

Tenda

User Guide

Web 配置指南

三层网管型 PoE 交换机
TEG5328P-24-410W



本指南仅作为功能配置参考，不代表产品支持指南内全部功能。
不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

声明

版权所有©2024 深圳市吉祥腾达科技有限公司。保留一切权利。

未经本公司书面许可，任何单位或个人不得擅自复制、摘抄及翻译本档部分或全部内容，且不得以任何形式传播。

Tenda 是深圳市吉祥腾达科技有限公司在中国和（或）其它国家与地区的注册商标。文中提及的其它品牌和产品名称均为其相应持有人的商标或注册商标。

由于产品版本升级或其它原因，本档内容会不定期更新。除非另有约定，本档仅作为产品使用指导，文中的所有陈述、信息和建议均不构成任何形式的担保。

前言

感谢选择腾达产品。开始使用本产品前，请先认真阅读本指南并妥善保存以备日后参考。

约定

本指南适用于三层网管型 PoE 交换机 TEG5328P-24-410WV2.0。



文中使用的产品 Web 管理页面截图、IP 地址等数据信息均为举例说明，具体请以实际为准。

正文中，如无特别说明，三层网管型 PoE 交换机 TEG5328P-24-410WV2.0 软件版本以 V65.30.14.1 为例。

本文用到的格式说明如下。

项目	格式	举例
菜单项	「」	选择「状态」菜单。
连续菜单选项	>	进入「常用功能」>「管理维护」页面。
按钮	边框+底纹	点击  确定。
窗口	【】	在【新增】窗口。

本文用到的标识说明如下。

标识	含义
	表示重要信息或需要特别关注的信息。若忽略此等信息，可能导致配置失效、数据丢失或设备故障。
	表示对配置操作进行补充与说明。

更多服务与支持

若您在使用设备过程中遇到问题，或者您对我们有任何的意见或建议，均可以反馈给我们，我们会尽快为您解答。



Tenda 在线技术客服



邮箱: tenda@tenda.com.cn

若您想获取相关设备的更多资料（如 Web 配置指南、产品彩页等），请扫描“更多资料”二维码。



更多资料

（如 Web 配置指南）

若您需要咨询客服、查看安装视频、了解设备使用小技巧等，建议关注“Tenda 腾达”微信公众号。



Tenda 腾达

如需获取更多信息，请访问 Tenda 官网。



Tenda 官方网站

修订记录

文档版本	修订内容	发布日期
V1.0	首次发行。	2024-1-30

目录

1	登录 Web 管理页面	1
1.1	登录	1
1.2	退出登录	3
2	Web 页面简介	4
2.1	页面布局	4
2.2	常用元素	5
3	常用功能	6
3.1	系统概览	6
3.1.1	系统概念	6
3.1.2	一键助手	8
3.2	端口管理	10
3.2.1	基本设置	10
3.2.2	端口镜像	12
3.2.3	端口汇聚	13
3.2.4	端口限速	15
3.2.5	包统计	16
3.3	VLAN 划分	18
3.3.1	概述	18
3.3.2	配置 VLAN	19
3.3.3	802.1Q VLAN 配置举例	21
3.4	管理维护	24
3.4.1	升级软件	24
3.4.2	导入配置	25

3.4.3 备份配置.....	26
3.4.4 重启交换机.....	27
3.4.5 恢复出厂设置.....	28
3.5 用户管理.....	29
3.6 网络诊断.....	30
3.6.1 Ping 检测.....	30
3.6.2 Tracert 检测.....	31
4 交换设置.....	32
4.1 DHCP 中继.....	32
4.2 DHCP 侦听.....	35
4.2.1 概述.....	35
4.2.2 配置 DHCP 侦听.....	37
4.2.3 DHCP 侦听配置举例.....	38
4.3 生成树.....	41
4.3.1 概述.....	41
4.3.2 全局配置.....	49
4.3.3 端口设置.....	53
4.3.4 端口统计.....	54
4.3.5 实例信息.....	55
4.4 LLDP 设置.....	56
4.4.1 概述.....	56
4.4.2 全局设置.....	58
4.4.3 端口设置.....	59
4.4.4 邻居信息.....	60
4.5 LLDP-MED.....	61
4.5.1 概述.....	61
4.5.2 基本设置.....	62

4.5.3 TLV 设置	63
4.5.4 本地信息.....	64
4.5.5 邻居信息.....	65
4.6 IGMP 侦听.....	66
4.6.1 概述.....	66
4.6.2 全局设置.....	68
4.6.3 快速离开.....	70
4.6.4 IGMP 侦听配置举例.....	71
4.7 MAC 设置	77
4.7.1 MAC 地址表.....	77
4.7.2 静态 MAC 地址.....	78
5 路由设置.....	79
5.1 静态路由.....	79
5.1.1 概述.....	79
5.1.2 配置 IPv4 静态路由.....	79
5.1.3 配置 IPv6 静态路由.....	80
5.1.4 IPv4 静态路由配置举例.....	80
5.2 动态路由.....	84
5.2.1 概述.....	84
5.2.2 RIP 动态路由.....	85
5.3 路由表.....	87
5.3.1 查看 IPv4 路由表.....	87
5.3.2 查看 IPv6 路由表.....	88
5.4 ARP	89
5.5 DHCP 服务器.....	91
5.5.1 概述.....	91
5.5.2 DHCP 设置.....	92

5.5.3 静态地址分配	93
5.5.4 客户端列表	94
5.6 IPv6 设置	95
5.6.1 概述	95
5.6.2 IPv6 接口设置	97
5.6.3 IPv6 ND 设置	98
6 QoS 策略	99
6.1 概述	99
6.2 配置向导	105
6.3 QoS 调度	106
6.4 802.1P	107
6.5 DSCP	108
6.6 端口优先级	109
7 网络安全	110
7.1 ACL	110
7.1.1 概述	110
7.1.2 配置向导	110
7.1.3 MAC ACL	111
7.1.4 IP ACL	112
7.1.5 应用 ACL	113
7.1.6 ACL 配置举例	114
7.2 MAC 过滤	117
7.3 802.1X	118
7.3.1 概述	118
7.3.2 全局设置	119
7.3.3 端口设置	120
7.4 攻击防御	122
7.4.1 概述	122
7.4.2 防 ARP 攻击	122

7.4.3 防 DoS 攻击	124
7.4.4 防 MAC 地址攻击	126
8 设备管理	127
8.1 SNMP	127
8.1.1 概述	127
8.1.2 配置向导	129
8.1.3 基本设置	130
8.1.4 权限控制	131
8.1.5 通告	133
8.2 系统时间	134
8.3 日志管理	135
8.3.1 日志信息	135
8.3.2 服务器设置	136
8.4 时间段管理	137
8.5 RMON	138
8.5.1 概述	138
8.5.2 统计组	139
8.5.3 历史组	140
8.5.4 告警组	140
8.5.5 事件组	142
8.5.6 日志	143
9 可视化	144
9.1 全局地图	144
9.2 设备列表	148
10 PoE 管理	149
10.1 概述	149
10.2 全局设置	150

10.3 端口设置.....	151
附录.....	153
A 缩略语.....	153

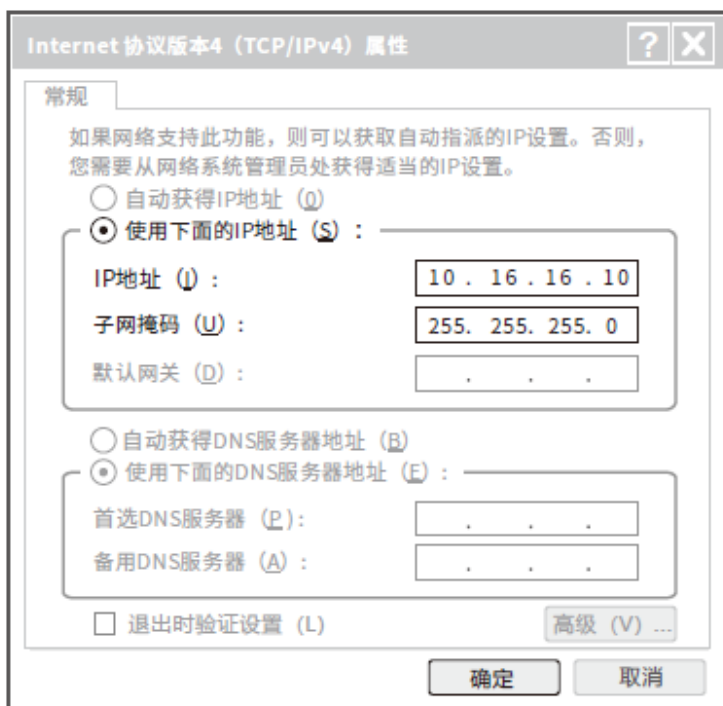
1 登录 Web 管理页面

1.1 登录

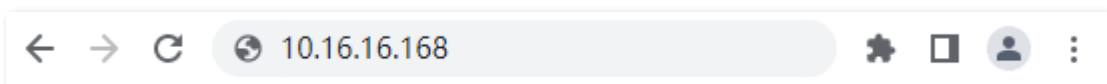
步骤 1 使用网线将电脑连接到交换机任一 RJ45 口。

步骤 2 设置电脑的以太网（或本地连接）IP 地址，使其与交换机的 IP 地址在同一网段。

交换机的默认 IP 地址为 10.16.16.168，因此电脑的 IP 地址可设为 10.16.16.X（X 为 2~254 除开 168，且未被局域网中其他设备占用），子网掩码为 255.255.255.0。



步骤 3 打开浏览器，在地址栏中输入交换机的管理 IP 地址（默认为 10.16.16.168），进入其管理页面。



步骤 4 输入登录用户名与密码（默认均为 admin），点击 **登录**。



 **提示**

若未出现上述页面，请尝试使用以下办法解决：

- 确保交换机已通电（电源灯长亮）。
- 确保电脑与交换机网线连接正常，网线无松动现象。
- 确保网线没有损坏，且网线长度符合要求。
- 确保电脑的 IP 地址和交换机的 IP 地址在同一网段。如果交换机的 IP 地址为 10.16.16.168，电脑 IP 地址应为 10.16.16.X（X 为 2~254 除开 168，且未被其它设备占用）。
- 确保网络中没有其他设备与交换机的 IP 地址一致。
- 清空浏览器的缓存或更换浏览器进行尝试。
- 若经过上述操作仍无法登录，请将交换机[恢复出厂设置](#)后重新尝试。

步骤 5 修改登录密码，点击 **确认**。

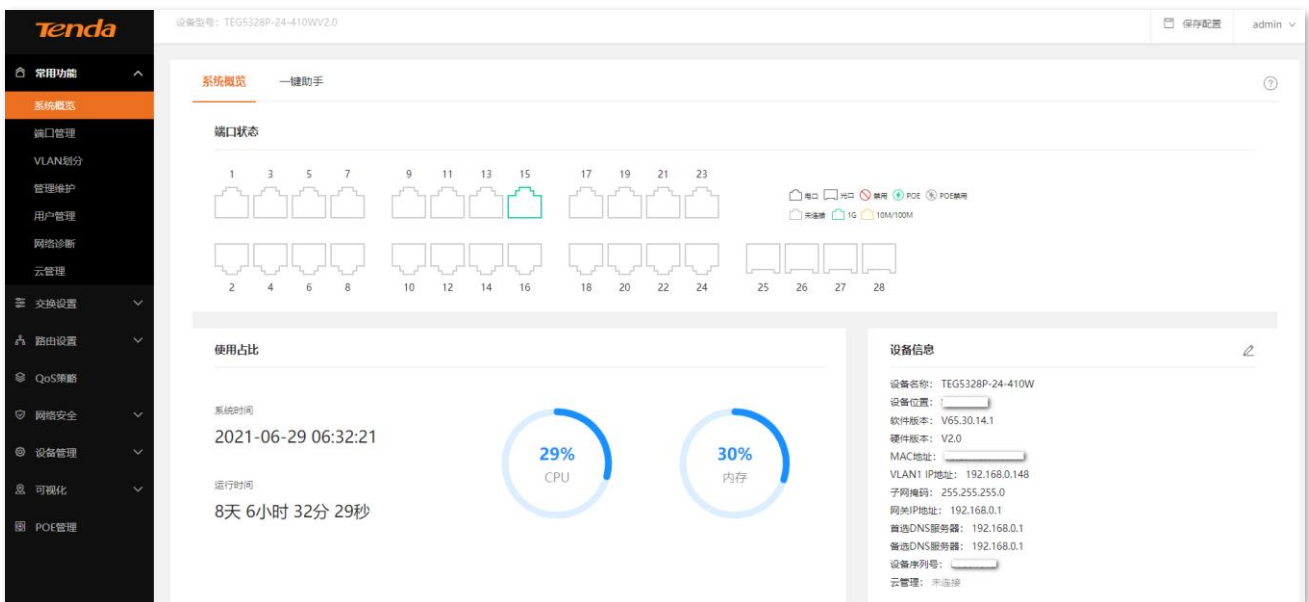


提示

- 您也可以在[用户管理](#)页面更改登录用户名与密码。
- 为确保网络安全，登录后请及时更改登录用户名。
- 建议您记录并保存修改后登录密码，以备后续忘记进行查阅。

---完成

成功登录到交换机的 Web 管理页面，您可以开始配置交换机。



1.2 退出登录

登录到交换机的管理页面后，如果在[超时时间](#)内没有任何操作，系统将自动退出登录。您也可以点击管理页面右上角的「admin」>「退出」，安全退出管理页面。

2 Web 页面简介

2.1 页面布局

交换机的管理页面共分为：一级导航栏、二级导航栏、页签和配置区四部分。如下图所示。













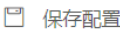
提示

管理页面上显示为灰色的功能或参数，表示路由器不支持或在当前配置下不可修改。

序号	名称	说明
1	一级导航栏	
2	二级导航栏	以导航树的形式组织路由器的功能菜单。用户在导航栏中可以方便地选择功能菜单，选择结果显示在配置区。
3	页签	
4	配置区	用户进行配置或查看配置的区域。

2.2 常用元素

交换机管理页面中常用元素的功能介绍如下表。

常用元素	说明
	用于刷新当前页面内容。
	用于批量配置当前页面的规则参数。
	用于保存当前页面配置，并使配置生效。
	配置信息更改后，仅点击  ，交换机重启后会丢失更改的配置信息。
	用于取消当前页面未保存的配置，并恢复到修改前的配置。
	用于查看当前页面功能的帮助信息。
	用于在当前页面中添加规则。
	用于删除当前页面中的规则。
	用于编辑对应规则。
	用于保存所有页面配置，并使配置生效。交换机重启后，配置信息不会丢失。

3 常用功能

3.1 系统概览

3.1.1 系统概念

在「常用功能」>「系统概览」>「系统概览」页面中，您可以查看各端口连接状态、CPU 和内存使用率、系统时间与设备信息。



参数说明


标题项	说明	
端口状态	<p>交换机各端口连接状态。</p> <ul style="list-style-type: none"> / ：表示端口已连接设备，对应端口速率可参考页面“端口状态”模块右侧的端口状态图标说明。：表示端口未连接设备。：表示端口已禁用。：表示端口正在给 PoE 受电设备供电。：表示端口已禁用 PoE 供电功能。	
使用占比	交换机的 CPU 使用率和内存使用率。	
系统时间	交换机的系统时间。	
运行时间	交换机最近一次启动后连续运行的时长。	
设备信息	设备名称	交换机的设备名称，可以点击  进行修改。
	设备位置	交换机的设备位置，可以点击  进行修改。
	软件版本	交换机的系统软件版本号。
	硬件版本	交换机的硬件版本号。
	MAC 地址	交换机的 MAC 地址。
	IP 获取方式	交换机 IP 地址的获取方式，可点击  修改为手动分配或自动获取。
VLAN1 IP 地址	<p>交换机管理 VLAN 的 IP 地址。IP 获取方式设置为手动分配时可修改。</p> <p>只有连接到管理 VLAN 成员端口的电脑可以使用该 IP 地址登录到交换机的 Web 管理页面。</p> <p> 提示</p> <p>除了此处显示的管理 IP 地址可以登录到交换机的 Web 管理页面，还可以使用 10.16.16.168（默认 IP 地址，固定不变）登录到交换机的 Web 管理页面。</p>	
子网掩码	交换机管理 VLAN 的子网掩码。IP 获取方式设置为手动分配时可修改。	

标题项	说明
网关 IP 地址	交换机管理 VLAN 的网关地址。
DNS 分配方式	交换机的首/备选 DNS 服务器地址的分配方式，可点击  修改为手动分配或自动获取。
首选 DNS 服务器	交换机的首/备选 DNS 服务器地址。
备选 DNS 服务器	默认为从上级自动获取。DNS 分配方式设置为手动分配时可修改。
设备序列号	交换机的设备序列号。


3.1.2 一键助手

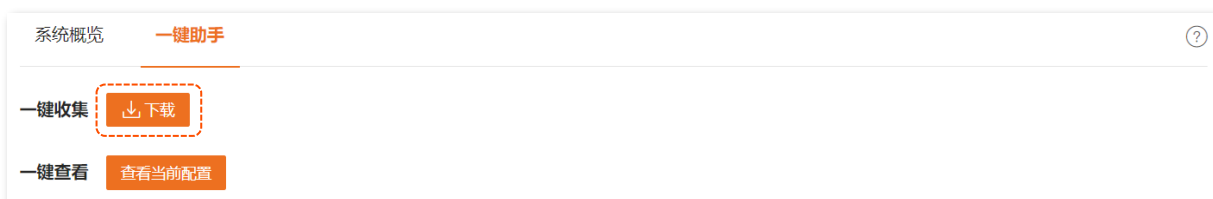
一键收集

通过一键收集功能，可以一键收集交换机的当前所有配置、系统信息、端口信息、LLDP 邻居信息、生成树摘要信息、MAC 地址表、ARP 表、所有日志，方便运维人员排查分析问题。

操作方法：在「常用功能」>「系统概览」>「一键助手」页面中，点击 ，浏览器将下载名称为 diagnosis 的压缩包文件。将文件解压缩，可集中查看交换机当前所有配置、日志等信息来排查分析问题。




一键收集前，请先点击页面右上角的  进行全局保存。



一键查看

通过一键查看功能，可以一键查看交换机的端口配置、VLAN 配置、生成树配置、DHCP 服务器配置和静态路由配置，方便快速了解交换机的基本配置。

操作方法：在「常用功能」>「系统概览」>「一键助手」页面中，点击 ，页面将显示交换机基本配置信息。点击 [端口配置](#)、[VLAN 配置](#)、[生成树配置](#)、[DHCP 服务器配置](#) 或 [静态路由配置](#) 可跳转到相应的配置页面。

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。

不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

系统概览 **一键助手** ?

一键收集 [↓ 下载](#)

一键查看 [查看当前配置](#)



一键收集 [↓ 下载](#)

一键查看 [查看当前配置](#)

端口配置

端口	端口状态	速率/双工	PoE状态	DHCP 侦听	入口流控	出口流控	入口流量	出口流量	端口隔离	链路类型	所属VLAN
1	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
2	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
3	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
4	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
5	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
6	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
7	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1
8	未连接	自动协商 1000M/FDX	0.00W	--	关闭	关闭	0.0MB	0.0MB	关闭	Access	PVID:1 T:-- U:1

共 28 条数据

VLAN配置

VLAN ID	三层接口	IP地址	子网掩码
1	开启	192.168.0.148	255.255.255.0

共 1 条数据

生成树配置
生成树状态 关闭

DHCP服务器配置
DHCP服务器状态 关闭

静态路由配置

目的IP	子网掩码	下一跳
0.0.0.0	0.0.0.0	192.168.0.1

3.2 端口管理

3.2.1 基本设置

在「常用功能」>「端口管理」>「基本设置」页面中，您可以查看和设置端口的基本参数。



端口	端口状态	速率/双工	端口隔离	入口流控	出口流控	入口流量	出口流量	操作
1	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
2	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
3	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
4	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
5	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
6	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
7	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
8	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎
9	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	30.4MB	27.6MB	✎
10	未连接	自动协商 1000M/FDX	关闭	关闭	关闭	0.0MB	0.0MB	✎

参数说明

标题项	说明
端口	端口编号。
端口状态	端口当前的连接状态，有已连接、未连接和禁用三种状态。
速率/双工 (速率/模式)	端口配置的连接速率与双工模式。 <ul style="list-style-type: none">- 自动协商：表示速率与双工模式自适应。- 强制模式：表示速率与双工模式固定，不与对端设备协商。- HDX：表示半双工模式。- FDX：表示全双工模式。

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。

不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

标题项	说明
端口隔离	端口所属隔离组。 相同隔离组的端口之间不可通讯，不同隔离组的端口之间可以通讯；未划到隔离组的端口显示为“关闭”状态，可以与所有端口相互通讯。
入口流控	开启后，将对本端口的入口流量进行监控，当本端口拥塞时给对端设备发送 pause 帧，使对端设备端口暂停或减慢报文发送速率，避免接收报文的丢失。
出口流控	开启后，当本端口接收到对端设备拥塞发送的 pause 帧时，本端口暂停或减慢报文发送速率，避免对端设备丢弃报文。
入口流量	统计端口已接收的数据流量。
出口流量	统计端口已发送的数据流量。

3.2.2 端口镜像

端口镜像是将交换机一个或多个端口（镜像源端口）的数据复制到指定的端口（镜像目的端口）。镜像目的端口一般接有数据监测设备，便于您进行流量监控、性能分析和故障诊断。

在「常用功能」>「端口管理」>「端口镜像」页面中，您可以配置端口镜像规则。

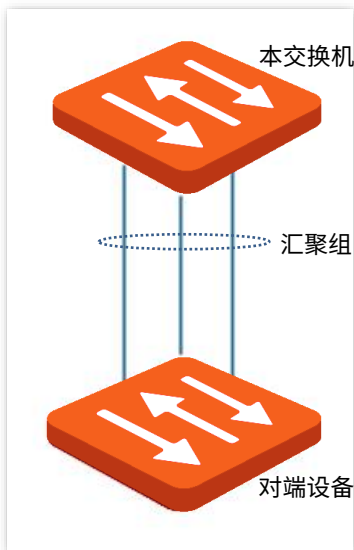


参数说明

标题项	说明
序号	镜像组编号。
镜像组类型	本交换机只支持本地镜像组类型。
镜像源端口	被镜像的端口，可选择多个端口。
镜像目的端口 (目的端口)	镜像源端口的数据包会复制到该端口。1 个镜像组内只可选择 1 个镜像目的端口。
镜像方向	镜像数据包的类型。 <ul style="list-style-type: none">- 入方向：将镜像源端口接收的数据包复制到镜像目的端口。- 出方向：将镜像源端口发送的数据包复制到镜像目的端口。- 双向：将镜像源端口接收和发送的数据包都复制到镜像目的端口。

3.2.3 端口汇聚

端口汇聚是将交换机的多个物理端口汇聚在一起形成一个逻辑上的汇聚组，同一汇聚组内的多条物理链路视为一条逻辑链路。端口汇聚将几条物理链路捆绑在一起，实现流量在汇聚组中各个成员端口之间分担，以增加交换机与对端设备之间的网络带宽；同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。端口汇聚的组网拓扑图如下：



注意

- 同一个汇聚组中各端口的配置必须保持一致，基本配置主要包括 STP、QoS、VLAN、端口属性等相关配置。
- 已被镜像的端口无法添加到汇聚组。

在「常用功能」>「端口管理」>「端口汇聚」页面中，您可以配置端口汇聚规则。



参数说明

标题项	说明
汇聚组	汇聚组编号。 汇聚模式为“静态聚合”时，汇聚组编号取值范围为 1~8。汇聚模式为“动态聚合”时，汇聚组编号取值范围为 9~16。

标题项	说明
汇聚模式	<p>包括静态聚合或动态聚合。</p> <ul style="list-style-type: none">- 静态汇聚：汇聚组中的所有成员端口聚合成一个逻辑端口。- 动态聚合：开启汇聚组中所有成员端口的 LACP 协议，实际形成汇聚的端口须与对端的设备通过 LACP 协议确定。
	<p> 注意</p> <p>汇聚模式需要与对端设备相同，否则会出现端口数据转发异常或形成环路。</p>
汇聚算法	<p>该汇聚组选路算法：</p> <ul style="list-style-type: none">- src-dst-mac：汇聚组中各成员端口根据接收数据包中的源 MAC 地址、目的 MAC 地址进行负荷分担。- src-dst-ip：汇聚组中各成员端口根据接收数据包中的源 IP 地址、目的 IP 地址进行负荷分担。- src-dst-mac-ip-port：汇聚组中各成员端口根据接收数据包中的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、TCP/UDP 源端口号、TCP/UDP 目的端口号进行负荷分担。
成员端口	<p>汇聚组的端口成员。</p> <ul style="list-style-type: none">- 静态聚合模式下，成员端口即为汇聚组成员。- 动态聚合模式下，成员端口为开启 LACP 协议的端口，实际形成汇聚的端口须与对端设备通过 LACP 协议确定。

3.2.4 端口限速

在「常用功能」>「端口管理」>「端口限速」页面中，您可以限定端口的出口速率，还可以抑制端口接收广播、组播及未知单播报文的速率。

端口	出口速率 (Mbps)	广播包抑制	组播包抑制	未知单播抑制	抑制值	操作
1	--	关闭	关闭	关闭	100	
2	--	关闭	关闭	关闭	100	
3	--	关闭	关闭	关闭	100	
4	--	关闭	关闭	关闭	100	
5	--	关闭	关闭	关闭	100	
6	--	关闭	关闭	关闭	100	
7	--	关闭	关闭	关闭	100	
8	--	关闭	关闭	关闭	100	
9	--	关闭	关闭	关闭	100	
10	--	关闭	关闭	关闭	100	

参数说明

标题项	说明
端口	端口编号。
出口速率	端口最大的发送速率，"--"表示不限速。
广播包抑制	开启或关闭广播报文抑制功能。
组播包抑制	开启或关闭组播报文抑制功能。
未知单播抑制 (未知包抑制)	开启或关闭未知单播报文抑制功能。
抑制值	在抑制功能开启状态下，端口每秒允许通过的最大广播、组播和未知单播报文总流量。广播、组播和未知单播总流量超过该抑制值后，系统将丢弃超出广播、组播和未知单播总流量限制的报文，从而使端口广播、组播和未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

3.2.5 包统计

在「常用功能」>「端口管理」>「包统计」页面中，您可以查看和清理各端口接收和发送的数据包信息。

基本设置	端口镜像	端口汇聚	端口限速	包统计	?
清除 刷新					
端口	发送数据包	发送字节数	接收数据包	接收字节数	操作
1	0	0	0	0	🗑️
2	0	0	0	0	🗑️
3	0	0	0	0	🗑️
4	0	0	0	0	🗑️
5	0	0	0	0	🗑️
6	0	0	0	0	🗑️
7	0	0	0	0	🗑️
8	0	0	0	0	🗑️
9	227297	28890799	196224	31832976	🗑️
10	0	0	0	0	🗑️


参数说明

标题项	说明
端口	端口编号。
发送数据包	端口发送的数据包总数。
发送字节数	端口发送的字节总数。
接收数据包	端口接收的数据包总数。
接收字节数	端口接收的字节总数。

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。

不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

如需查看某一端口接收和发送的数据包详细信息，请点击该端口后的  按钮，进行查看。

查看包统计		×
端口	5	
接收统计		
总字节数	21110010	
广播包(个)	2512	
单播包(个)	148081	
错误包(个)	0	
丢弃包(个)	0	
发送统计		
总字节数	116861427	
广播包(个)	34669	
单播包(个)	0	
错误包(个)	0	
丢弃包(个)	0	

参数说明

标题项	说明
总字节数	端口接收/发送的字节总数。
广播包	端口接收/发送的广播包个数。
单播包	端口接收/发送的单播包个数。
错误包	端口接收/发送的错误包个数。
丢弃包	端口接收/发送时丢弃的数据包个数。

3.3 VLAN 划分

3.3.1 概述

VLAN (Virtual Local Area Network, 虚拟局域网), 是一种将局域网内的设备在逻辑上而不是在物理上划分成不同网段, 从而实现虚拟工作组的技术。VLAN 的用途是将局域网交换机构成的网络中的工作站作逻辑分组, 分组间隔绝广播。组内工作站位于同一个 VLAN, 不管地理位置都可以像连接在同一个网段上一样正常通讯, 由于广播包隔绝, VLAN 间不能直接通信, 必须通过路由器或其它三层包转发设备转发。

通过 802.1Q VLAN 功能, 交换机可以与支持 802.1Q VLAN 的设备 VLAN 互通。

802.1Q VLAN 由 IEEE 802.1q 协议定义, 通过识别报文中的 Tag 标记来对报文进行处理。802.1Q VLAN 端口类型有以下三种:

- Access 类型: 端口只能属于 1 个 VLAN, 一般用于连接计算机的端口。
- Trunk 类型: 端口可以允许多个 VLAN 通过, 可以接收和发送多个 VLAN 的报文, 一般用于交换机之间连接的端口。
- Hybrid 类型: 端口可以允许多个 VLAN 通过, 可以接收和发送多个 VLAN 的报文, 可以用于交换机之间连接, 也可以用于连接计算机。

各端口对数据包的处理方式如下表所示:

类型	接收 Tag 数据	接收 Untag 数据	发送数据
Access 端口			删除报文的 Tag 再发送
Trunk 端口	按 Tag 中的 VID 转发到相应 VLAN 的其他端口	按该端口的 PVID 转发到相应 VLAN 的其他端口	若报文的 VID 值与 PVID 值相同, 拆除 Tag 发送; 反之保留 Tag 发送
Hybrid 端口			若报文的 VID 值属于 Tagged VLAN, 则带 Tag 发送 若报文的 VID 值属于 Untagged VLAN, 则拆除 Tag 发送

3.3.2 配置 VLAN

配置 802.1Q VLAN 规则

为保证出厂状态下的交换机能够正常通信，系统默认创建了一条 VLAN 规则。所有端口默认属于该 VLAN 的成员，VLAN ID 为 1。该规则不可删除。

在「常用功能」>「VLAN 划分」>「802.1Q VLAN」页面中，您可以配置 802.1Q VLAN 规则。

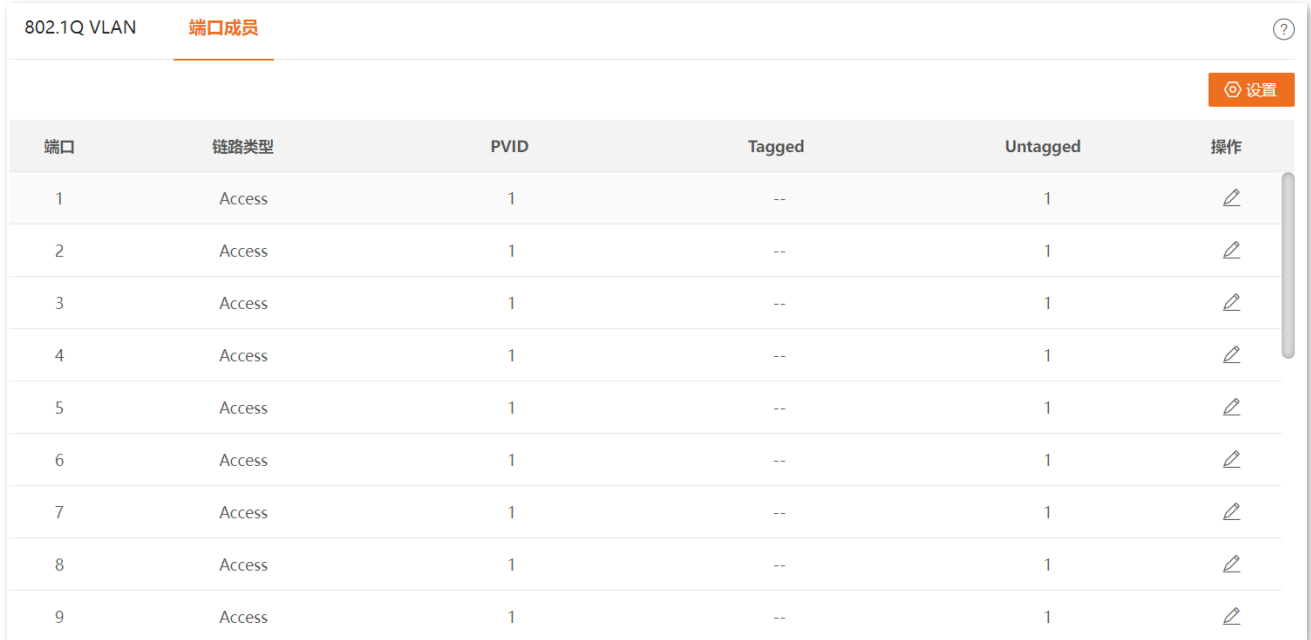
802.1Q VLAN		端口成员			?
					+ 添加
					🗑️
<input type="checkbox"/>	VLAN ID	VLAN描述	IPv4地址	子网掩码	操作
<input type="checkbox"/>	1	default	192.168.0.148	255.255.255.0	✎

参数说明

标题项	说明
VLAN ID	VLAN ID 号，用来标识数据包所属 VLAN。VLAN ID 为“1”的为管理 VLAN。
VLAN 描述	对 VLAN 组进行标识。如未设置，默认为“VLAN+四位 VLAN ID”，例如 VLAN ID 为 3 时，VLAN 描述为 VLAN0003。
三层虚接口	开启三层虚接口后，可以为 VLAN 接口配置 IP 地址和子网掩码。 配置 VLAN 接口 IP 地址信息后，可以通过静态路由实现 VLAN 之间的通信。
IP 获取方式	管理 VLAN 的 IP 地址获取方式。三层虚接口开启才能进行设置。 <ul style="list-style-type: none"> - 手动分配：手动配置管理 VLAN 的 IP 地址与子网掩码。 - DHCP 自动获取：自动获取 DHCP 服务器下发的 IP 地址信息。
	<div style="display: flex; align-items: center;"> 提示 </div> 选择 IP 地址获取方式为自动获取时，需确保管理 VLAN 中有连接 DHCP 服务器。
IPv4 地址/掩码	VLAN 接口的 IP 地址。VLAN 组内端口连接的设备可使用该 IP 地址登录交换机 Web 管理页面。
子网掩码	VLAN 接口的子网掩码。

配置端口成员

在「常用功能」>「VLAN 划分」>「端口成员」>页面中，您可以通过配置交换机各端口的 PVID 和 Tag 处理策略来实现 VLAN 隔离效果。



端口	链路类型	PVID	Tagged	Untagged	操作
1	Access	1	--	1	
2	Access	1	--	1	
3	Access	1	--	1	
4	Access	1	--	1	
5	Access	1	--	1	
6	Access	1	--	1	
7	Access	1	--	1	
8	Access	1	--	1	
9	Access	1	--	1	

参数说明

标题项	说明
端口	端口编号。
链路类型	可配置 Access、Trunk、Hybrid 三种链路类型。 <ul style="list-style-type: none">- Access：只属于一个 VLAN，且发送报文为 Untag，一般用于连接用户终端设备（如计算机）。- Trunk：允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，常用于交换机之间级联的端口。- Hybrid：允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可用于交换机之间级联，也可连接用户终端设备。
PVID	端口默认所属 VLAN ID。 端口接收到 Untag 的数据包时，根据该端口的 PVID 转发到相应的 VLAN。
Tagged	端口接收 Tag 数据包的 VID 与 Tagged 的 VLAN 相同时，保留数据包的 Tag 并发送该数据包。

标题项	说明
Untagged	端口接收 Tag 数据包的 VID 与 Untagged 的 VLAN 相同时，去掉数据包的 Tag 并发送该数据包。

3.3.3 802.1Q VLAN 配置举例

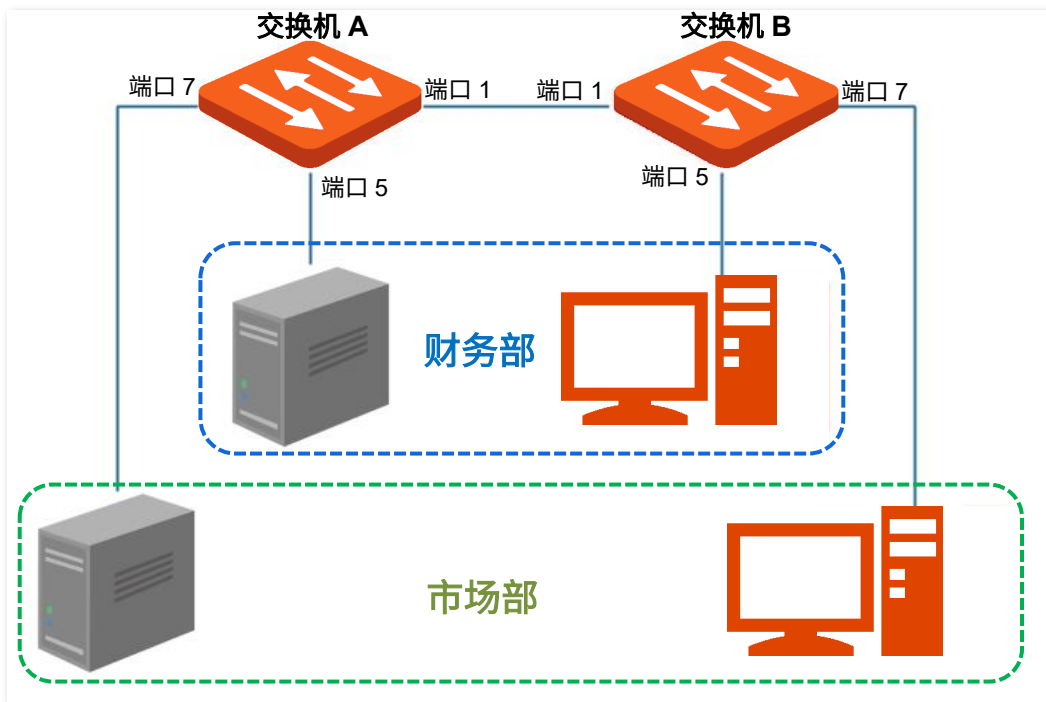
组网需求

某公司财务部和市场部的工作人员在二楼办公，财务部和市场部的服务器在三楼。现要实现各部门内部能互相通信并访问其服务器，部门之间不能互相通信。

方案设计

在两台交换机上设置 802.1Q VLAN：

- 在交换机上添加两个 VLAN，将连接财务部设备的端口添加到 VLAN5，连接到市场部设备的端口添加到 VLAN7。
- 连接两个交换机的端口同时添加到 VLAN5 和 VLAN7。



配置步骤

一、设置交换机 A

步骤 1 [登录交换机 A 的 Web 管理页面](#)。

步骤 2 添加 VLAN。

1. 点击「常用功能」>「VLAN 划分」>「802.1Q VLAN」。
2. 点击 **+ 添加**，在弹出的窗口中输入如下参数后点击 **确定**。
 - “VLAN ID”为“5”。
 - “VLAN 描述”为“财务部”。
3. 重复 2，设置一条“VLAN ID”为“7”，“VLAN 描述”为“市场部”的 VLAN 规则。



<input type="checkbox"/>	VLAN ID	VLAN描述	IPv4地址	子网掩码	操作
<input type="checkbox"/>	1	default	192.168.0.148	255.255.255.0	
<input type="checkbox"/>	5	财务部	--	--	
<input type="checkbox"/>	7	市场部	--	--	

步骤 3 配置端口属性。

1. 点击「常用功能」>「VLAN 划分」>「端口成员」。
2. 点击端口 5 后面的 按钮，设置“PVID”为“5”。
3. 点击端口 7 后面的 按钮，设置“PVID”为“7”。
4. 点击端口 1 后面的 按钮，设置“链路类型”为“Trunk”，“Tagged”为“5,7”。

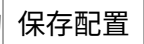


端口	链路类型	PVID	Tagged	Untagged	操作
1	Trunk	1	5,7	1	
2	Access	1	--	1	
3	Access	1	--	1	
4	Access	1	--	1	
5	Access	5	--	5	
6	Access	1	--	1	
7	Access	7	--	7	

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。
不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

步骤 4 保存配置。

点击管理页面右上角的  进行全局保存。

二、设置交换机 B

登录到交换机 B 的 Web 界面进行设置。交换机 B 的设置步骤与交换机 A 的设置步骤相同，这里就不再赘述。

---完成

验证配置

员工能访问本部门服务器，不能访问其他部门服务器；本部员工之间可以通信；市场部员工和财务部员工不能通信。

3.4 管理维护

3.4.1 升级软件

在「常用功能」>「管理维护」页面中，您可以点击 **升级** 对交换机进行软件升级。升级后您将体验更多功能，获得更好的用户体验。



为了避免交换机损坏，确保升级正确：

- 在升级之前，请务必确认新的软件是从 Tenda 官方网站 www.tenda.com.cn 下载的，且适用于此交换机。一般情况，升级文件后缀为.bin。
- 升级过程中，请确保交换机的供电正常。



3.4.2 导入配置

在「常用功能」>「管理维护」页面中，您可以点击 **导入**，将之前备份的配置文件导入到交换机，使交换机恢复到当时的配置状态。



交换机不校验配置文件的内容，导入前请确保文件的正确性。



3.4.3 备份配置

当您对交换机进行了大量的配置，使其在运行时较好的状态和性能，或更符合当前环境的需求，此时建议对交换机的配置进行备份；当您对交换机进行升级，恢复出厂设置等操作后，可以使用该配置文件将交换机恢复到原来的配置状态。

在「常用功能」>「管理维护」页面中，您可以选择将交换机的配置信息备份到本地电脑。



提示

备份配置前，请先点击页面右上角的 **保存配置** 进行全局保存。

本地备份

点击 **本地备份**，浏览器将下载文件名为 switch.cfg 的配置文件并保存到本地电脑。



提示

如果浏览器提示如“此类型的文件可能损害您的计算机”的安全提醒时，请选择“保留”文件即可。

3.4.4 重启交换机

当您设置的某项参数不能正常生效时，可以尝试重启交换机解决。

在「常用功能」>「管理维护」页面中，您可以点击 **重启** 按钮重启交换机。



重启前，先点击管理页面右上角的 **保存配置** 进行全局保存，以免配置信息丢失。



3.4.5 恢复出厂设置

当交换机出现无法定位的问题，或您忘记了登录交换机管理页面的密码时，可以将交换机恢复出厂设置，然后使用默认用户名与密码（均为 admin）登录。您可以通过[软件复位](#)或[硬件复位](#)方式将交换机恢复出厂设置。

软件复位

在「常用功能」>「管理维护」页面中，您可以点击 **恢复** 将交换机恢复到出厂状态，所有配置信息将被清除。



恢复过程中，请确保交换机的供电正常。



硬件复位

在 SYS 指示灯闪烁时，按住复位按钮（LED Mode）约 10 秒，待所有指示灯长亮时松开。SYS 指示灯重新闪烁时，交换机恢复出厂设置完成。

3.5 用户管理

您可以参考以下对用户类型的权限说明，为不同类型的用户分配不同的访问权限，来减少交换机配置被篡改的风险。

■ 管理员

超级管理员，有且只有一个，由系统默认创建，可以进行所有功能的操作。默认用户名与密码均为“admin”。

■ 操作用户

普通操作用户，可以进行除软件升级、恢复出厂设置、管理用户以外的所有操作。

■ 普通用户

普通查询用户，只能进行交换机配置查询。

在「常用功能」>「用户管理」页面中，您可以配置交换机的用户。最多可以配置 8 个用户。

用户	用户类型	超时时间	操作
admin	管理员	300s	

参数说明

标题项	说明
用户	用户名。
用户类型	用户的账户类型。有管理员、操作用户和普通用户三种用户类型。
超时时间	Web 闲置超时时间。在该时间范围内，如果用户没有在 Web 页面进行任何操作，系统将自动退出登录。

3.6 网络诊断

在「常用功能」>「网络诊断」页面，您可以进行 Ping/Tracert 检测。

- Ping：用于检测网络的连通性和连通质量。
- Tracert：用于检测数据包从交换机到目标主机所经过的路由。

3.6.1 Ping 检测

在「常用功能」>「网络诊断」>「Ping 检测」页面中，您可以进行网络的连通性检查。

The screenshot shows the 'Ping检测' configuration page. It has two tabs: 'Ping检测' and 'Tracert检测'. The 'Ping检测' tab is active. Below the tabs, there are three input fields: '目标IP地址' (Target IP address) with a placeholder '(输入IP地址或域名)', '发送次数' (Number of sends) set to 5 with a range of 1-100, and '发送报文长度' (Packet length) set to 64 with a range of 18-512. A '开始检测' (Start detection) button is located below the input fields.

参数说明

标题项	说明
目标 IP 地址	Ping 检测的目标设备的 IP 地址或域名。
发送次数	发送 Ping 包的个数。
发送报文长度	Ping 包的大小。

3.6.2 Tracert 检测

在「常用功能」>「网络诊断」>「Tracert 检测」页面中，您可以检测交换机到目标设备所需经过的路由。

Ping检测 **Tracert检测**

目标IP地址 (输入IP地址或域名)

最大跳数 次 (范围: 1-30)

开始检测

参数说明

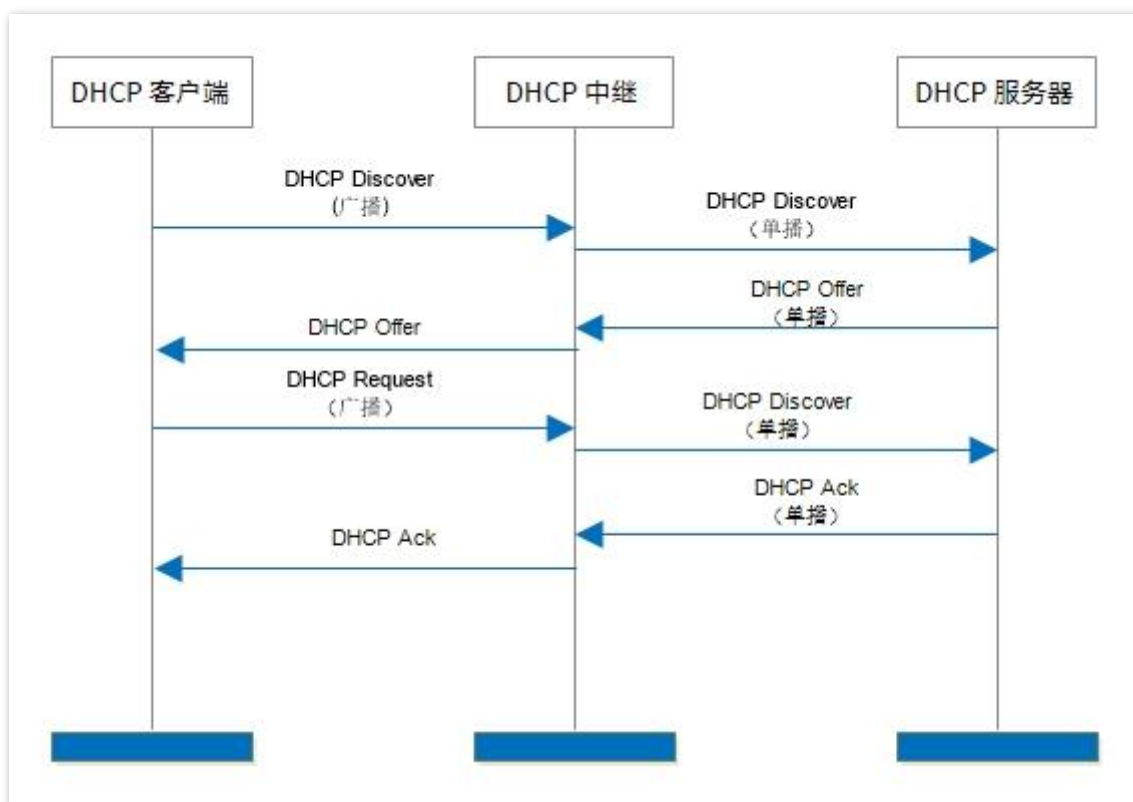
标题项	说明
目标 IP 地址	Tracert 检测的目标设备的 IP 地址或域名。
最大跳数	检测报文发送的最大跳数。

4 交换设置

4.1 DHCP 中继

在 DHCP 的基本网络模型中,要求客户端和服务端处于同一个局域网。这样在划分了多个 VLAN 的网络中,需要为每个 VLAN 都配置一个 DHCP 服务器,组网成本高。本交换机提供 DHCP 中继代理功能,能够在不同局域网之间转发 DHCP 请求和应答消息,使得多个局域网可以共享一个 DHCP 服务器。

DHCP 中继代理工作原理如下图。



- 当 DHCP 中继收到 DHCP 客户端的以广播方式发送的 DHCP discover 或 DHCP request 报文后, 将报文中的 giaddr 字段填充为 DHCP 中继的 IP 地址, 并根据配置将报文单播转发给指定的 DHCP 服务器。
- DHCP 服务器根据报文中的 giaddr 字段在地址池中选择相同地址段的 IP 地址, 并将携带有该 IP 地址信息的应答报文发送给 DHCP 中继。

- 当收到来自服务器的应答报文时，DHCP 中继将删除数据包中的 Option 82 字段，将 DHCP 应答报文向中继设备的接口网络中广播。

Option 82 选项又被称为 DHCP 中继代理信息选项 (Relay Agent Information Option)，是 DHCP 报文中的一个 Option 选项，该选项记录了 DHCP 客户端的位置信息。您可以通过该选项定位到对应的 DHCP 客户端，从而实现对客户端的认证、计费等控制功能；也可以在 DHCP 服务器上根据该选项信息配置相应的 IP 地址和其他参数分配策略，从而实现 IP 地址的灵活分配。

本交换机默认关闭 Option 82 选项工作机制。开启后，本交换机的 Option 82 选项工作机制如下表：

收到报文类型	处理策略
不带 Option 82 选项的 DHCP 请求报文	<p>将本交换机默认的内容增加到 DHCP 请求报文的 Option 82 选项信息中，再转发该报文。</p> <p> 提示</p> <p>本交换机默认的内容为接收到 DHCP 客户端请求包的端口编号、DHCP 客户端 MAC 地址和所属 VLAN。</p>
带 Option 82 选项的 DHCP 请求报文	<p>根据配置的 Option 选项策略对 DHCP 请求报文进行处理。</p> <ul style="list-style-type: none">- 替换：将本交换机默认的内容替换报文中原有的 Option 82 选项信息并进行转发。- 保留：保留报文中原有的 Option 82 选项状态并转发该报文。- 丢弃：丢弃带有 Option 82 选项的 DHCP 请求报文，转发不带 Option 82 选项的 DHCP 请求报文。
DHCP 应答报文	删除 DHCP 应答报文中的 Option 82 选项，再转发该报文。

在「交换设置」>「DHCP 中继」页面中，您可以配置 DHCP 中继规则。



DHCP 中继

Option 82 选项状态

Option 82 选项策略

中继设置

<input type="checkbox"/>	VLAN ID	服务器 IP	操作
暂无数据			

参数说明

标题项	说明
DHCP 中继	开启或关闭 DHCP 中继功能。默认关闭。
Option 82 选项状态	开启或关闭 Option 82 选项。Option 82 选项记录了 DHCP 客户端的位置信息，开启了 Option 82 选项，Option 82 选项策略才会生效。
Option 82 选项策略	<p>您可以参考以下描述选择合适的 Option 82 选项策略：</p> <ul style="list-style-type: none">- 替换：将本交换机默认的内容替换报文中原有的 Option 82 选项信息并进行转发。- 保留：保留报文中原有的 Option 82 选项状态并转发该报文。- 丢弃：丢弃带有 Option 82 选项的 DHCP 请求报文，转发不带 Option 82 选项的 DHCP 请求报文。
VLAN ID	<p>客户端所在的 VLAN。</p> <p>该 VLAN 必须是已存在的，且已配置三层虚接口的 VLAN。</p>
服务器 IP	<p>远程 DHCP 服务器的地址。</p> <p>远程 DHCP 服务器与客户端所在 VLAN 的 IP 地址不应在同一个网段。</p>

4.2 DHCP 侦听

4.2.1 概述

DHCP 侦听 (DHCP Snooping) 是一种保护 DHCP 服务的安全机制。具体如下：

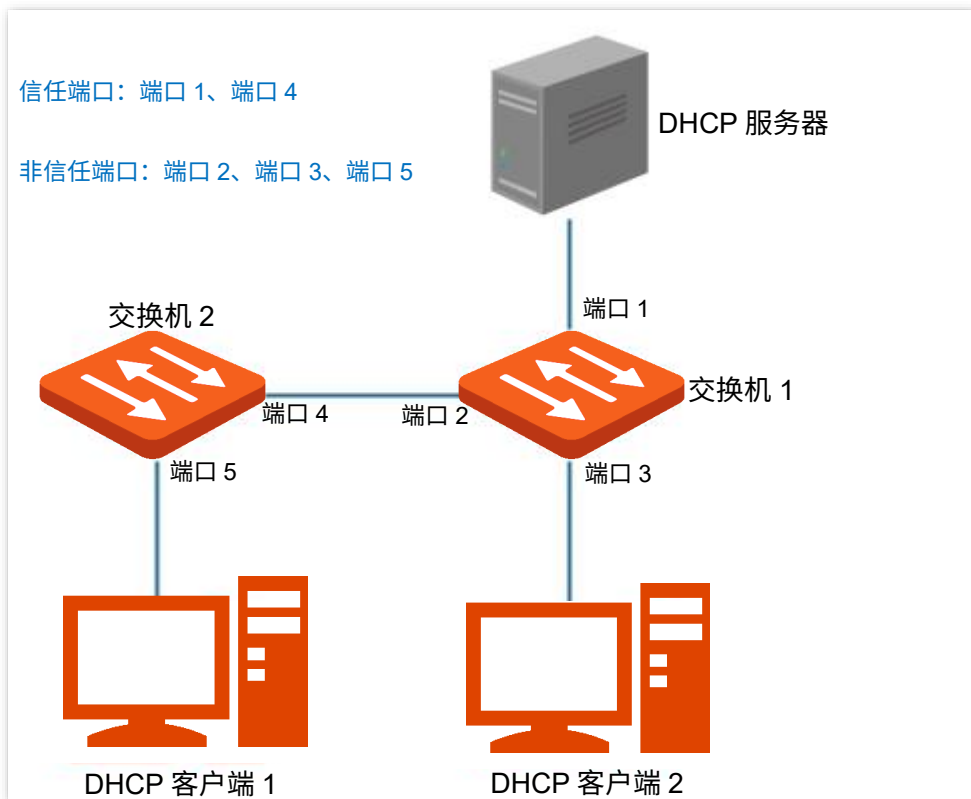
- 保证 DHCP 客户端能够从合法的服务器获取到 IP 地址。

在本交换机上将指向合法的 DHCP 服务器方向的端口设置为信任端口，其他端口设置为非信任端口。交换机对信任端口的 DHCP 报文进行转发，丢弃非信任端口的 DHCP 响应报文，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址。

- 记录 DHCP Snooping 表项。

本交换机通过侦听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。DHCP Snooping 表是 ARP 合法性校验的重要依据。

DHCP 侦听功能简易组网拓扑如下，假设交换机 1 和交换机 2 都开启了 DHCP 侦听功能。





开启了 DHCP 侦听功能的交换机只有位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间时，DHCP 侦听功能才有效；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP 侦听功能无效。

Option 82 选项又被称为 DHCP 中继代理信息选项（Relay Agent Information Option），是 DHCP 报文中的一个 Option 选项，该选项记录了 DHCP 客户端的位置信息。您可以通过该选项定位到对应的 DHCP 客户端，从而实现对客户端的认证、计费等控制功能；也可以在 DHCP 服务器上根据该选项信息配置相应的 IP 地址和其他参数分配策略，从而实现 IP 地址的灵活分配。

本交换机默认关闭 Option 82 选项工作机制。开启后，本交换机的 Option 82 选项工作机制如下表：

收到报文类型	处理策略
不带 Option 82 选项的 DHCP 请求报文	<p>将本交换机默认的内容增加到 DHCP 请求报文的 Option 82 选项信息中，再转发该报文。</p> <p> 提示</p> <p>本交换机默认的内容为接收到 DHCP 客户端请求包的端口编号、DHCP 客户端 MAC 地址和所属 VLAN。</p>
带 Option 82 选项的 DHCP 请求报文	<p>根据配置的 Option 选项策略对 DHCP 请求报文进行处理。</p> <ul style="list-style-type: none">- 替换：将本交换机默认的内容替换报文中原有的 Option 82 选项信息并进行转发。- 保留：保留报文中原有的 Option 82 选项状态并转发该报文。- 丢弃：丢弃带有 Option 82 选项的 DHCP 请求报文，转发不带 Option 82 选项的 DHCP 请求报文。
DHCP 应答报文	删除 DHCP 应答报文中的 Option 82 选项，再转发该报文。

4.2.2 配置 DHCP 侦听

在「交换设置」>「DHCP 侦听」页面中，您可以配置 DHCP 侦听规则。

端口	端口属性	Option 82选项	选项策略	操作
1	非信任端口	关闭	替换	
2	非信任端口	关闭	替换	
3	非信任端口	关闭	替换	
4	非信任端口	关闭	替换	
5	非信任端口	关闭	替换	
6	非信任端口	关闭	替换	
7	非信任端口	关闭	替换	
8	非信任端口	关闭	替换	
9	非信任端口	关闭	替换	

参数说明

标题项	说明
DHCP 侦听	开启或关闭 DHCP 侦听功能。
端口	端口编号。
端口属性	端口的 DHCP 侦听属性。 <ul style="list-style-type: none">- 信任端口：可以正常转发接收到的 DHCP 报文，用于连接合法的 DHCP 服务器。- 非信任端口：丢弃接收到 DHCP 响应报文，确保这些端口上架设的 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。
Option 82 选项	Option 82 选项状态。Option 82 选项记录了 DHCP 客户端的位置信息，开启了 Option 82 选项，选项策略才会生效，Option 82 选项工作机制请参照 Option 82 。

标题项	说明
-----	----

您可以参考以下描述选择合适的 Option 82 选项策略：

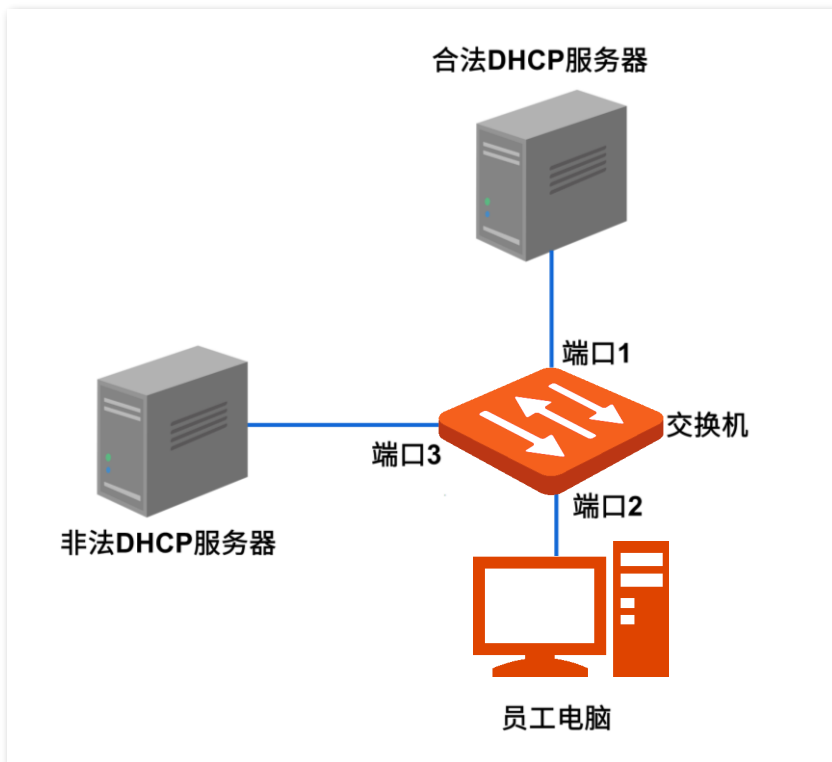
选项策略

- 替换：将本交换机默认的内容替换报文中原有的 Option 82 选项信息并进行转发。
- 保留：保留报文中原有的 Option 82 选项状态并转发。
- 丢弃：丢弃带有 Option 82 选项的 DHCP 请求报文，转发不带 Option 82 选项的 DHCP 请求报文。

4.2.3 DHCP 侦听配置举例

组网需求

如下图所示，某公司在办公楼层部署了交换机。交换机端口 2 连接员工电脑，员工电脑采用 DHCP 获取 IP 地址。该网络中部署了合法 DHCP 服务器，交换机端口 1 连接合法 DHCP 服务器。目前办公楼层经常出现非法 DHCP 服务器的接入，导致员工电脑获取到错误的地址而上不了网或者导致员工电脑获取到冲突的地址。



方案设计

在交换机上开启 DHCP 侦听功能，交换机接 DHCP 服务器的端口 1 设置为信任端口，其他端口设置为非信任端口，保证员工电脑能够从合法的服务器获取到 IP 地址。

配置步骤

步骤 1 进入配置页面。

[登录到交换机 Web 管理页面](#)，点击「交换设置」>「DHCP 侦听」。

步骤 2 开启 DHCP 侦听功能。

打开“DHCP 侦听”开关。

端口	端口属性	Option 82 选项	选项策略	操作
1	非信任端口	关闭	替换	
2	非信任端口	关闭	替换	
3	非信任端口	关闭	替换	
4	非信任端口	关闭	替换	
5	非信任端口	关闭	替换	
6	非信任端口	关闭	替换	
7	非信任端口	关闭	替换	
8	非信任端口	关闭	替换	
9	非信任端口	关闭	替换	

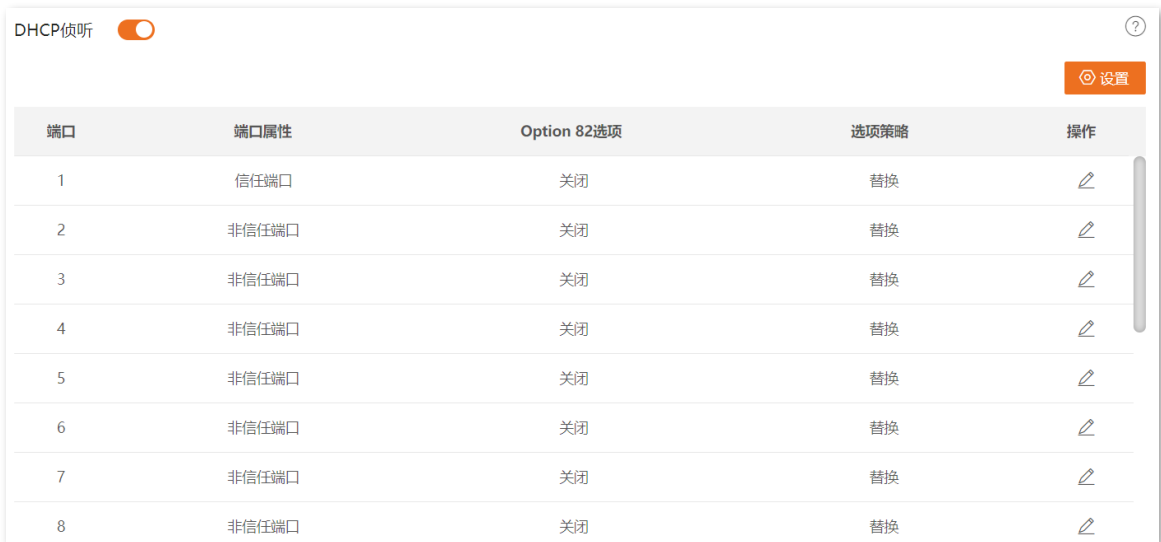
步骤 3 交换机接 DHCP 服务器的端口 1 设置为信任端口，其他端口设置为非信任端口。以下以配置端口 1 为例，其他端口配置类似。

点击端口 1 后面的 ，设置“端口属性”为“信任端口”，点击 **确定**。

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。

不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0



步骤 4 保存配置。

点击管理页面右上角的 **保存配置** 进行全局保存。

---完成

验证配置

完成以上配置后，员工电脑只能从合法 DHCP 服务器获取 IP 地址信息，非法 DHCP 服务器无法为员工电脑分配 IP 地址信息。

4.3 生成树

4.3.1 概述

生成树用于消除链路环路，避免环路产生的广播风暴，并提供链路冗余备份。

STP、RSTP、MSTP 是生成树的三种版本。

STP

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1d 标准建立的，用于在局域网中消除数据链路层物理环路，并提供链路冗余备份的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择地对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止因报文在环路网络中不断增生和无限循环，导致设备报文处理能力下降。

STP 协议报文

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息，BPDU 中包含了足够的信息来保证交换机完成生成树的计算过程。

STP 通过在设备之间传递 BPDU 来确定网络的拓扑结构。STP 协议中的 BPDU 分为两类：

- 配置 BPDU（Configuration BPDU）：用来进行生成树计算和维护生成树拓扑的报文。
- TCN BPDU（Topology Change Notification BPDU）：当拓扑结构发生变化时，用来通知相关设备网络拓扑结构发生变化的报文。

STP 基本概念

■ 桥 ID

桥 ID 是桥的优先级和 MAC 地址组成，其中桥优先级是一个可以设定的参数。桥 ID 越小，则桥的优先级越高。桥 ID 最小的桥为根桥。

■ 根桥

树形的网络结构必须有树根，于是 STP 引入了根桥（Root Bridge）的概念。根桥在全网中有且只有一个，且根据网络拓扑的变化而改变，因此根桥并不是固定的。

在网络初始化过程中，所有设备都视自己为根桥，生成各自的配置 BPDU 并周期性地向外发送；当网络拓扑稳定后，只有根桥设备才会向外发送配置 BPDU，其它设备只对其进行转发。

■ 根端口

根端口，指一个非根桥设备上离根桥最近的端口，负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。

■ 指定桥与指定端口

- 指定桥：对于一台设备而言，指与本机直接相连并负责向本机转发 BPDU 的设备；对于一个局域网而言，指负责向本网段转发 BPDU 的设备。

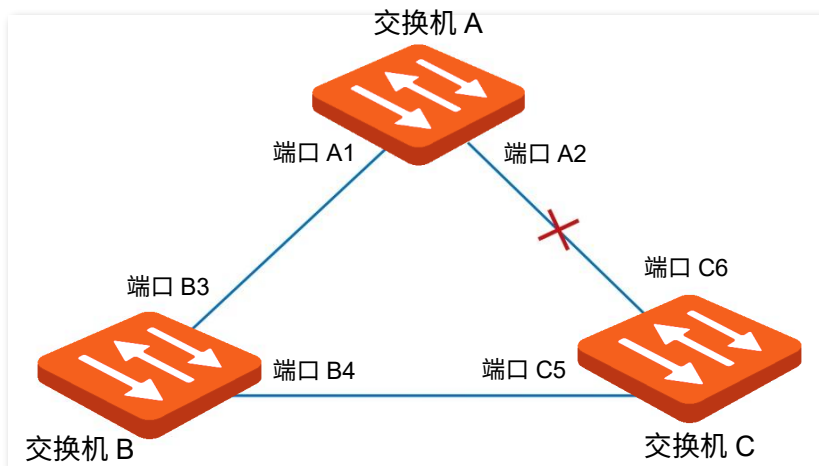
在每个网段，到根桥的路径开销最小的设备会成为指定桥，当所有交换机具有相同的根路径开销时，网桥 ID 最低的设备会被选为指定桥。

- 指定端口：对于一台设备而言，为指定桥向本机转发 BPDU 的端口；对于一个局域网而言，为指定桥向本网段转发 BPDU 的端口。

■ 路径开销

STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

下图为 STP 基本概念组网图，交换机 A、B、C 三者顺次相连。



经 STP 计算过后，交换机 A 被选为根桥，端口 A2 和端口 C6 之间的线路被阻塞。

- 桥：交换机 A 为整个网络的根桥；交换机 B 是交换机 C 的指定桥。
- 端口：端口 B3 和端口 C5 分别为交换机 B 和交换机 C 的根端口；端口 A1 和端口 B4 分别为交换机 A 和交换机 B 的指定端口；端口 C6 为交换机 C 的阻塞端口。

BPDU 优先级比较

根桥 ID 越小的 BPDU 优先级更高；若根桥 ID 相同，则比较根路径开销，比较方法为：用 BPDU 中的根路径开销加上本端口对应的路径开销，假设两者之和为 S，则 S 较小的 BPDU 优先级较高。

若根路径开销也相同，则依次比较指定桥 ID、指定端口 ID、接收该 BPDU 的端口 ID 等，上述值较小的 BPDU 优先级较高。

STP 的计算过程

步骤 1 初始状态

各设备的各个端口在初始状态时会生成以自己为根桥的 BPDU，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

步骤 2 选择最优 BPDU

各设备都向外发送自己的 BPDU，同时也会收到其它设备发送的 BPDU。最优 BPDU 的选择过程如下：

步骤	内容
1	当端口收到的 BPDU 比本端口 BPDU 的优先级低时，设备会将接收到的 BPDU 丢弃，对该端口的 BPDU 不作任何处理。 当端口收到的 BPDU 比本端口 BPDU 的优先级高时，设备就用接收到的 BPDU 中的内容替换该端口的 BPDU 中的内容。
2	设备将所有端口的 BPDU 进行比较，选出最优的 BPDU。

步骤 3 选举根桥

网络中所有的设备通过交换 BPDU，比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。

步骤 4 选举根端口、指定端口

根端口、指定端口的选择过程如下：

步骤	内容
1	非根桥设备将接收最优 BPDU 的那个端口定为根端口。 设备根据根端口的 BPDU 和根端口的路径开销，为每个端口计算一个指定端口 BPDU： <ul style="list-style-type: none">- 根桥 ID 替换为根端口的 BPDU 的根桥 ID。
2	<ul style="list-style-type: none">- 根路径开销替换为根端口 BPDU 的根路径开销加上根端口对应的路径开销。- 指定桥 ID 替换为自身设备的 ID。- 指定端口 ID 替换为自身端口 ID。

步骤	内容
3	<p>设备使用计算出来的 BPDU 和需要确定端口角色的端口上的 BPDU 进行比较，并根据比较结果进行不同的处理：</p> <ul style="list-style-type: none">- 如果计算出来的 BPDU 更优，则设备就将该端口定为指定端口，端口上的 BPDU 被计算出来的 BPDU 替换，并周期性向外发送。- 如果端口上的 BPDU 更优，则设备不更新该端口的 BPDU 并将此端口阻塞，此端口将不再转发数据，只接收但不发送 BPDU。



在拓扑稳定状态，只有根端口和指定端口转发流量，其它端口都处于阻塞状态，它们只接收 STP 协议报文 (BPDU) 而不转发用户数据。

STP 定时器

■ 联络时间 (Hello Time)

根桥交换机向周围的交换机发送 BPDU 报文的时间间隔，用来检测链路是否存在故障。

■ 老化时间 (Max Age)

如果在超出老化时间后，还没有收到根桥交换机发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。

■ 转发延时 (Forward Delay)

指交换机端口状态迁移的延迟时间。

链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新 BPDU 无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻开始转发数据，可能会产生暂时性的环路。因此，STP 采用了一种状态迁移的机制，新选出的根端口和指定端口要经过 2 倍的转发延时后才能进入转发状态，这个转发延时可确保新的 BPDU 已经传遍整个网络。

RSTP 简介

RSTP (Rapid Spanning Tree Protocol, 快速生成树协议) 由 IEEE 制定的 802.1w 标准定义，完全向下兼容 802.1d STP 协议，除了和 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快速收敛”。如果一个局域网内的网桥都支持 RSTP 协议且管理员配置得当，一旦网络拓扑改变而要重新生成拓扑树只需要极短时间 (传统的 STP 需要大约 50 秒，RSTP 只需要 1 秒左右)。

RSTP 也是通过在设备之间传递 BPDU 来确定网络的拓扑结构。但 RSTP 的 BPDU 格式和 STP 的 BPDU

格式有少许不同。在拓扑改变时，使用 RST-BPDU 报文通过泛洪方式快速的通知到整个网络。

RSTP 中，实现根端口和指定端口的状态快速迁移的前提条件如下：

- 根端口：本设备上旧的根端口已经停止转发数据，而且上游指定端口已开始转发数据。
- 指定端口：若指定端口是边缘端口，则指定端口可以直接进入转发状态；若指定端口是 P2P 端口，则设备可通过与下游设备握手，得到响应后即刻进入转发状态。

■ 边缘端口

边缘端口是一个位于交换区域边缘的指定端口，可直连无环路的网络端口，通常直连终端设备（用户端）。指定为边缘端口可快速迁移到转发状态，而不需要经历监听和学习的状态。若边缘端口接收到 BPDU 报文，将变为非边缘端口，作为一个普通的生成树端口，参与生成树的计算。

■ P2P 端口

P2P 端口是指连接其他交换机的端口，在 RSTP/MSTP 下，所有在全双工模式下的端口被认为是 P2P 端口。

MSTP 简介

在日常工作环境中 STP 和 RSTP 存在如下一些不足：

- STP 不能快速迁移，即使是在点对点链路或边缘端口，也必须等待两倍的转发延时，端口才能迁移到转发状态。
- RSTP 虽然可以快速收敛，但和 STP 一样，由于局域网内所有 VLAN 都共享一棵生成树，因此所有 VLAN 的报文都沿这棵生成树进行转发，不能按 VLAN 阻塞冗余链路，也无法在 VLAN 间实现数据流量的负载均衡。

MSTP（Multiple Spanning Tree Protocol，多生成树协议）由 IEEE 制定的 802.1s 标准定义，兼容 STP 和 RSTP 协议，不但可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制，弥补了 STP 和 RSTP 的缺陷。

MSTP 的特点如下：

- MSTP 通过“VLAN-实例”映射表，把 VLAN 和生成树联系起来，将多个 VLAN 捆绑到一个实例中，并以实例为基础实现负载均衡。
- MSTP 把一个生成树网络划分成多个域，每个域内形成多棵内部生成树，各个生成树之间彼此独立。

- MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载分担。

■ MST 域

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台设备以及它们之间的网段所构成。这些设备具有下列特点：

- 都开启了生成树协议。
- 域名相同。
- 配置摘要相同，即 VLAN 与 MSTI 间映射关系的配置相同。
- MSTP 修正等级的配置相同。
- 这些设备之间通过物理链路连通。

■ MSTI

一个 MST 域内可以有多棵生成树，每棵生成树都称为一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。在 MST 域内，MSTP 根据“VLAN-实例”映射表，生成多个生成树，并将 VLAN 映射到生成树，生成树计算方式与 STP 相同。

■ IST

IST（Internal Spanning Tree，内部生成树）是 MST 域内的一棵特殊的生成树，通常我们称之为 MSTI 0。

■ CST

CST（Common Spanning Tree，公共生成树）是连接网络内所有 MST 域的单生成树。MSTP 将 MST 域看做单台设备，在域间计算并生成 CST。

■ CIST

CIST（Common and Internal Spanning Tree，公共和内部生成树）是一棵连接网络内所有设备的单生成树，由所有 MST 域的 IST 再加上 CST 共同构成整个网络的一棵完整的单生成树。

■ 域根

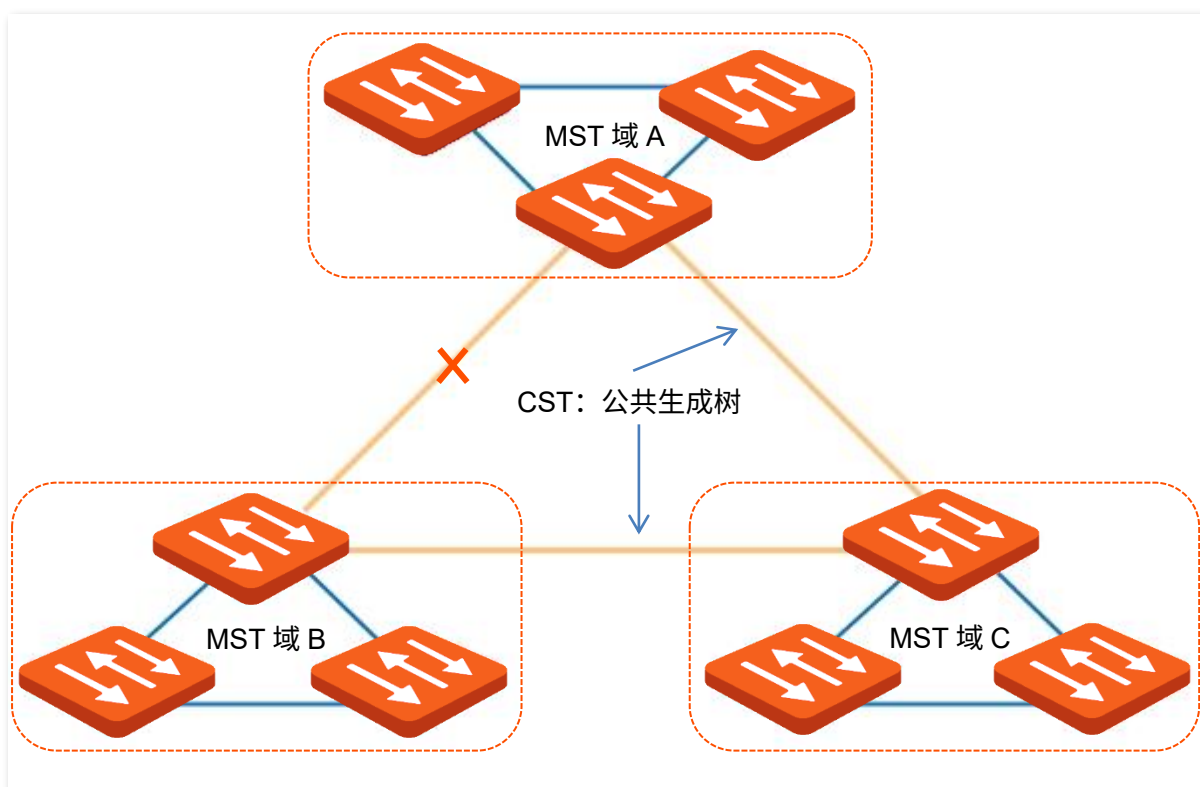
域根（Regional Root）是 MST 域内 IST 或 MSTI 的根桥。各生成树拓扑不同，其域根也可能不相同。

■ 总根

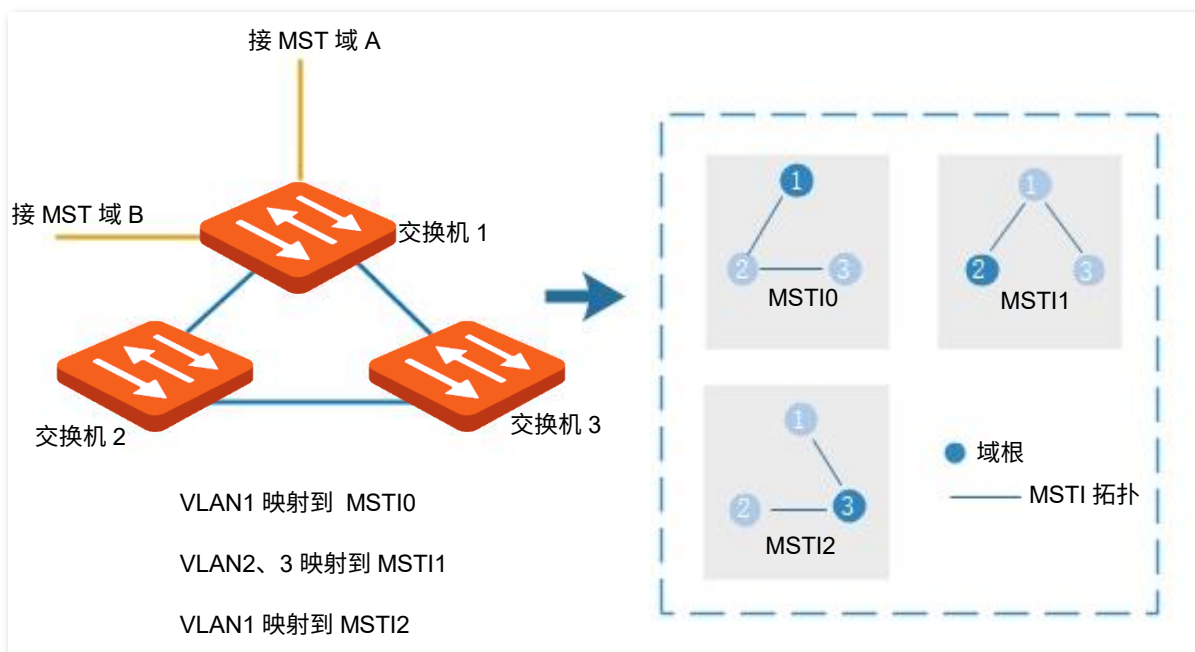
总根（Common Root Bridge）就是 CIST 的根桥。MSTP 通过 BPDU 比较，在整个网络中选出一个最优的设备作为总根。

MSTP 同 STP 一样，使用 BPDU 进行生成树的计算，只是 BPDU 中携带的是 MSTP 的配置信息。

MSTP 基本概念示意图如下：



MST 域 C 中的各 MSTI 拓扑示意图如下：



端口状态

MSTP 中，根据端口是否转发数据和如何处理 BPDU 报文，可将端口状态划分为以下四种：

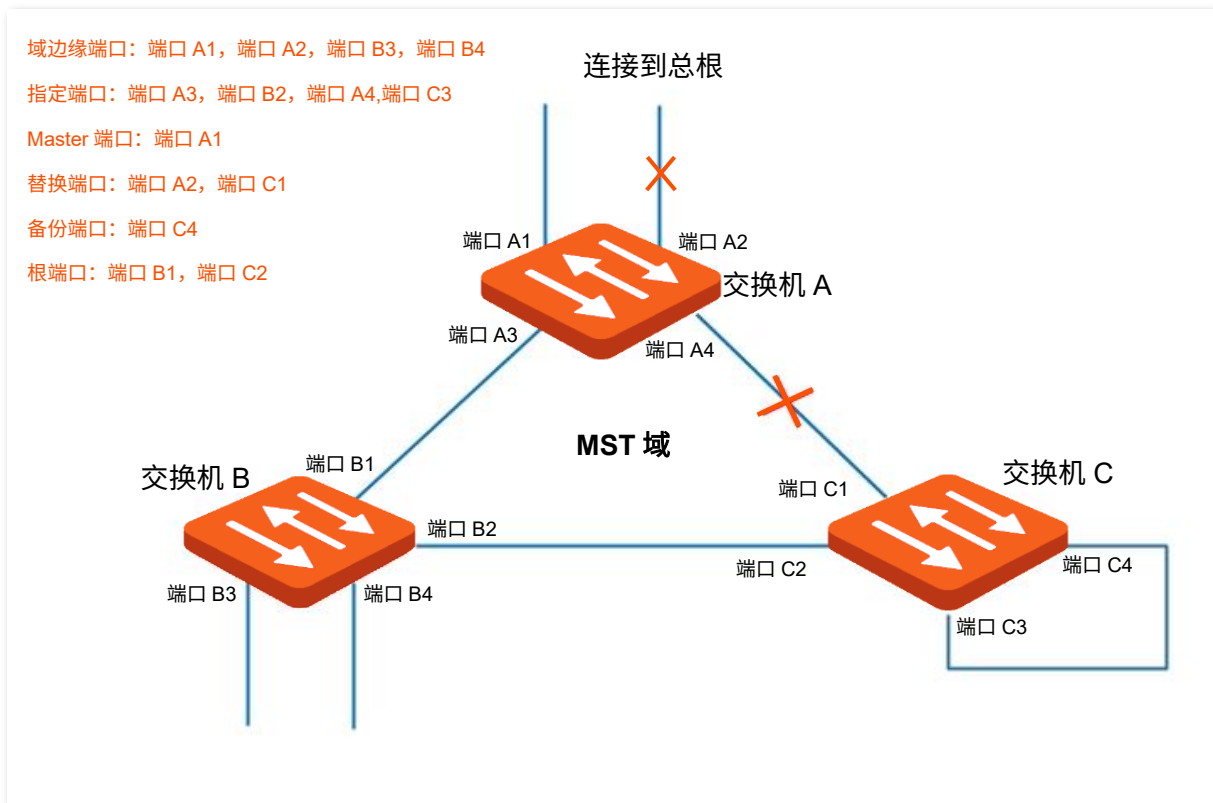
- Forwarding：接收并转发数据，接收并发送 BPDU 报文，进行地址学习。
- Learning：不接收或转发数据，接收并发送 BPDU 报文，进行地址学习。
- Discarding：不接收或转发数据，接收但不发送 BPDU 报文，不进行地址学习。
- Disabled：物理链路断开。

端口角色

MSTP 的端口角色分为以下几种：

- Root：根端口，到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- Designated：指定端口，负责向下游网段或设备转发数据的端口。
- Master：Master 端口，连接 MST 域到总根的端口，位于整个域到总根的最短路径上。
- Alternate：替换端口，根端口和 Master 端口的备份端口。
- Backup：备份端口，指定端口的备份端口。
- Disable：禁用端口，物理链路断开的端口。

端口角色的示意图如下所示。



4.3.2 全局配置

在「交换设置」>「生成树」>「全局配置」页面中，您可以配置生成树的全局参数。

全局配置



参数说明

标题项	说明
生成树状态	开启/关闭生成树功能。

标题项	说明
生成树版本	交换机的生成树协议版本。 <ul style="list-style-type: none">- STP：生成树协议。- RSTP：快速生成树协议。兼容 STP 协议，同时提供快速收敛的过程。- MSTP：多生成树协议。兼容 RSTP 和 STP 协议，同时还为冗余链路提供了更好的负载分担机制。

桥设置

桥设置

最大老化时间 s (范围: 6-40)

Hello Time s (范围: 1-10)

转发延时 s (范围: 4-30)

最大跳数 (范围: 6-40)

桥优先级 ▼

注意: 最大老化时间 $\geq 2 \times (\text{Hello Time} + 1)$ 最大老化时间 $\leq 2 \times (\text{转发延时} - 1)$

参数说明

标题项	说明
最大老化时间	BPDU 在交换机中能够保存的最长时间，最大老化时间设置限制如下： <ul style="list-style-type: none">- 最大老化时间 $\geq 2 \times (\text{Hello Time} + 1)$- 最大老化时间 $\leq 2 \times (\text{转发延时} - 1)$
Hello Time	交换机发送 BPDU 的时间间隔，默认为 2 秒。
转发延时	在网络拓扑改变后，交换机的端口状态迁移的延时时间。默认为 15 秒。
最大跳数	协议报文被转发的最大次数，用于限制生成树的规模。
桥优先级	交换机参与生成树计算的系统优先级。优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。

MSTP 域设置

MSTP域设置

域名 (范围: 1-32个字符)

修正等级 (范围: 0-65535)

配置摘要 0xAC36177F50283CD4B83821D8AB26DE62

参数说明

标题项	说明
域名	MST 域的标识（Multiple Spanning Tree Regions，多生成树域），默认为交换机的 MAC 地址。
修正等级	交换机的 MSTP 修正等级，默认为 0。
配置摘要	根据 VLAN 与 MSTI 映射关系计算出来的值。

MSTP 实例

MSTP实例

<input type="checkbox"/>	实例ID	映射的VLAN列表	桥优先级	操作
<input type="checkbox"/>	0	1,5,7	32768	

参数说明

标题项	说明
实例 ID	最多可配置 32 个实例，0 为内部生成树，每个实例单独计算生成树。
映射的 VLAN 列表	实例映射的 VLAN。
桥优先级	实例的系统优先级，用于 MST 域内的各实例的根桥的选举。

指定根桥

指定根桥 	
桥ID 32768:d838.0dc9.081a	根桥ID 32768:d838.0dc9.081a
域根ID 32768:d838.0dc9.081a	根端口 none
根路径开销 0	内部根路径开销 0
拓扑状态 Topological_stability	最后拓扑变化时间 2022-09-07 03:38:54

参数说明

标题项	说明
桥 ID	本交换机的桥优先级+桥 MAC 地址。
域根 ID	本交换机所在域的域根设备的桥优先级+桥 MAC 地址。
根路径开销	根端口的路径开销与数据包经过的所有交换机的根路径开销之和。根桥的根路径开销是 0。
拓扑状态	<p>本交换机所在生成树的拓扑状态。</p> <ul style="list-style-type: none">- Topology_calculation 表示生成树计算中，端口状态还未稳定，暂时不能正常转发数据包。通常 STP 协议计算时间较长，默认情况下，Topology_calculation 状态最长持续 50 秒；而 RSTP 与 MSTP 则在 3 秒内。- Topological_stability 表示端口状态稳定，此时网络正常。
根桥 ID	STP 和 RSTP 协议时，为根桥设备的优先级+MAC 地址；MSTP 协议时，为总根设备的优先级+MAC 地址。
根端口	本交换机上离根桥最近的端口。
内部根路径开销	在 MST 域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。
最后拓扑变化时间	上一次拓扑变化的时间。

4.3.3 端口设置

在「交换设置」>「生成树」>「端口设置」页面中，您可以配置交换机端口的 STP 参数。

端口	STP状态	边缘端口	P2P端口	操作
1	开启	关闭	自动	
2	开启	关闭	自动	
3	开启	关闭	自动	
4	开启	关闭	自动	
5	开启	关闭	自动	
6	开启	关闭	自动	
7	开启	关闭	自动	
8	开启	关闭	自动	

参数说明

标题项	说明
端口	端口编号。
STP 状态	<p>端口生成树功能的启用状态。</p> <p>当全局配置和端口的生成树功能都开启时，该端口才参与生成树的计算。</p>
边缘端口	<p>通常直接连接终端设备。指定为边缘端口可快速迁移到转发状态，而不需要经历监听和学习的状态。若边缘端口接收到 BPDU 报文，将自动变为非边缘端口。默认所有端口都为非边缘端口。</p> <ul style="list-style-type: none"> - 关闭：表示端口为非边缘端口。 - 开启：表示端口为边缘端口。
P2P 端口	<p>点对点端口可以进行快速的迁移。在 RSTP/MSTP 下，所有在全双工模式下的端口被认为点对点端口。默认端口自动识别。</p> <ul style="list-style-type: none"> - 自动：端口自动识别是否为 P2P 端口。 - 开启：端口是 P2P 端口。 - 关闭：端口不是 P2P 端口。

4.3.4 端口统计

在「交换设置」>「生成树」>「端口统计」页面中，您可以查询各端口发送、接收和丢弃的生成树数据包情况。

全局设置 端口设置 端口统计 实例信息 ?										
端口	发送				接收				丢弃	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0

参数说明

标题项	说明
端口	端口编号。
MSTP	端口发送/接收的 MSTP 配置 BPDU 的数量。
RSTP	端口发送/接收的 RSTP 配置 BPDU 的数量。
STP	端口发送/接收的 STP 配置 BPDU 的数量。
TCN	端口发送/接收的 TCN BPDU 的数量。
Unknown	端口丢弃的未知 STP 包数量。
Illegal	端口丢弃的错误 STP 包数量。

4.3.5 实例信息

在「交换设置」>「生成树」>「实例信息」页面中，您可以查看和设置 MSTP 实例信息。

端口	端口角色	端口状态	域根ID	指定桥ID	指定端口	优先级	路径开销	操作
1	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	1	128	20000	
2	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	2	128	20000	
3	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	3	128	20000	
4	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	4	128	20000	
5	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	5	128	20000	
6	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	6	128	20000	
7	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	7	128	20000	
8	Disabled	Disabled	32768-00e0.4c11...	32768-00e0.4c11...	8	128	20000	

参数说明

标题项	说明
实例 ID	选择实例 ID，可查看该实例内端口的 STP 状态信息。
端口	端口编号。
端口角色	端口在生成树实例中担任的角色。具体请参见 端口角色 。
端口状态	端口所处的工作状态。具体请参见 端口状态 。
域根 ID	域根设备的桥优先级+桥 MAC 地址。
指定桥 ID	与本交换机直连并且负责向本交换机转发 BPDU 的设备的桥 ID。 根端口和备份端口的指定桥 ID 是发送 BPDU 报文给它的设备的桥 ID；指定端口的指定桥 ID 是设备本身的桥 ID。
指定端口	指定桥向本交换机转发 BPDU 的端口。
优先级	当根桥 ID、根路径开销、桥 ID 都相同时，端口优先级是确定该端口是否会被选为根端口的依据，端口优先级值越小时，优先级越高。

标题项	说明
路径开销	在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

4.4 LLDP 设置

4.4.1 概述

当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) 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。网络管理系统可以通过 SNMP (Simple Network Management Protocol, 简单网络管理协议) 获取到这些信息，以查询及判断链路的通信状况。

基本概念

■ LLDP 报文

封装有 LLDPDU 的报文称为 LLDP 报文。

■ 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。

■ TLV

TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。

■ 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，帮助网络拓扑绘制，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。

工作机制

LLDP 是用于信息通告和获取的单向协议，它主动通告一种工作方式，无需确认，不能查询。

LLDP 主要完成如下工作：

- 初始化并维护本地 MIB 库中的信息。
- 从本地 MIB 库中提取信息，并将信息封装到 LLDP 帧中。LLDP 帧的发送有两种触发方式，一是定时器到期触发，二是设备状态发生了变化触发。
- 识别并处理接收到的 LLDPDU 帧。
- 维护远端设备 LLDP MIB 信息库。
- 当本地或远端设备 MIB 信息库中有信息发生变化时，发出通告事件。

■ LLDP 的工作状态

LLDP 有以下四种工作状态：

- 发送接收：既发送又接收 LLDP 报文。
- 只发送：只发送而不接收 LLDP 报文。
- 只接收：只接收而不发送 LLDP 报文。
- 禁用：既不发送也不接收 LLDP 报文。

当端口的 LLDP 工作状态发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作状态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，当端口工作状态改变时，延迟一段时间再执行初始化操作。

■ LLDP 报文的发送机制

端口工作在“发送接收”或“只发送”状态时，交换机会周期性地向邻居设备发送 LLDP 报文。

如果交换机的本地信息发生了变化，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 报文后都需要延迟一段时间后再继续发送下一个报文。

当交换机的工作状态由“禁用/只接收”切换为“发送接收/只发送”时，将立即发送一个 LLDP 报文。

■ LLDP 报文的接收机制

当端口工作在“发送接收”或“只接收”状态时，交换机会对收到的 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。

4.4.2 全局设置

在「交换设置」>「LLDP 设置」>「全局设置」页面，您可以配置 LLDP 的全局参数。

LLDP 功能

全局设置 端口设置 邻居信息

发送间隔时间 s (范围: 5-3600)

TTL 乘数 s (范围: 2-10)

初始化延迟时间 s (范围: 1-10)

参数说明

标题项	说明
LLDP 功能	开启或关闭 LLDP 功能。
发送间隔时间	交换机向邻居设备发送 LLDPDU 的时间间隔。
TTL 乘数	TTL 乘数用以控制本地设备发送的 LLDPDU 中 TTL 字段的值，TTL 即为本地信息在邻居设备上的存活时间。 $TTL = \text{Min}(65535, (\text{TTL 乘数} \times \text{LLDPDU 发送间隔}))$ ，即取 65535 与 (TTL 乘数 × LLDPDU 发送间隔) 中的最小值。
初始化延迟时间	为了避免端口工作状态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，当端口工作状态改变时，延迟一段时间再执行初始化操作。

4.4.3 端口设置

在「交换设置」>「LLDP 设置」>「端口设置」页面，您可以配置各端口的 LLDP 工作状态。

端口	LLDP工作状态	操作
1	发送接收	
2	发送接收	
3	发送接收	
4	发送接收	
5	发送接收	
6	发送接收	
7	发送接收	
8	发送接收	

参数说明

标题项	说明
端口	端口编号。
LLDP 工作状态	端口的 LLDP 工作状态。 <ul style="list-style-type: none">- 禁用：表示端口不开启 LLDP 功能。- 只发送：表示端口只发送而不接收 LLDP 报文。- 只接收：表示端口只接收而不发送 LLDP 报文。- 发送接收：表示端口既发送又接收 LLDP 报文。- 不改变：保留当前配置，不改变 LLDP 工作状态。

4.4.4 邻居信息

在「交换设置」>「LLDP 设置」>「邻居信息」页面，您可以查看交换机的邻居信息。

端口	系统名称	端口ID	邻居ID	管理地址	操作
15		94C6.9129.C21A	94C6.9129.C21A		🗑️
15	linux-8888884c9000.(none)	br0	0090.4C88.8888	192.168.0.252	🗑️

参数说明

标题项	说明
端口	端口编号。
系统名称	邻居设备的系统名称。
端口 ID	邻居设备的端口信息。  提示 端口信息可能是端口号、MAC 地址或其他信息，由邻居设备的 LLDP 报文中携带的信息定义。
邻居 ID	邻居设备的 MAC 地址。
管理地址	邻居设备的管理 IP 地址。
存活时间	邻居信息保存在本设备上的剩余时间。
端口描述	邻居设备上发送了 LLDP 报文的端口的详细描述。
系统描述	邻居设备的详细描述。
系统性能	邻居设备支持的特性。

4.5 LLDP-MED

4.5.1 概述

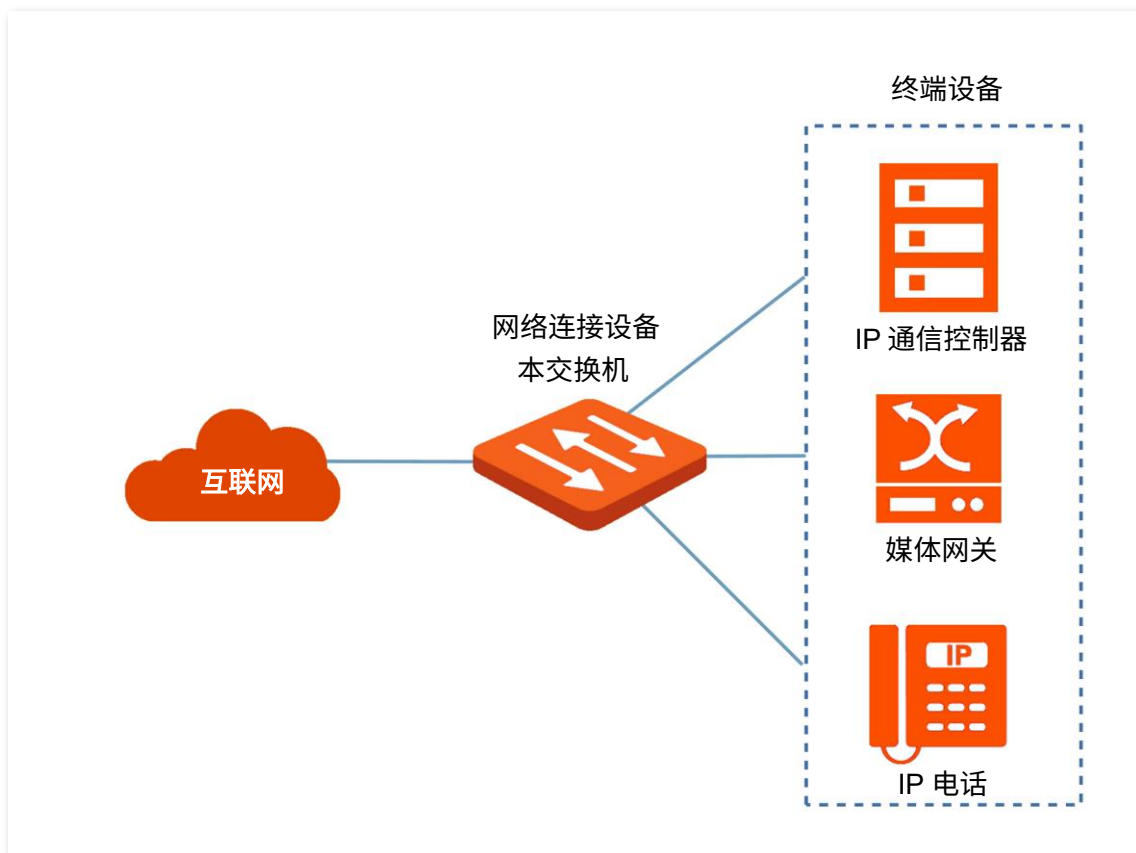
LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery，用于媒体终端发现的链路层发现协议）是 LLDP 协议的一个扩展，主要用于 VoIP（Voice over Internet Protocol，基于 IP 的语音传输）网络环境，方便 VoIP 设备的部署。

本交换机的 LLDP-MED 为媒体能力、网络策略、设备地址和扩展供电能力提供附加的 TLV，这些应用满足了 VoIP 设备的不同生产厂商在投资收效、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 设备类型

LLDP-MED 规定了两种设备类型，分别是网络连接设备（Network Connectivity Device）和终端设备（Endpoint Device）。本交换机属于网络连接设备。

下图为 LLDP-MED 网络部署示例图。



网络连接设备

LLDP-MED 网络连接设备是基于以下任一技术的 LAN 接入设备，为 LLDP-MED 终端设备提供基于 IEEE 802 的 LAN 基础设施的访问。

- 局域网交换机/路由器
- IEEE 802.1 网桥
- IEEE 802.3 中继器
- IEEE 802.11 无线接入点
- 支持 IEEE 802.1AB 和 MED 扩展，并可以通过任何方法中继 IEEE 802 帧的任何设备

终端设备

LLDP-MED 终端设备位于 IEEE 802 LAN 网络边缘，分为 I、II 和 III 类三种。

■ 通用终端 (I 类)

LLDP-MED 中的基本参与者端点，如 IP 通信控制器等。

■ 媒体终端 (II 类)

支持 IP 媒体流，如语音/媒体网关、会议桥、媒体服务器等。

■ 通信终端 (III 类)

支持 IP 通信终端用户，如 IP 电话、软件电话等。

4.5.2 基本设置

在「交换设置」>「LLDP-MED」>「基本设置」页面，您可以配置 LLDP-MED 的基本参数。

基本设置	TLV设置	本地信息	邻居信息
快速报文个数	<input type="text" value="4"/>	个 (范围: 1-10)	
设备类型	Network Connectivity		
<input type="button" value="确定"/>			

参数说明

标题项	说明
快速报文个数	当 LLDP-MED 的快速发送机制启动时，会连续发送指定个数的包含 LLDP-MED 信息的 LLDPDU，其默认值为 4。
设备类型	本交换机的 LLDP-MED 设备类型。本交换机为 LLDP-MED 网络连接设备。

4.5.3 TLV 设置

在「交换设置」>「LLDP-MED」>「TLV 设置」页面，您可以配置 LLDP-MED 的 TLV 信息。



参数说明

标题项	说明
端口	本交换机的端口号。
TLV 字段	<p>选择发送的 LLDPDU 中包含的 LLDP-MED 的 TLV 信息。</p> <ul style="list-style-type: none"> 媒体能力：媒体能力 TLV 标识网络连接设备所支持的 LLDP-MED TLV 类型。 网络策略：网络策略 TLV 允许互联的交换机和终端设备间相互通告 VLAN 配置，以及端口上为特定应用关联的二层/三层属性。 设备地址：设备地址 TLV 提供了向相邻设备发布本地设备物理地址信息的能力。 扩展供电能力：扩展供电能力 TLV 允许 LLDP-MED 连接设备和终端设备之间交换详细的供电信息，例如供电优先级、供电状态等。

4.5.4 本地信息

在「交换设置」>「LLDP-MED」>「本地信息」页面，您可以查看所有端口的 LLDP-MED 配置信息。



本地端口	设备类型	应用类型	媒体策略未知标记	VLAN ID	QoS DSCP值	操作
暂无数据						

参数说明

标题项	说明
本地端口	本交换机的端口号。
设备类型	LLDP-MED 规定的本地设备类型。
应用类型	本地设备支持的各种应用。
媒体策略未知标记	网络策略 TLV 中包含的未知标记位设置。
VLAN ID	端口所处 802.1Q VLAN 的 ID 值。
QoS DSCP 值	特定应用使用的 DSCP 值。

4.5.5 邻居信息

在「交换设置」>「LLDP-MED」>「邻居信息」页面，您可以查看所有端口邻居的 LLDP-MED 信息。



参数说明

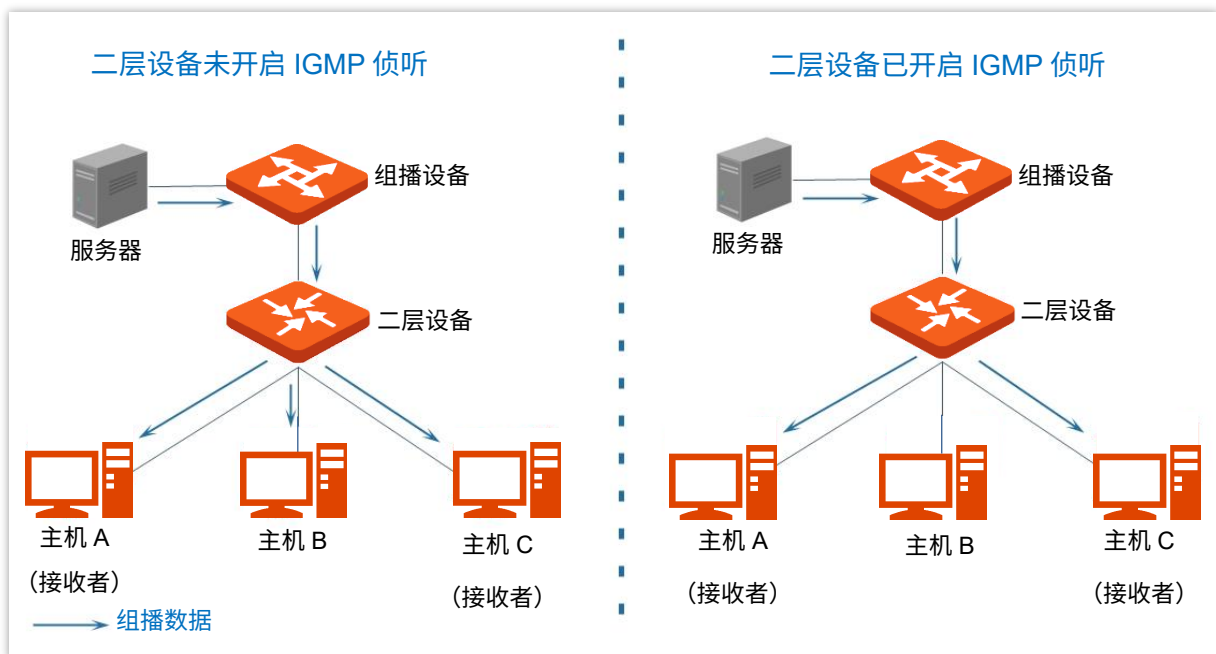
标题项	说明
本地端口	本交换机的端口号。
系统名称	邻居设备的系统名称。
邻居 ID	邻居设备的 MAC 地址。
设备类型	邻居设备的 LLDP-MED 设备类型。
应用类型	邻居设备支持的各种应用。
设备地址类型	邻居设备的地址类型。
供电类型	邻居设备的供电设备类型。

4.6 IGMP 侦听

4.6.1 概述

IGMP 侦听（Internet Group Management Protocol Snooping）是运行在二层以太网交换机上的组播约束机制，用于管理和控制组播组。

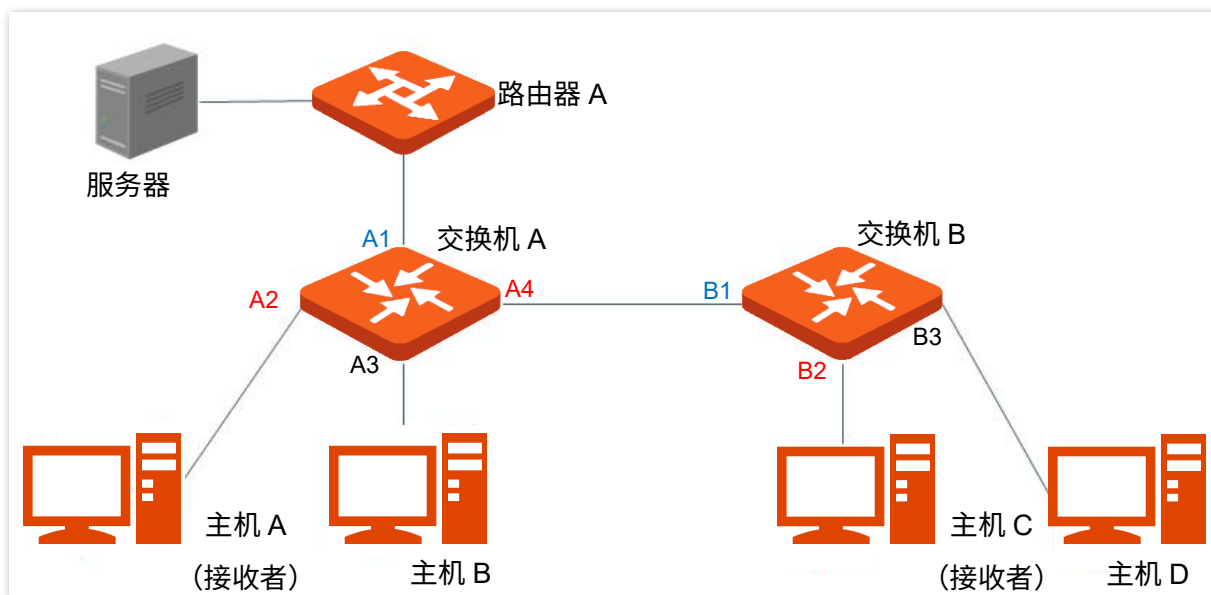
如下图所示，组播数据在没有运行 IGMP 侦听的二层设备中被广播；当二层设备运行了 IGMP 侦听后，设备通过对收到的 IGMP 报文进行分析，为端口和组播 MAC 地址建立起映射关系表，并根据这样的映射关系将组播数据转发给指定的接收者。



IGMP 侦听通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

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

如下图，路由器 A 连接组播源，交换机 A 和交换机 B 已开启 IGMP 侦听，主机 A 和主机 C 为组播数据的接收者。



■ 路由端口

在运行了 IGMP 侦听的二层设备上，朝向上游三层组播设备的端口。如上图中的端口 A1 和端口 B1。

■ 主机端口

在运行了 IGMP 侦听的二层设备上，朝向下游组播组成员的端口称为成员端口。如上图中的端口 A2、端口 A4 和端口 B2。

■ 普遍组查询

IGMP 查询器（如上图中的路由器 A）定期向本地网段内的所有主机与设备发送 IGMP 普遍组查询报文，以查询该网段有哪些组播组的成员。

在收到 IGMP 普遍组查询报文时，二层设备（如上图中的交换机 A 和交换机 B）将其转发出去，并对接收到该报文的端口（如 A1 和 B1）做如下处理：

- 如果在映射关系表中已包含该路由端口，则重置其老化定时器。
- 如果在映射关系表中尚未包含该路由端口，则将其添加到映射关系表中，并启动其老化定时器。

■ 特定组查询

运行了 IGMPv2 或 IGMPv3 的主机离开组播组时，会发送 IGMP 离开组报文。当二层设备（如上图中的交换机 A 和交换机 B）的主机端口接收到 IGMP 离开组报文时，会根据映射关系表做如下处理：

- 如果不存在该组播组对应的转发表项，或者该组播组对应转发表项的出端口列表中不包含该端口，二层设备不会向任何端口转发该报文，而将其直接丢弃。
- 如果存在该组播组对应的转发表项，且该转发表项中还有其他主机端口时，二层设备不会向任何端口转发该报文，而将其丢弃；同时向该主机端口发送 IGMP 特定组查询报文。
- 如果存在该组播组对应的转发表项，且该转发表项中没有其他主机端口时，二层设备会将该报文从路由端口转发出去，同时向该主机端口发送 IGMP 特定组查询报文。

4.6.2 全局设置

在「交换设置」>「IGMP 侦听」>「全局设置」页面，您可以配置 IGMP 侦听的全局参数。

IGMP侦听

全局设置 快速离开

VLAN ID ▾

所属VLAN ▾

组播VLAN状态 ▾

协议版本 ▾

路由端口老化时间 s (范围: 1-1000)

普遍组查询最大响应时间 s (范围: 1-25)

特定组查询最大响应时间 s (范围: 1-5)

主机端口老化时间 s (范围: 200-1000)

未知组播丢弃 ▾

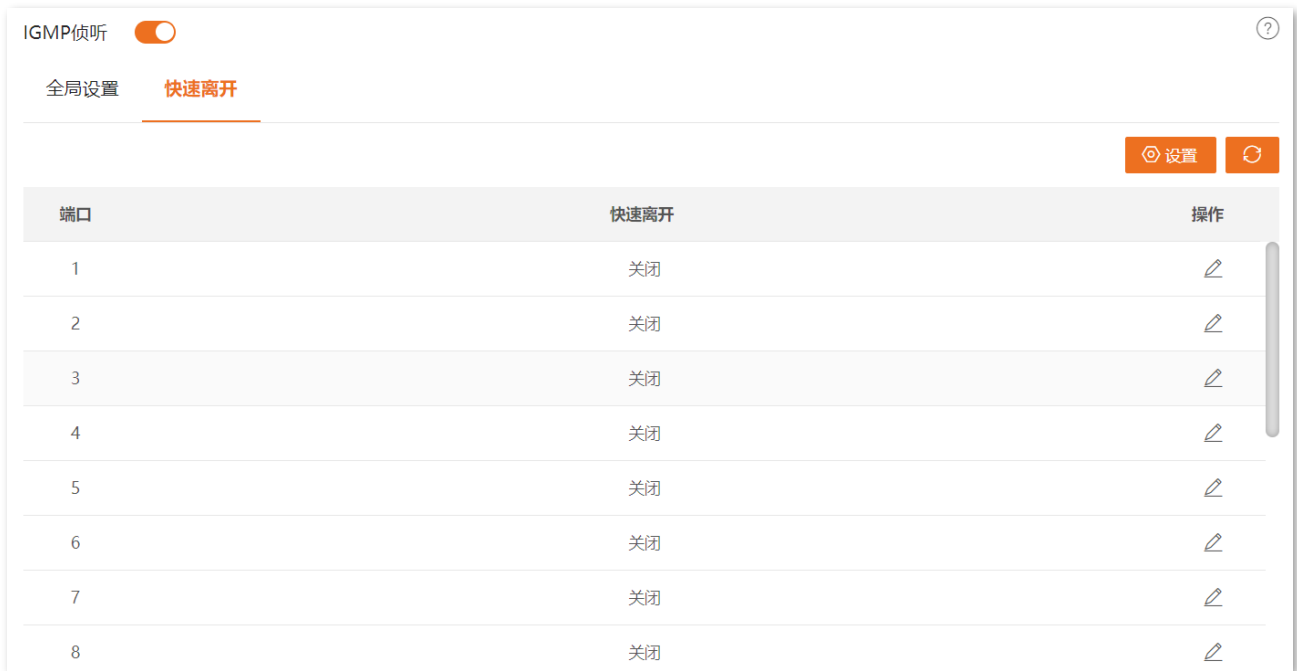
参数说明

标题项	说明
IGMP 侦听	开启或关闭 IGMP 侦听功能。

标题项	说明
VLAN ID	要开启 IGMP 侦听功能的 VLAN。
VLAN (所属 VLAN)	开启或关闭该 VLAN 的 IGMP 侦听功能。
组播 VLAN 状态	<p>开启或关闭该 VLAN 的组播状态。</p> <p>默认情况下，交换机组播 VLAN 为关闭状态，如果局域网内有多个不同 VLAN 的设备点播同一组播组，组播设备则需要为每个 VLAN 复制一份组播数据；开启后，组播设备只需发送一份组播数据到本交换机，由本交换机将其分发到组播数据的接收者，从而节省带宽资源和减少组播设备的负担。</p>
协议版本	<p>IGMP 侦听可处理的 IGMP 报文的版本。</p> <ul style="list-style-type: none">- v1: 只对 IGMPv1 版本的报文进行处理。- v2: 对 IGMPv1 和 IGMPv2 版本的报文进行处理。- v3: 可以对 IGMPv1、IGMPv2 和 IGMPv3 的报文进行处理。
路由端口老化时间	路由端口老化定时器时间。在该时间段内，路由端口没有收到 IGMP 普遍组查询报文，交换机将该端口从映射关系表中删除。
普遍组查询最大响应时间	普遍组查询的最大响应时间。交换机转发普遍组查询报文后，在该时间段内，端口未收到应该普遍组查询的 IGMP 成员关系报文时，则在映射关系表中将该端口删除。
特定组查询最大响应时间	特定组查询的最大响应时间。交换机向主机端口转发 IGMP 特定组查询报文后，在该时间段内，主机端口未收到主机响应该特定组查询的 IGMP 成员关系报文时，则在映射关系表中将该主机端口删除。
主机端口老化时间	主机端口老化定时器时间。在该时间段内，主机端口没有收到 IGMP 成员关系报文时，交换机将该端口从映射关系表中删除。
未知组播丢弃	开启未知组播丢弃后，交换机只向其路由端口转发未知组播数据报文，不在 VLAN 内广播；如果交换机没有路由端口，未知组播数据报文会被丢弃，不再转发。

4.6.3 快速离开

在「交换设置」>「IGMP 侦听」>「快速离开」页面，您可以配置各端口的快速离开模式。



参数说明

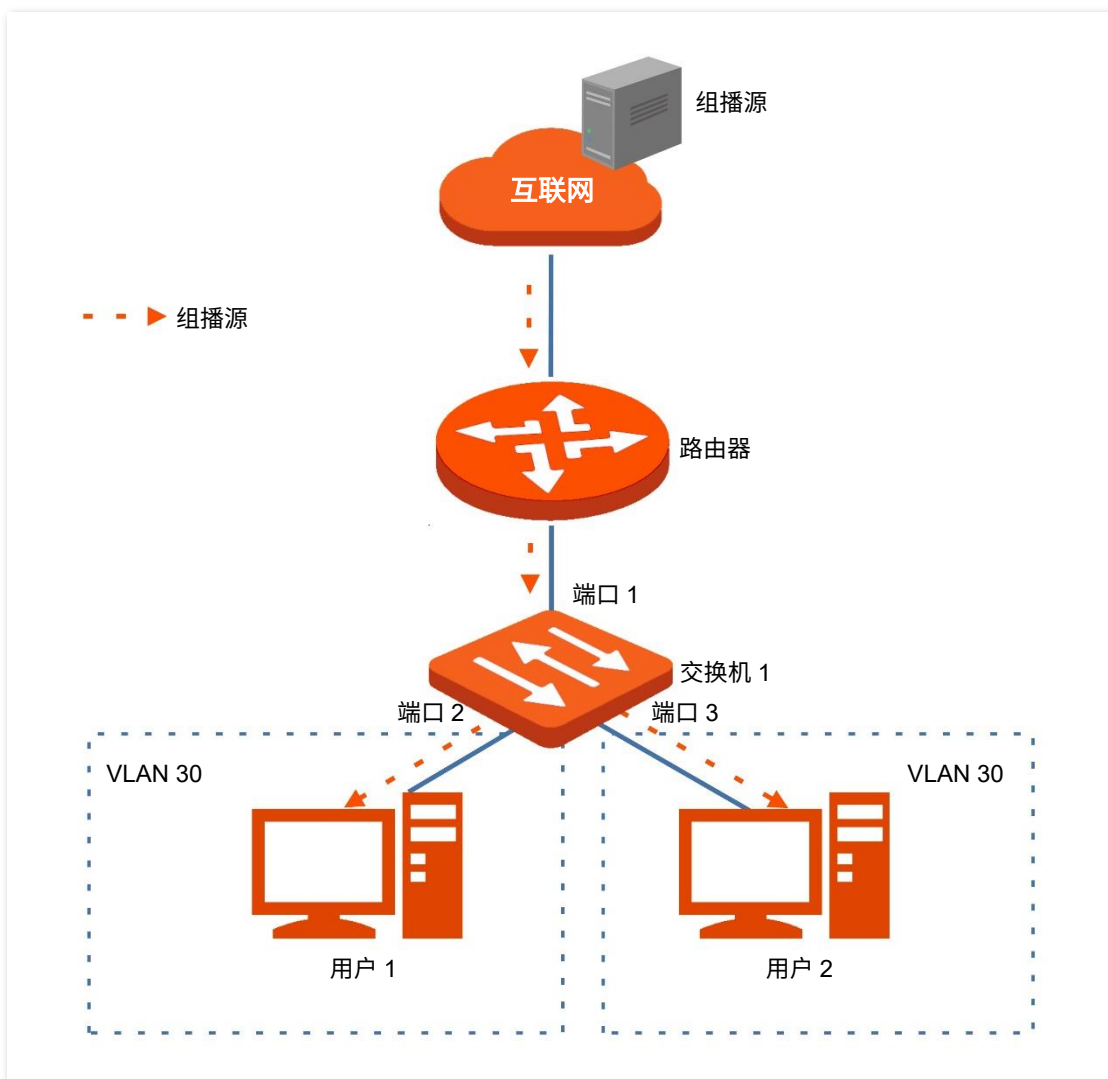
标题项	说明
端口	端口编号。
快速离开	开启端口的快速离开功能后，当交换机从该端口收到主机发送的离开某组播组的 IGMP 离开组报文时，直接把该端口从对应 IGMP 侦听组播转发表中删除，不用等到主机端口老化时间超时。

4.6.4 IGMP 侦听配置举例

组网需求

如下图所示，用户网络通过交换机接入组播网络。组播网络中的组播源向局域网用户提供组播视频服务，现在希望组播视频服务可以精准地转发给有组播视频服务需求的局域网用户（如用户 1 和用户 2），避免组播数据在局域网中广播而引起的网络带宽浪费和无法预知的网络信息安全问题。

路由器上已部署 IGMPv2，作为 IGMP 查询器。交换机为二层交换机，支持 IGMP Snooping。路由器和交换机之间用于传输组播数据的业务 VLAN 为 VLAN 10，下游用户 1 属于 VLAN 20，用户 2 属于 VLAN 30。



方案设计

要实现上述需求，可以在交换机上：

- 将端口 1、2、3 以 Hybrid 方式分别加入 VLAN 10、20、30。

- 开启全局和 VLAN 10、20、30 的 IGMP 侦听功能，使交换机可以在 VLAN 内建立和维护二层组播转发表，指导组播数据只转发给有组播数据需求的用户。
- 配置 VLAN 10 为组播 VLAN，对于不同 VLAN 的用户同时点播同一组播组时，路由器只需将组播数据通过组播 VLAN 向交换机发送一份即可，而不必向每个 VLAN 都复制一份，从而节省了网络带宽，也减轻了路由器的负担。
- 配置 VLAN 10、20、30 的 IGMP 侦听版本为 v2，使其可以处理 VLAN 内的 IGMPv1、IGMPv2 报文。
- 开启端口 2、3 的快速离开功能，当交换机从端口 2、3 收到用户主机发送的离开某组播组的 IGMP 离开组报文时，直接把该端口从对应 IGMP 侦听组播转发表中删除，不用等到主机端口老化时间超时。

配置步骤

步骤 1 [登录到交换机 Web 管理页面](#)。

步骤 2 配置 VLAN。

将端口 1、2、3 以 Hybrid 方式分别加入 VLAN10、20、30。具体配置信息如下。

端口	链路类型	PVID	Tagged	Untagged
端口 1	Hybrid	10	/	10,20,30
端口 2	Hybrid	20	/	10,20
端口 3	Hybrid	30	/	10,30

1. 添加 VLAN10、20、30。

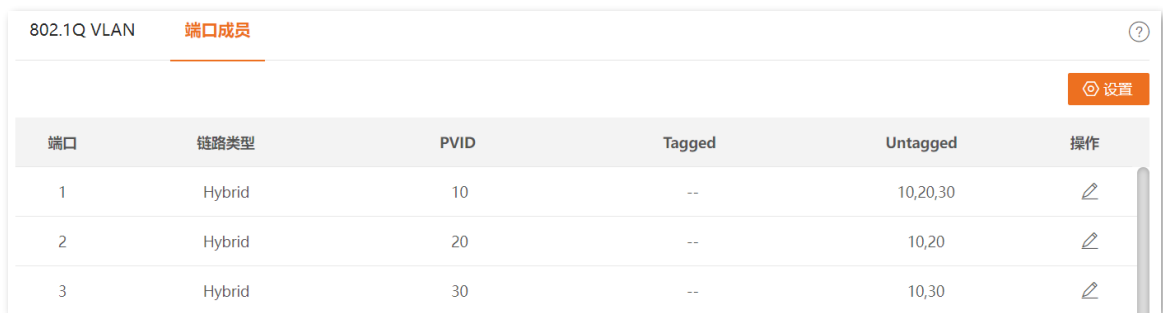
(1) 点击「常用功能」>「VLAN 划分」>「802.1Q VLAN」。




(2) 点击 **+ 添加**，配置如下 3 条 VLAN。



2. 将端口 1、2、3 以 Hybrid 方式分别加入 VLAN10、20、30。

- (1) 点击「常用功能」>「VLAN 划分」>「端口成员」。
- (2) 点击端口 1 后面的  按钮，设置“链路类型”为“Hybrid”，“PVID”为“10”，“Untagged”为“10,20,30”，点击 **确定**。
- (3) 点击端口 2 后面的  按钮，设置“链路类型”为“Hybrid”，“PVID”为“20”，“Untagged”为“10,20”，点击 **确定**。
- (4) 点击端口 3 后面的  按钮，设置“链路类型”为“Hybrid”，“PVID”为“30”，“Untagged”为“10,30”，点击 **确定**。



端口	链路类型	PVID	Tagged	Untagged	操作
1	Hybrid	10	--	10,20,30	
2	Hybrid	20	--	10,20	
3	Hybrid	30	--	10,30	

步骤 3 开启全局 IGMP 侦听功能。

1. 点击「交换设置」>「IGMP 侦听」。
2. 打开“IGMP 侦听”开关。
3. 点击 **确定**。



步骤 4 配置 VLAN 10、20、30 的 IGMP 侦听功能。

配置 VLAN 10、20、30 的 IGMP 侦听功能。具体配置信息如下。

VLAN ID	VLAN	组播 VLAN 状态	协议版本	路由端口老化时间	普遍组查询最大响应时间	特定组查询最大响应时间	主机端口老化时间	未知组播丢弃
10	开启	开启	v3	260	10	2	260	关闭
20	开启	关闭	v3	260	10	2	260	关闭
30	开启	关闭	v3	260	10	2	260	关闭

1. 配置 VLAN 10 的 IGMP 侦听功能。

- (1) 点击「交换设置」>「IGMP 侦听」>「全局设置」。
- (2) 在“VLAN ID”下拉框中选择“10”。
- (3) 在“VLAN”下拉框中选择“开启”。
- (4) 在“组播 VLAN 状态”下拉框中选择“开启”。
- (5) 在“协议版本”下拉框中选择“v2”。
- (6) 设置路由端口老化时间，本例保持默认设置。可根据实际情况修改。
- (7) 设置普遍组查询最大响应时间，本例保持默认设置。可根据实际情况修改。
- (8) 设置特定组查询最大响应时间，本例保持默认设置。可根据实际情况修改。
- (9) 设置主机端口老化时间，本例保持默认设置。可根据实际情况修改。
- (10) “未知组播丢弃”保持默认设置，为“关闭”。
- (11) 点击 **确定**。

The screenshot shows the 'IGMP侦听' (IGMP Snooping) configuration page with the '全局设置' (Global Settings) tab selected. The 'IGMP侦听' toggle is turned on. The configuration items are as follows:

VLAN ID	10	▼
所属VLAN	开启	▼
组播VLAN状态	开启	▼
协议版本	v2	▼
路由端口老化时间	260	s (范围: 1-1000)
普遍组查询最大响应时间	10	s (范围: 1-25)
特定组查询最大响应时间	2	s (范围: 1-5)
主机端口老化时间	260	s (范围: 200-1000)
未知组播丢弃	关闭	▼

At the bottom of the form is a '确定' (Confirm) button.

2. 参考配置步骤 4 中的 [1](#)，配置 VLAN 20、30 的 IGMP 侦听功能。

步骤 5 开启端口 2、3 的快速离开功能。

1. 点击「交换设置」>「IGMP 侦听」>「快速离开」。
2. 点击 **设置**，勾选端口 2、3，在“快速离开”下拉框中选择“开启”，点击 **确定**。

The screenshot shows the 'IGMP侦听' (IGMP Snooping) configuration page with the '快速离开' (Quick Leave) tab selected. The 'IGMP侦听' toggle is turned on. In the top right corner, there are '设置' (Settings) and '刷新' (Refresh) buttons. Below is a table with columns for '端口' (Port), '快速离开' (Quick Leave), and '操作' (Action).

端口	快速离开	操作
1	关闭	✎
2	开启	✎
3	开启	✎
4	关闭	✎

A dashed red box highlights the rows for ports 2 and 3.

步骤 6 保存全局配置。

点击管理页面右上角的 **保存配置** 进行全局保存。

---完成

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。

不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

验证配置

完成以上配置后，组播视频服务可以精准地转发给有组播视频服务需求的局域网用户，防止组播数据在二层网络中广播。

同时，对于 VLAN 20、30 的用户同时点播同一组播组时，路由器只需将组播数据通过组播 VLAN 10 向交换机发送一份即可，而不必向每个 VLAN 都复制一份，省了网络带宽，也减轻了路由器的负担。

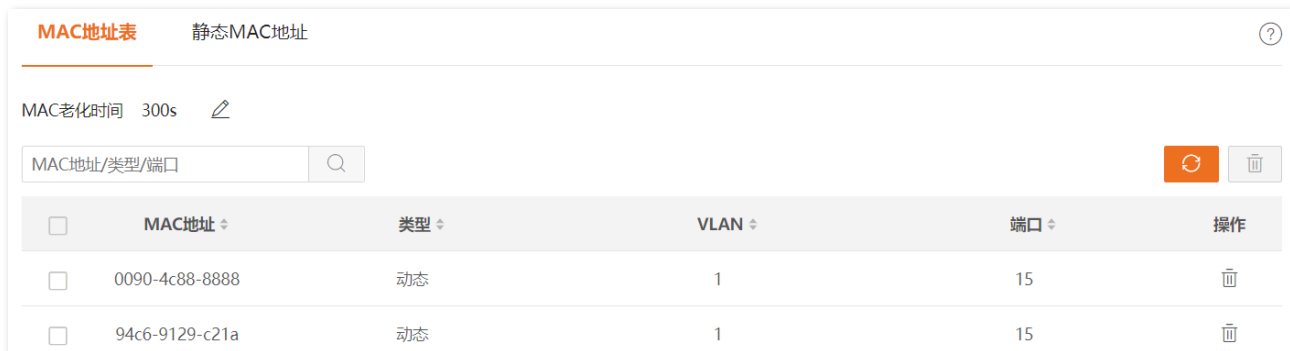
4.7 MAC 设置

4.7.1 MAC 地址表

交换机通过地址学习机制，创建 MAC 地址转发表，表项中包含：MAC 地址、VLAN ID、端口号。当交换机在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：

- 单播方式：当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文从该表项中的端口发送。
- 广播方式：当交换机收到目的 MAC 地址第二字节最低位为 1 的报文，或 MAC 地址转发表中没有包含对应报文目的 MAC 地址的表项时，交换机将采取广播方式将报文向除接收端口外的所有端口转发。即广播报文、组播报文、未知单播报文都将广播转发。

在「交换设置」>「MAC 设置」>「MAC 地址表」页面中，您可以查看和删除 MAC 地址表项。



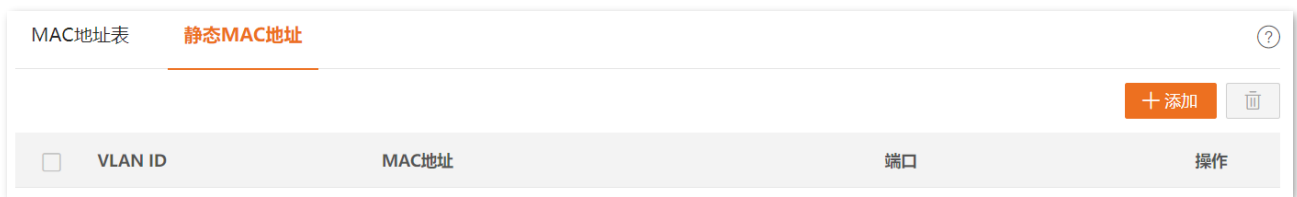
参数说明

标题项	说明
MAC 老化时间	MAC 地址表项的老化时间，只对动态类型的表项有效。 当交换机距离上一次收到源地址与表项中的源 MAC 地址一致的报文的时间超过老化时间时，自动把该 MAC 地址表项删除。
MAC 地址	MAC 地址，格式为 XXXX-XXXX-XXXX。
类型	该 MAC 地址的类型。 <ul style="list-style-type: none">- 静态：管理员手动配置的 MAC 地址表项。- 动态：交换机自动生成的 MAC 地址表项。

标题项	说明
VLAN	该 MAC 地址所属的 VLAN。
端口	该 MAC 地址所在的交换机物理端口。

4.7.2 静态 MAC 地址

在「交换设置」>「MAC 设置」>「静态 MAC 地址」页面中，您可以配置静态 MAC 地址表项。配置后会在 MAC 地址表中以静态类型表项存在，不受 MAC 老化时间限制。



参数说明

标题项	说明
VLAN ID	MAC 地址所属 VLAN。
MAC 地址	MAC 地址，格式为 XXXX-XXXX-XXXX。
端口	该 MAC 地址所在的交换机物理端口。

5 路由设置

5.1 静态路由

5.1.1 概述

静态路由是由管理员手动设置的固定的路由，一般用在网络规模不大、网络拓扑固定的网络中。静态路由的优点为简单、高效、可靠，所以合理的配置静态路由可以提高数据包的转发速度；但静态路由不能自动适应网络拓扑变化，当网络发生故障或网络拓扑变化时，则需要管理员手动修改静态路由配置。



在所有路由中，静态路由由优先级最高。

5.1.2 配置 IPv4 静态路由

在「路由设置」>「静态路由」>「静态路由」页面中，您可以查看和配置 IPv4 静态路由规则。

静态路由		IPv6静态路由		
<input type="checkbox"/>	目的地址	子网掩码	下一跳	操作
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.0.252	

参数说明

标题项	说明
目的地址	目的网络的 IPv4 网段/地址。
子网掩码	目的网络的子网掩码。
下一跳	数据包从本交换机出去后，下一跳路由的入口的 IPv4 地址。

5.1.3 配置 IPv6 静态路由

在「路由设置」>「静态路由」>「IPv6 静态路由」页面中，您可以查看和配置 IPv6 静态路由规则。



参数说明

标题项	说明
目的地址	目的网络的 IPv6 网段/地址。
前缀长度	目的网络的前缀长度。
下一跳	数据包从本交换机出去后，下一跳路由的入口的 IPv6 地址。

5.1.4 IPv4 静态路由配置举例

组网需求

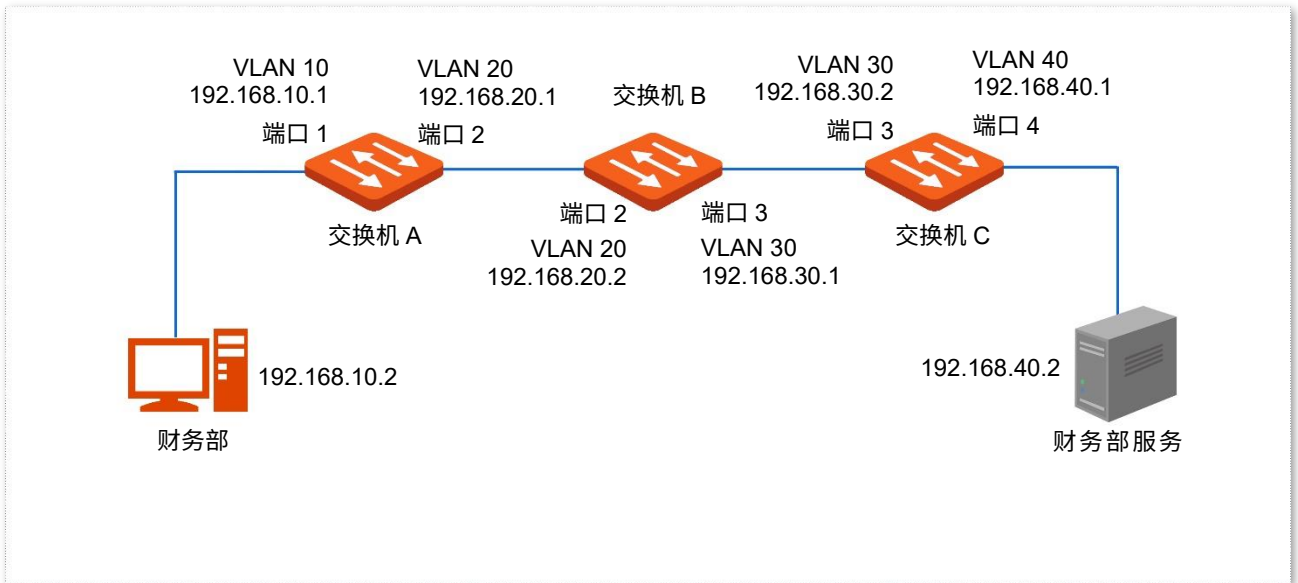
某公司财务部的员工在二楼，财务部的服务器在三楼，现在要实现财务部员工可以访问财务部服务器。

方案设计

采用如下思路进行配置：

- 交换机上创建 VLAN 并配置各 VLAN 接口的 IP 地址、配置各端口所属 VLAN，实现相邻设备网络互通。
- 交换机上配置静态路由，实现不同网段互通。
- 为财务部服务器静态分配 IP 地址，防止因 IP 地址改变，财务部员工无法访问财务部服务器。
- 财务部员工的电脑设置为“自动获得 IP 地址，自动获得 DNS 服务器地址”，通过 DHCP 动态获取 IP 地址。假设某财务部员工的电脑获取的 IP 地址信息如下：
 - IP 地址：192.168.10.2

- 子网掩码：255.255.255.0
- 默认网关：192.168.10.1



配置步骤

一、配置交换机

步骤 1 配置 VLAN。

为交换机 A、B、C 分别设置 VLAN，假设各交换机的 VLAN 配置信息如下。

交换机	端口	VLAN	IP 地址
交换机 A	1	10	192.168.10.1/24
	2	20	192.168.20.1/24
交换机 B	2	20	192.168.20.2/24
	3	30	192.168.30.1/24
交换机 C	3	30	192.168.30.2/24
	4	40	192.168.40.1/24

下面以配置交换机 A 为例，交换机 B 与交换机 C 的配置与交换机 A 类似。

1. 添加 VLAN。

- (1) [进入交换机 A Web 管理页面](#)，点击「常用功能」>「VLAN 划分」>「802.1Q VLAN」。
- (2) 点击 **+ 添加**，配置如下 2 条 VLAN。

VLAN ID	VLAN描述	IPv4地址	子网掩码	操作
1	default	192.168.0.11	255.255.255.0	
10	VLAN0010	192.168.10.1	255.255.255.0	
20	VLAN0020	192.168.20.1	255.255.255.0	

2. 配置端口属性。

- (1) [进入交换机 A Web 管理页面](#)，点击「常用功能」>「VLAN 划分」>「端口成员」。
- (2) 点击端口 1 后面的 按钮，设置“PVID”为“10”。
- (3) 点击端口 2 后面的 按钮，设置“PVID”为“20”。

端口	链路类型	PVID	Tagged	Untagged	操作
1	Access	10	--	10	
2	Access	20	--	20	

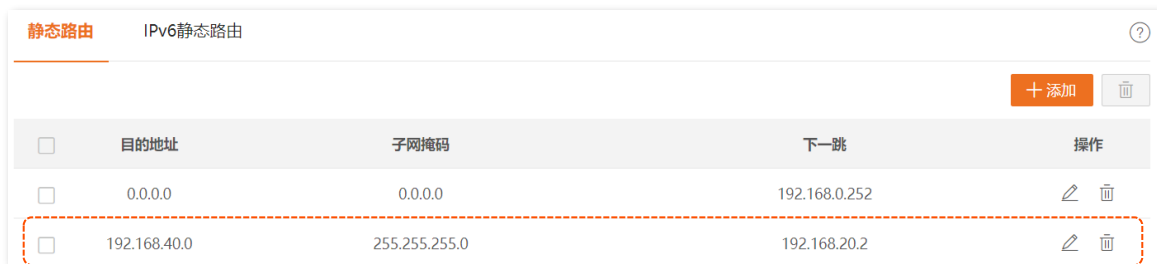
步骤 2 配置静态路由。

为交换机 A、B、C 分别设置静态路由，假设各交换机的静态路由配置信息如下。

交换机	目的地址	子网掩码	下一跳
交换机 A	192.168.40.0	255.255.255.0	192.168.20.2
交换机 B	192.168.40.0	255.255.255.0	192.168.30.2
	192.168.10.0	255.255.255.0	192.168.20.1
交换机 C	192.168.10.0	255.255.255.0	192.168.30.1

下面以配置交换机 A 为例，交换机 B 与交换机 C 的配置与交换机 A 类似。

1. [进入交换机 A Web 管理页面](#)，点击「路由设置」>「静态路由」>「静态路由」。
2. 点击 添加，配置如下 1 条静态路由。



步骤 3 为财务部员工的电脑动态分配 IP 地址。

1. [进入交换机 A Web 管理页面](#)，点击「路由设置」>「DHCP 服务器」。
2. 打开“DHCP 服务器”开关，并打开 VLAN10 接口的“DHCP 使能”开关。
3. 点击 **+ 添加**，配置如下 1 条 DHCP 地址池。



步骤 4 保存配置。

点击管理页面右上角的 **保存配置** 进行全局保存。

二、配置财务部服务器的 IP 地址与网关

为财务部服务器静态分配 IP 地址，配置信息如下。

设备	IP 地址	子网掩码	默认网关
财务部服务器	192.168.40.2	255.255.255.0	192.168.40.1

---完成

验证配置

完成以上配置后，财务部员工的电脑可以正常访问财务部服务器。

5.2 动态路由



OSPF 动态路由需要通过命令行进行配置。

5.2.1 概述

RIP (Routing Information Protocol, 路由信息协议) 和 OSPF (Open Shortest Path First, 开放最短路径优先) 是两种动态路由协议。RIP 是一种较为简单的内部网关协议, 相比 OSPF 来说, 易于管理和维护, 一般用于校园网等规模不大的网络。

■ RIP 基本原理

RIP 定义了两种类型的报文:

- 请求报文: 向相邻路由设备请求整个或部分路由表信息。
- 响应报文: 响应相邻路由设备的请求报文, 或者周期性主动向相邻设备发送的更新报文。

RIP 路由表初始时仅包含本交换机的直连接口路由信息, 须通过与相邻路由设备互相学习路由表项, 最终生成自己的 RIP 路由表, 具体步骤如下。

- (1) RIP 初始化时, 本交换机会从每个开启了 RIP 功能的接口发送请求报文, 该请求报文包含本交换机的整个路由表信息。
- (2) 相邻的路由设备接收到请求报文后, 响应请求, 回送包含本设备的路由表信息的响应报文。
- (3) 本交换机接收到响应报文后, 更新自己的路由表, 同时向相邻的路由设备发送更新 (响应) 报文。相邻路由设备在接收到的更新报文后, 又向各自的相邻路由设备发送更新报文。

经过一连串的报文交互, 本交换机的 RIP 路由表生成, 且各路由设备都能得到并保持最新的路由信息。在此之后, 本交换机周期性地发送更新报文进行路由更新, 同时启用老化机制对超时的路由老化处理, 以保证路由表的实时性和有效性。

■ RIP 版本

RIP 有 RIPv1 和 RIPv2 两个版本。

RIPv1 为有类别路由协议, 只支持以广播方式发送协议报文。RIPv1 的协议报文无法携带掩码信息, 它只能识别 A、B、C 类这样的自然网段的路由, 因此 RIPv1 不支持不连续子网。

RIPv2 为无类别路由协议, 向后兼容 RIPv1。与 RIPv1 相比, 具有如下优势。

- 支持路由标记，在路由策略中可根据路由标记对路由进行灵活的控制。
- 携带掩码信息，支持路由聚合和无类域间路由。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播发送更新报文，可以减少资源消耗。
- 支持对协议报文进行认证，提供 Simple 和 MD5 两种认证模式，验证更新报文的发送源的合法性，增强安全性。

5.2.2 RIP 动态路由

在「路由设置」>「动态路由」页面中，您可以查看和配置 RIP 动态路由规则。



参数说明

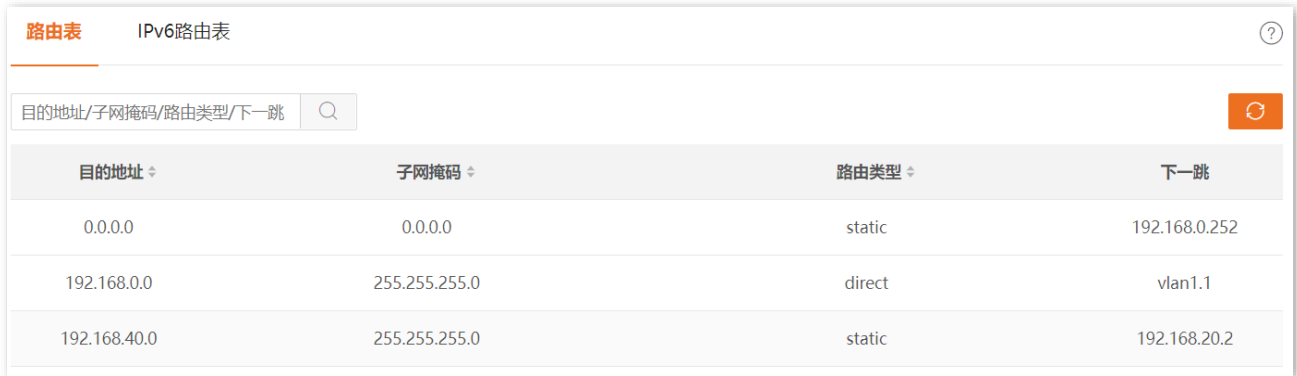
标题项	说明
路由引入	勾选后，交换机可以将其他进程或协议的路由信息引入到 RIP 路由表中，从而丰富 RIP 路由表。当前支持引入直连路由、静态路由和 OSPF 路由信息。
RIP 生效网段	网段 子网掩码 开启 RIP 功能的 IP 地址段，该 IP 地址段内的交换机接口都支持 RIP 协议。
接口配置	VLAN 接口 运行 RIP 协议的 VLAN 接口。

标题项	说明
发送报文	<p>VLAN 接口发送的 RIP 协议报文的版本。</p> <ul style="list-style-type: none">- 不发送：本接口不发送 RIP 协议报文。- RIPv1：本接口发送 RIPv1 版本的请求报文和响应报文。- RIPv2：本接口以组播方式发送 RIPv2 版本的请求报文和响应报文。- RIPv2 广播：本接口以广播方式发送 RIPv2 版本的请求报文和响应报文。
接收报文	<p>VLAN 接口支持接收的 RIP 协议报文的版本。</p> <ul style="list-style-type: none">- 不接收：本接口不接收 RIP 协议报文。- RIPv1：本接口只接收 RIPv1 版本的请求报文和响应报文。- RIPv2：本接口只接收 RIPv2 版本的请求报文和响应报文。- RIPv1&RIPv2：本接口接收 RIPv1 和 RIPv2 版本的请求报文和响应报文。
认证模式	<p>VLAN 接口在接收和发送 RIP 报文时使用的认证模式。只有认证模式和认证密码相同的路由设备才能互相交换路由信息。</p> <ul style="list-style-type: none">- 不认证：接口不开启认证功能。- Simple：接口开启简单认证。该接口在发送 RIP 报文时会将 密码 添加到报文首部，用于对端路由设备认证；同时该接口对接收到的 RIP 报文根据 密码 进行认证，认证通过后会响应。- MD5：接口开启 MD5 认证。该接口在发送 RIP 报文时会将 keyID 和 密码 添加到报文首部，用于对端路由设备认证；同时该接口对接收到的 RIP 报文根据 keyID 和 密码 进行认证，认证通过后会响应。
	<p> 注意</p> <p>由于 RIPv1 协议不支持认证，当发送报文或接收报文支持 RIPv1 时，该配置不生效。</p>
keyID	认证模式为 MD5 时需要填入。
密码	开启了接口认证时需要填入。
接口 RIP 状态	VLAN 接口的 RIP 协议运行状态。

5.3 路由表

5.3.1 查看 IPv4 路由表

在「路由设置」>「路由表」>「路由表」页面中，您可以查看本交换机的 IPv4 路由表。此路由表包含交换机学习到的所有路由信息，包括直连路由、静态路由、动态路由。



目的地址	子网掩码	路由类型	下一跳
0.0.0.0	0.0.0.0	static	192.168.0.252
192.168.0.0	255.255.255.0	direct	vlan1.1
192.168.40.0	255.255.255.0	static	192.168.20.2

标题项	说明
目的地址	<p>目的网络的 IP 地址。目的地址和子网掩码均为“0.0.0.0”表示默认路由。</p> <p> 提示</p> <p>当在路由表中找不到与数据包的目的地址精确匹配的路由时，交换机会选择默认路由来转发该数据包。</p>
子网掩码	<p>目的网络的子网掩码。</p>
路由类型	<p>此条路由的类型。</p> <ul style="list-style-type: none">- direct: 直连路由。- static: 静态路由。- RIP: RIP 动态路由。- OSPF: OSPF 动态路由。
下一跳	<p>数据包从本交换机出去后，下一跳路由的入口的 IPv4 地址。</p>

5.3.2 查看 IPv6 路由表

在「路由设置」>「路由表」>「IPv6 路由表」页面中，您可以查看本交换机的 IPv6 路由表。此路由表包含交换机学习到的所有路由信息，包括直连路由、静态路由、动态路由。



目的地址	前缀长度	路由类型	下一跳
fe80::	64	direct	vlan1.1

标题项	说明
目的地址	<p>目的网络的 IP 地址。“.”表示默认路由。</p> <p> 提示</p> <p>当在路由表中找不到与数据包的目的地址精确匹配的路由时，交换机会选择默认路由来转发该数据包。</p>
前缀长度	<p>目的网络的前缀长度。</p>
路由类型	<p>此条路由的类型。</p> <ul style="list-style-type: none">- direct: 直连路由。- static: 静态路由。- RIP: RIP 动态路由。- OSPF: OSPF 动态路由。
下一跳	<p>数据包从本交换机出去后，下一跳路由的入口的 IPv6 地址。</p>

5.4 ARP

数据传输过程中，IP 地址只是主机在网络层中的地址，如果要将网络层中数据包传送给目的主机，必须知道目的主机的数据链路层地址（比如以太网网络 MAC 地址）。

ARP（Address Resolution Protocol，地址解析协议）用于将 IP 地址解析为 MAC 地址，并在交换机内部维护一张 ARP 表，记录最近与本交换机通信的其它主机的 MAC 地址与 IP 地址的对应关系。当交换机需要与目标主机通信时，首先进行 ARP 地址解析，具体步骤如下：

- (1) 交换机在自己的 ARP 表中查询是否存在目标主机的 IP 地址与 MAC 地址对应规则。如果是，则按照查询到的规则向目标主机发送数据；如果否，交换机则在局域网的数据链路层内广播一份“ARP 请求”的数据帧，该请求包含交换机自己的 IP 地址和 MAC 地址，以及目的主机的 IP 地址。
- (2) 局域网设备都会接收到该请求，当目的主机收到该请求时，会给交换机回应一个“ARP 应答”，该帧包含目的主机的 MAC 地址。
- (3) 交换机收到该 ARP 应答后，将目的主机的 IP 地址和 MAC 地址对应关系写入自己的 ARP 表中，以便后续继续使用。

在「路由设置」>「ARP」页面中，您可以查看和配置 ARP 表。

IP地址	MAC地址	VLAN ID	类型	老化时间	操作
192.168.0.125	94c6.9129.c21a	vlan1.1	动态	920s	删除
192.168.0.252	0090.4c88.8888	vlan1.1	动态	1200s	删除

参数说明

标题项	说明
ARP 老化时间	ARP 表项的老化时间。当交换机在该时间内未收到相应的 ARP 报文，则将该 ARP 表项从 ARP 表中删除。
IP 地址	主机的 IP 地址。
MAC 地址	IP 地址对应主机的 MAC 地址。
VLAN ID	该 ARP 表项所在的 vlan 三层接口。

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。

不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

标题项	说明
	该表项的类型。
类型	<ul style="list-style-type: none">- 动态：交换机根据 ARP 协议自动生成的 ARP 表项，生命周期为 ARP 老化时间。- 静态：手动配置的 ARP 表项，永久有效，不受 ARP 老化时间限制。
老化时间	该 ARP 表项的剩余老化时间。

5.5 DHCP 服务器

5.5.1 概述

不断增长的网络需求，使得网络规模不断扩大和网络复杂度提高，经常会导致计算机数量超过可分配 IP 地址的数量。同时无线网络的普及，无线设备的位置会时常变化，导致设备 IP 地址需要时常更新。而 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通过 IP 地址动态分配策略可以解决上述问题。



本交换机的 DHCP 服务器暂不支持基于 Option 82 选项进行地址分配。

IP 地址分配策略

针对客户端的不同需求，DHCP 服务器提供两种 IP 地址分配策略：

- 动态地址分配：DHCP 服务器为客户端分配有效期限的 IP 地址，到达使用期限后，客户端需要重新申请地址。绝大多数客户端得到的都是这种动态分配的地址。
- 静态地址分配：由管理员为少数特定客户端静态绑定固定的 IP 地址。让 DHCP 服务器始终分配某一固定 IP 地址给客户端，可以避免一些基于 IP 地址生效的功能因客户端 IP 地址变化而失效。

5.5.2 DHCP 设置

在「路由设置」>「DHCP 服务器」>「DHCP 设置」页面中，您可以查看和配置 DHCP 服务器。

The screenshot shows the DHCP configuration page with the following sections:

- DHCP 设置** (DHCP Settings): Includes tabs for '静态地址分配' (Static IP Allocation) and '客户端列表' (Client List). A 'DHCP 服务器' (DHCP Server) toggle switch is turned on.
- 地址池** (Address Pools): A table with columns: 地址池名称 (Address Pool Name), 地址范围 (Address Range), 子网掩码 (Subnet Mask), 默认网关 (Default Gateway), 租约时间 (Lease Time), DNS, 不分配的IP段 (Unassigned IP Range), and 操作 (Actions). One pool named 'caigoubu' is listed with range 192.168.10.2 ~ 192.168.10.250, subnet 255.255.255.0, gateway 192.168.10.1, and lease time 30 minutes.
- 接口使能DHCP** (Interface DHCP Enablement): A table with columns: VLAN接口 (VLAN Interface), 三层接口 (Layer 3 Interface), 子网掩码 (Subnet Mask), and DHCP使能 (DHCP Enable). Three interfaces (1, 10, 20) are listed with their respective layer 3 interfaces and subnet masks. Interface 10 has DHCP enabled.

参数说明

标题项	说明
DHCP 服务器	开启或关闭 DHCP 服务器功能。
地址池名称	地址池策略的名称。
地址范围	可分配的 IP 地址范围。
子网掩码	分配给客户端的子网掩码。
默认网关	分配给客户端的默认网关。
地址池	<p>分配给客户端的 IP 地址的有效时间。当 IP 地址到期后：</p> <ul style="list-style-type: none"> 如果该客户端仍连接在交换机上，客户端将自动续约，继续占用该 IP 地址。
租约时间	<ul style="list-style-type: none"> 如果客户端未连接（关机、网线已拔掉等）到交换机，交换机将释放该 IP 地址。以后若有其它客户端请求 IP 地址信息，交换机可将该 IP 地址分配给其它客户端。 <p>为减少交换机的资源消耗，请根据实际网络环境合理设置租约时间，减少报文发送次数。如无特殊需要，建议设置为“1 天”。</p>

标题项	说明	
DNS	分配给客户端的 DNS 服务器。	
不分配的 IP 段	地址池中不进行动态分配的 IP 地址。	
VLAN 接口	地址池策略生效的 VLAN。	
接口使能	三层接口	VLAN 接口的 IP 地址。
DHCP	子网掩码	VLAN 接口的子网掩码。
DHCP 使能	开启后，VLAN 接口的 DHCP 服务器生效。	

5.5.3 静态地址分配

在「路由设置」>「DHCP 服务器」>「静态地址分配」页面中，您可以查看和配置静态地址分配策略。



参数说明

标题项	说明
客户端名称	静态地址分配策略的备注信息，若是从客户端列表绑定过来的，则显示客户端的设备名称，也可自定义。
客户端 IP	DHCP 服务器固定分配给该客户端的 IP 地址。
客户端 MAC	客户端的 MAC 地址。

5.5.4 客户端列表

在「路由设置」>「DHCP 服务器」>「客户端列表」页面中，您可以对从本交换机获取 IP 地址的设备进行以下操作：

- 查看客户端名称、获取的 IP 地址等信息。
- 点击[绑定](#)按钮，可以将分配好的 IP 地址加入到静态分配列表，使 DHCP 服务器始终给该设备分配同一个 IP 地址。

客户端名称	已分配IP	客户端MAC	剩余时间	分配方式	操作
暂无数据					

参数说明

标题项	说明
客户端名称	客户端的名称。
已分配 IP	DHCP 服务器分配给该客户端的 IP 地址。
客户端 MAC	客户端的 MAC 地址。
剩余时间	租约剩余时间。
分配方式	DHCP 服务器给该客户端分配 IP 地址的策略。 <ul style="list-style-type: none">- 动态：DHCP 服务器使用动态 IP 地址分配策略给该客户端分配 IP 地址。- 静态：DHCP 服务器使用静态 IP 地址分配策略给该客户端静态地址分配。

5.6 IPv6 设置

5.6.1 概述

IPv6 (Internet Protocol Version 6) 是网络层协议的第二代标准协议，属于 IPv4 的升级版，解决了当前 IPv4 在地址空间等方面的不足之处。

IPv6 地址的结构

IPv6 地址总长度为 128 比特，通常分为 8 组，每组为 4 个十六进制数的形式，每组十六进制数间用冒号分隔。一个 IPv6 地址可以分为如下两部分：

- 网络前缀：n 比特，相当于 IPv4 地址中的网络 ID。
- 接口标识：128-n 比特，相当于 IPv4 地址中的主机 ID。

网络前缀生成方式

IPv6 地址的网络前缀可以通过四种方法生成：

- 手动分配：手动进行配置。
- 无状态获取：通过 RS (Router Solicitation, 路由器请求)、RA (Router Advertisement, 路由器通告) 报文与路由器进行交互获得对应的前缀。
- 有状态获取：通过 DHCPv6 服务器获取对应的前缀。
- 设备随机生成：设备系统自动生成。

接口标识生成方式

IPv6 地址的接口标识可通过三种方法生成：

- 手动分配：手动进行配置。
- 设备随机生成：设备系统自动生成。
- IEEE EUI-64 标准生成：IEEE EUI-64 标准采用接口的 MAC 地址生成 IPv6 接口标识，是生成接口标识最常用的方式。

MAC 地址的前 24 位代表厂商标识，后 24 位代表制造商分配的唯一扩展标识。MAC 地址的第七高位是一个 U/L 位，值为 1 时表示 MAC 地址全球唯一，值为 0 时表示 MAC 地址本地唯一。

MAC 地址向 EUI-64 格式的转换过程：在 MAC 地址的前 24 位和后 24 位之间插入 FFFE，然后将 U/L 位的值从 0 改为 1，这样就生成一个 64 比特的接口标识，且接口标识的值全球唯一。

IPv6 全球单播地址

全球单播地址是带有全球单播前缀的 IPv6 地址，其作用类似于 IPv4 中的公网地址，可以在 IPv6 网络上进行全局路由和访问。这种地址类型允许路由前缀的聚合，从而限制了全球路由表项的数量。

全球单播地址由全球路由前缀（Global routing prefix）、子网 ID（Subnet ID）和接口标识（Interface ID）组成。

- 全球路由前缀：由提供商（Provider）指定给一个组织机构，通常全球路由前缀至少为 48 位。目前已经分配的全球路由前缀的前 3bit 均为 001。
- 子网 ID：组织机构可以用子网 ID 来构建本地网络（Site）。子网 ID 通常最多分配到第 64 位。子网 ID 和 IPv4 中的子网号作用相似。
- 接口标识。用来标识一个设备（Host）。

链路本地地址

链路本地地址用于在同一网络中的 IPv6 计算机进行通信。在 IPv6 邻居节点之间的通信协议中广泛应用，如邻居发现协议、动态路由协议等。

链路本地地址由一个特定的前缀和接口 ID 两部分组成。其特定的链路本地前缀为 FE80::/64，接口标识通过 IEEE EUI-64 标准生成。

ND 协议

ND（Neighbor Discovery，邻居发现）协议是 IPv6 的一个关键协议，它综合了 IPv4 中的 ARP、ICMP 路由器发现和 ICMP 重定向等协议，并对它们做了改进。作为 IPv6 的基础性协议，ND 协议还提供了前缀发现、邻居不可达检测、重复地址检测、地址自动配置等功能。

5.6.2 IPv6 接口设置

在「路由设置」>「IPv6 设置」>「IPv6 接口设置」页面中，您可以配置交换机 VLAN 接口的 IPv6 全球单播地址。

IPv6接口设置		IPv6 ND设置							
								+ 添加	🗑️
<input type="checkbox"/>	接口	生成树状态	IPv6单播地址	类型	前缀长度	链路本地地址	RA自动配置	操作	
<input type="checkbox"/>	1	UP	--	--	--	fe80::2e0:4cff:fe11:1111	未启用	--	

参数说明

标题项	说明
接口	交换机 VLAN 接口。
生成树状态	接口的工作状态。包含 UP、DOWN 两种状态。
IPv6 全球单播地址	交换机 VLAN 接口的 IPv6 全球单播地址。 本交换机 IPv6 全球单播地址的网络前缀仅支持手动配置，接口标识支持手动配置或 IEEE EUI-64 标准自动生成。
类型	IPv6 全球单播地址的接口标识的生成方式。 <ul style="list-style-type: none"> - 手动分配：手动进行配置。您需在“IPv6 全球单播地址”输入框中手动输入完整的 IPv6 全球单播地址。 - EUI-64 生成：由 IEEE EUI-64 标准自动生成。您在“IPv6 全球单播地址”输入框中手动输入 IPv6 全球单播地址的网络前缀即可。 <p> 提示</p> <p>当“类型”选择“EUI-64 生成”，即使您在“IPv6 全球单播地址”输入框中手动输入完整的 IPv6 全球单播地址，保存配置后，IPv6 全球单播地址的接口标识也会自动由 IEEE EUI-64 标准生成。</p>
前缀长度	IPv6 全球单播地址的前缀长度。
链路本地地址	交换机 VLAN 接口的链路本地地址。当接口为 UP 状态时，会自动生成链路本地地址。
RA 自动配置	开启后，交换机将周期性自动发送 RA 报文，客户端接收 RA 报文后，通过 RA 报文中网络前缀信息，自动生成 IPv6 全球单播地址。默认为关闭状态。

5.6.3 IPv6 ND 设置

当主机需要和目标主机通信时必须先获得目标主机的链路层地址。将邻居节点的 IPv6 地址解析为链路层地址，可以通过邻居发现机制来动态实现，也可以通过手工配置静态邻居表项来实现。设备根据邻居节点的 IPv6 地址和与此邻居节点相连的三层接口号来唯一标识一个静态邻居表项。另外，当用户需要过滤掉一些非法的报文时，可以通过静态配置邻居表项，将这些非法报文的目的 IPv6 地址绑定到某个不存在的 MAC 地址。

在「路由设置」>「IPv6 设置」>「IPv6 ND 设置」页面中，您可以配置静态邻居表项，查看静态与动态邻居表项。



参数说明

标题项	说明
IPv6 单播地址	邻居的 IPv6 单播地址。
MAC 地址	邻居的 MAC 地址。
类型	邻居表项的类型。 <ul style="list-style-type: none">- 静态：由网络管理员手工配置。- 动态：通过邻居请求消息 NS 与邻居通告消息 NA 动态创建。
接口	与邻居节点相连的交换机 VLAN 接口。
老化时间	邻居表项的老化时间。超过老化时间的邻居表项将从 ND 表项中移除。 静态邻居表项没有老化时间，动态邻居表项老化时间为 20 分钟，不可修改。

6 QoS 策略

6.1 概述

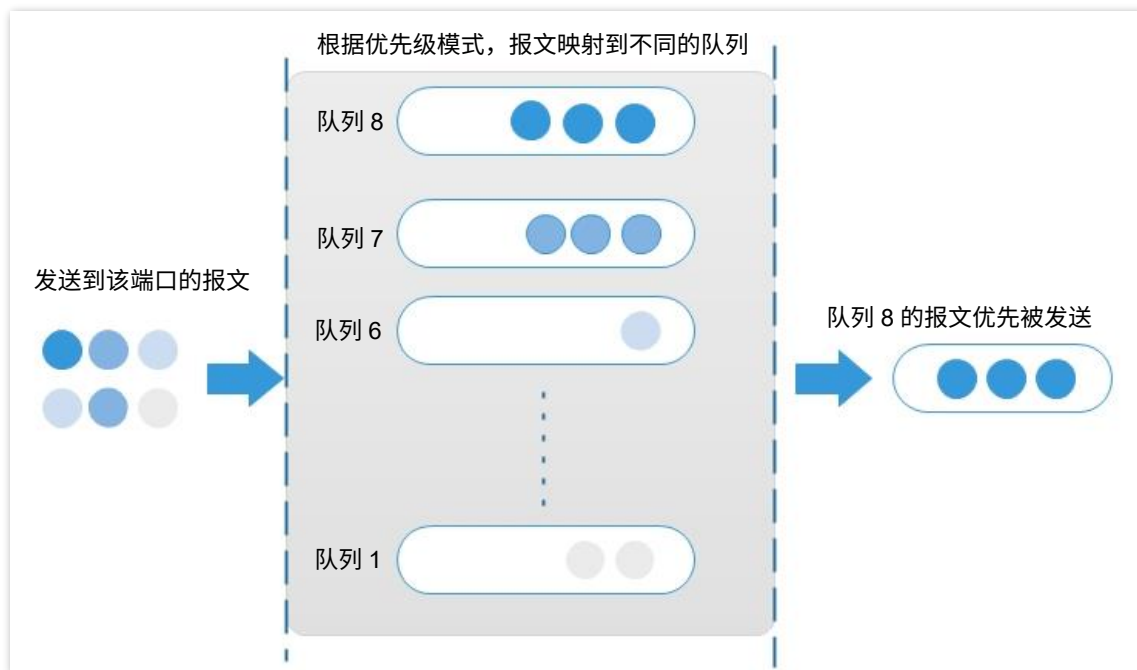
在传统的 IP 网络中，所有的报文都被无区别地对待，网络尽最大努力 (Best-Effort) 发送报文，但对时延、可靠性等性能不能提供任何保证。随着网络技术的发展，IP 网络在 www, FTP, E-mail 等服务的基础上，拓展新的业务如电视会议、远程教学、视频点播、可视电话等，这些新业务对带宽、延迟、抖动等传输性能有着新的要求。因此，根据实际网络环境中的业务需求合理配置 QoS (Quality of Service, 服务质量) 策略，可以提高网络的服务质量。

本交换机通过在入口阶段对数据流进行分类，然后在出口阶段将不同类型的数据流映射到不同优先级的队列，最后依据调度模式来转发不同优先级队列的报文，从而保障网络的服务质量。

调度模式

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。严格优先级、简单加权优先级和加权优先级是队列调度的三种调度模式。每种调度模式都提供 8 个队列来确定数据的转发优先级。

■ 严格优先级



严格优先级调度算法是针对关键业务型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要优先获得服务以减小响应的延迟。

在队列调度时，严格按照优先级从高到低的次序（队列 8 > 队列 7... > 队列 1）优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如 E-mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

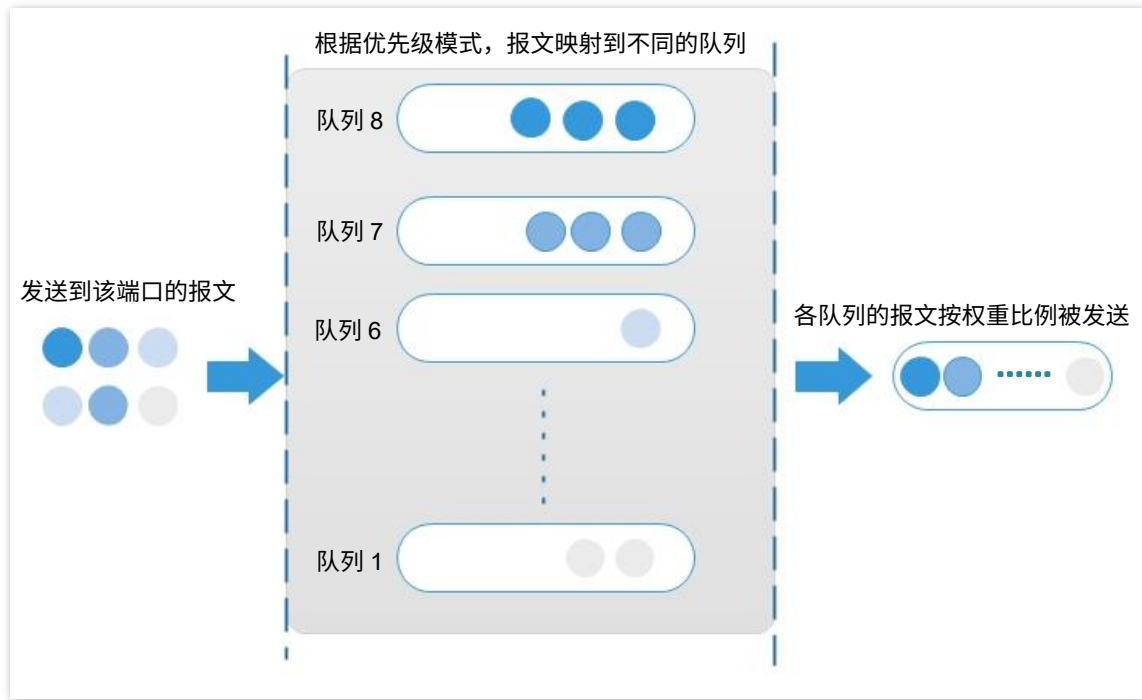
严格优先级的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

■ 简单加权优先级

该模式下，没有优先级，所有队列公平地占用带宽。

■ 加权优先级

该调度算法是在队列之间按权重比值进行轮流调度，以保证每个队列都得到一定的服务时间。加权值表示获取资源的比重。以端口有 8 个输出队列为例，该模式可为每个队列配置一个加权值，如一个 100Mbps 的端口，配置它的调度算法的加权值为 25、20、15、15、10、5、5、5，这样可以保证最低优先级队列至少获得 5Mbps 带宽，避免了采用严格优先级调度时低优先级队列中的报文可能长时间得不到服务的缺点。加权优先级队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。



优先级

下文介绍 [802.1P 优先级](#)、[DSCP 优先级](#)和[端口优先级](#)三种优先级模式。

802.1P 优先级

802.1P 优先级位于二层报文头部，适用于不需要分析三层报文头部，而需要在二层环境下保证 QoS 的场合。带有 802.1Q 标签的数据包才支持 802.1P 优先级，如下图所示，4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID (Tag Protocol Identifier, 标签协议标识, 取值为 0x8100) 和 2 个字节的 TCI (Tag Control Information, 标签控制信息)。

Destination Address	Source Address	802.1Q header		Length/Type	Data	FCS (CRC-32)
		TPID	TCI			
6 bytes	6 bytes	4 bytes		2 bytes	46~1500 bytes	4 bytes

下图显示了 802.1Q 标签头的详细内容，TCI 中 Priority 字段就是 802.1P 优先级。它由 3 个 bit 组成，取值范围为 0~7。

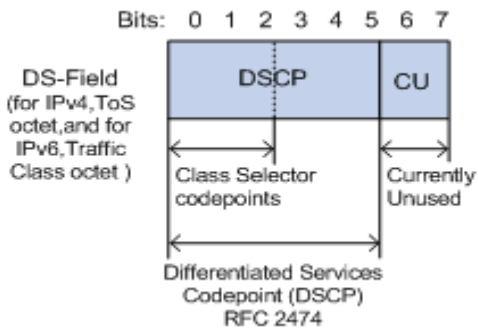
Byte 1		Byte 2		Byte 3		Byte 4																	
TPID(Tag protocol identifier)				TCI(Tag control information)																			
1	0	0	0	0	0	0	0	Priority	C	VLAN ID													
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0

本交换机默认的 802.1P 优先级、队列及关键字映射关系如下表。

802.1P 优先级	队列	关键字
0	1	best-effort
1	2	background
2	3	spare
3	4	excellent-effort
4	5	controlled-load
5	6	video
6	7	voice
7	8	network-management

■ DSCP 优先级

RFC2474 重新定义了 IP 报文头部的 ToS (Type of Service, 服务类型) 字段, 称之为 DS (Differentiated Services, 差分服务) 域, 其中 DSCP (Differentiated Services Codepoint, 差分服务编码点) 优先级用该域的前 6 个 bit (0~5bit) 表示 (如下图), 取值范围为 0~63, 后 2 个 bit (6、7bit) 是保留位。



DSCP 优先级与关键字对应关系如下表所示。

DSCP 优先级 (十进制)	DSCP 优先级 (二进制)	关键字
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。
不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

DSCP 优先级（十进制）	DSCP 优先级（二进制）	关键字
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

交换机默认 DSCP 优先级与队列映射关系如下表。

DSCP 优先级	队列
0~7	1
8~15	2
16~23	3
24~31	4
32~39	5
40~47	6

DSCP 优先级	队列
48~55	7
56~63	8

■ 端口优先级

手动配置交换机物理端口的 Cos 优先级，实现物理端口与队列的映射关系。当出现以下两种情况之一时，端口按照配置的映射关系将报文映射到对应的队列。

- 端口收到的报文不带本端口信任的优先级标签。例如已开启了 802.1P 优先级模式的端口，收到的报文中不带 802.1Q 标签。
- 端口未信任 802.1P 优先级和 DSCP 优先级模式。

本交换机物理端口 Cos 优先级与队列映射关系如下表所示。

Cos 优先级	队列
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

6.2 配置向导

根据 802.1P 优先级映射队列

步骤	任务	任务说明
1	QoS 调度	必选。 根据实际需要选择本交换机的调度模式。
2	802.1P	必选。 配置 802.1P 优先级与队列映射表。
3	端口优先级	必选。 将相应端口的信任模式设置为“802.1P 信任”，同时配置所有端口 Cos 优先级。

根据 DSCP 优先级映射队列

步骤	任务	任务说明
1	QoS 调度	必选。 根据实际需要选择本交换机的调度模式。
2	DSCP	必选。 配置 DSCP 优先级与队列映射表。
3	端口优先级	必选。 将相应端口的信任模式设置为“DSCP 信任”，同时配置所有端口 Cos 优先级。

6.3 QoS 调度

在「QoS 策略」>「QoS 调度」页面中，您可以配置 QoS 调度模式及拥塞处理策略。



参数说明

标题项	说明
QoS 模式	<p>端口流量的调度模式。</p> <ul style="list-style-type: none">- 严格优先级：严格按照优先级从高到低的次序优先发送较高优先级队列中的报文，只有当高优先级队列为空时，才会转发较低优先级的队列报文。- 简单加权优先级：8 个队列平分带宽。- 加权优先级：需为每个队列配置一个加权值，加权值表示获取资源的权重。当端口出现拥塞时，按照各队列的权重分配带宽。
队列设置	<p>调度模式选择为加权优先级时，在此处设置各队列的加权值。</p>
队列出口丢弃	<p>开启后，交换机强制关闭流控，以满足各种复杂场景的网络克隆需求。</p> <p> 提示</p> <p>只在需要进行网络克隆操作才开启该功能，一般不建议开启。</p>

6.4 802.1P

在「QoS 策略」>「802.1P」页面中，您可以配置 802.1P 优先级与队列的映射关系。

QoS调度 **802.1P** DSCP 端口优先级

CoS优先级设置

优先级0 队列1 ▾

优先级1 队列2 ▾

优先级2 队列3 ▾

优先级3 队列4 ▾

优先级4 队列5 ▾

优先级5 队列6 ▾

优先级6 队列7 ▾

优先级7 队列8 ▾

确定

参数说明

标题项	说明
优先级 0	Priority 字段为 0 的 VLAN 报文对应的队列。
优先级 1	Priority 字段为 1 的 VLAN 报文对应的队列。
优先级 2	Priority 字段为 2 的 VLAN 报文对应的队列。
优先级 3	Priority 字段为 3 的 VLAN 报文对应的队列。
优先级 4	Priority 字段为 4 的 VLAN 报文对应的队列。
优先级 5	Priority 字段为 5 的 VLAN 报文对应的队列。
优先级 6	Priority 字段为 6 的 VLAN 报文对应的队列。
优先级 7	Priority 字段为 7 的 VLAN 报文对应的队列。

6.5 DSCP

在「QoS 策略」>「DSCP」页面中，您可以配置 DSCP 优先级与队列的映射关系。

QoS调度 802.1P **DSCP** 端口优先级 ?

DSCP

DSCP	端口队列	DSCP	端口队列	DSCP	端口队列	DSCP	端口队列
0	队列1	16	队列3	32	队列5	48	队列7
1	队列1	17	队列3	33	队列5	49	队列7
2	队列1	18	队列3	34	队列5	50	队列7
3	队列1	19	队列3	35	队列5	51	队列7
4	队列1	20	队列3	36	队列5	52	队列7
5	队列1	21	队列3	37	队列5	53	队列7
6	队列1	22	队列3	38	队列5	54	队列7
7	队列1	23	队列3	39	队列5	55	队列7

参数说明

标题项	说明
DSCP	根据 IP 包的 DS 域决定的优先级。优先级级别从 0 到 63。
端口队列	该 DSCP 优先级对应队列。

6.6 端口优先级

在「QoS 策略」>「端口优先级」页面中，您可以配置交换机各物理端口的优先级模式及各端口的 Cos (Class of Service, 服务等级) 优先级。

端口	Cos 优先级	信任模式	操作
1	0	非信任	
2	0	非信任	
3	0	非信任	
4	0	非信任	
5	0	非信任	
6	0	非信任	
7	0	非信任	
8	0	非信任	

参数说明

标题项	说明
端口	端口编号。
Cos 优先级	物理端口的 Cos 优先级。当交换机接收到的报文不符合信任模式的规则或端口为非信任模式时，则按照 Cos 优先级对报文进行归队。
信任模式	<p>端口接收到的报文的处理方式。</p> <ul style="list-style-type: none"> - 非信任：端口接收到的所有报文都根据端口 Cos 优先级进行归队。 - 802.1P 信任：端口接收到 VLAN 报文时，将该报文按照 802.1P 所配置的映射关系进行归队；端口接收到其他报文时，将该报文按照 Cos 优先级的对应关系进行归队。 - DSCP 信任：端口接收到 IP 报文时，将该报文按照 DSCP 所配置的对应关系进行归队；端口接收到其他报文时，将该报文按照 Cos 优先级的对应关系进行归队。

7 网络安全

7.1 ACL

7.1.1 概述

ACL（Access Control List，访问控制列表）即通过配置对报文的匹配规则和处理操作来实现报文过滤的功能。当交换机的端口接收到报文后，将根据当前端口上应用的 ACL 规则对报文的字段进行分析，在识别出特定的报文之后，根据预先设定的策略允许或禁止相应的报文通过。

通过 ACL 功能，可以有效的防止非法用户对网络的访问，提高网络安全性。

您可以基于 MAC 地址和 IP 地址两种匹配规则的 ACL 来实现报文过滤功能的功能。

- MAC ACL：根据二层数据帧中的源 MAC 地址和目的 MAC 地址匹配过滤规则。
- IP ACL：根据三层数据包 IP 头的源 IP 地址和目的 IP 地址匹配过滤规则。

一个 ACL ID 可以配置多条 ACL 匹配规则，报文在匹配 ACL 规则时，会根据规则的优先级，优先匹配优先级高的规则，一旦有一条规则被匹配，则该报文不再匹配其他规则。

7.1.2 配置向导

基于 MAC 地址的过滤规则

步骤	任务	任务说明
1	MAC ACL	必选。 配置根据二层数据帧中的源和目的 MAC 地址匹配的过滤规则。一个 ACL ID 可以配置多条 MAC ACL 规则。
2	应用 ACL	必选。 只有将 MAC ACL 规则应用到交换机相应的端口后，规则才会生效。

基于 IP 地址的过滤规则

步骤	任务	任务说明
1	IP ACL	必选。 配置根据三层数据包中的源和目的 IP 地址匹配的过滤规则。一个 ACL ID 可以配置多条 IP ACL 规则。
2	应用 ACL	必选。 只有将 IP ACL 规则应用到交换机相应的端口后，规则才会生效。

7.1.3 MAC ACL

在「网络安全」>「ACL」>「MAC ACL」页面中，您可以查看和配置 MAC ACL 规则。



参数说明

标题项	说明
ACL ID	MAC ACL 规则的 ACL ID。配置 MAC ACL 规则之前，需要先在此处配置 ACL ID。
优先级	此字段为规则的优先级，值越小，优先级越高。 报文从优先级最高的规则开始匹配，当匹配上后不再匹配后面的规则。
VLAN ID	报文所在的 VLAN。 不配置则表示所有 VLAN 的报文。
源 MAC	报文的源 MAC 地址。 <ul style="list-style-type: none">- 任意 MAC：表示所有 MAC 地址。- 指定 MAC：与掩码组合使用，表示某个特定的 MAC 地址或 MAC 地址段。

标题项	说明
目的 MAC	报文的目的地 MAC 地址。 - 任意 MAC：表示所有 MAC 地址。 - 指定 MAC：与掩码组合使用，表示某个特定的 MAC 地址或 MAC 地址段。
报文类型	二层数据帧的报文类型。 不配置则表示任意报文类型。
动作（执行动作）	交换机对匹配本规则的报文的处理方式，可设定为允许（即转发）或禁止（即丢弃）。
时间段 ID	MAC ACL 规则生效的时间段，需先在 时间段管理 模块配置好。不指定表示 MAC ACL 规则一直生效，不受时间限制。

7.1.4 IP ACL

在「网络安全」>「ACL」>「IP ACL」页面中，您可以查看和配置 IP ACL 规则。



参数说明

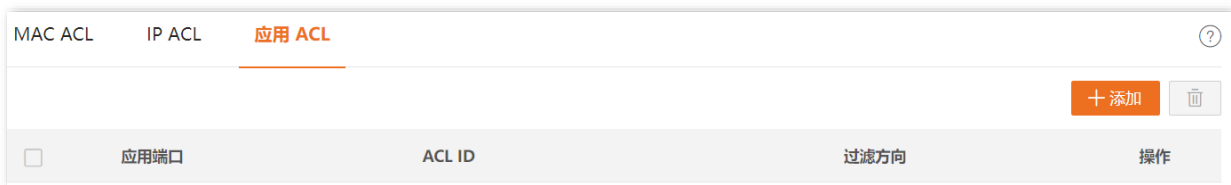
标题项	说明
ACL ID	IP ACL 规则的 ACL ID。配置 IP ACL 规则之前，需要先在此处配置 ACL ID。
优先级	此字段为规则的优先级，值越小，优先级越高。 报文从优先级最高的规则开始匹配，当匹配上后不再匹配后面的规则。
协议	三层 IP 头的协议类型字段，如 IP、ICMP 等。您也可手动输入协议号。

标题项	说明
源 IP	报文的源 IP 地址。 <ul style="list-style-type: none">- 任意 IP：表示所有 IP 地址。- 指定 IP：与掩码组合使用，表示某个特定的网络地址。
目的 IP	报文的的目的 IP 地址。 <ul style="list-style-type: none">- 任意 IP：表示所有 IP 地址。- 指定 IP：与掩码组合使用，表示某个特定的网络地址。
源端口	协议类型为 TCP 或 UDP 时，此处配置协议源端口号。
目的端口	协议类型为 TCP 或 UDP 时，此处配置协议目的端口号。
动作	交换机对匹配本规则的报文的处理方式，可设定为允许（即转发）或禁止（即丢弃）。
时间段 ID	IP ACL 规则生效的时间段，需先在 时间段管理 模块配置好。不指定表示 IP ACL 规则一直生效，不受时间限制。

7.1.5 应用 ACL

只有将 ACL 应用到相应的端口后，匹配规则才会生效。

在「网络安全」>「ACL」>「应用 ACL」页面中，您可以将配置好的 ACL 应用到相应的端口。



参数说明

标题项	说明
应用端口	ACL 生效的物理端口号。
ACL ID	该端口生效的 ACL 规则。
过滤方向	端口报文过滤方向。本交换机当前只支持入方向过滤。

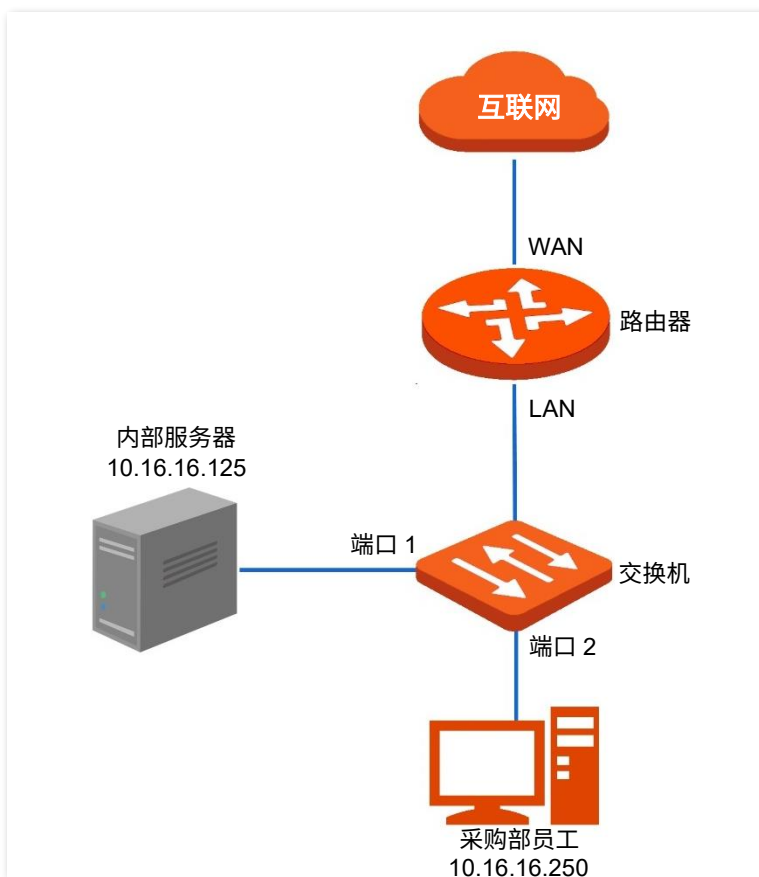
7.1.6 ACL 配置举例

组网需求

某公司要求采购部某员工仅允许访问公司内部服务器，禁止访问互联网。

方案设计

使用交换机的 IP ACL 功能实现上述需求。如下图，假设该采购员工电脑的 IP 地址为 10.16.16.250，公司内部服务器的 IP 地址为 10.16.16.125。



配置步骤

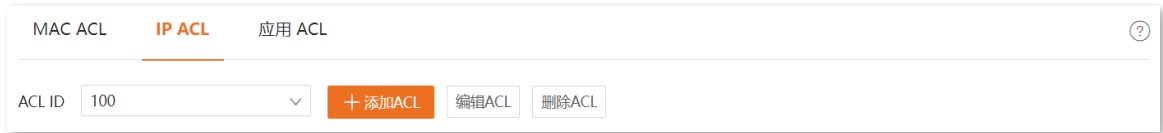
步骤 1 添加 IP ACL 规则。

1. 进入配置页面。

[进入交换机 Web 管理页面](#)，点击「网络安全」>「ACL」>「IP ACL」。

2. 添加 ACL。

点击 **+ 添加 ACL**，添加一条 ACL，如 ACL ID 为“100”的 ACL。



3. 添加 IP ACL 规则。

点击 **+ 添加规则**，添加两条 IP ACL 规则，配置信息如下：

序号	ACL ID	优先级	协议	源 IP	目的 IP	执行动作
1	100	1	IP	10.16.16.250/32 (采购部员工主机的 IP 地址)	10.16.16.125/32 (公司内部服务器的 IP 地址)	允许
2	100	2	IP	10.16.16.250/32 (采购部员工主机的 IP 地址)	任意 IP	禁止

添加成功后，如下图所示。

IP ACL规则	优先级	协议	源IP	目的IP	源端口	目的端口	动作	时间段ID	操作
<input type="checkbox"/>	1	IP	10.16.16.250	10.16.16.125	任意	任意	允许	--	
<input type="checkbox"/>	2	IP	10.16.16.250	任意	任意	任意	禁止	--	

步骤 2 应用 ACL。

1. 进入配置页面。

[进入交换机 Web 管理页面](#)，点击「网络安全」>「ACL」>「应用 ACL」。

2. 应用 ACL。

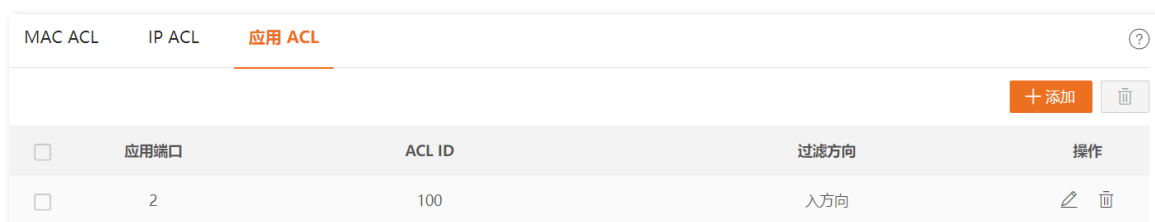
点击 **+ 添加**，添加一条应用 ACL，配置信息如下：



绑定 ACL	ACL ID	过滤方向	应用端口
IP ACL	100	入方向	端口 2

本指南仅作为功能配置参考，不代表产品支持指南内全部功能。
不同型号产品 Web 页面的功能也可能存在差异，请以实际产品的 Web 页面为准。

资料版本 V1.0

添加成功后，如下图所示。



<input type="checkbox"/>	应用端口	ACL ID	过滤方向	操作
<input type="checkbox"/>	2	100	入方向	 

步骤 3 保存配置。

点击管理页面右上角的 **保存配置** 进行全局保存。

---完成

验证配置

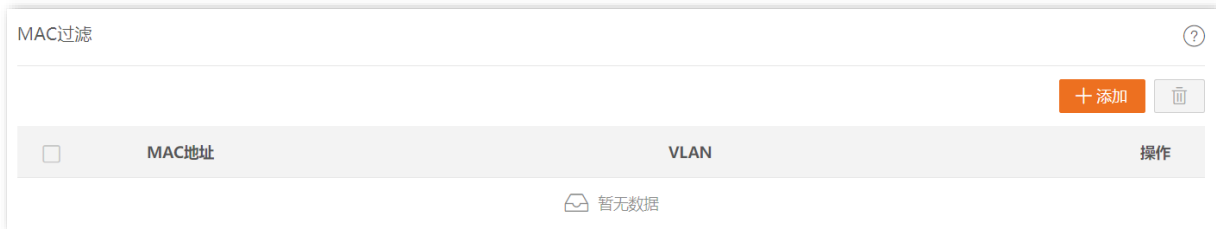
完成以上配置后，采购部该员工只能访问公司内部服务器，无法访问互联网。

7.2 MAC 过滤

通过 MAC 过滤功能，可以对进入交换机端口的数据包的源 MAC 地址和目的 MAC 地址进行检查，如果数据包的源 MAC 地址或目的 MAC 地址在 MAC 过滤表中存在，则将丢弃该数据包。

通过 MAC 过滤功能，可以防止非法用户对网络的访问，提高网络安全性。

在「网络安全」>「MAC 过滤」页面中，您可以配置 MAC 过滤规则。



参数说明

标题项	说明
MAC 地址	要过滤的 MAC 地址，当数据包的源 MAC 地址或目的 MAC 地址与该 MAC 地址相同时，则丢弃该数据包。
VLAN	MAC 过滤规则生效的 VLAN。

7.3 802.1X

7.3.1 概述

802.1X 是 IEEE 提出的基于端口的网络接入控制协议，用于对局域网用户进行认证控制，以提高网络安全性。其认证系统由认证客户端、认证设备端和认证服务器三部分组成。

- 认证客户端：发起认证请求的用户终端，由局域网中的认证服务器对其进行合法性检验。该用户终端必须安装了支持 802.1X 认证的客户端软件。
- 认证设备端：为认证客户端提供接入局域网接口的设备，位于认证客户端和认证服务器之间，并根据认证服务器返回的信息来执行是否允许认证客户端接入局域网。
- 认证服务器：用于对认证客户端进行合法性检验，通常为 RADIUS（Remote Authentication Dial-in User Service，远程认证拨号用户服务）服务器。认证服务器根据认证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认证设备端，由认证设备端决定是否允许认证客户端接入。

本交换机在认证系统中属于认证设备端，采用 EAP 终结方式与认证服务器进行交互。交换机在接收到认证客户端的 EAP 报文后，先将该报文中的客户端认证信息封装到标准 RADIUS 报文中，再将 RADIUS 报文转发给认证服务器。简易的认证系统示意图如下。



本交换机仅支持基于端口的接入认证方式。如果端口下某一用户认证成功，则端口变为授权状态，其他后续接入此端口的用户无需认证即可访问网络资源，当该用户下线后，端口变为非授权状态，此端口下的所有用户会被拒绝访问网络资源。

7.3.2 全局设置

在「网络安全」>「802.1X」>「全局设置」页面中，您可以配置 802.1X 认证服务器相关参数。



802.1X认证

全局设置 端口设置

认证服务器IP地址

授权共享密钥

确定

参数说明

标题项	说明
认证服务器 IP 地址	RADIUS 认证服务器的 IP 地址，需要与本交换机路由可达。
授权共享密钥	认证/授权报文的共享密钥，需要与认证服务器侧设置的密钥一致。

7.3.3 端口设置

在「网络安全」>「802.1X」>「端口设置」页面中，您可以配置交换机各端口的 802.1X 认证相关参数。

端口	端口控制方式	端口认证状态	端口重认证	重认证超时时间	客户端超时时间	最大重认证次数	操作
1	关闭	非授权	关闭	3600	30	2	✎
2	关闭	非授权	关闭	3600	30	2	✎
3	关闭	非授权	关闭	3600	30	2	✎
4	关闭	非授权	关闭	3600	30	2	✎
5	关闭	非授权	关闭	3600	30	2	✎
6	关闭	非授权	关闭	3600	30	2	✎
7	关闭	非授权	关闭	3600	30	2	✎
8	关闭	非授权	关闭	3600	30	2	✎

参数说明

标题项	说明
端口	本交换的端口编号。
端口控制方式	<p>该端口对用户访问网络的控制方式：</p> <ul style="list-style-type: none"> - 自动：端口开启 802.1X 认证，初始状态为非授权状态，用户不能访问网络资源。如果用户认证通过，端口变为授权状态，则允许用户访问网络资源。 - 强制授权：端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。 - 强制非授权：端口始终处于非授权状态，不允许用户访问网络资源。 - 关闭：该端口不开启 802.1X 认证，允许用户访问网络资源。
端口认证状态	<p>该端口的认证状态。</p> <ul style="list-style-type: none"> - 授权：允许用户访问网络资源。 - 非授权：不允许用户访问网络资源。
端口重认证	开启/关闭端口的 802.1X 重认证功能。开启后，交换机会周期性对端口上在线的认证客户端发起重认证请求，以检测认证客户端的连接状态，确保认证客户端在线。

标题项	说明
重认证超时时间	交换机向认证客户端发起重认证请求的时间间隔。 端口开启重认证功能后，交换机以此时间为周期对该端口的在线认证客户端发起重认证请求。
客户端超时时间	客户端响应重认证请求的超时时间。 当交换机向认证客户端发送重认证请求报文后，如果在此时间内，交换机没有收到认证客户端的响应，交换机将重新发送该报文。
最大重认证次数	客户端的最大可重认证次数。如果认证客户端的重认证失败次数超过最大重认证次数，则认证客户端将被强制下线。  注意 客户端认证超时也会计算为重认证失败的次数。即客户端认证超时次数超过最大重认证次数时，该客户端将会被强制下线。

7.4 攻击防御

7.4.1 概述

本交换机提供三种攻击防御：防 ARP 攻击、防 DoS 攻击、防 MAC 地址攻击。

■ 防 ARP 攻击

通过 ARP 限速设置来防止局域网内大量的 ARP 报文发往交换机，导致交换机 CPU 负担过重，从而造成其它功能无法正常运行甚至设备瘫痪。

如果交换机的 ARP 报文接收速率超过了您设定的阈值，交换机将会随机丢弃部分 ARP 报文，以确保 ARP 报文接收速率在您设定的阈值范围内。

■ 防 DoS 攻击

防 DoS 攻击功能可以防止攻击者利用被攻击主机所提供程序或传输协议本身的实现缺陷，反复发送畸形攻击报文引发系统错误分配大量系统资源，使主机处于挂起状态甚至死机。

■ 防 MAC 地址攻击

防 MAC 地址攻击功能通过限制交换机端口的 MAC 地址学习，来防止交换机因不断地学习局域网中大量无效的报文源 MAC 地址，使得 MAC 地址转发表过于庞大，导致其转发性能急剧下降。

7.4.2 防 ARP 攻击

在「网络安全」>「攻击防御」>「防 ARP 攻击」页面中，您可以配置交换机的防 ARP 攻击功能相关参数。



端口	防ARP攻击	ARP接收速率	操作
1	禁用	100	
2	禁用	100	
3	禁用	100	
4	禁用	100	
5	禁用	100	
6	禁用	100	
7	禁用	100	

参数说明

标题项	说明
接口	交换机的端口号。
防 ARP 攻击	启用/禁用交换机的防 ARP 攻击功能。
ARP 接收速率	<p>设置交换机对应端口每秒最多可接收的 ARP 报文数。一秒钟内，如果交换机收到超过此阈值的 ARP 报文，则认为正受到 ARP 攻击。此时交换机将会随机丢弃部分 ARP 报文，以确保 ARP 报文接收速率在此阈值范围内，来有效避免 ARP 泛洪攻击。</p> <p>启用交换机的防 ARP 攻击功能可设置。</p>

7.4.3 防 DoS 攻击

DoS (Denial of Service)，即拒绝服务。防 DoS 攻击功能用于防止某些主机通过发送大量的服务请求，恶意消耗服务器资源，导致其它主机无法正常使用网络服务的情况。

在「网络安全」>「攻击防御」>「防 DOS 攻击」页面中，您可以配置交换机的防 DoS 攻击规则。

防ARP攻击 **防DoS攻击** 防MAC地址攻击

[ALL] 检测所有

[ICMP-FRAG-PKTS] ICMPv4 分段数据包检测

[LAND] IPv4/IPv6 源地址等于目标地址检测

[MAC-DA-EQ-SA] 源 MAC 地址等于目标 MAC 地址检测

[NULL-SCAN] TCP 控制标志和序列等于 0 检测

[POD] 检测 IP 第一个片段

[SYN-FIN] 带有 TCP SYN 和 FIN 标志的 TCP 数据包检测

[SYN-RST] 带有 TCP SYN 和 RST 标志的 TCP 数据包检测

[SYN-SPORT-LESS-1024] TCP控制标志SYN为1且ACK为0且SPORT小于1024检测

[TCP-BLAT] SPORT 等于 DPORT 的 TCP 数据包检测

[UDP-BLAT] SPORT 等于 DPORT 的 UDP 数据包检测

[XMA] 带有 TCP FIN、URG 和 PSH 标志的 TCP 数据包检测

确定

参数说明

标题项	说明
【ALL】检测所有	勾选后，下面所有项均被勾选，交换机将不转发以下描述的所有报文。
【ICMP-FRAG-PKTS】 ICMPv4 分段数据包检测	勾选后，交换机不转发 ICMPv4 分片报文。
【LAND】IPv4/IPv6 源地址等 于目标地址检测	勾选后，交换机不转发源地址等于目标地址的 IPv4/IPv6 报文。
【MAC-DA-EQ-SA】源 MAC 地址等于目标 MAC 地址检测	勾选后，交换机不转发源 MAC 地址等于目标 MAC 地址的报文。

标题项	说明
【NULL-SCAN】TCP 控制标志和序列等于 0 检测	勾选后，交换机不转发序列和所有标志位等于 0 的 TCP 报文。
【POD】检测 IP 第一个片段	勾选后，交换机不转发 IP 第一个分片报文。
【SYN-FIN】带有 TCP SYN 和 FIN 标志的 TCP 数据包检测	勾选后，交换机不转发 SYN、FIN 标志位均为 1 的 TCP 报文。
【SYN-RST】带有 TCP SYN 和 RST 标志的 TCP 数据包检测	勾选后，交换机不转发 SYN、RST 标志位均为 1 的 TCP 报文。
【SYN-SPORT-LESS-1024】TCP 控制标志 SYN 为 1 且 ACK 为 0 且 SPORT 小于 1024 检测	勾选后，交换机不转发 SYN 标志位为 1，ACK 标志位为 0，且源端口号小于 1024 的 TCP 报文。
【TCP-BLAT】SPORT 等于 DPORT 的 TCP 数据包检测	勾选后，交换机不转发源端口号与目的端口号相同的 TCP 报文。
【UDP-BLAT】SPORT 等于 DPORT 的 UDP 数据包检测	勾选后，交换机不转发源端口号与目的端口号相同的 UDP 报文。
【XMA】带有 TCP FIN、URG 和 PSH 标志的 TCP 数据包检测	勾选后，交换机不转发 FIN、URG 和 PSH 标志位均为 1 的 TCP 报文。

7.4.4 防 MAC 地址攻击

在「网络安全」>「攻击防御」>「防 MAC 地址攻击」页面中，您可以配置交换机端口是否转发未知单播报文。



端口	未知MAC丢弃	操作
1	关闭	
2	关闭	
3	关闭	
4	关闭	
5	关闭	

参数说明

标题项	说明
端口	端口编号。
未知 MAC 丢弃	开启后，该端口不再进行 MAC 地址学习，丢弃收到的未知单播报文。

8 设备管理

8.1 SNMP

8.1.1 概述

SNMP (Simple Network Management Protocol)，即简单网络管理协议。通过 SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

SNMP 能够屏蔽不同设备的物理差异，实现对不同厂商设备的自动化管理。

SNMP 的管理框架

SNMP 包括三个网络元素：SNMP 管理者(SNMP Manager)，SNMP 代理(SNMP Agent)，MIB 库 (Management Information Base，管理信息库)。

- SNMP 管理者：一个利用 SNMP 协议对网络节点进行控制和监视的系统。其中网络环境中最常见的 SNMP 管理者被称为网络管理系统 (NMS, Network Management System)。网络管理系统既可以指一台专门用来进行网络管理的服务器，也可以指某个网络设备中执行管理功能的一个应用程序。
- SNMP 代理：被管理设备中的一个软件模块，用来维护被管理设备的管理信息数据并可在需时把管理数据汇报给一个 SNMP 管理系统。
- MIB 库：被管理对象的集合。NMS 在管理设备时，需要获取被管理对象的一些功能参数，例如接口状态、CPU 利用率等参数，这些参数就是被管理对象。MIB 库定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个 SNMP 代理都有自己的 MIB。SNMP 管理者根据权限可以对 MIB 中的对象进行读/写操作。

SNMP 管理者是 SNMP 网络的管理者，SNMP 代理是 SNMP 网络的被管理者，他们之间通过 SNMP 协议来交互管理信息。

SNMP 基本操作

本交换机中，SNMP 提供以下三种基本操作来实现 SNMP 管理者和 SNMP 代理的交互。

- Get 操作：SNMP 管理者使用该操作查询 SNMP 代理的一个或多个对象的值。
- Set 操作：SNMP 管理者使用该操作重新设置 MIB 库中的一个或多个对象的值。
- Trap 操作：SNMP 代理使用该操作向 SNMP 管理者发送告警信息。

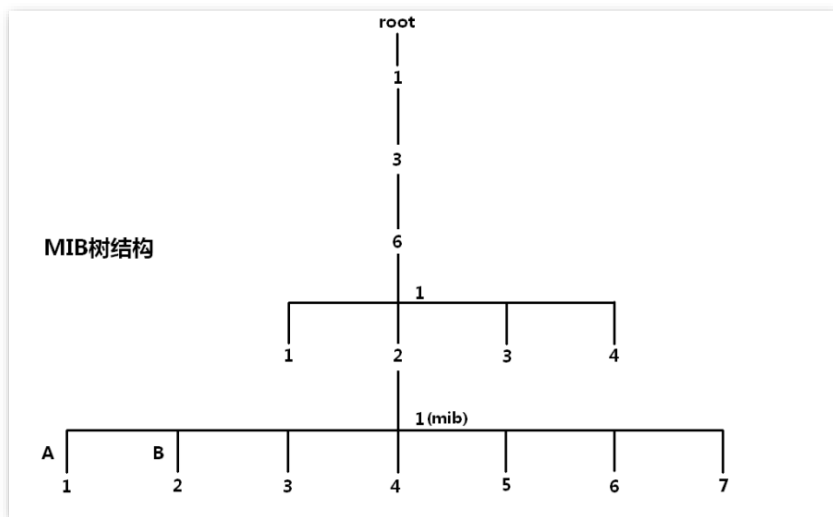
SNMP 协议版本

本交换机兼容 SNMPv1、SNMPv2c、SNMPv3。

- SNMPv3 采用用户名和密码认证方式。
- SNMPv1、SNMPv2c 采用团体名（Community Name）认证，如果 SNMP 报文携带的团体名没有得到交换机认可，则该 SNMP 报文将被丢弃。SNMP 团体名用来定义 SNMP 管理者和 SNMP 代理的关系。团体名起到了类似于密码的作用，可以限制 SNMP 管理者访问交换机上的 SNMP 代理。

MIB 简介

MIB 是以树状结构进行组织的。树的节点表示被管理对象，它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）。MIB 的结构如图所示。图中，A 的 OID 为（1.3.6.1.2.1.1），B 的 OID 为（1.3.6.1.2.1.2）。



视图

MIB 视图是全部 MIB 管理对象的一个子集。管理对象以 OID（Object Identifier，对象标识符）来表示，通过配置管理对象的视图规则（include/exclude），来达到控制该管理对象能否被管理的目的。各管理对象的 OID 可以在 SNMP 管理软件上找到。

组

创建完视图之后，需要创建 SNMP 组。可以为各 SNMP 组添加只读/读写/通知视图，从而满足了处于不同组内的用户对交换机功能的访问权限不同的需求。

用户

用户创建于 SNMP 组中，SNMP 管理端使用此处创建的用户及其认证/加密密码来登录 SNMP 代理端。

团体

SNMPv1 和 SNMPv2c 时，创建完视图后，需要创建团体。团体名称类似于密码的作用，对 SNMP 管理者进行认证；同时可以为各团体添加视图访问权限，从而达到权限管理的目的。

8.1.2 配置向导

■ SNMPv3 版本

步骤	操作	说明
1	基本设置	必选。 开启 SNMP 代理功能。
2	创建视图	可选。 在 权限控制 页面的视图列表中创建管理对象的视图。系统默认创建了一个视图名称为 Default 的视图。
3	创建组	必选。 在 权限控制 页面的组列表中创建 SNMP 组，并为组添加不同访问权限的视图。
4	创建用户	必选。 在 权限控制 页面的用户列表中创建 SNMP 用户，并配置用户的认证/加密模式及密码。
5	配置通告	可选。 在 通告 页面中配置安全模型为 v3 的通告。

■ SNMPv1 或 SNMPv2c 版本

步骤	操作	说明
1	基本设置	必选。 开启 SNMP 代理功能。
2	创建视图	可选。 在 权限控制 页面的视图列表中创建管理对象的视图。系统默认创建了一个视图名称为 Default 的视图。
3	创建团体	必选。 在 权限控制 页面的团体列表中创建 SNMP 团体。
5	配置通告	可选。 在 通告 页面中配置安全模型为 v1 和 v2c 的通告。

8.1.3 基本设置

在「设备管理」>「SNMP」>「基本设置」页面中，您可以配置 SNMP 的基本参数。

SNMP功能

基本设置 权限控制 通告

联系信息 (1-255字符)

物理位置信息 (1-255字符)

本地引擎ID (10-64位16进制数)

注：本设备兼容SNMP v1/v2c/v3

参数说明

标题项	说明
SNMP 功能	开启/关闭 SNMP 功能。
联系信息	交换机的联系信息，便于 SNMP 管理者快速定位到本交换机。
物理位置信息	交换机的物理位置信息，便于 SNMP 管理者快速定位到本交换机。
本地引擎 ID	交换机的本地引擎 ID，需在 SNMP 管理者侧填入该 ID，SNMP 管理者才能将本交换机纳入管理。

8.1.4 权限控制

在「设备管理」>「SNMP」>「权限控制」页面中，您可以进行 SNMP 的权限配置。



参数说明

标题项	说明	
团体列表	团体名称	团体的名称。
	访问规则	团体对视图的访问权限，包括“只读”和“读写”两种。
	MIB 视图	团体可访问的视图。需先在“视图列表”中配置好 MIB 视图。
组列表	组名称	组的名称。
	安全级别	组的安全级别。包括不认证不加密、只认证不加密、既认证又加密。

标题项	说明
只读视图	通过视图来控制组内用户访问的权限，三类视图至少配置一类。 需先在“视图列表”中配置好 MIB 视图。
读写视图	
通知视图	
用户名称	用户名称。
用户所在组	用户所属的组。需先在“组列表”中配置好组。
安全级别	用户的安全级别。选择用户所在组后，此处自动填入。
认证模式	用户的认证模式，本交换机仅支持 MD5（信息摘要算法）。 只有所属组的安全级别为“只认证不加密”或“既认证又加密”时，该参数才需设置。
用户列表	用户的认证密码。
认证密码	只有安全级别为“只认证不加密”或“既认证又加密”时，该参数才需设置。
加密方式	用户的加密方式，本交换机支持“AES”和“DES”两种加密标准。 只有所属组的安全级别为“既认证又加密”时，该参数才需设置。
加密密码	用户的加密密码。 只有安全级别为“既认证又加密”时，该参数才需设置。
视图名称	视图名称。
视图列表	OID 规则。 - include：该 OID 可以被 SNMP 管理者管理。 - exclude：该 OID 不能被 SNMP 管理者管理。
MIB 子树 OID	视图的管理变量（OID）。

8.1.5 通告

通告功能是交换机主动向 SNMP 管理者报告某些视图的重要事件（如设备重启等），便于管理员通过 SNMP 管理软件对交换机一些特定事件进行及时监控和处理。

在「设备管理」>「SNMP」>「通告」页面中，您可以配置 SNMP 的通告功能。



参数说明

标题项	说明
使能所有 trap	开启/关闭 Trap 功能。
目标主机 IP	Trap 目标主机的 IP 地址，即管理主机的 IP 地址。需确保目标主机的 IP 地址与本交换机的路由可达。
安全字	用于认证的安全字，需输入对应的组名称、用户名称或团体名称。如果安全模型选择 v3，则安全字为组名称或用户名称；如果安全模型为 v1 和 v2c，则安全字为团体名称。
UDP 端口	管理主机上启用供 Trap 使用的 UDP 端口。
安全模型	Trap 使用的安全模型，可选 v1、v2c 或 v3。需与 SNMP 管理者的软件版本保持一致。
安全级别	安全模型为 v3 时需设置 Trap 报文的认证加密方式。安全级别包括不认证不加密、只认证不加密、既认证又加密。

8.2 系统时间

为了保证交换机基于时间的功能正常生效，需确保交换机的系统时间准确。本交换机支持[手动设置](#)和[网络校时](#)两种时间设置方式，默认为“网络校时”。

手动设置

网络管理员需手动设置交换机的系统时间。交换机每次重启后，您都需要重新设置其系统时间。

在「设备管理」>「系统时间」页面中，您可以手动修改日期与时间，也可以点击 同步本地时间 将当前正在管理交换机的电脑的时间同步到交换机。

系统时间

当前时间 **2024-01-15 10:31:45**

本地时间 网络时间

日期 时间

网络校时

交换机自动同步互联网上的时间服务器。只要将交换机成功连接至互联网就能自动校准其系统时间，交换机重启后也能自行校准，无需重新设置。

在「设备管理」>「系统时间」页面中，您可以设置交换机的时区。

系统时间

当前时间 **2024-01-15 10:32:38**

本地时间 网络时间 时间同步操作需联网

时区

8.3 日志管理

8.3.1 日志信息

交换机的日志记录了系统从上一次恢复出厂设置后出现的各种情况及用户对交换机的操作记录。若遇网络故障，您可以利用交换机的日志信息进行问题排查。

本交换机默认保存最新的 2000 条日志信息，如果超过可显示的最大日志条数，设备会自动清除前面的日志。

交换机的日志按重要性划分为七种等级，可按等级进行信息过滤。数值越小，紧急程度越高。

信息级别	数值	描述
Emergency	1	系统不可用信息
Alert	2	需要立刻做出反应的信息
Critical	3	严重信息
Error	4	错误信息
Warning	5	警告信息
Info	6	需要记录的通知信息
Debug	7	调试过程产生的信息

在「设备管理」>「日志管理」>「日志信息」页面中，您可以查看、下载及删除交换机的日志信息。

序号	日志时间	系统日志	信息等级
1	2021/07/04 01:55:48	web client user admin login from 192.168.0.125	Info
2	2021/07/04 01:29:54	web client user admin login from 192.168.0.125	Info
3	2021/07/04 01:20:44	web client user admin login from 192.168.0.125	Info
4	2021/07/04 00:56:33	web client user admin login from 192.168.0.125	Info
5	2021/07/04 00:49:58	web client user admin login from 192.168.0.125	Info

参数说明

标题项	说明
日志信息等级分类	日志信息分类，根据日志信息的等级来筛选显示日志。All 表示显示所有日志。
序号	日志序号。
日志时间	日志信息产生的具体时间。
系统日志	日志的内容。
信息等级	日志信息的等级。

8.3.2 服务器设置

在「设备管理」>「日志管理」>「服务器设置」页面中，您可以配置日志服务器，将交换机的日志上传到该服务器中。

日志信息 **服务器设置**

服务器使能

日志等级 debug

服务器IP地址 . . .

端口

确定

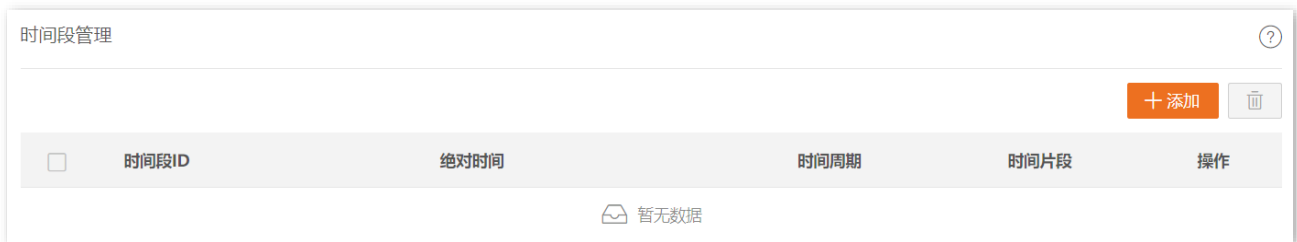
参数说明

标题项	说明
服务器使能	开启/关闭日志服务器功能。
日志等级	该级别及以上的的日志信息将上传到服务器。
服务器 IP 地址	日志服务器的 IP 地址。需确保该日志服务器与本交换机路由可达。
端口	日志服务器使用的端口号。

8.4 时间段管理

时间段管理，通过设置特定的绝对时间、时间周期、时间片段，来控制 [ACL 功能](#)或 [PoE 功能](#)在指定的时间段生效。

在「设备管理」>「时间段管理」页面中，您可以根据实际需要配置时间段。



参数说明

标题项	说明
时间段 ID	时间段编号。
绝对时间	时间段的绝对时间区间。
时间周期	时间段的周期。
时间片段	时间段的时间片段。最多配置三个片段。



- 绝对时间、时间周期、时间片段若只配置一种，则按照一种时间生效；若配置 2 种或 3 种，则取时间的交集生效。例如：绝对时间为“2019-11-13 00:00~2019-12-13 23:59”，时间周期为“周一”，时间片段为“08:00-20:00”。则时间段生效时间为 2019-11-13~2019-12-13 内的每周一早上 8 点到晚上 8 点。
- 若只配置时间片段，则默认为每天的这个时间片段生效。
- 若只配置时间周期，如周一，则默认为每个周一的 24 小时都生效。

8.5 RMON

8.5.1 概述

RMON (Remote Monitoring, 远程网络监控) 基于 SNMP 体系结构, 是 IETF (Internet Engineering Task Force, 因特网工程任务组) 提出的标准监控规范, 它使 SNMP 更为有效地监控远程设备。利用 RMON 功能, 网络管理员可以快速跟踪网络、子网或设备出现的故障, 积极采取防范措施, 防止网络资源失效。同时 RMON MIB 也可以记录网络性能和故障的数据, 网络管理员可以在任何时候访问历史数据从而进行有效的故障诊断。RMON 减少了 SNMP 管理者同代理间的通信流量, 使得网络管理员可以简单而有效地管理大型网络。

RMON 的工作机制

RMON 系统由代理和网管工作站两部分构成。本交换机属于 RMON 代理。

RMON 代理在 RMON MIB 中存储网络信息, 交换机置入 RMON 代理后, 具备了 RMON 探测功能。网管工作站使用 SNMP 的基本命令与 RMON 代理交互数据信息, 收集网络管理信息。

RMON 组

本交换机支持 RMONv1, RMONv1 中定义了多个 RMON 组, 本交换机实现了公有 MIB 中支持的统计组、历史组、事件组、告警组。

■ 统计组

统计组规定系统将持续地对以太网接口的各种流量信息进行统计, 并将统计结果存储在以太网统计表中以便网络管理者随时查看。在指定接口下创建统计表项成功后, 统计组就对当前接口的报文数进行统计, 它统计的结果是一个连续的累加值。

统计信息包括网络冲突数、校验错误报文数、过小 (或超大) 的数据报文数、广播\组播的报文数以及接收字节数、接收数据包数等。

■ 历史组

历史组规定系统将按指定周期对端口的各种流量信息进行统计, 并将统计结果存储在历史记录表中以便网络管理者随时查看。历史组统计的是每个周期内端口接收报文的情况, 周期的长短可以自定义设置。

统计信息包括丢包次数、接收字节数、单播\广播\组播的报文数、校验错误报文数、过小 (或超大) 的数据报文数、冲突包数等。

■ 告警组

RMON 告警管理可对指定的告警变量（如端口收到的报文总数）进行监视。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

■ 事件组

事件组用来定义事件索引号及事件的处理方式。事件组定义的事件用于告警组表项中。当监控对象达到告警条件时，就会触发事件，事件有 Log 和 Trap 两种处理方式。

8.5.2 统计组

在「设备管理」>「RMON」>「统计组」页面，您可以配置 RMON 的统计组。



参数说明

标题项	说明
索引	该统计表项对应的索引号。
端口	要定义统计表项的端口，每个端口下只能定义一个统计表项。
所有者	该表项的创建者。
状态	与该索引对应的统计表项的状态。

8.5.3 历史组

在「设备管理」>「RMON」>「历史组」页面，您可以配置 RMON 的历史组。



参数说明

标题项	说明
索引	该历史表项对应的索引号。
端口	要定义历史表项的端口。
采样条数	该历史表项对应的历史表容量，当历史表的容量达到最大值时，系统会删除最早的记录来保存新的统计值。
采样周期（秒）	采样的时间间隔。
所有者	该表项的创建者。
状态	与该索引对应的统计表项的状态。

8.5.4 告警组

在「设备管理」>「RMON」>「告警组」页面，您可以配置 RMON 的告警组。



参数说明

标题项	说明
索引	该告警表项对应的索引号。
采样时间间隔(秒)	采样的时间间隔。
监控节点	监控统计组的数据类型。
监控端口	进行统计和监控的端口。
采样类型	<p>采样类型包括绝对值采样和变化值采样。</p> <ul style="list-style-type: none">- 绝对值采样：设备按照采样间隔获取告警节点的值，直接用告警节点的值或者计算后获得的值和上限阈值、下限阈值进行比较，来触发对应的事件。- 变化值采样：设备按照采样间隔对告警节点进行采样，并用当前采样时间点获取的值减去上一个采样时间点获取的值，得到告警节点在采样间隔内的变化值，直接用告警节点的变化值或者计算后得到的值和上限阈值、下限阈值进行比较，来触发对应的事件。
最近一次采样值	最近一次采样的数据。
上限	告警阈值上限/下限。
下限	
超过阈值上限所执行的事件	当告警变量的值超过阈值上限/低于阈值下限时所执行的事件。
低于阈值下限所执行的事件	
所有者	该表项的创建者。
状态	与该索引对应的告警表项的状态。

8.5.5 事件组

在「设备管理」>「RMON」>「事件组」页面，您可以配置 RMON 的事件组。



参数说明

标题项	说明
索引	该事件表项对应的索引号。
描述	事件的描述信息。
动作	当该事件被触发时，系统会执行的动作。 <ul style="list-style-type: none">Log：将事件相关信息（事件发生的时间、事件的内容等）记录在本设备 RMON MIB 的事件日志表中，以便管理设备通过 SNMP Get 操作进行查看。Trap：表示事件被触发时，本交换机会生成 Trap 信息发送给网管工作站。
最近一次事件发生的时间	最近一次事件发生的时间。
所有者	该表项的创建者。
状态	与该索引对应的事件表项的状态。

8.5.6 日志

在「设备管理」>「RMON」>「日志」页面，您可以查看 RMON 事件触发生成的相关日志。



参数说明

标题项	说明
索引	日志所对应的事件表项的索引号。
日志表项	日志序号。
日志生成时间	日志信息产生的具体时间。
日志描述	日志的内容。

9 可视化

对于一些无需接入互联网的网络（如：大中型安防监控网络），无法使用云管理方式进行统一管理维护，日常网络维护繁琐。

通过交换机的可视化功能，您在本地即可对网络中的设备进行统一管理。该功能使用 LLDP、UPnP、ARP 等协议，能够自动发现连接到本交换机的设备（如：路由器、交换机、网络摄像机、AP 等），并自动生成网络拓扑图，您可以在该拓扑图上统一查看和设置这些设备的基本参数。

9.1 全局地图

在「可视化」>「全局地图」页面中，您可以查看和设置连接到本交换机的设备的基本参数。




参数说明

标题项	说明
全局地图	统计本交换机所在局域网中各类型设备的在线数量和离线数量。

● 在线

标题项	说明
<input type="radio"/> 离线	地图中绿色表示设备在线，灰色表示设备已离线。
<input checked="" type="checkbox"/> 显示端口	勾选后，在拓扑图中显示设备连接到交换机的物理端口号。 如“ge5”表示物理端口 5。
<input checked="" type="checkbox"/> 显示IP	勾选后，在拓扑图中显示设备的 IP 地址和设备名称。
<input checked="" type="checkbox"/> 显示设备名	当前网络的拓扑视图样式。 <ul style="list-style-type: none">- 本地视图：以本交换机为根节点的拓扑视图。- 主视图：以主设备为根节点的拓扑视图。
本地视图/主视图	 注意 <ul style="list-style-type: none">- 本交换机不是主设备，且拓扑中只有一台主设备时，才能查看主视图。- 主设备为网络中的核心交换设备，您可自定义某设备为主设备。
<input type="checkbox"/> 自动刷新	勾选后，将自动更新网络拓扑图。更新周期为 10 分钟。
 刷新	手动更新网络拓扑图。
 保存	将网络拓扑图以 png 格式图片保存到本地电脑。 根据电脑处理器配置的不同，最大支持下载保存 1000 个设备拓扑图。
 清除离线	清除拓扑图中的离线设备，同时删除这些设备在可视化页面的所有配置。
 清除所有	清除拓扑图中的所有设备，然后重新生成拓扑图。
	查看拓扑中的环路警告信息。警告信息每 30 秒自动刷新。
	拓扑图纵向/横向展开显示。
	
<input type="button" value="+"/> <input type="button" value="-"/>	放大或缩小拓扑图，您也可以使用鼠标滚轮实现该操作。

搜索设备

点击 ，您可以搜索相应设备。


可以根据预置的设备类型分类进行快速搜索，也可以在搜索栏中进行精确搜索。点击具体设备，可以快速定位到拓扑图中相应的位置。




查看或修改本设备相关参数

点击本交换机图标，您可以查看和修改交换机的相关参数。




 **发现设备**：刷新网络拓扑图。


 **端口配置**：禁用或启用各端口。

查看或修改其他设备相关参数

点击其它设备图标，您可以查看和修改这些设备的相关参数。



 : 跳转到设备的 Web 管理页面。
WEB登录

 : 检查设备的网络连通性。
连通性检测

9.2 设备列表

在「可视化」>「设备列表」页面中，您可以查看和修改所有设备的基本信息。

<input type="checkbox"/>	设备名称	设备类型	设备型号	设备状态	MAC地址	IP地址	操作
<input type="checkbox"/>	TEG5328P-...	路由器	TEG5328P-24-410W	在线	00E0.4C11.1111	192.168.0.11	
<input type="checkbox"/>		其他设备		离线	0000.0000.0001	192.168.50.226	

参数说明

标题项	说明
设备名称	<p>设备的名称。为空则表示协议报文中没有该字段，您可以点击 修改设备名称。</p> <p> 提示</p> <p>在此处修改设备名称，只会修改此设备在可视化管理页面的显示，而不是修改协议报文的对应字段。</p>
设备类型	<p>设备的类型。您可以点击 修改设备。</p> <p> 提示</p> <p>在此处修改设备类型，只会修改此设备在可视化管理页面的显示，而不是修改协议报文的对应字段。</p>
设备型号	<p>设备的型号。为空则表示协议报文中没有该字段，您可以点击 修改设备名称。</p>
设备状态	<p>设备在线状态。</p>
MAC 地址	<p>设备的 MAC 地址。</p>
IP 地址	<p>设备的 IP 地址。</p>

10 PoE 管理

10.1 概述

PoE（Power over Ethernet，以太网供电，又称远程供电）是指设备通过以太网线对外接 PD（Powered Device，受电设备）设备（如 IP 电话、无线 AP、网络摄像头等）进行供电。

PoE 供电具有以下优点：

- 连接简捷：网络终端不需外接电源，只需要一根网线。
- 可靠：PD 设备通过 PoE 电源供电，也可以连接其他电源，实现电源冗余备份。
- 标准：符合 IEEE 802.3af 标准和 IEEE 802.3at 标准，使用全球统一的电源接口。
- 应用广泛：可以用于 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、数据采集等。

交换机支持 PoE 功能的端口能自动检测 PD 设备，并为符合 IEEE 802.3af 和 IEEE 802.3at 标准的 PD 设备供电。由于系统及每个端口的功率有限，为了保证给每个 PD 设备提供合适的功率以及充分利用系统功率，必须要对交换机进行一些设置。

10.2 全局设置

在「PoE 管理」>「全局设置」页面中，您可以查看电源信息，配置电源管理模块。

全局设置	端口设置
电源管理模式	动态分配
可用总功率	370W
剩余总功率	370.00W
PoE芯片温度	39.94°C

确定

参数说明

标题项	说明
电源管理模式	<p>交换机 PoE 供电的电源管理模式。</p> <ul style="list-style-type: none">- 静态分配：手动设置交换机各端口的功率，当该端口供电时，该部分功率将被强行预留到该端口，不可被其他端口使用。- 动态分配：根据端口实际使用功率自动分配，当达到满负荷时，根据端口优先级（优先级+端口号）设置进行分配，优先级相同时比较端口号，端口越小优先级越高。
可用总功率	交换机支持的最大供电总功率。
剩余总功率	交换机剩余的功率。
PoE 芯片温度	PoE 芯片的温度。

10.3 端口设置

在「PoE 管理」>「端口设置」页面中，您可以配置交换机各端口的 PoE 功能相关参数。

端口	启用PoE	供电标准	输送功率	PD等级	优先级	静态分配功率	时间段ID	操作
1	启用	AT	0.00W	--	低	30.0W	--	
2	启用	AT	0.00W	--	低	30.0W	--	
3	启用	AT	0.00W	--	低	30.0W	--	
4	启用	AT	0.00W	--	低	30.0W	--	
5	启用	AT	0.00W	--	低	30.0W	--	

参数说明

标题项	说明
端口	端口编号。
启用 PoE	端口的 PoE 供电状态。 <ul style="list-style-type: none"> - 启用：端口供电功能开启。 - 禁用：端口供电功能关闭。 - 不改变：端口供电状态保持不变。
供电标准	当前端口的供电标准。 <ul style="list-style-type: none"> - AT：IEEE 802.3at 供电标准，每个端口的分配功率最大为 30W。 - AF：IEEE 802.3af 供电标准，每个端口的分配功率最大为 15.4W。
输送功率	端口实时的 PoE 供电功率。
PD 等级	正常供电时当前端口连接的受电设备的等级，交换机自动获取设备该等级。
优先级	当前端口优先级，只在电源管理模式为动态模式才生效。 <p>配置合理的端口优先级，可保证满负荷供电状态下特定端口仍能正常供电。优先级不同的端口之间，先保证高优先级端口的所需分配功率。优先级相同的端口之间，先保证序号较小端口的所需分配功率。</p>

标题项	说明
静态分配功率	当前端口的静态分配功率，只在电源管理模式为静态分配才生效。
时间段 ID	端口开启 PoE 供电功能的时间，需先在 时间段管理 章节配置好，不指定表示端口的 PoE 供电功能正常生效，不受时间限制。

附录

A 缩略语

缩略语	全称
ACL	访问控制列表 (Access Control List)
ARP	地址解析协议 (Address Resolution Protocol)
BPDU	桥协议数据单元 (Bridge Protocol Data Unit)
Cos	服务等级 (Class of Service)
CIST	公共和内部生成树 (Common and Internal Spanning Tree)
DHCP	动态主机配置协议 (Dynamic Host Configuration Protocol)
DNS	域名系统 (Domain Name System)
DoS	拒绝服务 (Denial of Service)
DSCP	差分服务编码点 (Differentiated Services Codepoint)
ID	身份标识号码 (Identity Document)
IETF	因特网工程任务组 (Internet Engineering Task Force)
IGMP	网络群组管理协议 (Internet Group Management Protocol)
IP	网际协议 (Internet Protocol)
IST	内部生成树 (Internal Spanning Tree)
LLDP	链路层发现协议 (Link Layer Discovery Protocol)

缩略语	全称
LLDP-MED	用于媒体终端发现的链路层发现协议 (Link Layer Discovery Protocol-Media Endpoint Discovery)
LLDPDU	链路层发现协议数据单元 (Link Layer Discovery Protocol Data Unit)
MAC	媒体接入控制 (Medium Access Control)
MIB	管理信息库 (Management Information Base)
MST	多生成树 (Multiple Spanning Tree)
MSTI	多生成树实例 (Multiple Spanning Tree Instance)
MSTP	多生成树协议 (Multiple Spanning Tree Protocol)
ND	邻居发现 (Neighbor Discovery)
OID	对象标识符 (Object Identifier)
OSPF	开放式最短路径优先 (Open Shortest Path First)
PD	受电设备 (Powered Device)
PVID	端口的虚拟局域网标识号 (Port-base VLAN ID)
PoE	以太网供电 (Power over Ethernet)
QoS	QoS 服务质量 (Quality of Service)
RA	路由器通告 (Router Advertisement)
RIP	路由信息协议 (Routing Information Protocol)
RMON	远程网络监控 (Remote Monitoring)
RSTP	快速生成树协议 (Rapid Spanning Tree Protocol)
SNMP	简单网络管理协议 (Simple Network Management Protocol)
STP	生成树协议 (Spanning Tree Protocol)
SYN	同步序列编号 (Synchronize Sequence Numbers)

缩略语	全称
TCI	标签控制信息 (Tag Control Information)
TCN	拓扑更改通知 (Topology Change Notification)
TCP	传输控制协议 (Transmission Control Protocol)
TLV	类型/长度/值 (Type/Length/Value)
ToS	服务类型 (Type of Service)
TPID	标签协议标识 (Tag Protocol Identifier)
TTL	生存时间 (Time to Live)
UDP	用户数据报协议 (User Datagram Protocol)
VoIP	基于 IP 的语音传输 (Voice over Internet Protocol)
VLAN	虚拟局域网 (Virtual Local Area Network)