



S5300系列万兆三层核心交换机

WEB 配置手册

©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

总部地址：深圳市南山区中山园路 1001 号国际 E 城 E3 栋

工厂地址：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：518052

服务电话：400-088-7500

网址：<http://www.tg-net.cn>

资料编号：20150422-S5300_V 4.2.1

目 录

| | | |
|-------|------------------------|----|
| 第 1 章 | 配置准备 | 5 |
| 1.1 | 通过 Web 访问交换机..... | 5 |
| 1.2 | Web 界面介绍..... | 5 |
| 第 2 章 | 系统状态 | 7 |
| 2.1 | 系统信息 | 7 |
| 2.2 | 系统日志 | 8 |
| 2.3 | 端口统计 | 8 |
| 2.4 | 详细统计 | 9 |
| 2.5 | ACL 统计 | 9 |
| 2.6 | AAA 统计 | 10 |
| 2.7 | LACP 状态 | 10 |
| 2.8 | STP 桥状态 | 11 |
| 2.9 | STP 端口 | 11 |
| 2.10 | LLDP 邻居 | 12 |
| 2.11 | 二层转发表 | 12 |
| 2.12 | 环路保护状态 | 13 |
| 第 3 章 | 系统设置 | 14 |
| 3.1 | IP 配置 | 14 |
| 3.2 | 日志配置 | 14 |
| 3.3 | 用户配置 | 15 |
| 3.4 | NTP 配置 | 16 |
| 第 4 章 | 端口配置 | 17 |
| 4.1 | 端口配置 | 17 |
| 4.2 | 端口隔离 | 19 |
| 4.3 | 端口镜像 | 20 |
| 4.4 | 端口安全 | 20 |
| 4.5 | 带宽策略 | 21 |
| 第 5 章 | 高级配置 | 22 |
| 5.1 | 链路聚合 | 22 |
| 5.2 | VLAN 管理 | 25 |
| 5.3 | VCL | 26 |
| 5.4 | DHCP 侦听配置 | 27 |
| 5.5 | DHCP 服务器 | 28 |
| 5.6 | DHCP 中继 | 31 |
| 5.7 | IGMP Snooping 配置 | 31 |
| 5.8 | 路由配置 | 32 |
| 第 6 章 | 网络安全 | 35 |
| 6.1 | MAC 地址表 | 35 |
| 6.2 | 风暴抑制 | 36 |
| 6.3 | IP 源保护 | 37 |
| 6.4 | ARP 检测 | 39 |
| 6.5 | ACL 配置 | 40 |

| | | |
|-------|----------------|----|
| 6.6 | STP 配置..... | 42 |
| 6.7 | 环路保护..... | 45 |
| 6.8 | ERPS 配置..... | 46 |
| 第 7 章 | 网络管理 | 49 |
| 7.1 | SSH 配置..... | 49 |
| 7.2 | HTTPS 配置..... | 50 |
| 7.3 | LLDP 配置..... | 50 |
| 7.4 | 802.1X 配置..... | 52 |
| 7.5 | SNMP 配置..... | 54 |
| 7.6 | RMON 配置..... | 59 |
| 第 8 章 | 系统维护 | 63 |
| 8.1 | 设备重启 | 63 |
| 8.2 | 恢复出厂配置 | 63 |
| 8.3 | 固件升级 | 64 |
| 8.4 | 配置导出 | 64 |
| 8.5 | 配置导入 | 64 |
| 8.6 | PING 诊断..... | 65 |
| 8.7 | 关于我们..... | 66 |

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 S5300 系列万兆三层核心交换机；
- 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1章 配置准备

1.1 通过 Web 访问交换机

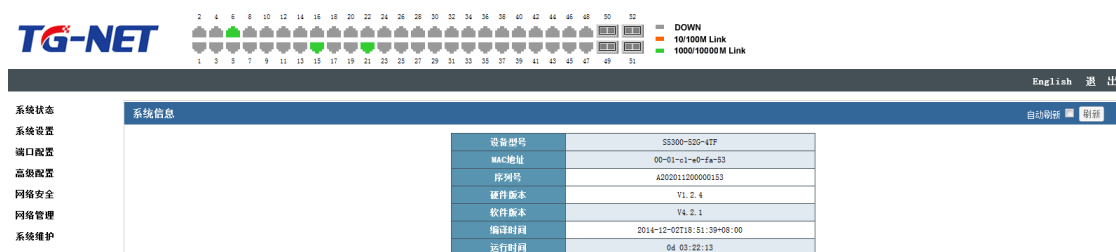
通过 Web 浏览器访问交换机，请确保您所使用的浏览器能够符合以下几点要求：

- HTML 版本 7.0
- HTTP 版本 1.1
- JavaScript™ 版本 1.5

此外，请确保交换机运行的主程序文件支持 Web 访问，且您的计算机已经连接到交换机所在的网络。如果是第一次使用交换机，无需额外配置，您已经可以使用 Web 访问：

- 1、修改您计算机网络适配器的 IP 地址为“192.168.255.2”，子网掩码为“255.255.255.0”。
 - 2、打开 Web 浏览器，在地址栏中输入“192.168.255.1”。
- 注意“192.168.255.1”是交换机的缺省管理地址。
- 3、在登录验证对话框中输入用户名和密码，初始的用户名和密码均为“admin”，请注意区分字母的大小写。
 - 4、若认证成功，浏览器中会显示交换机的系统信息页。

1.2 Web 界面介绍



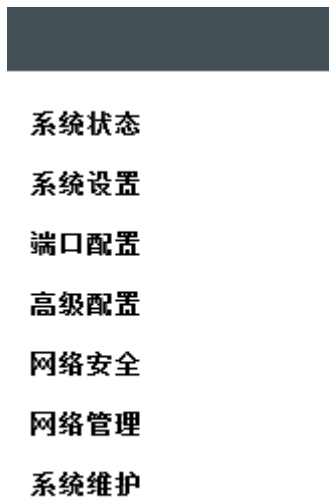
整个页面又分为顶部显示区、导航栏和配置区等部分。

1.2.1 顶部显示区



可以查看每个端口的链接状态，1000/10000M 端口显示绿灯；10/100M 端口显示橘黄色等。右侧“退出登录”按钮，提供注销功能；“English”按钮可以将界面切换到英文页面。

1.2.2 导航栏



导航栏控制配置区中显示的内容。导航栏的内容以列表的形式显示，并按类别分组。如需进行某项配置，请先点击组名，待列表展开后点击子项。比如，如果需要查看当前的端口流量，请先点击“系统状态”，然后点击“端口统计”。

1.2.3 配置显示区

| 系统信息 | | English | 退出 |
|-------|---------------------------|---------|----|
| 系统信息 | | 自动刷新 | 刷新 |
| 设备型号 | S5300-52G-4TF | | |
| MAC地址 | 00-01-e1-e0-fa-53 | | |
| 序列号 | A202011200000153 | | |
| 硬件版本 | V1. 2. 4 | | |
| 软件版本 | V4. 2. 1 | | |
| 编译时间 | 2014-12-02T18:51:39+08:00 | | |
| 运行时间 | 0d 00:00:46 | | |

配置显示区显示设备的状态信息和配置，通过点击导航栏的列表项可以改变该区域的内容。

1.2.4 配置区

配置区显示从导航栏中选中的内容，配置区提供查看、修改配置操作。

下面通过七章节来介绍 S5300 的五大配置模块：系统状态、系统配置、端口配置、高级配置、网络安全、网络管理、系统维护。



注意：

本手册中所有图示如无特殊说明均以 S5300-52G-4TF 交换机为例

第2章 系统状态

点击系统状态，您可以看到：

系统状态

系统信息

系统日志

端口统计

详细统计

ACL统计

AAA统计

LACP状态

STP桥状态

STP端口

LLDP邻居

二层转发表

环路保护状态

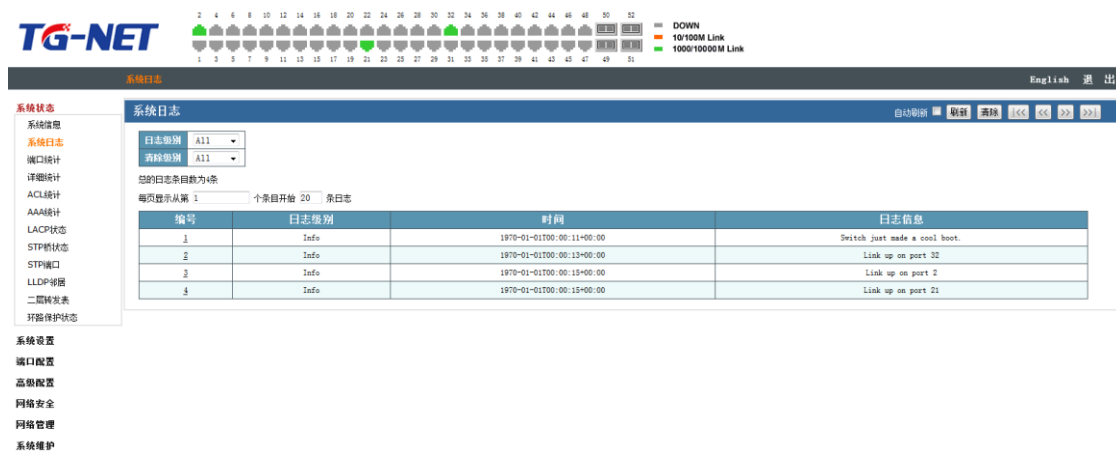
2.1 系统信息

The screenshot shows the TG-NET web interface. At the top, there is a status bar with port indicators (1-52) and a legend for link speeds (DOWN, 10/100M Link, 1000/10000M Link). Below this is a navigation menu on the left with '系统状态' (System Status) selected. The main content area displays '系统信息' (System Information) with a table of system details.

| 设备型号 | S5300-S20-4TF |
|-------|---------------------------|
| MAC地址 | 00-01-e1-e0-fa-53 |
| 序列号 | A2020011200000153 |
| 软件版本 | V1.2.4 |
| 软件版本 | V4.2.1 |
| 编译时间 | 2014-12-02T18:51:39+08:00 |
| 运行时间 | 0d 00:03:24 |

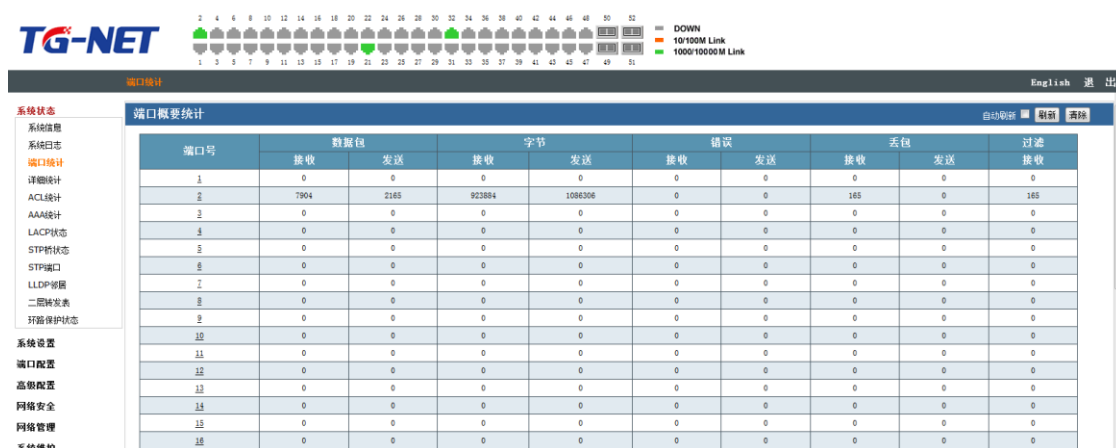
图为交换机系统信息显示界面。在系统信息页面中，可以查询看到本设备的型号、硬件版本、MAC 地址、设备序列号、软件版本、编译时间、运行时间。

2.2 系统日志



图为交换机系统日志显示界面。在系统日志页面中，可查看设备运行过程中的一些系统日志信息，方便维护人员分析问题。

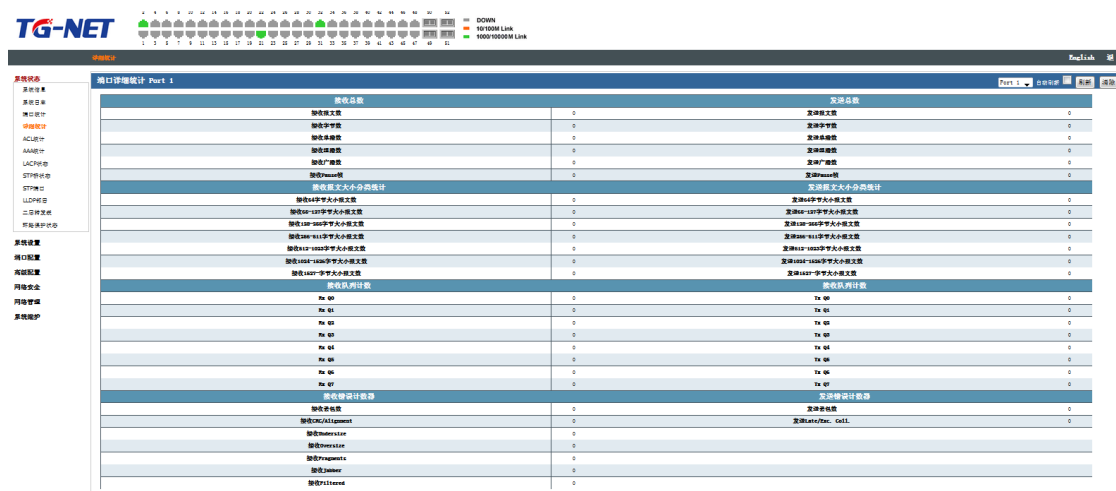
2.3 端口统计



图为交换机端口统计信息界面。在端口统计页面中，可以查看每个端口发送/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线缆或者对方网卡是否存在问题。

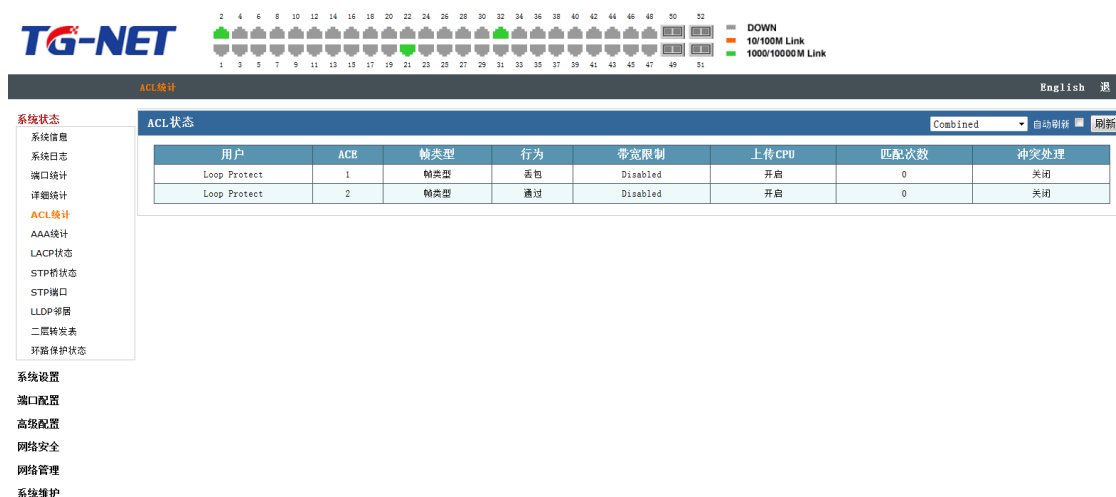
在该项功能中，用户可勾选“自动刷新”按钮，来实时刷新数据信息，也可人工点击“刷新”按钮来查看新的数据信息，“清除”按钮提供清空统计数据功能。

2.4 详细统计



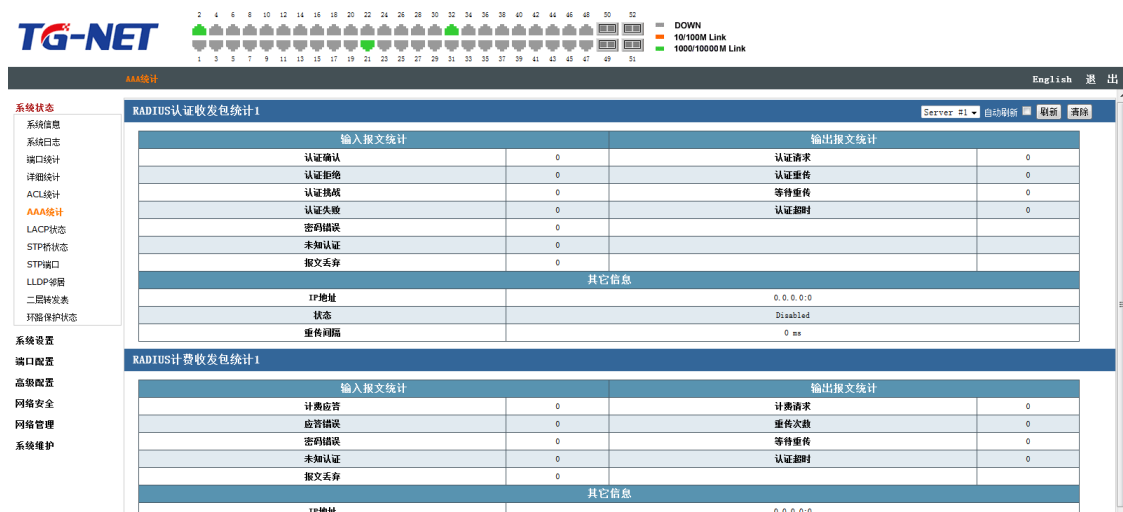
图为交换机所有端口的详细统计界面。在详细统计页面中，可以查询每个端口的详细工作情况，包括接收/发送报文数、广播包、错误包等等，便于网管人员进行网络维护。通过端口下拉菜单来查看指定端口流量信息，用户可勾选“自动刷新”按钮，来实时刷新数据信息，也可人工点击“刷新”按钮来查看新的数据信息，“清除”按钮提供清空统计数据功能。

2.5 ACL 统计



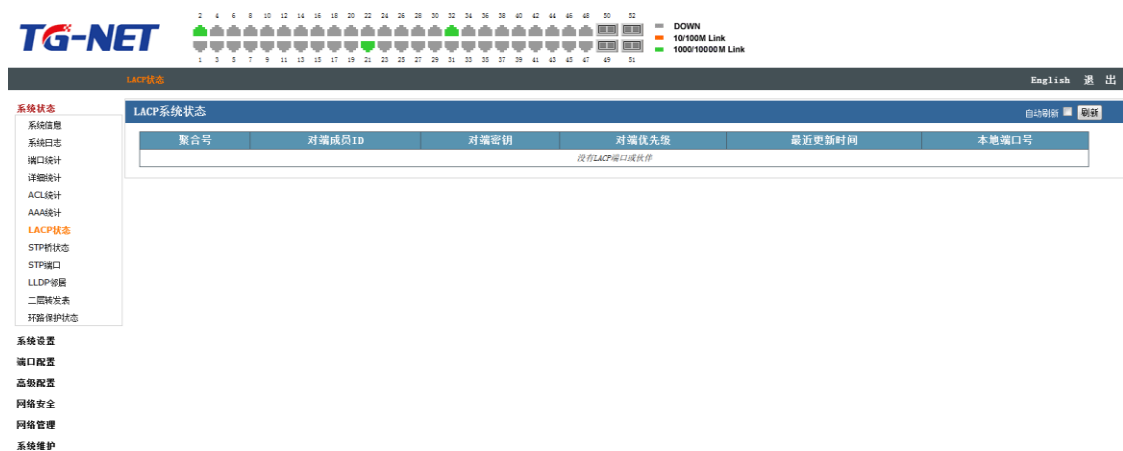
图为交换机 ACL 信息显示界面；在 ACL 统计页面，可查看相关安全信息，用户可通过下拉菜单选择“combined”、“static”、“ipmc”、“conflicts”查看各类网络安全信息。可勾选“自动刷新”按钮来实时显示，也可人工点击“刷新”按钮来查看新的信息。

2.6 AAA 统计



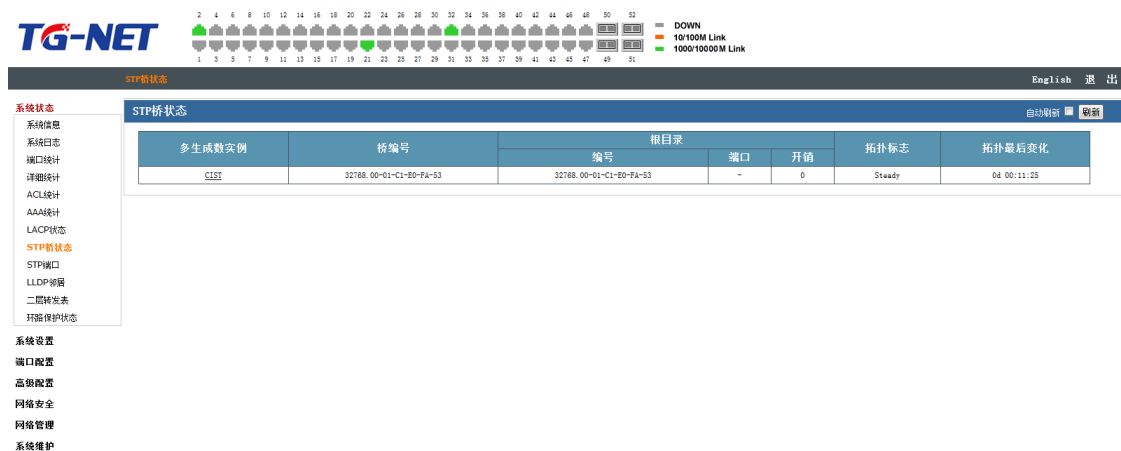
图为交换机系统 AAA 统计信息界面。若网络中已配置远程 radius 服务器，可通过此页面查看相关认证报文统计信息。

2.7 LACP 状态



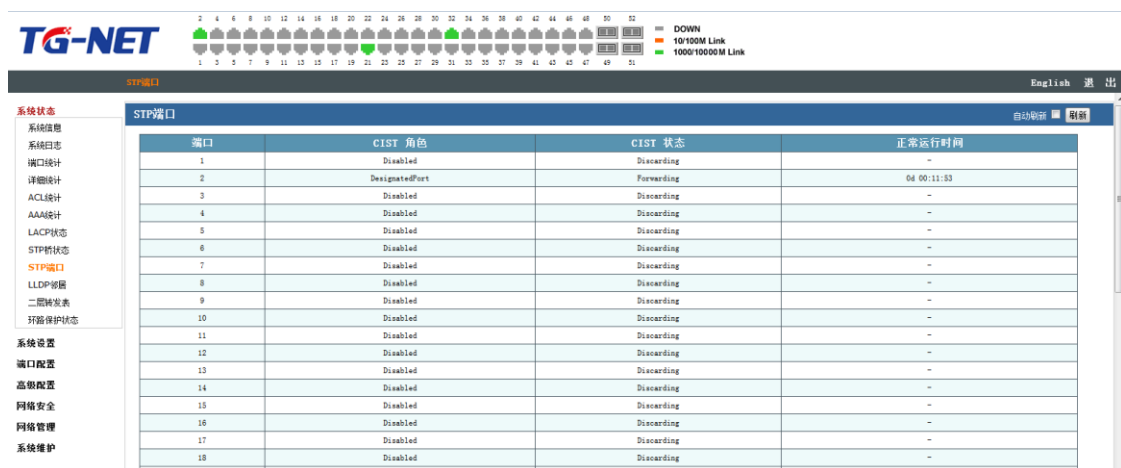
图为交换机 LACP 状态界面；在 LACP 状态页面，可以看到端口上 LACP 协议的运行状态，自动聚合的组号、本端端口号、对端成员 ID 号及通信密钥等信息。

2.8 STP 桥状态



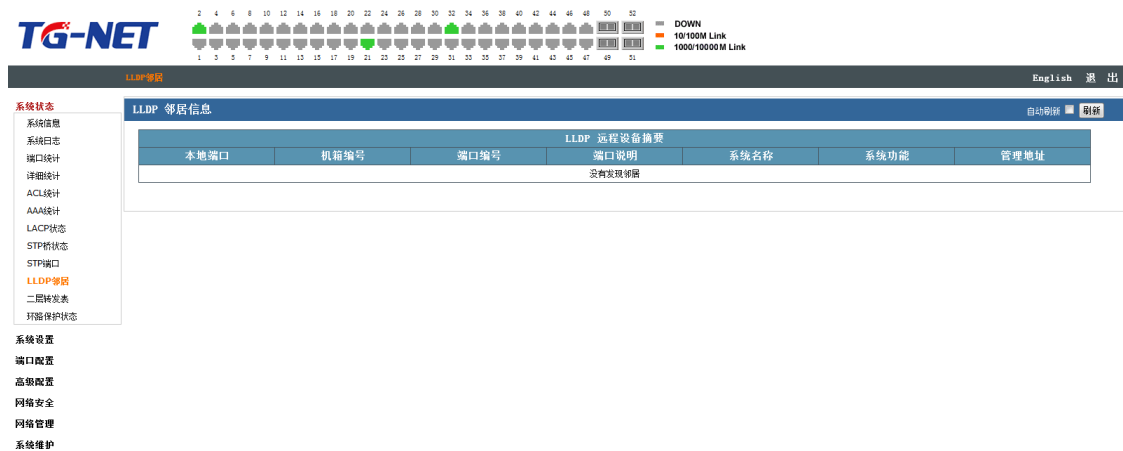
图为交换机生成树信息显示界面。在 STP 桥状态页面中，可以查看桥 ID、根桥 ID、端口路径开销等信息。

2.9 STP 端口



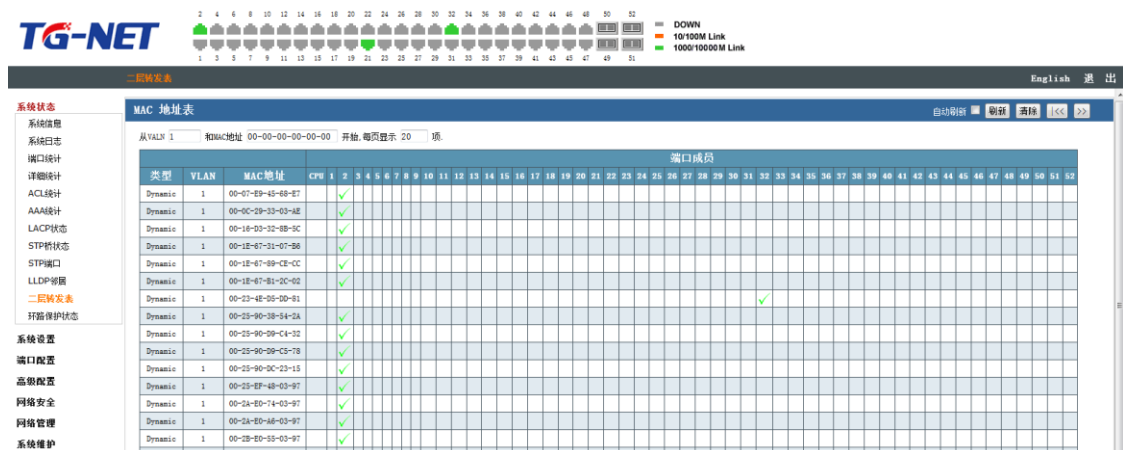
图为交换机生成树端口状态界面。可查看每个 STP 端口状态，包括 STP 角色、端口状态、更新时间等信息。

2.10 LLDP 邻居



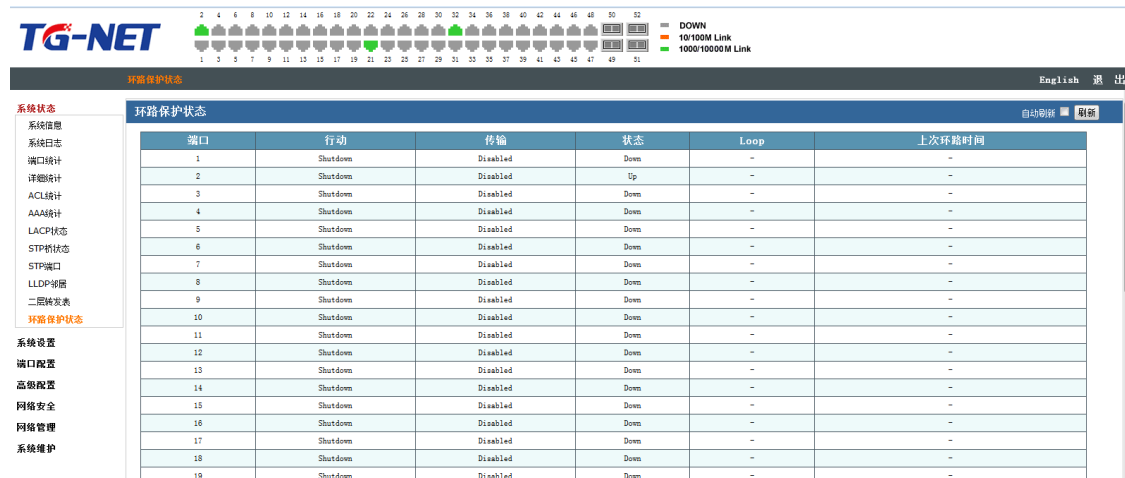
图为交换机 LLDP 信息显示界面。设备开启 LLDP（链路层发现协议）功能以后，可在此页面查看邻居信息，包括对端端口、系统名、端口说明、系统性能、管理地址等信息。

2.11 二层转发表



图为交换机二层转发表信息显示界面。此页面可查看交换机的所有二层 MAC 地址转发表，类型、端口、MAC 地址、VLAN 等表项。

2.12 环路保护状态



The screenshot shows the TG-NET web interface with the 'Loop Protection Status' page selected. The page displays a table of port status information. The table has the following columns: 端口 (Port), 行动 (Action), 传输 (Transmission), 状态 (State), Loop, and 上次环路时间 (Last Loop Time). The table lists ports 1 through 19. All ports are in a 'Shutdown' state with 'Disabled' transmission and 'Down' state. The 'Loop' column shows '-' for all ports, and the 'Last Loop Time' column shows '-' for all ports.

| 端口 | 行动 | 传输 | 状态 | Loop | 上次环路时间 |
|----|----------|----------|------|------|--------|
| 1 | Shutdown | Disabled | Down | - | - |
| 2 | Shutdown | Disabled | Up | - | - |
| 3 | Shutdown | Disabled | Down | - | - |
| 4 | Shutdown | Disabled | Down | - | - |
| 5 | Shutdown | Disabled | Down | - | - |
| 6 | Shutdown | Disabled | Down | - | - |
| 7 | Shutdown | Disabled | Down | - | - |
| 8 | Shutdown | Disabled | Down | - | - |
| 9 | Shutdown | Disabled | Down | - | - |
| 10 | Shutdown | Disabled | Down | - | - |
| 11 | Shutdown | Disabled | Down | - | - |
| 12 | Shutdown | Disabled | Down | - | - |
| 13 | Shutdown | Disabled | Down | - | - |
| 14 | Shutdown | Disabled | Down | - | - |
| 15 | Shutdown | Disabled | Down | - | - |
| 16 | Shutdown | Disabled | Down | - | - |
| 17 | Shutdown | Disabled | Down | - | - |
| 18 | Shutdown | Disabled | Down | - | - |
| 19 | Shutdown | Disabled | Down | - | - |

图为交换机系统信息界面。此页面可查看，环网网络中环网端口所处的一些状态信息。

第3章 系统设置

点击系统设置，您可以看到：

系统设置

IP配置

日志配置

用户配置

NTP配置

3.1 IP 配置

IP 配置页面可配置交换机的管理 IP 地址。交换机管理 VLAN 默认 VLAN 1，不可修改。



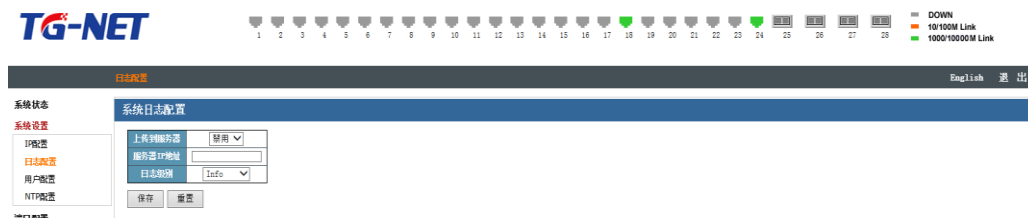
如图，IP 配置页面，可以查看设备的 IP 地址、掩码、管理 VLAN。交换机默认 IP 是 192.168.255.1，可以在此页面修改。

- DHCP 客户端：配置勾选表示交换机管理 IP 是由网络中的 DHCP 服务器分配；
- IP 地址：交换机管理 IP 地址，可以修改交换机管理 IP；
- 子网掩码：交换机子网掩码地址，可以修改配置；
- VLAN ID：交换机管理 VLAN，默认为 VLAN1，不可修改。

提示：请不要随意修改交换机子网掩码，如修改不当，会出现无法登陆交换机的情况。

3.2 日志配置

日志配置可将交换机的日志信息上传给远端日志服务器。



如图，日志配置页面，可配置远端日志服务器信息，将设备日志信息保存到远端服务

器，提供备份查看功能。

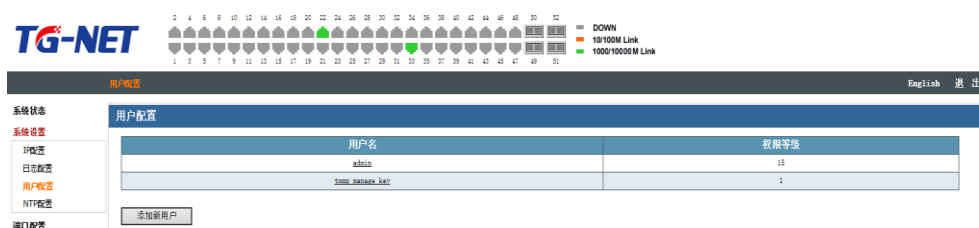
- 上传到服务器：全局开关，“使能”表示功能开启、“禁止”表示功能关闭；
- 服务器 IP 地址：填写远端日志服务器的 IP 地址；
- 日志级别：选择上传日志的级别

| 级别 | 含义 |
|---------|-----------|
| Info | 表示一般状态的日志 |
| Warning | 表示警告信息的日志 |
| Error | 表示错误信息的日志 |

提示：目前交换机只能显示 Info 级别的日志。目前该功能暂后期通过软件升级改善。

3.3 用户配置

用户配置可以访问交换机 **WEB** 界面的用户属性，达到保护交换机设置的目的。用户权限等级分 15 个等级。



用户配置

如图，用户配置界面。此页面可修改已存在用户的信息或者删除已有用户，也可以添加新的用户。



- 修改已存在用户的信息或删除该用户:

如修改用户“12345”，点击用户名 12345”，会弹出如下页面

您可以在此页面修改用户“12345”的登录密码和权限等级，或者点击“删除用户”按钮，删除该用户。

- 添加新用户：

点击“添加新用户”按钮，会弹出如下页面：

您可以在此处设置新用户的用户名，密码，权限等级。

提示：用户“admin”为管理员用户，默认不可删除。交换机默认用户名密码为 admin，如有修改密码，请牢记新密码，防止密码丢失登录设备失败。用户“tnmp_manage_key”为 TG 云盒子对接用户，默认不可删除。

3.4 NTP 配置

NTP（Network Time Protocol，网络时间协议）是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。

如图 3-4， NTP 配置界面。使用 NTP 的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

- 模式：实际为全局开关，“禁用”表示功能关闭、“使能”表示功能开启；
- 服务器 1-5：填写 NTP 服务器地址。

提示：由于交换机无法配置网关，NTP 功能暂无法正常使用，后期通过软件升级进行完善。

第4章 端口配置

点击端口配置，您可以看到：

端口配置

端口配置

端口隔离

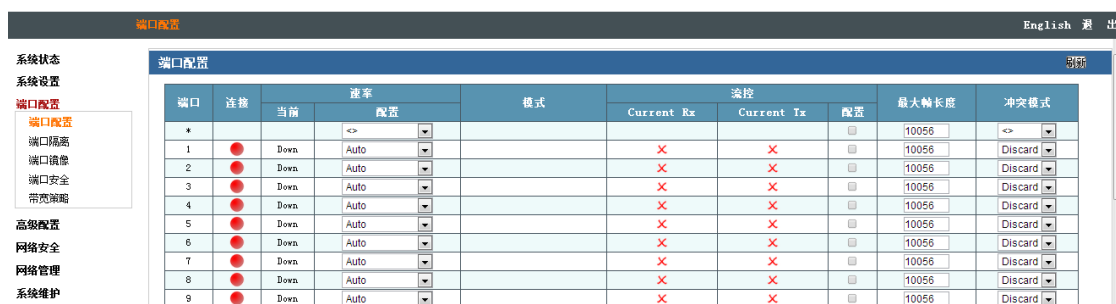
端口镜像

端口安全

带宽策略

4.1 端口配置

端口配置可配置交换机端口相关的各项基本参数。端口基本参数将直接影响端口的工作方式，请结合实际需求情况进行配置。



端口配置

如图，交换机端口配置界面，可查看每个端口的连接状态、端口速率双工方式、流控状态、最大帧长度配置及冲突模式配置，可配置端口的速率双工方式、收发方向流控功能、最大帧长度及冲突模式。

- 端口：显示交换机端口号；
- 连接：显示端口连接状态标识；

| 颜色 | 含义 |
|----|------------|
| 绿色 | 表示链路为连接状态 |
| 红色 | 表示链路为未连接状态 |

- 速率—当前：显示端口当前速率状态；

| 当前速率 | 速率双工模式 |
|--------|---------|
| 10Gfdx | 10G 全双工 |
| 1Gfdx | 1G 全双工 |

| | |
|--------|----------|
| 100fdx | 100M 全双工 |
| 100hdx | 100M 半双工 |
| 10fdx | 10M 全双工 |
| 10hdx | 10M 半双工 |
| Down | 端口未连接 |

- 速率—配置：配置端口速率双工方式；

提示：更改端口速率双工方式，会直接影响到的端口的通信，请谨慎修改。

| 端口类别 | 速率模式 | 含义 |
|------|-----------------|-------------------|
| 电口 | Auto（默认值） | 端口速率双工方式自适应 |
| | Disabled | 禁用端口 |
| | 10Mbps HDX | 端口速率双工方式 10M 半双工 |
| | 10Mbps FDX | 端口速率双工方式 10M 全双工 |
| | 100Mbps HDX | 端口速率双工方式 100M 半双工 |
| | 100Mbps FDX | 端口速率双工方式 100M 全双工 |
| | 1Gbps FDX | 端口速率双工方式 1G 全双工 |
| 复用光口 | 1000-X_AMS（默认值） | 光口速率双工方式千兆自适应 |
| | 1000-X | 光口强制千兆全双工模式 |
| | Disabled | 禁用光口 |
| 万兆口 | 10Gbps FDX | 端口速率双工方式 10G 全双工 |
| | Disabled | 禁用万兆口 |

- 模式：配置万兆口兼容模式；

| 模式 | 含义 |
|------------|---------------------|
| switch（默认） | 表示万兆口端口兼容模式为 switch |
| auto | 表示万兆口端口兼容模式为 auto |

万兆口设计兼容模式，用于解决对接不同品牌的万兆交换机端口或不同厂商的万兆网卡的兼容性问题，默认情况下，请使用 switch 模式，出现万兆口对接不兼容情况下，可以考虑更改万兆口模式为 auto。

提示：配置万兆口兼容模式，可能会影响到的端口的通信，请谨慎修改。

- 流控：配置交换机端口流控功能（默认关闭）；

在端口流控-配置处，勾选表示启用端口流控功能；未勾选表示未启用端口流控功能；

Current Tx/Rx 表示端口在发送/接收方向上的流控状态（“✗ 红色叉号”状态表示端口流控功能未启用或端口当前未发生流控，“绿色对号”状态表示端口流控正在生效）；

提示：“电口”可开启端口流控，同步接收端和发送端的速度，防止因速率不一致导致的网络丢包。

- 最大帧大小：可配置端口传输最大单元，范围在 1518-10056 字节之间，默认配为 10056，适用于使用端口；

- 冲突模式：当端口检测到冲突以后，可选择“Discard”或“restart”动作，“discard”表示丢弃报文；“restart”表示重启端口。默认 Discard，只适用于千兆端口。

| 端口配置 | | | | | | | | | |
|------|----|------|------|----|------------|------------|----|-------|---------|
| 端口 | 连接 | 速率 | | 模式 | 流控 | | | 最大帧长度 | 冲突模式 |
| | | 当前 | 配置 | | Current Rx | Current Tx | 配置 | | |
| * | | | <> | | | | | 10056 | <> |
| 1 | ● | Down | Auto | | × | × | | 10056 | Restart |
| 2 | ● | Down | Auto | | × | × | | 10056 | Discard |
| 3 | ● | Down | Auto | | × | × | | 10056 | Discard |

| 端口配置 | | | | | | | | | |
|------|----|------|-----------|----|------------|------------|----|-------|---------|
| 端口 | 连接 | 速率 | | 模式 | 流控 | | | 最大帧长度 | 冲突模式 |
| | | 当前 | 配置 | | Current Rx | Current Tx | 配置 | | |
| * | | | 1Gbps FDX | | | | | 10000 | Restart |
| 1 | ● | Down | 1Gbps FDX | | × | × | | 10000 | Restart |
| 2 | ● | Down | 1Gbps FDX | | × | × | | 10000 | Restart |
| 3 | ● | Down | 1Gbps FDX | | × | × | | 10000 | Restart |

提示：端口速率配置、流控配置、最大帧大小配置、冲突模式配置，可进行批量配置，如下图，在*行可实现对应批量配置，在配置端口速率时，请谨慎操作。

4.2 端口隔离

端口隔离功能，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，即可实现隔离组内端口之间二层数据通信的隔离。端口隔离功能为用户提供了更安全、更灵活、更便捷的组网方案。

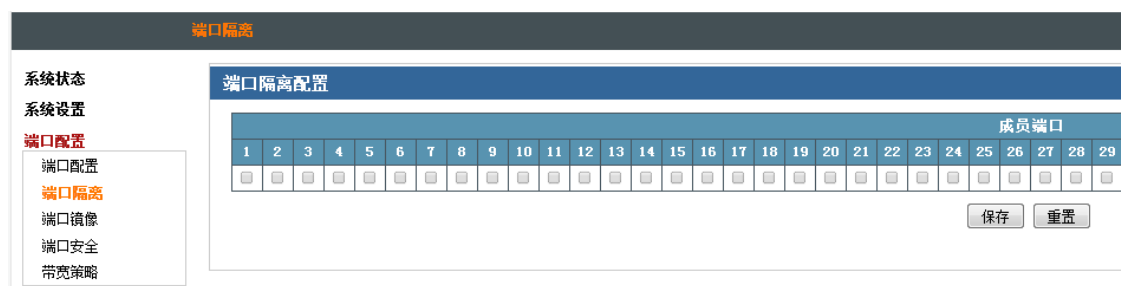


图 4-1 端口隔离配置页面

图为交换机端口隔离配置页面，这里可以实现属于同一 vlan 的端口在二层隔离。

提示：该页面底部有水平滚动条，滑动滚动条可以看到后面的所有端口。

配置举例：1-6 口属于 vlan2，需要实现 1、2、3 口之间的两两隔离，但 1-3 端口与 4-6 端口能正常通信。配置如下：

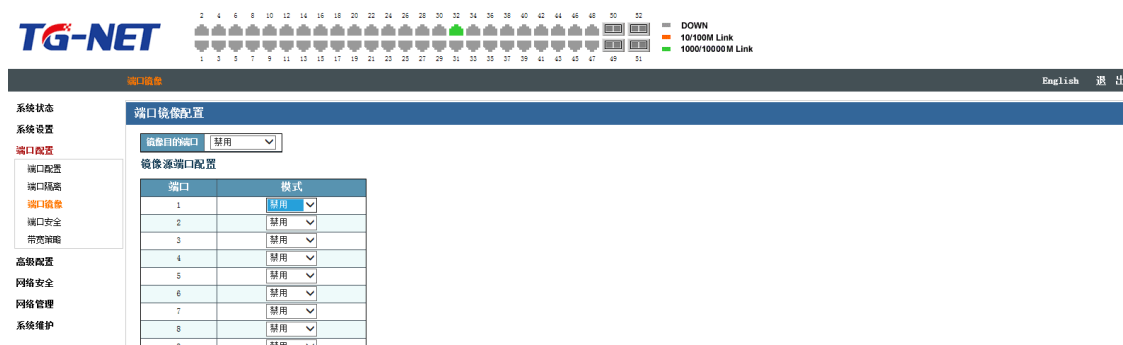


在端口隔离配置页面，1、2、3 口对应的勾选框，进行勾选，保存，即实现 1、2、3 端口两两之间通信隔离。此时 4-6 端口与 1-3 任意端口的通信正常，不会隔离。

4.3 端口镜像

端口镜像也叫端口监控。端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（镜像源端口）的数据包复制到一个特定的端口（镜像目的端口），在镜像目的端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

本页对端口镜像进行配置，包括以下设置（如下图）

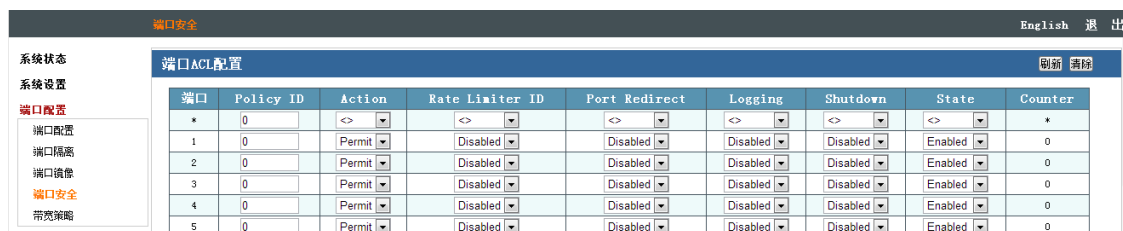


- 镜像目的端口：监控端口，只能选择一个，默认禁用；
- 镜像源端口-端口：被监控口，可以选择一个或者多个；
- 镜像源端口-模式：禁用、Tx only、Rx only、使能四个模式

| 模式 | 含义 |
|---------|-----------|
| 禁用（默认） | 未开启被监控功能 |
| Tx only | 输出监控 |
| Rx only | 输入监控 |
| 使能 | 输入/输出都受监控 |

4.4 端口安全

在端口安全页面可配置基于端口的 ACL 策略，，用户可指定一些 ACL 策略来防范网络威胁。主要关联的参数有策略 Action、带宽限制策略、Port Redirect（端口重定向）、Logging 功能、端口 Shutdown、State 和 Counter。



如图，端口安全页面可配置每个端口的安全策略，ACL 策略参数介绍如下：

- 端口：显示端口列表；
- Policy ID：策略 ID，默认 0，合法值范围 0-255，【网络安全—ACL 配置】页面会调

用策略 ID;

- Action: 默认 Permit, 可选项有 Permit、Deny, 分别表示端口 ACL 策略的允许、禁止转发指定类型数据包;
- Policy ID: 策略 ID, 这里直接调用【带宽策略】页面的 ACL Rate Limiter ID 即可, 默认值为 0;
- Port Redirect: 端口重定向, 默认 Disabled, 可选项有 Disabled、Enabled, 可选择复制其他端口流量或禁止复制功能;
- Logging: 日志功能, 默认 Disabled, 可选项有 Disabled、Enabled, 分别表示开启、关闭日志功能;
- Shutdown: 关闭功能, 默认 Disabled, 可选项有 Disabled、Enabled, 分别表示对端口启用、禁用操作;
- State: 显示状态, 默认 Enabled, 可选项有 Disabled、Enabled, 分别表示状态显示使能、关闭;
- Counter: 显示 ACL 策略报文统计。

4.5 带宽策略

带宽策略功能是配置 ACL 的带宽策略, 限制符合 ACL 规则的报文转发速率。

| 带宽策略 | |
|-----------------|------------|
| 系统状态 | ACL带宽策略配置 |
| 系统设置 | |
| 端口配置 | |
| 端口配置 | |
| 端口隔离 | |
| 端口镜像 | |
| 端口安全 | |
| 带宽策略 | |
| Rate Limiter ID | Rate (pps) |
| * | 0 |
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |

如图, 带宽策略页面, 【带宽策略】可配置 16 条宽带策略, Rate Limiter ID 会对应 Rate 范围, Rate 合法值范围 0-131071pps, 默认值为 1。

带宽策略在【端口安全】页面, 配置端口 ACL 策略会调用 ACL Rate Limiter ID, 实现 ACL 策略的速率限制。

第5章 高级配置

高级配置菜单下，包括链路聚合、VLAN 管理、VCL、DHCP 侦听、DHCP 服务器、DHCP 中继、IGMP 侦听、MVR 配置、路由配置功能菜单项。

高级配置

链路聚合

VLAN管理

VCL

DHCP侦听

DHCP服务器

DHCP中继

IGMP侦听

MVR配置

路由配置

5.1 链路聚合

链路聚合是将交换机的多个物理端口形成一个逻辑端口，属于同一汇聚组内的多条链路可视为一条更大带宽逻辑链路。

链路聚合可以实现通信流量在聚合组中各个成员端口之间分担，以增加带宽。同时，同一聚合组的各个成员端口之间彼此动态备份，提高了链路的可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、VLAN、端口属性、MAC 地址学习、ERPS 配置、loop Protect 配置、镜像、802.1x、IP 过滤、Mac 过滤、端口隔离等。

提示：不建议用于链路汇聚的端口，进行端口及高级功能方面的配置。

链路聚合分为静态聚合和动态聚合（LACP），与交换机链路聚合的对端设备一般是交换机、网卡。

5.1.1 静态聚合

静态聚合，需用户手动配置，不允许系统自动添加或删除聚合组中的端口，静态聚合配置逻辑简单，易于理解和使用。

静态聚合 LACP配置

系统状态

系统设置

端口配置

高级配置

链路聚合

VLAN管理

VCL

DHCP监听

DHCP服务器

DHCP中继

IGMP监听

聚合模式配置

负载均衡模式 IP Address

聚合组配置

| Group ID | 端口成员 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| Normal | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

如图，静态聚合配置页面，可以看到主要包括负载均衡模式、聚合组、端口成员三部分。

提示：该页面底部有水平滚动条，滑动滚动条可以看到后面的所有端口。

- 负载均衡模式

端口汇聚共有 5 种负载均衡算法，如下表：

| 负载均衡模式 | 说明 |
|-------------------------|------------------------------|
| IP Address（默认模式） | 将报文的源 IP 地址和目的 IP 地址进行负载均衡计算 |
| Source MAC Address | 基于报文的源 MAC 地址进行负载均衡计算 |
| Destination MAC Address | 基于报文的源 MAC 地址进行负载均衡计算 |
| SMAC&DMAC Address | 基于报文的源和目的 MAC 地址进行负载均衡计算 |
| TCP/UDP Port Number | 基于报文的 TCP/UDP 端口号进行负载均衡计算 |

- 聚合组

聚合组是一组以太网端口的集合，S5300 系列交换机，默认支持的聚合组数为实际端口总数/2，默认创建了所有聚合组，端口成员默认为空。

- 端口成员

交换机默认创建了所有聚合组，端口成员为空，要为聚合组配置成员端口，点选端口到对应的聚合组，即可实现端口加入汇聚组。

特别提示：

- （1）同一端口静态汇聚不能与动态 LACP 汇聚同时配置；
- （2）聚合组成员端口请保持配置方面的一致性；
- （3）聚合组成员端口数目为 2-8 个，建议使用偶数个端口加入汇聚组。

配置举例：将交换机 49-50 口加入汇聚组 1，将 45-48 口加入汇聚组 2，负载均衡算法配为 SMAC&DMAC Address。配置如下：

静态汇聚页面，点选 49-50 口加入汇聚组 1，点选 45-48 口加入汇聚组 2，保存。配置参考结果如下图：

聚合模式配置

负载均衡模式 SMAC & DMAC

聚合组配置

| Group ID | 端口成员 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----|----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 |
| Normal | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |

5.1.2 LCAP 配置

LACP (Link Aggregation Control Protocol, 链路汇聚控制协议) 是基于 IEEE 802.3ad 标准用来实现链路动态汇聚与拆汇聚的协议。汇聚设备双方通过 LACPDU 报文交互汇聚信息, 将匹配的链路汇聚在一起收发数据, 汇聚组内端口的添加和删除是协议自动完成的, 具有很高的灵活性并提供了负载均衡的能力。

启用端口的 LACP 功能后, 该端口向对端通告本端的系统优先级、系统 MAC、端口优先级、端口号和操作 Key (由端口的物理属性、上层协议信息和管理 Key 决定)。

设备优先级高的一端将主导汇聚及拆汇聚, 设备优先级由系统优先级和系统 MAC 决定, 系统优先级值小的设备优先级高, 系统优先级值相同时系统 MAC 较小的设备优先级高。设备优先级高的一端将根据端口优先级、端口号以及操作 Key 选择汇聚端口, 操作 Key 相同的端口才能被选入同一个汇聚组, 同一个汇聚组内端口优先级值小的端口会被优先选择, 当端口优先级相同的时候, 端口号小的会被优先选择。双方交互汇聚信息后被选择的端口将汇聚在一起收发数据。

| 端口 | LACP Enabled | 键值 | 角色 | 超时 | 优先级 |
|----|-------------------------------------|------|--------|------|-------|
| * | <input type="checkbox"/> | <> | <> | <> | 32768 |
| 1 | <input checked="" type="checkbox"/> | Auto | Active | Fast | 32768 |
| 2 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 3 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |

LACP 协议的配置参数主要包括: 端口 LACP 功能使能、键值、端口角色 (主动/被动模式)、超时配置、端口优先级。

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。密钥是协商的基础, 具有相同密钥的端口才能协商组成一个汇聚链路。协商模式 “active|passive”, 当选择 “active”, 设备会主动发起汇聚协商; 当选择 “passive”, 设备被动接受其他设备发起的汇聚协商。两台设备互联, 至少有一端或两端需设置成 “active” 模式才能协商成功。

- 端口: 显示交换机端口号;
- LACP Enabled: 勾选端表示使能端口 LACP 功能, 不勾选则为未使能;
- 键值: 同一汇聚组的成员, 需配置相同的管理 Key, 键值可以选择 auto 和 Specific (需手动配置, 允许值范围 1-65535);
- 角色: 默认 Active 可选项为 Active 和 Passive, 参与动态汇聚的设备一端要选配 Active 模式, 另一端要配置 Passive 模式;
- 超时: 默认 Fast, 可选项为 Fast 和 Slow, 分别表示快超时和慢超时;
- 端口优先级: 默认值 32768, 该值决定了成为汇聚组成员的端口的优先级。端口优先级值小的端口会被选为动态汇聚组成员;

配置举例: 将 S5300-52G-4TF 的 49-50 口使能动态汇聚功能, 键值 auto, 角色 Active, 其它默认; 将 S5300-32F-4TF 的 25-26 口使能动态汇聚功能, 键值 Specific 168, 角色 Passive, 使。配置如下:

S5300-52G-4TF LACP 配置页面, 点选 49-50 口 LACP 功能使能, 键值 auto, 角色 Active,

其它默认，保存；S5300-32F-4TF LACP 配置页面，点选 25-26 口 LACP 功能使能，键值 specific，角色 Passive，其它默认；保存。

5.2 VLAN 管理

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问）技术的共享通讯介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域，当网络中主机数目较多时会导致冲突严重，广播泛滥、性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN。处于同一 VLAN 的主机能直接互通，而处于不同 VLAN 的主机则不能直接互通。这样，广播报文被限制在同一个 VLAN 内，即每个 VLAN 是一个广播域。

本页对 VLAN 进行配置，包括以下配置（如下图）：

- 模式：Access、Trunk、Hybrid 三种模式。

| 模式 | 含义 |
|--------|---|
| Access | 端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。一般用于和不能识别 VLAN Tag 的用户终端设备相连，或者不需要区分不同 VLAN 成员时使用。 |
| Trunk | 端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。通常用于网络传输设备之间的互连。 |
| Hybrid | 端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。Hybrid 类型端口既可以用于网络传输设备之间的互连，又可以直接连接终端设备。 |

- 端口默认 VLAN：端口缺省 VLAN，即端口 PVID。Access 端口的缺省 VLAN 就

是它所在的 VLAN；Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，能够配置缺省 VLAN。

- 端口类型：C-Port、Unaware、S-Port、S-Custom-Port。一般情况默认 C-port，无非必要，请勿修改端口类型。
- Egress Tagging：设置端口是否加 Tag，Access 端口不加 Tag，Trunk 端口一般加 Tag。
- Allowed VLANs：设置端口的所属 VLAN。如设置 1-3 或者 1,2,3，说明端口属于 VLAN1-3。

VLAN 状态页面可以查看端口当前所属 VLAN 的信息。

配置举例：端口 1-3 属于 VLAN2，端口 4-6 属于 VLAN3，配置如下：

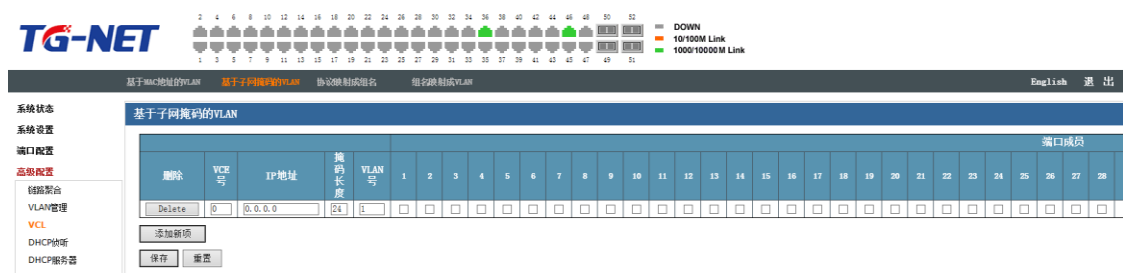
5.3 VCL

5.3.1 基于 MAC 地址的 VLAN

图为交换机基于 MAC 地址的 Vlan 配置界面。【VCL】是根据 MAC 地址划分交换机

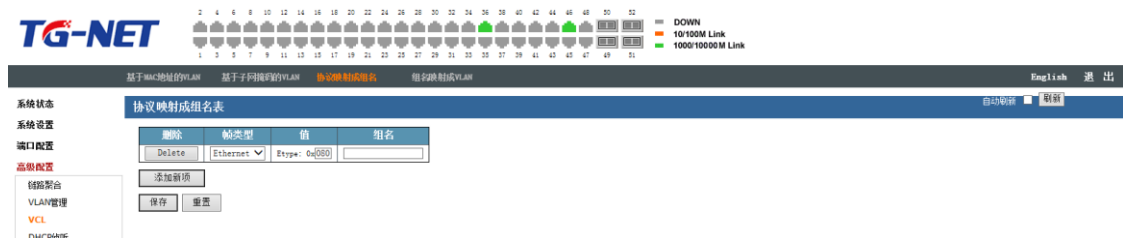
VLAN，并将交换机的端口划入 Vlan 中。

5.3.2 基于子网掩码的 VLAN



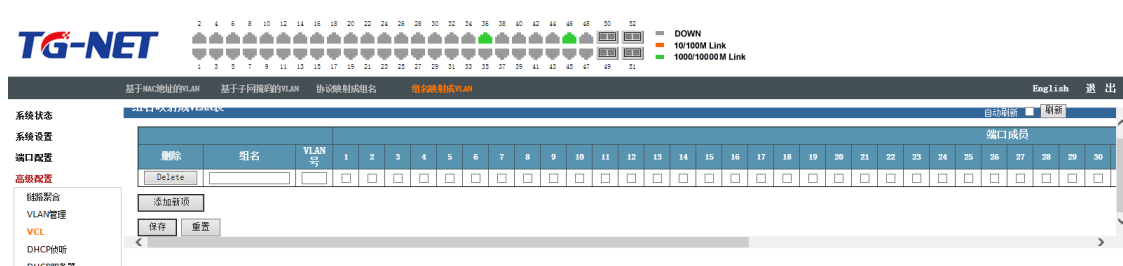
图为交换机基于子网掩码的 Vlan 配置界面。根据 IP 地址的掩码划分交换机 VLAN，并将交换机的端口划入 Vlan 中。

5.3.3 协议映射成组名



图为交换机基于网络协议的 Vlan 配置界面。将网络的协议如：Ethernet、SNAP、LLC

5.3.4 组名映射成 VLAN



将上节中定义的协议组名称，映射成 Vlan，按照协议划分 Vlan，并将各种端口加入到 Vlan 中。

5.4 DHCP 侦听配置

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

1. 保证客户端从合法的服务器获取 IP 地址

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 DHCP 客户端获取到错误的 IP 地址和网络配置参数，从而无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服

务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

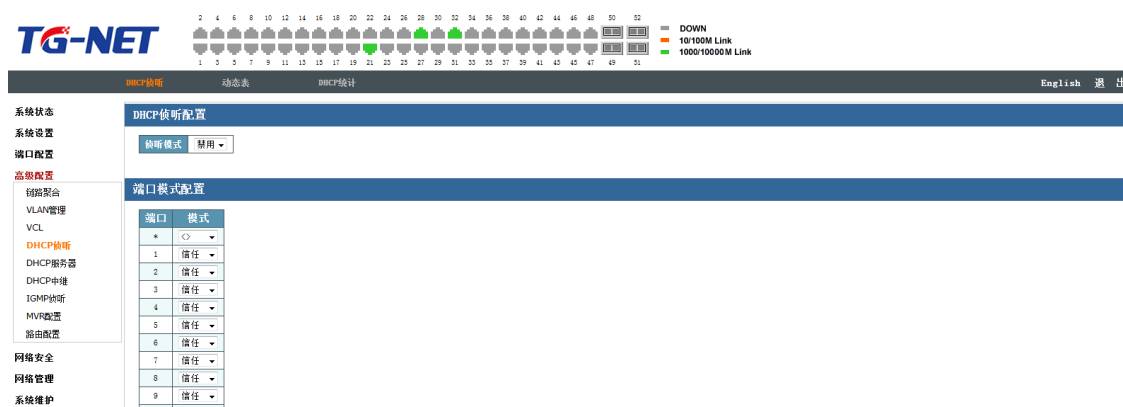
- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

在 DHCP Snooping 设备上指向 DHCP 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2. 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系

DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现：

- ARP Detection（ARP 检测）：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。
- IP Source Guard（IP 源保护）：通过动态获取 DHCP Snooping 表项对端口转发的报文进行过滤，防止非法报文通过该端口。



图为 DHCP Snooping 配置界面。进入此页面可以开启全局的 DHCP Snooping 功能，并限定端口接收“信任”或“不信任”区域的信息。

- 侦听模式：禁用/使能；“禁用”表示功能未开启，“使能”表示功能开启；
- 端口模式配置：信任/非信任；

| 端口模式 | 含义 |
|--------|--|
| 信任（默认） | 端口正常转发接收到的 DHCP 报文 |
| 非信任 | 端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。 |

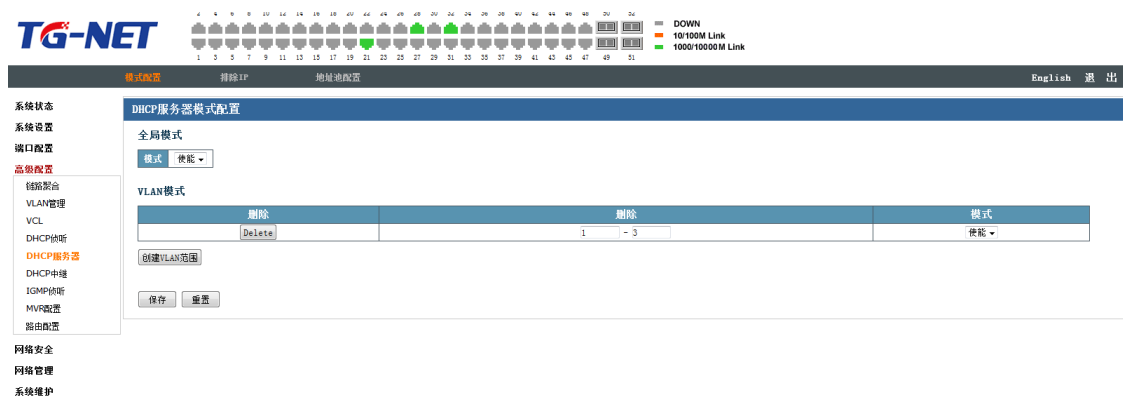
5.5 DHCP 服务器

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
 - 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。例如，Internet 接入服务提供商限制同时接入网络的用户数目，用户必须动态获得自己的 IP 地址。
 - 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。
- DHCP 服务器的配置分为三部分：模式配置、排除 IP、地址池配置。

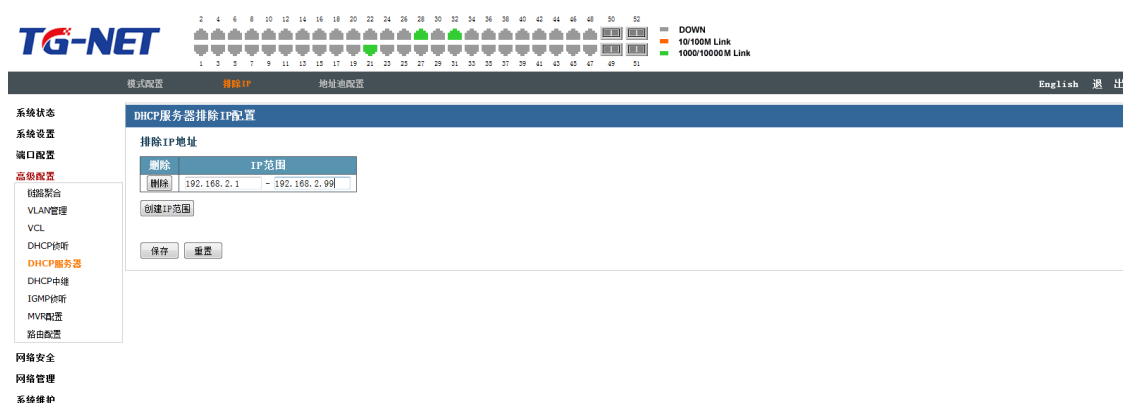
5.5.1 DHCP 模式配置

本页对 DHCP 模式进行配置，包括以下配置（如下图）：



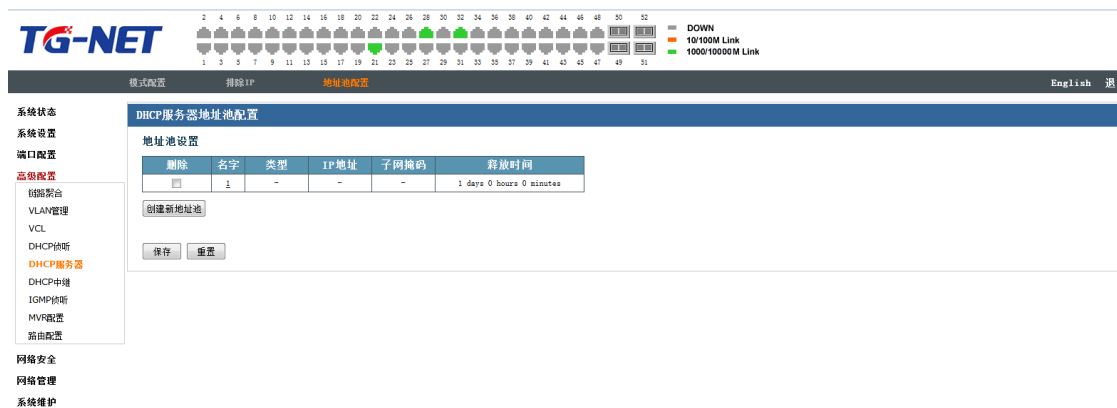
- 全局模式：即全局开关，使能或者禁用此功能。
- VLAN 模式：添加开启 DHCP 服务器的 VLAN。

5.5.2 排除 IP 配置

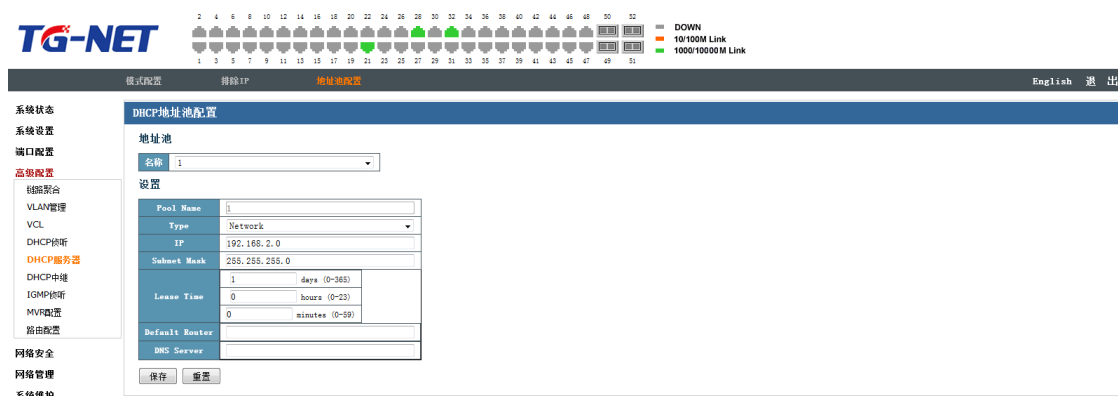


- 排除 IP 地址：创建排除 IP 范围，这部分 IP 不用于客户端自动获取 IP 中。特别注意排除 VLAN 接口 IP，否则可能导致客户端获取不到 IP。

5.5.3 地址池配置

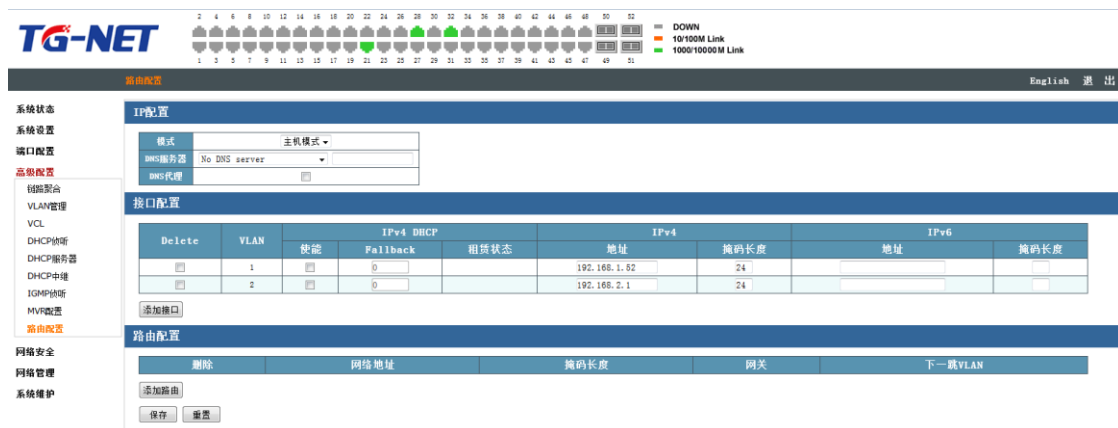


- 地址池设置：先创建一个地址池名字，地址池名字保存在列表后，点开列表名字对地址池进行配置。



5.5.4 VLAN 接口配置

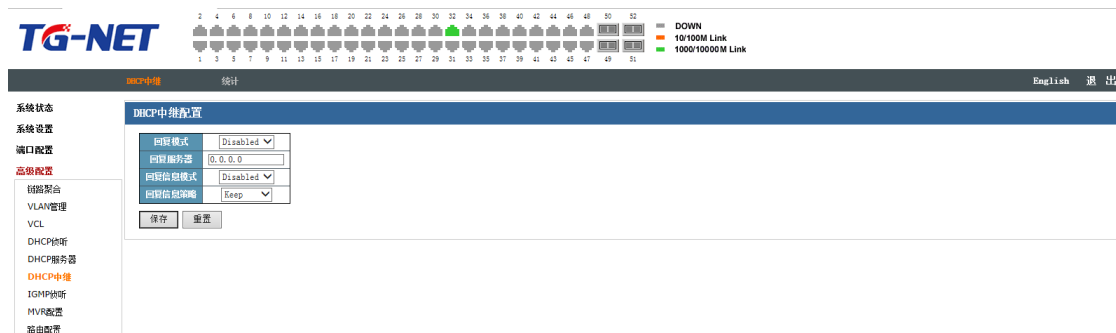
需要在“路由配置”界面，配置 VLAN 的接口 IP。



IP 配置下，模式选择主机模式；接口配置下，配置相应 VLAN 的接口 IP。

5.6 DHCP 中继

由于在 IP 地址动态获取过程中采用广播方式发送请求报文，因此 DHCP 只适用于 DHCP 客户端和服务端处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。DHCP 中继功能的引入解决了这一难题：客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，最终获取到 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

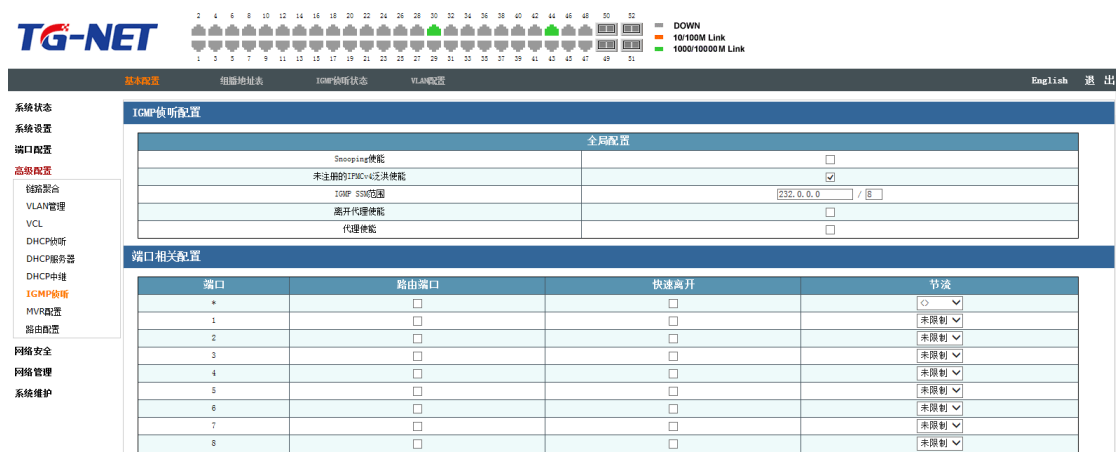


如果 DHCP 客户机与 DHCP 服务器在同一个物理网段，则客户机可以正确地获得动态分配的 ip 地址。如果不在同一个物理网段，则需要 DHCP Relay Agent(中继代理)。

5.7 IGMP Snooping 配置

IGMP Snooping 是 Internet Group Management Protocol Snooping(互联网组管理协议窥探)的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。

5.7.1 IGMP Snooping 基本配置



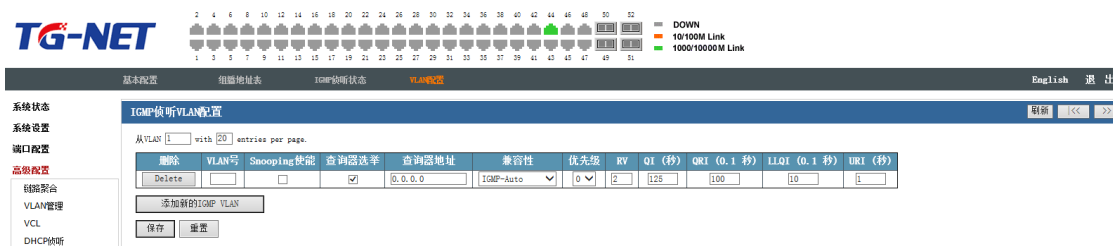
IGMP 侦听配置：

- Snooping 使能：全局开关，勾选表示开启该功能，默认不开；
- 未注册的 IPMCv4 泛洪使能：勾选表示开启
- IGMP SSM 范围：设置组播地址范围；

端口相关配置：

- 路由器端口：交换机上朝向三层组播设备（DR 或 IGMP 查询器）一侧的端口。
交换机将本设备上的所有路由器端口都记录在路由器端口列表中。
- 快速离开：勾选表示“快速离开”开启，默认不勾选；
- 节流：默认未限制，有 1-10 限制选项。

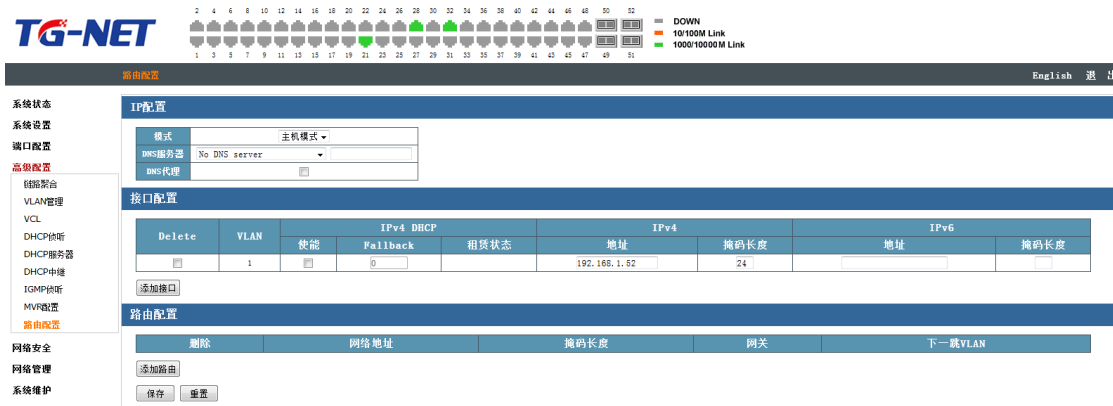
5.7.2 IGMP Snooping VLAN 配置



图中显示是组播 Vlan 配置页面，此页面可以将组播地址进行划分 Vlan；

5.8 路由配置

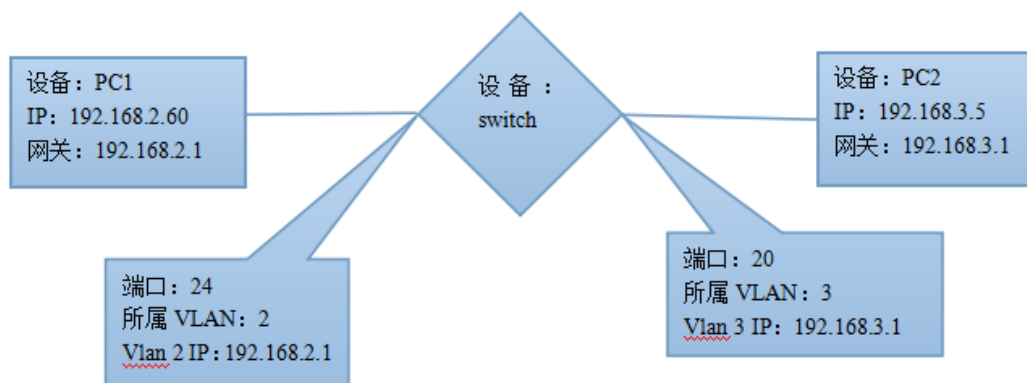
本页对静态路由进行配置，包括以下配置（如下图）：



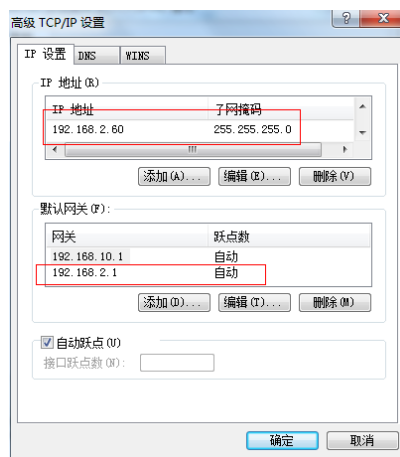
- 接口配置：此处是根据交换机三层路由原理，对每个 Vlan 建立虚接口，从而设置每个 Vlan 的三层地址信息；
- 路由配置：此处设置交换机路由功能配置，点击“添加路由”，在“网络地址”项填入设置交换机三层路由地址；“掩码长度”、“网关”项根据三层路由地址信息填入相应数值；“下一跳 Vlan”项和【接口配置】Vlan 关系是相互对应。
- 配置实例

同一交换机不同 VLAN 之间实现的通信，配置如下：

Step1: 组网拓扑图，如下图；



Step2: PC 参数的配置, PC1 配置如图示:



PC2 配置与 PC1 类似。

Step3: 交换机上 VLAN 配置 (高级设置-VLAN 管理), 如图示:

| | VLAN配置 | VLAN状态 | VLAN端口状态 | | | | | |
|---------|--------|--------|----------|--------|-------------------------------------|---------------------|-----------------|---|
| 系统状态 | 6 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| 系统设置 | 7 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| 端口配置 | 8 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| 高级配置 | 9 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| 链路聚合 | 10 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| VLAN管理 | 11 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| VCL | 12 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| VLAN转换 | 13 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| MAC地址表 | 14 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| DHCP服务器 | 15 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| DHCP中继 | 16 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| IGMP监听 | 17 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| MLD监听 | 18 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| MVR配置 | 19 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| UPnP配置 | 20 | Access | 2 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 2 |
| 网络管理 | 21 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| 网络安全 | 22 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| 系统维护 | 23 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| | 24 | Access | 3 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 3 |
| | 25 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |
| | 26 | Hybrid | 1 | C-Port | | Tagged and Untagged | Untag Port VLAN | 1 |

Step4: 静态路由的配置 (系统设置-路由配置);

- ①IP 配置里面的“主机模式”配置成“路由模式”;
- ②接口配置里面添加 Vlan 2 的 IP 为 192.168.2.1, 掩码长度为 24

添加 Vlan 3 的 IP 为 192.168.3.1，掩码长度为 24。

配置如图所示：

路由配置

系统状态

系统设置

IP配置

路由配置

日志配置

用户配置

NTP配置

端口配置

高级配置

网络管理

网络安全

系统维护

IP配置

模式 路由模式

DNS服务器 No DNS server

DNS代理 ☐

接口配置

| Delete | VLAN | IPv4 DHCP | IPv4 | IPv6 | | |
|--------------------------|------|--------------------------|----------|----------------|------|----|
| | | 使能 | Fallback | 地址 | 掩码长度 | 地址 |
| <input type="checkbox"/> | 1 | <input type="checkbox"/> | 0 | 192.168.200.51 | 24 | |
| <input type="checkbox"/> | 2 | <input type="checkbox"/> | 0 | 192.168.2.1 | 24 | |
| <input type="checkbox"/> | 3 | <input type="checkbox"/> | 0 | 192.168.3.1 | 24 | |

添加接口

路由配置

| 删除 | 网络地址 | 掩码长度 | 网关 | 下一跳VLAN |
|----|------|------|----|---------|
|----|------|------|----|---------|

添加路由

第6章 网络安全

点开网络安全，您可以看到：

网络安全

MAC地址表

端口隔离

风暴抑制

IP源保护

ARP检测

ACL配置

STP配置

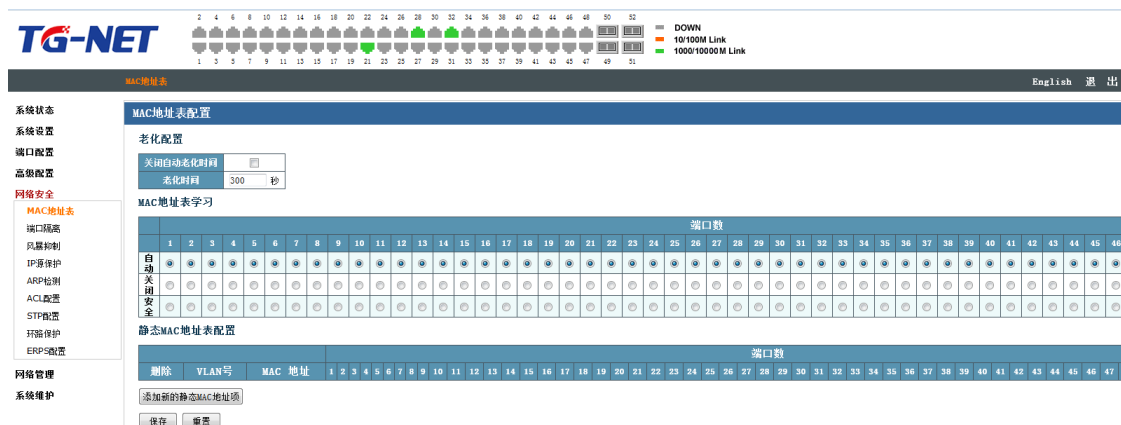
环路保护

ERPS配置

6.1 MAC 地址表

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果 MAC 地址表中包含与报文目的 MAC 地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

本页对 MAC 地址表进行配置，包括以下配置（如下图）：



- 老化配置：可以配置 MAC 地址表老化时间，可以关闭老化。

| 配置项 | 含义 |
|----------|-----------------|
| 关闭自动老化时间 | 勾选后表示关闭老化 |
| 老化时间 | 设置老化时间，默认 300 秒 |

● MAC 地址动态学习：

自动：自动学习动态 MAC 地址表；

关闭：禁止了动态 MAC 地址的自动学习功能，能够学习静态 MAC 地址，但对于端口接收和发送数据没有限制。

安全：禁止了 MAC 地址的自动学习功能，能够学习静态 MAC 地址，且只接收转发绑定了静态 MAC 的 PC 的数据，接收到的其它 PC 的数据都将被过滤丢弃，对于发送功能未做限制。

● 静态 MAC 地址表配置：配置静态地址表，表项不老化。

提示：静态 MAC 地址表项优先级高于自动生成的 MAC 地址表项。

6.2 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

本页对端口风暴进行配置，包括以下设置（如下图）

| 端口 | 单播报文 | | | 广播报文 | | | 未知单播报文 | | |
|----|--------------------------|-----|------|--------------------------|-----|------|--------------------------|-----|------|
| | 使能 | 速率 | 单位 | 使能 | 速率 | 单位 | 使能 | 速率 | 单位 |
| 0 | <input type="checkbox"/> | 500 | k | <input type="checkbox"/> | 500 | k | <input type="checkbox"/> | 500 | k |
| 1 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 2 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 3 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |

如图，端口风暴控制配置页面，可以看到主要包括端口、单播报文、广播报文、未知单播报文四部分。

- 端口：显示交换机端口号；
- 单播报文使能：勾选端表示使能端口风控制功能，不勾选则为未使能；
- 单播报文速率：单播报文速率默认值 500；
- 单播报文单位：单播报文单位为 kbps、mbps、fps、kfps,默认单位为 kbps
- 广播报文使能：勾选端表示使能端口风控制功能，不勾选则为未使能
- 广播报文速率：广播报文速率默认值 500；

- 广播报文单位：广播报文单位为 kbps、mbps、fps、kfps,默认单位为 kbps
- 未知单播报文使能：勾选端表示使能端口风控制功能，不勾选则为未使能
- 未知单播报文速率：未知单播报文速率默认值 500；
- 未知单播报文单位：未知单播报文单位为 kbps、mbps、fps、kfps,默认单位为 kbps

配置举例：将 1-2 口使能单播、广播、未知单播风暴使能，且单位设置为 100kbps。

配置如下：

风暴抑制页面，点选 1-2 口，速率改为 100，保存。配置参考结果如下图：



6.3 IP 源保护

IP 源保护主要是防止 IP 地址欺骗，以 DHCP 监听为基础，根据 DHCP 监听绑定表产生一个 IP 源绑定表，根据 IP 源绑定表 IP 源保护自动在端口加载相应的策略对流量进行检测，符合的数据允许发送，不符合的数据被丢弃。

对于使用固定 IP 地址的服务器，需要使用静态 IP 源绑定将静态绑定的条目加入到 IP 源绑定表中。IP 源保护只支持二层接口，包括接入接口或干道接口，对于非信任端口，IP 源防护有两种过滤策略：源 IP 地址过滤、源 IP 和源 MAC 地址过滤。

使用源 IP 地址过滤时，IP 源保护和端口安全是相互独立的。使用源 IP 和源 MAC 地址过滤时，二者合并为一，数据包源 IP 和源 MAC 地址必须符合 IP 源绑定表中的条目才能转发，并且为了确保 DHCP 工作正常，启用 DHCP 监听时必须启用选项 82。



如图，IP 源保护-全局配置页面。主要包含 IP 源保护配置和端口模式配置。

- IP 源保护配置一模式默认禁用，表示全局关闭 IP 源保护功能，可选项启用，表示全局启用 IP 源保护功能；
- 动态转静态一将 IP 源动态保护表转为静态表项；

- 端口模式配置-Port—显示端口号；
- 端口模式配置-Mode—配置端口的 IP 源保护功能启用、禁用，默认禁用；
- 端口模式配置-Max Dynamic Clients—端口最大动态客户端数配置，默认不限制，可选项有 0、1、2、不限制（配置为 0 则端口，客户端获取到 ip 后，无法访问内网资源）；

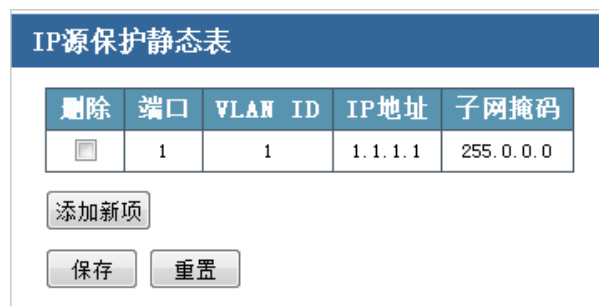


如图，IP 源保护-动态表页面。该页面显示端口的动态 IP 源保护动态表，为四元条目（端口+VLAN ID+IP 地址+MAC 地址），可基于初始端口、VLAN 号、IP 地址过滤查看动态表，可配置每页显示条目（最大值为 99）。



如图，IP 源保护-静态表项页面。该页面显示 IP 源保护静态表信息，静态表条目由“端口+VLAN ID+IP 地址+子网掩码”组成。

- 添加新项—可以手动添加一个 IP 源保护静态条目，选择端口、填写 VLAN ID、IP 地址、子网掩码，保存即可；



删除一个 IP 源保护静态条目，勾选相应条目行首的“删除”勾选框，保存即可。

提示：IP 源保护全局配置页面的“动态转静态”按钮可将 IP 源动态保护表中条目转为静态表项中的条目；

6.4 ARP 检测

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。

- 攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表项不正确，从而对网络进行攻击。
- 攻击者通过向设备发送大量目标 IP 地址不能解析的 IP 报文，使得设备试图反复地对目标 IP 地址进行解析，导致 CPU 负荷过重及网络流量过大。
- 攻击者向设备发送大量 ARP 报文，对设备的 CPU 形成冲击。

关于 ARP 攻击报文的特点以及 ARP 攻击类型的详细介绍，请参见“ARP 攻击防范技术白皮书”。目前 ARP 攻击和 ARP 病毒已经成为局域网安全的一大威胁，为了避免各种攻击带来的危害，设备提供了多种技术对攻击进行防范、检测 and 解决。

下面将详细介绍一下这些技术配置。

6.4.1 端口配置

| 端口 | 模式 | 检查VLAN | 日志类型 |
|----|----|--------|------|
| * | 禁用 | 禁用 | 无 |
| 1 | 禁用 | 禁用 | 无 |
| 2 | 禁用 | 禁用 | 无 |
| 3 | 禁用 | 禁用 | 无 |
| 4 | 禁用 | 禁用 | 无 |
| 5 | 禁用 | 禁用 | 无 |

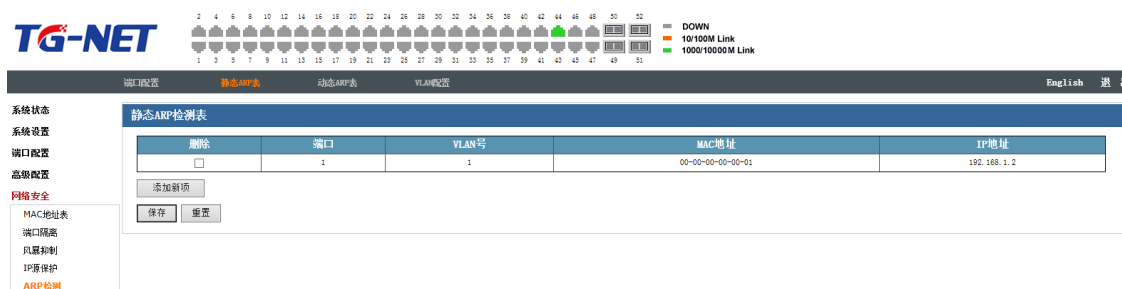
ARP 检测配置

- 模式：全局开关，“禁用”表示关闭功能，“使能”表示开启功能；
- 将动态转换为静态：点击此按钮，“动态 ARP 表”中的条目会转换成静态条目，显示在“静态 ARP 表”中；

端口模式配置

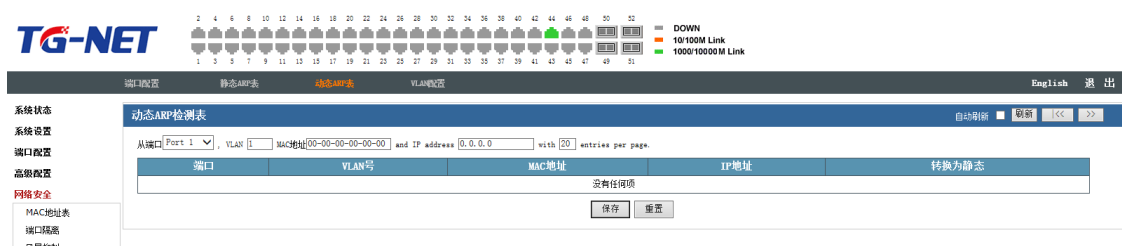
- 端口：对应端口号；
- 模式：“禁用”表示端口关闭该功能，“使能”表示开启该功能；
- 检查 VLAN：“禁用”表示端口开启检测 VLAN，“使能”表示端口关闭检测 VLAN；
- 日志类型：分为“无”、“拒绝”、“允许”、“全部”。

6.4.2 静态 ARP 表



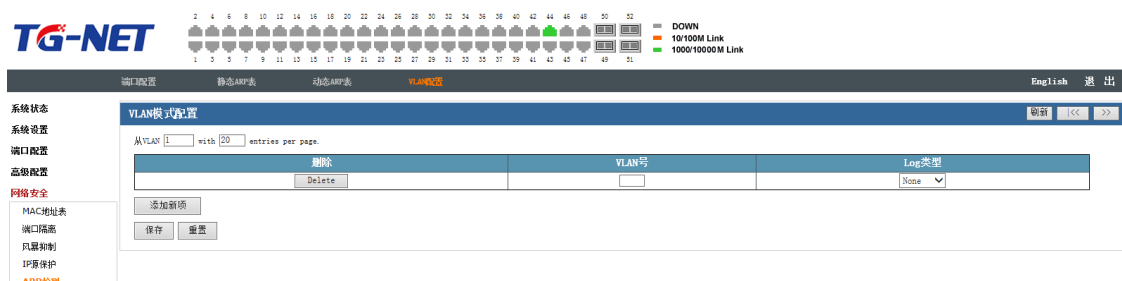
点击“添加新项”按钮，可以添加静态 ARP 条目。

6.4.3 动态 ARP 表



此页面可以查看设备当前动态 ARP 信息。

6.4.4 VLAN 配置



6.5 ACL 配置

ACL，Access Control List，访问控制列表。ACL 是通过配置对报文的匹配规则和处理操作来实现包过滤的功能，端口上应用的 ACL 规则对报文的字段进行分析，在识别出特定的报文之后，根据预先设定的操作（允许/禁止通过、限速、重定向、关闭端口等）来进行相应的处理。

ACL 配置会关联端口安全（端口 ACL 策略配置）和带宽策略（端口 ACL 带宽策略），ACE 条目按需调用 ACL 策略 ID 和带宽策略 ID。



如图，ACL 配置页面，ACE（Access Control Entry）条目主要参数项说明如下：

- ACE—显示 ACE ID，ACL 功能最大支持 512 条 ACE，默认从 1 开始顺序计数；
- 入端口—显示 ACE 条目的入方向端口信息，默认 ALL，可选项有 ALL、Port 号；



- 策略/位图—显示 ACE ID，ACL 功能最大支持 512 条 ACE，从 1 开始计数；
- 入端口—显示 ACE 条目的入方向端口信息，默认 ALL，可选项有 ALL、Port 号；
- 帧类型—显示 ACE 条目的帧类型；
- 行为—显示 ACE 条目转发动作，可选项有 Permit、Deny，Permit 表示匹配 ACE 条目的帧会转发并学习，Deny 表示匹配 ACE 条目的帧会被丢弃；
- 限制率—显示 ACE 条目的带宽限制策略号；
- Port Copy—显示 ACE 条目入端口的镜像操作，匹配 ACE 条目的帧会被镜像到目的端口；
- 端口重定向—显示 ACE 条目的端口重定向操作，符合 ACE 条目的帧会被重定向到指定端口；
- 计数—显示符合 ACE 条目的数据帧统计；
- 编辑—点击“加号”，可以进入新增 ACE 条目的配置页面；
- ACE 条目图标含义说明：

| ACL配置 | | | | | | | | | 自动刷新 | 刷新 | 清除 | 全部清除 |
|-------|--------|----------|-------|------|-----|-----------|-------|----|------|----|----|------|
| ACE | 入端口 | 策略/位图 | 帧类型 | 行为 | 限制率 | Port Copy | 端口重定向 | 计数 | | | | |
| 1 | Port 1 | 3 / 0x10 | EType | Deny | 1 | Port 2 | 0 | | | | | |

⊕:在当前行前新增一个 ACE 条目；

⊞:编辑当前 ACE 条目；

⬆:上移当前 ACE 条目；

⬇:下移当前 ACE 条目；

⊗:删除当前 ACE 条目;

⊕:点击最底部的加号, 会进入 ACE 配置页面, 配置保存后, 为新增一个 ACE 条目;

● ACE 配置页面按键说明:

| ACL配置 | | | | | | | | |
|-------|--------|----------|-------|--------|----------|-----------|-------|-----------------|
| | | | | | 自动刷新 | 刷新 | 清除 | 全部清除 |
| ACE | 入端口 | 策略/位图 | 帧类型 | 行为 | 限制率 | Port Copy | 端口重定向 | 计数 |
| 1 | Port 1 | 3 / 0x10 | EType | Deny | 1 | Port 2 | 0 | ⊕ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗ |
| 2 | Port 8 | Any | Any | Permit | Disabled | Disabled | 0 | ⊕ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗ ⊗ |

点击 ACE 条目的 ⊕ 或 ⊗ 图标可进入下图的 ACE 配置页面, ACE 配置主要包括入端口、过滤策略、帧类型配置, ACE 行为、关联动作配置, IP、MAC、VLAN 参数配置等。

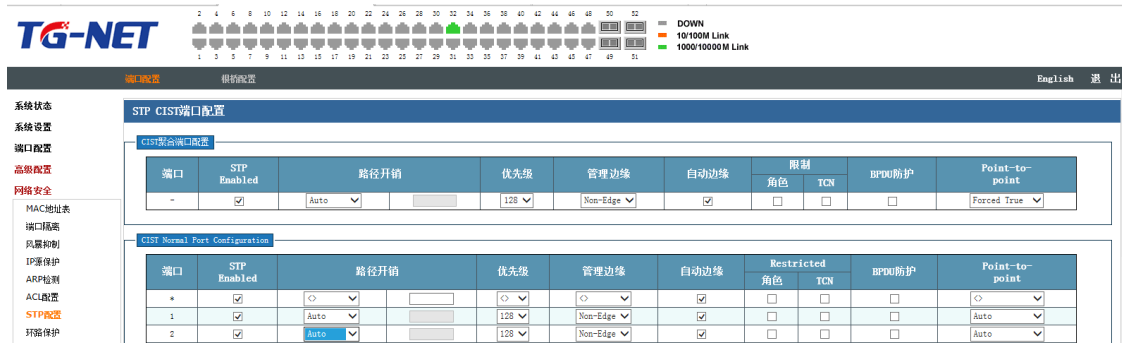
| ACE配置 | |
|--|---|
| <div>入端口 <input type="text" value="All"/></div> <div>过滤策略 <input type="text" value="Any"/></div> <div>帧类型 <input type="text" value="Any"/></div> | <div>行为 <input type="text" value="Permit"/></div> <div>限制率 <input type="text" value="Disabled"/></div> <div>日志 <input type="text" value="Disabled"/></div> <div>关闭 <input type="text" value="Disabled"/></div> <div>计数 <input type="text" value="0"/></div> |
| <div>MAC地址参数</div> <div>目的地址过滤 <input type="text" value="Any"/></div> | <div>VLAN参数</div> <div>VLAN号过滤 <input type="text" value="Any"/></div> <div>Tag优先级 <input type="text" value="Any"/></div> |
| <div>保存 重置 取消</div> | |

6.6 STP 配置

STP (Spanning Tree Protocol, 生成树协议) 是根据 IEEE 802.1D 标准建立的, 用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路, 并有选择的对某些端口进行阻塞, 最终将环路网络结构修剪成无环路的树型网络结构, 从而防止报文在环路网络中不断增生和无限循环。

6.6.1 Stp 端口配置

本页对 stp 端口进行配置, 包括以下设置 (如下图)



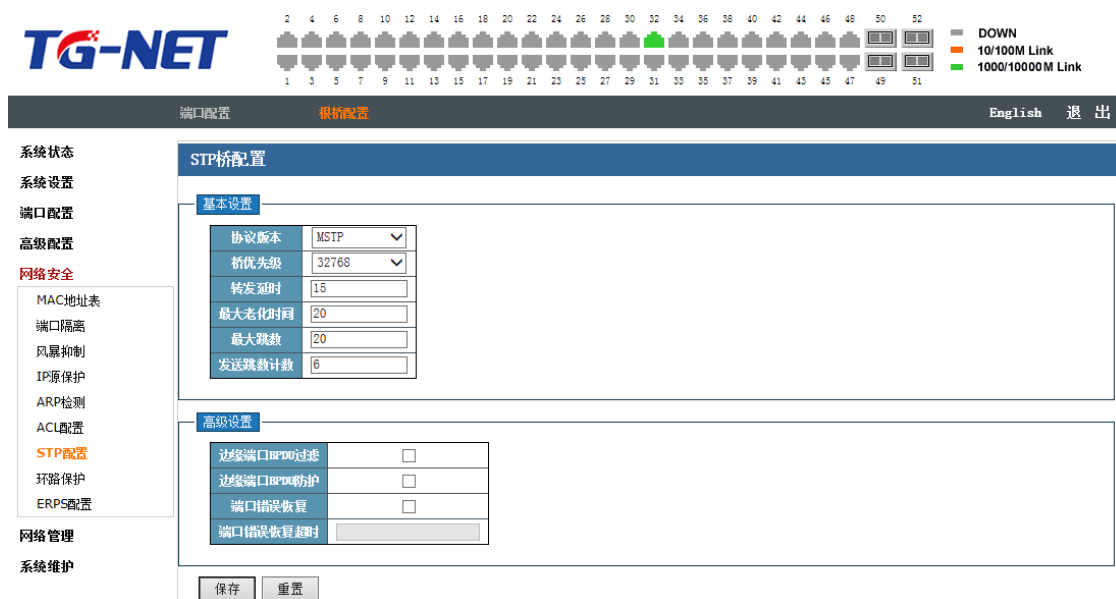
图表 6-7.1 stp 端口配置页面

如图 6-7.1，stp 端口配置页面，可以看到主要包括 cist 聚合端口和普通端口配置、端口、Stp enable、路径开销、优先级、管理边缘、自动边缘、restricted、bpdu 防护、point-to-point。

- 端口：显示交换机端口号；
- Stp enable：勾选端表示使能端口 stp 功能，不勾选则为未使能，缺省为开启
- 路径开销：STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构，auto 自动协商的，specific 手动设置，缺省为自动。
- 优先级：端口优先级改变时，STP 会重新计算端口的角色并进行状态迁移，端口的优先级的值只能是 16 的倍数，配置范围是 0-240,缺省配置 128
- bpdu 防护：bpdu guard 使具备边缘端口特性的端口在接收到 BPDU 时进入 err-disable 状态来避免桥接环路，bpdu filter 将能够防止交换机在启用了边缘端口特性的端口上发送 BPDU 给主机，缺省关闭。
- point-to-point：端口相连的链路类型，Force true：设置端口与一条点到点链路相连 Force false：设置端口与一条共享链路相连 Auto：设置端口自动建立链路，缺省端口自动建立链路

6.6.2 根桥配置

本页对跟桥进行配置，包括以下设置（如下图）



如图，stp 跟桥配置页面，可以看到主要 stp 跟桥基本配置：协议版本、桥优先级、转发延时、最大老化时间、最大跳数、发送跳数计数；高级配置：边缘端口 bpdu 过滤/防护、端口错误恢复/超时。

基本配置

- 协议版本：协议版本包括 mstp、rstp、stp 三个版本；
- 桥优先级：桥优先级的大小决定了本设备是否能够被选作生成树的树根，桥优先级范围为 0-61440，缺省情况下，桥优先级为 32768
- 转发延时：状态迁移的延迟时间，延时范围为 4-30，缺省情况下，延时时间为 15s
- 最大老化时间：用来判断配置消息在交换机内保存时间是否“过时”的参数，老化时间范围为 6-40s，缺省情况下，老化时间为 20s
- 最大跳数：决定 bpdu 的传递范围，跳数范围为 6-40，缺省情况下，跳数为 20

高级配置

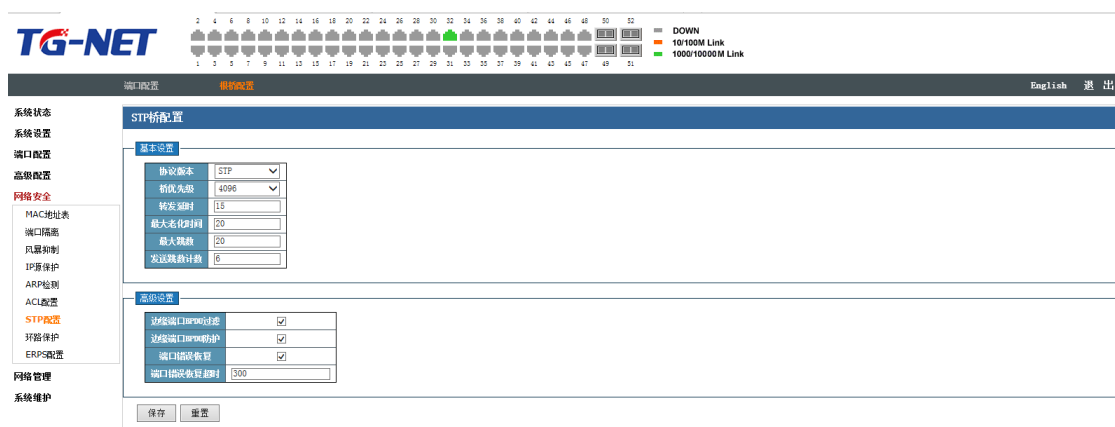
- 边缘端口 BPDU 过滤：bpdu 过滤将能够防止交换机在启用了边缘端口特性的端口上发送 BPDU 给主机，缺省关闭
- 边缘端口 BPDU 防护：bpdu 防护使具备边缘端口特性的端口在接收到 BPDU 时进入 err-disable 状态来避免桥接环路
- 端口错误恢复：对 err-disable 状态的端口开启恢复功能，勾选为开启，缺省不勾选为关闭。

端口错误恢复超时：超时时间后重新启动这个端口；

配置举例：设置协议版本为 stp，桥优先级为 4096，转发延时、最大老化时间、最大跳数、发送跳数计数为默认；边缘端口 bpdu 和防护开启，端口错误恢复开启，端口错误恢复时间设置为 300。

配置如下：点击协议版本下拉菜单选中 stp；点击桥优先级下拉菜单选中 4096；转发延时、最大老化时间、最大跳数、发送跳数计数为默认；勾选边缘端口 bpdu 和防护、端口恢复；在端口错误恢复框输入 300；最后点击保存。

配置参考结果如下图：



6.7 环路保护

环路保护功能功能方面类似 STP，但环路保护没有 IEEE 标准，属于私有协议，配置使用简单，对于简单的环网拓扑和普通网络业务，在线路备份方面的优势也很明显。



如图，环路保护页面，主要包括全局配置、端口使能和主检测模式配置三个部分。

- 全局配置—使能环路保护：默认 Disable，表示全局关闭，可选项 Enable，表示全局使能环路保护；
- 全局配置—发送时间：默认 30 毫秒，不可配；
- 端口—显示端口号；
- 使能—勾选框，选中表示开启端口的环路保护功能，不勾选则表示不开启端口环路保护功能；
- 行为—环网行为默认丢弃报文，不可配，表示环网协议阻塞的端口会丢弃报文；
- 主检测模式—默认 Disable，表示未开启主检测，可选项 Enable，表示开启主检测模式；开启主检测模式，表示端口可周期性发送环路探测包，探测网络上是否存在环路；

提示：STP、ERPS、Loop Protect 三个环网功能不能同时开启使用！参与组环的端口都必须启用全局、端口环路保护功能，且至少有一个端口要开启主检测模式。

配置举例：配置 S5300-52F-4TF 51-52 口开启环路保护，51 口启用主检测模式、52 口不启用主检测；S5300-52G-4TF 51-52 口开启环路保护，51-52 口不启用主检测模式；配置如下：

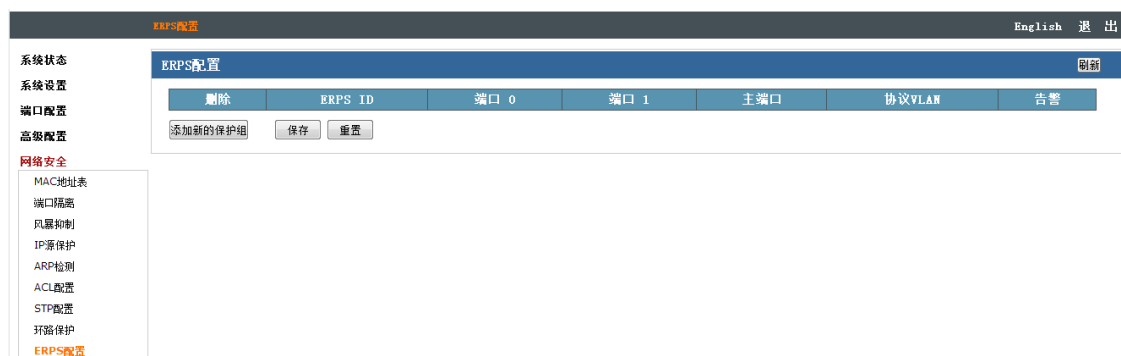
- (1) 检查 S5300-52F-4TF、S5300-52G-4TF，确认 51-52 口未启用 STP、ERPS 功能；
- (2) S5300-52F-4TF 环路保护页面，全局开启环路保护，51-52 端口开启环路保护，51 口启用主检测模式、52 口不启用主检测，保存即可；
- (3) S5300-52G-4TF 环路保护页面，全局开启环路保护，51-52 端口开启环路保护，51-52 口不启用主检测模式，保存即可；
- (4) 配置 OK 后，线路连接两设备的 51-52 口，组环成功，在系统信息-环路保护状态页面可以查看组环端口状态。

6.8 ERPS 配置

ERPS（Ethernet Ring Protection Switching）：以太网多环保护技术，协议标准为 ITU-TG.8032 多环标准。ERPS 追求更高性能、更加安全是网络永远的发展方向，以太环网技术成为二层网络中重要的冗余保护手段。

在二层网络中，对于网络可靠性一般采用 STP 协议，还有上节提到的环路保护协议，STP 协议是由 IEEE 开发的一种标准的环网保护协议，已得到广泛应用，但实际应用中受到网络大小的限制，收敛时间受网络拓扑影响。STP 一般收敛时间为秒级，网络直径较大时收敛时间更长，采用 RSTP/MSTP 虽然可以减少收敛时间，达到毫秒级，但是对于 3G/NGN 语音等高服务质量要求的业务仍然不能满足要求。为更大缩短收敛时间，消除网络尺寸的影响，ERPS 协议应运而生。

ERPS 是一个专门应用于以太网环的链路层协议，它在以太网环中能够防止数据环路引起的广播风暴；当以太网环上一条链路断开时，能迅速启用备份链路以恢复环网上各个节点之间的通信。和 STP 协议相比，ERPS 协议具有拓扑收敛速度快（低于 20ms）和收敛时间与环网上节点数无关的特点。环路保护功能功能方面类似 STP、erps，但环路保护没有 IEEE 标准，属于私有协议，配置使用简单，收敛时间也是秒级，对于简单的环网拓扑和普通网络业务，在线路备份方面的优势也很明显。



如图，ERPS 配置页面，可以实现配置 ERPS 组。

- ERPS ID——是一个 ERPS 域 ID 标识，添加环路保护组时，首条 ERPS 组的 ID 为 1，第二条的为 2，依次类推；

- 端口 0——参与组环的端口 1，可选项为所有端口；
- 端口 1——参与组环的端口 2；可选项为所有端口，不能与端口 0 所选端口重复；
- 主端口——默认 None，表示不配置主端口，可选项有 None、端口 0、端口 1。端口 0、端口 1 中可选其中一个端口作为主端口，选为主端口，则对应的实际端口会负责控制转发状态；
- 协议 VLAN——属于同一协议 VLAN 的 ERPS 组，才能组环，首个新增 ERPS 组，协议 VLAN 默认 3001，协议 VLAN 有效值范围 1-4095；
- 告警——显示 ERPS 状态，有红色、绿色两种状态，分别表示环网状态正常、异常；

配置举例 1—新增 ERPS 组：S5300-52G-4TF，新增 ERPS 组 1，端口 0、端口 1 分别选为 51、52 口，主端口为 51，协议 VLAN 3001。配置如下：

S5300-52G-4TF ERPS 配置页面，点击“添加环路保护组”，端口 0、端口 1 分别选为 51、52 口，主端口选 Port 0（即 51 口），协议 VLAN 默认 3001 即可，保存。

| ERPS配置 | | | | | | |
|--------------------------|---------|------|------|--------|--------|------------------------------------|
| 删除 | ERPS ID | 端口 0 | 端口 1 | 主端口 | 协议VLAN | 告警 |
| <input type="checkbox"/> | 1 | 51 | 52 | Port 0 | 3001 | ● |

提示：上例可以看出 1 个 erps 组中只有两个端口（51、52 口），主端口可选择 port 0、port 1 中的一个或都不选；

提示：ERPS、STP、Loop Protect 三个环网功能不能同时开启使用！端口要使用 ERPS 功能，要确认参与组环端口的 STP、Loop Protect 功能未启用。

配置举例 2—删除 ERPS 组：勾选指定的 ERPS ID 行首列的删除勾选框，保存即可。

配置举例 3—修改 ERPS 组：先是删除旧的 ERPS 组，添加新的 ERPS 组。

配置举例 4—ERPS 组环实例：三台 S5300-52G-4TF（编号为 DUT A、DUT B、DUT C）的 51、52 口组 ERPS 环。

【基本原则 1】组环网，请先配置，后连线；若需要修改环网配置，请先断环（即拔掉任一根线），再修改配置；

【基本原则 2】一个 ERPS 环中，所有 ERPS 组的协议 VLAN 要相同。

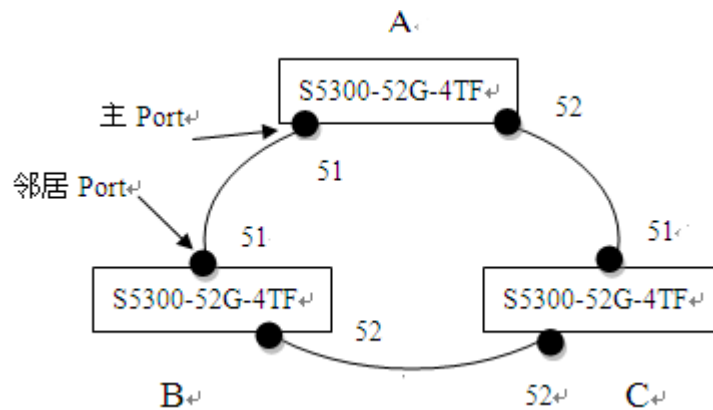
推荐配置方式：参与组环端口不配置主端口，配置快捷、方便，配置过程如下：

（1）确认 DUT A、B、C 的 51-52 口，STP、环路保护功能为开启（建议直接不启用 STP、环路保护功能）；

（2）DUT A 按照实例 1 配置即可，新增 ERPS 组 1，端口 0、端口 1 分别选择 51、52 口，协议 VLAN 默认 3001，保存即可，配置完成；

（3）物理接线，ERPS 环网组建成功，检查 ERPS 配置页面的告警指示灯，会变为绿色状态。

标准配置方式：环网标准配置和推荐配置方式的差异在于，标配方式可指定环网中处于阻塞的端口，推荐组环方式，协议会自动协商出阻塞端口，标准配置过程如下：



(1) 确认 DUT A、B、C 的 51-52 口，STP、环路保护功能为开启（建议直接不启用 STP、环路保护功能）；

(2) DUT A 按照实例 1 配置即可，DUT B、C，分别参考实例 1，新增 ERPS 组 1，端口 0、端口 1 分别选择 51、52 口，协议 VLAN 默认 3001，主端口 None，保存即可，配置完成；

(3) DUT B，51 口要配置为邻居端口（和主端口连接的对端设备的端口要配置为主端口），点击 ERPS ID，可进入 ERPS 详细配置页面，在 RPL 配置栏，RPL 角色选择 RPL_Neighbour，RPL 端口选择 Port 0，保存，配置完成，其他配置默认即可。

ERPS配置

系统状态

系统设置

端口配置

高级配置

网络安全

MAC地址表

端口隔离

风暴抑制

IP源保护

ARP检测

ACL配置

STP配置

环路保护

ERPS配置

网络管理

系统维护

ERPS配置

ERPS参数

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | 环类型 |
|---------|--------|--------|---------------|---------------|----------------|----------------|------------|
| 1 | 1 | 2 | 1 | 2 | 1 | 2 | Major Ring |

ERPS配置

状态 ●

警戒时间

WTR时间

持续时间

版本

倒换 ☒

VLAN配置

RPL配置

| | | |
|--|------------------------------------|--------------------------|
| RPL角色 | RPL端口 | 清除 |
| <input type="text" value="RPL_Neighbour"/> | <input type="text" value="Port0"/> | <input type="checkbox"/> |

ERPS命令

命令

端口

提示：这里配置邻居端口的方法也适合与配置主端口，如开始创建 ERPS 组未指定主端口，可以在这里 RPL 配置栏配置，如果已配置了主端口或邻居端口，需要修改配置，则要先清除原有配置，在重新配置即可。删除原有 RPL 配置，勾选 RPL 配置栏的清除可选框，保存即可。

(4) 物理接线，ERPS 环网组建成功，检查 ERPS 配置页面的告警指示灯，会变为绿色状态，在 ERPS 详细配置页面最底端可查看 ERPS 状态，会看到整个参与组环的 6 个端口中，DUTA 的 51 口、DUTB 的 51 口处于 Blocked 状态。

第7章 网络管理

点开网络管理，您可以看到：

网络管理

SSH配置

HTTPS配置

LLDP配置

802.1X配置

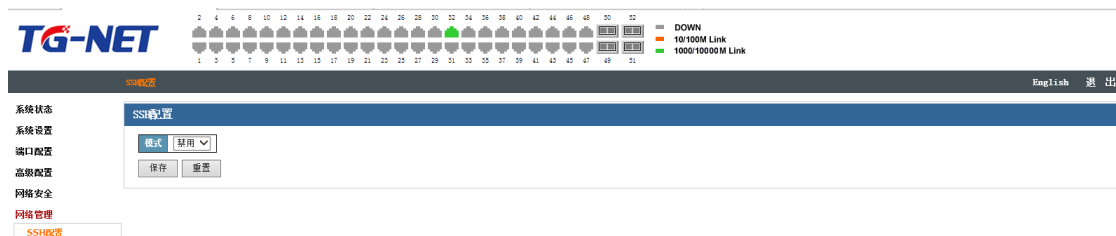
SNMP配置

RMON配置

7.1 SSH 配置

SSH 加密连接所提供的功能类似于一个 telnet 连接，但是传统的 telnet 远程管理方式在本质上是不安全的，因为它在网络上使用明文传送口令和数据的，别有用心的人可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境远程登录到设备时，SSH 功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

本页对 SSH 进行配置，包括以下设置（如下图）



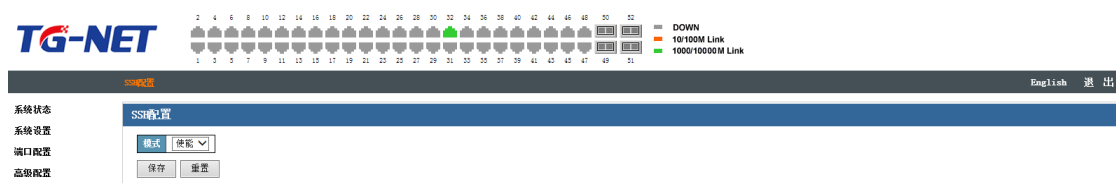
如图，配置页面，可以看到 ssh 模式。

模式：禁用和使能 ssh，缺省禁用；

配置举例：使能 ssh。

配置如下：点击模式下拉菜单使能 ssh，点击保存。

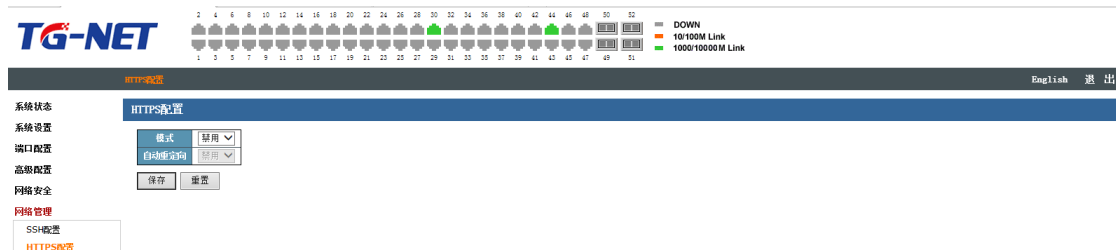
配置参考结果如下图：



7.2 HTTPS 配置

HTTPS 是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。

本页对 stp 端口进行配置，包括以下设置（如下图）



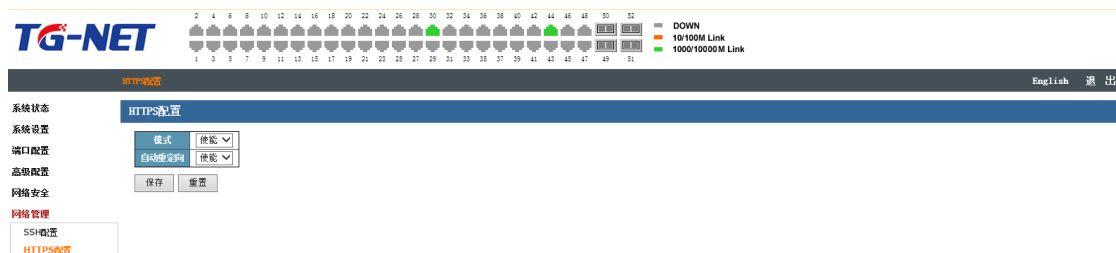
如图 7-2，HTTPS 配置页面，可以看到主要包括模式和自动重定向。

- 模式：禁用和使能 https，缺省禁用；

配置举例：使能 https，使能自动重定向。

配置如下：点击模式下拉菜单使能 https，点击自动重定向下拉菜单使能自动重定向，点击保存。

配置参考结果如下图：

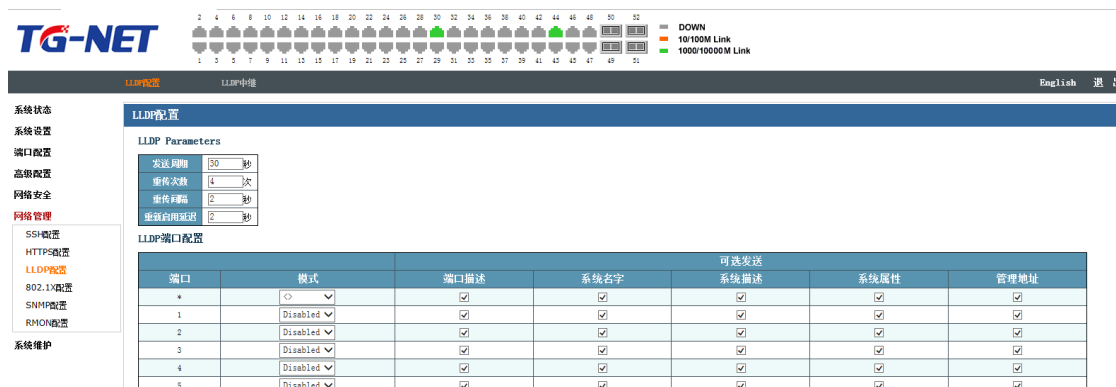


7.3 LLDP 配置

LLDP 是一种邻近发现协议。它为以太网网络设备接入点定义了一种标准的方法，使其可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息。

7.3.1 LLDP 配置

本页对 LLDP 进行配置，包括以下设置（如下图）



如图，LLDP 配置页面，可以看到主要包括 lldp 配置：发送周期、重传次数、重传间隔、重新启用延迟；lldp 端口配置：端口、模式、端口描述、系统名字、系统描述、系统属性、管理地址。

- 发送周期：本地设备向邻居设备发送 lldpdu 的时间间隔，缺省为 30 秒；
- 重传次数：lldpdu 老化时间,缺省为 120 秒
- 重传间隔：lldpdu 重传时间间隔, 缺省为 2 秒
- 重新启用延迟：lldpdu 发送延迟时间, 缺省为 2 秒
- 端口：显示交换机端口号
- 模式:端口工作模式有 Disable、txrx、rx、tx
- 端口描述:勾选使能端口描述，对端设备将会保存本设备端口描述信息，未勾选将会隐藏端口信息
- 系统名字:勾选使能系统名字，对端设备将会保存本设备系统名字，未勾选将会隐藏系统名字
- 系统描述: 勾选使能系统描述，对端设备将会保存本设备系统描述信息，未勾选将会隐藏系统信息
- 系统属性: 勾选使能系统属性，对端设备将会保存本设备的系统属性信息，未勾选将会隐藏系统属性
- 管理地址: 勾选使能管理地址，对端设备将会保存本设备的管理地址，未勾选将会隐藏管理地址
- **配置举例：**使能 1-2 端口 lldp 模式、端口描述、系统名字、系统描述、系统属性、管理地址。

配置如下：点击 1-2 端口模式下拉菜单选择 enable 模式，点击保存。

配置参考结果如下图：

LLDP配置

LLDP Parameters

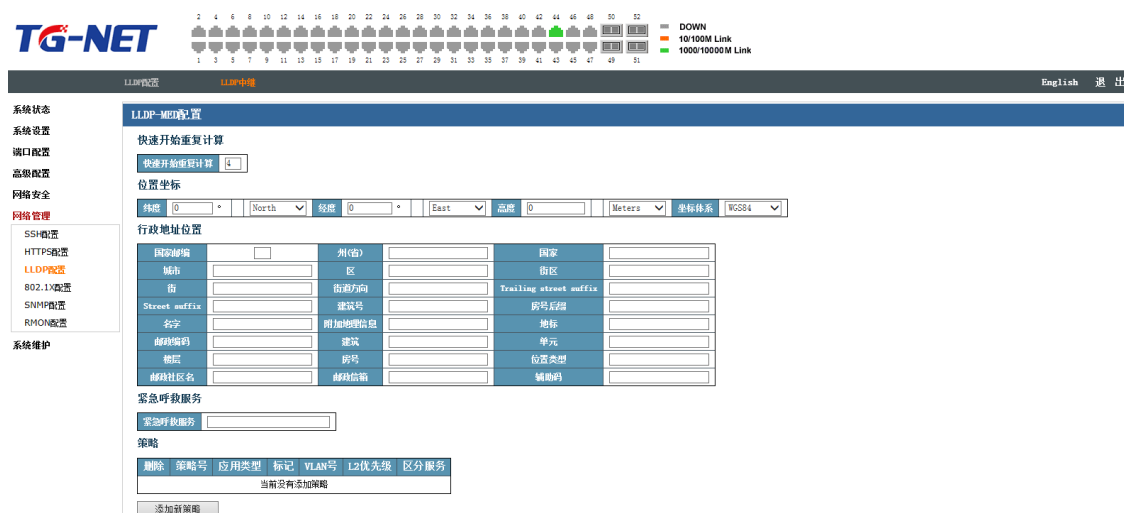
| | | |
|--------|----|---|
| 发送周期 | 30 | 秒 |
| 重传次数 | 4 | 次 |
| 重传间隔 | 2 | 秒 |
| 重新启用延迟 | 2 | 秒 |

LLDP端口配置

| 端口 | 模式 | 端口描述 | 系统名字 | 系统描述 | 系统属性 | 管理地址 |
|----|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| * | <> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1 | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

7.3.2 LLDP 中继

本页对 LLDP 中继进行配置，包括以下设置（如下图）

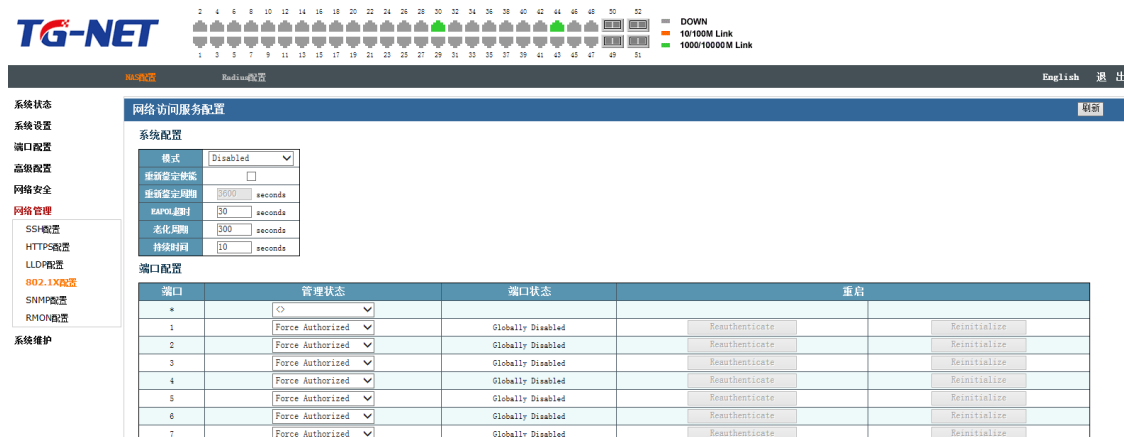


7.4 802.1X 配置

802.1x 是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

7.4.1 NSA 配置

本页对 NSA 进行配置，包括以下设置（如下图）



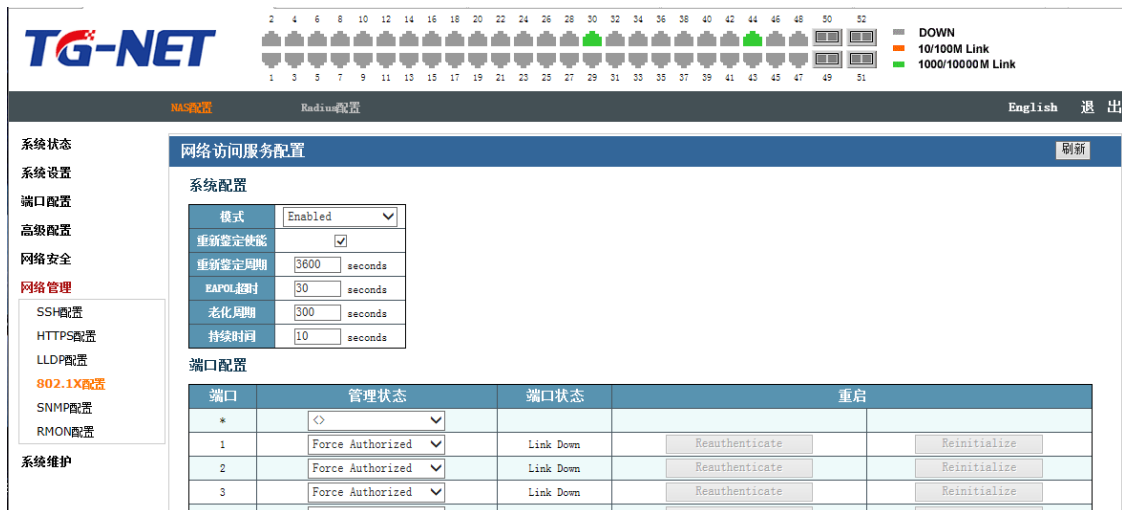
如图，网络访问配置页面，可以看到主要包括系统配置：模式、重新鉴定使能、重新鉴定周期、eapol 超时、老化周期、持续时间；端口设置：端口、管理状态、端口状态、重启。

- 模式：禁用和使能，缺省为禁用；
- 重新鉴定使能：勾选使能重新鉴定功能，未勾选为禁用，缺省为禁用
- 重新鉴定周期：当认证时间到达，交换机发起重新认证，缺省为 3600s
- eapol 超时：重发 EAP-Request 的超时时间间隔，缺省为 30 秒
- 老化周期：
- 持续时间：服务端超时重发的时间间隔，缺省为 10 秒
- 端口：显示交换机的端口

- 管理状态：管理状态有 fore authorized、force unauthorized、port-based 802.1x、single 802.1x、multi802.1x、mac-based auth，缺省为 fore authorized。
- 端口状态：全局关闭。
- 配置举例：使能 dot1x、重新鉴定使能。

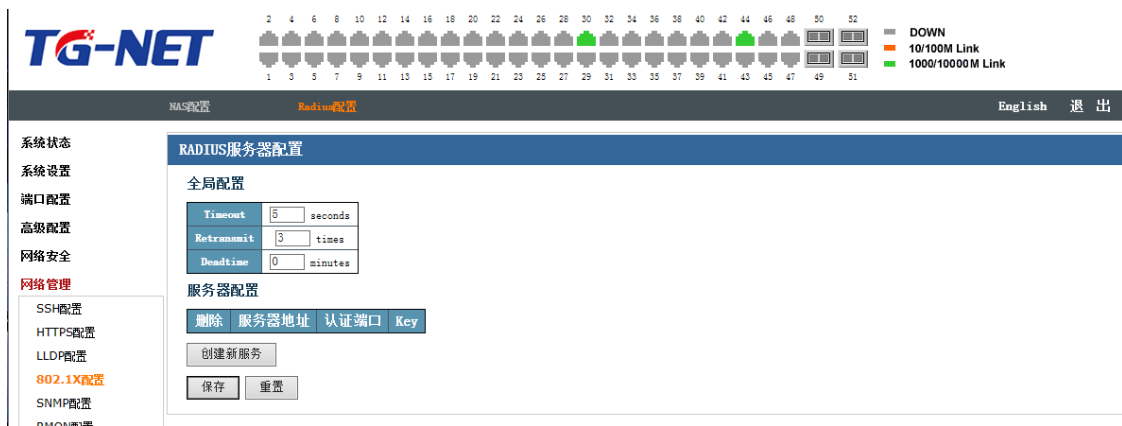
配置如下：点击模式下拉菜单使能 dot1x，勾选重新鉴定使能，点击保存。

配置参考结果如下图：



7.4.2 Radius 配置

本页对 radius 进行配置，包括以下设置（如下图）



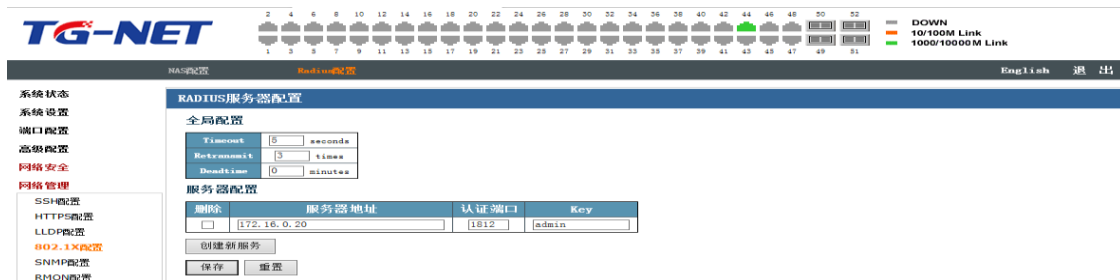
如图，radius 配置页面，可以看到主要包括全局配置:timeout、retransmit、deadtime;服务器配置：删除、服务器地址、认证端口、key；创建新服务。

- timeout: 超时时间,等待回复的 RADIUS 服务器之前重新发送请求,范围为 1-1000,缺省为 5 秒
- retransmit: 重新发送的次数,缺省为 3 次
- deadtime:
- 删除: 用来删除服务器配置。
- 服务器地址: 服务器的 ip 地址。

- 认证端口: RADIUS 认证 UDP 端口, 缺省为 1812
- Key: 交换机和认证服务器之间要相互鉴权, 交换机和认证服务器上都需要设置一个相同的共享密钥
- 创建新服务: 当没有服务器配置时, 可用来创建新的服务器配置
- 配置举例: 创建新服务器, ip 地址为 172.16.0.20, key 为 admin。

配置如下: 点击创建新服务, 在服务器地址框输入 ip 地址 172.16.0.20, 在 key 框里输入密码 admin, 点击保存。

配置参考结果如下图:

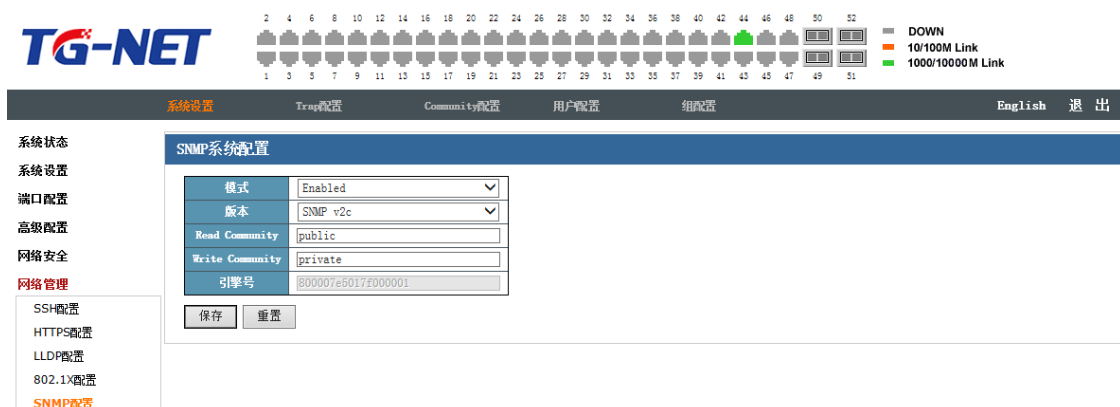


7.5 SNMP 配置

Snmp 是目前 UDP/IP 网络中应用最为广泛的网络管理协议, 它提供了一个管理框架来监控和维护互联网设备。

7.5.1 Snmp 系统配置

本页对 snmp 系统进行配置, 包括以下设置 (如下图)



如图, snmp 系统配置页面, 可以看到主要包括: 模式、版本、read community、write community、引擎号。

模式: 两种模式为 enable 和 disable, 缺省为 enable。

版本: 有 3 个版本 snmpv1、v2、v3, 缺省为 v2 版本。

Read community: 访问网管的共用体名称, 权限为可读, 缺省为 public。

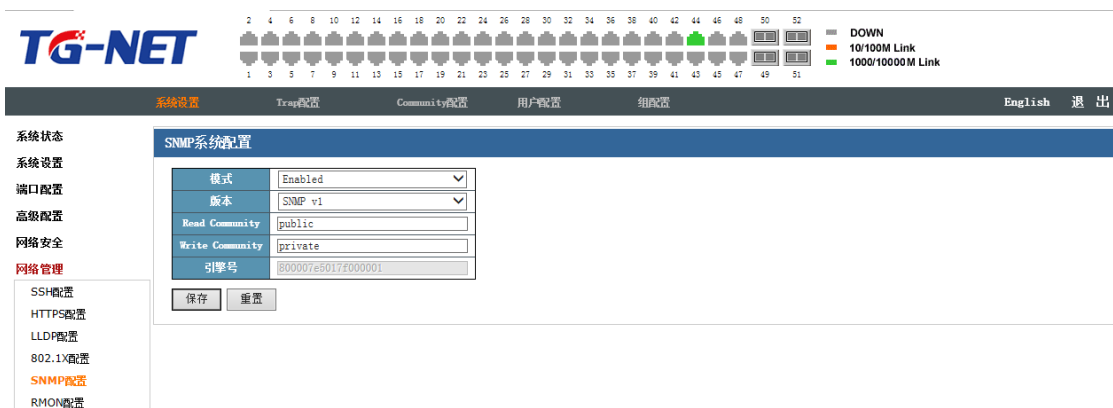
Write community: 访问网管的共用体名称, 权限为可写, 缺省为 private。

引擎号: 标识 snmpEngineID, snmpEngineID 与 SNMP 实体是一一对应的

- **配置举例：**使能 snmpv1 版本，共用体名字不变。

配置如下：点击模式下拉菜单选择 enable，点击版本下拉菜单选择 snmpv1，点击保存。

配置参考结果如下图



7.5.2 Trap 配置

本页对 trap 进行配置，包括以下设置（如下图）



如图，trap 配置页面，可以看到主要包括全局配置：模式；trap 目的配置：删除、名字、使能版本、目的地址、目的端口。

模式：使能和关闭 trap

删除：删除 trap 目的配置

名字：trap 的名字

使能：使能 trap，使用该操作向 NMS 发送报警信息

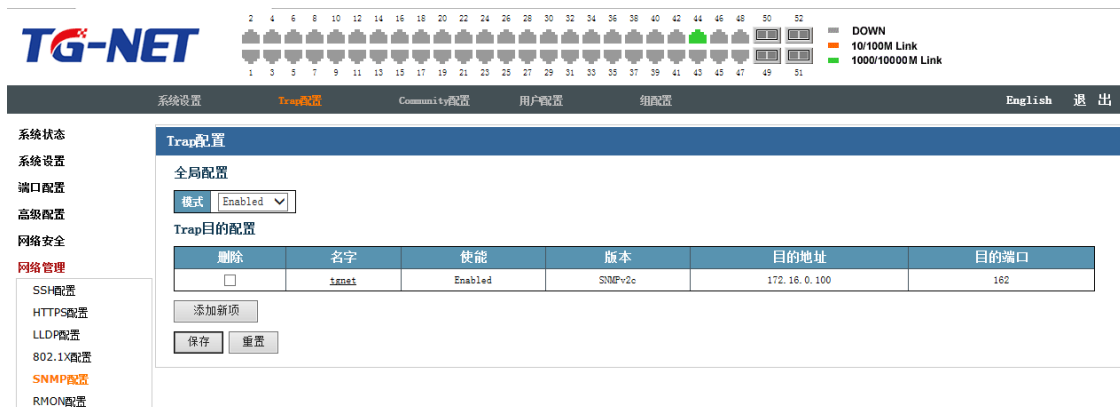
版本：trap 版本有 v1、v2c、v3，缺省为 v2c

目的地址：指定服务器的 ip 地址

目的端口：缺省 trap 目的端口为 162

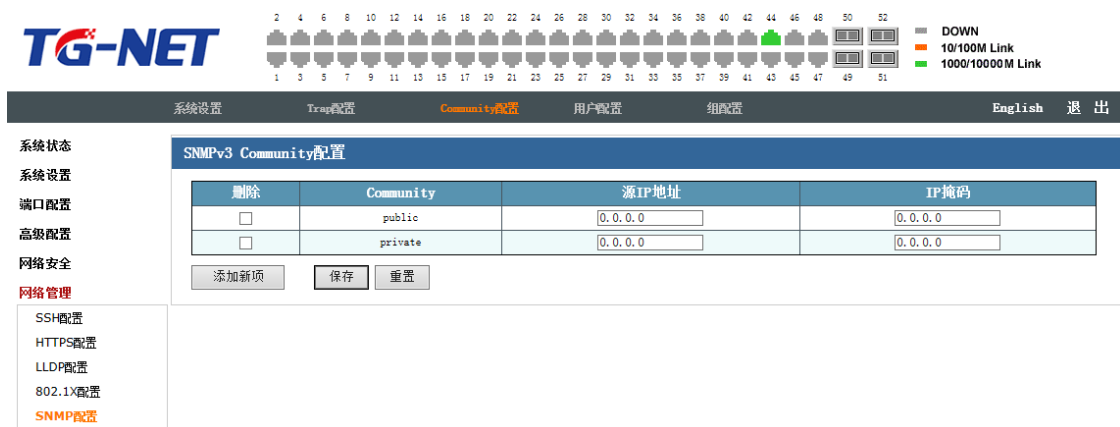
- **配置举例：**使能全局配置，trap 名字为 tgnnet，使能 trap，版本为 v2，目的地址为 172.16.0.100 目的端口为 162

- 配置如下：点击添加新项，在 trap config name 输入 tgnet，点击 trap mode 下拉菜单选择 enable，在 trap destination address 输入 172.16.0.100，点击保存。
- 配置参考结果如下图



7.5.3 community 配置

本页对 community 进行配置，包括以下设置（如下图）



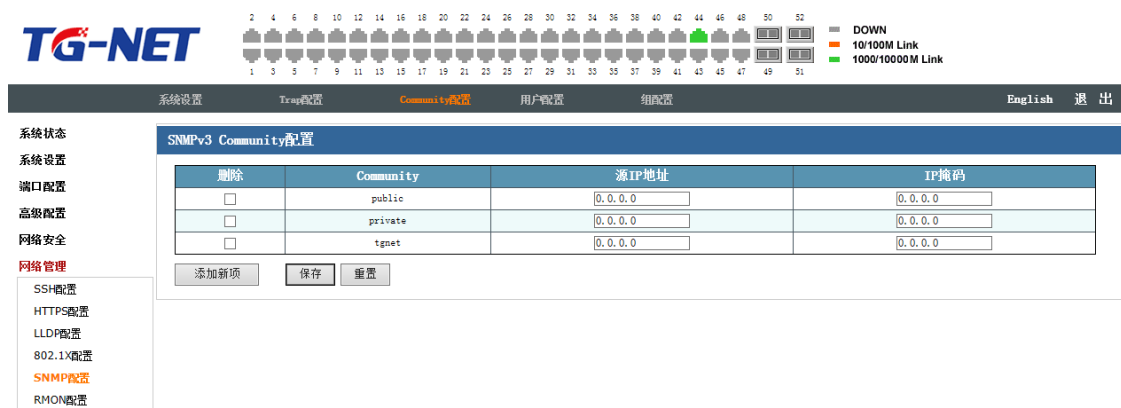
如图，trap 配置页面，可以看到主要包括 snmpv3 community 配置：删除、community、源 ip 地址、ip 掩码；添加新项。

删除：勾选为删除 snmpv3 community 配置

Community：访问网管的共用体名称。

添加新项：增加 snmpv3 community

- **配置举例：**增加 snmpv3 community；community 为 tgnet，源 ip 地址和掩码为 0.0.0.0
配置如下：点击添加新项，在 community 输入 tgnet 点击保存。
配置参考结果如下图



7.5.4 用户配置

本页对用户进行配置，包括以下设置（如下图）



如图，用户配置页面，可以看到主要包括 snmpv3 用户配置：删除、引擎号、user name、security level、 authentication protocol、 authentication password、privacy protocol、privacy password；添加新项。

删除：勾选删除 snmpv3 用户配置。

引擎号：标识 snmpEngineID，snmpEngineID 与 SNMP 实体是一一对应的

user name：用户名

security level：安全级别有认证加密，认证不加密，不认证不加密，用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP NMS 和 SNMP Agent 之间的通信提供更高的安全性

authentication protocol：验证协议 MD5 为密文，SHA 为明文。

authentication password：认证的密码。

privacy protocol：私有协议。

privacy password：私有密码。

添加新项：新添加 snmpv3 用户配置。

- **配置举例：**增加 snmpv3 用户配置；引擎号为 800007e5017f000002，username 为 tgnnet，security level 为认证和加密，authentication protocol 为 md5，authentication password 为 12345678，privacy protocol 为 des，privacy password 为 12345678。

配置如下：点击添加新项，引擎号栏输入 800007e5017f000002，username 输入 tgnnet，点击 security level 下拉菜单选择 auth，priv，点击 authentication protocol 下拉菜单选择 MD5，在 privacy password 栏中输入密码 12345678，点击 privacyprotocol 下拉菜单选择 DES，在 privacy password 输入密码 12345678，点击保存。

配置参考结果如下图

7.5.5 组配置

本页对组进行配置，包括以下设置（如下图）

如图，组配置页面，可以看到主要包括 snmpv3 组配置：删除、安全模型、security name、组名；添加新项。

删除：勾选删除 snmpv3 组配置

安全模型：安全模型有 v1、v2、csm

security name：安全名字

组名：snmpv3 组的名字

7.6 RMON 配置

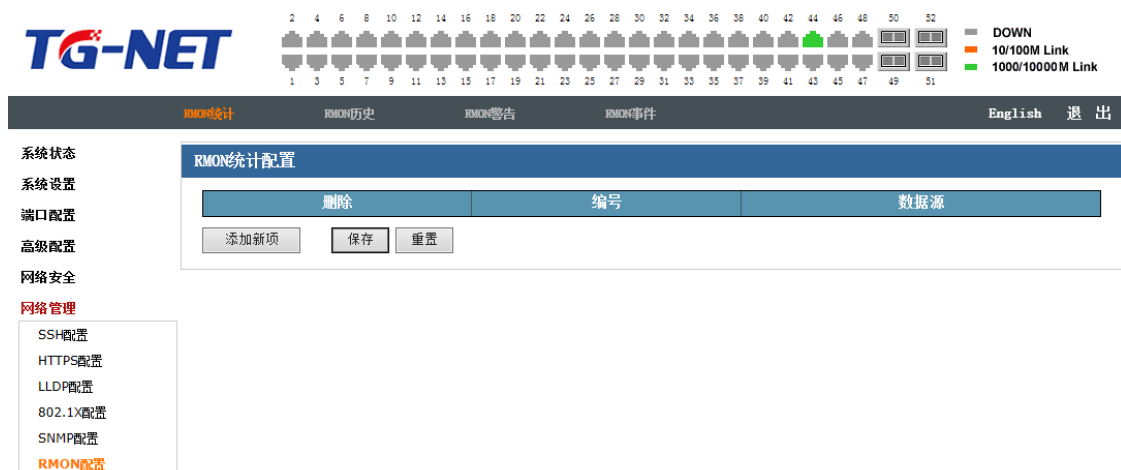
RMON 是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。RMON 首先实现了对异构环境进行一致的远程管理，它为通过端口远程监视网段提供了解决方案。主要实现对一个网段乃至整个网络的数据流量的监视功能，目前已成为成功的网络管理标准之一。

7.6.1 RMON 统计

利用 RMON 统计管理功能，可以监视端口的使用情况。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。

在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。

本页对 rmon 统计进行配置，包括以下设置（如下图）



如图，rmon 统计配置页面，可以看到主要包括删除、编号、数据源；添加新项。

删除：勾选删除 rmon 统计配置

编号：rmon 统计配置编号

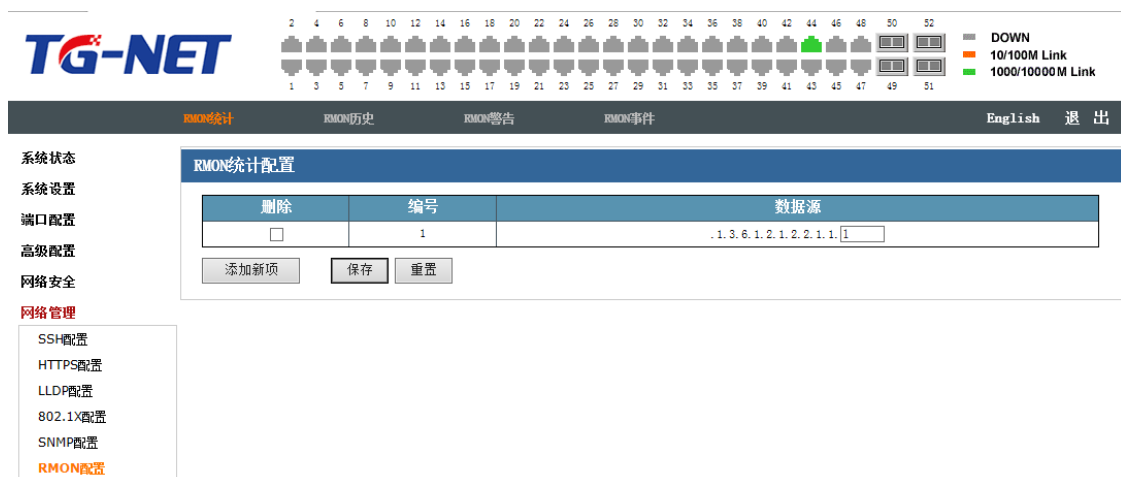
数据源：mib 节点，表示被管理对象

添加新项：增加 rmon 统计配置。

- **配置举例：**rmon 统计配置；编号为 1，数据源为 1。

配置如下：点击添加新项，编号栏输入 1，数据源输入 1，点击保存。

配置参考结果如下图：



7.6.2 RMON 历史

历史组是按周期对端口的使用情况进行统计，并将统计结果存储在历史记录表中以便以后查看。统计数据包括带宽利用率、错误包数和总包数等。在指定接口下创建历史表项成功后，统计组就对当前接口的报文数按周期进行统计，它统计的结果是一个周期内端口收发报文的情况。

本页对 rmon 历史进行配置，包括以下设置（如下图）



如图，rmon 历史配置页面，可以看到主要包括删除、编号、数据源间隙 buckets、bucketsgranted；添加新项。

删除：勾选删除 rmon 历史配置

编号：rmon 历史配置编号

数据源：mib 节点，表示被管理对象。

间隙：采样时间间隔。

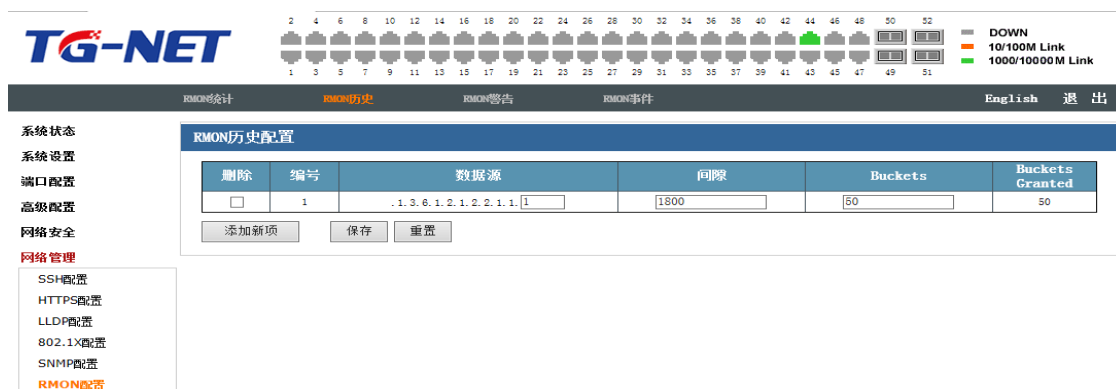
Buckets：桶量数，保存的数据量。

添加新项：增加 rmon 历史配置。

- **配置举例：**rmon 历史配置；编号为 1，数据源为 1，间隙 1800，buckets 为 50。

配置如下：点击添加新项，编号栏输入 1，数据源输入 1，点击保存。

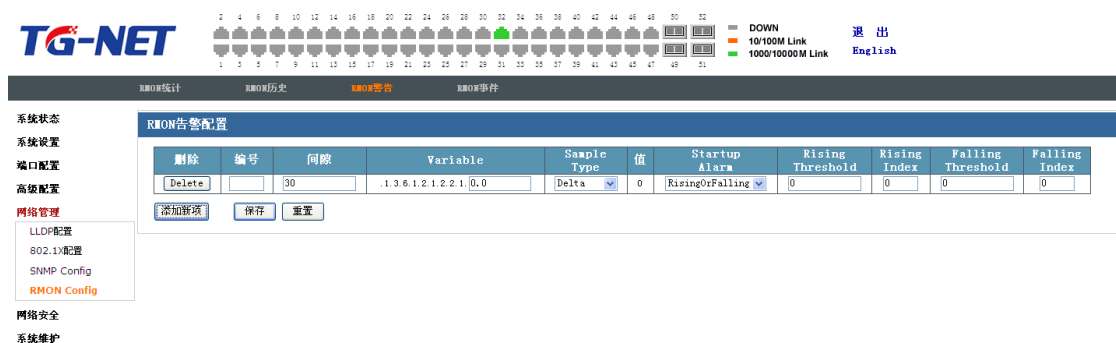
配置参考结果如下图：



7.6.3 RMON 警告

RMON 告警管理可对指定的告警变量（如端口的统计数据）进行监视。被监视的告警变量的采样值大于或等于上限阈值时，触发一次上限告警事件；被监视的告警变量的采样值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

本页对 rmon 警告进行配置，包括以下设置（如下图）



如图，rmon 警告页面，可以看到主要包括删除、编号、间隙、variable、sampletype、值、startup alarm、rising threshold、rising index、falling threshold、falling index；添加新项。

删除：勾选删除 rmon 警告配置

编号：rmon 告警编号

间隙：采样时间间隔。

Variable: mib 节点，表示被管理对象

Sample type: absolutely 或 delta 分别表示绝对值（每次采样的数值）和相对值（每次采样相对上次采样的增量）

值：值为 0

startup alarm: 启动告警有，rising、falling、risingorfalling

rising threshold: 上限阈值

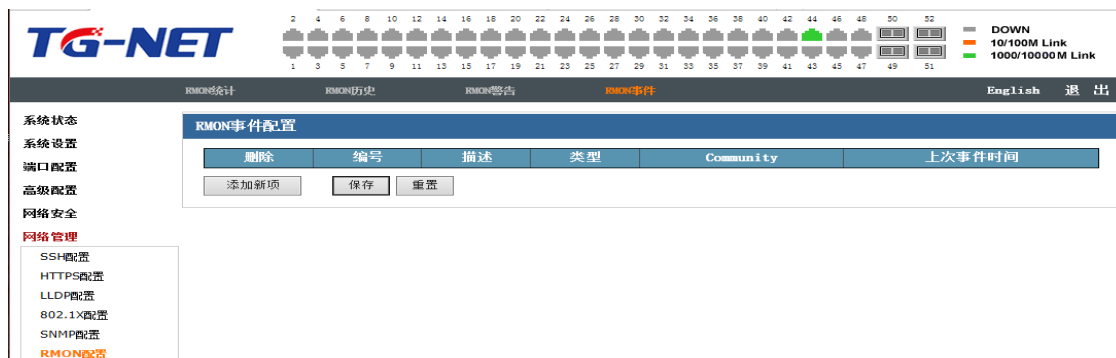
falling threshold: 下限阈值

添加新项：增加 rmon 告警配置

7.6.4 RMON 事件

事件组用来定义事件索引号及事件的处理方式。事件组定义的事件主要用在告警组配置项和扩展告警组配置项中。当监控对象达到告警条件时，必然会触发事件，事件有如下几种处理方式：将事件相关信息记录在事件日志表中、向网管站发送 Trap 消息、将事件相关信息记录在事件日志表中并向网管站发送 Trap 消息、不做任何处理

本页对 rmon 事件进行配置，包括以下设置（如下图）



如图，rmon 事件页面，可以看到主要包括删除、编号、描述、类型、community、上次事件时间；添加新项

删除：勾选删除 rmon 事件配置

编号：rmon 事件配置编号

描述：事件的描述

类型：事件类型 none（无任何动作）log（记录日志）snmptrap(发送 trap) logandtrap（记录日志并发出 Trap）

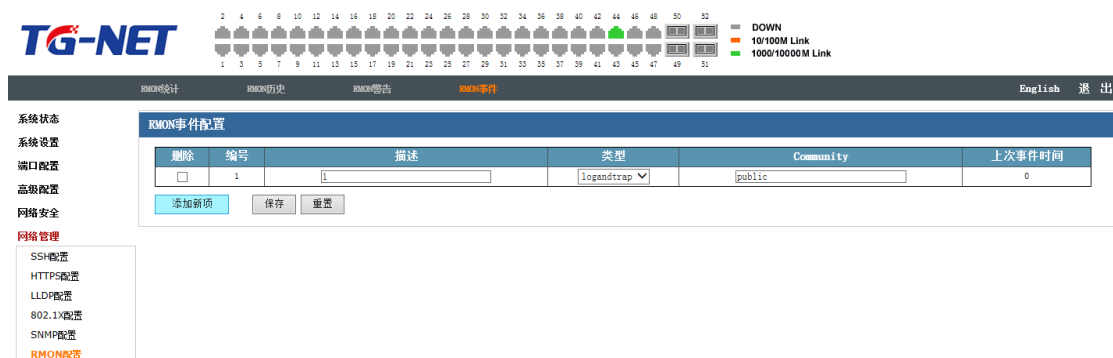
Community：共用体名

上次事件时间：上次事件的时间

添加新项:增加 rmon 事件配置

- **配置举例:** rmon 事件配置; 编号为 1, 描述为 1, 类型为 logandtrap, community 为 public。配置如下: 点击添加新项, 编号栏输入 1, 描述输入 1, 点击类型下拉菜单选择 logandtrap 点击保存。

配置参考结果如下图:



第8章 系统维护

点开系统维护，您可以看到：

系统维护

设备重启

恢复出厂配置

固件升级

配置导出

配置导入

PING诊断

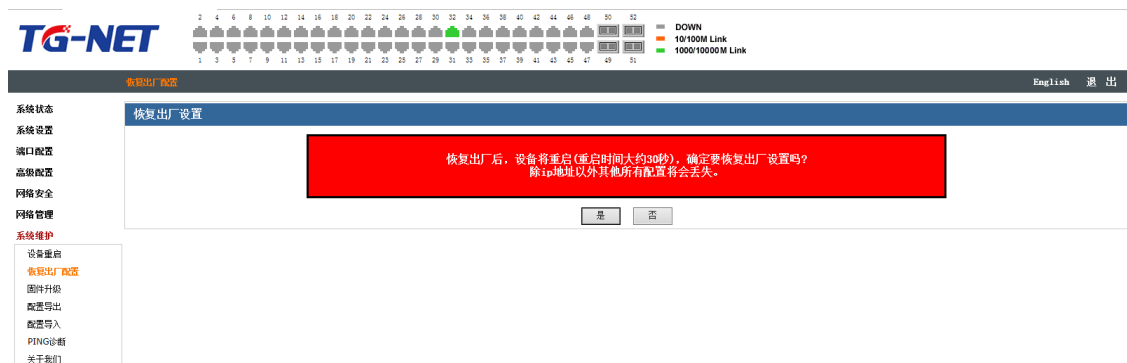
关于我们

8.1 设备重启



交换机的一些功能配置，除了需要提交保存配置以外还需要重启才能使配置生效。

8.2 恢复出厂配置

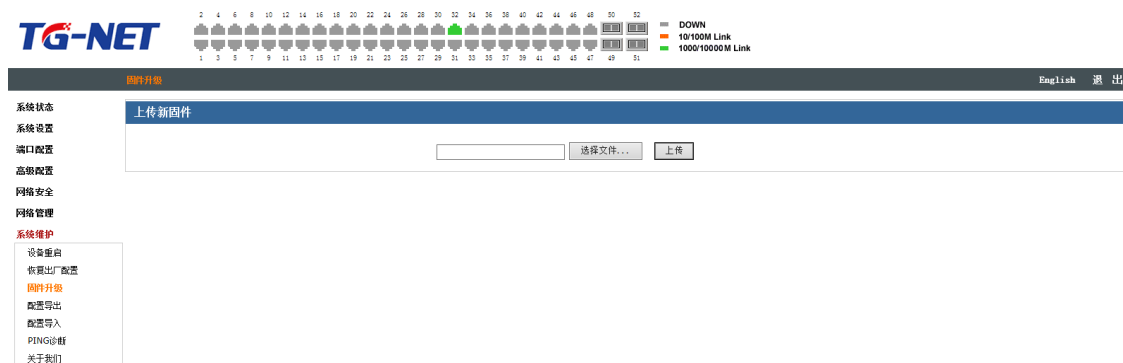


当需要将交换机配置还原到最初的系统默认值时，可选择恢复出厂配置功能。除管理IP外，其他信息均会恢复为出厂设置。

提示：恢复出厂配置前请注意当前配置是否需要备份。

8.3 固件升级

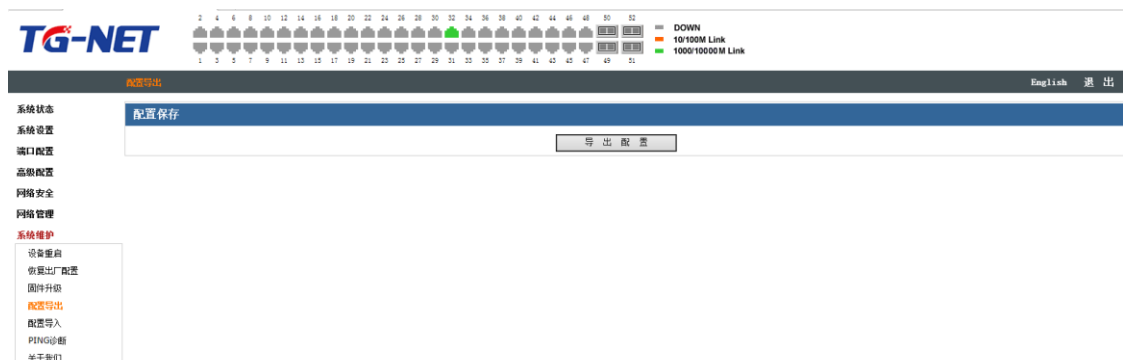
本页提供交换机通过 WEB 方式升级系统文件功能。你可以在 <http://www.tg-net.cn> 网站上下载最新版本的系统文件。



点击“选择文件”按钮，选中相应升级文件，点击“上传”，交换机开始升级。

8.4 配置导出

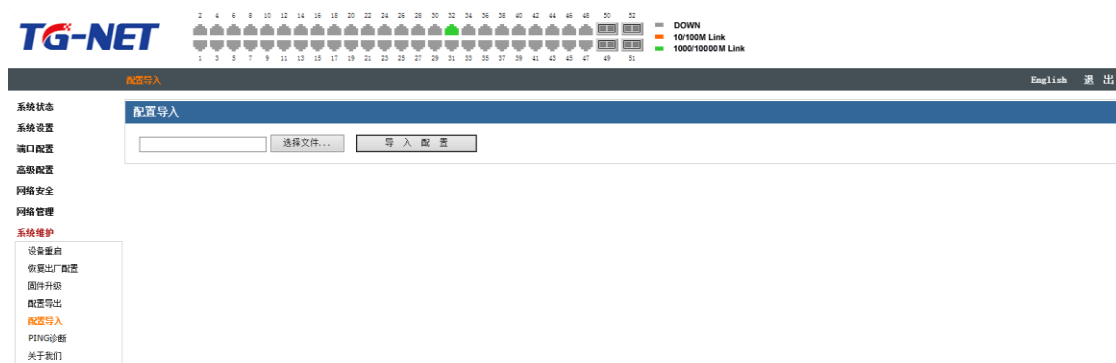
配置导出，可将交换机目前的配置导出到本地电脑中备份。



点击“导出配置”按钮，交换机当前配置文件导出。

8.5 配置导入

您可通过配置导入功能，将之前备份的配置文件导入到交换机中，实现配置的更新。



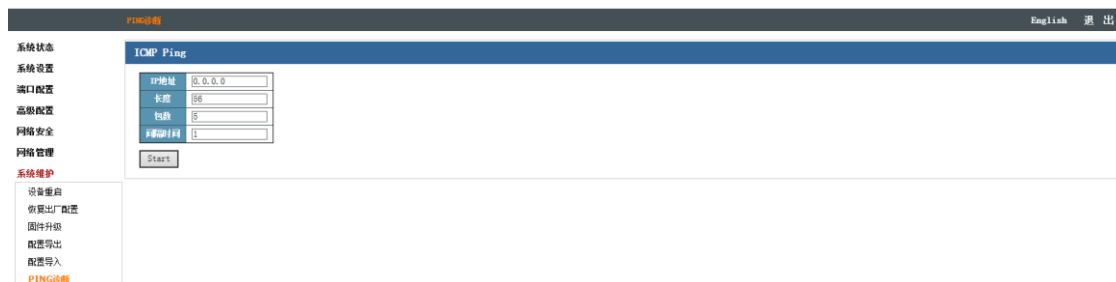
点击“选择文件”按钮，选中您要导入的配置文件，单击“配置导入”，完成配置文件的导入。

提示：配置导入以后，设备管理 IP 地址将变成之前备份配置里的 IP 地址，请最好记录，以防管理失败！

8.6 PING 诊断

Ping 诊断和普通计算机上的 ping 命令一样，都是用来检测网络中两个节点之间的链路是否连通。两者区别在于，两台普通计算机之间的 ping 命令是为了检测物理链路连接是否正常，而交换机的 ping 检测功能是为了方便网络管理员检测局域网中的网络设备是否已经断开连接，定位网络故障。

本页对 ping 检测行配置，包括以下设置（如下图）：



- IP 地址：测试的目的的节点的 IP 地址；
- 长度： 设置发起 ping 检测时 ping 报文长度，建议使用缺省值；
- 包数： 设置发起 ping 检测时 ping 包的个数；
- 时间间隔： 发起 ping 检测时，若没有收到回复，则在配置的时间间隔后再发送ping 报文，直到所发送的报文数达到所设置的发送次数；

8.7 关于我们

本页显示交换机厂家信息，如图示：

The screenshot shows the TG-NET web configuration interface. At the top, there is a status bar with a row of 48 port indicators (1-48) and a legend for link speeds: DOWN (grey), 10/100M Link (orange), and 1000/10000M Link (green). Below the status bar is a navigation menu with the following items: 系统状态 (System Status), 系统设置 (System Settings), 端口配置 (Port Settings), 高级配置 (Advanced Settings), 网络安全 (Network Security), 网络管理 (Network Management), and 系统维护 (System Maintenance). The main content area displays the '公司信息' (Company Information) section. It includes a table with the following information:

| 公司名称 | 深圳前海万得通科技有限公司 |
|------|---|
| 客服电话 | 400-088-7500 |
| 公司网址 | http://www.tg-net.cn |

如您对产品有任何问题或者建议，您可以致电我司技术支持热线：400-088-7500。您也可以登录我司官方网站 www.tg-net.cn 查询更多产品信息。