600系列工业以太网交换机WEB使用说明

2022 年 8 月 15 日

版本：V1.0

修订记录

日期	版本	修改人	描述
2022-08-15	V 1.0		第一版

目录

前言

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。

本书约定

本手册采用以下约定方式。

GUI 约定	描述
 说明	对操作内容的描述，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。

1 概述

本使用说明对产品WEB页面进行描述，用户可以通过交换机的WEB页面对交换机进行管理。本说明书只对各个WEB页面的操作进行简单的介绍。

交换机为用户提供Web访问功能。用户可以通过Web浏览器访问交换机，对交换机进行管理和配置。WEB访问的主要特点是：

- 易于访问：用户可以从网络的任何地方轻松访问交换机。
- 用户可以用熟悉的 Google,Microsoft Internet Explorer 等浏览器对 WEB 页面进行访问，WEB 页面以图形化和表格化的形式呈现给用户。
- 交换机提供了丰富的 WEB 页面，用户可以通过这些 WEB 页面对交换机的绝大部分功能进行配置和管理。
- WEB 页面功能的分类整合，便于用户找到相关的页面进行配置和管理。

 说明

1、请客户使用 **Internet Explorer 8.0** 以上版本的浏览器。

2、登录交换机时，对 Web 页面有设置或更改时，需注意保存。点击 WEB 菜单栏下的“保存配置”，否则，交换重启后，设置或更改不会保存。

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://192.168.1.254，按 Enter 键。

此时出现登录窗口，如下图所示，支持中英切换。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。

说明

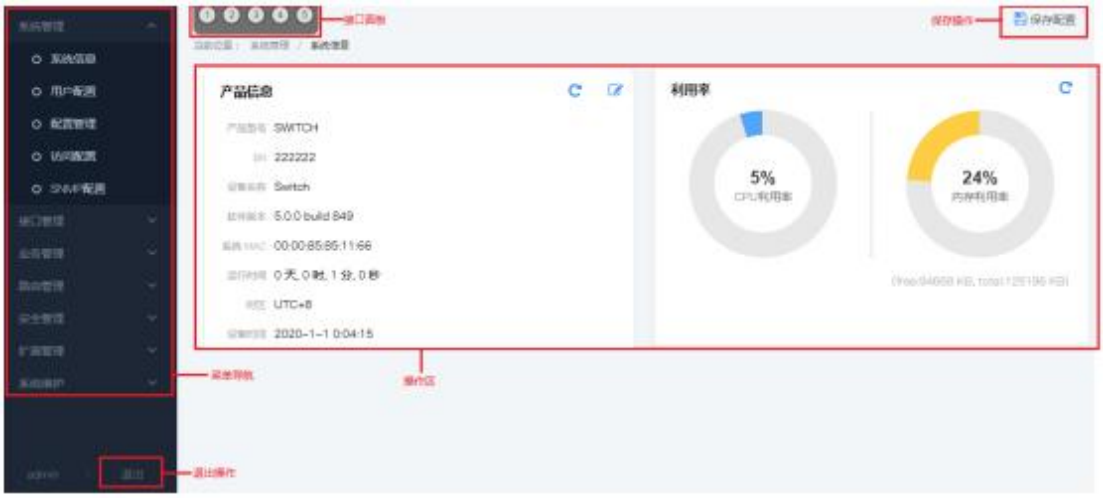
1、登录交换机时，应使 PC 的 IP 网段与交换机网段一致。

2、首次登录时，设置 PC 的 IP 地址为 192.168.1.x（x 代表 1~254，除 254），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 192.168.1.254。

3、该交换机的 WebServer 有提供 5 次机会输入用户名和密码，如果 5 次输入错误，登录界面上有红色字体 “错误次数太多，请 1 分钟后再试”错误提示信息。1 分钟后用户可重新刷新页面，输入正确的用户名和密码，登录到 WebServer 后，推荐修改用户名和密码。

2.2 客户端界面组成

Web 网管系统的客户端如下图所示，包含接口面板，设置导航、操作区、退出状态。



区域	说明
接口面板	接口的状态说明
设置导航	可以对所有的操作功能选择对应的导航
退出	显示当前登录的用户，“退出”到登录界面
操作区	对所有的功能模块进行具体的设置和操作

2.3 Web界面导航树

Web 网管的菜单主要提供系统配置、接口配置、业务管理、安全管理、路由管理、系统维护六个菜单项。每个菜单选项下又有子菜单，如下表所示。

菜单项	子菜单	说明
系统配置	系统信息	显示产品信息与运行信息
	配置管理	可进行配置保存，恢复出厂设置及下载和上传配置文件
	用户配置	设置用户包括用户名、密码、权限（viewer/administrator）
	访问配置	启用/禁用 TELNET 服务及设置 HTTP/HTTPS 服务设置
	SNMP 配置	提供配置和查询 SNMP 系统配置、Trap 配置和用户配置的功能
接口管理	物理端口	设置端口速率（自协商、10M、100M、1000M），设置流控方式（disable、tx、rx、both），启用与关闭接口及最大帧长设置
	风暴抑制	设备支持对接口下的广播、未知组播以及未知单播报文分别按包速率进行风暴控制，防止这三类报文产生广播风暴
	端口限速	提供配置和查询接口限速的功能。
	端口镜像	提供配置和查询端口镜像功能
	链路聚合	提供配置和查询静态与动态 LACP 功能
	端口隔离	提供配置和查询二层端口隔离功能
	端口统计	提供查询端口概要与详细统计功能
业务管理	VLAN 配置	提供配置和查询 VLAN、接口信息的功能
	MAC 配置	提供配置和查询 MAC 地址表信息、MAC 的老化时间、MAC 学习、静态 MAC 的功能
	MSTP 配置	提供配置和查询设备 STP 全局配置、实例配置、实例端口配置和端口配置的功能。
	ERPS 配置	提供配置和查询设备 ERPS 功能
	A-RING 配置	支持静态和动态环网类型配置
	二层组播配置	提供配置和查询 IGMP Snooping 配置和静态组播的功能
	MLD-snooping	提供 IPV6 组播地址侦听功能
	QOS 配置	提供配置和查询 QOS 全局配置与端口配置的功能
	LLDP 配置	邻居发现功能
	UDLD 配置	单通链路检测功能

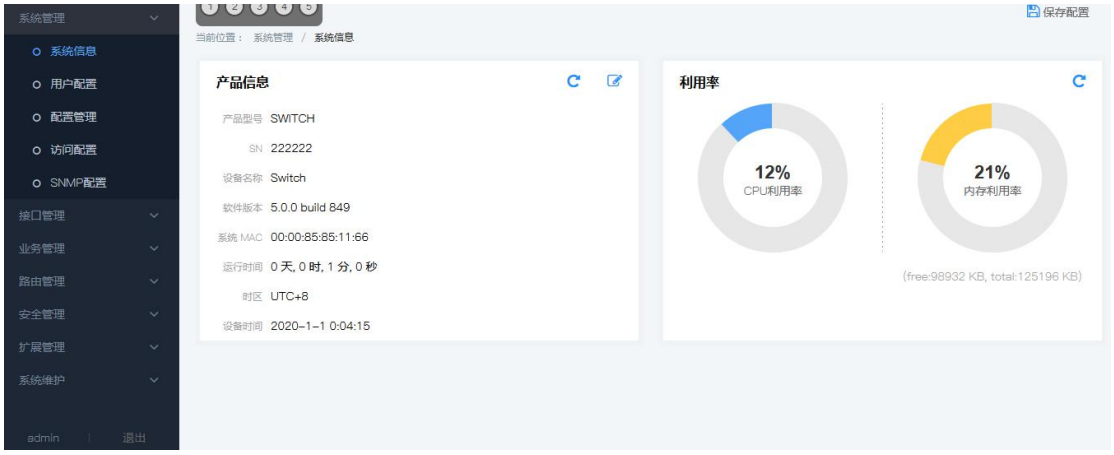
	Link-flap 配置	链路振荡检测功能
	DHCP Server 配置	提供配置和查询 DHCP Server 配置、地址池配置、客户端列表、静态客户端配置、端口绑定的功能
安全管理	访问控制	提供配置和查询过滤规则和设备访问规则的功能
	防攻击设置	提供配置和查询防攻击的功能
	ACL 配置	提供配置和查询 ACL 信息的功能
	流量监控	可监控各接口入口，接口数据
	告警配置	可设置电源，接口告警
	802.1X 配置	提供配置和查询全局 802.1X 认证配置、Radius 服务器配置的功能
扩展功能	Time-rang 配置	时间周期设置
	Devices 配置	连接设备信息显示
	POE 配置	配置或者查看 POE 功能
网络管理	接口 IP	配置接口 IP
	Static 配置	配置静态路由参数
	ARP 设置	配置 ARP 路由参数
系统维护	NTP 设置	提供配置和查询 NTP 服务器的功能
	日志配置	显示设备上日志信息。
	诊断测试	提供 Ping、Traceroute、端口环回的功能
	重启设备	将交换机重启
	在线升级	升级交换机的软件版本

3 系统配置

3.1系统信息

1.面板描述

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，各端口连接状态，产品信息，运行状态。界面显示如下图：



2.关键字说明

配置项	含义
产品型号	设备使用的批次编号，以方便判断设备的标签管理
设备名称	设备使用的网络标识，以方便集成管理工具判断
软件版本	当前使用的软件版本信息，更新的软件版本具有更多的功能
运行时间	当前设备使用多长时间
时区	当前设备使用时区的信息
CPU 利用率	当前设备使用 CPU 的信息
内存利用率	当前设备使用内存的信息
系统 MAC	设备的硬件地址，是由 48 比特长(6 字节)，16 进制的数字组成，其具有惟一性

3.操作步骤说明

步骤一	单击导航栏中“系统配置”菜单，进入“系统配置”界面。单击“系统信息”。
步骤二	可进行设备名称，时间相关的修改设置。修改完成点击“设置”即完成设置。
步骤三	如需作为启动配置，需点击“保存配置”进行设置保存。

3.2用户配置

1.面板描述

用户可以查看交换机当前的用户名、密码以及权限，也可以添加新的用户，设置新的用户名、密码以及权限。界面显示如下图：

2.关键字说明

配置项	含义
用户名	访问者的标识，最多 31 个字符，不能为空或包含&或;或”或’或\或/ 字符。
密码	访问者使用的密码为最多 31 个字符，最少 8 个字符，且必须是大小写字母和数字的组合，不能为空或包含&或;或”或’或\或/ 字符。
权限	访问者的权限为 Viewer 时用户只能进行查看，只有登录用户等级为 Administrator 时，用户才能进行相关配置。

3.操作步骤说明

步骤一	单击导航栏中“系统配置”菜单，进入“系统配置”界面。单击“用户配置”页签，可以看到默认用户名：admin，密码：admin，权限：Administrator
步骤二	如用户需要添加新用户，点击“添加用户”，设置“用户名”“密码”“权限”，即可。如用户需要删除某项用户名，点击“删除”即可。
步骤三	如需作为启动配置，需点击“保存配置”进行设置保存。

3.3 配置管理

3.3.1 运行配置

用户可查看当前设备运行配置。单击导航树中的“系统管理> 配置管理”菜单，进入“配置管理”界面， 显示的即为“运行配置”，如下图所示。

若用户需要把当前运行配置作为启动文件，只需点击“保存配置”即可。

3.3.2 启动配置

用户可查看当前设备启动配置内容。单击导航树中的“系统管理> 配置管理”菜单，进入“配置管理”界面， 点击“启动配置”即可，如下图所示。

若用户需要把默认出厂设置作为启动文件，只需点击“恢复出厂设置”即可，需重启才生效；用户也可下载启动配置文件，只需点击“下载”即可获取.conf 文件。

说明

恢复出厂设置除了通过软件设置处理外，也可通过硬件上处理恢复。用户只需在设备上电启动后的状态，长按前面板的灯板旁的 Deault 按钮 10 秒左右重启即可。

3.3.3 配置管理

用户可查看当前设备启动配置内容。单击导航树中的“系统管理> 配置管理”菜单，进入“配置管理”界面， 点击“配置管理”即可，如下图所示。

若用户需要把下载的配置文件作为当前启动文件，只需点击“选择文件”选择相应.conf 文件，在点击“上传”即可，需重启才生效；

3.4 访问配置

3.4.1 Telnet配置

1.面板描述

启用 TELNET 服务后，TELNET 终端可以通过 PC 使用 Telnet 程序连接到该交换机。界面显示如下图：

2.操作步骤说明

步骤一	单击导航栏中“系统管理”菜单，进入“访问配置”界面。勾选即为选择启用，设置端口号，默认端口号“23”，单击”设置“即可。
步骤二	如需作为启动配置，需点击“保存配置”进行设置保存。

说明

终端通过 PC 使用 Telnet 程序连接到该交换机需要具备如下条件：

1、启用交换机的 TELNET 服务

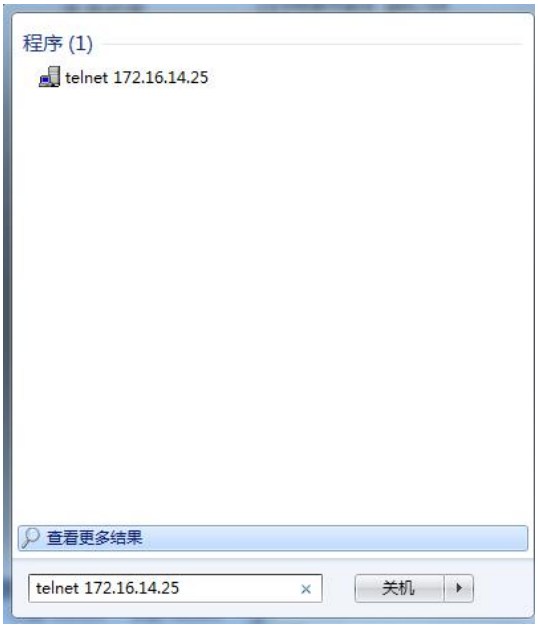
2、知道该交换机设备的 IP 地址，可通过修改获得（在系统管理视图下可使用 ip 命令）；

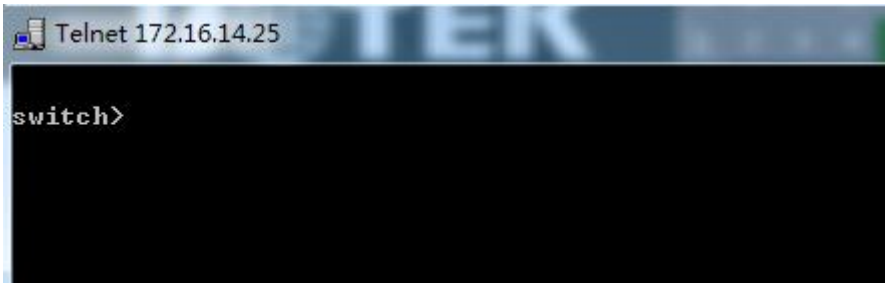
3、如果终端 PC 和该交换机相连的端口在同一局域网内，则其 IP 地址必须设置在同一网段；否

则，终端和该交换机必须跨路由器。
满足以上条件即可利用 Telnet 登录到该交换机，然后对该交换机进行设置。

3.举例说明

#通过 Telnet 登录该交换机之前需要输入 **“Telnet+空格+产品 IP”** 进行验证
在 PC “运行” 处输入回车即可，如下图所示：





3.4.2 HTTPS配置

1.面板描述

HTTPS（全称：Hypertext Transfer Protocol over Secure Socket Layer），是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。HTTPS 提供数据加密服务，防止攻击者截取 Web 浏览器和网站服务器之间的传输报文，从而窃取其中的一些敏感信息，比如信用卡号、密码等。用户可以修改端口号，也可以关闭 HTTP 与 HTTPS 服务。
界面显示如下图：

2.关键字说明

配置项	含义
HTTP	访问时格式：如 HTTP://192.168.9.2：端口号
HTTPS	访问时格式：如 HTTPS://192.168.9.2。
端口号	默认为 80

3.操作步骤说明

步骤一	单击导航栏中“系统配置”菜单，进入“系统配置”界面。单击“访问配置”，进入“HTTP 设置”页面，用户可以看到系统默认配置。
步骤二	用户可通过修改端口号进行访问。修改好端口号，点击“设置”即可。
步骤三	如需作为启动配置，需点击“保存配置”进行设置保存。

4.举例说明

#访问端口号为 8000 的 IP 地址 192.168.1.70。浏览器 IP 设置如下：

说明

当端口修改为 8000 时，重新登录交换机时，输入 IP 地址应加上端口号，即在 web 上输入 http://192.168.1.254:8000

3.4.3 SSH配置

1.面板描述

SSH 是 Secure Shell（安全外壳）的简称，标准协议端口号 22。SSH 是一个网络安全协议，通过对网络数据的加密，使它在一个不安全的网络环境中，提供了安全的远程登录和其他安全网络服务。界面显示如下图：

2.操作步骤说明

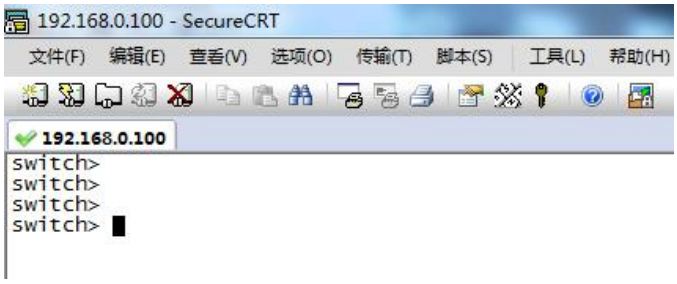
步骤一	单击导航栏中“系统配置”菜单，进入“系统配置”界面。单击“访问配置”，进入“SSH 设置”页面，用户可以看到系统默认配置。

步骤二	用户可通过修改端口号进行访问。修改好端口号，点击“设置”即可。
步骤三	如需作为启动配置，需点击“保存配置”进行设置保存。

3.举例说明

#勾选 SSH 服务设置，默认端口号为 22，设置如下：

通过 SercureCRT 启用 ssh 功能，在弹出的如下窗口中输入相应用户名和密码即可。



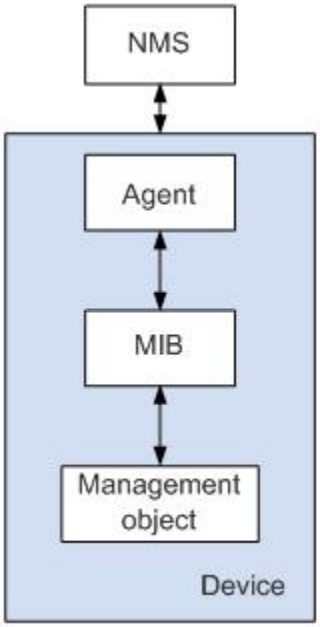
3.5 SNMP配置

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

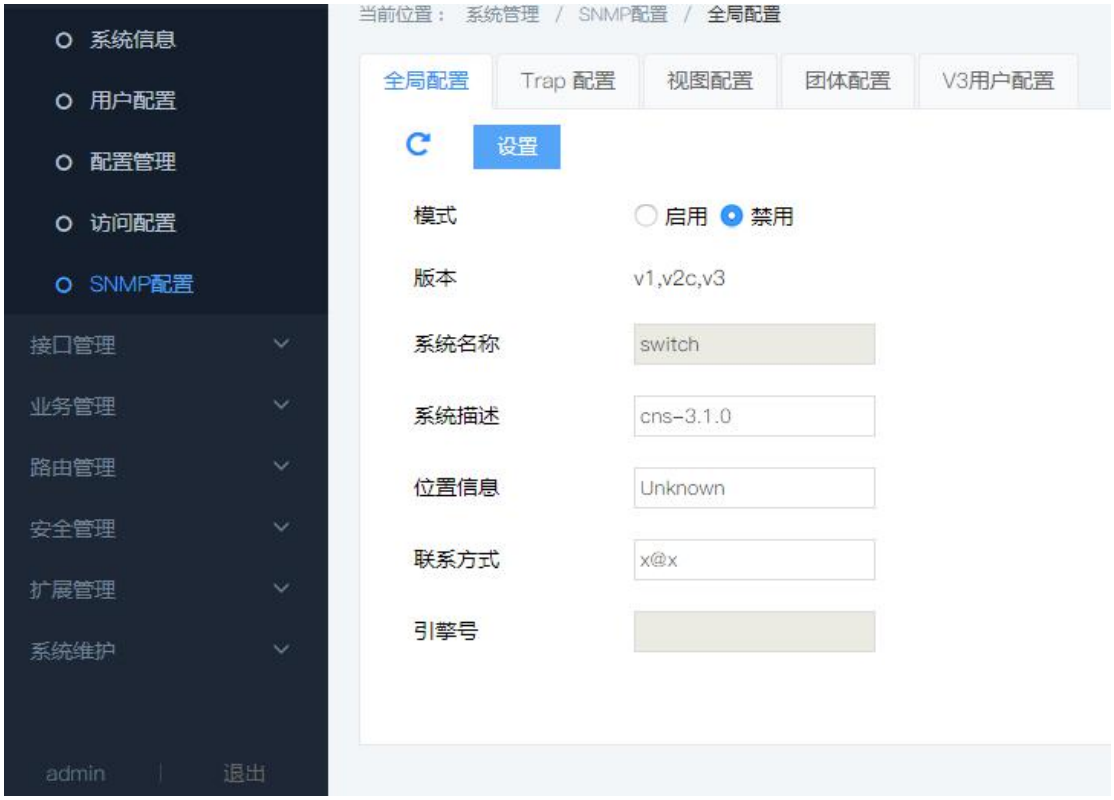
- Management object 指被管理对象。每一个设备可能包含多个被管理对象，被管理对象可以是设备中的某个硬件（如一块接口板），也可以是某些硬件，软件（如路由选择协议）及其的配置参数的集合。

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。

操作步骤

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



界面含义如下表

配置项	配置子项	说明
SNMP 系统配置	模式	可选，开启或者禁用
	版本	不可选，设备默认支持三个 SNMP 版本，分别为 SNMPv1、SNMPv2c 和 SNMPv3
	读区域/写区域	不可选，设备默认支持，用于在 Agent 与 NMS 之间完成认证，字符串形式，用户可自行定义。团体名包括“可读”和“可写”两种，执行 GetRequest、GetNextRequest 操作时，采用 “public” 进行认证；执行 Set 操作时，则采用 “private” 认证。 假定 NMS 想要获取被管理设备 MIB 节点 sysContact 的值，使用可读团体名为 public 假定 NMS 想要获取被管理设备 MIB 节点 sysContact 的下一个节点 sysName 值，使用可读团体名为 public 假定 NMS 想要设置被管理设备 MIB 节点 sysName 的值为 RUNDATA，使用可写团体名为 private，
Trap 配置	模式	可选，开启或者禁用，Trap 是被管理设备不经请求，主动向 NMS 发送的信息，用于报告一些紧急的重要事件（如被管理设备重新启动等）。需要注意的是，在配置 Trap 基本功能前必须完成 SNMP 基本配置。

	Trapv1 接收端	必填，设置 Trap 目标主机地址
	Trapv2 接收端	必填，设置 Trap 目标主机地址
用户配置	读用户	设置读用户，安全级别为需要认证和加密，指定认证协议为 MD5 和 SHA、指定加密协议为 AES 和 DES
	写用户	设置写用户，安全级别为需要认证和加密，指定认证协议为 MD5 和 SHA、指定加密协议为 AES 和 DES

2.填写相应的配置项。

3.单击“添加”，完成配置。

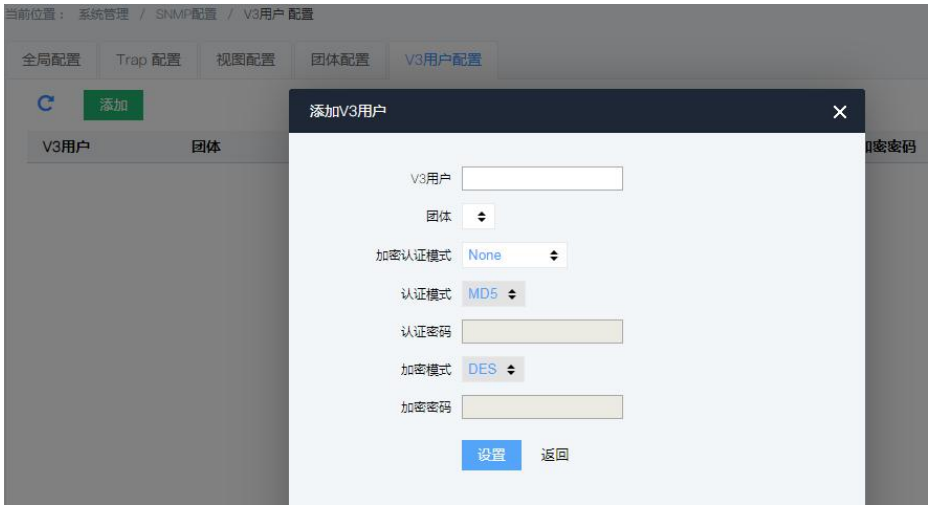
下面举个例子来说明，网管工作站（NMS）与 Switch A（SNMP Agent）通过以太网相连，网管工作站 IP 地址为 10.10.10.1。在 Switch A 上进行如下配置：设置团体名和访问权限、管理员标识、联系方法以及交换机的位置信息、 允许交换机发送 Trap 消息。 使得通过 NMS 可以获取对交换机的访问权限，并接收交换机发送的 Trap 消息。

操作步骤

1.启用 SNMP Agent 服务，并设置 SNMP v1、v2、V3 版本的团体名，单击导航树中的“系统配置> SNMP 配置”菜单，进入“SNMP 系统配置”界面，单击启用模式，如下图所示。

2.允许交换机向网管工作站 10.10.10.1 发送 Trap 报文，单击导航树中的“系统配置> SNMP 配置”菜单，进入“Trap 配置”界面，单击启用模式，在“Trapv1 接收端”输入 10.10.10.1，如下图所示。

3.设置 V3，安全级别为需要认证和加密，指定认证协议为 MD5、认证密码为 12345，指定加密协议为 des，指定密码为 12345，单击“设置”，如下图所示。

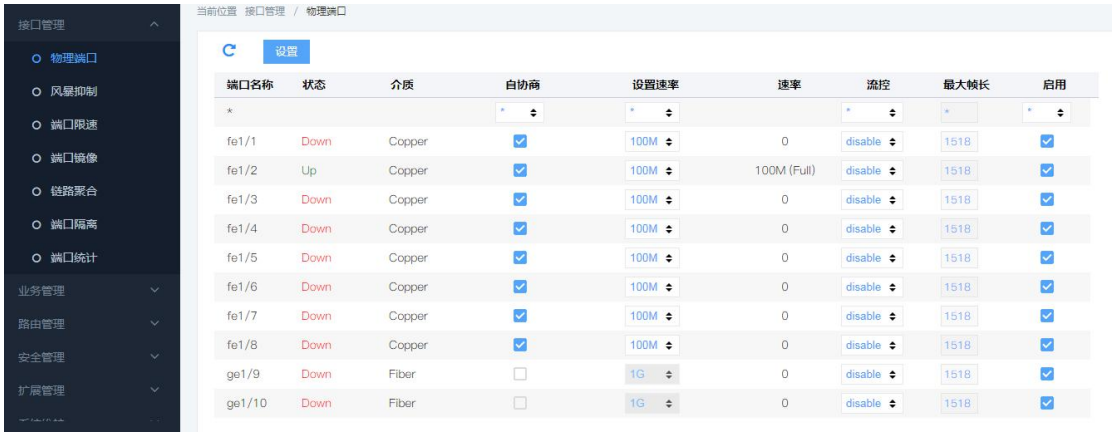


4 端口配置

4.1 物理端口

1.面板描述

物理端口页面主要包括查看端口类型（电口或光口），设置速率模式和双工模式，端口使能，流控。只有启用端口时针对该端口的速率、双工、流控才会起作用。选择自动协商时，速率、双工自动协商获得。界面显示如下图：



2.关键字说明

配置项	含义
端口名称	对应端口的名称，与面板上的标识相对应
状态	显示端口是否连接
介质	电口和光口。光纤接口采用的 mini-GBIC 光纤传输，可根据不同的传输距离选择不同类型的光纤传输。
自协商	可配置自协商，强制十兆，强制百兆，强制千兆。千兆接口支持 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。
速率	显示端口传输速率。共有十兆、百兆、千兆三种速率类型。
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 Disable ：禁用 PAUSE 帧的接收和传输 rx（Rx PAUSE ）：启用 PAUSE 帧的接收 both （ Rx/Tx PAUSE）： 启用 PAUSE 帧的接收和传输 tx（Tx PAUSE ）：启用 PAUSE 帧的传输
最大帧长	显示端口传输最大帧长，范围是 64-16356。
启用	显示端口转发数据状态，如果某端口显示关闭，则不可以转发数据

3.操作步骤说明

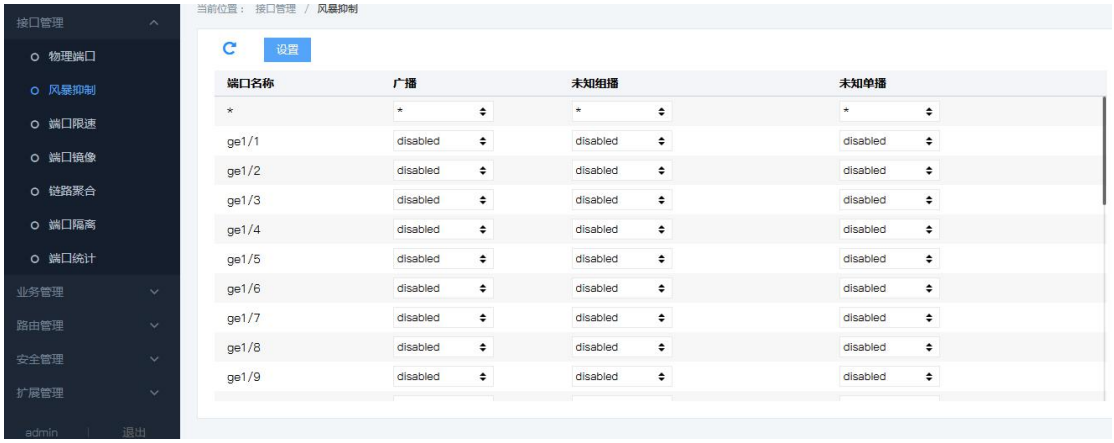
步骤一	单击导航栏中“端口配置>物理端口”菜单，进入“物理端口”界面。
步骤二	选择需要配置的接口，选择可配置项“自协商”，“流控”，“最大帧长”
步骤三	接口设置完成，点击“设置”。
步骤四	如需作为启动配置，需点击“保存配置”进行设置保存。

4.2 风暴抑制

1.面板描述

风暴抑制的基本原理：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。界面显示如下图：



2.关键字说明

配置项	含义
广播包	目的地址为 FF-FF-FF-FF-FF-FF 的数据帧
组播包	目的地址为 XX-XX-XX-XX-XX-XX 的数据帧，第二个 X 为奇数数字。
未知单播包	该数据帧的 MAC 地址不存在设备的内部索引表中。

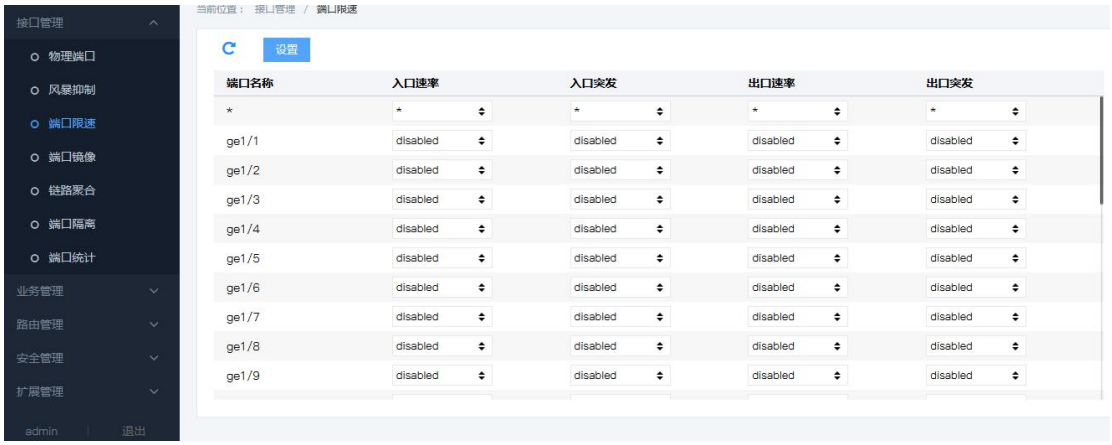
3.操作步骤说明

步骤一	单击导航栏中“端口配置 > 风暴控制 ”菜单，进入“风暴控制”界面。
步骤二	选择需要配置的接口，可对广播、未知组播、未知单播设置相应抑制值。
步骤三	接口相应抑制值设置完成，点击“设置”。
步骤四	如需作为启动配置，需点击“保存配置”进行设置保存。

4.3 端口限速

1.面板描述

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。用户能够限制每个端口的通讯流量或取消端口流量限制，可以选择一个固定的速度，其范围在： 0kbps~1000Mbps（千兆）。界面显示如下：



说明

1、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。

2、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。

2.关键字说明

配置项		说明
接口入方向	入口速率	输入入方向的承诺信息速率。范围是 64k-800M。
	入口突发	输入入方向的承诺突发尺寸。范围是 64k-800M。
接口出方向	出口速率	输入出方向的承诺信息速率。范围是 64k-800M。
	出口突发	输入出方向的承诺突发尺寸。范围是 64k-800M。

3.操作步骤说明

步骤一	单击导航栏中"端口配置> 端口限速"菜单，进入"端口限速"界面
步骤二	选择需要配置的接口，可对出入口速率设置。
步骤三	接口设置完成，点击“设置”。
步骤四	如需作为启动配置，需点击“保存配置”进行设置保存。

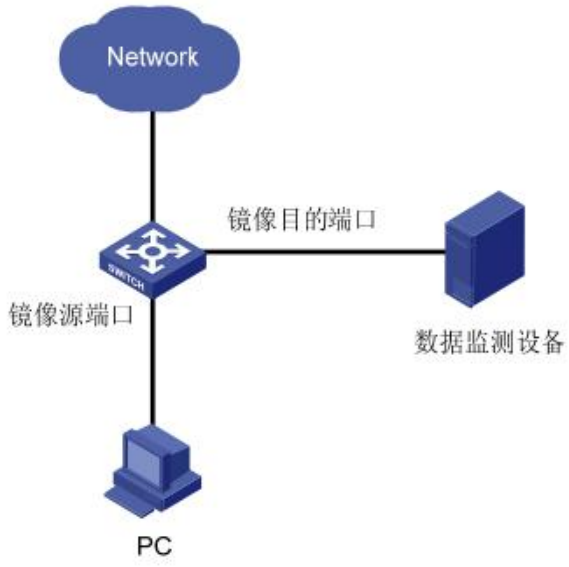
注意

设置了入口或出口速率必须设置入口或出口突发且配置的入口或出口突发不能大于入口或出口速率。

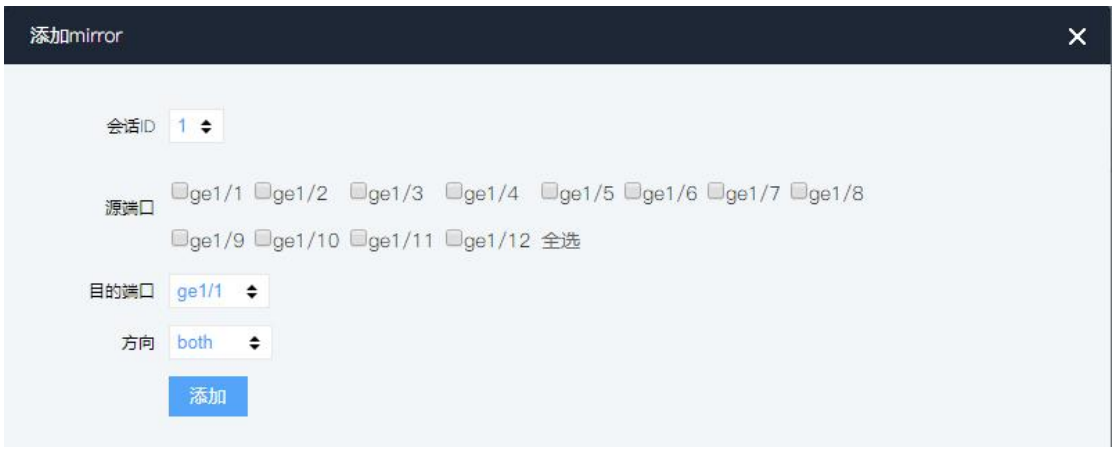
4.4 端口镜像

1.面板描述

端口镜像是把交换机指定端口的报文复制给目的端口；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：



设备界面显示如下：



2.关键字说明

配置项	含义
源端口	该组定义了一组被监控端口，设备将从这些端口采集被指定方向的数据，镜像端口可以是一个或者多个。
目的端口	该组定义了一个用于监控端口，设备将从该端口输出被指定方向的数据 。
方向	该参数指定了监视端口数据的方向，一共分"ingress"，"egress"，"both"

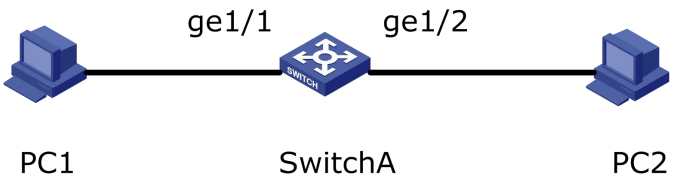
	三个选择。监视者可以根据自己的选择 。 ingress：进口数据，端口收到的报文会被镜像到目的端口； egress：出口数据，端口发送的报文会被镜像到目的端口； both：全部数据，同时对端口接收和发送的报文进行镜像。

3.操作步骤说明

步骤一	单击导航栏中"端口配置> 端口镜像"菜单，进入"端口镜像"界面，选择会话ID。
步骤二	勾选源端口和目的端口及方向，点击“添加”
步骤三	如需作为启动配置，需 点击“保存配置”进行设置保存。

4.举例说明

#配置要求：用户希望通过监控设备 PC2 对 PC1 发送的报文进行监控。
#配置图如下：PC1 通过接口 ge1/1 接入 SwitchA。PC2 直连在 SwitchA 的 ge1/2 接口上。



#设置：网页上选择“添加”，同时勾选源端口 ge1/1，选择目的端口 ge1/2，选择方向 both，单击添加。页面显示如下：

会话ID	源端口	目的端口	方向	操作
1	ge1/1	ge1/2	both	

4.5 链路聚合

4.5.1 链路聚合的介绍

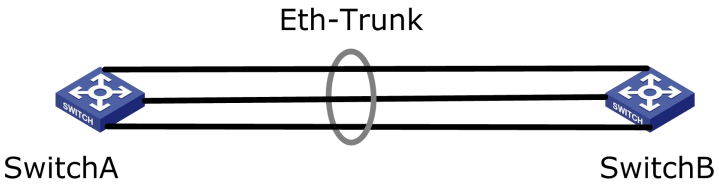
1.面板描述

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。



链路聚合示意图

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，链路聚合分为手工负载分担模式和 LACP 模式。手工负载分担模式下，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，可以使用手工负载分担模式。

4.5.2 添加静态链路聚合

1.面板描述

静态聚合由用户手工配置，不允许系统自动添加或删除汇聚组中的端口。汇聚组中必须至少包含一个端口。当汇聚组只有一个端口时，只能通过删除汇聚组的方式将该端口从汇聚组中删除。界面下图所示：

2.关键字说明

配置项	含义
组 ID	链路聚合组 ID，ID 可选 1 ~ 32
Src Mac	根据报文的源 MAC 地址进行负载分担，当源 MAC 地址相同时报文在同一个端口通过，否则，报文从不同的端口通过。
Dst Mac	根据报文的目的 MAC 地址进行负载分担，当目的 MAC 地址相同时报文在同一个端口通过，否则，报文从不同的端口通过。
Src&Dst Mac	根据报文的源和目的 MAC 地址进行负载分担，当源和目的 MAC 地址相同时报文在同一个端口通过，否则，报文从不同的端口通过。

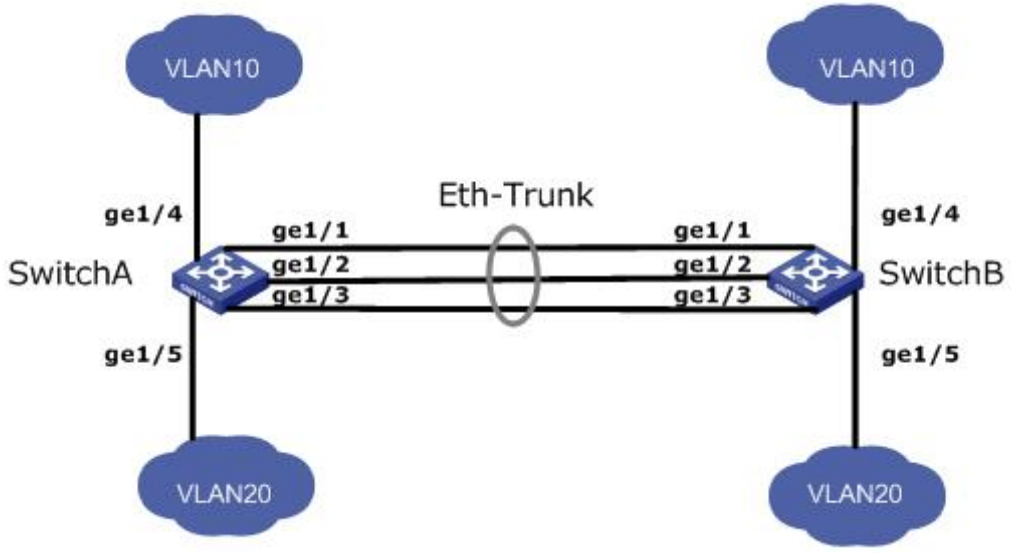
3.操作步骤说明

步骤一	单击导航栏中"端口配置> 静态链路聚合> 添加"菜单，进入"添加静态链路聚合界面，
步骤二	选择组 ID(1-32)，选择负载分担方式(Src Mac,Dst Mac , Src& Dst Mac)，选择需要聚合的端口，单击"添加"
步骤三	如需作为启动配置，需点击 **"保存配置"** 进行设置保存。

4.举例说明

- #组网要求 1：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。
- #组网要求 2：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。

#组网配置图：如下所示



#配置步骤:

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。

2）单击导航栏中"端口配置> 链路聚合> 全局配置"菜单，进入"添加静态链路聚合界面，选择组 ID"1"，选择负载分担方式(Src& Dst Mac),选择需要聚合的端口 ge1/1、ge1/2、ge1/3，单击"添加"，如下图所示。

2）在 SwitchA 配置 ge1/4 接口允许 VLAN10 通过，配置 ge1/5 接口允许 VLAN20 通过。SwitchB 配置与 SwitchA 类似，不再赘述。单击导航树中的"业务管理 > VLAN 配置，进入 " VLAN 配置" 界面，在设置 Vlan 的下方的 Vlan ID 处输入 10，在 Tag 端口列表勾选 "ge1/4"，单击 "添加"，在设置 Vlan 的下方的 Vlan ID 处输入 20，在 Tag 端口列表勾选 "ge1/5"，单击 "添加"，如下图所示。

4）在 SwitchA 配置聚合的端口 ge1/1、ge1/2、ge1/3 允许 VLAN10 和 VLAN20 通过。SwitchB 配置与 SwitchA 类似，不再赘述。单击导航树中的“业务管理 > VLAN 配置，进入“ VLAN 配置”界面，在设置 Vlan 的下方的 Vlan ID 处输入 10，在 Tag 端口列表勾选“ge1/1、ge1/2、ge1/3”，单击“添加”，在设置 Vlan 的下方的 Vlan ID 处输入 20，在 Tag 端口列表勾选“ge1/1、ge1/2、ge1/3”，单击“添加”，如下图所示。

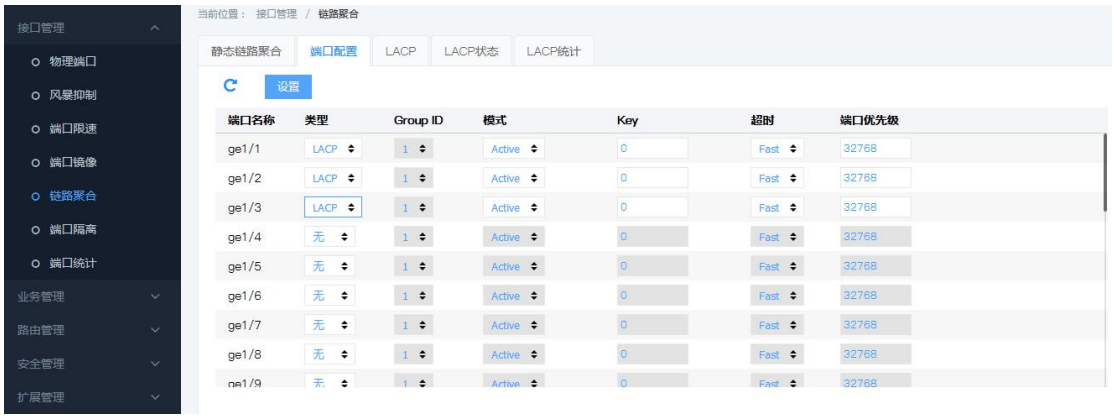
4.5.3 添加动态链路聚合

1.面板描述

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汇聚组达成一致。

动态 LACP 汇聚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。界面显示如下：



2.关键字说明

配置项	含义
类型	静态和动态 LACP，

	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。 动态 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。
模式	Passive（被动状态）：端口不自动发送 LACP 协议数据包；只响应对端设备中发出的 LACP 协议数据包。 Active（主动状态）：端口自动发送 LACP 协议数据包。 有一个或两个主动 LACP 端口的链路可进行动态 LACP 聚合。如果所互相连接的两个端口都是被动 LACP 端口，此两端口将不进行动态 LACP 聚合，因为两个端口都在等候对端设备的 LACP 协议数据包。
端口优先级	LACP 在确定动态汇聚组成员时，将根据设备 ID 优的一端的端口 ID 的优先级的来确定。其中，设备 ID 由两字节的系统优先级和 6 字节的系统 MAC 构成，即设备 ID=系统优先级+系统 MAC 地址。比较设备 ID 时，先比较系统优先级，如果相同则再比较系统 MAC 地址，数值小的一方将被认为优。 范围：0-65535，默认值：32768。

3.操作步骤说明

步骤一	单击导航栏中"端口配置> 链路聚合> 端口配置"菜单，进入"端口配置"，
步骤二	选择需要配置的端口，选择类型(此次选择动态 LACP),选择模式（Active 或 Passive），选择端口优先级（范围：0-65535，默认值：32768），单击"添加"
步骤三	如需作为启动配置，需点击 “保存配置” 进行设置保存。

说明

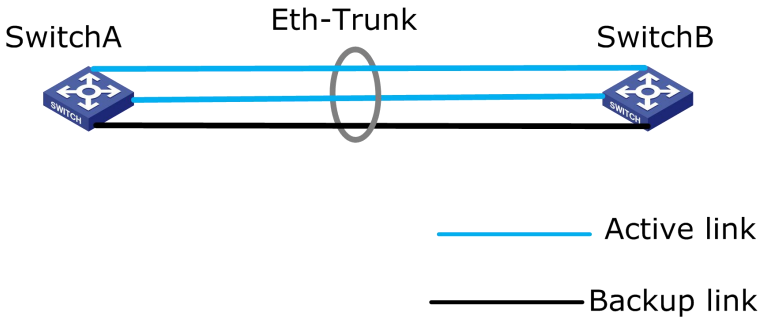
1、改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。

2、本端和对端配置的工作模式应保持一致。

4.举例说明

在两台 Switch 设备上配置 LACP 模式链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

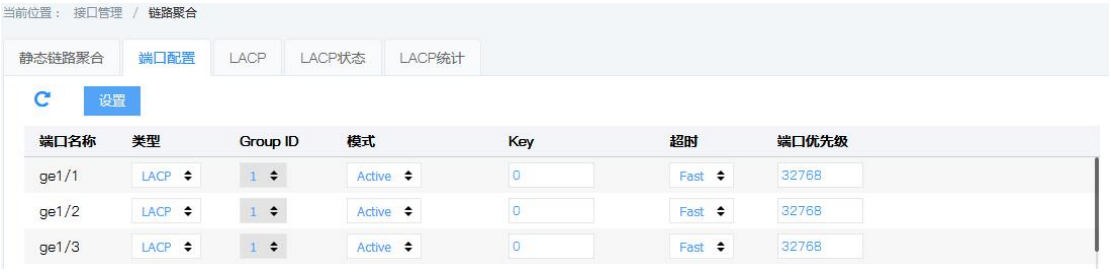
- 两条活动链路具有负载分担的能力。
- 两设备间的链路具有 1 条冗余备份链路，当活动链路出现故障链路时，备份链路替代故障链路，保持数据传输的可靠性。



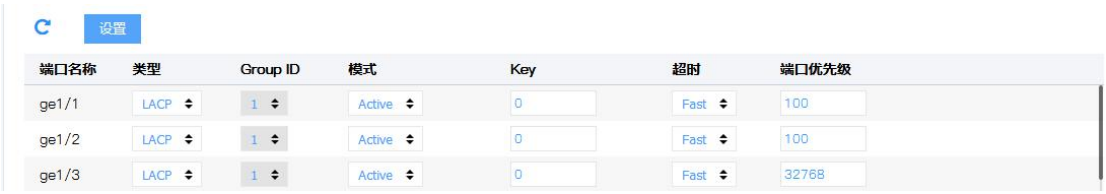
LACP 模式的链路聚合图

#配置步骤

1） 在 SwitchA 上配置 LACP 模式。SwitchB 配置过程与 SwitchA 类似，不再赘述。单击导航栏中"接口管理> 链路聚合> 端口配置"菜单，进入"端口配置 "，选择需要配置的端口 ge1/1、ge1/2、ge1/3，选择类型 "动态 LACP" ,选择模式 "Active" ，单击 "设置" ，完成配置。如下图所示。



3） 在 SwitchA 上配置接口优先级确定活动链路。单击导航栏中"接口管理> 链路聚合> 端口配置"菜单，进入"端口配置 "，将端口 ge1/1、ge1/2 优先级设置为 100，保证此两个端口为活动链路，单击 "设置" ，完成配置。如下图所示。



4.6 端口隔离

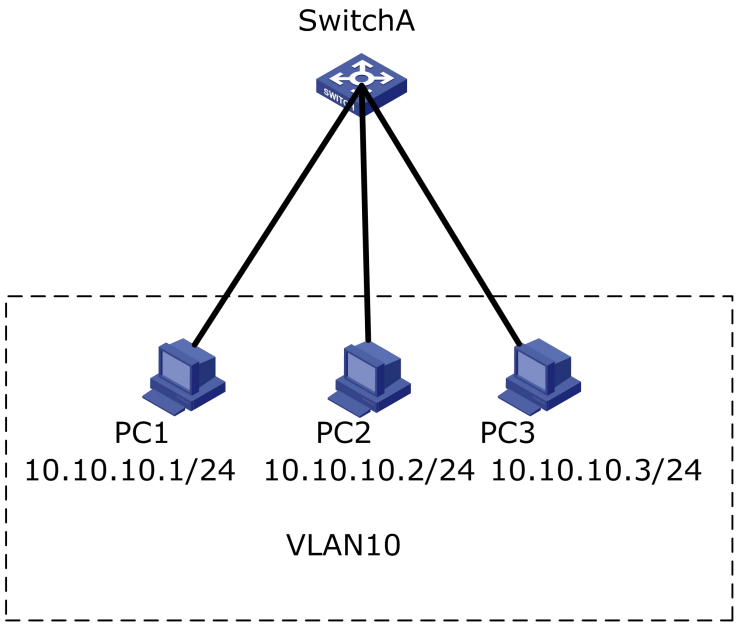
同一端口隔离组的接口之间互相隔离，不同端口隔离组的接口之间不隔离。

操作步骤

1.单击导航栏中"接口管理> 端口隔离"菜单，进入"端口隔离 "，通过勾选端口建立隔离组，单击"设置"，完成配置，如下图所示。

#举例说明,如下图所示，PC1、PC2 和 PC3 同属于 VLAN10，用户希望 PC1 与 PC2 之间在 VLAN10 内不能互相访问，PC1 与 PC3 之间可以互相访问，PC2 与 PC3 之间可以互相访问。

配置端口隔离示例组网图

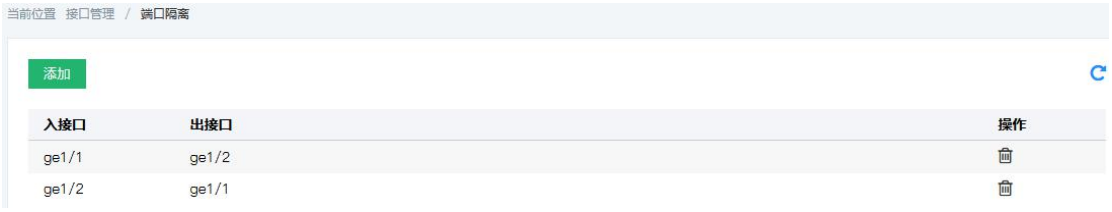


操作步骤

1.创建 VLAN，确定 PC 所属的 VLAN。单击导航树中的“业务管理> VLAN 配置 > VLAN 配置”菜单，进入“VLAN 配置”界面，添加 VLAN10，选择端口 ge1/1，ge1/2，ge1/3，单击“添加”，完成配置，如下图所示。

2. 配置各以太网接口以正确的方式加入 VLAN，实现接口允许 VLAN 报文通过。单击导航树中的“业务管理 > VLAN 配置 > 端口配置”菜单，进入“端口配置”界面，选择端口 ge1/1，ge1/2，ge1/3，分别将 PVID 框里面的数值改为 10，单击“设置”，完成配置，如下图所示。

3.配置 ge1/1，ge1/2 的端口隔离功能，单击导航栏中“端口配置> 链路聚合> 端口隔离”菜单，进入“端口隔离“，通过勾选端口 ge1/1，ge1/2 建立隔离组，单击”设置”，完成配置，如下图所示。



4.验证配置结果

PC1 和 PC2 不能互相 ping 通。

PC1 和 PC3 可以互相 ping 通。

PC2 和 PC3 可以互相 ping 通。

4.7 端口统计

4.7.1 端口概要统计

介绍所有接口流量统计的详细信息以及用户可以手动的刷新或清零统计的信息。

注意：流量统计信息清空后，不能恢复。操作前请仔细确认。。

操作步骤

1.单击导航栏中"接口管理>端口统计> 端口概要统计"菜单，进入"端口概要统计 "，如下图所示。

端口名称	接收报文数	发送报文数	接收字节数	发送字节数	丢弃报文数
ge1/1	0	0	0	0	0
ge1/2	0	0	0	0	0
ge1/3	0	0	0	0	0
ge1/4	0	0	0	0	0
ge1/5	0	0	0	0	0
ge1/6	0	0	0	0	0
ge1/7	0	0	0	0	0
ge1/8	0	0	0	0	0
ge1/9	11960	15381	1837211	3631799	192
ge1/10	10073	11771	1509515	2633592	103

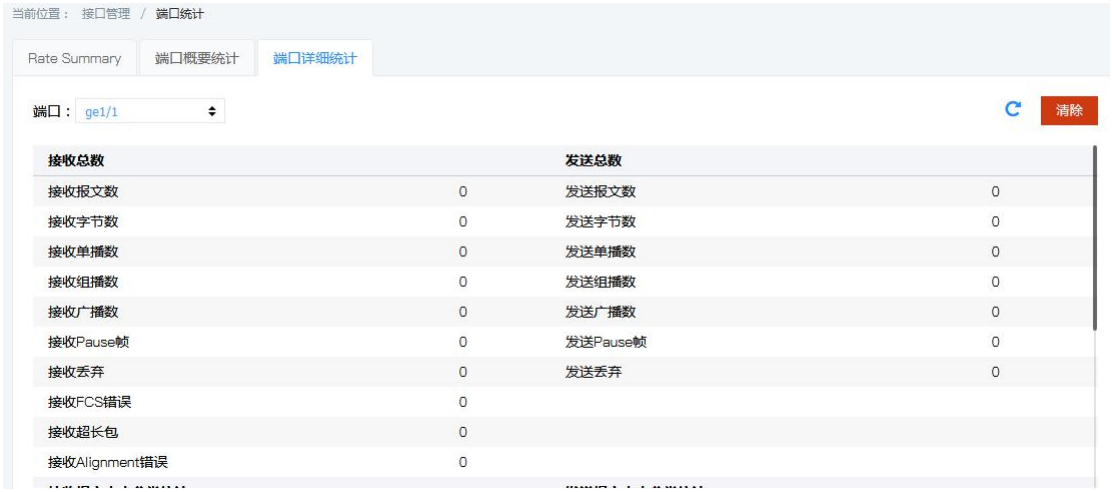
说明：

单击“刷新”，页面获取最新的流量统计信息。
单击“清空”，所有端口的流量统计信息清零，并刷新页面。

4.7.2 端口详细统计

介绍某个接口流量统计的详细信息以及用户可以手动的刷新或清零统计的信息。

1.单击导航栏中"接口管理>端口统计> 端口详细统计"菜单，进入"端口详细统计”，如下图所示。



接收总数		发送总数	
接收报文数	0	发送报文数	0
接收字节数	0	发送字节数	0
接收单播数	0	发送单播数	0
接收组播数	0	发送组播数	0
接收广播数	0	发送广播数	0
接收Pause帧	0	发送Pause帧	0
接收丢弃	0	发送丢弃	0
接收FCS错误	0		
接收超长包	0		
接收Alignment错误	0		

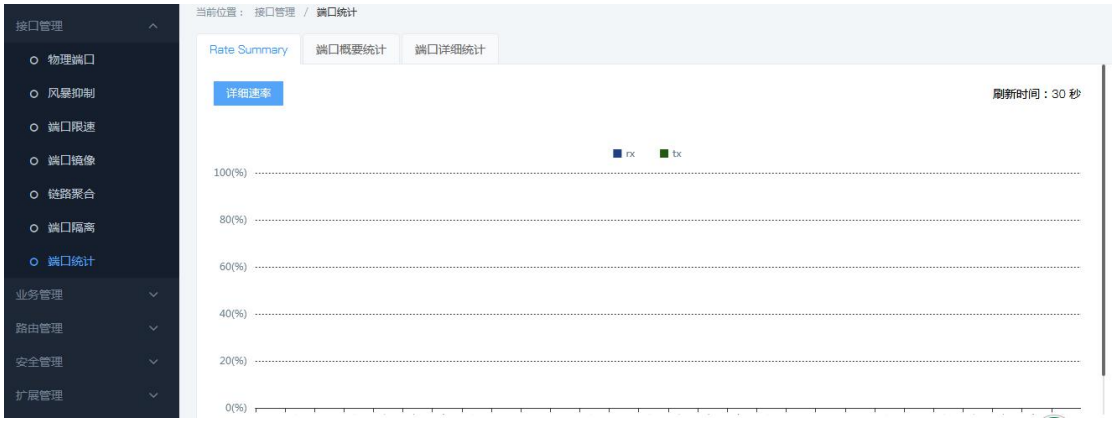
说明:

单击“刷新”，页面获取最新的流量统计信息。
单击“清除”，当前端口的流量统计信息清零，并刷新页面。

4.7.3 速率

介绍接口当前的速率统计的信息以及用户可以手动的刷新。

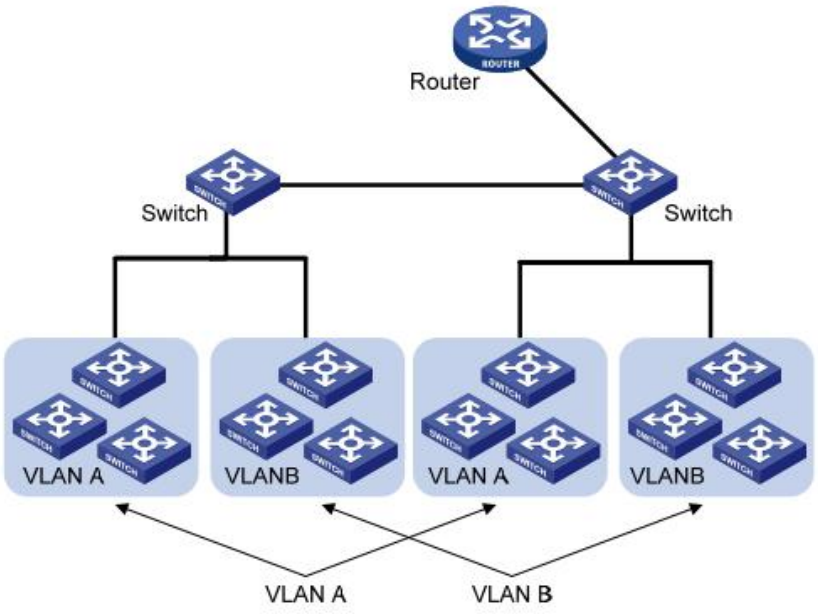
1.单击导航栏中“接口管理>端口统计> 速率”菜单，进入“速率”，如下图所示。



5 业务管理

5 .1 VLAN配置

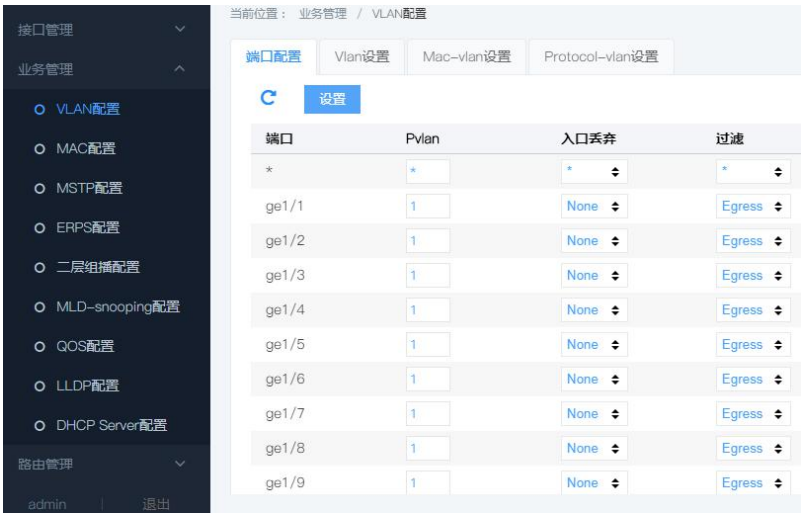
VLAN 的组成不受物理位置的限制，因此同一 VLAN 内的主机也无须放置在同一物理空间里。如下图所示，VLAN 把一个物理上的 LAN 划分成多个逻辑上的 LAN ，每个 VLAN 是一个广播域。VLAN 内的主机间通过传统的以太网通信方式即可进行报文的交互，而处在不同 VLAN 内的主机之间如果需要通信，则必须通过路由器或三层交换机等网络层设备才能够实现。



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。

5.1.1 端口配置

a.新建 VLAN 操作步骤
1.单击导航树中的“业务管理 > VLAN 配置 > VLAN 配置”菜单，进入“VLAN 配置”界面，如下图所示。



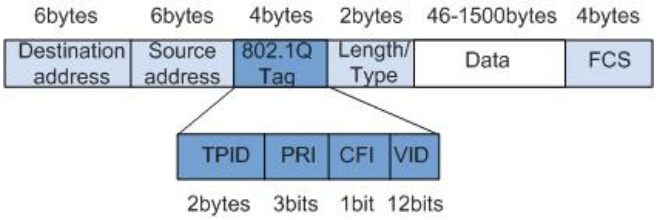
界面信息含义如下表所示。

配置项	说明
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。
Untag	有标记帧
tag	无标记帧
组播	必选,指定组播的处理方式，默认是 Flood-unknown

802.1Q 介绍

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	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

		位），表示 MAC 地址是否是经典格式。	牌环网。在以太网中，CFI 的值为 0。
VID	12bits	VLAN ID，表示该帧所属的 VLAN。	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。

2.填写相应的配置项。

3.单击“添加”，完成配置，如下图所示。

5.1.2 VLAN配置

1.单击导航树中的“业务管理 > VLAN 配置 > 端口配置”菜单，进入“端口配置”界面，如下图所示。

界面信息含义如下表所示。

配置项	说明

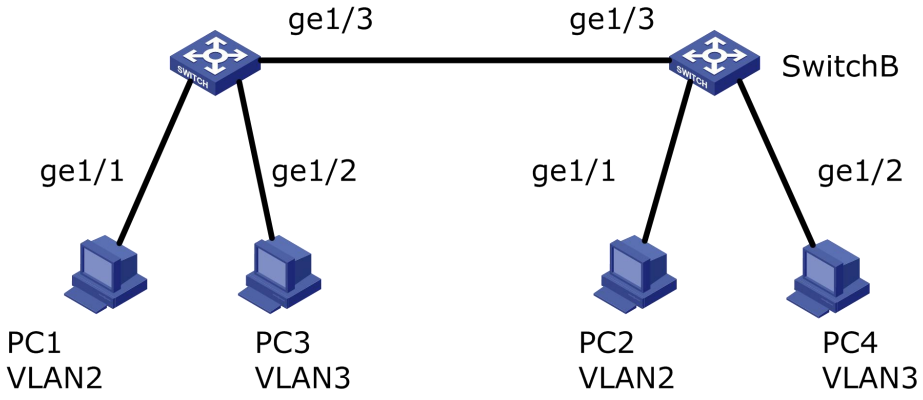
PVID	每个端口只能有一个端口 VLAN ID（PVID）。当不带标签的以太网数据包到达端口时，它将带上 PVID VID 标签。每个端口的缺省 PVID 为 1。
入口丢弃	4 中数据类型：none（不丢弃），untag(丢弃不带 tag 数据)，tag（丢弃带 tag 数据），all（丢弃全部数据）
过滤	对入口和出口做检查，包括 4 中类型：egress（出口），ingress(入口)，both（入口和出口），none（无）

2.填写相应的配置项。

3. 单击“设置”，完成配置，如下图所示。

#配置举例

为了让 SwitchA 和 SwitchB 之间的链路既支持 VLAN2 内的用户通讯又支持 VLAN3 内的用户通讯，需要配置连接接口同时加入两个 VLAN。即应配置 SwitchA 的以太网接口 ge1/3 和 SwitchB 的以太网接口 ge1/3 同时加入 VLAN2 和 VLAN3。



操作步骤：

1.在 SwitchA 创建 VLAN2 和 VLAN3，并将连接用户的接口分别加入 VLAN，将 ge1/3 设置成 trunk 工作模式。单击导航树中的“业务管理 > VLAN 配置 > 端口配置”菜单，进入“端口配置”界面，填写相应的配置项，单击“设置”，完成配置，SwitchB 配置与 SwitchA 类似，不再赘述。如下图所示。

2.配置 SwitchA 上与 SwitchB 连接的接口类型及通过的 VLAN。单击导航树中的“业务管理 > VLAN 配置 > VLAN 配置”菜单，进入“VLAN 配置”界面，填写相应的配置项，单击“添加”，完成配置，SwitchB 配置与 SwitchA 类似，不再赘述。如下图是添加通过 VLAN2 的步骤，添加通过 VLAN3，VLAN2 类似，不再赘述。

3.验证配置结果

将 User1 和 User2 配置在一个网段，比如 192.168.100.0/24；将 User3 和 User4 配置在一个网段，比如 192.168.200.0/24。

User1 和 User2 能够互相 ping 通，但是均不能 ping 通 User3 和 User4。User3 和 User4 能够互相 ping 通，但是均不能 ping 通 User1 和 User2。

5.1.3 mac-vlan

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“业务管理 >VLAN 配置> mac-vlan 设置”菜单，进入“mac-vlan 设置”界面，如下图所示。

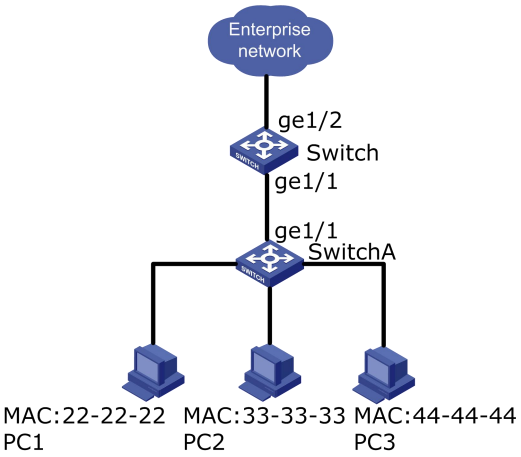
界面信息含义如下表所示。

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。其他 VLAN 必须存在，且以 untag 方式加入需要链接的端口。
MAC	必选，输入计算机网卡的 MAC 地址

2. 填写相应的配置项。
3.单击“添加”，完成配置。

#举例说明
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 ge1/1 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:
1. 创建相关 VLAN。
2. 配置各以太网接口以正确的方式加入 VLAN。
3. 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 ge1/1 的 PVID 为 100。
在 Switch 上配置接口 ge1/1 以 untagged 方式加入 VLAN10。
在 Switch 上配置接口 ge1/2 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。

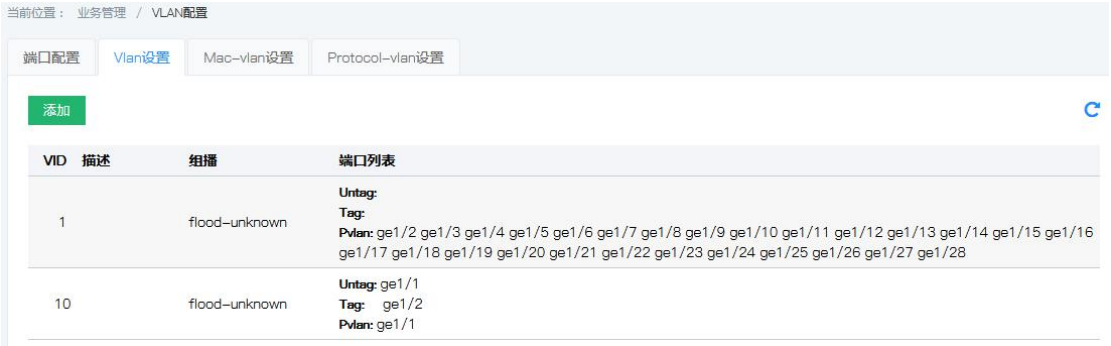
配置基于 MAC 地址的 VLAN 划分组网图



操作步骤

1.配置 Switch 以太网接口 ge1/1 的 PVID 为 100。单击导航树中的“业务管理 > VLAN 配置 > 端口配置”菜单，进入“端口配置”界面，选择端口 ge1/1，输入 PVID 为“100”，单击“设置”，完成配置，如下图所示。

2. 配置 Switch 以太网接口 ge1/1 以 untag 方式、ge1/2 以 tagged 方式加入加入 VLAN10。单击导航树中的“业务管理 > VLAN 配置 > VLAN 配置”菜单，进入“VLAN 配置”界面，输入 Vlan ID “10”，在 “Untag 端口列表”选择端口 ge1/1，在 “Tag 端口列表”选择端口 ge1/2，单击 “添加”，完成配置，如下图所示。



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。此步不需要做操作，因交换机默认配置是所有接口以 untagged 方式加入 VLAN1。

5.配置 PC1、PC2、PC3 的 MAC 地址与 VLAN 关联，实现根据报文中的源 MAC 地址确定 VLAN。单击导航树中的“业务管理 >VLAN 配置> mac-vlan 配置”菜单，进入“mac-vlan 配置”界面，VLAN ID 输入已创建好的 vlan10，分别输入 PC1（0022-0022-0022）、PC2（0033-0033-0033）、PC3（0044-0044-0044）的 MAC 地址，单击“添加”，完成配置，如下图所示。

4.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。

5.1.4 protocol-vlan

基于协议划分 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“业务管理 >VLAN 配置> protocol-vlan 配置 ”菜单，进入“protocol-vlan 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
端口	通过下拉菜单选择端口（ge1/1- ge1/24，xe1/25- xe1/28）
帧类型	可选，帧类型有 ether2，802.3，snap，llc，snap-priv
以太网类型	可选，以太网类型 arp，ip,ipv6,802.1d.1q, 802.1d.1x
Vlan Id	必选，指定加入 VLAN ID 号，取值范围是 1¯4094。如：1-3，5，

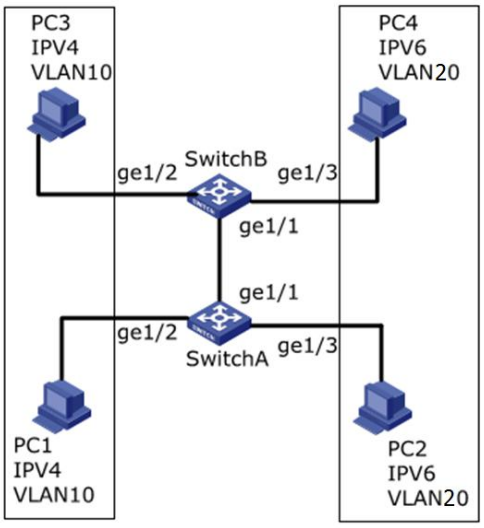
	7，9。其中 VLAN 1 是默认的。VLAN 必须存在，且以 untag 方式加入需要链接的端口。

2．填写相应的配置项。

3.单击“添加”，完成配置。

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。

基于协议划分 VLAN 组网图



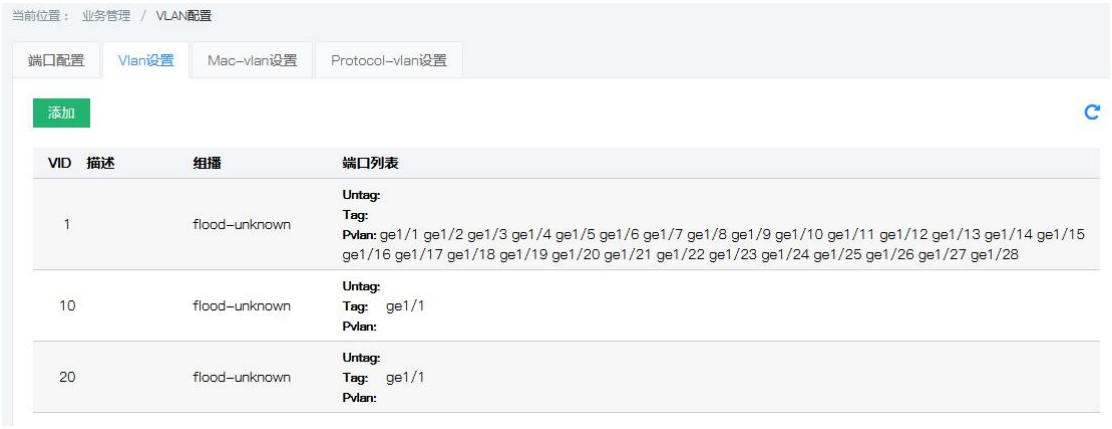
操作步骤

1．创建 VLAN，确定每种业务所属的 VLAN。单击导航树中的“业务管理 >VLAN 配置> VLAN 配置”菜单，进入“端口配置”界面，修改 PVID 值，单击“设置”，完成配置，如下图所示。

2．配置 SwitchA 以太网接口 ge1/2 与 ge1/3 以 untag 方式加入需要链接的端口方式加入 VLAN。单击导航树中的“业务管理 >VLAN 配置 > VLAN 配置”菜单，进入“VLAN 配置”界面，输入 Vlan ID“10”，在“Untag 端口列表”选择端口 ge1/2。同理进入“VLAN 配置”界面，输入 Vlan ID“20”，在“Untag 端口列表”选择端口 ge1/3。单击“添加”，完成配置，如下图所示。

3. 配置 SwitcB 以太网接口 ge1/2 与 ge1/3 以 untag 方式加入需要链接的端口方式加入 VLAN。操作同 2，不再赘述。

4. 在 SwitchA 上配置接口 ge1/1 以 tagged 方式加入 VLAN10 与 VLAN 20。单击导航树中的“业务管理 >VLAN 配置> VLAN 配置”菜单，进入“VLAN 配置”界面，输入 Vlan ID “10”，在“Tag 端口列表”选择端口 ge1/1，单击“添加”。同理进入“VLAN 配置”界面，输入 Vlan ID “20”，在“Tag 端口列表”选择端口 ge1/1，单击“添加”完成配置，如下图所示。



5. 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“业务管理 >VLAN 配置> protocol-vlan 配置”菜单，进入“protocol-vlan 配置”界面，输入相应数值，将 vlan10 绑定 ipv4，vlan20 绑定 ipv6，单击“添加”。完成配置，如下图所示。

5.2 MAC配置

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

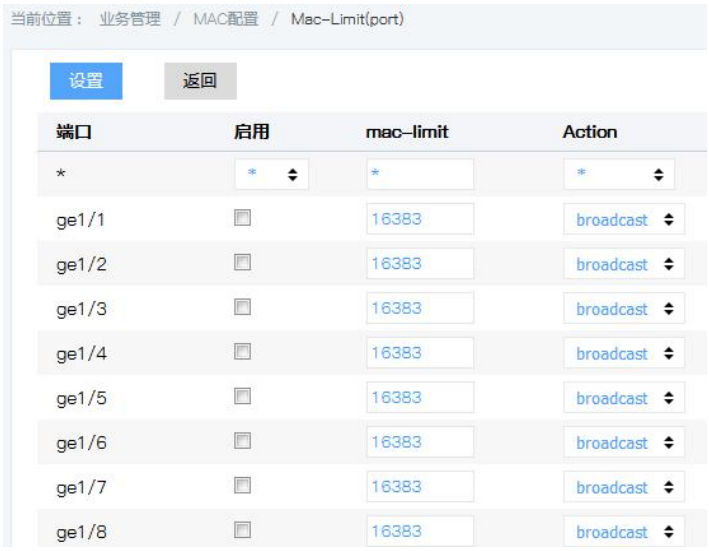
以太网交换机在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：

- 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。

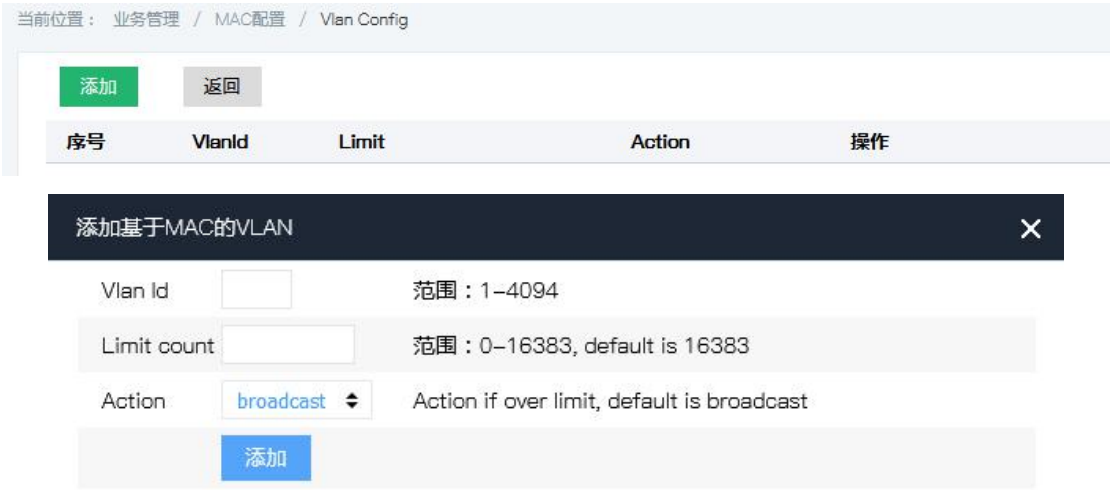
5.2.1 MAC配置

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“业务管理> MAC 配置 > MAC 配置”菜单，进入“MAC 配置”界面。

MAC Limit(port)界面如下：



MAC Limit(VLAN)界面如下：



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，默认老化时间为 300s，范围值为 10-1000000 秒。
Mac-limit	Mac 地址限制。范围值为 0-16383，默认为 16383。 注意：需修改该值才能进行设置保存。

2. 填写相应的配置项。
3.单击“设置”，完成配置。

5.2.2 静态MAC

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“业务管理 > MAC 配置 > 静态 MAC”菜单，进入“静态 MAC”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：H-H-H。
Vlan Id	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。如：ge1/3。 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。

3.单击“添加”，完成配置。

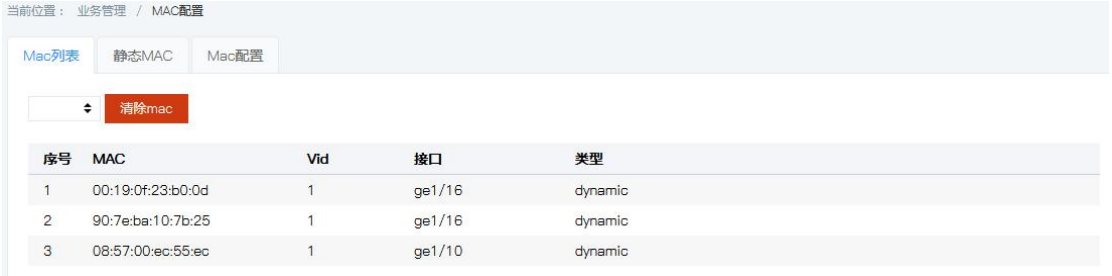
5.2.3 MAC列表

界面信息含义如下表所示。

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。

查看 MAC 地址表操作步骤

1.单击导航树中的“业务管理 > MAC 配置 > MAC 列表”菜单，进入“MAC 列表”界面如下图所示。



界面信息含义如下表所示。

查询项	说明

序号	排序编号
MAC	目的 MAC 地址
Vid	端口所属的 VLAN ID
接口	本设备上的转发出端口编号
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。

5.3 MSTP配置

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。

5.3.1全局配置

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“业务管理 > MSTP 配置 > 全局配置”菜单，进入“全局配置”界面如下图所示。

界面信息含义如下表所示。

配置项	说明
启用 Spanning-tree	默认勾选，代表交换机启用 Spanning-tree
模式	支持三个生成树模式，即 STP、RSTP 和 MSTP。
优先级	范围值 0-61440，步阶值为 4096。
Max age	表示消息的最大生存期，此值的范围为 6 到 40 秒，缺省值为 20 秒。
Hello time	表示消息发送的周期，网桥每隔一定时间会向周围的网桥发送 hello 报文，以确认链路是否存在故障，这个时间间隔为 hello time
Forward Delay	表示端口状态迁移的延时，此值的范围为 4 到 30 秒之间，缺省值是 15 秒。
Max Hops	选择最大跳数。此值的范围是 1 到 40，缺省值为 20。MST 域内生成树的最大跳数用来限制 MST 域内生成树的网络规模。从 MST 域内的生成树的根桥开始，域内的配置消息每经过一台交换机的转发，跳数就被减 1；交换机将丢弃跳数为 0 的配置消息，使处于最大跳数外的交换机无法参与生成树的计算，从而限制了 MST 域的规模。
Revison	MSTP 修订级别。 MSTP 的修订级别用来同域名、VLAN 映射表一起确定交换机设备所属的 MST 域。
Name	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。
3.单击“设置”，完成配置

5.3.2实例配置

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“业务管理> MSTP 配置 > 实例配置”菜单，进入“实例配置”，界面如下图所示。

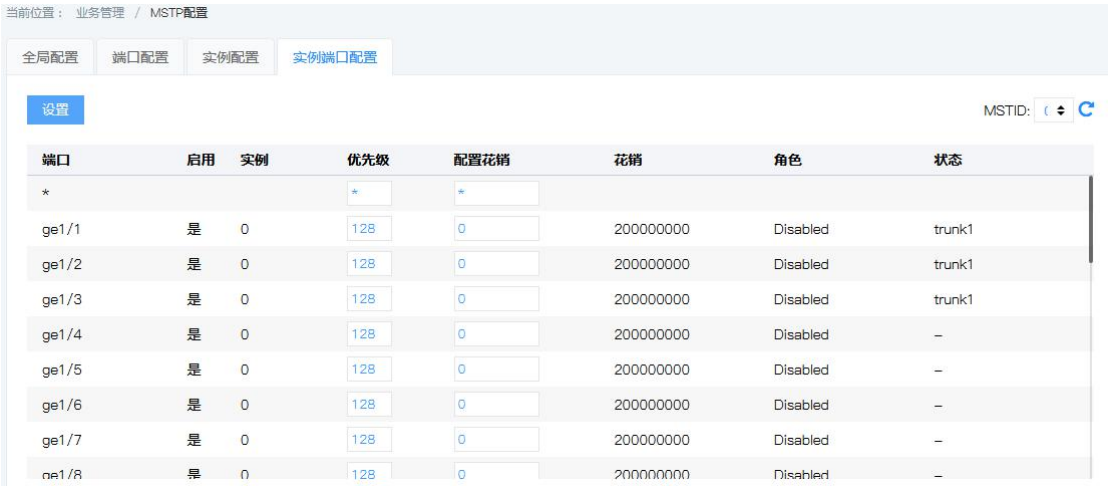
界面含义如下表所示

配置项	说明
MSTI ID	输入 1-63 之内的任一实例号。
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。
Vlan Mapped	输入需要映射的 VLAN

2. 填写相应的配置项。
3.单击“设置”，完成配置，如下图所示。

5.3.3实例端口配置

1.单击导航树中的“业务管理 > MSTP 配置 > 实例端口配置”菜单，进入“实例端口配置”界面如下图所示。



界面信息含义如下表所示。

配置项	说明
MSTID	通过下拉菜单选择已配置好的实例
端口	固定值，根据用户选择而显示的，不支持多选。
启用	固定值，根据用户选择而显示的，不支持多选。
实例	最大可以创建 63 个实例
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。
配置花销	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 1—200000000
花销	使用 IEEE 802.1t 标准方法时取值范围是 1—200000000
角色	分为三类根端口，指定端口，候补端口，Disabled
状态	包括 2 种状态，discarding 与 forwarding

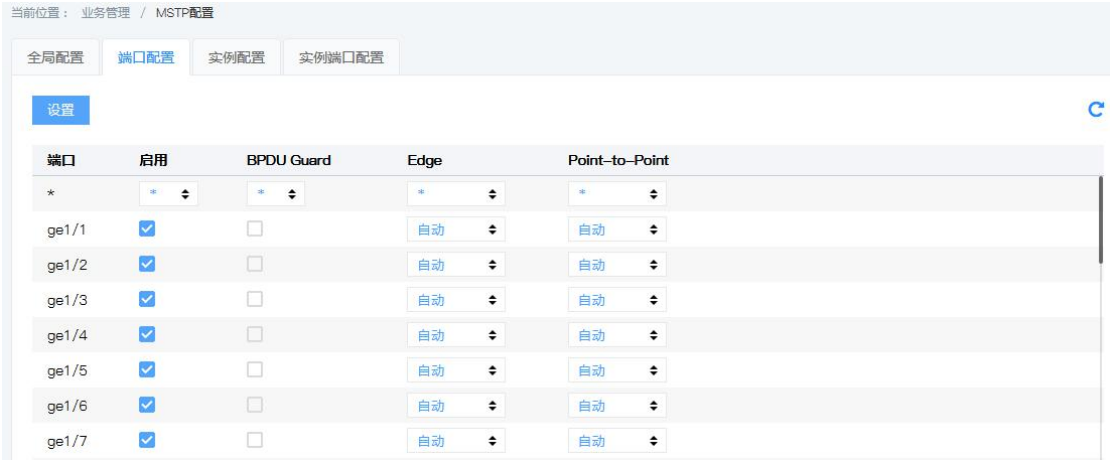
2. 填写相应的配置项。

3.单击“设置”，完成配置。

5.3.4 端口配置

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“业务管理 > MSTP 配置 > 端口配置”菜单，进入“端口配置”界面如下图所示。



界面信息含义如下表所示。

配置项	说明
端口	不可选。端口列表
启用	单选。选择是否开启端口配置。有勾选和不勾选两种情况。默认是不勾选。
BPDU Guard	单选。选择是否开启 BPDU 的保护功能。有勾选和不勾选两种情况。默认是不勾选。当设备上启动 BPDU 保护功能，如果边缘接口收到了 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。
Edge	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。 选择 Force_True、Force_False 和自动。
Point-to-Point	选择 Force_True、Force_False 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。 Force-true 表示特定端口与点对点链路相连。 Force-false 表示特定端口没有与点对点链路相连。

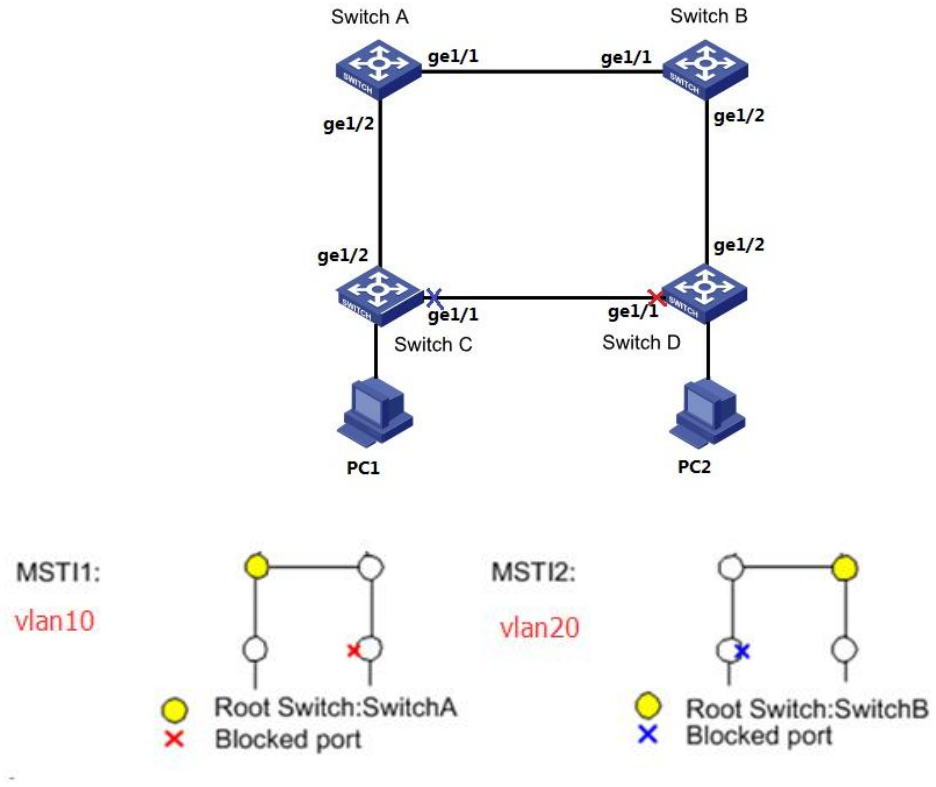
2. 填写相应的配置项。

3.单击“设置”，完成配置。

#示例说明

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。

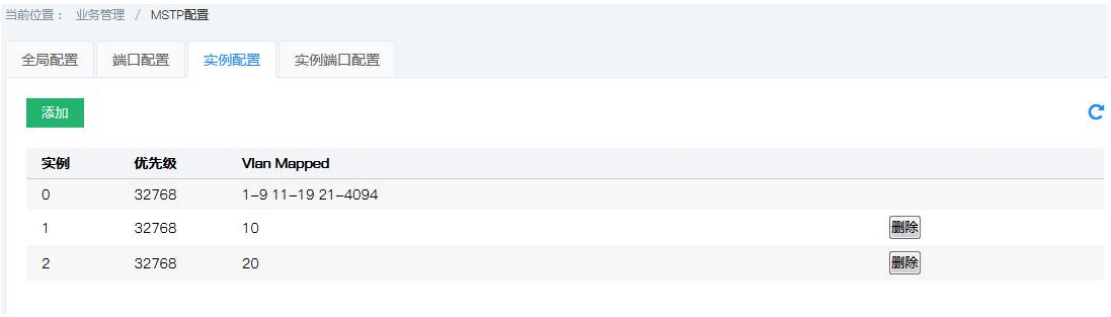


操作步骤

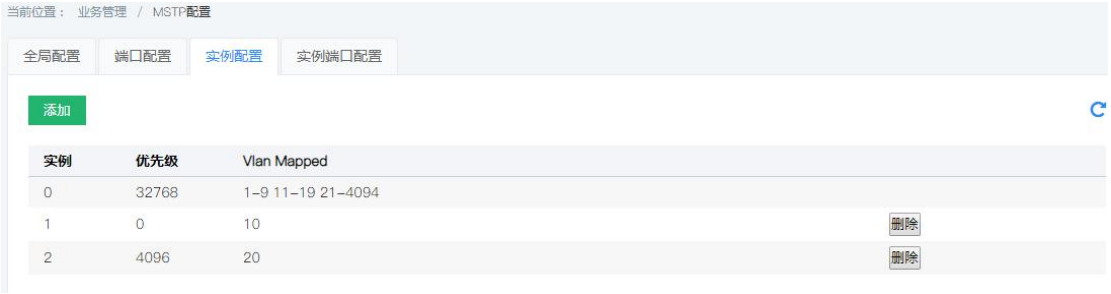
1. 将交换设备上接入环路中的端口加入 VLAN。单击导航树中的 “业务管理> VLAN 配置 >VLAN 配置”菜单，进入“VLAN 配置”界面，分别输入允许 VLAN10，VLAN20 通过 Trunk 口， Tag 端口列表中勾选 “ge1/1、ge1/2” 单击 “添加”，完成配置，

2.配置 SwitchA、SwitchB、SwitchC 和 SwitchD 到域名为 RUNDATA 的域内。单击导航树中的 “业务管理> MSTP 配置 > 全局配置” 菜单，进入 “全局配置”，填写相应配置，界面如下图所示。

3. 创建实例 MSTI1 和实例 MSTI2。单击导航树中的“业务管理 > MSTP 配置 > 实例配置”菜单，进入“实例配置”，填写相应参数，单击“添加”，界面如下图所示。



4. 在域 RUNDATA 内，配置 MSTI1 与 MSTI2 的根桥与备份根桥，配置 SwitchA 为 MSTI1 的根桥，配置 SwitchA 为 MSTI2 的备份根桥。单击导航树中的“业务管理 > MSTP 配置 > 实例配置”菜单，进入“实例配置”，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。

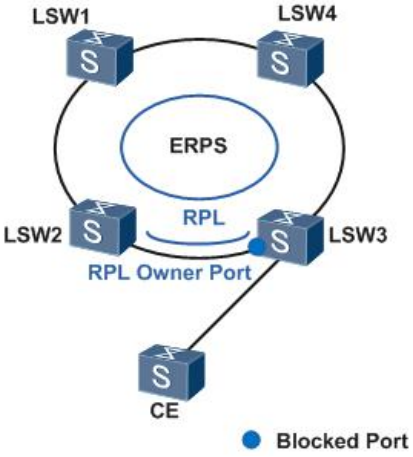
优先级必须是 4096 的倍数

5.在域 RUNDATA 内，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 4 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。

5.4 ERPS配置

ERPS（Ethernet Ring Protection Switching，以太环网保护倒换）是一个用于以太网链路层破除环路的协议。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 Discarding 之间切换，达到消除环路的目的。同时我们利用控制 VLAN、数据 VLAN 和保护实例等机制，以更好地实现 ERPS 的功能。

如下图所示，CE 接入 LSW1—LSW4 组成的环形网络。这样的接入方式可使网络具备一定的可靠性，但为了消除网络中的环路，有效地保证链路连通性，需要启动一种环路破除机制。



端口角色

ERPS 协议中规定的端口角色主要有 RPL owner 端口、RPL neighbour 端口和普通端口三种类型。其中 RPL neighbour 端口类型只有 ERPSv2 版本支持，v1 版本不支持。

- RPL owner 端口

一个 ERPS 环只有一个 RPL owner，由用户配置决定，通过阻塞 RPL owner 端口来防止 ERPS 环中产生环路。
当 RPL owner 所在设备收到故障报文得知 ERPS 环上其他节点或链路故障时，会自动放开 RPL owner 端口，此端口恢复流量的接收和发送，保证流量不会中断。
RPL owner 所在的链路即为环保护链路 RPL（Ring Protection Link）。

- RPL neighbour 端口

RPL neighbour 端口指的是与 RPL owner 端口直接相连的端口。
正常情况下，RPL owner 端口和 RPL neighbour 端口都会被阻塞，以防止环路产生。
当 ERPS 环出现故障时，RPL owner 端口和 RPL neighbour 端口都会被放开。
引入 RPL neighbour 端口角色可以减少 RPL neighbour 端口所在设备刷新 FDB 表项的次数。

- 普通端口

在 ERPS 环中，除 RPL owner 和 RPL neighbour 以外的端口都是普通端口。
普通端口负责监测自己直连的 ERPS 协议的链路状态，并把链路状态的变化消息及时通

知其他端口。

控制 VLAN

在 ERPS 环中，控制 VLAN 用来传递 ERPS 协议报文。

每个 ERPS 环必须配置控制 VLAN。当端口加入已经配置控制 VLAN 的 ERPS 环后，端口将自动加入控制 VLAN。

不同 ERPS 环不能使用相同 ID 的控制 VLAN。

与控制 VLAN 相对，数据 VLAN 用来传递数据报文。

5.4.1 ERPS配置信息显示

操作步骤

1.单击导航树中的“业务管理 > ERPS 配置 ”菜单，进入“ERPS 配置”界面如下图所示。

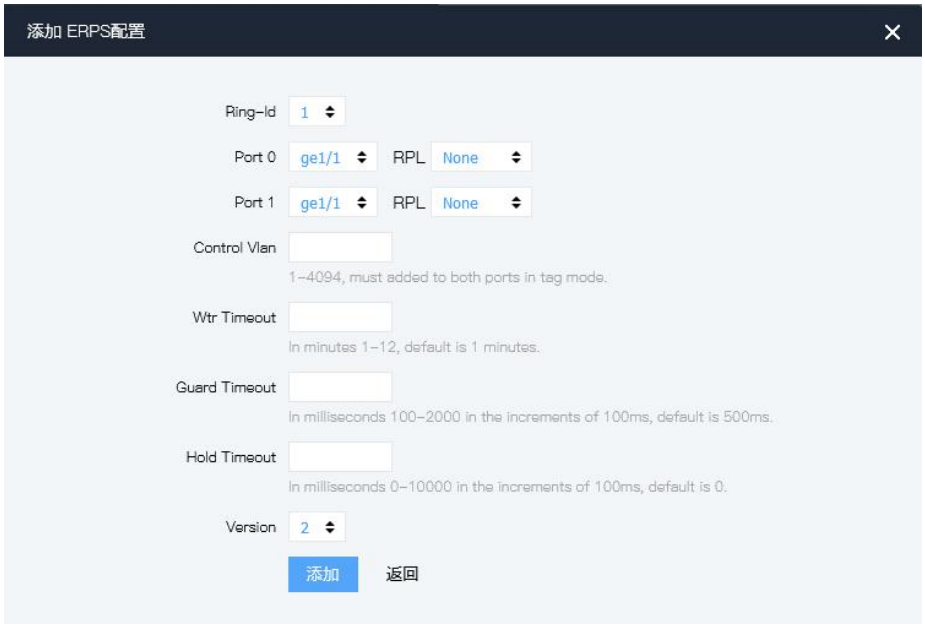
界面信息含义如下表所示。

配置项	说明
Ring- Id	ERPS 环 ID
Ring 状态	ERPS 环状态（protected,idle, PENDING）

5.4.2 添加ERPS

操作步骤

1.单击导航树中的“业务管理 > ERPS 配置 ”菜单，点击“添加 ERPS”界面如下图所示。



界面信息含义如下表所示。

配置项	说明
Ring- Id	ERPS 环 ID
端口角色	RPL Neighbor\Owner\none
Control vlan	控制 VLAN
Wtr Timeout	当 RPL owner 端口由于其他设备或链路故障而被放开后，如果故障恢复，而有的端口可能还未由 Down 状态变为 Up 状态，为了防止立即阻塞 RPL owner 端口而引起阻塞点震荡，当 RPL owner 端口收到某端口的 NR RAPS 报文后，启动 WTR Timer，如果在定时器未超时前收到其他端口的 SF RAPS 报文，关闭 WTR Timer。如果在 WTR Timer 超时前始终没有收到其他端口的 SF RAPS 报文，则当 WTR Timer 超时后，阻塞 RPL owner 端口，发送 NRRB RAPS 报文。其他端口在收到该报文后，再将自己端口的转发状态设置为 Forwarding 状态。
Guard Timeout	链路故障或节点故障所涉及到的设备在故障恢复或执行清除操作后，向其他设备发送 NR RAPS 报文，并同时启动 Guard Timer，在该定时器超时前不处理 RAPS 报文，目的是防止收到过期的 NR RAPS 报文。如果定时器超时后还能收到其他端口发送的 NR 报文，则本端口的转发状态变为 Forwarding 状态。
Hold Timeout	对于运行 ERPS 的二层网络，保护倒换的顺序可能会有不同的要求，例如：多层业务的应用中，服务器出现故障后，用户可能会希望能有一段时间恢复服务器的故障，而客户端感知不到，即不会立即进行保护倒换。可设置合适的 Holdoff Timer

	定时器，当发生故障时，故障并不会立即上报 ERPS，而只有当 Holdoff Timer 定时器超时后，如果故障仍未能恢复才会上报。
Version	版本 V2、V1

5.5 A-Ring管理

5.5.1 概述

5.5.1.1 节点类型

一个 A-RING 环物理上对应一个环形连接的以太网拓扑。A-RING 环的角色由用户通过管理决定。

5.5.1.1.1 主节点

主节点是 A-RING 环上的主要决策和控制节点。每个 A-RING 环上必须有一个主节点，而且只能有一个。

以太网环上每一台交换机都称为一个节点，每个 A-RING 环上必须有一个主节点，而且只能有一个。主节点是 Polling 机制（环网状态主动检测机制）的发起者，也是网络拓扑发生改变后执行操作的决策者。

主节点周期性的从其主端口发送 HELLO（健康检测报文）报文，依次经过各传输节点在环上传播。如果从主节点副端口能够收到自己发送的 HELLO 报文，说明环网链路完整；如果在规定时间内收不到 HELLO 报文，就认为环网发生链路故障。

主节点有如下 2 种状态：

1) Complete State（完整状态）

当环网上所有的链路都处于 UP 状态，主节点可以从副端口收到自己发送的 HELLO 报文，就说主节点处于 Complete 状态。主节点的状态即反映了 A-RING 环的状态，因此 A-RING 环也处于 Complete 状态，此时主节点会阻塞副端口以防止数据报文在环形拓扑上形成广播环路。

2) Failed State（故障状态）

当环网上存在链路处于 Down 状态时，则主节点将处于 Failed 状态，此时主节点放开副端口以保证环网上各节点通信不被中断。

5.5.1.1.2 传输节点

环上除主节点之外的其它节点都可以称为传输节点。一个 A-RING 环上可以有多个传输节点，也可以没有传输节点（事实上这样的组网没有实际意义）。

每一个 A-RING 环物理上对应一个环形连接的以太网拓扑，A-RING 环同样由整数表示的 ID 来标识。

A-RING 环上除主节点外的所有其它节点都是传输节点。传输节点负责监测自己的直连 A-RING 链路的状态，并把链路变化通知主节点，然后由主节点来决策如何处理。传输节点有如下 3 种状态：

1) Link-Up State（UP 状态）

传输节点的主端口和副端口都处于 UP 状态时，就说传输节点处于 Link-Up 状态。
2) Link-Down State（Down 状态）

传输节点的主端口或副端口处于 Down 状态时，就说传输节点处于 Link-Down 状态。
3) Preforwarding State（临时阻塞状态）

传输节点的主端口或副端口处于阻塞状态时，就说传输节点处于 Preforwarding 状态。处于 Link-Up 状态的传输节点检测到主端口或者副端口发生链路 Down 时，就从 Link-Up 迁移到 Link-Down 状态，并通过发送 Link-Down 报文通知主节点。
传输节点不从 Link-Down 状态直接迁移回 Link-Up 状态。当处于 Link-Down 状态的传输节点某端口发生链路 Up，并且由此主端口和副端口都恢复成 Up 状态，传输节点迁移到 Preforwarding 状态，并阻塞恢复的端口。传输节点主、副端口都恢复的瞬间，主节点还不能马上知道这一信息，因此其副端口还处于放开状态，如果传输节点立即迁移回 Link-Up 状态，势必造成数据报文在环网上形成广播环路，因此传输节点从 Link-Down 先迁移到 Preforwarding 状态。
当处于 Preforwarding 状态的传输节点收到主节点发送的 COMPLETE-FLUSH-FDB 报文时，将迁移到 Link-Up 状态。如果 COMPLETE-FLUSH-FDB 报文在传输过程中不幸丢失，A-RING 协议还提供了一种备份机制来恢复临时阻塞的端口并触发状态切换，就是传输节点在规定的时间内收不到 COMPLETE-FLUSH-FDB 报文，自行迁移到 Link-Up 状态，并放开临时阻塞端口。

5.5.1.2 端口角色

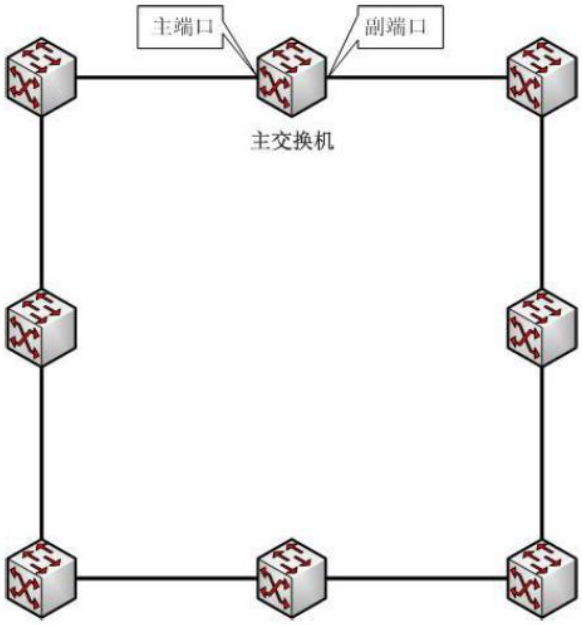
5.5.1.2.1 主端口和副端口

主节点和传输节点接入以太网环的两个端口中，一个为主端口，另一个为副端口，端口的角色由用户的管理决定。
主节点的主端口和副端口在功能上是有区别的。主节点从其主端口发送环路状态探测报文，如果能够从副端口收到该报文，说明本节点所在 A-RING 环网完整，因此需要阻塞副端口以防止数据环路；相反如果在规定时间内收不到探测报文，说明环网故障，此时需要放开副端口以保证环上所有节点的正常通信。传输节点的主端口和副端口在功能上没有区别。端口的角色同样由用户的管理决定。

5.5.1.3 拓扑类型

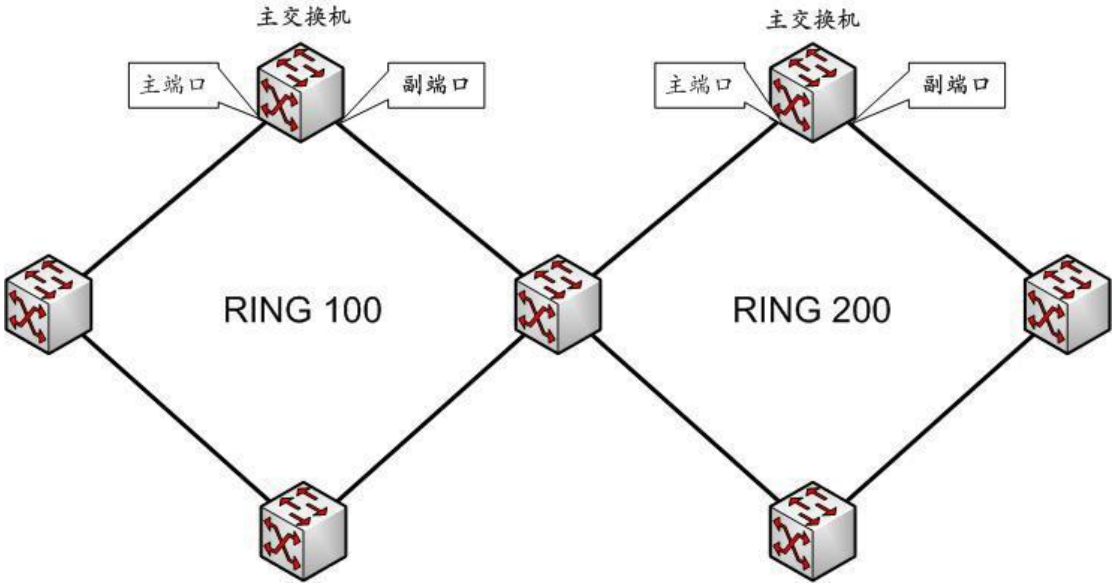
5.5.3.1 单环

一个 A-RING 环物理上对应一个环形连接的以太网拓扑，该环形拓扑中存在一个主交换机，而且只能有一个，该主交换机是 Polling 机制（环网状态主动检测机制）的发起者，也是网络拓扑发生改变后执行操作的决策者。在使用时分为静态模式和动态模式。静态模式在管理时已经确定主交换机的位置，不管拓扑怎么变化，主机始终不变，这种模式在链路恢复时也有自愈时间。动态模式在管理时所有交换机的地位平等，在环网形成后，系统自动确定环网中的某个交换机为主交换机，而且，主交换机会随拓扑的变化而改变位置，这种模式在链路恢复时的自愈时间为零。 典型拓扑图如下：

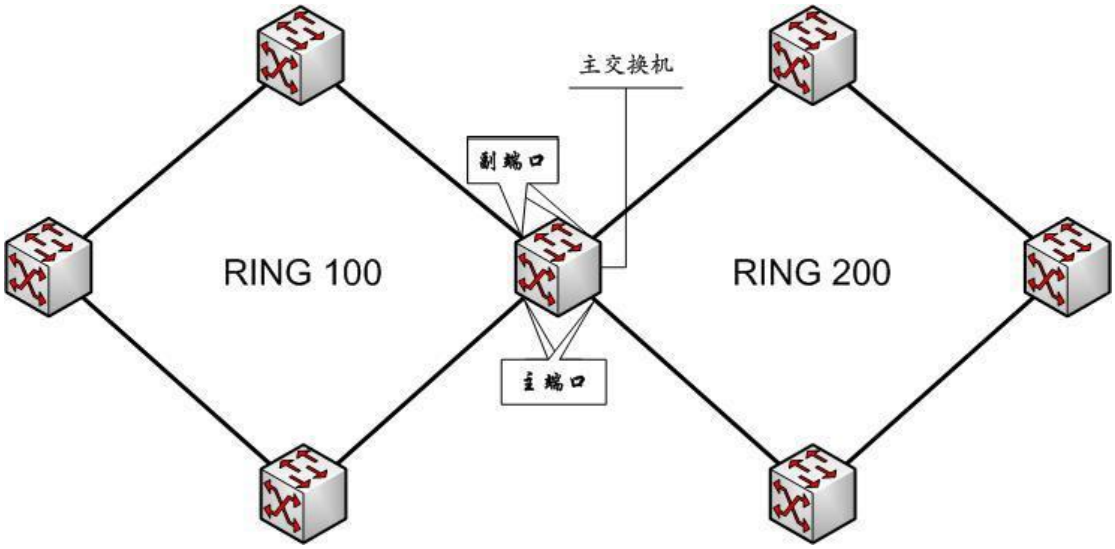


5.5.3.2 相切环

相切环即是两个或以上 A-RING 有一个公共的交换机，但不存在公共的端口。相切环中的各 A-RING 均遵循单环机制，互不影响。管理上和单环管理基本一致，不同的是需要在公共交换机上管理多个 A-RING。 典型拓扑图如下：



相切在传输节点的相切环



相切在主节点的相切环

5.5.1.4 消息类型

1. HEALTH(HELLO)

健康检测报文，由主节点发起，对网络进行环路完整性检测。

2. LINK-UP

链路 UP 报文，由发生直连链路状态 UP 的传输节点、边缘节点或者辅助边缘节点发起，通知主节点环路上有链路恢复。

3. LINK-DOWN

链路 DOWN 报文，由发生直连链路状态 DOWN 的传输节点、边缘节点或者辅助边缘节点发起，通知主节点环路上有链路 DOWN，物理环路消失。

4. A_CONF_COMM_FD_FDB

刷新 FDB 报文，由主节点发起，通知传输节点、边缘节点或者辅助边缘节点更新各自 MAC 地址转发表。

5. A_CONF_CPLT_FLD_FDB

环网恢复刷新 FDB 报文，由主节点发起，通知传输节点、边缘节点或者辅助边缘节点更新各自 MAC 地址转发表，同时通知传输节点放开临时阻塞端口。

6. UTR_FLAGS_FAULT

边缘节点与辅助边缘节点间的通道中断时，辅助边缘节点将该消息通知边缘节点，边缘节点收到后将阻塞对应的边缘端口，并通知该环的主节点打开其副端口。

7. UTR_FLAGS_RING_DETECT

该消息用于检测相交环整个拓扑是否存在环路，边缘节点与辅助边缘节点间的通道中断时，辅助边缘节点定时的将该消息通过各环发往边缘节点，边缘节点收到该消息后判断是否存在环路，若存在则阻塞相应边缘端口。

边缘节点与辅助边缘节点间的通道中断时，各环主节点将收不到自己发出的Hello报文，

于是 Fail 定时器超时，各环主节点迁移到 Failed 状态，放开副端口，
所有环的主节点副端口放开，各环之间势必形成广播环路，为了消除这一缺陷，引入了通道状态检测机制，这一机制需要边缘节点和辅助边缘节点配合完成，目的就是在各环主节点副端口放开之前，阻塞边缘节点的边缘端口，从而避免各环间形成数据环路。
边缘节点与辅助边缘节点间的通道连通时，按照单环机制进行收敛，并打开各阻塞的边缘端口。
8. UTR_FLAGS_YOUWORK

当主或备份链路断开时发送消息给对方，通知对方打开链路。收到此消息，无论主备都无条件打开对应端口。
9. UTR_FLAGS_MEWORK

当主或备份链路网口 up 时发送该消息给对方，如果接收方是主链路且处于转发状态，则不回应此消息，如果处于断开状态则回应 UTR_FLAGS_YOUWORK 消息。如果接收方是备份链路且处于转发状态，立即阻塞自己并回应 UTR_FLAGS_YOUWORK 消息，如果处于断开状态则直接回应 UTR_FLAGS_YOUWORK 消息。
10. UTR_FLAGS_LINKHELLO

此消息用于主备链路之间循环探测，当主链路处于正常工作状态时，间隔的在 A_ring 环中发送此消息，备份链路收到则将自己从其他状态设置为阻塞状态，如果在一定的时间内没有收到则打开备份链路。

5.5.2 静态环网管理

1.单击导航树中的“业务管理 > A-Ring 管理 ”菜单，进入“A-Ring 管理”界面如下图所示。

界面信息含义如下表所示。

查询项	说明
环网类型	动态环网和静态环网。动态环网表示主交换机不确定，随拓扑的变化而变化，主要特点是当链路恢复时不需要收敛时间。静态环网主要特点是不管拓扑怎么变化，主交换机是确定不变的，但链路恢复时需要收敛时间。
ring ID	环网的编号，环与环之间可以根据 ring ID 进行区别，其范围为 1~16
端口成员 1	环网的第一个端口成员，每个环的成员最多包括两个端口，每个交换机可以有多个环。
端口成员 2	环网的第二个端口成员
系统类型	系统类型分为 Transfer（传输节点）、Master（主节点）

节点角色	端口成员的类型根据系统类型改变而改变，当系统为 Master 时，其成员的类型为 Master 和 Subsidiary；当系统为 Transfer 时，其成员的类型为 None；

2. 点击“添加”填写相应的管理项。
3.单击“设置”，完成管理。

5.5.3 动态环网管理

1.单击导航树中的“业务管理 > A-Ring 管理 ”菜单，进入“ A-Ring 管理”界面如下图所示。

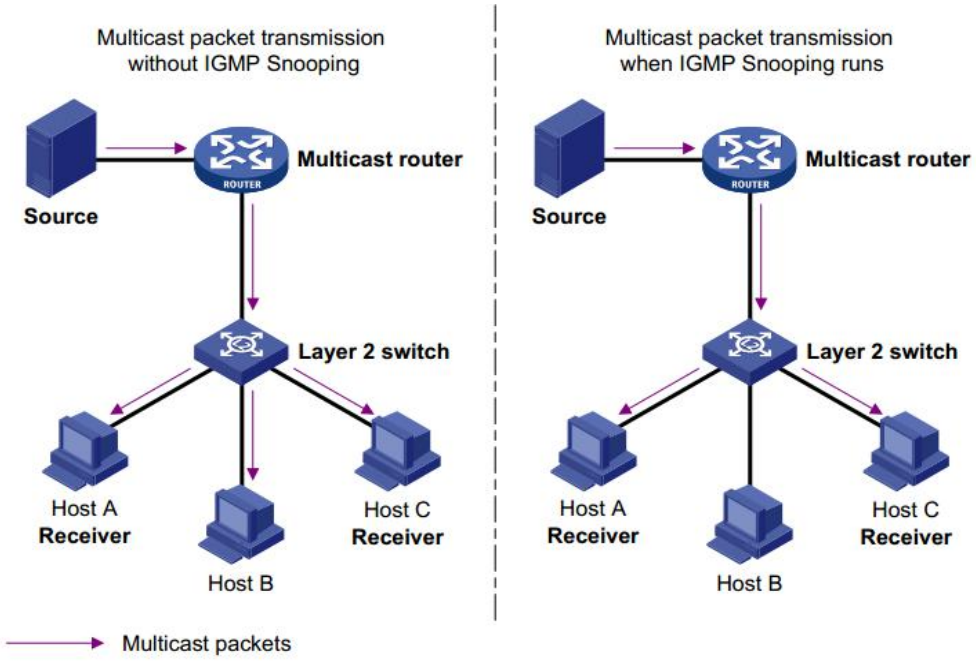
2. 点击“添加”填写相应的管理项。
3.单击“设置”，完成管理。

5.6 二层组播配置

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。



5.6.1 IGMP-snooping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“业务管理 >二层组播配置 > IGMP-snooping 配置”菜单，进入“IGMP-snooping 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
启用 IGMP-snooping 配置	全局去使能 IGMP Snooping 的情况下，是不能在 VLAN 下配置 IGMP Snooping 的。 单选，分为使能和去使能两种状态。默认是去使能。
主机老化时间	当一个端口加入某组播组时，交换机为该端口启动一个定时器，其超时时间为主机端口老化时间。超时后，交换机将该端口从组播组的转发表中删除。该值取值范围为 200-1000 秒，缺省值为 260 秒。

2.填写相应的配置项。

3.单击“设置”，完成配置。

5.6.2 静态组播

基于以往的组播点播方式，当处于不同 VLAN 的用户点播同一个组播组时，数据在组播路由器上会为每个包含接收者的 VLAN 进行复制和转发。 这样的组播点播方式，浪费了大量的带宽。 在启动了 IGMP Snooping 功能后，通过配置组播 VLAN 的方式，将交换机的端口加入到组播 VLAN，使不同 VLAN 内的用户共用一个组播 VLAN 接收组播数据，组播流只在一个组播 VLAN 内进行传输，从而节省了带宽。而且由于组播 VLAN 与用户。VLAN 完全隔离，安全和带宽都得以保证。

操作步骤

1.单击导航树中的“业务管理 > 二层组播配置 > 静态组播”菜单，进入“静态组播”界面如下图所示。

界面信息含义如下表所示。

配置项	说明
Vlan Id	固定的，根据用户选择的数据而固定 说明：保证 VLAN 已经创建。输入一个已创建好的 VLAN
组播源	输入组播源地址
组播地址	输入组播地址
端口列表	加入组播成员，可以多选

2.填写相应的配置项。

3.单击“设置”，完成配置，如下图。

5.6.3 IGMP-Snooping group列表

1.单击导航树中的“业务管理 > 二层组播配置 > IGMP-Snooping 配置 > IGMP-Snooping group 列表”菜单，进入“IGMP-Snooping group 列表”界面如下图所示。

2.选择相应的接口，单击“清除”即可。

5.6.4 VLAN设置

操作步骤

1.单击导航树中的“二层组播配置 > IGMP-snooping 配置 > VLAN 设置”菜单，进入“VLAN 设置”界面如下图所示。

界面信息含义如下表所示。

配置项	说明
Vlan Id	固定的，根据用户选择的数据而固定 说明：保证 VLAN 已经创建。输入一个已创建好的 VLAN
快速离开组播	启用/禁用快速离开组播。启用显示 1，禁用显示为 0
查询报文间隔	范围值为 2-1800 秒

2.填写相应的配置项。

3.单击“设置”，完成配置，如下图。

5.6.5 端口绑定

操作步骤

1. 单击导航树中的“业务管理 > DHCP-snooping 配置 >端口绑定”菜单，进入“全局配置”界面如下图所示。

界面含义如下表所示：

配置项	说明
DHCP Pool	固定值。已创建好的地址池。
IP 地址	用户的静态 IP 地址
端口	映射交换机端口

2.填写相应的配置项。

3.单击“添加”，完成配置，如下图。

5.6.6 静态客户端配置

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。

为了满足特定的设备（如服务器）需要固定的 IP 地址，可以采取静态客户端配置。

操作步骤：

1.单击导航树中的“业务管理> DHCP Server 配置>静态客户端配置”菜单，进入“静态客户端配置”界面，如下图所示。

界面含义说明如下表：

配置项	说明
DHCP Pool	固定值。已创建好的地址池。
IP 地址	输入需要绑定的 IP 地址。
MAC 地址	输入需要绑定的 MAC 地址

5.6.7 客户端列表

查看客户端 IP 地址列表操作步骤

1.单击导航树中的“业务管理> DHCP Server 配置>客户端列表”菜单，进入“客户端列表”界面，如下图所示。

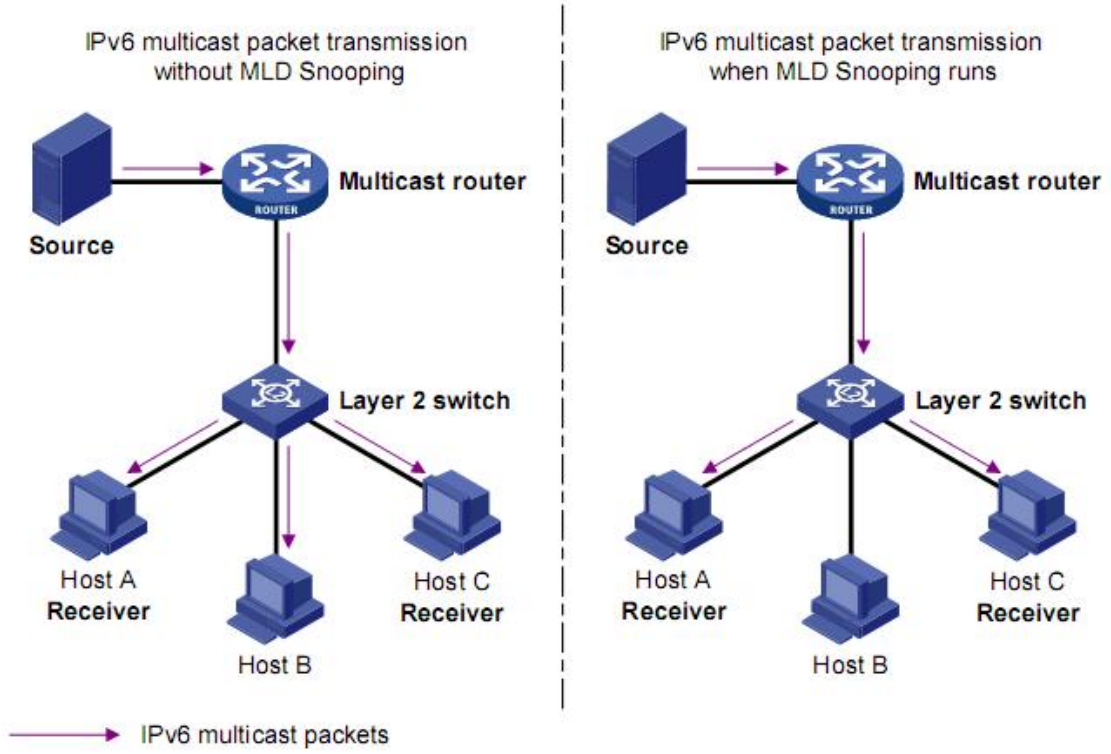
5.7 MLD-Snooping

MLD Snooping 是 Multicast Listener Discovery Snooping （组播侦听者发现协议窥探）的简称。它是运行在二层设备上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组。

5.7.1 MLD Snooping原理

运行 MLD Snooping 的二层设备通过对收到的 MLD 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 IPv6 组播数据。

如下图所示，当二层设备没有运行 MLD Snooping 时，IPv6 组播数据报文在二层被广播；当二层设备运行了 MLD Snooping 后，已知 IPv6 组播组的组播数据报文不会在二层被广播，而在二层被组播给指定的接收者。



二层设备运行 MLD Snooping 前后的对比

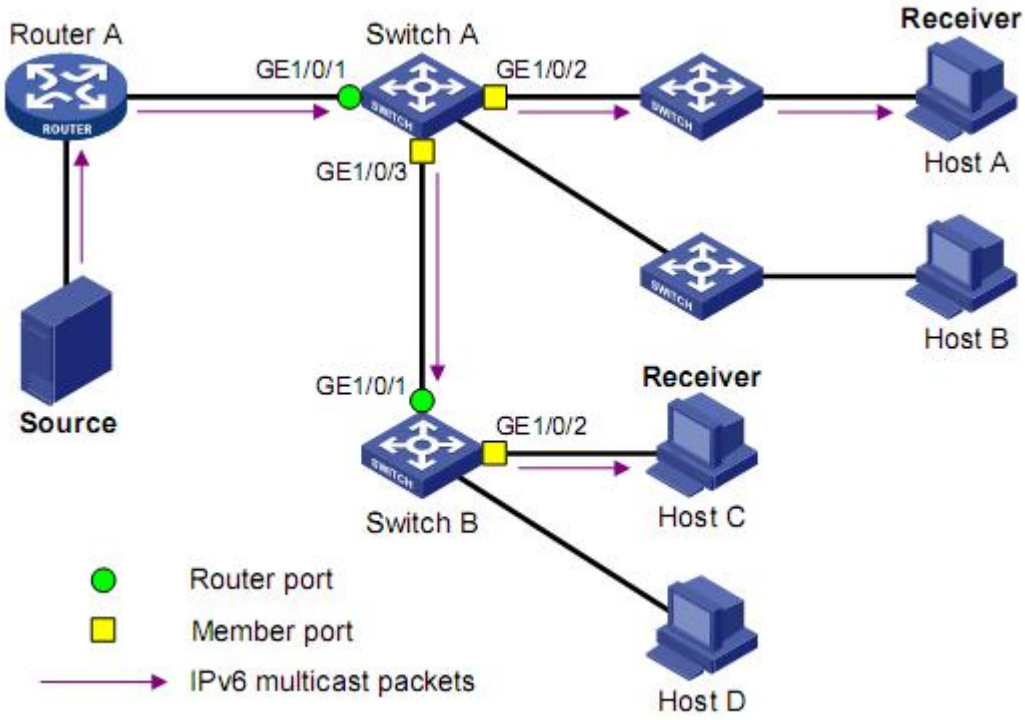
MLD Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

- 减少了二层网络中的广播报文，节约了网络带宽；
- 增强了 IPv6 组播信息的安全性；
- 为实现对每台主机的单独计费带来了方便。

5.7.2 MLD Snooping基本概念

1. MLD Snooping 相关端口

如下图所示，Router A 连接组播源，在 Switch A 和 Switch B 上分别运行 MLD Snooping 。Host A 和 Host C 为接收者主机（即 IPv6 组播组成员）。



结合上图，介绍一下 MLD Snooping 相关的端口概念：

路由器端口（Router Port）：交换机上朝向三层组播设备（DR 或 MLD 查询器）一侧的端口，如 Switch A 和 Switch B 各自的 GigabitEthernet1/0/1 端口。交换机将本设备上的所有路由器端口都记录在路由器端口列表中。

成员端口（Member Port）：又称 IPv6 组播组成员端口，表示交换机上朝向 IPv6 组播

组成员一侧的端口，如 Switch A 的 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 端口，以及 SwitchB 的 GigabitEthernet1/0/2 端口。交换机将本设备上的所有成员端口都记录在 MLD Snooping 转发表中。

5.7.3 MLD Snooping工作机制

运行了 MLD Snooping 的交换机对不同 MLD 动作的具体处理方式如下：

1. 普遍组查询

MLD 查询器定期向本地网段内的所有主机与路由器（FF02::1）发送 MLD 普遍组查询报文，以查询该网段有哪些 IPv6 组播组的成员。

在收到 MLD 普遍组查询报文时，交换机将其通过 VLAN 内除接收端口以外的其它所有端口转发出去，并对该报文的接收端口做如下处理：

- 如果在路由器端口列表中已包含该动态路由器端口，则重置其老化定时器。
- 如果在路由器端口列表中尚未包含该动态路由器端口，则将其添加到路由器端口列表中，并启动其老化定时器。

2. 报告成员关系

以下情况，主机会向 MLD 查询器发送 MLD 成员关系报告报文：

- 当 IPv6 组播组的成员主机收到 MLD 查询报文后，会回复 MLD 成员关系报告报文。
- 如果主机要加入某个 IPv6 组播组，它会主动向 MLD 查询器发送 MLD 成员关系报告报文以声明加入该 IPv6 组播组。

在收到 MLD 成员关系报告报文时，交换机将其通过 VLAN 内的所有路由器端口转发出去，从该报
文中解析出主机要加入的 IPv6 组播组地址，并对该报文的接收端口做如下处理：

- 如果不存在该 IPv6 组播组所对应的转发表项，则创建转发表项，将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；
- 如果已存在该 IPv6 组播组所对应的转发表项，但其出端口列表中不包含该端口，则将该端口作为动态成员端口添加到出端口列表中，并启动其老化定时器；

如果已存在该 IPv6 组播组所对应的转发表项，且其出端口列表中已包含该动态成员端口，则重置其老化定时器。

3. 离开组播组

当主机离开 IPv6 组播组时，会通过发送 MLD 离开组报文，以通知组播路由器自己离开了某个 IPv6
组播组。当交换机从某动态成员端口上收到 MLD 离开组报文时，首先判断要离开的 IPv6 组播组所
对应的转发表项是否存在，以及该 IPv6 组播组所对应转发表项的出端口列表中是否包含该接收端口：

- 如果不存在该 IPv6 组播组对应的转发表项，或者该 IPv6 组播组对应转发表项的出端口列表中不包含该端口，交换机不会向任何端口转发该报文，而将其直接丢弃；
- 如果存在该 IPv6 组播组对应的转发表项，且该 IPv6 组播组对应转发表项的出端口列表中包含该端口，交换机会将该报文通过 VLAN 内的所有路由器端口转发出去。同时，由于并不知道该接收端口下是否还有该 IPv6 组播组的其它成员，所以交换机不会立刻把该端口从该 IPv6 组播组所对应转发表项的出端口列表中删除，而是重置其老化定时器。

当 MLD 查询器收到 MLD 离开组报文后，从中解析出主机要离开的 IPv6 组播组的地址，并通过接收端口向该 IPv6 组播组发送 MLD 特定组查询报文。交换机在收到 MLD 特定组查询报文后，将其通过 VLAN 内的所有路由器端口和该 IPv6 组播组的所有成员端口转发出去。对于 MLD 离开组报文的接收端口（假定为动态成员端口），交换机在其老化时间内：

- 如果从该端口收到了主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下还有该 IPv6 组播组的成员，于是重置其老化定时器；
- 如果没有从该端口收到主机响应该特定组查询的 MLD 成员关系报告报文，则表示该端口下已没有该 IPv6 组播组的成员，则在其老化时间超时后，将其从该 IPv6 组播组所对应转发表项的出端口列表中删除。

5.7.4 MLD-Snooping配置

操作步骤

1.单击导航栏中"业务管理> MLD-Snooping 配置"菜单，进入"MLD-Snooping 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
启用 MLD-Snooping 配置	全局去使能 MLD-Snooping 的情况下，是不能在 VLAN 下配置 MLD-Snooping 的。 单选，分为使能和去使能两种状态。默认是去使能。
主机老化时间	当一个端口加入某组播组时，交换机为该端口启动一个定时器，其超时时间为主机端口老化时间。超时后，交换机将该端口从组播组的转发表中删除。该值取值范围为 200-1000 秒，缺省值为 260 秒。

2.填写相应的配置项。

3.单击“设置”，完成配置。

5.7.5 静态组播

基于以往的组播点播方式，当处于不同 VLAN 的用户点播同一个组播组时，数据在组播路由器上会为每个包含接收者的 VLAN 进行复制和转发。 这样的组播点播方式，浪费了大量的带宽。 在启动了 MLD-Snooping 功能后，通过配置组播 VLAN 的方式，将交换机的端口加入到组播 VLAN，使不同 VLAN 内的用户共用一个组播 VLAN 接收组播数据，组播流只在一个组播 VLAN 内进行传输，从而节省了带宽。而且由于组播 VLAN 与用户。VLAN 完全隔离，安全和带宽都得以保证。

操作步骤

1.单击导航树中的“业务管理 > MLD-Snooping > 静态 IP 组播”菜单，进入“静态 IP 组播”界面如下图所示。

界面信息含义如下表所示。

配置项	说明
Vlan Id	固定的，根据用户选择的数据而固定 说明：保证 VLAN 已经创建。输入一个已创建好的 VLAN
组播源	输入组播源地址
组播地址	输入组播地址
端口列表	加入组播成员，可以多选

2.点击“添加”填写相应的配置项。

3.单击“设置”，完成配置，如下图。

5.7.6 group列表

1.单击导航树中的“业务管理 > MLD-Snooping 配置 > group 列表”菜单，进入“group 列表”界面如下图所示。

2.选择相应的接口，单击“清除”即可。

5.7.7 VLAN设置

操作步骤

1.单击导航树中的“业务管理 > MLD-Snooping 配置 > VLAN 设置”菜单，进入“VLAN 设置”界面如下图所示。

界面信息含义如下表所示。

配置项	说明
Vlan Id	固定的，根据用户选择的数据而固定 说明：保证 VLAN 已经创建。输入一个已创建好的 VLAN
快速离开组播	启用/禁用快速离开组播。启用显示 1，禁用显示为 0

查询报文间隔	范围值为 2-1800 秒

2.点击“添加”填写相应的配置项。

3.单击“设置”，完成配置，如下图。

5.8 QOS配置

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 k bit/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，它尽最大的努力（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。

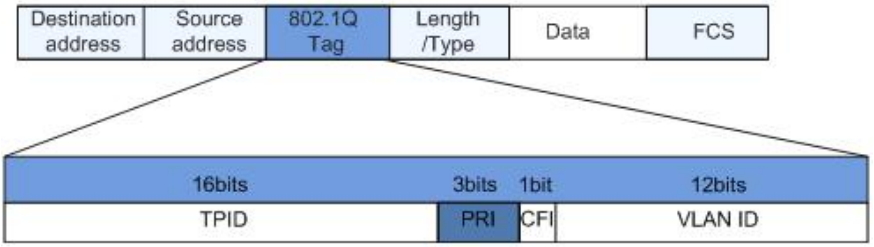
网络发展日新月异，随着 IP 网络上新应用的不断出现，对 IP 网络的服务质量也提出了新的要求。例如 VoIP 和视频等时延敏感业务对报文的传输时延提出了较高要求。如果报文传送延时太长，将是用户所不能接受的。为了支持具有不同服务需求的语音、视频以及数据等业务，要求网络能够区分出不同的业务类型，进而为之提供相应的服务。传统 IP 网络的尽力服务不可能识别和区分出网络中的各种业务类型，而具备业务类型的区分能力正是为不同的业务提供差异化服务的前提，所以传统网络的尽力服务模式已不能满足应用的需要。QoS 技术的出现便致力于解决这个问题。QoS 可以对网络流量进行调控，避免并管理网络拥塞，减少报文丢包率。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

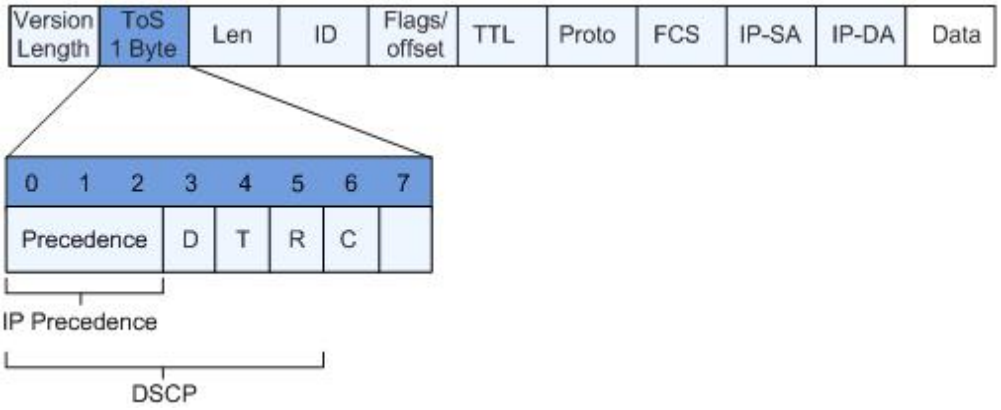


在 802.1Q 头部中包含 3 比特长的 PRI 字段。PRI 字段定义了 8 种业务优先级 CoS，按照优先级从高到低顺序取值为 7、6、……、1 和 0。

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）。

5.8.1 QOS全局配置

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）、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）。

配置接口调度类型操作步骤

1.单击导航树中的“业务管理> QOS 配置> 全局配置”菜单，进入“全局配置”界面，如下图所示。

界面含义如下表

配置项	说明
SP	SP 队列调度算法，是针对关键业务型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有 8 个输出队列为例，优先队列将端口的 8 个输出队列分成 8 类，依次为 7、6、5、4、3、2、1、0 队列，它们的优先级依次降低。
WRR	WRR 队列调度算法在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 8 个输出队列为例，WRR 可为每个队列配置一个加权值(queue7¯queue0 对应的加权值依次为 w7、w6、w5、w4、w3、w2、w1、w0)
DRR	DRR（Deficit Round Robin）调度同样也是 RR 的扩展，相对于 WRR 来言，解决了 WRR 只关心报文，同等调度机会下大尺寸报文获得的实际带宽要大于小尺寸报文获得的带宽的问题，通过调度过程中考虑了包长的因素，从而达到调度的速率公平性。
DSCP	范围 0-63
New DSCP	范围 0-63
Cos	范围 0-7
Queue	范围 0-7
Weight	权重值，范围是 0-100，使用于 WRR 和 DRR

5.8.2 QOS端口配置

QOS 端口配置端口配置操作步骤

1.单击导航树中的“业务管理> QOS 配置> 端口配置”菜单，进入“端口配置”界面，，单击“设置”，完成配置，如下图所示。

界面含义如下表

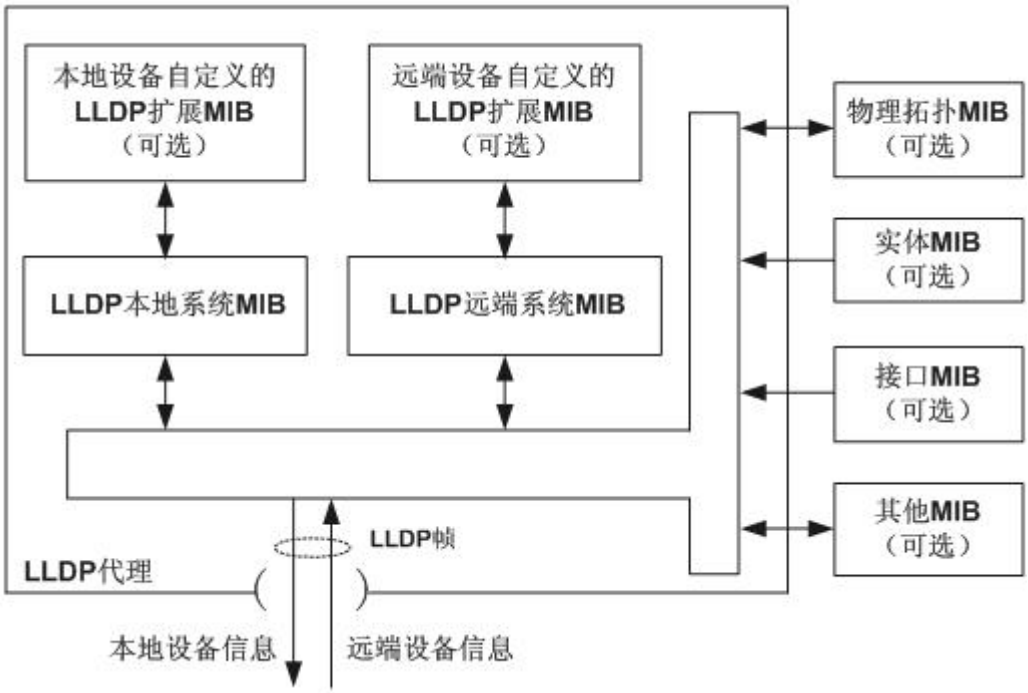
配置项	说明
端口	可选多个端口
默认 cos	范围 0-7

5.9 LLDP配置

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。

5.9.1 LLDP全局配置

操作步骤：

1.单击导航树中的“业务管理> LLDP 配置> 全局配置”菜单，进入“全局配置”界面，如下图所示。

界面含义如下表

配置项	说明
LLDP	单选。启用或禁用 LLDP 协议
发送周期	默认 30 秒，范围：5-65535 秒
重传时间	默认 120 秒，范围：5-65535 秒
发送间隔	默认 2 秒，范围：2-5 秒
重新启用延迟	默认 2 秒，范围：2-5 秒
TLV 可选发送	管理地址，端口描述、系统属性、系统描述、系统名字

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。

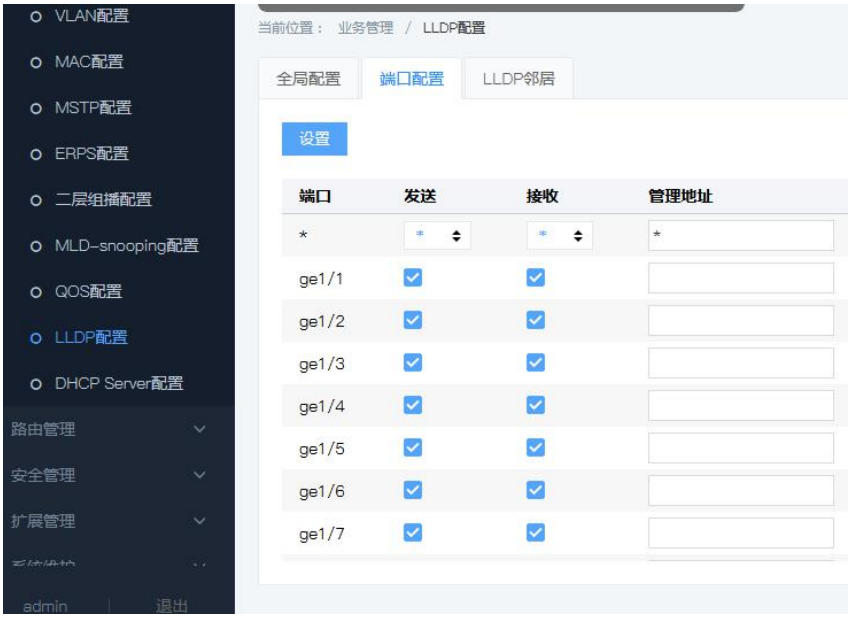
2.填写相应的配置项。

3.单击“添加”，完成配置。

5.9.2 端口配置

操作步骤

1.单击导航树中的“业务管理> LLDP 配置> 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
发送	发送 LLDP 报文
接收	接收 LLDP 报文
管理地址	输入本端交换机的 IP 地址。如 192.168.1.254

LLDP 有以下两种工作模式。TxRx：既发送也接收 LLDP 报文。Disable：既不发送也不接收 LLDP 报文。

2.配置既发送也接收 LLDP 报文，单击导航树中的“高级配置> LLDP 配置> 端口配置”菜单，进入“端口配置”界面，在 ge1/1 勾选“发送”，“接收”，输入本端交换机的 IP 地址，如 192.168.1.254。单击“设置”完成配置，如下图所示。

5.9.3 LLDP邻居

LLDP 邻居显示操作步骤

单击导航树中的“业务管理> LLDP 配置> LLDP 邻居”菜单，进入“LLDP 邻居”界面，如下图所示。

界面含义说明如下表

配置项	说明

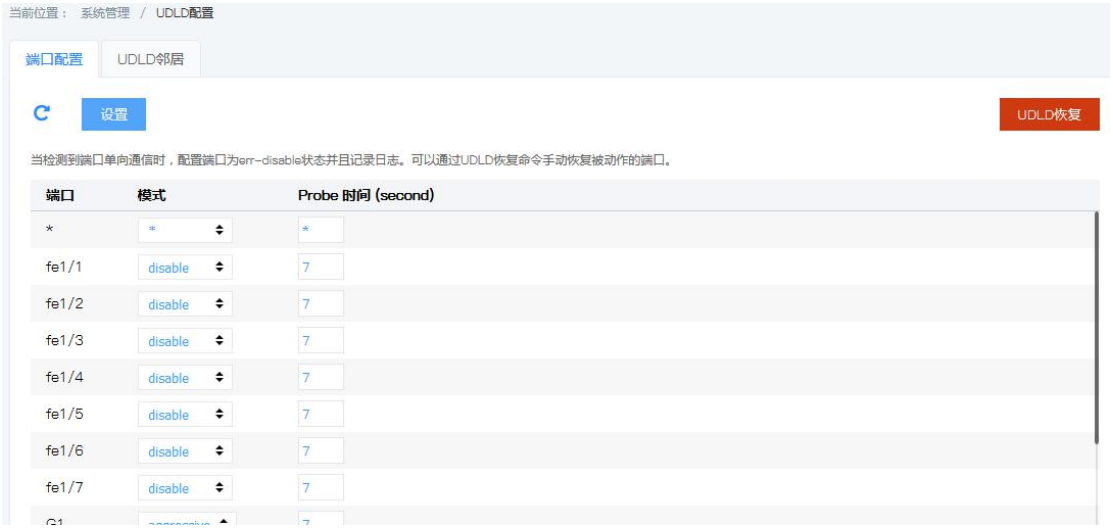
端口名称	可选择多个端口
启用	勾选或不勾选
ForwardAll	ForwardAll
Join 时间	通过定期发送新的 join 消息来刷新其成员身份，定期时间范围是 1-400000000，默认是 20
Leave 时间	工作站通过发送一个 leave 消息来退出一个组，如果退出消息丢失，则交换机仍认为该工作站仍希望保留在组内。退出消息保存时间范围是 1-400000000，默认是 60
Leave all 时间	在较长的一段时间之后，交换机发送一个 leave all 消息，声明如果它没有很快收到新的 join 消息，就将终止端口中所有的登记。时间范围是 1-400000000，默认是 60

5.10 UDLD配置

UDLD （UniDirectional Link Detection 单向链路检测）：用于监听利用光纤或双绞线连接的以太链路的物理配置的二层协议。当出现单向链路（只能向一个方向传输）时，UDLD 可以检测出这一状况，关闭相应接口并发送警告信息。

UDLD 支持两种工作模式；普通（normal）模式（默认）和激进（aggressive）模式。

单击导航树中的“业务管理>UDLD 配置”菜单，进入“UDLD 配置”界面，如下图所示。



界面含义说明如下表

配置项	说明
normal	UDLD 可以检测单向链路，并标记端口为 undetermined 状态产生系统日志
aggressive	UDLD 可以检测到由单向链路。并且会尝试重建链路，周期 7 秒的发送 UDLD message 探测包，如果此间没有任何的 UDLD echo 应答，此端口会被放置于 errdisable 状态

Probe 时间	探测时间

5.11 Link-flap配置

链路振荡是将物理状态频繁 Up/Down 变化的接口关闭，使之处于 Down 状态，这样网络拓扑结构将停止来回频繁变化。当链路在轮询间隔时间内发生动荡次数超过设置的阀值，将产生告警日志，并且将端口设置为 err-disable 状态。

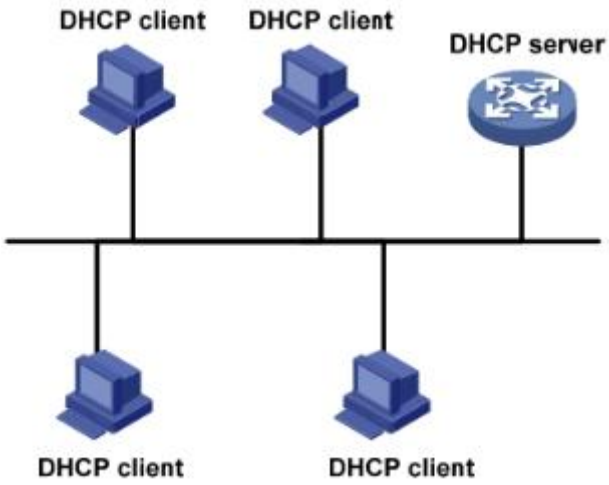
单击导航树中的“业务管理>Link-flap”菜单，进入“Link-flap 配置”界面，如下图所示。

界面含义说明如下表

配置项	说明
轮询间隔	系统需要统计单位时间内链路振荡的次数，单位时间记为链路振荡时间间隔
动荡阀值	接口状态 Up/Down 切换一次，记为一次链路振荡
恢复时间	接口 down 之后经过设置的恢复时间后可以 UP，0 为禁用

5.12 DHCP Server配置

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通常被应用在大型的局域网络环境中，主要作用是集中的管理、分配IP地址，使网络环境中的主机动态的获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。



5.12.1 DHCP IP 的地址分配

5.12.1.1 IP地址分配策略

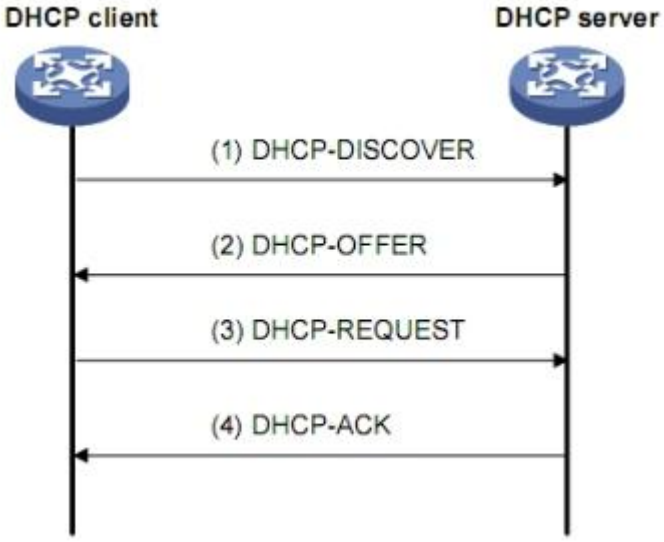
针对客户端的不同需求，DHCP 提供三种 IP 地址分配策略：

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 为客户端分配具有一定有效期限的 IP 地址，到达使用期限后，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。

5.12.1.2 IP地址动态获取过程



IP 地址动态获取过程

如上图所示，DHCP 客户端从 DHCP 服务器动态获取 IP 地址，主要通过四个阶段进行：

（1）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。

（2）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，根据 IP 地址分配的优先次序选出一个 IP 地址，与其他参数一起通过 DHCP-OFFER 报文发送给客户端。DHCP-OFFER 报文的发送方式由 DHCP-DISCOVER 报文中的 flag 字段决定。

（3）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，然后以广播方式发送 DHCP-REQUEST 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。

（4）确认阶段，即 DHCP 服务器确认 IP 地址的阶段。DHCP 服务器收到 DHCP 客户端发来的 DHCP-REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认将地址分配给该客户端，则返回 DHCP-ACK 报文；否则返回 DHCP-NAK 报文，表明地址不能分配给该客户端。

5.12.2 地址池配置

启用 DHCP Server

操作步骤

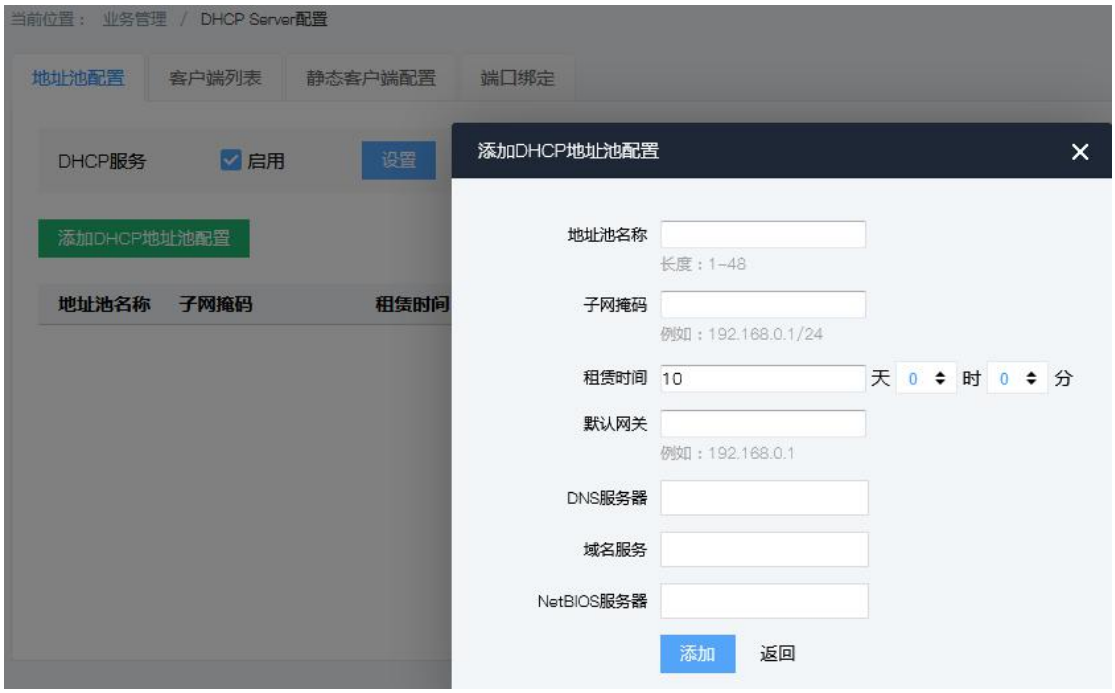
1.单击导航树中的“业务管理 > DHCP Server 配置 > 地址池配置”菜单，进入“全局配置”界面如下图所示。

界面含义说明如下表

配置项	含义
地址池名称	DHCP Server 中地址池的名称长度范围为 1~48
子网掩码	DHCP 客户端能自动获取到的 IP
租赁时间	DHCP 客户端能自动获取到的地址的有效时间。范围为 0-999 天
默认网关	DHCP 客户端能自动获取到的网关
DNS 地址	DHCP 客户端能自动获取到的 DNS 地址
域名服务	DHCP 客户端能自动获取到的域名
NetBIOS 服务器	DHCP 客户端能自动获取到的 NetBIOS 服务器地址

2.填写相应的配置项。

3.单击“设置”，完成配置，如下图。



6 路由管理

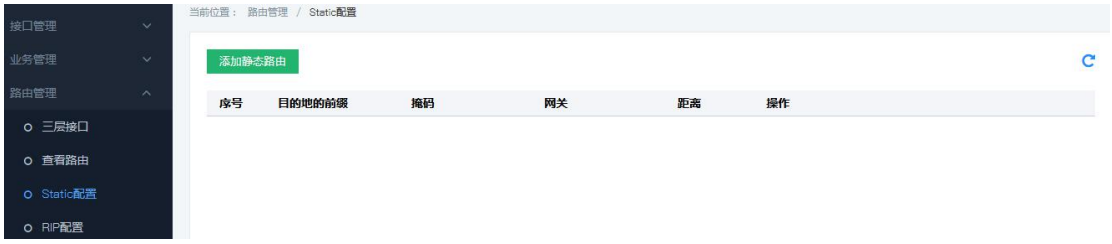
6.1 查看路由

6.2 Static配置

静态路由是由网络管理员手动设置的路由，在组网结构比较简单的网络中，网络管理员只需手工配置静态路由即可实现网络互通。静态路由一般在规模不大、拓扑结构固定的网络中配置。在网络中使用合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。当网络发生改变时则需要网络管理员再次修改配置参数以保证网络正常通信。

操作步骤

1.单击导航树中的“路由管理>Static 配置”菜单，进入“Static 配置”界面，如下图所示。



界面含义如下表

配置项	说明
目的地的前缀	设置路由条目需要到达的目标网络。
网关	设置通往目标网络的路由路径上下一个节点的 IP 地址。
距离	指定路由条目的管理距离。管理距离越小，优先级越高。

2.填写相应的配置项。

3.单击“添加”，完成配置，如下图所示。

6.3 ARP配置

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

在局域网中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报文必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。ARP 就是实现这个功能的协议。

设备通过 ARP 解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址到 MAC 地址的映射表项，以用于后续到同一目的地报文的转发。

ARP 表项分为动态 ARP 表项和静态 ARP 表项。

1. 动态 ARP 表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口 down 时会删除相应的动态 ARP 表项。

2. 静态 ARP 表项

静态 ARP 表项通过手工配置和维护，不会被老化，不会被动态 ARP 表项覆盖。

配置静态 ARP 表项可以增加通信的安全性。静态 ARP 表项可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

静态 ARP 表项分为长静态 ARP 表项、短静态 ARP 表项和多端口 ARP 表项。

在配置长静态 ARP 表项时，除了配置 IP 地址和 MAC 地址项外，还必须配置该 ARP 表项所在 VLAN 和出接口。长静态 ARP 表项可以直接用于报文转发。

在配置短静态 ARP 表项时，只需要配置 IP 地址和 MAC 地址项。如果出接口是三层以太网端口，短静态 ARP 表项可以直接用于报文转发；如果出接口是 VLAN 接口，短静态 ARP 表项不能直接用于报文转发，当要发送 IP 数据包时，先发送 ARP 请求报文，如果收到的响应报文中的源 IP 地址和源 MAC 地址与所配置的 IP 地址和 MAC 地址相同，则将接收 ARP 响应报文的接口加入该静态 ARP 表项中，之后就可以用于 IP 数据包的转发。

多端口 ARP 表项通过配置短静态 ARP 表项和组播 MAC 地址表项形成，当短静态 ARP 表项中的 MAC 地址与组播 MAC 地址表项中的 MAC 地址相同时，则生成多端口 ARP 表项。当设备要发送 IP 数据包时，多端口 ARP 表项将指导 IP 数据包从多个出端口发送。

6.3.1 查看ARP

操作步骤：

1.单击导航树中的“路由管理> ARP 配置”菜单，进入“查看 ARP”界面，如下图所示。

6.3.2 静态ARP

操作步骤：

1.单击导航树中的“路由管理> ARP 配置”菜单，进入“静态 ARP”界面，如下图所示。

配置项	说明

IP 地址	添加的静态 IP
Mac	IP 地址对应的 mac 地址

6.3.3 ARP老化时间

操作步骤:

1.单击导航树中的“路由管理> ARP 配置”菜单，进入“ARP 老化时间”界面，如下图所示。

配置项	说明
老化时间	取值范围 1-2147483 秒，默认为 600 秒

7 安全管理

7.1 访问控制

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。

下面对交换机制定过滤规则以及访问规则

操作步骤

1. 单击导航树中的“ 安全管理> 访问控制”菜单，进入“访问控制”界面如下图所示。

界面含义如下表：

配置项	子选项	说明
设置过滤规则	禁用	默认禁用
	凡符合下列规则主机，允许访问本设备相应服务	
	凡符合下列规则主机，禁止访问本设备相应服务	
设置本设备访问规则	IP 地址	输入 IP 地址
	服务	All 包含三者，http,telnet,SSH

注意

默认禁用。如果设置为允许，会禁止所有不在规则列表的访问。请先添加规则，再设置访问规则，否则可能导致当前 web 不能访问

2. 先设置本设备访问规则，单击导航树中的“业务管理 > 网络安全> 访问控制>设置本设备访问规则”菜单，输入 IP 地址 192.168.1.1/24，服务选 all，单击“添加”；在选择“凡符合下列规则主机，允许访问本设备相应服务”，单击“设置”，完成配置，

如下图所示：

7.2 防攻击设置

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“安全管理 > 防攻击设置”菜单，进入“防攻击设置”，分别启用“忽略 ping 包“，“防范 SYN DOS 攻击”，设置“CPU 接收数据包阀值“，单击”设置“，完成配置，界面如下图所示。

界面含义如下表

配置项	说明
忽略 ping 包	忽略 ping 包的攻击
防范 SYN DOS 攻击	防范 TCP SYN 攻击
CPU 接收数据包阀值	范围：0-100000（默认为 0，表示不限速），超过阀值，不予接收该数据包

7.3 ACL配置

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。

7.3.1 TIME RANGE配置

生效时间段的配置可以使用户区分时间段对报文进行 ACL 控制。
时间段用于描述一个特殊的时间范围。用户可能有这样的需求：一些 ACL 规则需要在某个或某些特定时间内生效，而在其他时间段则不利用它们进行报文过滤，即通常所说的按时间段过滤。这时，用户就可以先配置一个或多个时间段，然后在配置 ACL 规则时引用该时间段，从而实现基于时间段的 ACL 过滤。
对时间段的配置有如下内容：配置周期时间段和绝对时间段。配置周期时间段采用的是每周的周几的形式；配置绝对时间段采用从起始时间到结束时间的形式。
操作步骤
单击导航树中的“业务管理> TIME RANGE 配置”菜单，进入“TIME RANGE 配置”界面，如下图所示。

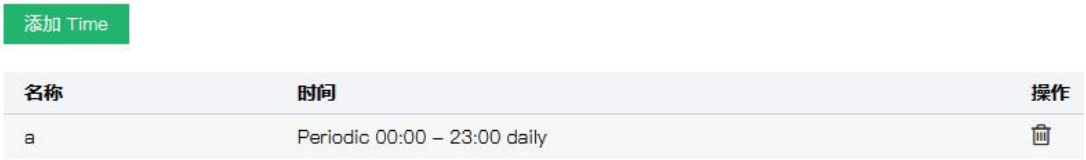
通过点击“添加 time”可设置时间范围，如下图所示：

界面信息含义说明如下表所示

配置项	说明
Time-Range 名称	输入 Time-Range 名称，可选（绝对时间与周期时间）
绝对时间	配置绝对时间段采用从起始时间到结束时间的形式。可以配置多个绝对时间段，也可以不配置绝对时间段。
周期时间	配置周期时间段采用的是每周的周几的形式。可以配置多个周期时间段，也可以不配置周期时间段，

2.填写相应的配置项（本次以周期时间为例子）。

3.单击“添加”，完成配置，如图所示。



7.3.2 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“安全管理> ACL 配置> 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
组 ID	二层 ACL 取值范围是：1-99
规则	表示每个规则编号范围是：1-127

动作	ACL 的规则分为“permit”（允许）规则或者“deny”（拒绝）规则。
源 MAC	输入 ACL 规则的源 MAC 地址。格式为 H-H-H。
目的 MAC	输入 ACL 规则的目的 MAC 地址。格式为 H-H-H。
Time-Range 名称	输入已配置好的生效时间段名称。

2.点击“添加 group”“添加 rule”填写相应的配置项。

3.单击“添加”，完成配置，如图所示。

7.3.3 IP ACL配置

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

操作步骤

1.单击导航树中的“安全管理> ACL 配置> IP ACL 配置”菜单，进入“IP 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
组 ID	二层 ACL 取值范围是：100-999
规则	表示每个规则编号范围是：1-127
动作	ACL 的规则分为“permit”（允许）规则或者“deny”（拒绝）规则。
协议	必选，选择协议的类型。Any、icmp、igmp、ip、tcp、udp
源 IP	输入 ACL 规则的源 IP
源掩码	输入 ACL 规则的源掩码
源端口	输入 ACL 规则的源端口
目的 IP	输入 ACL 规则的目的 IP
目的掩码	输入 ACL 规则的目的掩码
目的端口	输入 ACL 规则的目的端口
Time-Range 名称	输入已配置好的生效时间段名称。

2.点击“添加 group” “添加 rule”填写相应的配置项。
3.单击“添加”，完成配置，如图所示。

7.3.4 ACL GROUP配置

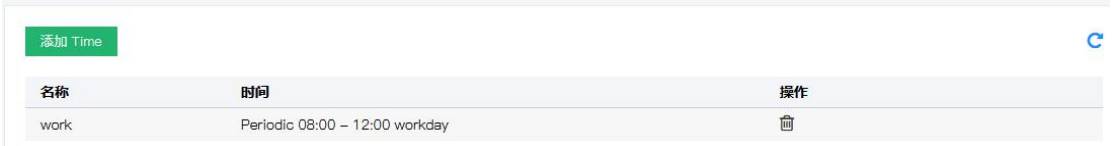
创建好列表以后，接下来还必须将它应用到每个想用它的接口上
操作步骤：
1.单击导航树中的“安全管理> ACL 配置> ACL GROUP 配置”菜单，进入“ACL GROUP 配置”界面，如下图所示。

界面含义如下表

配置项	说明
MAC 访问列表 ID	已创建好的 MAC 访问列表 ID 应用到端口上
IP 访问列表 ID	已创建好的 IP 访问列表 ID 应用到端口上

2.点击“添加”填写相应的配置项，以创建好的 acl 100 为例子，应用到 ge1/1 上。
3.单击“设置”，完成配置，如图所示。

#举例说明
基于时间的 ACL 的定义方法。假如某单位希望在交换机上使用基于时间的 ACL 实现：周一到周五（工作日）的上午从 8:00 到 12:00，只允许用户收发邮件，非工作时间允许所有访问。
实验步骤
1.定义时间范围。单击导航树中的“网络安全> ACL 配置> TIME RANGE 配置”菜单，进入“TIME RANGE 配置”界面，选择 “添加 time “，分别输入周一到周五（工作日）的上午从 8:00 到 12:00，如下图所示。



2.编辑 ACL。单击导航树中的“网络安全> ACL 配置> IP ACL 配置”菜单，进入“IP ACL 配置”界面，分别创建以下 5 个 ACL，如下图所示。

组ID	规则ID	动作	协议	源IP	源掩码	源端口	目的IP	目的掩码	目的端口	TimeRange
100										
	1	permit	tcp	any	any		any	any	25	work
	2	permit	any	any	any		any	any	110	work
	3	permit	udp	any	any		any	any	502	work
	4	deny	ip	any	any		any	any		work
	5	permit	ip	any	any		any	any		

刷新

3.调用 ACL，将 ACL100 应用到 ge1/1 上。单击导航树中的“网络安全> ACL 配置> ACL GROUP 配置”菜单，进入“ACL GROUP 配置”界面，如下图所示。

端口	MAC访问列表ID	IP访问列表ID
ge1/1		100

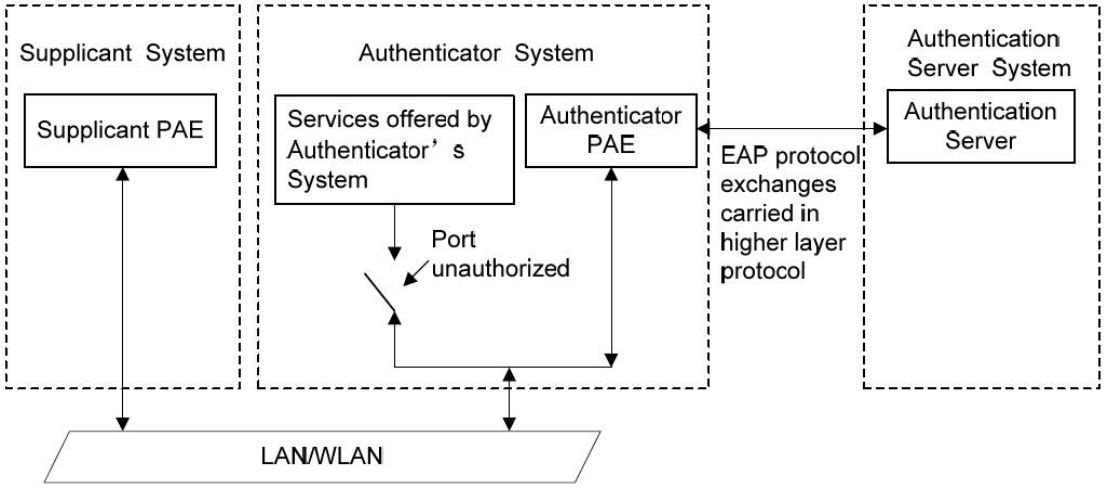
刷新

7.4 802.1x配置

IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。后来，802.1x 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1x 协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”是指，在局域网接入设备的端口这一级，对所接入的用户设备通过认证来控制对网络资源的访问。

如下图所示，使用 802.1x 的系统为典型的 Client/Server 体系结构，包括三个实体，分别为：Supplicant System（客户端）、Authenticator System（设备端）以及 Authentication Server System（认证服务器）。



- 客户端是位于局域网段一端的一个实体，由该链路另一端的设备端对其进行认证。客户端一般为一个用户终端设备，用户可以通过启动客户端软件发起 802.1x 认证。客户端必须支持局域网上的可扩展认证协议 EAPOL（Extensible Authentication Protocol over LAN）。
- 设备端是位于局域网段一端的另一个实体，用于对所连接的客户端进行认证。设备端通常为支持 802.1x 协议的网络设备（如 WL-66408GM 交换机），它为

客户

端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。

- 认证服务器用于实现对用户进行认证、授权和计费，通常为 RADIUS 服务器。该服务器可以存储用户的相关信息，例如用户的账号、密码以及用户所属的 VLAN、优先级、用户的访问控制列表等。

802.1x 的基本概念

1、受控/非受控端口

设备端为客户端提供接入局域网的端口，这个端口被划分为两个逻辑端口：受控端口和非受控端口。

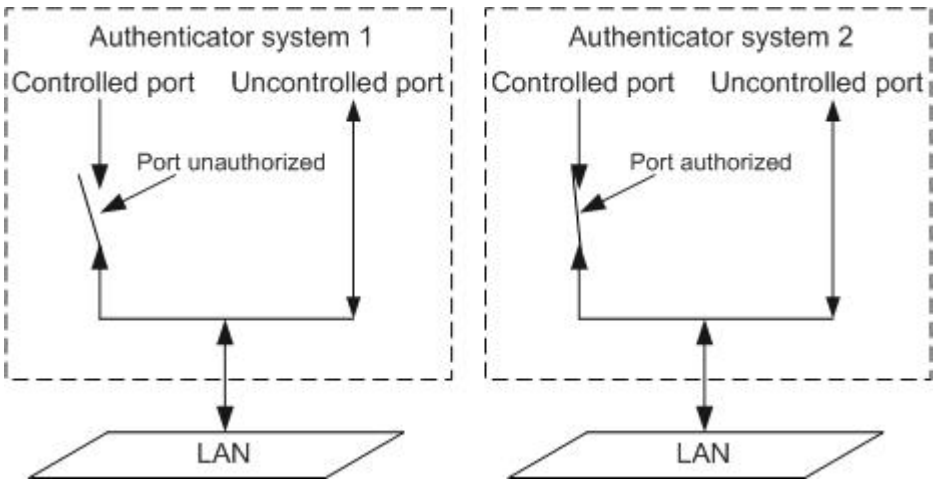
非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接收认证报文。

受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

2、授权/非授权状态

设备端利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权/非授权状态进行相应地控制。

下图显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1x 认证系统的端口状态。系统 1 的受控端口处于非授权状态（相当于端口开关打开），系统 2 的受控端口处于授权状态（相当于端口开关闭合）。



802.1x 的工作机制

IEEE 802.1x 认证系统利用 EAP（Extensible Authentication Protocol，可扩展认证协议）协议，在客户端和认证服务器之间交换认证信息。

- 在客户端 PAE 与设备端 PAE 之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。
- 在设备端 PAE 与 RADIUS 服务器之间，EAP 协议报文可以使用 EAPOR（EAP over RADIUS）封装格式，承载于 RADIUS 协议中；也可以由设备端 PAE 进行终结，而在设备端 PAE 与 RADIUS 服务器之间传送 PAP 协议报文或 CHAP 协议报文。
- 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端 PAE 根

据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

7.4.1 全局配置

通过配置 802.1X 接入控制可以实现基于接口的网络接入控制，即在局域网接入控制设备的接口这一级对所接入的设备进行认证和控制。

操作步骤：

1.单击导航树中的“安全管理> 802.1X 配置> 全局配置”菜单，进入“全局配置”界面，如下图所示。

界面含义如下表

配置项	说明
模式	单选。有启用和禁用两种选择，默认是禁用。
Radius 服务器	单选。有远端和本地两种选择，默认本地。
认证更新间隔	认证更新间隔，默认为 30 秒，范围： 1~65535。802.1X 认证成功之后，每隔一定的时间间隔，就要对接入用户进行重认证，该时间间隔由重认证定时器进行控制。
IP 地址	输入 Radius 服务器配置 IP 地址。
端口	输入 Radius 服务器配置 IP 端口。范围：1~65535。
认证共享密码	与 Radius 服务器认证密码保持一致
认证重试次数	认证重试次数。范围：1~10 交换机初次向用户发送认证请求帧后，在规定的时间里没有收到用户的响应，交换机将再次向用户发送该认证请求。当发送次数达到最大次数后仍没有收到响应，交换机不再重复向用户发送该认证请求。

2.填写相应的配置项。

3.单击“设置”，完成配置，如图所示。

7.4.2 端口配置

通过配置 802.1X 接入控制可以实现基于接口的网络接入控制，即在局域网接入控制设备的接口这一级对所接入的设备进行认证和控制。

操作步骤：

1.单击导航树中的“安全管理> 802.1X 配置> 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
认证端口	单选。固定值，显示用户选择的接口名称，支持创建多个。
认证模式	选择接口接入认证模式： 自动模式 强制认证通过 强制认证不通过 Mac 认证 默认是自动模式。

2.填写相应的配置项。

3.单击“添加”，完成配置，如图所示。

7.4.3 用户配置

通过配置 802.1X 接入控制可以实现基于接口的网络接入控制，即在局域网接入控制设备的接口这一级对所接入的设备进行认证和控制。

操作步骤：

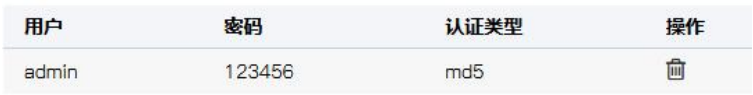
1.单击导航树中的“安全管理> 802.1X 配置> 端口配置”菜单，进入“端口配置”界面，如下图所示。

界面含义如下表

配置项	说明
用户	需认证的用户
密码	需认证的密码
认证类型	包括 MD5, TLS, MSCHAPV2, PEAP, TTLS, TLV, GTC, SIM

2.填写相应的配置项。

3.单击“添加”，完成配置，如图所示。



7.5 告警配置

7.5.1 系统配置

设备支持电源告警，用户可根据需求进行设置。

1.单击导航树中的“安全管理>告警配置”菜单，进入“系统告警”界面，如下图所示。

界面含义如下表

配置项	说明
启用	告警全局设置
Power	启用/禁用电源告警

7.5.2 链路告警

用户可对接口链路进行告警设置。

1.单击导航树中的“安全管理>链路告警”菜单，进入“链路告警”界面，单击“设置”，完成配置，如下图所示。

界面含义如下表

配置项	说明

端口	可选多个端口

8 扩展管理

8.1 Time Range 配置

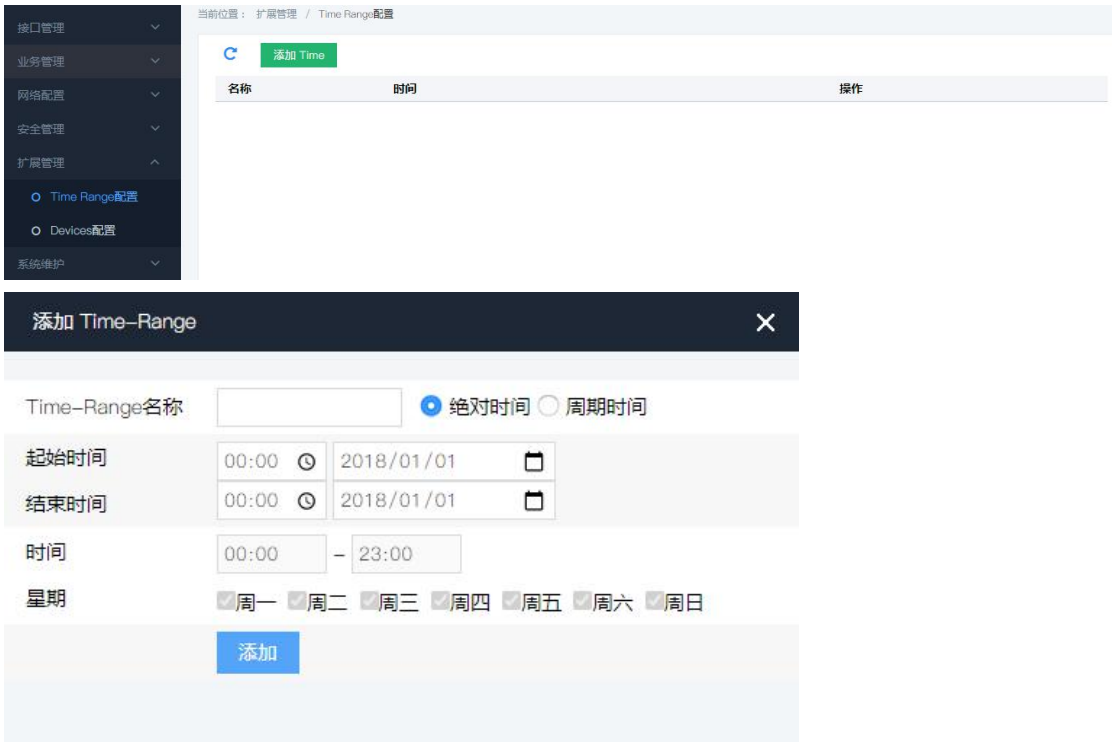
生效时间段的管理可以使用户区分时间段对报文进行 ACL 控制。

时间段用于描述一个特殊的时间范围。用户可能有这样的需求：一些 ACL 规则需要在某个或某些特定时间内生效，而在其他时间段则不利用它们进行报文过滤，即通常所说的按时间段过滤。这时，用户就可以先管理一个或多个时间段，然后在管理 ACL 规则时引用该时间段，从而实现基于时间段的 ACL 过滤。

对时间段的管理有如下内容：管理周期时间段和绝对时间段。管理周期时间段采用的是每周的周几的形式；管理绝对时间段采用从起始时间到结束时间的形式。

操作步骤

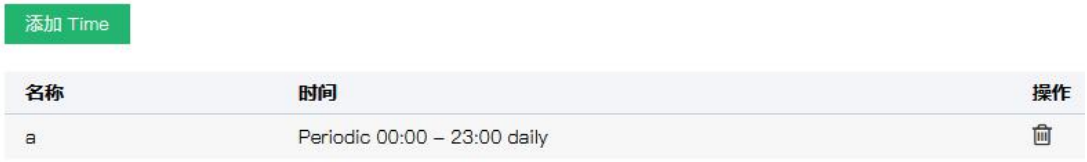
1. 单击导航树中的“扩展管理>Time Range 配置”菜单，进入设置界面，如下图所示。



界面信息含义说明如下表所示

管理项	说明
Time-Range 名称	输入 Time-Range 名称，可选（绝对时间与周期时间）
绝对时间	管理绝对时间段采用从起始时间到结束时间的形式。可以管理多个绝对时间段，也可以不管理绝对时间段。
周期时间	管理周期时间段采用的是每周的周几的形式。可以管理多个周期时间段，也可以不管理周期时间段，

2.填写相应的管理项（本次以周期时间为例子）。
3.单击“添加”，完成管理，如图所示。



8.2 Devices 配置

便于用户查看设备接口连接设备相关信息。

操作步骤
单击导航树中的“扩展管理>Devices 配置”菜单，进入界面，如下图所示。

8.3 POE 配置

用户可进行 POE 接口相关参数查询。

操作步骤
单击导航树中的“扩展管理>POE 配置”菜单，进入界面，如下图所示。

9 系统维护

9.1 日志配置

1.面板描述

日志配置的主要功能作用：查看设备的日志信息（历史配置信息记录），上传设备日志信息到 tftp 服务器。界面显示如下图：

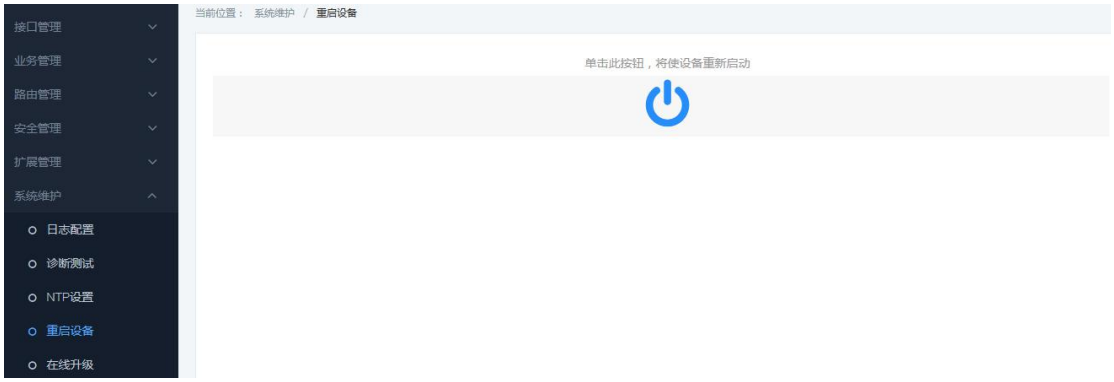
2.操作步骤说明

步骤一	单击导航栏中“系统维护>日志配置”菜单，进入“上传日志”，输入 TFTP 服务器地址：“如：192.168.1.125”，文件名，“diary”，单击“上传”即可。
步骤二	如需作为启动配置，需进入”系统管理”，“运行配置”下点击“保存配置”进行设置保存。

9.2 重启设备

操作步骤：

1.单击导航树中的“系统维护> 重启设备”菜单，进入“重启设备”界面，单击“重启设备“，如下图所示。



9.3 NTP设置

网络时间协议 NTP（Network Time Protocol）是 TCP/IP 协议族里面的一个应用层协议。NTP 用于在一系列分布式时间服务器与客户端之间同步时钟。NTP 的实现基于 IP 和 UDP。NTP 报文通过 UDP 传输，端口号是 123。随着网络拓扑的日益复杂，整个网络内设备的时钟同步将变得十分重要。如果依靠管理员手工修改系统时钟，不仅工作量巨大，而且时钟的准确性也无法得到保证。NTP 的出现就是为了解决网络内设备系统时钟的同步问题。

NTP 基本原理，NTP 实现过程如下图所示。RouterA 和 RouterB 通过广域网 WAN（Wide Area Network）相连，它们都有自己独立的系统时钟，通过 NTP 实现系统时钟自动同步。

作如下假设：

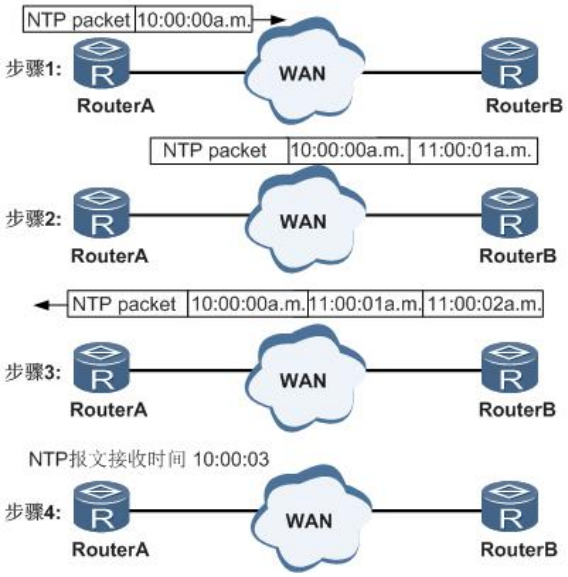
在 RouterA 和 RouterB 的系统时钟同步之前，RouterA 的时钟设定为 10:00:00a.m.，RouterB 的时钟设定为 11:00:00a.m.。

RouterB 作为 NTP 时间服务器，RouterA 的时钟要与 RouterB 的时钟进行同步。

报文在 RouterA 和 RouterB 之间单向传输需要 1 秒。

RouterA 和 RouterB 处理 NTP 报文的时间都是 1 秒。

NTP 实现图



系统时钟的同步流程如下所示：

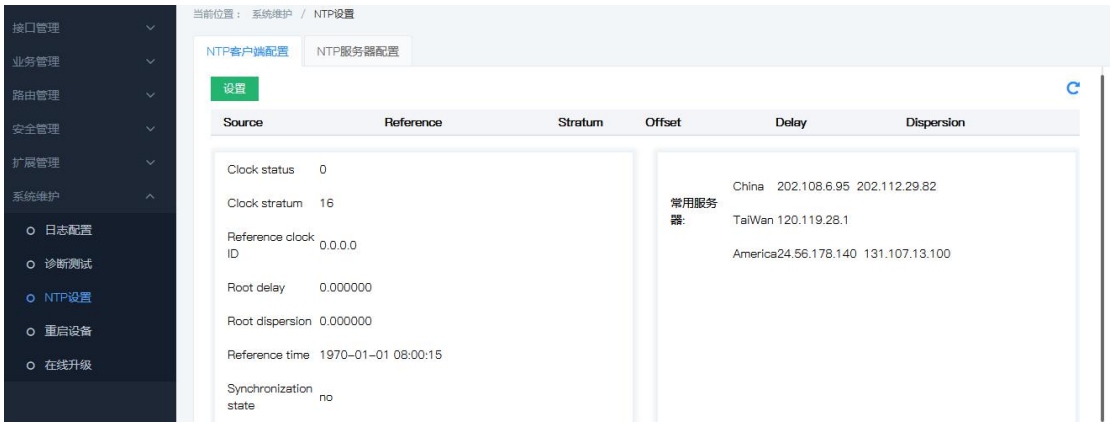
RouterA 发送一个 NTP 报文给 RouterB，该报文中带有它离开 RouterA 时的时间戳 10:00:00a.m.（T1）。

此 NTP 报文到达 RouterB 时，RouterB 加上到达时间戳 11:00:01a.m.（T2）。
此 NTP 报文离开 RouterB 时，RouterB 再加上离开时间戳 11:00:02a.m.（T3）。
RouterA 接收到该响应报文时，加上新的时间戳 10:00:03a.m.（T4）。
至此，RouterA 获得了足够信息来计算以下两个重要参数：
NTP 报文来回一个周期的时延：Delay=（T4 - T1）-（T3 – T2）。
RouterA 相对 RouterB 的时间差：Offset=（（T2- T1）+（T3 – T4））/ 2。
RouterA 根据计算得到 Delay 为 2 秒，Offset 为 1 小时。RouterA 根据这些信息来设定自己的时钟，实现与 RouterB 的时钟同步。

📖 说明：
以上是 NTP 工作原理的简略描述，RFC1305 为 NTP 定义了复杂的算法来确保时钟同步的精确性。

9.3.1 NTP客户端配置

操作步骤
1.单击导航树中的“系统维护>NTP 设置>NTP 客户端设置”菜单，进入“NTP 客户端设置”界面，如下图所示。



界面含义如下表

配置项	说明
模式	disable 禁用、unicast 单播、broadcast（多播，暂不支持）
服务器	最大支持 3 个服务器 IP 地址

9.3.2 NTP服务端配置

操作步骤
1.单击导航树中的“系统维护>NTP 设置>NTP 服务端设置”菜单，进入“NTP 服务端设置”界面，如下图所示。

界面含义如下表

配置项	说明
模式	Enable 使能作为 ntp 服务端
Local as master	设置本地时钟作为 NTP 主时钟，为其它设备提供同步时间
stratum	指定 NTP 主时钟所处的层数。整数形式，取值范围是 1~15。缺省值是 2。值越小表示时钟准确度越高。

9.4 在线升级

操作步骤：

1.单击导航树中的“系统维护> 在线升级”菜单，进入“在线升级”界面，单击“在线升级“，单击“选择文件”，单击“上传”，完成配置。如下图所示。

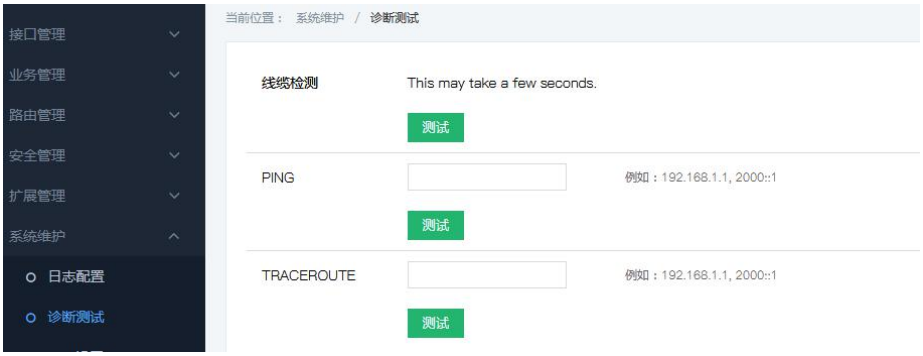
9.5诊断测试

9.5.1 ping

1.面板描述

ping 是用来检查网络是否通畅或者网络连接速度的命令。它是利用网络上机器 IP 地址的唯一性，给目标 IP 地址发送一个数据包，再要求对方返回一个同样大小的数据包来

确定两台网络机器是否连接相通，时延是多少。



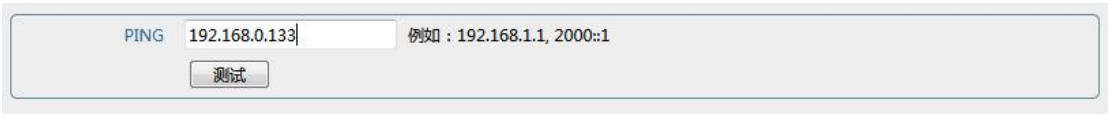
2.操作步骤说明

步骤一	单击导航栏中“系统配置”菜单，进入“系统配置”界面。单击“诊断测试”，单击“ping “，输入 IP 地址。
步骤二	点击“测试”即可获取结果。

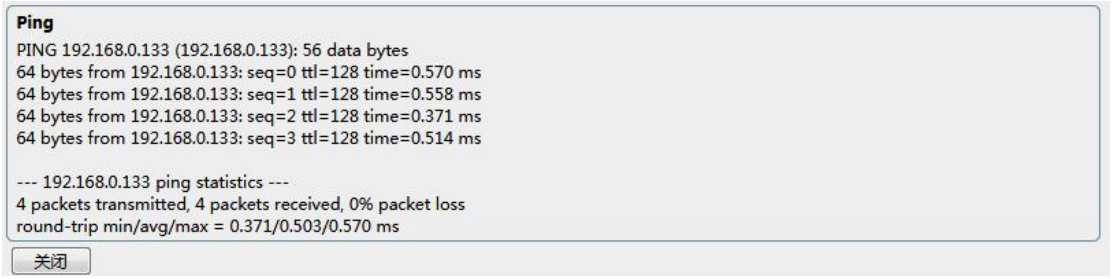
3.举例说明

#ping 测试 IP 地址为 192.168.0.133

1）网页上填写 IP 地址：192.168.0.133，点击“测试”。



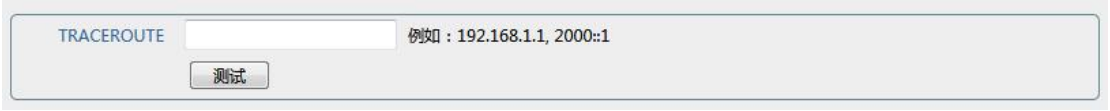
2）测试结果如下显示



9.5.2 Traceroute

1.面板描述

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。端口环回包括 PHY 层环回和 MAC 环回。界面显示如下图：



2.操作步骤说明

步骤一	单击导航栏中“系统维护”菜单，进入“诊断测试”界面。单击“tracroute”，输入 IP 地址。

步骤二	点击“测试”即可获取结果。

9.5.3 线缆检测

1.面板描述

可粗略计算两台设备间通过网线连接的距离。界面显示如下图：

2.操作步骤说明

步骤一	单击导航栏中“系统维护”菜单，进入“诊断测试”界面。单击“tracroute”，输入 IP 地址。
步骤二	点击“测试”即可获取结果。