



## S3100系列全千兆管理型交换机

# 用户手册

©copyright 2011 by Shenzhen TG-NET Botone Technology Co.,Ltd. All rights reserved.

事先未征得深圳市万网博通科技有限公司(以下简称TG-NET)的书面同意, 任何人不得以任何方式拷贝或复制本文档中的任何内容。

TG-NET不做与本文档相关的任何保证, 不做商业性、质量或特定用途适用性的任何隐含保证。本文档中的信息随时可能变更, 而不另行通知。TG-NET保留对本出版物做修订而不通知任何个人或团体此类变更的权利。

### 深圳市万网博通科技有限公司

地址: 深圳市龙华新区大浪街道华荣路北昱南通科技工业园2栋

邮编: 518109

服务电话: 400-088-7500

网址: <http://www.tg-net.cn>

## 目 录

<b>第一部分 硬件安装指导 .....</b>	<b>5</b>
第1章 使用说明 .....	5
1.1 用途 .....	5
1.2 前面板 .....	5
1.3 后面板 .....	7
第2章 安装前的准备 .....	7
2.1 注意事项 .....	7
2.2 检查安装场所 .....	8
2.3 安装工具 .....	8
第3章 安装 .....	9
3.1 交换机的安装 .....	9
3.2 电源线及地线连接 .....	9
3.3 安装完后的检查 .....	10
第4章 技术资料详细说明 .....	11
<b>第二部分 WEB配置指导 .....</b>	<b>13</b>
第1章 系统登陆 .....	13
第2章 设备状态 .....	14
2.1 系统状态 .....	14
2.2 端口统计 .....	15
2.3 端口详细统计 .....	16
2.4 LACP 状态统计 .....	16
2.5 RSTP 信息统计 .....	17
2.6 IGMP 状态统计 .....	18

第3章 设备基本配置 .....	19
3.1 系统配置 .....	19
3.2 端口配置 .....	20
3.3 流量控制 .....	21
第4章 设备高级配置 .....	22
4.1 IGMP配置 .....	22
4.2 VLAN配置 .....	22
4.3 ARP配置 .....	27
4.4 链路汇聚 .....	28
4.5 LACP端口配置 .....	29
4.6 RSTP系统配置 .....	30
4.7 802.1X配置 .....	31
4.8 端口镜像配置 .....	32
4.9 QoS配置 .....	33
4.10 风暴控制 .....	34
4.11 PING .....	35
第5章 系统维护 .....	36
5.1 软件升级 .....	36
5.2 配置管理 .....	37
5.3 系统热重启 .....	38
5.4 恢复出厂设置 .....	38
<b>第三部分 CLI配置指导 .....</b>	<b>40</b>
第1章 系统配置 .....	42
第2章 CONSOLE参数配置 .....	43
第3章 端口配置 .....	44
第4章 MAC配置 .....	45
第5章 VLAN配置 .....	47
第6章 ARP配置 .....	48
第7章 端口聚合配置 .....	49
第8章 LACP配置 .....	51

第9章 快速生成树配置 .....	52
第10章 用户组配置 .....	53
第11章 Qos配置 .....	54
第12章 端口镜像配置 .....	56
第13章 IP地址配置 .....	57
第14章 DOT1X配置 .....	59
第15章 IGMP配置 .....	60
<b>第四部分 附录 常见故障诊断 .....</b>	<b>62</b>

## 物品清单

小心打开交换机包装盒，检查包装盒里面应有以下配件：

- 一台S3100系列全千兆管理型交换机；
- 一根交流电源连接线；
- 一根DB9-RJ45串口线；
- 一张用户手册光盘；
- 一张保修卡与合格证；
- 安装组件和其它配件；

如果发现有所损坏或者任何配件短缺情况，请及时和当地经销商联系；

# 第一部分 硬件安装指导

## 使用说明

### 用途

S3100系列交换机包括以下四个型号：

- 1) S3100-24G: 24个10/100/1000M电口, 1个Console口;
- 2) S3100-24G-2F:  
2F: 24个10/100/1000M电口, 2个千兆SFP复用光口, 1个Console口;
- 3) S3100-16F-8G:  
8G: 16个千兆SFP光口, 8个10/100/1000M电口, 1个Console口;
- 4) S3100-8F-8G:  
8G: 8个千兆SFP光口, 8个10/100/1000M电口, 1个Console口;

本手册的用途是帮助您正确地使用S3100系列全千兆管理型交换机。

### 前面板

- 1) S3100-24G

提供24个10/100/1000M电口, 交换机的前面板示意图如1.1.1所示。



图1.1.1 S3100-24G以太网交换机前面板示意图

- 2) S3100-24G-2F

提供24个10/100/1000M电口，2个千兆SFP复用光口，交换机的前面板示意图如1.1.2所示。



图1.1.2 S3100-24G-2F以太网交换机前面板示意图

### 3) S3100-16F-8G

提供16个千兆SFP光口，8个10/100/1000M电口，交换机的前面板示意图如1.1.3所示。



图1.1.3 S3100-16F-8G以太网交换机前面板示意图

### 4) S3100-8F-8G

提供8个千兆SFP光口，8个10/100/1000M电口，交换机的前面板示意图如1.1.4所示。



图1.1.4 S3100-8F-8G以太网交换机前面板示意图

## ➤ 指示灯

指示灯位于机器前面板的左侧。

1 □ Power指示灯(电源指示灯)

它的位置在面板的最左侧的上边, 交换机接上电源后, 此指示灯为常亮。如果指示灯不亮, 请检查是否连接好了电源。

#### 2) System指示灯(系统指示灯)

它的位置在面板的最左侧的下边即Power正下方, 当该指示灯闪亮时, 表示交换机上的系统工作正常。

#### 3) 10/100Mbps Link/ACT指示灯

当某端口协商为10/100Mbps连通时, 相对应端口左边的10/100Mbps

Link/ACT指示灯点亮为黄色; 当端口有数据通讯时, 相对应端口左边的10/100Mbps Link/ACT黄色指示灯开始闪烁;

#### 4) 1000Mbps Link/ACT指示灯

当某端口协商为1000Mbps连通时, 相对应端口左边的1000Mbps

Link/ACT指示灯点亮为绿色; 当端口有数据通讯时, 相对应端口左边的1000Mbps

Link/ACT绿色指示灯开始闪烁;

## 后面板

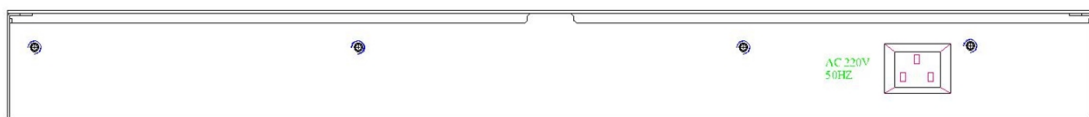


图1.1.5 S3100以太网交换机后面板示意图

**电源插座:**这是一个三芯电源插座, 把电源线母头接到这个插座上, 公头接到交流电源上。



## 安装前的准备

### 注意事项

为避免使用不当造成设备损坏及对人身伤害，请遵从以下的注意事项：

- 在清洁交换机前，应先将交换机电源插头拔出。不要用湿润的布料擦拭交换机，不可用液体清洗交换机。
- 请不要将交换机放在水边或潮湿的地方，并防止水或湿气进入交换机机壳。
- 请不要将交换机放在不稳定的箱子或桌子上，万一跌落，会对交换机造成严重损害。
- 应保持室内通风良好并保持交换机通气孔畅通。
- 交换机要在正确的电压下才能正常工作，请确认工作电压同交换机所标示的电压相符。
- 为减少受电击的危险，在交换机工作时不要打开外壳，即使在不带电的情况下，也不要随意打开交换机机壳。
- 在更换接口板时一定要使用防静电手腕，防止静电损坏单板。

### 检查安装场所

以太网交换机必须在室内使用，无论您将交换机安装在机柜内还是直接放在工作台上，都需要保证以下条件：

- 确认交换机的入风口及通风口处留有空间，以利于交换机机箱的散热。
- 确认机柜和工作台自身有良好的通风散热系统。
- 确认机柜及工作台足够牢固，能够支撑交换机及其安装附件的重量。

- 确认机柜及工作台的良好接地。

### 安装工具

- 一字螺丝刀
- 十字螺丝刀
- 防静电手腕

## 安装

### 交换机的安装

#### 交换机安装到19英寸机柜

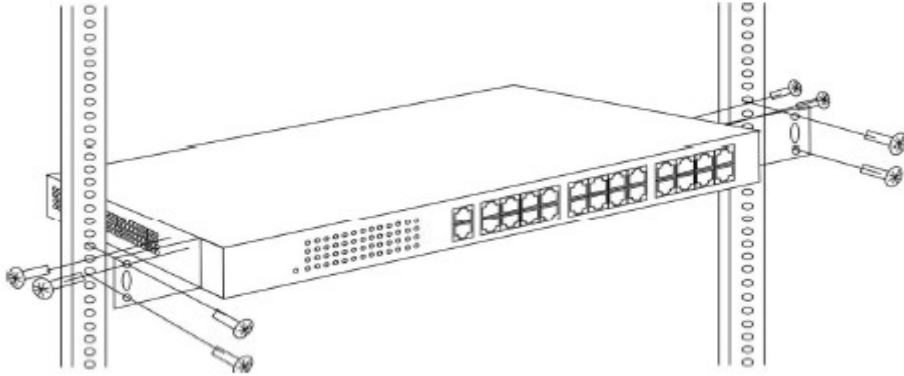


图1.3.1交换机可以安装到19英寸标准机柜中

#### 交换机安装到工作台

很多情况下，用户并不具备19英寸标准机柜，此时，人们经常用到的方法就是将交换机放置在干净的工作台上，此种操作比较简单，操作中，只要注意如下事项即可：

- 保证工作台的平稳性与良好接地；
- 交换机四周留出10cm的散热空间；
- 不要在交换机上放置重物

### 电源线及地线连接

#### 交流电源插座(建议)

建议使用有中性点接头的单相三线电源插座，或多功能计算机电源插座

。电源的中性点在建筑物中要可靠接地，一般楼房在施工布线时，已将本楼供电系统的电源中性点埋地，用户需要确认本楼电源是否已经接地

。

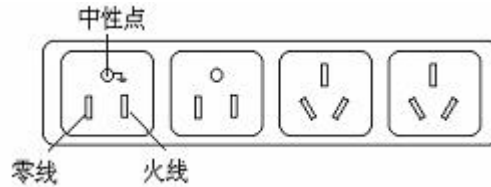


图1.3.2建议使用的电源插座

## 交流电源线连接

第一步：将交换机的电源线一端插到交换机机箱后面板的电源插座上，另一端插到外部的供电交流电源插座上。

第二步：检查交换机前面板的电源指示灯(PWR)是否变亮，灯亮则表示电源连接正确。

## 安装完后的检查

- 检查选用电源与交换机的标识电源是否一致；
- 检查地线是否连接；
- 检查配置电缆、电源输入电缆连接关系是否正确；
- 检查接口线缆是否都在室内走线，无户外走线现象；若有户外走线情况，请检查是否进行了交流电源防雷插排、网口防雷器等的连接

。

## 技术资料详细说明

### ➤ 硬件规格

项目	S3100-16F-8G	S3100-8F-8G	S3100-24G-2F	S3100-24G
固定端口	16个千兆SFP光口	8个千兆SFP光口	24个10/100/1000M电口	24个10/100/1000M电口
	8个10/100/1000M电口	8个10/100/1000M电口	2个千兆SFP复用光口	
管理端口	1个Console口			
交换容量	≥48Gbps			
包转发率	36Mpps			
工作温度	-20~50°C			
存储温度	-40~70°C			
工作湿度	10%~90%无凝结			
存储湿度	5%~95%无凝结			
外观尺寸	440(L)×285(W)×44.5(H)mm			
整机重量	<4Kg			
输入电压	AC:110~240V/50~60Hz			
整机功耗	<30W			

图表 4-1 S3100系列交换机硬件功能说明

### ➤ 软件功能

项目	S3100-16F-8G	S3100-8F-8G	S3100-24G-2F	S3100-24G
支持协议标准	IEEE 802.3ad, 链路聚合协议;			
	IEEE 802.3, 10BASE-T以太网;			
	IEEE 802.3u, 快速以太网标准;			
	IEEE 802.3ab, 千兆以太网标准;			
	IEEE 802.3z, 千兆以太网光纤标准;			
	IEEE 802.3x, 全双工以太网数据链路层流控;			
	IEEE 802.1q, VLAN标准;			
	IEEE 802.1p, QoS/CoS服务质量;			
	IEEE 802.1d, 生成树协议;			
IEEE 802.1w, 快速生成树协议;				
MAC地址	支持8K MAC地址表; 支持自动更新, 双向学习;			
VLAN	最多支持64个VLAN;			
	支持基于端口的 VLAN; 支持802.1Q标准 VLAN;			
生成树	支持STP生成树协议;			
	支持RSTP快速生成树协议;			
端口汇聚	支持12组汇聚, 每组最多支持12个端口;			
	支持静态聚合、动态聚合;			
端口镜像	支持多对一的端口镜像, 对镜像源端口的数量没有限制			
环路保护	支持环路检测/环路避免			
端口流控	支持半双工基于背压式控制;			
	支持全双工基于PAUSE帧;			
端口限速	支持基于端口的输入/输出带宽管理			

组播控制	支持IGMP Snooping
风暴抑制	支持对广播、组播、DLF泛洪、ICMP等进行抑制
安全特性	支持用户端口+IP地址+MAC地址； 支持IEEE 802.1x端口认证；
QOS	SP (Strict Priority), 严格优先级轮转算法； WFQ (Weighted Fair Queuing) 加权公平排队； WRR (Weighted Round Robin), 加权优先级轮转算法； 802.1p端口队列优先级算法； Differentiated Service, 区分式服务；
网线线序	支持Auto-MDIX功能, 自动识别直通网线和交叉网线
协商模式	支持端口自动协商功能(自协商传输速率和双工模式)
系统维护	支持配置文件上传/下载； 支持升级包上传； 支持WEB恢复出厂配置；
网络管理	支持TGCP云平台管理； 支持WEB界面管理； 支持CLI界面管理； 支持SNMP网管；

图表 4-2 S3100系列交换机软件功能说明

# 第一部分 WEB配置指导



**注意:**

本手册中所有图示如无特殊说明均以S3100-24G-2F交换机为例。

## 系统登陆

S3100系列交换机采用web视图方式进行管理, 交换机的缺省IP是192.168.255.1。在登陆之前, 请确保管理PC的IP地址与交换机IP地址在同一网段内, 否则无法访问交换机管理IP地址。设置好后, 在浏览器中输入192.168.255.1, 即可访问交换机的配置页面。

该WEB界面分为四大模块, 分别为设备状态、设备基本配置、设备高级配置、系统维护。下面将分别对各模块进行介绍。

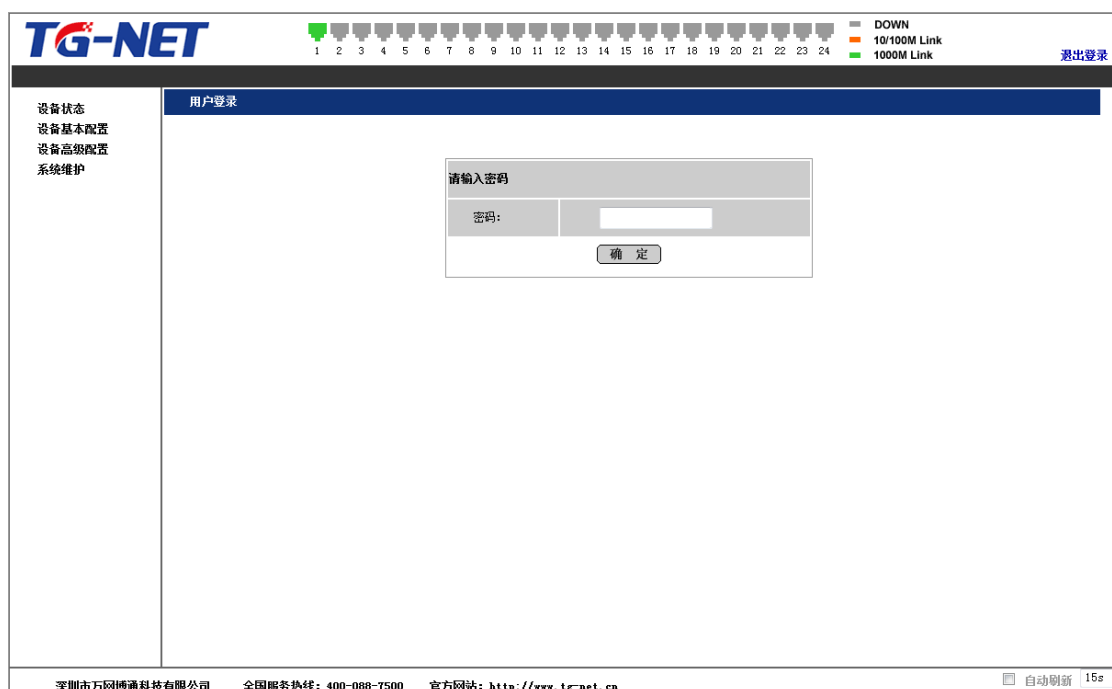


图2. 1. 1交换机登陆页面

上图是交换机登陆页面, 系统缺省的密码是admin(注意大小写), 系统仅允许单一管理员登陆, 当管理员登陆时, 来自其他的登陆请求会被拒绝。当管理员退出登陆后, 来自其他IP的用户可以登陆配置设备。

如果出现管理IP地址冲突, 则表明上次管理时没有正常退出, 设备里仍然保存着上一管理员信息。此时可以选择重新启动设备或者静止等待180s后再登陆。

建议管理员第一次登陆后即修改交换机IP地址和密码, 交换机不要和DHCP服务器或者网关设备分配在同一个网段。



# 第1章 设备状态

## 系统状态

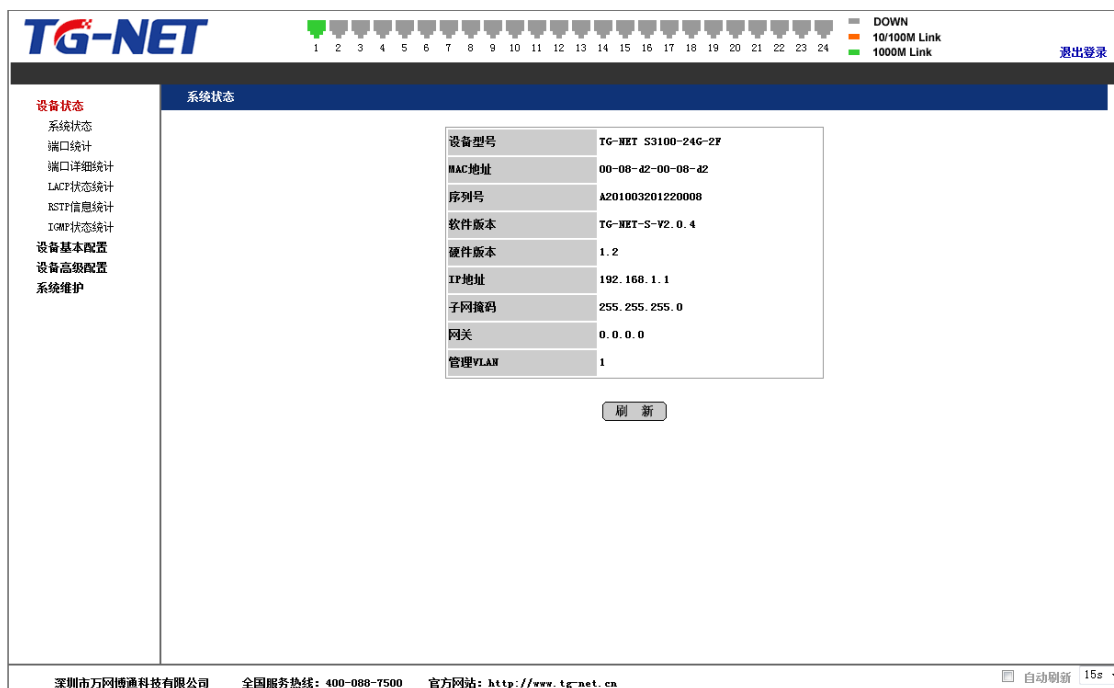


图2.2.1系统状态

在系统状态页面中，可以查询看到本设备的型号、MAC地址、设备序列号、软件版本、硬件版本、IP地址、子网掩码、网关及管理VLAN。

## 端口统计

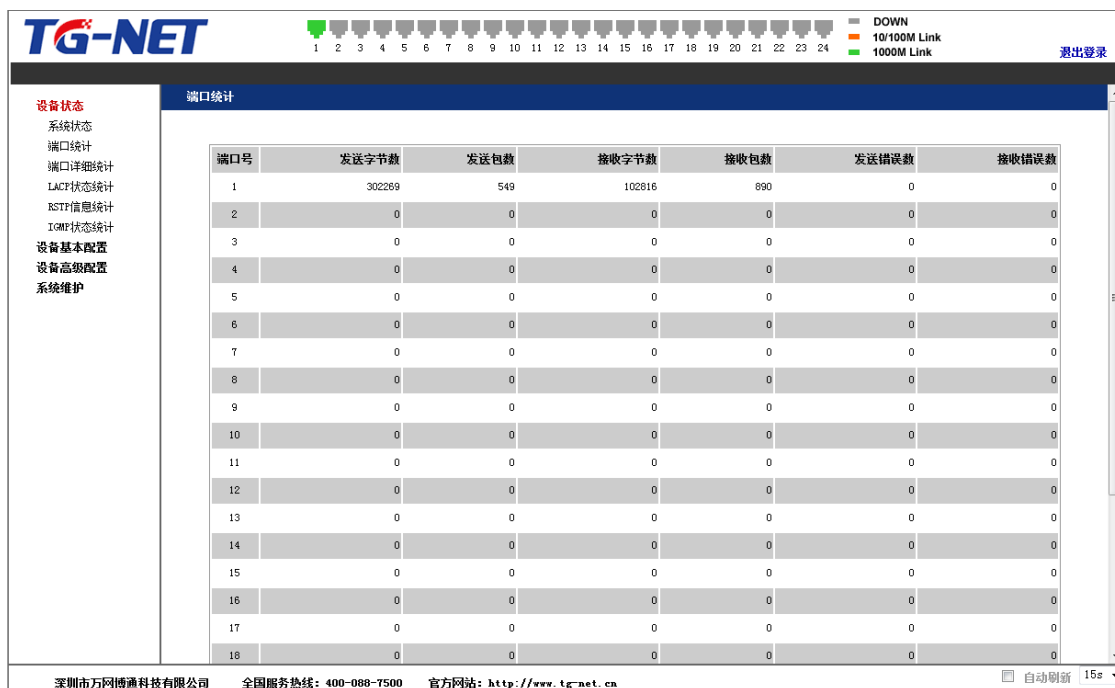


图2.2.2端口统计

端口统计, 在这里可以看到每个端口发送/接收的包数量、字节数, 发送/接收错误报文数。当端口的错误报文数过多则说明该端口的工作状态很差, 需要检查端口所连的网线或者对方网卡是否存在问题。

在该项功能中, 本软件版本不支持数据的实时刷新, 需要人工点击“刷新”按钮来查看新的数据信息。

## 端口详细统计

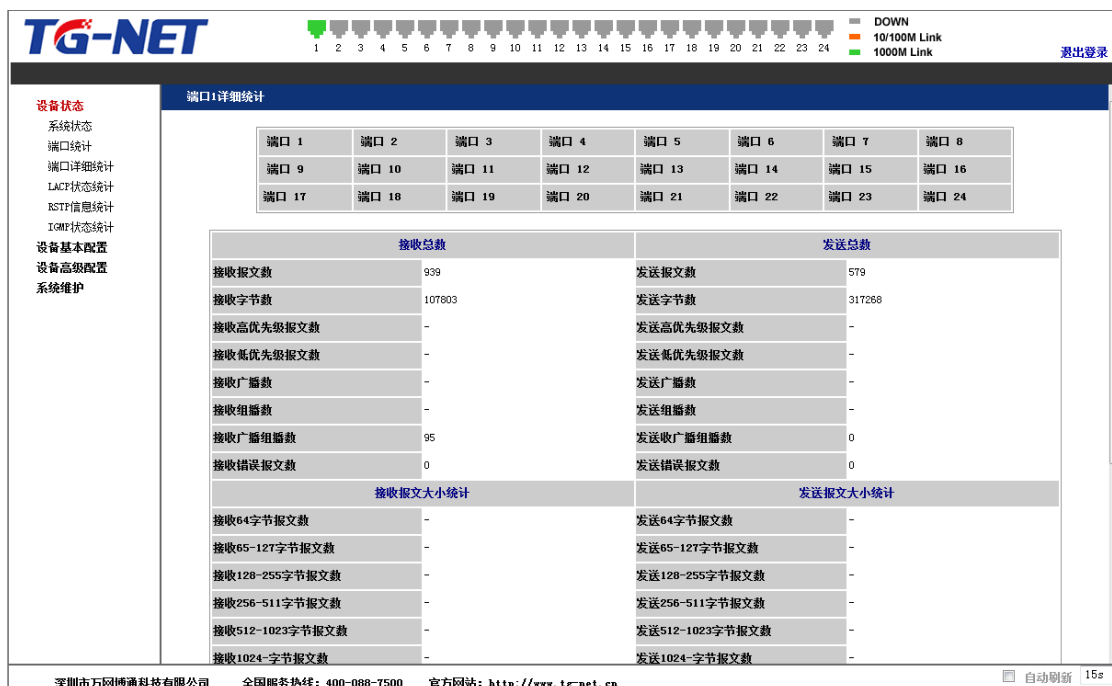


图2. 2. 3端口详细统计

端口详细, 可以查询每个端口的详细工作情况, 包括接收/发送报文数、广播包、错误包等等, 便于网管人员进行网络维护。

## LACP状态统计

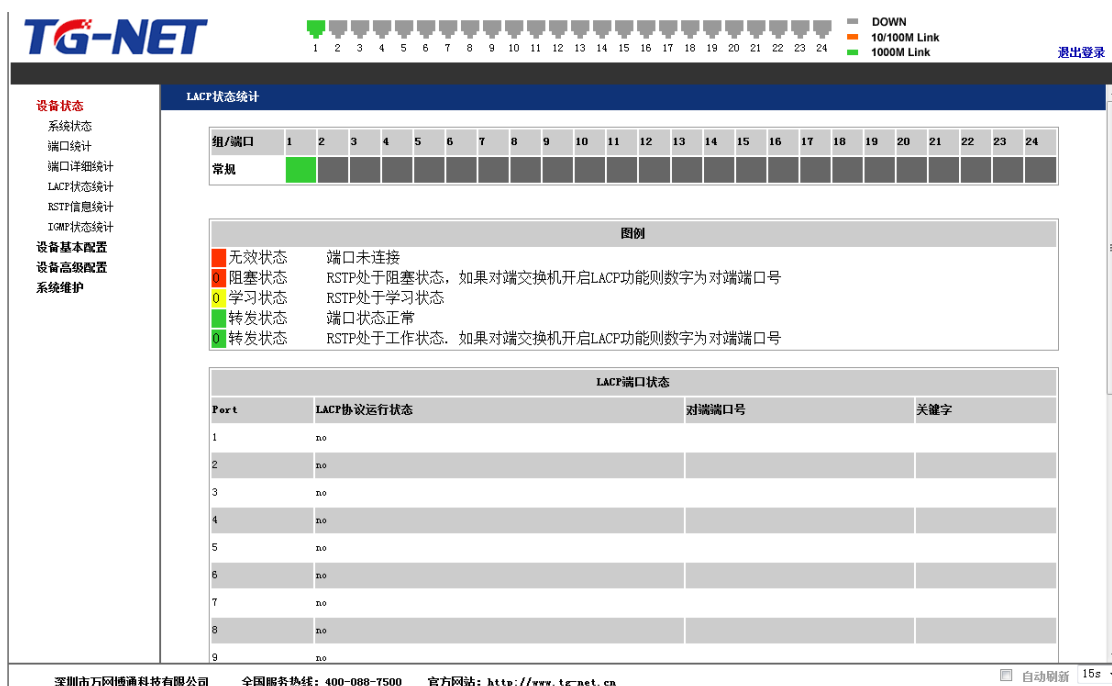


图2. 2. 4 LACP状态统计

通过LACP状态统计, 可以看到端口上LACP协议的运行状态, 端口状态可以通过显见的端口色彩来判断(如上图)。LACP端口状态中显示了LACP协议的详细信息, 包括对方端口号和有效关键字。

## RSTP信息统计

RSTP端口状态						
端口/汇聚组	Vlan Id	路径开销	边缘端口	P2P端口	协议启用	端口状态
端口 1						Non-STP
端口 2						Non-STP
端口 3						Non-STP
端口 4						Non-STP
端口 5						Non-STP
端口 6						Non-STP
端口 7						Non-STP
端口 8						Non-STP
端口 9						Non-STP
端口 10						Non-STP
端口 11						Non-STP
端口 12						Non-STP
端口 13						Non-STP
端口 14						Non-STP
端口 15						Non-STP
端口 16						Non-STP
端口 17						Non-STP
端口 18						Non-STP
端口 19						Non-STP

图2. 2. 5 RSTP信息统计

在概览中可以看到每个VLAN中对应RSTP的网桥ID和该RSTP的一些基本参数。在端口状态中可以看到该端口对应的VLAN、该端口的路径开销、是否为边缘端口、是否是点到点连接(全双工)、当前端口运行的协议(STP/RSTP)。

## IGMP状态统计

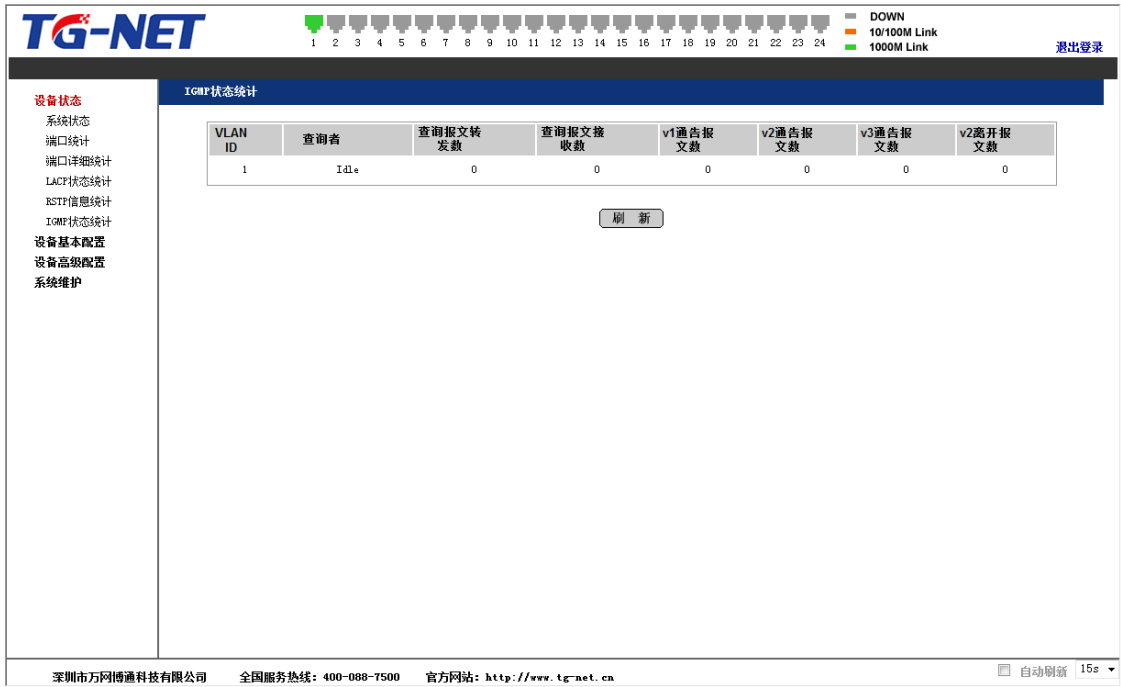


图2.2.6 IGMP状态统计

IGMP状态信息中可以看到当前VLAN对应IGMP状态的报文统计。

## 第2章 设备基本配置

### 系统配置

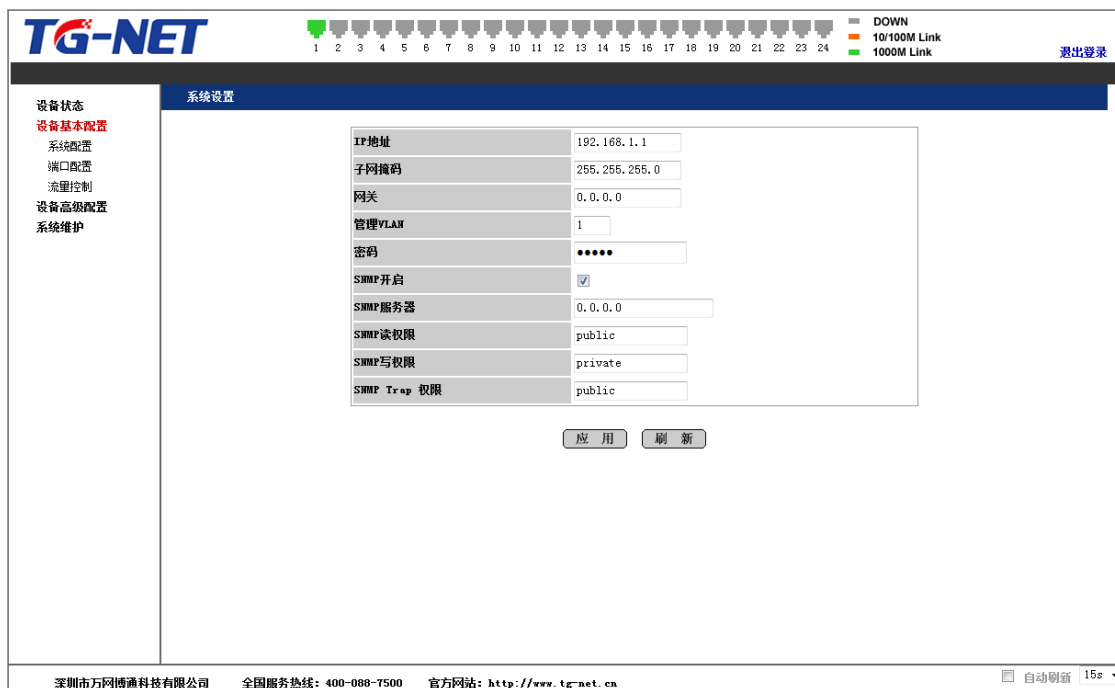


图2.3.1 系统配置

本页面提供了对系统的基本参数的修改, 对于需要修改的参数, 如: IP地址、子网掩码、密码, 修改其值, 然后点击应用即可, 对于不需要修改的值则不要做改变。

注意: 在没有特殊情况要求下, 请不要随意修改交换机子网掩码的值。如修改不当, 会出现无法登陆交换机的情况。

## 端口配置

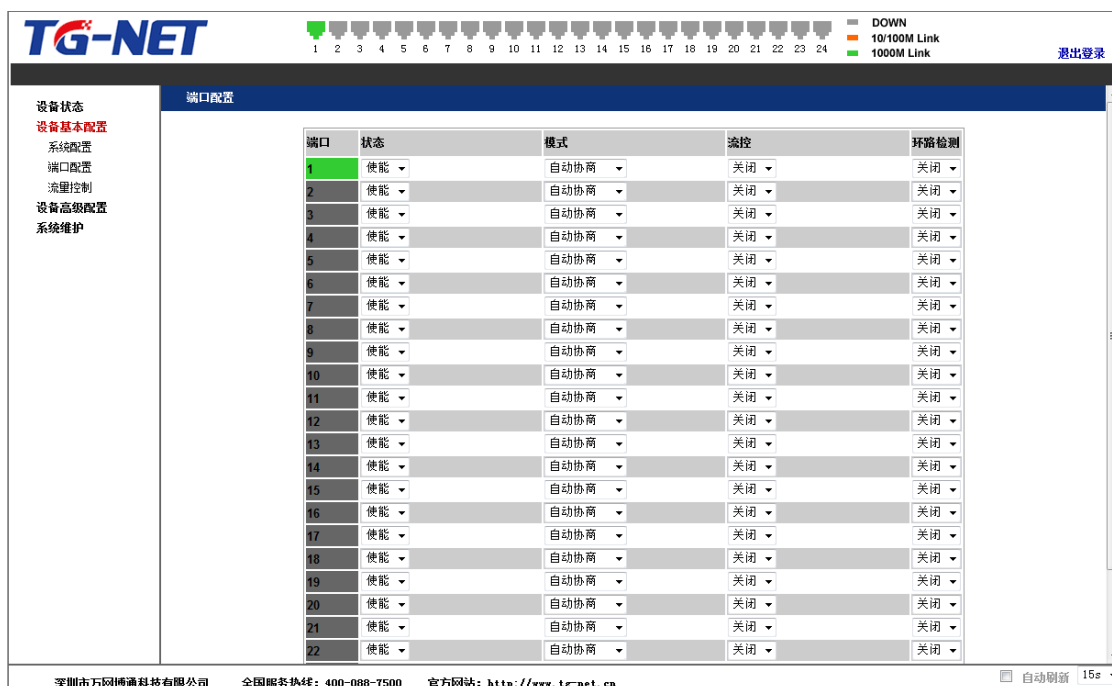


图2.3.2 端口配置

端口状态有2种状态：使能、禁用。端口使能即打开此端口；端口禁用即关闭此端口，默认端口为使能状态。端口模式有6种选择：自动协商、10Harf、10Full、100Harf、100Full、1000Full，可以根据需求在模式下拉列表中指定，缺省状态是自动协商。本系统流控默认为关闭状态，可以根据业务需求打开流控开关。端口环路检测功能默认为关闭状态，当需要用到环路检测功能时，可以选择打开，此时若设备检测到环路，会阻塞一个端口，防止环路出现。（提示：当某一端口被阻塞时，设备面板上Link指示灯依然显示亮，表示物理链路正常；web页面顶端Link指示灯会变暗，表示端口被逻辑阻塞。）

## 流量控制

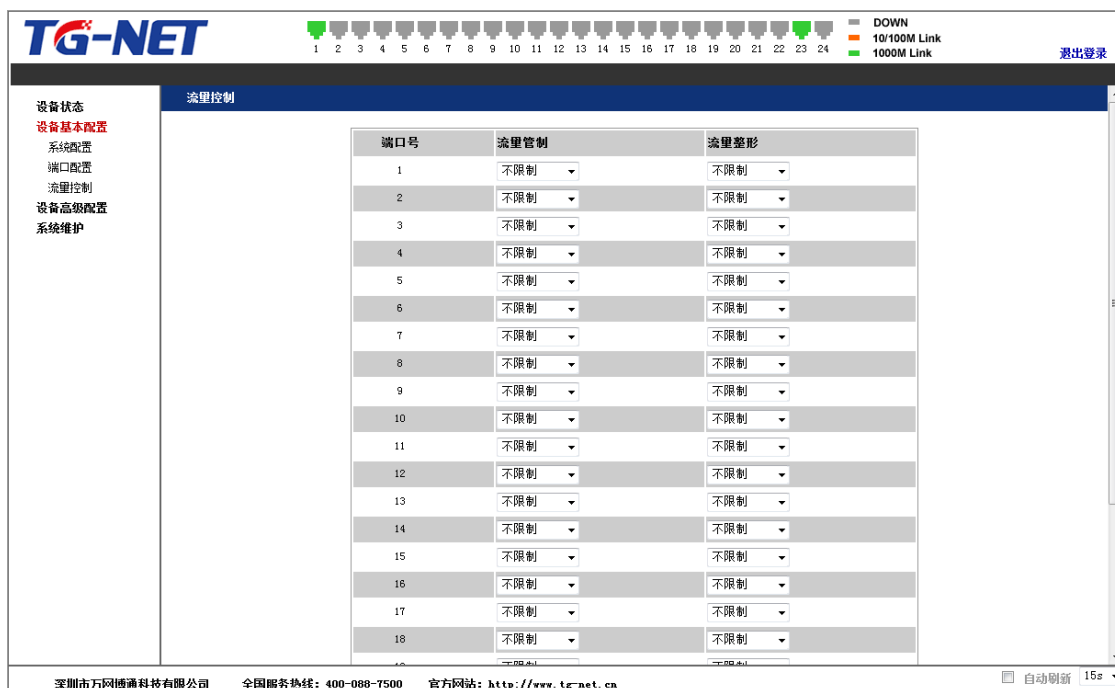


图2.3.3 流量控制

流量管制指的是入口带宽限制，可以控制端口可接收的最大突发流量，超过该限制带宽将触发对端口的流控。流量管制默认为“不限制”，可根据业务需求，设置管制大小：128kbps-

3968kbps之间。流量整形指的是出口带宽限制，可以控制端口可发送的最大突发流量，超过该限制带宽将引起对端口的流控，实现对出口流量的整形。流量整形默认为“不限制”，可根据业务需求，设置整形大小：128kbps-3968kbps之间。



## 第3章 设备高级配置

### IGMP配置

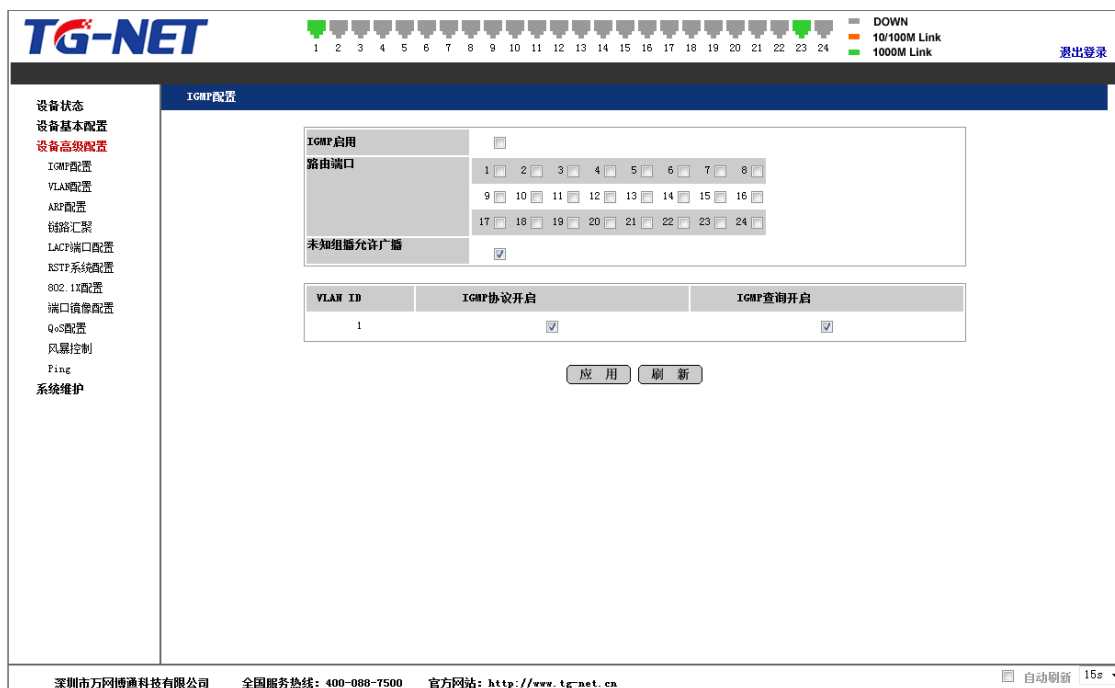


图2. 4. 1 IGMP配置

上图是IGMP组播配置界面，其中配置的路由端口为静态路由端口，不会老化。当没有配置为静态路由端口的端口上收到IGMP查询报文时，交换机认为该端口连接着IGMP路由器（直接或者间接），就将该端口记录为动态路由端口。当交换机接收到IGMP报告报文时，会向路由端口转发。

本设备通过运行IGMP侦听实现对IGMP报文的侦测，并为主机及其对应端口与相应的组播组地址建立映射关系。

IGMP查询功能是IGMP路由器会定时向IP组播成员发送查询报文（特定查询和一般查询），IP组播成员通过发送报告报文来保持组播路由处于有效状态。如果路由器在某段时间出现故障，不能发送查询报文，可以使用此功能配置来使交换机代为发送查询报文，从而使交换机下游的IP组播转发路径不受影响，不被老化，直至不再有IP组播组成员为止。

### VLAN配置

系统提供二种VLAN配置方式：一是快速配置，主要是针对初级用户及简单的VLAN划分需求；二是高级配置，主要是针对高级用户及复杂的VLAN划分需求。

## 快速配置

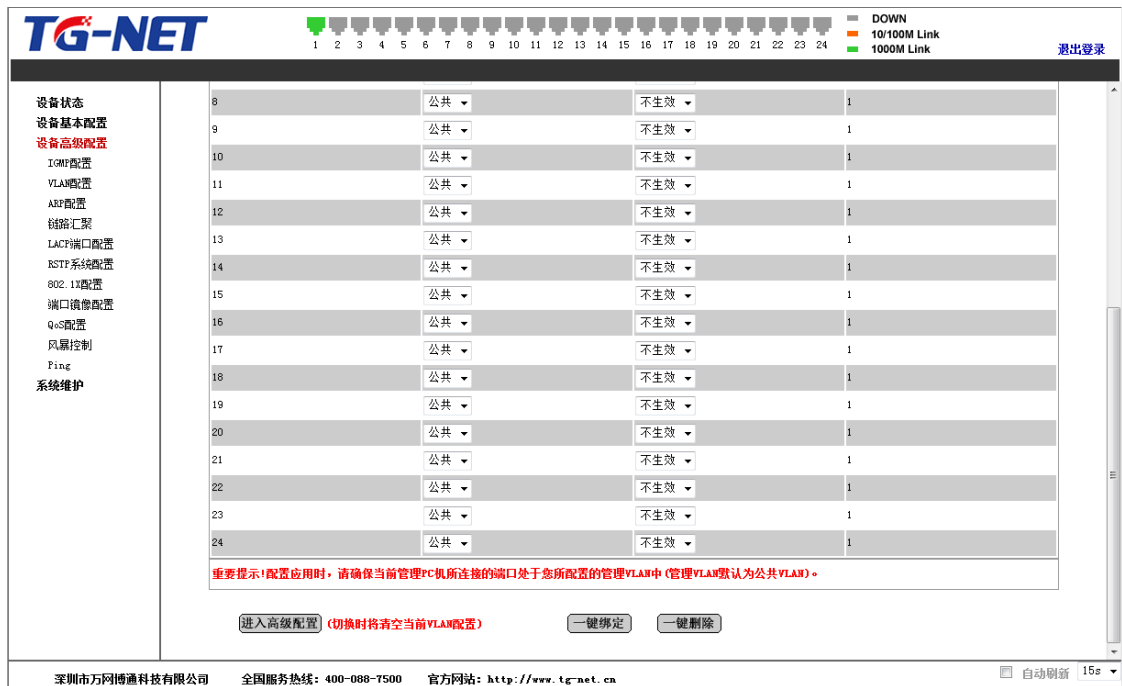


图2. 4. 2 VLAN快速配置

“公共VLAN保护”是一个VLAN的隔离开关，当交换机存在公共端口即公共VLAN的情况下，选中其开关，可以有效地实现公共VLAN的数据隔离，即当公共端口中存在低速率影响源时，其他终端互访速度不受其影响；如果只是正常的使用VLAN，就不需要选中，系统默认为不启用“公共VLAN保护”。启用公共VLAN保护功能需要对设备进行重新启动。点击应用并重启按钮，交换机进入热启动状态，等待1分钟左右后重新登陆交换机，可以发现公共VLAN保护配置已经启动。

VLAN快速配置支持的VLAN ID的范围是[1-24]，最大的VLAN个数为24。页面上依次排列着交换机的24个端口，每个端口对应的VLAN下拉框可选择2-24号VLAN及公共VLAN。您可以根据网络需求，选择端口加入到各个VLAN中，同时配置某个或某几个端口为公共VLAN端口（一般上行端口、服务器端口、路由器端口、打印机端口等），选择好后，点击“一键绑定”按钮后完成配置。此时，不需要另行配置PVID，系统会根据您所选的端口VLAN ID自动配置PVID。正常配置公共VLAN应用时，VLAN标签都默认为“不生效”即可，不需要勾选。**【重要提示：配置应用时，请确保当前管理PC机所连接的端口处于您所配置的管理VLAN中（管理VLAN默认为公共VLAN）】。**

如果需要清除当前配置，可点击“一键删除”按钮。

如果你需要更丰富的VLAN配置功能，可点击“进入高级配置”按钮。进入高级配置页面时，将会清空当前VLAN配置信息。

## 高级配置

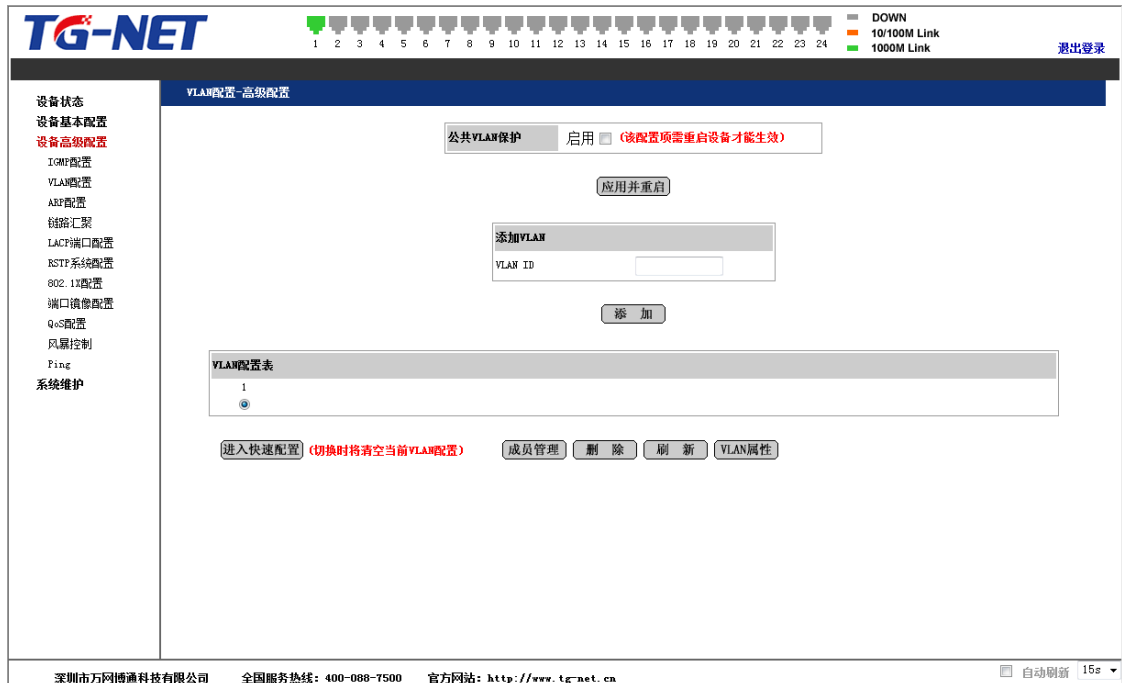


图2. 4. 3 VLAN高级配置

在VLAN高级配置界面中，可以添加、删除VLAN。目前支持的VLAN ID的范围是[1-4094]，最大的VLAN个数为255。

点击“成员管理”按钮，将会进入以下页面中，可以对当前VLAN成员端口进行增减。

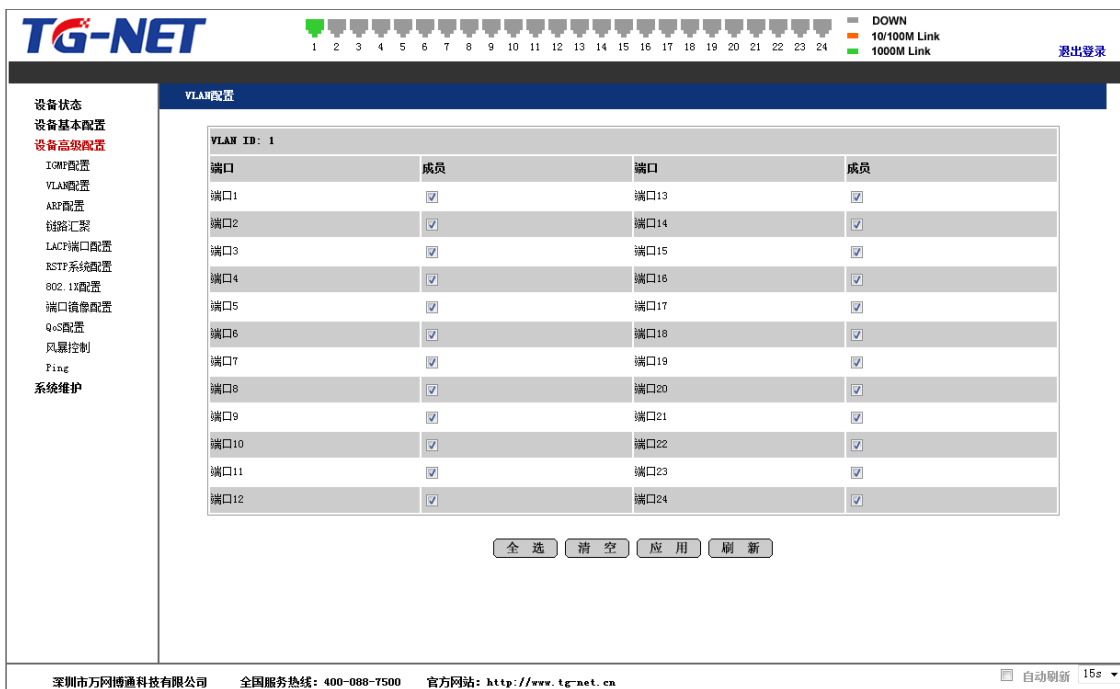


图2. 4. 4 VLAN成员管理

点击VLAN属性按钮，可以对VLAN基本特性进行配置。

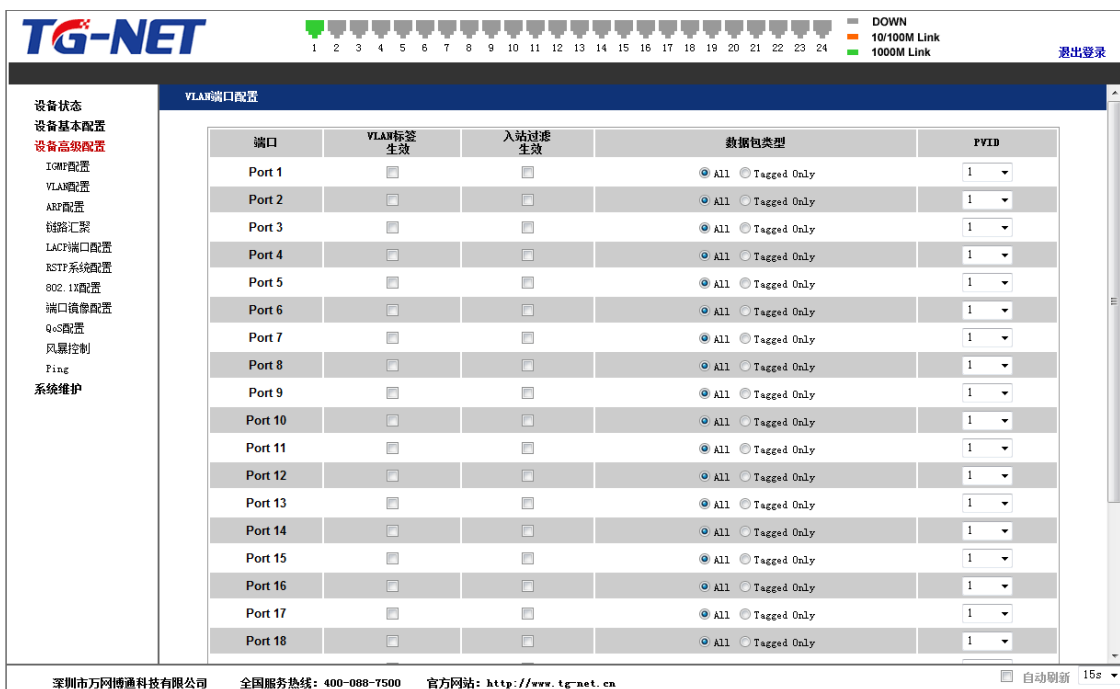


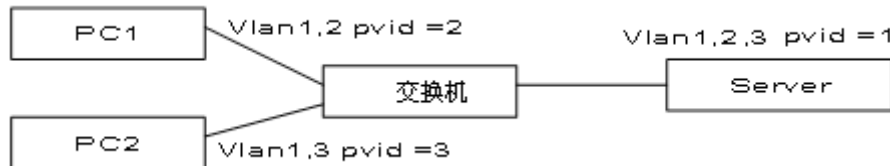
图2. 4. 5 VLAN属性配置

对所配好的VLAN还必须进行VLAN属性配置。“VLAN标签生效”指该端口输出带VLAN标签的报文。“入站过滤生效”指对于非该VLAN的报文，则不学习地址

。“数据包类型”指端口接收的报文是否是带tag帧和不带tag帧都能接收。PVID指的是当前VLAN收到不带VLAN标签的报文的时候，将其发送到哪个VLAN去，当将端口加入某个特定VLAN的时候，需要配置该项目。

### [举例一，公共VLAN模式]

假设有两台PC机(PC1与PC2)，要求两台PC不能互访，但要都能访问服务器，组网如下：



#### 操作步骤：

第一步：启用公共VLAN保护功能，并重启设备后登陆。

第二步：创建VLAN2，在VLAN成员管理中将PC1对应端口（假设为端口1）与Server对应的端口（假设为端口24）加入到VLAN2，并点击“应用”。

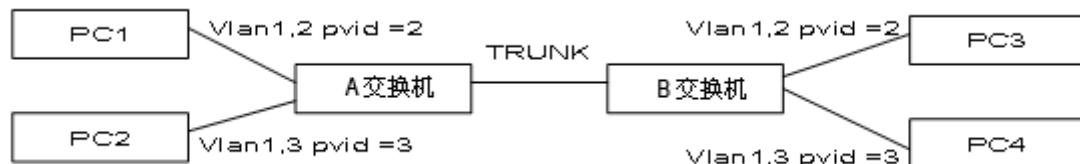
第三步：创建VLAN3，在VLAN成员管理中将PC2对应端口（假设为端口2）与Server对应的端口（假设为端口24）加入到VLAN3，并点击“应用”。

第四步：打开VLAN属性页面，将PC1对应端口（假设为端口1）的PVID选择2，将PC2对应端口（假设为端口2）的PVID选择3，Server对应的端口（假设为端口24）的PVID默认为1即可，其它选项不用设置。

第五步：测试结果为PC1、PC2不能互访（属于不同vlan，被隔离）；PC1、PC2均能访问Server（属于公共vlan端口）。

### [举例二，Tag VLAN模式]

有四台PC机(PC1, PC2, PC3, PC4)，要求PC1与PC3能互访，PC2与PC4能互访，但PC1与PC4不能互访，PC2与PC3不能互访，组网如下：



#### A交换机操作步骤：

第一步：在A交换机上，创建VLAN2，将PC1对应端口（假设为端口1）以及与B交换机相连的端口（假设为端口24）加入VLAN2，并点击“应用”。

第二步:在A交换机上,创建VLAN3,将PC2对应端口(假设为端口2)以及与B交换机相连的端口(假设为端口24)加入VLAN3,并点击“应用”。

第三步:在A交换机上,打开VLAN属性,将端口1的PVID选择2,将端口2的PVID选择3,端口24的PVID默认为1,并同时勾选端口24的“VLAN标签生效”。

#### B交换机操作步骤:

第一步:在B交换机上,创建VLAN2,将PC3对应端口(假设为端口1)以及与A交换机相连的端口(假设为端口24)加入VLAN2,并点击“应用”。

第二步:在B交换机上,创建VLAN3,将PC4对应端口(假设为端口2)以及与A交换机相连的端口(假设为端口24)加入VLAN3,并点击“应用”。

第三步:在B交换机上,打开VLAN属性,将端口1的PVID选择2,将端口2的PVID选择3,端口24的PVID默认为1,并同时勾选端口24的“VLAN标签生效”。

第四步:测试结果为PC1与PC3能互访、PC2与PC4能互访(属于同一VLAN);PC1与PC4不能互访,PC2与PC3不能互访(属于不同VLAN,被隔离)。

如果您想进行简易的VLAN配置功能,可点击进入“快速配置”按钮,进入快速配置页面时,此时将会清空当前VLAN配置信息。

## ARP配置

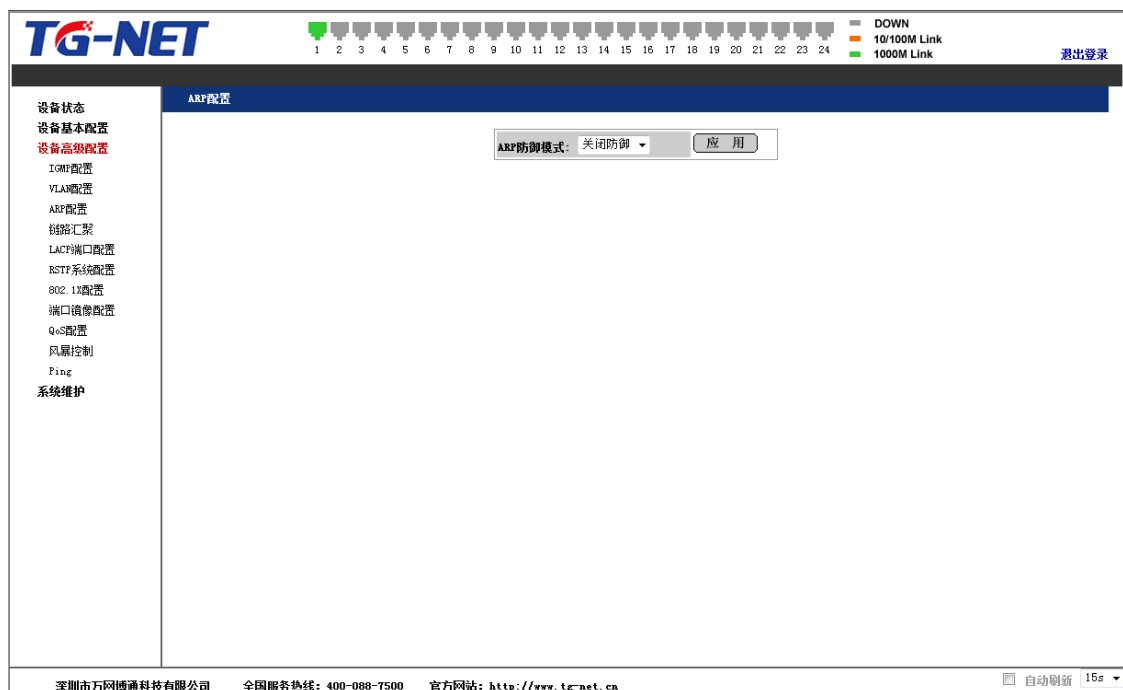


图2.4.6 ARP配置

ARP功能默认是处于“关闭防御”状态，根据业务需求，可选择ARP防御模式为“静态绑定”，点击应用生效，进入下图：

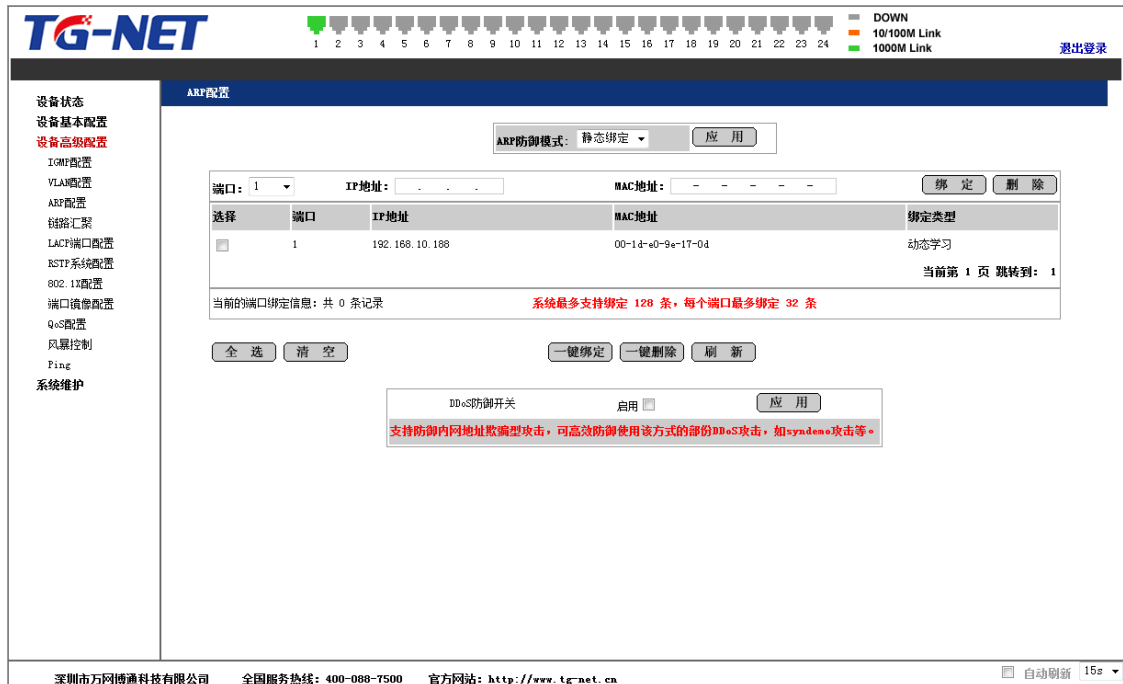


图2.4.7 ARP静态绑定

第一栏为手动添加需要绑定的端口与IP、MAC地址，点击绑定生效，或者输入需要删除的端口与IP、MAC地址，点击删除生效。

中间带有复选框的这一栏会显示当前交换机各个端口所学习到的IP与MAC信息，可以单选、复选或者全选进行一键绑定或一键删除。系统最大绑定条目数为128条，每个端口最大绑定数为32条。

当选择某端口进行静态绑定，对于该端口接收到的ARP报文，仅允许与静态ARP绑定相匹配的才能够通过。对于该端口下的其它IP与MAC信息，只能动态学习，但不允许通过。如果需要该端口下的其它ARP信息通过，必须把该端口对应的其它IP与MAC信息进行静态绑定。

本系统ARP功能还支持防御内网地址欺骗型攻击，可高效防御使用该方式的部份DDoS攻击，如syndemo攻击等。勾选“启用”框，点击“应用”按钮即生效。该功能仅对上述进行过静态绑定的端口及IP生效。注意！该功能生效后，静态绑定过的端口将不再学习其它的ARP信息，如果该端口下需要增加绑定信息，需先解除该端口对应的所有静态绑定或者取消DDoS防御功能，然后重新把端口下所有的ARP信息进行静态绑定后开启DDoS防御功能即可。

## 链路汇聚

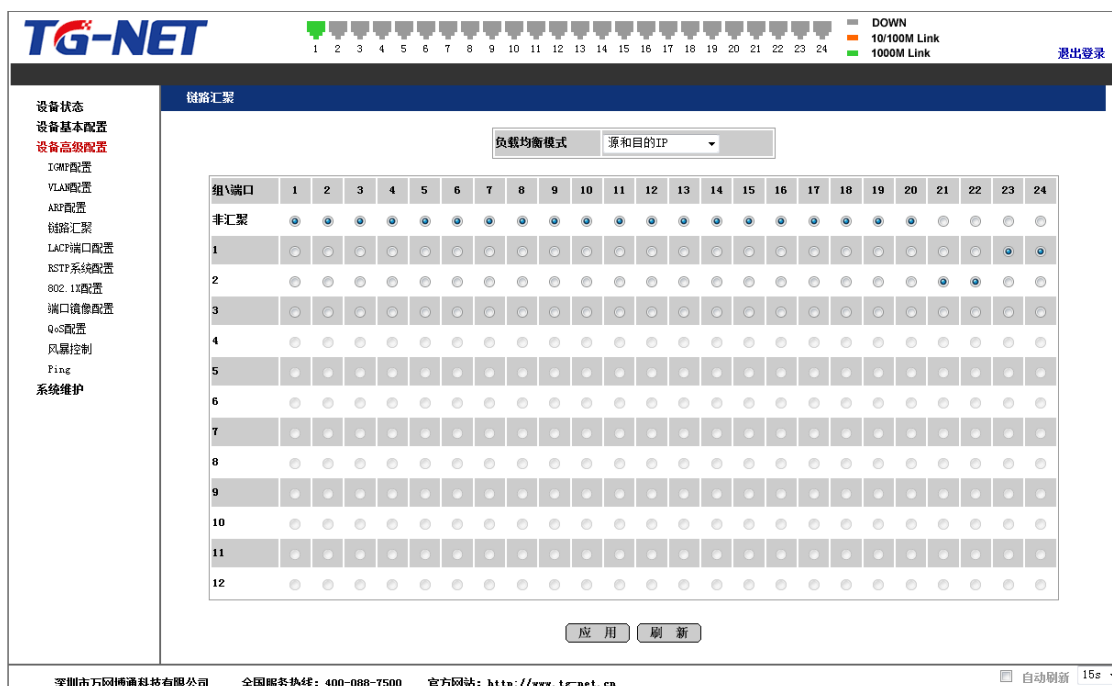


图2.4.8 链路汇聚

链路汇聚的负载均衡模式支持：“源MAC地址”模式，表示基于报文的源MAC地址进行负载均衡计算；“目的MAC地址”模式，表示基于报文的源MAC地址进行负载均衡计算；“源和目的MAC地址”模式，表示将报文的源MAC地址和目的MAC地址进行异或之后再行负载均衡计算；“源和目的IP”模式，表示将报文的源IP地址和目的IP地址进行异或之后再行负载均衡计算；“MAC和IP混杂模式”，表示将报文的MAC地址和IP地址信息综合进行异或之后再行负载均衡计算。均衡算法的指定是全局性的，系统默认为“源和目的IP”模式，如果没有特殊需要，则不须改动。

在链路汇聚页面，会直接列出12组聚合组，当没有汇聚组时，汇聚组1是可配置状态，当汇聚组1配置完成后，汇聚组2会自动打开给用户配置。交换机支持最大的聚合组数为12组，每个聚合组最大支持12个端口。

当配置的端口数大于12时，提交后会提示错误代码为44。如下图：



图2.4.9 链路汇聚错误提示



## LACP端口配置

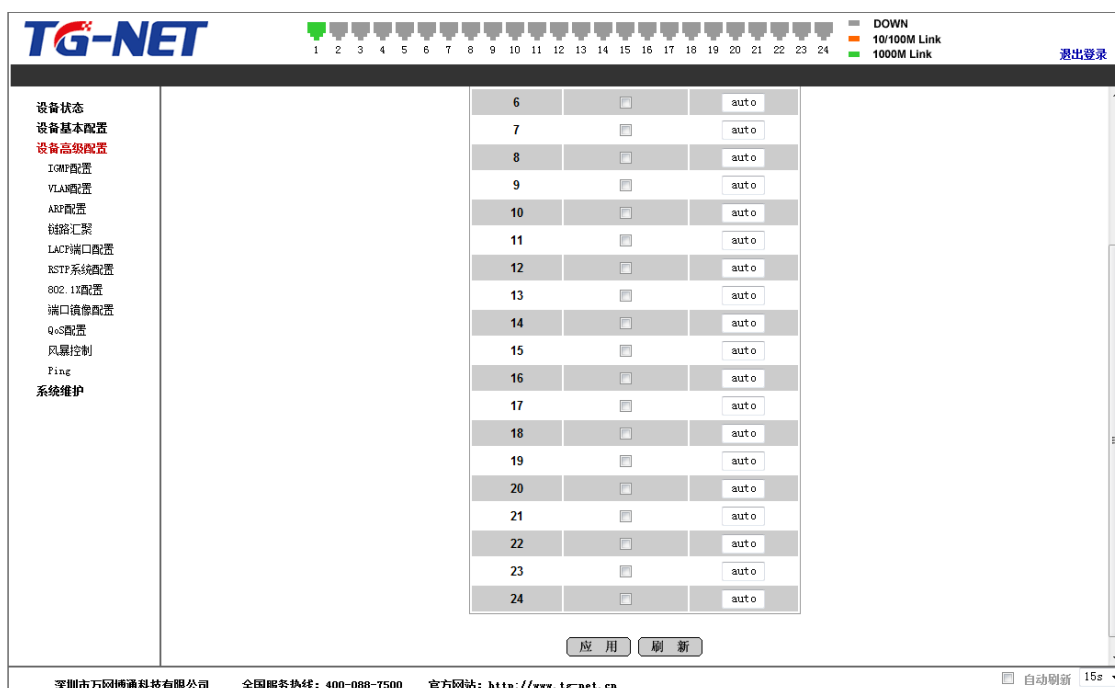


图2.4.10 LACP端口配置

端口开启LACP协议以后，汇聚的双方设备通过协议交互汇聚信息，根据双方的参数和状态，自动将匹配的链路汇聚在一起收发数据。汇聚形成后，交换设备维护汇聚链路状态，当双方配置变化时，自动调整或解散汇聚链路。

LACP协议的配置参数包括协议开关状态和协商关键字(KEY)。只有开启LACP协议的端口才会进行LACP协商，从而有可能形成汇聚链路。协商关键字是协商的基础，具有相同关键字的端口才能协商组成一个汇聚链路。

如果某些端口已经进行了静态的端口汇聚，在这里该端口的LACP和KEY值均处于无效配置状态。反之，如果某些端口进行了LACP汇聚，则在静态链路汇聚功能中，这些端口均处于无效配置状态。

本产品的动态汇聚建议使用在与服务器连接的网络环境中，前提需要服务器能够支持双网卡的汇聚功能。

## RSTP系统配置



图2.4.11 RSTP系统配置

上图是快速生成树RSTP配置页面。边缘端口是当交换机连接电脑或者没有生成树功能的网络设备时使用。此时端口直接进入转发状态，不会参与RSTP逻辑拓扑计算。

版本兼容性选项在默认情况下，配置为Normal，在此版本下，交换机可以识别STP格式的BPDU，也可以识别RSTP格式的BPDU，并进而自动确定是发送RSTP格式还是STP格式BPDU；当交换机连接的设备中既有运行STP的交换机也有运行RSTP的交换机时，交换机端口发送的BPDU报文格式可能在RSTP和STP之间频繁切换，不利于网络稳定运行。此时可以强制设置以compatible兼容版本运行，在此版本下，交换机只接收和发送STP格式的BPDU，从而和STP保持兼容。

注：在实际应用中，多个VLAN用一棵生成树实际上没有必要，因为vlan间根本就无法通讯，所以在启用RSTP时应该将交换机设置成一个vlan。此种协议是改进的RSTP协议，但不是MSTP协议。

## 802.1X配置



图2.4.11 802.1X配置

交换机支持基于端口的802.1x认证。在这里可以配置802.1x服务器IP、端口号、密钥等。并且可以对每个端口的认证状态进行修改与配置，也可以根据需要对端口进行“重新认证”、“强制初始化”、“统计查询”。

## 端口镜像配置

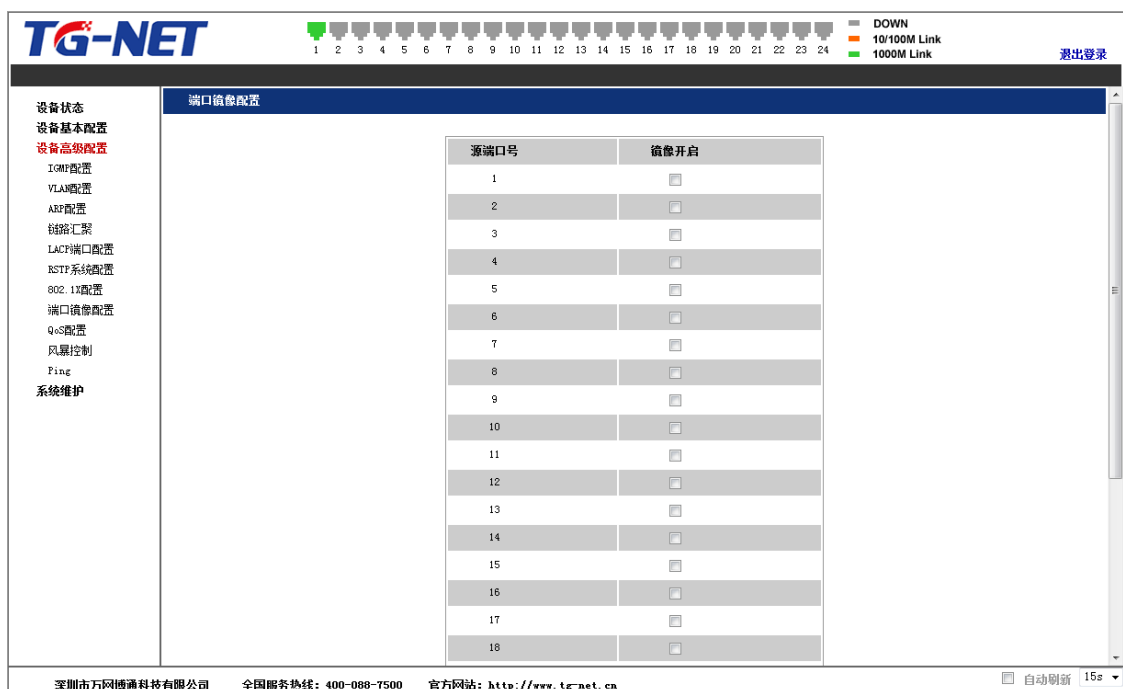


图2. 4. 12 端口镜像配置

端口镜像功能, 将某些端口的业务或者控制报文流量完整地映射到指定的端口, 该指定的端口为“镜像端口”, 被映射的端口为“镜像源端口”。在镜像端口连接网络分析仪器, 可以清楚的分析镜像源端口的报文而不破坏镜像源端口的正常业务, 端口镜像是一种方便的在线监控功能。系统的所有端口都可以配置为镜像源端口, 但镜像端口只能配置一个。当某个端口被配置镜像端口时, 其相应的端口则不能配置为源端口。源端口指的是被镜像端口, 可以配置多个, 镜像到的目的端口只能配置一个。

## QoS配置

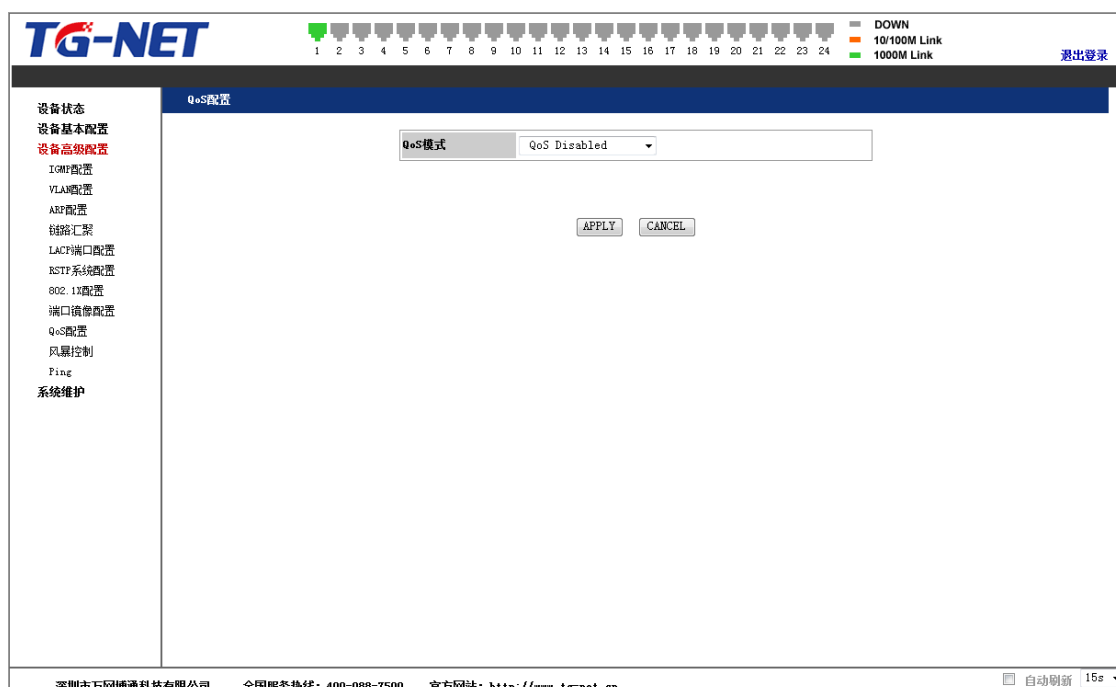


图2. 4. 12 QoS配置

QoS模式默认为关闭状态, 下拉框中可选择为802.1p模式和DSCP模式。



图2. 4. 13 QoS 802.1p配置页面

在QoS

802.1p优先级配置中, 用户可配置优先级调度算法或者自定义8个802.1p值在设备中被对应的服务级别, 高优先级别的报文会被设备优先处理, 特别是在某些需要持续连接的场合如VOIP。



图2. 4. 14 QoS DSCP配置页面

在QoS

DSCP优先级配置中, 用户可根据报文自带的DSCP值, 来控制其转发的优先级。DSCP字段的取值范围是0-63。

## 风暴控制

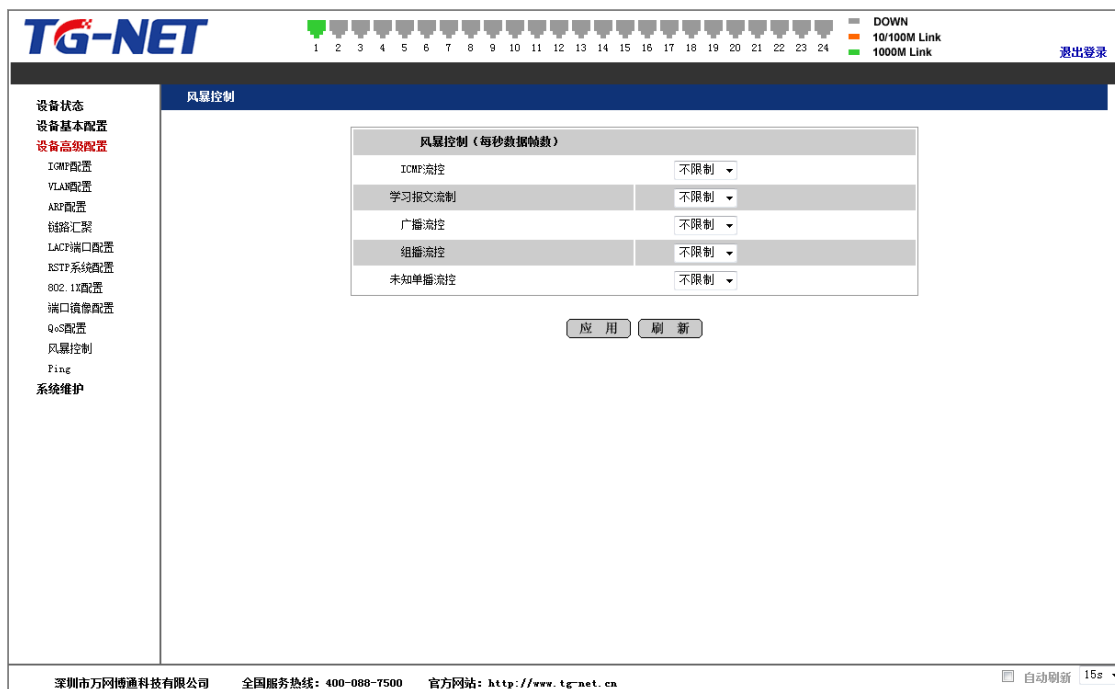


图2.4.15 风暴控制

设备支持多种风暴控制模式, 如ICMP流控、上传CPU的报文速率的流控、广播流控、组播流控和未知单播流控, 未知单播流控指的是目的地址查找失败的报文, 设备会将这样的报文广播到所有的端口, 如果这样的报文过多则会对网络造成冲击。

# PING

The screenshot shows the TG-NET web management interface. At the top, there is a status bar with 24 port indicators (1-24) and a legend for link status: DOWN (grey), 10/100M Link (orange), and 1000M Link (green). A '退出登录' (Logout) link is visible in the top right. The left sidebar contains a navigation menu with categories like '设备状态', '设备基本配置', '设备高级配置', 'IGMP配置', 'VLAN配置', 'ARP配置', '链路汇聚', 'LACP端口配置', 'RSTP系统配置', '802.1X配置', '端口镜像配置', 'QoS配置', '风扇控制', 'Ping', and '系统维护'. The main content area is titled 'Ping参数' (Ping Parameters) and includes a form for configuration: '目标IP地址' (Target IP Address) with an input field, '次数' (Count) with a dropdown set to '1', and '超时时间(秒)' (Timeout (s)) with a dropdown set to '1'. Below the form is an '应用' (Apply) button. The 'Ping结果显示' (Ping Results Display) section shows a table with the following data:

Ping结果显示	
目标IP地址	192.168.1.188
状态	Test complete
接受应答数	5
请求超时	0
平均应答时间(毫秒)	11

Below the results table is a '刷新' (Refresh) button. At the bottom of the page, there is a footer with the company name '深圳市万网博通科技有限公司', a national service hotline '400-088-7500', the official website 'http://www.tg-net.cn', and an '自动刷新 15s' (Auto Refresh 15s) option.

图2.4.15 PING测试

Ping功能是用来测试网络上某个具体的Client是否可以到达，功能与windows命令行下的ping命令相同，注意，被PING的PC机IP必须与交换机的IP在相同网段。

。

## 第4章 系统维护

### 软件升级



图2.5.1 软件升级

软件升级用于升级交换机版本，界面会显示当前系统的软件版本号，可与需要升级的版本号进行比对。公司网站(<http://www.tg-net.cn>)提供交换机的升级文件，用户可从网站下载升级文件进行升级交换机版本。



## 配置管理

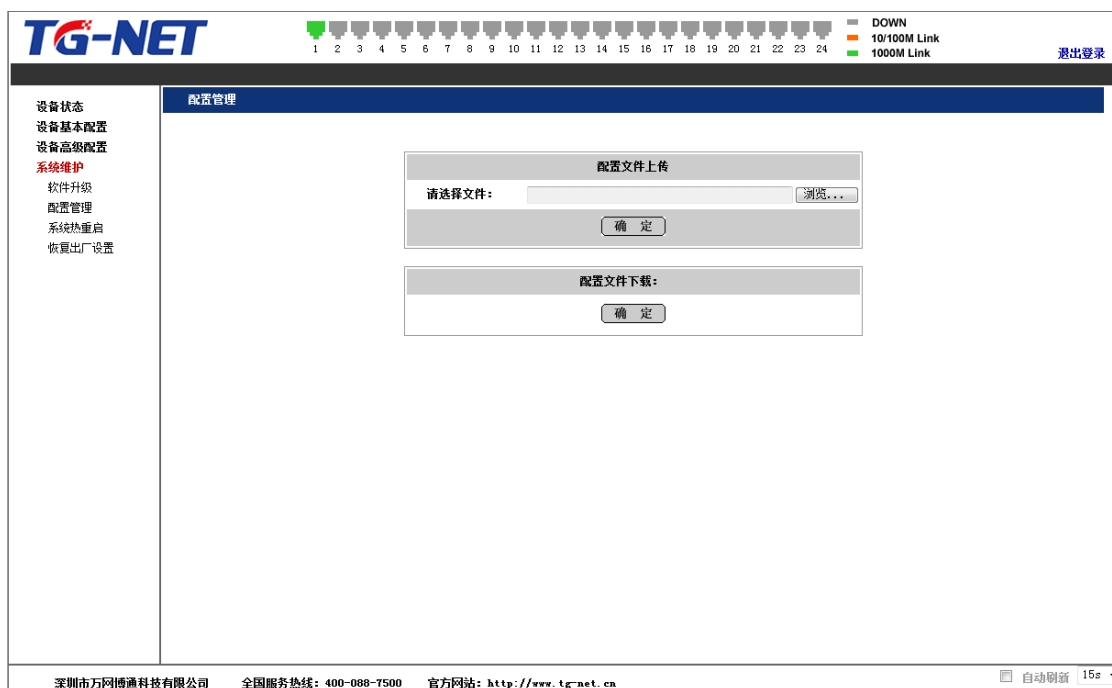


图2.5.2 配置管理

配置管理可以上传/下载系统配置文件，通过这个页面来备份和恢复系统的配置。（注意：通过“配置文件下载”导出的配置文件不包括IP地址信息；通过“配置文件上传”导入的配置文件不会覆盖当前的IP地址信息）

## 系统热重启

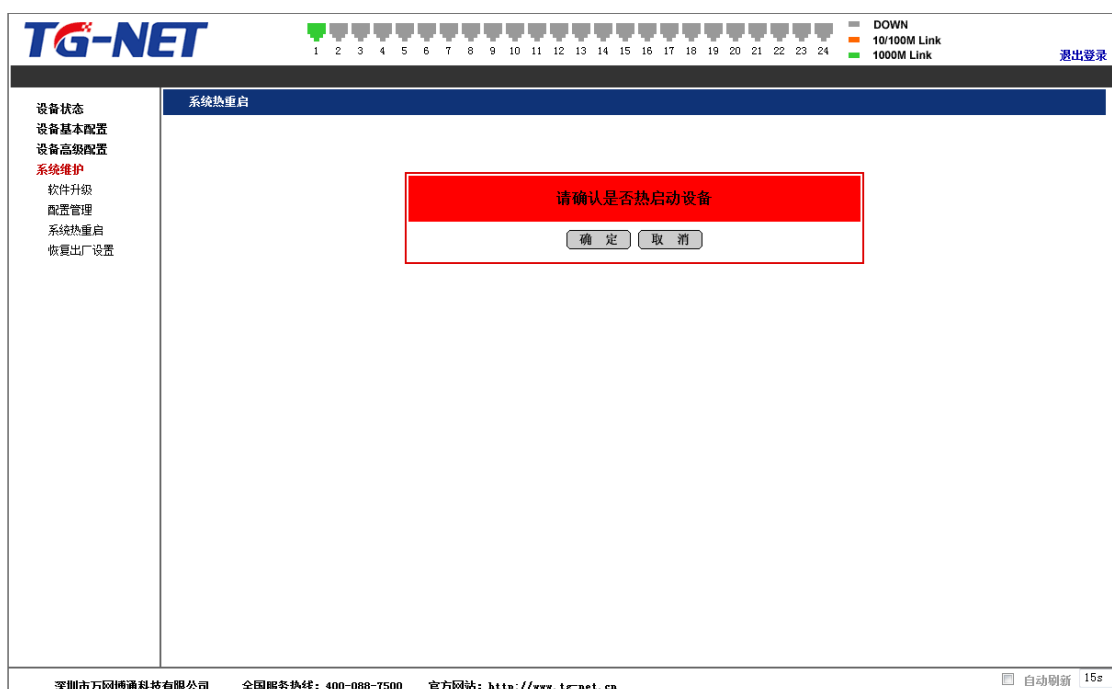


图2.5.3 系统热启动

当修改系统MAC地址等需要重启的设置后，建议重新启动设备来使设置生效。

。

## 恢复出厂设置

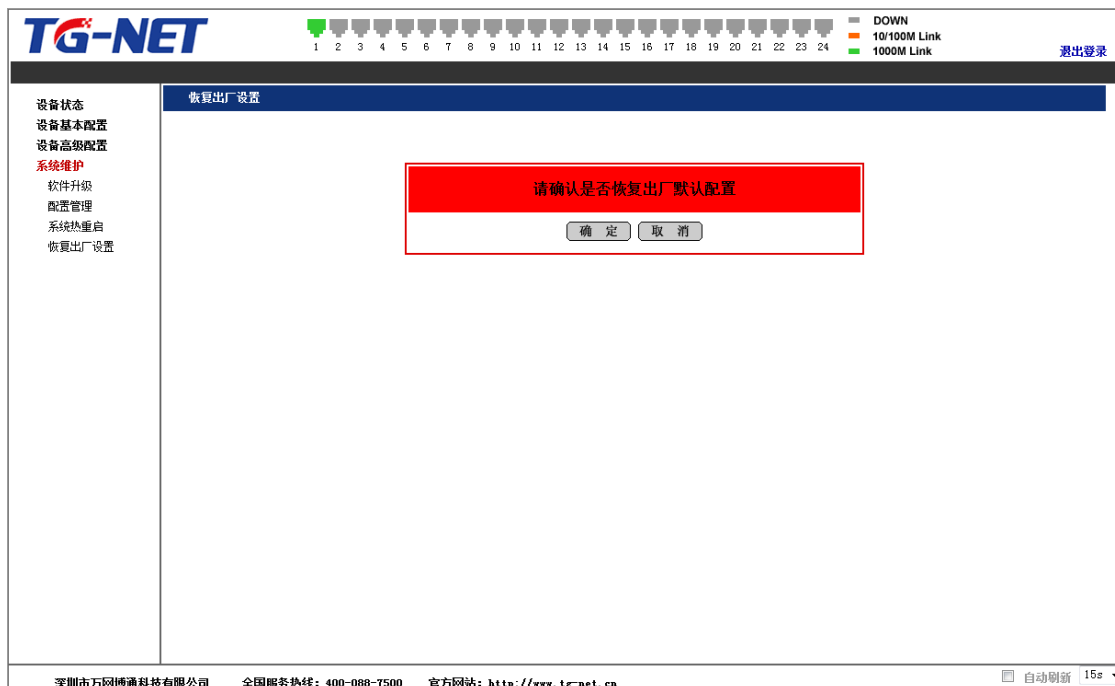


图2.5.4 恢复出厂设置

可以将系统恢复到出厂设置，包括各项配置以及IP地址和管理员密码均会回到初始化设置。

如果忘记设备IP地址或密码而登陆不了WEB管理页面，可以选择通过CLI命令(需支持该功能设备才能使用)来恢复出厂设置，或者通过端口短接来硬恢复。下面就详细介绍如何通过端口短接来恢复出厂设置。

**第一步:**找一根网线，将交换机的9号端口跟16号端口连接起来。

**第二步:**断开电源，等待十秒钟后重新插上电源启动设备。

**第三步:**设备启动后，9号端口跟16号端口会闪烁，大约闪烁几秒钟后，系统会重启。在系统灯常亮或者端口指示灯依次全部亮起的时候，将9号端口跟16号端口断开，此时设备恢复到出厂配置，可以依照第1章系统登陆介绍登陆交换机并进行管理。

## CLI配置指导

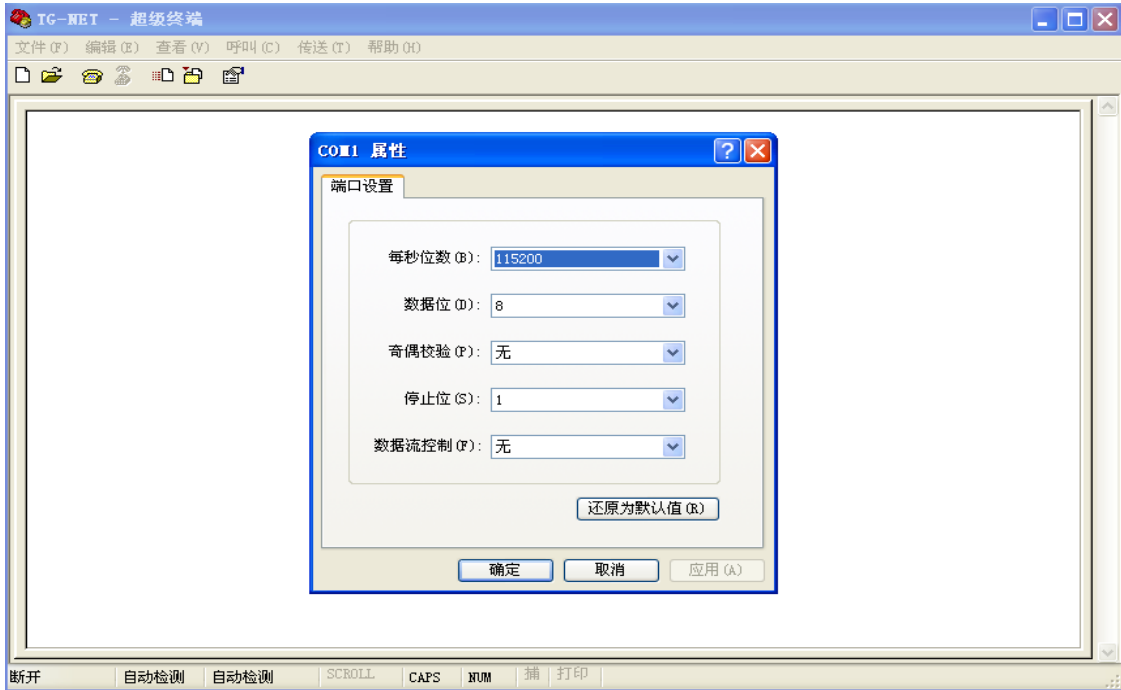


图3.0.1 超级终端配置参数界面

设备通过CONSOLE口进行管理时，相关参数配置如上图所示，“COM1”根据所连接PC上端口号来设定）然后点击上图中的确认后进入到下面的操作界面：

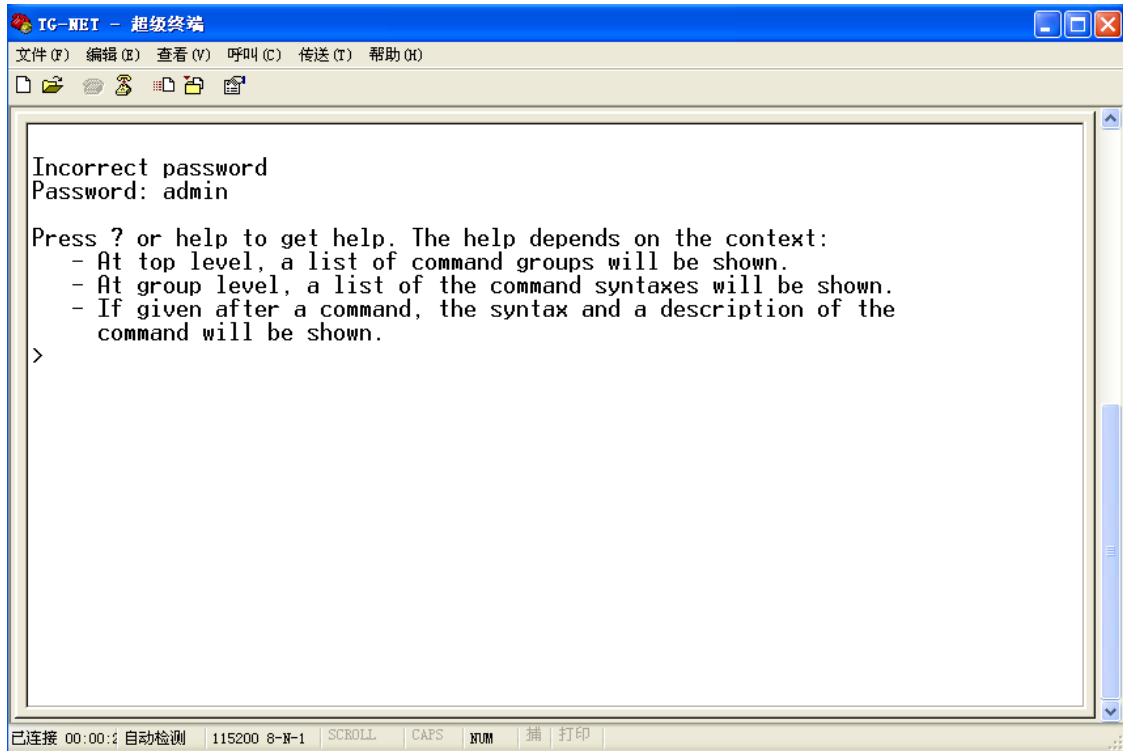


图3.1.1 登陆界面

如上图:CONSOLE登陆后,

- 默认密码为:admin
- 帮助命令:“?”
- 主要命令模式有:
  - System -系统配置
  - Console - Console参数配置
  - Port - 端口配置
  - MAC - MAC配置
  - VLAN - VLAN 配置
  - ARP - ARP配置
  - Aggr -端口聚合配置
  - LACP - LACP配置
  - RSTP - 快速生成树配置
  
  - User Group -用户组配置
  - QoS - QoS配置
  - Mirror -端口镜像配置
  - IP - IP地址配置

Dot1x - Dot1x配置  
IGMP - IGMP配置  
Debug -调试命令, 在本手册中不进行说明

通过输入上述命令字符串, 即可以进入对应的命令配置模式, 如上图  
输入“system”后, 将可以对system模式下的命令进行配置, 此时, 如您需要  
进入到另外一种配置模式, 您必须先退出当前模式。

- 退出到上一级配置模式:“/”

## 第5章 系统配置

通过输入“system”命令, 您将可以进入system配置模式, 如下图:

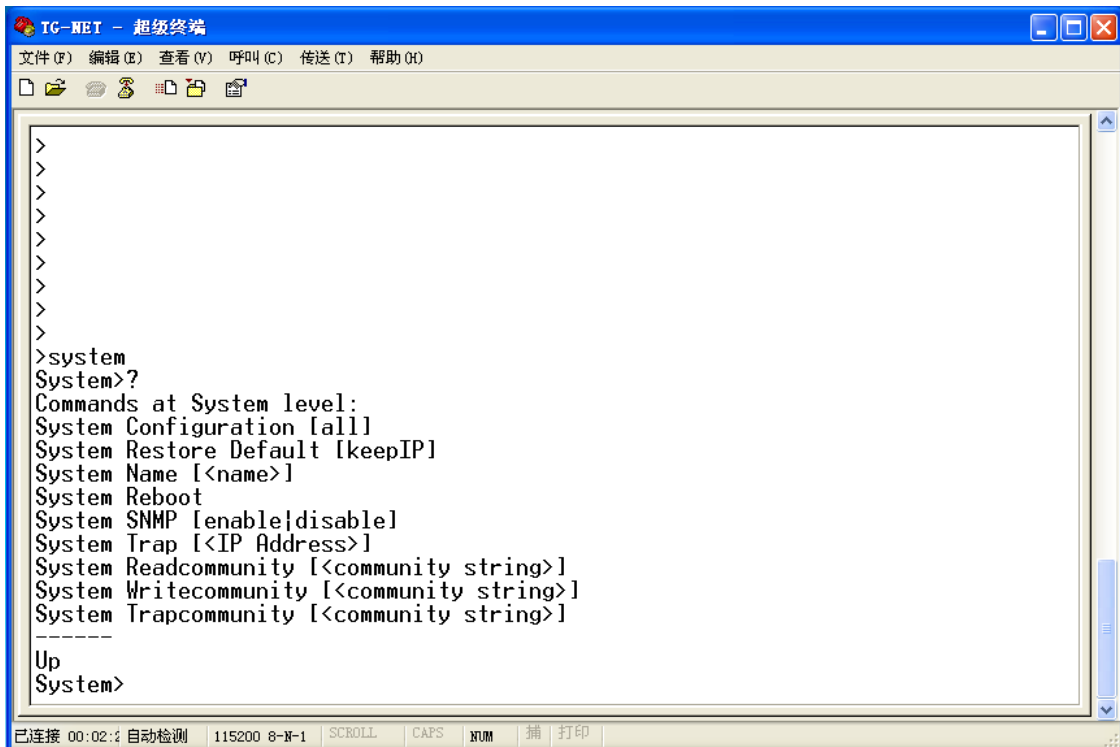


图3.1.3 System 配置界面

其中：

#### 1. 系统配置查询

命令: configuration [all]

[all] — 可选参数, 输入该参数可查看整个系统的配置信息

描述: 查看system全局配置信息;

#### 2. 恢复缺省配置

命令: restore default [keepIP]

[keepIP] — 可选参数, 输入该参数即不对系统IP地址进行复位

描述: 恢复系统缺省配置;

#### 3. 系统重命名

命令: Name [<name>]

<name> — 系统名字

描述: 对系统进行命名;

#### 4. 系统热重启

命令: Reboot

描述:对系统进行热重启;

#### 5. SNMP开关

命令:SNMP [enable|disable]

enable — 启动snmp功能

disable — 关闭snmp功能

描述:开关snmp功能, 默认关闭;

#### 6. SNMP agent地址

命令:Trap [<IP Address>]

<ip Address> — SNMP Agent的IP地址

描述:配置snmp trap报文默认发往的IP地址;

#### 7. SNMP读权限密码

命令:Readcommunity [<community string>]

<community string> — 读权限密码

描述:配置snmp读权限密码;

#### 8. SNMP写权限密码

命令:Writecommunity [<community string>]

<community string> — 写权限密码

描述:配置snmp写权限密码;

#### 9. SNMP trap密码

命令:Trapcommunity [<community string>]

<community string> — trap密码

描述:配置snmp trap密码

## 第6章 Console参数配置

通过输入“console”命令, 您将可以进入console配置模式, 如下图:





## 第7章 端口配置

通过输入“port”命令，您将可以进入端口配置模式，如下图：

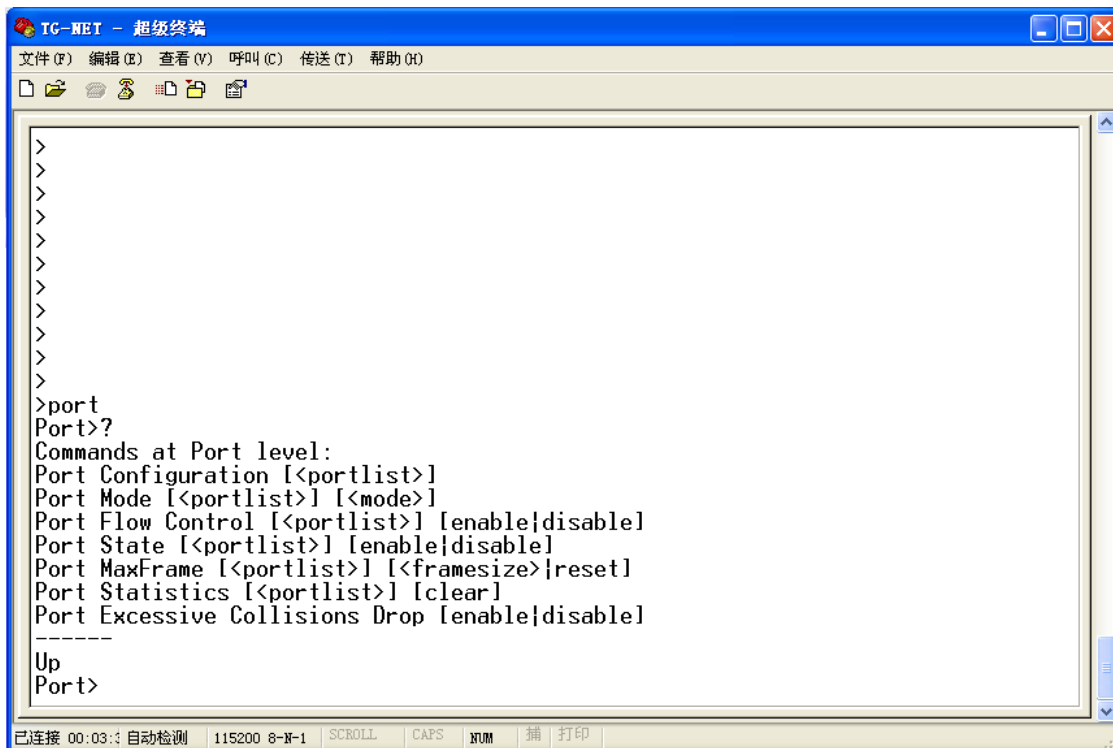


图3.1.3 端口配置

其中：

### 1. 端口配置查询

命令：Configuration [<portlist>]

<portlist> — 端口号列表，如：1,2,4-5，可选

描述：查询端口配置信息；

### 2. 端口工作模式

命令：Mode [<portlist>] [<mode>]

<portlist> — 端口号列表，如：1,2,4-5，可选

<mode> — 端口工作模式，其中对应参数如下：

auto — 自动协商

10hdx — 10M半双工

10fdx — 10M全双工

100hdx — 100M半双工

100fdx — 100M全双工

## 1000fdx – 1G全双工

描述:静态配置端口的工作模式,默认为自动协商;

### 3. 端口流控开关

命令:Flow Control [<portlist>] [enable|disable]

<portlist> – 端口号列表,如:1,2,4-5,可选

[enable|disable] – enable表示打开,disable表示关闭

描述:配置端口是否支持pause流控功能,默认不支持

### 4. 端口使能开关

命令:State [<portlist>] [enable|disable]

<portlist> – 端口号列表,如:1,2,4-5,可选

[enable|disable] – enable表示打开,disable表示关闭

描述:配置端口转发功能是否启动,默认端口都处于工作模式;

### 5. 端口传输最大单元

命令:MaxFrame [<portlist>] [<framesize>|reset]

<portlist> – 端口号列表,如:1,2,4-5,可选

<framesize> – 传输的最大帧大小,范围为1518– 9600;

reset – 恢复成默认值为1518;

描述:配置端口最大的传输单元,默认为1518;

### 6. 端口统计查询

命令:Statistics [<portlist>] [clear]

<portlist> – 端口号列表,如:1,2,4-5,可选

[clear] – 统计复位,可选;

描述:查询端口的统计信息;

### 7. 流控处理模式

命令:Excessive Collisions Drop [enable|disable]

enable – 丢包流控



描述:增加二层转发表;

### 3. 删除二层转发表

命令:Delete <macaddress> [<vid>]  
    <macaddress> – MAC地址, 如:00:00:11:22:33:44  
    [<vid>] – VLAN ID号, 可选, 默认为1

描述:删除二层转发表;

### 4. 查询转发表

命令:Lookup <macaddress> [<vid>]  
    <macaddress> – MAC地址  
    [<vid>] – VLAN ID号, 可选, 默认为1

描述:查询指定二层转发表的状态;

### 5. 特定VLAN二层转发表查询

命令:Table <vidlist>  
    <vidlist> – VLAN列表, 如1,3,5-6

描述:查询指定VLAN的所有二层转发表;

### 6. 转发表老化时间

命令:Agetime [<agetime>]  
    [<agetime>] – 老化时间, 单位为秒, 默认为300

描述:动态二层转发表的老化时间配置;

## 第9章 VLAN配置

通过输入“vlan”命令, 您将可以进入vlan配置模式, 如下图:

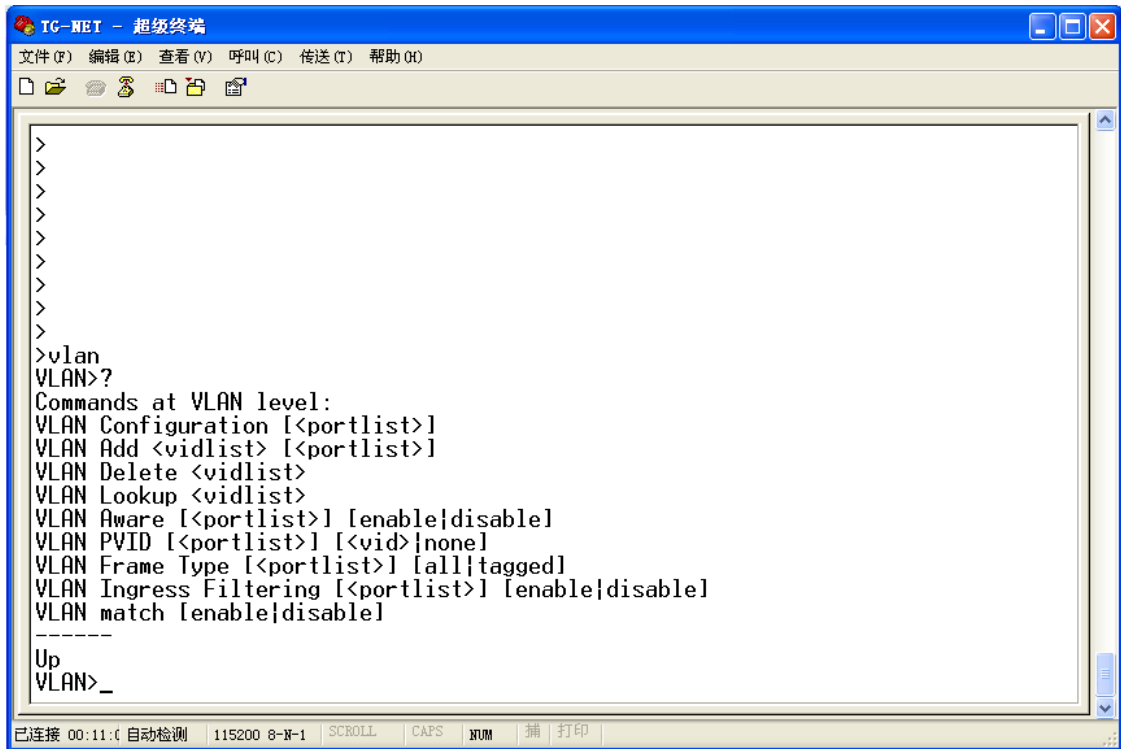


图3. 1. 5 VLAN配置

其中:

#### 1. VLAN配置查询

命令: Configuration [<portlist>]

<portlist> - 端口号列表, 如:1,2,4-5

描述: 查询指定端口的VLAN配置信息, 默认为所有端口。

#### 2. 添加VLAN

命令: Add <vidlist> [<portlist>]

<vidlist> - VLAN列表, 可以是单个或者一组VLAN ID, 如1,3,5-6

<portlist> - 端口号列表, 默认为所有端口□如:1,2,4-5

描述: 把一组端口加入到一组VLAN中去;

#### 3. 删除VLAN

命令: Delete <vidlist>

<vidlist> - VLAN列表, 如1,3,5-6

描述: 删除一组VLAN时, 对应PVID也会被删除;

#### 4. VLAN查询

命令: Lookup <vidlist>

<vidlist> – VLAN列表, 可以是单个或者一组VLAN ID如1,3,5-6

描述: 查询VLAN对应的端口信息;

## 5. TAG设置

命令: Aware [<portlist>] [enable|disable]  
[<portlist>] – 端口号列表, 如: 1,2,4-5

enable – 表示对应端口输出打TAG标记

disable – 表示对应端口输出不打TAG标记

描述: 配置对应的端口输出报文是否打上TAG标记;

## 6. 端口PVID

命令: PVID [<portlist>] [<vid>|none]  
[<portlist>] – 端口号列表, 如: 1,2,4-5

[<vid>|none] – VLAN ID号, 如果为none, 表示采用默认VLAN;

描述: 配置端口的默认VLAN ID号;

## 7. 配置端口的接收帧类型

命令: VLAN Frame Type [<portlist>] [all|tagged]

<portlist> 端口列表, 默认为所有端口。

all表示接收所有类型帧, 包括不带tag的帧, 带tag的帧, 带tag但是VLAN ID为0的帧等。

tagged表示只接收带tag的帧, 并且tag中的VLAN ID不应为0。

## 8. VLAN输入过滤

命令: Ingress Filtering [<portlist>] [enable|disable]  
[<portlist>] – 端口号列表, 如: 1,2,4-5

enable – 表示不匹配VLAN的包丢弃;

disable – 表示不匹配VLAN的包接受

描述: 配置是否允许非法VLAN通过, 默认是不匹配的VLAN报文接受

## 9. 配置VLAN match

命令: VLAN match [enable|disable]  
enable – 表示匹配VLAN信息;



命令: Delete <ipaddress> [<macaddress>] [<port>]

<ipaddress> - IP地址

<macaddress> - MAC地址

<port> - 端口号

描述: 在指定端口删除ARP表项;

#### 4. 清空所有ARP

命令: Flush

描述: 清空ARP表项。

## 第11章 端口聚合配置

通过输入“aggr”命令, 您将可以进入端口聚合配置模式, 如下图:

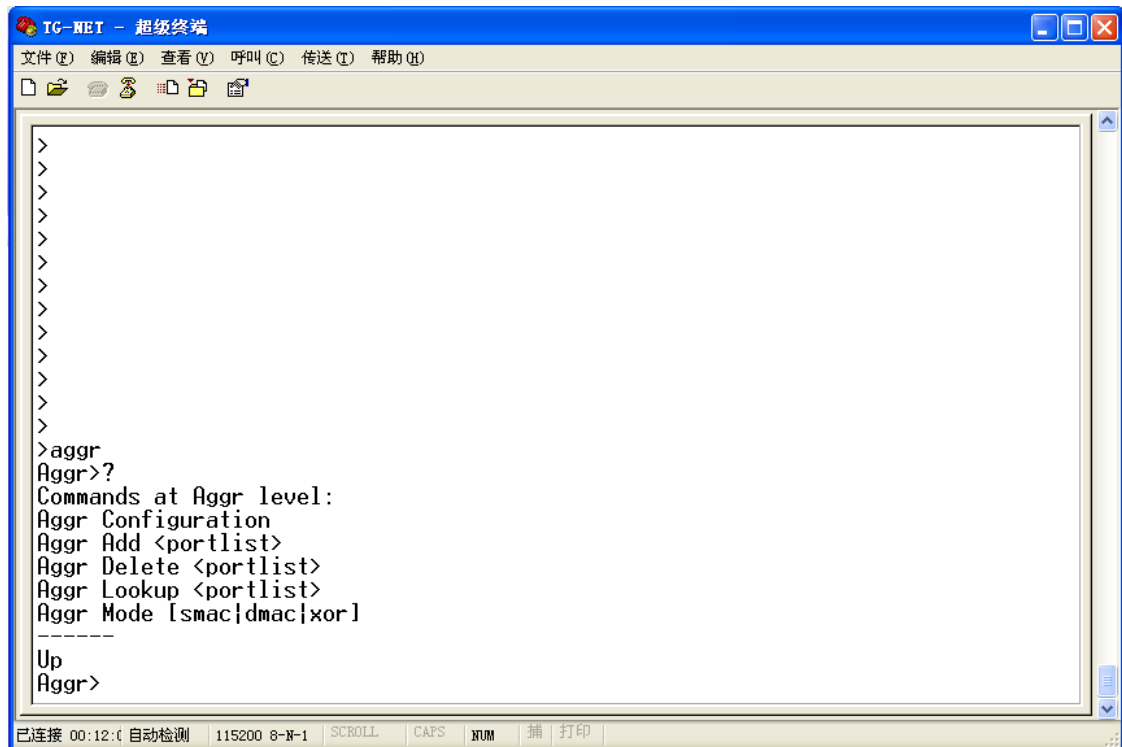


图3. 1. 7 端口聚合配置

其中:

#### 1. 聚合配置查询

命令: Configuration

描述: 查询端口聚合配置信息;

#### 2. 增加端口聚合组

命令: Add <portlist>



[<portlist>] –端口号列表, 如:1,2,4-5

描述:创建一个聚合组, 并配置该聚合组的端口列表;

### 3. 删除端口聚合组

命令:Delete <portlist>

[<portlist>] –端口号列表, 如:1,2,4-5

描述:删除一个端口聚合组;

### 4. 端口聚合组查询

命令:Lookup <portlist>

[<portlist>] –端口号列表, 如:1,2,4-5

描述:查询特定端口所属聚合组;

### 5. 设定汇聚链路的均衡算法

命令:Aggr Mode [smac|dmac|xor]

smac –表示基于报文的源MAC地址进行均衡计算;

Dmac –表示基于报文的的目的MAC地址进行均衡计算;

Xor –表示将报文的源MAC地址和目的MAC地址进行异或之后再行均衡计算;

描述:均衡算法的指定是全局性的。

## 第12章 LACP配置

通过输入“lacp”命令, 您将可以进入LACP配置模式, 如下图:

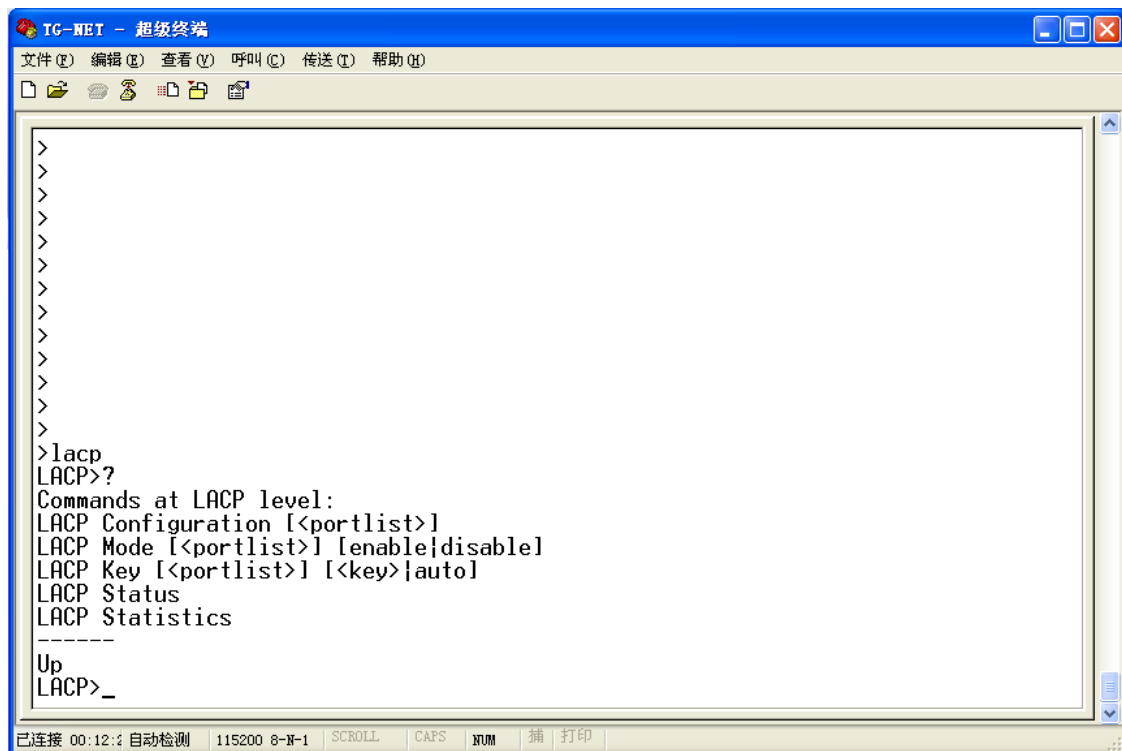


图3. 1. 8 LACP配置

其中:

1. 显示LACP配置信息

命令:LACP Configuration [<portlist>]  
[<portlist>]-端口号列表, 如:1,2,4-5

描述:显示指定端口LACP配置信息;

2. 配置指定端口LACP协议

命令:LACP Mode [<portlist>] [enable|disable]  
[<portlist>]-端口号列表, 如:1,2,4-5

描述:配置指定端口开启或禁用LACP协议;

3. 配置指定端口Key值

命令:LACP Key [<portlist>] [<key>|auto]  
[<portlist>]-端口号列表, 如:1,2,4-5, 默认所有端口.

[<key>]-key值在 1 – 255之间;[Auto] 表示自动协商Key值

描述:配置端口Key值

4. 查询LACP组和端口状态

命令:LACP Status

描述:查询LACP组和端口状态,本端组号、本端端口号、对端设备MAC地址、对端端口号等信息

## 5. 查询LACP协议端口统计

命令:LACP Statistics

描述:查询LACP协议端口统计

# 第13章 快速生成树配置

通过输入“rstp”命令,您将可以进入快速生成树配置模式,如下图:

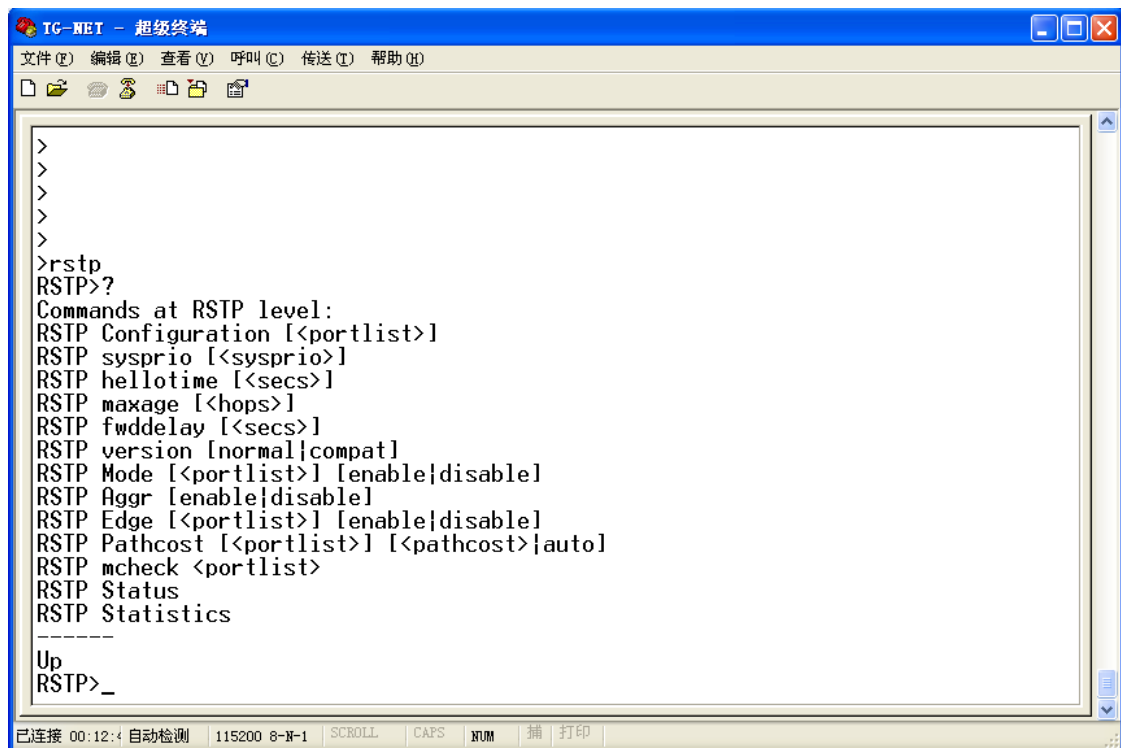


图3.1.9 快速生成树配置

其中:

### 1. 显示当前交换机的快速生成树配置情况

命令:RSTP Configuration [<portlist>]  
[<portlist>] –端口号列表,如:1,2,4-5

描述:显示当前的快速生成树配置情况。

### 2. 修改当前交换机的生成树优先级

命令:RSTP sysprio [<sysprio>]

[<sysprio>] –优先级列表, 0 – 61440之间, 为4.96的整数倍

描述:修改、查询当前交换机的生成树优先级, 默认为32768。

### 3. 修改当前交换机的Hello时间

命令:RSTP hellotime [<secs>]

[<secs>] – 时间列表, 如:1, 2, 3

描述:生成树的HELLO时间为1-10S内, 默认为2S。

### 4. 修改当前交换机的生成树最大老化时间

命令:RSTP maxage [<hops>]

[<hops >] – 老化时间列表, 6-40之间, 默认为20

描述:修改、查询当前交换机的生成树最大老化时间。

### 5. 修改当前交换机的生成树转发延迟时间

命令:RSTP fwddelay [<secs>]

[<secs>] –时间列表, 如4-30之间, 默认为15

描述:修改、查询当前交换机的生成树转发延迟时间

### 6. 修改当前交换机的生成树版本

命令:RSTP version [normal | compat]

Normal –表示版本正常, 在此版本下, 交换机可以识别STP格式的B

PDU, 也可以识别RSTP格式的BPDU

Compat –表示版本兼容, 在此版本下, 交换机只接收和发送STP格式的BPD

U

描述:修改、查询当前交换机的生成树版本, 默认为Normal。

### 7. 修改当前交换机的生成树状态

命令:RSTP Mode [<portlist>] [enable | disable]

[<portlist >] –端口列表, 如:1,2,4-5, 默认所有端口

Enable—表示开启端口RSTP

Disable—表示关闭端口RSTP

描述:修改当前交换机每个端口的生成树状态

#### 8、修改当前交换机交换机汇聚链路上RSTP协议状态

命令:RSTP aggr [enable | disable]

Enable—表示在交换机汇聚链路上开启RSTP协议;

Disable—表示在交换机汇聚链路上关闭RSTP协议;

描述:修改当前交换机交换机汇聚链路上RSTP协议状态

#### 9、配置当前交换机的生成树边缘端口

命令:RSTP edge [<portlist>] [enable | disable]

[<portlist >]—端口列表, 如:1,2,4-5

Enable—表示指定端口为生成树边缘端口;

Disable—表示指定端口非生成树边缘端口;

描述:配置当前交换机的生成树边缘端口, 默认所有端口均为边缘端口

#### 10、修改当前交换机的生成树端口的路径开销值

命令:RSTP pathcost [<portlist>] [<pathcost> | auto]

[<portlist >]—端口列表, 如:1,2,4-5, 默认为所有端口

<pathcost>—表示路径开销值, 1 – 200000000之间

Auto—表示自动计算路径开销

描述:修改生成树端口的路径开销, 值越小,路径越优先

#### 11、强制端口迁移到RSTP模式下运行

命令:RSTP mcheck <portlist>

[<portlist >]—端口列表, 如:1,2,4-5;

描述:将指定端口强制迁移到RSTP模式下运行

#### 12. RSTP状态信息

命令:RSTP Status

描述:查询RSTP系统及端口信息。

### 13. RSTP信息统计

命令:RSTP Statistics

描述:统计RSTP端口信息。

## 第14章 用户组配置

通过输入“User Group”命令，您将可以进入User Group配置模式，如下图：

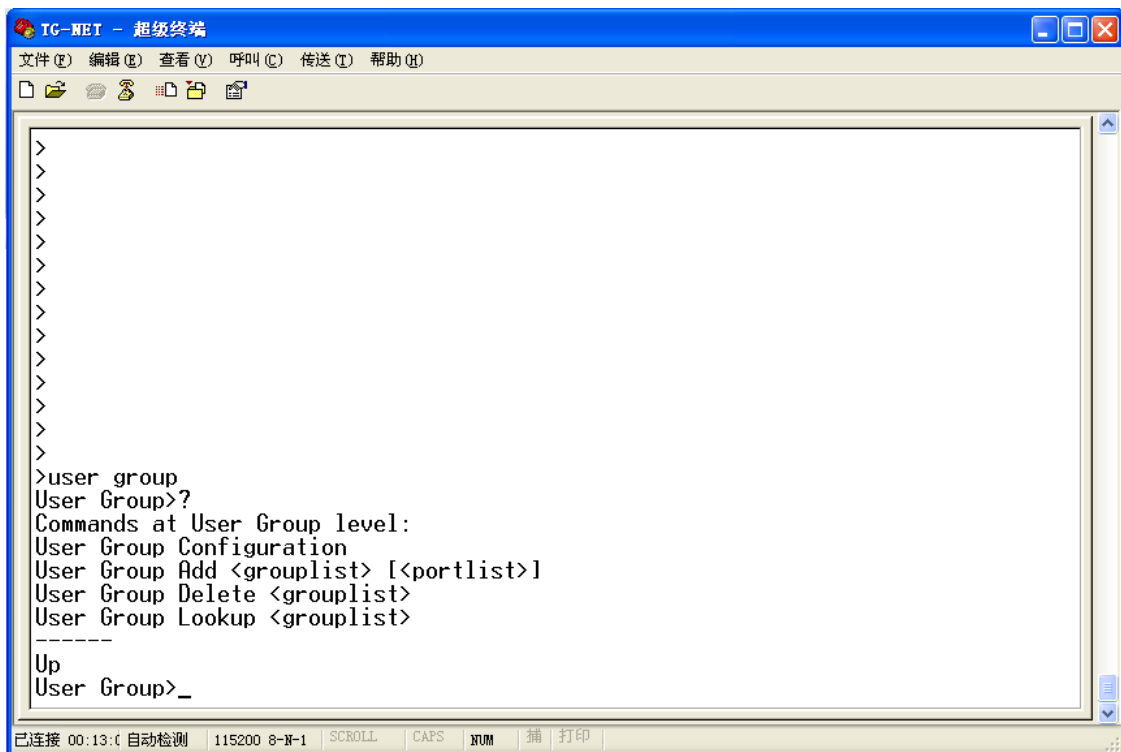


图3. 1. 10 用户组配置

其中：

#### 1. 显示当前的用户组配置情况

命令:User Group Configuration

描述:显示当前的用户组配置情况，显示信息包括已经配置的各用户组及其成员  
端口列表；

#### 2. 创建用户组或者向用户组追加端口

命令:User Group Add <grouplist> [<portlist>]

<grouplist> 一用户组列表，可配置范围为1~24；

<portlist>— 端口列表, 默认为所有端口。

描述:

当指定的用户组不存在时, 创建新的用户组, 并添加指定的端口, 当用户组已经存在时, 则向该用户组追加端口。

### 3. 删除指定的用户组

命令: User Group Delete <grouplist>

<grouplist>— 组列表, 如: 1,2,4-5

描述: 删除选中的user group组

### 4. 查询指定的用户组

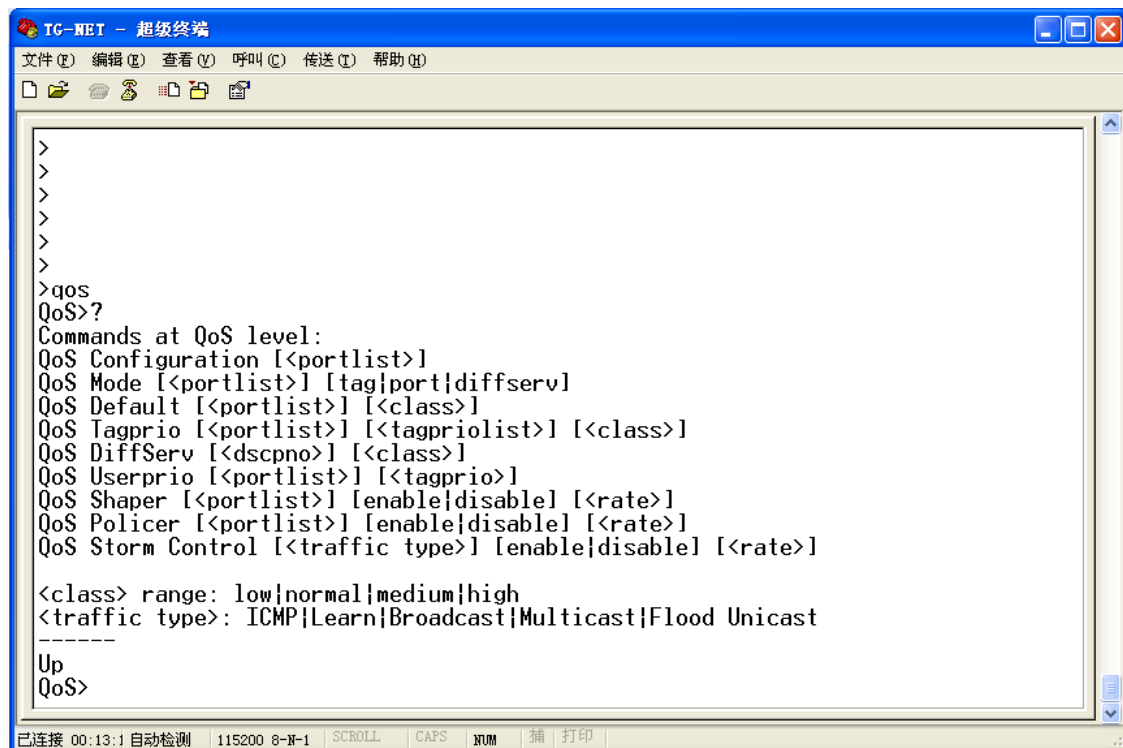
命令: User Group Lookup <grouplist>

<grouplist>— 用户组列表, 可选范围为1~24, 如: 1,2,4-5

描述: 查询指定的用户组, 显示指定用户组的端口列表

## 第15章 Qos配置

通过输入“qos”命令, 您将可以进入QOS配置模式, 如下图:



```

>
>
>
>
>
>
>
>qos
QoS>?
Commands at QoS level:
QoS Configuration [<portlist>]
QoS Mode [<portlist>] [tag|port|diffserv]
QoS Default [<portlist>] [<class>]
QoS Tagprio [<portlist>] [<tagpriolist>] [<class>]
QoS DiffServ [<dscpno>] [<class>]
QoS Userprio [<portlist>] [<tagprio>]
QoS Shaper [<portlist>] [enable|disable] [<rate>]
QoS Policer [<portlist>] [enable|disable] [<rate>]
QoS Storm Control [<traffic type>] [enable|disable] [<rate>]

<class> range: low|normal|medium|high
<traffic type>: ICMP|Learn|Broadcast|Multicast|Flood Unicast
-----
Up
QoS>
```

图3. 1. 11 Qos配置

其中:

### 1. 查询QOS配置

命令: Configuration [<portlist>]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5

描述: 查询QOS的配置信息

### 2. QOS工作类型

命令: Mode [<portlist>] [tag|port|diffserv]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5  
          tag – 支持802.1Q  
          port – 支持基于端口的QOS  
          diffserv – 支持差距服务

描述: 配置对应端口支持的QOS类型;

### 3. 端口优先级

命令: Default [<portlist>] [<class>]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5  
          [<class>] – 优先级别, 包括: low, normal, medium, high

描述: 配置对应的端口的优先级别, 其中low优先级最低;

### 4. 802.1Q优先级转换

命令: Tagprio [<portlist>] [<tagpriolist>] [<class>]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5  
          <tagpriolist> – TAG中优先级值0-7;

          [<class>] – 优先级别, 包括: low, normal, medium, high

描述: 配置如何把802.1Q中优先级值转换成交换机本地的处理优先级;

### 5. 差距服务转换

命令: DiffServ [<dscpno>] [<class>]  
          <dscpno> – IP报文的差距服务值, 范围为1-63

          [<class>] – 优先级别, 包括: low, normal, medium, high



**描述:**配置如何把IP报文中DiffServ值转换成交换机本地的处理优先级

## 6. 输出802.1Q优先级

**命令:** Userprio [<portlist>] [<tagprio>]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5  
          <tagprio>] – TAG报文对应的输出优先级

**描述:**配置对应端口输出时对应的TAG优先级;

## 7. 输入报文流控

**命令:** Shaper [<portlist>] [enable|disable] [<rate>]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5  
          [enable|disable] – 启动流控开关  
          <rate> – 输入流控值, 取值范围为0-3968K

**描述:**配置对应端口的最大输入流量值, 单位为bits/s;

**举例:** Shaper 1-2 enable 128K

## 8. 输出报文流控

**命令:** Policer [<portlist>] [enable|disable] [<rate>]  
          [<portlist>] – 端口号列表, 如: 1,2,4-5  
          [enable|disable] – 启动流控开关  
          <rate> – 输出流控值, 取值范围为0-3968K

**描述:**配置对应端口的最大输出流量值, 单位为bits/s;

**举例:** Policer 1-2 enable 128K

## 9. 广播风暴限制

**命令:** Storm Control [<traffic type>] [enable|disable] [<rate>]  
          <traffic type> –  
          进行风暴控制的类型, 包括: ICMP|Learn|Broadcast|Multicast|Flood Unicast  
          [enable|disable] – 风暴控制开关  
          <rate> – 风暴流控值, 单位为pps;



enable — 允许输入镜像

disable — 不允许输入镜像

描述: 配置镜像的源端口

## 第17章 IP地址配置

通过输入“ip”命令, 您将可以进入Ip地址配置模式, 如下图:

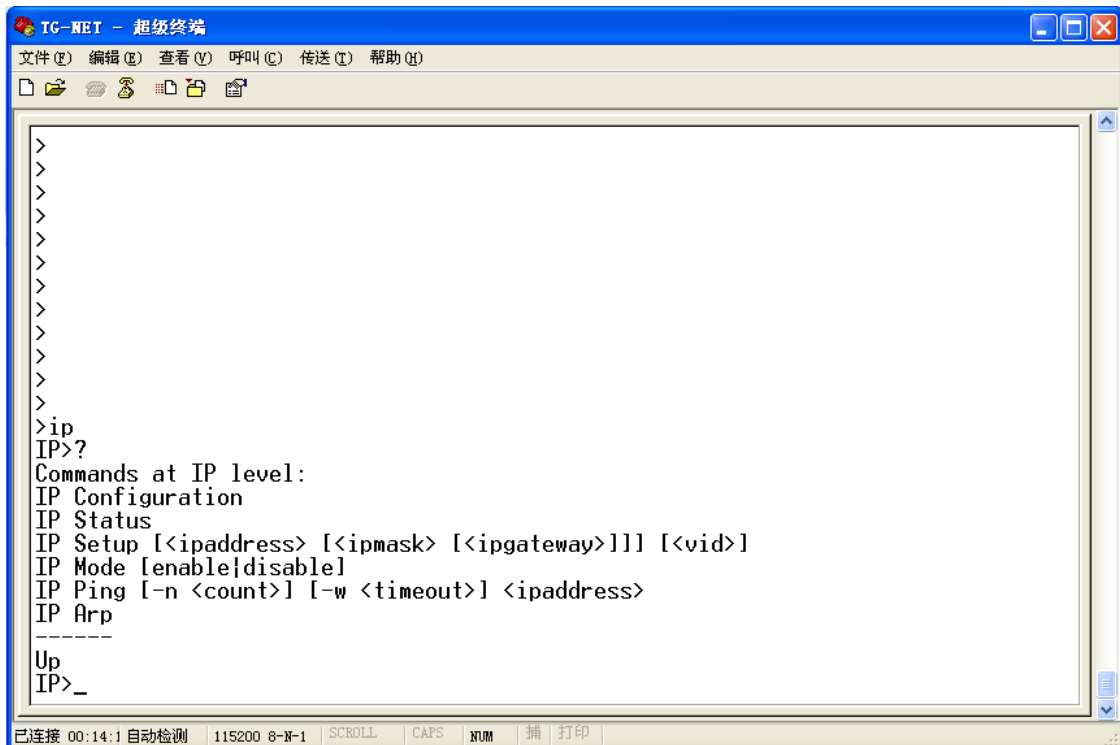


图3. 1. 13 IP地址配置

其中:

### 1. IP配置查询

命令: Configuration

描述: 查询IP命令模式下的配置信息

### 2. 交换机管理IP地址

命令: Setup [<ipaddress> [<ipmask> [<ipgateway>]] [<vid>]

<ipaddress> — IP地址

<ipmask> — IP掩码

<ipgateway> — IP网关

<vid> — 管理VLAN ID, 可选, 默认为1;

描述: 配置交换机管理IP地址;

### 3. IP访问使能开关

命令: Mode [enable|disable]

enable — 表示该交换机可以通过IP地址进行访问

disable — 表示该交换机不能通过IP地址进行访问

描述: 配置对应的交换机是否支持通过IP进行HTTP访问, 默认为支持;

### 5. Ping功能

命令: Ping [-n <count>] [-w <timeout>] <ipaddress>

[-n <count>] — 表示PING的次数;

[-w <timeout>] — 表示每次PING失败超时等待时间;

<ipaddress> — PING的IP地址

描述: PING功能, 在测试与其它设备的网络连通性时有用。

### 6. ARP地址查询

命令: Arp

描述: 查询访问本交换机所有建立的ARP表;

## 第18章 Dot1x配置

通过输入“dot1x”命令, 您将可以进入dot1x配置模式, 如下图:



描述:配置交换机端口的Dot1x认证状态, 自动、强制授权、强制断开

#### 4.配置RADIUS 服务器IP地址

命令:Dot1x Server [<IP Address>]

[<IP Address>] -RADIUS 服务器IP地址

描述:配置RADIUS 服务器IP地址

#### 5.配置RADIUS 服务器协议端口号

命令:Dot1x UDP Port [<value>]

[<value>] -RADIUS 服务器协议端口号

描述:配置RADIUS 服务器协议端口号

#### 6.配置RADIUS通信密钥

命令:Dot1x Secret [<Shared Secret>]

[<Shared Secret>] -RADIUS 通信密钥

描述:配置RADIUS通信密钥

#### 6. 查询设备端口802.1X统计信息

命令:Dot1x Statistics [<portlist>]

[<portlist>] - 端口号列表, 如:1,2,4-5, 默认为所有端口

描述:查询设备端口802.1X统计信息

#### 7. 配置端口重新认证

命令:Dot1x Reauthenticate [<portlist>] [now]

[<portlist>] - 端口号列表, 如:1,2,4-5, 默认为所有端口

[now] - 立即进行重新认证

描述:配置端口重新认证

#### 8. Dot1x参数配置

命令:Dot1x Parameters [<parameter>] [<value>]

[<parameter>] -Reauthentication、Reauth-period、EAP-Timeout参数配置

描述:系统默认关闭Reauthentication;Reauth-period为3600秒;EAP-Timeout为30秒

## 第19章 IGMP配置

通过输入“igmp”命令，您将可以进入IGMP snooping配置模式，如下图：

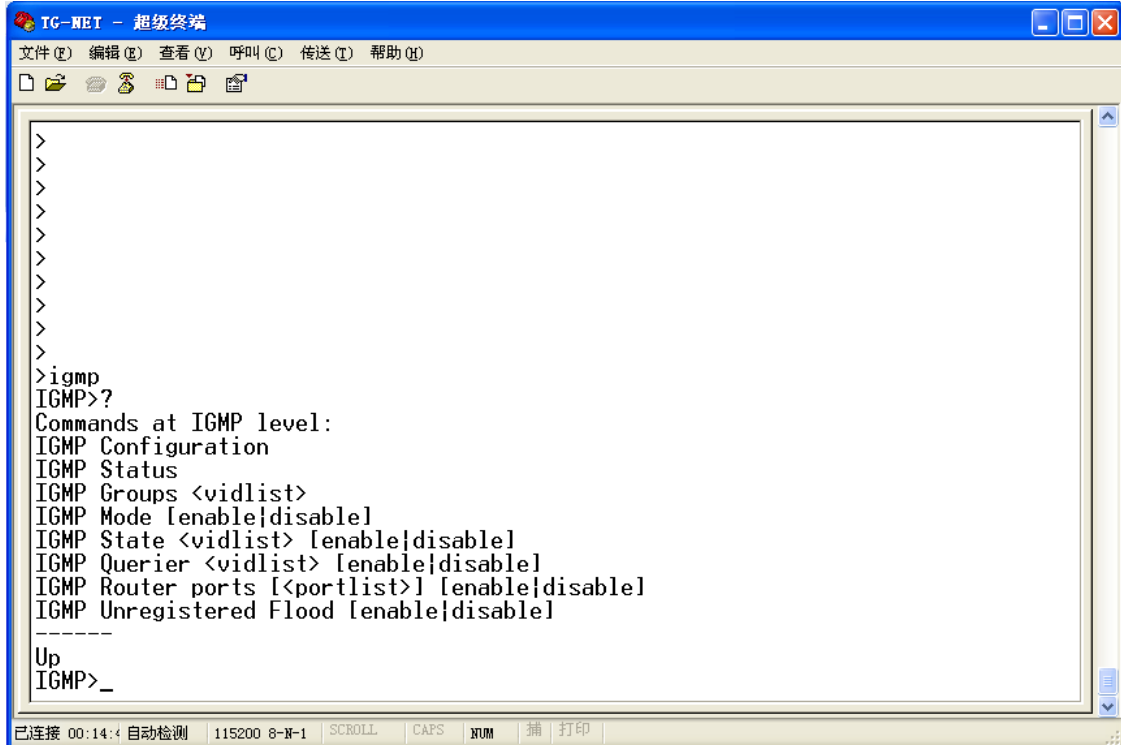


图3.1.15 IGMP配置

其中：

### 1. IGMP SNOOP配置查询

命令: Configuration

描述: 查询IGMP SNOOPING的配置信息

### 2. IGMP SNOOPING工作状态查询

命令: Status

描述: 查询IGMP SNOOPING的工作状态；

### 3. 组播VLAN

命令: Groups <vidlist>

<vidlist> — VLAN列表

描述: 配置IGMP SNOOPING的VLAN组；

### 4. IGMP SNOOPING使能开关

命令: Mode [enable|disable]

描述:配置是否启动IGMP SNOOPING功能;

#### 5. 配置VLAN启动IGMP SNOOPING功能

命令: State <vidlist> [enable|disable]

<vidlist> – VLAN列表

enable – 启动igmp snooping功能

disable – 关闭igmp snooping功能

描述:指定哪些VLAN支持IGMP SNOOPING功能

#### 6. 查询VLAN配置

命令: Querier <vidlist> [enable|disable]

<vidlist> – VLAN列表

enable – 支持igmp snooping路由器端口协商

disable – 不支持igmp snooping路由器端口协商

描述:配置哪些VLAN支持igmp snooping路由器端口协商;

#### 7. 路由器端口配置

命令: Router ports [<portlist>] [enable|disable]

[<portlist>] – 端口号列表, 如: 1,2,4-5

enable – 配置对应端口为路由器端口

disable – 关闭对应端口为路由器端口

描述:静态配置对应交换机端口是否为igmp snooping路由器端口;

#### 8. 未注册组播处理模式

命令: Unregistered Flood [enable|disable]

enable – 未注册的组播报文广播

disable – 未注册的组播报文丢弃

描述:配置对未注册的组播数据是否进行广播处理;



## 附录 常见故障诊断

故障现象	可能的故障原因	解决方法
加电时所有指示灯均不亮	电源连接错误或供电不正常	检查电源线和插座
LINK指示灯不亮	1. 网线损坏或连接不牢。 2. 网线类型错误或网线过长, 超出允许范围	更换网线
网络能通, 但传输速度变慢, 有丢包现象	交换机与网络终端以太网口工作模式不匹配	设置以太网口工作模式使其匹配或将其设为自适应工作模式
在某一口可通, 将网线换到其他口时则不通	将网线换到其他网口时, 如果此端口所连接的设备没有发送数据, 交换机将学不到新地址, 因此此端口会暂时不通	120秒后交换机的地址会自动更新, 此现象会自动消失; 或者从此网口发送数据也会使交换机立即更新其地址表
所有ACT指示灯闪烁, 网络速率变慢	广播风暴	1□ 检查网络连接是否成环路, 合理配置网络; 2□ 检查是否有站点发送大量的广播包
正常工作一段时间后停止工作	1. 电源不正常; 2. 过热;	1. 检查电源是否有接触不良, 电压过低或过高; 2. 检查周围环境, 通风孔是否畅通, 交换机风扇是否工作正常