交换机 Web 配置指南

本手册对应的软件版本为： Release 7.1.x

文档版本号：V4.0

发布时间：2024.03.25

1 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。Web 网管的运行环境如图 1-1 所示。

图 1-1 Web 网管运行环境

1.2 登录 Web 网管

用户首次登录 Web 网管时需要使用缺省账号进行登录，登录完成后为了确保设备的安全性，需要立即更改密码，具体操作步骤如下：

- 使用缺省账号登录 Web 网管
- 更改用户密码

说明

- 更改密码具体操作过程见用户管理 5.3 章节。

设备出厂时已经默认启用了 Web server 服务，并且有缺省的登录账号：用户名为 admin、登录密码为 admin，IP 地址为 192.168.56.166，用户可以使用这些信息完成 Web 网管的首次登录。

下面以 2GX8GT 交换机为例，介绍如何通过 Web 方式登录设备，具体步骤如下：

图 1-2 Web 登录界面

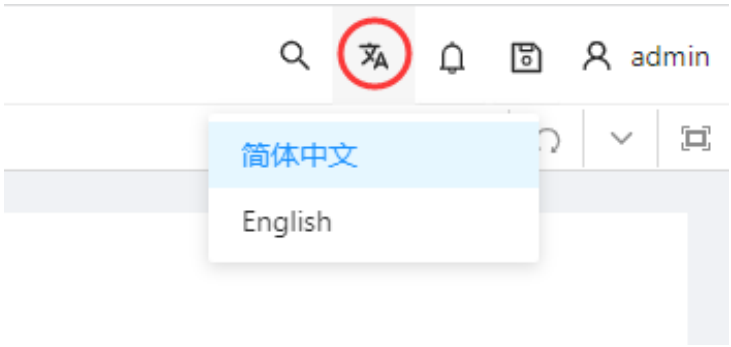
(1) 连接设备和 PC，用网线将 PC 和设备上的以太网口（缺省情况下，所有端口均属于 VLAN 1）相连。

(2) 为 PC 配置 IP 地址，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 192.168.56.20。

(3) 启动浏览器，输入登录信息 。

在 PC 上启动浏览器，在地址栏中输入“192.168.56.166”后回车，进入设备的 Web 登录页面，如图 1-2 所示。输入缺省账号“admin”、密码“admin”，单击【登录】按钮登录 Web 网管。系统会根据用户使用的操作系统语言来进行语言的自动选择，用户也可以进行手动切换（包括中文、English 两种），如图 1-3 所示。

图 1-3 语言切换界面



为了获得更好的显示效果，推荐使用 Edge、火狐 Firefox 或者 Chrome 浏览器，Chrome 浏览器请升级到最新版本。

1.3 Web 网管的退出

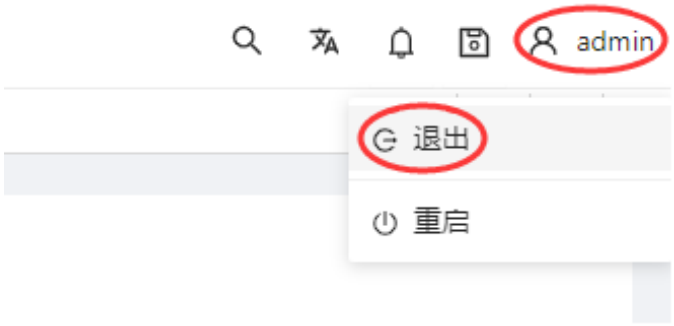
注意

- 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。

操作步骤：

单击 Web 网管页面右上角的用户图标按钮（如图 1-4 所示），在弹出的对话框里单击“退出”即可退出 Web 网管。

图 1-4 Web 网管的退出



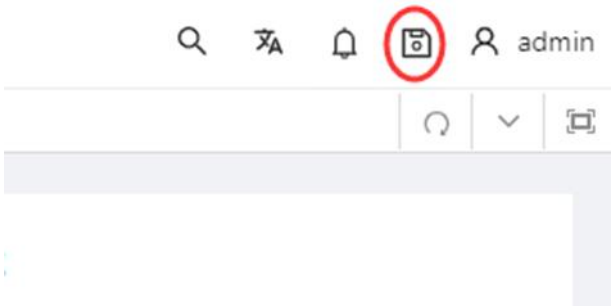
1.4 保存配置

注意

- 在页面上配置完所有项目后，请务必保存配置，否则未保存的配置信息会因为重启等操作而丢失。

单击 Web 网管页面右上角的保存图标按钮（如图 1-5 所示），即可将当前的配置保存到配置文件中，配置在重启或掉电重启后依然有效。

图 1-5 保存配置



保存配置有两种情况：

（1）在当前配置界面单击【确定】或【应用】按钮，即把当前的配置保存到内存中。此时的保存并不是把配置项真正的保存到配置文件中，若是此时交换机出现断电等故障时，则界面的配置失效。

（2）单击导航栏下方的【保存】按钮，则系统会自动的把所有的页面的配置保存到配置文件中。

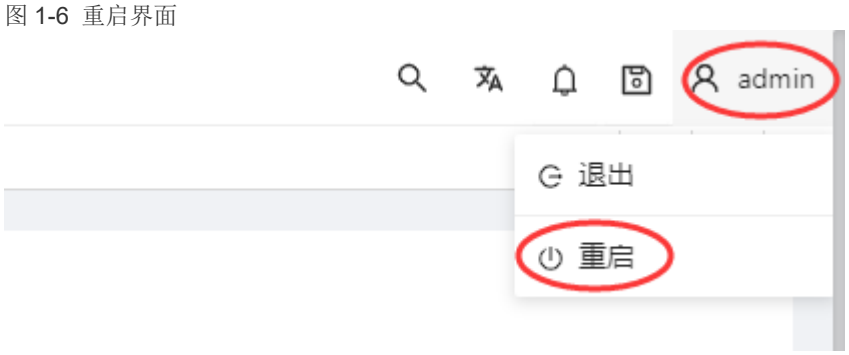
1.5 重启设备

注意

- 重启设备前请务必保存配置，否则重启后，未保存的配置将会全部丢失。
- 设备重启后，用户需重新登录设备。

步骤 1：单击 Web 网管页面右上角的用户图标按钮（如图 1-6 所示），在弹出的对话框里单击“重启”按钮。

图 1-6 重启界面



步骤 2：单击【确定】按钮或者等待倒计时结束，设备进入重启状态。设备重启需要一定时间，请耐心等待。

图 1-7 重启等待界面

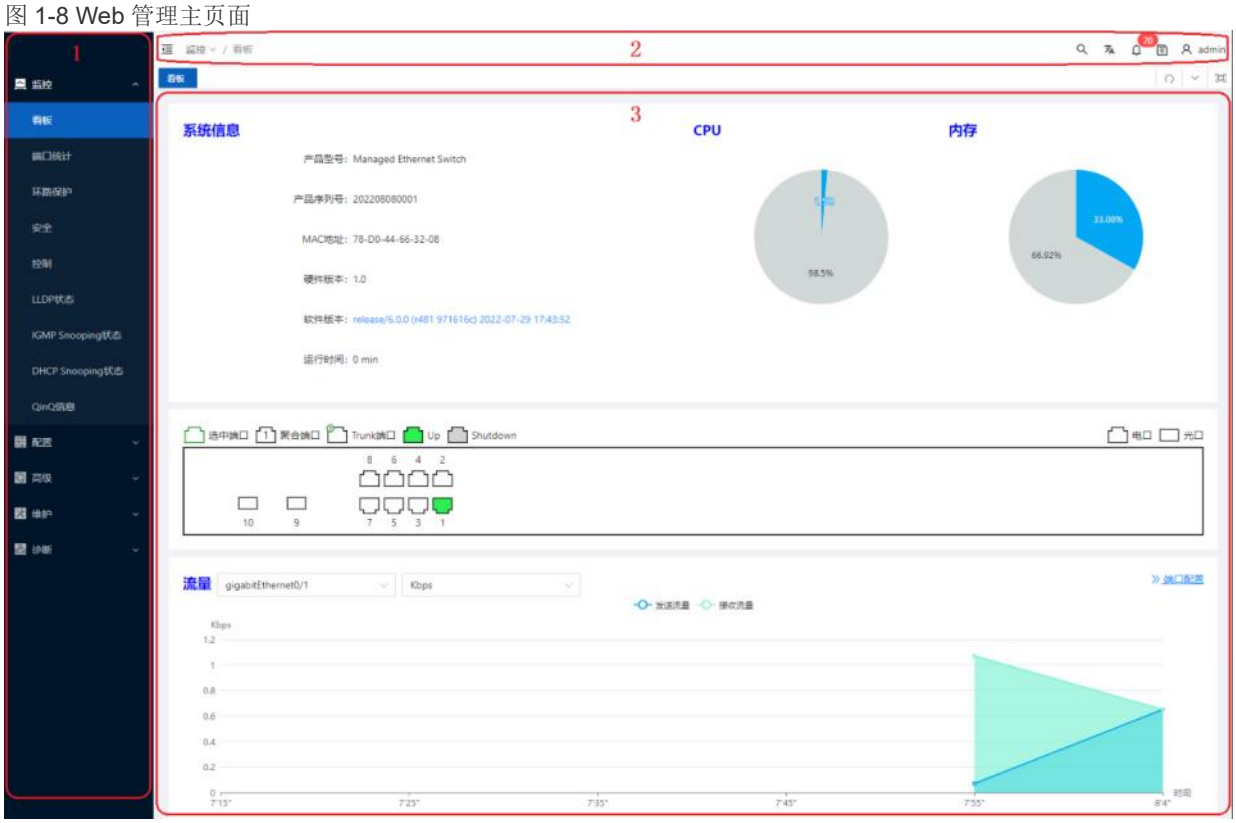
1.6 Web 管理页面布局介绍

如图 1-8 所示，Web 管理主页面共分为：导航栏、辅助区、配置区三部分，各部分功能描述如表 1-1 所示。

表 1-1 Web 布局说明

配置项	说明
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
辅助区	用于搜索、语言切换、告警信息提示、保存、退出、重启等操作。
配置区	用户进行配置和查看的区域

图 1-8 Web 管理主页面



（1）导航栏	（2）辅助区	（3）配置区

1.7 Web 管理功能介绍

Web 网管功能的具体说明如表 1-2 所示。

表 1-2 Web 网管功能说明

菜单/页签			功能说明
监控	概况		显示设备的 MAC 地址，序列号，软硬件版本， CPU 占用率，运行时间等状态，显示端口的 link 状态，端口的流量。
	端口统计		显示端口的计数
	环路保护		显示设备的环路保护状态
	安全		显示设备的安全类相关状态
	PoE 状态		显示设备 PoE 供电状态
	串口服务器状态		显示设备的串口服务器工作状态
	LLDP 状态		显示设备的 LLDP 工作状态
	IGMP Snooping 状态		显示设备 IGMP Snooping 状态
	DHCP Snooping 状态		显示设备 DHCP Snooping 状态
	QinQ 信息		显示设备 QinQ 状态
	环路检测状态		显示端口环路状态
	ARP 信息		显示端口 ARP 信息
配置	VLAN		新建、修改、删除 VLAN，配置端口属性、VLAN 归属
	端口	端口配置	设置端口的相关属性
		端口扩展	设置端口限速、风暴抑制、端口隔离
		端口镜像	设置/删除端口的镜像
		端口聚合	设置/删除聚合口
		端口违例	设置端口违例规则
	生成树		设置 STP、RSTP、MSTP 功能
	ERPS		设置 ERPS 单环，相切环，相交环
	PoE		设置 PoE 功率，非标模式，使能/关闭 PoE 端口供电
	安全	端口安全	配置、删除端口安全功能
		IP Source Guard	配置、删除 IP Source Guard 功能

		Dot1x	配置 802.1X 认证
		MAC 认证	配置 MAC 认证概况
		RADIUS	配置 RADIUS 服务器
	控制	串口服务器	配置串口服务器
		IO 控制	配置 DI，DO
	环路检测		配置端口环路检测功能
高级	二层	LLDP 配置	配置、删除设备的 LLDP 功能
		IGMP Snooping 配置	显示/配置 IGMP Snooping
		MAC 配置	配置设备的 MAC 地址管理模式
		DHCP Snooping 配置	配置设备的 DHCP Snooping 功能
		QinQ 配置	配置设备的 QinQ 功能
	安全	ACL 配置	配置设备的 ACL 功能
		Qos 配置	配置设备的 Qos 功能
	路由	静态 ARP	配置静态 ARP
		路由	配置静态路由
维护	系统配置		设置设备的电子标签、开启/关闭 telnet、ssh、http、https 功能，设置管理 IP
	文件管理		固件升级管理，配置管理，证书管理，页面包管理
	用户管理		创建/删除用户，设置用户密码
	时间管理		显示/设置系统当前日期和时间
	SNMP		新建、修改、删除 SNMP 配置
诊断	网络工具		执行 ping/trace route 操作并显示执行结果
	光模块信息		查看光模块信息，如厂家信息，序列号，光功率等
	一键收集		生成诊断信息文件，并将文件打开查看或保存到本地主机
	掉电告警		开启/关闭 dying gasp 掉电告警功能
	线缆检测		检测电口线缆状态

2 监控

2.1 概况

在导航栏里点击【监控】→【概况】，进入概览界面，如图 2-1 所示。概览界面分为 3 个部分，分别为“系统信息”，“面板端口”，“流量”。

（1）在“系统信息”页面，可以看到设备的产品型号、序列号、MAC 地址、软硬件版本等信息，具体参数说明如表 2-1 所示。

图 2-1 系统基本信息

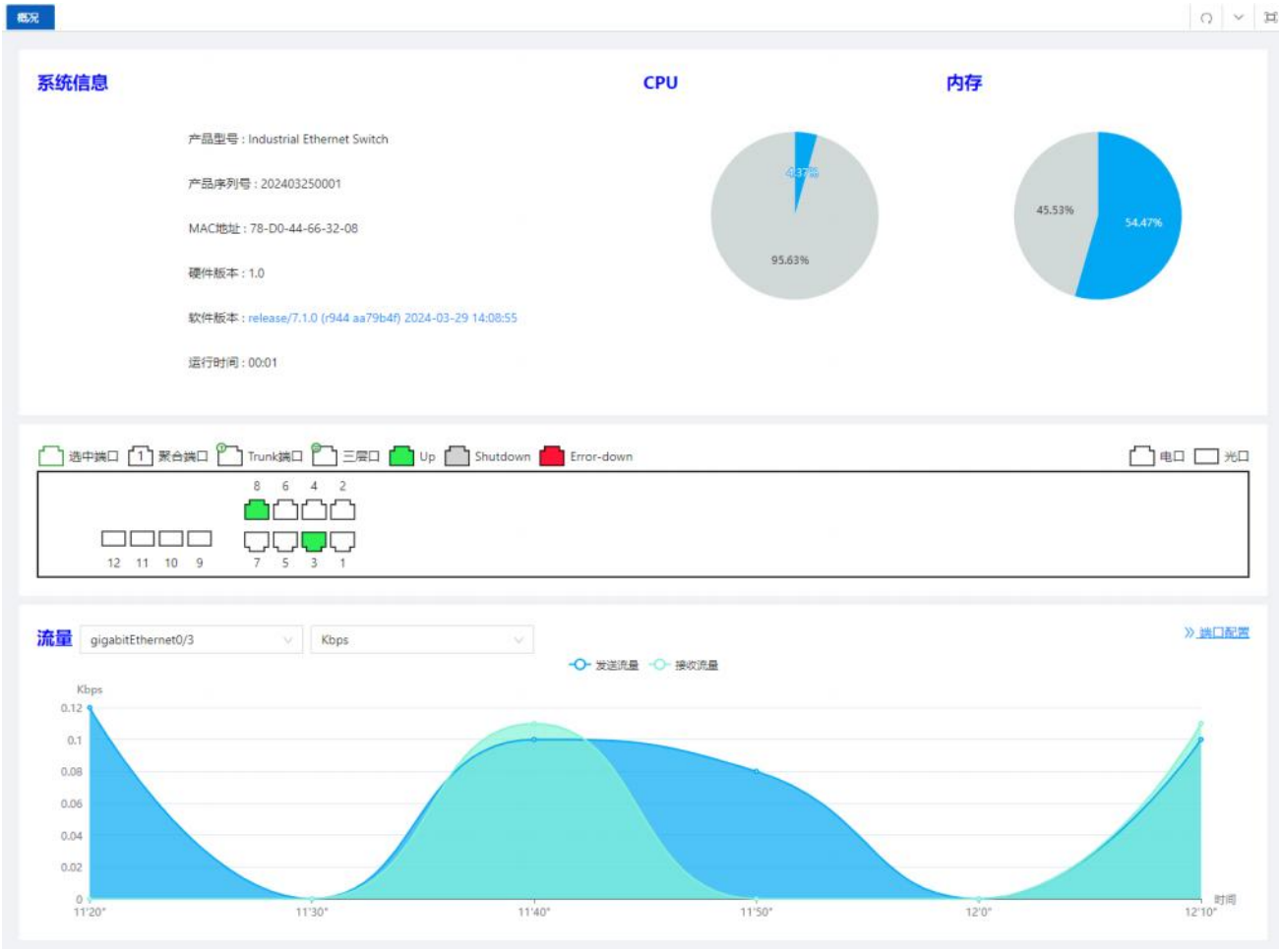


表 2-1 基本信息参数说明

配置项	说明
产品型号	用以指示该设备的产品型号
产品序列号	用以指示该设备的产品序列号
MAC 地址	用以指示该设备的 MAC 地址
硬件版本	用以指示该设备的硬件版本号
软件版本	用以指示该设备的软件版本号
运行时间	用以指示该设备最近一次启动后连续运行的时长，设备重启后将重新计时

CPU	用以显示当前 CPU 的占用率
内存	用以显示当前系统可用内存

（2）“面板端口”页面，可以看到设备的面板示意图以及面板端口的工作情况。

（3）“流量”页面，可以观察到端口的流量情况。

2.2 端口统计

“端口统计”页面用于显示端口接收和发送报文数量的相关统计信息。

（1）在导航栏中选择【监控】→【端口统计】，进入端口统计页面，如图 2-2 所示。

（2）在页面中查看设备端口接收和发送负载、端口速率，错误报文统计，具体参数说明如表 2-2 所描述。

（3）点击端口最后的【清除】按钮可以清除端口计数。

（4）点击【端口配置】按钮可以直接切换到端口配置界面。

图 2-2 端口统计页面

表 2-2 参数说明

配置项	说明
端口	交换机的端口
接收负载	端口接收负载率
发送负载	端口发送负载率
速率	端口工作速率
不完整数据包	端口接收的报文小于 64 字节的数量
过大数据包	端口接收的报文大于 MTU 配置上限的数量
CRC 错误	端口的接收的 CRC 校验错误的报文数量
冲突次数	端口的接收的冲突报文数量
清除	报文清零

2.3 环路保护

“环路保护”页面用于显示设备环路相关协议的工作状态，如 ERPS 和生成树协议。

（1）在导航栏中选择【监控】→【环路保护】，进入环路保护状态页面，如图 2-3 所示。

（2）在页面中可以看到已经开启的 ERPS 和生成树协议工作状态，具体参数说明见协议相关章节。

（3）点击【ERPS 配置】、【生成树配置】按钮可以直接切换到相关配置界面。

图 2-3 环路保护状态

2.4 安全

“安全”页面用于显示设备安全相关协议的工作状态，有端口安全，IP Source Guard，MAC 认证三个部分。

（1）在导航栏中选择【监控】→【安全】，进入安全显示页面，如图 2-4，图 2-5，图 2-6 所示。

图 2-4 端口安全状态

图 2-5 IP Source Guard 状态

图 2-6 MAC 认证状态

（2）在页面中可以看到已经开启的端口安全、IP Source Guard、MAC 认证工作状态，具体参数说明见协议相关章节。

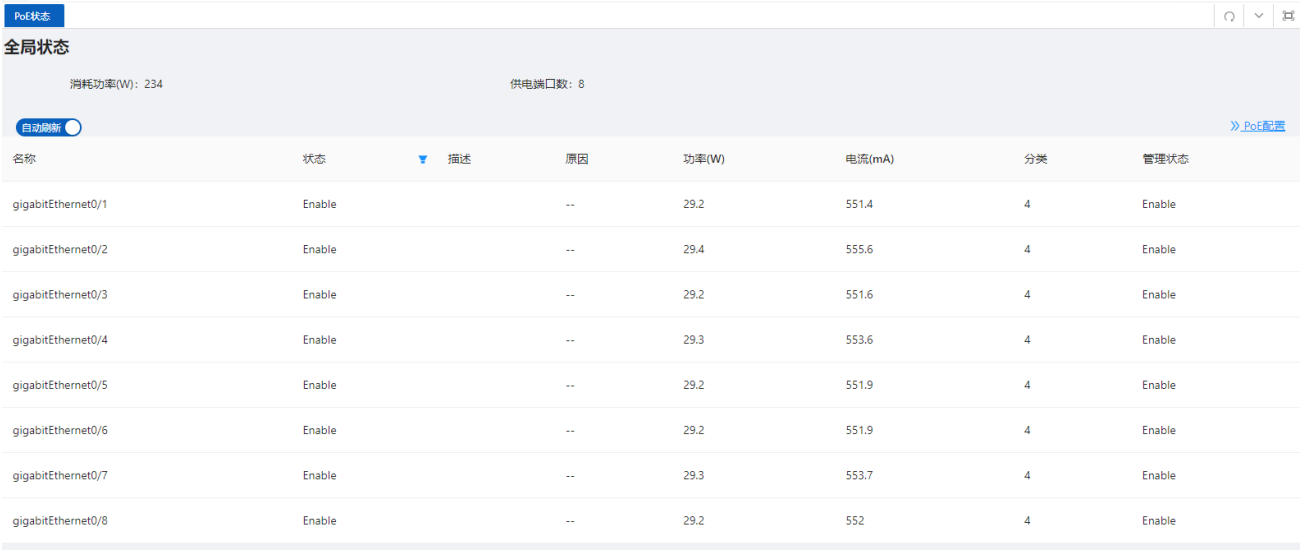
（3）点击对应的配置按钮可以直接切换到相关配置界面。

2.5 PoE 状态

“PoE 状态”页面用于显示设备当前 PoE 工作状态。

（1）在导航栏中选择【监控】→【PoE 状态】，进入 PoE 状态页面，如图 2-7 所示。

图 2-7 PoE 状态



（2）在页面中可以看到设备总的供电功率、供电端口数、每个端口的供电状态。具体参数说明，如表格 2-3 所示。

表 2-3 PoE 全局配置参数说明

配置项	说明	
全局状态	消耗功率(W)	当前设备 PoE 对外供电的总功率
	供电端口数	当前设备对外供电的端口总数
端口	名称	指示面板端口号
	状态	PoE 目前的供电状态，disable 供电关闭状态，enable 供电状态
	描述	PoE 端口描述
	原因	端口无法供电的原因， short：负载短路 management：功率不足
	功率	当前端口的消耗的功率
	电流	当前端口的工作电流
	分类	接入此端口 PD 设备的 Class 等级
	管理状态	显示此端口的 PoE 功能是使能或禁止

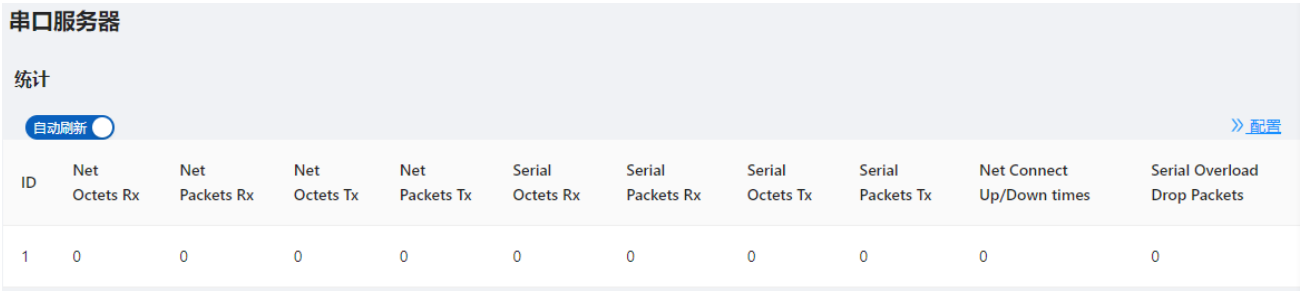
（3）点击【PoE 配置】按钮可以直接切换到 PoE 配置界面。

2.6 串口服务器状态

“串口服务器状态”页面用于显示设备的串口服务器工作情况。

（1）在导航栏中选择【监控】→【串口服务器状态】，进入串口服务器状态页面，如图 2-8 所示。

图 2-8 串口服务器状态



（2）在页面中可以看到串口服务器的报文收发状态，具体参数说明如表格 2-4 所示。

表 2-4 串口服务器参数说明

配置项	说明
ID	串口服务器的串口 ID 号
Net Octets Rx	网络端接收字节数
Net Packets Rx	网络端接收报文数

Net Octets Tx	网络端发送字节数
Net Packets Tx	网络端发送报文数
Serial Octets Rx	串口端接收字节数
Serial Packets Rx	串口端接收报文数
Serial Octets Tx	串口端发送字节数
Serial Packets Tx	串口端发送报文数
Net Connect Up/Down times	网络端连接次数
Serial Overload Drop Packets	串口端溢出丢弃报文数

（3）点击【配置】按钮可以直接切换到串口服务器配置界面。

2.7 LLDP 状态

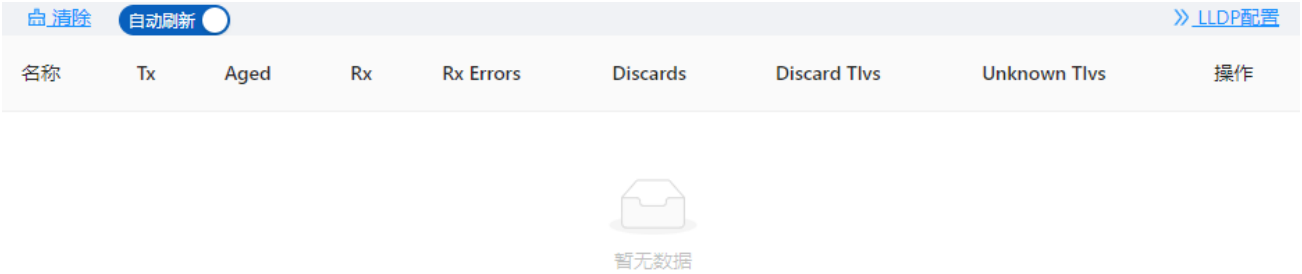
“LLDP 状态”页面用于显示设备 LLDP 工作状态。

（1）在导航栏中选择【监控】→【LLDP 状态】，进入 LLDP 状态页面，如图 2-9 所示。

（2）在页面中可以看到已经开启的 LLDP 协议工作状态，具体参数说明见协议相关章节。

（3）点击【LLDP 配置】按钮可以直接切换到 LLDP 配置界面。

图 2-9 LLDP 状态



2.8 IGMP Snooping 状态

“IGMP Snooping 状态”用于显示设备 IGMP Snooping 协议工作状态。

（1）在导航栏中选择【监控】→【IGMP Snooping 状态】，进入 IGMP Snooping 状态页面，如图 2-10 所示。

（2）在页面中可以看到已经开启的 IGMP Snooping 协议工作状态，具体参数说明见协议相关章节。

（3）点击【IGMP Snoooing 配置】按钮可以直接切换到 IGMP Snoooing 配置界面。

图 2-10 IGMP Snooping 状态

2.9 DHCP Snooping 状态

“DHCP Snooping 状态”页面用于显示设备 DHCP Snooping 协议工作状态。

（1）在导航栏中选择【监控】→【DHCP Snooping 状态】，进入 DHCP Snooping 状态页面，如图 2-11 所示。

（2）在页面中可以看到已经开启的 DHCP Snooping 协议工作状态，具体参数说明见协议相关章节。

（3）点击【DHCP Snooping 配置】按钮可以直接切换到 DHCP Snooping 配置界面。

图 2-11 DHCP Snooping 状态

2.10 QinQ 信息

“QinQ 信息”页面用于显示设备 QinQ 信息工作状态。

（1）在导航栏中选择【监控】→【QinQ 信息】，进入 QinQ 状态页面，如图 2-12 所示。

（2）在页面中可以看到已经开启的 QinQ 工作状态，具体参数说明见协议相关章节。

（3）点击【QinQ 配置】按钮可以迅速切换到 QinQ 配置界面。

图 2-12 QinQ 信息

2.11 环路检测状态

“环路检测状态”页面用于显示设备端口环路状态。

（1）在导航栏中选择【监控】→【环路检测状态】，进入环路检测状态页面，如图 2-13 所示。

（2）在页面中可以看到设备端口的环路状态，具体参数说明见协议相关章节。

（3）点击【环路检测配置】按钮可以迅速切换到环路检测配置界面。

图 2-13 环路检测状态

2.12 ARP 信息

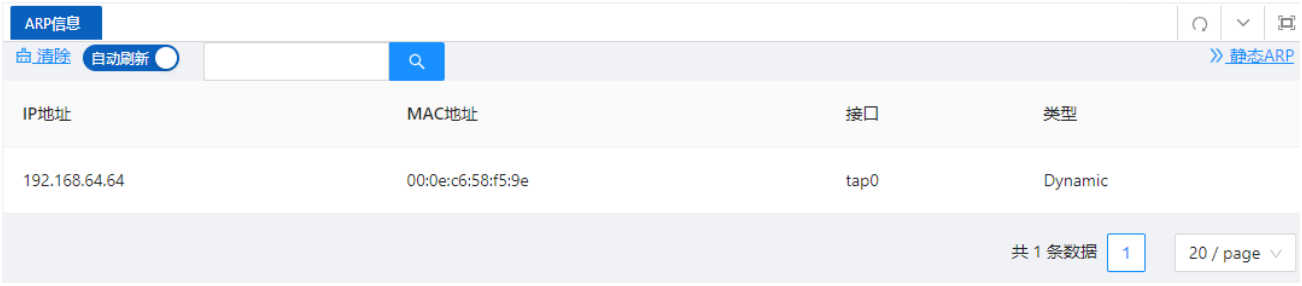
“ARP 信息”页面用于显示设备 ARP 表项信息。

（1）在导航栏中选择【监控】→【ARP 信息】，进入 ARP 状态页面，如图 2-14 所示。

（2）在页面中可以看到设备所有的 ARP 表项信息，具体参数说明见协议相关章节。

（3）点击【静态 ARP】按钮可以迅速切换到三层静态 ARP 配置界面。

图 2-14 ARP 信息



3 配置

3.1 VLAN

3.1.1 概述

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。

3.1.1.1 链接类型

根据端口在转发报文时对 VLAN Tag 的不同处理方式，可将端口的链路连接类型分为两种：

Access ：

端口发出去的报文不带 VLAN Tag，一般用于和不能识别 VLAN Tag 的终端设备相连，或者不需要区分不同 VLAN 成员时使用。

Trunk ：

端口发出去的报文，端口缺省 VLAN 内的报文不带 Tag，其它 VLAN 内的报文都必须带 Tag。通常用于网络传输设备之间的互连。

Hybrid ：

端口发出去的报文可根据需要设置某些 VLAN 内的报文带 Tag，某些 VLAN 内的报文不带 Tag。Hybrid 类型端口既可以用于网络传输设备之间的互连，又可以直接连接终端设备。

3.1.1.2 缺省 VLAN（PVID）

除了可以设置端口允许通过的 VLAN，还可以设置端口的缺省 VLAN。在缺省情况下，所有端口的缺省 VLAN 均为 VLAN 1，但用户可以根据需要进行配置。

• Access 端口的缺省 VLAN 就是它所属的 VLAN。

• Trunk 端口和 Hybrid 端口可以允许多个 VLAN 通过，能够配置缺省 VLAN。

• 当删除某个 VLAN 时，如果该 VLAN 是某个端口的缺省 VLAN，则对 Access 端口，端口的缺省 VLAN 会恢复到 VLAN 1；对 Trunk 或 Hybrid 端口，端口的缺省 VLAN 配置不会改变，即它们可以使用已经不存在的 VLAN 作为缺省 VLAN。

说明

- 建议本端设备端口的缺省 VLAN 和相连的对端设备端口的缺省 VLAN 保持一致。
- 建议保证端口的缺省 VLAN 为端口允许通过的 VLAN。如果端口不允许某 VLAN 通过，但是端口的缺省 VLAN

为该 VLAN，则端口会丢弃收到的该 VLAN 的报文或者不带 VLAN Tag 的报文。

- Web 网管不支持配置 Hybrid 口，如需此功能请使用 CLI 配置方式。

3.1.1.3 端口对报文的处理方式

在配置了端口连接类型和缺省 VLAN 后，端口对报文的接收和发送的处理有几种不同情况，具体情况如表 3-1 所示。

表 3-1 端口收发报文的处理

端口类型	对接收报文的处理		对发送报文的处理
	接收的报文不带 Tag 时	接收的报文带有 Tag 时	
Access	为报文添加缺省 VLAN 的 Tag	• 当 VLAN 与缺省 VLAN 相同时，接收该报文 • 当 VLAN 与缺省 VLAN 不同时，丢弃该报文	去掉 Tag，发送该报文
Trunk	• 当缺省 VLAN 在端口允许通过的 VLAN 列表中时，接收该报文，为报文添加缺省 VLAN 的 Tag • 当缺省 VLAN 不在端口允许通过的 VLAN 列表中时，丢弃该报文	• 当 VLAN 在端口允许通过的 VLAN 列表中时，接收该报文 • 当 VLAN 不在端口允许通过的 VLAN 列表中时，丢弃该报文	• 当 VLAN 与缺省 VLAN 相同，且在端口允许通过的 VLAN 列表中时，去掉 Tag，发送该报文 • 当 VLAN 与缺省 VLAN 不同，且在端口允许通过的 VLAN 列表中时，保持原有 Tag，发送该报文
Hybrid			当 VLAN 在端口允许通过的 VLAN 列表中时，发送该报文，是否去掉 Tag 可由用户手动配置

3.1.2 配置 VLAN

3.1.2.1 VLAN 配置简介

配置基于 Access 端口的 VLAN

表 3-2 基于 Access 端口的 VLAN 配置步骤

步骤	配置任务	说明
1	配置端口的连接类型	可选 配置端口的连接类型为 Access ，缺省情况下，端口的连接类型为 Access
2	创建 VLAN	必选创建一个或多个 VLAN
3	配置端口的缺省 VLAN	配置 Access 端口的缺省 VLAN

配置基于 Trunk 端口的 VLAN

表 3-3 基于 Trunk 端口的 VLAN 配置步骤

步骤	配置任务	说明

1	配置端口的连接类型	必选 配置端口的连接类型为 Trunk 缺省情况下，端口的连接类型为 Access	缺省情况下，Trunk 端口的 Untagged VLAN（即缺省 VLAN）为 VLAN 1 提示 改变 Trunk 端口的 Untagged VLAN（即其缺省 VLAN）时，该端口原来的 UntaggedVLAN 将自动变为其 Tagged VLAN
2	创建需要添加到该 Trunk 口中的 VLAN	必选创建一个或多个 VLAN	
3	配置 VLAN 所属的 Trunk	选择对应的 Trunk 口，将 VLAN 添加	必选 Trunk 端口只有一个 Untagged VLAN，即其缺省 VLAN。

3.1.2.2 配置 VLAN 中的端口

VLAN 配置界面如图 3-1 所示，各参数详细说明如表 3-4 所示。

图 3-1 VLAN 配置界面

表 3-4 VLAN 配置相关参数说明

配置项	说明
ID	VLAN 序号
名称	VLAN 名称，不支持配置，默认 VLAN 1 为 default，VLAN 2 为 VLAN0002。
类型	Static\Dynamic，当前版本仅支持 Static
成员	端口成员列表
编辑	选择需要编辑的 VLAN ID，点击此按钮进入编辑界面。
添加	点击此按钮进入 VLAN 添加界面。
删除	选择需要编辑的 VLAN ID，点击此按钮删除该 VLAN。

配置步骤：

（1）在导航栏中选择【配置】→【VLAN】，进入 VLAN 配置界面，如图 3-2 所示。

（2）单击【添加】按钮，进入如图 3-1-2-2 所示的页面。

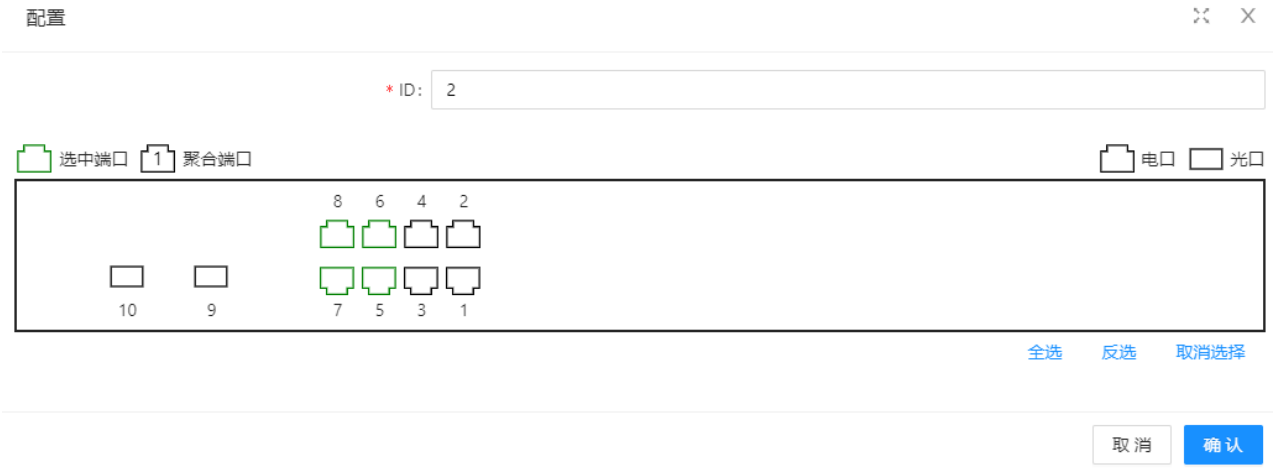
（3）在 ID 框里，输入需要创建的 VLAN。

（3）选取需要加入该 VLAN 的端口成员，单击【确认】按钮完成操作。

（4）单击辅助区的【保存】按钮，保存配置。

（5）当多个 VLAN 需要被同时创建时，可以用“n-m”的方式，如“2-10”。当单次创建的 VLAN 数量大于 100 时，请使用 CLI 命令行进行配置。

图 3-2 创建 VLAN



3.1.2.3 配置 Trunk 口

Trunk 口配置界面如图 3-3 所示，各参数详细说明如表 3-5 所示。

图 3-3 Trunk 配置界面

表 3-5 接口配置相关参数说明

配置项		说明
模式	Access	配置端口类型为 Access 口
	Trunk	配置端口类型为 Trunk 口
PVID/Native VLAN		配置 Access 口的 PORT-BASE VLAN ID 或者 Trunk 口的 Native VLAN
Allow VLANs		选择端口 VLAN，适用于 Trunk 口

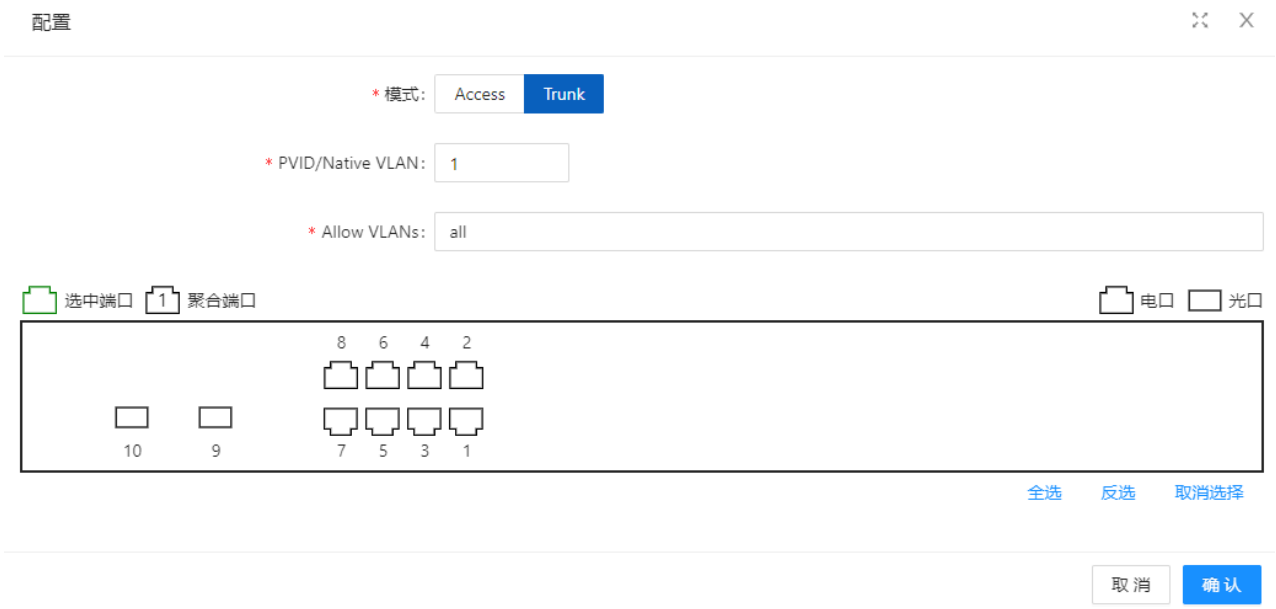
配置步骤：

（1）在导航栏中选择【配置】→【VLAN】，进入接口配置界面，如图 3-4 所示。

（2）点击 Trunk 口配置下方的【批量编辑】按钮，进入接口配置页面。

（3）配置端口的 VLAN 模式，以及 PVID 或者 Native Vlan，一般情况下，建议 Trunk 口的 Native Vlan 配置为“1”，Allow VLANs 为“all”，配置界面如图 3-4 所示，单击【确认】按钮完成配置。

图 3-4 VLAN 配置界面



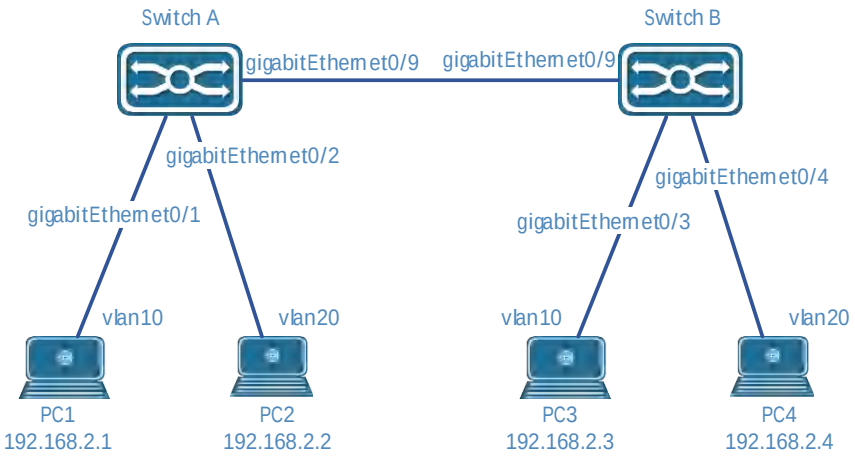
（4）单击辅助栏的【保存】按钮，保存配置。

3.1.3 VLAN 配置举例

配置范例：

案例需求:Switch A 与 Switch B 通过 trunk 口互连，相同 VLAN 的 PC 之间可以互访，不同 VLAN 的 PC 之间禁止互访，网络拓扑如图 3-5 所示；

图 3-5 网络拓扑图

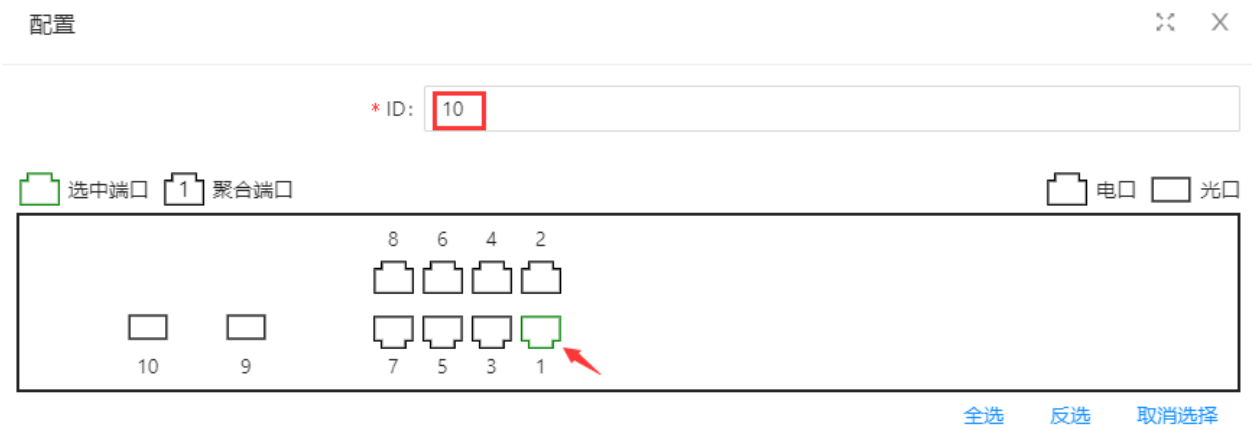


Switch A 配置：

步骤 1：配置 GigabitEthernet 0/1 为 access 口，PVID 为 10，GigabitEthernet 0/2 为 access 口，PVID 为 20。

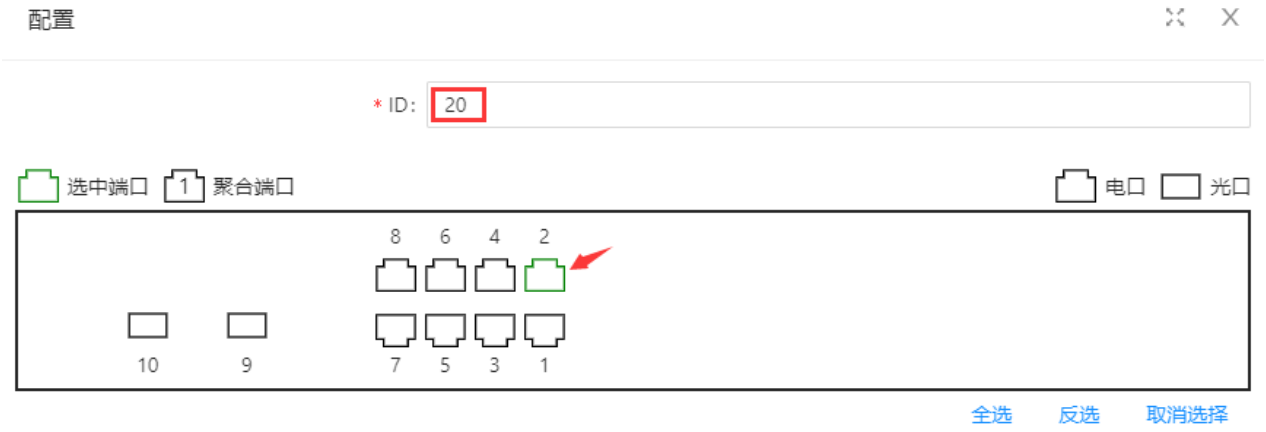
在导航栏【配置】选择【VLAN】，进入 VLAN 配置界面。点击【添加】按钮，在弹出的对话框里，ID 框里输入“10”，点击选中端口 GigabitEthernet 0/1，点击【确认】按钮，完成配置，如图 3-6 所示。

图 3-6 VLAN 配置界面



使用同样的步骤完成对端口 GigabitEthernet 0/2 的配置，如图 3-7 所示。

图 3-7 SWITCH B VLAN 配置界面



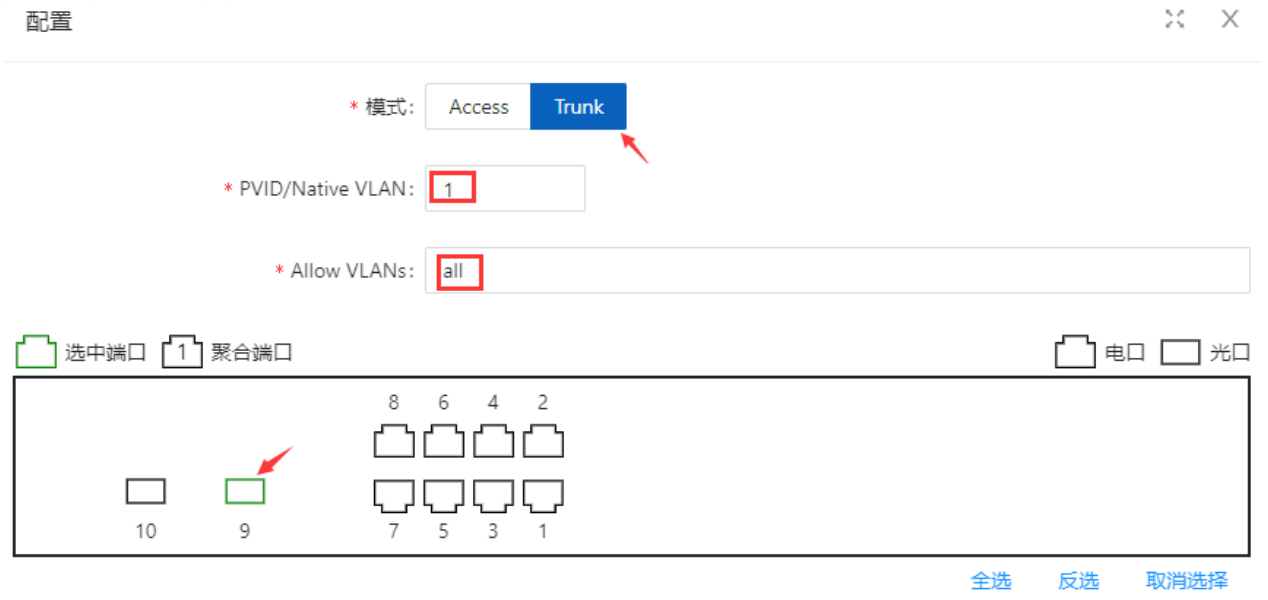
配置完成后的 VLAN 界面如图 3-8 所示。

图 3-8 SWITCH B VLAN 配置界面

步骤 2：创建 Trunk 口 GigabitEthernet 0/9

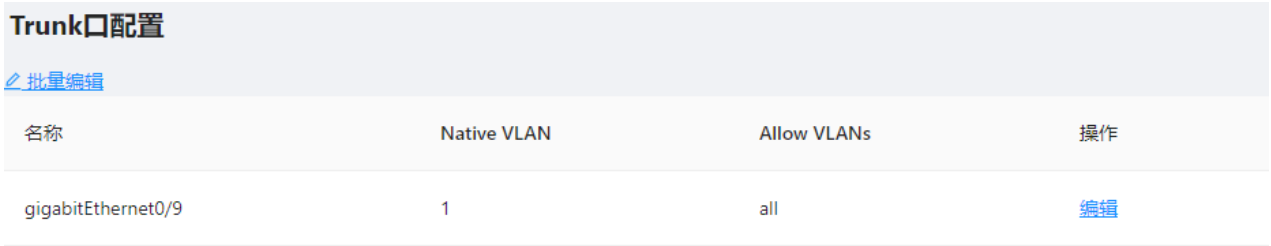
在当前界面，点击 Trunk 口下方的【批量编辑】按钮，如图 3-9 所示，依次选择“Trunk”，Native VLAN “1”，Allow VLANs “all”，端口面板单击选择 GigabitEthernet 0/9，点击【确定】按钮完成配置。

图 3-9 添加 VLAN 界面



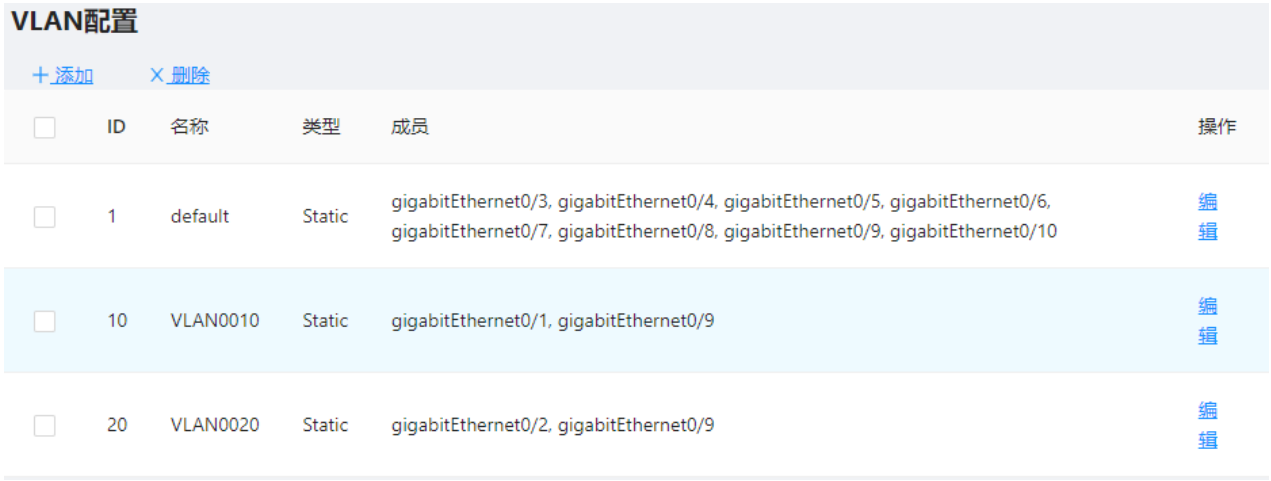
配置成功的 Trunk 口 GigibitEthernet0/9 如图 3-10 所示。

图 3-10 Trunk 口配置界面



配置完成后的 VLAN 列表如图 3-11 所示。

图 3-11 VLAN 界面



步骤 5：点击辅助区的【保存】按钮，保存配置。

Switch B 配置：

配置方法同 Switch A，把 GigabitEthernet 0/9 配置为 trunk 口。创建 VLAN 10 和 VLAN 20 并完成对应的端口配置。配置完成后，VLAN 界面如图 3-12 所示。

图 3-12 Switch B VLAN 界面

3.2 端口

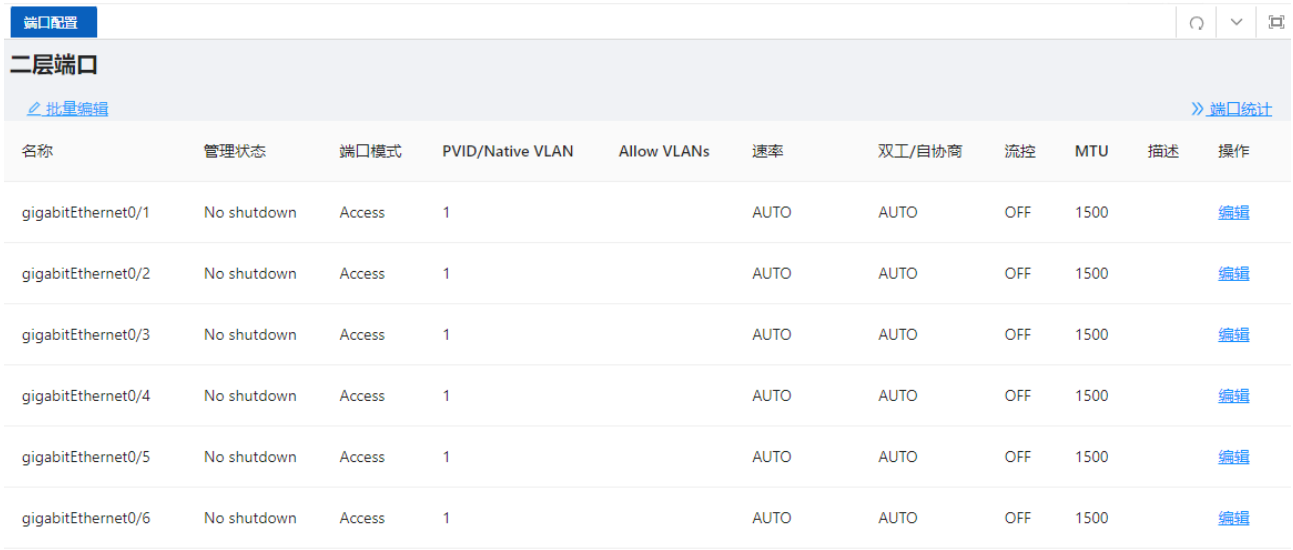
3.2.1 端口配置

说明

- 由于电口和光口的部分参数不同，选择多端口配置时，建议对电口和光口分开进行配置。

端口管理模块用于配置以太网接口的工作参数，包括：描述、端口模式、介质类型、速率、双工状态、流控、MTU、状态，如图 3-13 所示。

图 3-13 端口管理界面



操作步骤：

（1）在导航栏中选择【配置】→【端口】→【端口配置】，如图 3-13 所示。

（2）单击【编辑】或【批量编辑】按钮，进入如图 3-14 所示的页面。

（3）配置端口的工作参数，具体参数说明如表 3-6 所示。

（4）单击【确定】按钮完成操作。

（5）单击导航栏的【保存】按钮保存配置。

表 3-6 接口工作参数说明

配置项	说明
描述	设置端口的描述信息，可以使用字母和数字组合。
介质类型	配置复用端口的介质类型，仅对支持光电复用(Combo)的端口有效。 • RJ45：设置端口工作在电口模式。 • SFP：设置端口工作在光口模式。 • 这里是否需要加上光点自适应的？
速率	设置端口的速率 • 10M：10Mbps • 100M：100Mbps • 1000M：1000Mbps

	• AUTO：自动协商端口速率
双工状态	设置端口的双工状态 • AUTO：自协商双工状态 • FULL：全双工状态 • HALF：半双工状态
端口模式 （仅适用于光口）	设置端口的工作模式以支持不同的工作模式，不同的模式需要相应的光模块支持。 • 100BASE-FX：设置端口工作在百兆光模式。 • 1000BASE-X：设置端口工作在千兆光模式。 • SGMII：设置端口工作在 SGMII 模式，当光口插入的模块为千兆转百兆光（SFP GE-FX）或者是光转电模块（Mini-GBIC-GT）时，需要配置为此模式。 • 2500BASE-X：设置端口工作在 2.5G 光口模式。 • 10G BASE-X:设置端口工作在 10G 光口模式。 提示 • 2500BASE-X 模式，与其他厂家的端口互联可能存在不兼容的情况。 • 不同型号的设备的光口能力是不一样的，具体请参考具体产品型号对应的说明文档。
自协商 （仅适用于光口）	开启/关闭光口的自协商功能。 OFF：光口关闭自协商，工作在强制状态。 ON：光口开启自协商。
流控	设置使能（Enable）或禁止（Disable）端口流量控制功能 当本端和对端设备都使能了流量控制功能后，如果本端设备发生拥塞，就向对端设备发送消息，通知对端设备暂时停止发送报文；对端设备在接收到该消息后将暂时停止向本端发送报文；反之亦然。从而避免了报文丢失现象的发生 提示 只有本端和对端端口都开启了流量控制功能，才能实现流量控制
MTU	设置允许转发的帧长，支持的帧长范围 46-10222 bytes，默认为 1500 bytes。
管理状态	设置端口的打开/关闭状态。 • No shutdown：设置端口工作在正常工作状态。 • Shutdown：设置端口工作在关闭状态。

图 3-14 接口配置界面

配置举例：

案例需求：配置端口 GigabitEthernet0/9 为 2.5G 工作模式，关闭流控，MTU 设置为 10000 bytes，端口描述为 abc。

步骤 1：在导航栏中选择【接口】→【端口管理】,进入端口管理界面。

步骤 2：选择端口 GigabitEthernet0/9，点击【编辑】按钮进入端口配置界面，如图 3-15 所示。

步骤 3: 按照图 3-2-3 所示，按照描述“abc”，介质类型“SFP”，端口模式“2500BASE-X”，流控“OFF”，MTU“10000”，管理状态“No shutdown”，配置好参数。

步骤 4：单击【确认】按钮完成操作。

步骤 5：单击辅助栏的【保存】按钮保存配置。

图 3-15 接口配置举例

3.2.2 端口扩展

3.2.2.1 端口限速

端口限速就是基于端口的速率限制，它对端口输入、输出报文的总速率进行限制。在流量从接口发出前，在接口的出方向上配置限速，对流出的所有报文流量进行控制。在流量从接口接收前，在接口的入口方向上配置限速，对流入的所有报文流量进行控制。

操作步骤：

（1）在导航栏中选择【配置】→【端口】→【端口扩展】,进入端口限速配置界面，如图 3-16 所示。

（2）对需要配置限速的端口，在对话框中输入相应数值，具体参数定义如表 3-7 所示。

（3）单击对应端口的【应用】按钮完成操作。

（4）单击导航栏的【保存】按钮保存配置。

图 3-16 端口限速界面

说明

- limit 数值是可确定的，比如限速 1M，那么 limit 数值为 1024，但是 burst 的数值却取自经验数值。当 burst 数值配大，流量尖峰更高，限速较稳定，但平均速率可能高于限速值；当 burst 数值配小，流量尖峰较低，限速波动较大，平均速率可能小于限速值。建议 burst 配置取 limit 的 4 倍值与 16384 的小值。

表 3-7 参数说明

配置项	说明
名称	端口名称
输入速率（kbps）	输入方向的每秒钟的带宽限制量(KBits)
输入突发流量（KB）	输入方向的突发流量限制值(Kbytes)
输出速率（kbps）	输出方向的每秒钟的带宽限制量(KBits)
输出突发流量（KB）	输出方向的突发流量限制值(Kbytes)
操作	编辑或者删除此条例

配置举例：

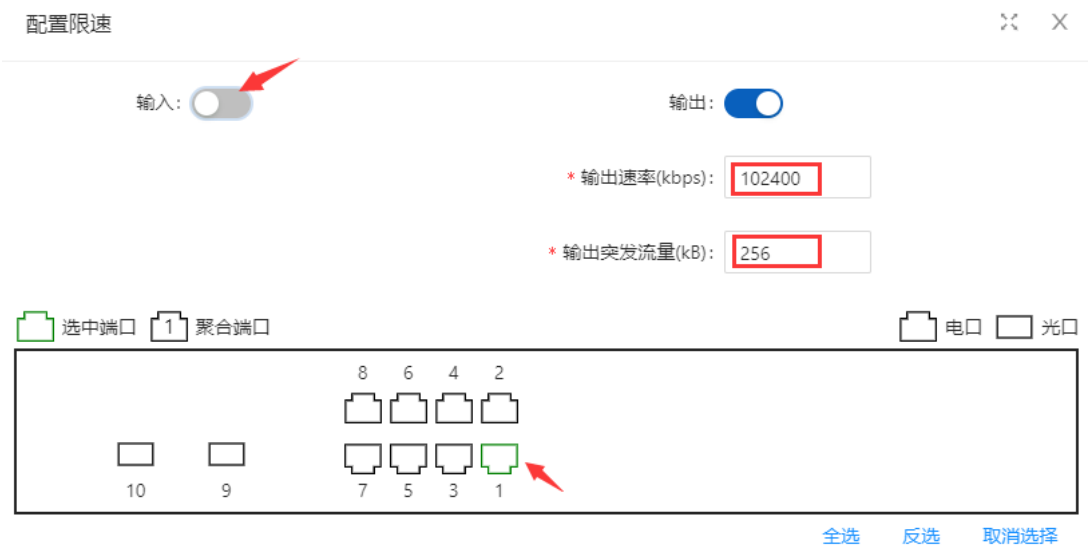
案例需求：假设交换机的端口 GigabitEthernet0/1 连到 Internet，需要在端口 GigabitEthernet0/1 出口流量限制，带宽限制每秒 102400KBits，突发流量限制每秒 256Kbytes。

步骤 1：在导航栏中选择【配置】→【端口】→【端口扩展】，进入端口限速配置界面。

步骤 2：点击关闭输入限速按钮，在输出限速对话框里输入对应的数值，面板图上点击选择端口 1，如图 3-17 所示。

步骤 3：点击【确定】按钮，完成配置。

图 3-17 端口限速配置界面



步骤 4：单击辅助区的【保存】按钮保存配置。

3.2.2.2 风暴抑制

当局域网中存在过量的广播、多播或未知单播数据流时，将导致网络性能下降，甚至网络瘫痪的现象，称为广播风暴。风暴控制针对广播、多播和未知单播数据流进行限速，当交换机端口接收到的广播、未知名多播或未知单播数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，从而避免过量的泛洪数据流进入 LAN 中形成风暴。

风暴控制模块，用于设置端口对于广播、组播、未知名单播报文的抑制比。采用的是基于带宽百分比的风暴控制模式。当设备端口接收到的数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，直到数据流恢复正常。

配置步骤：

（1）在导航栏中选择【配置】→【端口】→【端口扩展】，进入风暴控制界面，如图 3-18 所示。

图 3-18 风暴控制状态界面

（2）点击“风暴控制”下方的【批量编辑】按钮，进入如图 3-19 所示的页面。

（3）配置端口的风暴抑制类型及带宽抑制比，详细配置如表 3-8 所示，在端口面板上选择需要配置的端口。

（4）单击【确认】按钮完成操作。

（5）单击导航栏的【保存】按钮保存配置。

图 3-19 端口配置界面

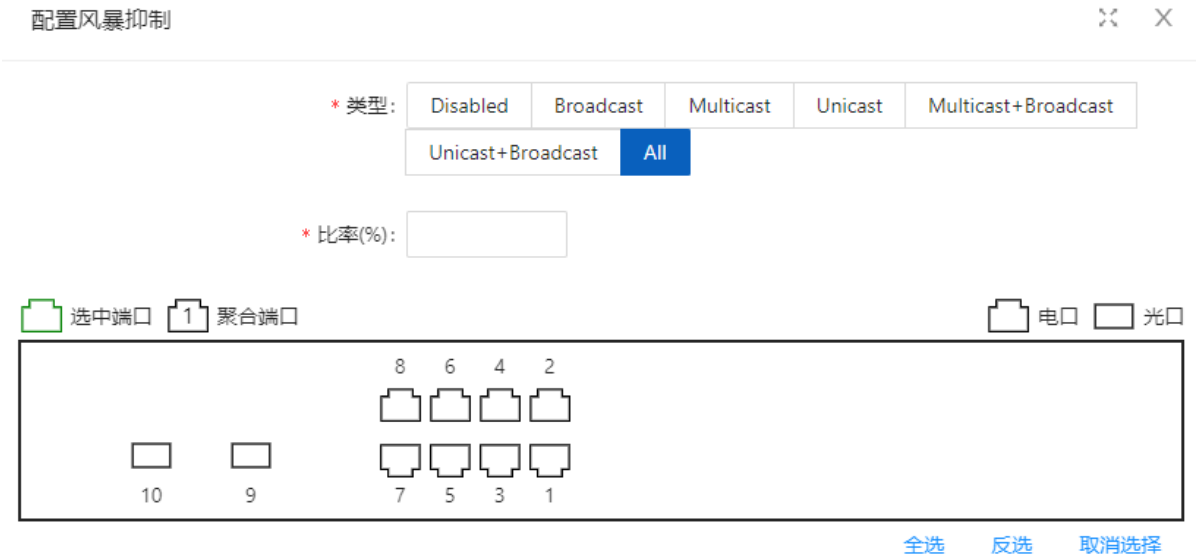


表 3-8 参数说明

配置项		说明
名称		选中的端口
类型	disabled	关闭此功能。
	broadcast	开启广播报文风暴抑制功能，可以实现对广播报文的流量限制。
	multicast	开启未知名组播报文风暴抑制功能，可以实现对未知名组播报文的流量限制。
	unicast	开启未知名单播报文风暴抑制功能，可以实现对未知名单播报文的流量限制。
	multicast – broadcast	开启组播报文+广播报文风暴抑制功能，可以实现对未知名组播报文和广播报文的流量限制。
	unicast-broadcast	开启未知名单播报文+广播报文风暴抑制功能，可以实现对未知名单播报文和广播报文的流量限制。
	all	选择抑制广播、多播、未知名单播
带宽比率（%）		允许通过的最大广播流量占该端口传输能力的百分比，选择此项后需输入具体的百分数

配置举例：

案例需求：开启端口 GigabitEthernet0/1 的风暴控制，对广播报文的抑制比设置为 10%。

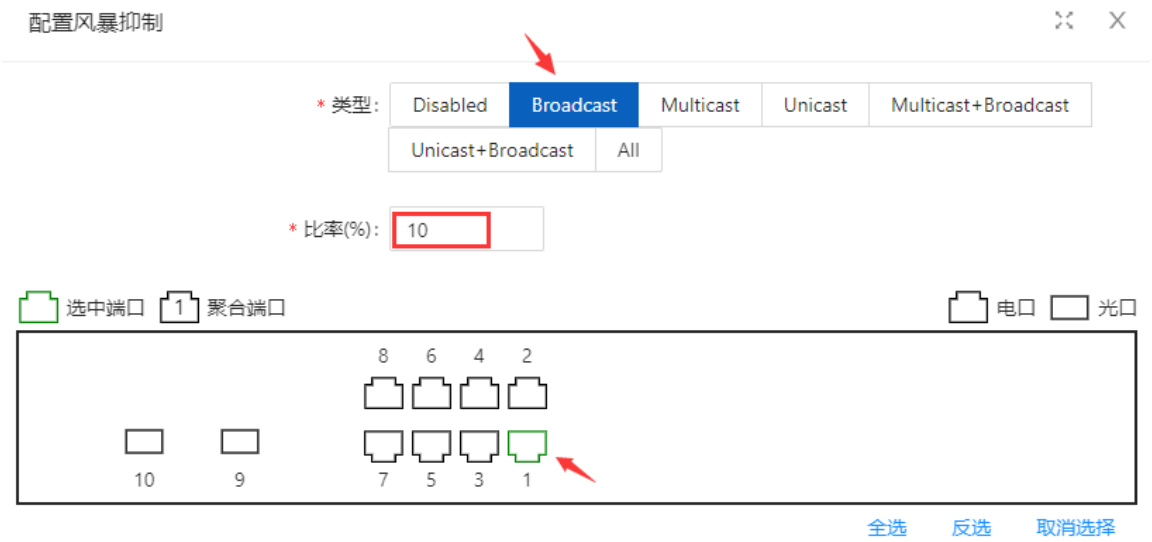
步骤 1：在导航栏中选择【配置】→【端口】→【端口扩展】,进入风暴控制界面。

步骤 2：点击【批量配置】按钮，进入配置界面。

步骤 3：类型选择 broadcast，带宽比率设置为 10，如图 3-20 所示，端口面板选择 Gigabitethernet0/1。

步骤 4：单击【确定】按钮完成操作。

图 3-20 风暴控制配置界面



步骤 5：单击辅助区的【保存】按钮保存配置。

3.2.2.1 端口隔离

为了实现报文之间的二层隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。端口隔离特性与端口所属的 VLAN 无关。不支持上行端口的设备，隔离组内的端口和隔离组外端口二层流量双向互通。

配置步骤：

（1）在导航栏中选择【配置】→【端口】→【端口扩展】，进入端口隔离界面，如图 3-21 所示。

（2）点击“端口隔离”下方的【批量编辑】按钮，进入端口隔离配置界面，点击【确认】按钮完成配置。

（3）单击辅助区【保存】按钮，保存配置。

图 3-21 端口隔离界面

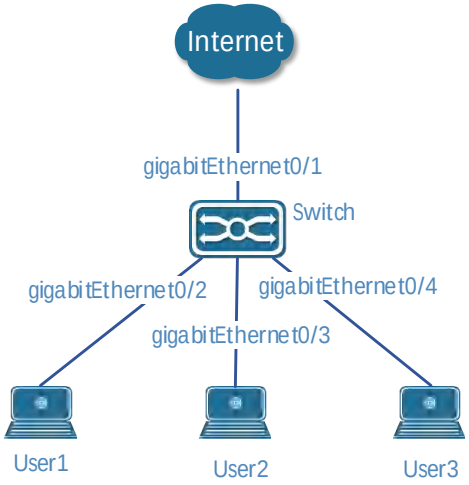
配置举例：

组网需求，如图 3-22 所示：

- 小区用户 User1、 User2、 User3 分别与 Switch 的端口 GigabitEthernet 0/2、GigabitEthernet 0/3、GigabitEthernet 0/4 相连。
- 设备通过 gigabitGigabitEthernet 0/1 端口与外部网络相连。

- GigabitEthernet0/1、GigabitEthernet 0/2、GigabitEthernet 0/3、GigabitEthernet 0/4 属于同一 VLAN；实现小区用户 User1、 User2 和 User3 彼此之间二层报文不能互通，但可以和外部网络通信。

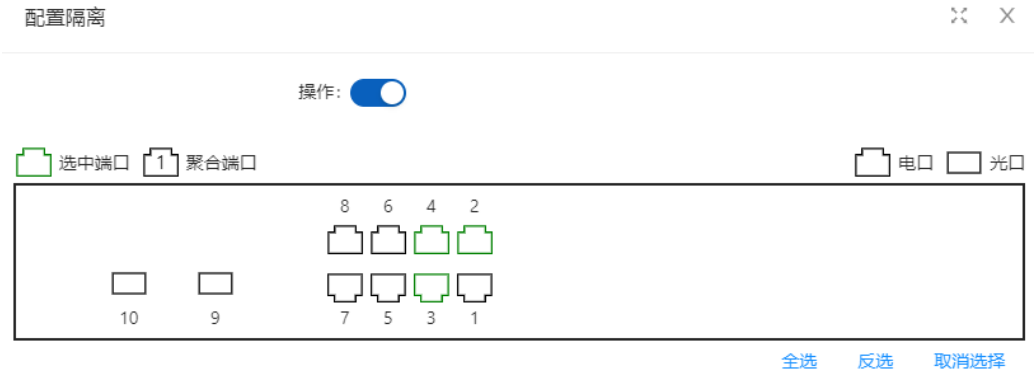
图 3-22 组网拓扑



步骤 1：在导航栏中选择【配置】→【端口】→【端口扩展】，进入端口隔离界面。

步骤 2：在端口面板选择 GigabitEthernet 0/2、GigabitEthernet 0/3、GigabitEthernet 0/4，如图 3-23 所示，点击【Ok】按钮完成配置，。

图 3-23 端口隔离配置界面



步骤 3:点击导航栏的【保存】按钮，保存配置。

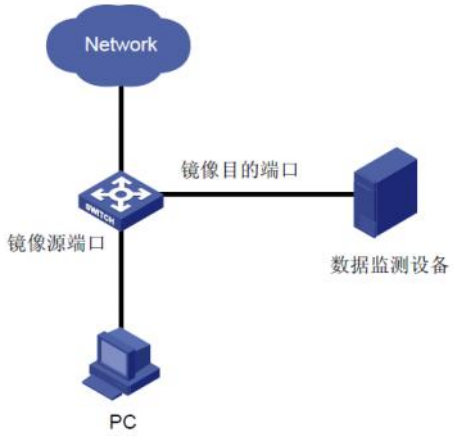
3.2.3 端口镜像

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，如图 3-24 所示。

SPAN 并不影响源端口和目的端口的报文交换，只是将源端口所有进入和输出的报文原样复制了一份到目的端口。当源端口的镜像流量超过目的端口带宽的情况下，例如 100Mbps 目的端口监控 1000Mbps 源端口的流量，可能导致报文被丢弃。

SPAN 基于会话管理，在会话中配置 SPAN 的源端口与目的端口。在一个会话中，只能有一个目的端口，但是可以同时配置多个源端口。

图 3-24 端口镜像



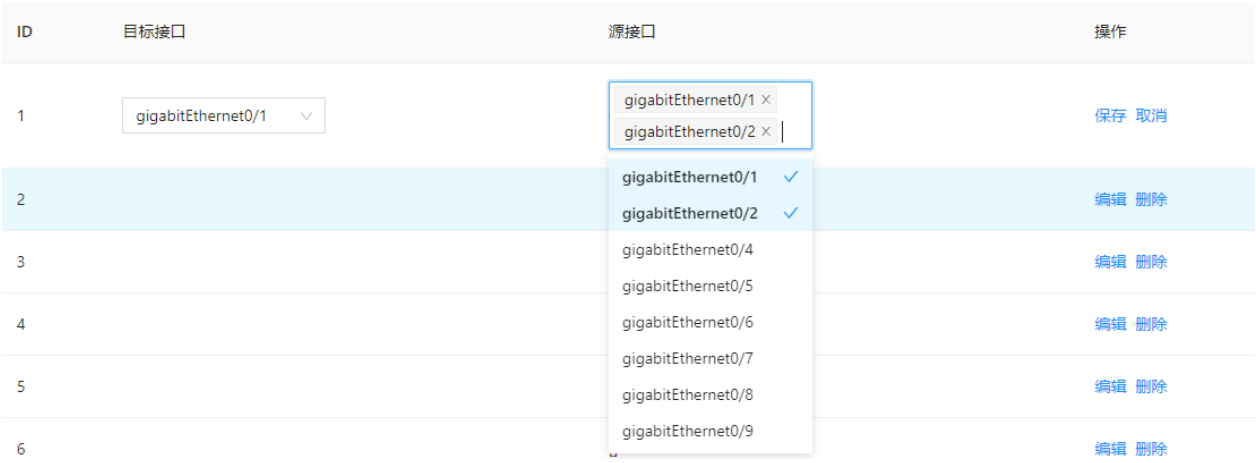
配置步骤：

（1）在导航栏中选择【配置】→【端口】→【端口镜像】，进入如图 3-25 所示的页面。

图 3-25 端口镜像界面

（2）点击对应 ID 的【编辑】按钮，选择目标接口，源接口，如图 3-26 所示，具体参数如表 3-9 所描述。

图 3-26 端口镜像配置界面



（3）单击【保存】按钮完成操作。

（4）单击辅助区的【保存】按钮保存配置。

表 3-9 参数说明

配置项	说明
ID	选择要进行配置的端口镜像组的组号，一共可以创建 7 个镜像组。
目的接口	选择镜像目的端口，每个会话只允许有一个目的接口
源接口	选择镜像源端口，允许有多个源端口同时存在

配置举例：

案例需求：利用端口 GigabitEthernet0/3 监控 GigabitEthernet0/1 口以及 GigabitEthernet0/2 的出口/入口报文。

步骤 1：在导航栏中选择【配置】→【端口】→【端口镜像】，进入端口镜像配置界面。

步骤 2：点击对应 ID1 的【编辑】按钮。

步骤 3：按照图 3-27 所示，目的接口选择 GigabitEthernet 0/3，源接口选择 GigabitEthernet 0/1 和 GigabitEthernet 0/2，点击【保存】按钮完成配置。

图 3-27 端口镜像配置界面

步骤 4：单击辅助区的【保存】按钮保存配置。

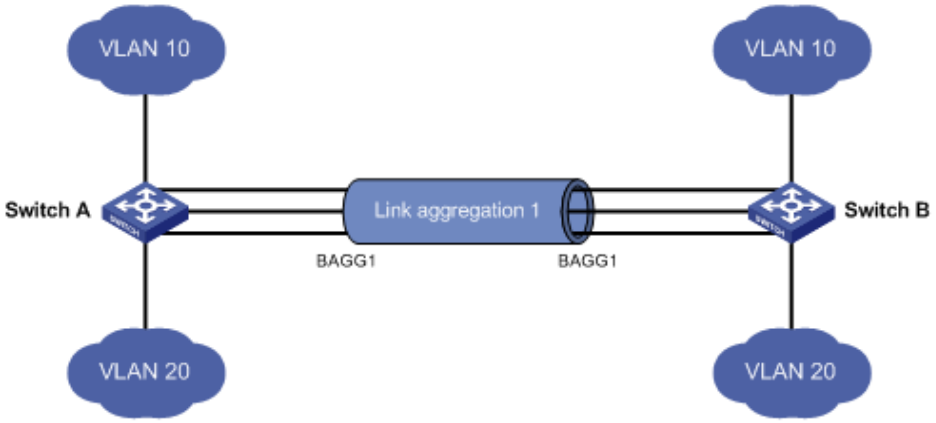
3.2.4 端口聚合

3.2.4.1 概述

聚合口

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，以下简称 PO 口)。该功能符合 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，如图 3-28 所示。

图 3-28 端口聚合组网模型



聚合口具备以下几个特性：

（1）高带宽，聚合口总带宽为物理成员口带宽总和；

（2）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；

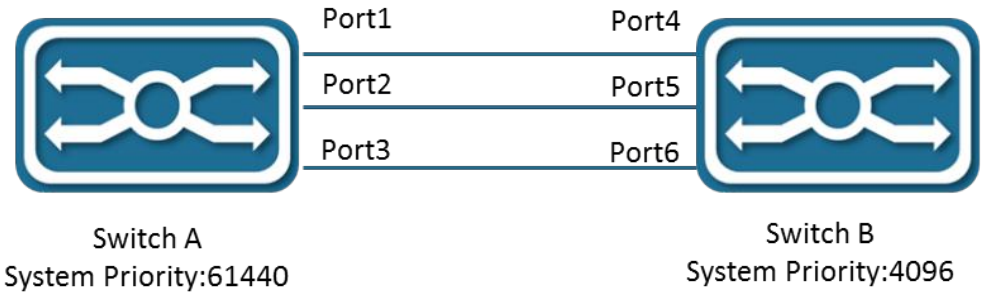
（3）支持链路备份，当聚合口中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到聚合口中的其它有效成员链路上。

LACP

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口上达到一致。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:长超时模式和短超时模式。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 3-29 端口聚合模型



如图 3-29 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 端口聚合，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 设置成聚合状态了。

3.2.4.2 配置聚合端口

配置步骤：

(1)在导航栏中选择【配置】→【端口】→【端口聚合】，进入端口聚合配置界面，在全局配置界面选择负载均衡算法，如图 3-30 所示，参数说明如表 3-10 所示。

图 3-30 合配置界面

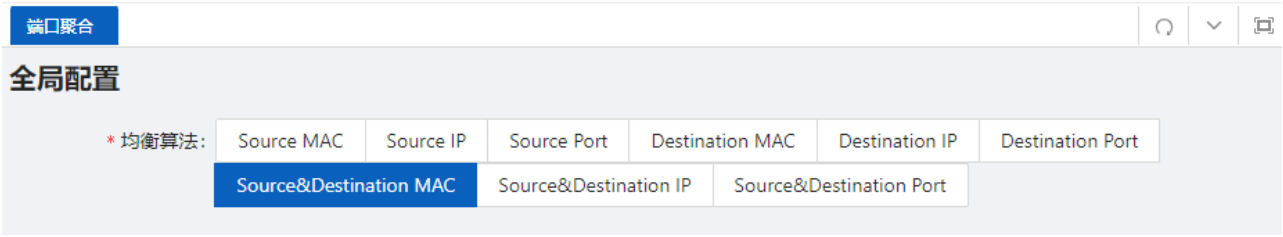


表 3-10 全局配置参数说明

配置项		说明	
全局配置	均衡算法	dst-mac	根据目的 MAC 地址进行均衡。
		src-mac	根据源 MAC 地址进行均衡。
		src-dst-mac	根据源 MAC 地址和目的 MAC 进行均衡。
		dst-ip	根据目的 IP 地址进行均衡。
		srt-ip	根据源 IP 地址进行均衡。
		src-dst-ip	根据源 IP 地址和目的 IP 地址进行均衡。
		dst-port	根据 L4 TCP/UDP 目的端口号进行均衡。
		src-port	根据 L4 TCP/UDP 源端口号进行均衡。
		src-dst-port	根据 L4 TCP/UDP 源端口号和目的端口号进行均衡。

(2) 点击“聚合口”下方的【添加】按钮，配置“类型”，“ID”,点击选择端口面板的端口序号，如图 3-31 所示，参数说明表 3-10 所示。

图 3-31 聚合口成员配置界面

表 3-11 聚合成员口配置参数说明

配置项		说明	
端口配置	ID	聚合口成员的 ID	
	类型	Manual	设置为手动模式
		Active	该端口会主动发起 LACP 聚合运算
		Passive	该端口不会主动发起 LACP 聚合运算，但是在接收到邻居的 LACP 报文后会被动参与 LACP 计算。

点击【确定】完成配置，在聚合口界面会显示创建成功的聚合口 ID 和成员口信息，如图 3-32 所示，参数说明表 3-12 所示。

图 3-32 聚合口显示界面

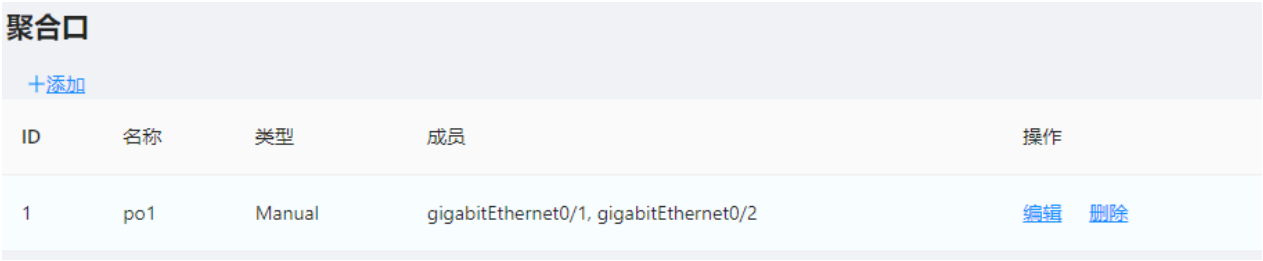


表 3-12 聚合口参数说明

配置项		说明
聚合口	ID	聚合口的 ID。
	名称	聚合口名称
	成员	具体的聚合口成员名称。

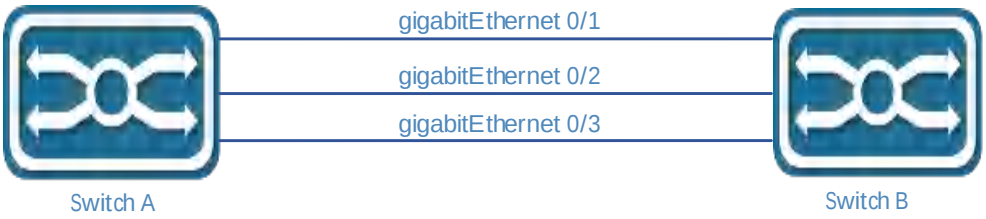
3.2.4.3 配置举例

1. 组网需求

- 如图 3-33 所示，Switch A 与 Switch B 通过各自的二层以太网端口 GigabitEthernet 0/1～GigabitEthernet /0/3 相互连接。

• Switch A 和 Switch B 由三条物理链路连接。在 Switch A 和 Switch B 上把端口配置成端口聚合组，从而实现出/入负载在各成员端口中分担。

图 3-33 端口聚合举例



2. 配置步骤

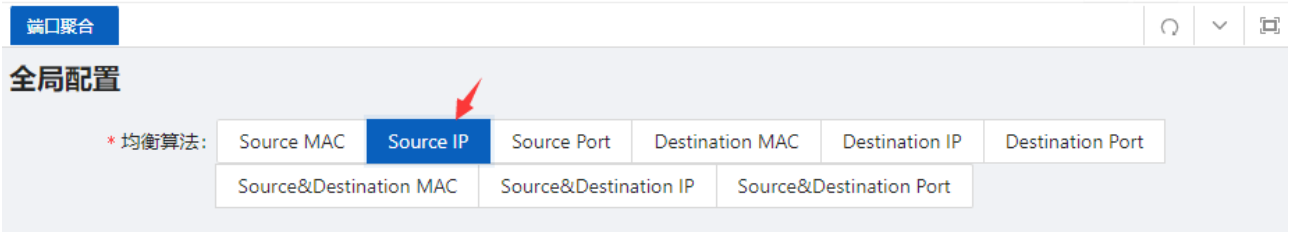
使用静态聚合口和动态聚合口均可以实现负载分担，下面将分别介绍这两种聚合口的配置方法，使用任何一种方法都可以实现需求。

方法一：配置静态聚合口

步骤 1：在导航栏中选择【配置】→【端口】→【端口聚合】，进入端口聚合配置界面。

步骤 2：在全局配置项中，选择“负载均衡算法”为 src-ip，如图 3-34 所示。

图 3-34 全局配置



步骤 3：点击“聚合口”下方的【添加】按钮，端口面板选择 GigabitEthernet 0/1、GigabitEthernet 0/2、GigabitEthernet 0/3， ID 设置为“1”，模式选择“Manual”，如图 3-35 所示。

图 3-35 聚合成员口静态配置

点击【确定】完成配置，在聚合口界面中，看到创建成功的聚合口 po1，如图 3-36 所示。

图 3-36 创建成功的静态聚合口

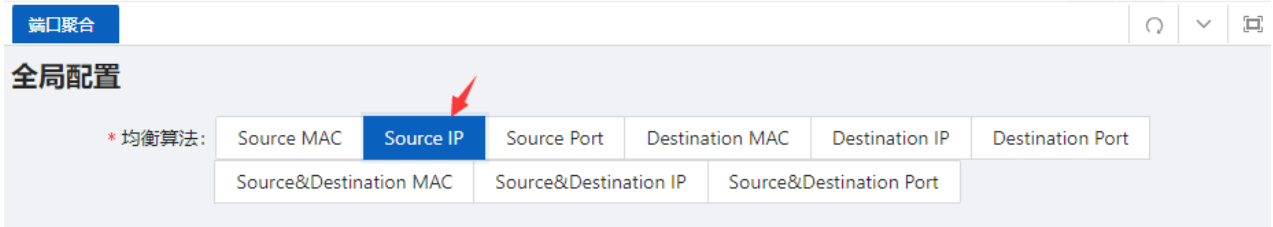
步骤 4：点击辅助区的【保存】按钮，保存当前配置。

方法二：配置动态聚合组

步骤 1：在导航栏中选择【配置】→【端口】→【端口聚合】，进入端口聚合配置界面。

步骤 2：在全局配置项中，选择“负载均衡算法”为 src-ip，如图 3-37 所示。

图 3-37 全局配置



步骤 3：点击“聚合口”下方的【添加】按钮，端口面板选择 GigabitEthernet 0/1、GigabitEthernet 0/2、GigabitEthernet 0/3， ID 设置为“1”，模式选择“Active”，如图 3-38 所示。

图 3-38 聚合成员口动态配置

点击【确定】完成配置，在聚合口界面中，看到创建成功的聚合口 po1，如图 3-39 所示。

图 3-39 创建成功的动态聚合口

步骤 4：点击辅助区的【保存】按钮，保存当前配置。

3.2.5 端口违例

在设备使用过程中，交换机端口会发生主动或者被动的违例行为，比如端口安全的违例、端口震荡违例、端口环路检测违例等。端口违例模块用于配置违例端口的恢复使能及恢复时间，并显示端口的违例行为。

配置端口违例：

在导航栏中选择【配置】→【端口】→【端口违例】，进入端口违例全局配置界面，勾选需要违例的服务，打开自动恢复按钮并配置恢复时间，点击【应用】按钮完成配置，如图 3-40 所示，全局配置参数如表 3-13 所示。

图 3-40 端口违例全局配置

表 3-13 端口违例参数说明

配置项		说明
服务	BPDU Guard	端口 BPDU 保护引起的违例行为
	Port Up/Down	端口频繁 Up/Down 导致的违例行为
	Port Security	违法端口安全导致的违例行为
	Loop Detect	端口下联设备存在环路导致的违例行为
自动恢复		开启/关闭违例端口的自动恢复
恢复时间		配置违例端口的恢复时间，单位秒

当需要手工恢复违例端口时，选择需要恢复的端口，点击【恢复】按钮，恢复端口功能。

图 3-41 端口违例状态

3.3 生成树

3.3.1 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。

3.3.2 生成树配置

生成树模块提供了生成树的全局配置、MST 配置、实例、接口等配置。

生成树全局配置

在导航栏中选择【配置】→【生成树】→【全局配置】，进入生成树全局配置界面，如图 3-42 所示。全局配置参数如表 3-14 所示。

图 3-42 生成树全局配置

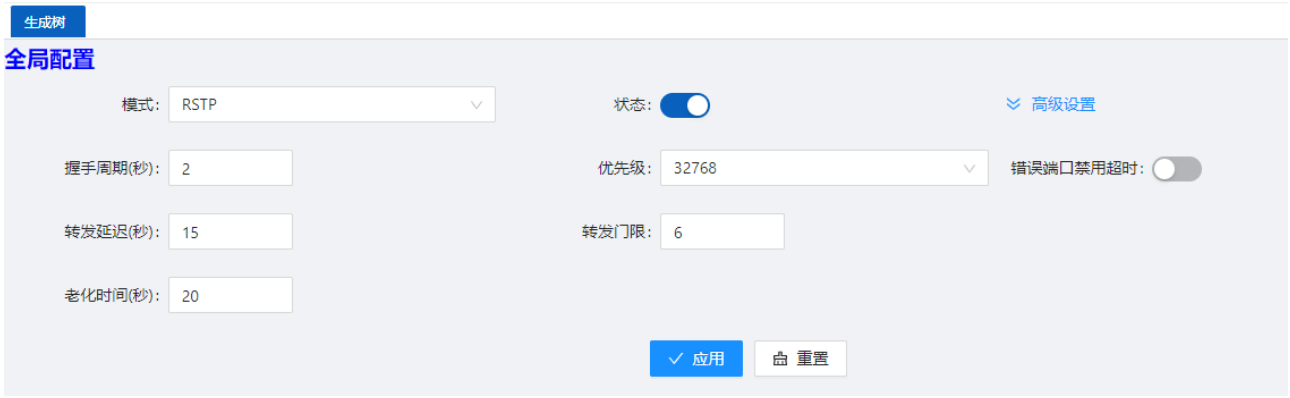


表 3-14 生成树概况参数说明

配置项		说明
全局配置	模式	设置 STP 的工作模式，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
	状态	设置是否使能全局 STP 功能
	握手周期（秒）	设置设备为检测链路故障，发送 hello 报文的周期
	优先级	桥优先级
	转发延迟（秒）	设置设备状态迁移的延迟时间

	转发门限	桥每秒最多发送的 BPDU 报文数
	老化时间（秒）	设置消息在设备内保存的最大时长
	错误端口禁用超时	配置错误端口自动禁用功能
	错误端口禁用超时时间	配置错误端口自动禁用后超时解除禁用的时间

生成树实例配置

在导航栏中选择【配置】→【生成树】→【实例配置】，进入生成树实例配置界面，如图 3-43 所示。实例配置参数如表 3-15 所示。

图 3-43 生成树实例配置

表 3-15 生成树实例配置参数说明

配置项		说明
实例	ID	实例 ID
	VLAN 列表	实例关联的所有 VLAN，以列表形式显示
	优先级	当前实例中桥的优先级
	编辑	点击对改实例进行编辑
	删除	点击删除此实例

生成树端口配置

在导航栏中选择【配置】→【生成树】→【端口配置】，进入生成树端口配置界面，如图 3-44 所示。端口配置参数如表 3-16 所示。

图 3-44 生成树全局配置

表 3-16 生成树概况参数说明

配置项		说明
端口配置	名称	接口名称
	状态	接口的生成树开关状态
	链路类型	配置接口链路类型

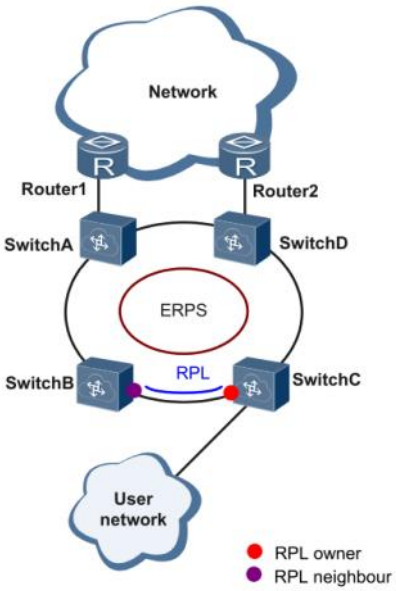
根保护	配置接口开启根保护功能
自动边缘端口	配置接口自动识别边缘端口的功能
边缘端口	配置接口为边缘端口
快速端口	配置接口为快速端口
BDPU 过滤	配置接口开启 BPDU 过滤
BDPU 保护	配置接口开启 BPDU 保护
实例/优先级/TCN 报文限制	配置实例 ID、优先级、拓扑变化通告报文抑制功能

3.4 ERPS

3.4.1 ERPS 功能概述

ERPS（GigabitEthernet ernet 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 3-45 ERPS 典型组网



3.4.2 ERPS 原理简介

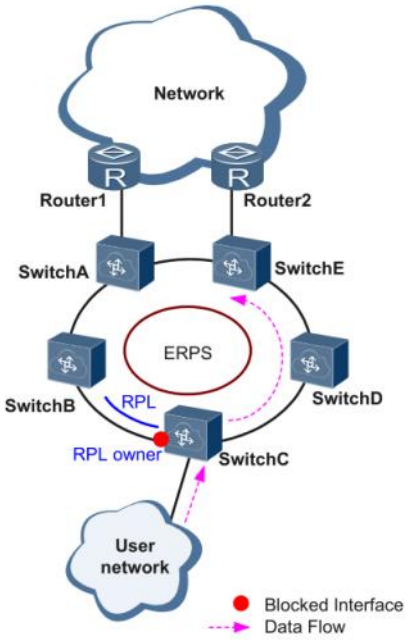
ERPS 是一种专用于以太网链路层的标准环网协议，以 ERPS 环为基本单位。每台二层交换设备上只能有两个端口加入同一个 ERPS 环。在 ERPS 环中，为了防止出现环路，可以启动破除环路机制，阻塞 RPL owner 端口，消除环路。当环网发生链路故障时，运行 ERPS 协议的设备可以迅速地放开阻塞端口，进行

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。

3.4.2.1 链路正常

如图 3-44 所示，由 Switch A～Switch E 组成的环路上各设备通信正常。

图 3-46 ERPS 链路正常

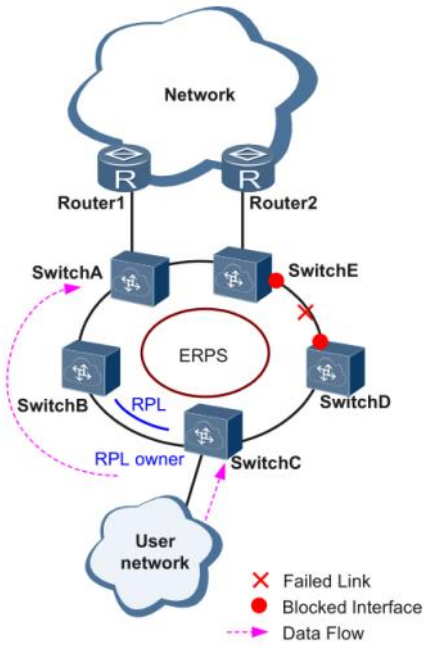


为防止环路产生，ERPS 首先会阻塞 RPL owner 端口，如果配置了 RPL neighbor 端口，该端口同样会被阻塞，其他端口可以正常转发业务流量。

3.4.2.2 链路故障

如图 3-45 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 3-47 ERPS 链路故障



3.4.2.3 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。

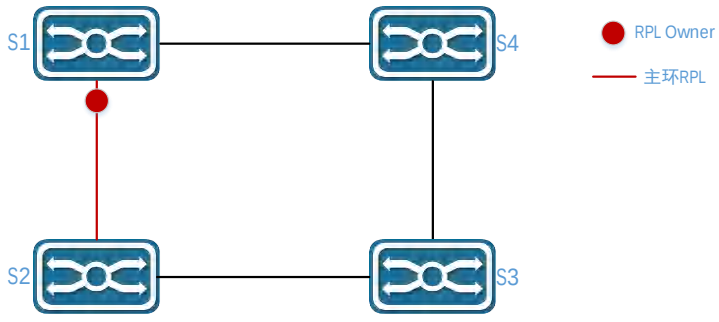
3.4.2.4 ERPS 环种类

单环：

以图 3-48 为例，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 3-48 ERPS 单环模型

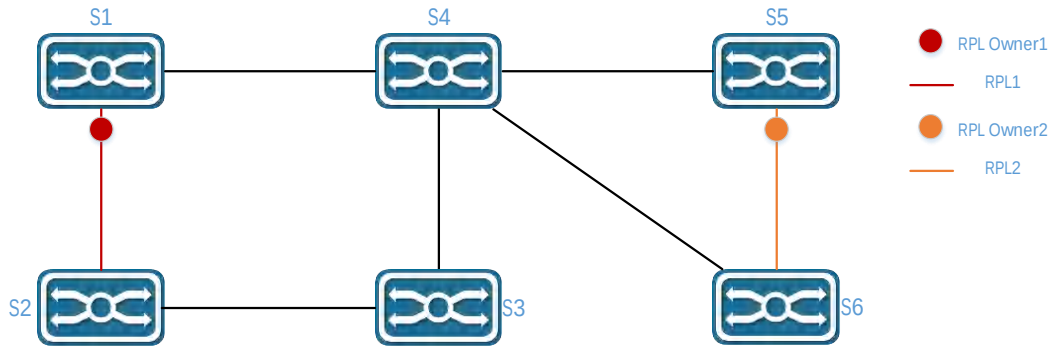


相切环：

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。以图 3-49 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 3-49 ERPS 相切环模型

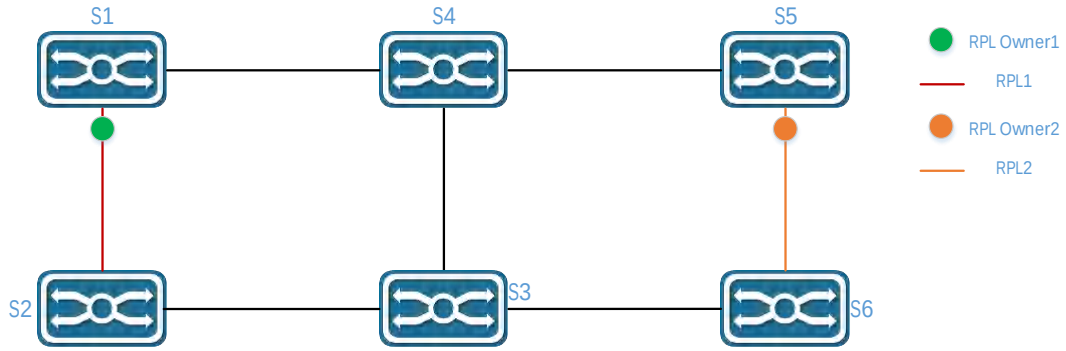


相交环：

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）。以图 3-50 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 3-50 ERPS 相交环模型



3.4.3 ERPS 配置简介

注意

- 生成树协议和 ERPS 协议不能同时开启。

3.4.3.1 ERPS 环配置

点击导航栏中选择【配置】→【ERPS】→【环配置】，进入 ERPS 环配置界面，如图 3-51 所示，参数信息具体描述如表 3-17 所示。

图 3-51 ERPS 环配置界面

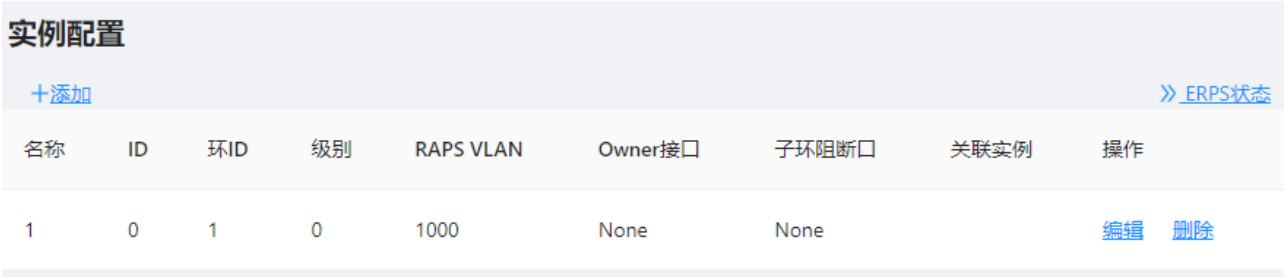
表 3-17 环配置参数说明

配置项	说明
环编号	ERPS 环 ID，可以为任意数字。每个 ERPS 环的环编号必须唯一。
东接口	ERPS 环的东向接口
西接口	ERPS 环的西向接口
操作	删除 ERPS 实例

3.4.3.2 ERPS 实例配置

点击导航栏中选择【配置】→【ERPS】→【实例配置】，进入 ERPS 实例配置界面，如图 3-52 所示。

图 3-52 ERPS 实例配置



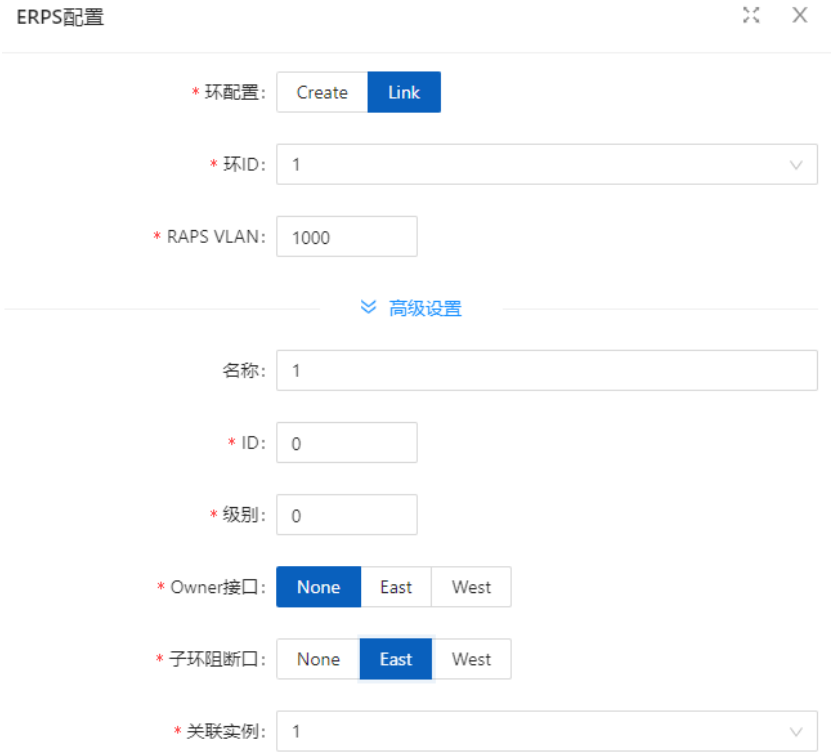
点击 ERPS“实例配置”下方的【+添加】按钮，进入 ERPS 实例配置界面，如图 3-53 所示，实例配置具体参数说明如表 3-18 描述。

表 3-18 环配置参数说明

配置项	说明
名称	实例名称，字符串格式，需要确保唯一，如数字“1”，字符“aa”
ID	配置 ERPS 实例保护的 VLAN Instance；默认所有 VLAN 属于 Instance 0；默认 id 为 0。
环编号	关联的环 ID，必须是已经创建的环
级别	ERPS 优先级，默认为 0
RAPS 管理 VLAN	同一个环中的每台交换机必须配置相同的 RAPS 管理 VLAN，用于传输 ERPS 协议报文。 RAPS 管理 VLAN 可以是虚拟 VLAN，要求与数据 VLAN 区别即可，不需要实际创建。
数据 VLAN	ERPS 数据 VLAN，设置允许在 ERPS 环中传输的 VLAN。必须是已经存在的 VLAN，如果不存在请在 VLAN 配置中新增； 支持 VLAN Range 类配置，比如“1-3,5”表示 VLAN 1,2,3,5；
Owner 接口	主环 ERPS Owner 节点，可以选择 east 接口或者 west 接口为 Owner 节点。 每个 ERPS 环有且仅有一个设备配置为 RPL owner 节点，该节点控制需要阻断的端口。

子环阻断口	子环阻断口，一个子环只有一个阻断口，可以选择 east 或者 west。 只有在相切环时才需要配置此参数，环相切的两台设备的子环必须设置子环阻断口。
关联实例	仅在需要配置子环阻断口时才需要设置，设置为与当前子环相切的环 ID。

图 3-53 ERPS 实例配置

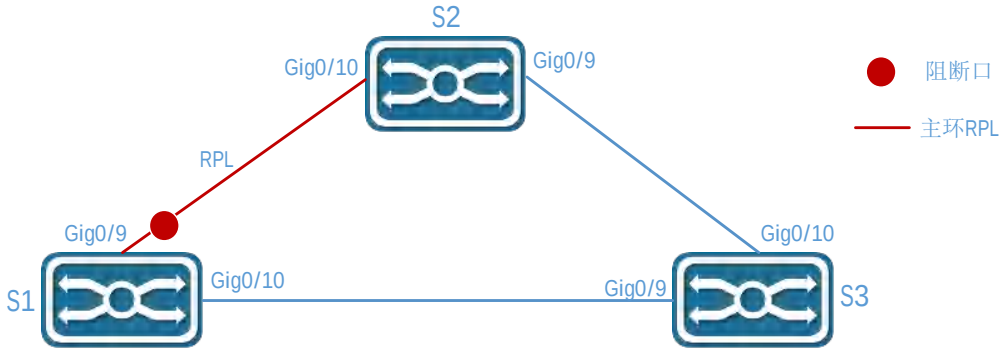


3.4.4 单环配置举例

案例需求：

3 台交换机组环网，如图 3-54 所示，配置默认阻断口为 S1 的 GigabitEthernet 0/9 口，发生故障时可以及时恢复链路确保网络可用。

图 3-54 ERPS 网络拓扑



3.4.4.1 配置交换机 S1

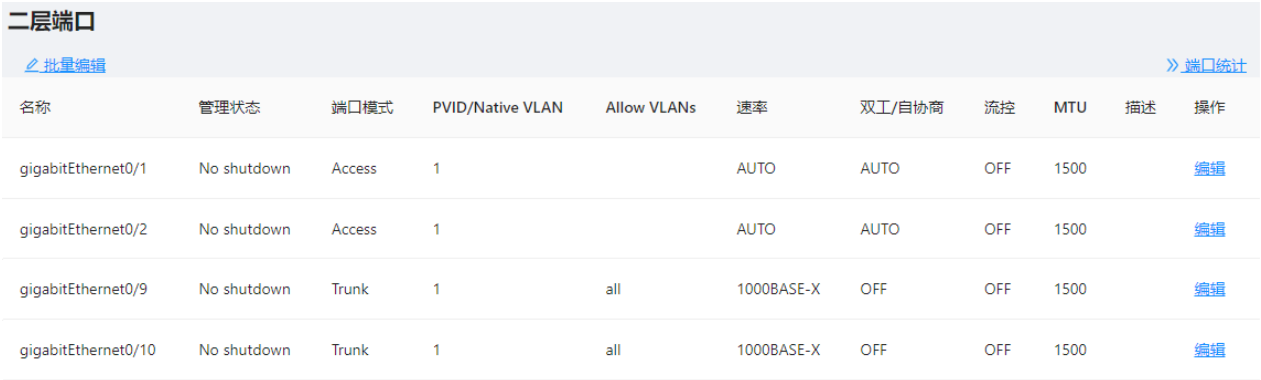
步骤 1：配置端口 9 和 10 为 trunk 口，Native Vlan 为缺省值 1。

在导航栏选择【配置】→【端口】→【端口配置】，进入接口配置界面，点击【批量编辑】按钮，如图 3-55 所示，选择端口 GigabitEthernet 0/9、GigabitEthernet 0/10，端口模式选择“Trunk”，Native Vlan 默认为“1”，Allows VLANs 为“all”。

图 3-55 端口配置界面

点击【确认】按钮，返回的接口界面如图 3-56 所示。

图 3-56 端口状态显示界面

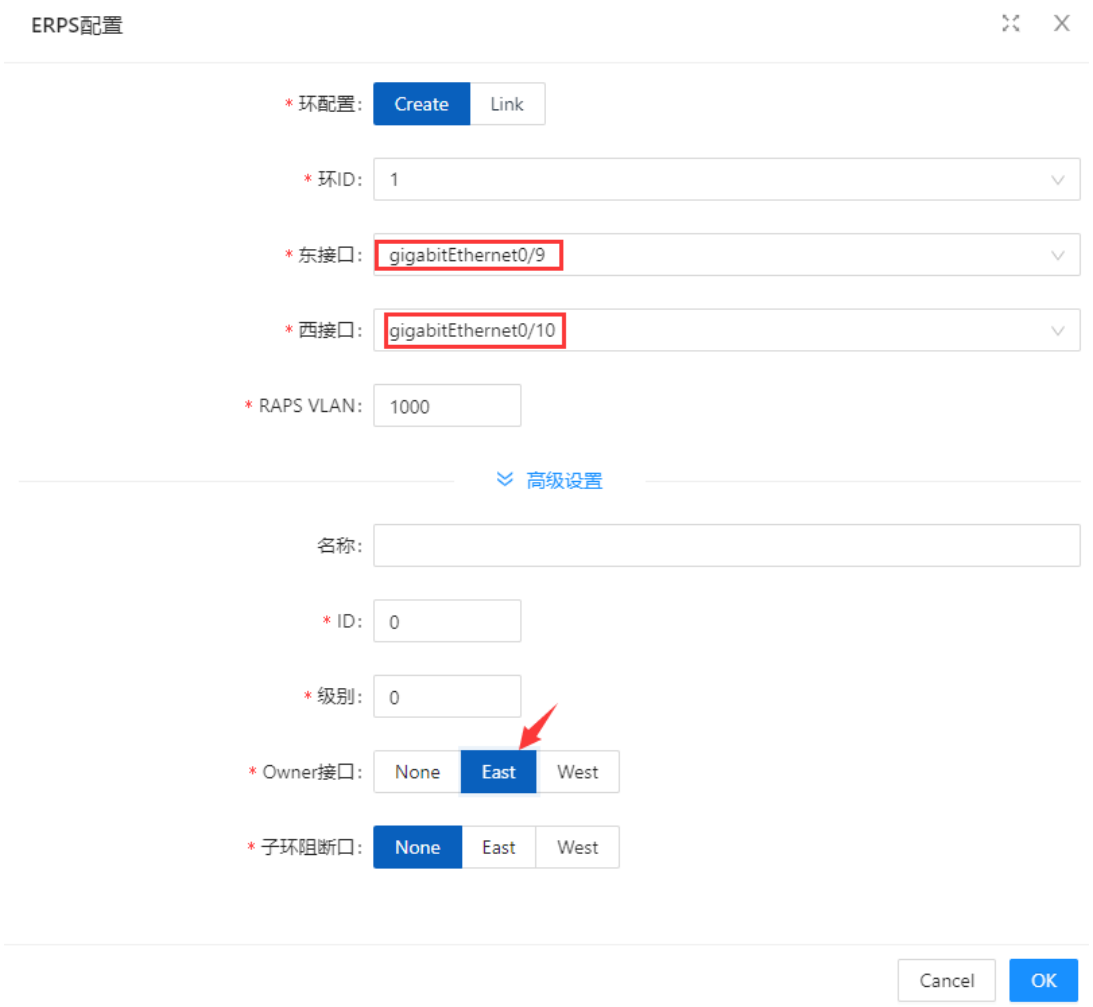


名称	管理状态	端口模式	PVID/Native VLAN	Allow VLANs	速率	双工/自协商	流控	MTU	描述	操作
gigabitEthernet0/1	No shutdown	Access	1		AUTO	AUTO	OFF	1500		编辑
gigabitEthernet0/2	No shutdown	Access	1		AUTO	AUTO	OFF	1500		编辑
gigabitEthernet0/9	No shutdown	Trunk	1	all	1000BASE-X	OFF	OFF	1500		编辑
gigabitEthernet0/10	No shutdown	Trunk	1	all	1000BASE-X	OFF	OFF	1500		编辑

步骤 2：创建 ERPS 环。

在导航栏中选择【配置】→【ERPS】，进入 ERPS 配置界面，点击换配置下方的【+添加】按钮，进入 ERPS 环配置界面，如图 3-57 所示。环编号设置为“1”，东接口设置为“GigabitEthernet 0/9”，西接口设置为“GigabitEthernet 0/10”。RAPS VLAN 默认为“1000”，ID 默认为“0”，级别默认“0”，Owner 接口“East”，子环阻断口“None”。

图 3-57 ERPS 环配置界面



点击【确认】按钮，返回如下页面，如图 3-58 所示。

图 3-58 创建成功的 ERPS 环

步骤 3：点击辅助区的【保存】按钮，保存配置。

说明

- 单环情况下，只需要设置一个阻断点就可以，阻断点的选择一般考虑在环的中间。

3.4.4.2 配置交换机 S2 和 S3

步骤 1：配置端口 9 和 10 为 trunk 口，Native Vlan 为缺省值 1。

在导航栏选择【配置】→【端口】→【端口配置】，进入接口配置界面，点击【批量编辑】按钮，如图 3-53 所示，选择端口 GigabitEthernet 0/9、GigabitEthernet 0/10，端口模式选择“Trunk”，Native Vlan 默认为“1”，Allows VLANs 为“all”，点击【OK】按钮完成配置。

步骤 2：创建 ERPS 实例

在导航栏中选择【配置】→【ERPS】，进入 ERPS 配置界面，点击“环配置”下方的【+添加】按钮，进入 ERPS 环配置界面，环编号设置为“1”，东接口设置为“GigabitEthernet 0/9”，西接口设置为“GigabitEthernet 0/10”。RAPS VLAN 默认为“1000”，ID 默认为“0”，级别默认“0”，Owner 接口“None”，子环阻断口“None”，点击【确认】按钮完成配置。创建成功的 ERPS 环如图 3-59 所示。

图 3-59 创建成功的 ERPS 环

步骤 3：选择导航栏上的【保存】按钮，保存配置。

说明

- 与 S1 不同的地方，S2 和 S3 在于阻断点 Owner 接口=None。

3.5 PoE

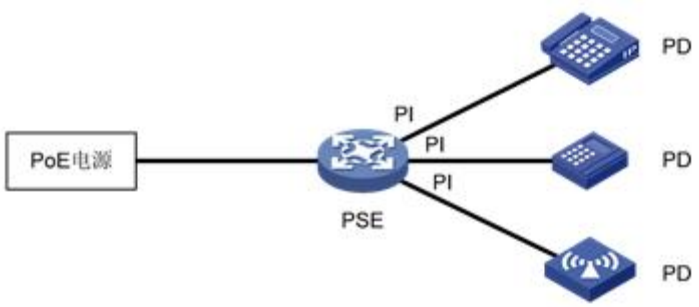
3.5.1 PoE 简介

PoE（Power over GigabitEthernet ernet，以太网供电，又称远程供电）是指设备通过以太网电口，利用双绞线对外接 PD（Powered Device，受电设备）进行远程供电。

PoE 系统组成

PoE 系统如图 3-60 所示，包括 PoE 电源、PSE（Power Sourcing Equipment，供电设备）、PI（Power Interface，电源接口）和 PD。

图 3-60 PoE 系统



1. PoE 电源

PoE 电源为整个 PoE 系统供电。

2. PSE

PSE 是直接给 PD 供电的设备。PSE 分为内置（Endpoint）和外置（Midspan）两种：内置指的是 PSE 集成在交换机内部，外置指的是 PSE 与交换机相互独立。我司的 PSE 均采用内置方式，PSE 支持的主要功能包括寻找、检测 PD，对 PD 分类，并向其供电，进行功率管理，检测与 PD 的连接是否断开等。

3. PI

PI 是指具备 PoE 供电能力的以太网接口，也称为 PoE 接口，包括 FE 和 GE 接口。

PoE 接口远程供电有两种模式：

信号线供电模式：PSE 使用 3/5 类双绞线中传输数据所用的线对（1、2、3、6）向 PD 传输数据的同时传输直流电。

空闲线供电模式：PSE 使用 3/5 类双绞线中没有用于数据传输的线对（4、5、7、8）向 PD 来传输直流电。

4. PD

PD 是接受 PSE 供电的设备，如 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头等。

PD 设备在接受 PoE 电源供电的同时，可以连接其它电源，进行电源冗余备份。

3.5.2 配置 PoE

说明

1、在配置 PoE 功能前，请确保 PoE 电源或 PSE 已经处于正常工作状态，否则，可能无法进行 PoE 配置或者配置的 PoE 功能不能生效。

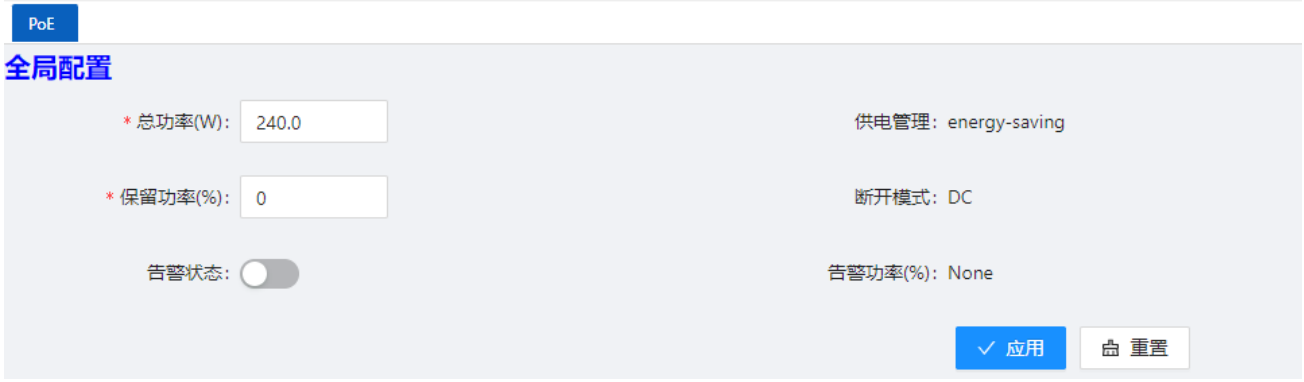
2、对于外置电源的交换机，输入电压范围为 44-57V，为了获得更稳定的供电，建议 AT 设备供电电压大于 50V，BT 设备供电电压大于 53V。

PoE 配置步骤：

（1）在导航栏中选择【配置】→【PoE 管理】，进入 PoE 管理界面。

（2）在 PoE 全局配置中设置“最大功率”和“保留功率”，点击【应用】完成配置，如图 3-61 所示。

图 3-61 PoE 全局配置



PoE 全局配置参数说明，如表 3-19 所示。

表 3-19 PoE 全局配置参数说明

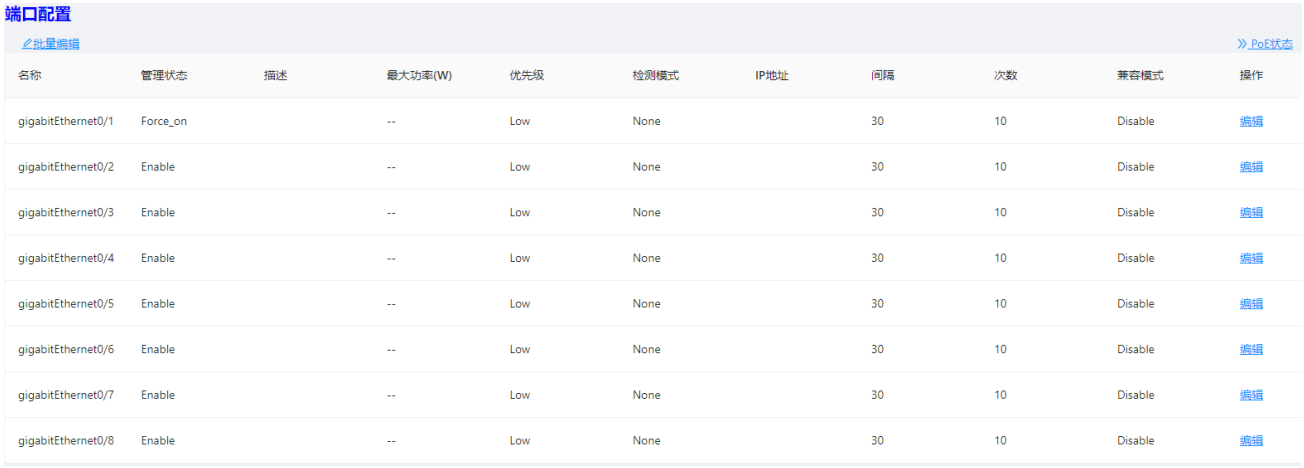
配置项	说明
总功率	默认情况下，设备默认提供的功率为 15.4W*端口数，如 8 口设备所能提供的最大功率为 123.2W • 外接电源的设备，此参数请根据实际配置的电源功率来填写 • 内置电源的设备，此参数请参考产品手册里对于 PoE 功率的描述
保留功率	为防止电源波动设置的预留功率 • 外接电源的设备，此参数建议填写主板的消耗功率 • 内置电源的设备，此参数可以默认为 0
供电管理	默认为节能模式，每个端口分配的功率以实际消耗的功率计算，PSE 会默认把多余的功率分配给其他端口
端口模式	默认为 DC disconnect 模式
告警状态	开启/关闭电源不足时 log 告警
告警功率(%)	告警水线设置，PoE 消耗功率超过此水线值时，系统会自动输出 log 告警

（3）选择需要配置的端口，点击【编辑】，进入接口配置界面，如图 3-62 所示。

图 3-62 PoE 接口配置

（4）单击【确定】按钮完成操作，返回 PoE 主界面，如图 3-63 所示。

图 3-63 PoE 接口配置主界面



（5）单击辅助区的【保存】按钮，保存配置。

PoE 端口状态参数说明，如表 3-20 所示。

表 3-20 PoE 参数说明

配置项	说明
名称	指示面板端口号
管理状态	Disabled：关闭端口的 PoE 供电 Enable：开启端口的 PoE 供电 Force_on：强制开启端口的 PoE 供电，该功能的实现方式为跳过 PD 负载检测和 PD 分级检测，直接对 PD 负载供电。在该模式下，默认最大负载功率为 15w，如果需要对大于 15w 的设备进行供电，需要同时配置最大功率参数。
描述	添加 PoE 端口的描述
最大功率	配置该端口的最大功率。 对于 AF/AT 端口，端口最大功率范围为 1-30 对于 BT 端口，端口最大功率范围为 1-90 默认模式下，该端口将根据 PD 等级进行功率管理。
优先级	配置端口的供电优先级 用户可以配置 PoE 交换机的接口供电优先级。优先级从高到低依次为：high、medium 和 low。在 PoE 交换机整机功率不足的时候，低优先级的端口先掉电。 相同优先级的端口优先级按照端口号顺序排列，端口号小的优先级高，比如端口 0/1 的优先级就比端口 0/2 和 0/3 高。 相同优先级端口，新插入的端口，不会影响到已经处于供电状态的 PD 设备的供电情况。不同优先级的端口不受这个特性影响，高优先级端口可以抢占低优先级的端口。
检测模式	None：关闭 PD 检测功能 Flow：开启 Flow 模式的 PD 检测功能。此功能通过监控端口计数器实现，如果一段时间内端口计数器没有改变，则判断为该端口下挂的 PD 设备处于死机状态，则关闭供电几秒后再开启供电。 Ping：开启 Ping 模式的 PD 检测功能。此功能通过不断对 PD 负载 ping 包来实现，如果一段时间内 ping 包不通，则判断为该端口下挂的 PD 设备处于死机状态，则关闭供电几秒后再开启供

	电。建议启用此功能前，先用交换机【诊断】→网络工具】→【ping】来测试 PD 设备 ping 包可达。
IP 地址	Ping 模式下，PD 负载的 IP 地址，要求交换机和 PD 负载处于同一个网段。
间隔	检测模式开启时，检测时间间隔
次数	检测模式开启时，检测次数 提示 PD 负载的启动时间必须要小于间隔*次数，不然会造成 PD 负载一直处于启动→下电→启动这个状态。
兼容模式	ON/OFF，默认为 OFF。 OFF：只支持标准的 PD 设备，检测电阻在 19k-26.5k 之间，检测电容小于 150nF。 ON：支持非标的 PD 设备，可以对检测电阻和电容值超过标准值之外的部分 PD 设备进行供电。

3.6 安全

3.6.1 端口安全

3.6.1.1 概述

Port Security 功能通过对端口合法 MAC 地址个数限制，达到限制非法用户对该端口访问的目的，对于非法 MAC 的报文，将直接丢弃。

合法 MAC 可通过静态或动态的方式生成。静态合法 MAC 通过用户命令行配置生成；动态合法 MAC 则通过 MAC 地址学习功能动态生成。

当端口上安全地址个数已经达到最大安全地址个数配置值后，新 MAC 访问端口将认定为非法 MAC，产生违例事件，用户可配置违例事件产生时的应对操作，分别为 restrict 或 shutdown 端口。

Restrict: 禁止非法 MAC 数据通过，并产生告警 log 提示信息。非法 MAC 将在 MAC 地址老化时间内禁止访问端口。通过 shutdown、no shutdown 端口可恢复。

Shutdown: 强制端口 down 掉，并可配置端口恢复时间，时间到了端口自动恢复；也可通过 shutdown，no shutdown 命令恢复。

若希望将动态安全用户转换为静态安全用户，可开启端口上 sticky 功能。端口开启 sticky 功能，端口上学习到的动态用户将以静态用户的方式存在，若保存配置，设备重启后依然存在。

说明

- 仅支持 L2 端口配置端口安全，如普通物理口，聚合口。
- 仅支持在 access 模式下配置端口安全功能。
- 不支持聚合口成员口配置端口安全功能。
- 不支持 SPAN 的目的端口配置端口安全功能。
- 不支持在已配置静态 MAC 地址端口配置端口安全功能。

3.6.1.2 配置端口安全

端口配置

在导航栏中选择【配置】→【安全】→【端口安全】→【端口配置】，进入端口配置概况界面，如图 3-64 所示。

图 3-64 端口配置概况

点击“端口配置”下方的【批量编辑】按钮，进入端口配置页面，如图 3-65 所示。端口配置各参数说明如表格 3-21 所示。

图 3-65 端口配置页面

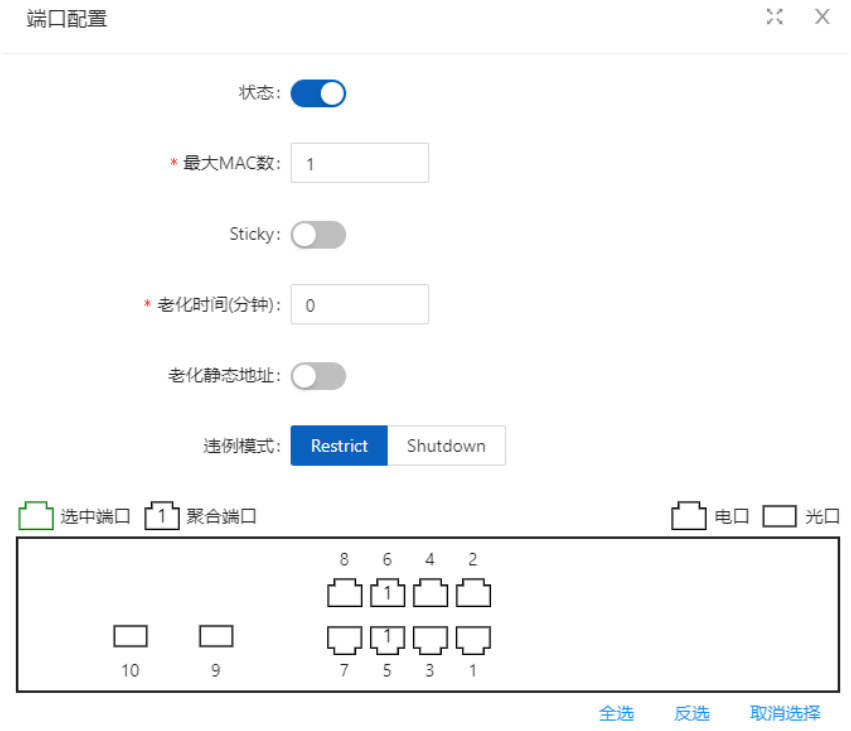


表 3-21 端口配置参数说明

配置项		说明
端口配置	状态	使能/关闭接口上端口安全功能
	最大 MAC 数	配置端口最大安全 MAC 地址个数，默认最大安全地址个数为 1，范围<1-1024>

Sticky	开启/关闭 Sticky 功能
老化时间	配置安全地址老化时间，单位分钟。默认老化时间为 0，表示关闭老化功能 老化时间范围<0-1440> 默认老化功能仅对动态、sticky 安全地址生效
老化静态地址	配置使能静态安全地址老化功能
违例模式	配置端口安全违例处理，默认违例处理模式 restrict Restrict：禁止非法用户数据通过，并 log 提示 Shutdown：shutdown 端口，并在 errdisable 恢复时间后恢复，通过 shutdown/no shutdown 命令，同样可恢复

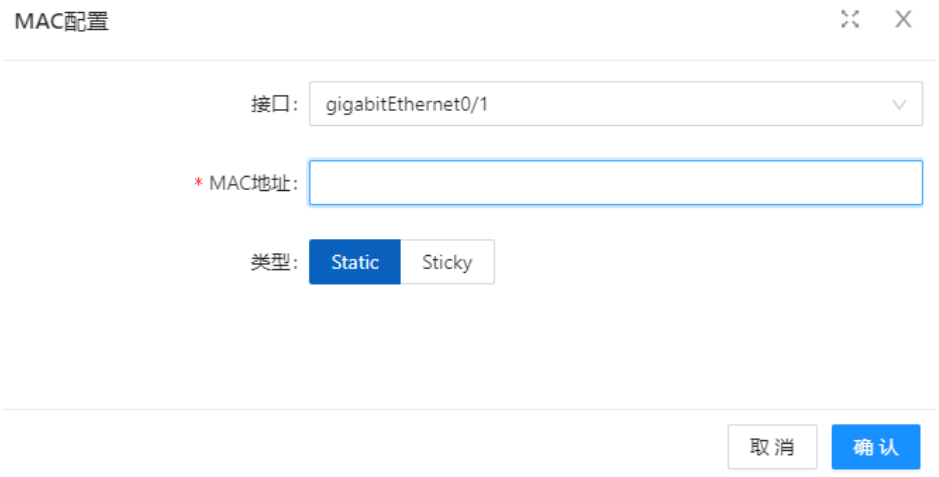
MAC 配置

在导航栏中选择【配置】→【安全】→【端口安全】→【MAC 配置】，进入 MAC 配置概况界面，如图 3-66 所示。

图 3-66 MAC 概况界面

点击“MAC 配置”下方的【添加】按钮，进入 MAC 配置页面，如图 3-67 所示。

图 3-67 MAC 配置界面



MAC 配置各参数说明如表格 3-22 所示。

表 3-22 MAC 配置参数说明

配置项		说明
端口配置	接口	选择需要配置的接口
	MAC 地址	配置静态安全地址，安全地址格式：XXXX.XXXX.XXXX 安全地址不能是广播或组播地址
	类型	配置 MAC 地址为 Static 或者 Sticky

3.6.1.3 配置举例

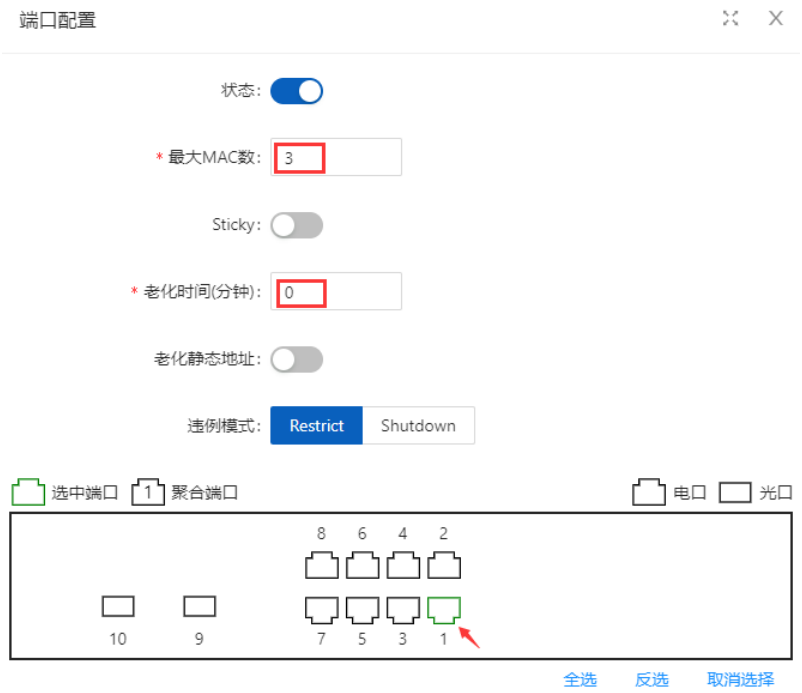
1) 需求

- 限制接口 GigabitEthernet 0/1 合法用户数 3 个，MAC 分别为 0001.0001.0001、0001.0001.0002、和 0001.0001.0003 的非法用户不能访问设备。

2) 典型配置举例

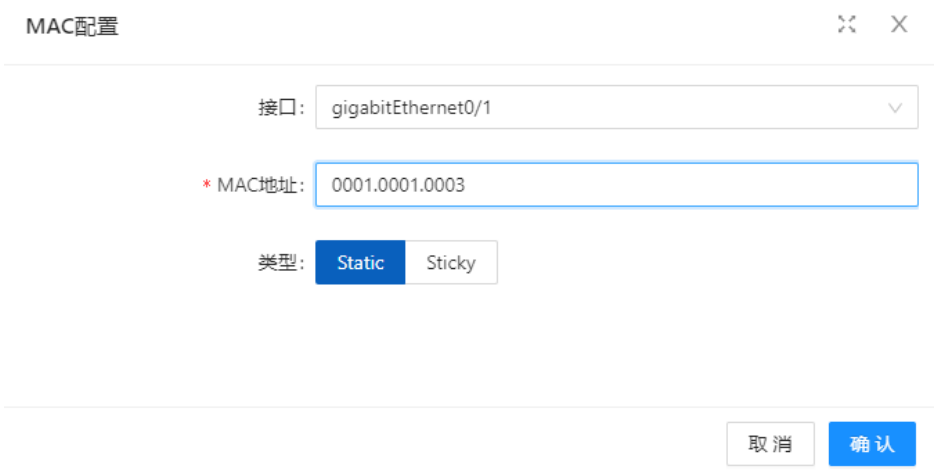
步骤 1：在导航栏中选择【配置】→【安全】→【端口安全】，点击“端口安全”下方的【批量配置】按钮，进入端口配置界面，在端口面板选择 GigabitEthernet 0/1，其他配置如下图 3-68 所示。

图 3-68 配置端口 GigabitEthernet 0/1



步骤 2：在当前页面点击“MAC 配置”下方的【添加按钮】，进入 MAC 配置界面，接口选择 GigabitEthernet 0/1，在 MAC 地址对话框输入“0001.0001.0003”，类型选择“Static”，具体配置如下图 3-69 所示。

图 3-69 MAC 配置界面



在 MAC 地址栏，依次输入三个静态地址，配置成功后的界面如图 3-70 所示。

图 3-70 配置成功的 MAC 地址

3.6.2 IP Source Guard

3.6.2.1 概述

IP Source Guard：

Ip Source Guard 绑定功能，允许符合 IP+MAC 绑定的 IP 报文通过端口，不符合的报文则直接丢弃，从而达到防止 IP/MAC 欺骗攻击的目的。

Ip Source Guard 的绑定条目，主要有两个来源：用户静态配置与 ip dhcp snooping 环境中动态获取。

用户静态配置：主要应对局域网络中 IP 地址静态配置的主机用户。

Ip dhcp snooping 动态获取：主要应对局域网络中通过 dhcp 动态获取到 IP 地址的主机用户。

IP/MAC 欺骗攻击：非法 MAC 用户，发送带合法源 IP 的 IP 报文，实现访问身份的合法化。

ARP Check：

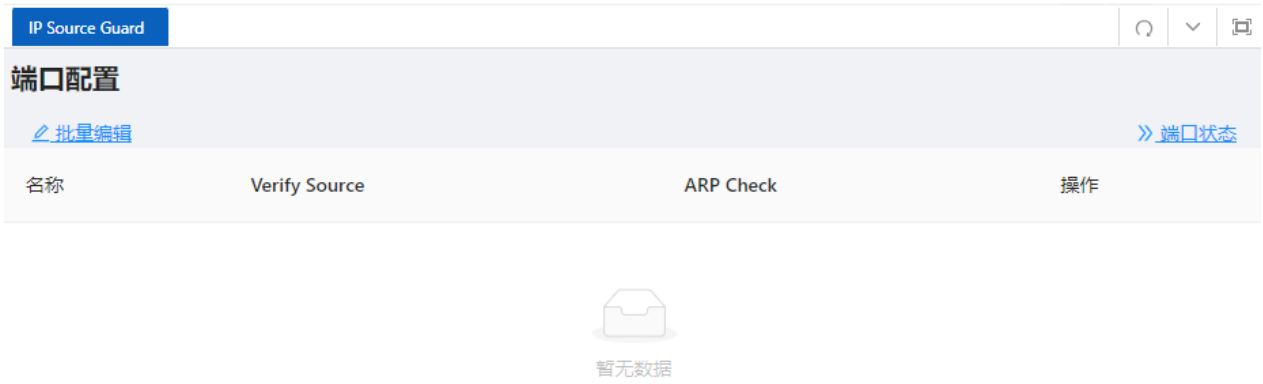
Arp-check(ARP 报文检查)功能，对端口下所有的 ARP 报文进行过滤，对所有非法的 ARP 报文进行丢弃，能够有效的防止网络中 ARP 欺骗，提高网络的稳定性。

在支持 Arp-check 功能的设备中，Arp-check 功能能够根据 IP Source Guard 等安全应用模块所生成的合法用户信息(IP+MAC)产生相应的 ARP 过滤信息，从而实现对网络中的非法 ARP 报文的过滤。

3.6.2.2 配置 IP Source Guard

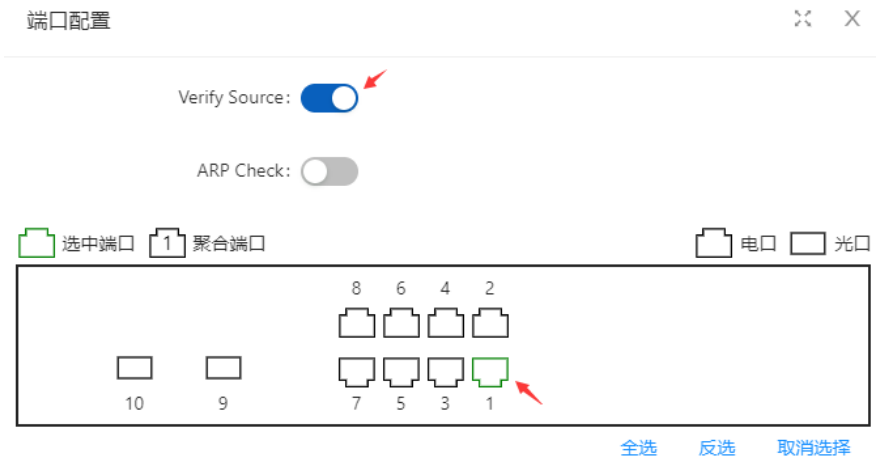
步骤 1：在导航栏中选择【配置】→【安全】→【IP Source Guard】，进入 IP Source Guard 端口配置概况页面，如图 3-71 所示。

图 3-71 IP Source Guard 概况界面



步骤 2：在当前页面，点击“端口配置”下方的【批量配置】按钮，进入 IP Source Guard 端口配置界面。选中需要配置的端口，点击“Verify Source”开启按钮，如图 3-72 所示，点击【确认】按钮，完成配置。

图 3-72 IP Source Guard 端口配置界面



步骤 3：在当前页面，点击“用户配置”下方的【添加】按钮，进入 IP Source Guard 用户配置界面。选择需要配置的接口、VID，输入 MAC 地址和 IP 地址，如图 3-73 所示。

图 3-73 IP Source Guard 用户配置界面

点击【确认】按钮，完成配置，在用户配置界面可以看到创建成功的 IP Source Guard 规则，如图 3-74 所示。

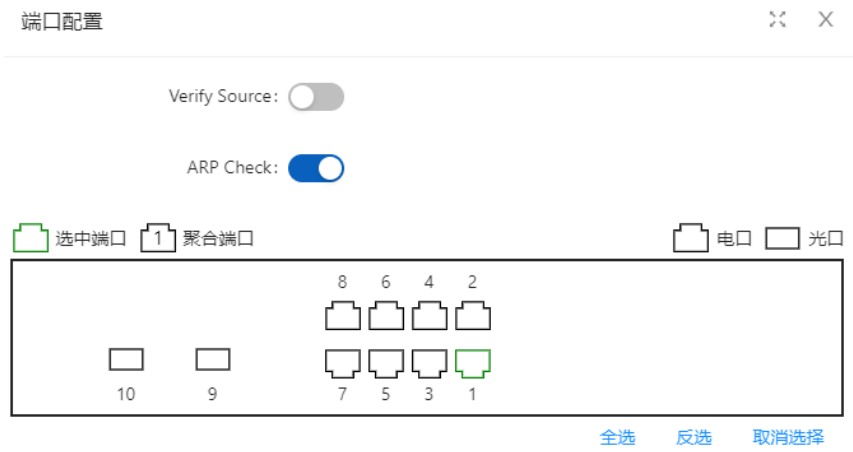
图 3-74 创建成功的 IP Source Guard 规则

3.6.2.3 配置 ARP Check

步骤 1：在导航栏中选择【配置】→【安全】→【IP Source Guard】，进入 IP Source Guard 端口配置概况页面。

步骤 2：在当前页面，点击“端口配置”下方的【批量配置】按钮，进入 IP Source Guard 端口配置界面。选中需要配置的端口，点击“ARP Check”开启按钮，如图 3-75 所示，点击【确认】按钮，完成配置。

图 3-75 ARP Check 端口配置界面



步骤 3：在当前页面，点击“用户配置”下方的【添加】按钮，进入 IP Source Guard 用户配置界面。选择需要配置的接口、VID，输入 MAC 地址和 IP 地址，如图 3-76 所示。

图 3-76 ARP Check 端口配置界面

点击【应用】按钮，完成配置，在用户配置界面看到创建成功的 ARP Check 规则，如图 3-77 所示。

图 3-77 创建成功的 ARP Check 规则

3.6.3 Dot1X

3.6.3.1 概述

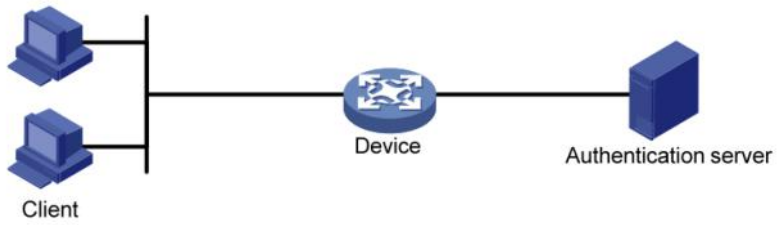
最初，IEEE 802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户设备进行认证，以便用户设备控制对网络资源的访问。

802.1X 的体系结构

802.1X 系统中包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Authentication server），如图 3-78 所示。

图 3-78 802.1X 体系结构



- 客户端是请求接入局域网的用户终端设备，它由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端是局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口（物理端口或逻辑端口），并通过与服务器的交互来对所连接的客户端进行认证。
- 认证服务器用于对客户端进行认证、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。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。在一些规模较小的网络环境中，认证服务器的角色也可以由设备端来代替，即由设备端对客户端进行本地认证、授权和计费。

802.1X 对端口的控制

1、受控/非受控端口

设备端为客户端提供接入局域网的端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

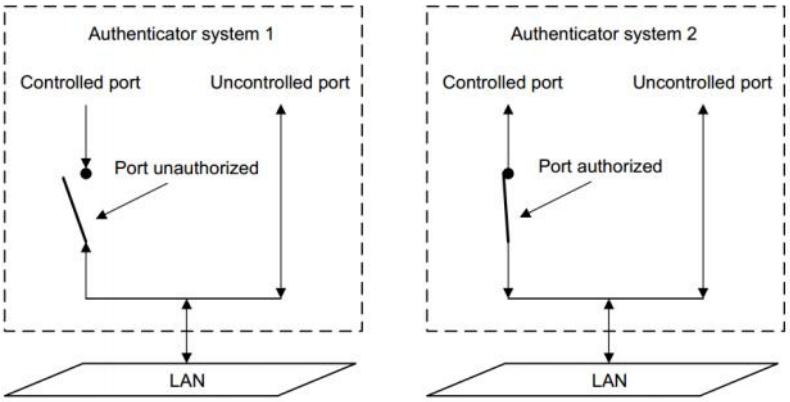
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

2、授权/非授权状态

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

图 3-79 显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1X 认证系统的端口状态。系统 1 的受控端口处于非授权状态，不允许报文通过；系统 2 的受控端口处于授权状态，允许报文通过。

图 3-79 受控端口上授权状态的影响



3、受控方向

在非授权状态下，受控端口可以被设置成单向受控和双向受控。

- 处于双向受控状态时，禁止帧的发送和接收；
- 处于单向受控状态时，禁止从客户端接收帧，但允许向客户端发送帧。

说明

我司设备上的受控端口只能处于单向受控状态。

4.4.1.3 802.1X 的认证触发方式

802.1X 的认证过程可以由客户端主动发起，也可以由设备端发起。

1、客户端主动触发方式

- 组播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文目的地址为组播 MAC 地址 01-80-C2-00-00-03。
- 广播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文的目的地址为广播 MAC 地址。该方式可解决由于网络中有些设备不支持上述的组播报文，而造成认证设备无法收到客户端认证请求的问题。

说明

目前我司设备仅支持组播触发方式。

2、设备端主动触发方式

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 组播触发：设备每隔 N 秒（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。

- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

802.1X 的认证过程

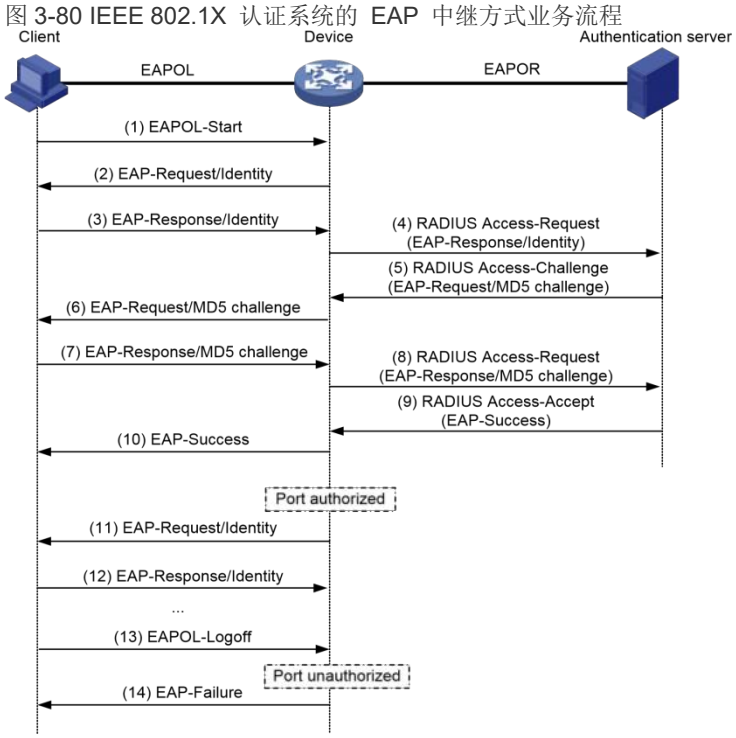
802.1X 系统支持采用 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互。

EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP 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，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 MD5-Challenge 认证方法为例介绍基本业务流程，认证过程如图 3-80 所示。

图 3-80 IEEE 802.1X 认证系统的 EAP 中继方式业务流程



(2) 当用户需要访问外部网络时打开 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。此时，客户端程序将向设备端发出认证请求帧（EAPOL-Start），开始启动一次认证过程。

(3) 设备端收到认证请求帧后，将发出一个 Identity 类型的请求帧（EAP-Request/Identity）要求用户的客户端程序发送输入的用户名。

(4) 客户端程序响应设备端发出的请求，将用户名信息通过 Identity 类型的响应帧（EAP-Response/Identity）发送给设备端。

(5) 设备端将客户端发送的响应帧中的 EAP 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给认证服务器进行处理。

(6) 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列表中对比，找到该用户名对应的密码信息，用随机生成的一个 MD5 Challenge 对密码进行加密处理，同时将此 MD5 Challenge 通过 RADIUS Access-Challenge 报文发送给设备端。

(7) 设备端将 RADIUS 服务器发送的 MD5 Challenge 转发给客户端。

(8) 客户端收到由设备端传来的 MD5 Challenge 后，用该 Challenge 对密码部分进行加密处理，生成 EAP-Response/MD5 Challenge 报文，并发送给设备端。

(9) 设备端将此 EAP-Response/MD5 Challenge 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给 RADIUS 认证服务器。

(10) RADIUS 服务器将收到的已加密的密码信息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，并向设备端发送认证通过报文（RADIUS Access-Accept）。

(11) 设备收到认证通过报文后向客户端发送认证成功帧（EAP-Success），并将端口改为授权状态，允许用户通过端口访问网络。

(12) 用户在线期间，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。

(13) 客户端收到握手报文后，向设备发送应答报文，表示用户仍然在线。缺省情况下，若设备端发送的两次握手请求报文都未得到客户端应答，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。

(14) 客户端可以发送 EAPOL-Logoff 帧给设备端，主动要求下线。

(15) 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。

说明

EAP 中继方式下，需要保证在客户端和 RADIUS 服务器上选择一致的 EAP 认证方法，而在设备上，只需要配置 802.1X 用户的认证方式为 EAP 即可。

802.1X 的接入控制方式

设备不仅支持协议所规定的基于端口的接入认证方式（Port Based），还对其进行了扩展、优化，支持基于 MAC 的接入控制方式（MAC Based）。

- 当采用基于端口的接入控制方式时，只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 采用基于 MAC 的接入控制方式时，该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。

3.6.3.2 配置 802.1X

查看 802.1X 概况

在导航栏中选择【配置】→【安全】→【Dot1x】，进入 Dot1x 概况界面，如图 3-81 所示。在概况界面中可以显示 802.1X 配置情况，各参数说明如表格 3-23 所示。

图 3-81 802.1X 概况界面

表 3-23 802.1X 概况参数说明

配置项		说明
全局配置	状态	功能开关
	RADIUS 配置	点击跳转到 RADIUS 配置界面
端口配置	名称	物理端口
	端口受控	端口受控模式
	协议版本	使用的 802.1X 协议版本
	静默时间	设置静默定时器的值，当 802.1X 用户认证失败以后，设备需要静默一段时间（通过“静默时长”设定）后再重新发起认证。在静默期间，设备不进行 802.1X 认证的相关处理。
	发送周期	报文重传周期
	重认证周期	设置周期性重认证定时器的值 当端口上启用了周期性重认证功能时，设备端会在用户认证成功后启动周期性重认证定时器，用于周期性的对在线用户发起重认证，以便定时更新服务器对用户的授权信息
	客户端超时时间	设置客户端超时定时器的值 当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备端启动此定时器，若在该定时器设置的时长内，设备端没有收到客户端的响应，设备端将重发该报文
	服务器超时时间	设置服务器超时定时器的值 当设备端向认证服务器发送了 RADIUS Access-Request 请求报文后，设备端启动服务器超时定时器，若在该定时器设置的时长内，设备端没有收到认证服务器的响应，设备端将重发认证请求报文

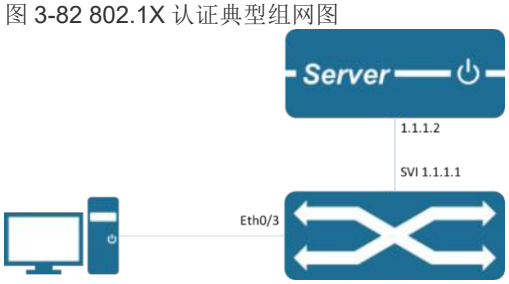
3.6.3.3 802.1X 配置举例

1) 场景需求

- 要求在端口 GigabitEthernet 0/3 上对接入用户进行认证，以控制其访问 Internet。
- RADIUS 服务器组 IP 地址 1.1.1.2。
- 设置系统与 RADIUS 服务器交互报文时的共享密钥为 name。

2) 组网图

图 3-82 802.1X 认证典型组网图



3) 典型配置举例

步骤 1：配置服务器端

服务器端：

配置 NAS 认证设备 1.1.1.1 及通信密钥 name。

本例中使用 freeradius 作为服务器，主要配置如下：

vim /etc/freeRADIUS/3.0/clients.conf

添加

```
client 1.1.1.1 {
        ipaddr = 1.1.1.1
        secret = name
}
```

添加用户账户 test 密码 test。

cat /etc/freeRADIUS/3.0/mods-config/files/authorize | grep "password"

testing Cleartext-Password := "password"

需要支持对应的认证方法，比如 EAP-MSCHAPv2

步骤 2：配置 RADIUS 服务器。

在导航栏中选择【配置】→【安全】→【RADIUS】，进入如图 3-83 所示页面。

图 3-83 RADIUS 服务器概况界面

点击“服务器”下方的【添加】按钮，进入 RADIUS 服务器配置界面，如图 3-84 所示，配置 RADIUS 服务器 IP 为 1.1.1.2，认证端口默认为 1812，输入密码，超时时间为默认 5S，重传次数为 3，点击【确认】按钮完成配置。

图 3-84 RADIUS 服务器配置界面

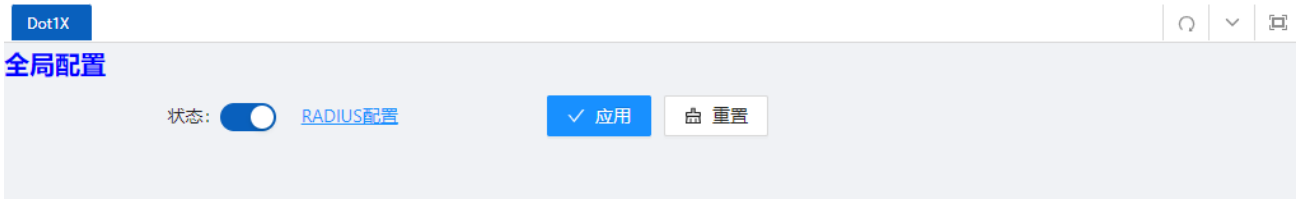
配置完成后，自动返回如下界面，如图 3-85 所示，可以看到创建成功的 RADIUS 服务器。

图 3-85 RADIUS 服务器显示界面

步骤 3：开启 802.1X 认证全局使能。

在导航栏中选择【配置】→【安全】→【Dot1x】，进入如图 3-86 所示页面，点击“状态”【启用/禁用】按钮，，点击【应用】按钮开启 802.1X 认证。

图 3-86 802.1X 全局配置界面



步骤 4：配置交换机端口 3 开启 802.1X 认证全局使能。

在当前界面下，点击“端口配置”下方的【批量配置】按钮，进入 802.1X 端口配置页面，开启端口受控，协议版本为“2”，端口面板选择 GigabitEthernet 0/3，如图 3-87 所示。

图 3-87 802.1X 端口配置界面

点击【确认】按钮完成配置，自动返回如下界面，如图 3-88 所示，可以看到创建成功的条例。

图 3-88 802.1X 端口配置显示界面

步骤 5：配置认证客户端

开启 802.1X 认证客户端，使用账户 test 登录。

需要支持对应的认证方法，比如 EAP-MSCHAPv2 方法。

3.6.4 MAC 认证

3.6.4.1 概述

MAC 地址认证简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或者密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被添加为静默 MAC。在静默时间内（可通过静默定时器配置），来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

注意

若配置的静态 MAC 与静默 MAC 相同，则 MAC 地址认证失败后的 MAC 静默功能将会失效。

目前设备支持 MAC 地址认证：

- 通过 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器进行远程认证。

目前，MAC 地址认证支持两种类型的用户名格式：

- MAC 地址用户名：使用用户的 MAC 地址作为认证时的用户名和密码。

RADIUS 服务器认证方式进行 MAC 地址认证

当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作：

- 采用 MAC 地址用户名时，设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器。
- 采用固定用户名时，设备将已经在本地配置的用户名和密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器。

RADIUS 服务器完成对该用户的认证后，认证通过的用户可以访问网络。

MAC 地址认证定时器

MAC 地址认证过程受以下定时器的控制：

- 认证超时定时器：用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果认证超时定时器超时时设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

3.6.4.2 配置 MAC 认证

查看 MAC 认证概况

在导航栏中选择【配置】→【安全】→【MAC 认证】，进入 MAC 认证概况界面，如图 3-89 所示页面。在“概况”中可以显示 MAC 认证配置情况，各参数说明如表格 3-24 所示。

图 3-89 MAC 认证概况界面

表 3-24 MAC 概况参数说明

配置项		说明
全局配置	状态	功能开关
	RADIUS 配置	点击跳转到 RADIUS 配置界面
端口配置	名称	端口名称
	状态	功能状态，开启或关闭
	MAC 地址老化	是否启用 MAC 老化功能
	操作	点击编辑该条例

配置 MAC 认证

在导航栏中选择“安全 >MAC 认证 > 配置 ”，进入如图 3-90 所示页面。在此页面，可以进行 802.1X 的全局配置以及基于各个端口的配置。配置参数说明如表格 3-25 所示。

图 3-90 MAC 认证配置界面

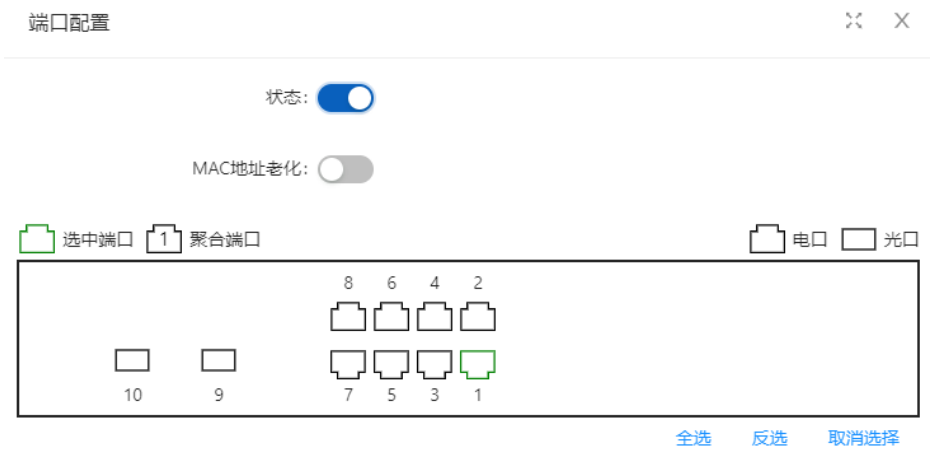


表 3-25 MAC 概况参数说明

配置项		说明
端口配置	状态	开启/关闭此功能
	MAC 地址老化	是否启用 MAC 老化功能

3.6.5 RADIUS

3.6.5.1 概述

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是实现 AAA（Authentication, Authorization and Accounting，认证、授权和计费）的一种常用的协议。

RADIUS 简介

RADIUS 是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了 RADIUS 的报文格式及其消息传输机制，并规定使用 UDP 作为封装 RADIUS 报文的传输层协议（UDP 端口 1812、1813 分别作为认证、计费端口）。

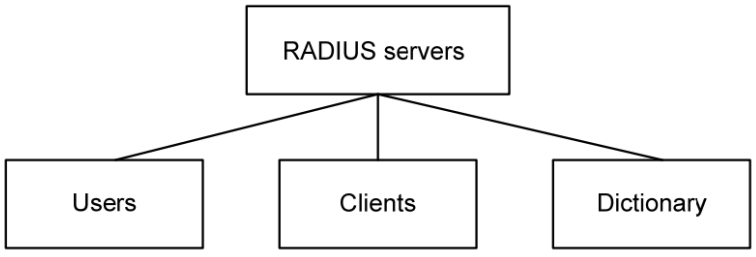
RADIUS 初仅是针对拨号用户的 AAA 协议，后来随着用户接入方式的多样化发展，RADIUS 也适应多种用户接入方式，如以太网接入、ADSL 接入。它通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。

客户端/服务器模式

- 客户端：RADIUS 客户端一般位于 NAS 设备上，可以遍布整个网络，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- 服务器：RADIUS 服务器一般运行在中心计算机或工作站上，维护相关的用户认证和网络服务访问信息，负责接收用户连接请求并认证用户，然后给客户端返回所有需要的信息（如接受/拒绝认证请求）。

RADIUS 服务器通常要维护三个数据库，如图 3-91 所示。

图 3-91 RADIUS 服务器的组成创建成功的 MAC 认证端口



- “Users”：用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置信息）。
- “Clients”：用于存储 RADIUS 客户端的信息（如接入设备的共享密钥、IP 地址等）。
- “Dictionary”：用于存储 RADIUS 协议中的属性和属性值含义的信息。

安全和认证机制

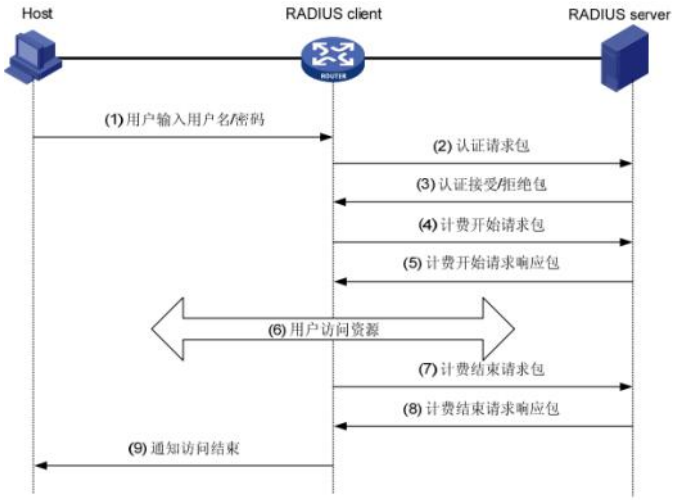
RADIUS 客户端和 RADIUS 服务器之间认证消息的交互是通过共享密钥的参与来完成的，并且共享密钥不能通过网络来传输，增强了信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在传输过程中对密码进行了加密。

RADIUS 服务器支持多种方法来认证用户，如基于 PPP 的 PAP、CHAP 认证。另外，RADIUS 服务器还可以作为一个代理，以 RADIUS 客户端的身份与其它的 RADIUS 认证服务器进行通信，负责转发 RADIUS 认证和计费报文。

RADIUS 的基本消息交互流程

用户、RADIUS 客户端和 RADIUS 服务器之间的交互流程如图 3-92 所示。

图 3-92 RADIUS 的基本消息交互流程



消息交互流程如下：

(1) 用户发起连接请求，向 RADIUS 客户端发送用户名和密码。

(2) RADIUS 客户端根据获取的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），其中的密码在共享密钥的参与下由 MD5 算法进行加密处理。

(3) RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 RADIUS 客户端发送认证接受包（Access-Accept）；如果认证失败，则返回认证拒绝包（Access-Reject）。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受包中也包含了用户的授权信息。

(4) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request）。

(5) RADIUS 服务器返回计费开始响应包（Accounting-Response），并开始计费。

(6) 用户开始访问网络资源；

(7) 用户请求断开连接，RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）。

(8) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费。

用户结束访问网络资源。

说明

我司设备不支持 RADIUS 计费功能

3.6.5.2 配置 RADIUS

RADIUS 全局配置

在导航栏中选择【配置】→【安全】→【RADIUS】，进入 RADIUS 全局配置界面，如图 3-93 所示。全局配置各参数说明如表格 3-26 所示。

图 3-93 RADIUS 全局配置界面

表 3-26 RADIUS 全局配置参数说明

配置项		说明
全局配置	密码	全局默认密码配置；可配置，不可读；可选配置
	超时	全局服务器超时时间；可选配置
	重传	全局服务器重传次数；可选配置
	死亡时间	服务器死亡持续时间；可选配置；默认 0，表示服务器死亡后立即复活

RADIUS 服务器配置

在当前界面，点击“服务器配置”下方的【添加】按钮，进入服务器配置界面，如图 3-94 所示。服务器各参数说明如表格 3-27 所示。

图 3-94 RADIUS 服务器配置界面

表 3-27 MAC 概况参数说明

配置项	说明
IP	服务器 IP 地址
认证端口	服务器认证端口号；默认 1812
密码	服务器密钥；无配置的时候采用全局配置
超时	服务器超时时间；默认 5s
重传	服务器重传次数，默认 3 次

3.7 控制

3.7.1 串口服务器

3.7.1.1 概述

串口服务器：serial device servers。

串口服务器作用于将串口设备接入到以太网中。串口服务器支持网络数据与串口数据的双向转换、传输。

tcp-client 工作模式

TCP Client 为 TCP 网络服务提供客户端连接。主动发起连接并连接服务器，用于实现串口数据和服务器数据的交互；网络与串口数据双向透传；串口服务器支持建立多个 TCP Client 与多个 Tcp Server 连接。

tcp-server 工作模式

TCP Server 即 TCP 服务器。在 TCP Server 模式下，模块监听本机端口，有连接请求发来时接 受并建立连接进行数据通信，当模块串口收到数据后会同时将数据发送给所有与模块建立 连接的客户端设备；通常用于局域网内与 TCP 客户端的通信。适合于局域网内没有服务器并且有多台电脑或是手机向模块请求数据的场景。

3.7.1.2 配置串口服务器

在导航栏中选择【配置】→【控制】→【串口服务器】，进入串口服务器配置界面，如图 3-95 所示。

图 3-95 串口服务器配置界面

点击串口 ID 的【编辑】按钮，进入详细配置界面，如图 3-96 所示，配置参数如表 3-28 所示。

表 3-28 串口服务器参数说明

配置项		说明
基础	ID	串口服务器端口号
模式	None	关闭串口服务器
	tcp-client	配置工作模式为 tcp-client
	tcp-server	配置工作模式为 tcp-server
串口	波特率	配置串口的波特率，有 9600、19200、38400、57600、115200 五种可选
	数据位	配置串口的数据位，有 7、8 两种可选
	校验	配置校验方式，有 none、even、odd、mark、space 五种可选
	停止位	配置停止位，有 1、2 两种可选
通信	缓冲区大小	串口数据位低速传输，数据从网络端转串口端增加 fifo ，提高转发能力，范围<0-128>，默认 64
	最大报文长度	串口数据报文长度，超出 LENGTH 值则分包转发到网络端，范围<0-1460>，默认 1460
	间隔	串口数据前后字节间隔时间超出 MILLISECONDS，则后字节数据认定为新报文头字节范围<1-1000>，默认 10ms
	保活检测时间	配置串口服务器保活时间，在该时间段内无数据交互，则启动 alive 检测
客户端	远端 IP	配置远端连接 IP 地址
	远端端口	配置远端连接的端口号，范围<1-65535>
	本地端口	为可选配置，默认系统自动分配
服务器	端口	配置 tcp-server 的端口号，范围<1-65535>
	最大连接数	tcp-server 模式下最大连接数，范围<1-65535>

图 3-96 串口服务器配置界面

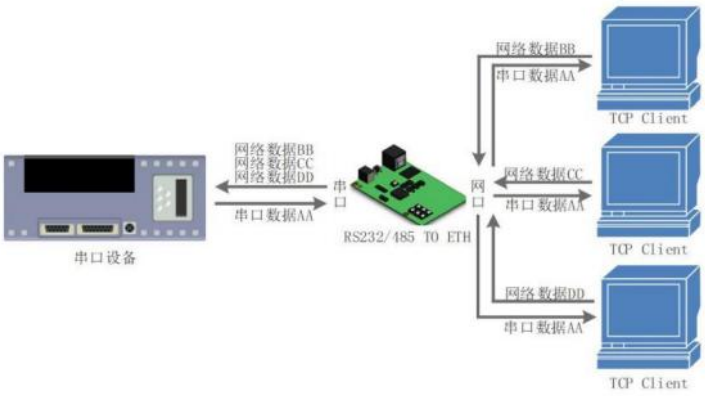
3.7.1.3 配置举例

案例需求 1：

如图 3-97 所示，配置串口服务器工作在 tcp-server 模式；配置本地端口号 2000；配置最大连接数为 3。TCP Client0/1/2 接入到 server。

串口参数 baud-rate 115200；data-bits 8；parity none；stop-bits 1，均为默认值。

图 3-97 串口服务器配置界面



配置步骤：

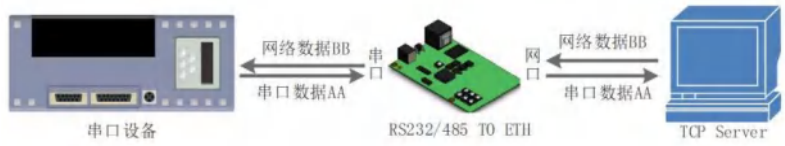
（1）在导航栏中选择【配置】→【控制】→【串口服务器】，进入串口服务器配置界面。

（2）点击串口 ID 的【编辑】按钮，进入详细配置界面，配置参数如图 3-98 所示，点击【确认】按钮完成配置。

图 3-98 串口服务器配置界面

案例需求 2：

图 3-99 串口服务器配置界面



TCP Server 的 IP 地址 192.168.56.2，端口号 2000。

配置串口服务器工作在 tcp-client 模式；配置 tcp-client 1 连接目标 TCP Server，本地端口由系统动态生成。

串口参数 baud-rate 115200；data-bits 8；parity none；stop-bits 1，均为默认值。

配置步骤：

（1）在导航栏中选择【配置】→【控制】→【串口服务器】，进入串口服务器配置界面。

（2）点击串口 ID 的【编辑】按钮，进入详细配置界面，配置参数如图 3-100 所示，点击【确认】按钮完成配置。

图 3-100 串口服务器配置界面

3.7.2 IO 控制

IO 控制模块分为 DI，DO 两部分，目前 DO 仅支持简单的手动控制继电器（DO）的 ON/OFF 切换功能，如图 3-101 所示，DI 仅支持输入电平的高低判断，如图 3-102 所示。

图 3-101 DI 配置界面

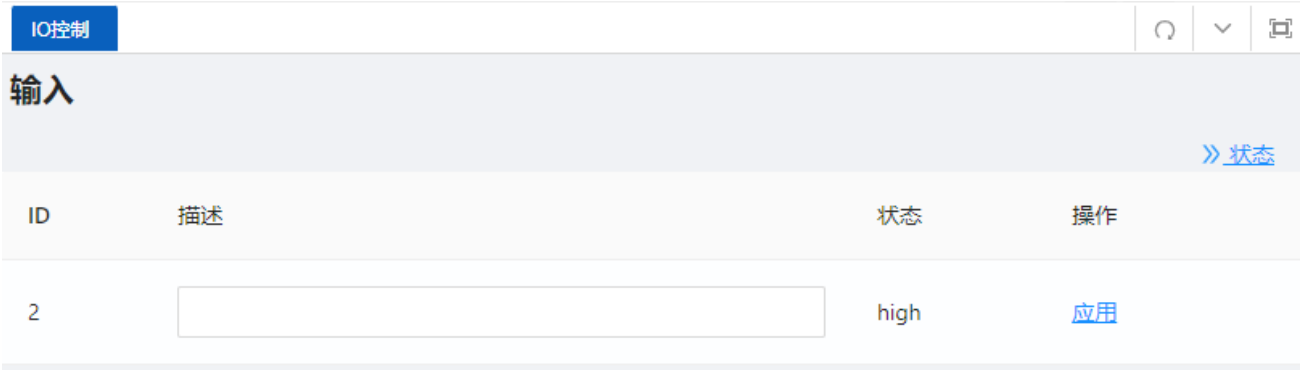
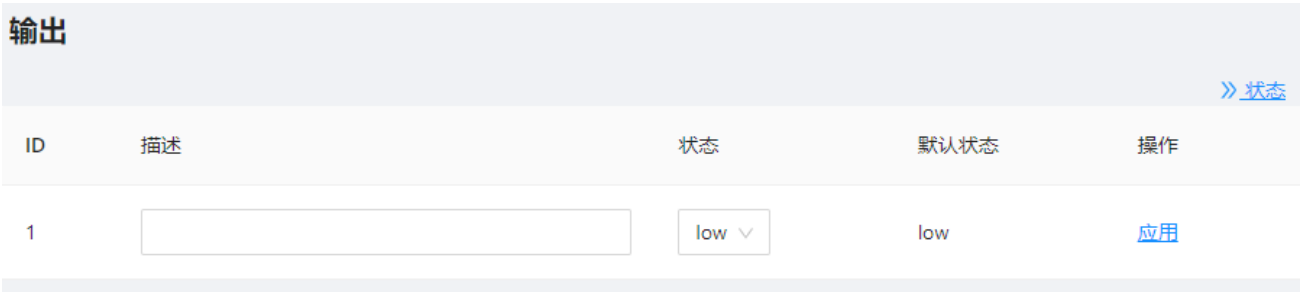


图 3-102 DO 配置界面



3.8 环路检测

3.8.1 概述

LOOP-DETECT 是一种以太网环路检测协议，用于快速检测下联接口环路故障。如果发现故障存在，LOOP-DETECT 会根据用户配置的故障处理方式，通知用户手工关闭或自动关闭相关端口，以避免因环路影响正常数据交互。

使能控制：使能控制分全局使能控制与接口使能控制，当全局使能，且接口上开启环路检测时，该接口支持环路检测功能。

违例处理：当接口上检测到环路故障，默认通过 log 通告用户手工处理环路故障，也可配置自动关闭端口方式。当采用自动关闭端口方式，且端口触发违例事件时，可通过等待违例超时、shutdown/no shutdown 端口、违例恢复命令或重启设备等方式实现端口从违例中恢复。

指定 vlan：默认情况下，当链路存在环路数据通路，忽略端口 vlan 属性，则认为单口环路；若需检测具体某 vlan 域内是否发生环路故障，可在端口上配置指定 vlan，仅检测该 vlan 域内是否存在环路数据通路。

设备支持环路故障告警与环路故障恢复消息 trap 到 snmp 服务器，默认关闭，支持全局开启。

3.8.2 配置环路检测

配置步骤：

（1）在导航栏中选择【配置】→【环路检测】，进入环路检测界面。此页面包含“全局配置”和“端口配置”两部分。

（2）在全局配置打开环路检测开关，配置探测间隔，开启 Trap 开关（可选），点击【应用】按钮完成配置，如图 3-103 所示，参数说明如表格 3-29 所示。

图 3-103 环路检测全局配置界面

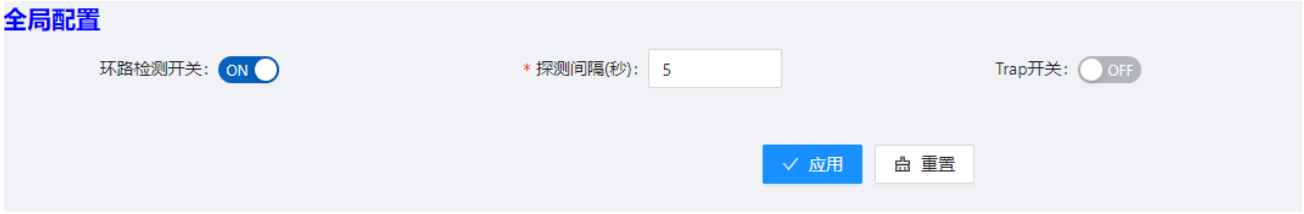


表 3-29 环路检测全局配置参数说明

配置项	说明
环路检测开关	开启/关闭环路检测功能，默认为全局关闭，端口关闭
探测间隔	配置环路探测时间间隔，范围 5-300 秒，默认 5 秒
Trap 开关	开启/关闭环路故障 Trap 告警

（2）点击“端口配置”下方的【批量配置】按钮或者需要配置的端口后的【编辑】按钮，进入环路检测端口配置界面，分别配置管理状态，违例处理方式，VLAN 域检测，选择需要开启此功能的端口，如图 3-104 所示，参数说明如表格 3-30 所示。

图 3-104 环路检测端口配置界面

表 3-30 环路检测端口参数说明

配置项	说明
管理状态	Enable：开启端口的环路检测功能 Disabled：关闭端口的环路检测功能
违例处理方式	Alarm：环路发生时，Trap 告警 Error-down：环路发生时，把环路端口 shudown
VLAN 域检测	在指定 vlan 域内检测是否发生数据通路环路

4 高级

4.1 LLDP

4.1.1 概述

4.1.1.1 LLDP 产生的背景

目前，网络设备的种类日益繁多且各自的配置错综复杂，为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息，需要有一个标准的信息交流平台。

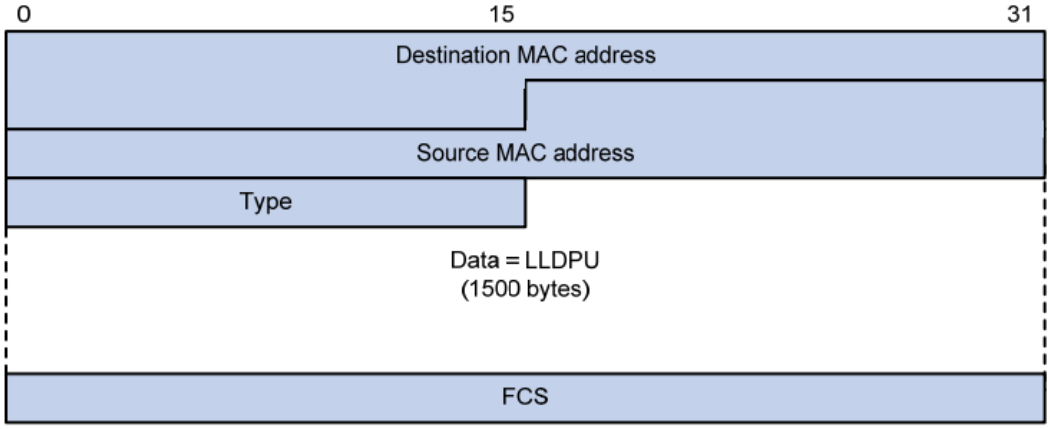
LLDP（Link Layer Discovery Protocol，链路层发现协议）就是在这样的背景下产生的，它提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

4.1.1.2 LLDP 基本概念

1. LLDP 报文

封装有 LLDPDU 的报文称为 LLDP 报文，其封装格式有两种：Ethernet II 和 SNAP（Subnetwork Access Protocol，子网访问协议）。

图 4-1 Ethernet II 格式封装的 LLDP 报文



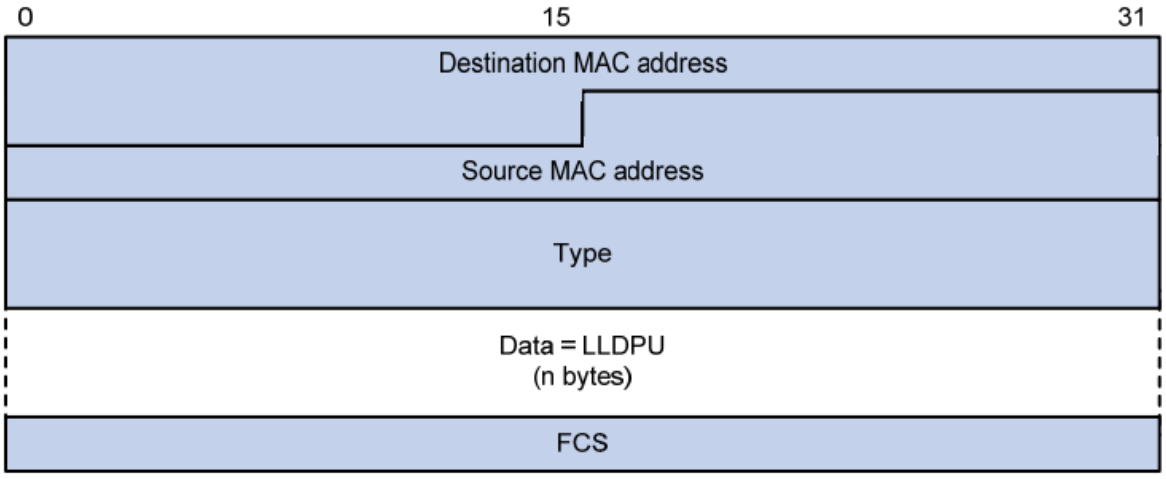
(1) Ethernet II 格式封装的 LLDP 报文

如图 4-1 所示，是以 Ethernet II 格式封装的 LLDP 报文，其中各字段的含义如下：

- Destination MAC address：目的 MAC 地址，为固定的组播 MAC 地址 0x0180-C200-000E。
- Source MAC address：源 MAC 地址，为端口 MAC 地址。
- Type：报文类型，为 0x88CC。
- Data：数据内容，为 LLDPDU。
- FCS：帧检验序列，用来对报文进行校验。

(2) SNAP 格式封装的 LLDP 报文

图 4-2 SNAP 格式封装的 LLDP 报文



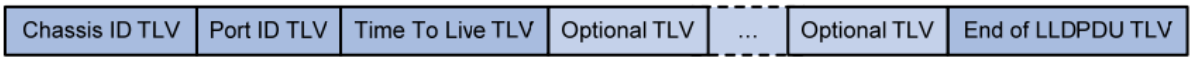
如图 4-2 所示，是以 SNAP 格式封装的 LLDP 报文，其中各字段的含义如下：

- Destination MAC address：目的 MAC 地址，为固定的组播 MAC 地址 0x0180-C200-000E。
- Source MAC address：源 MAC 地址，为端口 MAC 地址或设备桥 MAC 地址（如果有端口地址则使用端口 MAC 地址，否则使用设备桥 MAC 地址）。
- Type：报文类型，为 0xAAAA-0300-0000-88CC。
- Data：数据内容，为 LLDPDU。
- FCS：帧检验序列，用来对报文进行校验。

2. LLDPDU

LLDPDU 就是封装在 LLDP 报文数据部分的数据单元。在组成 LLDPDU 之前，设备先将本地信息封装成 TLV 格式，再由若干个 TLV 组合成一个 LLDPDU 封装在 LLDP 报文的数据部分进行传送。

图 4-3 LLDPDU 的封装格式



如图 4-3 示，深蓝色的 Chasis ID TLV、Port ID TLV、Time To Live TLV 和 End of LLDPDU TLV 这四种 TLV 是每个 LLDPDU 都必须携带的，其余的 TLV 则为可选携带。每个 LLDPDU 多可携带 28 种 TLV。

3. TLV

TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。LLDP 可以封装的 TLV 包括基本 TLV、802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED（Media Endpoint Discovery，媒体终端发现）TLV。

基本 TLV 是网络设备管理基础的一组 TLV，802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED TLV 则是由标准组织或其他机构定义的 TLV，用于增强对网络设备的管理，可根据实际需要选择是否在 LLDPDU 中发送。

(1) 基本 TLV

在基本 TLV 中，有几种 TLV 对于实现 LLDP 功能来说是必选的，即必须在 LLDPDU 中发布，如表 4-1 所示。

表 4-1 基本 TLV

TLV 名称	说明	是否必须发布
Chassis ID	发送设备的桥 MAC 地址	是
Port ID	标识 LLDPDU 发送端的端口。如果 LLDPDU 中携带有 LLDP-MED TLV，其内容为端口的 MAC 地址，没有端口 MAC 时使用桥 MAC；否则，其内容为端口的名称	是
Time To Live	本设备信息在邻居设备上的存活时间	是
End of LLDPDU	LLDPDU 的结束标识，是 LLDPDU 的 后一个 TLV	是
Port Description	端口的描述	否
System Name	设备的名称	否
System Description	系统的描述	否
System Capabilities	系统的主要功能以及已使能的功能项	否
Management Address	管理地址，以及改地址所对应的接口号和 OID（Object Identifier，对象标识符）	否

(2) 802.1 组织定义 TLV

IEEE 802.1 组织定义 TLV 的内容如表格 4-2 所示。

表 4-2 IEEE 802.1 组织定义的 TLV

TLV 名称	说明
Port VLAN ID	端口的 PVID（Port VLAN ID），一个 LLDPDU 中 多携带一个该类型 TLV
Port And Protocol VLAN ID	端口的 PPVID（Port and Protocol VLAN ID），一个 LLDPDU 中可携带多个互不重复的该类型 TLV
VLAN Name	端口所属 VLAN 的名称，一个 LLDPDU 中可携带多个互不重复的该类型 TLV
Protocol Identity	端口所支持的协议类型，一个 LLDPDU 中可携带多个互不重复的该类型 TLV
DCBX	数据中心桥能力交换协议（Data Center Bridging Exchange Protocol）

(3) 802.3 组织定义 TLV

IEEE 802.3 组织定义 TLV 的内容如表格 4-3 所示。

表 4-3 IEEE 802.3 组织定义的 TLV

TLV 名称	说明
MAC/PHY Configuration/Status	端口支持的速率和双工状态、是否支持端口速率自动协商、是否已使能自动协商功能以及当前的速率和双工状态
Power Via MDI	端口的供电能力，包括 PoE（Power over Ethernet，以太网供电）的类型（PSE （Power Sourcing Equipment，供电设备）或 PD（Powered Device，受电设备））、PoE 端口的远程供电模式、是否支持 PSE 供电、是否已使能 PSE 供电以及供电方式是否可控
Link Aggregation	端口是否支持链路聚合以及是否已使能链路聚合
Maximum Frame Size	端口支持的 大帧长度，取端口配置的 MTU（Maximum Transmission Unit，大传输单元）
Power Stateful Control	端口的电源状态控制，包括 PSE/PD 所采用的电源类型、供/受电的优先级以及供/受电的功率

说明

我司产品暂不支持 PoE 相关部分的 TLV。

(3) LLDP-MED TLV

LLDP-MED TLV 为 VoIP（Voice over IP，在 IP 网络上传送语音）提供了许多高级的应用，包括基本配置、网络策略配置、地址信息以及目录管理等，满足了语音设备的不同生产厂商在成本有效、易部署、易管理等方面的要求，并解决了在以太网中部署语音设备的问题，为语音设备的生产者、销售者以及使用者提供了便利。LLDP-MED TLV 的内容如表格 4-4 所示。

表 4-4 LLDP-MED TLV

TLV 名称	说明
LLDP-MED Capabilities	网络设备所支持的 LLDP-MED TLV 类型
Network Policy	网络设备或终端设备上端口的 VLAN 类型、VLAN ID 以及二三层与具体应用类型、相关的优先级等等
Extended Power-via-MDI	网络设备或终端设备的扩展供电能力，对 Power Via MDI TLV 进行了扩展
Hardware Revision	终端设备的硬件版本
Firmware Revision	终端设备的固件版本

Software Revision	终端设备的软件版本
Serial Number	终端设备的序列号
Manufacturer Name	终端设备的制造厂商名称
Model Name	终端设备的模块名称
Asset ID	终端设备的资产标识符，以便目录管理和资产跟踪
Location Identification	网络设备的位置标识信息，以供终端设备在基于位置的应用中使用

说明

我司产品暂不支持 VoIP 相关部分的 TLV。

(4) 管理地址

管理地址是供网络管理系统标识网络设备并进行管理的地址。管理地址可以明确地标识一台设备，从而有利于网络拓扑的绘制，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 中向外发布。

4.1.1.3 LLDP 工作机制

1. LLDP 的工作模式

LLDP 有以下四种工作模式：

- TxRx：既发送也接收 LLDP 报文。
- Tx：只发送不接收 LLDP 报文。
- Rx：只接收不发送 LLDP 报文。
- Disable：既不发送也不接收 LLDP 报文。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

2. LLDP 报文的发送机制

当端口工作在 TxRx 或 Tx 模式时，设备会周期性地向邻居设备发送 LLDP 报文。如果设备的本地配置发生变化则立即发送 LLDP 报文，以将本地信息的变化情况尽快通知给邻居设备。但为了防止本地信息的频繁变化而引起 LLDP 报文的大量发送，每发送一个 LLDP 报文后都需延迟一段时间后再继续发送下一个报文。

当设备的工作模式由 Disable/Rx 切换为 TxRx/Tx，或者发现了新的邻居设备（即收到一个新的 LLDP 报文且本地尚未保存发送该报文设备的信息）时，该设备将自动启用快速发送机制，即将 LLDP 报文的发送周期缩短为 1 秒，并连续发送指定数量的 LLDP 报文后再恢复为正常的发送周期。

3. LLDP 报文的接收机制

当端口工作在 TxRx 或 Rx 模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 Time To Live TLV 中 TTL（Time to Live，生存时间）的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

4.1.2 配置 LLDP

4.1.2.1 LLDP 配置任务简介

步骤	配置任务	说明
1	配置全局 LLDP 功能	设置使能全局的 LLDP 功能，并配置 LLDP 的全局参数 全局 LLDP 功能默认处于关闭状态，必选
2	配置端口 LLDP 参数	配置端口 LLDP 功能相关参数，包括：LLDP 管理状态、Chassis Subtype、Port ID Subtype、Management Address Subtype 和允许发布的 TLV 类型，可选
3	查看端口信息	查看指定端口的 LLDP 本地信息、邻居信息、统计信息和状态信息，可选
4	查看统计	查看全局的 LLDP 本地信息和统计信息，可选
5	查看邻居信息	查看全局的 LLDP 邻居信息，即从邻居收到的 LLDP 信息，邻居将这些信息组织成 TLV 发送给当前设备，可选

4.1.2.2 配置全局 LLDP 功能

在导航栏中选择【高级】→【二层】→【LLDP 配置】，进入 LLDP 配置界面，如图 4-4 所示，详细参数如表格 4-5。

图 4-4 LLDP 全局配置

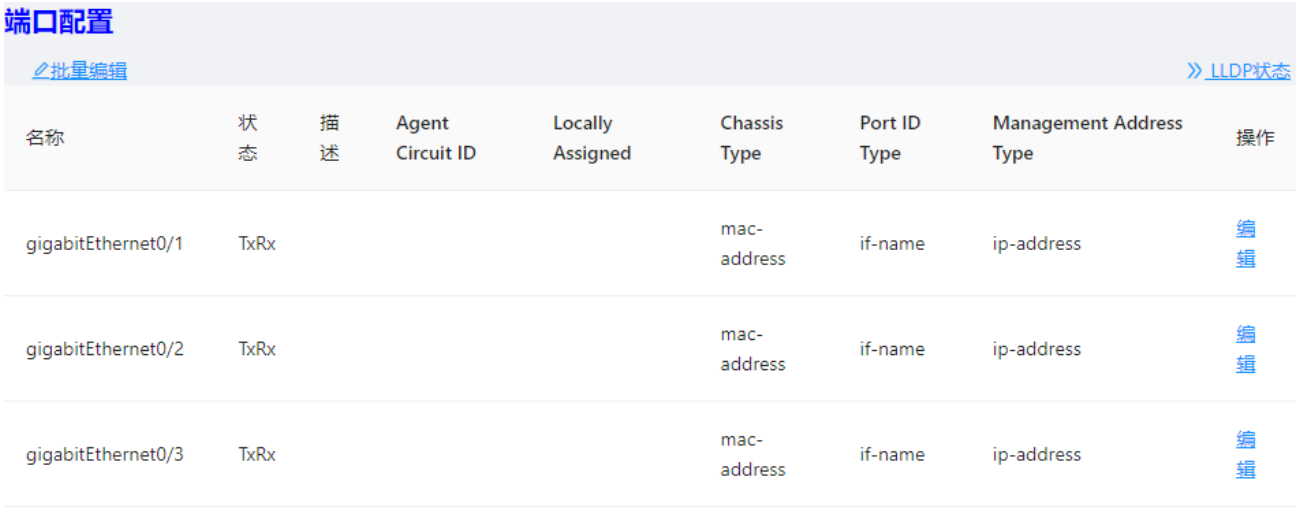
表 4-5 LLDP 全局配置参数说明

配置项	说明
状态	Disabled:全局使能关闭 Enabled:全局使能
系统名	设备的名称，可以为空
系统描述	系统的描述，可以为空

4.1.2.3 配置端口 LLDP 参数

步骤 1：在当前界面，点击右上角的“端口”页签，进入 LLDP 端口配置概览界面，如图 4-5 所示。

图 4-5 LLDP 端口配置概览



步骤 2：选择需要配置的端口，点击【编辑】按钮，进入端口详细配置界面，如图 4-6 所示，端口配置详细参数如表格 4-6 所示。

图 4-6 LLDP 端口详细配置界面

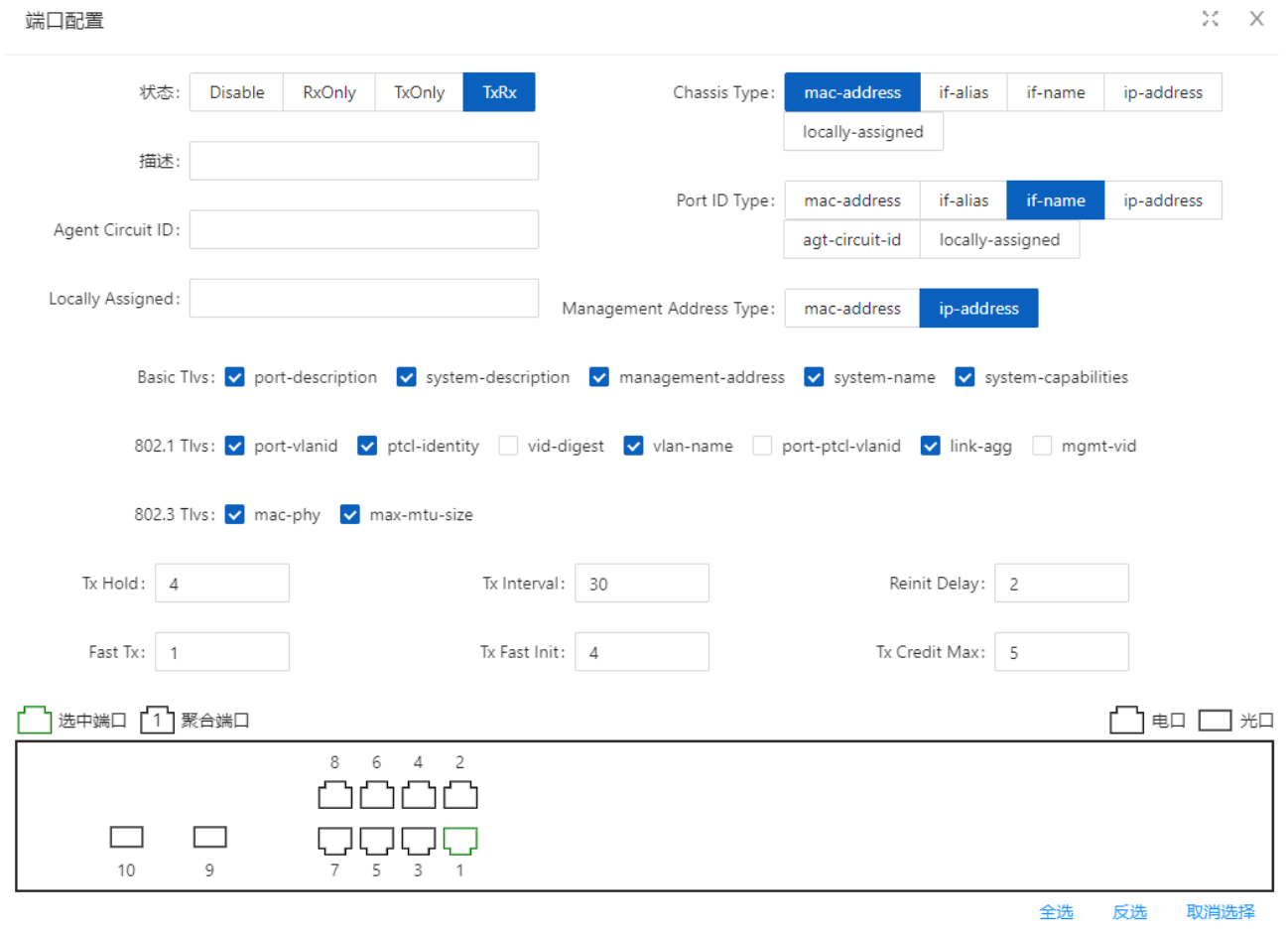


表 4-6 LLDP 端口配置参数说明

配置项	说明
状态	Disabled：既不发送也不接收 LLDPDU TxOnly: 只发送不接收 LLDPDU RxOnly: 只接收不发送 LLDPDU TxRx: 既发送也接收 LLDPDU
Chassis Subtype	Mac-address:表示 MAC 地址 If-alias:表示接口化名 If-name:表示接口名称 Ip-address:表示 IP 地址 Locally-assigned:表示本地配置
描述	显示当前配置的 LLDP 端口的名称
Agent Circuit ID	代理巡回标识
Locally Assigned	本地配置
Port ID Subtype	Mac-address: 表示 MAC 地址 If-alias: 表示接口化名 If-name: 表示接口名称 Ip-address: 表示 IP 地址 Agt-circuit-id: 表示代理巡回标识 Locally-assigned: 表示本地配置
Management Address Subtype	Mac-address:设备 MAC 地址 Ip-address:设备 IP 地址
Basic Tlvs	port-description:端口描述符 system-description:系统描述符 management-address:管理地址 system-name:系统名 system-capabilities:系统能力
802.1 Tlvs	port-vlanid:端口 vlanid ptcl-identity:协议 id vid-digest:vid 摘要 vlan-name:vlan 名称 port-ptcl-vlanid:端口协议 vlanid link-agg mgmt-vid:链路聚合管理 vid
802.3 Tlvs	mac-phy:mac-phy max-mtu-size:最大 mtu 值
Tx hold	传输保持，默认值 txFastInit 为 4，用于报文 TTL 计算；TTL=msgTxInterval * msgTxHold + 1
Tx interval	传输间隔，默认值为 30 s； 管理员可以将此值更改为 5 到 3600 之间的任何值。
Reinit delay	表示从 adminStatus 变为“禁用”到尝试重新初始化之间的延迟量。 reinitDelay 的默认值为 2 s。

Fast tx	定义了在快速传输周期内两次传输之间的计时器间隔的时间间隔(即 txFast 不为零)。msgFastTx 的默认值是 1; 管理员可以将此值更改为 1 到 3600 之间的任何值。
Tx fast init	该变量用作 txFast 变量的初始值。 该值确定在快速传输周期内传输的 LLDPDU 的数量。
Tx credit max	配置 txCredit 的最大值。默认值为 5。 管理员可以将此值更改为 1 到 10 范围内的任何值。

4.1.2.4 查看统计

在当前界面，点击右侧的【LLDP 状态】按钮，进入 LLDP 状态界面，如图 4-7 所示，具体参数描述如表格 4-7 所描述。

图 4-7 LLDP 统计信息

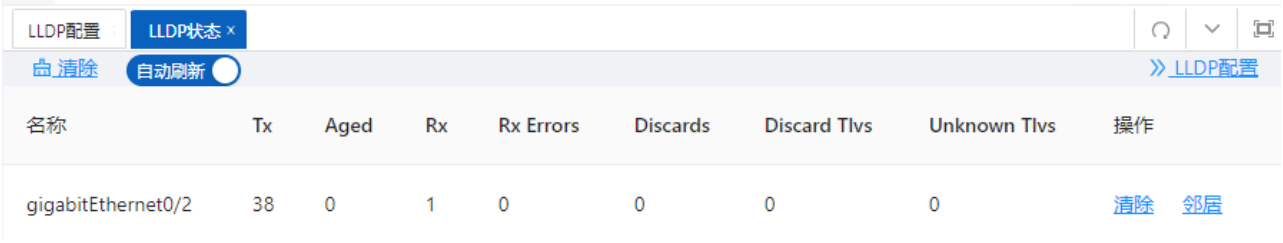


表 4-7 LLDP 端口配置参数说明

配置项	说明
名称	显示接口名称
Tx	发送报文数
Aged	老化报文数
Rx	接收报文数
Rx Errors	接收错误数
Discards	丢弃报文数
Ddiscard Tlvs	丢弃 Tlv 数
Unknown Tlvs	不知名 Tlv 数
清除	清除当前计数

4.1.2.5 查看邻居信息

在“端口”页签，点击对应端口的“邻居”按钮，进入邻居信息查看界面，如图 4-8 所示。

图 4-8 LLDP 邻居信息

gigabitEthernet0/2 ×

```
Neighbor            : 00-0E-C6-C1-38-8E
    System Name         :
    System Description  :
    Port Description    :
    TTL                 : 3601
    System Capabilities : Routing
    Mandatory TLVs :
      CHASSIS ID TYPE :
       Chassis MAC Address: 000e.c6c1.388e
      PORT ID TYPE :
       Port MAC Address: 000e.c6c1.388e
    8021 ORIGIN SPECIFIC TLV
     Port Vlan id  :0
     PP Vlan id    :0
     Remote Protocols Advertised  :
     Remote VID Usage Digest  : 0
     Remote Management Vlan   : 0
     Link Aggregation Status  : Disabled
     Link Aggregation Port ID : 0
    8023 ORIGIN SPECIFIC TLV
     AutoNego Support     :  Supported Enabled
     AutoNego Capability  : 1
     Operational MAU Type : 0
     Max Frame Size       : 0
     MED Capabilities  :  Capabilities
     MED Capabilities Dev Type : End Point Class-1
     MED Application Type : Reserved
     MED Vlan id : 0
     MED Tag/Untag: Untagged
     MED L2 Priority : 0
     MED DSCP Val : 0
```

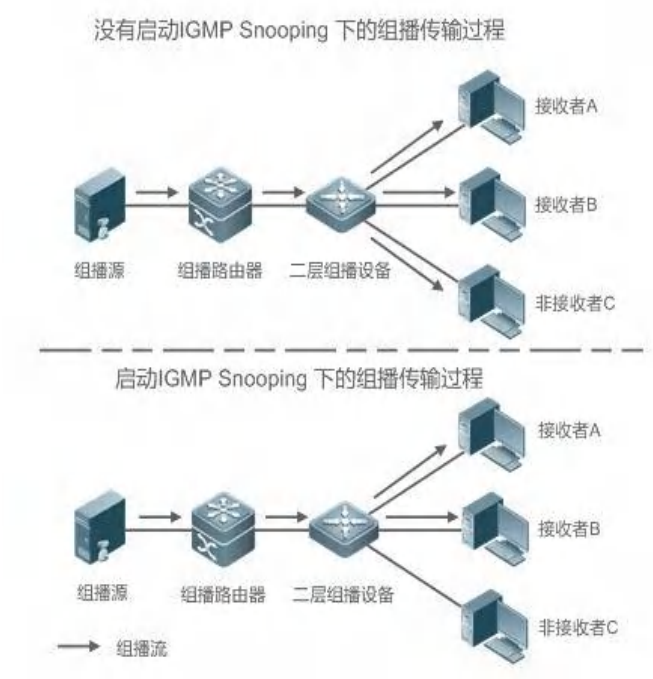
4.2 IGMP Snooping

4.2.1 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。

图 4-9 IGMP Snooping 工作原理



如图 4-9 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。

4.2.2 IGMP Snooping 配置

4.2.2.1 IGMP 全局配置说明

(1) 在导航栏中选择【高级】→【二层】→【IGMP Snooping 配置】，进入 IGMP Snooping 界面。

(2) 在当前界面，点击“状态”按钮，全局使能 IGMP Snooping 功能，如图 4-10 所示。

(3) 单击丢弃未知名组播“已禁用”按钮，使能丢弃未知名组播功能，此功能为可选。

(4) 单击拓扑变化抑制“已禁用”按钮，使能拓扑变化抑制功能，此功能为可选。

图 4-10 IGMP 全局配置界面

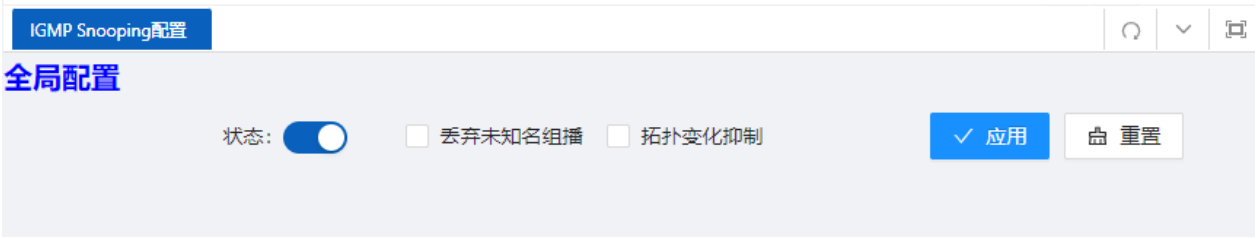


表 4-8 全局配置参数说明

配置项		说明
IGMP Snooping	状态	开启/关闭 IGMP Snooping 功能，默认为关闭。
	丢弃未知名组播	开启/关闭丢弃未知名组播功能 未知组播数据报文是指在 IGMP Snooping 转发表中不存在对应转发表项的那些组播数据报文： • 当使能丢弃未知组播数据报文功能时，交换机将丢弃所有收到的未知组

		播数据报文 • 当禁止丢弃未知组播数据报文功能时，交换机将在未知组播数据报文所属的 VLAN 内广播该报文
	拓扑变化抑制	开启/关闭拓扑变化抑制功能

4.2.2.2 IGMP 路由口配置说明

(1) 在导航栏中选择【高级】→【二层】→【IGMP Snooping 配置】，进入 IGMP 路由口页面，如图 4-11 所示。

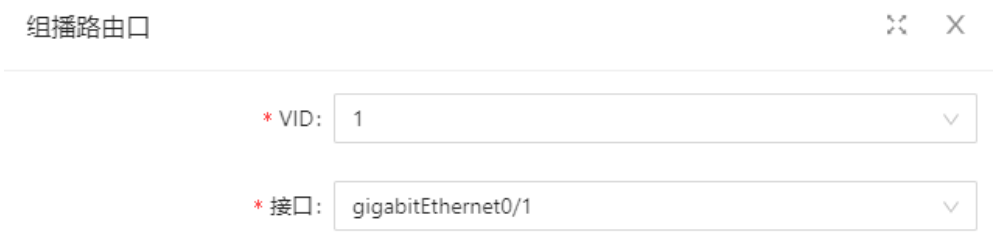
图 4-11 IGMP 路由口界面

表 4-9 IGMP 路由口参数说明

配置项		说明
IGMP 路由口	VID	组播表项所属 VLAN 的 ID
	接口	所有成员端口
	删除	删除该 IGMP 路由

(2) 单击“组播路由口”下方的【添加】按钮，进入 IGMP 路由口设置界面，如图 4-12 所示，配置 VID，选择需要应用的端口。点击【确认】按钮完成配置。

图 4-12 IGMP 路由口配置界面



4.2.2.3 IGMP 静态组配置说明

(1) 在导航栏中选择【高级】→【二层】→【IGMP Snooping 配置】，进入 IGMP 静态组显示页面，如图 4-13 所示，参数说明如表 4-10 所示。

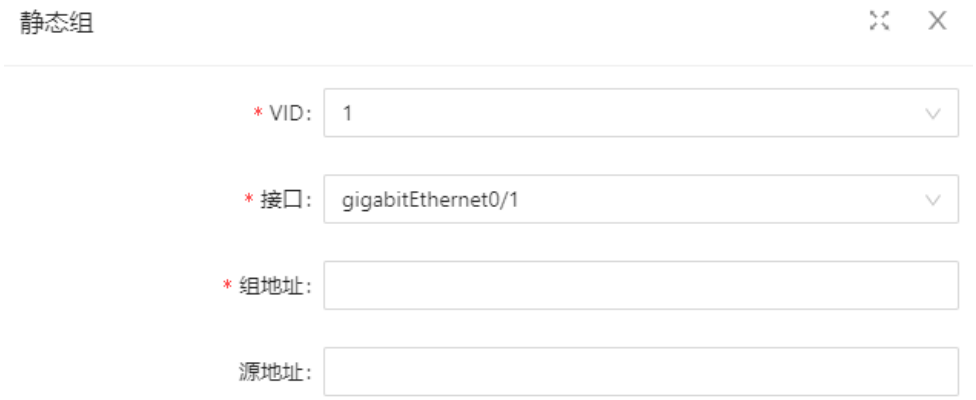
图 4-13 IGMP 静态组显示界面

表 4-10 IGMP 静态组参数说明

配置项		说明
IGMP 静态组	VID	组播表项所属 VLAN 的 ID
	组地址	组播组地址
	源地址	组播源地址
	接口	所有成员端口
	删除	删除该 IGMP 静态组

(2) 单击“静态组”下方的【添加】按钮，进入 IGMP 静态组配置界面，如图 4-14 所示。依次配置 VID、组地址、源地址以及接口名称。点击【确认】按钮完成配置。

图 4-14 IGMP 静态组配置界面



4.3 MAC 管理

4.3.1 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。

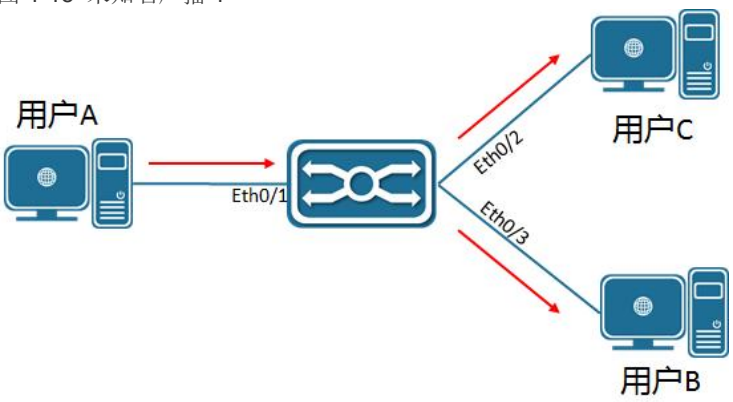
知名单播：以太网交换机在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。

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。

如图 4-15 所示，用户 A 发送报文到交换机的端口 GigabitEthernet 0/1，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 GigabitEthernet 0/1 以外的同属 VLAN 1 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 4-15 未知名广播 1



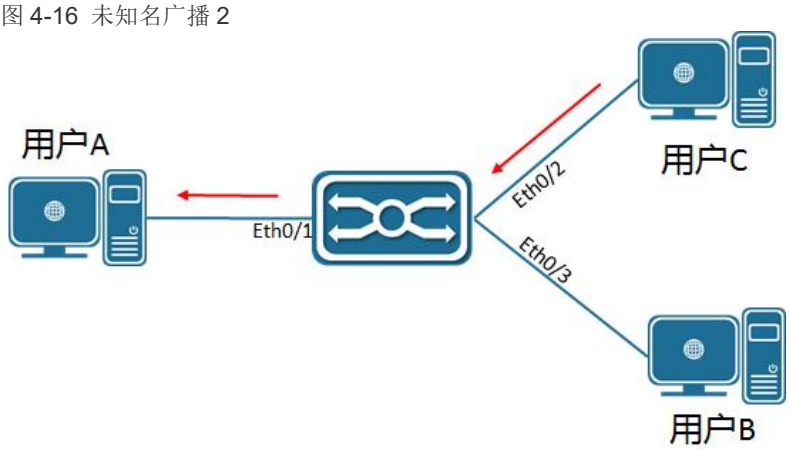
当前动态 MAC 地址表信息如表 4-11 所示：

表 4-11 设备参数列表

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	GigabitEthernet 0/1

如图 4-16 所示，用户 B 收到报文后将回应报文通过以太网交换机的端口 GigabitEthernet 0/2，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 GigabitEthernet 0/1 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 4-16 未知名广播 2



当前动态 MAC 地址表信息如表 4-12 所示：

表 4-12 设备参数列表

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	Gigabit Ethernet 0/1
用户 C	1	000E.C6C1.C8AD	Gigabit Ethernet 0/2

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。

4.3.2 配置 MAC 地址

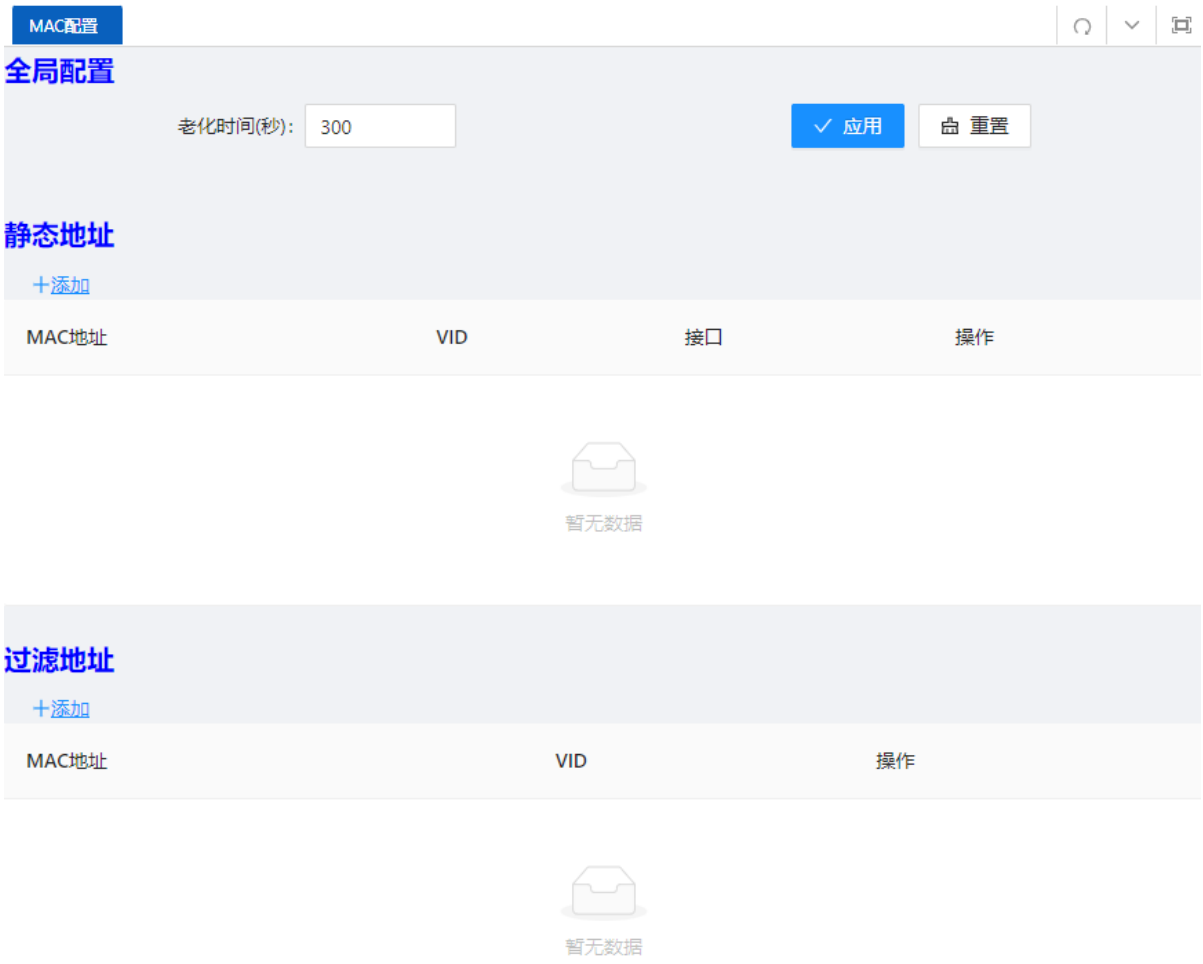
MAC 地址表项分为：静态 MAC 地址表项、动态 MAC 地址表项和过滤 MAC 地址表项。

静态 MAC 地址表项：由用户手工配置，表项不老化。

动态 MAC 地址表项：包括用户配置的以及设备通过源 MAC 地址学习得来的，表项有老化时间。

过滤 MAC 地址表项：用于丢弃含有特定 MAC 地址的报文（例如，出于安全考虑，可以屏蔽某个用户接收报文），由用户手工配置，表项不老化。

图 4-17 MAC 配置界面



在导航栏中选择【高级】→【二层】→【MAC 配置】，进入 MAC 配置界面，如图 4-17 所示，MAC 配置各参数如表 4-13 所示。

表 4-13 MAC 地址管理参数说明

配置项		说明
全局配置	老化时间	<30,1000>，默认老化时间是 300 秒，MAC 地址在最后一次更新 300 到 600 秒时间范围内被系统老化
	应用	点击配置生效
静态地址	MAC 地址	配置的静态 MAC 地址，格式如：00-00-00-00-00-01
	VID	MAC 地址的 vlan 属性
	接口	MAC 地址的端口属性
	操作	点击删除该静态 MAC 地址
过滤地址	MAC 地址	配置过滤 MAC 地址，格式如：00-00-00-00-00-01
	VID	MAC 地址的 vlan 属性
	操作	点击删除该过滤 MAC 地址

4.5.3 MAC 地址配置举例

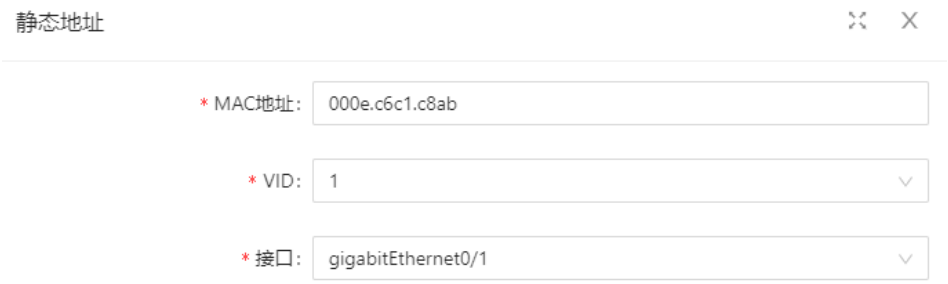
配置范例：

案例需求：所有目的 MAC 地址 000E.C6C1.C8AB，VLAN 1 的报文从端口 GigabitEthernet 0/1 转发，同时过滤 MAC 地址 000E.C6C1.C8CC，VLAN 10 的报文

步骤 1：创建静态 MAC 地址，MAC：000E.C6C1.C8AB，VLAN 1，端口 GigabitEthernet 0/1。

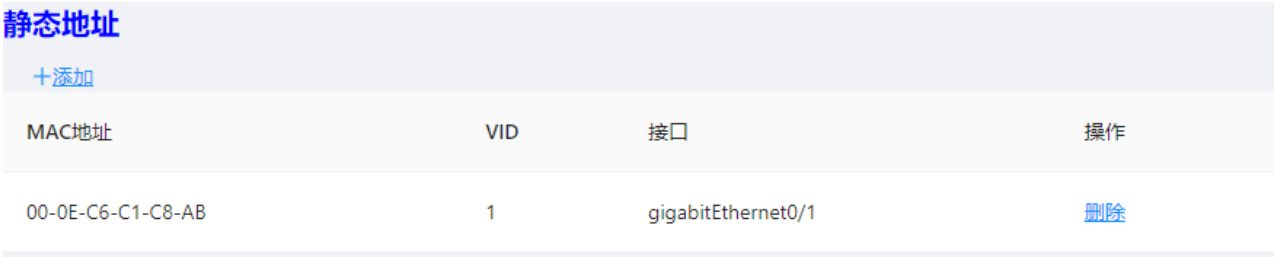
在导航栏中选择【高级】→【二层】→【MAC 配置】，进入 MAC 地址配置界面，点击“静态地址”下方的【添加】按钮，进入静态地址添加界面，如图 4-18 所示，依次配置 MAC 地址，VID 和接口。

图 4-18 静态地址配置



点击【确认】按钮完成配置，返回界面如图 4-19 所示。

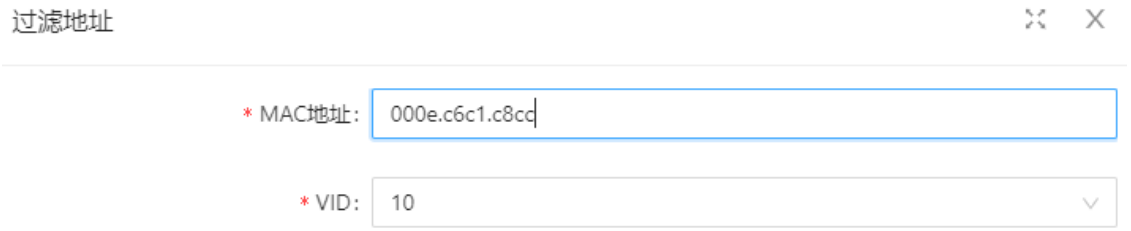
图 4-19 静态地址显示



步骤 2：创建过滤 MAC 地址，MAC：000E.C6C1.C8CC,VLAN10

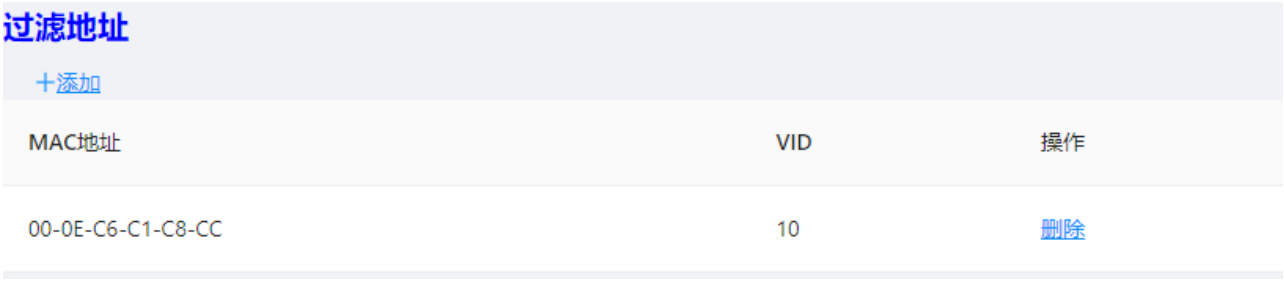
在导航栏中选择【高级】→【二层】→【MAC 配置】，进入 MAC 地址配置界面，点击“过滤地址”下方的【添加】按钮，进入过滤地址添加界面，如图 4-20 所示，依次配置 MAC 地址，VID。

图 4-20 过滤地址添加界面



点击【确认】按钮完成配置，返回界面如图 4-21 所示。

图 4-21 静态地址显示



步骤 3：点击辅助区 的【保存】按钮，保存配置。

4.4 DHCP Snooping

4.4.1 概述

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议， 被广泛用来动态分配可重用的网络资源，是一种用户或者内部网络管理员对所有计算机作中央管理的手段。

DHCP Snooping 是 DHCP 安全技术，通过侦测管理 DHCP 交互报文，实现对非法 DHCP Server 的隔离功能，DHCP 隔离功能可基于 VLAN 生效。

DHCP TRUST 端口

对于连接合法 DHCP Server 的端口，认定为 TRUST 端口，其他端口为 UNTRUST 端口。当开启 DHCP Snooping 功能时，设备将阻止客户端的 DHCP 广播报文发送往 UNTRUST 端口。

DHCP 报文端口限速

针对端口部分用户的 DHCP 报文流量攻击，支持 DHCP 报文端口限速，降低或消除该端口下用户攻击对网络环境影响。

MAC Address 检验

UNTRUST 端口送上来的 DHCP 报文,检测报文中二层头部源 MAC 地址与数据段中 CLIENT HARDWARE ADDRESS 字段，不一样则为非法报文。

Option-82 选项

DHCP Option82 选项又称为 DHCP 中继代理信息选项（Relay Agent Information Option），是 DHCP 报文中的一个选项。Option82 选项是为了增强 DHCP 服务器的安全性，改善 IP 地址的分配策略而提出的一种 DHCP 选项，由中继组件实现选项的添加与剥离。

DHCP 合法用户

DHCP Snooping 通过监控 DHCP 报文，统计合法服务器分配的用户信息。当端口开启 ip verify source 功能时，作为端口上的合法用户。

4.4.2 DHCP Snooping 配置

配置步骤：

（1）在导航里选择【高级】→【二层】→【DHCP Snooping 配置】，跳转到 DHCP Snooping 配置界面，如图 4-22 所示，全局配置参数如表 4-14 所示。

图 4-22 DHCP Snooping 全局配置

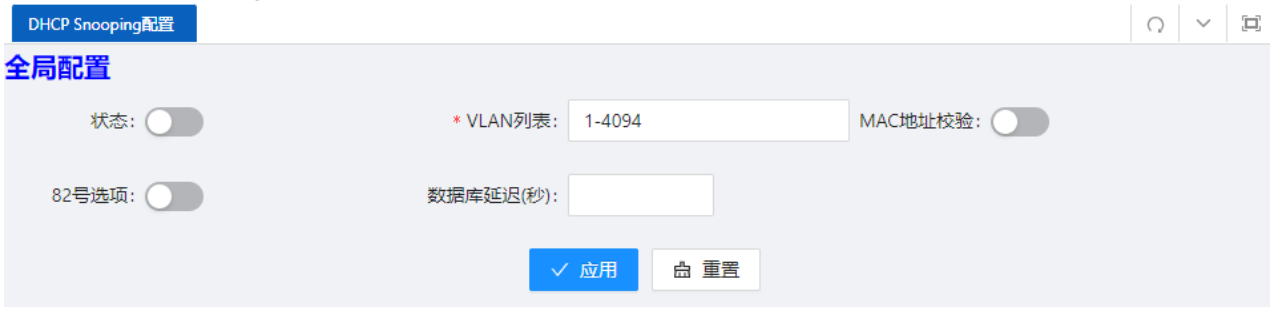


表 4-14 DHCP Snooping 全局配置

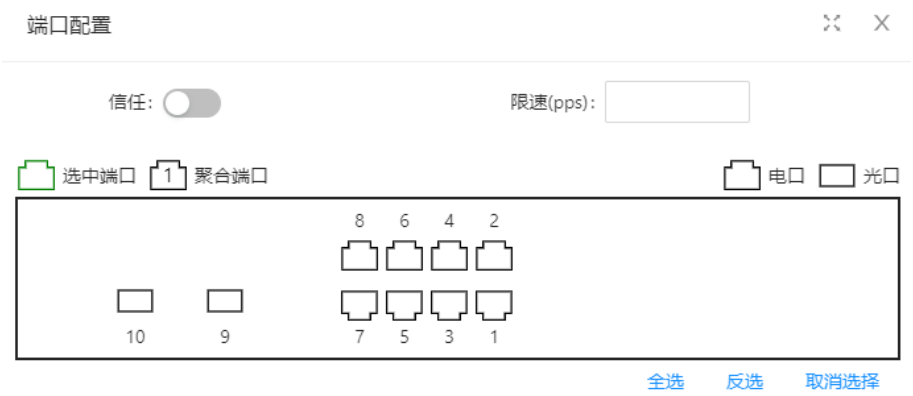
配置项	说明
状态	全局使能或者禁用 DHCP Snooping
VLAN 列表	配置 DHCP Snooping 的 VLAN 生效范围，默认是所有 VLAN 都生效
MAC 地址校验	开启/关闭 DHCP 报文 MAC 地址校验功能
82 号选项	配置在 DHCP 请求报文中添加 option-82 信息，在应答报文中剔除 option-82 信息
数据库延迟	配置 DHCP Snooping database 数据定时写入 flash 的时间间隔
应用	点击此应用完成配置

（2）选择对应的需要打开此功能的端口，点击【编辑】按钮或者点击“端口配置”下方的【批量配置】按钮，进入端口配置界面，如图 4-23 所示，端口配置参数描述如表格 4-15 所示。

表 4-15 DHCP Snooping 信任口配置参数

配置项	说明
信任	开启 DHCP Snooping 信任口
限速	设置端口 DHCP 限速，PPS 为每秒报文数，范围 0-128

图 4-23 DHCP Snooping 信任口配置



4.5 QinQ

4.5.1 概述

QinQ 是 802.1Q in 802.1Q 的简称，它是基于 IEEE 802.1Q 技术的一种二层隧道协议，通过将用户的私网报文封装上外层 VLAN Tag，使其携带两层 VLAN Tag 穿越运营商的骨干网络（又称公网），从而为用户提供了一种比较简单的二层 VPN 隧道技术，也使运营商能够利用一个 VLAN 为包含多个 VLAN 的用户网络提供服务成为了可能。

QinQ 的产生背景和优点

在 IEEE 802.1Q 定义的 VLAN Tag 域中，只有 12 个比特位用于表示 VLAN ID，最多可以表示 4094 个 VLAN。但在实际应用中，尤其是在城域网中，需要大量的 VLAN 来隔离用户，4094 个 VLAN 远远不能满足需求。QinQ 使整个网络最多可提供 4094×4094 个 VLAN，从而满足了城域网对 VLAN 数量的需求。它具备以下优点：

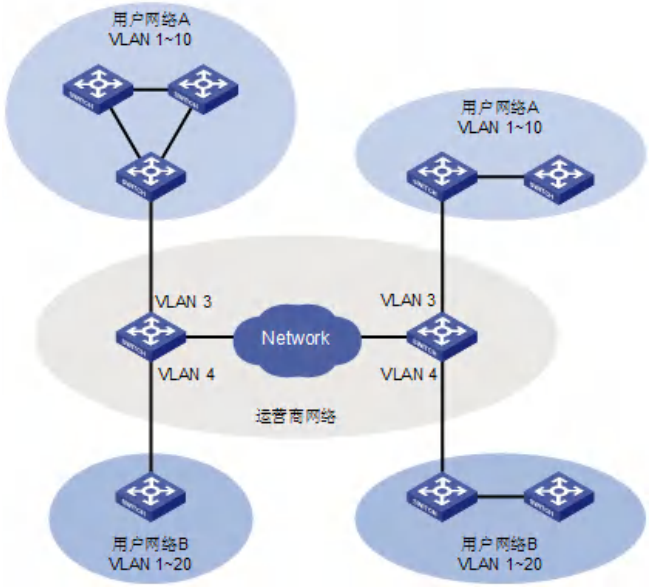
- 缓解公网 VLAN ID 资源日益紧缺的问题。
- 用户可以规划自己的私网 VLAN ID，不会导致与公网 VLAN ID 冲突。
- 为小型城域网和企业网提供了一种简单、灵活的二层 VPN 解决方案。
- 当运营商升级网络时，用户网络不必更改原有配置，使用户网络具有了较强的独立性。

QinQ 的实现原理

在公网的传输过程中，设备只根据外层 VLAN Tag 转发报文，并将报文的源 MAC 地址表项学习到外层 VLAN Tag 所在 VLAN 的 MAC 地址表中，而用户的私网 VLAN Tag 将被当作报文的数据部分进行传输。

如图 4-24 所示，用户网络 A 和 B 的私网 VLAN 分别为 VLAN 1～10 和 VLAN 1～20。运营商为用户网络 A 和 B 分配的 VLAN 分别为 VLAN 3 和 VLAN 4。当用户网络 A 和 B 中带 VLAN Tag 的报文进入运营商网络时，报文外面就会被分别封装上 VLAN 3 和 VLAN 4 的 VLAN Tag。这样，来自不同用户网络的报文在运营商网络中传输时被完全分开，即使这些用户网络各自的 VLAN 范围存在重叠，在运营商网络中传输时也不会产生冲突。

图 4-24 QinQ 典型应用组网图

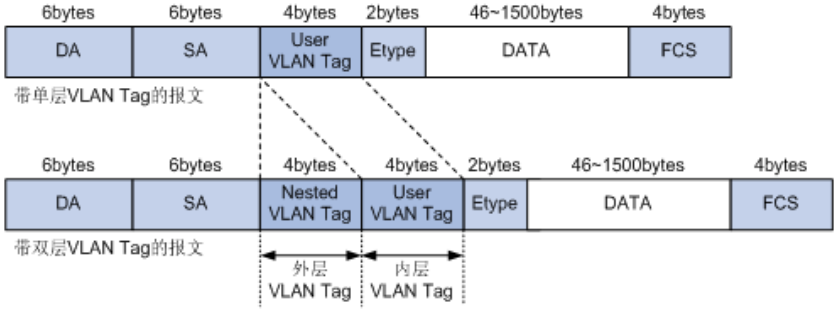


QinQ 的报文结构

如图 4-25 所示，QinQ 报文在运营商网络中传输时带有双层 VLAN Tag：

- 内层 VLAN Tag：为用户的私网 VLAN Tag；
- 外层 VLAN Tag：为运营商分配给用户的公网 VLAN Tag。

图 4-25 QinQ 的报文结构



QinQ 的实现方式

QinQ 的实现方式可分为以下两种：

1. 基本 QinQ

基本 QinQ 是基于端口方式实现的。当端口上配置了基本 QinQ 功能后，不论从该端口收到的报文是否带有 VLAN Tag，设备都会为该报文打上本端口缺省 VLAN 的 Tag：

- 如果收到的是带有 VLAN Tag 的报文，该报文就成为带双 Tag 的报文；
- 如果收到的是不带 VLAN Tag 的报文，该报文就成为带有本端口缺省 VLAN Tag 的报文。

2. 灵活 QinQ

灵活 QinQ 是基于端口与 VLAN 相结合的方式实现的，它对 QinQ 的功能进行了扩展，是对 QinQ 的一种更灵活的实现。灵活 QinQ 除了能实现所有基本 QinQ 的功能外，对于从同一个端口收到的报文，还可以根据 VLAN 的不同进行不同的操作，包括：

- 为具有不同内层 VLAN ID 的报文添加不同的外层 VLAN Tag。

- 根据报文内层 VLAN 的 802.1p 优先级标记外层 VLAN 的 802.1p 优先级。

通过使用灵活 QinQ 技术，在能够隔离运营商网络和用户网络的同时，又能够提供丰富的业务特性和更加灵活的组网能力。

4.5.2 QinQ 配置

VPN 配置

在导航栏中选择【高级】→【二层】→【QinQ 配置】，进入 QinQ VPN 配置概况界面，如图 4-26 所示。

图 4-26 VPN 配置概况

点击“VPN 配置”下方的【添加】按钮，进入创建 VPN 界面，如图 4-27 所示，各参数说明如表格 4-16 所示。

图 4-27 VPN 创建界面

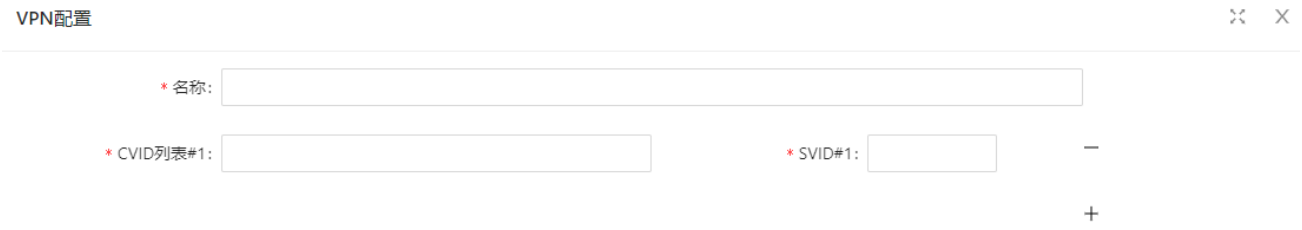


表 4-16 VPN 配置参数说明

配置项	说明
名称	QinQ 规则名
CVID	客户端 VLAN ID
SVID	服务端 VLAN ID

端口配置

在当前界面，点击对应端口的【编辑】按钮或者点击“端口配置”下方的【批量编辑】按钮，进入端口配置界面，如图 4-28 所示，各参数说明如表格 4-17 所示。。

图 4-28 端口配置界面

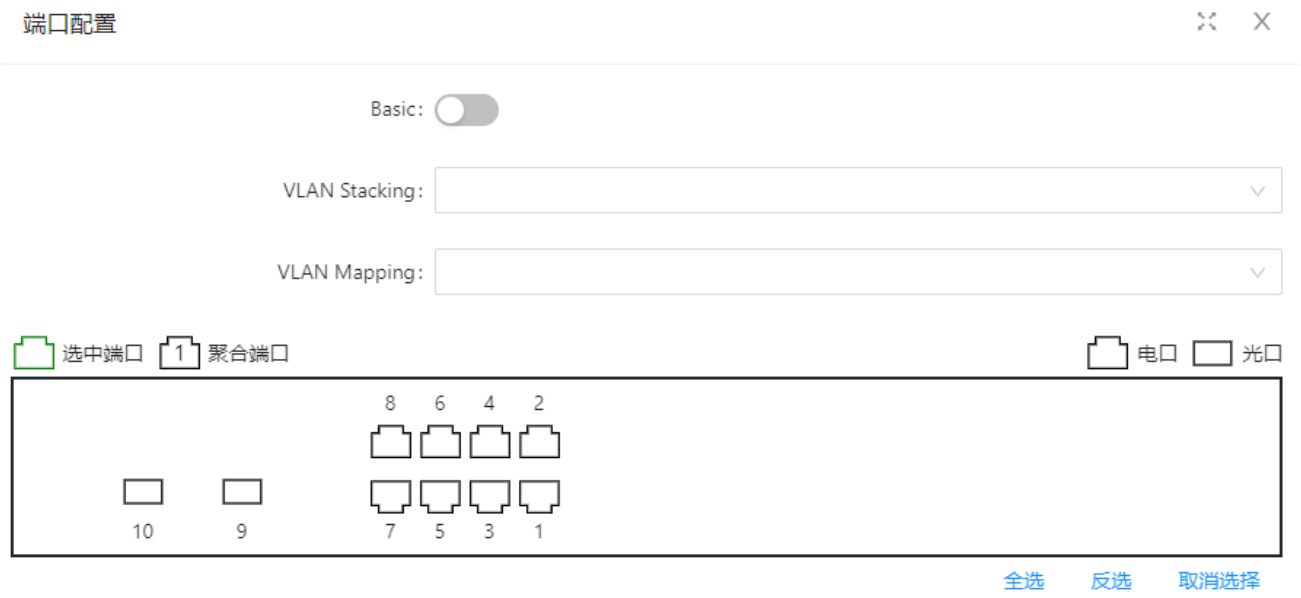


表 4-17 端口配置参数说明

配置项	说明
名称	接口名称
Basic	基础 QinQ 规则应用状态
VLAN Stacking	多层 QinQ 规则应用状态
VLAN Mapping	替换型 QinQ 规则应用状态

4.6 ACL

4.6.1 概述

ACL（Access Control List，访问控制列表）通过配置对报文的匹配规则和处理操作来实现包过滤的功能。可以有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。由 ACL 定义的数据包匹配规则，也可以被其它需要对流量进行区分的功能引用，如 QoS 中流分类规则的定义。

ACL 通过一系列匹配条件对数据包进行分类，这些条件可以是数据包的 SMAC、DMAC、SIP、DIP 等。根据匹配条件，可将 ACL 分为以下几种：

基于 IP 的标准 ACL：只根据数据包的源 IP 地址制定规则。

基于 IP 的扩展 ACL：根据数据包的源 IP 地址、目的 IP 地址、ETYPE、protocol 制订规则。

基于 MAC 的 ACL：根据数据包的源 MAC 地址、目的 MAC 地址制订规则。

基于 IPV6 的 ACL：根据数据包的源 IPV6 地址、目的 IPV6 地址、protocol 等制订规则。

4.6.2 ACL 配置

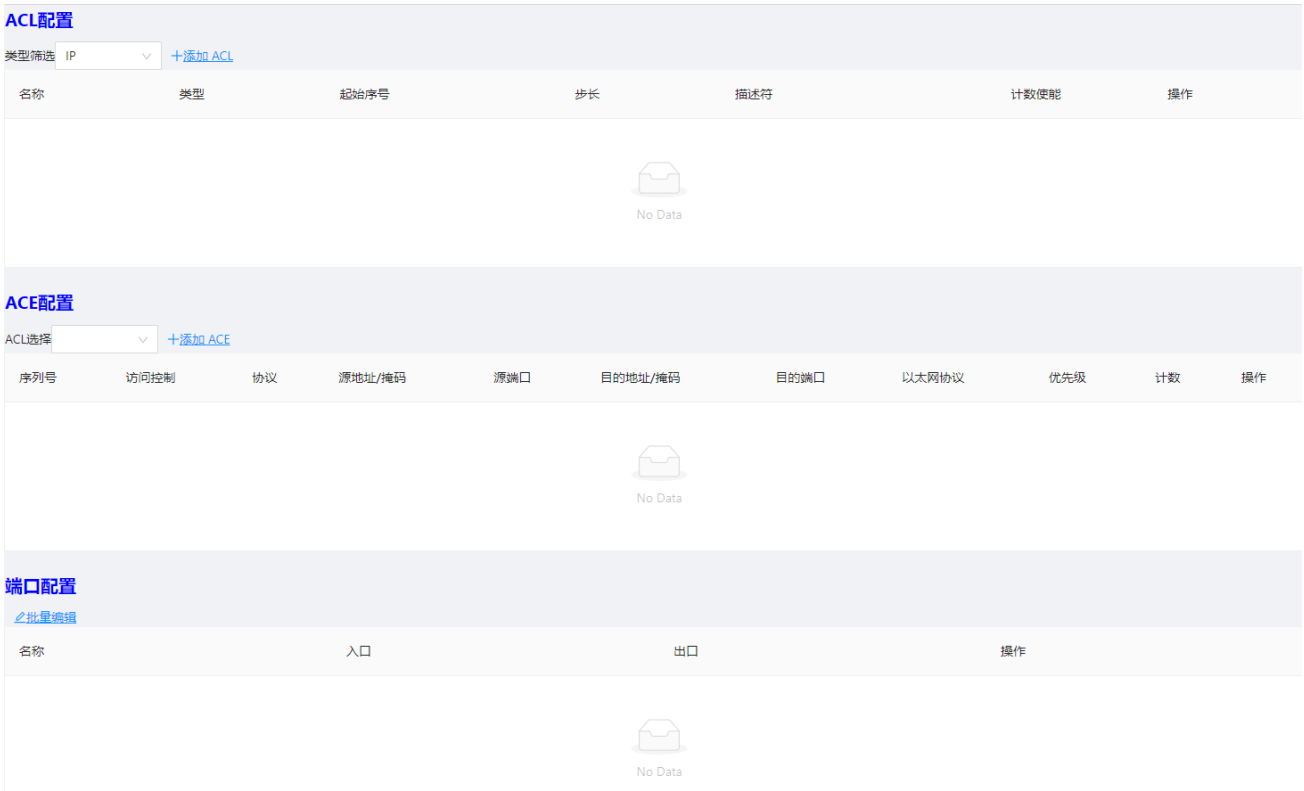
说明

- 单个 ACL-ID 下最多可以配置 128 条规则；因硬件资源限制，单设备最大支持应用规则数参考具体产品规格文档。

- 当 ACL 已经应用在端口上时，若需要添加删除规则，需先从端口解应用。

在导航栏中选择【高级】→【安全】→【ACL 配置】，进入 ACL 配置界面，如图 4-29 所示，此页面包含“ACL 配置”，“ACE 配置”，“端口配置”三个部分。

图 4-29 ACL 配置界面



创建 ACL 规则

ACL 模块提供了基于 ACL 类型的配置，包括 IP、IP-Extend、IPV6、MAC，ACL 配置界面如图 4-30~34 所示，各参数说明如表 4-18~22 所示。

表 4-18 ACL 类型参数说明

配置项		说明
ACL 类型	IP	标准 IP 的 ACL，可匹配 IPv4 报文中的源 IP 字段
	IP-Extend	扩展 ACL，可匹配 IPv4 报文的协议号、源 IP 地址、目的 IP 地址、4 层端口号等
	IPV6	IPv6 ACL，可匹配 IPv6 报文源 IP 地址、目的 IP 地址、协议号等
	MAC	MAC ACL，可匹配目的 MAC 地址、源 MAC 地址、Etype 等字段
名称		标准 IP 有效数字范围：<1-99>	<1300-1999> 扩展 IP 有效数字范围：<100-199>	<2000-2699> MAC ACL 有效数字范围：<200-699> IPv6 ACL 仅支持字符串命名，所有 ACL 均支持字符串命名，字符串长度范围<1-64>
计数使能		使能计数功能，当报文命中 ACL 时，计数值加 1
起始序号		规则表项序号起始值，缺省值:10，范围<1-2147483647>

步长	序号地增值，缺省值:10，范围<1-2147483647>
描述符	定义该 ACL 描述信息

图 4-30 ACL 类型配置界面

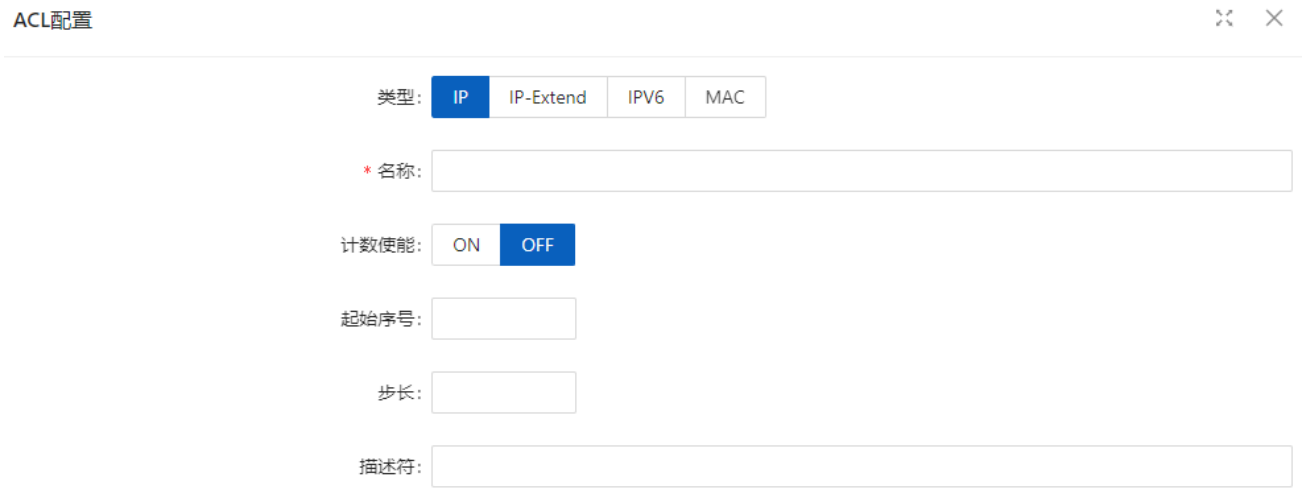


表 4-19 ACL IP 类型参数说明

配置项		说明
访问控制	Permit	放行命中该规则的报文
	Deny	丢弃命中该规则的报文
序列号		规则表项序号
源地址		源 IP 地址，如 192.168.64.1
源掩码		IP 的掩码取反,如匹配 IP 地址前 24 位,掩码为 255.255.255.0,这里需配置为 00.00.00.255

图 4-31 IP 类型 ACE 配置界面

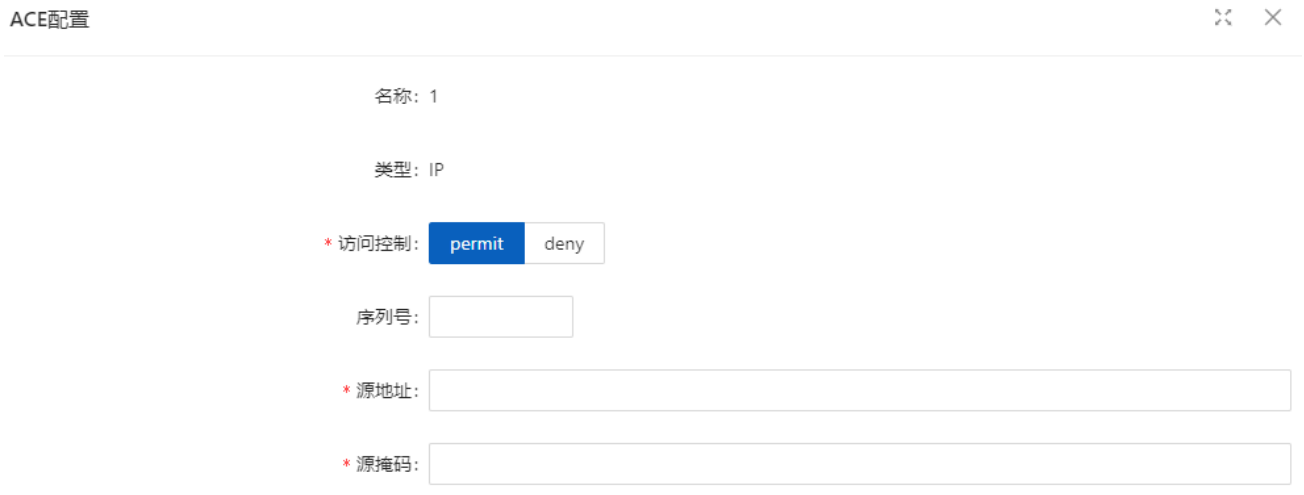


表 4-20 IP-Extend 类型 ACE 参数说明

配置项		说明
访问控制	Permit	放行命中该规则的报文
	Deny	丢弃命中该规则的报文
序列号		规则表项序号

协议	支持常用协议报文选项，包含 tcp、udp、vrrp、igmp、gre、ipcomp、ospf、pim、rsvp 等 支持所有 IPv4 报文 支持自定义 protocol 的 IPv4 报文
源地址	源 IP 地址，如 192.168.64.1
源掩码	IP 的掩码取反,如匹配 IP 地址前 24 位,掩码为 255.255.255.0,这里需配置为 00.00.00.255
目标地址	目的 IP 地址，如 192.168.64.100
目标掩码	同源掩码

图 4-32 IP-Extend 类型 ACE 配置界面

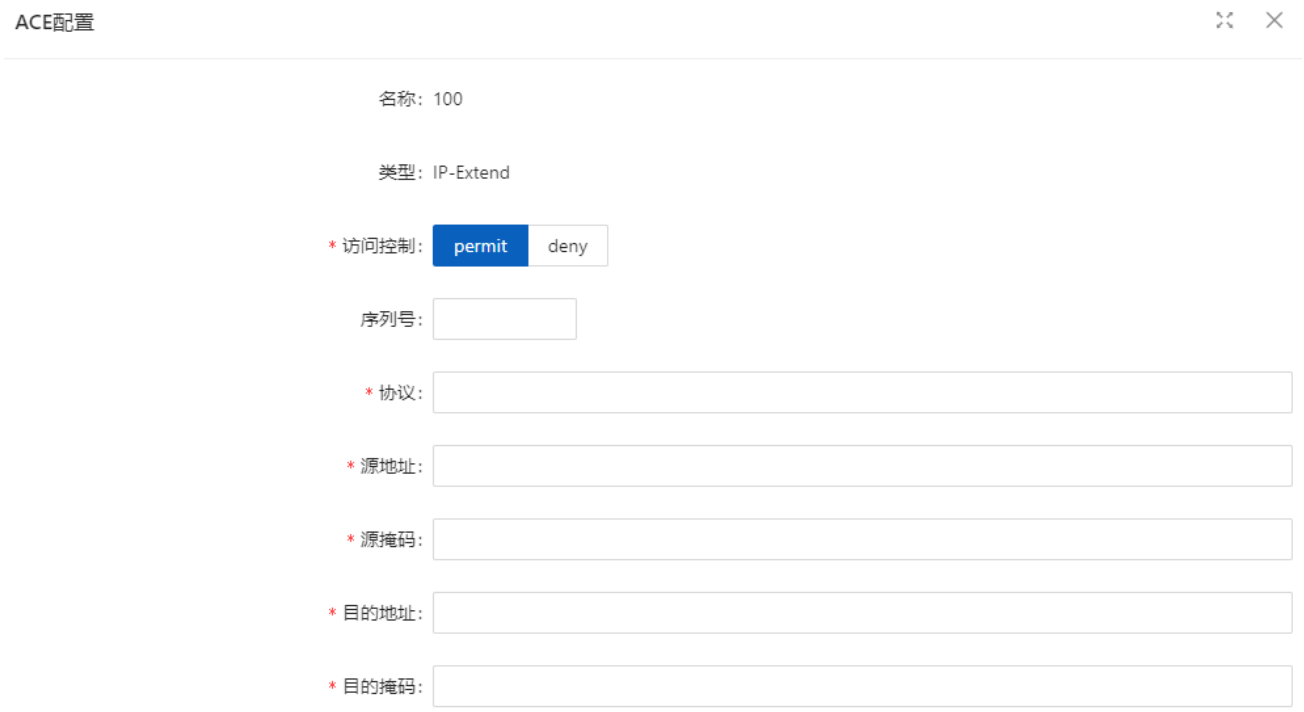


表 4-21 IPV6 类型 ACE 参数说明

配置项		说明
访问控制	Permit	放行命中该规则的报文
	Deny	丢弃命中该规则的报文
序列号		规则表项序号
协议		支持常用协议报文选项，包含 tcp、udp、icmp 等 支持所有 IPv6 报文 支持自定义 protocol 的 IPv6 报文
源地址		源 MAC 地址，如 00.d0.f8.22.33.40
源掩码		MAC 地址掩码取反，如匹配 MAC 地址前 24 位，掩码为 ffff.ff00.0000，这里需配置为 0000.00ff.ffff
目标地址		目的 MAC 地址，如 00.d0.f8.22.33.41
目标掩码		同源掩码

图 4-33 IPV6 类型 ACE 配置界面

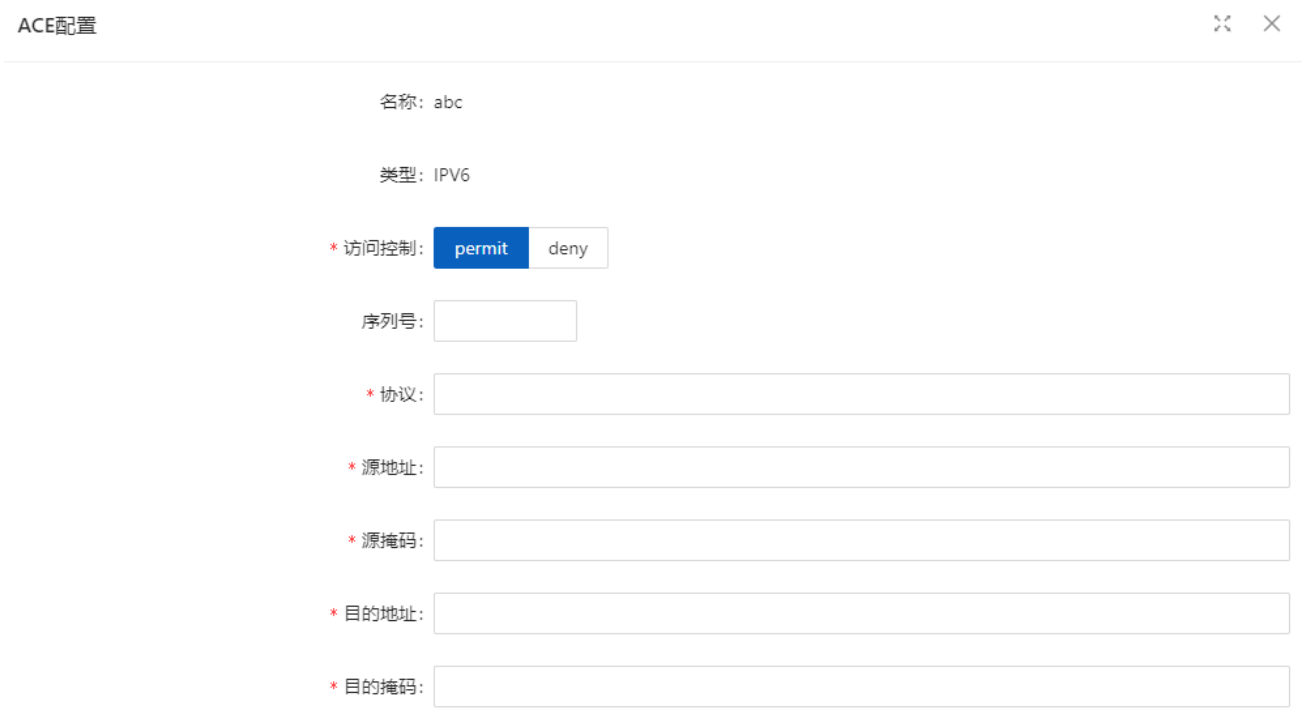
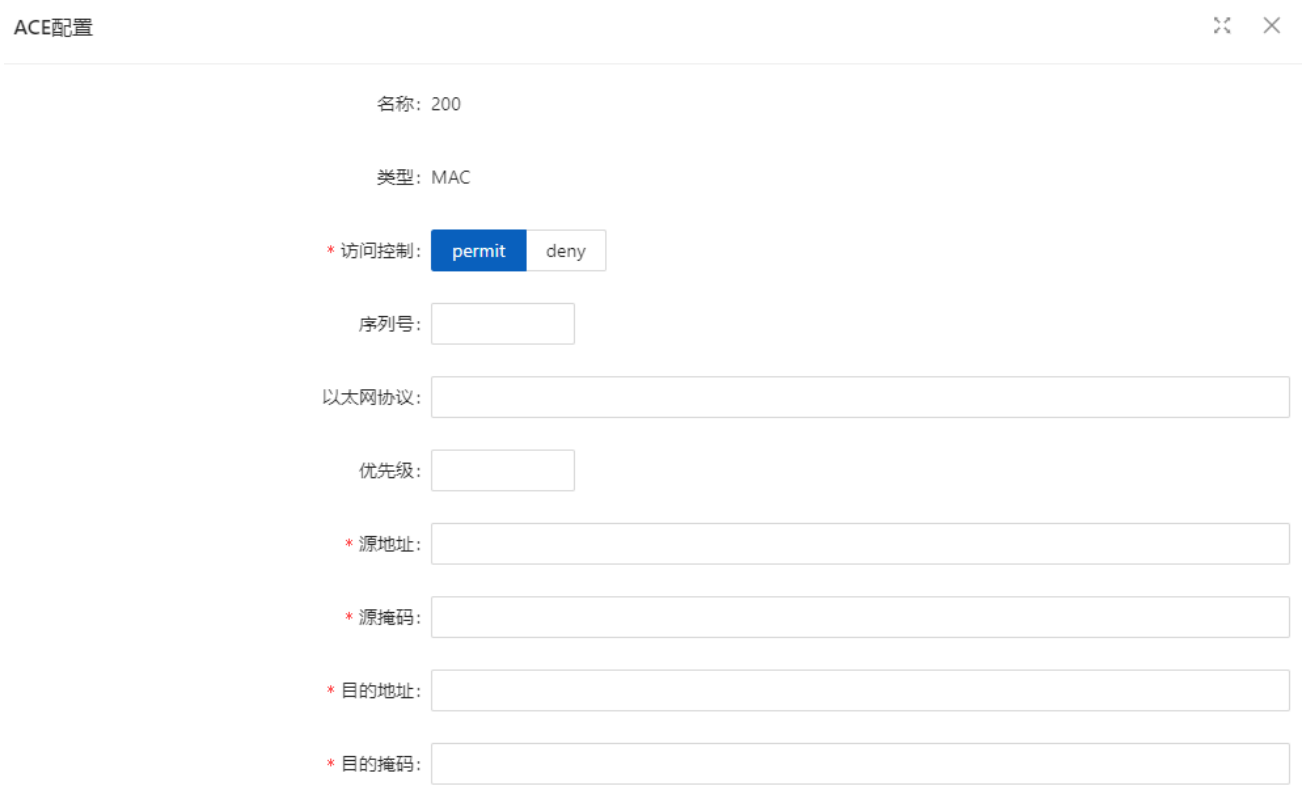


表 4-22 MAC 类型 ACE 参数说明

配置项		说明
访问	Deny	放行命中该规则的报文
	Permit	丢弃命中该规则的报文
序列号		规则表项序号
以太网协议		以太网协议类型 ，范围(0x05DD-0xFFFF)
优先级		报文的 cos 值，范围（0-7）
源地址		报文源 MAC 地址
源掩码		源 MAC 地址掩码取反，比如选择 MAC 地址的前 32 位，掩码为 0000.0000.ffff
目的地址		报文目的 MAC 地址
目的掩码		目的 MAC 地址掩码取反，比如选择 MAC 地址的前 32 位，掩码为 0000.0000.ffff

图 4-34 MAC 类型 ACE 配置界面

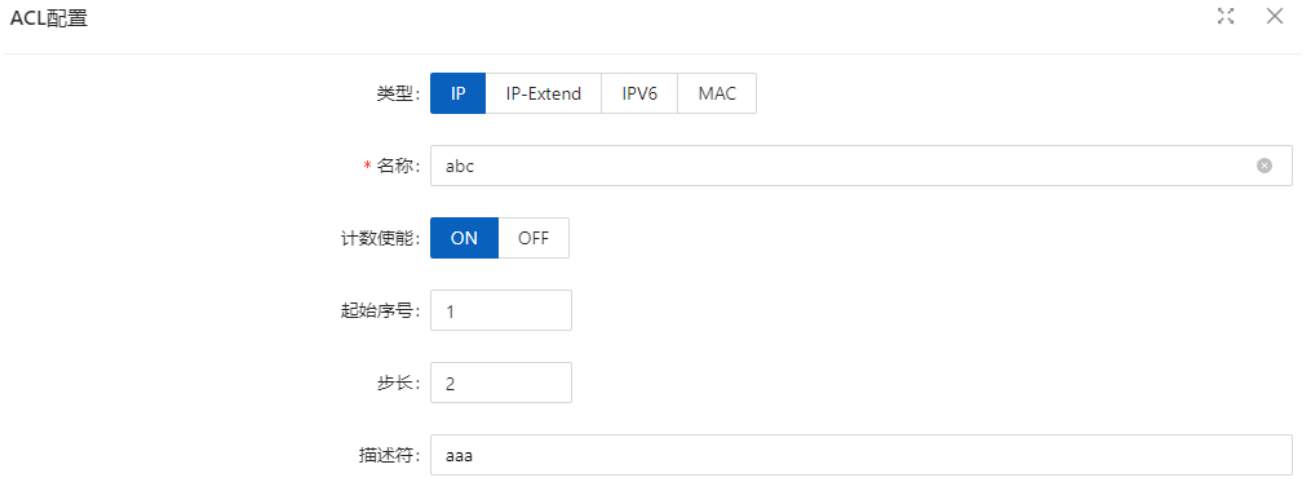


操作步骤：

（1）在导航栏中选择【高级】→【安全】→【ACL 配置】，进入 ACL 配置界面。

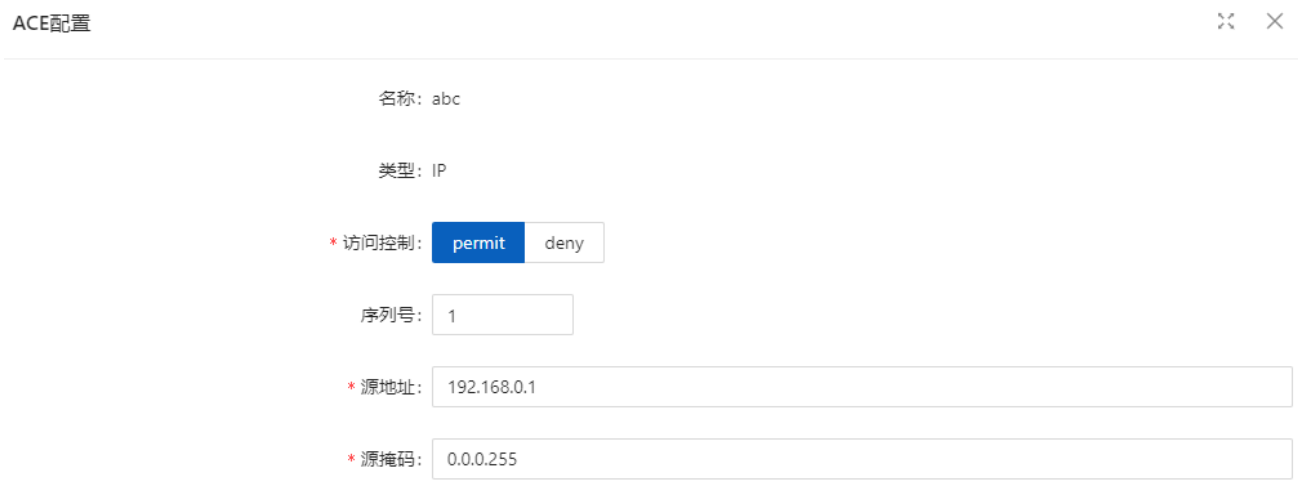
（2）点击“ACL 配置”下方的【添加 ACL】按钮，进入 ACL 规则创建界面，根据要求填写好参数，如图 4-35 所示，点击【确认】按钮完成配置。

图 4-35 创建 IP 类型的 ACL



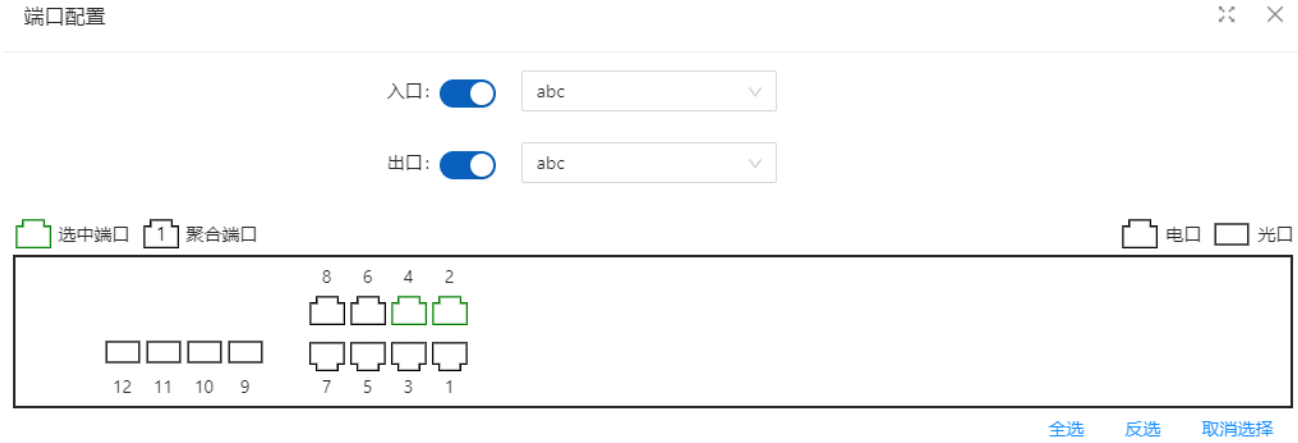
（3）点击“ACE 配置”下方的【添加 ACE】按钮，进入 ACE 配置界面，根据要求填写好参数，如图 4-36 所示，点击【确认】按钮完成配置。

图 4-36 配置 IP 类型的 ACE



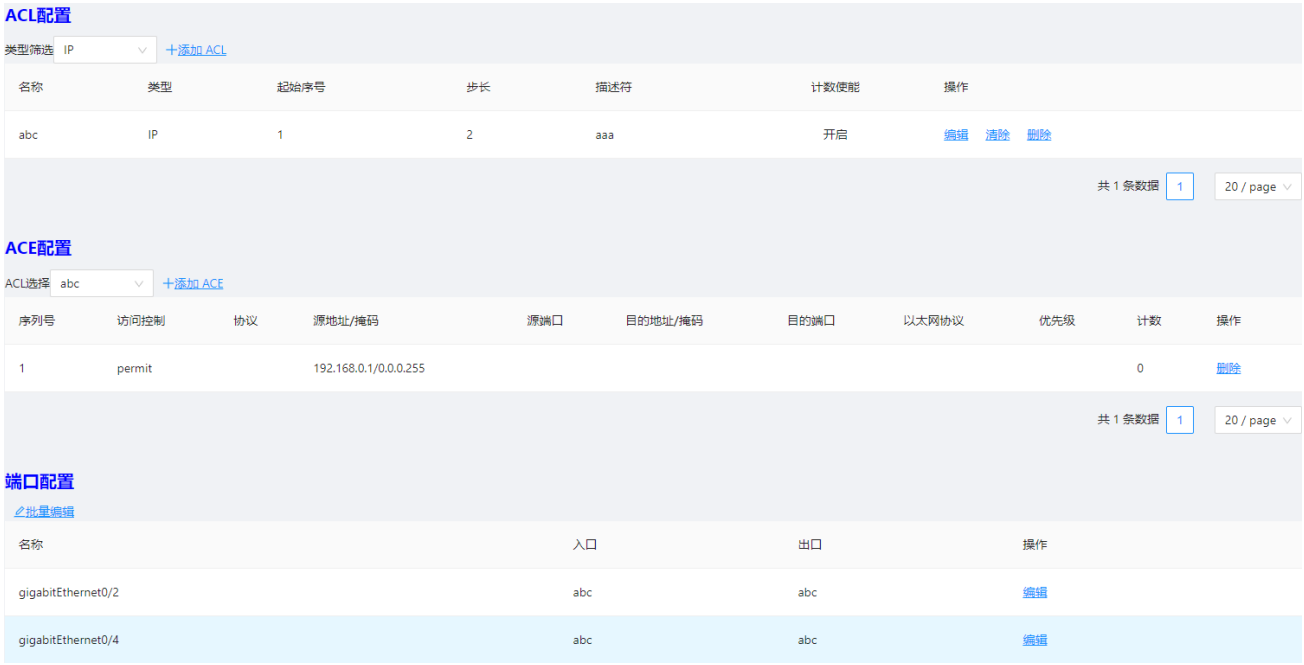
（4）点击“端口配置”下方的【批量配置】按钮，选择 ACL 条例“abc”，端口面板选择 2，4，如图 4-37 所示，点击【确认】按钮完成配置。

图 4-37 ACL 端口配置



创建成功后的 ACL 完整界面如图 4-38 所示

图 4-38 创建成功的 ACL 规则



（5）点击辅助区的【保存】按钮，保存配置。

4.7 QoS

4.7.1 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。

4.7.2 QoS 配置

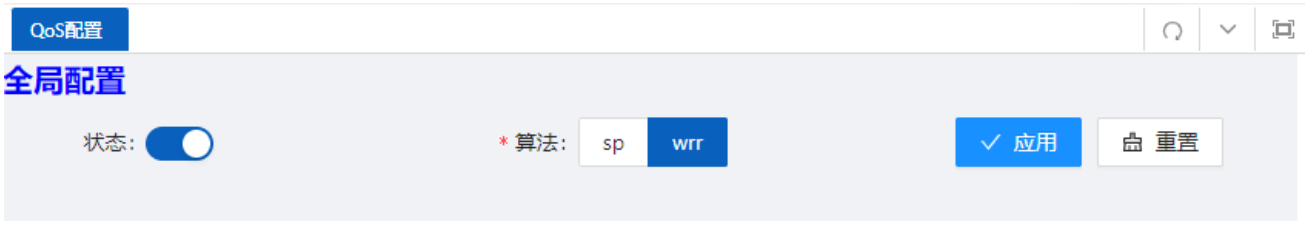
说明

cir 数值是可确定的，比如限速 1M，那么 cir 数值为 1024，但是 cbs 的数值却取自经验数值。当 cbs 数值配大，流量尖峰更高，限速较稳定，但平均速率可能高于限速值；当 cbs 数值配小，流量尖峰较低，限速波动较大，平均速率可能小于限速值。建议 cbs 配置取 cir 的 4 倍值与 31250 的小值。

使能 QoS

（1）在导航栏中选择【高级】→【安全】→【QoS 配置】，进入 QoS 配置界面，如图 4-39 所示。

图 4-39 QoS 全局配置界面



（2）点击【状态】按钮，选择算法，点击【确认】按钮使能 QoS。

表 4-23 QoS 全局配置参数说明

配置项	说明		
全局配置	状态		启用 QOS，在启用前所有 QOS 功能不支持配置
	算法	Sp	绝对优先级调度，队列 ID 大优先级高，高优先级队列处理完成后处理低优先级队列
		Wrr	轮转调度算法，根据队列权重，从队列 ID 最大到最小，依次调度各个队列。

配置 Qos 映射

（1）在当前界面，点击“QoS 映射”下方的【队列】按钮，进入队列配置界面，如图 4-40 所示，参数说明如表格 4-24 所示。

图 4-40 队列配置界面

表 4-24 队列参数说明

配置项	说明	
队列权重	队列	<0， 7>
	权重	<0， 32>，数值越大，权重越高，在通道拥堵情况下该队列报文优先处理概率越大，0 表示无穷大。

（2）点击“QoS 映射”下方的【CoS】按钮，进入 CoS 配置界面，如图 4-41 所示，参数说明如表格 4-25 所示。

图 4-41 CoS 配置界面

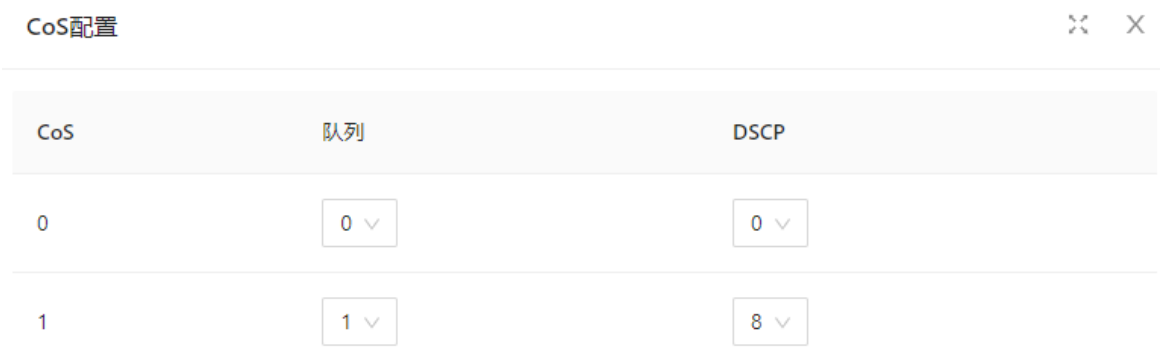


表 4-25 CoS 参数说明

配置项		说明
CoS 配置	CoS	<0， 7>
	队列	<0， 7>， Cos-queue 映射关系，在端口标记的 cos 基础上，修改报文出口队列，在配置端口为 no trust、trust cos 或 trust dscp 且非 ip 报文时生效。
	DSCP	cos-dscp 映射关系，在配置端口为 no trust、trust cos 或 trust dscp 且非 ip 报文时生效，修改报文 dscp 数值

（3）点击“QoS 映射”下方的【DSCP】按钮，进入 DSCP 配置界面，如图 4-42 所示，参数说明如表格 4-26 所示。

图 4-42 DSCP 配置界面

表 4-26 DSCP 参数说明

配置项		说明
DSCP 映射	DSCP	<0， 63>
	队列	<0， 7>， dsp-queue 映射关系，在配置端口为 trust dscp 且 ip 报文时生效，修改报文出口队列
	CoS	<0， 7>， dscp-cos 映射关系，在配置端口为 trust dscp 且 ip 报文时生效，修改报文 cos 字段
	新 DSCP 值	<0， 63>， dscp-dscp 映射关系，在配置端口为 trust dscp 且 ip 报文时生效，先进行 dscp-dscp 映射，后进行 dscp-cos 映射

Qos 分类配置

在当前 QoS 界面，点击“分类配置”下方的【添加】按钮，进入分类配置界面，如图 4-43 所示，参数说明如表格 4-27 所示。

图 4-43 分类配置界面

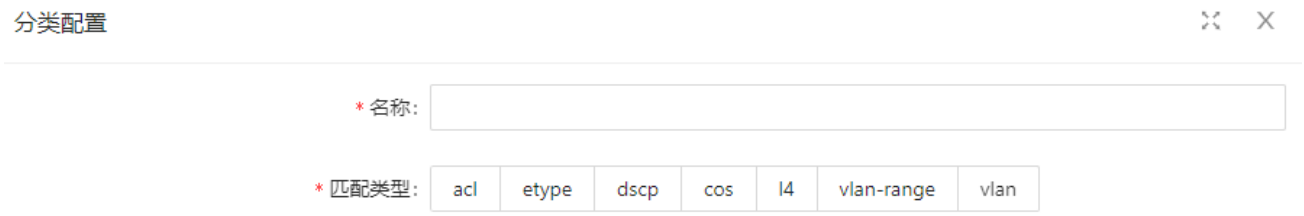


表 4-27 分类配置参数说明

配置项		说明
分类配置	名称	创建分类，定义分类名称
	匹配类型	定义匹配类型，支持关联 acl，etype，dscp，cos，l4，vlan-rangge，vlan

Qos 策略配置

在当前 QoS 界面，点击“策略配置”下方的【添加策略规则】按钮，进入规则配置界面，如图 4-44 所示，参数说明如表格 4-28 所示。

图 4-44 规则配置界面

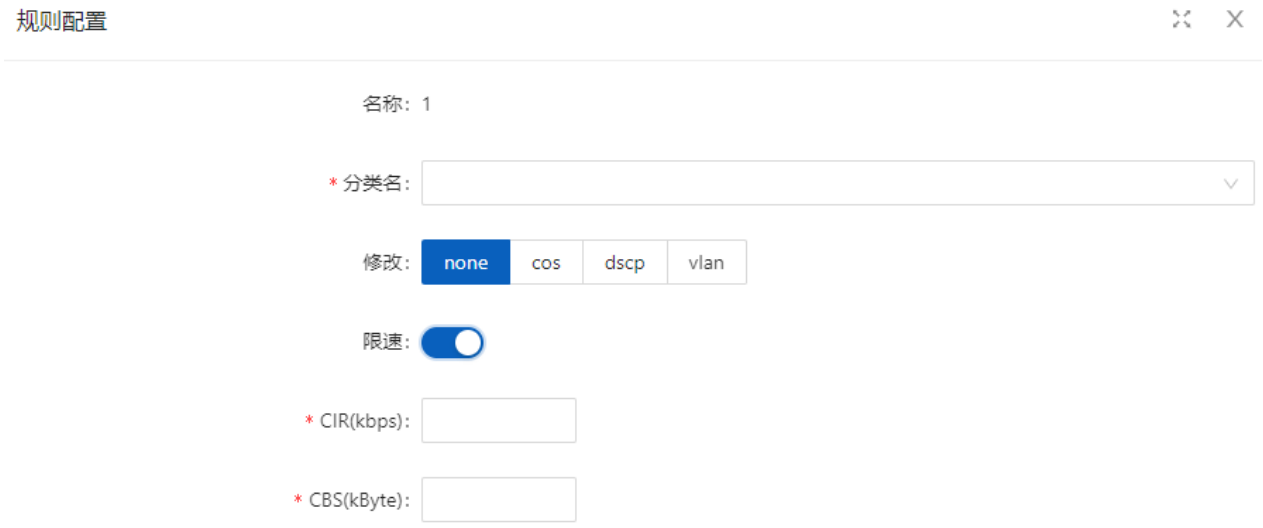


表 4-28 规则配置参数说明

配置项		说明
规则配置	名称	规则名称
	分类名	选择分类名称
	修改	策略对应的动作一，支持修改 cos、dscp、vlan 等动作
	限速	策略对应的动作二，限速
	CIR	限速水线，单位 kbps
	CBS	burst 能力，单位 Kbyte

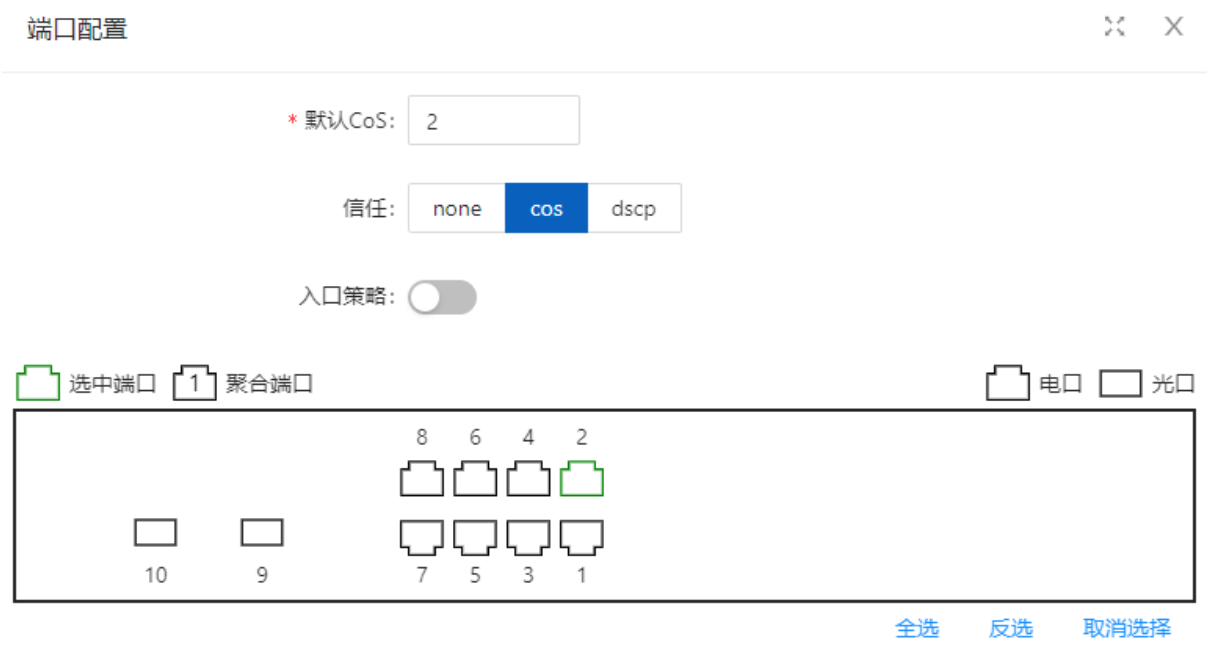
Qos 端口配置

在 QoS 界面，点击“端口配置”下方的【批量编辑】按钮，进入端口配置界面，如图 4-45 所示，端口配置参数说明如表格 4-29 所示。

表 4-29 规则配置参数说明

配置项		说明
端口配置	默认 CoS	<0， 7>，当配置端口不信任，或配置信任但报文不满足信任条件时，采用端口默认 cos 标记入口报文
	信任	支持不信任、信任 cos、信任 dscp 配置。当处于 no trust 模式时，入口阶段根据端口默认 cos 修改报文 cos 字段以及 dscp 字段；当配置 trust cos 时，对于 untagged 报文同 no trust 模式，对于带 tag 报文，选择报文自带 cos；当配置 trust dscp 时，对于 ip 报文，选择报文自带 dscp，对于非 ip 报文，同 trust cos 模式。
	入口策略	选择创建的策略

图 4-45 QoS 端口配置界面



4.8 路由

4.8.1 静态 ARP

4.8.1.1 概述

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

在局域网中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报文必须封装成帧才能通过物理网络发送，

因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。ARP 就是实现这个功能的协议。

ARP 表

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

ARP 表项分为动态 ARP 表项和静态 ARP 表项。

1. 动态 ARP 表项

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

2. 静态 ARP 表项

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

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

4.8.1.2 配置 ARP 管理

查看 ARP 表项

在导航栏中选择【高级】→【三层】→【静态 ARP】→【ARP 信息】，进入静态 ARP 信息页面，如图 4-46 所示。在“概况”中可以 ARP 表项信息，各参数说明如表格 4-30 所示。

图 4-46 ARP 表项信息

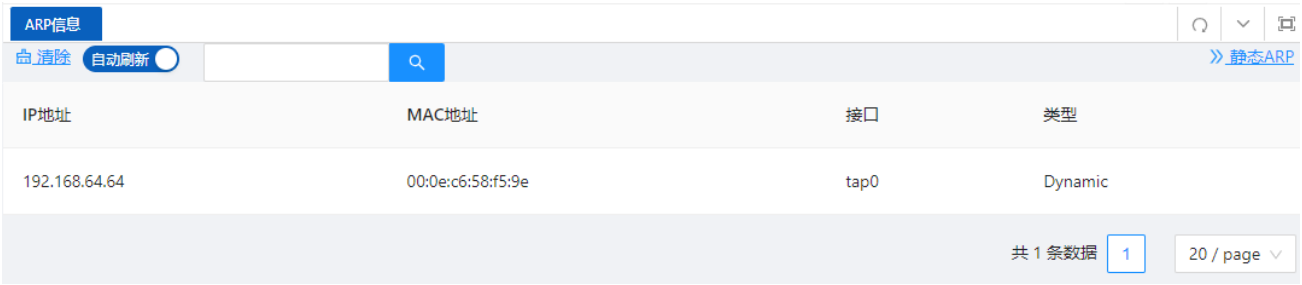


表 4-30 ARP 表项参数说明

配置项	说明
IP	终端 IP 地址
MAC 地址	终端 MAC 地址
接口	终端所在的三层接口名
类型	ARP 地址类型

配置 ARP 表项

（1）在导航栏中选择【高级】→【三层】→【静态 ARP】，进入 ARP 配置界面，如图 4-47 所示。

（2）点击【添加】按钮进入静态 ARP 创建界面，如图 4-48 所示；

（3）配置静态 ARP 的信息，详细配置信息如表 4-30 所示；

（4）点击【确认】按钮完成操作。

图 4-47 静态 ARP 配置界面

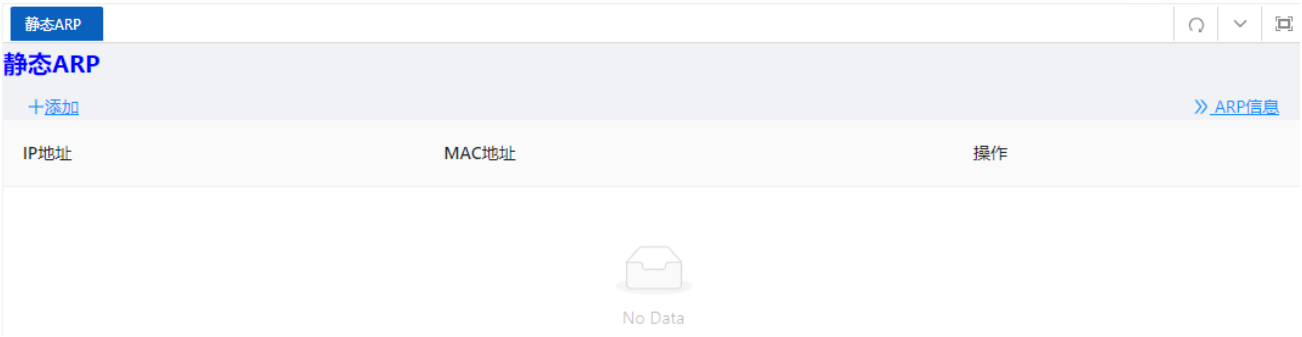


图 4-48 新建静态 ARP 界面

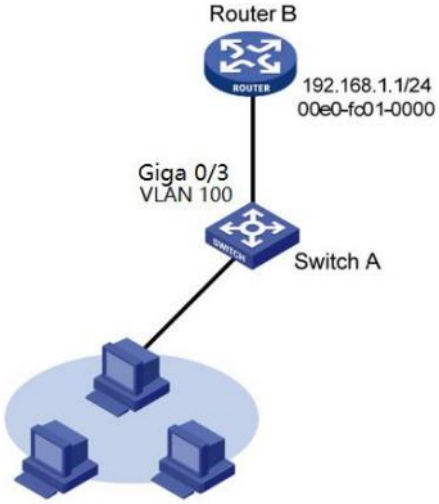
4.8.1.3 配置 ARP 举例

1. 组网需求

- Switch A 连接主机，通过接口 GigabitEthernet 0/3 连接 Router B。接口 GigabitEthernet 0/3 属于 VLAN 100。
- Router B 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-0000。

为了增加 Switch A 和 Router B 通信的安全性，可以在 Switch A 上配置静态 ARP 表项。

图 4-49 静态 ARP 配置组网图



2. 配置步骤

（1）创建 VLAN 100，配置端口 GigabitEthernet 0/3 VLAN 100。

选择【配置】→【VLAN】，进入 VLAN 配置界面，在 VLAN 配置页面，点击【添加】按钮，创建 VLAN100，选择端口 GigabitEthernet 0/3 为 Untagged 成员口，如图 4-50 所示。

图 4-50 新建 VLAN100 界面

（2）创建三层 SVI 口

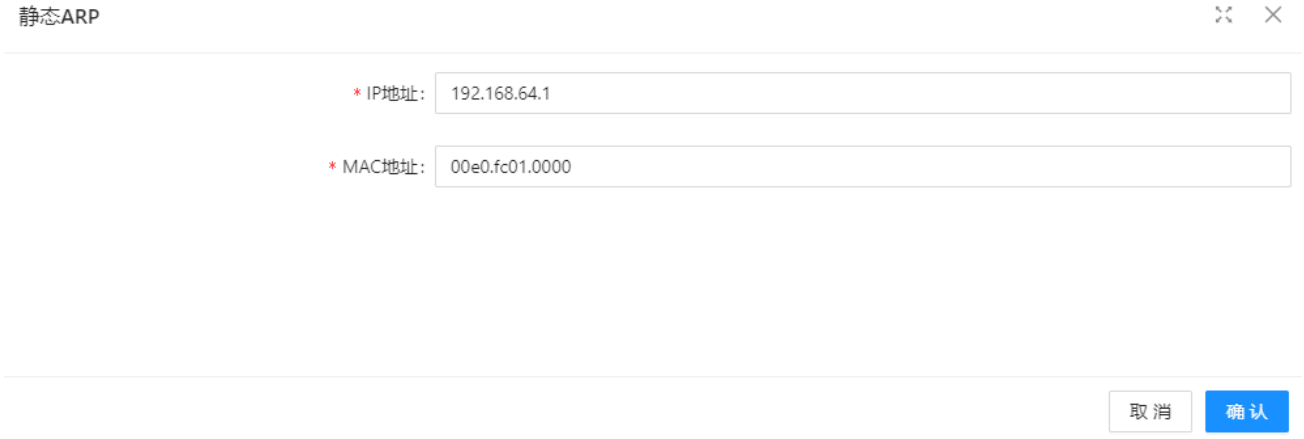
选择【配置】→【端口】→【端口配置】，进入三层端口配置界面，点击【添加】按钮，配置 VLAN ID、Ipv4 地址/掩码，如图 4-51 所示，点击【确认】按钮完成配置。

图 4-51 创建三层 SVI 口

(4) 配置 Router B 为静态 ARP

在导航栏中选择【高级】→【三层】→【静态 ARP】，进入静态 ARP 配置界面，点击【添加】按钮进入 ARP 配置界面，配置 IP 地址、MAC 地址，如图 4-52 所示，点击【确认】按钮完成配置。

图 4-52 ARP 配置页面



4.8.2 路由

在网络中路由器根据所收到的报文的目的地址选择一条合适的路径，并将报文转发到下一个路由器。路径中最后的路由器负责将报文转发给目的主机。路由就是报文在转发过程中的路径信息，用来指导报文转发。

4.8.2.1 路由表

路由器通过路由表选择路由，把优选路由下发到 FIB（Forwarding Information Base，转发信息库）表中，通过 FIB 表指导报文转发。每个路由器中都至少保存着一张路由表和一张 FIB 表。

路由表中保存了各种路由协议发现的路由，根据来源不同，通常分为以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。
- 静态路由：网络管理员手工配置的路由。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。其缺点是每当网络拓扑结构发生变化，都需要手工重新配置，不能自动适应。
- 动态路由：动态路由协议发现的路由。

FIB 表中每条转发项都指明了要到达某子网或某主机的报文应通过路由器的哪个物理接口发送，就可到达该路径的下一个路由器，或者不需再经过别的路由器便可传送到直接相连的网络中的目的主机。

4.8.2.2 静态路由

静态路由是一种特殊的路由，由管理员手工配置。当组网结构比较简单时，只需配置静态路由就可以使网络正常工作。

静态路由不能自动适应网络拓扑结构的变化。当网络发生故障或者拓扑发生变化后，必须由网络管理员手工修改配置。

4.8.2.3 配置静态路由

查看静态路由配置

在导航栏中选择【高级】→【三层】→【静态路由】，进入静态路由配置页面，如图 4-53 所示。在“概况”中可以显示静态路由配置情况，各参数说明如表格 4-31 所示。

图 4-53 静态路由显示界面

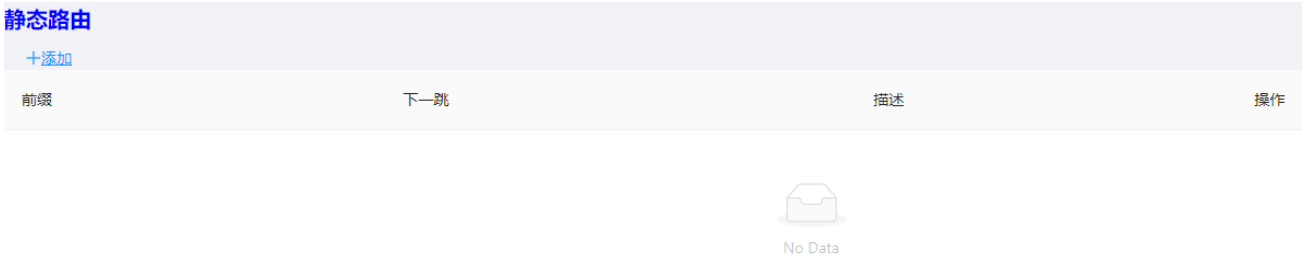


表 4-31 静态路由参数说明

配置项	说明
前缀 IP	即路由前缀地址，或者路由网段；比如常见路由 0.0.0.0/0 192.168.1.1 中，前缀 IP 为 0.0.0.0
前缀长度	路由网段长度；比如上述举例中长度为 0
下一条地址	路由下一跳地址；比如上述举例中下一跳为 192.168.1.1
描述	路由描述信息，可选配置

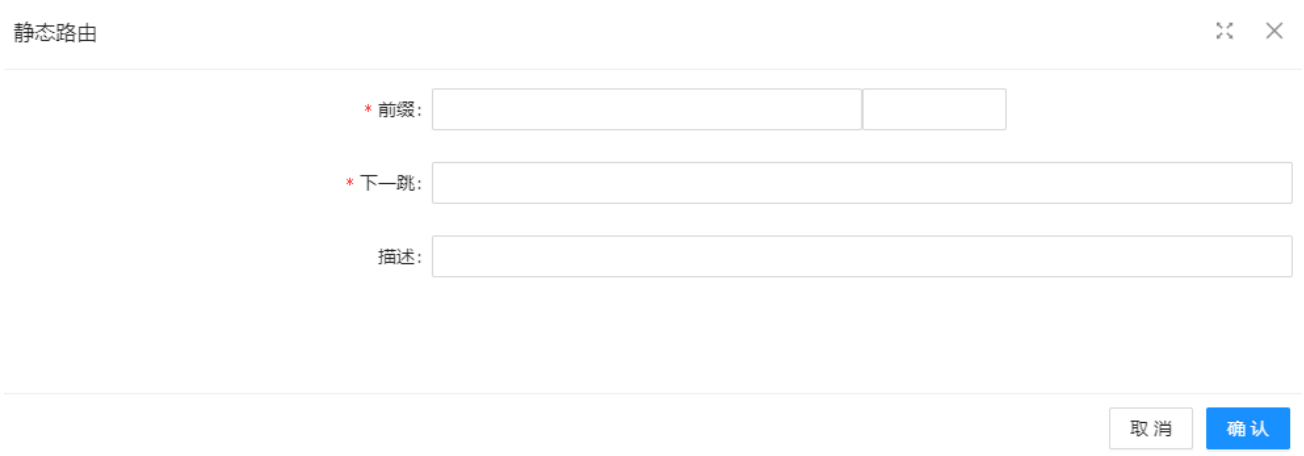
新建静态路由步骤

（1）在导航栏中选择【配置】→【VLAN】，创建 VLAN 并选择 Untagged 成员口。

（2）在导航栏中选择【配置】→【端口】→【端口配置】，添加三层 SVI 口。

（3）在导航栏中选择【高级】→【三层】→【静态路由】，如图 4-51 所示，创建静态路由。

图 4-51 新建静态路由界面



注意

- 添加新的 SVI 口时，会自动将默认的管理 IP 地址删除。请确保新的 SVI 口可以继续访问。

5 维护

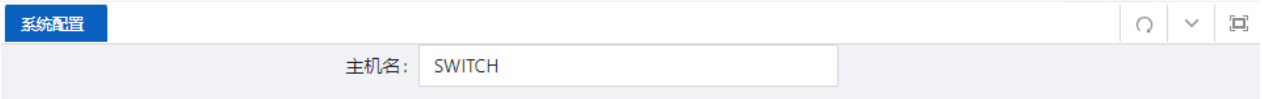
5.1 系统配置

系统配置管理模块提供了主机名称设置、服务（Telnet、 SSH、HTTP、HTTPS）开启\关闭功能，管理 IP 设置功能。

5.1.1 主机名称设置

如图 5-1 所示，用户可以使用此功能来设置交换机的名称。

图 5-1 主机名称设置



5.1.2 开启\关闭服务

服务管理概述：

1. Telnet 服务

Telnet 协议在 TCP/IP 协议族中属于应用层协议，用于在网络中提供远程登录和虚拟终端的功能。

2. SSH 服务

SSH 是 Secure Shell（安全外壳）的简称。用户通过一个不能保证安全的网络环境远程登录到设备时， SSH 可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

3. HTTP 服务

HTTP 是 Hypertext Transfer Protocol（超文本传输协议）的简称。它用来在 Internet 上传递 Web 页面信息。 HTTP 位于 TCP/IP 协议栈的应用层。

在设备上使能 HTTP 服务后，用户就可以通过 HTTP 协议登录设备，利用 Web 功能访问并控制设备。

4. HTTPS 服务

HTTPS（ Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（ Secure Sockets Layer，安全套接字层）协议的 HTTP 协议。HTTPS 通过 SSL 协议，从以下几方面提高了设备的安全性：

- 通过 SSL 协议保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备；
- 客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现了对设备的安全管理；
- 为设备制定基于证书属性的访问控制策略，对客户端的访问权限进行控制，进一步避免了非法客户对设备进行攻击。

配置步骤：

（1）如图 5-2 所示，在导航栏选择【维护】→【系统设置】，进入配置界面。

（2）点击服务选项前的复选框，点击【确认】按钮启用/禁用该服务。

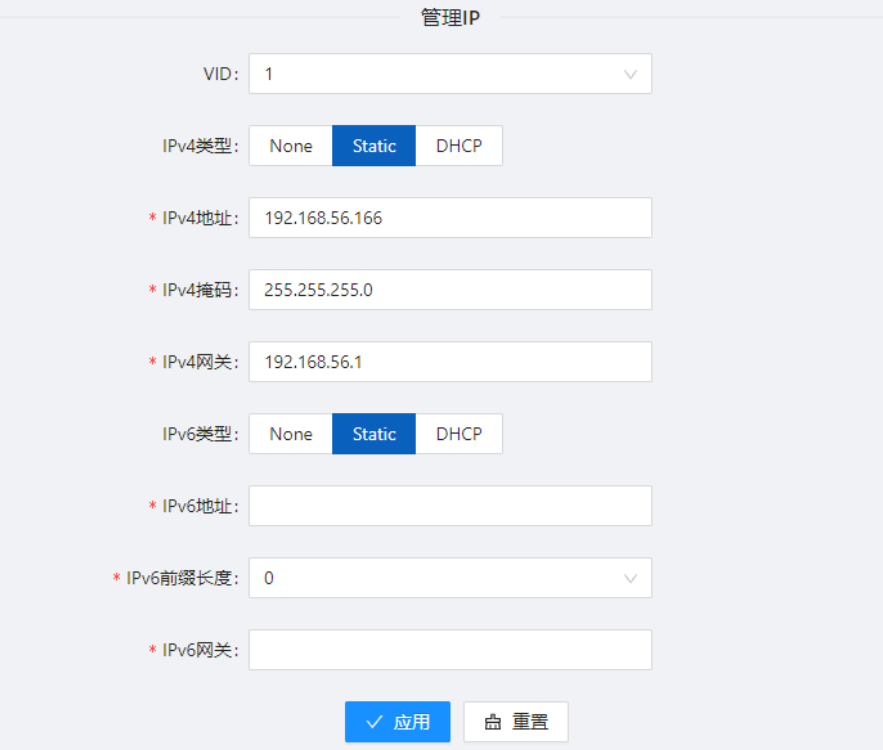
图 5-2 服务配置界面

5.1.3 管理 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。

图 5-3 管理 IP 配置界面



如图 5-3，在导航栏选择【维护】→【系统设置】，进入 IP 地址管理界面，各参数说明如表格 5-1 所示。

表 5-1 参数说明

配置项	说明
VID	管理 VLAN 配置，指定使用哪个 VLAN 作为管理 VLAN，该 VLAN 必须已经存在。
IPV4 类型	None：不使用 IPV4 管理地址 Static：表示通过手工配置指定 IPv4 地址，选择此项时需要设置 IPv4 地址和掩码长度 DHCP：表示通过 DHCP 分配获取 IPv4 地址
IPV4 地址	设置 IPV4 管理 IP 地址，IPv4 地址的获取方式选择“static”时可用

IPV4 掩码	设置子网掩码，默认为 255.255.255.0，IPv4 地址的获取方式选择“static”时可用
IPV4 网关	指定网关的 IP 地址，IPv4 地址的获取方式选择“static”时可用
IPV6 类型	None：不使用 IPV6 管理地址 Static：表示通过手工配置指定 IPv6 地址，选择此项时需要设置 IPv6 地址 DHCP：表示通过 DHCP 分配获取 IPv6 地址
IPV6 地址	设置 IPV6 管理 IP 地址，IPv6 地址的获取方式选择“static”时可用
IPV6 前缀长度	设置 IPV6 前缀长度，IPv6 地址的获取方式选择“static”时可用
IPV6 网关	设置 IPV6 网关，IPv6 地址的获取方式选择“static”时可用

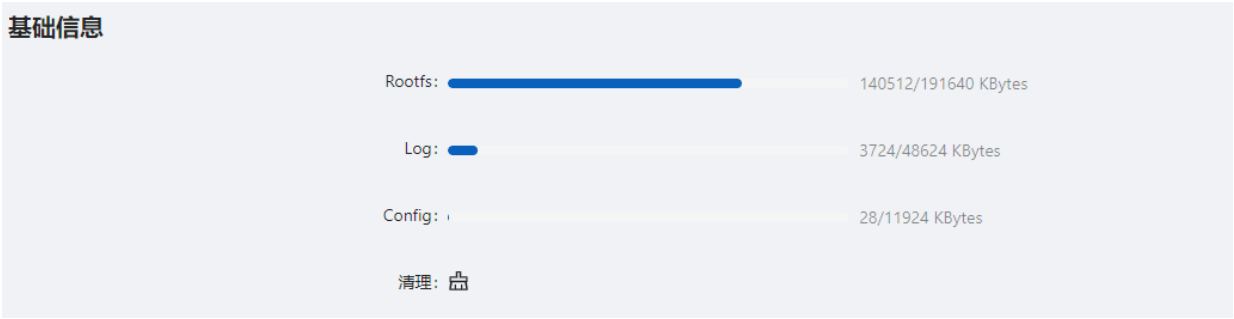
5.2 文件管理

文件管理模块包含基础信息、固件管理、配置管理、证书管理、包管理功能。

5.2.1 基础信息

在基础信息页面，可以查看设备的各个分区的使用情况，点击【清理】按钮，可以清除系统 log。

图 5-4 基础信息界面



5.2.2 固件管理

固件管理模块提供了从本地主机上获取目标应用程序文件，并将该文件设置为设备下次启动时使用的启动文件的功能。

注意

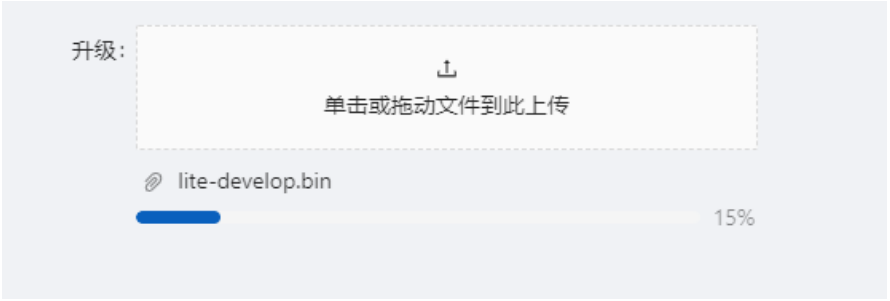
- 软件升级需要一定的时间。在软件升级的过程中，请不要在 Web 上进行任何操作，否则可能会导致软件升级中断。
- 升级完成后设备会自动重启。

图 5-5 固件界面

步骤 1：在导航栏中选择【维护】→【文件管理】，进入文件管理页面，点击“固件管理”。

步骤 2：单击【升级】按钮，在弹出的对话框里选择设备对应的升级文件，升级文件为.bin 格式，升级过程如图 5-6 所示。

图 5-6 升级界面



5.2.3 配置管理

配置管理模块提供了“备份配置”，“还原配置”，“恢复出厂设置”功能，配置管理界面如图 5-7 所示。

图 5-7 配置管理界面

备份配置

配置备份功能，可以实现将本机的配置下载到电脑，用于恢复配置或者导入到其他设备中。

步骤 1：在导航栏中选择【维护】→【文件管理】，进入文件管理页面，点击“配置管理”。

步骤 2：单击【备份配置】按钮，弹出“文件下载”对话框，将配置文件保存到本地。

还原配置

配置恢复功能，可以实现将配置文件快速导入到本机中。

步骤 1：在导航栏中选择【维护】→【文件管理】，进入文件管理页面，点击“配置管理”。

步骤 2：单击【还原配置】按钮，选择需要导入的配置文件，导入完成后设备会自动重启。

恢复出厂设置

恢复出厂配置模块提供将设备中的所有配置恢复到出厂时的缺省配置，删除当前的配置文件，并重新启动设备的功能。

步骤 1：在导航栏中选择【维护】→【文件管理】，进入文件管理页面，点击“配置管理”。

步骤 2：单击【恢复出厂配置】按钮，点击【确定】按钮，设备会自动重启。

步骤 3：等待设备重启完成，设备重启完成后使用默认 IP、用户名和密码登录。

5.2.4 证书管理

开启 HTTPS 时，需要上传证书及私钥，如图 5-8 所示。不指定证书情况下，设备将使用默认的证书。

图 5-8 证书管理界面

5.2.5 页面包管理

页面包管理模块提供了从本地主机上获取目标页面包文件，并应用该文件作为设备页面包文件的功能，如图 5-9 所示。

图 5-9 页面包管理

5.3 用户管理

注意

- 为提高设备安全，请尽快更改密码，更改后的密码请务必保存，忘记密码会导致无法登录设备。

点击导航栏【维护】→【用户管理】，进入用户管理界面，如图 5-10 界面所示。

图 5-10 用户管理界面

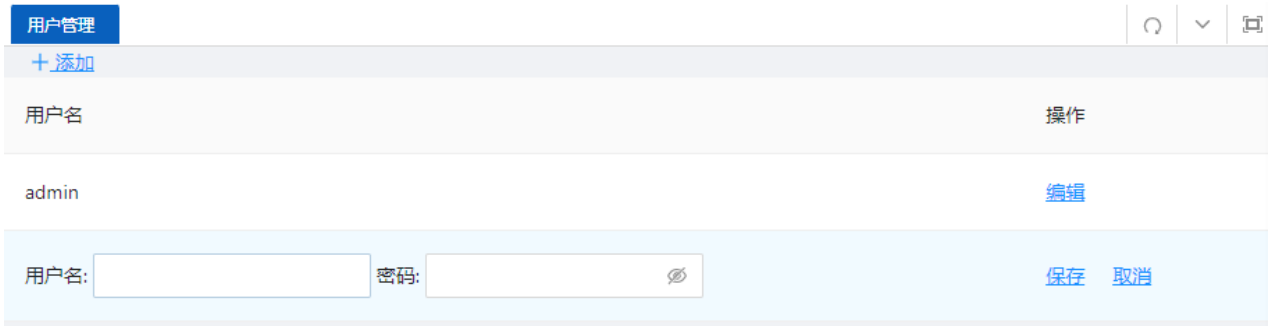
添加账号步骤：

步骤 1：点击导航栏中【维护】→【用户管理】，进入用户管理界面。

步骤 2：点击【添加】按钮，进入添加账号界面，如图 5-11 所示。

首次登录设备后，请尽快修改密码，根据提示重复两次输入新密码，如图 5-13 所示。密码由数字和字母组成，密码长度为 0-32 字节，字母区分大小写。

图 5-11 添加账号界面



步骤 3：点击【保存】按钮，完成配置，界面自动返回账号显示界面，如图 5-12 所示，可以看到新创建的账号。

图 5-11 添加账号界面

步骤 4：点击辅助区的【保存】按钮，保存配置。

5.4 时间管理

为了保证本设备与其它设备协调工作，用户需要将系统时间配置准确。日期和时间设置模块用于在 Web 网管上显示和设置系统时间，以及设置系统时区。设备支持手动配置系统时间和自动同步 NTP（Network Time Protocol，网络时间协议）服务器的时间。

NTP（Network Time Protocol，网络时间协议）是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。使用 NTP 的目的是对网络内所有具有时钟的设备进行时钟同步，使网

络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

5.5.1 查看系统当前的日期和时间

（1）在导航栏里选择【维护】→【时间管理】，进入日期和时间界面，如图 5-12 所示，参数说明如表格 5-2 所示。

（2）在页面上查看实时显示的系统当前日期和时间。

图 5-12 日期与时间配置界面

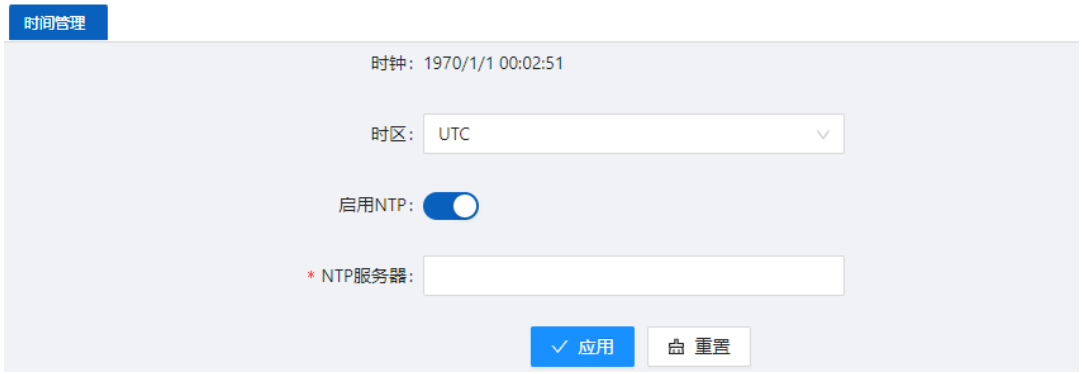


表 5-2 NTP 参数说明

配置项	说明
时区	选择时区
日期	系统日期
时间	系统时间
NTP 服务器 IP	NTP 服务器 IP 地址

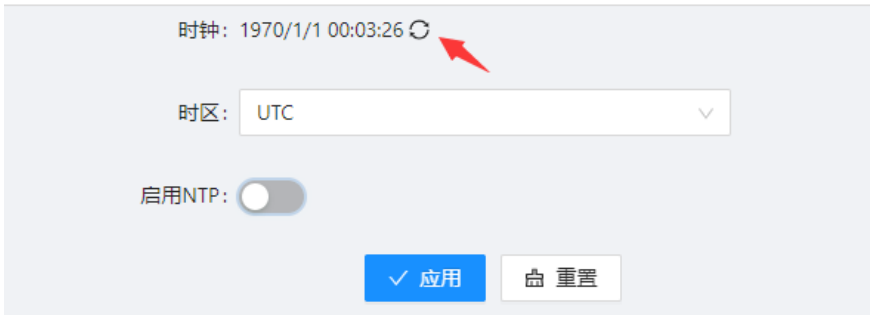
5.5.2 手动配置系统的日期和时间

（1）在导航栏里选择【维护】→【时间管理】，进入时间管理界面。

（2）点击时钟后面的同步按钮，再点击【应用】按钮，如图 5-13 所示，这样就实现了交换机时间和 PC 时间的同步。

（3）点击辅助区的【保存】按钮，保存当前配置。

图 5-13 日期与时间配置界面



说明

- 对于没有内置 RTC 的设备，设备重启后时间和日期会恢复成出厂设置，需要重新配置时间和日期。

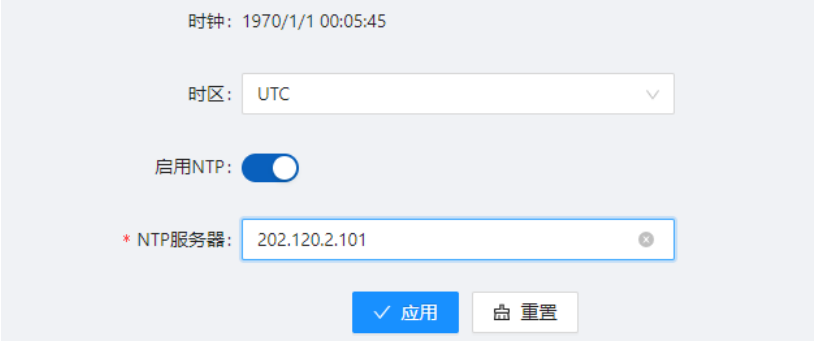
5.5.3 配置网络时间

（1）在导航栏里选择【维护】→【时间管理】，进入时间管理界面。

（2）在 NTP 服务器 IP 文本框里输入相应的服务器地址，点击【应用】完成配置，如图 5-14 所示。

（3）点击导航栏的【保存】按钮，保存当前配置。

图 5-14 日期与时间配置界面



说明

- 要求设备必须能访问 NTP 服务器。
- 在配置完成后，设备将自动从服务器同步时间信息，第一次完成时间同步大概耗时 4-8 分钟。
- 对于没有内置 RTC 的设备，设备重启后时间和日期会恢复成出厂设置，之前配置过 NTP 服务器的设备会自动同步网络时间。

5.5 SNMP

5.5.1 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。

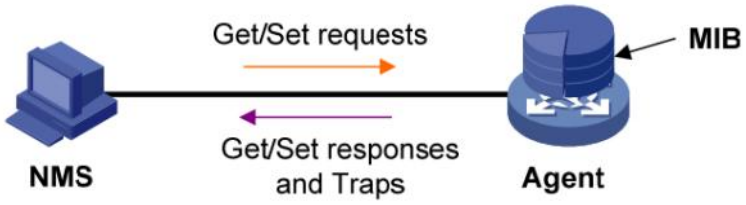
5.5.2 SNMP 的工作机制

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 之间的关系如图 5-15 所示。

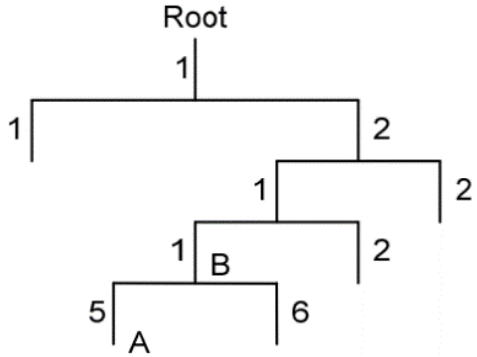
图 5-15 NMS、Agent 和 MIB 关系



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）。

如图 5-16 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 5-16 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。

5.5.3 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。

5.5.4 配置 SNMP

（1）在导航栏里选择【维护】→【SNMP】，进入 SNMP 配置界面。

（2）如图 5-17 所示，选择 SNMP 版本，配置用户、认证\加密密码，Trap 主机，点击【应用】按钮完成配置。

图 5-17 NMS、Agent 和 MIB 关系

6 诊断

6.1 网络工具

6.1.1 概述

Ping

通过使用 ping 工具，用户可以检查指定 IP 地址的设备是否可达，测试网络连接是否出现故障。

ping 的成功执行过程为：

(1) 源设备向目的设备发送 ICMP 回显请求（ ECHO-REQUEST）报文。

(2) 目的设备在接收到该请求报文后，向源设备发送 ICMP 回显应答（ ECHO-REPLY）报文。

(3) 源设备在收到该应答报文后，显示相关的统计信息。

ping 的输出信息分为以下几种情况：

• ping 的执行对象可以是目的设备的 IP 地址或者主机名，如果该目的设备的主机名不可识别，则源设备上输出提示信息。

• 如果在超时时间内源设备没有收到目的设备回的 ICMP 回显应答报文，则输出提示信息和 ping 过程报文的统计信息；如果在超时时间内源设备收到响应报文，则输出响应报文的字节数、报文序号、TTL（Time to Live，生存时间）、响应时间和 ping 过程报文的统计信息。ping 过程报文的统计信息包括发送报文个数、接收到响应报文个数、未响应报文数百分比、响应时间的最小值、平均值和最大值。

Trace route

通过使用 trace route 工具，用户可以查看报文从源设备传送到目的设备所经过的三层设备。当网络出现故障时，用户可以使用该命令分析出现故障的网络节点。trace route 的执行过程为：

(1) 源设备发送一个 TTL 为 1 的报文给目的设备。

(2) 第一跳（即该报文所到达的第一个三层设备）回应一个 TTL 超时的 ICMP 报文（该报文中含有第一跳的 IP 地址），这样源设备就得到了第一个三层设备的地址。

(3) 源设备重新发送一个 TTL 为 2 的报文给目的设备。

(4) 第二跳回应一个 TTL 超时的 ICMP 报文，这样源设备就得到了第二个三层设备的地址。

(5) 以上过程不断进行，直到最终到达目的设备，源设备就得到了从它到目的设备所经过的所有三层设备的地址。

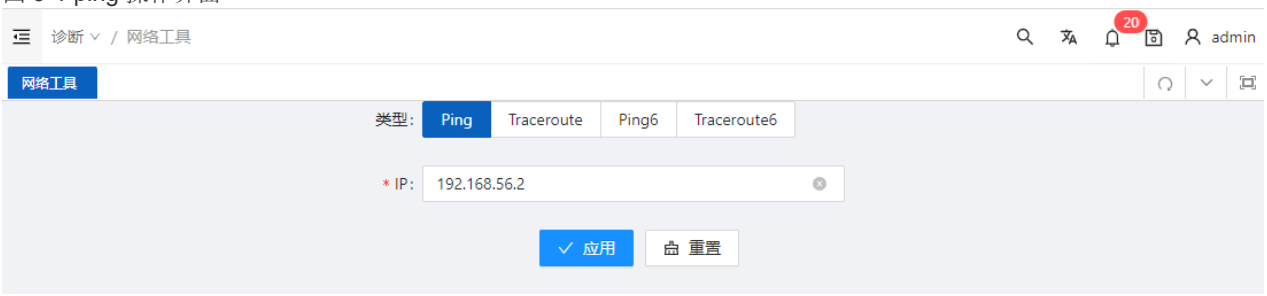
trace route 的执行对象可以是目的设备的 IP 地址或者主机名，如果该目的设备的主机名不可识别，则源设备上输出提示信息。

6.1.2 ping 和 trace route 操作

Ping 操作

（1）在导航栏中选择【诊断】→【网络工具】，进入 ping/trace route 页面，如图 6-1 所示。在 ping 操作 IP 地址栏输入需要 ping 的 IP 地址，点击【应用】按钮。

图 6-1 ping 操作界面



（2）在下方的信息框中查看 ping 操作的返回结果，如图 6-2 所示。

图 6-2 ping 操作返回结果

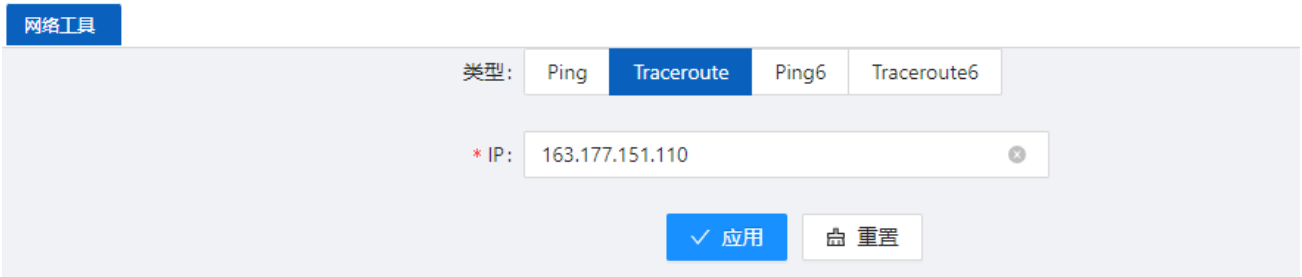
```
结果: PING 192.168.56.2 (192.168.56.2) 56(84) bytes
      of data.
      64 bytes from 192.168.56.2: icmp_req=1 ttl=64
      time=0.805 ms
      64 bytes from 192.168.56.2: icmp_req=2 ttl=64
      time=0.562 ms
      64 bytes from 192.168.56.2: icmp_req=3 ttl=64
      time=0.547 ms
      64 bytes from 192.168.56.2: icmp_req=4 ttl=64
      time=0.749 ms
      64 bytes from 192.168.56.2: icmp_req=5 ttl=64
      time=0.613 ms

      --- 192.168.56.2 ping statistics ---
      5 packets transmitted, 5 received, 0% packet
      loss, time 3996ms
      rtt min/avg/max/mdev = 0.547/0.655/0.805/0.104
      ms
```

Trace route 操作

（1）在导航栏中选择【诊断】→【网络工具】，进入 ping/trace route 页面，如图 6-3 所示。在 ping 操作 IP 地址栏输入需要 ping 的 IP 地址，点击【应用】按钮。

图 6-3 trace route 操作界面



（2）在下方的信息框中查看 ping 操作的返回结果，如图 6-4 所示。

图 6-4 trace route 操作返回结果

```
结果: traceroute to 163.177.151.110
      (163.177.151.110), 20 hops max, 60 byte
      packets
       1  192.168.1.1  0.598 ms
       2  100.69.0.1  3.784 ms
       3  218.104.224.29  3.628 ms
       4  218.104.229.66  16.026 ms
       5  218.104.229.37  24.969 ms
       6  *
       7  120.83.0.86  20.729 ms
       8  120.80.137.202  21.808 ms
```

6.2 光模块信息

在导航栏中选择【诊断】→【光模块信息】，进入光模块信息监控页面。如图 6-5 所示，可以查询光模块的数字诊断信息。

图 6-5 光模块数字诊断信息

光模块信息

名称	状态	收发器状态	温度(℃)	电压(伏)	电流(毫安)	接收功率(分贝毫瓦)	发送功率(分贝毫瓦)	操作
gigabitEthernet0/9	Down	OK	42(OK)	3.236(OK)	16.366(OK)	-40(ALARM)	-5.63(OK)	详细
gigabitEthernet0/10	Down	OK	32(OK)	3.2616(OK)	16.016(OK)	-40(ALARM)	-5.49(OK)	详细

点击【详细】按钮，可以查询光模块的供应商，序列号，生产日期等基本信息，如图 6-6 所示。

图 6-6 光模块基本信息

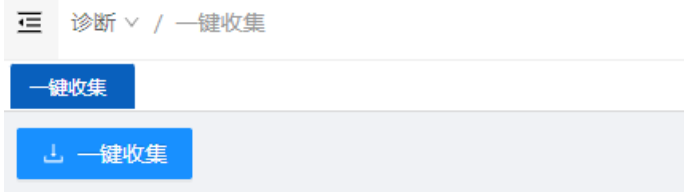
6.3 一键收集

因为各个功能模块都有其对应的运行信息，所以一般情况下，用户需要逐个模块查看显示信息。为了在日常维护或系统出现故障时能够一次性收集更多信息，设备支持诊断信息模块。用户执行生成诊断信息文件的操作时，系统会将当前多个功能模块运行的统计信息保存在一个名为“backup-SWITCH-year-mon-day-log”的文件中，用户可以通过查看该文件来更快的定位问题。

步骤 1：在导航栏中选择【诊断】→【一键收集】。

步骤 2：单击【一键收集】按钮，弹出“文件下载”对话框，将日志文件保存到本地。

图 6-7 光模块基本信息



6.4 掉电告警

6.4.1 概述

Dying-gasp 功能为断掉设备供电瞬间，依靠设备内部电容等储能器件供电 10-20ms 时间，支持设备发出掉电告警信息。

根据 802.3ah 中定义，当发生设备掉电事件后，设备向其连接设备发出 OAM 事件报文，由于 OAM 为点到点协议，掉电事件报文在送达到下一个支持 OAM 的设备后，不再继续转发。接收到掉电事件的设备将输出掉电 LOG 提示信息。

除 OAM 告警信息，掉电设备还将发出一条 trap 信息到 smmp 服务器。

节点信息	数据
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

6.4.2 配置掉电告警

在导航栏中选择【诊断】→【掉电告警】，进入 Dying Gasp 掉电告警页面，如图 6-8 所示，点击启用/禁用下的按钮来使能或关闭 Dying Gasp 功能，此功能默认情况下为关闭状态。

图 6-8 Dying Gasp 配置界面

6.5 线缆检测

说明

仅电口支持此命令

执行该操作会使得已经 Up 的端口自动 Down Up 一次

当线长小于 6 米时，测试结果与实际值存在偏差

线缆检测是指，用户可以检测设备上以太网接口连接电缆的当前状况，系统将在 5 秒内返回检测结果。检测内容包括线缆是否存在短路或开路现象以及故障线缆的长度。

步骤 1：在导航栏中选择【诊断】→【线缆检测】，进入线缆检测的页面，如图 6-9 所示。

步骤 2：选择要检测的接口，单击【检测】按钮开始进线检测，系统在 5 秒内返回检测结果。

步骤 3：如图 6-10 所示，在弹出的页面中查看检测结果。

图 6-9 线缆检测界面

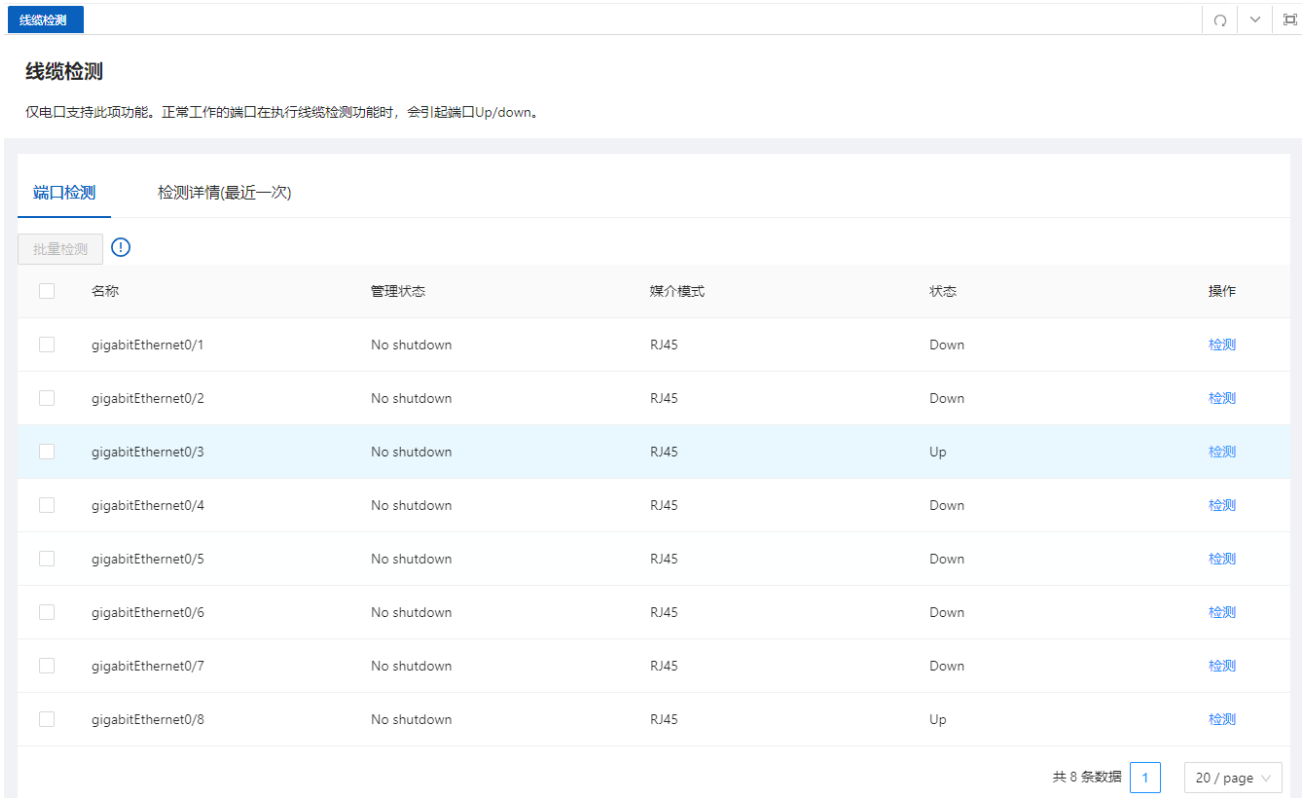


图 6-10 线缆检测结果

说明

Pair X 长度：单位米，电缆长度，有故障时为接口到故障位置的长度

Pair X 状态：

OK（正常）：表示线对（PAIR）正常终结

Open（开路）：表示线对开路

Short（短路）：表示线对短路

Unknown（未知）：其他未知故障原因