AOKWAY工业网管型交换机 Web配置指南

（6系V1.5.0）

本手册对应的软件版本为： release/1.5.0

文档版本号：V1.5.0

发布时间：2020.03.20

目录

图表目录

1 WEB 管理概述

1.1 简介

为了方便网络管理员对网络设备进行操作和维护，我司特推出了设备的 Web 管理功能，管理员可以使用 Web 界面直观地对设备进行管理和维护。

同时，对于 Web 管理的相关操作会提供相应的 CLI 参考命令。

Web 网管的运行环境如下。

图表 1-1 WEB 网管运行环境

1.2 登录 Web 网管

设备出厂时已经默认启用了 Web server 服务，server 的 IP 地址为 192.168.1.234。用户首次登录 Web 网管时需要使用缺省账号”admin”进行登录，密码也为“admin”。登录完成后为了确保设备的安全性，需要立即更改密码。

说明

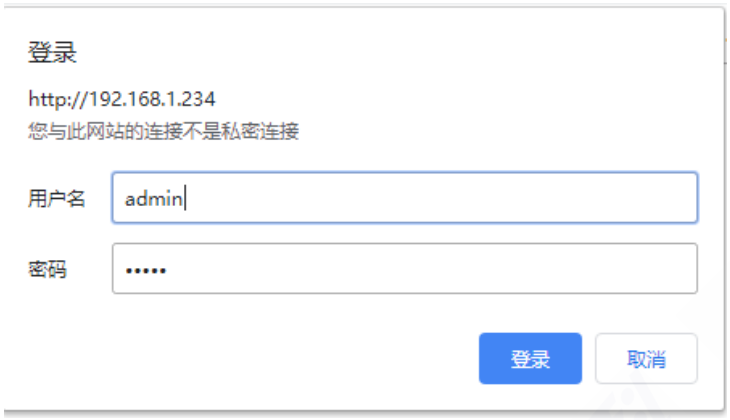
- 更改密码具体操作过程见用户管理章节。

下面以 IS2500-8GT2GS 交换机为例，介绍如何通过 Web 方式登录设备，具体步骤如下：

1）连接设备和 PC，用网线将 PC 和设备上的千兆以太网口（缺省情况下，所有端口均属于 VLAN 1）相连。

2）为 PC 配置 IP 地址，确保能与设备互通设置 PC 的 IP 地址与设备的缺省 VLAN 接口 IP 地址同网段（除设备的默认 IP 地址外），例如 192.168.1.100。

图表 1-2 用户登陆



3）在 PC 上启动浏览器，在地址栏中输入“192.168.1.234”后回车，进入设备的 Web 登录页面。输入缺省账号“admin”，密码栏输入“admin”，单击<登录>按钮登录 Web 网管。

1.3 Web 网管的退出

注意

- 退出 Web 网管时，系统不会自动保存当前配置。因此建议用户在退出 Web 网管前先设置保存当前配置。保存配置操作请参考保存配置章节。

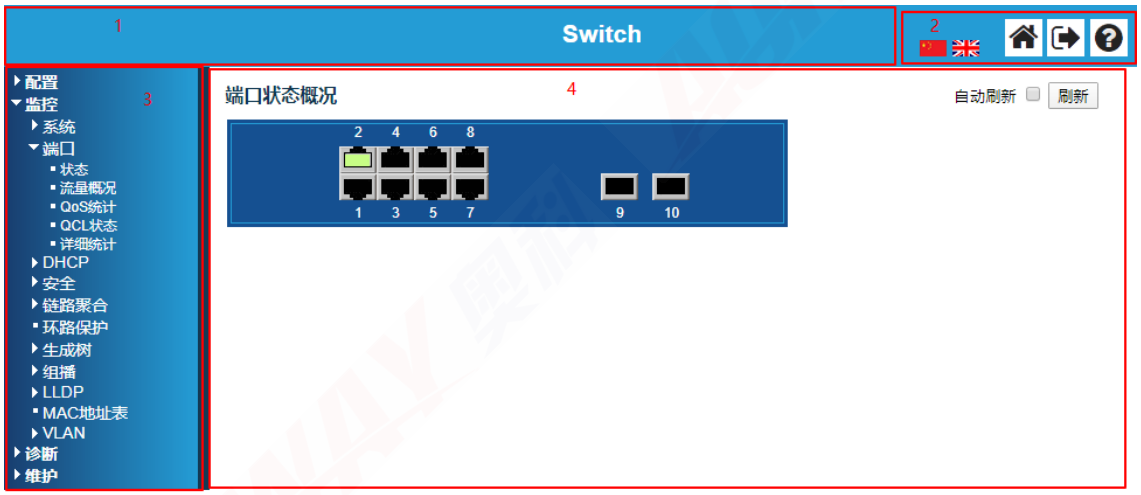
在 Web 网管页面上单击右上角的【注销】按钮，即可退出 Web 网管，回到登录界面。

图表 1-3 Web 注销

1.4 Web 管理页面布局介绍

Web 管理主页面共分为：产品型号、导航栏、快捷功能区、配置区四部分。

图表 1-4 Web 管理主页面



🕮 Web 布局介绍

1- 产品型号：用以显示产品的型号。

2- 快捷功能区：提供语言切换、切换到主界面、退出登录、帮助功能。

3- 导航栏：以导航树的形式组织设备的 Web 网管功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在配置区中。

4- 配置区：用户进行配置和查看的区域。

1.5 通用功能说明

1.5.1 配置页面

在每个配置页面的下面均有两个按钮。如下图所示：

图表 1-5 配置页面保存复位按钮

- 保存：此处的“保存”指页面保存，即将本页面配置的信息下发到交换机，类似在交换机 CLI 输入相关命令，不涉及到交换机的配置保存。若未点击“保存”按钮，页面的修改仅在管理端，并未下发到交换机，并且点击其他页面切换后，该页面的修订即消失，无法找回，因此，在本页面配置完成后，务必需要点击此按钮，完成配置下发到交换机。
- 复位：此处的“复位”指页面修订的复位，即将本页面本次修订的全部内容回退，页面恢复到上一次保存的状态（或者从未保存过，恢复到缺省状态）。

1.5.2 监控页面

- 分页显示

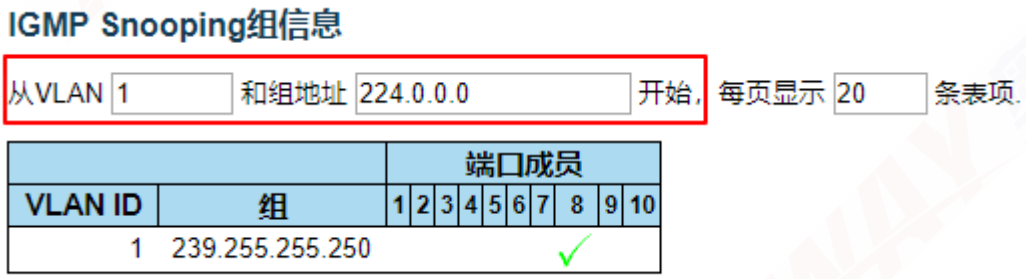
  在可能显示内容较多的页面，有一个区域用于表述分页显示，比如 VLAN 的成员关系页面。如下图所示。在修改分页显示的文本框内容后，点击右上角的“刷新”按钮才能完成页面的刷新。

图表 1-6 VLAN 成员关系分页显示

该区域由三部分组成：

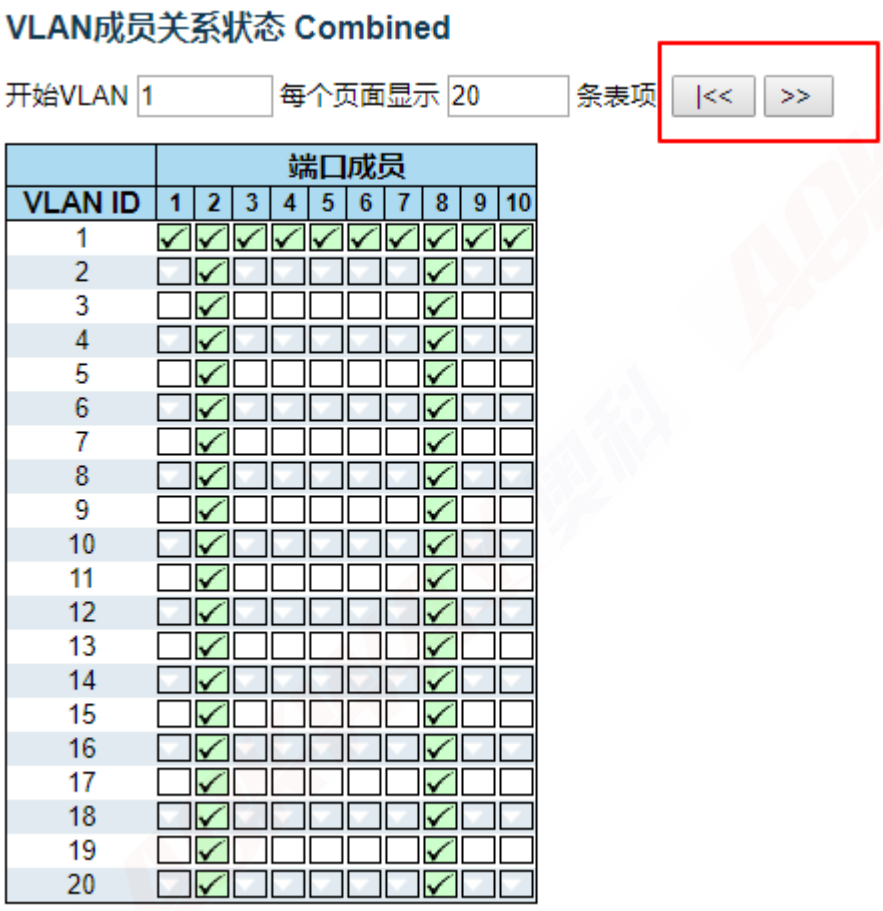
- 表示显示开始表项的 KEY 的文本框，有些表项的 KEY 可能不止一个，所以可能会有多个文本框。比如 IGMP Snooping 组信息有 VLAN 和组地址两个 Key。

图表 1-7 显示开始表项的多个 KEY

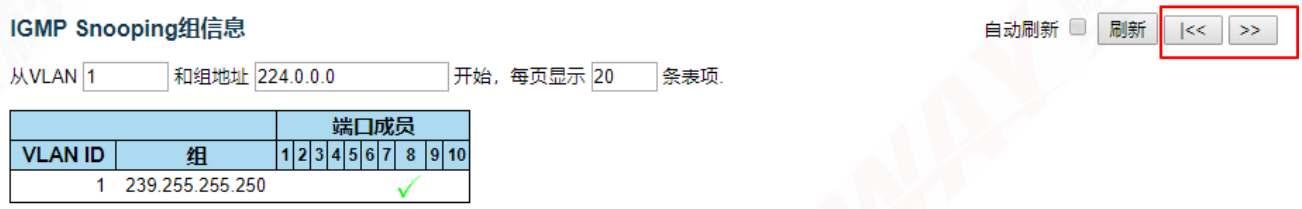


- 表示每页显示多少个表项的文本框，默认均为 20。可以配置的范围为 1-99。
- 用于页面切换的按钮。这些按钮有些页面放在分页显示区域，有些放在刷新区域。

图表 1-8 页面切换按钮 1



图表 1-9 页面切换按钮 2



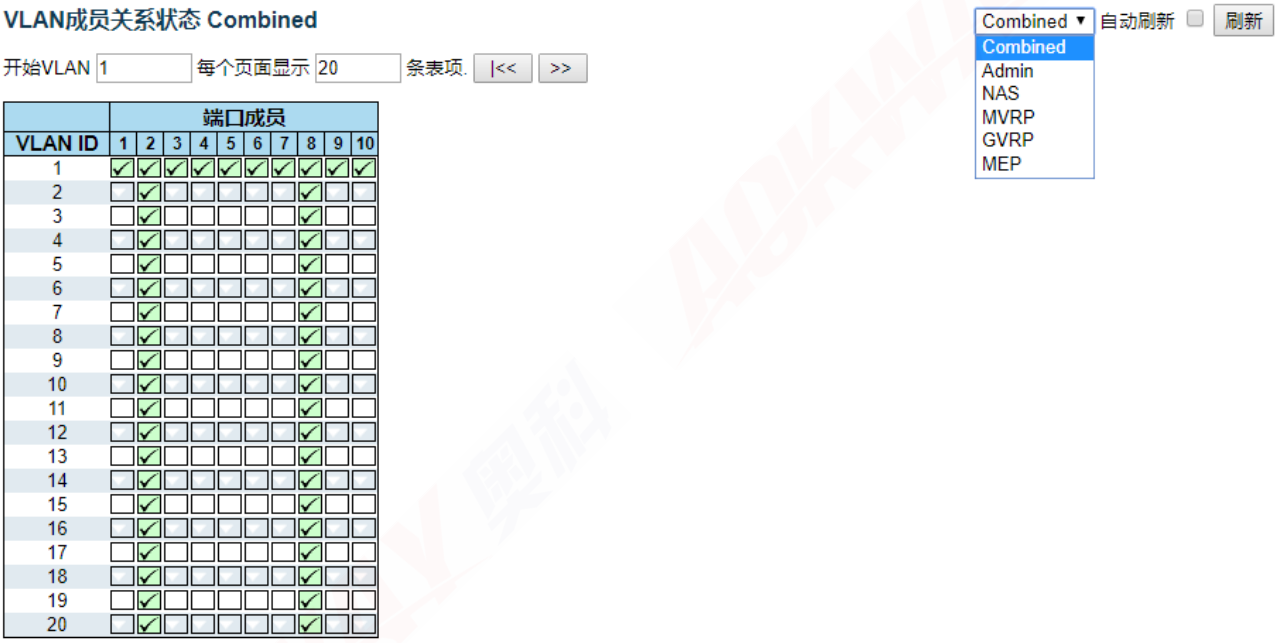
✧ “|<<”：表示退回到首页，即通过分页显示区域设置的开始表项开始的那个页面。

✧ “>>”：表示下一页。

■ 页面筛选

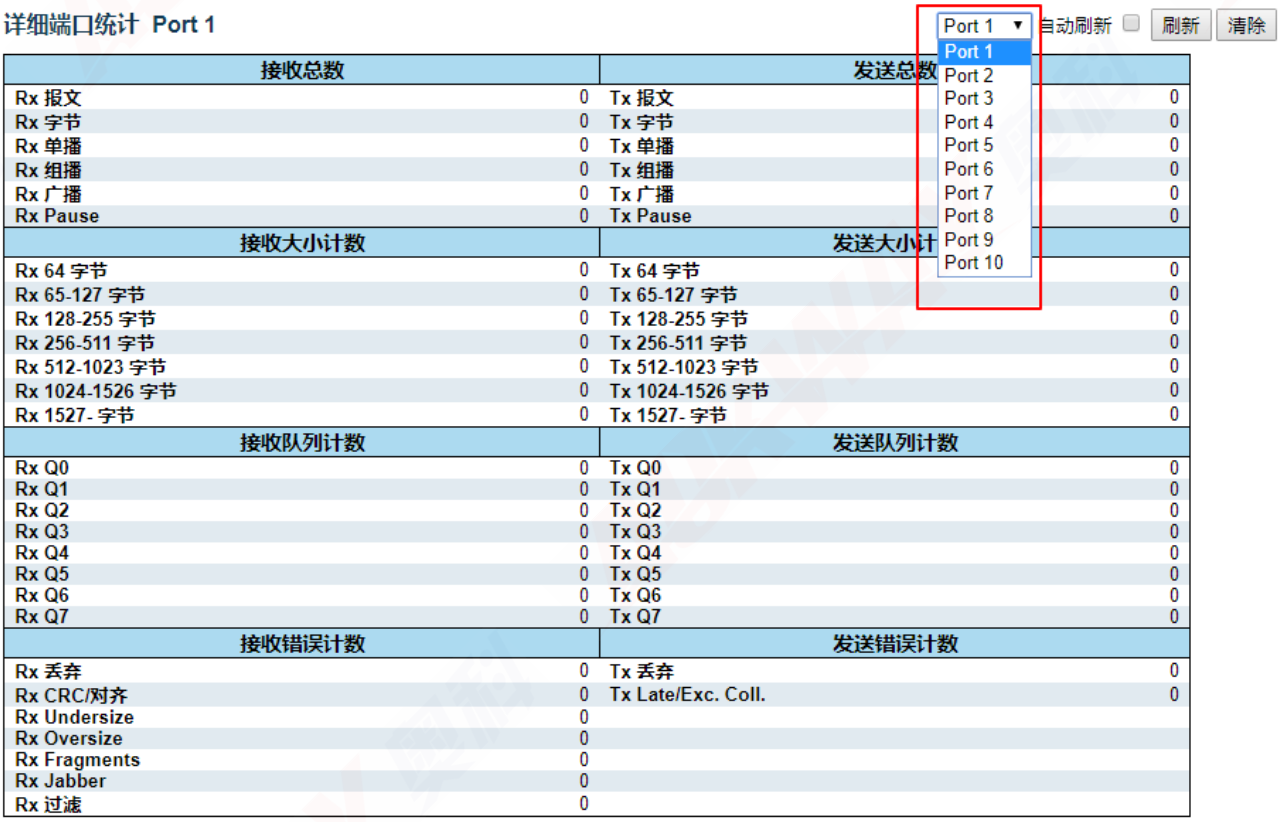
有些显示页面只是显示了部分内容，跟前述的分页显示不同，而是通过某个 Key 直接筛选得到。主要有两种情况。

➢ 根据来源筛选，比如 VLAN 成员关系页面。其中 Combined 表示所有来源。



➢ 根据 Key（比如端口，比如 Server）进行筛选，前者见“详细端口统计”页面，后者见“RADIUS 详情”页面。

图表 1-10 详细端口统计页面筛选



图表 1-11 RADIUS 详情页面筛选

RADIUS认证状态 Server #1

Server #1 ▾ 自动刷新 刷新 清除

Server #1
Server #2
Server #3
Server #4
Server #5

接收报文		发送报文	
访问接受	0	访问请求	0
访问拒绝	0	访问重传	0
访问Challenge	0	Pending请求	0
畸形访问应答	0	超时	0
非法认证者	0		
未知类型	0		
丢弃报文	0		
其他信息			
IP地址			
状态			禁用
Round-Trip时间			0 ms

RADIUS记账统计 Server #1

接收报文		发送报文	
应答	0	请求	0
畸形应答	0	重传	0
非法认证者	0	Pending请求	0
未知类型	0	超时	0
丢弃报文	0		
其他信息			
IP地址			
状态			禁用
Round-Trip时间			0 ms

■ 刷新区域

几乎的监控页面显示内容都是状态信息或者统计信息，存在变动。因此在监控页面还存在一个刷新区域，以“NAS 端口统计”为例。

图表 1-12 刷新区域 1

NAS统计 Port 6

Port 6 ▾ 自动刷新 刷新 清除所有 清除当前

端口状态

管理状态	多用户802.1X
端口状态	0个授权/1个未授权
端口VLAN	

端口计数

接收EAPOL计数		发送EAPOL计数	
总数	1	总数	1
应答ID	0	请求ID	1
应答计数	0	请求计数	0
开始	0		
下线	0		
非法类型	0		
非法长度	0		
接收后端服务器计数		发送后端服务器计数	
访问Challenge	0	应答计数	0
其他请求	2		
认证成功	0		
认证失败	0		
上次请求信息			
MAC地址		7c-ec-9b-01-00-52	
VLAN ID		1	
版本		2	
身份			

所选计数

接收EAPOL计数	发送EAPOL计数
总数	总数
应答ID	请求ID
应答计数	请求计数
开始	
下线	
非法类型	
非法长度	
接收后端服务器计数	发送后端服务器计数
访问Challenge	应答计数
其他请求	
认证成功	
认证失败	
请求信息	
MAC地址	
VLAN ID	
版本	
身份	*No supplicant selected*

关联 请求

Identity	MAC地址	VLAN ID	状态	上次认证
	7c-ec-9b-01-00-52	1	未授权	1970-01-01T00:02:20+00:00

- 自动刷新

  勾选后每隔 3S 页面将会自动刷新。

- 刷新

  点击刷新后，页面即时进行刷新。

- 清除区域

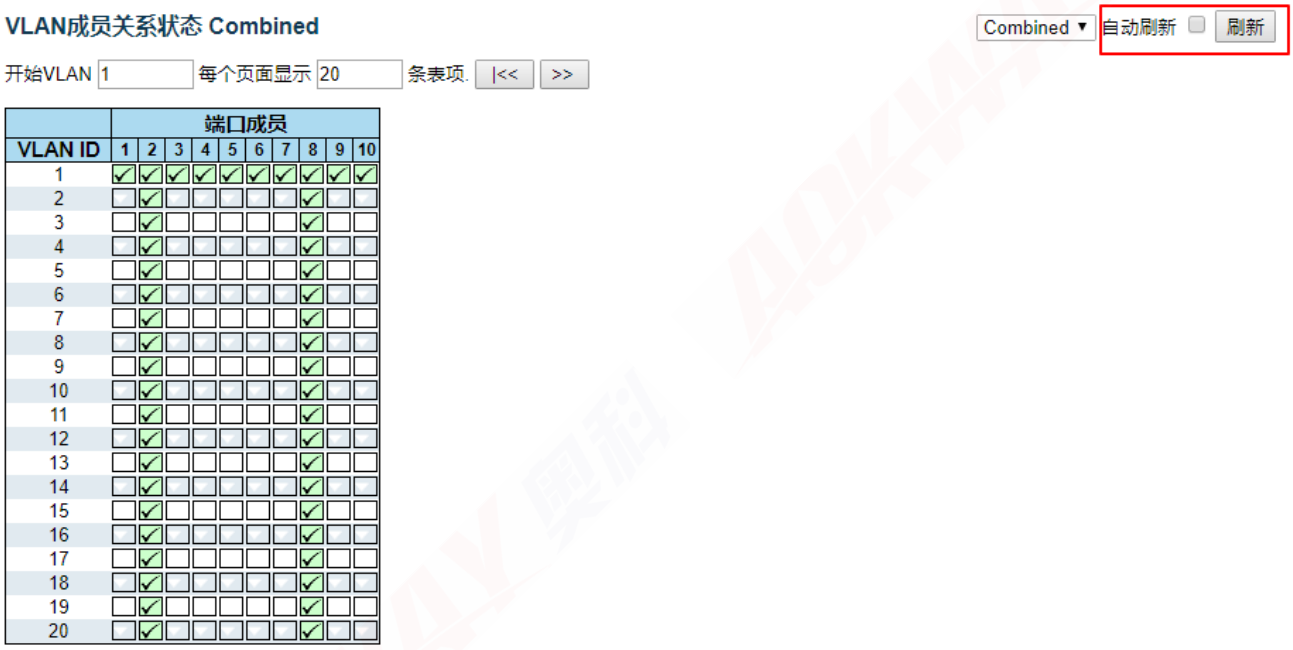
  如上页面在本页面内还存在筛选的（根据 Client 进行选择进行显示的），清除分为“清除当前”和“清除所有”。显而易见，清除当前指清除所选 Client 相关的统计，而清除所有指清除所有 Client 的统计。

  另外，大部分情况在本页面内不再存在筛选的，只有一个“清除”按钮。如下图所示：

图表 1-13 刷新区域 2

还有些显示页面不存在统计信息的，没有清除相关的按钮，如下图所示：

图表 1-14 刷新区域 3



1.5.3 配置保存

交换机端的配置分为 running-config 和 startup-config 两个。其中 running-config 表示的当前配置，但设备重启后 running-config 将会重置（按照 startup-config 进行设置）。

不管 CLI 还是 WEB 的配置，都是配置到 running-config 中的，因此，要让配置保存起来，重启设备后配置依然生效，需要将 running-config 的配置覆盖到 startup-config。

因此，在 Web 配置完成后，需要进行配置保存操作，具体参见“保存配置”章节描述。

2 系统

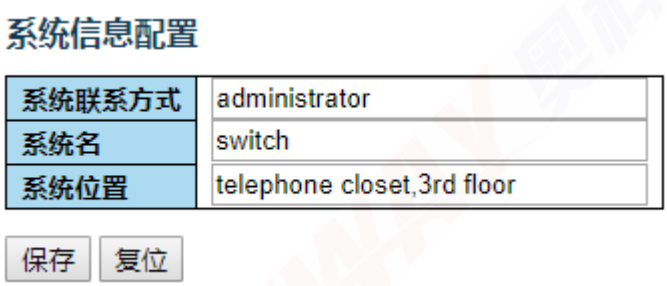
2.1 信息

系统信息主要包括设备的基本信息，如软件版本信息、硬件信息、系统时间信息等。设备支持在 WEB 界面对 MIB2 节点的 sysContact、sysName、sysLocation 子节点进行配置。

2.1.1 配置系统信息

在【导航栏】下拉菜单中选择：配置->系统->信息，进入配置界面。

图表 2-1 系统信息配置

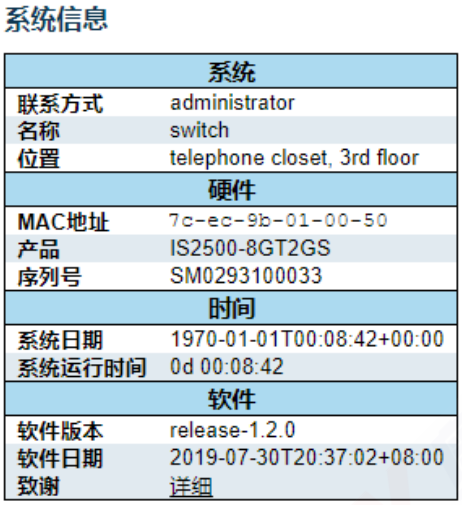


配置项	说明
系统联系方式	记录提供该设备支持的机构和（或）联系人的信息，长度 0-255 字符
系统名	设备的名字，长度 0-255 字符
系统位置	该设备安装的物理位置，长度 0-255 字符

2.1.2 查看系统信息

在【导航栏】下拉菜单中选择：监控->系统->信息，进入查看界面。

图表 2-2 系统信息查看



2.1.3 CLI 参考命令

命令	switch(config)# snmp-server contact administrator
描述	配置系统联系方式

命令	switch(config)# hostname switch
描述	配置系统名

命令	switch(config)# snmp-server location telephone closet,3rd floor
描述	配置系统位置

2.2 IP

设备默认一个 SVI 口，VLAN 1，IP 192.168.1.234/24，终端可从设备任意端口接入，以远程访问设备。

以下行为可能导致当前远程设备访问断开，并无法重新连接，修改前请确认配置合理性：

- 修改端口的 VLAN 属性，例如修改 access 口的端口 VLAN。
- Shutdown 连接正访问的终端设备的端口。

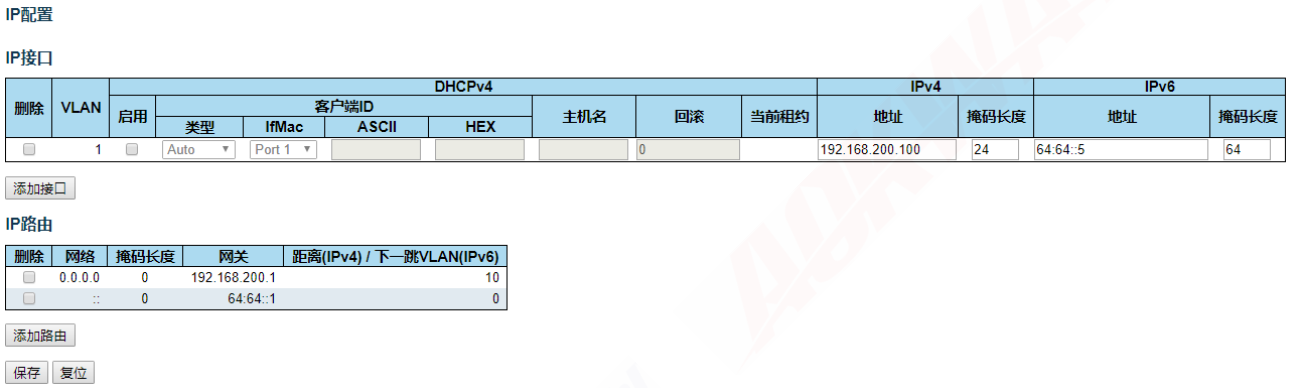
2.2.1 配置 IP

注意

- 在修改 IP 地址后，需要手动将网页指向新地址重新访问交换机。
- 修改管理 IP 地址，需注意保存配置，以确保重启或掉电后配置依然生效。

在【导航栏】下拉菜单中选择：配置->系统->IP，进入配置界面。

图表 2-3 IP 配置



■ IP 接口

IP 接口的配置分为 IPv4 地址的设置和 IPv6 地址的设置，两者是相互独立的，IPv4 地址可以通过 DHCP 自动分配，也可以静态配置，而 IPv6 地址只支持静态配置。

IPv4 地址要么选择 DHCP，要么选择静态配置，后配置的会覆盖之前配置（比如开启 DHCP，那么静态配置的 IPv4 地址会自动删除，配置了回滚的情况除外，具体见下面描述）。

配置项	说明
VLAN	开启/关闭日志送服务器功能
服务器地址	服务器的 IP 地址
日志级别	送服务器的日志级别，从低到高 Informational<Notice<Warning<Error

配置项	子参数	说明
删除	无	勾选表示删除该 SVI 接口。
VLAN	无	SVI 所对应的 VLAN ID。
DHCPv4	启用	选中此框以启用 DHCPv4 客户端。如果启用此选项，系统将使用 DHCPv4 协议配置接口的 IPv4 地址和掩码。
	客户端 ID	客户端 ID，体现在 DHCPv4 报文的 option61 当中，类型有四种： ➢ Auto：自动选择，无需配置 ID。（会根据系统 MAC 地址自动生成 ID）。 ➢ IF_MAC：使用所配置端口的 MAC 地址作为 ID。 ➢ ASCII：使用所配置的字符串作为 ID。 ➢ HEX：使用所配置的 16 进制数作为 ID。
	主机名	当前版本未支持 DNS，因此不支持主机名的配置。主机名体现在 DHCPv4 报文的 option12 当中，系统会自动生成主机名，该配置暂不使用。
	回滚	尝试获取 DHCP 租约的秒数。在此期限到期后，配置的 IPv4 地址将用作 IPv4 接口地址。值为零会禁用回滚机制，这样 DHCP 将继续重试，直到获得有效的租约。合法值为 0 到 4294967295 秒。

		因此，配置了该参数未非 0，必须配置 IPv4 回滚地址及掩码。以便到期后，使用 IPv4 回滚地址。
	当前租约	对于具有活动租约的 DHCP 接口，此列显示 DHCP 服务器提供的当前接口地址。
IPv4	地址	接口的 IPv4 地址，点分十进制格式。 如果 DHCP 启用后，此字段配置回滚地址。如果不希望在接口上进行 IPv4 操作，则该字段可以留空 - 或者不需要 DHCP 回滚地址。
	掩码长度	IPv4 网络掩码，以位数（前缀长度）表示。有效值介于 1 到 31 位之间。 如果 DHCP 启用后，此字段配置回滚地址网络掩码。如果不希望在接口上进行 IPv4 操作，则该字段可以留空 - 或者不需要 DHCP 回滚地址。
IPv6	地址	接口的 IPv6 地址。IPv6 地址在 128 位记录中，表示为八个字段，最多四个十六进制数字，冒号分隔每个字段（:)。例如，FE80 :: 215：c5ff：FE03：4dc7。符号::是一种特殊的语法，可以用作表示多个 16 位连续零组的简写方式; 但它只能出现一次。 如果不希望在接口上进行 IPv6 操作，则该字段可以留空。
	掩码长度	IPv6 网络掩码，以位数（前缀长度）表示。对于 IPv6 地址，有效值介于 1 到 127 位之间。 如果不希望在接口上进行 IPv6 操作，则该字段可以留空。

- IP 路由

  对于二层设备，需要通过 IP 路由配置设备的默认网关（即默认路由）。

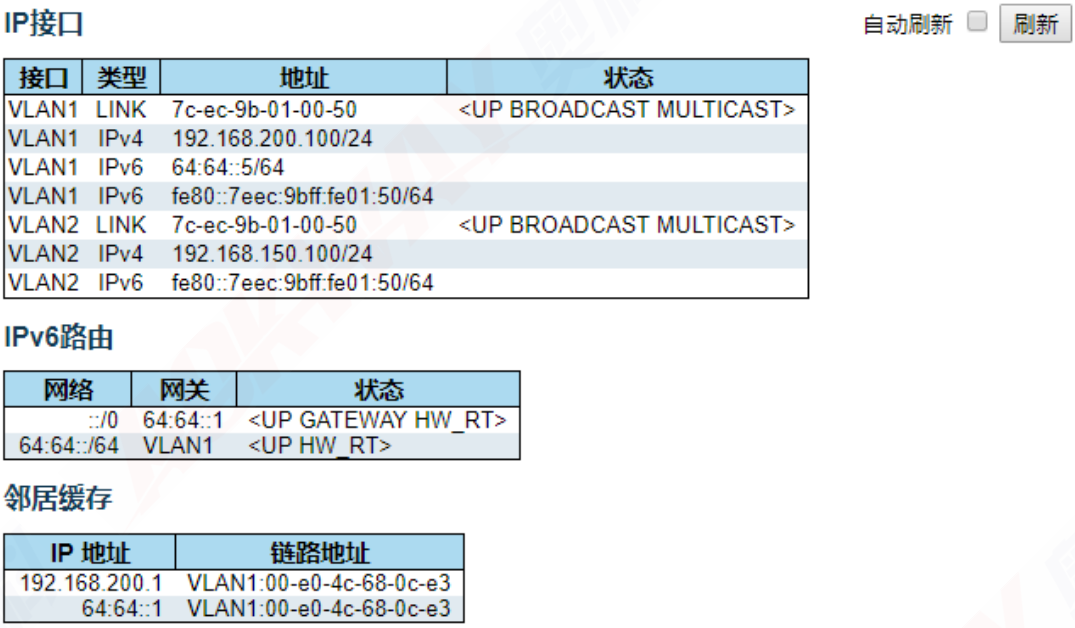
配置项	说明
删除	勾选表示删除该路由。
网络	此路由的目标 IP 网络或主机地址。有效格式为点分十进制表示法或有效的 IPv6 表示法。默认路由可以使用 0.0.0.0 或 IPv6 ::符号。
掩码长度	目标 IP 网络或主机的掩码，以位数（前缀长度）表示。IPv4 路由的有效值为 0-32，IPv6 路由的有效值为 0-128。只有默认路由的掩码长度为 0（因为它会匹配所有）。
网关	IP 网关的 IP 地址。有效格式为点分十进制表示法或有效的 IPv6 表示法。网关和网络必须属于同一网段。
距离(IPv4)	路由条目的距离值用于向路由器提供路由协议的优先级信息。当涉及两个或更多个不同的路由协议并且具有相同的目的地时，距离值可用于选择最佳路径。对当

	前设备而言，该配置项无意义。
下一跳 VLAN(IPv6)	与网关关联的特定 IPv6 接口的 VLAN ID（VID）。给定的 VID 范围为 1 到 4095，仅在相应的 IPv6 接口有效时才有效。 如果 IPv6 网关地址是链路本地的，则必须为网关指定下一跳 VLAN。 如果 IPv6 网关地址不是链路本地，则系统会忽略网关的下一跳 VLAN。

2.2.2 查看 IP

在【导航栏】下拉菜单中选择：监控->系统->IP 状态表，进入查看界面。

图表 2-4 IP 显示



配置项	说明
IP 接口	类型可以为 LINK，IPv4 或者 IPv6。链路层地址表示本机的 MAC 地址。
IPv6 路由	显示 IPv6 配置及生成的路由。配置一个 IPv6 接口，会生成一条对应的网络路由。
邻居缓存	与本机交互的主机信息，ARP 表和 ND 表合集。

2.2.3 CLI 参考命令

命令	switch(config)# interface vlan 10 switch(config)# no interface vlan 10
描述	创建/进入 Vlan 的 IP 接口； 删除 Vlan 的 IP 接口；

命令	switch(config-if-vlan)# ip address 192.168.200.100 255.255.255.0 switch(config-if-vlan)# ipv6 address 64:64::5/64

描述	配置 IPv4 地址以及掩码； 配置 IPv6 地址以及掩码；

命令	switch(config-if-vlan)# ip address dhcp switch(config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/3 switch(config-if-vlan)# ip address dhcp client-id ascii dhcp switch(config-if-vlan)# ip address dhcp client-id hex 1234ABCD
描述	配置接口通过 DHCPv4 协议配置接口的 IPv4 地址和掩码；客户端 ID 为 AUTO； 配置接口通过 DHCPv4 协议配置接口的 IPv4 地址和掩码；客户端 ID 为 IF_MAC； 配置接口通过 DHCPv4 协议配置接口的 IPv4 地址和掩码；客户端 ID 为 ASCII； 配置接口通过 DHCPv4 协议配置接口的 IPv4 地址和掩码；客户端 ID 为 HEX；

命令	switch(config-if-vlan)# ip address dhcp fallback 192.168.200.100 255.255.255.0 timeout 10
描述	配置接口通过 DHCPv4 协议配置接口的 IPv4 地址和掩码，同时配置回滚地址和回滚时间；

命令	switch(config)# ip route 1.1.1.0 255.255.255.0 192.168.1.1 100 switch(config)# no route 1.1.1.0 255.255.255.0 192.168.1.1
描述	配置 IPv4 路由表项，同时配置距离； 删除 IPv4 路由表项；

命令	switch(config)# ipv6 route 11:22::34/64 interface vlan 6 fe80::11 switch(config)# no ipv6 route 11:22::34/64 interface vlan 6 fe80::11
描述	配置 IPv6 路由表项，同时配置下一跳 vlan； 删除 IPv6 路由表项；

命令	switch# show interface vlan switch# show ipv6 route switch# show ip arp switch# show ipv6 neighbor
描述	查看 IP 接口； 查看 IPv6 路由； 查看 IPv4 邻居缓存； 查看 IPv6 邻居缓存；

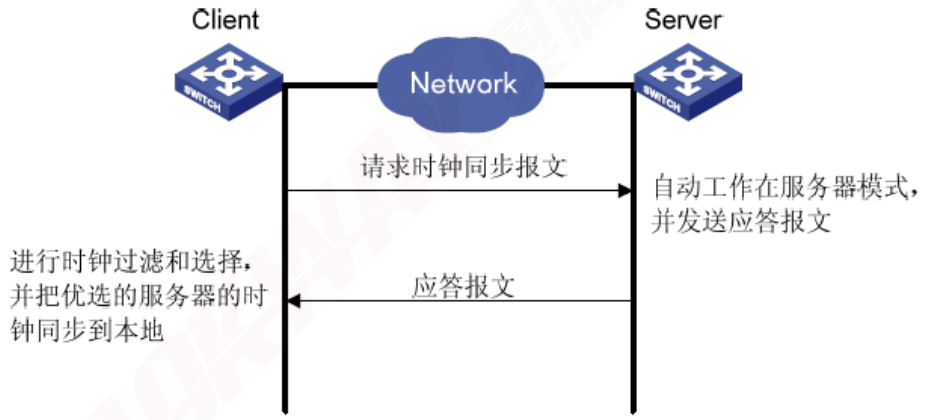
2.3 NTP

2.3.1 NTP 简述

NTP（Network Time Protocol，网络时间协议）是由 RFC1305 定义的时间同步协议，用于在分布式时间服务器和客户端之间进行时间同步。NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。

标准 NTP 支持服务器/客户端模式、对等体模式、广播模式、组播模式等。本设备仅支持服务器/客户端模式，且只能作为客户端。具体工作流程如下。

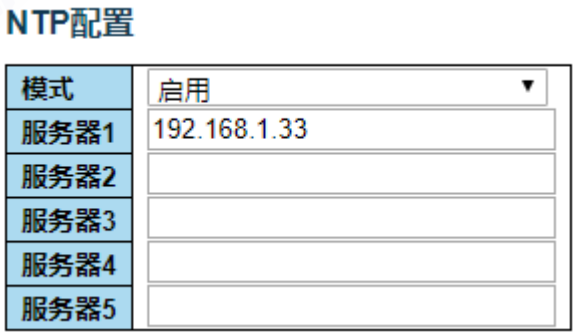
图表 2-5 NTP 服务器/客户端模式



2.3.2 配置 NTP

在【导航栏】下拉菜单中选择：配置->系统->NTP，进入配置界面。

图表 2-6 NTP 配置



配置项	说明
模式	使能控制 NTP 功能，默认关闭
服务器 1~5	NTP 服务器的 IP 地址，可在系统信息中查看时间信息确认 NTP 是否生效

2.3.3 CLI 参考命令

命令	switch(config)# ntp switch(config)# no ntp

描述	开启 NTP； 关闭 NTP；

命令	switch(config)# ntp server 1 ip-address 120.25.115.20 switch(config)# ntp server 2 ip-address 1::1 switch(config)# no ntp server 1
描述	配置 NTP 服务器地址为 IPv4； 配置 NTP 服务器地址为 IPv6； 删除 NTP 服务器地址；

2.4 时间

2.4.1 配置时间

在【导航栏】下拉菜单中选择：配置->系统->时间，进入配置界面。

图表 2-7 配置时间

配置项	子参数	说明
时区配置	时区	选择标准时区
	缩写	描述符
夏令时配置	夏令时	Disabled：关闭功能 Recurring：每年执行 Non-Recurring：只执行一次
	开始时间设置	夏令开始时间

	结束时间设置	夏令结束时间
	偏移设置	偏移分钟数

2.4.2 CLI 参考命令

命令	switch(config)# clock timezone '' 8 switch(config)# clock timezone china 8
描述	配置时区； 配置时区以及缩写；

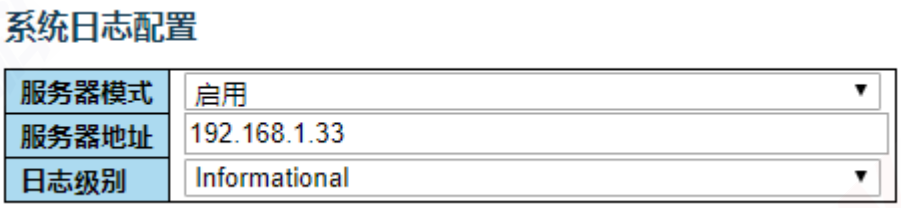
命令	switch(config)# clock summer-time '' recurring 1 3 3 03:04 4 1 4 07:06 123 switch(config)# clock summer-time '' date 3 1 2014 03:04 4 1 2097 07:06 100
描述	配置夏令时每年执行的循环开始、结束时间和偏移时间； 配置夏令时开始、结束日期时间和偏移时间，只执行 1 次；

2.5 日志

2.5.1 配置日志服务器

在【导航栏】下拉菜单中选择配置->系统->日志，进入配置界面。

图表 2-8 配置日志服务器



配置项	说明
服务器模式	开启/关闭日志送服务器功能
服务器地址	服务器的 IP 地址
日志级别	送服务器的日志级别，从低到高 Informational<Notice<Warning<Error

2.5.2 查看日记信息

在【导航栏】下拉菜单中选择：监控->系统->日志，进入查看界面。

图表 2-9 日志信息查看

系统日志信息

级别	All
清除级别	All

指定级别中总共有43条日志.

开始于ID 1 且 20 条每页.

ID	级别	时间	消息
1	Informational	1970-01-01T00:00:26+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T00:00:27+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	1970-01-01T00:00:27+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	1970-01-01T00:00:27+00:00	LINK-UPDOWN: Interface Vlan 1000, changed state to down.
5	Notice	1970-01-01T00:00:27+00:00	LINK-UPDOWN: Interface Vlan 1000, changed state to down.
6	Notice	1970-01-01T00:00:28+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.
7	Notice	1970-01-01T00:00:28+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/2, changed state to up.
8	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to up (MEP).
9	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/2, changed state to up (MEP).
10	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/3, changed state to up (MEP).
11	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/4, changed state to up (MEP).
12	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/5, changed state to up (MEP).
13	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/6, changed state to up (MEP).
14	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/7, changed state to up (MEP).
15	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/8, changed state to up (MEP).
16	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/9, changed state to up (MEP).
17	Notice	1970-01-01T00:00:30+00:00	LINK-CHANGED: Interface GigabitEthernet 1/10, changed state to up (MEP).
18	Notice	1970-01-01T00:00:30+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
19	Notice	1970-01-01T00:00:30+00:00	LINK-UPDOWN: Interface Vlan 1000, changed state to up.
20	Notice	1970-01-01T00:01:16+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

2.5.3 查看具体某条日记信息

在【导航栏】下拉菜单中选择：监控->系统->详细日志，进入查看界面。

图表 2-10 单条日志信息查看

详细系统日志信息

ID	14

消息

级别	Notice
时间	1970-01-01T00:00:30+00:00
消息	LINK-CHANGED: Interface GigabitEthernet 1/7, changed state to up (MEP).

2.5.4 CLI 参考命令

命令	switch(config)# logging on switch(config)# no logging on
描述	开启日志服务器; 关闭日志服务器;

命令	switch(config)# logging host 192.168.6.22 switch(config)# no logging host
描述	配置日志服务器 IPv4 地址; 删除日志服务器 IPv4 地址;

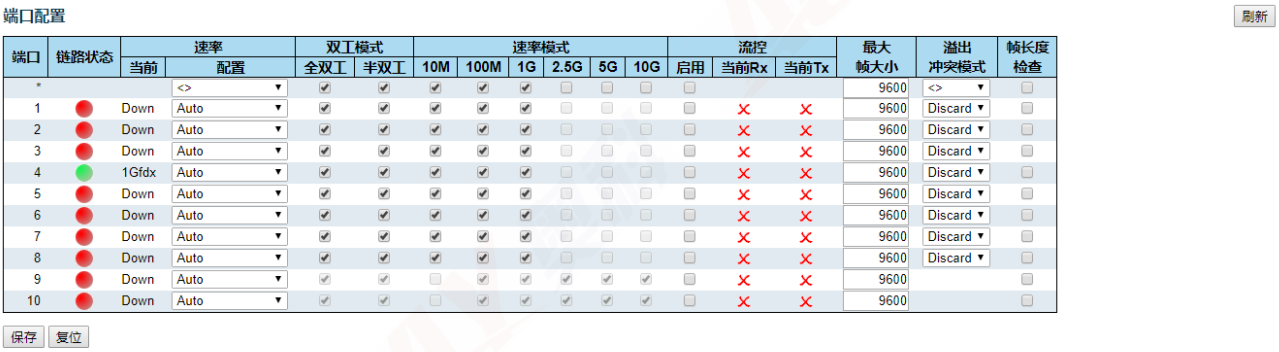
命令	switch# show logging switch# show logging 48
描述	查看日志信息; 查看具体某条日记信息;

3 端口

3.1 端口配置

在【导航栏】下拉菜单中选择：配置->端口，进入配置界面。

图表 3-1 端口配置



配置项	说明
端口	面板端口号
链路状态	当前端口 link 状态，绿灯表示端口 link，红灯表示端口 down
速率	分为配置速率与当前实际速率。当速率配置为 Auto 时以双工模式/速率模式所配置的能力通告为准，非 Auto 时表示强制设置成所配置的速率双工模式
双工模式/速率模式	端口能力通告，在 Speed Configured 配置为 Auto 时生效
流控	端口流控，默认关闭。当打开流控功能，Curr Rx 表示是否接收到对端流控信号，Curr Tx 表示是否发送流控信号。当端口为 100M 全双工时，不支持流控功能，自动关闭
最大帧大小	端口转发最大报文长度，范围 1518~9600bytes，已含 FCS 字段
溢出冲突模式	检测到端口发送冲突时处理行为，Discard 表示当冲突次数达到 16 次后丢弃报文，Restart 表示当冲突次数达到 16 次后，重启检测
帧长度检查	检测报文中 EtherType/Length 字段与实际报文数据长度是否一致

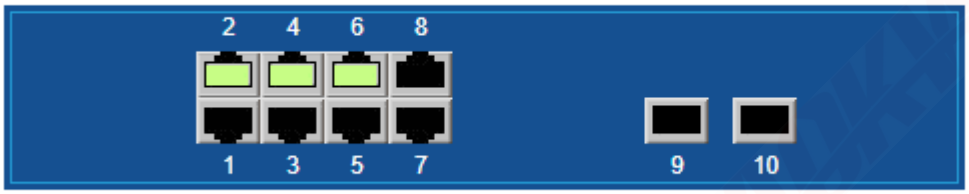
3.2 端口信息查看

3.2.1 端口状态

在【导航栏】下拉菜单中选择：监控->端口->状态，进入查看界面。

图表 3-2 端口状态显示

端口状态概况



亮绿灯表示端口 link，不亮灯表示端口 down。点击端口，自动跳转到端口报文统计详细信息页面。

3.2.2 端口报文统计概览

在【导航栏】下拉菜单中选择：监控->端口->流量概况，进入查看界面。

图表 3-3 端口统计概况

端口统计概况

端口	报文		字节		错误		丢弃		过滤
	接收	发送	接收	发送	接收	发送	接收	发送	接收
1	24609	3072	4514520	1351529	0	0	1294	0	10795
2	0	404	0	61908	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	3052	0	207536	0	0	0	0	0
10	0	3052	0	207536	0	0	0	0	0

3.2.3 端口队列报文统计

在【导航栏】下拉菜单中选择：监控->端口->Qos 统计，进入查看界面。

图表 3-4 端口 QOS 统计信息

队列计数

端口	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	24714	3054	0	0	0	0	0	0	0	0	0	0	0	0	0	167
2	0	235	0	0	0	0	0	0	0	0	0	0	0	0	0	169
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	3059	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	3059	0	0	0	0	0	0	0	0	0	0	0	0	0	0

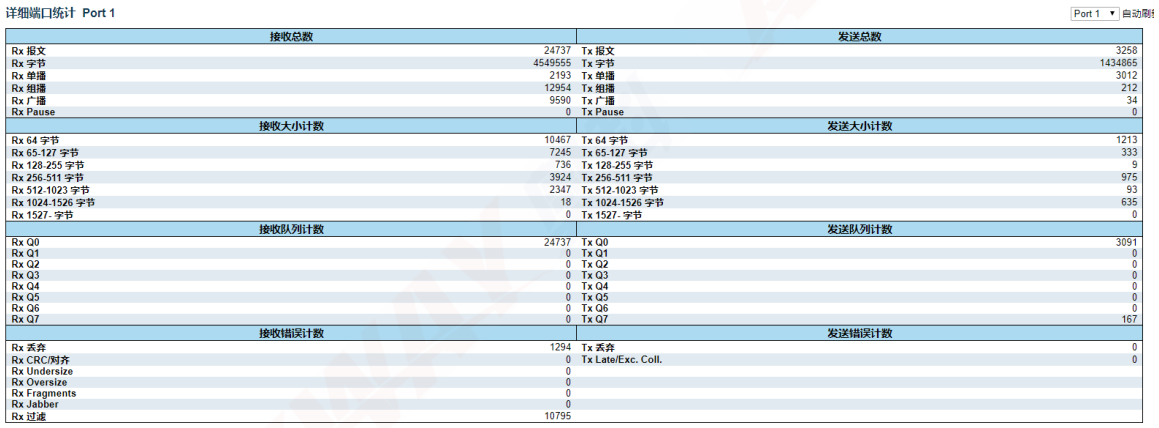
配置项	说明
端口	面板端口号，点击端口号进入该端口报文统计详细信息页面

Qn	端口队列 ID
Rx/Tx	队列接收、发送报文统计

3.2.4 端口报文统计详细信息

在【导航栏】下拉菜单中选择：监控->端口->详细统计，进入查看界面。

图表 3-5 端口详细统计信息


详细端口统计 Port 1

Port 1 自动刷

接收总数		发送总数	
Rx 报文	24737	Tx 报文	3258
Rx 字节	4549555	Tx 字节	1434865
Rx 单播	2193	Tx 单播	3012
Rx 组播	12954	Tx 组播	212
Rx 广播	9590	Tx 广播	34
Rx Pause	0	Tx Pause	0
接收大小计数		**发送大小计数**	
Rx 64 字节	10467	Tx 64 字节	1213
Rx 65-127 字节	7245	Tx 65-127 字节	333
Rx 128-255 字节	736	Tx 128-255 字节	9
Rx 256-511 字节	3924	Tx 256-511 字节	975
Rx 512-1023 字节	2347	Tx 512-1023 字节	93
Rx 1024-1526 字节	18	Tx 1024-1526 字节	635
Rx 1527- 字节	0	Tx 1527- 字节	0
接收队列计数		**发送队列计数**	
Rx Q0	24737	Tx Q0	3091
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	167
接收错误计数		**发送错误计数**	
Rx 丢弃	1294	Tx 丢弃	0
Rx CRC/对齐	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx 过滤	10795		

配置项	说明
接收总数	接收统计列表，包括报文个数、字节个数、单播、组播、广播、流控报文等
发送总数	发送统计列表，包括报文个数、字节个数、单播、组播、广播、流控报文等
接收大小计数	根据报文长度划分的接收统计列表
发送大小计数	根据报文长度划分的发送统计列表
接收队列计数	接收队列统计列表
发送队列计数	发送队列统计列表
接收错误计数	接收错包统计，包括丢弃报文、CRC 错误、过短、过长、分片报文、存在 CRC 错误的长包、过滤报文等
发送错误计数	发送错包统计，包括丢弃报文、因碰撞检测丢弃报文等

3.3 CLI 参考命令

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# speed auto switch(config-if)# duplex auto
描述	配置端口速率自动，能力通告所有支持的能力； 配置端口双工自动，能力通告所有支持的能力；

命令	switch(config-if)# speed auto 100 1000 switch(config-if)# speed 1000 switch(config-if)# duplex full
描述	配置端口速率自动，能力通告支持 100M/1000M； 配置端口速率强制为 1000M； 配置端口双工强制为 Full；

命令	switch(config-if)# flowcontrol on switch(config-if)# flowcontrol off
描述	启用端口流控； 关闭端口流控；

命令	switch(config-if)# mtu 9600
描述	配置端口最大帧大小；

命令	switch(config-if)# excessive-restart switch(config-if)# no excessive-restart
描述	配置端口溢出冲突模式为 Restart； 配置端口溢出冲突模式为 Discard；

命令	switch(config-if)# frame-length-check switch(config-if)# no frame-length-check
描述	启用端口帧长度检查； 关闭端口帧长度检查；

命令	switch# show interface * status switch# show interface GigabitEthernet 1/3 status
描述	查看所有端口状态； 查看指定端口状态；

命令	switch# show interface * statistics priority switch# show interface GigabitEthernet 1/3 statistics priority
描述	查看端口队列报文统计； 查看指定端口队列报文统计；

命令	switch# show interface * statistics switch# show interface GigabitEthernet 1/3 statistics
描述	查看端口报文统计详细信息； 查看指定端口报文统计详细信息；

4 DHCP

4.1 Snooping

DHCP Snooping 通过监控 DHCP 请求应答报文生成 DHCP Snooping 表，该表记录了 MAC 地址，VLAN ID，端口以及 IP 地址的关系。该数据表可以作用于安全的接入控制功能，主要是“IP Source Guard”和“ARP Inspection”功能，前者对 IP 报文进行接入控制，非法的 IP 报文不允许接入网络；后者对 ARP 报文进行接入控制，非法的 ARP 报文不允许接入网络。所以 DHCP Snooping 功能往往和安全接入控制功能同时作用在接入设备上。

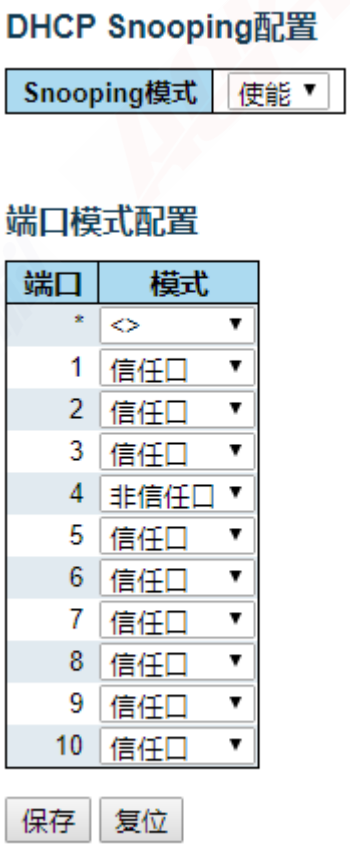
同时 DHCP Snooping 功能还可以做到防止 DHCP 服务器欺骗，通过其“信任口”功能做到。

- 收到的 DHCP 请求报文，只转发到信任口。
- 只有从信任口收到的 DHCP 应答报文才进行转发。

4.1.1 配置 Snooping

在【导航栏】下拉菜单中选择：配置->DHCP->Snooping，进入配置页面。

图表 4-1 DHCP Snooping 配置



- 全局使能

  DHCP Snooping 全局开关，默认禁用，只有使能，该功能才生效。

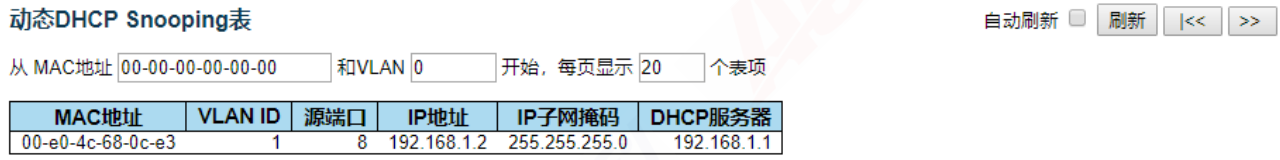
- 配置信任口

指定端口为信任口或者非信任口，默认所有端口均为信任口。

4.1.2 查看 Snooping

在【导航栏】下拉菜单中选择：监控->DHCP->Snooping 表，进入显示页面。

图表 4-2 DHCP Snooping 表显示



表头	说明
MAC 地址	表项对应的 DHCP 客户端的 MAC 地址。
VLAN ID	表项对应的 DHCP 客户端请求 IP 使用的 VLAN ID。
源端口	表项对应的 DHCP 客户端对应于交换机的面板端口。
IP 地址	表项对应的 DHCP 客户端申请得到的 IP 地址。
IP 子网掩码	表项对应的 DHCP 客户端申请得到的 IP 子网掩码。
DHCP 服务器	DHCP 服务器的 IP 地址。

4.1.3 CLI 参考命令

命令	switch(config)# ip dhcp snooping switch(config)# no ip dhcp snooping
描述	开启全局 DHCP Snooping； 关闭全局 DHCP Snooping；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# ip dhcp snooping trust switch(config-if)# no ip dhcp snooping trust
描述	配置端口为 DHCP Snooping 信任口； 配置端口为 DHCP Snooping 非信任口；

命令	switch# switch# show ip dhcp snooping table
描述	查看 DHCP Snooping 表；

4.2 Client

DHCP Client 功能在“配置 IP”章节描述。

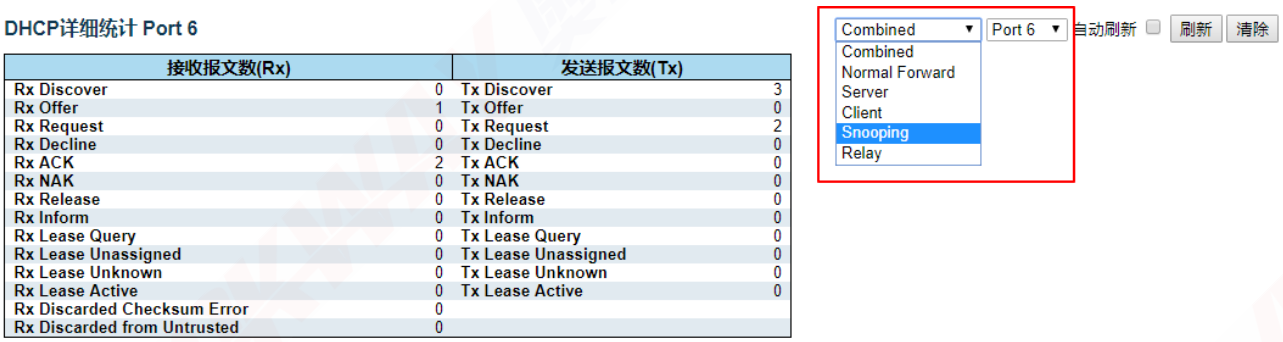
4.3 统计信息

4.3.1 查看统计信息

该页面统计了各种 DHCP 相关功能的 DHCP 报文的收发情况。当前只有 DHCP Snooping 和 DHCP Client 有效。

在【导航栏】下拉菜单中选择：监控->DHCP->详细统计，进入显示页面。

图表 4-3 DHCP 统计信息显示



参数	说明
RX/TX Discover	选项 53，值为 1。
RX/TX Offer	选项 53，值为 2。
RX/TX Request	选项 53，值为 3。
RX/TX Decline	选项 53，值为 4。
RX/TX ACK	选项 53，值为 5。
RX/TX NAK	选项 53，值为 6。
RX/TX Release	选项 53，值为 7。
RX/TX Inform	选项 53，值为 8。
RX/TX Lease Query	选项 53，值为 10。
RX/TX Lease Unassigned	选项 53，值为 11。
RX/TX Lease Unkown	选项 53，值为 12。
RX/TX Lease Active	选项 53，值为 13。
RX Discarded Checksum Error	IP / UDP 校验和错误丢弃的 DHCP 报文。
RX Discarded from Untrust	来自非信任口丢弃的 DHCP 报文。

第一个复选框用于选择 DHCP 应用，Combined 表示所有；

第二个复选框用于选择端口。

4.3.2 CLI 参考命令

命令	switch# show ip dhcp detailed statistics snooping switch# show ip dhcp detailed statistics snooping interface GigabitEthernet 1/3
描述	查看端口 DHCP Snooping 统计信息； 查看指定端口 DHCP Snooping 统计信息；

命令	switch# show ip dhcp detailed statistics client switch# show ip dhcp detailed statistics client interface GigabitEthernet 1/3
描述	查看端口 DHCP Client 统计信息； 查看指定端口 DHCP Client 统计信息；

5 安全

5.1 交换机

5.1.1 用户

系统默认用户名“admin”，无密码保护，管理用户登录后请尽快修改密码，并妥善保管好密码，避免出现因忘记密码无法登录的情况，设备不支持密码找回。

在【导航栏】下拉菜单中选择：配置->安全->交换机->用户，进入配置界面。

5.1.1.1 配置用户

图表 5-1 配置用户

在配置用户界面点击“添加用户”按键，进入新用户配置界面。

图表 5-2 添加用户

配置项	说明
用户名	用户名称，支持数字、字母、下划线组合，长度范围 1-31 字符
密码	支持所有键盘输出字符，包括空格，长度范围 0-31，为 0 表示不设置密码
密码（重复）	要求与上面的密码一致
优先级	设备针对用户划分 0-15 共 16 个优先级，不同优先级的用户可以执行的命令是不同的。数字小的级别权限较小，其中 0 级为最低级别，15 级为最高级别，可以执行所有的命令。用户优先级需高于模块读/写优先级，才可执行命令。

■ 编辑用户

在配置用户界面，直接点击用户名，进入用户编辑界面。

图表 5-3 编辑用户

支持密码与优先级的编辑操作，支持删除用户操作。

5.1.1.2 CLI 参考命令

命令	switch(config)# username user1 privilege 13 password unencrypted password1 switch(config)# no username user1
描述	添加用户； 删除用户；

5.1.2 优先级

5.1.2.1 配置优先级

设备支持对特定组独立设置其配置读写、状态读写优先级。若登录用户优先级大于组操作项的优先级，才可进行相应操作。如用户优先级为 5，组“Aggregation”配置/执行读/写优先级为 10，则用户无法对：配置->链路聚合->静态页面进行写操作。

在【导航栏】下拉菜单中选择：配置->安全->交换机->优先级，进入配置界面。

图表 5-4 配置模块优先级

优先级配置

组名	优先级			
	配置只读	配置/执行读/写	状态/统计只读	状态/统计读/写
Aggregation	5	10	5	10
Alarm	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
Firmware	5	10	5	10
FRR	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Mirroring	5	10	5	10
Miscellaneous	15	15	15	15
MRP	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
VLANs	5	10	5	10
XXRP	5	10	5	10

保存 复位

配置项	说明
组名	功能模块名称
配置 只读	配置界面的读权限优先级，当用户优先级小于模块的读权限优先级，不支持页面显示
配置/执行，读/写	配置界面的读/写权限优先级，当用户优先级小于模块的读/写权限优先级，页面不支持配置，模块的读/写优先级需大于只读优先级
状态/统计 只读	监控界面的读权限优先级，当用户优先级小于模块的读权限优先级，不支持页面显示
状态/统计 读/写	监控界面的读/写权限优先级，当用户优先级小于模块的读/写权限优先级，页面不支持配置，模块的读/写优先级需大于只读优先级

5.1.2.2 CLI 参考命令

命令	switch(config)# web privilege group Debug level configRoPriv 10 configRwPriv 10 statusRoPriv 5 statusRwPriv 10 switch(config)# no web privilege group Debug level

描述	配置模块优先级； 恢复模块默认优先级；

5.1.3 认证方法

5.1.3.1 配置认证方法

用户登录网络设备进行管理的时候，如果线路上设置了服务器认证（radius），需要通过远程 radius 服务器进行用户认证。如果线路上设置了本地认证（local），则需要通过本地用户数据库来根据用户名和密码进行用户的管理权限的认证。为提高网络安全，设备支持关闭认证，防止非法用户攻击。

支持 radius 和 local 2 个方法同时打开。

在【导航栏】下拉菜单中选择：配置->安全->交换机->认证方法，进入配置界面。

图表 5-5 配置认证方法

配置项	说明
客户端	支持的认证方式
方法	认证选择 radius 打开服务器认证，选择 local 打开本地认证，选择 no 关闭认证

5.1.3.2 CLI 命令

命令	switch(config)# aaa authentication login ssh radius local switch(config)# no aaa authentication login ssh
描述	配置认证方式； 关闭认证方式；

5.1.4 SSH

5.1.4.1 配置 SSH

注意

- SSH 认证请采用 SSH2 协议。

- 在 SSH2 的客户端，对“key exchange”内容，请选中“diffie-hellman”选项。

在【导航栏】下拉菜单中选择：配置->安全->交换机->SSH，进入配置界面。

图表 5-6 SSH 认证

配置项	说明
模式	Enabled 打开 SSH 认证，Disabled 关闭 SSH 认证

5.1.4.2 CLI 参考命令

命令	switch(config)# ip ssh switch(config)# no ip ssh
描述	开启 SSH； 关闭 SSH；

5.1.5 HTTPS

5.1.5.1 配置 HTTPS

在【导航栏】下拉菜单中选择：配置->安全->交换机->HTTPS，进入配置界面。

图 5-1 HTTPS 认证

图表 5-7 HTTPS 认证

配置项	说明
模式	使能 HTTPS 模式

自动重定向	使能开关，开启时 HTTP 连接会自动重定向到 HTTPS 连接
证书维护	None 表示无操作；Delete 表示删除当前证书，Upload 表示上传证书；Generate 表示重新生产证书。只有在关闭 HTTPS 模式的情况下才可以进行证书维护相关操作。
证书密码短语	在证书维护选择 Upload 时显示，输入通行短语
证书上传	选择证书上传方式，WEB 浏览器或网址
文件上传/网址	WEB 浏览器为选择本地上传文件，网址为输入 URL
证书状态	显示当前证书状态，有 presented、generating、not 三种状态

5.1.5.2 CLI 参考命令

命令	switch(config)# ip http secure-server switch(config)# no ip http secure-server
描述	开启 HTTPS 模式； 关闭 HTTPS 模式；

命令	switch(config)# ip http secure-redirect switch(config)# no ip http secure-redirect
描述	开启 HTTPS 自动重定向； 关闭 HTTPS 自动重定向；

命令	switch(config)# ip http secure-certificate delete switch(config)# ip http secure-certificate generate switch(config)# ip http secure-certificate upload http://192.168.6.100/cert-test.pem
描述	删除当前 HTTPS 证书； 生成一个自签名的 RSA 证书； 上传 HTTPS 证书；

命令	switch# show ip http
描述	查看 HTTPS 配置状态；

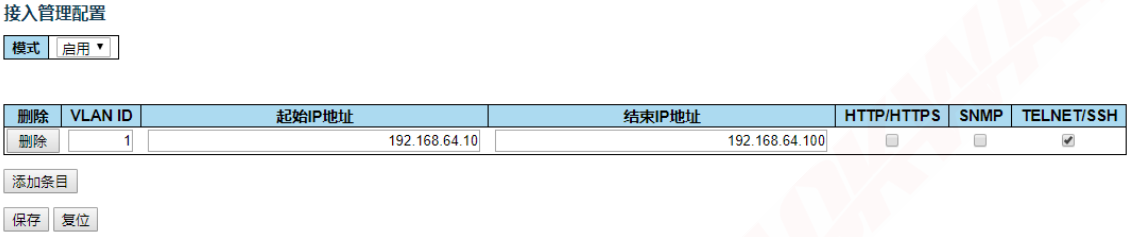
5.1.6 接入管理

5.1.6.1 配置接入管理

接入管理功能针对不同接入方式，对接入用户的 IP 地址范围进行限制，以提高接入安全。设备最多可配置 16 条接入安全策略，接入用户只需满足任何一条接入安全策略，则可正常访问设备。

在【导航栏】下拉菜单中选择：配置->安全->交换机->接入管理，进入配置界面。

图表 5-8 接入管理

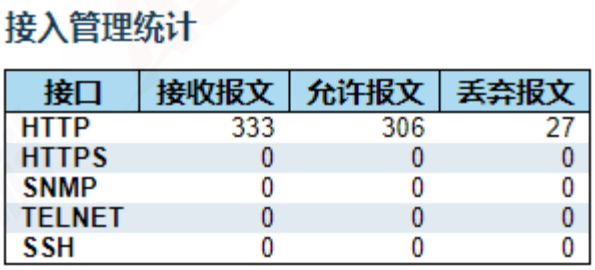


配置项	说明
模式	全局使能开关
VLAN ID	安全策略命中规则
起始 IP 地址	
结束 IP 地址	
HTTP/HTTPS	安全策略接入方式选择，至少选择一种，可选多种
SNMP	
TELNET/SSH	

5.1.6.2 查看接入管理统计

在【导航栏】下拉菜单中选择：监控->安全->接入管理统计，进入显示界面。

图表 5-9 接入管理统计



5.1.6.3 CLI 参考命令

命令	switch(config)# access management switch(config)# no access management
描述	开启接入管理策略； 关闭接入管理策略；

命令	switch(config)# access management 2 1 192.168.64.10 to 192.168.64.100 telnet switch(config)# no access management 2
描述	添加接入管理策略； 删除接入管理策略；

命令	switch# show access management switch# show access management statistics
描述	查看接入管理策略状态； 查看接入管理策略统计；

5.1.7 SNMP

5.1.7.1 概述

SNMP（Simple Network Management Protocol，简单网络管理协议）是因特网中的一种网络管理标准协议，被广泛用于实现管理设备对被管理设备的访问和管理。SNMP 具有以下特点：

- 支持网络设备的智能化管理。利用基于 SNMP 的网络管理平台，网络管理员可以查询网络设备的运行状态和参数，设置参数值，发现故障、完成故障诊断，进行容量规划和生成报告。
- 支持对不同物理特性的设备进行管理。SNMP 只提供基本的功能集，使得管理任务与被管理设备的物理特性和联网技术相对独立，从而实现对不同厂商设备的管理。

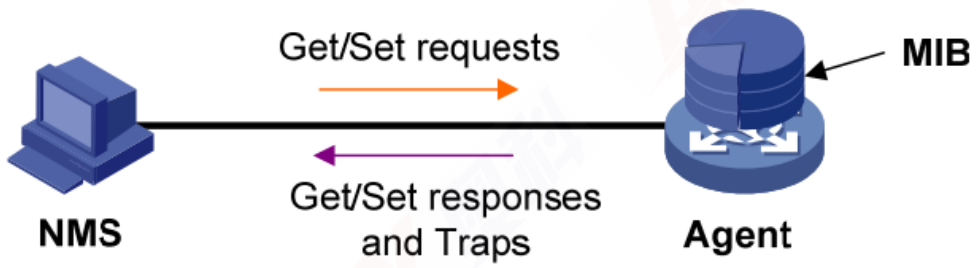
5.1.7.2 SNMP 的工作机制

SNMP 网络包含 NMS 和 Agent 两种元素。

- NMS（Network Management System，网络管理系统）是 SNMP 网络的管理者，能够提供非常友好的人机交互界面，方便网络管理员完成绝大多数的网络管理工作。
- Agent 是 SNMP 网络的被管理者，负责接收、处理来自 NMS 的请求报文。在一些紧急情况下，如接口状态发生改变等，Agent 会主动向 NMS 发送告警信息。

NMS 管理设备的时候，通常会对一些参数比较关注，比如接口状态、CPU 利用率等，这些参数的集合称为 MIB（Management Information Base，管理信息库）。这些参数在 MIB 中称为节点。MIB 定义了节点之间的层次关系以及对象的一系列属性，比如对象的名字、访问权限和数据类型等。每个 Agent 都有自己的 MIB。被管理设备都有自己的 MIB 文件，在 NMS 上编译这些 MIB 文件，就能生成该设备的 MIB。NMS 根据访问权限对 MIB 节点进行读/写操作，从而实现对 Agent 的管理。NMS、Agent 和 MIB 之间的关系如下。

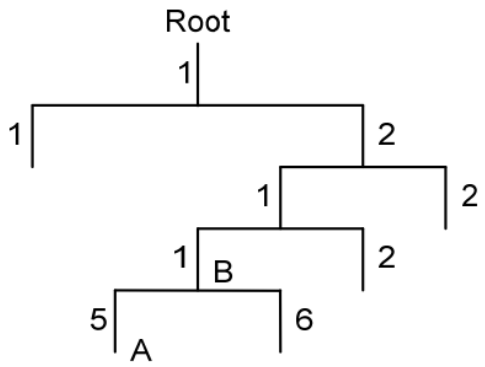
图表 5-10 NMS,Agent 和 MIB 的关系



MIB 是按照树型结构组织的，它由很多个节点组成，每个节点表示被管理对象，被管理对象可以用从根开始的一串表示路径的数字唯一地识别，这串数字称为 OID（Object Identifier，对象标识符）。

如下图所示，被管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字就是被管理对象 B 的 OID。

图表 5-11 MIB 树结构



SNMP 提供四种基本操作来实现 NMS 和 Agent 的交互：

- GET 操作：NMS 使用该操作查询 Agent MIB 中的一个或多个节点的值。
- SET 操作：NMS 使用该操作设置 Agent MIB 中的一个或多个节点的值。
- Trap 操作：Agent 使用该操作向 NMS 发送 Trap 信息。Agent 不要求 NMS 发送回应报文。

NMS 也不会对 Trap 信息进行回应。SNMPv1、SNMPv2c 和 SNMPv3 均支持 Trap 操作。

5.1.7.3 SNMP 的协议版本

目前 Agent 支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本：

- SNMPv1 采用团体名（Community Name）认证机制。团体名类似于密码，用来限制 NMS 和 Agent 之间的通信。如果 NMS 设置的团体名和被管理设备上设置的团体名不同，则 NMS 和 Agent 不能建立 SNMP 连接，从而导致 NMS 无法访问 Agent，Agent 发送的告警信息也会被 NMS 丢弃。
- SNMPv2c 也采用团体名认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展：提供了更多的操作类型；支持更多的数据类型；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以设置认证和加密功能。认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。采用认证和加密功能，可以为 NMS 和 Agent 之间的通信提供更高的安全性。

说明

NMS 和 Agent 成功建立连接的前提条件是 NMS 和 Agent 使用的 SNMP 版本必须相同。

5.1.7.4 SNMP 安全

SNMPv1 和 SNMPv2 版本使用认证名用来鉴别是否有权使用 MIB 对象。为了能够管理设备，网络管理系统 (NMS)的认证名必须同设备中定义的某个认证名一致。

一个认证名可以有以下属性：

- 只读(Read-only)：为被授权的管理工作站提供对所有 MIB 变量的读权限。

- 读写(Read-write)：为被授权的管理工作站提供对所有 MIB 变量的读写权限。

在SNMPv2的基础上，SNMPv3通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理；目前可用的安全模型有三种类别：SNMPv1、SNMPv2C、SNMPv3。

下表为目前可用的安全模型以及安全级别：

安全模型	安全级别	鉴别	加密	说明
SNMPv1	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv2c	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv3	noAuthNoPriv	用户名	无	通过用户名确认数据的合法性
SNMPv3	authNoPriv	MD5 或者 SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制
SNMPv3	authPriv	MD5 或者 SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制 提供基于 CBC-DES 的数据加密机制

5.1.7.5 SNMP 引擎标识

引擎标识用于唯一标识一个 SNMP 引擎。由于每个 SNMP 实体仅包含一个 SNMP 引擎，它将在一个管理域中唯一标识一个 SNMP 实体。因此，作为一个实体的 SNMPv3 Agent 必须拥有一个唯一的引擎标识，即 Engine ID。

引擎标识为一个 OCTET STRING，长度为 5～32 字节长。在 RFC3411 中定义了引擎标识的格式：

- 前 4 个字节标识厂商的私有企业号（由 IANA 分配），用 HEX 表示。
- 第 5 个字节表示剩下的字节如何标识：
- 0：保留
- 1：后面 4 个字节是一个 Ipv4 地址。
- 2：后面 16 个字节是一个 Ipv6 地址。
- 3：后面 6 个字节是一个 MAC 地址。
- 4：文本，最长 27 个字节，由厂商自行定义。
- 5：16 进制值，最长 27 个字节，由厂商自行定义。
- 6-127：保留。
- 128-255：由厂商特定的格式。

5.1.7.6 SNMP 配置

5.1.7.6.1 SNMP 系统配置

点击导航栏中：配置->安全->交换机->SNMP->系统，进入 SNMP 系统配置界面。

图表 5-12 SNMP 系统配置

配置项	说明
模式	SNMP 系统全局开关。
引擎 ID	SNMPv3 引擎 ID。 仅在版本号配置为 SNMP v3 时有效。 默认情况下会根据设备信息生成初始的引擎 ID。

5.1.7.6.2 SNMP 团体配置

点击导航栏中：配置->安全->交换机->SNMP->团体，进入 SNMP 团体配置界面。

仅 SNMP v1、SNMPv2 有效。

图表 5-13 SNMP 团体配置

配置项	说明
删除	选中后再下次保存时删除对应表项。
团体名称	通信团体名称。
团体 secret	通信团体字符串。
源 IP	允许使用该团体的服务器 IP 范围。
源掩码长度	允许使用该团体的服务器 IP 掩码长度。

注意

- 需要在 SNMP 组配置中添加对应团体名称的权限设置之后才能正常访问。系统默认配置了 public、private 这 2 个用户的访问权限。
- 团体配置仅对 SNMPv1、SNMPv2 生效，如果需要配置 SNMPv3，需要配置 SNMP 用户以及组。
- 实际应用中配置读、写团体时，如果设备配置团体名称和团体 secret 不一致时以团体 secret 为准。

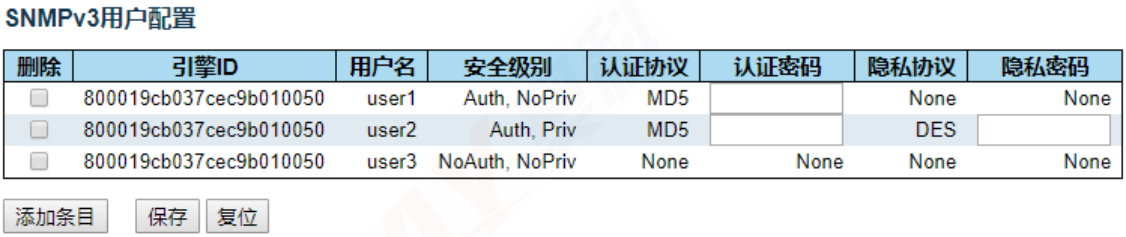
- 如果不关心团体服务器的 IP，请将源 IP 配置为 0.0.0.0，源掩码长度配为 0。

5.1.7.6.3 SNMP 用户配置

点击导航栏中：配置->安全->交换机->SNMP->用户，进入 SNMP 用户配置界面。

仅 SNMP v3 有效。

图表 5-14 SNMP 用户配置



配置项	说明
删除	选中后再下次保存时删除对应表项。
引擎 ID	用户所在引擎 ID。 通过引擎 ID 是否为本机引擎 ID 可以判断该用户是否为本地用户。 本机引擎 ID 参考系统配置中引擎 ID 配置。
用户名	用户名字符串。
安全级别	配置用户安全级别。
认证协议	认证协议类型。
认证密码	认证的密码字符串。
隐私协议	信息加密协议类型。
隐私密码	信息加密的密钥。

注意

- 需要在 SNMP 组配置中添加对应用户名的权限设置之后才能正常访问。

5.1.7.6.4 SNMP 组配置

点击导航栏中：配置->安全->交换机->SNMP->组，进入 SNMP 组配置界面。

图表 5-15 SNMP 组配置

SNMP组配置

删除	安全模型	安全名	组名
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	test	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	user1	v3_rw_gourp
☐	usm	user2	v3_rw_gourp
☐	usm	user3	v3_rw_gourp

添加条目 保存 复位

配置项	说明
删除	选中后再下次保存时删除对应表项。
安全模型	配置安全模型版本。 V1：兼容 SNMP v1 的安全模型。 V2c：兼容 SNMP v2 的安全模型。 Usm：SNMP v3 基于用户的安全模型。
安全名	V1/v2c 版本为对应团体名称。 V3 为用户名。
组名	SNMP 组名字符串。

⚠ 注意

- 需要在 SNMP 访问控制配置中添加对应的组名的相关配置之后才能正常访问。

5.1.7.6.5 SNMP 视图配置

点击导航栏中：配置->安全->交换机->SNMP->视图，进入 SNMP 视图配置界面。

图表 5-16 SNMP 视图配置

SNMP视图配置

删除	视图名称	视图类型	OID子树
☐	v3_view	included ▼	.1.3.6
☐	v3_view	excluded ▼	.1.3.6.2
☐	default_view	included ▼	.1

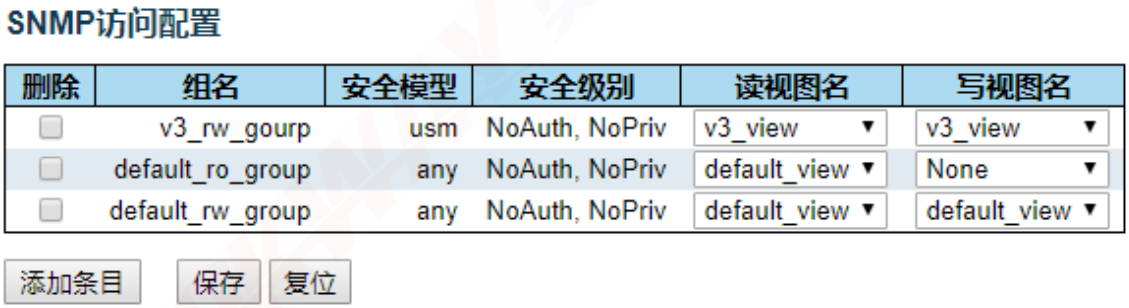
添加条目 保存 复位

配置项	说明
删除	选中后再下次保存时删除对应表项。
视图名称	视图名称字符串。
视图类型	Included：包含哪些 OID 子树。 Excluded：去除哪些 OID 子树。
OID 子树	OID 子树信息。

5.1.7.6.6 SNMP 访问控制配置

点击导航栏中：配置->安全->交换机->SNMP->访问，进入 SNMP 访问配置界面。

图表 5-17 SNMP 访问配置



配置项	说明
删除	选中后再下次保存时删除对应表项。
组名	SNMPv3 组名。
安全模型	配置安全模型版本。 V1：兼容 SNMP v1 的安全模型。 V2c：兼容 SNMP v2 的安全模型。 Usm：SNMP v3 基于用户的安全模型。 Any：所有安全模型均有效。
安全级别	配置安全级别。安全级别从大到小依次为“Auth,Priv” > “Auth,NoPriv” > “NoAuth,NoPriv”。
读视图名	读视图的名称。 None 表示无视图。
写视图名	写视图的名称。 None 表示无视图。

注意

- SNMP 访问控制中可配置的组名来自 SNMP 组配置，先在 SNMP 组配置中添加组名，再在 SNMP 访问控制中配置该组的安全及视图。
- SNMPv1、SNMPv2 用户所关联的组所对应的安全级别必须包含“NoAuth,NoPriv”，否则无法访问。

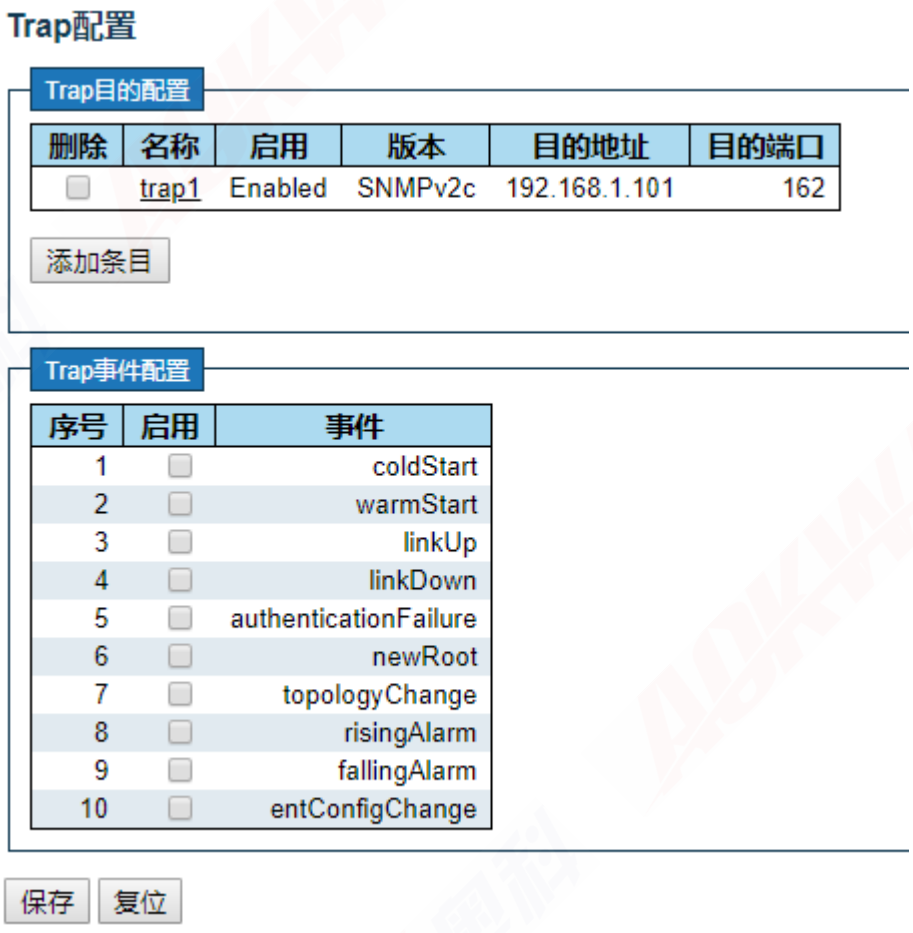
- SNMP 访问控制中的安全级别的优先级高于 SNMP 用户安全级别，SNMPv3 用户的安全级别如果小于所属组的访问控制安全级别，那么该 SNMP 用户将无法访问。例如：访问控制的安全级别是“Auth,NoPriv”，该访问控制所在组下的安全级别是“NoAuth,NoPriv” 的 SNMPv3 用户无法访问，“Auth,NoPriv”、“Auth,Priv” 的 SNMPv3 用户可以访问。

- SNMP 访问控制中的安全模型，相同的组名允许存在多个不同的安全模型，当相同组的不同安全模型存在交集（如：any，usm），但是配置的安全级别不一致的时候，取安全级别小的生效。即 SNMPv3 用户同时满足多个访问控制时，只需要满足其中一个的安全级别即可。

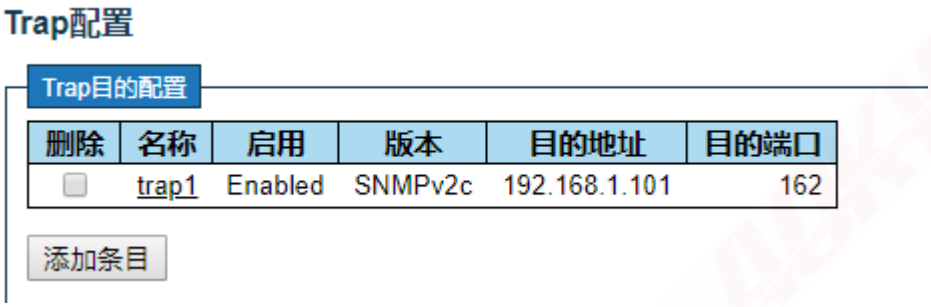
- SNMP 访问控制中的可配置的读、写视图来自 SNMP 视图配置，先在 SNMP 视图配置中添加视图，再在 SNMP 访问控制中关联该视图。

5.1.7.6.7 SNMP Trap 配置

点击导航栏中：配置->安全->交换机->SNMP->Trap，进入 SNMP Trap 配置界面。



图表 5-18 SNMP Trap 目的配置



点击【添加条目】按钮，进入 Trap 目的配置界面。

图表 5-19 SNMP Trap 目的配置

配置项	说明
Trap 配置名称	配置名称字符串。1-32 字节。
Trap 模式	当前 Trap 配置开关状态。
Trap 版本	当前 Trap 支持的协议版本。 需要保证 Trap 服务器能支持该版本。
Trap Community	Trap 通信 community。 仅 SNMPv2 有效。
Trap 目标地址	Trap 服务器 IP 地址。
Trap 目标端口	Trap 服务器侦听端口。
Trap 通告模式	使能/关闭 Trap 通告模式。 仅 SNMPv2 有效。
Trap 通告超时(秒)	通告报文超时时间设置。
Trap 通告重传次	通告报文超时重传次数设置。

数	
Trap 探测安全引擎 ID	使能/关闭自动探测 Trap 服务器安全引擎 ID。 仅 SNMP v3 有效。
Trap 安全引擎 ID	配置 Trap 安全引擎 ID。 当开启探测安全引擎 ID，系统会自动填充该字段，无需配置。 仅 SNMP v3 有效。
Trap 安全名称	Trap 通信的安全名。 仅 SNMP v3 有效。

图表 5-20 SNMP Trap 事件配置

配置项	说明
Trap 事件配置启用	选择需要支持的 Trap 事件。

5.1.7.7 CLI 参考命令

命令	switch(config)# snmp-server switch(config)# no snmp-server switch(config)# snmp-server engine-id local 800019cb037cec9b010051 switch(config)# no snmp-server engine-id local
描述	开启 SNMP 服务； 关闭 SNMP 服务； 配置 SNMP 引擎 ID 恢复 SNMP 默认引擎 ID

命令	switch(config)# snmp-server community user ip-range 0.0.0.0 0.0.0.0 user1 switch(config)# no snmp-server community user

描述	添加 SNMP 团体配置; 删除 SNMP 团体配置;

命令	switch(config)# snmp-server user v3user engine-id 800019cb037cec9b010050 switch(config)# snmp-server user v3user engine-id 800019cb037cec9b010050 md5 password switch(config)# snmp-server user v3user engine-id 800019cb037cec9b010050 md5 password priv des password switch(config)# no snmp-server user v3user engine-id 800019cb037cec9b010050
描述	添加 SNMP”NoAuth, NoPriv”用户配置; 添加 SNMP”Auth, NoPriv”用户配置; 添加 SNMP”Auth, Priv”用户配置; 删除 SNMP 用户配置;

命令	switch(config)# snmp-server community user ip-range 0.0.0.0 0.0.0.0 user1 switch(config)# no snmp-server security-to-group model v2c name test
描述	添加 SNMP 组配置; 删除 SNMP 组配置;

命令	switch(config)# snmp-server view v3_view .1.3.6.2 include switch(config)# no snmp-server view v3_view .1.3.6.2
描述	添加 SNMP 视图配置; 删除 SNMP 视图配置;

命令	switch(config)# snmp-server access v3_rw_gourp model v3 level noauth read default_view write default_view switch(config)# snmp-server access v3_rw_gourp model v3 level auth read default_view write default_view switch(config)# snmp-server access v3_rw_gourp model v3 level priv read default_view write default_view switch(config)# no snmp-server view v3_view .1.3.6.2
描述	添加 SNMP”NoAuth, NoPriv”访问控制配置; 添加 SNMP”Auth, NoPriv” 访问控制配置; 添加 SNMP”Auth, Priv” 访问控制配置; 删除 SNMP 访问控制配置;

命令	switch (config)# snmp-server host traphost switch (config)# no snmp-server host traphost

描述	创建/进入 SNMP Trap 目的配置； 删除 SNMP Trap 目的配置；

命令	switch(config-snmps-host)# shutdown switch(config-snmps-host)# no shutdown switch(config-snmps-host)# version v2 public switch(config-snmps-host)# version v3 engineID 800019cb037cec9b010050 user3 switch(config-snmps-host)# host 192.168.1.101 162 informs switch(config-snmps-host)# informs retries 5 timeout 3
描述	关闭该 SNMP Trap； 启用该 SNMP Trap； 配置该 SNMP Trap 的版本为 SNMPv2，且配置 Community； 配置该 SNMP Trap 的版本为 SNMPv3，且配置引擎 ID 和安全名称； 配置该 SNMP Trap 的目标地址、目标端口以及通告模式(informs、traps)； 配置该 SNMP Trap 的通告重传次数以及通告超时时间；

命令	switch(config)# snmp-server view v3_view .1.3.6.2 include switch(config)# no snmp-server view v3_view .1.3.6.2
描述	启用 SNMP Trap linkUp 事件； 关闭 SNMP Trap linkUp 事件；

命令	switch# show snmp switch# show snmp host switch# show snmp trap
描述	查看 SNMP 配置信息（包括系统、团体、组、视图以及访问控制）； 查看 SNMP Trap 目的配置； 查看 SNMP Trap 事件配置；

5.1.7.8 SNMP 配置案例

5.1.7.8.1 SNMPv2 配置

■ 案例需求

添加 SNMPv2 用户，读团体为 v2read；写团体为 v2write。限制只能 192.168.1.0/24 网段的用户访问。

■ 操作步骤

1. 添加 SNMP 读、写团体

图表 5-21 添加 SNMP 读、写团体配置

SNMPv1/SNMPv2团体配置

删除	团体名称	团体secret	源IP	源掩码长度
	public	public	0.0.0.0	0
	private	private	0.0.0.0	0
删除	v2user1	v2read	192.168.1.0	24
删除	v2user2	v2write	192.168.1.0	24

添加条目 保存 复位

2. 添加 SNMP 组配置，使用默认的 default_ro_group、default_rw_group 组。

图表 5-22 添加 SNMP 组配置

SNMP组配置

删除	安全模型	安全名	组名
	v1	public	default_ro_group
	v1	private	default_rw_group
	v2c	public	default_ro_group
	v2c	private	default_rw_group
删除	v2c	v2user1	default_ro_group
删除	v2c	v2user2	default_rw_group

添加条目 保存 复位

3. 客户端添加该SNMPv2用户，读团体为v2read；写团体为v2write。确定访问ip限制在192.168.1.0/24网段。

5.1.7.8.2 SNMPv3 配置

■ 案例需求

添加 SNMPv3 用户，安全级别为”Auth，Priv”。

■ 操作步骤

1. 添加 SNMP 用户，配置安全级别为”Auth，Priv”，同时配置上对应的协议、密码。

图表 5-23 添加 SNMP 用户配置

SNMPv3用户配置

删除	引擎ID	用户名	安全级别	认证协议	认证密码	隐私协议	隐私密码
删除	800019cb037cec9b010050	v3user	Auth, Priv	MD5	•••••••	DES	••••••

添加条目 保存 复位

2. 添加 SNMP 组配置，安全模型为 usm。使用默认的 default_rw_group 组。

图表 5-24 添加 SNMP 组配置

SNMP组配置

删除	安全模型	安全名	组名
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	v2c	v2user1	default_ro_group
☐	v2c	v2user2	default_rw_group
删除	usm ▼	v3user ▼	default_rw_group

添加条目 保存 复位

3. 客户端添加该 SNMPv3 用户，安全级别为”Auth，Priv”，同时输入对应的协议、密码。

注意！如果需要填写 Context Name 字段，请留空。

5.1.8 RMON

5.1.8.1 概述

RMON 全称是 Remote Network Monitoring，远端网络监控。RMON 用来解决从一个中心点管理各局域分网和进程站点的问题。RMON 中，网络监规数据包含了一组统计数据和性能指标，这些数据可以用来监控网络利用率，以用于网络规划，性能优化和协助网络错误诊断。RMON 主要用于管理设备向被监控管理设备迆行进程监控管理。

RMON 定义了多个 RMON 组，我司产品支持其中的统计组、历史组、告警组、事件组。下面对四个组做简要的介绍:

- 统计组

统计组(Statistics)用于对以太网接口的流量信息进行监控、统计，是从创建表项起到当前阶段的累加值，统计的内容包括丢弃的数据包、广播数据包、多播数据包、CRC 错误、大小块、冲突等，统计结果将保存在以太网统计表中以便管理员随时查看。

- 历史组

历史组(History)用于定期收集网络流量信息，记录每一个周期内的网络流量信息的累加值以及带宽利用率，并保存在历史控制表中以便管理员日后处理，它包含两个小组:

- HistoryControl 组用来设置采样间隔时间、采样数据源等控制信息。
- EthernetHistory 组为管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等统计信息的历叱数据。

- 告警组

告警组(Alarm)用于监控指定的 MIB(Management Information Base，管理信息库)对象，当这个 MIB 对象的值超过设定的上限值或低于设定的下限值时，会触发警报，警报被当作事件来处理。

■ 事件组

事件组（Event）用于定义事件的处理方式。当监控的 MIB 对象达到告警条件时，就会触发事件，事件有如下四种处理方式：

➢ 无：不做任何动作。

➢ 日志：将事件相关信息记录在日志记录表中，以便管理员随时查看。

➢ trap：向网管发送 Trap 消息告知该事件的发生。

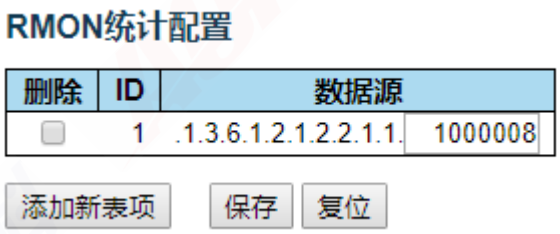
➢ 日志及 trap：将事件相关信息记录在日志记录表中，同时向网管发送 Trap 消息。

5.1.8.2 统计

■ 配置

在【导航栏】下拉菜单中选择：配置->安全->交换机->RMON->统计，进入配置界面。

图表 5-25 RMON 统计组配置



➢ 删除：选中后再下次保存时删除对应表项。

➢ ID：该表项唯一标识，范围从 1 到 65535。

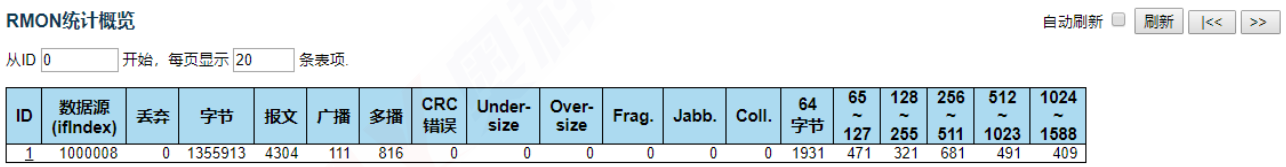
➢ 数据源：表示要监控的端口。要填写的文本框内容构成为：交换机 ID * 1000000 + 端口号。非堆叠系统交换机 ID 为 1，所以，端口 8 需要填写 1000008。

➢ 添加新表项：添加一条新表项。

■ 显示

在【导航栏】下拉菜单中选择：监控->安全->交换机->RMON->统计，进入显示界面。

图表 5-26 RMON 统计组显示



表头	说明

ID	统计表项的 ID。
数据源	要监视的端口的 ID。(交换机 ID * 1000000 + 端口号)，比如端口 8 为 1000008。
丢弃	由于缺少资源而导致探测器丢弃数据包的事件总数
字节	收到的报文的字节总数（包括坏报文的数据）。
报文	收到的报文总数（包括坏报文，广播报文和组播报文）。
广播	收到的指向广播地址的正常报文总数。
多播	收到的指向多播地址的正常报文总数。
CRC 错误	收到的报文长度（不包括帧起始位，但包括 FCS）在 64-1518 字节之间的，但 FCS 错误的报文总数。也包含对齐错误。
Undersize	收到的报文长度小于 64 字节的报文总数。
Oversize	收到的报文长度超过 1518 字节的报文总数。
Frag.	收到的 CRC 错误且报文长度小于 64 字节的报文总数。
Jabb.	收到的 CRC 错误且报文长度大于 1518 字节的报文总数。
Coll.	由于冲突导致的丢包总数。
64 字节	收到的报文长度为 64 字节的报文总数。
65~127	收到的报文长度为 65-127 字节的报文总数。
128~255	收到的报文长度为 128-255 字节的报文总数。
256~511	收到的报文长度为 256-511 字节的报文总数。
512~1023	收到的报文长度为 512-1023 字节的报文总数。
1024~1588	收到的报文长度为 1024-1588 字节的报文总数。

5.1.8.3 历史

- 配置

在【导航栏】下拉菜单中选择：配置->安全->交换机->RMON->历史，进入配置界面。

图表 5-27 RMON 历史组配置

配置项	说明
删除	选中后再下次保存时删除对应表项。
ID	该表项唯一标识，范围为 1-65535。
数据源	要监视的端口的 ID。(交换机 ID * 1000000 + 端口号)，比如端口 8 为

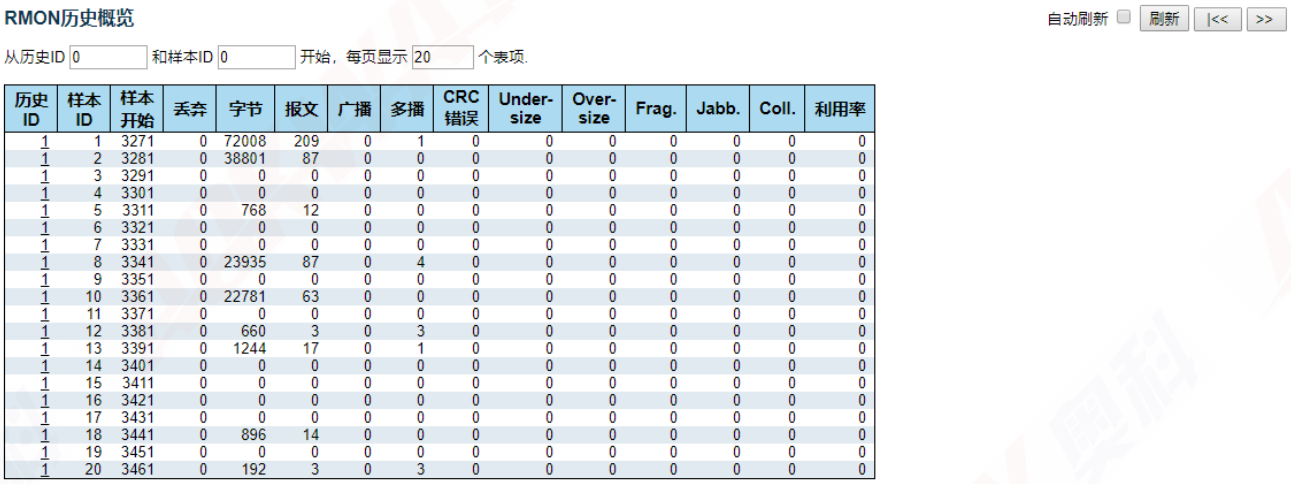
	1000008。
间隔	表示采样历史统计数据的时间间隔（秒）。范围为 1 到 3600，默认值为 1800 秒。
Buckets	表示存储在 RMON 中的此历史记录控制表项关联的最大数据条目。范围为 1 到 3600，默认值为 50。
Buckets Granted	表示授权的存储在 RMON 中的此历史纪录控制条目管理数据条目数。不可配置，根据配置值系统分配。

■ 显示

➢ 概览

在【导航栏】下拉菜单中选择：监控->安全->交换机->RMON->历史，进入配置界面。

图表 5-28 RMON 历史组概览



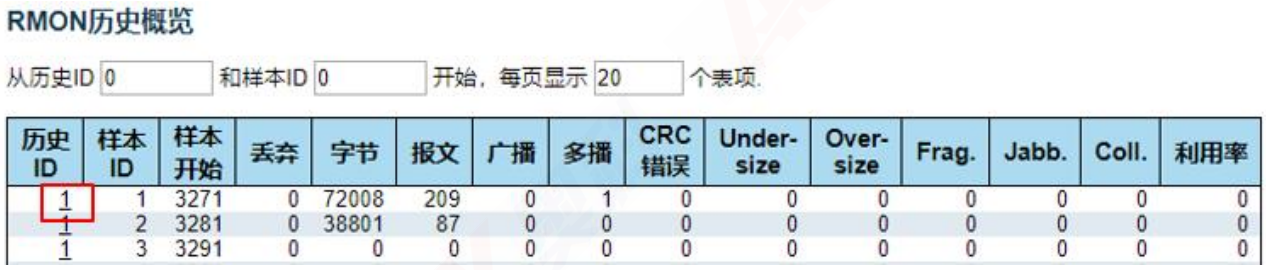
历史ID	样本ID	样本开始	丢弃	字节	报文	广播	多播	CRC错误	Under-size	Over-size	Frag.	Jabb.	Coll.	利用率
1	1	3271	0	72008	209	0	1	0	0	0	0	0	0	0
1	2	3281	0	38801	87	0	0	0	0	0	0	0	0	0
1	3	3291	0	0	0	0	0	0	0	0	0	0	0	0
1	4	3301	0	0	0	0	0	0	0	0	0	0	0	0
1	5	3311	0	768	12	0	0	0	0	0	0	0	0	0
1	6	3321	0	0	0	0	0	0	0	0	0	0	0	0
1	7	3331	0	0	0	0	0	0	0	0	0	0	0	0
1	8	3341	0	23935	87	0	4	0	0	0	0	0	0	0
1	9	3351	0	0	0	0	0	0	0	0	0	0	0	0
1	10	3361	0	22781	63	0	0	0	0	0	0	0	0	0
1	11	3371	0	0	0	0	0	0	0	0	0	0	0	0
1	12	3381	0	660	3	0	3	0	0	0	0	0	0	0
1	13	3391	0	1244	17	0	1	0	0	0	0	0	0	0
1	14	3401	0	0	0	0	0	0	0	0	0	0	0	0
1	15	3411	0	0	0	0	0	0	0	0	0	0	0	0
1	16	3421	0	0	0	0	0	0	0	0	0	0	0	0
1	17	3431	0	0	0	0	0	0	0	0	0	0	0	0
1	18	3441	0	896	14	0	0	0	0	0	0	0	0	0
1	19	3451	0	0	0	0	0	0	0	0	0	0	0	0
1	20	3461	0	192	3	0	3	0	0	0	0	0	0	0

表头	说明
历史 ID	历史控制表项的 ID。
样本 ID	指示与控制表项关联的数据条目的 ID。
样本开始	测试此样本开始时的时间，时间表示为设备启机开始到当前经过的秒数。
丢弃	此采样间隔期间由于缺少资源而导致探测器丢弃数据包的事件总数
字节	此采样间隔期间收到的报文的字节总数（包括坏报文的数据）。
报文	此采样间隔期间收到的报文总数（包括坏报文，广播报文和组播报文）。
广播	此采样间隔期间收到的指向广播地址的正常报文总数。
多播	此采样间隔期间收到的指向多播地址的正常报文总数。
CRC 错误	此采样间隔期间收到的报文长度（不包括帧起始位，但包括 FCS）在 64-1518 字节之间的，但 FCS 错误的报文总数。也包含对齐错误。
Undersize	此采样间隔期间收到的报文长度小于 64 字节的报文总数。
Oversize	此采样间隔期间收到的报文长度超过 1518 字节的报文总数。
Frag.	此采样间隔期间收到的 CRC 错误且报文长度小于 64 字节的报文总数。
Jabb.	此采样间隔期间收到的 CRC 错误且报文长度大于 1518 字节的报文总数。

Coll.	此采样间隔期间由于冲突导致的丢包总数。
利用率	此采样间隔期间此端口上平均物理层网络利用率的最佳估计值，以百分之一为单位。

➢ 详情

点击历史 ID，会显示对应历史 ID+样本 ID 确定数据条目详情。



图表 5-29 RMON 历史组详情

如上，显示历史 ID 为 1，样本 ID 为 168 的详情。

5.1.8.4 告警

■ 配置

在【导航栏】下拉菜单中选择：配置->安全->交换机->RMON->告警，进入配置界面。

图表 5-30 RMON 告警组配置

配置项	说明
删除	选中后再下次保存时删除对应表项。
ID	该表项唯一标识，范围为 1-65535。

间隔	采样时间间隔（秒），比较上升阈值和下降阈值。范围从 1 到 2 ^ 31-1。
变量	由两部分构成。 ➢ 第一段：采样类型，表示要采样的是哪种数据，值的范围为 10-21。 10：表示 InOctets，接口接收的字节数，包括帧间距。 11：表示 InUcastPkts，接口接收的单播报文数。 12：表示 InNUcastPkts，接口接收的非单播报文（即广播或多播）数。 13：表示 InDiscards，接收接收到但丢弃的报文数（即使正常报文被丢弃的也算在内）。 14：表示 InErrors，接口接收的错误报文数。 15：表示 InUnknownProtos，接口接收的属于未知协议或者不支持协议而丢弃的报文数。 16：表示 OutOctets，接口发送的字节数，包括帧间距。 17：表示 OutUcastPkts，接口发送的单播报文数。 18：表示 OutNUcastPkts，接口发送的非单播报文（即广播或多播）数。 19：表示 OutDiscards，接口上输出阶段丢弃的报文数（即使正常报文被丢弃也算在内）。 20：表示 OutErrors，接口由于报文错误而无法输出的报文数。 21：表示 OutQLen，接口输出队列的长度（以报文为单位，表示了报文在接口输出时的排队情况）。 ➢ 第二段:数据源,要监视的端口的 ID(交换机 ID * 1000000 + 端口号)，比如端口 8 为 1000008。
样本类型	对所选变量进行采样并计算要与水线进行比较的方法,可能的样本类型是: ➢ 绝对值：直接使用采样的值与水线进行比较。 ➢ 差值：使用两次相邻采样的值的差值与水线进行比较。
值	上次采样得到的值，非配置。
启动告警	启动告警的类型: ➢ 上升：当采样的绝对值或者差值（取决于样本类型）第一次大于上升水线时触发告警。 ➢ 下降：当采样的绝对值或者差值（取决于样本类型）第一次小于下降水线时触发告警。 ➢ 上升或下降：当采样的绝对值或者差值（取决于样本类型）第一次大于上升水线或者第一次小于下降水线时均可触发告警。
上升水线	取值 1-2147483647，且大于下降水线。
上升 ID	上升事件 ID，当触发上升告警时，对应的 ID。取值 1-65535。
下降水线	取值 1-2147483647，且小于上升水线。
下降 ID	下降事件 ID，当触发下降告警时，对应的 ID。取值 1-65535。

■ 显示

在【导航栏】下拉菜单中选择：监控->安全->交换机->RMON->告警，进入显示界面。

图表 5-31 RMON 告警组概览

RMON告警概览

从告警ID 0 开始，每页显示 20 条表项.

ID	间隔	变量	样本类型	值	启动告警	上升水线	上升ID	下降水线	下降ID
1	5	.1.3.6.1.2.1.2.2.1.12.1000002	差值	1	下降	1000	111	100	222
55	5	.1.3.6.1.2.1.2.2.1.11.1000002	差值	1	上升	1000	333	100	444

如上为概览信息，通过点击对应 ID，进入对应告警的详情页。

图表 5-32 RMON 告警组详情

RMON告警详情 ID 55

接收总计	
间隔	5
变量	.1.3.6.1.2.1.2.2.1.11.1000002
样本类型	差值
值	0
启动告警	上升
上升水线	1000
上升ID	333
下降水线	100
下降ID	444

这两个页面显示的信息页配置页信息并无差别。

5.1.8.5 事件

■ 配置

在【导航栏】下拉菜单中选择：配置->安全->交换机->RMON->告警，进入配置界面。

图表 5-33 RMON 事件组配置

RMON事件配置

删除	ID	描述	类型	最近产生事件的时间
☐	1	xxx	日志	6337

添加新表项 保存 复位

配置项	说明

删除	选中后再下次保存时删除对应表项。
ID	该表项唯一标识，范围为 1-65535。
描述	事件描述，字符串长度为 0 到 127，默认为空字符串。
类型	表示事件的处理类型，可能的类型是： 无：即无 SNMP 日志，也无 SNMP Trap。 日志：触发事件时创建 SNMP 日志条目。 trap：触发事件时发送 SNMP Trap。 日志及 trap：触发事件时创建 SNMP 日志条目并发送 SNMP Trap。
最近产生事件的时间	此事件条目上次触发事件时的时间。时间表示为设备启机开始到当前经过的秒数。非配置。

注意

- 如果要使得告警 Trap 生效，必须在 SNMP Trap 配置中配置目的 Trap，并在 SNMP Trap 事件中打开 risingAlarm、fallingAlarm 这两个 Trap 事件。

■ 显示

在【导航栏】下拉菜单中选择：监控->安全->交换机->RMON->告警，进入显示界面。

图表 5-34 RMON 事件组概览

RMON事件概览

从事件ID 0 和样本ID 0 开始,每页显示 20 条表项.

事件ID	日志ID	日志时间	日志描述
1	1	46	Startup Falling .1.3.6.1.2.1.2.2.1.12.1000002=97 <= 100 (1,222)
1	2	321	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1500 >= 1000 (1,111)
1	3	331	Falling .1.3.6.1.2.1.2.2.1.12.1000002=0 <= 100 (1,222)
1	4	346	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1501 >= 1000 (1,111)
1	5	361	Falling .1.3.6.1.2.1.2.2.1.12.1000002=1 <= 100 (1,222)
1	6	446	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1200 >= 1000 (1,111)
1	7	466	Falling .1.3.6.1.2.1.2.2.1.12.1000002=0 <= 100 (1,222)
1	8	728	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1500 >= 1000 (1,111)
1	9	748	Falling .1.3.6.1.2.1.2.2.1.12.1000002=1 <= 100 (1,222)
1	10	1314	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1500 >= 1000 (1,111)
1	11	1349	Falling .1.3.6.1.2.1.2.2.1.12.1000002=0 <= 100 (1,222)
1	12	1729	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1503 >= 1000 (1,111)
1	13	1759	Falling .1.3.6.1.2.1.2.2.1.12.1000002=0 <= 100 (1,222)
55	1	682	Startup Rising .1.3.6.1.2.1.2.2.1.11.1000002=1520 >= 1000 (55,333)
55	2	712	Falling .1.3.6.1.2.1.2.2.1.11.1000002=0 <= 100 (55,444)
55	3	1954	Rising .1.3.6.1.2.1.2.2.1.11.1000002=1206 >= 1000 (55,333)
55	4	1984	Falling .1.3.6.1.2.1.2.2.1.11.1000002=7 <= 100 (55,444)

表头	说明
事件 ID	指示事件标目的 ID。
日志 ID	一个事件可能触发多次，每触发一次即会产生一个日志条目，该 ID 表示日

	志条目的 ID。
日志时间	产生日志条目的时间。时间表示为设备启机开始到当前经过的秒数。
日志描述	日志内容，记录对应哪个告警产生的事件。其中 Startup 表示告警第一次触发。

点击上图的事件 ID，即可进入对应事件 ID+日志 ID 对应的日志条目详情页。

图表 5-35 RMON 事件组详情

RMON事件详情 ID 1

接收总计	
日志时间	9699
日志描述	Rising .1.3.6.1.2.1.2.2.1.12.1000002=1202 >= 1000 (1,111)

5.1.8.6 CLI 参考命令

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# rmon collection stats 22 switch(config-if)# no rmon collection stats 22 switch(config-if)# rmon collection history 34 buckets 50 interval 5 switch(config-if)# no rmon collection history 34
描述	添加 RMON 端口统计配置； 删除 RMON 端口统计配置； 添加 RMON 端口历史配置； 删除 RMON 端口历史配置；

命令	switch(config)# rmon alarm 1 ifInNUcastPkts 1000002 5 delta rising-threshold 1000 111 falling-threshold 100 222 falling switch(config)# no rmon alarm 1 switch(config)# rmon event 1 log trap description test switch(config)# no rmon event 1
描述	添加 RMON 告警配置； 删除 RMON 告警配置； 添加 RMON 事件配置； 删除 RMON 事件配置；

命令	switch# show rmon statistics

	switch# show rmon history switch# show rmon alarm switch# show rmon event
描述	打印 RMON 端口统计； 打印 RMON 端口历史统计； 打印 RMON 告警配置； 打印 RMON 事件位置以及相关日志；

5.2 网络

5.2.1 端口安全

端口安全，通过约束端口合法访问用户个数，达到降低单端口受攻击而导致系统不稳定的风险。用户可根据经验数值配置端口最大访问用户个数，当一定时间范围内访问用户个数超出用户限制个数时，将触发端口安全违例处理。处理有三种：Protect，Restrict 以及 Shutdown。

- Protect：当端口学习的 MAC 地址个数超过用户限制个数后触发违例。只允许源 MAC 为端口已学到 MAC 地址的报文被放行。
- Restrict：当端口学习的 MAC 地址个数超过用户限制个数后触发违例。超过个数的 MAC 地址被标记为违例地址，违例地址个数不超过配置的违例限制个数。违例地址在保持时间后将被删除。只允许源 MAC 为端口已学到 MAC 地址（不包括违例地址）的报文被放行。
- Shutdown：当端口学习的 MAC 地址个数达到用户限制个数后，任何一个新的 MAC 地址将会触发违例，端口 shutdown，之前学习的所有安全地址全部被清除，端口不可用，所有报文都不会被放行。

5.2.1.1 配置端口安全

在【导航栏】下拉菜单中选择：配置->安全->网络->端口安全，进入配置界面。

■ 系统配置

图表 5-36 端口安全系统配置

配置项	说明
启用老化	启用老化使能开关，默认关闭。
老化周期	端口正常 MAC 的老化周期，范围 10-10000000 秒，默认 3600 秒。只有启用老化后该参数才有意义。
持续时间	确定违例 MAC 地址在 MAC 表中的保留时间，范围 10-10000000 秒，默

	认 300 秒。

■ 端口配置

图表 5-37 端口安全端口配置

端口配置

端口	模式	用户限制	违例模式	违例限制	状态
*	<>	4	<>	4	
1	Disabled	4	Protect	4	Disabled
2	Disabled	4	Protect	4	Disabled
3	Disabled	4	Protect	4	Disabled
4	Disabled	4	Protect	4	Disabled
5	Disabled	4	Protect	4	Disabled
6	Disabled	4	Protect	4	Disabled
7	Disabled	4	Protect	4	Disabled
8	Enabled	4	Restrict	4	Ready
9	Disabled	4	Protect	4	Disabled
10	Disabled	4	Protect	4	Disabled

保存 复位

配置项	说明
端口	面板端口号。
模式	端口使能端口安全功能，默认关闭。
用户限制	端口最大用户数，范围 1-1023，默认为 4。
违例模式	Protect，Restrict，Shutdown，具体参见前文描述，默认为 Protect。
违例限制	当违例模式使用 Restrict 时使用，表示最多允许的违例 MAC 的个数。范围为 1-1023，默认为 4。
状态	Disabled，端口安全关闭。 Ready，端口安全开启，但用户数未达到用户限制个数。 Limite Reached，端口安全开启，用户数达到用户限制个数。 Shutdown，端口安全开启，违例模式为 Shutdown，且用户数超过用户限制个数。

注意

- 开启端口安全后，该端口学习到的 MAC 地址均变为静态地址（对 MAC 地址表模块而言），正常 MAC(未超过用户限制个数时)根据端口安全的“老化周期”来控制老化(默认不启动老化)，违例 MAC(在行为为 Restrict，且超过用户限制个数时)根据端口安全的“持续时间”来控制存在于表项中的时间。

- 违例模式配置成 Shutdown 时，当触发违例端口 shutdown 后，可以通过关闭端口安全或者更改安全违例模式为 Protect、Restrict 来恢复。

5.2.1.2 查看端口安全信息

在【导航栏】下拉菜单中选择：监控->安全->网络->端口安全->交换机，进入全局查看界面。

图表 5-38 查看端口安全信息

端口安全交换机状态

用户模块说明

用户模块名	缩写
Port Security (Admin)	P
802.1X	8

端口状态

清除	端口	用户	违例模式	状态	MAC计数		
					当前	违例	限制
清除	1	--	Disabled	Disabled	-	-	-
清除	2	--	Disabled	Disabled	-	-	-
清除	3	--	Disabled	Disabled	-	-	-
清除	4	--	Disabled	Disabled	-	-	-
清除	5	--	Disabled	Disabled	-	-	-
清除	6	--	Disabled	Disabled	-	-	-
清除	7	--	Disabled	Disabled	-	-	-
清除	8	P-	Restrict	Limit Reached	8	4	4
清除	9	--	Disabled	Disabled	-	-	-
清除	10	--	Disabled	Disabled	-	-	-

- 用户模块说明

  当前有两个模块会使用端口安全功能，一个就是端口安全模块，还有一个是 802.1X 模块，这里表明缩写方式。

- 端口状态

表头	说明
清除	点击清除该端口的所有端口安全 MAC 地址。只有当该端口的 MAC 地址不为 0 才能点击。
端口	面板端口号，点击可进入端口 MAC 地址信息查看界面。
用户	说明该 MAC 地址对应了哪个/哪些用户模块。
状态	Disabled，端口安全关闭。 Ready，端口安全开启，但用户数未达到用户限制个数。 Limite Reached，端口安全开启，用户数达到用户限制个数。

	Shutdown，端口安全开启，违例模式为 Shutdown，且用户数超过用户限制个数。
MAC 计数/当前	端口当前 MAC 地址数。
MAC 计数/违例	端口当前的违例 MAC 地址个数。
MAC 计数/限制	用户配置的端口用户限制个数。

在上图中点击对应端口，或者在【导航栏】下拉菜单中选择：监控->安全->网络->端口安全->端口，进入端口查看界面。

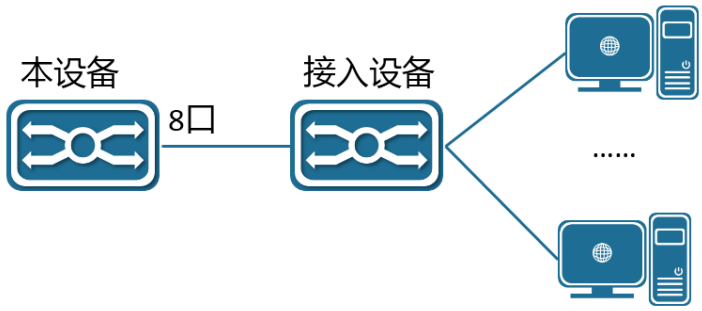
表头	说明
清除	点击清除对应用户信息。
VLAN ID	用户对应的 VLAN ID。
MAC 地址	用户对应的 MAC 地址。
状态	Forwarding：表示该用户为正常用户。 Violating：表示该用户为违例用户。
老化/保持	对正常用户，表示剩余老化时间，若未开启老化，显示为“-”。 对违例用户，表示剩余保持时间。

5.2.1.3 端口用户限制典型配置案例

■ 案例需求

系统环境中，端口 8 下联接入设备，扩展终端接入数量。正常运行时接入 8 口的用户应该不超过 10 个，若超过 10 个可能是非法用户接入或是终端发起 MAC 地址泛洪攻击，这时设备需自动执行防范操作，避免影响整个设备运行。

图表 5-39 端口用户限制案例



■ 操作步骤

端口用户限制配置界面，系统配置，全局使能端口限速功能；端口配置使能 8 口用户限制功能，用户限制为 10，选择行为 Shutdown。

图表 5-40 端口安全案例配置

端口安全配置

系统配置

启用老化	☐
老化周期	3600 秒
持续时间	300 秒

端口配置

端口	模式	用户限制	违例模式	违例限制	状态
*	<>	4	<>	4	
1	Disabled	4	Protect	4	Disabled
2	Disabled	4	Protect	4	Disabled
3	Disabled	4	Protect	4	Disabled
4	Disabled	4	Protect	4	Disabled
5	Disabled	4	Protect	4	Disabled
6	Disabled	4	Protect	4	Disabled
7	Disabled	4	Protect	4	Disabled
8	Enabled	10	Shutdown	4	Ready
9	Disabled	4	Protect	4	Disabled
10	Disabled	4	Protect	4	Disabled

保存 复位

在终端模拟 MAC 地址泛洪攻击，触发端口违例，通过查看界面查看，端口 8 处于 Shutdown 状态。

图表 5-41 端口安全案例状态

端口安全交换机状态

用户模块说明

用户模块名	缩写
Port Security (Admin)	P
802.1X	8

端口状态

清除	端口	用户	违例模式	状态	MAC计数		
					当前	违例	限制
清除	1	--	Disabled	Disabled	-	-	-
清除	2	--	Disabled	Disabled	-	-	-
清除	3	--	Disabled	Disabled	-	-	-
清除	4	--	Disabled	Disabled	-	-	-
清除	5	--	Disabled	Disabled	-	-	-
清除	6	--	Disabled	Disabled	-	-	-
清除	7	--	Disabled	Disabled	-	-	-
清除	8	P-	Shutdown	Shut Down	0	0	10
清除	9	--	Disabled	Disabled	-	-	-
清除	10	--	Disabled	Disabled	-	-	-

5.2.1.4 CLI 参考命令

命令	switch(config)# port-security aging switch(config)# port-security aging time 3600 switch(config)# port-security hold time 300
描述	开启端口安全地址老化； 配置端口安全地址老化周期； 配置端口安全违例地址持续时间；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# port-security switch(config-if)# no port-security switch(config-if)# port-security maximum 5 switch(config-if)# port-security violation shutdown switch(config-if)# port-security maximum-violation 4

描述	开启端口安全； 关闭端口安全； 配置端口安全用户限制数； 配置端口安全违例模式； 配置端口安全违例限制数；

命令	switch# clear port-security dynamic address 00-bb-60-2e-01-e4 vlan 1
描述	清除端口安全地址；

命令	switch# show port-security switch# show port-security address
描述	打印端口安全状态； 打印端口安全地址信息；

5.2.2 NAS

5.2.2.1 802.1X 协议概述

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（port based network access control protocol）。“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。

5.2.2.1.1 802.1X 的体系结构

802.1X 系统为典型的 Client/Server 结构，如下图所示，包括三个实体：客户端（Client）、设备端（Device，也叫做 NAS）和认证服务器（Server）。

图表 5-42 802.1X 体系结构

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 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）。

- 设备端是位于局域网段一端的另一个实体，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，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。

- 认证服务器是为设备端提供认证服务的实体。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（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。

5.2.2.1.2 802.1X 的认证方式

802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议），来实现客户端、设备端和认证服务器之间认证信息的交换。

- 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。
- 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文由设备端进行中继，使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是 EAP 协议报文由设备端进行终结，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocal，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证交互。

5.2.2.1.3 802.1X 的认证过程

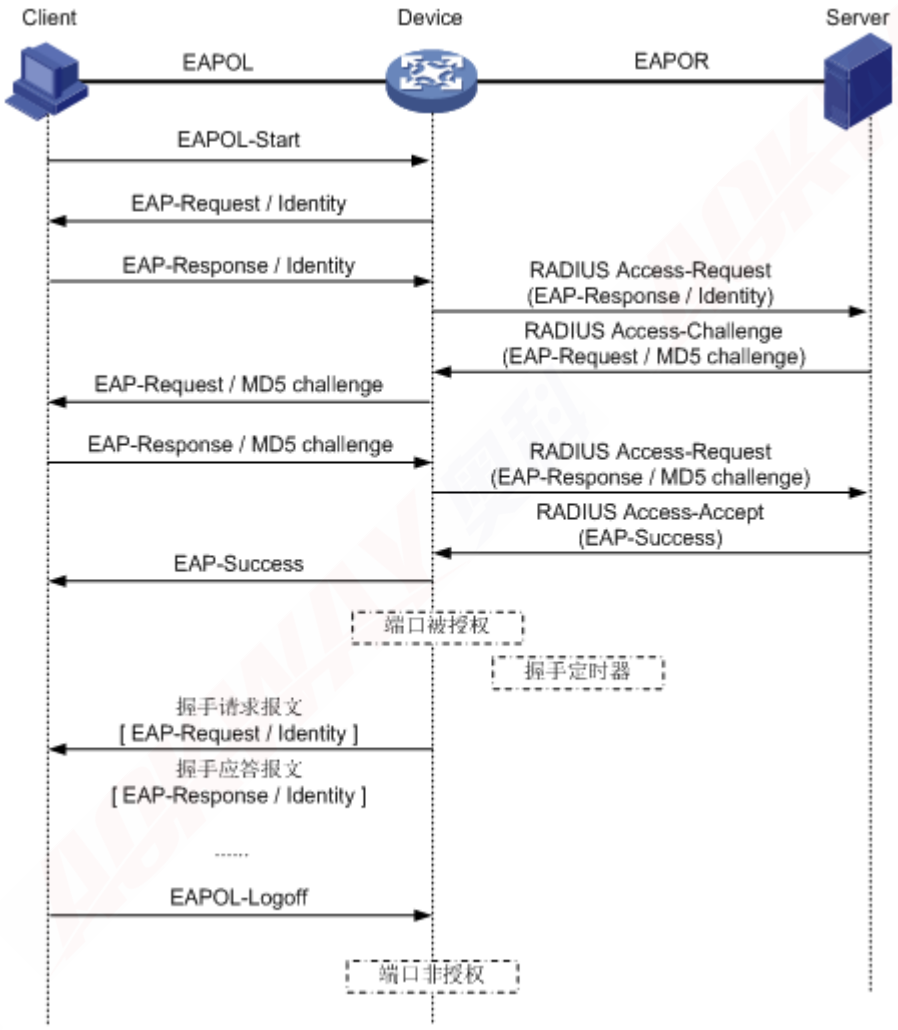
802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

■ EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP（可扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

下面以 EAP-MD5 方式为例介绍基本业务流程。

图表 5-43 802.1X EAP 中继方式认证



认证过程如下：

1) 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。
2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。
3) 客户端程序响应设备端发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。
4) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。
5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的），生成 EAP-Response/MD5 Challenge 报文，并通过设备端传给认证服务器。

6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。
7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。
8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线。设备端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

5.2.2.2 配置 NAS

NAS(Network Access Server)是对用户进行网络接入控制的功能，可以是基于 IEEE 802.1X 的认证，也可以是基于 MAC 的认证。

IEEE 802.1X 标准定义了基于端口的访问控制过程，该过程通过要求用户首先提交用于认证的凭证来防止对网络的未授权访问。一个或多个中央服务器（后端服务器）确定是否允许用户访问网络。这些后端（RADIUS）服务器在“配置→安全→AAA”页面上配置。

基于 MAC 的认证允许在同一端口上对多个用户进行认证，并且不要求用户在其系统上安装特殊的 802.1X 请求者软件。交换机使用用户的 MAC 地址对后端服务器进行认证。入侵者可以创建伪造的 MAC 地址，这使得基于 MAC 的认证不如 802.1X 认证安全。

在【导航栏】下拉菜单中选择：配置->安全->网络->NAS，进入配置界面。

■ 系统配置

图表 5-44 NAS 系统配置

配置项	说明
模式	指示交换机上是否全局使能或禁用 NAS 。如果全局禁用，则允许所有端口

	转发帧。
重认证使能	如果选中，则在重认证周期指定的间隔后，将成功通过认证的请求者/客户端重新进行认证。启用 802.1X 的端口的重新认证可用于检测新设备是否已插入交换机端口或是否已不再连接请求方。 对于基于 MAC 的认证，重认证仅在 RADIUS 服务器配置已更改时才有用。它不涉及交换机和客户端之间的通信，因此并不意味着客户端仍然存在于端口上。
重认证周期	确定必须重新进行认证的连接客户端的时间段（以秒为单位）。仅在选中“重认证使能”复选框时，此选项才处于活动状态。有效值的范围为 1 到 3600 秒。
EAPOL 超时时间	确定重新发送请求标识 EAPOL 帧的时间。有效值的范围为 1 到 65535 秒。这对基于 MAC 认证的端口没有影响。
老化周期	此设置适用于以下模式，即使用端口安全功能保护 MAC 地址的模式： •单用户 802.1X •多用户 802.1X •基于 MAC 的认证。 当 NAS 模块使用端口安全模块来保护 MAC 地址时，端口安全模块需要定期检查对应 MAC 是否活动，如果在给定的时间段内没有看到任何活动，则需要释放资源。此参数精确控制此时间段，可以设置为 10 到 1000000 秒之间的数字。如果启用了重认证且端口处于单用户 802.1X 认证或者多用户 802.1X 认证的模式，老化周期并不重要，因为不再连接到端口的请求者将在下次重新认证时被删除。但是，如果未启用重新认证，则释放资源的唯一方法是使条目老化。 对于基于 MAC 认证的端口。重新认证不会导致交换机和客户端之间的直接通信，因此这不会检测客户端是否仍然连接，并且释放任何资源的唯一方法是使条目老化。
保持时间	此设置适用于以下模式，即使用端口安全功能保护 MAC 地址的模式： •单用户 802.1X •多用户 802.1X •基于 MAC 的认证。 如果客户端被拒绝访问 - 要么是因为 RADIUS 服务器拒绝客户端访问，要么是因为 RADIUS 服务器请求超时（根据“配置→安全→AAA”页面上指定的超时） - 客户端被置于保持状态未经授权的状态。保持计时器在正在进行的认证期间不计数。对基于 MAC 的认证模式，交换机将在保持时间内忽略来自客户端的新帧。保持时间可以设置为 10 到 1000000 秒之间的数字。
RADIUS 指定 QOS 使能	RADIUS 指定 QoS 提供了一种集中控制流量类的方法，来自成功通过认证的请求方的流量在交换机上分配。必须将 RADIUS 服务器配置为传输特殊 RADIUS 属性才能利用此功能。 该复选框提供了一种全局启用/禁用 RADIUS 服务器指定 QoS 类功能的快

	速方法。选中后，各个端口的设置将确定是否在该端口上使能 RADIUS 指定 QoS 类。未选中时，将在所有端口上禁用 RADIUS 服务器指定 QoS 类。
RADIUS 指定 VLAN 使能	RADIUS 指定 VLAN 提供了一种集中控制成功通过认证的请求者在交换机上分配 VLAN 的方法。传入流量将被分类并切换到 RADIUS 分配的 VLAN。必须将 RADIUS 服务器配置为传输特殊 RADIUS 属性才能利用此功能。 该复选框提供了一种全局启用/禁用 RADIUS 服务器分配的 VLAN 功能的快速方法。选中后，各个端口的设置将确定是否在该端口上使能 RADIUS 指定 VLAN。未选中时，将在所有端口上禁用 RADIUS 服务器指定 VLAN
Guest VLAN 使能	Guest VLAN 是一个特殊的 VLAN - 通常具有有限的网络访问权限 - 在网络管理员定义的超时后，在该 VLAN 上放置不关注 802.1X 的客户端。交换机遵循一组用于进入和离开 Guest VLAN 的规则。 该复选框提供了全局启用/禁用 Guest VLAN 功能的快捷方式。选中时，各个端口的设置确定是否可以将端口移动到 Guest VLAN。取消选中后，将禁用所有端口移动到 Guest VLAN 的功能
Guest VLAN ID	如果端口移入 Guest VLAN，则此端口的端口 VLAN ID 设置为该值。只有全局使能了 Guest VLAN 选项，才可以更改它。有效值为 1-4095。
最大请求标识帧数	在考虑进入 Guest VLAN 之前，交换机在没有响应的情况下发送 EAPOL 请求标识帧的次数通过此设置进行调整。仅当全局使能了 Guest VLAN 选项时，才能更改该值。有效值为 1-255。
收到 EAPOL 允许进入 Guest VLAN	交换机会记住在生命周期内是否已在端口上收到 EAPOL 帧。一旦交换机考虑端口是否进入 Guest VLAN，它将首先检查是使能还是禁用此选项。如果禁用（未选中;默认），则只有在端口的生命周期内未在端口上收到 EAPOL 帧时，交换机才会进入访客 VLAN。如果启用（选中），即使在端口的生命周期内收到过 EAPOL 帧，交换机也会考虑进入 Guest VLAN。仅当全局使能了 Guest VLAN 选项时，才能更改该值。

■ 端口配置

配置端口的管理状态为基于端口的 802.1X，单用户 802.1X，多用户 802.1X 或者基于 MAC 的认证前，需要先关闭对应端口的 STP。（配置->生成树->CIST 端口页面，将“CIST 普通端口配置表”的“STP 启用”对应端口的复选框勾选去掉）

图表 5-45 NAS 端口配置

端口配置

端口	管理状态	RADIUS指定 QOS 使能	RADIUS指定 VLAN 使能	Guest VLAN 使能	端口状态	重启	
*	<>						
1	强制授权				全局禁用	重新认证	重新初始化
2	强制授权				全局禁用	重新认证	重新初始化
3	强制授权				全局禁用	重新认证	重新初始化
4	强制授权				全局禁用	重新认证	重新初始化
5	强制授权				全局禁用	重新认证	重新初始化
6	强制授权				全局禁用	重新认证	重新初始化
7	强制授权				全局禁用	重新认证	重新初始化
8	强制授权				全局禁用	重新认证	重新初始化
9	强制授权				全局禁用	重新认证	重新初始化
10	强制授权				全局禁用	重新认证	重新初始化

配置项	说明
管理状态	如果 NAS 全局使能，则此选择控制端口的认证模式。可以使用以下模式: ➢ 强制授权 在此模式下，交换机将在端口链路启动时发送一个 EAPOL Success 帧，并且端口上的任何客户端都将被允许进行网络访问而无需认证。 ➢ 强制未授权 在此模式下，当端口链路启动时，交换机将发送一个 EAPOL Failure 帧，并且端口上的任何客户端都将被禁止网络访问。 ➢ 基于端口的 802.1X 在 802.1X 中，用户称为请求者，交换机是验证者，RADIUS 服务器是验证服务器。验证者充当中间人，在请求者和验证服务器之间转发请求和响应。在请求者和交换机之间发送的帧是特殊的 802.1X 帧，称为 EAPOL（EAP Over LANs）帧。EAPOL 帧封装了 EAP PDU（RFC3748）。交换机和 RADIUS 服务器之间发送的帧是 RADIUS 数据包。RADIUS 数据包还将 EAP PDU 与其他属性（如交换机的 IP 地址，名称和交换机上的请求方端口号）一起封装。EAP 非常灵活，因为它允许不同的认证方法，如 MD5-Challenge，PEAP 和 TLS。重要的是认证者（交换机）不需要知道请求者和认证服务器正在使用哪种认证方法，或者特定方法需要多少信息交换帧。交换机简单地将帧的 EAP 部分封装到相关类型（EAPOL 或 RADIUS）中并转发它。 认证完成后，RADIUS 服务器会发送包含成功或失败指示的特殊数据包。除了将此决定转发给请求者之外，交换机还使用它来打开或阻止连接到请求者的交换机端口上的流量。 ➢ 单用户 802.1X 在基于端口的 802.1X 认证中，一旦在端口上成功验证请求者，就会为网络流量打开整个端口。这允许连接到端口的其他客户端（例如通过集线器）在成功通过认证的客户端上捎带并获得网络访问，即使它们确实未经过认

	证。要克服此安全漏洞，可以使用单用户 802.1X 认证模式。 单用户 802.1X 实际上不是 IEEE 标准，但具有许多与基于端口的 802.1X 相同的特性。在单用户 802.1X 中，一次最多只能有一个请求者在端口上进行认证。正常的 EAPOL 帧用于请求者和交换机之间的通信。如果多个请求者连接到一个端口，那么当端口链接出现时首先出现的请求者将是第一个请求者。如果该请求者在一定时间内未提供有效凭证，则另一个请求者将有机会获得。成功验证请求者后，只允许该请求者访问。这是所有模式中最安全的。在此模式下，端口安全模块用于在成功通过认证后保护请求方的 MAC 地址。 ➢ 多用户 802.1X 多用户 802.1X - 就像单用户 802.1X - 不是 IEEE 标准，而是具有许多相同特征的变体。在多用户 802.1X 中，一个或多个请求者可以同时在同一端口上进行认证。每个请求者都单独进行认证，并使用端口安全模块在 MAC 表中进行保护。 在多用户 802.1X 中，不能将组播 BPDU MAC 地址用作从交换机向请求方发送的 EAPOL 帧的目标 MAC 地址，因为这会导致连接到端口的所有请求方回复从交换机发送的请求。相反，交换机使用请求者的 MAC 地址，该地址是从请求者发送的第一个 EAPOL Start 或 EAPOL Response Identity 帧获得的。例外情况是还没有任何请求者，在这种情况下，交换机使用 BPDU 多播 MAC 地址作为目标发送 EAPOL 请求标识帧 - 以唤醒可能在端口上的任何请求者。可以使用端口安全限制控制功能限制可以连接到端口的最大请求者数。 ➢ 基于 MAC 的认证 与基于端口的 802.1X 不同，基于 MAC 的认证不是标准，而仅仅是业界采用的最佳实践方法。在基于 MAC 的认证中，用户称为客户端，交换机代表客户端充当请求者。客户端发送的初始帧（任何类型的帧）都被交换机窥探，交换机在随后与 RADIUS 服务器的 EAP 交换中使用客户端的 MAC 地址作为用户名和密码。交换机仅支持 MD5-Challenge 认证方式，因此必须相应配置 RADIUS 服务器。 认证完成后，RADIUS 服务器会发送成功或失败指示，从而导致交换机使用端口安全模块打开或阻止该特定客户端的流量。只有这样，才能在交换机上转发来自客户端的帧。此认证中不涉及 EAPOL 帧，因此，基于 MAC 的认证与 802.1X 标准无关。基于 MAC 的认证优于基于 802.1X 的认证的优势在于客户端不需要特殊的请求者软件进行认证。缺点是恶意用户可能会欺骗 MAC 地址 - 任何人都可以使用 MAC 地址为有效 RADIUS 用户的设备，此外，仅支持 MD5-Challenge 方法。可以使用端口安全限制控制功能限制可以连接到端口的最大客户端数。
RADIUS 指定 QOS 使能	当 RADIUS 指定 QoS 全局使能并在给定端口上使能（选中）时，交换机会对请求方成功通过认证时 RADIUS 服务器发送的 RADIUS Access-Accept 数

	据包中携带的 QoS 类信息作出反应。如果存在且有效，则在请求者端口上接收的流量将被分类到给定的 QoS 等级。如果（重新）认证失败或 RADIUS Access-Accept 数据包不再携带 QoS 类或无效，或者请求者在端口上不再存在，则端口的 QoS 类会立即恢复为原始 QoS 类（管理员可以在不影响 RADIUS 指定的情况下进行更改。此选项仅适用于基于端口的 802.1X。 用于标识 QoS 类的 RADIUS 属性（User-Priority-Table）：RFC4675 中定义了 Access-Accept 数据包中 QoS 类。只考虑数据包中第一次出现的属性，属性值中的 8 个字节均为范围为“0” – “7”的 ASCII 字符'。该属性给出了用户优先级[0:7]的映射值，第 0 个字节给出了优先级为 0 报文映射后的用户优先级，第 1 个字节给出了优先级为 1 的报文映射后的用户优先级。以此类推。
RADIUS 指定 VLAN 使能	当 RADIUS 指定 VLAN 全局使能并使能（选中）对应端口时，交换机会对请求方成功通过身份验证时 RADIUS 服务器传输的 RADIUS Access-Accept 数据包中携带的 VLAN ID 信息作出反应。如果存在且有效，则端口的端口 VLAN ID 将更改为此 VLAN ID，该端口将设置为该 VLAN ID 的成员，并且该端口将被强制进入 VLAN 不感知模式。分配后，到达端口的所有流量将被分类并切换到 RADIUS 分配的 VLAN ID。 如果(重新)身份验证失败或 RADIUS Access-Accept 数据包不再携带 VLAN ID 或无效，或者端口上不再存在请求者，则端口的 VLAN ID 会立即恢复为原始 VLAN ID（管理员可以在不影响 RADIUS 分配的情况下进行更改。 该选项仅适用于单客户端模式，即 •基于端口的 802.1X •单用户 802.1X 有关 VLAN 分配的故障排查，请使用“监控→VLAN→VLAN 成员和 VLAN 端口”页面。这些页面显示哪些模块覆盖了当前的端口 VLAN 配置。 用于标识 VLAN ID 的 RADIUS 属性：RFC2868 和 RFC3580 定义了 Access-Accept 数据包中的 VLAN ID 的属性。 •Tunnel-Medium-Type,Tunnel-Type 以及 Tunnel-Private-Group-ID 在 Access-Accept 数据包的属性中都必须同时存在至少一次。 •交换机查找具有相同 Tag 值并满足以下要求的第一组属性(如果使用 Tag 为 0，Tunnel-Private-Group-ID 则不需要包含 Tag）： -Tunnel-Medium-Type 必须设置为“IEEE-802”的值（序数 6）。 -Tunnel-Type 必须设置为“VLAN”（序号 13）。 -Tunnel-Private-Group-ID 必须是“0” - “9”范围内的 ASCII 字符串，它被解释为表示 VLAN ID 的十进制字符串。最终值范围为 1-4095。
Guest VLAN 使能	当 Guest VLAN 全局使能并使能（选中）指定端口时，交换机会根据下面列出的规则考虑将端口移动到 Guest VLAN。此选项仅适用于基于 EAPOL 的模式，即:

	•基于端口的 802.1X •单用户 802.1X •多用户 802.1X 有关 VLAN 分配的故障排查，请使用“监控→VLAN→VLAN 成员和 VLAN 端口”页面。这些页面显示哪些模块覆盖了当前的端口 VLAN 配置。 当使能了 Guest VLAN 的端口链接时，交换机开始发送 EAPOL Request Identity（请求标识）帧。如果这些帧的传输次数超过限制值（参见“系统配置”中的“最大请求标识帧数”）同时没有收到 EAPOL 帧，交换机考虑进入 Guest VLAN。EAPOL 请求标识帧的传输间隔使用“EAPOL 超时时间”（参见”系统配置”）配置。如果使能了“收到 EAPOL 允许进入 Guest VLAN”选项，则该端口现在将进入 Guest VLAN。如果禁用了选项，交换机将首先检查其历史记录，以查看端口上是否先前收到过 EAPOL 报文（如果端口链路断开或端口的管理状态已更改，则清除此历史记录），若未收到过 EAPOL 报文，则端口将被移动到 Guest VLAN 中。否则它将不会移动到 Guest VLAN，而是继续以“EAPOL 超时时间”给定的速率发送 EAPOL 请求标识帧。 进入 Guest VLAN 后，该端口将被视为已通过身份验证，并且允许该端口上的所有连接客户端访问此 VLAN。进入 Guest VLAN 时，交换机不会发送 EAPOL Success 帧。 在 Guest VLAN 中，交换机将监视这个链路的 EAPOL 报文，如果收到一个 EAPOL 报文，交换机立即将该端口从 Guest VLAN 中取出，并根据端口模式开始验证请求者。如果禁用“收到 EAPOL 允许进入 Guest VLAN”选项，且收到 EAPOL 报文，则端口将永远无法返回 Guest VLAN。
端口状态	端口的当前状态。可以采用以下值之一： **全局禁用**： NAS 全局禁用。 **Link Down**： NAS 全局启用，但端口没有 link。 **授权**：端口处于强制授权状态或单一请求方模式，授权方为授权方。 **未授权**：端口处于强制未授权状态或单一请求方模式，并且 RADIUS 服务器未成功授权请求方。 **X 个授权/ Y 个未授权**：端口处于多请求方模式。目前 X 个客户端已获得授权，Y 个客户端未经授权。 基于端口的 802.1X 和单用户 802.1X 属于单一请求方模式；多用户 802.1X 和基于 MAC 的认证属于多请求方模式。
重启	每行有两个按钮。仅当全局使能 NAS 且端口的管理状态处于基于 802.1X 的模式或基于 MAC 的认证模式时，才会启用这些按钮。 单击这些按钮不会导致页面上的设置更改生效。 **重新认证**：每当端口的静默期用完时安排重新认证（基于 802.1X 的模式）。对于基于 MAC 的认证，将立即尝试重新认证。该按钮仅对端口上成功通过认证的客户端有效，并且不会导致客户端出现瞬时的未经授权。

	重新初始化：强制重新初始化端口上的客户端，从而立即重新进行认证。在重新认证过程中，客户端将转移到未授权状态。

5.2.2.3 查看 NAS

在【导航栏】下拉菜单中选择：监控->安全->网络->NAS，将展开两个 NAS 的显示子菜单。分别为“交换机”和“端口”

■ 交换机

图表 5-46 NAS 交换机状态显示

表头	说明
端口	交换机端口号。单击可跳转到此端口的详细 NAS 统计信息。
管理状态	端口的当前管理状态，详细说明参见端口的 NAS 配置。
端口状态	端口的当前状态，详细说明参见端口的 NAS 配置。
上次源	对于基于 EAPOL 的认证，指最近一次收到的 EAPOL 帧中携带的源 MAC 地址，对基于 MAC 的认证，指最近一次收到的来自新客户端的帧携带的源 MAC 地址。
上次 ID	对于基于 EAPOL 的认证，指最近一次收到的响应标识 EAPOL 帧中携带的用户名（请求者身份），对基于 MAC 的认证，指最近一次收到的来自新客户端的帧的源 MAC 地址。
QOS 分类	如果使能“RADIUS 指定 QOS”，RADIUS 服务器分配给端口的 QoS 分类。如果未分配，显示为“-”。
端口 VLAN	NAS 将端口放入的 VLAN ID。如果端口 VLAN ID 未被 NAS 覆盖，则该字段为空。 如果 VLAN ID 由 RADIUS 服务器分配，"(RADIUS-assigned)"则附加到 VLAN ID 后面。 如果端口移动到 Guest VLAN，"(Guest)"则会附加到 VLAN ID 后面。

■ 端口

该页面提供运行基于 EAPOL 的 IEEE 802.1X 认证的特定交换机端口的详细 NAS 统计信息。对于基于 MAC 认证的端口，它仅显示选定的后端服务器（RADIUS 认证服务器）统计信息。使用端口选择框选择要显示的端口详细信息。针对不同的管理状态，端口显示的相应信息不尽相同。

针对单用户认证模式，即基于端口的 802.1X 和单用户 802.1X，显示分为两个部分：

端口状态和端口计数。

图表 5-47 NAS 端口状态及计数显示 1

针对多用户认证模式，即多用户 802.1X 和基于 MAC 的认证，显示分为四个部分：

端口状态，端口计数，所选计数以及关联请求者（针对多用户 802.1X）或者关联客户（针对基于 MAC 的认证）。

图表 5-48 NAS 端口状态及计数显示 2

- 端口状态

  该表中的信息时在“交换机”页面中基于端口的每行中显示信息的子集，不再详述。

- 端口计数

  端口计数信息分为三个部分：EAPOL 计数，后端服务器计数和上次请求者信息。

  - EAPOL 计数

    EAPOL 计数可用于以下管理状态：

    •强制授权

    •强制未授权

    •基于端口的 802.1X

    •单用户 802.1X

    •多用户 802.1X

EAPOL 计数			
方向	名称	IEEE 名称	描述
RX	总数	dot1xAuthEapolFramesRx	交换机已接收的任何类型的有效 EAPOL 帧数。
RX	应答 ID	dot1xAuthEapolRespIdFramesRx	交换机已收到的有效 EAPOL 响应标识帧数。
RX	应答计数	dot1xAuthEapolRespFramesRx	交换机已收到的有效 EAPOL 响应帧数（响应标识帧除外）。
RX	开始	dot1xAuthEapolStartFramesRx	交换机已收到的 EAPOL Start 帧数。
RX	下线	dot1xAuthEapolLogoffFramesRx	交换机已收到的有效 EAPOL Logoff 帧数。
RX	非法类型	dot1xAuthInvalidEapolFramesRx	无法识别帧类型的交换机已接收的 EAPOL 帧数。
RX	非法长度	dot1xAuthEapLengthErrorFramesRx	数据包正文长度字段无效的交换机已接收的 EAPOL 帧数。

TX	**总数**	dot1xAuthEapolFramesTx	由交换机传输的任何类型的 EAPOL 帧数。
TX	**请求 ID**	dot1xAuthEapolReqIdFramesTx	交换机已传输的 EAPOL 请求标识帧数。
TX	**请求计数**	dot1xAuthEapolReqFramesTx	交换机发送的有效 EAPOL 请求帧数（请求标识帧除外）。

✧ 后端服务器计数

后端服务器计数可用于以下管理状态:

•基于端口的 802.1X

•单用户 802.1X

•多用户 802.1X

•基于 MAC 的认证

后端服务器计数			
方向	**名称**	**IEEE 名称**	**描述**
RX	**访问 Challege**	dot1xAuthBackendAccessChallenges	**基于 802.1X：** 计算交换机在请求者的第一个响应之后从后端服务器接收第一个请求的次数。表示后端服务器与交换机进行通信。 **基于 MAC：** 计算从后端服务器为此端口（最左侧的表）或客户端（最右侧的表）接收的所有访问质询。
RX	**其他请求**	dot1xAuthBackendOtherRequestsToSupplicant	**基于 802.1X：** 计算交换机在第一个之后向请求方发送 EAP 请求数据包的次数。表示后端服务器选择了 EAP 方法。 **基于 MAC：** 不适用。
RX	**认证成功**	dot1xAuthBackendAuthSuccesses	**基于 802.1X 和 MAC：** 计算交换机收到成功指示的次数。表示请求者 /客户端已成功通过认证
RX	**认证失败**	dot1xAuthBackendAuthFails	**基于 802.1X 和 MAC：** 计算交换机收到失败消息的次数。这表示请求者 /客户端尚未向后端服务器进行认证。
TX	**应答计数**	dot1xAuthBackendResponses	**基于 802.1X：** 计算交换机尝试将请求方的第一个响应数据包发送到后端服务器的次数。表示交换机尝试与后端服务器通信。可能的重传不计算在内。 **基于 MAC：** 计算从交换机发送到后端服务器的所有后端服务器数据包，用于给定端口（最左边的表）或客户端（最右边的表）。可能的重传不计算在内。

✧ 上次请求者信息（针对基于 802.1X）或者上次客户信息（针对基于 MAC 的认证）

尝试进行认证的最后一个请求者/客户端的信息。此信息适用于以下管理状态:

•基于端口的 802.1X

•单个 802.1X

•多个 802.1X

•基于 MAC 的身份验证。

最后的请求者/客户信息		
名称	IEEE 名称	描述
MAC 地址	dot1xAuthLastEapolFrameSource	最后一个请求者/客户的 MAC 地址。
VLAN ID	-	收到最后一个请求者/客户的最后一帧的 VLAN ID 。
版本	dot1xAuthLastEapolFrameVersion	**基于 802.1X：** 最近收到的 EAPOL 帧中携带的协议版本号。 **基于 MAC：** 不适用。
ID	-	**基于 802.1X：** 最近收到的响应标识 EAPOL 帧中携带的用户名（请求者标识）。 **基于 MAC：** 不适用。

- 所选计数

当端口处于以下管理状态之一，并且端口状态不为“未授权”时（处于“X 个授权/Y 个未授权”，可以看到该表：

•多用户 802.1X

•基于 MAC 的认证

该表与端口计数表相同并位于其旁边，如果当前未选择 ID(针对多用户 802.1X)或者 MAC 地址（针对基于 MAC 的认证），则该表将为空。要填充表格，请从关联请求者/客户表中选择一个 ID 或者 MAC 地址。

- 关联请求者（多用户 802.1X）/客户（基于 MAC 的认证）

表头	说明
ID	显示应答标识 EAPOL 帧中收到的请求者的标识。单击该链接会使请求者的 EAPOL 和后端服务器计数显示在“所选计数”表中。此列不适用于基于 MAC 的认证。
MAC 地址	对于多用户 802.1X，此列保存关联的请求者的 MAC 地址。 对于基于 MAC 的认证，此列包含连接的客户端的 MAC 地址，且形成超链接，单击该链接会使客户端的后端服务器计数显示在“所选计数”表中。
VLAN ID	此列包含当前通过端口安全模块保护相应客户端的 VLAN ID。
状态	客户端可以是“已授权”的，也可以是“未授权”的。在已授权的状态下，允许在端口上转发帧，在未授权的状态下，它将被阻止。只要后端服务器未成功验证客户端，它就是未授权的。如果由于某种原因导致认证失败，则客户端将保持未授权状态若干秒（其具体时间由 NAS 的系统配置的“保持时间”确定。
上次认证	显示上次认证客户端的日期和时间（成功和失败）。

- 清除

✧ 清除：此按钮在以下模式下可用：

•强制授权

•强制未授权

•基于端口的 802.1X

•单用户 802.1X

单击以清除所选端口的计数。

✧ 全部清除：此按钮在以下模式下可用：

•多个 802.1X

•基于 MAC 的 Auth.X

单击以清除端口计数器和所有连接的客户端计数器。但是，“上次请求/客户信息”不会被清除。

✧ 清除当前：此按钮在以下模式下可用：

•多个 802.1X

•基于 MAC 的 Auth.X

单击仅清除当前选定的请求者或者客户端计数，即“所选计数”。

5.2.2.4 CLI 参考命令

命令	switch(config)# dot1x system-auth-control switch(config)# no dot1x system-auth-control switch(config)# dot1x re-authentication switch(config)# no dot1x re-authentication
描述	开启 NAS 功能； 关闭 NAS 功能； 开启 NAS 重认证； 关闭 NAS 重认证；

命令	switch(config)# dot1x authentication timer re-authenticate 3600 switch(config)# dot1x timeout tx-period 30 switch(config)# dot1x authentication timer inactivity 300 switch(config)# dot1x timeout quiet-period 11
描述	配置 NAS 重认证周期； 配置 NAS EAPOL 超时时间； 配置 NAS 老化周期； 配置 NAS EAPOL 超时保持时间；

命令	switch(config)# dot1x feature radius-qos

	switch(config)# no dot1x feature radius-qos switch(config)# dot1x feature radius-vlan switch(config)# no dot1x feature radius-vlan
描述	开启 NAS RADIUS 指定 QoS 使能; 关闭 NAS RADIUS 指定 QoS 使能; 开启 NAS RADIUS 指定 VLAN 使能; 关闭 NAS RADIUS 指定 VLAN 使能;

命令	switch(config)# dot1x feature guest-vlan switch(config)# no dot1x feature guest-vlan switch(config)# dot1x guest-vlan 2 switch(config)# dot1x max-reauth-req 3 switch(config)# dot1x guest-vlan supplicant switch(config)# no dot1x guest-vlan supplicant
描述	开启 NAS Guest VLAN 使能; 关闭 NAS Guest VLAN 使能; 配置 NAS Guest VLAN ID; 配置 NAS 最大请求标识帧数; 开启 NAS 收到 EAPOL 允许进入 Guest VLAN; 关闭 NAS 收到 EAPOL 允许进入 Guest VLAN;

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口;

命令	switch(config-if)# dot1x port-control force-authorized switch(config-if)# dot1x port-control force-unauthorized switch(config-if)# dot1x port-control auto switch(config-if)# dot1x port-control single switch(config-if)# dot1x port-control multi switch(config-if)# dot1x port-control mac-based switch(config-if)# dot1x radius-qos switch(config-if)# dot1x radius-vlan switch(config-if)# dot1x guest-vlan
描述	配置端口强制授权; 配置端口强制未授权; 配置端口基于端口的 802.1X; 配置端口基于单用户的 802.1X; 配置端口基于多用户的 802.1X; 配置端口基于 MAC 的认证; 配置端口 RADIUS 指定 QoS 使能; 配置端口 RADIUS 指定 VLAN 使能;

	配置端口 Guest VLAN 使能；

命令	switch# show dot1x status switch# show dot1x statistics all
描述	打印 NAS 状态； 打印 NAS 端口统计信息；

5.2.3 ACL

ACLs (Access Control Lists，接入控制列表)，也称为访问列表（Access Lists），俗称为防火墙。其通过定义一些规则对网络设备接口上的数据报文进行控制。

设备支持基于端口的 ACL、基于流的 ACL。基于端口的 ACL 对端口所有入口报文生效；基于流的 ACL 只对命中用户配置规则的报文生效。对于命中报文，支持以下动作策略。

- Permit/deny：选择放行或丢弃
- 限速：设备支持全局配置 16 条限速策略，端口或基于流的 ACL 关联策略 ID 以实现限速
- 镜像：送命中报文到 CPU
- 日志：当端口接收到报文时生成系统日志，日志生成本身是限速的，因此未必每个命中报文均生成日志
- 禁用：shutdown 端口，关闭端口 MAC 地址学习，丢弃所有入口报文
- 重定向：将入口报文直接重定向到特定端口输出

5.2.3.1 配置 ACL

■ 端口

在【导航栏】下拉菜单中选择：配置->安全->网络->ACL->端口，进入配置界面。

图表 5-49 ACL 端口配置

ACL端口配置

端口	策略ID	行为	限速ID	端口重定向	镜像	日志	禁用	状态	统计
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	351384
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	322923
8	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	322919
9	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

保存 复位

配置项	说明
端口	面板端口号
策略 ID	保留
行为	选择放行、丢弃。该行为相当于指定端口的默认行为，一般配合访问控制列表使用。
限速 ID	Disable 或 1-16 的限速 ID，在行为为 permit 时有效，默认 Disabled
端口重定向	报文重定向到其他端口，在行为为 permit 时有效，默认 Disabled
镜像	使能开关，默认关闭
日志	
禁用	
状态	当端口因 ACL 禁用使能的情况下发生 shutdown 时，配置 Enabled 恢复端口。也可以手动指定其 shutdown，即配置成 Disable。
统计	端口命中报文数统计

■ 限速

在【导航栏】下拉菜单中选择：配置->安全->网络->ACL->限速，进入配置界面。

图表 5-50 ACL 限速配置

ACL限速配置

限速ID	速率	单位
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

保存 复位

配置项	说明
限速 ID	范围 1-16，支持 16 条限速策略
速率	范围 0-3276700 pps 或 0、100、200 、…、1000000 kbps
单位	支持 pps、kbps 两种单位

■ 访问控制列表

在【导航栏】下拉菜单中选择：配置->安全->网络->ACL->访问控制列表，进入配置界面。

图表 5-51 访问控制列表配置

访问控制列表配置

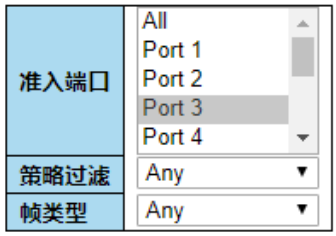
ACE	准入端口	策略/掩码	帧类型	行为	限速	端口重定向	镜像	计数	
1	3	Any	Any	Deny	Disabled	Disabled	Disabled	0	

显示 ACE 的简要信息，支持 ACE 表项上、下移动、前面添加、后面添加、删除、编辑操作。

点击下添加按键，进入 ACE 创建界面。

图表 5-52 ACE 表项信息

ACE配置



VLAN参数

配置项	子项	细分项	说明
准入端口	-	-	支持匹配所有端口或仅匹配单一面板端口
策略过滤	-	-	保留
帧类型	Any	-	命中所有报文
	Ethernet Type	SMAC	Any：命中所有 SMAC Specific：命中具体某一 SMAC
		DMAC	Any：命中所有 DMAC BC：命中所有广播报文 MC：命中所有组播报文 UC：命中所有单播报文 Specific：命中具体某一 DMAC
		Etype	Any：命中所有 Etype Specific：命中具体某一 Etype
	ARP	SMAC	Any：命中所有 SMAC Specific：命中具体某一 SMAC
		DMAC	Any：命中所有 DMAC BC：命中所有广播报文 MC：命中所有组播报文 UC：命中所有单播报文
		ARP/ARPA	Any：命中所有 op code ARP：命中 ARP 的 op code

			RARP:命中 RARP 的 op code Other：命中非 ARP/RARP 的 op code
		请求/应答	Any：命中所有 op code Request：命中 ARP/RARP request 的 op code Reply：命中 ARP/RARP reply 的 op code
		发送 IP 过滤	Any：命中所有 IP 地址 Host：命中某特定 IP 地址 Network：命中后特定 IP 网段
		目标 IP 过滤	Any：命中所有 IP 地址 Host：命中某特定 IP 地址 Network：命中后特定 IP 网段
		ARP 发送 MAC 命中	Any：命中所有 0：发送者硬件地址与 SMAC 不等 1：发送者硬件地址与 SMAC 相等
		RARP 目标 MAC 命中	Any：命中所有 0：目标硬件地址与 DMAC 不等 1：目标硬件地址与 DMAC 相等
		IP/以太网长度	Any：命中所有 0：硬件地址长度不等 6 或协议地址长度不等 4 1：硬件地址长度等 6 且协议地址长度等 4
		IP	Any：命中所有 0：硬件类型不为 1 1：硬件类型为 1
		以太网	Any：命中所有 0：协议类型不等 0x0800 1：协议类型等 0x0800
	IPv4	DMAC	Any：命中所有 DMAC BC：命中所有广播报文 MC：命中所有组播报文 UC：命中所有单播报文
		IP 协议过滤	Any：命中所有 ICMP：ICMP 协议报文 UDP：UCP 协议报文 TCP：TCP 协议报文 Other：其他协议报文
		IP TTL	Any：命中所有 None-Zero：TTL 不等 0 Zero：TTL 等 0

		IP 分片	Any：命中所有 Yes：命中分片报文 No：命中非分片报文
		IP Option	Any：命中所有 Yes：命中设置了 option 标志位报文 No：命中未设置 option 标志位报文
		SIP 过滤	Any：命中所有 IP 地址 Host：命中某特定 IP 地址 Network：命中后特定 IP 网段
		DIP 过滤	Any：命中所有 IP 地址 Host：命中某特定 IP 地址 Network：命中后特定 IP 网段
	IPv6	DMAC	Any：命中所有 DMAC BC：命中所有广播报文 MC：命中所有组播报文 UC：命中所有单播报文
		下一个头部过滤	Any：命中所有 ICMP：ICMP 协议报文 UDP：UCP 协议报文 TCP：TCP 协议报文 Other：其他协议报文
		SIP 过滤	Any：命中所有 Specific：命中具体某 SIP 报文
		跳数限制	Any：命中所有 0：命中 hop 为 0 报文 1：命中 hop 为非 0 报文
VLAN 参数	802.1Q Tagged	-	any，匹配所有报文 Disabled，匹配 Untagged 报文 Enabled，匹配带 Tag 报文
	VLAN ID 过滤	-	Any：所有 vlan Specific：特定 VLAN ID
	Tag 优先级	-	Any:所有优先级值 其他：某特定值或范围
行为/限速/镜像/日志/禁用/计数	-	-	具体动作同基于端口的 ACL

5.2.3.2 查看 ACL 状态

在【导航栏】下拉菜单中选择：监控->安全->网络->ACL 状态，进入查看界面。

图表 5-53 ACL 状态信息

ACL状态

用户	ACE	帧类型	行为	限速器	镜像	CPU	计数	冲突
static	1	IPv4/TCP 80 HTTP	Deny	Disabled	Disabled	No	0	No

显示 ACE 的简要信息，包括匹配项、行为的简要信息配置信息，以及当前报文命中、是否产生冲突等状态信息。

5.2.3.3 ACL 典型配置案例

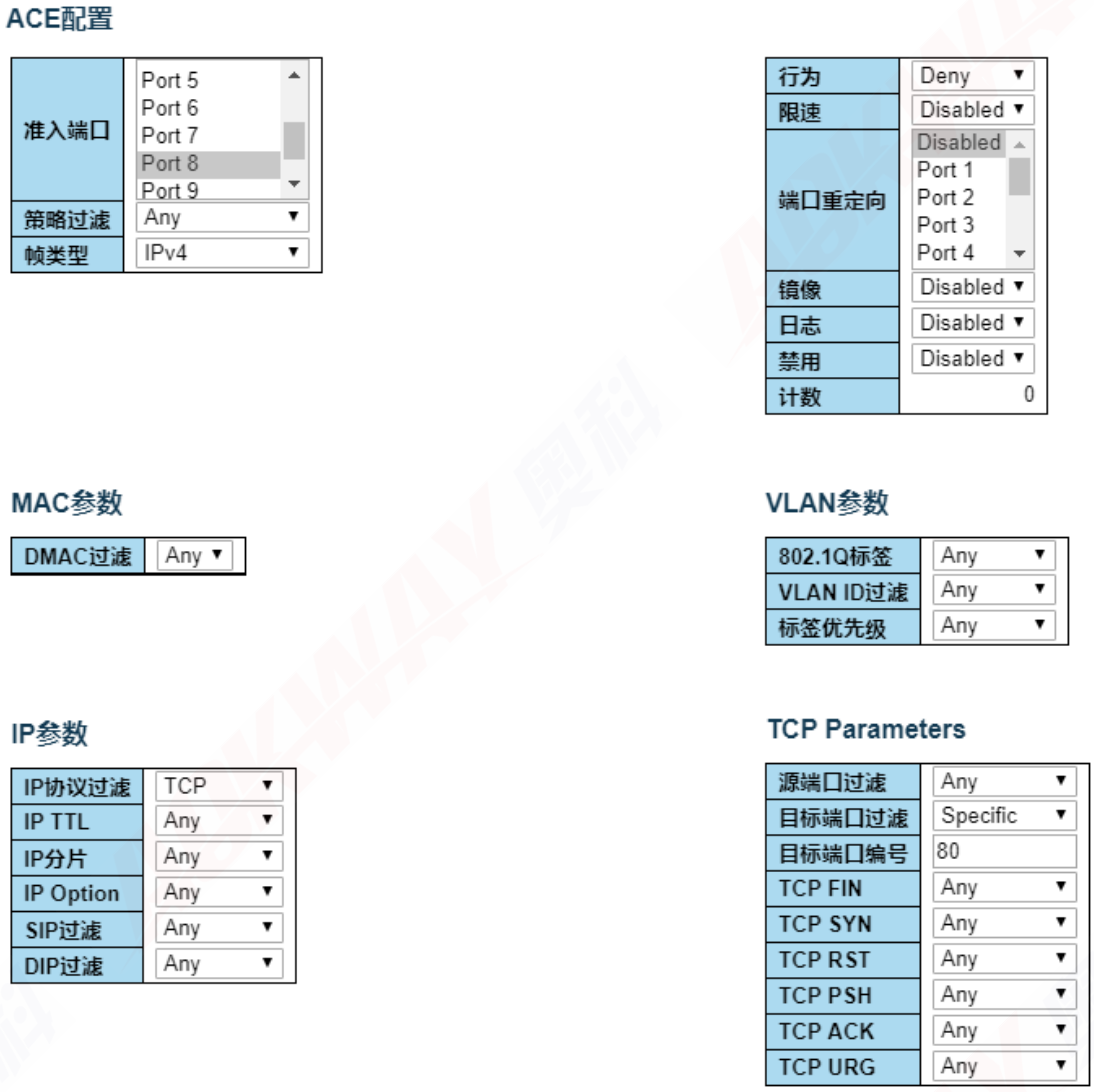
■ 案例需求

在端口 8 应用 ACL 功能，禁止端口源端口号为 80 的 TCP 报文通过。

■ 操作步骤

在访问控制列表配置界面创建 ACE，准入端口选择 8；帧类型选择 IPv4；IP 协议过滤选择 TCP；源端口过滤选择 Specific，源端口编号 80；行为选择 Deny。

图表 5-54 ACL 案例配置



配置完成，在查看界面可看到 ACL 状态:

图表 5-55 ACL 案例状态

5.2.3.4 CLI 参考命令

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# access-list action permit

	switch(config-if)# access-list action deny switch(config-if)# access-list rate-limiter 1 switch(config-if)# no access-list rate-limiter switch(config-if)# access-list redirect interface GigabitEthernet 1/2 switch(config-if)# access-list mirror switch(config-if)# no access-list mirror switch(config-if)# access-list logging switch(config-if)# no access-list logging switch(config-if)# access-list shutdown switch(config-if)# no access-list shutdown switch(config-if)# access-list port-state switch(config-if)# no access-list port-state
描述	配置端口 ACL 行为是 permit; 配置端口 ACL 行为是 deny; 配置端口 ACL 关联限 ID; 配置端口 ACL 关闭限速; 配置端口 ACL 重定向端口; 配置端口 ACL 镜像使能; 配置端口 ACL 镜像关闭; 配置端口 ACL 日志使能; 配置端口 ACL 日志关闭; 配置端口 ACL 禁用端口使能; 配置端口 ACL 禁用端口关闭; 配置端口 ACL 端口状态使能; 配置端口 ACL 端口状态关闭;

命令	switch(config)# access-list rate-limiter 1 pps 20 switch(config)# access-list rate-limiter 1 100kbps 100 switch(config)# no access-list rate-limiter 1
描述	配置 ACL 基于报文数量的限速，单位 pps; 配置 ACL 基于流量的限速，单位 100kbps; 恢复 ACL 默认限速;

命令	switch(config)# access-list ace 1 ingress interface GigabitEthernet 1/1-3 frame-type ipv4 sip 1.1.1.0/24 action deny switch(config)# access-list ace 2 next 1 ingress interface GigabitEthernet 1/1 frame-type ipv4 sip 1.1.1.1/24 switch(config)# no access-list ace 1
描述	配置 ACL 访问控制列表配置 1，作用在端口 1-3 入口，过滤源 IP 为 1.1.1.0/24 网络的报文; 配置 ACL 访问控制列表配置 2，作用在端口 1 入口，放行源 IP 为 1.1.1.1 主机的报文。其优先级高于访问控制列表配置 1; 删除 ACL 访问控制列表配置 1;

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# dot1x port-control force-authorized switch(config-if)# dot1x port-control force-unauthorized switch(config-if)# dot1x port-control auto switch(config-if)# dot1x port-control single switch(config-if)# dot1x port-control multi switch(config-if)# dot1x port-control mac-based switch(config-if)# dot1x radius-qos switch(config-if)# dot1x radius-vlan switch(config-if)# dot1x guest-vlan
描述	配置端口强制授权； 配置端口强制未授权； 配置端口基于端口的 802.1X； 配置端口基于单用户的 802.1X； 配置端口基于多用户的 802.1X； 配置端口基于 MAC 的认证； 配置端口 RADIUS 指定 QoS 使能； 配置端口 RADIUS 指定 VLAN 使能； 配置端口 Guest VLAN 使能；

命令	switch# show access-list interface * switch# show access-list rate-limiter switch# show access-list ace statistics
描述	打印 ACL 端口配置以及命中报文计数； 打印 ACL 限速配置； 打印 ACL 访问控制列表配置以及命中报文计数；

5.2.4 IP Source Guard

IP Source Guard 功能用于对 IP 报文进行接入控制，通过端口+VLAN ID+MAC+IP 四元组，对输入的 IP 报文进行校验，若 IP Source Guard 表中不存在对应表项，则报文丢弃。IP Source Guard 表中表项可以是动态表项，来自于 DHCP Snooping 表；也可以是静态配置的。

报文的四元组提取:

- 端口：指交换机输入的源端口（面板端口）。
- VLAN ID: 报文进入交换机后所分配的 VLAN ID。
- MAC：报文的源 MAC 地址。
- IP：报文的源 IP 地址。

5.2.4.1 配置 IP Source Guard

在【导航栏】下拉菜单中选择：配置->安全->网络->IP Source Guard->配置，进入配置页面。

图表 5-56 IP Source Guard 配置

- 全局模式

  全局模式默认为禁用，只要模式为禁用，IP Source Guard 功能。

- 动态转为静态

  只要点击该按钮，就会将当前已经存在的 IP Source Guard 动态表项转换为静态表项。动态表项的来源为 DHCP snooping 表，如果 DHCP Snooping 表中表项删除（比如租约到期，设备下电老化等等），则 IP Source Guard 的动态表项也会删除，但静态表项会一直存在，除非人为删除。

- 端口模式

  - 模式：指定 IP Source Guard 在哪些端口上启用。仅当全局模式和对应端口模式均使能时，才会在此给定端口上启用 IP Source Guard。
  - 最大动态客户数:指定可在对应端口上学习的最大动态客户端数。该值可以是 0,1,2 或无限制。如果使能了端口模式且该值为 0，则表示仅允许在对应端口上的静态表项中匹配的 IP 报文转发。

⚠ 注意

• 由于 IP Source Guard 功能的动态表项来自于 DHCP Snooping 表，因此必须保证 DHCP Snooping 配置开启以及设置正确的 DHCP Snooping 信任口。

5.2.4.2 配置静态表

在【导航栏】下拉菜单中选择：配置->安全->网络->IP Source Guard->静态表，进入配置页面。

图表 5-57 静态 IP Source Guard 表配置

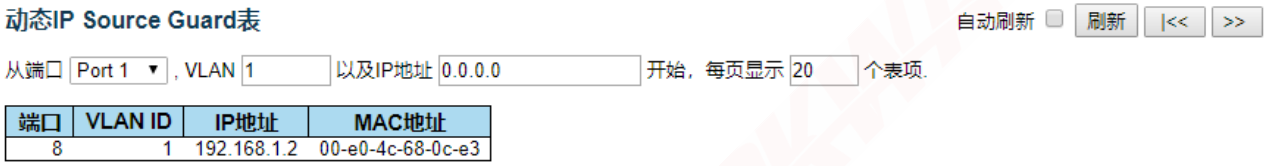
配置 IP Source Guard 静态表项的四元组。IP 地址使用点分十进制形式（A.B.C.D），MAC 地址支持两种格式。XX-XX-XX-XX-XX-XX 或者 XX:XX:XX:XX:XX:XX。

- 删除：勾选后下次保存时删除对应表项。
- 添加新表项：点击添加一条新的表项。

5.2.4.3 显示动态表

在【导航栏】下拉菜单中选择：监控->安全->网络->IP Source Guard，进入显示页面。

图表 5-58 动态 IP Source Guard 表显示



显示 IP Source Guard 动态表项的四元组。如果动态表项转为静态表项后，此页面将不再显示对应表项。

5.2.4.4 CLI 参考命令

命令	switch(config)# ip verify source switch(config)# no ip verify source
描述	配置 IP Source Guard 全局开启； 配置 IP Source Guard 全局关闭；

命令	switch(config)# ip verify source translate
描述	配置 IP Source Guard 所有的动态地址转成静态地址；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# ip verify source switch(config-if)# no ip verify source switch(config-if)# ip verify source limit 2
描述	配置 IP Source Guard 端口开启； 配置 IP Source Guard 端口关闭； 配置 IP Source Guard 端口最大动态客户数；

命令	switch(config)# ip source binding interface GigabitEthernet 1/6 6 192.168.6.34 f4-93-9f-f3-4f-ef switch(config)# no ip source binding interface GigabitEthernet 1/6 6 192.168.6.34 f4-93-9f-f3-4f-ef
描述	添加 IP Source Guard 静态表项； 删除 IP Source Guard 静态表项；

命令	switch# show ip verify source switch# show ip source binding static switch# show ip source binding dhcp-snooping
描述	打印 IP Source Guard 全局配置以及端口配置； 打印 IP Source Guard 静态表项； 打印 IP Source Guard 动态表项；

5.2.5 ARP Inspection

ARP Inspection 功能用于对 ARP 报文进行接入控制，通过端口+VLAN ID+MAC+IP 四元组，对输入的 ARP 报文进行校验，若 ARP Inspection 表中不存在对应表项，则报文丢弃。ARP Inspection 表中表项可以是动态表项，来自于 DHCP Snooping 表；也可以是静态配置的。

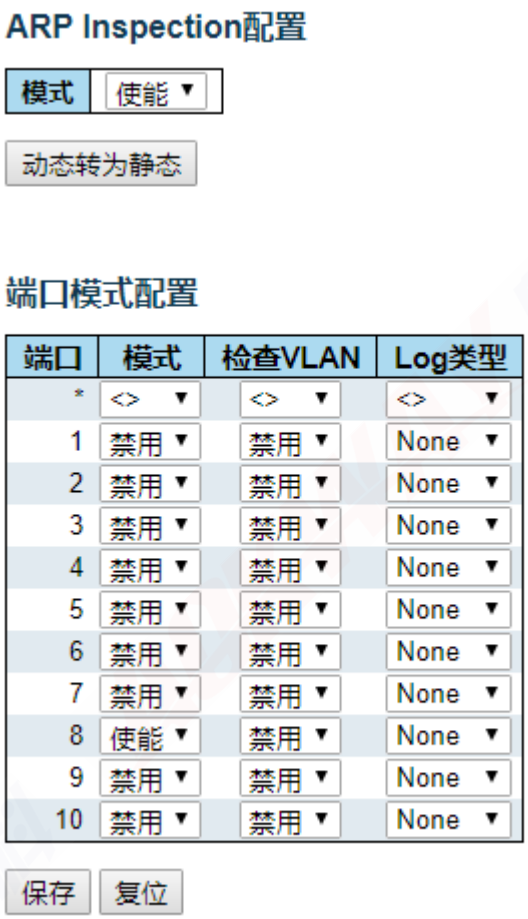
报文的四元组提取:

- 端口：指 ARP 报文输入交换机时的源端口（面板端口）。
- VLAN ID: 指 ARP 报文进入交换机所分配的 VLAN ID。
- MAC：指 ARP 报文的 Sender MAC 地址。
- IP：指 ARP 报文的 Sender IP 地址。

5.2.5.1 配置端口

在【导航栏】下拉菜单中选择：配置->安全->网络->ARP Inspection->端口配置，进入配置页面。

图表 5-59 ARP Inspection 配置



- 全局模式

  全局模式默认为禁用，只要模式为禁用，ARP Inspection 功能不开启。

- 动态转为静态

  只要点击该按钮，就会将当前已经存在的 ARP Inspection 动态表项转换为静态表项。动态表项的来源为 DHCP snooping 表，如果 DHCP Snooping 表中表项删除（比如租约到期，设备下电老化等等），则 ARP Inspection 的动态表项也会删除，但静态表项会一直存在，除非人为删除。

- 端口模式

  - 模式：指定 IP Source Guard 在哪些端口上启用。仅当全局模式和对应端口模式均使能时，才会在此给定端口上启用 ARP Inspection。默认端口模式为禁用。
  - 检查 VLAN：如果要检查 VLAN 配置，则必须启用“检查 VLAN”设置。默认“检查 VLAN”被禁用。禁用“检查 VLAN”的设置时，ARP Inspection 的 Log 类型将参考端口设置。使能“检查 VLAN”设置后，ARP Inspection 的 Log 类型将参考 VLAN 设置。

- Log 类型：只有当全局模式使能，对应端口模式也使能，并且检查 VLAN 禁用时，Log 类型将参考端口设置。有四种 Log 类型，可能的类型有：

  None：什么都不记录。

  Deny：被过滤的 ARP 报文触发 Log。

  Permit：被允许的 ARP 报文触发 Log。

  ALL：所有 ARP 报文触发 Log。

5.2.5.2 配置 VLAN

在【导航栏】下拉菜单中选择：配置->安全->网络->ARP Inspection->VLAN 配置，进入配置页面。

图表 5-60 ARP Inspection VLAN 配置

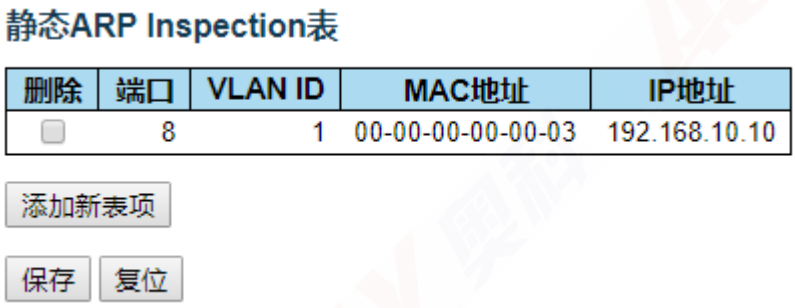
Log 类型跟端口配置的 Log 类型一样。当端口配置中将对应端口的“检查 VLAN”使能时，对应的 Log 类型将参考 VLAN 设置。

- 删除：勾选后下次保存时删除对应表项。
- 添加新表项：点击添加一条新的表项。

5.2.5.3 配置静态表

在【导航栏】下拉菜单中选择：配置->安全->网络->ARP Inspection->静态表，进入配置页面。

图表 5-61 ARP Inspection 静态表配置



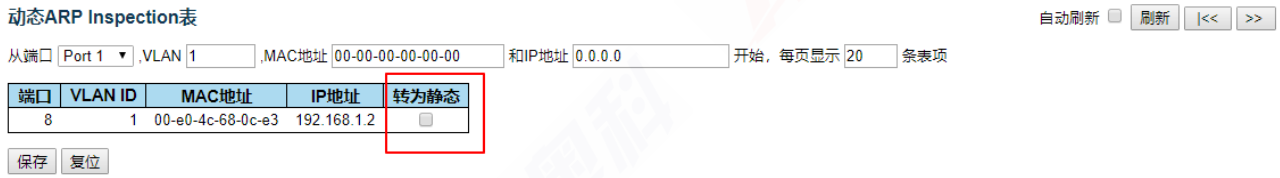
配置 ARP Inspeciton 静态表项的四元组。IP 地址使用点分十进制形式（A.B.C.D），MAC 地址支持两种格式。XX-XX-XX-XX-XX-XX 或者 XX:XX:XX:XX:XX:XX。

- 删除：勾选后下次保存时删除对应表项。
- 添加新表项：点击添加一条新的表项。

5.2.5.4 配置动态表

在【导航栏】下拉菜单中选择：配置->安全->网络->ARP Inspection->动态表，进入配置页面。

图表 5-62 ARP Inspection 动态表配置

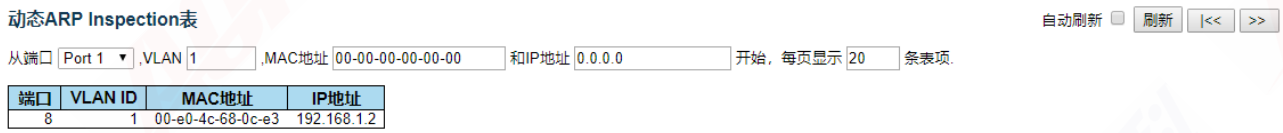


该页面只有“转为静态”可以配置，用于将某条动态表项转为静态。如果动态表项转为静态表项后，此页面将不再显示对应表项。

5.2.5.5 显示动态表

在【导航栏】下拉菜单中选择：监控->安全->网络->ARP Inspection->动态表，进入显示页面。

图表 5-63 ARP Inspection 动态表显示



显示 ARP Inspection 动态表项的四元组信息。如果动态表项转为静态表项后，此页面将不再显示对应表项。

5.2.5.6 CLI 参考命令

命令	switch(config)# ip arp inspection switch(config)# no ip arp inspection
描述	配置 ARP Inspeciton 全局开启； 配置 ARP Inspeciton 全局关闭；

命令	switch(config)# ip arp inspection translate switch(config)# ip arp inspection translate interface GigabitEthernet 1/6 6 00-00-00-11-22-33 1.2.3.4
描述	配置 ARP Inspeciton 所有的动态地址转成静态地址； 配置 ARP Inspeciton 指定的动态地址转静态地址；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# ip arp inspection switch(config-if)# no ip arp inspection switch(config-if)# ip arp inspection check-vlan switch(config-if)# no ip arp inspection check-vlan switch(config-if)# ip arp inspection logging deny
描述	配置 ARP Inspeciton 端口开启； 配置 ARP Inspeciton 端口关闭； 配置 ARP Inspeciton 端口检查 VLAN 开启； 配置 ARP Inspeciton 端口检查 VLAN 关闭； 配置 ARP Inspeciton 端口 LOG 类型；

命令	switch(config)# ip arp inspection vlan 10 switch(config)# ip arp inspection vlan 10 logging all switch(config)# no ip arp inspection vlan 10
描述	添加 ARP Inspeciton VLAN 模式配置； 配置 ARP Inspeciton VLAN 模式的 LOG 类型； 删除 ARP Inspeciton VLAN 模式配置；

命令	switch(config)# ip arp inspection entry interface GigabitEthernet 1/6 6 00-00-00-11-22-33 1.2.3.4 switch(config)# no ip arp inspection entry interface GigabitEthernet 1/6 6 00-00-00-11-22-33 1.2.3.4

描述	添加 ARP Inspeciton 静态表项； 删除 ARP Inspeciton 静态表项；

命令	switch# show ip arp inspection switch# show ip arp inspection entry static switch# show ip arp inspection entry dhcp-snooping switch# show ip arp inspection vlan 10
描述	打印 ARP Inspeciton 全局配置以及端口配置； 打印 ARP Inspeciton 静态表项； 打印 ARP Inspeciton 动态表项； 打印 ARP Inspeciton VLAN 模式配置；

5.3 AAA

5.3.1 RADIUS

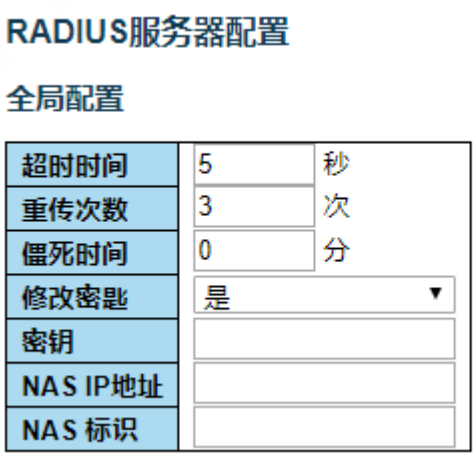
5.3.1.1 配置 RADIUS

在【导航栏】下拉菜单中选择：配置->安全->AAA->RADIUS，进入配置界面。

■ 全局配置

全局配置项对所有的 RADIUS 服务器是通用的。

图表 5-64 RADIUS 全局配置



配置项	说明
超时时间	在重新发送请求之前等待 RADIUS 服务器回复的秒数，范围为 1 到 1000。
重传次数	将 RADIUS 请求重新发送到未响应的服务器的次数，范围为 1 到 1000。如果服务器在上次重新传输后没有响应，则认为它已死。
僵死时间	可以设置为 0 到 1440 分钟之间的数字，在该时间段内交换机不会向未能响应先前请求的服务器发送新请求。当配置了多个服务器，如果将僵死时间设置为大于 0 的值，可以阻止交换机不断尝试联系已确定为已死的服务器。

修改密钥	指定是否更改密钥。如果为该选项选择“是”，则可以更改密钥，在 RADIUS 服务器和交换机之间共享。
密钥	具体要修改的密匙，最多 63 个字符。保存后，该字段内容不可显示。
NAS IP 地址	在 RADIUS Access-Request 数据包中用作属性 4 的 IPv4 地址。如果此字段留空，则使用传出接口的 IP 地址。
NAS 标识	标识符 - 最多 253 个字符 - 用作 RADIUS Access-Request 数据包中的属性 32。如果此字段留空，则 NAS-Identifier 不包含在数据包中。

■ 服务器配置

最多可以添加 5 个服务器。

图表 5-65 RADIUS 服务器配置

配置项	说明
删除	要删除 RADIUS 服务器条目，请选中此框。该条目将在下一次保存期间删除。
主机名（IP 地址）	RADIUS 服务器的 IPv4 地址。
认证端口	在 RADIUS 服务器上用于认证的 UDP 端口。设置为 0 将禁用认证。
记账端口	在 RADIUS 服务器上用于记帐的 UDP 端口。设置为 0 将禁用记帐。。
超时时间	此可选设置将覆盖全局设置的超时时间。将其留空将使用全局设置的超时时间。
重传次数	此可选设置将覆盖全局设置的重新次数。将其留空将使用全局设置的重传次数。
修改密匙	指定是否更改密钥。选中复选框后，您可以更改设置覆盖全局设置的密钥。将其留空将使用全局密钥。
添加新服务器按钮	以添加新的 RADIUS 服务器。表中添加了一个空行，可以根据需要配置 RADIUS 服务器。最多支持 5 台服务器。
删除按钮	在点击添加新服务器按钮，尚未保存时存在，点击用于撤销刚添加的新服务器。

5.3.1.2 查看 RADIUS

在【导航栏】下拉菜单中选择：监控->安全->AAA，将展开两个显示子菜单。分别为“RADIUS 概述”和“RADIUS 详情”。

■ RADIUS 概述

图表 5-66 RADIUS 状态概述

RADIUS服务器状态概述

自动刷新 刷新

#	IP地址	认证端口	认证状态	记账端口	记账状态
1	192.168.200.1	1812	就绪	1813	就绪
2			禁用		禁用
3			禁用		禁用
4			禁用		禁用
5			禁用		禁用

表头	说明
#	RADIUS 服务器号。单击以导航到此服务器的详细统计信息。
IP 地址	该服务器的 IP 地址。
认证端口	该服务器用于认证的 UDP 端口号。
认证状态	该服务器的认证功能当前状态。此字段采用以下值之一： **禁用**：服务器已禁用。 **未就绪**：服务器已启用，但 IP 通信尚未启动并正在运行。 **就绪**：服务器已启用，IP 通信已启动并正在运行，并且 RADIUS 已准备好接受访问尝试。 **僵死（X 秒剩余）**：已对此服务器进行了访问尝试，但未在配置的超时时间内进行回复。服务器已暂时禁用，但在“僵死时间”到期后将重新启用。在此之前剩余的秒数显示在括号中。只有在启用多个服务器时才能访问此状态。
记账端口	该服务器用于记帐的 UDP 端口号。
记账状态	该服务器的记账功能当前状态。此字段采用以下值之一： **禁用**：服务器已禁用。 **未就绪**：服务器已启用，但 IP 通信尚未启动并正在运行。 **就绪**：服务器已启用，IP 通信已启动并正在运行，并且 RADIUS 已准备好接受访问尝试。 **僵死（X 秒剩余）**：已对此服务器进行了访问尝试，但未在配置的超时时间内进行回复。服务器已暂时禁用，但在“僵死时间”到期后将重新启用。在此之前剩余的秒数显示在括号中。只有在启用多个服务器时才能进入此状态。

■ RADIUS 详情

图表 5-67 RADIUS 状态详情

RADIUS认证统计 Server #1

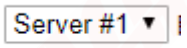
Server #1 自动刷新 刷新 清除

接收报文		发送报文	
访问接受	0	访问请求	0
访问拒绝	0	访问重传	0
访问Challenge	0	Pending请求	0
畸形访问应答	0	超时	0
非法认证者	0		
未知类型	0		
丢弃报文	0		
其他信息			
IP地址		192.168.200.1:1812	
状态		就绪	
Round-Trip时间		0 ms	

RADIUS记账统计 Server #1

接收报文		发送报文	
应答	0	请求	0
畸形应答	0	重传	0
非法认证者	0	Pending请求	0
未知类型	0	超时	0
丢弃报文	0		
其他信息			
IP地址		192.168.200.1:1813	
状态		就绪	
Round-Trip时间		0 ms	

使用如下复选框可以在不同服务器之间切换。



- RADIUS 认证统计
  - 计数器

方向	名称	RFC4668 名称	描述
RX	**访问接受**	radiusAuthClientExtAccessAccepts	从服务器收到的 RADIUS Access-Accept 数据包（有效或无效）的数量。
RX	**访问拒绝**	radiusAuthClientExtAccessRejects	从服务器收到的 RADIUS Access-Reject 数据包（有效或无效）的数量。
RX	**访问 Challenge**	radiusAuthClientExtAccessChallenges	从服务器收到的 RADIUS Access-Challenge 数据包的数量（有效或无效）。
RX	**畸形访问应答**	radiusAuthClientExtMalformedAccessResponses	从服务器收到的畸形的 RADIUS 访问应答数据包的数量。畸形数据包包括长度无效的数据包。错误的身份验证器或 Message Authenticator 属性或未知类型不包括在畸形访问应答中。
RX	**非法认证者**	radiusAuthClientExtBadAuthenticators	从服务器收到的包含无效身份验证器或 Message Authenticator 属性的 RADIUS Access-Response 数据包的数量。
RX	**未知类型**	radiusAuthClientExtUnknownTypes	从身份验证端口上的服务器接收到的未知类型的 RADIUS 数据包数并被丢弃。
RX	**丢弃报文**	radiusAuthClientExtPacketsDropped	在认证端口上从服务器接收的 RADIUS 数据包的数量，并由于某些其他原因而丢弃。
TX	**访问请求**	radiusAuthClientExtAccessRequests	发送给服务器的 RADIUS Access-Request 报文数。这不包括重新传输。
TX	**访问重传**	radiusAuthClientExtAccessRet	重新发送到 RADIUS 认证服务器的 RADIUS Access-Request

		ransmissions	报文数。
TX	**pending 请求**	radiusAuthClientExtPendingRequests	发往服务器的 RADIUS 访问请求数据包的数量尚未超时或收到响应。当由于接收到访问接受，访问-拒绝，访问-质询，超时或重传而发送和减少访问请求时，该变量递增。
TX	**超时**	radiusAuthClientExtTimeouts	服务器的认证超时数。超时后，客户端可能会重试到同一台服务器，发送到其他服务器或放弃。对同一服务器的重试计为重新传输以及超时。发送到其他服务器的计数被视为请求以及超时。

✧ 其他信息

名称	RFC4668 名称	描述
IP 地址	-	有问题的认证服务器的 IP 地址和 UDP 端口。
状态	-	显示服务器的状态。它采用以下值之一： 禁用：禁用所选服务器。 未就绪：服务器已启用，但 IP 通信尚未启动并正在运行。 就绪：服务器已启用，IP 通信已启动并正在运行，并且 RADIUS 已准备好接受访问尝试。 僵死 (X 秒剩余)：已对此服务器进行了访问尝试，但未在配置的超时内进行回复。服务器已暂时禁用，但在僵死时间到期后将重新启用。在此之前剩余的秒数显示在括号中。只有在启用多个服务器时才能进入此状态。
Round-Trip 时间	radiusAuthClientExtRoundTripTime	最近的 Access-Reply / Access-Challenge 与从 RADIUS 认证服务器匹配的 Access-Request 之间的时间间隔（以毫秒为单位）。该测量的粒度为 100 毫秒。若为 0 毫秒表示尚未与服务器进行往返通信。

➢ RADIUS 记账统计

✧ 计数器

方向	名称	RFC4670 名称	描述
RX	**应答**	radiusAccClientExtResponses	从服务器收到的 RADIUS 数据包数（有效或无效）。
RX	**畸形应答**	radiusAccClientExtMalformedResponses	从服务器收到的畸形的 RADIUS 数据包的数量。畸形数据包包括长度无效的数据包。错误的身份验证者或未知类型不包括在畸形应答中。
RX	**非法认证者**	radiusAcctClientExtBadAuthenticators	包含从服务器收到的无效认证的 RADIUS 数据包数。
RX	**未知类型**	radiusAccClientExtUnknownTypes	在记账端口上从服务器接收的未知类型的 RADIUS 数据包数。
RX	**丢弃报文**	radiusAccClientExtPacketsDropped	在记账端口上从服务器接收的 RADIUS 数据包数量，由于某些其他原因而丢弃。
TX	**请求**	radiusAccClientExtRequests	发送给服务器的 RADIUS 报文数。这不包括重新传输。
TX	**重传**	radiusAccClientExtRetransmissions	重新发送到 RADIUS 记账服务器的 RADIUS 报文数。
TX	**Pending 请求**	radiusAccClientExtPendingRequests	发往服务器的 RADIUS 数据包数量尚未超时或收到响应。当由于接收到响应，超时或重传而发送和递减请求时，此变量会递增。
TX	**超时**	radiusAccClientExtTimeouts	服务器的记账超时数。超时后，客户端可能会重试到同一台服务器，发送到其他服务器或放弃。对同一服务器的重试计为重新传输以及超时。发送到其他服务器的计数被视为请求以及超时。

✧ 其他信息

与 RADIUS 认证统计的其他信息类似，不再细述。

- 清除：清除所选服务器的计数器。此操作不会清除“pending 请求”计数器。

5.3.1.3 CLI 参考命令

命令	switch(config)# radius-server timeout 5 switch(config)# radius-server retransmit 3 switch(config)# radius-server deadtime 1 switch(config)# radius-server key password switch(config)# radius-server attribute 4 192.168.1.3 switch(config)# radius-server attribute 95 4ff1:3301 switch(config)# radius-server attribute 32 server
描述	配置 RADIUS 超时时间； 配置 RADIUS 重传次数； 配置 RADIUS 僵死时间； 配置 RADIUS 秘钥； 配置 RADIUS NAS IPv4 地址； 配置 RADIUS NAS IPv6 地址； 配置 RADIUS NAS 标识；

命令	switch(config)# radius-server host 192.168.1.10 auth-port 1812 acct-port 1813 timeout 10 retransmit 3 key password switch(config)# no radius-server host 192.168.1.10 auth-port 1812 acct-port 1813 timeout 10 retransmit 3 key password
描述	添加 RADIUS 服务器； 删除 RADIUS 服务器；

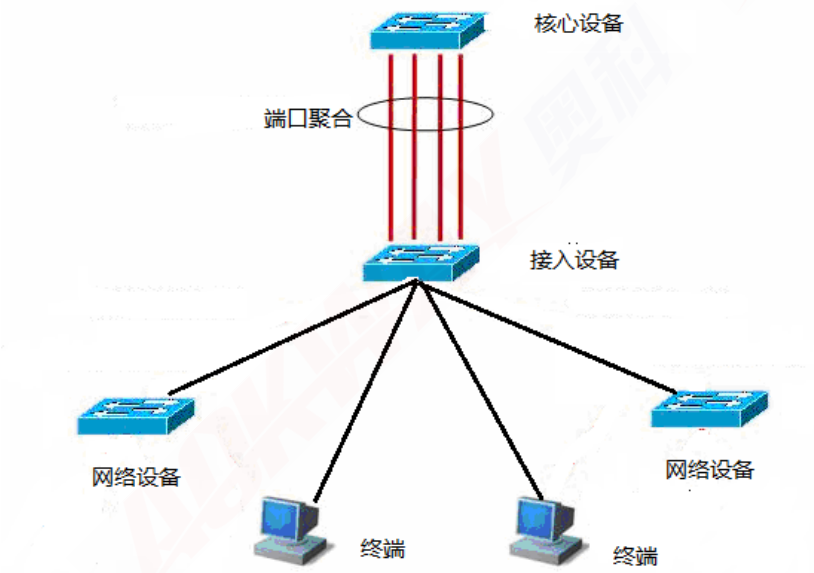
命令	switch# show radius-server switch# show radius-server statistics
描述	打印 RADIUS 配置以及服务器状态； 打印 RADIUS 认证报文统计；

6 端口聚合

6.1 聚合口概述

将多个物理链接捆绑在一起建立一个逻辑链接，这个逻辑链接我们称之为聚合口（port-channel，后者 PO 口），该功能称为端口聚合功能。聚合口功能符合 IEEE802.3ad 标准， 它可以用于扩展链路带宽，提供更高的连接可靠性，常用于端口上联，如下图所示。

图表 6-1 聚合口说明



聚合口具备以下几个特性：高带宽，聚合口总带宽为物理成员口带宽总和；支持流量均衡策略，可以根据策略把流量地分配给各成员链路；支持链路备份，当聚合口中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到聚合口中的其它有效成员链路上。

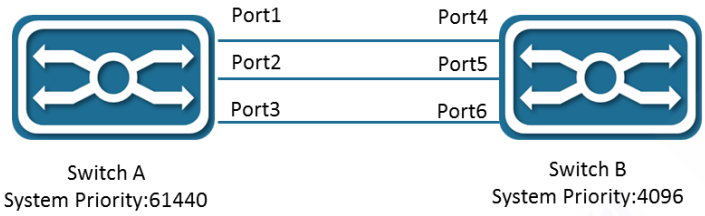
6.2 LACP 概述

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的协议。如果端口启用 LACP 协议，端口会发送 LACPDU 来通告自己的系统优先级、系统 MAC、端口的优先级、端口号和操作 key 等。相连设备收到对端的 LACP 报文后，根据报文中的系统 ID 比较两端的系统优先级。在系统 ID 优先级较高的一端，将按照端口 ID 优先级从高到低的顺序，设置聚合组内端口处于聚合状态，并发出更新后的 LACP 报文，对端设备收到报文后，也会把相应的端口设置成聚合状态，从而使双方在端口退出或者加入聚合组上达到一致。只有双方的端口都完成动态聚合绑定操作后，该物理链路才能进行数据报文的转发。

LACP 成员口链路绑定之后，还会进行周期性的 LACP 报文交互，在一段时间没有收到 LACP 报文时，就认为收包超时，成员口链路解除绑定，端口重新处于不可转发状态。这里的超时时间有两种模式:长超时模式（或者叫做慢超时模式）和短超时模式（或者叫做快超时模式）.在长超时模式下，端口间隔

30 秒发送一个报文，若 90 秒没有收到对端报文，就处于收包超时；在短超时模式下，端口间隔 1 秒发送一个报文，若 3 秒钟没有收到对端报文，就处于收包超时。

图表 6-2 LACP 说明



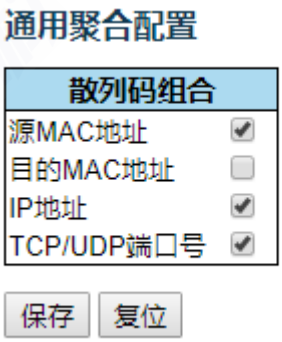
如上图所示，交换机 A 和交换机 B 通过 3 个端口连接在一起。设置交换机 A 的系统优先级为 61440，设置交换机 B 的系统优先级为 4096。在交换机 A 和 B 的 3 个直连端口上打开 LACP 链路聚合，设置 3 个端口的聚合模式为主动模式，设置 3 个端口的端口优先级为默认优先级 32768。

在收到对端的 LACP 报文后，交换机 B 发现自己的系统 ID 优先级比较高(交换机 B 的系统优先级比交换机 A 高)，于是按照端口 ID 优先级的顺序(端口优先级相同的情况下，按照端口号从小到大的顺序)设置端口 4、5、6 处于聚合状态。交换机 A 收到交换机 B 更新后的 LACP 报文后，发现对端的系统 ID 优先级比较高，并且把端口设置成聚合状态了，也把端口 1、2、3 设置成聚合状态。

6.3 通用配置

在【导航栏】下拉菜单中选择：配置->链路聚合->通用，进入配置页面。

图表 6-3 链路聚合通用配置



聚合口的 Hash 计算（即均衡方式），支持源 MAC 地址、目标 MAC 地址、IP 地址、TCP/UDP 端口号的哈希散列组合。

6.4 聚合组配置

6.4.1 配置聚合组

在【导航栏】下拉菜单中选择：配置->链路聚合->聚合组，进入配置页面。

图表 6-4 聚合组配置

聚合组配置

	端口成员										聚合组配置		
组ID	1	2	3	4	5	6	7	8	9	10	模式	重收敛	最大成员数
Normal	◉	○	○	○	○	○	○	◉	◉	◉			
1	○	○	○	○	○	○	○	○	○	○	Disabled	☑	16
2	○	◉	◉	○	○	○	○	○	○	○	Static	☑	16
3	○	○	○	○	○	○	○	○	○	○	Disabled	☑	16
4	○	○	○	◉	◉	○	○	○	○	○	LACP (Active)	☑	16
5	○	○	○	○	○	◉	◉	○	○	○	LACP (Passive)	☑	16

保存　复位

配置项	说明
组 ID	聚合组 ID，支持的聚合组数为物理端口数除 2。比如 IS2500-8GT2GS，共 10 个物理端口，则支持的聚合组数为 5。
端口成员	选择每个聚合组的端口成员，默认所有端口均不属于任何聚合组。一个端口最多只能属于一个聚合组。一个聚合组最多配置 16 个成员口。 只有全双工端口才能加入聚合，每个聚合组中的所有端口的速率必须相同。如果物理端口的有些配置不同，也不能加入聚合组，比如其中一个成员口开启 802.1X，另外的成员口未开启，则不能加入同一个聚合组。
模式	➢ Disable：该组已禁用。 ➢ 静态：该组以静态聚合模式运行。 ➢ LACP(Active)：该组以 LACP 主动聚合模式运行。 ➢ LACP(Passive)：该组以 LACP 被动聚合模式运行。
重收敛	此参数仅适用于启用 LACP 的组。它确定当具有较高优先级的链接可用时，该组是否将执行自动链接（重新）计算。
最大成员数	此参数仅适用于启用 LACP 的组。它确定聚合中允许的最大活动捆绑 LACP 端口数。范围为 1-16，默认为 16。

6.4.2　查看聚合组

在【导航栏】下拉菜单中选择：监控->链路聚合->状态，进入显示页面。

图表 6-5 聚合状态显示

聚合状态

自动刷新 ☐ 刷新

聚合ID	名称	类型	速率	配置端口	聚合端口
2	LLAG2	STATIC	1G	GigabitEthernet 1/2-3	GigabitEthernet 1/2-3
4	LLAG4	LACP_ACTIVE	Undefined	GigabitEthernet 1/4-5	none
5	LLAG5	LACP_PASSIVE	Undefined	GigabitEthernet 1/6-7	none

配置项	说明
聚合 ID	聚合组 ID

名称	聚合组名称
类型	聚合组类型，静态，LACP_ACTIVE 或者 LACP_PASSIVE
速率	聚合组端口速率，根据实际的聚合端口成员口来确定，若无实际的聚合成员口，则显示未 Undefined。
配置端口	用户配置的聚合组成员口
聚合端口	聚合组实际参与聚合的成员口，端口未 link（静态组）或者 LACP 协议未加入（LACP 组）时，配置的成员口不显示。

6.5 LACP

6.5.1 配置 LACP

在【导航栏】下拉菜单中选择配置->链路聚合->LACP，进入配置页面。

图表 6-6 LACP 配置

- LACP 系统配置

  LACP 系统优先级，当运行 LACP 协议的两端设备都为 ACTIVE 模式时，优先级高的作为主。数字越小，优先级越高，范围为 1-65535，默认为 32768。

- LACP 端口配置

配置项	说明
端口	面板端口号。
LACP	显示该端口是否启用了 LACP。

超时	LACP 报文超时模式，Fast 为 1 秒，Slow 为 30 秒，默认为 Fast。
优先级	端口加入聚合口优先级，数值小的优先级高，在端口数大于聚合口最大成员口数场景生效，确定哪些端口作为活动状态，哪些端口作为备份状态。范围为 1-65535，默认为 32768。

6.5.2 查看 LACP 信息

■ LACP 系统状态

在【导航栏】下拉菜单中选择：监控->链路聚合->LACP->系统状态，进入查看界面。

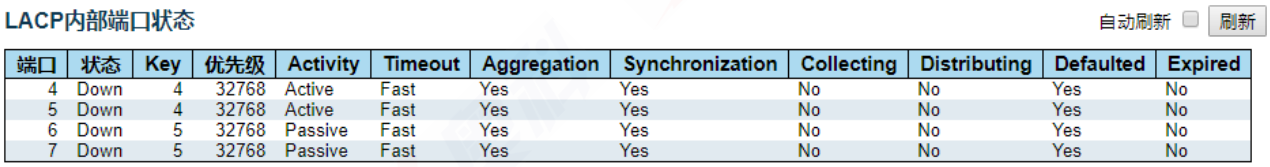
图表 6-7 LACP 系统状态显示

参数	说明
优先级	本设备的系统优先级
MAC 地址	本设备的 MAC 地址。
聚合 ID	聚合组 ID
合作者系统 ID	对端设备 MAC 地址信息
合作者秘钥	对端设备聚合组 ID
合作者优先级	对端设备聚合组优先级
上次改变	聚合组发生变动的最新时间点
本地端口	加入聚合组的本地端口集合

■ LACP 内部状态

在【导航栏】下拉菜单中选择：监控->链路聚合->LACP->内部状态，进入查看界面。

图表 6-8 LACP 内部状态显示



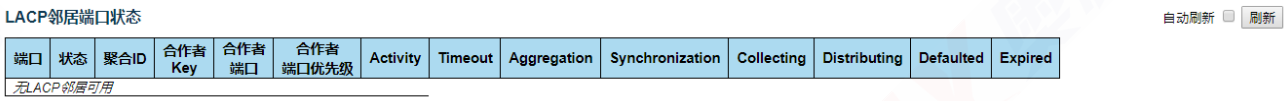
参数	说明
端口	面板端口号

状态	➢ Down：端口 Link down。 ➢ Active：端口处于活动状态。 ➢ Standby：端口处于备份状态。当活动状态的端口异常（比如 link down 或者协议不通），则备份状态的端口可以转为活动状态。
Key	LACP 组的 Key，一般而言即为聚合组 ID。只有相同 Key 的端口才能聚合在一起。
优先级	端口优先级。
Activity	LACP 组的工作模式，Active 或者 Passive。
Timeout	LACP 组的超时模式，Fast 或者 Slow。
Aggregation	系统认为该端口是否可聚合，即潜在的聚合候选者。
Synchronization	显示系统是否认为此链接为“IN_SYNC”；即，它已被分配给正确的 LACP 组，该组已与兼容的聚合组相关联，并且标识与发送的系统 ID 和操作密钥信息一致。
Collecting	显示是否已启用此链接上的传入帧集合。
Distributing	显示是否启用了此链接上的传出帧分发。
Defaulted	显示 Actor 的接收设备是否正在使用默认的合作伙伴信息。
Expired	显示 Actor 的接收设备是否正处在 Expired 状态。

■ LACP 邻居状态

在【导航栏】下拉菜单中选择：监控->链路聚合->LACP->邻居状态，进入查看界面。

图表 6-9 LACP 邻居状态显示



该表显示的信息与内部状态信息类似，只不过显示的信息来源于邻居。其中合作者 Key，合作者端口和合作者端口优先级对应的是本地信息（邻居的合作者即本地），通过这些本地信息可以观察到与邻居的连接关系具体是怎样的。

■ LACP 端口统计

在【导航栏】下拉菜单中选择：监控->链路聚合->LACP->端口统计，进入查看界面。

图表 6-10 LACP 端口统计信息

LACP统计

端口	LACP 接收	LACP 发送	丢弃	
			未知	非法
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	679	669	0	0
8	679	669	0	0

配置项	说明
端口	面板端口号
LACP 接收	端口接收到的 LACP 报文统计
LACP 发送	端口发送的 LACP 报文统计
丢弃	端口接收到的未知或非法的 LACP 报文统计

6.6 CLI 参考命令

命令	switch(config)# aggregation mode smac dmac ip port switch(config)# lacp system-priority 32768
描述	配置聚合口散列码组合； 配置聚合口 LACP 系统优先级；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# aggregation group 1 mode active switch(config-if)# no aggregation group 1
描述	配置端口为聚合口； 配置端口退出聚合口；

命令	switch(config-if)# lacp port-priority 32768 switch(config-if)# lacp timeout fast
描述	配置端口聚合口 LACP 优先级； 配置端口聚合口 LACP 超时模式；

命令	switch# show aggregation switch# show aggregation mode
描述	打印聚合口配置以及状态； 打印聚合口散列码组合状态；

命令	switch# show lacp system-id switch# show lacp internal switch# show lacp neighbor switch# show lacp statistics
描述	打印聚合口 LACP 系统优先级； 打印聚合口 LACP 内部状态； 打印聚合口 LACP 邻居及端口状态； 打印聚合口 LACP 报文统计；

7 环路保护

随着环网技术在网络中应用的增加，网络拓扑越来越复杂，时常有发生因为误连接导致局部网络出现环路的情况。设备的环路保护功能，具备了检测环路、实时解决环路问题、提供日志信息以方便管理人员解决环路故障的能力。

设备端口定时发送私有协议报文，并检测是否有接收到本机发送出的私有协议报文，以判断拓扑是否发生环路。当检测到环路时，选定违例口，并执行配置动作，如 Shutdown 端口、记录系统日志等。

Shutdown 端口：清除端口 MAC 地址，关闭端口 MAC 地址学习能力，禁止端口转发功能。

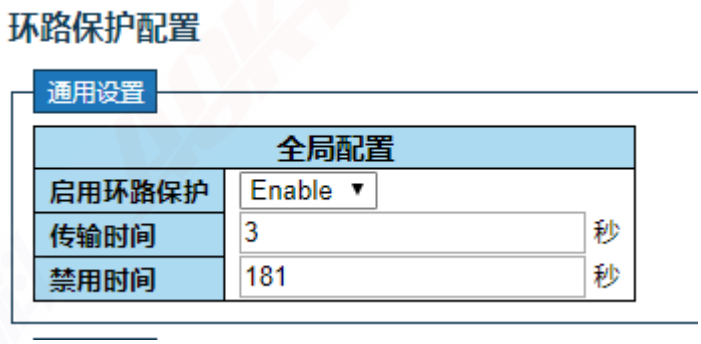
日志：将违例口信息记录在设备系统日志中，方便管理者定位排查故障。

7.1 配置环路保护

在【导航栏】下拉菜单中选择：配置->环路保护，进入配置界面。

■ 全局配置

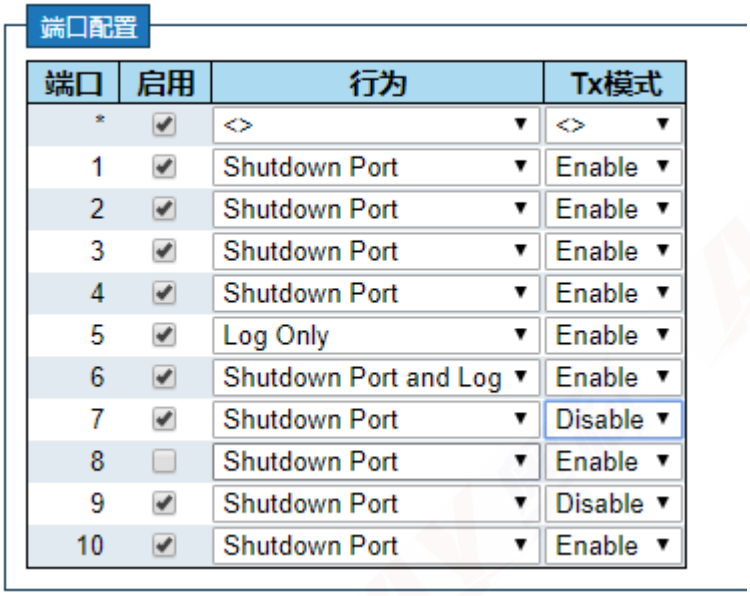
图表 7-1 环路保护全局配置



配置项	说明
启用环路保护	全局使能环路保护功能
传输时间	每个端口环路保护协议报文传输间隔，范围 1-10 秒，默认 5 秒
禁用时间	保护端口恢复时间，范围 0-604800 秒，默认 180 秒，配置 0 秒保护口将不恢复

■ 端口配置

图表 7-2 环路保护端口配置

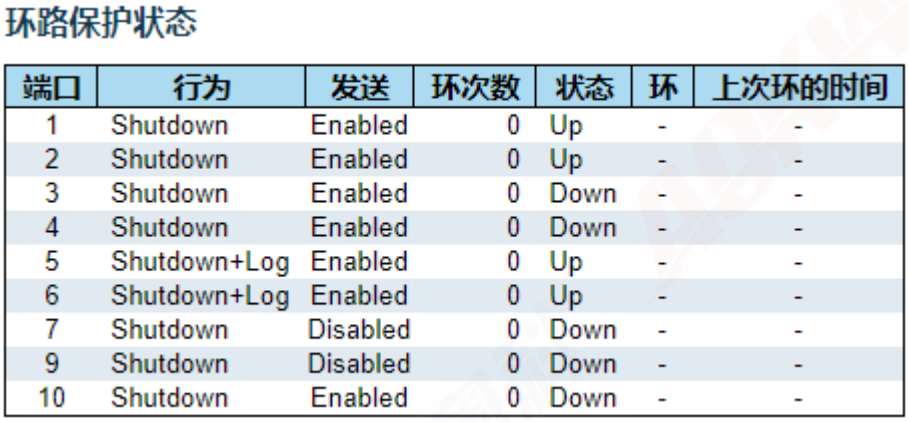


配置项	说明
端口	面板端口号
启用	端口使能环路保护功能
行为	当环路发现时对端口的动作，支持 Shutdown Port、ShutdownPort and Log、Log Only 三种动作
Tx 模式	端口使能发送环路保护协议报文，若 disable 只能被动接收环路保护协议报文

7.2 查看环路保护状态

在【导航栏】下拉菜单中选择：监控->环路保护，进入查看界面。

图表 7-3 环路保护状态显示



配置项	说明
端口	面板端口号
行为	端口使能环路保护功能

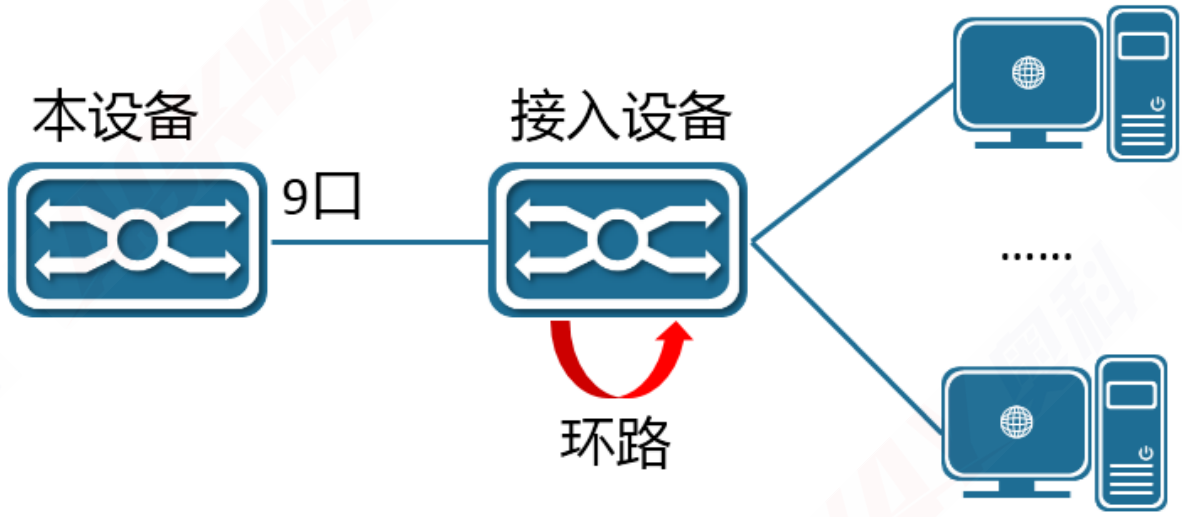
发送	端口是否使能 Tx 模式
环次数	端口检测到环路的次数
状态	当前端口状态，如行为 Shutdown，当检测到环路时端口处于 Disabled 状态
环	当前端口是否处于环路状态
上次环的时间	端口最新检测到环路的时间

7.3 环路保护典型配置案例

■ 案例需求

系统环境中，端口 9 下联接入设备，扩展终端接入。为防止接入设备网络发生环路，在 9 口打开环路保护功能，在检测到环路时及时 Shutdown 端口 9 并且产品日志，避免影响设备网路环境。

图表 7-4 环路保护案例



■ 操作步骤

全局使能环路保护功能，端口 9 使能环路保护功能，行为 Shutdown Port and Log。

图表 7-5 环路保护案例配置

环路保护配置

通用设置

全局配置	
启用环路保护	Enable
传输时间	5 秒
禁用时间	180 秒

端口配置

端口	启用	行为	Tx模式
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable
6	☑	Shutdown Port	Enable
7	☑	Shutdown Port	Enable
8	☑	Shutdown Port	Enable
9	☑	Shutdown Port and Log	Enable
10	☑	Shutdown Port	Enable

在接入设备制造环路，查看环路保护状态信息。

图表 7-6 环路保护案例状态

环路保护状态

端口	行为	发送	环次数	状态	环	上次环的时间
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Up	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown+Log	Enabled	81	Disable	Loop	1970-01-02T01:04:51+00:00
10	Shutdown	Enabled	0	Down	-	-

7.4 CLI 参考命令

命令	switch(config)# loop-protect switch(config)# no loop-protect switch(config)# loop-protect transmit-time 5 switch(config)# loop-protect shutdown-time 180
描述	配置开启环路保护； 配置关闭环路保护； 配置环路保护传输时间； 配置环路保护恢复时间；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# loop-protect switch(config-if)# no loop-protect switch(config-if)# loop-protect action shutdown log switch(config-if)# loop-protect tx-mode switch(config-if)# no loop-protect tx-mode
描述	配置端口开启环路保护； 配置端口关闭环路保护； 配置端口环路保护行为； 配置端口开启环路保护 Tx 模式； 配置端口关闭环路保护 Tx 模式；

命令	switch# show loop-protect
描述	打印环路保护配置以及状态；

8 生成树

8.1 概述

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。

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 STP（Spanning Tree Protocol，生成树协议）到 RSTP（Rapid Spanning Tree Protocol，快速生成树协议），再到最新的 MSTP（Multiple SpanningTree Protocol，多生成树协议）。

对二层以太网来说，两个 LAN 间只能有一条活动着的通路，否则就会产生广播风暴。但是为了加强一个局域网的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。手工控制这样的过程显然是一项非常艰苦的工作，STP 协议就自动地完成这项工作。它能使一个局域网中的设备起到以下作用:

- 发现并启动局域网的一个最佳的树型拓扑结构。
- 发现故障并随之进行恢复，自动更新网络拓扑结构，使在任何时候都选择了可能的最佳的树型结构。

8.2 生成树配置简介

8.2.1 桥参数配置

点击导航栏中：配置->生成树->桥设置，进入桥参数配置界面。

图表 8-1 生成树桥配置

配置项	说明

协议版本	设置 STP 的版本模式，包括 STP、 RSTP 和 MSTP STP：在 STP 模式下，设备的各个端口将向外发送 STP BPDU 报文 RSTP：在 RSTP 模式下，设备的各个端口将向外发送 RSTP BPDU 报文，当发现与运行 STP 的设备相连时，该端口会自动迁移到 STP 模式下工作 MSTP：在 MSTP 模式下，设备的各个端口将向外发送 MSTP BPDU 报文，当发现与运行 STP 的设备相连时，该端口会自动迁移到 STP 模式下工作
桥优先级	生成树协议参数，用于最优生成树计算。值越小表示优先级越高。 对于 MSTP 协议，该配置仅针对 CIST 有效。
Hello Time	设置设备为检测链路故障，发送 hello 报文的周期。
Forward Delay	设置设备状态迁移的延迟时间。
Max Age	设置消息在设备内保存的最大时长。
Maximum Hop Count	设置 MST 域的最大跳数，该参数决定了 MST 域的规模 只有在域根上配置的该参数才会在域内生效，在非域根上的配置无效。
Transmit Hold Count	桥每秒最多发送的 BPDU 报文数。
边缘端口 BPDU 过滤	设置是否使能 BPDU 过滤功能。 使能 BPDU 过滤功能后，边缘端口收到 BPDU 报文时会启用 BPDU 报文收发处理。
边缘端口 BPDU 保护	设置是否使能 BPDU 保护功能。 使能 BPDU 保护功能后，边缘端口收到 BPDU 报文会进入错误状态，可以防止人为伪造配置消息恶意攻击设备，避免网络震荡。
端口错误恢复	设置是否使能端口错误恢复功能。 使能端口错误恢复功能时，端口进入错误状态后，设备会自动在指定的超时时间后恢复错误端口，使端口重新参与协议计算及转发。
端口错误恢复超时	端口错误后重新恢复需要等待的超时时间。

8.2.2 MSTI 映射配置

点击导航栏中：配置->生成树->MSTI 映射，进入 MSTI 映射配置界面。

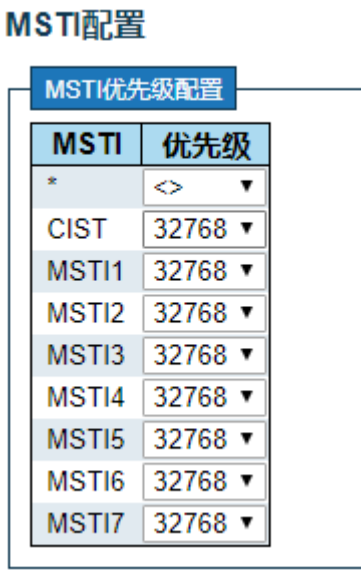
图表 8-2 MSTI 映射配置

配置项	说明
配置名称	MSTI 域配置名称，同一个域内交换机的 MSTI 配置名称必须相同。
配置版本号	MSTI 版本级别，同一个域内交换机的 MSTI 版本级别必须相同。
映射的 VLAN	配置 MSTI 实例和 VLAN 的映射关系。

8.2.3 MSTI 优先级配置

点击导航栏中：配置->生成树->MSTI 优先级，进入 MSTI 优先级配置界面。

图表 8-3 MSTI 优先级配置

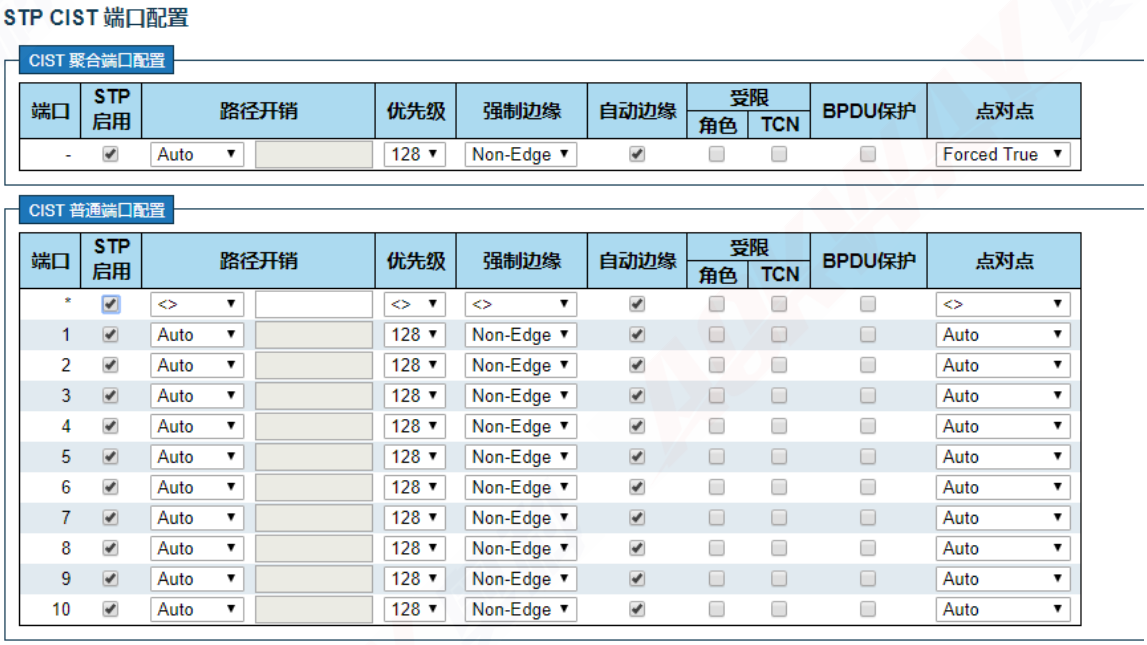


配置项	说明
优先级	生成树桥优先级。 其中 CIST 优先级和桥参数配置中的桥优先级等同，MSTI 优先级为多生成树实例桥优先级，用于在各自生成树中参与协议计算。

8.2.4 CIST 端口配置

点击导航栏中：配置->生成树->CIST 端口，进入 CIST 端口配置界面。

图表 8-4 CIST 端口配置



配置项	说明
STP 启用	生成树开关。
路径开销	Auto：自动计算，系统会自动依据端口速率/类型等参数计算。

	Specific：手动指定，取值为 1-200000000 的数字。
优先级	端口优先级，值越小优先级越高。
强制边缘	Non-Edge：非边缘口。 Edge：强制识别为边缘口。 边缘端口默认不参与 STP 协议计算。
自动边缘	设置启用自动识别端口为边缘口。
受限角色	保护端口不被选举为根端口，效果和根保护功能相似。
受限 TCN	限制端口转发拓扑变化通告的能力。
BPDU 保护	使能 BPDU 保护后，端口收到 BPDU 报文会立即进入错误状态。 可以通过错误恢复功能重新恢复端口，也可以通过重置端口管理状态来恢复端口。
点对点	Auto：自动识别端口链路模式是否点对点模式。 Force True：强制端口链路模式为点对点模式。 Force False：强制端口链路模式为非点对点模式。 点对点模式的链路可以进行快速协商和收敛，无需等待延迟和定时器超时。

8.2.5 MSTI 端口配置

点击导航栏中：配置->生成树->MSTI 端口，选择需要配置的 MST 实例，点击【获取】按钮，进入该 MST 端口配置界面。

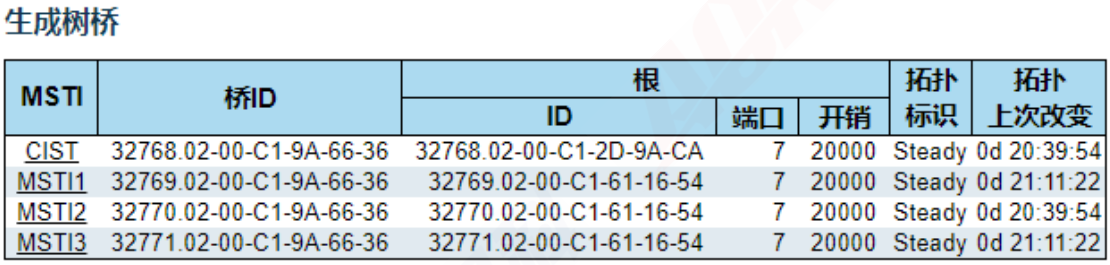
图表 8-5 MSTI 端口配置

配置项	说明
路径开销	Auto：自动计算，系统会自动依据端口速率/类型等参数计算。 Specific：手动指定，取值为 1-200000000 的数字。
优先级	端口优先级，值越小优先级越高。

8.2.6 查看桥状态

点击导航栏中：监控->生成树->桥状态，进入生成树桥状态界面。

图表 8-6 生成树桥状态



配置项	说明
桥 ID	MST 域或 CIST 域的桥 ID。
根 ID	MSTI 或 CIST 生成树中选举的根桥 ID。
根端口	当前生成树中的根端口角色。

根开销	当前节点到生成树根的总路径开销。
拓扑标识	当前节点的生成树拓扑变化标识。
拓扑上次改变	上次检测到拓扑变化的时间。

点击桥状态页面中具体的 MSTI，比如点击【CIST】，可以查看该 MST/CIST 的详细状态信息，以及生成树内端口信息。

图表 8-7 桥详细状态

生成树详细桥状态

生成树桥状态	
桥实例	CIST
桥ID	32768.02-00-C1-9A-66-36
根ID	32768.02-00-C1-2D-9A-CA
根开销	20000
根端口	7
域根	32768.02-00-C1-61-16-54
内部根开销	20000
拓扑标识	Steady
拓扑变化计数	625
拓扑上次改变	0d 20:40:10

CIST 端口 & 聚合 状态

端口	端口 ID	角色	状态	路径开销	边缘	点对点	运行时间
6	128:006	DesignatedPort	Forwarding	20000	No	Yes	0d 21:38:11
7	128:007	RootPort	Forwarding	20000	No	Yes	0d 21:15:17
8	128:008	AlternatePort	Discarding	20000	No	Yes	0d 21:15:17

配置项	说明
桥实例	当前查看的桥实例名称。
桥 ID	当前桥 ID。
根 ID	MSTI 或 CIST 生成树中选举的根桥 ID。
根开销	当前节点到生成树根的总路径开销。
根端口	当前生成树中的根端口角色。
域根	MST 域根 ID。 CIST 的域根就是整个网络的根桥。
内部根开销	当前节点到域根的总路径开销。
拓扑标识	当前节点的生成树拓扑变化标识。
拓扑变化计数	检测到拓扑变化的次数。
拓扑上次改变	上次检测到拓扑变化的时间。
端口	桥的端口号。
端口 ID	由端口优先级和端口号合成的协议端口 ID。
角色	端口角色，包括 Root：根端口，接口连接根桥方向

	Designated：指定端口，连接根端口的端口 Alternate：备选端口，备用根端口 Backup：备份端口 Disable：接口 Down 或者关闭生成树协议的端口
状态	端口当前协议状态，包括: Forwarding：转发 Discarding：丢弃 Learning：学习 Listening：侦听
路径开销	端口的路径开销。
边缘	是否边缘端口。
点对点	是否点对点链路。
运行时间	端口协议运行时间。

8.2.7 查看端口状态

点击导航栏中：监控->生成树->端口状态，进入生成树端口状态界面。

图表 8-8 生成树端口状态

生成树端口状态

端口	CIST角色	CIST状态	运行时间
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	DesignatedPort	Forwarding	0d 21:37:35
7	RootPort	Forwarding	0d 21:14:41
8	AlternatePort	Discarding	0d 21:14:41
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-

配置项	说明
CIST 角色	CIST 端口角色，主要包括 Root：根端口，接口连接根桥方向 Designated：指定端口，连接根端口的端口 Alternate：备选端口，备用根端口 Backup：备份端口 Disable：接口 Down 或者关闭生成树协议的端口
CIST 状态	CIST 端口当前协议状态，包括: Forwarding：转发 Discarding：丢弃 Learning：学习

	Listening：侦听
运行时间	端口协议运行时间。

8.2.8 查看端口统计

点击导航栏中：监控->生成树->端口统计，进入生成树端口统计界面。

图表 8-9 生成树端口统计

生成树统计

端口	发送				接收				丢弃	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	未知	非法
6	38957	0	0	0	43	0	0	0	0	0
7	38231	0	0	0	38189	0	0	0	0	0
8	15	0	0	0	38178	0	0	0	0	0

表 8-1 端口统计参数说明

配置项	说明
端口	端口号
发送 MSTP	发送 MSTP 报文数。
发送 RSTP	发送 RSTP 报文数。
发送 STP	发送 STP 报文数。
发送 TCN	发送 TCN 报文数。
接收 MSTP	接收 MSTP 报文数。
接收 RSTP	接收 RSTP 报文数。
接收 STP	接收 STP 报文数。
接收 TCN	接收 TCN 报文数。
丢弃未知	丢弃未知 BPDU 报文数。
丢弃非法	丢弃非法 BPDU 报文数。

8.3 MSTP 配置举例

8.3.1 组网需求

配置 MSTP，如下图中不同 VLAN 的报文按照不同的生成树实例转发，具体配置为：

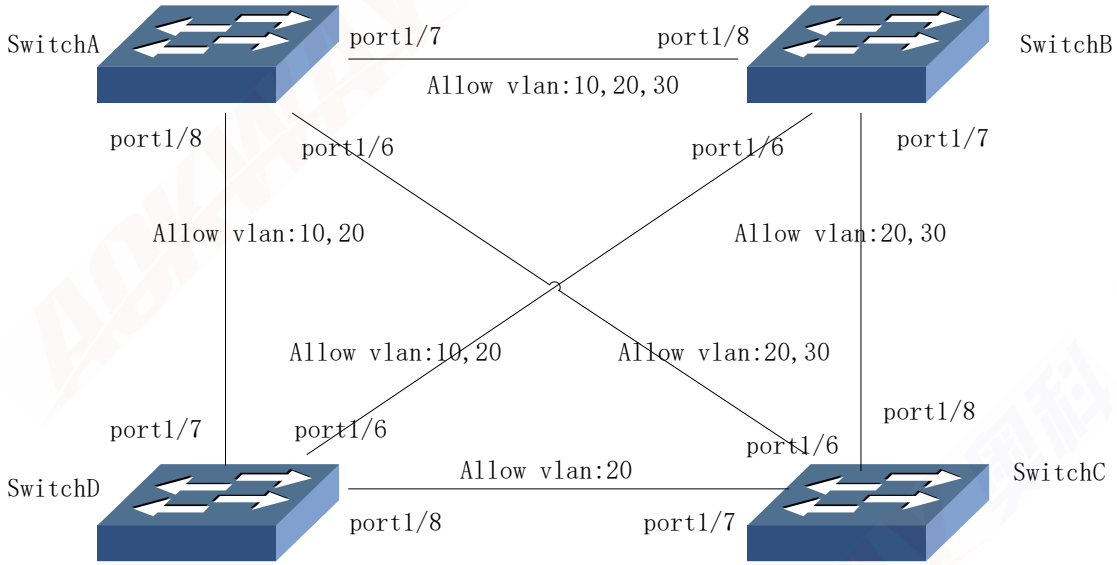
- 网络中所有设备属于同一个 MST 域，假设为 global 域；
- VLAN 20 沿着实例 0（即默认桥接实例 CIST）转发，VLAN 10 的报文沿着实例 1 转发，VLAN 30 沿着实例 3 转发。

各设备的参数配置如下表所示：

参数 / 设备	VLAN	实例	端口

Switch A	10	1	port1/7，port1/8
	20	0	port1/7，port1/8，port1/6
	30	3	port1/7，port1/6
Switch B	10	1	port1/8， port1/6
	20	0	port1/7，port1/8，port1/6
	30	3	port1/7，port1/8
Switch C	20	0	port1/7，port1/8，port1/6
	30	3	port1/8，port1/6
Switch D	10	1	port1/7，port1/6
	20	0	port1/7，port1/8，port1/6

图表 8-10 MSTP 案例



说明

- 图中链路上的说明“Allow vlan”表示该链路允许哪些 VLAN 的报文通过。

8.3.2 配置 Switch A

步骤 1：配置 VLAN 和端口。

在导航栏选择：配置->VLAN，配置端口 6、7、8 为 trunk 口，配置对应的 allow vlan，点击【保存】按钮保存配置。

图表 8-11 MSTP 案例 Switch A VLAN 配置

全局VLAN配置

允许访问VLANs	1,10,20,30
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入 过滤	准入 接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1000	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20,30	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

步骤 2：配置生成树桥参数。

在导航栏选择：配置->生成树->桥设置，配置协议版本为 MSTP，点击【保存】按钮保存配置。

图表 8-12 MSTP 案例 Switch A 桥配置

STP桥设置

基本设置

协议版本	MSTP
桥优先级	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop计数	20
Transmit Hold计数	6

高级设置

边缘端口BPDU过滤	☐
边缘端口BPDU保护	☐
端口错误恢复	☐
端口错误恢复超时	

步骤 3：配置生成树 MSTI 映射。

在导航栏选择：配置->生成树->MSTI 映射，配置 VLAN 10 映射到 MSTI 1，VLAN 30 映射到 MSTI 3，点击【保存】按钮保存配置。

图表 8-13 MSTP 案例 Switch A MSTI 映射配置

MSTI配置

添加由空格或逗号分隔的VLAN.

未映射的VLAN被映射到CIST. (默认桥接实例).

配置标识

配置名称	global
配置版本号	0

MSTI映射

MSTI	映射的VLAN
MSTI1	10
MSTI2	
MSTI3	30
MSTI4	
MSTI5	
MSTI6	
MSTI7	

步骤 3：配置端口使能生成树协议。

在导航栏选择：配置->生成树->CIST 端口，配置端口 6、7、8 为 STP 启用状态。

图表 8-14 MSTP 案例 Switch A CIST 端口配置

STP CIST 端口配置

CIST 聚合端口配置

端口	STP 启用	路径开销	优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
						角色	TCN		
-	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Forced True

CIST 普通端口配置

端口	STP 启用	路径开销	优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
						角色	TCN		
*	☐	<>	<>	<>	☑	☐	☐	☐	<>
1	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
6	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
7	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
8	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto

8.3.3 配置 Switch B

步骤 1：配置 VLAN 和端口。

在导航栏选择：配置->VLAN，配置端口 6、7、8 为 trunk 口，配置对应的 allow vlan，点击【保存】按钮保存配置。

图表 8-15 MSTP 案例 Switch B VLAN 配置

全局VLAN配置

允许访问VLANs	1,10,20,30
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20,30	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

全局VLAN配置

允许访问VLANs	1,10,20,30,40
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20,30,40	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

步骤 2：配置生成树桥参数。

在导航栏选择：配置->生成树->桥设置，配置协议版本为 MSTP，点击【保存】按钮保存配置。

图表 8-16 MSTP 案例 Switch B 桥配置

步骤 3：配置生成树 MSTI 映射。

在导航栏选择：配置->生成树->MSTI 映射，配置 VLAN 10 映射到 MSTI 1，VLAN 30 映射到 MSTI 3，点击【保存】按钮保存配置。

图表 8-17 MSTP 案例 Switch B MSTI 映射配置

MSTI配置

添加由空格或逗号分隔的VLAN.

未映射的VLAN被映射到CIST. (默认桥接实例).

配置标识

配置名称	global
配置版本号	0

MSTI映射

MSTI	映射的VLAN
MSTI1	10
MSTI2	
MSTI3	30
MSTI4	
MSTI5	
MSTI6	
MSTI7	

步骤 3：配置端口使能生成树协议。

在导航栏选择：配置->生成树->CIST 端口，配置端口 8、9、10 为 STP 启用状态。

图表 8-18 MSTP 案例 Switch B CIST 端口配置

STP CIST 端口配置

CIST 聚合端口配置

端口	STP 启用	路径开销	优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
						角色	TCN		
-	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Forced True

CIST 普通端口配置

端口	STP 启用	路径开销	优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
						角色	TCN		
*	☐	<>	<>	<>	☑	☐	☐	☐	<>
1	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
6	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
7	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
8	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto

8.3.4 配置 Switch C

步骤 1：配置 VLAN 和端口。

在导航栏选择：配置->VLAN，配置端口 6、7、8 为 trunk 口，配置对应的 allow vlan，点击【保存】按钮保存配置。

图表 8-19 MSTP 案例 Switch C VLAN 配置

全局VLAN配置

允许访问VLANs	1,20,30
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

步骤 2：配置生成树桥参数。

在导航栏选择：配置->生成树->桥设置，配置协议版本为 MSTP，点击【保存】按钮保存配置。

图表 8-20 MSTP 案例 Switch C 桥配置

STP桥设置

基本设置

协议版本	MSTP
桥优先级	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop计数	20
Transmit Hold计数	6

高级设置

边缘端口BPDU过滤	☐
边缘端口BPDU保护	☐
端口错误恢复	☐
端口错误恢复超时	

步骤 3：配置生成树 MSTI 映射。

在导航栏选择：配置->生成树->MSTI 映射，配置 VLAN 30 映射到 MSTI 3，点击【保存】按钮保存配置。

图表 8-21 MSTP 案例 Switch C MSTI 映射配置

步骤 3：配置端口使能生成树协议。

在导航栏选择：配置->生成树->CIST 端口，配置端口 6、7、8 为 STP 启用状态。

图表 8-22 MSTP 案例 Switch C CIST 端口配置

STP CIST 端口配置

CIST 聚合端口配置

端口	STP 启用	路径开销		优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
							角色	TCN		
-	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Forced True

CIST 普通端口配置

端口	STP 启用	路径开销		优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
							角色	TCN		
*	☐	<>		<>	<>	☑	☐	☐	☐	<>
1	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
6	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
7	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
8	☑	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto		128	Non-Edge	☑	☐	☐	☐	Auto

8.3.5 配置 Switch D

步骤 1：配置 VLAN 和端口。

在导航栏选择：配置->VLAN，配置端口 6、7、8 为 trunk 口，配置对应的 allow vlan，点击【保存】按钮保存配置。

图表 8-23 MSTP 案例 Switch D VLAN 配置

全局VLAN配置

允许访问VLANs	1,10,20
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入 过滤	准入 接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

步骤 2：配置生成树桥参数。

在导航栏选择：配置->生成树->桥设置，配置协议版本为 MSTP，点击【保存】按钮保存配置。

图表 8-24 MSTP 案例 Switch D 桥配置

步骤 3：配置生成树 MSTI 映射。

在导航栏选择：配置->生成树->MSTI 映射，配置 VLAN 10 映射到 MSTI 1，点击【保存】按钮保存配置。

图表 8-25 MSTP 案例 Switch D MSTI 映射配置

MSTI配置

添加由空格或逗号分隔的VLAN.

未映射的VLAN被映射到CIST. (默认桥接实例).

配置标识

配置名称	global
配置版本号	0

MSTI映射

MSTI	映射的VLAN
MSTI1	10
MSTI2	
MSTI3	30
MSTI4	
MSTI5	
MSTI6	
MSTI7	

步骤 3：配置端口使能生成树协议。

在导航栏选择：配置->生成树->CIST 端口，配置端口 6、7、8 为 STP 启用状态。

图表 8-26 MSTP 案例 Switch D CIST 端口配置

STP CIST 端口配置

CIST 聚合端口配置

端口	STP 启用	路径开销	优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
						角色	TCN		
-	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Forced True

CIST 普通端口配置

端口	STP 启用	路径开销	优先级	强制边缘	自动边缘	受限		BPDU保护	点对点
						角色	TCN		
*	☐	<>	<>	<>	☑	☐	☐	☐	<>
1	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
2	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
3	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
4	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
5	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
6	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
7	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
8	☑	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
9	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto
10	☐	Auto	128	Non-Edge	☑	☐	☐	☐	Auto

8.4 CLI 参考命令

命令	switch(config)# spanning-tree mode mstp switch(config)# spanning-tree mst 0 priority 32768 switch(config)# spanning-tree mst hello-time 2 switch(config)# spanning-tree mst max-age 20 forward-time 15 switch(config)# spanning-tree mst max-hops 20 switch(config)# spanning-tree transmit hold-count 6
描述	配置生成树协议版本； 配置生成树 CIST/MSTI 优先级； 配置生成树 hello 报文的周期； 配置生成树最大时长以及延迟时间； 配置生成树 MST 域最大跳数； 配置生成树每秒发送 BPDU 报文的最大数量；

命令	switch(config)# spanning-tree edge bpdu-filter switch(config)# no spanning-tree edge bpdu-filter switch(config)# spanning-tree edge bpdu-guard switch(config)# no spanning-tree edge bpdu-guard switch(config)# spanning-tree recovery interval 33 switch(config)# no spanning-tree recovery interval
描述	配置生成树开启边缘端口 BPDU 过滤； 配置生成树关闭边缘端口 BPDU 过滤； 配置生成树开启边缘端口 BPDU 保护； 配置生成树关闭边缘端口 BPDU 保护； 配置生成树开启端口错误恢复及恢复超时时间； 配置生成树关闭端口错误恢复；

命令	switch(config)# spanning-tree mst name global revision 0 switch(config)# spanning-tree mst 3 vlan 1-10 switch(config)# spanning-tree edge bpdu-guard switch(config)# no spanning-tree edge bpdu-guard switch(config)# spanning-tree recovery interval 33 switch(config)# no spanning-tree recovery interval
描述	配置生成树 MSTI 域配置名称和版本； 配置生成树 MSTI VLAN 映射；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# spanning-tree switch(config-if)# no spanning-tree switch(config-if)# spanning-tree mst 0 cost auto switch(config-if)# spanning-tree mst 1 port-priority 32 switch(config-if)# spanning-tree edge switch(config-if)# no spanning-tree edge switch(config-if)# spanning-tree auto-edge switch(config-if)# no spanning-tree auto-edge switch(config-if)# spanning-tree restricted-role switch(config-if)# no spanning-tree restricted-role switch(config-if)# spanning-tree restricted-tcn switch(config-if)# no spanning-tree restricted-tcn switch(config-if)# spanning-tree bpdu-guard switch(config-if)# no spanning-tree bpdu-guard switch(config-if)# spanning-tree link-type point-to-point
描述	配置端口开启生成树； 配置端口关闭生成树； 配置端口生成树 CIST/MSTI 路径开销； 配置端口生成树 CIST/MSTI 优先级； 配置端口开启生成树强制边缘； 配置端口关闭生成树强制边缘； 配置端口开启生成树自动边缘； 配置端口关闭生成树自动边缘； 配置端口开启生成树受限角色； 配置端口关闭生成树受限角色； 配置端口开启生成树受限 TCN； 配置端口关闭生成树受限 TCN； 配置端口开启生成树 BPDU 保护； 配置端口关闭生成树 BPDU 保护； 配置端口配置生成树链路模式；

命令	switch# show spanning-tree active switch# show spanning-tree interface GigabitEthernet 1/3 switch# show spanning-tree detail
描述	打印生成树桥状态； 打印生成树端口状态； 打印生成树端口统计；

9 组播

9.1 组播配置表

组播配置表（IPMC Profile）用于对 IP 组播流进行访问控制。每个配置表由若干规则组成，规则按照顺序存放，规则通过关联地址表项来完成对 IGMP 的 Report 报文的匹配。基于端口来配置对组播配置表的关联，对该端口输入的 IGMP 的 Report 报文，依次查找所关联的组播配置表的规则，根据最先匹配的规则，确定处理行为。若对应行为为“Deny”，则进行过滤，从而达到对 IP 组播流下游端口访问控制的目的。整个配置流程如下：

- 配置地址表项：参见“地址表项”章节。
- 配置配置表：参见“配置表”章节。
- 关联配置表：参见“组播->IGMP Snooping->配置->端口过滤”章节。

9.1.1 配置表

最多可创建 64 个组播配置表，每个组播配置表最多可设置 128 个规则。

9.1.1.1 配置表配置

在【导航栏】下拉菜单中选择：配置->组播配置表->配置表，进入配置表配置页面。

图表 9-1 组播配置表配置

- 全局模式：

  启用/禁用全局 IPMC 配置表。仅当启用全局配置表时，系统才会开始基于配置表设置进行过滤。

- 配置表设置：

配置项	说明
删除	下次保存时将删除指定的配置表。
配置表名字	用于索引配置表的名称。每个条目都有唯一的名称，最多包含 16 个字母和数字字符。至少有一个字母。
配置表描述	关于配置文件的附加说明，最多包含 64 个字符。不允许中文。

规则	创建配置表后，单击编辑按钮以进入指定配置表的规则设置页面。单击视图按钮将显示有关指定配置表的摘要。 视图按钮：列出指定配置表的规则。 编辑按钮：编辑与指定配置表的规则。

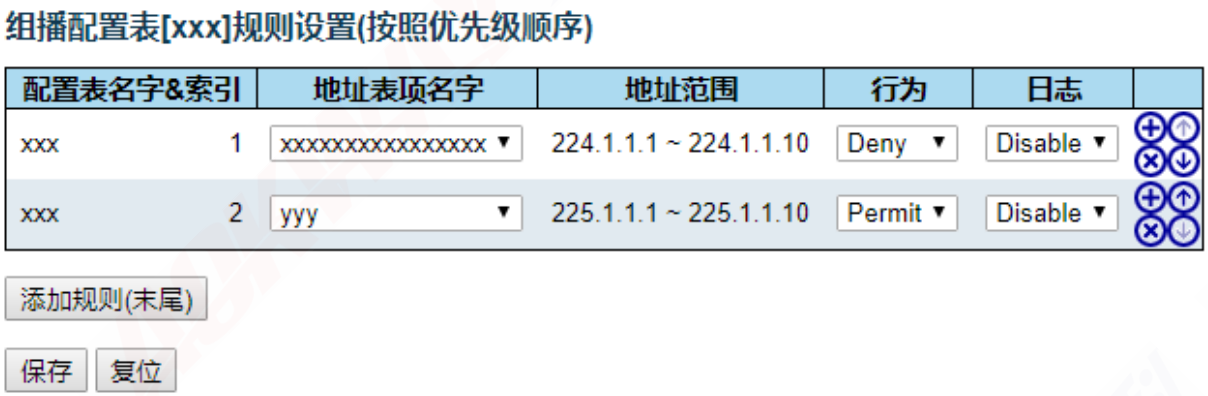
点击“添加新配置表”按钮将创建一个新的配置表。

9.1.1.2 规则配置

以优先顺序显示已配置的规则条目。第一个规则条目在查找中具有最高优先级，而最后一个规则条目在查找中具有最低优先级。

点击配置表页面的编辑按钮进入规则配置页面。

图表 9-2 组播配置表规则设置



配置项	说明
配置表名字&索引	要关联的指定配置表的名称以及规则对应的索引。此字段不可编辑。
地址表项名字	用于指定用于此规则的地址表项的名称。 仅在选定的框中选择现有的配置表地址表项。保存规则时，不允许将此字段选为无（“ - ”）。
地址范围	所选配置表地址表项对应的地址范围。此字段不可编辑，将根据所选的地址表项自动调整。
行为	表示接收到的组地址与规则的地址范围匹配的 IGMP Report 帧的学习操作。 ➢ Permit：允许学习。 ➢ Deny：禁止学习。
日志	表示接收到的组地址与规则的地址范围匹配的 IGMP Report 帧的日志记录首选项。 ➢ Enable：将记录与规则中指定的范围匹配的组地址的相应信息。 ➢ DIsable：不会记录与规则中指定的范围匹配的组地址的相应信息。
规则管理按钮	您可以使用以下按钮管理规则和相应的优先顺序 ：在当前规则之前插入新规则。

	: 删除当前规则。 : 在列表中向上移动当前规则。 : 在列表中向下移动当前规则。

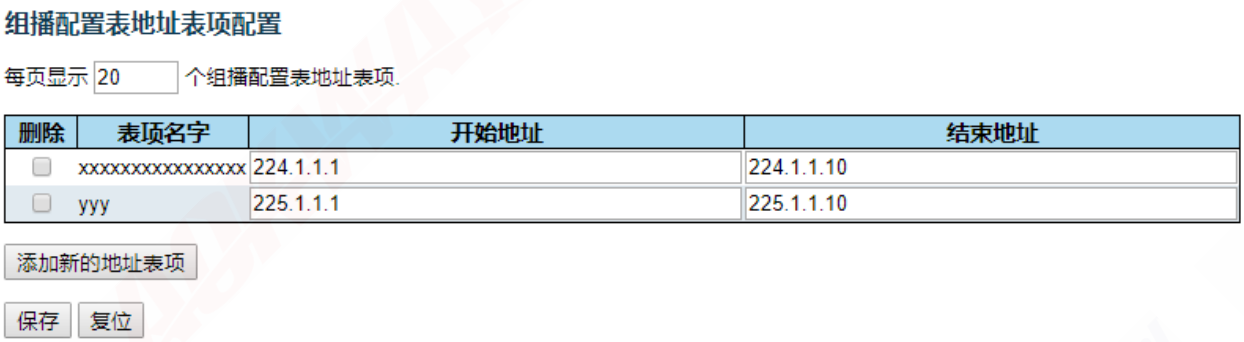
点击“添加规则（末尾）”按钮将在列表的最后添加一个新的规则。

9.1.2 地址表项

地址表项最多可创建 128 条，每个表项可以定义个组播地址范围，用于关联组播配置表的规则，用于进行规则查找时匹配报文。

在【导航栏】下拉菜单中选择：配置->组播配置表->地址表项，进入组播配置表地址表项配置页面。

图表 9-3 组播配置表地址表项配置



配置项	说明
删除	下次保存时将删除指定的地址表项。
表项名字	用于索引地址表项的名称。 每个表项都有唯一的名称，最多包含 16 个字母和数字字符。至少有一个字母。
开始地址	将用作地址范围的起始 IP 多播组地址。
结束地址	将用作地址范围的结束 IP 多播组地址。

点击“添加新的地址表项”按钮将添加一个新的地址表项。

9.1.3 CLI 参考命令

命令	switch(config)# ipmc profile switch(config)# no ipmc profile
描述	配置组播配置表全局开启； 配置组播配置表全局关闭；

命令	switch(config)# ipmc range config1 224.1.1.1 224.1.1.10 switch(config)# no ipmc range config2

描述	配置组播添加地址表； 配置组播删除地址表；

命令	switch(config)# ipmc profile table1 switch(config-ipmc-profile)#description description1 switch(config-ipmc-profile)#range config1 deny log switch(config-ipmc-profile)#range config2 permit next config1 switch(config-ipmc-profile)#no range config2
描述	创建/进入配置表； 配置组播配置表描述； 配置组播配置表添加地址表规则 config1,行为 deny 且开启日志； 配置组播配置表添加地址表规则 config2,行为 permit 且优先级在 config1 后； 配置组播配置表删除地址表规则；

命令	switch# show ipmc profile switch# show ipmc range
描述	打印组播配置表状态； 打印组播地址表状态；

9.2 IGMP Snooping

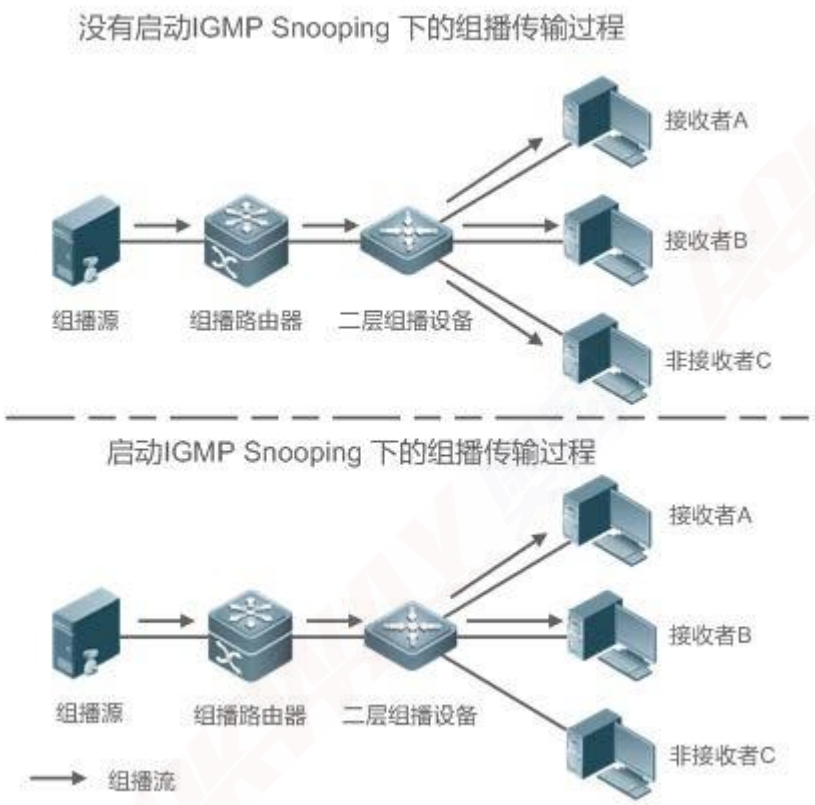
9.2.1 概述

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束的机制，用于管理和控制组播组。

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 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。

如下图所示，当二层组播设备没有运行 IGMP Snooping 时，IP 组播报文在 VLAN 内被广播；当二层组播设备运行了 IGMP Snooping 后，IP 组播报文只发给组成员接收者。

图表 9-4 IGMP Snooping 组播传输过程



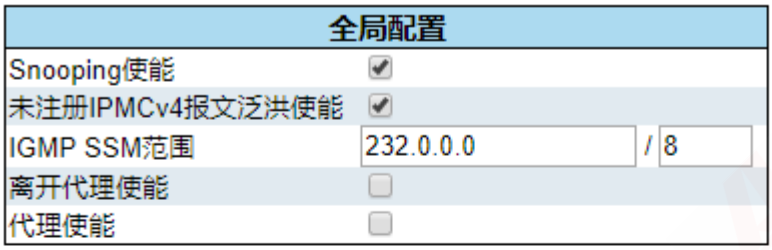
9.2.2 配置

9.2.2.1 基础

在【导航栏】下拉菜单中选择：配置->组播->IGMP Snooping->基础，进入配置页面。

图表 9-5 IGMP Snooping 基础配置

IGMP Snooping配置



端口配置

■ 全局配置

配置项	说明
Snooping 使能	勾选表项全局使能 IGMP Snooping 功能。
未注册 IPMCV4 报文泛洪使能	启用未注册的 IPMCv4 报文泛洪功能。 泛洪使能控制仅在启用 IGMP Snooping 时生效。禁用 IGMP Snooping 时，尽管有此设置，但未注册的 IPMCv4 报文始终可以泛洪。
IGMP SSM 范围	SSM（源特定多播）范围允许 SSM 感知主机和路由器为地址范围内的组运行 SSM 服务模型。将有效的 IPv4 多播地址分配为前缀，并为该范围指定前缀长度（从 4 到 32）。
离开代理使能	启用 IGMP 离开代理。此功能可用于避免将不必要的 Leave 消息转发到路由器端。
代理使能	启用 IGMP 代理。此功能可用于避免转发不必要的 Join 和 Leave 消息转发到路由器端。

■ 端口配置

配置项	说明

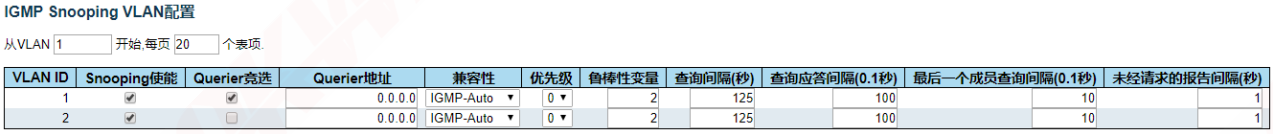
端口	面板端口号
路由器端口	指定哪些端口充当路由器端口。路由器端口是以太网交换机上的一个端口，通向三层组播设备或 IGMP 查询器（IGMP Querier）。如果选择聚合成员端口作为路由器端口，则整个聚合口将充当路由器端口。
快速离开	启用端口快速离开功能。开启此功能后，系统将在收到 IGMPv2 离开消息时删除组记录并停止转发数据，而不发送最后成员查询消息。仅当单个 IGMPv2 主机连接到特定端口时，才建议启用此功能。
组播数限制	限制端口可以属于的组播组数量。也可以配置为不限制。

9.2.2.2 VLAN

下图中显示的 VLAN 为已经创建 SVI 的 VLAN，具体参见“配置 IP”章节。如果对应的 SVI 删除，则其上的 IGMP Snooping 配置将自动删除。

在【导航栏】下拉菜单中选择：配置->组播->IGMP Snooping->VLAN，进入配置页面。

图表 9-6 IGMP Snooping VLAN 配置



配置项	说明
VLAN ID	IGMP VLAN 接口（SVI 口）的 VLAN ID。
Snooping 使能	基于 SVI 口开启 Snooping 功能，最多开启 8 个 SVI 口。
Querier 竞选	勾选表示此 VLAN 允许本设备参与 IGMP Querier 竞选。若未勾选，只能作为 IGMP Non-Querier 设备。
Querier 地址	设置 IGMP Querier IP 头中使用的源地址。未设置 Querier 地址时，系统使用与该 SVI 接口的 IPv4 管理地址。若该 SVI 未设置 IPv4 管理地址时，系统使用第一个可用的 IPv4 管理地址。否则，系统使用预定义的值。默认情况下，此值为 192.168.1.234。
兼容性	主机和路由器采取适当的操作来维护兼容性，具体取决于在网络中的主机和路由器上运行的 IGMP 的版本。 允许的选择是 IGMP-Auto， 强制 IGMPv1， 强制 IGMPv2， 强制 IGMPv3，默认兼容性值为 IGMP-Auto。
优先级（PRI）	SVI 接口优先级。它表示系统生成的 IGMP 控制帧优先级。这些值可用于确定不同类别流量的优先级。允许的范围是 0-7，默认接口优先级值为 0。
鲁棒性变量（RV）	调整网络上预期的数据包丢失数量。允许的范围是 1-255，默认的鲁棒性变量值为 2。
查询间隔（QI）	查询间隔是 Querier 发送的常规查询之间的间隔。 单位为秒，允许的范围是 1-31744 ，默认查询间隔为 125，即 125 秒
查询应答间隔	查询应答间隔用于计算插入到周期性常规查询中的最大应答时间。

（QRI）	单位为 0.1 秒，允许的范围是 0-31744，默认查询应答间隔为 100，即 10 秒。
最后一个成员查询间隔（LLQI）	最后成员查询时间是最后一个成员查询间隔表示的时间值，乘以最后成员查询计数。 单位为 0.1 秒，允许的范围是 0-31744，默认最后一个成员查询间隔为 10，即 1 秒。
未经请求的报告间隔（URI）	未经请求的报告间隔是主机刚成为组成员时重复报告之间的时间。单位为 1 秒，允许的范围是 0-31744，默认未经请求的报告间隔为 1，即 1 秒。

9.2.2.3 端口过滤

端口过滤通过在端口关联组播配置表来完成，组播配置表通过规则配置了针对一系列的组播地址范围的处理行为（Permit or Deny），如果对应行为为 Deny，那么从该端口进入的相应 Report 报文（作为 Join）将被丢弃处理。关于组播配置表配置参见“组播配置表”章节。

在【导航栏】下拉菜单中选择：配置->组播->IGMP Snooping->端口过滤，进入配置页面。

图表 9-7 IGMP Snooping 端口过滤配置

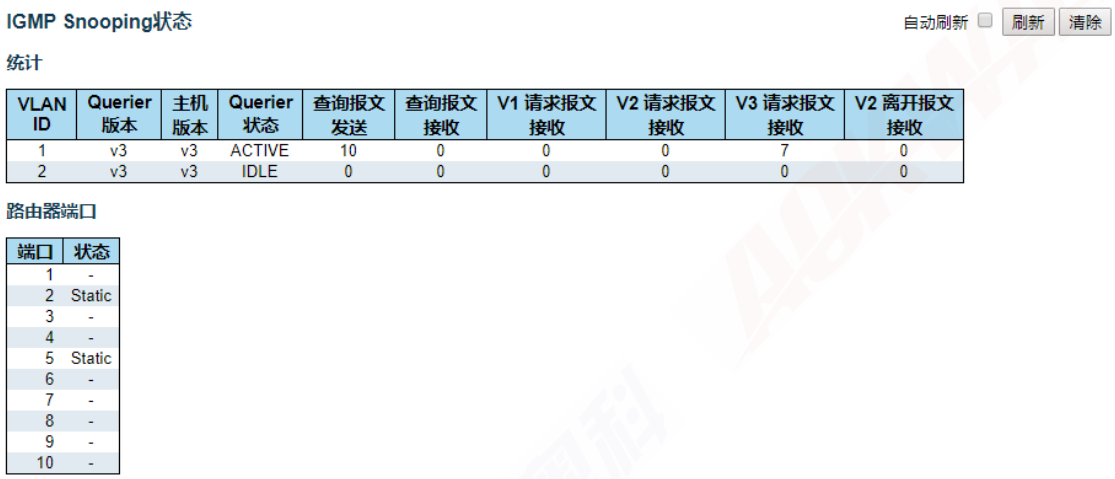
配置项	说明
端口	面板端口号
组播配置表	选择 IPMC 配置表作为对应端口的过滤条件。
	单击将列出所关联配置表的规则。未关联配置表时无显示。

9.2.3 显示

9.2.3.1 状态

在【导航栏】下拉菜单中选择：监控->组播->IGMP Snooping->状态，进入显示页面。

图表 9-8 IGMP Snooping 状态显示



■ 统计

表头	说明
VLAN ID	IGMP SVI 接口的 VLAN ID。
Querier 版本	对应 VLAN 活动 Querier 的版本。
主机版本	对应 VLAN 工作主机的版本。
Querier 状态	显示查询器状态为“ACTIVE”或“IDLE”。如果为“DISABLE”表示对应 SVI 口的管理状态为 Down。
查询报文发送	对应 VLAN 发送的 IGMP Query 报文的数目。
查询报文接收	对应 VLAN 接收的 IGMP Query 报文的数目。
V1 请求报文接收	对应 VLAN 接收的 IGMPV1 Report 报文的数目。
V2 请求报文接收	对应 VLAN 接收的 IGMPV2 Report 报文的数目。
V3 请求报文接收	对应 VLAN 接收的 IGMPV3 Report 报文的数目。
V2 离开报文接收	对应 VLAN 接收的 IGMPV2 Leave 报文的数目。

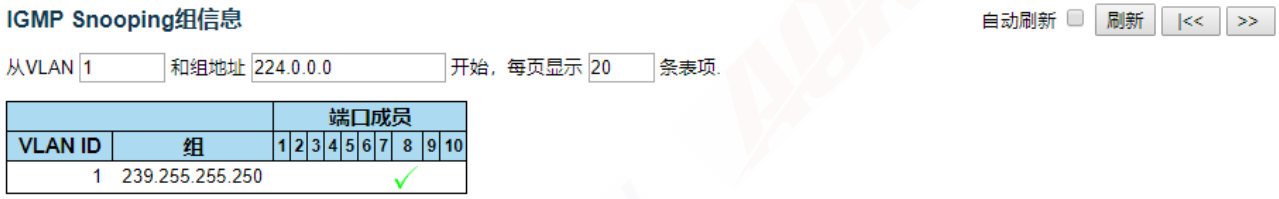
■ 路由器端口

表头	说明
端口	面板端口号
状态	显示哪些端口充当路由器端口。路由器端口是以太网交换机上通向三层组播设备或 IGMP Querier 的端口。 ➢ Static 表示特定端口配置为路由器端口。 ➢ Dynamic 表示特定端口被学习为路由器端口。 ➢ Both 表示特定端口已配置或学习为路由器端口。

9.2.3.2 组信息

在【导航栏】下拉菜单中选择：监控->组播->IGMP Snooping->组信息，进入显示页面。

图表 9-9 IGMP Snooping 组信息



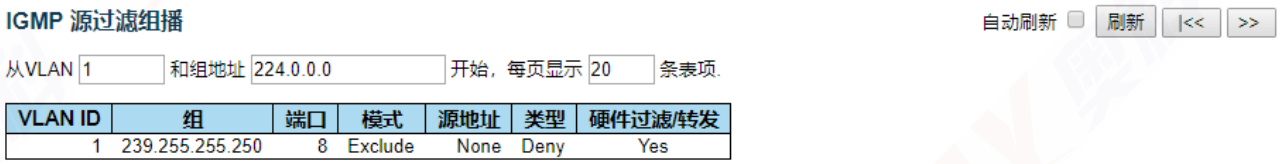
表头	说明
VLAN ID	对应组所属的 VLAN
组	对应组的组播地址
端口成员	对应组的下游端口

9.2.3.3 源过滤组播

IGMP SFM（源过滤组播）信息表还包含 SSM（源特定组播）信息。该表首先按 VLAN ID 排序，然后按组排序，再按端口排序。属于同一组的不同源地址被视为单个条目。

在【导航栏】下拉菜单中选择：监控->组播->IGMP Snooping->源过滤组播，进入显示页面。

图表 9-10 IGMP Snooping 源过滤组播



表头	说明
VLAN ID	对应组所属的 VLAN
组	对应组的组播地址
端口	对应组的下游端口
模式	基于（VLAN ID，组地址，端口）的过滤模式。 ➢ Exclude：组播流的源 IP 属于源地址列表的组播流被过滤。（若源地址为 none，则表示允许所有源）。 ➢ Include：组播流的源 IP 属于源地址列表的组播流被允许，源 IP 不属于源地址列表的组播流被过滤。（SSM 即属于这种情况）
源地址	目前，用于过滤的 IPv4 源地址的最大数量（每组）为 8。当没有任何源过滤地址时，源地址字段中显示文本“无”。
类型	表示过滤还是允许，跟模式的值强相关。 模式为 Exclude 时，类型为 Deny，表示对源 IP 属于源地址列表的组播流进行过滤。

	模式为 Include 时，类型为 Allow，表示对源 IP 属于源地址列表的组播流允许转发。
硬件过滤/转发	表示硬件是否支持对组播流进行过滤或者转发。 Yes 表示支持; No 表示不支持，由软件完成。

9.2.4 CLI 参考命令

命令	switch(config)# ip igmp snooping switch(config)# no ip igmp snooping switch(config)# ip igmp unknown-flooding switch(config)# no ip igmp unknown-flooding switch(config)# ip igmp ssm-range 232.0.0.0 8 switch(config)# ip igmp host-proxy switch(config)# no ip igmp host-proxy switch(config)# ip igmp host-proxy leave-proxy switch(config)# no ip igmp host-proxy leave-proxy
描述	配置 IGMP Snooping 开启； 配置 IGMP Snooping 关闭； 配置 IGMP 未注册 IPMCV4 报文泛洪开启； 配置 IGMP 未注册 IPMCV4 报文泛洪关闭； 配置 IGMP SSM 范围； 配置 IGMP 代理开启； 配置 IGMP 代理关闭； 配置 IGMP 离开代理开启； 配置 IGMP 离开代理关闭；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# ip igmp snooping mrouter switch(config-if)# no ip igmp snooping mrouter switch(config-if)# ip igmp snooping immediate-leave switch(config-if)# no ip igmp snooping immediate-leave switch(config-if)# ip igmp snooping max-groups 4 switch(config-if)# ip igmp snooping filter table1
描述	配置端口开启 IGMP Snooping 路由器端口； 配置端口关闭 IGMP Snooping 路由器端口； 配置端口开启 IGMP Snooping 快速离开； 配置端口关闭 IGMP Snooping 快速离开； 配置端口 IGMP Snooping 组播数限制； 配置端口 IGMP Snooping 端口过滤功能（关联组播配置表）；

命令	switch(config)# interface vlan 10
描述	进入 Vlan 的 IP 接口；

命令	switch(config-if)# ip igmp snooping

	switch(config-if)# no ip igmp snooping switch(config-if)# ip igmp snooping querier election switch(config-if)# no ip igmp snooping querier election switch(config-if)# ip igmp snooping querier address 192.168.1.1 switch(config-if)# ip igmp snooping compatibility auto switch(config-if)# ip igmp snooping priority 1 switch(config-if)# ip igmp snooping robustness-variable 2 switch(config-if)# ip igmp snooping query-interval 125 switch(config-if)# ip igmp snooping query-max-response-time 100 switch(config-if)# ip igmp snooping last-member-query-interval 10 switch(config-if)# ip igmp snooping unsolicited-report-interval 1
描述	配置 SVI 开启 IGMP Snooping; 配置 SVI 关闭 IGMP Snooping; 配置 SVI 开启 IGMP Snooping Querier 竞选; 配置 SVI 关闭 IGMP Snooping Querier 竞选; 配置 SVI IGMP Snooping Querier 地址; 配置 SVI IGMP Snooping 兼容版本; 配置 SVI IGMP Snooping 控制帧优先级; 配置 SVI IGMP Snooping 鲁棒性变量; 配置 SVI IGMP Snooping 查询间隔; 配置 SVI IGMP Snooping 查询应答间隔; 配置 SVI IGMP Snooping 最后一个成员查询间隔; 配置 SVI IGMP Snooping 未经请求的报告间隔;

命令	switch# show ip igmp snooping detail switch# show ip igmp snooping group-database detail switch# show ip igmp snooping group-database sfm-information
描述	打印 IGMP Snooping 状态; 打印 IGMP Snooping 组成员; 打印 IGMP Snooping 源过滤组播;

10 LLDP

10.1 概述

LLDP（Link Layer Discovery Protocol，链路层发现协议）是由 IEEE 802.1AB 定义的一种链路层发现协议。通过 LLDP 协议能够进行拓扑的发现及掌握拓扑的变化情况。LLDP 将设备的本地信息组织成 TLV 的格式（Type/Length/Value，类型/长度/值）封装在 LLDPDU（LLDP data unit，链路层发现协议数据单元）中发送给邻居设备，同时它将邻居设备发送的 LLDPDU 以 MIB（Management Information Base，管理信息库）的形式存储起来，提供给网络管理系统访问。

通过 LLDP，网络管理系统可以掌握拓扑的连接情况，比如设备的哪些端口与其它设备相连接，链路连接两端的端口的速率、双工是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

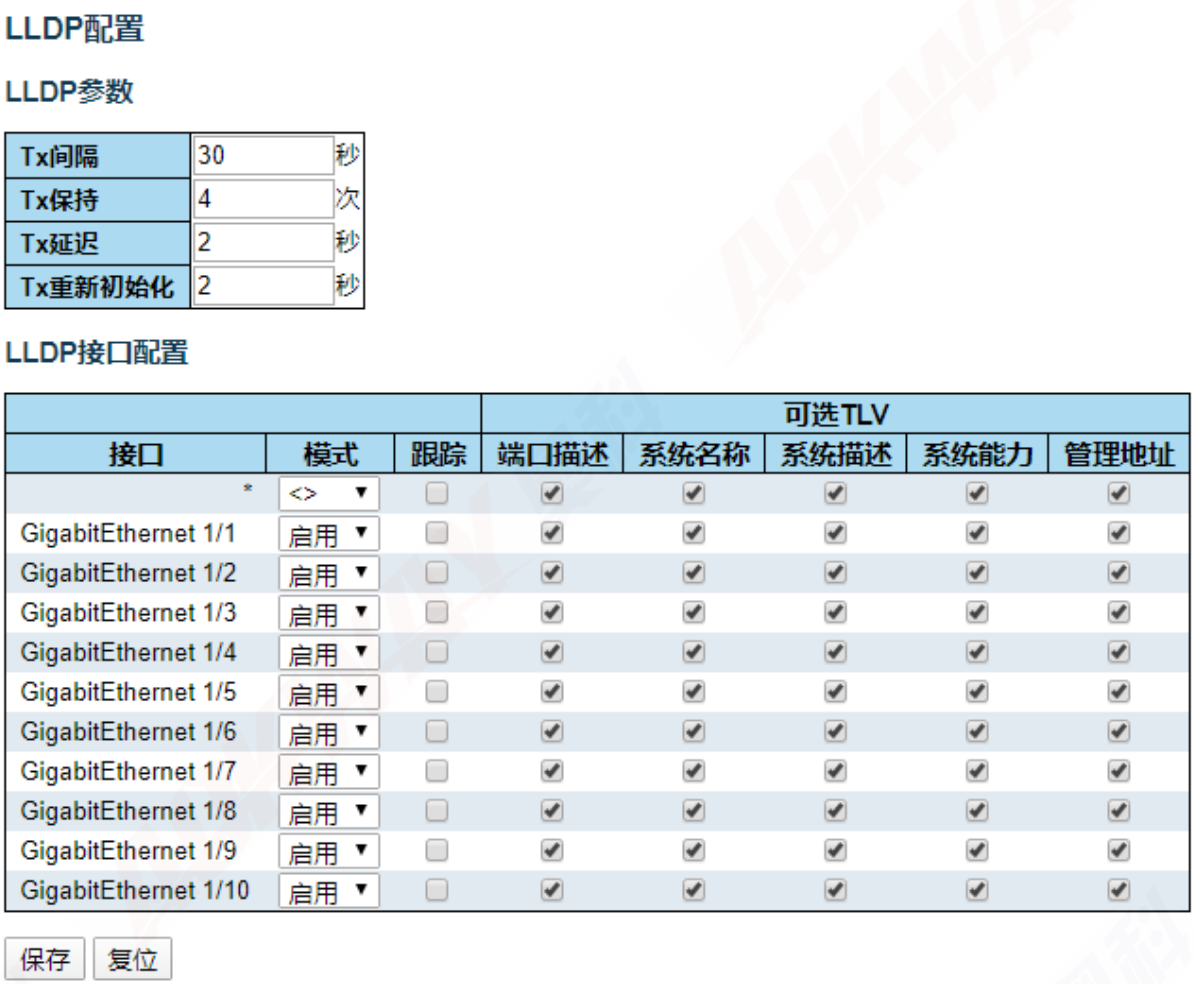
LLDP-MED（Link Layer Discovery Protocol for Media Endpoint Devices）是一个在工作在端点设备（如 IP 电话、）间的 LLDP 扩展。它特别为 IP 语音（Voice over IP）应用提供支持，并且为能力发现、网络策略、以太网供电、地址信息等提供附加的 TLV。默认情况下，所有 LLDP-MED TLV 都是启用的。

10.2 配置

10.2.1 LLDP

在【导航栏】下拉菜单中选择：配置->LLDP->LLDP，进入配置页面。

图表 10-1 LLDP 配置



■ LLDP 参数

配置项	说明
Tx 间隔	交换机会周期性的发送 LLDP 报文，以使得邻居获得的信息是更新后的。该配置项用于控制发送的周期，范围为 5-32768，单位为秒，默认值为 30。
Tx 保持	LLDP 报文中的信息在一段时间会认为是有效的，这段时间称为保持时间，保持时间=Tx 保持 * Tx 间隔。Tx 保持范围为 2-10，单位是次数，默认值为 4。
Tx 延迟	当配置修改时，需要发送新的 LLDP 报文，但新的 LLDP 报文并不会马上发送，必须等待至少“Tx 延迟”时间那么长。Tx 延迟时间不能超过 Tx 间隔时间的 1/4。范围为 1-8192，单位为秒，默认值为 2。
Tx 重新初始化	当 LLDP 禁用时，会发送一个 LLDP Shutdown 报文告知邻居 LLDP 信息不再有效，LLDP 再次初始化与 LLDP Shutdown 报文之间必须有一个间隔时间，即为此配置项。范围为 1-10，单位为秒，默认值为 2。

■ 接口配置

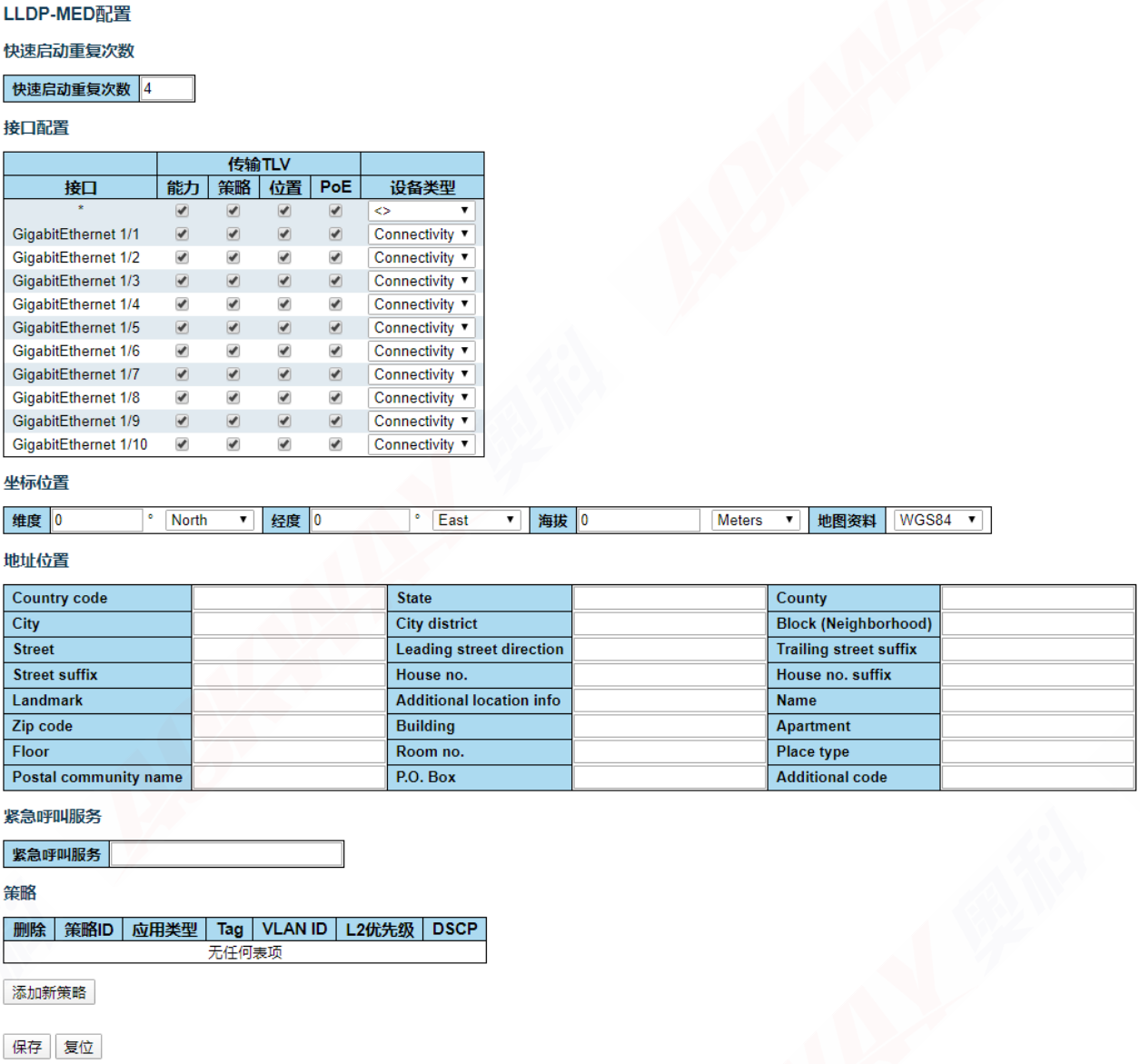
配置项	说明

接口	交换机的接口名称
模式	➢ 仅 Rx：交换机不会发送 LLDP 信息，但是会分析来自邻居单元的 LLDP 信息。 ➢ 仅 Tx：交换机将丢弃从邻居收到的 LLDP 信息，但会发出 LLDP 信息。 ➢ 禁用：交换机将不会发送 LLDP 信息，并将丢弃从邻居收到的 LLDP 信息。 ➢ 启用：交换机将发出 LLDP 信息，并将分析从邻居收到的 LLDP 信息。
跟踪	是否开启 LLDP-TRAP 功能，默认关闭该功能。 通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。
可选 TLV	表中 5 种 TLV 为可选的，默认全部开启，可以通过取消选择将某种 TLV 关闭。开启的 TLV 将会包含在发送的 LLDP 报文中。

10.2.2 LLDP-MED

在【导航栏】下拉菜单中选择：配置->LLDP->LLDP-MED，进入配置页面。

图表 10-2 LLDP-MED 配置



紧急呼叫服务和策略均与 Voice VLAN 功能相关，暂不支持 Voice VLAN，因此，相关内容不做描述。

■ 快速启动重复次数

网络连接设备将仅在 LLDPDU 中传输 LLDP TLV。仅在检测到 LLDP-MED 端点设备之后，具有 LLDP-MED 功能的网络连接设备才会开始在关联接口上传出的 LLDPDU 中通告 LLDP-MED TLV。当检测到新的 LLDP-MED 邻居时，LLDP-MED 应用程序将暂时加快 LLDPDU 的传输速度，将在一秒内开始，以便与新邻居尽快共享 LLDP-MED 信息。

由于在邻居之间传输期间可能会丢失 LLDP 帧，因此建议多次重复快速启动传输，以增加邻居接收 LLDP 帧的可能性。使用快速启动重复计数，可以指定重复快速启动传输的次数。如果接收到具有新信息的 LLDP 帧，则假设发送 4 个间隔为 1 秒的 LLDP 帧，推荐值为 4 倍。

应当注意，LLDP-MED 和 LLDP-MED 快速启动机制仅旨在在 LLDP-MED 网络连接设备和端点设备之间的链接上运行，因此不适用于 LAN 基础设施元素之间的链接，包括网络连接设备或其他类型的链接。

■ 接口配置

配置项	说明
接口	交换机的接口名称。
传输 TLV	表中 4 种 TLV 为可选的，默认全部开启，可以通过取消选择将某种 TLV 关闭。开启的 TLV 将会包含在发送的 LLDP-MED 信息中。
设备类型	任何 LLDP-MED 设备都作为特定类型的 LLDP-MED 设备运行，可以是网络连接设备（Connectivity），也可以是端点设备（End-Point）。 ➢ 网络连接设备是一种 LLDP-MED 设备，可为 LLDP-MED 端点设备提供基于 IEEE 802 LAN 技术的网络访问。 ➢ 端点设备位于网络边缘，基于 IEEE802 LAN 技术提供 IP 通信服务。 网络连接设备和端点设备之间的主要区别在于，只有端点设备才能启动 LLDP-MED 信息交换。 一般而言，交换机应该始终属于网络连接设备，但与其他交换机相连时，若希望启动 LLEP-MED 信息交换，也可以将其配置为端口设备。

■ 坐标位置

配置项	说明
维度	选择“North”或者“South”，取值范围 0-90。支持 4 位小数。
经度	选择“East”或者“West”，取值范围 0-180。支持 4 位小数。
海拔	选择“Meters”或者“Floors”。取值范围-2097151.9 to 2097151.9，支持 1 位小数。 Meters 表示海拔高度。 Floors 表示楼层高度，如果在室外，即表示海拔高度，如果在室内，表示与建筑物地面的相对高度。
地图资料	WGS84:（地理 3D）-1984 年世界大地测量系统，CRS 代码 4327，原始子午线名称：格林威治。 NAD83 / NAVD88：北美基准 1983，CRS 代码 4269，子午线名称：格林威治；相关的垂直基准是 1988 年的北美垂直基准（NAVD88）。当参考陆地上而非潮水附近的位置（将使用基准= NAD83 / MLLW）时，将使用此基准对。 NAD83 / MLLW：北美基准 1983，CRS 代码 4269，子午线名称：格林威治；关联的垂直基准是平均低水位（MLLW）。当参考水/海/海洋上的位置时，将使用此基准对。

■ 地址位置

基于 IETF 公民地址的位置配置信息。合并的市民地址信息的字符总数不得超过 250 个字符。

有关限制 250 个字符的注意事项。

1）如果使用了多个市民地址位置，则每个市民地址位置都会在市民地址位置文本中加上 2 个额外的字符。

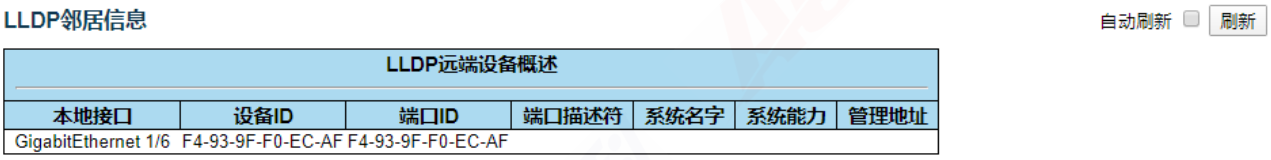
2）2 个字母的国家代码不属于 250 个字符的限制。

10.3 显示

10.3.1 LLDP 邻居

在【导航栏】下拉菜单中选择：监控->LLDP->邻居，进入显示页面。

图表 10-3 LLDP 邻居信息

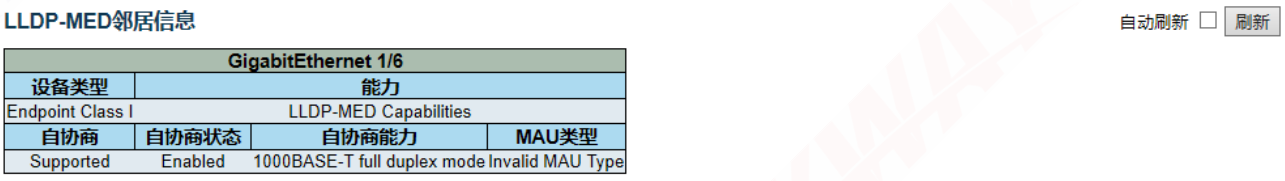


表头	说明
本地接口	收到 LLDP 报文的本地接口名称。
设备 ID	对应邻居的 LLDP 报文的标识。
端口 ID	对应邻居的端口信息的标识。
端口描述符	对应邻居通告的端口的描述信息。
系统名字	对应邻居通告的系统的名称。
系统能力	对应邻居通告的能力信息。
管理地址	对应邻居单元的地址，用于更高层的实体，以帮助网络管理进行发现。例如，这可以保存邻居的 IP 地址。

10.3.2 LLDP-MED 邻居

在【导航栏】下拉菜单中选择：监控->LLDP->MED 邻居，进入显示页面。

图表 10-4 LLDP-MED 邻居信息



表头	说明
接口	收到 LLDP 报文的本地接口名称。
设备类型	LLDP-MED 设备由两种主要的设备类型组成：网络连接设备和端点设备。 LLDP-MED 网络连接设备：TIA-1057 中定义的 LLDP-MED 网络连接设备可以是基于以下任何技术的 LAN 访问设备： 1.局域网交换机/路由器 2. IEEE 802.1 桥接 3. IEEE 802.3 转发器（出于历史原因被包括在内） 4. IEEE 802.11 无线访问点 5.任何支持 TIA-1057 定义的 IEEE 802.1AB 和 MED 扩展并且可以通过任何方法中继 IEEE 802 帧的设备。

	LLDP-MED 端点设备：TIA-1057 中定义的 LLDP-MED 端点设备位于 IEEE 802 LAN 网络边缘，并使用 LLDP-MED 框架参与 IP 通信服务。在 LLDP-MED 端点设备类别中，LLDP-MED 方案分为更多的端点设备类，如下所示。 每个 LLDP-MED 端点设备类的定义都基于为先前的端点设备类定义的功能。例如，任何声称符合媒体端点标准的 LLDP-MED 端点设备（II 类）也将支持适用于通用端点（I 类）的 TIA-1057 的所有方面，以及任何声称符合标准的 LLDP-MED 端点设备作为通信设备。 （III 类）还将支持适用于媒体端点（II 类）和通用端点（I 类）的 TIA-1057 的所有方面。 LLDP-MED 通用端点（I 类） LLDP-MED 通用端点（I 类）定义适用于所有需要 TIA-1057 中定义的基本 LLDP 发现服务的端点产品，但是不支持 IP 媒体或充当最终用户通信设备。这样的设备可以包括（但不限于）IP 通信控制器，其他与通信相关的服务器，或任何需要 TIA-1057 中定义的基本服务的设备。 此类中定义的发现服务包括 LAN 配置，设备位置，网络策略，电源管理和清单管理。 LLDP-MED 媒体端点（II 类） LLDP-MED 媒体端点（II 类）定义适用于具有 IP 媒体功能的所有端点产品，但是可能会或可能不会与特定的最终用户关联。功能包括为先前的通用端点类（I 类）定义的所有功能，并且已扩展为包括与媒体流相关的方面。预期符合该类别的示例产品类别包括（但不限于）语音/媒体网关，会议桥，媒体服务器等。 此类中定义的发现服务包括特定于媒体类型的网络层策略发现。 LLDP-MED 通信端点（III 类） LLDP-MED 通信端点（III 类）定义适用于充当支持 IP 媒体的最终用户通信设备的所有端点产品。功能包括为先前的通用端点（I 类）和媒体端点（II 类）定义的所有功能，并且已扩展为包括与最终用户设备有关的方面。预期符合该类别的示例产品类别包括（但不限于）最终用户通信设备，例如 IP 电话，基于 PC 的软电话或直接支持最终用户的其他通信设备。 此类中定义的发现服务包括位置标识符的提供（包括 ECS / E911 信息），嵌入式 L2 交换机支持，库存管理。
能力	描述了邻居单元的 LLDP-MED 能力。可能的能力是: 1.LLDP-MED 能力 2.网络策略 3.位置识别 4.通过 MDI-PSE 扩展电源 5.通过 MDI-PD 扩展电源 6.库存 7.保留

自协商	自动协商标识邻居是否支持 MAC / PHY 自动协商。
自协商状态	自动协商状态标识当前是否在邻居上启用了自动协商。如果自动协商的支持或者自动协商状态被禁用，IEEE 802.3 PMD 的操作模式将操作 MAU 类型字段的值，而不是通过自动协商确定的。
自协商能力	自动协商功能显示了邻居的 MAC / PHY 的自动协商能力。
MAU 类型	显示了邻居的 MAU 类型。

10.3.3 以太网供电

只有支持以太网供电功能的交换机，才有此页面。

在【导航栏】下拉菜单中选择：监控->LLDP->以太网供电，进入显示页面。

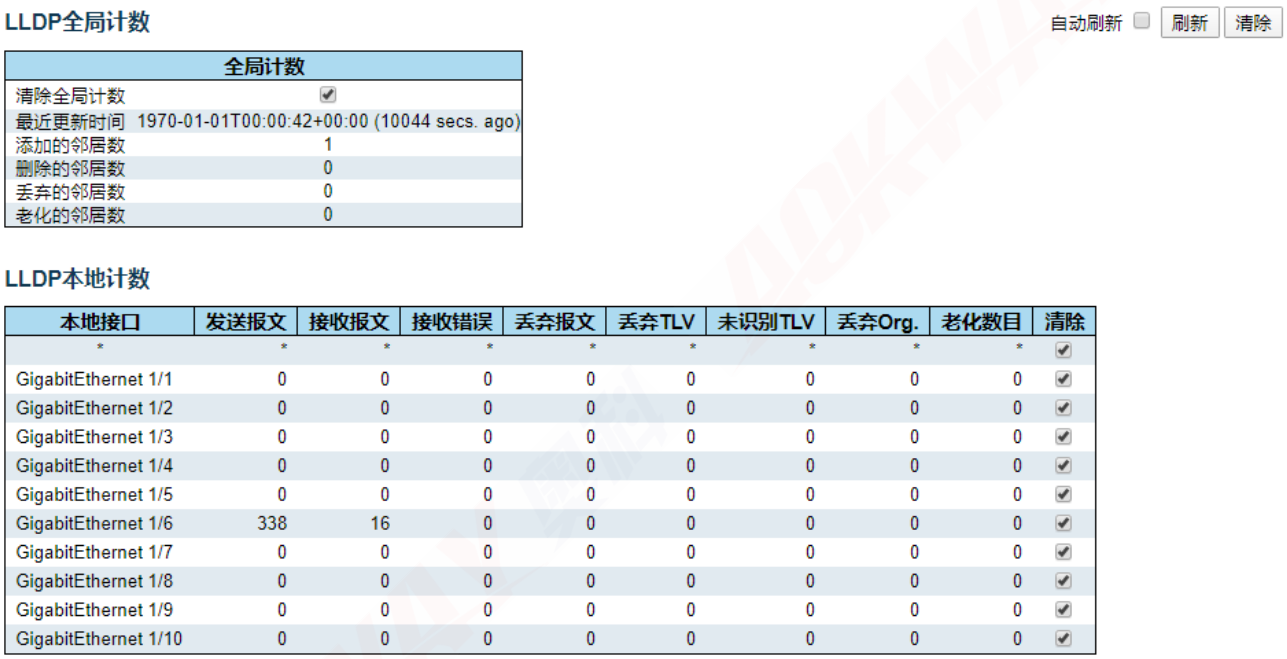
图表 10-5 LLDP 邻居以太网供电信息

表头	说明
本地接口	收到 LLDP 报文的本地接口名称。
电源类型	电源类型表示该设备是否是一个 PSE 设备或 PD 设备，如果电源类型未知，则将其表示为“保留”。
电源 source	如果是 PSE 设备，电源 source 在其主电源或备用电源上运行。如果不清楚 PSE 设备是使用其主电源还是备用电源，则将其指示为“未知”。 如果设备是 PD 设备，则可以使用其本地电源运行，也可以使用 PSE 作为电源。它也可以同时使用本地电源和 PSE。如果不清楚使用哪个电源，则将其指示为“未知”。
电源优先级	电源优先级表示 PD 设备的优先级，或与正在供电的 PSE 类型设备的接口关联的电源优先级。 电源优先级分为三个级别。这三个级别是：Critical，High 和 Low。 如果电源优先级未知，则指示为“未知”。
最大功率	“最大功率指示 PD 设备从 PSE 设备所需的最大功率（以 W 为单位），或者表示 PSE 设备根据其当前配置能够通过最大长度电缆提供的最小功率。最大允许值为 102.3W。

10.3.4 端口统计

在【导航栏】下拉菜单中选择：监控->LLDP->端口统计，进入显示页面。

图表 10-6 LLDP 统计信息



■ 全局计数

表头	说明
清除全局计数	选中后，点击“清除”按钮则清除全局计数。
最近更新时间	显示最近一次删除或添加条目的时间。它还显示自检测到上一次更改以来经过的时间。
添加的邻居数	显示自交换机重启以来添加的条目数。
删除的邻居数	显示自交换机重启以来已删除的条目数。
丢弃的邻居数	显示由于条目表已满而丢弃的 LLDP 报文数。
老化的邻居数	显示由于老化时间到期而删除的条目数。

■ 本地计数

表头	说明
本地接口	接收或者发送 LLDP 报文的本地接口名称。
发送报文	接口发送的 LLDP 报文数目。
接收报文	接口接收的 LLDP 报文数目。
接收错误	接口接收到的包含某种错误的 LLDP 报文数目。
丢弃报文	如果在接口上收到 LLDP 报文，并且交换机的内部表已满，则对 LLDP 报文进行计数并丢弃。这种情况在 LLDP 标准中被称为“邻居太多”。如果表中尚未包含设备 ID 或远程端口 ID，则 LLDP 报文需要在表中添加新条目。当给定接口的链路断开，接收到 LLDP Shutdown 报文或者条目老化时，将从表中删除条目。
丢弃 TLV	每个 LLDP 报文可以包含多条信息，称为 TLV(TLV 是“类型长度值”的缩写)。如果 TLV 格式错误，则将其计数并丢弃。

未识别 TLV	格式正确但类型值未知的 TLV 的数量。
丢弃 Org.	如果 LLDP 报文携带组织 TLV(organizationally TLV)，但是该 TLV 不支持，则进行计数并丢弃。
老化数目	每个 LLDP 报文包含有关 LLDP 信息有效时间（超时时间）的信息。如果在有效时间内没有新的 LLDP 报文收到，LLDP 信息将被删除，而老化数目增加。
清除	选中后，点击“清除”按钮则清除对应接口的本地计数。

10.4 CLI 命令参考

命令	switch(config)# lldp timer 20 switch(config)# lldp holdtime 5 switch(config)# lldp transmission-delay 3 switch(config)# lldp reinit 4 switch(config)# no lldp timer switch(config)# no lldp holdtime switch(config)# no lldp transmission-delay switch(config)# no lldp reinit
描述	配置 LLDP 发送间隔时间为 20 秒。 配置 LLDP 发送保持次数为 5 次。 配置 LLDP 发送延迟为 3 秒。 配置 LLDP 发送重新初始化时间为 4 秒。 恢复 LLDP 发送间隔时间为默认值 30 秒。 恢复 LLDP 发送保持次数为默认值 4 次。 恢复 LLDP 发送延迟为默认值 2 秒。 恢复 LLDP 发送重新初始化时间为默认值 2 秒。

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp receive switch(config-if)# lldp transmit switch(config-if)# no lldp receive switch(config-if)# no lldp transmit
描述	开启 LLDP 报文接收。（默认开启） 开启 LLDP 报文发送。（默认开启） 关闭 LLDP 报文接收。 关闭 LLDP 报文发送。

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp trap switch(config-if)# no lldp trap
描述	开启 LLDP Trap 功能。 关闭 LLDP Trap 功能。（默认关闭）

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp tlv-select port-description switch(config-if)# lldp tlv-select system-name switch(config-if)# lldp tlv-select system-description switch(config-if)# lldp tlv-select system-capabilities switch(config-if)# lldp tlv-select management-address switch(config-if)# no lldp tlv-select port-description switch(config-if)# no lldp tlv-select system-name switch(config-if)# no lldp tlv-select system-description switch(config-if)# no lldp tlv-select system-capabilities switch(config-if)# no lldp tlv-select management-address
描述	开启 LLDP 可选 TLV“端口描述”。（默认开启） 开启 LLDP 可选 TLV“系统名称”。（默认开启） 开启 LLDP 可选 TLV“系统描述”。（默认开启） 开启 LLDP 可选 TLV“系统能力”。（默认开启） 开启 LLDP 可选 TLV“管理地址”。（默认开启） 关闭 LLDP 可选 TLV“端口描述”。 关闭 LLDP 可选 TLV“系统名称”。 关闭 LLDP 可选 TLV“系统描述”。 关闭 LLDP 可选 TLV“系统能力”。 关闭 LLDP 可选 TLV“管理地址”。

命令	switch(config)# lldp med fast 5 switch(config)# no lldp med fast
描述	配置 LLDP-MED 快速启动重复次数为 5 次。 恢复 LLDP-MED 快速启动重复次数为默认值 4 次。

命令	switch(config)# lldp med location-tlv latitude north 33.2507 switch(config)# lldp med location-tlv longitude east 105.2371 switch(config)# lldp med location-tlv altitude meters 300.5 switch(config)# no lldp med location-tlv latitude switch(config)# no lldp med location-tlv longitude switch(config)# no lldp med location-tlv altitude
描述	配置 LLDP-MED 坐标位置-维度：北纬 33.2507 度 配置 LLDP-MED 坐标位置-精度：东经 105.2371 度 配置 LLDP-MED 坐标位置-海拔：330.5 米 取值 LLDP-MED 坐标位置-维度配置。（默认为北纬 0 度） 取消 LLDP-MED 坐标位置-精度配置。（默认为东经 0 度） 取消 LLDP-MED 坐标位置-海拔配置。（默认为海拔 0 米）

命令	switch(config)# lldp med datum nad83-navd88 switch(config)# no lldp med datum
描述	配置 LLDP-MED 坐标位置资料为“NAD80-NAVD88”。 取消 LLDP-MED 坐标位置资料配置，默认为“WGS84”。

命令	switch(config)# lldp med location-tlv civic-addr *XXXX* switch(config)# no lldp med location-tlv civic-addr *XXXX*
描述	配置 LLDP-MED 地址位置。参数很多，不一一列举。 取值 LLDP-MED 坐标位置-地址位置配置。

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp med type end-point switch(config-if)# no lldp med type
描述	配置 LLDP-MED 设备类型为“end-point”。 取消 LLDP-MED 设备类型配置。（默认为“connectivity”）

命令	switch(config)# interface GigabitEthernet 1/1

	switch(config-if)# lldp med transmit-tlv capabilities switch(config-if)# lldp med transmit-tlv location switch(config-if)# lldp med transmit-tlv poe switch(config-if)# no lldp med transmit-tlv capabilities switch(config-if)# no lldp med transmit-tlv location switch(config-if)# no lldp med transmit-tlv poe
描述	开启 LLDP-MED 可选 TLV“能力”。（默认开启） 开启 LLDP-MED 可选 TLV“位置”。（默认开启） 开启 LLDP-MED 可选 TLV“POE”。（默认开启） 关闭 LLDP-MED 可选 TLV“能力”。 关闭 LLDP-MED 可选 TLV“位置”。 关闭 LLDP-MED 可选 TLV“POE”。

命令	switch# show lldp neighbor interface GigabitEthernet 1/1 switch# show lldp neighbor interface * switch# show lldp neighbor
描述	显示接口 1/1 的 LLDP 邻居信息。 显示所有接口的 LLDP 邻居信息。 显示所有 LLDP 邻居信息。

命令	switch# show lldp med remote-device interface GigabitEthernet 1/1 switch# show lldp med remote-device interface * switch# show lldp med remote-device
描述	显示接口 1/1 的 LLDP-MED 邻居信息。 显示所有接口的 LLDP-MED 邻居信息。 显示所有 LLDP-MED 邻居信息。

命令	switch# show lldp statistics interface GigabitEthernet 1/1 switch# show lldp statistics interface * switch# show lldp statistics
描述	显示接口 1/1 的 LLDP 统计信息。 显示所有接口的 LLDP 统计信息。 显示所有的 LLDP 统计信息。

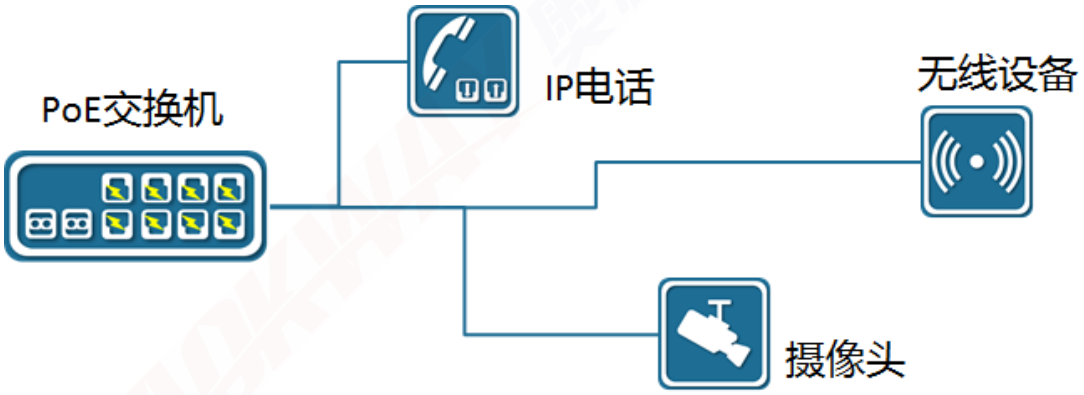
11 以太网供电

只有 IS2503 子系列的交换机支持以太网供电功能，不支持以太网功能的交换机 WEB 管理时以太网供电页面不可见。

11.1 POE 概述

Power over Ethernet，简称 PoE，是一个可以在以太网路中通过双绞线与终端进行数据交互同时，提供直流供电的技术。常用对网络电话、WIFI AP、网络摄影机、集线器、电脑等设备进行供电。按照标准其供电最长距离为 100m。

图表 11-1 POE 供电示意



PSE（Power Sourcing Equipment，供电设备），如上图中 PoE 交换机。PSE 在 PoE 端口的线路上寻找、检测 PD，对 PD 分级，并向其供电。 当检测到 PD 拔出后，PSE 停止供电。PD 是接受 PSE 供电的设备，如上图中 IP 电话、无线设备、摄像头。

PoE 发展经历了两套标准:

IEEE 802.3af(15.4W)是首个 PoE 供电标准，规定了以太网供电标准，是现在 PoE 应用的主流实现标准。它明确规定了远程系统中的电力检测和控制事项，并对路由器、交换机和集线器通过以太网电缆向 IP 电话、安全系统以及无线 LAN 接入点等设备供电的方式进行了规定。

IEEE802.3at(30W)应大功率终端的需求而诞生，在兼容 802.3af 的基础上，提供更大的供电需求，满足新的需求。根据 IEEE 802.3af 规范，供电设备(PSE)单端口可提供的功率不超过 15.4W。而 IEEE 802.3at，它将功率要求高于 15.4W 的设备定义为 Class 4(该级别在 IEEE 802.3af 中有描述，但留作将来使用)，可将功率水平扩展到 30W。

11.2 配置

在【导航栏】下拉菜单中选择：配置->以太网供电，进入配置页面。

图表 11-2 POE 配置页面

以太网供电配置

预留功率模式	○ PD等级 ◉ 静态分配 ○ LLDP-MED
功率管理模式	○ 实际消耗 ◉ 预留功率
电容检测	◉ 禁用 ○ 启用

电源配置

主电源额定功率[W]
280

端口配置

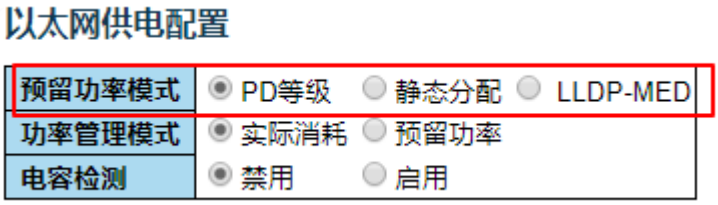
端口	PoE模式	优先级	最大功率 [W]
*	<>	<>	0
1	PoE+	Low	0
2	PoE+	Low	0
3	PoE+	Low	0
4	PoE+	Low	0
5	Disabled	Low	0
6	PoE+	Low	0
7	PoE+	Low	0
8	PoE+	Low	0

保存　复位

11.2.1　预留功率模式

预留功率：预留功率用于确定为端口预留的最大功率，该最大功率设定了端口功率过载的阈值。即当端口的输出功率超过了预留功率，会出现过载，端口 POE 停止供电。

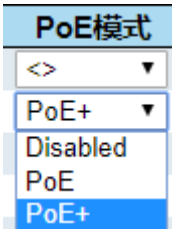
图表 11-3 POE 预留功率模式配置



- PD 等级：根据端口接入的 PD 设备的 Class 来确定预留功率，具体如下：
  - Class 0：　15.4W
  - Class 1：　4W
  - Class 2：　7W
  - Class 3：　15.4W
  - Class 4：　15.4W(for poe)　30W(for poe+)

  需要注意的是：Class4 对应的预留功率跟端口选择的 POE 模式有关，对 poe 模式（AF 标准），class 4 对应 15.4W，对 poe+标准（AT 标准），class 4 对应 30W。若 Poe 模式为 Disable，表示端口关闭 POE 供电。

图表 11-4 POE 端口模式配置



- 静态分配，根据设置的端口最大功率来确定预留功率。所以，当选择静态分配模式时，端口的最大功率必须进行配置。

图表 11-5 POE 端口最大功率配置

- LLDP-MED，PSE 与 PD 通过 LLDP-MED 协商需求功率（即预留功率）。通过 LLDP-MED 协商的方式预留功率比根据 PD 等级或者静态分配预留功率更加精准，但要求 PD 设备必须支持 LLDP-MED。如果 PD 设备不支持 LLDP-MED，则 LLDP-MED 模式跟 PD 等级模式表现一样，即根据 PD 设备的 Class 来确定预留功率。
- 缺省配置：预留功率模式缺省为“PD 等级”。

11.2.2 功率管理模式

功率管理的目的在于协调端口间的供电关系。电源的额定功率作为稀缺资源，当额定功率不足时，需要决策哪些端口下电，这就是功率管理的目的。

显然，功率管理有两个关键步骤：

- 端口功率计算：功率管理模式就用于确定端口的功率如何计算，如果使用预留功率模式，则使用分配功率计算，如果使用实际消耗模式，则用使用功率计算。

图表 11-6 POE 功率管理模式配置

以太网供电配置

预留功率模式	PD等级 静态分配 LLDP-MED
功率管理模式	实际消耗 预留功率
电容检测	禁用 启用

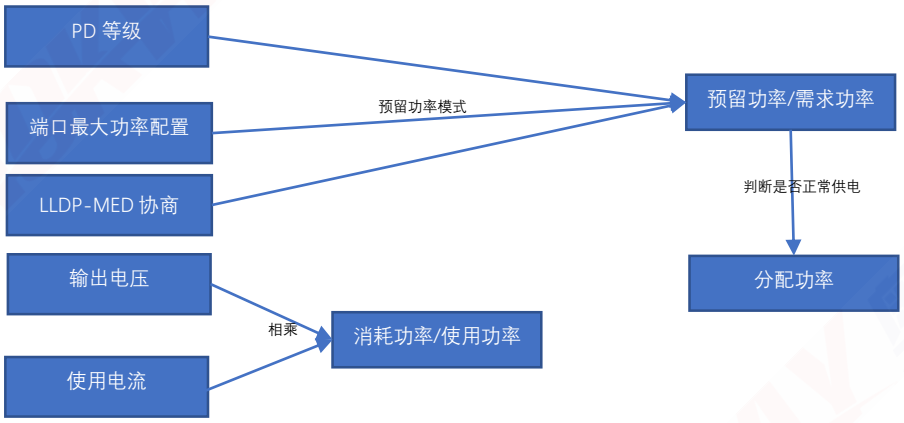
- 实际消耗：根据端口的实际消耗（使用功率）来计算系统功率是否足够。
- 预留功率：根据端口的分配功率来计算系统功率是否足够（分配功率与预留功率模式相关）。
- 缺省配置：功率管理模式缺省为“实际消耗”。

在 POE 模块中，涉及到三种功率：需求功率，分配功率，使用功率。

结合之前所述，几种功率的计算如下：

1，需求功率，即预留功率。
2，分配功率：如果端口未供电，端口的分配功率为 0，如果端口供电，其分配功率为端口的预留功率。
3，使用功率：即消耗功率，根据电压和使用电流计算得到，表明了 PD 实际消耗的功率。

图表 11-7 POE 各种功率计算示意



- 判断和决策：

根据不同的功率管理模式（实际消耗模式根据使用功率来计算，预留功率模式根据分配功率来计算）判断系统功率是否足够，根据如下电源配置判断：

图表 11-8 电源额定功率配置

电源配置

主电源额定功率[W]
280

若系统功率不足，则对某个/些端口断电。选择哪个/些端口，依赖于端口优先级配置。

图表 11-9 POE 端口优先级配置

端口配置

端口	PoE模式	优先级	最大功率 [W]
*	<>	<>	35
1	PoE+	Low	0
2	PoE+	Low	0
3	PoE+	High	0
4	PoE+	Critical	0
5	PoE+	Low	0
6	PoE+	Low	0
7	PoE+	Low	0
8	PoE+	Low	0

需要注意的是：当预留功率模式选择静态分配，功率管理模式选择预留功率时，不能配置优先级，因为，这种情况下，分配功率等于端口配置的最大功率，而最大功率的配置会直接判断是否超过电源额定功率，只要配置合法，就一定不会出现功率不足，所以，实际上无需进行功率管理下电。

图表 11-10 POE 静态模式说明

以太网供电配置

预留功率模式	PD等级	静态分配	LLDP-MED
功率管理模式	实际消耗	预留功率	
电容检测	禁用	启用	

电源配置

主电源额定功率[W]
280

端口配置

端口	PoE模式	优先级	最大功率 [W]
*	<>	<>	0
1	PoE+	Low	0
2	PoE+	Low	0
3	PoE+	Low	0
4	PoE+	Low	0
5	Disabled	Low	0
6	PoE+	Low	0
7	PoE+	Low	0
8	PoE+	Low	0

保存 复位

11.2.3 组合方式

模式	功率管理模式	预留功率模式	需求功率/预留功率	分配功率
自动模式/Class 模式	预留功率	PD 等级	根据 PD 等级确定。	等于需求功率。
静态模式	预留功率	静态分配	根据端口配置的最大功率确定。	等于需求功率。
LLDP 模式	预留功率	LLDP-MED	根据 LLDP-MED 协商（协商失败，根据 PD 等级确定）	等于需求功率。
消耗模式	实际消耗	PD 等级	根据 PD 等级确定。	等于使用功率
		静态分配	根据端口配置的最大功率确定。	等于使用功率
		LLDP-MED	根据 LLDP-MED 协商（协商失败，根据 PD 等级确定）	等于使用功率

注意：在消耗模式下，预留功率模式的选择与功率管理无关（因为分配功率等于使用功率），预留功率模式的选择仅仅用于确定端口功率阈值，判断端口是否出现功率过载。

缺省时，使用消耗模式。

11.3 显示

在【导航栏】下拉菜单中选择：监控->以太网供电，进入显示页面。

以太网供电状态

本地端口	PD等级	需求功率	分配功率	使用功率	使用电流	优先级	端口状态
1	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		107.8 [W]	0 [W]	0 [W]	0 [mA]		

需求功率，分配功率，使用功率参见“功率管理模式”章节说明。

11.4 CLI 参考命令

命令	switch(config)# poe supply 200 switch(config)# no poe supply
描述	配置 POE 电源额定功率； 恢复 POE 电源额定功率为默认值。

命令	switch(config)# poe management mode allocation-consumption switch(config)# poe management mode allocation-reserved-power switch(config)# poe management mode class-consumption switch(config)# poe management mode class-reserved-power switch(config)# poe management mode lldp-consumption switch(config)# poe management mode lldp-reserved-power switch(config)# no poe management
描述	配置 POE 预留功率模式和功率管理模式组合方式。 恢复 POE 预留功率模式和功率管理模式为缺省值（class-consumption）。

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# poe mode standard switch(config-if)# poe mode plus switch(config-if)# no poe mode
描述	配置接口 1/1 的 POE 模式为 POE（802.3AF）。 配置接口 1/1 的 POE 模式为 POE+(802.3AT)。 关闭接口 1/1 的 POE 供电。 默认为 POE+模式。

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# poe power limit 27.8 switch(config-if)# no poe power limit
描述	配置接口 1/1 的 POE 最大功率为 27.8W。 删除接口 1/1 的 POE 最大功率配置，默认为 0W。

命令	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# poe priority critical switch(config-if)# poe priority high switch(config-if)# poe priority low switch(config-if)# no poe priority
描述	配置接口 1/1 的 POE 优先级。

	配置接口 1/1 的 POE 优先级为默认值，默认为 low。

命令	switch# show poe interface GigabitEthernet 1/1 switch# show poe interface * switch# show poe
描述	显示接口 1/1 的 POE 信息。 显示所有接口的 POE 信息。 显示所有的 POE 信息。

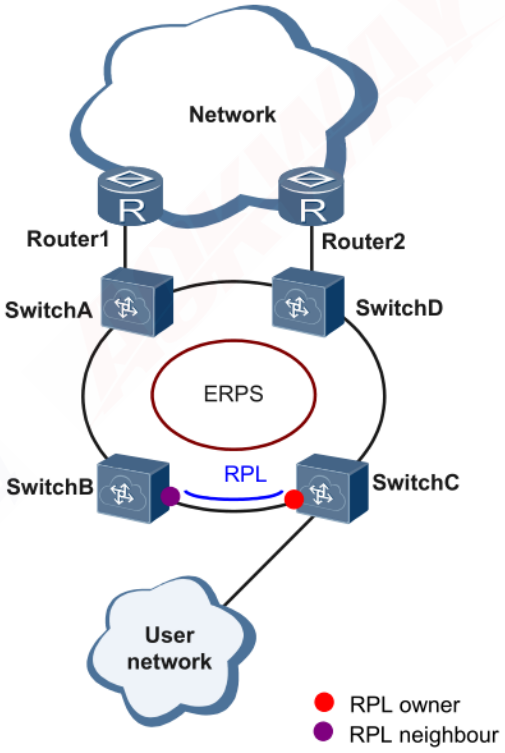
12 ERPS

12.1 ERPS 功能概述

ERPS (Ethernet Ring Protection Switching，以太环网保护切换协议) 为 ITU 开发的一种环网保护协议，也称 G.8032。它是一个专门应用于以太环网的链路层协议。它在以太环网完整时能够防止数据环路引起的广播风暴，而当以太环网上一条链路断开时能迅速恢复环网上各个节点之间的通信。

目前，解决二层网络环路问题的技术还有 STP。STP 应用比较成熟，但其收敛的时间比较长（秒级）。ERPS 是专门应用于以太环网的链路层协议，二层收敛性能达 50ms 以内，具有比 STP 更快的收敛速度。

图表 12-1 EPS 典型组网



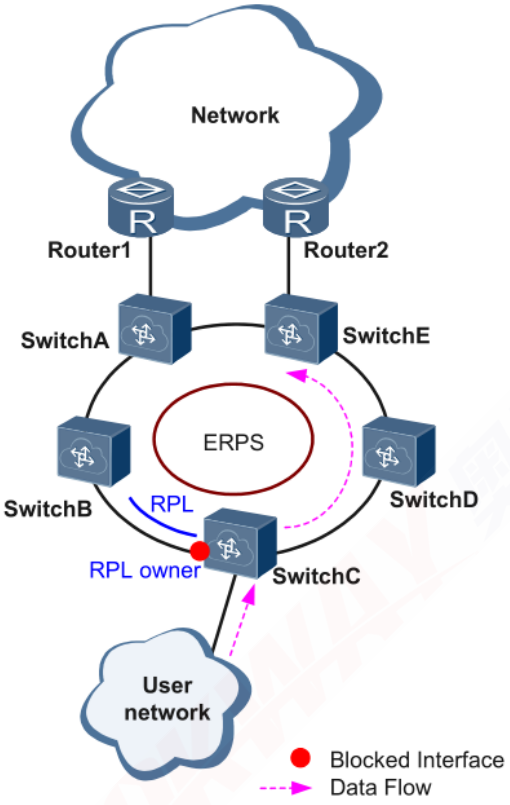
12.2 ERPS 原理简介

ERPS 是一种专用于以太网链路层的标准环网协议，以 ERPS 环为基本单位。每台二层交换设备上只能有两个端口加入同一个 ERPS 环。在 ERPS 环中，为了防止出现环路，可以启动破除环路机制，阻塞 RPL owner 端口，消除环路。当环网发生链路故障时，运行 ERPS 协议的设备可以迅速地放开阻塞端口，进行链路保护倒换，恢复环网上各节点间链路通信。本节主要以示例的形式按照链路正常-链路故障-链路恢复的过程（包括保护倒换操作），介绍基本的单环组网下 ERPS 的实现原理。

12.2.1 链路正常

由 Switch A ~ Switch E 组成的环路上各设备通信正常。

图表 12-2 ERPS 链路正常场景

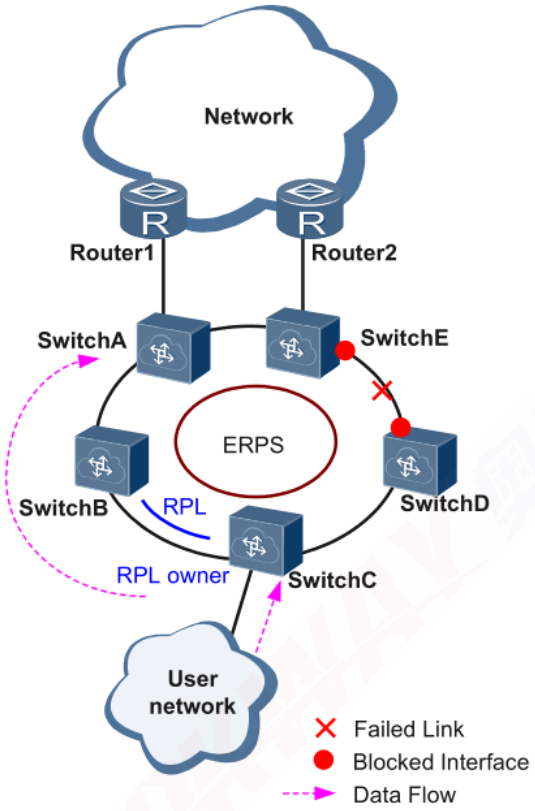


为防止环路产生，ERPS 首先会阻塞 RPL owner 端口，如果配置了 RPL neighbor 端口，该端口同样会被阻塞，其他端口可以正常转发业务流量。

12.2.2 链路故障

如下图所示，当 Switch D 和 Switch E 之间的链路发生故障时，ERPS 协议启动保护倒换机制，将故障链路的两端端口阻塞，然后放开 RPL owner 端口，这两个端口重新恢复用户流量的接收和发送，从而保证了流量不中断。

图表 12-3 ERPS 链路故障场景



12.2.3 链路恢复

链路恢复正常后，默认情况下，ERPS 环配置的是回切模式，RPL owner 端口所在设备会重新阻塞 RPL 链路上的流量，原故障链路重新被用来完成用户流量的传送。

12.2.4 ERPS 环种类

单环：

网络拓扑中只有一个环；有且仅有一个 RPL Owner；有且仅有一条 RPL 链路；所有节点需具有相同的 RAPS 管理 Vlan

- 环网中所有设备都需要支持 ERPS 功能。
- 环网中的设备之间的链路必须直连，不能有中间设备。

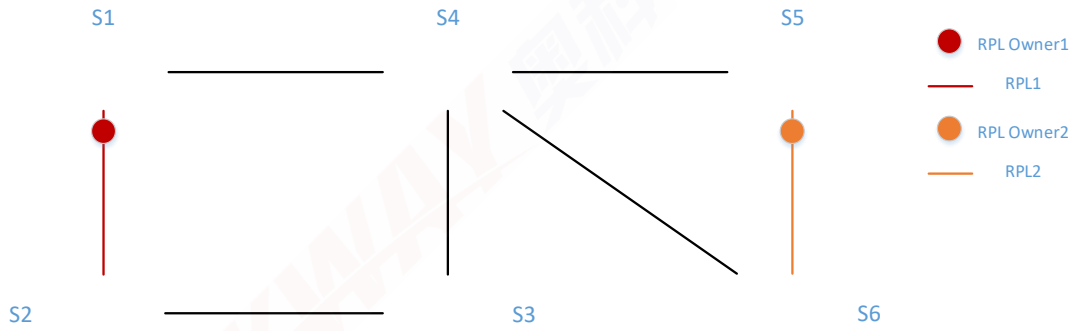
图表 12-4 ERPS 单环模型

相切环：

网络拓扑中两个或两个以上共用一台设备的环网需要保护的应用场景。以为下图为例，网络拓扑中的两个环共用一台设备；每个环有且仅有一个阻断点，每个环有且仅有一条 RPL 链路；不同环需具有不同的 RAPS 管理 Vlan。

- 环网中所有设备都需要支持 ERPS 功能。
- 环网中的设备之间的链路必须直连，不能有中间设备。

图表 12-5 ERPS 相切环模型

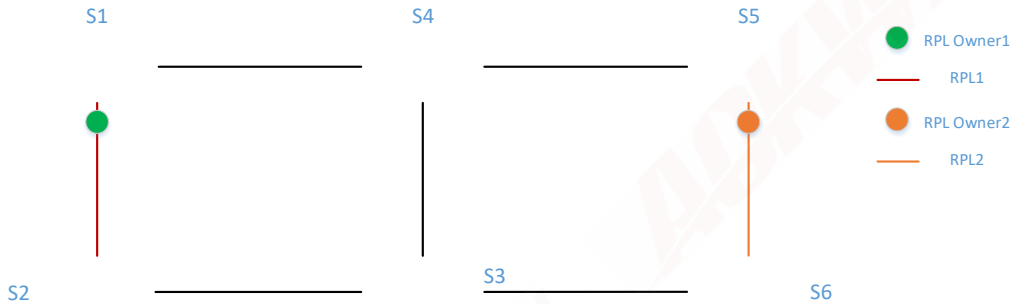


相交环：

网络拓扑中有两个或两个以上的环共用一条链路（相交的两个节点间必须直连，不能再有其它节点）。以**错误!未找到引用源。**为例，网络拓扑中有 2 个环；每个环有且仅有一个 RPL owner 节点，每个环有且仅有一条 RPL 链路；不同环需具有不同的 RAPS 管理 Vlan。

- 环网中所有设备都需要支持 ERPS 功能。
- 环网中的设备之间的链路必须直连，不能有中间设备。

图表 12-6 ERPS 相交环模型



12.3 ERPS 配置简介

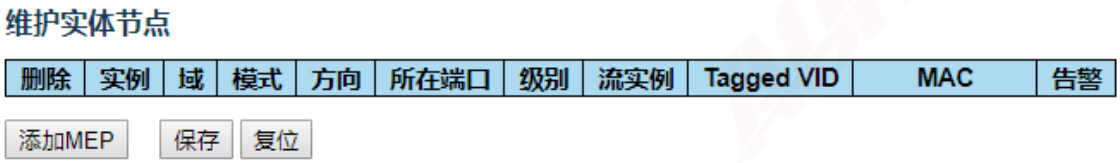
注意

- 生成树协议和 ERPS 协议不能同时开启。

12.3.1 MEP 配置界面

点击导航栏中：配置->MEP，进入 MEP 配置界面。

图表 12-7 MEP 配置 1



12.3.2 添加 MEP 节点

点击 MEP 配置界面中的【添加 MEP】按钮，添加 MEP 节点，配置完成后点击【保存】按钮完成 MEP 节点添加。

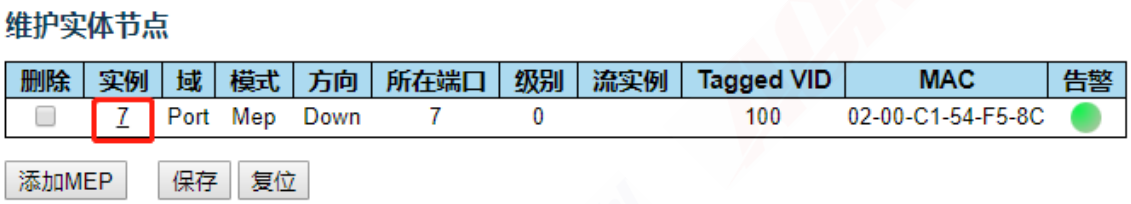
图表 12-8 MEP 配置 2

配置项	说明
实例	MEP 实例编号，1-100 的数字。 MEP 节点实例必须唯一，为了映射简单，可以采用所在端口号直接作为 MEP 实例。
域	Port：基于端口。 VLAN：基于 VLAN。 ERPS 使用 Port 域。
模式	MEP：终端模式。 MIP：中间模式。 ERPS 使用 MEP 模式。
方向	Down：处理准入方向的流量。 Up：处理准出方向的流量。 ERPS 使用 Down 方向。
所在端口	物理端口号。
级别	实例优先级。 ERPS 使用默认 0 即可。
流实例	流实例 ID，仅在 VLAN 域中有效。 ERPS 无需配置。
Tagged VID	VLAN 标签。 ERPS 使用 RAPS 管理报文的 VLAN。

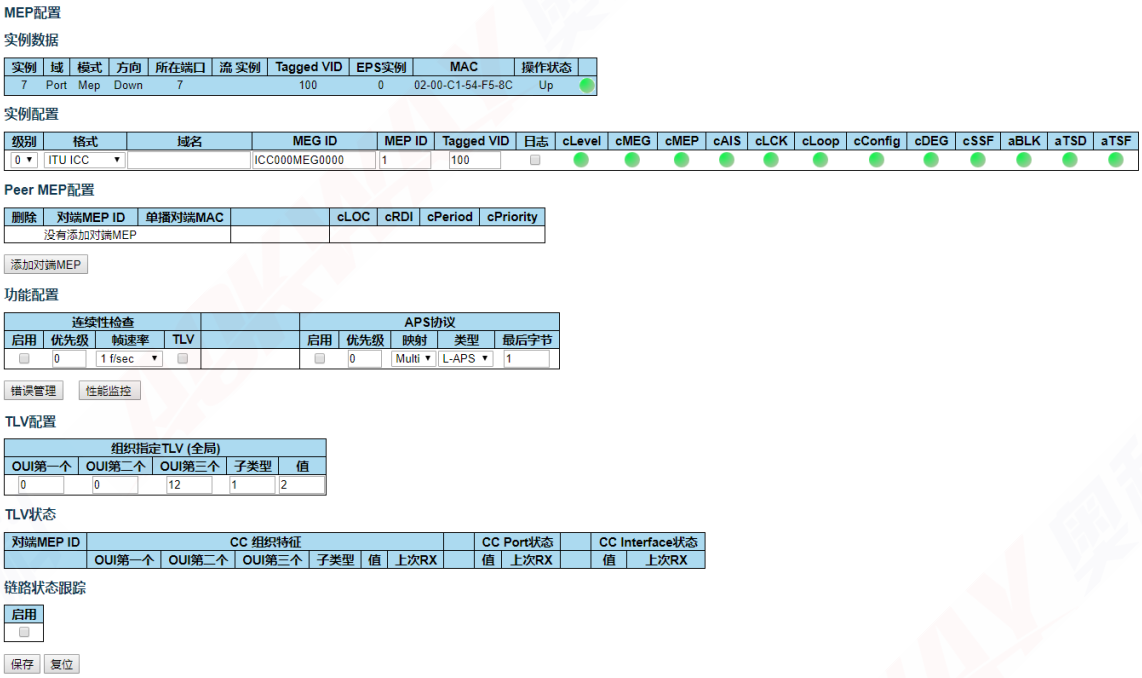
12.3.3 使能 MEP 的 RAPS 功能

点击配置的 MEP 节点实例，进入实例配置页面，启用 APS 协议，点击保存完成配置。

图表 12-9 MEP 实例进入



图表 12-10 MEP 实例配置



配置项	说明
优先级	RAPS 优先级， 0-7 的数字。 ERPS 使用默认 0 即可。
映射	Uni：单播地址，前提是需要知道对端 MEP。 Multi：多播地址。 ERPS 使用标准多播地址。
类型	R-APS：ERPS 报文。 L-APS：ELPS 报文。 ERPS 使用 R-APS 类型。
最后字节	MAC 地址最后一字节的内容。 ERPS 使用环 ID 作为 MAC 的最后一个字节，环 1 则为 1.

12.3.4 ERPS 配置界面

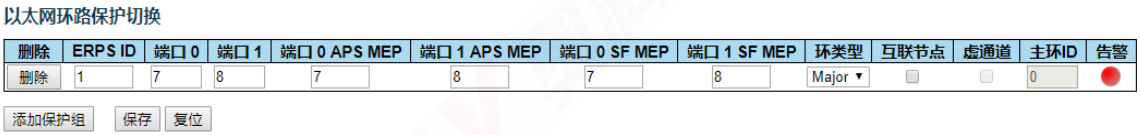
点击导航栏中：配置->ERPS，进入 ERPS 管理界面。

图表 12-11 ERPS 配置 1

12.3.5 添加 ERPS 保护组

在 ERPS 配置页面中点击【添加保护组】按钮，在出现的输入框中输入保护组信息，点击【保存】按钮完成配置。

图表 12-12 ERPS 配置 2

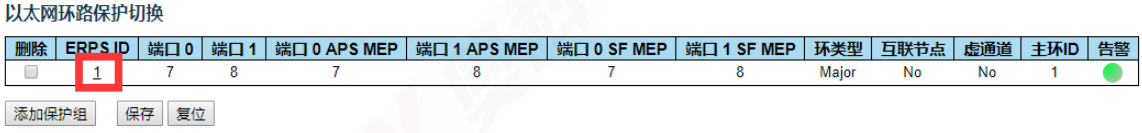


配置项	说明
ERPS ID	环编号。在同一个环中的不同交换机需要配置相同环编号。环编号应该与 MEP 节点的 RAPS MAC 地址最后一字节相同。
端口 0	又称 Port0，左接口，东接口。
端口 1	又称 Port1，右接口，西接口。
端口 0 APS MEP	端口 0 协议报文关联的 MEP 节点。
端口 1 APS MEP	端口 1 协议报文关联的 MEP 节点。
端口 0 SF MEP	端口 0 故障检测关联的 MEP 节点。
端口 1 SF MEP	端口 1 故障检测关联的 MEP 节点。
环类型	Major：主环 Sub：子环
互联节点	当前节点是否为互联节点，仅多环相交节点需要设置。
虚通道	是否采用虚通道模式，当前不支持虚通道模式。
主环 ID	仅环类型为子环时可配置。

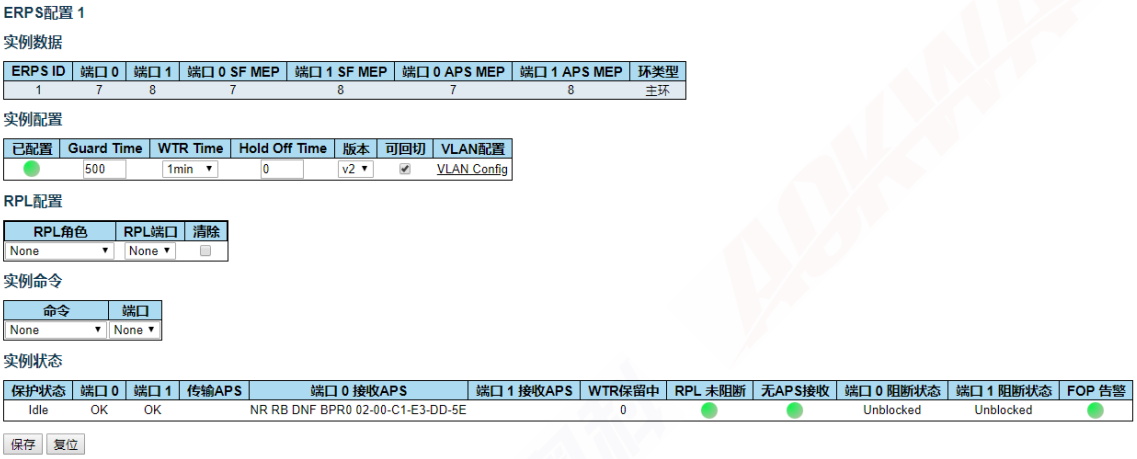
12.3.6 ERPS 保护组参数配置

在 ERPS 配置页面中点击具体 ERPS ID，进入保护组参数配置页面，修改保护组参数，点击【保存】按钮完成配置。

图表 12-13 ERPS 保护组进入



图表 12-14 ERPS 保护组配置

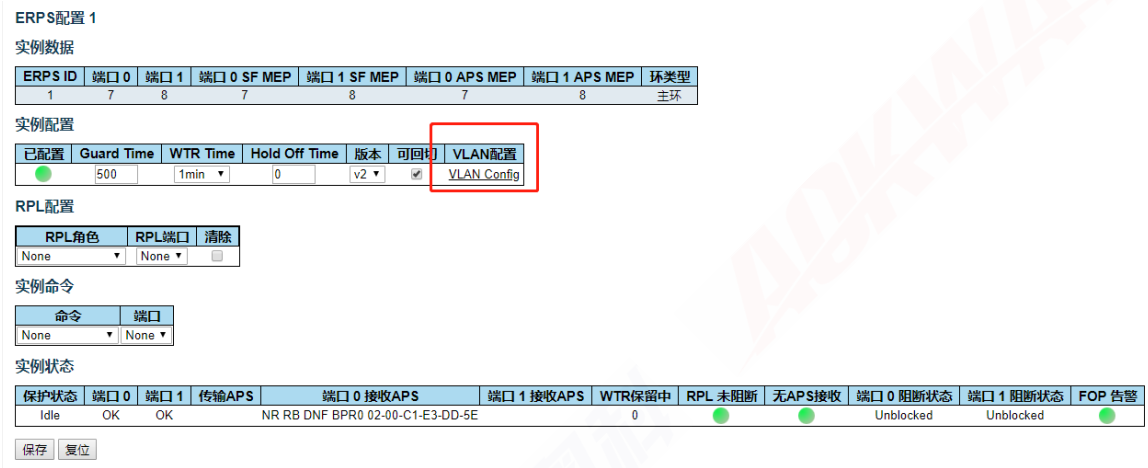


配置项	说明
Guard Time	协议防护时间，默认 500 毫秒。
WTR Time	协议回切时间，默认为 1 分钟。
Hold Off Time	协议延迟时间，默认 0 秒。
版本	协议版本号，默认 v2.
可回切	是否允许环回切，默认为允许。
VLAN 配置	保护 VLAN 的配置，通常需要将所有 VLAN 加入为保护 VLAN，未加入保护的 VLAN 可能出现环路故障。
RPL 角色	None：非 RPL 节点。 RPL_Owner：Owner 节点。 RPL_Neighbour：Neighbour 节点。
RPL 端口	None：无 RPL 端口。 Port0：Port0 端口，又称东接口或左接口。 Port1：Port1 端口，又称西接口或右接口。
清除	勾选表示执行协议故障清除/回切动作。
命令	None：无。 Manual Switch：人为切换指令。 Force Switch：强制切换指令。 Clear：清除命令状态。
端口	None：无 Port0/Port1：指令生效的端口。

12.3.7 ERPS 保护组 VLAN 配置

在 ERPS 保护组配置页面中点击 VLAN Config，进入 VLAN 配置页面，修改 VLAN 配置，点击【保存】按钮完成配置。

图表 12-15 ERPS 保护组 VLAN 配置进入



图表 12-16 ERPS 保护组 VLAN 配置

配置项	说明
删除	下次保存时将删除指定的配置表。
VLAN ID	保护组 VLAN ID。

12.3.8 CLI 参考命令

命令	switch(config)# mep 7 down domain port level 0 interface GigabitEthernet 1/7 switch(config)# no mep 7 switch(config)# mep 7 vid 100 switch(config)# mep 7 aps 0 raps octet 1 switch(config)# no mep 7 aps
描述	配置 MEP 创建实例； 配置 MEP 删除实例； 配置 MEP 实例 Tagged VID； 配置 MEP 实例开启 RAPS，配置最后字节； 配置 MEP 实例关闭 RAPS；

命令	switch(config)# erps 1 major port0 interface GigabitEthernet 1/7 port1 interface GigabitEthernet 1/8 switch(config)# no erps 1

	switch(config)# erps 1 mep port0 sf 7 aps 7 port1 sf 8 aps 8 switch(config)# erps 1 rpl owner port0 switch(config)# no erps 1 rpl switch(config)#erps 1 vlan 1,2,3,100
描述	配置 ERPS 保护组创建并设置环类型以及端口 0、端口 1； 配置 ERPS 保护组删除； 配置 ERPS 保护组端口 0、端口 1 的 SF、APS 所关联 MEP； 配置 ERPS 保护组 RPL 角色以及对应端口； 配置 ERPS 保护组删除 RPL 角色； 配置 ERPS 保护组 VLAN 配置；

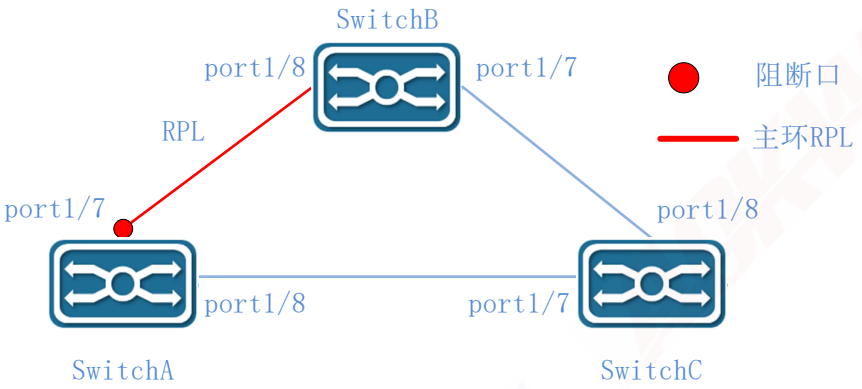
命令	switch# show mep 7 detail switch# show erps 1 detail switch# show erps 1 statistics
描述	打印 MEP 节点状态； 打印 ERPS 保护组状态； 打印 ERPS 保护组报文统计；

12.4 单环配置举例

12.4.1 案例需求

3 台交换机组环网，如下图所示，配置默认阻断口为 SwitchA 的 port1/9 口，数据 VLAN 为 1，2，3，发生故障时可以及时恢复链路确保网络可用。

图表 12-17 ERPS 单环案例



12.4.2 配置规划

在本例中，把 SwitchA、SwitchB、SwitchC 组成的环定义编号为“1”，阻断口为 SwitchA 的“port1/7”，RAPS 管理 VLAN 为“100”，具体参数如下所示。

参数 / 设备	环编号	RAPS VLAN	Owner 接口	Neighbor 接口	互联节点	关联实例

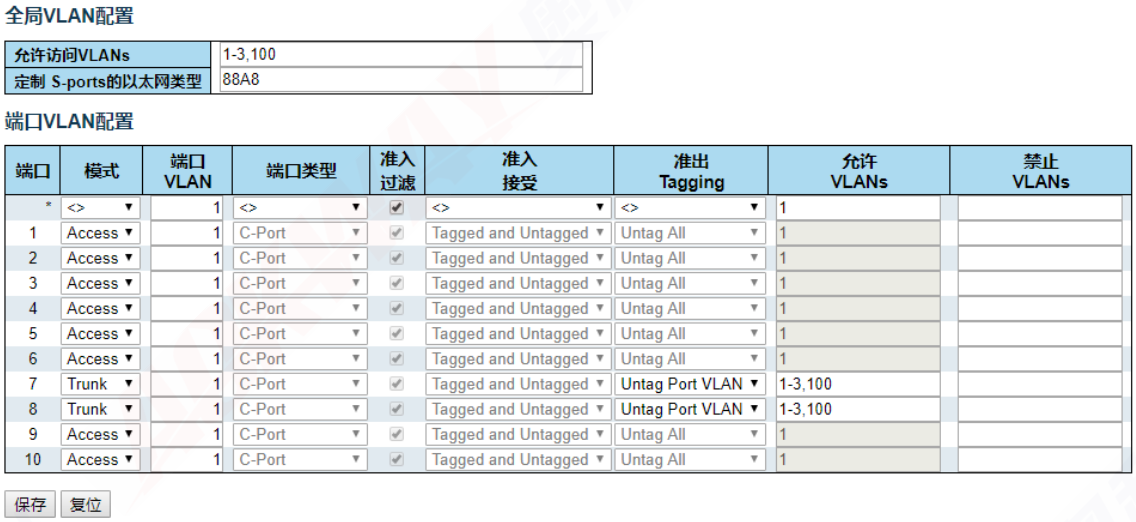
SwitchA	1	100	port1/7	None	\	\
SwitchB	1	100	None	port1/8	\	\
SwitchC	1	100	None	None	\	\

12.4.3 配置交换机 SwitchA

步骤 1：VLAN 和端口的配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-18 单环案例 SwitchA VLAN 配置



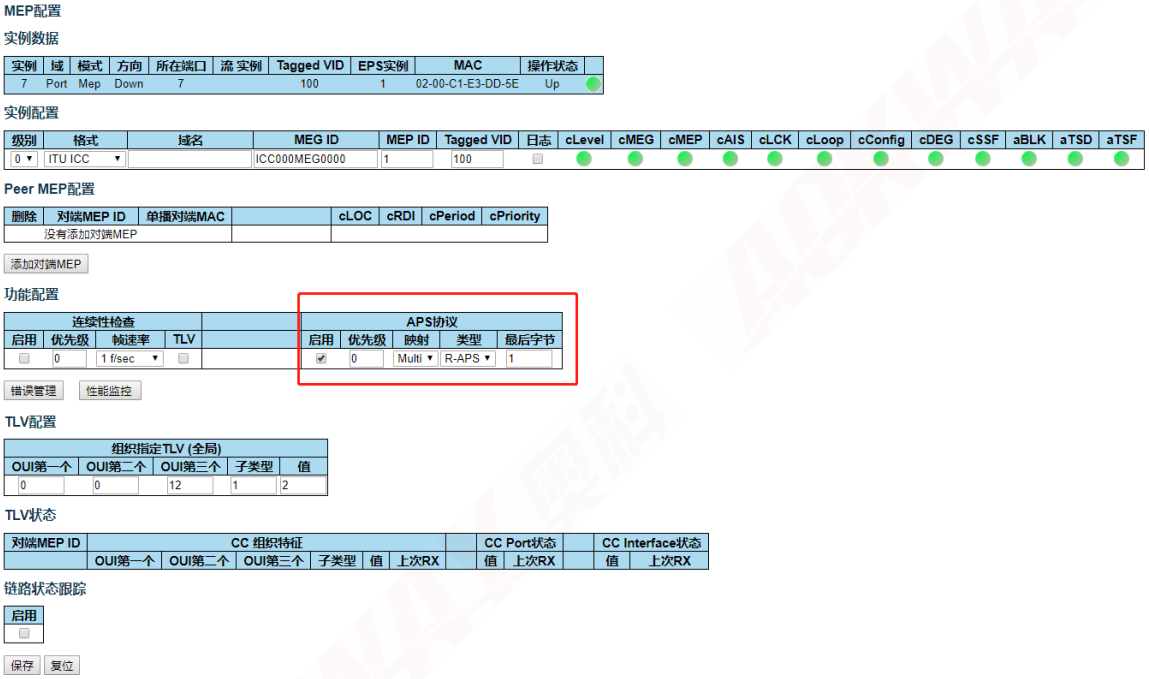
步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 100。

图表 12-19 单环案例 SwitchA MEP 配置 1

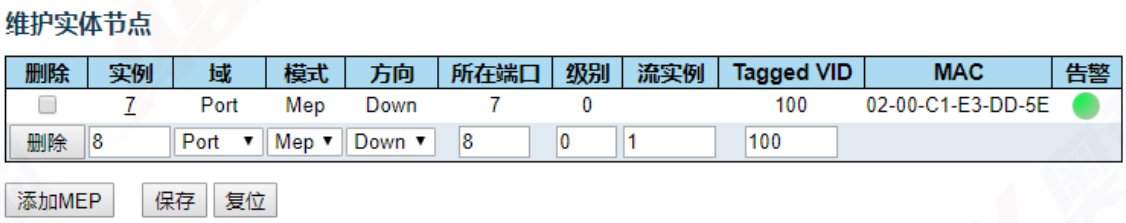
2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能。

图表 12-20 单环案例 SwitchA MEP 配置 2

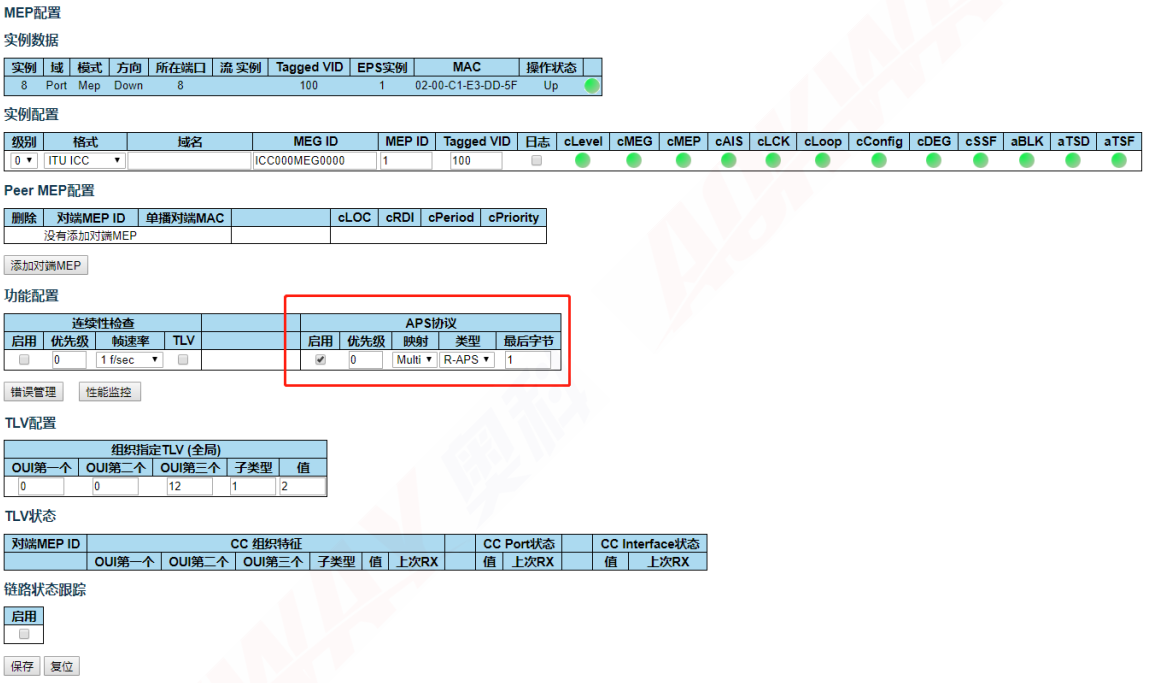


3) 同理添加端口 8 为 MEP 8，Tagged VID 为 100，进入实例数据配置中使能 RAPS 功能。

图表 12-21 单环案例 SwitchA MEP 配置 3



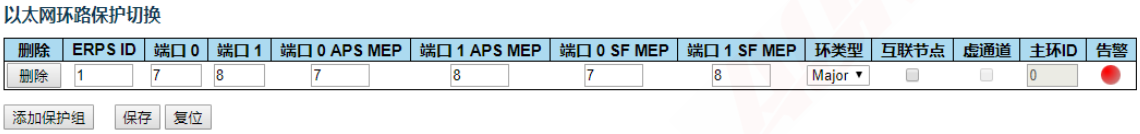
图表 12-22 单环案例 SwitchA MEP 配置 4



步骤 3：创建和配置 ERPS 保护组。

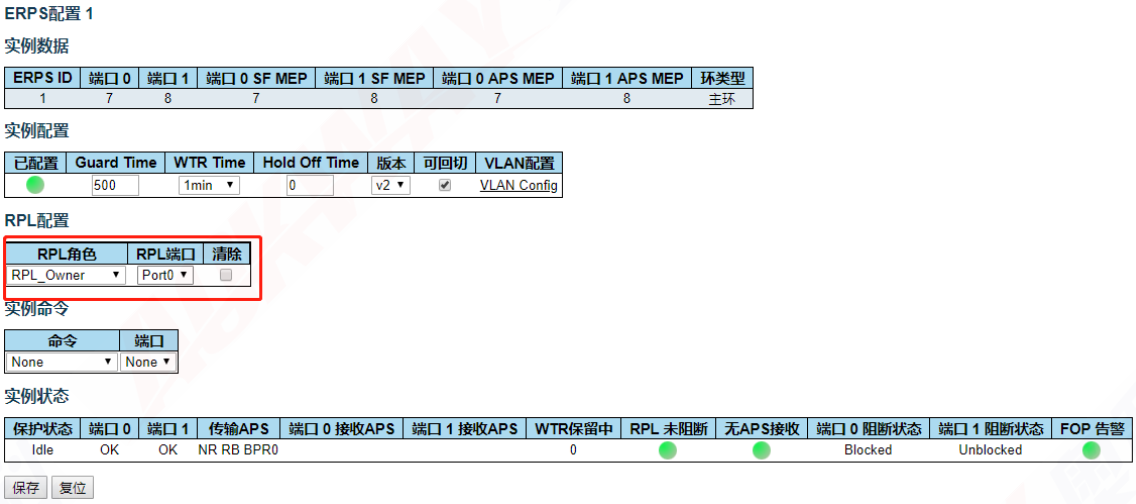
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1。

图表 12-23 单环案例 SwitchA ERPS 配置 1



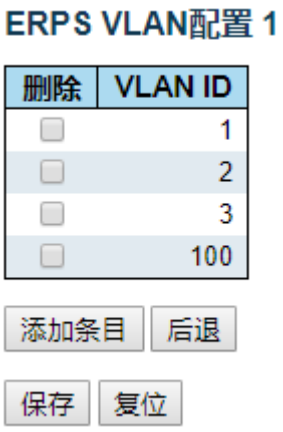
点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面。按照规划配置把 Port0 设置为 RPL Owner 角色。

图表 12-24 单环案例 SwitchA ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-25 单环案例 SwitchA ERPS 配置 3



步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.4.4 配置交换机 SwitchB

步骤 1：VLAN 和端口的配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-26 单环案例 SwitchB VLAN 配置

全局VLAN配置

允许访问VLANs	1-3,100
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 100。

图表 12-27 单环案例 SwitchB MEP 配置 1

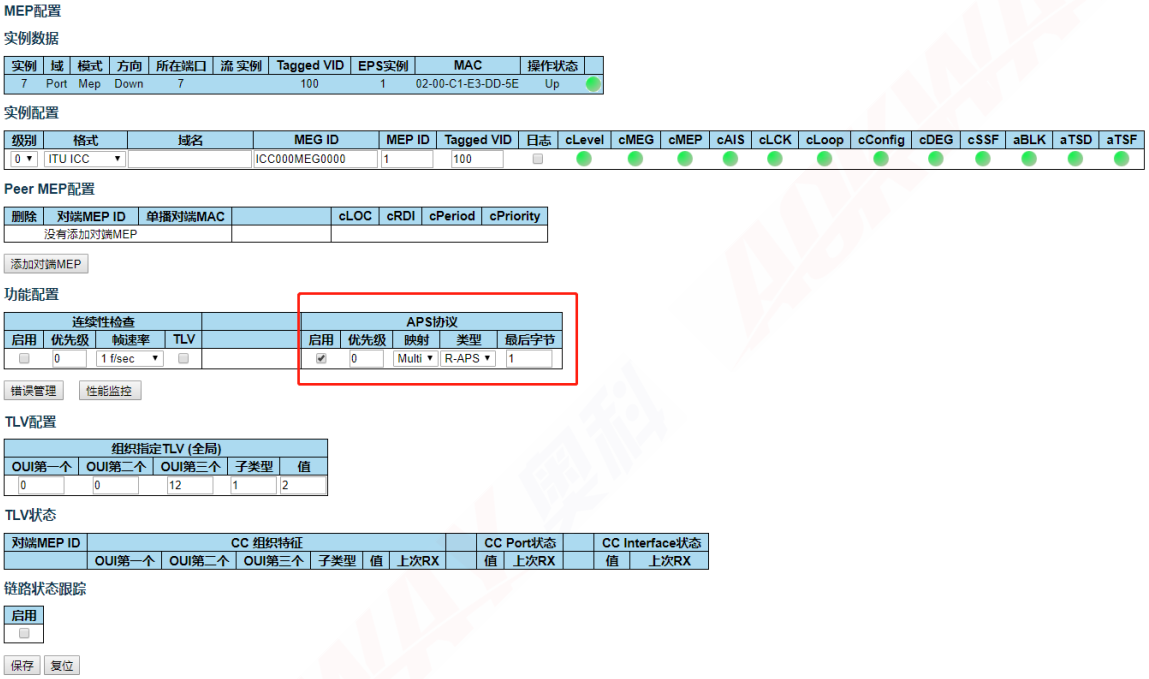
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	100		

添加MEP 保存 复位

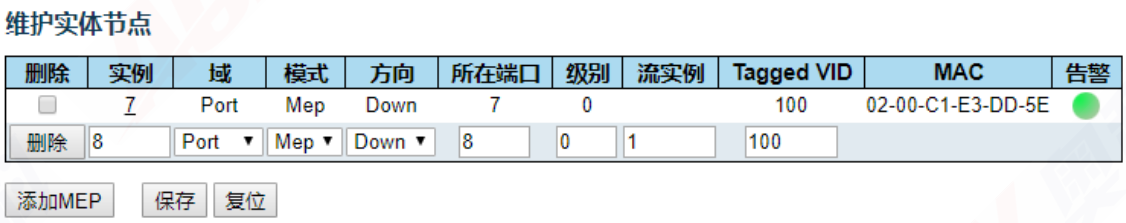
2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能。

图表 12-28 单环案例 SwitchB MEP 配置 2

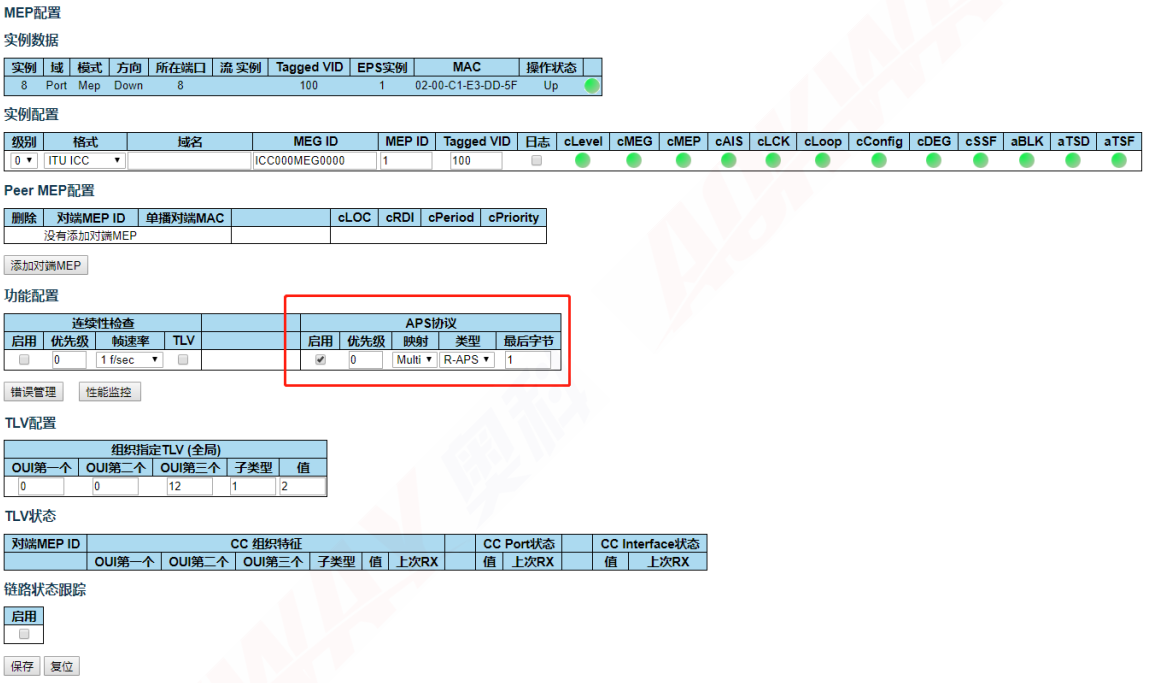


3) 同理添加端口 8 为 MEP 8，Tagged VID 为 100，进入实例数据配置中使能 RAPS 功能。

图表 12-29 单环案例 SwitchB MEP 配置 3



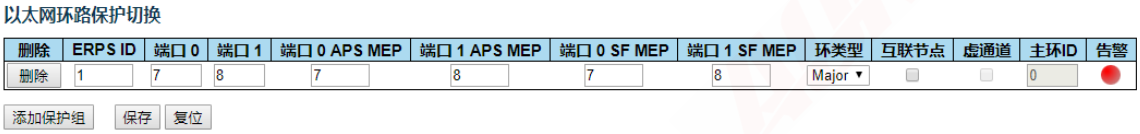
图表 12-30 单环案例 SwitchB MEP 配置 4



步骤 3：创建和配置 ERPS 保护组。

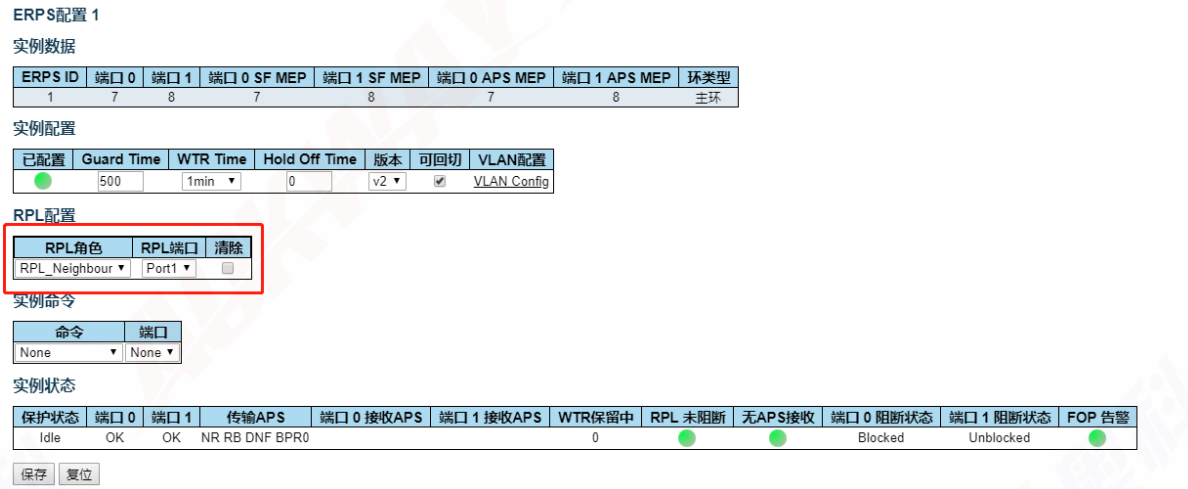
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1。

图表 12-31 单环案例 SwitchB ERPS 配置 1



点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置把 Port1 设置为 RPL Neighbour 角色。

图表 12-32 单环案例 SwitchB ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-33 单环案例 SwitchB ERPS 配置 3

步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.4.5 配置交换机 SwitchC

步骤 1：VLAN 和端口的配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-34 单环案例 SwitchC VLAN 配置

全局VLAN配置

允许访问VLANs	1-3,100
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存　复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 100。

图表 12-35 单环案例 SwitchC MEP 配置 1

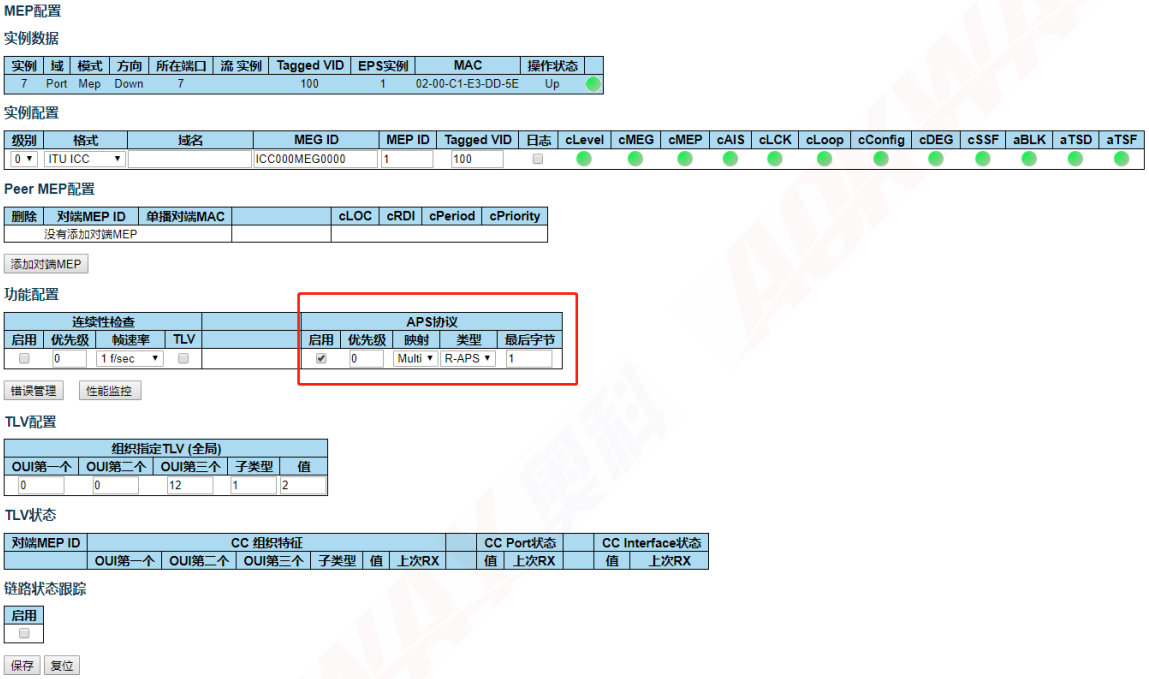
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	100		

添加MEP　保存　复位

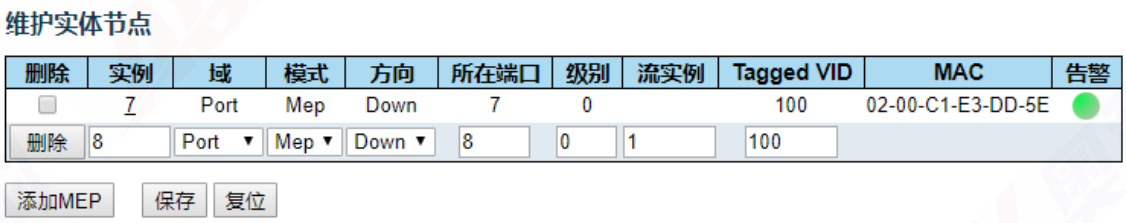
2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能。

图表 12-36 单环案例 SwitchC MEP 配置 2

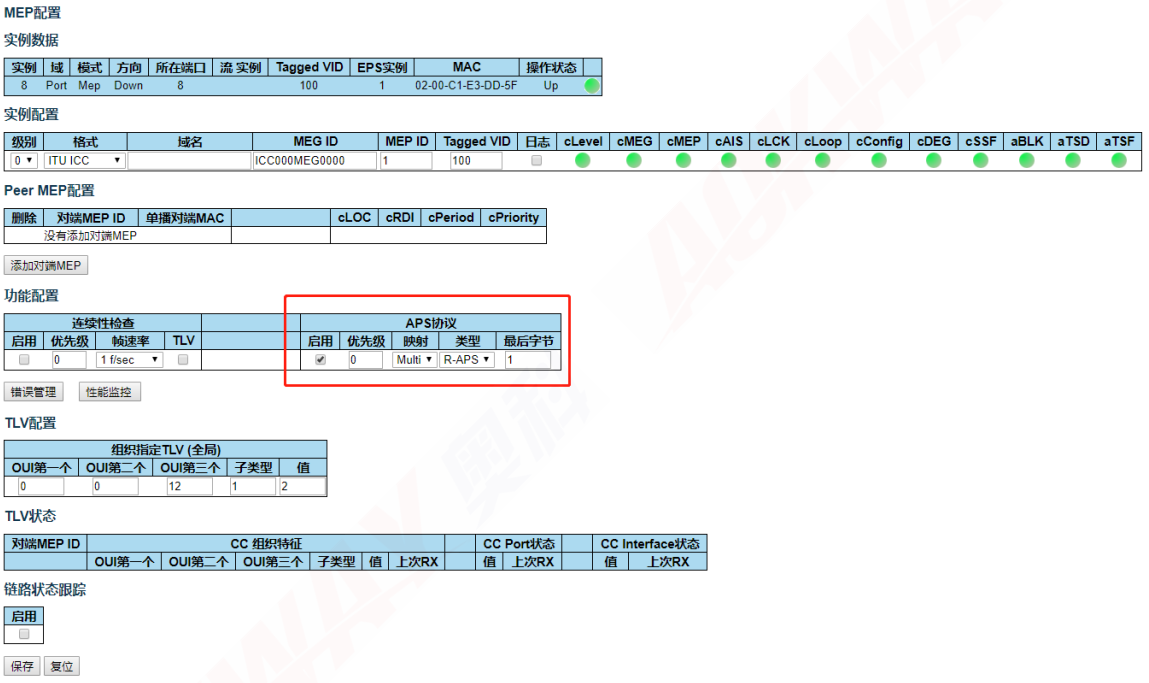


3) 同理添加端口 8 为 MEP 8，Tagged VID 为 100，进入实例数据配置中使能 RAPS 功能。

图表 12-37 单环案例 SwitchC MEP 配置 3



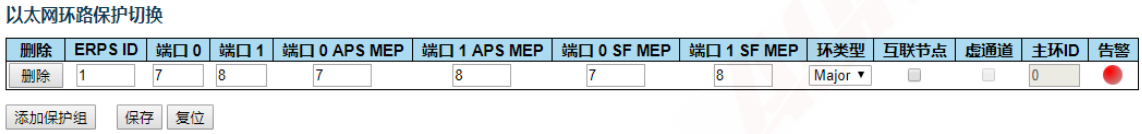
图表 12-38 单环案例 SwitchC MEP 配置 4



步骤 3：创建和配置 ERPS 保护组。

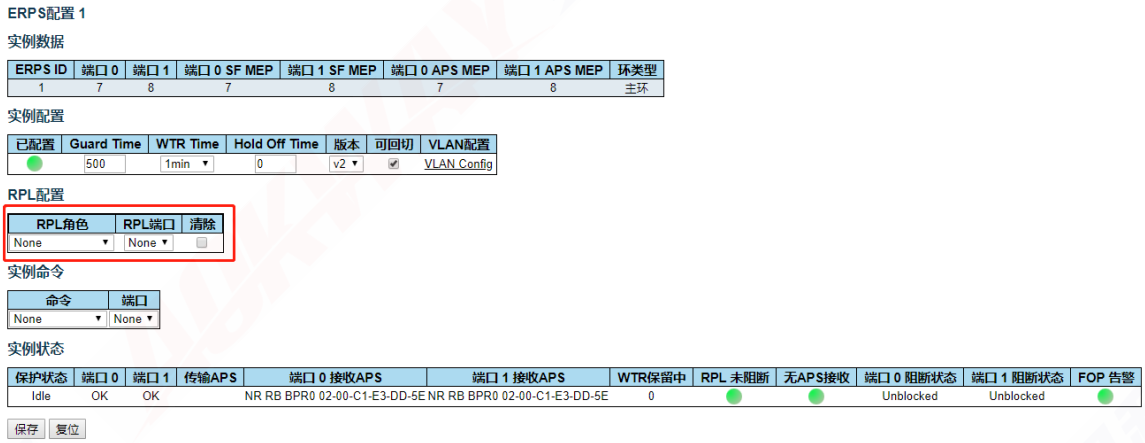
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1。

图表 12-39 单环案例 SwitchC ERPS 配置 1



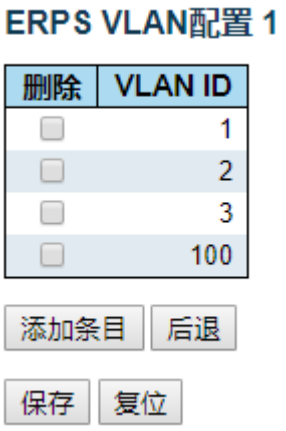
点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置无需设置 RPL 角色。

图表 12-40 单环案例 SwitchC ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-41 单环案例 SwitchC ERPS 配置 3



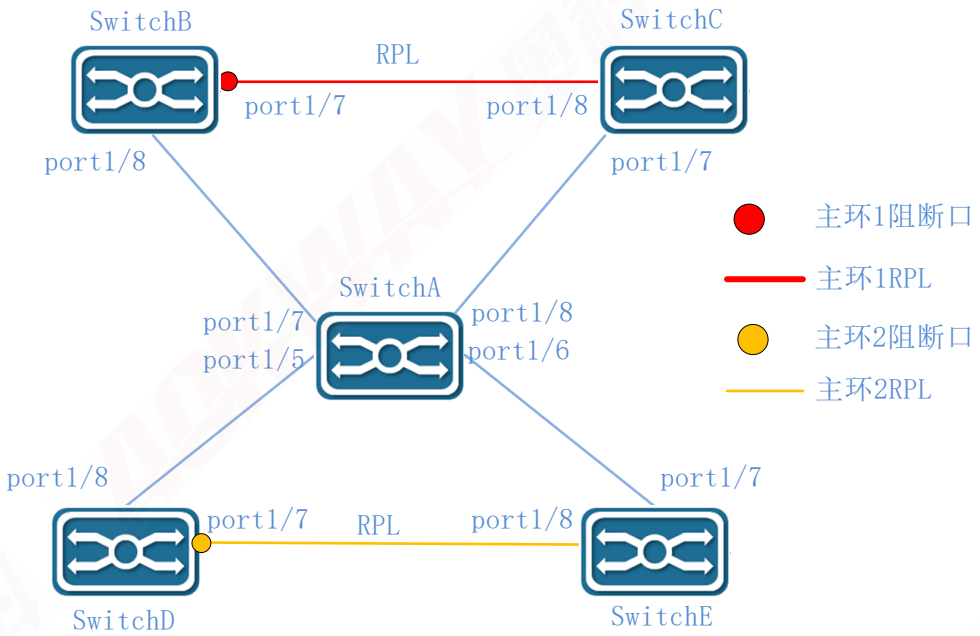
步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.5 相切环配置举例

12.5.1 案例需求

拓扑图如下，SwitchA 位于中心机房，可以被管理员实时监督和维护，具备较高可靠性；SwitchB-E 分布在各地部署点，为了提高组网的可靠性，避免出现单链路外连的单点故障风险，同时避免双链路外连单机可能出现的单机故障风险，采用双链路外连组成环网的方式。数据 VLAN 分别为 1、2、3，要求每个环网出现单点故障时均能够快速收敛，避免用户网络中断。

图表 12-42 相切环案例



12.5.2 配置规划

相切环与单环的配置类似，相当于配置 2 个独立的主环。

在本例中，把 SwitchA、SwitchB、SwitchC 组成的环定义编号为“1”，阻断口为 SwitchB 的“port1/7”，RAPS 管理 VLAN 为“100”，SwitchA、SwitchD、SwitchE 组成的环编号为“2”，阻断口为 SwitchD 的“port1/7”，RAPS 管理 VLAN 为“101”，具体参数如下所示。

参数 / 设备	环编号	RAPS VLAN	Owner 接口	Neighbor 接口	互联节点	关联主环
SwitchA	1	100	None	None	\	\
	2	101	None	None	\	\
SwitchB	1	100	port1/7	None	\	\
SwitchC	1	100	None	port1/8	\	\
SwitchD	2	101	port1/7	None	\	\
SwitchE	2	101	None	port1/8	\	\

12.5.3 配置交换机 SwitchA

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，101，端口 port1/5、port1/6、port1/7、port1/8 模式为 Trunk，端口 port1/5、port1/6 允许 VLANs 为 1，2，3，101，端口 port1/7、port1/8 允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-43 相切环案例 SwitchA VLAN 配置

全局VLAN配置

允许访问VLANs	1,2,3,100,101
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 5 为 MEP 5，Tagged VID 为 101。

图表 12-44 相切环案例 SwitchA MEP 配置 1

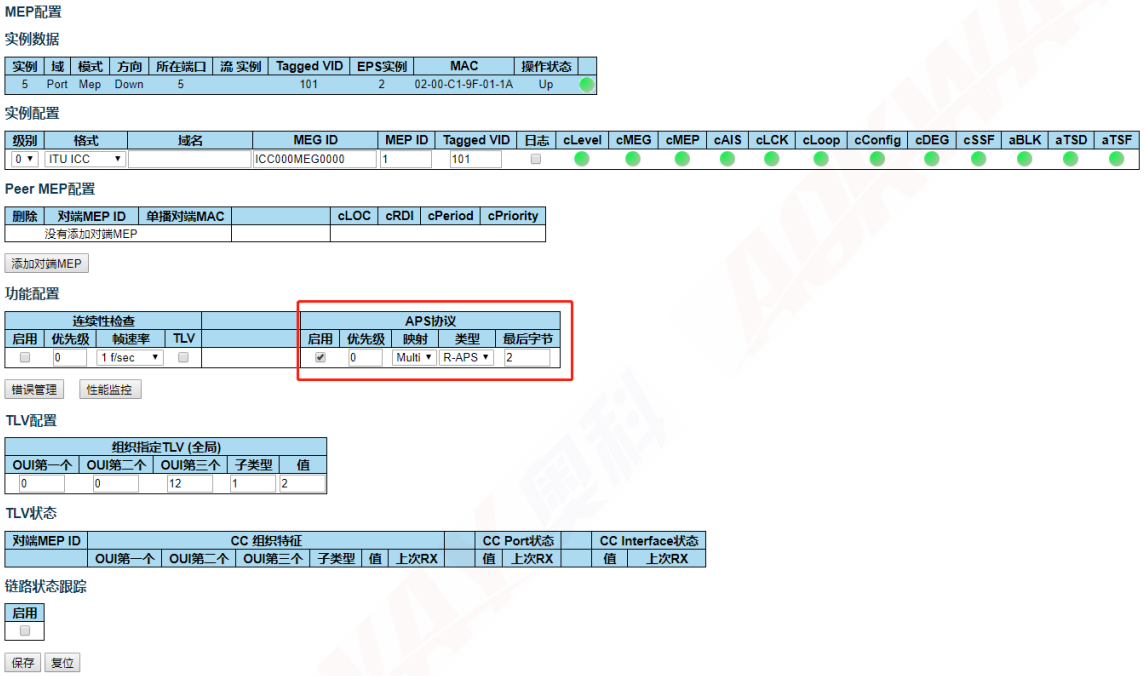
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	5	Port	Mep	Down	5	0	1	101		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 5 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 2。

图表 12-45 相切环案例 SwitchA MEP 配置 2

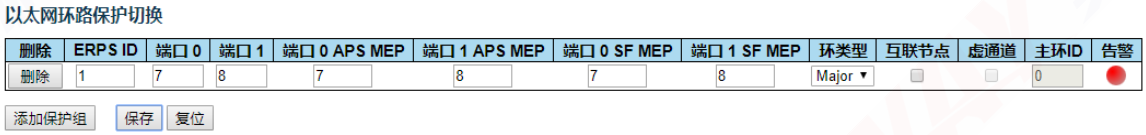


3) 同理添加端口 6-8 的 MEP 节点，进入实例数据配置中使能 RAPS 功能；6 端口属于环 2，Tagged VID 为 101，RAPS 最后字节为 2；7-8 端口属于环 1，Tagged VID 为 100，RAPS 最后字节为 1。

步骤 3：创建和配置 ERPS 保护组。

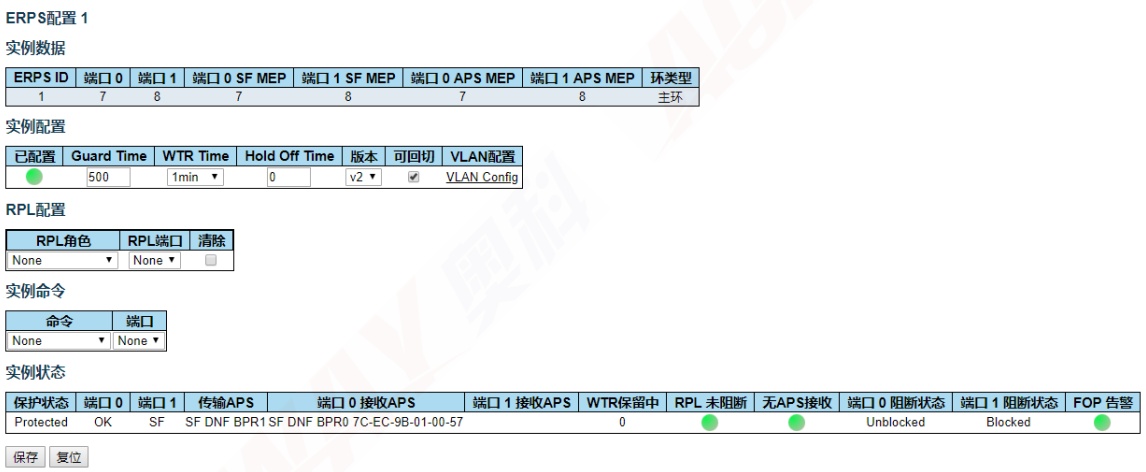
1) 在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-46 相切环案例 SwitchA ERPS 配置 1



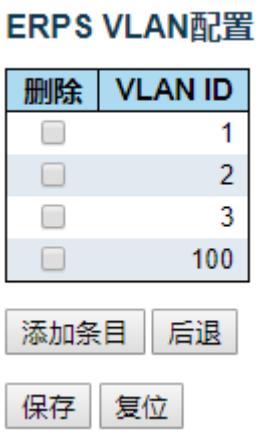
点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面。

图表 12-47 相切环案例 SwitchA ERPS 配置 2



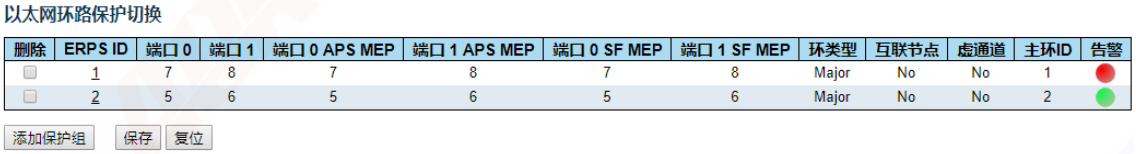
点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-48 相切环案例 SwitchA ERPS 配置 3



2) 同理，添加 ERPS 保护组 2 并配置相应的 VLAN。

图表 12-49 相切环案例 SwitchA ERPS 配置 4



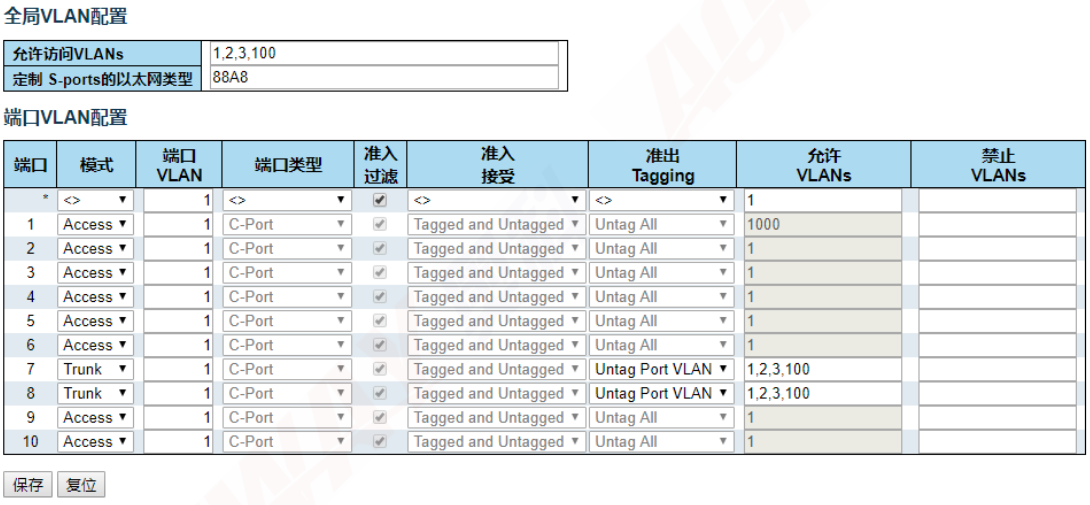
步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.5.4 配置交换机 SwitchB

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-50 相切环案例 SwitchB VLAN 配置



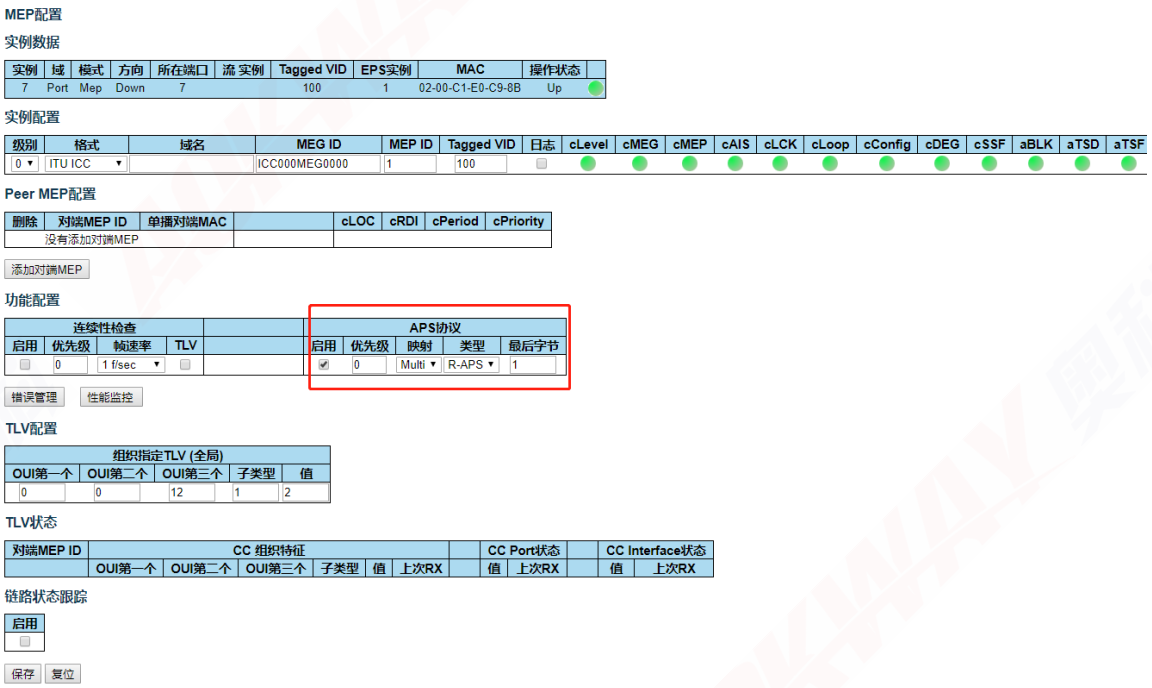
步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 100。

图表 12-51 相切环案例 SwitchB MEP 配置 1

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 1

图表 12-52 相切环案例 SwitchB MEP 配置 2

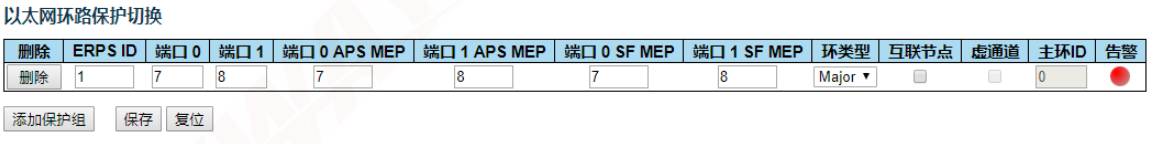


3) 同理添加端口 8 的 MEP 节点，Tagged VID 为 100，进入实例数据配置中使能 RAPS 功能，最后字节与环 ID 一致，设置为 1。

步骤 3：创建和配置 ERPS 保护组。

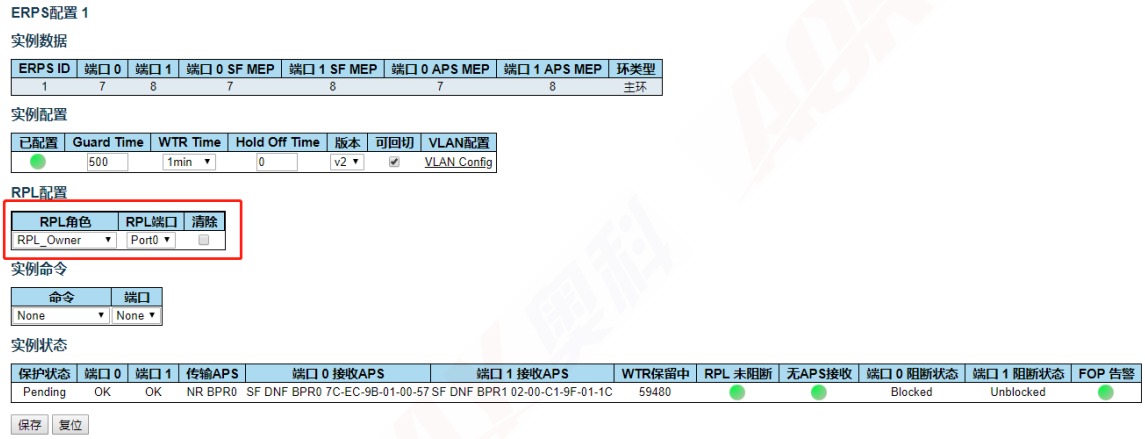
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-53 相切环案例 SwitchB ERPS 配置 1



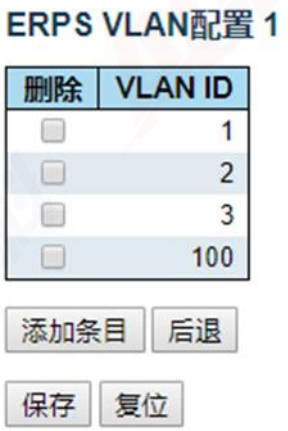
点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置把 Port0 设置为 RPL Owner 角色。

图表 12-54 相切环案例 SwitchB ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-55 相切环案例 SwitchB ERPS 配置 3



步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.5.5 配置交换机 SwitchC

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-56 相切环案例 SwitchC VLAN 配置

全局VLAN配置

允许访问VLANs	1,2,3,100
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入 过滤	准入 接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1000	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 100。

图表 12-57 相切环案例 SwitchC MEP 配置 1

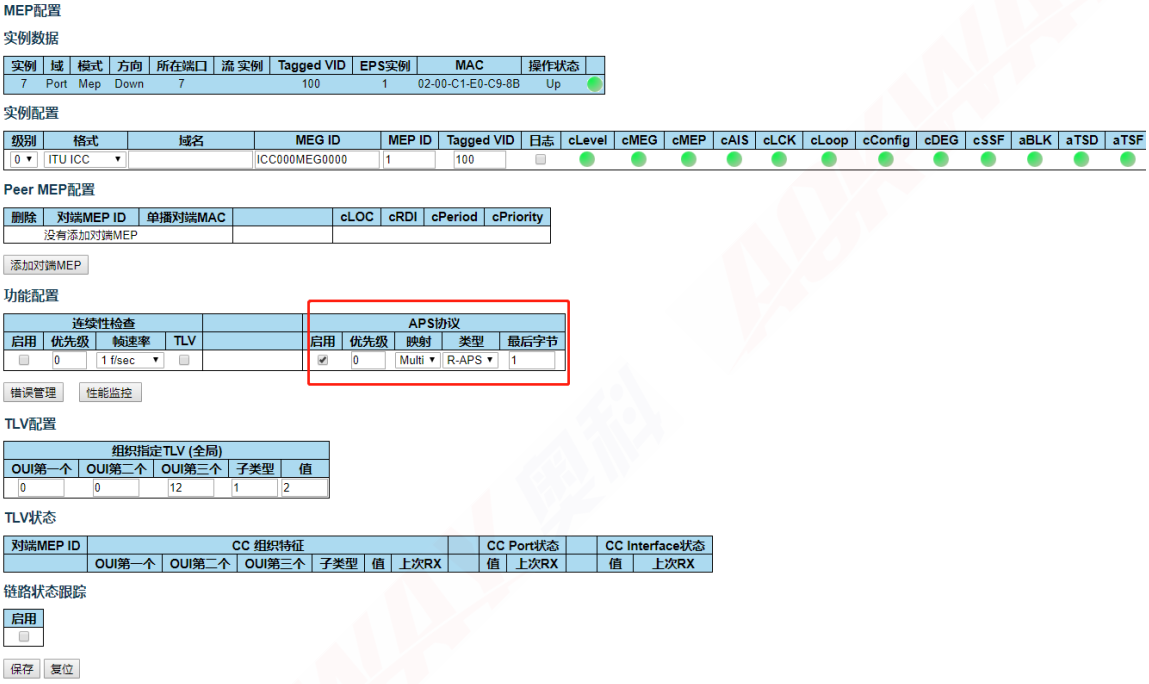
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	100		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 1

图表 12-58 相切环案例 SwitchC MEP 配置 2

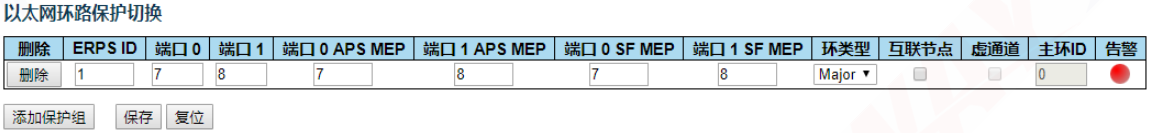


4) 同理添加端口 8 的 MEP 节点，Tagged VID 为 100，进入实例数据配置中使能 RAPS 功能，最后字节与环 ID 一致，设置为 1。

步骤 3：创建和配置 ERPS 保护组。

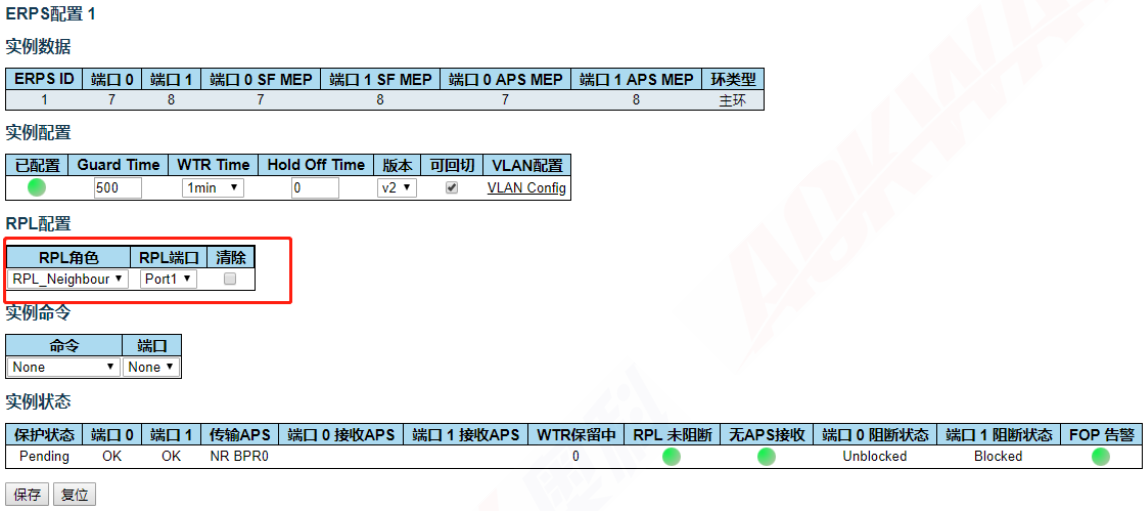
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-59 相切环案例 SwitchC ERPS 配置 1



点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置把 Port1 设置为 RPL Neighbour 角色。

图表 12-60 相切环案例 SwitchC ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-61 相切环案例 SwitchC ERPS 配置 3

步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.5.6 配置交换机 SwitchD

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，101，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，101，点击【保存】按钮完成配置。

图表 12-62 相切环案例 SwitchD VLAN 配置

全局VLAN配置

允许访问VLANs	1,2,3,101
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入 过滤	准入 接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1000	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 101。

图表 12-63 相切环案例 SwitchD MEP 配置 1

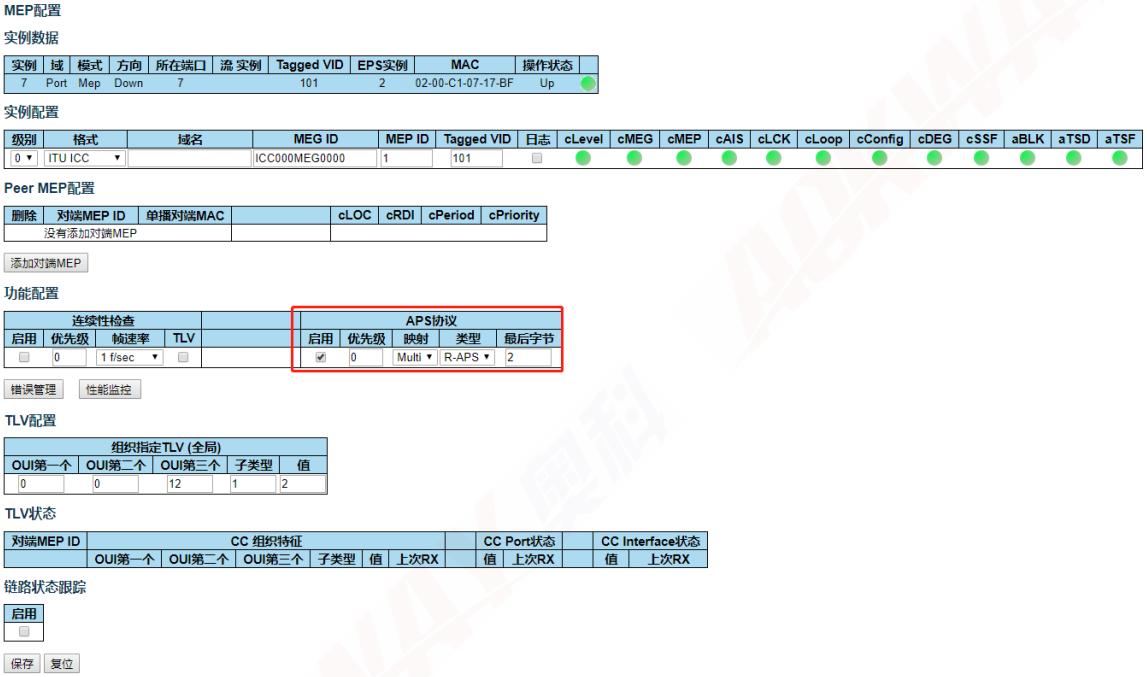
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	101		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 2

图表 12-64 相切环案例 SwitchD MEP 配置 2

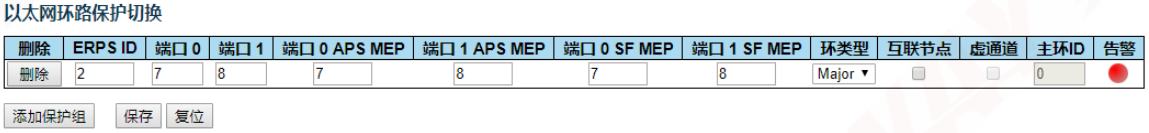


3) 同理添加端口 8 的 MEP 节点，Tagged VID 为 101，进入实例数据配置中使能 RAPS 功能，最后字节与环 ID 一致，设置为 2。

步骤 3：创建和配置 ERPS 保护组。

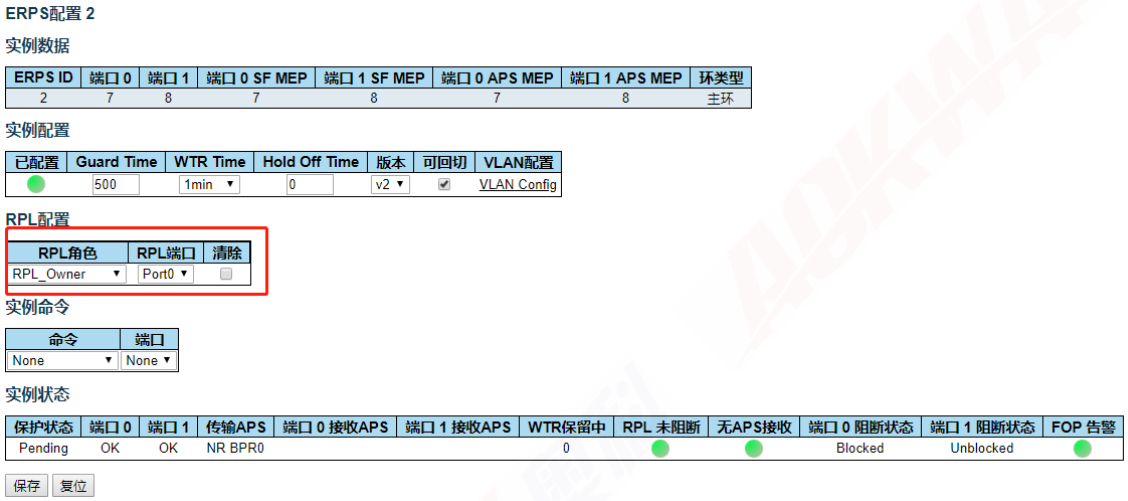
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 2，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-65 相切环案例 SwitchD ERPS 配置 1



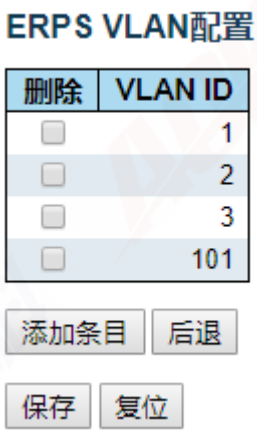
点击【保存】按钮完成保护组的添加。重新点击保护组 2 进入参数配置界面，按照规划配置把 Port0 设置为 RPL Owner 角色。。

图表 12-66 相切环案例 SwitchD ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，101 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-67 相切环案例 SwitchD ERPS 配置 3



步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.5.7 配置交换机 SwitchE

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，101，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，101，点击【保存】按钮完成配置。

图表 12-68 相切环案例 SwitchE VLAN 配置

全局VLAN配置

允许访问VLANs	1,2,3,101
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入 过滤	准入 接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1000	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 101。

图表 12-69 相切环案例 SwitchE MEP 配置 1

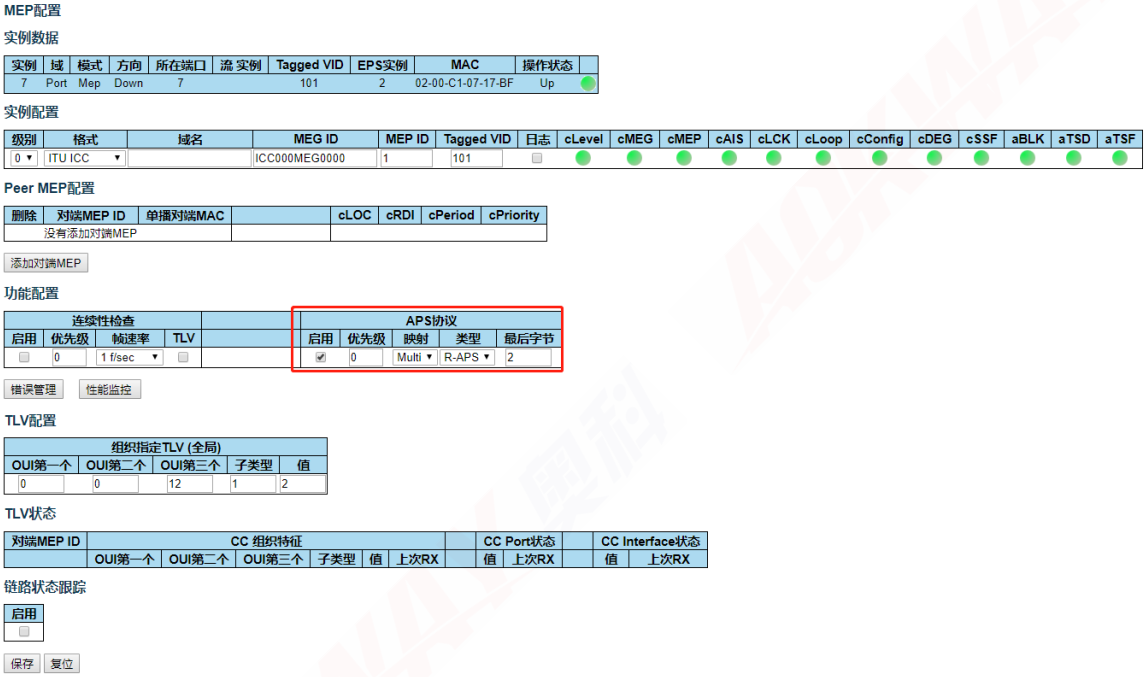
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	101		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 2

图表 12-70 相切环案例 SwitchE MEP 配置 2

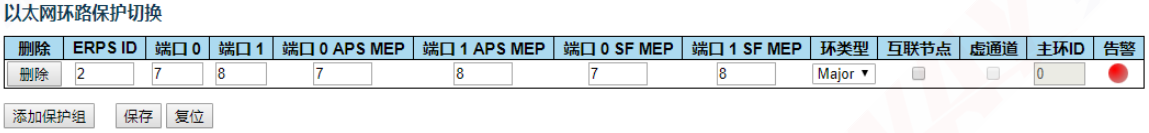


3) 同理添加端口 8 的 MEP 节点，Tagged VID 为 101，进入实例数据配置中使能 RAPS 功能，最后字节与环 ID 一致，设置为 2。

步骤 3：创建和配置 ERPS 保护组。

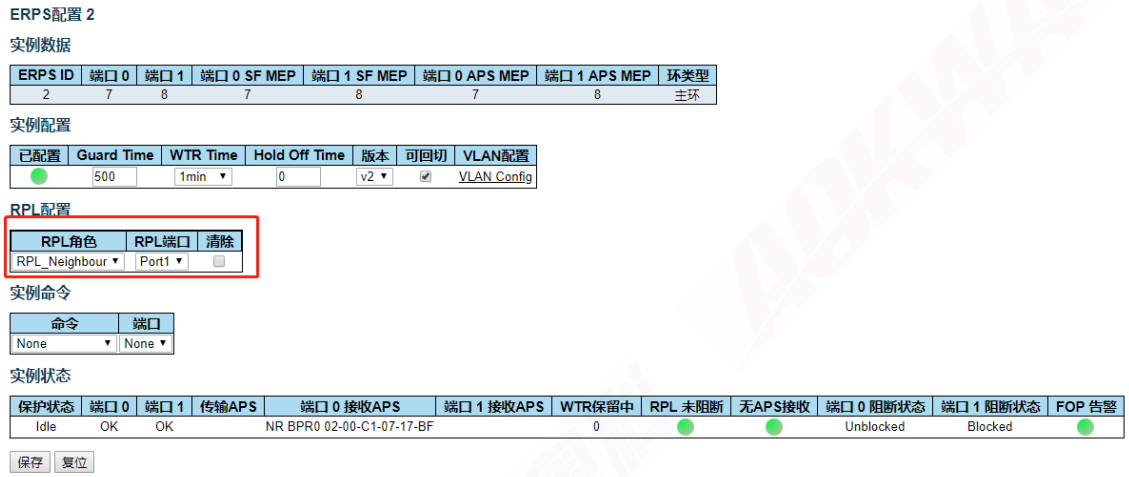
在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 2，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-71 相切环案例 SwitchE ERPS 配置 1



点击【保存】按钮完成保护组的添加。重新点击保护组 2 进入参数配置界面，按照规划配置把 Port1 设置为 RPL Neighbour 角色。

图表 12-72 相切环案例 SwitchE ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，101 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-73 相切环案例 SwitchE ERPS 配置 3

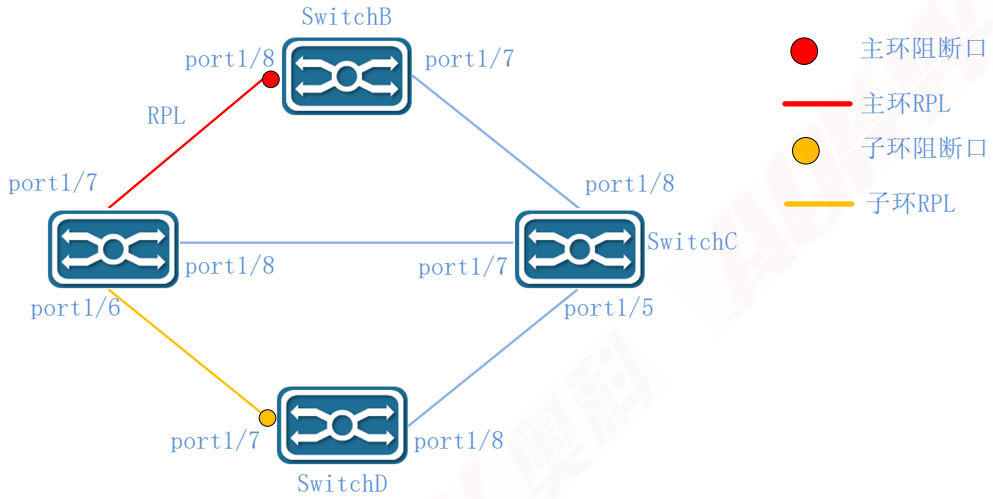
步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.6 相交环配置举例

12.6.1 案例需求

SwitchA、SwitchB、SwitchC、SwitchD 组成相交环，数据 VLAN 为 1，2，3，要求每个环中出现单点故障时都能够实现快速收敛；网络中最多可以出现两个故障点(不同环)，而不出现用户断网，达到最优可靠性。

图表 12-74 相交环案例



12.6.2 配置规划

说明

- 主环和子环的环 ID 必须不同。
- 主环和子环内的 RAPS 管理 VLAN 必须不同
- 在子环中，连接子环与主环的设备定义为互联节点，关联实例设置为主环。

主环和子环没有严格意义上的区分，一般都是假定其中一个为主环，则其中另外一个为子环。在本例中，把 SwitchA、SwitchB、SwitchC 组成的环定义为主环，环编号为“1”，阻断点为 SwitchB 的 port1/7 口，RAPS 管理 VLAN 为“100”。SwitchA、SwitchB、SwitchD 组成的环为子环，环编号为“2”，阻断点为 SwitchD 的 port1/7 口，RAPS 管理 VLAN 为“101”。具体参数如下所述。

参数 / 设备	环编号	RAPS VLAN	Owner 接口	Neighbor 接口	互联节点	关联主环
SwitchA	1	100	None	port1/7	\	\
	2	101	None	port1/6	Yes	1
SwitchB	1	100	port1/8	None	\	\
SwitchC	1	100	None	None	\	\
	2	101	None	None	Yes	1
SwitchD	2	101	port1/7	None	\	\

12.6.3 配置交换机 SwitchA

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，101，端口 port1/6、port1/7、port1/8 模式为 Trunk，端口 port1/6 允许 VLANs 为 1，2，3，101，端口 port1/7、port1/8 允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-75 相交环案例 SwitchA VLAN 配置

全局VLAN配置

允许访问VLANs	1,2,3,100,101
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 6 为 MEP6，Tagged VID 为 101。

图表 12-76 相交环案例 SwitchA MEP 配置 1

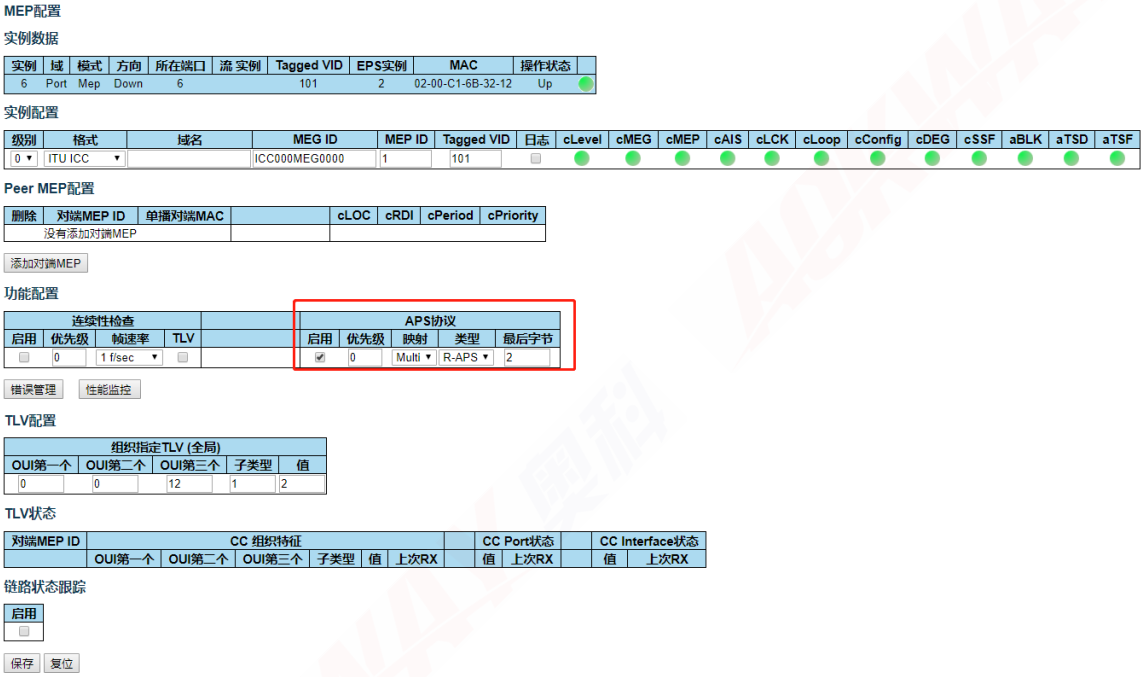
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	6	Port	Mep	Down	6	0	1	101		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 6 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 2。

图表 12-77 相交环案例 SwitchA MEP 配置 2

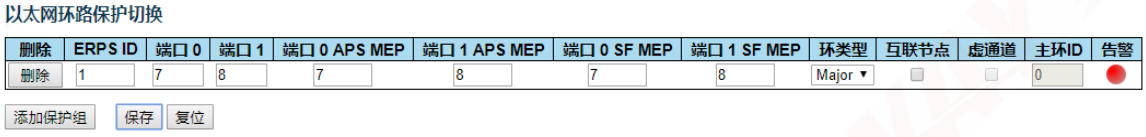


3) 同理添加端口 7-8 的 MEP 节点，进入实例数据配置中使能 RAPS 功能；7-8 端口属于环 1，Tagged VID 为 100，RAPS 最后字节为 1。

步骤 3：创建和配置 ERPS 保护组。

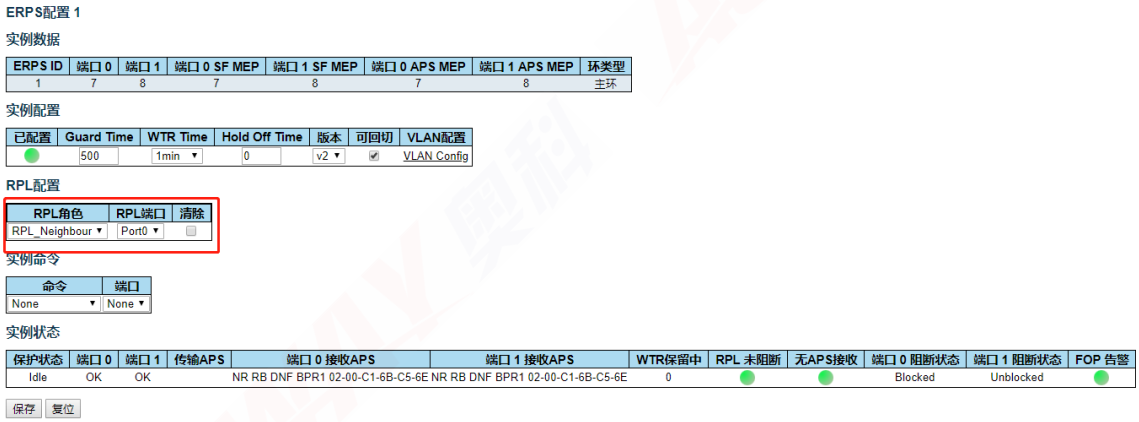
1) 在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-78 相交环案例 SwitchA ERPS 配置 1



点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置把 Port0 设置为 RPL Neighbour 角色。

图表 12-79 相交环案例 SwitchA ERPS 配置 2

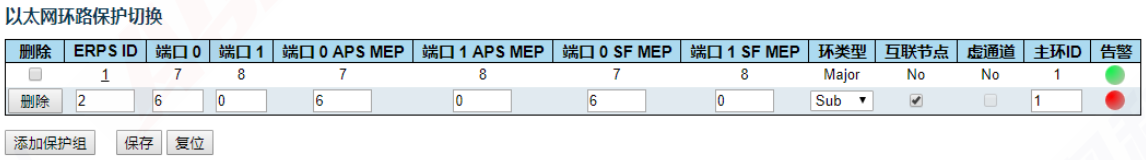


点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-80 相交环案例 SwitchA ERPS 配置 3

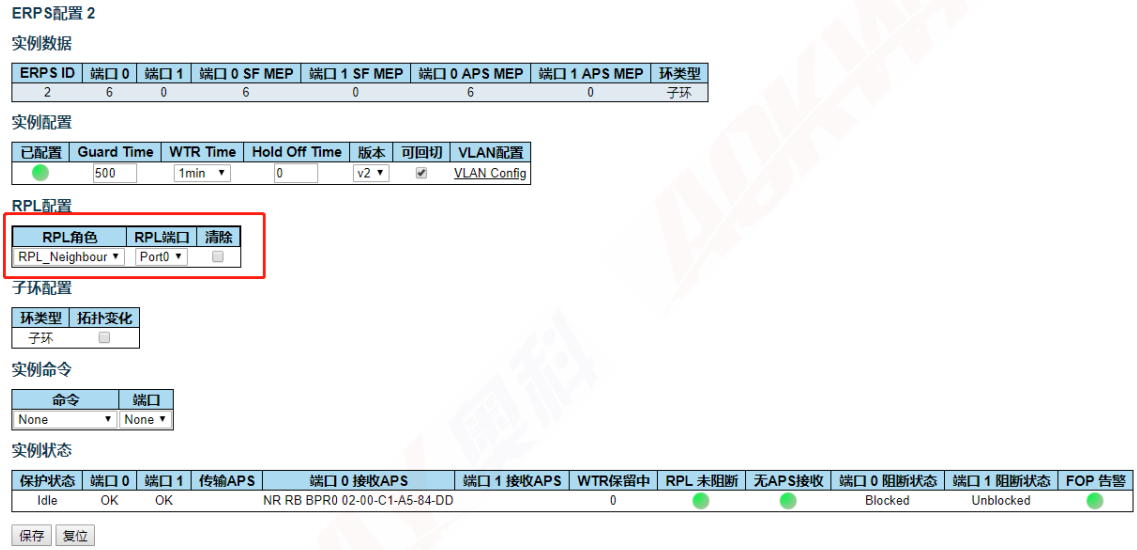
2) 继续添加 ERPS 保护组 2，端口 0 为 port1/6，端口 1 为 0，对应的 MEP 为 6 和 0，环类型设置为子环，互联节点，主环 ID 为 1。

图表 12-81 相交环案例 SwitchA ERPS 配置 4



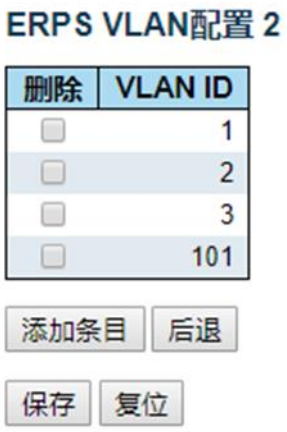
点击【保存】按钮完成保护组的添加。重新点击保护组 2 进入参数配置界面，按照规划配置把 Port0 设置为 RPL Neighbour 角色。

图表 12-82 相交环案例 SwitchA ERPS 配置 5



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，101 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-83 相交环案例 SwitchA ERPS 配置 6



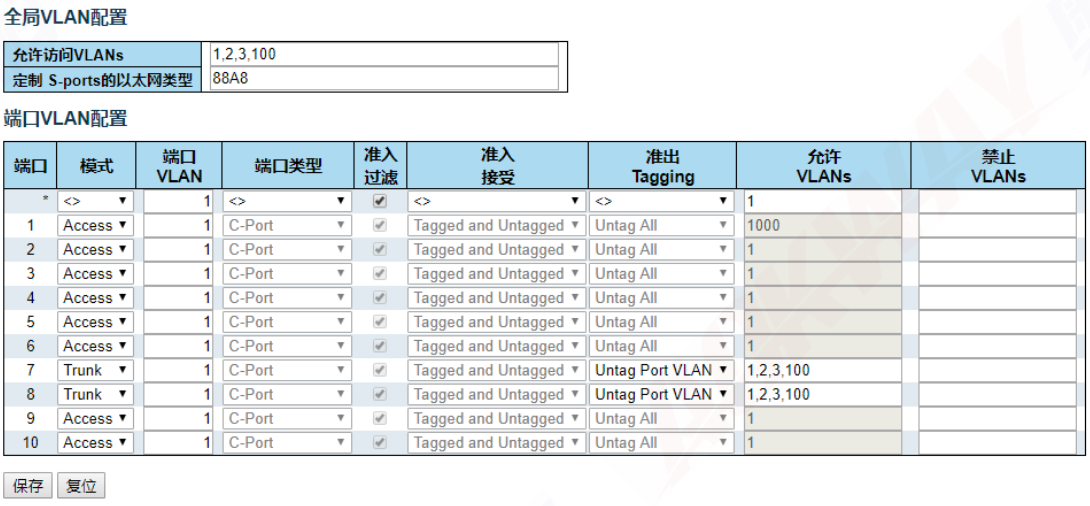
步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.6.4 配置交换机 SwitchB

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-84 相切环案例 SwitchB VLAN 配置



步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 100。

图表 12-85 相切环案例 SwitchB MEP 配置 1

维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	100		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 1

图表 12-86 相切环案例 SwitchB MEP 配置 2

MEP配置

实例数据

实例	域	模式	方向	所在端口	流 实例	Tagged VID	EPS实例	MAC	操作状态
7	Port	Mep	Down	7		100	1	02-00-C1-E0-C9-8B	Up

实例配置

级别	格式	域名	MEG ID	MEP ID	Tagged VID	日志	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cDEG	cSSF	aBLK	aTSD	aTSF
0	ITU ICC		ICC000MEG0000	1	100													

Peer MEP配置

删除	对端MEP ID	单播对端MAC		cLOC	cRDI	cPeriod	cPriority
没有添加对端MEP							

添加对端MEP

功能配置

连续性检查					APS协议				
启用	优先级	帧速率	TLV		启用	优先级	映射	类型	最后字节
	0	1 f/sec			✓	0	Multi	R-APS	1

错误管理 性能监控

TLV配置

组织指定TLV (全局)				
OUI第一个	OUI第二个	OUI第三个	子类型	值
0	0	12	1	2

TLV状态

对端MEP ID	CC 组织特征							CC Port状态			CC Interface状态	
	OUI第一个	OUI第二个	OUI第三个	子类型	值	上次RX		值	上次RX		值	上次RX

链路状态跟踪

启用

保存 复位

3) 同理添加端口 8 的 MEP 节点，Tagged VID 为 100，进入实例数据配置中使能 RAPS 功能，最后字节与环 ID 一致，设置为 1。

步骤 3：创建和配置 ERPS 保护组。

在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-87 相切环案例 SwitchB ERPS 配置 1

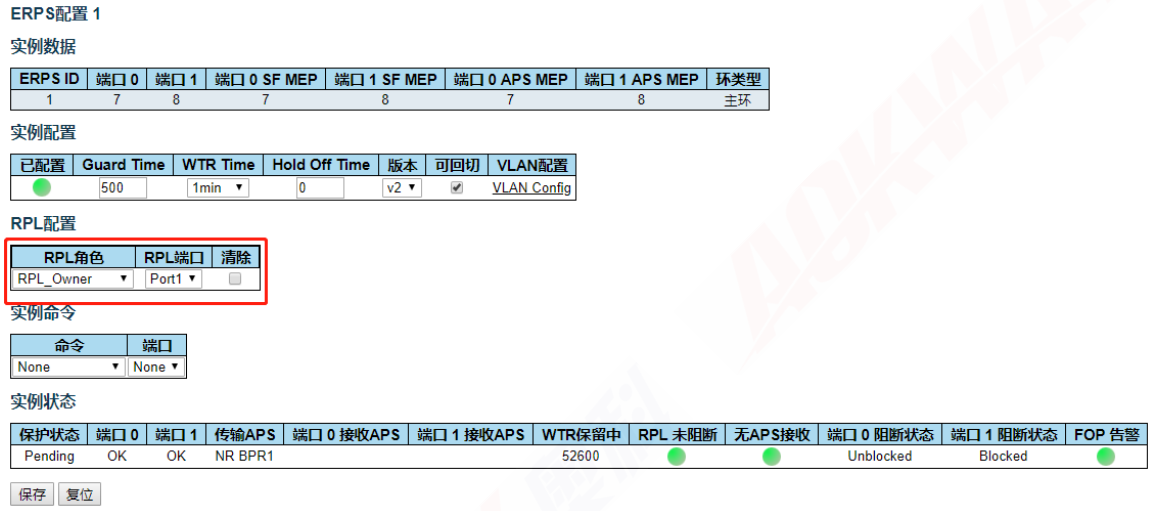
以太网环路保护切换

删除	ERPS ID	端口 0	端口 1	端口 0 APS MEP	端口 1 APS MEP	端口 0 SF MEP	端口 1 SF MEP	环类型	互联节点	虚通道	主环ID	告警
删除	1	7	8	7	8	7	8	Major			0	

添加保护组 保存 复位

点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置把 Port1 设置为 RPL Owner 角色。

图表 12-88 相切环案例 SwitchB ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-89 相切环案例 SwitchB ERPS 配置 3

步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.6.5 配置交换机 SwitchC

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，100，101，端口 port1/5、port1/7、port1/8 模式为 Trunk，端口 port1/5 允许 VLANs 为 1，2，3，101，端口 port1/7、port1/8 允许 VLANs 为 1，2，3，100，点击【保存】按钮完成配置。

图表 12-90 相交环案例 SwitchC VLAN 配置

全局VLAN配置

允许访问VLANs	1,2,3,100,101
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入 过滤	准入 接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,101	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

保存 复位

步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 5 为 MEP5，Tagged VID 为 101。

图表 12-91 相交环案例 SwitchC MEP 配置 1

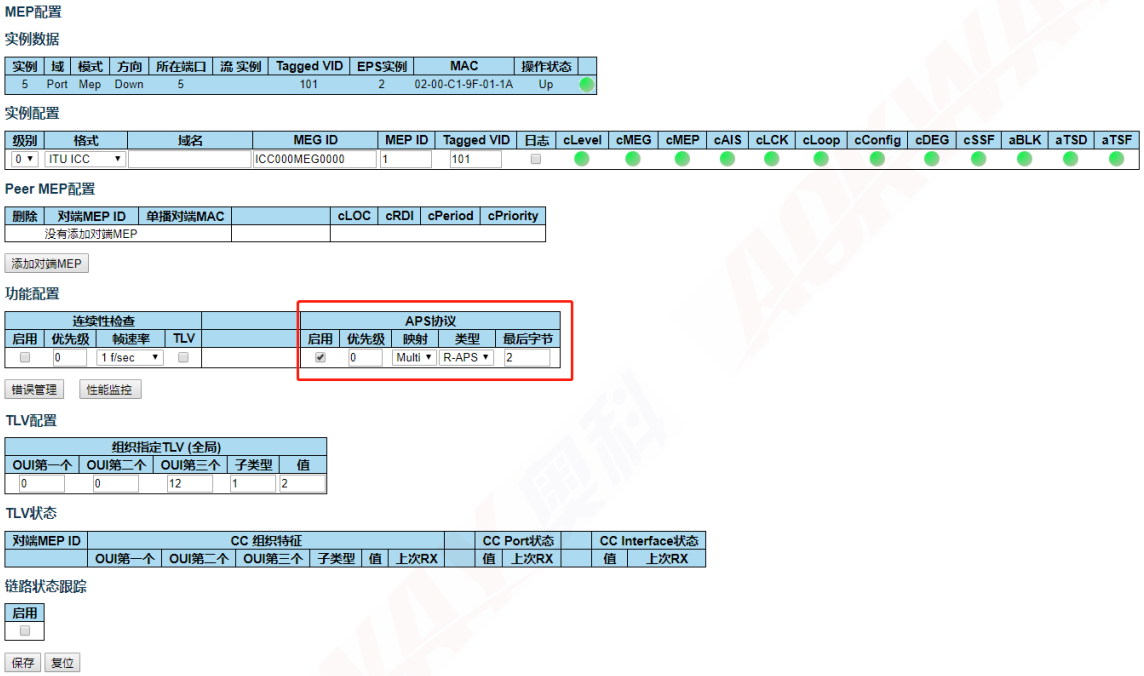
维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	5	Port	Mep	Down	5	0	1	101		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 5 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 2。

图表 12-92 相交环案例 SwitchC MEP 配置 2

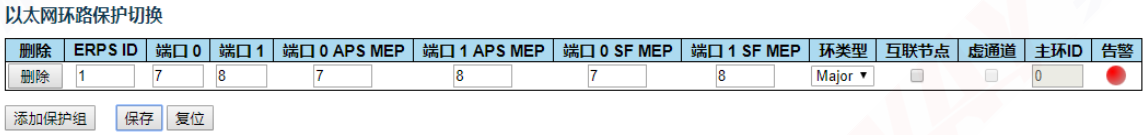


3) 同理添加端口 7-8 的 MEP 节点，进入实例数据配置中使能 RAPS 功能；7-8 端口属于环 1，Tagged VID 为 100，RAPS 最后字节为 1。

步骤 3：创建和配置 ERPS 保护组。

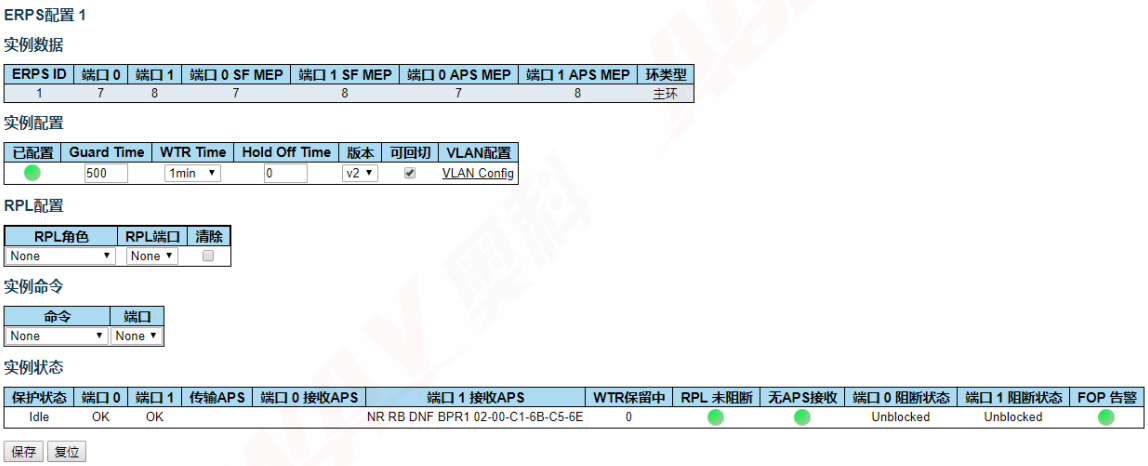
1) 在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 1，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8。

图表 12-93 相交环案例 SwitchC ERPS 配置 1



点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面。

图表 12-94 相交环案例 SwitchC ERPS 配置 2

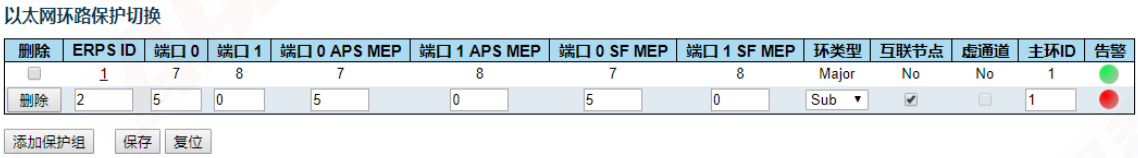


点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，100 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-95 相交环案例 SwitchC ERPS 配置 3

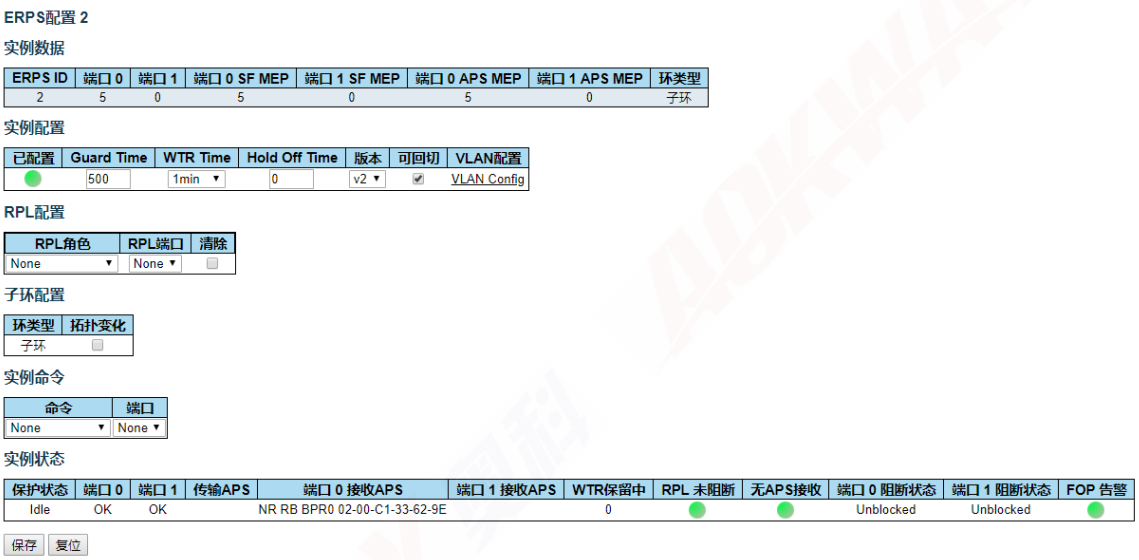
2) 继续添加 ERPS 保护组 2，端口 0 为 port1/5，端口 1 为 0，对应的 MEP 为 5 和 0，环类型设置为子环，互联节点，主环 ID 为 1。

图表 12-96 相交环案例 SwitchC ERPS 配置 4



点击【保存】按钮完成保护组的添加。重新点击保护组 2 进入参数配置界面。

图表 12-97 相交环案例 SwitchC ERPS 配置 5



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，101 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-98 相交环案例 SwitchC ERPS 配置 6

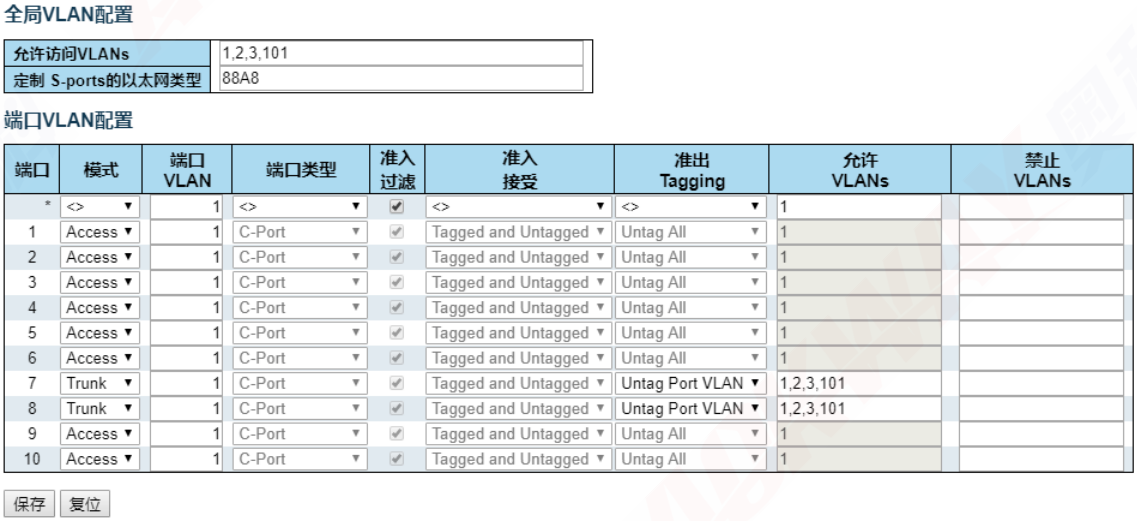
步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

12.6.6 配置交换机 SwitchD

步骤 1：VLAN 和端口配置。

在导航栏【配置】子项中选择【VLAN】，配置允许访问 VLANs 为 1，2，3，101，端口 port1/7、port1/8 模式为 Trunk，允许 VLANs 为 1，2，3，101，点击【保存】按钮完成配置。

图表 12-99 相切环案例 SwitchD VLAN 配置



步骤 2：创建和配置 MEP 节点。

1) 在导航栏【配置】子项中选择【MEP】，点击【添加 MEP】按钮添加端口 7 为 MEP 7，Tagged VID 为 101。

图表 12-100 相切环案例 SwitchD MEP 配置 1

维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
删除	7	Port	Mep	Down	7	0	1	101		

添加MEP 保存 复位

2) 点击【保存】按钮完成实体节点的添加。重新点击实例 7 进入实例数据配置中，使能 RAPS 功能，最后字节与环 ID 一致，设置为 2

图表 12-101 相切环案例 SwitchD MEP 配置 2

MEP配置

实例数据

实例	域	模式	方向	所在端口	流 实例	Tagged VID	EPS实例	MAC	操作状态
7	Port	Mep	Down	7		101	2	02-00-C1-33-62-9E	Up

实例配置

级别	格式	域名	MEG ID	MEP ID	Tagged VID	日志	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cDEG	cSSF	aBLK	aTSD	aTSF
0	ITU ICC		ICC000MEG0000	1	101													

Peer MEP配置

删除	对端MEP ID	单播对端MAC		cLOC	cRDI	cPeriod	cPriority
没有添加对端MEP							

添加对端MEP

功能配置

连续性检查					APS协议				
启用	优先级	帧速率	TLV		启用	优先级	映射	类型	最后字节
	0	1 f/sec				0	Multi	R-APS	2

错误管理 性能监控

TLV配置

组织指定TLV (全局)				
OUI第一个	OUI第二个	OUI第三个	子类型	值
0	0	12	1	2

TLV状态

对端MEP ID	CC 组织特征						CC Port状态		CC Interface状态	
	OUI第一个	OUI第二个	OUI第三个	子类型	值	上次RX	值	上次RX	值	上次RX

链路状态跟踪

启用

保存 复位

3) 同理添加端口 8 的 MEP 节点，Tagged VID 为 101，进入实例数据配置中使能 RAPS 功能，最后字节与环 ID 一致，设置为 2。

步骤 3：创建和配置 ERPS 保护组。

在导航栏【配置】下选择【ERPS】，进入 ERPS 配置界面，点击【添加保护组】按钮，添加保护组 2，端口 port1/7 和 port1/8，对应的 MEP 为 7 和 8，环类型设置为子环。

图表 12-102 相切环案例 SwitchD ERPS 配置 1

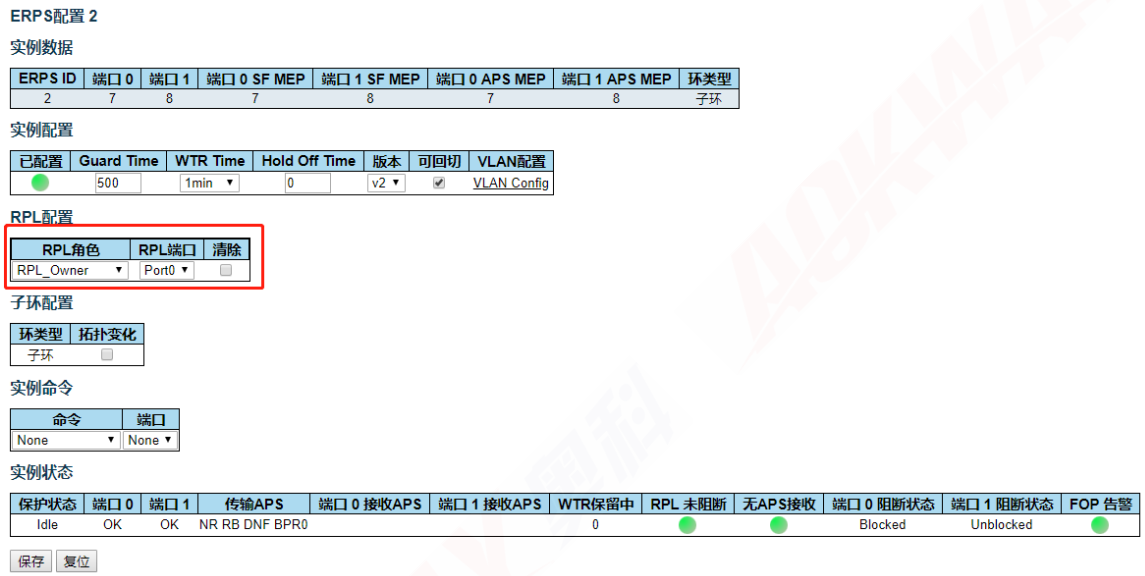
以太网环路保护切换

删除	ERPS ID	端口 0	端口 1	端口 0 APS MEP	端口 1 APS MEP	端口 0 SF MEP	端口 1 SF MEP	环类型	互联节点	虚通道	主环ID	告警
删除	2	7	8	7	8	7	8	Sub			0	

添加保护组 保存 复位

点击【保存】按钮完成保护组的添加。重新点击保护组 1 进入参数配置界面，按照规划配置把 Port0 设置为 RPL Owner 角色。

图表 12-103 相切环案例 SwitchD ERPS 配置 2



点击【VLAN_Config】进入 VLAN 配置页面，点击【添加条目】依次添加 VLAN 1，2，3，101 为保护 VLAN，点击【保存】按钮完成配置。

图表 12-104 相切环案例 SwitchD ERPS 配置 3

步骤 4：选择导航栏上的【维护】-【配置】-【保存配置】页面，点击【保存配置】按钮保存配置。

13 MAC 地址表

13.1 MAC 地址概述

以太网交换机通过解析报文所携带的目的 MAC 地址，查询 MAC 地址表，将报文发送到相应的端口。MAC 地址表记录了与该设备相连的设备的 MAC 地址、接口以及所属的 VLAN ID 信息。以太网交换机根据 MAC 地址表查找的结果决定采用知名单播或未知名广播的转发方式。

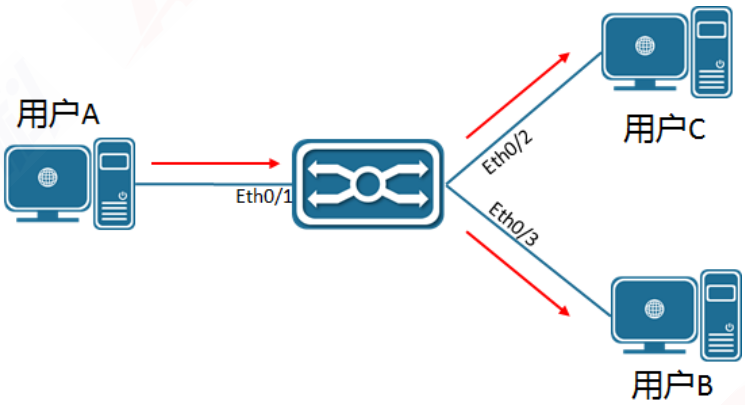
知名单播：以太网交换机在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。

未知名广播：以太网交换机在地址表中没有找到目标 MAC 地址对应的表项，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

以太网交换机的 MAC 地址可通过动态获取或静态配置，一般情况下通过动态获取得到。下面通过分析用户 A 与用户 C 交互过程，给出 MAC 地址动态学习的工作原理。

用户 A 发送报文到交换机的端口 1，此时以太网交换机将用户 A 的 MAC 地址学习到 MAC 地址表中。由于地址表中没有用户 C 的源 MAC 地址，因此以太网交换机以广播的方式将报文发送到除连接用户 A 的 1 以外的同属 VLAN1 的所有端口，包括用户 B 与用户 C 的端口，此时用户 B 能够收到用户 A 所发出的不属于它的报文。

图表 13-1 MAC 地址学习举例

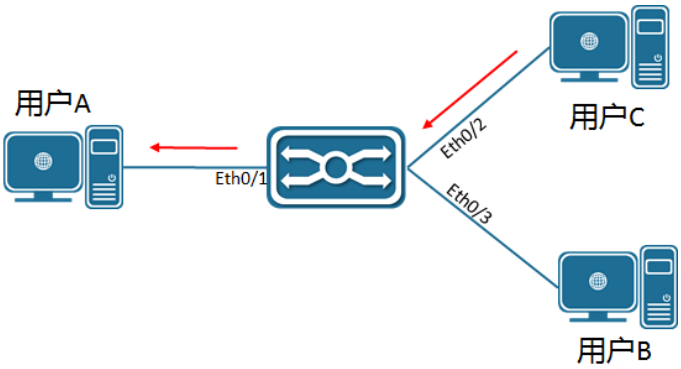


当前动态 MAC 地址表信息：

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	1

用户 B 收到报文后将回应报文通过以太网交换机的端口 2，发送给用户 A，此时以太网交换机的 MAC 地址表中已存在用户 A 的 MAC 地址，报文被以单播的方式转发到 1 端口，同时以太网交换机将学习用户 C 的 MAC 地址，与前面所不同的是用户 B 此时接收不到用户 C 发送给用户 A 的报文。

图表 13-2 单播转发示意



当前动态 MAC 地址表信息：

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	1
用户 C	1	000E.C6C1.C8AD	2

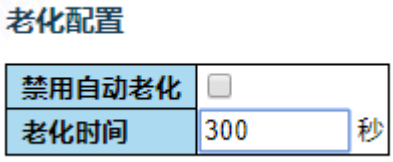
通过用户 A 与用户 C 的一次交互过程后，设备学习到了用户 A 与用户 C 的源 MAC 地址，之后用户 A 与用户 C 之间的报文交互则采用单播的方式进行转发，此后用户 B 将不再接收到用户 A 与用户 C 之间的交互报文。

13.2 配置 MAC 地址

在【导航栏】下拉菜单中选择：配置->MAC 地址表，进入配置界面。

■ 配置 MAC 地址老化

图表 13-3 MAC 地址老化配置



配置项	说明
禁用自动老化	使能禁用自动老化功能，默认关闭
老化时间	MAC 地址老化时间，范围 10-1000000 秒，默认 300 秒

■ 端口 MAC 地址学习

图表 13-4 端口 MAC 地址学习配置

配置项	说明
端口成员	面板端口号
自动	当接收到未知源 MAC 地址报文时，端口自动学习 MAC 地址
禁用	端口关闭 MAC 地址学习
安全	源 MAC 地址命中端口静态 MAC 地址的报文放行，否则报文丢弃

注意

- 端口安全配置开启的端口，无法更改地址学习模式。

■ 配置静态 MAC 地址

图表 13-5 静态 MAC 配置

静态MAC地址表配置

			端口成员									
删除	VLAN ID	MAC地址	1	2	3	4	5	6	7	8	9	10
☐	1	00-00-12-34-56-78	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

配置项	说明
VLAN ID	VLAN ID
MAC 地址	MAC 地址
端口成员	面板端口号

13.3 查看 MAC 地址

在【导航栏】下拉菜单中选择：监控->MAC 地址表，进入查看界面。

图表 13-6 查看 MAC 地址表

MAC地址表

开始VLAN 1 和MAC地址 00-00-00-00-00-00 每个页面显示 20 条表项.

			端口成员									
类型	VLAN	MAC地址	CPU	1	2	3	4	5	6	7	8	9	10
Static	1	00-00-12-34-56-78			✓								
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-01-00-50	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	7C-EC-9B-01-00-50	✓										
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1000	02-0B-34-50-9F-A7		✓									
Static	1000	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1000	33-33-FF-01-00-50	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1000	7C-EC-9B-01-00-50	✓										
Static	1000	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

配置项	说明

类型	Static 与 Dynamic 两种类型
VLAN	VLAN ID
MAC 地址	MAC 地址列表，其中包括几条特殊的 MAC 地址，如本机的 IPv4 的 MAC 地址、广播 MAC 地址、IPv6 的 MAC 地址
端口成员	面板端口号以及 CPU 端口

13.4 CLI 参考命令

命令	switch(config)# mac address-table aging-time 300 switch(config)# mac address-table learning vlan 10 switch(config)# no mac address-table learning vlan 10 switch(config)# mac address-table static 00:00:12:34:56:78 vlan 1 interface GigabitEthernet 1/2
描述	配置 MAC 地址表老化时间; 配置 VLAN 上开启 MAC 地址学习; 配置 VLAN 上关闭 MAC 地址学习; 配置 MAC 地址表静态地址;

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口;

命令	switch(config-if)# mac address-table learning switch(config-if)# mac address-table learning secure switch(config-if)# no mac address-table learning
描述	配置端口 MAC 地址学习模式为自动; 配置端口 MAC 地址学习模式为安全; 配置端口 MAC 地址学习模式为禁止;

命令	switch# show mac address-table
描述	打印 MAC 地址表状态;

14 VLAN

VLAN 是虚拟局域网（Virtual Local Area Network）的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。VLAN 的划分不受网络端口的 实际物理位置的限制。VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其它的 VLAN 之中。

基于端口的 VLAN 是最简单的一种 VLAN 划分方法。用户可以将设备上的端口划分到不同的 VLAN 中，此后从某个端口接收的报文将只能在相应的 VLAN 内进行传输，从而实现广播域的隔离和虚拟工作组的划分。

以太网交换机的端口链路类型可以分为三种：Access、Trunk、Hybrid。这三种端口在加入 VLAN 和对报文进行转发时会进行不同的处理。

Access 类型：端口只能属于 1 个 VLAN，即端口 VLAN，当输入报文带 VLAN 非端口 VLAN 时，将其过滤，一般用于交换机与终端用户之间的连接；

Trunk 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文。当输入报文不带 VLAN 属性时，默认为端口 VLAN。

Hybrid 类型：在 Trunk 类型基础上，增加端口类型选择、准入过滤等功能，其支持下面几种端口类型。

Unware：输入报文 VLAN 参数保持不变，若输出端口准出配置要求带 TAG，则增加一输出端口 VLAN 的外 TAG，即输出报文带双 TAG。

C-Port：其基本实现与 trunk 一样，对输入报文只识别 TPID=0x8100 的 TAG，若输出带 TAG，其 TPID=0x8100。

S-Port：其基本实现与 trunk 一样，对输入报文只识别 TPID=0x88A8 的 TAG，若输出带 TAG，其 TPID=0x88A8。

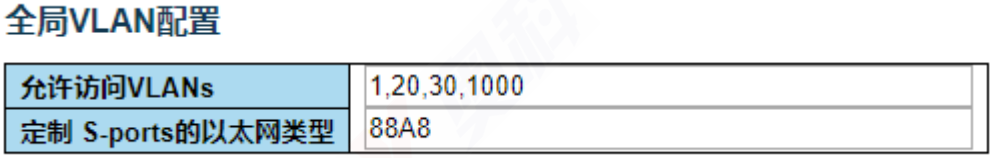
S-Custom-Port：其基本实现与 S-Port 一样，其 TPID 为用户配置值。

14.1 配置 VLAN

在【导航栏】下拉菜单中选择：配置->VLANs，进入配置界面。

■ 全局 VLAN 配置

图表 14-1 全局 VLAN 配置



配置项	说明
允 许 访 问	创建 vlan，支持“,”和“-”两种格式，“,”表示多个配置段，每个配置段可以是

VLANs	单个 vlan，也可以是通过“-”表示的一个 vlan 范围。比如“10-13”表示 vlan10，11，12，13 4 个 vlan。 只服务于 access 类型端口
定制 S-ports 的以太网类型	定义 VLAN TAG 中的 TPID 字段 对所有 S-Custom-Port 类型端口有效

■ 端口 VLAN 配置

图表 14-2 端口 VLAN 配置

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1000	<>	☑	<>	<>	1000	
1	Access	1000	C-Port	☑	Tagged and Untagged	Untag All	1000	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

配置项	说明
端口	面板端口号
模式	access、trunk、hybrid 三种模式，默认 access
端口 VLAN	端口默认 VLAN ID
端口类型	支持 Unaware、C-Port、S-Port、S-Custom-Port 该参数仅对 hybrid 模式有效
准入过滤	使能入口 VLAN 过滤 该参数仅对 hybrid 模式有效
准入接受	选择入口放行是否带 TAG 报文，支持 Tagged and Untagged、Tagged、Untagged 三种选择 该参数仅对 hybrid 模式有效
准出 Tagging	选择出口报文否带 TAG，支持 Untag Port Vlan、Tag all、Untag all 三种选择 该参数仅对 hybrid/trunk 模式有效
允许 VLANs	定义 trunk/hybrid 口的允许 vlan，默认 1-4095
禁止 VLANs	定义 trunk/hybrid 口的禁止 vlan，默认为空

14.2 查看 VLAN

14.2.1 查看 VLAN 与端口映射关系

在【导航栏】下拉菜单中选择：监控->VLANs->成员关系，进入查看界面。

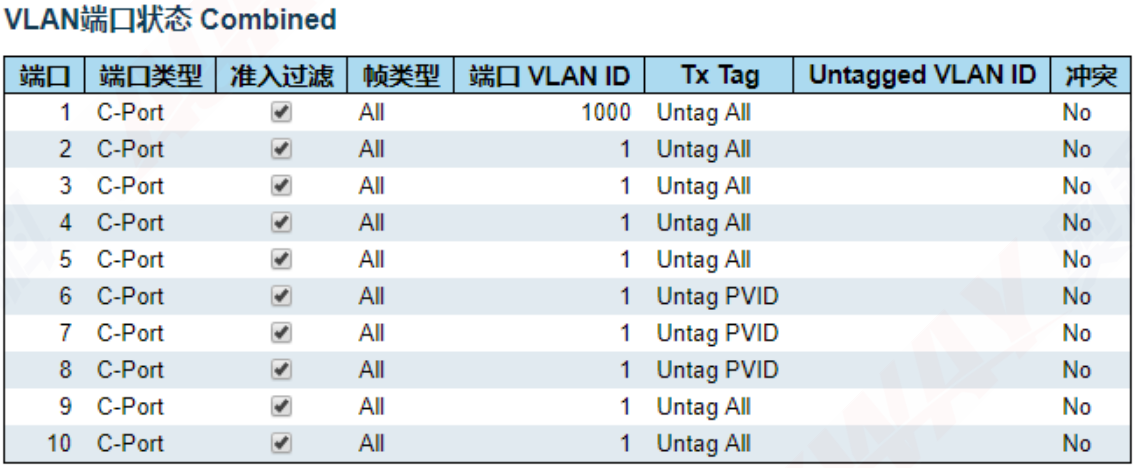
图表 14-3 查看 VLAN 成员关系

配置项	说明
VLAN ID	VLAN ID
端口成员	端口输入 VLAN，则显示绿色，并选中

14.2.2 查看 VLAN 端口配置

在【导航栏】下拉菜单中选择：监控->VLANs->端口，进入查看界面。

图表 14-4 查看 VLAN 端口状态



配置项	说明
端口	面板端口号
端口类型	配置的端口类型
准入过滤	端口是否使能准入过滤
帧类型	用户配置的准入接受，支持 All、Tagged、Untagged
端口 VLAN ID	用户配置端口 VLAN ID
Tx Tag	用户配置的出口带 TAG 模式，支持 Untag Port Vlan、Tag all、Untag all 三种选择
Untagged VLAN ID	保留

冲突	保留

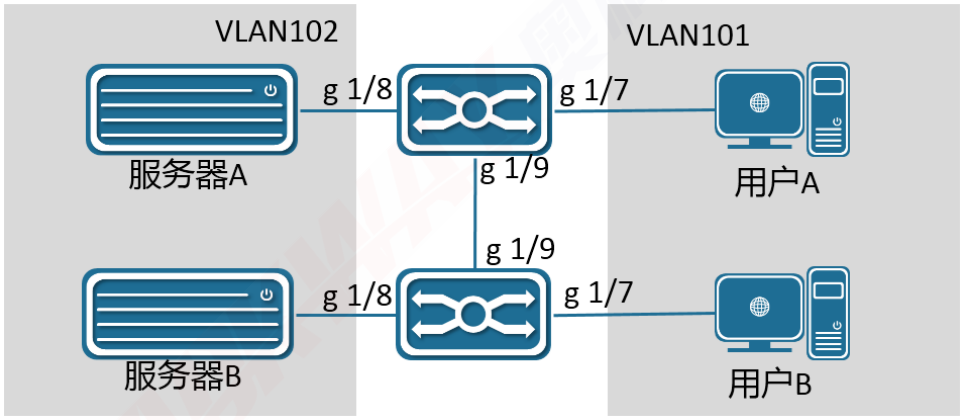
14.3 VLAN 典型配置案例

■ 案例需求

下图是常见办公网络，用户 A 与用户 B 在同一 VLAN 域内，连接两不同交换设备。服务器 A 与服务器 B 在同一个域内，也连接两不同交换设备。

要求交换设备上 VLAN 的划分，能满足用户间能正常访问，用户无法访问服务器。

图表 14-5 VLAN 案例



■ 操作步骤

两台交换设备做同样配置：全局创建 VLAN101、102；端口 7 配置端口 VLAN101，端口 8 配置端口 VLAN102；端口 9 配置模式 Trunk，具体配置如下。

图表 14-6 VLAN 案例配置

全局VLAN配置

允许访问VLANs	1,101,102
定制 S-ports的以太网类型	88A8

端口VLAN配置

端口	模式	端口 VLAN	端口类型	准入过滤	准入接受	准出 Tagging	允许 VLANs	禁止 VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	101	C-Port	☑	Tagged and Untagged	Untag All	101	
8	Access	102	C-Port	☑	Tagged and Untagged	Untag All	102	
9	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

14.4 CLI 参考命令

命令	switch(config)# vlan 1,20,30,1000 switch(config)# no vlan 1000 switch(config)# vlan ethertype s-custom-port 0x88a8

描述	配置添加 VLAN； 配置删除 VLAN； 配置定制 S-ports 的以太网类型；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# switchport mode hybrid
描述	配置端口 VLAN 模式；

命令	switch(config-if)# switchport access vlan 1000
描述	配置端口 Access 模式端口 VLAN；

命令	switch(config-if)# switchport trunk native vlan 20 switch(config-if)# switchport trunk vlan tag native switch(config-if)# no switchport trunk vlan tag switch(config-if)# switchport trunk allowed vlan 1,1000
描述	配置端口 Trunk 模式端口 VLAN； 配置端口 Trunk 模式准出 Tagging 模式为 Tag All； 配置端口 Trunk 模式准出 Tagging 模式为 Untag Port VLAN； 配置端口 Trunk 模式允许的 VLANs；

命令	switch(config-if)# switchport hybrid native vlan 30 switch(config-if)# switchport hybrid port-type s-port switch(config-if)# switchport hybrid ingress-filtering switch(config-if)# no switchport hybrid ingress-filtering switch(config-if)# switchport hybrid acceptable-frame-type tagged switch(config-if)# switchport hybrid egress-tag all switch(config-if)# switchport hybrid egress-tag none switch(config-if)# no switchport hybrid egress-tag switch(config-if)# switchport hybrid allowed vlan 20-23
描述	配置端口 Hybrid 模式端口 VLAN； 配置端口 Hybrid 模式端口类型； 配置端口 Hybrid 模式开启准入过滤； 配置端口 Hybrid 模式关闭准入过滤； 配置端口 Hybrid 模式准入接受模式； 配置端口 Hybrid 模式准出 Tagging 模式为 Tag All； 配置端口 Hybrid 模式准出 Tagging 模式为 Untag All；

	配置端口 Hybrid 模式准出 Tagging 模式为 Untag Port VLAN; 配置端口 Hybrid 模式允许的 VLANs;

命令	switch(config-if)# switchport forbidden vlan add 20 switch(config-if)# switchport forbidden vlan remove 20
描述	配置端口添加禁止 VLANs; 配置端口删除禁止 VLANs;

命令	switch# show vlan brief switch# show vlan status
描述	打印 VLAN 成员关系; 打印 VLAN 端口;

15 私有 VLAN

15.1 私有 VLAN 成员表

私有 VLAN 基于源端口掩码，跟 VLAN 没有任何关系，这意味着私有 VLAN ID 和 VLAN ID 可以相同，也可以不同。端口必须同时是 VLAN 和私用 VLAN 的成员才能转发数据包。默认情况下，所有端口都是私有 VLAN 1 的成员。

两个端口只要同时属于至少一个私有 VLAN 的成员，那么两个端口就是互通的，反之，则两个端口间隔离。

每个端口都可以属于多个私有 VLAN。私有 VLAN 总共支持的数量为面板端口总数。

在【导航栏】下拉菜单中选择：配置->私有 VLAN->成员表，进入配置页面。

图表 15-1 PVLAN 成员表配置

- PVLAN ID：不同的 PVLAN, ID 必须不同，但没有要求一定要连续。
- 删除：勾选后下次保存时将删除对应 PVLAN。
- 添加新的 PVLAN：增加一个新的 PVLAN，PVLAN ID 需要手工填写。
- 如上配置，端口组 1（1，2，3，4）和端口组 2（5，6，7，8）相互隔离。

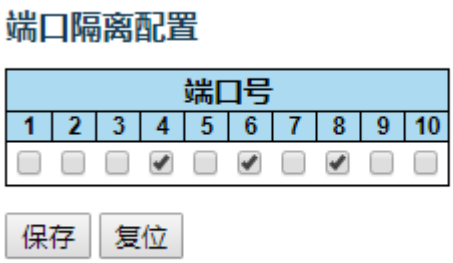
15.2 端口隔离

端口隔离功能将端口分为两种角色，隔离端口和非隔离端口。

- 隔离端口与隔离端口：隔离
- 隔离端口与非隔离端口：互通
- 非隔离端口与非隔离端口：互通

在【导航栏】下拉菜单中选择：配置->私有 VLAN->端口隔离，进入配置页面。

图表 15-2 端口隔离配置



如上图所示，勾选的端口作为隔离端口，未勾选的端口作为非隔离端口，默认情况，所有端口均为非隔离端口。

15.3 CLI 参考命令

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

命令	switch(config-if)# pvlan 2 switch(config-if)# no pvlan 2 switch(config-if)# pvlan isolation switch(config-if)# no pvlan isolation
描述	配置端口加入 PVLAN(PVLAN 关联第一个端口时自动创建)； 配置端口退出 PVLAN(PVLAN 不存在关联端口时自动删除)； 配置端口开启 PVLAN 端口隔离； 配置端口关闭 PVLAN 端口隔离；

16 QOS

16.1 QOS 概述

QoS（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力。

传统网络采用“尽力而为”的转发机制，当网络带宽充裕的时候，所有的数据流都得到了较好的处理，当网络发生拥塞的时候，所有的数据流都有可能被丢弃。为满足不同应用不同服务质量的要求，需要网络能根据用户的要求分配和调度资源，对不同的数据流提供不同的服务质量。

支持 QoS 功能的设备，能够提供传输品质服务，针对某种类别的数据流，可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。

配置了 QoS 的网络环境，增加了网络性能的可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

下面对 QOS 中部分常用术语进行说明:

CoS：Class Of Service 缩写，端口为报文打的优先级标记，与报文队列选择对应。

DPL：Drop Precedence Level 缩写，丢弃级别，也称丢弃优先级。交换机服务参数中的一个参数，取值为 0、1、或 2。为报文分配丢弃级别也称为报文着色，丢弃级别为 2 的报文为红色报文，1 为黄色报文，0 为绿色报文。丢弃级别主要在发生拥塞后交换机需要丢弃报文时使用

PCP：Priority Code Point 缩写，802.1Q 的 VLAN Priority 字段。

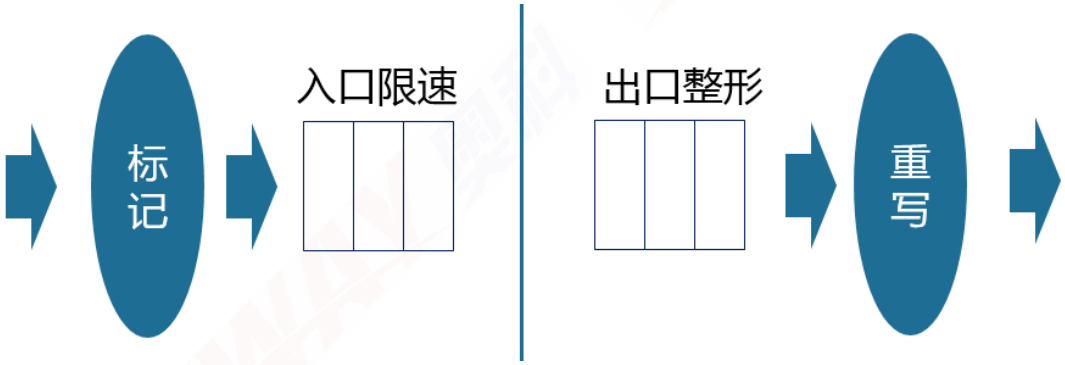
DEI： Drop Eligible Indicator 缩写，802.1Q 的 VLAN CFI 位。

DSCP：Differentiated Services Code Point 缩写，差分服务代码点，RFC 2474 中对 TOS 进行的新的定义，使用 6 个 bit 表示优先级关系，DSCP 的值得范围为 0-63。

16.2 QOS 工作原理

QOS 工作流程从报文进入端口开始，到报文从另一端口发出结束，中间经历了入口标记、入口限速、出口整形、出口重写等流程。

图表 16-1 QOS 工作原理



■ 入口标记

QOS 的入口标记支持基于 DSCP 的入口标记以及基于非 DSCP 的入口标记。当满足下面情况时，入口报文基于 DSCP 标记：

- QOS 准入端口分类，端口选中“基于 DSCP”。
- 基于 DSCP 的 QOS，选中信任基于 DSCP 标记的数值。
- 入口报文为 IPv4 报文，带 DSCP 字段。

对于非 DSCP 的入口标记

若配置使能标签分类，且入口报文带 TAG，则根据报文的 PCP/DEI 字段与 CoS/DPL 的映射关系，标记 CoS，选择入口队列；若配置关闭标签分类，且入口报文带 TAG，则采用报文自带 Cos/DPL 作为标记，选择入口队列；若报文不带 TAG，则采用端口默认 CoS/DPL 作为标记，选择入口队列。

若端口 DSCP 的准入配置，使能分类功能，则标记阶段将根据 DSCP 分类中的 QoS 分类到 DSCP 映射关系，重新标记 DSCP 值。

对于 DSCP 的入口标记

支持 DSCP 到 DSCP 的映射转换，转换结果再进行 DSCP 到 CoS 的映射转换，作为标记输出。

■ 入口限速

入口限速包括入口端口限速与入口队列限速。报文根据标记的 CoS 进入对应的入口队列，队列限速值应小于端口限速。

■ 出口整形

出口整形包括出口队列整形、出口队列调度、出口端口整形。报文根据标记的 CoS 进入出口队列，首先进行单队列整形，然后 0-5 这 6 个队列，需根据调度模式与队列权重，进行出口队列调度，最后统一进行出口端口整形。

■ 重写

重写部分主要为修改报文 TAG 的 PCP/DEI 字段以及报文的 DSCP 字段内容。

对 PCP/DEI 的重写，支持 Classified、Default、Mapped 三种方式。

Classified 根据端口分类结果重写，如不带 TAG 的报文采用默认 PCP/DEI，带 TAG 报文采用报文的 PCP/DEI；

Default 强制写入配置值；

Mapped 在标记的 CoS/DPL 基础上，根据配置的 CoS/DPL 与 PCP/DEI 映射关系再进行一次映射。

对报文 DSCP 的重写，支持 Disabled、Enable、Remap 三种方式。

Disabled 保持报文原 DSCP 值不变；

Enable 支持入口标记的修改结果；

Remap，在入口标记的基础上，根据配置再进行一次映射。

16.3 配置 QOS

16.3.1 端口分类

在【导航栏】下拉菜单中选择：配置->QOS->端口分类，进入配置界面。

图表 16-2 QOS 端口分类配置

配置项	说明
端口	面板端口号
Cos/DPL	端口默认 Cos/DPL 值
PCP/DEI	端口默认 PCP/DEI 值
标签分类	使能对带 TAG 的报文，用报文 TAG 中 PCP/DEI 字段，映射生成 CoS/DPL
基于 DSCP	使能端口基于 DSCP 分类
地址模式	选择 Qos 控制列表分类依据，Source 基于 SMAC/SIP，Destination 基于 DMAC/DIP 分类

16.3.2 端口策略

在【导航栏】下拉菜单中选择：配置->QOS->端口策略，进入配置界面。

图表 16-3 QOS 端口策略配置

QoS准入端口策略

端口	启用	速率	单位	流控
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐

配置项	说明
端口	面板端口号
启用	使能限速端口策略
速率	与单位组合，bps、fps 范围为 100-3276700，kbps、kfps 为 1-32767
单位	支持 bps、kbps、fps、kfps 四种单位
流控	使能端口限速流控，若端口流控开启，发送 pause 报文，过限速报文不丢弃

16.3.3 队列策略

在【导航栏】下拉菜单中选择：配置->QOS->队列策略，进入配置界面。

图表 16-4 QOS 队列策略配置

QoS准入队列策略

端口	队列 0			队列 1	队列 2	队列 3	队列 4	队列 5	队列 6	队列 7
	E	速率	单位	启用	启用	启用	启用	启用	启用	启用
*	☐	500	<>	☐	☐	☐	☐	☐	☐	☐
1	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
2	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
3	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
4	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
5	☑	500	kbps	☐	☐	☐	☐	☐	☐	☐
6	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
7	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
8	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
9	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
10	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐

配置项	说明
端口	面板端口号
E	使能端口队列入口限速策略
队列 0-7	限速值，范围 100-3276700bps，或 1-32767kbps

16.3.4 端口调度

在【导航栏】下拉菜单中选择：配置->QOS->端口调度，进入配置界面。

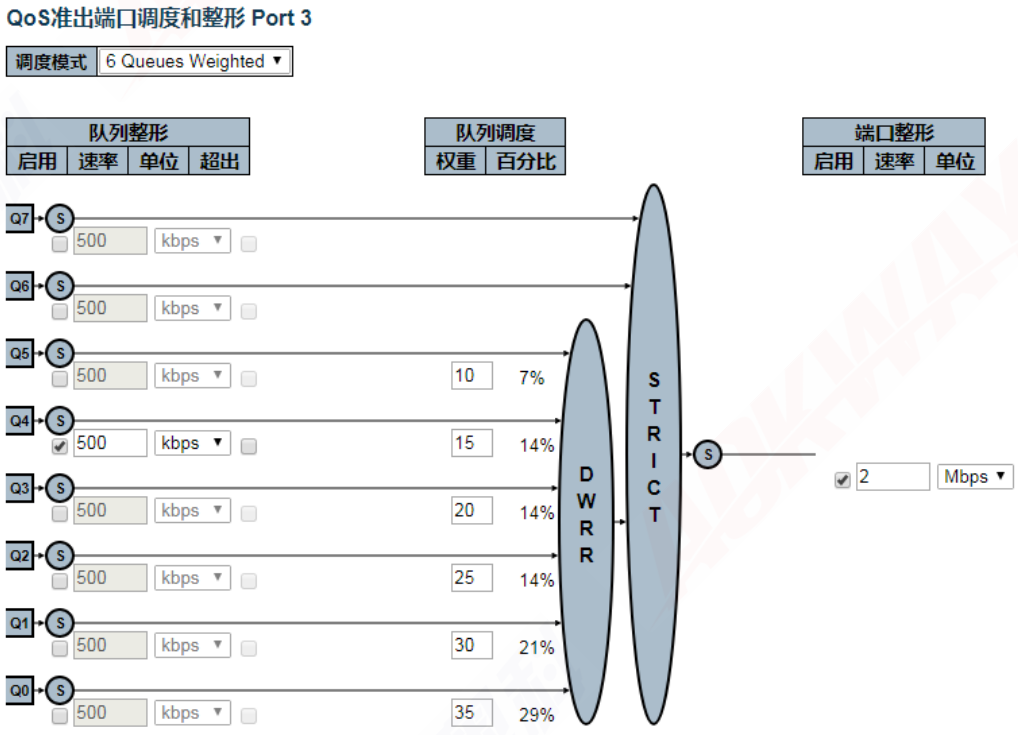
图表 16-5 QOS 端口调度配置

QoS准出端口调度

端口	模式	权重					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	6 Queues Weighted	29%	21%	14%	14%	14%	7%
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

配置项	说明
端口	面板端口号，点击进入端口准出调度整形配置界面
模式	支持 Strict Priority 与 6 Queues Weighted 两种模式
权重 0-6	出口队列权重，在模式 6 Queues Weighted 时有效

图表 16-6 QOS 端口调度和整形配置



配置项	说明
调度模式	支持 Strict Priority 与 6 Queues Weighted 两种模式
队列整形	基于队列使能控制，范围 100-3281943kbps，或 1-3281Mbps，支持使能队列使用超出带宽

队列调度	配置队列权重，范围 1-100，6 个队列根据配置重新计算队列占比
端口整形	基于端口使能控制，范围 100-3281943kbps，或 1-3281Mbps

16.3.5 端口整形

在【导航栏】下拉菜单中选择：配置->QOS->端口整形，进入配置界面。

图表 16-7 QOS 端口整形配置

QoS准出端口整形

端口	整形器								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	端口
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	500 kbps	-	-	-	2 Mbps
4	-	-	-	-	500 kbps	-	-	-	2 Mbps
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-

配置项	说明
端口	面板端口号，点击进入端口准出调度整形配置界面
整形器/Q0-Q7	队列整形限速
整形器/端口	端口限速值

16.3.6 端口标签

在【导航栏】下拉菜单中选择：配置->QOS->端口标签，进入配置界面。

图表 16-8 QOS 端口标签配置

QoS准出端口标签重设

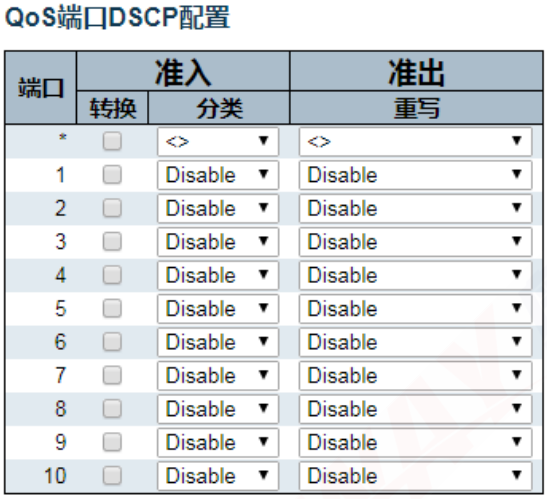
端口	模式
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

配置项	说明
端口	面板端口号，点击进入模式配置界面
模式	Classified 模式在出口不做变更； Default 模式采用默认配置的 PCP/DEI 数值 Mapped 根据 QOS/DP 与 PCP/DEI 的映射关系，修改 PCP/DEI 数值

16.3.7 端口 DSCP

在【导航栏】下拉菜单中选择：配置->QOS->端口 DSCP，进入配置界面。

图表 16-9 QOS 端口 DSCP 配置



配置项	说明
端口	面板端口号
准入/转换	使能准入转换功能，具体配置在“DSCP 转换配置界面”
准入/分类	支持 Disable、DSCP=0、Selected、ALL 四种分类方式，Disable 表示不支持分类；DSCP=0 表示仅支持 DSCP=0 的报文分类；Selected 表示仅支持 DSCP 转换配置页面中选择的项进行分类；表示对所有 DSCP 数值分类
准出/重写	准出重写报文 DSCP 内容，支持 Disable、Enable、Remap DP Unware、Remap DP Aware 四种方式，Disable 表示不支持重写；Enable 表示支持重写，但不支持 DSCP 转换准出映射；Remap DP Unware 表示根据 DSCP 转换准出 DP0 表重写；Remap DP Aware 表示根据 DSCP 转换准出 DP0/DP1 表重写

16.3.8 基于 DSCP 的 Qos

在【导航栏】下拉菜单中选择：配置->QOS->基于 DSCP 的 Qos，进入配置界面。

图表 16-10 基于 DSCP 的 QOS 分类配置

基于DSCP的QoS准入分类

DSCP	信任	QoS分类	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0

配置项	说明
DSCP	DSCP 值，范围 0-63
信任	使能信任某具体 DSCP 数值
QOS 分类	QOS 分类值，范围 0-7
DPL	DPL 数值，范围 0-1

16.3.9 DSCP 转换

在【导航栏】下拉菜单中选择：配置->QOS->DSCP 转换，进入配置界面。

图表 16-11 QOS DSCP 转换配置

DSCP转换

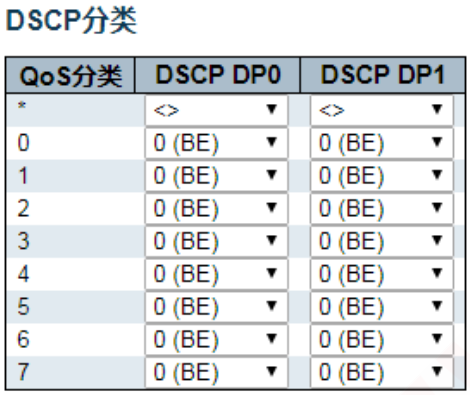
DSCP	准入		准出	
	转换	分类	重新映射 DP0	重新映射 DP1
*	<>	☐	<>	<>
0 (BE)	0 (BE)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)

配置项	说明
DSCP	DSCP 值，范围 0-63
转入/转换	DSCP to DSCP 转换配置，范围 0-63
准入/分类	使能准入基于 DSCP 分类
准出/重新映射 DP0	DP=0 的准出映射关系
准出/重新映射 DP1	DP=1 的准出映射关系

16.3.10 DSCP 分类

在【导航栏】下拉菜单中选择：配置->QOS->DSCP 分类，进入配置界面。

图表 16-12 QOS DSCP 分类配置

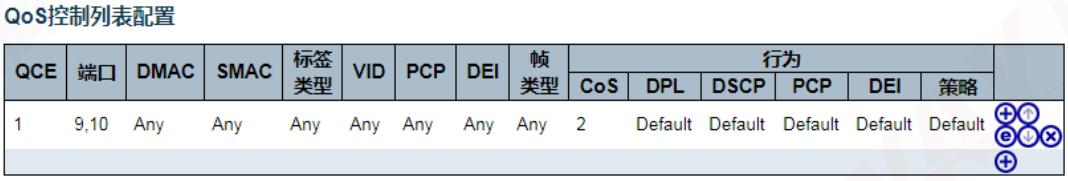


配置项	说明
QOS 分类	QOS 分类，范围 0-7
DSCP DP0	DP=0 时 COS to DSCP 转换配置，范围 0-63
DSCP DP1	DP=1 时 COS to DSCP 转换配置，范围 0-63

16.3.11 Qos 控制列表

在【导航栏】下拉菜单中选择：配置->Qos->QOS 控制列表，进入配置界面。

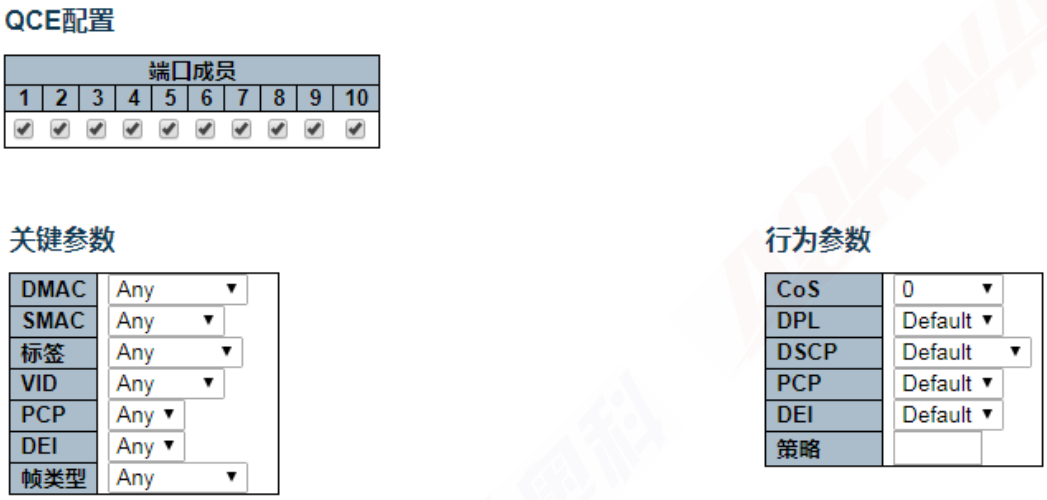
图表 16-13 QOS 控制列表配置



显示 QCE 的简要信息，支持 QCE 表项上、下移动、前面添加、后面添加、删除、编辑操作。

点击下添加按键，进入 QCE 创建界面。

图表 16-14 QCE 配置



配置项	子项	说明
端口成员	-	面板端口号，支持选择多个端口，默认选择所有端口
关键参数	DMAC	支持 Any、Unicast、Multicast、Broadcast 选项
	SMAC	支持 Any、Specific 选项
	标签	支持 Any、Untagged、Tagged、C-Tagged：带 C-tagged、S-Tagged 选项
	VID	支持 Any、Specific、Range 选项
	PCP	支持 Any、 0-7 组合选项
	DEI	支持 Any、0、1 选项
	帧类型	支持 Any、EtherType、LLC、SNAP、IPv4、IPv6 选项
行为参数	CoS	QOS 分类，范围 0-7
	DPL	Default：不变 0-7：目标数值
	DSCP	Default：不变 0-63：目标数值
	PCP	Default：不变 0-7：目标数值
	DEI	Default：不变 0-1：目标数值
	策略	保留

16.3.12 风暴控制

在【导航栏】下拉菜单中选择：配置->QOS->风暴控制，进入配置界面。

图表 16-15 风暴控制配置

全局风暴策略配置

帧类型	启用	速率	单位
单播	☐	1	fps
组播	☐	1	fps
广播	☐	1	fps

配置项	说明
帧类型	支持广播、组播、单播选择
启用	使能该类型帧风暴控制功能
速率	基于报文个数限速，范围 1-1024000fps，或 1-1024kfps
单位	支持 fps、kfps 两种选择

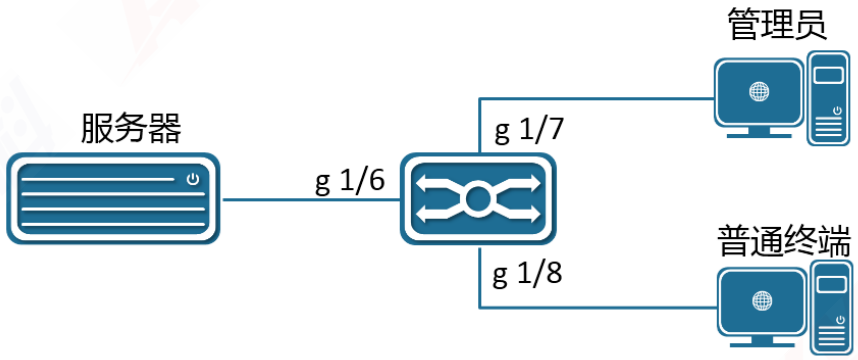
16.4 QOS 典型配置案例

16.4.1 优先转发服务

■ 案例需求

下图是常见办公网络，服务器因性能问题，入口限速 10Mbits，要求在业务繁忙时，管理员能正常范文服务器。

图表 16-16 QOS 案例



■ 操作步骤

配置 7 口标志优先级为 3，8 口标志优先级为 0。

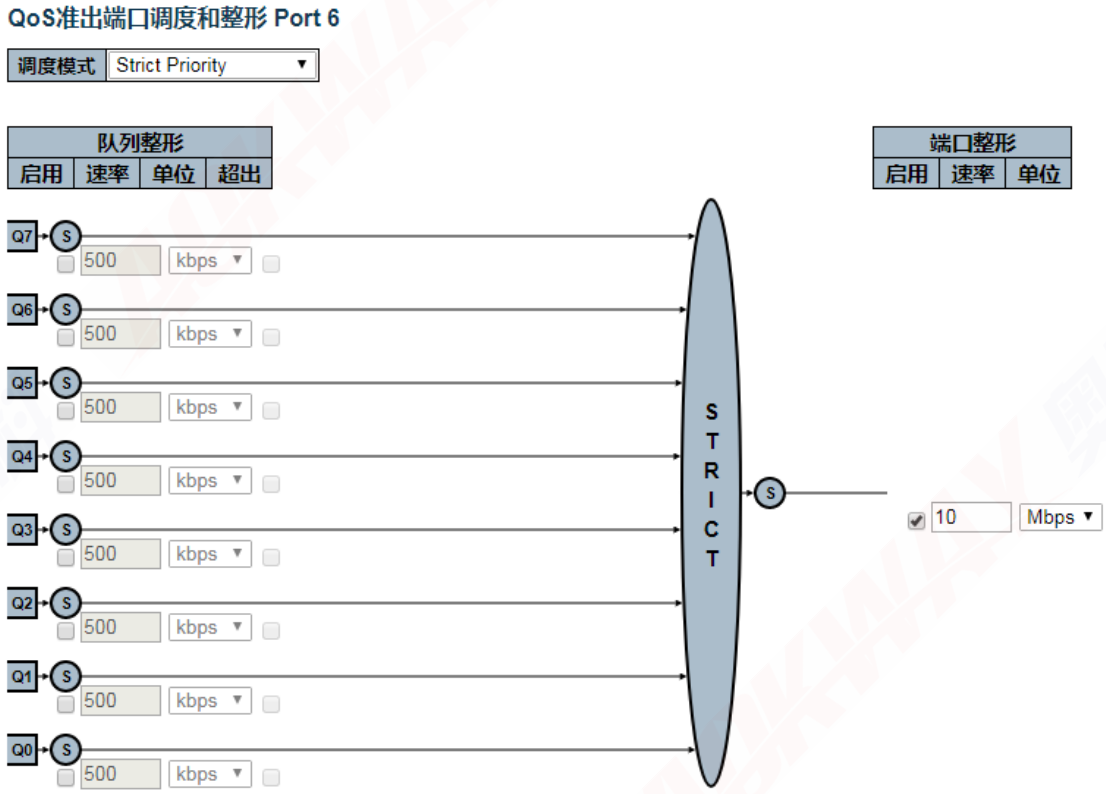
图表 16-17 QOS 案例端口分类配置

QoS准入端口分类

端口	CoS	DPL	PCP	DEI	标签分类	基于DSCP	地址模式
*	<>	<>	<>	<>			<>
1	0	0	0	0	Disabled		Source
2	0	0	0	0	Disabled		Source
3	0	0	0	0	Disabled		Source
4	0	0	0	0	Disabled		Source
5	0	0	0	0	Disabled		Source
6	0	0	0	0	Disabled		Source
7	3	0	0	0	Disabled		Source
8	0	0	0	0	Disabled		Source
9	0	0	0	0	Disabled		Source
10	0	0	0	0	Disabled		Source

配置 6 口出口整形，速率 10Mbits，配置调度方式为严格优先级调度。

图表 16-18 QOS 案例端口调度和整形配置



16.4.2 风暴控制

■ 案例需求

设备广播风暴抑制，要求广播报文不超过 1000kfps。

■ 操作步骤

进入风暴控制配置界面，启用广播帧，设置限制速率。

图 11-19 风暴控制案例配置

全局风暴策略配置

帧类型	启用	速率	单位
单播	☐	1	fps
组播	☐	1	fps
广播	☑	1000	kfps

17 端口镜像

17.1 镜像概述

SPAN (Local Switched Port Analyzer) 为本地镜像功能。SPAN 功能将指定端口的报文复制到目的端口，一般 SPAN 目的端口会接入数据检测设，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。

⚠ 注意

当端口配置成镜像目的口时，端口处于 block 状态，丢弃所有输入报文。请勿将管理端口配置成镜像目的口，避免出现远程连接断开情况。

17.2 配置镜像

在【导航栏】下拉菜单中选择：配置->镜像，进入镜像会话界面。

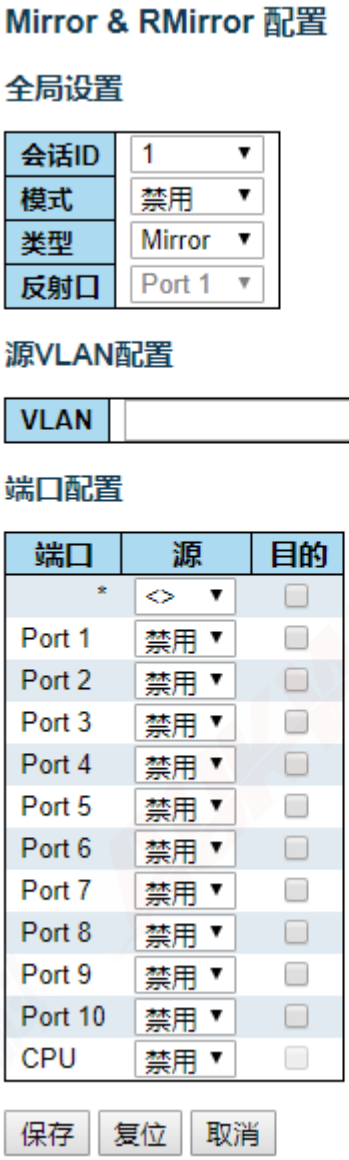
图表 17-1 镜像会话

Mirror & RMirror配置表

会话ID	模式	类型	VLAN	反射口
1	禁用	Mirror	-	-

当前系列产品只支持一个会话，如上图点击对应会话 ID，进入镜像配置界面。

图表 17-2 镜像配置



- 全局设置

  当前系列只支持模式配置。

  - 禁用：禁用当前镜像会话，默认为禁用。
  - 启用：启用当前镜像会话。

- 源 VLAN 设置

  支持“,”和“-”两种格式，“,”表示多个配置段，每个配置段可以是单个 vlan，也可以是通过“-”表示的一个 vlan 范围。比如“10-13”表示 vlan10，11，12，13 这 4 个 vlan。

  源 VLAN 设置的 VLAN 的流量将会镜像到镜像目的口。

- 端口设置

配置项	说明

端口	面板端口号以及 CPU 口
源	选择镜像模式。 禁用：发送的帧和接收的帧都不会被镜像。此为 默认模式。 双向：接收到的帧和发送的帧在目标端口上进行镜像。 输入：此端口接收的帧镜像的目的端口。发送的帧不镜像。 输出：在此端口上发送的帧在目标端口上进行镜像。接收的帧不镜像。
目的	勾选上表示该端口为镜像目的口，只能有一个端口作为镜像目的口。

注意：1，基于端口的镜像和基于 VLAN 的镜像不能同时配置，如果有配置基于 VLAN 的镜像，基于端口的镜像配置将会被禁止；如果有配置基于端口的镜像，再配置基于 VLAN 的镜像，基于端口的镜像配置将会被取消。

2，如果端口被配置为镜像目的口，则该端口的“源”配置只能为“禁用”或者“输入”，如果之前有配置为“双向”或者“输出”，则该端口作为进行目的将禁止被勾选。

17.3 CLI 参考命令

命令	switch(config)# monitor session 1 switch(config)# no monitor session 1 switch(config)# monitor session 1 source vlan 20 switch(config)# no monitor session 1 source vlan 20 switch(config)# monitor session 1 source cpu tx switch(config)# no monitor session 1 source cpu tx switch(config)# monitor session 1 source interface GigabitEthernet 1/1-2,5 both switch(config)# no monitor session 1 source interface GigabitEthernet 1/2 rx switch(config)# monitor session 1 destination interface GigabitEthernet 1/8 switch(config)# no monitor session 1 destination interface GigabitEthernet 1/8
描述	配置镜像启用; 配置镜像关闭; 配置镜像源 VLAN 添加; 配置镜像源 VLAN 删除; 配置镜像源端口添加 Cpu 口及方向; 配置镜像源端口删除 Cpu 口及方向; 配置镜像源端口添加面板口及方向; 配置镜像源端口删除面板口及方向; 配置镜像目的端口添加; 配置镜像目的端口删除;

18 GVRP

GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）是 GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用，GARP 提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息（如 VLAN、组播地址等）。GARP 本身不作为一个实体存在于设备中，遵循 GARP 协议的应用实体称为 GARP 应用，GVRP 就是 GARP 的一种应用。

GVRP 基于 GARP 的工作机制，维护设备中的 VLAN 动态注册信息，并传播该信息到其它的设备中。设备启动 GVRP 特性后，能够接收来自其它设备的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个端口到达等。而且设备能够将本地的 VLAN 注册信息向其它设备传播，以便使同一局域网内所有设备的 VLAN 信息达成一致。GVRP 传播的 VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

18.1 全局配置

在【导航栏】下拉菜单中选择：配置->GVRP->全局，进入配置页面。

图表 18-1 GVRP 全局配置

- 使能 GVRP

  默认全局关闭 GVRP，勾选上全局开启 GVRP。

- GVRP 协议定时器
  - 加入超时：单位为厘秒（即 0.01 秒），范围为 1-20，默认值为 20。
  - 离开超时：单位为厘秒，范围为 60-300，默认值为 60。
  - 所有离开超时：单位为厘秒，范围为 1000-5000，默认值为 1000。
- 最大 VLAN 数

  使能 GVRP 后，GVRP 支持的最大 VLAN 数。默认值为 20. 该参数只能在关闭 GVRP 时更改。

18.2 端口配置

在【导航栏】下拉菜单中选择：配置->GVRP->端口，进入配置页面。

图表 18-2 GVRP 端口配置

基于交换机面板端口使能或者禁用 GVRP，默认全部端口都禁用。只有当全局和端口均使能 GVRP，在该端口上才会运行 GVRP 协议。

18.3 CLI 参考命令

命令	switch(config)# gvrp switch(config)# no gvrp switch(config)# gvrp time join-time 20 leave-time 60 leave-all-time 1000 switch(config)# gvrp max-vlans 20
描述	配置 GVRP 启用； 配置 GVRP 关闭； 配置 GVRP 加入超时、离开超时以及所有离开超时时间； 配置 GVRP 最大 VLAN 数；

命令	switch(config)# interface GigabitEthernet 1/3
描述	进入配置端口；

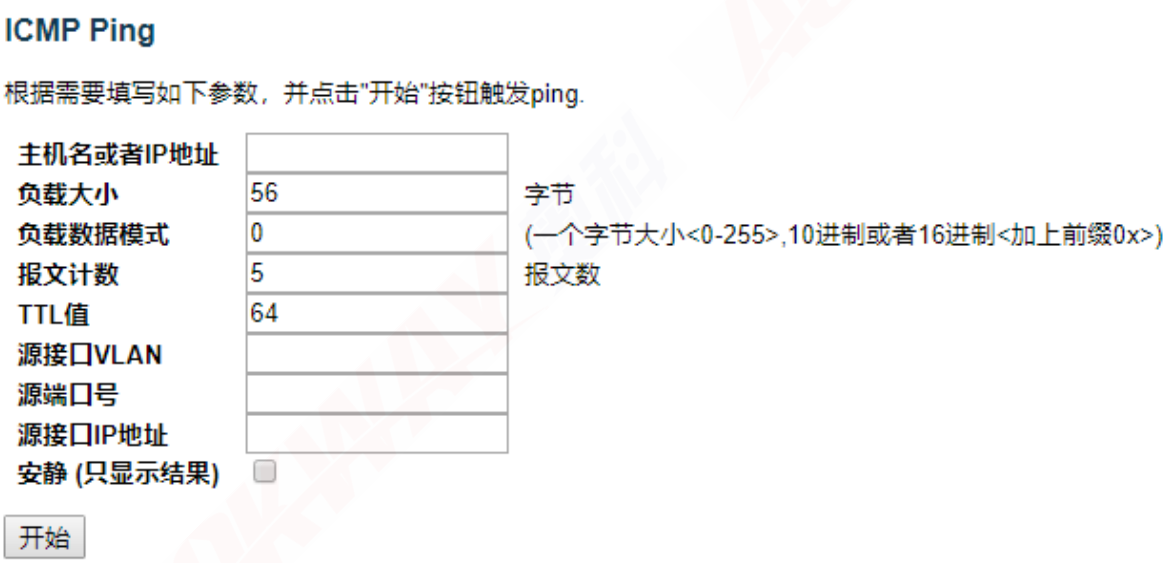
命令	switch(config-if)# gvrp switch(config-if)# no gvrp
描述	配置端口 GVRP 启用； 配置端口 GVRP 关闭；

19 诊断

19.1 Ping(IPv4)

在【导航栏】下拉菜单中选择：诊断->Ping(IPv4)，进入诊断界面。

图表 19-1 ping(IPv4)诊断



配置项	说明
主机名或者 IP 地址	目标主机的地址，可以是符号主机名，也可以是 IP 地址。（不支持 DNS，只能是 IP 地址）
负载大小	确定 ICMP 数据有效负载的大小（以字节为单位）（不包括以太网，IP 和 ICMP 头的大小）。默认值为 56 个字节。有效范围是 2-1452 字节。
负载数据模式	确定 ICMP 数据有效内容中使用的模式（即报文填充内容）。默认值为 0.有效范围为 0-255。
报文计数	确定发送的 PING 请求数。默认值为 5.有效范围为 1-60。
TTL 值	确定 IPv4 报文头中的 TTL 字段值。默认值为 64.有效范围为 1-255。
源接口 VLAN	此字段可用于强制测试使用特定的本地 VLAN 接口作为源接口。将此字段留空以根据路由配置自动选择。
源端口号	此字段可用于强制测试使用具有指定端口号的特定本地接口作为源接口。将此字段留空以根据路由配置自动选择。
源接口 IP 地址	此字段可用于强制测试使用具有指定 IP 地址的特定本地接口作为源接口。必须在本地接口上配置指定的 IP 地址。将此字段留空以根据路由配置自动选择。
安静	选中此选项不会打印每个 ping 请求的结果，只显示最终结果。

注意：源接口 VLAN，源端口号，源接口 IP 地址，三者最多配置一个（或者全部都不配置）。

点击“开始”按钮后进入 ping 诊断显示页面。

图表 19-2 ping(IPv4)诊断结果

Ping (IPv4) 输出

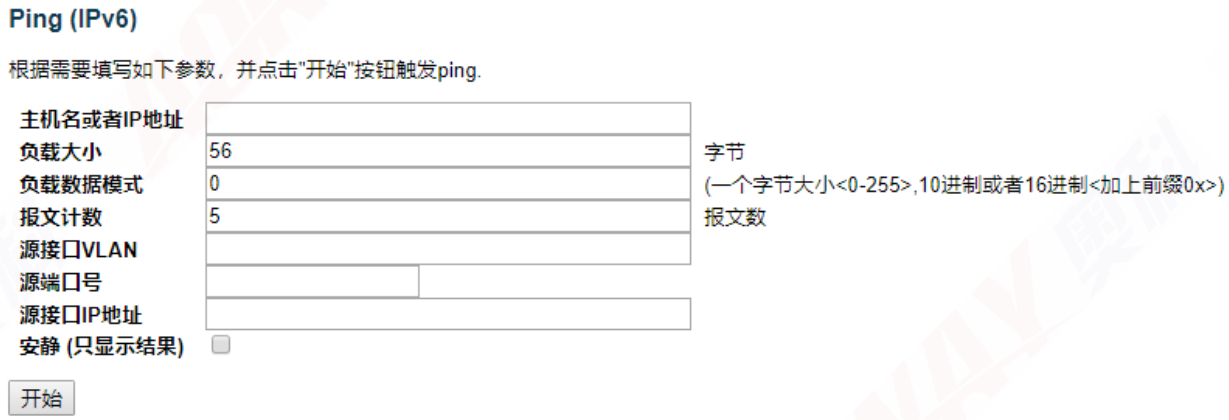
```
PING 192.168.200.1 (192.168.200.1) from 192.168.200.100: 56 data bytes
64 bytes from 192.168.200.1: seq=0 ttl=128 time=33.239 ms
64 bytes from 192.168.200.1: seq=1 ttl=128 time=62.183 ms
64 bytes from 192.168.200.1: seq=2 ttl=128 time=78.840 ms
64 bytes from 192.168.200.1: seq=3 ttl=128 time=52.398 ms
64 bytes from 192.168.200.1: seq=4 ttl=128 time=331.399 ms

--- 192.168.200.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 33.239/111.611/331.399 ms

Ping session completed.
```

新Ping

19.2 Ping(IPv6)

在【导航栏】下拉菜单中选择：诊断->Ping(IPv6)，进入诊断界面。

图表 19-3 ping(IPv6)诊断



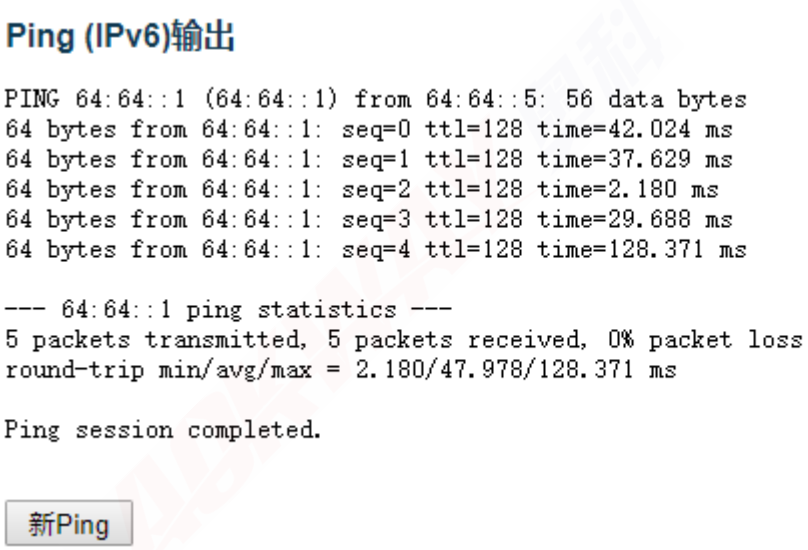
配置项	说明
主机名或者 IP 地址	目标主机的地址，可以是符号主机名，也可以是 IP 地址。（不支持 DNS，只能是 IP 地址）
负载大小	确定 ICMPv6 数据有效负载的大小（以字节为单位）（不包括以太网，IPv6 和 ICMPv6 头的大小）。默认值为 56 个字节。有效范围是 2-1452 字节。
负载数据模式	确定 ICMPv6 数据有效内容中使用的模式（即报文填充内容）。默认值为 0.有效范围为 0-255。
报文计数	确定发送的 PING 请求数。默认值为 5.有效范围为 1-60。
源接口 VLAN	此字段可用于强制测试使用特定的本地 VLAN 接口作为源接口。将此字段留空以根据路由配置自动选择。
源端口号	此字段可用于强制测试使用具有指定端口号的特定本地接口作为源接口。将此字段留空以根据路由配置自动选择。

源接口 IP 地址	此字段可用于强制测试使用具有指定 IP 地址的特定本地接口作为源接口。必须在本地接口上配置指定的 IP 地址。将此字段留空以根据路由配置自动选择。
安静	选中此选项不会打印每个 ping 请求的结果，只显示最终结果。

注意：源接口 VLAN，源端口号，源接口 IP 地址，三者最多配置一个（或者全部都不配置）。

点击“开始”按钮后进入 ping 诊断显示页面。

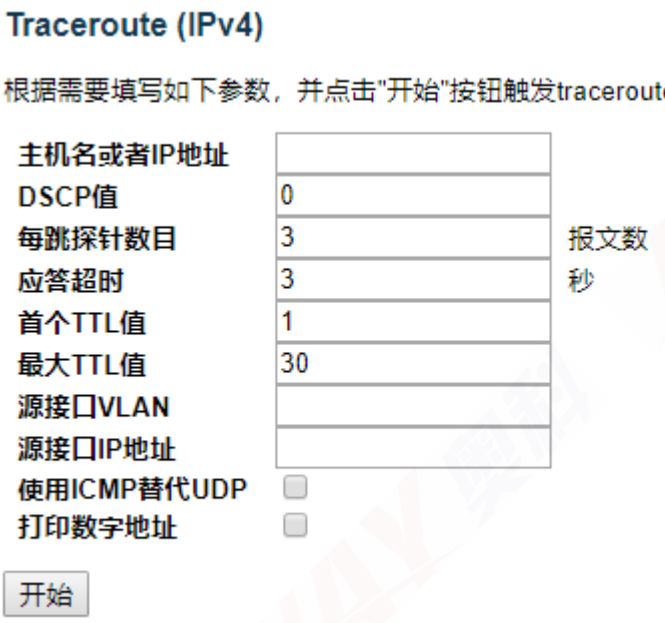
图表 19-4 ping(IPv6)诊断结果



19.3 Traceroute(IPv4)

在【导航栏】下拉菜单中选择：诊断->Traceroute(IPv4)，进入诊断界面。

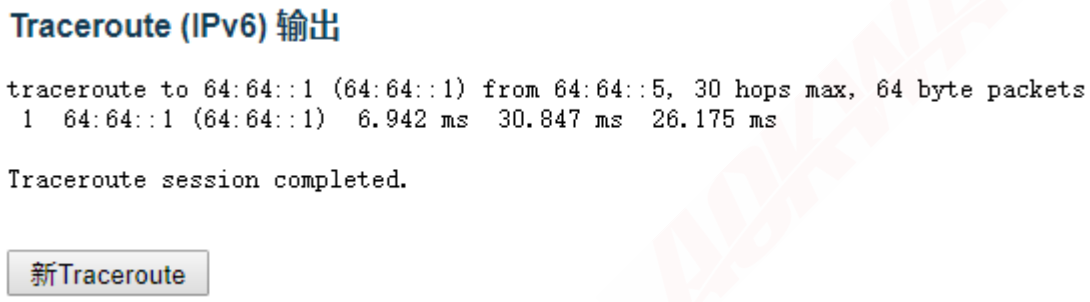
图表 19-5 Traceroute(IPv4)诊断



配置项	说明
主机名或者 IP 地址	目标主机的地址，可以是符号主机名，也可以是 IP 地址。（不支持 DNS，只能是 IP 地址）
DSCP 值	此值用于 IPv4 报文头中的 DSCP 值。默认值为 0.有效范围为 0-63。
每跳探针数目	确定为每跳发送的探针（数据包）的数量。默认值为 3.有效范围为 1-60。
应答超时	确定等待回复已发送请求的秒数。默认编号为 3.有效范围为 1-86400。
首个 TTL 值	确定发送的第一个数据包中 IPv4 报文头中的生存时间（TTL）字段的值。默认编号为 1.有效范围为 1-30。
最大 TTL 值	确定 IPv4 报文头中的生存时间（TTL）字段的最大值。如果在达到指定的远程主机之前达到此值，则测试将停止。默认编号为 30.有效范围为 1-255。
源接口 VLAN	此字段可用于强制测试使用特定的本地 VLAN 接口作为源接口。将此字段留空以根据路由配置自动选择。
源接口 IP 地址	此字段可用于强制测试使用具有指定 IP 地址的特定本地接口作为源接口。必须在本地接口上配置指定的 IP 地址。将此字段留空以根据路由配置自动选择。
使用 ICMP 替代 UDP	默认情况下，traceroute 命令将使用 UDP 数据包。选择此选项会强制它使用 ICMP ECHO 数据包。
打印数字地址	默认情况下，traceroute 命令将使用反向 DNS 查找为获取的主机 IP 地址打印出每条的相关信息。如果 DNS 信息不可用，这可能会降低显示速度。选择此选项将阻止反向 DNS 查找并强制 traceroute 命令改为打印数字 IP 地址。

点击“开始”按钮进入 traceroute 诊断显示页面。

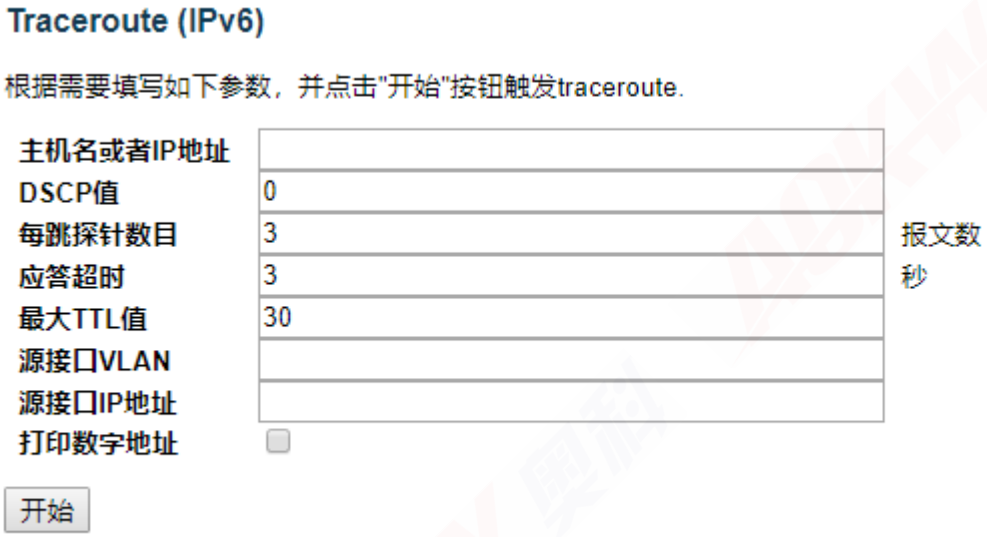
图表 19-6 Traceroute(IPv6)诊断结果



19.4 Traceroute(IPv6)

在【导航栏】下拉菜单中选择：诊断->Traceroute(IPv6)，进入诊断界面。

图表 19-7 Traceroute(IPv6)诊断



配置项	说明
主机名或者 IP 地址	目标主机的地址，可以是符号主机名，也可以是 IP 地址。（不支持 DNS，只能是 IP 地址）
DSCP 值	此值用于 IPv4 报文头中的 DSCP 值。默认值为 0.有效范围为 0-63。
每跳探针数目	确定为每跳发送的探针（数据包）的数量。默认值为 3.有效范围为 1-60。
应答超时	确定等待回复已发送请求的秒数。默认编号为 3.有效范围为 1-86400。
最大 TTL 值	确定 IPv6 报文头中的生存时间（TTL）字段的最大值。如果在达到指定的远程主机之前达到此值，则测试将停止。默认编号为 30.有效范围为 1-255。
源接口 VLAN	此字段可用于强制测试使用特定的本地 VLAN 接口作为源接口。将此字段留空以根据路由配置自动选择。
源接口 IP 地址	此字段可用于强制测试使用具有指定 IP 地址的特定本地接口作为源接口。必须在本地接口上配置指定的 IP 地址。将此字段留空以根据路由配置自动选择。
打印数字地址	默认情况下，traceroute 命令将使用反向 DNS 查找为获取的主机 IP 地址打印出每条的相关信息。如果 DNS 信息不可用，这可能会降低显示速度。选择此选项将阻止反向 DNS 查找并强制 traceroute 命令改为打印数字 IP 地址。

点击“开始”按钮进入 traceroute 诊断显示页面。

图表 19-8 Traceroute(IPv4)诊断结果

Traceroute (IPv4) 输出

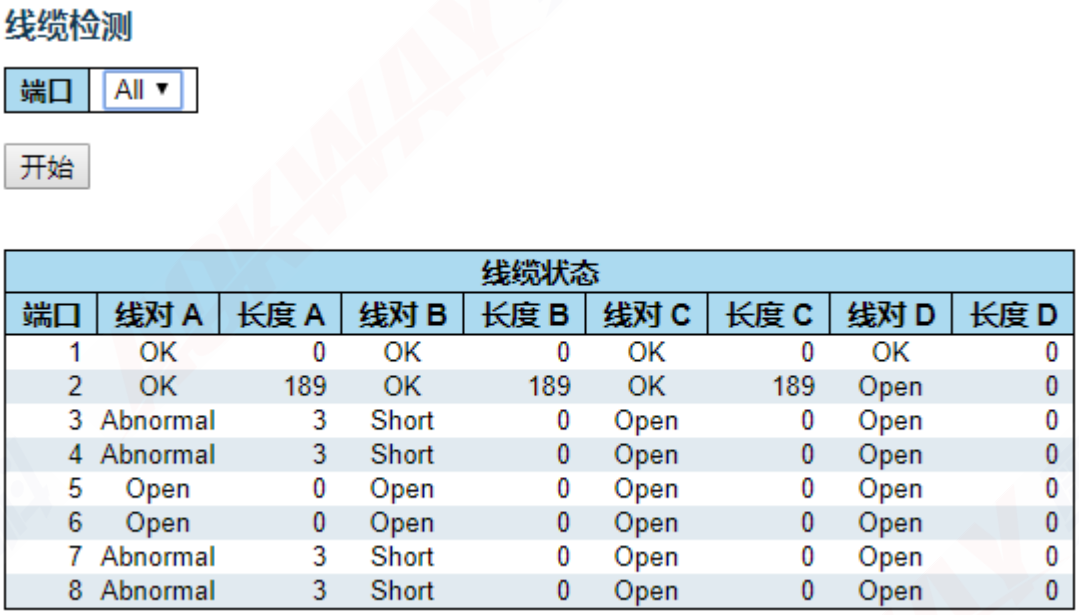
```
traceroute to 192.168.200.1 (192.168.200.1) from 192.168.200.100, 30 hops max, 38 byte packets
 1  192.168.200.1 (192.168.200.1)  29.525 ms  *  35.615 ms

Traceroute session completed.
```

新Traceroute

19.5 线缆检测

在【导航栏】下拉菜单中选择：诊断->线缆检测，进入配置界面。

图表 19-9 线缆检测



线缆状态								
端口	线对 A	长度 A	线对 B	长度 B	线对 C	长度 C	线对 D	长度 D
1	OK	0	OK	0	OK	0	OK	0
2	OK	189	OK	189	OK	189	Open	0
3	Abnormal	3	Short	0	Open	0	Open	0
4	Abnormal	3	Short	0	Open	0	Open	0
5	Open	0	Open	0	Open	0	Open	0
6	Open	0	Open	0	Open	0	Open	0
7	Abnormal	3	Short	0	Open	0	Open	0
8	Abnormal	3	Short	0	Open	0	Open	0

配置项	说明
端口	选择测试端口，选择 ALL 表示所有端口
线缆状态/端口	面板端口号
线缆状态/线对 A-D	线对状态有 Open、Short、OK、Cross 等
线缆状态/长度 A-D	线对长度，单位厘米

19.6 CLI 参考命令

命令	switch# ping ip 192.168.6.1 size 56 data 0 repeat 5 ttl 64 switch# ping ip 192.168.6.1 saddr 192.168.6.2 switch# ping ip 192.168.6.1 sif vlan 20 switch# ping ip 192.168.6.1 sif GigabitEthernet 1/2 switch# ping ip 192.168.6.1 quiet

描述	IPv4 ping 指定参数； IPv4 ping 指定源接口 IP 地址； IPv4 ping 指定源接口 VLAN； IPv4 ping 指定源端口号； IPv4 ping 安静模式；

命令	switch# ping ipv6 2001::1 size 56 data 0 repeat 5 switch# ping ipv6 2001::1 saddr 2001::2 switch# ping ipv6 2001::1 sif vlan 30 switch# ping ipv6 2001::1 sif GigabitEthernet 1/2 switch# ping ipv6 2001::1 quiet
描述	IPv6 ping 指定参数； IPv6 ping 指定源接口 IP 地址； IPv6 ping 指定源接口 VLAN； IPv6 ping 指定源端口号； IPv6 ping 安静模式；

命令	switch# traceroute ip 192.168.6.1 dscp 0 probes 3 timeout 3 firstttl 1 maxttl 30 switch# traceroute ip 192.168.6.1 saddr 192.168.6.2 switch# traceroute ip 192.168.6.1 sif vlan 20 switch# traceroute ip 192.168.6.1 sif GigabitEthernet 1/2 switch# traceroute ip 192.168.6.1 icmp switch# traceroute ip 192.168.6.1 numeric
描述	IPv4 traceroute 指定参数； IPv4 traceroute 指定源接口 IP 地址； IPv4 traceroute 指定源接口 VLAN； IPv4 traceroute 指定源端口号； IPv4 traceroute 使用 ICMP 替代 UDP； IPv4 traceroute 打印数字地址；

命令	switch# traceroute ipv6 2001::1 dscp 0 probes 3 timeout 3 maxttl 30 switch# traceroute ipv6 2001::1 saddr 2001::2 switch# traceroute ipv6 2001::1 sif vlan 20 switch# traceroute ipv6 2001::1 sif GigabitEthernet 1/2 switch# traceroute ipv6 2001::1 numeric
描述	IPv6 traceroute 指定参数； IPv6 traceroute 指定源接口 IP 地址； IPv6 traceroute 指定源接口 VLAN； IPv6 traceroute 指定源端口号； IPv6 traceroute 打印数字地址；

命令	switch# veriphy switch# veriphy interface GigabitEthernet 1/3
描述	线缆检测所有端口； 线缆检测指定端口；

20 维护

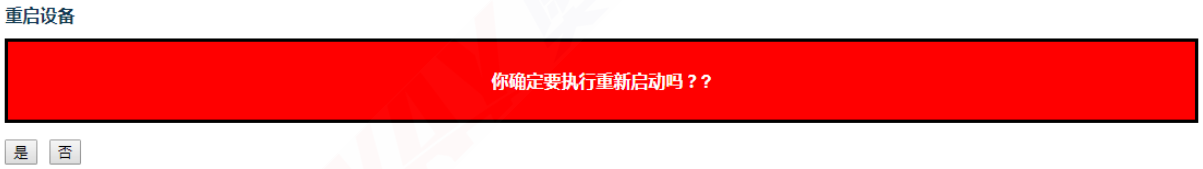
20.1 重启设备

注意

重启设备不会自动保存已修改的配置，需转到保存配置页面手动保存。

在【导航栏】下拉菜单中选择：维护->重启设备，进入配置界面。

图表 20-1 重启设备



点击“是”重启设备，点击“否”跳回到端口概况页面。

20.2 恢复出厂设置

在【导航栏】下拉菜单中选择：维护->恢复出厂设置，进入配置界面。

图表 20-2 恢复出厂设置

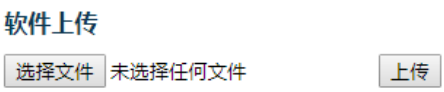
点击“是”设备还原到默认配置，点击“否”跳回到端口概况页面。

20.3 软件

20.3.1 升级

在【导航栏】下拉菜单中选择：维护->软件->升级，进入配置界面。

图表 20-3 软件升级



点击“选择文件”，选择本地程序文件，点击“上传”启动软件上传。

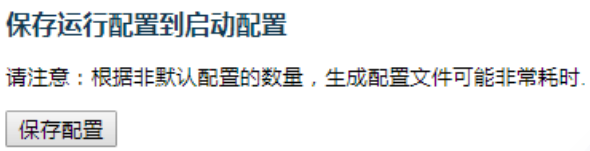
上传结束前，将重启设备以完成软件上传操作，若设备重启后管理 IP 与当前管理 IP 不一致，将出现无法回到该界面的情况。

20.4 配置

20.4.1 保存配置

在【导航栏】下拉菜单中选择：维护->配置->保存配置，进入配置界面。

图表 20-4 保存配置

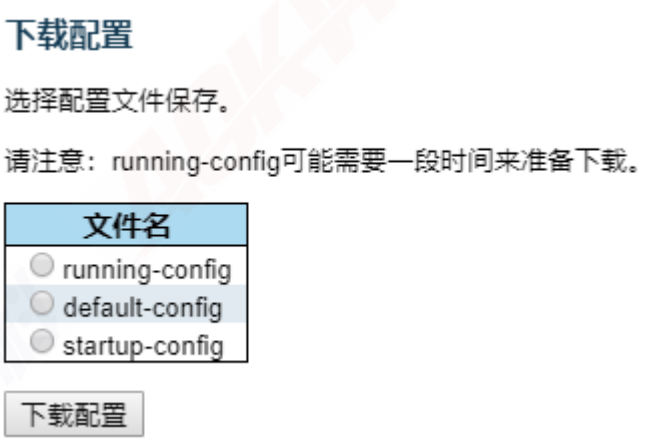


点击“保存配置”，页面将提示操作结果。

20.4.2 下载

在【导航栏】下拉菜单中选择：维护->配置->下载，进入配置界面。

图表 20-5 下载配置



running-config：系统当前配置信息，CLI 命令行显示。

default-config：设备出厂配置。

startup-config：上电默认配置，若执行“保存配置”，则为“保存配置”时系统配置信息。

20.4.3 上传

在【导航栏】下拉菜单中选择：维护->配置->上传，进入配置界面。

图表 20-6 上传配置

点击“选择文件”按键，选择要上传的本地文件。

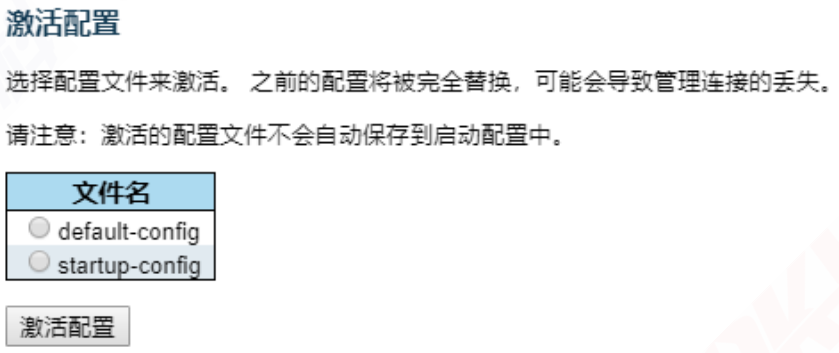
选择上传对象，若选择 running-config，支持 Replace 与 Merge 选项，其中 Replace 是直接替代系统当前文件，Merge 是合并到系统当前文件中。

点击上传配置，完成配置上传，页面将返回操作结果。

20.4.4 激活

在【导航栏】下拉菜单中选择：维护->配置->激活，进入配置界面。

图表 20-7 激活配置



选择文件名，点击“激活配置”，系统将根据选择的配置运行，当前系统配置不再存在。

20.4.5 删除

在【导航栏】下拉菜单中选择：维护->配置->删除，进入配置界面。

图表 20-8 删除配置

仅进行配置文件删除，不影响当前系统运行。

20.5 CLI 参考命令

命令	switch# reload cold
描述	重启设备；

命令	switch# reload defaults
描述	恢复出厂配置；

命令	switch# firmware upgrade http://192.168.6.183/is2500-release.mfi
描述	软件升级；

命令	switch# copy running-config startup-config switch# copy running-config tftp://192.168.6.183/running-config switch# copy flash:backup-config tftp://192.168.6.183/backup-config switch# copy tftp://192.168.6.183/running-config running-config switch# copy tftp://192.168.6.183/backup-config flash:backup-config switch# copy startup-config running-config switch# copy flash:backup-config running-config switch# delete flash:startup-config
描述	配置保存； 配置下载； 配置下载自定义文件； 配置上传； 配置上传自定义文件； 配置激活； 配置激活自定义文件； 配置删除；