier	对象标识符
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial-In User Service	远程认证拨号用户服务
RID	Router ID	路由器 ID
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Network Monitoring	远程网络监控

RSTP	Rapid Spanning Tree Protocol	快速生成树协议
SFTP	Secure File Transfer Protocol	安全文件传输协议
RTC	Real Time Clock	实时时钟
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
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	安全套接层
STP	Spanning Tree Protocol	生成树协议
TACACS+	Terminal Access Controller Access Control System	终端访问控制器访问控制系统
TC	Transparent Clock	透传时钟
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
UDP	User Datagram Protocol	用户数据报协议
USM	User-Based Security Model	安全模型
VLAN	Virtual Local Area Network	虚拟局域网
WINS	Windows Internet Naming Service	Windows Internet 名称服务
WRR	Weighted Round Robin	加权轮询调度