

**TP-LINK®**

# 简单网管交换机

---

TL-SL2428/TL-SL2452/TL-SG2452

用户手册

REV1.2.0  
1910040420

# 声明

Copyright © 2014 普联技术有限公司

版权所有，保留所有权利

未经普联技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本书部分或全部内容。不得以任何形式或任何方式（电子、机械、影印、录制或其它可能的方式）进行商品传播或用于任何商业、赢利目的。

**TP-LINK®**为普联技术有限公司注册商标。本文档提及的其它所有商标或注册商标，由各自的所有人拥有。

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。可随时查阅我们的万维网页。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

# 目录

<b>第 1 章</b>	<b>用户手册简介</b>	<b>1</b>
1.1	目标读者	1
1.2	本书约定	1
1.3	章节安排	1
<b>第 2 章</b>	<b>产品介绍</b>	<b>4</b>
2.1	产品简介	4
2.2	产品特性	4
2.3	产品外观	5
2.3.1	前面板	5
2.3.2	后面板	8
<b>第 3 章</b>	<b>配置指南</b>	<b>10</b>
3.1	登录 Web 页面	10
3.2	Web 页面简介	11
3.2.1	页面总览	11
3.2.2	页面常见按键及操作	12
<b>第 4 章</b>	<b>系统管理</b>	<b>14</b>
4.1	系统配置	14
4.1.1	系统信息	14
4.1.2	设备描述	16
4.1.3	系统时间	17
4.1.4	夏令时	18
4.1.5	管理 IP	19
4.2	用户管理	20
4.2.1	用户列表	21
4.2.2	用户配置	21
4.3	系统工具	22
4.3.1	配置导入	22
4.3.2	配置导出	23
4.3.3	软件升级	23
4.3.4	系统重启	24

4.3.5	软件复位.....	24
<b>4.4</b>	<b>安全管理 .....</b>	<b>25</b>
4.4.1	安全配置.....	25
4.4.2	SSL 配置 .....	26
4.4.3	SSH 配置 .....	27
<b>第 5 章</b>	<b>二层交换.....</b>	<b>34</b>
5.1	端口管理 .....	34
5.1.1	端口配置.....	34
5.1.2	端口监控.....	35
5.1.3	端口安全.....	37
5.1.4	端口隔离.....	39
5.1.5	环路监测.....	40
5.2	汇聚管理 .....	41
5.2.1	汇聚列表.....	42
5.2.2	手动配置.....	43
5.2.3	LACP 配置 .....	44
5.3	流量统计 .....	46
5.3.1	流量概览.....	46
5.3.2	详细统计.....	47
5.4	地址表管理.....	48
5.4.1	地址表显示.....	49
5.4.2	静态地址表.....	50
5.4.3	动态地址表.....	51
5.4.4	过滤地址表.....	53
5.5	DHCP 过滤.....	54
<b>第 6 章</b>	<b>VLAN .....</b>	<b>55</b>
6.1	802.1Q VLAN.....	55
6.1.1	VLAN 配置 .....	57
6.2	802.1Q VLAN 功能的组网应用.....	58
<b>第 7 章</b>	<b>生成树 .....</b>	<b>61</b>
7.1	基本配置 .....	67
7.1.1	基本配置.....	67

7.1.2	生成树信息 .....	69
7.2	端口配置 .....	70
7.3	MSTP 实例 .....	71
7.3.1	域配置 .....	71
7.3.2	实例配置 .....	72
7.3.3	实例端口 .....	74
7.4	安全配置 .....	75
7.4.1	端口保护 .....	75
7.4.2	TC 保护 .....	78
7.5	STP 功能的组网应用 .....	78
<b>第 8 章</b>	<b>组播管理 .....</b>	<b>83</b>
8.1	IGMP 侦听 .....	85
8.1.1	基本配置 .....	86
8.1.2	端口参数 .....	87
8.1.3	VLAN 参数 .....	88
8.1.4	组播 VLAN .....	89
8.2	IGMP 侦听功能组网应用 .....	91
8.3	组播地址表 .....	92
8.3.1	地址表显示 .....	92
8.3.2	静态地址表 .....	93
8.4	组播过滤 .....	95
8.4.1	过滤地址 .....	95
8.4.2	端口过滤 .....	96
8.5	报文统计 .....	97
<b>第 9 章</b>	<b>服务质量 .....</b>	<b>99</b>
9.1	QoS 配置 .....	99
9.1.1	端口配置 .....	102
9.1.2	802.1P/CoS 映射 .....	104
9.1.3	DSCP 映射 .....	105
9.1.4	队列调度模式 .....	106
9.2	流量管理 .....	107
9.2.1	带宽控制 .....	107

9.2.2	风暴抑制.....	108
9.3	语音 VLAN .....	111
9.3.1	全局配置.....	112
9.3.2	端口配置.....	113
9.3.3	OUI 配置 .....	115
<b>第 10 章</b>	<b>访问控制.....</b>	<b>117</b>
10.1	ACL 配置.....	117
10.1.1	ACL 列表.....	117
10.1.2	新建 ACL.....	118
10.1.3	MAC ACL .....	118
10.1.4	标准 IP ACL.....	119
10.1.5	扩展 IP ACL.....	120
10.2	Policy 配置 .....	120
10.2.1	Policy 列表.....	121
10.2.2	新建 Policy .....	121
10.2.3	配置 Policy .....	122
10.3	绑定配置 .....	122
10.3.1	绑定列表.....	122
10.3.2	端口绑定.....	123
10.3.3	VLAN 绑定 .....	124
10.4	访问控制功能组网应用 .....	125
<b>第 11 章</b>	<b>SNMP .....</b>	<b>127</b>
11.1	SNMP 配置 .....	128
11.1.1	全局配置.....	129
11.1.2	视图管理.....	129
11.1.3	组管理 .....	130
11.1.4	用户管理.....	132
11.1.5	团体管理.....	133
11.2	通知管理 .....	135
11.3	RMON.....	137
11.3.1	历史采样.....	138
11.3.2	事件配置.....	138

11.3.3  警报管理.....	139
<b>第 12 章  系统维护.....</b>	<b>141</b>
12.1  运行状态 .....	141
12.1.1  CPU 监控.....	141
12.1.2  内存监控.....	142
12.2  系统日志 .....	142
12.2.1  日志列表.....	143
12.2.2  本地日志.....	144
12.2.3  远程日志.....	144
12.2.4  日志导出.....	145
12.3  系统诊断 .....	146
12.3.1  线缆检测.....	146
12.3.2  环回检测.....	147
12.4  网络诊断 .....	148
12.4.1  Ping 检测.....	148
12.4.2  Tracert 检测.....	149
<b>附录 A  术语表 .....</b>	<b>150</b>
<b>附录 B  技术参数规格 .....</b>	<b>155</b>

# 第1章 用户手册简介

本手册旨在帮助您正确使用这款交换机。手册中包括对交换机性能特征的描述以及配置交换机的详细说明。请在操作交换机前，详细阅读本手册。

## 1.1 目标读者



本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

## 1.2 本书约定

在本手册中，

- 所提到的“交换机”、“本产品”等名词，如无特别说明，系指TL-SL2428/TL-SL2452/TL-SG2452简单网管交换机，下面简称为TL-SL2428/TL-SL2452/TL-SG2452。
- 鉴于简单网管交换机TL-SL2428/TL-SL2452/TL-SG2452功能相近，本手册中均以TL-SL2428为例。
- 用 >> 符号表示配置页面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**。
- 正文中出现的<>尖括号标记的文字，表示Web页面的按钮名称，如<确定>。
- 正文中出现的**加粗**标记的文字，表示交换机的各个功能的名称，如**端口配置**页面。
- 正文中出现的“ ”双引号标记的文字，表示配置页面上出现的名词，如“IP地址”。

本手册中使用的特殊图标说明如下：

图标	含义
 <b>注意：</b>	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
 <b>说明：</b>	该图标表示此部分内容是对相应设置、步骤的补充说明。

## 1.3 章节安排

章节	章节说明
<a href="#">第1章 用户手册简介</a>	帮助您快速掌握本手册的结构、了解本手册的约定，从而更有效地使用本手册。
<a href="#">第2章 产品介绍</a>	介绍本产品的特性、应用以及外观。
<a href="#">第3章 配置指南</a>	介绍如何登录交换机的Web页面，并简要介绍页面特点。



章节	章节说明
<a href="#">第4章 系统管理</a>	<p>本模块主要用于配置交换机的系统属性，主要介绍了：</p> <ul style="list-style-type: none"> <li>● 系统配置：配置交换机的描述、时间和网络参数。</li> <li>● 用户管理：配置登录交换机Web页面的用户的访问权限和身份。</li> <li>● 系统工具：集中对交换机的配置文件进行管理。</li> <li>● 安全管理：针对不同的登录方式，增强用户管理交换机的安全性。包括安全配置、SSL配置和SSH配置。</li> </ul>
<a href="#">第5章 二层交换</a>	<p>本模块主要用于配置交换机的基本功能，主要介绍了：</p> <ul style="list-style-type: none"> <li>● 端口管理：配置交换机端口的基本属性，包括端口配置、端口监控、端口安全、端口隔离和环路监测。</li> <li>● 汇聚管理：配置端口汇聚组。汇聚是将交换机的多个物理端口聚合在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。</li> <li>● 流量统计：统计流经各个端口的数据信息。</li> <li>● 地址表管理：配置交换机的地址表。地址表是交换机实现报文快速转发的基础。</li> <li>● DHCP过滤：监视主机从DHCP服务器获取IP地址的过程。</li> </ul>
<a href="#">第6章 VLAN</a>	<p>VLAN主要用于隔离广播域，通过划分虚拟工作组来简化网络管理，主要介绍了：</p> <ul style="list-style-type: none"> <li>● 802.1Q VLAN：划分基于端口的VLAN。</li> </ul>
<a href="#">第7章 生成树</a>	<p>生成树主要用于在局域网中消除环路。本模块主要用于配置交换机的生成树功能，主要介绍了：</p> <ul style="list-style-type: none"> <li>● 基本配置：配置和查看交换机生成树功能的全局属性。</li> <li>● 端口配置：配置端口的CIST参数。</li> <li>● MSTP实例：配置MSTP实例。</li> <li>● 安全配置：配置保护功能，以防止生成树网络中的设备遭受恶意攻击。</li> </ul>
<a href="#">第8章 组播管理</a>	<p>本模块主要用于配置交换机的组播管理功能，主要介绍了：</p> <ul style="list-style-type: none"> <li>● IGMP侦听：配置IGMP侦听的全局参数、端口属性、VLAN参数和组播VLAN。IGMP侦听可以有效抑制组播数据在网络中扩散。</li> <li>● 组播地址表：配置组播地址表。交换机在转发组播数据时是根据组播地址表来进行的。</li> <li>● 组播过滤：配置组播过滤功能，可以限制用户对组播节目的点播。</li> <li>● 报文统计：查看各端口的组播报文流量，帮助您监控网络中IGMP报文。</li> </ul>
<a href="#">第9章 服务质量</a>	<p>本模块主要为网络中某些特殊应用程序提供保障，主要介绍了：</p> <ul style="list-style-type: none"> <li>● QoS配置：给网络中的数据流划分优先级，保障重要数据的传输，可分为端口优先级、802.1P优先级和DSCP优先级。</li> <li>● 流量管理：可通过带宽控制来限制端口的数据流量；风暴抑制可限制局域网中各类广播包的传输带宽，节约网络资源。</li> <li>● 语音VLAN：在指定VLAN中传输语音数据，提高语音数据的传输优先级，保证通话质量。</li> </ul>

章节	章节说明
<a href="#">第10章 访问控制</a>	<p>本模块通过配置对报文的匹配规则和处理操作来实现对数据包的过滤功能，有效防止非法用户对网络的访问，节约网络资源，主要介绍了：</p> <ul style="list-style-type: none"> <li>● ACL配置：配置ACL条目。</li> <li>● Policy配置：配置ACL规则的处理方式。</li> <li>● 绑定配置：将Policy下发到端口和VLAN，使之正式生效。</li> </ul>
<a href="#">第11章 SNMP</a>	<p>SNMP提供了一个管理框架来监控和维护互联网设备。本模块主要用于配置交换机的SNMP功能，主要介绍了：</p> <ul style="list-style-type: none"> <li>● SNMP配置：配置SNMP的基本属性。</li> <li>● 通知管理：配置SNMP通知管理，便于管理软件对交换机某些事件进行及时监控和处理。</li> <li>● RMON：配置RMON功能，便于网管更有效的监控网络。</li> </ul>
<a href="#">第12章 系统维护</a>	<p>系统维护模块将管理交换机的常用系统工具组合在一起，主要介绍了：</p> <ul style="list-style-type: none"> <li>● 运行状态：对交换机内存和CPU进行监控。</li> <li>● 系统日志：查看在交换机上配置的参数。</li> <li>● 系统诊断：检测与交换机连接的线缆及对端设备的可用性。</li> <li>● 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。</li> </ul>
<a href="#">附录 A 术语表</a>	整理用户手册中出现的术语。
<a href="#">附录 B 技术参数规格</a>	技术参数规格表。

[回目录](#)

## 第2章 产品介绍

### 2.1 产品简介

TL-SL2428/TL-SL2452/TL-SG2452交换机是由普联技术有限公司自主设计和开发的，为构建高安全、高性能网络需求而专门设计的新一代简单网管交换机，具有完备的安全策略、完善的QoS策略、丰富的VLAN特性、易管理维护等特点。系统采用全新的软硬件平台，在安全接入策略、多业务支持、易管理和维护等方面为用户提供了全新的技术特性和解决方案，是理想的办公网、校园网以及中小企业、分支机构的汇聚、接入层交换机。

### 2.2 产品特性

- 符合IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3z标准；
- TL-SL2428提供24个10/100Mbps自适应RJ45端口和4个10/100/1000Mbps自适应RJ45端口，TL-SL2452提供48个10/100Mbps自适应RJ45端口和2个10/100/1000Mbps自适应RJ45端口，TL-SG2452提供48个10/100/1000Mbps自适应RJ45端口；
- TL-SL2428提供2个共享的100/1000Mbps SFP光口，TL-SL2452提供2个1000Mbps SFP光口，TL-SG2452提供4个1000Mbps SFP光口；
- 采用两级用户管理方式，增强交换机的管理安全性；
- 全双工流控符合IEEE 802.3x标准，半双工采用Backpressure标准；
- 端口支持N-Way自协商功能，自动调整传输方式和传输速度；
- 支持16K MAC地址；
- 支持MAC地址自动学习、自动老化及老化时间设置；
- 支持静态MAC地址、过滤MAC地址、动态MAC绑定等地址表管理功能；
- 基于IEEE 802.1Q的Tag VLAN；
- 支持端口安全控制、广播风暴抑制、环路监测等功能；
- 支持基于端口的入口/出口带宽控制；
- 支持手动和LACP两种方式端口汇聚功能；
- 支持端口镜像和流量统计功能；
- 支持L2-L4数据流的访问控制列表（ACL）；
- 支持基于端口、IEEE 802.1p及DSCP的优先级配置模式；
- 支持QoS功能；
- 支持组播侦听功能；
- 提供方便易用的WEB可视化管理；
- 提供多级用户、身份过滤等安全管理功能；
- 提供电缆检测（VCT）功能。

## 2.3 产品外观

### 2.3.1 前面板

TL-SL2428的前面板由24个10/100Mbps端口、4个10/100/1000Mbps端口、2个SFP模块扩展槽、Reset按钮以及相关的LED灯组成，如图 2-1所示。

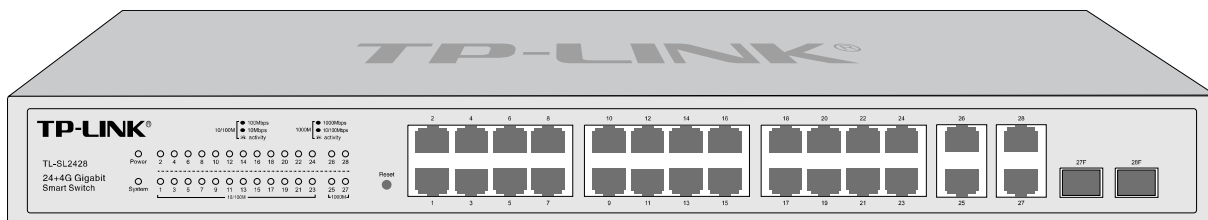


图 2-1 TL-SL2428前面板

#### ➤ 24个10/100Mbps自适应RJ45端口

本交换机的1-24端口均支持10/100Mbps带宽的连接设备。每个端口对应一个10/100Mbps指示灯。

#### ➤ 4个10/100/1000Mbps自适应RJ45端口

本交换机的25-28端口均支持10/100/1000Mbps带宽的连接设备。每个端口对应一个1000Mbps指示灯。

#### ➤ 2个SFP端口

SFP模块卡扩展槽位于千兆RJ45端口的右边，同与其Combo共享的千兆RJ45端口共用指示灯，其中27F与端口27共用，28F与端口28共用。

#### ➤ Reset键

复位键。复位操作为：通电状态下长按Reset键5秒，待System指示灯快速闪烁3次后松开Reset键，交换机将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为<http://192.168.0.1>，默认用户名和密码均为admin。

#### ➤ 指示灯

指示灯包括Power、System、10/100Mbps、1000Mbps指示灯。通过指示灯您可以监控交换机的工作状态，下表将详细说明指示灯工作状态：

指示灯	名称	状态	描述
Power	电源指示灯	常亮	系统供电正常
		闪烁	系统供电异常
		熄灭	系统未通电或供电异常
System	系统指示灯	常亮	系统出现异常
		闪烁	系统正常工作
		熄灭	系统出现异常

指示灯	名称	状态	描述
10/100Mbps	端口指示灯	常亮	端口连接网络设备
		闪烁	端口接收和发送数据
		绿色	端口与设备相连且工作在百兆模式
		黄色	端口与设备相连且工作在十兆模式
		熄灭	端口未连接网络设备
1000Mbps	端口指示灯	常亮	端口连接网络设备
		闪烁	端口接收和发送数据
		绿色	端口与设备相连且工作在千兆模式
		黄色	端口与设备相连且工作在十兆或百兆模式
		熄灭	端口未连接网络设备



### 注意:

- 对于TL-SL2428，若需要使用SFP端口，插入光纤模块后，请登录交换机管理界面配置SFP端口的端口参数（出厂默认设置的速率双工模式为1000Mbps全双工）。如果使用的是百兆光纤模块，相应SFP口的速率双工模式请配置为100Mbps全双工；如果使用的是千兆光纤模块，相应SFP口的速率双工模式请配置为1000Mbps全双工。详见[5.1.1 端口配置](#)。

TL-SL2452的前面板由48个10/100Mbps端口、2个10/100/1000Mbps端口、2个SFP模块扩展槽、Reset按钮以及相关的LED灯组成，如图 2-3所示。

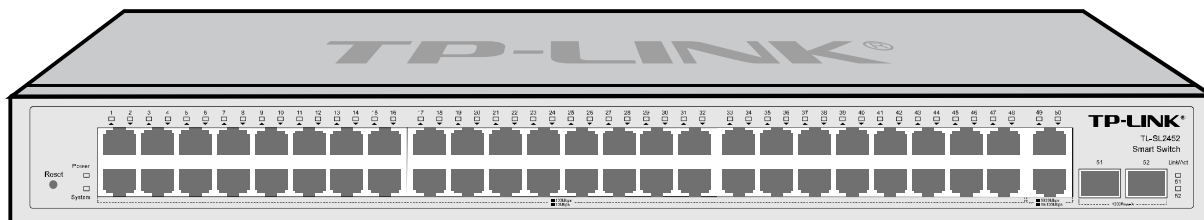


图 2-2 TL-SL2452前面板

#### ➤ 48个10/100Mbps自适应RJ45端口

本交换机的1-48端口均支持10/100Mbps带宽的连接设备。每个端口对应一个10/100Mbps指示灯。

#### ➤ 2个10/100/1000Mbps自适应RJ45端口

本交换机的49-50端口均支持10/100/1000Mbps带宽的连接设备。每个端口对应一个10/100/1000Mbps指示灯。

#### ➤ 2个SFP端口

SFP模块卡扩展槽位于千兆RJ45端口的右边，每个端口对应有一个Link/Act指示灯。

#### ➤ Reset键

复位键。复位操作为：通电状态下长按Reset键5秒，待System指示灯快速闪烁3次后松开Reset键，交换机将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为http://192.168.0.1，默认用户名和密码均为admin。

## ➤ 指示灯

指示灯包括Power、System、10/100Mbps、10/100/1000Mbps、Link/Act指示灯。通过指示灯您可以监控交换机的工作状态，下表将详细说明指示灯工作状态：

指示灯	名称	状态	描述
Power	电源指示灯	常亮	系统供电正常
		闪烁	系统供电异常
		熄灭	系统未通电或供电异常
System	系统指示灯	常亮	系统出现异常
		闪烁	系统正常工作
		熄灭	系统出现异常
10/100Mbps	端口指示灯	常亮	端口连接网络设备
		闪烁	端口接收和发送数据
		绿色	端口与设备相连且工作在百兆模式
		黄色	端口与设备相连且工作在十兆模式
		熄灭	端口未连接网络设备
10/100/1000Mbps	端口指示灯	常亮	端口连接网络设备
		闪烁	端口接收和发送数据
		绿色	端口与设备相连且工作在千兆模式
		黄色	端口与设备相连且工作在十兆或百兆模式
		熄灭	端口未连接网络设备
Link/Act	SFP口指示灯	常亮	SFP口连接千兆设备但没有数据传输
		闪烁	SFP口连接千兆设备且正在接收或发送数据
		熄灭	SFP口未连接千兆设备或连接异常



**注意：**

- TL-SL2452的SFP端口只支持千兆光纤模块。

TL-SG2452的前面板由48个10/100/1000Mbps端口、4个SFP模块扩展槽、Reset按钮以及相关的LED灯组成，如图 2-3所示。

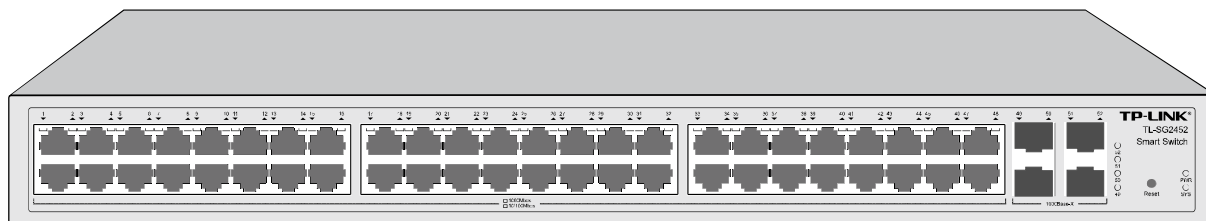


图 2-3 TL-SG2452前面板

### ➤ 48个10/100/1000Mbps自适应RJ45端口

本交换机的1-48端口均支持10/100/1000Mbps带宽的连接设备。每个端口对应一个1000Mbps指示灯。

### ➤ 4个SFP端口

SFP模块卡扩展槽位于千兆RJ45端口的右边，每个端口对应一个1000Mbps指示灯。

### ➤ Reset键

复位键。复位操作为：通电状态下长按Reset键5秒，待SYS指示灯快速闪烁3次后松开Reset键，交换机将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为http://192.168.0.1，默认用户名和密码均为admin。

### ➤ 指示灯

指示灯包括PWR、SYS、10/100/1000Mbps指示灯。通过指示灯您可以监控交换机的工作状态，下表将详细说明指示灯工作状态：

指示灯	名称	状态	描述
PWR	电源指示灯	常亮	系统供电正常
		闪烁	系统供电异常
		熄灭	系统未通电或供电异常
SYS	系统指示灯	常亮	系统出现异常
		闪烁	系统正常工作
		熄灭	系统出现异常
10/100/1000Mbps	端口指示灯	常亮	端口连接网络设备
		闪烁	端口接收和发送数据
		绿色	端口与设备相连且工作在千兆模式
		黄色	端口与设备相连且工作在十兆或百兆模式
		熄灭	端口未连接网络设备



注意：

- TL-SG2452的SFP端口只支持千兆光纤模块。

## 2.3.2 后面板

TL-SL2428/TL-SL2452/TL-SG2452后面板由电源接口和防雷接地柱组成，如图 2-4所示（以TL-SL2428为例）：

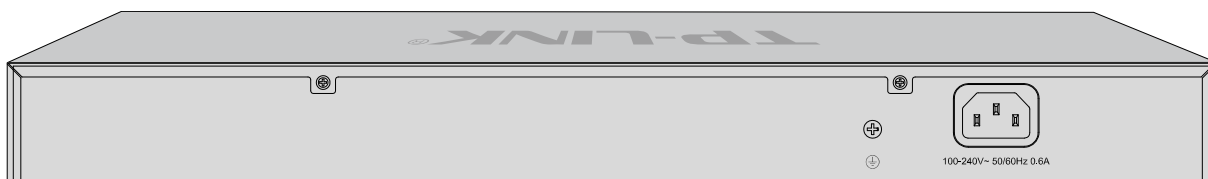


图 2-4 后面板

➤ 电源接口

位于后面板右侧，接入电源需为100-240V~ 50/60Hz的交流电源。

➤ 防雷接地柱

位于电源接口左侧，请使用导线接地，以防雷击。



**注意：**

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

[回目录](#)



## 第3章 配置指南

### 3.1 登录Web页面

第一次登录时，请确认以下几点：

- 1) 交换机已正常加电启动，任一端口已与管理主机相连。
- 2) 管理主机已正确安装有线网卡及该网卡的驱动程序、并已正确安装IE 6.0或以上版本的浏览器。
- 3) 管理主机IP地址已设为与交换机端口同一网段，即192.168.0.X（X为2至254之间的任意整数），子网掩码为255.255.255.0。
- 4) 为保证您更好地体验Web页面显示效果，建议您将显示器的分辨率调整到1024×768或以上像素。

打开IE浏览器，在地址栏输入<http://192.168.0.1> 登录交换机的Web页面。



交换机登录页面如图 3-1所示。



图 3-1 登录页面

在此页面输入交换机管理帐号的用户名和密码，出厂默认值为admin/admin。成功登录后可以看到交换机的系统信息，如图 3-2所示。

系统信息	
系统描述：	24FE+4GE Smart Switch
设备名称：	TL-SL2428
设备位置：	SHENZHEN
联系方法：	www.tp-link.com.cn
硬件版本：	TL-SL2428 1.0
软件版本：	1.0.0 Build 20130104 Rel.37783
IP地址：	192.168.0.1
子网掩码：	255.255.255.0
默认网关：	
MAC地址：	00-0A-EB-13-12-7C
系统时间：	2006-01-01 08:52:06
运行时间：	0 day - 0 hour - 52 min - 8 sec

图 3-2系统信息

## 3.2 Web页面简介

### 3.2.1 页面总览

交换机典型的Web页面如图 3-3所示。

**TP-LINK**

TL-SL2428

基本配置 端口参数 VLAN参数 组播VLAN

**VLAN参数**

VLAN ID:  (1-4094)

路由器端口时间:  秒 (60-600, 推荐300秒)

成员端口时间:  秒 (60-600, 推荐260秒)

离开滞后时间:  秒 (1-30, 推荐1秒)

静态路由端口:  (格式为: 1-3,6,8)

**VLAN列表**

选择	VLAN ID	路由器端口时间	成员端口时间	离开滞后时间	路由器端口
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**注意：**  
当组播VLAN功能启用时，此处配置将失效。

图 3-3 典型Web页面

在图 3-4中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，您可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域可分为三部分，条目配置区、列表管理区以及提示和注意区。



图 3-4 Web页面区域划分

### 3.2.2 页面常见按键及操作

#### 主菜单区按键

按键	含义
<a href="#">配置保存</a>	保存最终的配置。
<a href="#">退出登录</a>	退出Web页面。



#### 注意:

- 配置交换机后，点击<提交>按键当前配置立即生效，但重启后参数将失效；若需要当前配置在交换机重启后依旧生效，则需要点击<配置保存>按钮，建议在交换机断电或重启前<配置保存>。

#### 条目配置区常见按键





按键	含义
<a href="#">提交</a>	提交当前的配置。
<a href="#">添加</a>	添加当前配置条目。
<a href="#">修改</a>	修改并保存编辑后的配置信息。
<a href="#">清空</a>	快速清空当前配置项中已输入的所有信息。
<a href="#">帮助</a>	打开当前功能的帮助页面。



#### 说明:

- <修改>按键只有在编辑列表中的条目时才会出现，取代原本的<新增>按键。

➤ 列表管理区常见按键

按键	含义
	选中当前列表中所有条目。
	删除选中的条目，可批量操作。
	刷新列表。
	根据所输序号，快速选择至列表中的对应条目。

[返回目录](#)

## 第4章 系统管理

系统管理模块主要用于配置交换机的系统属性，包括系统配置、用户管理、系统工具以及安全管理四个部分。

### 4.1 系统配置

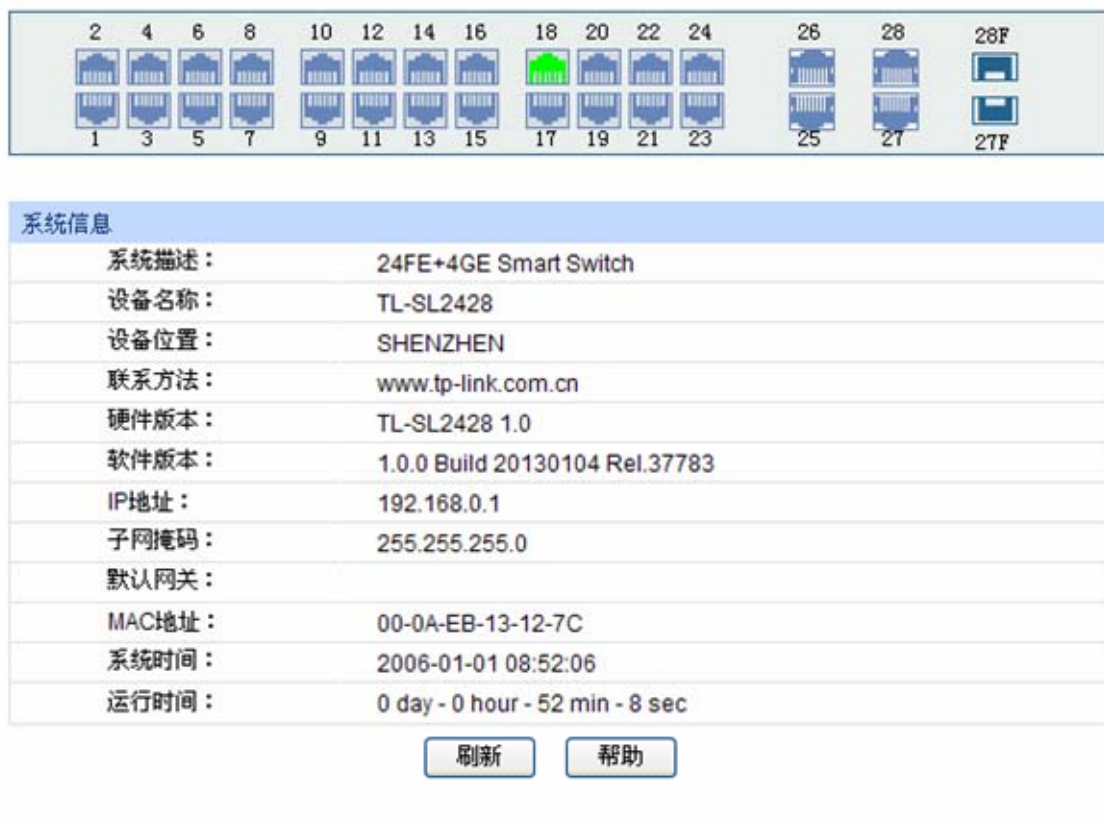
系统配置用于配置交换机的基本属性，本功能包括系统信息、设备描述、系统时间、夏令时和管理IP五个配置页面。

#### 4.1.1 系统信息

本页面用来查看本交换机的端口连接信息和系统信息。

端口状态界面指示了交换机的10/100Mbps RJ45端口、10/100/1000Mbps RJ45端口以及SFP扩展模块槽的工作状态。

进入页面的方法：系统管理>>系统配置>>系统信息



系统信息	
系统描述：	24FE+4GE Smart Switch
设备名称：	TL-SL2428
设备位置：	SHENZHEN
联系方法：	www.tp-link.com.cn
硬件版本：	TL-SL2428 1.0
软件版本：	1.0.0 Build 20130104 Rel.37783
IP地址：	192.168.0.1
子网掩码：	255.255.255.0
默认网关：	
MAC地址：	00-0A-EB-13-12-7C
系统时间：	2006-01-01 08:52:06
运行时间：	0 day - 0 hour - 52 min - 8 sec

图 4-1 系统信息

条目介绍：

#### > 端口状态



100Mbps端口未接入设备。



100Mbps端口工作速率为100Mbps。



100Mbps端口工作速率为10Mbps。



1000Mbps端口未接入设备。



1000Mbps端口工作速率为1000Mbps。



1000Mbps端口工作速率为100Mbps/10Mbps。



SFP端口未接入设备。



SFP端口工作速率为1000Mbps。



SFP端口工作速率为100Mbps。

当鼠标移到某端口上时，会显示该端口的详细信息，如下图所示。

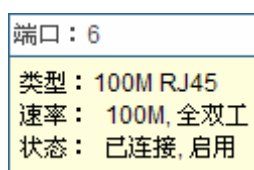


图 4-2 端口信息

条目介绍：

#### ➤ 端口信息

<b>端口：</b>	显示交换机的端口号。
<b>类型：</b>	显示端口的端口类型。
<b>速率</b>	显示端口当前连接速率及传输模式。
<b>状态：</b>	现在端口的状态。

点击某端口，会显示此端口的带宽利用率，即实际传输速率与其最大传输速率的百分比，图中每隔4秒反馈一次监控值。查看各个端口的带宽利用率，可以帮助您及时了解各端口的流量概况，便于监控网络流量和分析网络异常。如下图所示。

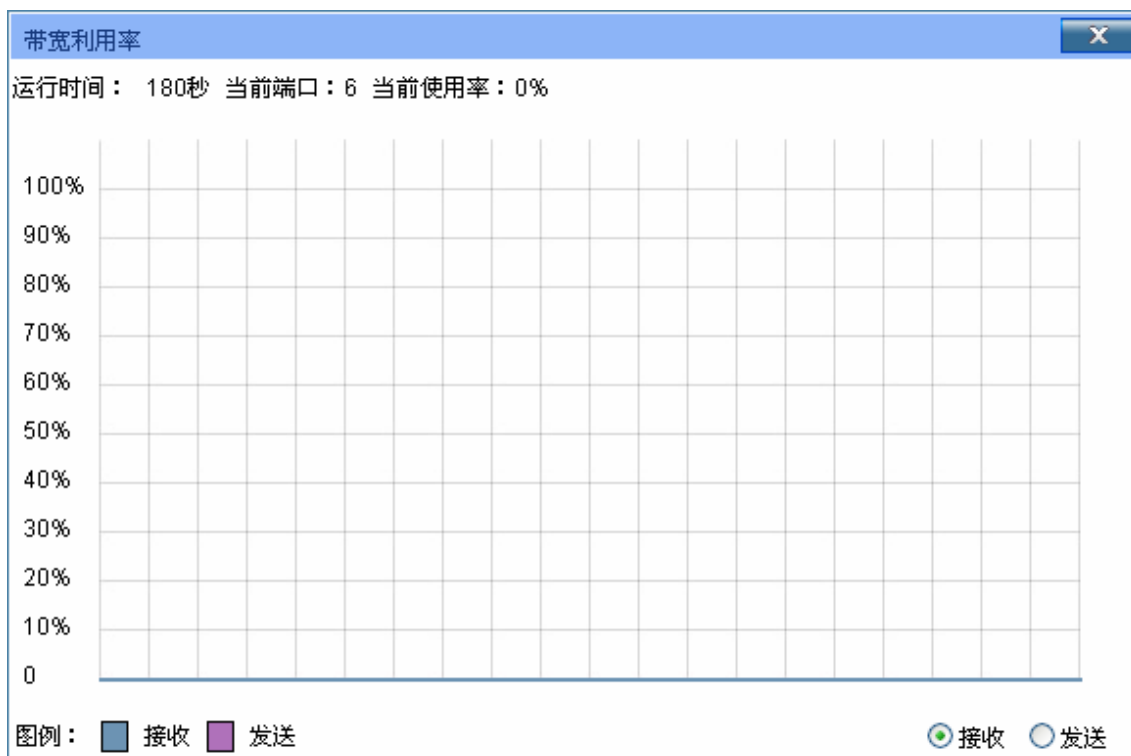


图 4-3 带宽利用率

条目介绍:

➤ 带宽利用率

**接收**

点击后，显示此端口接收数据的带宽利用率。

**发送**

点击后，显示此端口发送数据的带宽利用率。

### 4.1.2 设备描述

本页面用来配置交换机的描述信息，包括设备名称、设备位置、联系方法。

进入页面的方法：系统管理>>系统配置>>设备描述

设备描述	
设备名称：	<input type="text" value="TL-SL2428"/>
设备位置：	<input type="text" value="SHENZHEN"/>
联系方法：	<input type="text" value="www.tp-link.com.cn"/>

**注意：**

设备名称、设备位置和联系方法最长可输入32个字符。

图 4-4 设备描述

条目介绍:

➤ 设备描述

**设备名称:** 填写交换机的名称。

**设备位置:** 填写交换机的位置信息。

**联系方法:** 填写您的联系方法。

### 4.1.3 系统时间

本页面用来配置交换机的系统时间。系统时间是交换机工作时使用的时间，其它功能（如访问控制）中的时间信息以此处为准。可以选择手动设置时间或者连接到一个NTP（网络时间协议）服务器获取UTC时间，也可以获取当前管理PC的时间作为交换机的系统时间。

进入页面的方法：系统管理>>系统配置>>系统时间

时间信息

当前系统时间： 2006-01-01 10:16:08 星期日

当前时间来源： 手动配置时间

时间配置

手动配置时间

日期： 2006 01 01

时间： 10 16 08

从NTP服务器获取时间

时区： (UTC+08:00)北京, 重庆, 香港特别行政区, 乌鲁木齐, 新加坡

首选NTP服务器： 133.100.9.2

备选NTP服务器： 139.78.100.163

更新周期： 12 小时

获取管理PC时间

提交

刷新

帮助

图 4-5 系统时间

条目介绍:

➤ 时间信息

**当前系统时间:** 显示交换机当前的日期、时间。

**当前时间来源:** 显示交换机当前系统时间的来源。

➤ 时间配置

**手动配置时间:** 勾选后，手动配置日期、时间。

**从NTP服务器获取时间:** 勾选后，配置时区和NTP服务器的IP地址，交换机将自动获取UTC时间。此时交换机必须连接至NTP服务器。

- 时区：选择您所在的时区。
- 首选/备选NTP服务器：填写NTP服务器的IP地址。
- 更新周期：设定从NTP服务器获取时间的周期。



**获取管理PC时间:**

勾选后，将管理主机的时间配置为交换机的系统时间。

**注意:**

- 如果向指定的时间服务器请求时间不成功，交换机会选择向上一次成功获取时间的服务器地址和网络上默认的公用时间服务器地址来获取时间。

## 4.1.4 夏令时

本页面用来配置交换机的夏令时功能，包括夏令时状态，预定义模式，循环模式和日期模式。

进入页面的方法：[系统管理](#)>>[系统配置](#)>>[夏令时](#)

夏令时配置

夏令时状态:

预定义模式  
 美国       澳大利亚       欧洲       新西兰

循环模式  
 偏移:  (分钟)

开始时间: 周  日  月

结束时间: 周  日  月

日期模式  
 偏移:  (分钟)

开始时间:    (MM/DD HH:MM)

结束时间:    (MM/DD HH:MM)

图 4-6 夏令时

条目介绍:

### ➤ 夏令时配置

**夏令时状态:**

选择是否启用夏令时。

**预定义模式:**

选择一个事先预定义好的夏令时配置。

- 美国：三月的第二个星期天02:00 ~ 十一月的第一个星期天02:00。
- 澳大利亚：十月的第一个星期天02:00 ~ 四月的第一个星期天03:00。
- 欧洲：三月的最后一个星期天01:00 ~ 十月的最后一个星期天01:00。
- 新西兰：九月的最后一个星期天02:00 ~ 四月第一个星期天03:00。

**循环模式：**

配置夏令时功能。在这一模式下做的配置可以循环使用。

- 偏移：指定当夏令时来临时，需要调整的时间额度。单位为分钟。
- 开始/结束时间：分别选择夏令时开始和结束的时间。

**日期模式：**

配置夏令时功能。在这一模式下做的配置只能生效一次（开始时间的年份为当前年份）。

- 偏移：指定当夏令时来临时，需要调整的时间额度。单位为分钟。
- 开始/结束时间：分别选择夏令时开始和结束的时间。

## 4.1.5 管理IP

网络中的设备都有自己的IP地址，您可以使用交换机的IP地址登录交换机的Web页面。本交换机提供“静态IP”、“DHCP”和“BOOTP”三种IP获取方式，但交换机的IP地址是唯一的，所以使用新的配置方式获取的IP地址会覆盖原有的IP地址。

- “静态IP”获取方式。

需要手动配置交换机的IP地址、子网掩码和默认网关，使用时应根据自己网络的实际情况对这些参数进行配置。管理主机的IP地址必须与此处所配置的IP地址处于同一网段内，才能访问交换机的Web页面。

- “DHCP”获取方式。

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在BOOTP协议基础上进行了优化和扩展而产生的一种网络配置协议，可以实现网络资源的动态配置。交换机作为DHCP客户端，可以从网络中的DHCP服务器上动态获得网络参数，既方便配置，又便于管理。

- “BOOTP”获取方式。

BOOTP（Bootstrap Protocol，自举协议）。交换机作为BOOTP客户端，可以从BOOTP服务器获得网络参数。但是，在自动获取之前，网管需要在BOOTP服务器上为每个客户端配置BOOTP参数，所以BOOTP一般运行在相对稳定的网络环境中，当网络规模较大、变化频繁时，建议选择DHCP获取方式。

本页面用来配置交换机的管理IP地址。

**进入页面的方法：系统管理>>系统配置>>管理IP**

IP配置	
MAC地址：	00-0A-EB-13-12-7C
获取方式：	<input checked="" type="radio"/> 静态IP <input type="radio"/> DHCP <input type="radio"/> BOOTP
管理VLAN：	<input type="text" value="1"/> (VLAN ID: 1-4094)
IP地址：	<input type="text" value="192.168.0.1"/>
子网掩码：	<input type="text" value="255.255.255.0"/>
默认网关：	<input type="text"/>

**注意：**

IP地址的变更可能导致当前网络连接的中断，请保持IP地址与内网IP地址在同一网段。

图 4-7 管理IP

条目介绍：

➤ **IP配置**

- MAC地址：** 显示交换机的物理地址。
- 获取方式：** 选择交换机网络参数的获取方式。
- 静态IP：手动填写交换机的IP地址、子网掩码和默认网关。
  - DHCP：从网络中的DHCP服务器获取交换机的网络参数。
  - BOOTP：从网络中的BOOTP服务器获取交换机的网络参数。
- 管理VLAN：** 配置交换机的管理VLAN。交换机只存在一个管理VLAN，只有通过它才可以管理交换机，默认的管理VLAN是VLAN1，您可以通过交换机的所有端口登录并管理交换机。但是，如创建了其他VLAN并更改了管理VLAN，则需重新连接设备到新的管理VLAN中的某个成员端口，才可访问交换机。
- IP地址：** 填写交换机的管理IP地址。该IP地址出厂默认值为192.168.0.1，您可以根据需要改变它。
- 子网掩码：** 填写本交换机的子网掩码。
- 默认网关：** 填写本交换机的默认网关。

**注意：**

- IP地址的变更可能导致当前网络连接的中断，请保持IP地址与内网IP地址在同一网段。
- 交换机只有一个IP地址。新配置的IP地址将覆盖原有的IP地址。
- 当交换机通过DHCP服务器请求IP参数时，交换机会一直向网络发出申请，直到成功，你可以在给交换机分配IP参数的DHCP服务器上了解到交换机的配置信息。
- 交换机出厂时，默认的IP地址是：192.168.0.1。

## 4.2 用户管理

用户管理用来限制登录交换机Web页面的用户的访问权限和身份，以保护交换机的有效配置。

本功能包括**用户列表**和**用户配置**两个配置页面。

## 4.2.1 用户列表

可以在本页查看到当前交换机存在的全部用户。

进入页面的方法：系统管理>>用户管理>>用户列表

用户列表			
序号	用户名	类型	状态
1	admin	管理员	启用

图 4-8 用户列表

## 4.2.2 用户配置

本页用来配置登录交换机Web页面的用户的身份类型。本交换机提供两种类型的用户：受限用户和管理员。受限用户，仅可以查看部分功能的配置数据，不能对交换机进行任何配置；管理员，可以配置交换机的全部功能。本说明书内如无特殊说明，均以“管理员”身份登录时的Web页面为准。

进入页面的方法：系统管理>>用户管理>>用户配置

用户信息

用户名：

用户类型：

用户状态： 启用  禁用

密码：

确认密码：

口令模式：

用户列表

选择	序号	用户名	类型	状态	操作
<input type="checkbox"/>	1	admin	管理员	启用	<a href="#">编辑</a>

### 注意：

用户名只允许1-16个字符，密码只允许1-31个字符，且只能包含数字、英文字母和下划线。

图 4-9 用户配置

条目介绍：

### > 用户信息

**用户名：** 填写登录Web页面的用户名。

- 用户类型:** 选择该用户名的用户类型。
- 管理员：可以编辑、修改和查看交换机各个功能的配置。
  - 受限用户：仅可以查看交换机各个功能的配置情况。
- 用户状态:** 选择是否启用该用户。
- 密码:** 填写该用户名的登录密码。
- 确认密码:** 再次输入该用户名的登录密码，两次输入的密码需保持一致。
- 口令模式:** 选择口令模式。
- 明文模式：在配置文件中以明文显示密码。
  - 密文模式：在配置文件中以密文显示密码。
- **用户列表**
- 选择:** 勾选条目进行删除，可多选。但是不可以对当前登录用户自身进行删除。
- 序号、用户名、类型、状态:** 显示当前用户的序号、用户名、用户类型和用户状态。
- 操作:** 点击对应条目的<编辑>按键，可以修改该条目的用户信息。修改完毕后点击<修改>按键，修改内容生效。但是不允许修改当前登录用户自身的用户类型和状态。



说明:

- TL-SG2452不支持口令模式。

## 4.3 系统工具

系统工具功能集中对交换机的配置文件进行管理，包括**配置导入**、**配置导出**、**软件升级**、**系统重启**和**软件复位**五个配置页面。

### 4.3.1 配置导入

配置导入功能是将以前备份的配置文件导入至交换机中，使交换机恢复到当时的配置状态。

进入页面的方法：**系统管理>>系统工具>>配置导入**

#### 配置文件导入

从用户备份的配置文件中恢复配置信息。

选择一个以前备份的配置文件，然后点击“导入配置文件”按钮，可以恢复到当时的配置状态。

配置文件：

#### 注意：

- 1、恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 4-10 配置导入

条目介绍:

➤ 配置文件导入

**导入配置文件:** 将备份文件中保存的配置信息恢复到当前状态，交换机自动重启后配置生效。



**注意:**

- 恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。
- 导入配置文件的过程不能关闭交换机电源，否则将导致交换机损坏而无法使用。
- 导入配置文件后，交换机中原有的配置信息将会丢失。如果您导入的配置文件有误，可能会导致交换机无法被管理。

### 4.3.2 配置导出

配置导出功能是将交换机当前的配置信息打包成文件保存到PC中，方便您日后通过该文件恢复配置。

进入页面的方法：系统管理>>系统工具>>配置导出

#### 配置文件备份

备份系统配置信息

点击“备份配置文件”按钮，可以把所有配置信息打包成一个文件，备份到您的电脑上。

备份配置文件

帮助

**注意:**

备份当前配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 4-11 配置导出

条目介绍:

➤ 配置文件备份

**备份配置文件:** 以文件形式保存您的设置。建议升级前进行备份。



**注意:**

- 备份当前配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

### 4.3.3 软件升级

本交换机可以通过Web方式升级系统文件，系统升级后将获得更完善的功能，请在<http://www.tp-link.com.cn>网站上下载最新版本的系统文件。

进入页面的方法：系统管理>>系统工具>>软件升级

## 升级系统文件

通过升级交换机的软件，您将获得新的功能。

升级文件：

浏览...

升级

当前软件版本：1.0.0 Build 20130104 Rel.37783

帮助

当前硬件版本：TL-SL2428 1.0

**注意：**

1. 升级时请选择与当前硬件版本一致的软件。
2. 升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。
3. 当升级结束后，设备将会自动重新启动。
4. 建议升级前备份您的配置信息。

图 4-12 软件升级

**注意：**

- 升级过程中不能被中断。
- 升级时请选择与当前硬件版本一致的软件。
- 升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。
- 建议升级前备份您的配置信息。

### 4.3.4 系统重启

在此处可以重新启动交换机，交换机重启后自动返回到登录页面。重启前请先保存当前配置，否则重启后，未保存的配置信息将丢失。

进入页面的方法：系统管理>>系统工具>>系统重启

## 系统重启

重启前保存配置：

重启交换机：

重启

**注意：**

在设备重启期间，请不要关闭设备电源，以免损坏设备。

图 4-13 系统重启

**注意：**

- 在设备重启期间，请不要关闭设备电源，以免损坏设备。

### 4.3.5 软件复位

通过软件复位，可以将交换机恢复为出厂设置状态，所有配置数据将被清除。

进入页面的方法：系统管理>>系统工具>>软件复位

## 软件复位

软件复位：

**注意：**

软件复位后，交换机配置将恢复成出厂默认状态，用户配置数据将丢失。

图 4-14 软件复位

**注意：**

- 软件复位后，交换机配置将恢复成出厂默认状态，您配置的数据将丢失。

## 4.4 安全管理

安全管理功能是针对不同的远程登录方式，采取相应的安全措施，以增强用户管理交换机的安全性。包括安全配置、SSL配置、SSH配置三个配置页面。

### 4.4.1 安全配置

本页用来限制登录交换机Web页面的用户的身份及人数，从而增强了交换机配置管理的安全性。其中，管理员及受限用户的定义请参考[4.2用户管理](#)。

进入页面的方法：系统管理>>安全管理>>安全配置

## 身份限制

限制类型：

禁用 

IP地址：

掩码：

MAC地址：

端口号：

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7	<input type="checkbox"/> 8
<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16
<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28				

## 超时配置

超时时间：

 分钟（5-30）

## 管理人数限制

人数限制功能：

 启用  禁用

管理员人数：

 名（1-16）

受限用户人数：

 名（0-15）

图 4-15 安全配置



条目介绍:

➤ 身份限制

- 限制类型:** 选择限制用户身份的类型。
- 基于IP: 用来限制访问交换机Web页面的用户的IP网段。
  - 基于MAC: 用来限制访问交换机Web页面的用户的主机MAC地址。
  - 基于端口: 用来限制访问交换机Web页面的交换机端口号。
- IP地址、掩码:** 选择“基于IP”时才能进行配置。只允许指定IP网段的用户才可以通过Web页面访问交换机。
- MAC地址:** 选择“基于MAC”时才能进行配置。只允许指定MAC地址的用户才可以通过Web页面访问交换机。
- 端口号:** 选择“基于端口”时才能进行配置。只允许指定端口上的用户才可以通过Web页面访问交换机。

➤ 超时配置

- 超时时间:** 如果在超时时间之内没有对交换机管理页面进行操作, 系统会自动退出管理页面, 若要再次进行管理请重新登录。默认为10分钟。

➤ 管理人数限制

- 人数限制功能:** 选择是否启用人数限制功能。
- 管理员人数:** 填写可同时登录交换机Web页面的管理员总数。
- 受限用户人数:** 填写可同时登录交换机Web页面的受限用户总数。

## 4.4.2 SSL配置

SSL (Secure Sockets Layer, 安全套接层) 是一个安全协议, 它为基于TCP的应用层协议提供安全连接, 如为普通的HTTP连接提供更安全的HTTPS连接。SSL协议广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输, 多使用在电子商务、网上银行等领域, 为网络上数据通讯提供安全性保证。

SSL协议提供的服务主要有:

1. 对用户和服务器进行基于证书的身份认证, 确保数据发送到正确的用户和服务器;
2. 对传输数据进行加密, 以防止数据中途被窃取;
3. 维护数据的完整性, 确保数据在传输过程中不被改变。

SSL采用非对称加密技术, 使用“密钥对”进行数据的加密/解密, “密钥对”由一个公钥(包含在证书中)和一个私钥构成。初始时交换机里已有默认的证书(自签名)和对应私钥, 也可以通过证书/密钥导入功能替换默认的密钥对, 但SSL证书/密钥必须配对导入, 否则HTTPS不能正常连接。

本功能生效后，即可通过<https://192.168.0.1>登录交换机的Web页面。初次使用交换机默认的证书通过HTTPS登陆交换机时，浏览器可能会提示“该证书是自签名的而不被信任”或“证书错误”，此时请将此证书添加为信任证书，或者继续浏览此网站即可。

进入页面的方法：**系统管理>>安全管理>>SSL配置**

**全局配置**

SSL功能： 启用  禁用

提交 帮助

**证书导入**

SSL证书： 浏览... 导入证书

**密钥导入**

SSL密钥： 浏览... 导入密钥

**注意：**

- 1、SSL证书/密钥导入后，需要重启交换机才能生效。
- 2、SSL证书/密钥必须配对导入，否则HTTPS不能正常连接。

图 4-16 SSL证书管理

条目介绍：

➤ **SSL证书管理**

**SSL功能：** 选择是否启用交换机的SSL功能。

➤ **证书导入**

**SSL证书：** 选择要导入的SSL证书。证书必须为BASE64编码格式。

➤ **密钥导入**

**SSL密钥：** 选择要导入的SSL密钥。密钥必须为BASE64编码格式。



**注意：**

- SSL证书/密钥必须配对导入，否则HTTPS不能正常连接。
- SSL证书/密钥导入后，需要重启交换机才能生效。
- 要使用HTTPS建立安全连接，必须在浏览器的地址栏指定“https://提示符”。
- HTTPS连接涉及身份认证、加密、解密等过程，故响应速度可能会比普通的HTTP连接稍慢。

### 4.4.3 SSH配置

SSH（Secure Shell，安全外壳）是由IETF（Internet Engineering Task Force，因特网工程任务组）所制定，建立在应用层和传输层基础上的安全协议。SSH加密连接所提供的功能类似于一个telnet连接，但是传统的telnet远程管理方式在本质上是不安全的，因为它在网络上使用明文传送口令和

数据的，别有用心的可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境远程登录到设备时，SSH功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

SSH是由服务器端和客户端组成的，并且有V1和V2两个不兼容的版本。在通讯过程中，SSH服务器与客户端会自动互相协商SSH版本号和加密算法，协商一致后，由客户端向服务器端发起请求登录的认证请求，认证通过后双方即可进行信息的交互。本交换机支持SSH服务器功能，可以使用SSH客户端软件通过SSH连接方式登录交换机。

SSH密钥导入是将SSH的公钥文件导入至交换机中。如果密钥导入成功，交换机会优先选用密钥认证的方式接受SSH登入。

进入页面的方法：系统管理>>安全管理>>SSH配置

**全局配置**

SSH功能： 启用  禁用

Protocol V1： 启用  禁用

Protocol V2： 启用  禁用

静默时长： 秒（1-120）

最大连接数： （1-5）

**密钥导入**

选择你要导入交换机的密钥。

密钥类型：

密钥文件：

**注意：**

1、导入密钥可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 4-17 SSH配置

条目介绍：

➤ 全局配置

- SSH功能：** 选择是否启用SSH功能。
- Protocol V1：** 选择是否启用对SSH V1的支持。
- Protocol V2：** 选择是否启用对SSH V2的支持。
- 静默时长：** 填写静默时长。该时间内客户端无任何操作时，连接会自动断开。默认为120秒。
- 最大连接数：** 填写SSH同时可允许的最大连接数，连接数若满，将无法再建立新的连接。默认为5。

➤ 密钥导入

**密钥类型:** 选择所要导入的密钥类型。本机支持SSH-1 RSA, SSH-2 RSA和SSH-2 DSA三种类型的密钥。

**密钥文件:** 选择要导入的密钥文件。

**导入密钥:** 点击此按钮, 将所选的SSH密钥导入交换机。



**注意:**

- 请确保导入的文件是密钥长度为256至3072比特的SSH公钥。
- 导入密钥文件后, 交换机中此用户原有的同类型密钥将会被覆盖。如果您导入的密钥文件有误, SSH会转用密码认证的方式登陆。

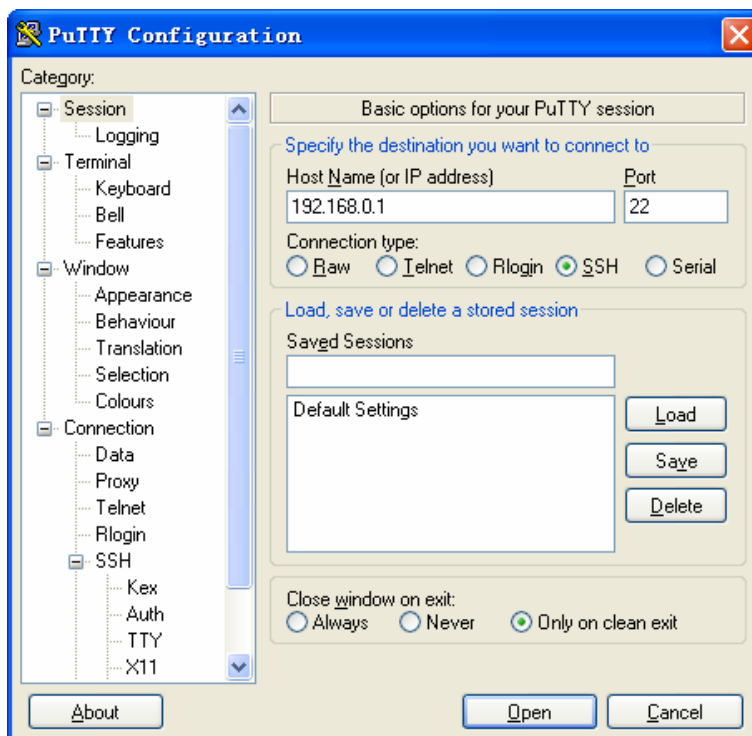
组网应用1:

➤ 组网需求

1. 使用SSH功能的“密码认证”的方式登录交换机, 交换机已启用SSH功能。
2. 推荐使用第三方客户端软件PuTTY。

➤ 配置步骤

1. 打开软件, 登录PuTTY的主界面。在“Host Name”处填写交换机的IP地址; “Port”保持默认的22; “Connection type”处选择SSH的接入方式。如下图所示。



2. 点击<Open>按键，即可登录到交换机。操作方法与telnet相同，输入登录用户名和登录密码，即可继续进行配置操作。如下图所示。



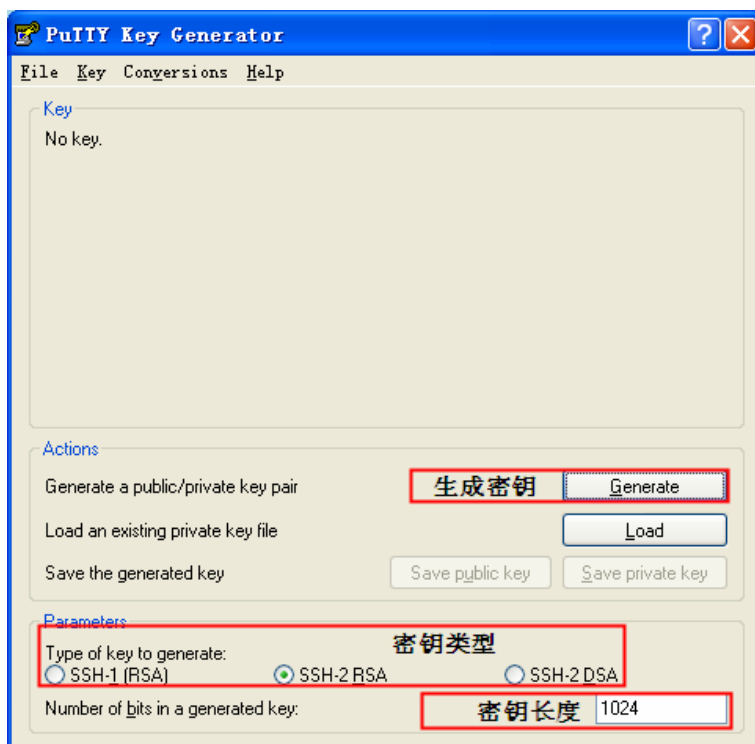
## 组网应用2:

### > 组网需求

1. 使用SSH功能的“密钥认证”的方式登录交换机，交换机已启用SSH功能。
2. 推荐使用第三方客户端软件PuTTY。

### > 配置步骤

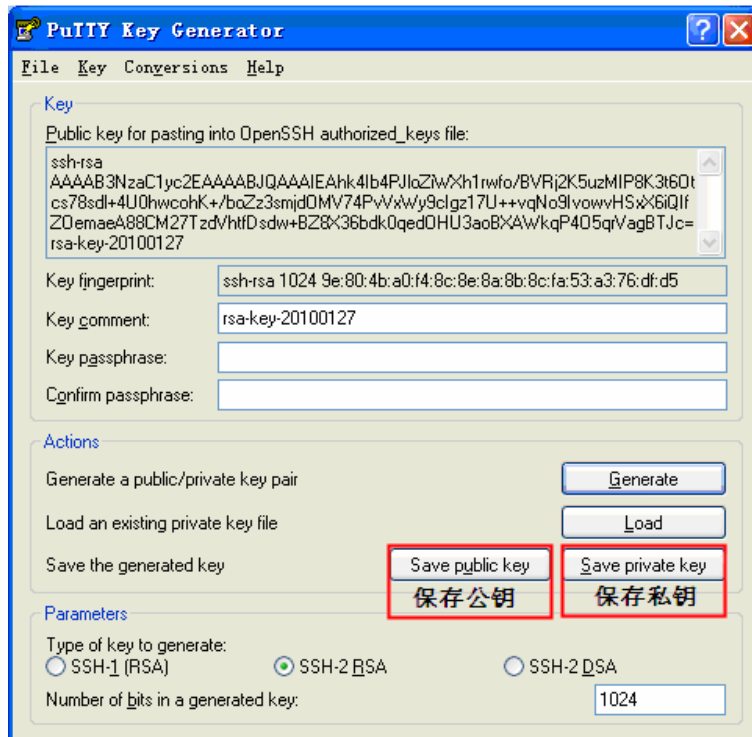
1. 选择密钥类型和密钥长度，并生成SSH密钥。如下图所示。



### 注意:

- 密钥长度的范围为256至3072比特。
- 生成密钥的过程中，在软件的空白处快速的随意晃动鼠标，产生随机数据，可以加快密钥生成的速度。

2. 密钥生成后，将公钥和私钥文件保存在主机上。如下图所示。



3. 在交换机配置页面上，将保存至主机上的公钥文件导入交换机中。

#### 密钥导入

选择你要导入交换机的密钥。

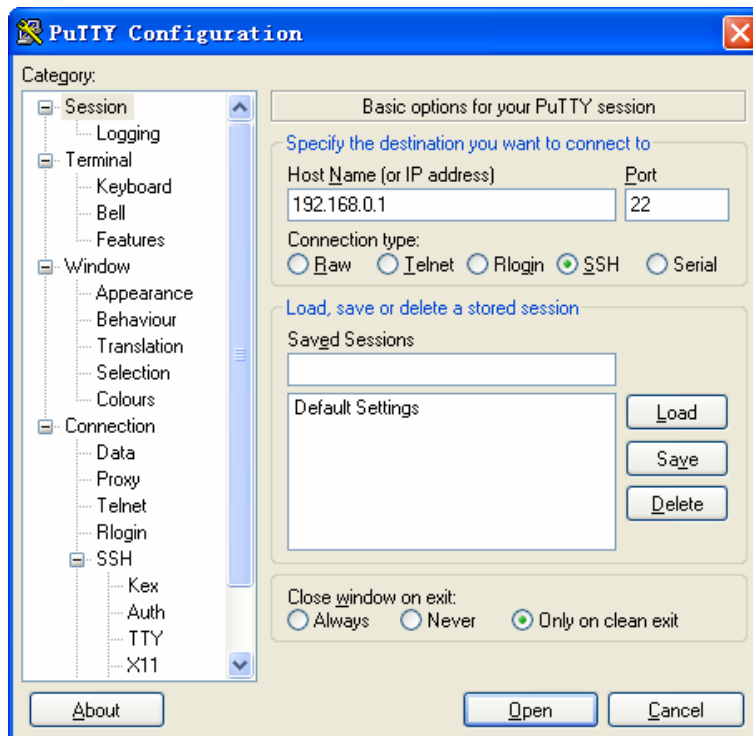
密钥类型：

密钥文件：

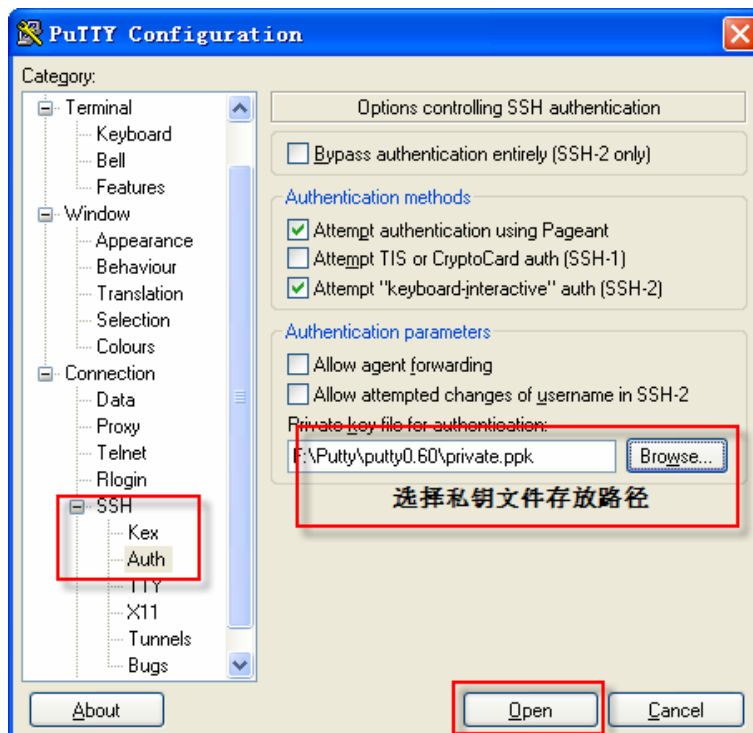
#### 注意：

- 密钥类型要与密钥文件的类型保持一致。
- 载入SSH密钥的过程不能被中断。

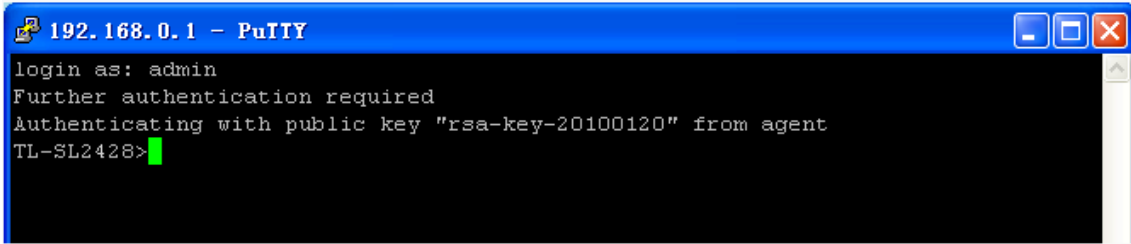
4. 打开PuTTY的主界面，输入IP地址并选择连接类型为SSH，如下图所示。



5. 点击左边的目录栏进入SSH目录下的Auth菜单，将私钥文件导入至SSH客户端软件中，再点击<open>按钮与服务器建立连接并进行协商。如下图所示。



- 协商成功后，输入用户名进行登录，如果你不需要输入密码即可登陆成功，表明密钥认证已经成功。如下图所示。



```
192.168.0.1 - PuTTY
login as: admin
Further authentication required
Authenticating with public key "rsa-key-20100120" from agent
TL-SL2428>
```

[回目录](#)



## 第5章 二层交换

二层交换模块主要用于配置交换机的基本功能，包括端口管理、汇聚管理、流量统计、地址表管理以及DHCP过滤五个部分。

### 5.1 端口管理

端口管理用于配置交换机端口的基本属性，包括端口配置、端口监控、端口安全、端口隔离和环路监测五个功能配置页面。

#### 5.1.1 端口配置

端口配置用来配置交换机端口的各项基本参数。端口状态选择“禁用”时，交换机将丢弃来自这个端口的数据包。当交换机端口长时间不使用时，可以将该端口设为禁用，可有效减小交换机的功耗，待使用时再将该端口设为启用。

端口基本参数将会直接影响端口的工作方式，请结合实际情况进行配置。

进入页面的方法：二层交换>>端口管理>>端口配置

选择	端口	描述	状态	速率双工	流控	LAG
<input type="checkbox"/>		<input type="text"/>	禁用	10M半双工	禁用	
<input type="checkbox"/>	1		启用	Auto	禁用	--
<input type="checkbox"/>	2		启用	Auto	禁用	--
<input type="checkbox"/>	3		启用	Auto	禁用	--
<input type="checkbox"/>	4		启用	Auto	禁用	--
<input type="checkbox"/>	5		启用	Auto	禁用	--
<input type="checkbox"/>	6		启用	Auto	禁用	--
<input type="checkbox"/>	7		启用	Auto	禁用	--
<input type="checkbox"/>	8		启用	Auto	禁用	--
<input type="checkbox"/>	9		启用	Auto	禁用	--
<input type="checkbox"/>	10		启用	Auto	禁用	--
<input type="checkbox"/>	11		启用	Auto	禁用	--
<input type="checkbox"/>	12		启用	Auto	禁用	--
<input type="checkbox"/>	13		启用	Auto	禁用	--
<input type="checkbox"/>	14		启用	Auto	禁用	--
<input type="checkbox"/>	15		启用	Auto	禁用	--

**注意：**

端口描述1-16个字符。

图 5-1 端口配置

条目介绍：

➤ 端口配置

**端口选择：**

点击<选择>按键，可根据所输端口号，快速选择相应端口。

**选择：**

勾选端口配置端口参数，可多选。

- 端口：**显示交换机的端口号。
- 描述：**填写端口的描述信息，便于您区分各个端口的用途。
- 状态：**选择端口状态。只有状态为启用时，端口才能正常转发数据包。
- 速率双工：**选择端口的传输速率及传输模式。与交换机相连的设备必须与交换机的传输速率及双工状态保持一致。当选择“Auto”选项时，该端口的速率双工由自动协商决定。默认为Auto。对于SFP端口，本交换机暂不提供自动协商。
- 流控：**选择端口的流控状态。启用流控能够同步接收端和发送端的速度，防止因速率不一致导致的网络丢包。
- LAG：**显示端口当前所属的汇聚组。

**注意：**

- 端口状态配置为禁用则不能通过该端口管理交换机，请将要进行管理的端口配置为启用状态。
- 从属于同一个汇聚组的所有成员端口的相应参数配置应该保持一致。
- 对于TL-SL2428，若需要使用SFP端口，插入光纤模块后，请手动配置SFP端口的端口参数（出厂默认设置的速率双工模式为1000Mbps全双工）。如果使用的是百兆光纤模块，相应SFP口的速率双工模式请配置为100Mbps全双工；如果使用的是千兆光纤模块，相应SFP口的速率双工模式请配置为1000Mbps全双工。
- TL-SL2452/TL-SG2452的SFP端口只支持千兆光纤模块。

## 5.1.2 端口监控

端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个或几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

进入页面的方法：二层交换>>端口管理>>端口监控

监控组列表				
监控组	监控端口	监控方式	被监控端口	操作
1	0	入口监控	--	<a href="#">编辑</a>
		出口监控	--	
2	0	入口监控	--	<a href="#">编辑</a>
		出口监控	--	
3	0	入口监控	--	<a href="#">编辑</a>
		出口监控	--	
4	0	入口监控	--	<a href="#">编辑</a>
		出口监控	--	

[帮助](#)

图 5-2 端口监控

条目介绍:

➤ 监控组列表

- 监控组:** 显示监控组的组号。
- 监控端口:** 显示每个监控组的唯一的一个监控端口号。
- 监控方式:** 显示每个监控组的监控方式。分为入口监控和出口监控。
- 被监控端口:** 显示每个监控组的所有被监控端口。
- 操作:** 点击<编辑>按键, 对每个监控组的配置进行修改。

点击<编辑>按键, 显示界面如下图所示:

**监控组选择**

选择组号:

**监控端口配置**

监控端口:

**被监控端口**

端口

选择	端口	入口监控	出口监控	LAG
<input type="checkbox"/>		<input type="text" value="禁用"/>	<input type="text" value="禁用"/>	
<input type="checkbox"/>	1	禁用	禁用	--
<input type="checkbox"/>	2	禁用	禁用	--
<input type="checkbox"/>	3	禁用	禁用	--
<input type="checkbox"/>	4	禁用	禁用	--
<input type="checkbox"/>	5	禁用	禁用	--
<input type="checkbox"/>	6	禁用	禁用	--
<input type="checkbox"/>	7	禁用	禁用	--
<input type="checkbox"/>	8	禁用	禁用	--
<input type="checkbox"/>	9	禁用	禁用	--
<input type="checkbox"/>	10	禁用	禁用	--
<input type="checkbox"/>	11	禁用	禁用	--
<input type="checkbox"/>	12	禁用	禁用	--

图 5-3 编辑监控组

条目介绍:

➤ 监控组选择

- 选择组号:** 选择需要进行配置的监控组组号。

### ➤ 监控端口配置

**监控端口：** 在此处选择该监控组的监控端口。

### ➤ 被监控端口

**端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。

**选择：** 勾选端口配置为被监控端口，可多选。

**端口：** 显示交换机的端口号。

**入口监控：** 对被监控端口收到的数据进行监控，复制到监控端口。

**出口监控：** 对被监控端口发出的数据进行监控，复制到监控端口。

**LAG：** 显示端口当前所属的汇聚组。汇聚组成员端口不能选为监控端口和被监控端口。



#### 注意：

- 汇聚组的成员端口既不能作为监控端口，也不能作为被监控端口。
- 一个端口不可以既作为监控端口又作为被监控端口。
- 端口监控功能可以跨越VLAN进行监控。

## 5.1.3 端口安全

交换机地址表维护着端口和接入端的MAC地址的对应关系，并以此建立交换路径，地址表的大小是固定的。地址表攻击是指利用工具产生欺骗MAC，快速填满地址表，交换机地址表被填满后，交换机将以广播方式处理通过交换机的报文，这时攻击者可以利用各种嗅探，攻击获取网络信息。地址表满了后，数据流以洪泛的方式发送到所有端口，会造成交换机负载过大，网络缓慢和丢包甚至瘫痪。

端口安全通过限制端口的最大学习MAC数目，来防范MAC地址攻击并控制端口的网络流量。如果端口启用端口安全功能，将动态学习接入的MAC地址，当学习地址数达到最大值时停止学习。此后，MAC地址未被学习的网络设备将不能再通过该端口接入网络，以保证安全性。

进入页面的方法：二层交换>>端口管理>>端口安全

端口安全					
选择	端口	最大学习地址数	已学习地址数	学习模式	状态
<input type="checkbox"/>		<input type="text"/>		动态 <input type="button" value="v"/>	禁用 <input type="button" value="v"/>
<input type="checkbox"/>	1	64	0	动态	禁用
<input type="checkbox"/>	2	64	0	动态	禁用
<input type="checkbox"/>	3	64	0	动态	禁用
<input type="checkbox"/>	4	64	0	动态	禁用
<input type="checkbox"/>	5	64	0	动态	禁用
<input type="checkbox"/>	6	64	0	动态	禁用
<input type="checkbox"/>	7	64	0	动态	禁用
<input type="checkbox"/>	8	64	0	动态	禁用
<input type="checkbox"/>	9	64	0	动态	禁用
<input type="checkbox"/>	10	64	0	动态	禁用
<input type="checkbox"/>	11	64	0	动态	禁用
<input type="checkbox"/>	12	64	0	动态	禁用

**注意：**

最大学习地址数的范围为0-64。

图 5-4 端口安全

条目介绍：

► 端口安全

- 选择：** 勾选端口配置端口安全，可多选。
- 端口：** 显示交换机的端口号。
- 最大学习地址数：** 填写对应端口最多可以学习的MAC地址数目。默认为64。
- 已学习地址数：** 显示对应端口已经学习的MAC地址数目。
- 学习模式：** 选择MAC地址学习的模式。
- 动态：MAC地址学习受老化时间的限制，老化时间过后，所学的MAC地址将被删除。
  - 静态：MAC地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目清空。
  - 永久：MAC地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目保持不变。
- 状态：** 选择是否启用端口安全功能。

**注意：**

- 当端口为汇聚组成员，该端口的端口安全功能被禁用。只有将端口从汇聚组中去掉，才可以使端口使用端口的端口安全功能。

## 5.1.4 端口隔离

通过端口隔离功能，可以为交换机的任意物理端口指定转发端口。设置了端口隔离功能后，每个物理端口只能向自己的转发端口转发数据包。

进入页面的方法：二层交换>>端口管理>>端口隔离

端口隔离配置

端口:  ▼

转发端口:

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12
<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18
<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28		

端口隔离列表

端口	转发端口
1	1-28
2	1-28
3	1-28
4	1-28
5	1-28
6	1-28
7	1-28
8	1-28
9	1-28
10	1-28
11	1-28
12	1-28
13	1-28
14	1-28
15	1-28

图 5-5 端口隔离

条目介绍：

➤ 端口隔离配置

**端口：** 选择一个物理端口，以配置其转发端口。

**转发端口：** 选择报文可以被转发到的端口。

➤ 端口隔离列表

**端口：** 显示交换机的端口号。

**转发端口：** 显示可转发的端口列表。

## 5.1.5 环路监测

环路监测（Loopback Detection）通过环路监测数据包检测交换机连接的网络中是否存在环路，当检测出环路时根据用户设定处理相应的端口。

进入页面的方法：二层交换>>端口管理>>环路监测

全局配置

环路监测功能：  启用  禁用

环路监测间隔：  秒（1-1000）

自动恢复时间：  倍监测间隔（1-100）

页面自动刷新：  启用  禁用

自动刷新间隔：  秒（3-100）

端口配置

端口

选择	端口	状态	处理模式	恢复模式	环路状态	阻塞状态	LAG
<input type="checkbox"/>		禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	1	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	2	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	3	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	4	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	5	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	6	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	7	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	8	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	9	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	10	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	11	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	12	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	13	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	14	禁用	Alert	Auto	---	---	---
<input type="checkbox"/>	15	禁用	Alert	Auto	---	---	---

### 注意：

恢复模式设定只对处于非Alert处理模式的端口有效。

环路监测务必与风暴抑制配合使用。

图 5-6 环路监测

条目介绍：

#### ➤ 全局配置

- 环路监测功能：** 选择是否启用交换机的环路监测功能。
- 环路监测间隔：** 设置环路监测的时间间隔，默认值为30。
- 自动恢复时间：** 设置被阻塞环路端口的自动恢复时间，设置值为环路监测间隔的整数倍，默认为3。
- 页面自动刷新：** 选择是否启用页面的自动刷新。

- 自动刷新间隔：** 设置页面自动刷新的时间间隔，默认值为3。
- **端口配置**
- 端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：** 勾选端口配置端口参数，可多选。
- 端口：** 显示交换机的端口号。
- 状态：** 选择是否启用此功能。
- 处理模式：** 选择端口发现环路时的处理模式：
- **Alert：** 端口上发现环路时只发出报警信息。
  - **Port based：** 端口上发现环路时发出报警信息，同时阻塞端口。
- 恢复模式：** 选择端口被阻塞后的恢复模式：
- **Auto：** 端口被阻塞后经过自动恢复时间后会自动解除阻塞。
  - **Manual：** 端口被阻塞后只能手动解除阻塞状态。
- 环路状态：** 端口上是否监测到外部环路。
- 阻塞状态：** 端口是否因为监测到环路而处于阻塞状态。
- LAG：** 显示端口当前所属的汇聚组。
- 手动恢复：** 重置选定端口状态，解除阻塞。

**注意：**

- 恢复模式设定只对处于非Alert处理模式的端口有效。
- 环路监测务必与风暴抑制配合使用。

## 5.2 汇聚管理

LAG（Link Aggregation Group，端口汇聚组）是将交换机的多个物理端口汇聚在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。端口汇聚可以实现流量在汇聚组中各个成员端口之间进行分担，以增加带宽。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。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括STP、QoS、GVRP、VLAN、端口属性、MAC地址学习等。具体说明如下：

- 开启**GVRP、802.1Q VLAN、语音VLAN、生成树、QoS配置、DHCP侦听及端口配置**（速率、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。
- 开启**端口安全、端口监控、MAC地址过滤、静态MAC地址绑定、半双工及802.1X认证**功能的端口，不能加入汇聚组。
- 开启**ARP防护、DoS防护**功能的端口，建议不要将其加入汇聚组。

如果您需要配置汇聚组，建议您在本功能处优先配置汇聚组后，再去其它功能处配置汇聚组的其它功能。



**说明:**

- LAG带宽的计算: 当使用四个全双工1000Mbps端口构成LAG时, 由于每一个端口上行和下行各是1000Mbps, 所以每一个端口的带宽为2000Mbps。它们使用LAG技术汇聚在一起可以形成的最大带宽为8000Mbps。
- LAG的流量会根据选路算法均衡分配到各个成员端口中。当LAG中的一个或几个端口连接断开的时候, 这些端口的流量会转移到LAG中其它链接正常的端口中, 具备链路冗余备份功能。

按照汇聚方式的不同, 端口汇聚可以分为两类: 手动配置和LACP配置。本功能包括**汇聚列表**、**手动配置**和**LACP配置**三个配置页面。

## 5.2.1 汇聚列表

在本页, 您可以查看到交换机当前的全部汇聚组。

进入页面的方法: 二层交换>>汇聚管理>>汇聚列表

全局配置

选路算法:

汇聚列表

选择	组号	描述	成员	操作
<input type="checkbox"/>	LAG1	Static LAG	17, 18, 19, 20	<a href="#">编辑</a>   <a href="#">查看</a>

图 5-7 汇聚列表

条目介绍:

➤ 全局配置

**选路算法:**

根据选路算法规则, 选择转发数据的端口。

- 源目的MAC地址: 仅使用数据包中的源目的MAC地址信息。
- 源目的IP地址: 仅使用数据包中的源目的IP地址信息。

➤ 汇聚列表

**选择:**

勾选汇聚组进行删除, 可多选。

**组号:**

显示汇聚组的序号。

**描述:**

显示汇聚组的描述信息。

**成员:**

显示属于汇聚组的物理端口。

**操作:**

对单个汇聚组进行相应配置。

- 编辑: 修改汇聚组的描述和成员端口。
- 查看: 查看汇聚组的端口状态信息。

点击<查看>按键，您可以看到所选汇聚组的详细信息。

详细信息	
组号：	LAG1
汇聚类型：	手动设置
端口状态：	启用
速率双工：	Auto
端口流控：	禁用
入口带宽(bps)：	--
出口带宽(bps)：	--
广播包抑制(bps)：	--
多播包抑制(bps)：	--
UL包抑制(bps)：	--
QoS优先级：	CoS 0
加入的VLAN：	1

图 5-8 汇聚组状态

## 5.2.2 手动配置

您可以在本页对汇聚组进行手动配置，手动配置的汇聚端口的LACP状态为禁用。

进入页面的方法：二层交换>>汇聚管理>>手动配置

汇聚组配置					
选择组号：	<input type="text" value="LAG1"/>				
该组描述：	<input type="text" value="Static LAG"/>				
成员端口					
<input checked="" type="checkbox"/> 1 (LAG1)	<input checked="" type="checkbox"/> 2 (LAG1)	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12
<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18
<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28		
<input type="button" value="提交"/>		<input type="button" value="清空"/>		<input type="button" value="帮助"/>	

### 注意：

- 1、LAG\*表示该端口当前所属的汇聚组(Link Aggregation Group)。
- 2、不推荐一个汇聚组内同时有100M端口和1000M端口。
- 3、LACP动态创建的汇聚组不能被编辑。

图 5-9 手动配置

条目介绍:

➤ 全局配置

**选择组号:** 选择汇聚组的序号，组号格式为LAG\*。

**该组描述:** 显示汇聚组的描述信息。

➤ 成员端口

**成员端口:** 勾选属于汇聚组的物理端口，清空表示删除该汇聚组。



**说明:**

- 要删除一个已配置的LAG，将该LAG的成员清空并提交即可。
- 一个端口仅可以处于一个汇聚组中。即若端口已成为其它LAG的成员端口，或者已汇聚成为LACP中的成员时，该端口处于灰化状态，不能勾选。

### 5.2.3 LACP配置

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是基于 IEEE802.3ad 标准用来实现链路动态汇聚与解汇聚的协议。汇聚的双方通过协议交互汇聚信息，将匹配的链路汇聚在一起收发数据，汇聚组内端口的添加和删除是协议自动完成的，具有很高的灵活性并提供了负载均衡的能力。

启用端口的LACP功能后，该端口向对端通告本端的系统优先级、系统MAC、端口优先级、端口号和操作Key（由端口的物理属性、上层协议信息和管理Key决定）。设备优先级高的一端将主导汇聚及解汇聚，设备优先级由系统优先级和系统MAC决定，系统优先级值小的设备优先级高，系统优先级值相同时系统MAC较小的设备优先级高。设备优先级高的一端将根据端口优先级、端口号以及操作Key选择汇聚端口，操作Key相同的端口才能被选入同一个汇聚组，同一个汇聚组内端口优先级值小的端口会被优先选择，当端口优先级相同的时候，端口号小的会被优先选择。双方交互汇聚信息后被选择的端口将汇聚在一起收发数据。

您可以在本页配置交换机的LACP功能。

**进入页面的方法：** 二层交换>>汇聚管理>>LACP配置

**全局配置**

系统优先级:  (0 - 65535)

---

**LACP 配置**

端口

选择	端口	管理Key	端口优先级 (0-65535)	模式	状态	LAG
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	被动 <input type="button" value="v"/>	禁用 <input type="button" value="v"/>	
<input type="checkbox"/>	1	1	32768	被动	禁用	LAG1
<input type="checkbox"/>	2	1	32768	被动	禁用	LAG1
<input type="checkbox"/>	3	1	32768	被动	禁用	---
<input type="checkbox"/>	4	1	32768	被动	禁用	---
<input type="checkbox"/>	5	1	32768	被动	禁用	---
<input type="checkbox"/>	6	1	32768	被动	禁用	---
<input type="checkbox"/>	7	1	32768	被动	禁用	---
<input type="checkbox"/>	8	1	32768	被动	禁用	---
<input type="checkbox"/>	9	1	32768	被动	禁用	---
<input type="checkbox"/>	10	1	32768	被动	禁用	---
<input type="checkbox"/>	11	1	32768	被动	禁用	---
<input type="checkbox"/>	12	1	32768	被动	禁用	---
<input type="checkbox"/>	13	1	32768	被动	禁用	---
<input type="checkbox"/>	14	1	32768	被动	禁用	---
<input type="checkbox"/>	15	1	32768	被动	禁用	---

**注意:**

- 1、为防止LACP功能使用过程中产生广播风暴，建议启用生成树功能。
- 2、已经属于静态LAG组的成员端口无法启用LACP功能。
- 3、管理Key的值不能与已启用静态LAG组的组号相同，反之亦然。

图 5-10 LACP配置

## 条目介绍:

## ➤ 全局配置

**系统优先级:**

与系统的MAC地址一起决定设备优先级，设备优先级高的一端将主导汇聚及解汇聚。默认为32768。

## ➤ LACP配置

**端口选择:**

点击<选择>按键，可根据所输端口号，快速选择相应端口。

**选择:**

勾选端口配置端口LACP功能，可多选。

**端口:**

显示交换机的端口号。

**管理Key:**

处于同一汇聚组的成员，需配置相同的管理Key。

**端口优先级:**

决定了成为汇聚组成员的端口的优先级。端口优先级值小的端口会被优先选择。若端口优先级相同，则端口号小的会被优先选择。默认为32768。

**模式:**

选择相应端口的LACP模式。

**状态:**

选择相应端口是否启用LACP功能。

**LAG:** 显示端口当前所属的汇聚组。

## 5.3 流量统计

流量统计用于统计流经各个端口的数据信息，本功能包括**流量概览**和**详细统计**两个配置页面。

### 5.3.1 流量概览

流量概览用来显示交换机各端口的流量信息，便于您监控网络流量和分析网络异常。

进入页面的方法：二层交换>>流量统计>>流量概览

自动刷新

自动刷新： 启用  禁用

刷新周期： 秒（3-300）

流量概览

端口

端口	接收数据包数	发送数据包数	接收字节数	发送字节数	信息查询
1	0	0	0	0	<a href="#">详细信息</a>
2	0	0	0	0	<a href="#">详细信息</a>
3	0	0	0	0	<a href="#">详细信息</a>
4	0	0	0	0	<a href="#">详细信息</a>
5	0	0	0	0	<a href="#">详细信息</a>
6	0	0	0	0	<a href="#">详细信息</a>
7	0	0	0	0	<a href="#">详细信息</a>
8	0	0	0	0	<a href="#">详细信息</a>
9	0	0	0	0	<a href="#">详细信息</a>
10	0	0	0	0	<a href="#">详细信息</a>
11	0	0	0	0	<a href="#">详细信息</a>
12	0	0	0	0	<a href="#">详细信息</a>

图 5-11 流量概览

条目介绍：

➤ **自动刷新**

**自动刷新:** 选择是否启用自动刷新功能。

**刷新周期:** 填写自动刷新的时间周期。默认为30秒。

➤ **流量概览**

**端口选择:** 点击<选择>按键，可根据所输端口号，快速查找端口条目。

**端口:** 显示交换机的端口号。

- 接收数据包数：**统计交换机各端口接收的数据包数，不包括错误的数据包。
- 发送数据包数：**统计交换机各端口发送的数据包数。
- 接收字节数：**统计交换机各端口接收的字节数，包括错误的数据包的字节数。
- 发送字节数：**统计交换机各端口发送的字节数。
- 信息查询：**点击查询相应端口的详细统计信息。

### 5.3.2 详细统计

详细统计用来统计各端口传输数据包的详细信息，便于您定位网络问题。

进入页面的方法：二层交换>>流量统计>>详细统计

自动刷新

自动刷新： 启用  禁用

刷新周期： 秒（3-300）

---

详细统计

端口

接收信息统计		发送信息统计	
广播包	0	广播包	0
多播包	0	多播包	0
单播包	0	单播包	0
Alignment错误包	0	冲突包	0
小于64字节包	0		
64字节包	0		
65-127字节包	0		
128-255字节包	0		
256-511字节包	0		
512-1023字节包	0		
大于1023字节包	0		

图 5-12 详细统计

条目介绍：

➤ 自动刷新

**自动刷新：**选择是否启用自动刷新功能。

**刷新周期：**填写自动刷新的时间周期。

➤ 详细统计

**端口：**输入您所要查看流量信息的交换机端口号。

<b>接收信息统计:</b>	统计该端口接收数据包的详细信息。
<b>发送信息统计:</b>	统计该端口发送数据包的详细信息。
<b>广播包:</b>	端口接收/发送的含有效广播地址的数据包数目（不含错误帧）。
<b>多播包:</b>	端口接收/发送的含有效多播地址的数据包数目（不含错误帧）。
<b>单播包:</b>	端口接收/发送的含有效单播地址的数据包数目（不含错误帧）。
<b>Alignment错误包:</b>	端口接收的长度为64-9216字节的校验和错误且字节数对齐的数据帧（CRC Error）数目。（TL-SL2428/TL-SL2452） 端口接收的长度为64-10240字节的校验和错误的的数据帧数目。（TL-SG2452）
<b>小于64字节包:</b>	端口接收的长度小于64字节的数据帧数目（不含错误帧）。
<b>64字节包:</b>	端口接收的长度为64字节的数据帧数目（包含错误帧）。
<b>65-127字节包:</b>	端口接收的长度为65-127字节的数据帧数目（包含错误帧）。
<b>128-255字节包:</b>	端口接收的长度为128-255字节的数据帧数目（包含错误帧）。
<b>256-511字节包:</b>	端口接收的长度为256-511字节的数据帧数目（包含错误帧）。
<b>512-1023字节包:</b>	端口接收的长度为512-1023字节的数据帧数目（包含错误帧）。
<b>大于1023字节包:</b>	端口接收的长度大于1023字节小于1519字节（如果带VLAN-tag则小于1523字节）帧长的数据帧数目（包含错误帧）。（TL-SL2428/TL-SL2452） 端口接收的长度大于1023字节（小于等于10240字节）帧长的数据帧数目（包含错误帧）。（TL-SG2452）
<b>冲突包:</b>	端口工作在半双工模式下发送数据包时产生的冲突包数目。

## 5.4 地址表管理

交换机的主要功能是对报文进行转发，也就是根据报文的目的地MAC地址将报文输出到相应的端口。地址表包含了端口间报文转发的地址信息，是交换机实现报文快速转发的基础。地址表中的表项可以通过自动学习和手动绑定两种方式进行更新和维护，多数地址表条目都是通过自动学习功能来创建和维护的，而对于某些相对固定的连接来说，手动绑定可以提高交换机的效率，通过MAC地址过滤功能可以使交换机对不期望转发的数据帧进行过滤，从而提升了网络安全性。

地址表的分类及特点如下表所示：

地址表类别	配置方式	有无老化时间	重启后是否被保留 (配置保存后)	已绑定的MAC地址与端口的关系
静态地址表	手动配置	无	是	在同一VLAN中，已绑定的MAC地址不能被其它端口学习
动态地址表	自动学习	有	否	已绑定的MAC地址可以重新被其它端口学习
过滤地址表	手动配置	无	是	-

本功能包括地址表显示、静态地址表、动态地址表和过滤地址表四个配置页面。

### 5.4.1 地址表显示

在本页可以查看到交换机地址表的全部信息。

进入页面的方法：二层交换>>地址表管理>>地址表显示

显示配置

MAC地址：  （格式为：00-00-00-00-00-01）

VLAN ID：  （1-4094）

端口：  ▼

地址类型：  全部  静态  动态  过滤

地址表					
MAC地址	VLAN ID	端口	地址类型	老化状态	
00-19-66-35-E1-11	1	2	动态地址	正在老化	▲
00-19-66-CA-87-E7	1	2	动态地址	正在老化	
00-19-66-CA-87-CB	1	2	动态地址	正在老化	
00-23-AE-08-E3-63	1	2	动态地址	正在老化	
00-19-66-80-F8-A3	1	2	动态地址	正在老化	
00-19-66-CA-64-FA	1	2	动态地址	正在老化	
00-19-66-82-9A-4D	1	2	动态地址	正在老化	
00-19-66-82-9A-4C	1	2	动态地址	正在老化	
00-19-66-5E-EC-11	1	2	动态地址	正在老化	
00-19-66-CB-44-E5	1	2	动态地址	正在老化	
00-19-66-CB-44-D9	1	2	动态地址	正在老化	
00-19-66-CB-44-D8	1	2	动态地址	正在老化	▼

当前地址总数：58

**注意：**

默认显示条目上限为100条，请点击显示按钮获取完整的地址表信息。

图 5-13 地址表显示

条目介绍：

➤ 显示配置

**MAC地址：** 填写欲查找条目需包含的MAC地址信息。

**VLAN ID：** 填写欲查找条目需包含的VLAN ID信息。

**端口：** 选择欲查找条目需包含的交换机端口。



**地址类型：** 选择欲查找条目需包含的地址类型信息。

- 全部：显示全部地址表条目。
- 静态：显示静态地址表条目。
- 动态：显示动态地址表条目。
- 过滤：显示过滤地址表条目。

#### ➤ 地址表

**MAC地址：** 显示交换机学习到的MAC地址。

**VLAN ID：** 显示MAC地址条目对应的VLAN ID。

**端口：** 显示MAC地址条目对应的交换机端口。

**地址类型：** 显示MAC地址的类型。

**老化状态：** 显示MAC地址的老化状态。

### 5.4.2 静态地址表

静态地址表记录了端口上配置的静态地址。静态地址是不会老化的MAC地址，它区别于一般的由端口学习得到的动态地址。静态地址只能手动添加和删除，不受最大老化时间的限制。这对于某些相对固定的连接来说，可减少地址学习步骤，从而提高交换机的转发效率。静态地址表也可以显示在端口安全功能中自动学习到的静态MAC地址。

进入页面的方法：二层交换>>地址表管理>>静态地址表

**新建条目**

MAC地址： (格式为：00-00-00-00-00-01)

VLAN ID： (1-4094) 添加

端口： ▼

**查找条目**

查找选项： ▼  查找

**静态地址表**

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
<input type="checkbox"/>			端口 1 <span style="font-size: 0.8em;">▼</span>		

提交
删除
帮助

当前地址总数：0

**注意：**

默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

图 5-14 静态地址表

条目介绍:

➤ 新建条目

- MAC地址:** 填写静态绑定的MAC地址。
- VLAN ID:** 填写MAC地址条目对应的VLAN ID。
- 端口:** 选择静态绑定的交换机端口号。

➤ 查找条目

- 查找选项:** 选择静态地址表的显示规则，可以帮助您快速查找到所需的条目。
- **MAC:** 填写欲查找条目需包含的MAC地址信息。
  - **VLAN ID:** 填写欲查找条目需包含的VLAN ID信息。
  - **端口号:** 配置欲查找条目需包含的交换机端口号。

➤ 静态地址表

- 选择:** 勾选条目进行删除或修改该条目对应的交换机端口号，可多选。
- MAC地址:** 显示静态绑定的MAC地址。
- VLAN ID:** 显示MAC地址条目对应的VLAN ID。
- 端口:** 显示MAC地址条目对应的交换机端口。您可以在这里修改与静态MAC地址绑定的端口，但是修改后的端口必须是VLAN的成员端口。
- 地址类型:** 显示MAC地址的类型。
- 老化状态:** 显示MAC地址的老化状态。



**注意:**

- 如果地址的端口指定错误，或使用过程中端口（或设备）被人为改变，必须重新设置该静态地址表项，否则交换机将无法正确转发数据。
- 静态地址一旦被设置，如果把有此地址的网络设备连接到交换机的其它端口，交换机将不能动态识别。因此必须保证静态地址表中的表项都是正确有效的。
- 凡是加入到静态地址表的地址，不能同时加入到过滤地址表，也不能被端口动态绑定。

### 5.4.3 动态地址表

动态地址是交换机通过自动学习获取的MAC地址，交换机通过自动学习和老化来不断更新其动态地址表。

交换机的地址表的容量是有限的，为了最大限度利用地址表的资源，交换机使用老化机制来更新地址表，即：系统在动态学习地址的同时，开启老化定时器，如果在老化时间内没有再次收到相同地址的报文，交换机就会把该MAC地址从表项删除。

在本页可以配置交换机的动态地址表功能。

进入页面的方法：[二层交换](#)>>[地址表管理](#)>>[动态地址表](#)

**老化配置**

自动老化： 启用  禁用

老化时间： 秒（10-630秒，默认为300秒）

**查找条目**

查找选项：

**动态地址表**

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
<input type="checkbox"/>	00-19-66-80-54-36	1	9	动态地址	正在老化

---

当前地址总数：1

**注意：**  
默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

图 5-15 动态地址表

条目介绍：

➤ 老化设置

**自动老化：** 选择是否启用自动老化。

**老化时间：** 填写您需要的地址老化时间。默认为300秒。

➤ 查找条目

**查找选项：** 选择动态地址表的显示规则，可以帮助您快速查找到所需的条目。

- **MAC：** 填写欲查找条目需包含的MAC地址信息。
- **VLAN ID：** 填写欲查找条目需包含的VLAN ID信息。
- **端口号：** 选择欲查找条目需包含的交换机端口号。
- **LAG ID：** 选择欲查找条目需包含的LAG ID。

➤ 动态地址表

**选择：** 勾选动态地址条目进行删除或将该条目绑定为静态地址，可多选。

**MAC地址：** 显示动态绑定的MAC地址。

**VLAN ID：** 显示MAC地址条目对应的VLAN ID。

**端口：** 显示MAC地址条目对应的交换机端口。

**地址类型：** 显示MAC地址的类型。

**老化状态：** 显示MAC地址的老化状态。

**绑定：** 将动态绑定的地址条目转化为静态绑定。

**说明：**

- 老化时间过长会导致交换机的地址表中保存过多过时的地址表项，从而耗尽地址表的资源，导致交换机无法根据网络的变化更新地址表。老化时间过短，又会造成地址表刷新过快，大量接收到的数据包的目的地址在地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这将降低交换机的性能。建议您使用默认值。

## 5.4.4 过滤地址表

通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤，过滤地址不会被老化，只能手工进行添加和删除。在过滤地址表中添加受限的MAC地址后，交换机将自动过滤掉源/目的地址为这个地址的帧，以达到安全的目的。过滤地址表中的地址对所有的交换机端口都生效。

进入页面的方法：二层交换>>地址表管理>>过滤地址表

**新建条目**

MAC地址：  （格式为：00-00-00-00-00-01）

VLAN ID：  （1-4094） 添加

**查找条目**

查找选项： 全部  查找

**过滤地址表**

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">全选</span> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">删除</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">帮助</span>					

---

当前地址总数： 0

**注意：**  
默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

图 5-16 过滤地址表

条目介绍：

➤ **新建条目**

**MAC地址：** 填写过滤的MAC地址。

**VLAN ID：** 填写MAC地址条目对应的VLAN ID。

➤ **查找条目**

**查找选项：** 选择过滤地址表的显示规则，可以帮助您快速查找到所需的条目。

- **MAC：** 填写欲查找条目需包含的MAC地址信息。
- **VLAN ID：** 填写欲查找条目需包含的VLAN ID信息。

## ➤ 静态地址表

- 选择:** 勾选过滤地址条目进行删除，可多选。
- MAC地址:** 显示过滤的MAC地址。
- VLAN ID:** 显示MAC地址条目对应的VLAN ID。
- 端口:** 此处为"--", 表示无指定端口。
- 地址类型:** 显示MAC地址的类型。
- 老化状态:** 显示MAC地址的老化状态。



### 注意:

- 已加入到过滤地址表中的地址不能被加入到静态地址表中，也不能被端口动态绑定。

## 5.5 DHCP过滤

通过DHCP过滤功能可以侦听用户动态申请IP地址的过程，并通过设置信任端口对客户请求进行过滤。

进入页面的方法：二层交换>>DHCP过滤>>DHCP过滤

DHCP过滤

DHCP过滤： 启用  禁用 提交

信任端口					
<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12
<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18
<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28		

提交
全选
清空
帮助

图 5-17 DHCP过滤

条目介绍:

### ➤ DHCP过滤

**DHCP过滤:** 选择是否启用DHCP过滤功能。

### ➤ 信任端口

**信任端口:** 选择是否配置端口为信任端口，只有信任端口才能接收来自DHCP服务器端的消息。

[回目录](#)

## 第6章 VLAN

以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机实现LAN互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了VLAN（Virtual Local Area Network）技术，这种技术可以把一个LAN划分成多个逻辑的LAN——VLAN，每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文被限制在一个VLAN内。同一个VLAN内的主机通过传统的以太网通信方式进行报文的交互，而不同VLAN内的主机之间则需要通过路由器或三层交换机等网络层设备进行通信。如图 6-1所示。

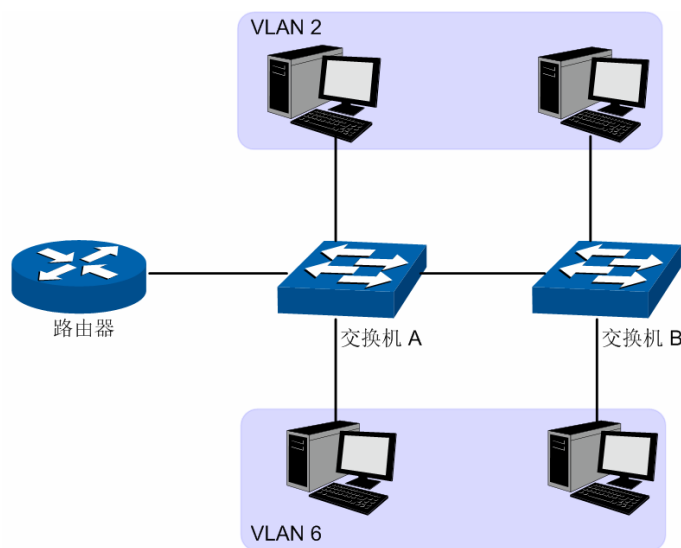


图 6-1 VLAN示意图

VLAN的优点如下：

- 1) 提高网络性能。将广播包限制在VLAN内，从而有效控制网络的广播风暴，节省了网络带宽，从而提高网络处理能力。
- 2) 增强网络安全。不同VLAN的设备不能互相访问，不同VLAN的主机不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。
- 3) 简化网络管理。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

VLAN的划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个VLAN；一个VLAN包含的用户可以连接在同一个交换机上，也可以跨越交换机。本交换机支持的VLAN划分方式为802.1Q VLAN。当交换机收到带VLAN tag的数据包时，会根据VLAN tag来判断此数据包属于哪个VLAN；若数据包不带VLAN tag，则根据数据包接收端口的PVID值添加802.1Q VLAN的标识tag，并在相应的VLAN中转发数据包。

### 6.1 802.1Q VLAN

由于普通交换机工作在OSI模型的数据链路层，若要交换机能够识别不同VLAN的数据包，只能对数据包的数据链路层封装进行VLAN识别。因此，VLAN识别字段被添加到数据链路层封装中。

IEEE 802.1Q协议为了标准化VLAN实现方案，对带有VLAN标识的数据包结构进行了统一规定。协议规定在目的MAC地址和源MAC地址之后封装4个字节的VLAN Tag，用以标识VLAN的相关信息，如图 6-2所示。VLAN Tag包含四个字段，分别是TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和VLAN ID。

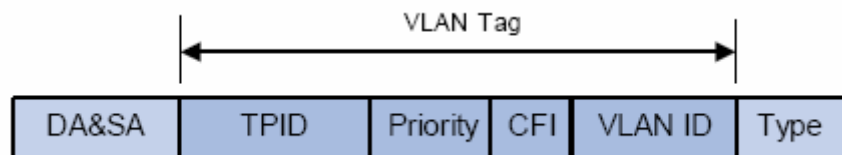


图 6-2 VLAN Tag组成字段

- 1) TPID: 用来表示本数据帧是带有VLAN Tag的数据。该字段长度为16bit。协议规定的缺省取值为0x8100。
- 2) Priority: 用来表示数据包的传输优先级。
- 3) CFI: 以太网交换机中，CFI总被设置为0。由于兼容特性，CFI常用于以太网类网络和令牌环类网络之间，如果在以太网端口接收的帧CFI设置为1，表示该帧不进行转发，这是因为以太网端口是一个无标签端口。
- 4) VLAN ID: 用来标识该报文所属VLAN的编号。该字段长度为12bit，取值范围为0~4095。由于0和4095通常不使用，所以VLAN ID的取值范围一般为1~4094。VLAN ID简称VID。

交换机利用VLAN ID来识别报文所属的VLAN，当接收到的数据包不携带VLAN Tag时，交换机会为该数据包封装带有接收端口缺省VLAN ID的VLAN Tag，将数据包在接收端口的缺省VLAN中进行传输。

本手册中，对包含VLAN Tag字段的数据包我们简称为tag帧，untag帧指数据包中没有VLAN Tag字段的数据包，优先级tag帧指数据包中有VLAN Tag字段，但VLAN ID为0的数据包。

#### ➤ 端口的链路类型

在创建802.1Q VLAN时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面两种：

- 1) Untagged: Untagged端口可以加入多个VLAN。当带tag的VLAN数据包到达一个端口，而其VLAN ID与该端口允许进入的VLAN都不匹配，则该数据包将被丢弃。Untagged端口转发的数据包都是不带tag的。
- 2) Tagged: Tagged端口可以加入多个VLAN。当带tag的VLAN数据包到达一个端口，而其VLAN ID与该端口允许进入的VLAN都不匹配，则该数据包将被丢弃。Tagged端口转发VLAN的数据包时，不改变其携带的VLAN信息。

#### ➤ PVID与VLAN数据包处理关系

PVID（Port VLAN ID），就是端口的缺省VID。当交换机的端口接收到的报文不带VLAN Tag时，交换机会根据接收端口的PVID值为该报文插入VLAN Tag，并进行转发。

当在局域网中划分VLAN时，PVID是每个端口的一个重要参数，表示端口默认所属的VLAN。它有两个用途：

- 1) 当端口收到untag报文时，将根据PVID为数据包插入VLAN Tag。

- 2) PVID指定了端口的默认广播域，即当端口接收到UL包或广播包的时候，交换机将这些数据包在该端口的缺省VLAN内广播。

端口的链路类型本质上是交换机对出入端口的VLAN Tag的处理方式，详细规则如表 6-1所示。

端口类型	对接收报文的处理		发送报文时的处理	
	报文不带Tag	报文带Tag	报文不带Tag	报文带Tag
Untagged	接收报文，并为报文添加缺省的VLAN Tag，即输入端口的PVID。	当VID属于端口允许通过的VLAN ID时，接收报文。	不改变数据包而发送报文。	去掉Tag后，发送报文。
Tagged		当VID不属于该端口允许通过的VLAN ID时，丢弃报文。	以出口端口的PVID为其VLAN Tag而发送报文。	

表 6-1 端口类型与VLAN数据处理关系

IEEE 802.1Q VLAN功能包括VLAN配置配置页面。

### 6.1.1 VLAN配置

在VLAN配置页面中可以设置802.1Q VLAN和其包含的端口。

进入页面的方法：**VLAN>>802.1Q VLAN>>VLAN配置**

创建VLAN

VLAN ID:  (2-4094) 创建

名称:  (1-16个字符)

---

VLAN总表

选择	VLAN ID	名称	Untagged端口	Tagged端口	操作
<input type="checkbox"/>	1	Default VLAN	1-52		删除

---

VLAN配置表

	VLAN ID														VLAN名称													
端口	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
非成员	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	
LAG	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

提交
帮助

图 6-3 VLAN配置

在缺省情况下，为了保证交换机在出厂情况下能正常通信，所有端口的缺省VLAN均为VLAN1，只有属于VLAN1的端口才能访问交换机Web页面。VLAN1无法删除。



条目介绍:

➤ **创建VLAN**

**VLAN ID:** 填写VLAN ID。

**名称:** 填写VLAN的名称，便于区分各个VLAN的用途。不同的VLAN之间名称不能相同。

点击<创建>按钮即可创建VLAN。

➤ **VLAN总表**

**VLAN ID选择:** 点击<选择>按键，可根据所输VLAN ID，快速选中VLAN条目。

**选择:** 勾选条目进行操作，只能选中一个VLAN。

**VLAN ID:** 显示VLAN ID。

**名称:** 显示选中VLAN的名称。

**不带tag的端口:** 显示选中VLAN的不带tag端口。

**带tag端口:** 显示选中VLAN的带tag端口。

**操作:** 点击“删除”，可以删除选中的VLAN。

➤ **VLAN配置表**

**VLAN ID:** 选中的VLAN ID。

**VLAN名称:** 选中的VLAN的名称。

**端口:** 显示交换机的端口号。

**Untagged:** 如果选择此项，则该端口作为不带tag的成员加入到VLAN中。

**Tagged:** 如果选择此项，则该端口作为带tag的成员加入到VLAN中。

**非成员:** 如果选择此项，则该端口将不作VLAN的端口成员。

**PVID:** 可以在此更改端口的PVID。

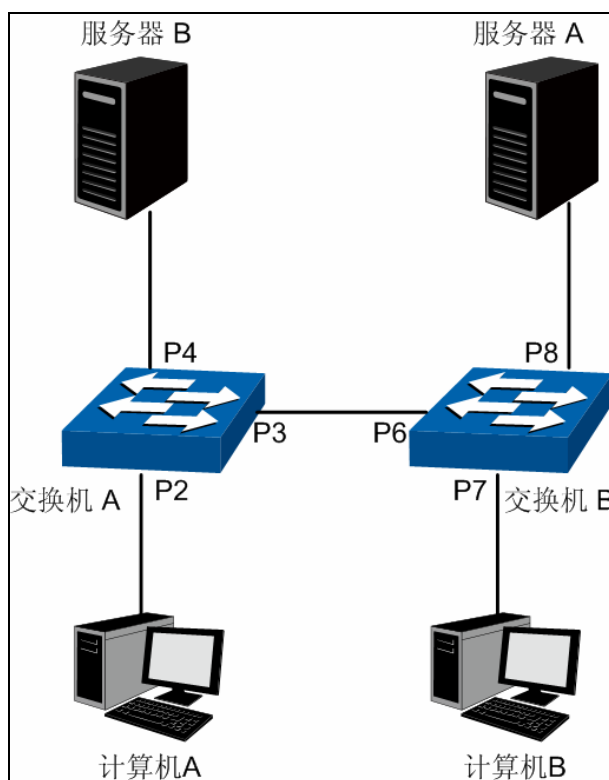
**LAG:** 显示端口当前所属的汇聚组。

## 6.2 802.1Q VLAN功能的组网应用

➤ **组网需求**

- 交换机A连接了计算机A和服务器B;
- 交换机B连接了计算机B和服务器A;
- 计算机A和服务器A同属于一个部门;
- 计算机B和服务器B同属于一个部门;
- 两个部门以VLAN划分，相互之间不能通信。

## 组网图



图中的“P数字”表示交换机的端口号。

## 配置步骤

### 配置交换机A:

步骤	操作	说明
1	创建VLAN10	必选操作。在 <b>VLAN&gt;&gt;802.1Q VLAN&gt;&gt;VLAN配置</b> 页面， <b>创建VLAN</b> 区域，设置VLAN ID为10，点击<创建>按钮创建VLAN；然后在 <b>VLAN总表</b> 区域，选择VLAN ID为10的条目，且在 <b>VLAN配置表</b> 区域，设置端口2的类型为Untagged，端口3的类型为Tagged。
2	创建VLAN20	必选操作。在 <b>VLAN&gt;&gt;802.1Q VLAN&gt;&gt;VLAN配置</b> 页面， <b>创建VLAN</b> 区域，设置VLAN ID为20，点击<创建>按钮创建VLAN；然后在 <b>VLAN总表</b> 区域，选择VLAN ID为20的条目，且在 <b>VLAN配置表</b> 区域，设置端口3的类型为Tagged，端口4类型为Untagged。

### 配置交换机B:

步骤	操作	说明
1	创建VLAN10	必选操作。在 <b>VLAN&gt;&gt;802.1Q VLAN&gt;&gt;VLAN配置</b> 页面， <b>创建VLAN</b> 区域，设置VLAN ID为10，点击<创建>按钮创建VLAN；然后在 <b>VLAN总表</b> 区域，选择VLAN ID为10的条目，且在 <b>VLAN配置表</b> 区域，设置端口6的类型为Tagged，端口8的类型为Untagged。

步骤	操作	说明
2	创建VLAN20	必选操作。在 <b>VLAN&gt;&gt;802.1Q VLAN&gt;&gt;VLAN配置</b> 页面， <b>创建VLAN</b> 区域，设置VLAN ID为20，点击<创建>按钮创建VLAN；然后在 <b>VLAN总表</b> 区域，选择VLAN ID为20的条目，且在 <b>VLAN配置表</b> 区域，设置端口6的类型为Tagged，端口7的类型为Untagged。

[回目录](#)

## 第7章 生成树

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，并有选择的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，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文所造成的报文处理能力下降的问题发生。

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设备完成生成树的计算过程。STP即是通过在设备之间传递BPDU来确定网络的拓扑结构。

### ➤ BPDU格式及字段说明

要实现生成树的功能，交换机之间传递BPDU报文实现信息交互，所有支持STP协议的交换机都会接收并处理收到的报文。该报文在数据区里携带了用于生成树计算的所有有用信息。

标准生成树的BPDU帧格式及字段说明：

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
8	2	2	2	2	2
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay

**Protocol identifier:** 协议标识

**Version:** 协议版本

**Message type:** BPDU类型

**Flag:** 标志位

**Root ID:** 根桥ID，由两字节的优先级和6字节MAC地址构成

**Root path cost:** 根路径开销

**Bridge ID:** 桥ID，表示发送BPDU的桥的ID，由2字节优先级和6字节MAC地址构成

**Port ID:** 端口ID，标识发出BPDU的端口

**Message age:** BPDU生存时间

**Maximum age:** 当前BPDU的老化时间，即端口保存BPDU的最长时间

**Hello time:** 根桥发送BPDU的周期

**Forward delay:** 表示在拓扑改变后，交换机在发送数据包前维持在监听和学习状态的时间

### ➤ STP的基本概念

**桥ID (Bridge Identifier):** 桥ID是桥的优先级和其MAC地址的综合数值，其中桥优先级是一个可以设定的参数。桥ID越低，则桥的优先级越高，这样可以增加其成为根桥的可能性。

**根桥 (Root Bridge):** 具有最小桥ID的交换机是根桥。请将环路中所有交换机当中最好的一台设置为根桥交换机，以保证能够提供最好的网络性能和可靠性。

**指定桥 (Designated Bridge):** 在每个网段中，到根桥的路径开销最低的桥将成为指定桥，数据包将通过它转发到该网段。当所有的交换机具有相同的根路径开销时，具有最低的桥ID的交换机会被选为指定桥。

**根路径开销 (Root Path Cost):** 一台交换机的根路径开销是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零。

**桥优先级 (Bridge Priority):** 是一个用户可以设定的参数，数值范围从0到61440。设定的值越小，优先级越高。交换机的桥优先级越高，才越有可能成为根桥。

**根端口 (Root Port):** 非根桥的交换机上离根桥最近的端口，负责与根桥进行通信，这个端口到根桥的路径开销最低。当多个端口具有相同的到根桥的路径开销时，具有最高端口优先级的端口会成为根端口。

**指定端口 (Designated Port):** 指定桥上向本交换机转发数据的端口。

**端口优先级 (Port Priority):** 数值范围从0到255，值越小，端口的优先级就越高。端口的优先级越高，才越有可能成为根端口。

**路径开销 (Path Cost):** 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。

生成树基本概念的组网示意图如图 7-1所示。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2和端口6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3和端口5分别为交换机B和交换机C的根端口；端口1和端口4分别为交换机A和交换机B的指定端口；端口6为交换机C的阻塞端口。

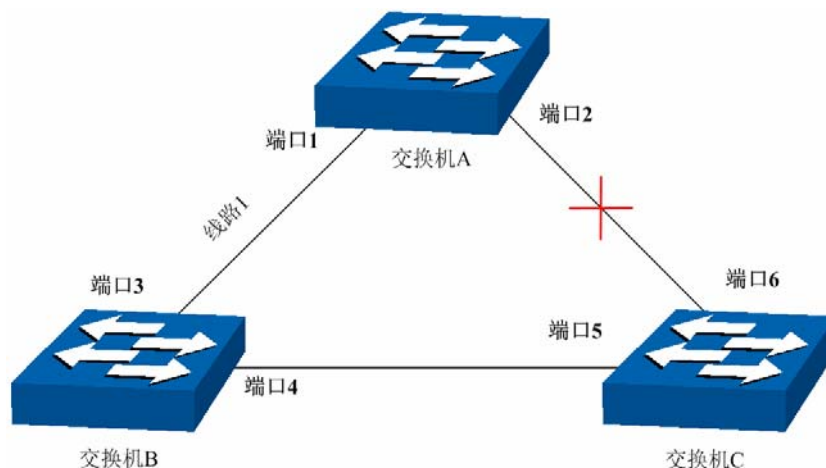


图 7-1 生成树基本概念组网图

## ➤ STP定时器

**联络时间 (Hello Time):**

数值范围从1秒到10秒。是指根桥向其它所有交换机发出BPDU数据包的时间间隔，用于交换机检测链路是否存在故障。

**老化时间 (Max. Age):**

数值范围从6秒到40秒。如果在超出老化时间之后，还没有收到根桥发出的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。

**传输时延 (Forward Delay):**

数值范围从4秒到30秒。是指交换机的端口状态迁移所用的时间。

当网络故障引发生成树重新计算时，生成树的结构将发生相应的变化。但是重新计算得到的新配置消息无法立刻传遍整个网络，如果端口状态立刻迁移的话，可能会产生暂时性的环路。为此，生成树协议采用了一种状态迁移的机制，新的根端口和指定端口开始数据转发之前要经过2倍的传输时延，这个延时保证了新的配置消息已经传遍整个网络。

**➤ STP模式的BPDU的优先级比较原则**

假定有两条BPDU X和Y，则：

如果X的根桥ID小于Y的根桥ID，则X优于Y；

如果X和Y的根桥ID相同，但X的根路径开销小于Y，则X优于Y；

如果X和Y的根桥ID和根路径开销相同，但X的桥ID小于Y，则X优于Y；

如果X和Y的根桥ID、根路径开销和桥ID相同，但X的端口ID小于Y，则X优于Y。

**➤ STP的计算过程**

- 初始状态

每台交换机在初始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。

- 最优BPDU的选择

每台交换机都向外发送自己的BPDU，同时也会收到其它交换机发送的BPDU。比较过程如下表所述：

步骤	内容
1	当端口收到的BPDU比本端口BPDU的优先级低时，交换机将丢弃接收到的BPDU，保留该端口的BPDU；否则，交换机将接收到的BPDU替换成为该端口的BPDU。
2	交换机将所有端口的BPDU进行比较，选出最优的BPDU作为本交换机的BPDU。

表 7-1 最优BPDU的选择

- 根桥的选择

通过交换配置消息，设备之间比较根桥ID，网络中根桥ID 最小的设备被选为根桥。

- 根端口、指定端口的选择

根端口、指定端口的选择过程如下表所述：

步骤	内容
1	非根桥交换机将接收到最优BPDU的那个端口指定为根端口。

步骤	内容
2	交换机根据根端口的BPDU和根端口的路径开销，为其它端口计算一个端口BPDU： <ul style="list-style-type: none"> <li>根桥ID替换为根端口的根桥ID；</li> <li>根路径开销替换为根端口的根路径开销加上本端口到根端口的路径开销；</li> <li>指定桥ID替换为自身设备的ID；</li> <li>指定端口ID替换为自身端口ID。</li> </ul>
3	交换机使用计算出来的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： <ul style="list-style-type: none"> <li>如果计算出来的BPDU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。</li> <li>如果端口上的BPDU优，则设备不更新该端口BPDU并将此端口阻塞，该端口将不再转发数据，只接收但不发送配置消息；</li> </ul>

表 7-2 根端口、指定端口的选择

**说明：**

- 在拓扑稳定状态，只有根端口和指定端口转发数据，其它的端口都处于阻塞状态，它们只接收BPDU报文而不转发数据。

**> RSTP**

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是优化版的STP，他大大缩短了端口进入转发状态的延时，从而缩短了网络最终达到拓扑稳定所需要的时间。RSTP的端口状态实现快速迁移的前提如下：

- 根端口的端口状态快速迁移的条件是：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经开始转发数据。
- 指定端口的端口状态快速迁移的条件是：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

**> RSTP的基本概念**

**边缘端口（Edge Port）：**直接与终端相连而不是与其它交换机相连的端口。

**点对点链路：**是两台交换机之间直接连接的链路。

**> MSTP**

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在STP和RSTP的基础上，根据IEEE协会制定的802.1S标准建立的，他既可以快速收敛，也能使不同VLAN的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

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在数据转发过程中实现VLAN数据的负载分担。
- MSTP兼容STP和RSTP。

#### ➤ MSTP的基本概念

**MST域**（Multiple Spanning Tree Region，多生成树域）：由具有相同域配置和相同Vlan-实例映射关系的交换机所构成。

**IST**（Internal Spanning Tree，内部生成树）：MST域内的一棵生成树。

**CST**（Common Spanning Tree，公共生成树）：连接网络内所有MST域的单生成树。

**CIST**（Common and Internal Spanning Tree，公共和内部生成树）：连接网络内所有设备的单生成树，由IST和CST共同构成。

MSTP基本概念的组网图如图 7-2所示。

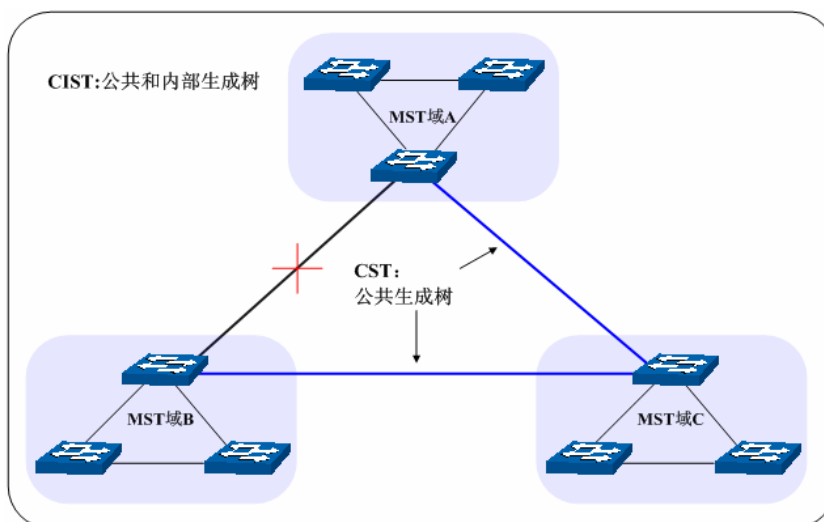


图 7-2 MSTP基本概念组网图

#### ➤ MSTP的基本原理

MSTP将整个网络划分为多个MST域，各个域之间通过计算生成CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。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模式的BPDU优先级比较原则

假定有两条MSTP的BPDU X和Y，则：

如果X的总根ID小于Y的总根ID，则X优于Y；

如果X和Y的总根ID相同，但X的外部路径开销小于Y，则X优于Y；

如果X和Y的总根ID和外部路径开销相同，但X的域根ID小于Y的域根ID，则X优于Y；

如果X和Y的总根ID、外部路径开销和域根ID相同，但X的内部路径开销小于Y，则X优于Y；

如果X和Y的总根ID、外部路径开销、域根ID和内部路径开销相同，但X的桥ID小于Y，则X优于Y；



如果X和Y的总根ID、外部路径开销、域根ID、内部路径开销和桥ID均相同，但X的端口ID小于Y，则X优于Y。

### ➤ 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：

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

### ➤ 端口角色

MSTP的端口角色分为以下几种：

- 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。
- 指定端口：负责向下游网段或设备转发数据的端口。
- 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。
- 替换端口：根端口和Master端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口角色的示意图如图 7-3所示。

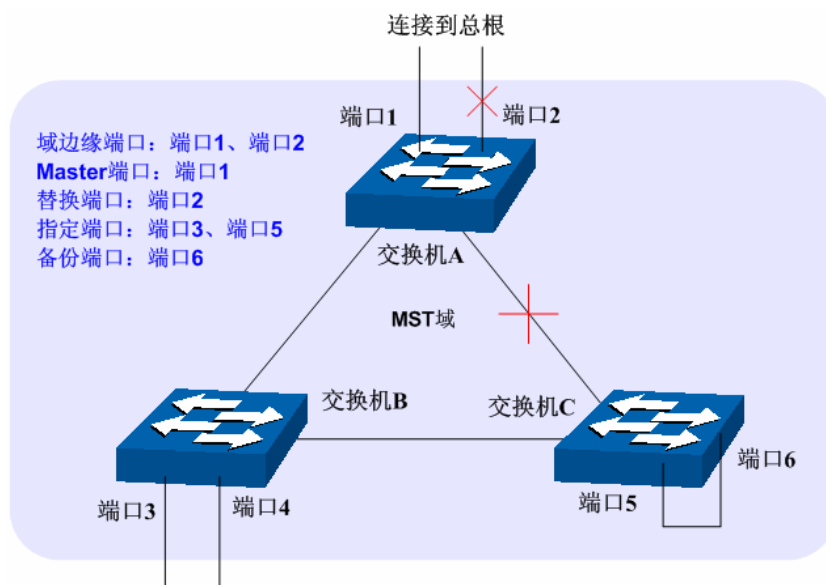


图 7-3 端口角色示意图

生成树模块主要用于配置交换机的生成树功能，包括基本配置、端口配置、MSTP实例以及安全配置四个部分。

## 7.1 基本配置

基本配置用于配置和查看交换机生成树功能的全局属性，本功能包括**基本配置**和**生成树信息**两个配置页面。

### 7.1.1 基本配置

配置生成树前您需要明确各交换机在每个生成树实例中所处的地位，每个生成树实例中只有一台交换机处于根桥地位。配置交换机的生成树功能，首先需要在本页配置交换机生成树的全局功能和相关参数。

进入页面的方法：**生成树>>基本配置>>基本配置**

**全局配置**

生成树功能： 启用  禁用

生成树模式： ▼

**参数配置**

CIST优先级： (0 - 61440, 4096为间隔)

联络时间： 秒 (1-10)

老化时间： 秒 (6-40)

传输时延： 秒 (4-30)

流量限制： pps (1-20)

最大跳数： 跳 (1-40)

图 7-4 基本配置

条目介绍：

#### ➤ 全局配置

**生成树功能：** 选择是否启用交换机的生成树功能。

**生成树模式：** 选择交换机的生成树模式。

- STP：生成树兼容模式。
- RSTP：快速生成树兼容模式。
- MSTP：多重生成树模式。

#### ➤ 参数配置

**CIST优先级：** 填写交换机的CIST优先级。CIST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。值越小，表示优先级越高。默认为32768，且必须是4096的倍数。

- 联络时间:** 填写交换机发送协议报文的周期，用于检测链路是否存在故障。并且， $2 \times (\text{联络时间} + 1) \leq \text{老化时间}$ 。默认为2秒。
- 老化时间:** 填写协议报文在交换机中能够保存的最大生存期。默认为20秒。
- 传输时延:** 在网络拓扑改变后，交换机的端口状态迁移的延时时间。并且， $2 \times (\text{传输时延} - 1) \geq \text{老化时间}$ 。默认为15秒。
- 流量限制:** 填写在每个联络时间内，端口最多能够发送的协议报文的速率。默认为5pps。
- 最大跳数:** 填写协议报文被转发的最大跳数，限制生成树的规模，默认20跳。

**注意:**

- 设备的传输时延参数的长短与STP的规模有关。如果传输时延过小，可能会引入临时的环路；如果传输时延过大，网络可能会较长时间不能恢复连通，建议采用默认值。
- 合适的联络时间可以保证设备能够及时发现网络中的链路故障，又不会占用过多的网络资源。如果联络时间过长，在链路发生丢包时，交换机会误以为链路出现了故障，从而引发网络中生成树的重新计算；如果联络时间过短，交换机将频繁发送重复的配置消息，增加了交换机的负担，浪费了网络资源，建议采用默认值。
- 如果老化时间过小，交换机会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果老化时间过大，交换机不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力，建议采用默认值。
- 如果流量限制过大，每个联络时间内发送的MSTP报文数会很多，从而占用过多的网络资源，建议采用默认值。

## 7.1.2 生成树信息

本页用来查看交换机生成树功能的相关参数。

进入页面的方法：生成树>>基本配置>>生成树信息

生成树信息	
开启状态：	启用
STP版本：	MSTP
本桥：	32768---00-02-03-c0-9a-d3
总根：	32768---00-02-03-c0-9a-d3
外部路径开销：	0
域根：	32768---00-02-03-c0-9a-d3
内部路径开销：	0
指定桥：	32768---00-02-03-c0-9a-d3
根端口：	---
上次拓扑改变时间：	2006-01-01 10:43:30
拓扑改变次数：	1

MSTP实例信息	
实例ID：	1 ▾
开启状态：	启用
本桥：	32768---00-02-03-c0-9a-d3
域根：	32768---00-02-03-c0-9a-d3
内部路径开销：	0
指定桥：	32768---00-02-03-c0-9a-d3
根端口：	---
上次拓扑改变时间：	2006-01-01 10:44:41
拓扑改变次数：	1

图 7-5 基本信息

## 7.2 端口配置

本页用来配置交换机端口的CIST参数。

进入页面的方法：生成树>>端口配置>>端口配置

端口配置												
选择	端口	状态	优先级	外部路径开销	内部路径开销	边缘端口	点对点链路	协议迁移	工作模式	端口角色	端口状态	LAG
<input type="checkbox"/>		禁用	128	自动	自动	禁用	自动	不改变	---	---	---	---
<input type="checkbox"/>	1	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	2	启用	128	19(自动)	19(自动)	禁用	开启(自动)	---	STP	指定端口	转发	---
<input type="checkbox"/>	3	启用	128	100(自动)	100(自动)	禁用	关闭(自动)	---	---	禁用端口	断开	---
<input type="checkbox"/>	4	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	5	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	6	启用	128	100(自动)	100(自动)	禁用	关闭(自动)	---	---	禁用端口	断开	---
<input type="checkbox"/>	7	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	8	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	9	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	10	启用	128	19(自动)	19(自动)	禁用	开启(自动)	---	STP	指定端口	转发	---
<input type="checkbox"/>	11	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	12	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	13	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	14	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
<input type="checkbox"/>	15	禁用	128	自动	自动	禁用	自动	---	---	---	---	---

**注意：**

将路径开销设置为0，即可根据端口连接速率自动设置路径开销。

图 7-6 端口配置

条目介绍：

➤ **端口配置**

- 端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：** 勾选端口配置端口STP功能，可多选。
- 端口：** 显示交换机的端口号。
- 状态：** 选择该端口是否启用STP功能。
- 优先级：** 确定与该端口连接的端口是否会被选为根端口的的重要依据。同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。默认为128，范围0-240，且为16的倍数。
- 外部路径开销：** 在不同MST域之间的路径上，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。
- 内部路径开销：** 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。
- 边缘端口：** 选择是否启用边缘端口。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

- 点对点链路:** 选择端口的点对点链路状态。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。
- 协议迁移:** 启用端口开始一次协议迁移检查。
- 工作模式:** 显示端口所处的生成树模式。
- 端口角色:** 显示端口在生成树实例中担任的角色。
- 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。
  - 指定端口：负责向下游网段或设备转发数据的端口。
  - Master端口：连接多生成树域到总根的端口，位于整个域到总根的最短路径上。
  - 替换端口：根端口和Master端口的备份端口。
  - 备份端口：指定端口的备份端口。
  - 禁用端口：物理链路断开的端口。
- 端口状态:** 显示端口所处的工作状态。
- 转发：接收并转发数据，接收并发送协议报文，进行地址学习。
  - 学习：不接收或转发数据，接收并发送协议报文，进行地址学习。
  - 阻塞：不接收或转发数据，接收但不发送协议报文，不进行地址学习。
  - 断开：物理链路断开。
- LAG:** 显示端口当前所属的汇聚组。

**注意:**

- 对于直接与终端相连的端口，请将该端口设置为边缘端口，同时启动BPDU保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。
- 对于属于汇聚组的端口，所有端口都可以被配置成与点对点链路相连。
- 当端口被设置为与点对点链路相连，则该端口所在的所有生成树实例均被设置为与点对点链路相连。如果端口实际物理链路不是点对点链路，而您配置为强制点对点链路，则有可能会引入临时环路。

## 7.3 MSTP实例

MSTP设置了VLAN-实例映射表（即VLAN和生成树的对应关系表），把VLAN和生成树联系起来。通过增加MSTP实例（将多个VLAN整合到一个集合中），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。

只有当多台交换机的MST域名、MST域的修订级别、VLAN-实例映射表完全相同时，它们才能属于同一个MST域。本功能包括**域配置**、**实例配置**和**实例端口**三个配置页面。

### 7.3.1 域配置

本页用来配置MST域的域名和修订级别。

进入页面的方法：**生成树>>MSTP实例>>域配置**

域配置	
域名：	<input type="text" value="00-02-03-c0-9a-d3"/>
修订级别：	<input type="text" value="0"/> ( 0 - 65535 )
<input type="button" value="提交"/>	
<input type="button" value="帮助"/>	

图 7-7 域配置

条目介绍：

➤ 域配置

**域名：** 填写域名来标识MST域，最长可用32个字符。

**修订级别：** 填写修订级别来标识MST域。

### 7.3.2 实例配置

实例配置是MST域的一个属性，用来描述VLAN和生成树实例的映射关系。您可以按需要将VLAN分配至不同的实例，每个实例就是一个“VLAN组”，不受其它实例和公共生成树的影响。

进入页面的方法：生成树>>MSTP实例>>实例配置

实例配置					
选择	实例ID	状态	优先级	VLAN ID	实例ID <input type="text"/> <input type="button" value="选择"/>
<input type="checkbox"/>			<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	1	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	2	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	3	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	4	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	5	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	6	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	7	禁用	32768		<a href="#">删除映射</a>
<input type="checkbox"/>	8	禁用	32768		<a href="#">删除映射</a>
	CIST	启用	32768	1-4094,	

VLAN-实例映射	
VLAN ID：	<input type="text"/> ( 1 - 4094 )
实例ID：	<input type="text"/> ( 0 - 8 , 0代表CIST )
<input type="button" value="提交"/>	

**注意：**

VLAN ID输入格式例如：'1,3,4-7,9,11-30'，且VID范围取1-4094

图 7-8 实例配置

条目介绍:

➤ **实例配置**

- 实例ID选择:** 点击<选择>按键, 可根据所输ID号, 快速选择相应实例。
- 选择:** 勾选条目配置实例状态及优先级, 可多选。
- 实例ID:** 显示交换机的实例ID号。
- 状态:** 显示相应实例的状态。
- 优先级:** 在对应实例ID中, 确定该交换机是否会被选为根桥的重要依据。默认为32768, 且必须是4096的倍数。
- VLAN ID:** 填写该实例ID所包含的VLAN ID。若之前已存在VLAN ID, 在此修改后, 之前的VLAN ID将被清空, 并映射至CIST中。

➤ **VLAN-实例映射**

- VLAN ID:** 填写需要添加的VLAN ID。若对应实例ID中已有VLAN ID, 在此修改后, 新的VLAN ID将被添加, 而不会将之前的覆盖。
- 实例ID:** 填写实例ID。



### 7.3.3 实例端口

端口在不同的生成树实例中可以担任不同的角色，本页用来配置不同实例ID中的端口的参数，同时在此可以查看端口在特定实例中的状态信息。

进入页面的方法：生成树>>MSTP实例>>实例端口

实例端口配置

实例ID 
端口

选择	端口	优先级	路径开销	端口角色	端口状态	LAG
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>			
<input type="checkbox"/>	1	128	自动	---	---	---
<input type="checkbox"/>	2	128	自动	---	---	---
<input type="checkbox"/>	3	128	自动	---	---	---
<input type="checkbox"/>	4	128	自动	---	---	---
<input type="checkbox"/>	5	128	自动	---	---	---
<input type="checkbox"/>	6	128	自动	---	---	---
<input type="checkbox"/>	7	128	自动	---	---	---
<input type="checkbox"/>	8	128	自动	---	---	---
<input type="checkbox"/>	9	128	自动	---	---	---
<input type="checkbox"/>	10	128	自动	---	---	---
<input type="checkbox"/>	11	128	自动	---	---	---
<input type="checkbox"/>	12	128	自动	---	---	---
<input type="checkbox"/>	13	128	自动	---	---	---
<input type="checkbox"/>	14	128	自动	---	---	---
<input type="checkbox"/>	15	128	自动	---	---	---

#### 注意：

将路径开销设置为0，即可根据端口连接速率自动设置路径开销。

图 7-9 实例端口

条目介绍：

#### 实例端口配置

- 实例ID：**选择需要配置端口属性的实例ID。
- 端口选择：**点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：**勾选端口配置端口的优先级和路径开销，可多选。
- 端口：**显示交换机的端口号。
- 优先级：**在对应实例ID中，确定与该端口连接的端口是否会被选为根端口的重要依据。默认为128，范围0-240，且为16的倍数。
- 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。
- 端口角色：**显示端口在生成树实例中担任的角色。

**端口状态:** 显示端口所处的工作状态。

**LAG:** 显示端口当前所属的汇聚组。



**注意:**

- 同一端口在不同的生成树实例中的端口状态可以不同。

安全树功能全局配置步骤:

步骤	操作	说明
1	明确交换机在生成树实例中的角色: 根桥或指定桥	准备工作。
2	配置MSTP的全局参数	必选操作。在生成树>>基本配置>>基本配置页面, 开启交换机的生成树功能, 并配置MSTP的参数。
3	配置端口的MSTP参数	必选操作。生成树>>端口配置>>端口配置页面进行配置。
4	配置MST域	必选操作。生成树>>MSTP实例>>域配置、实例配置页面, 创建MST域, 及交换机在MST域中的角色。
5	配置实例端口的MSTP参数	可选操作。生成树>>MSTP实例>>实例端口页面, 为MST域内不同的实例, 配置实例端口的MSTP属性。

## 7.4 安全配置

通过配置设备的保护功能, 来防止生成树网络中的设备遭受各种形式的恶意攻击。本功能包括**端口保护**和**TC保护**两个配置页面。

### 7.4.1 端口保护

#### > 环路保护:

在网络拓扑稳定时, 交换机通过不断接收上游交换机发送的BPDU报文, 来保持本机各个端口的端口状态。但是当发生链路拥塞或者单向链路故障时, 位于下游的交换机无法收到BPDU报文, 将会重新计算生成树, 重新选择端口角色, 这时阻塞端口会迁移到转发状态, 从而导致网络中产生环路。

环路保护功能会抑制这种环路的产生。对于启用了环路保护的端口, 当没有接收到上游交换机发送的BPDU报文, 引起STP重新计算时, 不论其端口角色如何, 该端口将一直被设置为阻塞状态。

#### > 根桥保护:

在设计网络拓扑时, CIST的根桥和备份根桥大多处于一个高带宽的核心域内。但是, 当维护人员错误配置或遭受到网络中的恶意攻击时, 网络中的合法根桥有可能会收到优先级更高的BPDU报文, 致使当前合法根桥失去了根桥的地位, 从而导致网络拓扑结构的错误变动。这种错误的变动, 使得原来应该通过高速链路的流量被牵引到低速链路上, 引起网络拥塞。

为了防止这种情况发生, MSTP提供根桥保护功能: 对于启用了根桥保护功能的端口, 他在所有实例上的端口角色只能为“指定端口”。当该端口收到优先级更高的BPDU时, 立刻将该端口的端口状态转化为“阻塞”状态, 不再转发报文(相当于将此端口相连的链路断开)。当在2倍的传输时延时间内没有收到更优的配置消息时, 端口会恢复原来的正常状态。

### ➤ TC保护

交换机收到TC-BPDU报文（网络拓扑发生变化的通知报文）后，会将本机的地址表项删除。当有人伪造TC-BPDU报文恶意攻击交换机时，交换机短时间内收到大量TC-BPDU报文，频繁的删除操作给交换机带来很大负担，给网络的稳定带来很大隐患。通过在交换机上启用TC保护功能，可以避免交换机频繁地删除地址表项。

启用TC保护功能后，交换机在“TC保护周期”内，收到TC-BPDU的最大数目为“TC保护阈值”处所设的数目，超过该数目后，交换机在该周期内不再进行地址表删除操作。这样就可以避免频繁地删除转发地址表项。

### ➤ BPDU保护

交换机上直接与PC或服务器相连的端口会被设置为“边缘端口”，以实现这些端口的快速迁移。当这些端口接收到BPDU报文时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑结构的变化。而这些端口一般情况下不会收到BPDU报文。如果有人用伪造的BPDU报文恶意攻击交换机，就会引起网络拓扑的震荡。

MSTP提供BPDU保护功能来防止这种攻击：启用了BPDU保护功能后，如果边缘端口收到了BPDU报文，MSTP就将这些端口关闭，同时通知网管这些端口被MSTP关闭，被关闭的端口只能由网络管理人员来恢复。

### ➤ BPDU过滤

BPDU过滤用来防止恶意的BPDU洪泛攻击。交换机收到恶意的BPDU报文以后，会向网络中的其它交换机转发，致使网络内的交换机不停的进行STP计算，从而导致交换机的CPU占用率过高或者BPDU报文的协议状态错误等。

启用了BPDU报文过滤功能的端口，将不再接收和转发任何BPDU报文，但是会向外发送自身的BPDU报文，从而防止交换机受到BPDU报文的攻击，保证STP计算的正确性。

在本页可以对交换机的各个端口配置上述几种保护功能，建议您对符合条件的端口启用相应的保护功能。

**进入页面的方法：**生成树>>安全配置>>端口保护

端口保护

端口

选择	端口	环路保护	根桥保护	TC保护	BPDU保护	BPDU过滤	LAG
<input type="checkbox"/>		禁用	禁用	禁用	禁用	禁用	
<input type="checkbox"/>	1	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	2	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	3	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	4	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	5	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	6	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	7	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	8	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	9	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	10	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	11	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	12	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	13	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	14	禁用	禁用	禁用	禁用	禁用	---
<input type="checkbox"/>	15	禁用	禁用	禁用	禁用	禁用	---

图 7-10 端口保护

条目介绍:

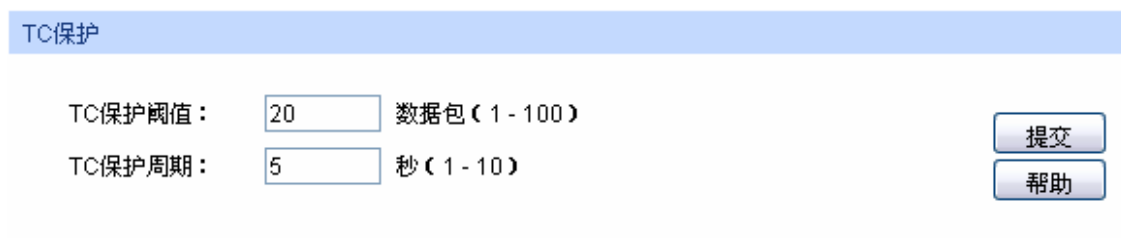
➤ 端口保护

- 端口选择:** 点击<选择>按键, 可根据所输端口号, 快速选择相应端口。
- 选择:** 勾选端口配置端口保护功能, 可多选。
- 端口:** 显示交换机的端口号。
- 环路保护:** 防止由于链路拥塞或者单向链路故障, 导致下游设备重新计算生成树, 由此产生的网络环路现象。
- 根桥保护:** 防止当前合法根桥失去根桥的地位而引起网络拓扑结构的错误变动。
- TC保护:** 防止由于恶意伪造的TC报文在STP协议网络中传播而导致桥设备的地址表不断清空所引起的网络吞吐量下降。
- BPDU保护:** 防止边缘端口受到恶意伪造的协议报文的攻击。
- BPDU过滤:** 防止STP协议网络中协议报文泛洪。
- LAG:** 显示端口当前所属的汇聚组。

## 7.4.2 TC保护

当端口保护页面开启端口的“TC保护”功能后，需要在本页对TC保护的TC保护阈值和TC保护周期进行配置。

进入页面的方法：生成树>>安全配置>>TC保护



TC保护			
TC保护阈值：	<input type="text" value="20"/>	数据包 (1 - 100)	<input type="button" value="提交"/>
TC保护周期：	<input type="text" value="5"/>	秒 (1 - 10)	<input type="button" value="帮助"/>

图 7-11 TC保护

条目介绍：

### ➤ TC保护

**TC保护阈值：**在TC保护周期内，交换机收到TC报文的最大数目。超过该数目后，交换机在该周期内不再进行地址表删除操作。默认为20数据包。

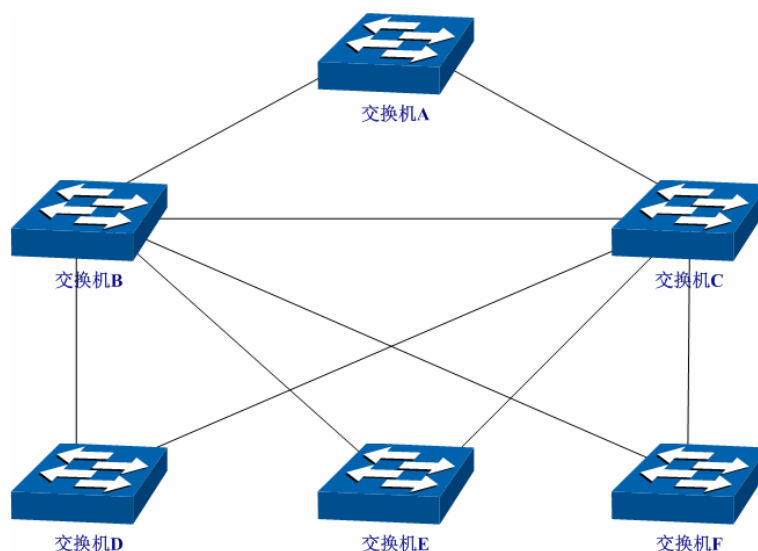
**TC保护周期：**填写TC保护的周期。默认为5秒。

## 7.5 STP功能的组网应用

### ➤ 组网需求

- 交换机A、B、C、D、E均支持MSTP功能；
- A为中心交换机；
- B、C为汇聚层交换机，D、E、F为接入层交换机；
- 整个网络中共有6个VLAN，为VLAN101-VLAN106；
- 所有设备运行MSTP，并且所有设备均属于同一个MST域；
- VLAN101、103和105的数据流量以B为根桥，VLAN102、104和106的数据流量以C为根桥。阻断网络中的环路，并能达到数据转发过程中VLAN数据的冗余备份以及负载分担效果。

## 组网图



## 配置步骤

### 配置交换机A:

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，配置相应端口类型为Tagged，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见 <a href="#">6.1 802.1Q VLAN</a> 。
2	启用生成树功能	在生成树>>基本配置>>基本配置页面，启用生成树功能，选择MSTP生成树模式。 在生成树>>基本配置>>端口配置页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在生成树>>MSTP实例>>域配置页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在生成树>>MSTP实例>>实例配置页面，配置VLAN-实例映射表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。

### 配置交换机B:

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，配置相应端口类型为Tagged，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见 <a href="#">6.1 802.1Q VLAN</a> 。
2	启用生成树功能。	在生成树>>基本配置>>基本配置页面，启用生成树功能，选择MSTP生成树模式。 在生成树>>基本配置>>端口配置页面，启用端口的MSTP功能。

步骤	操作	说明
3	配置MST域的域名和修订级别	在生成树>>MSTP实例>>域配置页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在生成树>>MSTP实例>>实例配置页面，配置VLAN-实例映射表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。
5	将交换机B配置为实例1的根桥	在生成树>>MSTP实例>>实例配置页面，将实例1的优先级设置为0。
6	将交换机B配置为实例2的指定桥	在生成树>>MSTP实例>>实例配置页面，将实例2优先级设置为4096。

- 配置交换机C:

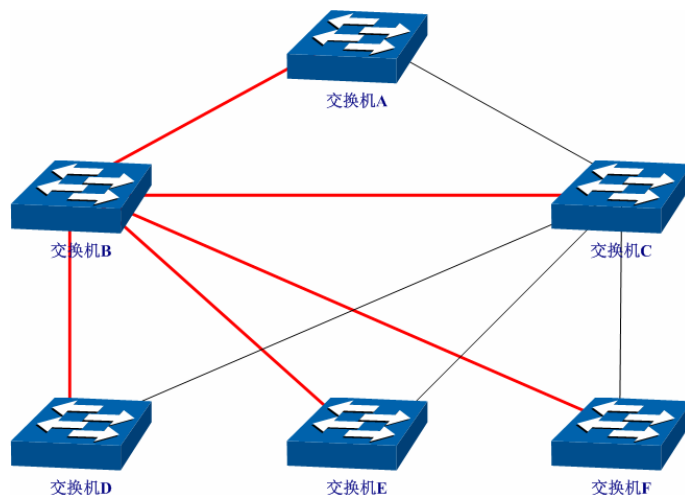
步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，配置相应端口类型为Tagged，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见 <a href="#">6.1 802.1Q VLAN</a> 。
2	启用生成树功能。	在生成树>>基本配置>>基本配置页面，启用生成树功能，选择MSTP生成树模式。 在生成树>>基本配置>>端口配置页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在生成树>>MSTP实例>>域配置页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在生成树>>MSTP实例>>实例配置页面，配置VLAN-实例映射表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。
5	将交换机C配置为实例1的指定桥	在生成树>>MSTP实例>>实例配置页面，将实例1的优先级设置为4096。
6	将交换机C配置为实例2的根桥	在生成树>>MSTP实例>>实例配置页面，将实例2优先级设置为0。

- 配置交换机D

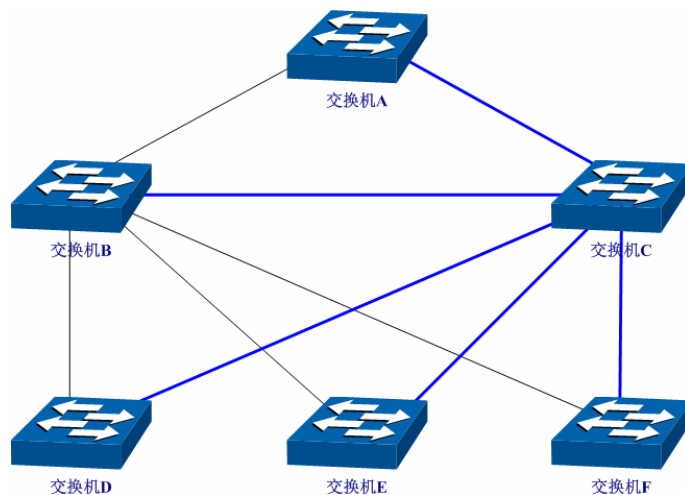
步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，配置相应端口类型为Tagged，并将端口加入VLAN 101到VLAN 106。具体配置方法请参见 <a href="#">6.1 802.1Q VLAN</a> 。

步骤	操作	说明
2	启用生成树功能。	在生成树>>基本配置>>基本配置页面，启用生成树功能，选择MSTP生成树模式。 在生成树>>基本配置>>端口配置页面，启用端口的MSTP功能。
3	配置MST域的域名和修订级别	在生成树>>MSTP实例>>域配置页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置MST域的VLAN-实例映射	在生成树>>MSTP实例>>实例配置页面，配置VLAN-实例映射表。将VLAN101、103和105映射到实例1，将VLAN102、104和106映射到实例2。

- 交换机E和交换机F的配置方法同交换机D
- 拓扑稳定以后两个实例所生成的动态拓扑结构
- 对于实例1（VLAN 101 103 105）而言，连通的链路为下图中红色的路径，灰色的路径断开。



- 对于实例2（VLAN 102 104 106）而言，连通的链路为下图中蓝色的路径，灰色的路径断开。



#### ➢ 配置建议

- 所有交换机的端口均建议启用“TC保护”功能。



- 根桥交换机的所有端口建议启用“根桥保护”功能。
- 非边缘端口建议启用“环路保护”功能。
- 连接PC与服务器的边缘端口，建议启用“BPDU保护”或“BPDU过滤”功能。

[回目录](#)

## 第8章 组播管理

### ➤ 组播概述

在网络中，存在着三种发送报文的方式：单播、广播、组播。数据采用单播（Unicast）方式传输时，服务器会为每一个接收者单独传输一份信息，如果有多个接收者存在，网络上就会重复地传输多份相同内容的信息，这样将会大量占用网络资源。数据采用广播（Broadcast）方式传输时，系统会把信息一次性的传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。

当前，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（multicast）应运而生，它实现了网络中单点到多点的高效数据传送，能够节约大量网络带宽，降低网络负载。组播传输信息的方式如图 8-1所示。

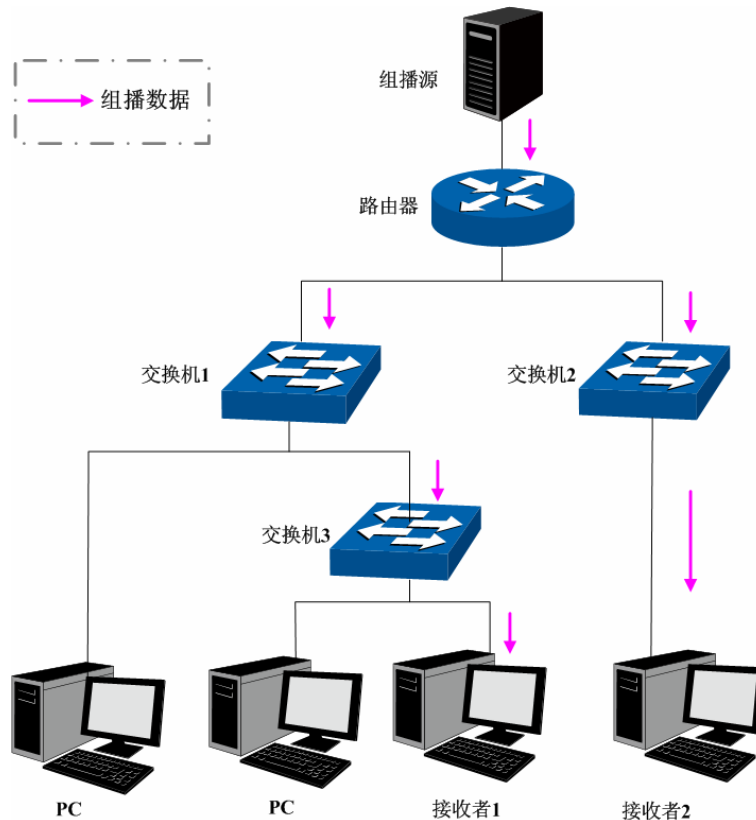


图 8-1 组播传输信息的方式

组播的特点是：

- 服务对象不固定，通常是一对多的关系；
- 把服务对象看成一个组，发送端只需要发送一次数据到相关网络设备即可；
- 每个用户可以随时加入或退出组播组；
- 实时性要求较高，允许一定的丢帧现象发生。

### ➤ 组播地址

组播IP地址：

根据IANA（Internet Assigned Numbers Authority，因特网编号授权委员会）规定，组播报文的IP地址使用D类IP地址，组播IP地址范围是224.0.0.0~239.255.255.255。其中，几个特殊组播IP地址段的范围及说明如下：

组播地址范围	说明
224.0.0.0~224.0.0.255	路由协议及其它底层拓扑发现和维护协议的保留地址
224.0.1.0~224.0.1.255	会议及电视会议
239.0.0.0~239.255.255.255	局域网内部使用地址，不能用于internet

表 8-1 特殊的组播IP地址段

组播MAC地址：

以太网传输单播IP报文的时候，目的MAC地址使用的是接收者的MAC地址。但是在传输组播报文时，传输目标不再是一个具体的接收者，而是一个成员不确定的组，所以需要使用组播MAC地址作为目的地址，组播MAC地址是一个逻辑的MAC地址。

IANA规定，组播MAC地址的高24bit位是以01-00-5E开头，低23bit为组播IP地址的低23bit，映射关系如图 8-2所示：

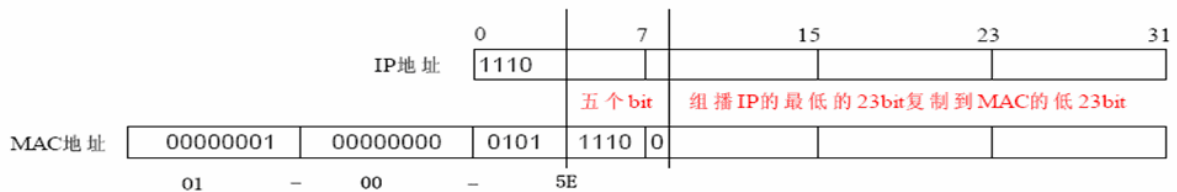


图 8-2 组播MAC地址和组播IP地址的对应关系

由于IP组播地址的高4bit是1110，标识了组播组，而低28bit中只有23bit被映射到组播MAC地址上，这样IP组播地址中就会有5bit没有使用，从而出现了32个IP组播地址映射到同一MAC地址上的结果。

### ➤ 组播地址表

交换机在转发组播数据时是根据组播地址表来进行的。由于组播数据不能跨越VLAN传输，因此组播地址表的第一部分是VLAN ID，当交换机收到组播数据包时，数据包只能在接收端口所在的VLAN内转发。组播地址表对应的出口端口不是一个，而是一组端口列表。转发数据时，交换机根据组播数据的目的组播地址查找组播地址表，如果在组播地址表中查不到相应的条目，则把该组播数据广播，即向接收端口所在VLAN内的所有端口上转发；如果能查找到对应的条目，则目的地址应该是一组端口列表，于是交换机把这个组播数据复制成多份，每份转发到一个端口，从而完成组播数据的交换。组播地址表一般格式如图 8-3所示。

VLAN ID	组播IP	端口
---------	------	----

图 8-3 组播地址表

## ➤ IGMP侦听

网络中的主机通过发送IGMP（Internet Group Management Protocol，互联网组管理协议）报文向临近的路由器申请加入（或离开）组播组，当上层路由设备将组播数据转发下来后，交换机负责将组播数据转发给主机。IGMP侦听（IGMP Snooping）是组播约束机制，交换机用它来完成组播组的动态注册，运行IGMP侦听的交换机通过侦听和分析主机与组播路由器之间交互的IGMP报文来管理和控制组播组，从而可以有效抑制组播数据在网络中扩散。

组播管理模块主要用于配置交换机的组播管理功能，包括IGMP侦听、组播地址表、组播过滤以及报文统计四个部分。

## 8.1 IGMP侦听

### ➤ IGMP侦听的工作过程

交换机侦听用户主机与路由器之间的交互IGMP报文，跟踪组播信息及其申请的端口。当交换机侦听到主机向路由器发出报告报文（IGMP Report）时，交换机便把该端口加入组播地址表中；当交换机侦听到主机发送的离开报文（IGMP Leave）时，路由器会发送该端口的特定组查询报文（Group-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若路由器收不到任何主机的回应，交换机便把该端口从组播地址表中删除。路由器会定时发查询报文（IGMP Query），交换机收到查询报文后，如果在一定的时间段内没有收到主机的报告报文，便把该端口从组播表中删除。

### ➤ IGMP报文

运行了IGMP侦听的交换机对不同类型的IGMP报文的处理方法如下。

#### 1. 查询报文（IGMP Query）。

由路由器发出，又可分为通用查询报文和特定组查询报文。路由器定时发出通用查询报文，以查询该网段有哪些组播组的成员。当路由器收到IGMP离开报文后，会通过接收端口向该组播组发送IGMP特定组查询报文，交换机会将此报文转发，以确定该端口中是否还有组播组的其它组成员。

对于通用查询报文，交换机会将此报文通过VLAN内除接收端口以外的其它端口转发，并对接收端口做出相应的处理：如果接收端口不是已有路由器端口，则将其加入路由器端口列表，并启用路由器端口时间；如果是已有路由器端口，则直接重置路由器端口时间。

对于特定组查询报文，交换机要向被查询的组播组的成员转发IGMP特定组查询报文。

#### 2. 报告报文（IGMP Report）。

由主机发出，当主机想主动加入某一组播组或对路由器查询报文给予响应时产生此种报文。

在收到IGMP报告报文时，交换机将此报文通过VLAN内的路由器端口转发出去，同时从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做相应的处理：如果接收端口是新成员端口，则将其加入到组播地址表中，并启用该端口的成员端口时间；如果接收端口是旧成员端口，则直接重置成员端口时间。

#### 3. 离开报文（IGMP Leave）。

运行IGMPv1的主机离开组播组时不会发送IGMP离开报文，因此交换机无法立即获知主机离开的信息。但是，由于主机离开组播组后不会再发送IGMP报告报文，因此当其对应的成员端口时间超时后，交换机就会将该端口从相应的组播地址表中删除。运行IGMPv2或IGMPv3的主机离开组播组时，会通过发送IGMP离开报文，以通知组播路由器自己离开了某个组播组。

当交换机从某一端口收到IGMP离开报文时，为了确认此端口下是否还有其它组成员存在，交换机向此端口转发特定组查询报文，然后重置成员端口时间为离开滞后时间，离开滞后时间超时后，交换机将此端口从相应的组播地址表中删除。如果删除离开端口后组播组中没有其它组成员存在，则将整个组播组删除。

### ➤ IGMP侦听的基本概念

#### 1. 相关端口

**路由器端口 (Router Port):** 交换机上连接路由组播设备的端口。

**成员端口 (Member Port):** 交换机上连接组播组成员的端口。

#### 2. 相关定时器

**路由器端口时间:** 这段时间内，如果交换机没从路由器端口接收到查询报文，就认为该路由器端口失效。默认是300秒。

**成员端口时间:** 这段时间内，如果交换机没从成员端口接收到报告报文，就认为该成员端口不再有主机属于多播组。默认是260秒。

**离开滞后时间:** 从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。默认是1秒。

本功能包括**基本配置**、**端口参数**、**VLAN参数**和**组播VLAN**四个配置页面。

## 8.1.1 基本配置

配置本交换机的IGMP侦听功能，首先要在本页配置IGMP侦听的全局功能和相关参数。

如果交换机收到的组播数据没有在组播地址表内，该组播数据会在VLAN内广播；当交换机启用“未知组播报文丢弃”功能后，交换机收到不在组播地址表中的组播数据报文时，会将此报文丢弃，从而节省带宽，并提高系统的处理效率，请根据实际情况配置该功能。

进入页面的方法：**组播管理>>IGMP侦听>>基本配置**

**基本配置**

IGMP侦听：  启用  禁用

未知组播报文：  通过  丢弃

IGMP侦听信息	
描述	成员
已启用的端口	2, 6, 10-12
已启用的VLAN	5, 8-9

#### 注意：

基本配置、端口参数、VLAN参数同时启用，IGMP侦听才能启用。

图 8-4 基本配置

条目介绍:

➤ 端口配置

**IGMP侦听:** 选择是否启用交换机的IGMP侦听功能。

**未知组播报文:** 选择交换机对未知组播报文的处理方法。

➤ IGMP侦听信息

**描述:** 显示IGMP侦听的配置项。

**成员:** 显示对应配置项的成员。

## 8.1.2 端口参数

本页用来配置交换机端口的IGMP侦听属性。

进入页面的方法: 组播管理>>IGMP侦听>>端口参数

选择	端口	IGMP侦听	快速离开功能	LAG
<input type="checkbox"/>		禁用	禁用	
<input type="checkbox"/>	1	禁用	禁用	---
<input type="checkbox"/>	2	启用	启用	---
<input type="checkbox"/>	3	禁用	禁用	---
<input type="checkbox"/>	4	禁用	禁用	---
<input type="checkbox"/>	5	禁用	禁用	---
<input type="checkbox"/>	6	启用	启用	---
<input type="checkbox"/>	7	禁用	禁用	---
<input type="checkbox"/>	8	禁用	禁用	---
<input type="checkbox"/>	9	禁用	禁用	---
<input type="checkbox"/>	10	启用	启用	---
<input type="checkbox"/>	11	启用	启用	---
<input type="checkbox"/>	12	启用	启用	---

图 8-5 端口参数

条目介绍:

➤ 端口配置

**端口选择:** 点击<选择>按键, 可根据所输端口号, 快速选择相应端口。

**选择:** 勾选条目配置端口的IGMP侦听功能, 可多选。

**端口:** 显示交换机的端口号。

**IGMP侦听:** 选择该端口是否启用IGMP侦听功能。

**快速离开功能:** 当端口启动快速离开功能后，交换机收到IGMP离开报文时，直接将该端口从组播组中删除。

**LAG:** 显示端口当前所属的汇聚组。



**注意:**

- 端口的快速离开功能只能在主机支持IGMPv2或v3时生效。
- 当快速离开功能与“未知组播报文丢弃”功能同时开启的情况下，如果某个端口下有多个用户，一个用户的快速离开，可能会造成同一组播组中其它用户的组播业务中断。

### 8.1.3 VLAN参数

IGMP侦听所建立的组播组是基于VLAN广播域的，不同的VLAN可以设置不同的IGMP参数。本页用于配置每个VLAN的IGMP侦听参数。

进入页面的方法：[组播管理](#)>>[IGMP侦听](#)>>[VLAN参数](#)

VLAN参数

VLAN ID:  ( 1-4094 )

路由器端口时间:  秒 ( 60-600, 推荐300秒 )

成员端口时间:  秒 ( 60-600, 推荐260秒 ) 添加

离开滞后时间:  秒 ( 1-30, 推荐1秒 )

静态路由端口:  (格式: 1-3,6,8)

VLAN列表

选择	VLAN ID	路由器端口时间	成员端口时间	离开滞后时间	VLAN ID <input type="text" value=""/> <span style="border: 1px solid #ccc; padding: 2px 5px;">选择</span>
<input type="checkbox"/>		<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>

提交
删除
帮助

**注意:**

当组播VLAN功能启用时，此处配置将失效。

图 8-6 VLAN参数

条目介绍:

➤ **VLAN参数**

**VLAN ID:** 填写启用IGMP侦听功能的VLAN ID。

**路由器端口时间:** 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。推荐300秒。

**成员端口时间:** 在所设时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口失效。推荐260秒。

**离开滞后时间:** 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐1秒。

**静态路由端口:** 配置静态路由端口，多用于拓扑稳定的网络中。

## ➤ VLAN列表

- VLAN ID选择:** 点击<选择>按键，可根据所输VLAN ID，快速查找VLAN条目。
- 选择:** 勾选条目配置VLAN参数，可多选。
- VLAN ID:** 显示VLAN ID。
- 路由器端口时间:** 显示VLAN的路由器端口时间。
- 成员端口时间:** 显示VLAN的成员端口时间。
- 离开滞后时间:** 显示VLAN的离开滞后时间。
- 路由器端口:** 显示VLAN的路由器端口。



### 注意:

- 当“组播VLAN”功能启用时，本页的配置将失效。

### 配置步骤:

步骤	操作	说明
1	启用IGMP侦听功能	必选操作。在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;基本配置、端口参数</b> 页面，启用交换机的IGMP侦听功能和端口的IGMP侦听功能。
2	配置VLAN的组播参数	可选操作。在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;VLAN参数</b> 页面，为交换机的各个VLAN配置组播参数。 没有配置组播参数的VLAN，表示没有在该VLAN内开启IGMP侦听功能，那么该VLAN中的组播数据会广播。

## 8.1.4 组播VLAN

对于传统的组播数据转发方式，当处于不同VLAN的用户加入同一个组播组时，组播路由器会为每个包含接收者的VLAN复制并转发一份组播数据。这样的组播点播方式，浪费了大量的带宽。

通过配置组播VLAN，可以有效的解决上述问题。将交换机的端口加入到组播VLAN中，使不同VLAN内的用户共用一个组播VLAN接收组播数据，组播数据只在组播VLAN内进行传输，从而节省了带宽。同时由于组播VLAN与普通的VLAN完全隔离，安全和带宽都得以保证。

配置组播VLAN之前，需要在**802.1Q VLAN**功能处预先配置一个VLAN作为组播VLAN，并将相应的端口加入此VLAN中。组播VLAN启用后，在**VLAN参数**页面中为其它VLAN配置的组播参数将失效，即组播数据不再通过除组播VLAN以外的其它VLAN转发。

**进入页面的方法:** 组播管理>>IGMP侦听>>组播VLAN



## 组播VLAN

组播VLAN： 启用  禁用

VLAN ID： (2-4094)

路由器端口时间： 秒 (60-600, 推荐300秒)

成员端口时间： 秒 (60-600, 推荐260秒)

离开滞后时间： 秒 (1-30, 推荐1秒)

静态路由端口： (格式: 1-3,6,8)

提交

帮助

## 注意：

- 1、创建了组播VLAN后，所有的IGMP报文都在组播VLAN内处理。
- 2、必须在VLAN配置页面完成端口的相关VLAN属性配置，组播VLAN才能正常运行。

图 8-7 组播VLAN

条目介绍：

➤ 组播VLAN

- 组播VLAN：** 选择是否启用组播VLAN。
- VLAN ID：** 填写组播VLAN的VLAN ID。
- 路由器端口时间：** 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。推荐300秒。
- 成员端口时间：** 在所设时间内，如果交换机没有从成员端口接收到报告报文，就认为该成员端口失效。推荐260秒。
- 离开滞后时间：** 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐1秒。
- 静态路由端口：** 配置静态路由器端口，多用于拓扑稳定的网络中。



## 注意：

- 路由器端口必须均在组播VLAN中，否则成员端口无法收到组播数据。
- 必须在802.1Q VLAN功能处完成端口的相关VLAN属性配置，组播VLAN才能正常运行。
- 组播VLAN中的路由器端口的端口类型必须配置为Tagged，否则组播VLAN内的所有的组播成员端口都无法接收到组播数据。
- 建立了组播VLAN后，所有的IGMP报文只在组播VLAN内处理。

配置步骤：

步骤	操作	说明
1	启用IGMP侦听功能	必选操作。在组播管理>>IGMP侦听>>基本配置、端口参数页面，启用交换机的IGMP侦听功能和端口的IGMP侦听功能。

步骤	操作	说明
2	创建组播VLAN	必选操作。在 <b>VLAN&gt;&gt;802.1Q VLAN</b> 功能处，创建组播VLAN，并将所有成员端口和路由器端口加入该VLAN中。 <ul style="list-style-type: none"> <li>配置成员端口的端口类型为Tagged。</li> </ul>
3	配置组播VLAN的参数	可选操作。进入 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;组播VLAN</b> 页面，启用组播VLAN并配置组播VLAN的组播参数。 时间参数建议使用默认值。
4	查看配置情况	若配置成功，则在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;基本配置</b> 页面中的“已启用的VLAN”条目处，显示组播VLAN的VLAN ID。

## 8.2 IGMP侦听功能组网应用

### ➤ 组网需求

组播源通过路由器转发组播数据，组播数据流通过交换机被转发到接收端用户A和用户B。

路由器：WAN口与组播源相连；LAN口与交换机相连，且通过VLAN3转发数据。

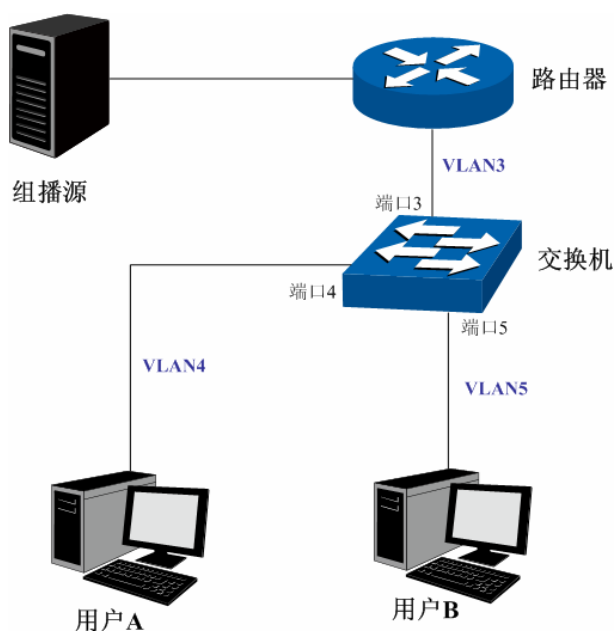
交换机：端口3与路由器相连，且通过VLAN3转发数据；端口4与用户A相连，且通过VLAN4转发数据；端口5与用户B相连，且通过VLAN5转发数据。

用户A：与交换机的端口4相连。

用户B：与交换机的端口5相连。

配置组播VLAN，使用户A和用户B通过组播VLAN接收组播数据。

### ➤ 组网图



## ➤ 配置步骤

配置交换机：

步骤	操作	说明
1	创建VLAN	在 <b>VLAN&gt;&gt;802.1Q VLAN</b> 功能处，创建VLAN3、4、5，并将VLAN3的名称填写为“组播VLAN”。
2	配置端口属性	在 <b>VLAN&gt;&gt;802.1Q VLAN</b> 功能处。 选择VLAN3，且配置端口3为Tagged、端口4为Untagged、端口5为Untagged。 选择VLAN4，且配置端口3为Tagged、端口4为Untagged。 选择VLAN5，且配置端口3为Tagged、端口5为Untagged。
3	启用IGMP侦听	在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;基本配置</b> 页面，启用IGMP侦听功能。 在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;端口配置</b> 页面，启用端口3、4、5的IGMP侦听功能。
4	启用组播VLAN	在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;组播VLAN</b> 页面，启用组播VLAN，并配置组播VLAN的VLAN ID为3，其它参数建议使用默认值。
5	检查组播VLAN	在 <b>组播管理&gt;&gt;IGMP侦听&gt;&gt;基本配置</b> 页面，“IGMP侦听信息”处，“已启用的端口”显示为3、4、5，“已启用的VLAN”显示为3。

## 8.3 组播地址表

在网络中，信息接收者可以加入各自所需的组播组，交换机在转发组播数据时是根据组播地址表来进行的。本功能包括**地址表显示**和**静态地址表**两个配置页面。

### 8.3.1 地址表显示

在本页可以查看到交换机中已存在的所有组播地址表信息。

进入页面的方法：**组播管理>>组播地址表>>地址表显示**

显示设置

组播IP:  (格式为: 225.0.0.1)

VLAN ID:  (1-4094)

端口:  ▼

地址类型:  全部  静态  动态

---

组播IP表

组播IP	VLAN ID	转发端口	地址类型
224.0.1.24	8	6	动态
235.80.68.83	8	6	动态
239.255.255.254	8	6	动态

---

当前组播IP总数: 3

图 8-8 地址表显示

条目介绍:

➤ 基本配置

- 组播IP:** 选择欲查找条目需包含的组播IP地址信息。
- VLAN ID:** 选择欲查找条目需包含的VLAN ID信息。
- 端口:** 选择欲查找条目需包含的端口号。
- 地址类型:** 选择欲查找条目需包含的地址类型信息。
- 全部: 显示全部组播地址表条目。
  - 静态: 显示静态组播地址表条目。
  - 动态: 显示动态组播地址表条目。

➤ 组播IP表

- 组播IP:** 显示组播IP地址。
- VLAN ID:** 显示组播组对应的VLAN ID。
- 转发端口:** 显示组播组的转发端口。
- 地址类型:** 显示组播IP的类型



**注意:**

- 若改变**VLAN参数**或**组播VLAN**页面中的参数,交换机组播地址表中的动态组播地址表项会受到影响。

### 8.3.2 静态地址表

静态组播地址表不是通过IGMP侦听学习到的,不受动态组播组及组播过滤的影响,对于某些固定的组播组,可以提高数据传输质量并增加安全性。

进入页面的方法：组播管理>>组播地址表>>静态地址表

新建条目

组播IP：（格式为：225.0.0.1）

VLAN ID：（1-4094）

转发端口：（格式为：1-3,6,8）

---

查找条目

查找选项：

---

静态组播IP表

选择	组播IP	VLAN ID	转发端口
<div style="display: flex; justify-content: center; gap: 20px;"> <input type="button" value="全选"/> <input type="button" value="删除"/> <input type="button" value="帮助"/> </div>			

---

当前静态组播IP总数：0

图 8-9 静态地址表

条目介绍：

➤ 新建条目

**组播IP：** 填写静态绑定的组播IP地址。

**VLAN ID：** 填写组播IP对应的VLAN ID。

**转发端口：** 填写组播IP的转发端口。

➤ 查找条目

**查找选项：** 选择静态组播IP表的显示规则，可以帮助您快速查找到所需的条目。

- 全部：显示全部静态组播IP表条目。
- 组播IP：设置欲查找条目需包含的组播IP地址信息。
- VLAN ID：设置欲查找条目需包含的VLAN ID信息。
- 端口ID：设置欲查找条目需包含的端口。

➤ 静态组播IP表

**选择：** 勾选条目进行删除，可多选。

**组播IP：** 显示绑定的组播IP地址。

**VLAN ID：** 显示组播组对应的VLAN ID。

**转发端口：** 显示组播组的转发端口。

## 8.4 组播过滤

在启用了IGMP侦听后，可以通过配置组播过滤，来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。

当用户申请加入某个组播组时，会发送IGMP报告报文，该报文到达交换机后，交换机首先检查接收端口上所配置的组播过滤规则，如果此端口可以加入这个组播组，则将这个端口加入到该组播组的地址表中；否则交换机就丢弃该IGMP报告报文，这样组播数据就不会转发到该端口，从而控制了用户加入组播组。

### 8.4.1 过滤地址

本页用来配置需要过滤的组播地址段。

进入页面的方法：[组播管理](#)>>[组播过滤](#)>>[过滤地址](#)

新建条目

过滤地址ID:  (1-30)

起始组播IP:  (格式为: 225.0.0.1)

结束组播IP:  (格式为: 225.0.0.1)

---

过滤地址表

	过滤地址ID	起始组播IP	结束组播IP
选择			
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>

---

当前过滤地址总数: 0

图 8-10 过滤地址

条目介绍:

#### > 新建条目

- 过滤地址ID:** 填写过滤地址ID号。
- 起始组播IP:** 填写过滤地址段的起始组播IP地址。
- 结束组播IP:** 填写过滤地址段的结束组播IP地址。

#### > 过滤地址表

- 过滤ID选择:** 点击<选择>按键，可根据所输过滤地址ID号，快速查找条目。
- 选择:** 勾选条目进行删除或修改过滤地址范围，可多选。
- 过滤地址ID:** 显示过滤地址ID号。
- 起始组播IP:** 显示过滤地址段的起始组播IP地址。

**结束组播IP:** 显示过滤地址段的结束组播IP地址。

## 8.4.2 端口过滤

本页用来配置端口的组播过滤规则，与“过滤地址”页面想结合，共同实现交换机的组播过滤功能。

进入页面的方法：**组播管理>>组播过滤>>端口过滤**

选择	端口	过滤	动作模式	绑定过滤地址 (ID)	最多加入组播组	LAG
<input type="checkbox"/>		禁用	允许			
<input type="checkbox"/>	1	禁用	允许	---	256	---
<input type="checkbox"/>	2	禁用	允许	---	256	---
<input type="checkbox"/>	3	禁用	允许	---	256	---
<input type="checkbox"/>	4	禁用	允许	---	256	---
<input type="checkbox"/>	5	禁用	允许	---	256	---
<input type="checkbox"/>	6	禁用	允许	---	256	---
<input type="checkbox"/>	7	禁用	允许	---	256	---
<input type="checkbox"/>	8	禁用	允许	---	256	---
<input type="checkbox"/>	9	禁用	允许	---	256	---
<input type="checkbox"/>	10	禁用	允许	---	256	---
<input type="checkbox"/>	11	禁用	允许	---	256	---
<input type="checkbox"/>	12	禁用	允许	---	256	---

### 注意：

- 1、此处的过滤设置对静态组播IP不生效。
- 2、一个端口最多只能绑定15个过滤地址ID，请使用如下的输入格式：1-3,5。
- 3、端口最多加入组播组是独立于端口过滤功能工作的。

图 8-11 端口过滤

条目介绍：

### ➤ 端口过滤配置

**端口选择:** 点击<选择>按键，可根据所输端口号，快速选择相应端口。

**选择:** 勾选条目配置端口的组播过滤功能，可多选。

**端口:** 显示交换机的端口号。

**过滤:** 选择是否启用端口组播过滤功能。

**动作模式:** 选择当组播地址属于过滤地址范围时，交换机对数据包的处理方式。

- 允许：只有组播地址属于过滤地址范围时，才处理组播报文。
- 拒绝：只处理组播地址不在过滤地址范围内的组播报文。

**绑定过滤地址:** 配置该端口需要绑定的过滤地址ID号。

**最多加入组播数:** 通过限制端口最多加入组播组数，来避免某些端口占据过多带宽。

**LAG:** 显示端口当前所属的汇聚组。

**注意:**

- 组播过滤功能只对启用了IGMP侦听的VLAN生效。
- 组播过滤功能对静态组播IP不生效。
- 一个端口最多只能绑定15个过滤地址。

配置步骤:

步骤	操作	说明
1	配置过滤地址段	必选操作。在 <b>组播管理&gt;&gt;组播过滤&gt;&gt;过滤地址</b> 页面，为过滤地址ID配置对应的过滤地址段。
2	配置端口的组播过滤规则	必选操作。在 <b>组播管理&gt;&gt;组播过滤&gt;&gt;端口过滤</b> 页面，配置端口的组播过滤规则。

## 8.5 报文统计

在本页可以查看交换机各端口的组播报文流量信息，便于监控网络中IGMP报文。

进入页面的方法：**组播管理>>报文统计**

**自动刷新**

自动刷新： 启用  禁用

刷新周期： 秒 (3-300) 提交

**IGMP报文统计**

端口  选择

端口	查询报文	报告报文(V1)	报告报文(V2)	报告报文(V3)	离开报文	错误报文
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0

刷新
清空
帮助

图 8-12 报文统计



条目介绍:

➤ 自动刷新

**自动刷新:** 选择是否启用自动刷新功能。

**刷新周期:** 填写自动刷新的时间周期。默认为5秒。

➤ IGMP报文统计

**端口选择:** 点击<选择>按键, 可根据所输端口号, 快速选择相应端口。

**端口:** 显示交换机的端口号。

**查询报文数:** 显示端口接收到的查询报文的数目。

**报告报文(V1):** 显示端口接收到的IGMPv1报告报文的数目。

**报告报文(V2):** 显示端口接收到的IGMPv2报告报文的数目。

**报告报文(V3):** 显示端口接收到的IGMPv3报告报文的数目。

**离开报文:** 显示端口接收到的离开报文的数目。

**错误报文:** 显示端口接收到的错误报文的数目。

[返回目录](#)

## 第9章 服务质量

服务质量模块主要用于流量控制管理和优先级配置，针对各种网络应用的不同需求，为其提供不同的服务质量，对带宽资源进行最优配置，从而提供更高质量的网络服务体验，包括**QoS配置**、**流量管理**以及**语音VLAN**三个部分。

### 9.1 QoS配置

QoS（Quality of Service，服务质量）功能用以提高网络传输的可靠性，并为您提供更高质量的网络服务体验。在传统的IP网络中，所有的报文都被无区别的等同对待，网络尽最大的努力（Best-Effort）发送报文，但对时延、可靠性等性能不能提供任何保证。伴随着网络技术、多媒体技术的飞速发展，IP网在现有的www，FTP，E-mail等服务的基础上，越来越多承载交互式多媒体通信业务如电视会议、远程教学、视频点播、可视电话等，而每种业务要求的传输时延、可变时延、吞吐量和丢包率都不同。因此，为用户各种业务提供不同的服务质量（QoS）成为Internet发展的重要挑战。

通常所说的QoS，是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。

#### ➤ QoS工作原理

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决定不同优先级队列的数据包被转发的方式，从而实现了QoS功能。

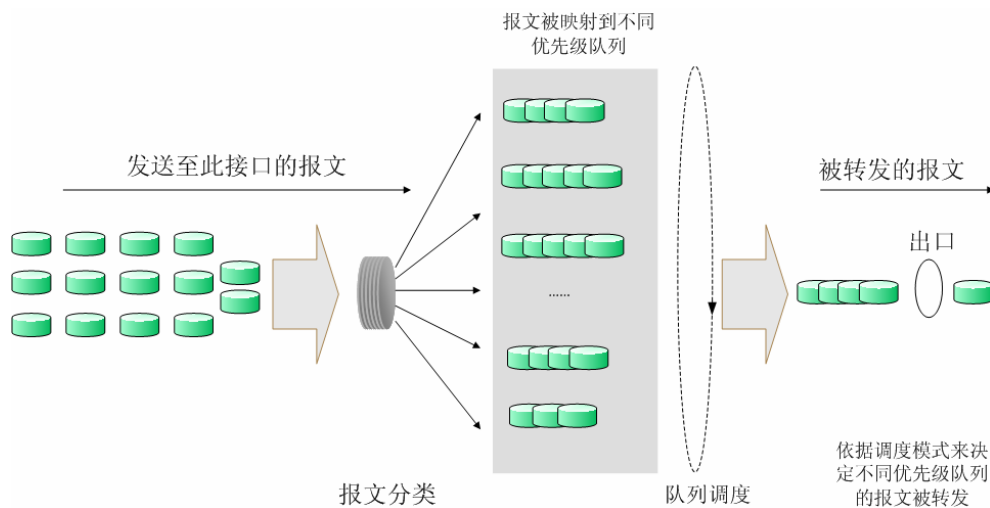


图 9-1 QoS工作原理

- **报文分类：**依据一定的匹配规则识别出对象。
- **映射：**用户可以根据优先级模式，将进入交换机的报文映射到不同的优先级队列中。本交换机提供三种优先级模式：基于端口的优先级、802.1P优先级和DSCP优先级。
- **队列调度：**当网络拥塞时，必须解决多种数据流同时竞争使用资源的问题，通常采用队列调度加以解决。本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR模式和无优先级模式（Equ）。

## ➤ 优先级模式

本交换机共有基于端口的优先级、IEEE 802.1P优先级和DSCP优先级三种模式。其中基于端口的优先级是默认被启用的，其它两种优先级模式可供选择。

### 1. 基于端口的优先级

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据优先级来确定数据流的出口队列。

### 2. 802.1P优先级

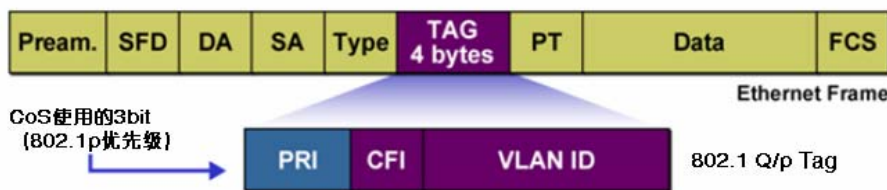


图 9-2 802.1Q的帧格式

如图所示，每一个802.1Q Tag中都有一个Pri域，该域由三个bit为组成，取值范围是0~7。802.1P优先级就是根据Pri的域值来决定数据帧的优先级。通过交换机的配置页面可配置不同的Pri域对应不同的优先级，交换机发送数据帧时，会根据数据帧的Tag决定发送的优先级。对于Untagged帧，交换机则按照该入口端口的默认优先级对数据帧进行QoS处理。

### 3. DSCP优先级

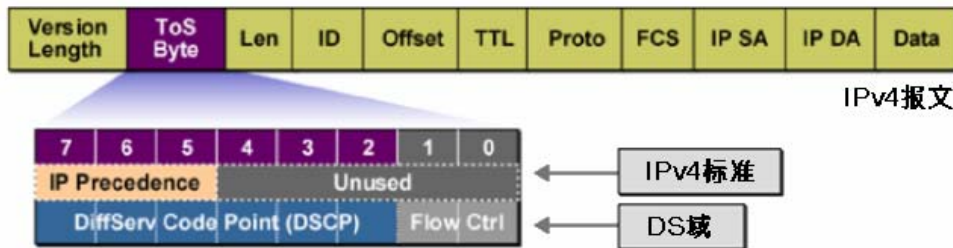


图 9-3 IP报文

如图所示，IP报文头部的ToS（Type of Service，服务类型）字段共有8bit，可以表征不同优先级特征的报文，前3个bit表示的是IP的优先级，取值范围是0~7。RFC2474重新定义了IP报文头部的ToS域，称之为DS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，取值范围为0~63，后2个bit（6、7bit）是保留位。通过交换机的配置页面，可以配置不同的DS字段对应不同的优先级，交换机发送IP包时，会根据IP包的DS域决定发送的优先级。对于非IP包，交换机则根据是否启用802.1P优先级以及数据帧是否带有Tag来决定采用哪种优先级模式。

#### ⚠ 注意:

- 当没有启用DSCP优先级时，交换机根据数据包是否带有802.1Q Tag确定使用哪种优先级模式。对于带有Tag的数据包，应用802.1P优先级；否则应用端口优先级。当启用DSCP优先级时，如果接收的数据包是IP包，则应用DSCP优先级；对于非IP包，如果数据帧带有Tag则应用802.1P优先级，否则应用端口优先级。

## ➤ 调度模式

在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。本交换机共实现了4个调度队列—TC0到TC3，其中TC0对应最低优先级的队列，TC3对应到最高优先级的队列。同时，本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR模式和无优先级模式（Equ）。

1. **SP-Mode: 严格优先级模式。** SP模式的调度算法是交换机优先转发当前优先级最高的数据帧，等最高优先级数据帧全部转发完后，再转发次高级优先级的数据帧。本交换机有4个出口队列，依次为TC0-TC3，在SP队列模式下他们的优先级依次升高，TC3有最高优先级。SP队列的缺点是，在拥塞发生时，如果较高优先级队列中长时间有报文存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

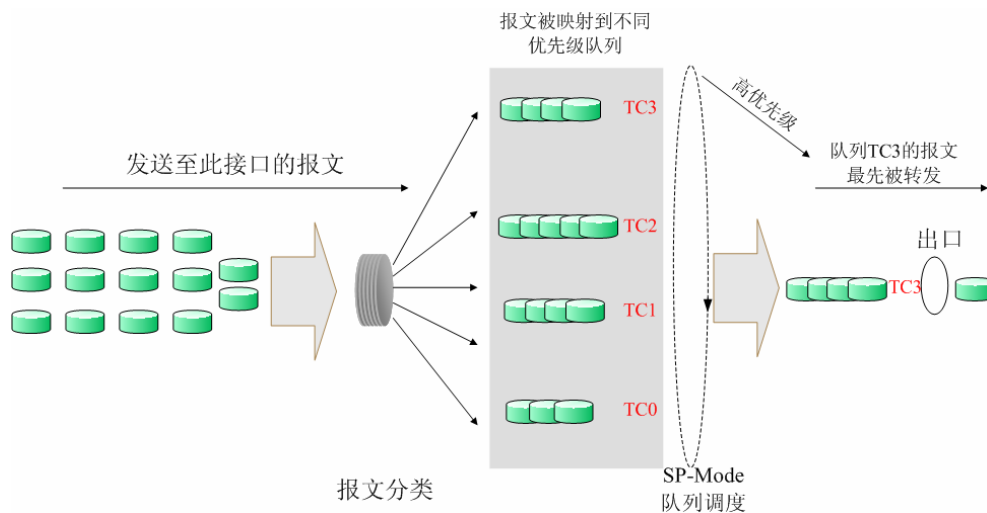


图 9-4 严格优先级模式

2. **WRR-Mode: WRR优先级模式。** WRR模式的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。WRR队列避免了采用SP调度时低优先级中的报文可能长时间得不到服务的缺点，并且虽然多个队列调度是轮询进行的，但是对每个队列不是固定的分配服务时间，如果队列为空则马上更换下一个队列调度，这样可以充分利用带宽资源。TC0-TC3的默认权重比是1:2:4:8。

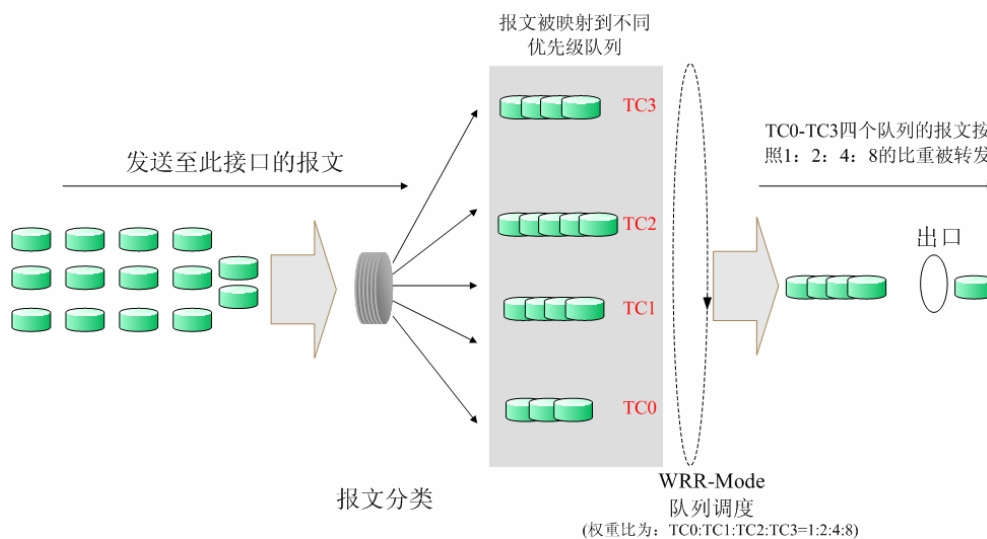


图 9-5 WRR优先级模式

3. **SP+WRR-Mode:** SP+WRR优先级模式，这种模式是前两种模式的混合。在这种模式下，交换机提供了两个调度组，分别是SP组和WRR组。其中SP组和WRR组之间遵循的是严格优先级调度规则，而WRR组内部队列遵循的是WRR调度模式。在该调度模式下TC3属于SP组；TC0、TC1、TC2属于WRR组，权重比是1: 2: 4。这样在调度的时候首先是TC3按照SP的调度模式独自占用带宽，然后是WRR组的成员TC0、TC1、TC2按照权重比1: 2: 4的比例占用带宽。
4. **Equ-Mode:** 无优先级模式。这种模式下所有队列公平的占用带宽，实际上这是WRR模式的一种特殊情况，所有的队列权重比是1:1:1:1。

本交换机实现了基于端口、基于802.1P和基于DSCP的三种优先级模式以及四个队列调度模式。端口优先级以CoS 0,CoS1...CoS 7表示。QoS配置功能包括端口配置、802.1P/CoS映射、DSCP映射和队列调度模式四个配置页面。TL-SG2452功能配置页面顺序略有不同，是端口配置、DSCP映射、802.1P/CoS映射和队列调度模式。

### 9.1.1 端口配置

在端口配置页面中，您可以进行基于端口优先级的配置。

进入页面的方法：**服务质量>>QoS配置>>端口配置**

TL-SL2428/TL-SL2452页面显示如下图所示：

端口优先级配置				
选择	端口	优先级	LAG	
<input type="checkbox"/>		TC 0		
<input type="checkbox"/>	1	TC 0	--	
<input type="checkbox"/>	2	TC 0	--	
<input type="checkbox"/>	3	TC 0	--	
<input type="checkbox"/>	4	TC 0	--	
<input type="checkbox"/>	5	TC 0	--	
<input type="checkbox"/>	6	TC 0	--	
<input type="checkbox"/>	7	TC 0	--	
<input type="checkbox"/>	8	TC 0	--	
<input type="checkbox"/>	9	TC 0	--	
<input type="checkbox"/>	10	TC 0	--	
<input type="checkbox"/>	11	TC 0	--	
<input type="checkbox"/>	12	TC 0	--	

#### 注意：

优先级等级TC0、TC1...TC3中，数字越大，表示优先级越高。

图 9-6 TL-SL2428/TL-SL2452 端口配置

条目介绍：

#### ➤ 端口优先级配置

**选择：** 勾选端口配置端口优先级，可多选。

**端口：** 显示交换机的物理端口。

**优先级：**配置端口的所属优先级等级。

**LAG：**显示当前端口所属的 LAG 组。



**注意：**

- 在此页面完成配置之后，需进入**队列调度模式**页面选择调度模式才能完成 QoS 功能的配置。

配置步骤：

步骤	操作	说明
1	进入页面	
2	选择端口进行配置	勾选所需端口，可多选。
3	选择端口的优先级	必选操作。可选择 TC 0-TC 3。
4	选择队列调度模式	必选操作。进入队列调度模式页面选择调度模式。

TL-SG2452页面显示如下图所示：

端口优先级配置			
选择	端口	优先级	LAG
<input type="checkbox"/>		CoS 0	
<input type="checkbox"/>	1	CoS 0	LAG1
<input type="checkbox"/>	2	CoS 0	LAG1
<input type="checkbox"/>	3	CoS 0	---
<input type="checkbox"/>	4	CoS 0	---
<input type="checkbox"/>	5	CoS 0	---
<input type="checkbox"/>	6	CoS 0	---
<input type="checkbox"/>	7	CoS 0	---
<input type="checkbox"/>	8	CoS 0	---
<input type="checkbox"/>	9	CoS 0	---
<input type="checkbox"/>	10	CoS 0	---
<input type="checkbox"/>	11	CoS 0	---
<input type="checkbox"/>	12	CoS 0	---

**注意：**

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据入端口的 CoS 值以及 802.1P/CoS 映射中 CoS 到 TC 之间的映射关系来确定数据流的出口队列。

图 9-7 TL-SG2452 端口配置

条目介绍：

➤ 端口优先级配置

**选择：**勾选端口配置端口优先级，可多选。

**端口：**显示交换机的物理端口。

**优先级：**配置端口的所属优先级等级。

**LAG：**显示当前端口所属的LAG组。

配置步骤：

步骤	操作	说明
1	选择端口的优先级	必选操作。在 <b>服务质量&gt;&gt;QoS配置&gt;&gt;端口配置</b> 页面设置各端口的优先级。
2	设置优先级与队列的映射关系	必选操作。在 <b>服务质量&gt;&gt;QoS配置&gt;&gt;802.1P/CoS映射</b> 页面的 <b>优先级等级</b> 表格中设置优先级与队列的映射关系。
3	选择调度模式	必选操作。进入 <b>服务质量&gt;&gt;QoS配置&gt;&gt;队列调度模式</b> 页面设置调度模式。

### 9.1.2 802.1P/CoS映射

在802.1P配置页面中，可以配置802.1P优先级。802.1P对802.1Q tag中的Pri字段进行了的定义，利用该字段可以将数据包划分为8个优先级。开启802.1P优先级后，交换机根据数据包是否带有802.1Q tag来确定所使用的优先级模式。对于带有tag的数据包，应用802.1P优先级；否则应用端口优先级。

进入页面的方法：**服务质量>>QoS配置>>802.1P/CoS映射**

802.1P优先级配置

802.1P优先级：  启用  禁用 提交

tag与CoS到出口队列映射配置

Tag-id/CoS-id:  队列TC-id:

Tag-id/CoS-id	队列TC-id	Tag-id/CoS-id	队列TC-id
0	TC1	1	TC0
2	TC0	3	TC1
4	TC2	5	TC2
6	TC3	7	TC3

提交
帮助

**注意：**

队列TC-id TC0、TC1...TC3中，数字越大，表示优先级越高。

图 9-8 802.1P/CoS映射

条目介绍：

➤ **802.1P优先级配置**

**802.1P优先级：**选择是否启用802.1P优先级。

➤ **tag与CoS到出口队列映射配置**

**Tag-id/CoS-id:** IEEE802.1P 协议里规定的或者是服务类型中8个优先级等级。

**队列TC-id:** 对应不同等级的优先级出口队列。以TC0、TC1 ... TC3表示。

配置步骤:

步骤	操作	说明
1	设置优先级与队列的映射关系	必选操作。在 <b>服务质量&gt;&gt;QoS配置&gt;&gt;802.1P/CoS映射</b> 页面中的 <b>优先级等级</b> 表格中设置优先级与队列的映射关系。
2	选择调度模式	必选操作。进入 <b>服务质量&gt;&gt;QoS配置&gt;&gt;队列调度模式</b> 页面设置调度模式。

### 9.1.3 DSCP映射

在DSCP映射配置页面中，可以进行DSCP优先级的配置。DSCP（DiffServ Code Point，区分服务编码点）是IEEE对IP ToS字段的重定义，利用该字段可以将IP报文划分为64个优先级。开启DSCP优先级后，如果转发的数据包是IP报文，则交换机应用DSCP优先级；对于非IP报文，交换机则根据是否启用802.1P优先级以及数据帧是否带有tag来决定采用哪种优先级模式。

进入页面的方法：**服务质量>>QoS配置>>DSCP映射**

优先级配置

DSCP优先级：  启用  禁用 提交

优先级等级

DSCP：  优先级等级：

DSCP	优先级等级	DSCP	优先级等级
0	TC0	1	TC0
2	TC0	3	TC0
4	TC0	5	TC0
6	TC0	7	TC0
8	TC0	9	TC0
10	TC0	11	TC0
12	TC0	13	TC0
14	TC0	15	TC0
16	TC1	17	TC1
18	TC1	19	TC1

提交
帮助

**注意：**

优先级等级TC0、TC1...TC3中，数字越大，表示优先级越高。

图 9-9 DSCP映射



条目介绍:

➤ 优先级配置

**DSCP优先级:** 选择是否启用DSCP优先级。

➤ 优先级等级

**DSCP:** 根据IP包的DS域决定的优先级。优先级级别从0到63。

**优先级:** 对应不同等级的优先级队列。以TC0、TC1 ... TC3表示。

配置步骤:

步骤	操作	说明
1	设置DSCP优先级与CoS优先级的映射关系	必选操作。在 <b>服务质量&gt;&gt;QoS配置&gt;&gt;DSCP映射</b> 页面启用DSCP优先级，设置DSCP优先级与802.1P优先级的映射关系。
2	设置优先级与队列的映射关系	必选操作。在 <b>服务质量&gt;&gt;QoS配置&gt;&gt;802.1P/CoS映射</b> 页面的 <b>优先级等级</b> 表格中设置优先级与队列的映射关系。
3	选择调度模式	必选操作。进入 <b>服务质量&gt;&gt;QoS配置&gt;&gt;队列调度模式</b> 页面设置调度模式。

### 9.1.4 队列调度模式

在本页面可以进行交换机调度模式的选择。在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。交换机将根据设置的优先级队列和队列调度算法来控制报文的转发次序。本交换机以TC0,TC1...TC3表示不同的优先级队列。

进入页面的方法：**服务质量>>QoS配置>>队列调度模式**

图 9-10 队列调度模式

条目介绍:

➤ 调度模式配置

**SP-Mode:** 严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。

**WRR-Mode:** 加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。TC0到TC3的权重比值是1: 2: 4: 8。

**SP+WRR-Mode:**

SP+WRR模式，这种队列调度模式是SP和WRR模式的混合。在此模式下，交换机提供了SP和WRR两个调度组，其中SP组和WRR组之间遵循的是严格优先级调度规则，而WRR组内部队列遵循的是WRR调度模式。

在该调度模式下TC3属于SP组；TC0、TC1、TC2属于WRR组，权重比是1: 2: 4。调度时，首先TC3按照SP模式独自占用带宽，然后是WRR组的成员TC0~TC2按照1: 2: 4权重比共享带宽。

**Equ-Mode:**

无优先级模式。在此模式下所有队列公平的占用带宽，所有的队列权重比是1: 1: 1: 1。

## 9.2 流量管理

流量管理用于限制交换机端口的带宽和广播流量，保证网络正常有效的运行，包括**带宽控制**和**风暴抑制**两个配置页面。

### 9.2.1 带宽控制

带宽控制是通过设定端口可用带宽，来控制端口的输入/输出数据传输速率，从而合理地分配和利用网络带宽。

进入页面的方法：**服务质量>>流量管理>>带宽控制**

带宽控制				
			端口 <input type="text"/>	<input type="button" value="选择"/>
选择	端口	入口带宽(Kbps)	出口带宽(Kbps)	LAG
<input type="checkbox"/>		128 <input type="button" value="v"/>	1024 <input type="button" value="v"/>	
<input type="checkbox"/>	1	---	---	---
<input type="checkbox"/>	2	---	---	---
<input type="checkbox"/>	3	---	---	---
<input type="checkbox"/>	4	---	---	---
<input type="checkbox"/>	5	---	---	---
<input type="checkbox"/>	6	---	---	---
<input type="checkbox"/>	7	---	---	---
<input type="checkbox"/>	8	---	---	---
<input type="checkbox"/>	9	---	---	---
<input type="checkbox"/>	10	---	---	---
<input type="checkbox"/>	11	---	---	---
<input type="checkbox"/>	12	---	---	---

**注意:**

1. 同一个端口的入口带宽限制和风暴抑制不能同时开启。
2. 如果您选择“手动输入”来设置入口/出口速率，系统会自动设置为与您设置的入口/出口速率最相近的64Kbps的整数倍。

图 9-11 带宽控制

条目介绍:

➤ **带宽控制**

**端口选择:** 点击<选择>按键, 可根据所输端口号, 快速选中相应端口。

**选择:** 勾选端口以配置端口带宽, 可多选也可不选。

**入口带宽(bps):** 配置端口接收数据时的带宽, 可从下拉菜单中选择或者手动输入。若选择“手动输入”, 则系统会自动选择与**64Kbps**整数倍最近的值作为入口带宽。若选择“禁用”选项, 则该端口的入口带宽控制会被取消, 该端口的入口带宽将恢复为最大带宽。

**出口带宽(bps):** 配置端口转发数据时的带宽, 可从下拉菜单中选择或者手动输入。若选择“手动输入”, 则系统会自动选择与**64Kbps**整数倍最近的值作为出口带宽。若选择“禁用”选项, 则该端口的出口带宽控制会被取消, 该端口的出口带宽将恢复为最大带宽。

**LAG:** 显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时, 会自动选择所有该汇聚组成员, 以保证同一汇聚组中所有成员的端口风暴抑制参数一致。



**注意:**

- 若端口已启用广播风暴抑制, 再启用入口带宽限制将使其失效。
- 若在设置入口带宽或出口带宽时选择了手动输入, 则系统会自动选择与**64Kbps**整数倍最近的值作为出口带宽。例如: 输入**1023Kbps**作为出口带宽, 则系统会自动选择**1024Kbps**作为真正的出口带宽。
- 在一个或多个端口上启用出口带宽限制时, 建议将各端口的流量控制禁用, 以保证交换机的正常工作。

## 9.2.2 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯, 严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。风暴抑制是指用户可以限制端口上允许接收的广播流量大小, 当该类流量超过用户设置的阈值后, 系统将丢弃超出流量限制的广播帧, 防止广播风暴的发生, 从而保证网络的正常运行。

交换机可以对三种常见的广播帧(广播包、组播包、UL包)进行限制。

**进入页面的方法:** 服务质量>>流量管理>>风暴抑制

TL-SL2428/TL-SL2452页面显示如下图所示：

风暴抑制					
选择	端口	广播包抑制(bps)	组播包抑制(bps)	UL包抑制(bps)	LAG
<input type="checkbox"/>		128K	128K	128K	
<input type="checkbox"/>	1	--	--	--	--
<input type="checkbox"/>	2	--	--	--	--
<input type="checkbox"/>	3	--	--	--	--
<input type="checkbox"/>	4	--	--	--	--
<input type="checkbox"/>	5	--	--	--	--
<input type="checkbox"/>	6	--	--	--	--
<input type="checkbox"/>	7	--	--	--	--
<input type="checkbox"/>	8	--	--	--	--
<input type="checkbox"/>	9	--	--	--	--
<input type="checkbox"/>	10	--	--	--	--
<input type="checkbox"/>	11	--	--	--	--
<input type="checkbox"/>	12	--	--	--	--

**注意：**

风暴抑制和入口带宽限制不能同时开启。

图 9-12 TL-SL2428/TL-SL2452 风暴抑制

条目介绍：

➤ **风暴抑制**

**端口选择：**

点击<选择>按键，可根据所输端口号，快速选中相应端口。

**选择：**

勾选端口以配置风暴抑制参数，可多选也可不选。

**广播包抑制：**

对由普通广播引起的风暴进行抑制。配置广播包的最大接收速度，可选择 128K、256K、512K、1M、2M、4M、5M、10M、20M、40M、50M，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的广播包抑制。

**组播包抑制：**

对由组播引起的风暴进行抑制。配置组播包的最大接收速度，可选择 128K、256K、512K、1M、2M、4M、5M、10M、20M、40M、50M，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的组播包抑制。

**UL 包抑制：**

交换机对未学习到地址的单播包（UL 包）进行广播，对由此引起的风暴进行控制。配置 UL 包的最大接收速度，可选择 128K、256K、512K、1M、2M、4M、5M、10M、20M、40M、50M，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的 UL 包抑制。

**LAG:**

显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

TL-SG2452页面显示如下图所示：

选择	端口	广播包抑制	组播包抑制	UL包抑制	速率(bps)	LAG
<input type="checkbox"/>		<input type="text" value="禁用"/>	<input type="text" value="禁用"/>	<input type="text" value="禁用"/>	128K	
<input type="checkbox"/>	1	禁用	禁用	禁用	---	---
<input type="checkbox"/>	2	禁用	禁用	禁用	---	---
<input type="checkbox"/>	3	禁用	禁用	禁用	---	---
<input type="checkbox"/>	4	禁用	禁用	禁用	---	---
<input type="checkbox"/>	5	禁用	禁用	禁用	---	---
<input type="checkbox"/>	6	禁用	禁用	禁用	---	---
<input type="checkbox"/>	7	禁用	禁用	禁用	---	---
<input type="checkbox"/>	8	禁用	禁用	禁用	---	---
<input type="checkbox"/>	9	禁用	禁用	禁用	---	---
<input type="checkbox"/>	10	禁用	禁用	禁用	---	---
<input type="checkbox"/>	11	禁用	禁用	禁用	---	---
<input type="checkbox"/>	12	禁用	禁用	禁用	---	---

**注意:**

同一个端口，风暴抑制和入口带宽限制不能同时开启。

图 9-13 TL-SG2452风暴抑制

条目介绍：

➤ **风暴抑制**

**端口选择:**

点击<选择>按键，可根据所输端口号，快速选中相应端口。

**选择:**

勾选端口以配置风暴抑制参数，可多选也可不选。

**广播包抑制:**

对由普通广播引起的风暴进行抑制。启用广播包抑制功能后超出流量部分的广播包将被丢弃。选择“禁用”选项时将关闭相应端口的广播包抑制。

**组播包抑制:**

对由组播引起的风暴进行抑制。启用组播包抑制功能后超出流量部分的组播包将被丢弃。选择“禁用”选项时将关闭相应端口的组播包抑制。

**UL包抑制:**

交换机对未学习到地址的单播包（UL包）进行广播，对由此引起的风暴进行控制。启用UL包抑制功能后超出流量部分的UL包将被丢弃。选择“禁用”选项时将关闭相应端口的UL包抑制。

**速率(bps):**

配置所抑制的数据包的最大接受速度，单位为bps，可选择128K，256K，512K，1M，2M，4M，5M，10M，20M，40M，50M。

**LAG:**

显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

**注意:**

- 若端口已启用入口带宽限制，再启用广播风暴抑制将使其失效。

## 9.3 语音VLAN

语音VLAN是为语音数据流而专门划分的VLAN。通过划分语音VLAN可以使语音数据自动被划分到语音VLAN中进行传输，便于对语音流进行有针对性的QoS（Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

### ➤ 语音数据流识别方法

本交换机可以根据数据包中的源MAC地址字段来判断该数据流是否为语音数据流。源MAC地址符合系统设置的语音设备OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到语音VLAN中传输。

OUI（Organizationally Unique Identifier）是MAC地址的前24位（二进制），是IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符，从OUI地址可以判断出该设备是哪一个厂商的产品。下表是常见语音设备商家产品的OUI地址，已在本交换机中设置为缺省OUI地址，设定不同的掩码可以调节交换机对MAC地址匹配的深度。

序号	OUI地址	设备商家
1	00-01-E3-00-00-00	Siemens phone
2	00-03-6B-00-00-00	Cisco phone
3	00-04-0D-00-00-00	Avaya phone
4	00-60-B9-00-00-00	Philips/NEC phone
5	00-D0-1E-00-00-00	Pingtel phone
6	00-E0-75-00-00-00	Polycom phone
7	00-E0-BB-00-00-00	3com phone

表 9-1 本交换机中缺省OUI地址

### ➤ 端口的语音VLAN模式

端口的语音VLAN模式包括自动模式和手动模式，是指端口加入语音VLAN的方式。

**自动模式:** 系统利用IP电话上电时发出的协议报文（UNTAG报文），通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将自动把语音报文的输入端口加入语音VLAN，配置报文的优先级。在设备上可以设置语音VLAN的老化时间。如果在老化时间内，系统没有从输入端口收到任何语音报文，系统将把该端口从语音VLAN中删除。端口的添加/删除过程由系统自动实现。

**手动模式:** 需要手动把IP电话接入端口加入语音VLAN中，再通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将下发ACL规则、配置报文的优先级。

在实际应用中，端口模式的设置需要结合语音设备发出的报文形式和端口的链路类型来进行设置，具体请参考下表。

端口语音 VLAN模式	语音流类型	端口链路类型及处理方式
自动模式	TAG语音流	Untagged: 不支持。
		Tagged: 支持，但接入端口的缺省VLAN不能是语音VLAN。
	UNTAG语音流	Untagged: 支持。
		Tagged: 不支持。
手动模式	TAG语音流	Untagged: 不支持。
		Tagged: 支持，但接入端口的缺省VLAN不能是语音VLAN。
	UNTAG语音流	Untagged: 支持。
		Tagged: 不支持。

表 9-2 端口模式与语音数据流的处理关系

### ➤ 语音VLAN的安全模式

当启用了端口的语言VLAN后，可以通过配置其安全模式来过滤数据流。如果启用了安全模式，则该端口仅转发语音数据包，并丢弃源MAC地址与OUI地址不匹配的其它数据包。如果没有启用安全模式，则该端口转发所有数据包。

安全模式	数据包类型	处理方式
Enable	UNTAG数据包	当数据包的源MAC地址是可识别的OUI地址时，该数据包可以在语音VLAN中传输。否则，数据包将被丢弃。
	带语音VLAN TAG的数据包	
	带其他VLAN TAG的数据包	设备处理此类数据包的方式取决于该端口是否允许VLAN。此为独立的语音VLAN的安全模式。
Disable	UNTAG数据包	不检查数据包的源MAC地址，所有数据包都可以在语音VLAN中传输。
	带语音VLAN TAG的数据包	
	带其他VLAN TAG的数据包	设备处理此类数据包的方式取决于该端口是否允许VLAN。此为独立的语音VLAN的安全模式。

表 9-3 安全模式与数据包的处理关系



#### 注意:

- 除非有特殊需求，请不要在语音VLAN中同时传输语音和其它业务数据。

### 9.3.1 全局配置

在全局配置页面中，可以设置语音VLAN的全局参数，包括VLAN ID、老化时间等。

进入页面的方法：[服务质量](#)>>[语音VLAN](#)>>[全局配置](#)

全局配置

语音VLAN：  启用  禁用

VLAN ID：  ( 2 - 4094 )

老化时间：  分钟 ( 1 - 43200 , 默认1440 )

语音优先级：  ▼

图 9-14 语音VLAN全局配置

条目介绍：

➤ 全局配置

- 语音VLAN：** 选择是否启用语音VLAN功能。
- VLAN ID：** 输入该语音VLAN的VLAN ID。
- 老化时间：** 设置自动模式下的端口成员在OUI地址老化后的存活时间。
- 语音优先级：** 选择发送语音数据时端口的优先级。



说明：

- TL-SG2452的全局配置功能没有语音优先级选项。

### 9.3.2 端口配置

在启用语音VLAN功能之前，需要在端口配置页面中配置各端口的功能参数。

进入页面的方法：[服务质量](#)>>[语音VLAN](#)>>[端口配置](#)



端口配置					
选择	端口	成员模式	安全模式	成员状态	LAG
<input type="checkbox"/>		<input type="text" value="自动"/>	<input type="text" value="禁用"/>		
<input type="checkbox"/>	1	自动	禁用	退出	---
<input type="checkbox"/>	2	自动	禁用	退出	---
<input type="checkbox"/>	3	自动	禁用	退出	---
<input type="checkbox"/>	4	自动	禁用	退出	---
<input type="checkbox"/>	5	自动	禁用	退出	---
<input type="checkbox"/>	6	自动	禁用	退出	---
<input type="checkbox"/>	7	自动	禁用	退出	---
<input type="checkbox"/>	8	自动	禁用	退出	---
<input type="checkbox"/>	9	自动	禁用	退出	---
<input type="checkbox"/>	10	自动	禁用	退出	---
<input type="checkbox"/>	11	自动	禁用	退出	---
<input type="checkbox"/>	12	自动	禁用	退出	---
<input type="checkbox"/>	13	自动	禁用	退出	---
<input type="checkbox"/>	14	自动	禁用	退出	---

图 9-15 语音VLAN端口配置

**注意:**

- 若LAG组成员端口要启用语音VLAN功能，请保持端口的成员模式和端口模式一致。
- 当端口为语音VLAN的成员端口时，修改该端口的成员模式为“自动”，此端口首先会退出语音VLAN，直到收到语音数据时再自动加入语音VLAN。

## 条目介绍:

➤ **端口配置**

- 端口选择:** 点击<选择>按键，可根据所输端口号快速选择相应条目。
- 选择:** 勾选端口配置端口的语音VLAN参数，可多选。
- 端口:** 显示交换机的端口号。
- 成员模式:** 设置端口加入语音VLAN的方式，有手动和自动两种方式。
- 自动：交换机根据端口是否收到语音数据自动维护端口加入或退出语音VLAN。
  - 手动：请根据需要手动设置端口加入或退出语音VLAN。
- 安全模式:** 设置端口安全模式。
- 成员状态:** 显示端口当前在语音VLAN中的状态。
- LAG:** 显示端口当前所属的汇聚组。

### 9.3.3 OUI配置

本交换机支持新建OUI条目，将特殊语音设备的MAC地址添加到交换机支持的OUI信息中，并以此OUI地址判断数据是否是语音数据。当交换机接收到数据包时，将分析数据包并判断是否是语音数据，如果是语音数据则将该端口自动添加到语音VLAN中。

进入页面的方法：**服务质量>>语音VLAN>>OUI配置**

新建条目

OUI地址：（格式为：00-00-00-00-00-01）

OUI掩码：（默认为：FF-FF-FF-00-00-00） 添加

OUI描述：（1-16个字符）

OUI列表

选择	OUI地址	OUI掩码	OUI描述
<input type="checkbox"/>	00-01-e3-00-00-00	ff-ff-ff-00-00-00	Siemens Phone
<input type="checkbox"/>	00-03-6b-00-00-00	ff-ff-ff-00-00-00	Cisco Phone
<input type="checkbox"/>	00-04-0d-00-00-00	ff-ff-ff-00-00-00	Avaya Phone
<input type="checkbox"/>	00-60-b9-00-00-00	ff-ff-ff-00-00-00	Philips Phone
<input type="checkbox"/>	00-d0-1e-00-00-00	ff-ff-ff-00-00-00	Pingtel Phone
<input type="checkbox"/>	00-e0-75-00-00-00	ff-ff-ff-00-00-00	PolyCom Phone
<input type="checkbox"/>	00-e0-bb-00-00-00	ff-ff-ff-00-00-00	3Com Phone

全选
删除
帮助

图 9-16 语音VLAN OUI配置

条目介绍：

➤ **新建条目**

- OUI地址：**输入语音设备的OUI地址。
- OUI掩码：**输入OUI地址掩码，常见为FF-FF-FF-00-00-00。
- OUI描述：**对此OUI进行描述，以便区分不同VoIP设备。

➤ **OUI列表**

- 选择：**选择所需条目进行删除。
- OUI地址：**显示语音设备的OUI地址。
- OUI掩码：**显示语音设备的OUI地址掩码。
- OUI描述：**显示此OUI的描述信息。

语音VLAN配置步骤:

步骤	操作	说明
1	创建 VLAN 与设置端口类型	必选操作。在 <b>VLAN&gt;&gt;802.1Q VLAN&gt;&gt;VLAN配置</b> 页面中创建VLAN，然后选择此VLAN包含的端口及该端口的端口类型。
2	添加OUI地址	可选操作。在 <b>服务质量&gt;&gt;语音VLAN&gt;&gt;OUI配置</b> 页面中的查看交换机是否支持相应的OUI模板，若不支持请在此页面中添加。
3	使能端口语音VLAN特性	必选操作。在 <b>服务质量&gt;&gt;语音VLAN&gt;&gt;端口配置</b> 页面设置语音VLAN中各端口的功能参数。
4	使能语音VLAN	必选操作。在 <b>服务质量&gt;&gt;语音VLAN&gt;&gt;全局配置</b> 页面中使能语音VLAN功能，并设置全局参数。

[回目录](#)

## 第10章 访问控制

随着网络规模的扩大以及流量的增加，如何有效地控制网络安全和分配带宽已成为网络管理的重要内容。ACL（Access Control List，访问控制列表）功能，通过配置报文的匹配规则和处理方式来实现对数据包的过滤功能，从而有效防止非法用户对网络的访问。另外ACL功能也可以控制流量，节约网络资源。ACL功能对网络安全的控制提供了很大的方便。

在本交换机中，ACL功能可以对数据包的L2-L4层的协议字段进行匹配。通过配置policy可以对匹配了ACL规则的数据包进行处理。

### 10.1 ACL配置

在ACL功能中，一个ACL可以包括多个规则，而每个规则可以针对数据包中特定字段内容进行匹配。在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，交换机将对该报文执行第一次匹配的规则指定的动作，以此来提高交换机的效率。

ACL配置功能包括ACL列表、新建ACL、MAC ACL、标准IP ACL和扩展IP ACL五个配置页面。

#### 10.1.1 ACL列表

在ACL列表页面，可以查看交换机中当前已配置的ACL详细信息。

进入页面的方法：访问控制>>ACL配置>>ACL列表

ACL显示					
选择ACL:	ACL 2				
ACL类型:	MAC ACL		删除		
规则排序:	用户配置				

规则列表					
选择	序号	RuleID	源MAC地址	目的MAC地址	操作
<input type="checkbox"/>	1	1	00-19-66-80-54-36	--	编辑   查看   上移   下移

全选 删除 帮助

图 10-1 查看ACL列表

条目介绍：

► **ACL显示**

**选择ACL:** 选择已创建的ACL。

**ACL类型:** 显示该ACL的类型。

**规则排序:** 显示该ACL内部的规则如何排序。

## ➤ 规则列表

此处可以查看或编辑ACL内部的详细规则信息，点击条目的操作按钮可以对规则条目进行排序。

### 10.1.2 新建ACL

在新建ACL页面，可以创建ACL。

进入页面的方法：访问控制>>ACL配置>>新建ACL



图 10-2 创建ACL

条目介绍：

## ➤ 创建ACL

**ACL ID:** 配置ACL ID。

**规则排序:** 配置该ACL内部的规则如何排序。默认为用户配置。

用户配置：按照用户配置规则的先后顺序进行规则匹配。

### 10.1.3 MAC ACL

MAC ACL根据数据包的源MAC地址和目的MAC地址信息制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL配置>>MAC ACL



图 10-3 为MAC ACL添加规则

条目介绍:

➤ **MAC ACL**

- 访问控制列表ID:** 选择需要配置的ACL ID。
- 规则ID:** 填写规则ID。
- 安全操作:** 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。
- 允许: 转发数据包。
  - 丢弃: 丢弃数据包。
- 源MAC:** 填写规则包含的源MAC地址信息。
- 目的MAC:** 填写规则包含的目的MAC地址信息。
- 地址掩码:** 填写MAC地址掩码, 掩码置1表示严格匹配。

### 10.1.4 标准IP ACL

标准IP ACL可以根据数据包的IP地址信息制定匹配规则, 对数据包进行相应的分析处理。

进入页面的方法: 访问控制>>ACL配置>>标准IP ACL

标准IP ACL

访问控制列表ID: 标准IP访问控制列表

规则ID:

安全操作: 允许

源IP:  地址掩码:

目的IP:  地址掩码:

提交 帮助

图 10-4 为标准IP ACL添加规则

条目介绍:

➤ **标准IP ACL**

- 访问控制列表ID:** 选择需要配置的ACL ID。
- 规则ID:** 填写规则ID。
- 安全操作:** 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。
- 允许: 转发数据包。
  - 丢弃: 丢弃数据包。
- 源IP:** 填写规则包含的源IP地址信息。
- 目的IP:** 填写规则包含的目的IP地址信息。
- 地址掩码:** 填写IP地址掩码, 掩码置1表示严格匹配。

## 10.1.5 扩展IP ACL

扩展IP ACL可以根据报文的源IP地址信息、目的IP地址信息、IP承载的协议类型、协议的特性等信息来制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL配置>扩展IP ACL

图 10-5 为扩展IP ACL添加规则

条目介绍：

### ➤ 扩展IP ACL

- 访问控制列表ID：** 选择需要配置的ACL ID。
- 规则ID：** 填写规则ID。
- 安全操作：** 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。
- 允许：转发数据包。
  - 丢弃：丢弃数据包。
- 源IP：** 填写规则包含的源IP地址信息。
- 目的IP：** 填写规则包含的目的IP地址信息。
- 地址掩码：** 填写IP地址掩码，掩码置1表示严格匹配。
- IP协议：** 选择规则包含的IP协议信息。
- 源端口号：** 当IP协议选择TCP/UDP时，此处配置规则包含的TCP/UDP源端口号。
- 目的端口号：** 当IP协议选择TCP/UDP时，此处配置规则包含的TCP/UDP目的端口号。

## 10.2 Policy配置

Policy功能是将ACL规则和处理方式组合起来，组成一个访问控制策略，对符合相应ACL规则的数据包进行控制。

Policy配置功能包括Policy列表、新建Policy、配置Policy三个配置页面。

## 10.2.1 Policy列表

在Policy页面可以查看和编辑ACL规则的数据包处理方式，此动作是对匹配了相应ACL规则的数据包的处理方式。

进入页面的方法：访问控制>>Policy配置>Policy列表

选择	序号	ACL ID
<input type="checkbox"/>	1	2

图 10-6 查看Policy列表

条目介绍：

### > Policy显示

#### 选择Policy:

选择需要查看的policy名称。当需要删除相应的policy时，选择后点击删除按钮即可。

### > Action列表

#### 选择:

选择动作条目进行删除。

#### 序号:

显示动作条目的序号。

#### ACL ID:

显示此Policy中包含的ACL。

## 10.2.2 新建Policy

在此页面中可以创建Policy。

进入页面的方法：访问控制>>Policy配置>新建Policy

Policy名称:

图 10-7 创建Policy



条目介绍:

➤ **创建Policy**

**Policy名称:** 填写Policy的名称。

### 10.2.3 配置Policy

在此页面中，可以配置Policy对应的ACL规则以及包含的动作，此动作是对匹配了相应ACL规则的数据包的处理方式。

进入页面的方法：访问控制>>Policy配置>Policy设置

Policy设置:

选择Policy: 选择Policy名称

选择ACL: 选择ACL

提交 帮助

图 10-8 为Policy添加ACL并设置动作

条目介绍:

➤ **Policy设置**

**选择Policy:** 选择Policy的名称。

**选择ACL:** 选择ACL作为Policy作用的对象。

## 10.3 绑定配置

只有将Policy和端口/VLAN绑定，Policy才能生效；将Policy与端口/VLAN进行绑定后，端口和VLAN会对接收到的数据包根据Policy进行匹配处理。绑定配置功能将Policy应用到某个端口或者VLAN上。

绑定配置功能包括绑定列表、端口绑定、VLAN绑定三个配置页面。

### 10.3.1 绑定列表

在此页面中可以查看已进行端口/VLAN绑定的Policy条目。

进入页面的方法：访问控制>>绑定配置>>绑定列表



图 10-9 查看Policy与端口/VLAN绑定信息

条目介绍:

➤ 选择显示模式

**选择显示模式:** 请根据需要选择参考已绑定的条目类别。

➤ Policy绑定列表

**选择:** 选择绑定条目进行删除。

**序号:** 显示绑定条目的序号。

**Policy名称:** 显示绑定的Policy名称。

**绑定接口:** 显示与相应Policy绑定的端口号或VID。

**方向:** 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

### 10.3.2 端口绑定

在此页面中可以将Policy与端口进行绑定。

进入页面的方法: 访问控制>>绑定配置>>端口绑定



图 10-10 将Policy与端口进行绑定

条目介绍:

➤ 端口绑定配置

**Policy名称:** 选择需要绑定的Policy名称。

**端口:** 配置需要绑定的端口号。

➤ 端口绑定列表

- 序号:** 显示绑定条目的序号。
- Policy名称:** 显示绑定的Policy名称。
- 端口:** 显示与相应Policy绑定的端口号。
- 方向:** 显示绑定的方向。本交换机当前仅支持入口方向的过滤。



**说明:**

- 对于TL-SL2428/TL-SL2452，一个Policy可以绑定到多个端口；对于TL-SG2452，则一个Policy只能绑定到一个端口。

### 10.3.3 VLAN绑定

在此页面中可以将Policy与VLAN进行绑定。

进入页面的方法：访问控制>>绑定配置>VLAN绑定

VLAN绑定配置

Policy名称： 添加

VLAN ID： 帮助

VLAN绑定列表

序号	Policy名称	VLAN ID	方向

图 10-11 将Policy与VLAN进行绑定

条目介绍：

➤ VLAN绑定配置

- Policy名称:** 选择需要绑定的Policy名称。
- VLAN ID:** 填写需要绑定的已建立的VLAN ID。

➤ VLAN绑定列表

- 序号:** 显示绑定条目的序号。
- Policy名称:** 显示绑定的Policy名称。
- VLAN ID:** 显示与相应Policy绑定的VLAN ID。
- 方向:** 显示绑定的方向。本交换机当前仅支持入口方向的过滤。



**说明:**

- 对于TL-SL2428/TL-SL2452，一个Policy可以绑定到多个VLAN；对于TL-SG2452，则一个Policy只能绑定到一个VLAN。

配置步骤:

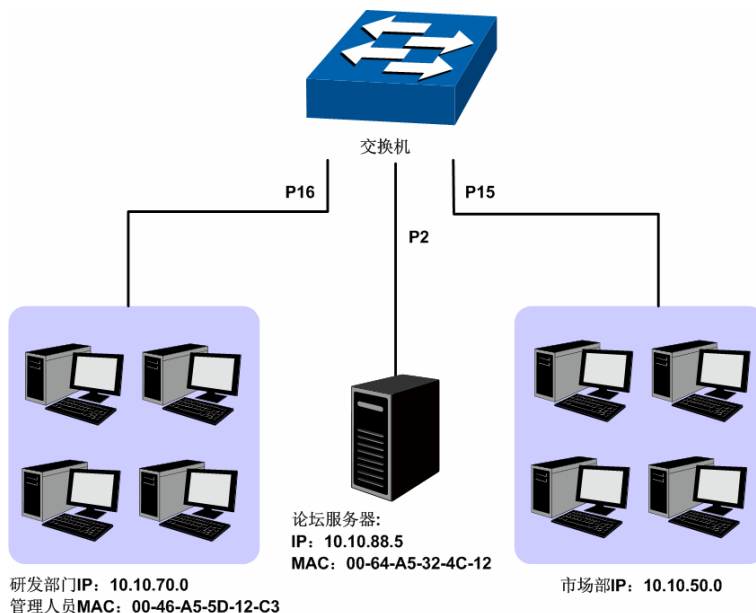
步骤	操作	说明
1	配置ACL规则	必选操作。在 <b>访问控制&gt;&gt;ACL配置</b> 的标签页中配置ACL规则对数据包进行匹配。
2	配置Policy	必选操作。在 <b>访问控制&gt;&gt;Policy配置</b> 的标签页中配置Policy,对匹配了相应ACL规则的数据包,可以通过Policy设置处理方式。
3	将Policy与端口/VLAN绑定	必选操作。在 <b>访问控制&gt;&gt;绑定配置</b> 的标签页中将Policy与端口/VLAN进行绑定,将Policy应用到相应的端口/VLAN上。

## 10.4 访问控制功能组网应用

### ➤ 组网需求

1. 研发部门的管理人员可以自由访问公司论坛, 管理人员MAC地址为00-46-A5-5D-12-C3。
2. 研发部门工作人员可以访问公司论坛。
3. 市场部人员不能访问公司论坛。
4. 市场部和研发部门之间互相不能访问。

### ➤ 组网图



➤ 配置步骤

步骤	操作	说明
1	需求1配置	<p>在访问控制&gt;&gt;ACL配置&gt;&gt;新建ACL页面，创建ACL 11。</p> <p>在访问控制&gt;&gt;ACL配置&gt;&gt;MAC ACL页面，选择ACL 11，创建规则1，安全操作设置为允许；勾选源MAC设置为00-46-A5-5D-12-C3，掩码为FF-FF-FF-FF-FF-FF。</p> <p>在访问控制&gt;&gt;Policy配置&gt;&gt;新建Policy页面，创建Policy，名称定为manager。</p> <p>在访问控制&gt;&gt;Policy配置&gt;&gt;配置Policy页面，将ACL 11应用到Policy manager。</p> <p>在访问控制&gt;&gt;绑定配置&gt;&gt;端口绑定页面，选择Policy manager与端口16绑定。</p>
2	需求2、4配置	<p>在访问控制&gt;&gt;ACL配置&gt;&gt;新建ACL页面，创建ACL 100。</p> <p>在访问控制&gt;&gt;ACL配置&gt;&gt;标准IP ACL页面，选择ACL 100，创建规则1，安全操作设置为丢弃；设置源IP为10.10.70.0，掩码为255.255.255.0；设置目的IP为10.10.50.0，掩码为255.255.255.0。</p> <p>在访问控制&gt;&gt;ACL配置&gt;&gt;标准IP ACL页面，选择ACL 100，创建规则2，安全操作设置为允许；设置源IP为10.10.70.0，掩码为255.255.255.0；设置目的IP为10.10.88.5，掩码为255.255.255.255。</p> <p>在访问控制&gt;&gt;Policy配置&gt;&gt;新建Policy页面，创建Policy，名称定为limit1。</p> <p>在访问控制&gt;&gt;Policy配置&gt;&gt;配置Policy页面，将ACL 100应用到Policy limit1。</p> <p>在访问控制&gt;&gt;绑定配置&gt;&gt;端口绑定页面，选择Policy limit1与端口16绑定。</p>
3	需求3、4配置	<p>在访问控制&gt;&gt;ACL配置&gt;&gt;新建ACL页面，创建ACL 101。</p> <p>在访问控制&gt;&gt;ACL配置&gt;&gt;标准IP ACL页面，选择ACL 101，创建规则3，安全操作设置为丢弃；设置源IP为10.10.50.0，掩码为255.255.255.0；设置目的IP为10.10.70.0，掩码为255.255.255.0。</p> <p>在访问控制&gt;&gt;ACL配置&gt;&gt;标准IP ACL页面，选择ACL 101，创建规则4，安全操作设置为丢弃；设置源IP为10.10.50.0，掩码为255.255.255.0；设置目的IP为10.10.88.5，掩码为255.255.255.255。</p> <p>在访问控制&gt;&gt;Policy配置&gt;&gt;新建Policy页面，创建Policy，名称定为limit2。</p> <p>在访问控制&gt;&gt;Policy配置&gt;&gt;配置Policy页面，将ACL 101应用到Policy limit2。</p> <p>在访问控制&gt;&gt;绑定配置&gt;&gt;端口绑定页面，选择Policy limit2与端口15绑定。</p>

[回目录](#)

# 第11章 SNMP

## ➤ SNMP概述

SNMP (Simple Network Management Protocol, 简单网络管理协议) 是目前UDP/IP网络中应用最为广泛的网络管理协议, 它提供了一个管理框架来监控和维护互联网设备。SNMP结构简单, 使用方便, 并且能够屏蔽不同设备的物理差异, 实现对不同设备的自动化管理, 所以得到了广泛的支持和应用, 目前大多数网络管理系统和平台都是基于SNMP的。

SNMP的最大优势就是设计简单, 他既不需要复杂的实现过程, 也不会占用太多的网络资源, 便于使用。SNMP的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时, SNMP可实现统计、配置和测试等功能; 当网络出故障时, 可实现各种错误检测和恢复功能。

## ➤ 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:** 运行在SNMP客户端程序的工作站, 提供了非常友好的人机交互页面, 方便网络管理员完成绝大多数的网络设备管理工作。

**SNMP代理:** 驻留在被管理设备上的一个进程, 负责接受、处理来自SNMP管理者的请求报文。在一些紧急情况下, SNMP代理也会通知SNMP管理者事件的变化。

**MIB库:** 被管理对象的集合。它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管理者、SNMP代理、MIB库三者的关系如图 11-1所示。

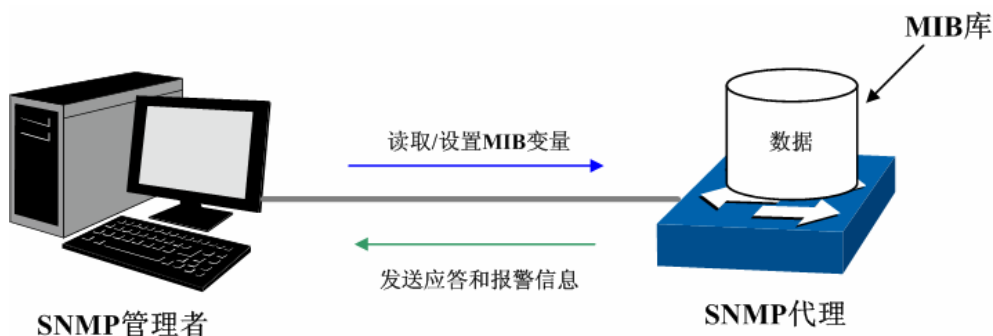


图 11-1 SNMP网元关系图

## ➤ SNMP的协议版本

本交换机提供了SNMPv3的管理功能, 同时兼容SNMPv1和SNMPv2c, SNMP管理者和SNMP代理的SNMP版本需要一致, 它们之间才能相互通信, 可以根据自己的应用需求, 选择不同安全级别的管理模式。

**SNMPv1:** 采用团体名 (Community Name) 认证。团体名用来定义SNMP管理者和SNMP代理的关系。如果SNMP报文携带的团体名没有得到设备的认可, 该报文将被丢弃。团体名起到了类似于密码的作用, 用来限制SNMP管理者对SNMP代理的访问。

**SNMPv2c:** 也采用团体名认证。它在兼容SNMPv1的同时又扩充了SNMPv1的功能。

**SNMPv3:** SNMPv3在前两个版本v1、v2c的基础上大大加强了安全性和用户可控制性，他采用了VACM（View-based Access Control Model，基于视图的访问控制模型）及USM（User-Based Security Model，基于用户的安全模型）的认证机制。用户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SNMP管理者和SNMP代理之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为SNMP管理者和SNMP代理之间的通信提供更高的安全性。

#### ➤ MIB库简介

MIB是以树状结构进行存储的。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别，被管理对象可以用一串数字唯一确定，这串数字是被管理对象的OID（Object Identifier，对象标识符）。MIB的结构如图 11-2所示。图中，B的OID为{1.2.1.1}，A的OID为{1.2.1.1.5}。

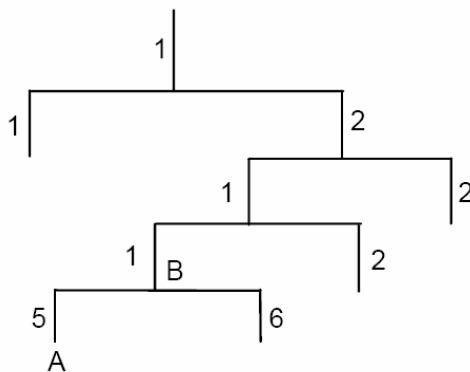


图 11-2 MIB树结构

#### ➤ SNMP配置概要

##### ● 创建视图

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类型（包括/排除），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。

##### ● 创建SNMP组

创建完视图之后，需要创建SNMP组，只有“组名”、“安全模式”、“安全级别”三项均相同的组，才被认为是同一个组。同时可以为各个SNMP组添加只读/只写/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。

##### ● 创建用户

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。

SNMP模块主要用于配置交换机的SNMP功能，包括SNMP配置、通知管理和RMON三个部分。

## 11.1 SNMP配置

在本功能处可以配置SNMP的各项基本功能，包括全局配置、视图管理、组管理、用户管理和团体管理五个配置页面。

### 11.1.1 全局配置

配置交换机的SNMP功能，首先需要在本页配置交换机SNMP的全局功能。

进入页面的方法：**SNMP>>SNMP配置>>全局配置**

全局配置

SNMP功能：  启用  禁用 提交

---

本地引擎配置

本地引擎ID：  (10-64个十六进制字符) 默认ID  
提交

---

远程引擎配置

远程引擎ID：  (0或10-64个十六进制字符) 提交  
帮助

**注意：**

引擎ID的字符个数必须为偶数。

图 11-3 全局配置

条目介绍：

➤ 全局配置

**SNMP功能：** 选择是否启用交换机的SNMP功能。

➤ 本地引擎配置

**本地引擎ID：** 填写本地SNMP实体的引擎ID。本地用户建立在本地引擎之下。

➤ 远程引擎配置

**远程引擎ID：** 填写SNMP管理端的引擎ID。请根据实际的SNMP管理端的引擎ID填写。远程用户建立在远程引擎之下。



**注意：**

- 引擎ID的字符个数必须为偶数。

### 11.1.2 视图管理

在SNMP报文中使用管理变量(OID)来描述交换机中的管理对象，MIB (Management Information Base, 管理信息库) 是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。本页用来配置SNMP的视图。



进入页面的方法：**SNMP>>SNMP配置>>视图管理**

新建视图

视图名称： (1-16个字符)

MIB子树OID： (1-61个字符) 添加

视图类型： 包括  排除

视图列表

选择	视图名称	类型	MIB子树OID
<input type="checkbox"/>	viewDefault	包括	1
<input type="checkbox"/>	viewDefault	排除	1.3.6.1.6.3.15
<input type="checkbox"/>	viewDefault	排除	1.3.6.1.6.3.16
<input type="checkbox"/>	viewDefault	排除	1.3.6.1.6.3.18

全选
删除
帮助

图 11-4 视图管理

条目介绍：

➤ **新建视图**

**视图名称：** 填写视图条目的名称。一个视图可以有多个同名的视图条目。

**MIB子树OID：** 填写该视图条目的管理变量（OID）。

**视图类型：** 选择OID的类型。

- 包括：该OID可以被管理软件管理。
- 排除：该OID不能被管理软件管理。

➤ **视图列表**

**选择：** 勾选条目进行删除。同一视图下的所有视图条目会被同时选择。

**视图名称：** 显示视图名称。

**类型：** 显示对应OID的类型。

**MIB子树OID：** 显示对应视图下的管理变量（OID）。

### 11.1.3 组管理

本页用来配置SNMP的组，组内的用户通过只读、只写、通知视图来达到访问控制的目的。

进入页面的方法：**SNMP>>SNMP配置>>组管理**

**组配置**

组名： (1-16个字符)

安全模式：

安全级别：

只读视图：

只写视图：

通知视图：

**组列表**

选择	组名	安全模式	安全级别	只读视图	只写视图	通知视图	操作
<input type="button" value="全选"/> <input type="button" value="删除"/> <input type="button" value="帮助"/>							

**注意：**

一个组必须具备一个只读视图，默认只读视图为viewDefault。

图 11-5 组管理

## 条目介绍：

➤ **组配置**

**组名：** 填写组名。与“安全模式”和“安全级别”三项共同组成该组的标识，三项均相同才被认为是同一组。

**安全模式：** 选择组的安全模式。

- v1: SNMP v1, 采用团体名 (Community Name) 认证, 也可以在**团体管理**页面直接进行配置。
- v2c: SNMP v2c, 采用团体名 (Community Name) 认证, 也可以在**团体管理**页面直接进行配置。
- v3: SNMP v3, 采用USM认证。

**安全级别：** 选择SNMP v3的组的安全级别。

**只读视图：** 选择只读视图，对所选的视图只能被查看不能被编辑。

**只写视图：** 选择只写视图，对所选的视图只能被编辑不能被查看。若您想要进行读写操作，则需要同时在“只读视图”中添加。

**通知视图：** 选择通知视图，管理软件可以接收到所选视图发送的异常警报信息。

➤ **组列表**

**选择：** 勾选条目进行删除，可多选。

**组名：** 显示SNMP组的组名。

**安全模式：** 显示组的安全模式。

**安全级别：** 显示组的安全级别。

**只读视图：** 显示组中具有只读权限的视图名称。

- 只写视图：** 显示组中具有只写权限的视图名称。
- 通知视图：** 显示组中具有通知权限的视图名称。
- 操作：** 点击对应条目的<编辑>按键，可以修改该条目的视图。修改完毕后点击<修改>按键，修改内容生效。



**注意：**

- 一个组必须具备一个只读视图，默认只读视图为viewDefault。

### 11.1.4 用户管理

SNMP管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。本页用来配置SNMP的用户。

进入页面的方法：**SNMP>>SNMP配置>>用户管理**

用户配置

用户名：	<input type="text"/>	( 1-16个字符 )			
用户类型：	<input type="text" value="本地用户"/>	组名：	<input type="text"/>		
安全模式：	<input type="text" value="v1"/>	安全级别：	<input type="text" value="不认证不加密"/>		
认证模式：	<input type="text" value="无"/>	认证密码：	<input type="text"/>	( 1-16个字符 )	
加密模式：	<input type="text" value="无"/>	加密密码：	<input type="text"/>	( 1-16个字符 )	

用户列表

选择	用户名	用户类型	组名	安全模式	安全级别	认证模式	加密模式	操作

**注意：**

用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

图 11-6 用户管理

条目介绍：

#### ➤ 用户配置

**用户名：** 填写用户名。

**用户类型：** 选择用户类型。

- 本地用户：建立在本地引擎下的用户。
- 远程用户：建立在远程引擎下的用户。

**组名：** 选择组名。通过“组名”、“安全模式”、“安全级别”来确定用户所属的组。

**安全模式：** 选择安全模式。

- 安全级别:** 选择安全级别。
- 认证模式:** 选择SNMP v3用户的认证模式。
- 无: 不认证。
  - MD5: 信息摘要算法。
  - SHA: 安全散列算法, 比MD5的安全性更高。
- 认证密码:** 输入认证密码。
- 加密模式:** 选择SNMP v3用户的加密模式。
- 无: 不加密。
  - DES: 数据加密标准。
- 加密密码:** 输入加密密码。
- **用户列表**
- 选择:** 勾选条目进行删除, 可多选。
- 用户名:** 显示用户名。
- 用户类型:** 显示用户类型。
- 组名:** 显示组名。
- 安全模式:** 显示安全模式。
- 安全级别:** 显示安全级别。
- 认证模式:** 显示认证模式。
- 加密模式:** 显示加密模式。
- 操作:** 点击对应条目的<编辑>按键, 可以修改该用户所属的组。修改完毕后点击<修改>按键, 修改内容生效。

**注意:**

- 用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

### 11.1.5 团体管理

SNMP v1和SNMP v2c采用团体名 (Community Name) 认证, 团体名起到了类似于密码的作用。若您使用的是SNMP v1和SNMP v2c, 配置完视图之后, 可以直接在本页配置SNMP的团体。

进入页面的方法: **SNMP>>SNMP配置>>团体管理**

团体配置

团体名： (1-16个字符)

权限：

MIB视图：

---

团体列表

选择	团体名	权限	MIB视图	操作
<div style="display: flex; justify-content: center; gap: 20px;"> <input type="button" value="全选"/> <input type="button" value="删除"/> <input type="button" value="帮助"/> </div>				

**注意：**

团体的默认MIB视图为viewDefault。

图 11-7 团体管理

条目介绍：

➤ 团体配置

**团体名：** 填写团体名。

**权限：** 选择该团体对视图的访问权限。

- 只读：团体对相应视图具有只读权限。
- 读写：团体对相应视图具有读写权限。

**MIB视图：** 选择团体可访问的视图。

➤ 团体列表

**选择：** 勾选条目进行删除，可多选。

**团体名：** 显示团体名。

**权限：** 显示团体对视图的访问权限。

**MIB视图：** 显示团体可访问的视图。

**操作：** 点击对应条目的<编辑>按键，可以修改该团体的访问视图及访问权限。修改完毕后点击<修改>按键，修改内容生效。

**注意：**

- 团体的默认MIB视图为viewDefault。

SNMP功能配置步骤:

- 若您使用SNMPv3版本

步骤	操作	说明
1	启用SNMP全局功能	必选操作。在 <b>SNMP&gt;&gt;SNMP配置&gt;&gt;全局配置</b> 页面，启用交换机的SNMP功能。
2	创建视图	可选操作。在 <b>SNMP&gt;&gt;SNMP配置&gt;&gt;视图管理</b> 页面，创建管理对象的视图。默认视图名为viewDefault，OID为1。
3	创建SNMP组	必选操作。在 <b>SNMP&gt;&gt;SNMP配置&gt;&gt;组管理</b> 页面，创建SNMPv3类型的组，并为组添加不同访问权限的视图。
4	创建SNMP组内的用户	必选操作。在 <b>SNMP&gt;&gt;SNMP配置&gt;&gt;用户管理</b> 页面，创建SNMPv3组内的用户，并配置用户的认证/加密模式及密码。

- 若您使用SNMPv1版本或SNMPv2c版本

步骤	操作		说明
1	启用SNMP全局功能。		必选操作。在 <b>SNMP&gt;&gt;SNMP配置&gt;&gt;全局配置</b> 页面，启用交换机的SNMP功能。
2	创建视图		可选操作。在 <b>SNMP&gt;&gt;SNMP配置&gt;&gt;视图管理</b> 页面，创建管理对象的视图。默认视图名为viewDefault，OID为1。
3	配置访问权限	直接设置 创建团体	二者必选其一。 <ul style="list-style-type: none"> <li>● 直接设置是在<b>SNMP&gt;&gt;SNMP配置&gt;&gt;团体管理</b>页面，以SNMPv1和v2c版本的团体名进行设置。</li> <li>● 间接设置采用与SNMPv3版本一致的命令形式，添加用户到v1/v2c类型的组，即相当于SNMPv1和SNMPv2c版本的团体名。在SNMP管理软件上用来登录交换机的团体名需要跟这里配置的用户名一致，该组下创建的v1/v2c用户（团体）的读、写视图与该组的读写视图对应。</li> </ul>
间接设置 创建SNMP组			
间接设置 创建SNMP组内的用户			

## 11.2 通知管理

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

通知报文分为以下两种：

**Trap:** 发送Trap报文通知SNMP管理者。

**Inform:** 发送Inform报文通知SNMP管理者，并且要求SNMP管理者返回信息。交换机发送Inform报文后，若经过超时时间仍没有收到Inform回应报文，则会重发Inform报文。超过重传次数后，将不再重复发送该Inform报文。Inform具有更高的可靠性，仅在SNMP v2c和SNMP v3可以使用。

本页用来配置SNMP的通知管理功能。

进入页面的方法：**SNMP>>通知管理>>通知管理**

新建条目

目的IP地址：	<input type="text"/>	UDP端口：	<input type="text" value="162"/>	
团体名/用户名：	<input type="text"/>			
安全模式：	<input type="text" value="v1"/>	安全级别：	<input type="text" value="不认证不加密"/>	<input type="button" value="添加"/>
通知类型：	<input type="text" value="Trap"/>			<input type="button" value="清空"/>
重传：	<input type="text"/>	( 1-255 )		
超时：	<input type="text"/>	秒 ( 1-3600 )		

目的主机列表

选择	目的IP地址	UDP端口	团体名/用户名	安全模型	安全级别	通知类型	超时	重传	操作
<input type="button" value="全选"/> <input type="button" value="删除"/> <input type="button" value="帮助"/>									

图 11-8 通知管理

条目介绍：

➤ **新建条目**

- 目的IP地址：** 填写管理主机的IP地址。
- UDP端口：** 填写管理主机上启用供通知过程使用的UDP端口，与IP地址共同作用。默认为162。
- 团体名/用户名：** 配置管理软件的团体名/用户名。
- 安全模式：** 选择用户的安全模式。
- 安全级别：** 配置SNMP v3的用户的的安全级别。
- 通知类型：** 选择使用的通知报文的类型。
- **Trap：** 以Trap方式发送通知。
  - **Inform：** 以Inform方式发送通知，Inform具有更高的可靠性。
- 重传：** 填写Inform报文的重传次数。交换机发送Inform报文后，若经过超时时间仍没有收到Inform回应报文，则会重发Inform报文。超过重传次数后，将不再重复发送Inform报文。默认为3。
- 超时：** 填写交换机等待Inform回应报文的时间。超过该时间后，将重新发送Inform报文。默认为100秒。

➤ **目的主机列表**

- 选择：** 勾选条目进行删除，可多选。
- 目的IP地址：** 显示管理主机的IP地址。
- UDP端口：** 显示管理主机上启用供通知过程使用的UDP端口。

<b>团体名/用户名:</b>	显示管理软件的团体名/用户名。
<b>安全模型:</b>	显示用户的安全模式。
<b>安全级别:</b>	显示SNMP v3的用户的的安全级别。
<b>通知类型:</b>	显示使用的通知报文的类型。
<b>超时:</b>	显示Inform报文的的重传次数。
<b>重传:</b>	显示收到Inform报文回应报文的超时时间。
<b>操作:</b>	点击对应条目的<编辑>按键，可以修改该通知条目的参数。修改完毕后点击<修改>按键，修改内容生效。

## 11.3 RMON

RMON（Remote Monitoring，远程网络监视）完全基于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，他使SNMP更为有效、更为积极主动地监控远程设备。利用RMON功能，网管可以快速跟踪网络、网段或设备出现的故障，积极采取防范措施，防止网络资源的失效，同时RMON MIB也可以记录网络性能和故障的数据，您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，使得网管可以简单而有效地管理大型网络。

### ➤ RMON的工作原理

RMON代理在RMON MIB中存储网络信息，交换机置入RMON代理后，具有了RMON探测的功能。管理者使用SNMP的基本命令与RMON代理交互数据信息，收集网络管理信息。但是由于设备资源的限制，管理者无法获取RMON MIB的全部数据，一般只可以收集到四个组的信息，这四个组是：历史组、事件组、统计组和警报组。

### ➤ RMON组

本交换机支持RMON 规范（RFC1757）中定义的历史组、事件组、统计组和警报组。

RMON组	功能	元素
历史组	周期性地收集网络统计信息，存储起来以便日后提取，从而有效的监测网络。	采样端口、采用间隔、创建者。
事件组	定义事件序号及事件的处理方式。此处定义的事件主要用在警报组中警报触发产生的事件。	事件描述、事件类型、创建者、用户名。
统计组	监测报警变量在指定端口的统计值。	丢弃数据包、丢弃字节、数据包发送、广播数据包、组播数据包、CRC错误帧、过小（或超大）的数据报文、冲突帧以及各种长度的数据包，包括64、65~127、128~255、256~511、512~1023以及1024~10240字节。



RMON组	功能	元素
警报组	定期对指定的警报变量进行监测，一旦计数器超过阈值则触发警报。	警报变量、样例类型、时间间隔、阈值上限、阈值下限、警报触发方式。

在本功能处可以配置RMON的各个组，包括**历史采样**、**事件配置**和**警报管理**三个配置页面。

### 11.3.1 历史采样

本页用来配置RMON的历史组。

进入页面的方法：**SNMP>>RMON>>历史采样**

历史采样控制					
选择	序号	采样端口	采样间隔(秒)	创建者	状态
<input type="checkbox"/>		端口1	<input type="text"/>	<input type="text"/>	禁用
<input type="checkbox"/>	1	端口1	1800	monitor	禁用
<input type="checkbox"/>	2	端口1	1800	monitor	禁用
<input type="checkbox"/>	3	端口1	1800	monitor	禁用
<input type="checkbox"/>	4	端口1	1800	monitor	禁用
<input type="checkbox"/>	5	端口1	1800	monitor	禁用
<input type="checkbox"/>	6	端口1	1800	monitor	禁用
<input type="checkbox"/>	7	端口1	1800	monitor	禁用
<input type="checkbox"/>	8	端口1	1800	monitor	禁用
<input type="checkbox"/>	9	端口1	1800	monitor	禁用
<input type="checkbox"/>	10	端口1	1800	monitor	禁用
<input type="checkbox"/>	11	端口1	1800	monitor	禁用
<input type="checkbox"/>	12	端口1	1800	monitor	禁用

图 11-9 历史采样

条目介绍：

#### ➤ 历史采样控制

- 选择：** 勾选条目配置采样属性。
- 序号：** 显示采样条目的序号。
- 采样端口：** 选择进行采样的端口。
- 采样间隔：** 填写端口采样的时间间隔。默认为1800秒。
- 创建者：** 填写创建该采样条目的实体。
- 状态：** 选择是否启用所选采样条目。

### 11.3.2 事件配置

本页用来配置RMON的事件组。

进入页面的方法：**SNMP>>RMON>>事件配置**

事件配置						
选择	序号	用户名	描述	类型	创建者	状态
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	无	<input type="text"/>	禁用
<input type="checkbox"/>	1	public		无	monitor	禁用
<input type="checkbox"/>	2	public		无	monitor	禁用
<input type="checkbox"/>	3	public		无	monitor	禁用
<input type="checkbox"/>	4	public		无	monitor	禁用
<input type="checkbox"/>	5	public		无	monitor	禁用
<input type="checkbox"/>	6	public		无	monitor	禁用
<input type="checkbox"/>	7	public		无	monitor	禁用
<input type="checkbox"/>	8	public		无	monitor	禁用
<input type="checkbox"/>	9	public		无	monitor	禁用
<input type="checkbox"/>	10	public		无	monitor	禁用
<input type="checkbox"/>	11	public		无	monitor	禁用
<input type="checkbox"/>	12	public		无	monitor	禁用

图 11-10 事件配置

条目介绍:

➤ 事件配置

- 选择:** 勾选条目配置事件属性。
- 序号:** 显示事件条目的序号。
- 用户名:** 填写事件所属的用户。当对应事件需要发送通知时，将会根据此用户名进行发送。
- 描述:** 填写该事件的描述信息。
- 类型:** 选择事件的类型。
- 无：不做任何操作。
  - 日志：将事件记录在交换机中，通过SNMP管理软件读取。
  - 通知：向管理主机发送报警消息。
  - 日志&通知：将事件记录在交换机中并向管理主机发送报警消息。
- 创建者:** 填写创建该事件条目的实体。
- 状态:** 选择是否启用所选事件条目。

### 11.3.3 警报管理

本页用来配置RMON的统计组和警报组。

进入页面的方法：**SNMP>>RMON>>警报管理**

警报配置												
选择	序号	计数器	端口	样例类型	上升阈值	上升事件	下降阈值	下降事件	启动警报	时间间隔(秒)	创建者	状态
<input type="checkbox"/>		DropEvents		绝对值					全部			禁用
<input type="checkbox"/>	1	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	2	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	3	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	4	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	5	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	6	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	7	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	8	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	9	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	10	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	11	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用
<input type="checkbox"/>	12	DropEvents	端口1	绝对值	100	1	100	1	全部	1800	monitor	禁用

图 11-11 警报配置

条目介绍:

#### ➤ 事件配置

- 选择:** 勾选条目配置警报属性。
- 序号:** 显示警报条目的序号。
- 计数器:** 选择警报变量。
- 端口:** 选择进行警报监视的端口号。
- 样例类型:** 为警报变量选择取样的方法，再将取样的值与阈值进行比较。
- 绝对值：在一个取样周期结束时将取样结果与阈值进行比较。
  - 增量：将现在值减去上一次取样值之后的增量与阈值进行比较。
- 上升阈值:** 填写触发警报的上升阈值。默认为100。
- 上升事件:** 选择触发上升阈值警报的事件的序号。
- 下降阈值:** 填写触发警报的下降阈值。默认为100。
- 下降事件:** 选择触发下降阈值警报的事件的序号。
- 启动警报:** 选择警报触发的方式。
- 上升：只在触发上升阈值后触发警报。
  - 下降：只在触发下降阈值后触发警报。
  - 全部：触发上升和下降阈值均触发警报。
- 时间间隔:** 填写警报的时间间隔。默认为1800秒。
- 创建者:** 填写创建该警报条目的实体。
- 状态:** 选择是否启用所选警报条目。



#### 注意:

- 当警报变量的采样值在同一方向上连续多次超过阈值时，只会在第一次产生警报事件。即上升警报和下降警报是交替产生的，出现了一次上升警报，则下一次必为下降警报。

[回目录](#)

## 第12章 系统维护

系统维护模块将管理交换机的常用系统工具组合在一起，为定位并排除交换机和网络故障提供便捷的方法。

- 1) 运行状态：对交换机内存和CPU进行监控。
- 2) 系统日志：通过系统日志查看在交换机上的配置参数并找出错误的配置。
- 3) 系统诊断：检测与交换机连接的线缆及对端设备的可用性。
- 4) 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。

### 12.1 运行状态

在本功能中可以通过曲线数据监控交换机CPU和内存的使用情况，CPU和内存使用率应该在一定数值上下波动。当CPU和内存使用率波动较大且明显增大时，请检查网络是否受到攻击。

本功能包括**CPU监控**和**内存监控**两个配置页面。

#### 12.1.1 CPU监控

进入页面的方法：系统维护>>运行状态>>CPU监控

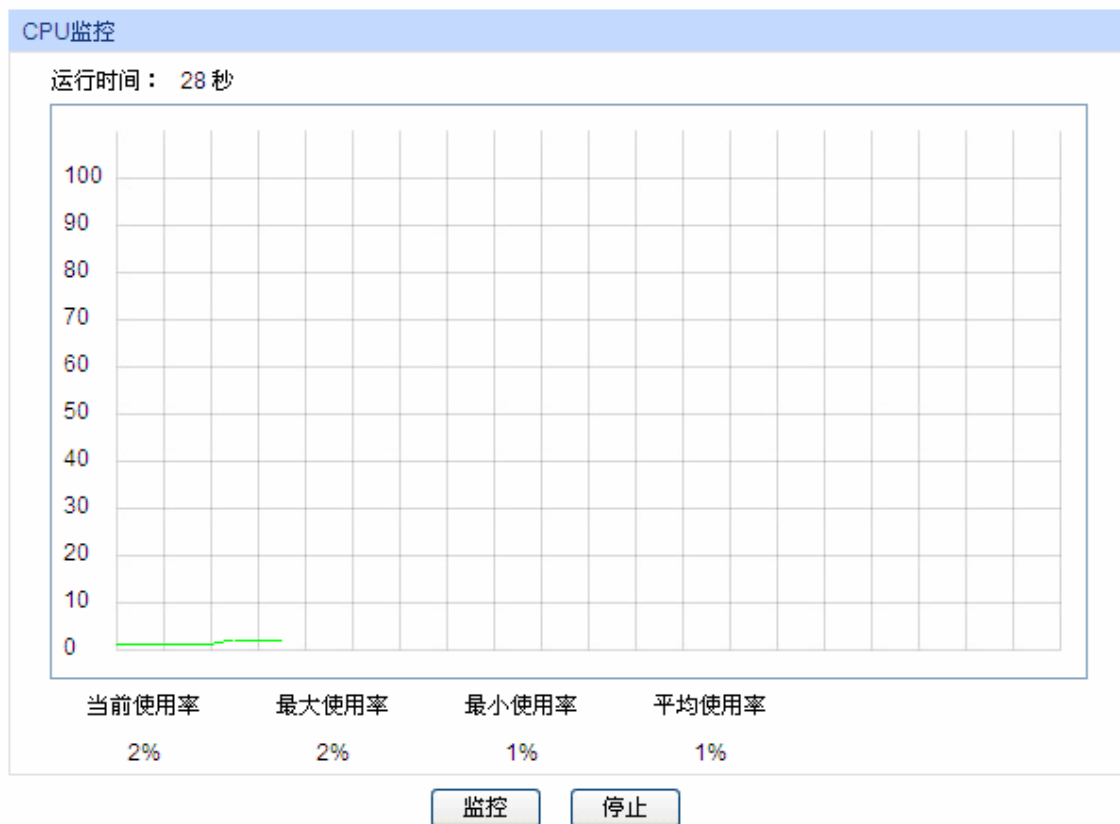


图 12-1 CPU监控

点击<监控>按键，图中会每隔4秒反馈一次监控数值，显示交换机CPU使用率。

## 12.1.2 内存监控

进入页面的方法：系统维护>>运行状态>>内存监控

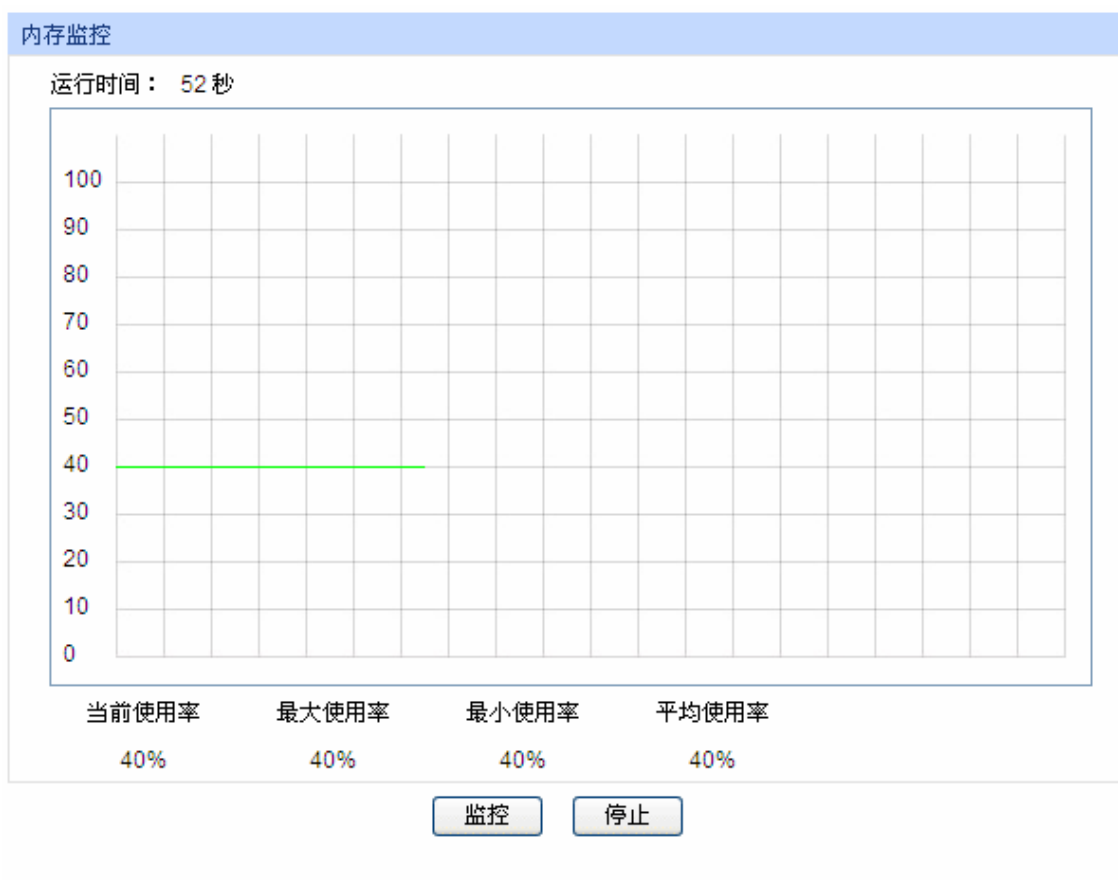


图 12-2 内存监控

点击<监控>按键，图中会每隔4秒反馈一次监控数值，显示交换机内存使用率。

## 12.2 系统日志

本交换机提供的日志系统能够对所有的系统信息进行记载、分类、管理，为网络管理员监控设备运行情况和诊断设备故障提供强有力的支持。

本交换机的系统日志分为八个等级，如表 12-1所示。

级别名称	等级	描述
emergencies	0	系统不可用信息
alerts	1	需要立刻做出反应的信息
critical	2	严重信息
errors	3	错误信息
warnings	4	警告信息
notifications	5	正常出现但是重要的信息
informational	6	需要记录的通知信息

级别名称	等级	描述
debugging	7	调试过程产生的信息

表 12-1 日志等级

本功能包括日志列表、本地日志、远程日志和日志导出四个功能页面。

## 12.2.1 日志列表

系统日志可以保存到两个不同的地方：日志缓冲区和日志文件。日志缓冲区的日志信息在交换机重启后将会丢失，日志文件里的日志信息在交换机重启后仍然有效。日志列表显示了日志缓冲区中的系统日志信息。

进入页面的方法：系统维护>>系统日志>>日志列表

系统日志列表				
序号	时间	模块名	严重级别	日志信息
		所有模块	所有级别	
1	2006-01-01 09:52:43	QoS	level_6	端口1取消出口带宽。 by admin on web (192.168.0.100).
2	2006-01-01 09:52:43	QoS	level_6	端口1设置入口带宽为120K。 by admin on web (192.168.0.100).
3	2006-01-01 09:49:53	FDB	level_6	交换机学习新地址 90:2b:34:63:59:68, vid:1, port:16. .
4	2006-01-01 09:49:39	Link	level_3	端口FastEthernet1/0/20, 状态变为DOWN. .
5	2006-01-01 09:49:38	Link	level_3	端口FastEthernet1/0/16, 状态变为UP. .
6	2006-01-01 09:28:16	User	level_5	禁用身份过滤。 by admin on web (192.168.0.101).
7	2006-01-01 08:41:38	FDB	level_6	交换机学习新地址 00:19:66:ca:8a:d9, vid:1, port:20. .
8	2006-01-01 08:29:40	FDB	level_6	交换机学习新地址 00:19:66:ca:8a:d9, vid:1, port:20. .
9	2006-01-01 08:00:17	FDB	level_6	交换机学习新地址 00:19:66:ca:8a:d9, vid:1, port:20. .
10	2006-01-01 08:00:14	Link	level_3	端口FastEthernet1/0/20, 状态变为UP. .
11	2006-01-01 08:00:12	Link	level_3	端口FastEthernet1/0/20, 状态变为DOWN. .
12	2006-01-01 08:00:02	SNMP	level_2	SNMP初始化成功. .
13	2006-01-01 08:00:01	Link	level_3	端口FastEthernet1/0/20, 状态变为UP. .
14	2006-01-01 08:00:00	System	level_6	系统IP地址变更为192.168.0.1.
15	2006-01-01 08:00:00	MSTP	level_6	MSTP模块在Port28上关闭STP功能. .
16	2006-01-01 08:00:00	MSTP	level_6	MSTP模块在Port27上关闭STP功能. .
17	2006-01-01 08:00:00	MSTP	level_6	MSTP模块在Port26上关闭STP功能. .
18	2006-01-01 08:00:00	MSTP	level_6	MSTP模块在Port25上关闭STP功能. .

刷新      帮助

### 注意：

- 1、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。
- 2、本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为512条。

图 12-3 日志列表

条目介绍：

### ➤ 系统日志列表

- 序号：** 显示该日志信息的序号。
- 时间：** 显示该日志信息的发生时间。需先在**系统管理>>系统配置>>系统时间**页面进行配置后，系统日志才能获取到正确的时间。
- 模块名：** 显示该日志信息所属功能模块，从下拉列表可选择显示某一模块的日志信息。

**严重级别：** 显示该日志信息的严重级别，从下拉列表选择某一级别，可显示小于或等于该级别值的日志信息。

**日志信息：** 显示该日志信息的内容。



**注意：**

- 严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。
- 本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为512条。

## 12.2.2 本地日志

本地日志是指保存在本交换机上的所有系统日志信息。在缺省情况下，所有的系统日志将保存到日志缓冲区，而等级为level\_0到level\_4的系统日志将同时保存到日志文件中。在此页面中可以对日志的存储区进行配置。

进入页面的方法：系统维护>>系统日志>>本地日志

本地日志配置			
选择	输出方向	严重级别	状态
<input type="checkbox"/>		<input type="text" value=""/>	<input type="text" value=""/>
<input type="checkbox"/>	日志缓冲区	level_7	启用
<input type="checkbox"/>	日志文件	level_4	启用

**注意：**

- 1、本地日志包括日志缓冲区和日志文件两个输出方向。
- 2、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。

图 12-4 本地日志

条目介绍：

➤ 系统日志列表

**选择：** 勾选相应的日志输出方向进行配置。

**日志缓冲区：** 日志列表页面上显示的即为缓冲区中的信息，在断电重启后这些信息将会丢失。

**日志文件：** 日志文件中的日志信息在断电重启后不会丢失，可通过导出日志文件来查看。

**严重级别：** 限定各个输出方向上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会进行输出。

**状态：** 启用/禁用该输出方向。

## 12.2.3 远程日志

远程日志功能可以将本交换机的系统日志发送到日志服务器上。日志服务器相当于一个可维护的共用消息区，它可以对网络中各设备产生的日志信息进行集中的监控和管理。

TP-LINK日志服务器提供了一个用于日志监视、存储和管理的窗口系统，并提供自动备份的功能。日志格式遵循RFC3164标准，TP-LINK日志服务器的安装过程及操作方法请登录我司官方网站<http://www.tp-link.com.cn>下载安装软件和操作指南。

进入页面的方法：**系统维护>>系统日志>>远程日志**

日志服务器					
选择	序号	服务器IP	UDP端口号	严重级别	状态
<input type="checkbox"/>		<input type="text"/>		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1	0.0.0.0	514	level_6	禁用
<input type="checkbox"/>	2	0.0.0.0	514	level_6	禁用
<input type="checkbox"/>	3	0.0.0.0	514	level_6	禁用
<input type="checkbox"/>	4	0.0.0.0	514	level_6	禁用

**注意：**

- 1、共支持4个日志服务器。
- 2、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。

图 12-5 日志服务器

条目介绍：

➤ **日志服务器**

- 选择：** 勾选相应的日志服务器进行配置。
- 序号：** 日志服务器序号。本交换机共支持4个日志服务器。
- 服务器IP：** 配置日志服务器的IP地址。
- UDP端口号：** 发送/接收系统日志时所用到的UDP端口号，这里使用标准的514端口。
- 严重级别：** 限定发往各个服务器上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会发送到相应的服务器。
- 状态：** 启用/禁用该服务器。

## 12.2.4 日志导出

日志导出功能可以将保存在交换机里的日志信息以文件的形式导出，作为设备诊断和统计分析之用。尤其在发生严重错误导致系统崩溃时，可在重启后导出日志信息，以获取相关的一些重要信息，为诊断设备提供支持。

进入页面的方法：**系统维护>>系统日志>>日志导出**



## 日志文件导出

点击此处按钮，可将日志文件导出，以作设备诊断和统计分析之用。

导出日志文件

帮助

**注意：**

导出日志文件可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 12-6 日志导出

条目介绍：

➤ 日志文件导出

**导出日志文件：** 点击此按钮导出日志文件中的日志信息。

## 12.3 系统诊断

本交换机提供了线缆检测和环回检测功能。

### 12.3.1 线缆检测

线缆检测功能能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

进入页面的方法：[系统维护](#)>>[系统诊断](#)>>[线缆检测](#)

线缆检测			
检测端口：	--		单位：米
线对	线路状态	线路长度	出错长度
线对A	--	--	--
线对B	--	--	--
线对C	--	--	--
线对D	--	--	--

**注意：**

- 1、对同一个端口前后两次诊断，请间隔3秒以上。
- 2、当电缆对端未连接时，诊断结果比较准确。
- 3、诊断结果可能存在误差，仅供参考。
- 4、如果端口为百兆口并且连接状态为正常，不能获取线缆的长度。

图 12-7 线缆检测

条目介绍：

➤ 线缆检测

**检测端口：** 选择要进行线缆检测的端口。

- 线对：**显示线对序号。
- 线路状态：**检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。
- 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。
  - 短路：线路金属内芯互相接触，导致短路。
  - 阻抗失配：网线质量问题。
- 线路长度：**若线路为正常状态，显示该线缆的长度范围。
- 出错长度：**若线路为短路、开路或阻抗失配状态，则显示该线缆的出错长度。

**注意：**

- 这里的长度是指线缆绕对的长度，不是线缆表皮长度，线缆检测的长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

### 12.3.2 环回检测

环回检测可以在不依赖外部设备的情况下检查端口是否可用，同时可以检测对端设备的可用性，有助于确定和解决网络故障，能够迅速方便地定位网络故障。本交换机的环回检测分为内环检测和外环检测。

- 1) 内环检测：无须借助外部设备，即可检测交换机端口是否正常。
- 2) 外环检测：可以检测与交换机相连的对端设备是否正常，同时插入自环头还可以检测交换机的自身性能。自环头的做法是用网线将一个水晶头的1/3、2/6、4/7、5/8管脚成对短接即可。

进入页面的方法：[系统维护](#)>>[系统诊断](#)>>环回检测

**检测类型**

检测类型： 内环  外环

**检测端口**

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12
<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18
<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28		

**检测结果**

测试端口:无
测试类型:无
测试结果:无

图 12-8 环回检测

条目介绍:

➤ 检测类型

**检测类型:** 选择要进行检测的类型。外环检测需要连接到外部设备或者自环头。

➤ 检测端口

**检测端口:** 勾选端口进行环回测试。

**检测:** 点击此按钮进行检测。

## 12.4 网络诊断

本交换机提供了Ping检测和Tracert检测功能。

### 12.4.1 Ping检测

Ping检测功能可以检测交换机与某网络设备是否可达，方便网络管理员检查网络的连通性，定位网络故障。

Ping检测过程如下:

- 1) 交换机向目标设备发送ICMP请求报文;
- 2) 如果网络工作正常，则目标设备在接收到该报文后，向交换机返回ICMP应答报文；显示相关统计信息；
- 3) 如果网络工作异常，源设备将显示目的地址不可达或超时等提示信息。

进入页面的方法：[系统维护](#)>>[网络诊断](#)>>[Ping检测](#)

Ping 检测	
目标IP地址：	<input type="text" value="192.168.0.1"/>
发送次数：	<input type="text" value="4"/> 次 (1-10)
发送报文长度：	<input type="text" value="64"/> 字节 (1-1024)
时间间隔：	<input type="text" value="100"/> 毫秒 (100-1000)
<input type="button" value="Ping"/> <input type="button" value="帮助"/>	

Ping 结果
Pinging 192.168.0.1 with 64 bytes of data :
Destination Host Unreachable!
Destination Host Unreachable!
Destination Host Unreachable!
Destination Host Unreachable!
Ping statistics for 192.168.0.1:
Packets: Sent = 4 , Received = 0 , Lost = 4 (100% loss)
Approximate round trip times in milli-seconds:
Minimum = 0ms , Maximum = 0ms , Average = 0ms

图 12-9 Ping检测

条目介绍:

➤ **Ping检测**

- 目标IP地址:** 填写需要测试的目标节点的IP地址。
- 发送次数:** 填写Ping检测时发送的检测包次数。建议使用缺省值。
- 发送报文长度:** 填写Ping检测时发送的检测包长度。建议使用缺省值。
- 时间间隔:** 发送ICMP 请求报文的时间间隔。

## 12.4.2 Tracert检测

Tracert检测可以查看交换机到目标节点所经过的路由器。当网络出现故障时，使用该命令可以分析出现故障的网络节点。

在IP数据包首部中包含一个TTL字段，当数据包在网络中转发时，每经过一个路由TTL字段的值减1。当接收的IP数据包的TTL字段为0或1时，路由器将此数据包丢弃，并给发送源回复一个ICMP超时报文。这样能有效防止数据包在网络发生故障时，无休止地在网络中流动。

Tracert检测过程如下:

- 1) 交换机发送一个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路由器）回应一个TTL超时的ICMP报文（该报文中含有第一跳的IP地址），这样交换机就得到了第一个路由器的地址;
- 3) 交换机重新发送一个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，这样交换机就得到了第二个路由器的地址;
- 5) 重复以上过程直到最终到达目的设备，交换机就得到了从它到目的设备所经过的所有路由器的地址。

进入页面的方法：[系统维护](#)>>[网络诊断](#)>>[Tracert检测](#)

Tracert 检测

目标IP:

最大跳数:  跳 (1-30)

Tracert 结果

图 12-10 Tracert检测

条目介绍:

➤ **Tracert检测**

- 目标IP:** 填写目的设备的IP地址。
- 最大跳数:** 填写测试报文发送的最大跳数。

[回目录](#)

## 附录A 术语表

[【 # A B C D E F G H I J L M N O P Q R S T U V W 】](#)

英文缩写	英文全称	中文全称
<b>A</b> <a href="#">回首页</a>		
AAA	Authentication, Authorization and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
-	Auto-Negotiation	自协商
<b>B</b> <a href="#">回首页</a>		
BOOTP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
-	Broadcast Storm	广播风暴
-	Broadcast	广播
-	Broadcast Domain	广播域
<b>C</b> <a href="#">回首页</a>		
CFI	Canonical Format Indicator	标准格式指示位
CHAP	Challenge Handshake Authentication Protocol	质询握手验证协议
CIST	Common and Internal Spanning Tree	公共和内部生成树
CMP	Cluster Management Protocol	集群管理协议
CRC	Cyclic Redundancy Check	循环冗余校验
CoS	Class of Service	服务等级
CSMA/CD	Carrier Sense Multiple Access/Collision Detect	载波侦听多路访问/冲突检测
CST	Common Spanning Tree	公共生成树
<b>D</b> <a href="#">回首页</a>		
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
-	DHCP Client	DHCP客户端
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务
DSCP	Differentiated Services Code Point	差分服务编码点
<b>E</b> <a href="#">回首页</a>		
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPOL	Extensible Authentication Protocol over LAN	局域网上的可扩展认证协议

英文缩写	英文全称	中文全称
EAPOR	EAP over RADIUS	承载于RADIUS协议的EAP
-	Ethernet	以太网
<b>F</b> <a href="#">回首页</a>		
FE	Fast Ethernet	快速以太网
FDB	Forward Data Base	地址表
-	Flow Control	流控
-	Frame	帧
FTP	File Transfer Protocol	文件传输协议
-	Full-Duplex	全双工
<b>G</b> <a href="#">回首页</a>		
GARP	General Attributes Registration Protocol	通用属性注册协议
GBIC	Giga Bitrate Interface Converter	千兆接口转换器
GE	Gigabit Ethernet	千兆以太网
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
<b>H</b> <a href="#">回首页</a>		
-	Half-Duplex	半双工
HTTP	Hyper Text Transport Protocol	超级文本传送协议
HTTPS	Secure Hyper Text Transfer Protocol	安全超文本传输协议
<b>I</b> <a href="#">回首页</a>		
IANA	Internet Assigned Numbers Authority	因特网编号授权委员会
ICMP	Internet Control Message Protocol	因特网控制报文协议
IEEE	Institute of Electrical and Electronics Engineers	电机工程师协会
IETF	Internet Engineering Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	互联网组管理协议
-	IGMP-Snooping	互联网组管理协议窥探
IP	Internet Protocol	互联网协议、网际协议
-	IP Address	IP地址
-	IP Multicast	IP组播
ISO	International Organization for Standardization	国际标准化组织
ISP	Internet service provider	因特网服务提供商
IST	Internal Spanning Tree	内部生成树
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	国际电信联盟-电信标准部
<b>J</b> <a href="#">回首页</a>		
-	Jumbo Frame	超长帧

英文缩写	英文全称	中文全称
<b>L</b> <a href="#">回首页</a>		
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元
LAG	Link Aggregated Group	链路聚合组
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
<b>M</b> <a href="#">回首页</a>		
MAC	Media Access Control	媒体访问控制
MAPT	Network Address Port Translation	网络地址端口转换
MIB	Management Information Base	管理信息库
MODEM	MOdulator-DEModulator	调制解调器
MSTI	Multi-Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议
MTU	Maximum Transmission Unit	最大传输单元
-	Multicast	组播
<b>N</b> <a href="#">回首页</a>		
NAPT	Network Address Port Translation	网络地址端口转换
NAT	Net Address Translation	网络地址转换
NDP	Neighbor Discovery Protocol	邻居发现协议
NMS	Network Management Station	网络管理站
NPDU	Network Protocol Data Unit	网络协议数据单元
NTDP	Neighbor Topology Discovery Protocol	邻居拓扑发现协议
NTP	Network Time Protocol	网络时间协议
-	NTP Server	网络时间服务器
<b>O</b> <a href="#">回首页</a>		
OID	Object Identifier	对象标识符
OSI	Open Systems Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
OUI	Organizationally Unique Identifier	全球统一标识符
<b>P</b> <a href="#">回首页</a>		
P2P	Point To Point	点到点
-	Packet	数据包
PAP	Password Authentication Protocol	密码认证协议

英文缩写	英文全称	中文全称
PCB	Printed Circuit Board	印制电路板
PDU	Protocol Data Unit	协议数据单元
PING	Packet Internet Groper	Internet包探测器
PoE	Power over Ethernet	以太网供电
-	Port	端口
PPP	Point-to-Point Protocol	点到点协议
PPTP	Point to Point Tunneling Protocol	点对点隧道协议
PQ	Priority Queuing	优先队列
<b>Q</b> <a href="#">回首页</a>		
QoS	Quality of Service	服务质量
-	Query	查询
<b>R</b> <a href="#">回首页</a>		
RADIUS	Remote Authentication Dial in User Service	远程认证拨号用户服务
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Monitoring	远程网络监视
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
-	Router	路由器
<b>S</b> <a href="#">回首页</a>		
-	Server	服务器
SFTP	Secure FTP	安全文件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SP	Strict Priority Queuing	严格优先级队列
SPF	Shortest Path First	最短路径优先
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	加密套接字协议层
STP	Spanning Tree Protocol	生成树协议
-	Switch	交换机
<b>T</b> <a href="#">回首页</a>		
TCP	Transmission Control Protocol	传输控制协议
-	Telnet	远程登录
TFTP	Trivial File Transfer Protocol	简单文件传输协议
ToS	Type of Service	服务类型
TPID	Tag Protocol Identifier	标签协议标识符
TRIP	Trigger RIP	触发路由信息协议



英文缩写	英文全称	中文全称
TTL	Time to Live	生存时间
-	Trap	陷阱
<b>U</b> <a href="#">回首页</a>		
UDP	User Datagram Protocol	用户数据包协议
-	Unicast	单播
URL	Uniform Resource Locators	统一资源定位
USM	User-Based Security Model	基于用户的安全模型
UTP	Unshielded Twisted Pair	非屏蔽双绞线
<b>V</b> <a href="#">回首页</a>		
VACM	View-based Access Control Model	基于视图的访问控制模型
VLAN	Virtual Local Area Network	虚拟局域网
VOS	Virtual Operate System	虚拟操作系统
<b>W</b> <a href="#">回首页</a>		
WAN	Wide Area Network	广域网
WLAN	wireless local area network	无线局域网
WRR	Weighted Round Robin Queuing	加权轮询队列
WWW	World Wide Web	万维网

[回目录](#)

## 附录B 技术参数规格

参数项	参数内容
支持的标准和协议	IEEE 802.3 10Base-T以太网 IEEE 802.3u 100Base-TX快速以太网 IEEE 802.3ab 1000Base-T千兆以太网 IEEE 802.3z 千兆以太网(光纤) IEEE 802.3x流量控制 IEEE 802.1p优先级 IEEE 802.1q VLAN桥操作
数据传输速率	以太网 10Mbps半双工, 20Mbps全双工 快速以太网 100Mbps半双工, 200Mbps全双工 千兆以太网 2000Mbps全双工
网络介质	10Base-T: 3类或以上UTP/STP(≤100m) 100Base-TX: 5类或以上UTP/STP(≤100m) 1000Base-T: 4对5类(推荐超5类)UTP/STP(≤100m)
指示灯	Power、System、10/100Mbps、1000Mbps (TL-SL2428) Power、System、10/100Mbps、10/100/1000Mbps、Link/Act (TL-SL2452) PWR、SYS、10/100/1000Mbps (TL-SG2452)
传输方式	存储转发
背板带宽	12.8Gbps (TL-SL2428) 17.6Gbps (TL-SL2452) 104Gbps (TL-SG2452)
MAC地址学习	自动更新, 支持16K地址空间
包转发速率	10Base-T: 14881pps/端口 100Base-TX: 148810pps/端口 1000Base-T: 1488095pps/端口
交流输入	100-240V~ 50/60Hz
工作温度	0℃~40℃
存储温度	-40℃~70℃
工作湿度	10%~90% (RH无凝结)
储存湿度	5%~90% (RH无凝结)
尺寸(长×宽×高)	440mm×180mm×44mm (TL-SL2428) 440mm×180mm×44mm (TL-SL2452) 440mm×260mm×44mm (TL-SG2452)

[回目录](#)