ZXR10 5009（V1.0）千兆接入交换机
用户手册

中兴通讯股份有限公司

ZXR10 5009（V1.0）千兆接入交换机
用户手册

资料版本　20060701-R1.0
产品版本　V1.0

策　　划　中兴通讯学院　文档开发部

编　　著　胡鹏 赵志强 周继华

审　　核　虞成军

*　*　*　*

中兴通讯股份有限公司

地址：深圳市高新技术产业园科技南路中兴通讯大厦

邮编：518057

技术支持网站：http://support.zte.com.cn

客户支持中心热线：（0755）26770800　　800-830-1118

传真：（0755）26770801

E-mail：doc@zte.com.cn

*　*　*　*

编号：sjzl20061267

声　明

ZTE和ZTE中兴是中兴通讯股份有限公司的注册商标。中兴通讯产品的名称和标志是中兴通讯的专有标志或注册商标。在本手册中提及的其他产品或公司的名称可能是其各自所有者的商标或商名。在未经中兴通讯或第三方商标或商名所有者事先书面同意的情况下，本手册不以任何方式授予阅读者任何使用本手册上出现的任何标记的许可或权利。

本产品符合关于环境保护和人身安全方面的设计要求，产品的存放、使用和弃置应遵照产品手册、相关合同或相关国法律、法规的要求进行。

由于产品和技术的不断更新、完善，本资料中的内容可能与实际产品不完全相符，敬请谅解。如需查询产品的更新情况，请联系当地办事处。

若需了解最新的资料信息，请访问网站 http://support.zte.com.cn

FAX：0755-26772236

意见反馈表

为提高中兴通讯用户资料的质量，更好地为您服务，希望您在百忙之中提出您的建议和意见，并请传真至：0755-26772236，或邮寄至：深圳市高新技术产业园科技南路中兴通讯大厦中兴通讯学院文档开发部收，邮编：518057，邮箱：doc@zte.com.cn。对于有价值的建议和意见，我们将给予奖励。

资料名称	ZXR10 5009（V1.0）千兆接入交换机用户手册					
产品版本	V1.0		资料版本	20060701-R1.0		
您单位安装该设备的时间						
为了能够及时与您联系，请填写以下有关您的信息						
姓名		单位名称				
邮编		单位地址				
电话		E-mail				
您对本资料的评价		好	较好	一般	较差	差
	总体满意					
	工作指导					
	查阅方便					
	内容正确					
	内容完整					
	结构合理					
	图表说明					
	通俗易懂					
您对本资料的改进建议		详细说明				
	内容结构					
	内容详细					
	内容深度					
	表达简洁					
	增加图形					
	增加实例					
	增加 FAQ					
	其　　他					
您对中兴通讯用户资料的其他建议						

前　言

手册说明

本手册为《ZXR10 5009（V1.0）千兆接入交换机用户手册》，适用于 ZXR10 5009 千兆接入交换机。

ZXR10 5009（V1.0）千兆接入交换机，在正文中简称 ZXR10 5009，在通用部分也简称为交换机。

在 5~9 章的配置、使用、维护描述中只列出相关的命令，所有命令详细的使用方法请参见第 10 章命令参考。

内容介绍

本手册共有 10 章，1 个附录。

第 1 章 安全说明。介绍安全说明和符号说明。

第 2 章 系统介绍。对 ZXR10 5009 系统进行整体介绍。

第 3 章 结构和原理。介绍 ZXR10 5009 的结构和原理。

第 4 章 安装和调试。介绍 ZXR10 5009 的安装步骤和调试方法。

第 5 章 使用和操作。介绍 ZXR10 5009 的配置方式、命令模式，以及命令行的使用。

第 6 章 系统管理。介绍 ZXR10 5009 的系统管理。

第 7 章 业务配置。介绍 ZXR10 5009 的业务数据配置。

第 8 章 网络管理。介绍 ZXR10 5009 的网络管理配置。

第 9 章 维护。介绍 ZXR10 5009 的日常维护。

第 10 章 命令参考。介绍 ZXR10 5009 支持的命令。

附录 A 缩略语。

本书约定

1. 符号约定

带尖括号“< >”表示键名、按钮名以及操作员从终端输入的信息；带方括号“[ ]”表示人机界面、菜单条、数据表和字段名等，多级菜单用“→”隔开。如［文件→新建→文件夹］多级菜单表示［文件］菜单下的［新建］子菜单下的［文件夹］菜单项。

2. 键盘操作约定

格式	意义
加尖括号的字符	表示键名、按钮名。如＜Enter＞、＜Tab＞、＜Backspace＞、＜a＞等分别表示回车、制表、退格、小写字母 a
＜键 1+键 2＞	表示在键盘上同时按下几个键。如＜Ctrl+Alt+A＞表示同时按下“Ctrl”、“Alt”、“A”这三个键
＜键 1，键 2＞	表示先按第一键，释放，再按第二键。如＜Alt，F＞表示先按＜Alt＞键，释放后，紧接着再按＜F＞键

3. 鼠标操作约定

格式	意义
单击	快速按下并释放鼠标的左键
双击	连续两次快速按下并释放鼠标的左键
右击	快速按下并释放鼠标的右键
拖动	按住鼠标的左键不放，移动鼠标

4. 本手册中命令的格式约定如下：

约定	描述
/* */	注释，不需要输入的内容
粗体字	表示命令或关键字
<斜体字>	表示需设置的参数
|	用于分隔若干选项，表示二选一或多选一
[ ]	方括号中的关键字或参数为可选项
{ }	大括号中的关键字或参数为必选项
{x|y|z}	表示必须选择 x，y，z 中的一个
[x{y|z}]	方括号中的内容是可选的，但如果选择了方括号中的内容，就必须选择大括号中 y，z 中的一个

5. 标志

本书采用四个醒目标志来表示在操作过程中应该特别注意的地方。

 **注意**、  **小心**、  **警告**、  **危险**：提醒操作中应注意的事项。

目 录

图目录

表目录

第1章 安全说明

摘要

本章介绍安全说明和符号说明。

1.1 安全说明

本设备只有经过培训合格的专业人员才能进行安装、操作和维护。

在设备安装、操作和维护中，必须遵守所在地的安全规范和相关操作规程，否则可能会导致人身伤害或设备损坏。手册中提到的安全注意事项只作为当地安全规范的补充。

中兴通讯不承担任何因违反通用安全操作要求或违反设计、生产和使用设备安全标准而造成的责任。

1.2 符号说明

对交换机进行配置操作时需要注意的一些内容，采用如下格式进行说明。

注意：

表示若忽视安全告诫，就有可能发生故障。

说明：

除安全说明以外的需要特别注意的内容。

第2章 系统介绍

摘要

本章对 ZXR10 5009 进行了整体介绍，具体描述了 ZXR10 5009 提供的丰富的软硬件功能、组网方式、技术特性和参数。

2.1 产品概述

ZXR10 5009 千兆接入交换机主要定位于企业网和宽带 IP 城域网的接入层，提供不同数量的以太网端口，适合作为信息化智能小区、商务楼、宾馆、大学校园网和企业网（政务网）的用户侧接入设备或者小型网络的汇聚设备，为用户提供高速、高效、高性价比的接入和汇聚方案。

2.2 功能介绍

ZXR10 5009 采用存储转发（Store and Forward）模式，支持线速（Wire-speed）二层交换，所有端口全线速交换。

ZXR10 5009 具有以下功能：

1. 支持 MAC 地址自学习能力，MAC 地址表大小为 8K。
2. 支持端口 MAC 地址捆绑，支持地址过滤。
3. 支持 802.1q 标准的 VLAN，支持私有边界 VLAN，VLAN 数最多为 4094 个，支持 VLAN 堆叠功能。
4. 支持按 DA、SA、VID、TOS/DSCP 来进行优先级划分，支持多队列、支持固定优先级调度、支持加权优先级调度，交换机中的端口多队列。
5. 支持 802.1d 标准的生成树（STP）、802.1w 快速生成树（RSTP）和 802.1s 标准的多生成树（MSTP）。
6. 支持 802.3ad 标准的 LACP 端口捆绑，支持端口静态捆绑，支持最多 8 组端口捆绑，每组最多 8 个成员端口。
7. 支持跨 VLAN 的 IGMP snooping。
8. 支持 IPTV 可控组播功能。

9. 支持端口入口镜像、出口镜像。
10. 支持 802.3x 流控（全双工）和背压式流控（半双工）。
11. 支持端口入口和出口带宽限制。
12. 支持单端口环路检测。
13. 支持 VCT 功能，故障线路测试。
14. 提供详细的端口流量统计。
15. 支持广播风暴抑制。
16. 支持网络管理静态路由设置。
17. 支持 802.1x 透传和认证。
18. 支持 syslog 日志功能。
19. 支持 NTP 客户端功能。
20. 支持 GARP/GVRP 动态 VLAN。
21. 支持 Console 配置、Telnet 远程登录、WEB 页面访问和 SNMP 网管，ZXNM01 统一网管，支持集群管理技术 ZGMP，支持 Secure shell V2.0。
22. 支持 TFTP 版本上传和下载。

2.3 组网方式

ZXR10 5009 系列千兆接入交换机的组网方式非常灵活,下面介绍两种典型的组网方式。

2.3.1 工作组级组网方式

对于企业、部门等工作组级的组网，ZXR10 5009 可以灵活方便地应用于多种网络。ZXR10 5009 提供 9 个 10/100/1000M 接口，并可通过级联方式扩展接口数量。

典型的组网结构图如 图 2.3-1所示。

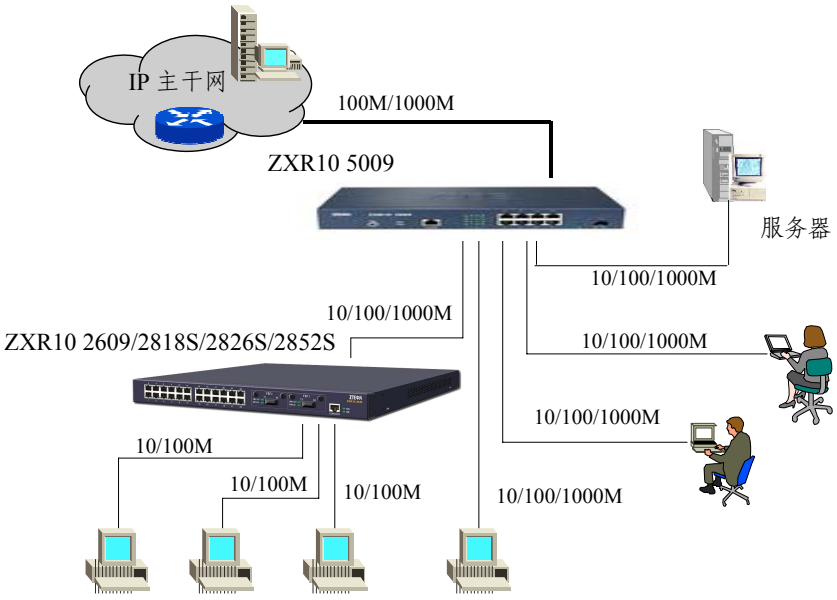


图2.3-1　工作组典型组网图

2.3.2 城域网宽带接入组网方式

在宽带城域网建设中，ZXR10 5009 可用于小区的接入层或楼宇的汇聚层，直接对用户提供 10/100M 接入或下带接入层交换机（如 ZXR10 2826S 等）。利用 ZXR10 5009 GE 端口上联到小区的汇聚节点，协同 BRAS（宽带接入服务器）、AAA 服务器等网络管理系统，完成信息化小区宽带业务网的组建。

对小区 ZAN（驻地网）设备的管理，可采用带内或带外方式，纳入整个城域网的网络管理系统或在小区内部自行设立网络管理和业务管理系统。

典型的组网结构图如 图 2.3-2所示。

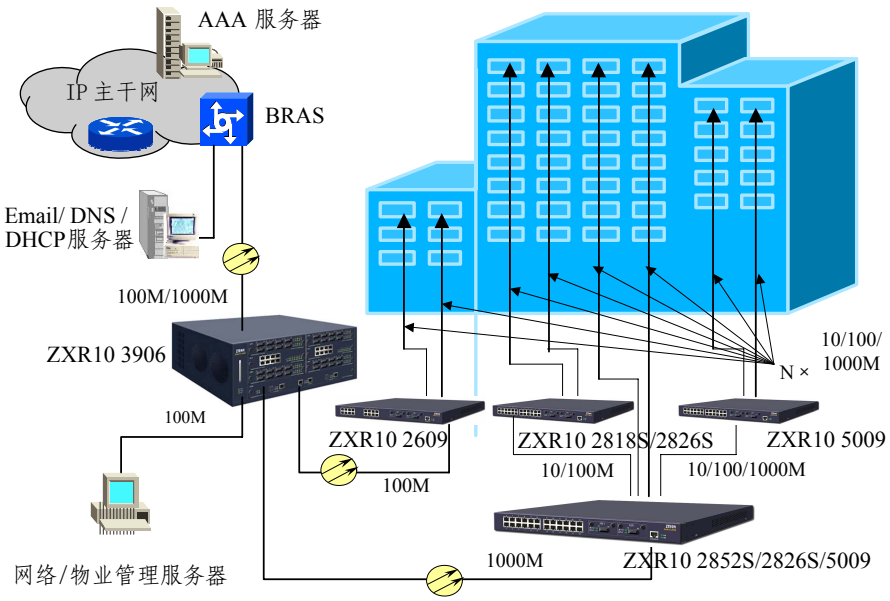


图2.3-2　城域网宽带接入典型组网图

2.4 技术特性和参数

表 2.4-1详细列出了ZXR10 5009 的技术特性和参数。

表2.4-1　技术特性和参数

型号 / 项目	ZXR10 5009
尺寸（高×宽×深，mm）	43.6× 280× 180
重量（最大配置，kg）	≈2
最大功耗（W）	15
电源	交流电源：100V~240V，48Hz~62Hz，波形失真<5% 直流电源：-57V~-40V

第3章 结构和原理

摘要

本章介绍了 ZXR10 5009 的结构和原理，并对系统的硬件结构进行了详细的描述。

3.1 工作原理

ZXR10 5009 是中兴通讯推出的一款 2 层可网管的中低端纯千兆以太网交换产品，用于用户的千兆接入，主要在大企业网、高档行业用户中使用。本款产品按照系统功能划分，主要包括控制模块、交换模块、接口模块、电源模块。系统原理图如 图 3.1-1所示。

1. 控制模块：控制模块由主处理器和一些外部功能芯片组成，实现对交换模块的控制、管理以满足各种组网应用的需要。它对外提供串口，以进行数据操作和维护。
2. 交换模块：交换模块主要为专门的以太网交换处理芯片，完成对各端口送来数据包的处理和交换，同时芯片内部集成有数据包收发功能模块，可以直接出用户千兆光口。
3. 接口模块：接口模块主要由物理层芯片组成，主要完成对外用户连接和数据包的收发，接口模块和交换模块之间采用标准接口互连。
4. 电源模块：电源模块采用 220V 交流供电，为系统内其他部分提供所需的电源。

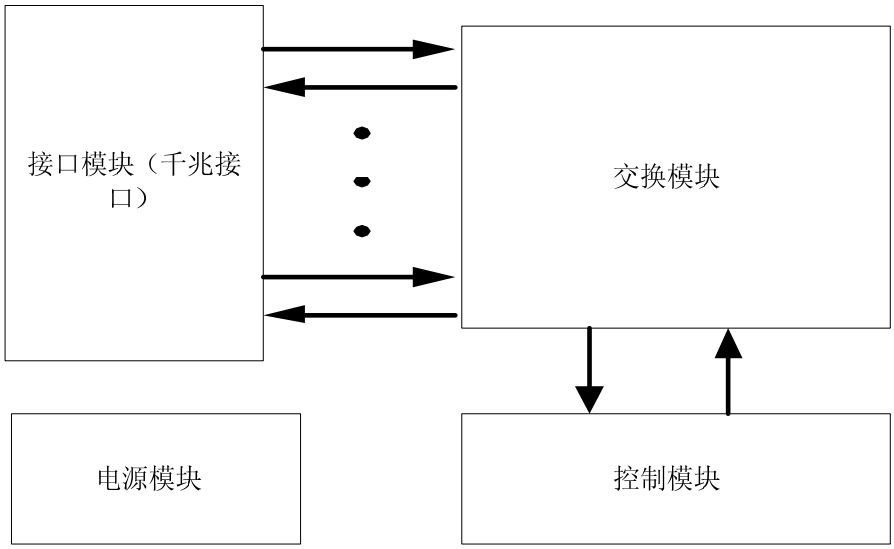


图3.1-1　ZXR10 5009 系统原理示意图

ZXR10 5009 整机尺寸小巧，既可以单独外置，也可以通过特制的挂耳固定安装在标准机柜中。

3.2 硬件结构

ZXR10 5009 采用 1U 高度的盒式结构，独立电源供电，采用风扇强制散热方式，后面和左、右两面开通风孔。盒体主要由底壳和外壳组成，重量轻，结构简单，所有零、部件都安装在底壳上，安装、拆卸较方便。

ZXR10 5009 的前面板上有电源指示灯、运行指示灯、固定以太网电口、以太网光接口及 1 个串行配置口，后面板上有交流电源接口。

ZXR10 5009 的基本硬件为以太网交换主板，其中以太网主板在任何配置时都必不可少。

ZXR10 5009 的前面板如 图 3.2-1所示。

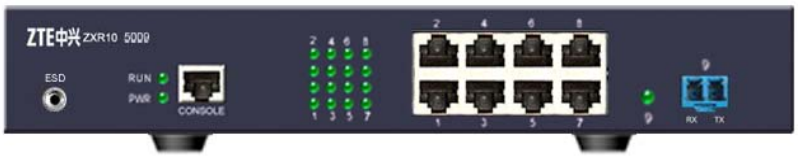


图3.2-1　ZXR10 5009 前面板

ZXR10 5009 的以太网交换主板为 LEBN，其接口和指示灯如下所示：

1. 接口

ZXR10 5009 提供如下类型的接入端口：

（1） 提供 8 个 10/100/1000BASE-T 以太网电口和 1 个 1000BASE-X 上行光口。

（2） 1 个 Console 口，用于实现对各种业务的管理和配置。

2. 指示灯

ZXR10 5009 在机壳的前面板采用 16 个指示灯来表示 8 个千兆电口的状态，每端口 2 个指示灯，分别表示端口的 LNK/ACT 和 DUP/COL 状态，采用一个指示灯表示千兆光口的 LINK/ACT 状态，2 个系统指示灯分别表示电源指示灯（PWR）和运行指示灯（RUN）。

（1） 系统指示灯包括电源指示灯（PWR）和运行指示灯（RUN），它们的指示状况如下：

- 系统上电后，电源指示灯（PWR）亮，运行灯（RUN）灭；
- BootROM 开始加载版本，如果没有版本，指示灯无变化；如果版本正常加载，运行灯（RUN）以 1 秒为周期闪烁。

（2） 16 个端口口指示灯对应 8 个固定以太网电口：LNK/ACT 指示灯常亮，表示 LINK 有效，指示灯闪烁，表示有数据收发。DUP/COL 指示灯在全双工时常亮，半双工时灭，有冲突时闪烁。

（3） 千兆光口的指示灯指示灯常亮，表示 LINK 有效，指示灯闪烁，表示有数据收发。

3.3 电源模块

ZXR10 5009 支持 110V/220V交流供电方式。当使用交流供电时，采用交流电源线。交流供电时的后面板图如 图 3.3-1所示。

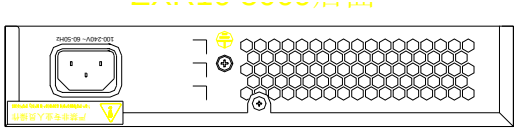


图3.3-1 ZXR10 5009 后面板（交流供电）

第4章 安装和调试

摘要

本章详细介绍 ZXR10 5009 的安装和调试过程，使用户掌握产品的安装和调试方法。

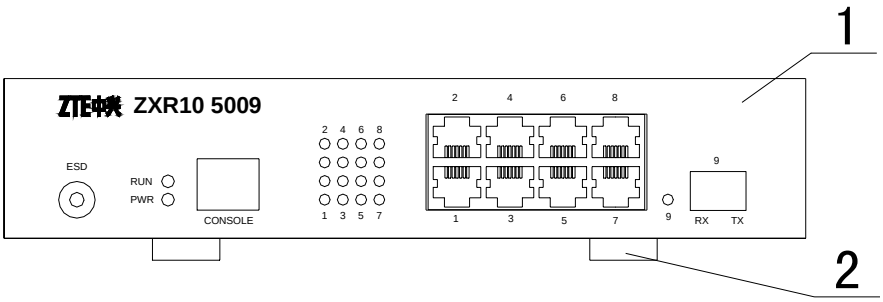
4.1 设备安装

ZXR10 5009 千兆接入交换机整机尺寸小巧既可以安放在桌面上，也可以通过特制的挂耳固定安装在标准机柜中。

其中 19 英寸标准机柜可以由用户提供，当中兴通讯提供机柜时，机柜的安装请参见《19 英寸标准机柜安装手册》。

4.1.1 桌面安装

将交换机放到桌面上工作时，应在交换机的底板安装四个塑料垫脚（塑料垫脚和安装螺钉随机附带）。安装方法如 图 4.1-1所示。

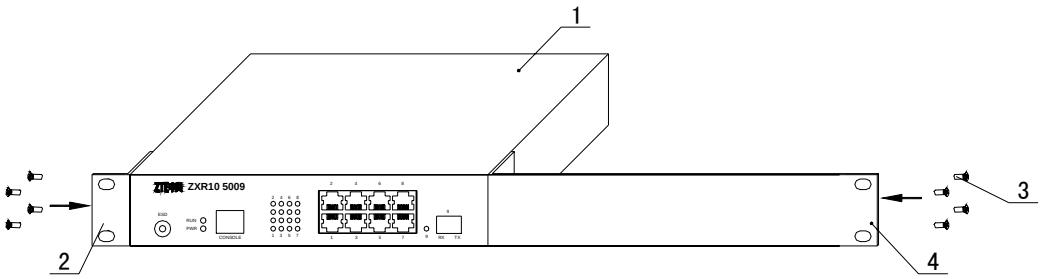


1 机盒　2 垫脚

图4.1-1　塑料垫脚安装

4.1.2 上架安装

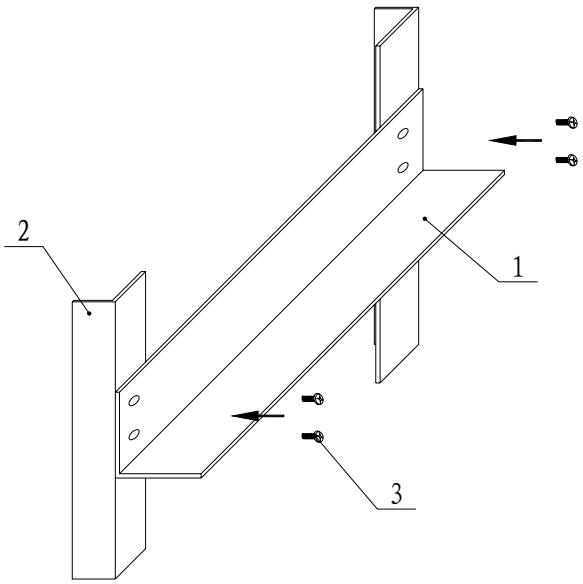
为了将交换机安装到 19 英寸机柜上，需要在交换机的壳体两侧安装一个法兰和特制的挂耳（随机附带），如 图 4.1-2所示。



1 机盒　2 法兰　3 安装螺钉 4 特制挂耳

图4.1-2　法兰安装

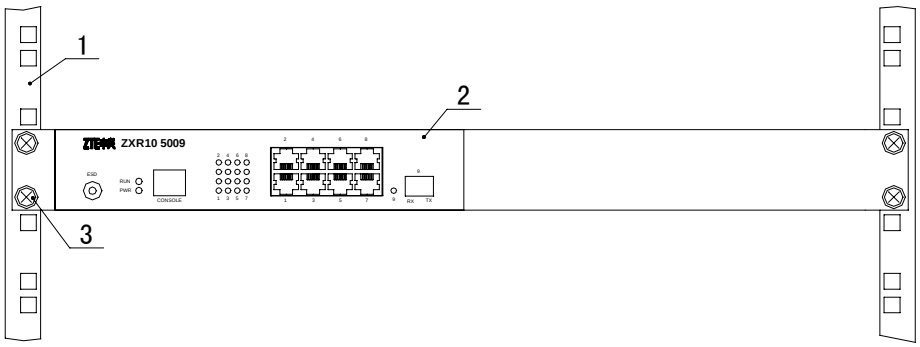
在 19 英寸机柜的两侧安装两个对称的托板，用于支撑交换机，如 图 4.1-3所示。



1 托板　2 机架　3 螺钉　4 特制挂耳

图4.1-3　托板的安装

在安装好托板以后，将交换机沿着托板推入，并用螺钉将法兰固定到机柜上。如图 4.1-4所示。



1 机架 2 机盒 3 皇冠螺钉

图4.1-4 设备的固定

4.2 线缆安装

ZXR10 5009 的线缆包括电源线、配置线、网线和光纤。

4.2.1 电源线安装

交流电源线外形基本与标准的打印机电源线相同，除了线径相对略细，如 图 4.2-1 所示。

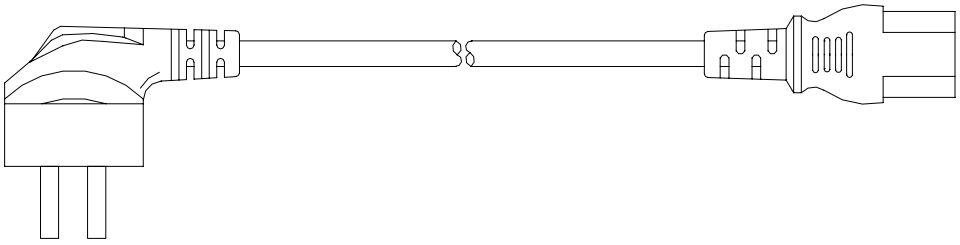


图4.2-1 交流电源线

交流电源线一端连接到 ZXR10 5009 交流电源模块的交流电源插座，另一端连接到 220V 交流电源插座。

4.2.2 配置线安装

串口配置线是配置 ZXR10 5009 的基本线缆，用于对设备进行配置和日常维护。

ZXR10 5009 随机附带串口配置线，一头为DB9 串行接口（与计算机串口连接），另一头为RJ45 口（与ZXR10 5009 的Console口连接）。串口配置线的示意图如 图 4.2-2所示，线序如 表 4.2-1所示。

A向放大

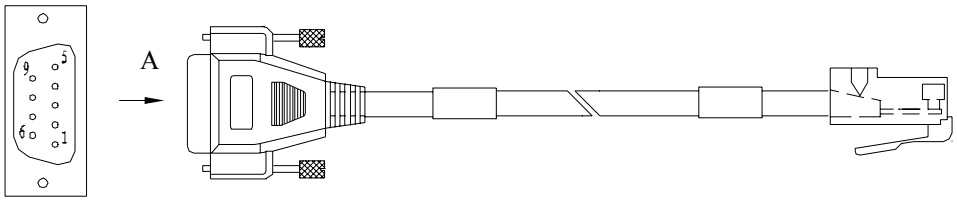


图4.2-2　串口配置线示意图

表4.2-1　串口配置线线序表

A 端	色谱	B 端
2	白	3
3	蓝	6
5	白	4
	橙	5
4	白	7
6	绿	2
7	白	8
8	棕	1

4.2.3 网线安装

网线的两端压接RJ45 插头，结构如 图 4.2-3所示。

- 电缆插头名称为：8P8C 直式电缆压接插头。
- 规格型号为：E5088-001023。
- 技术参数为：额定电流 1.5A 额定电压 125V 压接 AWG24-28#线规圆线。

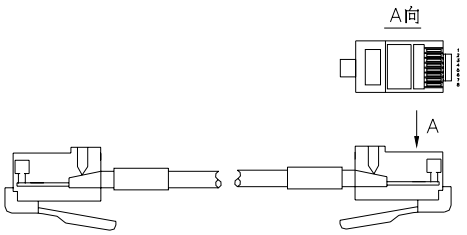


图4.2-3 网线结构示意图

电缆在插头中压接线序的不同可以将电缆分为如下两类：

- 平行网线RJ45，电缆的连接关系基本为两端一一对应，具体的接线关系如表 4.2-2所示。

表4.2-2 平行网线 RJ45 线序表

A 端	电缆色谱	B 端
1	白橙	1
2	橙	2
3	白绿	3
6	蓝	6
4	白蓝	4
5	绿	5
7	白棕	7
8	棕	8

- 交叉网线RJ45J，电缆的连接关系为两端的两对双绞线互调位置对应，具体的接线关系如 表 4.2-3所示。

表4.2-3 交叉网线 RJ45J 线序表

A 端	电缆色谱	B 端
1	白橙	3
2	橙	6
3	白绿	1
6	蓝	2
4	白蓝	4
5	绿	5
7	白棕	7
8	棕	8

4.2.4 光纤安装

ZXR10 5009 的每个光接口有两根光纤，一根收，一根发，注意面板上TX，RX标记，不要插错。光纤分为单模和多模两种，用户可根据实际使用情况配置如 表 4.2-4 所示 6 种类型的光纤。

表4.2-4　光纤类型表

模式	交换机端接头类型	对端接头类型
单模光纤	SC-PC 头（方形平头） LC-PC（小方形平头）	FC/PC 头
		SC/PC 头
		ST/PC 头
		LC-PC 头
多模光纤	SC-PC 头（方形平头） LC-PC（小方形平头）	FC/PC 头
		SC/PC 头
		ST/PC 头
		LC-PC 头

对于出机柜的光纤布线，一定要用塑料的波纹保护套管保护光纤不受损伤。在保护套管内的光纤尽量保证不互相缠绕，拐弯处做成圆弧形。光纤两端的标签标志要清晰，标签的含义需要正确反映出机柜和机柜之间、行与行的对应序号以及对应关系。

4.2.5 标签式样

1. 插头上粘贴的标签样式以及含义

   插头上粘贴的标签名称为：面板、插头用横式英文版标签，标签结构尺寸如 图 4.2-4所示。

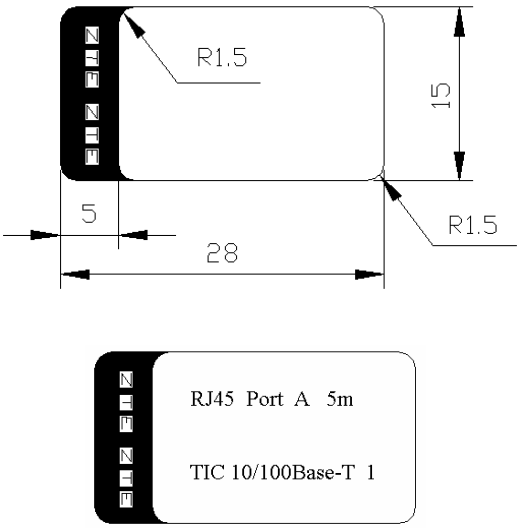


图4.2-4　面板、插头用横式英文版标签

标签内容含义如下：

RJ45－－电缆英文编号，对应的中文名称为：平行网线。

Port A－－电缆插头的 A 端，对应于 B 端或者其他端头。

5m－－电缆的成品长度，是从电缆一端插头开始到另一端插头结束时直线长度。

TIC 10/100Base-T 1－－插接位置，TIC 板 10/100Base-T 的第一个网口。

2．　电缆上卷贴标签的标签样式以及含义

电缆上卷贴的标签名称为：卷式自覆盖激光打印II型标签，标签结构尺寸如 图 4.2-5所示。

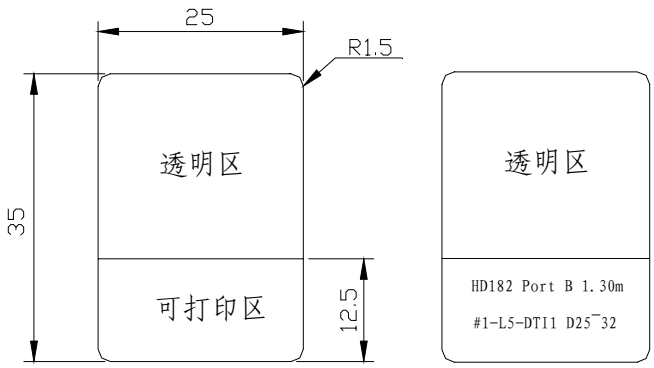


图4.2-5　卷式自覆盖激光打印 II 型标签

图 4.2-5标签内容含义同 图 4.2-4的标签内容描述，和面板、插头用横式英文版标签的不同之处在于其使用场合不同：面板，插头用横式英文版标签只能够使用于粘贴面积大于标签面积的插头或者面板上。而卷式自覆盖激光打印标签是当电缆插头较小，或者用该标签影响电缆的美观时，不能够使用横式英文版标签时，在电缆上用自带的透明胶纸将标签卷贴在电缆上的方式实现。

3. 机柜设备出厂前内部互连电缆上卷贴的旗帜式样的去向标签

电缆上卷贴的标签名称为：横式英文版I型标签，标签的结构尺寸如 图 4.2-6 所示。标签内容标注方法同 图 4.2-4。

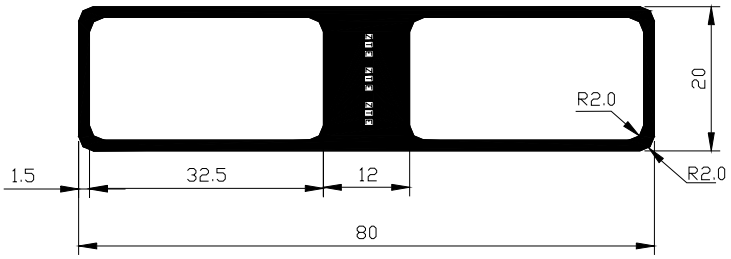


图4.2-6　横式英文版 I 型标签

4. 光纤工程标签内容含义以及结构示意图如 图 4.2-7所示。

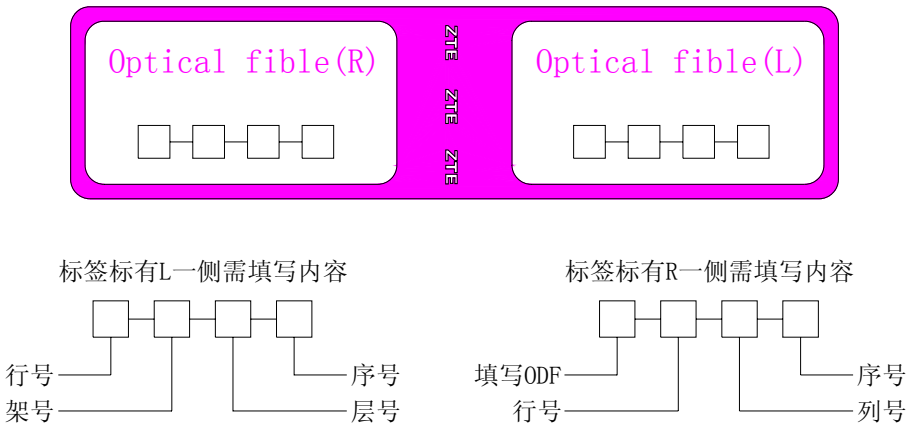


图4.2-7 光纤工程标签图及含义

光纤工程用去向标签上两侧分别标有 L 和 R，其具体含义分别如下：

- 当标签是粘贴在 ZXR10 5009 一侧的光纤上时，标签中 R 一侧的内容应该填写的是远端连接的光口设备侧机柜的行号、列号、光纤在机柜的层数以及光纤的序号。而此时标签上标有 L 一侧的内容应该填写的是光纤所在的设备所处的行号、列号、光纤所在的层数以及光纤的序号。
- 当标签是粘贴在局方的光口设备时，标签中填写的内容于粘贴在 ZXR10 5009 一侧标签的内容相反。

4.3 布线防雷要求

雷击按照其危害程度主要分为直击雷和感应雷，直击雷的雷击损坏几乎难以避免，而良好的防护措施能有效的防范感应雷的危害。对此提出以下工程防雷要求，以降低雷击多发地区设备故障率。

1. 以太网交换机应放在楼道内，且最好放在一楼，不得放在室外无气候防护条件下使用，以避免日晒、雨淋和雷击。保证除上行、下行及级联线外的所有用户线全部在楼内布置以尽量避免感应雷的袭击。

   如 图 4.3-1所示为一幢四层三个单元大楼的以太网交换机布线示意图。其中一单元的交换机A为整幢楼的汇聚交换机，其余的B和C为接入交换机，A、B、C互相级联，即A的级联线作为B的上行线，B的级联线作为C的上行线，而剩下的用户线均在楼内布线，由下至上由楼道内接入用户。

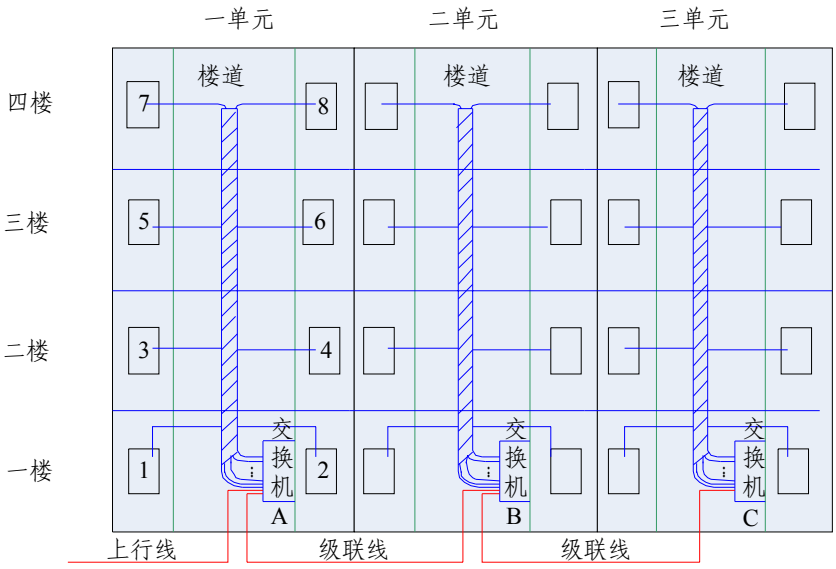


图4.3-1　某大楼以太网交换机楼内布线示意图

其中图中的 1~8 代表用户，级联线指连接交换机的线缆。

2. 引到室外的上行、下行、级联等以太网端口应保证采取加强防雷措施，增加防雷排，若特殊情况下普通用户线需要室外布线，也应该增加防雷排。防雷排的雷击防护能力应达 6KV 以上，电流泻放能力应达到 5KA，防雷排的接地线直径应达到 16mm^2，长度不大于 30cm。大楼的汇聚交换机的上行端口建议采用光口，如采用电口应增加防雷排。

   如 图 4.3-2为某汇聚交换机的端口线布局示意图，其中上行线采用光口，下行或级联线采用防雷排进行防雷保护，防雷排通过机壳地与大地相连，其余的用户线在楼内布线。

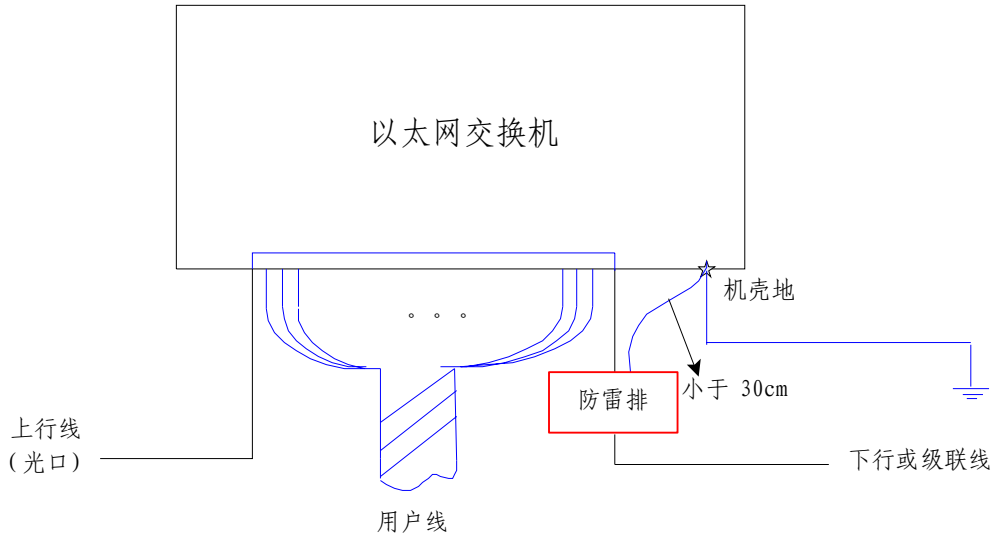


图4.3-2 某汇聚交换机布线示意图

3. 交换机的接地优先采用有良好接地网的大楼的接地系统（很多接地良好的居民楼有小于 1 欧姆的接地电阻），若经过测试不满足要求，再考虑单独设置接地桩，接地线的直径应达到 16 mm^2，长度尽可能的短。无论何种接地方式，应保证接地电阻小于 5 欧姆，最大不得超过 10 欧姆。

4. 禁止交换机直接从室外架空电源线上取电。若遇必须采用室外架空线电源线取电时，电源应该增加专门的防雷措施，如防雷插座和防雷排等，电源防雷排的指标要高于上述端口线的防雷排指标。

5. 以太网交换机受到雷击的影响因素很多（包括接地、电源及布线等），雷击的引入机理差别也比较大，仅仅做到一项措施是远远不够的，防雷必须多种措施同时实施。但是如果做到良好的接地、合适的电源、合理的布线及适当的防雷措施，雷击损坏现象肯定会得到很好的改善。

4.4 系统调试

4.4.1 配置连接

ZXR10 5009 的调试配置一般是通过 Console 口连接的方式进行，Console 口连接配置采用 VT100 终端方式，下面以 Window 操作系统提供的超级终端工具配置为例进行说明。

1. 将PC机与ZXR10 5009 进行正确连线之后，点击系统的[开始→程序→附件→通讯→超级终端]，进行超级终端连接，如 图 4.4-1所示。

图4.4-1　超级终端连接

2. 在出现 图 4.4-2时，按要求输入有关的位置信息：国家/地区代码、地区电话号码编号和用来拨外线的电话号码。

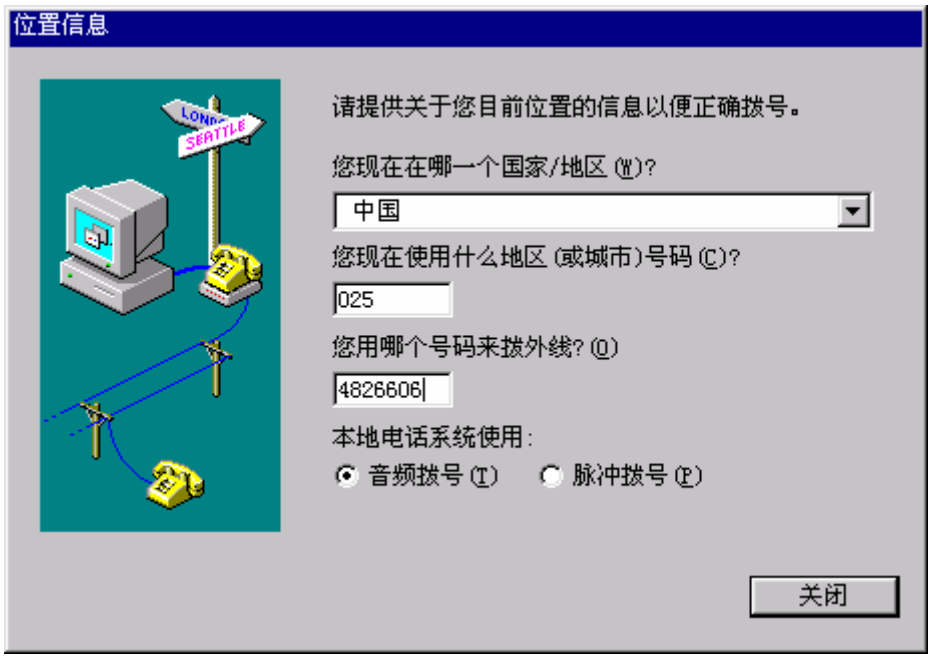


图4.4-2　位置信息

3. 弹出[连接说明]对话框时，为新建的连接输入名称并为该连接选择图标。如 图 4.4-3所示。

图4.4-3 新建连接

4. 根据配置线所连接的串行口，选择连接串行口为COM1 或者COM2。如 图4.4-4所示。

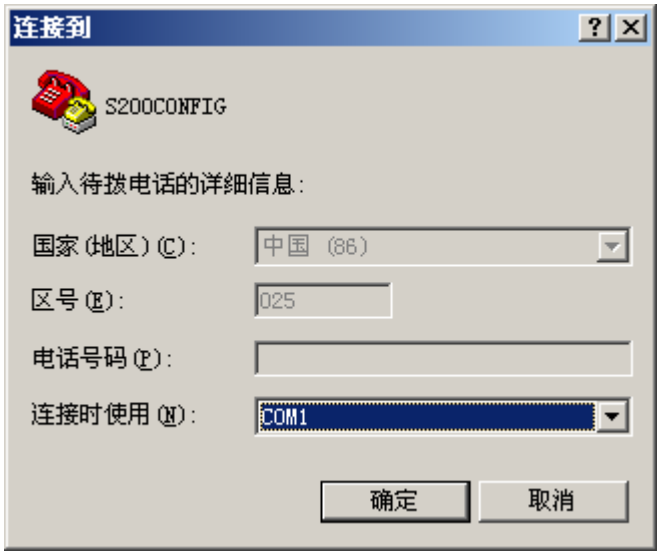


图4.4-4 连接配置资料

5. 设置所选串行口的端口属性

端口属性的设置主要包括以下内容：波特率“9600”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”，如 图 4.4-5所示。

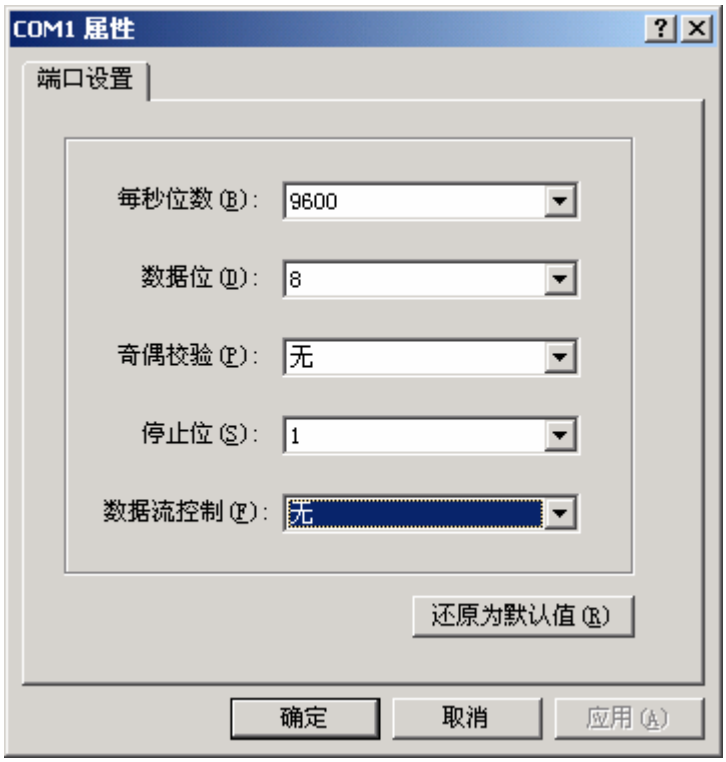


图4.4-5　端口属性配置设置

检查前面设定的各项参数正确无误后，ZXR10 5009 就可以加电启动，进行系统的初始化，进入配置模式进行操作。

4.4.2 上电步骤

ZXR10 5009 上电之前，需要对机房环境、硬件安装情况进行检查。

1. 检查机房温度、湿度和电源电压是否符合如 表 4.4-1所示的安装要求。

表4.4-1　温湿度表

项目	温度（℃）		相对湿度（%）	
	长期工作条件（注 1）	短期工作条件（注 2）	长期工作条件	短期工作条件
范围	15℃~30℃	-5℃~45℃	30%~70%	20%~90%

注：

1．ZXR10 5009 正常工作环境下，温、湿度的测量值系指：在地板以上 2m 和设备前方 0.4m 外测量的数值（机柜前后没有保护板时测量）。

2．短期工作条件系指连续不超过 48 小时和每年累计不超过 15 天。

2. 检查电源线、电缆线是否正确，可靠。

3. 检查其他硬件

（1） 设备标签是否齐全、正确、清晰。

（2） 设备安装到 19 英寸标准机架是否牢固。

（3） 交换机的电源开关是否处于关闭位置。

（4） 机架接地是否良好，接地电阻是否符合技术要求。

ZXR10 5009 上电步骤如下：

1. 接上以太网交换机后面的电源线。

2. 开启外部电源。

下电步骤与上电步骤相反：

ZXR10 5009 下电步骤如下：

1. 关闭外部电源。

2. 拔下以太网交换机后面的电源线。

4.4.3 指示灯状态

交换机加电后，系统指示灯变化如下：

1. 系统上电后，前面板电源系统指示灯（PWR）亮，运行灯（RUN）不亮；

2. BootROM 开始加载版本，如果没有版本，指示灯无变化；如果版本正常加载，运行灯（RUN）以 1 秒为周期闪烁。

4.4.4 系统引导过程

系统的启动过程如下：

1. 上电后，首先进行硬件启动，当硬件检测无误后，管理终端上出现下列信息：

```
                Welcome to use ZTE eCarrier!!



Copyright(c) 2004-2006,  ZTE Co., Ltd.
System Booting......
```

```
CPU: WindBond ARM7TDMI
Version: VxWorks5.5.1
BSP version: 1.2/0
Creation date: Apr 28 2006, 17:24:03




Press any key to stop auto-boot...
 7
```

2. 出现上述信息后，等待大约 7 秒，用户可以在这段时间内按任意键进入 boot 状态，修改启动参数。当系统在规定时间未检测到用户输入时，系统便开始自动加载版本，并提示下列信息：

```
auto-booting...


boot device         : wbdEnd
unit number         : 1
processor number    : 0
host name           : tiger
file name           : vxWorks
inet on ethernet (e) : 10.40.47.89
host inet (h)       : 10.40.47.78
gateway inet (g)    : 10.40.47.78
flags (f)           : 0x80

Attaching to TFFS... done.
Loading file :kernel
Uncompressing...
Uncompressed 3209428 bytes Ok.
Loading image... 9418384
Starting at 0x10000...

 (省略)
Welcome !
ZTE Corporation.
All rights reserved.


login:
```

3. 系统启动成功后，出现提示符“login：”，要求输入登录用户名和密码，缺省用户名 admin，密码 zhongxing。

第5章 使用和操作

摘要

本章介绍了 ZXR10 5009 的常见配置方式、命令模式以及命令行的使用。

5.1 配置方式

ZXR10 5009 提供了多种配置方式，如 图 5.1-1所示，用户可以根据所连接的网络选用适当的配置方式。

1. 串口连接配置
2. Telnet 连接配置
3. SNMP 连接配置
4. WEB 连接配置

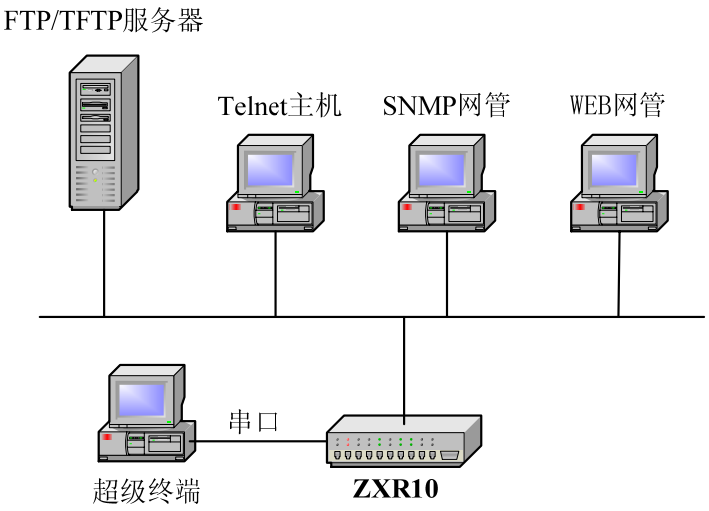


图5.1-1 ZXR10 5009 配置方式

5.1.1 Console 口连接配置

Console口连接配置是ZXR10 5009 的主要配置方式。操作步骤请参见 4.4.1节。也可以在设备运行中进行配置连接。

5.1.2 Telnet 连接配置

Telnet方式通常在远程配置交换机时使用，通过连接到本地以太网口的主机登录到远程交换机上进行配置。交换机上需要设置登录用户名和密码，并且本地主机能够ping通交换机上三层端口的IP地址（三层端口IP地址的配置方法参见 7.12节）。

使用 **create user** <*name*>命令创建一个新的管理用户，使用 **loginpass** [<*string*>]命令设置登录密码。

说明：

缺省的用户名/密码为　admin/zhongxing

假设交换机上三层端口的 IP 地址为 192.168.3.1，本地主机能 ping 通该地址，远程配置操作如下。

1. 在主机上运行telnet命令，如 图 5.1-2所示。

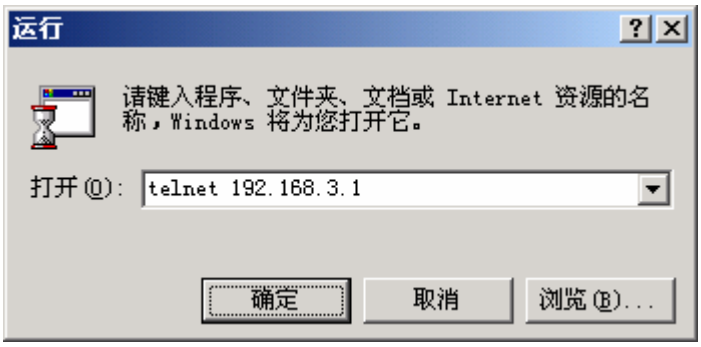


图5.1-2　运行 telnet

2. 点击<确定>按钮，显示Telnet窗口，如 图 5.1-3所示。

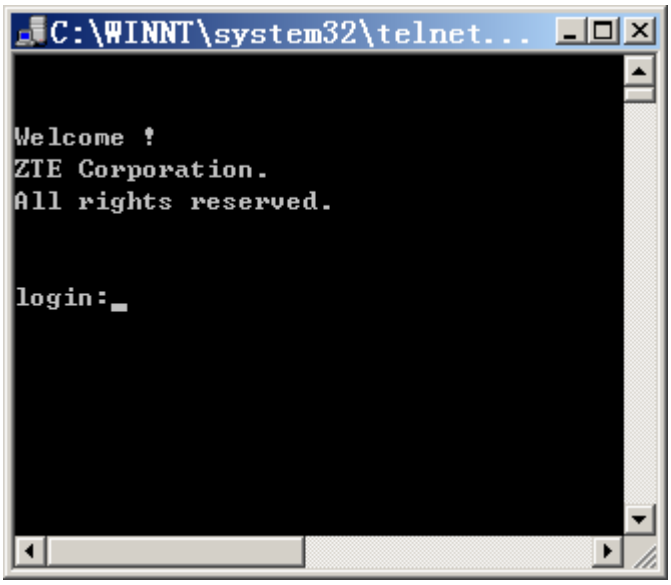


图5.1-3 交换机远程登录示意图

3. 根据提示输入用户名和密码，即可进入交换机的用户模式。

5.1.3 SNMP 连接配置

简单网络管理协议（SNMP，Simple Network Management Protocol）是目前最流行的一种网管协议，通过该协议可以使用一台网管服务器来管理网络中的所有设备。

SNMP 采用基于服务器和客户端的管理，后台网管服务器作为 SNMP 服务器，前台网络设备 ZXR10 5009 作为 SNMP 客户端。前后台共享同一个 MIB 管理库，通过 SNMP 协议进行通讯。

后台网管服务器需安装支持SNMP协议的网管软件，通过网管软件对ZXR10 5009进行管理配置。ZXR10 5009 上SNMP的具体配置请参见 8.3节。

5.1.4 WEB 连接配置

Web是实现远程管理交换机的又一途径，与Telnet相似，通过连接到本地以太网口的主机登录到远程交换机上进行配置。交换机上需要设置登录用户名、登录密码和管理密码，然后使能Web功能，并且本地主机能够ping通交换机上三层端口的IP地址（三层端口IP地址的配置方法参见 7.12节）。

1. 首先创建一个新的管理用户

   create user <*name*>

2. 然后设置登录密码

loginpass <*string*>

3. 再设置管理员密码

   adminpass <*string*>

4. 然后使能 web 网管功能，并设置监听端口

   set web enable

   set web listen-port < 80,1025-49151 >

说明：

缺省的用户名/密码为 admin/zhongxing，管理员密码为空。缺省的 http 监听端口为 80。

假设交换机上三层端口的IP地址为 192.168.1.1，本地主机能ping通该地址，通过Web远程登录并配置交换机请参见 8.6节。

5.2 命令模式

为方便用户对交换机进行配置和管理，ZXR10 5009 根据功能和权限将命令分配到不同的模式下，一条命令只有在特定的模式下才能执行。ZXR10 5009 的命令模式主要包括以下几种：

1. 用户模式
2. 全局配置模式
3. SNMP 配置模式
4. 三层配置模式
5. 文件系统配置模式
6. NAS 配置模式
7. 集群管理配置模式

5.2.1 用户模式

当使用超级终端方式或 Telnet 方式登录交换机时，用户输入登录的用户名和密码后即进入用户模式。用户模式的提示符是交换机的主机名后跟一个“>”号，如下所示：

```
zte>
```

缺省的主机名是 zte，用户可以使用 **hostname** <*name*>命令改变主机名。

在用户模式下可以执行 **exit** 命令退出交换机配置，还可以执行 **show** 命令查看系统的配置信息和运行信息。

说明：

show 命令可以在所有模式下执行。

5.2.2 全局配置模式

在用户模式下输入 **enable** 命令和相应口令后，即可进入全局配置模式，如下所示：

```
zte>enable
Password:***
zte(cfg)#
```

在全局配置模式下可以对交换机的各种功能进行配置，因此必须使用 **adminpass** [<*string*>]命令设置进入全局配置模式的密码，以防止未授权的用户使用。

要从全局配置模式返回到用户模式，可使用 **exit** 命令。

5.2.3 SNMP 配置模式

在全局配置模式下使用 **config snmp** 命令进入 SNMP 配置模式，如下所示：

```
zte(cfg)#config snmp
zte(cfg-snmp)#
```

在 SNMP 配置模式下可以设置 SNMP 和 RMON 的参数。

要退出 SNMP 配置模式返回到全局配置模式，使用 **exit** 命令或按<Ctrl＋Z>。

5.2.4 三层配置模式

在全局配置模式下使用 **config router** 命令进入三层配置模式，举例如下：

```
zte(cfg)#config router
```

```
zte(cfg-router)#
```

在三层配置模式下可以配置三层端口、静态路由以及 ARP 实体。

要退出三层配置模式返回到全局配置模式，使用 **exit** 命令或按<Ctrl＋Z>。

5.2.5 文件系统配置模式

在全局配置模式下使用 **config tffs** 命令进入文件系统配置模式，如下所示：

```
zte(cfg)#config tffs
zte(cfg-tffs)#
```

在文件系统配置模式下可以对交换机文件系统进行操作，包括增加文件或目录、删除文件或目录、更改文件名称、显示文件和目录、改变文件目录、TFTP 文件上/下载、拷贝文件和格式化 Flash 等操作。

要退出文件系统配置模式到全局配置模式，使用 **exit** 命令或按<Ctrl＋Z>。

5.2.6 NAS 配置模式

在全局配置模式下使用 **config nas** 命令进入 NAS 配置模式，如下所示：

```
zte(cfg)#config nas
zte(cfg-nas)#
```

在 NAS 配置模式下可以对交换机接入服务进行配置，包括对用户接入的认证和管理。

要退出 NAS 配置模式到全局配置模式，使用 **exit** 命令或按<Ctrl＋Z>。

5.2.7 集群管理配置模式

在全局配置模式下使用 **config group** 命令进入集群管理配置模式，如下所示：

```
zte(cfg)#config group
zte(cfg-group)#
```

在集群管理配置模式下可以对交换机集群管理服务进行配置。

要退出集群管理配置模式到全局配置模式，使用 **exit** 命令或按<Ctrl＋Z>。

5.3 命令行使用

5.3.1 在线帮助

在任意命令模式下，只要在系统提示符后面输入一个问号（?），就会显示该命令模式下可用命令的列表。利用在线帮助，还可以得到任何命令的关键字和参数列表。

1. 在任意命令模式的提示符下输入问号（?），可显示该模式下的所有命令和命令的简要说明。举例如下：

```
zte>?
  enable            enable configure mode
  exit              exit from user mode
  help              description of the interactive help system
  show              show config information
zte>
```

2. 在字符或字符串后面输入问号（?），可显示以该字符或字符串开头的命令或关键字列表。注意在字符（字符串）与问号之间没有空格。举例如下：

```
zte(cfg)#c?
config  clear  create
zte(cfg)#c
```

3. 在命令、关键字、参数后输入问号（?），可以列出下一个要输入的关键字或参数，并给出简要解释。注意问号之前需要输入空格。举例如下：

```
zte(cfg)#config ?
  snmp              enter SNMP config mode
  router            enter router config mode
  tffs              enter file system config mode
  nas               enter nas config mode
  group             enter group management config mode
zte(cfg)#config
```

4. 如果输入不正确的命令、关键字或参数，回车后用户界面会出现命令未找到的提示。举例如下：

```
zte(cfg)#conf ter
  %  Command not found (0x40000066)
zte(cfg)#
```

在下列实例中，利用在线帮助设置一个用户名。

```
zte(cfg)#cre?
create
zte(cfg)#create ?
  port              create descriptive name for port
  vlan              create descriptive name for vlan
  user              create user
zte(cfg)#create user
  %  Parameter not enough (0x40000071)
zte(cfg)#create user ?
  <name>            user name
zte(cfg)#create user wangkc
zte(cfg)#
```

5.3.2 命令缩写

ZXR10 5009 允许把命令和关键字缩写成能够唯一标识该命令或关键字的字符或字符串。例如，可以把 **exit** 命令缩写成 **ex**；把 **show port** 命令缩写成 **sh po**。

5.3.3 命令历史

用户界面提供了对所输入命令的记录功能，最多可以记录 20 条历史命令，该功能对重新调用长的或复杂的命令特别有用。

从记录缓冲区中重新调用命令，执行下列操作之一。

命令	作用
Ctrl-P 或上箭头<↑>	恢复前一条命令（在命令历史记录中向前翻滚）
Ctrl-N 或下箭头<↓>	恢复下一条命令（在命令历史记录中向后翻滚）

5.3.4 功能键

ZXR10 5009 为用户界面提供了多种功能键，方便用户操作，如 表 5.3-1所示。

表5.3-1 功能键说明表

功能键	用途
Ctrl-P 或上箭头	恢复前一条命令（在命令历史记录中向前翻滚）
Ctrl-N 或下箭头	恢复下一条命令（在命令历史记录中向后翻滚）
Ctrl-B 或左箭头	在提示符当前命令行上向左移动
Ctrl-F 或右箭头	在提示符当前命令行上向右移动
Tab	显示以该字符或字符串开头的命令，如果只有一条命令，则将该命令补齐

功能键	用途
Ctrl-A	跳到命令行首部
Ctrl-E	跳到命令行末端
Ctrl-K	从光标处删除至行尾
Backspace 或 Ctrl-H	删除光标左边的字符
Ctrl-C	退出命令执行，显示提示符
Ctrl-L	清屏
Ctrl-Y	恢复最后执行的一条命令
Ctrl-Z	退回到全局配置模式下

当命令输出超过一页时，会进行自动分页，并在当前页底部用“----- more ----- Press Q or Ctrl+C to break -----”进行提示，这时敲任意键翻页，按< Q >或< Ctrl-C >中止输出。

第6章 系统管理

摘要

本章介绍了 ZXR10 5009 的系统管理，描述了交换机的文件系统及其操作，详细说明了软件版本升级的步骤。

6.1 文件系统管理

6.1.1 文件系统介绍

在 ZXR10 5009 中，主要的存储设备是 FLASH，交换机的版本文件和配置文件都存储在 FLASH 中。升级版本、保存配置都需要对 FLASH 进行操作。

- 版本文件名称为 kernel.z
- 配置文件名称为 running.cfg
- 文本方式配置文件名称为 config.txt

6.1.2 文件系统操作

ZXR10 5009 提供许多命令用于文件系统操作，常见的命令如下。

1. 进入文件系统配置模式

   config tffs

2. 创建目录

   md <*name*>

3. 删除指定文件或目录

   remove <*name*>

4. 更改文件名

   rename <*name*> <*name*>

5. 更改当前目录

   cd

6. 列出当前目录清单

ls

7. TFTP 下载/上载版本

   tftp <*A.B.C.D*> {**download**|**upload**} <*name*>

8. 拷贝文件

   copy <*name*> <*name*>

9. 格式化 FLASH

   format

6.2 设置 TFTP

通过使用 TFTP，可以对交换机版本文件、配置文件进行备份与恢复。在后台启动 TFTP 服务器应用软件，ZXR10 5009 作为 TFTP 的客户端进行通信，实现文件备份与恢复。

下面以 TFTP 服务器软件 tftpd 为例说明后台 TFTP 服务器的设置。

1. 在后台主机运行tftpd软件，出现如 图 6.2-1所示界面。

图6.2-1 TFTPD 界面

2. 点击菜单项[Tftpd→Configure]，在弹出的对话框中点击上面一个<Browse>按钮，选择存放版本文件或配置文件的目录，如 D 盘的 IMG 目录。

3. 点击下面一个<Browse>按钮用来选择日志文件。点击<OK>按钮完成设置。

完成设置后对话框如 图 6.2-2所示。

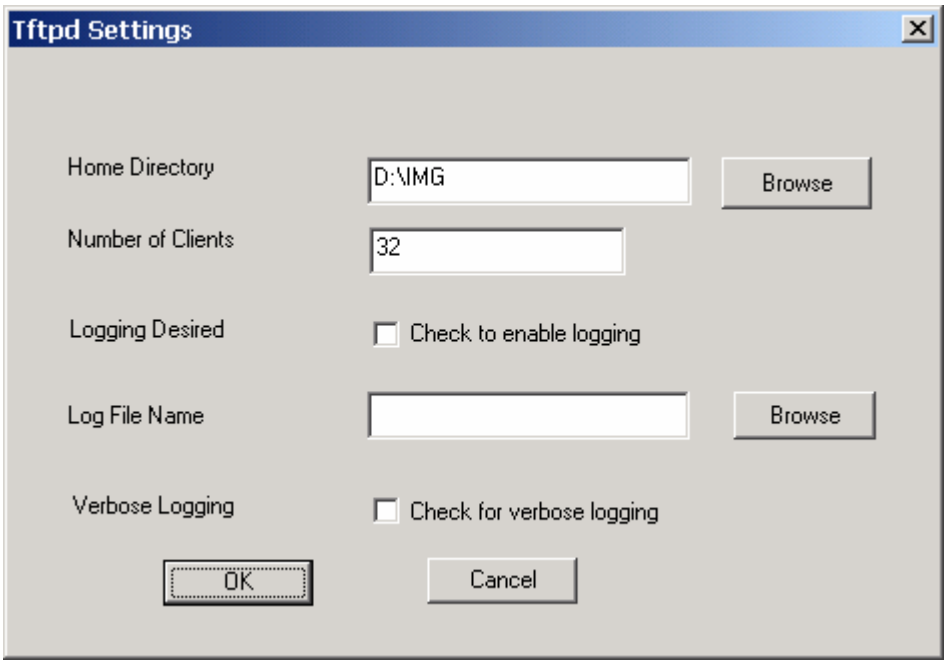


图6.2-2 Configure 对话框

设置完 TFTP 后，就可以对交换机进行 TFTP 应用操作，具体见后续章节。

6.3 配置的导入和导出

ZXR10 5009 提供配置信息的导入和导出功能，使交换机的配置和管理更为简便。

1. 配置导出

利用 **show running-config toFile** 命令，可以将 **show running-config** 命令的执行结果导出到config.txt 文件，存放在FLASH 中。可将该文件上传到TFTP 服务器进行查看。

```
zte(cfg-tffs)#tftp 192.168.1.102 upload config.txt
```

2. 配置导入

使用 **readconfig** 命令，可以将 FLASH 中 config.txt 文件中的配置命令读出并交给交换机解析执行。config.txt 中的内容可以根据需要手动编辑，然后用 **tftp** 命令下载到交换机。

```
zte(cfg-tffs)#tftp 192.168.1.102 download config.txt
```

说明：

readconfig 命令最好在交换机配置为空的时候使用。如果 config.txt 中的配置命令和交换机已有配置有冲突，将导致 config.txt 中的命令在执行过程中发生错误而提前中止。

手动编辑 config.txt 文件时要注意命令执行的先后顺序（部分命令执行时有先后顺序），否则，**readconfig** 也可能会由于执行 config.txt 中的某条命令出错而中止。

6.4 文件的备份和恢复

这里提到的文件备份与恢复是指 FLASH 中的配置文件和版本文件的备份与恢复。

1. 配置文件备份

   当使用命令修改交换机的配置时，这些信息在内存中实时运行。如果交换机重新启动，所有新配置的内容将会丢失，因此需要执行 **saveconfig** 命令将当前配置信息写入 FLASH 中。下面是 **saveconfig** 命令的操作：

```
zte(cfg)#saveconfig
```

   为防止配置信息遭到破坏，可以将其备份。备份操作可用 **tftp** 命令实现。

   执行如下命令可将 FLASH 中的配置文件上传到后台 TFTP 服务器：

```
zte(cfg-tffs)#tftp 192.168.1.102 upload running.cfg
```

   还可以利用**show running-config toFile**命令将配置写入config.txt文件，然后将它备份到TFTP服务器，方法请参见 6.3节。

2. 配置文件恢复

   执行如下命令可将后台 TFTP 服务器中的配置文件下载到 FLASH：

```
zte(cfg-tffs)#tftp 192.168.1.102 download running.cfg
```

3. 版本文件备份

   版本文件备份与配置文件备份类似，使用 **tftp** 命令将前台版本文件上传到后台服务器中。举例如下：

```
zte(cfg-tffs)#tftp 192.168.1.102 upload kernel.z
```

4. 版本文件恢复

版本恢复的目的是把在后台备份的版本文件通过TFTP重新传到前台。在升级失败时进行恢复操作非常重要。版本恢复操作跟版本升级操作步骤基本相同，请参见 6.5节软件版本升级。

6.5 软件版本升级

通常只有在某些功能原有版本不支持或者某些特殊原因导致设备无法正常运行时，才需要进行版本升级。如果版本升级操作不当，可能会导致升级失败，造成系统无法启动。因此，在进行版本升级之前，要求维护人员必须熟悉 ZXR10 5009 的原理和操作，认真学习升级步骤。

版本升级分为交换机系统正常运行状态下的升级和交换机系统运行异常状态下的升级。

6.5.1 查看版本信息

系统状态允许的情况下，在版本升级前和升级完成后都需要查看版本信息。

在全局配置模式下执行 **version** 命令可以显示系统软硬件版本信息。

显示信息如下：

```
zte(cfg)#version
   The System's Hardware Info:
     Switch's Mac Address: 00.d0.d0.f0.11.22

     Module 0: ZXR10  5009; fasteth:  0; gbit: 9;

   The System's Software Info:
     Version number   : V1.1.11.b
     Version make date: Jun 16 2006
     Version make time: 16:27:13

     System has run 0 years 2 days 3 hours 8 minutes 43 seconds

Zte(cfg)#
```

6.5.2 系统正常时的版本升级

如果版本升级之前交换机运行正常，可以使用以下步骤进行升级。

1. 用随机附带的配置线将交换机的 Console 口与后台主机串口相连，用网线将交换机的某一以太网口与后台主机网口相连，确保连接正确。
2. 设置交换机的以太网口地址，设置用于升级的后台主机的地址，与交换机的以太网口同一网段，保证后台主机能够 ping 通交换机。
3. 在后台主机上启动TFTP服务器软件，参见 6.2节进行TFTP服务器配置。
4. 在交换机上用 **version** 命令查看当前运行版本的信息。
5. 进入文件系统配置模式，用 **remove** 命令将 FLASH 中旧的版本文件删除。如果 FLASH 的空间足够，也可以不用删除旧版本，将其改名即可。

```
zte(cfg)#config tffs
zte(cfg-tffs)#remove kernel.z
```

6. 使用 **tftp** 命令进行版本升级。下面是将版本文件从 TFTP 服务器下载到 FLASH 的操作过程：

```
zte(cfg-tffs)#tftp 192.168.1.102 download kernel.z
.................................................................
.....................................
  1,979,157 bytes downloaded
zte(cfg-tffs)#
```

7. 重启交换机，正常启动后，查看运行的版本，确认升级是否成功。

6.5.3 系统异常时的版本升级

当交换机无法正常启动或者运行不正常时，往往不能以正常的方式进行版本升级，此状态下版本升级的具体步骤如下。

1. 用随机附带的配置线将交换机的 Console 口与后台主机串口相连，用网线将交换机的任一以太网口与后台主机网口相连，确保连接正确。
2. 重新启动交换机，在超级终端下根据提示按任意键进入[VxWorks Boot]状态。

```
                Welcome to use ZTE eCarrier!!



Copyright(c) 2004-2006,  ZTE Co., Ltd.
System Booting......
CPU: WindBond ARM7TDMI
```

```
Version: VxWorks5.5.1
BSP version: 1.2/0
Creation date: Apr 28 2006, 17:24:03




Press any key to stop auto-boot...
 5

[ZxR10 Boot]:
```

3. 在[ZxR10 Boot]状态下输入<c>，回车后进入参数修改状态。设置以太网口的地址和 TFTP 服务器的地址，两地址一般设为同一网段。

```
[ZxR10 Boot]: c

'.' = clear field;  '-' = go to previous field;  ^D = quit

boot device          : wbdEnd1         /*使用缺省*/
processor number     : 0               /*使用缺省*/
host name            : tiger           /*使用缺省*/
file name            : vxWorks         /*使用缺省*/
inet on ethernet (e) : 10.40.89.106    /*以太网口的 IP 地址*/
inet on backplane (b):                 /*使用缺省*/
host inet (h)        : 10.40.89.78     /*TFTP 服务器的 IP 地址*/
gateway inet (g)     : 10.40.89.78     /*使用缺省*/
user (u)             :                 /*使用缺省*/
ftp password (pw) (blank = use rsh):   /*使用缺省*/
flags (f)            : 0x80            /*使用缺省*/
target name (tn)     :                 /*使用缺省*/
startup script (s)   :                 /*使用缺省*/
other (o)            :                 /*使用缺省*/
[ZxR10 Boot]:
```

4. 将后台主机地址设为与上述 TFTP 服务器的 IP 地址一致。

5. 后台主机启动TFTP服务器软件，参见 6.2节进行后台主机的TFTP配置。

6. 在[ZxR10 Boot]状态下输入<zte>，进入交换机的[BootManager]状态，输入<?>能够看到该状态下的命令清单。

```
[ZXR10 Boot]: zte
Load wbdEnd Begin
```

```
W90N740 MAC0: 100MB - Full Duplex

BoardType=0x59

Board 5009 !
Marvell has been initialized !
boot device         : wbdEnd
unit number         : 0
processor number    : 0
host name           : tiger
file name           : vxWorks
inet on ethernet (e) : 10.40.47.89
host inet (h)       : 10.40.47.78
gateway inet (g)    : 10.40.47.78
flags (f)           : 0x80

Attached TCP/IP interface to wbdEnd0.
Warning: no netmask specified.
Attaching network interface lo0... done.
Attaching to TFFS...
test flash passed perfectly!
Board type has not been written.
Welcome to boot manager!
Type '?' for help

[BootManager]:?

ls                                          /*列出当前目录清单*/
pwd                                         /*显示当前绝对路径*/
devs                                        /*显示 flash 信息*/
show                                       /*显示交换机类型和 mac 地址*/
reboot                                      /*重启交换机*/
format                                     /*格式化 flash*/
del    file_name                           /*删除指定文件*/
md     dir_name                            /*创建目录*/
mf     file_name                           /*创建文件*/
cd     absolue-pathname                    /*更改当前目录*/
tftp   ip_address file_name                /*TFTP 上传/下载版本*/
update file_name                            /*升级 boot*/
rename  file_name newname                   /*文件重新命名*/
[BootManager]:
```

7. 在[BootManager]状态通过 **tftp** 命令进行版本升级。下面是将版本文件从 TFTP 服务器下载到 FLASH 的操作过程：

```
[BootManager]:tftp 10.40.89.78 kernel.z
Loading... done!
[BootManager]:ls
RUNNING.CFG
KERNEL.Z
[BootManager]:
```

8. 在[BootManager]状态通过 **reboot** 命令用新的版本重启交换机。如果交换机正常启动，通过 **version** 命令查看新的版本是否已在内存中运行；如果交换机不能正常启动，说明版本升级失败，须从步骤 1 开始重新进行操作。

第7章 业务配置

摘要

本章介绍 ZXR10 5009 接入交换机各种业务的配置方法。

7.1 端口配置

7.1.1 基本配置

在 ZXR10 5009 上，可以对端口参数进行配置，如自动协商、双工模式、速率、流量控制、端口优先级、MAC 数目限制等。

端口参数的配置在全局配置模式下进行，主要包括以下内容。

1. 配置端口状态

   set port <*portlist*> {**enable**|**disable**}

2. 设置端口的自适应功能

   set port <*portlist*> **auto** {**enable**|**disable**}

   电口的自适应功能在缺省情况下是打开的，而光口的自适应功能在缺省情况下是关闭的，设置端口工作方式或端口速率后，自适应功能将自动关闭。

3. 设置端口的工作方式

   set port <*portlist*> **duplex** {**full**|**half**}

   对于以太网光口，端口的工作方式只能是全双工，无法改变。

4. 设置端口的速率

   set port <*portlist*> **speed** {**10**|**100**|**1000**}

   对于以太网光口，无法改变端口的速率。

5. 设置端口的带宽

   set port <*portlist*> **bandwidth ingress** {**off**|**on rate** <*70-256000*>}[**tcpdrop**|**flowcontrol**]

   set port <*portlist*> **bandwidth egress** {**off**|**on rate** <*70-256000*>}

交换机以 kbps 为单位进行端口带宽限制，端口的入口带宽和出口带宽可以根据需要分别设置。在设置端口的入口带宽限制时，有三种方式：

- 对无连接的数据包的速率限制，如对广播包进行过滤，粒度在设置的值比较小时为 1K。
- 对有连接的数据包进行速率限制，如 TCP 连接的数据包，此时速率限制的粒度为 70K，范围为 70K~1536K。
- 使用流控的方式对无连接和有连接的数据包进行速率限制，此时必须将端口设置为 10M 半双工的工作方式，粒度在设置的值比较小时为 1K。

对入口端口限速功能，用户可以使用 **set port ingess_limit_mode** 命令选择限速过滤的数据包类型。

说明：

当设置端口入向带宽限制的过滤包类型为广播包时，可以用来实现广播抑止的功能。

在设置端口入向和出向带宽限制时，速率的限制范围为 70k~256M，对于 100M 端口，带宽的最大值为 100M，在设置的速率比较小时，带宽限制的精度很高，当限制速率增大时，带宽限制的精度会逐渐降低，当设置的限制速率大于端口的最大带宽时，端口的速率为端口的最大速率。

配置实例（使用端口带宽限制实现广播风暴的抑制）：设置端口 1 广播抑制功能，限制广播包为 500K。

```
zte(cfg)# set port 1 bandwidth ingress on rate 500
zte(cfg)# set port 1 ingess_limit_mode broadcast
zte(cfg)# show port 1 qos
  PortId :  1
  PortQoSParams:
    IngressRateLimit: 500           EgressRateLimit: 0
    IngressType     : normal        RateLimitMode  : broadcast
    SAPriority      : disable       VlanPriority   : disable
    UserPriority    : enable        DscpPriority   : disable
    DefaultPriority : 0
  PortPriorityRemapTable:
    COS(802.1p user priority), RMP(Remapped priority)
    COS 0   1   2   3   4   5   6   7
```

```
   RMP 0   1   2   3   4   5   6   7
Zte(cfg)#
```

6. 设置端口的流量控制

   set port <*portlist*> **flowcontrol** {**enable**|**disable**}

7. 设置端口的优先级

   set port <*portlist*> **default-priority** <*0-7*>

8. 设置端口的地址学习功能开启/关闭

   set port <*portlist*> **security** {**enable**|**disable**}

   设置为 enable 时关闭端口的 MAC 地址学习功能，设置为 disable 时打开地址学习功能。

9. 设置端口对组播包过滤功能开启/关闭

   set port <*portlist*> **multicast-filter** {**enable**|**disable**}

10. 设置端口对外供电模式

    set port <*portlist*> **poe** {**auto**|**force**|**never**}

11. 设置端口速率宣称

    set port <*portlist*> **speedadvertise** {**maxspeed**|{{**speed 10**|**speed 100**|**speed 1000**} {**fullduplex**|**halfduplex**}}}

12. 设置端口学习 MAC 地址数目

    set port <*portlist*> **macaddress** {**on** <*1-16*>|**off**}

    缺省情况下端口的 MAC 地址限制为关闭，即无限制。

13. 为端口创建描述名称

    create port <*portname*> **name** <*name*>

14. 为端口添加描述

    set port <*portlist*> **description** <*string*>

15. 端口的 QoS 功能

    在每个端口上都支持对数据包优先级的设置，进入端口的数据包的优先级有数据包本身参数和端口上的设置共同决定。在端口上可以对任意一种优先级决定机制进行开启或关闭，没有端口上的接收数据包的优先级决定方

式可以不一样。（各种优先级决定方式的顺序请参照“QoS 参数配置”一节中的说明）

- 开启/关闭端口源 mac 地址优先级功能

  set port <*portlist*> **sa-priority** {**enable**|**disable**}

  当且仅当接收的数据包的源 MAC 地址为静态 mac 地址，并且端口的源 mac 地址优先级决定功能使能时，此时才可能使用设置的源 MAC 地址的优先级决定数据包的优先级。数据包的队列优先级与 SA 优先级的对应关系为：

  （0，1）→0；（2，3）→1；（4，5）→2；（6，7）→3

- 开启/关闭端口 VLAN 优先级

  set port <*portlist*> **vlan-priority** {**enable**|**disable**}

  当且仅当接收数据包所在的 VLAN 的优先级使能，并且端口的 VLAN 优先级决定功能使能时，此时才可能使用设置 VLAN 优先级决定数据包的优先级。数据包的队列优先级与 SA 优先级的对应关系为：

  （0，1）→0；（2，3）→1；（4，5）→2；（6，7）→3

- 开启/关闭端口 802.1P 用户优先级

  set port <*portlist*> **user-priority** {**enable**|**disable**}

  当且仅当接收的数据包是 TAG 数据包，并且端口的 802.1P 用户优先级决定功能使能时，此时才可能使用 802.1P 用户优先级决定数据包的优先级。数据包的队列优先级由 802.1P 用户优先级到队列优先级决定。

- 开启/关闭端口三层 DSCP 优先级

  set port <*portlist*> **dscp-priority** {**enable**|**disable**}

  当且仅当接收的数据包是 IP 数据包，并且端口的三层 DSCP 优先级决定功能使能时，此时才可能使用三层 DSCP 优先级决定数据包的优先级。 数据包的队列优先级由 IP DSCP 优先级到队列优先级对应表决定。

- 设置端口 802.1P 用户优先级重映射表

  set port <*portlist*> **remapping-tag** <0-7> **priority** <0-7>

  当端口收到的数据包是 TAG 数据包时，交换机先使用此映射表对数据包中的优先级进行重新映射，然后使用此优先级作为新的 802.1P 用户优先级来进行以后的优先级决定。此映射表的默认值为：

0→0，1→1，2→2，3→3，4→4，5→5，6→6，7→7

不建议对此默认值进行更改。

端口参数的缺省配置如 表 7.1-1所示。

表7.1-1 端口参数缺省配置

参数	缺省配置
端口状态	打开（enable）
自适应功能	打开（enable）
流量控制	关闭（disable）
带宽限制	关闭（disable）
端口优先级	0

7.1.2 端口信息查看

使用 **show** 命令可以查看端口的相关信息。

1. 显示端口的配置信息和工作状态

show port [<*portlist*>]

查看端口 1 的配置和当前的工作状态。

```
zte(cfg)#show port 1
  PortId    : 1            MediaType : 1000BaseT
  PortParams:
    PortEnable    : enabled    PortAutoNeg    : enabled
    DefaultVlanId  : 1         FlowControl    : disabled
    Multicastfilter: disabled   Security      : disabled
    SpeedAdvertise : MaxSpeed   Twist         : auto
    PortMacLimit   : disabled
  PortStatus:
    PortClass     : 802.3      Link          : down
    Duplex        : half       Speed         : 10Mbps

zte(cfg)#
```

2. 显示端口 QoS 配置数据

show port <*portlist*> **qos**

查看端口 1 的 QoS 配置数据。

```
zte(cfg)#show port 1 qos
```

```
  PortId :  1
  PortQoSParams:
    IngressRateLimit: 0              EgressRateLimit: 0
    IngressType     : normal         RateLimitMode  : broadcast
    SAPriority      : disable        VlanPriority   : disable
    UserPriority    : enable         DscpPriority   : disable
    DefaultPriority : 0
  PortPriorityRemapTable:
    COS(802.1p user priority), RMP(Remapped priority)
    COS 0   1   2   3   4   5   6   7
    RMP 0   1   2   3   4   5   6   7
Zte(cfg)#
```

说明：

当 IngressRateLimit 或 EgressRateLimit 的值为 0，表示端口没有设置带宽限制功能。

3. 显示端口的统计数据

show port <*portlist*> **statistics**

查看端口 1 的统计数据。

```
zte(cfg)#show port 1 statistics
  PortId: 1    PortName:
    ReceivedFrames      : 0          ReceivedBroadcastFrames: 0
    ReceivedBytes       : 0          ReceivedMulticastFrames: 0
    CrcError            : 0          InPause              : 0
    InMACRcvErr         : 0          Jabber               : 0
    Fragments           : 0          UndersizeFrames      : 0
    Frames64Bytes       : 0          Frames65_127Bytes    : 0
    Frames128_255Bytes  : 0          Frames256_511Bytes   : 0
    Frames512_1023Bytes : 0          Frames1024_UpBytes   : 0
    OversizeFrames      : 0
    SendUnicastFrames   : 0          SendBytes            : 0
    SendNoneUnicastFrames: 0         SendFrames           : 0
    SendBroadcastFrames : 0          SendMulticastFrames  : 0
    SendSingleCollision : 0          SendMultiCollision   : 0
    SendLateCollision   : 0          SendExcessCollision  : 0
    SendCollision       : 0          SendDefferTrans      : 0
    OutPause            : 0
```

```
zte(cfg)#
```

4. 清除端口的统计数据

clear port <*portlist*> {**name**|**statistics**|**description**}

可以清除端口的统计数据。执行该命令后，端口的所有统计数据都将被清零。

5. 显示端口的单位时间流量的统计数据

show port statistics

查看端口 2 的 1 分钟内的单位流量统计值。

```
zte(cfg)#set  port 2 unit-statistics enable
zte(cfg)#show port 2 statistics 1min_unit
  PortId: 2    PortName:
(Unit : Packets/sec or Bytes/sec)
   ReceivedFrames       : 0         ReceivedBroadcastFrames: 0
   ReceivedBytes        : 0         ReceivedMulticastFrames: 0
   CrcError             : 0         InPause                : 0
   InMACRcvErr          : 0          Jabber                : 0
   Fragments            : 0         UndersizeFrames        : 0
   Frames64Bytes        : 0         Frames65_127Bytes      : 0
   Frames128_255Bytes   : 0         Frames256_511Bytes     : 0
   Frames512_1023Bytes  : 0         Frames1024_UpBytes     : 0
   OversizeFrames       : 0
   SendUnicastFrames    : 0          SendBytes             : 0
   SendNoneUnicastFrames: 0          SendFrames            : 0
   SendBroadcastFrames  : 0         SendMulticastFrames    : 0
   SendSingleCollision  : 0         SendMultiCollision     : 0
   SendLateCollision    : 0         SendExcessCollision    : 0
   SendCollision        : 0         SendDefferTrans        : 0
   OutPause             :0
zte(cfg)#
```

7.2 端口镜像

7.2.1 概述

端口镜像用于将进入交换机端口（入向镜像端口）的数据包镜像到一个入向目的端口（入向监控端口），或将出交换机端口（出向镜像端口）的数据包镜像到一个出向目的端口（出向监控端口）。

通过端口镜像可以对进入或流出某端口的数据包进行监控，为交换机的维护和监控提供一个有用的工具。

交换机只能设置一个入向监控端口和一个出向监控端口，入向监控端口和出向监控端口可以设置为同一个端口。而入向镜像源端口和出向镜像源端口可以同时设置多个。

说明：

默认情况下，交换机没有镜像端口，入向和出向的监控端口为端口 1。入向镜像端口接收的 **GOOD** 的数据包被镜像到监控端口，对于在入端口直接丢弃的数据包（如 CRC 错误）不进行镜像。

7.2.2 基本配置

端口镜像功能的配置包括以下内容。

1. 添加监控端口

   set mirror add dest-port <*portname*> {**ingress**|**egress**}

2. 删除监控端口

   set mirror delete dest-port <*portname*> {**ingress**|**egress**}

3. 添加镜像源端口

   set mirror add source-port <*portlist*> {**ingress**|**egress**}

4. 删除镜像源端口

   set mirror delete source-port <*portlist*> {**ingress**|**egress**}

5. 显示端口镜像的配置

   show mirror

7.2.3 配置实例

假设要将端口 1 和端口 6 接收到的数据包镜像到监控端口 4 上，具体配置如下：

```
zte(cfg)# set mirror dest-port 4 ingress
zte(cfg)# set mirror add source-port 1,6 ingress
```

使用 **show mirror** 命令可以查看端口镜像的配置信息。

```
zte(cfg)#show mirror
  Ingress mirror information:
    Source port: 1,6
    Destination port: 4
  Egress mirror information:
    Source port: none
    Destination port: none
zte(cfg)#
```

假设要将端口 2 和端口 3 发送的数据包镜像到监控端口 4 上，具体配置如下：

```
zte(cfg)# set mirror dest-port 4 ingress
zte(cfg)# set mirror add source-port 2,3 egress
```

7.3 VLAN 配置

7.3.1 概述

VLAN（Virtual Local Area Network）协议是二层交换设备的一个基本协议，它使管理员能够把一个物理的局域网划分为多个“虚拟局域网”。每个 VLAN 都有一个 VLAN 标识号（VLAN ID），在整个局域网中唯一的标识该 VLAN。多个 VLAN 共享物理局域网的交换设备和链路。

每个 VLAN 在逻辑上就像一个独立的局域网，同一个 VLAN 中的所有帧流量都被限制在该 VLAN 中。跨 VLAN 的访问只能通过三层转发，不能直接访问。这样就提高了这个网络的性能，有效的减少了物理局域网上的整体流量。

VLAN 的具体作用体现在：

1. 减少网络上的广播风暴；
2. 增强网络的安全性；
3. 集中化的管理控制。

ZXR10 5009 支持 tagged-based VLAN，即基于标签的 VLAN。这是 IEEE 802.1Q 定义的方式，是通用的工作方式。这种模式下 VLAN 的划分基于端口的 VLAN 信息（PVID：port VLAN ID）或者 VLAN 标签中的信息。

7.3.2 基本配置

交换机上 VLAN 的配置包括以下内容。

1. 使能/关闭 VLAN

   set vlan <*vlanlist*> {**enable**|**disable**}

2. 在 VLAN 中加入指定的端口

   set vlan <*vlanlist*> **add port** <*portlist*> [**tag**|**untag**]

3. 删除 VLAN 中指定的端口

   set vlan <*vlanlist*> **delete port** <*portlist*>

4. 在 VLAN 中加入指定的 trunk

   set vlan <*vlanlist*> **add trunk** <*trunklist*> [**tag**|**untag**]

5. 删除 VLAN 中指定的 trunk

   set vlan <*vlanlist*> **delete trunk** <*trunklist*>

6. 设置端口的 PVID

   set port <*portlist*> **pvid** <*1-4094*>

7. 设置 trunk 的 PVID

   set trunk < *trunklist* > **pvid** <*1-4094*>

8. 设置 VLAN 的优先级

   set vlan <*vlanlist*> **priority** {**off**|**on** <0-7>}

9. 配置 VLAN 的 FID

   set vlan <*vlanlist*> **fid** <*1-256*>

   相同 FID 的 VLAN 可以共享转发表的条目，大多数厂家不提供 FID 的设置，而是缺省的让 FID=VID。

10. 设置禁止学习端口

    set vlan <*vlanlist*> **forbid port** <*portlist*>

启用 GVRP 协议时，禁止学习的端口不能学习该 VLAN。

11. 允许学习端口

set vlan <*vlanlist*> **permit port** <*portlist*>

启用 GVRP 协议时，允许学习的端口可以学习 VLAN，默认允许学习。

12. 设置禁止学习 trunk

set vlan <*vlanlist*> **forbid trunk** <*trunklist*>

启用 GVRP 协议时，禁止学习的 trunk 不能学习该 VLAN。

13. 允许学习 trunk

set vlan <*vlanlist*> **permit trunk** <*trunklist*>

启用 GVRP 协议时，允许学习的 trunk 可以学习 VLAN，默认允许学习。

14. 创建一个 VLAN 的描述名称

create vlan <*1-4094*> **name** <*name*>

15. 清除 VLAN 的名称

clear vlan <*vlanlist*> **name**

16. 显示 VLAN 的信息

show vlan [<*vlanlist*>]

7.3.3 配置实例

说明：

建议在配置前先删除缺省 VLAN。

1. 配置一个 VLAN

配置 VLAN 100，加入 Untagged 端口 1 和 2，加入 Tagged 端口 7 和 8。具体配置如下。

```
zte(cfg)#set vlan 100 add port 1,2 untag
zte(cfg)#set vlan 100 add port 7,8 tag
zte(cfg)#set port 1,2 pvid 100
zte(cfg)#set vlan 100 enable
```

```
zte(cfg)#show vlan 100
  VlanId  : 100    Fid  : 100    Priority: off   VlanStatus: enabled
  VlanName:
  Tagged ports  : 7-8
  Untagged ports: 1-2

zte(cfg)#
```

2. VLAN 重叠的配置

如 图 7.3-1所示，交换机的端口 6 接服务器，端口 1~3 接客户端，要求端口 1~3 相互隔离，但都能访问服务器。

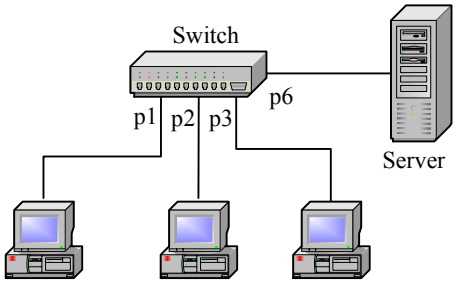


图7.3-1　VLAN 重叠实例

交换机的具体配置如下：

```
zte(cfg)#set vlan 2 add port 1,6 untag
zte(cfg)#set vlan 3 add port 2,6 untag
zte(cfg)#set vlan 4 add port 3,6 untag
zte(cfg)#set vlan 100 add port 1-3,6 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 2 pvid 3
zte(cfg)#set port 3 pvid 4
zte(cfg)#set port 6 pvid 100
zte(cfg)#set vlan 2-4,100 fid 5
zte(cfg)#set vlan 2-4,100 enable
```

3. VLAN 透传的配置

如 图 7.3-2所示，交换机A和交换机B通过端口 6 相连，交换机A的端口 1 与交换机B的端口 2 是VLAN2 的成员，交换机A的端口 3 与交换机B的端口 4 是VLAN3 的成员，相同VLAN的成员之间能够互相通信。

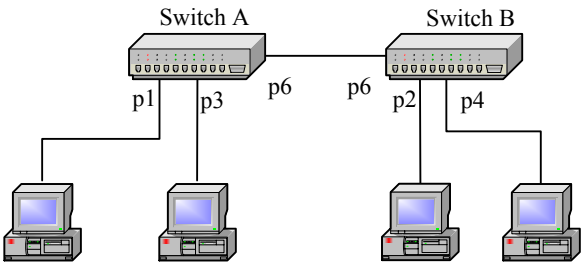


图7.3-2 VLAN 透传实例

交换机 A 的具体配置如下：

```
zte(cfg)#set vlan 2 add port 6 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add port 6 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

交换机 B 的具体配置如下：

```
zte(cfg)#set vlan 2 add port 6 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add port 6 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

7.4 MAC 表操作

7.4.1 概述

对 MAC 表的操作主要包括 MAC 过滤功能、静态地址捆绑功能和 MAC 表老化时间的设置。

- MAC 过滤功能是使交换机在接收到源或目的 MAC 地址为特定 MAC 地址的数据包时执行丢弃操作。
- 静态地址捆绑功能是将特定的 MAC 地址与交换机的端口进行绑定，捆绑后对该 MAC 不再进行动态学习。

- MAC 表老化时间是指动态 MAC 地址在 FDB 表中从最后一次更新到被删除的时间段。

通过设置 MAC 地址过滤和静态地址捆绑，可以有效地控制非法用户侵入网络，防止一些关键的 MAC 地址被冒用，对网络安全起到重要的作用。

7.4.2 基本配置

1. 配置 fdb 的过滤地址

   set fdb filter <*xx.xx.xx.xx.xx.xx*> **fid** <*1-256*>

2. 在地址表中加入静态绑定地址

   set fdb add <*xx.xx.xx.xx.xx.xx*> **fid** <*1-256*> {**port** <*portname*>|**trunk** <*trunkid*>} [**priority** <0-*7*>]

3. 在地址表中删除一条记录

   set fdb delete <*xx.xx.xx.xx.xx.xx*> **fid** <*1-256*>

4. 设置地址老化时间

   set fdb agingtime <*15-3600*>

5. 显示 fdb 地址老化时间

   show fdb agingtime

6. 显示 fdb 的信息

   show fdb [[**static**|**filter**|**dynamic**][**detail**]]

7. 显示基于 MAC 的 fdb 信息

   show fdb mac <*xx.xx.xx.xx.xx.xx*>

8. 显示基于 PORT 的 fdb 信息

   show fdb port <*portname*>

9. 显示基于 VLAN 的 fdb 信息

   show fdb vlan <*vlanname*>

10. 显示基于 TRUNK 的 fdb 信息

    show fdb trunk <*trunkid*>

7.5 LACP 配置

7.5.1 概述

LACP（Link Aggregation Control Protocol）即链路聚合控制协议，是 IEEE 802.3ad 描述的标准协议。

链路聚合（Link Aggregation）是指将具有相同传输介质类型、相同传输速率的物理链路段“捆绑”在一起，在逻辑上看起来好像是一条链路。链路聚合又称中继（Trunking），它允许交换机之间或交换机和服务器之间的对等的物理链路同时成倍地增加带宽。因此，它在增加链路的带宽、创建链路的传输弹性和冗余等方面是一种很重要的技术。

聚合的链路又称干线（Trunk）。如果 Trunk 中的一个端口发生堵塞或故障，那么数据包会被分配到该 Trunk 中的其他端口上进行传输。如果这个端口恢复正常，那么数据包将被重新分配到该 Trunk 中所有正常工作的端口上进行传输。

ZXR10 5009 最多支持 8 个聚合组，每个聚合组参与聚合的端口不超过 8 个。参与聚合的端口应具有相同的传输介质类型、相同的传输速率。

7.5.2 基本配置

在交换机上配置 LACP 包括以下内容。

1. 使能或关闭 LACP 功能

   set lacp {**enable**|**disable**}

   LACP 功能的缺省状态是关闭的。

2. 在聚合组中加入指定端口

   set lacp aggregator <*trunkid*> **add port** <*portlist*>

3. 在聚合组中删除指定端口

   set lacp aggregator <*trunkid*> **delete port** <*portlist*>

   端口处于自动协商模式时允许聚合；否则如果端口处于双工模式则允许聚合，处于半双工模式则不允许聚合。

4. 设置聚合组聚合模式

   set lacp aggregator <*trunkid*> **mode** {**dynamic**|**static | mixed** }

当聚合组配置成动态模式时，则只能与运行 LACP 的设备对接。当配置成静态模式时，如果对端是静态的 Trunk（不运行 LACP 协议），则进行静态聚合；当聚合组配置成混合模式时，如果对端是静态的 Trunk（不运行 LACP 协议），则进行静态聚合；当对端同时存在静态 Trunk 和 LACP 时，优先考虑 LACP 聚合。

5. 配置参与聚合的端口的超时情况

set lacp port <*portlist*> **timeout** {**long**|**short**}

超时情况是指处于聚合状态的端口没有收到对端的 LACP 协议包时，经过多长时间退出聚合，短超时是 3 秒，长超时是 90 秒。

6. 设置端口参与聚合的模式

set lacp port <*portlist*> **mode** {**active**|**passive**}

端口参与聚合的模式是指在聚合组非静态模式下，聚合组内端口以主动或被动方式发送 LACP 协议包来更新状态信息的方式。当本端端口配置为主动协商模式时，对端端口可配置为主动或被动协商模式；当本端端口配置为被动协商模式时，对端端口只能配置为主动协商模式，否则不能成功参与聚合（运行 LACP 协议时）。

7. 设置 LACP 的优先级

set lacp priority <*1-65535*>

8. 显示 LACP 的配置信息

show lacp

9. 显示 LACP 聚合组聚合信息

show lacp aggregator [<*trunkid*>]

10. 显示 LACP 参与聚合的端口信息

show lacp port [<*portlist* >]

配置聚合组后，可以对它进行各种设置，如设置 PVID、加入 VLAN、静态绑定 MAC 地址等。

7.5.3 配置实例

如 图 7.5-1所示，交换机A和交换机B通过聚合端口相连（将端口 5 和 6 捆绑而成），交换机A的端口 1 与交换机B的端口 2 属于VLAN2，交换机A的端口 3 与交换机B的端口 4 属于VLAN3，相同VLAN的成员之间能够互相通信。

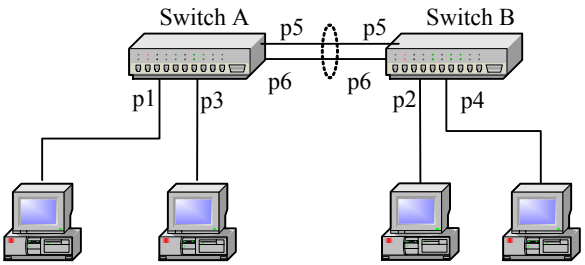


图7.5-1 LACP 配置实例

交换机 A 的具体配置如下：

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 5-6
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

交换机 B 的具体配置如下：

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 5-6
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

7.6 IGMP Snooping 配置

7.6.1 概述

由于组播地址不可能出现在报文的源地址中，所以交换机无法学习到组播地址。当交换机收到组播信息时，会向同一个 VLAN 中的所有端口广播。如果不采取措施，就会出现不想要的组播信息扩散到网络中每一点的严重问题，浪费网络带宽资源。

IGMP Snooping 通过对主机和路由器之间的 IGMP 协议通信的“监听”，使组播包只发送给在组播转发表中的端口，而不是所有端口，从而限制了局域网交换机上的组播信息扩散，减少了不必要的网络带宽的浪费，提高了交换机的利用率。

基于源或目的地址的组播过滤，能够按照用户在监听 VLAN 添加的过滤条目对主机向路由器发送的 IGMP 协议报文进行过滤处理，增强交换机对组播监听的控制。

7.6.2 基本配置

在交换机上配置 IGMP Snooping 包括以下内容。

1. 使能或关闭 IGMP Snooping 功能

   set igmp snooping {**enable**|**disable**}

   IGMP Snooping 功能的缺省状态是关闭的。

   当 IGMP Snooping 功能关闭时，对于组播流根据 **set port multicast** 命令的配置进行处理，如果选择参数 **forward** 则对相应端口进行转发，如果选择 **discard** 则对相应端口丢弃。

   使能 IGMP Snooping 功能后，对于组播流首先根据监听到的组播转发表来转发，如果没有查找到该组播转发表，则按照上述的配置针对端口决定转发或丢弃。

说明：

当 IGMP Snooping 关闭时，对于非路由端口，最好关闭端口的组播转发功能；而对于路由端口，最好开启端口的组播转发功能。

2. 添加对指定 VLAN 的 IGMP Snooping 功能

   set igmp snooping add vlan <*vlanlist*>

3. 删除对指定 VLAN 的 IGMP Snooping 功能

set igmp snooping delete vlan <*vlanlist*>

只有添加对指定的 VLAN 进行组播监听的功能，才能监听到相应的组播转发表。本交换机最多支持同时监听 256 个 VLAN。

4. 使能或关闭对指定 VLAN 的 IGMP Query 功能

set igmp snooping query vlan <*vlanlist*> {**enable**|**disable**}

使能了 IGMP Snooping 功能后，如果没有 IGMP Query 路由器存在，则无法完成正常的 IGMP Snooping 的功能，这时可以开启交换机的 IGMP Query 的功能。

如果所监听的 VLAN 存在 IGMP Query 路由器，最好关闭本交换机的 IGMP Query 功能。交换机运行的 IGMP Query 版本是 V2.0，遵循 V2.0 IGMP Query 路由器选举功能。当配置了三层端口的 IP 和 MAC 地址，则 IGMP Query 的源 IP 和源 MAC 使用三层配置；否则使用 223.255.255.255 和交换机的 MAC 地址作为 IGMP Query 的源。

5. 添加基于 VLAN 的静态组播组

set igmp snooping vlan <*vlanname*> **add group** <*A.B.C.D*>

6. 删除基于 VLAN 的静态组播组

set igmp snooping vlan <*vlanname*> **delete group** <*A.B.C.D*>

说明：

当已添加了基于此 VLAN 和某些端口的静态组播组后，则不再允许添加仅基于此 VLAN 的静态组播组；同时，当删除基于 VLAN 的静态组播组时，则已添加了基于此 VLAN 和某些端口的静态组播组也被同时清除。

7. 添加基于 VLAN+端口或 VLAN+聚合口的静态组播组

set igmp snooping vlan <*1-4094*> **add group** <*A.B.C.D*> port <*portlist*>

或 **set igmp snooping vlan** <*1-4094*> **add group** <*A.B.C.D*> trunk <*trunklist*>

8. 删除基于 VLAN+端口或 VLAN+聚合口的静态组播组

set igmp snooping vlan <*1-4094*> **delete group** <*A.B.C.D*> port <*portlist*>

或 **set igmp snooping vlan** *<1-4094>* **delete group** *<A.B.C.D>* trunk *<trunklist>*

当运行了 IGMP Snooping 的功能，允许以本交换机的名义注册基于 VLAN 或基于 VLAN+端口的静态组播组，本交换机支持最多对 64 个静态组播组的注册。

说明：

注册的静态组播组只能是用户组播地址 224.x.x.x~239.x.x.x，不能是保留的组播地址。224.0.0.x 的组播地址不允许注册。

注册的静态组播组所在 VLAN 必须是已被监听的 VLAN。

9. 添加静态路由端口或聚合口

set igmp snooping vlan *<1-4094>* **add smr port** *<portlist>*

或 **set igmp snooping vlan** *<1-4094>* **add smr trunk** <trunk*list*>

10. 删除静态路由端口或聚合口

set igmp snooping vlan *<1-4094>* **delete smr port** *<portlist>*

或 **set igmp snooping vlan** *<1-4094>* **delete smr trunk** <trunk*list*>

当为某个监听 VLAN 添加了静态路由端口或聚合口后，能够将此端口或聚合口添加到此监听 VLAN 对应的所有组播组中，并且组播组中成员端口的加入、离开等报文将同时向路由端口和此静态路由端口转发；

11. 设置基于 VLAN 的组播组数目限制

set igmp snooping add maxnum *<1-256>* **vlan** *<vlanlist>*

12. 清除基于 VLAN 的组播组数目限制

set igmp snooping delete maxnum vlan *<vlanlist>*

说明：

缺省状态下，每个被监听的 VLAN 所能建立的组播组数目为 256，当设置了此 VLAN 的组播组数目后，此 VLAN 上所能建立的组播组条目不会大于此 VLAN 限制的组播组数目。

13. 设置组播成员/路由超时

set igmp snooping timeout *<100-2147483647>* {**host**|**router**}

14. 设置查询周期

set igmp snooping query_interval *<10-2147483647>*

15. 设置查询响应周期

set igmp snooping response_interval *<10-250>*

16. 设置最后的成员查询周期

set igmp snooping lastmember_query *<10-250>*

17. 使能或关闭 IGMP 的快速离开功能

set igmp snooping fastleave {**enable**|**disable**}

运行了 IGMP Snooping 功能，并正确地监听到了主机加入的端口后，当该端口收到 IGMP 离开报文时，如果关闭了 IGMP 的快速离开功能，则交换机将向该端口发送两次特定组查询，以确认是否在组播转发表中删除该端口；如果使能了 IGMP 的快速离开功能，则不进行特定组查询，直接从组播转发表中删除该端口。

当跨 VLAN 的组播监听从使能状态变为关闭状态时，经过跨 VLAN 组播监听的某些监听结果要经过相应的超时时长才能正确删除掉。

18. 使能或关闭跨 VLAN 的 IGMP Snooping 功能

set igmp snooping crossvlan {**enable**|**disable**}

当运行了 IGMP Snooping 功能，并利用 PVID（default vlan_id）正确地配置一对多的端口转发形式后，可以利用本交换机跨 VLAN 的 IGMP Snooping 功能对不同 VLAN 之间的 IGMP 信息进行监听并进行跨 VLAN 的组播转发。

19. 使能或关闭组播过滤功能

set igmp filter {**enable**|**disable**}

组播过滤功能的缺省状态是关闭的。

当使能组播过滤功能后，对于组播加入请求的处理，将按照添加的组播过滤条目对其进行过滤后再进行处理；如果组播过滤功能关闭，对于端口的加入请求，将不作任何基于源地址或组地址的过滤操作。

20. 添加基于 VLAN 的组播组地址过滤

set igmp filter add groupip <*A.B.C.D*> vlan <*vlanlist*>

在组播过滤使能后，设置了基于 VLAN 的组播组地址过滤条目后，此 VLAN 内的端口如果收到组地址为此过滤地址的组播加入请求时，本端交换机不对此端口的加入请求进行处理。

21. 删除基于 VLAN 的组播组地址过滤

set igmp filter delete groupip <*A.B.C.D*> vlan <*vlanlist*>

22. 添加基于 VLAN 的组播源地址过滤

set igmp filter add sourceip <*A.B.C.D*> vlan <*vlanlist*>

在组播过滤使能后，设置了基于 VLAN 的组播源地址过滤条目后，此 VLAN 内的端口如果收到源地址为此过滤地址的组播加入请求时，本端交换机不对此端口的加入请求进行处理。

23. 删除基于 VLAN 的组播源地址过滤

set igmp filter delete sourceip <*A.B.C.D*> vlan <*vlanlist*>

24. 显示组播监听的配置

show igmp snooping

25. 显示组播监听结果

show igmp snooping vlan [<*vlanname*> [**host**|**router**]]

26. 显示组播过滤状态

show igmp filter

27. 显示某监听 VLAN 的组播地址过滤条目

show igmp filter vlan <*1-4094*>

7.6.3 配置实例

实例一：

如 图 7.6-1所示，端口 1、3、5 接主机，端口 8 接路由器，实现一对多通讯方式，即端口 8 可以和 1、3、5 通讯，而 1、3、5 相互之间不能通讯。在交换机上开启 IGMP Snooping功能并显示监听结果。

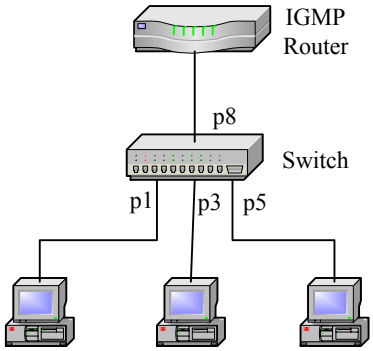


图7.6-1 一对多通信方式的网络拓扑结构示意图

具体配置如下：

```
zte(cfg)#set vlan 200 add port 1,3,5,8 untag
zte(cfg)#set vlan 210 add port 1,8 untag
zte(cfg)#set vlan 230 add port 3,8 untag
zte(cfg)#set vlan 250 add port 5,8 untag
zte(cfg)#set port 8 pvid 200
zte(cfg)#set port 1 pvid 210
zte(cfg)#set port 3 pvid 230
zte(cfg)#set port 5 pvid 250
zte(cfg)#set vlan 200,210,230,250 fid 200
zte(cfg)#set vlan 200,210,230,250 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200,210,230,250
zte(cfg)#set igmp snooping crossvlan disable
```

显示组播监听结果：

```
zte(cfg)#show igmp snooping vlan

Num  VlanId  Group           Last_Report     PortMember
1    210     224.1.1.1       192.168.1.1     1
2    230     224.1.1.1       192.168.1.2     3
3    250     224.1.1.1       192.168.1.3     5
```

在交换机上开启跨 VLAN 组播监听，经过组播监听的显示结果：

```
zte(cfg)#set igmp snooping crossvlan enable
zte(cfg)#show igmp snooping vlan
Num  VlanId  Group           Last_Report     PortMember
1    210     224.1.1.1       192.168.1.1     1
```

```
2    230     224.1.1.1        192.168.1.2     3
3    250     224.1.1.1        192.168.1.3     5
4    200     224.1.1.1        192.168.1.3     1,3,5,8
```

实例二：

如上 图 7.6-1所示，端口 1，3，5 接主机，端口 8 接路由器，将端口 8，1，3，5 加入到vlan 200，端口 1、3，5 上的用户分别发送组地址为 230.44.45.167、230.44.45.157 组播加入请求，在vlan200 上添加组播过滤组地址 230.44.45.167。在交换机上开启IGMP Snooping和IGMP Filter功能并显示监听结果。

具体配置如下：

```
zte(cfg)#set vlan 200 add port 1,3,5,8 untag
zte(cfg)#set port 1,3,5,8 pvid 200
zte(cfg)#set vlan 200 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200
zte(cfg)#set igmp filter enable
zte(cfg)#set igmp filter groupip 230.44.45.167 vlan 200
```

显示组播监听及过滤结果：

```
zte(cfg)#show igmp snooping vlan
  Num  VlanId  Group            Last_Report     PortMember
  1    200     230.44.45.157    192.168.1.1     1,3,5,8

zte(cfg)#sho igmp filter
  IGMP Filter: enabled
  Index FilterIpAddress   Vlan          Port           Type
  ----- ---------------- -------------- -------------- ---------
  1     230.44.45.167    200             ------         Groupip

zte(cfg)#show igmp filter vlan 200
  Maximal group number: 256
  Current group number: 0
  The filter address list of this vlan:
  Index FilterIpAddress  Vlan   Type
  ----- ---------------- -----  ------
  1     230.44.45.167    200    Groupip
```

7.7 IPTV 配置

7.7.1 概述

IPTV 又称交互式网络电视，是由运营商基于宽带基础推出的，利用 IP 宽带网络，集互联网、多媒体、通信等多种技术于一体，向用户提供直播电视、视频点播、上网浏览等多种交互式服务的业务，用户可以通过 PC 或“IP 机顶盒＋电视”的方式使用的业务。

7.7.2 基本配置

交换机上 IPTV 的配置包括以下内容。

1. IPTV 全局参数配置：

- 设置用户的最小观看时间

  iptv control login-time

- 设置全局最大预览次数

  iptv control prvcount count

- 设置全局最小预览间隔

  iptv control prvinterval

- 设置全局最大预览时间

  iptv control prvtime

- 设置全局复位预览次数的周期

  iptv control prvcount reset-period

- IPTV 使能功能

  iptv control {**enable**|**disable**}

2. IPTV 频道配置

- 创建 IPTV 的频道

  create iptv channel

- 设置频道名

  iptv channel name

- 设置频道所属组播 vlan

  iptv channel mvlan

- 删除频道

  clear iptv channel

3. CAC（频道访问控制）配置

- 创建 CAC 规则

  create iptv cac-rule

- 设置规则名

  iptv cac-rule name

- 设置规则的最大预览次数，缺省为全局最大预览次数

  iptv cac-rule prvcount

- 设置规则的最大预览时间，缺省为全局最大预览时间

  iptv cac-rule prvtime

- 设置规则的最小预览间隔，缺省为全局最小预览间隔

  iptv cac-rule prvinterval

- 设置规则对频道的权限

  iptv cac-rule right

- 删除规则

  clear iptv cac-rule

4. IPTV 用户的管理命令

   删除在线的 IPTV 用户

   clear iptv client

7.7.3 配置实例

1. 如果端口 gei_1/1 下的用户是组播组 224.1.1.1 的定购用户，组播组所在的 vlan 为 100，配置如下

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
```

```
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right order 1
```

2. 如果端口 gei_1/1,vlan1 下的用户是组播组 224.1.1.1 的预览用户，最大预览时间为 2 分钟，最小预览间隔为 20 秒，最大预览次数为 10，组播组所在的 vlan 为 100，配置如下

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# iptv channel 1 name cctv1
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1 vlan 1
ZXR10(config-nas)# iptv cac-rule 1 prvcount 10
ZXR10(config-nas)# iptv cac-rule 1 prvtime 120
ZXR10(config-nas)# iptv cac-rule 1 prvinterval 20
ZXR10(config-nas)# iptv cac-rule 1 right preview 1
```

3. 如果端口 gei_1/1 下的用户可以看 vlan100 中所有组播组，配置如下

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)# create iptv channel general 256
ZXR10(config-nas)# iptv channel 256 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right order 256
```

4. 如果端口 gei_1/1 只允许接受组播组 224.1.1.1 的查询报文，组播组所在的 vlan 为 100，配置如下

```
ZXR10(config-nas)# iptv control enable
ZXR10(config-nas)#  create iptv channel special 1 address 224.1.1.1
ZXR10(config-nas)# iptv channel 1 mvlan 100
ZXR10(config-nas)# create iptv cac-rule 1 port gei_1/1
ZXR10(config-nas)# iptv cac-rule 1 right query 1
```

7.7.4 IPTV 的维护和诊断

当 IPTV 遇到问题时，我们可以通过相关的调试命令来帮助定位故障，排除错误，其中用到的命令主要是与其相关的 **show** 命令。

1. 显示 IPTV 的全局配置信息

   show iptv control

2. 显示 IPTV 频道信息

show iptv channel

3. 显示特定频道号的频道统计信息

show iptv channel statistics

4. 显示 CAC 规则

show iptv cac-rule

5. 显示 CAC 规则统计

show iptv cac-rule statistics

6. 显示在线的 IPTV 用户

show iptv client

7. 显示在线的 IPTV 用户统计

Show iptv client statistics

7.8 MSTP 配置

7.8.1 概述

STP（生成树协议）应用于有环路的网络，通过一定的算法得到一条通路，并阻断冗余路径，将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。当这条通路正常工作时，其余路径是关闭的；当这条通路出现故障时，将重新进行计算得到一条新的通路。

RSTP（快速生成树协议）在普通 STP 协议的基础上增加了端口可以快速由 Blocking 状态转变为 Forwarding 状态的机制，加快了拓扑的收敛速度。

MSTP（多生成树协议）是在快速和普通生成树协议基础上，增加对带有VLAN ID的帧转发的处理。整个网络拓扑结构可以规划为总生成树CIST，分为CST（主干生成树）和IST（区域生成树），如 图 7.8-1所示。

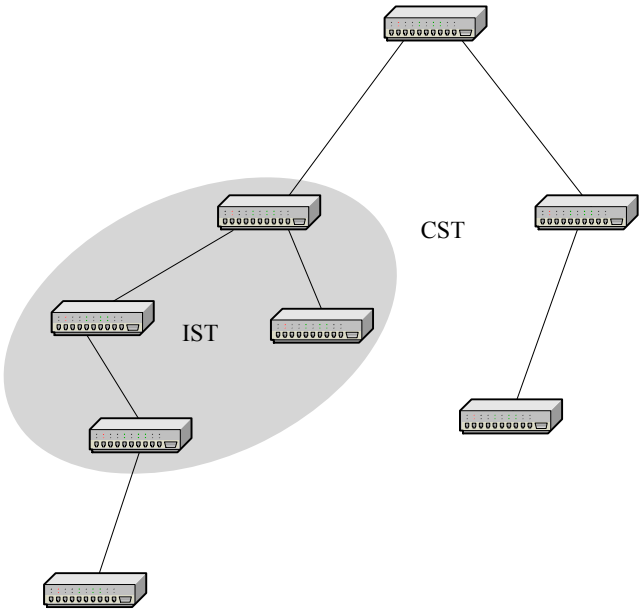


图7.8-1 多生成树的拓扑结构

在整个多生成树的拓扑结构中，可以把一个 IST 看作一个单个的网桥（交换机），这样就可以把 CST 作为一个 RSTP 生成树来进行配置信息（BPDU）的交互。在一个 IST 区域内可以创建多个实例，这些实例只在本区域内有效。可以把每一个实例等同于一个 RSTP 生成树，不同的是还要与区域外的网桥进行 BPDU 的交互。

用户在创建某个实例时，必须将一个或多个 VLAN ID 划入此实例中。IST 区域内的网桥上属于这些 VLAN 的端口通过 BPDU 的交互，最终构成一个生成树结构（每个实例对应一个生成树结构）。

这样，该区域内的网桥在转发带有这些 VLAN ID 的数据帧时，将根据对应实例的生成树结构进行转发。对于要转发到该区域外的数据帧，无论它带有何种 VLAN ID，均按照 CST 的 RSTP 生成树结构进行转发。

与 RSTP 相比，MSTP 的优点在于：在某个 IST 区域中，可以按照用户设定的生成树结构对带有某个 VLAN ID 的数据帧进行转发，并保证不会造成环路。

7.8.2 基本配置

默认配置中，MSTP 只有实例为 0 的实例，并且此实例永远存在，用户无法通过手工删除。此实例映射的 VLAN 为 1~4094。

1. 使能/关闭 STP

set stp {**enable**|**disable**}

2. 设置 STP 的强制类型

set stp forceversion {**mstp**|**rstp**|**stp**}

3. 设置 VLAN 和 instance 的映射关系

set stp instance <*0-15*>[**add**|**delete**] **vlan** <*vlanlist*>

该命令新建一个实例，并设置 VLAN 与该实例的映射关系。这些 VLAN 将自动从 instance 0 的 VLAN 映射表中删除，加入新建实例的 VLAN 映射表中。

4. 设置网桥优先级

set stp instance <*0-15*> **bridgeprio** <*0-61440*>

5. 设置实例端口优先级

set stp instance <*0-15*> **port** <*portname*> **priority** <*0-255*>

6. 设置实例 trunk 的优先级

set stp instance <*0-15*> **trunk** <*trunkid*> **priority** <*0-255*>

7. 设置实例端口费用

set stp instance <*0-15*> **port** <*portname*> **cost** <*1-200000000*>

8. 使能/关闭实例端口 root 保护

set stp instance <*0-15*> **port** <*portname*> **root-guard {enable|disable}**

9. 使能/关闭实例端口 loop 保护

set stp instance <*0-15*> **port** <*portname*>**loop-guard{enable|disable}**

10. 设置实例 trunk 费用

set stp instance <*0-15*> **trunk** <*trunkname*> **cost** <*1-200000000*>

11. 使能/关闭实例 trunk root 保护

set stp instance <*0-15*> **trunk** <*trunkname*> **root-guard {enable|disable}**

12. 使能/关闭实例 trunk loop 保护

set stp instance <*0-15*> **trunk** <*trunkname*>**loop-guard{enable|disable}**

13. 使能/关闭端口 stp 功能

set stp port <*portlist*>**{enable|disable}**

14. 使能/关闭 trunk 的 stp 功能

set stp trunk <*trunklist*>**{enable|disable}**

15. 使能/关闭端口 bpdu 保护

set stp port <*portlist*> **bpdu-guard{enable|disable}**

16. 设置端口 stp 类型检查

set stp port <*portlist*> **pcheck**

17. 设置 BPDU 保护端口 linkdown 的时间间隔

set stp bpdu_interval *〈10-65535〉*

18. 设置实例端口的 Linktype 类型

set stp port <*portlist*> **linktype {point-point|shared}**

19. 设置实例 trunk 的 Linktype 类型

set stp trunk < *trunklist* > **linktype** {**point-point**|**shared**}

20. 设置实例端口的包类型

set stp port <*portlist*> **packettype** {**IEEE|CISCO|HUAWEI|HAMMER|extend**}

21. 设置实例 trunk 的包类型

set stp trunk < *trunklist* > **packettype** {**IEEE|CISCO|HUAWEI|HAMMER|extend**}

22. 设置 MSTP 的时间参数

- 设置 STP 的通告间隔时间

set stp hellotime <*1-10*>

- 设置 STP 的转发延迟时间

set stp forwarddelay <*4-30*>

- 设置 STP 的老化时间

set stp agemax <*6-40*>

23. 设置 MST 的任意两终端间的最大跳数

set stp hopmax <*1-40*>

24. 设置 MST 的区域名称

set stp name <*name*>

25. 设置 MST 的版本号

set stp revision <*0-65535*>

同一区域内 MST 的版本号必须相同。

26. 使能/关闭 STP Relay

set stp relay {**enable**|**disable**}

27. 设置边缘端口

set stp edge-port {**add**|**delete**} **port** <*portlist*>

28. 设置 stp 的 hmd5 摘要

set stp hmd5-digest {CISCO|HUAWEI}*<0,0x00..0-0xff..f>*

29. 设置 stp 的 hmd5 关键字

set stp hmd5-key {CISCO|HUAWEI}*<0,0x00..0-0xff..f>*

30. 查看 STP 的相关信息

- 显示 STP 的信息

  show stp

- 显示 STP 实例的信息

  show stp instance [<*0-15*>]

- 显示 STP 端口的信息

  show stp port [<*portlist*>]

- 显示 STP trunk 的信息

  show stp trunk <*trunklist*>

- 显示 STP relay 的信息

  show stp relay

7.8.3 配置实例

下面的例子介绍了 MSTP 的具体配置。

1. 新建 instance 1，与 VLAN 10-20 建立映射，并设置名称为 zte，MST 版本号为 10。

```
zte(cfg)#set stp instance 1 add vlan 10-20
zte(cfg)#set stp name zte
zte(cfg)#set stp revision 10
  The spanning_tree protocol is enabled!

  The STP ForceVersion is MSTP !
  Revision: 10    Name: zte
  Bpdu interval: 100
  Cisco key:    0x13ac06a62e47fd51f95d2ba243cd0346
  Cisco digest:  0x00000000000000000000000000000000
  Huawei key:   0x13ac06a62e47fd51f95d2ba243cd0346
  Huawei digest: 0x00000000000000000000000000000000
  Instance VlanMap
  -------- -------------------
  0       1-9,21-4094
  1       10-20
zte(cfg)#
```

2. 设置实例的网桥优先级和实例端口的优先级。

```
zte(cfg)#set vlan 10 add port 2 untag
zte(cfg)#set stp instance 1 bridgeprio 7
zte(cfg)#set stp instance 1 port 2 priority 112

zte(cfg)#show stp instance 0
  RootID:
  Priority      : 32768      Address    : 00.d0.d0.ff.ff.0a
  HelloTime(s)   : 2         MaxAge(s)   : 20
  ForwardDelay(s): 15

  Reg  RootID:
  Priority      : 32768      Address    : 00.d0.d0.ff.ff.0a
  RemainHops    : 20

  BridgeID:
  Priority      : 32768      Address    : 00.d0.d0.ff.ff.0a
  HelloTime(s)   : 2         MaxAge(s)   : 20
  ForwardDelay(s): 15         MaxHops    : 20

  Interface PortId Cost     Status  Role      Bound GuardStatus
```

```
 --------- ------ --------- ------- ---------- ----- -----------
 2       128.2  200000   Forward Designated RSTP  None
zte(cfg)#show stp instance 1
 RootID:
 Priority      : 1         Address    : 00.d0.d0.ff.ff.0a
 HelloTime(s)  : 2         MaxAge(s)  : 20
 ForwardDelay(s): 15       RemainHops : 20
 BridgeID:
 Priority      : 1         Address    : 00.d0.d0.ff.ff.0a
 HelloTime(s)  : 2         MaxAge(s)  : 20
 ForwardDelay(s): 15       MaxHops    : 20

 Interface PortId Cost     Status  Role      GuardStatus
 --------- ------ --------- ------- ---------- -----------
 2       112.2  200000   Discard Designated None

zte(cfg)#show stp port 2
The following ports are active!
 PortId     : 2           MSTI       : 00
   Priority   : 128         Cost       : 200000
   Status     : Forward     Role       : Designated
   EdgePort   : Disabled    GuardType  : None
   LinkType   : P2P         PacketType : IEEE

 PortId     : 2           MSTI       : 01
   Priority   : 112         Cost       : 200000
   Status     : Forward     Role       : Designated
   EdgePort   : Disabled    GuardType  : None
   LinkType   : P2P         PacketType : IEEE
```

7.9 QoS 配置

7.9.1 概述

交换机提供一定的 QoS 功能，提供优先级控制功能，可以基于数据包的源 MAC 地址优先级、VLAN 优先级、802.1P 用户优先级、三层 DSCP 优先级或端口默认优先级来决定数据包的优先级。一个数据包优先级决定顺序为（前面的优先）：

1. CPU 发送的数据包优先级（由 CPU 决定）；

2. MGMT 数据包（管理数据包，如 BPDU 包）优先级（初始化决定管理包的优先级）；
3. 静态源 MAC 地址优先级；
4. VALN 优先级；
5. 802.1P 用户优先级；
6. 三层 DSCP 优先级；
7. 端口默认优先级。

当前面的优先级决定机制决定数据包的优先级后，后面的优先级决定策略被忽略。如果要使用端口的默认优先级决定端口接收的数据包的优先级时，需满足以下的所有条件：

- 数据包必须不是 CPU 发送的数据包和管理包。
- 数据包的源 mac 地址不是静态地址或端口源地址优先级没有使能。
- 数据包所在 VLAN 的优先级没有使能或端口的 VLAN 优先级没有使能。
- 端口的 802.1P 用户优先级没有使能或数据包不是 TAG 数据包。
- 端口的 DSCP 优先级没有使能。

为交换机配置优先级控制策略后，当交换机接收到相应的数据帧，高优先级的数据帧可以优先传输，从而保证关键应用。

说明：

默认情况下，端口上 802.1P 用户优先级功能是使能的，其他的优先级决定策略是关闭的，用户可以根据实际需要，基于端口开启或关闭任意优先级决定策略。

在同时使能端口的 802.1P 用户优先级和三层 DSCP 优先级，且端口接收的数据包有 802.1P 用户优先级的 IP 数据包时，交换机使用数据包的 802.1P 用户优先级决定数据包优先级。

7.9.2 基本配置

交换机上 QoS 的设置包括以下内容：

1. 设置队列调度模式

set qos queue-schedule {**sp**|**wfq**}

当设置队列调度方式为 wfq 时，四个出口队列的权重分别如下：

优先级队列	权重
0	1
1	2
2	4
3	8

2. 设置 802.1P 用户优先级到队列优先级映射

set qos priority-map user-priority <0-*7*> **traffic-class** <0-*3*>

默认情况下，802.1P 用户优先级到队列优先级对应关系为：

（0，3）→1；（1，2）→0；（4，5）→2；（6，7）→3

此对应关系在端口使用 802.1P 用户优先级或默认优先级决定数据包优先级时来决定数据包所上的队列。

3. 设置 IP DSCP 优先级到队列优先级映射

set qos priority-map ip-priority <0-*63*> **traffic-class** <0-*3*>

默认情况下，802.1P 用户优先级到队列优先级对应关系为：

（0~15）→0；（16~31）→1；（32~47）→2；（48~63）→3

此对应表在端口有三层 DSCP 优先级决定数据包优先级时来决定数据包所上的队列。

4. 显示队列调度配置

show qos queue-schedule

5. 显示 qos 的 802.1P 用户优先级到队列优先级映射/三层 DSCP 优先级到队列优先级映射

show qos priorty-map {**user-priority**|**ip-priority**}

7.9.3 配置实例

配置 QoS 模式为 sp，具体配置如下：

```
zte(cfg)#set qos queue-schedule sp
zte(cfg)#show qos queue-schedule
  Queue-schedule mode is SP(Strict Priority).
```

```
zte(cfg)#
```

配置交换机 802.1P 用户优先级到队列优先级映射为（0~6）→0，7→2。此时如果端口上 UserPriority 时 enable 的，并且端口上接收的数据包是 TAG 的数据包，TAG 中的优先级为 0~6 时，数据包在出口时上队列 0；TAG 中的优先级为 7 时，数据包在出口时上队列 2。具体配置如下：

```
zte(cfg)# set qos priority-map user-priority 0 traffic-class 0
zte(cfg)# set qos priority-map user-priority 1 traffic-class 0
zte(cfg)# set qos priority-map user-priority 2 traffic-class 0
zte(cfg)# set qos priority-map user-priority 3 traffic-class 0
zte(cfg)# set qos priority-map user-priority 4 traffic-class 0
zte(cfg)# set qos priority-map user-priority 5 traffic-class 0
zte(cfg)# set qos priority-map user-priority 6 traffic-class 0
zte(cfg)# set qos priority-map user-priority 7 traffic-class 2
zte(cfg)#show qos priority-map  user-priority
 Map of user priority to traffic class:
   COS(802.1p user priority), TC(Traffic-Class)
   COS 0   1   2   3   4   5   6   7
   TC  0   0   0   0   0   0   0   2
```

配置交换机 IPDSCP 优先级到队列优先级映射为（0~31）→1，（32，33）→3，其它的使用默认值。此时如果端口上 IpPriority 时 enable 的，并且端口上接收的数据包是 IP，DSCP 优先级为 0~31 时，数据包在出口时上队列 1；T DSCP 优先级为 32 或 33 时，数据包在出口时上队列 3。具体配置如下：

```
zte(cfg)# set qos priority-map ip-priority 0-31 traffic-class 1
zte(cfg)# set qos priority-map ip-priority 32,33 traffic-class 2
zte(cfg)#show qos priority-map ip-priority
 Map of ip dscp priority to traffic class:
   DSCP(ip dscp priority), TC(Traffic-Class)
   DSCP 0   1   2   3   4   5   6   7   8   9   10  11  12  13  14  15
   TC   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1

   DSCP 16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31
   TC   1    1   1   1   1   1    1   1   1   1    1   1   1   1   1   1

   DSCP 32  33  34  35  36  37  38  39  40  41  42  43  44  45  46  47
   TC   3   3   2   2   2   2   2   2   2   2   2   2   2   2   2   2

   DSCP 48  49  50  51  52  53  54  55  56  57  58  59  60  61  62  63
   TC   3   3   3   3   3   3   3   3   3   3   3   3   3   3   3   3
```

7.10 PVLAN 配置

7.10.1 概述

PVLAN（Private VLAN）是一个基于端口的 VLAN。PVLAN 是由若干个共享端口和若干个隔离端口组成，隔离端口之间不能相互访问，但隔离端口和共享端口之间可以互相访问。目前一个交换机设备中之支持一个 PVLAN。

PVLAN 的具体应用如只允许用户访问服务器，不允许用户之间的直接互访。因此 PVLAN 的设置只会在一个完整的 PVLAN（既有共享端口又有隔离端口）中生效，如果只配置了共享端口，或者只配置了隔离端口，PVLAN 的设置将失效。

在 ZXR10 5009 上，共享端口的设置是有约束的。所有共享端口必须在同一个组内。

5009 只存在一个组，即所有端口在一组之内。

7.10.2 基本配置

交换机上 PVLAN 的配置包括以下内容。

1. 在 PVLAN 中增加/删除隔离端口/共享端口

   set pvlan session <*id*> {**add**|**delete**} {**isolated-port** <*portlist*> | **promiscuous** {**port**<*portname*>|**trunk**<*trunkid*>}}

2. 显示 PVLAN 配置

   show pvlan

7.10.3 配置实例

如 图 7.10-1所示，配置PVLAN 加入共享端口 6，加入隔离端口 1、2、3。

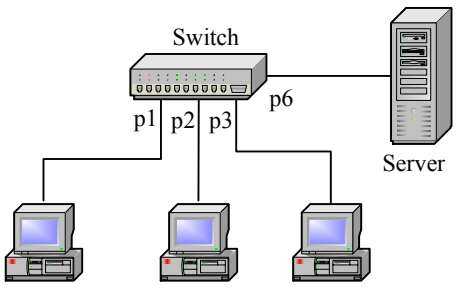


图7.10-1 PVLAN 配置实例

具体配置如下。

```
zte(cfg)#set pvlan session 1 add promiscuous port 6
zte(cfg)#set pvlan session 1 add isolated-port 1-3
zte(cfg)#show pvlan
  pvlan session  : 1
  promiscuous-port: 6
  isolated-port   : 1-3
```

7.11 802.1x 透传配置

IEEE 802.1x 是基于端口的访问控制协议（Port-Based Network Access Control）。基于端口的访问控制是对连接到局域网（LAN）设备的用户进行认证和授权的一种手段。这种认证在局域网环境中提供了一种点对点的识别用户的方式。

ZXR10 5009 提供 802.1x 透传功能，它能将客户端的 802.1x 协议包透传到认证服务器进行认证。

802.1x 透传的配置主要包括以下内容。

1. 开启/关闭 802.1x 透传功能

   set 802.1xrelay {**enable**|**disable**}

2. 显示 802.1x 透传配置

   show 802.1xrelay

7.12 三层配置

7.12.1 概述

ZXR10 5009 提供少量的三层功能，主要供用户远程配置和管理使用。为了实现用户的远程登录，需要在交换机上配置 IP 端口，当远程配置主机与交换机上的 IP 端口不在同一个网段时，还需要进行静态路由的配置。

静态路由是一种简单的单播路由协议，由用户指定到达某一目的网段的“下一跳”地址，其中“下一跳”也称为网关。静态路由的内容主要包括目的地址、目的地址掩码、下一跳地址、出接口。目的地址和目的地址掩码描述目的网络信息，下一跳地址和出接口描述本交换机转发此目的报文的方法。

ZXR10 5009 允许增加和删除静态 ARP 表项。ARP 表主要记录同一网络中各节点 IP 地址和 MAC 地址的对应关系。发送 IP 包时，交换机会先查看目的 IP 地址是

否属于同一网段，如果是，则检查 ARP 表中有没有对方 IP 地址和 MAC 地址对应关系的条目：

1. 如果有就直接将 IP 包发送到该 MAC 地址；
2. 如果 ARP 表中找不到对方 IP 地址对应的 MAC 地址，则会向网络发出一个 ARP Request 广播包，查询对方的 MAC 地址。

一般情况下交换机上的 ARP 表项都是动态的，只有在连接的主机不能响应 ARP Request 的情况下，需要在交换机上设置静态的 ARP 表项。

配置三层功能首先必须使用 **config router** 命令进入三层配置模式。

7.12.2 IP 端口配置

在交换机上配置 IP 端口包括以下内容。

1. 设置三层端口的 IP 地址和掩码

   set ipport *<0-63>* **ipaddress** {*<A.B.C.D/M>*|*<A.B.C.D>* *< A.B.C.D>*}

2. 为三层端口绑定 VLAN

   set ipport *<0-63>* **vlan** *<vlanname>*

3. 设置三层端口 MAC 地址

   set ipport *<0-63>* **mac** *<xx.xx.xx.xx.xx.xx>*

   如果不设置，则使用交换机的 MAC 地址。

4. 使能/关闭三层端口

   set ipport *<0-63>* {**enable**|**disable**}

在更改一个 IP 端口的设置时，先要将端口设置为 disable 状态，然后设置需要修改的项，新的设置将覆盖原来的设置。

可以用以下命令清除端口的某个参数或全部参数，在清除之前同样要将端口设置为 disable 状态。

clear ipport *<0-63>* [**mac**|**ipaddress** {*<A.B.C.D/M>*|*<A.B.C.D>* *<A.B.C.D>*}|**vlan** *<vlanname>*]

例如：要在交换机上配置一个 IP 地址 192.1.1.1，掩码为 24 位，将端口绑定在 vlan 100 上，端口使用交换机的默认地址，具体配置如下。

```
zte(cfg)#config router
```

```
zte(cfg-router)#set ipport 1 ipaddress 192.1.1.1/24
zte(cfg-router)#set ipport 1 vlan 100
zte(cfg-router)#set ipport 1 enable
zte(cfg-router)#exit
zte(cfg)#
```

配置完成后，可以使用 **show ipport** [*<0-63>*]命令对 IP 端口的配置进行查看。

7.12.3 静态路由配置

在配置好一个 IP 端口后，如果要接入的远端用户不在接口的网段中，需要使用以下命令设置一条到远端网络的静态路由。

iproute {<A.B.C.D/M>|<A.B.C.D> < A.B.C.D>} < A.B.C.D> [<1-15>]

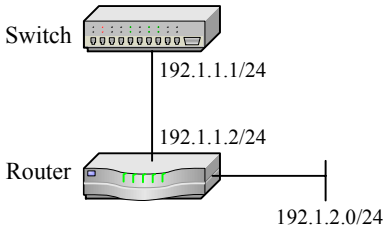


图7.12-1 静态路由配置实例

如 图 7.12-1所示，远程主机所在的网段是 192.1.2.0/24，与交换机不在同一网段。

要使交换机可以和 192.1.2.0/24 上的主机通信，需要配置如下静态路由：

```
zte(cfg)#config router
zte(cfg-router)#iproute 192.1.2.0/24 192.1.1.2
```

用户可以通过 **show iproute** 命令对交换机上的直连路由和静态路由进行查看。

命令中显示静态路由的目的网段、下一跳地址、路由的 metric 值和出接口。显示结果如下所示。

```
zte(cfg-router)#show iproute
  Type   IpAddress      Mask           Gateway        Metric IPport
  ------ -------------- -------------- -------------- ------ ------
  direct 192.1.1.0      255.255.252.0  192.1.1.1       0     0
  static 192.1.2.0      255.255.255.0  192.1.1.2       0     0
  Total: 2
```

使用 **clear iproute** 命令可以用来删除一条或多条静态路由。

7.12.4 ARP 表项配置

交换机上对 ARP 表项的操作包括以下内容。

1. 增加静态 ARP 表项

   arp add *<A.B.C.D> <xx.xx.xx.xx.xx.xx> <0-63> <vlanname>*

2. 删除静态 ARP 表项

   arp delete *<A.B.C.D>*

3. 删除所有的 ARP 表项

   clear arp

4. 设置 IP 端口 ARP 表项的老化时间

   arp ipport *<0-63>* **timeout** *<1-1000>*

   当 ARP 表项在交换机上存在的时间（此间没有接收到此 IP 地址的报文）大于 IP 端口上的老化时间时，交换机将删除此 ARP 表项。

5. 查看 ARP 表中的表项

   show arp [**static**|**dynamic**|**invalid**|**ipport** *<0-63>* {**static**|**dynamic**|**invalid**}|**ipaddress** *<A.B.C.D>*]

7.13 接入服务配置

7.13.1 概述

随着宽带以太网建设规模的迅速扩大，为了满足接入用户数量急剧增加和宽带业务多样性的要求，在交换机上嵌入了接入服务（NAS），以完备接入用户的认证和管理功能，更好地支持宽带网络的计费、安全、运营和管理。

接入服务在运用 802.1x 协议和 RADIUS 协议的基础上，实现对用户接入的认证和管理功能，具有高效、安全、易于运营等优点。

IEEE 802.1x 称为基于端口的访问控制协议（Port-Based Network Access Control）。它的协议体系结构包括三个重要部分：客户端系统、认证系统和认证服务器。

1. 客户端系统一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 IEEE 802.1x 协议的认证过程。为支持基于端口的接入控制，客户端系统需支持扩展认证协议（EAPOL：Extensible Authentication Protocol Over LAN）。

2. 认证系统通常为支持 IEEE 802.1x 协议的网络设备，如交换机。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等）有两个逻辑端口：受控（controlled Port）端口和不受控端口（uncontrolled Port）。

- 不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终可以发出或接受认证。
- 受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。

  IEEE 802.1x 协议中的“可控端口”与“非可控端口”是逻辑上的理解，设备内部并不存在这样的物理开关。对于每个用户而言，IEEE 802.1x 协议均为其建立一条逻辑的认证通道，该逻辑通道其他用户无法使用，不存在端口打开后被其他用户利用问题。

3. 认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。认证系统和 RADIUS 服务器之间通过 RADIUS 协议进行通信。

RADIUS（远程用户拨号认证系统）是一个在 Radius Server 和 Radius Client 之间进行认证、授权、配置数据信息交互的协议标准。

RADIUS 采用 Client/Server 模型。在 NAS 上运行的是 Client 端，负责传送用户信息到指定的 RADIUS 服务器，并根据服务器返回的结果进行相应的操作。

授权认证服务器（Radius Authentication Server）负责接受用户的连接请求，验证用户身份，并返回给客户需要的相关配置信息。一个授权认证服务器可以作为一个 RADIUS 客户代理连接另一个授权认证服务器。

计费服务器（Radius Accounting Server）负责接受用户计费开始请求和计费结束请求，实现计费功能。

接入服务通过 RADIUS 报文同 Radius Server 通信，RADIUS 报文中的属性用来传递认证、授权和计费的详细信息。本交换机中使用的属性主要是 rfc2865，rfc2866，rfc2869 中规定的标准属性。

交换机与用户之间使用 EAP 协议。交换机与 RADIUS 服务器之间提供三种身份验证方式：PAP，CHAP 和 EAP-MD5。根据业务运营的不同需求，可以使用其中任何一种身份验证方式。

- PAP（Password Authentication Protocol）

  PAP 是一种简单的明文验证方式。NAS 要求用户提供用户名和密码，用户以明文方式返回用户信息。服务器端根据用户配置查看是否有此用户以及密码是否正确，然后返回不同的响应。这种验证方式的安全性较差，传送的用户名和密码容易被窃取。

  使用PAP方式进行身份验证的过程如 图 7.13-1所示。

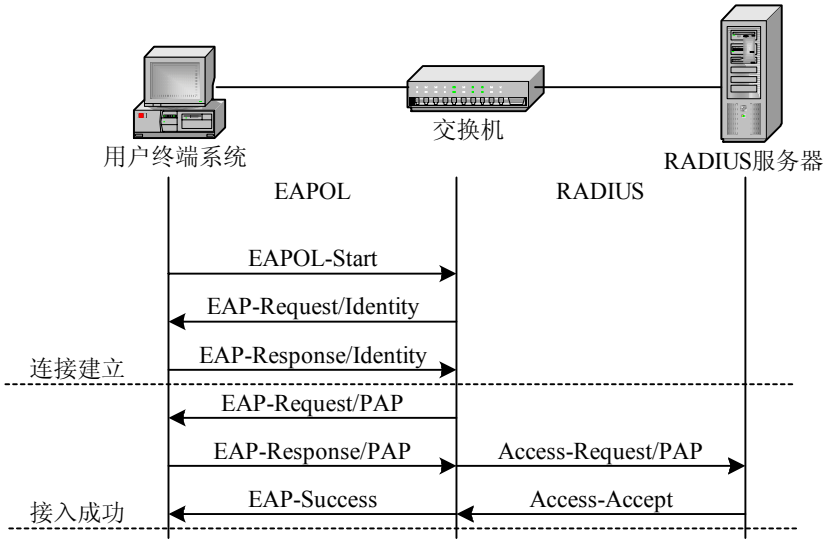


图7.13-1　使用 PAP 方式进行身份验证的过程

- CHAP（Challenge Handshake Authentication Protocol）

  CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向用户发送一个随机产生的挑战口令，用户用自己的密码和 MD5 算法对挑战口令进行加密，并返回用户名和加密的挑战口令（加密口令）。

  服务器端用自己保存的用户密码和 MD5 算法对挑战口令进行加密。比较用户和服务器端的加密口令，根据比较结果返回不同的响应。

  使用CHAP方式进行身份验证的过程如 图 7.13-2所示。

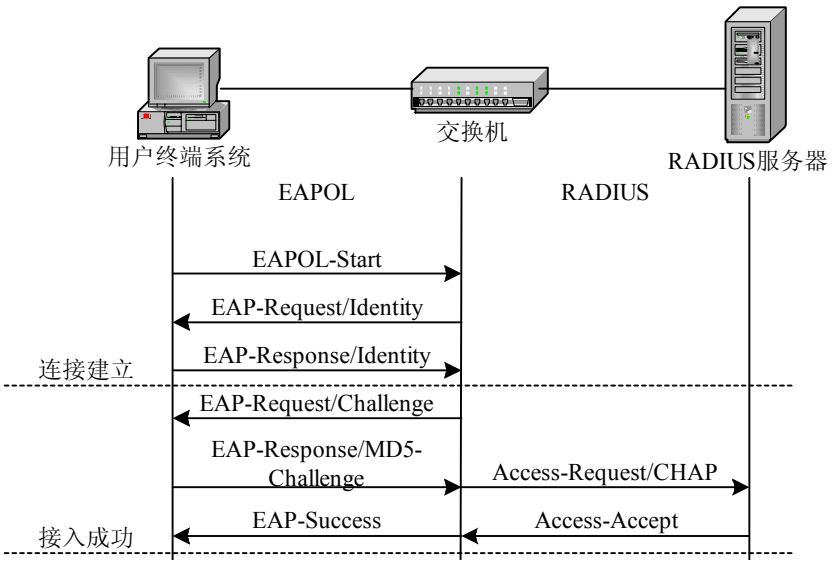


图7.13-2 使用 CHAP 方式进行身份验证的过程

- EAP-MD5（Extensible Authentication Protocol - Message Digest 5）

  EAP-MD5 是EAP框架结构中使用的CHAP身份验证机制。使用EAP-MD5方式进行身份验证的过程如 图 7.13-3所示。

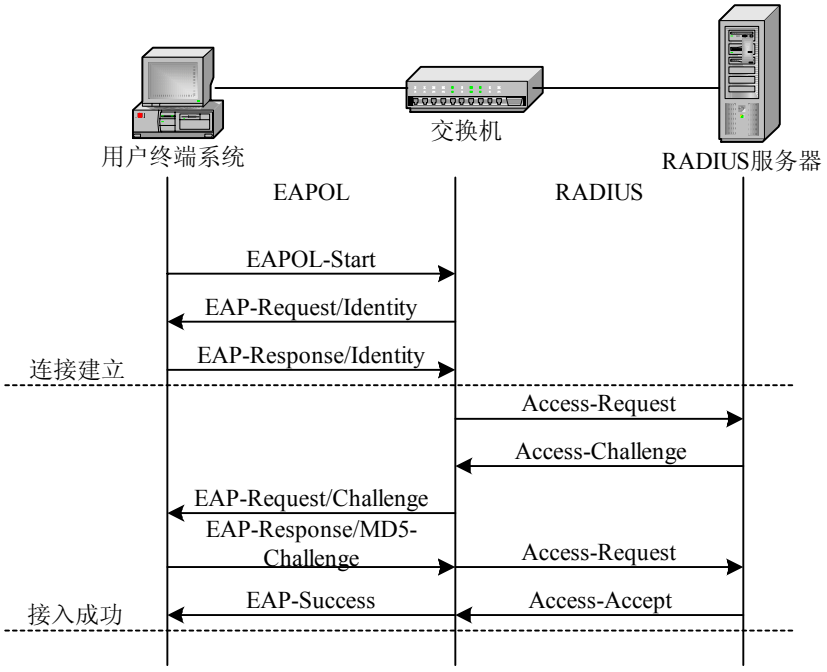


图7.13-3 使用 EAP-MD5 方式进行身份验证的过程

7.13.2 基本配置

在交换机上配置 802.1x 包括以下内容。

1. 开启/关闭端口的 802.1x 功能

   aaa-control port *<portlist>* **dot1x** {**enable**|**disable**}

2. 配置端口的认证控制模式

   aaa-control port *<portlist>* **port-mode** {**auto**|**force-unauthorized**|**force-authorized**}

   可以配置的模式如下：

- **auto**：从配置成 auto 的端口接入的用户必须通过认证，认证成功与否决定了用户能否接入成功。
- **force-authorized**：强制认证通过，用户不需要认证便可以通过该端口接入。
- **force-unauthorized**：强制认证不通过，用户不能通过该端口接入。

   默认的认证控制模式为 auto。

3. 允许/禁止端口多用户接入

   aaa-control port *<portlist>* **multiple-hosts** {**enable**|**disable**}

4. 配置端口的最大用户接入数目

   aaa-control port *<portlist>* **max-hosts** *<0-64>*

   一个端口可以接入多个用户，每个用户有自己独立的认证和计费过程。一个端口允许有多个用户接入时，**aaa-control port max-hosts** 命令才有意义。

5. 打开/关闭配置重认证机制

   dot1x re-authenticate {**enable**|**disable**}

6. 配置重认证的时间间隔

   dot1x re-authenticate period *<1-4294967295>*

   为了判断接入的用户是否一直保持连接，NAS 可以定时要求接入的用户进行重认证。重认证需要为每个在线用户启动一次完整的认证过程，如果用户量较大，认证报文将非常频繁，会对交换机造成一定的负担。

7. 打开/关闭端口的异常下线检测机制

   aaa-control port *<portlist>* **keepalive** {**enable**|**disable**}

8. 设置端口的异常下线检测周期

aaa-control port *<portlist>* **keepalive period** *<1-3600>*

除了重认证机制，为判断接入用户是否保持连接，NAS 模块还提供了异常下线检测机制。异常下线检测只需要少量的报文交互便可以确定用户是否在线。

异常下线检测机制是通过设备主动向客户端定期发送检测请求来实现的。请求报文利用了 802.1x 协议定义的 EAPOL/EAP RepId 报文，如果收到客户端的 EAPOL/EAP RespId 响应说明该用户在线；如果未收到响应则说明用户已经下线。

9. 配置端口的认证方式

aaa-control port *<portlist>* **protocol** {**pap**|**chap**|**eap**}

用户接入认证时，在认证服务器与认证系统之间有三种用户身份识别方式，包含 PAP，CHAP 和 EAP 方式。系统默认为 EAP。

10. 配置协议参数

- 设置认证系统一次认证失败后到接受下一次认证请求的间隔

  dot1x quiet-period *<0-65535>*

- 设置认证系统接收不到客户端回复而重发 EAPOL 数据包的等待时间

  dot1x tx-period *<1-65535>*

- 设置认证系统接收来自认证客户端系统的数据包的超时时间

  dot1x supplicant-timeout *<1-65535>*

- 设置认证系统接收来自认证服务器的数据包的超时时间

  dot1x server-timeout *<1-65535>*

- 设置认证系统接收来自客户端的 challenge 响应的超时重传次数

  dot1x max-request *<1-10>*

  802.1x 通过在客户端系统和认证系统之间传递 EAPOL 数据包，在认证系统和认证服务器之间传递 RADIUS 数据包实现访问控制。在传递数据包的过程中有如下的参数控制：

- quietPeriod 是指在一次认证失败后多长时间内认证系统不接收来自客户端系统的认证请求，这项功能可以防止用户试图不停的进行认证。

- txPeriod 是指认证系统在多长时间内没有收到客户端系统的回复，将会重发 EAPOL 数据包到客户端系统。
- supplicant Timeout 和 serverTimeout 是用来表示在认证过程中认证系统接收来自客户端系统和认证服务器的数据包的超时时间。
- max-request 是指在认证过程中，认证系统接收来自客户端系统的 challenge 响应的超时重传次数。

11. 查看端口的 802.1x 配置

    show aaa-control port [<*portlist*>]

12. 查看 802.1x 协议参数

    show dot1x

在交换机上配置 RADIUS 包括以下内容。

1. 添加/删除一个 ISP 域

   radius isp <*ispname*> {**enable**|**disable**}

   在 RADIUS 配置中，我们引入了域（isp-domain）的概念。不同的域可能由不同的 ISP 经营，接入设备根据用户输入的用户名中的域名部分（用户名@域名）来区分用户所属的域，并将其认证和计费请求发送到相应域的认证和计费服务器。每个域都有自己的 RADIUS 服务器。

   删除某个域后时，同该域相关的所有配置都被删除。

2. 在域中添加认证服务器

   radius isp <*ispname*> **add authentication** <*A.B.C.D*> [<*0-65535*>]

3. 在域中删除认证服务器

   radius isp <*ispname*> **delete authentication** <*A.B.C.D*>

   每个域最多可配置 3 个认证服务器。服务器的优先级同配置顺序相关，最先配置的服务器的优先级最高，最后配置的服务器优先级最低。当删除一个服务器时，后面的服务器的优先级依次递增。

4. 在域中添加记帐服务器

   radius isp <*ispname*> **add accounting** <*A.B.C.D*> [<*0-65535*>]

5. 在域中删除记帐服务器

radius isp <*ispname*> **delete accounting** <*A.B.C.D*>

每个域最多可配置 3 个记帐服务器。服务器的优先级同配置顺序相关，最先配置的服务器的优先级最高，最后配置的服务器优先级最低。当删除一个服务器时，后面的服务器的优先级依次递增。

6. 配置域的客户端 IP 地址

radius isp <*ispname*> **client** <*A.B.C.D*>

域的客户端的 IP 地址必须是交换机上一个接口的 IP 地址。

7. 配置域的共享密码

radius isp <*ispname*> **sharedsecret** <*string*>

共享密码用于 RADIUS 客户端与 RADIUS 服务器进行数据加密，客户端与服务器的配置必须一致。

8. 指定默认域

radius isp <*ispname*> **defaultisp** {**enable**|**disable**}

系统中只能将一个域指定为默认域，系统将所有的没有指定域名的用户认证请求都发送到默认域中的 RADIUS 认证服务器。

9. 配置域全帐号

radius isp <*ispname*> **fullaccount** {**enable**|**disable**}

当指定使用全帐号时，RADIUS 客户端使用“用户名@域名”做为用户名请求 RADIUS 服务器认证；如果没有指定使用全帐号，用户名中不包含域名。

10. 配置域描述符

radius isp <*ispname*> **description** <*string*>

11. 配置 RADIUS 参数

- 配置服务器响应超时时间

  radius timeout <*1-255*>

- 配置服务器响应超时重传次数

  radius retransmit <*1-255*>

- 配置接入服务器名称

radius nasname <*nasname*>

- 配置 radius 记帐中止包的保存时间

  radius keep-time <*0-4294967295*>

12. 打开/关闭端口的计费功能

    aaa-control port <*portlist*> **accounting** {**enable**|**disable**}

13. 删除发送失败的 radius 记帐中止包

    clear accounting-stop {session-id <*session-id*> **| user-name** <*user-name*> **| isp-name** <*isp-name*> **| server-ip** <*A.B.C.D*>**}**

14. 查看 RADIUS 配置

    show radius [**ispname** <*ispname*>|**accounting-stop** [**session-id** <*session-id*> |**user-name** <*user-name*>| **isp-name** <*isp-name*>|**server-ip** <*A.B.C.D*>]]

15. 增加私有的 802.1x 协议包的目的 MAC 地址

    dot1x add fid <*1-256*> **mac** [<*mac-address*>]

    一般的 802.1x 包的目的 MAC 地址为 0180c2000003，在有些交换机上这个目的 MAC 地址包不能透传到认证交换机，为了能透传，客户端发出的包就不能用这个目的 MAC 地址，而使用一个约定的 MAC 地址，在认证交换机上必须配置这个 MAC 地址已识别 802.1x 包。

    如果增加 MAC 地址时不输入 MAC 地址，则为缺省值 01d0d0ffffff。

16. 删除 DOT1X 协议可使用的私有 MAC 地址

    dot1x delete fid <*1-256*>

7.13.3 配置实例

1. 打开端口 1 的 802.1x 功能，将 quient-period 配置为 5 秒，tx-period 配置为 5 秒，supp-timeout 配置为 3 秒，server-timeout 配置为 3 秒；打开 keepalive 功能，并将 keepalive 时间间隔配置为 180 秒。

```
zte(cfg-nas)#aaa-control port 1 dot1x enable
zte(cfg-nas)#dot1x quiet-period 5
zte(cfg-nas)#dot1x tx-period 5
zte(cfg-nas)#dot1x supplicant-timeout 3
zte(cfg-nas)#dot1x server-timeout 3
zte(cfg-nas)#aaa-control port 1 keepalive enable
```

```
zte(cfg-nas)#aaa-control port 1 keepalive period 180

zte(cfg-nas)#show aaa-control port 1
  PortId      : 1              PortControl           : auto
  Dot1x       : enabled        AuthenticationProtocol: eap
  KeepAlive   : enabled        KeepAlivePeriod       : 180
  Accounting  : disabled       MultipleHosts         : disabled
  MaxHosts    : 0              HistoryHostsTotal     : 0
  OnlineHosts: 0

zte(cfg-nas)#show dot1x
  TxPeriod     : 5               QuietPeriod    : 5
  SuppTimeout  : 3               ServerTimeout  : 3
  ReAuthPeriod: 3600             ReAuthenticate: disabled
  MaxReq       : 2
zte(cfg-nas)#
```

2. 打开重认证功能，并将重认证时间间隔设为 60 秒。

```
zte(cfg-nas)#dot1x re-authenticate enable
zte(cfg-nas)#dot1x re-authenticate period 60

zte(cfg-nas)#show dot1x
  TxPeriod     : 5              QuietPeriod    : 5
  SuppTimeout  : 3              ServerTimeout  : 3
  ReAuthPeriod: 60              ReAuthenticate: enabled
  MaxReq       : 2
zte(cfg-nas)#
```

3. 配置端口 1 的认证控制状态为 auto，认证方式为 chap，允许多用户接入，接入的最大用户数为 5。

```
zte(cfg-nas)#aaa-control port 1 port-mode auto
zte(cfg-nas)#aaa-control port 1 protocol chap
zte(cfg-nas)#aaa-control port 1 multiple-hosts enable
zte(cfg-nas)#aaa-control port 1 max-hosts 5

zte(cfg-nas)#show aaa-control port 1
  PortId      : 1              PortControl           : auto
  Dot1x       : enabled        AuthenticationProtocol: chap
  KeepAlive   : enabled        KeepAlivePeriod       : 180
  Accounting  : disabled       MultipleHosts         : enabled
  MaxHosts    : 5              HistoryHostsTotal     : 0
```

```
  OnlineHosts: 0
```

4. 按以下要求配置 RADIUS 域 188：

   认证与记帐服务器地址：10.40.92.212 和 10.40.92.215

   共享密码：123456

   客户端 IP：10.40.92.100，且为默认域

```
zte(cfg-nas)#radius isp 188 enable
zte(cfg-nas)#radius isp 188 add authentication 10.40.92.212
zte(cfg-nas)#radius isp 188 add authentication 10.40.92.215
zte(cfg-nas)#radius isp 188 add accounting 10.40.92.215
zte(cfg-nas)#radius isp 188 add accounting 10.40.92.212
zte(cfg-nas)#radius isp 188 sharedsecret 123456
zte(cfg-nas)#radius isp 188 client 10.40.92.100
zte(cfg-nas)#radius isp 188 defaultisp enable

zte(cfg-nas)#show radius 188
  Client       : 10.40.92.100   IspName     : 188
  DefaultIsp   : Yes            Description :
  FullAccounts: No              SharedSecret: 123456
  Authentication servers  Auth-port
  ----------------------  ---------
  10.40.92.212            1812
  10.40.92.215            1812
  Accounting servers     Acct-port
  ----------------------  ---------
  10.40.92.215            1813
  10.40.92.212            1813

zte(cfg-nas)#
```

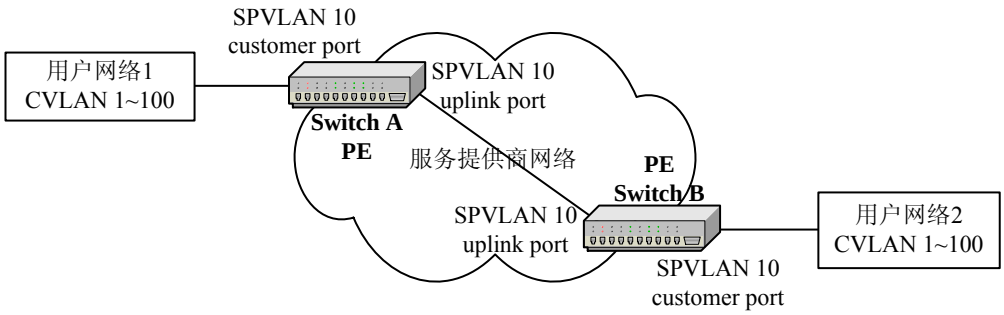
7.14 QinQ 配置

7.14.1 概述

QinQ 是对基于 IEEE 802.1Q 封装的隧道协议的形象称呼，又称 VLAN 堆叠。QinQ 技术是在原有 VLAN 标签（内层标签）之外再增加一个 VLAN 标签（外层标签），外层标签可以将内层标签屏蔽起来。

QinQ 不需要协议的支持，通过它可以实现简单的 L2VPN（二层虚拟专用网），特别适合以三层交换机为骨干的小型局域网。

QinQ技术的典型组网如 图 7.14-1所示，连接用户网络的端口称为Customer端口，连接服务提供商网络的端口称为Uplink端口，服务提供商网络边缘接入设备称为PE（Provider Edge）。



SPVLAN：Service Provider VLAN；CVLAN：Customer VLAN

图7.14-1 QinQ 典型组网

用户网络一般通过 Trunk VLAN 方式接入 PE，服务提供商网络内部的 Uplink 端口通过 Trunk VLAN 方式对称连接。

1. 当报文从用户网络 1 到达交换机 A 的 customer 端口时，由于基于 portbase vlan 的 customer 端口接受数据时不认 tag，不论该数据包里是否打了 vlan tag，都把该数据报当作 untag 包处理，在其 pvid 决定的 vlan 即 vlan10 内转发。
2. 交换机 A 的 uplink 端口在转发从 customer 端口收来的数据包时强行插入外层标签（VLAN ID 为 10），该 tag 的 tpid 可在交换机上进行设置。在服务提供商网络内部，报文沿着 VLAN 10 的端口传播，直至到达交换机 B。
3. 交换机 B 发现与用户网络 2 相连的端口为 customer 端口，于是按照传统的 802.1Q 协议剥离外层标签，恢复成用户的原始报文，发送到用户网络 2。
4. 这样，用户网络 1 和 2 之间的数据可以通过服务提供商网络进行透明传输，用户网络可以自由规划自己的私网 VLAN ID，而不会导致和服务提供商网络中的 VLAN ID 冲突。

7.14.2 基本配置

交换机上 PVLAN 的配置包括以下内容。

1. 添加/删除 customer 端口

   set qinq customer port <*portlist*> {**enable**|**disable**}

2. 添加/删除 uplink 端口

   set qinq uplink port <*portlist*> {**enable**|**disable**}

3. 设置外层标签的 tpid

   set qinq tpid <*tpid*>

4. 显示 QinQ 配置

   show qinq

说明：

配置 QinQ 时，SPVLAN 的 customer 端口既可以设置为 untagged 端口，也可以设置为 tagged 端口。uplink 端口也是如此。

7.14.3 配置实例

如 图 7.14-1所示，假设交换机A的customer端口为port 1，uplink端口为port 4；交换机B的customer端口为port 1，uplink端口为port 4。

交换机 A 的配置：

```
zte(cfg)#set vlan 10 enable
zte(cfg)#set vlan 10 add port 1,4
zte(cfg)#set port 1,4 pvid 10
zte(cfg)#set qinq customer port 1 enable
zte(cfg)#set qinq uplink port 4 enable
```

交换机 B 的配置与交换机 A 配置相同。

7.15 Syslog 配置

7.15.1 概述

Syslog 日志系统是以太网交换机中不可或缺的一部分，它是系统软件模块的信息枢纽。日志系统管理大多数的重要信息输出，并且能够进行细致的分类，从而能够有效地进行信息筛选，为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

Syslog 日志系统按照信息来源进行划分，依功能模块进行信息过滤，满足用户的定制要求。

Syslog日志系统可将日志信息按重要性划分为如 表 7.15-1所示的八种等级，按等级进行信息过滤。

表7.15-1 Syslog 日志系统的日志信息

严重等级	描述
emergencies	极其紧急的错误
alerts	需立即纠正的错误
critical	关键错误
errors	需关注但不关键的错误
warnings	警告，可能存在某种差错
notifications	需注意的信息
informational	一般提示信息
debugging	调试信息

7.15.2 基本配置

交换机上 Syslog 的配置包括以下内容：

1. 开启/关闭 Syslog 功能

   set syslog

说明：

Syslog 功能缺省是关闭的。开启 Syslog，当信息量较多时影响交换机的系统性能。

2. 定义 Syslog 信息的等级

   set syslog level

   Syslog 信息的等级如概述中所述，缺省设置为 informational。

说明：

配置 Syslog 信息的等级为 emergencies 时，信息将优先发送。

3. 设置 Syslog 信息接收服务器

   set syslog add |delete server

本交换机最多可配置 5 个 syslog server 地址。

4. 开启/关闭发送 Syslog 的模块

set syslog module

开启/关闭发送 Syslog 的功能模块。

5. 显示 Syslog 配置

show syslog status

7.15.3 配置实例

假设开启交换机的 Syslog 功能，信息等级为 informational,开启所有功能模块，服务器 IP 地址为 192.168.1.1，名称为 Srv1。

交换机的配置：

```
zte(cfg)#set syslog level informational
zte(cfg)#set syslog add server 1 ipaddress 192.168.1.1 name Srv1
zte(cfg)#set syslog module all enable
zte(cfg)#set syslog enable
zte(cfg)#show syslog status
  Syslog status: enable
  Syslog alarm level: informational
  Syslog enabled modules:
  alarm        commandlog
  Syslog server IP          Name
  1           192.168.1.1   Srv1
```

7.16 NTP 配置

7.16.1 概述

NTP（网络时间协议）是以太网交换机用来实现网络设备之间时间同步功能的模块，ZXR10 5009 提供 NTP 客户端的功能，可以与网络上的其他 NTP 服务器之间进行时间同步。

7.16.2 基本配置

交换机上 NTP 的配置包括以下内容：

1. 开启/关闭 NTP 功能

set ntp

说明：

本命令相当于 NTP 功能的总开关，配置后其余的 NTP 命令才能生效。NTP 功能打开后，必须在配置了 NTP 服务器 IP 地址之后才会真正进行时间同步动作，即要 NTP 协议生效的必要条件是:设置了 NTP 服务器 IP 地址和 NTP 协议功能使能。

2. 设置 NTP 服务器的 IP 地址

   set ntp server

   目前只允许配置从一个时间服务器同步时间。若配置多条命令，则后面的配置将覆盖前面的。

3. 设置 NTP 协议发送同步时间请求时使用的源地址

   set ntp source

   默认情况下，交换机没有配置源地址，NTP 发送同步时间请求时，由 IP 层决定报文所使用的 IP 地址。

4. 显示 NTP 状态

   show ntp

7.16.3 配置实例

假设交换机与 NTP 服务器（IP 地址是 202.10.10.10）进行时间同步。首先需要保证交换机可以与 NTP 服务器所在的网段可以互通。NTP 模块的配置如下：

```
zte(cfg)#set ntp server 202.10.10.10
zte(cfg)#set ntp enable
zte(cfg)#show ntp
  ntp protocol is enable
  ntp protocol version : 3
  ntp server address   : 202.10.10.10
  ntp source address   : None
  ntp is_synchronized  : No
  ntp rcv stratum     : 16
  no reference clock.
```

在显示的信息中 ntp is_synchronized 表示当前交换机是否与服务器的时间同步。

7.17 GARP/GVRP 配置

7.17.1 概述

GARP（Generic Attribute Registration Protocol）是一种通用的属性 Attribute 注册协议，通过不同的应用协议，为相同交换网内成员之间动态分发 VLAN、组播 MAC 地址等属性信息。

GVRP（GARP VLAN Registration Protocol） GARP VLAN 注册协议是 GARP 所定义的一种应用协议，它基于 GARP 的协议机制动态维护交换机中的 VLAN 信息。所有支持 GVRP 特性的交换机能够接收来自其他交换机的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，其中包括交换机上当前的 VLAN，以及这些 VLAN 包含了哪些端口等，而且所有支持 GVRP 特性的交换机能够将本地的 VLAN 注册信息向其他交换机传播，以便根据需要使同一交换网内所有支持 GVRP 特性的设备的 VLAN 配置在互通性上达成一致。

7.17.2 GARP 配置

交换机中设置 GARP 主要包括以下内容：

1. 使能/关闭系统 GARP 功能

   set garp

   系统 GARP 功能缺省处于关闭状态，该命令用于全局开启/关闭 GARP 。

2. 设置 GARP 定时器

   set garp timer {**hold**|**join**|**leave**|**leaveall**}*<timer_value>*

   共有四种定时器：hold 定时器, join 加入定时器，leave 离开定时器，leaveall 离开所有定时器。

3. 显示 GARP 信息及定时器设置情况

   show garp

说明：

配置 GARP 定时器时，要保证在同一交换网络中所有启用该协议的定时器完全相同，否则应用协议不能正常工作。

7.17.3 GVRP 配置

交换机中 GVRP 设置主要包括以下内容：

1. 使能/关闭系统 GVRP 功能

   set gvrp

   系统 GVRP 功能缺省处于关闭状态，该命令用于全局开启/关闭 GVRP 。GVRP 使能要在 GARP 使能的情况下才能进行。

2. 端口使能/关闭 GVRP 功能

   set gvrp port <*portlist*> {**enable**|**disable**}

   系统端口 GVRP 功能缺省处于关闭状态，该命令用于开启/关闭端口 GVRP 功能，端口 GVRP 功能开启后可以接受 GVRP 协议报文。

3. 配置端口的 GVRP 注册类型功能

   set gvrp port <*portlist*> **registration** {**normal**|**fixed**|**forbidden**}

   系统端口的 GVRP 注册类型缺省处于 normal 状态，该命令用于设置端口 GVRP 注册类型，端口注册类型有三种：

- Normal：实体对接收到的 GARP 消息正常处理,可动态创建、注册和注销 VLAN。
- Fixed：忽略所有的 GARP 消息，但仍然在注册状态, 允许手工创建和注册 VLAN，防止 VLAN 的注销和其他接口注册此接口所知 VLAN。
- Forbidden：忽略所有的 GARP 消息，注销除了 VLAN1 以外的所有 VLAN，禁止在接口上创建和注册其他 VLAN。

4. Trunk 端口使能/关闭 GVRP 功能

   set gvrp trunk <*trunklist*> {**enable**|**disable**}

5. 系统 Trunk 端口 GVRP 功能缺省处于关闭状态，该命令用于开启/关闭 Trunk 端口 GVRP 功能，Trunk 端口 GVRP 功能开启后可以接受 GVRP 协议报文。

6. 配置 Trunk 端口的 GVRP 注册类型功能

   set gvrp trunk <*trunklist*> **registration** {**normal**|**fixed**|**forbidden**}

   系统 Trunk 端口的 GVRP 注册类型缺省处于 normal 状态，该命令用于设置 Trunk 端口 GVRP 注册类型，Trunk 端口注册类型有三种，每种注册类型的功能和端口的功能相同。

7. 显示 GVRP 配置信息

show gvrp

该命令用于显示 GVRP 配置信息，包括 GVRP 使能与否，各端口和 Trunk 端口 GVRP 的配置情况。

7.17.4 配置实例

1. 下面的实例中，分别对交换机上的 GARP 使能与否，GARP 定时器进行了设置。

```
zte(cfg)#set garp enable
zte(cfg)#set garp disable

zte(cfg)#set garp timer hold 100
zte(cfg)#set garp timer join 200
zte(cfg)#set garp timer leave 600
zte(cfg)#set garp timer leaveall 10000
```

2. 下面的实例中，显示了 GARP 的设置情况。

```
zte(cfg)#show garp
  GARP is enabled!
  GARP Timers:
  Hold Timeout      :100 millisecond
  Join Timeout      :200 millisecond
  Leave Timeout     :600 millisecond
  LeaveAll Timeout  :10000 millisecond
```

3. 下面的实例中，分别对交换机上的 GVRP 使能与否，GVRP 端口使能与否，端口注册类型进行了设置。

```
zte(cfg)#set gvrp enable
zte(cfg)#set gvrp disable

zte(cfg)#set gvrp port 2 enable
zte(cfg)#set gvrp port 2 disable

zte(cfg)#set gvrp port 2 registration fixed
zte(cfg)#set gvrp port 2 registration forbidden
zte(cfg)#set gvrp port 2 registration normal
```

4. 下面的实例中，对交换机上的 GVRP Trunk 端口使能与否，Trunk 端口注册类型进行了设置。

```
zte(cfg)#set gvrp trunk 2 enable
zte(cfg)#set gvrp trunk 2 disable

zte(cfg)#set gvrp trunk 2 registration fixed
zte(cfg)#set gvrp trunk 2 registration forbidden
zte(cfg)#set gvrp trunk 2 registration normal
```

5. 下面的实例中，显示了 GVRP 的设置情况。

```
zte(cfg)#show gvrp
  GVRP is enabled!

  PortId Status   Registration LastPduOrigin
  ------ -------- ------------ -----------------
  2      Enabled  Fixed        00.00.00.00.00.00
  T2     Enabled  Normal       00.00.00.00.00.00
```

第8章 网络管理

摘要

本章介绍ZXR10 5009交换机的网络管理功能，包括Remote-Access 、SSH、SNMP、RMON、集群管理和WEB。

8.1 Remote-Access

8.1.1 概述

Remote-Access是限制网管用户通过Telnet登录的一种机制，即受限制登录，其目的是增强网管的安全性。

开启受限制登录功能后，可以通过配置，指定网管用户只能从指定的IP地址登录交换机，从其他地址不能登录。取消受限制登录功能时，网管用户可以从任意的IP地址，通过Telnet登录到交换机。

8.1.2 基本配置

交换机上Remote-Access的配置包括以下内容。

1. 取消/打开受限制登录

   set remote-access {**any**|**specific**}

   系统缺省情况下，受限制登录为取消状态。

2. 配置允许登录的IP地址

   set remote-access ipaddress <*A.B.C.D*> [<*A.B.C.D*>]

3. 删除所有允许登录的IP地址

   clear remote-access all

4. 删除某个允许登录的IP地址

   clear remote-access ipaddress <*A.B.C.D*> [<*A.B.C.D*>]

5. 显示Remote-Access的配置信息

   show remote-access

8.1.3 配置实例

示例一：只允许网管从 10.40.92.0/24 网段，通过 Telnet 登录到交换机。

```
zte(cfg)#set remote-access specific
zte(cfg)#set remote-access ipaddress 10.40.92.0 255.255.255.0
zte(cfg)#show remote-access
  Whether check remote manage address: YES
  Allowable remote manage address list:
    10.40.92.0/255.255.255.0
zte(cfg)#
```

示例二：只允许网管从地址 10.40.92.212，通过 Telnet 登录到交换机。

```
zte(cfg)#set remote-access specific
zte(cfg)#set remote-access ipaddress 10.40.92.212
zte(cfg)#show remote-access
  Whether check remote manage address: YES
  Allowable remote manage address list:
    10.40.92.212/255.255.255.255
zte(cfg)#
```

示例三：允许网管从任意 IP 地址，通过 Telnet 登录到交换机。

```
zte(cfg)#set remote-access any
zte(cfg)#show remote-access
  Whether check remote manage address: NO
  Allowable remote manage address list:
    any
zte(cfg)#
```

8.2 SSH

8.2.1 概述

SSH（Secure Shell）是 IETF 的 Network Working Group 所制定的一个协议，用于在非安全网络上提供安全的远程登录和其他安全网络服务。

SSH 协议的本意是要解决互联网络中远程登录的安全问题，为 Telnet、Rlogin 等提供一个更安全的替代手段（虽然目前 SSH 协议的发展已经远远超出了远程登录的功能范围），所以 SSH 连接协议必须要具备对交互会话的支持。

使用 SSH 可以对传输的所有数据进行加密，即使有人截获这些数据也无法得到有用的信息。

目前 SSH 协议有两个不兼容的版本：SSH v1.x 和 SSH v2.x。本交换机只支持 SSH v2.0，并采用密码认证的方式。SSH 使用端口号为 22。

8.2.2 基本配置

在交换机上配置 SSH 包括以下内容。

1. 使能或关闭 SSH 功能

   set ssh {**enable**|**disable**}

   SSH 功能的缺省状态是关闭的。SSH 方式通常在远程登录交换机进行配置时使用，交换机上需要设置登录用户名和密码（或者设置远端的 RADIUS 登录方式），并且本地主机能够 ping 通交换机上 IP 端口的地址。

   本交换机仅支持单用户的 SSH 登录方式，允许用户尝试登录 3 次，尝试 3 次后自动关闭与用户的连接。用户登录后，可以使用 **set ssh disable** 命令关闭与用户的连接，禁止用户使用 SSH 登录方式，但如果用户处于 Diffie-Hellman key exchange 状态，则禁止使用该命令。

2. 显示 SSH 的配置和用户的登录状态

   show ssh

8.2.3 配置实例

如 图 8.2-1所示，一台主机要通过SSH登录到交换机。交换机上配置了一个三层端口，IP地址为 192.1.1.1/24，主机的IP地址为 192.1.1.100/24。

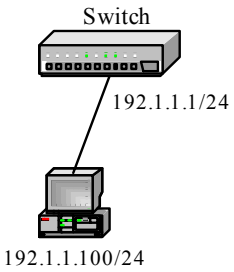


图8.2-1 SSH 配置实例

交换机的具体配置如下：

```
zte(cfg)#creat user zte
zte(cfg)#loginpass zte
zte(cfg)#set ssh enable
```

SSH v2.0 的客户端可以使用 Simon Tatham 开发的免费软件 Putty。使用 Putty 登录交换机时需进行如下设置。

1. 设置SSH Server的IP地址和端口号，如 图 8.2-2所示。

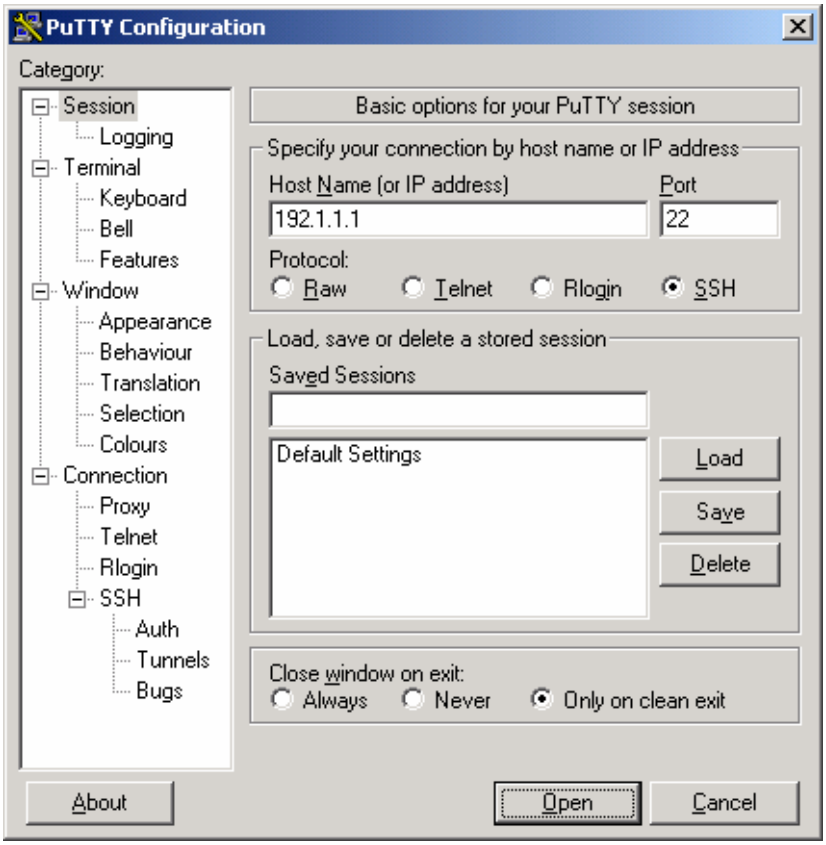


图8.2-2　设置 SSH Server 的 IP 地址和端口号

2. 设置SSH的版本号，如 图 8.2-3所示。

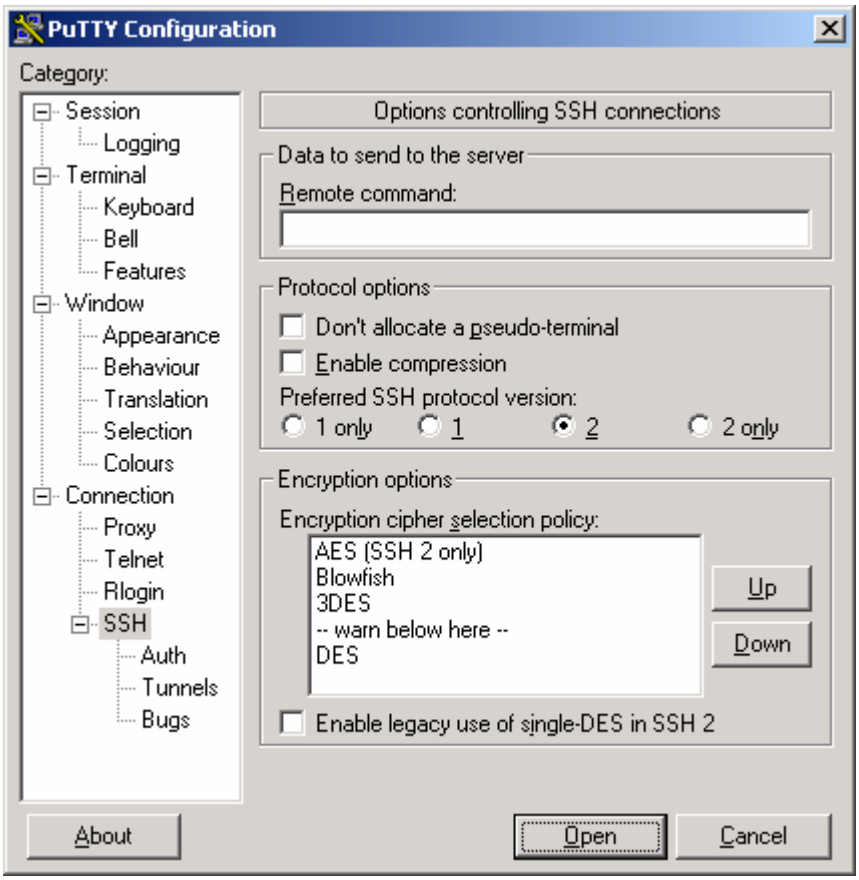


图8.2-3 设置 SSH 的版本号

3. 第一次登录时需要用户进行确认，如 图 8.2-4所示。

图8.2-4 第一次登录时需要用户进行确认

4. SSH登录结果，如 图 8.2-5所示。

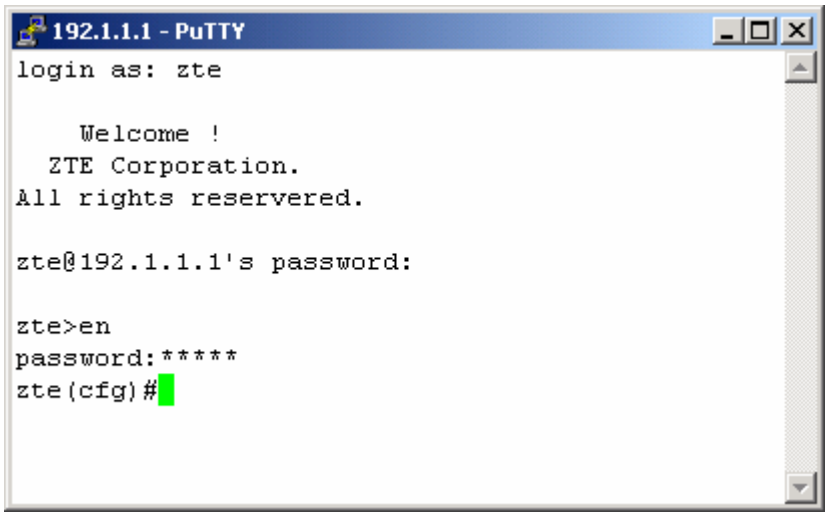


图8.2-5　SSH 登录结果

8.3 SNMP

8.3.1 概述

SNMP（简单网络管理协议）是目前最流行的一种网管协议，包括一系列协议组和规范：

- MIB：管理信息库
- SMI：管理信息的结构和标识
- SNMP：简单网络管理协议

它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。任何一个网络管理者都可以利用 SNMP 管理交换机。ZXR10 5009 系列交换机支持 SNMPv1、v2c 和 v3 多个版本（v3 在 v1、v2c 的基础上增强了 SNMP 管理的安全性）。

SNMP 采用“管理进程－代理进程”模型来监视和控制 Internet 上各种可管理的网络设备。SNMP 网络管理必须具备三个要素：

1. 被管理设备，具备在 Internet 上通信的能力，每个设备都含有一个代理；
2. 网络管理站（Network Management Station，NMS），网络管理进程必须具备在 Internet 上通信的能力；
3. 用于交换代理进程和 NMS 之间的管理信息的协议，这个协议就是 SNMP。

网络管理站通过轮询在被管理设备中的代理来收集数据。被管理设备中的代理可以在任何时候向网络管理站报告错误情况，而不需要等到管理站对它进行轮询。这些错误情况称为 Trap。当设备产生了一个 Trap 时，可以使用网络管理站来查询该设备（假设它仍然是可到达的），以获得更多的信息。Snmp v2c 和 v3 还支持 inform（一个需要得到响应的 SNMPv2 Trap）向 NMS 通告异常事件，NMS 如果收到 inform 报文会给交换机发送一个收到确认报文，若交换机在一定的时间内收不到 NMS 发来的收到确认报文，交换机将原 inform 报文重发两次。

网络中的所有变量都存放在 MIB 数据库中。SNMP 协议对网络设备状态的监视主要通过查询代理 MIB 中相应对象的值来完成。ZXR10 5009 实现了 rfc1213，rfc1493，rfc2674，rfc2819 规定的标准 MIB 及私有 MIB。

8.3.2 基本配置

SNMP 的配置包括以下内容。

1. 创建团体名并设置访问权限

   create community

   community 字符串提供了远程网络管理员配置交换机的用户确认机制，pubilc 表示允许对交换机进行只读访问，private 表示对交换机有读/写操作的权限。

   交换机第一次启动时缺省配置了权限为 public 的名字为“public”的团体。

   如果用此命令创建的 community 字符串已经存在，则新创建的字符串将覆盖原来的。

2. 创建视图（view），并指定该 view 是否包含某 mib 子树

   create view

   view 是 MIB 的一个对象子集，参数<*mib-oid*>指定了 mib 子树。如果不指定 exclude 或 include 的 mib 子树，则缺省 include 1.3.6.1。

   交换机第一次启动时缺省配置了名字为“zteView”的视图，参数缺省。

   如果用此命令创建的 view 已经存在，则新创建的 view 将覆盖原来的。

3. 设置视图包含指定的团体名

   set community view

   一个 community 只能对应一个 view，一个 view 可以对应多个 community。

4. 设置组名及其安全级别

   set group

   group 的权限可以为不认证不加密、认证不加密和认证且加密三种级别。可以为 group 配置读、写和通知视图。如果不指定视图，则会将读、写和通知视图都配置为缺省视图“zteView”。可以在交换机上配置名字相同但安全等级不同的 group。

5. 设置用户名及其所属组和安全属性

   set user

   user 的安全属性包括认证和加密的密码，认证和加密所采用的算法（MD5\SHA\DES），并且 user 和 group 的安全级别应一致。

6. 设置引擎标识

   set engineID

说明：

engineID 唯一地标识一个 SNMP 实体，故修改后，原 engineID 下的配置将不再起作用。

---

7. 设置 trap 或 inform 主机的 IP 地址、团体名和版本

   set host

   host 主机是 trap 或 inform 发送的目的主机 IP 地址，同时可以指明 trap 或 inform 的版本和 community 或 user。

8. 使能/关闭 SNMP 的 trap

   set trap

   使能状态下，当发生上述 5 中情况时会发送 trap 到管理台。其中冷启动和热启动 trap 要等系统启动完成以后才会向管理台发送，一般会有几分钟的时延。

9. 删除团体名

   clear community

10. 删除视图名

clear view

11. 删除组名

clear group

12. 删除用户名

clear suer

13. 删除 trap 或 inform 主机

clear host

14. 显示 SNMP 信息

show snmp

8.3.3 配置实例

1. SNMPv1、SNMPv2c 基本配置

假设网管服务器地址为 10.40.92.105，交换机上有一个 IP 地址为 10.40.92.200 的三层端口，要通过网管服务器管理交换机。

创建一个名为 zte 的具有读写权限的团体和一个名为 vvv 视图，关联团体 zte 和视图 vvv 指定接收 trap 的主机地址为 10.40.92.105，commnity 为 zte。

```
zte(cfg)#config router
zte(cfg-router)#set ipport 0 ipaddress 10.40.92.200 255.255.255.0
zte(cfg-router)#set ipport 0 vlan 2
zte(cfg-router)#set ipport 0 enable
zte(cfg-router)#exit

zte(cfg)#config snmp
zte(cfg-snmp)#create community zte private
zte(cfg-snmp)#create view vvv
zte(cfg-snmp)#set community zte view vvv
zte(cfg-snmp)#set host 10.40.92.105 trap v1 zte

zte(cfg-snmp)#show snmp community
  CommunityName  Level     ViewName
  -------------- --------- ------------
  zte            private    vvv

zte(cfg-snmp)#show snmp view
```

```
 ViewName     Exc/Inc  MibFamily
 ------------ -------- ------------------------
 vvv          Include  1.3.6.1

zte(cfg-snmp)#show snmp host
 HostIpAddress    Comm/User   Version  type   SecurityLevel
 ---------------- ----------- ------- ------ -------------
 10.40.92.77       zte         Ver.1    Trap   -
zte(cfg-snmp)#
```

2. SNMPv3 基本配置

假设网管服务器地址为 10.40.92.77，交换机上有一个 IP 地址为 10.40.92.11 的三层端口，使用用户安全模式（User Security Model，USM）通过网管服务器管理交换机。

创建一个名为 zteuser 的用户，配置其所属组名字 ztegroup，此组的安全级别为 priv（即认证且加密），其读、写和通知视图均为缺省。指定接收 trap 或 inform 的主机地址为 10.40.92.77，user 为 zteuser。

```
zte(cfg)#config router
zte(cfg-router)#set ipport 1 ipaddress 10.40.92.11/24
zte(cfg-router)#set ipport 1 vlan 1
zte(cfg-router)#set ipport 1 enable
zte(cfg-router)#exit

zte(cfg)#config snmp
zte(cfg-snmp)# set group ztegroup v3 priv
zte(cfg-snmp)# set user zteuser ztegroup v3 md5-auth zte des56-priv
               zte
zte(cfg-snmp)# set host 10.40.89.77 inform v3 zteuser priv

zte(cfg-snmp)#show snmp group
 groupName: ztegroup
 secModel : v3                    readView  : zteView
 secLevel : AuthAndPriv           writeView : zteView
 rowStatus: Active                notifyView: zteView

zte(cfg-snmp)#show snmp user
 UserName   : zteuser
 GroupName  : ztegroup(v3)
 EngineID   : 830900020300010289d64401
 AuthType   : Md5                  StorageType: NonVolatile
```

```
  EncryptType: Des_Cbc                RowStatus  : Active

zte(cfg-snmp)#show snmp host
  HostIpAddress    Comm/User   Version type    SecurityLevel
  ---------------- ----------- ------- ------ -------------
  10.40.89.77      zteuser     Ver.3   Inform  AuthAndPriv

zte(cfg-snmp)#
```

8.4 RMON

8.4.1 概述

RMON（Remote Monitoring）即远程监视，它定义了标准网络监视功能以及在管理控制台和远程监视器之间的通信接口。RMON 提供了一个有效而且高效的方法，它可以在降低其它代理和管理站负载的情况下监视子网的行为。

RMON 的规范主要是 RMON 管理信息库的定义。ZXR10 5009 实现了 RMON MIB 中的 4 个组，分别是：

- 历史（history）：记录从统计组可得到的信息的周期性统计样本；
- 统计（statistics）：维护代理监视的每一个子网的基本使用和错误统计；
- 事件（event）：一个关于由 RMON 代理产生的所有事件的表；
- 告警（alarm）：允许管理控制台人员为 RMON 代理记录的任何计数或整数设置采样间隔和告警阈值。

这些组均用于存储由监视器收集到的数据及由此衍生出的数据和统计。其中 alarm 组需要 event 组的实现。这些数据可以用 MIB 浏览器来获取。

RMON 的控制信息的配置可以通过 MIB 浏览器进行，也可以通过超级终端或远程 telnet 的命令行进行配置。RMON 的采样信息和统计数据需要通过 MIB 浏览器获取。

8.4.2 基本配置

下面介绍通过超级终端或远程 telnet 方式配置 RMON 控制信息的方法。

1. 开启/关闭 RMON 功能

   set rmon {**enable**|**disable**}

缺省情况下 RMON 功能是关闭的。在 RMON 功能使能的情况下才能进行 history 组中 etherHistoryTable 和 statistics 组中 etherStatsTable 信息的采样。在采样过程中关闭 RMON 功能将停止数据采样。

2. 创建或配置 history 组的实例

set history *<1-65535>* {**datasource***<portname>*|**bucketRequested** *<1-65535>*|**owner** *<string>*|**interval** *<1-3600>*| **status** {**valid|underCreation|createRequest|invalid**}}

history 组的命令行配置是对 history 组中 historyControlTable 的历史组控制信息进行配置，主要包括：

- 数据源（historyControlDataSource）：是 rfc1213 interface 组中的 ifIndex oid 号，比如端口 6 的 oid 号是 1.3.6.1.2.1.2.2.1.1.6，命令行配置时直接输入端口号 6 即可。
- 采样桶个数（historyControlBucketsRequested），缺省为 50。
- 实例拥有者（historyControlOwner）。
- 采样间隔时间（historyControlInterval），缺省为 1800 秒。
- 实例状态（historyControlStatus）：实例状态共有四种：valid，underCreation，createRequest，invalid。当实例状态被置为 invalid 时，该实例会被删除。必须指定数据源才能够将实例状态置为 valid。

3. 创建或配置 statistics 组的实例

set statistics *<1-65535>* {**datasource** *<portname>*|**owner** *<string>*|**status** {**valid|underCreation|createRequest| invalid**}}

statistics 组的命令行配置是对 statistics 组中 etherStatsTable 的统计组信息进行配置，主要包括：

- 数据源（etherStatsDataSource）：与 history 组相同，数据源在命令行配置时直接输入端口号即可。
- 实例拥有者（etherStatsOwner）。
- 实例状态（etherStatsStatus）：实例状态共有四种：valid，underCreation，createRequest，invalid。当实例状态被置为 invalid 时，该实例会被删除。必须指定数据源才能够将实例状态置为 valid。

4. 创建或配置 event 组的实例

set event *<1-65535>* {**description** *<string>*|**type** {**none|log|snmptrap|logandtrap**}|**owner** *<string>*|**community** *<string>*| **status** {**valid|underCreation| createRequest|invalid**}}

event 组的命令行配置是对 event 组中 eventTable 的事件组信息进行配置，主要包括：

- 事件描述（eventDescription）。
- 事件类型（eventType）：事件类型有四种情况：none（1），log（2），snmp-trap（3），log-and-trap（4）。选 log 时，在 logTable 中为每一事件建立一个日志实例；选 snmp-trap 时，对于每个事件，监视器发送一个 SNMP 陷阱（trap）到一个或多个管理站；选 log-and-trap 时，既记录日志又发送 trap。
- 实例拥有者（eventOwner）。
- 事件团体串（eventCommunity）。
- 实例状态（eventStatus）：实例状态共有四种：valid，underCreation，createRequest，invalid。当实例状态被置为 invalid 时，该 event 实例会被删除。

5. 创建或配置 alarm 组的实例

set alarm *<1-65535>* {**interval** *<1-65535>*|**variable** *<mib-oid>*|**sampletype** {**absolute|delta**}|**startup** {**rising|falling|both**}|**threshold** *<1-65535>* **eventindex** *<1-65535>* {**rising|falling**}|**owner** *<string>*|**status** {**valid|underCreation|createRequest| invalid**}}

alarm 组的命令行配置是对 alarm 组中 alarmTable 的告警组信息进行配置，主要包括：

- 告警间隔时间（alarmInterval）。
- 告警变量（alarmVariable）：告警变量是指本地 mib 中要被采样的特定变量的对象标识符，如采样 etherHistoryBroadcastPkts 历史广播包个数，则变量值应该为 1.3.6.1.2.1.16.2.2.1.7.x.x，其中 x.x 表示某历史组实例的第几个采样桶。
- 告警采样类型（alarmSampleType）：告警采样类型选 absolute 表示绝对值，delta 表示相对值。
- 告警启动类型（alarmStartupAlarm）：告警启动类型有以下三种：risingAlarm（1），fallingAlarm（2），risingOrFallingAlarm（3），分别表示在该实例有

效后，采样值上升超过阈值、采样值下降低于阈值或者两种情况同时发生时开始第一次采样。

- 上升阈值（alarmRisingThreshold）
- 下降阈值（alarmFallingThreshold）
- 上升触发事件的索引值（alarmRisingEventIndex）
- 下降触发事件的索引值（alarmFallingEventIndex）
- 实例拥有者（alarmOwner）
- 实例状态（alarmStatus）：实例状态共有四种：valid，underCreation，createRequest，invalid。当实例状态被置为 invalid 时，该 alarm 实例会被删除。

  必须等待告警变量指定的被采样对象能够采样到数据时才能配置告警变量。告警变量配置成功才能将实例状态置为 valid。

6. 查看 RMON 的状态和配置信息

- 显示 rmon 的状态

  show rmon

- 显示 history 组的配置信息

  show history

- 显示 statistic 组的配置信息

  show statistic

- 显示 event 组的配置信息

  show event

- 显示 alarm 组的配置信息

  show alarm

8.4.3 配置实例

下面的实例中，分别对事件组 2、历史组 2、告警组 2、统计组 1 进行设置。

```
zte(cfg-snmp)#set event 2 description It'sJustForTest!!
zte(cfg-snmp)#set event 2 type logandtrap
zte(cfg-snmp)#set event 2 community public
```

```
zte(cfg-snmp)#set event 2 owner zteNj
zte(cfg-snmp)#set event 2 status valid

zte(cfg-snmp)#set history 2 datasource 6
zte(cfg-snmp)#set history 2 bucket 3
zte(cfg-snmp)#set history 2 interval 10
zte(cfg-snmp)#set history 2 owner zteNj
zte(cfg-snmp)#set history 2 status valid

zte(cfg-snmp)#set rmon enable

zte(cfg-snmp)#set alarm 2 interval 10
zte(cfg-snmp)#set alarm 2 variable 1.3.6.1.2.1.2.2.1.1.6
zte(cfg-snmp)#set alarm 2 sampletype absolute
zte(cfg-snmp)#set alarm 2 startup rising
zte(cfg-snmp)#set alarm 2 threshold 8 eventindex 2 rising
zte(cfg-snmp)#set alarm 2 threshold 15 eventindex 2 falling
zte(cfg-snmp)#set alarm 2 owner zteNj
zte(cfg-snmp)#set alarm 2 status valid

zte(cfg-snmp)#set statistics 1 datasource 6
zte(cfg-snmp)#set statistics 1 owner zteNj
zte(cfg-snmp)#set statistics 1 status valid
```

查看事件组 2 的配置信息：

```
zte(cfg-snmp)#show event 2
  EventIndex  : 2           Type  : logAndTrap
  Community   : public       Status: valid
  Owner       : zteNj
  Description : It'sJustForTest!!
zte(cfg-snmp)#
```

查看历史组 2 的配置信息：

```
zte(cfg-snmp)#show history 2
  ControlIndex : 2             BucketsRequest: 3
  Interval     : 10            BucketsGranted: 3
  ControlStatus: valid          ControlOwner  : zteNj
  DataSource   : 1.3.6.1.2.1.2.2.1.1.6
zte(cfg-snmp)#
```

查看告警组 2 的配置信息：

```
zte(cfg-snmp)#show alarm 2
  AlarmIndex   : 2          SampleType: absolute
  Interval     : 10         Value     : 0
  Threshold(R) : 8          Startup   : risingAlarm
  Threshold(F) : 15         Status    : valid
  EventIndex(R): 2          Variable  : 1.3.6.1.2.1.2.2.1.1.6
  EventIndex(F): 2          Owner     : zteNj
zte(cfg-snmp)#
```

查看统计组 1 的配置信息：

```
zte(cfg-snmp)#show statistics 1
  StatsIndex: 1
  DropEvents    : 0         BroadcastPkts      : 0
  Octets        : 0         MulticastPkts      : 0
  Pkts          : 0         Pkts64Octets       : 0
  Fragments     : 0         Pkts65to127Octets  : 0
  Jabbers       : 0         Pkts128to255Octets : 0
  Collisions    : 0         Pkts256to511Octets : 0
  CRCAlignErrors: 0         Pkts512to1023Octets : 0
  UndersizePkts : 0         Pkts1024to1518Octets: 0
  OversizePkts  : 0         DataSource(port)  : 1.3.6.1.2.1.2.2.1.1.6
  Status        : valid     Owner             : zteNj
zte(cfg-snmp)#
```

上述配置后，当端口 6 第 1 个 bucket 的 etherHistoryPkts 包个数在上升超过 8 或下降低于 15 时，都会触发索引为 2 的事件。索引为 2 的事件会发一个 trap 给管理站，同时创建一个 log 实例记录日志，该日志可以在 event 组的 logTable 中查看到。

8.5 集群管理

8.5.1 概述

集群是在某特定的广播域内，由一组交换机组成的一个集合。这组交换机构成一个统一的管理域，对外提供一个公网 IP 地址和一个管理接口，并提供了对集群中每个成员的管理和访问能力。

配置公网 IP 地址的管理交换机称为命令交换机，其它被管理的交换机称为成员交换机。一般情况下成员交换机不配置公网 IP 地址，它利用命令交换机的类 DHCP 功能来分配一个私有地址，命令交换机和成员交换机共同组成集群（私网）。

一个集群所处的广播域一般由四种角色的交换机组成：命令交换机、成员交换机、候选交换机、独立交换机。

一个集群中有且仅有一台命令交换机，命令交换机可以自动收集设备拓扑，并建立集群。集群建立后，命令交换机提供了一个对集群的管理通道，对成员交换机进行管理。成员交换机在加入集群之前为候选交换机，不支持集群管理的交换机称为独立交换机。

集群管理的组网如 图 8.5-1所示。

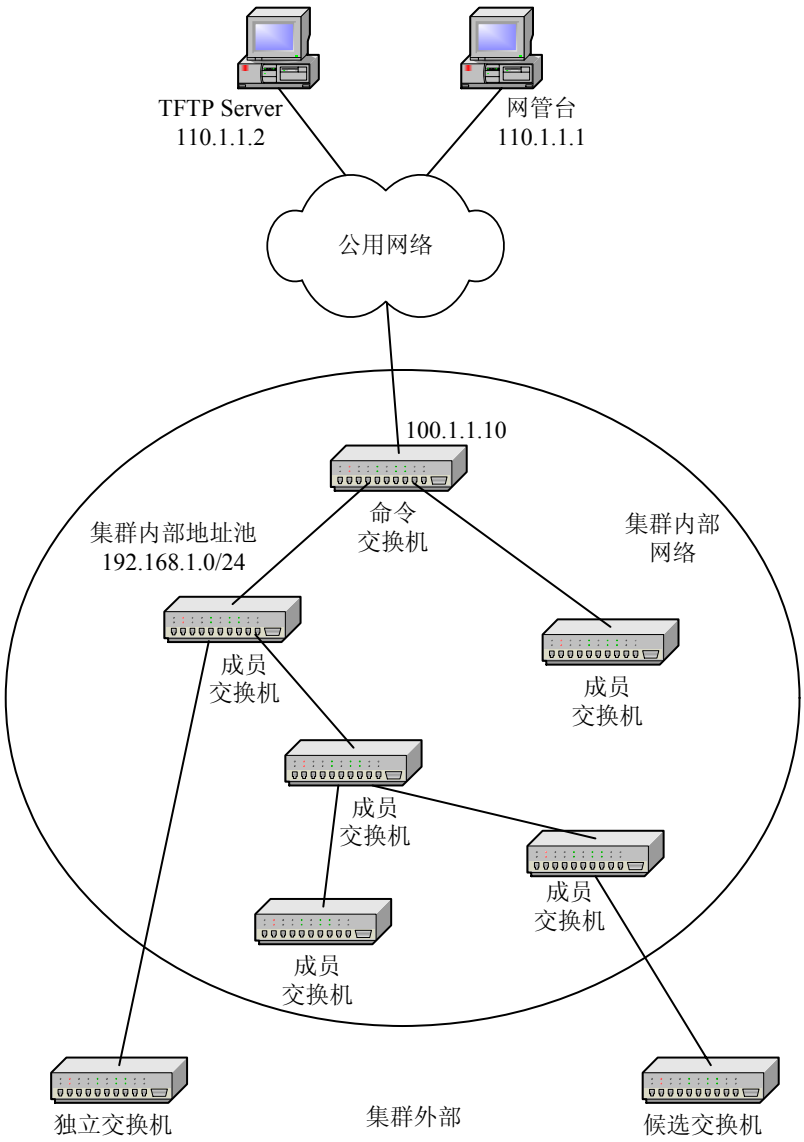


图8.5-1 集群管理组网图

建议在命令交换机上完成公网和私网之间广播域的隔离，屏蔽对私有地址的直接访问，由命令交换机对外提供一个管理维护通道，对集群进行集中、统一的管理。

集群中四种角色的交换机的切换规则如 图 8.5-2所示。

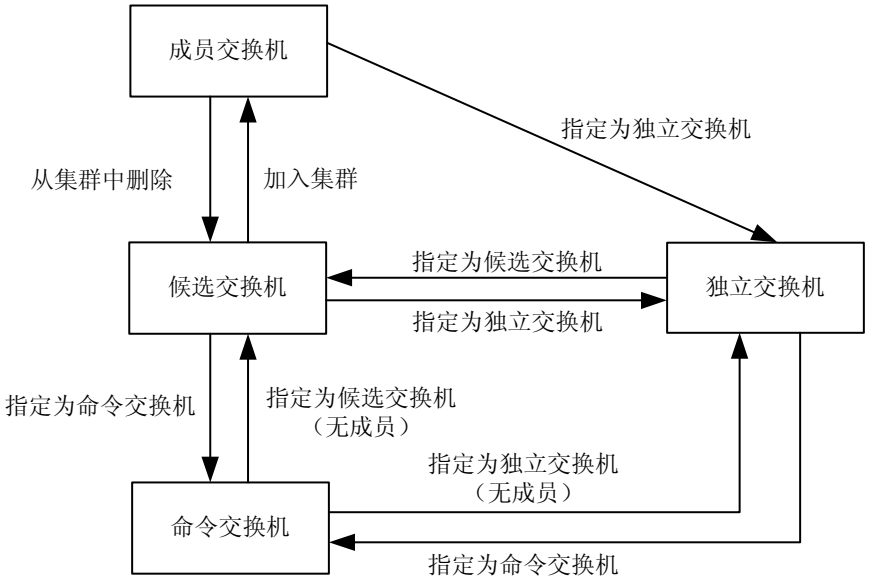


图8.5-2　交换机角色切换规则

配置集群管理功能首先必须使用 **config group** 命令进入集群管理配置模式。

8.5.2 ZDP 配置

ZDP（Discovery Protocol）是用来发现直接邻居节点相关信息的协议，包括邻接设备的 ID、设备类型、版本、端口等信息，支持邻居设备信息表的刷新与老化。

在交换机上配置 ZDP 包括以下内容。

1. 使能/关闭系统 ZDP 功能

   set zdp {**enable**|**disable**}

   系统 ZDP 功能缺省处于使能状态。当系统 ZDP 功能关闭时，将清除交换机邻居设备信息表的内容，停止处理 ZDP 报文。

2. 使能/关闭 port 的 ZDP 功能

   set zdp port <*portlist*> {**enable**|**disable**}

3. 使能/关闭 trunk 的 ZDP 功能

set zdp trunk <*trunklist*> {**enable**|**disable**}

所有端口/trunk 的 ZDP 功能缺省处于使能状态。当端口/trunk 的 ZDP 功能关闭时，将清除该端口/trunk 邻居设备信息表的内容，并停止处理 ZDP 报文。

说明：

只有在端口/trunk 的 ZDP 功能和系统的 ZDP 功能均使能的情况下，端口/trunk 才能正常进行 ZDP 信息的收集和发送。

4. 配置 ZDP 信息的有效保留时间

set zdp holdtime <*10-255*>

说明：

ZDP 的 holdtime 设置值需要大于 timer 设置值，建议设置为 timer 的 3 倍。

5. 配置 ZDP 报文发送时间间隔

set zdp timer <*5-255*>

6. 显示 ZDP 配置

show zdp

7. 显示邻居设备信息表

show zdp neighbour [**detail**]

8.5.3 ZTP 配置

ZTP（Topology Protocol）是用于收集网络拓扑信息的的协议，它利用 ZDP 收集到的邻居设备信息表，在指定 VLAN 的相关端口发送和转发 ZTP 拓扑收集报文，收集一定范围网络（跳数）内的拓扑信息，建立拓扑信息表，用于了解网络拓扑状态和集群管理。

在交换机上配置 ZTP 包括以下内容。

1. 使能/关闭系统 ZTP 功能

set ztp {**enable**|**disable**}

系统 ZTP 功能缺省处于使能状态。当系统 ZTP 功能关闭时，将清除交换机拓扑信息表的内容，停止处理 ZTP 报文。

2. 使能/关闭 port 的 ZTP 功能

set ztp port <*portlist*> {**enable|disable**}

3. 使能/关闭 trunk 的 ZTP 功能

set ztp trunk <*trunklsit*> {**enable|disable**}

所有端口/trunk 的 ZTP 功能缺省处于使能状态。当端口/trunk 的 ZTP 功能关闭时，将停止处理该端口/trunk 的 ZTP 报文。

说明：

只有在端口/trunk 的 ZTP 功能和系统的 ZTP 功能均使能的情况下，端口/trunk 才能正常进行 ZTP 报文的处理。

4. 配置 ZTP 参数

- 配置拓扑收集的指定 VLAN

  set ztp vlan *<1-4094>*

- 配置拓扑收集的范围（跳数）

  set ztp hop <*1-128*>

- 配置定时拓扑收集时间间隔

  set ztp timer <*0-60*>

- 配置拓扑请求转发的跳延迟时间

  set ztp hopdelay <*1-1000*>

- 配置拓扑请求转发的端口延迟时间

  set ztp portdelay <*1-100*>

  拓扑收集的指定 VLAN 缺省是 VLAN 1，拓扑收集范围是 4 跳。定时拓扑收集的时间间隔缺省是 0 分钟，即不进行定时拓扑收集。

  当配置交换机为命令交换机时，拓扑收集的 VLAN 用于命令交换机的管理 VLAN，此时不允许更改拓扑收集的指定 VLAN。

当网络的延迟比较大时，需更改拓扑转发的跳延迟和端口延迟时间以适应当前网络的状态。

当管理员想收集更大范围的网络拓扑信息时，可以增大收集跳数。

5. 手动启动拓扑收集

ztp start

为了便于用户随时了解网络的拓扑信息，用户可以手动启动拓扑收集过程，不需要依赖于定时的拓扑收集。

6. 显示 ZTP 配置

show ztp

7. 根据 MAC 地址显示指定设备的详细信息

show ztp mac <*xx.xx.xx*>

8. 显示拓扑信息表的信息

show ztp device [<*idlist*>]

说明：

拓扑信息表所提供的设备 id，是根据本次拓扑收集结果生成的临时标识，目的是为了方便显示和集群管理，只对本次拓扑收集结果有效。

8.5.4 集群配置

命令交换机被指定后，通过 ZDP/ZTP 了解网络的拓扑信息，从而进行集群的管理和监控。

集群的唯一标识由集群所处的 VLAN 和命令交换机的 MAC 地址两项构成。

1. 设置交换机的角色

- 设置交换机为候选交换机

set group candidate

- 设置交换机为独立交换机

set group independent

- 设定交换机为命令交换机，指定用于集群管理的三层端口号，并设定用户集群管理的 IP 地址池

  set group commander ipport <*0-63*> **ip-pool** < *A.B.C.D/M* >

  当候选交换机被命令交换机加入集群成为成员交换机后，不允许将自身更改为候选交换机或是命令交换机。

  设置命令交换机时三层端口所绑定的 VLAN 是拓扑收集的指定 VLAN，交换机一旦被配置成命令交换机，不允许更改拓扑收集的指定 VLAN。

  只有当集群中没有成员交换机时，命令交换机才允许被设置成为候选交换机或独立交换机。

2. 增加/删除集群成员

- 以设备 MAC 地址增加成员

  set group add mac <*xx.xx.xx*>

- 以设备 MAC 地址增加成员，并指定成员的 id 号

  set group add mac <*xx.xx.xx*> <*1-255*>

- 以拓扑收集到的设备临时 id 号增加成员

  set group add device <*idlist*>

- 从集群中删除指定成员 id 的设备

  set group delete member <*idlist*>

  当将设备加入到集群但不指定成员的 id 号时，系统会自动为该成员分配一个唯一的 id 标识。

3. 配置集群的参数

- 设置集群名称

  set group name <*name*>

- 设置命令交换机与成员交换机的握手时间间隔

  set group handtime <*1-300*>

- 设置集群的交换机信息的有效保留时间

  set group holdtime <*1-300*>

- 设置集群的内部公用 SYSLOG Server 的 IP 地址

set group syslogsvr < *A.B.C.D* >

如果配置了集群的 SYSLOG Server 的 IP 地址，则在成员交换机上如果开启了 syslog 功能，成员机会将 syslog 报文发送到命令交换机，命令交换机再将此报文转发到指定的 SYSLOG Server 上。

- 设置集群的内部公用 TFTP Server 的 IP 地址

  set group tftpsvr < *A.B.C.D* >

  以上参数只允许在命令交换机进行配置。

  集群的有效保留时间是指当命令交换机检测到成员交换机（或成员交换机检测到命令交换机）通讯故障时，如果在有效保留时间内恢复通讯，成员状态正常；如果经历了有效保留时间后，通讯没有恢复，则在命令交换机上显示该成员为 DOWN 状态，等通讯恢复后，成员会自动加入到集群，显示为 UP 状态。

  如果配置了集群的 TFTP Server 的 IP 地址，则在成员交换机上可以通过直接访问命令交换机达到访问 TFTP Server 的目的。

4. 集群成员的访问与控制

- 从命令交换机切换到指定的成员交换机

  rlogin member <*1-255*>

- 从成员交换机切换到命令交换机

  rlogin commander

- 利用命令交换机进行 TFTP 下载/上载版本

  tftp commander {**download**|**upload**} <*name*>

- 保存指定成员交换机的配置

  save member {<*idlist*>|**all**}

- 删除指定成员交换机的配置

  erase member {<*idlist*>|**all**}

- 重启指定的成员交换机

  reboot member {<*idlist*>|**all**}

5. 显示集群的配置和集群成员信息

- 显示集群配置信息

  show group

- 显示能够加入集群的候选交换机信息

  show group candidate

- 显示集群成员的信息

  show group member [<*1-255*>]

8.5.5 配置实例

如 图 8.5-1所示，初始时各交换机使用缺省配置，要求配置集群的命令交换机的公网地址所处的VLAN为 2525，IP地址为 100.1.1.10/24，网关为 100.1.1.1，集群的管理VLAN为 4000，私有地址池为 192.168.1.0/24，整个集群的TFTP Server的IP地址为 110.1.1.2。

具体配置如下：

1. 配置命令交换机的公网 IP 地址和网关

```
WYXX(cfg)#set vlan 2525 enable
WYXX(cfg)#set vlan 2525 add port 1-8 tag

WYXX(cfg)#config router
WYXX(cfg-router)#set ipport 25 ipaddress 100.1.1.10/24
WYXX(cfg-router)#set ipport 25 vlan 2525
WYXX(cfg-router)#set ipport 25 enable

WYXX(cfg-router)#iproute 0.0.0.0/0 100.1.1.1
```

2. 在命令交换机的三层端口 1、VLAN 1（缺省 VLAN）上建立集群

```
WYXX(cfg)#config group
WYXX(cfg-group)#set group commander ipport 1 ip-pool 192.168.1.1/24

Cmdr.WYXX(cfg-group)#ztp start
Cmdr.WYXX(cfg-group)#show ztp device
  Last collection vlan : 1
  Last collection time : 188 ms
   Id  MacAddress        Hop   Role  Platform
  ---  ----------------- ---  -----  ---------
    0  00.d0.d0.fc.08.6c    0  cmdr   ZXR10 5009
    1  00.d0.d0.fc.08.d6    1  candi  ZXR10 5009
```

```
   2  00.d0.d0.fc.08.cf    1  candi  ZXR10 5009
   3  00.d0.d0.fc.08.fa    1  candi  ZXR10 5009
   4  00.d0.d0.fc.08.d5    1  candi  ZXR10 5009
   5  00.d0.d0.fc.09.3a    1  candi  ZXR10 5009

Cmdr.WYXX(cfg-group)#set group add device 1-5
  Adding device id : 1   ...  Successed to add member!
  Adding device id : 2   ...  Successed to add member!
  Adding device id : 3   ...  Successed to add member!
  Adding device id : 4   ...  Successed to add member!
  Adding device id : 5   ...  Successed to add member!

Cmdr.WYXX(cfg-group)#show group member
  MbrId MacAddress       IpAddress          Status
  ----- ---------------- ------------------ ----------
  1     00.d0.d0.fc.08.d6 192.168.1.2/24     Up
  2     00.d0.d0.fc.08.cf 192.168.1.3/24     Up
  3     00.d0.d0.fc.08.fa 192.168.1.4/24     Up
  4     00.d0.d0.fc.08.d5 192.168.1.5/24     Up
  5     00.d0.d0.fc.09.3a 192.168.1.6/24     Up
```

3. 切换到各成员机上，将所有端口加入到 VLAN 4000（以成员 4 为例）

```
Cmdr.WYXX(cfg)#set vlan 4000 enable
Cmdr.WYXX(cfg)#set vlan 4000 add port 1-8 tag

Cmdr.WYXX(cfg)#rlogin member 4
  Trying  ...Open
  Connecting ...

Membr_4.zte>enable

Membr_4.zte(cfg)#set vlan 4000 enable
Membr_4.zte(cfg)#set vlan 4000 add port 1-8 tag
```

4. 解散在 VLAN 1 上建立的集群

```
Cmdr.WYXX(cfg-group)#set group delete member 1-5
  Deleting member id : 1   ...  Successed to del member!
  Deleting member id : 2   ...  Successed to del member!
  Deleting member id : 3   ...  Successed to del member!
  Deleting member id : 4   ...  Successed to del member!
  Deleting member id : 5   ...  Successed to del member!
```

```
Cmdr.WYXX(cfg-group)#set group candidate
WYXX(cfg-group)#
```

5. 在 VLAN 4000 上建立的集群

```
WYXX(cfg-group)#set ztp vlan 4000

WYXX(cfg-group)#set group commander ipport 1 ip-pool 192.168.1.1/24

Cmdr.WYXX(cfg-group)#ztp start
Cmdr.WYXX(cfg-group)#show ztp device
  Last collection vlan : 4000
  Last collection time : 176 ms
   Id  MacAddress        Hop   Role  Platform
  ---  ----------------- ---  -----  ---------
    0  00.d0.d0.fc.08.6c   0  cmdr   ZXR10 2818S
    1  00.d0.d0.fc.08.d6   1  candi  ZXR10 2818S
    2  00.d0.d0.fc.08.cf   1  candi  ZXR10 2818S
    3  00.d0.d0.fc.08.fa   1  candi  ZXR10 2818S
    4  00.d0.d0.fc.08.d5   1  candi  ZXR10 2818S
    5  00.d0.d0.fc.09.3a   1  candi  ZXR10 2818S

Cmdr.WYXX(cfg-group)#set group add device 1-5
  Adding device id : 1   ...  Successed to add member!
  Adding device id : 2   ...  Successed to add member!
  Adding device id : 3   ...  Successed to add member!
  Adding device id : 4   ...  Successed to add member!
  Adding device id : 5   ...  Successed to add member!

Cmdr.WYXX(cfg-group)#show group member
  MbrId MacAddress       IpAddress         Status
  ----- ---------------- ----------------- ----------
  1     00.d0.d0.fc.08.d6 192.168.1.2/24     Up
  2     00.d0.d0.fc.08.cf 192.168.1.3/24     Up
  3     00.d0.d0.fc.08.fa 192.168.1.4/24     Up
  4     00.d0.d0.fc.08.d5 192.168.1.5/24     Up
  5     00.d0.d0.fc.09.3a 192.168.1.6/24     Up
```

6. 配置集群 TFTP Server 的 IP 地址为 110.1.1.2

```
Cmdr.WYXX(cfg-group)#set group tftpsvr 110.1.1.2
```

7. 在成员 4 上下载版本 kernel.Z

```
Membr_4.zte(cfg-tffs)#tftp commander download kernel.Z
```

8.6 WEB

8.6.1 概述

ZXR10 5009 提供一个存储于闪存内的嵌入式 Web 服务器，允许用户通过网络使用一个标准的 Web 浏览器（推荐 IE4.0 以上版本、1024×768 分辨率）远程管理交换机。

8.6.2 系统登录

在交换机已配置了WEB连接（参见 5.1.4）的条件下：

1. 打开 Microsoft Internet Explore。
2. 在浏览器URL中输入交换机的IP地址（该地址是交换机可以连接的地址），按<Enter>键，打开系统登录界面。如 图 8.6-1所示。

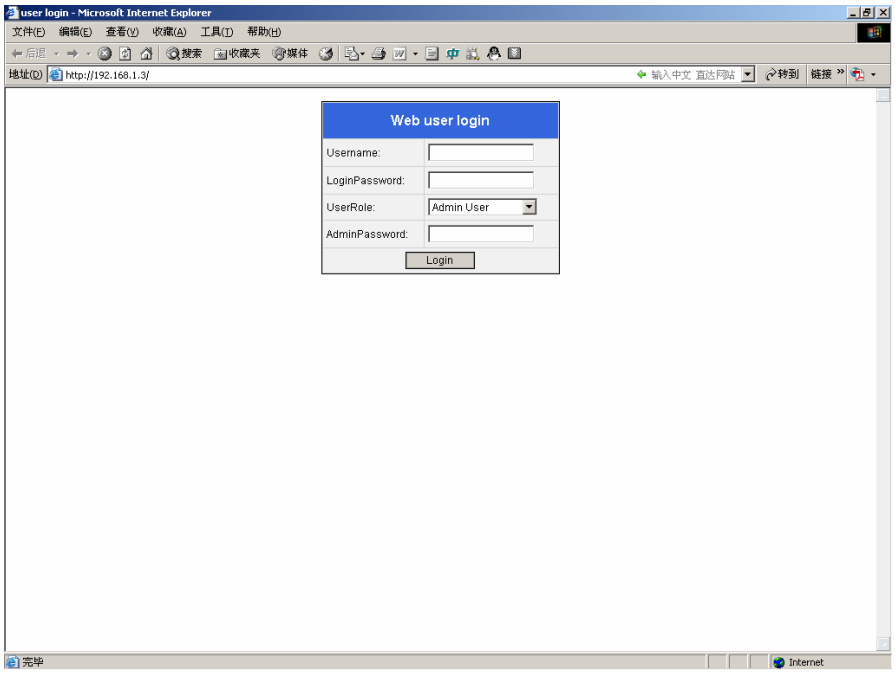


图8.6-1 系统登录界面

3. 输入合法的用户名和密码，选择用户权限，一般用户不需要管理密码，管理用户需要管理密码；单击<Login>按钮，登录到系统主页面，如 图 8.6-2 所示。

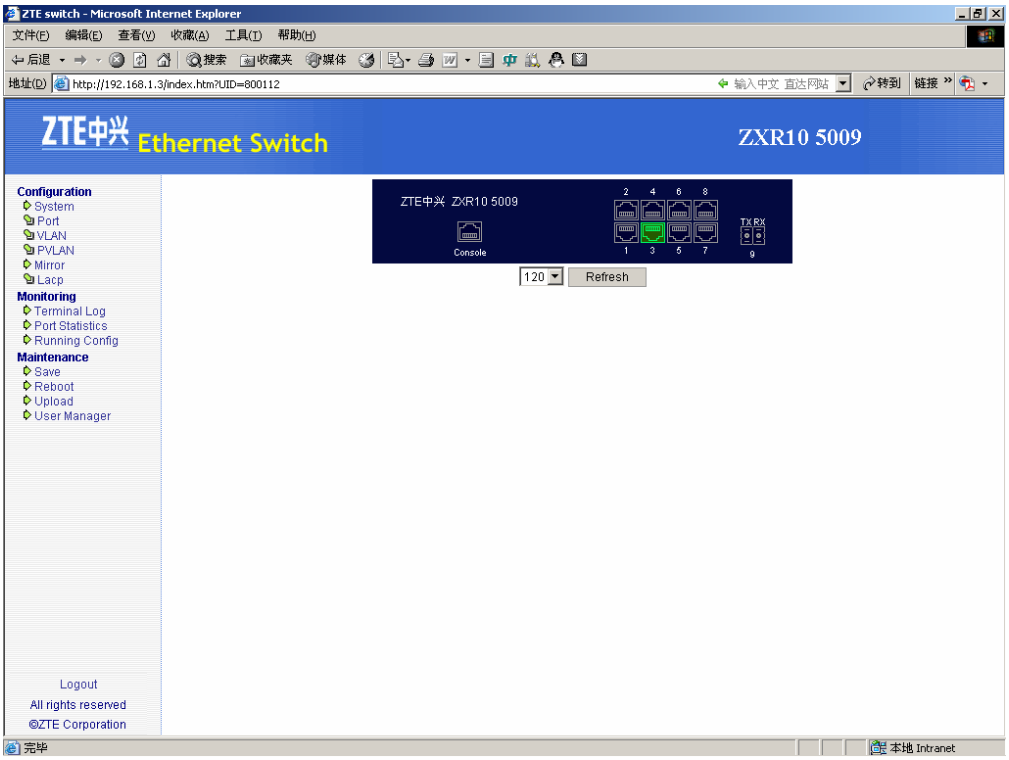


图8.6-2　系统主页面

8.6.3 配置管理

8.6.3.1 系统信息

点击系统主页面中左侧目录树[Configuration→System]，打开系统信息页面（Configuration目录默认是展开的），如图 8.6-3所示。

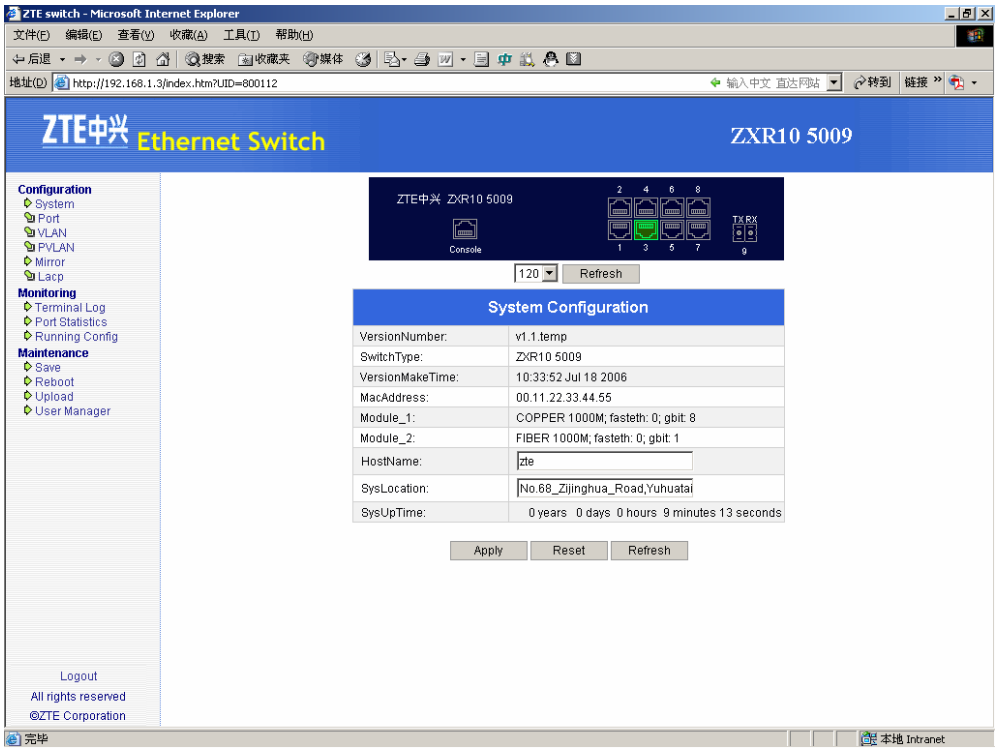


图8.6-3 系统信息页面

该页面显示了以下系统信息：

- [VersionNumber]：版本号
- [SwitchType]：交换机型号
- [VersionMakeTime]：版本制作时间
- [MacAddress]：交换机硬件地址
- [Module_1]：扩展卡 1 的信息
- [Module_2]：扩展卡 2 的信息
- [HostName]：系统名
- [SysLocation]：系统位置
- [SysUpTime]：系统启动后运行时间

其中“HostName”和“SysLocation”两个参数可以设置。设置后，单击<Apply>按钮提交，完成配置。

8.6.3.2 端口管理

1. 点击主页面中左侧目录树[Configuration→Port→Port State]，打开端口状态信息页面，如 图 8.6-4所示。

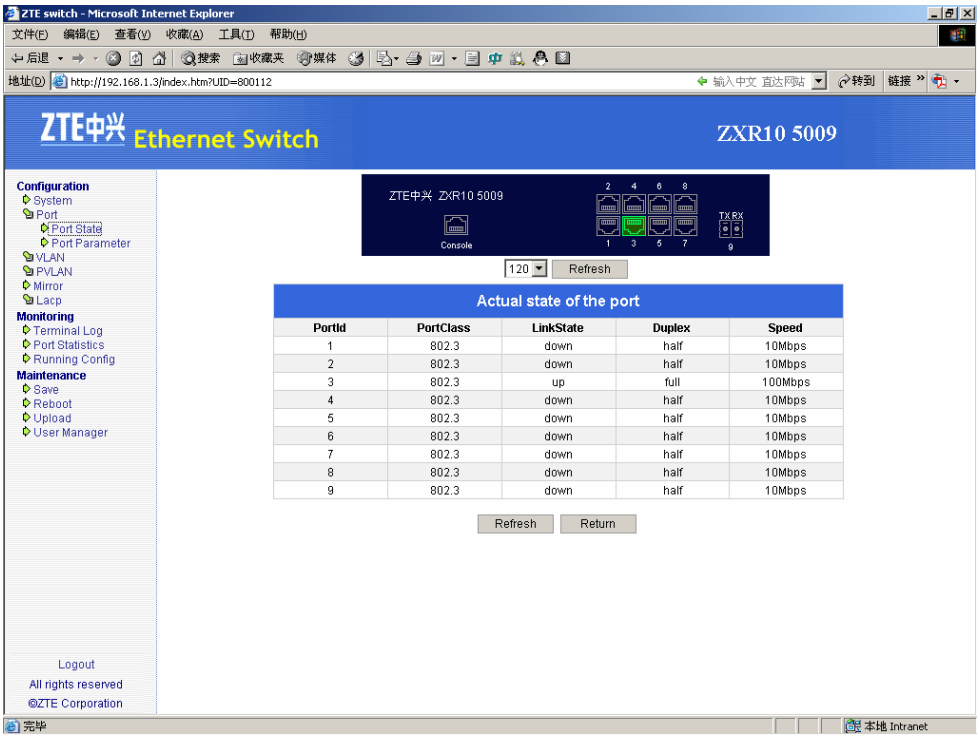


图8.6-4　端口状态信息页面

该页面显示了端口的以下信息：

- [PortClass]：端口类型
- [LinkState]：端口 linkup|linkdown 状态
- [Duplex]：端口工作双工状态
- [Speed]：端口工作速率

说明：

当端口 linkdown 时，“Duplex”和“Speed”项是没有意义的。

2. 点击主页面中左侧目录树[Configuration→Port→Port Parameter]，打开端口配置信息页面，如 图 8.6-5所示。

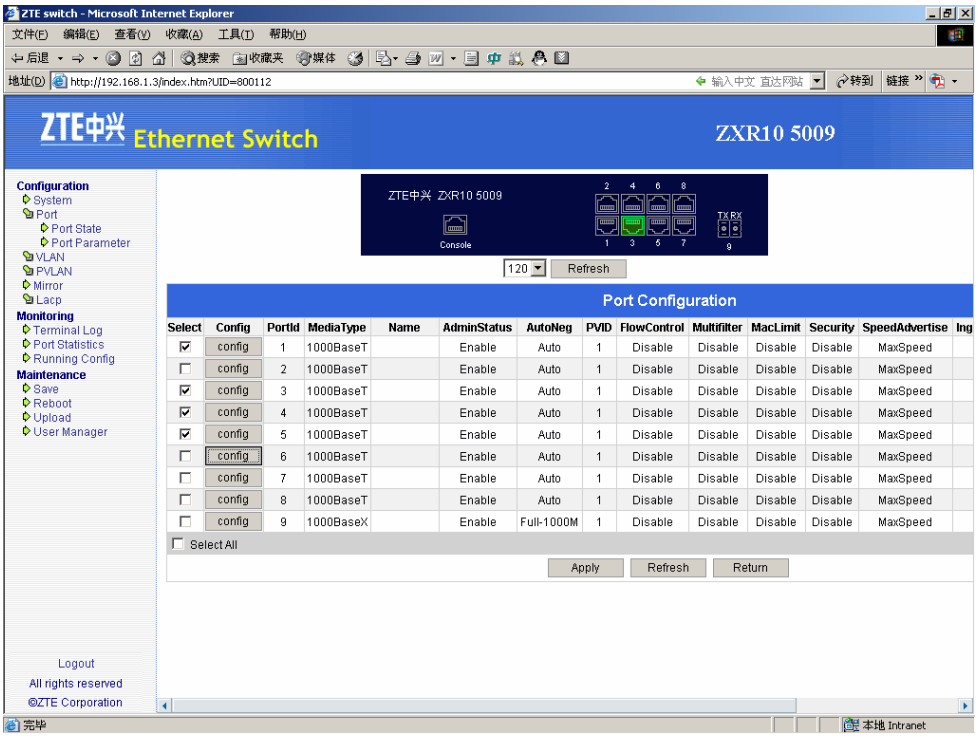


图8.6-5 端口配置信息页面

该页面显示了端口的以下信息（具体含义请参见 7.1.1节）：

- [MediaType]：端口介质类型
- [PortName]：端口名字
- [AdminStaus]：端口使能
- [AutoNeg]：端口工作模式，即工作速率和双工模式
- [PVID]：端口缺省 VLAN ID
- [FlowControl]：端口流控使能
- [MultiFilter]：端口组播过滤使能
- [MacLimit]：端口 Mac 地址学习限制
- [Security]：端口安全使能
- [SpeedAdvertise]：端口速率宣称
- [IngressType]：端口入向带宽限制类型
- [IngressRate]：端口入向带宽

- [EgressRate]：端口出向带宽

3. 单个端口配置：在端口配置信息页面列表中单击要配置端口行中的<Config>按钮，打开此端口的配置页面，如 图 8.6-6所示。

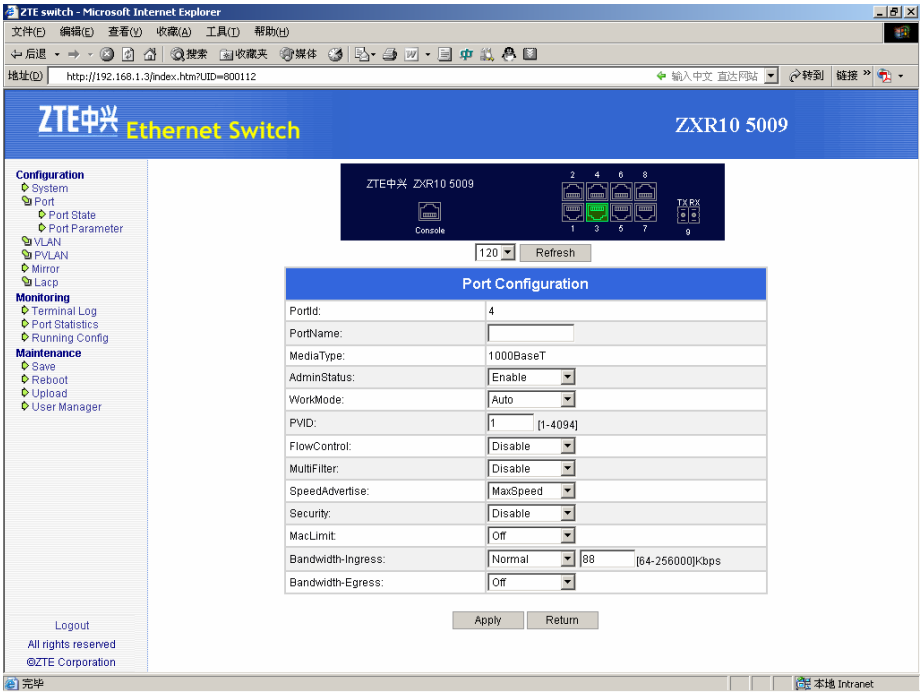


图8.6-6　单端口配置页面

在该页面可以对选中端口某（些）项属性进行设置；设置完成，单击<Apply>按钮提交，完成配置。

说明：

由于“Security”和“MacLimit”两项属性互相冲突，故不能同时设置为使能。

小心：

对与网管主机相连的端口进行配置时要小心！如：将此端口关闭，则网管中断。

4. 批量端口配置：在端口配置信息页面列表中选中多个端口（选中[Select All]则选择所有端口），然后单击<Apply>按钮，打开端口批量配置页面，如 图 8.6-7所示。

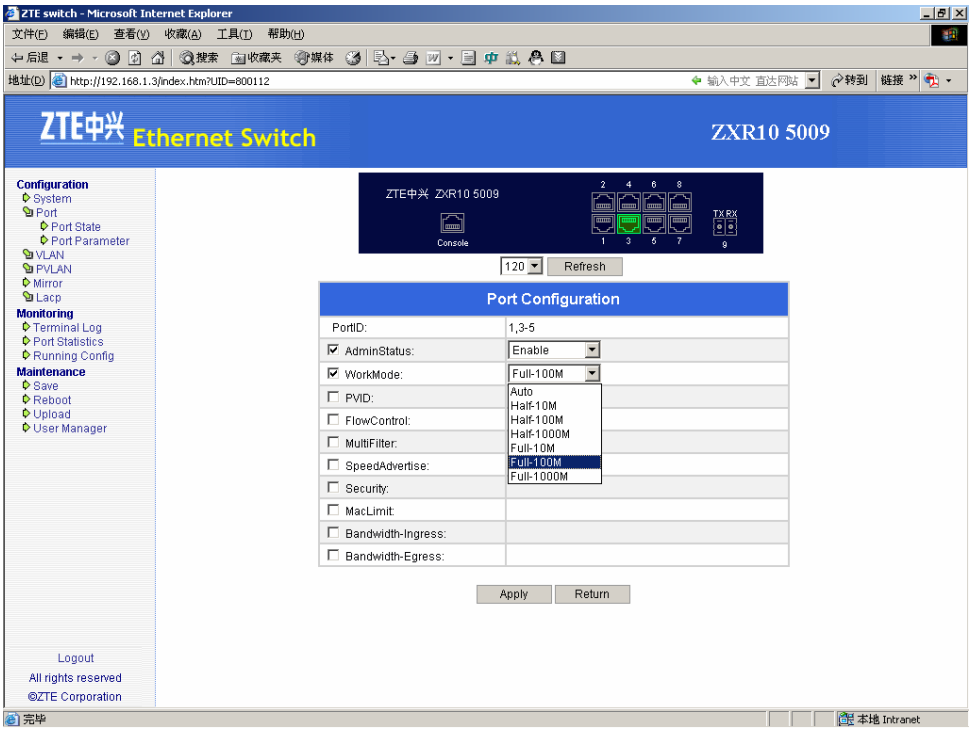


图8.6-7 端口批量配置页面

在该页面中点击属性前的复选框以选中要配置的属性进行设置，然后单击<Apply>按钮提交，完成配置。

8.6.3.3 VLAN 管理

1. 点击主页面中左侧目录树[Configuration→VLAN→Vlan Overview]，打开VLAN信息页面，显示最近被操作过的VLAN信息；若还没有对VLAN进行过操作，则显示缺省VLAN。如 图 8.6-8所示。

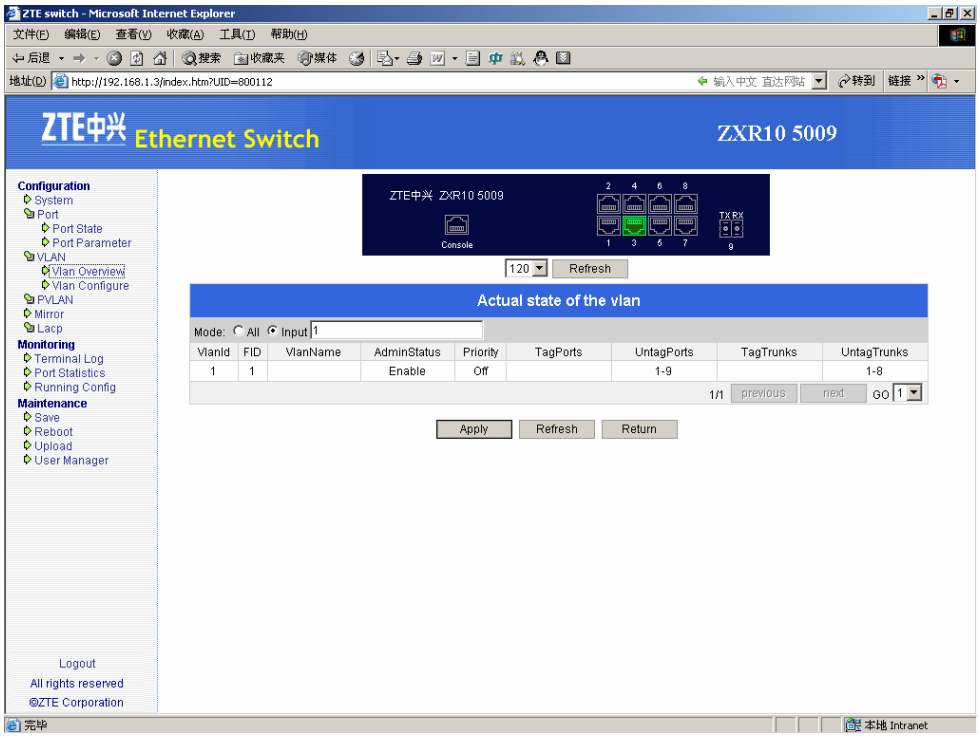


图8.6-8　VLAN 信息页面

该页面显示了VLAN的以下信息（具体含义请参见 7.3.2节）：

- [VlanName]：VLAN 名字
- [AdminStatus]：VLAN 使能
- [FID]：VLAN 的 FID
- [Priority]：VLAN 优先级
- [Tagged Ports]：VLAN 内打 tag 的端口
- [Untagged Ports]：VLAN 内不打 tag 的端口
- [Tagged Trunks]：VLAN 中打 tag 的 trunk
- [Untagged Trunks]：VLAN 中不打 tag 的 trunk

2. 查看特定 VLAN 信息：在 VLAN 信息页面中选中[Input]单选框，然后在其后的文本框中输入要查看的 VLAN 号，如“1,3-5”；或者选中[All]单选框。单击[Apply]按钮提交，即可得到相应的 VLAN 信息。当要显示的 VLAN 条目多于 20 时，会分页显示，页面右下角有页码提示；当页面多于一页时可以单击<previous>或<next>按钮进行上下页的切换，或者在[GO]下拉框中直接选择页码号。

3. 点击主页面中左侧目录树[Configuration→VLAN→Vlan Configure]，打开VLAN号输入页面，如 图 8.6-9所示。

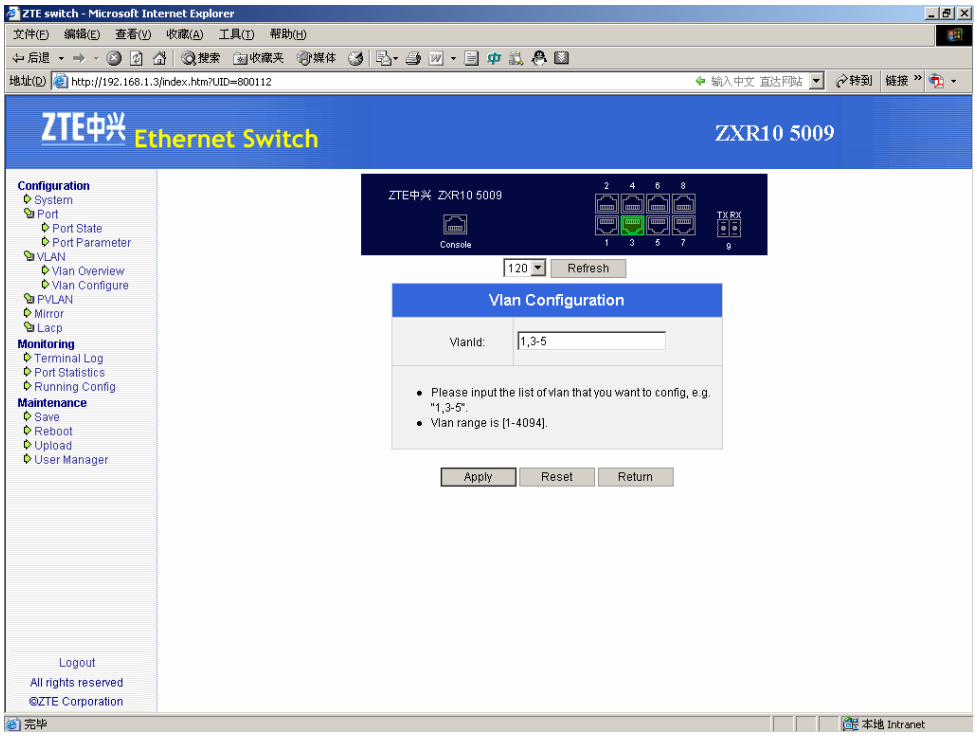


图8.6-9 VLAN 号输入页面

4. 在 VLAN 号页面中输入 VLAN 号（格式如“1,3-5”），单击<Apply>按钮，进入单 VLAN 配置或批量 VLAN 配置页面，依次描述如下：

- 单VLAN配置页面如 图 8.6-10所示。

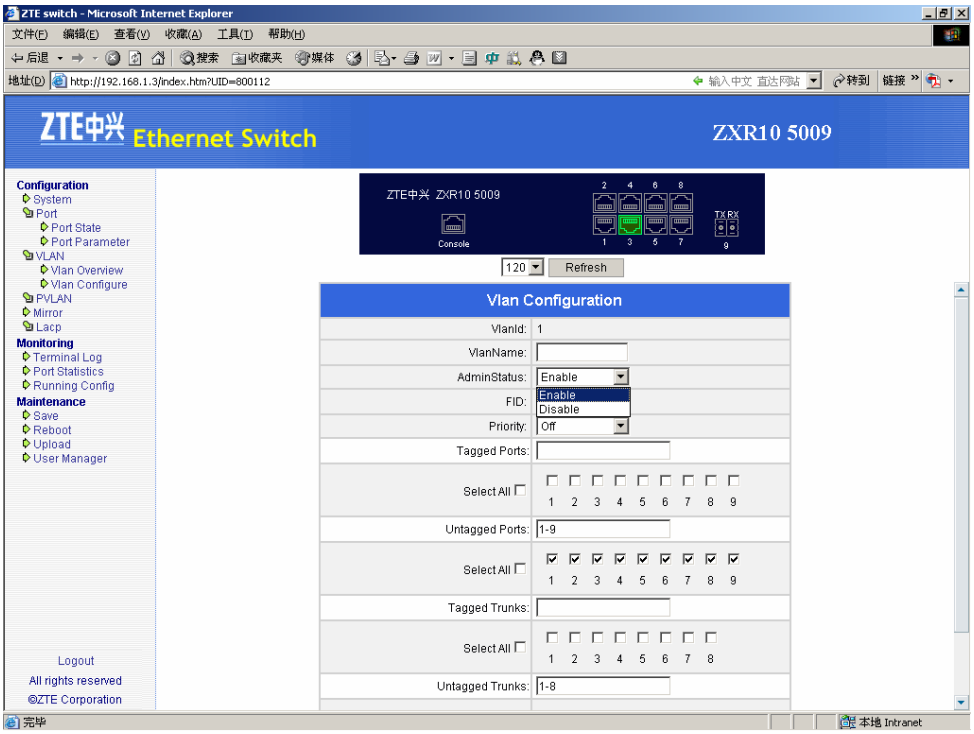


图8.6-10　单 VLAN 配置页面

在该页面中对 VLAN 的某（些）项属性进行设置后，单击<Apply>按钮提交，完成配置。

说明：

向 VLAN 中配置端口/Trunk 时，可以在其后的文本框中输入端口/Trunk 号，格式如“1,3-5”；也可以在对应的复选按钮中选择，要加入 VLAN 的选中即可。

- 批量VLAN配置如 图 8.6-11所示。

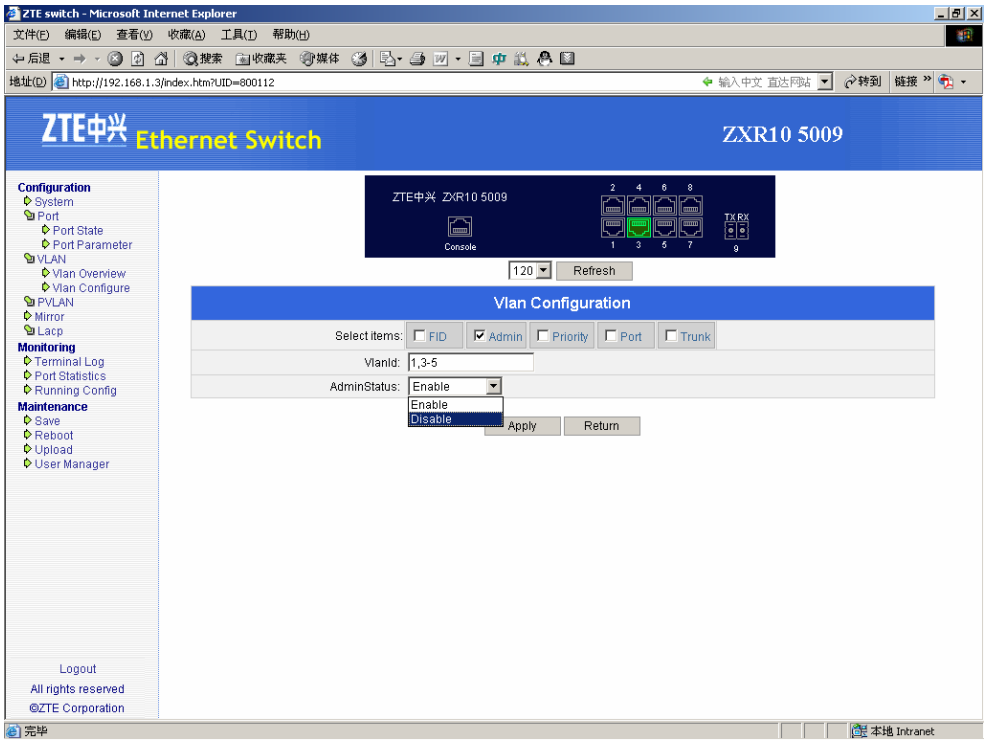


图8.6-11 批量 VLAN 配置页面

在该页面中选中并设置 VLAN 的某（些）项属性，，然后单击<Apply>按钮提交，完成配置。

8.6.3.4 PVLAN 管理

1． 点击主页面中左侧目录树[Configuration→PVLAN→Pvlan Overview]，打开打开PVLAN信息页面，如 图 8.6-12所示。

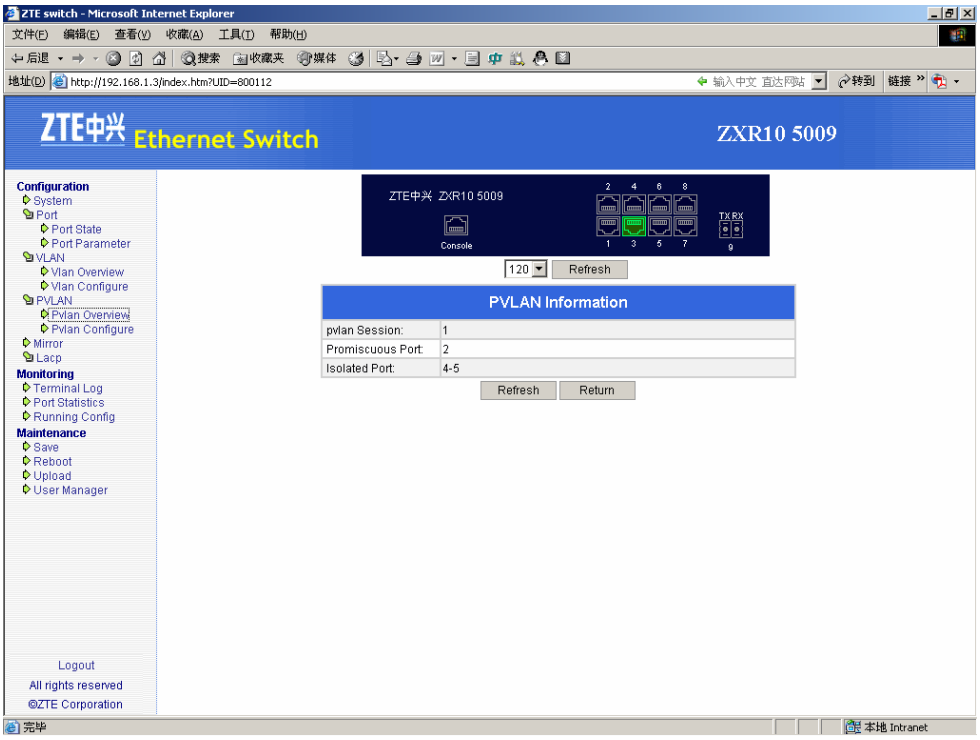


图8.6-12　PVLAN 信息页面

该页面显示了端口的以下信息：

- [pvlan Session]：pvlan 的实例
- [Promiscuous Port]：隔离端口
- [Isolated Port]：共享端口

2．点击主页面中左侧目录树[Configuration→PVLAN→Pvlan Configure]，打开打开PVLAN配置页面，如 图 8.6-13所示。

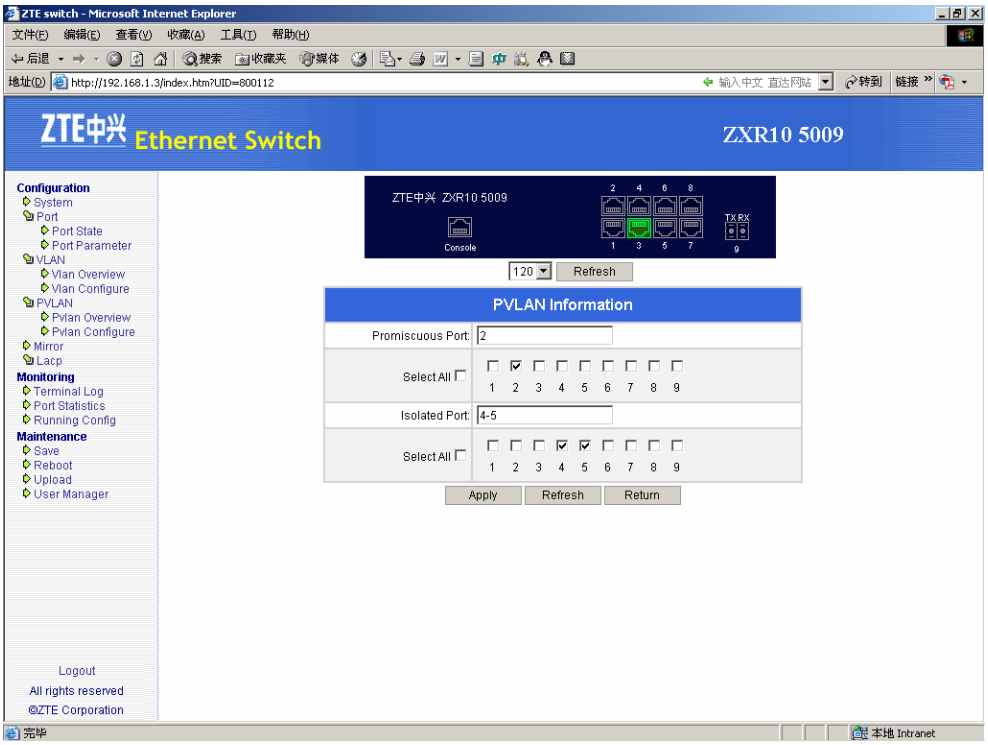


图8.6-13 Pvlan 配置页面

该页面显示了 PVLAN 的以下属性

- Promiscuous Port 隔离端口
- Isolated Port 共享端口

在该页面也可以对各属性进行设置，设置完成单击<Apply>按钮提交，系统配置成功后，显示配置后的信息页面。

8.6.3.5 端口镜像管理

1. 点击主页面中左侧目录树[Configuration→Mirror]，打开Mirror信息页面。如 图 8.6-14所示。

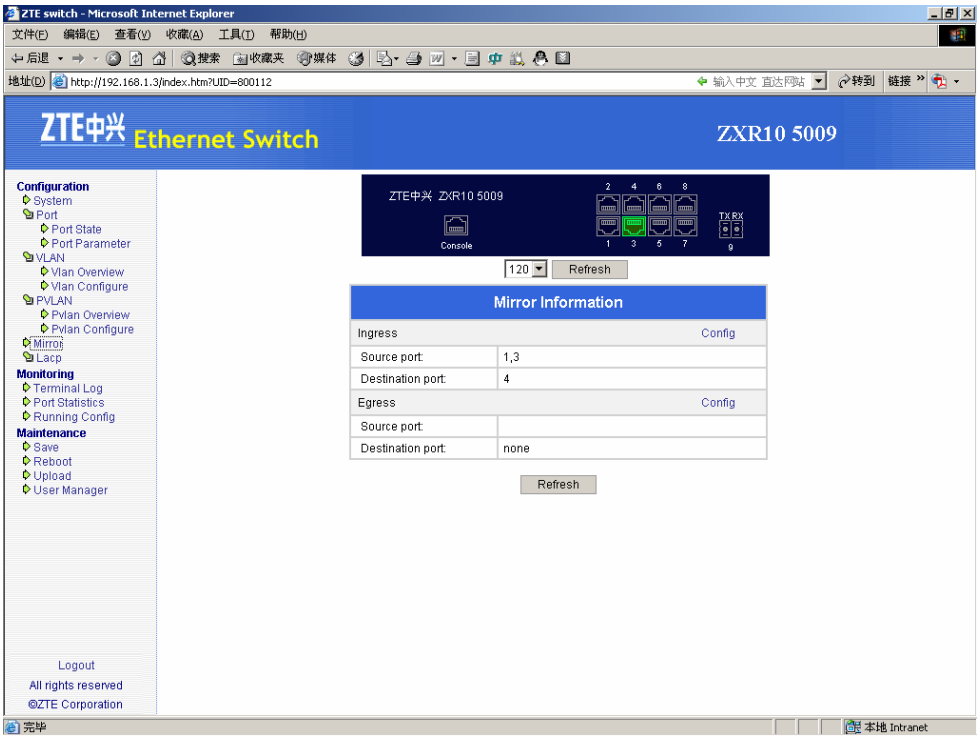


图8.6-14　Mirror 信息页面

该页面显示了端口镜像的以下信息（包括入向和出向）：

- [Source port]：镜像源端口
- [Destination port]：镜像目的端口

2. 单击Ingress栏右侧的<Config>链接，打开端口入向镜像配置页面。如 图8.6-15所示。

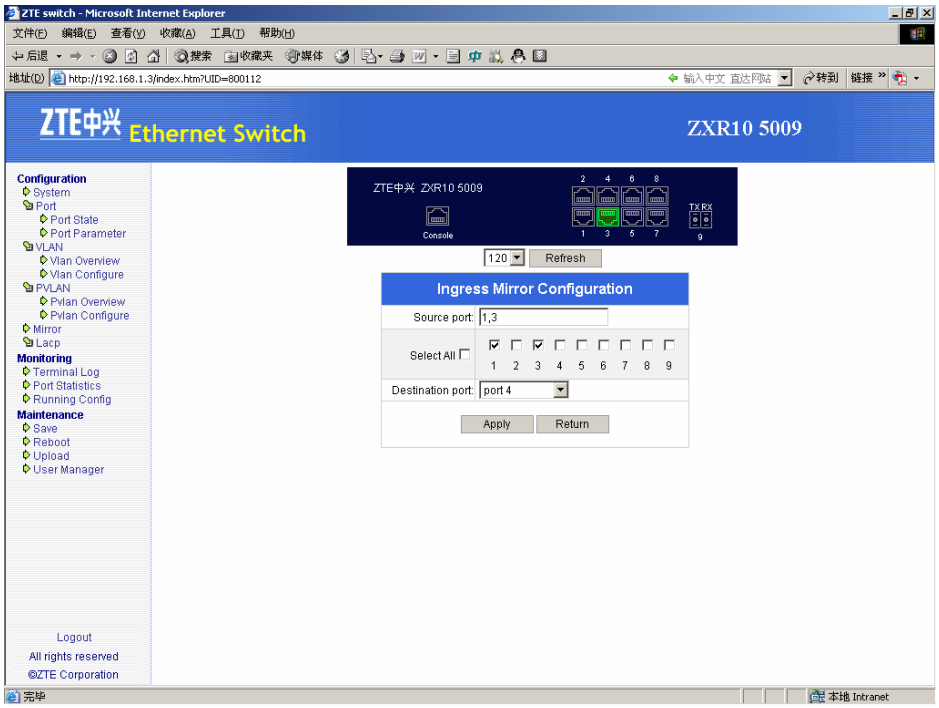


图8.6-15 端口入向镜像配置页面

在该页面可以对入向镜像目的端口和源端口进行设置，设置完成后单击<Apply>按钮提交，完成配置。

3. 单击Egress栏右侧的<Config>链接，打开端口出向镜像配置页面，如 图8.6-16所示。

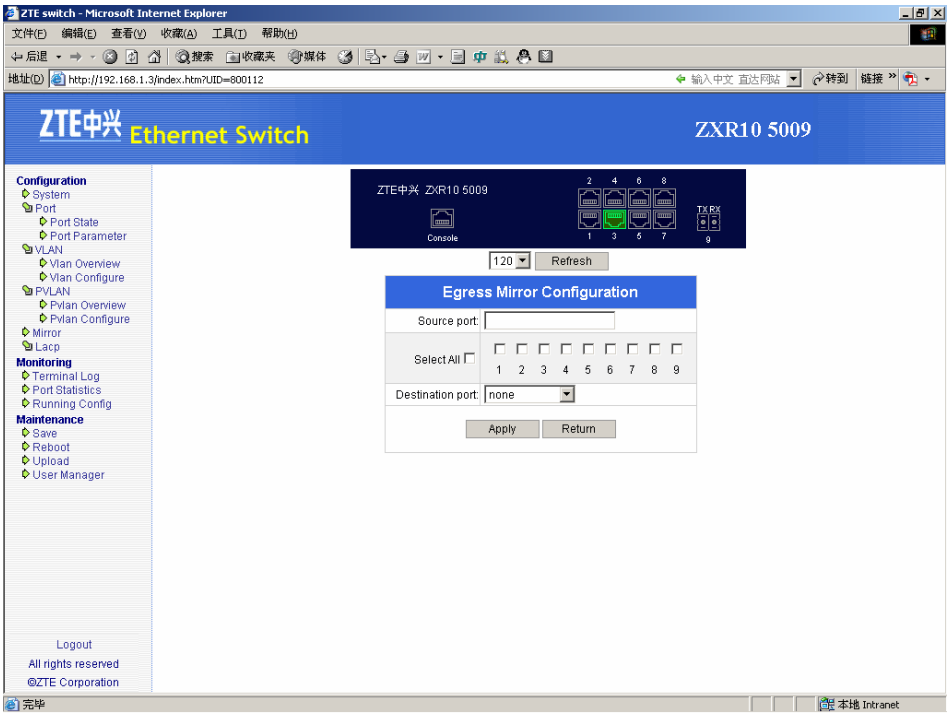


图8.6-16　端口出向镜像配置页面

在该页面可以对出向镜像目的端口和源端口进行设置，设置完成后单击<Apply>按钮提交，完成配置。

8.6.3.6 LACP 管理

1．点击主页面中左侧目录树[Configuration→Lacp→Lacp Port]，打开Lacp基本信息页面，如 图 8.6-17所示。

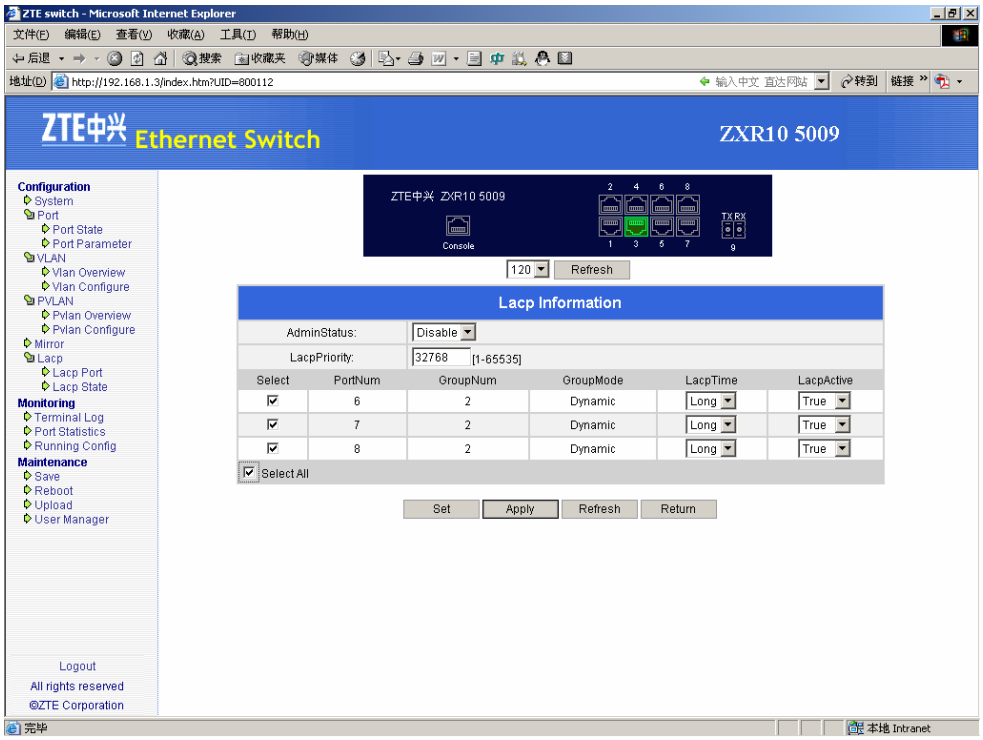


图8.6-17 Lacp 基本属性页面

该页面信息（具体含义请参见 7.5.2节）包括：

（1） Lacp 的基本信息

- [AdminStatus]：Lacp 使能状态
- [LacpPriority]：Lacp 优先级

（2） 聚合端口的信息

- [GroupNum]：聚合端口所属聚合组号
- [GroupMode]：端口所属聚合组聚合模式
- [LacpTime]：聚合端口超时模式
- [LacpActive]：聚合端口主动/被动模式

在该页面对 Lacp 的基本属性“AdminStatus”、“LacpPriority”进行设置；以及对聚合端口的“LacpTime”、“LacpActive”属性进行设置；设置好后单击<Apply>按钮提交，完成配置。

当要把批量聚合端口的属性进行相同配置时也可以点击对应复选框选中多个聚合端口（选中[Select All]则选中所有端口）；然后单击<Set>按钮，打开批量聚合端口配置页面，如 图 8.6-18所示。

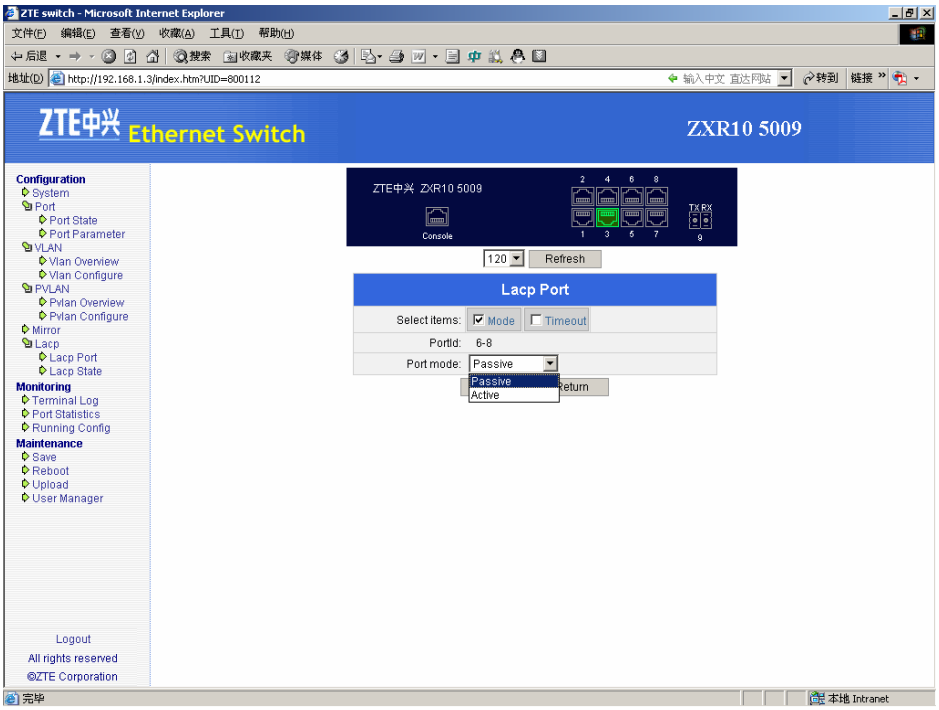


图8.6-18　批量聚合端口配置页面

在该页面中对聚合端口属性进行设置后单击<Apply>按钮提交即可。

2. 点击主页面中左侧目录树[Configuration→Lacp→Lacp State]，打开聚合组信息页面，如 图 8.6-19所示。

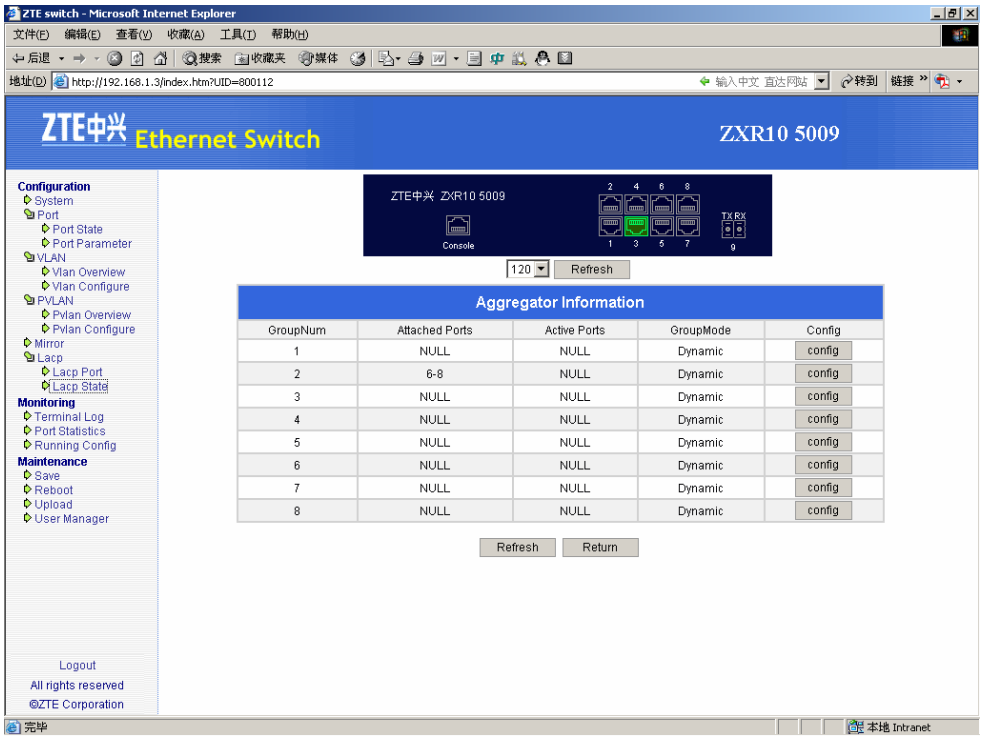


图8.6-19 聚合组信息页面

该页面显示了聚合组的以下信息：

- [Attached Ports]：聚合组中绑定的端口
- [Active Ports]：聚合组中成功激活的端口
- [GroupMode]：聚合组聚合模式

点击右侧一列中的某个<Config>按钮，打开相应聚合组的配置页面，如 图8.6-20所示。

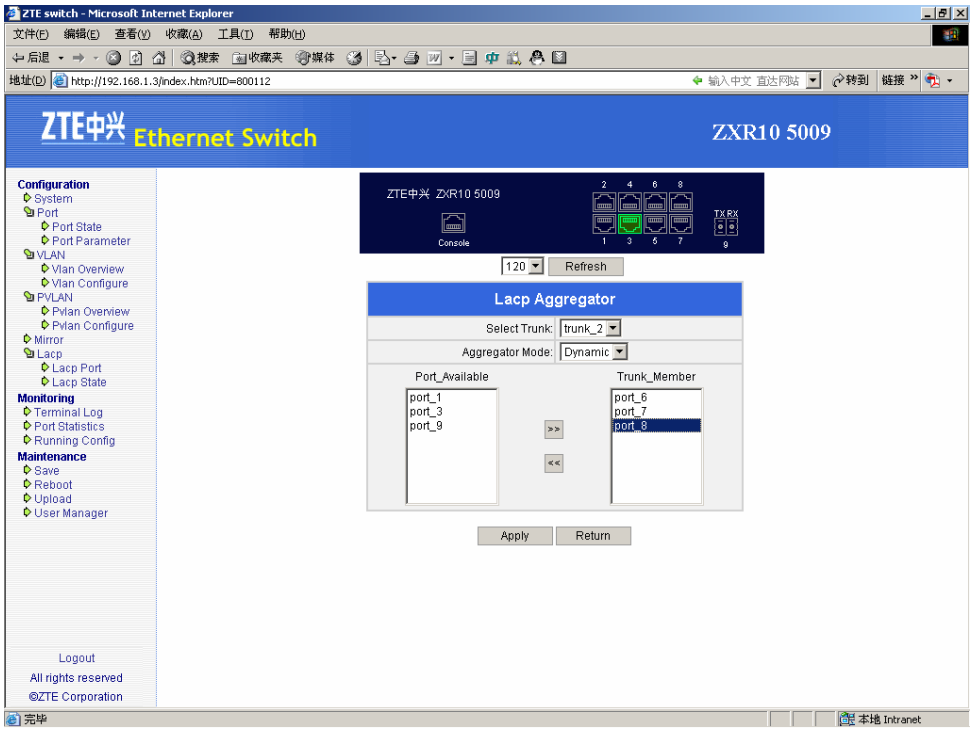


图8.6-20　聚合组配置页面

在该页面可以对选中的聚合组“Aggretator Mode（聚合模式）”属性进行设置，以及向聚合组中绑定端口（在可选端口栏中选中端口，单击<>>>按钮）和从聚合组中释放端口（在聚合端口栏中选中端口，单击<<<>按钮）。

说明：

只有属性相同的端口才可以绑定到同一聚合组中。每个聚合组最多可以绑定 8 个端口。

小心：

避免将与网管主机相连的端口绑定到聚合组！否则，会导致网管中断。

8.6.4 监控信息

8.6.4.1 终端记录

点击主页面中左侧目录树[Monitoring→Terminal Log]，打开终端日志信息页面，如 图 8.6-21所示。

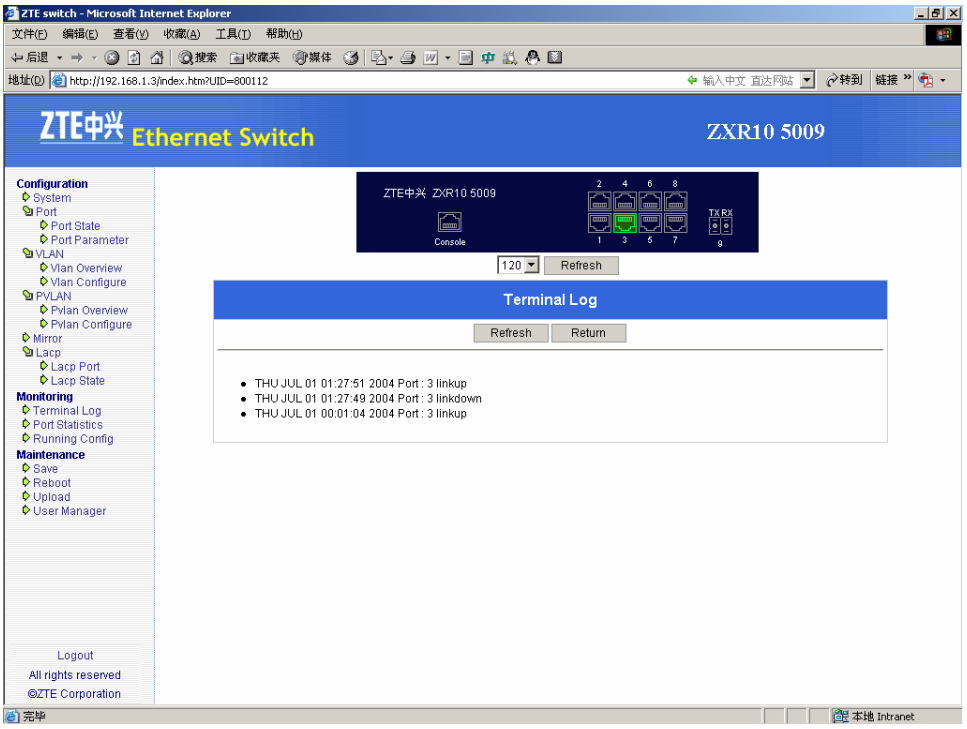


图8.6-21 终端日志信息页面

单击页面中的<Refresh>按钮，可以更新终端日志信息。

8.6.4.2 端口统计

点击主页面中左侧目录树[Monitoring→Port Statistics]，打开端口统计信息页面，如 图 8.6-22所示。

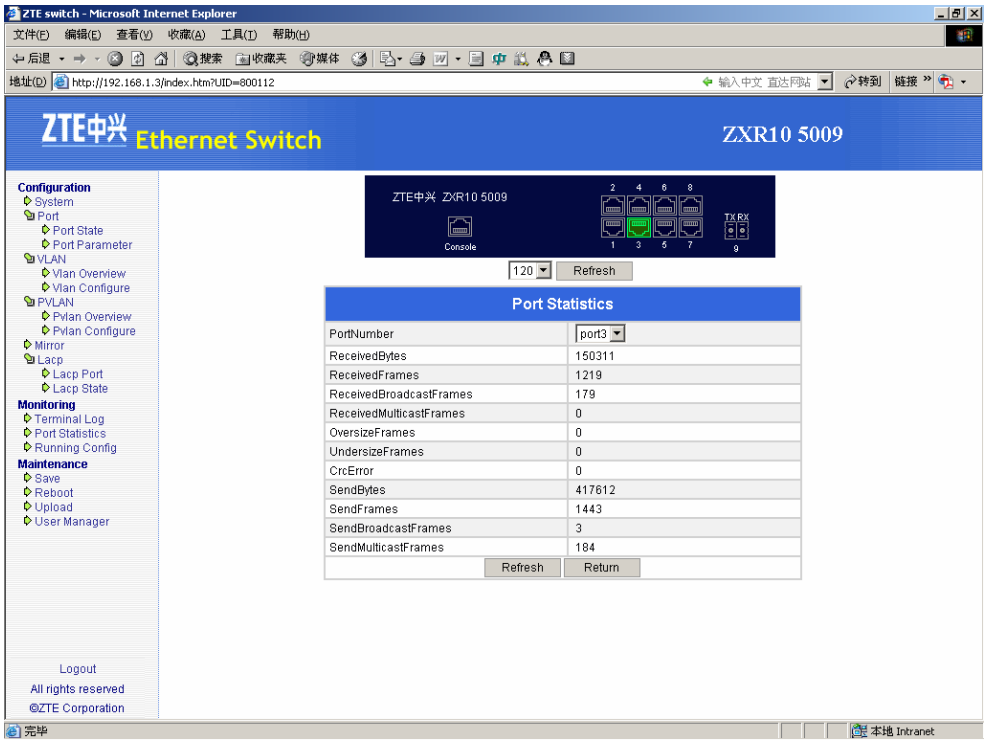


图8.6-22　端口统计信息页面

单击页面中的<Refresh>按钮，可以更新端口的统计信息。

在[PortNumber]下拉框内选中端口，即可得到该端口的统计数据。统计数据包括：

- [ReceivedBytes]：收到的字节数
- [ReceivedFrames]：收到的包数
- [ReceivedBroadcastFrames]：收到的广播包数
- [ReceivedMulticastFrames]：收到的组播包数
- [OversizeFrames]：超长的包数
- [UndersizeFrames]：长度不够的包数
- [CrcError]：校验和错误的包数
- [SendBytes]：发送的字节数
- [SendFrames]：发送的包数
- [SendBroadcastFrames]：发送的广播包数
- [SendMulticastFrames]：发送的组播包数

8.6.4.3 配置信息

点击主页面中左侧目录树[Monitoring→Running config]，打开配置信息页面，如 图8.6-23所示。

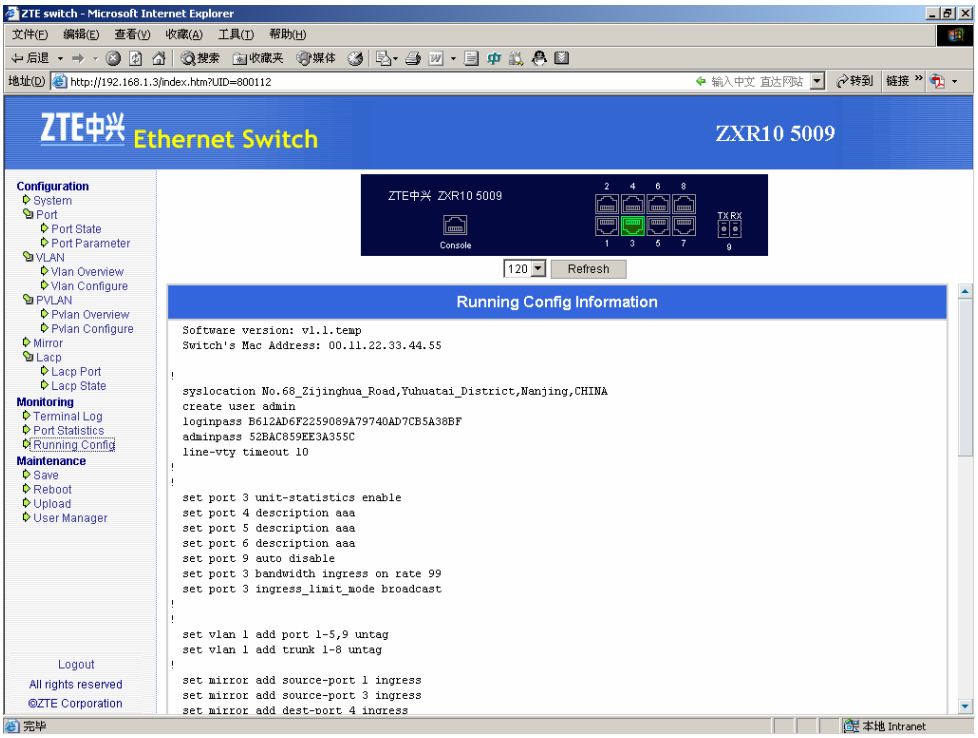


图8.6-23 配置信息页面

该页面显示交换机的配置信息。

8.6.5 系统维护

8.6.5.1 配置保存

点击主页面中左侧目录树[Maintenance→Save]，打开配置保存提示页面，如 图8.6-24所示。

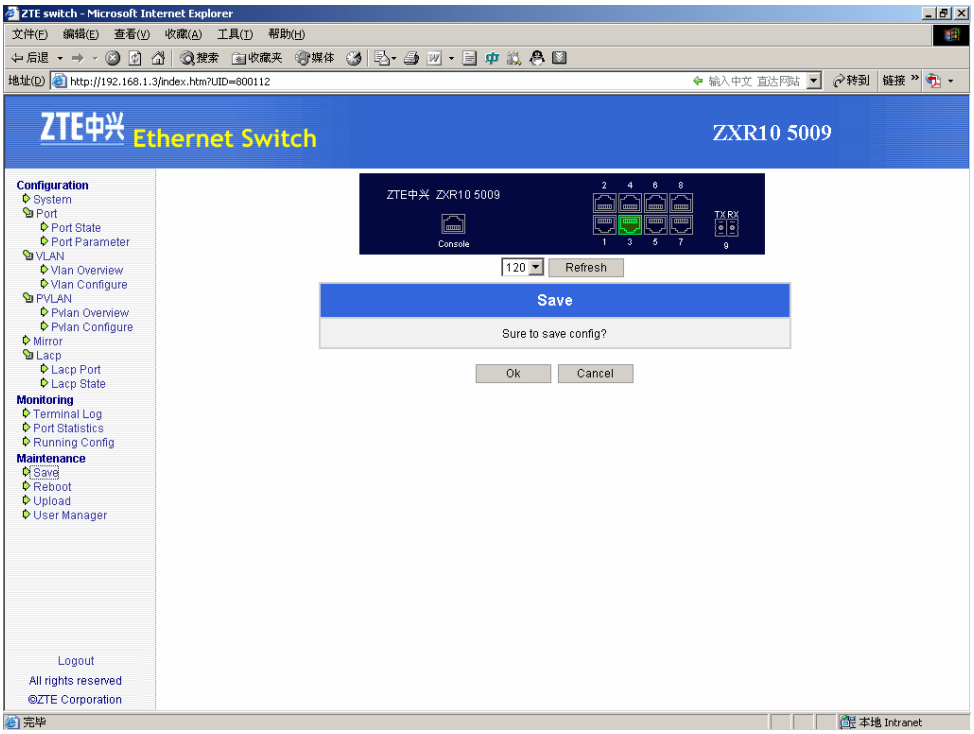


图8.6-24　配置保存提示页面

单击<Ok>按钮保存配置，或单击<Cancel>按钮放弃保存。

注意：

保存配置会将原有配置文件覆盖，请确认要覆盖再单击[Ok]按钮 。

8.6.5.2 交换机重启

点击主页面中左侧目录树[Maintenance→Reboot]，打开重启功能页面，如 图 8.6-25 所示。

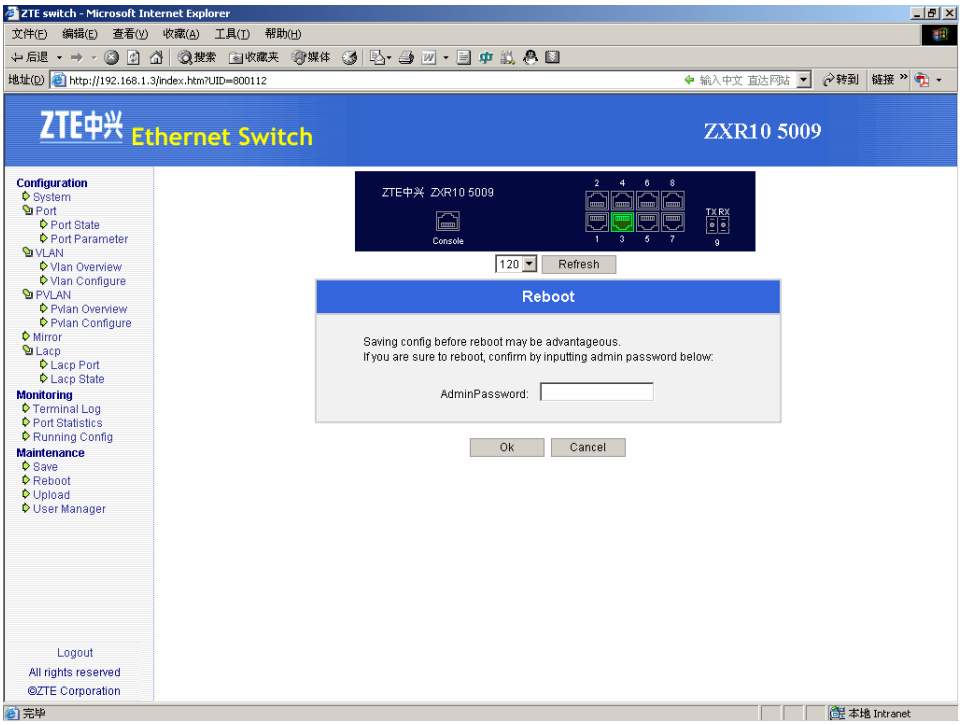


图8.6-25 重启功能页面

在 AdminPassword 中正确输入 Admin 密码，然后单击<Ok>按钮重新启动交换机，或单击<Cancel>按钮放弃重启。

8.6.5.3 文件上传

点击主页面中左侧目录树[Maintenance→Uplaod]，打开文件上传页面，如 图 8.6-26 所示。

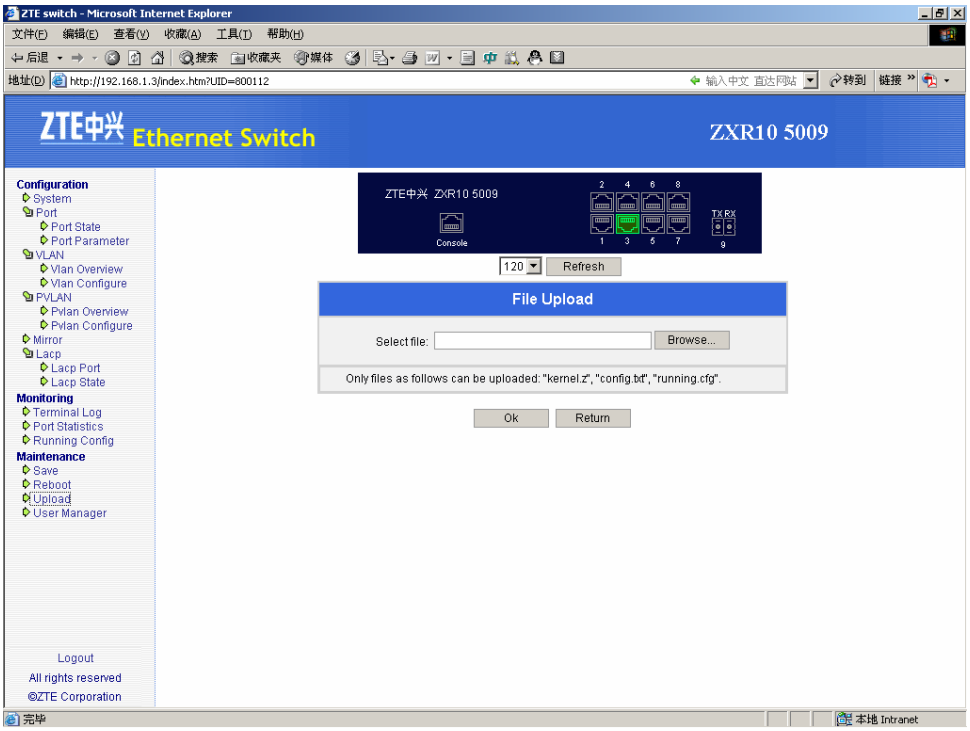


图8.6-26　文件上传页面

单击<Browse…>按钮，浏览并选中要上传的文件，如 图 8.6-27所示，然后单击<Ok>按钮上传文件。

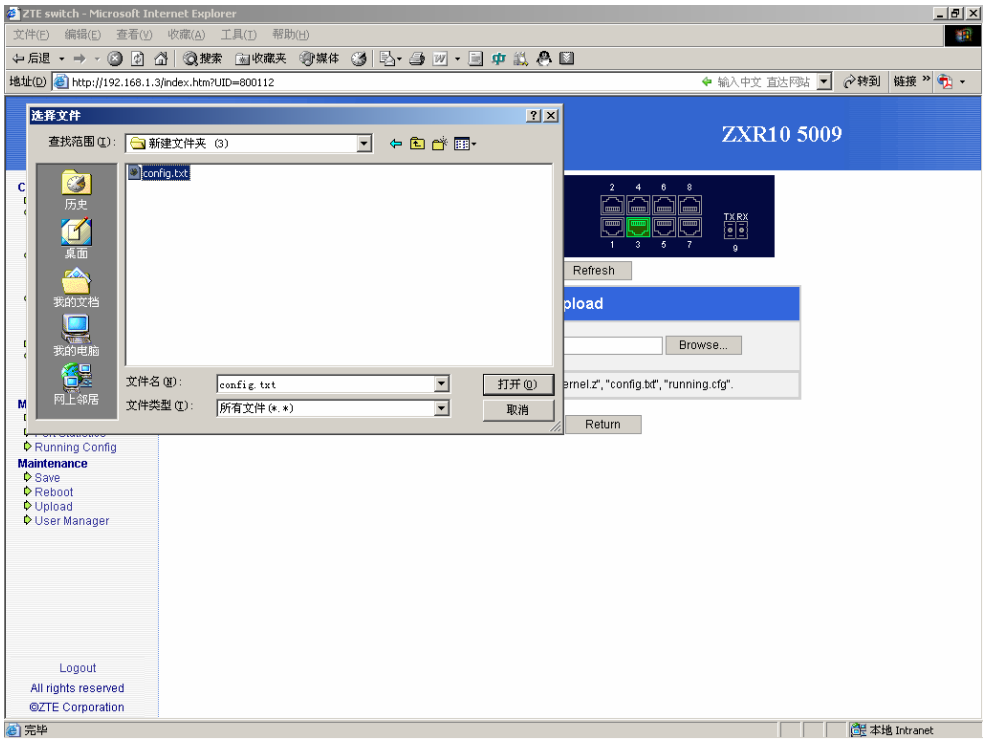


图8.6-27 浏览并选择文件

说明：

出于安全和应用考虑，只允许上传“running.cfg”、“config.txt”和“kernel.z”三种文件。

警告：

请确保要上传文件的合法行和可用性，上传文件会将原有文件覆盖；若操作不当将导致交换机无法工作！非专业人员不推荐使用此功能。

8.6.5.4 用户管理

1. 点击主页面中左侧目录树[Maintenance→User Manager]，打开用户管理页面，如 图 8.6-28所示。

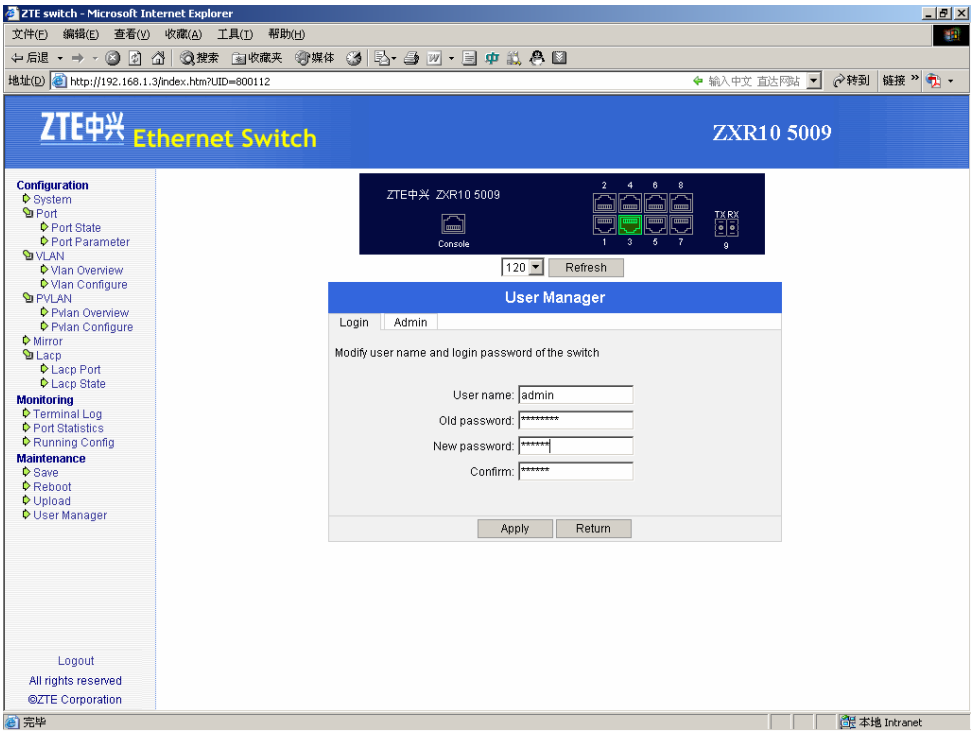


图8.6-28　用户管理页面

该页面显示了当前用户名，可以对用户名和登录密码进行修改。输入新用户名，密码，新密码并确认，单击<Apply>按钮提交。

2. 点击用户管理页面中的<Admin>按钮，打开管理密码修改页面，如 图 8.6-29 所示。

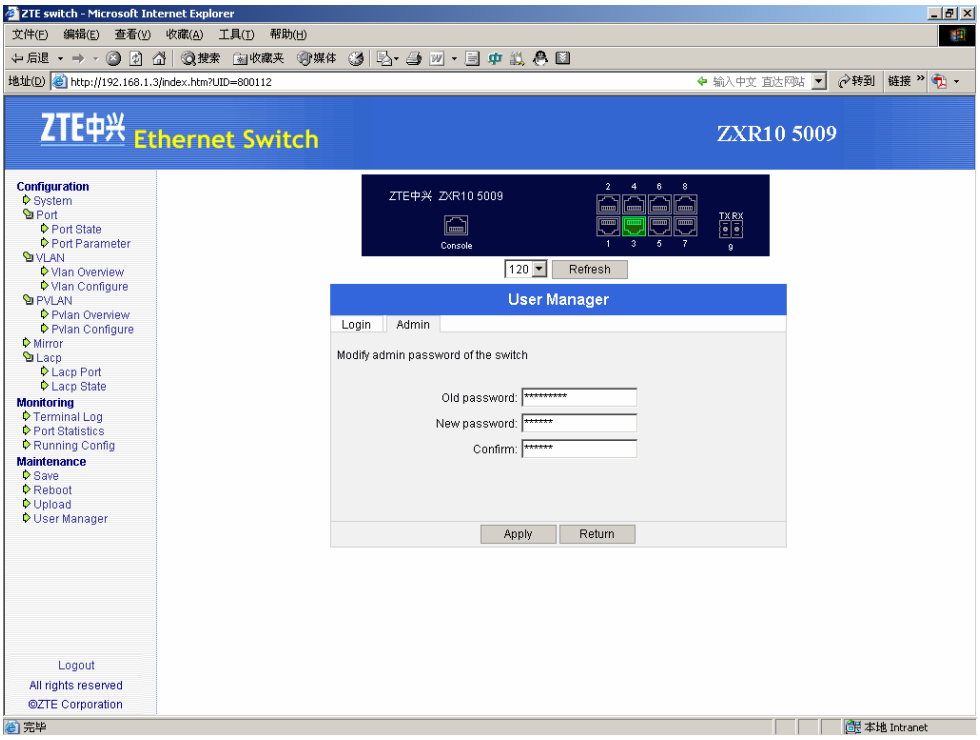


图8.6-29 管理密码页面

在页面中输入管理密码，新管理密码并确认，然后单击<Apply>按钮提交。

第9章 维护

摘要

本章主要介绍 ZXR10 5009 的日常维护工作、常用检测方法和故障处理方法，目的是使用户掌握产品的日常维护工作及常见故障的处理方法。

9.1 日常维护

日常维护通常指日维护及月维护。具体包括如下。

9.1.1 日维护项目

1. 检查交换机运行状态

（1） 查看后台终端界面是否能够正常操作。

（2） 查看交换机各指示灯状态是否正常。

（3） 检查交换机风扇是否正常运转。

（4） 检查交换机温度是否正常，机房是否有异味。

（5） 检查系统告警信息。

2. 检查交换机与各相连设备的通信状况

通过超级终端或 Telnet 等工具登录到交换机，使用 **ping** 命令对不同网段进行测试，检查连通性。

3. 检查交换机相关业务是否正常

4. 记录当天的操作及出现的现象

当天操作主要指当天对交换机所做的操作，记录现象应该包括交换机状态及机房环境等。

9.1.2 月维护项目

1. 对每日操作进行月总结

（1） 总结日常操作中遇到的问题，必要时可与中兴通讯维护人员进行探讨。

（2） 总结、积累日常维护中的维护经验，以便进行更高效的维护。

2. 清洁机房环境

（1） 注意空调的清洁，同时适时检查空调性能；

（2） 清洁走线槽，注意相关线路是否有松动，及时调整。

3. 清洁交换机设备

注意抹布不要过湿，同时注意不要影响接口。

4. 告警信息的备份、统计信息的备份、配置信息的备份。

9.1.3 维护周期

以太网交换机系统维护测试周期如 表 9.1-1所示，供维护人员参考。

表9.1-1 以太网交换机系统维护测试周期

序号	维护测试项目	测试周期
1	交换机运行状态	日
2	机房温湿度检查及电源检查	日
3	交换机与相连设备间通信状况	日
4	相关业务是否正常开展	日
5	日常问题月总结	月
6	日常维护经验月总结	月
7	机房环境清洁	月
8	交换机清洁	月
9	年度总结	年
10	监控室设备全面保养及检查	年

9.2 常用检测方法

9.2.1 单端口环路检测

单端口环路检测的作用是检测交换机的端口是否存在环路。如果端口存在环路，会导致 MAC 地址学习错误，且容易造成广播风暴，严重时会导致交换机及网络瘫痪。启用单端口的环路检测，关闭有环路的端口，可以有效的消除端口环路造成的影响。

单端口环路检测的工作原理是：交换机从某个端口发送一个检测报文，如果这个检测报文原封不动（或者仅打了一个 tag 头）地从这个端口接收回来，说明这个端口存在环路。

交换机发送的检测报文包含以下三个参数：

- 源 MAC 地址：交换机的 MAC 地址，每个交换机的 MAC 地址是唯一的。
- 端口号：端口号与端口在交换机上的编号一一对应。
- VLAN 号：VLAN 号与端口在交换机上使能环路检测的 VLAN 号一一对应。
- 鉴别域：每个交换机，每个端口的数字签名都是不同的。

当端口发出的和收到的检测报文中这三个参数完全相同，则该端口必定存在环路。

在交换机上配置单端口环路检测包括以下内容。

1. 使能或关闭指定端口的环路检测功能

   set loopdetect port <*portlist*> {**enable**|**disable**}

   此时检测端口的 PVID 所在的 vlan 中是否有自环路存在，端口的环路检测功能缺省状态是关闭的。

2. 使能或关闭指定端口在指定 vlan 的环路检测功能

   set loopdetect port <*portlist*> **vlan** <*vlanlist*> {**enable**|**disable**}

   每个端口最多可以在 24 个 vlan 中使能环路检测功能（如果已经使能了端口的环路检测功能，则最多可以在 23 个 vlan 中使能环路检测功能）。端口的环路检测功能缺省状态是关闭的。

3. 使能或关闭 Trunk 的环路检测功能

   set loopdetect trunk <*trunklist*> {**enable**|**disable**}

   此时检测 Trunk 的 PVID 所在的 vlan 中是否有自环路存在，Trunk 的环路检测功能缺省状态是关闭的。

4. 使能或关闭 Trunk 在指定 vlan 的环路检测功能

   set loopdetect trunk <*trunklist*> **vlan** <*vlanlist*> {**enable**|**disable**}

   每个 Trunk 最多可以在 24 个 vlan 中使能环路检测功能（如果已经使能了端口的环路检测功能，则最多可以在 23 个 vlan 中使能环路检测功能）。Trunk 的环路检测功能缺省状态是关闭的。

5. 使能或关闭指定端口的环路检测的保护功能

   set loopdetect port <*portlist*> **protect** {**enable**|**disable**}

环路检测的保护功能是指当端口检测到环路时自动关闭端口，消除端口环路造成的影响。

6. 使能或关闭 Trunk 的环路检测的保护功能

set loopdetect trunk *<trunklist>* **protect** {**enable**|**disable**}

7. 设置关闭环路端口的时间

set loopdetect blockdelay *<1-1080>*

关闭环路端口的时间是指当端口检测到环路时关闭端口的时间，即保护端口的时间，只有当端口的环路检测的保护功能打开时才起作用。

8. 设置端口发送检测报文的时间间隔

set loopdetect sendpktInterval *<5-60>*

在默认情况下，开启环路检测的端口每隔 15 秒发送一个环路检测报文，通过此命令可以对发送的数据报文的间隔进行更改。单位为秒。

9. 显示端口环路检测的配置和端口的检测状态

show loopdetect

如果端口不能正常工作，可以通过**show loopdetect**观察端口是否存在环路，如没有检测到环路并且该端口的生成树使能的话，可以根据生成树状态来排除故障。

9.2.2 虚拟线路检测

VCT（虚拟线路检测）利用 TDR（时域反射计）实现对线路的诊断，能够诊断出线路的出错状态，如 Open（开路）、Short（短路）、Impedance Mismatch（电阻不匹配）以及 Good termination（线路良好），并利用拟合出来的经验公式给出线路出错的距离。

在交换机上使用 **show vct port** *<portname>*命令可以看到指定端口的 VCT 检测结果。

本交换机只支持千兆电口的 VCT 检测，其他接口模块均不支持。

9.3 常见故障处理

故障按其种类可以分为硬件故障和软件故障两种。对于硬件故障，如果我们能够准确的定位，这种故障一般情况下是通过更换硬件来解决的。对于软件和配置上的故障，则可以通过正确的操作来解决。

在进行故障处理时，首先应当根据前面章节的介绍检查设备的配置是否正确、连接设备的线缆是否正确、设备所需的环境是否满足。

下面对 ZXR10 5009 上的常见故障及处理方法进行详细介绍。

9.3.1 无法通过 Console 口进行配置

1. 故障现象

   不能通过 Console 口登录交换机进行配置。

2. 相关部件检查

   配置线、超级终端串口、交换机 Console 口。

3. 故障分析与定位

（1） 配置线接线错误。

（2） 超级终端串口属性设置错误，终端串口发生故障。

（3） 交换机的 Console 口发生故障。

4. 故障处理

（1） 更换正确的配置线，配置线的接线详见 4.2.2。

（2） 检查超级终端的串口属性设置，正确设置应为：每秒位数（波特率）“9600”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”。

检查超级终端串口是否正常，更换配置终端。

（3） 检查交换机的 Console 口是否正常。

9.3.2 Telnet 无法连接

1. 故障现象

   无法使用 Telnet 连接到交换机。

2. 故障分析与定位

（1） 所使用的端口 PVID 设置错误。

（2） 所使用的端口被禁用。

（3） 所使用的 IP 端口捆绑的 VLAN 被禁用。

（4） 交换机未配置有效的 IP 地址、子网掩码和默认网关。

（5） 交换机 IP 地址与网络上其它设备的 IP 地址有冲突。

3. 故障处理

（1） 修改所使用端口的 PVID，与该端口所属的 VLAN ID 一致。

（2） 将所使用的端口打开。

（3） 将所使用的 IP 端口绑定的 VLAN 启用。

（4） 给交换机配置有效的 IP 地址、子网掩码和默认网关。

（5） 修改交换机的 IP 地址或其它设备的 IP，消除 IP 地址冲突。

9.3.3 Telnet 登录交换机失败

1. 故障现象

远程终端能够 Telnet 到交换机，但无法登录，提示用户没有设置。

2. 故障分析与定位

交换机上的登录密码设置为空。

3. 故障处理

设置非空的登录密码。

9.3.4 Web 管理无法连接

1. 故障现象

打开 Web 浏览器之后，无法打开 Web 管理页面。

2. 故障分析与定位

（1） 浏览器版本太低，无法支持。

（2） 浏览器地址栏填写错误地址和端口号。

（3） 主机和设备之间通信故障。

（4） 交换机未设置管理接口，或未设置正确的 IP 地址。

（5） 交换机未开启 Web 管理功能。

3. 故障处理

（1） 升级主机的浏览器版本，至少 4.0 以上。

（2） 察看交换机配置，获取正确的 IP 地址和端口号。

（3） 检查主机和设备之间的线路，保证主机和设备之间通信正常。

（4） 给交换机设置正确的管理接口，同时设置正确的 IP 地址。

（5） 开启交换机的 Web 管理功能，设置端口号。

9.3.5 Web 登录交换机失败

1. 故障现象

远程终端能够通过 Web 登录到交换机，但无法登录，提示用户名密码错误。

2. 故障分析与定位

交换机设置的用户名和密码不同于主机上输入的用户名和密码。

3. 故障处理

检查交换机配置，输入正确的用户名和密码。

9.3.6 遗失登录的用户名或密码

1. 故障现象

用户输入用户名和登录密码后无法登录交换机。

2. 故障分析与定位

登录交换机时使用的用户名或密码错误。

3. 故障处理

首先确认系统管理员是否还能找到原来设定的登录用户名和密码。如果无法找到，需要重启交换机删除配置文件，操作步骤如下。

（1） 重启交换机，在超级终端下根据提示按任意键进入 boot 状态。

```
                Welcome to use ZTE eCarrier!!



Copyright(c) 2004-2006,  ZTE Co., Ltd.
System Booting......
```

```
CPU: WindBond ARM7TDMI
Version: VxWorks5.5.1
BSP version: 1.2/0
Creation date: Apr 28 2006, 17:24:03




Press any key to stop auto-boot...
 7

[ZxR10 Boot]:
```

（2） 在 Boot 状态下输入<zte>，进入交换机的[BootManager]状态，输入<?>获得命令帮助。

```
[ZXR10 Boot]: zte
Load wbdEnd Begin
W90N740 MAC0: 100MB - Full Duplex

BoardType=0x59

Board 5009 !
Marvell has been initialized !
boot device         : wbdEnd
unit number         : 0
processor number    : 0
host name           : tiger
file name           : vxWorks
inet on ethernet (e) : 10.40.47.89
host inet (h)       : 10.40.47.78
gateway inet (g)    : 10.40.47.78
flags (f)           : 0x80

Attached TCP/IP interface to wbdEnd0.
Warning: no netmask specified.
Attaching network interface lo0... done.
Attaching to TFFS...
test flash passed perfectly!
Board type has not been written.
Welcome to boot manager!
Type '?' for help
```

```
[BootManager]:?

ls                                          /*列出当前目录清单*/
pwd                                         /*显示当前绝对路径*/
devs                                        /*显示 flash 信息*/
show                                        /*显示交换机类型和 mac 地址*/
reboot                                      /*重启交换机*/
format                                      /*格式化 flash*/
del    file_name                            /*删除指定文件*/
md     dir_name                             /*创建目录*/
mf     file_name                            /*创建文件*/
cd     absolue-pathname                     /*更改当前目录*/
tftp   ip_address file_name                 /*TFTP 上传/下载版本*/
update file_name                            /*升级 boot*/
rename  file_name newname                   /*文件重新命名*/
[BootManager]:
```

（3） 执行 **del** 命令删除配置文件，并重启交换机。

```
[BootManager]:ls
KERNEL
RUNNING.CFG
[BootManager]:del running.cfg
[BootManager]:reboot
```

（4） 交换机重启后，使用缺省用户名和密码就可以登录交换机。

```
Please Press any Key to Start!

Welcome !
ZTE Corporation.
All rights reserved.

login:admin
password:*********
zte>en
password:
zte(cfg)#
```

9.3.7 遗失 enable 密码

1. 故障现象

用户登录交换机后输入密码无法进入全局配置模式。

2. 故障分析与定位

进入全局配置模式时使用的密码错误。

3. 故障处理

处理方法参见 9.3.6节。

4. 注意事项

重启交换机之前，应将交换机的当前配置记录下来，以便重新配置。

9.3.8 同一 VLAN 中的两个设备不能互通

1. 故障现象

连接到交换机上同一 VLAN 中两个端口的两个设备不能互通。

2. 故障分析与定位

（1） 所使用的端口 PVID 设置错误。

（2） 所使用的端口被禁用。

（3） 该端口所使用的 VLAN 被禁用。

（4） 端口在加入 VLAN 时选择了 tag。

（5） 设备没有设置 IP 地址，或者所设置的 IP 地址没有处于同一网段。

3. 故障处理

（1） 修改所使用端口的 PVID，与该端口所属的 VLAN ID 一致。

（2） 将所使用的端口打开。

（3） 将所使用的 VLAN 启用。

（4） 将所使用的端口重新加入 VLAN，加入时选择 untag。

（5） 给设备设置正确的 IP 地址。

第10章 命令参考

摘要

本章介绍 ZXR10 5009 交换机的命令，对命令的功能、模式、格式、参数和使用等进行了说明。

10.1 概述

命令中常用的参数如 表 10.1-1所示。

表10.1-1 参数说明

参数	说明
<portlist>	以逗号分隔的端口号、端口名称或端口号范围。如： ● 1，2，4-8 ● p1，pp2，4-8 p1，pp2 是用户创建的端口的名称
<vlanlist>	以逗号分隔的 VLAN ID、VLAN 名称或 VLAN 范围。如： ● 1-19，77， 88，100-900 ● vlan1，v1，10，100-200
<trunklist>	以逗号分隔的 trunk ID 或 trunk 范围。如： 1-19，77，88，100-900
<portname>	表示一次只允许输入一个端口号或端口名称
<vlanname>	表示一次只允许输入一个 VLAN ID 或 VLAN 名称
<trunkid>	表示一次只允许输入一个 trunk ID
<xx.xx.xx.xx.xx.xx>	MAC 地址，如：11.22.33.44.55.66
<A.B.C.D>	IP 地址，如：10.40.47.254
<A.B.C.D/M>	IP 地址和掩码位数，M 为 1~32 的整数，如：10.40.47.254/24
<string>	不含空格的字符串
<mib-oid>	不定长的点分十进制数，如：1.3.6.2.19.2
<name>	名称，是一个不含空格的字符串

10.2 管理命令

10.2.1 adminpass

命令功能：设置进入全局配置模式的密码。

命令模式：全局配置模式

命令格式：**adminpass** [<*string*>]

参数解释：

参数	描述
<*string*>	进入配置模式的密码

使用说明：如果 **adminpass** 后面不跟任何参数直接回车，表示设置管理密码为空。

示例：设置进入全局配置模式的密码为 administrator。

```
adminpass administrator
```

10.2.2 config router

命令功能：进入三层配置模式。

命令模式：全局配置模式

命令格式：**config router**

10.2.3 config snmp

命令功能：进入 SNMP 配置模式。

命令模式：全局配置模式

命令格式：**config snmp**

10.2.4 config tffs

命令功能：进入文件系统配置模式。

命令模式：全局配置模式

命令格式：**config tffs**

10.2.5 create user

命令功能：创建一个新的管理用户。

命令模式：全局配置模式

命令格式：**create user** <*name*>

参数解释：

参数	描述
<*name*>	管理用户的名称

示例：创建名为 userx 的用户。

```
create user userx
```

10.2.6 delete user

命令功能：删除一个管理用户。

命令模式：全局配置模式

命令格式：**delete user** <*name*>

参数解释：

参数	描述
<*name*>	管理用户的名称

示例：删除名为 userx 的用户。

```
delete user userx
```

10.2.7 enable

命令功能：从用户模式进入全局配置模式。

命令模式：用户模式

命令格式：**enable**

使用说明：执行 **enable** 命令之后系统会提示用户输入管理密码（用 **adminpass** 命令设置）。

10.2.8 exit

命令功能：从当前模式退出到上一层模式。

命令模式：所有模式

命令格式：**exit**

10.2.9 hostname

命令功能：设置或改变主机名称。

命令模式：全局配置模式

命令格式：**hostname** <*name*>

参数解释：

参数	描述
<*name*>	主机的名称

示例：设置主机名为 hello。

```
hostname hello
```

10.2.10 line-vty

命令功能：设置 telnet 用户登录超时时间。

命令模式：全局配置模式

命令格式：**line-vty timeout** <*1-1080*>

参数解释：

参数	描述
<*1-1080*>	超时时间，单位：分钟，缺省为 10 分钟

10.2.11 list

命令功能：列出当前模式下所有可用的命令。

命令模式：所有模式

命令格式：**list**

10.2.12 loginpass

命令功能：设置登录密码。

命令模式：全局配置模式

命令格式：**loginpass** [<*string*>]

参数解释：

参数	描述
<*string*>	登录密码

使用说明：如果 **loginpass** 后面不跟任何参数直接回车，表示设置登录密码为空，此时 telnet 用户将不能登录系统。

示例：设置登录密码为 ok。

```
loginpass ok
```

10.2.13 ping

命令功能：检测网络的连通性。

命令模式：全局配置模式

命令格式：**ping** <*A.B.C.D*> [<*0-65535*>] [<*0-65535*>]

参数解释：

参数	描述
<*A.B.C.D*>	目的 IP 地址
<*0-65535*>	发送 echo 请求的次数
<*0-65535*>	等待响应的时延

10.2.14 readconfig

命令功能：从 config.txt 文件中读取交换机的配置。

命令模式：全局配置模式

命令格式：**readconfig**

10.2.15 reboot

命令功能：重启交换机。

命令模式：全局配置模式

命令格式：**reboot**

10.2.16 saveconfig

命令功能：保存配置信息。

命令模式：全局配置模式

命令格式：**saveconfig**

10.2.17 set date

命令功能：设置日期和时间。

命令模式：全局配置模式

命令格式：**set date** <*yyyy-mm-dd*> **time** <*hh:mm:ss*>

参数解释：

参数	描述
<*yyyy-mm-dd*>	日期（年月日）
<*hh:mm:ss*>	时间（时分秒）

使用说明：交换机重启之后，日期和时间需要重新配置。

10.2.18 set loginauth

命令功能：设置登录认证方式。

命令模式：全局配置模式

命令格式：**set loginauth** {**local**|**radius**}

参数解释：

参数	描述
local	设置登录用户为本地认证
radius	设置登录用户为 radius 认证

10.2.19 show date-time

命令功能：显示当前日期和时间。

命令模式：所有模式

命令格式：**show date-time**

使用说明：如果没有配置日期和时间，则缺省从 2004-07-01 开始计时。

10.2.20 show loginauth

命令功能：显示登录认证方式。

命令模式：所有模式

命令格式：**show loginauth**

10.2.21 show running-config

命令功能：显示系统当前所有非缺省的配置。

命令模式：所有模式

命令格式：**show running-config** [**toFile**]

参数解释：

参数	描述
[**toFile**]	将 **show running-config** 的结果输出到 config.txt 文件

10.2.22 show specialVlan1

命令功能：显示 specialVlan1 的配置信息。

命令模式：所有模式

命令格式：show specialVlan1

10.2.23 show start-config

命令功能：显示系统最后一次 save 时的所有非缺省的配置。

命令模式：所有模式

命令格式：**show start-config**

10.2.24 show terminal

命令功能：显示终端的监控和日志信息。

命令模式：所有模式

命令格式：**show terminal** [**log**]

参数解释：

参数	描述
[**log**]	显示日志内容

使用说明：**show terminal** 显示 monitor 和 log 的 on/off 状态，以及设置 timer 值。

10.2.25 show vct

命令功能：显示端口虚拟线路检测的结果。

命令模式：所有模式

命令格式：**show vct port** <*portname*>

参数解释：

参数	描述
<*portname*>	一个端口号

10.2.26 show user

命令功能：显示 telnet 登录用户信息和当前用户名。

命令模式：所有模式

命令格式：**show user**

10.2.27 sysLocation

命令功能：设置交换机的位置信息。

命令模式：全局配置模式

命令格式：**sysLocation** <*string*>

参数解释：

参数	描述
<*string*>	交换机的位置信息

10.2.28 terminal log

命令功能：允许/禁止写日志。

命令模式：全局配置模式

命令格式：**terminal log** {**on**|**off**}

参数解释：

参数	描述
on	允许写日志
off	禁止写日志

10.2.29 terminal log timer

命令功能：设置定时信息。

命令模式：全局配置模式

命令格式：**terminal log** {**enable**|**disable**|**interval**}

参数解释：

参数	描述
enable	使能定时器
disable	关闭定时器
interval	设置定时间隔

10.2.30 terminal log toFile

命令功能：保存 log 信息。

命令模式：全局配置模式

命令格式：terminal log toFile

10.2.31 terminal monitor

命令功能：允许/禁止向终端打印实时告警信息。

命令模式：全局模式

命令格式：**terminal monitor** {**on**|**off**}

参数解释：

参数	描述
on	允许打印实时告警信息
off	禁止打印实时告警信息

10.2.32 version

命令功能：显示版本、交换机运行时间、交换机 MAC 地址等系统信息。

命令模式：全局配置模式

命令格式：**version**

10.3 文件系统

10.3.1 cd

命令功能：更改当前目录。

命令模式：文件系统配置模式

命令格式：**cd** <*name*>

参数解释：

参数	描述
<*name*>	目录的名称

示例：文件系统中有一个名为 config 的目录，进入 config 目录。

```
cd config
```

10.3.2 copy

命令功能：拷贝文件。

命令模式：文件系统配置模式

命令格式：**copy** <*name*> <*name*>

参数解释：

参数	描述
<*name*>	原文件路径名称/目的文件路径名称

示例一：将根目录\中的文件 v1.txt 拷贝到目录\bak。

```
copy v1.txt bak\v1.txt
```

示例二：将目录\\test 中的文件 a.txt 拷贝到目录\\temp 中。

```
copy \\test\a.txt \\temp\a.txt
```

10.3.3 format

命令功能：格式化 flash。

命令模式：文件系统配置模式

命令格式：**format**

10.3.4 ls

命令功能：列出当前目录清单。

命令模式：文件系统配置模式

命令格式：**ls**

10.3.5 md

命令功能：创建目录。

命令模式：文件系统管理模式

命令格式：**md** <*name*>

参数解释：

参数	描述
<*name*>	目录的名称

示例：创建目录 group。

```
md group
```

10.3.6 remove

命令功能：删除指定文件或目录。

命令模式：文件系统配置模式

命令格式：**remove** <*name*>

参数解释：

参数	描述
<*name*>	文件或目录的名称

示例：删除目录 group。

```
remove group
```

10.3.7 rename

命令功能：更改文件名。

命令模式：文件系统配置模式

命令格式：**rename** <*name*> <*name*>

参数解释：

参数	描述
<*name*>	原文件名称/目的文件名称

示例：将文件 configbak.txt 改名为 config.txt。

```
rename configbak.txt config.txt
```

10.3.8 tftp

命令功能：TFTP 下载/上载版本。

命令模式：文件系统配置模式

命令格式：**tftp** {*<A.B.C.D>*|**commander**} {**download**|**upload**} *<name>*

参数解释：

参数	描述
<A.B.C.D>	指定主机的 IP 地址
commander	命令交换机
download	从主机下载文件到 FLASH
upload	将 FLASH 中的文件上载到主机
<name>	文件的名称

示例：将版本 version.o 从 10.40.44.167 下载到交换机。

```
tftp 10.40.44.167 download version.o
```

10.4 端口配置

10.4.1 clear port

命令功能：清除端口的名称/统计数据。

命令模式：全局配置模式

命令格式：**clear port** *<portlist>* {**name**|**statistics**|**description**}

参数解释：

参数	描述
<portlist>	端口列表
name	清除端口的名称
statistics	清除端口的统计数据
description	清除端口的描述信息

示例：清除端口 1，5，6，7 的名称。

```
clear port 1,5-7 name
```

10.4.2 create port name

命令功能：为端口创建描述名称。

命令模式：全局配置模式

命令格式：**create port** <*portname*> **name** <*name*>

参数解释：

参数	描述
<*portname*>	一个端口号
<*name*>	端口的名称

示例：为端口 1 创建描述名为 userx。

```
create port 1 name userx
```

10.4.3 set port

命令功能：使能/关闭端口。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	使能端口
disable	关闭端口

示例：使能端口 1，5，6，7。

```
set port 1,5-7 enable
```

10.4.4 set port auto

命令功能：开启/关闭端口的自适应功能。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **auto** {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	开启端口的自适应功能
disable	关闭端口的自适应功能

示例：开启端口 1，5，6，7 的自适应功能。

```
set port 1,5-7 auto enable
```

10.4.5 set port bandwidth

命令功能：设置端口的带宽。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **bandwidth ingress** {**off**|**on rate** <*70-256000*>}[**tcpdrop**|**flowcontrol**]

set port <*portlist*> **bandwidth egress** {**off**|**on rate** <*70-256000*>}

参数解释：

参数	描述
<*portlist*>	端口列表
ingress	设置输入带宽
egress	设置输出带宽
off	关闭带宽限制
on	开启带宽限制
tcpdrop	Tcp 连接方式
flowcontrol	流控连接方式
<*70-256000*>	速率，从 70 到 256000 的任意一个数，单位：kbps

示例：设置端口 1，5，6，7 的输入带宽为 1000kbps。

```
set port 1,5-7 bandwidth ingress on rate 1000
```

10.4.6 set port dscp-priority

命令功能：开启/关闭端口三层 DSCP 优先级。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **dscp-priority** {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	开启端口三层 DSCP 优先级
disable	关闭端口三层 DSCP 优先级

使用说明：当且仅当接收的数据包是 IP 数据包，并且端口的三层 DSCP 优先级决定功能使能时，此时才可能使用三层 DSCP 优先级决定数据包的优先级。 数据包的队列优先级由 IP DSCP 优先级到队列优先级对应表决定。

10.4.7 set port default-priority

命令功能：设置端口的默认优先级。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **default-priority** <*0-7*>

参数解释：

参数	描述
<*portlist*>	端口列表
<*0-7*>	端口的默认优先级

10.4.8 set port description

命令功能：设置端口的描述信息。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **description** <*string*>

参数解释：

参数	描述
< *portlist* >	端口列表
<*string*>	端口的描述信息

10.4.9 set port duplex

命令功能：设置端口的工作方式为全双工/半双工。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **duplex** {**full**|**half**}

参数解释：

参数	描述
<portlist>	端口列表
full	端口的工作方式为全双工
half	端口的工作方式为半双工

示例：设置端口 1，5，6，7 的工作方式为全双工。

```
set port 1,5-7 duplex full
```

10.4.10 set port flowcontrol

命令功能：开启/关闭端口的流量控制。

命令模式：全局配置模式

命令格式：**set port** *<portlist>* **flowcontrol** {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enbale	开启端口的流量控制
disable	关闭端口的流量控制

示例：开启端口 1，5，6，7 的流量控制。

```
set port 1,5-7 flowcontrol enable
```

10.4.11 set port ingress_limit_mode

命令功能：设置端口的带宽限制模式。

命令模式：全局配置模式

命令格式：

set port *<portlist>* **ingress_limit_mode** {**all**|**nonunicast**|**multi-broadcast**|**broadcast**}

参数解释：

参数	描述
<portlist>	端口列表
all	设置入口限速过滤类型为所有数据包
nonUnicast	设置入口限速过滤类型为非单播数据包
multi-broadcast	设置入口限速过滤类型为广播和组播数据包
broadcast	设置入口限速过滤类型为广播数据包

10.4.12 set port macaddress

命令功能：设定端口 MAC 地址学习数目。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **macaddress {off|on** <*1-16*>**}**

参数解释：

参数	描述
<*portlist*>	端口列表
<1-*16*>	端口 MAC 地址学习数目

10.4.13 set port multicast-filter

命令功能：设置端口对组播包过滤开启/关闭。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **multicast-filter** {**enable|disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	组播包过滤开启，即丢弃组播包
disable	组播包过滤关闭，即转发组播包

示例：设置端口 1，5，6，7 对组播包进行转发。

```
set port 1,5-7 multicast-filter disable
```

10.4.14 set port poe

命令功能：设置端口对外供电模式。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **poe** {**auto|force|never**}

参数解释：

参数	描述
<*portlist*>	端口列表
auto	设置供电模式为自动供电
force	设置供电模式为强制对外供电
never	设置供电模式为不对外供电

示例：设置端口 1 的对外供电模式为 auto。

```
set port 1 poe auto
```

10.4.15 set port priority

命令功能：配置端口的优先级控制。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **default-priority** <*0-7*>

参数解释：

参数	描述
<*portlist*>	端口列表
<*0-7*>	优先级值

示例：开启端口 1，5，6，7 的优先级为 3。

```
set port 1,5-7 default-priority 3
```

10.4.16 set port remapping-tag

命令功能：设置端口的 802.1P 用户优先级重映射表。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **remapping-tag** <0-7> **priority** <0-7>

参数解释：

参数	描述
<*portlist*>	端口列表
<0-7>	Remapping-tag 值，从 0 到 7 的任意一个数
<0-7>	Priority 值，从 0 到 7 的任意一个数

说明：当端口收到的数据包是 TAG 数据包是，交换机先使用此映射表对数据包中的优先级进行重新映射，然后使用此优先级作为新的 802.1P 用户优先级来进行以后的优先级决定。

此映射表的默认值为：0→0，1→1，2→2，3→3，4→4，5→5，6→6，7→7

示例：设置端口 1，5，6，7 的 802.1P 用户优先级重映射表的 remapping-tag 3 对应 priority 值为 2。

```
set port 1,5-7 remapping-tag 3 priority 2
```

10.4.17 set port sa-priority

命令功能：开启/关闭源 mac 地址优先级。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **sa-priority** {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	开启端口源 mac 地址优先级
disable	关闭端口源 mac 地址优先级

10.4.18 set port security

命令功能：开启/关闭端口的地址学习。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **security** {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	关闭端口的地址学习，不进行包转发
disable	开启端口的地址学习，进行包转发

示例：关闭端口 1，5，6，7 的地址学习。

```
set port 1,5-7 security enable
```

10.4.19 set port speed

命令功能：设置端口的速率为 10M/100M/1000M。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **speed** {**10**|**100**|**1000**}

参数解释：

参数	描述
<portlist>	端口列表
10	端口的速率为 10M
100	端口的速率为 100M
1000	端口的速率为 1000M

示例：设置端口 1，5，6，7 的速率为 10M。

```
set port 1,5-7 speed 10
```

10.4.20 set port speedadvertise

命令功能：设置端口速率宣称。

命令模式：全局配置模式

命令格式：**set port** *<portlist>* **speedadvertise** {**maxspeed**|{{**speed 10**|**speed 100**|**speed 1000**} {**fullduplex**|**halfduplex**}}}

参数解释：

参数	描述
<portlist>	端口列表
maxspeed	设置端口速率宣称为最大速率
speed 10	设置端口速率宣称为 10Mbps
speed 100	设置端口速率宣称为 100Mbps
speed 1000	设置端口速率宣称为 1000Mbps
fullduplex	全双工模式
halfduplex	半双工模式

10.4.21 set port user-priority

命令功能：开启/关闭 802.1P 用户优先级。

命令模式：全局配置模式

命令格式：**set port** *<portlist>* **user-priority** {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	开启端口 802.1P 用户优先级
disable	关闭端口 802.1P 用户优先级

10.4.22 set port vlan-priority

命令功能：开启/关闭 VLAN 优先级。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **vlan-priority** {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	开启端口 VLAN 优先级
disable	关闭端口 VLAN 优先级

10.4.23 set trunk multicast-filter

命令功能：设置 trunk 对组播包过滤开启/关闭。

命令模式：全局配置模式

命令格式：**set trunk** <*trunklist*> **multicast-filter** {**enable**|**disable**}

参数解释：

参数	描述
<*trunklist*>	Trunk 列表
enable	组播包过滤开启，即丢弃组播包
disable	组播包过滤关闭，即转发组播包

示例：设置 trunk 1 对组播包进行转发。

```
set trunk 1 multicast-filter disable
```

10.4.24 show port

命令功能：显示端口的配置和工作状态。

命令模式：所有模式

命令格式：**show port** [<*portlist*>]

参数解释：

参数	描述
<*portlist*>	端口列表

示例：显示端口 1，5，6，7 的配置和工作状态。

```
show port 1,5-7
```

10.4.25 show port qos

命令功能：显示端口 QoS 配置信息。

命令模式：所有模式

命令格式：**show port** <*portlist*> **qos**

参数解释：

参数	描述
<*portlist*>	端口列表

示例：显示端口 1，5，6，7 的 QoS 配置数据。

```
show port 1,5-7 qos
```

10.4.26 show port statistics

命令功能：显示端口的统计数据。

命令模式：所有模式

命令格式：**show port** <*portlist*> **statistics** {**1min_unit|5min_unit**}

参数解释：

参数	描述
<*portlist*>	端口列表
1min_unit	1 分钟内的流量统计
5min_unit	5 分钟内的流量统计

示例：显示端口 1，5，6，7 的统计数据。

```
show port 1,5-7 statistics
```

示例：显示端口 3 的 5 分钟内的流量统计。

```
show port 3 statistics 5min_unit
```

10.4.27 show trunk

命令功能：显示 trunk 的配置。

命令模式：所有模式

命令格式：**show trunk** [<*trunklist*>]

参数解释：

参数	描述
<trunklist>	Trunk ID 列表

示例：显示 trunk 1，5，6，7 的配置。

```
show trunk 1,5-7
```

10.5 端口镜像

10.5.1 set mirror add source-port

命令功能：增加入向/出向镜像端口。

命令模式：全局配置模式

命令格式：**set mirror add source-port** *<portlist>* {**ingress**|**egress**}

参数解释：

参数	描述
<portlist>	端口列表
ingress	入向
egress	出向

示例：增加出向镜像端口 1，5，6，7。

```
set mirror add source-port 1,5-7 egress
```

10.5.2 set mirror delete source-port

命令功能：删除入向/出向镜像端口。

命令模式：全局配置模式

命令格式：**set mirror delete source-port** *<portlist>* {**ingress**|**egress**}

参数解释：

参数	描述
<portlist>	端口列表
ingress	入向
egress	出向

示例：删除入向镜像端口 1，5，6，7。

```
set mirror delete source-port 1,5-7 ingress
```

10.5.3 set mirror add dest-port

命令功能：设置入向/出向监控端口。

命令模式：全局配置模式

命令格式：**set mirror add dest-port** <*portname*> {**ingress**|**egress**}

参数解释：

参数	描述
<*portname*>	一个端口号或者一个端口名称

交换机支持一个入向监控端口和一个出向监控端口。

示例：增加入向监控端口 1。

```
set mirror add dest-port 1 ingress
```

10.5.4 set mirror delete dest-port

命令功能：设置入向/出向监控端口。

命令模式：全局配置模式

命令格式：**set mirror delete dest-port** <*portname*> {**ingress**|**egress**}

参数解释：

参数	描述
<*portname*>	一个端口号或者一个端口名称

交换机支持一个入向监控端口和一个出向监控端口。

示例：删除入向监控端口 1。

```
set mirror delete dest-port 1 ingress
```

10.5.5 show mirror

命令功能：显示镜像配置信息。

命令模式：所有模式

命令格式：**show mirror**

10.6 VLAN 配置

10.6.1 clear vlan name

命令功能：清除 VLAN 的名称。

命令模式：全局配置模式

命令格式：**clear vlan** <*vlanlist*> **name**

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表

示例：清除 vlan 1，5，6，7 的名称。

```
clear vlan 1,5-7 name
```

10.6.2 create vlan name

命令功能：创建一个 VLAN 的描述名称。

命令模式：全局配置模式

命令格式：**create vlan** <*1-4094*> **name** <*name*>

参数解释：

参数	描述
<*1-4094*>	VLAN ID，从 1 到 4094 的任意一个数
<*name*>	VLAN 的名称

示例：设置 vlan 1 的名称为 group1。

```
create vlan 1 name group1
```

10.6.3 set port pvid

命令功能：设置端口的 PVID。

命令模式：全局配置模式

命令格式：**set port** <*portlist*> **pvid** <*1-4094*>

参数解释：

参数	描述
<*portlist*>	端口列表

<1-4094>	缺省的 VLAN ID，从 1 到 4094 的任意一个数

示例：设置端口 1，5，6，7 的 PVID 为 30。

```
set port 1,5-7 pvid 30
```

10.6.4 set trunk pvid

命令功能：设置 trunk 的 PVID。

命令模式：全局配置模式

命令格式：**set trunk** < *trunklist* > **pvid** *<1-4094>*

参数解释：

参数	描述
< *trunklist* >	Trunk 列表
<1-4094>	缺省的 VLAN ID，从 1 到 4094 的任意一个数

示例：设置 trunk 1，2，3 的 PVID 为 1000。

```
set trunk 1-3 pvid 1000
```

10.6.5 set vlan

命令功能：使能/关闭 VLAN。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> {**enable**|**disable**}

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
enable	使能 VLAN
disable	关闭 VLAN

示例：使能 vlan 1，5，6，7，12。

```
set vlan 1,5-7,12 enable
```

10.6.6 set vlan add port

命令功能：在 VLAN 中加入指定的端口。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **add port** <*portlist*> [**tag**|**untag**]

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*portlist*>	端口列表
tag	打标签
untag	不打标签，缺省为 untag

示例：在 vlan 1，5，6，7，12 中加入带标签端口 2，8，9。

```
set vlan 1,5-7,12 add port 2,8,9 tag
```

10.6.7 set vlan add trunk

命令功能：在 VLAN 中加入指定的 trunk。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **add trunk** <*trunklist*> [**tag**|**untag**]

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*trunklist*>	Trunk 列表
tag	打标签
untag	不打标签，缺省为 untag

示例：在 vlan 1，5，6，7，12 中加入带标签的 trunk 1。

```
set vlan 1,5-7,12 add trunk 1 tag
```

10.6.8 set vlan delete port

命令功能：删除 VLAN 中指定的端口。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **delete port** <*portlist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*portlist*>	端口列表

示例：删除 vlan 1，5，6，7，12 中的端口 2，8，9。

```
set vlan 1,5-7,12 delete port 2,8,9
```

10.6.9 set vlan delete trunk

命令功能：删除 VLAN 中指定的 trunk。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **delete trunk** <*trunklist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*trunklist*>	Trunk 列表

示例：删除 vlan 1，5，6，7，12 中的 trunk 1。

```
set vlan 1,5-7,12 delete trunk 1
```

10.6.10 set vlan fid

命令功能：配置 VLAN 的 FID。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **fid** <*1-256*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*1-256*>	FID，从 1 到 256 的任意一个数

示例：配置 vlan 1，5，6，7，12 中的 FID 为 1。

```
set vlan 1,5-7,12 fid 1
```

10.6.11 set vlan priority

命令功能：设置 VLAN 的优先级。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **priority** {**off**|**on** <0-7>}

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
off	关闭 VLAN 的优先级
on	开启 VLAN 的优先级
<0-7>	VLAN 的优先级值

示例：设置 vlan 1，5，6，7，12 的优先级为 3。

```
set vlan 1,5-7,12 priority on 3
```

10.6.12 set vlan forbid port

命令功能：设置 VLAN 中禁止学习端口。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **forbid port** < *portlist* >

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*portlist*>	端口列表

示例：禁止 vlan 1，5 中的 port 1 为学习端口。

```
set vlan 1,5 forbid port 1
```

10.6.13 set vlan permit port

命令功能：设置 VLAN 中允许学习的端口。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **permit port** <*portlist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*portlist*>	端口列表

示例：允许 vlan 1，5 中的 port 1 为学习端口。

```
set vlan 1,5 permit port 1
```

10.6.14 set vlan forbid trunk

命令功能：设置 VLAN 中禁止学习的 trunk。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **forbid trunk** <*trunklist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*trunklist*>	Trunk 列表

示例：禁止 vlan 1，5 中的 trunk 1 为学习端口。

```
set vlan 1,5 forbid trunk 1
```

10.6.15 set vlan permit trunk

命令功能：设置 VLAN 中允许学习的 trunk。

命令模式：全局配置模式

命令格式：**set vlan** <*vlanlist*> **permit trunk** <*trunklist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表
<*trunklist*>	Trunk 列表

示例：允许 vlan 1，5 中的 trunk 1 为学习端口。

```
set vlan 1,5 permit trunk 1
```

10.6.16 show vlan

命令功能：显示 VLAN 的信息。

命令模式：所有模式

命令格式：**show vlan** [<*vlanlist*>]

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表

示例一：显示所有 VLAN 的信息。

```
show vlan
```

示例二：显示 vlan 1，5，6，7，12 的信息。

```
show vlan 1,5-7,12
```

10.7 MAC 表操作

10.7.1 set fdb add

命令功能：在地址表中加入静态绑定地址。

命令模式：全局配置模式

命令格式：**set fdb add** <*xx.xx.xx.xx.xx.xx*> **fid** <*1-256*> {**port** <*portname*>|**trunk** <*trunkid*>} [**priority** <0-*7*>]

参数解释：

参数	描述
<*xx.xx.xx.xx.xx.xx*>	MAC 地址
<*1-256*>	FID，从 1 到 256 的任意一个数
<*portname*>	一个端口号或者一个端口名
< *trunkid* >	Trunk ID
< *0-7* >	优先级值

示例一：在地址表中加入 00.00.00.00.11.22，指定 FID 为 1，端口号为 1，优先级值为 3。

```
set fdb add 00.00.00.00.11.22 fid 1 port 1 priority 3
```

示例二：在地址表中加入 00.00.00.00.11.22，指定 FID 为 1，端口名为 userx。

```
set fdb add 00.00.00.00.11.22 fid 1 port userx
```

示例三：在地址表中加入 00.00.00.00.11.22，指定 FID 为 1，trunk 为 1。

```
set fdb add 00.00.00.00.11.22 fid 1 trunk 1
```

10.7.2 set fdb agingtime

命令功能：设置地址老化时间，缺省 240。

命令模式：全局配置模式

命令格式：**set fdb agingtime** <*15-3600*>

参数解释：

参数	描述
<15-3600>	老化时间，从 15 到 3600 的任意一个数，单位：秒

示例：设置地址老化时间为 100s。

```
set fdb agingtime 100
```

10.7.3 set fdb delete

命令功能：在地址表中删除一条记录。

命令模式：全局配置模式

命令格式：**set fdb delete** *<xx.xx.xx.xx.xx.xx>* **fid** *<1-256>*

参数解释：

参数	描述
<xx.xx.xx.xx.xx.xx>	MAC 地址
<1-256>	FID，从 1 到 256 的任意一个数

示例：在地址表中删除 mac 为 00.00.00.00.11.22，FID 为 1 的 fdb 条目。

```
set fdb delete 00.00.00.00.11.22 fid 1
```

10.7.4 set fdb filter

命令功能：配置 fdb 的过滤地址。

命令模式：全局配置模式

命令格式：**set fdb filter** *<xx.xx.xx.xx.xx.xx>* **fid** *<1-256>*

参数解释：

参数	描述
<xx.xx.xx.xx.xx.xx>	MAC 地址
<1-256>	FID，从 1 到 256 的任意一个数

示例：配置 fdb 的过滤地址为 00.00.00.00.11.22，FID 为 1。

```
set fdb filter 00.00.00.00.11.22 fid 1
```

10.7.5 show fdb

命令功能：显示 fdb 的信息。

命令模式：所有模式

命令格式：**show fdb** [**static**|**dynamic**|**filter**] [**detail**]

参数解释：

参数	描述
static	显示静态 fdb 的条目数
dynamic	显示动态 fdb 的条目数
filter	显示静态过滤 fdb 的条目数
detail	显示某类型 fdb 条目的详细信息

10.7.6 show fdb agingtime

命令功能：显示 fdb 地址表的老化时间。

命令模式：所有模式

命令格式：**show fdb agingtime**

10.7.7 show fdb mac

命令功能：显示某 MAC 地址的 fdb 信息。

命令模式：所有模式

命令格式：**show fdb mac** <*xx.xx.xx.xx.xx.xx*>

参数解释：

参数	描述
<*xx.xx.xx.xx.xx.xx*>	MAC 地址

10.7.8 show fdb port

命令功能：显示某端口的 fdb 信息。

命令模式：所有模式

命令格式：**show fdb port** <*portname*>

参数解释：

参数	描述
<*portname*>	一个端口号

10.7.9 show fdb trunk

命令功能：显示某 trunk 的 fdb 信息。

命令模式：所有模式

命令格式：**show fdb trunk** <*trunkid*>

参数解释：

参数	描述
< *trunkid* >	一个 trunk 组号

10.7.10 show fdb vlan

命令功能：显示某 VLAN 的 fdb 信息。

命令模式：所有模式

命令格式：**show fdb vlan** <*vlanname*>

参数解释：

参数	描述
<*vlanname*>	一个 VLAN ID 或者一个 VLAN 名

10.8 LACP 配置

10.8.1 set lacp

命令功能：使能/关闭 LACP。

命令模式：全局配置模式

命令格式：**set lacp** {**enable**|**disable**}

参数解释：

参数	描述
enable	使能 LACP
disable	关闭 LACP

10.8.2 set lacp aggregator add port

命令功能：在 LACP 聚合组中加入指定端口。

命令模式：全局配置模式

命令格式：**set lacp aggregator** <*trunkid*> **add port** <*portlist*>

参数解释：

参数	描述
<*trunkid*>	聚合组号
<*portlist*>	端口列表，最多聚合 8 个端口

示例：在聚合组 1 中加入端口 1，5，6，7。

```
set lacp aggregator 1 add port 1,5-7
```

10.8.3 set lacp aggregator delete port

命令功能：从 LACP 聚合组中删除指定端口。

命令模式：全局配置模式

命令格式：**set lacp aggregator** <*trunkid*> **delete port** <*portlist*>

参数解释：

参数	描述
<*trunkid*>	聚合组号
<*portlist*>	端口列表

示例：从聚合组 1 中删除端口 1，5，6，7。

```
set lacp aggregator 1 delete port 1,5-7
```

10.8.4 set lacp aggregator mode

命令功能：设置聚合组聚合模式。

命令模式：全局配置模式

命令格式：**set lacp aggregator** <*trunkid*> **mode** {**dynamic**|**static | mixed** }

参数解释：

参数	描述
<*trunkid*>	聚合组号
static	聚合模式为静态
dynamic	聚合模式为动态
mixed	聚合模式为混合

示例：设置聚合组 1 聚合模式为动态。

```
set lacp aggregator 1 mode dynamic
```

10.8.5 set lacp port mode

命令功能：设置端口参与聚合的模式。

命令模式：全局配置模式

命令格式：**set lacp port** <*portlist*> **mode** {**active**|**passive**}

参数解释：

参数	描述
<*portlist*>	端口列表
active	LACP 端口为主动协商模式
passive	LACP 端口为被动协商模式

示例：设置端口 1，5，6，7 参与聚合的模式为主动协商模式。

```
set lacp port 1,5-7 mode active
```

10.8.6 set lacp port timeout

命令功能：设置参与聚合的端口的超时情况。

命令模式：全局配置模式

命令格式：**set lacp port** <*portlist*> **timeout** {**long**|**short**}

参数解释：

参数	描述
<*portlist*>	端口列表
short	端口为短超时
long	端口为长超时

示例：设置参与聚合的端口 1，5，6，7 为长超时。

```
set lacp port 1,5-7 timeout long
```

10.8.7 set lacp priority

命令功能：设置 LACP 的优先级。

命令模式：全局配置模式

命令格式：**set lacp priority** <*1-65535*>

参数解释：

参数	描述
<*1-65535*>	优先级，从 1 到 65535 的任意一个数，缺省为 32768

示例：设置 LACP 的优先级为 100。

```
set lacp priority 100
```

10.8.8 show lacp

命令功能：显示 LACP 的配置信息。

命令模式：所有模式

命令格式：**show lacp**

10.8.9 show lacp aggregator

命令功能：显示 LACP 聚合组聚合信息。

命令模式：所有模式

命令格式：**show lacp aggregator** [<*trunkid*>]

参数解释：

参数	描述
<*trunkid*>	聚合组号

示例一：显示所有 LACP 聚合组的信息。

```
show lacp aggregator
```

示例二：显示 LACP 聚合组 1 的信息。

```
show lacp aggregator 1
```

10.8.10 show lacp port

命令功能：显示 LACP 参与聚合的端口信息。

命令模式：所有模式

命令格式：**show lacp port** [<*portlist* >]

参数解释：

参数	描述
<*portlist*>	端口列表

示例一：显示所有 LACP 参与聚合的端口信息。

```
show lacp port
```

示例二：显示 LACP 参与聚合的端口 1，5，6，7 的信息。

```
show lacp port 1,5-7
```

10.9 IGMP Snooping 配置

10.9.1 set igmp snooping

命令功能：允许/禁止组播监听。

命令模式：全局配置模式

命令格式：**set igmp snooping** {**enable**|**disable**}

参数解释：

参数	描述
enable	允许组播监听
disable	禁止组播监听

10.9.2 set igmp snooping add vlan

命令功能：添加组播监听 VLAN。

命令模式：全局配置模式

命令格式：**set igmp snooping add vlan** <*vlanlist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表

示例：添加组播监听 vlan 1，5，6，7，12。

```
set igmp snooping add vlan 1,5-7,12
```

10.9.3 set igmp snooping crossvlan

命令功能：允许/禁止跨 VLAN 组播监听。

命令模式：全局配置模式

命令格式：**set igmp snooping crossvlan** {**enable**|**disable**}

参数解释：

参数	描述
enable	允许跨 VLAN 组播监听
disable	禁止跨 VLAN 组播监听

示例：允许跨 VLAN 组播监听。

```
set igmp snooping crossvlan enable
```

10.9.4 set igmp snooping delete vlan

命令功能：删除组播监听 VLAN。

命令模式：全局配置模式

命令格式：**set igmp snooping delete vlan** *<vlanlist>*

参数解释：

参数	描述
<vlanlist>	VLAN 列表

示例：删除组播监听 vlan 1，5，6，7，12。

```
set igmp snooping delete vlan 1,5-7,12
```

10.9.5 set igmp snooping fastleave

命令功能：允许/禁止快速离开。

命令模式：全局配置模式

命令格式：**set igmp snooping fastleave** {**enable**|**disable**}

参数解释：

参数	描述
enable	允许快速离开
disable	禁止快速离开

10.9.6 set igmp snooping lastmember_query

命令功能：设置最后的成员查询周期。

命令模式：全局配置模式

命令格式：**set igmp snooping lastmember_query** *<10-250>*

参数解释：

参数	描述
<10-250>	最后的成员查询周期，单位：1/10 秒，缺省为 10（1s）

示例：设置最后的成员查询周期为 10s。

```
set igmp snooping lastmember_query 100
```

10.9.7 set igmp snooping query vlan

命令功能：开启/关闭组播对 VLAN 的轮询。

命令模式：全局配置模式

命令格式：**set igmp snooping query vlan** *<vlanlist>* {**enable**|**disable**}

参数解释：

参数	描述
<vlanlist>	VLAN 列表，只能是加入组播的 VLAN
enable	开启组播轮询
disable	关闭组播论询

示例：开启组播对 vlan 1，7，12 的轮询。

```
set igmp snooping query vlan 1,7,12 enable
```

10.9.8 set igmp snooping query_interval

命令功能：设置查询周期。

命令模式：全局配置模式

命令格式：**set igmp snooping query_interval** *<10-2147483647>*

参数解释：

参数	描述
<10-2147483647>	查询周期，单位：1/10 秒，缺省为 1250（125s）

示例：设置查询周期为 100s。

```
set igmp snooping query_interval 1000
```

10.9.9 set igmp snooping response_interval

命令功能：设置查询响应周期。

命令模式：全局配置模式

命令格式：**set igmp snooping response_interval** *<10-250>*

参数解释：

参数	描述
<10-250>	查询响应周期，单位：1/10 秒，缺省为 100（10s）

示例：设置查询响应周期为 12s。

```
set igmp snooping response_interval 120
```

10.9.10 set igmp snooping timeout

命令功能：设置组播成员/路由超时。

命令模式：全局配置模式

命令格式：**set igmp snooping timeout** *<100-2147483647>* {**host**|**router**}

参数解释：

参数	描述
<100-2147483647>	设置的超时时间，单位：1/10 秒，缺省为 2600（260s）
host	设置成员超时
router	设置路由超时

示例：设置组播成员超时为 100s。

```
set igmp snooping timeout 1000 host
```

10.9.11 set igmp snooping vlan add group

命令功能：在指定 VLAN 中添加静态组播组。

命令模式：全局配置模式

命令格式：**set igmp snooping vlan** *<1-4094>* **add group** *<A.B.C.D>*

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
<A.B.C.D>	IP 地址，范围在 224.x.x.x 到 239.x.x.x 之间，不包括 224.0.0.x

示例一：在 vlan 1 中添加静态组播组 230.40.44.167。

```
set igmp snooping vlan 1 add group 230.40.44.167
```

示例二：在 VLAN 名为 group1 中添加静态组播组 230.40.44.167。

```
set igmp snooping vlan group1 add group 230.40.44.167
```

10.9.12 set igmp snooping vlan delete group

命令功能：在指定 VLAN 中删除静态组播组。

命令模式：全局配置模式

命令格式：**set igmp snooping vlan** *<1-4094>* **delete group** *<A.B.C.D>*

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
<A.B.C.D>	IP 地址，范围在 224.x.x.x 到 239.x.x.x 之间，不包括 224.0.0.x

示例一：在 vlan 1 中删除静态组播组 230.40.44.167。

```
set igmp snooping vlan 1 delete group 230.40.44.167
```

示例二：在 VLAN 名为 group1 中删除静态组播组 230.40.44.167。

```
set igmp snooping vlan group1 delete group 230.40.44.167
```

10.9.13 set igmp snooping vlan add group port | trunk

命令功能：在指定 VLAN 中添加基于端口或聚合口的静态组播组。

命令模式：全局配置模式

命令格式：**set igmp snooping vlan** *<1-4094>* **add group** *<A.B.C.D>* port *<portlist>*

或 **set igmp snooping vlan** *<1-4094>* **add group** *<A.B.C.D>* trunk *<trunklist>*

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
<A.B.C.D>	IP 地址，范围在 224.x.x.x 到 239.x.x.x 之间，不包括 224.0.0.x
<portlist> 或 *<trunklist>*	端口列表 或 聚合口列表

示例一：在 vlan 1 中添加基于普通端口 1、2、3、5、8 的静态组播组 230.45.44.165。

```
set igmp snooping vlan 1 add group 230.45.44.165 port 1-3,5,8
```

示例二：在 vlan 名为 group1 中添加基于 trunk 口 1、2 的静态组播组 230.45.44.165。

```
set igmp snooping vlan group1 add group 230.45.44.165 trunk 1-2
```

10.9.14 set igmp snooping vlan delete group port | trunk

命令功能：在指定组播监听 VLAN 中删除基于端口或聚合口的静态组播组。

命令模式：全局配置模式

命令格式：**set igmp snooping vlan** *<1-4094>* **delete group** *<A.B.C.D>* port *<portlist>*

或 **set igmp snooping vlan** *<1-4094>* **delete group** *<A.B.C.D>* trunk *<trunklist>*

或 **set igmp snooping vlan** *<1-4094>* **delete group** *<A.B.C.D>*

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
<A.B.C.D>	IP 地址，范围在 224.x.x.x 到 239.x.x.x 之间，不包括 224.0.0.x
<portlist> 或 *<trunklist>*	端口列表 或 聚合口列表

示例一：在 vlan 1 中删除基于普通端口 1、2、3、5、8 的静态组播组 230.45.44.165。

```
set igmp snooping vlan 1 delete group 230.45.44.165 port 1-3,5,8
```

示例二：在 vlan 名为 group1 中删除基于 trunk 口 1、2 的静态组播组 230.45.44.165。

```
set igmp snooping vlan group1 delete group 230.45.44.165 trunk 1-2
```

示例三：在 vlan 名为 group1 中删除基于所有 trunk 口或普通端口的静态组播组 230.45.44.165。

```
set igmp snooping vlan group1 delete group 230.45.44.165
```

10.9.15 set igmp snooping vlan add smr port | trunk

命令功能：在指定组播监听 VLAN 中加入静态路由端口或静态路由聚合口。

命令模式：全局配置模式

命令格式：**set igmp snooping vlan** *<1-4094>* **add smr port** *<portlist>*

或 **set igmp snooping vlan** *<1-4094>* **add smr trunk** <trunk*list*>

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
<portlist> 或 <trunk*list*>	端口列表或聚合口列表

示例一：在 vlan 1 中添加静态路由端口 2，8，9。

```
set igmp snooping vlan 1 add smr port 2,8,9
```

示例二：在 vlan 名为 smr1 中添加静态路由聚合口 1、2。

```
set igmp snooping vlan smr1 add smr trunk 1-2
```

10.9.16 set igmp snooping vlan delete smr port | trunk

命令功能：在指定组播监听 VLAN 中删除静态路由端口或静态路由聚合口。

命令模式：全局配置模式

命令格式：**set igmp snooping vlan** *<1-4094>* **delete smr port** *<portlist>*

或 **set igmp snooping vlan** *<1-4094>* **delete smr trunk** <trunk*list*>

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
<portlist> 或 <trunk*list*>	端口列表或聚合口列表

示例一：在 vlan 1 中删除静态路由端口 2，8，9。

```
set igmp snooping vlan 1 delete smr port 2,8,9
```

示例二：在 VLAN 名为 smr1 中添加静态路由聚合口 1、2。

```
set igmp snooping vlan smr1 delete smr trunk 1-2
```

10.9.17 set igmp snooping add maxnum vlan

命令功能：设置指定组播监听 VLAN 的最大组播组数目限制。

命令模式：全局配置模式

命令格式：**set igmp snooping add maxnum** *<1-256>* **vlan** *<vlanlist>*

参数解释：

参数	描述
<1-256>	允许加入的最大组播组数目
<vlanlist>	VLAN 列表

示例一：设置组播监听 vlan 1，5，6，7，12 的最大组播数目均为 7。

```
set igmp snooping add maxnum 7 vlan 1,5-7,12
```

10.9.18 set igmp snooping delete maxnum vlan

命令功能：清除指定组播监听 VLAN 的最大组播组数目限制。

命令模式：全局配置模式

命令格式：**set igmp snooping delete maxnum vlan** <*vlanlist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表

示例一：清除组播监听 vlan 1，5，6，7，12 的最大组播数目限制。

```
set igmp snooping add maxnum vlan 1,5-7,12
```

10.9.19 set igmp filter

命令功能：允许/禁止组播过滤功能。

命令模式：全局配置模式

命令格式：**set igmp filter** {**enable**|**disable**}

参数解释：

参数	描述
enable	允许组播过滤
disable	禁止组播过滤

10.9.20 set igmp filter add groupip vlan

命令功能：添加指定组播监听 VLAN 的组播过滤组地址。

命令模式：全局配置模式

命令格式：**set igmp filter add groupip** <*A.B.C.D*> vlan <*vlanlist*>

参数解释：

参数	描述
<*A.B.C.D*>	IP 地址，范围在 224.x.x.x 到 239.x.x.x 之间，不包括 224.0.0.x
<*vlanlist*>	VLAN 列表

示例一：在 vlan 1，7，8，9，18 上添加组播过滤组地址 230.40.44.167。

```
set igmp filter add groupip 230.40.44.167 vlan 1,7-9,18
```

10.9.21 set igmp filter delete groupip vlan

命令功能：删除指定的组播监听 VLAN 的组播过滤组地址。

命令模式：全局配置模式

命令格式：**set igmp filter delete groupip** <*A.B.C.D*> vlan <*vlanlist*>

参数解释：

参数	描述
<*A.B.C.D*>	IP 地址，范围在 224.x.x.x 到 239.x.x.x 之间，不包括 224.0.0.x
<*vlanlist*>	VLAN 列表

示例一：删除在 vlan 1，7，8，9，18 上的组播过滤组地址 230.40.44.167。

```
set igmp filter delete groupip 230.40.44.167 vlan 1,7-9,18
```

10.9.22 set igmp filter add sourceip vlan

命令功能：添加指定组播监听 VLAN 的组播过滤源地址。

命令模式：全局配置模式

命令格式：**set igmp filter add sourceip** <*A.B.C.D*> vlan <*vlanlist*>

参数解释：

参数	描述
<*A.B.C.D*>	IP 地址，范围为 A、B 或 C 类 IP 地址
<*vlanlist*>	VLAN 列表

示例一：在 vlan 1，7，8，9，18 上添加组播过滤源地址 210.40.44.167。

```
set igmp filter add sourceip 210.40.44.167 vlan 1,7-9,18
```

10.9.23 set igmp filter delete sourceip vlan

命令功能：删除指定组播监听 VLAN 的组播过滤源地址。

命令模式：全局配置模式

命令格式：**set igmp filter delete sourceip** <*A.B.C.D*> vlan <*vlanlist*>

参数解释：

参数	描述
<A.B.C.D>	IP 地址，范围为 A、B 或 C 类 IP 地址
<vlanlist>	VLAN 列表

示例一：删除 vlan 1，7，8，9，18 上的组播过滤源地址 210.40.44.167。

```
set igmp filter delete sourceip 210.40.44.167 vlan 1,7-9,18
```

10.9.24 show igmp snooping

命令功能：显示组播监听的配置。

命令模式：所有模式

命令格式：**show igmp snooping**

10.9.25 show igmp snooping vlan

命令功能：显示组播监听结果。

命令模式：所有模式

命令格式：**show igmp snooping vlan** [*<1-4094>* [**host**|**router**]]

参数解释：

参数	描述
<1-4094>	一个 VLAN ID 或者一个 VLAN 名
host	显示成员的监听结果
router	显示路由的监听结果

示例一：显示所有 VLAN 的组播监听结果。

```
show igmp snooping vlan
```

示例二：显示 vlan 1 的组播监听结果。

```
show igmp snooping vlan 1
```

示例三：显示 VLAN 名为 group1 的组播监听结果。

```
show igmp snooping vlan group1
```

示例四：显示 vlan 1 组播路由的监听结果。

```
show igmp snooping vlan 1 router
```

10.9.26 show igmp filter

命令功能：显示组播过滤的配置。

命令模式：所有模式

命令格式：**show igmp filter**

10.9.27 show igmp filter vlan

命令功能：显示指定监听 VLAN 中的组播过滤地址条目。

命令模式：所有模式

命令格式：**show igmp filter vlan** <*1-4094*>

参数解释：

参数	描述
<*1-4094*>	一个 VLAN ID 或者一个 VLAN 名

示例一：显示 vlan 1 的组播过滤地址条目。

```
show igmp filter vlan 1
```

示例二：显示 VLAN 名为 filter1 的组播过滤地址条目。

```
show igmp filter vlan filter1
```

10.10 IPTV 配置

10.10.1 clear iptv cac-rule

命令功能：删除 CAC（频道访问控制）规则。

命令模式：NAS 配置模式

命令格式：**clear iptv cac-rule** <*rulelist*>

命令参数解释：

参数	描述
<*rulelist*>	一个或多个规则号，范围 1~64

删除 CAC 规则 1：

```
zte(cfg)#config nas
zte(cfg-nas)#clear iptv cac-rule 1
```

10.10.2 clear iptv channel

命令功能：删除频道。

命令模式：NAS 配置模式

命令格式：**clear iptv channel** <*channellist*>

命令参数解释：

参数	描述
<*channellist*>	一个或多个频道号，范围 0~263

删除频道 1：

```
zte(cfg-nas)#clear iptv channel 1
```

10.10.3 clear iptv client

命令功能：删除 iptv 用户。

命令模式：NAS 配置模式

命令格式：**clear iptv client** [{**index** <*client-index*>|**port** <*portname*>|**vlan** <*vlanid*>}]

命令参数解释：

参数	描述
<*client-index*>	用户编号，范围 0~63
<*portname*>	接口名
<*vlanid*>	Vlan 的 ID 号，范围 1~4094

删除接口 fei_1/1 下的用户：

```
zte(cfg)#config nas
zte(cfg-nas)#clear iptv client port fei_1/1
```

10.10.4 create iptv cac-rule

命令功能：创建 CAC（频道访问控制）规则。

命令模式：NAS 配置模式

命令格式：**create iptv cac-rule** <*rule-id*> [**port** <*port-name*>] [**vlan** <*vlan-id*>] [**mac-base**]

命令参数解释：

参数	描述
<*rule-id*>	规则的 ID 号，范围 1~64
<*port-name*>	物理接口名
<*vlan-id*>	VLAN 的 ID 号，范围 1~4094
mac-base	端口下用户的加入和离开必须是基于同一个 mac 地址

创建一个针对接口 1，vlan 1，基于 MAC 地址的 CAC 规则 1：

```
zte(cfg)#config nas
zte(cfg-nas)#create iptv cac-rule 1 port 1 vlan 1 mac-base
```

10.10.5 create iptv channel

命令功能：创建与组播组对应的频道。

命令模式：NAS 配置模式

命令格式：**create iptv channel** {**special** <*channel-id*> **address** <*address*> | **general** < *channel-id* > }

命令参数解释：

参数	描述
special <*channel-id*>	特定频道的 ID 号，范围 0~255
general <*channel-id*>	通用频道的 ID 号，范围 256~263
<*address*>	组播组地址，范围 224.0.0.0-239.255.255.255

特定频道与组播组地址一一对应，通用频道映射所有组播组。

创建与组播组 224.1.1.1 关联的特定频道 1：

```
zte(cfg)#config nas
zte(cfg-nas)#create iptv channel special 1 address 224.1.1.1
```

10.10.6 iptv cac-rule name

命令功能：给 CAC 规则指定名称。

命令模式：NAS 配置模式

命令格式：**iptv cac-rule** <*rule-list*> **name** <*rule-name*>

命令参数解释：

参数	描述
<*rule-list*>	一个或多个规则号，范围 1~64

<rule-name>	规则名，长度 1~50

给规则 1 指定名称 zte：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv cac 1 name zte
```

10.10.7 iptv cac-rule prvcount

命令功能：配置 CAC 规则的最大预览次数。

命令模式：NAS 配置模式

命令格式：**iptv cac-rule** *<rule-list>* **prvcount** *<preview-count>*

命令参数解释：

参数	描述
<rule-list>	一个或多个规则号，范围 1~64
<preview-count>	CAC 规则下预览用户的最大预览次数，范围 0~65535

如果不对一个规则配置最大预览次数，则此规则的最大预览次数为全局最大预览次数，此预览次数为这个规则在同一块线卡上的最大预览次数。

指定规则 1 的最大预览次数为 20：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv cac-rule 1 prvcount 20
```

10.10.8 iptv cac-rule prvinterval

命令功能：配置 CAC 规则的最小预览间隔。

命令模式：NAS 配置模式

命令格式：**iptv cac-rule** *<rule-list>* **prvinterval** *<preview-interval>*

命令参数解释：

参数	描述
<rule-list>	一个或多个规则号，范围 1－64
<preview-interval>	CAC 规则下预览用户的最小预览间隔，范围 2－65535

如果不对一个规则配置最小预览间隔，则此规则的最小预览间隔为全局最小预览间隔。

指定规则 1 的最小预览间隔为 20 秒：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv cac-rule 1 prvinterval 20
```

10.10.9 iptv cac-rule prvtime

命令功能：配置 CAC 规则的最大预览时间。

命令模式：NAS 配置模式

命令格式：**iptv cac-rule** <*rule-list*> **prvtime** <*preview-time*>

命令参数解释：

参数	描述
<*rule-list*>	一个或多个规则号，范围 1~64
<*preview-time*>	CAC 规则下预览用户的最大预览时间，范围 1~65535

如果不对一个规则配置最大预览时间，则此规则的最大预览时间为全局最大预览时间。

指定规则 1 的最大预览时间为 20 秒：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv cac-rule 1 prvtime 20
```

10.10.10 iptv cac-rule right

命令功能：配置 CAC 规则对频道的权限。

命令模式：NAS 配置模式

命令格式：**iptv cac-rule** <*rule-list*> **right** {**order**|**preview**|**query**} <*channel-list*>

命令参数解释：

参数	描述
<*rule-list*>	一个或多个规则号，范围 1~64
< *channel-list*>	一个或多个频道号，范围 0~263
order	定购频道，用户可以不受限的看这个频道
preview	预览频道，用户受预览次数、预览时间和预览间隔的限制
query	指定接收查询报文的权限

一个规则对一个频道只允许有一个权限。

指定规则 1 有预览频道 1 的权限：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv cac-rule 1 right preview 1
```

10.10.11 iptv channel mvlan

命令功能：指定频道的所在的 vlan。

命令模式：NAS 配置模式

命令格式：**iptv channel** <*channel-list*> **mvlan** <*vlan-id*>

命令参数解释：

参数	描述
< *channel-list*>	一个或多个频道号，范围 0~263
<*vlan-id*>	mvlan 的 id 号，范围 1~4094

指定频道 1 所在的 vlan 为 100：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv channel 1 mvlan 100
```

10.10.12 iptv channel name

命令功能：给频道取个名字。

命令模式：NAS 配置模式

命令格式：**iptv channel** <*channel-list*> **name** <*channel-name*>

命令参数解释：

参数	描述
< *channel-list*>	一个或多个频道号，范围 0~263
<*channel-name*>	频道名，长度 1~50

指定频道 1 的名字为 cctv1：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv channel 1 name cctv1
```

10.10.13 iptv control

命令功能：开启或关闭 iptv 控制功能。

命令模式：NAS 配置模式

命令格式：**iptv control** {**enable**|**disable**}

命令参数解释：

参数	描述
enable	开启 iptv 的控制功能
disable	关闭 iptv 的控制功能

开启 iptv 的控制功能：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control enable
```

10.10.14 iptv control log-time

命令功能：设置用户的最小识别时间。

命令模式：NAS 配置模式

命令格式：**iptv control log-time** *<log-time>*

命令参数解释：

参数	描述
<log-time>	识别用户的最小时间，范围为 1~65534

如果预览用户的预览时间小于最小识别时间，则不计预览次数。

设置用户的最小识别时间为 10 秒：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control log-time 10
```

10.10.15 iptv control prvcount count

命令功能：设置全局最大预览次数。

命令模式：NAS 配置模式

命令格式：**iptv control prvcount count** *<preview-count>*

命令参数解释：

参数	描述
<preview-count>	全局最大预览次数，范围为 0~65535

全局最大预览次数作为 CAC 规则的缺省最大预览次数。

设置全局最大预览次数为 20 次：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control prvcount count 20
```

10.10.16 iptv control prvcount reset-period

命令功能：设置将 CAC 规则预览次数清零的周期。

命令模式：NAS 配置模式

命令格式：**iptv control prvcount reset-period** *<reset-period>*

命令参数解释：

参数	描述
<reset-period>	清零 CAC 规则的预览次数周期，范围 1~4294967295

设置清零预览次数的周期为 600s：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control prvcount reset-period 600
```

10.10.17 iptv control prvinterval

命令功能：设置全局的最小预览间隔。

命令模式：NAS 配置模式

命令格式：**iptv control prvinterval** *<preview-interval>*

命令参数解释：

参数	描述
<preview-interval>	最小预览间隔，范围 2~65535

全局最小预览间隔作为 CAC 规则的缺省最小预览间隔。

设置全局最小预览间隔为 20s：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control prvinterval 20
```

10.10.18 iptv control prvtime

命令功能：设置全局的最大预览时间。

命令模式：NAS 配置模式

命令格式：**iptv control prvtime** <*preview-time*>

命令参数解释：

参数	描述
<*preview-time*>	最大预览时间，范围 1~65535

全局最大预览时间作为 CAC 规则的缺省最大预览时间。

设置全局最大预览时间为 20s：

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control prvtime 20
```

10.10.19 show iptv cac-rule

命令功能：显示已配的 CAC 规则。

命令模式：除用户模式外的所有模式

命令格式：**show iptv cac-rule** [{**id** <*rule-id*>|**name** <*rule-name*>}]

命令参数解释：

参数	描述
<*rule-id*>	规则的 ID 号，范围 1~64
<*rule-name*>	规则名，长度 1~50

显示所有的 CAC 规则：

```
zte(cfg)#show iptv cac-rule
  MaxRuleNum:256
  CurRuleNum:3
  HisRuleNum:3

  Id   Name          Port         Vlan   Order Prview Query  Mac-base
  ---- ------------ -----------  -----  ----- -----  -----  -------
  1    zte1          1                   1     1      1      FALSE
  2    zte2          2            1      2     0      1      TRUE
  3    zte3                       2      0     1             FALSE
```

显示信息说明：

信息	描述
MaxRuleNum	最大规则数
CurRuleNum	当前已配的规则数

HisRuleNum	曾经配置的规则数
Id	规则的 ID 号
Name	规则名
Port	规则针对的接口
Vlan	规则针对的 vlan
Mac-base	是否基于端口
Order	定购的频道数
Prview	预览的频道数
Query	以这个规则所针对的端口为源端口的频道数

显示 CAC 规则 1：

```
zte(cfg)#show iptv cac-rule id 1
  RuleNo             :1             UserName          :zte1
  Port               :              Vlan              :
  MacBase            :FALSE

  MaxPrvCount        :10            MinPrvInterval    :15
  MaxPrvTime         :60            CurPrvCount       :0
  CurOrdUserChanNum  :0             HisOrdUserChanNum :0
  CurPrvUserChanNum  :0             HisPrvUserChanNum :0
  CurUserChanNum     :0             HisUserChanNum    :0

  Order              :1             Preview           :1
  Query              :1

  Order channels     :1
  Preview channels   :2
  Query channels     :3
```

显示信息说明：

信息	描述
RuleNo	规则的 ID 号
UserName	规则名
Port	规则针对的接口
Vlan	规则针对的 vlan
MacBase	是否基于端口
MaxPrvCount	最大预览次数
MinPrvInterval	最小预览间隔
MaxPrvTime	最大预览时间
CurPrvCount	当前预览次数
CurOrdUserChanNum	当前定购用户频道数

HisOrdUserChanNum	历史定购用户频道数
CurPrvUserChanNum	当前预览用户频道数
HisPrvUserChanNum	历史预览用户频道数
CurUserChanNum	当前用户频道数
HisUserChanNum	历史用户频道数
Order	定购的频道数
Preview	预览的频道数
Query	可以接受查询报文的频道数
Order channels	定购的频道号
Preview channels	预览的频道号
Query channels	查询的频道号

10.10.20 show iptv channel

命令功能：显示已配的频道信息。

命令模式：除用户模式外的所有模式

命令格式：**show iptv channel** [{id <*channel-id*>|name <*channel-name*>}]

命令参数解释：

参数	描述
<*channel-id*>	频道号，范围 0~263
<*channel-name*>	频道名，长度 1~50

显示所有的频道：

```
zte(cfg)#show iptv channel
  MaxChannelNum:264
  CurChannelNum:3
  HisChannelNum:3
  Id     Name           GroupIp         MVlan
  -----  -------------  -------------  ------
  1      cctv1          224.1.1.1      100
  2      cctv2          224.1.1.2      101
  3      cctv3          224.1.1.3      102
```

显示信息说明：

信息	描述
MaxChannelNum	可配的最大频道数
CurChannelNum	当前已配的频道数
HisChannelNum	曾经配置的频道数

Id	频道号
Name	频道名
GroupIp	组播组地址
MVlan	组播组所属 vlan

10.10.21 show iptv client

命令功能：显示 iptv 用户信息。

命令模式：除用户模式外的所有模式

命令格式：**show iptv client** [{**channel** *<channel-id>*| **index** *<client-index>* |**name** *<user-name>*| **mac** *<HH.HH.HH.HH.HH.HH>*| **port** *<portid>*[**vlan** *<vlanid>*] | **vlan** *<vlanid>*}]

命令参数解释：

参数	描述
<channel-id>	频道号，范围 0~263
<client-index>	用户编号，范围 0~63
<user-name>	用户名，长度 1~50
<HH.HH.HH.HH.HH.HH>	用户的 MAC 地址
<portid>	用户登录端口号
<vlanid>	用户所属 VLAN 号

显示所有 iptv 用户：

```
zte(cfg)#show iptv client
  MaxClientNum:64
  CurClientNum:1
  HisClientNum:1

  Index   Name              Rule    Vlan    Port    ChNum
  ------  ----------------  ------  ------  ------  ------
  0       zte1              1       1       4       1
```

显示信息说明：

信息	描述
MaxClientNum	最大用户数
CurClientNum	当前用户数
HisClientNum	历史用户数
Index	用户编号

Name	用户名
Port	用户登陆端口
Vlan	用户所属 vlan
Rule	用户匹配的规则号
ChNum	用户请求加入的频道数

显示用户 0 的信息：

```
zte(cfg)#show iptv client index 0
  Index    :0                     Name  :zte1
  Rule     :1                     Vlan  :1
  Port     :4                     ChNum :1
  Mac      :00.14.2a.22.6d.06     Ip    :10.40.45.30

  Channel  UserType     MultiAddress      ElapsedTime
  -------  ----------  ----------------  --------------
  1        order         224.1.1.1         0:0:4:21
  1        preview      224.1.1.2         0:0:0:20
```

显示信息说明：

信息	描述
Index	用户编号
Name	用户名
Port	用户登陆端口
Vlan	用户所属 vlan
Rule	用户匹配的规则号
ChNum	用户请求加入的频道数
Channel	频道号
UserType	用户对频道的权限
MultiAddress	频道的组播地址
ElapsedTime	在线时间

10.10.22 show iptv control

命令功能：显示 IPTV 的全局配置。

命令模式：除用户模式外的所有模式

命令格式：**show iptv control**

显示所有的频道：

```
zte(cfg)#show iptv control
  LogTime      :10                MaxPrvCount   :10
```

```
MinPrvInterval:15                MaxPrvTime    :60
ResetPeriod   :300               State         :enabled
```

显示信息说明：

信息	描述
State	IPTV 的状态
LogTime	用户的最小识别时间
MaxPrvTime	最大预览次数
ResetPeriod	清零预览次数的周期
MinPrvInterval	最小预览间隔
MaxPrvTime	最大预览时间

10.11 MSTP 配置

10.11.1 clear stp instance

命令功能：删除实例。

命令模式：全局配置模式

命令格式：**clear stp instance** *<0-15>*

参数解释：

参数	描述
<0-15>	实例号，从 1 到 15 之间的任意一个数

使用说明：实例 0 不能被删除。

示例：删除 instance 1。

```
clear stp instance 1
```

10.11.2 clear stp instance port cost

命令功能：删除实例端口 cost 值

命令模式：全局配置模式

命令格式：**clear stp instance***<0-15>***port** *<portname>* **cost**

参数解释：

参数	描述
<0-15>	实例号，从 0 到 15 之间的任意一个数

<portname>	端口号

示例：删除 instance 1 中端口 2 的 cost。

```
clear stp instance 1 port 2 cost
```

10.11.3 clear stp instance trunk cost

命令功能：删除实例 trunk cost 值

命令模式：全局配置模式

命令格式：**clear stp instance**<*0-15*>**trunk**<*trunkid*>**cost**

参数解释：

参数	描述
<0-15>	实例号，从 0 到 15 之间的任意一个数
<trunkid>	一个 trunk 号

示例：删除 instance 1 中 Trunk 2 的 cost。

```
clear stp instance 1 trunk 2 cost
```

10.11.4 clear stp name

命令功能：删除 STP 区域名称。

命令模式：全局配置模式

命令格式：**clear stp name**

10.11.5 set stp

命令功能：使能/关闭 STP，缺省关闭 STP。

命令模式：全局配置模式

命令格式：**set stp** {**enable**|**disable**}

参数解释：

参数	描述
enable	使能 STP
disable	关闭 STP

10.11.6 set stp agemax

命令功能：设置 STP 的老化时间。

命令模式：全局配置模式

命令格式：**set stp agemax** <*6-40*>

参数解释：

参数	描述
<*6-40*>	STP 的老化时间，单位：秒

示例：设置 STP 的老化时间为 30s。

```
set stp agemax 30
```

10.11.7 set stp edge-port

命令功能：增加/删除 STP 的边缘端口。

命令模式：全局配置模式

命令格式：**set stp edge-port** {**add**|**delete**} **port** <*portlist*>

参数解释：

参数	描述
<*portlist*>	端口列表

示例：设置端口 1 为 STP 边缘端口。

```
set stp edge-port add port 1
```

10.11.8 set stp forceversion

命令功能：设置 STP 的强制类型为 mstp/rstp/stp。

命令模式：全局配置模式

命令格式：**set stp forceversion** {**mstp**|**rstp**|**stp**}

参数解释：

参数	描述
mstp	设置 STP 的强制类型为 mstp
rstp	设置 STP 的强制类型为 rstp
stp	设置 STP 的强制类型为 stp

示例：设置 STP 的强制类型为 stp。

```
set stp forceversion stp
```

10.11.9 set stp forwarddelay

命令功能：设置 STP 的转发延迟时间。

命令模式：全局配置模式

命令格式：**set stp forwarddelay** *<4-30>*

参数解释：

参数	描述
<4-30>	STP 的转发延迟时间，单位：秒

示例：设置 STP 的转发延迟时间为 10s。

```
set stp forwarddelay 10
```

10.11.10 set stp hellotime

命令功能：设置 STP 的通告间隔时间。

命令模式：全局配置模式

命令格式：**set stp hellotime** *<1-10>*

参数解释：

参数	描述
<1-10>	STP 的通告间隔时间，单位：秒

示例：设置 STP 的通告间隔时间为 6s。

```
set stp hellotime 6
```

10.11.11 set stp hmd5-digest

命令功能：设置 hmd5-digest 的值。

命令模式：全局配置模式

命令格式：**set stp hmd5-digest {CISCO|HUAWEI}***<0x00..0-0xff..f>*

参数解释：

参数	描述
CISCO	与 CISCO 设备对接时使用
HUAWEI	与 HUAWEI 设备对接时使用
<0x00..0-0xff..f>	32 比特的十六进制值

10.11.12 set stp hmd5-key

命令功能：设置 hmd5-key 的值。

命令模式：全局配置模式

命令格式：**set stp hmd5-key {CISCO|HUAWEI}** *<0x00..0-0xff..f>*

参数解释：

参数	描述
CISCO	与 CISCO 设备对接时使用
HUAWEI	与 HUAWEI 设备对接时使用
<0x00..0-0xff..f>	32 比特的十六进制值

10.11.13 set stp hopmax

命令功能：设置 MST 的任意两终端间的最大跳数。

命令模式：全局配置模式

命令格式：**set stp hopmax** *<1-40>*

参数解释：

参数	描述
<1-40>	MST 的任意两终端间的最大跳数

示例：设置 MST 的任意两终端间的最大跳数为 30。

```
set stp hopmax 30
```

10.11.14 set stp instance bridgeprio

命令功能：设置实例中桥的优先级。

命令模式：全局配置模式

命令格式：**set stp instance** *<0-15>* **bridgeprio** *<0-61440>*

参数解释：

参数	描述
<0-15>	实例号，从 0 到 15 之间的任意一个数
<0-61440>	桥的优先级，从 0 到 61440 之间的任意一个数

使用说明：优先级必须是 4096 的倍数，如果用户输入的不是 4096 的整数倍，则系统自动将该优先级转换成最接近的 4096 的倍数值。

示例：设置 instance 1 中桥的优先级为 4096。

```
set stp instance 1 bridgeprio 4096
```

10.11.15 set stp instance port cost

命令功能：设置实例端口费用。

命令模式：全局配置模式

命令格式：**set stp instance** *<0-15>* **port** *<portname>* **cost** *<1-200000000>*

参数解释：

参数	描述
<0-15>	实例号，从 1 到 15 之间的任意一个数
<portname>	一个端口号
<1-200000000>	端口费用

示例：设置 instance 1 的端口 1 费用为 20000。

```
set stp instance 1 port 1 cost 20000
```

10.11.16 set stp instance port priority

命令功能：设置实例端口的优先级。

命令模式：全局配置模式

命令格式：**set stp instance** *<0-15>* **port** *<portname>* **priority** *<0-255>*

参数解释：

参数	描述
<0-15>	实例号，从 0 到 15 之间的任意一个数
<portname>	一个端口号
<0-255>	优先级

示例：设置 instance 1 的端口 1 优先级为 100。

```
set stp instance 1 port 1 priority 100
```

10.11.17 set stp instance port root-guard

命令功能：设置实例端口的 root 保护。

命令模式：全局配置模式

命令格式：**set stp instance** <*0-15*> **port** <*portname*> **root-guard{enable|disable}**

参数解释：

参数	描述
<*0-15*>	实例号，从 0 到 15 之间的任意一个数
<*portname*>	一个端口
enable	开启实例端口 root 保护
disable	关闭实例端口 root 保护

示例：设置 instance 1 的端口 1 的 root 保护。

```
set stp instance 1 port 1 root-guard enable
```

示例：关闭 instance 1 的端口 1 的 root 保护。

```
set stp instance 1 port 1 root-guard disable
```

10.11.18 set stp instance port loop-guard

命令功能：设置实例端口的 loop 保护。

命令模式：全局配置模式

命令格式：**set stp instance** <*0-15*> **port** <*portname*> **loop-guard{enable|disable}**

参数解释：

参数	描述
<*0-15*>	实例号，从 0 到 15 之间的任意一个数
<*portname*>	一个端口
enable	开启实例端口 root 保护
disable	关闭实例端口 root 保护

示例：设置 instance 1 的端口 1 的 loop 保护。

```
set stp instance 1 port 1 loop-guard enable
```

示例：关闭 instance 1 的端口 1 的 loop 保护。

```
set stp instance 1 port 1 loop-guard disable
```

10.11.19 set stp instance trunk cost

命令功能：设置实例 trunk 费用。

命令模式：全局配置模式

命令格式：**set stp instance** <*0-15*> **trunk** < *trunkid* > **cost** <*1-200000000*>

参数解释：

参数	描述
<*0-15*>	实例号，从 1 到 15 之间的任意一个数
< *trunkid* >	Trunk ID
<*1-200000000*>	端口费用

示例：设置 instance 1 的 trunk1 费用为 20000。

```
set stp instance 1 trunk 1 cost 20000
```

10.11.20 set stp instance trunk priority

命令功能：设置实例端口的优先级。

命令模式：全局配置模式

命令格式：**set stp instance** <*0-15*> **trunk** < *trunkid* > **priority** <*0-255*>

参数解释：

参数	描述
<*0-15*>	实例号，从 0 到 15 之间的任意一个数
< *trunkid* >	Trunk ID
<*0-255*>	优先级

示例：设置 instance 1 的 trunk 1 优先级为 100。

```
set stp instance 1 trunk 1 priority 100
```

10.11.21 set stp instance trunk root-guard

命令功能：设置实例 trunk 的 root 保护。

命令模式：全局配置模式

命令格式：**set stp instance** <*0-15*> **trunk** <*trunkid*> **root-guard{enable|disable}**

参数解释：

参数	描述
<*0-15*>	实例号，从 0 到 15 之间的任意一个数
<*trunkid*>	一个 trunk 号
enable	开启实例端口 root 保护
disable	关闭实例端口 root 保护

示例：设置 instance 1 的 trunk1 的 root 保护。

```
set stp instance 1 trunk 1 root-guard enable
```

示例：关闭 instance 1 的端口 1 的 root 保护。

```
set stp instance 1 trunk 1 root-guard disable
```

10.11.22 set stp instance trunk loop-guard

命令功能：设置实例 trunk 的 loop 保护。

命令模式：全局配置模式

命令格式：**set stp instance** *<0-15>* **trunk** *<trunkid>* **loop-guard{enable|disable}**

参数解释：

参数	描述
<0-15>	实例号，从 0 到 15 之间的任意一个数
<trunkid>	一个 trunk 号
enable	开启实例端口 root 保护
disable	关闭实例端口 root 保护

示例：设置 instance 1 的 trunk1 的 loop 保护。

```
set stp instance 1 trunk 1 loop-guard enable
```

示例：关闭 instance 1 的端口 1 的 loop 保护。

```
set stp instance 1 trunk 1 loop-guard disable
```

10.11.23 set stp instance vlan

命令功能：设置 VLAN 和 instance 的映射关系。

命令模式：全局配置模式

命令格式：**set stp instance** *<0-15>*[**add|delete**] **vlan** *<vlanlist>*

参数解释：

参数	描述
<1-15>	实例号，从 1 到 15 之间的任意一个数
<vlanlist>	VLAN 列表

示例：设置 instance 1 映射 vlan 1，5，6，7，12。

```
set stp instance 1 add vlan 1,5-7,12
```

10.11.24 set stp name

命令功能：设置 MST 的区域名称。

命令模式：全局配置模式

命令格式：**set stp name** <*name*>

参数解释：

参数	描述
<*name*>	MST 的区域名称

示例：设置 MST 的区域名称为 education。

```
set stp name education
```

10.11.25 set stp port

命令功能：在端口上使能/关闭 STP。

命令模式：全局配置模式

命令格式：**set stp port** <*portlist*> {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	使能 STP
disable	关闭 STP

10.11.26 set stp port linktype

命令功能：设置端口连接类型。

命令模式：全局配置模式

命令格式：**set stp port** <*portlist*> **linktype** {**point-point**|**shared**}

参数解释：

参数	描述
<*portlist*>	端口列表
point-point	端口连接类型为 point-to-point
Shared	端口连接类型为 shared

10.11.27 set stp port packettype

命令功能：设置端口包类型。

命令模式：全局配置模式

命令格式：**set stp port** <*portlist*> **packettype** {**IEEE|CISCO|HUAWEI|HAMMER|extend**}

参数解释：

参数	描述
<*portlist*>	端口列表
IEEE	IEEE 方式
CISCO	CISCO 方式
HUAWEI	华为方式
HAMMER	港湾方式
extend	非标准协议方式，对 MSTP 协议包进行了扩充

10.11.28 set stp port pcheck

命令功能：设置端口 stp 类型检查。

命令模式：全局配置模式

命令格式：**set stp port** <*portlist*> **pcheck**

参数解释：

参数	描述
<*portlist*>	端口列表

10.11.29 set stp port bpdu-guard

命令功能：设置端口 bpdu 保护

命令模式：全局配置模式

命令格式：**set stp port** <*portlist*>**bpdu-guard{enable|disable}**

参数解释：

参数	描述
<*portlist*>	端口列表
enable	开启端口 bpdu 保护
disable	关闭端口 bpdu 保护

10.11.30 set stp bpdu_interval

命令功能：设置 BPDU 保护端口 linkdown 的时间间隔。

命令模式：全局配置模式

命令格式：**set stp bpdu_interval** *〈10-65535〉*

参数解释：

参数	描述
〈1-65535〉	超时时间间隔，单位秒。默认值 100 秒

10.11.31 set stp relay

命令功能：使能/关闭 STP Relay。

命令模式：全局配置模式

命令格式：**set stp relay** {**enable**|**disable**}

参数解释：

参数	描述
enable	使能 STP Relay
disable	关闭 STP Relay

10.11.32 set stp revision

命令功能：设置 MST 的版本号。

命令模式：全局配置模式

命令格式：**set stp revision** *<0-65535>*

参数解释：

参数	描述
<0-65535>	MST 的版本号，0-65535 之间的值

示例：设置 MST 的版本号为 10。

```
set stp revision 10
```

10.11.33 set stp trunk

命令功能：在 trunk 上使能/关闭 STP。

命令模式：全局配置模式

命令格式：**set stp trunk** <*trunklist*> {**enable**|**disable**}

参数解释：

参数	描述
< *trunklist* >	一个或多个 Trunk 组号
enable	使能 STP
disable	关闭 STP

10.11.34 set stp trunk linktype

命令功能：设置 trunk 连接类型。

命令模式：全局配置模式

命令格式：**set stp trunk** < *trunklist* > **linktype** {**point-point**|**shared**}

参数解释：

参数	描述
< *trunklist*>	一个或多个 Trunk 组号
point-point	端口连接类型为 point-to-point
shared	端口连接类型为 shared

10.11.35 set stp trunk packettype

命令功能：设置端口包类型。

命令模式：全局配置模式

命令格式：**set stp trunk** < *trunklist* > **packettype**

{**IEEE**|**CISCO**|**HUAWEI**|**HAMMER**|**extend**}

参数解释：

参数	描述
< *trunklist* >	Trunk 列表
IEEE	IEEE 方式
CISCO	CISCO 方式
HUAWEI	华为方式
HAMMER	港湾方式
extend	扩展方式

10.11.36 show stp

命令功能：显示 STP 的信息。

命令模式：所有模式

命令格式：**show stp**

10.11.37 show stp instance

命令功能：显示 STP 实例的信息。

命令模式：所有模式

命令格式：**show stp instance** [*<0-15>*]

参数解释：

参数	描述
<0-15>	实例号，从 0 到 15 之间的任意一个数

示例一：显示所有 STP 实例的信息。

```
show stp instance
```

示例二：显示 STP 实例 1 的信息。

```
show stp instance 1
```

10.11.38 show stp port

命令功能：显示 STP 端口的信息。

命令模式：所有模式

命令格式：**show stp port** [*<portlist>*]

参数解释：

参数	描述
<portlist>	端口列表

示例一：显示所有 STP 端口的信息。

```
show stp port
```

示例二：显示 STP 端口 1，5，6，7 的信息。

```
show stp port 1,5-7
```

10.11.39 show stp relay

命令功能：显示 STP relay 配置信息。

命令模式：所有模式

命令格式：**show stp relay**

10.11.40 show stp trunk

命令功能：显示 STP 聚合端口的信息。

命令模式：所有模式

命令格式：**show stp trunk** < *trunklist* >

参数解释：

参数	描述
< *trunklist* >	Trunk 列表

示例：显示 STP 聚合端口 1、2 的信息。

```
show stp trunk 1,2
```

10.12 QoS 配置

10.12.1 set qos queue-schedule

命令功能：设置队列调度模式。

命令模式：全局配置模式

命令格式：**set qos queue-schedule** {sp|wfq}

参数解释：

参数	描述
sp	sp 方式
wfq	wfq 方式

示例：设置队列调度模式为 sp。

```
set qos queue-schedule sp
```

10.12.2 set qos priority-map user-priority

命令功能：设置 802.1P 用户优先级到队列优先级映射。

命令模式：全局配置模式

命令格式：**set qos priority-map user-priority** <0-*7*> **traffic-class** <0-*3*>

参数解释：

参数	描述
<0-*7*>	802.1P 用户优先级
<0-*3*>	队列优先级

示例一：设置 802.1P 用户优先级 3 到应队列优先级 2。

```
set qos priority-map user-priority 3 traffic-class 2
```

10.12.3 set qos priority-map ip-priority

命令功能：设置一个三层 DSCP 优先级到队列优先级映射。

命令模式：全局配置模式

命令格式：**set qos priority-map ip-priority** <0-*63*> **traffic-class** <0-*3*>

参数解释：

参数	描述
<0-*63*>	三层 DSCP 优先级
<0-*3*>	队列优先级

示例一：设置三层 DSCP 优先级 13 到应队列优先级 2。

```
set qos priority-map ip-priority 13 traffic-class 2
```

10.12.4 show qos queue-schedule

命令功能：显示 qos 队列配置。

命令模式：所有模式

命令格式：**show qos queue-schedule**

10.12.5 show qos priority-map

命令功能：显示 qos 的 802.1P 用户优先级到队列优先级映射/三层 DSCP 优先级到队列优先级映射。

命令模式：所有模式

命令格式：**show qos priorty-map** {**user-priority**|**ip-priority**}

10.13 PVLAN 配置

10.13.1 set pvlan session

命令功能：在 PVLAN 中增加/删除隔离端口/共享端口。

命令模式：所有模式

命令格式：**set pvlan session** <*id*> {**add**|**delete**} {**isolated-port** <*portlist*> | **promiscuous** {**port**<*portname*>|**trunk**<*trunkid*>}}

参数解释：

参数	描述
<*id*>	目前只支持一个 PVLAN，因此 session 值必须为 1
add	增加隔离端口或共享端口
delete	删除隔离端口或共享端口
isolated-port	隔离端口
|promiscuous	共享端口或共享 trunk
<*portlist*>	端口列表
<*portname*>	一个端口号
<*trunkid*>	一个 trunk 号

10.13.2 show pvlan

命令功能：显示 pvlan 的配置。

命令模式：所有模式

命令格式：**show pvlan**

10.14 802.1x 透传配置

10.14.1 set 802.1xrelay

命令功能：开启/关闭 802.1x 透传功能。

命令模式：全局配置模式

命令格式：**set 802.1xrelay** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 802.1x 透传功能

disable	关闭 802.1x 透传功能

10.14.2 show 802.1xrelay

命令功能：显示 802.1x 透传配置。

命令模式：所有模式

命令格式：**show 802.1xrelay**

10.15 三层配置

10.15.1 arp add

命令功能：添加静态地址解析。

命令模式：三层配置模式

命令格式：**arp add** *<A.B.C.D> <xx.xx.xx.xx.xx.xx> <0-63> <vlanname>*

参数解释：

参数	描述
<A.B.C.D>	IP 地址
<xx.xx.xx.xx.xx.xx>	MAC 地址
<0-63>	三层端口号
<vlanname>	一个 VLAN ID 或者一个 VLAN 名

使用说明：其中 IP 地址必须在指定的 IP 端口 IP 子网范围内的地址，VLAN ID 必须为与此 IP 端口绑定的 VLAN ID。

示例一：添加静态地址解析 10.40.44.167，MAC 地址 00.00.00.00.11.22，三层端口 1，vlan 1。

```
arp add 10.40.44.167 00.00.00.00.11.22 1 1
```

示例二：添加静态地址解析 10.40.44.167，MAC 地址 00.00.00.00.11.22，三层端口 1，VLAN 名为 group1。

```
arp add 10.40.44.167 00.00.00.00.11.22 1 group1
```

10.15.2 arp delete

命令功能：删除静态地址解析。

命令模式：三层配置模式

命令格式：**arp delete** *<A.B.C.D>*

参数解释：

参数	描述
<A.B.C.D>	IP 地址

示例：删除 10.40.44.167 的静态地址解析。

```
arp delete 10.40.44.167
```

10.15.3 arp ipport timeout

命令功能：设置三层端口的超时时间。

命令模式：三层配置模式

命令格式：**arp ipport** *<0-63>* **timeout** *<1-1000>*

参数解释：

参数	描述
<0-63>	一个三层端口号
<1-1000>	超时时间，单位：分钟，缺省为 10 分钟

示例：设置三层端口 1 的超时时间为 100 分钟。

```
arp ipport 1 timeout 100
```

10.15.4 clear arp

命令功能：删除所有的 ARP 信息。

命令模式：三层配置模式

命令格式：**clear arp**

使用说明：此命令将删除交换机上的所有的 ARP 表信息，使用时请谨慎。

10.15.5 clear ipport

命令功能：删除 ipport 的配置。

命令模式：三层配置模式

命令格式：**clear ipport** *<0-63>* [**mac**|**ipaddress** {*<A.B.C.D/M>*|*<A.B.C.D>* *<A.B.C.D>*}|**vlan** *<vlanname>*]

参数解释：

参数	描述
<0-63>	一个三层端口号
<A.B.C.D/M>	IP 地址和掩码
<A.B.C.D>	IP 地址/掩码
<vlanname>	一个 VLAN ID 或者一个 VLAN 名

使用说明：IP 端口配置清除的命令要在端口 down 的情况下使用，命令将恢复端口的默认值（IP address：0.0.0.0，mac address：00.00.00.00.00.00，绑定 vlan 0）。

示例一：删除三层端口 1 的配置。

```
clear ipport 1
```

示例二：删除三层端口 1 的 MAC 地址。

```
clear ipport 1 mac
```

示例三：删除三层端口 1 的 IP 地址 10.40.44.167，掩码 255.255.255.0。

```
clear ipport 1 ipaddress 10.40.44.167/24
clear ipport 1 ipaddress 10.40.44.167 255.255.255.0
```

示例四：删除三层端口 1 的 vlan 1。

```
clear ipport 1 vlan 1
```

示例五：删除三层端口 1 名为 group1 的 VLAN。

```
clear ipport 1 vlan group1
```

10.15.6 clear iproute

命令功能：删除静态路由。

命令模式：三层配置模式

命令格式：**clear iproute** [{*<A.B.C.D/M>*|*<A.B.C.D>* *<A.B.C.D>*} *<A.B.C.D>*]

参数解释：

参数	描述
<A.B.C.D/M>	IP 地址和掩码
<A.B.C.D>	IP 地址/掩码/网关

使用说明：此命令将删除所有配置的静态路由，无法恢复。

示例一：删除所有静态路由。

```
clear iproute
```

示例二：删除到网络 10.40.44.0/24 的静态路由，网关 10.40.44.12。

```
clear iproute 10.40.44.0/24 10.40.44.12
clear iproute 10.40.44.0 255.255.255.0 10.40.44.12
```

10.15.7 iproute

命令功能：添加静态路由。

命令模式：三层配置模式

命令格式：**iproute** {*<A.B.C.D/M>*|*<A.B.C.D>* *<A.B.C.D>*} *<A.B.C.D>* [*<1-15>*]

参数解释：

参数	描述
<A.B.C.D/M>	IP 地址和掩码
<A.B.C.D>	IP 地址/掩码/网关
<1-15>	Metric

示例：添加到网络 10.40.44.0/24 的静态路由，网关 10.40.44.255，metric 为 3。

```
iproute 10.40.44.0/24 10.40.44.255 3
iproute 10.40.44.0 255.255.255.0 10.40.44.255 3
```

10.15.8 set ipport

命令功能：使能/关闭三层端口。

命令模式：三层配置模式

命令格式：**set ipport** *<0-63>* {**enable**|**disable**}

参数解释：

参数	描述
<0-63>	一个三层端口号
enable	使能三层端口
disable	关闭三层端口

使用说明：使能一个三层端口时必须已经配置了此端口的 IP 地址和 VLAN 数据，MAC 可以不用配置。

示例一：使能三层端口 1。

```
set ipport 1 enable
```

示例二：关闭三层端口 1。

```
set ipport 1 disable
```

10.15.9 set ipport ipaddress

命令功能：设置三层端口的 IP 地址和掩码。

命令模式：三层配置模式

命令格式：**set ipport** *<0-63>* **ipaddress** {*<A.B.C.D/M>*|*<A.B.C.D>* < *A.B.C.D>*}

参数解释：

参数	描述
<0-63>	一个三层端口号
<A.B.C.D/M>	IP 地址和掩码
<A.B.C.D>	IP 地址/掩码

使用说明：在要设置的 IP 端口已经设置 IP 地址时，此命令将用新设置 IP 地址代替原 IP 地址。

示例：设置三层端口 1 的 IP 地址为 10.40.44.167，掩码为 255.255.255.0。

```
set ipport 1 ipaddress 10.40.44.167/24
set ipport 1 ipaddress 10.40.44.167 255.255.255.0
```

10.15.10 set ipport mac

命令功能：设置三层端口 MAC 地址。

命令模式：三层配置模式

命令格式：**set ipport** *<0-63>* **mac** *<xx.xx.xx.xx.xx.xx>*

参数解释：

参数	描述
<0-63>	一个三层端口号
<xx.xx.xx.xx.xx.xx>	MAC 地址

使用说明：MAC 地址范围为 00.d0.d0.f0.00.00 到 00.d0.d0.ff.ff.ff。此项如果不设置，则此时的 MAC 地址为交换机的 MAC 地址。在要设置的 IP 端口已经设置 MAC 地址时，此命令将用新设置的 MAC 地址代替原 MAC 地址。

示例：设置三层端口 1 的 MAC 地址为 00.d0.d0.f0.11.22。

```
set ipport 1 mac 00.d0.d0.f0.11.22
```

10.15.11 set ipport vlan

命令功能：设置三层端口绑定 VLAN。

命令模式：三层配置模式

命令格式：**set ipport** <*0-63*> **vlan** <*vlanname*>

参数解释：

参数	描述
<*0-63*>	一个三层端口号
<*vlanname*>	一个 VLAN ID 或者一个 VLAN 名

使用说明：在要设置的IP端口已经绑定一个VLAN时，此命令将用新设置的VLAN值代替原 VLAN 值。

示例一：设置三层端口 1 绑定 vlan 1。

```
set ipport 1 vlan 1
```

示例二：设置三层端口 1 绑定 VLAN 名为 group1。

```
set ipport 1 vlan group1
```

10.15.12 show arp

命令功能：显示 ARP 信息。

命令模式：所有模式

命令格式：**show arp** [**static**|**dynamic**|**invalid**|**ipport** <*0-63*> {**static**|**dynamic**|**invalid**} |**ipaddress** <*A.B.C.D*>]

参数解释：

参数	描述
<*0-63*>	一个三层端口号
<*A.B.C.D*>	IP 地址

示例一：显示所有 ARP 的信息。

```
show arp
```

示例二：显示无效的 ARP 信息。

```
show arp invalid
```

示例三：显示三层端口 1 的静态 ARP 信息。

```
show arp ipport 1 static
```

示例四：显示 IP 地址 10.40.44.167 的 ARP 信息。

```
show arp ipaddress 10.40.44.167
```

10.15.13 show ipport

命令功能：显示三层端口的信息。

命令模式：所有模式

命令格式：**show ipport** [*<0-63>*]

参数解释：

参数	描述
<0-63>	三层端口号

示例一：显示所有三层端口的信息。

```
show ipport
```

示例二：显示三层端口 1 的信息。

```
show ipport 1
```

10.15.14 show iproute

命令功能：显示所有静态路由。

命令模式：所有模式

命令格式：**show iproute**

10.16 接入服务配置

10.16.1 aaa-control port accounting

命令功能：开启/关闭端口记帐。

命令模式：NAS 模式

命令格式：**aaa-control port** *<portlist>* **accounting** {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	开启端口记帐
disable	关闭端口记帐

10.16.2 aaa-control port dot1x

命令功能：开启/关闭端口的 802.1x 接入。

命令模式：NAS 模式

命令格式：**aaa-control port** *<portlist>* **dot1x** {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	开启端口的 dot1x 接入
disable	关闭端口的 dot1x 接入

10.16.3 aaa-control port keepalive

命令功能：开启/关闭端口的异常下线检测。

命令模式：NAS 模式

命令格式：**aaa-control port** *<portlist>* **keepalive** {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	开启端口的异常下线检测
disable	关闭端口的异常下线检测

10.16.4 aaa-control port keepalive period

命令功能：设置端口的异常下线检测周期。

命令模式：NAS 模式

命令格式：**aaa-control port** *<portlist>* **keepalive period** *<1-3600>*

参数解释：

参数	描述
<portlist>	端口列表
<1-3600>	端口的异常下线检测周期，单位：秒，缺省为 10 秒

10.16.5 aaa-control port max-hosts

命令功能：设置端口的最大用户接入数目。

命令模式：NAS 模式

命令格式：**aaa-control port** <*portlist*> **max-hosts** <*0-64*>

参数解释：

参数	描述
<*portlist*>	端口列表
<*0-64*>	最大用户接入数目，缺省为 0

使用说明：最大用户接入数目为 0 表示不限制端口接入的用户数，这时接入的用户数受限于整个交换机允许接入的最大用户数。

10.16.6 aaa-control port multiple-hosts

命令功能：允许/禁止端口多用户接入。

命令模式：NAS 模式

命令格式：**aaa-control port** <*portlist*> **multiple-hosts** {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	允许端口多用户接入
disable	禁止端口多用户接入

10.16.7 aaa-control port port-mode

命令功能：配置端口的认证控制模式。

命令模式：NAS 模式

命令格式：**aaa-control port** <*portlist*> **port-mode** {**auto**|**force-unauthorized**|**force-authorized**}

参数解释：

参数	描述
<*portlist*>	端口列表
auto	不强制，为系统缺省模式
force-unauthorized	强制认证不通过
force-authorized	强制认证通过

10.16.8 aaa-control port protocol

命令功能：配置端口的认证方式。

命令模式：NAS 模式

命令格式：**aaa-control port** <*portlist*> **protocol** {**pap**|**chap**|**eap** }

参数解释：

参数	描述
<*portlist*>	端口列表
pap	端口认证方式为 pap
chap	端口认证方式为 chap
eap	端口认证方式为 eap，为系统缺省认证方式

10.16.9 dot1x max-request

命令功能：设置认证系统接收来自客户端系统的 challenge 响应的超时重传次数。

命令模式：NAS 模式

命令格式：**dot1x max-request** <*1-10*>

参数解释：

参数	描述
<*1-10*>	超时重传次数，缺省为 2

10.16.10 dot1x quiet-period

命令功能：设置认证系统一次认证失败后到接受下一次认证请求的间隔。

命令模式：NAS 模式

命令格式：**dot1x quiet-period** <*0-65535*>

参数解释：

参数	描述
<*0-65535*>	时间间隔，单位：秒，缺省为 60 秒

10.16.11 dot1x re-authenticate

命令功能：开启/关闭重认证机制。

命令模式：NAS 模式

命令格式：**dot1x re-authenticate** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启重认证机制
disable	关闭重认证机制

10.16.12 dot1x re-authenticate period

命令功能：配置重认证的时间间隔。

命令模式：NAS 模式

命令格式：**dot1x re-authenticate period** *<1-4294967295>*

参数解释：

参数	描述
<1-4294967295>	时间间隔，单位：秒，缺省为 3600 秒

10.16.13 dot1x server-timeout

命令功能：认证系统接收来自认证服务器的数据包的超时时间。

命令模式：NAS 模式

命令格式：**dot1x server-timeout** *<1-65535>*

参数解释：

参数	描述
<1-65535>	时间间隔，单位：秒，缺省为 30 秒

10.16.14 dot1x supplicant-timeout

命令功能：认证系统接收来自认证客户端系统的数据包的超时时间。

命令模式：NAS 模式

命令格式：**dot1x supplicant-timeout** *<1-65535>*

参数解释：

参数	描述
<1-65535>	时间间隔，单位：秒，缺省为 30 秒

10.16.15 dot1x tx-period

命令功能：认证系统接收不到客户端系统回复而重发 EAPOL 数据包的等待时间。

命令模式：NAS 模式

命令格式：**dot1x tx-period** *<1-65535>*

参数解释：

参数	描述
<1-65535>	时间间隔，单位：秒，缺省为 30 秒

10.16.16 dot1x add fid

命令功能：设置交换机可以识别的私有 MAC 地址。

命令模式：NAS 模式

命令格式：**dot1x add fid** *<1-256>* [**mac** *<HH.HH.HH.HH.HH.HH>*]

参数解释：

参数	描述
<1-256>	Fid 值
<HH.HH.HH.HH.HH.HH>	指定的 mac 地址，可以是组播或单播地址

10.16.17 dot1x delete fid

命令功能：设置交换机可以识别的私有 MAC 地址。

命令模式：NAS 模式

命令格式：**dot1x delete fid** *<1-256>*

参数解释：

参数	描述
<1-256>	Fid 值

10.16.18 clear client

命令功能：删除所有客户端用户。

命令模式：NAS 模式

命令格式：**clear client**

10.16.19 clear client index

命令功能：删除某客户端用户。

命令模式：NAS 模式

命令格式：**clear client index** <*0-63*>

参数解释：

参数	描述
<*0-63*>	用户号

10.16.20 clear client port

命令功能：删除某端口上的客户端用户。

命令模式：NAS 模式

命令格式：**clear client port** <*portlist*>

参数解释：

参数	描述
<*portlist*>	端口列表

10.16.21 clear client vlan

命令功能：删除某 VLAN 上所有的客户端用户。

命令模式：NAS 模式

命令格式：**clear client vlan** <*vlantlist*>

参数解释：

参数	描述
<*vlanlist*>	VLAN 列表

10.16.22 radius isp

命令功能：添加/删除一个 ISP。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> {**enable**|**disable**}

参数解释：

参数	描述
<*ispname*>	ISP 域名称
enable	添加 ISP

disable	删除 ISP

10.16.23 radius isp add accounting

命令功能：在域中添加记帐服务器。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **add accounting** <*A.B.C.D*> [<*0-65535*>]

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*A.B.C.D*>	IP 地址
<*0-65535*>	记帐服务器的 UDP 端口，缺省为 1813

10.16.24 radius isp add authentication

命令功能：在域中添加认证服务器。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **add authentication** <*A.B.C.D*> [<*0-65535*>]

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*A.B.C.D*>	IP 地址
<*0-65535*>	认证服务器的 UDP 端口，缺省为 1812

10.16.25 radius isp defaultisp

命令功能：指定/取消这个域为默认域。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **defaultisp** {**enable**|**disable**}

参数解释：

参数	描述
<*ispname*>	ISP 域名称
enable	设置该 ISP 域为缺省 ISP 域
disable	取消该 ISP 域为缺省 ISP 域

10.16.26 radius isp delete accounting

命令功能：在域中删除记帐服务器。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **delete accounting** <*A.B.C.D*>

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*A.B.C.D*>	IP 地址

10.16.27 radius isp delete authentication

命令功能：在域中删除认证服务器。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **delete authentication** <*A.B.C.D*>

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*A.B.C.D*>	IP 地址

10.16.28 radius isp description

命令功能：配置域描述信息。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **description** <*string*>

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*string*>	ISP 域的描述信息

10.16.29 radius isp client

命令功能：配置 radius 客户端地址。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **client** <*A.B.C.D*>

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*A.B.C.D*>	IP 地址

10.16.30 radius isp fullaccount

命令功能：指定/取消这个域使用全帐号。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **fullaccount** {**enable**|**disable**}

参数解释：

参数	描述
<*ispname*>	ISP 域名称
enable	设置该 ISP 域使用全帐号
disable	取消该 ISP 域使用全帐号

10.16.31 radius isp sharedsecret

命令功能：配置域的共享密码。

命令模式：NAS 模式

命令格式：**radius isp** <*ispname*> **sharedsecret** <*string*>

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*string*>	共享密码

10.16.32 radius nasname

命令功能：配置 NAS 名称。

命令模式：NAS 模式

命令格式：**radius nasname** <*nasname*>

参数解释：

参数	描述
<*nasname*>	NAS 名称

10.16.33 radius retransmit

命令功能：设置远端认证请求重传次数。

命令模式：NAS 模式

命令格式：**radius retransmit** *<1-255>*

参数解释：

参数	描述
<1-255>	重传次数，缺省为 3

10.16.34 radius timeout

命令功能：设置远端认证请求重传时间间隔。

命令模式：NAS 模式

命令格式：**radius timeout** *<1-255>*

参数解释：

参数	描述
<1-255>	重传时间间隔，单位：秒，缺省为 3 秒

10.16.35 radius keep-time

命令功能：配置 radius 记帐中止包的保存时间。

命令模式：NAS 模式

命令格式：**radius keep-time** *<0-4294967295>*

参数解释：

参数	描述
<0-4294967295>	配置 radius 记帐中止包的保存时间，0 表示无时间限制

10.16.36 clear accounting-stop

命令功能：删除发送失败的 radius 记帐中止包。

命令模式：NAS 模式

命令格式：**clear accounting-stop** {**session-id** *<session-id>* | **user-name** *<user-name>* | **isp-name** *<isp-name>* | **server-ip** *<A.B.C.D>*}

参数解释：

参数	描述
<session-id>	会话 ID
<user-name>	用户名
<isp-name>	radius isp 名
<A.B.C.D>	计费服务器的 IP 地址

10.16.37 show aaa-control port

命令功能：显示 aaa 控制策略配置信息。

命令模式：所有模式

命令格式：**show aaa-control port** [*<portlist>*]

参数解释：

参数	描述
<portlist>	端口列表

10.16.38 show dot1x

命令功能：显示 dot1x 配置信息。

命令模式：所有模式

命令格式：**show dot1x**

10.16.39 show client

命令功能：显示所有接入用户的信息。

命令模式：所有模式

命令格式：**show client**

10.16.40 show client index

命令功能：显示某接入用户的信息。

命令模式：所有模式

命令格式：**show client index** *<0-63>*

参数解释：

参数	描述
<0-63>	用户号

10.16.41 show client mac

命令功能：显示某 MAC 地址的用户接入信息。

命令模式：所有模式

命令格式：**show client mac** <*xx.xx.xx.xx.xx.xx*>

参数解释：

参数	描述
<*xx.xx.xx.xx.xx.xx*>	MAC 地址

10.16.42 show client port

命令功能：显示某端口的用户接入信息。

命令模式：所有模式

命令格式：**show client port** <*portlist*>

参数解释：

参数	描述
<*portlist*>	端口列表

10.16.43 show radius

命令功能：显示 radius 配置信息。

命令模式：所有模式

命令格式：**show radius** [**ispname** <*ispname*>|**accounting-stop** [**session-id** <*session-id*> | **user-name** <*user-name*>| **isp-name** <*isp-name*>|**server-ip** <*A.B.C.D*>]]

参数解释：

参数	描述
<*ispname*>	ISP 域名称
<*session-id*>	
<*user-name*>	
<*isp-name*>	
<*A.B.C.D*>	

10.16.44 show radius accounting-stop

命令功能：显示发送失败的 radius 记帐中止包。

命令模式：所有模式

命令格式：**show radius accounting-stop** [{ **session-id** <*session-id*> | **user-name** <*user-name*> | **isp-name** <*isp-name*> | **server-ip** <*A.B.C.D*>**}**]

参数解释：

参数	描述
<*session-id*>	会话 ID
<*user-name*>	用户名
<*isp-name*>	radius isp 名
<*A.B.C.D*>	计费服务器的 IP 地址

10.17 QinQ 配置

10.17.1 set qinq customer port

命令功能：添加/删除 customer 端口。

命令模式：全局配置模式

命令格式：**set qinq customer port** <*portlist*> {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	添加 customer 端口
disable	删除 customer 端口

示例：设置端口 1、2、3、4 为 customer 端口。

```
set qinq customer port 1—4 enable
```

10.17.2 set qinq tpid

命令功能：设置外层标签的 tpid。

命令模式：全局配置模式

命令格式：**set qinq tpid** <*tpid*>

参数解释：

参数	描述
<*tpid*>	QinQ 中使用的外层标签值（0xaaaa 形式）

示例：设置外层标签的 tpid 为 0x8910。

```
set qinq tpid 0x8910
```

10.17.3 set qinq uplink port

命令功能：添加/删除 uplink 端口。

命令模式：全局配置模式

命令格式：**set qinq uplink port** <*portlist*> {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	添加 uplink 端口
disable	删除 uplink 端口

示例：设置端口 24 为 uplink 端口。

```
set qinq uplink port 24 enable
```

10.17.4 show qinq

命令功能：显示 QinQ 配置信息。

命令模式：所有模式

命令格式：**show qinq**

参数解释：无

示例：显示 QinQ 配置信息。

```
show qinq
```

10.18 Syslog 配置

10.18.1 set syslog

命令功能：开启/关闭 syslog 功能。

命令模式：全局配置模式

命令格式：**set syslog** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 syslog 功能
disnable	关闭 syslog 功能

示例：开启 syslog 功能。

```
set syslog enable
```

10.18.2 set syslog module

命令功能：开启/关闭 syslog 功能。

命令模式：全局配置模式

命令格式：**set syslog module** {**all|alarm|commandlog**}{**enable|disable**}

参数解释：

参数	描述
all	开启/关闭所有模块的 syslog 功能
alarm	开启/关闭 alarm 模块的 syslog 功能
commandlog	开启/关闭 commandlog 模块的 syslog 功能
enable	开启 syslog 功能
disnable	关闭 syslog 功能

示例：开启 commandlog 模块的 syslog 功能。

```
set syslog module commandlog enable
```

10.18.3 set syslog level

命令功能：设置 Syslog 信息的严重等级。

命令模式：全局配置模式

命令格式：**set syslog level** {**emergencies | alerts | critical | errors | warnings | notifications | informational | debugging}**

参数解释：

参数	描述
emergencies	等级 1，极其紧急的错误
alerts	等级 2，需立即纠正的错误
critical	等级 3，关键错误
errors	等级 4，需关注但不关键的错误
warnings	等级 5，警告，可能存在某种差错
notifications	等级 6，需注意的信息

informational	等级 7，一般提示信息
debugging	等级 8，调试信息

示例：设置 syslog 严重级别为 7，一般提示信息。

```
set syslog level informational
```

10.18.4 set syslog add server

命令功能：设置 syslog 服务器。

命令模式：全局配置模式

命令格式：**set syslog add server** <*id*> **ipaddress** <*A.B.C.D*> [**name** <*name*>]

参数解释：

参数	描述
<*id*>	Syslog 服务器 ID 号，最多可设 5 个
<*A.B.C.D*>	Syslog 服务器 IP 地址
<*name*>	Syslog 服务器名称

示例：设置 syslog 服务器。

```
set syslog add server 1 ipaddress 192.168.1.1 name srv1
```

10.18.5 set syslog delete server

命令功能：按 ID 号删除 syslog 服务器。

命令模式：全局配置模式

命令格式：**set syslog delete server** <*id*>

参数解释：

参数	描述
<*id*>	Syslog 服务器 ID 号，最多可设 5 个。

示例：删除 syslog 服务器 1。

```
set syslog delete server 1
```

10.18.6 show syslog status

命令功能：显示 Syslog 的配置信息。

命令模式：全局配置模式

命令格式：**show syslog status**

示例：显示 Syslog 的配置信息。

```
Show syslog status
```

10.19 NTP 配置

10.19.1 set ntp

命令功能：开启/关闭 NTP 功能。

命令模式：全局配置模式

命令格式：**set ntp** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 NTP 功能
disnable	关闭 NTP 功能

10.19.2 set ntp server

命令功能：设置 NTP 服务器 IP 地址和版本号。

命令模式：全局配置模式

命令格式：**set ntp server** *<A.B.C.D>* [**version** *<1,2,3>*]

参数解释：

参数	描述
<A.B.C.D>	NTP 服务器的 IP 地址
<1,2,3>	NTP 使用的版本号，默认为 3

示例：设置 NTP 服务器 IP 地址为 202.10.10.10 ,使用的协议版本号为 2。

```
set ntp server 202.10.10.10 version 2
```

10.19.3 set ntp source

命令功能：设置交换机发送 NTP 数据包使用的源 IP 地址。

命令模式：全局配置模式

命令格式：**set ntp source** *<A.B.C.D>*

参数解释：

参数	描述
<A.B.C.D>	本交换机的一个接口 IP 地址

使用说明：当输入的 IP 地址为 0.0.0.0，将源 IP 地址恢复到没有配置的情况。

10.19.4 show ntp

命令功能： 显示 NTP 模块配置信息和当前状态。

命令模式：全局配置模式

命令格式：**show ntp**

示例：显示 NTP 的配置信息。

```
Show ntp
```

10.20 GARP/GVRP 配置

10.20.1 set garp

命令功能：开启/关闭 garp 功能。

命令模式：全局配置模式

命令格式：**set garp** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 garp 功能
disable	关闭 garp 功能

10.20.2 set garp timer

命令功能：设置 GARP 定时器。

命令模式：全局配置模式

命令格式：**set garp timer**{**hold**|**join**|**leave**|**leaveall**}*<timer_value>*

参数解释：

参数	描述
<imer_value>	定时器超时时间

hold	hold 定时器
join	join 加入定时器
leave	leave 离开定时器
leaveall	leaveall 离开所有定时器

10.20.3 show garp

命令功能：显示 GARP 配置。

命令模式：所有模式

命令格式：**show garp**

10.20.4 set gvrp

命令功能：开启/关闭 gvrp 功能。

命令模式：全局配置模式

命令格式：**set gvrp** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 gvrp 功能
disable	关闭 gvrp 功能

10.20.5 set gvrp port

命令功能：开启/关闭端口 gvrp 功能。

命令模式：全局配置模式

命令格式：**set gvrp port** <*portlist*>{**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	设置 gvrp 功能的端口号
enable	开启端口 gvrp 功能
disable	关闭端口 gvrp 功能

10.20.6 set gvrp port registration

命令功能：设置端口 gvrp 注册类型。

命令模式：全局配置模式

命令格式：**set gvrp port** <*portlist*> **registration**{**normal**|**fixed**|**forbidden**}

参数解释：

参数	描述
<*portlist*>	设置端口 gvrp 注册类型的端口号
normal	端口注册类型设为 normal 状态
fixed	端口注册类型设为 fixed 状态
forbidden	端口注册类型设为 forbidden 状态

10.20.7 set gvrp trunk

命令功能：开启/关闭 Trunk 端口 gvrp 功能。

命令模式：全局配置模式

命令格式：**set gvrp trunk** <*trunklist*> {**enable**|**disable**}

参数解释：

参数	描述
<*trunklist*>	设置 gvrp 功能的 trunk 端口号
enable	开启 trunk 端口 gvrp 功能
disable	关闭 trunk 端口 gvrp 功能

10.20.8 set gvrp trunk registration

命令功能：设置 Trunk 端口 gvrp 注册类型。

命令模式：全局配置模式

命令格式：**set gvrp trunk**<*trunkid*> **registration**{**normal**|**fixed**|**forbidden**}

参数解释：

参数	描述
<*trunkid*>	设置 trunk 端口 gvrp 注册类型的 trunk 端口号
normal	trunk 端口注册类型设为 normal 状态
fixed	trunk 端口注册类型设为 fixed 状态
forbidden	trunk 端口注册类型设为 forbidden 状态

10.20.9 show gvrp

命令功能：显示 GVRP 配置。

命令模式：所有模式

命令格式：**show gvrp**

10.21 remote-access 配置

10.21.1 clear remote-access all

命令功能：删除所有受限登录的 IP 地址。

命令模式：全局配置模式

命令格式：**clear remote-access all**

10.21.2 clear remote-access ipaddress

命令功能：删除某个受限登录的 IP 地址。

命令模式：全局配置模式

命令格式：**clear remote-access ipaddress** <*A.B.C.D*> [<*A.B.C.D*>]

参数解释：

参数	描述
<*A.B.C.D*>	IP 地址/掩码

10.21.3 set remote-access

命令功能：配置 telnet 受限登录。

命令模式：全局配置模式

命令格式：**set remote-access** {**any**|**specific**}

参数解释：

参数	描述
any	任何 IP 地址都可以 telnet 交换机
specific	只有特定 IP 地址才可以 telnet 交换机

10.21.4 set remote-access ipaddress

命令功能：配置 telnet 受限登录的 IP 地址。

命令模式：全局配置模式

命令格式：**set remote-access ipaddress** <*A.B.C.D*> [<*A.B.C.D*>]

参数解释：

参数	描述
<A.B.C.D>	IP 地址/掩码

10.21.5 show remote-access

命令功能：显示 remote-access 的信息。

命令模式：所有模式

命令格式：**show remote-access**

10.22 SSH 配置

10.22.1 set ssh

命令功能：开启/关闭 ssh 功能。

命令模式：全局配置模式

命令格式：**set ssh** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 ssh 功能
disable	关闭 ssh 功能

10.22.2 show ssh

命令功能：显示 ssh 的配置和状态。

命令模式：所有模式

命令格式：**show ssh**

10.23 SNMP 配置

10.23.1 clear community

命令功能：删除团体名。

命令模式：SNMP 配置模式

命令格式：**clear community** <*string*>

参数解释：

参数	描述
< *string* >	团体的名称

示例：删除团体名 seu。

```
clear community seu
```

10.23.2 clear group

命令功能：删除组名。

命令模式：SNMP 配置模式

命令格式：**clear group** <*string*> **v3** {**auth**|**noauth**|**priv**}

参数解释：

参数	描述
<*string*>	组的名称
noauth	不认证不加密
Auth	认证不加密
Priv	认证且加密

示例：删除组名 gname，其安全级别为 auth。

```
clear group gname v3 auth
```

10.23.3 clear host

命令功能：删除 host。

命令模式：SNMP 配置模式

命令格式：**clear host** <*A.B.C.D*> {**trap**|**inform**} <*string*>

参数解释：

参数	描述
<*A.B.C.D*>	IP 地址
trap	类型为 trap
inform	类型为 inform
<*string*>	团体名或用户名

示例：删除接收 trap 报文的 host，其 IP 地址为 10.40.44.167，团体名为 cname 。

```
clear host 10.40.44.167 trap cname
```

示例：删除接收 inform 报文的 host，其 IP 地址为 10.40.44.167，其用户名为 uname。

```
clear host 10.40.44.167 inform uname
```

10.23.4 clear user

命令功能：删除用户名。

命令模式：SNMP 配置模式

命令格式：**clear user** <*string*> **v3**

参数解释：

参数	描述
<*string*>	用户名

示例：删除用户名 uname。

```
clear user uname v3
```

10.23.5 clear view

命令功能：删除视图名。

命令模式：SNMP 配置模式

命令格式：**clear view** <*string*>

参数解释：

参数	描述
< *string* >	视图名

示例：删除视图名 school。

```
clear view school
```

10.23.6 create community

命令功能：创建团体名并设置权限。

命令模式：SNMP 配置模式

命令格式：**create community** < *string* > {**public**|**private**}

参数解释：

参数	描述
< *string* >	团体的名称
public	团体名的属性为只读
private	团体名的属性为读写

示例：创建团体名 seu，属性为读写。

```
create community seu private
```

10.23.7 create view

命令功能：创建视图名，指定该 view 包含或不包含某 mib 子树。

命令模式：SNMP 配置模式

命令格式：**create view** < *string* > [{**include**|**exclude**} <*mib-oid*>]

参数解释：

参数	描述
< *string* >	视图的名称
<*mib-oid*>	信息的路径

使用说明：不指定{**include**|**exclude**} <*mib-oid*>时，此视图缺省包含 1.3.6.1

示例：创建视图名为 school，不包含 1.3.6.2.19.2。

```
create view school exclude 1.3.6.2.19.2
```

10.23.8 set community view

命令功能：设置视图包含指定的团体名。

命令模式：SNMP 配置模式

命令格式：**set community** < *string* > **view** < *string* >

参数解释：

参数	描述
< *string* >	团体的名称/视图的名称

示例：设置视图 school 包含团体 seu。

```
set community seu view school
```

10.23.9 set engineID

命令功能：设置引擎标识。

命令模式：SNMP 配置模式

命令格式：**set engineID** <*string*>

参数解释：

参数	描述
<*string*>	引擎标识（八位位串）

示例：设置交换机引擎标识为 830900020300010289d64401。

```
set engineID 830900020300010289d64401
```

10.23.10 set group

命令功能：设置组名及其安全级别。

命令模式：SNMP 配置模式

命令格式：**set group** <*string*> **v3** {**auth**|**noauth**|**priv**} [**read** <*string*> [**write** <*string*> [**notify** <*string*>]]]

参数解释：

参数	描述
<*string*>	组名/视图名
noauth	不认证不加密
Auth	认证不加密
Priv	认证且加密
Read	读视图
Write	写视图
Notify	通知视图

示例：设置组名为 gnmae，安全级别为 priv，读、写、通知视图分别为 rview、wview、nview（不指定时，三种视图都缺省配置为 zteView）。

```
set group gname v3 priv read rview write wview notify nview
```

10.23.11 set host

命令功能：设置 trap 和 inform 主机的 IP 地址、团体名、用户名和版本。

命令模式：SNMP 配置模式

命令格式：**set host** <*A.B.C.D*> {**trap**|**inform**} {**v1**|**v2c**} <*string*>

set host < *A.B.C.D* > {**trap**|**inform**} **v3** <*string*> {**auth**|**noauth**|**priv**}

参数解释：

参数	描述
<A.B.C.D>	IP 地址
<string>	团体名/用户名
trap	类型为 trap
inform	类型为 inform
v1	SNMP 版本为 1
v2c	SNMP 版本为 v2c
v3	SNMP 版本为 v3
noauth	不认证不加密
auth	认证不加密
priv	认证且加密

示例：设置 trap 主机 10.40.44.167，团体名为 cname，版本为 v2c。

```
set host 10.40.44.167 trap v2c cname
```

示例：设置 inform 主机 10.40.44.167，版本为 v3，用户名为 uname，安全级别为 auth。

```
set host 10.40.44.167 inform v3 uname auth
```

10.23.12 set trap

命令功能：使能/关闭 SNMP 的链路断开、链路连接、链路认证失败、冷启动、热启动、集群拓扑改变、集群成员 Up/Down、loopdetect 等 trap。

命令模式：SNMP 配置模式

命令格式：**set trap** {**linkdown**|**linkup**|**authenticationfail**|**coldstart**|**warmstart**|**topologychange**|**memberupdown**|**portloopdetect**|**trunkloopdetect**|**dynamicmacexceed**|**all**} {**enable**|**disable**}

参数解释：

参数	描述
linkdown	链路断开
Linkup	链路接通
authenticationfail	链路认证失败
coldstart	冷启动
warmstart	热启动
topologychange	拓扑改变
memberupdown	成员 Up/Down
portloopdetect	端口环路检测

参数	描述
trunkloopdetect	聚合端口环路检测
dynamicMacExceed	端口动态 MAC 地址超过设置数目
all	所有支持的 TRAP 功能
enable	使能 trap
disable	关闭 trap

10.23.13 set user

命令功能：设置用户名及其所属组和安全属性。

命令模式：SNMP 配置模式

命令格式：**set user** <*string*> <*string*> **v3** [{**md5-auth**|**sha-auth**} <*string*> [**des56-priv** <*string*>]]

参数解释：

参数	描述
<*string*>	用户名/组名/认证或加密密码
md5-auth	认证类型为 md5-auth
sha-auth	认证类型为 sha-auth
des56-priv	加密类型为 des56-priv

示例：设置用户名为 uname，所属组名 gname；认证类型 md5-auth,认证密码为 zte；加密类型 des56-priv,加密密码为 zte。

```
set user uname gname v3 md5-auth zte des56-priv zte
```

10.23.14 show snmp

命令功能：显示 SNMP 信息。

命令模式：所有模式

命令格式：**show snmp** [{**community**|**engineID**|**group**|**host**|**trap**|**user**|**view**}]

参数解释：

参数	描述
community	显示 snmp 团体的信息
engineID	显示 snmp 实体引擎标识信息
group	显示 snmp 组的信息
host	显示 snmp 主机的信息
trap	显示 snmp trap 的信息
user	显示 snmp 用户的信息

view	显示 snmp 视图的信息

示例一：显示所有 SNMP 的信息。

```
show snmp
```

示例二：显示 SNMP 配置的主机地址信息。

```
show snmp host
```

10.24 RMON 配置

10.24.1 set alarm

命令功能：设置 alarm 组。

命令模式：SNMP 配置模式

命令格式：**set alarm** *<1-65535>* {**interval** *<1-65535>*|**variable** *<mib-oid>*|**sampletype** {**absolute**|**delta**}|**startup** {**rising**|**falling**|**both**}|**threshold** *<1-65535>* **eventindex** *<1-65535>* {**rising**|**falling**}|**owner** *<name>*|**status** {**valid**|**underCreation**|**createRequest**|**invalid**}}

参数解释：

参数	描述
<1-65535>	alarm 组的索引/时间间隔（单位：秒）/峰值/事件索引
<mib-oid>	信息路经
<name>	所有者的名称
absolute	alarm 组的采样类型为绝对值采样
delta	alarm 组的采样类型为相对值采样
rising	alarm 组在数据上升时触发
falling	alarm 组在数据下降时触发
both	alarm 组在数据上升和下降时触发
vaild	alarm 组的状态为 valid
underCreation	alarm 组的状态为 underCreation
createRequest	alarm 组的状态为 createRequest
invalid	alarm 组的状态为 invalid

示例一：设置索引为 10 的 alarm 实例的时间间隔为 100s。

```
set alarm 10 interval 100
```

示例二：设置索引为 10 的 alarm 实例的采样对象为 1.3.6.2.19.2。

```
set alarm 10 variable 1.3.6.2.19.2
```

示例三：设置索引为 10 的 alarm 实例的采样类型为 delta。

```
set alarm 10 sampletype delta
```

示例四：设置索引为 10 的 alarm 实例在数据上升的时候触发。

```
set alarm 10 startup rising
```

示例五：设置索引为 10 的 alarm 实例在数据上升到 30000 时触发索引为 100 的事件。

```
set alarm 10 threshold 30000 eventindex 100 rising
```

示例六：设置索引为 10 的 alarm 实例的所有者为 user1。

```
set alarm 10 owner user1
```

示例七：设置索引为 10 的 alarm 实例的状态为 invalid。

```
set alarm 10 status invalid
```

10.24.2 set event

命令功能：设置 event 组。

命令模式：SNMP 配置模式

命令格式：**set event** *<1-65535>* {**description** *<string>*|**type** {**none**|**log**|**snmptrap**|**logandtrap**}|**owner** *<name>*|**community** *<name>*|**status** {**valid**|**underCreation**|**createRequest**|**invalid**}}

参数解释：

参数	描述
<1-65535>	event 组的索引
<string>	描述信息
<name>	所有者的名称/团体名
none	event 组的类型为无操作
log	event 组的类型为记录日志
snmptrap	event 组的类型为跟踪
logandtrap	event 组的类型为跟踪且记录日志
vaild	event 组的状态为 valid
underCreation	event 组的状态为 underCreation
createRequest	event 组的状态为 createRequest
invalid	event 组的状态为 invalid

示例一：设置索引为 10 的 event 实例的描述信息为 initial。

```
set event 10 description initial
```

示例二：设置索引为 10 的 event 实例的类型为 log。

```
set event 10 type log
```

示例三：设置索引为 10 的 event 实例的团体名为 seu。

```
set event 10 community seu
```

示例四：设置索引为 10 的 event 实例的所有者名称为 tom。

```
set event 10 owner tom
```

示例五：设置索引为 10 的 event 实例的状态为 invalid。

```
set event 10 status invalid
```

10.24.3 set history

命令功能：设置 history 组。

命令模式：SNMP 配置模式

命令格式：**set history** *<1-65535>* {**datasource** *<portname>*|**bucketRequested** *<1-65535>*|**owner** *<name>*|**interval** *<1-3600>*|**status** {**valid**|**underCreation**|**createRequest**|**invalid**}}

参数解释：

参数	描述
<1-65535>	history 组的索引/buckerRequest 的值
<portname>	一个端口号或者一个端口名
<name>	所有者的名称
<1-3600>	history 组的时间间隔，单位：秒
vaild	history 组的状态为 valid
underCreation	history 组的状态为 underCreation
createRequest	history 组的状态为 createRequest
invalid	history 组的状态为 invalid

示例一：设置索引为 10 的 history 实例的数据来源为端口 1。

```
set history 10 datasource 1
```

示例二：设置索引为 10 的 history 实例的数据来源为端口 userx。

```
set history 10 datasource userx
```

示例三：设置索引为 10 的 history 实例的 buckerRequest 为 100。

```
set history 10 bucketRequest 100
```

示例四：设置索引为 10 的 history 实例的所有者名称为 tom。

```
set history 10 owner tom
```

示例五：设置索引为 10 的 history 实例的时间间隔为 100s。

```
set history 10 interval 100
```

示例六：设置索引为 10 的 history 实例的状态为 invalid。

```
set history 10 status invalid
```

10.24.4 set rmon

命令功能：开启/关闭 rmon。

命令模式：SNMP 配置模式

命令格式：**set rmon** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 rmon
disable	关闭 rmon

10.24.5 set statistics

命令功能：设置 statistics 组。

命令模式：SNMP 配置模式

命令格式：**set statistics** *<1-65535>* {**datasource** *<portname>*|**owner** *<name>*|**status** {**valid**|**underCreation**|**createRequest**|**invalid**}}

参数解释：

参数	描述
<1-65535>	statistics 组的索引
<portname>	一个端口号或者一个端口名
<name>	所有者的名称
vaild	statistics 组的状态为 valid
underCreation	statistics 组的状态为 underCreation

参数	描述
createRequest	statistics 组的状态为 createRequest
invalid	statistics 组的状态为 invalid

示例一：设置索引为 10 的 statistics 实例的数据来源为端口 1。

```
set statistics 10 datasource 1
```

示例二：设置索引为 10 的 statistics 实例的数据来源为端口 userx。

```
set statistics 10 datasource userx
```

示例三：设置索引为 10 的 statistics 实例的所有者名称为 tom。

```
set statistics 10 owner tom
```

示例四：设置索引为 10 的 statistics 实例的状态为 invalid。

```
set statistics 10 status invalid
```

10.24.6 show alarm

命令功能：显示 alarm 组的配置信息。

命令模式：所有模式

命令格式：**show alarm** [*<1-65535>*]

参数解释：

参数	描述
<1-65535>	alarm 组的索引

示例一：显示所有 alarm 实例的 rmon 信息。

```
show alarm
```

示例二：显示索引为 10 的 alarm 实例的 rmon 信息。

```
show alarm 10
```

10.24.7 show event

命令功能：显示 event 组的配置信息。

命令模式：所有模式

命令格式：**show event** [*<1-65535>*]

参数解释：

参数	描述
<1-65535>	event 组的索引

示例一：显示所有 event 实例的 rmon 信息。

```
show event
```

示例二：显示索引为 10 的 event 实例的 rmon 信息。

```
show event 10
```

10.24.8 show history

命令功能：显示 history 组的配置信息。

命令模式：所有模式

命令格式：**show history** [*<1-65535>*]

参数解释：

参数	描述
<1-65535>	history 组的索引

示例一：显示所有存在的 history 实例的 rmon 信息。

```
show history
```

示例二：显示索引为 10 的 history 实例的 rmon 信息。

```
show history 10
```

10.24.9 show rmon

命令功能：显示 rmon 的状态。

命令模式：所有模式

命令格式：**show rmon**

10.24.10 show statistics

命令功能：显示 statistics 组的配置信息。

命令模式：所有模式

命令格式：**show statistics** [*<1-65535>*]

参数解释：

参数	描述
<1-65535>	statistics 组的索引

10.25 集群管理配置

10.25.1 erase member

命令功能：删除集群成员交换机配置。

命令模式：集群管理配置模式

命令格式：**erase member {<*idlist*>|all}**

参数解释：

参数	描述
<idlist>	成员交换机 ID 号
all	所有成员交换机

示例：删除集群成员 ID 号为 2 的交换机信息。

```
erase member 2
```

10.25.2 reboot member

命令功能：重启成员交换机。

命令模式：集群管理配置模式

命令格式：**reboot member {<*idlist*>|all}**

参数解释：

参数	描述
<idlist>	成员交换机 ID 号
all	所有成员交换机

示例：重启集群成员 ID 号为 1 的交换机。

```
reboot member 1
```

10.25.3 save member

命令功能：保存集群成员交换机信息。

命令模式：集群管理配置模式

命令格式：**save member {<*idlist*>|all}**

参数解释：

参数	描述
<*idlist*>	成员交换机 ID 号
all	所有成员交换机

示例：保存集群成员 ID 号为 4 的交换机信息。

```
save member 4
```

10.25.4 set group add device

命令功能：按设备号增加一个成员。

命令模式：集群管理配置模式

命令格式：**set group add device** <*idlist*>

参数解释：

参数	描述
<*idlist*>	设备 ID 号

示例：将设备号为 3 的设备加入集群。

```
set group add device 3
```

10.25.5 set group add mac

命令功能：按设备 MAC 地址增加一个成员，并指定成员 ID 号。

命令模式：集群管理配置模式

命令格式：**set group add mac** <*xx.xx.xx*> [<*1-255*>]

参数解释：

参数	描述
<*xx.xx.xx*>	设备 MAC 地址的后半部分
<*1-255*>	成员 ID 号

示例：将 MAC 地址为 00.d0.d0.f2.d0.f5 的设备加入集群，并指定成员 ID 号为 4。

```
set group add mac f2.d0.f5 4
```

10.25.6 set group candidate

命令功能：设定交换机角色为候选交换机。

命令模式：集群管理配置模式

命令格式：**set group candidate**

10.25.7 set group commander ipport

命令功能：设定交换机为命令交换机，指定用于集群管理的三层端口号，并设定用户集群管理的 IP 地址池。

命令模式：集群管理配置模式

命令格式：**set group commander ipport** *<0-63>* [**ip-pool** *<A.B.C.D/M>*]

参数解释：

参数	描述
<0-63>	三层端口号
<A.B.C.D/M>	IP 地址/掩码

示例：设定命令交换机，并指定三层端口 3 用作集群管理，同时设定 IP 地址池为 192.168.1.2/24。

```
set group commander ipport 3 ip-pool 192.168.1.2/24
```

10.25.8 set group delete member

命令功能：按成员 ID 号删除一个成员。

命令模式：集群管理配置模式

命令格式：**set group delete member** *<idlist>*

参数解释：

参数	描述
<idlist>	成员 ID 号

示例：删除成员 ID 号为 3 的成员。

```
set group delete member 3
```

10.25.9 set group independent

命令功能：设定交换机角色为独立交换机。

命令模式：集群管理配置模式

命令格式：**set group independent**

10.25.10 set group handtime

命令功能：设置成员交换机和命令交换机定时握手的间隔时间。

命令模式：集群管理配置模式

命令格式：**set group handtime** *<1-300>*

参数解释：

参数	描述
<1-300>	成员交换机和命令交换机定时握手间隔时间，单位：秒，缺省为 8 秒

示例：设置成员交换机和命令交换机定时握手间隔时间为 10 秒。

```
set group handtime 10
```

10.25.11 set group holdtime

命令功能：命令交换机配置成员交换机信息的有效保留时间。

命令模式：集群管理配置模式

命令格式：**set group holdtime** *<1-300>*

参数解释：

参数	描述
<1-300>	命令交换机配置成员交换机信息的有效保留时间，单位：秒，缺省为 80 秒

示例：设置命令交换机配置成员交换机信息的有效保留时间为 100 秒。

```
set group holdtime 100
```

10.25.12 set group name

命令功能：设置集群名称。

命令模式：集群管理配置模式

命令格式：**set group name** *<name>*

参数解释：

参数	描述
<name>	设置集群名称

示例：设置集群名称为 zte。

```
set group name zte
```

10.25.13 set group tftpsvr

命令功能：指定集群 TFTP 服务器的 IP 地址。

命令模式：集群管理配置模式

命令格式：**set group tftpsvr** < A.B.C.D>

参数解释：

参数	描述
<A.B.C.D>	IP 地址

示例：指定集群 TFTP 服务器的 IP 地址为 192.168.200.1。

```
set group tftpsvr 192.168.200.1
```

10.25.14 set group syslogsvr

命令功能：指定集群 SYSLOG 服务器的 IP 地址。

命令模式：集群管理配置模式

命令格式：**set group syslogsvr** < A.B.C.D>

参数解释：

参数	描述
<A.B.C.D>	IP 地址

示例：指定集群 SYSLOG 服务器的 IP 地址为 192.168.200.1。

```
set group syslogsvr 192.168.200.1
```

10.25.15 set zdp

命令功能：使能/关闭交换机的邻居发现功能。

命令模式：集群管理配置模式

命令格式：**set zdp** {**enable**|**disable** }

参数解释：

参数	描述
enable	使能交换机的邻居发现功能
disable	关闭交换机的邻居发现功能

10.25.16 set zdp holdtime

命令功能：接受设备保存本设备发送的 ZDP 报文的时间。

命令模式：集群管理配置模式

命令格式：**set zdp holdtime** <*10-255*>

参数解释：

参数	描述
<*10-255*>	接受设备保存本设备发送的 ZDP 报文的时间，缺省为 180 秒

10.25.17 set zdp port

命令功能：在某端口上使能/关闭交换机的邻居发现功能。

命令模式：集群管理配置模式

命令格式：**set zdp port** <*portlist*> {**enable**|**disable**}

参数解释：

参数	描述
<*portlist*>	端口列表
enable	使能交换机的邻居发现功能
disable	关闭交换机的邻居发现功能

示例：在端口 2 上使能交换机的邻居发现功能。

```
set zdp port 2 enable
```

10.25.18 set zdp timer

命令功能：ZDP 报文的发送时间间隔。

命令模式：集群管理配置模式

命令格式：**set zdp timer** <*5-255*>

参数解释：

参数	描述
<5-255>	ZDP 报文的发送时间间隔，单位：秒，缺省为 30 秒

示例：设置 ZDP 报文的发送时间间隔为 70 秒。

```
set zdp timer 70
```

10.25.19 set zdp trunk

命令功能：在某 trunk 上使能/关闭交换机的邻居发现功能。

命令模式：集群管理配置模式

命令格式：**set zdp trunk** <*trunklist*> {**enable**|**disable**}

参数解释：

参数	描述
<*trunklist*>	Trunk 列表
enable	使能交换机的邻居发现功能
disable	关闭交换机的邻居发现功能

示例：在 trunk 2 上使能交换机的邻居发现功能。

```
set zdp trunk 2 enable
```

10.25.20 set ztp

命令功能：使能/关闭交换机的拓扑收集功能。

命令模式：集群管理配置模式

命令格式：**set ztp** {**enable**|**disable**}

参数解释：

参数	描述
enable	使能交换机的拓扑收集功能
disable	关闭交换机的拓扑收集功能

10.25.21 set ztp hop

命令功能：配置拓扑收集范围（跳数）。

命令模式：集群管理配置模式

命令格式：**set ztp hop** <*1-128*>

参数解释：

参数	描述
<1-128>	拓扑收集范围（跳数），缺省为 4

10.25.22 set ztp hopdelay

命令功能：被收集设备转发拓扑收集报文前延迟等待的时间。

命令模式：集群管理配置模式

命令格式：**set ztp hopdelay** *<1-1000>*

参数解释：

参数	描述
<1-1000>	被收集设备转发拓扑收集报文前延迟等待的时间，单位：毫秒，缺省为 200 毫秒

示例：设置被收集设备转发拓扑收集报文前延迟等待的时间为 400 毫秒。

```
set ztp hopdelay 400
```

10.25.23 set ztp port

命令功能：在某端口上使能/关闭交换机的拓扑收集功能。

命令模式：集群管理配置模式

命令格式：**set ztp port** *<portlist>* {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	使能交换机的拓扑收集功能
disable	关闭交换机的拓扑收集功能

示例：在端口 2 上使能交换机的拓扑收集功能。

```
set ztp port 2 enable
```

10.25.24 set ztp portdelay

命令功能：被收集设备下一个端口转发拓扑收集报文前延迟等待的时间。

命令模式：集群管理配置模式

命令格式：**set ztp portdelay** *<1-100>*

参数解释：

参数	描述
<1-100>	被收集设备下一个端口转发拓扑收集报文前延迟等待的时间，单位：毫秒，缺省为 20 毫秒

示例：设置被收集设备转发拓扑收集报文前延迟等待的时间为 40 毫秒。

```
set ztp portdelay 40
```

10.25.25 set ztp timer

命令功能：启动自动拓扑收集的间隔时间。

命令模式：集群管理配置模式

命令格式：**set ztp timer** *<0-60>*

参数解释：

参数	描述
<0-60>	间隔时间，单位：分钟，0 表示不收集

示例：启动拓扑自动收集的间隔时间为 2 分钟。

```
set ztp timer 2
```

10.25.26 set ztp trunk

命令功能：在某 trunk 上使能/关闭交换机的拓扑收集功能。

命令模式：集群管理配置模式

命令格式：**set ztp trunk** *<trunklist>* {**enable**|**disable** }

参数解释：

参数	描述
<trunklist>	Trunk 列表
enable	使能交换机的拓扑收集功能
disable	关闭交换机的拓扑收集功能

示例：在 trunk 2 上使能交换机的拓扑收集功能。

```
set zdp trunk 2 enable
```

10.25.27 set ztp vlan

命令功能：指定在某个 VLAN 进行拓扑收集。

命令模式：集群管理配置模式

命令格式：**set ztp vlan** *<1-4094>*

参数解释：

参数	描述
<1-4094>	VLAN ID，从 1 到 4094 的任意一个数

示例：指定在 vlan 40 中进行拓扑收集。

```
set ztp vlan 40
```

10.25.28 show group

命令功能：显示集群管理信息。

命令模式：所有模式

命令格式：**show group**

10.25.29 show group candidate

命令功能：显示集群候选交换机信息。

命令模式：所有模式

命令格式：**show group candidate**

10.25.30 show group member

命令功能：显示集群成员交换机信息。

命令模式：所有模式

命令格式：**show group member** [*<1-255>*]

参数解释：

参数	描述
<1-255>	成员交换机 ID 号

示例：显示集群成员 ID 号为 6 的交换机信息。

```
show group member 6
```

10.25.31 show zdp

命令功能：显示交换机 ZDP 功能的配置信息。

命令模式：所有模式

命令格式：**show zdp**

10.25.32 show zdp neighbour

命令功能：显示被 ZDP 协议发现的邻居设备的信息。

命令模式：所有模式

命令格式：**show zdp neighbour** [**detail**]

10.25.33 show ztp

命令功能：显示拓扑收集协议的配置信息。

命令模式：所有模式

命令格式：**show ztp**

10.25.34 show ztp device

命令功能：按设备号显示拓扑收集协议的配置信息。

命令模式：所有模式

命令格式：**show ztp device** [<*idlist*>]

参数解释：

参数	描述
<*idlist*>	设备号

示例：显示拓扑收集结果中设备号为 2 的设备信息。

```
show ztp device 2
```

10.25.35 show ztp mac

命令功能：按设备 MAC 地址显示拓扑收集协议的配置信息。

命令模式：所有模式

命令格式：**set ztp mac** <*xx.xx.xx*>

参数解释：

参数	描述
<*xx.xx.xx*>	MAC 地址的后半部分

示例：按设备 MAC 地址显示拓扑收集协议的配置信息。

```
set ztp mac f2.d0.f5
```

10.25.36 ztp start

命令功能：启动拓扑信息收集过程。

命令模式：集群管理配置模式

命令格式：**ztp start**

10.26 WEB 配置

10.26.1 set web

命令功能：开启/关闭 web 功能。

命令模式：全局配置模式

命令格式：**set web** {**enable**|**disable**}

参数解释：

参数	描述
enable	开启 web 功能
disable	关闭 web 功能

10.26.2 set web listen-port

命令功能：设置 web 的监听功能。

命令模式：全局配置模式

命令格式：**set web listen-port** <80,1025-49151>

参数解释：

参数	描述
<80,1025-49151>	WEB 使用的 TCP 端口号，默认使用 80

10.27 单端口环路检测

10.27.1 set loopdetect blockdelay

命令功能：设置环路时端口被 block 的时间间隔。

命令模式：全局配置模式

命令格式：**set loopdetect blockdelay** *<1-1080>*

参数解释：

参数	描述
<1-1080>	时间间隔，单位：分钟，缺省为 5 分钟

10.27.2 set loopdetect sendpktinterval

命令功能：设置环路检测发送报文的间隔时间。

命令模式：全局配置模式

命令格式：**set loopdetect sendpktinterval** *<5-60>*

参数解释：

参数	描述
<5-60>	时间间隔，单位：秒，缺省为 15 秒

10.27.3 set loopdetect port

命令功能：开启/关闭端口环路检测，此时检测端口的 pvid 所在的 vlan。

命令模式：全局配置模式

命令格式：**set loopdetect port** *<portlist>* {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	开启端口环路检测
disable	关闭端口环路检测

10.27.4 set loopdetect port vlan

命令功能：开启/关闭端口在指定 vlan 中的环路检测。

命令模式：全局配置模式

命令格式：**set loopdetect port** *<portlist>* **vlan** *<1-4094>* {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
<1-4094>	Vlan ID
enable	开启端口环路检测
disable	关闭端口环路检测

10.27.5 set loopdetect port protect

命令功能：当发生端口环路时开启/关闭端口保护。

命令模式：全局配置模式

命令格式：**set loopdetect port** *<portlist>* **protect** {**enable**|**disable**}

参数解释：

参数	描述
<portlist>	端口列表
enable	开启端口保护
disable	关闭端口保护

10.27.6 set loopdetect trunk

命令功能：开启/关闭 trunk 环路检测，此时检测 trunk 的 pvid 所在的 vlan。

命令模式：全局配置模式

命令格式：**set loopdetect trunk** *<trunklist>* {**enable**|**disable**}

参数解释：

参数	描述
<trunklist>	Trunk ID 列表
enable	开启 trunk 环路检测
disable	关闭 trunk 环路检测

10.27.7 set loopdetect trunk vlan

命令功能：开启/关闭 trunk 在指定 vlan 中的环路检测。

命令模式：全局配置模式

命令格式：**set loopdetect trunk** *<trunklist>* **vlan** *<1-4094>* {**enable**|**disable**}

参数解释：

参数	描述
<trunklist>	Trunk ID 列表

<1-4094>	Vlan ID
enable	开启 trunk 环路检测
disable	关闭 trunk 环路检测

10.27.8 set loopdetect trunk protect

命令功能：当发生 trunk 环路时开启/关闭 trunk 保护。

命令模式：全局配置模式

命令格式：**set loopdetect trunk** *<trunklist>* **protect** {**enable**|**disable**}

参数解释：

参数	描述
<trunklist>	Trunk ID 列表
enable	开启 trunk 保护
disable	关闭 trunk 保护

10.27.9 show loopdetect

命令功能：显示端口环路信息。

命令模式：所有模式

命令格式：**show loopdetect**

附录A 缩略语

缩写	英文全称	中文全称
ABR	Area Border Router	区域边界路由器
ACL	Access Control List	访问控制列表
AD	Administrative Distance	管理距离
ARP	Address ResolutionProtocol	地址解析协议
AS	Autonomous System	自治系统
ASBR	Autonomous System Border Router	自治系统边界路由器
ATM	Asynchronous Transfer Mode	异步传输模式
BGP	Border Gateway Protocol	边界网关协议
BOOTP	BOOTstrap Protocol	引导程序协议
BRD	Backup Designate Router	备用指定路由器
CHAP	Challenge Handshake Authentication Protocol	Challenge 握手鉴别协议
CIDR	Classless Inter-Domain Routing	无类别域间路由
CLNP	ConnectionLess Network Protocol	无连接网络协议
CLNS	ConnectionLess Network Sevice	无连接网络服务
CoS	Class of Service	服务类别
CRC	Cyclic Redundancy Check	循环冗余校验
CRLDP	Constraint based Routing Label Distribution Protocol	受限的标记分布协议
CSN	Cryptographic Sequence Number	密码序列号
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DIS	Designate IS	指定 IS 路由器
DNS	Domain Name System	域名系统
DR	Designate Router	指定路由器
EBGP	External Border Gateway Protocal	外部边界网关协议
EGP	External Gateway Protocol	外部网关协议
ES	End System	末端系统
FEC	Forwarding Equivalence Class	转发等价类
FIFO	First In and First Out	先进先出
FPGA	Field Programmable Gate Array	现场可编程门阵列
FSM	FiniteState Machine	有限状态机
FTP	File Transfer Protocol	文件传输协议
GARP	Generic Attribute Registration Protocol	通用属性注册协议
GBIC	Gigabit Interface Converter	千兆位接口转换器
GRE	General Routing Encapsulation	通用路由封装
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
ICMP	Internet Control Message Protocol	Internet 控制报文协议

缩写	英文全称	中文全称
IETF	Internet Engineering Task Force	Internet 工程任务组
IGMP	Internet Group Mangement Protocol	Internet 组管理协议
IGP	Interior Gateway Protocol	内部网关协议
IP	Internet Protocol	网际协议
ISO	International Organization for Standardization	国际标准化组织
ISP	Internet Service Provider	Internet 服务提供商
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LAN	Local Area Network	局域网
LAPB	Link Access Procedure Balanced	平衡型链路访问规程
LCP	Link Control Protocol	链路控制协议
LDP	Label Distribution Protocol	标记分布协议
LSA	Link State Advertisement	链接状态通告
LSP	Link State PDU	链接状态 PDU
LSR	Label Switch Router	标签交换路由器
MAC	Media Access Control	介质访问控制
MD5	Message Digest 5	信息摘要 5
MED	MULTI_EXIT_DISC	多出口鉴别
MIB	Management Information Base	管理信息库
MPLS	Multi-Protocol Label Switching	多协议标记交换
MSTP	Multiple Spanning Tree Protocol	多生成树协议
MTU	Maximum Transmission Unit	最大传输单元
NAT	Network Address Translation	网络地址转换
NBMA	Non-Broadcast Multiple Access	非广播多路访问
NCP	Network Control Protocol	网络控制协议
NIC	Network Information Center	网络信息中心
NLRI	Network Layer Reachable Information	网络层可达信息
NMS	Network Management System	网络管理系统
NSAP	Network Service Access Point	网络服务访问点
NSP	Network Service Provider	网络服务提供商
NTP	Network Time Protocol	网络时间协议
NVT	Network Virtual Terminal	网络虚拟终端
OAM	Operation And Management	操作与管理
OSI	Open Systems Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
PAP	Passwork Authentication Protocol	密码鉴别协议
PAT	Port Address Translation	端口地址转换
PCM	Pulse Code Modulation	脉冲编码调制
PDU	Protocol Data Unit	协议数据单元
POS	Packet over SDH	包在 SDH 上传输

缩写	英文全称	中文全称
PPP	Point-to-Point Protocol	点对点协议
PSNP	Partial Sequence Num PDU	部分序列号 PDU
QoS	Quality of Service	服务质量
RARP	Reverse Address Resolution Protocol	逆地址解析协议
RADIUS	Remote Authentication Dial In User Service	远程认证拨入用户服务
RFC	Request For Comments	Internet 的文档
RIP	Routing Information Protocol	路由信息协议
RLE	Route lookup engine	路由查找引擎
RMON	Remote Monitoring	远程监控
ROS	Router Operation System	路由器操作系统
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
RSVP	Resource Reservation Protocol	资源预留协议
SDH	Synchronous Digital Hierarchy	同步数字系列
SDLC	Synchronous Data Link Control	同步数据链路控制
SMTP	Simple Mail Transfer Protocol	简单邮件传送协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SNP	Sequence Num PDU	序列号 PDU
SPF	Shortest Path First	最短路径优先
STP	Spanning Tree Protocol	生成树协议
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传送协议
ToS	Type Of Service	服务类型
TELNET	Telecommunication Network Protocol	远程登录协议
TTL	Time To Live	生存时间
UDP	User Datagram Protocol	用户数据报协议
VID	VLAN Identifier	VLAN 标识符
VLSM	Variable Length Subnet Mask	可变长子网掩码
VPN	Virtual Private Network	虚拟专用网
VRF	Virtual Routing Forwarding	虚拟路由转发
VRRP	Virtual Router Redundancy Protocol	虚拟路由器冗余协议
WAN	Wide Area Network	广域网
WWW	World Wide Web	万维网
ZGMP	Zte Group Manage Protocol	ZTE 集群管理协议