管理型 PoE 交换机

HR722P-8T4GS-X

Web 管理手册

版本：V1.0

目录

目录

修订记录

日期	版本	描述
Jun 02 2025	V 1.0	第一版

1 前言

1.1 目标读者

本手册适用于负责安装、配置或维护网络的安装人员和系统管理员。本手册假定您了解所有网络使用的传输和管理协议。

本手册也假定您熟知与组网有关的网络设备、协议和接口的专业术语、理论原理、实践技能以及特定专业知识。同时您还必须有图形用户界面、命令行界面、简单网络管理协议和 Web 浏览器的工作经验。

1.2 本书约定

本手册采用以下约定方式。

GUI 约定	描述
说明	操作内容的描述，进行必要的补充和说明。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。

2 登录 Web 页面

2.1 登录 Web 网管客户端

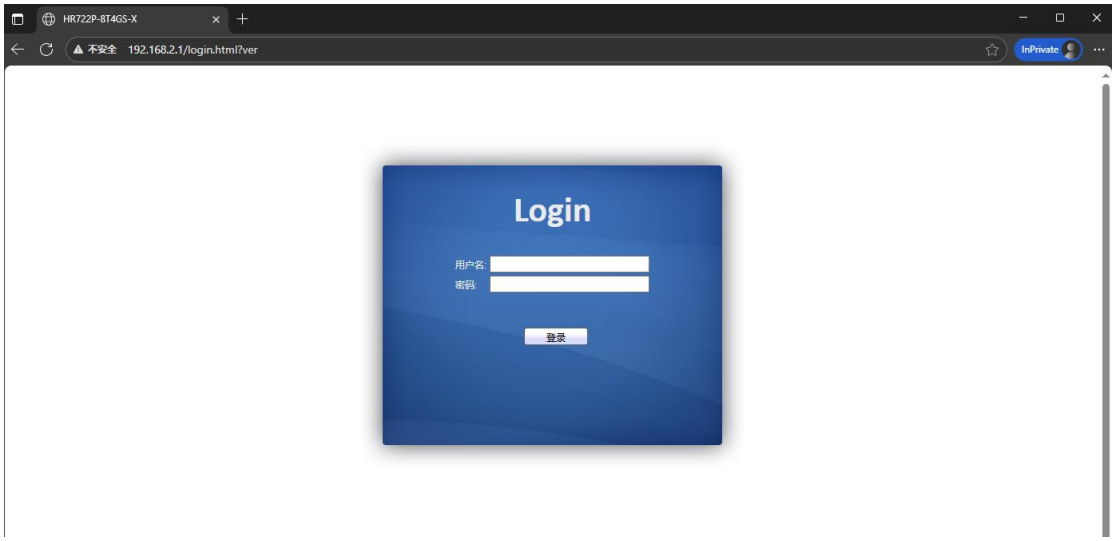
用户可通过打开 Web 浏览器，输入交换机缺省地址：**http://192.168.2.1**，按 Enter 键。

说明:

设备支持浏览器：IE9.0 以上，Chrome23.0 以上，Firefox20.0 以上

登录交换机时，应使 PC 的 IP 网段与交换机网段一致。首次登录时，设置 PC 的 IP 地址为 **192.168.2.x**（x 代表 1~254，除 1），子网掩码设置为 **255.255.255.0**， 但 PC 的 IP 不可与交换机相同， 即不能为 **192.168.2.1**。

此时出现登录窗口，如下图所示。输入缺省用户名: **admin** 和密码: **admin**。单击<登录>按钮，将看到交换机系统信息。



2.2 客户端界面组成

Web 网管系统的典型操作界面的介绍，如下图所示。

2.3 Web 界面导航树

Web 网管的菜单主要提供系统状态、网络配置、端口、POE 设置、VLAN 功能、MAC 地址表、生成树协议、拓扑发现、组播、路由、安全、ACL、QoS、设备诊断、设备管理等菜单项。每个菜单选项下又有子菜单。详细导航树的信息如下:

菜单项	子菜单	二级子菜单	说明
系统状态	系统信息		显示端口状态与产品信息
	日志信息		显示设备运行和操作日志信息
	端口信息	端口统计	显示详细端口统计信息
		端口异常保护	显示端口发生的异常信息
		带宽利用率	显示所有端口在单位时间内的带宽利用信息
	链路聚合		显示汇聚组状态和成员信息
	MAC 地址表		显示当前设备的 MAC 地址表信息
网络配置	DNS 配置		配置查看 DNS 信息及 DNS 服务器设置
	DNS 主机配置		配置查看 DNS 服务器信息和动态主机映射表信息
	系统时间		配置查看当前系统时间信息
端口	端口配置		配置查看设备所有端口信息
	端口异常保护		配置查看端口异常保护功能
	链路聚合	聚合组配置	配置查看链路聚合组包含端口和策略均衡算法

		端口配置	配置查看链路聚合组信息
		LACP 配置	配置查看 LACP 系统优先级和端口设置
	EEE 配置		配置查看端口 EEE 节能状态和信息
	巨型帧配置		配置查看系统转发最大报文长度
	端口安全		配置查看端口安全功能速率限制和端口状态信息
	端口隔离		配置查看端口隔离功能信息
	风暴控制		配置查看端口风暴抑制功能信息
	镜像功能		配置查看端口镜像功能信息
POE 设置	POE 端口设置		配置查看端口 POE 功能信息
	POE 端口定时设置		配置查看端口 POE 定时开关功能信息
	POE 端口定时重启设置		配置查看端口 POE 端口定时重启开关功能信息
VLAN 功能	VLAN 配置	创建 VLAN	配置查看设备包含 VLAN 信息
		设置 VLAN	配置查看 VLAN 在所有端口下配置信息
		成员配置	配置查看 VLAN 包含端口信息
		端口配置	配置查看端口的 PVID 和 VLAN 属性信息
	Voice VLAN	功能配置	配置查看 Voice VLAN 功能开启和端口状态信息
		Voice OUI 配置	配置查看 Voice VLAN OUI 表现信息
	协议 VLAN 配置	协议组配置	配置查看基于协议 VLAN 的协议组信息
		协议组绑定	配置查看基于协议 VLAN 的端口与协议组绑定信息
	MAC VLAN 配置	MAC 组配置	配置查看基于 MAC VLAN 的 MAC 组信息
		MAC 组绑定	配置查看基于 MAC VLAN 的端口与 MAC 组绑定信息
	Surveillance VLAN	功能配置	配置查看 Surveillance VLAN 功能开启和端口状态信息
		Surveillance OUI 配置	配置查看 Surveillance VLAN OUI 表现信息
	GVRP	功能配置	配置查看 GVRP 功能系统信息和端口状态信息
		成员列表	配置查看 GVRP 学习的 VLAN 和端口

			成员信息
		报文统计	配置查看端口 GVRP 相关报文统计信息
MAC 地址表	动态 MAC 地址表		配置查看设备动态 MAC 地址和老化时间信息
	静态 MAC 地址表		配置查看设备静态 MAC 地址表项
	MAC 地址过滤表		配置查看需要过滤的 MAC 地址表项
	端口安全 MAC 地址表		配置查看端口安全学习到的 MAC 地址表项
生成树协议	功能设置		配置查看设备生成树协议状态和相关属性信息
	端口设置		配置查看设备生成树协议端口属性信息
	实例设置		配置查看多生成树协议的实例属性信息
	实例端口设置		配置查看多生成树协议的实例包含端口信息
	报文统计		查看每个端口的生成树协议报文统计信息
ERPS	功能配置		配置查看 ERPS 开关
	ERPS 实例		配置查看 ERPS 实例
环路检测	环路检测配置		配置查看环路检测配置
拓扑发现	LLDP	功能配置	配置查看 LLDP 协议相关属性信息
		端口配置	配置查看各个端口的 LLDP 协议收发状态信息
		MED 网络策略配置	配置查看设备的 MED 网络策略表项
		MED 端口配置	配置查看各个端口的 MED 状态信息
		报文预览	查看各个端口的 LLDP 协议报文详细信息
		本设备信息	配置查看设备的 LLDP 协议和 LLDP-MED 状态信息
		邻居信息	查看设备的 LLDP 邻居信息
		报文统计	查看设备的各个端口 LLDP 协议报文收发信息
DHCP	功能配置		查看和配置 DHCP 全局和端口开关
	地址池配置		查看和配置 DHCP 地址池信息
	VLAN 接口地址组配置		查看和配置 VLAN 接口和服务器组绑定关系
	客户端列表		查看 DHCP 客户端列表

	客户端静态绑定表		查看和配置客户端静态分配绑定关系
	端口客户端静态绑定表		查看和配置端口客户端静态分配绑定关系
组播	基本功能	功能配置	配置查看组播功能配置信息
		静态组播配置	配置查看设备的静态组播相关信息
		路由端口配置	配置查看设备组播路由端口配置信息
		转发端口配置	配置查看设备组播转发端口配置信息
		端口限制	配置查看设备每个端口的组播限制信息
		过滤规则配置	配置查看设备对组播地址的过滤信息
		过滤规则绑定	配置查看设备组播过滤规则与端口的绑定信息
	IGMP Snooping	功能配置	配置查看设备的 IGMP-snooping 开关和版本等信息
		查询器配置	配置查看 IGMP-snooping 查询器状态信息
		报文统计	查看设备的 IGMP-snooping 协议报文信息
	MLD Snooping	功能配置	配置查看设备的 MLD-snooping 协议开关等信息
		报文统计	查看设备的 MLD-snooping 协议报文信息
	MVR	功能配置	配置查看设备的 MVR 功能开关等属性信息
		端口配置	配置查看每个端口的 MVR 功能状态信息
		组地址配置	配置查看 MVR 功能 VLAN 和组地址信息
路由	IPv4 管理接口	IPv4 接口	配置查看设备的 VLANIF 接口
		IPv4 路由	配置查看设备的 IPv4 路由表项
		ARP	配置查看设备的 ARP 表项
	IPv6 管理接口	IPv6 接口	配置查看设备的 IPv6 接口
		IPv6 地址	配置查看设备的 IPv6 地址
		IPv6 路由	配置查看设备的 IPv6 路由表项
		IPv6 邻居	配置查看设备的 IPv6 邻居表项

安全	RADIUS		配置查看 RADIUS 协议的服务器相关信息
	TACACS+		配置查看 TACACS+协议的服务器相关信息
	AAA	认证方式配置	配置查看设备的登录认证方式信息
		登录认证	配置查看设备各种终端的认证方式
	管理通道配置	管理 VLAN	配置查看设备当前的管理VLAN信息
		管理服务	配置查看设备的管理服务方式和相关属性信息
		管理 ACL	配置查看针对管理通道的 ACL
		管理 ACE	配置查看管理通道的 ACE 配置信息
	认证功能	功能配置	配置查看设备的认证功能属性信息
		端口配置	配置查看设备各个端口认证功能相关信息
		MAC-Based 本地账户	配置查看 MAC-Based 本地账户列表信息
		WEB-Based 本地账户	配置查看 WEB-Based 本地账户列表信息
		会话信息	配置查看设备中的认证会话相关信息
	DoS 防攻击	功能配置	配置查看 DoS 防攻击开关选项信息
		端口配置	配置查看设备端口的 DoS 防攻击开关选项信息
	动态 ARP 检查	功能配置	配置查看动态 ARP 检查功能状态信息
		报文统计	查看各个端口的 ARP 检查各状态的 ARP 报文统计信息
	DHCP Snooping	功能配置	配置查看 DHCP Snooping 开关和状态信息
		报文统计	查看各个端口收到的 DHCP 报文统计信息
		Option82 功能配置	配置查看 DHCP Snooping Option82 功能相关属性信息
		Option82 Circuit ID 配置	配置查看 DHCP Snooping Option82 的 Circuit ID 信息
	IP Source Guard	端口配置	配置查看端口的 IP Source Guard 功能状态信息
		IMPV 绑定	配置查看 IP+MAC+PORT+VLAN 绑定表信息
		数据库保存	配置查看 IP Source Guard 绑定表项

			存储状态和信息
ACL	MAC ACL 配置		配置查看基于 MAC 的 ACL 规则条目信息
	MAC ACE 配置		配置查看基于 MAC 的 ACE 表项信息
	IPv4 ACL 配置		配置查看基于 IPv4 的 ACL 规则条目信息
	IPv4 ACE 配置		配置查看基于 IPv4 的 ACE 表项信息
	IPv6 ACL 配置		配置查看基于 IPv6 的 ACL 规则条目信息
	IPv6 ACE 配置		配置查看基于 IPv6 的 ACE 表项信息
	ACL 绑定		配置查看 ACL 规则与端口绑定应用信息
QoS	基本功能	功能配置	配置查看 QoS 开关和状态信息
		队列调度	配置查看 QoS 队列调度算法信息
		CoS 映射	配置查看 CoS 优先级与本地队列映射表信息
		DSCP 映射	配置查看 DSCP 优先级与本地队列映射表信息
		IP 优先级映射	配置查看 IP 优先级与本地队列映射表信息
	带宽限速	端口限速	配置查看端口限速配置信息
		出口队列限速	配置查看基于出口队列限速配置信息
设备诊断	日志功能	功能配置	配置查看日志记录功能开关和状态信息
		远程服务器配置	配置查看日志远程服务器地址信息
	Ping		运行 Ping 操作进行网络诊断
	Traceroute		运行 Traceroute 操作进行网络诊断
	电口测试		运行线缆检测进行电口链路诊断
	光模块信息		查看光口 SFP 模块信息
	UDLD 协议	功能配置	配置查看 UDLD 协议功能开关和状态信息
		邻居信息	查看 UDLD 协议邻居状态信息
设备管理	用户配置		配置查看设备用户信息
	固件管理	升级	更新升级设备软件版本
	配置管理	升级	更新升级设备配置文件信息
		保存配置	保存设备运行的配置文件信息
	SNMP 配置	视图配置	配置查看 SNMP 功能视图表项信息

		组配置	配置查看 SNMP 组信息
		团体配置	配置查看 SNMP 团体信息
		用户配置	配置查看 SNMP 用户属性信息
		Engine ID 配置	配置查看 SNMP Engine ID 和远端 Engine ID 信息
		Trap 配置	配置查看 SNMP Trap 开关和状态信息
		Notification 配置	配置查看 SNMP Notification 服务器状态信息
	RMON 配置	报文统计	查看所有端口的历史报文统计信息
		历史配置	配置查看 RMON 历史记录状态信息
		事件配置	配置查看 RMON 事件状态信息
		告警配置	配置查看 RMON 告警状态信息

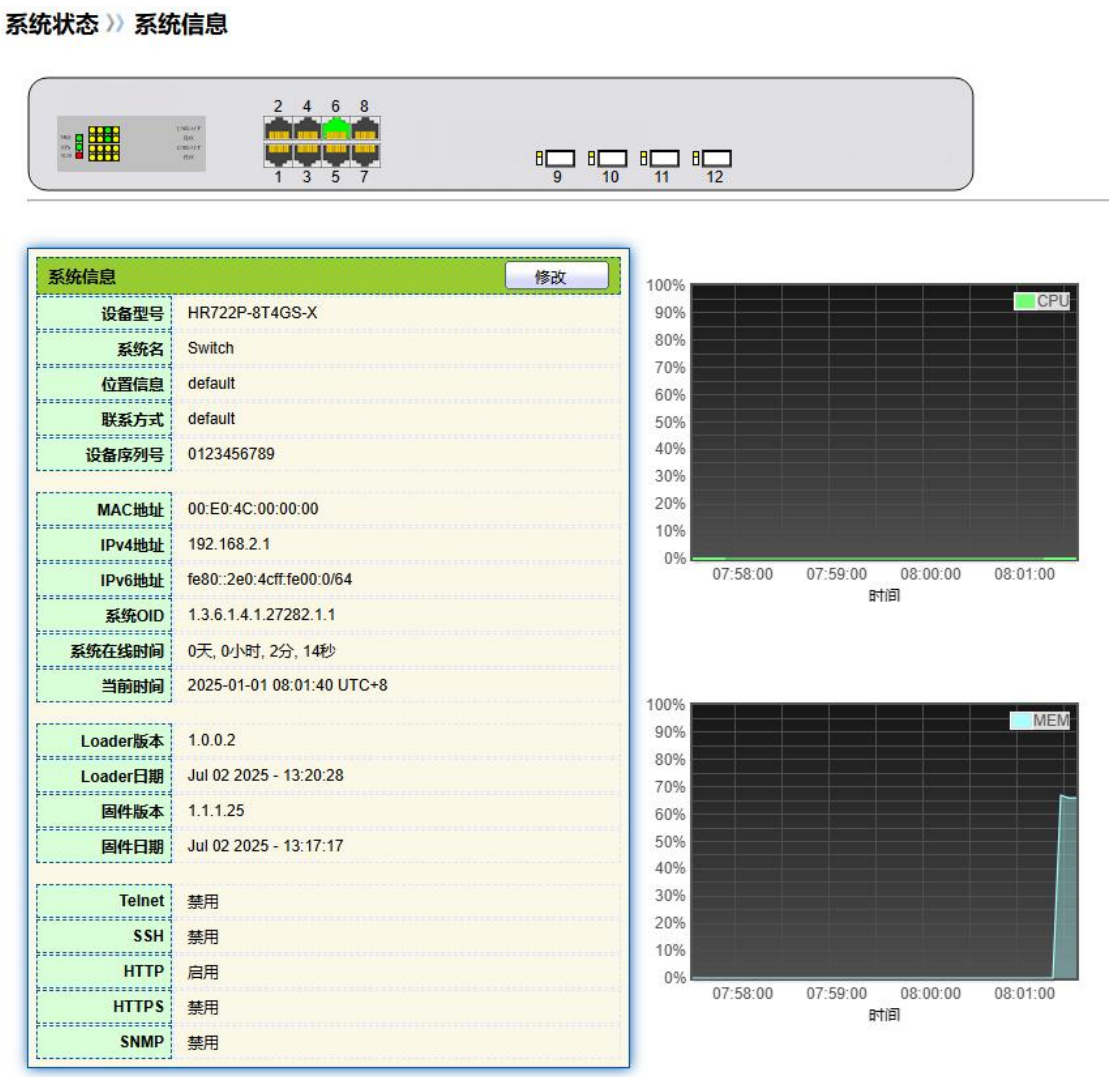
3 系统配置

3.1 系统信息

Web 网管的面板显示区根据所连接的交换机，能够非常直观地显示出该款交换机前面板上各端口的信息与产品信息，其显示内容包括：端口数量，各端口工作状态，产品信息，设备状态，功能开关状态等等。

操作步骤：

1. 单击导航树中的“系统状态 > 系统信息”菜单，进入系统信息查看界面，如下图所示：



说明:

将鼠标放在某个端口上，则会显示该端口的端口号、类型、速率和状态信息。

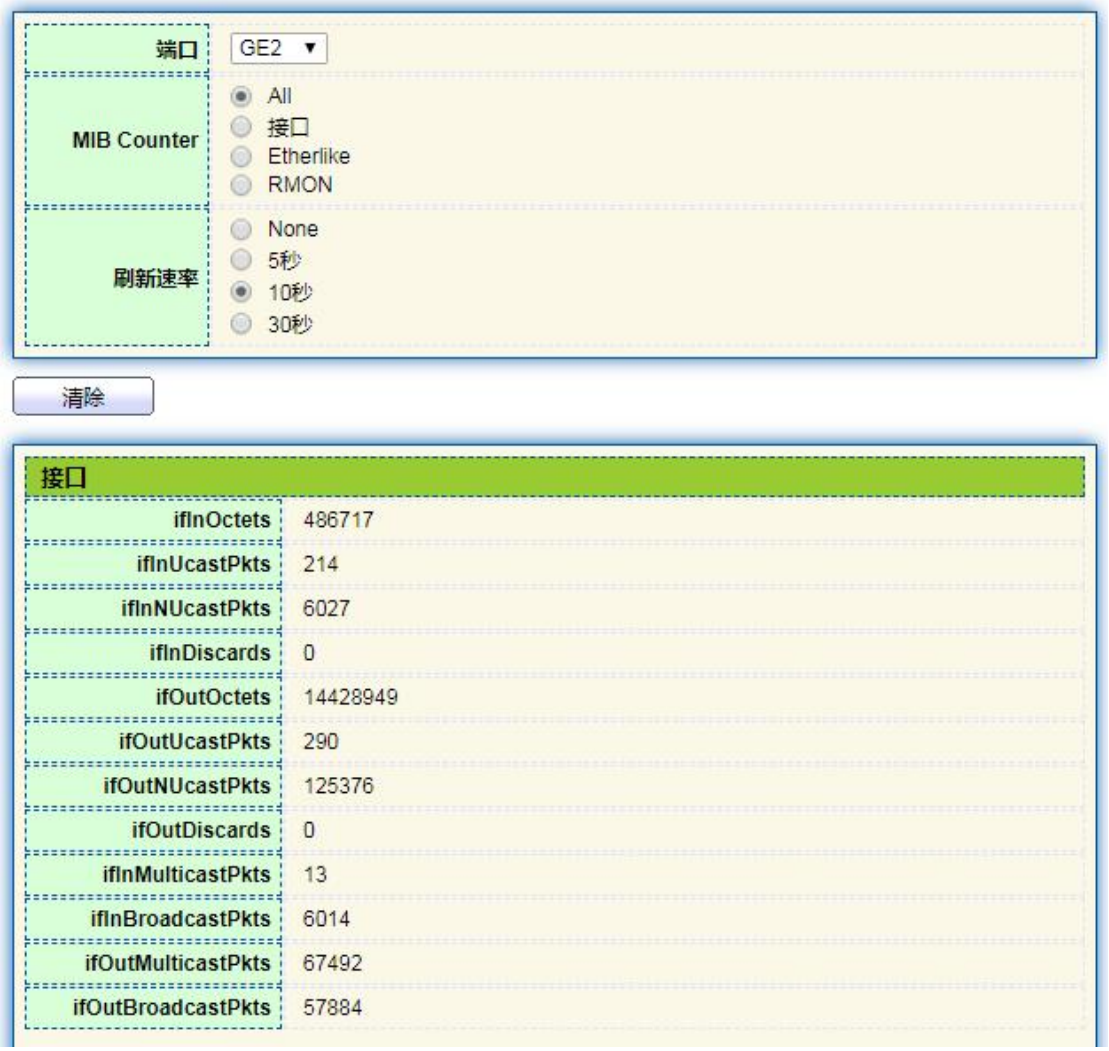
在产品信息中，可以进入修改界面修改“系统名”，“位置信息”，“联系方式”，单击“修改”，进入修改界面，填写完成后应用完成配置。

3.2 端口统计

介绍端口的详细流量统计信息，以及用户需要手动刷新或清除的信息。

操作步骤:

1. 单击导航树中的“系统状态 > 端口信息 > 端口统计”菜单，进入端口统计界面，如下图所示:



- 说明:
- “清除”当前端口的流量统计信息并刷新页面。

3.3 MAC 地址表

查看系统 MAC 地址表项

操作步骤:

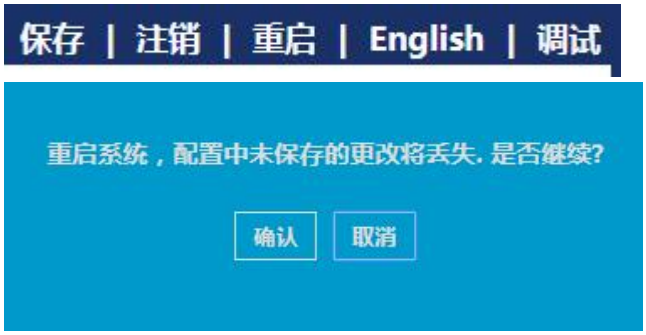
1. 单击导航树中的“系统状态 > MAC 地址表”菜单，进入端口统计界面，如下图所示:

界面信息含义如下表所示。

查询项	说明
MAC	目的 MAC 地址
VLAN	MAC 地址所属的 VLAN ID
端口	设备 MAC 地址对应的报文出端口
类型	动态 MAC 地址，指可以按照用户配置的老化时间而老化掉的 MAC 地址表项，交换机可以通过 MAC 地址学习机制或通过用户手工建立的方式添加动态 MAC 地址表项。 静态 MAC 地址，指用户手动配置指定的 MAC 地址表项，不会被老化。 管理 MAC 地址，指设备的管理接口 MAC 地址

3.4 重启

1. 单击页面右上角系统菜单“重启”，按提示可重启设备，如下图所示。



3.5 管理 IP

进入 web 界面可以更改交换机的管理 IP 地址

操作步骤:

1. 单击导航栏中“路由 > IPv4 管理接口 > IPv4 接口”菜单，可以看到默认 IPv4 地址是 **192.168.2.1/24**，如下图所示

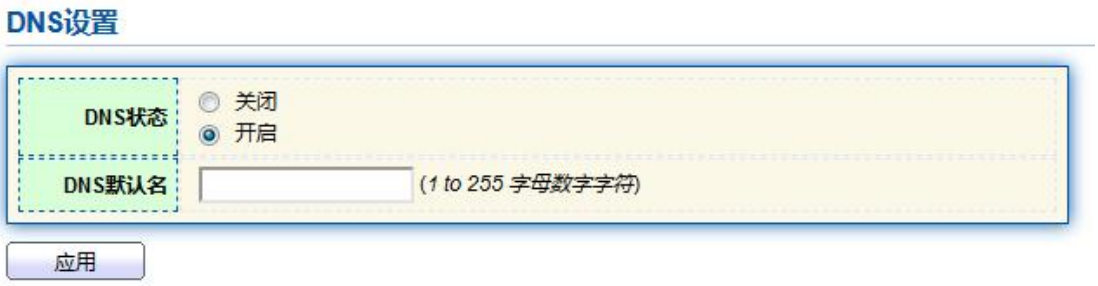
4 网络配置

4.1 DNS 配置

DNS 是域名系统(Domain Name System)的缩写，该系统用于命名组织到域的层次结构中的计算机和网络服务。域名是由圆点分开一串单词或缩写组成的，每一个域名都对应一个惟一的 IP 地址，在 Internet 上域名与 IP 地址之间是一一对应的，DNS 就是进行域名解析的服务器。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。DNS 是因特网的一项核心服务,它作为可以将域名和 IP 地址相互映射的一个分布式数据库。

操作步骤:

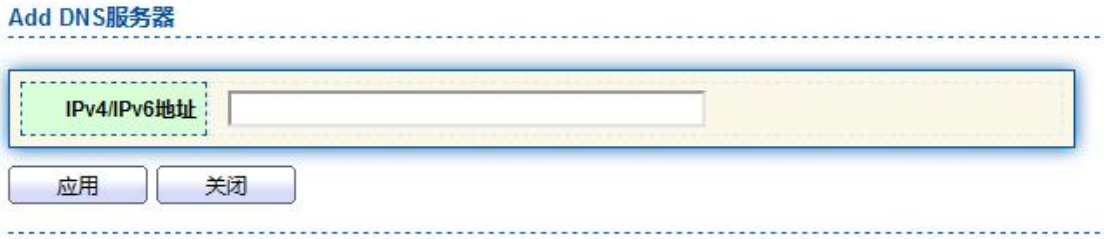
1. 单击导航树中的“网络配置> DNS 配置”菜单，进入“DNS 设置”界面，如下图所示。



界面含义如下表

配置项	说明
DNS 状态	DNS 开关
DNS 默认名	输入 DNS 默认名

2. 点击“添加”设置 DNS 服务器。



3. 单击“设置”，完成配置，如下图所示。

4.2 系统时间

系统时间功能主要用于配置设备系统时间，选择系统时间源，夏令时等配置。

操作步骤

1. 单击导航树中的“网络配置 > 系统时间”菜单，进入“系统时间”界面，如下图所示。

界面含义如下表

配置项	说明
时间源	用于选择时间源，可通过 SNTP 协议，PC 或者手工配置
时区	设置时区
地址类型	主机名或者 IPv4 地址（时间源为 SNTP 时设置）
服务器地址	服务器地址（时间源为 SNTP 时设置）
服务器端口号	服务器端口号（时间源为 SNTP 时设置）
日期	日期信息，年-月-日（时间源为手工设置）

时间	时间信息，小时-分-秒（时间源为手工设置）
类型	夏令时类型分 None,循环，非循环，美国，欧洲
补偿时间	夏令时补偿时间
循环	夏令时循环模式的设置
非循环	夏令时非循环模式的设置

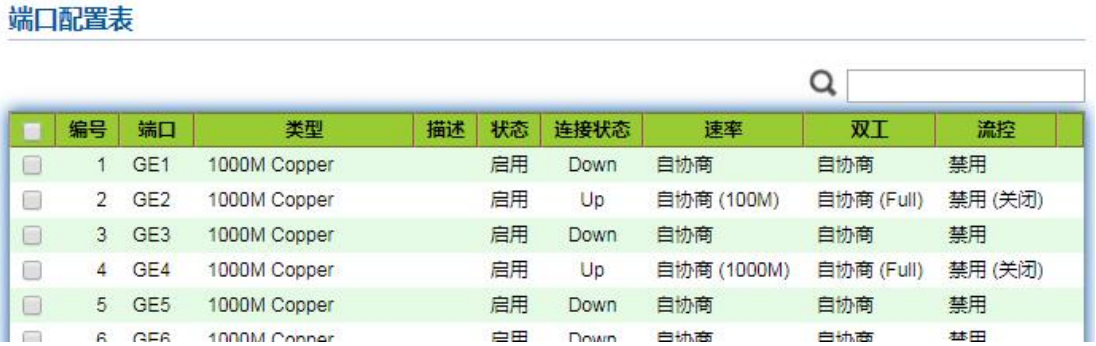
5 端口

5.1 端口配置

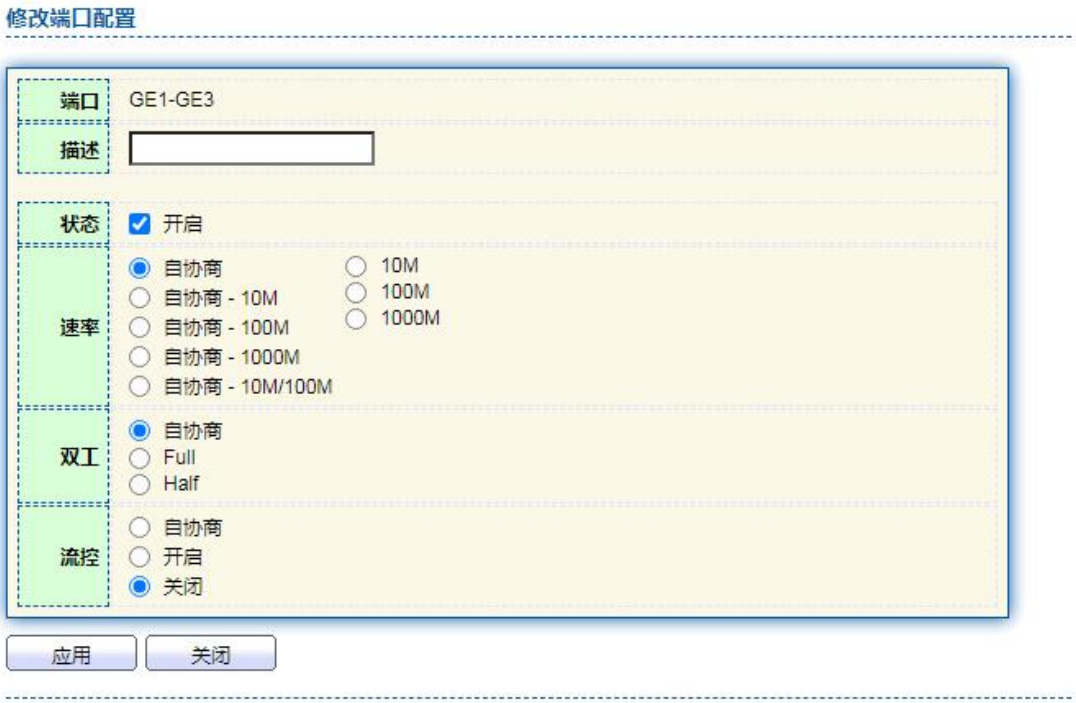
为便于识别接口，给接口配置标识它的描述信息。用户可以根据需要查询和配置以太网接口。

操作步骤:

1. 单击导航栏中“端口 > 端口配置”菜单，进入端口配置页面:



2. 选择需要配置的端口，可以同时选择多个端口，然后点击修改按钮，进入修改页面:



可配置项信息含义如下表:

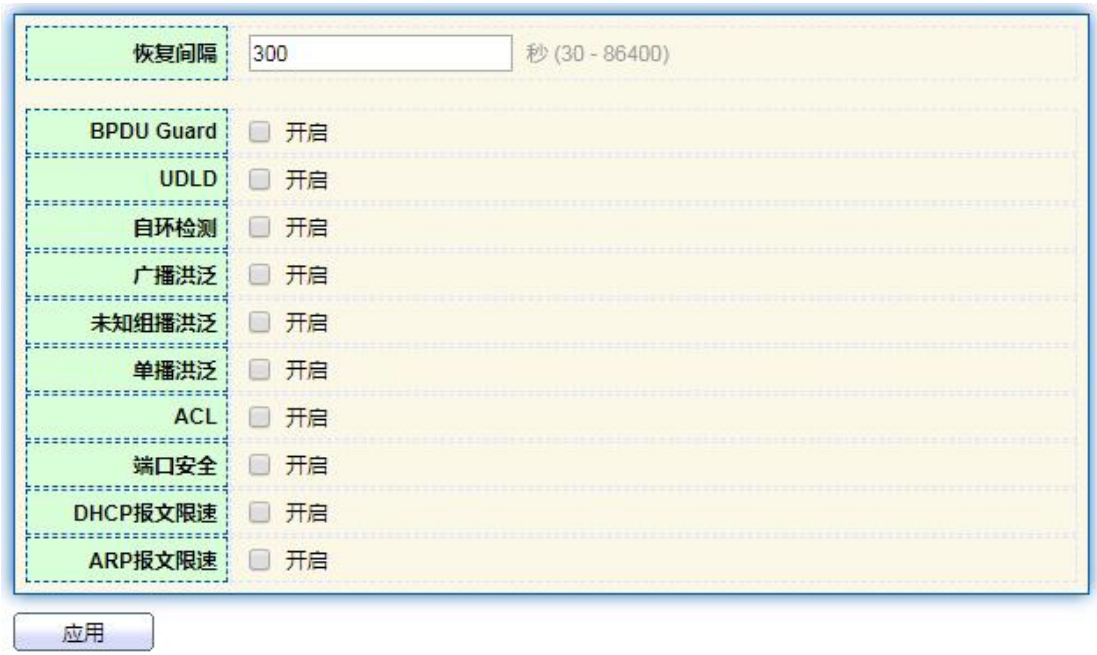
配置项	说明
描述	用户可以根据需要为端口添加描述信息，来标识特定端口
状态	端口开启和关闭选项，用户可以根据需要开关端口
速率	可配置自协商，强制十兆，强制百兆，强制千兆，千兆以太网电接口支持 10Mbits/s、100Mbits/s、1000Mbit/s 三种速率，可以根据需要选择合适的接口速率。
双工	可以配置自协商，全双工和半双工模式
流控	当本端和对端设备都开启了流量控制功能后，如果本端设备发生拥塞，它将向对端设备发送消息，通知对端设备暂时停止发送报文；而对端设备在接收到该消息后将暂时停止向本端发送报文，从而避免了报文丢失现象的发生 关闭 — 禁用 PAUSE 帧的接收和传输 开启 — 启用 PAUSE 帧的接收和传输 自协商 — 自动与对端协商 PAUSE 帧的处理能力。

5.2 端口异常保护

一般来说，如果交换机的软件检测到端口有错误，端口会立即关闭。换言之，当交换机的操作系统在交换机端口上检测到一些错误事件时，交换机将自动关闭端口。

操作步骤:

1. 单击导航树中的“端口 > 端口异常保护”菜单进入界面，如下图所示:



5.3 链路聚合

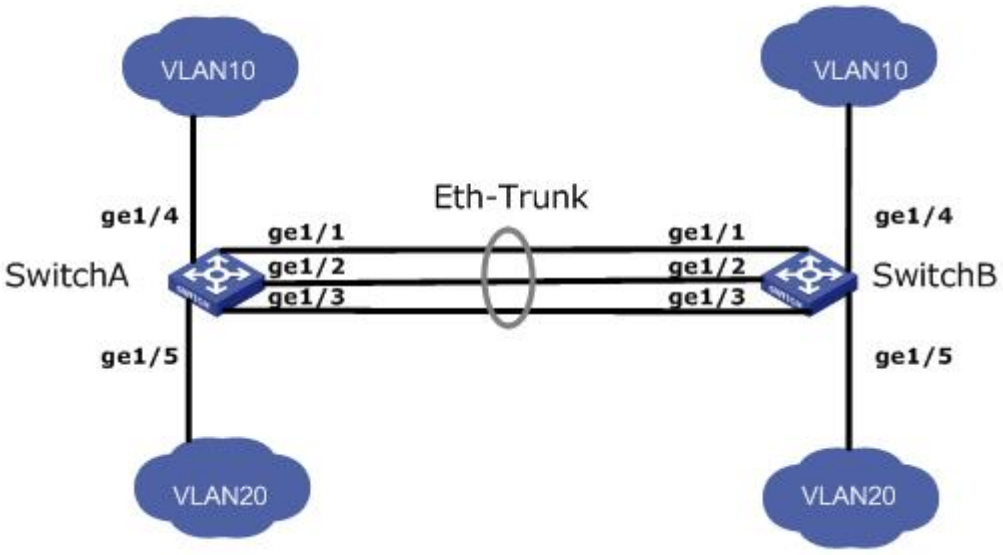
链路聚合（Link Aggregation）是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽和可靠性的一种方法。

链路聚合组 LAG（Link Aggregation Group）是指将若干条以太链路捆绑在一起所形成的逻辑链路，简写为 Eth-Trunk。

随着网络规模不断扩大，用户对链路的带宽和可靠性提出越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。

采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻辑接口，实现增加链路带宽的目的。链路聚合的备份机制能有效提高可靠性，同时，还可以实现流量在不同物理链路上的负载分担。

如下图所示，SwitchA 与 SwitchB 之间通过三条以太网物理链路相连，将这三条链路捆绑在一起，就成为了一条 Eth-Trunk 逻辑链路，这条逻辑链路的带宽等于原先三条以太网物理链路的带宽总和，从而达到了增加链路带宽的目的；同时，这三条以太网物理链路相互备份，有效地提高了链路的可靠性。



在有以下需求时，可通过配置链路聚合实现：

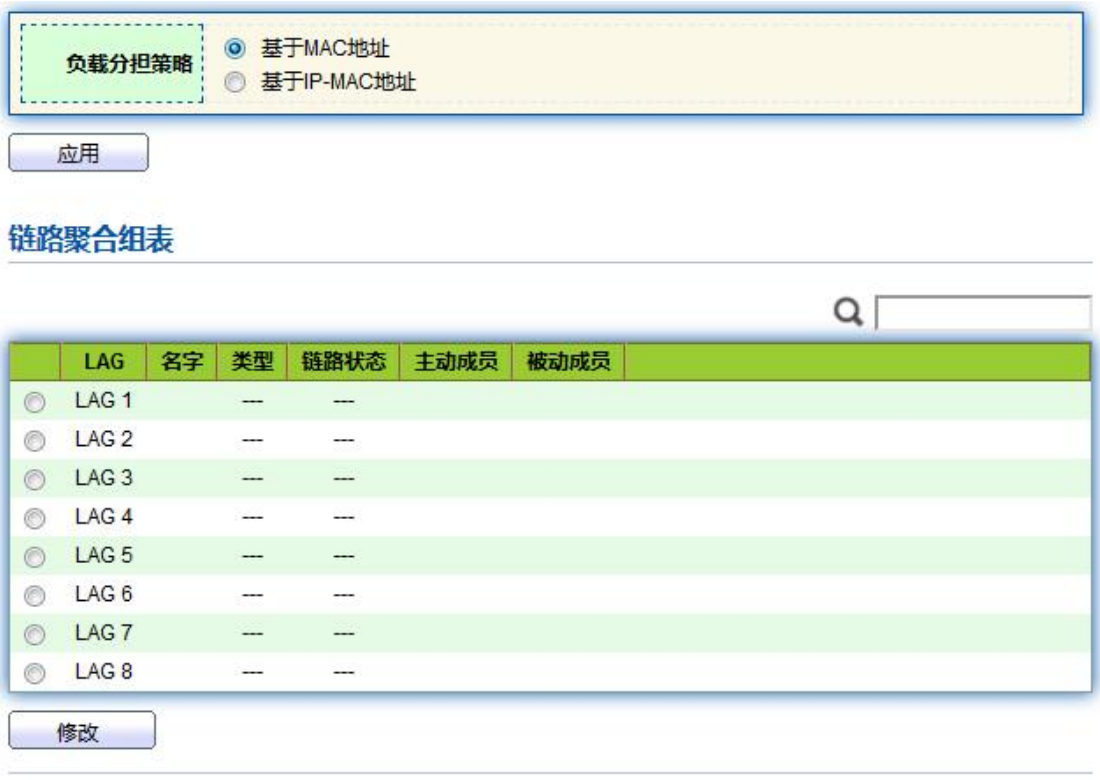
- 当两台交换机设备之间通过一条链路连接带宽不够时。
- 当两台交换机设备之间通过一条链路连接可靠性不满足要求时。

根据是否启用链路聚合控制协议 LACP，链路聚合分为静态模式和 LACP 模式。静态模式下，Eth-Trunk 的建立、成员接口的加入由手工配置，没有链路聚合控制协议的参与。该模式下所有活动链路都参与数据的转发，平均分担流量，因此称为负载分担模式。如果某条活动链路故障，链路聚合组自动在剩余的活动链路中平均分担流量。当需要在两个直连设备间提供一个较大的链路带宽而设备又不支持 LACP 协议时，可以使用静态模式。

5.3.1 聚合组配置

添加静态链路聚合操作步骤：

1. 单击导航栏中“端口 > 链路聚合 > 聚合组配置”菜单，进入链路聚合组配置界面，设备支持两种负载均衡算法，使用单选框选择其中之一，应用保存生效，如下图所示：



2. 设备支持 8 个链路聚合组，选择其中之一，点击修改按钮进入配置页面，如下图：

界面信息含义如下表：

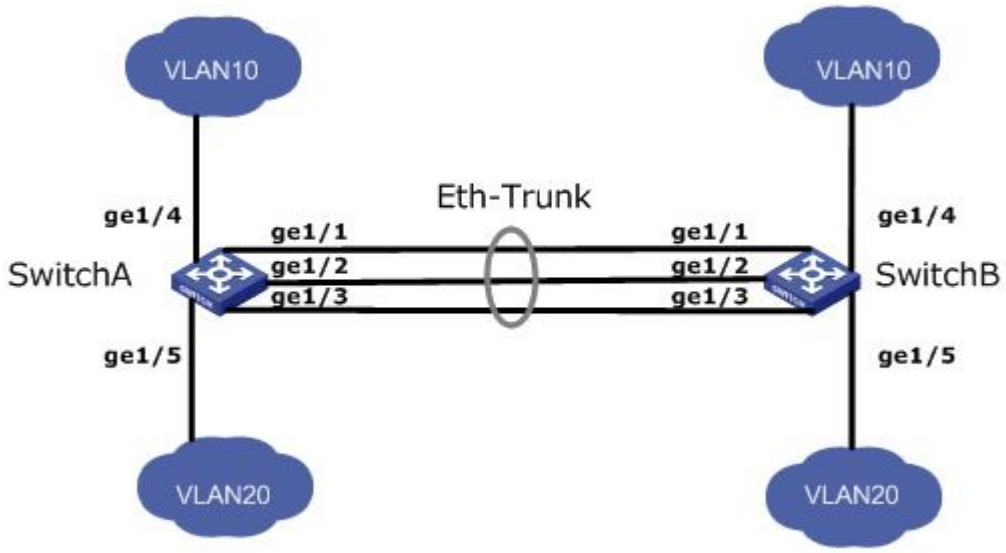
配置项	说明
LAG	链路聚合组 ID，共有 1 ~ 8，8 个聚合组
名字	对链路聚合组的描述信息，可以根据需要修改

类型	选择是静态聚合方式还是基于 LACP 动态聚合方式
成员	链路聚合组包含的成员端口，最多 8 个端口

示例：

如下图所示，SwitchA 和 SwitchB 通过以太链路分别都连接 VLAN10 和 VLAN20 的网络，且 SwitchA 和 SwitchB 之间有较大的数据流量。

用户希望 SwitchA 和 SwitchB 之间能够提供较大的链路带宽来使相同 VLAN 间互相通信。同时用户也希望能够提供一定的冗余度，保证数据传输和链路的可靠性。



操作步骤：

1. 在 SwitchA 创建 Eth-Trunk 接口并加入成员接口，实现增加链路带宽，SwitchB 配置与 SwitchA 类似，不再赘述。单击导航栏中“端口 > 链路聚合 > 聚合组配置”菜单，进入链路聚合组配置界面，选择组“LAG 1”，选择需要聚合的端口 ge1、ge2、ge3，点击向右箭头，移动到已选端口中，点击“应用”生效，如下图所示。

5.3.2 端口设置

聚合组成员端口的属性配置

操作步骤:

1. 单击导航树中的"端口 > 链路聚合 > 端口设置"菜单进入界面，如下图所示:

5.3.3 LACP 配置

基于 IEEE802.3ad 标准的 LACP (Link Aggregation Control Protocol, 链路汇聚控制协议）是一种实现链路动态汇聚与解汇聚的协议。LACP 协议通过 LACPDU （Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。

开启某端口的 LACP 协议后, 该端口将通过发送 LACPDU 向对端通告自己的系统优先级、系统 MAC、端口优先级、端口号和操作 Key。对端接收到这些信息后，将这些信息与其它端口所保存的信息比较以选择能够汇聚的端口, 从而双方可以对端口加入或退出某个动态聚合组达成一致。

动态 LACP 聚合是一种系统自动创建或删除的汇聚，动态汇聚组内端口的添加和删除是协议自动完成的。只有速率和双工属性相同、连接到同一个设备、有相同基本配置的端口才能被动态汇聚在一起。

添加动态链路聚合操作步骤:

1. 单击导航栏中"端口 > 链路聚合 > 聚合组配置"菜单，进入链路聚合组配置界面，选择要配置的链路汇聚组 ID，点击修改按钮进入修改页面，选择类型为 LACP，如下图所示:

2. 单击导航栏中“端口 > 链路聚合 > LACP 配置”菜单，进入 LACP 属性配置页面，可以配置 LACP 相关属性，如系统优先级，端口优先级，端口超时方式等，如下图：

界面信息含义如下表

配置项	说明
类型	静态模式：当需要增加两台设备之间的带宽或可靠性，而两台设备中有一台不支持 LACP 协议时，可在设备上创建静态链路聚合，并加入多个成员接口增加设备间的带宽及可靠性。 LACP 模式：在动态 LACP 模式下两设备间的链路具有冗余备份的能力，

	当部分链路故障时使用备份链路替代故障链路，保持数据传输的不中断。
系统优先级	LACP 确定两台设备之间选择主动、被动模式时根据优先级决策
端口优先级	LACP 在确定动态聚合组成员模式，根据系统优先级高的设备端口优先级来确定。
超时时间	决定 LACP 协议报文发送的频率

说明:

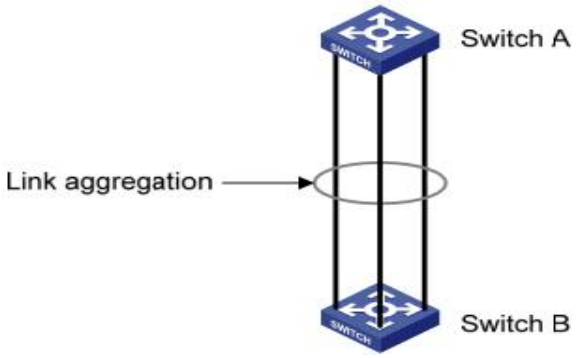
改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。本端和对端配置的工作模式应保持一致。

举例说明:

以太网交换机 Switch A 使用 3 个端口（GE1～GE3）汇聚

接入以太网交换机 Switch B，实现流量在各成员端口中的负载分担。

下面的实际配置中，将采用动态汇聚方式分别进行举例。

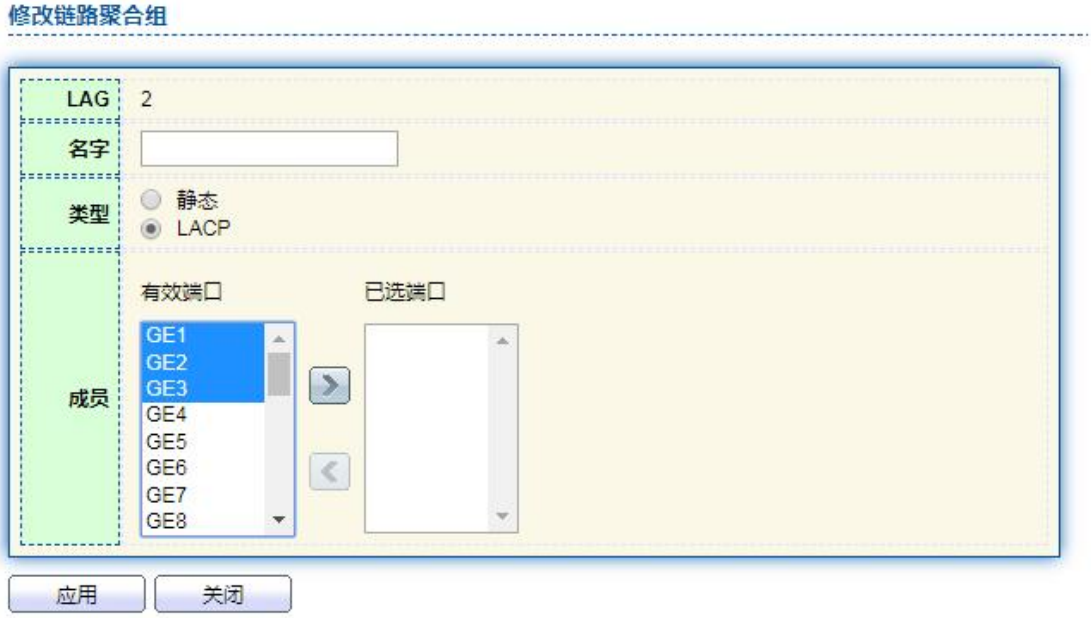


说明:

以下只列出对 Switch A 的配置，对 Switch B 也需要作相同的配置，才能实现端口汇聚。

操作步骤:

1. 单击导航栏中“端口 > 链路聚合 > 聚合组配置”菜单，进入链路聚合组配置界面，选择 LAG 2，单击“修改”，选择 GE1-GE3，选择类型为 LACP，点击“应用”即可，如下图:

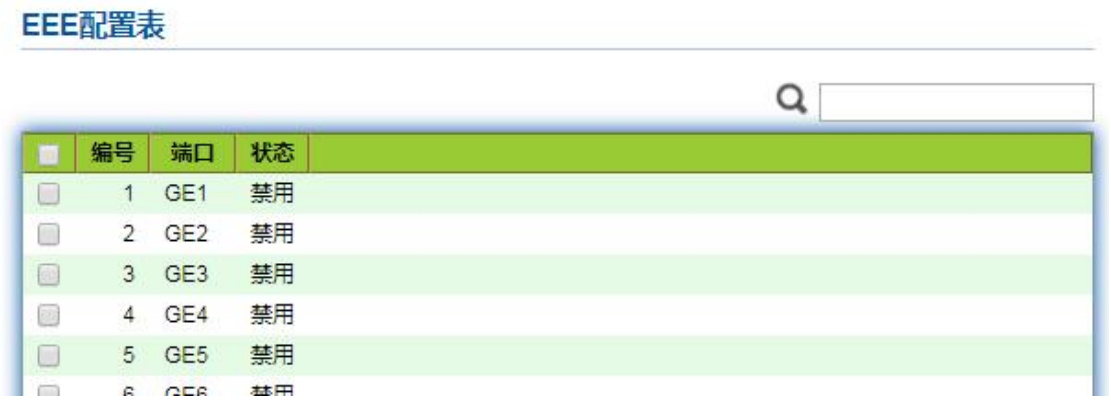


5.4 EEE 配置

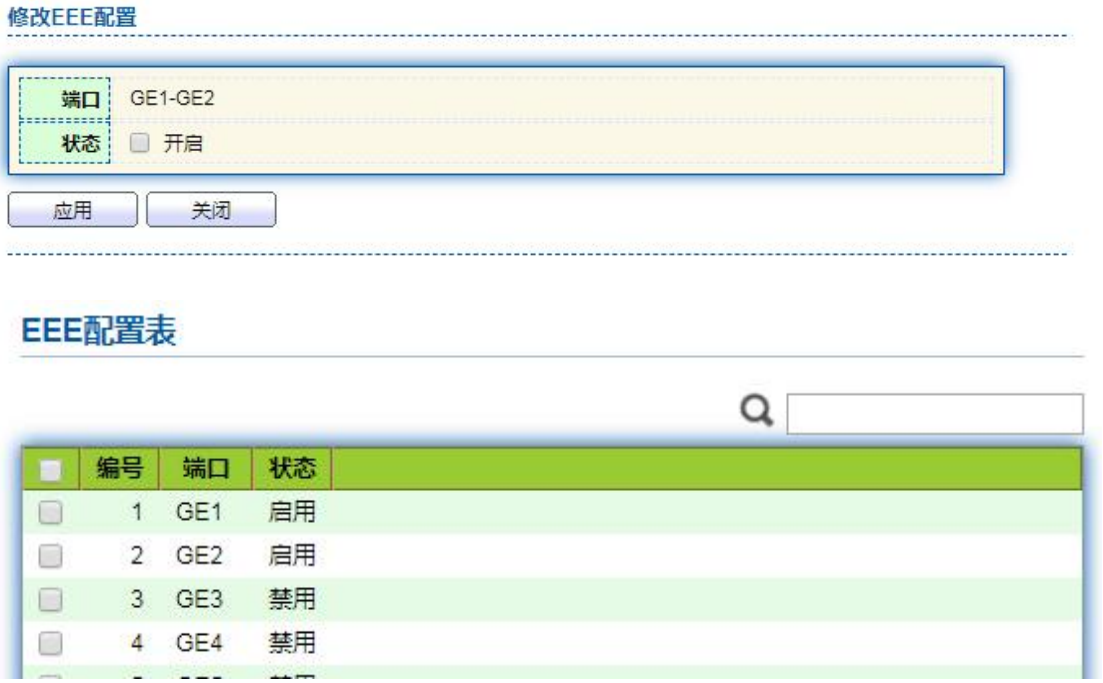
如果流量为零或更少，端口功率将被调低

操作步骤：

1. 单击导航树中的"端口 > EEE 配置"菜单进入界面，如下图所示：



2. 选择端口列表，然后点击“修改”，进行 EEE 开关配置，发下图所示：



5.5 巨型帧配置

操作步骤：

1. 单击导航树中的“端口 > 巨型帧配置”菜单进入界面，如下图所示：

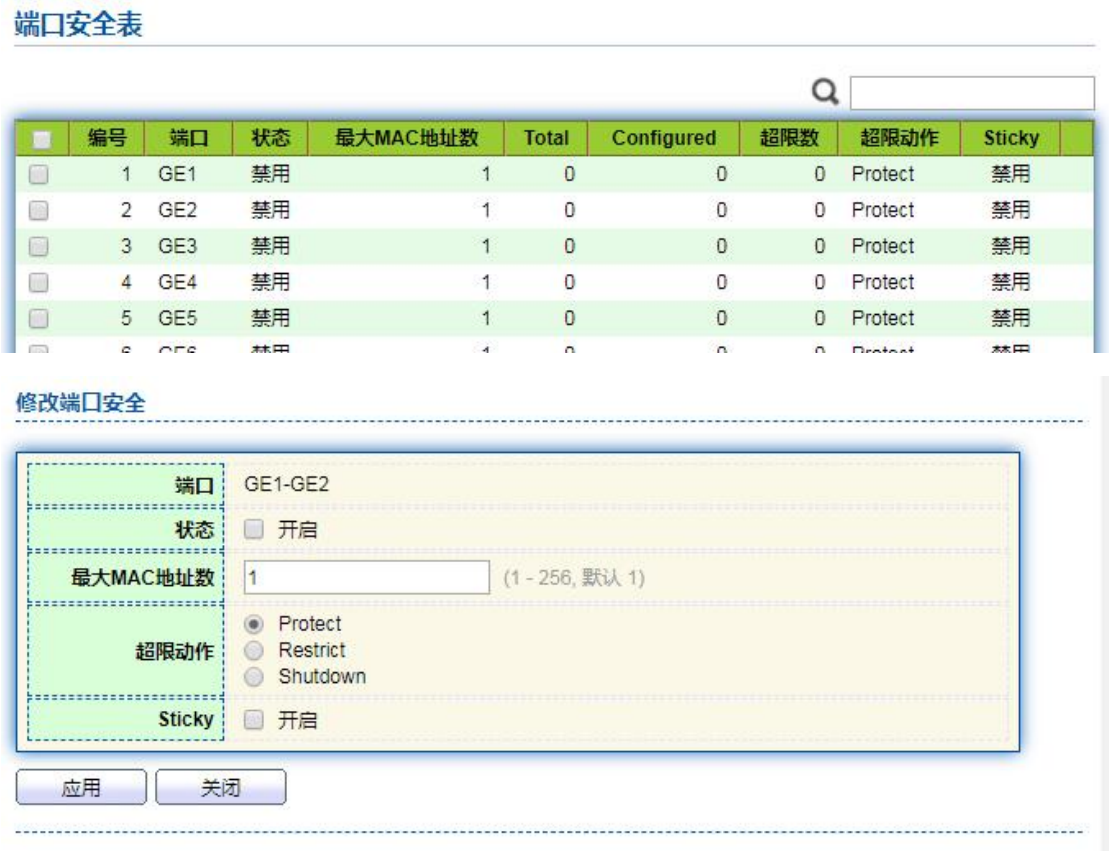
5.6 端口安全

端口安全功能通过 MAC 地址表记录连接到交换机端口的以太网 MAC 地址，只有一个 MAC 地址可以通过该端口进行通信。当其他 MAC 地址发送的数据包通过此端口时，端口安全功能会阻止它。使用端口安全功能可以防止未经授权的设备访问网络并增强安全性。此外，还可以使用端口安全功能来防止 MAC 地址表因 MAC 地址溢出而填满

操作步骤：

1. 单击导航树中的“端口 > 端口安全”菜单进入界面，如下图所示：

2. 端口安全表，选择端口列表，然后点击“修改“，进入端口配置界面，如下图所示：

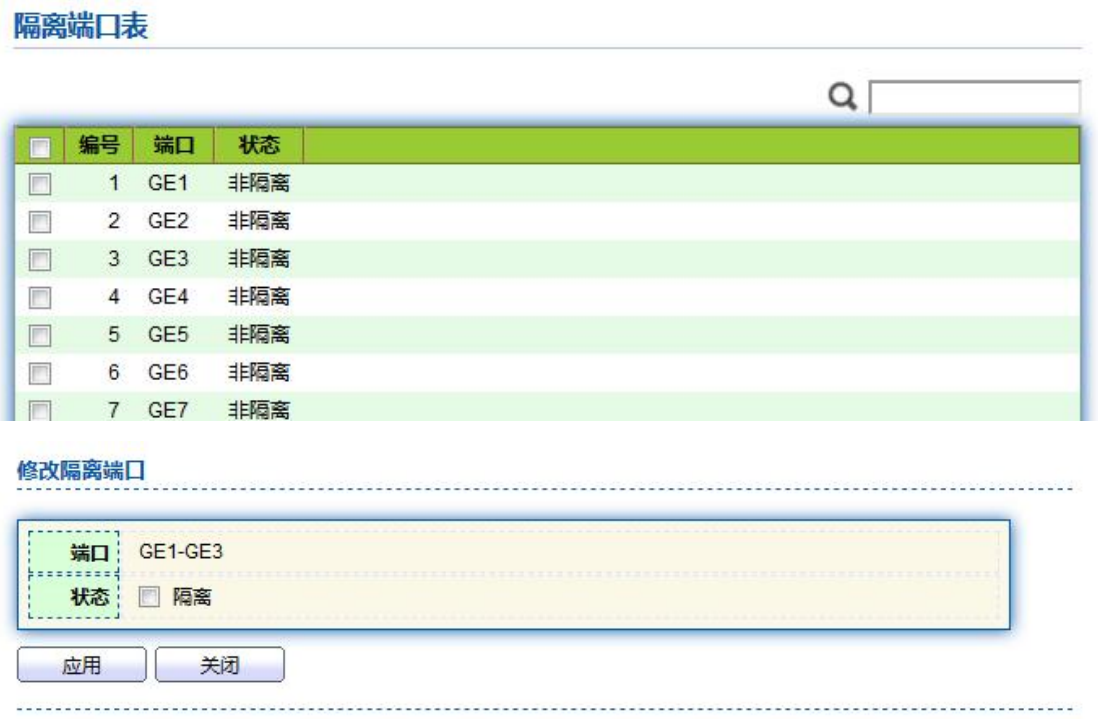


5.7 端口隔离

端口流量之间有时不需要互相通信，但是广播、组播等报文会泛洪到各个端口之间，此时可以通过端口隔离功能来实现端口与端口之间的报文隔离。

操作步骤：

1. 单击导航栏中“端口 > 端口隔离”菜单，进入端口隔离配置界面，选择需要隔离的端口，点击“修改”，配置隔离功能的开关，如下图所示：



5.8 风暴控制

风暴控制按以下形式来防止广播、未知组播以及未知单播报文产生广播风暴。设备支持对接口下的这三类报文分别按包速率进行风暴控制。在一个检测时间间隔内，设备监控接口下接收的三类报文的平均速率并和配置的最大阈值相比较，当报文速率大于配置的最大阈值时，设备会对该接口进行风暴控制，执行配置好的风暴控制动作。

当设备某个二层以太接口收到广播、组播或未知单播报文时，如果根据报文的目的 MAC 地址设备不能明确报文的出接口，设备会向同一 VLAN（Virtual Local Area Network）内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。

引入风暴抑制特性，可以控制这三类报文流量，防范广播风暴。

操作步骤：

1. 单击导航栏中"端口 > 风暴控制"菜单，进入风暴控制页面。页面可以配置风暴控制相关属性，例如模式等，界面如下：

2. 页面中可以为每个端口分别配置广播、组播以及未知单播风暴控制速率，选择需要配置

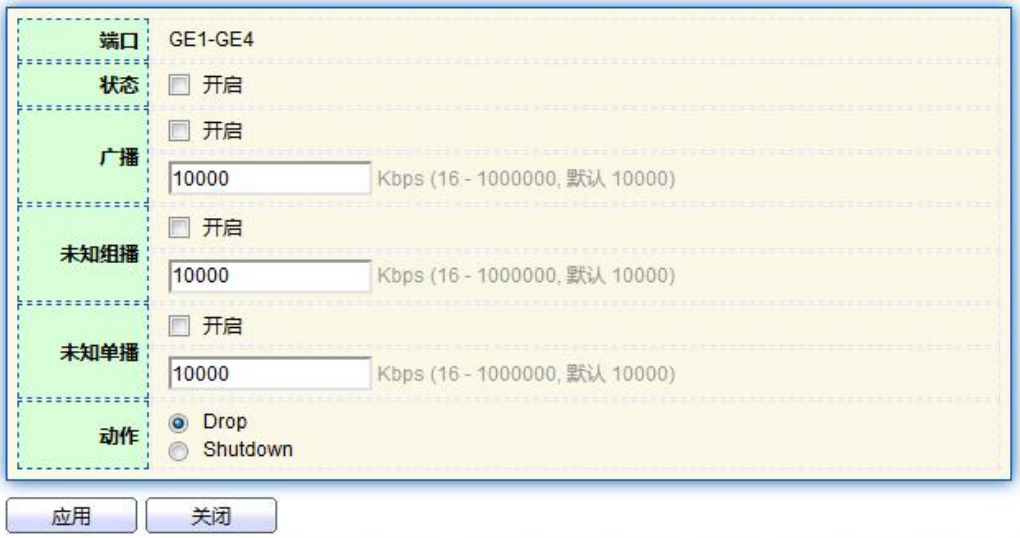
的端口，然后点击修改按钮：

端口配置表

编号	端口	状态	广播		未知组播		未知单播		动作
			状态	速率 (Kbps)	状态	速率 (Kbps)	状态	速率 (Kbps)	
1	GE1	禁用	禁用	10000	禁用	10000	禁用	10000	Drop
2	GE2	禁用	禁用	10000	禁用	10000	禁用	10000	Drop
3	GE3	禁用	禁用	10000	禁用	10000	禁用	10000	Drop
4	GE4	禁用	禁用	10000	禁用	10000	禁用	10000	Drop
5	GE5	禁用	禁用	10000	禁用	10000	禁用	10000	Drop
6	GE6	禁用	禁用	10000	禁用	10000	禁用	10000	Drop

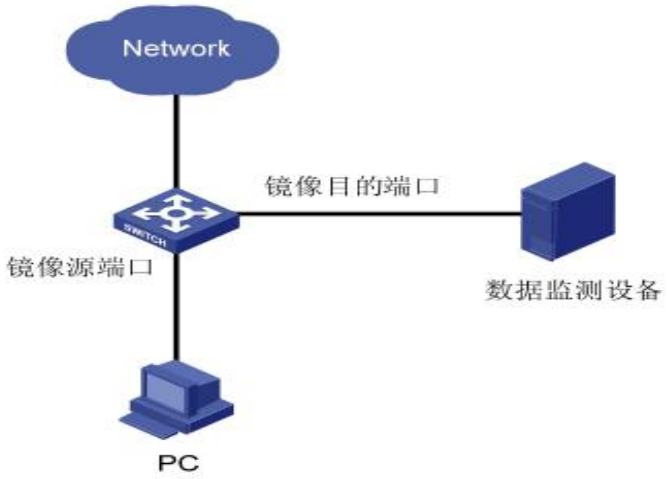
3. 进入修改界面，配置风暴控制开关，速率等信息，配置完成，点击应用保存，界面如下：

修改端口配置



5.9 镜像功能

端口镜像是把交换机指定端口的报文复制到目的端口；其中被复制的端口称为源端口，复制的端口称为目的端口。目的端口会接入数据检测设备，用户利用这些设备分析目的端口接收到的报文，进行网络监控和故障排除。如下图所示：



配置实例

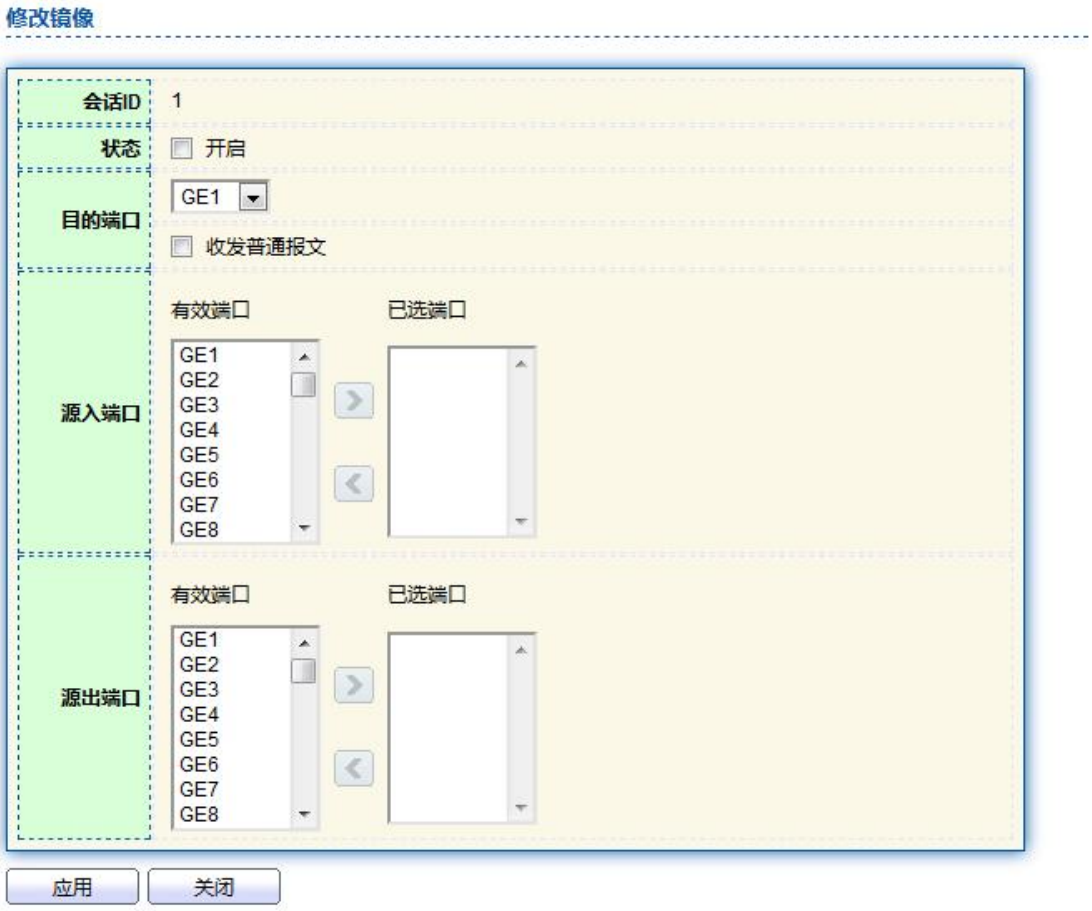
PC1 通过接口 ge1 接入 SwitchA。PC2 直连在 SwitchA 的 ge2 接口上。

用户希望通过监控设备 PC2 对 PC1 发送的报文进行监控。

操作步骤：

1. 单击导航栏中“端口 > 镜像功能”菜单，进入镜像配置页面。页面可以配置 4 组流镜像规则，界面如下：

2. 选择其中一组镜像会话，点击修改按钮，进入镜像组配置界面：



界面信息含义如下表

配置项	说明
会话 ID	交换机缺省有 4 个镜像会话 ID
状态	镜像组是否使能
目的端口	不能是链路汇聚端口，只能选择一个普通物理端口作为目的端口，不能同时选为源端口
源入端口	该端口的任何接收报文都被镜像到目的端口。
源出端口	该端口的任何发送报文都被镜像到目的端口。

6 POE 设置

POE (Power Over Ethernet)指的是在现有的以太网 Cat.5 布线基础架构不作任何改动的情况下，在为一些基于 IP 的终端（如 IP 电话机、无线局域网接入点 AP、网络摄像机等）传输数据信号的同时，还能为此类设备提供直流供电的技术。POE 技术能在确保现有结构化布线安全的同时保证现有网络的正常运作，最大限度地降低成本。

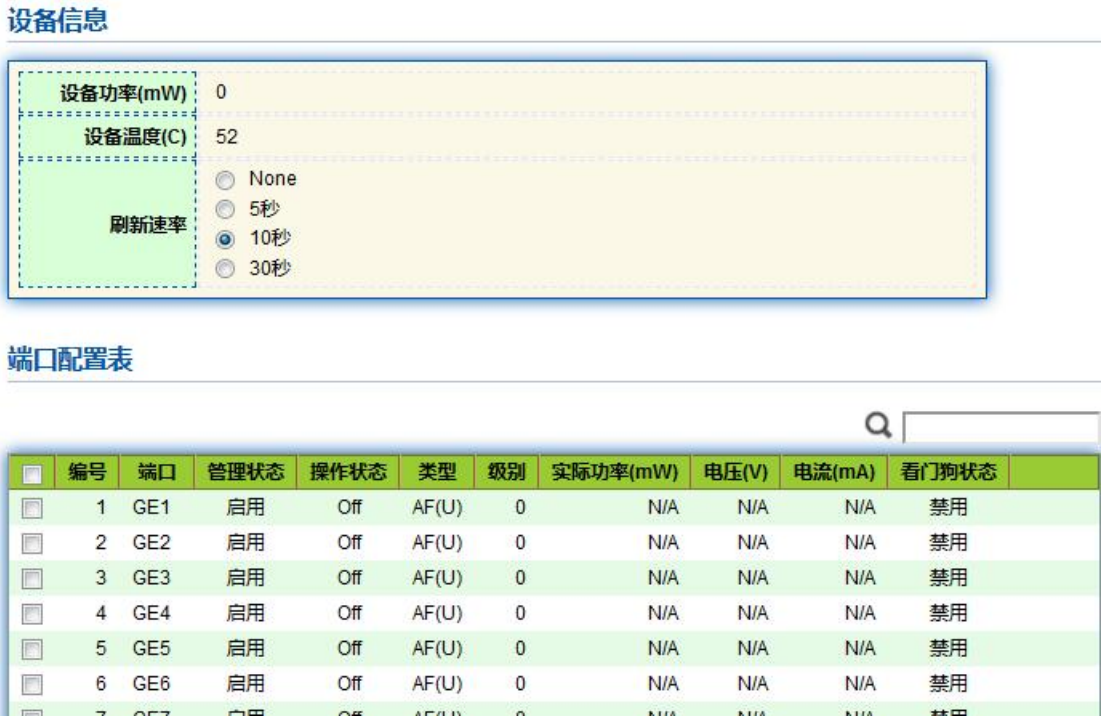
POE 也被称为基于局域网的供电系统(PoL, Power over LAN)或有源以太网(Active Ethernet)，有时也被简称为以太网供电，这是利用现存标准以太网传输电缆的同时传送数据和电功率的最新标准规范，并保持了与现存以太网系统和用户的兼容性。IEEE 802.3af 标准是基于以太网供电系统 POE 的新标准，它在 IEEE 802.3 的基础上增加了通过网线直接供电的相关标准，是现有以太网标准的扩展，也是第一个关于电源分配的国际标准。

6.1 POE 端口设置

通过 POE 端口管理页，可以对 POE 功能进行设置

操作步骤:

1. 单击导航栏中“POE 设置 > POE 端口设置”菜单，如下图所示:



2. 选择端口后点击“修改”，进入端口修改界面，如下图:

界面信息含义如下表

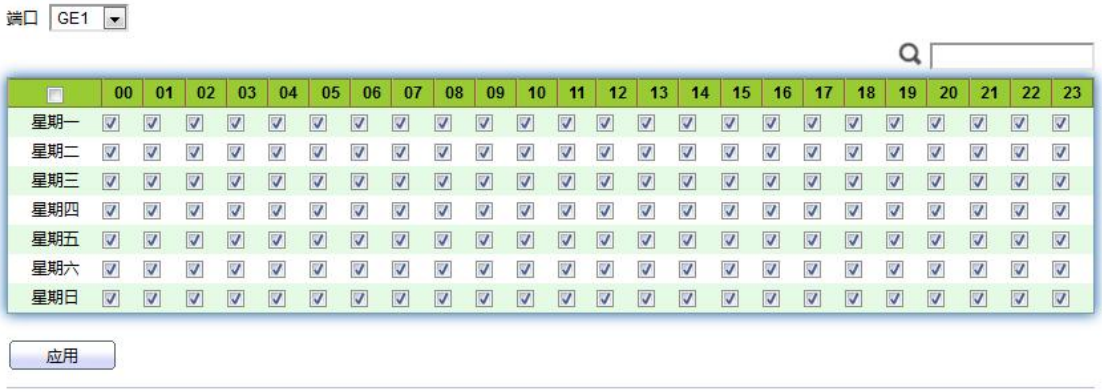
配置项	说明
端口	勾先的端口列表
管理状态	使能和去使能端口 POE 供电
看门狗状态	使能和去使能端口看门狗功能

6.2 POE 端口定时设置

通过 POE 端口定时设置，可以针对不需要在某段或全天不供电的设备所连接的端口定时的供电或取消供电，从而达到节能减排的功效

操作步骤：

1. 单击导航栏中“POE 设置 > POE 端口定时设置”菜单，如下图所示：

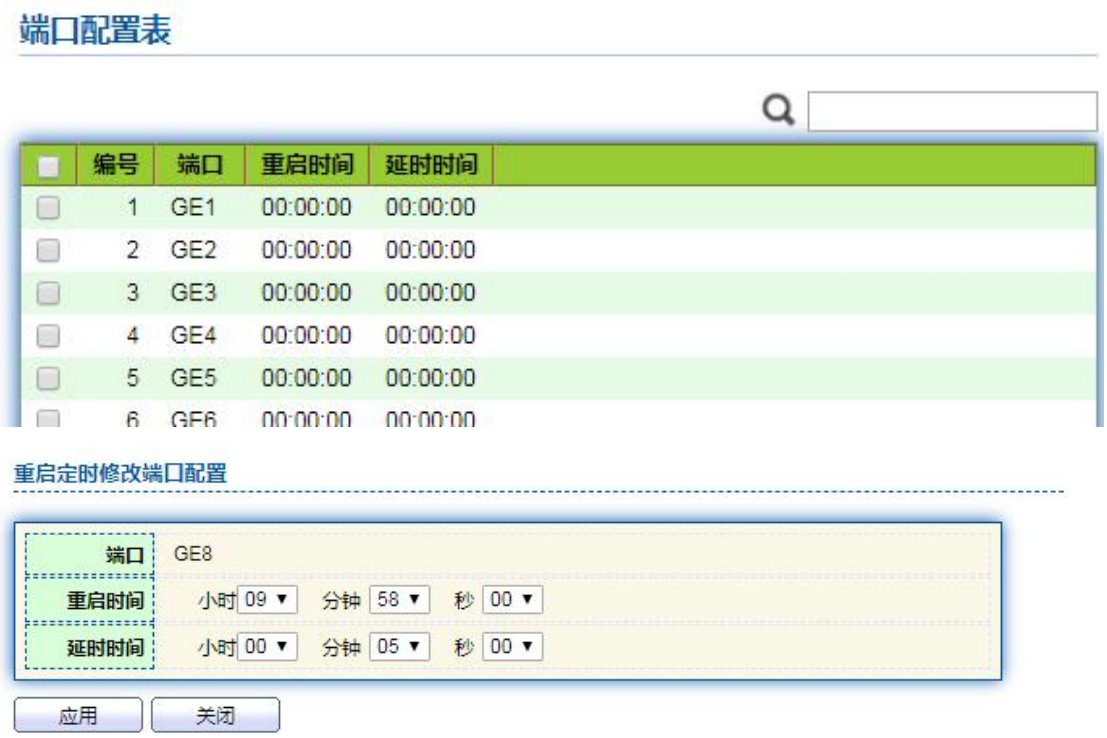


6.3 POE 端口定时重启设置

通过 POE 端口定时重启设置，可以基于端口周期性的进行供电的重启。

操作步骤：

1. 单击导航栏中“POE 设置 > POE 端口定时重启设置”菜单，如下图所示：



界面信息含义如下表

配置项	说明
端口	选择的端口列表
重启时间	设置 POE 端口关闭 POE 供电的对时时间，仅支持设置到分钟
延时时间	在重启时间关闭 POE 供电后，延时多久时间重启开启供电，仅支持设置到分钟

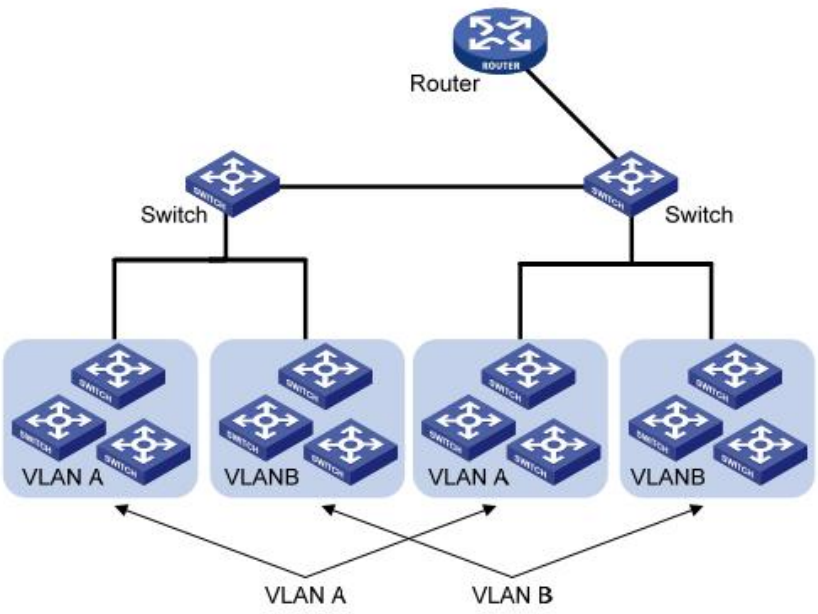
约束：

1. 使用该功能需要设置系统时间同步
2. POE 端口定时重启最小粒度时间为分钟
3. 当设置了重启时间时，延时时间需要设置
4. 当延时时间为 00:00:00 时，表示不再开启端口供电

7 VLAN 功能

VLAN 的组成不受物理位置的限制，因此同一 VLAN 内的主机也无须放置在同一物理空间里。如下图所示，VLAN 把一个物理上的 LAN 划分成多个逻辑上的 LAN ，每个 VLAN 是一个广播域。VLAN 内的主机间通过传统的以太网通信方式即可进行报文的交互，而处在不同 VLAN 内的主机之间如果需要通信，则必须通过路由器或三层交换机等网络层设备才能

够实现。



与传统以太网相比，VLAN 具有如下的优点：

- 控制广播域的范围：局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强了 LAN 的安全性：由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。
- 灵活创建虚拟工作组：使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。

此管理型交换机支持 802.1Q VLAN、基于协议的 VLAN、基于 MAC 的 VLAN 以及基于端口的 VLAN。在缺省配置时，VLAN 为 802.1Q VLAN 模式。

基于端口的 VLAN，其原理是根据交换设备的接口编号来划分 VLAN。网络管理员给交换机的每个接口配置不同的 PVID，即一个接口缺省属于的 VLAN。当一个数据帧进入交换机接口时，如果没有带 VLAN 标签，且该接口上配置了 PVID，那么，该数据帧就会被打上接口的 PVID。如果进入的帧已经带有 VLAN 标签，那么交换机不会再增加 VLAN 标签，即使接口已经配置了 PVID。

对 VLAN 帧的处理由接口类型决定。优点是定义成员简单。缺点是成员移动需重新配置 VLAN。

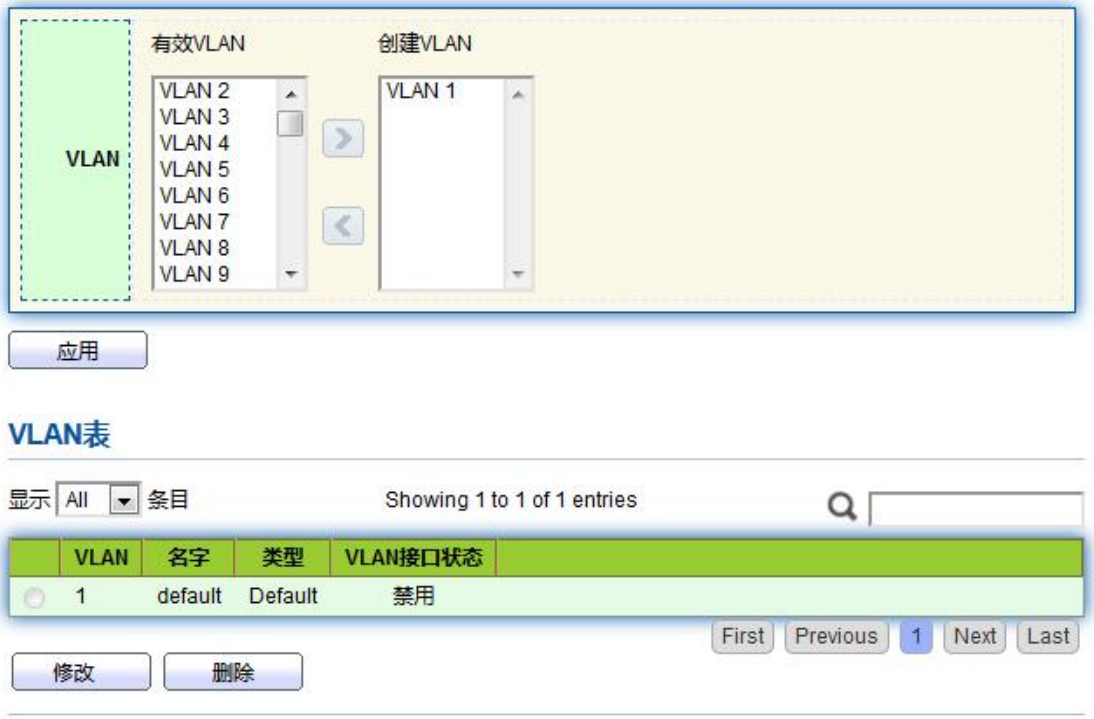
7.1 VLAN 配置

7.1.1 创建 VLAN

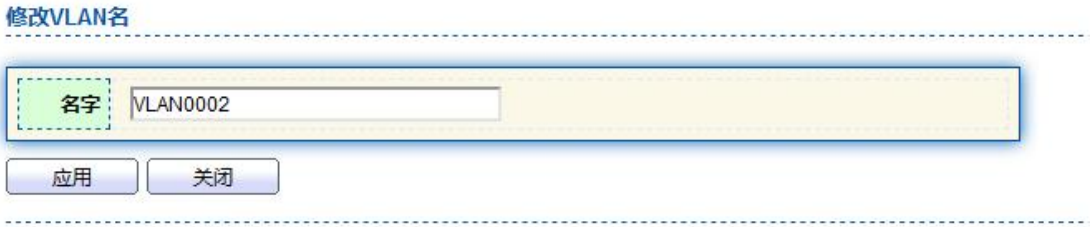
操作步骤：

1. 单击导航树中的“VLAN 功能 > VLAN 配置 > 创建 VLAN”菜单，进入创建 VLAN 界面，

选择有效 VLAN 框内的 VLAN 名称，点击向右箭头，移动到创建 VLAN 框中(最多可以创建 256 个 VLAN)，点击应用保存生效，如下图所示：



2. 创建 VLAN 之后，VLAN 会显示在 VLAN 表内，选择需要修改的 VLAN，点击修改按钮，进入 VLAN 修改页面，如下图：



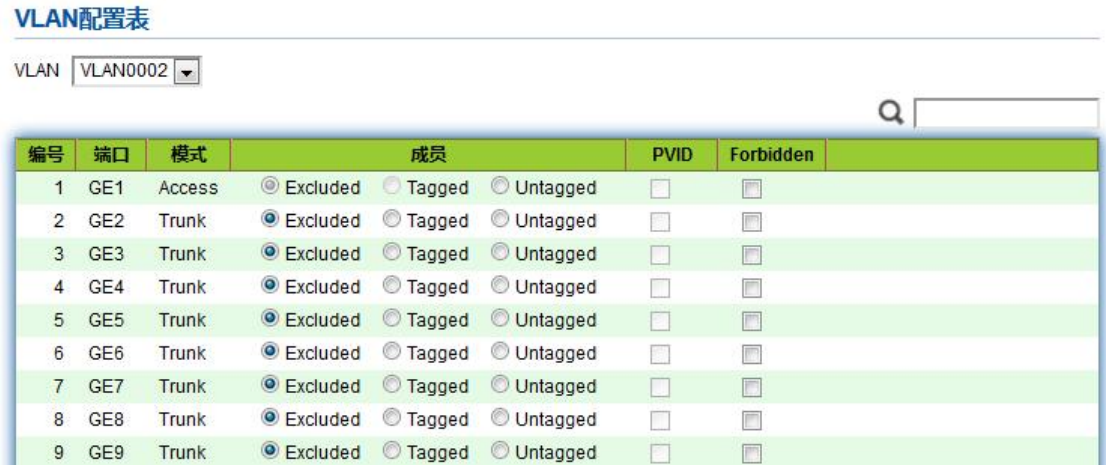
界面信息含义如下表所示。

配置项	说明
VLAN ID	必选，指定加入 VLAN ID 号，取值范围是 1～4094。如：1-3，5，7，9。其中 VLAN 1 是默认的，新建时不会重新创建 VLAN 1。
名字	可选，对 VLAN 的具体描述，可以根据需要进行修改。

7.1.2 设置 VLAN

将端口加入 VLAN 有两种方式，一种是一个 VLAN 下添加多个端口，一种是一个端口加

入到多个 VLAN 中，此两种操作方式因为目的不同，因此采用两种配置方式实现。
操作步骤：
1. 单击导航树中的“VLAN 功能 > VLAN 配置 > 设置 VLAN”菜单，进入 VLAN 配置界面，此时界面中先通过左上角选择需要配置的 VLAN ID，然后点选操作配置 VLAN 中的端口信息，如下图所示：

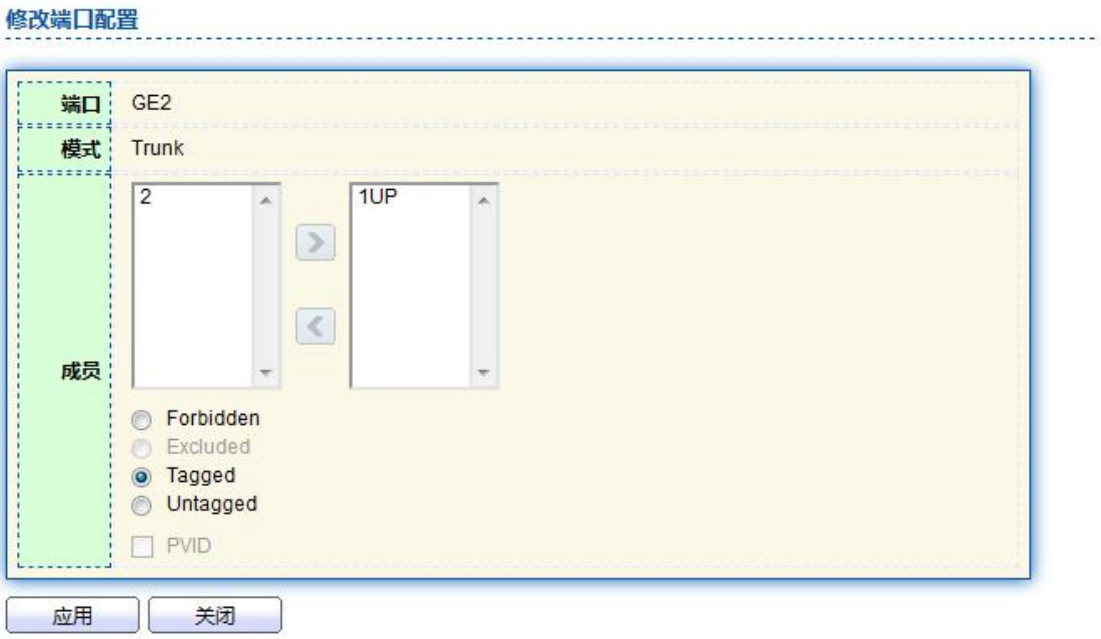


界面信息含义如下表所示。

配置项	说明
VLAN	需要配置的 VLAN ID
成员	该 VLAN 内端口的成员角色信息： Excluded：端口不属于此 VLAN Tagged：端口是此 VLAN 的 Tagged 成员 Untagged：端口是此 VLAN 的 Untagged 成员
PVID	此 VLAN 是否是端口的 PVID
Forbidden	端口是否禁止转发此 VLAN 报文

7.1.3 成员配置

一个端口添加到多个 VLAN：
1. 单击导航树中的“VLAN 功能 > VLAN 配置 > 成员配置”菜单，进入成员配置界面，选择需要配置的端口，点击修改，进行该端口的 VLAN 属性配置：



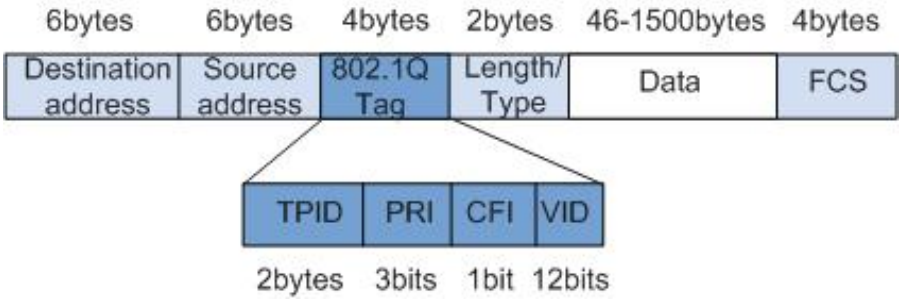
界面信息含义如下表所示。

配置项	说明
端口	需要配置的端口号
模式	端口当前的 VLAN 模式，在端口设置中修改： **Hybrid**：混合模式，该模式端口可以任意属于多个 VLAN 的 Tagged 端口和多个 VLAN 的 Untagged 端口 **Access**：该模式下端口只能属于一个 VLAN 成员 **Trunk**：该模式下端口只属于 PVID 的 Untagged 成员，可以属于多个 VLAN 的 Tagged 成员。
成员	此端口属于的 VLAN ID 及在 VLAN 内的属性： **Forbidden**：禁止转发此 VLAN 报文 **Excluded**：不属于此 VLAN **Tagged**：VLAN 的 Tagged 成员 **Untagged**：VLAN 的 Untagged 成员 **PVID**：此 VLAN 是否是端口的 PVLAN

7.1.4 端口配置

Trunk 配置，Trunk 类型的接口用来连接其它交换机设备，它主要连接干道链路。Trunk 接口允许多个 VLAN 的帧通过。Trunk 链路的封装协议是 IEEE 802.1q，IEEE 802.1q 是虚拟桥接局域网的正式标准，对 Ethernet 帧格式进行了修改，在源 MAC 地址字段和协议类型字段之间加入 4 字节的 802.1q Tag

802.1q 帧格式



802.1Q Tag 各字段含义介绍

字段	长度	名称	解析
TPID	2bytes	Tag Protocol Identifier（标签协议标识符），表示帧类型。	取值为 0x8100 时表示 802.1q Tag 帧。如果不支持 802.1q 的设备收到这样的帧，会将其丢弃。
PRI	3bits	Priority，表示帧的优先级。	取值范围为 0 ~ 7，值越大优先级越高。用于当交换机阻塞时，优先发送优先级高的数据帧。
CFI	1bit	Canonical Format Indicator（标准格式指示位），表示 MAC 地址是否是经典格式。	CFI 为 0 说明是经典格式，CFI 为 1 表示为非经典格式。用于兼容以太网和令牌环网。在以太网中，CFI 的值为 0。
VID	12bits	VLAN ID	VLAN ID 取值范围是 0 ~ 4095。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的有效取值范围是 1 ~ 4094。

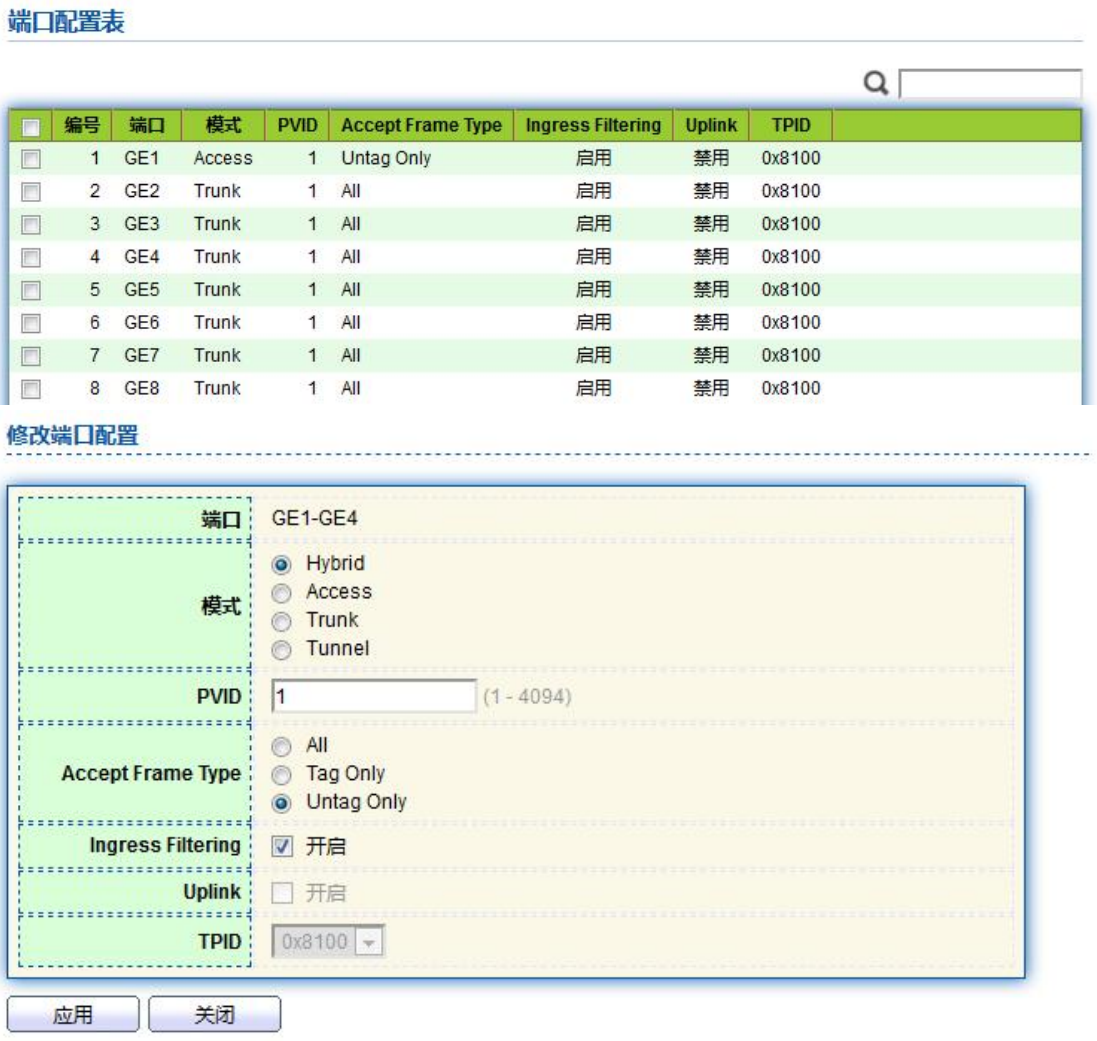
每台支持 802.1q 协议的交换机发送的数据包都会包含 VLAN ID，以指明交换机属于哪一个 VLAN。因此，在一个 VLAN 交换网络中，以太网帧有以下两种形式：

- 有标记帧（tagged frame）：加入了 4 字节 802.1q Tag 的帧
- 无标记帧（untagged frame）：原始的、未加入 4 字节 802.1q Tag 的帧

Trunk 类型的接口用来连接其它交换机设备，它主要连接干道链路。Trunk 接口允许多个 VLAN 的帧通过。

Trunk 口配置操作步骤：

1. 单击导航树中的“VLAN 功能 > VLAN 配置 > 端口配置”菜单，进入端口配置界面，选择需要配置的端口，点击修改，进行该端口的 VLAN 属性配置：



界面信息含义如下表所示。

配置项	说明
端口	需要配置的端口号
模式	端口当前的 VLAN 模式，在端口设置中修改： **Hybrid**：混合模式，该模式端口可以任意属于多个 VLAN 的 Tagged 端口和多个 VLAN 的 Untagged 端口 **Access**：该模式下端口只能属于一个 VLAN 成员 **Trunk**：该模式下端口只属于 PVID 的 Untagged 成员，可以属于多个 VLAN 的 Tagged 成员。
PVID	端口 PVLAN
Accept Frame Type	端口接收的报文类型： **All**：所有报文 **Tag Only**：只接收 Tagged 报文 **Untag Only**：只接收 Untagged 报文

Ingress Filtering	入口过滤功能开关，是否过滤不包含此端口的 VLAN 报文
Uplink	是否处于上行模式
TPID	VLAN Tag 的识别号

7.2 Voice VLAN

提高语音数据传输优先级的传统处理方法是使用 ACL（Access Control List）对语音数据进行区分，并使用 QoS（Quality of Service）保证传输质量。为简化用户配置，更方便的管理语音流的传输，提出了 Voice VLAN 特性。使能 Voice VLAN 功能的接口根据进入接口的数据流中的源 MAC 地址字段来判断该数据流是否为语音数据流。源 MAC 地址符合系统设置的语音设备 OUI（Organizationally Unique Identifier）地址的报文认为是语音数据流。接收到语音数据流的接口将自动加入 Voice VLAN 中传输。从而简化了用户配置，实现了用户方便管理语音数据。

Voice VLAN 的 OUI 地址：OUI 地址表示一个 MAC 地址段。将 48 位的 MAC 地址和掩码的对应位作与运算可以确定 OUI 地址。接入设备的 MAC 地址和 OUI 地址匹配的位数，由掩码中全“1”的长度决定。例如，MAC 地址为 1–1–1，掩码为 FFFF-FF00-0000，那么将 MAC 地址与其相应掩码位执行与运算的结果就是 OUI 地址 0001-0000-0000。
只要接入设备的 MAC 地址前 24 位和 OUI 地址的前 24 位匹配，那么使能 Voice VLAN 功能的接口将认为此数据流是语音数据流，接入的设备是语音设备。

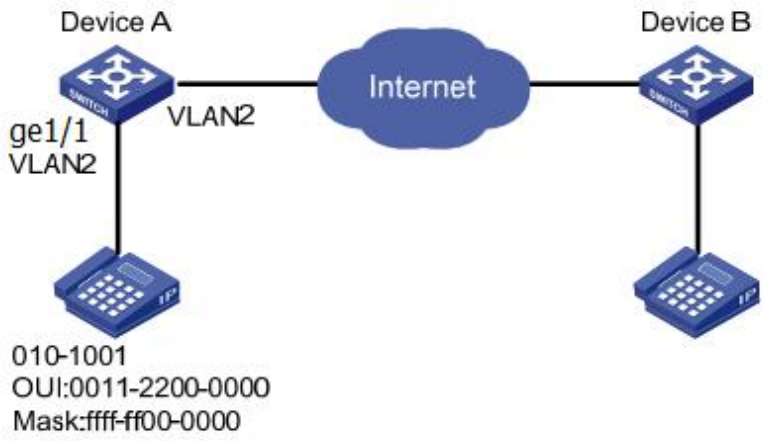
Voice VLAN 是为用户的语音数据流划分的 VLAN。用户通过创建 Voice VLAN 并将连接语音设备的接口加入到 Voice VLAN 中，使语音数据流集中在 Voice VLAN 中进行传输。
网络中经常同时存在语音数据和非语音数据两种流量。语音数据在传输时需要具有比其他业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。
1. 单击导航树中的“VLAN 功能 > Voice VLAN > 功能配置”菜单，进入语音 VLAN 的配置界面，如下图所示。

配置项	说明
状态	通过选择启用 Voice VLAN
VLAN	指定加入 VLAN ID 号，取值范围是 1～4094。如：1-3，5，7，9。其中 VLAN 1 是默认的。其他 VLAN 必须存在，且以 UNTAG 方式加入需要链接的端口。
CoS 重标记	选择是否需要重定义 Voice VLAN 报文优先级。
老化时间	表项老化时间
端口	使能 Voice VLAN 的端口
模式	端口 Voice VLAN 操作模式，分为自动模式和手工模式
QoS 策略	选择 QoS 对哪种报文生效

2. 单击导航树中的“VLAN 功能 > Voice VLAN > Voice OUI 配置”菜单，进入语音 VLAN 的 OUI 地址表配置界面，在此页面配置 Voice VLAN 的 OUI 地址段，如下图所示。

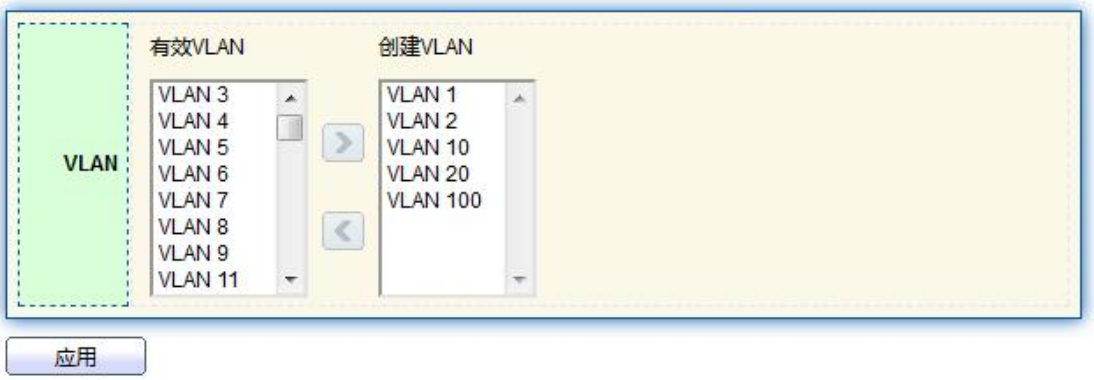
3. 填写相应的配置项，单击“应用”，完成配置，如下图所示。

下面举个例子来说明，通过配置手动模式下的 Voice VLAN，使接入 IP 电话的端口通过人为控制加入/退出 Voice VLAN，并将语音流在该 VLAN 内传输。创建 VLAN2 为 Voice VLAN，使其工作在 Voice VLAN 安全模式，只允许语音数据通过。IP 电话发送 UNTAG 语音流，接入端口是 Trunk 类型端口 GE1。用户需要设置一个自定义的 OUI 地址 0011-2231-05e1。配置自动模式下的 Voice VLAN 的组网图

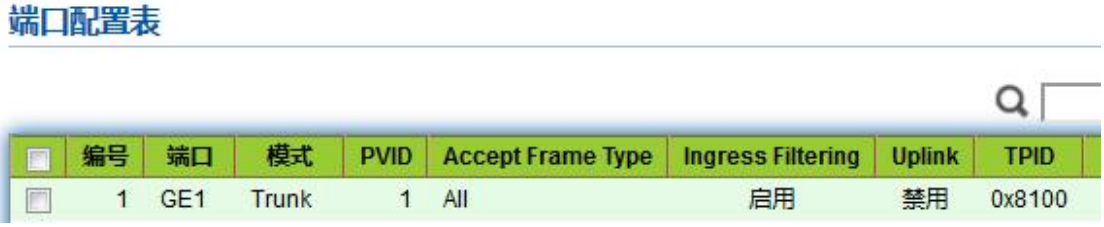


操作步骤：

1. 创建 VLAN，确定员工所属的 VLAN。单击导航树中的“VLAN 功能 > VLAN 配置 > 创建 VLAN”菜单，选择 VLAN2，向右添加到创建 VLAN 列表，点击应用生效：



2. 配置 SwitchA 以太网接口 GE1 为 Trunk 模式。单击导航树中的“VLAN 功能 > VLAN 配置 > 端口配置”菜单，选择 GE1，点击修改，选择端口模式为 Trunk



3. 单击导航树中的“VLAN 功能 > Voice VLAN > Voice OUI 配置”菜单，配置 OUI MAC 地址范围，点击添加，输入语音设备的 MAC 地址前 24 位：00:11:22，单击“应用”，完成配置，如下图所示：

4. 开启端口 GE1 的 Voice VLAN 功能。单击导航树中的“VLAN 功能 > Voice VLAN > 功能配置”菜单，全局配置点击开启，选择 VLAN2，点击应用。再端口配置列表中选择端口 GE1，点击修改，选择开启，模式配置为自动即可，点击应用，结果如下图：

注意：

- 不需要配置端口在 VLAN2 内，开启端口的 Voice VLAN 自动模式，端口会自动转发 Voice VLAN 报文。

7.3 协议 VLAN 配置

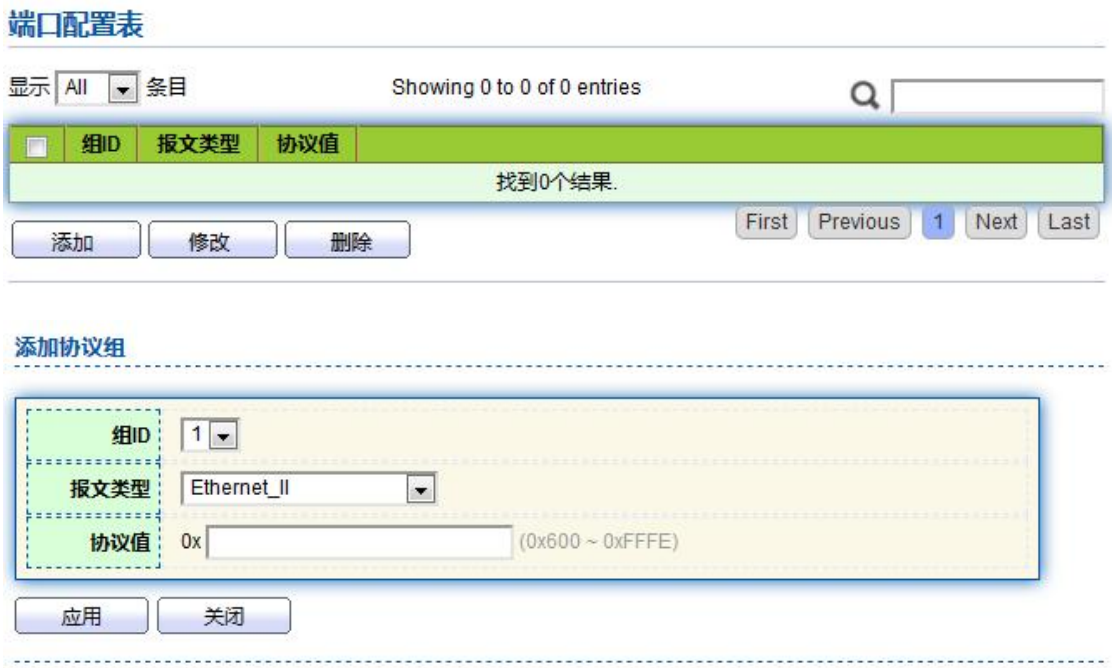
基于协议类型划分 VLAN，其原理是根据接口接收到的报文所属的协议（族）类型及封装格式来给报文分配不同的 VLAN ID。

网络管理员需要配置以太网帧中的协议域和 VLAN ID 的映射关系表，如果收到的是 untagged（不带 VLAN 标签）帧，则依据该表添加 VLAN ID。优点是：基于协议划分 VLAN，

将网络中提供的服务类型与 VLAN 相绑定，方便管理和维护。缺点是：需要对网络中所有的协议类型和 VLAN ID 的映射关系表进行初始配置。需要分析各种协议的地址格式并进行相应的转换，消耗交换机较多的资源，速度上稍具劣势。

操作步骤：

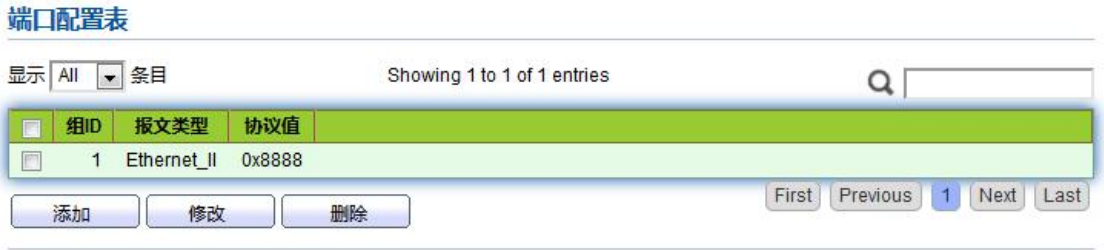
1. 单击导航树中的“VLAN 功能 > 协议 VLAN 配置 > 协议组配置”菜单，进入协议 VLAN 组配置界面，如下图所示。



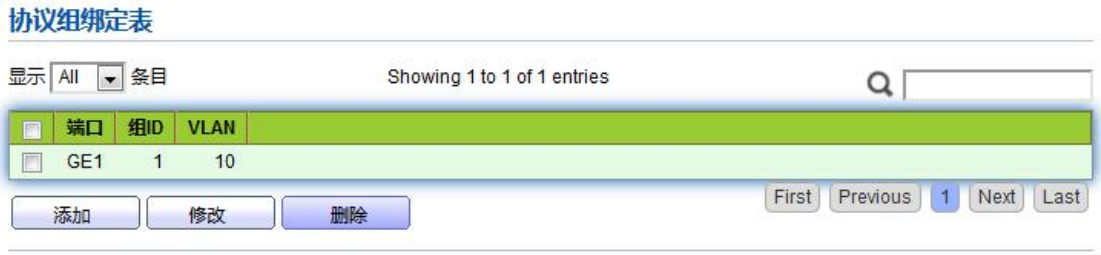
界面信息含义如下表所示。

配置项	说明
组 ID	协议 VLAN 组
报文类型	帧类型有 ETHER2，LLC，RFC-1042
协议值	协议值可以选填从 0x600~oxFFFE

2. 填写相应的配置项，单击“应用”，完成配置。



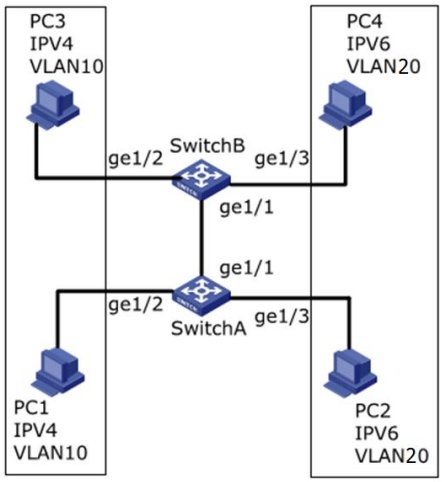
3. 单击导航树中的“VLAN 功能 > 协议 VLAN 配置 > 协议组绑定”菜单，绑定配置的协议号、端口号、VLANID，使协议 VLAN 配置生效，如下图：



说明:

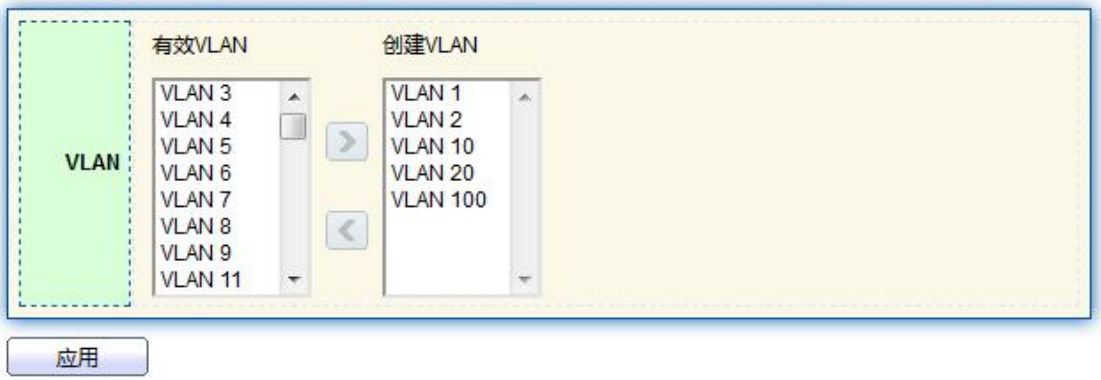
设置匹配协议 IPv4 与 IPv6，需要同时匹配设置 ARP 协议。

下面举个例子来说明，如下图 PC1 与 PC3 之间可以互访，通信协议采用 IPv4，将 IPv4 协议绑定到 VLAN10 中。PC2 与 PC4 之间可以互访，通信协议采用 IPv6，将 IPv6 协议绑定到 VLAN20 中。



操作步骤:

1. 创建 VLAN，确定员工所属的 VLAN。单击导航树中的“VLAN 功能 > VLAN 配置 > 创建 VLAN”菜单，选择 VLAN10、VLAN20，向右添加到创建 VLAN 列表，点击应用生效:



2. 配置 SwitchA 以太网接口 GE2 与 GE3 为 Hybrid 模式。单击导航树中的“VLAN 功能 > VLAN

配置 > 端口配置”菜单，选择 GE2、GE3，点击修改，选择端口模式为 Hybrid：

端口配置表

编号	端口	模式	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	GE1	Trunk	1	All	启用	禁用	0x8100
2	GE2	Hybrid	1	All	启用	禁用	0x8100
3	GE3	Hybrid	1	All	启用	禁用	0x8100
4	GE4	Trunk	1	All	启用	禁用	0x8100
5	GE5	Trunk	1	All	启用	禁用	0x8100

3. 配置 GE2 端口 Untagged 加入 VLAN10，GE3 端口 Untagged 加入 VLAN20。单击导航树中的“VLAN 功能 > VLAN 配置 > 设置 VLAN”菜单，下拉框中选择 VLAN10，再选择 GE2 为 Untagged 端口。相同配置，将 GE3 加入 VLAN20 的 Untagged 端口，如下图所示

VLAN配置表

VLAN VLAN0010

编号	端口	模式	成员			PVID	Forbidden
1	GE1	Trunk	Excluded	Tagged	Untagged		
2	GE2	Hybrid	Excluded	Tagged	Untagged		
3	GE3	Hybrid	Excluded	Tagged	Untagged		
4	GE4	Trunk	Excluded	Tagged	Untagged		

VLAN配置表

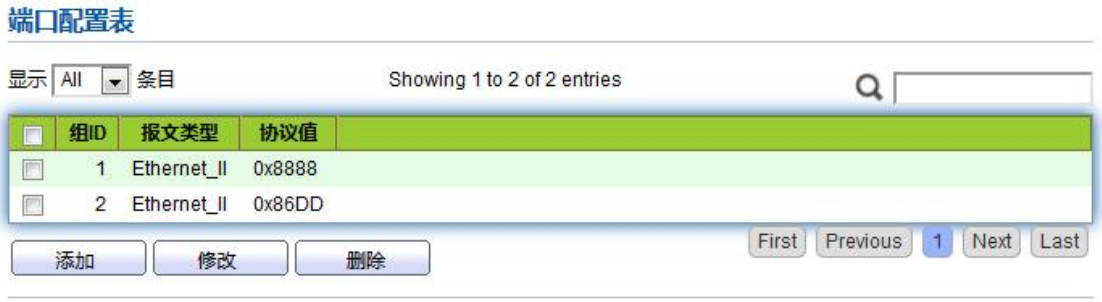
VLAN VLAN0020

编号	端口	模式	成员			PVID	Forbidden
1	GE1	Trunk	Excluded	Tagged	Untagged		
2	GE2	Hybrid	Excluded	Tagged	Untagged		
3	GE3	Hybrid	Excluded	Tagged	Untagged		
4	GE4	Trunk	Excluded	Tagged	Untagged		

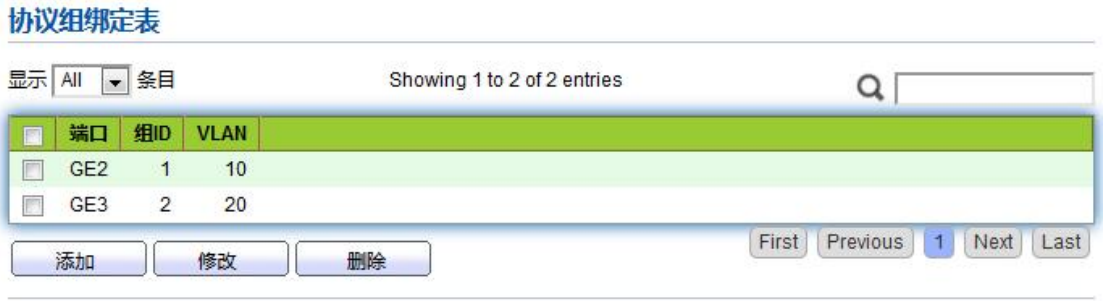
4. 配置 SwitchB 以太网接口 GE2 与 GE3 以 UNTAG 方式加入需要链接的端口方式加入 VLAN。操作同 2、3，不再赘述。

5. 在 SwitchA 上配置接口 GE1 以 Tagged 方式加入 VLAN10 与 VLAN 20。单击导航树中的“VLAN 功能 > VLAN 配置 > 设置 VLAN”菜单，下拉框选择 VLAN10，选择 GE1 为 Tagged 成员。同理配置 VLAN20

6. 关联协议和 VLAN，实现根据接口接收到的报文所属的协议（族）类型给报文分配不同的 VLAN ID。单击导航树中的“VLAN 功能 > 协议 VLAN 配置 > 协议组配置 ”菜单，进入协议 VLAN 组配置界面，添加两条协议组规则



7. 绑定端口、协议组和 VLAN。单击导航树中的“VLAN 功能 > 协议 VLAN 配置 > 协议组绑定 ”菜单，进入协议 VLAN 组配置界面，点击添加，分别将 GE2、绑定组 ID1 和 VLAN10 绑定，GE3、绑定组 ID2 和 VLAN20 绑定



7.4 MAC VLAN 配置

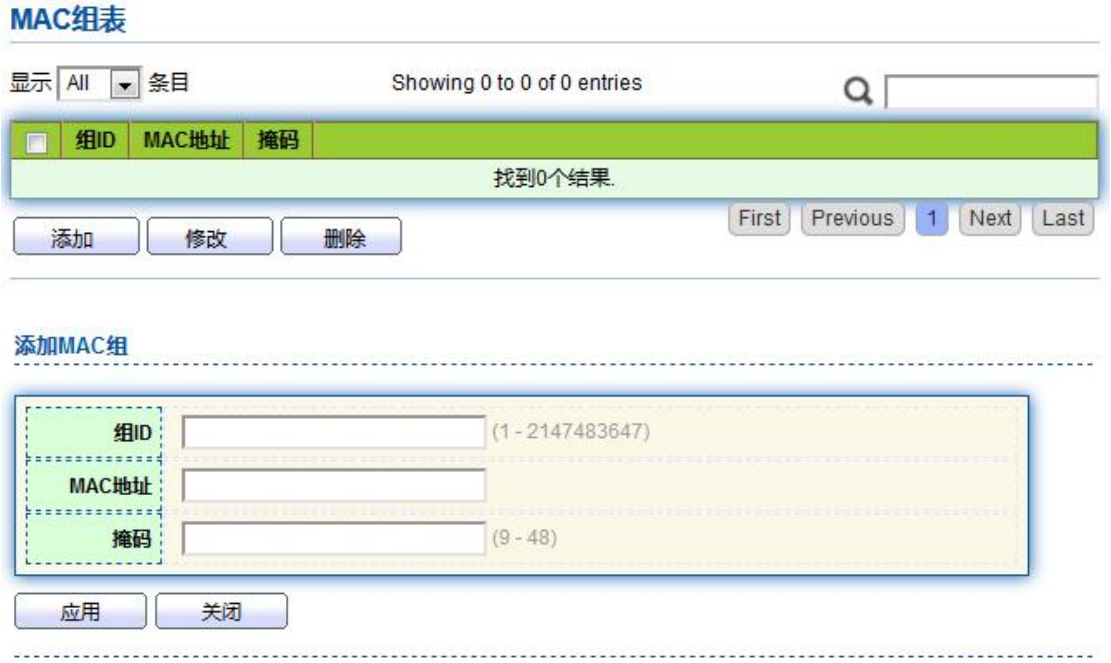
基于 MAC 的 VLAN,其原理是根据计算机网卡的 MAC 地址来划分 VLAN。网络管理员成功配置 MAC 地址和 VLAN ID 映射关系表，如果交换机收到的是 untagged（不带 VLAN 标

签）帧，则依据该表添加 VLAN ID。

优点是：当终端用户的物理位置发生改变，不需要重新配置 VLAN。提高了终端用户的安全性和接入的灵活性。缺点是：只适用于网卡不经常更换、网络环境较简单的场景中，需要预先定义网络中所有成员。

操作步骤：

1. 单击导航树中的“VLAN 功能 > MAC VLAN 配置 > MAC 组配置”菜单，进入 MAC 组配置界面，点击添加按钮，新增一个 MAC 组，如下图：



界面信息含义如下表所示。

配置项	说明
组 ID	MAC VLAN 组 ID
MAC 地址	需要绑定 VLAN 的 MAC 地址
掩码	用来指示 MAC 地址端，精确匹配 MAC 填写 48，其它与 IP 地址掩码效果一致

下面举个例子来说明，某公司对信息安全要求较高，要求只有本公司的 PC 才可以访问公司网络。 如图所示，Switch 的接口 GE1 与 SwitchA 上行口相连。 SwitchA 的下行接口分别与 PC1、PC2、PC3 相连。 要求 PC1、PC2、PC3 可以通过 SwitchA、Switch 访问公司网络，如换成其他 PC 则不能访问。

配置思路:采用如下的思路配置基于 MAC 地址的 VLAN 划分：

- 创建相关 VLAN。
- 配置各以太网接口以正确的方式加入 VLAN。
- 配置 PC1、PC2、PC3 的 MAC 地址与 VLAN 关联。

数据准备:为完成此配置例，需准备如下的数据：

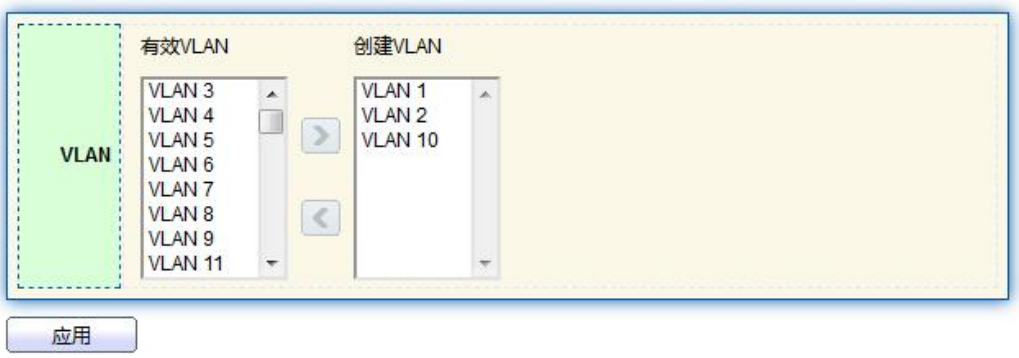
- 在 Switch 上配置接口 GE1 的 PVID 为 100。

- 在 Switch 上配置接口 GE1 以 untagged 方式加入 VLAN10。
- 在 Switch 上配置接口 GE2 以 tagged 方式加入 VLAN10。
- 在 SwitchA 上的接口使用默认配置，即所有接口以 untagged 方式加入 VLAN1。
- 获取 PC1、PC2、PC3 的 MAC 地址，配置 MAC 地址与 VLAN10 关联。

配置基于 MAC 地址的 VLAN 划分组网图:

操作步骤:

1. 创建 VLAN，确定员工所属的 VLAN。单击导航树中的"VLAN 功能 > VLAN 配置 > 创建 VLAN"菜单，选择 VLAN10，向右添加到创建 VLAN 列表，点击应用生效:



2. 配置 Switch 以太网接口 GE1 的模式为 Hybrid，端口 PVID 为 100，端口属于 VLAN 10 的 Untagged 成员，配置 Switch 以太网接口 GE2 的模式为 Trunk，并将端口添加到 VLAN 10 的 Tagged 成员列表中:

3. 在 SwitchA 上的接口使用默认配置，即所有接口以 untagged 方式加入 VLAN1。配置 PC1、PC2、PC3 的 MAC 地址与 VLAN10 关联。单击导航树中的"VLAN 功能 > MAC VLAN 配置 > MAC 组配置"菜单，进入 MAC 组配置界面，分别输入 PC1（0022-0022-0022）、PC2（0033-0033-0033）、PC3（0044-0044-0044）的 MAC 地址，掩码为 48 位精确匹配，如下图所示:

4. 单击导航树中的“VLAN 功能 > MAC VLAN 配置 > MAC 组绑定”菜单，进入 MAC 组绑定界面，点击添加，选择端口(只能为 Hybrid 端口)，选择绑定 MAC 组 ID，指定绑定 VLANID，点击应用完成配置：

5. 检查配置结果

PC1、PC2、PC3 可以访问公司网络，如换成其他外来人员的 PC 则不能访问。

7.5 Surveillance VLAN

视频 VLAN 主要用于视频流数据包。为了保证这些包在传输过程中的优先级，它高于普通包

操作步骤：

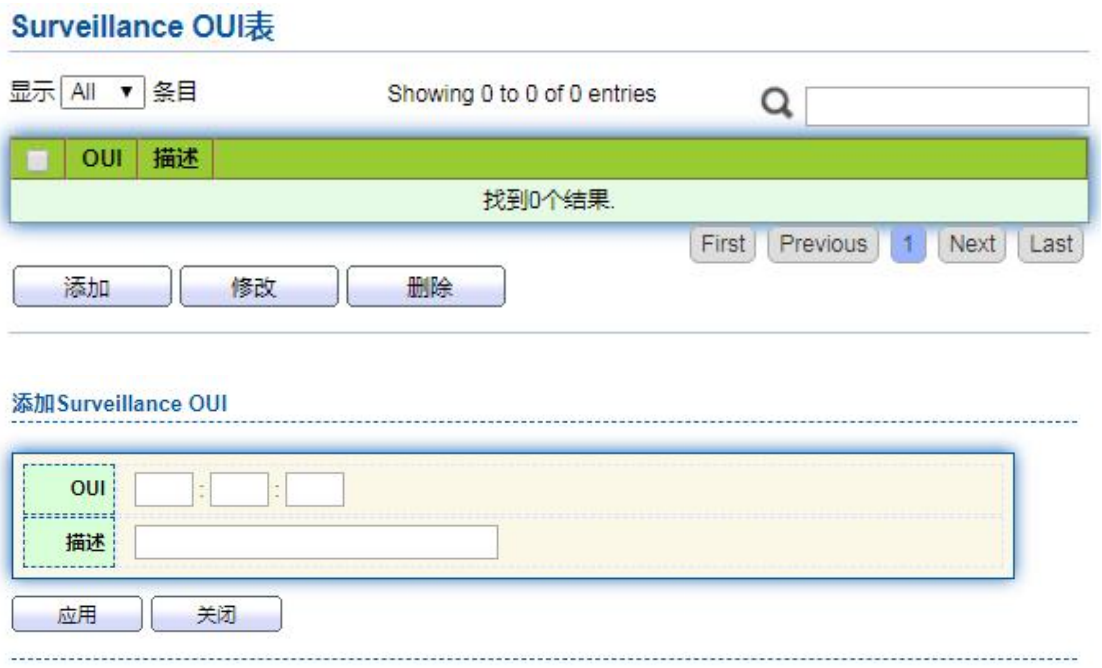
1. 单击导航树中的“VLAN 功能 > Surveillance VLAN > 功能配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
状态	通过选择启用 Surveillance VLAN
VLAN	指定加入 VLAN ID 号，取值范围是 1～4094。如：1-3，5，7，9。其中 VLAN 1 是默认的。其他 VLAN 必须存在，且以 UNTAG 方式加入需要链接的端口。
CoS 重标记	选择是否需要重定义 Surveillance VLAN 报文优先级。
老化时间	表项老化时间

端口	使能 Surveillance VLAN 的端口
模式	端口 Voice VLAN 操作模式，分为自动模式和手工模式
QoS 策略	选择 QoS 对哪种报文生效

2. 单击导航树中的“VLAN 功能 > Voice VLAN > Surveillance OUI 配置”菜单，进入 OUI 地址表配置界面，如下图所示。



3. 填写相应的配置项，单击“应用”，完成配置，如下图所示。

7.6 GVRP

GVRP-VLAN 注册协议是通用属性注册协议的一个应用，它提供了 802.1Q 兼容的 VLAN 剪枝功能和在 802.1Q 中继端口上动态建立 VLAN。

GVRP 交换机可以相互交换 VLAN 配置信息，切断不必要的广播和未知的单播业务，在通过 802.1Q 中继连接的交换机上动态创建和管理 VLAN。

GVRP 中使用了 GID 和 GIP，分别为基于 GARP 的应用提供了通用的状态机制描述和信息分发机制。GVRP 仅在 802.1Q 中继链路上运行。GVRP 切断了中继链路，以便在中继连接上只传输活动的 VLAN。在 GVRP 向干线添加 VLAN 之前，它首先从交换机接收连接信息。GVRP 更新信息和计时器可以更改。GVRP 端口有多种操作模式来控制如何定制 VLAN。GVRP 可以为 VLAN 数据库动态添加和管理 VLAN

GVRP 支持在设备之间传播 VLAN 信息。在 GVRP 中，可以手动配置交换机的 VLAN 信息，网络中的所有其他交换机都可以动态地理解 VLAN。终端节点可以访问任何交换机并连接到所需的 VLAN。为了使用 GVRP，应安装与 GVRP 兼容的网络接口卡（NIC）。与 GVRP 兼容的 NIC 可以配置为加入所需的 VLAN，然后访问启用 GVRP 的交换机。建立了网卡与交换机的通信连接，实现了网卡与交换机的 VLAN 连接。

7.6.1 功能配置

操作步骤：

1. 单击导航树中的“VLAN 功能 > GVRP > 功能配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
状态	GVRP 全局开关状态
Join	在 1-20 厘秒范围内的值，即以百分之一秒为单位。默认值为 20cs。
Leave	在 60-300 厘秒范围内的值，即以百分之一秒为单位。默认值为 60cs。
LeaveAll	在 1000-5000 厘秒范围内的值，即以百分之一秒为单位。默认值为 1000cs。

2. 选择端口列表，点击“修改”进入端口开关配置界面，如下图所示。

界面信息含义如下表所示。

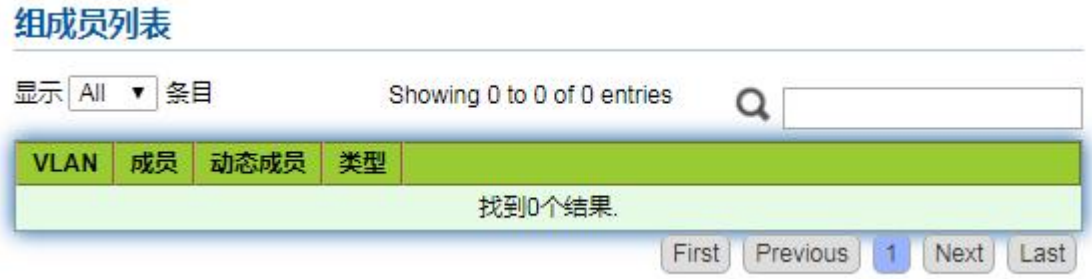
查询项	说明
端口	端口列表
状态	使能和去使能端口 GVRP 开关
VLAN 创建功能	使能和去使能自动创建 VLAN 开关
注册模式	Normal：允许动态 VLAN 在端口上注册，同时发送静态 VLAN 和动态 VLAN 的声明消息 Fixed：不允许在端口上注册动态 VLAN，只发送静态 VLAN 声明消息 Forbidden：不允许在端口上注册动态 VLAN。同时，删除端口上除 VLAN 1 以外的所有 VLAN，只发送 VLAN 1 声明消息

7.6.2 成员列表

查看 GVRP 动态成员信息表项

操作步骤：

1. 单击导航树中的“VLAN 功能 > GVRP > 成员列表”菜单进入界面，如下图所示：

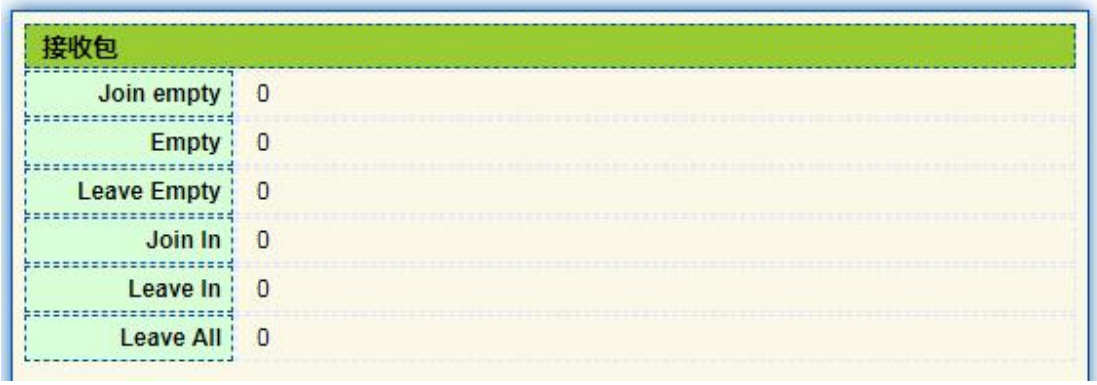


7.6.3 报文统计

查看 GVRP 端口报文统计

操作步骤:

1. 单击导航树中的“VLAN 功能 > GVRP > 报文统计”菜单进入界面，如下图所示:



8 MAC 地址表

以太网交换机的主要功能是在数据链路层对报文进行转发，也就是根据报文的目的 MAC 地址将报文输出到相应的端口。MAC 地址转发表是一张包含了 MAC 地址与转发端口对应关系的二层转发表，是以太网交换机实现二层报文快速转发的基础。

MAC 地址转发表的表项中包含如下信息：

- 目的 MAC 地址
- 端口所属的 VLAN ID
- 本设备上的转发出端口编号

以太网交换机在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：

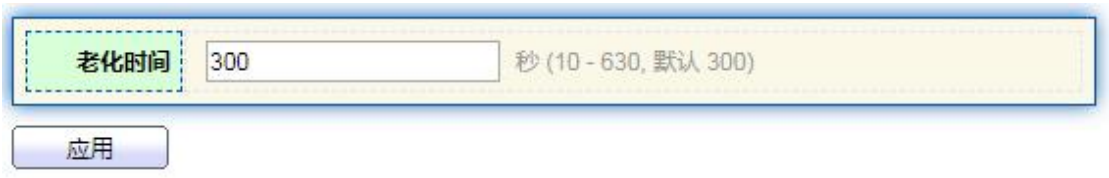
- 单播方式：当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文从该表项中的转发出端口发送。
- 广播方式：当交换机收到目的地址为全 F 的报文，或 MAC 地址转发表中没有包含对应报文目的 MAC 地址的表项时，交换机将采取广播方式将报文向除接收端口外的所有端口转发。

8.1 动态 MAC 地址表

在该页，可以设置 MAC 地址老化时间以及查看 MAC 地址表信息，为适应网络的变化，MAC 地址表需要不断更新。MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到刷新的表项将被删除，这个生存周期被称作老化时间。如果在到达生存周期前记录被刷新，则该表项的老化时间重新计算。设置合适的老化时间可以有效实现 MAC 地址的老化功能。用户设置的老化时间过短，可能导致交换机广播大量找不到目的 MAC 地址的数据报文，影响交换机的运行性能。如果用户设置的老化时间太长，交换机可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址转发表资源，导致交换机无法根据网络的变化更新 MAC 地址转发表。如果用户设置的老化时间太短，交换机可能会删除有效的 MAC 地址表项，降低转发效率。一般情况下，推荐使用老化时间的缺省值 300 秒。

设置 MAC 地址老化时间操作步骤：

1. 单击导航树中的“MAC 地址表 > 动态 MAC 地址表”菜单，进入动态 MAC 地址表配置和显示界面：



界面信息含义如下表

配置项	说明
MAC 老化时间	输入 MAC 的老化时间

说明:

MAC 表用于存放交换机所学习到的其它设备的 MAC 地址、VLAN 编号和出接口信息等。在转发数据时，根据以太网帧中的目的 MAC 地址和 VLAN 编号查询 MAC 表，快速定位设备的出接口。

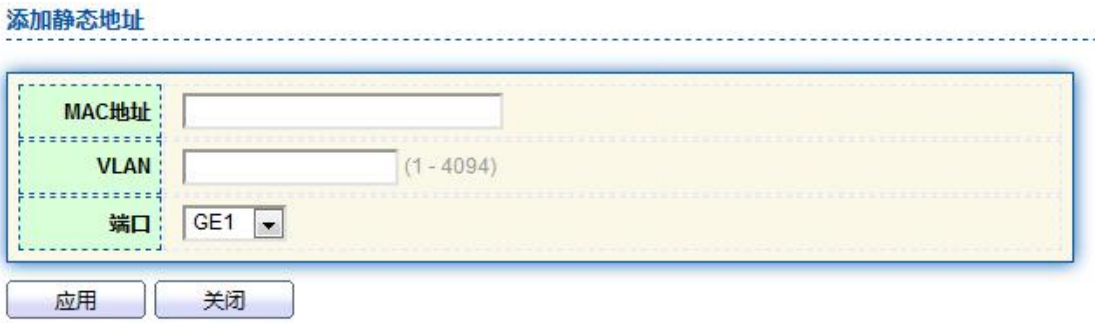
要检查系统 MAC 地址表，请参阅第 3 章第 3.3 节。

8.2 静态 MAC 地址表

静态表项由用户手工配置，并下发到各接口板，表项不老化。

新建静态 MAC 地址步骤:

1. 单击导航树中的“MAC 地址表 > 静态 MAC 地址表”菜单，进入静态 MAC 地址表界面，如下图所示。



界面信息含义如下表所示。

配置项	说明
MAC	必选。输入新建的 MAC 地址。如：HH:HH:HH:HH:HH:HH。
VLAN	必选。指定 VLAN 的 ID 号。
端口	必选。选择接口的类型输入接口的名称。 说明：接口必须是所配置 VLAN 的成员端口。

2. 填写相应的配置项。单击“应用”，完成配置。

8.3 MAC 地址过滤表

交换机按配置丢弃匹配的数据帧

操作步骤：

1. 单击导航树中的“MAC 地址表 > MAC 地址过滤表”菜单进入界面，如下图所示：

界面信息含义如下表所示。

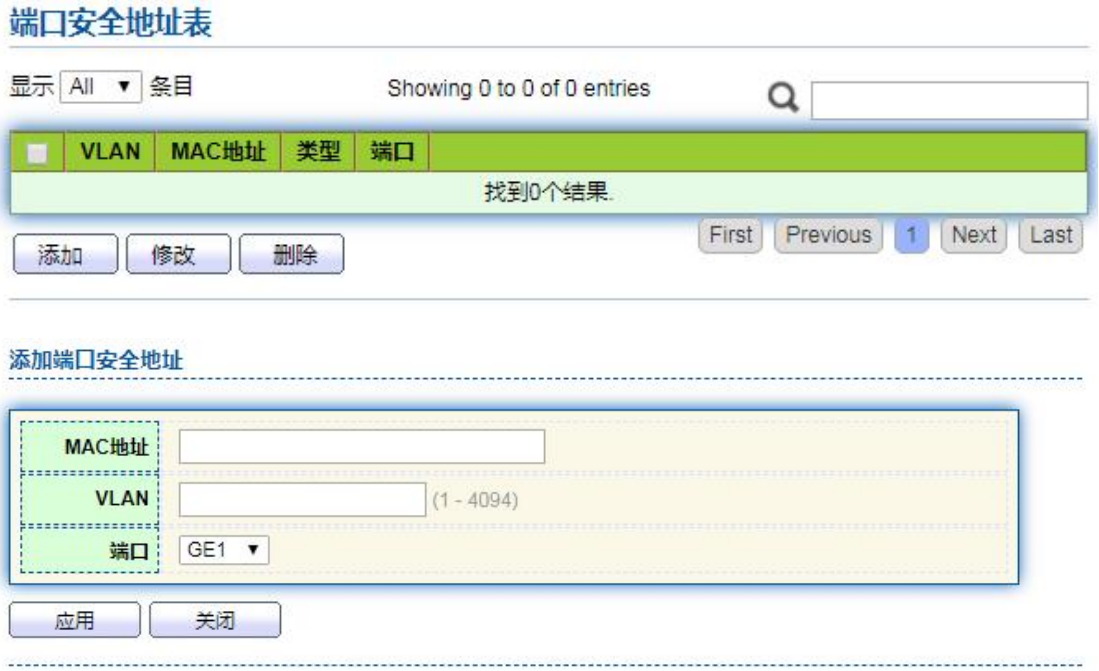
查询项	说明
MAC 地址	过滤的 MAC 地址
VLAN	MAC 地址所属的 VLAN ID

8.4 端口安全 MAC 地址表

如果 MAC 地址设置为安全 MAC，则该端口只允许安全 MAC 的数据帧永久通过，其他数据帧将被丢弃

操作步骤:

1. 单击导航树中的“MAC 地址表 > 端口安全 MAC 地址表”菜单进入界面，如下图所示:



界面信息含义如下表所示。

查询项	说明
MAC 地址	安全的 MAC 地址
VLAN	MAC 地址所属的 VLAN ID
端口	MAC 地址对应的接口 ID

9 生成树协议

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 IEEE 802.1D 中定义的 STP 到 IEEE 802.1W 中定义的快速生成树协议 RSTP（Rapid Spanning Tree Protocol），再到最新的 IEEE 802.1S 中定义的多生成树协议 MSTP（Multiple Spanning Tree Protocol）。

生成树协议中，MSTP 兼容 RSTP、STP，RSTP 兼容 STP。三种生成树协议的比较如表所示。

三种生成树协议的比较

生成树协议	特点	应用场景
STP	形成一棵无环路的树，解决广播风暴并实现冗余备份。 收敛速度较慢。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。
RSTP	形成一棵无环路的树，解决广播风暴并实现冗余备份。 收敛速度快。	
MSTP	形成一棵无环路的树，解决广播风暴并实现冗余备份。 收敛速度快。 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同的生成树转发流量，每棵生成树之间相互独立。

在以太网交换网中部署生成树协议后，如果网络中出现环路，生成树协议通过拓扑计算，可实现：

- 消除环路：通过阻塞冗余链路消除网络中可能存在的网络通信环路。
- 链路备份：当前活动的路径发生故障时，激活冗余备份链路，恢复网络连通性。

目录

9.1 功能设置

提供配置 STP 全局参数的功能，在一些特定的网络环境里，需要调整部分设备的 STP 参数，以便达到最佳的效果。

操作步骤：

1. 单击导航树中的“生成树协议 > 功能设置”菜单，进入生成树协议配置界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
开启	默认勾选，代表交换机启用 Spanning-tree
运行模式	支持三个生成树模式，即 STP、RSTP 和 MSTP。
路径花费模式	Long 模式和 Short 模式
BPDU 转发方式	表示设备收到 BPDU 报文后，处理完毕报文的行为方式
优先级	表示端口的优先级
Hello Time	Hello 报文的间隔时间
Max Age	Max Age 老化时间

Forward Delay	Forward Delay 时间
域名	MST 域名。缺省值为交换机设备主控板的 MAC 地址。 交换机设备的域名用来与 MST 域的 VLAN 映射表、MSTP 的修订级别共同确定该交换机设备可以属于哪个域。

2. 填写相应的配置项。单击“应用”，完成配置

9.2 端口设置

在一些特定的网络环境里，需要调整部分交换机设备接口的 STP 参数，以便达到最佳的效果。

1. 单击导航树中的“生成树协议 > 端口设置”菜单，进入端口配置界面，选中需要配置的端口后点击修改，进入详细修改界面，如下图所示：

端口配置表

编号	端口	状态	路径花费	优先级	BPDU Filter	BPDU Guard	边缘端口状态	点对点状态	端口角色	端口状态	指定桥ID	指定端口ID	端口花费
1	GE1	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
2	GE2	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
3	GE3	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
4	GE4	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
5	GE5	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	启用	20000	128	禁用	禁用	禁用	启用	Disabled	Forwarding	0-00:00:00:00:00:00	128-7	20000
8	GE8	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
9	GE9	启用	20000	128	禁用	禁用	禁用	禁用	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000

界面信息含义如下表所示。

配置项	说明
端口	需要配置属性的端口号
状态	是否开启生成树协议功能
边缘端口	边缘端口应直接连接到用户终端，而不是另一个交换机或网段。边缘端口可以快速过渡到转发状态，因为在边缘端口上，网络拓扑结构的变化不产生环路。通过设置一个端口成边缘端口时，生成树协议允许它迅速过渡到转发状态。建议把直接连接到用户终端的以太网端口配置成边缘端口，使它们可以快速过渡到转发状态。
BPDU Filter	是否开启 BPDU 过滤功能。
BPDU Guard	是否开启 BPDU 的保护功能。默认是不勾选。当设备上启动 BPDU 保护功能，如果接口收到了 BPDU，设备将这些接口关闭，同时通知网管系统。被关闭的接口只能由网络管理人员手动恢复。

Point-to-Point	选择开启、关闭和自动。 自动：表示端口设置为缺省的自动检测是否与点对点链路相连的状态。 开启：表示特定端口与点对点链路相连。 关闭：表示特定端口没有与点对点链路相连。

2. 填写相应的配置项。单击“应用”，完成配置。

9.3 实例设置

通过 MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个多生成树实例 MSTI（Multiple Spanning Tree Instance），每个域叫做一个 MST 域（MST Region：Multiple Spanning Tree Region）。

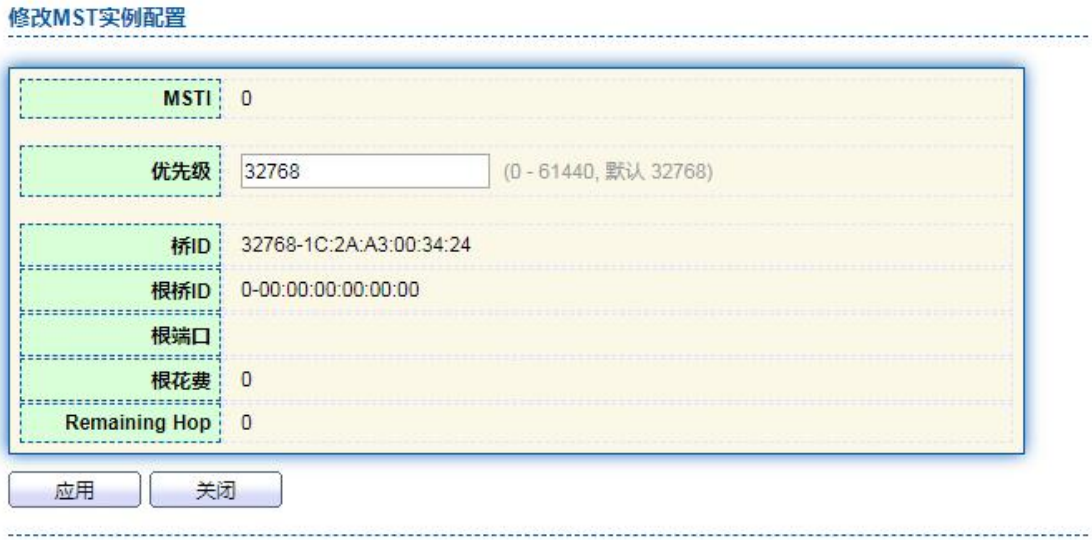
说明：

所谓实例就是多个 VLAN 的一个集合。通过将多个 VLAN 捆绑到一个实例，可以节省通信开销和资源占用率。MSTP 各个实例拓扑的计算相互独立，在这些实例上可以实现负载均衡。可以把多个相同拓扑结构的 VLAN 映射到一个实例里，这些 VLAN 在端口上的转发状态取决于端口在对应 MSTP 实例的状态。

简单地说，就是一个或多个 VLAN 到指定 MST 实例的映射。一次可分配一个或多个 VLAN 给一个生成树实例。

操作步骤：

1. 单击导航树中的“生成树协议 > 实例设置”菜单，进入实例配置页面，选择需要配置的多生成树实例，点击修改，进入修改界面，界面如下图所示。



界面含义如下表所示

配置项	说明
MSTI	多生成树实例号，0~15。
VLAN	实例映射的 VLAN 号
优先级	设置指定实例的优先级，必须是 4096 的倍数。它的范围是 0 到 65535，缺省值是 32768。
桥 ID	本设备对应的生成树实例桥 ID，由优先级+MAC 地址组成
根桥 ID	选举出的实例根桥 ID，由优先级+MAC 地址组成
根端口	选举出的实例根端口号
根花费	距离根桥的路径花费

2. 填写相应的配置项。单击“应用”，完成配置。

9.4 实例端口设置

1. 单击导航树中的“生成树协议 > 实例端口设置”菜单，进入多生成树实例端口配置界面，界面中列出了设备包含的所有端口，选择需要修改的端口，点击修改按钮，进入实例端口详细配置界面，如下图所示：

界面信息含义如下表所示。

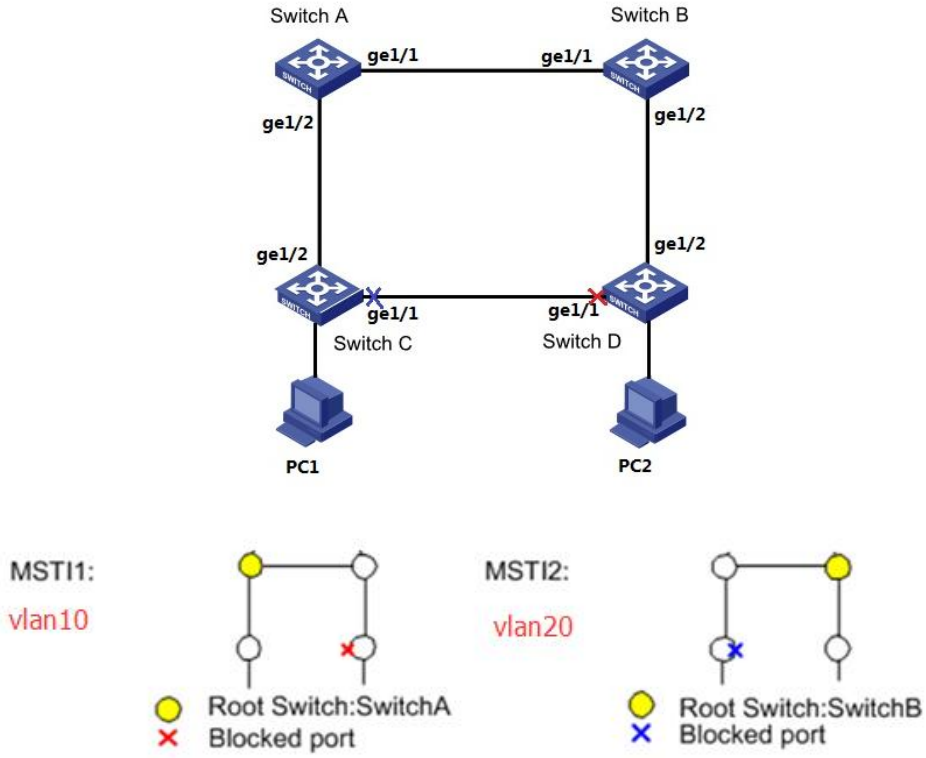
配置项	说明
MSTI	通过左上角下拉框选择需要配置的实例
端口	用户选择需要配置的端口
路径花费	输入接口的路径开销值。使用 IEEE 802.1t 标准方法时取值范围是 0 ~ 200000000
优先级	选择端口的优先级。数值越小表示优先级越高。 接口优先级可以影响接口在指定 MSTI 上的角色。用户可以在不同 MSTI 上对同一接口配置不同的优先级，从而使不同 VLAN 的流量沿不同的物理链路

	转发，完成按 VLAN 负载分担的功能。 说明：接口优先级的改变时，MSTP 会重新计算接口的角色并进行状态迁移。
端口角色	分为三类根端口，指定端口，备份端口，Disabled
端口状态	包括三种状态，Discarding，Forwarding，Disabled
模式	当前生成树协议模式
类型	端口在实例内的类型，包含边界端口和内部端口

2. 填写相应的配置项。单击“应用”，完成配置。

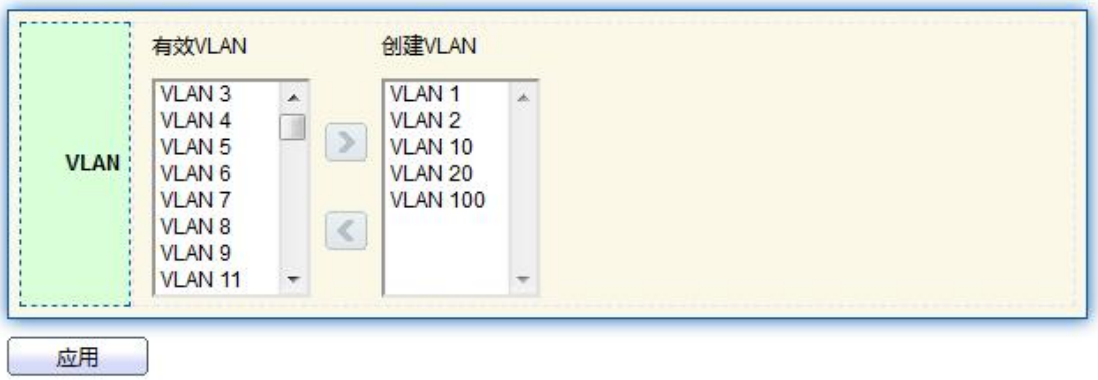
配置 MSTP 功能示例：

SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 MSTP。为实现 VLAN10 和 VLAN20 的流量负载分担，MSTP 引入了多实例。MSTP 可设置 VLAN 映射表，把 VLAN 和生成树实例相关联，实例 1 映射 VLAN10，实例 2 映射 VLAN20。

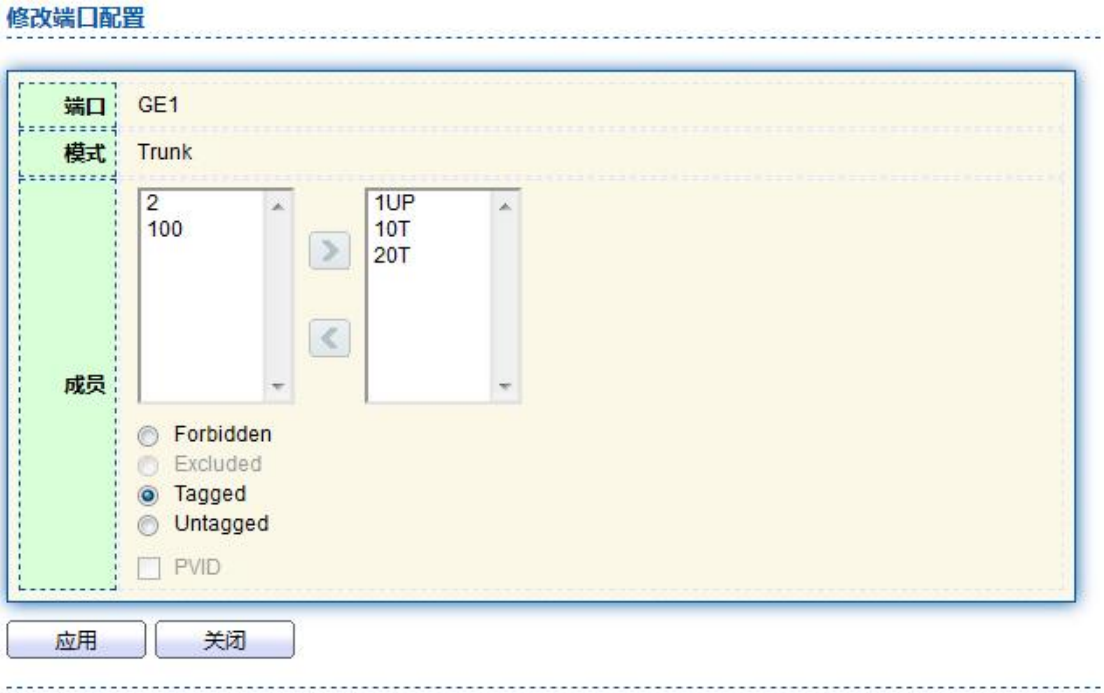


操作步骤：

1. 配置处于环网中的设备的二层转发功能，在交换设备 SwitchA、SwitchB、SwitchC 和 SwitchD 上创建 VLAN10，vlan20。单击导航树中的“VLAN 功能 > VLAN 配置>创建 VLAN”菜单，进入“创建 VLAN”界面，填写相应配置，单击“应用”，完成配置，如下图所示。



2. 将交换设备上接入环路中的端口加入 VLAN。单击导航树中的“VLAN 功能 > VLAN 配置 > 成员配置”菜单，进入“成员配置”界面，选择环端口，进入端口设置模式，分别将 VLAN10,VLAN20 移到右选框，属性为“Tagged”,单击“应用”，完成配置：



3. 单击导航树中的“生成树协议 > 功能设置”菜单，进入“功能设置”，填写相应配置，选择 MSTP 模式，界面如下图所示。

4. 配置实例 MSTI1 和实例 MSTI2 的 VLAN 映射关系。单击导航树中的“生成树协议 >实例设置”菜单，进入“实例设置”，，填写相应参数，单击“添加”，界面如下图所示。

注意：

- 配置 SwitchA 时将 MSTI1 的优先级改为 0，MSTI2 的优先级改为 4096。
- 配置 SwitchB 时将 MSTI1 的优先级改为 4096，MSTI2 的优先级改为 0。配置方法与 SwitchA 一致，不在赘述。
- 优先级必须是 4096 的倍数

5. 在域，配置 MSTI1 与 MSTI2 的根桥与备份根桥，配置 SwitchB 为 MSTI2 的根桥，配置 SwitchB 为 MSTI1 的备份根桥。操作步骤与 5 一样，不再赘述。
6. 经过以上配置，将网络修剪成树状，达到消除环路的目的。

9.5 报文统计

操作步骤:

1. 单击导航树中的“生成树协议 > 报文统计”菜单进入界面，如下图所示:

10 ERPS

ERPS（Ethernet Ring Protection Switching，以太环网保护倒换）是具备高可靠性和稳定性的以太环网链路层技术。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环发生链路故障时能迅速恢复环网上各个节点之间的通信通路，具备较高的收敛速度。

它以 ERPS 环为基本单位，包含若干个节点，通过阻塞 RPL Owner 端口，并控制其他普通端口，使得端口的状态在 Forwarding 和 Blocking 之间切换，达到消除环路的目的。同时利用控制 VLAN、数据 VLAN 和 MST 保护实例等机制，以更好地实现 ERPS 的功能。

10.1 功能配置

配置和查看全局 ERPS 功能的开启和关闭

1. 单击导航栏中“ERPS > 功能配置”菜单，进入功能配置界面

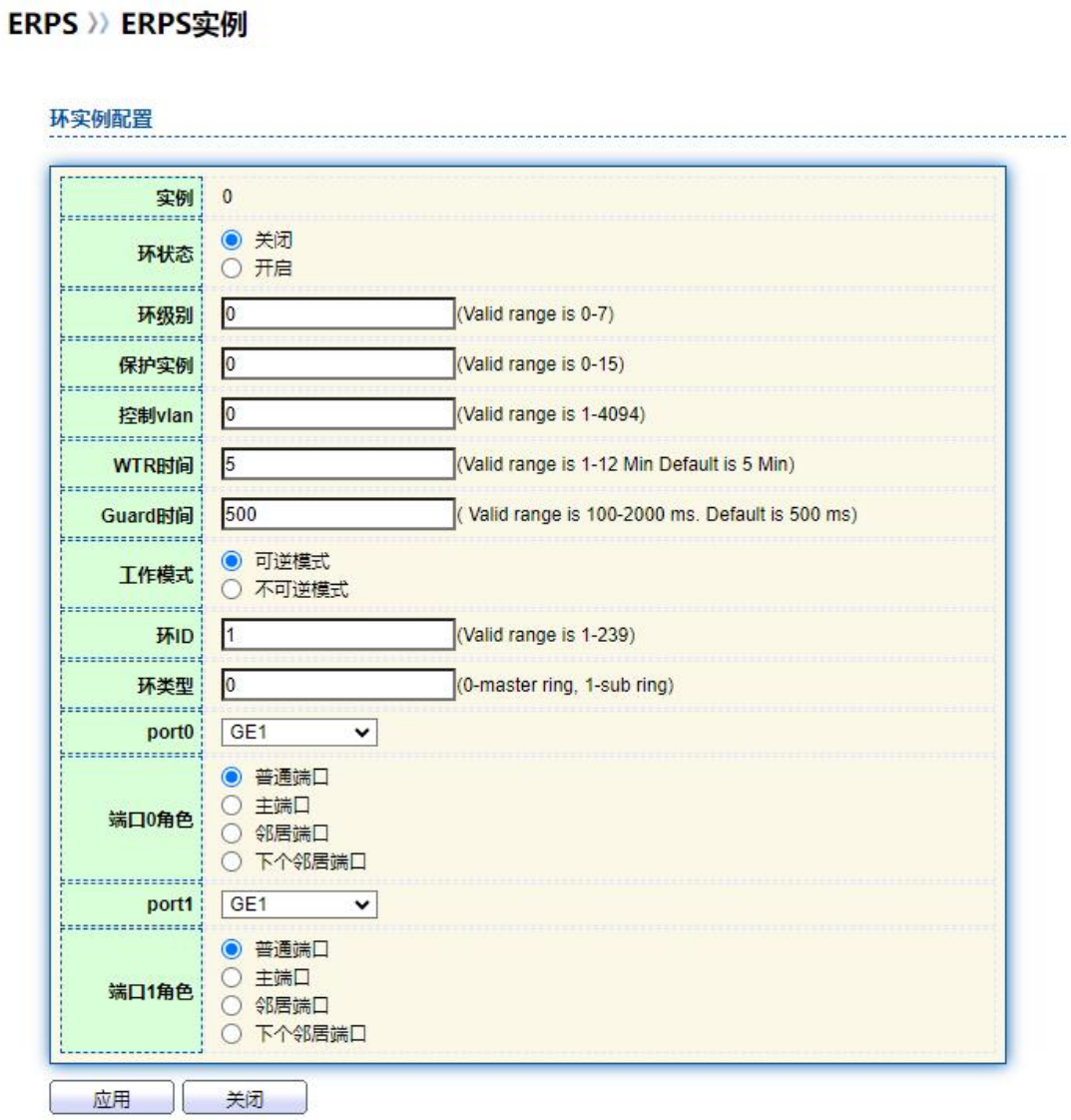
如下图所示:

10.2 ERPS 实例

ERPS 组网中一个环可以支持多个实例，每个实例都是一个逻辑环。每个实例中有自己的协议通道和数据通道，以及 Owner 节点；每个实例作为一个独立的协议实体，维护各自的状态和数据。

1. 单击导航栏中“ERPS > ERPS 实例”菜单，可以进入 ERPS 实例创建界面，点击应用创建实例，如下图所示：

2. 选中实例单击修改按钮，进入实例配置界面，如下图所示：



界面含义如下表

配置项	说明
环状态	开启/关闭
环级别	消息级别选择 0-7
保护实例	传递 ERPS 协议报文和数据报文的 VLAN 必须映射到保护实例中，这样 ERPS 协议才会按照其阻塞原则对这些报文进行转发或阻塞。否则，VLAN 报文可能会在成环的网络中产生广播风暴导致网络不可用。
控制 VLAN	控制 VLAN 用来传递 ERPS 协议报文
WTR 时间	在可逆模式下，RPL Owner 端口由于其他链路故障而被放开，当故障恢复时，等待 WTR 定时器超时后，重新阻塞 RPL Owner 端口
Guard 时间	在端口检测到链路恢复时启动 Guard 定时器，用于防止环网上转发延时导致的原 R-APS 消息残留对网络造成不必要的震荡
工作模式	当 ERPS 链路恢复正常后，可以通过设置 ERPS 的可逆模式/不可逆模式来决定是否重新阻塞 RPL owner 端口。

环 ID	ERPS 环编号
环类型	0 为主环，1 为子环
Port0	ERPS 环成员端口，用于 ERPS 环上协议报文和数据报文的传输
Port1	ERPS 环成员端口，用于 ERPS 环上协议报文和数据报文的传输
端口角色	普通端口；负责接收和转发链路中的协议报文和数据报文。 主端口；负责阻塞和放开本节点上位于 RPL 上的端口，防止形成环路，从而进行链路倒换 邻居端口；RPL 上和主端口相连的端口，协同主端口阻塞和放开本节点上位于 RPL 上的端口，进行链路倒换 下一邻居端口；

注意：

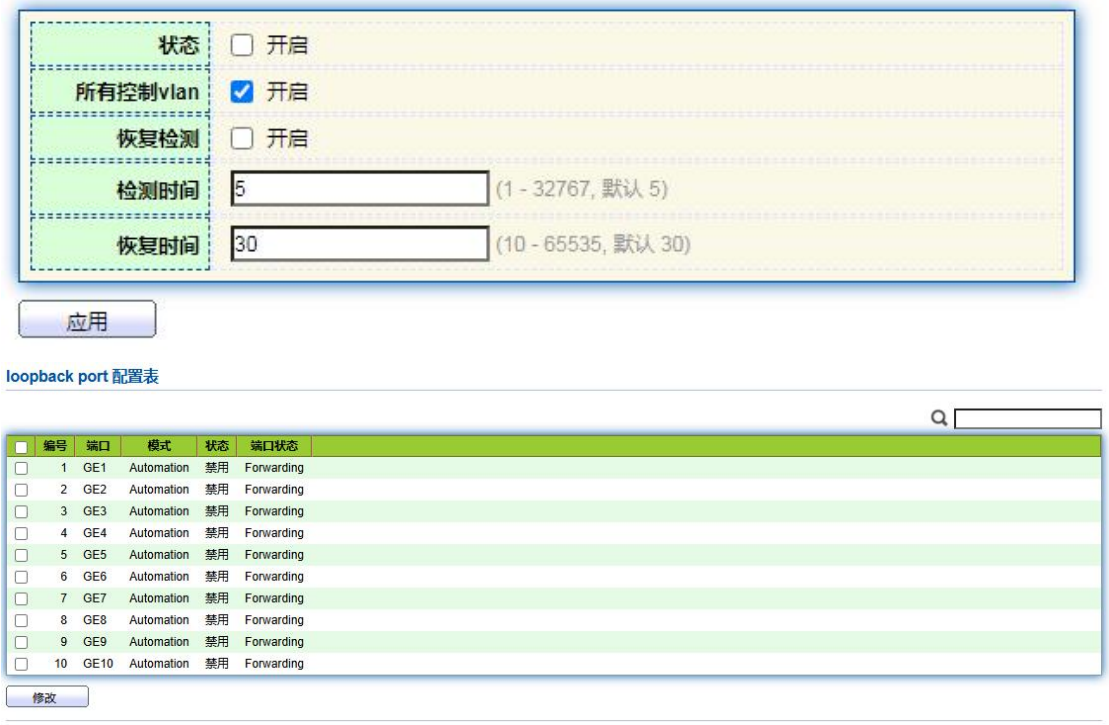
- ERPS 功能仅光口满足小于 20ms 切换/恢复延时

11 环路检测

环路检测(Loopback Detection)功能设置配置如下：对交换机端口进行全局和端口环网开启、关闭配置，用户可以更改

环网检测时间间隔，以及环网端口自动恢复时间周期。通过全局和端口使能，系统可以检测网络中的环路情况，从而减少环路风暴产生。支持自动检测和手动检测两种工作模式。

1. 单击导航栏中“环路检测 > 环路检测配置”，如下图所示。



界面含义如下表

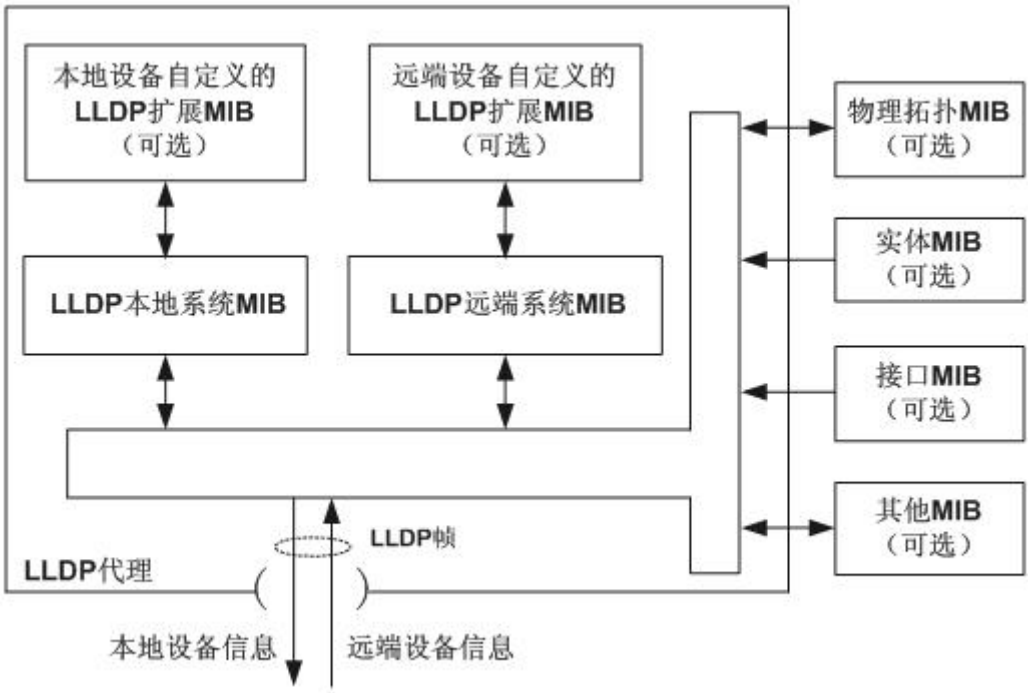
配置项	说明
状态	环路检测全局开关，开启/禁用
所有控制 VLAN	端口所有 VLAN，默认为开启
恢复检测	环路恢复检测
检测时间	环路检测周期，默认为 5 秒
恢复时间	环路自动检测恢复时间的周期，默认为 30 秒
端口	端口列表
模式	环路检测工作模式，自动和手动，默认为自动
状态	端口级环路检测开关
端口状态	端口的状态

12 拓扑发现

LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的链路层发现协议。LLDP 是一种标准的二层发现方式，可以将本端设备的管理地址、设备标识、接口标识等信息组织起来，并发布给自己的邻居设备，邻居设备收到这些信息后将其以标准的管理信息库 MIB（Management Information Base）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。

LLDP 可以将本地设备的信息组织起来并发布给自己的远端设备，本地设备将收到的远端设备信息以标准 MIB 的形式保存起来。工作原理如下图所示。

LLDP 原理框图



LLDP 基本实现原理为：

- LLDP 模块通过 LLDP 代理与设备上物理拓扑 MIB、实体 MIB、接口 MIB 以及其他类型 MIB 的交互，来更新自己的 LLDP 本地系统 MIB，以及本地设备自定义的 LLDP 扩展 MIB。
- 将本地设备信息封装成 LLDP 帧发送给远端设备。
- 接收远端设备发过来的 LLDP 帧，更新自己的 LLDP 远端系统 MIB，以及远端设备自定义的 LLDP 扩展 MIB。
- 通过 LLDP 代理收发 LLDP 帧，设备就很清楚地知道远端设备的信息，包括连接的是远端设备的哪个接口、远端设备的 MAC 地址等信息。
- LLDP 本地系统 MIB 用来保存本地设备信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、网络管理地址等信息。
- LLDP 远端系统 MIB 用来保存远端设备信息。包括设备 ID、接口 ID、系统名称、系统描述、接口描述、网络管理地址等信息。
- LLDP-MED 以 LLDP 为基础，其它组织可以通过 LLDP-MED 对其进行扩展。从网络设备查明的信息，可以帮助进行故障分析 并允许管理系统准确地了解网络拓扑结构。

12.1 LLDP 功能配置

操作步骤：

1. 单击导航树中的“拓扑发现> LLDP > 功能配置”菜单，进入“功能配置”界面，如下图所示。

界面含义如下表

配置项	说明
状态	开启或关闭 LLDP 协议
LLDP 报文处理方式	关闭 LLDP 协议时，LLDP 报文处理方式分“Filtering”（过滤），“Bridging”(转发),“Flooding”(泛洪)3 种
发送周期	默认 30 秒，范围：5-32768 秒
Hold Multiplier	发送周期乘积，默认 4，范围：2-10，发送周期*发送周期乘积不大于 65535
重新初始化延迟	默认 2 秒，范围：1-10 秒
传送延迟	默认 2 秒，范围：1-8191 秒
快速启动重复计数	LLDP-MED 端口快速启动重复次数 默认 3，范围：1-10

说明:

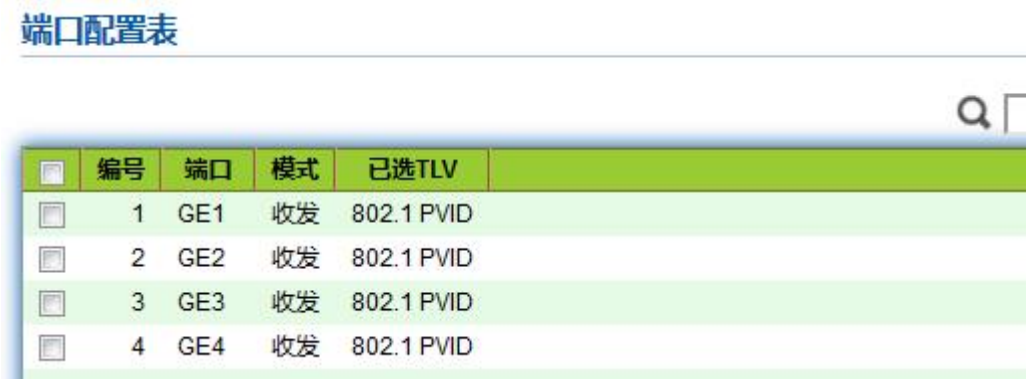
封装有 LLDP 数据单元 LLDPDU（LLDP Data Unit）的以太网报文称为 LLDP 报文。TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。

2. 填写相应的配置项。单击“应用”，完成配置。

12.2 端口配置

操作步骤

1. 单击导航树中的“拓扑发现> LLDP > 端口配置”菜单，进入“端口配置”界面，如下图所示。



界面含义如下表

配置项	说明
端口	支持配置多个端口
收发模式	收发 LLDP 报文模式
已选 TLV	已选 TLV 信息，VLAN 信息

说明:

LLDP 有以下四种工作模式。Transmit(只发)：只发 LLDP 报文， Receive (只收)：只收 LLDP 报文，Normal(收发)：既发送也接收 LLDP 报文。Disable(关闭)：既不发送也不接收 LLDP 报文。

2. 选择相应端口点击“修改”进入修改端口设置页。单击“应用”完成配置，如下图所示。

界面含义如下表

配置项	说明
端口	支持配置多个端口
收发模式	收发 LLDP 报文模式, Transmit(只发)：只发 LLDP 报文，Receive (只收)：只收 LLDP 报文，Normal(收发)：既发送也接收 LLDP 报文。Disable(关闭)：既不发送也不接收 LLDP 报文
可选 TLV	选择 TLV 信息，VLAN 信息
802.1 VLAN name	选择 VLAN name 信息

12.3 MED 网络策略配置

MED 是基于 IEEE802.1ab 的邻居发现协议，LLDP 是 IEEE 的邻居发现协议，可以被其他组织扩展。从网络设备（如交换机和无线接入点）识别的信息可以帮助进行故障分析，并允许管理系统准确地了解网络拓扑结构。

操作步骤：

1. 单击导航树中的“拓扑发现 > LLDP > MED 网络策略配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
策略 ID	MED 策略 ID
应用类型	配置和发布网络策略 TLV
VLAN	相应的 VLAN ID
VLAN 标签	VLAN 标签的方式
优先级	VLAN 的 COS 值
DSCP	IP 包的 DSCP 值

12.4 MED 端口配置

操作步骤:

1. 单击导航树中的“拓扑发现 > LLDP > MED 端口配置”菜单进入界面，如下图所示:

界面信息含义如下表所示。

查询项	说明
端口	选择的端口列表
状态	端口使能状态
可选 TLV	用于发布的 TLV
Network policy	已配置的策略

坐标位置	配置和发布的本地 TLV 的坐标位置
位置信息	配置和发布的本地 TLV 的位置信息
紧急电话	配置和发布的本地 TLV 的紧急电话

12.5 报文预览

操作步骤:

1. 单击导航树中的“拓扑发现 > LLDP > 报文预览”菜单进入界面，如下图所示:

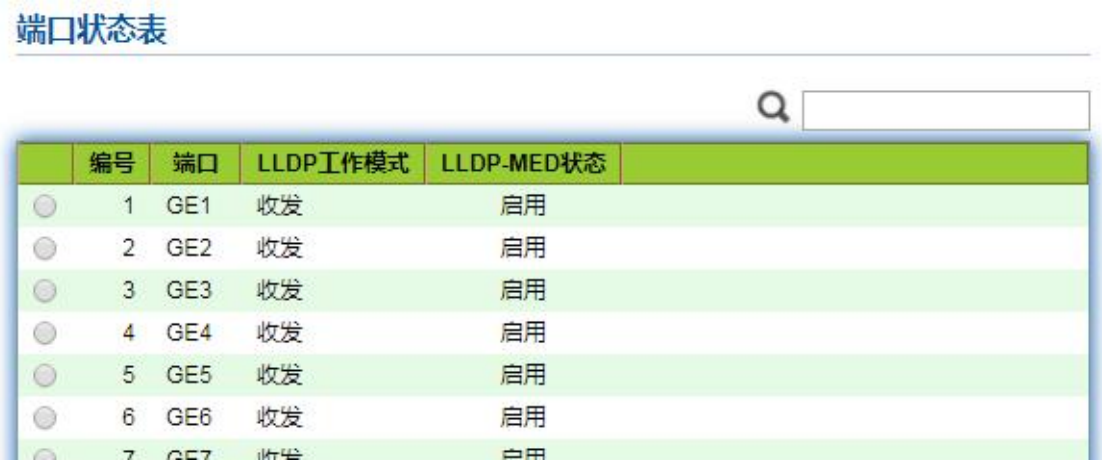
12.6 本设备信息

操作步骤:

1. 单击导航树中的“拓扑发现 > LLDP > 本设备信息”菜单进入界面，如下图所示:

2. 在端口状态表中选择端口，点击“详情”，可以查看端口发送的 LLDP 消息详细信息，如下

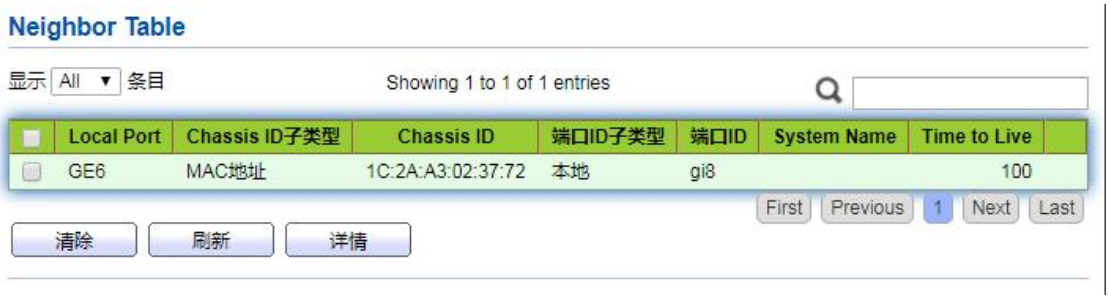
图所示：



12.7 邻居信息

LLDP 邻居显示操作步骤

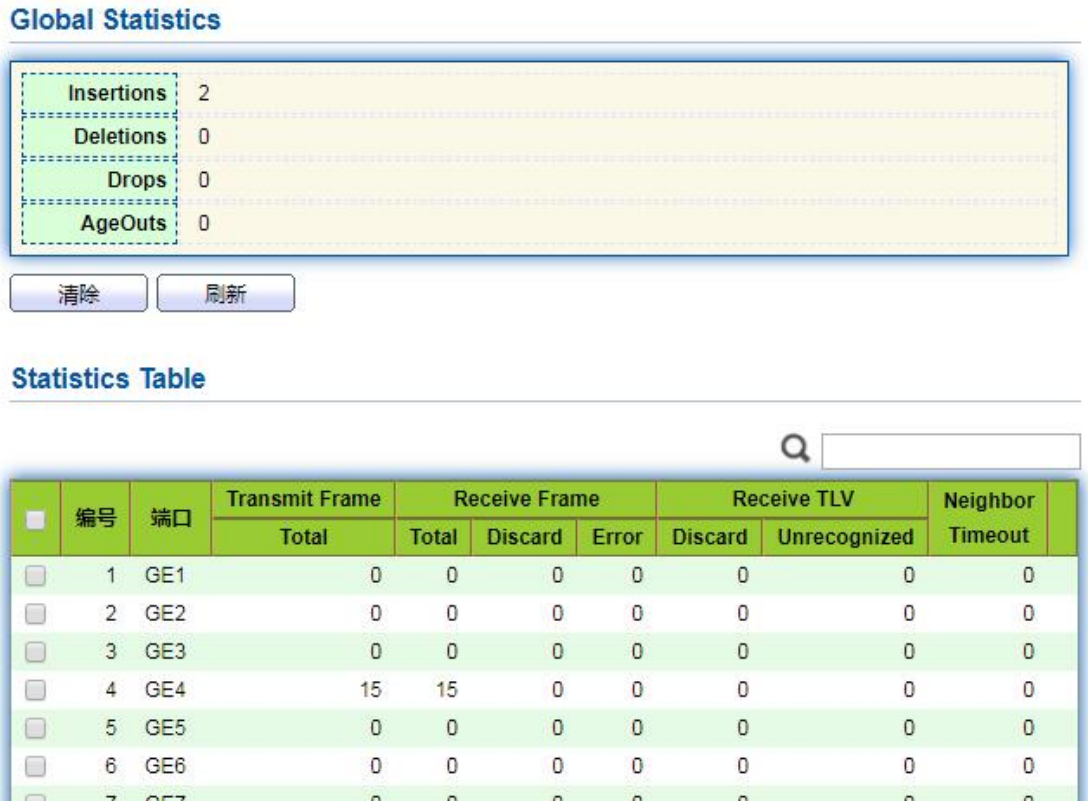
1. 单击导航树中的“拓扑发现> LLDP > 邻居信息”菜单，进入“LLDP 邻居”界面，如下图所示。



12.8 报文统计

操作步骤：

1. 单击导航树中的“拓扑发现 > LLDP > 报文统计”菜单进入界面，如下图所示：



13. DHCP

DHCP 简介

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）就是为满足这些需求而发展起来的。DHCP 协议采用客户端/服务器（Client/Server）方式工作，DHCP Client 向 DHCP Server 动态地请求配置信息，DHCP Server 根据策略返回相应的配置信息。

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如图 1-1 所示。

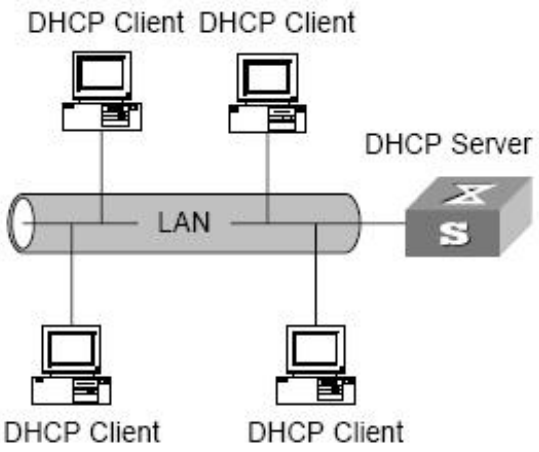


图 1-1. DHCP 典型应用

DHCP 的 IP 地址分配

IP 地址分配策略

针对客户端的不同需求，DHCP 提供三种 IP 地址分配策略：

- 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定固定的 IP 地址。通过 DHCP 将配置的固定 IP 地址发给客户端。
- 自动分配地址：DHCP 为客户端分配租期为无限长的 IP 地址。
- 动态分配地址：DHCP 为客户端分配有有效期限的 IP 地址，当使用期限到期后，客户端需要重新申请地址。绝大多数客户端得到的都是这种动态分配的地址。

IP 地址动态获取过程

DHCP Client 与 DHCP Server 间的报文交互过程如图 1-2 所示。

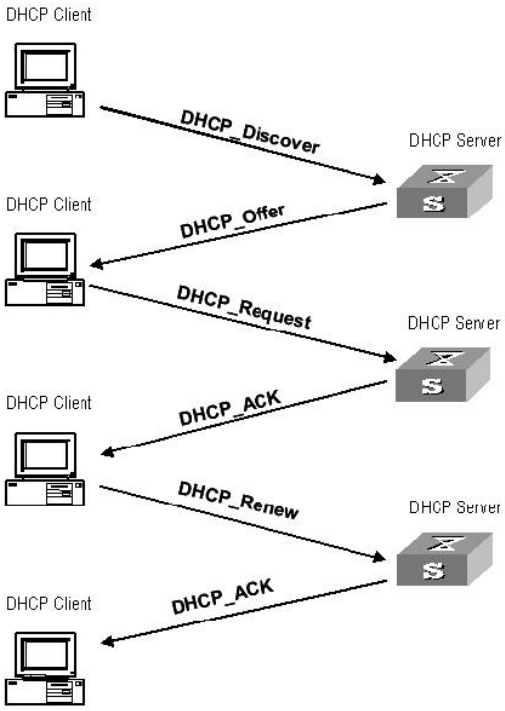


图 1-2. DHCP Client 与 DHCP Server 间的报文交互过程

DHCP 客户端为了获取合法的动态 IP 地址，在不同阶段与服务器之间交互不同的信息，通常存在以下三种模式：

(1) DHCP 客户端首次登录网络

DHCP 客户端首次登录网络时，主要通过四个阶段与 DHCP 服务器建立联系。

- 发现阶段：即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCP-Discover 报文，只有 DHCP 服务器才会进行响应。
- 提供阶段：即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCP-Discover 报文后，从 IP 地址池中挑选一个尚未分配的 IP 地址分配给客户端，向该客户端发送包含出租 IP 地址和其它设置的 DHCP-Offer 报文。
- 选择阶段：即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCP-Offer 报文，客户端只接受第一个收到的 DHCP-Offer 报文，然后以广播方式向各 DHCP 服务器回应 DHCP-Request 报文，该信息中包含向所选定的 DHCP 服务器请求 IP 地址的内容。
- 确认阶段：即 DHCP 服务器确认所提供 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户端回答的 DHCP-Request 报文后，便向客户端发送包含它所提供的 IP 地址和其它设置的 DHCP-ACK 确认报文；否则将返回 DHCP-NAK 报文，表明地址不能分配给该客户端。客户端收到服务器返回的 DHCP-ACK 确认报文后，会以广播的方式发送 ARP（目的地址是被分配到的地址）进行地址探测，如果在规定的时间内没有收到回应，客户端才使用此地址。
- 除 DHCP 客户端选中的服务器外，其它 DHCP 服务器本次未分配出的 IP 地址仍可用于其他客户端的 IP 地址申请。

(2) DHCP 客户端再次登录网络

当 DHCP 客户端再次登录网络时，主要通过以下几个步骤与 DHCP 服务器建立联系。

- DHCP 客户端首次正确登录网络后，以后再登录网络时，只需要广播包含上次分配 IP 地址的 DHCP-Request 报文即可，不需要再次发送 DHCP-Discover 报文。
- DHCP 服务器收到 DHCP-Request 报文后，如果客户端申请的地址没有被分配，则返回 DHCP-ACK 确认报文，通知该 DHCP 客户端继续使用原来的 IP 地址。
- 如果此 IP 地址无法再分配给该 DHCP 客户端使用（例如已分配给其它客户端），DHCP 服务器将返回 DHCP-NAK 报文。客户端收到后，重新发送 DHCP-Discover 报文请求新的 IP 地址。

(3) DHCP 客户端延长 IP 地址的租用有效期

DHCP 服务器分配给客户端的动态 IP 地址通常有一定的租借期限，期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要更新 IP 租约。

在实际使用中，DHCP 客户端缺省在 IP 地址租约期限达到一半时，向 DHCP 服务器发送 DHCP-Request 报文，以完成 IP 租约的更新。如果此 IP 地址有效，则 DHCP 服务器回应 DHCP-ACK 报文，通知 DHCP 客户端已经获得新的租约。

13.1 功能配置

DHCP 服务器全局配置

操作步骤：

1. 单击导航树中的“DHCP > 功能配置”菜单进入界面，如下图所示：

2. 在 DHCP Port 配置表中选择端口列表，点击“修改”进入端口配置界面，如下图所示：

注意：

- 使用 DHCP 服务器或 DHCP Relay 功能，端口都需要设置为使能状态

13.2 地址池配置

DHCP 服务器 IP 地址池配置

操作步骤：

1. 单击导航树中的“DHCP > 地址池配置”菜单进入界面，如下图所示：

注意：

- 起始地址和结束地址不能配置或包含网关地址

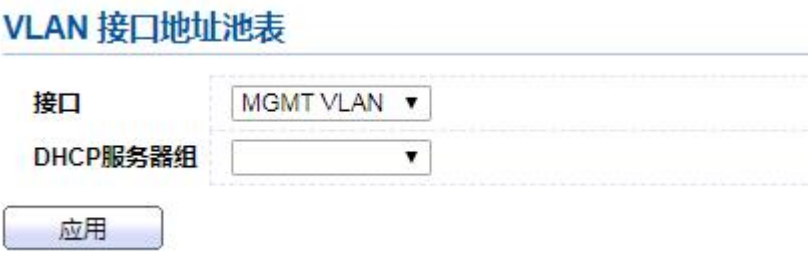
13.3 VLAN 接口地址组配置

DHCP 服务器组和接口关系配置

操作步骤：

1. 单击导航树中的“DHCP > VLAN 接口地址组配置”菜单进入 DHCP 服务器组表界面，单击“添加”进入服务器组配置，如下图所示：

2. 在 VLAN 接口地址池表中选择 VLAN 接口和 DHCP 服务器组，点击“应用”完成绑定关系，如下图所示：



13.4 客户端列表

查看客户端信息

操作步骤：

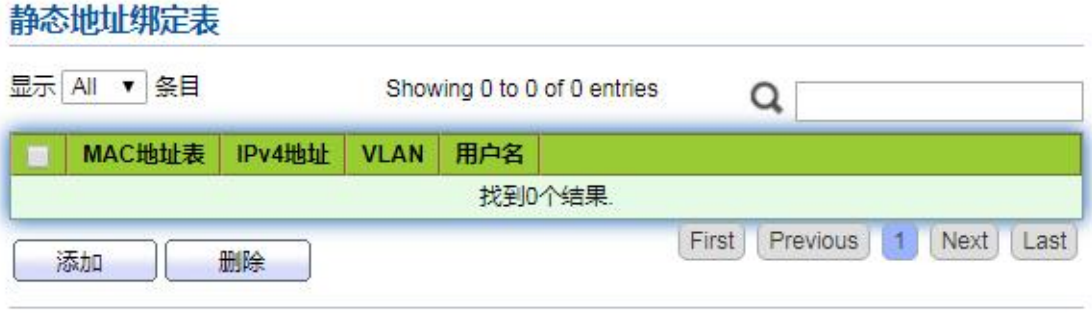
1. 单击导航树中的“DHCP > 客户端列表”菜单进入界面，如下图所示：

13.5 客户端静态绑定表

查看和配置客户端静态绑定表项

操作步骤：

1. 单击导航树中的“DHCP > 客户端静态绑定表”菜单进入界面，如下图所示：



注意:

- 静态绑定的 IP 配置要求在 IP 地址分配范围内

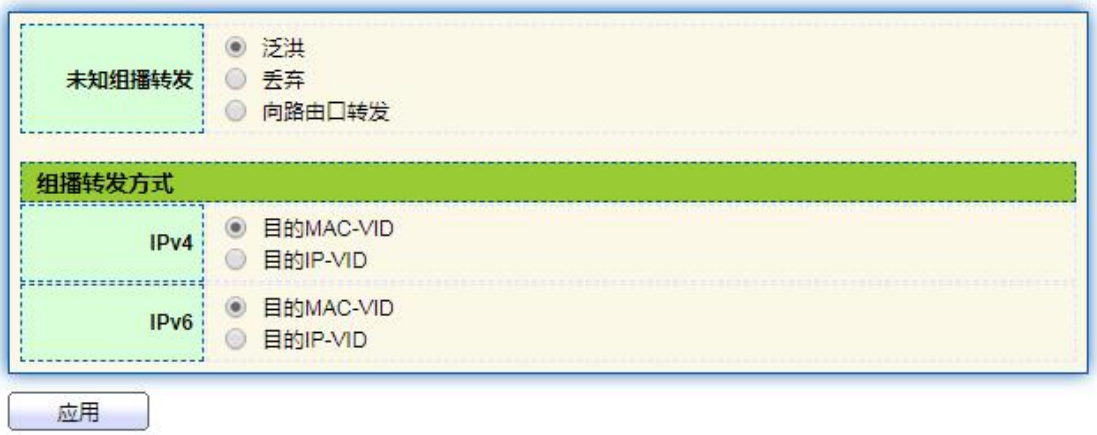
14 组播

14.1 基本功能

14.1.1 功能配置

操作步骤:

1. 单击导航树中的"组播 > 基本功能 > 功能配置"菜单进入界面，如下图所示:

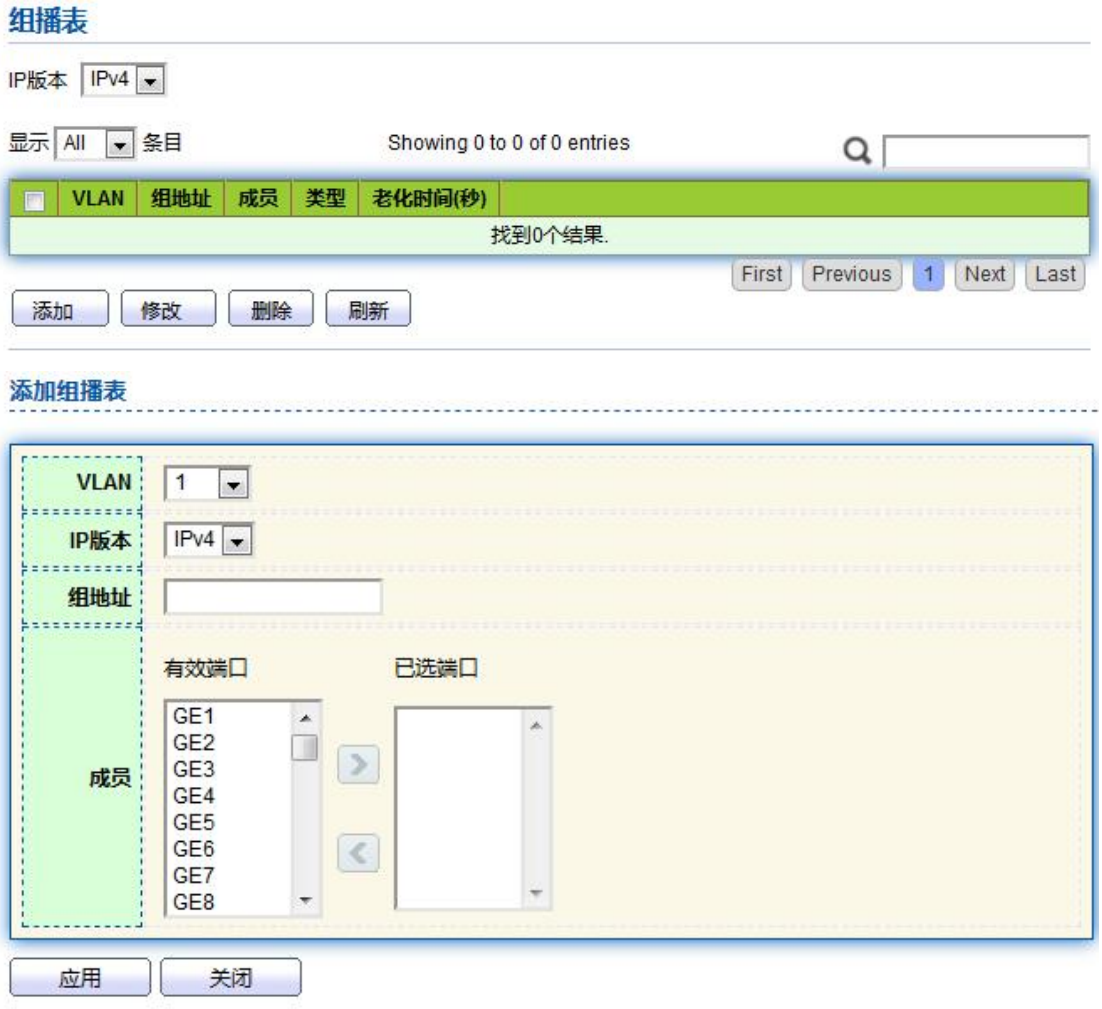


14.1.2 静态组播配置

根据以往的组播请求方式，当不同 VLAN 中的用户请求同一个组播组时，组播路由器会将数据复制转发到每个包含接收者的 VLAN 中，浪费了大量的带宽。IGMP 侦听通过将交换机端口的不同用户连接到同一个多播 VLAN 以接收多播数据来配置多播 VLAN。这样，组播流量只能在组播 VLAN 内传输，从而节省了带宽。此外，由于组播 VLAN 与用户 VLAN 完全隔离，因此安全性和带宽得到了保证。

操作步骤

1. 单击导航树中的"组播 > 基本功能 > 静态组播配置"菜单，进入静态组播配置界面，点击添加按钮新增静态组播项，点击修改按钮修改已经存在的静态组播项，界面如下图所示：



界面信息含义如下表所示。

配置项	说明
VLAN	组播组所属的 VLAN ID，下拉选择已经存在的 VLAN
IP 版本	组播 IP 地址的版本是 v4 还是 v6
组播地址	输入组播地址

成员	加入组播成员，可以多选

2. 填写相应的配置项，单击“应用”，完成配置。

14.1.3 路由端口配置

配置和查看组播路由端口信息

操作步骤：

1. 单击导航树中的“组播 > 基本功能 > 路由端口配置”菜单进入界面，如下图所示：

14.1.4 转发端口配置

配置和查看组播转发端口信息

操作步骤：

1. 单击导航树中的“组播 > 基本功能 > 转发端口配置”菜单进入界面，如下图所示：

14.1.5 端口限制

配置和查看端口组播组限制

操作步骤:

1. 单击导航树中的"组播 > 基本功能 > 端口限制"菜单进入界面，如下图所示:

14.1.6 过滤规则配置

配置和查看组播过滤模板

操作步骤:

1. 单击导航树中的"组播 > 基本功能 > 过滤规则配置"菜单进入界面，如下图所示:

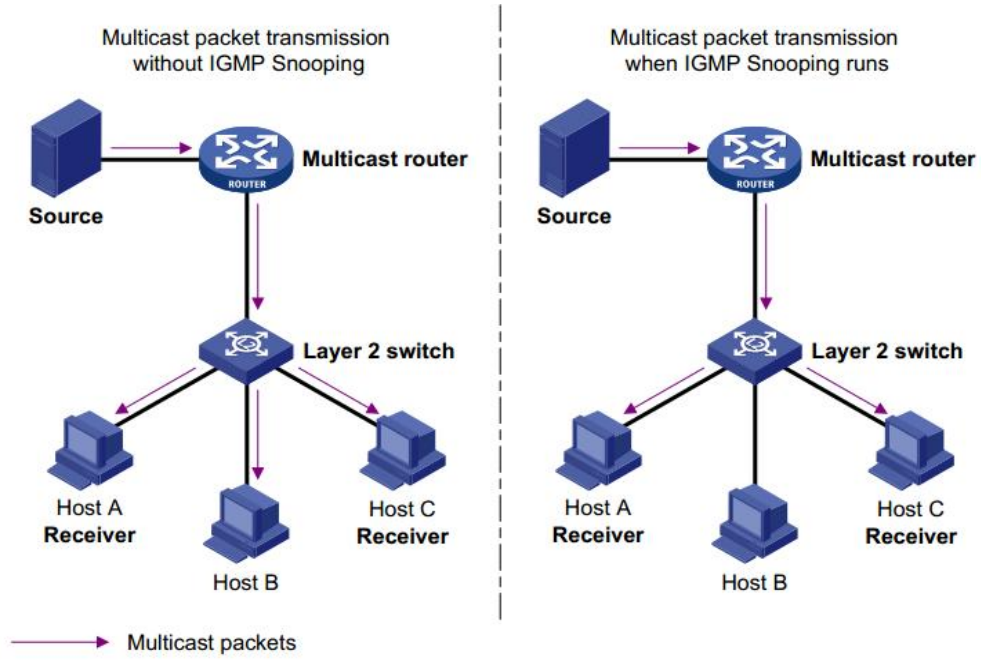
2. 单击导航树中的"组播 > 基本功能 > 过滤规则绑定"菜单进入过滤模板和端口绑定配置界面，如下图所示:

14.2 IGMP Snooping

IGMP 侦听（Internet Group Management Protocol Snooping）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 侦听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。

如下图所示，当二层设备没有运行 IGMP 侦听时，组播数据在二层被广播；当二层设备运行了 IGMP 侦听后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者，但是未知组播数据仍然会在二层广播。



14.2.1 功能配置

IGMP Snooping，用于 IPv4 网络，部署位置,组播路由器和用户主机之间的二层交换机上，配置在 VLAN 内，作用，侦听路由器和主机之间发送的 IGMP/MLD 报文建立组播数据的二层转发表，从而管理和控制组播数据在二层网络中的转发。

缺省情况下交换机的 IGMP Snooping 功能处于去使能状态，因此需要使能交换机的全局 IGMP Snooping 功能。

操作步骤：

1. 单击导航树中的"组播 > IGMP Snooping > 功能配置"菜单，进入 IGMP-snooping 配置界面，界面中包含已创建的 VLAN 信息，选择需要配置的 VLAN，点击修改进入详细配置界面，如下图所示：

组播VLAN配置表

VLAN	运行状态	路由端口学习	查询次数	查询间隔	最大查询响应时间	特定组查询次数	特定组查询间隔	快速离开
1	禁用	启用	2	125	10	2	1	禁用
2	禁用	启用	2	125	10	2	1	禁用
10	禁用	启用	2	125	10	2	1	禁用
20	禁用	启用	2	125	10	2	1	禁用
100	禁用	启用	2	125	10	2	1	禁用

修改

界面信息含义如下表所示。

配置项	说明
VLAN	需要配置的 VLANID
状态	在此 VLAN 下开启或关闭 IGMP-snooping 功能
路由端口学习	使能和去使能路由端口自动学习
快速离开	使能和去使能组播成员快速离开功能
查询次数	组播查询的最大次数
查询间隔	查询报文的间隔时间
最大查询响应时间	查询报文的超时时间，超过最大响应时间为超时
特定组查询次数	特定组查询的最大次数
特定组查询间隔	特定组查询报文的间隔时间

2. 填写相应的配置项，单击“应用”，完成配置。

14.2.2 查询器配置

配置和查看 IGMP Snooping 查询器配置信息

操作步骤：

1. 单击导航树中的“组播 > IGMP Snooping > 查询器配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
VLAN	组播 VLAN
状态	配置状态
运行状态	当前运行状态
版本	组播版本
查询器地址	查询器的组播地址

14.2.3 报文统计

查看 IGMP Snooping 的报文统计

操作步骤:

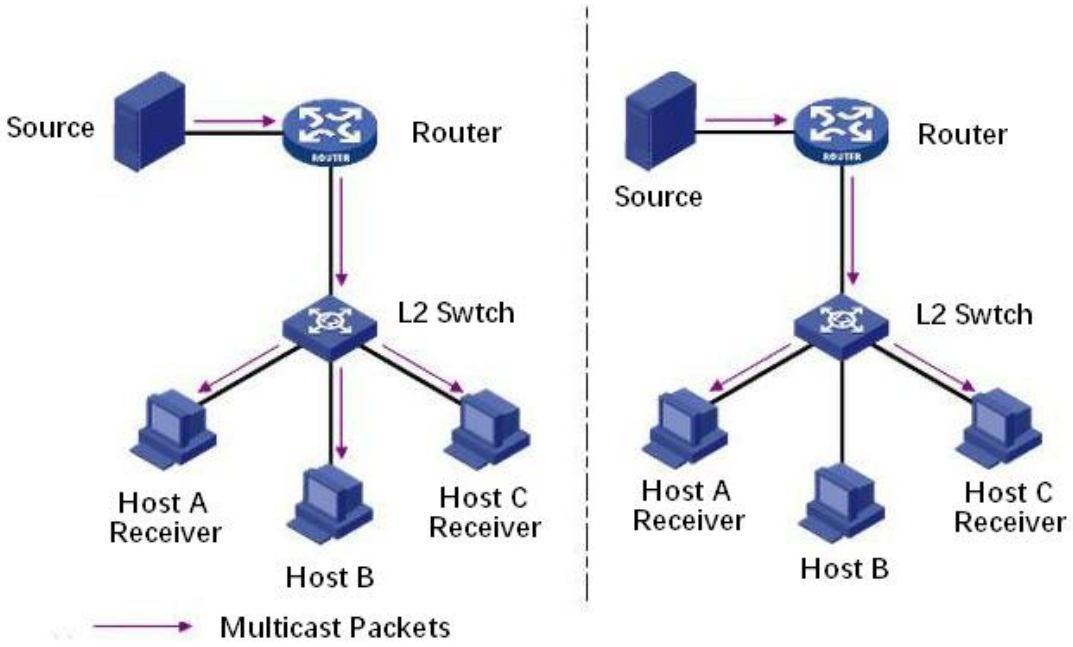
1. 单击导航树中的“组播 > IGMP Snooping > 报文统计”菜单进入界面，如下图所示:

14.3 MLD Snooping

MLD snooping 是多播侦听器发现 snooping 的缩写。它是一种运行在第二层设备上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组。

运行 MLD 侦听的第二层设备通过分析接收到的 MLD 消息建立端口和 MAC 组播地址之间的映射关系，并根据映射关系转发 IPv6 组播数据

如下图所示，当第二层设备不运行 MLD snooping 时，IPv6 组播数据包在第二层进行广播；当第二层设备运行 MLD snooping 时，已知 IPv6 组播组的组播数据包将不在第二层进行广播，而是组播到第二层的指定接收者。



MLD 窥探只能通过第二层组播将信息转发给需要的接收者，这样可以带来以下好处：

- 减少二层网络中的广播包，节省网络带宽；
- 增强 IPv6 组播信息的安全性；
- 每台主机单独充电方便。

14.3.1 功能配置

全局 MLD Snooping 功能配置，默认情况下是禁用的。

操作步骤：

1. 单击导航树中的“组播 > MLD Snooping > 功能配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
VLAN	需要配置的 VLANID

状态	在此 VLAN 下开启或关闭 MLD Snooping 功能
路由端口学习	使能和去使能路由端口自动学习
快速离开	使能和去使能组播成员快速离开功能
查询次数	组播查询的最大次数
查询间隔	查询报文的间隔时间
最大查询响应时间	查询报文的超时时间，超过最大响应时间为超时
特定组查询次数	特定组查询的最大次数
特定组查询间隔	特定组查询报文的间隔时间

2. 填写相应的配置项，单击“应用”，完成配置。

14.3.2 报文统计

查看 MLD Snooping 报文统计

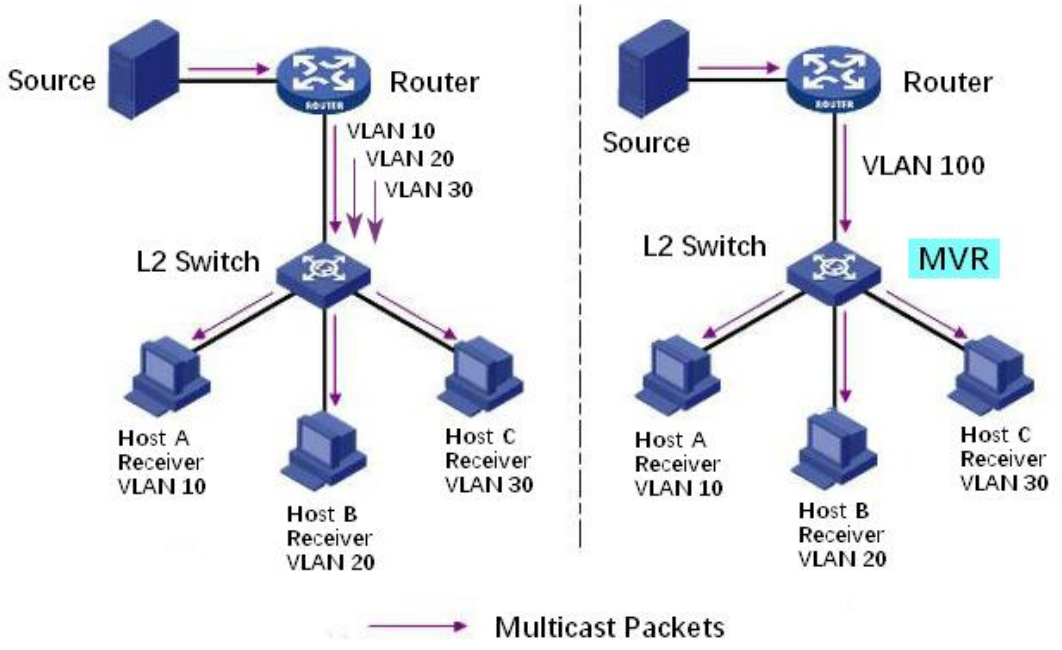
操作步骤：

1. 单击导航树中的“组播 > MLD Snooping > 报文统计”菜单进入界面，如下图所示：

14.4 MVR

为了解决二层网络中基于 VLAN 的组播业务广播问题，我们采用 IGMP 侦听协议来控制接收端，即只有接收端才能正常接收组播业务。

然而，IGMP 侦听只能有效地控制同一个组播 VLAN 的流量，而不能有效地控制跨 VLAN 的流量。因此，同一组播在不同 VLAN 中的多次复制效率仍然存在。为了解决跨 VLAN 的泛洪问题，我们采用了组播源流量的专用组播 VLAN，如下图所示



14.4.1 功能配置

查看和配置 MVR 全局功能，默认为去使能

操作步骤：

1. 单击导航树中的“组播 > MVR > 功能配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
状态	MVR 全局开关
VLAN	组播 MVR VLAN
Mode	兼容：MVR 交换机的 CPU 通常转发路由器的查询消息和客户端的加入消息，形成动态学习的组播转发表。但是，CPU 不会将 join 消息转发到路由器端口，因此上层路由器不会接收到下面的 join 消息，导致路由器数据无法正常转发到交换机。在此模式下，需要手动配置路由器多播转发表将数据转发给交换机 动态：动态模式和兼容模式的唯一区别是 CPU 可以在动态模式下将连接消息转发到路由器端口，这样上层路由器就可以动态地学习组播转发表，并且不需要手动配置路由器的组播转发表就可以将数据转发给交换机
起始组地址	组播组起始地址
组数	组播数量
查询时延	组播组查询时延

2. 填写相应的配置项，单击“应用”，完成配置。

14.4.2 端口配置

操作步骤：

1. 单击导航树中的“组播 > MVR > 端口配置”菜单进入界面，如下图所示：

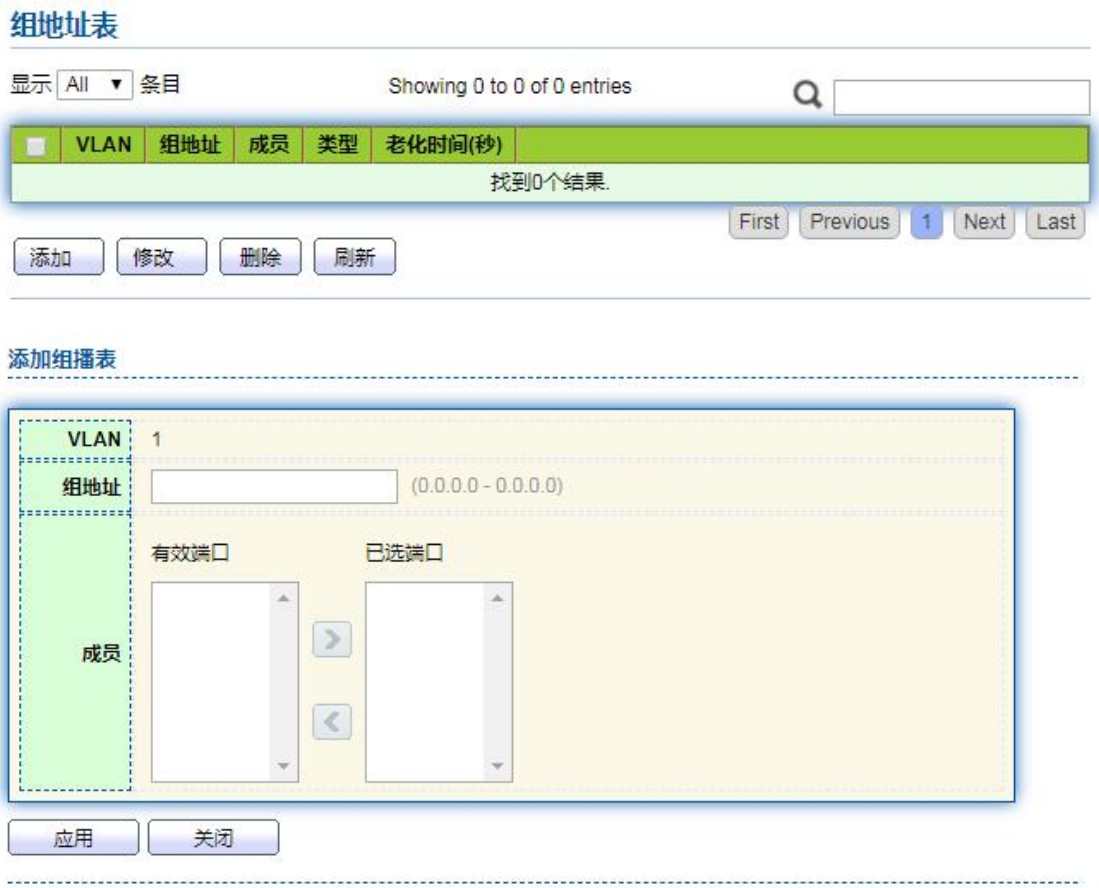
界面信息含义如下表所示。

查询项	说明
端口	选择的端口列表
角色	接收器：表示多播主机连接到的交换机的端口，用于接收多播流 组播源：源端口是指上层设备组播流的源端口，即组播源接入端口
快速离开	组播成员快速离开

14.4.3 组地址配置

操作步骤：

1. 单击导航树中的“组播 > MVR > 组地址配置”菜单进入界面，如下图所示：



界面信息含义如下表所示。

查询项	说明
VLAN	组播 VLAN
组地址	组地址
成员	成员端口列表

15. 路由

交换机提供三层 VLAN 接口，用于与网络层设备通信。VLANIF 接口为网络层接口，可配置 IP 地址。在创建 VLANIF 接口之前，首先要创建相应的 VLAN。通过 VLANIF 接口，交换机可以与其他网络层设备进行通信。

15.1 IPv4 管理接口

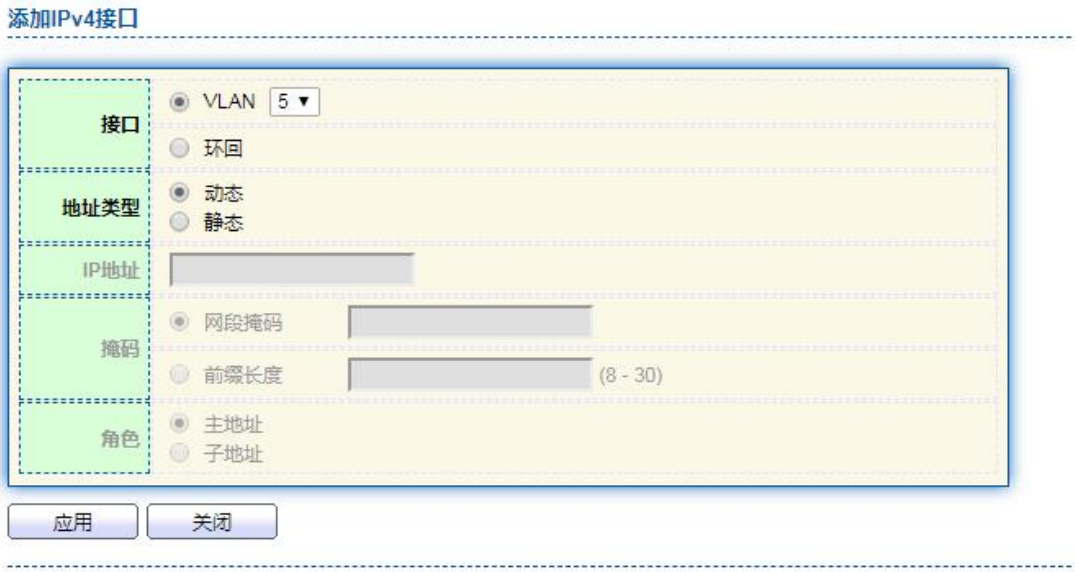
15.1.1 IPv4 接口

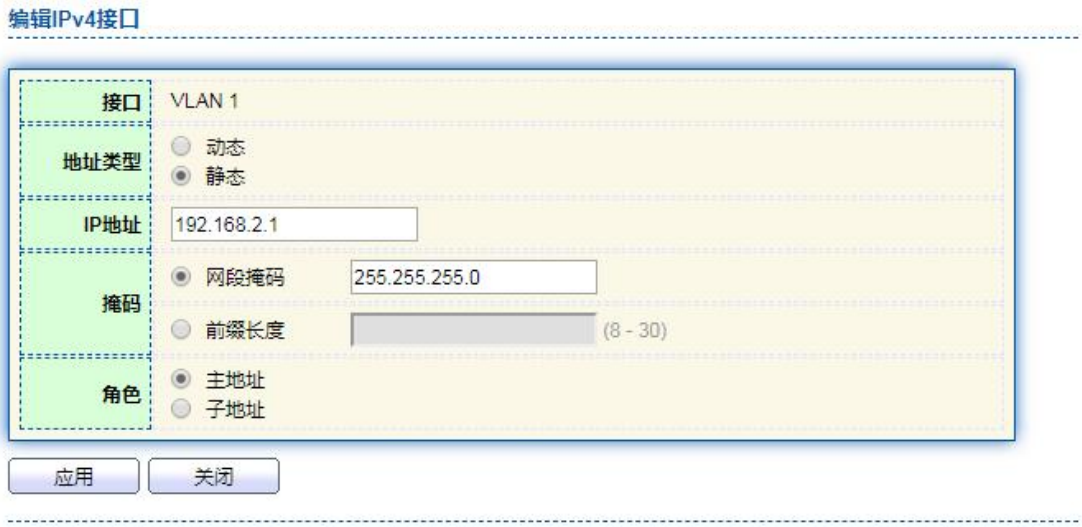
系统出厂时会启动 VLAN1 的接口地址为：**192.168.2.1**，该接口地址用于交换机的 WEB 登录

操作步骤：

1. 单击导航树中的“路由 > IPv4 管理接口 > IPv4 接口”菜单进入界面，如下图所示：

2. 单击“添加”或“修改”，进入接口的配置界面，如下图所示：





界面信息含义如下表所示。

查询项	说明
接口	可选 VLAN 接口或环回接口
地址类型	可选动态获取或静态配置
IP 地址	当地址类型为静态时，手工配置 IP 地址
掩码	当地址类型为静态时，手工配置 IP 地址掩码
角色	主地址：接口的主用地址 子地址：除接口主用地址外其他地址，必须先存在主用地址

15.1.2 IPv4 路由

操作步骤：

1. 单击导航树中的“路由 > IPv4 管理接口 > IPv4 路由”菜单进入界面，如下图所示：

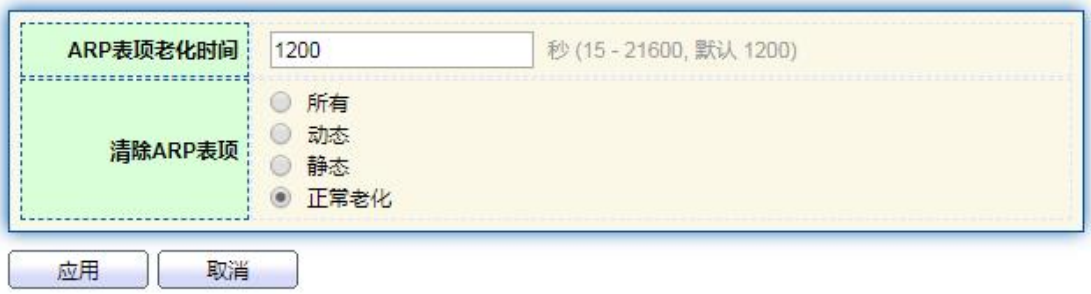
界面信息含义如下表所示。

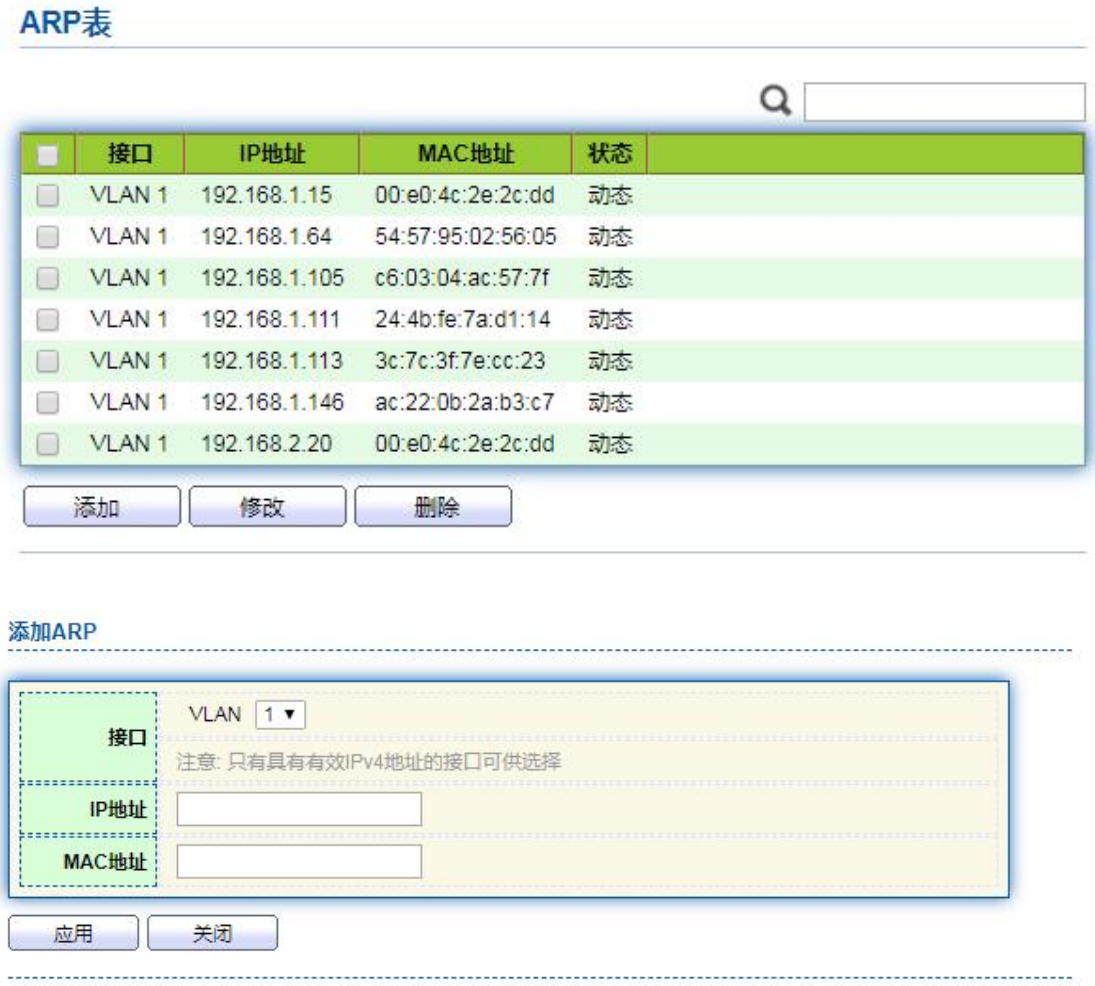
查询项	说明
IP 地址	目的网络地址
掩码	目的网络地址掩码
下一跳路由地址	下一跳网关地址
跃点数	路由跳数

15.1.3 ARP

操作步骤:

1. 单击导航树中的“路由 > IPv4 管理接口 > ARP”菜单进入界面，如下图所示:





界面信息含义如下表所示。

查询项	说明
接口	VLAN ID
IP 地址	IP 地址
MAC 地址	IP 地址对应的 MAC 地址

15.2 IPv6 管理接口

15.2.1 IPv6 接口

操作步骤：

1. 单击导航树中的“路由 > IPv6 管理接口 > IPv6 接口”菜单进入界面，如下图所示：

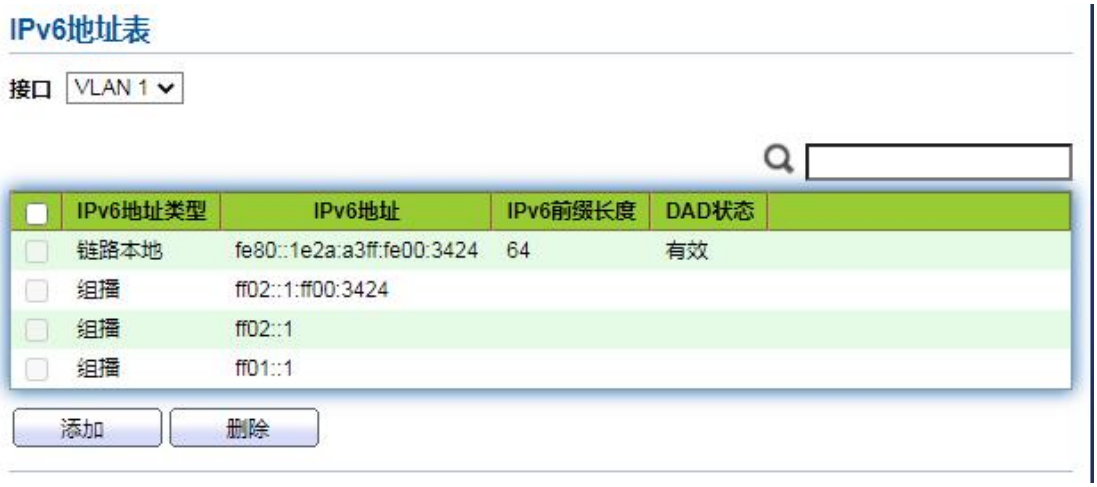
界面信息含义如下表所示。

查询项	说明
接口	可选 VLAN 接口或环回接口
自动分配	自动配置开关，默认使能
DAD 尝试	配置为重复地址检测发送邻居请求消息的次数
无状态	无状态自动配置开关
信息刷新时间	自动配置刷新时间
最短信息刷新时间	最大刷新时间次数

15.2.2 IPv6 地址

操作步骤：

1. 单击导航树中的“路由 > IPv6 管理接口 > IPv6 地址”菜单进入界面，如下图所示：



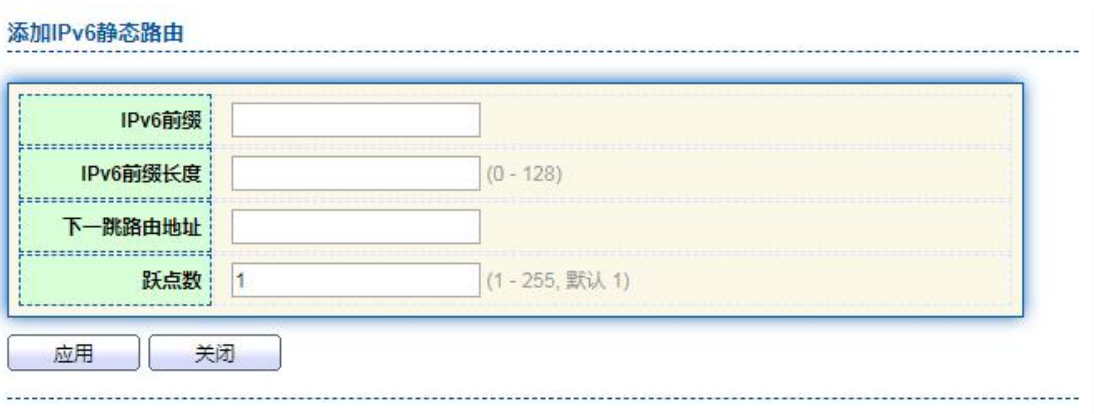
界面信息含义如下表所示。

查询项	说明
接口	VLAN 接口
IPv6 地址类型	可选全局或链路本地地址
IPv6 地址	IPv6 地址
前缀长度	IPv6 地址前缀
EUI-64	启用或禁用从 IEEE802 地址派生的地址

15.2.3 IPv6 路由

操作步骤：

1. 单击导航树中的“路由 > IPv6 管理接口 > IPv6 路由”菜单进入界面，如下图所示：



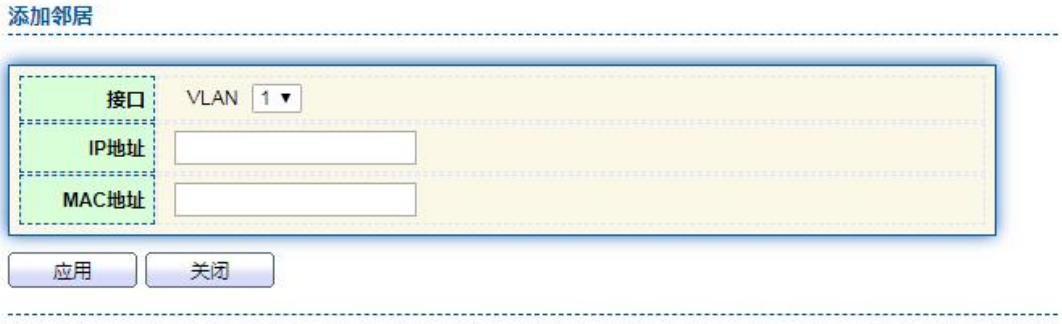
界面信息含义如下表所示。

查询项	说明
IPv6 前缀	IPv6 网络地址
IPv6 前缀长度	IPv6 网络地址前缀
下一跳路由地址	下一跳 IPv6 网关地址
跃点数	路由跳数

15.2.4 IPv6 邻居

操作步骤：

1. 单击导航树中的“路由 > IPv6 管理接口 > IPv6 邻居”菜单进入界面，如下图所示：



界面信息含义如下表所示。

查询项	说明
接口	VLAN ID
IP 地址	IPv6 地址
MAC 地址	IPv6 地址对应的 MAC 地址

16 安全

16.1 RADIUS

操作步骤：

1. 单击导航树中的“安全 > RADIUS”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
地址类型	可选主机名、IPv4 和 IPv6 地址

服务器地址	根据地址类型配置服务器 IP 地址
服务器端口号	服务器的端口号，默认为 1812
优先级	服务器优先级
密钥	服务器的密钥
重连次数	服务器的重新连接次数
超时时间	服务器连接超时时间
用途	服务器的应用场景，可选登录认证或 802.1X 认证或所有

16.2 TACACS+

操作步骤：

1. 单击导航树中的“安全 > TACACS+”菜单进入界面，如下图所示：

界面信息含义如下表所示。

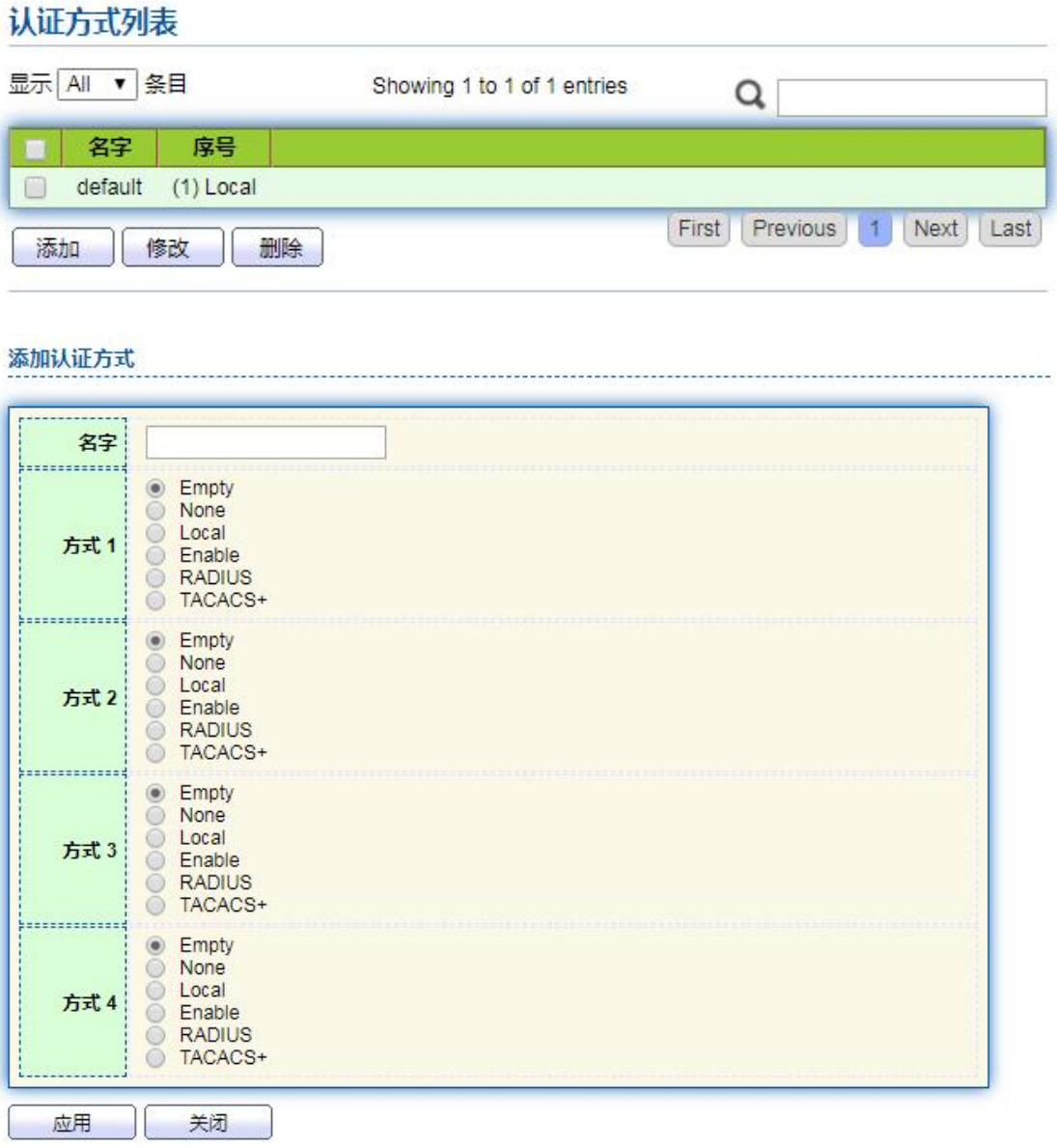
查询项	说明
地址类型	可选主机名、IPv4 和 IPv6 地址
服务器地址	根据地址类型配置服务器 IP 地址
服务器端口号	服务器的端口号，默认为 49
优先级	服务器优先级
Key 字符串	密钥字符串值
超时	服务器连接超时时间

16.3 AAA

16.3.1 认证方式配置

操作步骤：

1. 单击导航树中的“安全 > AAA > 认证方式配置”菜单进入界面，如下图所示：



界面信息含义如下表所示。

查询项	说明
名字	认证方式的名称
方式 1~4	Empty：方法被禁用 None：什么都不做，只是让用户通过身份验证 Local：使用本地用户数据库进行身份验证 Enable：使用本地启用密码数据库进行身份验证 RADIUS：使用远程 RADIUS 服务器进行身份验证 TACACS+：使用远程 TACACS+服务器进行身份验证

16.3.2 登录认证

操作步骤:

1. 单击导航树中的“安全 > AAA > 登录认证”菜单进入界面，如下图所示:

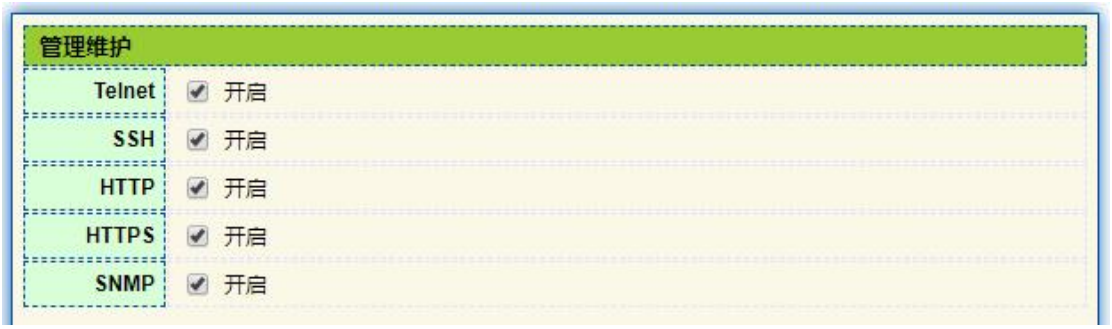
16.4 管理通道配置

16.4.1 管理服务

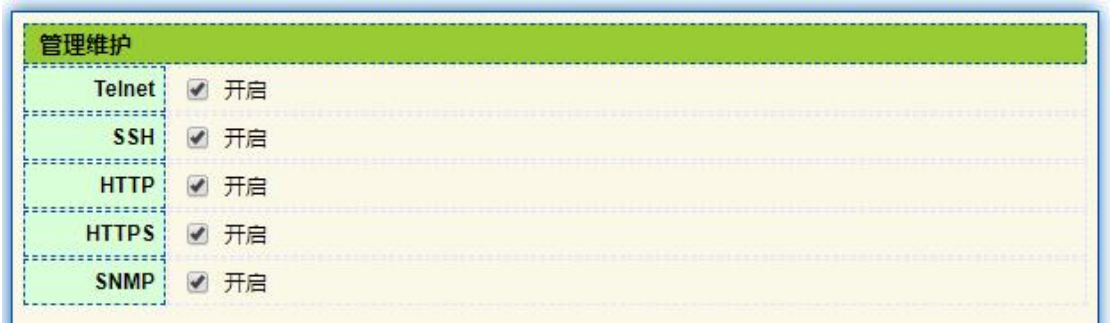
操作步骤:

1. 单击导航树中的“安全 > 管理通道配置 > 管理服务”菜单进入界面，如下图所示:

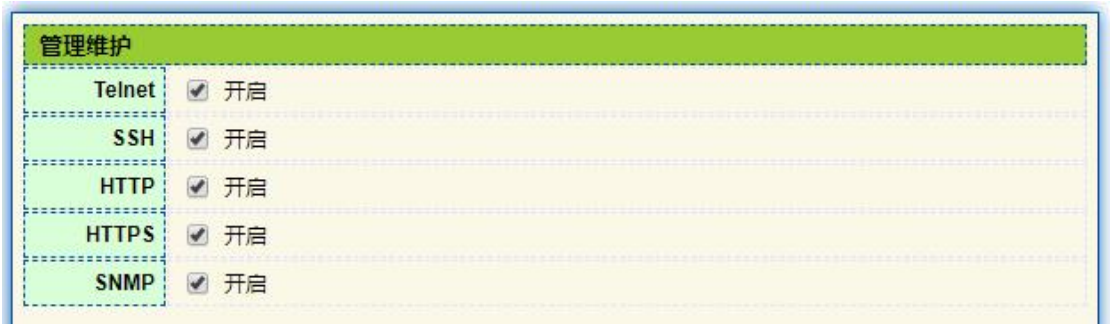
2. 在管理维护中选择 Telnet 服务，点击“应用”完成配置，如下图所示:



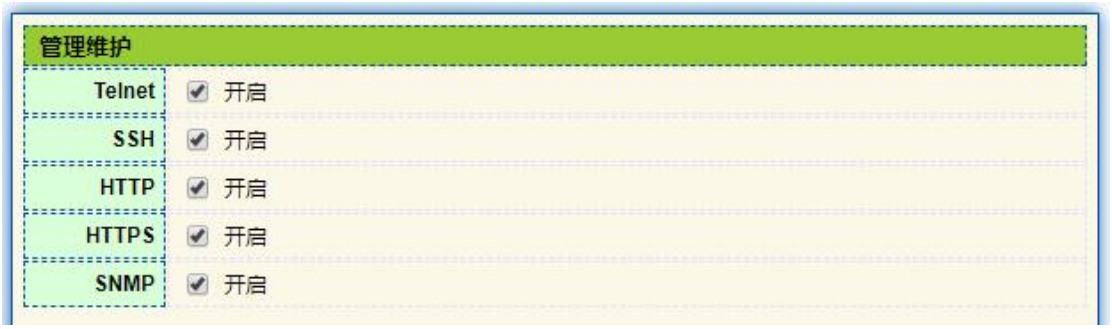
3. 在管理维护中选择 SSH 服务，点击“应用”完成配置，如下图所示：



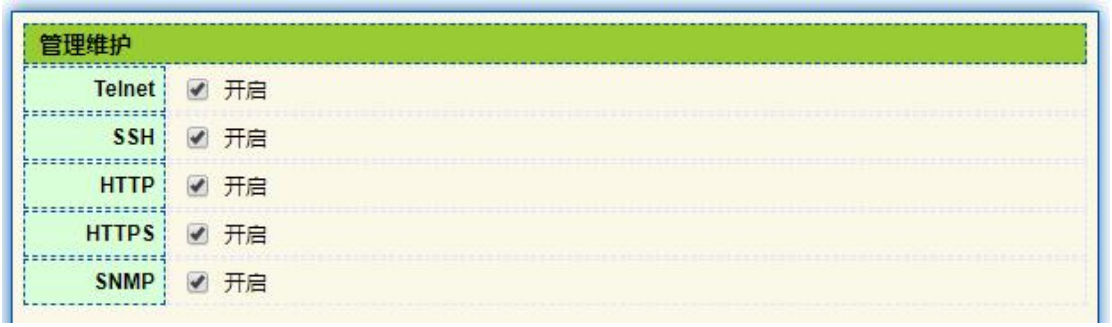
4. 在管理维护中选择 HTTP 服务，点击“应用”完成配置，如下图所示：



5. 在管理维护中选择 HTTPS 服务，点击“应用”完成配置，如下图所示：



6. 在管理维护中选择 SNMP 服务，点击“应用”完成配置，如下图所示：



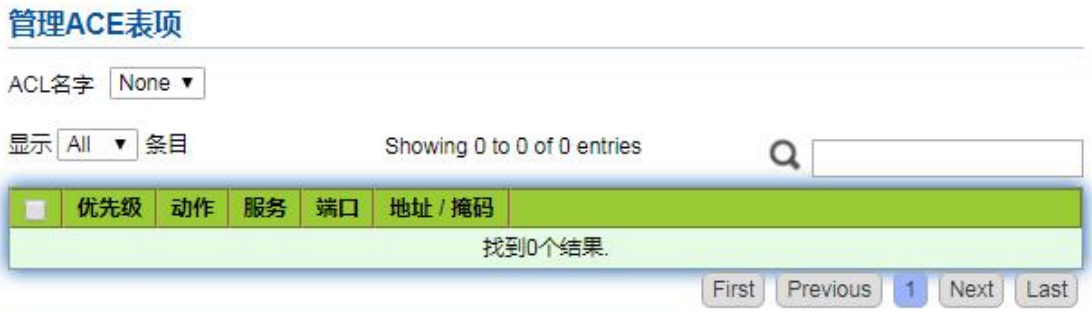
16.4.2 管理 ACL

配置和查看应用于管理的 ACL 规则

操作步骤:

1. 单击导航树中的"安全 > 管理通道配置 > 管理 ACL"菜单进入界面，如下图所示:

2. 单击导航树中的"安全 > 管理通道配置 > 管理 ACE"菜单进入界面，如下图所示:



界面信息含义如下表所示。

查询项	说明
ACL 名字	管理 ACL 的名称
优先级	ACE 规则的优先级
服务	可选所有、HTTP、HTTPS、SNMP、SSH、TELNET
动作	允许：匹配的数据帧允许通过 拒绝：匹配的数据帧丢弃
端口	应用管理 ACL 的端口列表
IP 版本	IP 的版本号
IPv4	根据 IP 的版本配置 IPv4 地址
IPv6	根据 IP 的版本配置 IPv6 地址

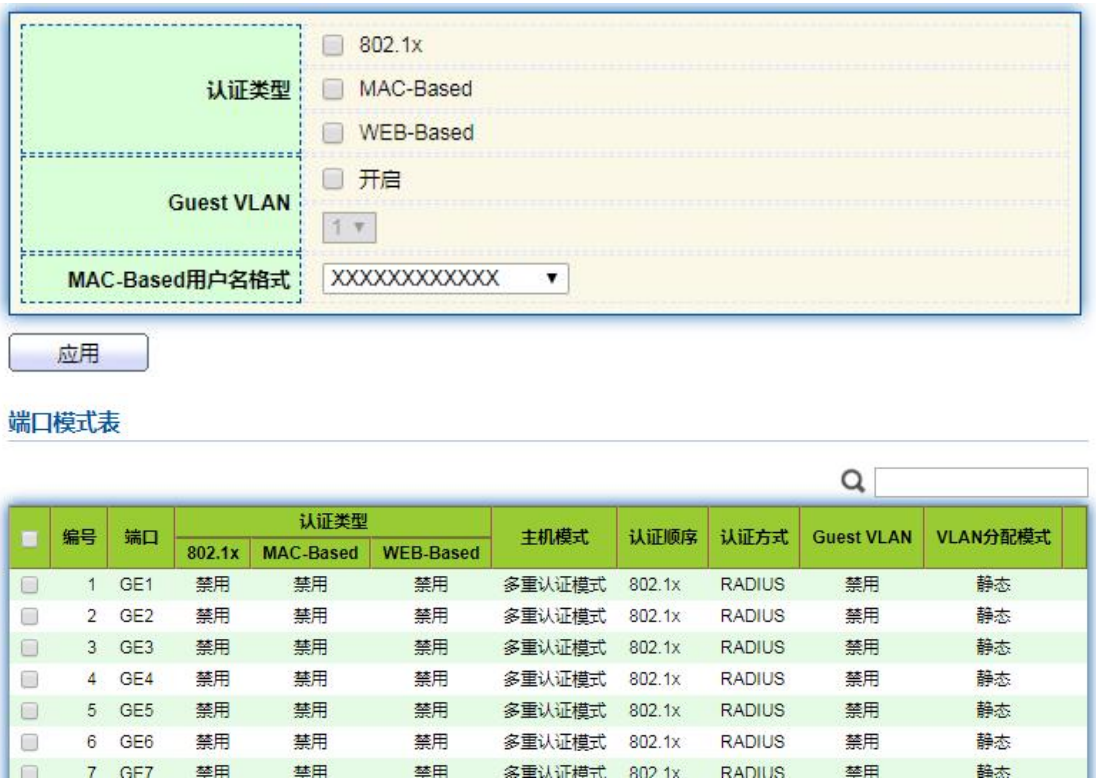
16.5 认证功能

16.5.1 功能配置

启用 802.1x/MAC/WEB 身份验证网络访问控制的全局设置

操作步骤:

1. 单击导航树中的“安全 > 认证功能 > 功能配置”菜单进入界面，如下图所示:



编号	端口	认证类型			主机模式	认证顺序	认证方式	Guest VLAN	VLAN分配模式
		802.1x	MAC-Based	WEB-Based					
1	GE1	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态
2	GE2	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态
3	GE3	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态
4	GE4	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态
5	GE5	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态
6	GE6	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态
7	GE7	禁用	禁用	禁用	多重认证模式	802.1x	RADIUS	禁用	静态

界面信息含义如下表所示。

查询项	说明
端口	端口列表
认证类型	可选 802.1x、MAC-Based 和 WEB-Based
主机模式	多重认证模式：在这种模式下，每个客户机都需要分别通过身份验证过程。 多主机模式：在这种模式下，只有一个客户端需要进行身份验证，其他客户端将获得相同的访问权限。 单主机模式：在这种模式下，只能对一个主机进行身份验证。它与最大主机数配置为 1 的多身份验证模式相同
认证顺序	认证的动作顺序
认证方式	认证的方式类型
Guest VLAN	访客 VLAN 的开关状态
VLAN 分配模式	拒绝：如果获得 VLAN 授权信息，就使用它。但是，如果没有 VLAN

	授权信息，拒绝主机并使其未经授权 静态：如果获得 VLAN 授权信息，就使用它。如果没有 VLAN 授权信息，则保留主机的原始 VLAN。

16.5.2 端口配置

操作步骤：

1. 单击导航树中的“安全 > 认证功能 > 功能配置”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
端口	端口列表
端口控制	强制认证：端口被强制授权，所有客户端都可以访问网络。 强制未授权：端口为强制未授权，所有客户端 自动：需要通过身份验证程序才能获得网络可访问性
重认证	端口重认证开关
最大主机数	多身份验证模式的端口最大主机数
重认证周期	如果本地数据库或远程身份验证服务器未分配重新验证时间，则端口重新验证周期值以秒为单位
保活周期	端口去激活的超时时间
静默周期	端口静默时间
发送周期	端口 802.1x EAP 报文发送周期
客户端超时时间	端口请求超时时间
服务器超时时间	802.1X 服务器响应超时时间
最大请求次数	端口 802.1x 最大 EAP 请求值
最大登录失败次数	端口 WEB 身份验证最大登录尝试次数

16.5.3 MAC-Based 本地账户

操作步骤：

1. 单击导航树中的“安全 > 认证功能 > MAC-Based 本地账户”菜单进入界面，如下图所示：

16.5.4 WEB-Based 本地账户

操作步骤：

1. 单击导航树中的“安全 > 认证功能 > WEB-Based 本地账户”菜单进入界面，如下图所示：

16.5.5 会话信息

操作步骤:

1. 单击导航树中的“安全 > 认证功能 > 会话信息”菜单进入界面，如下图所示:

16.6 DOS 防攻击

16.6.1 功能配置

为了提高交换机的安全性，可以开启交换机的防攻击选项

操作步骤

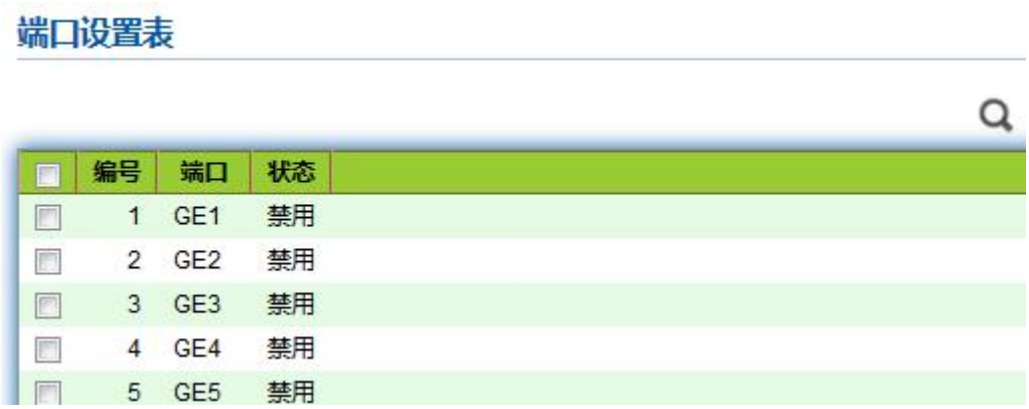
1. 单击导航树中的“安全 > DOS 防攻击 > 功能设置”菜单，进入“ DOS 防攻击全局设置”，分别启用“防止 POD 攻击”，“防止 Land 攻击”，“丢弃源目的 MAC 相同包”，“丢弃 ICMP 分片包”，单击 “应用”，完成配置，界面如下图所示。

16.6.2 端口配置

基于端口开启 DOS 防攻击选项

操作步骤

1. 单击导航树中的“安全 > DOS 防攻击 > 端口配置”菜单，进入“ DOS 防攻击端口设置”，如下图所示。



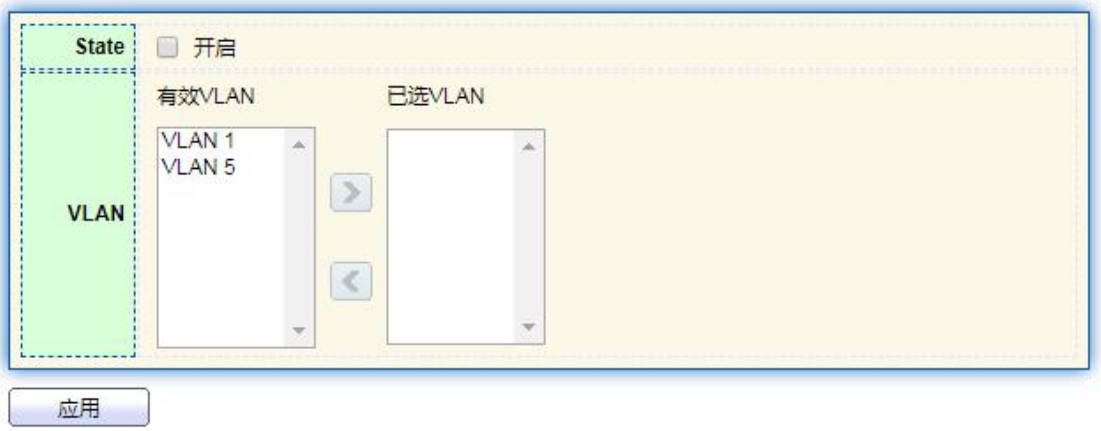
2. 选中端口并点击“修改”，进入修改端口配置，开启和关闭端口 DOS 防攻击设置，如下图所示。

16.7 动态 ARP 检查

16.7.1 功能配置

操作步骤：

1. 单击导航树中的“安全 > 动态 ARP 检查 > 功能配置”菜单进入界面，如下图所示：



2. 选择端口列表，单击“修改”进入端口配置界面，所下图所示：

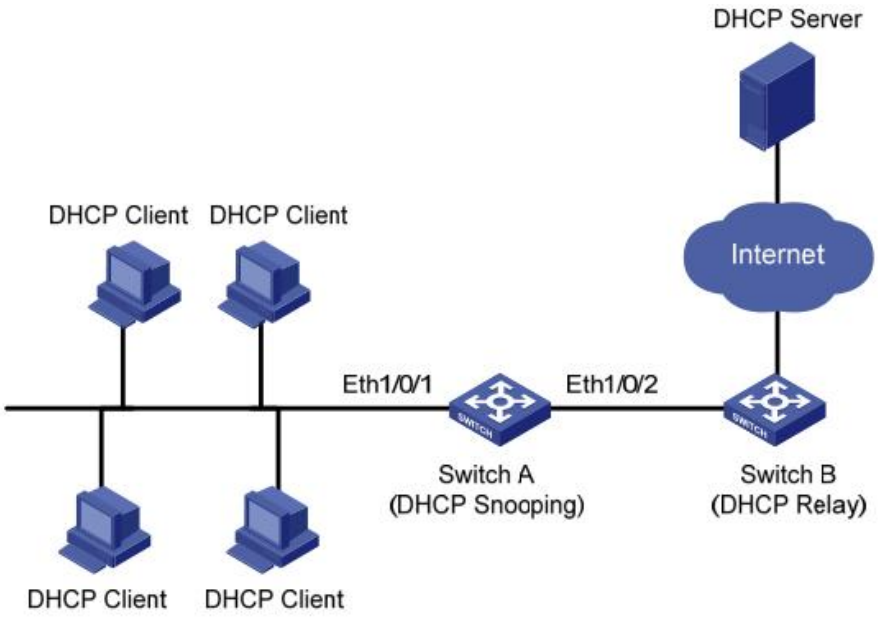
16.7.2 报文统计

操作步骤：

1. 单击导航树中的“安全 > 动态 ARP 检查 > 报文统计”菜单进入界面，如下图所示：

16.8 DHCP Snooping

出于安全性的考虑，网络管理员可能需要记录用户上网时所用的 IP 地址，确认用户从 DHCP 服务器获取的 IP 地址和用户主机的 MAC 地址的对应关系。交换机可以通过运行在网络层的 DHCP 中继的安全功能记录用户的 IP 地址信息。交换机可以通过运行在数据链路层的 DHCP Snooping 功能监听 DHCP 报文，记录用户的 IP 地址信息。另外，在网络中如果有私自架设的 DHCP 服务器，将可能导致用户得到错误的 IP 地址。为了使用户能通过合法的 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与不信任端口。信任端口是与合法的 DHCP 服务器直接或间接连接的端口。信任端口对接收到的 DHCP 报文正常转发，从而保证了 DHCP 客户端获取正确的 IP 地址。不信任端口是不与合法的 DHCP 服务器连接的端口。如果从不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文则会丢弃，从而防止了 DHCP 客户端获得错误的 IP 地址。



DHCP Snooping 典型组网

DHCP Snooping 通过以下两种方法来获得用户从 DHCP 服务器获取的 IP 地址和用户 MAC 地址信息：

- 监听 DHCP-REQUEST 报文
- 监听 DHCP-ACK 报文

16.8.1 功能配置

启用 DHCP-snooping

操作步骤：

1. 单击导航树中的“安全 > DHCP Snooping > 功能配置”菜单，进入 DHCP-snooping 配置界面，界面分为全局配置和端口配置，端口配置中点选需要修改的端口，点击修改，进入详细

修改界面，如下图所示

界面含义说明如下表

配置项	说明
状态	开启与关闭 DHCP-snooping
VLAN	DHCP-snooping 生效 VLAN 号
端口	配置 DHCP-snooping 的端口号
信任	该端口是否为信任端口

客户端地址检测	是否开启客户端地址一致性检查
限速	端口是否启用速率限制，限制值配置

2. 填写相应的配置项，单击“应用”，完成配置。

16.8.2 报文统计

操作步骤：

1. 单击导航树中的“安全 > DHCP Snooping > 报文统计”菜单进入界面，如下图所示：

16.8.3 Option82 功能配置

在网络中如果有私自架设的 DHCP 服务器，将可能导致用户得到错误的 IP 地址。为了使用户能通过合法的 DHCP 服务器获取 IP 地址，PS7024 以太网交换机的 DHCP Snooping 安全机制，允许将端口设置为信任端口与不信任端口。

- 信任端口 是与合法的DHCP服务器直接或间接连接的端口。信任端口对接收到的DHCP报文正常转发，从而保证了 DHCP 客户端获取正确的 IP 地址。

- 不信任端口 是不与合法的 DHCP 服务器连接的端口。如果从不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文则会丢弃，从而防止了 DHCP 客户端获得错误的 IP 地址。

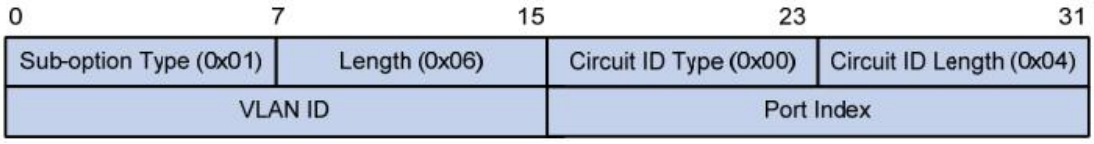
Option 82 是 DHCP 报文中的中继代理信息选项（Relay Agent Information option），该选项记录了 DHCP 客户端的位置信息。DHCP 中继（或 DHCP Snooping 设备）接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，可以在该报文中添加 Option 82 选项，以便管理员定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 选项的服务器还可以根据该选项的信息制订 IP 地址和其他参数的分配策略，提供更加灵活的地址分配方式。

Option 82 选项最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前设备支持二个子选项： Circuit ID 子选项与 Remote ID 子选项。

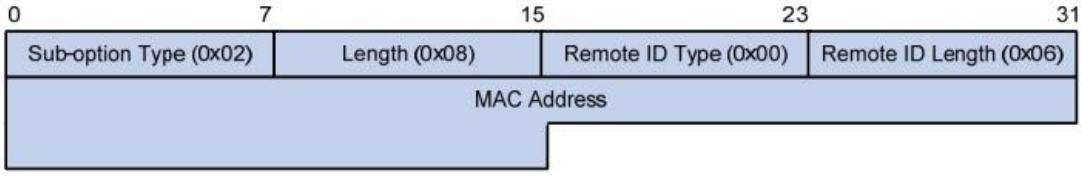
由于 RFC 3046 对于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。以太网交换机作为 DHCP 中继设备，支持 Option 82 子选项的扩展填充格式，其默认情况下的填充内容如下图。

sub-option 1 的内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引（端口索引的取值为端口物理编号减 1）。

sub-option 2 的内容是接收到 DHCP 客户端请求报文的 DHCP 中继设备的桥 MAC 地址。sub-option 1 的内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引（端口索引的取值为端口物理编号减 1）如下图。



sub-option 2 的内容是接收到 DHCP 客户端请求报文的 DHCP 中继设备的桥 MAC 地址。



DHCP 中继支持 Option 82 工作机制

DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取 IP 地址的过程与直接从 DHCP 服务器获取 IP 地址的过程基本相同，都要经历发现、提供、选择和确认四个阶段，这里将只介绍 DHCP 中继支持 Option 82 时的工作机制，具体如下：

(1) DHCP 中继设备收到 DHCP 请求报文后，将检查报文中是否已有 Option 82 选项，并进行相应的处理。

- 如果请求报文中已有 Option 82， DHCP 中继设备会按照配置的策略对该报文进行处理 （丢弃、 用中继设备本身的 Option 82 选项替代报文中原有的 Option82 选项或保持报文原有的 Option 82 选项），然后将请求报文转发给 DHCP 服务器。
- 如果请求报文中没有 Option 82 选项，则 DHCP 中继设备将 Option 82 选项添加到报文中后转发给 DHCP 服务器。

(2) DHCP 中继设备收到 DHCP 服务器的返回报文后， 将剥离报文中的 Option 82 信息，然后将带有 DHCP 配置信息的报文转发给 DHCP 客户端。

说明:

DHCP 客户端发送的请求报文有两种，分别为 DHCP-DISCOVER 报文和 DHCP-REQUEST 报文。由于不同厂商生产的 DHCP 服务器设备对请求报文的处理机制不同，有些设备处理 DHCP-DISCOVER 报文中的 Option 82 信息，而有些处理 DHCP-REQUEST 报文中的 Option 82 信息，因此 DHCP 中继设备将在这两种报文中都添加 Option 82 选项。

交换机配置了 DHCP Snooping，且支持 Option 82 功能后，当收到的 DHCP 客户端发送的 DHCP 请求报文中带有 Option 82 选项时，根据配置的处理策略和子选项内容不同，DHCP Snooping 对报文的处理机制不同。

操作步骤:

1. 单击导航树中的“安全 > DHCP Snooping > Option82 功能配置”菜单，进入 DHCP-snooping Option82 功能的配置界面，包含 Option82 全局设置和端口配置，选择需要配置的端口，点击修改按钮，进入端口 Option82 详细配置界面，如下图所示:

界面含义说明如下表:

配置项	说明
Remote-id	填充 Option 82 中 Remote-id 字段的内容（比如用户自定义内容 aaaaaaa）
端口	是否开启 Option82 的端口号
允许非信任	端口开启 Option82 功能后，非信任端口的报文处理方式: 保持：保持报文中的 Option 82 选项不变并进行转发 丢弃：丢弃报文 替换：替换报文中的 Option82 字段，根据 Circuit ID 配置来决定替换内容并转发

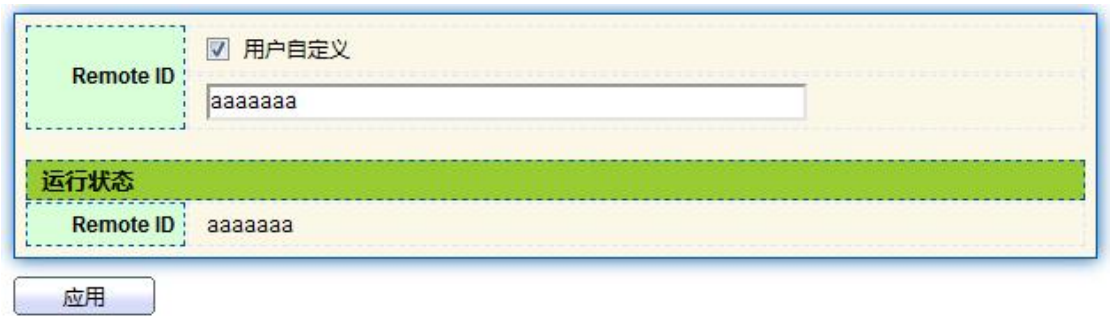
说明:

Option 82 字段中对 Circuit ID 子选项或 Remote ID 子选项的内容的配置相互独立，可以单独配置也可以同时配置，且配置顺序不分先后。

DHCP Option82 必须配置在设备的用户侧，否则设备向 DHCP Server 发出的 DHCP 报文不会携带 Option82 选项内容。

当接收到 DHCP 服务器的 DHCP 回应报文时，如果报文中含有 Option 82 选项，则删除 Option 82 字段进行转发；如果报文中没有 Option 82 选项，则直接转发。

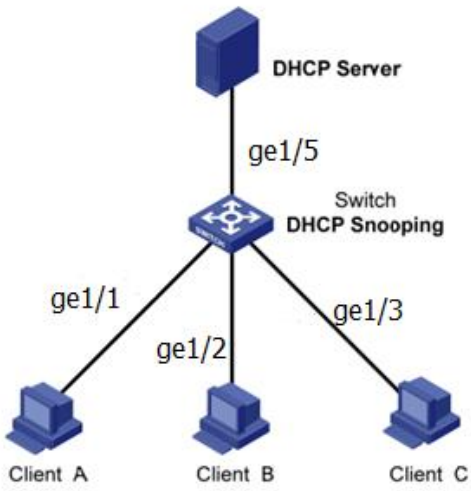
2. 填写相应的配置项。单击“应用”，完成配置，如下图。



D HCP Snooping 支持 Option 82 配置举例，如下图所示，Switch 的端口 ge1/5 与 DHCP 服务器端相连，端口 ge1/1、ge1/2、ge1/3 分别与 DHCP Client A、DHCP Client B、DHCP Client C 相连。

- 在 Switch 上开启 DHCP Snooping 功能。
- 设置 Switch 上端口 ge1/5 为 DHCP Snooping 信任端口。
- 在 Switch 上开启 DHCP Snooping 支持 Option 82 功能。对经过端口 ge1/3 的报文，填充 Option 82 按交换机 Circuit ID 与 Remote-id 默认的配置。

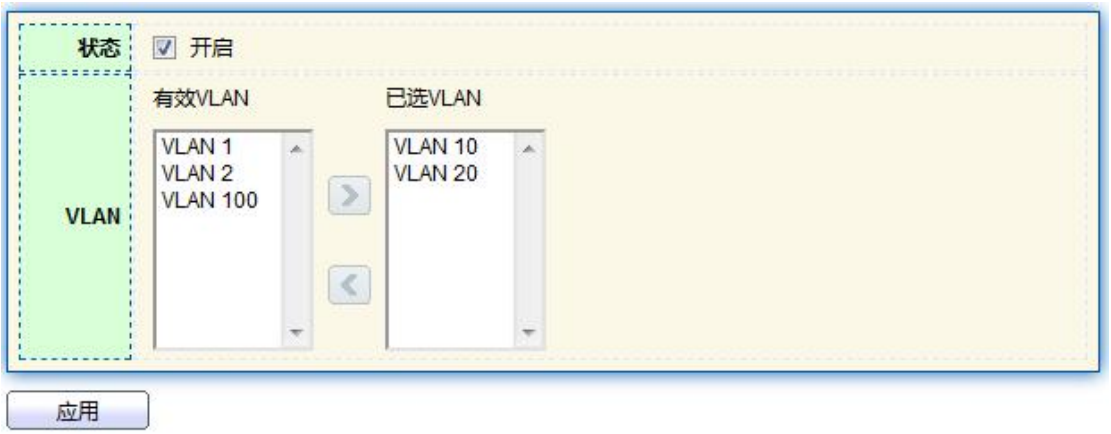
组网图



配置 DHCP Snooping 支持 Option 82 功能组网图

操作步骤:

1. 开启交换机 DHCP Snooping 功能。单击导航树中的“安全 > DHCP-Snooping > 功能配置”菜单，进入“功能配置”界面，开启功能，如下图所示。



2. 设置端口 ge1/5 为 DHCP Snooping 信任端口。，填写相应配置，单击“修改”。界面如下图所示。

端口设置表

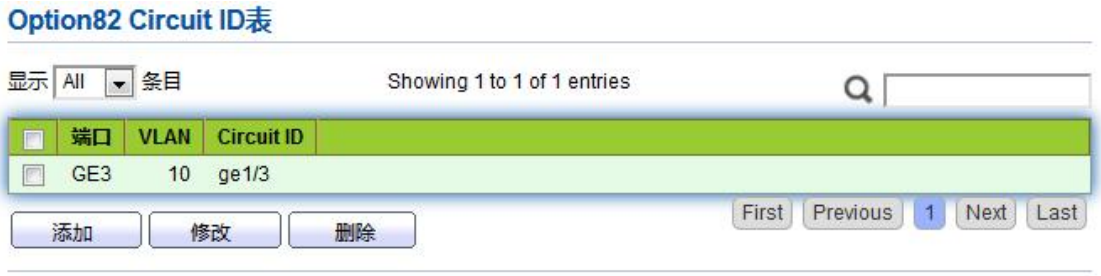
编号	端口	信任	客户端地址检查	限速
1	GE1	禁用	禁用	不限速
2	GE2	禁用	禁用	不限速
3	GE3	禁用	禁用	不限速
4	GE4	禁用	禁用	不限速
5	GE5	启用	禁用	不限速
6	GE6	禁用	禁用	不限速
7	GE7	禁用	禁用	不限速

3. 在以太网端口 ge1/3 上配置，对 DHCP 报文的 Option 82 中 Remote-id。单击导航树中的“安全 > DHCP Snooping > Option 82 功能配置”菜单，进入“Option 82 功能配置”，选择端口，进入端口设置页面，选择相应配置，单击“应用”完成配置。界面如下图所示。

端口设置表

编号	端口	状态	允许非信任
1	GE1	禁用	丢弃
2	GE2	禁用	丢弃
3	GE3	启用	替换
4	GE4	禁用	丢弃
5	GE5	禁用	丢弃

4. 在以太网端口 ge1/3 上配置，对 DHCP 报文的 Option 82 中 Circuit-id。单击导航树中的“安全 > DHCP Snooping > Option82 Circuit ID 功能配置”菜单，进入“Option 82Circuit-id 功能配置”，添加端口配置，进入端口设置页面，选择相应配置，单击“应用”完成配置。界面如下图所示。



16.9 IP Source Guard

IP 源防护（IPSG）是一种基于 IP/Mac 的端口流量过滤技术，可以有效地防止局域网中的 IP 地址欺骗攻击。IPSG 可以保证二层网络中终端设备的 IP 地址不被劫持，也可以保证未经授权的设备不能通过自己指定的 IP 地址访问网络或攻击网络，导致网络崩溃和瘫痪

16.9.1 端口配置

操作步骤:

1. 单击导航树中的“安全 > IP Source Guard > 端口配置”菜单进入界面，如下图所示:

界面信息含义如下表所示。

查询项	说明
端口	端口列表
状态	端口开关状态
校验模式	IP：默认 IP 源防护过滤源 IP 地址。 IP-MAC：不仅过滤源 IP 地址，而且过滤源 MAC 地址
最大条数	端口允许通过最大数据

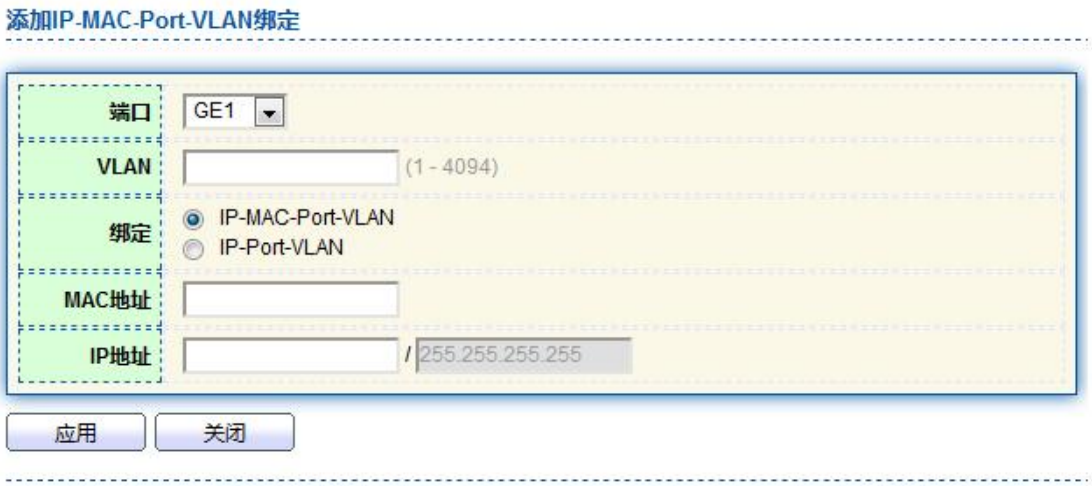
16.9.2 IMPV 绑定

在 DHCP 网络中，静态获取 IP 地址的用户（非 DHCP 用户）对网络可能存在多种攻击，譬如仿冒 DHCP Server、构造虚假 DHCP Request 报文等。这将为合法 DHCP 用户正常使用网络带来了一定的安全隐患。

为了有效的防止非 DHCP 用户攻击，可开启设备根据 DHCP Snooping 绑定表生成接口的静态 MAC 表项功能。之后，设备将根据接口下所有的 DHCP 用户对应的 DHCP Snooping 绑定表项自动执行命令生成这些用户的静态 MAC 表项，并同时关闭接口学习动态 MAC 表项的能力。此时，只有源 MAC 与静态 MAC 表项匹配的报文才能够通过该接口，否则报文会被丢弃。因此对于该接口下的非 DHCP 用户，只有管理员手动配置了此类用户的静态 MAC 表项，其报文才能通过，否则报文将被丢弃。

操作步骤：

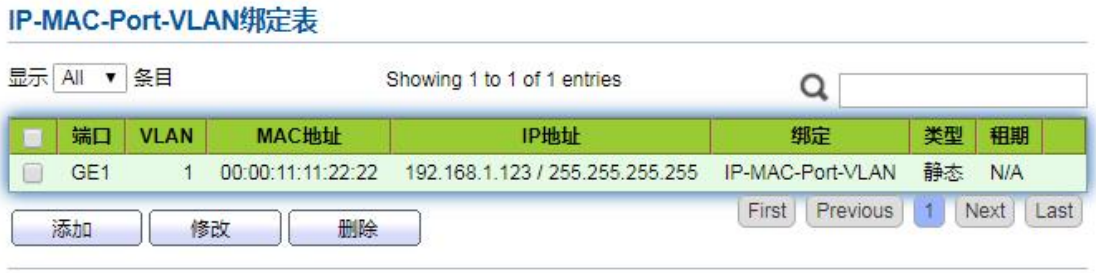
1. 单击导航树中的“安全 > IP Source Guard > IMPV 绑定”菜单，进入 IP Source Guard 的绑定配置界面，点击添加，新增 IP-MAC-Port-VLAN 绑定组，如下图所示：



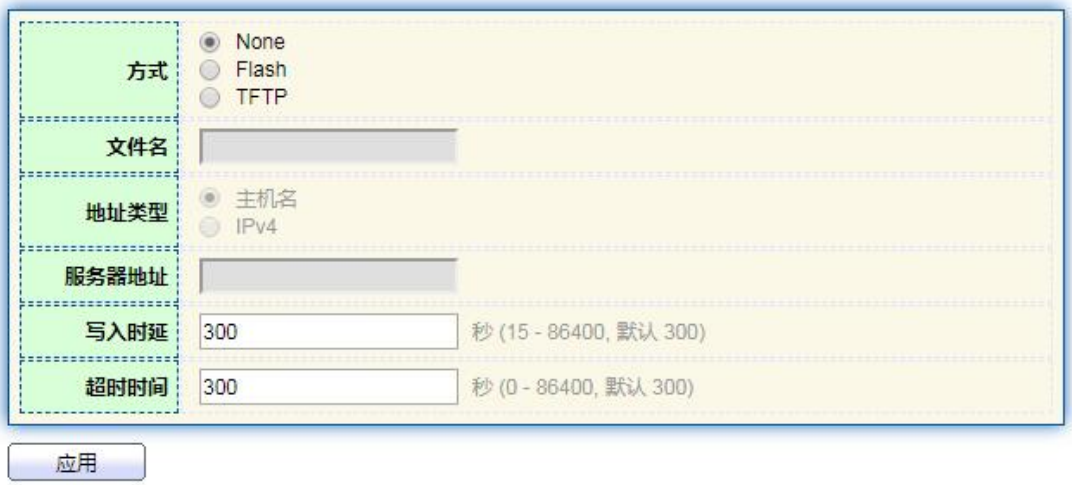
界面含义如下表所示:

配置项	说明
端口	绑定组中的端口号
VLAN	绑定的 VLAN ID
绑定	选择绑定关系，由 IPMV 和 IPV 两种
MAC 地址	绑定的 MAC 地址
IP 地址	绑定的 IP 地址

2. 填写相应的配置项，单击“应用”，完成配置。



3. 单击导航树中的“安全 > IP Source Guard > 数据库保存”菜单，如下图所示:



17 ACL

随着网络规模的扩大和流量的增加，对网络安全的控制和对带宽的分配成为网络管理的重要内容。通过对数据包进行过滤，可以有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。ACL（Access Control List，访问控制列表）即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。

当交换机的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文的字段进行分析，在识别出特定的报文之后，根据预先设定的策略允许或禁止相应的数据包通过。由 ACL 定义的数据包匹配规则，也可以被其它需要对流量进行区分的功能引用，如 QoS 中流分类规则的定义。通过设置匹配规则和操作处理，访问控制列表（ACL）可以实现数据包过滤功能。访问控制列表是适用于数据包的系列许可和拒绝条件的集合。当在接口上接收数据包时，交换机让数据包字段与所用的 ACL 相比，在访问列表中指定的标准基础上，确定数据包被许可转发。ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口号等。ACL 通过一系列 的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。根据应用目的，可将 ACL 分为以下几种：

- 基本 IP ACL（Basic IP ACL）：只根据数据包的源 IP 地址制定规则。ACL ID 范围：100~999。
- 高级 IP ACL（Advanced IP ACL）：根据数据包的源 IP 地址、目的 IP 地址、IP 承载的协议类型、协议特性等三、四层信息制定规则。ACL ID 范围：100~999。
- 二层 ACL （L2 ACL）：根据数据包的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定规则。 ACL ID 范围：1~99。

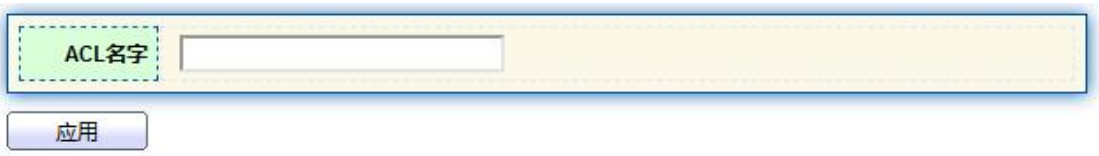
17.1 MAC ACL 配置

二层 ACL：根据源 MAC 地址、目的 MAC 地址、VLAN 优先级、二层协议类型等二层信

息制定规则。

操作步骤：

1. 单击导航树中的“ACL> MAC ACL 配置”菜单，进入“MAC ACL 配置”界面，如下图所示。



界面信息含义说明如下表所示

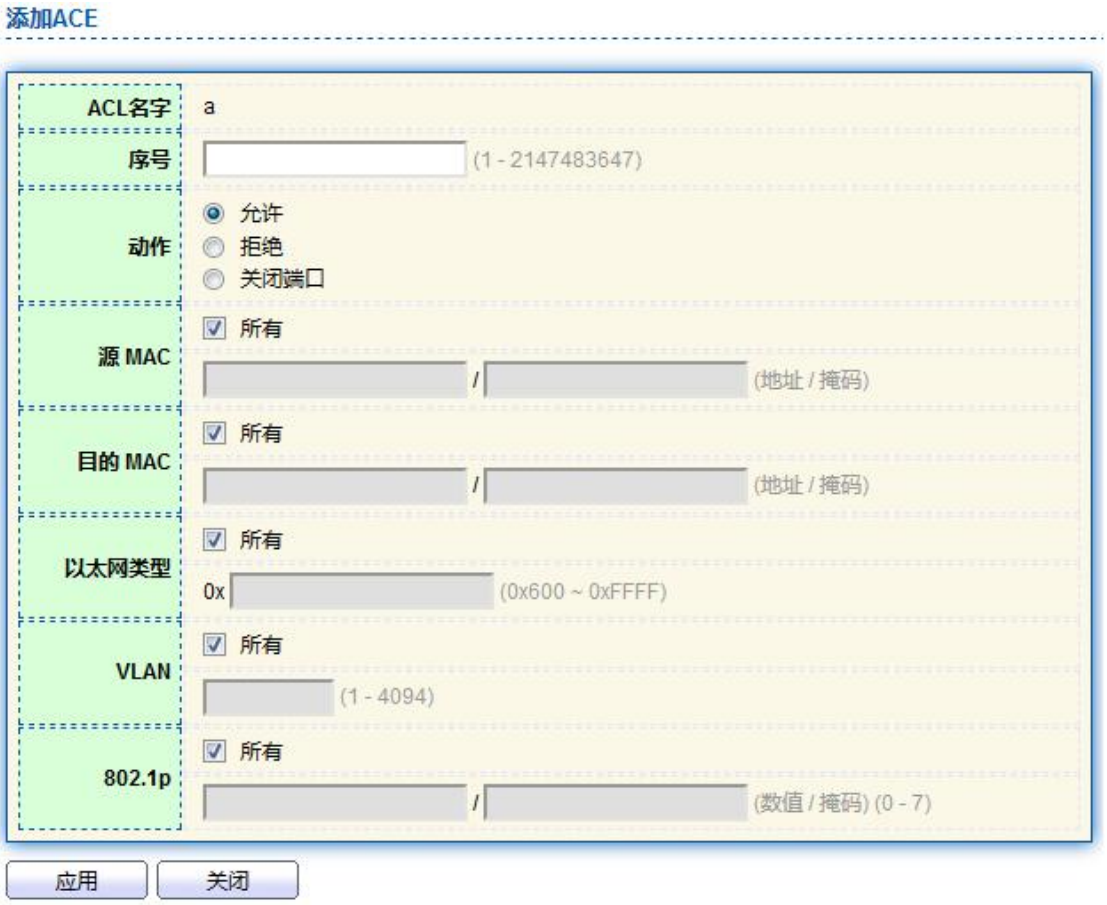
配置项	说明
ACL 名称	设置 MAC ACL 规则的名称

2. 单击导航树中的“ACL > MAC ACE 配置”菜单，选中 ACL 名称，单击“添加”如下图所示：

界面信息含义说明如下表所示

配置项	说明
ACL 名称	通过 MAC ACL 页面设置的 ACL 规则列表

3. 填写相应的配置项：



界面信息含义说明如下表所示

配置项	说明
序号	MAC ACL 取值范围是：1-2147483647
动作	ACL 动作的规则分为“Permit”（允许）规则或者“Deny”（拒绝）规则，以及“Shutdown”(关闭端口)。
源 MAC	输入 ACL 规则的源 MAC 地址和掩码。格式为 H.H.H.H.H.H。选“any”(所有)，则表示任意 MAC。
目的 MAC	输入 ACL 规则的目的 MAC 地址和掩码。格式为 H.H.H.H.H.H。选“any”(所有)，则表示任意 MAC。
以太网类型	输入 ACL 规则的以太网类型，取值范围是：0x600-0Xffff，选“any”(所有)，则表示任意以太网类型。
VLAN	输入 ACL 规则的 VLAN，取值范围是：1-4094，选“any”(所有)，则表示任意 VLAN。
802.1p	输入 ACL 规则的 VLAN 优先级和掩码，取值范围是：1-7，选“any”(所有)，则表示任意 VLAN 优先级。

4. 单击“应用”，完成配置，如图所示。

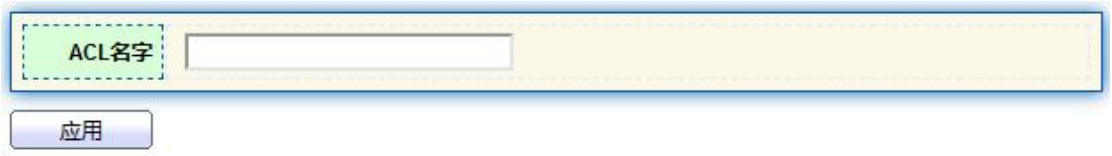
17.2 IPv4 ACL 配置

基本 IPv4 ACL（Basic IP ACL）：只根据数据包的源 IP 地址制定规则。ACL ID 范围：100~999。

高级 IP ACL（Advanced IP ACL）：根据数据包的源 IP 地址、目的 IP 地址、IP 承载的协议类型、协议特性等三、四层信息制定规则。ACL ID 范围：100~999

操作步骤

1. 单击导航树中的“ACL> IPv4 ACL 配置”菜单，进入“IPv4 ACL 配置”界面，如下图所示。



界面信息含义说明如下表所示

配置项	说明
ACL 名称	设置 IPv4 ACL 规则的名称

2. 单击导航树中的“ACL > IPv4 ACE 配置”菜单，选中 ACL 名称，单击“添加”如下图所示：

3. 填写相应的配置项：

界面信息含义说明如下表所示

配置项	说明
序号	IPv4 ACL 取值范围是：1-2147483647

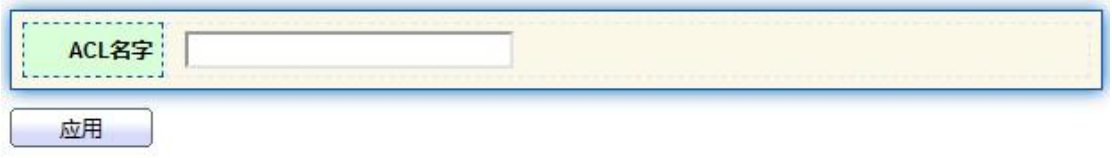
动作	ACL 动作的规则分为“Permit”（允许）规则或者“Deny”（拒绝）规则，以及“Shutdown”(关闭端口)。
协议	必选，选择协议的类型。ICMP、TCP、UDP 等，选“any”(所有)，则表示任意协议
源 IP	输入 ACL 规则的源 IP 和掩码，选“any”(所有)，则表示任意源 IP
目的 IP	输入 ACL 规则的目的 IP 和掩码，选“any”(所有)，则表示任意目的 IP
服务类型	输入 ACL 规则的服务类型，DSCP（范围 0-63）或 IP 优先级（范围 0-7），选“any”(所有)，则表示任意服务类型
源端口	输入ACL规则的源端口，单一端口号或者范围段（范围0-65535），选“any”(所有)，则表示任意源端口
目的端口	输入 ACL 规则的目的端口，单一端口号或者范围段（范围 0-65535），选“any”(所有)，则表示任意目的端口
TCP 标志位	输入 ACL 规则的 TCP 标志位， URG, Ack, PSH, RST, SYM, Fin 标志位，动作有“set”(设置)，“unset”(取消)，“Don’t care”(不作处理)
ICMP 类型	输入 ACL 规则的 ICMP 报文类型，选“any”(所有)，则表示任意 ICMP 类型
ICMP 字段	输入 ACL 规则的 ICMP 字段值，选“any”(所有)，则表示任意 ICMP 字段值

4. 单击“应用”，完成配置，如图所示。

17.3 IPv6 ACL 配置

操作步骤

1. 单击导航树中的“ACL> IPv6 ACL 配置”菜单，进入“IPv6 ACL 配置”界面，如下图所示。



界面信息含义说明如下表所示

配置项	说明
ACL 名称	设置 IPv6 ACL 规则的名称

2. 单击导航树中的“ACL > IPv6 ACE 配置”菜单，选中 ACL 名称，单击“添加”如下图所示：

3. 填写相应的配置项：

界面信息含义说明如下表所示

配置项	说明
序号	IPv6 ACL 取值范围是：1-2147483647

动作	ACL 动作的规则分为“Permit”（允许）规则或者“Deny”（拒绝）规则，以及“Shutdown”(关闭端口)。
序号	MAC ACL 取值范围是：1-2147483647
协议	必选，选择协议的类型。ICMP、TCP、UDP，选“any”(所有)，则表示任意协议
源 IP	输入 ACL 规则的源 IP 和掩码，选“any”(所有)，则表示任意源 IP
目的 IP	输入 ACL 规则的目的 IP 和掩码，选“any”(所有)，则表示任意目的 IP
服务类型	输入 ACL 规则的服务类型，DSCP（范围 0-63）或 IP 优先级（范围 0-7），选“any”(所有)，则表示任意服务类型
源端口	输入ACL规则的源端口，单一端口号或者范围段(范围0-65535)，选“any”(所有)，则表示任意源端口
目的端口	输入 ACL 规则的目的端口，单一端口号或者范围段（范围 0-65535），选“any”(所有)，则表示任意目的端口
TCP 标志位	输入 ACL 规则的 TCP 标志位，URG, Ack, PSH, RST, SYM, Fin 标志位，动作有“set”(设置)，“unset”(取消)，“Don’t care”(不作处理)
ICMP 类型	输入 ACL 规则的 ICMP 报文类型，选“any”(所有)，则表示任意 ICMP 类型
ICMP 字段	输入 ACL 规则的 ICMP 字段值，选“any”(所有)，则表示任意 ICMP 字段值

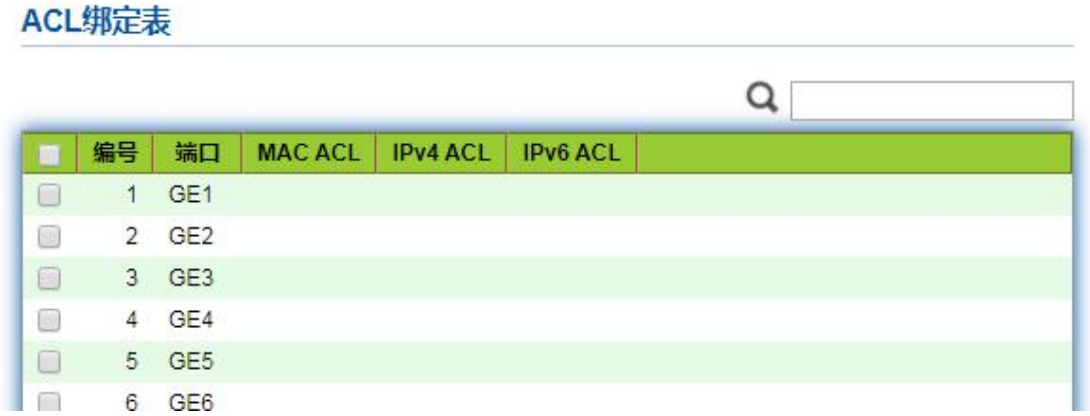
4. 单击“应用”，完成配置，如图所示。

17.4 ACL 绑定配置

创建好列表以后，接下来还必须将它绑定到每个想用它的接口上

操作步骤：

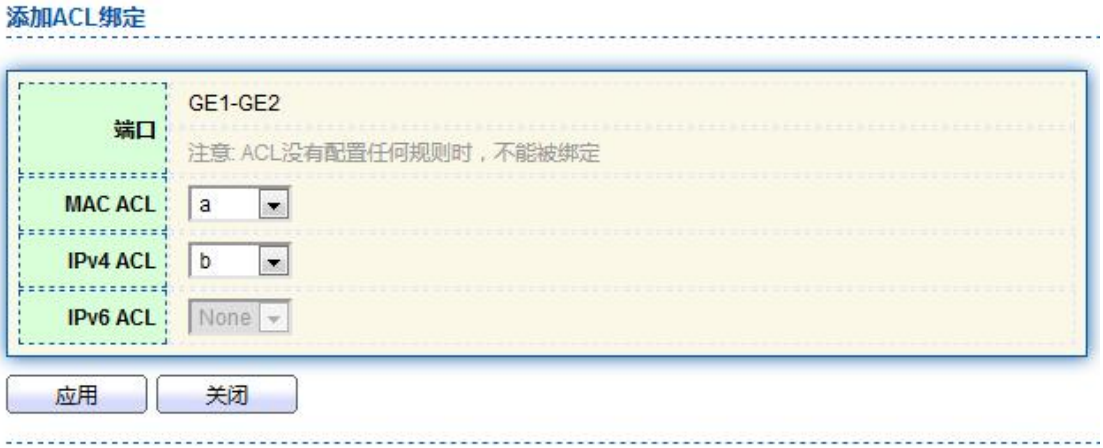
1. 单击导航树中的“ACL > ACL 绑定”菜单，进入“ACL 绑定配置”界面，如下图所示。



界面含义如下表

配置项	说明
MAC ACL	绑定到端口上 MAC ACL 名称
IPv4 ACL	绑定到端口上 IPv4 ACL 名称(与 IPv6 ACL 互斥)
IPv6 ACL	绑定到端口上 IPv6 ACL 名称(与 IPv4 ACL 互斥)

2. 填写相应的配置项，以创建好的 MAC ACL a, IPv4 ACL b, IPv6 ACL c 为例子.
3. 单击“应用”，完成配置，如图所示。



18 QoS

QoS（Quality of Service）用于评估服务方满足客户服务需求的能力，在 Internet 中，QoS 用于评估网络传送分组的服务能力。由于网络提供的服务是多样的，因此可以基于不同方面进行评估。通常所说的 QoS，是对分组投递过程中可为带宽、时延、时延抖动、丢包率等核心需求提供支持的服务能力的评估。带宽，又可称为吞吐量，表示一定时间内业务

流的平均速率，单位通常是 Kbit/s。时延，表示业务流穿过网络时需要的平均时间。对于网络中的一个设备来说，一般将时延的需求理解为几种等级。例如分为两种时延等级，通过优先队列的调度方法使得高优先级的业务尽可能快地获得服务，而低优先级的业务则需要等待没有高优先级业务时才能获得服务。时延抖动，表示业务流穿过网络的时间的变化。丢包率，表示业务流在传送过程中的丢失比率。由于现代的传输系统具有很高的可靠性，信息的丢失往往发生在网络出现拥塞时。最常见的情况是队列溢出导致分组丢失。在传统的 IP 网络中，所有的报文都被无区别的等同对待，每个网络设备对所有的报 文均采用先入先出的策略进行处理，尽最大的努力（Best-Effort）将报文送到目的地，但对报文传送的可靠性、传送延迟等性能不提供任何保证。

网络发展日新月异，随着 IP 网络上新应用的不断出现，对 IP 网络的服务质量也提出了新的要求。例如 VoIP 和视频等时延敏感业务对报文的传输时延提出了较高要求。如果报文传送延时太长，将是用户所不能接受的。为了支持具有不同服务需求的语音、视频以及数据等业务，要求网络能够区分出不同的业务类型，进而为之提供相应的服务。

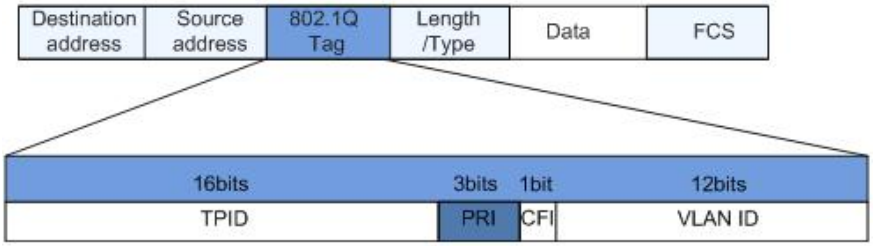
传统 IP 网络的尽力服务不可能识别和区分出网络中的各种业务类型，而具备业务类型的区分能力正是为不同的业务提供差异化服务的前提，所以传统网络的尽力服务模式已不能满足应用的需要。QoS 技术的出现便致力于解决这个问题。QoS 可以对网络流量进行调控，避免并管理网络拥塞，减少报文丢包率。同时支持为用户提供专用带宽，为不同业务提供不同的服务质量等，完善了网络的服务能力。

不同的报文使用不同的 QoS 优先级，例如 VLAN 报文使用 802.1p，或称 CoS（Class of Service）字段，IP 报文使用 DSCP。当报文经过不同网络时，为了保持报文的优先级，需要在连接不同网络的网关处配置这些优先级字段的映射关系。

VLAN 帧头中的 802.1p 优先级

通常二层设备之间交互 VLAN 帧。根据 IEEE 802.1Q 定义，VLAN 帧头中的 PRI 字段（即 802.1p 优先级），或称 CoS（Class of Service）字段，标识了服务质量需求。

VLAN 帧中的 802.1p 优先级

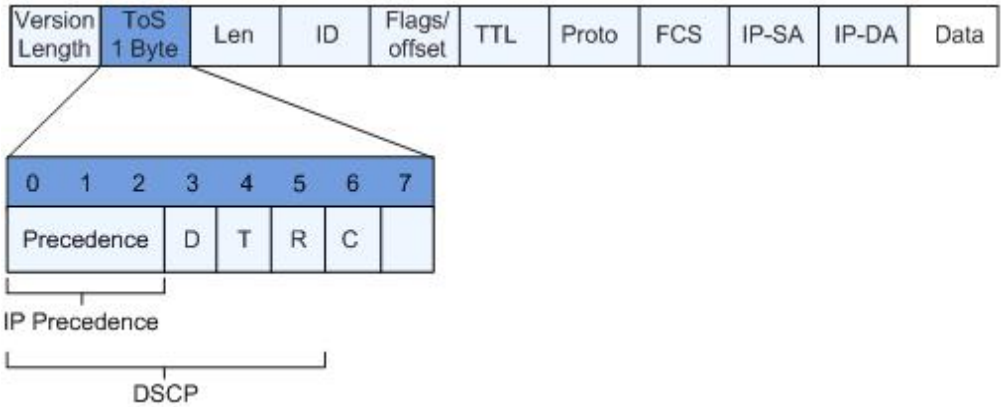


在 802.1Q 头部中包含 3 比特长的 PRI 字段。PRI 字段定义了 8 种业务优先级 CoS，按照优先级从高到低顺序取值为 7、6、……、1 和 0。

IP Precedence/DSCP 字段

根据 RFC791 定义，IP 报文头 ToS（Type of Service）域由 8 个比特组成，其中 3 个比特的 Precedence 字段标识了 IP 报文的优先级，Precedence 在报文中的位置如图所示。

IP Precedence/DSCP 字段



比特 0 ~ 2 表示 Precedence 字段，代表报文传输的 8 个优先级，按照优先级从高到低顺序取值为 7、6、……、1 和 0。最高优先级是 7 或 6，经常是为路由选择或更新网络控制通信保留的，用户级应用仅能使用 0 级 ~ 5 级。除了 Precedence 字段外，ToS 域中还包括 D、T、R 三个比特：D 比特表示延迟要求（Delay，0 代表正常延迟，1 代表低延迟）。T 比特表示吞吐量（Throughput，0 代表正常吞吐量，1 代表高吞吐量）。R 比特表示可靠性（Reliability，0 代表正常可靠性，1 代表高可靠性）。ToS 域中的比特 6 和 7 保留。

RFC1349 重新定义了 IP 报文中的 ToS 域，增加了 C 比特，表示传输开销（Monetary Cost）。之后，IETF DiffServ 工作组在 RFC2474 中将 IPv4 报文头 ToS 域中的比特 0 ~ 5 重新定义为 DSCP，并将 ToS 域改名为 DS（Differentiated Service）字节。DSCP 在报文中的位置如上图所示。DS 字段的前 6 位（0 位 ~ 5 位）用作区分服务代码点 DSCP（DS Code Point），高 2 位（6 位、7 位）是保留位。DS 字段的低 3 位（0 位 ~ 2 位）是类选择代码点 CSCP（Class Selector Code Point），相同的 CSCP 值代表一类 DSCP。DS 节点根据 DSCP 的值选择相应的 PHB（Per-Hop Behavior）。

18.1 基本功能

18.1.1 功能配置

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。拥塞管理一般采用队列调度技术来避免网络中间歇性的出现拥塞现象。队列调度技术有：SP（Strict-Priority，严格优先级队列）、WFQ（Weighted Fair Queue，加权公平队列）和 WRR（Weighted Round Robin，加权轮询队列）、DRR 调度（DRR（Deficit Round Robin）调度同样也是 RR 的扩展）。

配置全局和接口调度类型操作步骤

1. 单击导航树中的“QoS> 基本功能> 功能配置”菜单，进入“功能配置”界面，如下图所示。

全局配置界面含义如下表

配置项	说明
状态	全局 QOS 功能开关。
信任	信任模式分 CoS, DSCP, CoS-DSCP，IP 优先级 4 种

端口配置界面含义如下表

配置项	说明
CoS	范围 0-7
端口信任	端口 QOS 功能开关
CoS	标记 CoS 字段
DSCP	标记 DSCP 字段
IP 优先级	标记 IP 优先级字段

18.1.2 队列调度

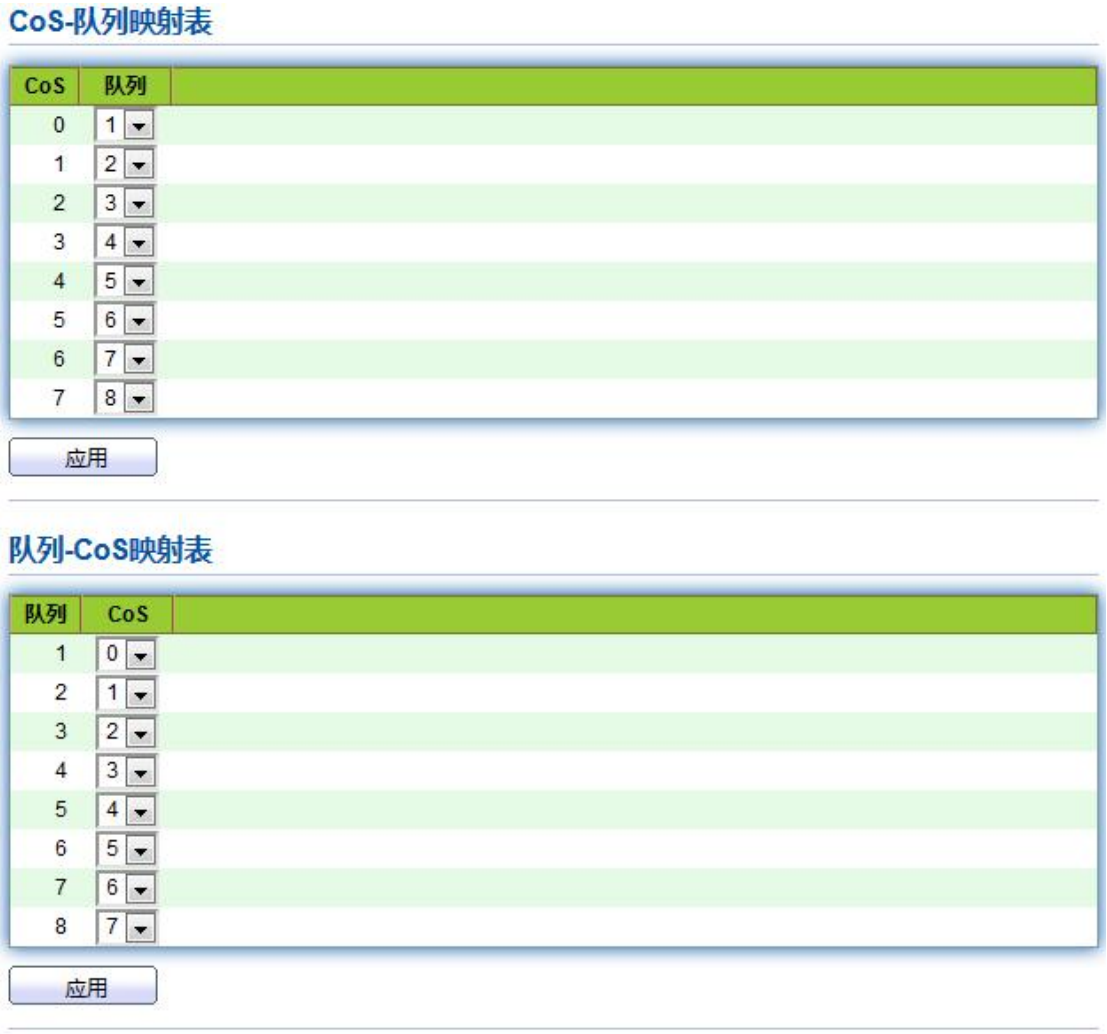
1. 单击导航树中的“QoS> 队列调度”菜单，进入“队列调度”界面，单击“应用”，完成配置，如下图所示。

界面含义如下表

配置项	说明
严格优先级（SP）	严格优先级模式
WRR	加权轮询模式
权重	队列占 WRR 的带宽比例

18.1.3 CoS 映射

1. 单击导航树中的“QoS > 基本功能 > CoS 映射”菜单，进入“CoS 映射”界面，，单击“应用”，完成配置，如下图所示。



界面含义如下表

配置项	说明
COS	802.1P COS 优先级：0-7
队列	端口队列：1-8

18.1.4 DSCP 映射

1. 单击导航树中的“QoS > 基本功能 > DSCP 映射”菜单，进入“DSCP 映射”界面，，单击“应用”，完成配置，如下图所示。

DSCP-队列映射表

DSCP	队列	DSCP	队列	DSCP	队列	DSCP	队列
0 [CS0]	1	16 [CS2]	3	32 [CS4]	5	48 [CS6]	7
1	1	17	3	33	5	49	7
2	1	18 [AF21]	3	34 [AF41]	5	50	7
3	1	19	3	35	5	51	7
4	1	20 [AF22]	3	36 [AF42]	5	52	7
5	1	21	3	37	5	53	7
6	1	22 [AF23]	3	38 [AF43]	5	54	7
7	1	23	3	39	5	55	7
8 [CS1]	2	24 [CS3]	4	40 [CS5]	6	56 [CS7]	8
9	2	25	4	41	6	57	8
10 [AF11]	2	26 [AF31]	4	42	6	58	8
11	2	27	4	43	6	59	8
12 [AF12]	2	28 [AF32]	4	44	6	60	8
13	2	29	4	45	6	61	8
14 [AF13]	2	30 [AF33]	4	46 [EF]	6	62	8
15	2	31	4	47	6	63	8

应用

队列-DSCP映射表

队列	DSCP
1	0 [CS0]
2	8 [CS1]
3	16 [CS2]
4	24 [CS3]
5	32 [CS4]
6	40 [CS5]
7	48 [CS6]
8	56 [CS7]

应用

界面含义如下表

配置项	说明
DSCP	IP 报文头 DSCP 域的优先级：0-63
队列	端口队列：1-8

18.1.5 IP 优先级映射

1. 单击导航树中的“QOS > 基本功能 > IP 优先级映射”菜单，进入“IP 优先级映射”界面，，单击“应用”，完成配置，如下图所示。

界面含义如下表

配置项	说明
IP 优先级	IP 报文头 TOS 域优先级：0-7
队列	端口队列：1-8

18.2 带宽限速

18.2.1 端口限速

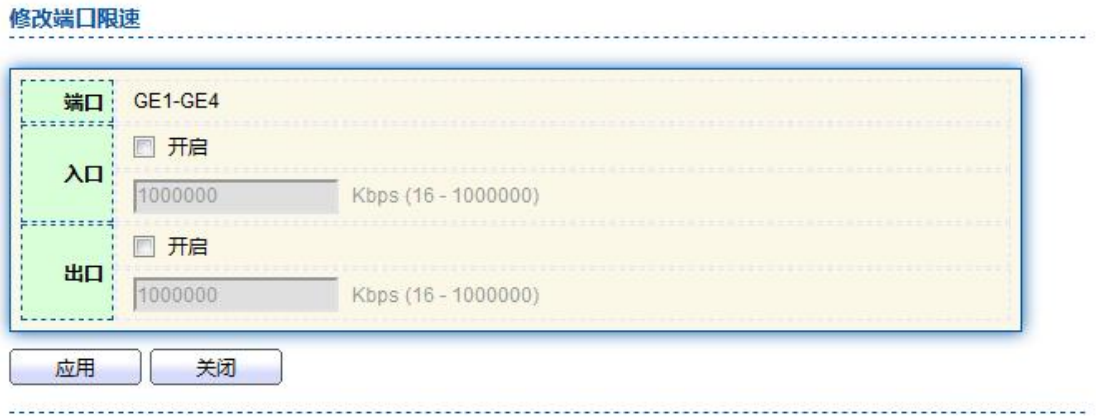
配置接口限速就是限制物理接口向外发送或向内接收数据的速率。在流量从接口发出前，在

接口的出方向上配置限速，对流出的所有报文流量进行控制。在流量从接口接收前，在接口的入方向上配置限速，对流入的所有报文流量进行控制。

操作步骤：

1. 单击导航栏中“QoS > 带宽限速 > 端口限速”菜单，进入端口限速配置页面，页面中可以选择限速端口，查看当前限速配置，如下图：

2. 选择需要限速的端口，可以多选，然后点击页面下方的修改按钮，进入修改页面，配置开启和关闭限速功能，指定限速速率，配置完成后应用保存，页面如下：



配置参数说明

配置项		说明
入口	开启	入方向的限速开关
	速率	入方向的限速速率，范围是 16-1000000(Kbps)
出口	开启	出方向的限速开关
	速率	出方向的限速速率，范围是 16-1000000(Kbps)

18.2.2 出口队列限速

配置和查看出口队列限速

1. 单击导航栏中“QoS > 带宽限速 > 出口队列限速”菜单进入界面，如下图所示：

出口队列表

	编号	端口	队列 1		队列 2		队列 3		队列 4		队列 5		队列 6		队列 7		队列 8	
			状态	平均速率(Kbps)	状态	平均速率(Kbps)	状态	平均速率(Kbps)	状态	平均速率(Kbps)	状态	平均速率(Kbps)	状态	平均速率(Kbps)	状态	平均速率(Kbps)	状态	平均速率(Kbps)
	1	GE1	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	
	2	GE2	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	
	3	GE3	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	
	4	GE4	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	
	5	GE5	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	
	6	GE6	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	
	7	GE7	禁用		禁用		禁用		禁用		禁用		禁用		禁用		禁用	

2. 选择端口，点击“修改”进入端口队列配置界面，如下图所示：

修改出口队列

19 设备诊断

19.1 日志功能

日志配置可以配置设备的日志开关，日志信息合并，日志老化时间，配置日志等级，以及将交换机工作日记上传到 TFTP 服务器上。

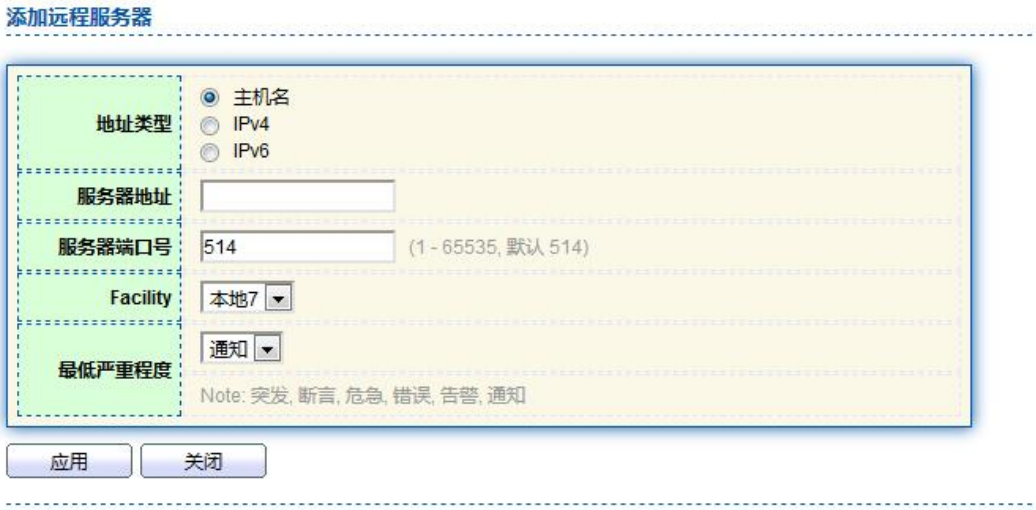
19.1.1 功能配置

操作步骤:

1. 单击导航栏中“设备诊断 > 日志功能 > 功能配置”菜单，进入日志功能配置页面，可以选择开启关闭日志，选择日志输出终端，配置日志严重等级等功能，界面如下:

2. 单击导航栏中“设备诊断 > 日志功能 > 远程服务器配置”菜单，进入日志远程服务器配置页面，此页面可以添加和查看远程日志服务器配置，界面如下:

3. 点击添加按钮可以新增远程日志服务器，修改按钮可以修改选中的日志服务器配置，修改完成后，点击“应用”按钮保存。界面如下：



19.2 Ping

Ping 命令用来检查指定的 IP 地址、主机名是否可达，并输出相应的统计信息。

操作步骤：

1. 单击导航栏中“设备诊断 > Ping”菜单，输入主机名或 IP 地址，输入测试次数，如下图所示：

2. 单击“Ping”，系统会进行发包测试，验证地址是否可以到达，并输出测试结果，如下图所示：

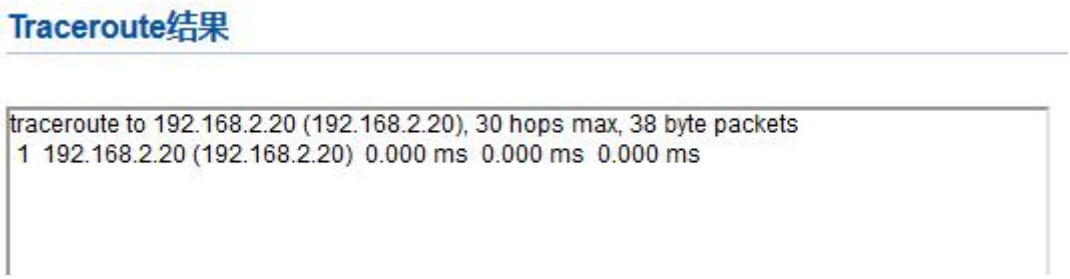
19.3 Traceroute

Traceroute 通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。

操作步骤：

1. 单击导航栏中“设备诊断 > Traceroute”菜单，输入主机名或 IP 地址，可以定义报文生存时间，如下图所示：

2. 单击“应用”，系统开始测试，等待测试完成，输出测试结果，如下图所示：

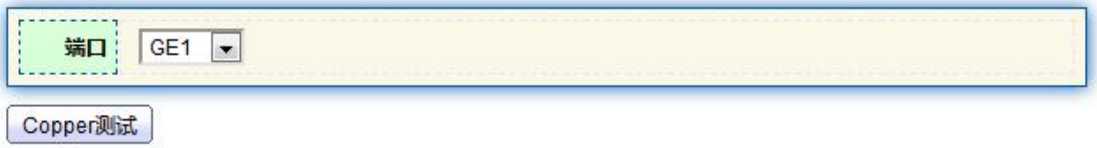


19.4 电口测试

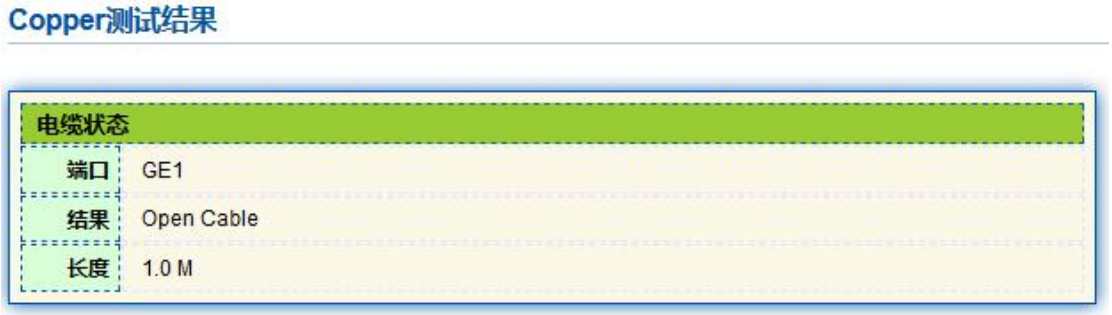
电口测试功能，通过反射电压强度来判断端口接入的网线当前状态，并定位网线故障长度位置(误差 5M 左右)。

操作步骤：

1. 单击导航栏中“设备诊断 > 电口测试”菜单，选择需要测试的端口，如下图所示：



2. 单击“Copper 测试”，系统开始测试，等待测试完成，输出测试结果，如下图所示：



19.5 光模块信息

查看光模块 DDM 信息

操作步骤：

1. 单击导航栏中“设备诊断 > 光模块信息”菜单进入界面，如下图所示：

19.6 UDLD 协议

UDLD（Unidirectional Link Detection，单向链路检测）：是一种 Cisco 专用第二层协议，用于监控光纤或双绞线连接的以太网链路的物理配置。当出现单向链接时（它只能向一个方向传输，例如，我可以向您发送数据，您也可以接收，但我无法接收您发送给我的数据），UDLD 可以检测到这种情况，关闭相应的接口并向其发送警告消息。单向链接可能会导致许多问题，特别是生成树，这可能会导致环回。注意：UDLD 需要链路两端的设备支持才能正常运行。

19.6.1 功能配置

配置和查看全局和端口开关配置

操作步骤：

1. 单击导航树中的“设备诊断> UDLD 协议 > 功能配置”菜单进入界面，如下图所示：

2. 选择端口，点击“修改”进入端口配置界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
端口	端口列表
模式	关闭：禁用端口功能 普通：UDLD 可以检测单向链接并将端口标记为未确定，以生成系统日志 主动：UDLD 可以检测单向链路。它将尝试重建链接并连续 8 秒发送 UDLD 消息。如果没有 UDLD echo 响应，端口将处于 errdisable 状态

19.6.2 邻居信息

UDLD 定期在每个活动接口上发送 HELLO 包（也称为播发或探测）。当交换机接收到 Hello 数据包时，消息将一直存储到过期时间。当在老化时间到期之前再次收到 Hello 时，老化时间被刷新。当新邻居或邻居请求重新同步缓存时，会发送一系列 UDLD probe/echo（Hello）数据包。

操作步骤：

1. 单击导航树中的“设备诊断> UDLD 协议 > 邻居信息”菜单进入界面，如下图所示：

界面信息含义如下表所示。

查询项	说明
编号	序号编号
Expiration Time	剩余老化时间
当前邻居状态	邻居的状态
设备 ID	邻居的设备 ID
设备名	邻居的设备名称
端口号	连接接口的 ID
消息间隔	邻居的消息间隔
超时时间	邻居的超时时间

20 设备管理

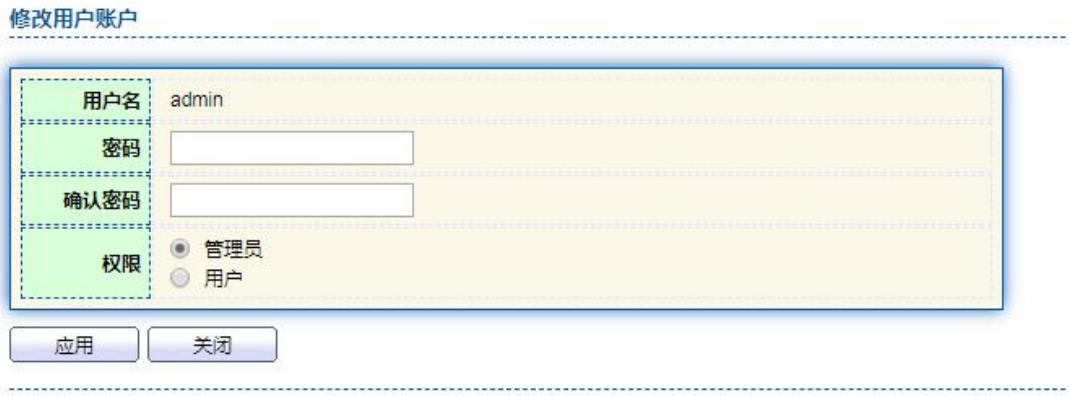
20.1 用户配置

用户可以查看交换机当前的用户名、密码以及权限，用户可以修改用户名、密码以及权限。

操作步骤：

1. 单击导航栏中“设备管理 > 用户配置”菜单，可以看到默认用户名：admin，权限：为管理员。如下图所示：

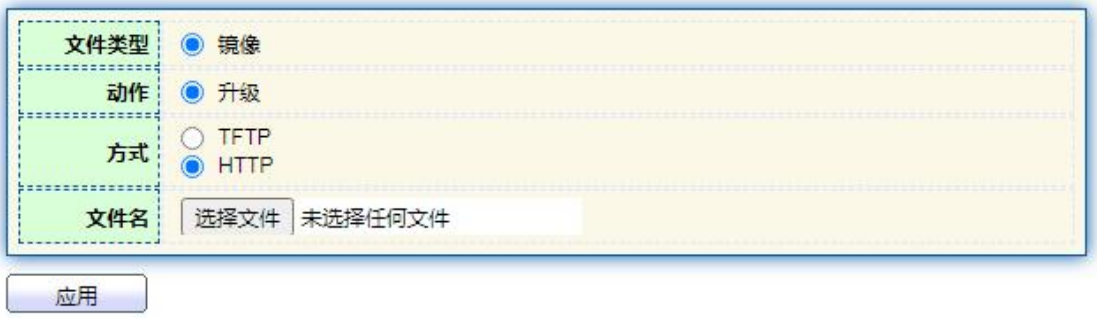
2. 点击添加按钮，添加用户账户，点击修改按钮，修改选择的用户属性，新增和修改界面如下图：



20.2 固件管理

操作步骤:

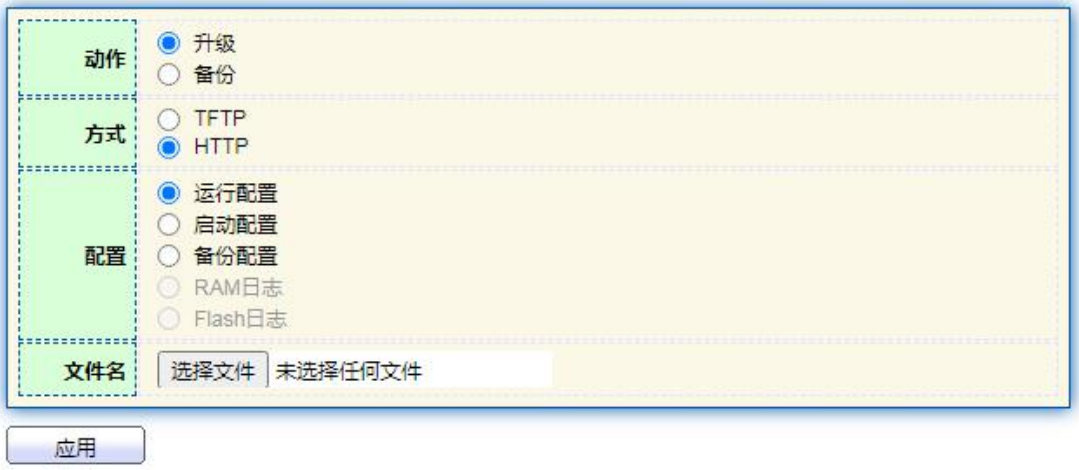
1. 单击导航树中的“设备管理 > 固件管理 > 升级”菜单，进入“升级”界面，可选方式“TFTP”或“HTTP”，选择需要升级的系统文件(xx.bix)。单击“应用”，如下图所示。



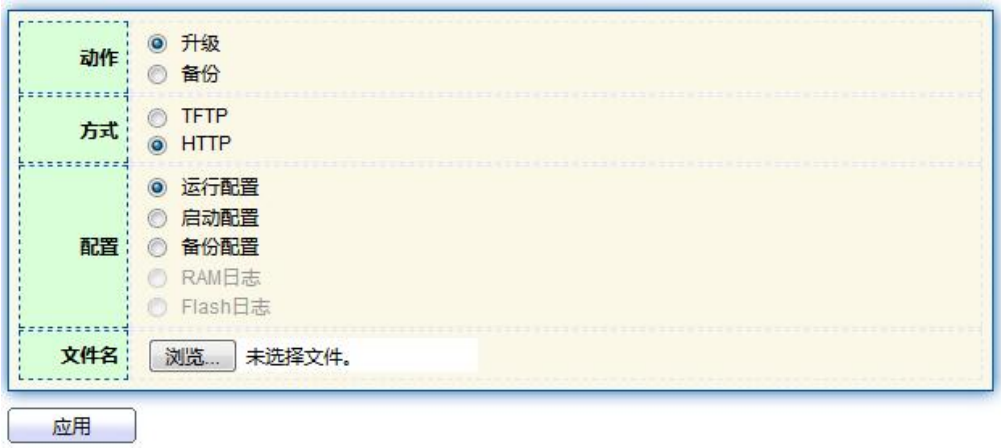
20.3 配置管理

20.3.1 升级

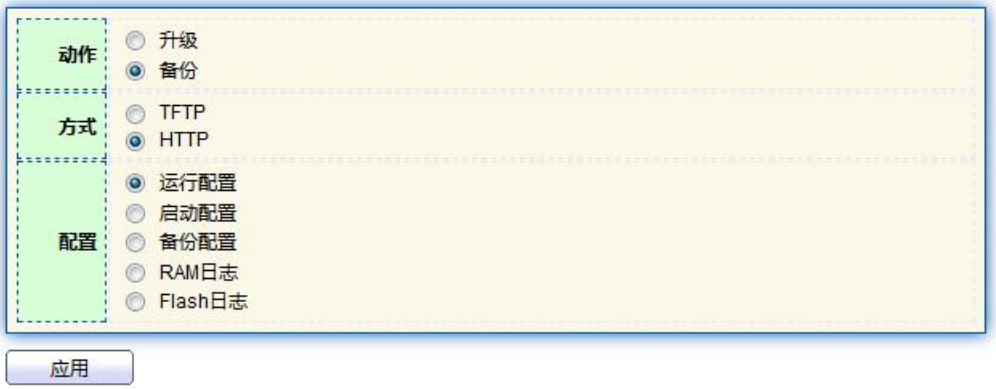
1. 单击导航树中的“设备管理 > 配置管理 > 升级”菜单，进入“升级/备份”界面，如下图所示。



2. 升级配置文件操作步骤，勾选“升级”，选项升级方式“TFTP”或“HTTP”，选择需要升级的配置文件（TFTP 方式需要填写相应服务器），选择相应的配置文件。单击“应用“，如下图所示。



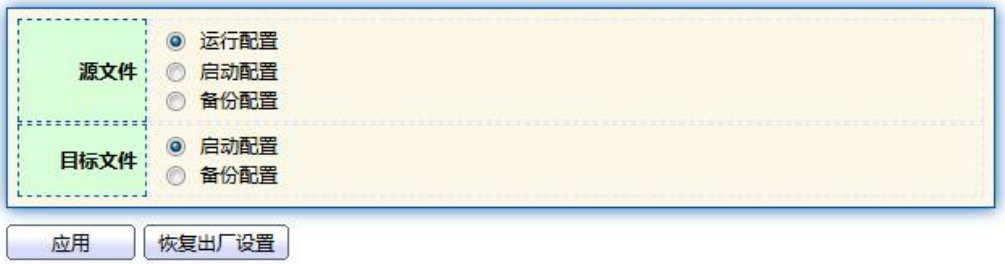
3. 备份配置文件操作步骤，选择“备份”，选项下载方式“TFTP”或“HTTP”，选择需要下载的配置文件或者日志（TFTP 方式需要填写相应服务器）。单击“应用”，如下图所示。



20.3.2 保存配置

操作方法:

1. 单击导航树中的“设备管理 > 配置管理 > 保存配置”菜单，进入“保存配置”界面，选择需要保存的源文件和目标文件，单击“应用”，完成保存，单击“恢复出厂设置”，可将配置恢复成出厂设置，如下图所示。



注意:

- 单击“恢复出厂设置”，需要再单击“重启设备”，设备才会回到出厂设置状态。
- “运行配置”可保存成“启动配置”或“备份配置”，“备份配置”可保存成“启动配置”或“运行配置”，“启动配置”可保存成“备份配置”或“运行配置”。

2. 单击页面右上角“保存”，按提示可将运行配置保存为启动配置，，如下图所示。

20.4 SNMP 配置

简单网络管理协议 SNMP(Simple Network Management Protocol)是广泛应用于 TCP/IP 网络的网络管理标准协议。SNMP 提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站）来管理设备的方法。

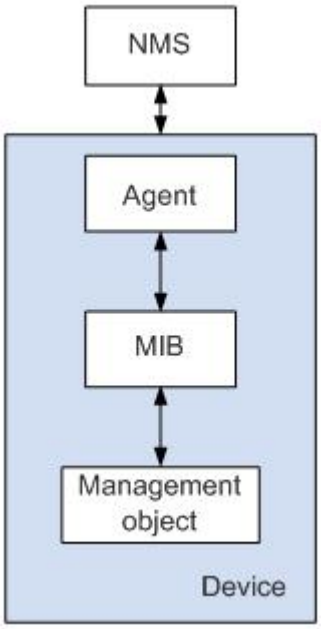
SNMP 的特点如下:

- 简单：SNMP 采用轮询机制，提供最基本的功能集，适合小型、快速、低价格的环境使用，而且 SNMP 以 UDP 报文为承载，因而受到绝大多数设备的支持。
- 强大：SNMP 的目标是保证管理信息在任意两点传送，以便于管理员在网络上的任何节点检索信息，进行修改和排查故障。

SNMP 协议应用较广的主要有 3 个版本，分别为 SNMPv1、SNMPv2c 和 SNMPv3。SNMP 系统包括网络管理系统 NMS（Network Management System）、代理进程 Agent、被管对象 Management object 和管理信息库 MIB（Management Information Base）四部分组成。

NMS 作为整个网络的网管中心，对设备进行管理。每个被管理设备中都包含驻留在设备上的 Agent 进程、MIB 和多个被管对象。NMS 通过与运行在被管理设备上的 Agent 交互，由 Agent 通过对设备端的 MIB 的操作，完成 NMS 的指令。

SNMP 管理模型



NMS

NMS 在网络中扮演管理者角色，是一个采用 SNMP 协议对网络设备进行管理/监视的系统，运行在 NMS 服务器上。NMS 可以向设备上的 Agent 发出请求，查询或修改一个或多个具体的参数值。NMS 可以接收设备上的 Agent 主动发送的 Trap 信息，以获知被管理设备当前的状态。

Agent

Agent 是被管理设备中的一个代理进程，用于维护被管理设备的信息数据并响应来自

NMS 的请求，把管理数据汇报给发送请求的 NMS。Agent 接收到 NMS 的请求信息后，通过 MIB 表完成相应指令后，并把操作结果响应给 NMS。当设备发生故障或者其它事件时，设备会通过 Agent 主动发送信息给 NMS，向 NMS 报告设备当前的状态变化。

Management object

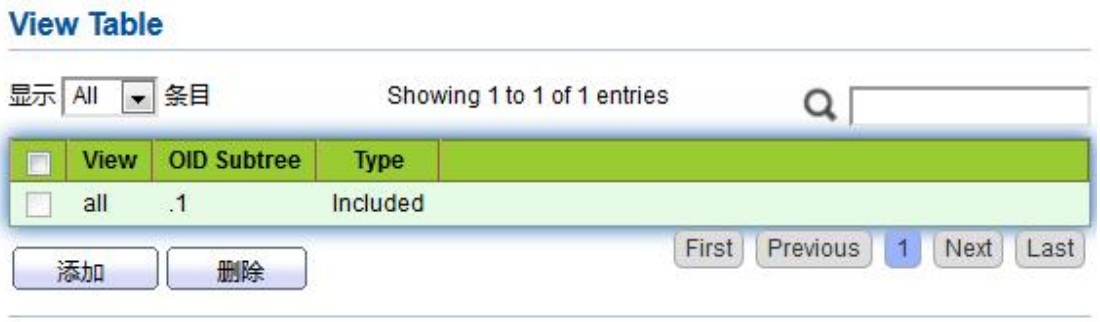
Management object 指被管理对象。每一个设备可能包含多个被管理对象，被管理对象可以是设备中的某个硬件（如一块接口板），也可以是某些硬件，软件（如路由选择协议）及其的配置参数的集合。

MIB

MIB 是一个数据库，指明了被管理设备所维护的变量（即能够被 Agent 查询和设置的信息）。MIB 在数据库中定义了被管理设备的一系列属性：对象的名称、对象的状态、对象的访问权限和对象的数据类型等。通过 MIB，可以完成以下功能：Agent 通过查询 MIB，可以获知设备当前的状态信息。Agent 通过修改 MIB，可以设置设备的状态参数。

20.4.1 视图配置

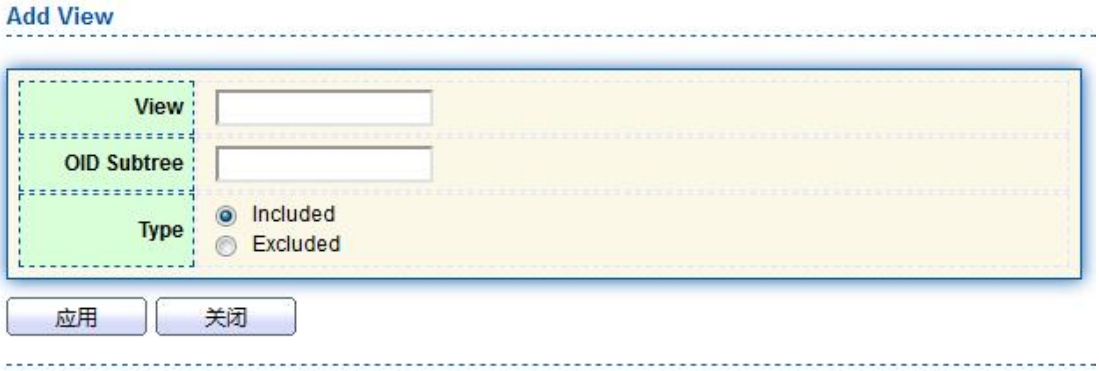
1. 单击导航树中的“设备管理 > SNMP 配置 > 视图配置”菜单，进入“视图配置”界面，如下图所示。



界面含义如下表

配置项	说明
View	视图名
OID	视图 OID
type	视图类型，“Included”或“Excluded”

2. 单击“添加”，填写相应配置，单击“应用”，完成配置。



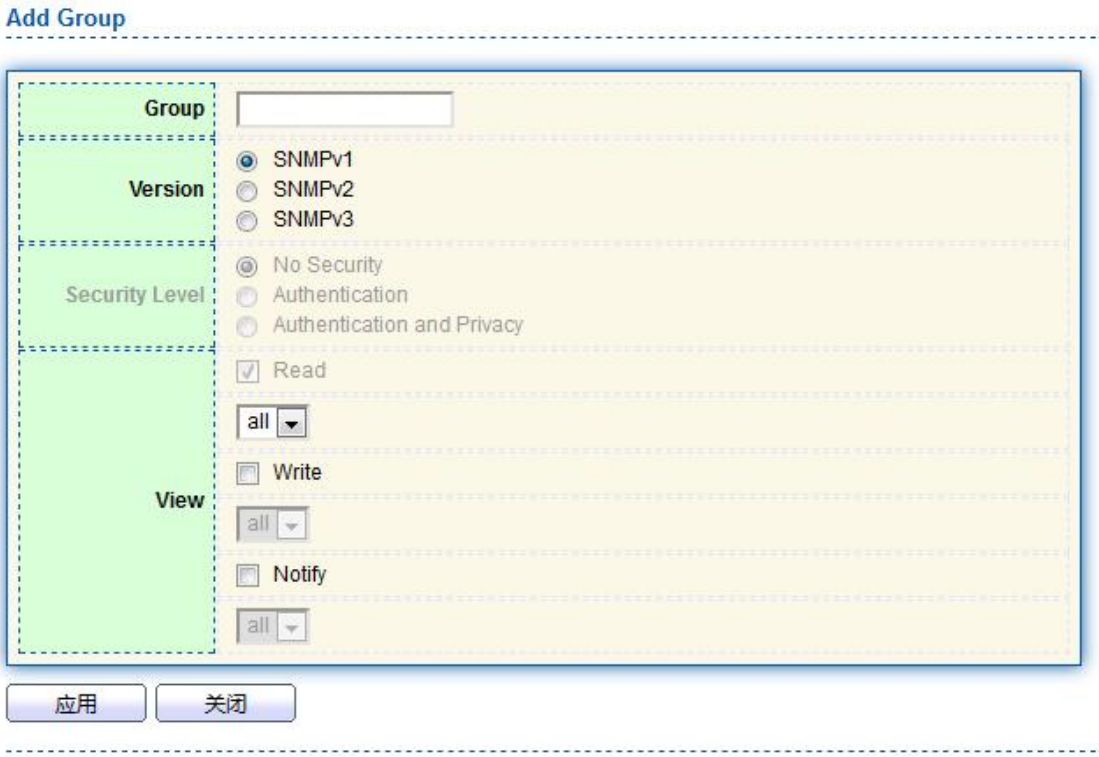
20.4.2 组配置

1. 单击导航树中的“设备管理 > SNMP 配置 > 组配置”菜单，进入“组配置”界面，如下图所示。

界面含义如下表

配置项	说明
Group	组名
Version	版本，v1,v2,v3
Security Level	安全级别
View	视图,分为读视图，写视图，通知视图

2. 单击“添加”，填写相应配置，单击“应用”，完成配置。



20.4.3 团体配置

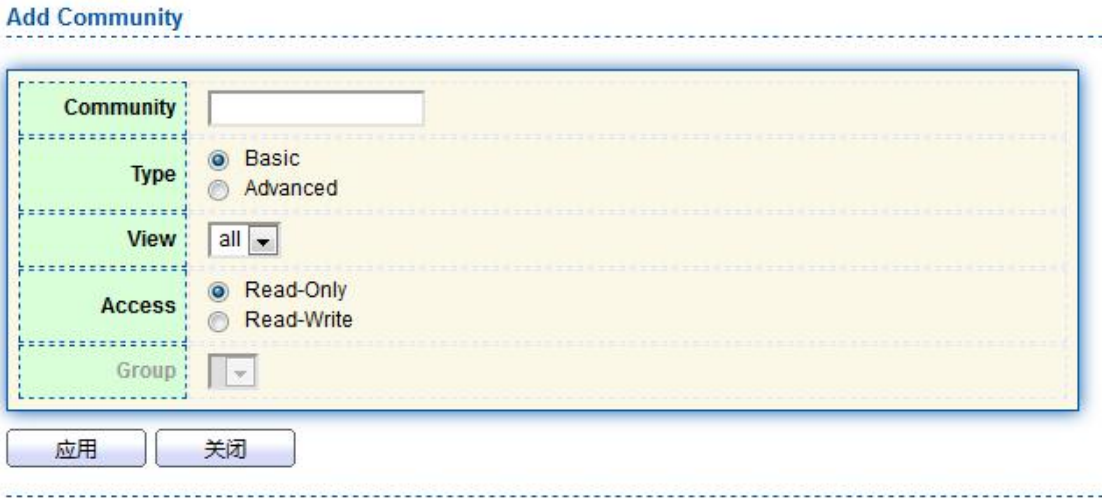
1.单击导航树中的“设备管理 > SNMP 配置 > 团体配置”菜单，进入“团体配置”界面，如下图所示。

界面含义如下表

配置项	说明
Community	团体名
Group	组名
View	视图名

Access	权限，“只读”或“读写”。

2. 单击“添加”，填写相应配置，单击“应用”，完成配置。



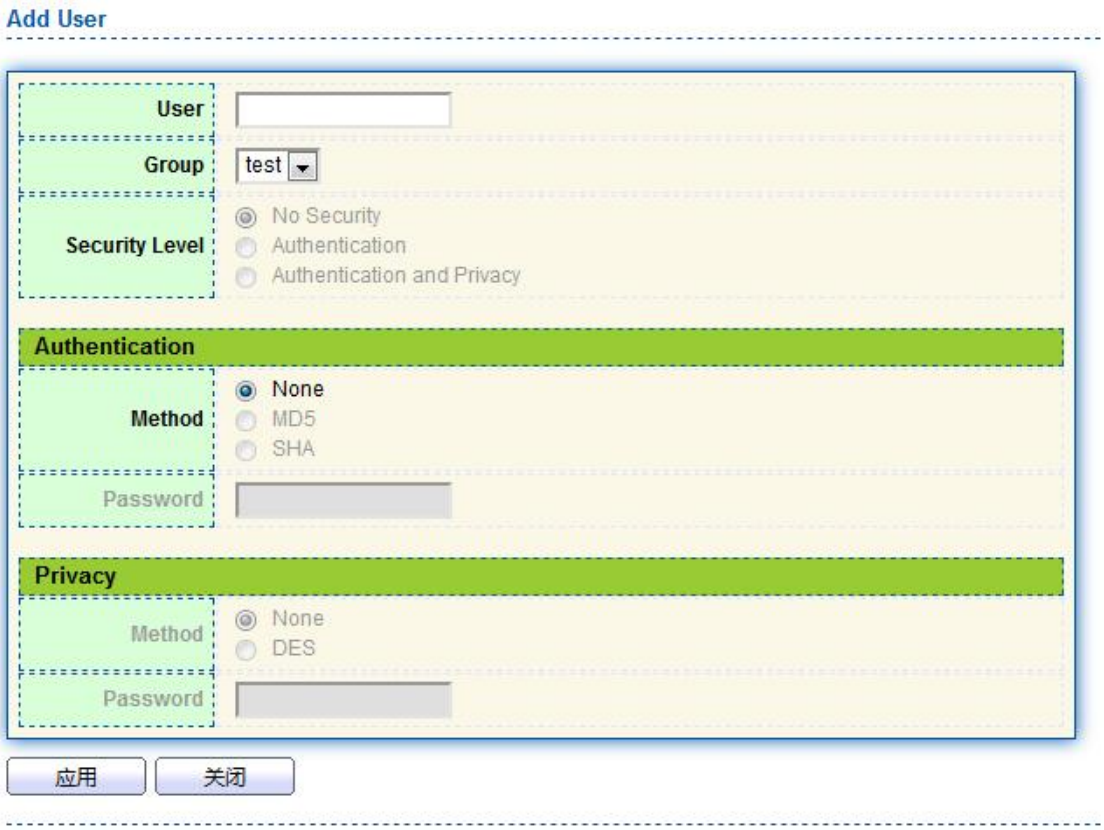
20.4.4 用户配置

1. 单击导航树中的“设备管理 > SNMP 配置 > 用户配置”菜单，进入“用户配置”界面，如下图所示。

界面含义如下表

配置项	说明
User	用户名
Group	组名
Security Level	安全级别
Authentication	认证模式
Privacy Method	加密模式

2. 单击“添加”，填写相应配置，单击“应用”，完成配置。



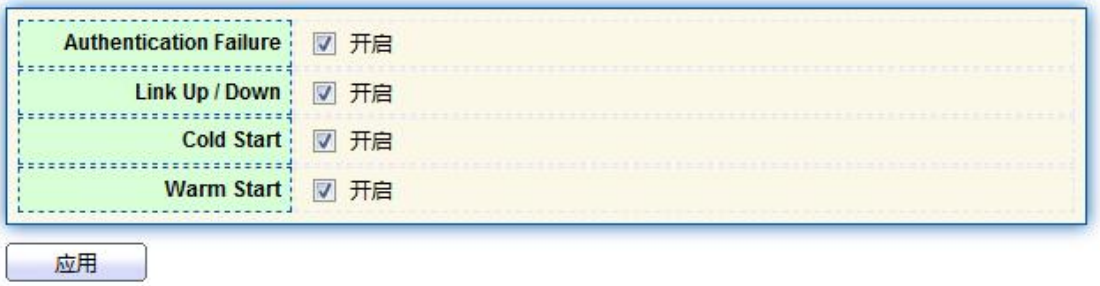
20.4.5 Engine ID 配置

1. 单击导航树中的“设备管理 > SNMP 配置 > Engine ID 配置”菜单，进入“Engine ID 配置”界面，如下图所示。

2. 选择“用户自动义”，填写相应 ID 值，单击“应用”，完成配置。

20.4.6 Trap 配置

1. 单击导航树中的“设备管理 > SNMP 配置 > Trap 配置”菜单，进入“Trap 配置”界面，如下图所示。



界面含义如下表

配置项	说明
Authentication Failure	认证错误
Link Up/Down	端口 Link Up/Down 事件
Cold start	冷启动
Warm start	热启动

2. 单击“应用”，完成配置。

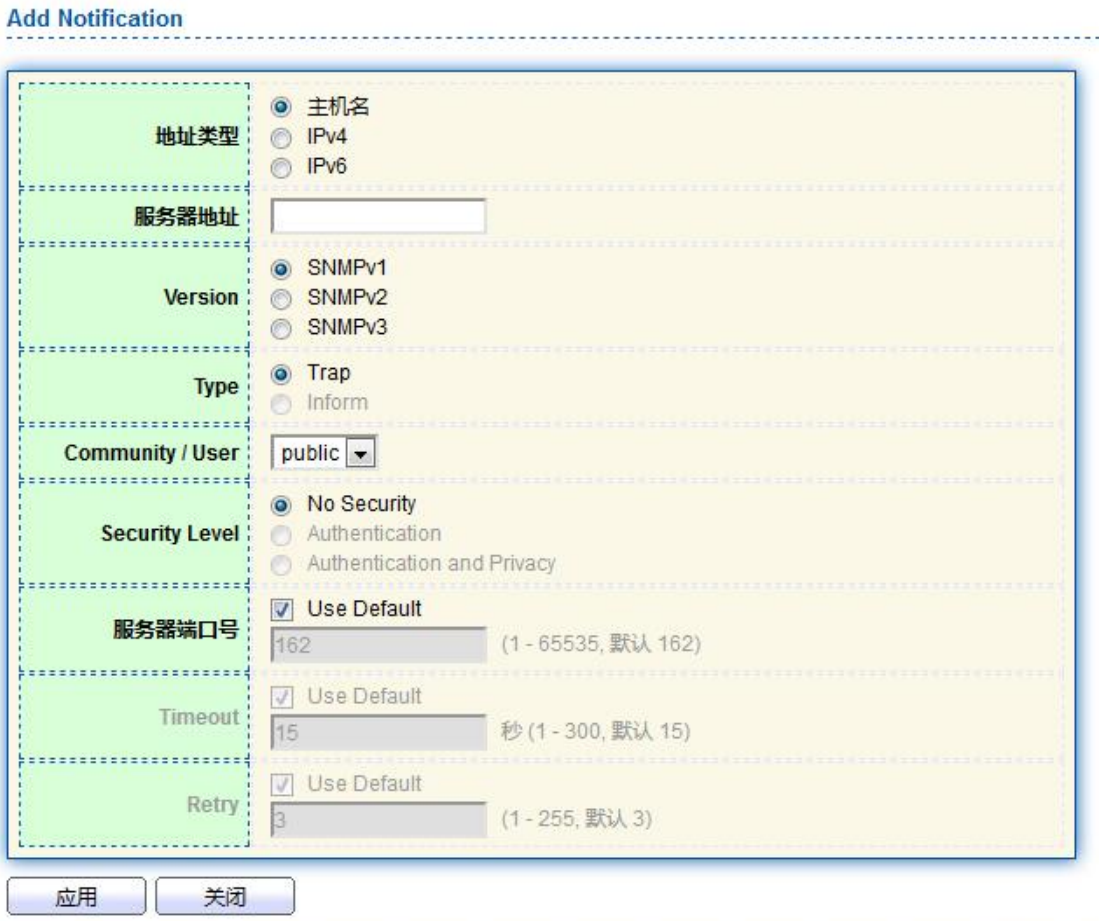
20.4.7 Notification 配置

1. 单击导航树中的“设备管理 > SNMP 配置 > Notification 配置”菜单，进入“Notification 配置”界面，如下图所示。

界面含义如下表

配置项	说明
地址类型	地址类型，“主机名”，“IPv4”或“IPv6”
服务器地址	服务器地址信息
Version	SNMP 版本，v1 v2 v3
Type	通知类型，“Trap”或“Inform”
Community/User	共同体或用户名
Security Level	安全级别
服务器端口号	端口号范围 1-65535，默认 162
Timeout	服务器超时时间，范围 1-300 秒，默认 15 秒。
Retry	重试间隔，范围 1-255 秒，默认 3 秒。

2. 单击“添加”，填写相应配置，单击“应用”，完成配置。



20.5 RMON 配置

RMON（Remote Monitoring，远程网络监视）是 IETF（Internet Engineering Task Force，Internet 工程任务组）定义的一种 MIB（Management Information Base，管理信息库），是对 MIB II 标准重要的增强。RMON 主要用于对一个网段乃至整个网络中数据流量的监视，是目前应用相当广泛的网络管理标准之一。RMON 包括 NMS（Network Management Station，网络管理站）和运行在各网络设备上的 Agent 两部分。RMON Agent 运行在网络监视器或网络探测器上，跟踪统计其端口所连接的网段上的各种流量信息（如某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等）。 RMON 的实现完全基于 SNMP 体系结构，它与现存的 SNMP 框架相兼容。 RMON 使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效的手段。 RMON 能够减少 NMS 与代理（SNMP Agent）间的通讯流量，从而可以简便而有效地管理大型互连网络。RMON 允许有多个监控者，它可用两种方法收集数据： 利用专用的 RMON probe（探测仪）收集数据，NMS 直接从 RMON probe 获取管理信息并控制网络资源。这种方式可以获取 RMON MIB 的全部信息； 将 RMON Agent 直接植入网络设备（路由器、交换机、HUB 等），使它们成为带 RMON probe 功能的网络设施。RMON NMS 使用 SNMP 的基本命令与 SNMP

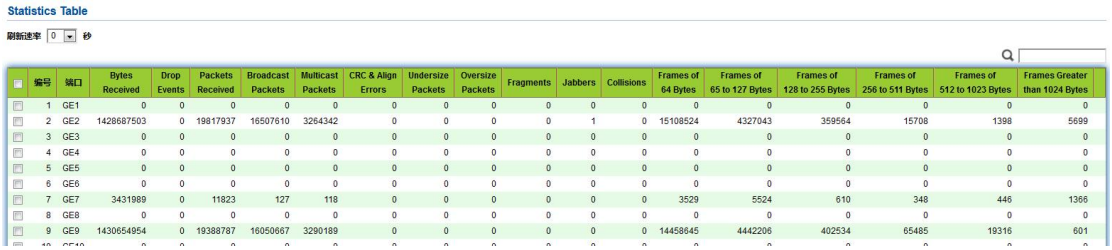
Agent 交换数据信息， 收集网络管理信息， 但这种方式受设备资源限制，一般不能获取 RMON MIB 的所有数据。大多数只收集四个组的信息，这四个组是告警组、事件组、历史组和统计组。 area 系列以太网交换机以第二种方法实现 RMON。 以太网交换机里直接植入 RMON Agent，成为带 RMON probe 功能的网络设施。通过运行在以太网交换机上支持 RMON 的 SNMP Agent，网管站可以获得与以太网交换机端口相连的网段上的整体流量、错误统计和性能统计等信息，实现对网络的管理。

20.5.1 报文统计

统计组信息反映交换机上每个监控接口的统计值。统计组统计的是从该统计组创建的时间开始的累计信息。 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。 利用 RMON 统计管理功能， 可以监视端口的使用情况、 统计端口使用中发生的错误。

操作步骤

1. 单击导航树中的“设备管理 > RMON 配置 > 报文统计”菜单，进入“报文统计”界面，主要显示各端口相关报文统计，如下图所示。



编号	端口	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	GE2	1428687503	0	19817937	16507610	3264342	0	0	0	0	1	0	15108524	4327043	359564	15708	1398	5699
3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	GE7	3431989	0	11823	127	118	0	0	0	0	0	0	3529	5524	610	348	446	1366
8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	GE9	1430654954	0	19388787	16050667	3290189	0	0	0	0	0	0	14458645	4442206	402534	65485	19316	601

2. 可选择端口，点击“清除”，“刷新”完成相应端口统计的清除和刷，点击“View”,可进入端口视图。如下图所示。

3. 可选择指定刷新频率，自动刷新统计信息。

20.5.2 历史配置

配置了 RMON 历史组以后，以太网交换机会周期性地收集网络统计信息，为了便于处理，这些统计信息被暂时存储起来，提供有关网段流量、错误包、广播包、带宽利用率等统计信息的历史数据。 利用历史数据管理功能，可以对设备进行设置。设置的任务包括：采集历史数据、定期采集并保存指定端口的数据。

操作步骤

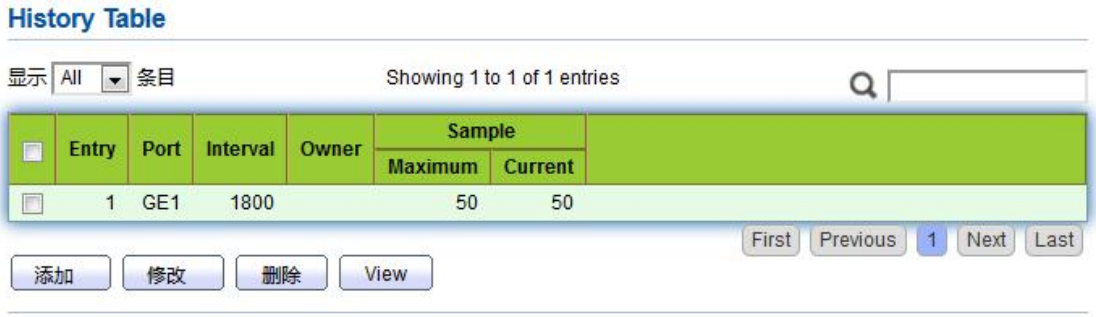
1. 单击导航树中的“设备管理 > RMON 配置 > 历史配置”菜单，进入“历史配置”界面，如下图所示。

界面含义如下表

配置项	说明
Entry	事件组序号
Port	需要统计端口
Interval	采样间隔在 1-3600 之间，单位：秒 默认为 1800 秒
Owner	所有者
Maximum	最大采样条数在 0-50 之间，默认为 50
Current	当前采样条数

2. 点击“添加”，进入历史组配置页面，填写相应的配置项。

3. 单击“应用”，完成配置，如下图所示。



20.5.3 事件配置

事件组用来定义事件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告警触发产生的事件。 事件有如下几种处理方式： 将事件记录在日志表中； 向网管站发 Trap 消息； 将事件记录在日志表中并向网管站发 Trap 消息； 不作任何处理。

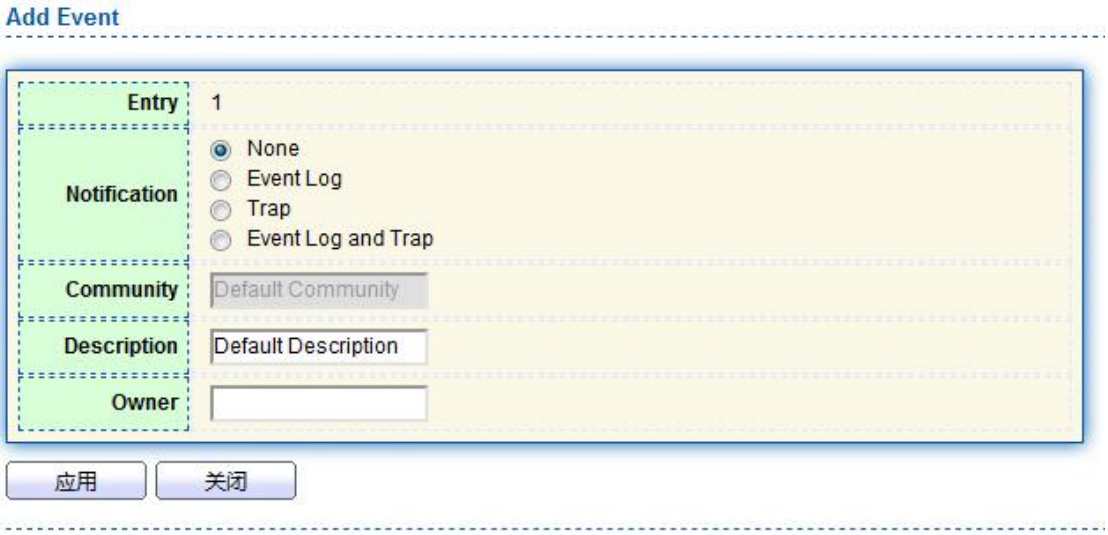
操作步骤

1. 单击导航树中的“设备管理 > RMON 配置 > 事件配置”菜单，进入“事件配置”界面，如下图所示。

界面含义如下表

配置项	说明
Entry	事件组序号
Community	共同体名
Description	描述
Notification	通知
Timer	时间
Owner	所有者

2. 点击“添加”，进入事件组配置页面，填写相应的配置项。



3. 单击“添加”，完成配置，如下图所示。

20.5.4 告警配置

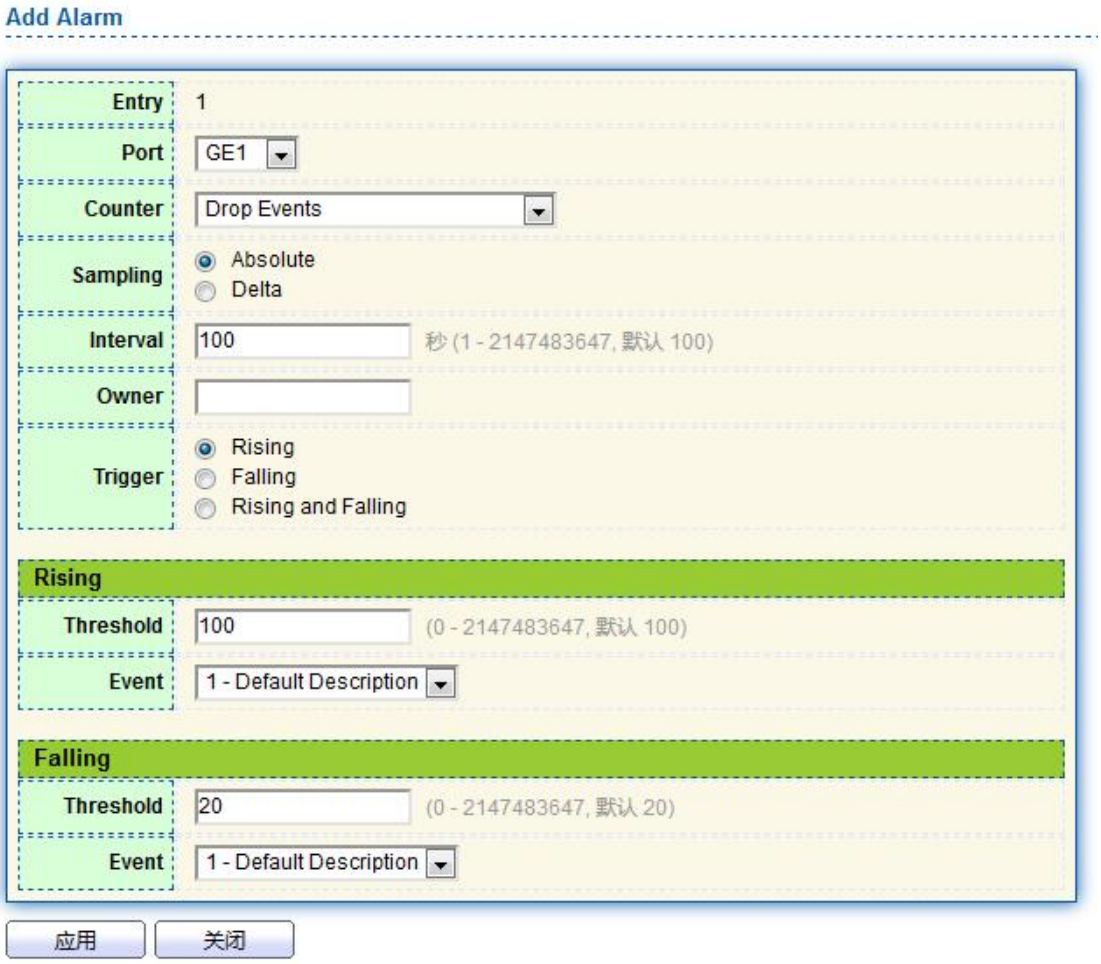
RMON 告警管理可对指定的告警变量（如端口的统计数据）进行监视，当被监视数据的值在相应的方向上越过定义的阈值时会产生告警事件，然后按照事件定义的处理方式进行相应的处理。事件的定义在事件组中实现。 用户定义了告警表项后，系统对告警表项的处理如下：对所定义的告警变量 alarm-variable 按照定义的时间间隔 sampling-time 进行采样； 将采样值和设定的阈值进行比较，一旦超过该阈值，即触发相应事件。

1. 单击导航树中的“设备管理 > RMON 配置 > 告警配置”菜单，进入“告警配置”界面，如下图所示。

界面含义如下表

配置项	说明
Entry	告警组序号
端口	输入需要统计端口
Counter	告警采样参数
Interval	采样间隔在 1-2147483647 之间，单位：秒 默认 100 秒
Sampling	采样类型 Absolute 与 Delte
Owner	所有者
Threshold (Rising)	上升沿阈值在 0-2147483647 之间
Event(Rising)	事件组索引，当告警触发时，将激活事件组相应事件
Threshold (Falling)	下降沿阈值在 0-21474836475 之间
Event(Falling)	事件组索引，当告警触发时，将激活事件组相应事件

2. 点击“添加”，进入告警组配置页面，填写相应的配置项。



3. 单击“应用”，完成配置，如下图所示。