Web 配置手册

网管以太网交换机

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知，请关注本公司网站提供的最新信息。本公司在编写本手册时已尽力保证其内容准确可靠，但对于本手册中的遗漏、不准确或错误，以及由此导致的损失和损害，本公司不承担责任。

前言

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

修订记录：

版本号	日期	原因
V2.1	2017.08	1，增加文档目录 和页眉 2，增加产品介绍和特性 3，增加三层静态路由与 IPV6 配置 4，修改 SNTP 为 NTP，增加时区设置 5，增加 SNMPv3 配置 6，增加 POE 调度配置 7，增加 MSTP 配置 8，增加静态组播过滤（IPMC Profile）配置 9，增加 IPV6 MLD Snooping 配置 10，增加附录 1 术语表，附录 2 常见问题处理

目录

1 产品概述

1.1 产品介绍

36 系列产品是一款高性能、高性价比的高端智能机架式核心三层交换机。该系列产品包括 36036FM 、36028FM 、36048FM 和 36032FM 四款产品，36036FM 提供 24 路 10/100/1000Base-T(X)以太网标准供电接口、 8 路千兆光接口(支持 10/100/1000Base-T(X)网络接口或 1000Base-SFP 接口) 以及 4 路 1000Base-SFP/10GbE SFP+光口，36028FM 提供 24 路 10/100/1000Base-T(X)以太网标准供电接口、4 路 1000Base-SFP/10GbE SFP+光口，36048FM 提供 48 路 10/100/1000Base-T(X)以太网标准供电接口、4 路 1000Base-SFP/10GbE SFP+光口，36032FM 提供 4 路 10/100/1000Base-T(X)以太网接口、28 路 1000Base-SFP/10GbE SFP+光口、4 路 1000Base-SFP/10GbE SFP+光口，带宽的增加提高了网络数据的通讯功能，非常适合大规模网络的应用。

该系列产品支持 IPv4/IPv6 双栈平台，支持多种高级管理功能，例如：MAC Table、VLANs、Port Isolation 、Loop Protection、IGMP Snooping、MLD Snooping 、ERPS、DHCP client、DHCP-snooping、STP/RSTP/MSTP、802.1x、 QoS、端口镜像、 LLDP、静态路由、NTP 等，支持 128 条静态路由，支持基本 QINQ，为用户提供完善的解决方案；同时该系列产品还支持 SNMP v1/v2/v3(Simple Network Management Protocol)、 CLI 命令行、 Web 网管、TELNET 的管理方式，使设备管理更方便，同时配合增强的 ACL 控制功能，防攻击功能，使得管理更加安全。

该系列产品符合 FCC、 CE 标准，支持 1 路交流电源输入。该产品采用静音风扇、能够适应-10℃～50℃工作温度范围环境，能够满足各种现场的要求，能为您的以太网连接提供可靠，经济的解决方案。

1.2 产品特性

- 支持 IEEE802.3、 IEEE802.3u、 IEEE802.3ab、 IEEE802.3z、 IEEE802.3ae
- 36036FM 提供 24 路 10/100/1000Base-T(X)以太网标准供电接口、 8 路千兆光接口(支持 10/100/1000Base-T(X)网络接口或 1000Base-SFP 接口) 以及 4 路 1000Base-SFP/10GbE SFP+光口

  36028FM 提供 24 路 10/100/1000Base-T(X)以太网标准供电接口、4 路 1000Base-SFP/10GbE SFP+光口

  36048FM 提供 48 路 10/100/1000Base-T(X)以太网标准供电接口、4 路 1000Base-SFP/10GbE SFP+光口

  36032FM 提供 4 路 10/100/1000Base-T(X)以太网标准供电接口、28 路 1000Base-SFP/10GbE SFP+光口、4 路 1000Base-SFP/10GbE SFP+光口
- 支持 V-Ring 环网冗余专利技术，网络故障自愈时间小于 20ms
- 支持 IGMP Snooping 、支持静态组播过滤和 MLD Snooping 过滤
- 支持 DHCP Snooping，防止 ARP 攻击，非法 DHCP 服务器的接入等攻击

- 支持 NTP，便于实时同步网络时间
- 支持 SNMP v1/v2/v3 简单网络管理协议
- 支持 LLDP 链路层发现协议
- 支持 ACL 功能，增强灵活度及网络管理安全
- 支持 IEEE802.1P QoS 功能，增加网络稳定性
- 支持端口镜像功能，便于在线调试
- 支持线缆检测，便于工程上检查网线长度
- 支持 STP/RSTP/MSTP，增加网络稳定性
- 支持 IEEE802.1Q VLAN 、IEEE802.1ad QINQ 便于网络规划
- 支持 802.1x 端口认证和 mac 地址认证，增强网络安全性
- 支持静态路由三层交换技术
- 支持工作温度范围-10℃～50℃
- 支持存储温度范围-40℃～85℃
- 支持静音风扇、机架式安装设计

1.3 登录 Web 管理器

在浏览器（已安装在您的计算机上）中输入设备的 IP 地址即可对交换机进行管理。地址栏中的 URL 格式为：http://xxx.xxx.xxx.xxx，其中 xxx 表示的是交换机的 IP 地址。

注意:默认出厂 IP 地址为 192.168.2.1.

弹出管理模块的用户认证窗口，如下所示。

图 1-3 输入网络密码窗口

“用户名”为 admin，“密码”为 system，输入后单击“OK”，打开基于 Web 管理的用户界面。

1.4 基于 Web 的用户界面

用户界面提供了对交换机不同配置和管理窗口的访问，允许用户查看性能统计并对系统状态进行图示监控。

下图显示了用户界面。用户界面分成三个不同的区域，如下图所示。

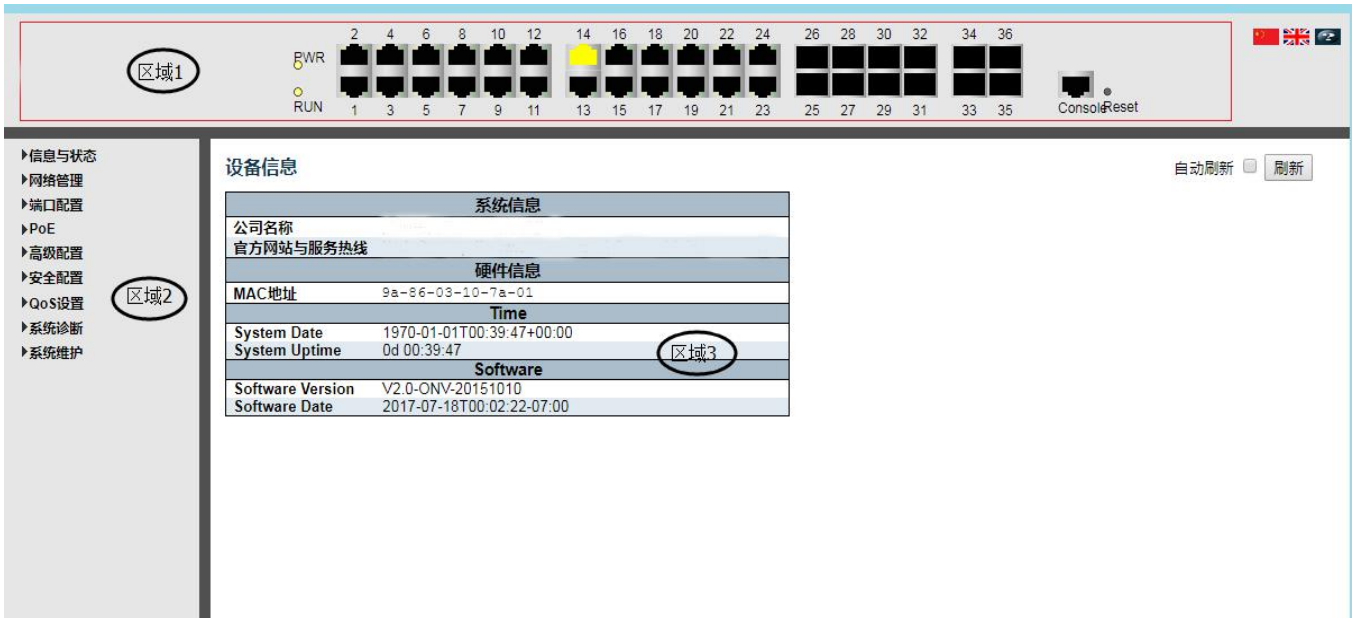


图 1-4web 管理界面

区域	功能
区域 1	显示厂商 LOGO, 端口的 PoE 以及 Link 工作状态, 中英文切换以及帮助.
区域 2	选择所显示的菜单或窗口, 单击其中的超链接菜单按钮和子文件夹，显示相应菜单内容。
区域 3	根据用户选择(区域 2)，显示交换机的相关信息和配置数据条目, 该区域为交换机配置与状态的主页面.

1.5Web 页面

当用户通过 web 浏览器连接交换机的管理模式时，会显示一个登录窗口。输入用户名和密码访问交换机的管理界面。

下面是 web 界面中的主要文件夹列表和说明:

信息与状态 - 用户可在此菜单下查看交换机的信息与工作状态。

网络管理 -用户可在此部分中配置交换机的相关网络管理特性。

端口配置 -用户可在此部分中配置交换机的端口相关特性。

PoE -用户可在此部分中配置与查看交换机的 PoE 相关配置与状态。

高级配置 -用户可在此部分中配置交换机的高级 L2 相关特性。

安全配置 -用户可在此部分中配置交换机的安全相关特性。

QoS 配置 -用户可在此部分中配置交换机的 QoS 相关特性。

系统诊断 -用户可在此部分中配置交换机的诊断相关特性。

系统维护-用户可在此部分中配置交换机的系统维护相关特性。

2 网络管理

2.1 IP 配置

注意:交换机的出厂默认 IP 地址为 192.168.2.1，子网掩码为 255.255.255.0(24)

单击“网络管理”>“IP”,显示如下窗口:

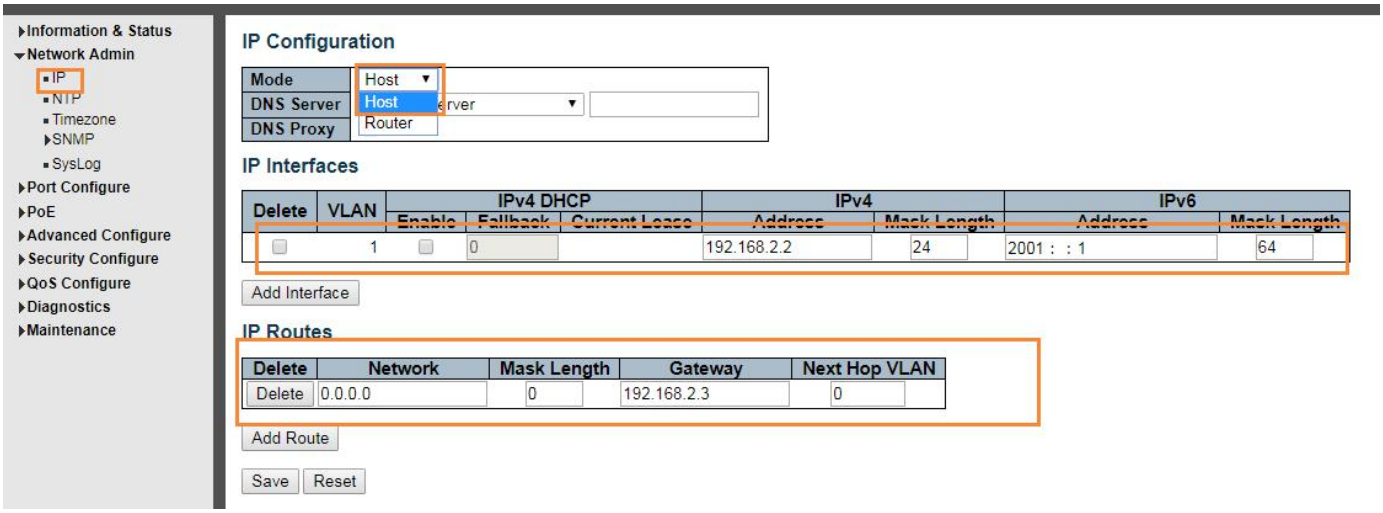


图 2-1 系统 IP 以及及 Router 配置地址设置窗口

以下为关于 IP 设置的说明信息:

参数	说明
模式	可选 Host 和 router
DNS Server	可选 No DNS server,Configuerd IPV4,From any DHCPv4 interfaces, From this DHCPv4 interfaces
DNS Proxy	DNS 代理
接口名称	显示系统接口名称。

VLAN	输入用于对交换机进行访问和管理的 VLAN。
IPv4 DHCP	- 如果使能, 则表示该 VLAN 接口开启 IPv4 DHCP client, 动态获取交换机的 IPv4 地址，否则采用交换机的静态 IP 配置 - 等待时间,表示交换机尝试通过 DHCP 获取动态 IP 地址的等待时间(单位为秒), 0 表示永不超时. - 当前 IP 地址, 表示通过 DHCP 获取到的 IP 地址.
IPv4	- IP 地址，用户输入的静态 IPv4 地址。 - IP 掩码，用户输入的静态 IPv4 子网掩码。
IPv6	- IP 地址，用户输入的静态 IPv6 地址。 - IP 掩码，用户输入的静态 IPv6 子网掩码。
IP Routes	- 目的网段，用户输入目的网段 IPv4 地址。 - IP 掩码，用户输入静态 IPv4 子网掩码。 - 下一跳地址，用户输入下一条 IPv4 地址

单击“添加”可以创建新的管理 VLAN 与 IP 地址。单击“保存”令更改生效。

 注意:交换机默认只创建了 VLAN1，如果用户需要使用其他 VLAN 的管理交换机，那么必须先在 VLAN 模块中先添加该 VLAN，并将相关端口加入到该 VLAN，可实现 vlan 之间的三层通信。

2.2 NTP 配置

简单网络时间协议（NTP），是通过互联网同步时钟的协议。 用户可以配置交换机的时间设定。

要查看此窗口，请单击“网络管理”>“NTP”，如下图所示：

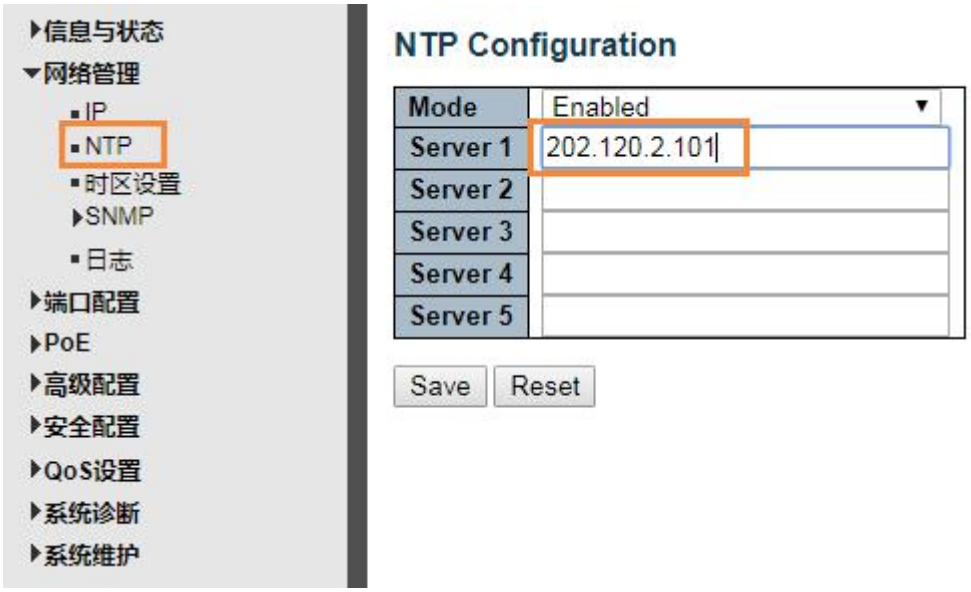


图 2-2 NTP 设置窗口

可配置的字段的说明如下：

参数	说明
模式	使用下拉菜单以启用(Enabled)或禁用(Disabled)NTP。
NTP 服务器	NTP 服务器的 IP 地址，NTP 信息将从该服务器中获取，可填写多个 NTP 服务器。

单击“保存”按钮接受所做的更改。

2.3 时区设置

时区设置，是通过设置时间来调整到相应国家的时间。 用户可以配置交换机的时间设定。

要查看此窗口，请单击“网络管理”>“时区设置”，如下图所示：

图 2-3 NTP 设置窗口

可配置的字段的说明如下：

参数	说明
时区设置	输入需要更改的时间。

单击“保存”按钮接受所做的更改。

2.4 SNMP 配置

简单网络管理协议（SNMP）设计用于管理和监控网络设备。SNMP 允许网络管理站点读取和更改网关、路由器、交换机和其它网络设备的设置。使用 SNMP 来保证交换机、交换机组或网络的正确运行、监控其性能和检测潜在问题。

支持 SNMP 的可网管设备，包括了一套在设备上本地运行的软件（这里叫代理）。SNMP 代理使用一套预定义的变量（可管理对象）来维护和管理设备。管理信息库（MIB）对这些对象进行定义，内置 SNMP 代理提供了标准的控制信息。SNMP 同时定义了 MIB 规格和访问该信息所用的协议。

目前，设备中的 SNMP Agent 支持 SNMP V1 版本、 SNMP V2C 和 SNMP V3 版本。不同版本的 SNMP 为管理站点和网络设备提供了不同级别的安全性。

在 SNMP 的 v1 和 v2c 中，使用“共同体字符串”进行用户认证，该字符串类似密码功能。远端用户 SNMP 应用程序和交换机 SNMP 必须使用相同的共同体字符串。任何未被授权站点的 SNMP 数据包都将被忽略（丢弃）。

交换机用于 SNMPv1 和 v2c 管理访问所使用的默认共同体字符串是：

1. public – 允许授权管理站点读取 MIB 对象。
2. private – 允许授权管理站点读写和更改 MIB 对象。

Trap 信息

Trap 信息用于通知网络管理员交换机上所发生的事件。这些事件可能很严重，比如重启（某人无意间关掉交换机），或者是一般信息，如接口状态改变。交换机产生 trap 信息并发送它们给 trap 信息接收者（或网络管理者）。

典型的 trap 包括认证失败、拓扑改变和冷热启动的 trap 信息。

MIB

交换机在管理信息库（MIB）中存储了管理和计数器信息。交换机使用标准的 MIB-II 管理信息库模块。因此，MIB 对象值可被任何 SNMP 的网络管理软件读取。

2.4.1 SNMP 系统设置

可以启用或禁用 SNMP 全局状态。单击“网络管理” > “SNMP ” >

“系统设置”， 显示如下窗口：

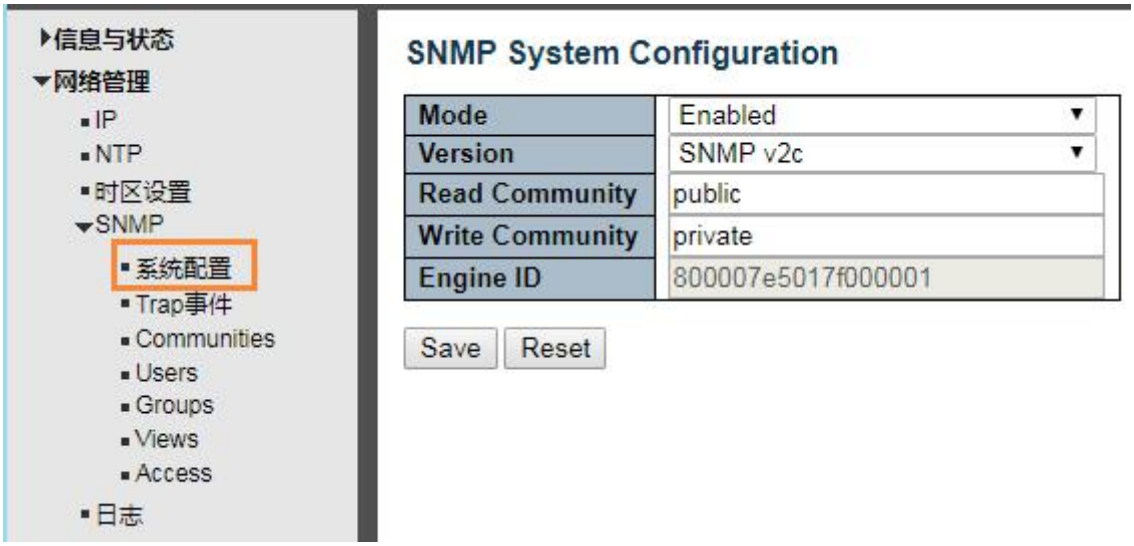


图 2-4-1 SNMP 系统设置窗口

配置字段的说明如下:

参数	说明
SNMP 模式	启用(Enabled)或者禁(Disable)SNMP 功能
版本	通过下拉菜单选择 SNMP v2c 或者 SNMP v1 或者 SNMPV3 版本
Read Community 团体	允许授权管理站点读取 MIB 对象, 默认名称为 public
Write Community 团体	允许授权管理站点读写和更改 MIB 对象, 默认名称为 private

单击“保存”令更改生效。

2.4.2 SNMP Trap 事件

用户可分别启用和禁用交换机的 SNMP Trap 支持功能和 SNMP 认证 Trap 支持功能。

单击“网络管理”>“SNMP”>“Trap 事件”， 显示如下窗口:

图 2-4-2 SNMP Trap 设置窗口

配置字段的说明如下:

参数	说明
Trap 名称	SNMP Trap 的别名
Trap 模式	使能(Enabled)或者禁用(Disabled)SNMP Trap
Trap 版本	该交换机支持 SNMPv1，SNMPv2c 和 SNMPv3
Trap Community 团体	指定 SNMP Trap 的团体名称
Trap 目的 IP 地址	指定 SNMP Trap 服务器的 IP 地址
Trap 目的 UDP 端口号	指定 SNMP Trap 服务器的 UDP 端口号

Trap 通知/应答模式	使能(Enabled)或者禁用(Disabled)SNMP Trap 通知/应答 模式
Trap 通知/应答超时(秒)	Trap 通知/应答 的超时时间
Trap 通知/应答重传次数	Trap 通知/应答 的重传次数

单击“保存”令更改生效。

2.4.3 Communities

用户可新建新的团体名称。单击“网络管理”>“SNMP”>“Communities”， 显示如下窗口：

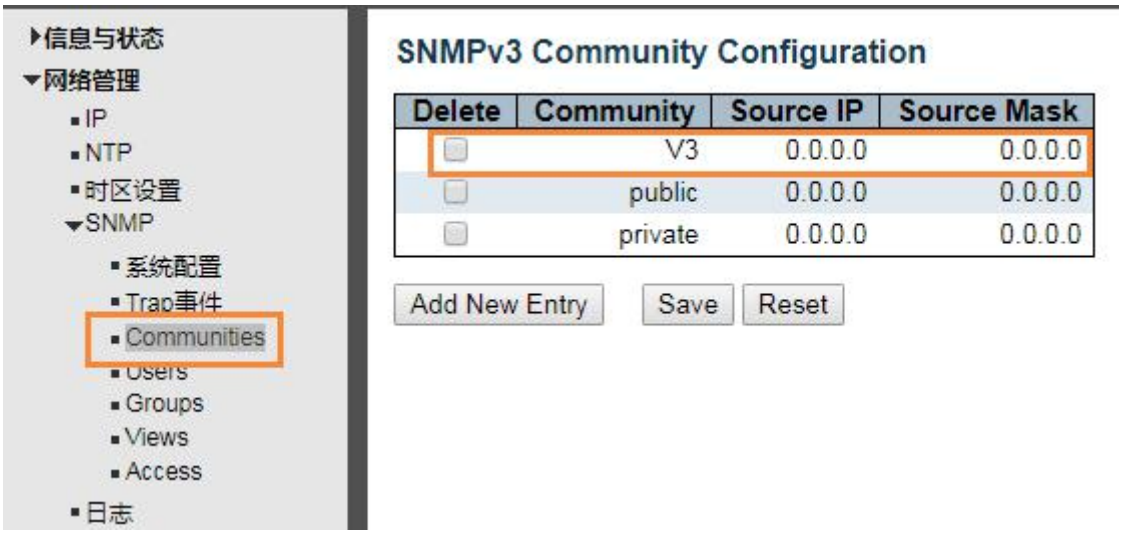


图 2-4-3 SNMPV3 添加团体窗口

配置字段的说明如下:

参数	说明
Community	输入需要新建的团体名称
Source IP	输入 IPV4 源地址
Source Mask	输入 IPV4 子网掩码

单击“保存”令更改生效。

2.4.4 Users

SNMP v3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员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。采用认证和加密功能，可以为 NMS 和 Agent 之间的通信提供更高的安全性。

用户可新建 SNMP v3 用户，可选择加密方式。单击“网络管理”>“SNMP”>“Users”， 显示如下窗口：

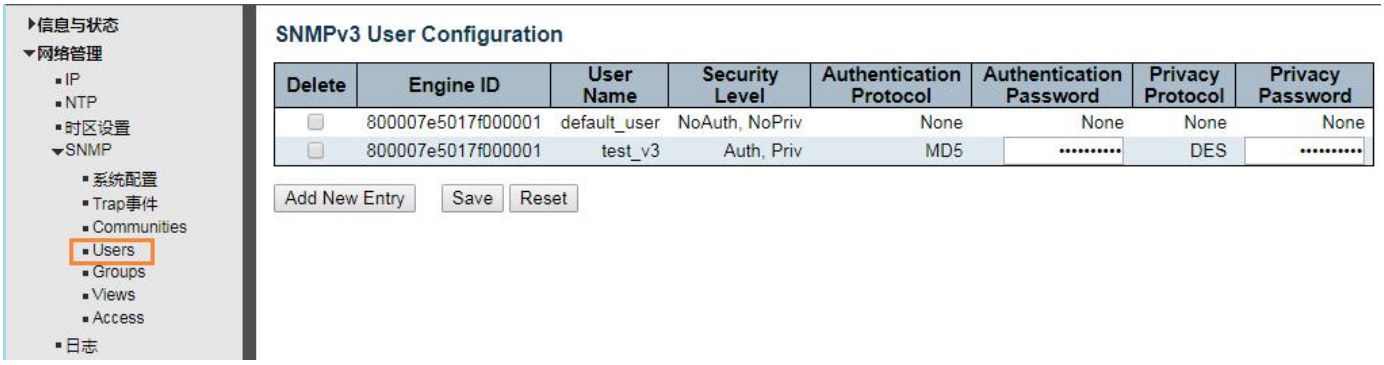


图 2-4-4 SNMPV3 用户添加窗口

配置字段的说明如下:

参数	说明
Engine ID	默认值 800007e5017f000001，建议使用交换机默认值
User Name	输入新增 SNMPv3 用户名称
Security Level	通过下拉菜单选择 NoAuth, NoPriv，Auth, NoPriv，Auth,Priv，三种加密方式
Authentication Protocol	通过下拉选择 MD5 SHA 加密协议
Authentication Password	输入加密密码
Privacy Protocol	通过下拉选择 DES AES 加密协议
Privacy Password	输入加密密码

单击“保存”令更改生效。

2.4.5 Views

用户可新建 SNMP v3 访问的视图。单击“网络管理”>“SNMP”>“Views”， 显示如下窗口：

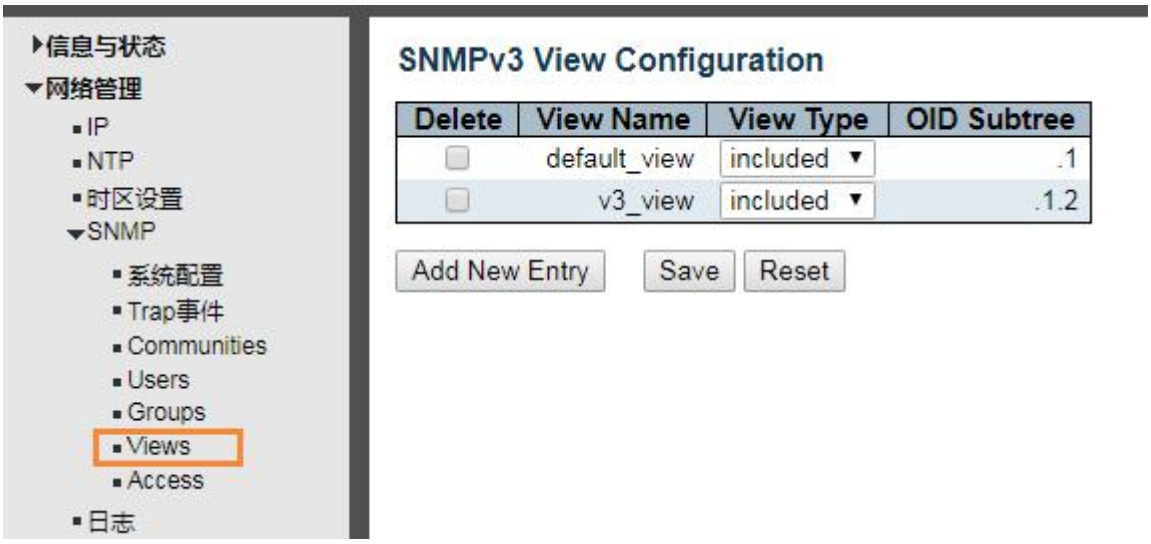


图 2-4-5 SNMPV3 视图添加窗口

配置字段的说明如下:

参数	说明
Views Name	输入视图的名称
Views Type	下拉菜单选择 included 和 excluded
OID Subtree	输入 OID 子树，例如.1.2

单击“保存”令更改生效。

2.4.6 Access

用户新建 Access 来调用已创建的 Views 视图。单击“网络管理”>“SNMP”>“Access”， 显示如下窗口：

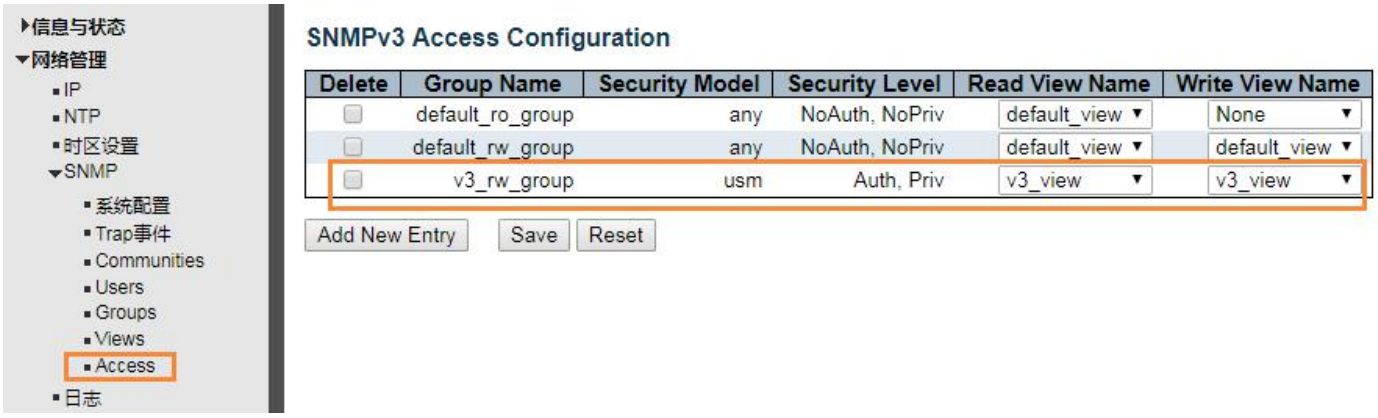


图 2-4-6 SNMPV3 Access 调用设置

配置字段的说明如下:

参数	说明
Group Name	输入新建组名称
Security Model	下拉选择 any v1 v2c usm
Security Level	下拉菜单选择 NoAuth, NoPriv，Auth, NoPriv，Auth,Priv，三种加密方式
Read View Name	下拉菜单选择已创建好的 views
Write View Name	下拉菜单选择已创建好的 views

单击“保存”令更改生效。

2.4.7 Groups

用户新建 Groups 来调用已创建的 Users 与 Access。单击“网络管理”>“SNMP”>“Groups”， 显示如下窗口:

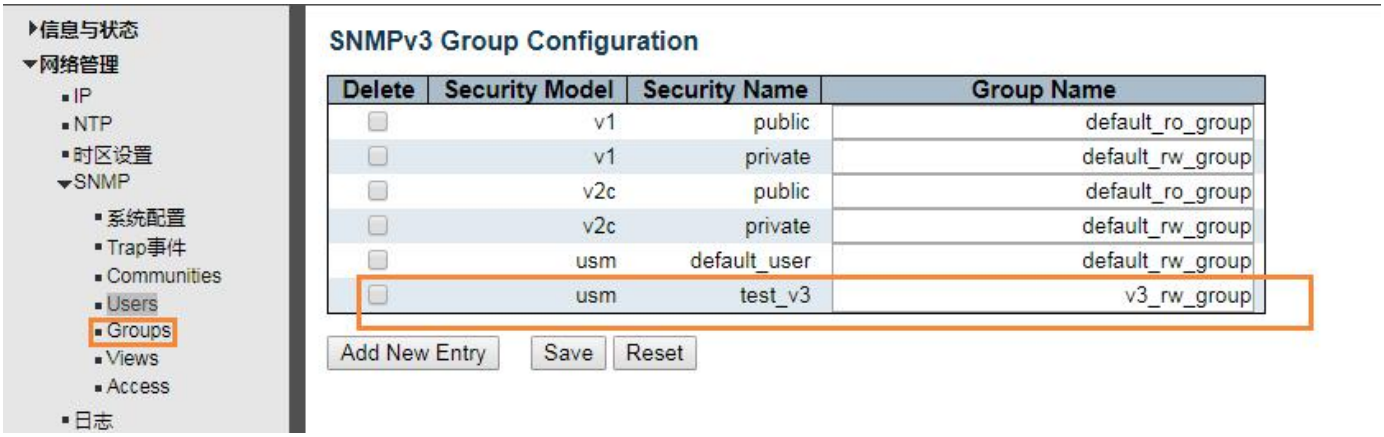


图 2-4-7 SNMPV3 Groups 调用设置

配置字段的说明如下:

参数	说明
Security Model	下拉选择 v1 v2c usm
Security Name	下拉选择已创建好的用户名，v1 v2c 下拉选择已创建好的团体名称，usm 下拉选择已创建好的用户名称
Group Name	输入已创建组名称

单击“保存”令更改生效。

2.4 日志配置

用户可配置交换机的系统日志。

单击 “网络管理” > “日志”， 显示如下窗口：

图 2-4 系统日志 设置窗口

配置字段的说明如下:

参数	说明
模式	选择启用或禁用系统日志功能。如果选择” Enabled”，交换机会将系统日志发送到指定的日志服务器
服务器 IP 地址	指定日志服务器的 IP 地址
日志级别	指定日志的级别, 可选的级别包括: **`Info`**: informations, warnings and errors. **`Warning`**: warnings and errors. **`Error`**: errors.

单击 “保存” 令更改生效。

3 端口配置

3.1 端口配置

该页面用于配置交换机端口的相关特性。

单击“端口配置”>“端口设置”，显示如下窗口:

图 3-1 端口设置窗口

配置字段的说明如下:

参数	说明
Link 状态	红色表示 Link Down, 橙色表示 Link Up
速率	选择端口的速率和全双工 / 半双工状态。 Disabled 表示禁用该端口. Auto 表示以全双工(FDX)或半双工模式(HDX)（1000mbps 总是在全双工模式下）在 10，100，1000Mbps 的设备之间自动商议。Auto 设置允许端口自动决定与该端口相连设备的最快设置，并能应用这些设置。 1000-X_AMS 表示该端口为光电复用, 光口优先. 其它选项是 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X。
流控(Flow Control)	显示用于各种端口配置的流控制机制。全双工端口使用 802.3x 流控制，半双工端口使用背压流控制。默认为禁用。 用户设置勾选表示启用流控.
最大帧长度	用于设置以太网最大的帧长度, 默认设置为 9600，即支持 Jumbo 帧.

单击“保存”令更改生效。

3.2 链路聚合

用户可以在多台交换机之间建立多条链路。链路聚合（Link Aggregation）是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽的一种方法。该交换机支持多达 13 个端口聚合组，每组中有 2 到 8 个端口。

注意：如果聚合组中的任一端口断开连接，发送到断开连接端口的数据包将与链路聚合组中连接的其它端口共享负载。

3.2.1 静态聚合设置

在此页面，用户可以配置交换机的端口静态聚合设置。

查看以下窗口，请单击”端口设置” > “链路聚合” > “静态聚合”，如下所示：

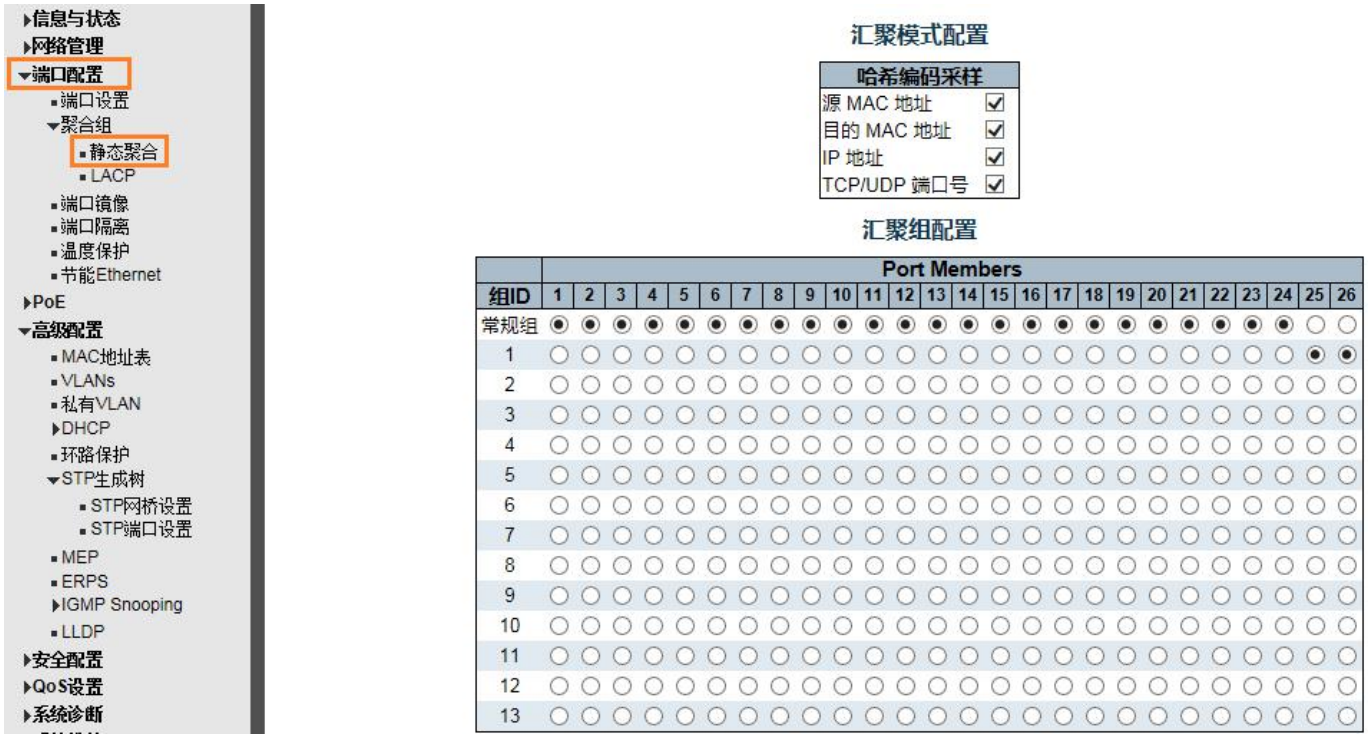


图 3-2-1 端口静态聚合设置窗口

可配置或显示的字段如下所述：

参数	说明
汇聚模式配置	该参数为链路聚合组中端口之间的流量哈希算法。

组 ID	静态聚合组 ID
成员端口(Port Members)	该交换机支持多达 13 个端口聚合组，每组中有 2 到 8 个端口.

单击“保存”按钮，接受各部分所做更改。

注意：一个静态 Trunk 组最多可以配置 8 个端口。

3.2.2 LACP 设置

用户可在交换机上创建动态聚合组。通过以下窗口，用户可以设置处理和发送 LACP 控制帧的主动或被动端口。

查看以下窗口，请单击“端口设置” > “链路聚合” > “LACP”，如下所示：

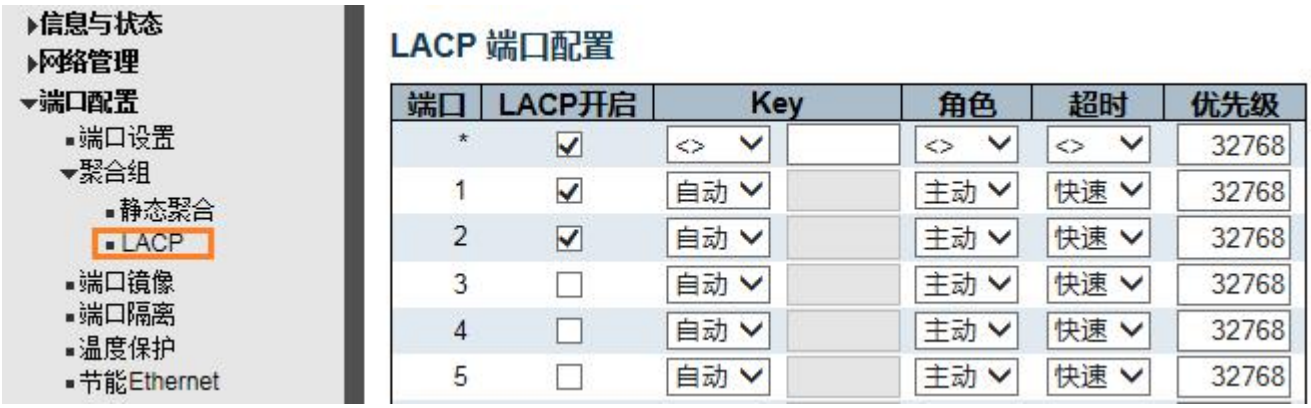


图 3-2-2 LACP 端口设置窗口

可配置的字段如下所述：

参数	说明
LACP 开启	启用或者禁用该端口的 LACP 功能.
Key	The Key value incurred by the port, range 1-65535 . The **Auto** setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the **Specific** setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
角色	The **Role** shows the LACP activity status. The **Active** will transmit LACP packets each second, while **Passive** will wait for a LACP packet from a partner (speak if spoken to).
超时	The **Timeout** controls the period between BPDU transmissions. **Fast** will transmit LACP packets each second, while **Slow** will wait for 30 seconds before sending a LACP packet.

优先级	The **Prio** controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

单击“保存”按钮，接受各部分所做更改。

3.3 端口镜像设置

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“目的端口”，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，但镜像目的端口只能配置一个。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。

要查看此窗口，请单击“端口设置”>“端口镜像设置”，如下所示：

图 3-3 端口镜像设置窗口

可配置或显示的字段说明如下：

参数	说明
镜像目的口	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. **Disabled** disables mirroring.
镜像源端口设置	Select mirror mode. **Rx only** Frames received on this port are mirrored on the **mirror port**. Frames transmitted are not mirrored. **Tx only** Frames transmitted on this port are mirrored on the **mirror port**. Frames received are not mirrored. **Disabled** Neither frames transmitted nor frames received are mirrored.

	Enabled Frames received and frames transmitted are mirrored on the **mirror port**. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror **mirror port** Tx frames. Because of this, **mode** for the selected **mirror port** is limited to **Disabled** or **Rx only**.

单击“保存”按钮接受所做的更改。

注意：您不能将快速端口镜像到一个低速的端口。例如，如果您尝试从 100 Mbps 端口镜像流量到一个 10 Mbps 端口，这可能会导致吞吐量问题。需复制帧的端口应始终支持比发送副本的端口具有相同或更低的速度。请注意，目标端口和源端口不能为同一端口。

3.4 温度保护设置

温度保护用于检测与保护交换机的工作, 当交换机检测到端口的工作温度高于设定的保护温度时，系统会采取禁用端口的方式来保护交换机。

单击“系统配置”>“温度保护”, 显示如下窗口:

图 3-4 温度保护设置窗口

配置字段的说明如下:

参数	说明
优先组的温度设置	该交换机支持 4 个温度保护优先级, 支持为不同的优先级组设置保护温度
端口优先级	指定该端口所属的优先级组

单击“保存”令更改生效。

注意：出厂默认下, 交换机所有端口属于优先级组 0，优先级组 0 的保护温度为 250 摄氏度.

3.5 温度告警设置

该窗口允许用户配置系统温度告警参数。

单击“系统配置”>“温度告警设置”, 显示如下窗口:

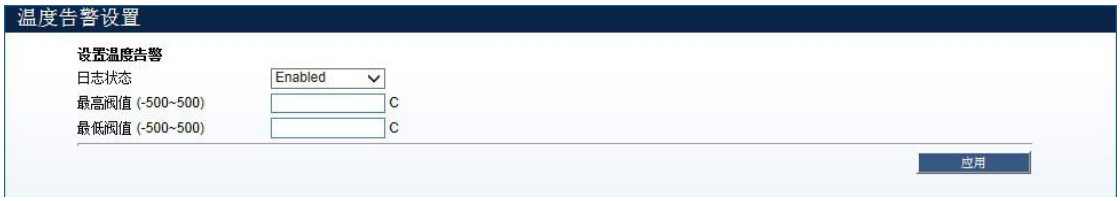


图 3-5 温度告警设置窗口

配置字段的说明如下:

参数	说明
日志状态	使用下拉菜单启用或禁用告警温度设置的日志状态选项。
最高阈值 (-500-500)	输入告警温度设置的最高阈值。
最低阈值 (-500-500)	输入告警温度设置的最低阈值。

单击“应用”令更改生效。

4 高级配置

4.1 VLAN

虚拟局域网 VLAN（Virtual Local Area Network）在逻辑上将一个局域网 LAN（Local Area Network）划分成多个子集，每个子集形成各自的广播域。简单地说，VLAN 是将一个物理的 LAN 在逻辑上划分成多个广播域（多个 VLAN）的通信技术。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通，从而将广播报文限制在一个 VLAN 内。由于 VLAN 间不能直接互访，因此提高了网络安全性。

单击“高级配置”>“VLANs”，查看 802.1Q VLAN 设置窗口，如下所示：

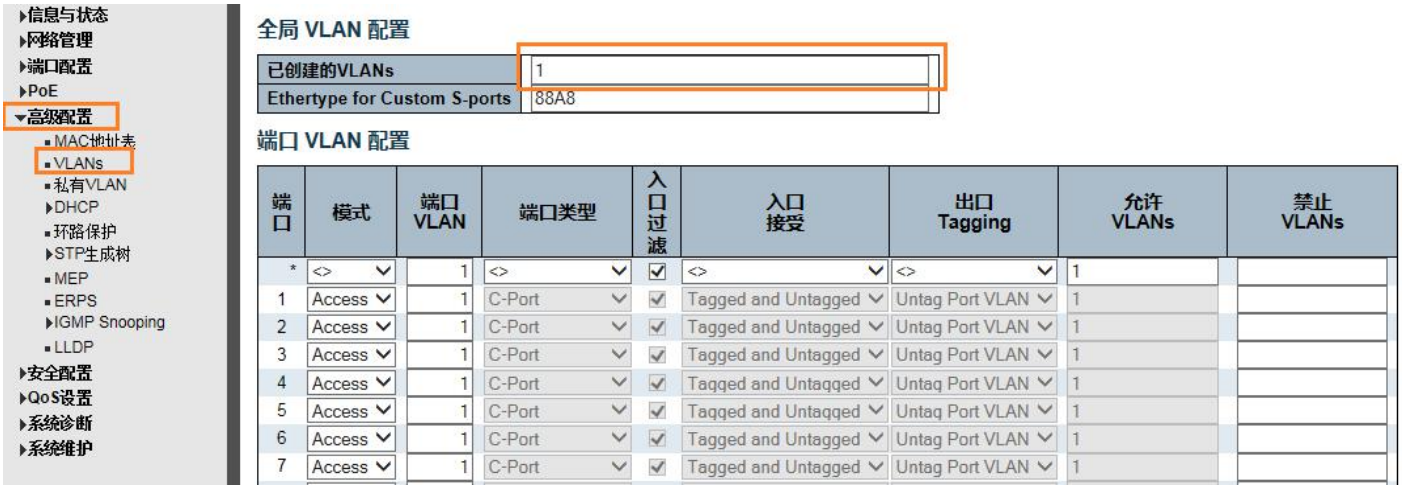


图 4-1 802.1Q VLAN 设置

参数	说明
已创建的 VLANs	显示已创建 VLAN 的 VLAN ID 列表，出厂默认时，系统只创建 VLAN 1。 如需创建新的 VLAN，请在此添加 VLAN ID。
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
模式	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. **Access:** Access ports are normally used to connect to end stations. Access ports have the following

	characteristics: • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN • On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged **Trunk:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: • By default, a trunk port is member of all VLANs (1-4094) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress • Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress **Hybrid:** Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware • Ingress filtering can be controlled • Ingress acceptance of frames and configuration of egress tagging can be configured independently
端口 VLAN(Port VLAN)	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
端口类型(Port Type)	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. **S-Custom-Port:**

	On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
入口过滤(Ingress Filter)	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.。
入口接受(Ingress Acceptance)	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. **Tagged Only** Only tagged frames are accepted on ingress. Untagged frames are discarded. **Untagged Only** Only untagged frames are accepted on ingress. Tagged frames are discarded.
出口 Tagging(Egress Tagging)	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
允许 VLANs(Allowed VLANs)	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to `1-4094`. The field may be left empty, which means that the port will not become member of any VLANs.
Forbidden VLANs	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.
非静态端口	单击单选按钮后，指定该端口为非静态端口。单击“全选”按钮表示选中所有端口。

单击“保存”让更改生效。

4.2 端口隔离

端口隔离用于限制端口之间的数据流。端口隔离方法与使用 VLAN 来限制流量相似，但是更加严格。

4.2.1 端口分组

该交换机可以支持将端口分组，组内的成员端口之间可以转发数据流。

注意:端口可以同时属于多个端口组，任意两个端口只要属于任意一个端口组，两个端口之间即可以转发数据流。

要查看此窗口，单击“端口设置”>“端口隔离”，如下图所示:

图 4-2-1 端口分组设置

4.2.2 端口隔离

要查看此窗口，单击“高级设置”>“端口隔离”> “端口隔离”，如下图所示:

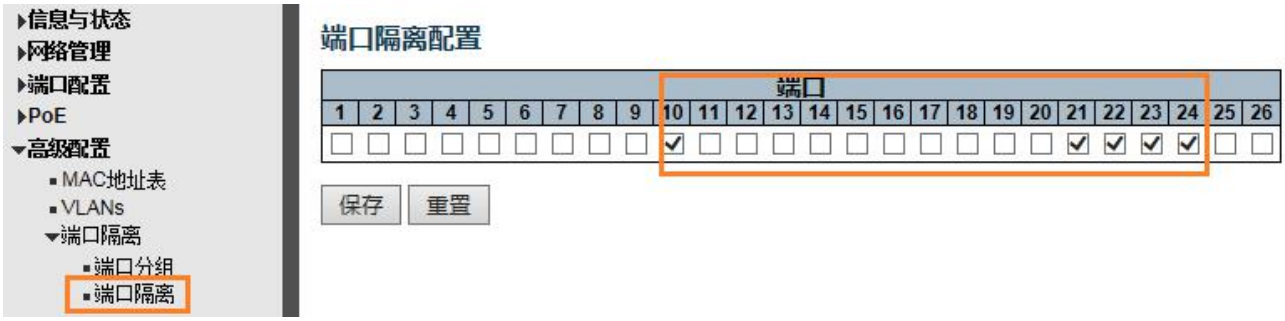


图 4-2-2 端口隔离设置窗口

可配置字段说明如下:

参数	说明
端口列表	所有勾选的端口之间不允许转发数据流。

单击“保存”按钮，接受所做更改。

4.3 STP

生成树协议（STP）设计用于在网络上减少链路失效并防止环路为网络提供防护。在复杂结构网络中很容易产生无意识的环路广播风暴。交换机的 STP 功能缺省时为启用。交换机支持三种版本的生成树协议：STP、RSTP、MSTP。

4.3.1 STP 全局设置

在此页面，用户可以配置 STP 网桥的全局参数。

查看以下窗口，请单击 “高级配置” > “STP 生产树” > “STP 网桥设置”，如下所示：

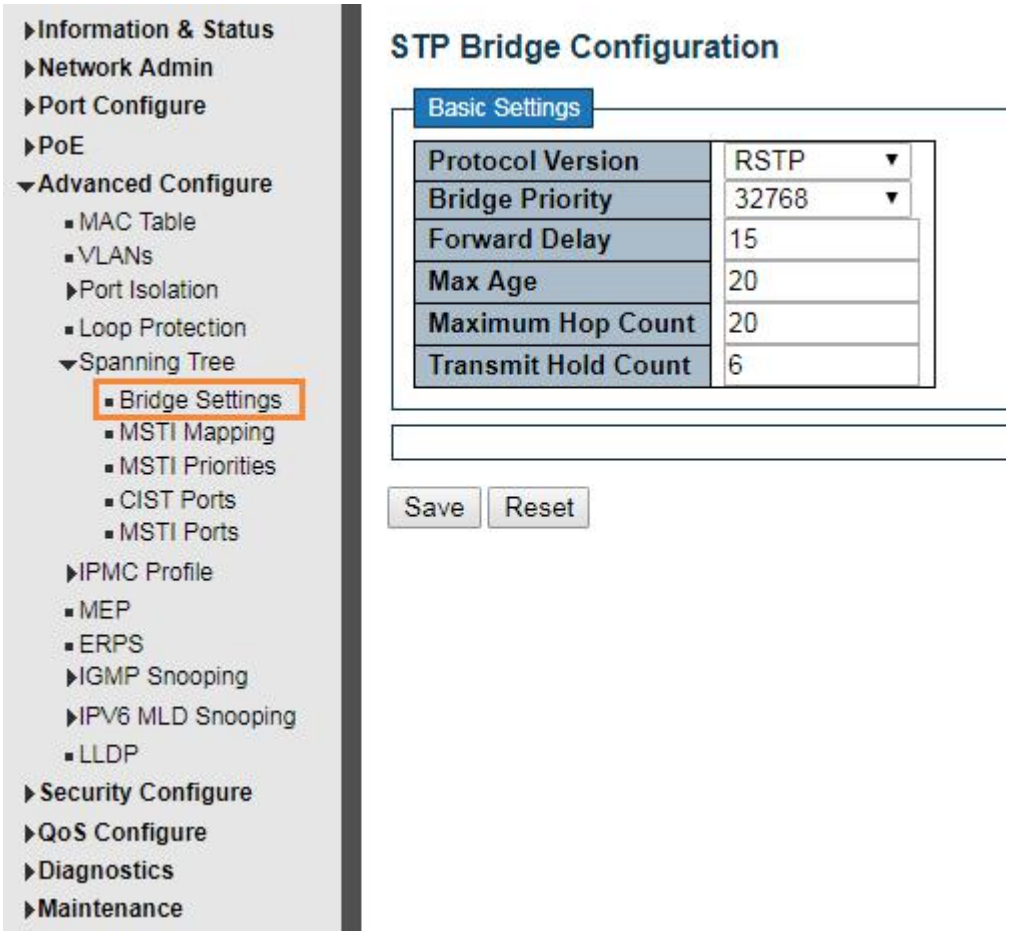


图 4-3-1 STP 全局设置窗口

可配置的字段如下所述：

参数	说明
协议版本	使用下拉菜单选择要在交换机上执行的 STP 版本，包括： STP - 选择此参数，在交换机上全局设置生成树协议（STP）。 RSTP - 选择此参数，在交换机上全局设置快速生成树协议（RSTP）。 MSTP-选择此参数，在交换机上全局设置多生成树协议（MSTP）。

Bridge Priority	控制该 STP 网桥的优先级，越低的数字代表越高的优先级。 Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.
转发延迟时间 Forward Delay（4-30）	转发延迟的设置范围为 4 至 30 秒。默认值为 15 秒。
最大生产时间 Max Age ((6-40)	设置最大老化时间可以确保旧信息不会在网络的冗余路径中无休止的循环，从而阻止新信息的有效传播。默认值为 20。
最大跳数（6-40）	用于设置在交换机发送的 BPDU（网桥协议数据单元）数据包被丢弃之前生成树区域中设备之间的跳数。数据包每经过一台交换机跳数将减少一跳，直到跳数值为 0。用户可以设置的跳数值为 6 至 40。默认值为 20。
发包速率限制(Transmit Hold Count)（1-10）	用于设置每个时间间隔所传输 Hello 数据包的最大数量。该数值范围为 1 至 10。默认值为 6。

单击“保存”按钮，接受对各部分所做的更改。

4.3.2 MSTI Mapping

在此页面，用户可以配置实例映射。

查看以下窗口，请单击 “高级配置” > “STP 生成树” > “MSTI”，如下所示：

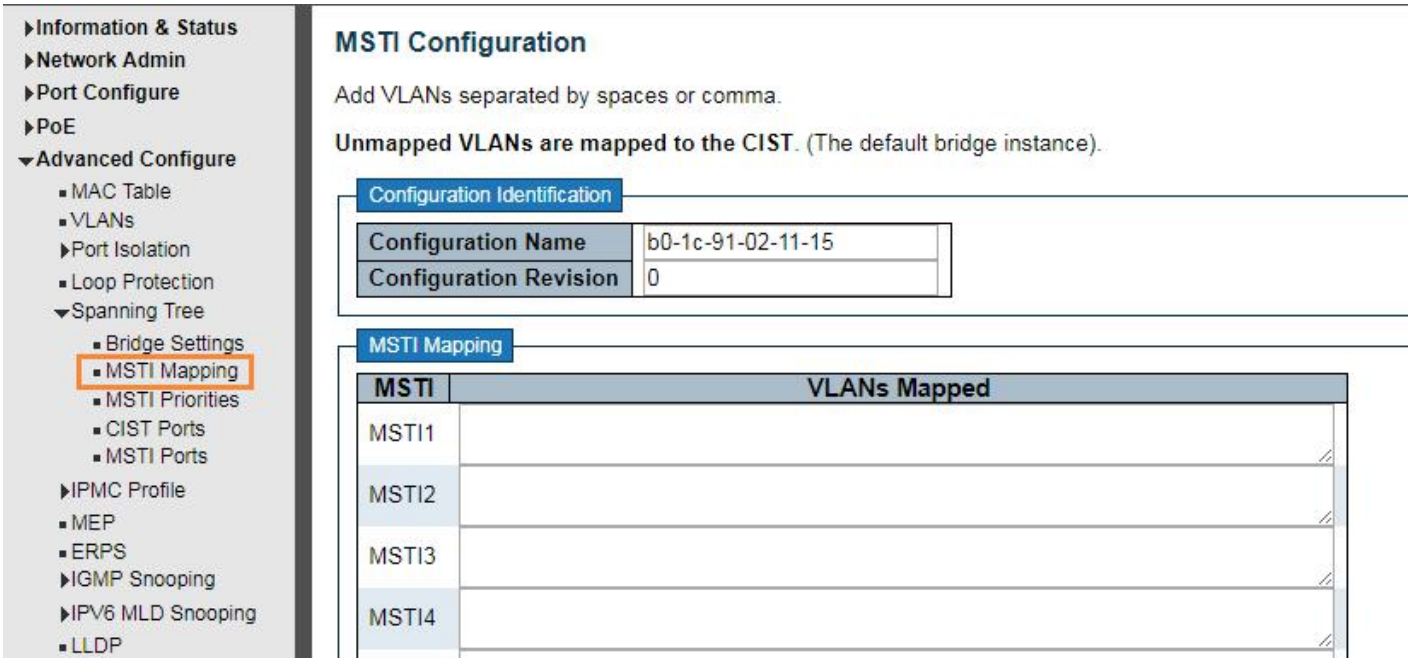


图 4-3-2 MSTI Mapping 设置窗口

可配置的字段如下所述：

参数	说明
Configuration Name	配置 MSTP 的域名

Configuration Revision	配置 Configuration Revision
MSTI Mapping	输入需要映射的 vlan

单击“保存”按钮，接受对各部分所做的更改。

注意:当选择配置 MSTP，环内的交换机需要做 Configuration Name，Configuration Revision 相同的配置.

4.3.3 MSTI Priorities

在此页面，用户可以配置实例映射。

查看以下窗口，请单击 “高级配置” > “STP 生成树” > “MSTI Priorities”，如下所示:

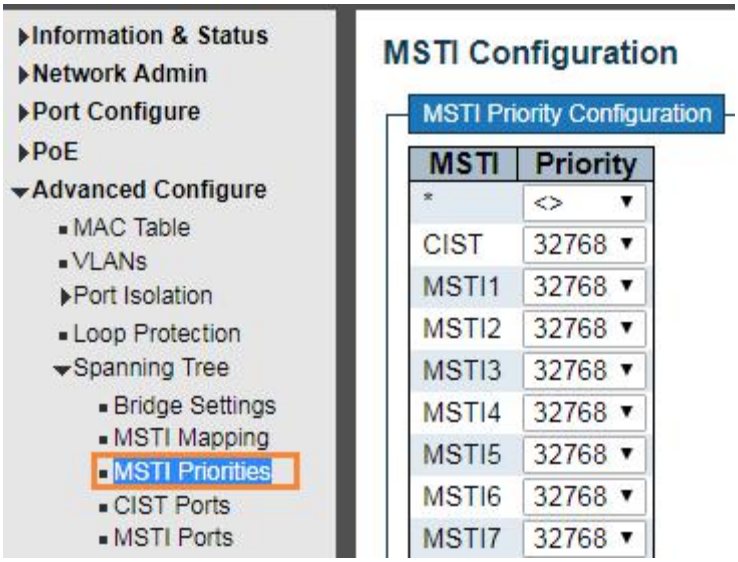


图 4-3-3 MSTI Priorities 设置窗口

可配置的字段如下所述:

参数	说明
MSTI Priorities	配置实例优先级，范围是 0-61440

单击“保存”按钮，接受对各部分所做的更改。

注意:配置实例优先级必须是 4094 的倍数，选择范围是 0-61440.

4.3.4 STP 端口设置

请单击 “高级设置” > “STP 生成树” > “STP 端口设置”，如下所示：

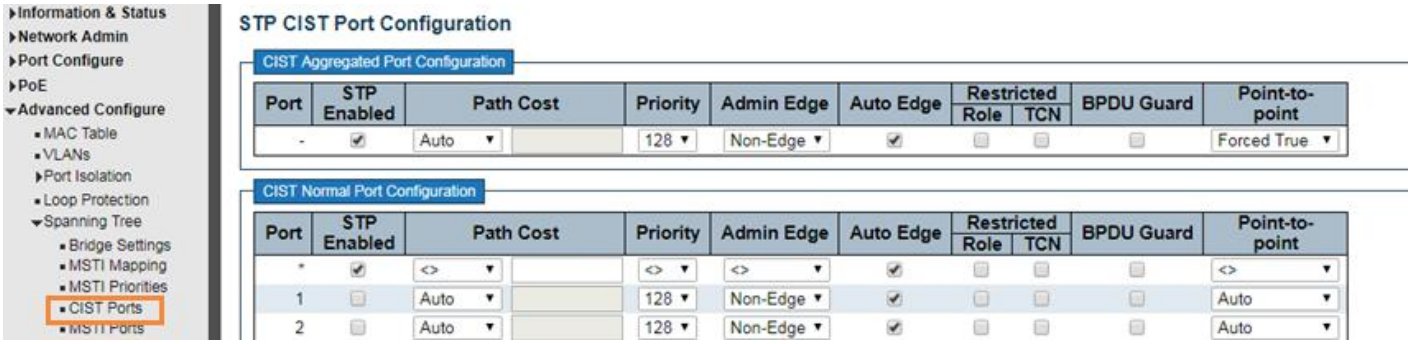


图 4-3-4 STP 端口设置窗口

可配置的字段如下所述：

参数	说明
环网启用	勾选表示启用该端口的 STP 功能。
路径开销（0=Auto）	用于定义一个度量值，表示转发数据包到指定端口列表的相关开销。端口开销可被自动设置或设置为一个度量值。默认值为 0（自动）。数字越低，选择该端口来转发数据包的可能性就更大。 Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
优先级	当端口的路径开销一样时，优先级用来判决端口的转发状态。
自动边界	选择 True 参数，可将端口指定为边界端口。选择“False”表示该端口不具有边界端口状态。另外，也可以选择“Auto”选项，选择”Auto”时，会根据端口是否收到 BPDU 报文来确定是否是边界端口。
端口角色限制(Restricted Role)	使用下拉菜单，选择 True 和 False 之间切换端口角色限制。如果设置为“True “，端口不会被选定为根端口。默认为”False”。
限制拓扑变化通知(Restricted TCN)	拓扑变化通知是网桥发送到其根端口的一个简单 BPDU，用于通知拓补变化。模式可在 True 和 False 之间切换。默认为“False”。
BPDU 保护	如果开启该功能，端口收到 BPDU 报文时，会进入 Disable(Shut Down)状态。

点对点	选择 True 表示点到点共享链路。P2P 端口类似于边缘端口。此参数的默认设置为“Auto”。

单击“保存”按钮，接受各部分所做更改。

4.3.5 MSTI Ports

用户可配置实例端口的优先级以及路径开销。

请单击 “高级设置” > “STP 生成树” > “MSTI Ports”，如下所示：

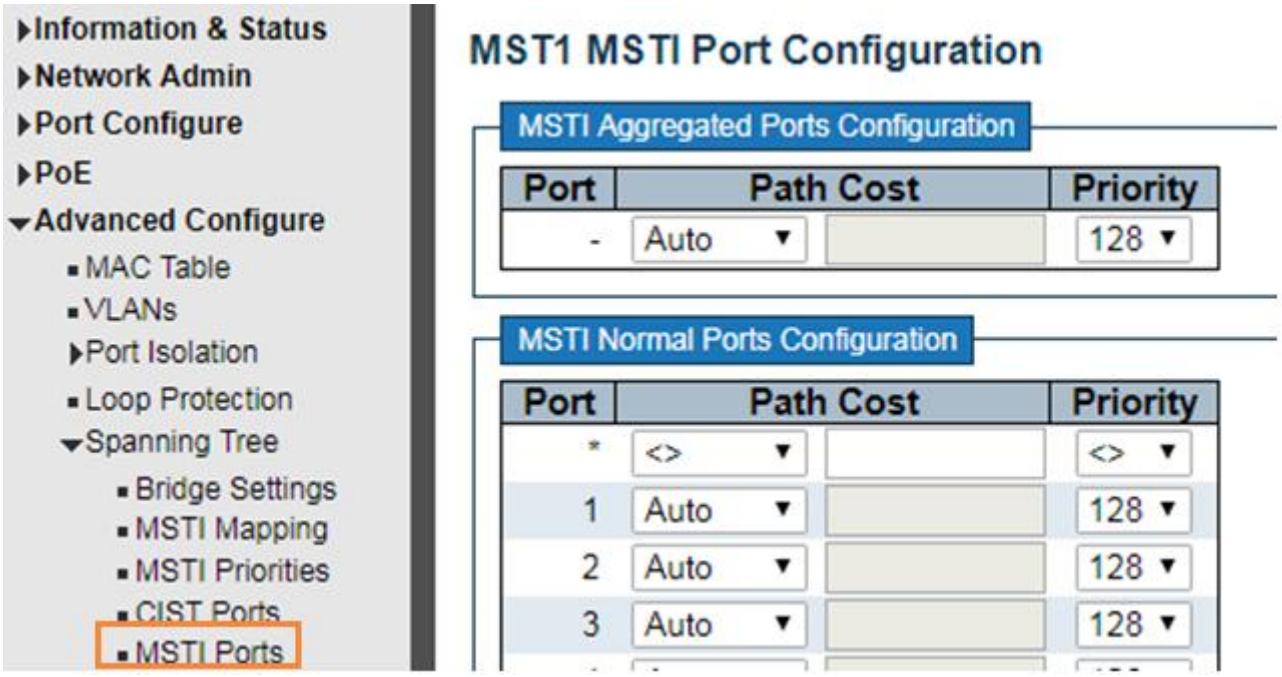


图 5-3-5 MSTI Ports 设置窗口

可配置的字段如下所述：

参数	说明
路径开销	用于定义一个度量值，表示转发数据包到指定端口列表的相关开销。端口开销可被自动设置或设置为一个度量值。默认值为 0（自动）。数字越低，选择该端口来转发数据包的可能性就更大。 Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
优先级	当端口的路径开销一样时，优先级用来判决端口的转发状态。

4.4 MAC 地址表

用户可以在交换机上配置 MAC 地址表相关的设置。

查看以下窗口，请单击 “高级设置” > “MAC 地址表”，如下所示：

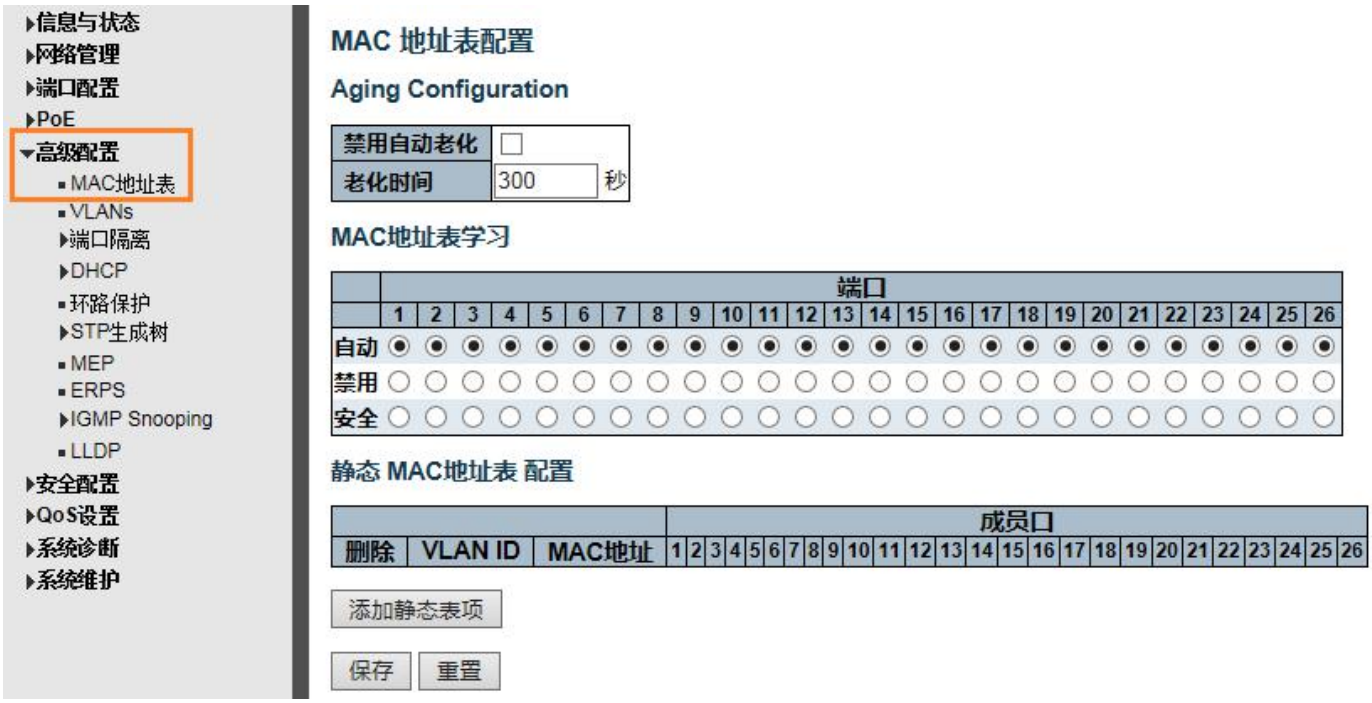


图 4-4 MAC 地址表设置窗口

可配置的字段如下所述：

参数	说明
禁用自动老化	如果勾选禁用自动老化，那么交换机学习的动态 MAC 地址将不会老化。
老化时间	出厂默认时，交换机学习的动态 MAC 地址在 300s 后将会被自动老化。允许的老化时间范围为 10-1000000 秒。
MAC 地址表学习	交换机支持 3 种 MAC 地址学习模式： 1. 自动，该模式下，端口将自动学习 MAC 地址。 2. 禁用，该模式下，端口将不学习 MAC 地址。 3. 安全，该模式下，端口只转发已配置静态 MAC 地址(源 MAC 地址)的数据流。

单击“保存”按钮，接受各部分所做更改。

4.5 IGMP Snooping

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP 侦听）是工作在二层以太网交换机上的组播管理和控制机制。

当启用了 IGMP Snooping，交换机通过侦听每个接口上接收到的 IGMP 报文，为交换机接口和组播组地址建立映射关系，并根据建立的映射关系来转发组播数据流。

4.5.1 基本配置

单击 “高级配置” > “IGMP Snooping” > “基本设置”，可查看交换机的 IGMP Snooping 基本配置信息，如下所示：

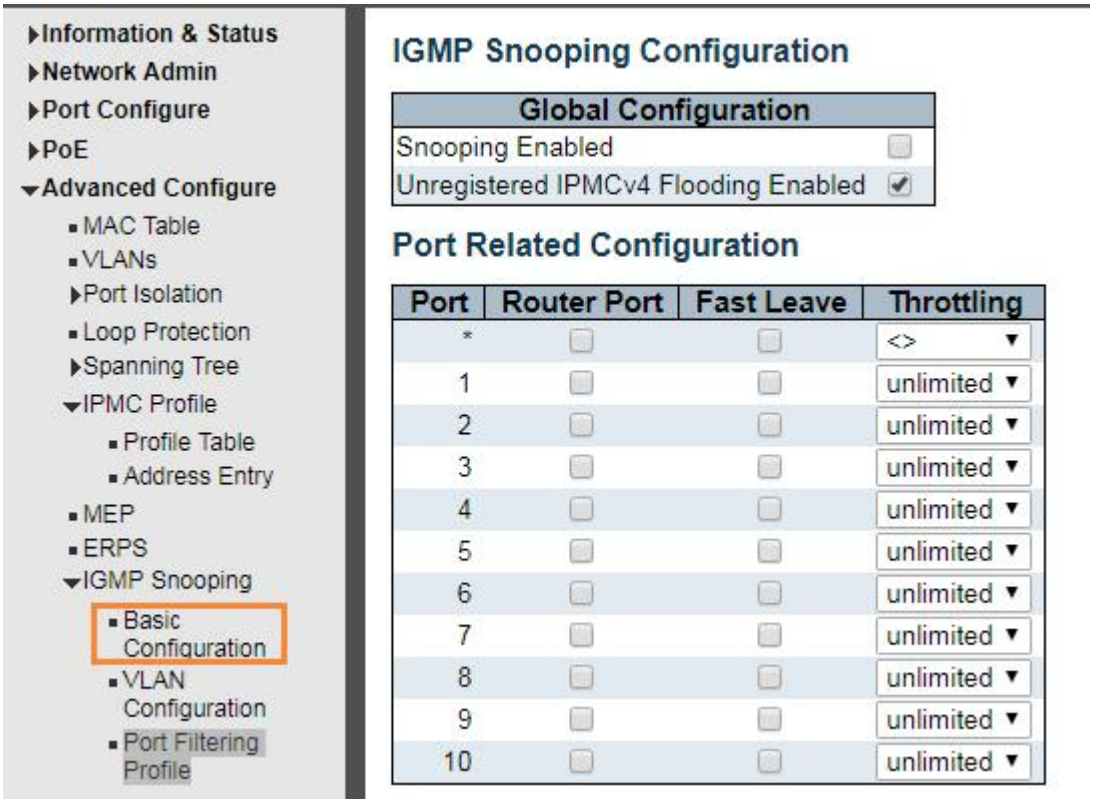


图 4-5-1 IGMP Snooping 基本配置

可配置的字段如下所述：

参数	说明
启用 Snooping	启用或禁用 IGMP Snooping 状态。

允许未注册 IPMCv4 泛洪	
路由端口	路由端口是指连接 3 层组播路由器或者 IGMP querier 的端口。 Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
快速离开	Fast leavePerforms deleting MAC forward entry immediately upon receiving message for group de-registration

单击“保存”按钮让更改生效。

4.5.2 VLAN 配置

单击 “高级配置” > “IGMP Snooping” > “VLAN 设置”，可查看交换机的 IGMP SnoopingVLAN 配置信息，

如下所示：

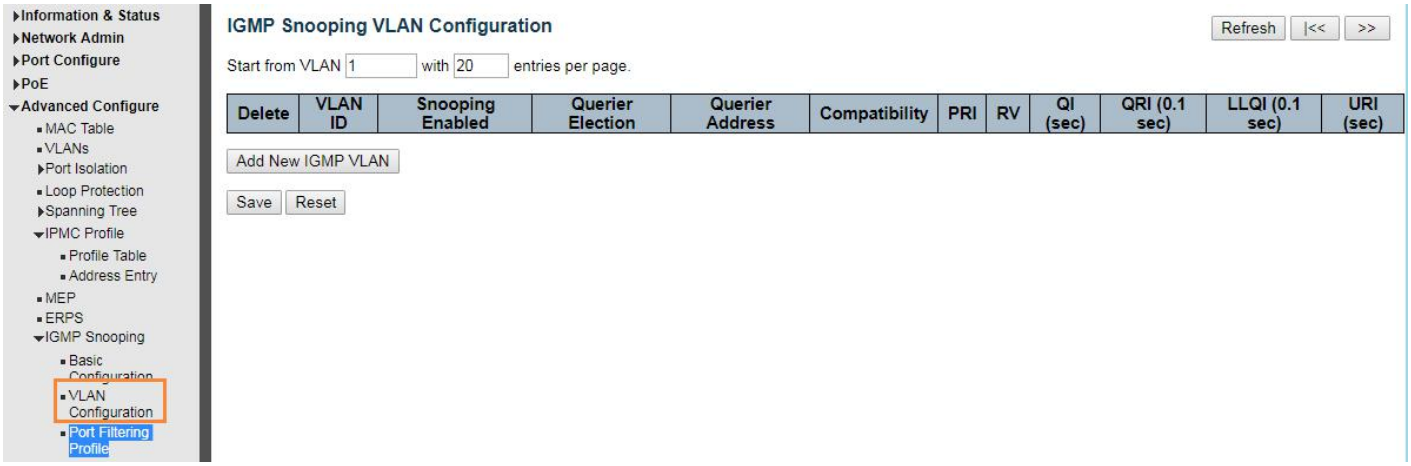


图 4-5-2 IGMP Snooping VLAN 配置

可配置的字段如下所述：

参数	说明
VLAN ID	
开启 Snooping	启用或者禁用基于 VLAN 的 IGMP Snooping。系统最大支持在 32 个 VLAN 上启用 IGMP Snooping。 Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier 竞选（Querier Election）	启用或者禁用 IGMP Querier 竞选 Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier 地址（Querier Address）	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

单击“保存”按钮让更改生效。

4.5.3 Port Filtering Profile

单击 “高级配置” > “IGMP Snooping” > “Port Filtering Profile”，可以调用 IPMC Profile 已配置好的组播列表

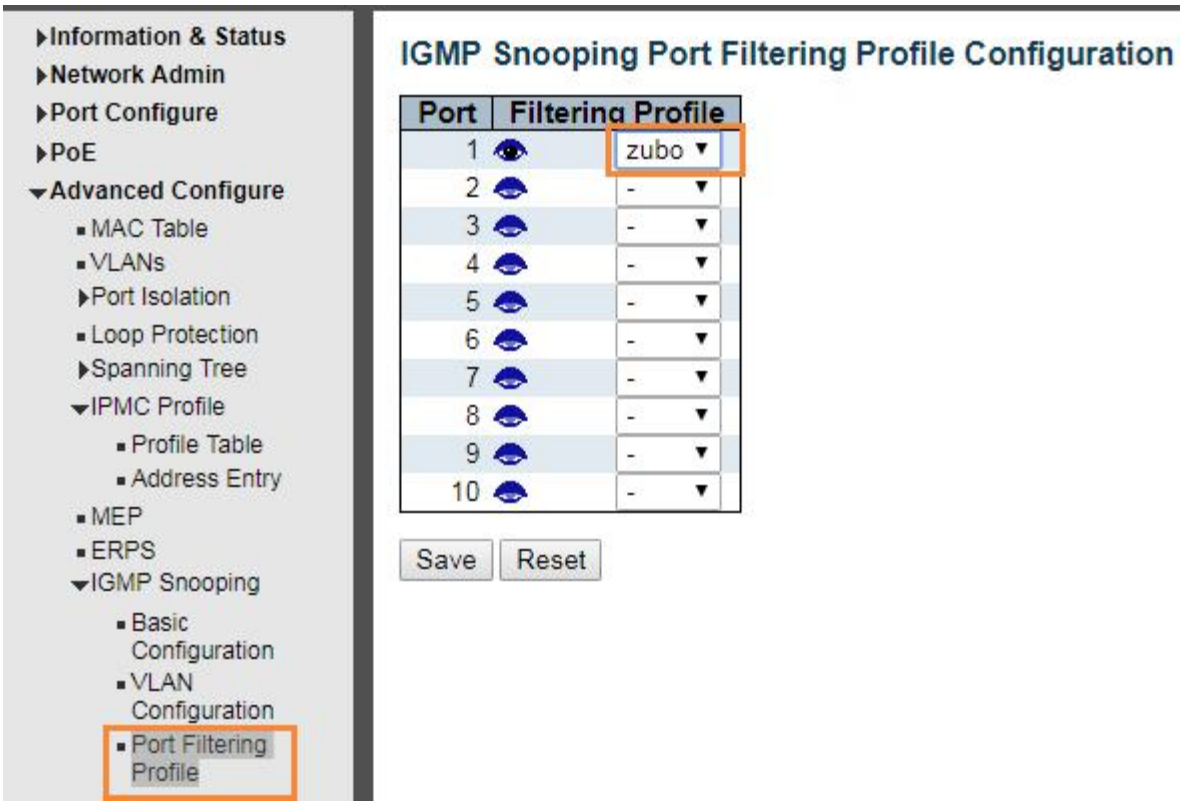


图 4-5-3 Port Filtering Profile 配置

可配置的字段如下所述：

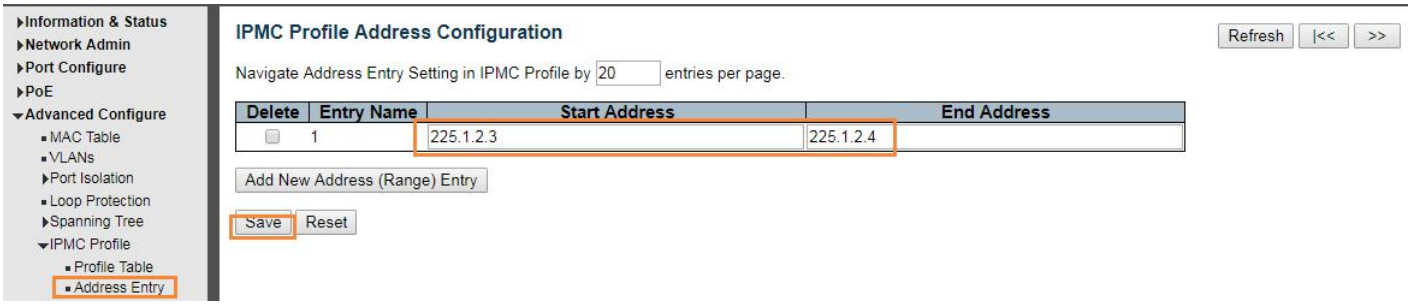
参数	说明
VLAN ID	
开启 Snooping	启用或者禁用基于 VLAN 的 IGMP Snooping。系统最大支持在 32 个 VLAN 上启用 IGMP Snooping。 Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier 竞选（Querier Election）	启用或者禁用 IGMP Querier 竞选 Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier 地址（Querier Address）	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

单击“保存”按钮让更改生效。

4.6 IPMC Profile

用户可配置过滤组播列表

单击 “高级配置” > “IPMC Profile” > “Address Entry”，如下所示：



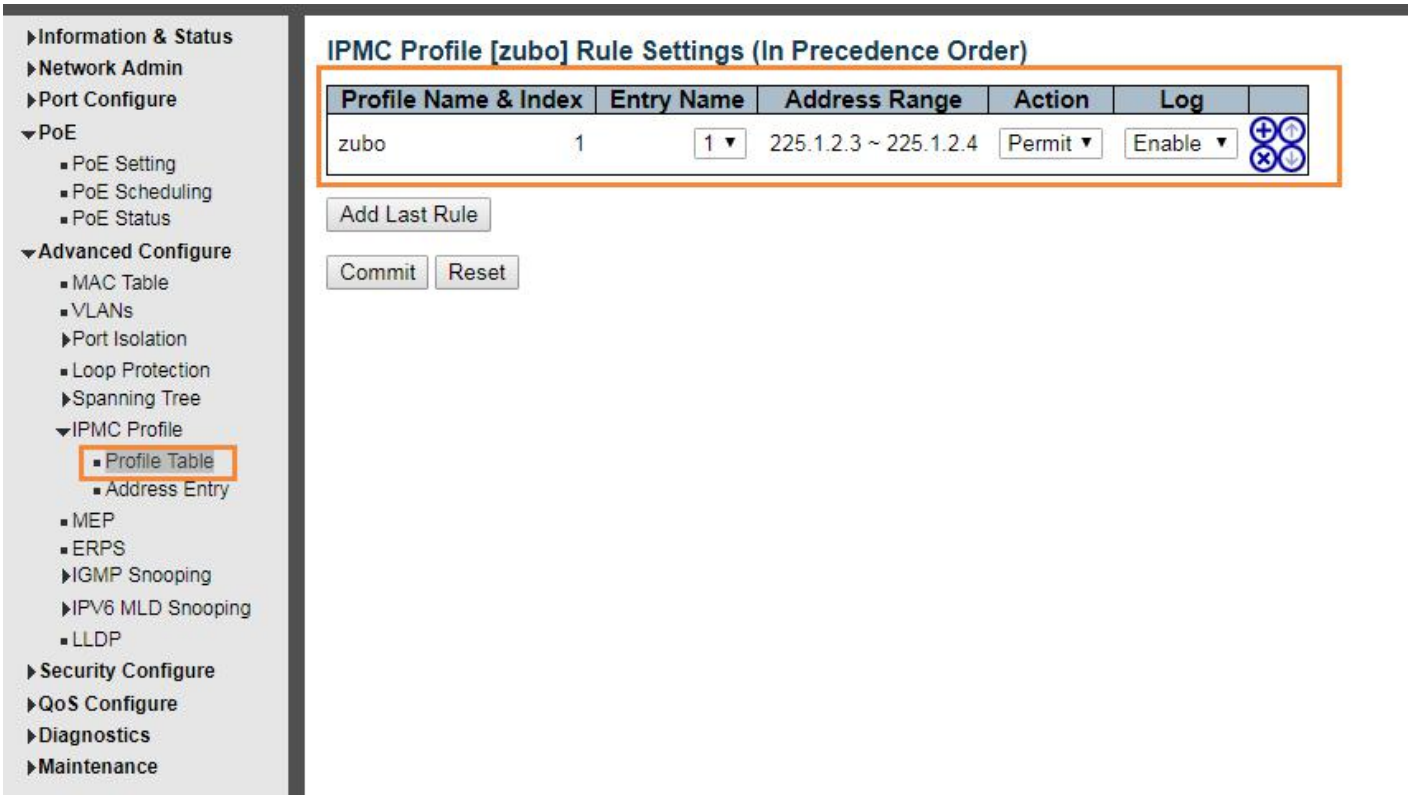
可配置的字段如下所述：

参数	说明
Entry Name	输入需要过滤的组播名称
Start Address	输入开始的组播地址
End Address	输入结束的组播地址

单击“保存”按钮让更改生效。

绑定过滤组播列表

单击 “高级配置” > “IPMC Profile” > “Profile Table”，如下所示：



参数	说明
Entry Name	下拉菜单选择已创建的 Address Entry
Action	下拉选择 Deny 或者 Permit
Log	下拉选择 disable 或者 enable

4.7 IPV6 MLD Snooping

IPV6 MLD Snooping 是工作在二层以太网交换机上的组播管理和控制机制。

当启用了 IPV6 MLD Snooping，交换机通过侦听每个接口上接收到的 IPV6 MLD 报文，为交换机接口和组播组地址建立映射关系，并根据建立的映射关系来转发组播数据流。

4.7.1 基本配置

单击 “高级配置” > “IPV6 MLD Snooping” > “基本设置”，可查看交换机的 IPV6 MLD Snooping 基本配置信息，如下所示：

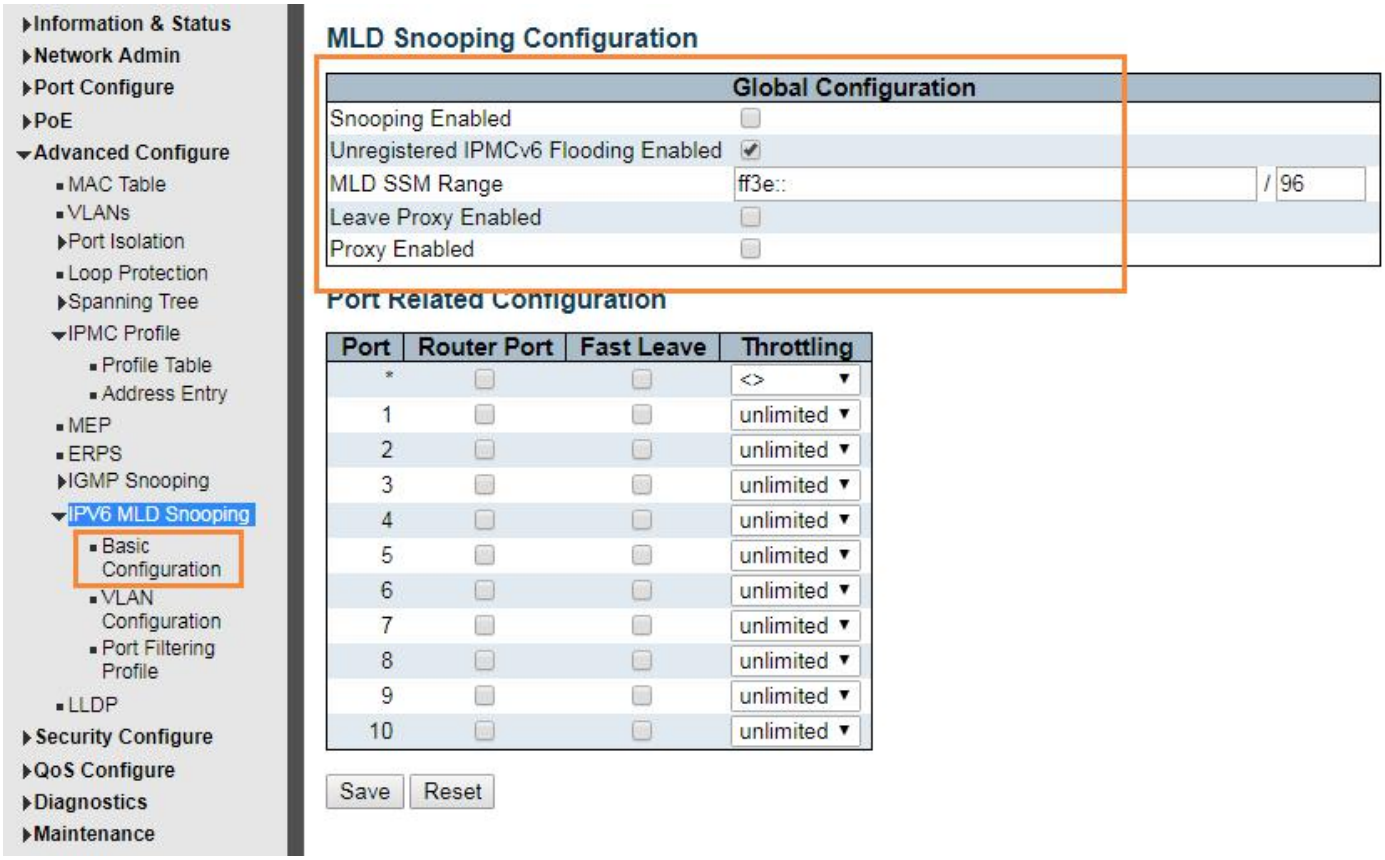


图 4-7-1 IGMP Snooping 基本配置

可配置的字段如下所述：

参数	说明
启用 Snooping	启用或禁用 IGMP Snooping 状态。
允许未注册 IPMCv6 泛洪	
路由端口	路由端口是指连接 3 层组播路由器或者 IGMP querier 的端口。 Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
快速离开	Fast leavePerforms deleting MAC forward entry immediately upon receiving message for group de-registration

单击“保存”按钮让更改生效。

4.7.2 VLAN 配置

单击 “高级配置” > “IPV6 MLD Snooping” > “VLAN 设置”，可查看交换机的 IPV6 MLD Snooping 配置信息，如下所示：

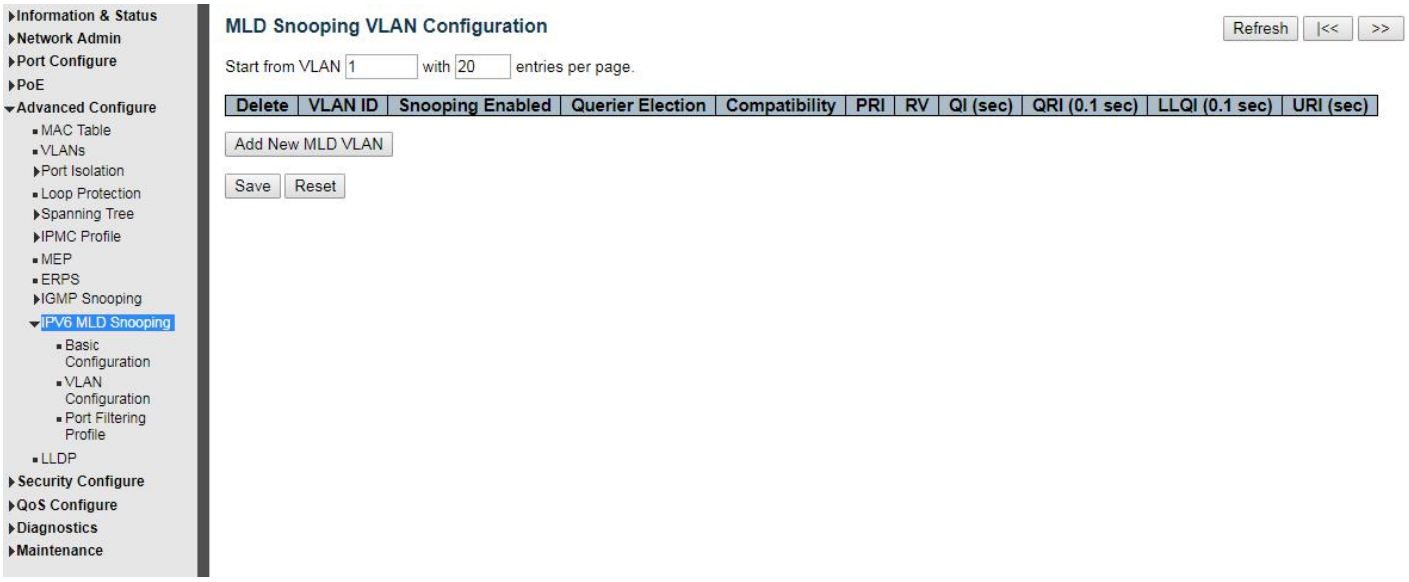


图 4-7-2 IPV6 MLD Snooping 配置

可配置的字段如下所述：

参数	说明
VLAN ID	
开启 Snooping	启用或者禁用基于 VLAN 的 MLD Snooping。系统最大支持在 32 个 VLAN 上启用 MLD Snooping。 Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier 竞选（Querier Election）	启用或者禁用 MLD Querier 竞选 Enable to join MLD Querier election in the VLAN. Disable to act as an MLD Non-Querier.

单击“保存”按钮让更改生效。

4.8 ERPS

ERPS（以太网环保护切换）是针对以太网环保护切换的首个行业标准（ITU-T G.8032）。它通过成熟的以太网操作维护管理（OAM）功能，以及以太网环网络的简单自动保护切换（APS）协议进行整合。ERPS 可为环形拓扑中的以太网流量提供小于 50ms 的路径保护。这确保了以太网层中不会形成环路。

在一个环中，ERPS 初始状态下阻塞 RPL 链路，防止环路形成，当链路发送故障时，通过保护切换功能恢复 RPL 链路连接，并在故障排除后再次阻塞 RPL 链路

ERPS 术语和概念

RPL（环保护链路）——空闲状态时被阻塞，指定用以防止在环上形成环路的链路。

RPL 拥有节点(RPL Owner)——连接到 RPL 的节点，用于空闲状态时阻塞 RPL 上的流量，以及在保护状态时解除阻塞。

RPL 邻居节点(RPL Neighbor)——与 RPL Owner 节点直接连接的链路节点。

R-APS（环-自动保护切换）——Y.1731 和 G.8032 定义的协议消息，用于通过 RAPS VLAN（R-APS 信道）功能协调环上的保护过程。

受保护的 **VLAN**——业务流量 VLAN，用于传输正常的网络流量。

注意：在启用 ERPS 之前，应在环端口上禁用 STP .

要查看下面的窗口，请点击“高级配置”>“ERPS ”，如下述：

图 4-8-1EPRS 设置

可配置的字段如下所述：

参数	说明
Ring ID	ERPS Ring 保护实例 ID
东向 Port(East Port)	东向端口，选择交换机中参与 Ring 保护的端口号
西向 Port(West Port)	西向端口，选择交换机中参与 Ring 保护的另一个端口号
Ring 类型	可选“ 主 Ring”或者“子 Ring “只有存在多环应用时，才需要配置”子 Ring “。默认 Ring 类型为”主 Ring “

互连节点	在多环(Multi Ring)应用中，同时连接 2 个或者多个环(Ring)的节点即为互连节点。
主 Ring ID	在单环(Single Ring)应用中，主 Ring ID 与 Ring ID 一致。 在多环(Multi Ring)应用中，子 Ring 必须填写主 Ring ID。
R-APS VLAN（1-4094）	指定将用作 R - APS VLAN 的 VLAN.

单击“创建新的 Ring 实例”按钮，即可添加新的 ERPS Ring 保护实例。

单击“保存”按钮，接受所做的更改。

单击“Ring ID”列中的链接，即可进入编辑 ERPS Ring 具体配置，将出现以下窗口：

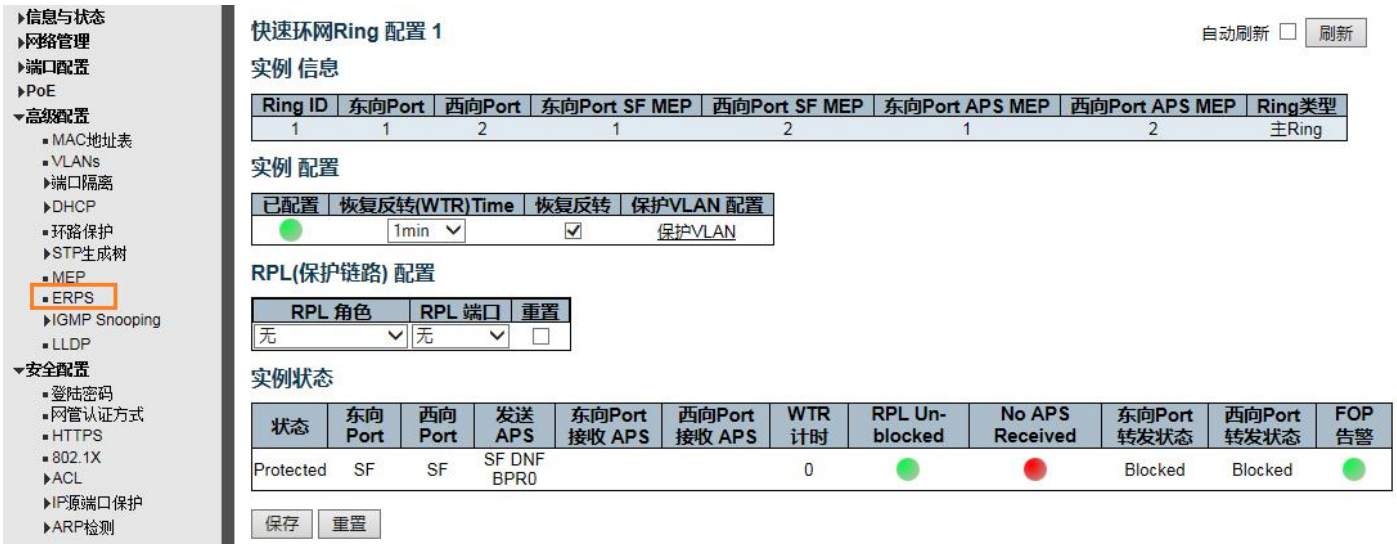


图 4-8-2EPRS 实例信息

参数	说明
WTR 时间（5-12）	勾选该复选框并输入 R-APS 功能的 WTR 时间，默认的 WTR 时间是 1 分钟。
恢复反转模式	勾选该复选框并使用下拉菜单，启用或禁用 R-APS 恢复选项的状态。
保护 VLAN	单击“保护 VLAN”连接，可进入并编辑受保护的 VLAN 组。
RPL 角色	使用下拉菜单，可选择”无”，” RPL Owner “，” RPL Neighbor “角色
RPL 端口	使用下拉菜单，可选择”无”，” 东向 Port “，” 西向 Port “。

单击“保存”按钮，接受所作更改。

单击“保护 VLAN”按钮，可进入编辑保护 VLAN 配置。

注意：系统默认添加 VLAN 1 作为保护 VLAN，如果用户需要修改或者添加其他 VLAN 作为保护 VLAN，可以在该页面进行编辑。

4.9 LLDP

S4500 交换机支持 LLDP（链路层发现协议），可以将本端设备的的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

可配置全局 LLDP 协议信息，报文发送周期、重传次数、重传间隔、延迟时间等信息。

端口可启用/禁用 LLDP 协议，并指定发送给对端邻居的信息，如：端口描述、系统名字、系统描述、系统属性、管理地址信息。

要查看如下窗口，请单击“高级配置”>“LLDP”，如下：

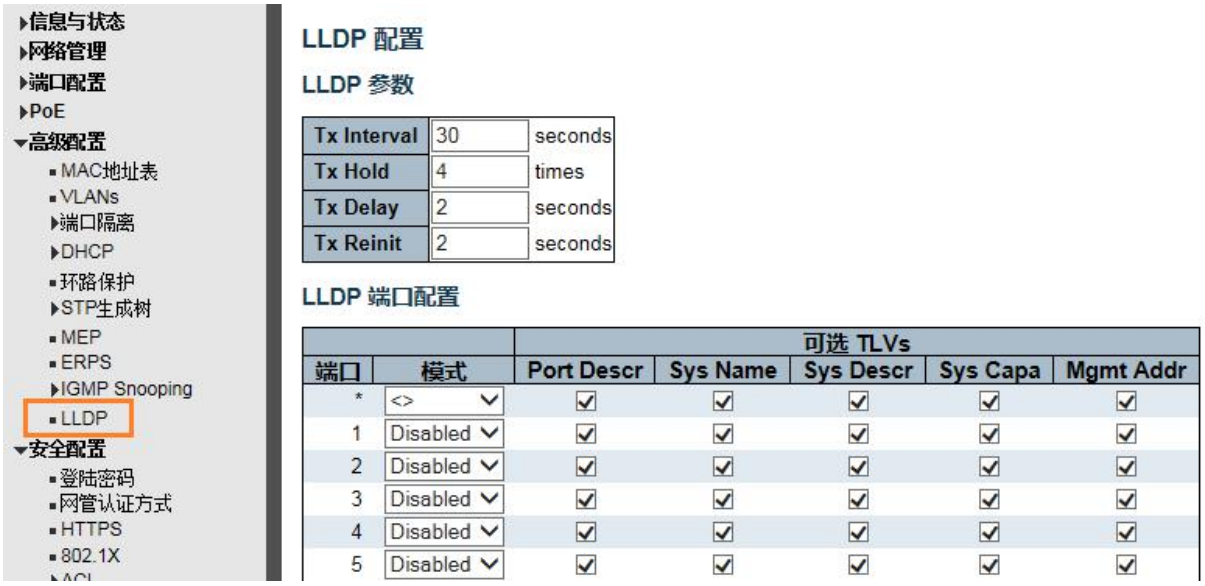


图 4-9 LLDP 配置窗口

4.10 环路保护(Loop Protection)

环路保护(Loop Protection)功能设置配置如下：对交换机端口进行全局环网开启、关闭配置，用户可以更改环网检测时间间隔，以及端口关闭保持时间。在环网功能全局开启时，能够对单个或多个端口进行环路配置，并可选择是否选择主动检测模式。端口检测到环路时提供 3 种处理方式：关端口、关端口并记日志、仅记日志；

若要查看该窗口，请单击“高级配置”> “环路保护(Loop Protection)”，如下。

图 4-10 环路保护设置窗口

可配置字段说明如下：

参数	说明
单播	单击创建 NLB 单播 FDB 条目。
组播	单击创建 NLB 组播 FDB 条目。
VLAN 名称	单击此单选按钮并输入要创建的 NLB 组播 FDB 条目的 VLAN。
VID (1-4094)	单击单选按钮并输入 VLAN ID。
MAC 地址	输入要创建的 NLB 单播或者组播 FDB 条目的 MAC 地址。
端口	单击要被配置的端口。单击“全部”按钮，选择全部端口。

单击“应用”按钮，接受所做更改。

单击“清空”按钮，清除全部输入的信息。单击“编辑”按钮，更新相应条目的信息。

单击“删除”按钮，删除相应条目。

5 QoS 配置

QoS 是 IEEE 802.1p 标准的一种实现，它是允许网络管理员为重要应用保留带宽或设置更高传输优先级的一种方式，如 VoIP（互联网协议语音技术），web 浏览应用程序，文件服务器应用程序或视频会议。此功能不但可以保
留带宽，还可限制其它并不重要的通信量。交换机在每个物理接口上有 8 个硬件队列，这样可映射不同应用程序的数据包，并依次区分优先级别。

请注意交换机对交换机上每个端口有八个可配置的优先级队列（八个等级服务）。

5.1 端口 QoS 分类

交换机允许为交换机上每个端口分配默认 802.1p 优先级以及 DPL, PCP, DEI 等信息。优先级和有效优先级标记为 0（最低优先级）到 7（最高优先级）。
若要查看如下窗口，请单击“QoS 配置” > “端口分类“, 如下：

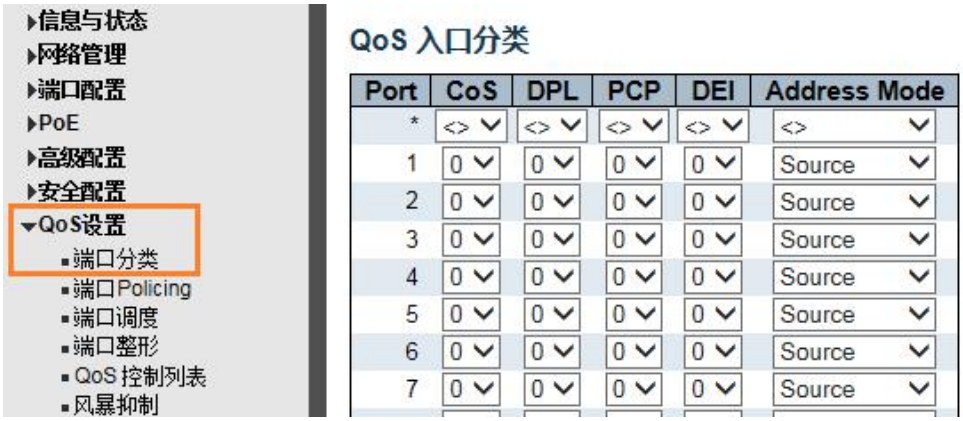


图 5-1 端口分类设置窗口

可配置字段说明如下：

CoS	Controls the default class of service. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. The classified DPL can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

单击“保存”按钮，接受所做更改。

5.2 端口 Policing

若要查看如下窗口，请单击“QoS 配置” > “端口 Policing “, 如下：

图 5-2 端口 Policing 设置窗口

可配置字段说明如下：

启用	启用或者禁用端口入口 Policing。
速率(Rate)	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
单位(Unit)	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
流控(Flow Control)	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

单击“保存”按钮，接受所做更改。

5.3 风暴抑制

若要查看如下窗口，请单击“QoS 配置” > “风暴抑制 “, 如下：

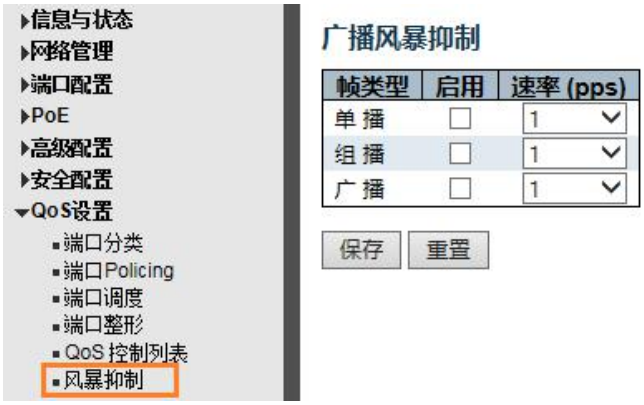


图 5-3 端口 Policing 设置窗口

可配置字段说明如下：

帧类型	该交换机支持对：未知名单播(Unkown Unicast)，未知名组播(Unknown Multicast)，广播(Broadcast)
启用	启用或者禁用风暴抑制。
速率	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

单击“保存”按钮，接受所做更改。

7 安全配置

6.1 登陆密码

交换机支持修改登陆密码。

若要查看如下窗口，请单击“安全配置”>“登陆密码”，如下：

单击“保存”按钮，接受所做更改。

6.2 802.1X

交换机能够以方便和开放的方式向所连接的计算机提供访问网络资源的方法。尽管自动配置和接入是重要的需求，但是也可能导致未授权用户接入网络或者非法访问网络中的敏感数据。
IEEE 802.1X 标准定义了一个基于接口的接入控制协议，以要求用户首先向认证服务器发送认证报文的方式，来防止未授权用户对网络的访问。对通过交换机接口访问网络的设备以服务器进行集中控制，这意味着用户可使用认证报文在网络的任何一个点通过认证。

交换机使用局域网扩展认证协议（EAPOL）在客户端和 RADIUS 认证服务器之间交换认证消息，用以验证用户身份和访问权限。当一个客户端连接到交换机的某个接口上时，交换机将会对 EAPOL 的请求发出一个响应。客户端在对交换机的应答报文中提供身份识别（比如用户名），而交换机将把这些信息转发给 RADIUS。RADIUS 将会验证这些信息并向客户端返回一个接受或拒绝报文。根据客户端和 RADIUS 的设置，客户可以拒绝这个认证方式而采用其他认证方式。
RADIUS 在验证内容后发出一个接受或拒绝报文。如果认证成功交换机将会允许用户访问网络。否则，这个接口上的非 EAP 数据流将会被阻塞。

基于接口的访问控制

在基于接口的访问控制下，一旦连接设备成功地通过认证，接口即变为授权状态，此后该接口上所有的数据流量将不受访问控制限制直到发生导致接口变为非授权状态的事件。因此，如果连接到接口的是一个共享网段，且这个网段连接了多个网络设备，只要此网段上有一个设备通过认证则此网段上的所有设备都能够通过此接口访问该交换机。显然，此控制方式易受攻击。

基于 MAC 地址的访问控制为了完全利用 802.1X 认证优势，有必要为访问交换机的每个连接设备创建“逻辑”接口。交换机把连接到其物理接口上的共享网段当作一系列的逻辑接口来处理，每个逻辑接口都必须经认证服务器单独认证和授权。交换机学习每个相连设备的 MAC 地址，并为其创建一个逻辑接口，这样相连设备通过此逻辑接口与交换机进行通信。

交换机支持基于端口的 802.1x 认证。在这里可以配置 802.1x 全局认证信息，认证开关及相关协议时间配置。并且可以对每个端口的认证状态进行修改与配置，如:强制授权、强制关闭、使能 802.1X、MAC 认证。

若要查看如下窗口，请单击“安全配置”>“802.1X”，如下：

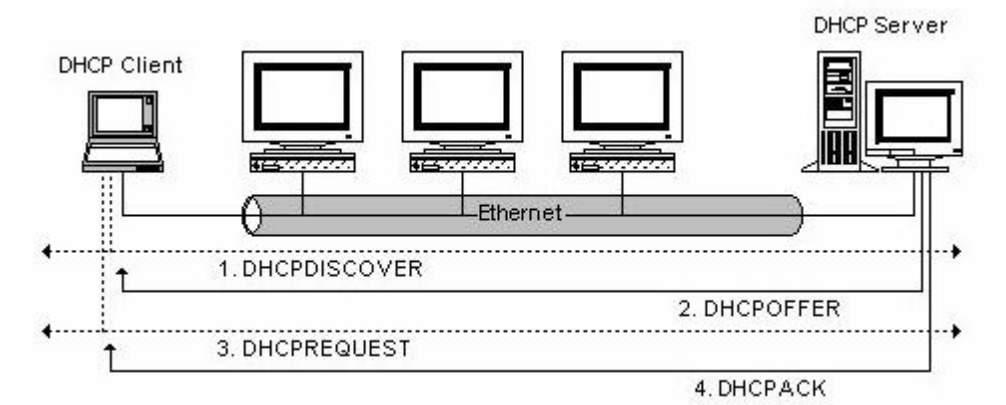
图 6-2 802.1X 配置窗口

单击“保存”按钮，接受所做更改。

6.3 DHCP Snooping

6.3.1 理解 DHCP

DHCP 协议被广泛用来动态分配可重用的网络资源，如IP 地址。一次典型的DHCP 获取IP 的过程如下所示：



DHCP Client 发出DHCP DISCOVER 广播报文给DHCP Server，若Client 在一定时间内没有收到服务器的响应，则重发DHCP DISCOVER 报文。

DHCP Server 收到DHCP DISCOVER 报文后，根据一定的策略来给Client 分配资源(如IP 地址)，然后发出DHCP OFFER 报文。

DHCP Client 收到DHCP OFFER 报文后，发出DHCP REQUEST 请求，请求获取服务器租约，

并通告其他服务器已接受此服务器分配地址。
服务器收到DHCP REQUEST 报文，验证资源是否可以分配，如果可以分配，则发送DHCP ACK 报文；如果不可分配，则发送DHCP NAK 报文。DHCP Client 收到DHCP ACK 报文，就开始使用服务器分配的资源。如果收到 DHCP NAK，则重新发送 DHCP DISCOVER 报文。

6.3.2 理解 DHCP Snooping

DHCP Snooping：意为DHCP 窥探，通过对Client 和服务器之间的DHCP 交互报文进行窥探，实现对用户的监控，同时DHCP Snooping 起到一个DHCP 报文过滤的功能，通过合理的配置实现对非法服务器的过滤。下边对DHCP Snooping 内使用到的一些术语及功能进行一些解释：
1） DHCP Snooping TRUST 口：由于DHCP 获取IP 的交互报文是使用广播的形式，从而存在着非法服务器影响用户正常IP 的获取，更有甚者通过非法服务器欺骗窃取用户信息的现象，为了防止非法服务器的问题，DHCP Snooping 把端口分为两种类型，TRUST 口和UNTRUST 口，设备只转发TRUST 口收到的DHCP Reply 报文，而丢弃所有来自UNTRUST 口DHCP Reply 报文，这样我们把合法的DHCP Server 连接的端口设置为TURST 口，其他口设置为UNTRUST 口，就可以实现对非法DHCP Server 的屏蔽。
2 DHCP Snooping 绑定数据库：在DHCP 环境的网络里经常会出现用户私自设置IP 地址的问题，用户私设IP 地址不但使网络难以维护，并且会导致一些合法的使用DHCP 获取IP 的用户因为冲突而无法正常使用网络，DHCP Snooping 通过窥探Client 和Server 之间交互的报文，把用户获取到的IP 信息以及用户MAC、VID、PORT、租约时间等信息组成一个用户记录表项，从而形成一个DHCP Snooping 的用户数据库，配合ARP 检测功能或ARP CHECK 功能的使用，从而达到控制用户上网的目的。
DHCP Snooping 通过对经过设备的DHCP 报文进行合法性检查，丢弃不合法的DHCP 报文，记录用户信息并生成DHCP Snooping 绑定数据库供其他功能查询使用。以下几种类型的报文被认为是非法的DHCP 报文：
1）、 UNTRUST 口收到的DHCP reply 报文，包括DHCPACK、DHCPNACK、DHCPOFFER 等。
2）、 UNTRUST 口收到的带有网管信息[giaddr]的DHCP request 报文。
3）、打开mac 校验时，源MAC 与DHCP 报文携带的DHCP Client 字段值分别为不同的报文。
4）、用户的信息存在于DHCP Snooping 绑定数据库中，但是端口信息与设备保存在DHCP 绑定数据库中的信息中的端口信息不一致的DHCPRELEASE 报文。

6.3.3 DHCP Snooping 的相关安全功能

在DHCP 的网络环境中，管理员经常碰到的一个问题就是一些用户私自修改使用静态的IP 地址，而不是使用动态获取IP 地址，而使用静态IP 又会导致一些使用动态获取IP 的用户的无法正常使用网络，从而使得网络应用环境变复杂，管理员管理网络的难度加大，而DHCP 动态绑定是指设备在DHCP snooping 的过程通过记录合法用户的IP 获取信息，并进行相关记录，从而进行相关的安全处理，当前的安全控制存在三种方式，一种是结合IP Source Guard 功能对合法用户进行地址绑定，第二种就是使用软件的DAI（动态ARP 检测），通过对ARP 的控制进行用户的合法性校验，第三种结合ARP CHECK 的功能，来对合法用户的ARP 报文进行绑定。注意：结合IP Source Guard 功能进行地址绑定时由于受硬件表项的限制，交换机能够支持的DHCP 用户数目有限，当交换机上用户过多时，可能出现合法用户也无法添加硬件表项而不能正常使用网络现

象，而使用DAI 功能时，由于所有的ARP 报文都需要通过CPU 转发和处理，所以会严重影响交换机的性能。

理解**DHCP Snooping**和**IP Source Guard**地址绑定的关系
IP Source Guard 功能维护一个IP 源地址数据库，通过将数据库中的用户信息[ip、mac]设置为硬件过滤表项，只允许对应的用户使用网络，更多信息请参考《IP&MAC Source Guard 配置章节》。
DHCP Snooping 通过对DHCP 过程的窥探，维护一个用户IP 的数据库，并将该数据提供给IP Source Guard 功能进行过滤，从而限制只有通过DHCP 获取IP 的用户才能够使用网络，从而阻止用户私设IP。
另外由于DHCP 绑定只是对IP 报文进行过滤，不能进行ARP 报文的过滤，所以为了增加安全性，防止ARP 欺骗等问题，对于DHCP 绑定的用户进行了ARP 合法性检查，更多信息参考《ARP Inspection 配置章节》。

6.3.4 DHCP Snooping 配置

单击 “安全配置” > “DHCP ” > “Snooping”，可查看交换机的 DHCP Snooping 配置，如下所示：

图 6-3-4DHCP Snooping 配置窗口

可配置的字段如下所述：

参数	说明
DHCP Snooping 模式	启用或禁用 DHCP Snooping。
端口模式	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.

单击“保存”按钮让更改生效。

6.4 IP&MAC Source Guard

IP&MAC Source Guard 维护一个源 IP 加源 MAC 绑定数据库，IP&MAC Guard 可以在对应的端口上主机报文进行基于源 IP 加源 MAC 的报文过滤，从而保证只有源 IP 加源 MAC 绑定数据库中的主机才能正常使用网络。

6.4.1 端口配置

用户可以在此页中编辑端口配置。

要查看此窗口，请单击“安全配置”>“IP & MAC Source Guard” >“端口配置”，如下图所示：

图 6-4-1 IP&MAC Guard 端口设置窗口

可配置的字段的说明如下：

参数	说明
全局模式	选择全局启用或禁用 IP&MAC Source Guard。

端口 Mode	基于端口启用或禁用 IP&MAC Source Guard。
Max Dynamic Clients	选择支持的最大客户数量, 可选择：Unlimited，0，1，2。

单击“保存”按钮，接受所做更改。

6.4.2 静态表项

用户可以在此页中通过手工配置 IP&MAC Guard 绑定表项来完成端口的控制功能。

要查看此窗口，请单击“安全配置”>“IP&MAC Source Guard” >“静态表项”，如下图所示：

图 6-4-2 静态表项设置窗口

可配置的字段的说明如下：

参数	说明
Port	输入需要绑定的端口 ID
VLAN	输入需要绑定的 VLAN ID
IP 地址	输入需要绑定的 IP 地址。
MAC 地址	输入需要绑定的 MAC 地址。

单击“添加新表项”按钮，根据输入的信息添加新条目。

单击“保存”按钮，应用该更改。

6.5 ARP Inspection

IP&MAC Source Guard 维护一个源 IP 加源 MAC 绑定数据库，IP&MAC Guard 可以在对应的端口上主机报文进行基于源 IP 加源 MAC 的报文过滤，从而保证只有源 IP 加源 MAC 绑定数据库中的主机才能正常使用网络。

6.5.1 端口配置

用户可以在此页中编辑端口配置。

要查看此窗口，请单击“安全配置”>“ARP Inspection”>“端口配置”，如下图所示：

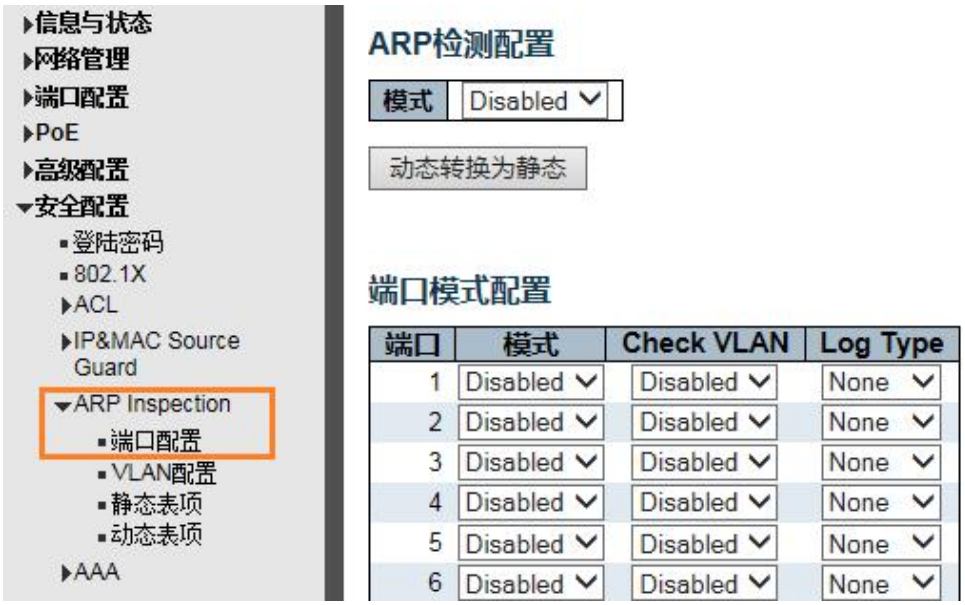


图 6-5-1 ARP Inspection 端口设置窗口

可配置的字段的说明如下：

参数	说明
全局模式	选择全局启用或禁用 ARP Inspection。
端口 Mode	基于端口启用或禁用 ARP Inspection。
Check VLAN	If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: **Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation.
Log Type	Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.

单击“保存”按钮，接受所做更改。

6.5.2 VLAN 配置

要查看此窗口，请单击“安全配置” > “ARP Inspection” > “VLAN 配置”，如下图所示：

图 6-5-2 ARP Inspection VLAN 设置窗口

可配置的字段的说明如下：

参数	说明
VLAN ID	基于 VLAN 的 ARP Inspection 配置
Log Type	基于端口启用或禁用 ARP Inspection。
Check VLAN	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.

单击“保存”按钮，接受所做更改。

单击“添加新条目”按钮，创建新的 VLAN 配置。

6.5.3 静态表项

用户可以在此页中通过手工配置 ARP Inspection 绑定表项来完成端口的控制功能。

要查看此窗口，请单击“安全配置” > “ ARP Inspection” > “静态表项”，如下图所示：

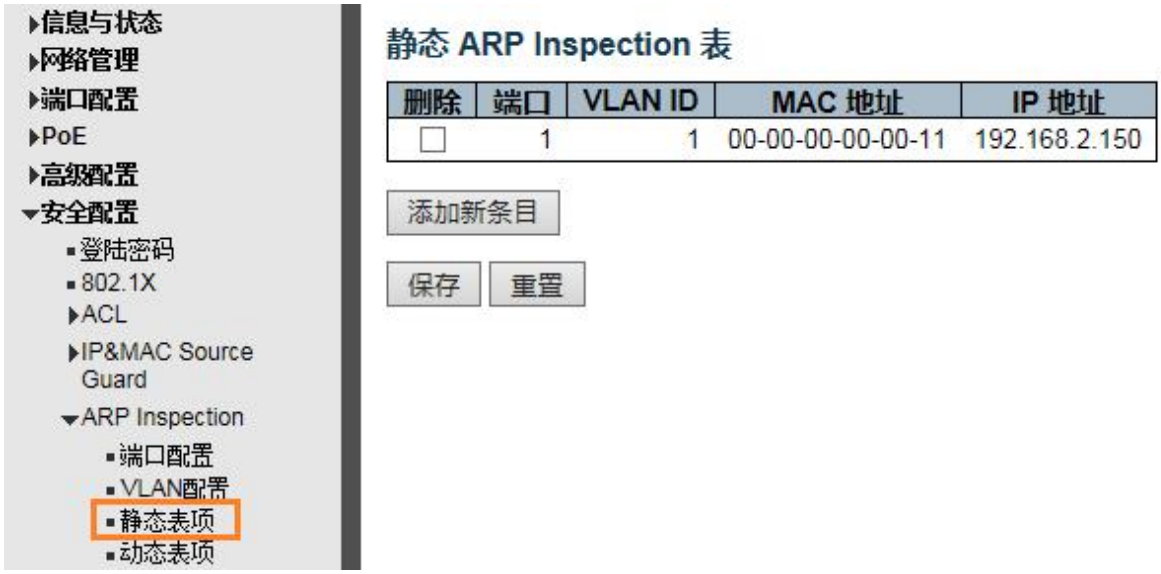


图 6-5-3 静态表项设置窗口

可配置的字段的说明如下：

参数	说明
Port	输入需要绑定的端口 ID
VLAN	输入需要绑定的 VLAN ID
IP 地址	输入需要绑定的 IP 地址。
MAC 地址	输入需要绑定的 MAC 地址。

单击“添加新条目”按钮，根据输入的信息添加新条目。

单击“保存”按钮，应用该更改。

6.6 ACL

ACLs 的全称为接入控制列表(Access Control Lists)，也称为访问列表（Access Lists），俗称为防火墙，在有的文档中还称之为包过滤。ACLs 通过定义一些规则对网络设备接口上的数据报文进行控制：允许通过或丢弃。按照其使用的范围，可以分为安全 ACLs 和 QoS ACLs。

对数据流进行过滤可以限制网络中的通讯数据的类型，限制网络的使用者或使用的设备。安全 ACLs 在数据流通过网络设备时对其进行分类过滤，并对从指定接口输入或者输出的数据流进行检查，根据匹配条件(Conditions)决定是允许其通过(Permit)还是丢弃(Deny)。

总的来说，安全 ACLs 用于控制哪些数据流允许从网络设备通过，Qos 策略对这些数据流进行优先级分类和处理。

ACLs 由一系列的表项组成，我们称之为接入控制列表表项(Access Control Entry：ACE)。每个接入控制列表表项都申明了满足该表项的匹配条件及行为。

访问列表规则可以针对数据流的源地址、目标地址、上层协议等信息。

6.6.1 ACL 端口配置

用户可以在此页中编辑 ACL 端口配置。

要查看此窗口，请单击“安全配置”>“ACL” >“Ports”，如下图所示：

图 6-6-1 ACL 端口设置窗口

可配置的字段的说明如下：

参数	说明
动作	许可表示该端口允许数据流通过。 决绝表示该端口禁止数据流通过。
速率限制 ID	端口绑定的速率限制 ID(Rate Limiter ID)，具体见 Rate Limiter 配置。
端口重定向(Port Redirect)	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
镜像(Mirror)	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
日志(Logging)	
关闭(Shut Down)	Specify the port shut down operation of this port. The allowed values are: **Enabled**: If a frame is received on the port, the port will be disabled. **Disabled**: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

状态	Specify the port state of this port. The allowed values are: **Enabled**: To reopen ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
计数(Counter)	Counts the number of frames that match this rule.

单击“保存”按钮，接受所做更改。

6.6.2 速率限制(Rate Limiter)配置

用户可以在此页中编辑 ACL 速率限制(Rate limiter)配置。

要查看此窗口，请单击“安全配置”>“ACL” >“Rate Limiter”，如下图所示：

图 6-6-2 ACL Rate Limiter 设置窗口

单击“保存”按钮，接受所做更改。

6.6.3 Access Control List 配置

用户可以在此页中编辑 Access Control List 配置。

要查看此窗口，请单击“安全配置”>“ACL” >“Access Control List”，如下图所示：

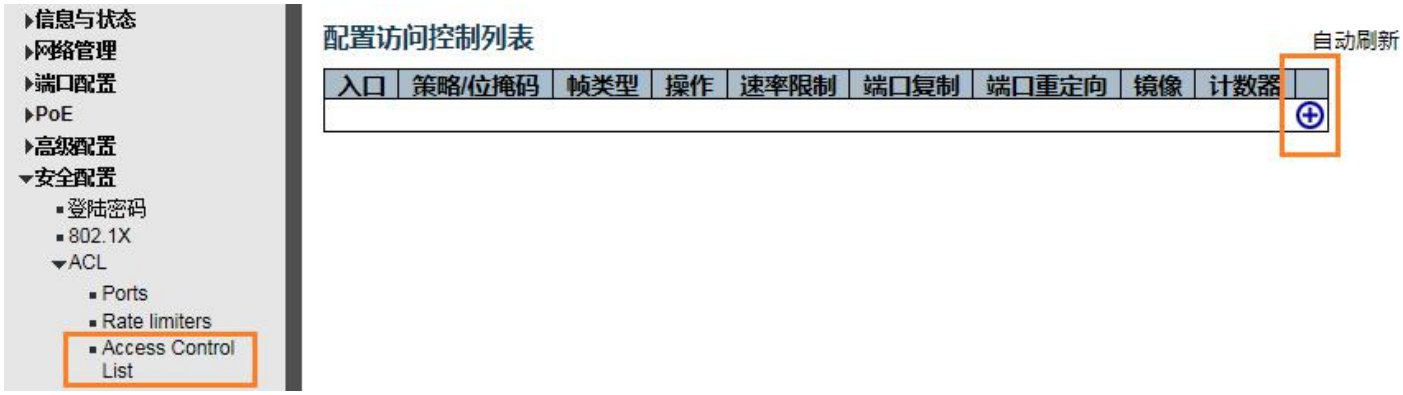


图 6-6-3 Access Control List 设置窗口

单击“+”按钮，进入编辑 Access Control List。

7 系统诊断

7.1 Ping 测试

Ping 是一个小程序，它发送 ICMP Echo 数据包到您指定的 IP 地址。目的节点对从交换机上发出的数据包进行回应。

要查看此窗口，请单击“系统诊断”>“Ping”，如下所示：

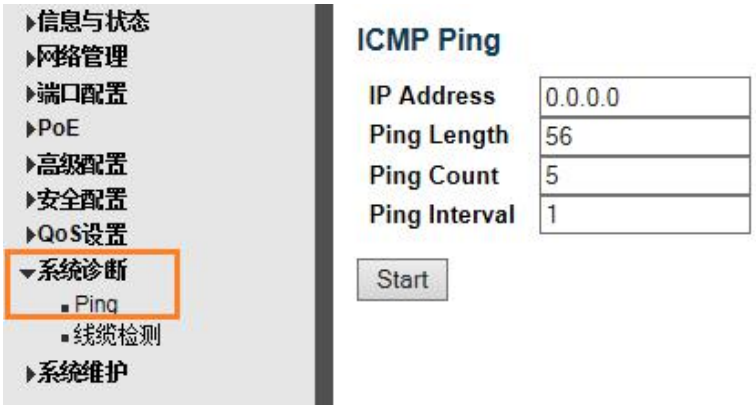


图 7-1 Ping 测试窗口

可配置或显示的字段说明如下：

参数	说明
IP Address	输入需要 Ping 的 IP 地址。
Ping Count	在窗口中输入尝试 Ping IPv4 地址或 IPv6 地址的次数。用户可以输入 1 和 60 之间的数值。
Ping Length	输入 1 和 1452 之间的一个值。默认值是 56。
Ping Interval	输入 Ping 的时间间隔

单击“Start”按钮，开始 Ping 测试。

7.2 线缆检测

线缆检测是一个小程序，用可以检测 10/100/1000BASE-T 电口的线缆状态，例如线对的开路，短路，线缆长度等状态信息。

要查看此窗口，请单击“系统诊断”>“线缆检测”，如下所示：

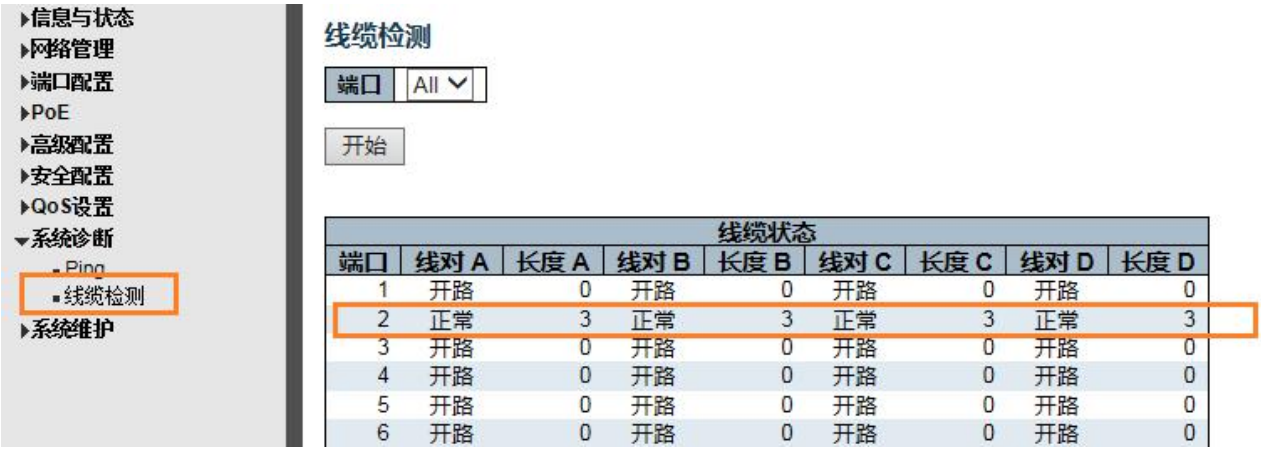


图 7-2 Ping 测试窗口

单击“开始”按钮，开始”线缆检测”测试。

7.3 利用率

可为用户显示 CPU 的使用百分比统计信息，以一个整数百分比表示，计算时间间隔内的简单平均值。

要查看此窗口，请单击“系统诊断”>“CPU 利用率”，如下所示：

图 7-3 CPU 利用率窗口

8 系统维护

8.1 设备重启

该窗口用于对重启复位交换机。请单击“系统维护”>“设备重启”，执行相关操作。

单击“是”重启设备。

8.2 恢复出厂设置

该窗口用于对交换机进行恢复出厂设置。请单击“系统维护”>“恢复出厂设置”，执行相关操作。

单击“是”进行恢复出厂设置。

8.3 系统升级

该窗口用于对系统固件进行升级。请单击“系统维护”>“固件升级”,执行相关操作。

单击“Browse”选择要升级的固件文件。

单击”上传“进行固件升级。

附录 1 术语表

	英文术语	中文名称	定义或描述
A	ARP（Address Resolution Protocol）	地址解析协议	一种把 IP 地址转换成物理地址的协议
	Auto-Negotiation	自协商	使交换机等设备两端按照最大的性能来自动协商工作速率和双工模式
B	Broadcast Storm	广播风暴	通过一个单端口在网络上同时发送过量广播帧。转发信息的响应在网络中将会堆积起来，消耗过多的网络资源或造成网络超时
	Broadcasting	广播	向网络中的所有网点发送数据的转发形式
C	CoS（Class of Service）	服务等级	即 802.1p 优先级方案。 CoS 提供了为数据包加入优先级标签的方法，将报文分为 8 个级别。 值的范围： 0～7
D	DHCP（Dynamic Host Configuration Protocol）	动态主机配置协议	为网络中的主机动态分配 IP 地址、子网掩码、网关等信息
	DSCP（DiffServe Code Point）	差分服务编码点	封装在 IP 报文头的一个 6 位域中，可以将报文分为 64 个级别。 取值范围： 0～63
E	Ethernet	以太网	以太网使用总线形或星形拓扑且支持的传输速率达到 10Mbps 数量级。称为快速以太网的新版本速率可达 100Mbps
F	Flow Control	流控	流控使低速设备能够和高速设备通讯。这种流控是通过高速端口暂停发包的方式，以达到高速端口发包速度与低速端口收包速度匹配
	Frame	帧	含有物理介质层所需的头和尾信息的数据包。
	Full-Duplex	全双工	采用 IEEE802.3x 标准，在一个时刻能可同时进行接收和发送两个方向的数据操作
H	Half-Duplex	半双工	采用 Backpressure 标准，在一个时刻只能进行收或发一个方向的数据操作
I	IGMP （Internet Group Management Protocol）	互联网组管理协议	规定了主机与三层组播设备之间建立和维护组播组成员关系的机制
	IEEE 802.1p	在数据链路层的介质访问控制子层上对网络流量加入优先级	
	IEEE 802.1q	定义 VLAN 桥的操作。在桥式局域网结构中允许对 VLAN 的	

		管理、定义和操作	
Q	QoS（Quality of Service）	服务质量	用来解决网络延迟和阻塞等问题的一种技术
T	Trunking	端口汇聚	将一组端口捆绑在一起形成一个聚合组，从而达到增加带宽，提高连接可靠性的目的
	ToS（Type of Service）	服务类型	封装在 IP 报文头的一个 8 位域中，表征不同优先级特征的报文
U	UDP（User Datagram Protocol）	用户数据报协议	面向无连接的、不可靠的传输层协议
	UTP(Unshielded Twisted Pair)	非屏蔽双绞线	双绞线外部没有屏蔽介质

附录 2 常见问题处理

1、为什么通过 WEB 浏览配置时显示页面不正常?

答：访问 WEB 前，请先清除 IE 的缓存和 cookIES。否则可能导致网页显示不正常。

2、忘记登录密码怎么办?

答：忘记登录密码可以通过恢复出厂设置初始化密码，按住一键恢复 10s 即可初始化密码。初始用户名“admin”和密码“system”。

3、通过 WEB 浏览器配置是否和通过 CLI 命令行下配置等效?

答：两者配置是一样的，并不冲突。

4、为什么配置完 Trunking 功能后，却不能增加带宽?

答：检查设置为 Trunking 的端口其端口属性是否保存一致，包括速率、双工模式、 VLAN 等属性。

5、交换机出现部分端口不通的问题该如何处理?

答：当交换机上出现部分端口不通时，可能是网线故障、网卡故障和交换机端口故障，可通过如下测试定位故障：

1、连接的计算机和交换机端口保持不变，更换其它网线；

2、连接的网线和交换机端口保持不变，更换其它计算机；

3、连接的网线和计算机保持不变，更换其它交换机端口；

4、若确认为交换机端口故障，请联系返厂维修；

6、端口自适应状态检测的顺序如何?

答：端口对状态进行检测时是按如下顺序进行： 1000Mbps 全双工， 100Mbps 全双工， 100Mbps 半双工， 10Mbps 全双工， 10Mbps 半双工，从高到低依次检测，并自动以所支持的最高速度连接。