TP-LINK®

三层网管交换机

用户手册

REV1.5.0
1910040987

声明

Copyright © 2021 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、誊抄或转译本手册部分或全部内容，且不得以营利为目的进行任何方式（电子、影印、录制等）的传播。

TP-LINK® 为普联技术有限公司注册商标。本手册提及的所有商标，由各自所有人拥有。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。除非有特殊约定，本手册仅作为使用指导，所作陈述均不构成任何形式的担保。

目录

第 1 章　用户手册简介 12

1.1　目标读者 12

1.2　本书约定 12

1.3　章节安排 12

第 2 章　产品介绍 16

2.1　产品简介 16

2.2　产品特性 17

2.3　产品外观 20

2.3.1　全千兆三层网管交换机前面板 20

2.3.2　全千兆三层网管 PoE 交换机前面板 22

2.3.3　千兆上联三层网管交换机前面板 24

2.3.4　后面板 26

第 3 章　配置指南 27

3.1　登录 Web 页面 27

第 4 章　系统管理 29

4.1　系统配置 29

4.1.1　系统信息 29

4.1.2　设备描述 31

4.1.3　系统时间 31

4.1.4　夏令时 32

4.1.5　DNS 配置 34

4.2　用户管理 34

4.2.1　用户列表 34

4.2.2　用户配置 35

4.3　系统工具 36

4.3.1　启动配置 36

4.3.2 配置导入 37
4.3.3 配置导出 37
4.3.4 软件升级 38
4.3.5 在线升级 38
4.3.6 系统重启 39
4.3.7 软件复位 39
4.4 安全管理 40
4.4.1 安全配置 40
4.4.2 HTTP 配置 41
4.4.3 HTTPS 配置 42
4.4.4 SSH 配置 44
4.4.5 TELNET 配置 50
4.5 云管理 50
4.5.1 全局配置 50
第 5 章 二层交换 53
5.1 端口管理 53
5.1.1 端口配置 53
5.1.2 端口监控 54
5.1.3 端口安全 56
5.1.4 端口隔离 58
5.1.5 环路监测 59
5.2 汇聚管理 61
5.2.1 汇聚列表 62
5.2.2 手动配置 63
5.2.3 LACP 配置 64
5.3 流量统计 65
5.3.1 流量概览 65
5.3.2 详细统计 66
5.4 地址表管理 68
5.4.1 地址表显示 68
5.4.2 静态地址表 70

5.4.3 动态地址表 71
5.4.4 过滤地址表 73
第 6 章 VLAN 75
6.1 802.1Q VLAN 76
6.1.1 VLAN 配置 77
6.1.2 端口配置 79
6.1.3 802.1Q VLAN 功能的组网应用 81
6.2 MAC VLAN 82
6.2.1 MAC VLAN 83
6.2.2 端口使能 84
6.3 协议 VLAN 84
6.3.1 协议组列表 85
6.3.2 协议组配置 86
6.3.3 协议模板 87
6.3.4 协议 VLAN 功能的组网应用 88
6.4 VLAN VPN 89
6.4.1 VPN 配置 90
6.4.2 VLAN 映射 91
6.5 GVRP 93
6.6 Private VLAN 96
6.6.1 PVLAN 配置 97
6.6.2 端口配置 98
6.6.3 Private VLAN 功能的组网应用 100
第 7 章 生成树 102
7.1 基本配置 108
7.1.1 基本配置 108
7.1.2 生成树信息 109
7.2 端口配置 110
7.3 MSTP 实例 112
7.3.1 域配置 112
7.3.2 实例配置 113

7.3.3 实例端口 114
7.4 安全配置 115
7.4.1 端口保护 115
7.4.2 TC 保护 118
7.5 STP 功能的组网应用 118
第 8 章 组播管理 123
8.1 IGMP 侦听 125
8.1.1 基本配置 126
8.1.2 端口配置 128
8.1.3 VLAN 配置 129
8.1.4 组播 VLAN 130
8.1.5 查询器配置 132
8.1.6 Profile 配置 133
8.1.7 Profile 绑定 135
8.1.8 报文统计 136
8.1.9 IGMP 侦听功能组网应用 137
8.2 MLD 侦听 138
8.2.1 基本配置 140
8.2.2 端口配置 141
8.2.3 VLAN 配置 142
8.2.4 组播 VLAN 143
8.2.5 查询器配置 145
8.2.6 Profile 配置 146
8.2.7 Profile 绑定 148
8.2.8 报文统计 150
8.2.9 MLD 侦听功能组网应用 151
8.3 组播地址表 152
8.3.1 IPv4 组播地址表 152
8.3.2 IPv4 静态组播地址表 153
8.3.3 IPv6 组播地址表 154
8.3.4 IPv6 静态组播地址表 154

第 9 章　路由功能 156
9.1　接口 156
9.2　路由表 161
9.2.1　IPv4 路由表 161
9.2.2　IPv6 路由表 162
9.3　静态路由 163
9.3.1　IPv4 静态路由条目 163
9.3.2　IPv6 静态路由条目 164
9.3.3　静态路由功能的组网应用 165
9.4　DHCP 服务器 166
9.4.1　DHCP 服务器 168
9.4.2　地址池设置 169
9.4.3　静态绑定 170
9.4.4　绑定表 171
9.4.5　DHCP 服务器功能的组网应用 172
9.5　DHCP 中继 173
9.5.1　全局配置 176
9.5.2　DHCP 服务器 177
9.6　代理 ARP 177
9.6.1　代理 ARP 178
9.6.2　本地代理 ARP 179
9.6.3　代理 ARP 功能的组网应用 179
9.7　ARP 180
9.7.1　ARP 表 180
9.7.2　静态 ARP 181
9.8　RIP 181
9.8.1　基本配置 187
9.8.2　接口配置 190
9.8.3　路由表 191
9.8.4　RIP 的组网应用 191
第 10 章　服务质量 193

10.1 QoS 配置 193
10.1.1 端口配置 196
10.1.2 调度模式 198
10.1.3 802.1P 199
10.1.4 DSCP 199
10.2 流量管理 201
10.2.1 带宽控制 201
10.2.2 风暴抑制 202
10.3 语音 VLAN 203
10.3.1 全局配置 205
10.3.2 端口配置 206
10.3.3 OUI 配置 207
第 11 章 访问控制 209
11.1 时间段配置 209
11.1.1 时间段列表 209
11.1.2 新建时间段 210
11.1.3 节假日定义 211
11.2 ACL 配置 211
11.2.1 ACL 列表 212
11.2.2 新建 ACL 212
11.2.3 MAC ACL 212
11.2.4 标准 IP ACL 213
11.2.5 扩展 IP ACL 214
11.3 Policy 配置 216
11.3.1 Policy 列表 216
11.3.2 新建 Policy 217
11.3.3 配置 Policy 217
11.4 ACL 绑定配置 218
11.4.1 绑定列表 218
11.4.2 端口绑定 219
11.4.3 VLAN 绑定 219

11.5 Policy 绑定配置 220
11.5.1 绑定列表 221
11.5.2 端口绑定 221
11.5.3 VLAN 绑定 222
11.6 访问控制功能组网应用 223
11.7 终端上网策略 225
11.7.1 全局配置 226
第 12 章 网络安全 227
12.1 四元绑定 227
12.1.1 绑定列表 227
12.1.2 手动绑定 228
12.1.3 扫描绑定 230
12.2 DHCP 侦听 232
12.2.1 全局配置 235
12.2.2 端口配置 236
12.2.3 Option 82 配置 237
12.3 ARP 防护 238
12.3.1 防 ARP 欺骗 241
12.3.2 防 ARP 攻击 242
12.3.3 报文统计 243
12.4 IP 源防护 244
12.5 DoS 防护 245
12.6 Flood CPU 防护 247
12.7 802.1X 认证 248
12.7.1 全局配置 252
12.7.2 端口配置 253
12.8 AAA 254
12.8.1 全局配置 254
12.8.2 方法列表 255
12.8.3 Dot1x 配置 256
12.8.4 服务器组 257

12.8.5 RADIUS 配置 258
12.8.6 TACACS+配置 258
第 13 章 SNMP 261
13.1 SNMP 配置 263
13.1.1 全局配置 263
13.1.2 视图管理 264
13.1.3 组管理 264
13.1.4 用户管理 266
13.1.5 团体管理 267
13.2 通知管理 269
13.3 RMON 271
13.3.1 统计组 272
13.3.2 历史组 273
13.3.3 事件组 274
13.3.4 警报组 275
第 14 章 LLDP 277
14.1 基本配置 280
14.1.1 全局配置 280
14.1.2 端口配置 281
14.2 设备信息 282
14.2.1 本地信息 282
14.2.2 邻居信息 283
14.3 设备统计 283
14.4 LLDP-MED 285
14.4.1 全局配置 285
14.4.2 端口配置 285
14.4.3 本地信息 288
14.4.4 邻居信息 289
第 15 章 系统维护 290
15.1 运行状态 290
15.1.1 CPU 监控 290

15.1.2 内存监控 291
15.2 系统日志 291
15.2.1 日志列表 292
15.2.2 本地日志 293
15.2.3 远程日志 293
15.2.4 日志导出 294
15.3 系统诊断 295
15.4 网络诊断 296
15.4.1 Ping 检测 296
15.4.2 Tracert 检测 297
第 16 章 配置保存 299
第 17 章 索引页面 300
第 18 章 软件系统维护 301
18.1 硬件连接图 301
18.2 配置超级终端 301
18.3 bootUtil 菜单下加载软件 302
附录 A 术语表 304
附录 B 技术参数规格 309

第1章 用户手册简介

本手册旨在帮助您正确使用交换机。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，系指三层网管交换机。
- 鉴于三层网管交换机功能相近，本手册以 TL-SG5428 为例介绍。
- 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
注意：	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。
说明：	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
第 1 章 用户手册简介	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。
第 2 章 产品介绍	介绍本产品的特性、应用以及外观。
第 3 章 配置指南	介绍如何登录交换机的 Web 页面。

章节	章节说明
第 4 章 系统管理	本模块主要用于配置交换机的系统属性，主要介绍了： ● 系统配置：配置交换机的描述、时间和网络参数。 ● 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。 ● 系统工具：集中对交换机的配置文件进行管理。 ● 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、HTTP 配置和 SSH 配置等内容。
第 5 章 二层交换	本模块主要用于配置交换机的基本功能，主要介绍了： ● 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、端口安全和端口隔离。 ● 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。 ● 流量统计：统计流经各个端口的数据信息。 ● 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。
第 6 章 VLAN	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： ● 802.1Q VLAN：划分基于端口的VLAN，是协议VLAN的基础。 ● MAC VLAN：配置基于MAC地址的VLAN，使指定MAC的设备接入网络时，其数据均在MAC VLAN中转发。 ● 协议VLAN：从应用层划分VLAN，使某些特殊网络数据只能在指定VLAN中传输。 ● VLAN VPN：通过VLAN映射将私网报文的VLAN Tag映射到公网VLAN Tag，并在公网VLAN传输报文。 ● Private VLAN：通过建立Private VLAN，上层设备只需识别少量的primary VLAN，从而节省上层设备的VLAN资源。 ● GVRP：通过在端口动态注册和注销 VLAN 信息来达到创建或删除 VLAN 的目的，并传播 VLAN 信息到其它交换机中，减少配置 VLAN 时烦琐的手动操作。
第 7 章 生成树	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： ● 基本配置：配置和查看交换机生成树功能的全局属性。 ● 端口配置：配置端口的 CIST 参数。 ● MSTP 实例：配置 MSTP 实例。 ● 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。

章节	章节说明
第 8 章 组播管理	本模块主要用于配置交换机的组播管理功能，主要介绍了： ● IGMP 侦听：配置 IGMP 侦听功能。 ● 组播地址表：显示和配置组播地址。 ● 组播过滤：配置组播过滤功能。 ● 报文统计：查看和监控各端口的组播报文流量信息。 ● IGMP 查询器：本页面主要用于配置 IGMP 侦听查询器相关参数。
第 9 章 路由功能	本模块用于配置交换机的路由功能，主要介绍了： ● 接口：配置三层接口。 ● 路由表：查看交换机的路由表。 ● 静态路由：为三层通信配置静态路由功能。 ● 代理ARP：配置代理ARP功能，为不同网络中的计算机提供ARP代理服务。 ● ARP：显示ARP表，可以查看本机中所有的静态或动态ARP条目。 ● DHCP服务器：配置DHCP服务器功能，为以太网中的客户端分配IP参数。 ● DHCP中继：配置DHCP中继功能，使不同子网内的DHCP客户端可以共享DHCP服务器。 ● RIP：配置交换机的RIP特性。
第 10 章 服务质量	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： ● 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。 ● 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。 ● 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。
第 11 章 PoE	本模块主要用于配置交换机的 PoE 功能，通过交换机给 PD 设备供电，主要介绍了： ● PoE 配置：配置 PoE 功能的全局属性。 ● PoE 时间段：通过时间段控制 PoE 端口的供电时间。
第 12 章 访问控制	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： ● 时间段配置：通过时间段控制 ACL 条目的生效时间。 ● ACL 配置：配置 ACL 条目。 ● Policy 配置：配置 ACL 规则的处理方式。 ● 绑定配置：将 Policy 下发到端口和 VLAN，使之正式生效。

章节	章节说明
第 13 章 网络安全	本模块针对局域网中常见的网络攻击进行防护，主要介绍了： ● 四元绑定：是将计算机的 MAC 地址和 IP 地址，所属 VLAN 以及连接交换机的端口号四者绑定。 ● ARP 防护：对局域网中的 ARP 攻击进行防护。 ● IP 源防护：根据四元绑定条目对接收的 IP 包进行过滤。 ● DoS 防护：对常见的 DoS 攻击进行防护。 ● 802.1X 认证：配置交换机对局域网接入用户进行接入认证。
第 14 章 SNMP	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： ● SNMP 配置：配置 SNMP 的基本属性。 ● 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。 ● RMON：配置 RMON 功能，便于网管更有效的监控网络。
第 15 章 LLDP	LLDP 功能主要用于不同的网络设备间相互学习对方的设备信息。SNMP 应用可以利用 LLDP 获取的信息，进行网络故障排除。本模块主要用于配置交换机的 LLDP 功能，主要介绍了： ● 基本配置：配置交换机 LLDP 功能的全局属性和端口属性。 ● 设备信息：查看本地信息和邻居设备信息。 ● 设备统计：查看 LLDP 全局统计信息和端口报文统计信息。 ● LLDP-MED：配置 LLDP-MED 全局参数和端口参数，查看 LLDP-MED 本地信息和邻居信息。
第 16 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，主要介绍了： ● 运行状态：对交换机内存和 CPU 进行监控。 ● 系统日志：查看交换机上的日志信息。 ● 系统诊断：检测与交换机连接的线缆的可用性。 ● 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。
第 17 章 软件系统维护	主要介绍了：当交换机出现软件故障时，如何进入交换机的 boot 菜单重新加载软件。
附录 A 术语表	整理用户手册中出现的术语。
附录 B 技术参数规格	技术参数规格表。

回目录

第2章 产品介绍

2.1 产品简介

普联技术有限公司自主研发设计并推出的新一代三层网管交换机，采用全新的软硬件平台，支持静态路由和 RIP 动态路由，提供完备的安全防护机制、完善的 QoS 策略及灵活的 VLAN 划分功能，易于管理维护，可作为中小企业、校园网络、酒店、医院、网吧等使用场景的核心交换机，为用户提供安全可靠、高性能、低成本的网络解决方案。

交换机目前具体包含型号如下：

类型	产品型号	10/100Mbps RJ45 端口	10/100/1000Mbps RJ45 端口	SFP 端口	Combo 口
全千兆三层网管交换机	TL-SG5452	无	48	4	无
	TL-SG5428	无	24	4	无
	TL-SG5828F	无	8	28	有
	TL-SG5820F	无	8	12	无
	TL-SG5218	无	16	2	无
	TL-SG5210	无	8	2	无
全千兆三层网管 PoE 交换机	TL-SG5428PE	无	24(PoE)	4	无
	TL-SG5226PE	无	24(PoE)	2	无
	TL-SG5226P	无	24(PoE)	2	无
	TL-SG5218PE	无	16(PoE)	2	无
	TL-SG5210PE	无	8(PoE)	2	无
千兆上联三层网管交换机	TL-SL5452-Combo	48	2	4	有
	TL-SL5428-Combo	24	4	4	有
	TL-SL5218-Combo	16	2	2	有
	TL-SL5210	8	1	1	无

说明：

- 若交换机的 SFP 端口与对应 RJ45 端口形成一个 Combo 口（即复用端口），则同一时刻 Combo 口的两个端口只能使用一个。Combo 口为“无”表示该交换机的 SFP 端口为独立的 SFP 端口。
- SFP 端口兼容多模、单模 SFP 光纤模块，可根据实际需求和组网情况选择光纤模块；推荐使用 TP-LINK 公司 SFP 光纤模块，如 TL-SM311LM 和 TL-SM311LS。
- (PoE)表示对应端口均支持 IEEE 802.3af/at 标准 PoE 供电。

2.2 产品特性

实用方便的路由功能

- 动态路由

支持RIP动态路由协议，能够解决各类中小型网络进行子网划分后的路由选路问题，简化网络配置。

- 静态路由

支持多条静态路由条目，通过简单的配置即可实现跨网段的通信,合理设置和使用静态路由,可有效改善网络性能。

- ARP代理

当计算机没有配置默认网关或者网络进行VLSM子网划分时，应用ARP代理功能，当网关收到源计算机向目标网络计算机发送的ARP请求时，使用自己的MAC地址与目标计算机的IP地址进行ARP应答，轻松实现不同网络间的互访。

- DHCP服务器

可作为DHCP服务器为DHCP客户端分配IP地址。能给不同VLAN指定特定的IP地址池，实现给不同的VLAN分配不同网段的IP地址。

- DHCP中继

支持DHCP中继功能，能为不同网段的DHCP客户端和DHCP服务器提供DHCP中继服务，将DHCP协议报文跨网段转发，使不同网段的DHCP客户端能共享一个DHCP服务器，有效降低网络组网成本。

完备的网络接入安全策略

- 一键快速绑定

支持 PORT/MAC/IP/VLAN ID 四元绑定，提供手动添加、自动扫描、DHCP 侦听三种绑定方式，支持跨 VLAN 扫描，根据不同网络环境，轻松实现快速绑定。

- ARP 攻击防护

内置特有的 ARP 入侵检测功能，对不匹配四元绑定表的非法 ARP 欺骗报文直接丢弃，有效杜绝内网 ARP 攻击；支持对非法 ARP 报文统计，帮助用户迅速定位 ARP 攻击源；同时还支持防合法 ARP 报文的泛滥攻击。

- IP 源防护

内置 IP 源防护功能，可根据四元绑定条目对接收的 IP 包进行过滤，只处理数据包相关字段与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

- DoS 攻击防护

内置深层次攻击检测功能，通过解析 IP 数据包，查看数据包中的特定字段是否符合 DoS 攻击数据包的特征，并采取相应的防护措施，直接丢弃非法数据包或者对合法的数据包进行限速，并且还能主动探测追踪 DoS 攻击的源头。

- 防 MAC 地址攻击

支持端口安全特性，可以有效防御 MAC 地址攻击。可以实现基于 MAC 地址允许或限制流量，每个端口允许设定最大 MAC 地址数量，支持静态配置或交换机动态学习，全面保障网络安全。

多层次，多元化的访问控制策略

- 访问控制（ACL）

强大硬件 ACL 能力，深度识别报文，支持 L2~L4 数据流分类，提供基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、IP 协议类型、TCP/UDP 端口等定义 ACL。

- 策略控制（Policy）

支持基于端口、VLAN 下发 ACL，对符合相应 ACL 规则的数据包实现流分类，可进行流镜像、流监控、QoS 重标记和端口重定向四种行为控制，轻松实现网络监控，数据流量控制，优先级重标记和数据转发控制。

- 时间段控制

新增基于时间段的 ACL 控制，提供节假日、绝对时间、周期以及时间片段设置功能，多种时间段的灵活组合可轻松实现对时间精确控制的访问需求。

- 802.1X 认证

支持基于端口和基于 MAC 的 802.1X 认证，在用户接入网络时完成必要的身份认证，保证接入用户的合法性，支持 Guest VLAN，轻松设置来宾用户接入访问权限。

丰富的VLAN特性

- IEEE 802.1Q VLAN

IEEE 802.1Q VLAN符合国际标准，完美融合了Port VLAN，与主流设备完全兼容，加上人性化的操作方式，使组网更加便捷、准确、高效。

- 协议VLAN

通过协议来划分VLAN，对特殊应用可设置自定义协议，实现安全通信。

- VLAN VPN（QinQ）

有效扩展VLAN资源，实现用户VLAN的透传技术，便于在智能小区、企业网或园区网中组建多层交换网络。

- Private VLAN

将多个Secondary VLAN和一个Primary VLAN组成VLAN对，下层用户通过Secondary VLAN相互隔离二层报文，上层设备只需识别Primary VLAN。有效解决了上层VLAN资源紧缺及传统VLAN中的广播问题。

- GVRP

基于GARP的工作机制，用来维护设备中的VLAN动态注册信息，使得局域网内的VLAN配置更快捷、方便。

完善多业务融合能力

- QoS

支持基于端口、IEEE802.1p 以及 DSCP 三种优先级模式，支持 Equ、SP（Strict Priority）、WRR（Weighted Round Robin）、SP+WRR 四种队列调度算法，每个端口 8 个输出队列，可以将不同优先级的报文映射到不同输出队列，保障关键业务数据优先处理，满足不同业务对基础网络的需求。

- 流量控制

带宽控制支持端口双向限速，限速的控制粒度为 64Kbps；风暴抑制支持对广播包、组播包、UL 包限速，避免网络资源被恶意浪费，提高网络效率。

- 语音 VLAN

内置语音设备 OUI 地址识别功能，通过 Voice VLAN 技术，对语音流进行有针对性的 QoS 配置，能够很好的解决语音设备数据流优先级的调整问题，保证通话质量。

- 组播管理

支持 IGMP V1/V2/V3，通过 IGMP Snooping 技术，能很好地支持组播应用，如 IPTV、视频会议等等；支持组播 VLAN，有效避免带宽浪费，减轻上游设备的组播负担；静态组播地址表减少学习时间，提高组播转发效率；未知组播报文丢弃功能，节省带宽，提高系统处理效率。

高可靠性设计

- 生成树

支持传统的 STP/RSTP/MSTP 二层链路保护技术，极大提高链路的容错、冗余备份能力，保证网络的稳定运行。支持 TC（Topology Change）报文保护，避免当设备受到恶意的 TC 报文攻击时，频繁的删除操作给设备带来很大负担。同时还支持环路保护、根桥保护、BPDU 保护、BPDU 过滤等功能。

- 链路汇聚

提供手工汇聚、动态 LACP 两种汇聚模式，能有效增加链路带宽，提高链路的可靠性，同时可以实现负载均衡、链路备份。

灵活、安全的网络管理

- 系统管理

支持 CLI 命令行（Console，Telnet，SSHV1/V2），Web 网管（HTTP、SSL V3/TLS V1），SNMP（V1/V2c/V3）等多种管理方式。

- 安全管理

通过身份过滤检测技术，能够很好的解决设备安全管理难题，支持两级用户管理，提供管理人员数限制功能，增强配置安全性。

- 网络监控

支持端口双向数据监控，结合网络分析软件可以实时监控网络运行状态，RMON 功能可以实现统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

- 系统维护

支持 CPU、内存实时监控，支持 VCT 电缆检查，方便定位网络故障点，同时支持 Ping、Tracert 命令操作，轻松分析出现故障的网络节点。

- 系统日志

提供免费的日志服务器软件，为用户提供对设备系统日志的数据库统计分析功能，有效监控设备运行和网络状况。

2.3 产品外观

2.3.1 全千兆三层网管交换机前面板

TL-SG5452 的前面板由 48 个 10/100/1000Mbps RJ45 端口、4 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

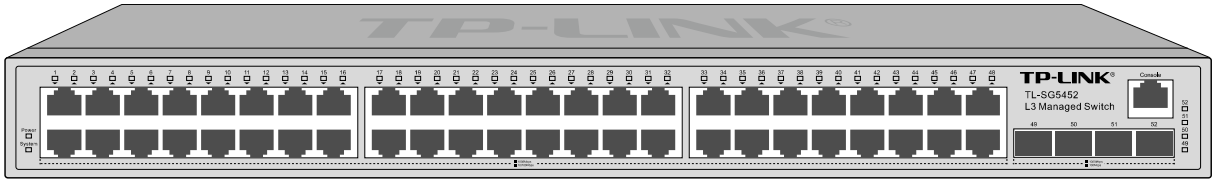


图 2-1 TL-SG5452 的前面板

TL-SG5428 的前面板由 24 个 10/100/1000Mbps RJ45 端口、4 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

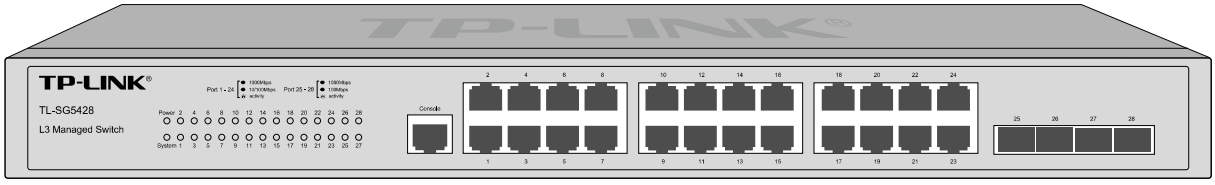


图 2-2 TL-SG5428 的前面板

TL-SG5828F 的前面板由 8 个 10/100/1000Mbps RJ45 端口、12 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

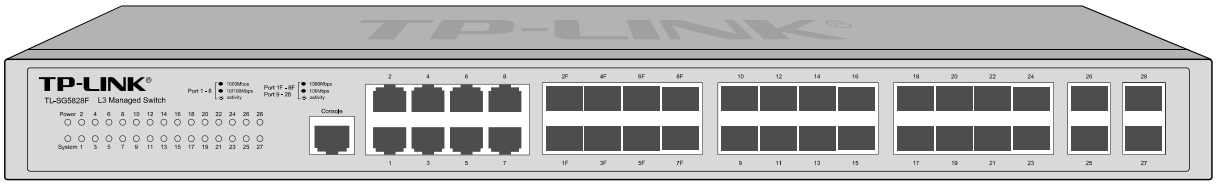


图 2-3 TL-SG5828F 的前面板

TL-SG5820F 的前面板由 8 个 10/100/1000Mbps RJ45 端口、12 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

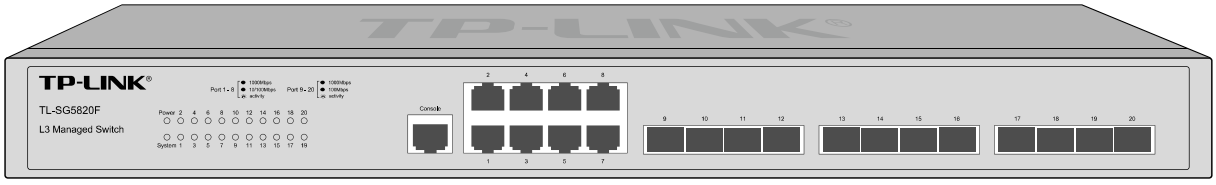


图 2-4 TL-SG5820F 的前面板

TL-SG5218 的前面板由 16 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

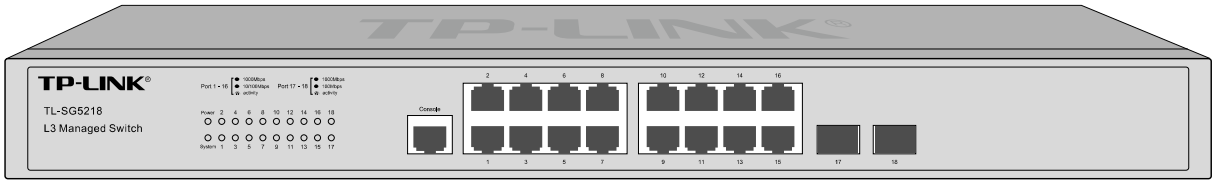


图 2-5 TL-SG5218 的前面板

TL-SG5210 的前面板由 8 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

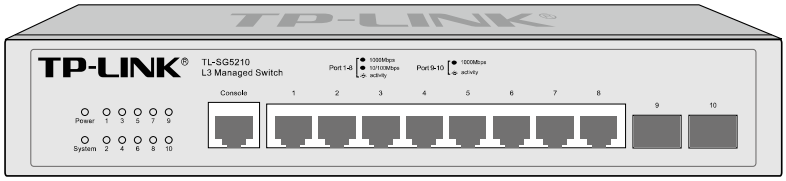


图 2-6 TL-SG5210 的前面板

- **10/100/1000Mbps RJ45 端口**

支持 10Mbps、100Mbps 或 1000Mbps 速率自适应功能，支持自动翻转（Auto-MDI/MDIX）功能，每个端口对应有一个指示灯，即 Link/Act 指示灯。

- **1000Mbps SFP 端口**

SFP 端口位于面板右侧。TL-SG5452/TL-SG5428/TL-SG5820F/TL-SG5218/TL-SG5210 为独立 SFP 端口，每个端口对应有一个指示灯，即 Link/Act 指示灯。TL-SG5828F 的 1F-8F 端口与 1-8 端口为 Combo 口，共用指示灯。

- **Console 端口**

Console 端口用于和计算机或其他终端的串口相连以管理或配置交换机。

- **指示灯**

指示灯，包括 Power，System，Link/Act 指示灯。通过指示灯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
		熄灭	系统未通电或供电异常
System	系统指示灯	常亮	系统异常
		闪烁	系统正常
		熄灭	系统启动过程中熄灭为正常，启动后熄灭为异常
Link/Act	状态指示灯	绿色常亮	端口正常连接设备且工作在 1000Mbps 速率下

指示灯	名称	状态	描述
		黄色常亮	端口正常连接设备且工作在 10/100Mbps（SFP 口为 100Mbps）速率下
		闪烁	端口正在传输数据
		熄灭	端口未连接设备

2.3.2 全千兆三层网管 PoE 交换机前面板

TL-SG5428PE 的前面板由 24 个 10/100/1000Mbps RJ45 端口、4 个 1000Mbps SFP 端口、1 个 Console 端口、1 个模式转换开关和指示灯组成，如下图所示。

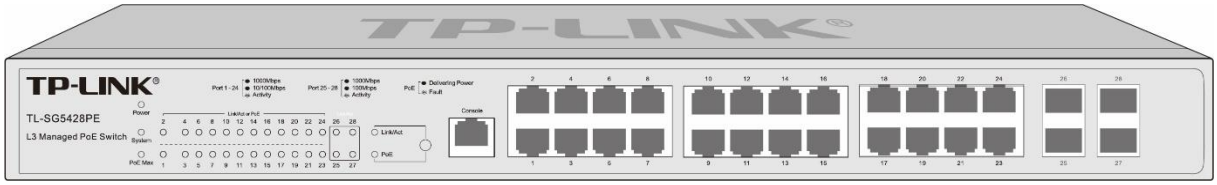


图 2-7 TL-SG5428PE 的前面板

TL-SG5226PE 的前面板由 24 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口、1 个模式转换开关和指示灯组成，如下图所示。

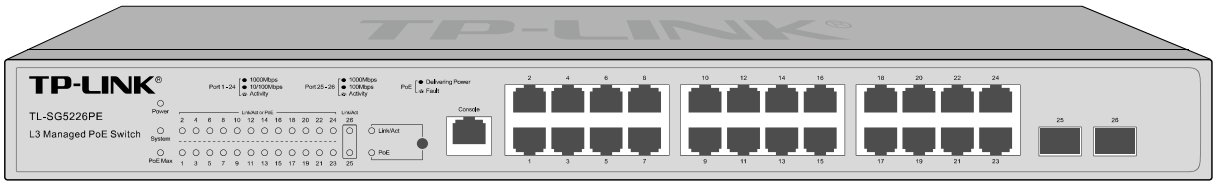


图 2-8 TL-SG5226PE 的前面板

TL-SG5226P 的前面板由 24 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口、1 个模式转换开关和指示灯组成，如下图所示。

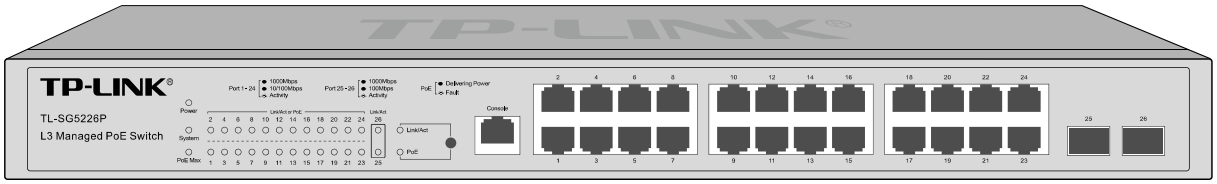


图 2-9 TL-SG5226P 的前面板

TL-SG5218PE 的前面板由 16 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口、1 个模式转换开关和指示灯组成，如下图所示。

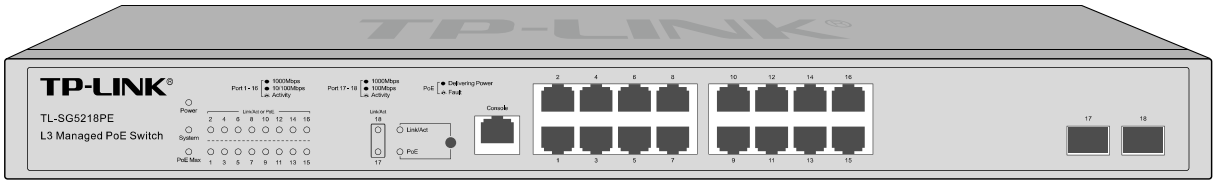


图 2-10 TL-SG5218PE 的前面板

TL-SG5210PE 的前面板由 8 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口、1 个模式转换开关和指示灯组成，如下图所示。

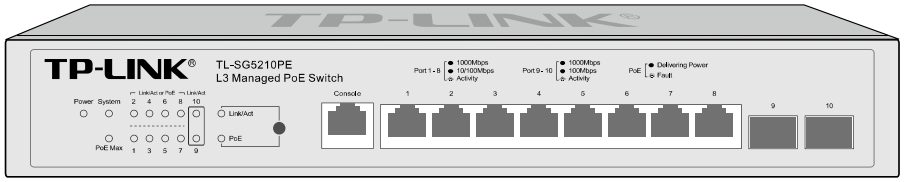


图 2-11 TL-SG5210PE 的前面板

- **10/100/1000Mbps RJ45 端口**

支持 10Mbps、100Mbps 或 1000Mbps 速率自适应功能，支持自动翻转（Auto-MDI/MDIX）功能，每个端口对应有一个指示灯，即 Link/Act or PoE 指示灯。

- **1000Mbps SFP 端口**

SFP 端口位于面板右侧，为独立 SFP 端口，每个端口对应有一个指示灯，即 Link/Act 指示灯。

- **Console 端口**

Console 端口用于和计算机或其他终端的串口相连以管理或配置交换机。

- **模式转换开关**

按下模式转换开关，可以切换 Link/Act or PoE 指示灯的指示状态。

- **指示灯**

指示灯，包括 Power、System、PoE Max、Link/Act or PoE、Link/Act 指示灯。

全千兆三层网管 PoE 交换机有一个模式转换开关，可以改变 Link/Act or PoE 指示灯的指示状态。当 Link/Act 指示灯点亮时，Link/Act or PoE 指示灯指示的是数据传输状态；当 PoE 指示灯点亮时，Link/Act or PoE 指示灯指示的是端口的供电状态。Link/Act 模式指示状态默认开启。

通过指示灯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
		熄灭	系统未通电或供电异常
System	系统指示灯	常亮	系统异常
		闪烁	系统正常
		熄灭	系统启动过程中熄灭为正常，启动后熄灭为异常
PoE Max	功率指示灯	常亮	PoE 总输出功率达到预警功率
		闪烁	PoE 总输出功率达到预警功率并且持续时间超过 2 分钟
		熄灭	PoE 总输出功率未达到预警功率

指示灯	名称	状态	描述	
Link/Actor PoE	状态指示灯		Link/Act 指示灯点亮	PoE 指示灯点亮
		绿色常亮	端口正常连接设备且工作在 1000Mbps 速率下	PoE 供电正常
		黄色常亮	端口正常连接设备且工作在 10/100Mbps 速率下	——
		闪烁	端口正在传输数据	PoE 供电异常
		熄灭	端口未连接设备	未进行 PoE 供电
Link/Act	状态指示灯	绿色常亮	端口正常连接设备且工作在 1000Mbps 速率下	
		黄色常亮	端口正常连接设备且工作在 100Mbps 速率下	
		闪烁	端口正在传输数据	
		熄灭	端口未连接设备	

2.3.3 千兆上联三层网管交换机前面板

TL-SL5452-Combo 的前面板由 48 个 10/100Mbps RJ45 端口、2 个 10/100/1000Mbps RJ45 端口、4 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

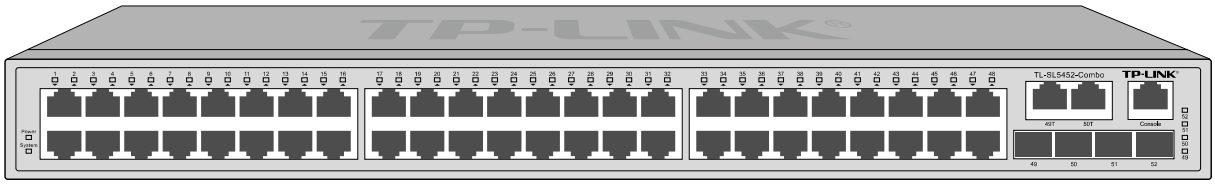


图 2-12 TL-SL5452-Combo 的前面板

TL-SL5428-Combo 的前面板由 24 个 10/100Mbps RJ45 端口、4 个 10/100/1000Mbps RJ45 端口、4 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

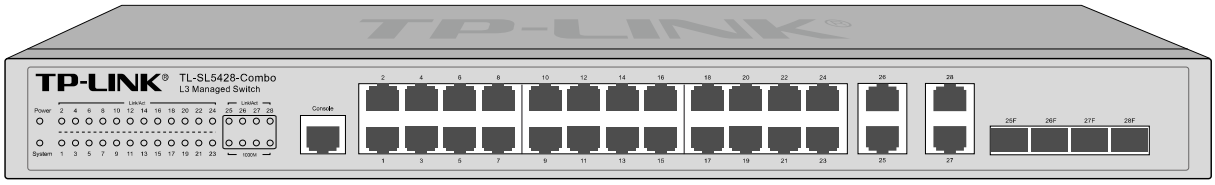


图 2-13 TL-SL5428-Combo 的前面板

TL-SL5218-Combo 的前面板由 16 个 10/100Mbps RJ45 端口、2 个 10/100/1000Mbps RJ45 端口、2 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

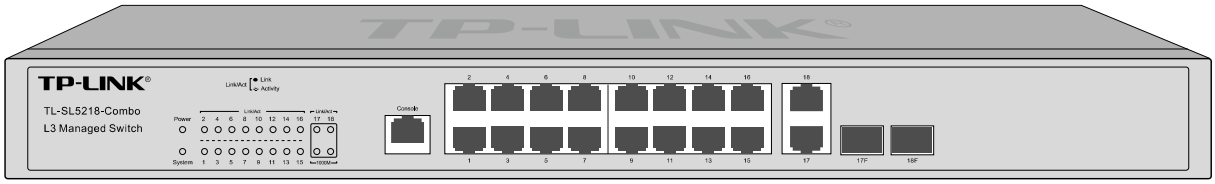


图 2-14 TL-SL5218-Combo 的前面板

TL-SL5210 的前面板由 8 个 10/100Mbps RJ45 端口、1 个 10/100/1000Mbps RJ45 端口、1 个 1000Mbps SFP 端口、1 个 Console 端口和指示灯组成，如下图所示。

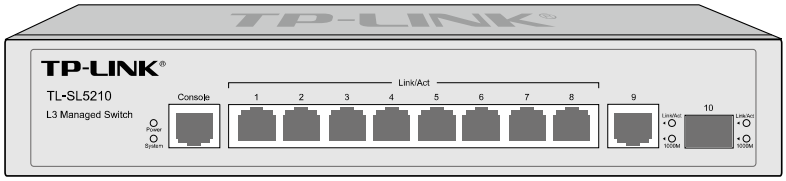


图 2-15 TL-SL5210 的前面板

- **10/100Mbps RJ45 端口**

支持 10Mbps 或 100Mbps 速率自适应功能，支持自动翻转（Auto- MDI/MDIX）功能，每个端口对应有一个指示灯，即 Link/Act 指示灯。

- **10/100/1000Mbps RJ45 端口**

支持 10Mbps、100Mbps 或 1000Mbps 速率自适应功能，支持自动翻转（Auto-MDI/MDIX）功能，每个端口对应有两个指示灯，即 Link/Act 和 1000M（TL-SL5452-Combo 无）指示灯。

- **1000Mbps SFP 端口**

SFP 端口位于面板右侧。TL-SL5452-Combo 的 49、50 端口同与其 Combo 共享的千兆 RJ45 端口共用指示灯，51、52 端口为独立 SFP 端口；TL-SL5428-Combo/TL-SL5218-Combo 同与其 Combo 共享的千兆 RJ45 端口共用指示灯；TL-SL5210 为独立 SFP 端口。

- **Console 端口**

Console 端口用于和计算机或其他终端的串口相连以管理或配置交换机。

- **指示灯**

指示灯，包括 Power、System、Link/Act、1000M（TL-SL5452-Combo 无）指示灯。通过指示灯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
		熄灭	系统未通电或供电异常
System	系统指示灯	常亮	系统异常
		闪烁	系统正常

指示灯	名称	状态	描述
		熄灭	系统启动过程中熄灭为正常，启动后熄灭为异常
Link/Act	状态指示灯	常亮	端口正常连接设备
		闪烁	端口正在传输数据
		熄灭	端口未连接设备
1000M	速率指示灯	常亮	端口正常连接设备且工作在 1000Mbps 速率下
		熄灭	端口未连接设备，或连接速率不是 1000Mbps

2.3.4 后面板

交换机后面板由电源接口和防雷接地柱组成，如下图所示（以 TL-SG5428 为例）。

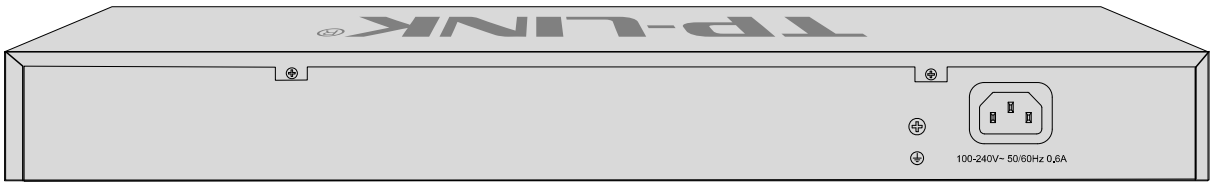


图 2-16 后面板

- **电源接口**

位于后面板右侧，接入交流电源。

- **防雷接地柱**

位于电源接口左侧，请参考光盘中的《防雷安装手册》进行防雷安装连接，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。

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 8.0 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) 为保证更好地体验 Web 页面显示效果，请将显示器的分辨率调整到 1024×768 或以上像素。

登录交换机 Web 页面方法如下：

1) 打开 IE 浏览器，在地址栏输入交换机默认管理地址 http://192.168.0.1 登录交换机的 Web 页面。

2) 交换机登录页面如图 3-1 所示，在此页面输入交换机管理帐号的用户名和密码，出厂默认值均为 admin。

图 3-1 登录页面

3) 成功登录后可以看到当前端口连接状态和交换机的系统信息，如图 3-2 所示。

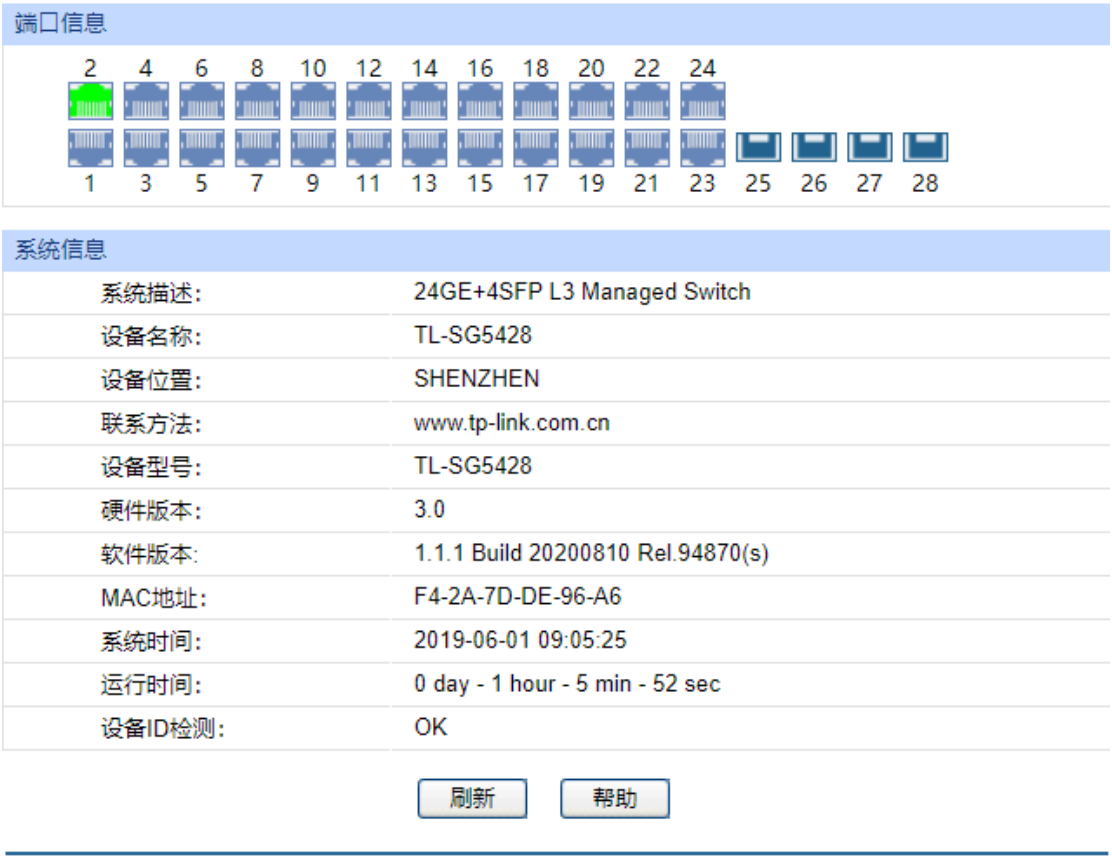


图 3-2 系统信息

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 **DNS 配置**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状态和系统信息。

端口状态指示了本交换机的 24 个 10/100/1000Mbps RJ45 端口以及 4 个 SFP 扩展模块槽的工作状态，其中标识 1-24 的端口是 10/100/1000Mbps RJ45 端口，标识 25-28 为 SFP 的端口是光纤模块端口。

进入页面的方法：系统管理>>系统配置>>系统信息

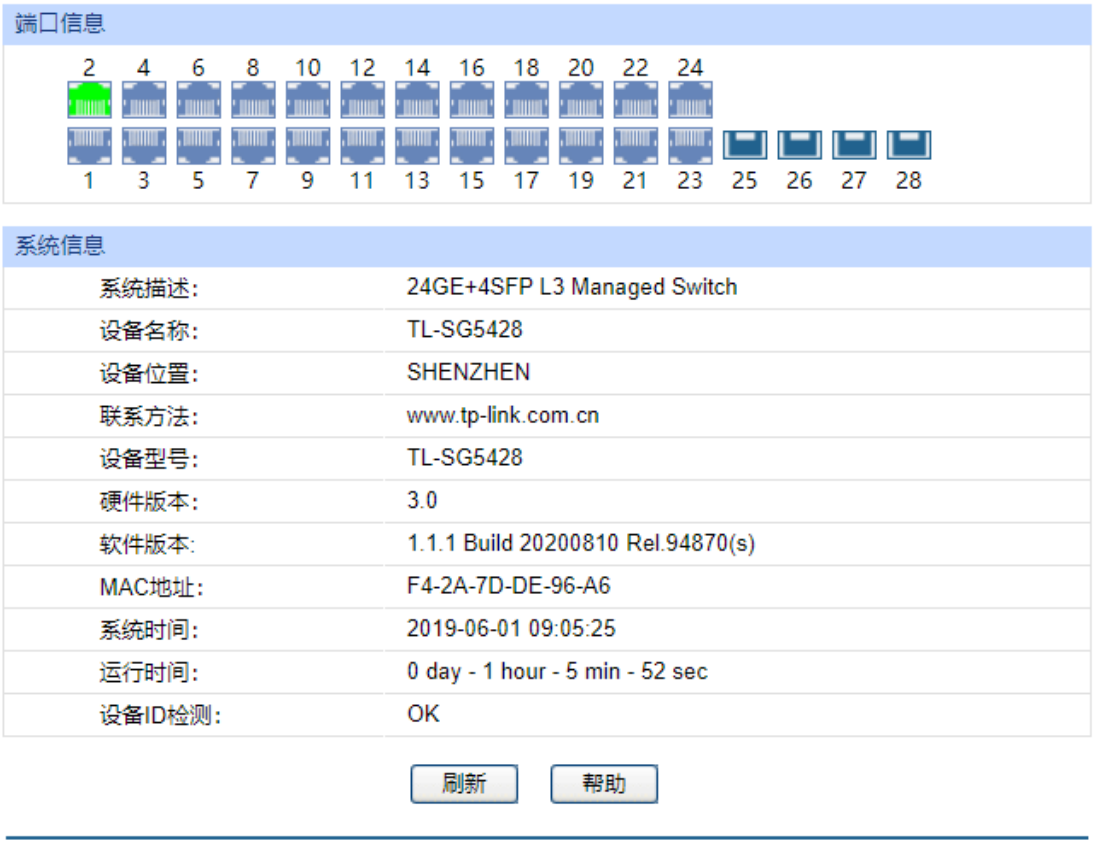


图 4-1 系统信息

条目介绍：

- **端口状态**

1000M 端口未接入设备。

　　1000M 端口工作速率为 1000Mbps。

　　1000M 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。

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**

端口：　　显示交换机的端口号。

类型：　　显示端口的端口类型。

速率　　显示端口当前连接速率和传输模式。

状态：　　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。

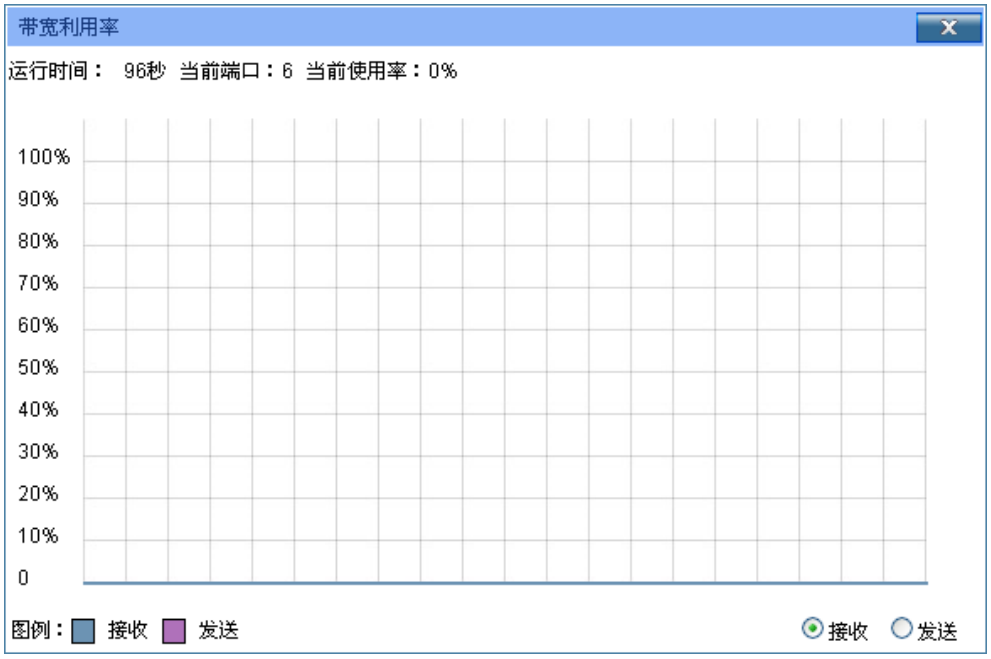


图 4-3 带宽利用率

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

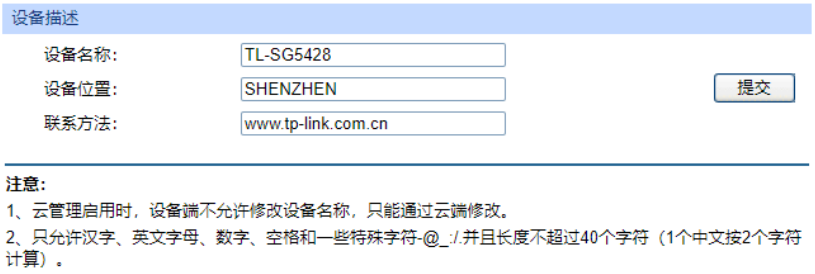


图 4-4 系统描述

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

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： 显示交换机当前的时间来源。

- **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：选择所在的时区。
  - 首选/备选 NTP 服务器：填写 NTP 服务器的 IP 地址。
  - 时间获取周期：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

本页面用于配置交换机的夏令时功能。

进入页面的方法：系统管理>>系统配置>>夏令时

图 4-6 夏令时

条目介绍：

- **夏令时配置**

夏令时状态： 选择启用或禁用夏令时功能。

预定义模式： 选择一个预定义的夏令时配置。

- 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。其中“周”表示一个月中的第几周；“日”表示星期几；“月”表示月份。

日期模式： 配置夏令时功能。在这一模式下做的配置只能在生效一次（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。其中“周”表示一个月中的第几周；“日”表示星期几；“月”表示月份。

注意：

- 当夏令时状态为禁用时，预定义模式、循环模式和日期模式都不可配置。
- 启用夏令时功能后，缺省配置为预定义模式下的欧洲配置模式。

4.1.5 DNS 配置

用于配置 DNS 服务器的 IP 地址，交换机默认配置三个 DNS 服务器 IP 地址：8.8.8.8、114.114.114.114 和 192.168.1.1。

进入页面的方法：系统管理>>系统配置>>DNS 配置。

图 4-7 DNS 配置

条目介绍：

- **服务器配置**

  服务器 IP 地址： 显示需要添加的服务器 IP 地址

- **服务器条目**

  选择： 您可以在此选择要修改或删除的服务器 IP 地址。

  IP 地址： 显示当前可选的 IP 地址。

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

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

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。
- 操作员：可以编辑、修改和查看交换机大部分功能的配置。
- 高级用户：可以编辑、修改和查看交换机部分功能的配置。
- 普通用户：仅可以查看交换机各个功能的配置情况。

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。

- **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： 显示当前用户的序号、用户名和用户类型。

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。

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**启动配置**、**配置导入**、**配置导出**、**软件升级**、**在线升级**、**系统重启**和**软件复位**七个配置页面。

4.3.1 启动配置

在本页面可以查看和修改交换机的启动配置参数。交换机上电后用“启动镜像”启动，如果失败则使用“备份镜像”启动。交换机启动后会尝试读取“启动镜像”的配置，如果失败则读取“备份镜像”的配置。

进入页面的方法：系统管理>>系统工具>>启动配置

图 4-7 启动配置

条目介绍：

- **启动参数**

  成员： 选择需要配置的成员。

  当前镜像： 显示当前启动所用到的镜像名称。

  启动镜像： 选择下一次启动的主镜像。

  备份镜像： 选择备份镜像。

- **镜像列表**

当前镜像/启动镜像/备份镜像：	显示当前镜像/启动镜像/备份镜像的状态。 点击当前镜像/启动镜像/备份镜像前“+”符号，展开如下显示项。

注意：

- 镜像名称应为“image1.bin”或“image2.bin”。
- 启动镜像和备份镜像应为不同镜像。
- 切换启动镜像和备份镜像后，为使配置生效请重启交换机。

4.3.2 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

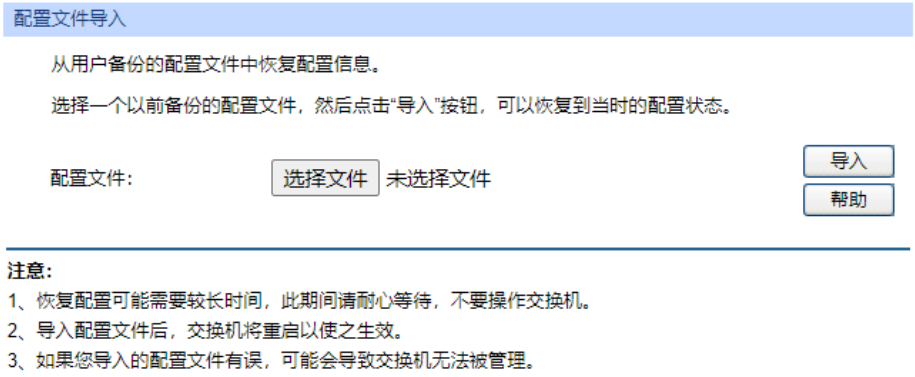


图 4-11 配置导入

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，交换机将重启以使之生效。
- 导入配置文件后，交换机中原有的配置信息将会丢失。如果导入的配置文件有误，可能会导致交换机无法被管理。

4.3.3 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

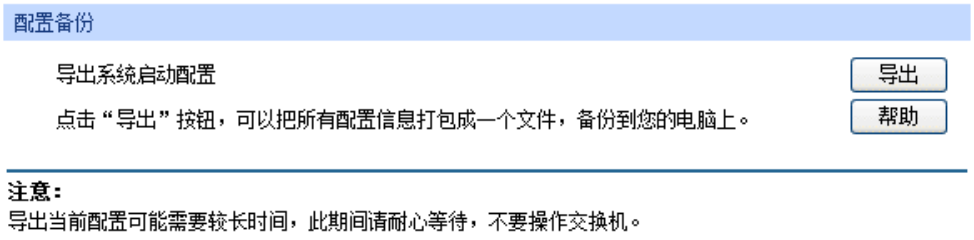


图 4-8 配置导出

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。

4.3.4 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

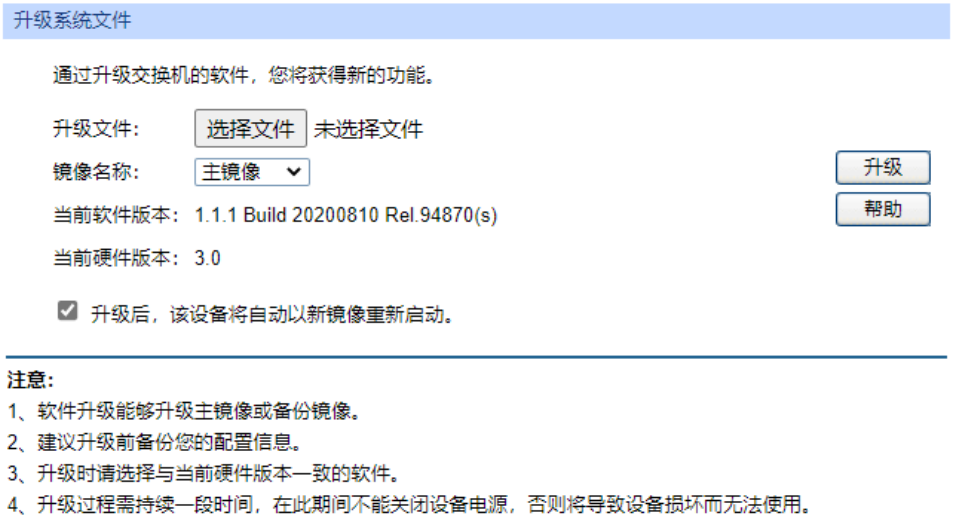


图 4-9 软件升级

注意：

- 软件升级只能升级备份镜像。
- 建议升级前备份配置信息。
- 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。

4.3.5 在线升级

本交换机可以通过在线检测最新版本软件，并在线升级系统文件，系统升级后将获得更完善的功能。

进入页面的方法：系统管理>>系统工具>>在线升级

图 4-10 在线升级

4.3.6 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

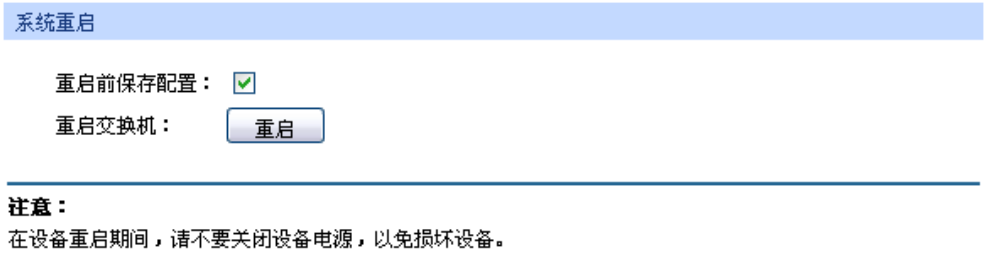


图 4-15 系统重启

注意:

在设备重启期间，请不要关闭设备电源，以免损坏设备。

4.3.7 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

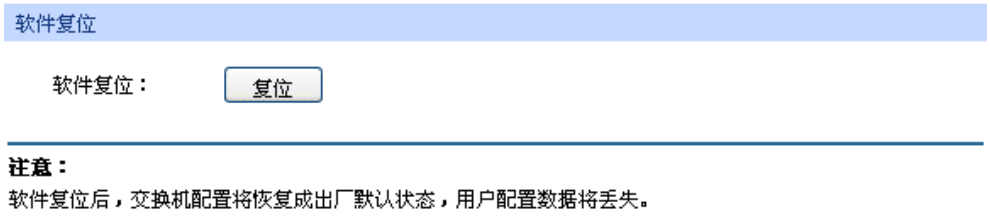


图 4-16 软件复位

注意:

软件复位后，交换机配置将恢复成出厂默认状态，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**、**HTTP 配置**、**HTTPS 配置**、**SSH 配置**、**TELNET 配置**五个配置页面。

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，从而增强了交换机配置管理的安全性。

进入页面的方法：系统管理>>安全管理>>安全配置

图 4-17 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的用户的 IP 网段。
- 基于 MAC：用来限制访问交换机的用户的主机 MAC 地址。
- 基于端口：用来限制访问交换机的交换机端口号。

接入方式： 选择接入方式。

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访问交换机。

4.4.2 HTTP 配置

通过 HTTP（HyperText Transfer Protocol，超文本传输协议），可以使用户在浏览器上管理交换机。 HTTP 标准是由互联网工程任务组（Internet Engineering Task Force）和万维网联盟（World Wide Web Consortium）共同合作研究的成果。本页可以配置 HTTP 功能。

进入页面的方法：系统管理>>安全管理>>HTTP 配置

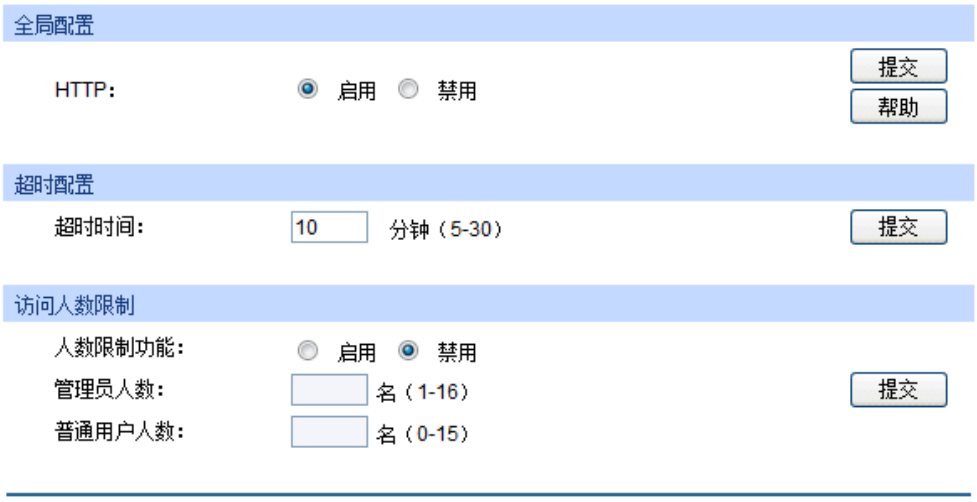


图 4-18 HTTP 配置

条目介绍：

- **全局配置**

HTTP 功能： 选择是否开启交换机的 HTTP 功能。

- **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。

- **接入人数限制**

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。

普通用户人数： 填写可同时登录交换机 Web 页面的普通用户总数。

4.4.3 HTTPS 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。

图 4-19 HTTPS 配置

条目介绍：

- **全局配置**

SSL 功能：	选择是否启用交换机的 SSL 功能。
SSL Version 3	可以在此选择是否开启 SSL 3.0。
TLS Version 1	可以在此选择是否开启 TLS1.0。

- **加密套件配置**

RSA_WITH_RC4_128_MD5:	通过 RC4 128-bit 加密进行密钥交换，消息摘要采用 MD5。
RSA_WITH_RC4_128_SHA：	通过 RC4 128-bit 加密进行密钥交换，消息摘要采用 SHA。
RSA_WITH_DES_CBC_SHA：	通过 DES_CBC 加密进行密钥交换，消息摘要采用 SHA。

RSA_WITH_3DES_EDE_CBC_SHA：	通过 3DES_EDE_CBC 加密进行密钥交换，消息摘要采用 SHA。

- **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。

- **接入人数限制**

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。
普通用户人数：	填写可同时登录交换机 Web 页面的普通用户总数。

- **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。
- 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。

4.4.4 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，因为它在网络上是使用明文传送口令和数据的，别有用心的人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

图 4-20 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。
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。

- **加密算法**

  勾选复选框，启用相应的加密算法。

- **数据完整性算法**

  勾选复选框，启用相应的数据完整性算法。

➢ **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：	点击此按键，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 512 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。

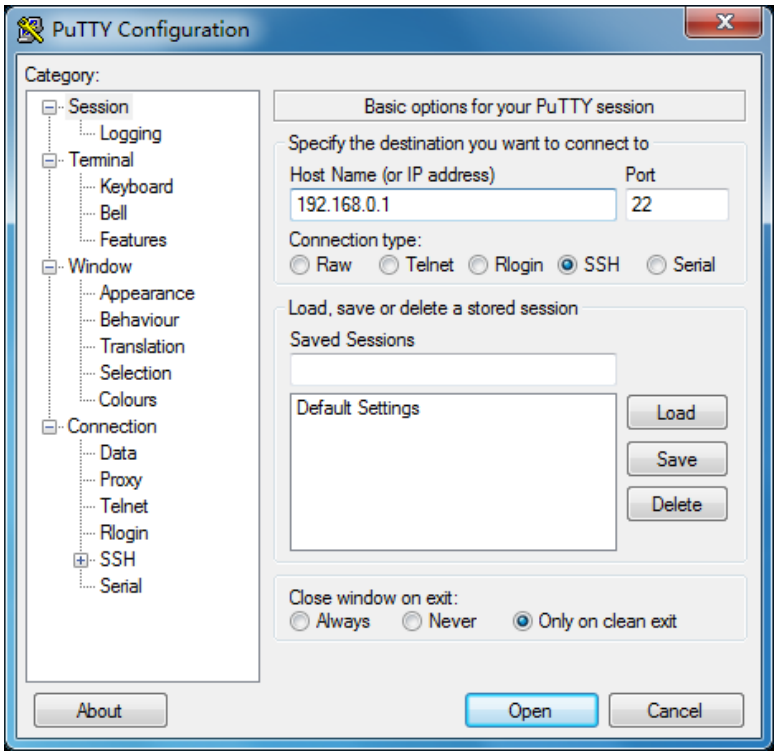
组网应用 1：

➢ **组网需求**

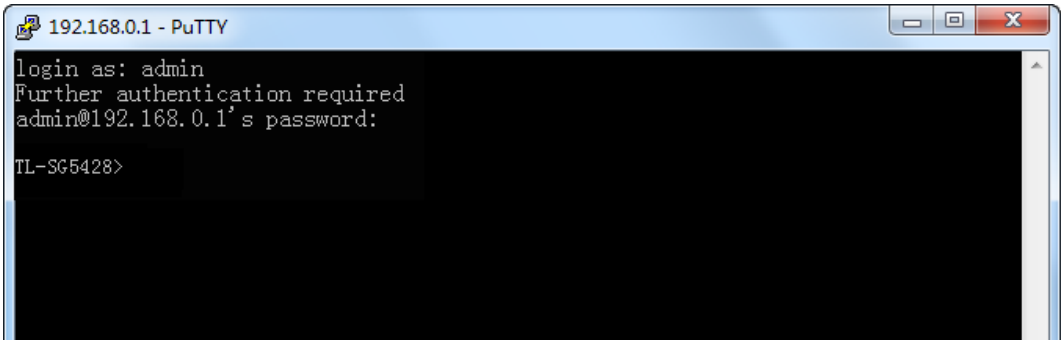
1. 使用 SSH 功能的“密码认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

➢ **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。



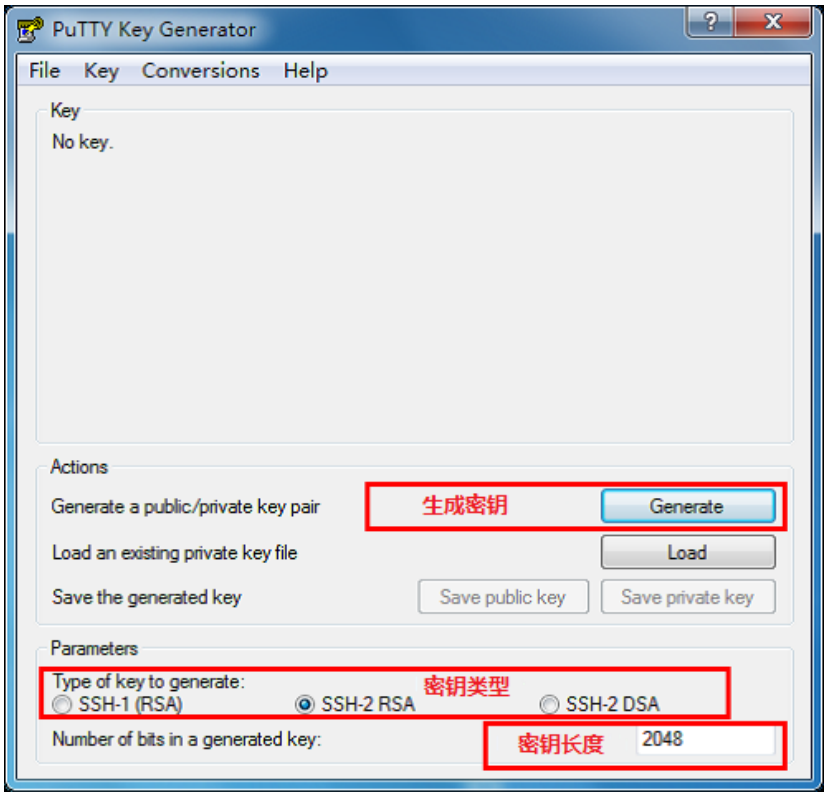
组网应用 2：

- **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**

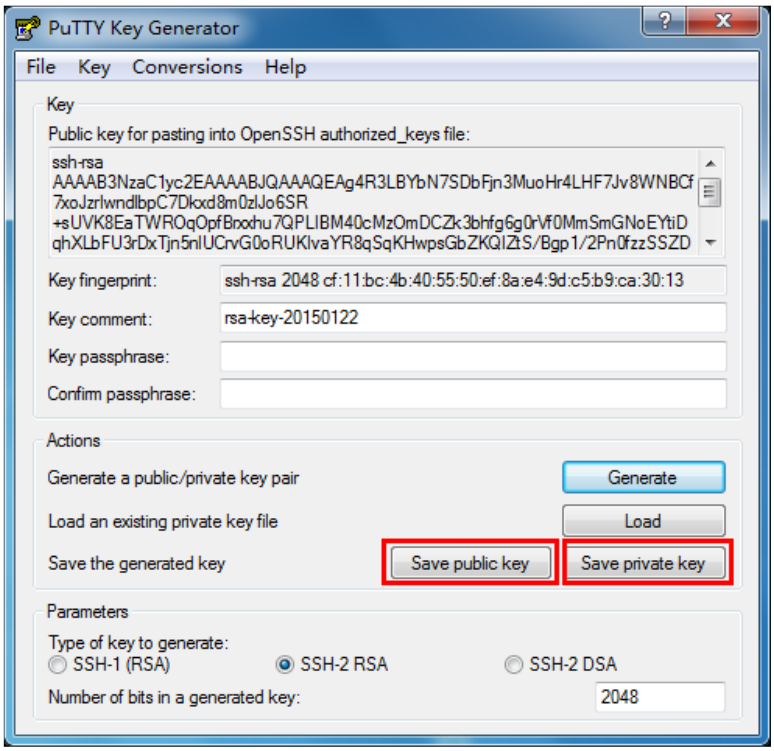
1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。



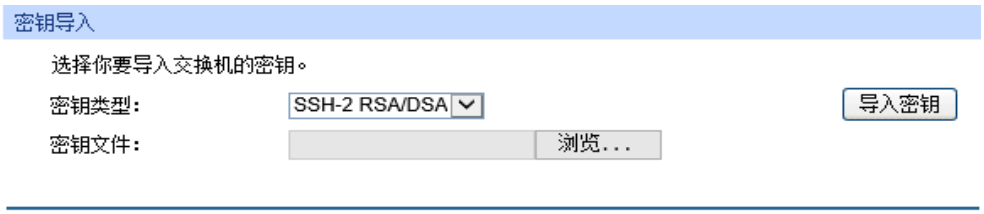
注意：

- 密钥长度的范围为 512 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。



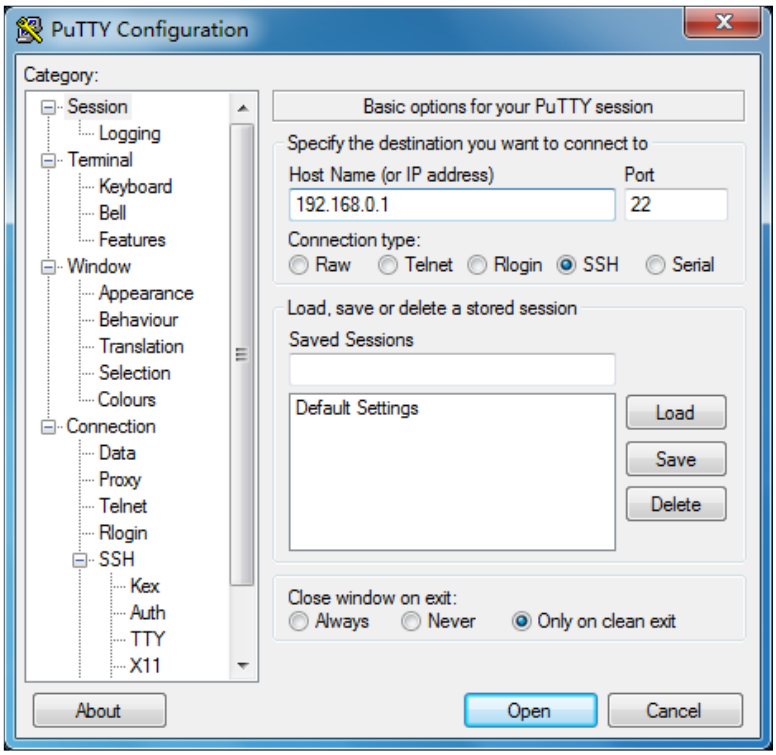
3. 在交换机配置页面上，将保存至主机上的公钥文件导入交换机中。



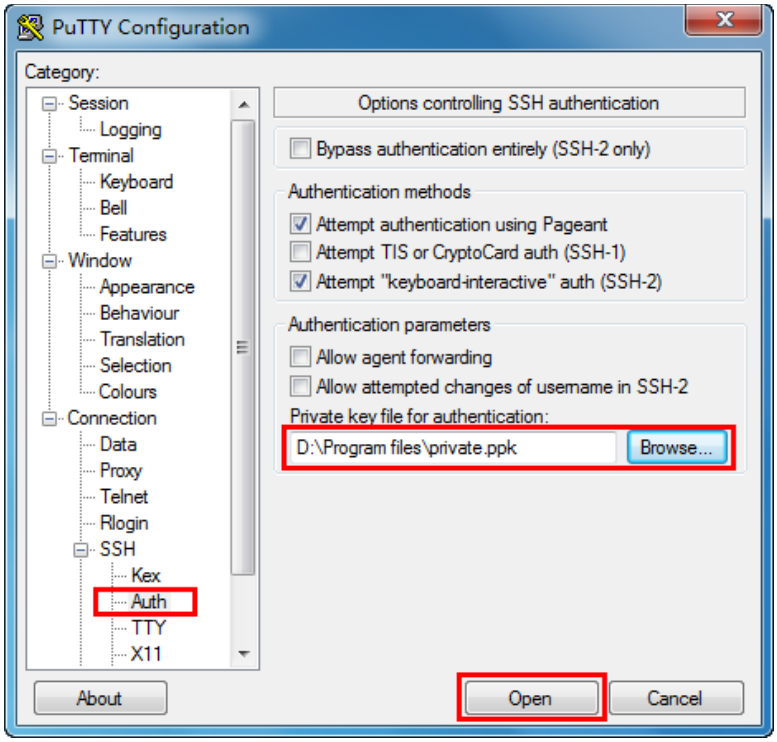
注意:

- 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。

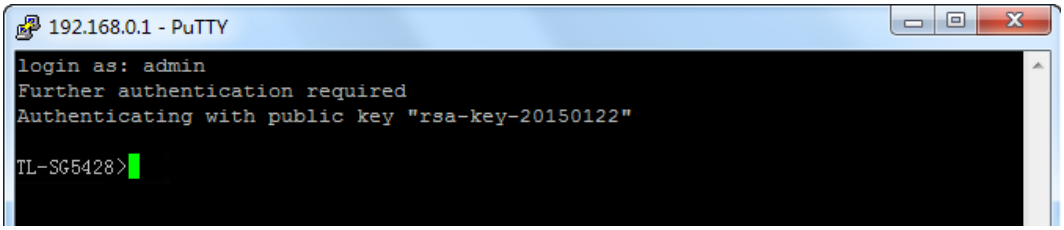
4. 打开 PuTTY 的主界面，输入 IP 地址并选择连接类型为 SSH，如下图所示。



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。



6. 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。



4.4.5 TELNET 配置

在此页面可以开启或禁用交换机的 Telnet 功能。

进入页面的方法：系统管理>>安全管理>>Telnet 配置

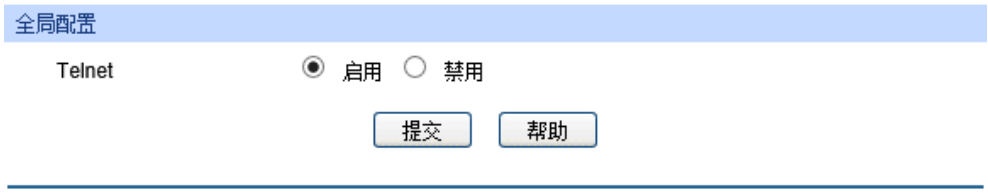


图 4-21 Telnet 配置

条目介绍：

- **全局配置**

  Telnet： 选择是否启用 Telnet 功能。

4.5 云管理

用户可以通过云平台远程管理交换机。

4.5.1 全局配置

本页用来开启或关闭云管理功能。

进入页面的方法：系统管理>>云管理>>全局配置

图 4-22 全局配置

条目介绍：

- **全局配置**

  全局开关： 选择是否启用云管理功能。

  导出配置： 导出当前配置文件

  保存配置： 保存当前配置文件

  导入配置： 导入本地配置文件

  恢复出厂： 将交换机恢复成出厂默认状态

  云类型 交换机支持"TP-LINK 商用网络云平台"和"TP-LINK 本地 NMS 管理平台"两种云管理平台

注意：

- 开启云管理可能会导致部分配置被修改，建议在开启前将配置导出。

- 导入配置后会覆盖当前配置文件，并将导致交换机重启。
- 设置软件恢复出厂后，交换机配置将恢复成出厂默认状态，所有用户配置数据将丢失，并将导致交换机重启。
- 云管理相关配置不会因为配置导入重启而更改。
- 关闭云管理或者切换到 TP-LINK 本地 NMS 管理平台时，云平台上绑定设备会解绑。
- 开启云管理功能后，可以登录“TP-LINK 商用网络云平台”配置交换参数。
- 请记住本设备 MAC 地址，在“TP-LINK 商用网络云平台”添加设备时需要使用该 MAC 地址。
- 为保证设备能正常使用云管理功能，请确保时间与当地时间保持一致。
- 还未下载 TP-LINK 商云 APP？可扫描图中二维码。

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**以及**地址表管理**四个部分。

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

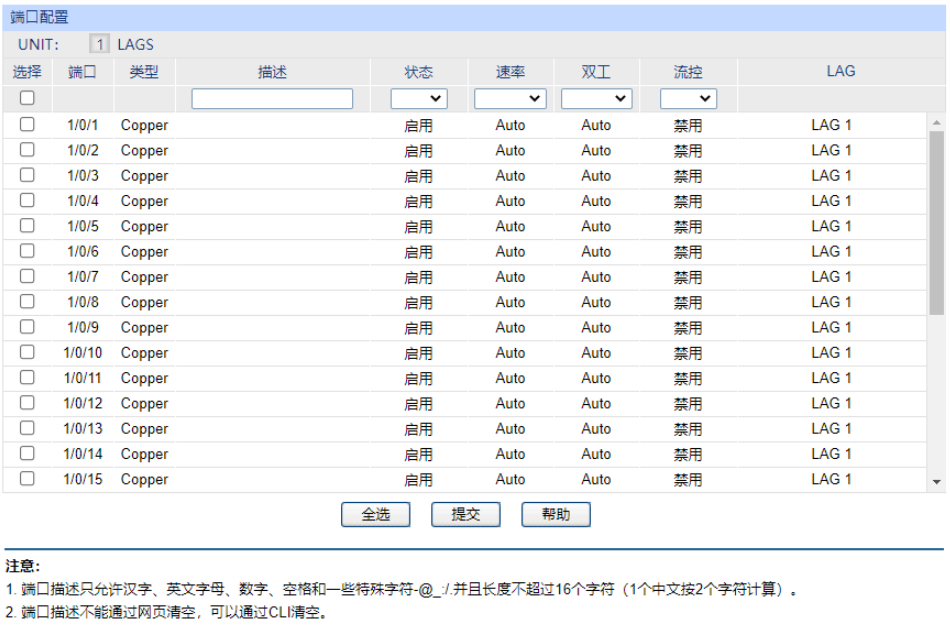


图 5-1 端口配置

条目介绍：

- **端口配置**

UNIT： 选择一个 UNIT 显示端口信息。

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。

类型： 显示端口的介质类型。

描述：	填写端口的描述信息，以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：	选择端口的工作速率。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，该端口的速率由自动协商决定。
双工：	选择端口的双工模式。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，该端口的双工由自动协商决定。
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。
巨帧：	选择端口的巨帧状态。默认的 MTU 是 1518 字节，开启巨帧后，MTU 为 9216 字节。
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。
- 端口描述不能通过网页清空，可以通过 CLI 清空。

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/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	---	仅入口监控	---	编辑 | 清空
		仅出口监控	---	
		出入口监控	---	
2	1/0/18	仅入口监控	---	编辑 | 清空
		仅出口监控	---	
		出入口监控	1/0/14	
3	---	仅入口监控	---	编辑 | 清空
		仅出口监控	---	
		出入口监控	---	
4	---	仅入口监控	---	编辑 | 清空
		仅出口监控	---	
		出入口监控	---	

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：

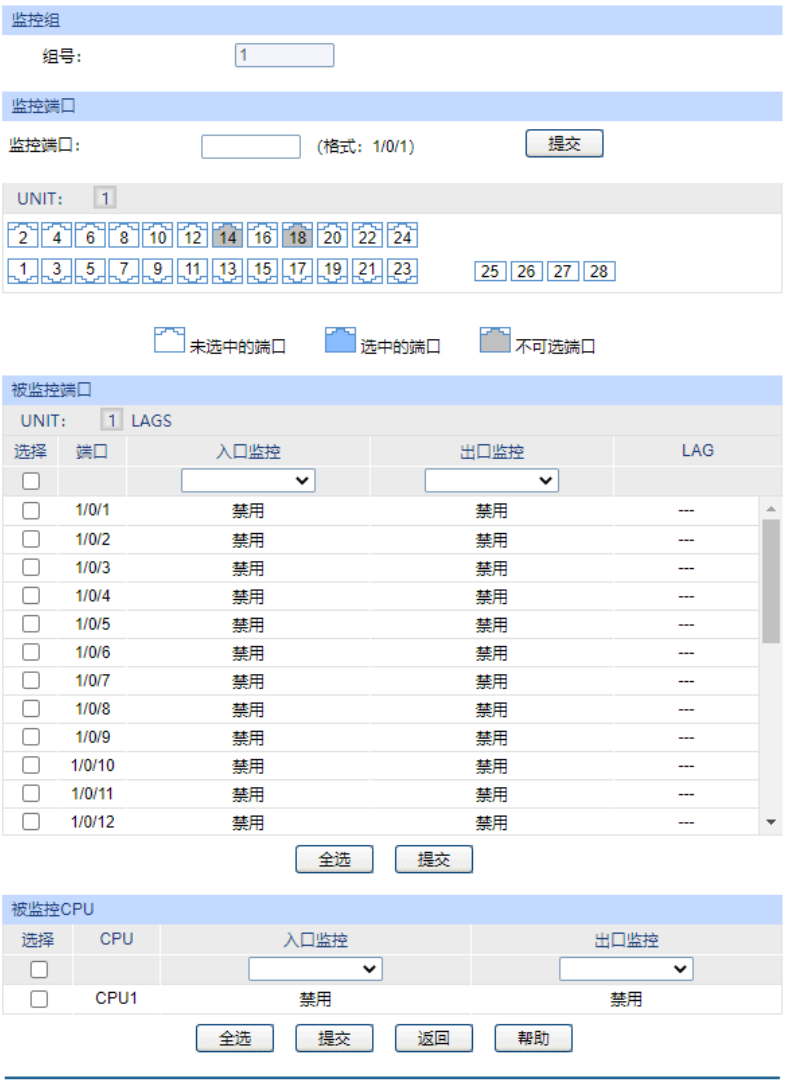


图 5-3 编辑监控组

条目介绍：

- **监控端口**

监控端口： 在此处选择该监控组的监控端口。

- **被监控端口**

UNIT： 选择一个 UNIT 显示端口信息。

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，数据流以泛洪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

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 1024。

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，才可以使用端口的端口安全功能。
- 若 802.1X 模块启用，此功能禁用。

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

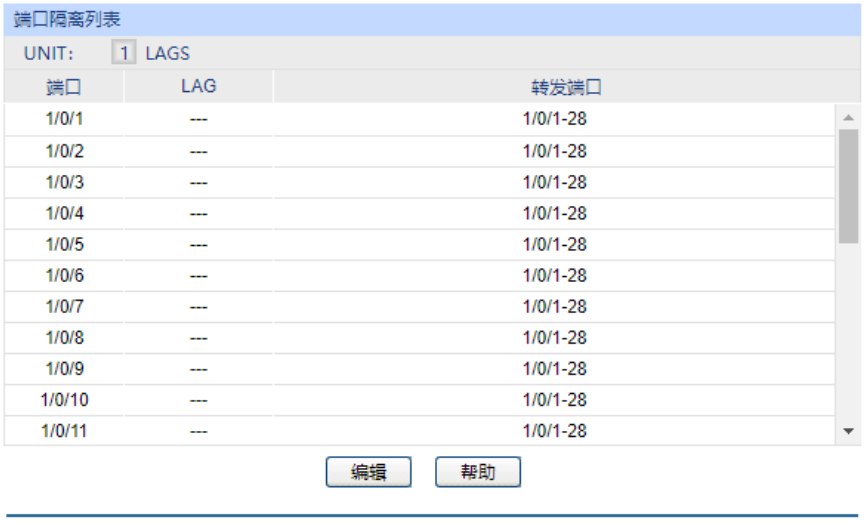


图 5-5 端口隔离

条目介绍：

- **端口隔离列表**

UNIT：	选择一个 UNIT 显示端口信息。
端口：	显示交换机的端口号。
LAG：	显示端口当前所属的汇聚组。
转发端口：	显示可转发的端口列表。

点击<编辑>按键，显示界面如下图所示：

图 5-6 端口隔离配置

- **端口隔离配置**

  端口： 选择一个指定端口，以对其转发端口进行设置。

  转发端口： 选择报文可以被转发到的端口。

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

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。

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。

页面自动刷新： 选择是否启用页面的自动刷新功能。

自动刷新间隔： 设置页面自动刷新的时间间隔。

- **端口配置**

UNIT： 选择一个 UNIT 显示端口信息。

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： ● 警告：端口上发现环路时只发出报警信息。 ● 阻塞端口：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： ● 自动：端口被阻塞后，经过自动恢复时间后将自动解除阻塞。 ● 手动：端口被阻塞后只能手动接触阻塞状态。
环路状态：	显示该端口是否监测到外部环路。
阻塞状态：	显示该端口是否因为监测到环路而处于阻塞状态。
LAG：	显示该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警告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、VLAN、端口属性、MAC 地址学习等。具体说明如下：

- 开启 **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。

如果需要配置汇聚组，建议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总带宽为 8000Mbps。

- LAG 的流量会根据选路算法均衡分配到各个成员端口中去。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去，即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

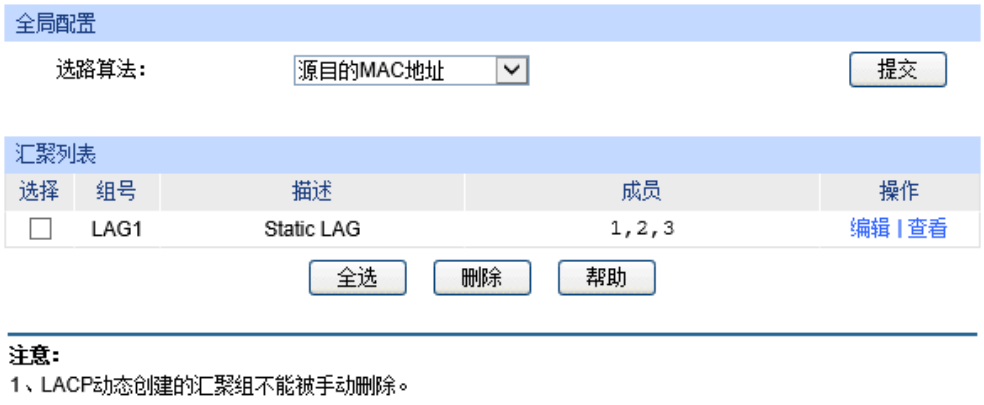


图 5-7 汇聚列表

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，可以看到所选汇聚组的详细信息。

图 5-8 汇聚组状态

5.2.2 手动配置

在本页可以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

图 5-9 手动配置

条目介绍：

- **汇聚组配置**

  汇聚组号： 选择汇聚组的序号，组号格式为 LAG*。

  汇聚组描述： 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。

在本页可以配置交换机的 LACP 功能。

进入页面的方法：二层交换>>汇聚管理>>LACP 配置

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。 ● 主动：周期性主动发送 LACP 报文。 ● 被动：被动应答 LACP 报文。
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

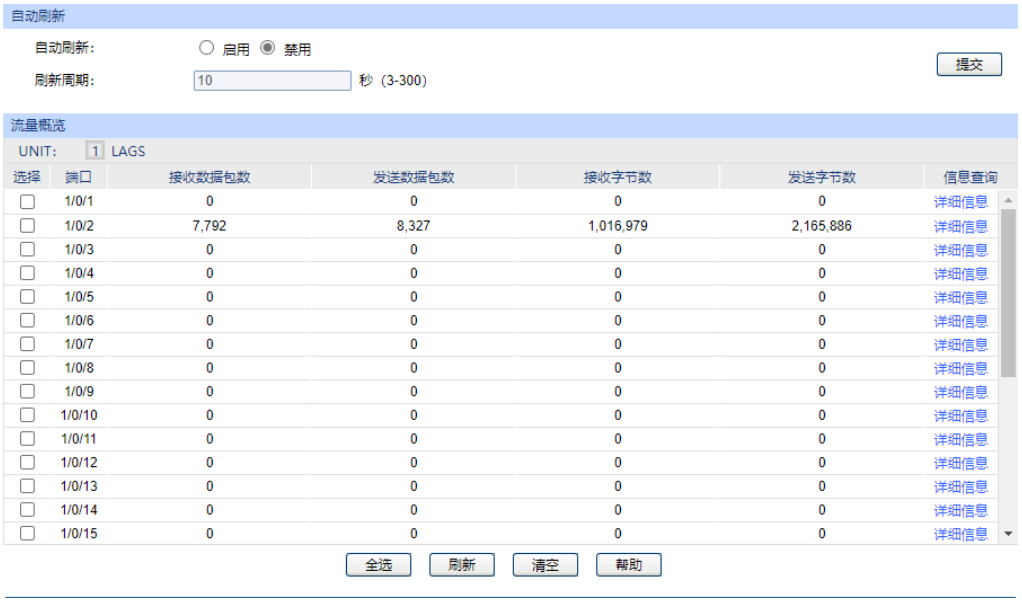


图 5-11 流量概览

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

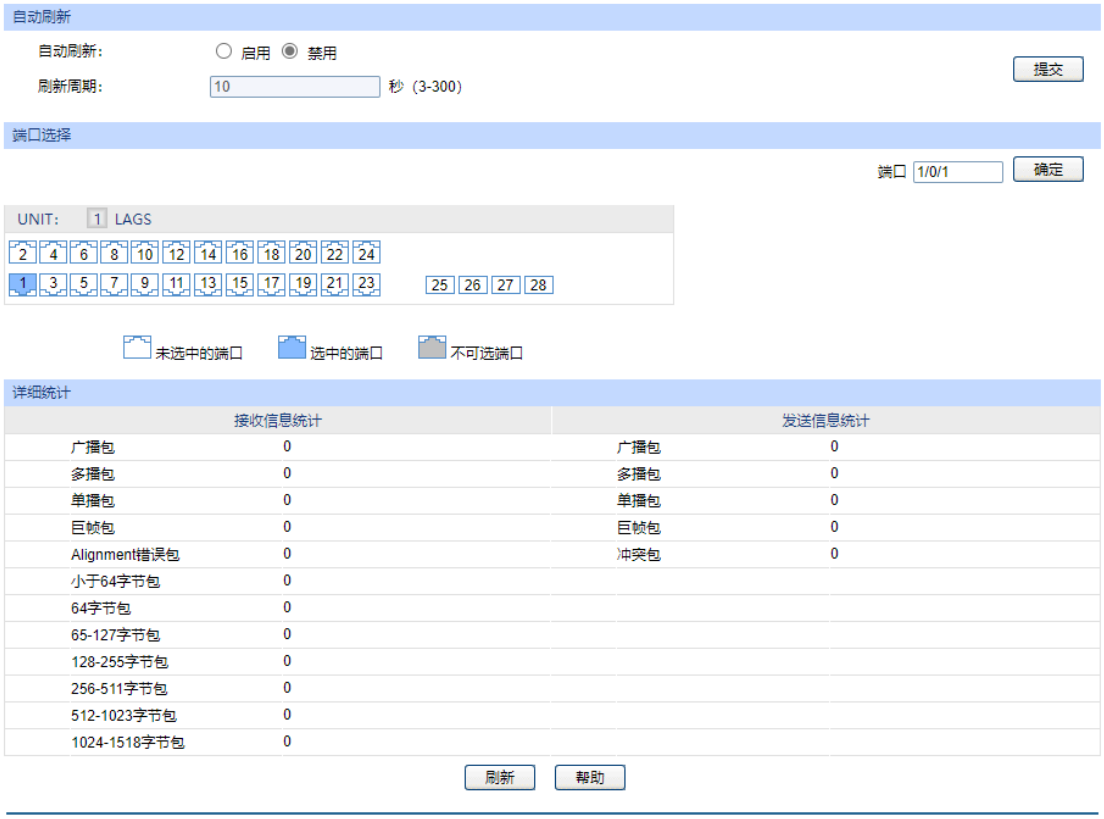


图 5-12 详细统计

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。

- **端口选择**

  端口： 输入要查看流量信息的交换机端口号。

- **详细统计**

  接收信息统计： 统计该端口接收数据包的详细信息。

  发送信息统计： 统计该端口发送数据包的详细信息。

  广播包： 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）。

  多播包： 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）。

  单播包： 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）。

  巨帧包： 端口发送的长度大于 1518 字节帧长的数据包数目。

Alignment 错误包：	端口接收的长度为 64-1518 字节的校验和错误且字节数不对齐的数据帧数目。
小于 64 字节包：	端口接收的长度小于 64 字节的数据帧数目（不含错误帧）。
64 字节包：	端口接收的长度为 64 字节的数据帧数目（包含错误帧）。
65-127 字节包：	端口接收的长度为 65-127 字节的数据帧数目(包含错误帧)。
128-255 字节包：	端口接收的长度为 128-255 字节的数据帧数目（包含错误帧）。
256-511 字节包：	端口接收的长度为 256-511 字节的数据帧数目（包含错误帧）。
512-1023 字节包：	端口接收的长度为 512-1023 字节的数据帧数目（包含错误帧）。
1024-1518 字节包：	端口接收的长度为 1024-1518 字节的数据帧数目（包含错误帧）。
冲突包：	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 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

图 5-14 地址表显示

条目介绍：

- **查询选项**

  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。

  地址类型： 选择欲查找条目需包含的地址类型信息。
  - 所有地址：显示全部地址表条目。
  - 静态地址：显示静态地址表条目。
  - 动态地址：显示动态地址表条目。
  - 过滤地址：显示过滤地址表条目。

  端口： 选择欲查找条目需包含的交换机端口。

- **地址表显示**

  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

图 5-15 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，可以快速查找到所需的条目。

- 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：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。可以在此修改与静态 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。
- 若 802.1X 模块开启，此功能禁用。

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新的地址和自动老化掉不再使用的地址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

图 5-16 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： 填写地址老化时间。

- **查找条目**

  查找选项： 选择动态地址表的显示规则，可以快速查找到所需的条目。
  - 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号。

- **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

图 5-17 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，可以快速查找到所需的条目。
  - 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。

- **过滤地址表**

  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。
- 若 802.1X 模块开启，此功能禁用。

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、性能显着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。如下图所示。

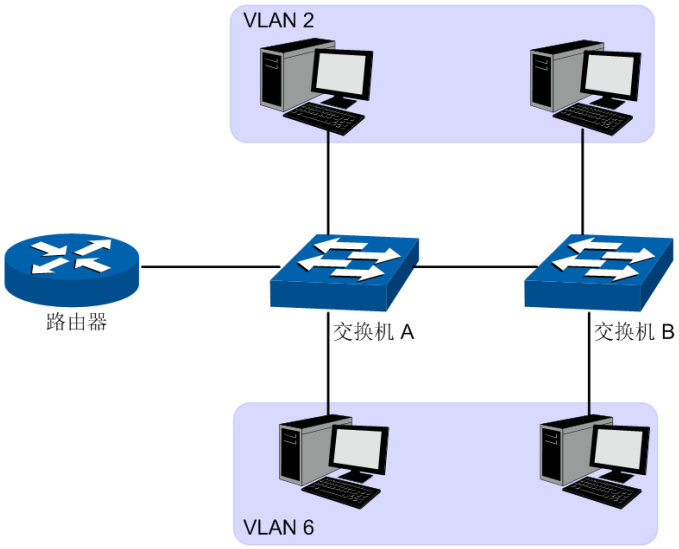


图 6-1 VLAN示意图

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类型有802.1Q VLAN、MAC VLAN和协议VLAN。协议VLAN仅对untag数据包和优先级tag数据包生效。当一个数据包同时满足802.1Q VLAN、MAC VLAN和协议VLAN时，交换机将按照MAC VLAN、协议VLAN、PVID的顺序来处理数据包，在相应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，如下图所示。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。

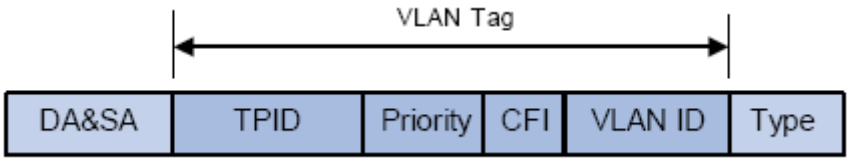


图 6-2 VLAN Tag组成字段

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为保留值，通常不给用户使用，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，当接收数据包不带VLAN Tag时，交换机会为该数据包封装带有接收端口默认VLAN ID，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。

- **端口的三种链路类型**

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三种：

1) ACCESS：端口只能属于1个VLAN，出口规则为UNTAG，多为连接用户终端设备的端口。当ACCESS类型端口加入了其它VLAN时，则自动退出原有VLAN。

2) TRUNK：端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，常用于网络设备之间级连。在网络中VLAN经常跨接在不同交换机上，TRUNK类型端口的默认出口规则为TAG，在转发端口默认VLAN数据时去掉VLAN信息，转发其余VLAN数据时保持原有VLAN信息。

3) GENERAL：端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，可以用于网络设备之间连接，也可以用于连接用户设备。GENERAL类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

- **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默认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。

<table>
<tr><th rowspan="2">端口类型</th><th colspan="2">对接收报文的处理</th><th rowspan="2">发送报文时的处理</th></tr>
<tr><th>报文不带Tag</th><th>报文带Tag</th></tr>
<tr><td>Access</td><td rowspan="3">接收报文，并为报文添加缺省的VLAN Tag即输入端口的PVID。</td><td>当VID＝端口PVID,接收报文。
当VID≠端口PVID,丢弃报文。</td><td>去掉Tag后，发送报文。</td></tr>
<tr><td>Trunk</td><td rowspan="2">当VID属于端口允许通过的VLAN ID时，接收报文。
当VID不属于该端口允许通过的VLAN ID时，丢弃报文。</td><td>转发端口默认VLAN数据时去tag后发送报文，其余保持原有Tag发送报文。</td></tr>
<tr><td>General</td><td>当出口规则配置为TAG时，保持原有tag发送报文。
当出口规则配置为UNTAG时，去tag后发送报文。</td></tr>
</table>

表 6-1 端口类型与VLAN数据处理关系

IEEE802.1Q VLAN功能包括**VLAN配置**、**端口配置**两个配置页面。

6.1.1 VLAN配置

在VLAN配置页面中可以查看当前已经创建的802.1Q VLAN。

进入页面的方法：VLAN>>802.1Q VLAN>>VLAN配置

图 6-3 查看VLAN列表

在缺省情况下，为了保证交换机在出厂情况下能正常通信，系统已创建缺省VLAN1，包含所有端口，该VLAN无法删除。

条目介绍：

- **VLAN配置列表**

选择： 勾选条目进行删除，可多选。

VLAN ID： 显示VLAN ID。

名称： 显示VLAN的描述信息。

成员： 显示VLAN的端口成员。

操作： 对单个VLAN条目进行相应操作。

- 编辑：修改VLAN配置。
- 详细：查看VLAN配置信息。

点击<编辑>按键，可以对相应的VLAN进行编辑。点击<新建>按键，可以创建新的VLAN。

图 6-4 创建或编辑802.1Q VLAN

条目介绍：

- **VLAN 信息**

VLAN ID：	填写 VLAN ID。
VLAN 名称：	填写 VLAN 的描述信息，以便区分各个 VLAN 的用途。
Untagged 端口：	显示可以配置不带 tag 的端口，该端口可能是 ACCESS 类型、TRUNK 类型或者 GENERAL 类型。
Tagged 端口：	显示可以配置带 tag 的端口，该端口可能是 TRUNK 类型或者 GENERAL 类型。

6.1.2 端口配置

在创建802.1Q VLAN时，需要对端口连接的设备进行了解，以便设置各端口的参数。

进入页面的方法：**VLAN>>802.1Q VLAN>>端口配置**

图 6-5 802.1Q VLAN - 端口配置

条目介绍：

- **VLAN 端口配置**

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。

选择： 勾选端口配置端口类型和 PVID 值，可多选。

端口： 显示交换机的端口号。

端口类型： 选择交换机的端口类型。默认为 ACCESS。

- ACCESS：该端口只能加入一个 VLAN，出口规则为 UNTAG。PVID 值与当前 VLAN ID 的值保持相同。如果 VLAN 删除，相应端口的 PVID 会自动置为默认值 1。
- TRUNK：该端口可加入多个 VLAN，出口规则为 TAG。PVID 值可设置为当前端口加入的任意一个 VLAN 的 VID 值。
- GENERAL：该端口可加入多个 VLAN，且允许根据不同 VLAN 选择不同的出口规则，默认出口规则为 UNTAG。PVID 值可设置为当前端口加入的任意一个 VLAN 的 VID 值。

PVID： 填写交换机物理端口的 PVID 值。默认为 1。

LAG： 显示端口当前所属的汇聚组。

所属 VLAN： 查询本端口所加入的 VLAN 信息。

点击<查询>按键，可以查询相应端口所属。

图 6-6 查看端口所属 VLAN

条目介绍：

- **端口所属 VLAN**

VLAN ID： 显示 VLAN ID。

名称： 显示 VLAN 的描述信息。

从该 VLAN 移除： 点击<移除>按键，将本端口从相应 VLAN 中移除。

802.1Q VLAN 配置步骤：

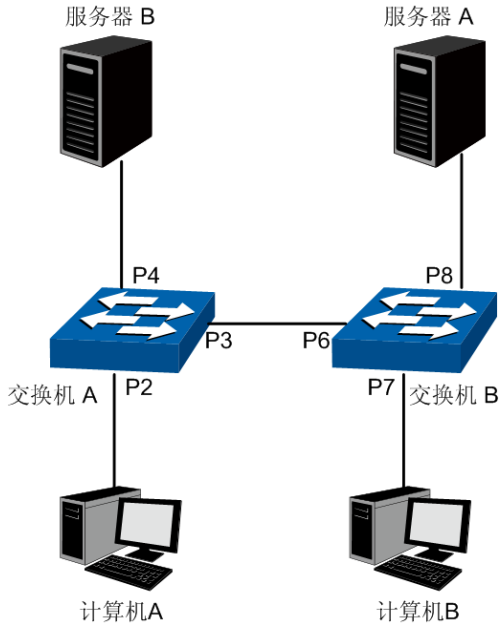
步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	编辑/查看 VLAN	可选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面点击<编辑>或<查看>按键，可以对相应的 VLAN 进行编辑和查看。
4	删除 VLAN	可选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面勾选相应的 VLAN 条目，点击<删除>按键进行删除。

6.1.3 802.1Q 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	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 2 的类型为 ACCESS；设置端口 3 的类型为 TRUNK；端口 4 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，并包含的端口 2 和端口 3。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，并包含的端口 3 和端口 4。

- 配置交换机B：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 7 的类型为 ACCESS；设置端口 6 的类型为 TRUNK；端口 8 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，并包含的端口 6 和端口 8。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，并包含的端口 6 和端口 7。

6.2 MAC VLAN

MAC VLAN是VLAN的另一种划分方法，根据每个主机的MAC地址来划分VLAN，即对每个主机的MAC地址均划分到VLAN中。MAC VLAN的优点在于，将MAC地址与VLAN绑定

后，该MAC地址对应的设备可以随意切换端口，只要连接到相应VLAN的成员端口即可，而不必改变VLAN成员的配置。

MAC VLAN 中数据包处理有如下特点：

1. 当端口收到 UNTAG 数据包时，首先查看是否创建配置相应的 MAC VLAN，若已创建 MAC VLAN，则给数据包插入 MAC VLAN 的 TAG；若没有相应的 MAC VLAN，则继续按照其它规则（例如协议 VLAN）进行匹配，如果匹配成功，则转发报文，如果匹配均失败，则根据该接收端口的 PVID 值给数据包插入 TAG，并将数据包在该缺省 VLAN 内转发。
2. 当端口收到 TAG 数据包时，交换机按照 802.1Q VLAN 的方式处理该帧。如果接收端口允许该 VLAN 的数据包通过，则正常转发；如果不允许，则丢弃该数据包。

将某个主机的 MAC 划分到 802.1Q VLAN 中后，为了保证该主机能够在此 VLAN 内正常通信，请将其接入端口设置成相应的 802.1Q VLAN 成员。详情请查看表 6-1。

6.2.1 MAC VLAN

在 MAC VLAN 页面中，可以创建 MAC VLAN 并查看当前已创建的 MAC VLAN。

进入页面的方法：VLAN>>MAC VLAN>>MAC VLAN

图 6-7 创建并查看 MAC VLAN

条目介绍：

- **MAC VLAN 配置**

MAC 地址：	输入 MAC 地址。
MAC 描述：	输入对 MAC 地址的描述，以便区分各个 MAC 的用途。
VLAN ID：	输入该 MAC VLAN 对应的 VLAN ID，此 VLAN 必须是输入端口所在的 802.1Q VLAN。

- **MAC VLAN 列表**

MAC 地址选择：	点击<选择>按键，可根据所输 MAC 快速查找 MAC VLAN 条目。

选择：	勾选条目进行删除，可多选。
MAC 地址：	显示 MAC 地址。
MAC 描述：	显示此 MAC 的描述信息，以便区分各个 MAC 的设备。
VLAN ID：	显示该 MAC 对应的 VLAN ID。
操作：	点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

6.2.2 端口使能

端口使能用来开启端口的 MAC VLAN 功能。只有配置了 MAC VLAN 并使能端口，才能正式启用 MAC VLAN 功能。

进入页面的方法：VLAN>>MAC VLAN>>端口使能

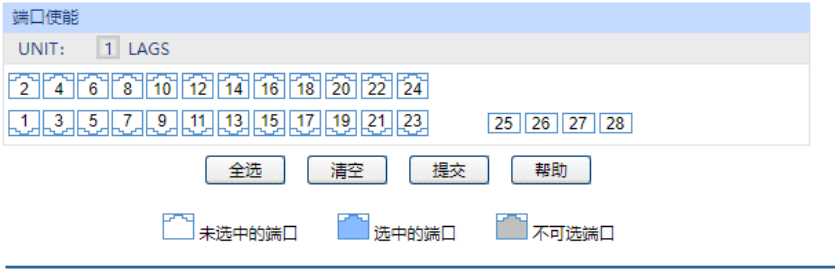


图 6-8 端口使能 MAC VLAN 特性

条目介绍：

- **端口使能**

  勾选端口启用 MAC VLAN 功能，默认情况下关闭所有端口的 MAC VLAN 功能。

MAC VLAN 配置步骤：

步骤	操作	说明
1	创建 MAC VLAN	必选操作。在 **VLAN>>MAC VLAN>>MAC VLAN** 页面创建 MAC VLAN。创建了 MAC VLAN 后，对应 MAC 地址的设备在交换机上的连接端口也必须是 VLAN 成员，才能保证正常通信。
2	端口使能	必选操作。在 **VLAN>>MAC VLAN>>端口使能**页面选择需要使能 MAC VLAN 特性的端口，点击<提交>使设置生效。

6.3 协议VLAN

协议VLAN是按照网络层协议来划分VLAN，可分为IP、IPX、DECnet、AppleTalk、Banyan等VLAN网络。这种按网络层协议来组成的VLAN，可使广播域跨越多个交换机，同时用户在

网络内部可以自由移动且无须改变其VLAN成员身份。对于希望针对具体应用和服务来管理用户的网络管理员，可通过划分协议VLAN来进行管理。

本交换机可针对常见的协议类型划分VLAN，常用协议类型值见下表。请根据实际需要创建协议VLAN。

协议类型	对应取值
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表 6-2 常用协议类型

协议VLAN中数据包处理有如下特点：

1. 当端口收到UNTAG数据包时，首先查看是否创建配置相应的协议VLAN，若已创建协议VLAN，则给数据包插入协议VLAN的TAG；若没有相应的协议VLAN，则根据接收端口的PVID值给数据包插入TAG，并将数据包在相应的VLAN中转发。
2. 当端口收到TAG数据包时，交换机按照802.1Q VLAN的方式处理该帧。如果接收端口属于携带该VLAN TAG的数据包通过，则正常转发；如果不属于，则丢弃该数据包。

划分了协议VLAN后，为了保证数据的正常传输，请将协议VLAN的使能端口设置为相应802.1Q VLAN成员。详情请查看表 6-1。

6.3.1 协议组列表

本页面中可以查看当前交换机上配置的协议VLAN，同时可以删除或编辑协议VLAN。

进入页面的方法：VLAN>>协议VLAN>>协议组列表

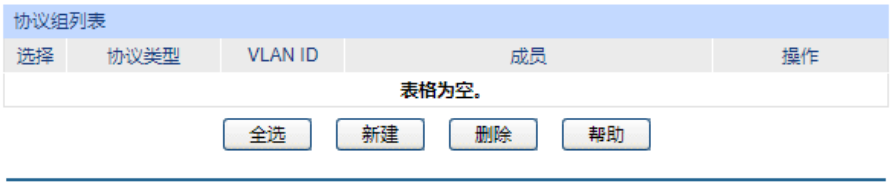


图 6-9 协议VLAN列表

条目介绍：

- **协议组列表**

  选择： 勾选条目进行删除，可多选。

协议类型：	显示协议VLAN的协议类型。
VLAN ID：	显示该协议对应的VLAN ID。
成员：	显示该协议组成员的端口号。
操作：	点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<提交>按键，使修改内容生效。

6.3.2 协议组配置

在协议组配置页面中，可以创建协议VLAN。

进入页面的方法：VLAN>>协议VLAN>>协议组配置

图 6-10 创建并查看协议 VLAN

条目介绍：

- **协议组配置**

协议类型：	选择交换机已定义的协议模板。
VLAN ID：	输入该协议VLAN对应的VLAN ID，此VLAN必须是输入端口所在的802.1Q VLAN。
协议组成员：	选择端口为该协议组成员。

6.3.3 协议模板

配置协议VLAN前应先配置协议模板，本交换机在出厂默认情况下已经定义了IP、ARP和RARP等协议模板，若需要更多的协议模板时，请在此页面中添加。

进入页面的方法：VLAN>>协议VLAN>>协议模板

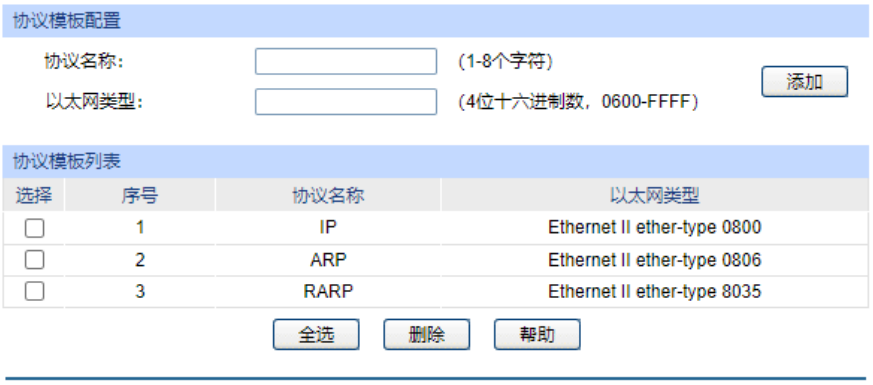


图 6-11 创建并查看协议模板

条目介绍：

- **协议模板配置**

  协议类型： 配置新定义的协议模板的名称。

  以太网协议类型： 配置该协议模板中以太网协议类型字段的值。

- **协议模板列表**

  选择： 勾选条目进行删除，可多选。

  协议类型： 显示协议模板的名称。

  以太网协议类型： 显示该协议模板中以太网协议类型字段的值。

注意：

- 当协议模板与VLAN绑定后，将无法删除协议模板。

协议VLAN配置步骤：

步骤	操作	说明
1	创建协议模板	必选操作。配置协议VLAN前应先在**VLAN>>协议VLAN>>协议模板**页面配置协议模板。
2	创建协议VLAN并使能端口	必选操作。在**VLAN>>协议VLAN>>协议组配置**页面中选择协议类型并输入VLAN ID来创建VLAN，同时选择支持协议VLAN的端口。
3	编辑/查看VLAN	可选操作。在**VLAN>>协议VLAN>>协议组列表**页面点击<编辑>按键对相应的VLAN进行编辑。

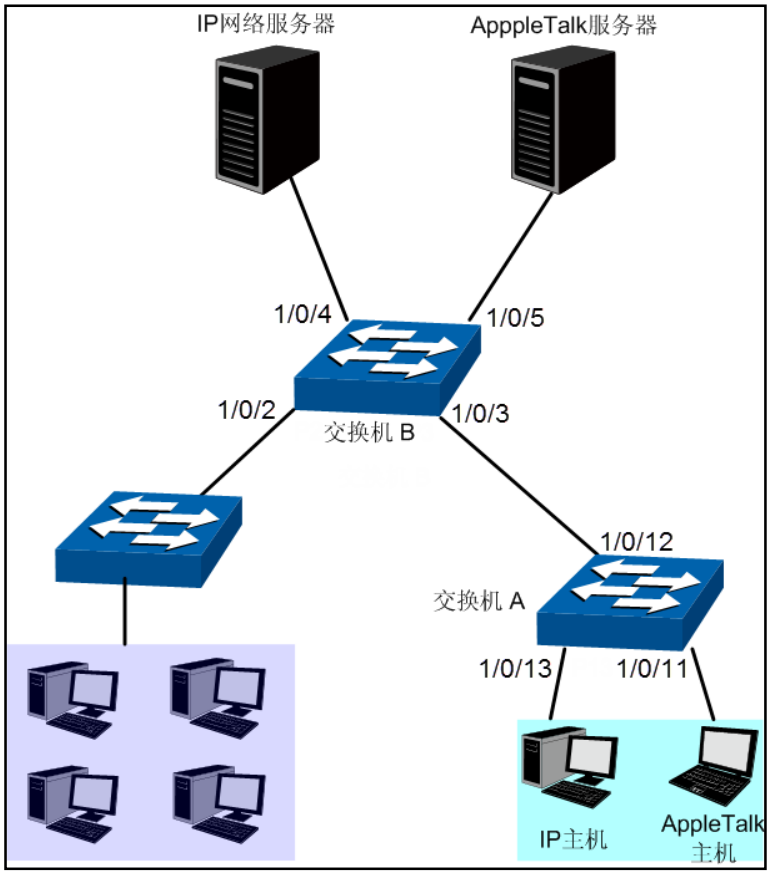
步骤	操作	说明
4	删除VLAN	可选操作。在**VLAN>>协议VLAN>>协议组列表**页面勾选相应的VLAN条目，点击<删除>按键进行删除。

6.3.4 协议VLAN功能的组网应用

➢ **组网需求**

- 平面部门通过内部交换机A的端口1/0/12连入公司局域网；
- 平面部门中分别有IP主机和AppleTalk主机；
- IP主机需要IP网络服务器提供服务，属于VLAN10；AppleTalk主机需要AppleTalk服务器提供服务，属于VLAN20；
- 交换机B分别连接了IP网络服务器和AppleTalk网络服务器。

➢ **组网图**



➢ **配置步骤**

- 配置交换机A：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面设置端口1/0/11和端口1/0/13的端口类型为ACCESS，端口12的端口类型为GENERAL。

步骤	操作	说明
2	创建VLAN10	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为10，包含Untagged端口1/0/12和1/0/13。
3	创建VLAN20	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为20，包含Untagged端口1/0/11和端口1/0/12。

- 配置交换机B：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面设置端口1/0/4和端口1/0/5的端口类型为ACCESS，端口1/0/3的端口类型为GENERAL。
2	创建VLAN10	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为10，包含Tagged端口1/0/3和Untagged端口1/0/4。
3	创建VLAN20	必选操作。在**VLAN>>802.1Q VLAN>>VLAN配置**页面中点击<新建>按键创建VLAN，VLAN ID为20，包含Tagged端口1/0/3和Untagged端口1/0/5。
4	创建协议模板	必选操作。此处请根据实际情况在**VLAN>>协议VLAN>>协议模板**页面配置协议模板。例如IP网络数据包以Ethernet II类型封装，Ether Type字段为0800；AppleTalk网络数据包以SNAP类型封装，PID字段为809B。
5	设置协议VLAN 10	在**VLAN>>协议VLAN>>协议组列表**页面中点击<新建>按键来创建协议VLAN10，关联IP协议，并勾选成员端口1/0/3。
6	设置协议VLAN 20	在**VLAN>>协议VLAN>>协议组列表**页面中点击<新建>按键来创建协议VLAN20，关联AppleTalk协议，并勾选成员端口1/0/3。

6.4 VLAN VPN

VPN（Virtual Private Network，虚拟私有网络）是随着Internet的广泛应用而迅速发展起来的一种新技术，用来实现在骨干网络上构建私人专用网络。通过在客户端或运营商接入端对指定报文进行处理，使骨干网络中的设备可以为其建立专用的传输隧道，保证数据的安全。

VLAN-VPN(Virtual Private Network)是一种简单、灵活的二层VPN技术，它通过在运营商接入端为用户的私网报文封装外层VLAN Tag，使报文携带两层VLAN Tag穿越运营商网络（骨干网）。在骨干网中，报文只根据外层VLAN Tag进行传输，用户的私网VLAN Tag则当作报文中的数据部分来进行传输。

VLAN-VPN主要可以解决如下几个问题：

（1） 为小型城域网或企业网提供一种较为简单的二层VPN解决方案。

（2） 缓解日益紧缺的公网VLAN ID资源问题。

（3） 用户可以规划自己的私网VLAN ID，不会导致和骨干网VLAN ID冲突。

（4） 当运营商升级网络时，用户网络不必更改原有配置，使用户网络具有了较强的独立性。

- 我司交换机VLAN-VPN实现方式

在本交换机中，将用户的原始VLAN称作C VLAN；而骨干网络中，运营商通常使用公网VLAN为不同的C VLAN提供服务，本交换机中将公网VLAN称为SP VLAN。在本交换机上，需要在入口端配置端口PVID为运营商的公网VLAN，以及将连接公网的端口设置为上联端口，使报文顺利穿越骨干网络到达目的地。

1. 启用VLAN-VPN功能后，不管端口收到tagged或者untagged报文，交换机都会根据PVID给报文封装外层VLAN Tag，然后通过上联端口在骨干网络中传输双Tag报文。
2. 如果开启了VLAN-VPN功能，为了保证报文能够在骨干网络中进行传输，请将连接到骨干网络的端口设置为上联端口。
3. 同时，本交换机还支持TPID值可调功能。TPID（Tag Protocol Identifier，标签协议标识）是VLAN Tag中的一个字段，IEEE802.1Q协议规定该字段的取值为0x8100。本交换机缺省采用协议规定的TPID值（0x8100）。某些厂商将网络设备可识别的TPID值设置为0x9100或其它数值。为了和这些设备兼容，本交换机提供了全局的VLAN-VPN报文TPID值可调功能，用户可以自行配置TPID值。VLAN-VPN上联端口在转发报文时会将报文外层VLAN Tag中的TPID值替换为设定值再进行发送，从而使发送到骨干网中的VLAN-VPN报文可以被其它厂商的设备识别。

   由于TPID字段在以太网报文中的位置与不带VLAN Tag的报文中协议类型字段所处位置相同，为避免网络中报文转发和接收造成混乱，用户在配置VLAN-VPN时，请勿配置TPID为表 6-3中列举的常用协议类型值。

协议类型	对应取值
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表 6-3 常用以太网数据包协议类型值

本功能包括**VPN配置**和**VLAN映射**两个配置页面。

6.4.1 VPN配置

在VPN配置页面中，可以启用交换机VPN功能、设置全局TPID值和启用上联端口。启用VPN模式后，交换机将在VLAN映射条目配置的端口对数据包的Tag标识插入外层Tag。

进入页面的方法：VLAN>>VLAN VPN>>VPN配置

图 6-12 VPN 全局功能配置

条目介绍：

- **VPN全局配置**

  VPN模式： 选择是否启用VLAN-VPN功能。

  全局TPID： 填写全局TPID。

- **VPN上联端口**

  选中端口设置为VPN上联端口，请将连接到骨干网络的端口设置为上联端口。

6.4.2 VLAN映射

VLAN映射页面可以配置基于端口的C VLAN和SP VLAN的映射关系，VLAN VPN功能将按照映射条目在指定端口添加外层VLAN Tag。

进入页面的方法：**VLAN>>VLAN VPN>>VLAN映射**

图 6-13 VLAN 映射配置

条目介绍：

- **全局配置**

  VLAN映射： 启用或禁用VLAN映射。

- **VLAN映射配置**

  端口： 选择进行VLAN映射的端口。

  C VLAN： Customer VLAN ID，数据的源VLAN。

  SP VLAN： Service Provider VLAN ID，数据的Tag标识字段将被加上SP VLAN标识。

  名称： 配置VLAN映射条目名称。

- **VLAN映射列表**

  在该表格中查看交换机上当前已配置的VLAN映射表。

VLAN VPN配置步骤：

步骤	操作	说明
1	设置全局VLAN VPN参数	必选操作。在**VLAN>>VLAN VPN>>VPN配置**功能页面，启用VPN模式功能，根据对端设备属性设置全局TPID值，并启用VPN上联端口。请将连接到骨干网络的端口设置为上联端口。
2	设置VLAN映射关系	必选操作。在**VLAN>>VLAN VPN>>VLAN映射**功能页面，配置C VLAN和SP VLAN的映射关系。

6.5 GVRP

GVRP（GARP VLAN Registration Protocol，GARP VLAN注册协议）是GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用。它通过在端口动态注册和注销VLAN信息来达到创建或删除VLAN的目的，并传播VLAN信息到其它交换机中，减少配置VLAN时烦琐的手动操作。

- **GARP简介**

GARP提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息。GARP本身不作为一个实体存在于设备中，遵循GARP协议的应用实体称为GARP应用，GVRP就是GARP的一种应用。当GARP应用实体存在于设备的某个端口上时，该端口称为GARP应用实体。

网络中的GARP应用实体之间通过传递GARP消息来完成相关的信息交换，GARP协议定义有三类消息，分别为Join消息、Leave消息和LeaveAll消息，三种消息完成相关属性信息的注册或注销。

Join消息：当一个GARP应用实体希望其它设备注册自己的属性信息时，它将对外发送Join消息；当收到其它实体的Join消息或本设备静态配置了某些属性，需要其它GARP应用实体进行注册时，它也会向外发送Join消息。

Leave消息：当一个GARP应用实体希望其它设备注销自己的属性信息时，它将对外发送Leave消息；当收到其它实体的Leave消息注销某些属性或静态注销了某些属性后，它也会向外发送Leave消息。

LeaveAll消息：每个GARP应用实体启动后，将同时启动LeaveAll定时器。当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，LeaveAll消息用来注销所有的属性，以使其它GARP应用实体重新注册本实体上所有的属性信息。

通过消息交互，所有待注册的属性信息可以传播到同一局域网中的所有GARP应用实体。

GARP消息发送的时间间隔通过定时器来控制。GARP协议定义了四种定时器，用于控制GARP消息的发送周期：

Hold定时器：当GARP应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条Join消息对外发送，而是启动Hold定时器，当该定时器超时后，GARP应用实体将此时段内收到的所有注册信息放在同一个Join消息中向外发送，从而节省带宽资源。

Join定时器：GARP应用实体可以通过将每个Join消息向外发送两次来保证消息的可靠传输，在第一次发送的Join消息没有得到回复的时候，GARP应用实体会第二次发送Join消息。两次Join消息发送之间的时间间隔用Join定时器来控制。

Leave定时器：当一个GARP应用实体希望注销某属性信息时，将对外发送Leave消息，接收到该消息的GARP应用实体启动Leave定时器，如果在该定时器超时之前没有收到Join消息，则注销该属性信息。

LeaveAll定时器：每个GARP应用实体启动后，将同时启动LeaveAll定时器，当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，以使其它GARP应用实体重新注册本实体上所有的属性信息。随后再启动LeaveAll定时器，开始新的一轮循环。

➢ **GVRP简介**

GVRP是GARP的一种应用。它基于GARP的工作机制，维护设备中的VLAN动态注册信息，并传播VLAN信息到其它设备中。

设备启动GVRP特性后，能够接收来自其它设备的VLAN注册信息，并动态更新本地的VLAN注册信息，包括当前的VLAN成员、这些VLAN成员可以通过哪个端口到达等；同时设备能够将本地的VLAN注册信息向其它设备传播，以便使同一局域网内所有设备的VLAN信息一致。GVRP传播的VLAN注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

在本交换机中，只有TRUNK类型端口才能作为GVRP应用实体，维护交换机的VLAN注册信息。GVRP的端口注册模式有三种：Normal、Fixed和Forbidden，各模式描述如下：

Normal模式：允许该端口动态注册、注销VLAN，传播动态VLAN以及静态VLAN信息。

Fixed模式：禁止该端口动态注册、注销VLAN，只传播静态VLAN信息，不传播动态VLAN信息。Fixed模式的端口只允许本端口所属的静态VLAN信息通过。

Forbidden模式：禁止该端口动态注册、注销VLAN，不传播除VLAN1以外的任何的VLAN信息。Forbidden模式的端口，只允许系统默认VLAN（VLAN1）通过。

进入页面的方法：VLAN>>GVRP>>GVRP配置

图 6-12 配置GVRP

条目介绍：

- **全局配置**

GVRP功能： 选择是否启用交换机的GVRP功能。

- **端口配置**

UNIT： 选择一个 UNIT 显示端口信息。

选择： 勾选端口，配置端口GVRP功能参数，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。端口启用GVRP功能之前需要将端口类型设置为Trunk。

注册模式： 选择端口的注册模式。

- Normal模式：允许该端口动态注册、注销VLAN，传播动态VLAN以及静态VLAN信息。
- Fixed：禁止该端口动态注册、注销VLAN，只传播静态VLAN信息，不传播动态VLAN信息。
- Forbidden：禁止该端口动态注册、注销VLAN，只允许缺省VLAN通过。

LeaveAll定时器： 每个端口启动GARP后，同时启动LeaveAll定时器，端口将对外循环发送LeaveAll消息，以使其它端口重新注册其所有的属性信息。LeaveAll定时器的取值范围为1000-30000厘秒。

Join定时器： GARP端口可以将每个Join数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用Join定时器来控制。Join定时器的取值范围为20-1000厘秒。

Leave定时器： 接收到Leave数据包的GARP端口启动Leave定时器，如果在该定时器超时之前没有收到Join数据包，则注销相应属性信息。Leave定时器的取值范围为60-3000厘秒。

LAG： 显示端口当前所属的汇聚组。

注意：

- 若启用了LAG组成员端口的GVRP功能，请保持所有成员端口的状态和注册模式一致。
- LeaveAll定时器要大于等于10倍Leave定时器，而Leave定时器要大于等于2倍Join定时器。

GVRP配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面将端口类型设置为TRUNK。
2	启用GVRP功能	必选操作。在**VLAN>>GVRP>>GVRP配置**页面启用GVRP功能。

3	配置端口的注册模式以及各定时器时长。	必选操作。在**VLAN>>GVRP>>GVRP配置**页面中根据实际应用情况设置端口的参数并启用端口。

6.6 Private VLAN

Private VLAN功能采用了分层结构，将多个Secondary VLAN与一个Primary VLAN组成VLAN对，下层用户通过Secondary VLAN相互之间进行二层报文隔离，上层设备仅需识别Primary VLAN从而节约了VLAN资源，解决了上层设备VLAN资源短缺以及传统VLAN中的广播问题。

在园区网和企业接入网中，为了保证用户信息安全，要求对接入用户进行认证接入并相互隔离，通过VLAN进行隔离是最常见的隔离方式。随着接入用户的数量日益增长，用传统VLAN的隔离方式将消耗大量的VLAN资源，上层设备为了识别所有的VLAN，不得不建立数量庞大的VLAN。然而，根据IEEE 802.1Q协议标准定义的4个字节的VLAN Tag，其中12bits用于表示VLAN ID，这也就限制的网络设备可识别的VLAN数最多为4094个。在VLAN资源消耗殆尽的情况下，Private VLAN功能应运而生，常用网络模型如下图 6-14 示。

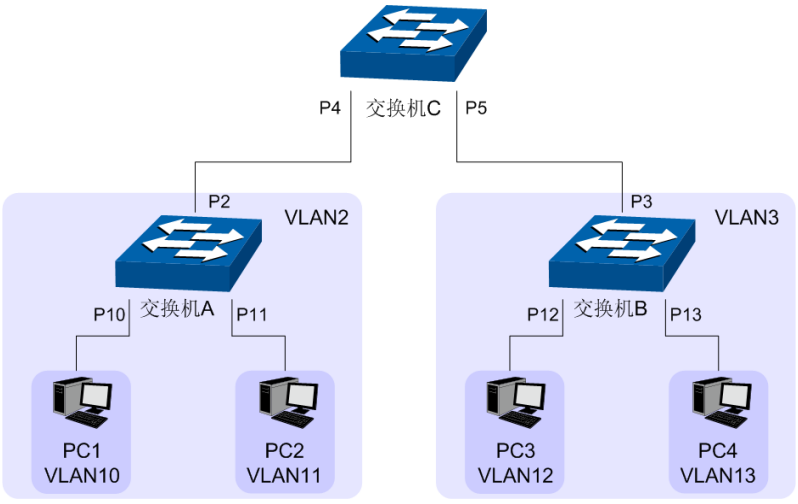


图 6-14 Private VLAN 网络模型

在图 6-14中，交换机A和交换机B分别运用Private VLAN功能，建立Secondary VLAN将终端相互隔离，并将Secondary VLAN与Primary VLAN组成VLAN对，上层设备交换机C只需识别Primary VLAN。

- **我司交换机的Private VLAN实现方式**

Private VLAN功能基于802.1Q VLAN建立Primary VLAN和Secondary VLAN的包含关系，通过这种包含关系，上联设备只需识别Primary VLAN信息，下联设备只需识别Secondary VLAN信息。

Primary VLAN： 上行设备感知的用户VLAN，不是用户真正所属的VLAN，一个Primary VLAN可以和多个Secondary VLAN建立包含关系，用于转发上层设备和Secondary VLAN之间的通信数据。

Secondary VLAN： 用户真正属于的VLAN，将用户划分到不同的Secondary VLAN中，Secondary VLAN之间相互隔离。

Secondary VLAN有两种类型，Community VLAN和Isolated VLAN。Community VLAN中的成员相互之间可以直接通信，Isolated VLAN中的成员相互隔离。

- **Private VLAN配置要点**

如图 6-14示，以图中的交换机A为例介绍我司交换机的Private VLAN功能，以下为功能配置要点。

（1） 交换机A建立Private VLAN 2/10（Primary VLAN为VLAN 2，Secondary VLAN为VLAN10，下面格式同此处）和Private VLAN 2/11。

（2） 交换机A的端口1/0/10和端口1/0/11作为Host类型端口连接终端用户，分别加入不同的Private VLAN，通过不同的Secondary VLAN相互之间进行隔离。端口1/0/2作为Promiscuous类型端口连接上层设备，通过Primary VLAN 2向上层设备交换机C屏蔽本交换机上的Secondary VLAN的信息。

（3） 交换机A内部执行端口同步机制。创建了Private VLAN 2/10和Private VLAN 2/11后，端口1/0/10和端口1/0/11同时成为Primary VLAN 2的成员端口，端口PVID为各自所属的Secondary VLAN，出口规则为UNTAG；端口1/0/2连接上层设备，同时也同步到Secondary VLAN中成为VLAN成员端口，PVID为Primary VLAN ID，出口规则为UNTAG。

本功能配置简单，包括**PVLAN配置**和**端口配置**两个配置页面。

6.6.1 PVLAN配置

在PVLAN配置页面中，可以创建Private VLAN，将Primary VLAN和Secondary VLAN关联。

进入页面的方法：VLAN>>Private VLAN>>PVLAN配置

图 6-15 PVLAN 配置

条目介绍：

- **Private VLAN创建**

Primary VLAN：	填写Primary VLAN ID。
Secondary VLAN：	填写Secondary VLAN ID。
Secondary VLAN类型：	选择Private VLAN的Secondary VLAN类型。

- **查找条目**

查找选项：	当创建的Private VLAN数过多时，可通过指定的Primary VLAN或Secondary VLAN查找相应的Private VLAN条目。

- **Private VLAN列表**

选择：	勾选条目进行删除或修改交换机Private VLAN配置信息，可多选。
Primary VLAN：	显示Private VLAN的Primary VLAN ID。
Secondary VLAN：	显示Private VLAN的Secondary VLAN ID。
VLAN类型：	显示Secondary VLAN Type类型。
端口成员：	显示Private VLAN的成员端口。

注意:

- 为避免响应时间过长，建议每次创建Private VLAN数量少于10个。
- 一个Private VLAN包含一个Primary VLAN和一个Secondary VLAN。
- 一个VLAN只能是Primary VLAN和Secondary VLAN中的一种。

6.6.2 端口配置

在本页面中，可以根据端口在网络中的连接状态配置端口类型，并将端口添加到Private VLAN中。

进入页面的方法：VLAN>>Private VLAN>>端口配置

图 6-16 端口配置

条目介绍：

- **端口配置**

选择的端口： 在此处选择需配置的端口号。你可以手动输入一个或者从下面的端口列表中选择一个。

端口类型： 选择端口类型。

- Promiscuous：和上行设备相连，负责和上行设备通信。
- Host：和下行设备相连，负责和下行设备通信。

Primary VLAN： 填写该端口加入的Primary VLAN。

Secondary VLAN： 填写该端口加入的Secondary VLAN。

- **Private VLAN端口列表**

端口号： 显示Private VLAN的端口号。

端口类型： 显示端口在Private VLAN中的端口类型。

操作： 删除Private VLAN的成员端口。

注意：

- 一个Host端口只能加入一个Private VLAN。
- 一个Promiscuous只能加入一个Primary VLAN。
- 如果需要把Promiscuous端口加入多个Private VLAN中且Primary VLAN相同时，只需把Promiscuous端口加入任意一个Private VLAN即可，端口将自动同步到其它Private VLAN。

Private VLAN配置步骤：

步骤	操作	说明
1	创建Private VLAN	必选操作。在**VLAN>>Private VLAN>>PVLAN配置**功能页面创建Private VLAN。

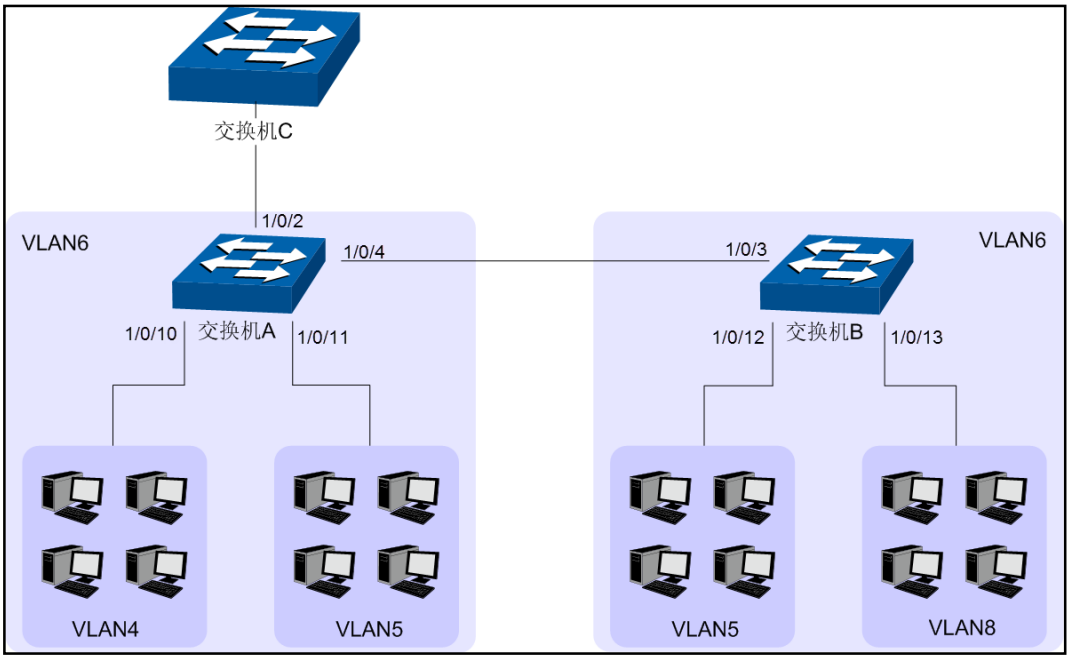
2	配置成员端口	必选操作。在**VLAN>>Private VLAN>>端口配置**功能页面，设置端口属性并将端口添加到Private VLAN中。

6.6.3 Private VLAN功能的组网应用

- **组网需求**

- ISP向某公司提供了网络接入服务，连接到ISP机房的接入交换机A上，并通过VLAN6向企业提供网络服务；
- 企业中心交换机上连接了许多用户，各用户之间要求通过VLAN功能进行二层隔离；
- 中心交换机向下级联了另外一台汇聚层交换机，汇聚层交换机上配置了VLAN功能，部分VLAN要求和中心交换机上的VLAN进行连通，且所连接的用户均能够访问网络。

- **组网图**



- **配置步骤**

- 配置交换机A：

步骤	操作	说明
1	创建Private VLAN	必选操作。在**VLAN>>Private VLAN>>PVLAN配置**页面设置创建Private VLAN 6/4和Private VLAN 6/5。
2	为Private VLAN添加端口	必选操作。在**VLAN>>Private VLAN>>端口配置**页面，配置端口1/0/10的端口类型为Host并添加到Private VLAN 6/4中；配置端口1/0/11的端口类型为Host并添加到Private VLAN 6/5中；配置端口1/0/2和端口1/0/4的端口类型为Promiscuous并添加到Private VLAN 6/4中。

- 配置交换机B：

步骤	操作	说明
1	创建 Private VLAN	必选操作。在**VLAN>>Private VLAN>>PVLAN配置**页面设置创建Private VLAN 6/5和Private VLAN 6/8。
2	为 Private VLAN 添加端口	必选操作。在**VLAN>>Private VLAN>>端口配置**页面，配置端口1/0/12的端口类型为Host并添加到Private VLAN 6/5中；配置端口1/0/13的端口类型为Host并添加到Private VLAN 6/8中；配置端口1/0/3的端口类型为Promiscuous并添加到Private VLAN 6/5中。

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
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

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 2 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。

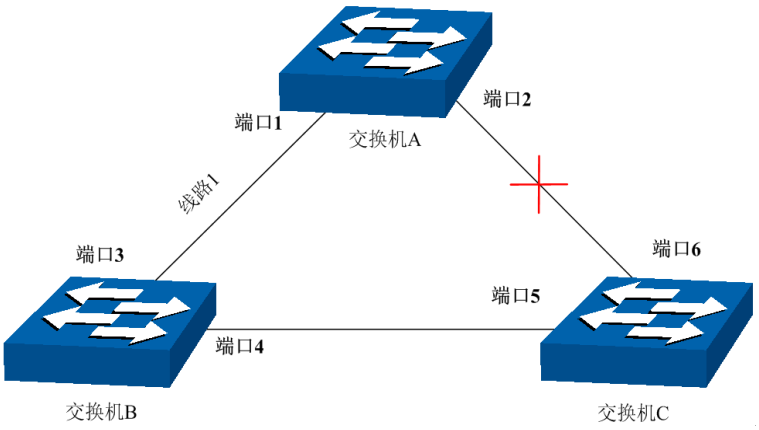


图 7-1 生成树基本概念组网图

➢ **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。
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： • 根桥 ID 替换为根端口的根桥 ID； • 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； • 指定桥 ID 替换为自身设备的 ID； • 指定端口 ID 替换为自身端口 ID。
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： • 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。 • 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；

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。

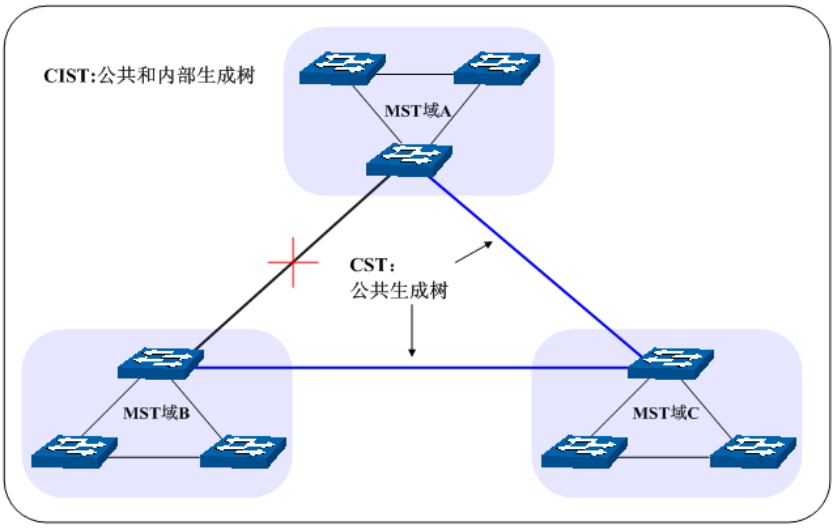


图 7-2 MSTP 基本概念组网图

➢ **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。

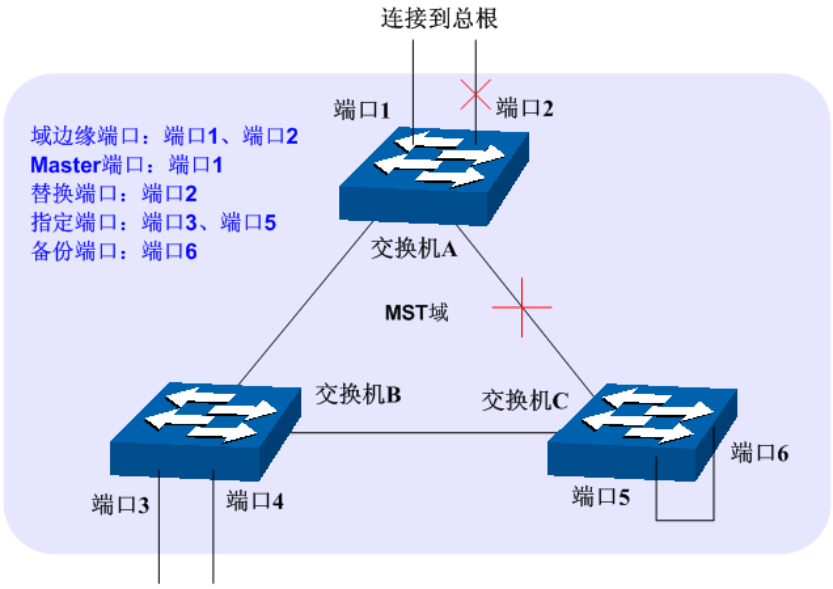


图 7-3 端口角色示意图

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

配置生成树前请明确各交换机在每个生成树实例中的地位，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

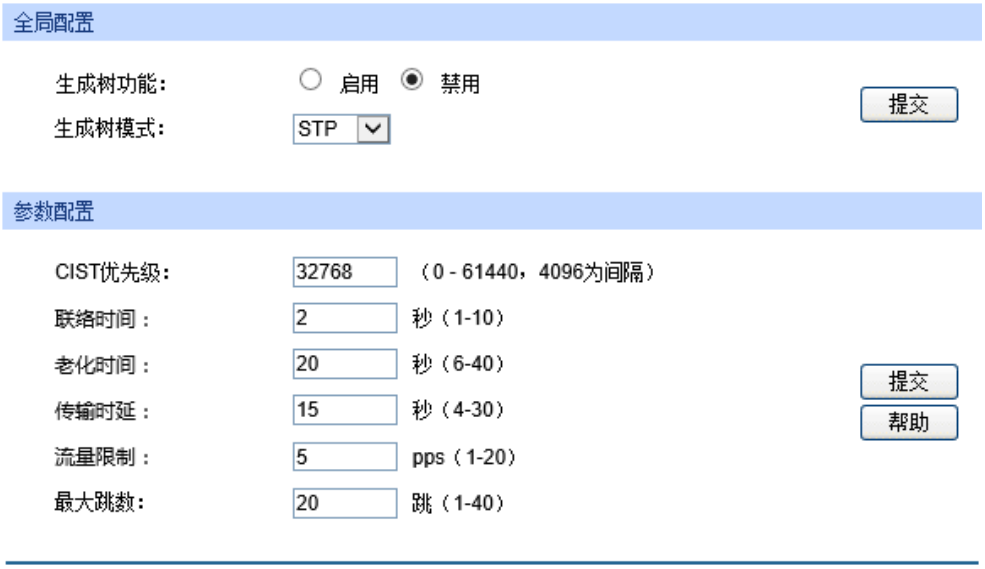


图 7-4 基本配置

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×(联络时间+1)≤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×(传输延时－1)≥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度。默认为 5pps。
最大跳数：	填写协议报文被转发的最大跳数，它限制了生成树的规模。默认为 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

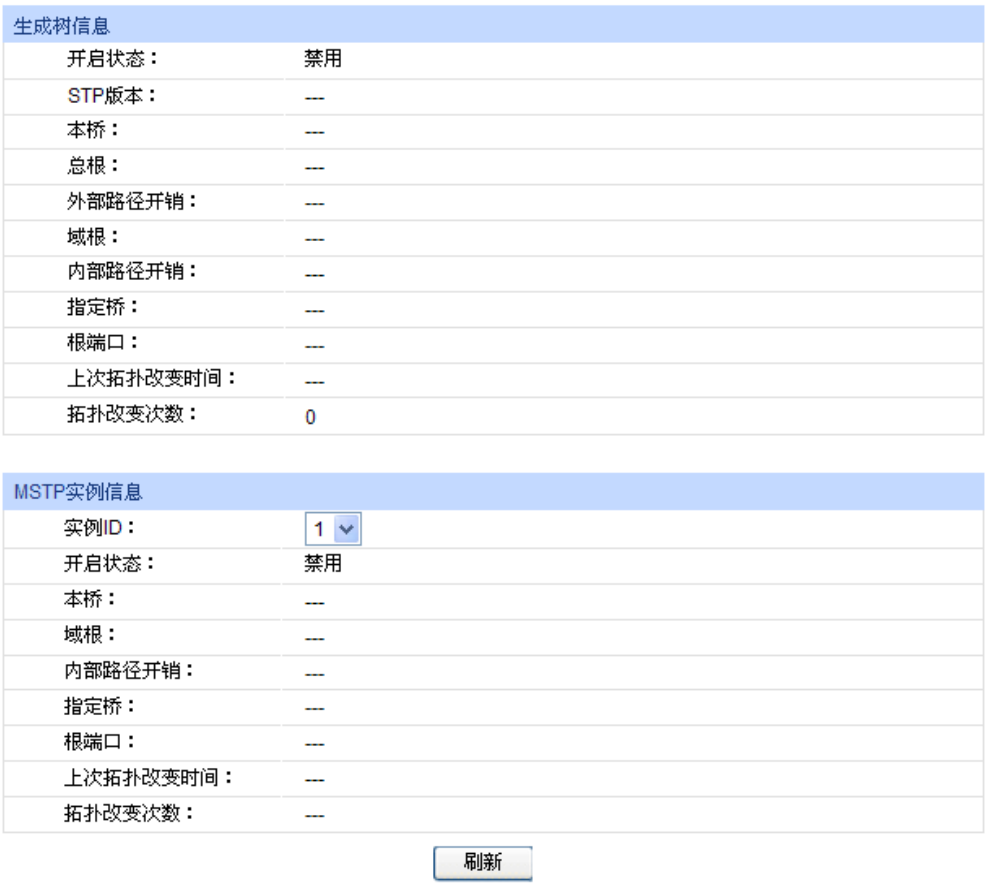


图 7-5 基本信息

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

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，却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

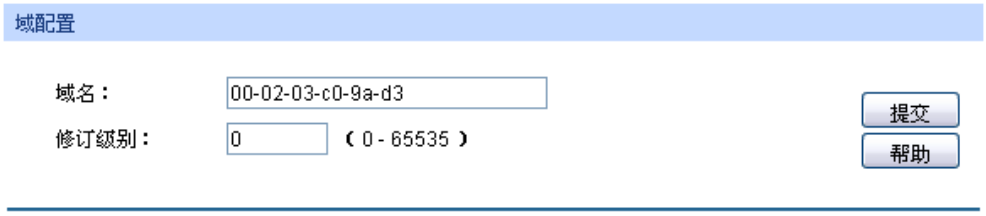


图 7-7 域配置

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。请按需要将 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

图 7-8 实例配置

条目介绍：

- **VLAN-实例映射**

实例 ID：	填写实例 ID。
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。

- **实例配置**

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：	选择是否启用相应实例。
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。

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

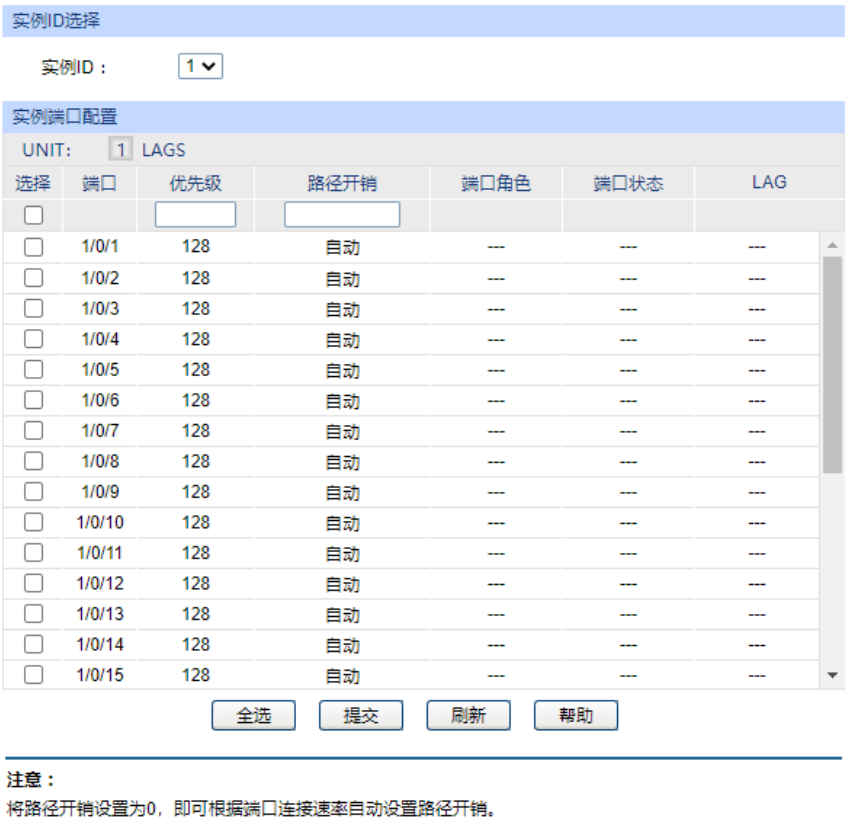


图 7-9 实例端口

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，建议对符合条件的端口启用保护功能。

进入页面的方法：生成树>>安全配置>>端口保护

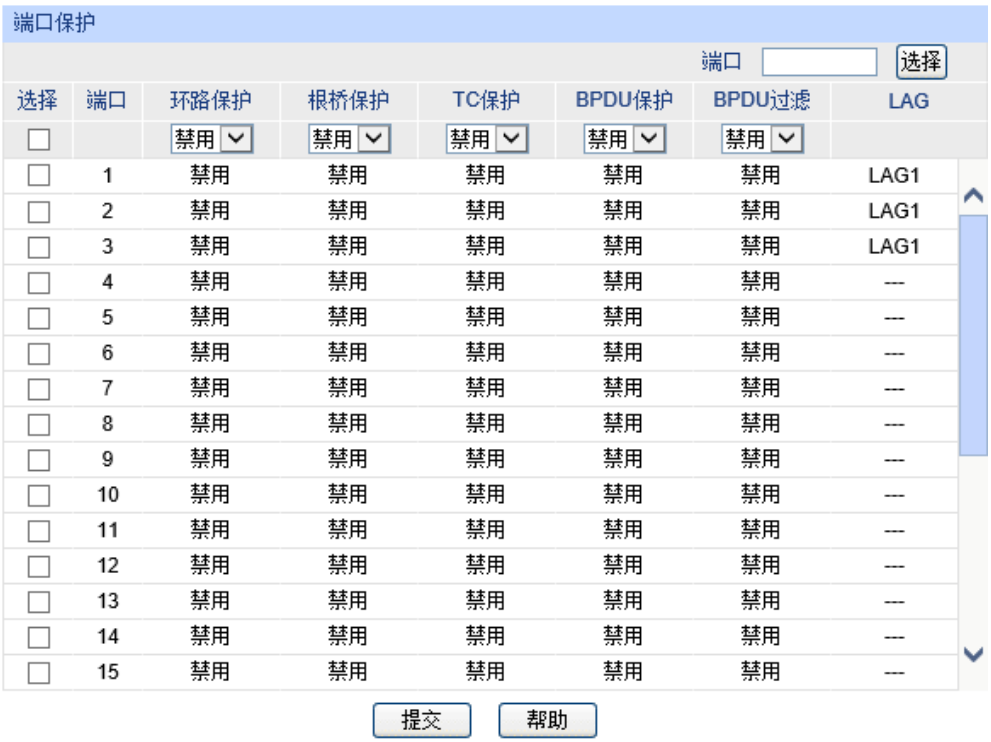


图 7-10 端口保护

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

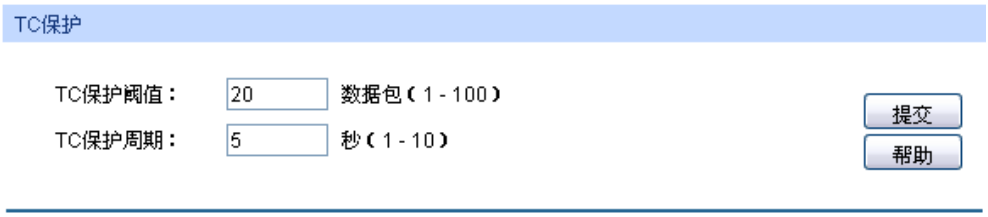


图 7-11 TC 保护

条目介绍：

- **TC 保护**

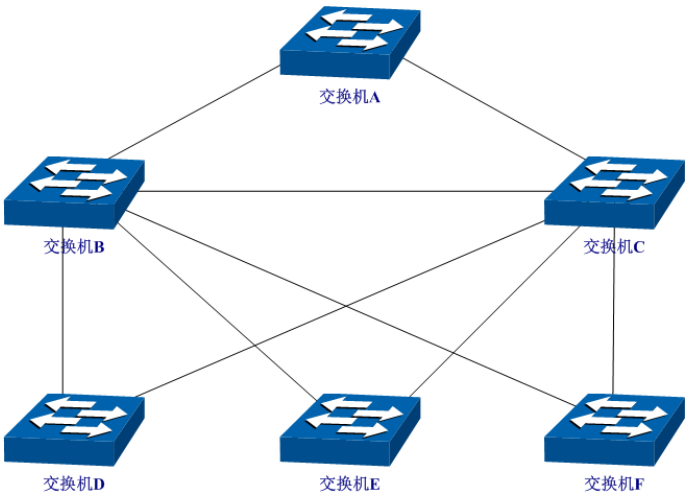
TC 保护阈值：	在 TC 保护周期内，交换机收到 TC 报文的最大数目。超过该数目后，交换机在该周期内不再进行地址表删除操作。默认为 20 数据包。
TC 保护周期：	填写 TC 保护的周期。默认为 5 秒。

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，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
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，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
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。

步骤	操作	说明
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，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
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

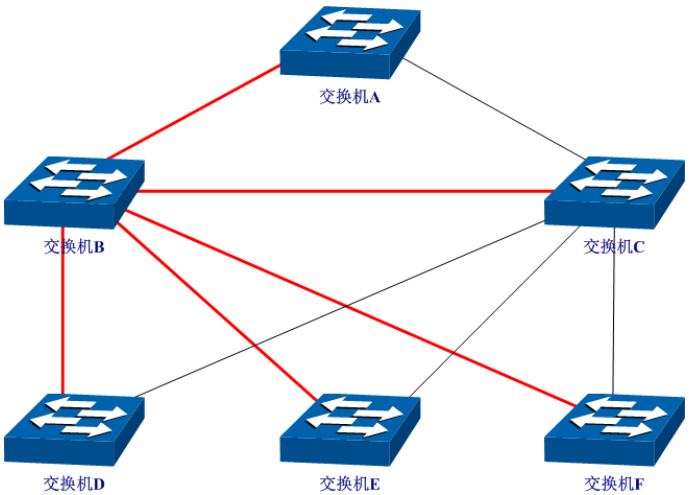
步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为 Trunk，并将端口加入 VLAN 101 到 VLAN 106。具体配置方法请参见 6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。

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。

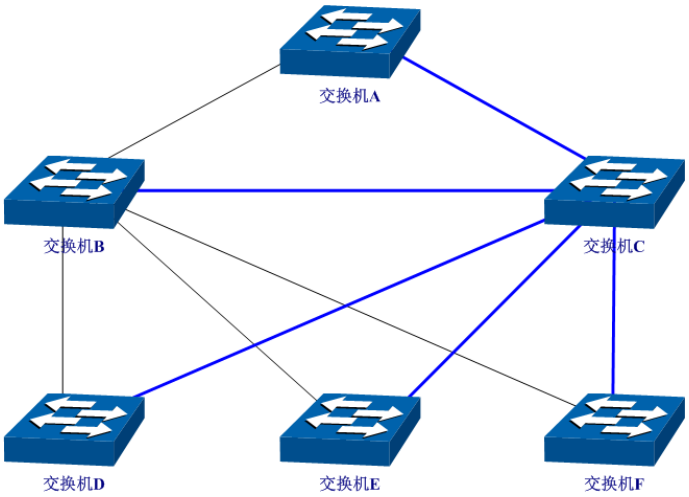
- 交换机 E 和交换机 F 的配置方法同交换机 D

➢ **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。

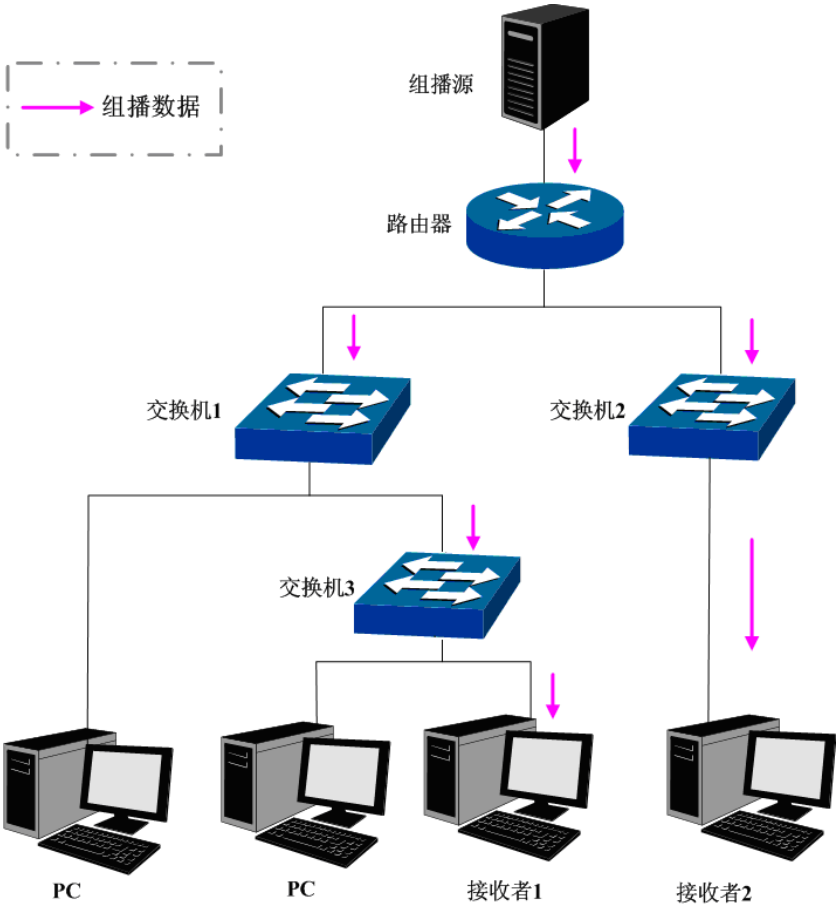


图 8-1 组播传输信息的方式

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**

1. 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

2. 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：

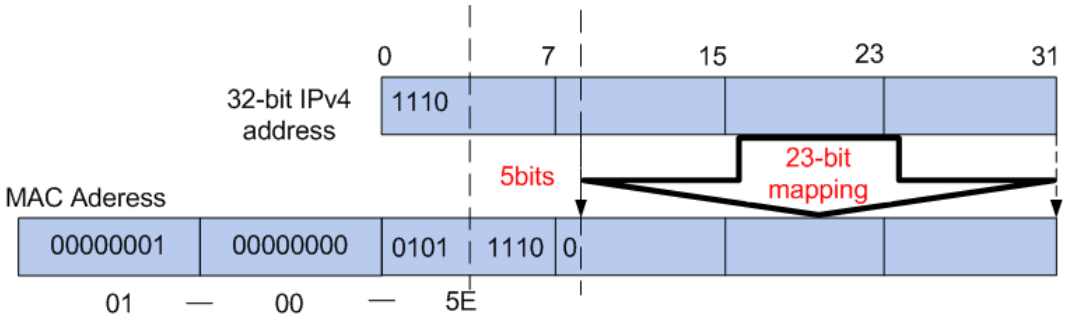


图 8-2 IPv4 组播 MAC 地址和组播 IP 地址的对应关系

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转发到每一个端口，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，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。

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，如果交换机没有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 配置**、**组播 VLAN**、**查询器配置**、**Profile 配置**、**Profile 绑定**和**报文统计**八个配置页面。

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

图 8-4 基本配置

条目介绍：

- **基本配置**

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。
Report 报文抑制：	选择是否开启 Report 报文抑制功能，如果开启该功能，则特定组播组的第一个 Report 报文将发往路由器端口，接下来的 Report 报文将被抑制，不发往路由器端口。Report 报文抑制功能有助于减少网络中 IGMP 数据包的流量。
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。
成员端口时间：	在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。
最后监听成员查询间隔：	输入最后监听成员查询间隔时间。当组播组没有其他组播成员端口，将会按照查询间隔发送特定组查询报文检查是否还有其他组播成员。
最后监听成员查询次数：	输入最后监听成员查询次数。当组播组没有其他组播成员端口，将会发送该次数的特定组查询报文检查是否还有其他组播成员。

- **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 端口配置

在此页面可以启用或禁用端口 IGMP 侦听功能和快速离开功能。

进入页面的方法：组播管理>>IGMP 侦听>>端口配置

图 8-6 端口配置

条目介绍：

- **端口配置**

UNIT：	选择一个 UNIT 显示端口信息。
选择：	勾选条目配置端口的 IGMP 侦听功能，可多选。
端口号：	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 配置

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 配置

图 8-7 VLAN 配置

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。
静态路由端口：	填写静态配置的路由器端口，多用于拓扑稳定的网络中。

- **VLAN 列表**

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。
静态路由器端口：	显示 VLAN 的静态路由器端口。
动态路由器端口：	显示 VLAN 的动态路由器端口。

操作： 对单个条目进行相应操作。

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**组播管理>>IGMP 侦听>>基本配置、端口配置**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**组播管理>>IGMP 侦听>>VLAN 配置**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

图 8-8 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。
动态路由器端口：	显示组播 VLAN 的动态路由器端口。
静态路由端口：	选择静态配置的路由器端口，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 中的成员端口的端口类型推荐为 GENERAL。
- 组播 VLAN 中的路由器端口的端口类型必须配置为 TRUNK 或者是出口规则为“带 tag”的 GENERAL 端口，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。

- 当建立了组播 VLAN 后，所有的 IGMP 报文均只在组播 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。
2	创建组播 VLAN	必选操作。在 **VLAN>>802.1Q VLAN** 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。 ● 配置成员端口的端口类型为 GENERAL。 ● 配置路由端口的端口类型为 TRUNK 或出口规则为“带 tag”的 GENERAL。
3	配置组播 VLAN 的参数	可选操作。进入**组播管理>>IGMP 侦听>>组播 VLAN** 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**组播管理>>IGMP 侦听>>基本配置**页面中的“已启用的 VLAN”条目处，显示组播 VLAN 的 VLAN ID。

8.1.5 查询器配置

在运行了IGMP的组播网络中，需要一台三层组播设备充当IGMP查询器，负责发送IGMP查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。而网络中的二层设备可以通过侦听三层组播设备与主机之间交互的IGMP报文来建立二层组播转发表项，实现二层组播转发。但是，在一个没有三层组播设备的网络中，由于没有设备负责IGMP查询器的功能，这样网络中不会周期性存在IGMP协议交互的报文，二层设备也无法通过侦听IGMP报文来建立二层的组播转发表项。为了解决这个问题，可以在二层设备上使用IGMP侦听查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。本页面主要用于配置IGMP侦听查询器的相关参数。

进入页面的方法：组播管理>>IGMP侦听>>查询器配置

图8-9 查询器配置

条目介绍：

- **IGMP侦听查询器配置**

VLAN ID：	输入需要启动查询器特性的VLAN ID。
查询间隔：	输入查询间隔时间。查询器会按照间隔时间发送通用查询报文。
最大响应时间：	输入查询报文的最大响应时间字段的值。
通用查询报文源IP：	输入通用查询报文源IP地址。

- **IGMP侦听查询器列表**

查看IGMP侦听查询器的详细配置参数。

8.1.6 Profile配置

本界面主要配置需要过滤的组播地址段。

进入页面的方法：组播管理>>IGMP侦听>>Profile配置

图 8-10 创建Profile

条目介绍：

- **创建IGMP Profile**

Profile ID：	输入Profile ID，区间为1-999。
模式：	配置该Profile的过滤模式。 ● 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。

- **显示设置**

显示设置： 选择IGMP Profile信息的显示规则，可以帮助您快速查找到所需的条目。

- 全部：显示全部IGMP Profile信息。
- Profile ID：输入欲查找条目需包含的Profile ID。

➢ **IGMP Profile信息**

选择： 勾选后可以删除Profile条目。

Profile ID： 显示Profile ID。

模式： 显示Profile的过滤模式。

绑定端口： 显示当前绑定了该Profile的端口。

操作： 点击<编辑>按键为Profile添加具体的过滤组播地址，如下图所示。

图 8-11 为Profile添加过滤组播地址

条目介绍：

➢ **Profile模式**

Profile ID： 显示Profile ID。

模式： 修改该Profile的过滤模式，需提交才能生效。

➢ **添加IP范围**

起始地址： 显示过滤地址段的起始组播IP地址。

结束地址： 显示过滤地址段的结束组播IP地址。

➢ **IP范围**

选择： 勾选后可以删除IP地址段条目。

序号： 显示IP地址段的序列号。

起始地址： 显示IP地址段的起始组播IP地址。

结束地址： 显示IP地址段的结束组播IP地址。

8.1.7 Profile绑定

本页用来配置端口与Profile进行绑定，使组播过滤功能生效。

进入页面的方法：组播管理>>IGMP侦听>>Profile绑定

图 8-12 Profile绑定

条目介绍：

- **Profile与最大加入组数目绑定**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

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。

Profile ID： 配置端口绑定的Profile组播过滤文件。

最大加入组数目： 配置端口可以加入到最大组播组数目。

溢出操作： 当端口所加入组播组数已达到最大组播组数时，如果要加入更多的组播组，交换机将执行的动作。

- 丢弃：不再加入新的组播组。
- 替换：端口加入新的组播组，并将端口从当前已加入的组播组IP地址最小的组播组中移除。

LAG： 显示端口当前所属的汇聚组。

清除绑定： 清除端口绑定的Profile。

注意：

Profile绑定设置对静态组播IP不生效。

配置步骤：

步骤	操作	说明
1	配置Profile	必选操作。在**组播管理>>IGMP侦听>>Profile配置**页面，创建Profile并设置组播过滤地址。
2	配置端口的组播过滤规则	必选操作。在**组播管理>>IGMP侦听>>Profile绑定**页面，配置端口与Profile绑定。

8.1.8 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>>IGMP侦听>>报文统计

图 8-13 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。

- **报文统计**

端口： 显示交换机的端口号。

查询报文： 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。

8.1.9 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。

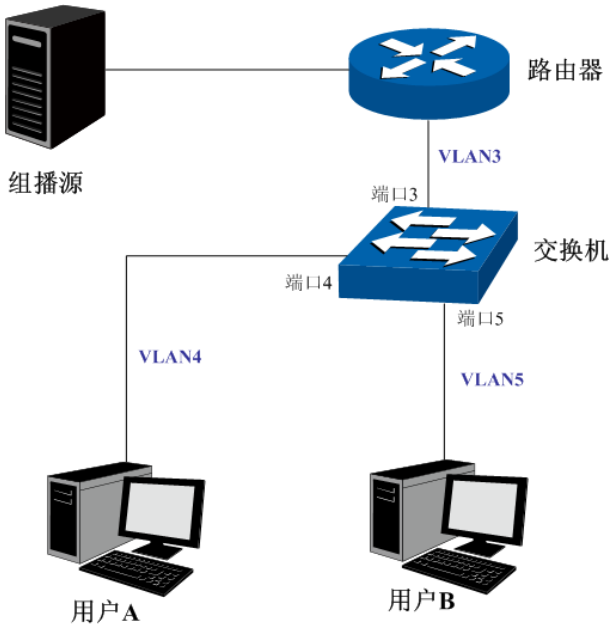
交换机：端口 3 与路由器相连，且通过 VLAN3 转发数据；端口 4 与用户 A 相连，且通过 VLAN4 转发数据；端口 5 与用户 B 相连，且通过 VLAN5 转发数据。

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 **VLAN>>802.1Q VLAN** 功能处，创建 VLAN3、4、5，并将 VLAN3 的描述填写为“组播 VLAN”。
2	配置端口属性	在 **VLAN>>802.1Q VLAN** 功能处。 配置端口 3 的端口类型为 GENERAL，出口规则 TAG，并加入 VLAN3、4、5 中。 配置端口 4 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、4 中。 配置端口 5 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、5 中。
3	启用 IGMG 侦听	在**组播管理>>IGMP 侦听>>基本配置**页面，启用 IGMP 侦听功能。 在**组播管理>>IGMP 侦听>>端口配置**页面，启用端口 3、4、5 的 IGMP 侦听功能。
4	启用组播 VLAN	在组播管理>>IGMP 侦听>>组播 VLAN 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	在组播管理>>IGMP 侦听>>基本配置页面，“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。

8.2 MLD 侦听

- **MLD 侦听概述**

MLD（Multicast Listener Discovery，组播侦听发现协议）侦听运行在二层网络中，负责管理 IPv6 组播数据在组播路由器和主机之间的传输。通过 MLD 侦听机制，交换机将 IPv6 组播数据有选择地转发给需要它的主机，而不是在整个 VLAN 中扩散。交换机通过 IPv6 组播控制数据包来创建和维护这些主机所对应的组播转发表。MLD 侦听在 IPv6 网络中的作用与 IGMP 侦听在 IPv4 网络中相似。

交换机侦听用户主机与路由器之间的交互 MLD 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（MLD 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（MLD Done）时，交换机会发送该端口的特定组查询报文（Multicast-Address-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若交换机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（MLD 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。

- **MLD 侦听的基本概念**

1. MLD 报文

查询报文（MLD Queries）：由 MLD 路由器发出，分为通用查询报文（General Queries）和特定组查询报文（Multicast-Address-Specific Queries，MASQs）。

报告报文（MLD Reports）：由主机发出，当主机想主动加入某一组播组或者对 MLD 查询报文给予响应时产生此种报文。

离开报文（MLD Done Messages）：主机离开 IPv6 组播组时会发送离开报文，以通知 IPv6 组播路由器自己离开了某个组播组。

2. 交换机上的相关端口

路由器端口（Router Port）：交换机中连接或者朝向路由器的端口被称为路由器端口。

成员端口（Member Port）：交换机中连接或者朝向组播成员的端口被称为成员端口。

3. 相关定时器

路由器端口老化时间（Router Port Aging Time）：这段时间内，如果交换机没有从路由器端口接收到查询报文，就会将此端口从路由器端口列表里删除。默认时间为 260 秒。

成员端口老化时间（Member port aging time）：这段时间内，如果交换机没有从成员端口接收到报告报文，就会将此端口从 MLD 组播地址表里删除。默认时间为 260 秒。

通用查询间隔（General Query Interval）：组播路由器发送通用查询报文的时间间隔。

特定组查询间隔（Last Listener Query Interval）：交换机发送特定组查询报文的时间间隔。

特定组播组查询计数（Last Listener Query Count）：当一个 IPv6 组播组因为未收到 MLD Report 报文而老化前，组播路由器发送特定组查询报文的个数。

- **MLD 侦听的工作过程**

1. 通用查询

MLD 查询路由器定时向本地网段发出通用查询报文（MLD General Query message），以查询该网段内有哪些 IPv6 组播组成员。交换机收到通用查询报文后，会将此报文向它的接收端口所在 VLAN 的所有其他端口转发，并对接收端口作相应处理：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，并启用路由器端口的老化时间；如果是已有路由器端口，则直接重置该路由器端口的老化时间。

2. 成员关系报告

当主机主动加入某一组播组或者对路由器查询报文进行响应时，会发送成员关系报告报文（MLD Report message）。交换机收到 MLD 报告报文后，会将此报文通过接收它的端口所在 VLAN 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，如果组播地址对应的组播组不存在，则新建组播组条目。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，则将其加入到组播组的转发列表中，并启用该端口的成员端口老化时间；如果接收端口已经存在于转发列表中，则直接重置其成员端口老化时间。

3. 成员离开

当主机离开 IPv6 组播组时，会发送 MLD 离开报文（MLD Done message），以通知组播路由器自己离开了某个组播组。

如果接收离开报文的端口所在的 VLAN 没有开启快速离开功能，交换机在收到离开报文后，会向该端口发送特定组查询报文（MASQs），以检测该端口下是否还有同一个组播组的成员存在。特定组查询报文的发送间隔和发送个数由用户配置，如果在最大响应时间内此端口上没有收到对应的报告报文，交换机就会将此端口从组播组的转发列表里删除，并将此离开报

文通过该 VLAN 内所有的路由器端口转发出去。

MLD 侦听是在 IPv6 中运行在二层交换机上的组播协议。交换机开启了 MLD 侦听功能之后，IPv6 组播数据将只会从希望得到这些数据的一系列端口转发出去，而不是在这个 VLAN 的所有端口中广播，减少网络中的数据流量。MLD 侦听机制利用 IPv6 组播控制报文来控制组播数据流的转发。

8.2.1 基本配置

您可以在此处配置 MLD 侦听的全局功能和查看 MLD 侦听的启用信息。

入页面的方法：组播管理>>MLD 侦听>>基本配置

图 8-14 基本配置

条目介绍：

- **全局配置**

MLD 侦听： 选择是否启用交换机的 MLD 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，需要全局使能 MLD 侦听功能。

Report 报文抑制： 选择是否开启 Report 报文抑制功能，如果开启该功能，则特定组播组的第一个 Report 报文将发往路由器端口，接下来的 Report 报文将被抑制，不发往 路由器端口。Report 报文抑制功能有助于减少网络中 MLD 数据包的流量。

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。

成员端口时间： 在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。

最后监听成员查询间隔： 输入最后监听成员查询间隔时间。当组播组没有其他组播成员端口，将会按照查询间隔发送特定组查询报文检查是否还有其他组播成员。

最后监听成员查询次数： 输入最后监听成员查询次数。当组播组没有其他组播成员端口，将会发送该次数的特定组查询报文检查是否还有其他组播成员。

- **MLD 侦听信息**

描述： 显示 MLD 侦听的配置项。

成员： 显示对应配置项的成员。

8.2.2 端口配置

在此页面可以启用或禁用端口 MLD 侦听功能和快速离开功能。

进入页面的方法：组播管理>>MLD 侦听>>端口配置

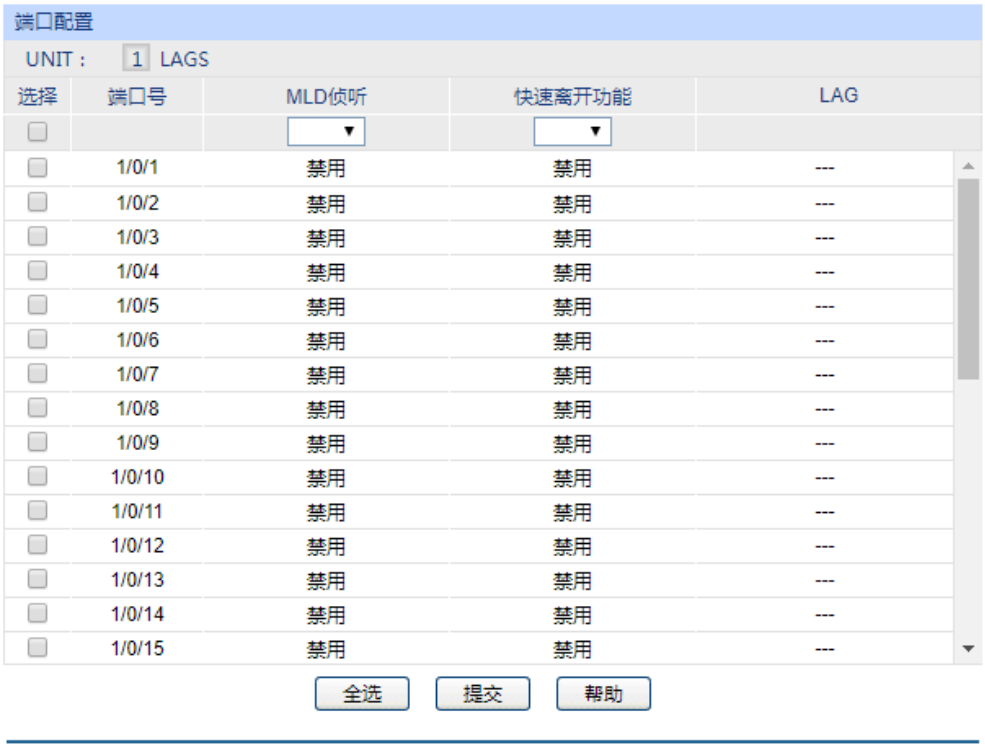


图 8-15 端口配置

条目介绍：

- **端口配置**

UNIT： 选择一个 UNIT 显示端口信息。

选择： 勾选条目配置端口的 MLD 侦听功能，可多选。

端口号： 显示交换机的端口号。

MLD 侦听： 选择该端口是否启用 MLD 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 MLD 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。

8.2.3 VLAN 配置

MLD 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 MLD 参数。本页用于配置每个 VLAN 的 MLD 侦听参数。

进入页面的方法：组播管理>>MLD 侦听>>VLAN 配置

图 8-16 VLAN 配置

条目介绍：

- **VLAN 参数**

VLAN ID： 填写启用 MLD 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。

静态路由端口： 填写静态配置的路由器端口，多用于拓扑稳定的网络中。

- **VLAN 列表**

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。

静态路由器端口： 显示 VLAN 的静态路由器端口。

动态路由器端口： 显示 VLAN 的动态路由器端口。

操作： 对单个条目进行相应操作。

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 MLD 侦听功能	必选操作。在**组播管理>>MLD 侦听>>基本配置、端口配置**页面，启用交换机的 MLD 侦听功能和端口的 MLD 侦听功能。
2	配置 VLAN 的组播参数	可选操作。在**组播管理>>MLD 侦听>>VLAN 配置**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 MLD 侦听功能，那么该 VLAN 中的组播数据会广播。

8.2.4 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>>MLD 侦听>>组播 VLAN

图 8-17 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。
动态路由器端口：	显示组播 VLAN 的动态路由器端口。
静态路由端口：	选择静态配置的路由器端口，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 中的成员端口的端口类型推荐为 GENERAL。
- 组播 VLAN 中的路由器端口的端口类型必须配置为 TRUNK 或者是出口规则为“带 tag”的 GENERAL 端口，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。

- 当建立了组播 VLAN 后，所有的 MLD 报文均只在组播 VLAN 内处理。

配置步骤：

步骤	操作	说明
1	启用 MLD 侦听功能	必选操作。在**组播管理>>MLD 侦听>>基本配置**、**端口配置**页面，启用交换机的 MLD 侦听功能和端口的 MLD 侦听功能。
2	创建组播 VLAN	必选操作。在 **VLAN>>802.1Q VLAN** 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。 ● 配置成员端口的端口类型为 GENERAL。 ● 配置路由端口的端口类型为 TRUNK 或出口规则为“带 tag”的 GENERAL。
3	配置组播 VLAN 的参数	可选操作。进入**组播管理>>MLD 侦听>>组播 VLAN** 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**组播管理>>MLD 侦听>>基本配置**页面中的“已启用的 VLAN”条目处，显示组播 VLAN 的 VLAN ID。

8.2.5 查询器配置

在运行了 MLD 的组播网络中，会有一台三层组播设备充当 MLD 查询器，负责发送 MLD 查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。而网络中的二层设备可以通过侦听三层组播设备与主机之间交互的 MLD 报文来建立二层组播转发表项，实现二层组播转发。但是，在一个没有三层组播设备的网络中，由于没有设备负责 MLD 查询器的功能，这样网络中不会周期性存在 MLD 协议交互的报文，二层设备也无法通过侦听 MLD 报文来建立二层的组播转发表项。为了解决这个问题，可以在二层设备上使用 MLD 侦听查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。本页面主要用于配置 MLD 侦听查询器的相关参数。

进入页面的方法：组播管理>>MLD 侦听>>查询器配置

图 8-18 MLD 查询器配置

条目介绍：

➢ **MLD 侦听查询器配置**

VLAN ID：	输入需要启动查询器的 VLAN ID。
查询间隔：	输入查询间隔时间。查询器会按照间隔时间发送通用查询报文。
最大响应时间：	输入查询报文的最大响应时间字段的值。
通用查询报文源 IP：	输入通用查询报文源 IP 地址。

➢ **MLD 侦听查询器列表**

查看MLD侦听查询器的详细配置参数。

8.2.6 Profile 配置

在启用了 MLD 侦听功能后，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。

进入页面的方法：组播管理>>MLD 侦听>>Profile 配置

图 8-19 Profile 配置

条目介绍：

➢ **创建 MLD Profile**

Profile ID：	输入 Profile ID，区间为 1-999。
模式：	Profile 的过滤模式 ● 允许：只允许加入 Profile 中 IP 地址范围内的组播组。 ● 拒绝：拒绝加入 Profile 中 IP 地址范围内的组播组。

- **显示设置**

  显示模式 选择MLD Profile信息的显示规则，可以帮助您快速查找到所需的条目。

  - 全部：显示全部 MLD Profile 信息。
  - Profile ID：输入欲查找条目需包含的 Profile ID。

- **MLD Profile 信息**

  选择： 勾选后可以删除Profile条目。

  Profile ID： 显示Profile ID。

  模式： 显示Profile的过滤模式。

  绑定端口： 显示当前绑定了该Profile的端口。

  操作： 点击<编辑>按键为Profile添加具体的过滤组播地址，如下图所示。

图 8-20 为Profile添加过滤组播地址

条目介绍：

- **Profile模式**

  Profile ID： 显示Profile ID。

  模式： 修改该Profile的过滤模式，需提交才能生效。

- **添加IP范围**

  起始地址： 显示过滤地址段的起始组播IP地址。

  结束地址： 显示过滤地址段的结束组播IP地址。

- **IP范围**

  选择： 勾选后可以删除IP地址段条目。

  序号： 显示IP地址段的序列号。

起始地址： 显示IP地址段的起始组播IP地址。

结束地址： 显示IP地址段的结束组播IP地址。

8.2.7 Profile 绑定

当端口接收 MLD 文时，交换机根据报文检查端口上配置的组播过滤地址 ID，如果组播地址未被过滤，则将这个端口加入到该组播组的转发端口列表中，否则交换机就丢弃该 MLD 文，从而控制了用户所能加入的组播组。

进入页面的方法：组播管理>>MLD 侦听>>Profile 绑定

图 8-21 Profile 绑定

条目介绍：

- **Profile与最大加入组数目绑定**

UNIT： 根据UNIT ID选择指定的交换机进行配置。

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。

Profile ID： 配置端口绑定的Profile组播过滤文件。

最大加入组数目： 配置端口可以加入到最大组播组数目。

溢出操作： 当端口所加入组播组数已达到最大组播组数时，如果要加入更多的组播组，交换机将执行的动作。

- 丢弃：不再加入新的组播组。
- 替换：端口加入新的组播组，并将端口从当前已加入的组播组IP地址最小的组播组中移除。

LAG： 显示端口当前所属的汇聚组。

清除绑定： 清除端口绑定的Profile。

注意：

Profile绑定设置对静态组播IP不生效。

配置步骤：

步骤	操作	说明
1	配置Profile	必选操作。在**组播管理>>MLD侦听>>Profile配置**页面，创建Profile并设置组播过滤地址。
2	配置端口的组播过滤规则	必选操作。在**组播管理>>MLD侦听>>Profile绑定**页面，配置端口与Profile绑定。

8.2.8 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 MLD 报文。

进入页面的方法：组播管理>>MLD 侦听>>报文统计

图 8-22 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。

- **报文统计**

  端口： 显示交换机的端口号。

  查询报文： 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 MLDv1 报告报文的数目。

  报告报文(V2)： 显示端口接收到的 MLDv2 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。

8.2.9 MLD 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。

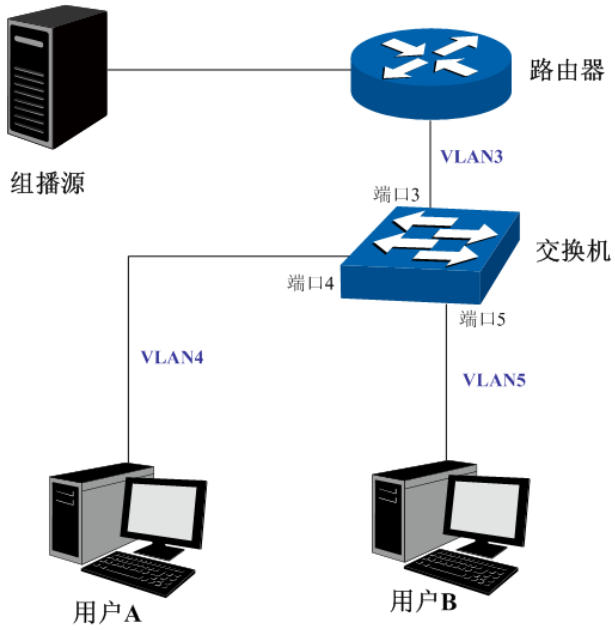
交换机：端口 3 与路由器相连，且通过 VLAN3 转发数据；端口 4 与用户 A 相连，且通过 VLAN4 转发数据；端口 5 与用户 B 相连，且通过 VLAN5 转发数据。

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 **VLAN>>802.1Q VLAN** 功能处，创建 VLAN3、4、5，并将 VLAN3 的描述填写为“组播 VLAN”。
2	配置端口属性	在 **VLAN>>802.1Q VLAN** 功能处。 配置端口 3 的端口类型为 GENERAL，出口规则 TAG，并加入 VLAN3、4、5 中。 配置端口 4 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、4 中。 配置端口 5 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、5 中。

步骤	操作	说明
3	启用 MLD 侦听	在**组播管理>>MLD 侦听>>基本配置**页面，启用 MLD 侦听功能。 在**组播管理>>MLD 侦听>>端口配置**页面，启用端口 3、4、5 的 MLD 侦听功能。
4	启用组播 VLAN	在**组播管理>>MLD 侦听>>组播 VLAN** 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**组播管理>>MLD 侦听>>基本配置**页面，“MLD 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 **IPv4 组播地址表**、**IPv4 静态组播地址表**、**IPv6 组播地址表**和**IPv6 静态组播地址表**四个配置页面。

8.3.1 IPv4 组播地址表

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>>IPv4 组播地址表

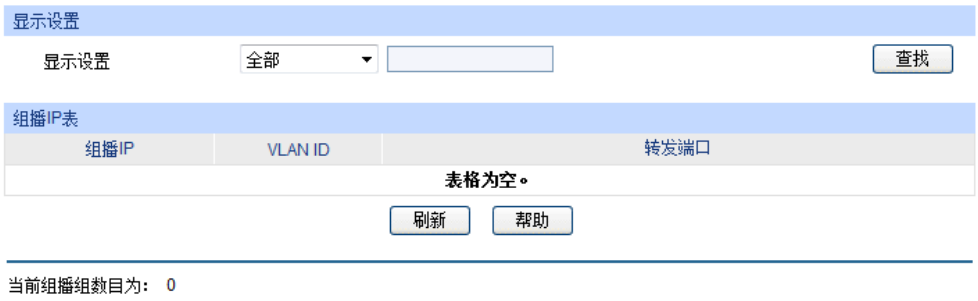


图 8-23 IPv4 组播地址表

条目介绍：

- **显示设置**

显示设置： 选择组播 IP 表的显示规则，可以快速查找到所需条目。

- 全部：显示全部组播 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：设置欲查找条目需包含的端口。

- **组播 IP 表**

显示查找到的组播地址表信息。

8.3.2 IPv4 静态组播地址表

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>>IPv4 静态组播地址表

图 8-5 IPv4 静态组播地址表

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。

  UNIT： 选择一个 UNIT 显示端口信息。

- **显示设置**

  显示设置： 选择静态组播 IP 表的显示规则，可以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。

- **静态组播表**

显示查找到的静态组播地址表信息。

8.3.3 IPv6 组播地址表

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>>IPv6 组播地址表

图 8-25 IPv6 组播地址表

条目介绍：

- **显示设置**

显示设置：	选择组播 IP 表的显示规则，可以快速查找到所需条目。 ● 全部：显示全部组播 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：设置欲查找条目需包含的端口。

- **组播 IP 表**

显示查找到的组播地址表信息。

8.3.4 IPv6 静态组播地址表

静态组播地址表不是通过 MLD 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>>IPv6 静态组播地址表

图 8-26 IPv6 静态组播地址表

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。

UNIT： 选择一个 UNIT 显示端口信息。

- **显示设置**

显示设置： 选择静态组播 IP 表的显示规则，可以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。

- **静态组播表**

显示查找到的静态组播地址表信息。

回目录

第9章 路由功能

说明:

本章节提及的路由器是指传统意义上的路由器或者运行了路由协议的以太网交换机。

在网络中通常由传统路由器或者运行了路由协议的以太网交换机实现不同网络间的数据转发。路由是指路由器根据收到的数据包的目的地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程，而此路径上的最后一个路由节点则将数据转发给目标主机。

在一次路由过程中选择最优路径是路由器需要完成的最重要的工作。路由器通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。常用的路由选择协议有 RIP、OSPF 和 BGP 等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。路由表中的每一个路由条目基本都包含如下基本属性：

- 目的网络地址：用于标识该条路由条目所指向的目标网络。
- 子网掩码：用于标识目标网络的子网掩码。
- 下一跳地址：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过 ping 工具测试是否可达。
- 下一跳接口：用于标识数据从本地发出的出接口。

路由条目的来源有三种，分别为直连路由、静态路由和动态路由。

1) 直连路由：通过数据链路层协议发现的，通常为与路由器直接连接的网络的路由。
2) 静态路由：由网络管理员手动配置的一种特殊路由，不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。
3) 动态路由：通过相互连接的路由器之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。

本交换机的路由模块主要支持直连路由和静态路由两种，也支持动态路由协议 RIP。直连路由即为本地直连网络的路由，如本地配置的 VLAN 进行工作组划分时，同时提供代理 ARP 功能来满足特定网络需求。

9.1 接口

网络接口是一种三层模式下的虚拟接口，主要用于实现 VLAN、路由端口之间的三层互通。每个 VLAN 接口对应一个 VLAN，路由端口对应一个物理端口，环回接口是纯软件接口的。网络接口通过地址与子网掩码参数确定了一个 IP 网段（或称为 IP 子网），并作为该网段的网关对需要跨网段的报文进行基于 IP 地址的三层转发。

进入界面的方法：路由功能>>接口>>接口设置

图 9-1 接口设置

条目介绍：

- **创建接口**

接口 ID： 选择需要配置 IP 地址的接口 ID，如 VLAN ID、交换机端口号、环回接口。

IP 地址模式： 设置 IP 地址申请模式。

- None：无 IP。
- Static：手动设置。
- DHCP：通过 DHCP 申请。
- BOOTP：通过 BOOTP 申请。

IP 地址： 设置网络接口的 IP 地址。

子网掩码： 设置网络接口 IP 地址的子网掩码。

管理状态： 设置网络接口的管理状态，默认为使能。选择“禁用”来关闭此接口的三层功能。

接口名称： 设置网络接口的接口名称。

- **接口列表**

选择： 选择接口条目进行修改或删除。

ID： 显示该网络接口对应的 ID。

模式： 显示 IP 地址申请模式。

IP 地址： 显示网络接口的 IP 地址。

子网掩码： 显示该网络接口的子网掩码。

接口名称： 显示该网络接口的接口名称。

状态： 显示网络接口的当前运行状态。

操作： 单击“编辑”修改网络接口设置，或单击“查看”查看详细信息。

点击“编辑”来修改选定接口条目的参数：

图 9-2 修改接口

- **修改接口**

接口 ID： 显示接口 ID。

IP 地址模式： 设置 IP 地址申请模式。

- None：无 IP。
- Static：手动设置。
- DHCP：通过 DHCP 申请。
- BOOTP：通过 BOOTP 申请。

IP 地址： 设置接口的 IP 地址。

子网掩码： 设置接口的子网掩码。

管理状态： 修改接口的管理状态。

接口名称： 修改接口名称。

- **创建第二 IP**

IP 地址： 设置接口的第二 IP 地址。

子网掩码： 设置接口的第二 IP 地址的子网掩码。

- **第二 IP 列表**

选择： 选择要删除的第二 IP 地址。

IP 地址： 显示当前接口的第二 IP 地址。

子网掩码： 显示第二 IP 地址的子网掩码。

单击“编辑 IPv6”可进行 IPv6 接口设置：

图 9-3 IPv6 接口设置

IPv6 链路本地地址： 当使用手动方式配置链路本地地址时，在此输入交换机的链路本地地址。

链路本地地址状态： 显示交换机链路本地地址的状态。

- 正常：表明链路本地地址状态是正常的。
- 试探：表明链路本地地址可能是新配置的。
- 重复：表明交换机的链路本地地址与链路上其它节点重复，此时不能用 IPv6 地址（包括链路本地地址和全球地址）访问交换机。

➢ **通过 RA 消息配置 IPv6 全球地址**

允许使用 RA 消息进行全球地址自动配置： 当该选项被启用时，系统将接受来自路由器的 RA 消息进行全球地址的自动配置。

- **通过 DHCPv6 获取全球地址**

  启用 DHCPv6 获取全球地址： 当该选项被启用时，系统将尝试使用DHCPv6获取全球地址。

- **手动添加 IPv6 全球地址**

  配置方式： 可以根据需要选择一种全球地址的配置方式。

  - EUI-64：当使用 EUI-64 方式时，仅需指定一个地址前缀，系统将自动生成一个全球地址。
  - 非 EUI-64：当使用非 EUI-64 方式时，需要指定一个完整的 IPv6 全球地址。

  IPv6 全球地址： 当使用 EUI-64 方式配置全球地址时，在此输入地址前缀。当使用非 EUI-64 方式配置全球地址时，在此输入完整的 IPv6 地址。

- **系统当前 IPv6 全球地址列表**

  选择： 在此选择要修改或删除的 IPv6 全球地址。

  IPv6 全球地址： 当修改 IPv6 全球地址的时候，在此输入新的 IPv6 全球地址。

  前缀长度： 当修改 IPv6 全球地址的时候，在此输入新的 IPv6 全球地址前缀长度。

  地址类型： 显示全球地址的配置方式。

  - 手动：表示对应地址是用户手动配置的。
  - 自动：表示对应地址是系统通过接收 RA 消息自动生成，或者通过 DHCPv6 获取。

  首选时间： 显示全球地址的首选时间。

  有效时间： 显示全球地址的有效时间。

  状态： 显示全球地址的状态。

  - 正常：表明全球地址状态是正常的。
  - 试探：表明全球地址可能是新配置的。
  - 重复：表明全球地址与链路上其它节点重复，此时不能用该 IPv6 全球地址访问交换机。

点击“详细”来查看接口的详细配置信息：

图 9-4 接口详细信息

- **IPv6 全局配置**

接口 ID： 显示需进行 IPv6 功能设置的接口名称。

IPv6 功能： 选择启用或禁用 IPv6 功能。

- **IPv6 链路本地地址配置**

链路本地地址配置方式： 可以根据需要，让系统自动生成一个链路本地地址，或者使用纯手工的方式配置链路本地地址。

- 手动：选择此选项时，您需要手工配置链路本地地址。
- 自动：选择此选项时，交换机会自动生成一个链路本地地址。

9.2 路由表

9.2.1 IPv4 路由表

此页面用来显示交换机上保存的路由条目，来源包括：直连路由，静态路由和动态路由协议。

进入界面的方法：路由功能>>路由表>>IPv4 路由表

图 9-4 IPv4 路由表

条目介绍：

- **路由信息汇总**

路由协议： 本条路由条目的来源：

- static：静态路由。
- connected：直连路由。
- RIP：RIP 路由协议。
- OSPF：OSPF 路由协议。
- BGP：BGP 路由协议

目的网络： 目的网络 IP 地址及子网掩码。

下一跳地址： 下一跳 IP 地址。

管理距离： 管理距离。

度量值： 度量值。

接口名称： 接口名称。

9.2.2 IPv6 路由表

此页面用来显示交换机上保存的 IPv6 路由条目，来源包括：直连路由，静态路由和动态路由协议。

进入界面的方法：路由功能>>路由表>>IPv6 路由表

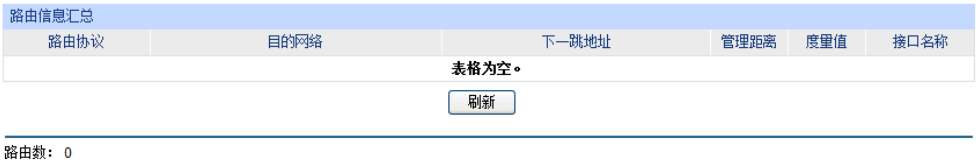


图 9-5 IPv6 路由表

条目介绍：

- **路由信息汇总**

路由协议： 本条路由条目的来源：

- static：静态路由。
- connected：直连路由。
- RIP：RIP 路由协议。

目的网络： 目的网络 IP 地址及子网掩码。

下一跳地址： 下一跳 IP 地址。

管理距离： 管理距离。

度量值： 度量值。

接口名称： 接口名称。

9.3 静态路由

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

9.3.1 IPv4 静态路由条目

本页面用于添加 IPv4 静态路由条目。管理员可以在该静态路由条目页面配置一条缺省路由来防止路由表过大。当路由表中不存在与 IP 报文的目的 IP 地址匹配表项时，就选择缺省路由转发。

进入界面的方法：路由功能>>静态路由>>IPv4 静态路由条目

图 9-6 IPv4 静态路由条目

条目介绍：

- **静态路由配置**

  目的地址： 设置路由条目需要到达的目标网络地址。

  子网掩码： 设置路由条目需要到达的目标网络的子网掩码。

  下一跳地址： 设置通往目标网络的路由路径上下一个节点的 IP 地址。

  管理距离： 指定路由条目的管理距离。管理距离越小，优先级越高。

- **静态路由条目**

  选择： 选择静态路由条目进行修改或删除。

  目的地址： 显示路由条目需要到达的目标网络地址。

  子网掩码： 显示路由条目需要到达的目标网络的子网掩码。

  下一跳地址： 修改通往目标网络的路由路径上下一个节点的 IP 地址。

  管理距离： 修改路由条目的管理距离。管理距离越小，优先级越高。

度量值： 显示路由条目的度量值。

接口名称： 显示接口名称。

9.3.2 IPv6 静态路由条目

本页面用于添加 IPv6 静态路由条目。管理员可以在该静态路由条目页面配置一条缺省路由来防止路由表过大。当路由表中不存在与 IP 报文的目的 IP 地址匹配表项时，就选择缺省路由转发。

进入界面的方法：路由功能>>静态路由>>IPv6 静态路由条目

图 9-7 IPv6 静态路由条目

条目介绍：

- **IPv6 路由**

  IPv6 路由： 选择开启或关闭 IPv6 路由功能。

- **静态路由配置**

  目的地址： 设置路由条目需要到达的目标网络地址。

  子网掩码长度： 设置路由条目需要到达的目标网络的子网掩码长度。

  下一跳地址： 设置通往目标网络的路由路径上下一个节点的 IP 地址。

  管理距离： 指定路由条目的管理距离。管理距离越小，优先级越高。

- **静态路由条目**

  选择： 选择静态路由条目进行修改或删除。

  目的地址： 显示路由条目需要到达的目标网络地址。

  下一跳地址： 修改通往目标网络的路由路径上下一个节点的 IP 地址。

  管理距离： 修改路由条目的管理距离。管理距离越小，优先级越高。

  度量值： 显示路由条目的度量值。

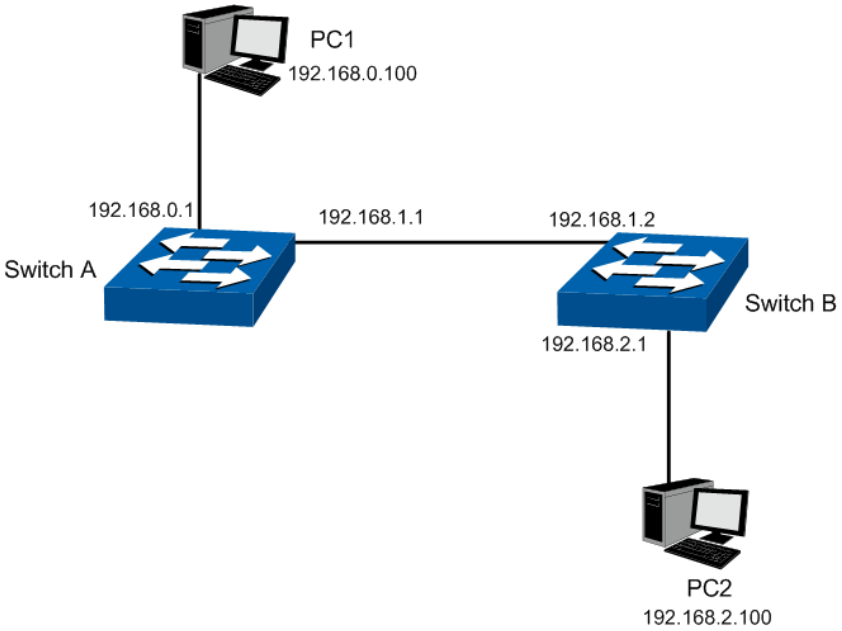
  接口名称： 显示接口名称。

9.3.3 静态路由功能的组网应用

- **组网需求**

1. 某小型企业网络中有三个 VLAN，分别为 VLAN10、20、30，VLAN ID 分别为 10、20、30。
2. PC1 在 VLAN10，PC2 在 VLAN30；PC1 和 PC2 可以网络互通。

- **组网图**



- **配置步骤**

- **配置交换机 A**

步骤	操作	说明
1	添加接口 10	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 10，IP 地址模式为 static，IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，接口名称为 VLAN10。
2	添加接口 20	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 20，IP 地址模式为 static，IP 地址为 192.168.1.1，子网掩码为 255.255.255.0，接口名称为 VLAN20。
3	添加静态路由条目	在**路由功能>>静态路由>>静态路由条目**页面添加一条静态路由条目，目的地址为 192.168.2.0，子网掩码为 255.255.255.0，下一跳为 192.168.1.2。

- **配置交换机 B**

步骤	操作	说明
1	添加接口 20	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 20，IP 地址模式为 static，IP 地址为 192.168.1.2，子网掩码为 255.255.255.0，接口名称为 VLAN20。
2	添加接口 30	在**路由功能>>接口>>接口设置**页面添加 VLAN 接口 30，IP 地址模式为 static，IP 地址为 192.168.2.1，子网掩码为 255.255.255.0，接口名称为 VLAN30。
3	添加静态路由条目	在**路由功能>>静态路由>>静态路由条目**页面添加一条静态路由条目，目的地址为 192.168.0.0，子网掩码为 255.255.255.0，下一跳为 192.168.1.1。

- **配置所有 PC**

设置 PC1 默认网关为 192.168.0.1；配置 PC2 的默认网关为 192.168.2.1。

9.4 DHCP 服务器

- **DHCP 服务器的应用环境**

DHCP 服务器可以在下列场景中高效完成网络设备的 IP 地址配置工作：

1) 网络规模大，为每台网络设备手工配置网络参数的工作量较大，且不便于对网络进行集中管理。

2) 网络中设备数目大于该网络支持的设备数量，相应的 IP 资源不足。例如，ISP 限制同时接入网络的用户数目，而网络中的设备并不需要同时访问网络，则用户可以动态按需获得网络 IP。

3) 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

➢ **DHCP 服务器在本交换机上的实现**

下图为本交换机配置为 DHCP 服务器时的网络拓扑图示范，具体的网络环境可能根据实际需求有所调整。

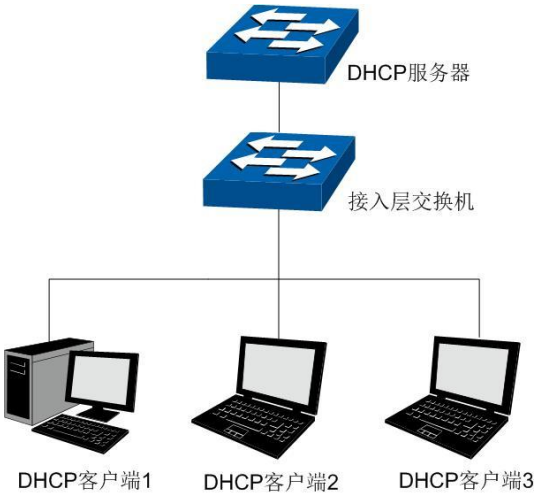


图 9-9 DHCP 服务器拓扑图示例

为了使网络中的设备能够安全顺利的获得 IP 地址，保证网络的稳定性，本交换机的 DHCP 服务器功能可以完成如下所示任务：

- 本交换机为网络中的多个 VLAN 指定特定的地址池，实现不同 VLAN 的设备获得不同网段的 IP 地址。
- 当客户端向本交换机申请 IP 地址时，交换机判断接收请求报文的端口所属的默认 VLAN，从该 VLAN 接口 IP 所属的地址池中选取合适的地址分配给客户端。
- 如果服务器和客户端之间搭建了 DHCP 中继设备，DHCP 请求报文经过 DHCP 中继设备时报文中的 giaddr 字段将被填入中继设备上客户端连接的接口 IP 地址，服务器将在此 IP 网段地址池中选择合适的 IP 地址分配给客户端。如果 DHCP 服务器上没有创建中继设备 IP 地址段的地址池，客户端将无法获得 IP 地址。
- IP 地址重复分配检测功能，避免因同一地址重复分配而造成的网络中 IP 冲突。

➢ **IP 地址重复分配检测**

当交换机配置了 DHCP 服务器功能为网络中的设备分配 IP 地址时，为防止 IP 地址重复分配导致 IP 地址冲突，交换机将对该地址进行 Ping 探测。地址检测方式如下：

DHCP 服务器发送目的 IP 地址为待分配地址的 ICMP 回显请求报文，如果在等待时间内收到响应报文，DHCP 服务器从地址池中选择新的 IP 地址，并重复上述探测操作；如果在指定时间内没有收到回显响应报文，则将地址分配给客户端，从而确保客户端被分得的 IP 地址唯一。

➢ **分配 IP 地址的优先次序**

交换机的 DHCP 服务器功能为客户端分配 IP 地址时，其分配规则如下：

1) DHCP 服务器中与客户端 MAC 地址手动绑定的 IP 地址。

2) DHCP 服务器曾经分配给客户端的 IP 地址。

3) 客户端发送的 DHCP-DISCOVER 报文中指定的 IP 地址。

4) 选择合适的地址池，从中顺序查找可供分配的第一个 IP 地址。

➢ **DHCP 服务器在本交换机上的配置要点**

1) 为每个网段保留特定的 IP 地址不做分配，如网关地址、网段广播地址、服务器地址等。

2) 为特殊用户群手动绑定静态 IP，当收到特殊用户群的 IP 申请时，交换机将为客户端分配租期为无限长的固定的 IP 地址。

3) 创建动态分配地址池，网络中的设备申请 IP 地址时，可以获得相应接口地址池中的空闲地址。

DHCP 服务器功能包括 **DHCP 服务器**、**地址池设置**、**静态绑定**和**绑定表**四个配置页面。

9.4.1 DHCP 服务器

在这个页面中，可配置 DHCP 服务器功能。

进入页面的方法：路由功能>>DHCP 服务器>>DHCP 服务器

图 9-10 DHCP 服务器

条目介绍：

➢ **全局配置**

DHCP 服务器：	选择是否启用 DHCP 服务器功能。
Option 60：	配置 DHCP Option 60 选项字段，如果该选项字段不为空且运行 CAPWAP 协议的客户端通过 DHCP 向服务器请求获取 option 138 选项时服务器发出的报文将会带上该选项。
Option 138：	配置 DHCP Option 138 选项字段，如果该选项字段不为空且运行 CAPWAP 协议的客户端通过 DHCP 向服务器请求获取 option 138 选项时服务器发出的报文将会带上该选项。

➢ **Ping 设置**

设置用于确定 IP 是否已存在的 Ping 报文的个数以及超时时间。

Ping 报文数：	每次确定 IP 存在的时候发出的报文数。

Ping 超时： Ping 超过该时间则认为指定 IP 不存在。

9.4.2 地址池设置

在这个页面中，请为不同的网段分别配置 DHCP 地址池，包含默认网关、DNS 域名服务器和租期等参数。

进入页面的方法：路由功能>>DHCP 服务器>>地址池设置

图 9-11 DHCP 服务器地址池

条目介绍：

- **DHCP 服务器地址池**

地址池名称： 填写地址池的名称，以便于区分各个地址池的实际属性。

网络号： 配置此地址池的网络地址，同一网段中的地址除了预留地址以及特殊地址外均可以作为可分配地址。

掩码： 配置此地址池的子网掩码。当客户端从此地址池获取 IP 地址时，其子网掩码以此参数为准。

起始地址： 地址池的起始地址。

结束地址： 地址池的结束地址。

租期： 配置此地址池中分配的 IP 地址租期。默认为 120 分钟。

默认网关： 展开右边的输入框在下方的输入框中配置此地址池的默认网关，最大可设置 8 个，为可选配置。默认情况下，也可以以 VLAN 接口 IP 地址作为默认网关。

DNS 服务器： 展开右边的输入框在下方的输入框中配置此地址池的 DNS 服务器，最大可设置 8 个，为可选配置。默认情况下，也可以以 VLAN 接口 IP 地址作为 DNS 服务器。

Netbios 服务器： 配给客户端的 WINS 服务器，最大可设置 8 个，为可选配置。

Netbios 节点类型： 客户端 Netbios 节点类型，可设置为空，为可选配置。

下一服务器地址： 引导过程的下一个服务器地址，为可选配置。

客户端域名： 给客户端设置的域名，为可选配置。

启动文件名： 引导过程中用到的镜像文件名，为可选配置。

- **地址池列表**

选择： 勾选地址池条目进行删除，可多选。

名称： 显示地址池名称。

网络号： 显示地址池的网络地址。

掩码： 显示地址池的子网掩码。

租期： 显示地址池的租期。

起始地址： 显示地址池的起始地址。

结束地址： 显示地址池的结束地址。

操作： 点击<编辑>或<查看>按钮来对条目进行编辑或查看。

9.4.3 静态绑定

在这个页面中，可以将可将 MAC 地址与 IP 地址进行绑定，服务器收到已绑定 MAC 的 DHCP 请求时，会将所绑定的 IP 地址发送给客户端。

进入页面的方法：路由功能>>DHCP 服务器>>静态绑定

图 9-12 静态绑定

条目介绍：

- **DHCP 服务器静态绑定设置**

地址池名称： 地址池的名称，从已配置地址池中选取。

绑定 IP： 与 MAC 地址绑定的 IP 地址。

绑定方式： 设定 IP 与客户端 ID 绑定或者 IP 与硬件地址绑定。

客户端 ID： 绑定的客户端 ID。

硬件地址： 所绑定的 MAC 地址。

硬件类型： 选择为 Ethernet 或者 IEEE802 类型。

- **静态绑定列表**

选择： 勾选静态绑定条目进行删除，可多选。

地址池名称： 显示地址池的名称。

客户端 ID/硬件地址： 显示绑定的客户端 ID/所绑定的 MAC 地址。

IP 地址： 显示与 MAC 地址绑定的 IP 地址。

硬件类型： 显示硬件类型。

绑定方式： 显示绑定方式。

操作： 点击<编辑>按钮来对选定条目进行编辑。

9.4.4 绑定表

在此页面中，可以查看从交换机成功获得 IP 地址的绑定信息和租约信息。

进入页面的方法：路由功能>>DHCP 服务器>>绑定表

图 9-13 绑定表

DHCP 服务器配置步骤（VLAN 接口为例）：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。

步骤	操作	说明
3	创建VLAN接口	必须操作。在**路由功能>>接口>>接口设置**页面中为 VLAN 建立 VLAN 接口。
4	启用 DHCP 服务器功能	必须操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**页面中启用 DHCP 服务器功能。
5	配置 IP 地址池	必须操作。在**路由功能>>DHCP 服务器>>地址池设置**页面中配置 IP 地址池参数，包括子网掩码、默认网关、DNS 和租期等。
6	手动绑定 IP 地址	可选操作。在**路由功能>>DHCP 服务器>>静态绑定**页面中可以为特殊客户端绑定特定的 IP 地址。

9.4.5 DHCP 服务器功能的组网应用

➢ **网络需求**

- 将校园中每一栋楼划分独立的 VLAN，并属于不同的 IP 网段；
- 每一栋楼中的接入点分成两部分，一部分是办公室，配有固定计算机，采用静态 IP 地址；另一部分是教室，多为笔记本电脑接入，采用动态 IP 地址，需要从网络中的 DHCP 服务器上获取 IP 地址；
- DNS 服务器位于 VLAN 1 中，IP 为 160.20.30.2。

➢ **组网图**

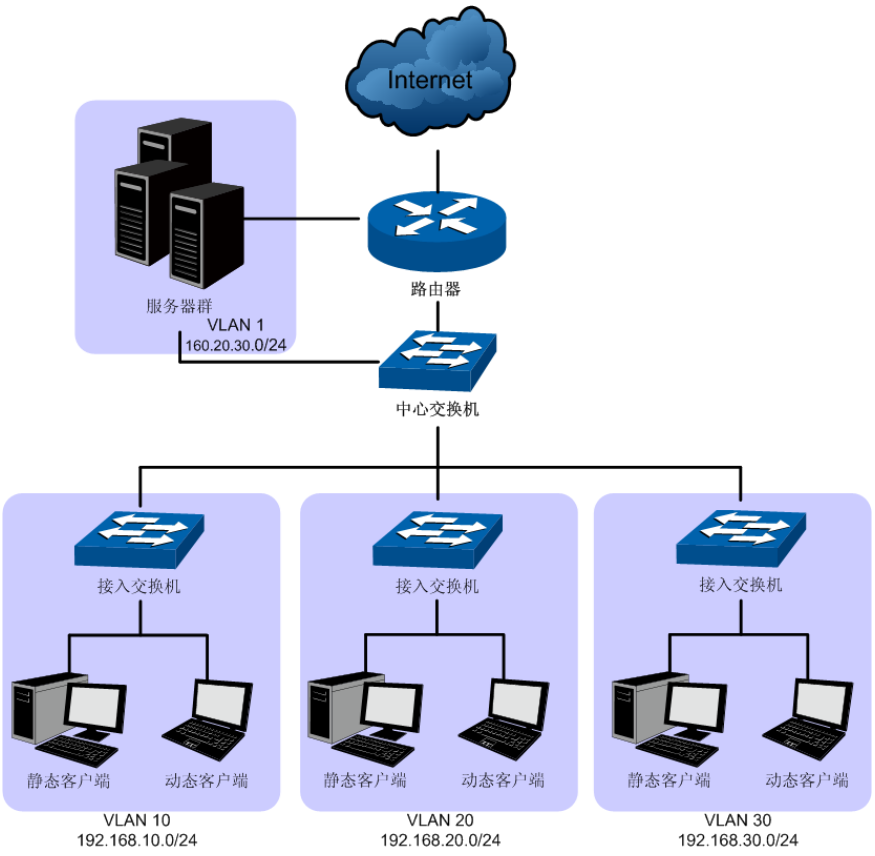


图 9-14 DHCP 服务器功能组网图

中心交换机采用本设备，并启用 DHCP 服务器为网络中的设备分配 IP 地址，配置步骤如下：

- **配置步骤**

配置中心交换机：

步骤	操作	说明
1	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN10, VLAN20 和 VLAN30，并配置端口。
2	创建 VLAN 接口	必须操作。在**路由功能>>接口>>接口设置**页面中为 VLAN10, VLAN20 和 VLAN30 建立 VLAN 接口，分别为 192.168.10.1/24, 192.168.20.1/24, 192.168.30.1/24。
3	启用 DHCP 服务器功能	必须操作。在**路由功能>>DHCP 服务器>>DHCP 服务器**页面中启用 DHCP 服务器功能。
4	配置 IP 地址池	必须操作。在**路由功能>>DHCP 服务器>>地址池设置**页面中为各 VLAN 接口配置 IP 地址池参数，以 VLAN10 为例，网络地址配置为 192.168.10.0，子网掩码为 255.255.255.0，网关配置为 VLAN 接口地址 192.168.10.1，DNS 服务器配置为 160.20.30.2，同时配置租约并为 IP 地址池命名等。
5	手动绑定 IP 地址	可选操作。在路由功能>>DHCP 服务器>>静态绑定页面中可以为特殊客户端指定特定的 IP 地址。

9.5 DHCP 中继

- **DHCP 中继的应用环境**

在 DHCP 的基本网络模型中，要求客户机和服务器处于同一个局域网，客户端设备通过广播的形式向服务器动态获取 IP 地址。这种模型要求每个网络中均需要配置 DHCP 服务器，这种方式无疑会提高网络建设成本。引入 DHCP Relay 可以有效解决这一问题。DHCP Relay 设备可以为不同网段间的 DHCP Client 和 DHCP Server 提供中继服务，将 DHCP 协议报文跨网段转发，使得多个网络上的 DHCP Client 可以共享一台 DHCP Server。

- **DHCP 中继在本交换机上的实现**

下图为本交换机配置为 DHCP 中继时的网络拓扑图示例，具体的应用环境可能根据实际需求有所调整。

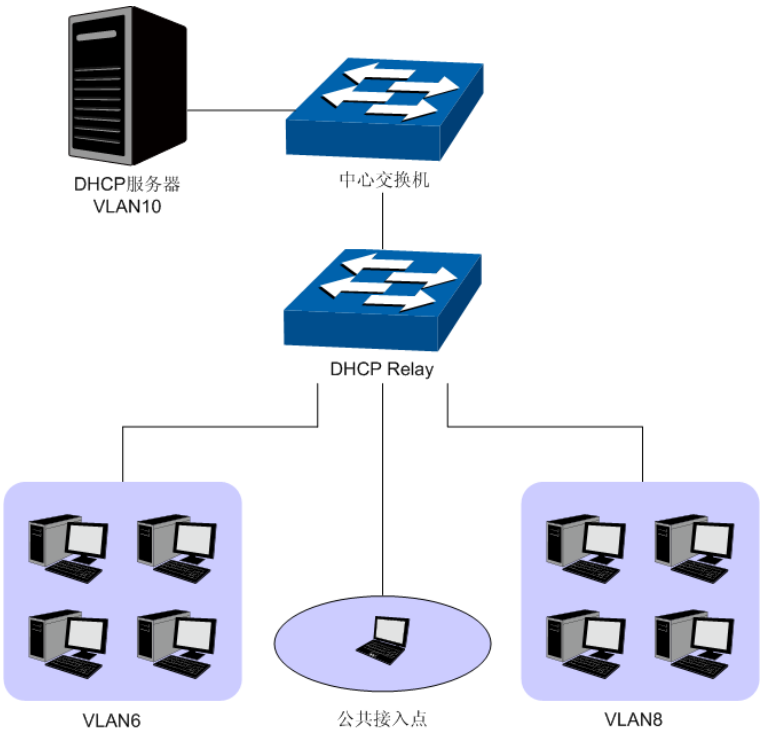


图 9-15 DHCP 中继典型拓扑图

为了保证所有 VLAN 中的设备能够安全顺利的获得 IP 地址，工作在 DHCP 中继模式的本交换机为多个 VLAN 与服务器之间转发 DHCP 协议报文，使所有 VLAN 中的设备均能够从网络中的 DHCP 服务器获得 IP 地址。

- 当交换机收到来自客户端的 DHCP-DISCOVER 和 DHCP-REQUEST 报文时，在报文中的 giaddr 字段写入接收端口的接口 IP 地址，同时插入可选项 option82，并以单播的形式将报文转发给指定的 DHCP 服务器；
- 当收到来自服务器的应答报文时，交换机将删除数据包中的 option 82 字段，将 DHCP 应答报文向中继设备的接口网络中广播。

详细的报文交换过程请参考下图，其中(B)表示广播，(U)表示单播。

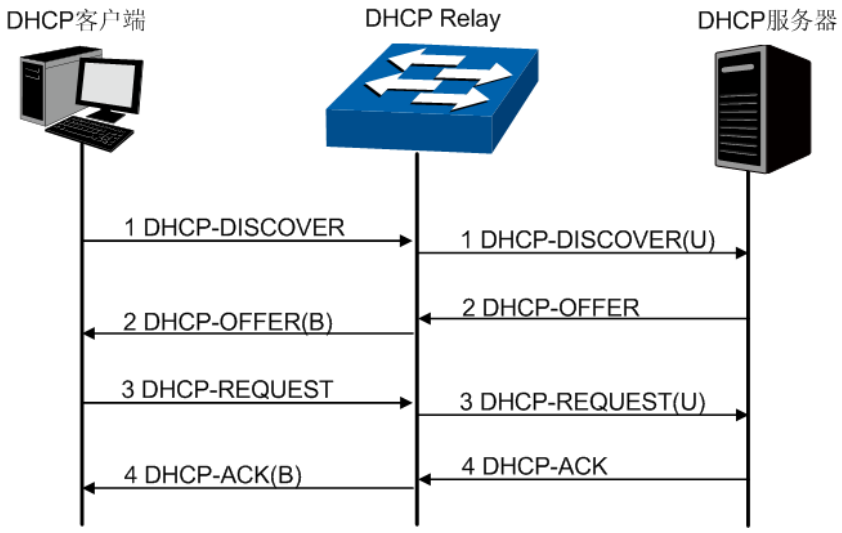


图 9-8 报文交互过程图片

- **DHCP Relay 在本交换机上的配置要点**

1) 配置 Option 82 参数。关于 Option 82 选项的详细说明请参考下一节。建议在最靠近 DHCP 客户端的 Relay 设备上启用 Option 82 功能，以便精确记录客户端位置信息。

2) 配置 DHCP Server 信息。

- **中继代理选项 Option 82**

在我司交换机上，Option 82 被定义为中继信息选项，用于记录 DHCP 客户端的位置信息，常见的信息有 VLAN 信息、连接端口。当在交换机上配置了 Option82 选项时，交换机在接收到的 DHCP-DISCOVER 和 DHCP-REQUEST 报文中添加 Option 82 字段标记客户端信息，并转发给 DHCP 服务器。DHCP 服务器可以从 Option 82 字段中获得相关信息，并执行相应的分配策略，实现对客户端的安全和计费等控制。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。

目前本交换机对子选项的填充内容如下，电路 ID 子选项的填充内容是接收到 DHCP 请求报文的所属 VLAN 以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 请求报文的 DHCP Relay 设备的 MAC 地址，填充格式如下图所示。同时，也支持自定义电路 ID 子选项和远程 ID 子选项。

下图为缺省情况下我司交换机定义的 option 82 填充格式，括号中的数字表示该字段的字节数。如图所示，缺省情况下，子选项 1 为电路 ID 子选项，其填充内容为 2 个字节的 VLAN 参数和 2 个字节的接收端口。子选项 2 为远程 ID 子选项，其填充内容为 6 个字节的客户端 MAC 地址。同时用户也可以自定义的两个子选项填充值。

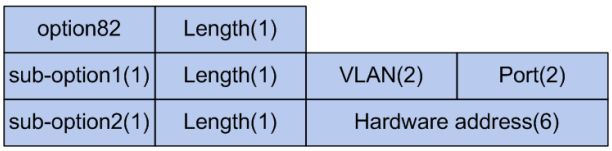


图 9-16 option 82 字段格式

注意:

Option82 的配置参数需要结合并满足网络需求。

通过 DHCP 中继功能，交换机能在不同的 VLAN 或子网中获取 IP 地址。在特定的 VLAN 中指定 DHCP 服务器，开启 DHCP 中继功能并指定服务器的地址，在其他 VLAN 的设备就能获取 IP 地址。DHCP 中继功能可以减少网络中 DHCP 服务器的数量。

DHCP 中继功能包括**全局配置**和**接口中继配置**两个配置页面。

9.5.1 全局配置

本页面用于配置 Option 82 选项来辅助 IP 地址分配。

进入页面的方法：路由功能>>DHCP 中继>>全局配置

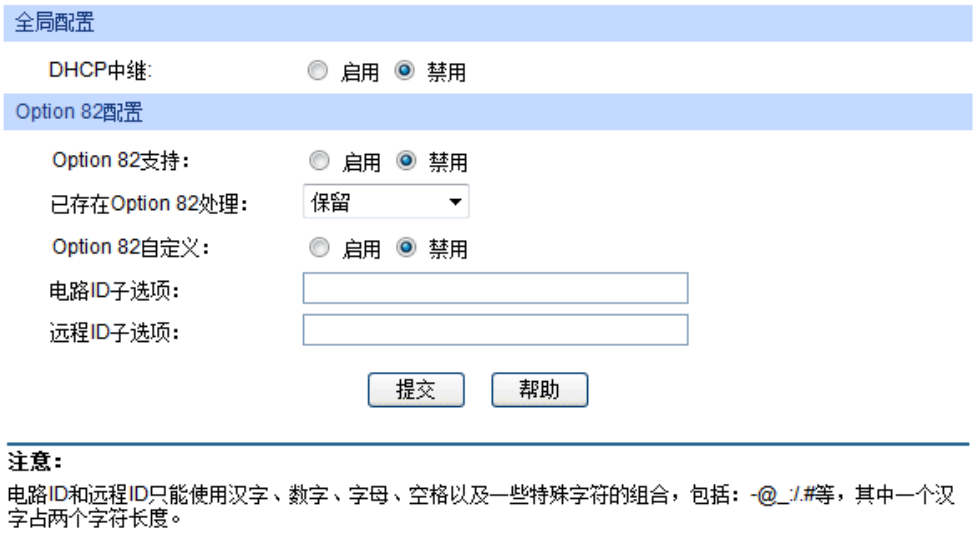


图 9-17 DHCP 中继全局配置

条目介绍：

- **全局配置**

  DHCP 中继： 选择是否启用 DHCP 中继功能。

- **Option 82 配置**

  Option 82 支持： 选择是否启用 Option 82 字段。默认关闭。

  已存在 Option 82 处理： 当客户端的 DHCP 请求报文已经有 Option 82 字段时，选择对此字段的操作。

  - 保留：保留数据包中的 Option 字段信息。
  - 替换：替换数据包中的 Option 字段信息，替换为交换机自定义的系统选项内容。
  - 丢弃：丢弃包含 Option 82 字段的数据包。

  Option 82 自定义： 开启或关闭 Option82 自定义功能，添加自定义的 Option 82 信息。

  电路 ID 子选项： 输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。

  远程 ID 子选项： 输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。

9.5.2 DHCP 服务器

本页面用来配置 DHCP 服务器的相关参数。

进入页面的方法：路由功能>>DHCP 中继>>DHCP 服务器

图 9-18 DHCP 服务器

条目介绍：

- **添加 DHCP 服务器地址**

  接口 ID： 选择接口类型，并输入对应接口号。

  服务器地址: 填写 DHCP 服务器的 IP 地址。

- **DHCP 服务器列表**

  选择： 勾选 DHCP 服务器条目进行删除，可多选。

  接口 ID： 显示 DHCP 服务器的接口 ID。

  服务器地址： 显示 DHCP 服务器的 IP 地址。

DHCP 中继配置步骤：

步骤	操作	说明
1	启用 DHCP 中继功能。	必选操作。在**路由功能>>DHCP 中继>>全局配置**功能页面中启用 DHCP 中继功能。
2	配置 Option 82 选项。	可选操作。在**路由功能>>DHCP 中继>>全局配置**功能页面中配置 Option 82 选项参数。
3	配置 DHCP Server。	必选操作。在**路由功能>>DHCP 中继>>接口中继配置**功能页面中配置 DHCP 服务器来提供 IP 分配服务。

9.6 代理 ARP

代理 ARP 是 ARP 协议的一种应用。通常应用于网关在连接不同网络时，为不同网络中的计算机提供 ARP 代理服务。网关收到源计算机向目标网络计算机发送的 ARP 请求时，使

用自己的 MAC 地址与目标计算机的 IP 地址对源计算机进行 ARP 应答，使得不同网络中的计算机能够正常通信而不必关心网络的划分。

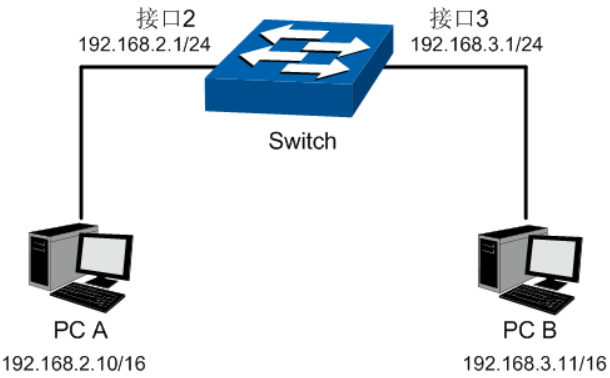
代理 ARP 多应用于下列两种环境：

1) 当不同网络中没有配置缺省网关的计算机要和其他网络中的计算机实现通信，其通过发送的 ARP 请求报文来试图通信，而网关在收到该 ARP 请求报文时，其代理 ARP 机制将代替目标计算机进行 ARP 应答，并为两个网络转发通信报文。

2) 当对网络进行 VLSM 子网划分时，可通过在网关上配置 ARP 代理，使得网络中计算机原有网络参数配置不做相应变更也可以进行通信。这种应用环境将在接下来的内容中详细介绍。

- **代理 ARP 工作机制**

上述两种代理 ARP 的应用环境可以简化为下图所示案例。



如图所示，由于PC A(192.168.2.10/16)与PC B(192.168.3.11/16)处于同一网段，当PC A需要与PC B通信时，会以广播方式发送ARP请求报文请求PC B的MAC地址。如果A、B分别属于不同的VLAN，则请求报文不能到达B，双方不能正常通信。当交换机开启了代理ARP功能后，接口2收到ARP请求报文时，发现ARP请求报文指向了另一个网络，则交换机会以接口2的MAC地址发送ARP应答报文给PC A。PC A收到伪应答报文后建立ARP表项，表项中PC B的IP地址对应着接口2的MAC地址。后续PC A发给PC B的报文都会发送到接口2，然后由交换机进行三层转发，从而实现A与B的通信。

9.6.1 代理 ARP

本页面用于配置代理 ARP 功能。

进入界面的方法：路由功能>>代理 ARP>>代理 ARP

图 9-19 代理 ARP

条目介绍：

- **代理 ARP 信息**

选择： 选择要设置的表项，可多选。

IP 地址： 显示网络接口的 IP 地址。

子网掩码： 显示网络接口的子网掩码。

接口： 显示网络接口。

接口名称： 显示网络接口的接口名称。

状态： 启用或禁用该接口上的代理 ARP 功能。

9.6.2 本地代理 ARP

本页面用于配置本地代理 ARP 功能。

进入界面的方法：路由功能>>代理 ARP>>本地代理 ARP

图 9-20 本地代理 ARP

条目介绍：

- **本地代理 ARP 信息**

选择： 选择要设置的表项，可多选。

IP 地址： 显示网络接口的 IP 地址。

子网掩码： 显示网络接口的子网掩码。

接口： 显示网络接口。

接口名称： 显示网络接口的接口名称。

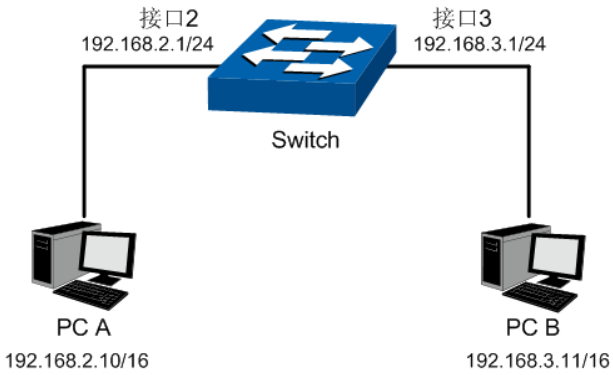
状态： 启用或禁用该接口上的本地代理 ARP 功能。

9.6.3 代理 ARP 功能的组网应用

- **组网需求**

1. PC A 和 PC B 在同一网段，PC A 的 IP 地址为 192.168.2.10/16，PC B 的 IP 地址为 192.168.3.11/16。
2. PC A 和 PC B 分别属于不同的子网 VLAN2 和 VLAN3。
3. 通过开启接口 2（192.168.2.1/24）和接口 3（192.168.3.1/24）的代理 ARP 功能实现 A、B 之间的通信。

➢ **组网图**



➢ **配置步骤**

● **配置交换机**

步骤	操作	说明
1	创建 VLAN2	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 2。
2	创建 VLAN3	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 3。
3	添加接口 2	在**路由功能>>接口>>接口设置**页面添加接口 2，IP 地址为 192.168.2.1，子网掩码为 255.255.255.0，VLANID 为 2，接口名称为 VLAN2。
4	添加接口 3	在**路由功能>>接口>>接口设置**页面添加接口 3，IP 地址为 192.168.3.1，子网掩码为 255.255.255.0，VLANID 为 3，接口名称为 VLAN3。
5	启用代理 ARP	在**路由功能>>代理 ARP** 页面启用接口 2 和接口 3 的代理 ARP 功能。

9.7 ARP

9.7.1 ARP 表

本页面用于显示 ARP 表，可以查看本机中所有的静态或动态 ARP 条目。

进入界面的方法：路由功能>>ARP>>ARP 表

图 9-21 ARP 表

条目介绍：

➢ **ARP 表**

接口： 显示 ARP 条目对应的网络接口。

IP 地址： 显示 ARP 条目中的 IP 地址。

MAC 地址： 显示 ARP 条目中 IP 对应的 MAC 地址。

类型： 显示 ARP 条目类型，例如“静态”或者“动态”。

9.7.2 静态 ARP

本页用于配置静态 ARP。

进入界面的方法：路由功能>>ARP>>静态 ARP

图 9-22 静态 ARP

条目介绍：

- **ARP 配置**

IP 地址： 设置 ARP 条目中的 IP 地址。

MAC 地址： 设置 ARP 条目中 IP 对应的 MAC 地址。

- **ARP 条目**

可以在此表中查看或删除当前的静态 ARP 条目。

9.8 RIP

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的动态路由协议，主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用RIP协议。RIP作为最早的内部网关协议（Interior Gateway Protocol，IGP）之一，由于实现比较简单，在配置和维护管理方面也远比OSPF和IS-IS容易，至今仍被广泛使用。RIP当前有RIPv1和RIPv2两个版本。

RIP采用距离矢量（Distance-Vector）算法，使用跳数来度量到达目的地址的距离，并定义含有跳数最少的路径为最优路径。路由器到与它直接相连网络的跳数为0，每经过一个路由器，跳数就加1。跳数被称为度量值。为限制收敛时间，RIP规定度量值的取值范围为0-15之间的整数，数值16表示无穷大，即目的网络不可达。正是由于这个限制，RIP不适合应用于大型网络。

- **RIP 应用场景**

RIP允许的最大跳数为15，因此RIP适用于规模较小的网络，比如校园网以及结构较简单的地区性网络，如下图所示：

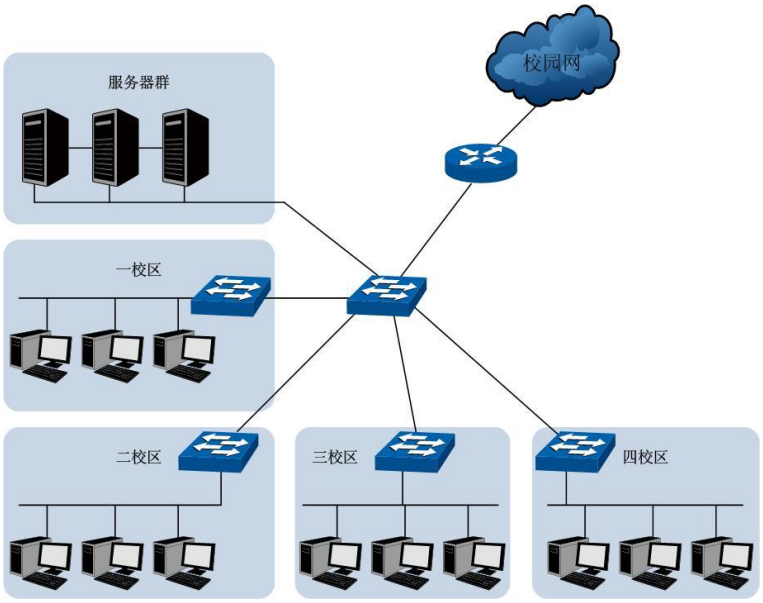


图 9-23 RIP典型应用场景

➢ **RIP 特性**

RIP有如下特性：

1) 设计单一。RIP 是典型的基于距离矢量（Distance-Vector）算法的动态路由协议，使用跳数作为度量值，并定义含有跳数最少的路径是最优路径。如果到相同目的站点有两条不同带宽的路径，但跳数相同，RIP 仍认为两条路径是等距离的。

2) 适用于规模较小的网络。RIP 规定度量值的取值范围为 0-15 之间的整数，数值 16 表示无穷大，即目的网络不可达。

3) RIP 是基于用户数据报协议（UDP）的协议。它通过 UDP 报文进行路由信息的交换，使用的端口号为 520。

4) 为提高性能，防止产生路由循环，RIP 支持水平分割和毒性逆转功能。

➢ **RIP 基本原理与实现**

RIP 要求路由器维护一个 RIP 路由表，该路由表记录了所有可达目的地的路由项。RIP 定期以广播形式（RIPv2 支持广播和组播两种方式）向所有邻居发送包含整个路由表的更新信息，并依赖邻居向它的邻居传递更新信息。其邻居路由器接收到这些信息后进行路由计算，更新路由表。

每条路由项都包含了如下信息：

- 目的网络：目的网络的 IP 地址和子网掩码。该 IP 地址和子网掩码共同决定了一个网络，到达该网络的报文可通过此路由条目进行转发。
- 下一跳地址：为到达目的网络，需要经过的相邻路由器的接口 IP 地址。
- 度量值：到达目的网络所需要的跳数。
- 接口名称：路由器转发报文通过的出接口。
- 老化时间：从路由条目最后一次被更新到现在所经过的时间。若该路由条目在超时计时器规定的时间内没有被更新，其跳数将被设为 16，表示网络不可达。

RIP 定义了两种报文类型：请求报文和响应报文（或称为更新报文）。

- 请求报文：向邻居路由器请求发送整个或部分路由表。
- 响应报文（更新报文）：可以是对邻居路由器的请求作出应答，也可以是主动向邻居路由器发送更新。

RIP 运行过程如下图所示：

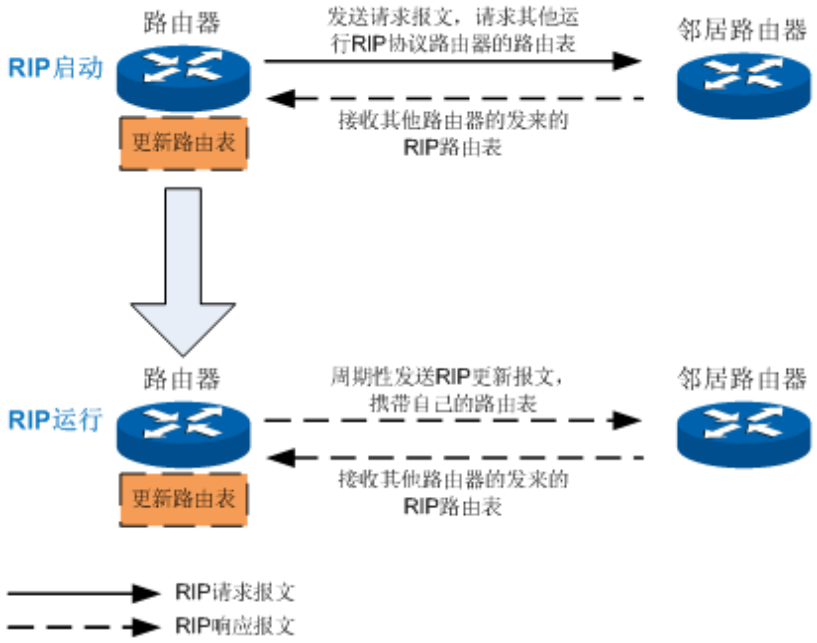


图 9-24 RIP 协议运行过程

1) RIP 路由表的形成

RIP 启动时的初始路由表中仅包含了本设备的一些直连接口路由信息。通过相邻设备互相学习路由表项，才能实现各网段路由互通。

a) RIP 初始化时，路由器会从每个启用 RIP 协议的接口广播请求报文。该请求报文包含当前路由器学习到的全部路由信息，即整个路由表，并向相邻设备请求完整的路由表。

b) 之后路由器不断地侦听来自其他路由器的 RIP 响应报文。接收到请求报文且启用 RIP 协议的邻居路由器会回送包含它们的路由表的响应报文。不关心路由更新信息的主机和其他设备则丢弃该请求报文。

c) 当发出请求报文的路由器收到响应报文时，它将开始处理附加在响应报文中的路由信息。对本地 RIP 路由表中尚未记录的路由表项，路由器直接将该路由信息添加到本地 RIP 路由表中；对本地已记录的路由表项，则按如下规则处理：

   - 如果已有表项和新表项的来源接口相同，则无条件地根据最新路由信息更新本地路由表；
   - 如果已有表项和新表现的来源接口不同，则比较它们的度量值，将度量值较小的作为自己的路由表项，如果度量值相同，则保留旧的表项。

这样，经过一段时间的路由信息收集以及更新，路由器就可以通过相邻设备收集整个网络的全部信息，完成网络收敛。

2) RIP 的更新与维护

为了应对网络拓扑变化，RIP 采用定期更新和老化机制来保证 RIP 路由表的实时性、有效性以及稳定性。RIP 协议在更新和维护路由信息时主要使用三个定时器，具体如下：

a) 更新计时器：路由器启动后，按照固定的时间间隔从每个启动 RIP 协议的接口广播更新报文（RIPv2 支持广播和组播两种方式发出更新报文）。该时间间隔由更新计时器决定，通常是 30 秒。更新报文包含了路由器的整个路由表。每个路由器的更新定时器都独立于网络中其他路由器，因此它们同时广播的可能性很小。

b) 超时计时器：路由器会为每一条新建的路由条目设置一个老化时间，如果路由器在老化时间内接收到该条目的更新报文，则保持该路由条目并将超时计时器初始化，重新计时；否则，该条目的跳数将被设置为 16，即目的网络不可达。该老化时间由超时计时器决定，通常是 180 秒即 6 个更新周期。

c) 垃圾回收计时器：路由器还为每条路由条目设置一个垃圾回收计时器，通常比超时计时器的时间长 60-240 秒。它定义了路由条目从跳数变为 16 到被清除的时间间隔。某个路由条目的超时计时器超时后，该条目的跳数将被设置为 16，如果到达垃圾回收计时器所规定的时间后，该路由条目仍没有得到更新，路由器将从路由表中彻底删除该条目。

防止环路机制：RIP 是通过邻居之间相互通告自己的路由表来建立和维护 RIP 路由表的，路由器并不知道网络的全局情况，不仅收敛速度慢，还存在发生路由环路的可能。为提高性能，防止产生路由环路，RIP 增加了下列特性，最大限度避免环路的产生。

1) 计数到无穷：将度量值等于 16 定义为无穷大，即网络不可达。当发生路由环路时，在环路中循环的路由条目的度量值增加到 16 之后即被认为不可达，这样可以有效防止路由条目在环路中无休止地传输。该功能默认启用。

2) 水平分割：路由器不会把从某个接口学到的路由信息再从该接口发送回去。这样路由器就不会接收到由自身传达出去的路由信息，既减少了带宽消耗，又可以防止路由环路。

3) 毒性逆转：RIP 从某个接口学到路由条目后，会将该路由条目的度量值设为 16，再从原来的接口发送回去，收敛速度比水平分割更快。当同时启用水平分割和毒性逆转时，只有毒性逆转功能生效。

4) 触发更新：一旦某条路由的度量值发生了变化，路由器就会立刻向邻居路由器发布更新报文，而不是等到更新周期到来再发送。触发更新机制可以避免在多个路由器之间形成路由环路，同时也可以加速网络的收敛速度。

说明：

RIPv2 有两种更新报文传送方式：广播方式和组播方式。RIPv2 默认通过组播方式发送报文，使用的组播地址是保留的 D 类地址 224.0.0.9。当开启 RIPv2 广播功能时，RIPv2 使用广播方式代替组播方式来通告信息，以便 RIPv1 接收。

➢ **RIP 的版本**

RIP 包括 RIPV1 和 RIPV2 两个版本，1988 年 RFC 1058 对 RIP 协议做了说明，后来被称为 RIPv1。1998 年，IETF 推出了 RIP 改进版本的正式标准 RFC 2453，即 RIPv2。需注意的是，RIPv2 不是 RIPv1 的替代，而是在 RIPv1 协议的基础上增加了一些扩展特性，应用更加灵活，以适用于现代网络的路由选择环境。

1) RIPv1

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

2) RIPv2

RIPv2 同 RIPv1 相比，是无类别路由协议，支持可变长子网掩码、报文认证、无类域间路由、外部路由标记和组播。在这些拓展特性中，最重要的就是路由选择更新条目增加了子网掩码的字段，因而 RIPv2 协议可以使用可变长的子网掩码，使其成为一个支持无类别路由选择的协议。拓展特性具体如下：

- 报文中携带自己的子网掩码信息，支持路由聚合和无类域间路由；
- 路由选择更新具有认证功能，能够验证某个路由选择更新报文的源的合法性；
- 报文中携带下一跳地址，在广播网上可以找到最优下一跳接口地址；
- 支持外部路由标记；
- 支持组播路由发送更新报文，减少资源消耗。

3) RIPv1 与 RIPv2 的兼容性

RIP 的协议规范充分考虑到 RIP 不同版本之间的兼容性。规范中约定如果 RIP 报文的版本字段值为 1 且报文中其他的未使用字段为非 0，那么 RIP 报文将被丢弃；如果版本字段值大于 1，那么 RIP 报文将会被处理，不过该报文中被 RIPv1 定义为未使用的字段将被忽略。因此，RIPv2 这种新协议版本可以向后兼容 RIPv1。

➢ **RIP 报文**

1) RIPv1 的报文格式

RIPv1 报文由头部和多个路由条目组成（一个 RIP 报文最多可以有 25 个路由条目）。报文头部包含一个命令标识和一个版本号。每个路由条目包含地址族标识、路由可达的 IP 地址和路由的跳数。如果某台路由器必须发送多于 25 条路由的更新报文，那么必须产生多条 RIP 报文。RIPv1 报文格式如图 10-30 所示：

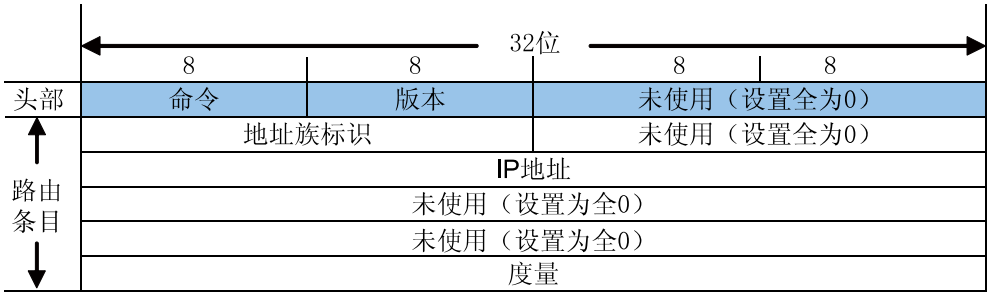


图 9-25 RIPv1 的报文格式

各字段的解释如下：

- 命令：取值 1 或 2，用以标识报文的类型。1 表示该报文为请求报文，2 表示该报文为响应报文。
- 版本：RIP 的版本号。取值 0x01，表示 RIPv1。
- 地址族标识：对于 IP 协议，该字段取值为 2。
- IP 地址：路由条目的目的 IP 地址，该字段可以是自然网段地址、子网地址或主机地址。

- 度量：即跳数，取值范围为 0-16。

2) RIPv2 的报文格式

RIPv2 的报文格式与 RIPv1 类似，所有相对于原来协议的拓展特性（路由标记，子网掩码和下一跳）都是由未使用的字段提供的，如图 10-31 所示。

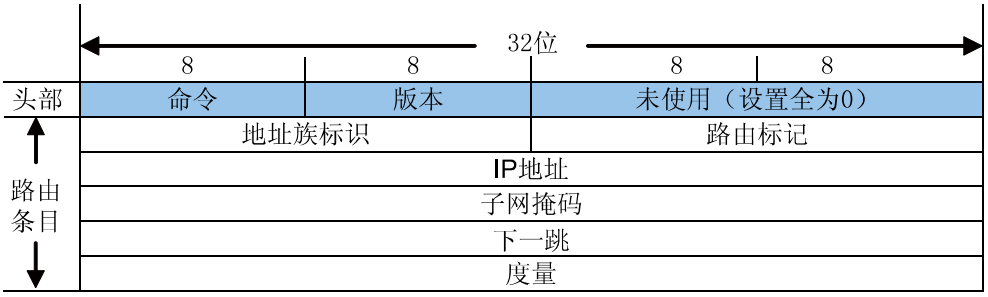


图 9-26 RIPV2 的报文格式

其中，与 RIPv1 不同的字段的解释如下：

- 版本：RIP 的版本号。取值 0x02，表示 RIPv2。
- 路由标记：用于支持外部网关协议。默认的情况是使用这个字段携带 RIP 引入的外部路由协议的路由的自主系统编号。如果使用 RIP 协议的路由器收到的路由条目中，该字段为非零，则直接向外通告该路由信息，如果该字段没有值，则需将该字段的值改为 0 再向外通告。RIP 协议本身并不使用这个字段。
- 子网掩码：是一个 32 位的掩码，用来标识 IPv4 地址的网络和子网部分。
- 下一跳：如果存在，它标识一个比发布此条路由信息的路由地址更优的下一跳地址。如果该字段为全 0（0.0.0.0），则表示发布此条路由信息的路由地址就是最优下一跳地址。

3) RIPv2 的认证报文格式

RIPv2 为了支持报文认证，使用第一个路由条目作为认证项，因此在含有认证的单个 RIPv2 响应报文中，最多可以携带的路由条目只有 24 条。RIPv2 通过将地址族标识字段的值设为 0xFFFF 标识报文携带认证信息。RIPv2 的认证报文格式如图 10-32 所示。

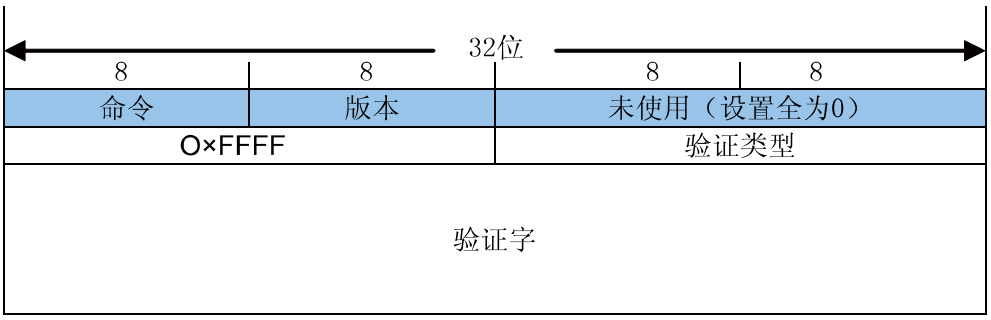


图 9-27 RIPv2 的认证报文格式

各字段的解释如下：

- 验证类型：取值 2 或 3。值为 2 时表示简单认证，值为 3 时表示 MD5 认证。
- 验证字：当使用简单认证时包含密码信息（密钥）；当使用 MD5 认证时包含密钥 ID 和密钥。该字段长度为 16 个八位组字节。

➢ **交换机特性**

1) 支持 RIPv1 和 RIPv2

本交换机同时支持 RIPv1 和 RIPv2 两种版本的协议，您可以根据实际的网络需求设置，以提高网络性能。

2) 自动汇聚

自动汇聚的原理是，同一个自然网段内的不同子网的路由在向外（其它网段）发送时聚合成一个网段的路由发送。RIPv1 的协议报文中没有携带掩码信息，故 RIPv1 发布的就是自然掩码的路由。RIPv2 支持自动汇聚，因为 RIPv2 报文携带掩码位，所以支持子网划分。在 RIPv2 中进行自动汇聚可提高大型网络的可扩展性和效率，缩减路由表。

本交换机支持基于 RIP 进程的有类聚合：聚合后的路由使用自然掩码的路由形式发布，RIPv2 聚合是按类聚和的，聚合得到最优的度量值。比如，对于 10.1.1.0 /24（度量值为 2）和 10.1.2.0 /24（度量值为 3）这两条路由，会聚合成自然网段路由 10.0.0.0 /8（度量值为 2）。但在启用了水平分割或毒性逆转的情况下，有类聚合将失效，这是因为水平分割或毒性逆转将抑制一些路由的发布，配置了有类聚合时一条聚合路由可能是聚合了从不同的接口上学到的路由，这样在向外发布时就会产生冲突。

3) 引入外部路由

在本交换机上，RIP 不仅可以通过与邻居交换路由表学习路由信息，还可以引入其他进程或其他协议例如静态路由学到的路由信息，从而丰富路由表项。

4) 路由重新分配

当路由器使用路由选择协议通告从其他方式学习到的路由时，路由器将执行重新分配。这里所谓的其他方式可能是另外一个路由选择协议、静态路由或直连目标网络。例如路由器可能同时运行静态路由进程和 RIP 进程。如果设置 RIP 进程通告来自静态路由进程的路由，这就叫做重新分配静态路由。IP 路由选择协议的能力相差非常大，对路由重新分配影响最大的协议特性是度量值和管理距离的差异性。

RIP 默认度量值：执行路由重新分配的路由器将为被重新分配的路由指派度量值。例如，运行 RIP 协议的路由器引入外部静态路由，路由器会为静态路由重新分配度量值，然后向其他运行 RIP 的路由器通告这些路由。在本交换机上，RIP 协议在引入外部路由时，为其重新分配的度量值默认为 12。

RIP 管理距离：当路由器正在运行多个路由选择协议，并从每个协议都学习到一条到达相同目标网络的路由。由于每一个路由选择协议均使用自己的度量方案定义最优路径，例如 RIP 使用跳数，而 EIGRP 使用带宽和时延，使得路由器无法通过比较度量值来选择最优路径。为了判断最优路径，各路由协议都被赋予了一个管理距离。管理距离被看作是一个可信度测度，管理距离的数值越小，协议的可信度越高。其中 255 表示任何来自不可信源端的路由。在本交换机上，RIP 的管理距离默认为 120。

RIP 模块主要用于配置交换机的 RIP 功能，包括**基本配置、接口配置**以及**路由表**三个部分。

9.8.1 基本配置

本页面用于开启全局 RIP 功能，配置 RIP 的全局属性以及使能和查看开启 RIP 协议的网段。

进入界面的方法：路由功能>>RIP>>基本配置

图 9-28 基本配置

条目介绍：

- **RIP 使能**

RIP 协议： 选择启用或禁用交换机的 RIP 该功能，默认为“禁用”。

- **全局配置**

RIP 版本： 选择使用的 RIP 协议版本，可选版本有 RIPv1 和 RIPv2。

- Default：仅发送 RIPv1 报文，但可接收 RIPv1 和 RIPv2 报文。
- RIPv1：仅发送和接收 RIPv1 报文。发送报文时采用广播方式。
- RIPv2：仅发送和接收 RIPv2 报文。发送报文时采用组播方式。

RIP 距离： 配置 RIP 协议的管理距离。取值范围为 1-255。管理距离被看作是一个可信度测度，管理距离数值越小，协议的可信度越高。其中 255 表示任何来自不可信源端的路由。默认为“120”。

默认度量值： 设置 RIP 协议在引入外部路由时的默认度量值，取值范围为 1-15，默认值为“1”。

引入外部静态路由： 选择使能或者禁用引入外部静态路由到 RIP 协议中，默认为“禁用”。

引入外部 OSPF 路由： 选择启用或者禁用引入外部 OSPF 路由到 RIP 协议中，默认为“禁用”。

引入静态路由度量值： 设置 RIP 协议在引入外部静态路由时的默认度量值，取值范围为 0-15。默认值为“0”。

引入 OSPF 路由的度量值： 设置 RIP 协议在引入外部 OSPF 路由时的默认度量值，取值范围为 0-15。

更新计时器： 填写 RIP 任务发送更新报文的间隔。取值范围为 1-100 秒，推荐设置为“30 秒”。

超时计时器： 填写路由条目的有效期，如果在此段时间内该条目未被更新，那么该条目所表达的路径将被自动设置为不可达。取值范围为 1-300 秒，推荐设置为“180 秒”（即 6 个更新周期）。

垃圾回收计时器： 垃圾回收计时器决定了路由条目从变为不可达到被彻底删除的时间间隔，如果一条路由条目变为不可达以后，并且在该段时间内仍未被更新，那么该条目将会被自动删除。取值范围为 1-500 秒，推荐设置为“120 秒”。

- **网段使能**

添加网段： 用于添加使能 RIP 协议的网段，是将交换机的接口开启 RIP 功能的唯一方法。添加一个网段之后，在该网段中的交换机接口将启动 RIP 协议。格式为 192.168.0.0。

- **RIP 网段列表**

选择： 列表中为已经使能 RIP 协议的网段，可勾选需要删除的条目并点击<删除>按钮进行删除，可多选。

已经添加网段： 显示已经使能 RIP 协议的网段。

说明：

如果需要修改交换机接口接收和发送 RIP 报文的版本，请在**路由功能>>RIP>>接口配置**进行相关配置。

RIP 全局配置步骤：

步骤	操作	说明
1	启用 RIP 协议	必选操作。在**路由功能>>RIP>>基本配置**页面选择启用 RIP 协议。
2	使能网段	必选操作。在**路由功能>>RIP>>基本配置**页面的网段使能部分，添加网段，开启该网段的 RIP 协议。该网段添加成功后，将在 RIP 网段列表中显示。

9.8.2 接口配置

本页面用于配置和查看运行 RIP 协议的接口及其运行参数。

进入界面的方法：路由功能>>RIP>>接口配置

图 9-29 接口配置

条目介绍：

- **接口配置**

选择： 勾选需要修改运行参数的接口，可多选。

接口 ID： 显示该接口的 ID。

接口状态： 显示接口的 RIP 运行状态，由 RIP 使能的网段决定。

RIP 发送版本： 选择接口所支持的发送报文的 RIP 版本号。

- RIPv1：发送报文使用 RIPv1 格式。
- RIPv2：发送报文使用 RIPv2 格式。

RIP 接收版本： 接口所支持的接收报文的 RIP 版本号。

- RIPv1：支持接收 RIPv1 格式的报文。
- RIPv2：支持接收 RIPv2 格式的报文。
- Both：同时支持接收 RIPv1 和 RIPv2 格式的报文。

被动接口： 抑制接口发送路由更新报文。

认证类型： 设置接口所接收和发送的报文是否使用认证功能，默认为“无”。只有使用相同认证类型和认证密码的设备能交换 RIP 报文。仅 RIPv2 支持报文认证功能。

- 无：不使用认证功能。
- 简单认证：使用简单密码进行认证。选择“简单认证”后，需要在“密钥”一栏输入认证时使用的密钥。该密钥将被添加在 RIP 报文首部，只有使用相同认证类型和密钥的设备能相互通信。
- MD5：使用 MD5 进行认证。选择“MD5”后，需要在“密钥 ID”和“密钥”栏中输入认证时使用的密钥 ID 和密钥。

密钥 ID: 设置 MD5 密钥时必须同时输入密钥 ID，该 ID 为 1-255 之间的一个整数。

密钥： 设置接口认证时使用的密匙。该密钥为一个字符串。

水平分割： 选择是否启用水平分割功能。启用以后，本设备不会把从某个接口学到的路由信息再从该接口发送回去。默认为“启用”。

毒性逆转： 选择是否启用毒性逆转功能。启用以后，RIP 从某个接口学到路由条目后，会将该路由条目的度量值设为 16，再从原来的接口发送回去。当同时启用水平分割和毒性逆转时，只有毒性逆转功能生效。该功能默认为“禁用”。

说明：

- 当 RIP 接收版本和发送版本的全局配置与接口配置不一致时，将以接口配置为准。
- RIPv1 不支持报文认证，因此当 RIP 版本号选择为 RIPv1，配置的认证信息（认证类型，密钥 ID 和密钥）不生效。当 RIP 的版本为 RIPv1 时，虽然在接口视图下仍然可以配置验证方式，但由于 RIPv1 不支持认证，因此该配置不会生效。

9.8.3 路由表

RIP 路由表为 RIP 协议独立维护的路由表，记录了通过 RIP 协议产生的路由信息。本页面用于显示目前通过 RIP 协议生成的路由信息。

进入界面的方法：路由功能>>RIP>>路由表

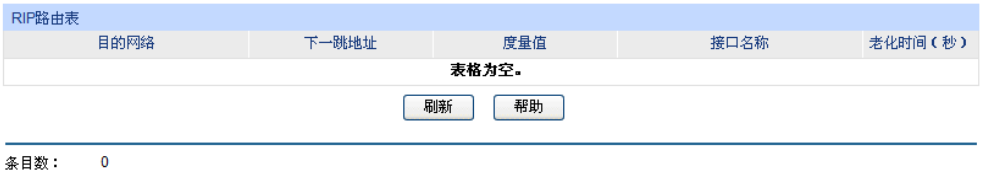


图 9-30 RIP 路由表

条目介绍：

- **RIP 路由表**

目的网络： 显示目的网络的 IP 地址和子网掩码。该 IP 地址和子网掩码共同决定了一个网络，到达该网络的报文可通过此路由条目进行转发。

下一跳地址： 显示为到达目的网络，需要经过的相邻路由器的接口 IP 地址。

度量值： 显示到达目的网络所需要的跳数。

接口名称： 显示对路由条目所指定的报文进行转发的接口名称。

老化时间： 显示从路由条目最后一次被更新到现在所经过的时间。若该路由条目未被更新，到达超时计时器所规定的时间后，其度量值会被设为无穷大；到达垃圾回收计时器所规定的时间后，路由条目将被删除。

9.8.4 RIP 的组网应用

- **组网需求**

1. 交换机 A 三个接口的 IP 地址分别为 1.1.1.1/24，2.1.1.1/24，3.1.1.1/24。交换机 B 三个接口的 IP 地址分别为 1.1.1.2/24，10.1.1.1/24，11.1.1.1/24。
2. 要求在交换机 A，B 的所有接口上使能 RIP，并使用 RIPv2 协议进行网络互连。

➢ **组网图**

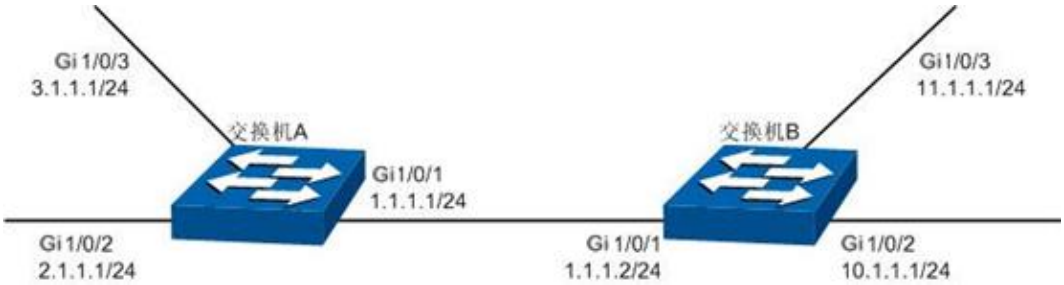


图 9-31 组网图

➢ **配置步骤**

● **配置交换机 A**

步骤	操作	说明
1	启用 RIP 协议	必选操作。在**路由功能>>RIP>>基本配置**页面启用 RIP 协议，选择 RIP 版本为 RIPv2。
2	使能接口所在网段	必选操作。在**路由功能>>RIP>>基本配置**页面的网段使能部分，添加网段 1.0.0.0，2.0.0.0，3.0.0.0，开启该网段的 RIP 协议。该网段添加成功后，将在 RIP 网段列表中显示。

● **配置交换机 B**

步骤	操作	说明
1	启用 RIP 协议	必选操作。在**路由功能>>RIP>>基本配置**页面开启 RIP 协议，选择 RIP 版本为 RIPv2。
2	使能接口所在网段	必选操作。在**路由功能>>RIP>>基本配置**页面网段使能部分，添加网段 1.0.0.0，10.0.0.0，11.0.0.0，开启该网段的 RIP 协议。该网段添加成功后，将在 RIP 网段列表中显示。

回目录

第10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。

10.1　QoS 配置

QoS(Quality of Service 即服务质量)功能用以提高网络传输的可靠性，提供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、可变迟延、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。

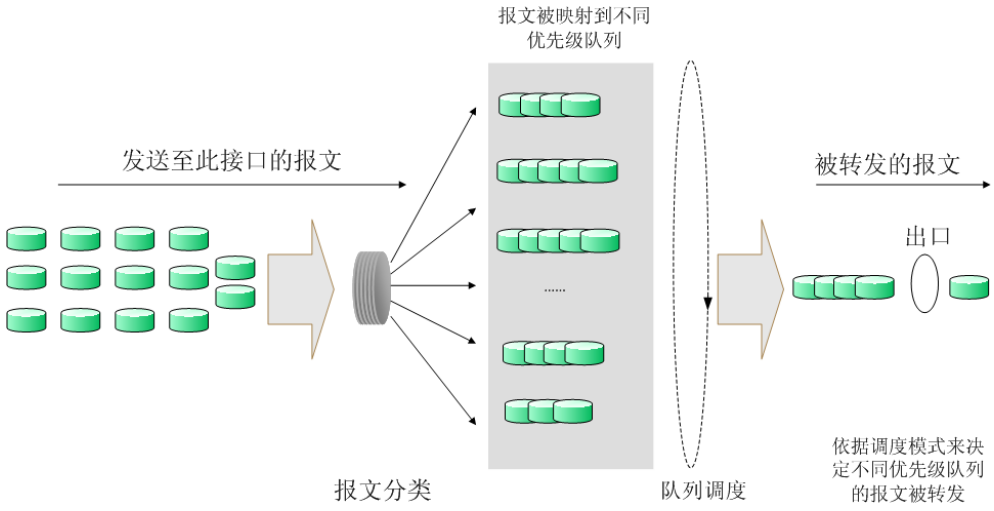


图 10-1 QoS 工作原理

- 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，数据流会根据入端口的 CoS 值以及 802.1P 中 CoS 到队列之间的映射关系来确定数据流的出口队列。

2. 802.1P 优先级

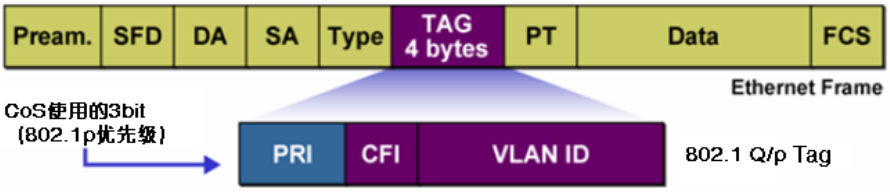


图 10-2 802.1Q 的帧格式

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

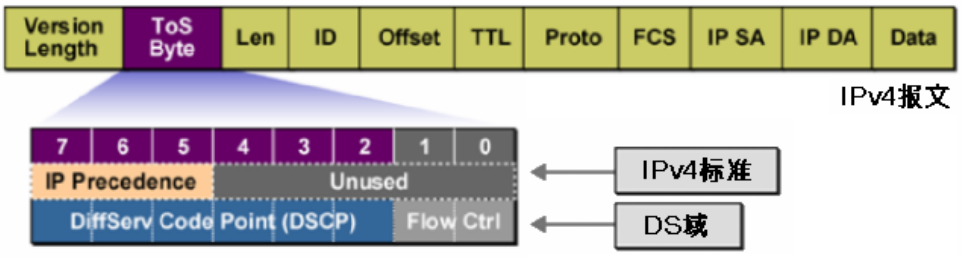


图 10-3 IP 报文

如图所示，IP 报文头部的 ToS（Type of Service，服务类型）字段共有 8bit，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 8 个调度队列—TC0 到 TC7，其中 TC0 对应最低优先级的队列，TC7 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 8 个出口队列，依次为 TC0-TC7，在 SP 队列模式下他们的优先级依次升高，TC7 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”。

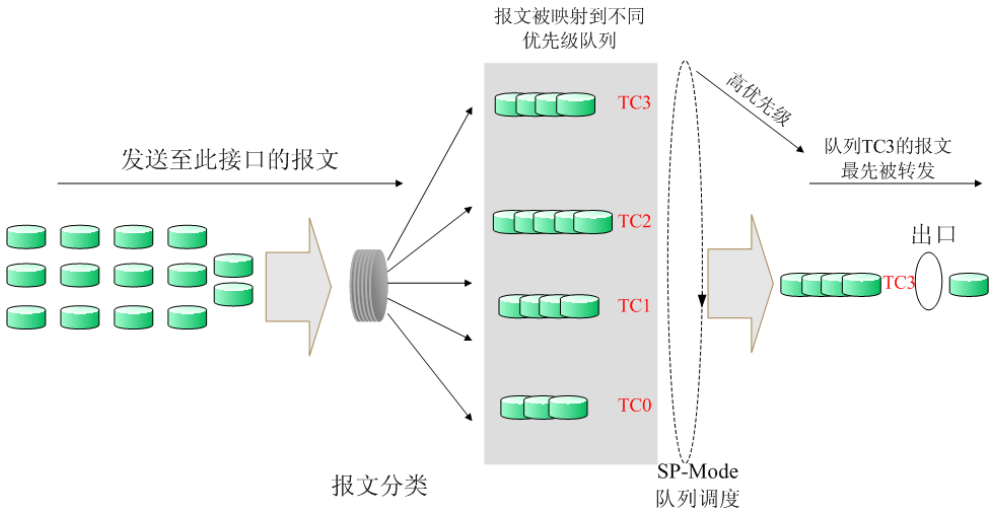


图 10-4 严格优先级模式

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-TC7 的默认权重比是 1:2:4:8:16:32:64:127。

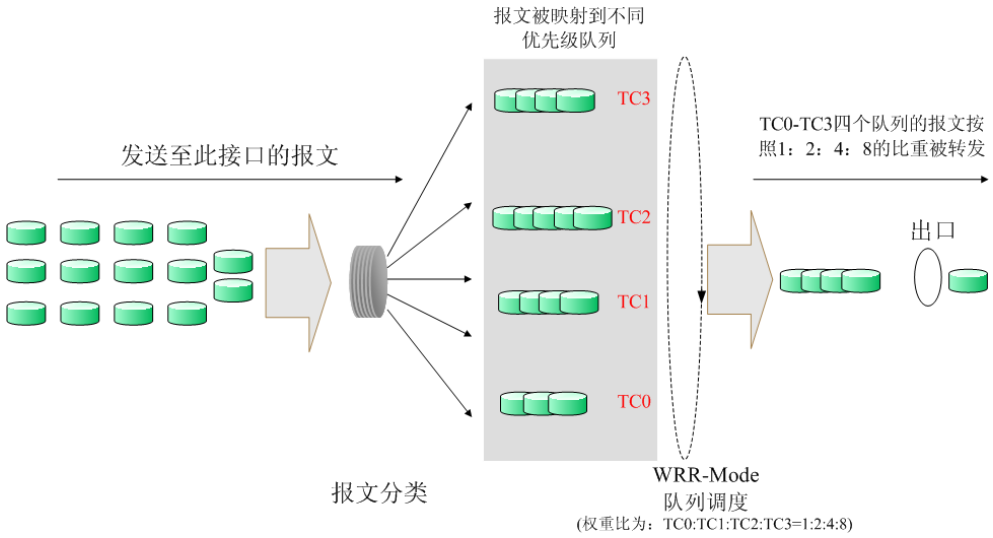


图 10-5 WRR 优先级模式

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 TC7 属于 SP 组；TC0~TC6 属于 WRR 组，权重比是 1:2:4:8:16:32:64。这样在调度的时候首先是 TC7 按照 SP 的调度模式独自占用带宽，然后是 WRR 组的成员 TC0~TC6 按照权重比 1:2:4:8:16:32:64 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 1:1:1:1:1:1:1:1。

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**、**调度模式**、**802.1P** 和 **DSCP** 四个配置页面。

10.1.1 端口配置

在基本配置页面中，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

图 10-6 基本配置

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**服务质量>>QoS 配置>>端口配置**页面设置各端口的优先级。
2	选择调度模式	必选操作。进入**服务质量>>QoS 配置>>队列调度模式**页面设置调度模式。

10.1.2 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…TC7 表示不同的优先级队列。

进入页面的方法：服务质量>>QoS 配置>>调度模式

图 10-7 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。 WRR 模式，TC 队列权重值配置范围为 1 到 127。
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 TC7 以及权重值配置为 0 的队列属于 SP 组。当进行队列调度时，TC7 以及其他权重值为 0 的队列按照 SP 模式占有带宽，其他的队列按照 WRR 模式及其配置的权重值占用相应的带宽。 SP+WRR 模式，队列权重值范围为 0 到 127，其中 0 代表队列配置为 SP 模式。
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 1:1:1:1:1:1:1:1。

队列权重值： 当选择为 WRR-Mode 或 SP+WRR-Mode 模式时，可以设置队列的权重值。

10.1.3 802.1P

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

图 10-8 802.1P

条目介绍：

- **优先级等级**

选择： 选择相应的 Tag-id/CoS-id 值进行优先级配置，可多选。

Tag-id/CoS-id： IEEE802.1P 协议里规定的 8 个优先级等级。

队列 TC-id： 对应不同等级的优先级队列。以 TC0,TC1…TC7 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**服务质量>>QoS 配置>>802.1P** 页面中，勾选条目，并设置优先级与队列的映射关系，点击<提交>。
2	选择调度模式	必选操作。进入**服务质量>>QoS 配置>>调度模式**页面设置调度模式。

10.1.4 DSCP

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

图 10-9 DSCP

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**

  选择： 选择相应的 DSCP 值进行优先级配置，可多选。

  DSCP： 数据包的 DSCP 优先级，优先级级别为 0-63。

  优先级： 对应不同优先级等级。以 COS0、COS1 … COS7 表示。

配置步骤：

步骤	操作	说明
1	启用 DSCP 优先级	必选操作。**服务质量>>QoS 配置>>DSCP** 页面中的**优先级配置**选择“启用”，点击<提交>。
2	设置 Dscp 值与优先级等级的映射关系	必选操作。在**服务质量>>QoS 配置>>DSCP** 页面中的**优先级等级**表格中设置 Dscp 值与优先级等级的映射关系。
3	选择调度模式	必选操作。进入**服务质量>>QoS 配置>>调度模式**页面设置调度模式。

10.2 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。

10.2.1 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

图 10-10 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。

10.2.2 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。

本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

图 10-11 风暴抑制

条目介绍：

- **风暴抑制**

UNIT：	选择一个 UNIT 显示端口信息。
选择：	勾选端口以配置风暴抑制参数，可多选也可不选。
端口：	勾选端口配置风暴抑制，可多选。
PPS 模式：	启用或禁用 PPS 模式。
广播包抑制单位：	选择广播包抑制单位。
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，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。
组播包抑制单位：	选择组播包抑制单位。
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，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 包抑制单位：	选择 UL 包抑制单位。
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，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。

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。

10.3 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 10-1 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	ACCESS：不支持。
		TRUNK：支持，但接入端口的缺省 VLAN 不能是语音 VLAN。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 TAG。
	UNTAG 语音流	ACCESS：支持。
		TRUNK：不支持。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 UNTAG。
手动模式	TAG 语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的缺省 VLAN 不能是语音 VLAN。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 TAG。
	UNTAG 语音流	ACCESS：支持。

		TRUNK：不支持。
		GENERAL：支持，但接入端口的缺省 VLAN 必须是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 UNTAG。

表 10-2 端口模式与语音数据流的处理关系

- **语音 VLAN 安全模式**

当端口使能了语音VLAN功能后，通过配置端口的安全模式还可以过滤数据流。若启用安全模式，则端口只转发语音数据包，对于其它源MAC地址不匹配OUI地址的数据包，端口将直接丢弃。若禁用安全模式，则端口转发所有数据包。

安全模式	报文类型	处理方式
启用	UNTAG 报文	当该报文源 MAC 地址是可识别的 OUI 地址时，允许该报文在语音 VLAN 内传输，否则将该报文丢弃。
	带有语音 VLAN TAG 的报文	
	带有其它 VLAN TAG 的报文	根据指定端口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受语音 VLAN 安全模式的影响。
禁用	UNTAG 报文	不对报文的源 MAC 地址进行检查，所有报文均可在语音 VLAN 内传输。
	带有语音 VLAN TAG 的报文	
	带有其它 VLAN TAG 的报文	根据指定端口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受语音 VLAN 安全模式的影响。

表 10-3 安全模式与各种数据的处理关系

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。

10.3.1 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、以及语音数据包的传输优先级等等。

进入页面的方法：服务质量>>语音 VLAN>>全局配置

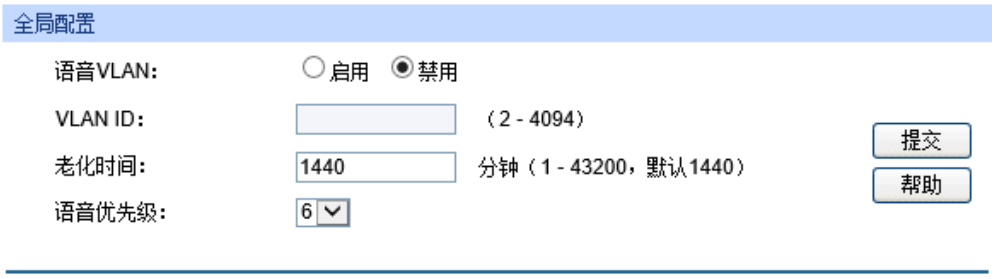


图 10-12 语音 VLAN 全局配置

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：	选择端口发送语音数据包时的数据传输优先级。

10.3.2 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

图 10-13 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： 设置端口转发数据包的模式。

- 禁用：端口转发所有数据。
- 启用：端口只转发语音数据。

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。

10.3.3 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加入语音 VLAN。

进入页面的方法：服务质量>>语音 VLAN>>OUI 配置

图 10-14 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**

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	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型，并根据表 10-2 设置语音设备连接端口的端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	添加 OUI 地址	可选操作。在**服务质量>>语音 VLAN>>OUI 配置**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。
4	使能端口语音 VLAN 特性	必选操作。在**服务质量>>语音 VLAN>>端口配置**页面设置语音 VLAN 中各端口的功能参数。
5	使能语音 VLAN	必选操作。在**服务质量>>语音 VLAN>>全局配置**页面中使能语音 VLAN 功能，并设置全局参数。

回目录

第11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。通过定义时间段可以设置 ACL 规则的生效时间，配置 policy 可以对匹配了 ACL 规则的数据包进行处理。

11.1 时间段配置

当用户配置的 ACL 规则需要在特定时间段生效时，可以先配置时间段，然后设置 ACL 规则直接引用该时间段即可。ACL 规则只在指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

本交换机可设置的时间段包括绝对时间、周期时间和节假日。绝对时间可以设置在自然日内的生效日期，周期时间则可以设置在每周的固定工作日生效，同时可以根据需要设置节假日来应对某些特殊意义的日期。在每个时间段内，还可以设置四个小的时间片段使生效时间更灵活。

本功能包括**时间段列表**、**新建时间段**和**节假日定义**三个配置页面。

11.1.1 时间段列表

在时间段列表页面，可以查看当前已添加的时间段信息。

进入页面的方法：访问控制>>时间段配置>>时间段列表

时间段列表

选择	序号	时间段名称	时间片段1	时间片段2	时间片段3	时间片段4	应用模式	操作
☐	1	t1	00:00-24:00	---	---	---	假日	编辑 | 查看
☐	2	t2	08:30-18:00	---	---	---	周期	编辑 | 查看

全选 删除 帮助

图 11-1 查看时间段列表

条目介绍：

- **时间段列表**

选择： 选择时间段条目进行删除。

序号： 显示时间段条目的序号。

时间段名称： 显示时间段的名称。

时间片段： 显示时间段中的时间片段。

应用模式： 显示时间段的应用模式。

操作： 点击相应按键可以查看或编辑相应时间段的详细配置信息。

11.1.2 新建时间段

在新建时间段页面，可以添加时间段信息。

进入页面的方法：访问控制>>时间段配置>>新建时间段

图 11-2 创建时间段

注意：

在此页面中，请先添加时间片段，点击<添加>按钮后，再定义时间段，否则无法配置成功。

条目介绍：

- **时间段定义**

  时间段名称： 填写时间段的名称，便于区分各个时间段的信息。

  节假日： 配置时间段的节假日模式。只有当系统日期在节假日内时，基于该时间段的 ACL 规则才能生效。

  绝对时间： 配置时间段的绝对时间模式。只有当系统日期在绝对时间内，基于该时间段的 ACL 规则才能生效。

  周期： 配置时间段的周期模式。只有当系统日期在周期时间内，基于该时间段的 ACL 规则才能生效。

- **时间片段**

  起始时间： 配置时间段中时间片段的起始时间。

  结束时间： 配置时间段中时间片段的结束时间。

- **时间片段列表**

  序号： 显示时间片段的序号。

  起始时间： 显示时间段中时间片段的起始时间。

  结束时间： 显示时间段中时间片段的结束时间。

操作： 点击删除即可删除相应的时间片段。

11.1.3 节假日定义

节假日定义可以提供与工作日不同的安全访问控制策略。在本页面，可以根据工作安排自行定义节假日。

进入页面的方法：访问控制>>时间段配置>>节假日定义

图 11-3 节假日定义

条目介绍：

- **节假日定义**

起始日期： 配置节假日起始日期。

终止日期： 配置节假日终止日期。

假日名称： 填写假日名称，请输入英文字符。

- **节假日列表**

选择： 选择节假日条目进行删除。

序号： 显示节假日条目的序号。

假日名称： 显示假日名称。

起始日期： 显示节假日起始日期。

终止日期： 显示节假日终止日期。

11.2 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**、**扩展 IP ACL** 和 **IPv6 ACL** 六个配置页面。

11.2.1 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

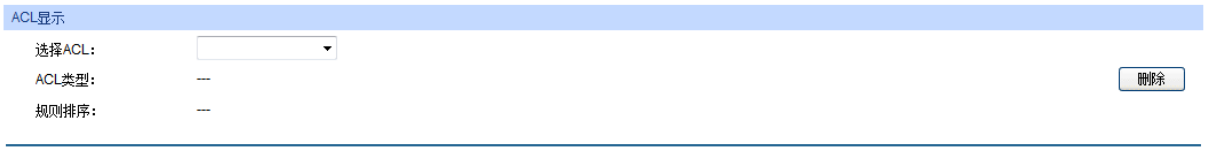


图 11-4 查看 ACL 列表

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。

11.2.2 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 11-5 创建 ACL

条目介绍：

- **创建 ACL**

ACL ID：	配置 ACL ID。
规则排序：	显示该 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。

11.2.3 MAC ACL

MAC ACL 根据数据包的源 MAC 地址、目的 MAC 地址、VLAN、二层协议类型等二层信息制定匹配规则，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

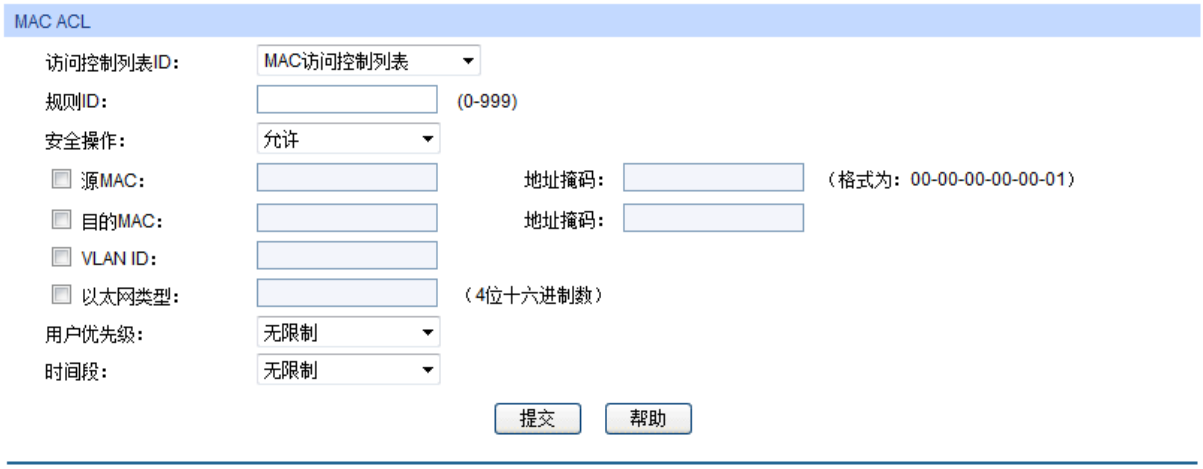


图 11-6 为 MAC ACL 添加规则

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。
VLAN ID：	配置规则包含的 VLAN 信息。
以太网类型：	配置规则包含的以太网类型信息。
用户优先级：	选择该规则对数据包的 tag 优先级字段的匹配要求。默认为无限制。
时间段：	选择规则生效的时间段名称。默认为无限制。

11.2.4 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

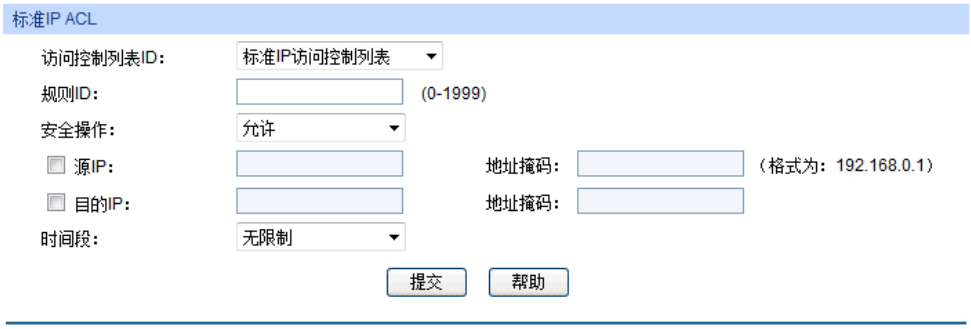


图 11-7 为标准 IP ACL 添加规则

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。
时间段：	选择规则生效的时间段名称。

11.2.5 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 11-8 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。

分片报文： 可勾选，作为分片报文。

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。

TCP Flag： 当 IP 协议选择 TCP 时，此处配置 Flag 匹配条件。

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。

DSCP： 填写规则包含的 DSCP 域信息。

IP ToS： 填写规则包含的 IP ToS 字段信息。

IP Pre： 填写规则包含的 IP Precedence 字段信息。

时间段： 选择规则生效的时间段名称。

11.3 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，处理方式包括流镜像、流监控、QoS 重标记和端口重定向。

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

11.3.1 Policy 列表

在 Policy 页面可以查看数据包处理方式，对匹配了 ACL 规则的数据包的执行相对应的处理方式。

进入页面的方法：访问控制>>Policy 配置>>Policy 列表

图 11-9 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，选择后点击删除按键即可。

- **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。

流镜像： 显示此 Policy 中的流镜像端口。

流监管： 显示该 Policy 中添加的流监管动作信息。

端口重定向： 显示该 Policy 中添加的端口重定向动作信息。

QoS 重标记： 显示该 Policy 中添加的 QoS 重标记动作信息。

操作： 点击<编辑>按键，可以对编辑相应的 policy 条目。

11.3.2 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

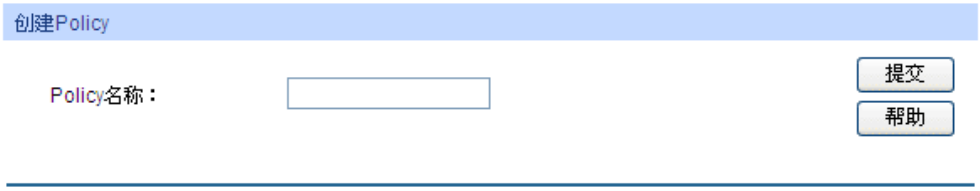


图 11-10 创建 Policy

条目介绍：

- **创建 Policy**

Policy 名称： 填写 Policy 的名称。

11.3.3 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>>配置 Policy

图 11-11 为 Policy 添加 ACL 并设置动作

条目介绍：

- **设置 Policy**

选择 Policy： 选择 Policy 的名称。

选择 ACL： 选择 ACL 作为 Policy 作用的对象。

流镜像： 配置该 Policy 的数据包执行流镜像动作，镜像到选定的端口。

流监管： 配置该 Policy 的数据包执行流限速动作。

- 额定速率：为匹配了相应 ACL 的数据包配置额定转发速率。
- 超速处理：为超过额定速率的数据包选择处理方式。

端口重定向： 配置该 Policy 的数据包执行端口重定向动作，改变转发端口。

- 指定出口端口：将匹配了相应 ACL 的数据包指定到固定端口转发。

QoS 重标记： 配置该 Policy 的数据包执行 QoS 动作，根据 QoS 功能具体配置情况转发。

- DSCP：为匹配了相应 ACL 的数据包指定 DSCP 域。
- 本地优先级：为匹配了相应 ACL 的数据包指定优先级。

11.4 ACL 绑定配置

绑定功能将 ACL 应用到某个端口或者 VLAN 上。只有将 ACL 和端口/VLAN 绑定才能生效；同样只有绑定了 ACL 的端口和 VLAN 才会对接收到的数据包根据规则进行匹配处理。

ACL 绑定配置功能包括**绑定列表、端口绑定**和 **VLAN 绑定**三个配置页面。

11.4.1 绑定列表

在此页面中可以查看已进行端口/VLAN 绑定的 ACL 条目。

进入页面的方法：访问控制>>ACL 绑定配置>>绑定列表

图 11-12 查看 ACL 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。

- **ACL 绑定 Vlan 列表**

显示 ACL 绑定 Vlan 条目信息。

- **ACL 绑定端口列表**

显示 ACL 绑定端口条目信息。

11.4.2 端口绑定

在此页面中可以将 ACL 与端口进行绑定。

进入页面的方法：访问控制>>ACL 绑定配置>>端口绑定

图 11-13 将 ACL 与端口进行绑定

条目介绍：

- **端口绑定配置**

ACL ID：	选择需要绑定的 ACL ID。
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。
ACL ID：	显示绑定的 ACL ID。
端口：	显示与相应 ACL 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。

11.4.3 VLAN 绑定

在此页面中可以将 ACL 与 VLAN 进行绑定。

进入页面的方法：访问控制>>ACL 绑定配置>>VLAN 绑定

图 11-14 将 ACL 与 VLAN 进行绑定

条目介绍：

- **VLAN 绑定配置**

  ACL ID： 选择需要绑定的 ACL ID。

  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。

  ACL ID： 显示绑定的 ACL ID。

  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。

配置步骤：

步骤	操作	说明
1	设置生效时间段	必选操作。在**访问控制>>时间段配置**三个标签页中配置 ACL 规则的生效时间段。
2	配置 ACL 规则	必选操作。在**访问控制>>ACL 配置**六个标签页中配置 ACL 规则对数据包进行匹配。
4	将 ACL 与端口/VLAN 绑定	必选操作。在**访问控制>>ACL 绑定配置**三个标签页中将 ACL 与端口/VLAN 进行绑定，将 ACL 应用到相应的端口/VLAN 上。

11.5 Policy 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。

Policy 绑定配置功能包括**绑定列表**、**端口绑定**和 **VLAN 绑定**三个配置页面。

11.5.1 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>>Policy 绑定配置>>绑定列表

图 11-15 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 Vlan 列表**

显示 Policy 绑定 Vlan 条目信息。

- **Policy 绑定端口列表**

显示 Policy 绑定端口条目信息。

11.5.2 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>>Policy 绑定配置>>端口绑定

图 11-16 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。

11.5.3 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>>Policy 绑定配置>>VLAN 绑定

图 11-17 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。

配置步骤：

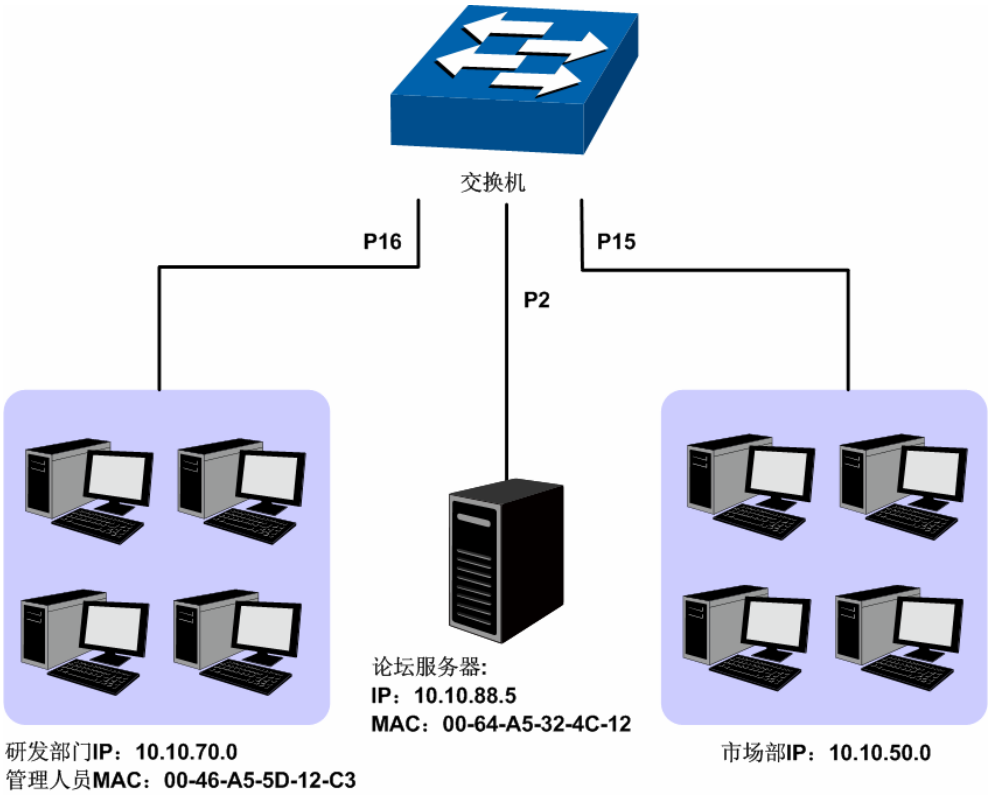
步骤	操作	说明
1	设置生效时间段	必选操作。在**访问控制>>时间段配置**三个标签页中配置 ACL 规则的生效时间段。
2	配置 ACL 规则	必选操作。在**访问控制>>ACL 配置**六个标签页中配置 ACL 规则对数据包进行匹配。
3	配置 Policy	必选操作。在**访问控制>>Policy 配置**三个标签页中配置 Policy，对匹配了相应 ACL 规则的数据包，可以通过 Policy 设置处理方式。
4	将 Policy 与端口/VLAN 绑定	必选操作。在**访问控制>>Policy 绑定配置**三个标签页中将 Policy 与端口/VLAN 进行绑定，将 Policy 应用到相应的端口/VLAN 上。

11.6 访问控制功能组网应用

- **组网需求**

1. 研发部门的管理人员自由访问公司论坛，管理人员 MAC 地址为 00-64-A5-5D-12-C3。
2. 研发部门工作人员在工作时间可以访问公司论坛。
3. 市场部人员在工作时间不能访问公司论坛。
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	配置时间段	在**访问控制>>时间段配置**功能处，新建时间段，描述为 work_time，时间段采用周期时间，周期时间选择工作日周一到周五，时间片段添加 08:00~18:00。
2	需求 1 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 11。 在**访问控制>>ACL 配置>>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；时间段选择无限制。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 manager。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 11 应用到 Policy manager。 在**访问控制>>Policy 绑定配置>>端口绑定**页面，选择 Policy manager 与端口 16 绑定。

步骤	操作	说明
3	需求 2、4 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 500。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 500，创建规则 1，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；时间段选择 work_time。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 500，创建规则 2，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；时间段选择无限制。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 500，创建规则 3，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 10.10.88.5，掩码为 255.255.255.255；时间段选择无限制。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 limit1。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 500 应用到 Policy limit1。 在**访问控制>>Policy 绑定配置>>端口绑定**页面，选择 Policy limit1 与端口 16 绑定。
4	需求 3、4 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 501。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 501，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 10.10.70.0，掩码为 255.255.255.0；时间段选择无限制。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 501，创建规则 5，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；时间段选择 work_time。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 limit2。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 501 应用到 Policy limit2。 在**访问控制>>Policy 绑定配置>>端口绑定**页面，选择 Policy limit2 与端口 15 绑定。

11.7 终端上网策略

终端上网策略：是一种能够满足不管用户身处何地、使用哪个 IP 地址，都可以保证该用户获得相同的网络访问权限的解决方案。

11.7.1 全局配置

在此页面中可以启用或禁止交换机的认证功能和策略功能。

进入页面的方法：访问控制>>终端上网策略>>全局配置

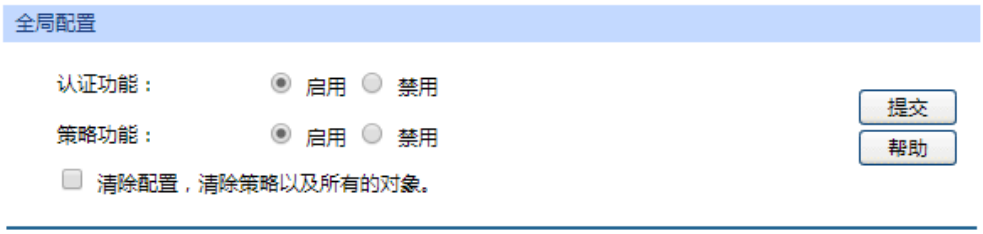


图 11-18 全局配置

条目介绍：

- **全局配置**

认证功能：	启用或禁用交换机的认证功能。
策略功能：	启用或禁用交换机的策略功能。
清除配置，清除策略以及所有对象	选择此选项以便清除策略以及所有的对象配置，包括用户组、IP 组、服务和时间段配置。

设置完成后，点击“提交”使配置生效。

回目录

第12章　网络安全

网络安全模块为保护局域网安全提供了多项安全措施，包括**四元绑定**、**DHCP 侦听**、**ARP 防护**、**IP 源防护**、**DoS 防护**、**802.1X 认证**和 **AAA** 七个部分，请根据实际需要进行配置。

12.1　四元绑定

四元绑定，是将计算机的 MAC 地址、IP 地址、所属 VLAN 以及与之相连的交换机的端口号四者绑定，以下这四个参数信息简称四元信息。该功能可以启用 ARP 防护，只有符合绑定关系的计算机才能访问网络。

本交换机支持如下三种四元绑定方式：

1) 手动绑定，通过手动方式绑定局域网用户的四元信息。当可以全面获取正确的局域网用户的四元信息时，可通过此方式进行绑定。

2) 扫描绑定：通过 ARP 扫描获取局域网用户的四元信息，并根据实际需要选择扫描结果进行绑定。此绑定方式只需在相应的功能页面输入 IP 地址段进行扫描。

3) DHCP 侦听：通过 DHCP 侦听功能侦听 DHCP 广播包，记录数据包中的 IP、MAC 和 VLAN ID 等信息。当局域网中搭建了 DHCP 服务器给局域网用户分配 IP 地址时，DHCP 侦听功能可以很方便地记录局域网用户的四元信息。

此三种方式也称为四元绑定条目的三个来源。三种来源的四元绑定条目信息必须完全不一致，以避免冲突。如果四元绑定条目发生冲突，只有“来源”优先级最高的条目生效。此三种来源方式中，手动绑定优先级最高，其次是扫描绑定，DHCP 侦听优先级最低。

本功能包括**绑定列表**、**手动绑定**和**扫描绑定**三个配置页面。

12.1.1 绑定列表

在绑定列表页面中，可以查看当前交换机已进行四元绑定的局域网计算机条目信息。

进入页面的方法：网络安全>>四元绑定>>绑定列表

图 12-1　查看四元绑定信息

条目介绍：

- **搜索条目**

来源： 选择查看不同来源的四元绑定条目。

- 全部来源：查看全部四元绑定条目。
- 手动添加：只查看手动添加的四元绑定条目。
- ARP 扫描：只查看通过 ARP 扫描获得的四元绑定条目。
- DHCP 侦听：只查看通过 DHCP 侦听获得的四元绑定条目。

IP： 根据所输 IP 快速查找四元绑定条目。

- **四元绑定表**

选择： 勾选条目可修改主机名、MAC 地址、VLAN ID、端口号以及防护范围，可多选。

主机名： 显示并编辑此条目的主机名。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示并编辑此条目的主机 MAC 地址。

VLAN ID： 显示并编辑此条目的 VLAN ID。

端口： 显示并编辑此条目的交换机端口号。

防护范围： 显示并编辑此条目支持的防护范围。

来源： 显示此条目的来源。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

注意：

- 冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。
- 多条“来源”优先级相同的条目中只有最后添加/修改的条目生效。

12.1.2 手动绑定

当已经获取了局域网用户的四元信息时，可以将四元信息静态绑定。

进入页面的方法：网络安全>>四元绑定>>手动绑定

图 12-2 手动绑定四元信息

条目介绍：

- **手动绑定**

主机名	输入主机描述名称
IP 地址	输入主机 IP 地址
MAC 地址	输入主机 MAC 地址
VLAN ID	输入 VLAN ID
防护范围：	选择此条目支持的防护范围。
端口：	选择主机连接的交换机端口。
绑定：	点击此按键将上述输入信息进行绑定。

- **手动绑定条目**

选择：	勾选条目进行删除。
主机名：	显示主机描述名称。
IP 地址：	显示主机 IP 地址。
MAC 地址：	显示主机 MAC 地址。
VLAN ID：	显示 VLAN ID。
端口：	显示主机连接的交换机端口。
防护范围：	显示此条目支持的防护范围。
来源：	显示条目来源。
冲突：	显示此绑定条目与其它条目的冲突状态。 ● 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。 ● 严重：已确定的冲突条目。

12.1.3 扫描绑定

ARP（Address Resolution Protocol，地址解析协议）用于将网络层的 IP 地址解析为数据链路层地址。IP 地址只是主机在网络层中的地址，如果要将网络层中数据包传送给目的主机，必须知道目的主机的数据链路层地址（比如以太网络 MAC 地址）。因此必须将 IP 地址解析为数据链路层地址。

ARP 协议用于将 IP 地址解析为 MAC 地址，并在主机内部维护一张 ARP 表，记录最近与本主机通信的其它主机的 MAC 地址与 IP 地址的对应关系。当主机需要与陌生主机通信时，首先进行 ARP 地址解析，ARP 地址解析过程如图 13-3 所示：

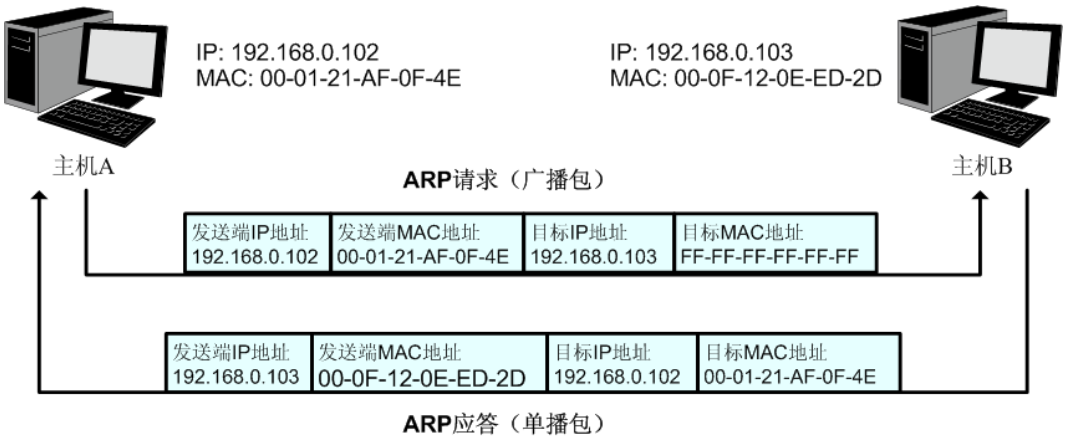


图 12-3 ARP 地址解析图

1) A 在自己的 ARP 表中查询是否存在主机 B 的 IP 地址和 MAC 地址的对应条目。若存在，直接向主机 B 发送数据。若不存在，则 A 向整个局域网中广播一份称为“ARP 请求”的数据链路帧，这个请求包含发送端（即主机 A）的 IP 地址和 MAC 地址以及接收端（即主机 B）的 IP 地址。

2) 局域网的每个主机接收到主机 A 广播的 ARP 请求后，目的主机 B 识别出这是发送端在询问它的 IP 地址，于是给主机 A 发出一个 ARP 应答。这个应答包含了主机 B 的 MAC 地址。

3) 主机 A 接收到主机 B 发出的 ARP 应答后，就将主机 B 的 IP 地址与 MAC 地址的对应条目添加自己的 ARP 表中，以便后续报文的转发。

扫描绑定功能即通过交换机向局域网或 VLAN 发送指定 IP 段的 ARP 请求报文，当收到相应的 ARP 应答报文时，将分析 ARP 应答报文来获得四元信息。由此可见，通过扫描绑定功能可以很方便的将局域网用户的四元信息进行绑定。

进入页面的方法：网络安全>>四元绑定>>扫描绑定

图 12-4 扫描绑定四元信息

条目介绍：

- **ARP 扫描**

  起始 IP 地址： 输入起始 IP 地址。

  结束 IP 地址： 输入结束 IP 地址。

VLAN ID: 输入 VLAN ID，在相应的 VLAN 中进行扫描。若留空，则发送 untag 数据包进行扫描。

扫描： 点击<扫描>按键将对局域网计算机进行扫描。

➢ **扫描结果**

选择： 勾选条目进行删除。

主机名： 显示主机描述名称或对主机进行描述以便区分。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示主机 MAC 地址。

VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示此条目支持的防护范围或者对此条目开启防护功能。

来源： 显示条目来源。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

12.2 DHCP 侦听

随着网络规模的不断扩大和网络复杂度的提高，经常出现计算机的数量超过可供分配的 IP 地址的情况。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。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，并有效解决了上面这些问题。

➢ **DHCP 工作原理**

DHCP 采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现网络资源的动态配置。通常一台服务器可以为多台客户端分配 IP，如图 13-5 所示：

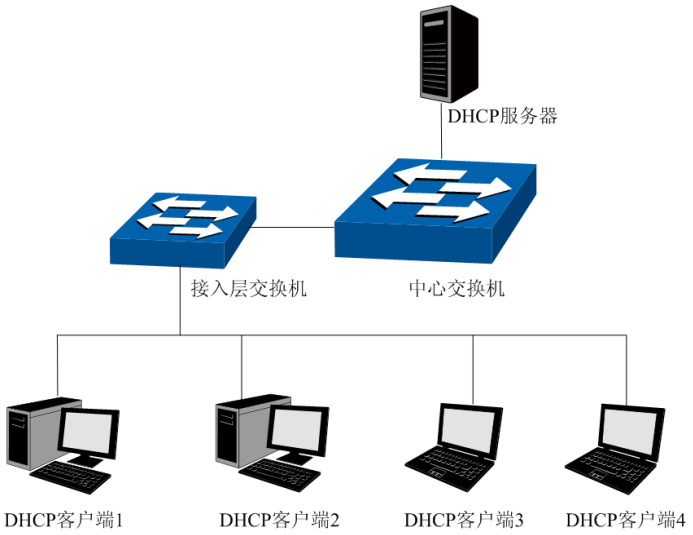


图 12-5 DHCP 网络典型应用

针对 DHCP 客户端的需求不同，DHCP 服务器提供三种 IP 地址分配策略：

1) 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定 IP 地址。通过 DHCP 将固定 IP 地址分配给客户端。

2) 自动分配地址：DHCP 服务器为客户端分配租期为无限长的 IP 地址。

3) 动态分配地址：DHCP 服务器为客户端分配具有一定有效期限的 IP 地址，当使用期限到期后，客户端需要重新申请地址。

绝大多数客户端均通过动态分配地址的方式获取 IP 地址，其获取 IP 地址的过程如下图所示：

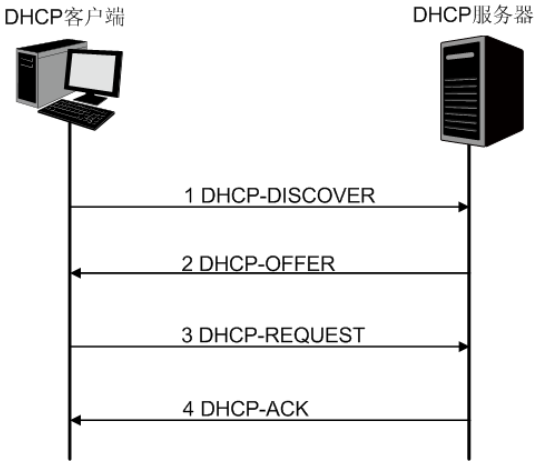


图 12-6 动态获取 IP 地址的过程

1) 发现阶段，客户端以广播方式发送 DHCP-DISCOVER 报文寻找 DHCP 服务器。

2) 提供阶段，DHCP 服务器接收到客户端发送的 DHCP-DISCOVER 报文后，根据 IP 地址分配的优先次序从地址池中选出一个 IP 地址，与其它参数一起通过 DHCP-OFFER 报文发送给客户端（发送方式根据客户端发送的 DHCP-DISCOVER 报文中的 flag 字段决定，具体请见 DHCP 报文格式的介绍）。

3) 选择阶段，如果有多台 DHCP 服务器向该客户端发来 DHCP-OFFER 报文，客户端只接受第一个收到的 DHCP-OFFER 报文，然后以广播方式发送 DHCP-REQUEST 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。

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

- **Option 82**

DHCP 报文格式基于 BOOTP 的报文格式，共有 8 种类型的报文，每种报文的格式相同。DHCP 和 BOOTP 消息的不同主要体现在选项（Option）字段，并利用 Option 字段来实现功能扩展。例如 DHCP 可以利用 Option 字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。更多 DHCP Option 选项的介绍，请参见 RFC 2132。

Option 82 选项记录了 DHCP 客户端的位置信息，交换机接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制订 IP 地址和其它参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。目前本交换机对子选项的填充内容如下，电路 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址。

- **DHCP 服务欺骗攻击**

在 DHCP 工作过程中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，不仅会给网络造成混乱，也对网络安全造成很大威胁。这种网络中出现非法的 DHCP 服务器，通常分为两种情况：

1) 用户不小心配置的 DHCP 服务器，由此引起的网络混乱非常常见。

2) 黑客将正常的 DHCP 服务器中的 IP 地址耗尽，然后冒充合法的 DHCP 服务器，为客户端分配 IP 地址等配置参数。例如黑客利用冒充的 DHCP 服务器，为用户分配一个经过修改的 DNS 服务器地址，在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站，骗取用户的帐户和密码，如图 13-7 所示。

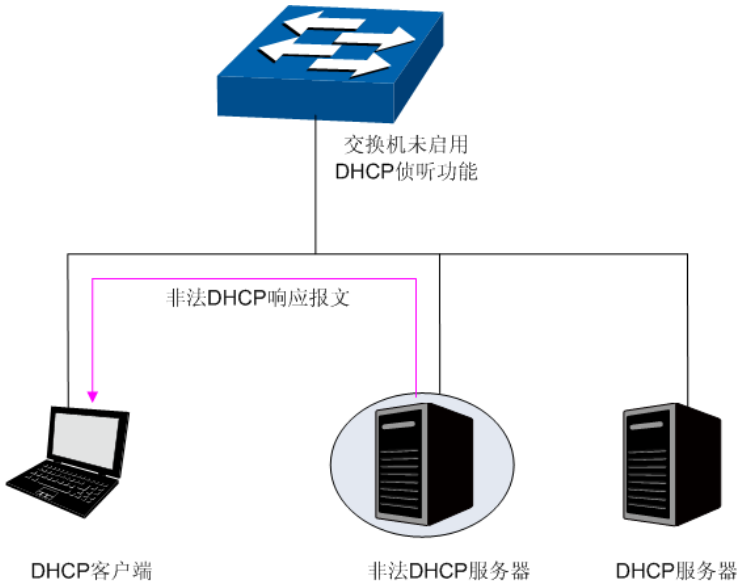


图 12-7 DHCP 服务欺骗攻击

DHCP 侦听是运行在交换机上的一种 DHCP 安全特性。通过设置 DHCP 服务器的连接端口为授信端口，只处理授信端口发来的 DHCP 响应报文；通过监听 DHCP 报文，记录用户从 DHCP 服务器获取局域网用户的四元信息，进行绑定后与 ARP 攻击防护配合使用；同时也可以过滤不可信任的 DHCP 信息，防止局域网中发生 DHCP 服务欺骗攻击，提高网络的安全性。

12.2.1 全局配置

在此页面可以配置 DHCP 侦听功能全局参数。

进入页面的方法：网络安全>>DHCP 侦听>>全局配置

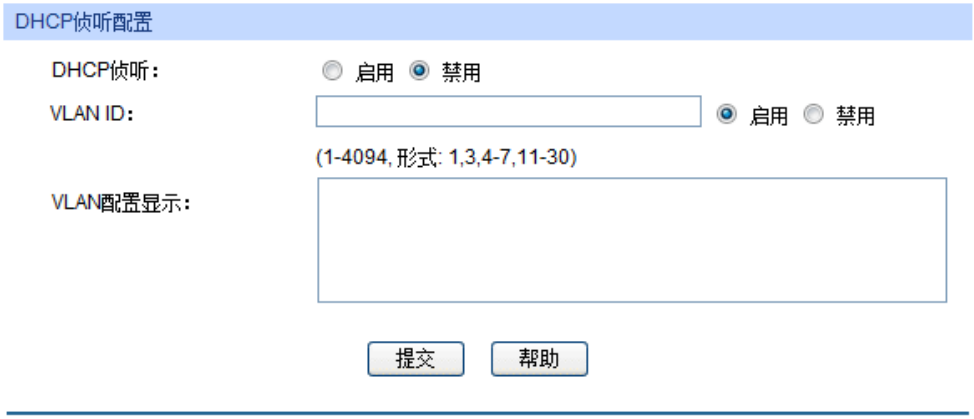


图 12-8 DHCP 侦听全局配置

条目介绍：

- **DHCP 侦听配置**

DHCP 侦听：	选择是否启用 DHCP 侦听功能。
VLAN ID：	在指定 VLAN 中使能或者禁用 DHCP 侦听功能。

VLAN 配置显示： 显示已使能 DHCP 侦听功能的 VLAN ID。

注意：

若 LAG 组成员端口需要配置 DHCP 侦听功能，请保持端口的参数一致。

12.2.2 端口配置

在此页面可以进行 DHCP 侦听端口配置。

进入页面的方法：网络安全>>DHCP 侦听>>端口配置

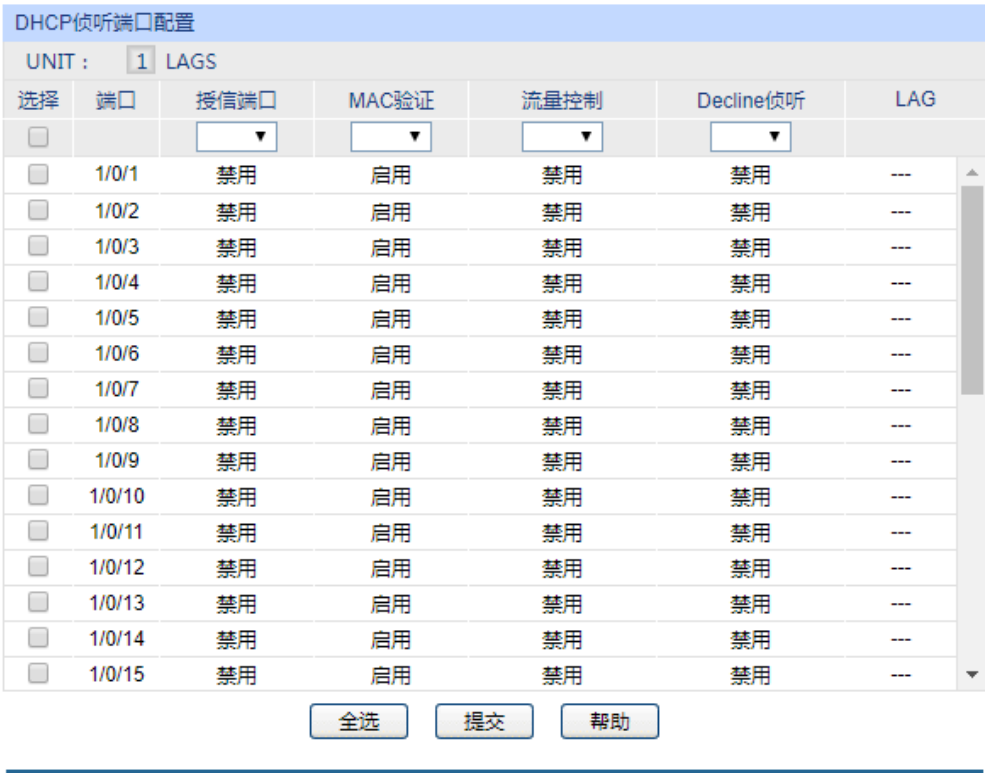


图 12-9 DHCP 侦听端口配置

条目介绍：

- **端口配置**

UNIT： 选择一个 UNIT 显示端口信息。

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。

授信端口： 选择是否配置端口为授信端口，只有授信端口才正常转发来自正常 DHCP 服务器端的消息，请将连接有 DHCP 服务器的端口设为授信端口。

MAC 验证： 选择是否启用 MAC 验证功能。DHCP 消息中有两个字段存储着客户端的 MAC 地址，MAC 验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

流量控制： 选择是否对 DHCP 数据包启用流量控制功能，超出流量部分的 DHCP 数据包将被丢弃。

Decline 侦听： 选择是否启用端口的 Decline 侦听功能。

LAG： 显示端口当前所属的汇聚组。

12.2.3 Option 82 配置

交换机可以利用 Option 82 字段传递控制信息和网络配置参数，为客户端提供更加丰富的网络配置信息。Option 82 功能的配置只有在 DHCP 侦听功能开启之后才会生效。

进入页面的方法：网络安全>>DHCP 侦听>>Option 82 配置

图 12-10 DHCP 侦听 Option 82 配置

条目介绍：

- **Option 82 配置**

UNIT： 选择一个 UNIT 显示端口信息。

选择： 勾选端口配置 Option 82 参数，可多选。

端口： 显示交换机的端口号。

Option 82 支持： 选择是否启用 Option 82 功能。

已有 Option 82 处理： 当客户端的 DHCP 请求报文已经有 Option 82 字段时，选择对此字段的操作。

- 保留：保留数据包中的 Option 字段信息。

- 替换：替换数据包中的 Option 字段信息，替换为交换机自定义的系统选项内容。
- 丢弃：丢弃包含 Option 82 字段的数据包。

电路 ID 自定义： 选择是否开启电路 ID 自定义。如果关闭，则 ID 默认为收到报文的 VLAN 和端口字段。

电路 ID 子选项： 输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。

远程 ID 自定义： 选择交换机是否自定义 Option 82 选项内容。

远程 ID 子选项： 输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。

LAG： 显示端口当前所属的汇聚组。

12.3 ARP 防护

根据 13.1.3 扫描绑定所述的 ARP 地址解析过程可知，利用 ARP 协议，可以实现相同网段内的主机之间正常通信或者通过网关与外网进行通信。但由于 ARP 协议是基于网络中的所有主机或者网关都为可信任的前提制定的，因此在实际复杂的网络中，此过程存在大量的安全隐患，从而导致针对 ARP 协议的欺骗攻击非常常见。网关仿冒、欺骗网关、欺骗终端用户和 ARP 泛洪攻击均是在学校等大型网络中常见的 ARP 攻击，以下简单介绍这几种常见攻击：

- **网关仿冒**

攻击者发送错误的网关 MAC 给受害者，而网络中的受害者收到这些 ARP 响应报文时，自动更新 ARP 表，导致不能正常访问网络。如图 13-11 所示。

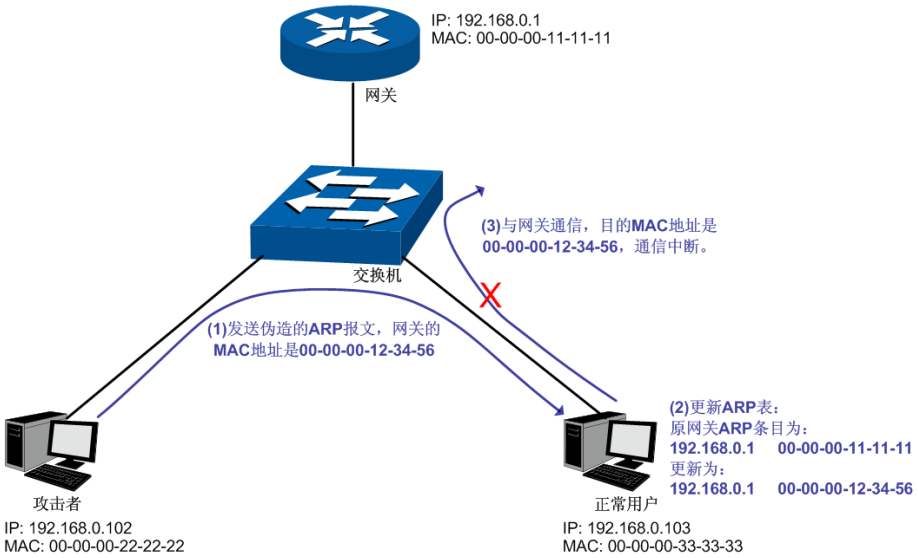


图 12-11 ARP 攻击-网关仿冒示意图

如图，攻击者发送伪造的网关 ARP 报文给局域网中的正常用户，相应的局域网用户收到此报文后更新自己的 ARP 表项。当局域网中正常用户要与网关进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **欺骗网关**

攻击者发送错误的终端用户的 IP/MAC 的对应关系给网关，导致网关无法和合法终端用户正常通信。如图 13-12 所示。

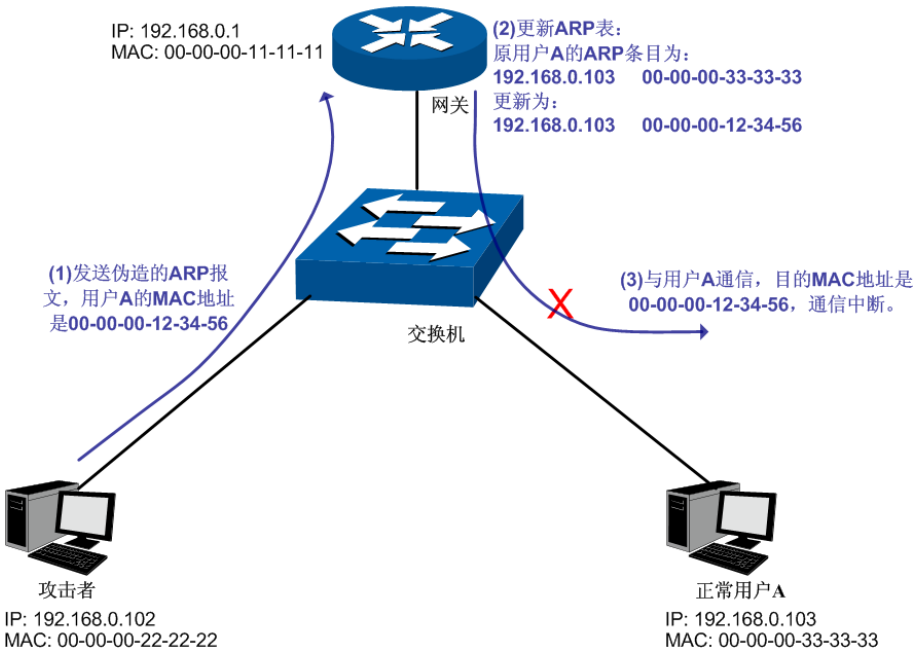


图 12-12 ARP 攻击-欺骗网关示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给网关，网关收到此报文后更新自己的 ARP 表项，当网关与局域网中用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **欺骗终端用户**

攻击者发送错误的终端用户/服务器的 IP/MAC 的对应关系给受害的终端用户，导致同网段内两个终端用户之间无法正常通信。如图 13-13 所示。

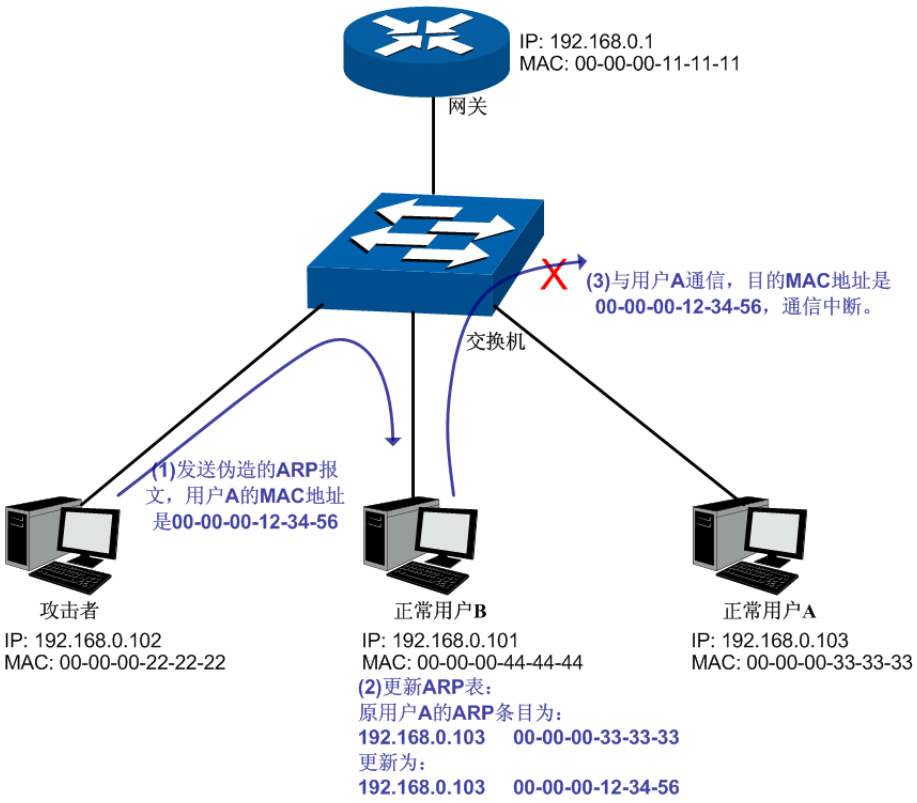


图 12-13 ARP 攻击-欺骗普通用户示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给用户 B，用户 B 收到此报文后更新自己的 ARP 表项，当用户 B 与用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- **中间人攻击**

攻击者不断向局域网中计算机发送错误的 ARP 报文，使受害主机一直维护错误的 ARP 表项。当局域网主机互相通信时，将数据包发给攻击者，再由攻击者将数据包进行处理后转发。在这个过程中，攻击者窃听了通信双方的数据，而通信双方对此并不知情。这就是中间人攻击。如图 13-14 所示。

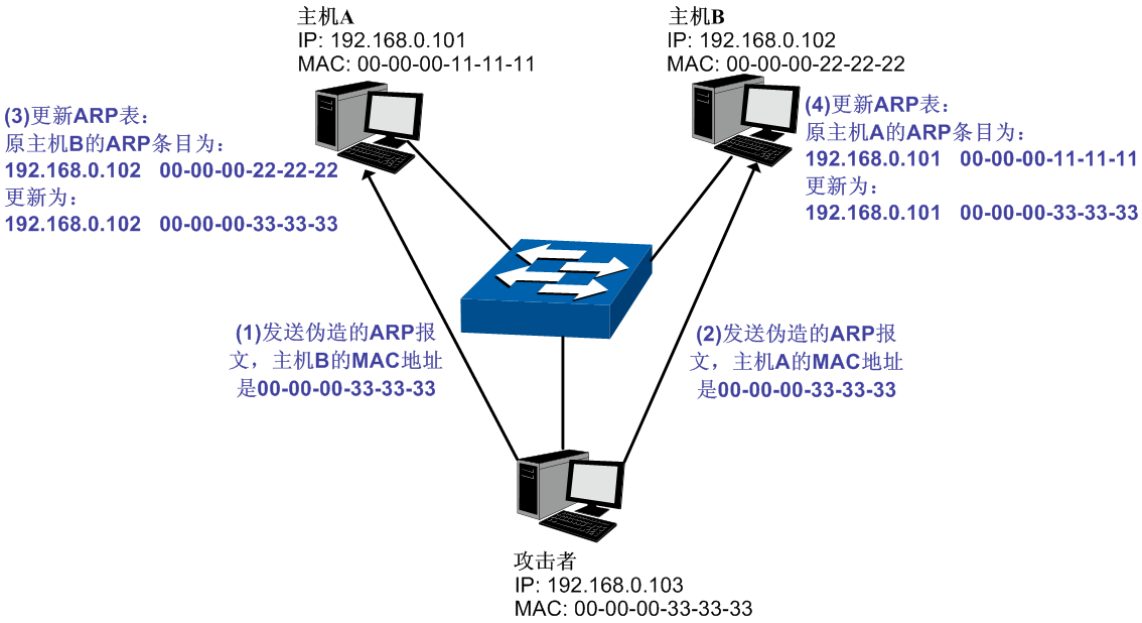


图 12-14 中间人攻击

假设同一个局域网内，有 3 台主机通过交换机相连：

A 主机：IP 地址为 192.168.0.101，MAC 地址为 00-00-00-11-11-11；

B 主机：IP 地址为 192.168.0.102，MAC 地址为 00-00-00-22-22-22；

攻击者：IP 地址为 192.168.0.103，MAC 地址为 00-00-00-33-33-33。

1. 首先，攻击者向主机 A 和主机 B 发送伪造的 ARP 应答报文。
2. A 主机和 B 主机收到此 ARP 应答后，更新各自的 ARP 表。
3. A 主机和 B 主机通信时，将数据包发送给错误的 MAC 地址，即攻击者。
4. 攻击者窃听了通信数据后，将数据包处理后再转发到正确的 MAC 地址，使 A 主机和 B 主机保持正常的通信。
5. 攻击者连续不断地向 A 主机和 B 主机发送伪造的 ARP 响应报文，使二者的始终维护错误的 ARP 表。

在 A 主机和 B 主机看来，彼此发送的数据包都是直接到达对方的，但在攻击者看来，其担当的就是“第三者”的角色。这种嗅探方法，也被称作“中间人”的方法。

- **ARP 泛洪攻击**

攻击者伪造大量不同 ARP 报文在同网段内进行广播，消耗网络带宽资源，造成网络速度急剧降低；同时，网关学习此类 ARP 报文，并更新 ARP 表，导致 ARP 表项被占满，无法学习合法用户的 ARP 表，导致合法用户无法访问外网。

在本交换机中，通过四元绑定功能在用户接入交换机时即对用户的四元信息进行绑定；而在 ARP 防护功能中则利用在交换机中绑定的四元信息对 ARP 报文进行检查，过滤非法 ARP 报文。通过上述两步可以很好的对局域网中 ARP 攻击进行防御。

本功能包括**防 ARP 欺骗**、**防 ARP 攻击**和**报文统计**三个功能配置页面。

12.3.1 防 ARP 欺骗

防 ARP 欺骗功能，通过四元绑定表对交换机收到的 ARP 报文进行检查，过滤非法的 ARP 报文，以此防御局域网中的 ARP 攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 欺骗

图 12-15 防 ARP 欺骗

条目介绍：

- **全局配置**

  源 MAC 验证： 当此功能开启后，ARP 防护功能会检查 ARP 报文的源 MAC 是否等于发送 MAC，如果不等则将报文丢弃。

  目的 MAC 验证： 当此功能开启后，ARP 防护功能会检查 ARP 回复报文的目的 MAC 是否等于目标 MAC，如果不等则将报文丢弃。

  IP 验证： 当此功能开启后，ARP 防护功能会检查报文的 IP 合法性，如果 IP 字段不合法则将报文丢弃。

- **使能 VLAN**

  VLAN ID： 需要配置的 VLAN ID。

  Logging： 是否开启 Log 功能。

- **VLAN 配置**

  选择： 勾选条目配置条目状态，可多选。

  VLAN ID： 显示 VLAN ID。

  状态： 显示功能使能状态。

  Logging： 显示 Log 功能使能状态。

12.3.2 防 ARP 攻击

防 ARP 攻击功能对交换机的各端口处理的合法 ARP 数据包设定阀值，在单位时间内不可超过设定值。超过设定值时，交换机将停止处理 ARP 数据包 300 秒，能够有效的避免 ARP 泛洪攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 攻击

图 12-16 防 ARP 攻击

条目介绍：

- **端口配置**

选择：	勾选端口配置端口防 ARP 攻击功能参数，可多选。
端口：	显示交换机的端口号。
信任：	选择是否启用端口的信任状态。
速率：	填写端口每秒允许接收的 ARP 数据包个数。
限速周期：	设置连续的周期时间来监视端口上是否超速，仅当周期内持续处于超速状态后，ARP 防护会断开端口的连接，防止 ARP 报文的冲击。
状态：	显示端口当前防 ARP 攻击状态。
操作：	点击<恢复>按键使端口恢复正常状态，并重新启用防 ARP 攻击功能。

12.3.3 报文统计

通过报文统计功能，可以直观地查看各个端口收到的非法 ARP 数据包个数，并以此定位网络问题，并采取相应的防护措施。

进入页面的方法：网络安全>>ARP 防护>>报文统计

图 12-17 报文统计

条目介绍：

- **自动刷新**

  自动刷新： 设置是否自动刷新端口统计情况。

  刷新周期： 设置自动刷新周期。

- **ARP 非法数据包统计**

  VLAN ID： 开启 ARP 防护的 VLAN ID。

  通过： 通过 ARP 防护的合法报文。

  丢弃： 被 APR 防护丢弃的非法 ARP 报文。

12.4 IP 源防护

IP 源防护功能是交换机根据四元绑定条目对接收的 IP 包进行过滤，只处理数据包相关字段与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

进入页面的方法：网络安全>>IP 源防护>>IP 源防护

图 12-18 IP 源防护

条目介绍：

- **IP 源防护配置**

选择： 勾选端口配置端口的 IP 源防护功能，可多选。

端口： 显示交换机的端口号。

防护类型： 选择端口的防护类型。

- 禁用：禁用端口的 IP 源防护功能。
- SIP+MAC：只处理源 IP 地址、源 MAC 地址和端口均符合四元绑定信息的数据包。

LAG： 显示端口当前所属的汇聚组。

12.5 DoS 防护

DoS（Denial of Service，拒绝服务）攻击是指攻击者利用网络协议实现的缺陷，耗尽被攻击对象的资源，使目标计算机或网络无法提供正常的服务或资源访问甚至崩溃。

DoS 攻击的具体的影响如下：

1) 耗尽服务器的资源，包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。使服务器疲于响应此类报文，导致网络瘫痪。

2) 由于交换机接收到此类报文需经过 CPU 处理，因此若请求报文数量过多，会导致交换机 CPU 利用率持续上升，无法正常工作。

本交换机通过解析 IP 数据包，分析数据包中的特定字段，并判断是否符合 DoS 攻击数据包的特征。对于非法的数据包，交换机将直接丢弃；而对于某些正常的数据包，由于流量过大可能导致受害主机瘫痪时，交换机可以对此类数据包进行限速。本交换机能够防护的 DoS 攻击种类如表 13-1 所示。

DoS攻击类型	**攻击特征**
Land Attack	向目标主机发送一个特别伪造的SYN包，其IP源地址和目的地址都被设置为目标主机的IP地址，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度上降低了系统性能。
Scan SYNFIN	TCP标志位SYN、FIN位被置1的数据包。由于SYN标志用来初始化连接的，FIN标志用来表示发端已完成发送任务请求关闭连接，所以SYN/FIN肯定是非法的数据包，本交换机能够识别此类攻击。
Xmascan	TCP序号置为0，FIN、URG、PSH位置为1的数据包。
NULL Scan	TCP序号置为0，所有控制位置为0的数据包。在正常的TCP连接以及数据传输过程中，不会出现所有控制位置0的情况，此类数据包为非法的数据包。
SYN sPort less 1024	TCP SYN标志位置1，源端口小于1024的数据包。
Blat Attack	数据包的L4源端口等于目的端口且URG置位。此攻击方式类似于Land Attack，被攻击主机因尝试和自己建立连接使系统性能下降。
Ping Flooding	利用Ping广播风暴，淹没整个目标系统，以至于该系统不能响应合法的通信。
SYN/SYN-ACK Flooding	每当我们进行一次标准的TCP连接，都会有一个三次握手的过程，而TCP-SYN Flood只进行前两个步骤，服务方在一定时间内等待请求方ASK消息。由于一台服务器可用的TCP连接是有限的，如果攻击方发送大量此类连接请求，则服务方TCP连接队列将会很快阻塞，系统资源和可用带宽急剧下降，无法提供正常的网络服务，从而造成拒绝服务。
winNuke Acctack	利用操作系统漏洞，向目标主机的TCP 139端口（NetBIOS）发送数据，可导致机器蓝屏。主要利用的是TCP包中的URG（Urgent Pointer，紧急指针），有漏洞的操作系统不能正确处理这一标志。

表 13-1 本交换机支持的 DoS 防护种类

在此页面中可以根据实际需要启用合适的 DoS 防护策略。

进入页面的方法：网络安全>>DoS 防护>>DoS 防护

图 12-19 DoS 防护

条目介绍：

- **全局配置**

  DoS 攻击防护： 选择是否启用交换机的 DoS 防护功能。

- **攻击防护列表**

  选择： 勾选启用相应 DoS 防护。

  防护类型： 显示防护类型。

说明：

还可以从以下三方面对 DoS 攻击进行防护，以进一步保证网络安全。

1) 检查并修补系统漏洞，及时安装系统补丁程序，对于重要信息要建立和完善备份机制。
2) 作为网络管理员，可检查系统的物理环境，禁止一些不必要的网络服务。
3) 利用硬件防火墙等网络安全设备提高网络的安全性。

12.6 Flood CPU 防护

TCP/UDP 泛洪的 CPU 防护功能用于避免交换机消耗大量的资源用于处理无意义的 IP 报文，同时可减少网络上因处理该类 IP 报文带来的大量 ARP 查询报文。

条目介绍：

- **防护目的端口号**

  起始目的端口号： 设置防护功能有效的起始目的端口号。

  结束目的端口号： 设置防护功能有效的结束目的端口号。

- **目的端口号列表：**

  选择： 勾选启用相应 DoS 防护。

  序号： 显示防护类型。

  起始目的端口号： 显示防护功能有效的起始目的端口号。

  结束目的端口号： 显示防护功能有效的结束目的端口号。

12.7 802.1X 认证

802.1X 协议是 IEEE802 LAN/WAN 委员会为了解决无线局域网网络安全问题提出的。后来该协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要用于解决以太网内认证和安全方面的问题，在局域网接入设备的端口这一级对所接入的设备进行认证和控制。

本交换机可以作为一个认证系统来对网络中的计算机进行认证。连接在端口上的用户设备如果能通过交换机认证，就可以访问局域网中的资源；如果不能通过交换机认证，则无法访问局域网中的资源。

- **802.1X 体系结构**

802.1X 的系统是采用典型的 Client/Server 体系结构，包括三个实体，如图 13-20 所示。

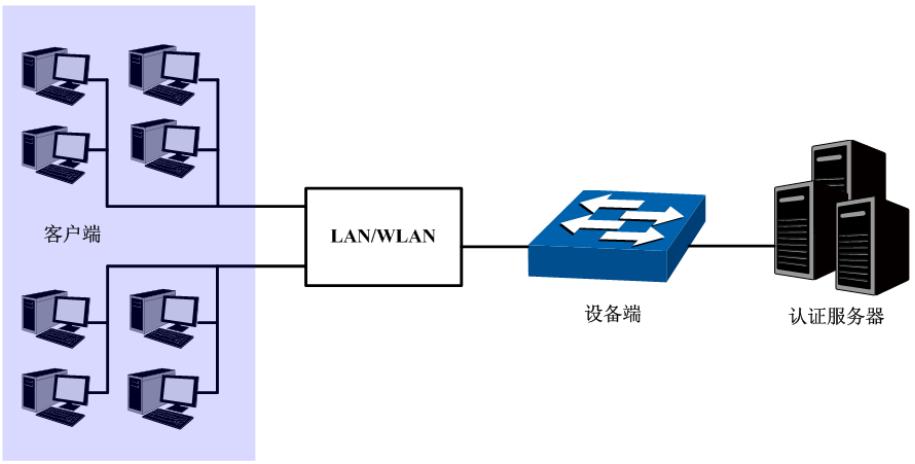


图 12-20 802.1X 认证的体系结构

1) 客户端：局域网中的一个实体，多为普通计算机，用户通过客户端软件发起 802.1X 认证，并由设备端对其进行认证。客户端软件必须为支持 802.1X 认证的用户终端设备。

2) 设备端：通常为支持 802.1X 协议的网络设备，如本交换机，为客户端提供接入局域网的物理/逻辑端口，并对客户端进行认证。

3) 认证服务器：为设备端提供认证服务的实体，例如可以使用 RADIUS 服务器来实现认证服务器的认证和授权功能。该服务器可以存储客户端的相关信息，并实现对客户端的认证和授权。为了保证认证系统的稳定，可以为网络设置一个备份认证服务器。当主认证服务器出现故障时，备份认证服务器可以接替认证服务器的工作，保证认证系统的稳定。

- **802.1X 认证工作机制**

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

1) 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

2) 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是设备端终结 EAP 协议报文，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证。

3) 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端根据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

- **802.1X 认证过程**

认证过程可以由客户端主动发起，也可以由设备端发起。一方面当设备端探测到有未经过认证的用户使用网络时，就会主动向客户端发送 EAP-Request/Identity 报文，发起认证；另一方面客户端可以通过客户端软件向设备端发送 EAPOL-Start 报文，发起认证。

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

1. EAP 中继方式

EAP 中继方式是 IEEE 802.1X 标准规定的，将 EAP（扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator。本交换机支持的 EAP 中继方式是 EAP-MD5，EAP-MD5 认证过程如图 13-21 所示。

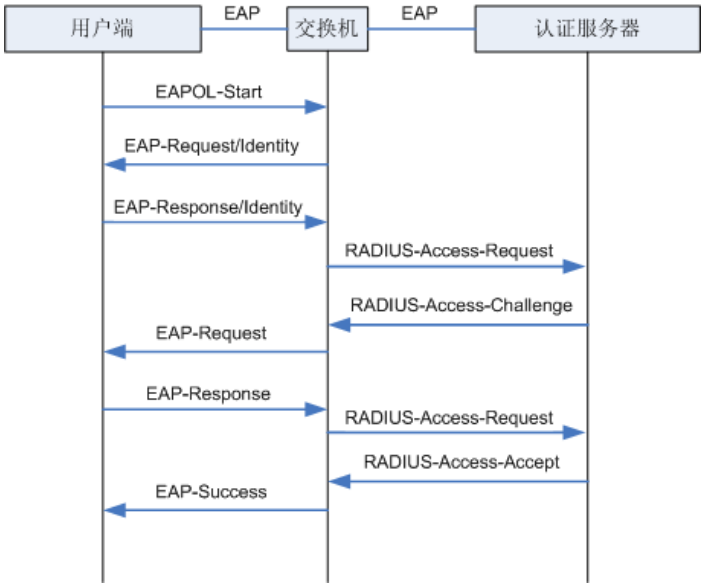


图 12-21 EAP-MD5 认证过程

1) 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。

2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。

3) 客户端程序响应设备端发出的请求， 将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。

4) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。

5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的，生成 EAP-Response/MD5 Challenge 报文），并通过设备端传给认证服务器。

6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。

7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线，设备端把端口状态从授权状态改变成未授权状态。

2. EAP 终结方式

EAP 终结方式将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费。设备端与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。本交换机支持的 EAP 终结方式是 PAP，PAP 认证过程如图 13-22 所示。

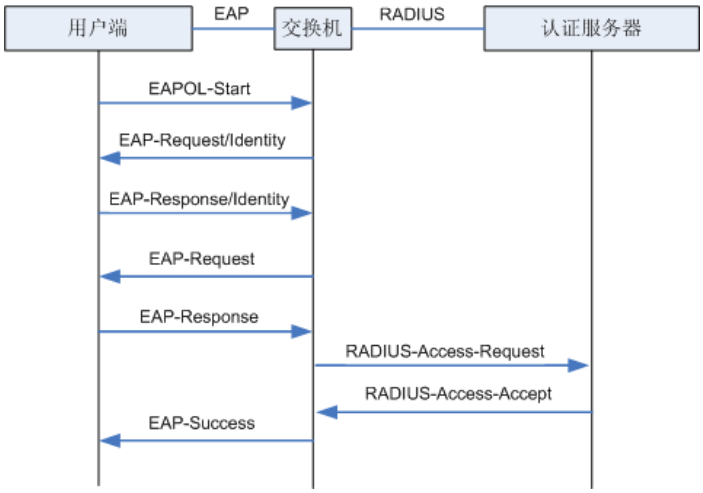


图 12-22 PAP 认证过程

在 PAP 模式中，交换机对用户口令信息进行加密，然后把用户名、随机加密字和客户端加密后的口令信息一起转发给认证服务器进行相关的认证处理；而在 EAP-MD5 模式中，随机加密字由认证服务器产生，交换机只负责把认证信息报文封装后转发。

- **802.1X 定时器**

802.1X 认证过程中会启动多个定时器以控制接入用户、设备以及 RADIUS 服务器之间进行合理、有序的交互。本交换机中的 802.1X 定时器主要有以下三种：

1) **客户端认证超时定时器**：当交换机向客户端发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到客户端的响应，交换机将重发该报文。

2) **认证服务器超时定时器**：当交换机向认证服务器发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到认证服务器的响应，交换机将重发认证请求报文。

3) **静默定时器**：对用户认证失败以后，交换机需要静默一段时间（该时间由静默定时器设置），在静默期间，交换机不再处理该用户的认证请求。

- **Guest VLAN**

Guest VLAN 功能用来允许未通过认证的用户访问某些特定资源。

用户认证端口在通过 802.1X 认证之前属于一个缺省 VLAN（即 Guest VLAN），用户访问该 VLAN 内的资源不需要认证，但此时不能够访问其它网络资源；认证成功后，端口离开 Guest VLAN，用户可以访问其它的网络资源。

用户可以在 Guest VLAN 中获取 802.1X 客户端软件、升级客户端或执行其它一些用户升级程序。如果因为没有专用的认证客户端或者客户端版本过低等原因，导致一定的时间内端口上无客户端认证成功，本交换机会把该端口加入到 Guest VLAN。

开启 802.1X 特性并正确配置 Guest VLAN 后，当交换机向客户端发送 EAP-Request/Identity 报文而没有收到客户端的回应时，该端口将按照各自的链路类型被加入到 Guest VLAN 内。此时如果 Guest VLAN

中有用户发起认证且认证失败，相应连接端口仍会留在 Guest VLAN 内；如果认证成功，端口离开 Guest VLAN，加入配置的 VLAN 中。用户下线后，端口将返回 Guest VLAN 中。

本交换机 802.1X 认证功能包括**全局配置**和**端口配置**两个配置页面。

12.7.1 全局配置

在全局配置功能页面，可以开启全局 802.1X 认证功能，选择本交换机提供的认证方法，并设置 Guest VLAN 以及各种定时器来协调整个系统的 802.1X 认证过程。

进入页面的方法：网络安全>>802.1X 认证>>全局配置

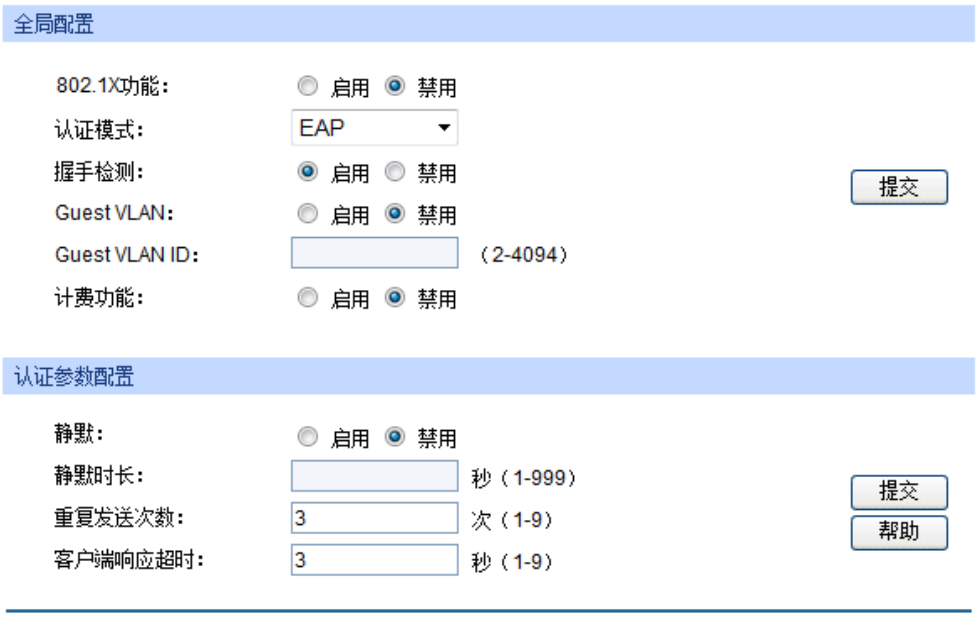


图 12-23 全局配置

条目介绍：

- **全局配置**

802.1X 功能： 选择是否启用 802.1X 认证功能。

认证模式： 选择 802.1X 认证方法。

- EAP：用户端与交换机之间运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其它高层次协议中(如 RADIUS)，以便穿越复杂的网络到达认证服务器。
- PAP：用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议(如 RADIUS)，传递用户认证信息给认证服务器系统。

握手检测： 选择是否启用握手检测功能。握手检测功能用于检测客户端与交换机的连接状态。如果使用其他客户端软件进行连接，请关闭握手检测功能。

Guest VLAN： 选择是否启用 Guest VLAN 功能。

Guest VLAN ID： 填写启用 Guest VLAN 的 VLAN ID。Guest VLAN 中的用户可以访问指定的网络资源。

计费功能： 选择是否启用计费功能。

- **认证参数配置**

静默： 选择是否启用静默计时器。

静默时长： 填写静默时长。用户认证失败后，在静默时间内不再处理同一用户的 802.1X 认证请求。

重复发送次数： 填写认证报文的最大重传次数。

客户端响应超时： 填写交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。

12.7.2 端口配置

在端口配置功能页面，可以根据实际的网络情况设置端口的 802.1X 功能特性。

进入页面的方法：网络安全>>802.1X 认证>>端口配置

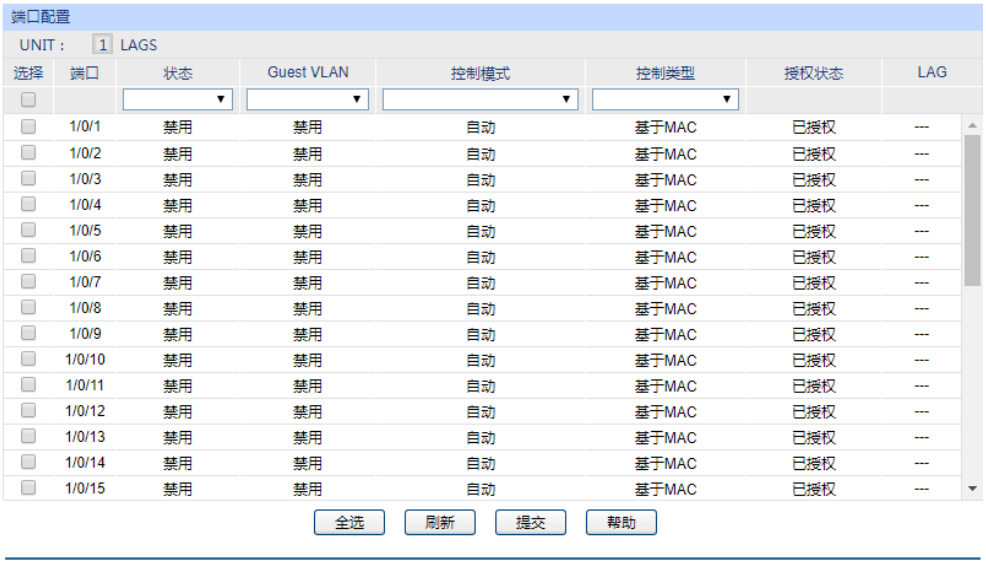


图 12-24 端口配置

条目介绍：

- **端口配置**

选择： 勾选端口，配置端口的 802.1X 认证状态，可多选。

端口： 显示交换机端口号。

状态： 选择该端口是否启用 802.1X 认证。

Guest VLAN： 选择该端口是否启用 Guest VLAN。

控制模式： 选择该端口的控制模式。

- 自动：端口需要进行认证。
- 强制已认证：端口不需要认证即可访问网络。
- 强制不认证：端口永远无法通过认证。

控制类型： 选择该端口的控制类型。

- 基于 MAC：该端口连接的所有计算机都需要认证。
- 基于 Port：该端口连接的某个用户通过认证后，其它用户均无须认证即可访问网络。

授权状态： 显示此端口的授权状态。

LAG： 显示端口当前所属的汇聚组。

12.8 AAA

AAA 是认证、授权和计费（Authentication、Authorization、Accounting）三个英文单词的简称。主要用于对试图访问交换机或者获得访问权限的用户进行认证，管理具有访问权的用户可以获得哪些服务，如何对正在使用网络资源的用户进行计费。具体功能表现为：

1. 认证(Authentication)：验证用户是否可以获得访问权限；
2. 授权(Authorization)：授权用户可以使用哪些服务；
3. 计费(Accounting)：记录用户使用网络资源的情况。

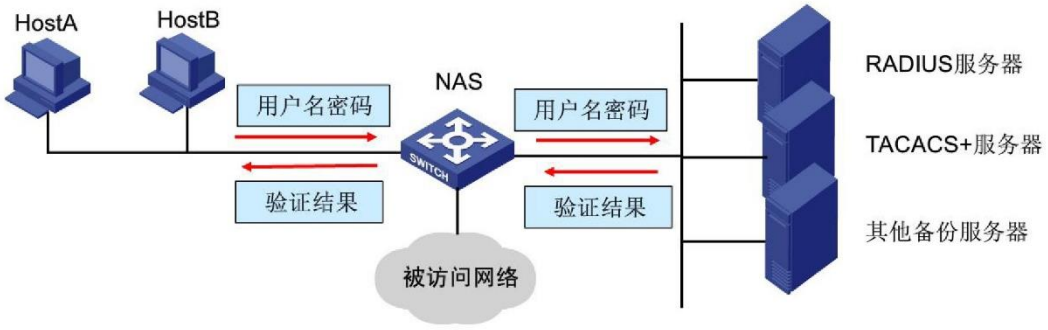


图 12-25 AAA 架构

12.8.1 全局配置

在此页面可对 AAA 功能进行全局配置。

进入页面的方法：网络安全>>AAA>>全局配置

图 12-26 全局配置

条目介绍：

- **全局配置**

  AAA： 选择开启或关闭 AAA 功能。

- **使能管理员权限**

  使能密码： 经过认证后使用户获得管理员权限。

- **AAA 配置列表**

  模块： 应用对应方法列表的终端名称。

  登录方法列表： 终端采用的登录方法列表。

  认证方法列表： 终端采用的认证方法列表。

12.8.2 方法列表

这里允许配置一个用户自定义的或者系统默认的方法列表，使用户经过认证后可以登录交换机或者提升为管理员权限。

进入页面的方法：网络安全>>AAA>>方法列表

图 12-27 认证列表

条目介绍：

- **添加方法列表**

方法列表名：	输入方法列表的名字。
列表类型：	选择一个方法列表类型。
方法一：	首选方法。None 表示不需要认证；local 表示使用本地认证；radius 表示使用所有配置好的 RADIUS 服务器进行验证；tacacs 表示使用所有配置好的 TACACS+服务器进行认证。
方法二/方法三/方法四：	备选方法。

- **登录方法列表**

这里可以配置一个方法列表对登录交换机的用户进行认证。如果认证通过，采用远程认证的用户将获得一个普通用户权限。可以在使能管理员权限中提升用户的权限为管理员权限。

- **认证方法列表**

配置一个方法列表使经过认证的用户可以获得管理员权限。

12.8.3 Dot1x 配置

本页面可以配置用于 802.1X 认证的默认方法列表。

进入页面的方法：网络安全>>AAA>>Dot1x 配置

图 12-28 认证列表

条目介绍：

- **Dot1x 认证方法列表**

  方法一　　首选方法，只支持 radius 服务器组。

- **Dot1x 计费方法列表**

  方法一　　首选方法，只支持 radius 服务器组。

12.8.4 服务器组

服务器组可以添加多个服务器 IP 作为一个认证集，交换机有两个默认的服务器组（radius 和 tacacs），它们不可被修改，所有配置的服务器 IP 都会自动加入到对应的默认组。

进入页面的方法：网络安全>>AAA>>服务器组

图 12-29 服务器组

条目介绍：

- **添加服务器组**

  服务器组：　　输入服务器组的名字。

  服务器组类型：　　选择服务器的类型。

- **服务器组列表**

查看和修改服务器组参数。

12.8.5 RADIUS 配置

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）认证服务器为交换机提供认证服务，其存储有关用户的信息，包括用户名、密码以及其它参数，用于实现对用户进行认证、授权和计费。RADIUS 配置功能页面用来设置网络中认证服务器的参数，保证认证过程通畅有序的进行。

进入页面的方法：网络安全>>AAA>>RADIUS 配置

图 12-30 RADIUS 配置

条目介绍：

- **服务器配置**

服务器 IP：	输入服务器的 IP 地址。
共享密钥：	输入交换机和服务器共享的加密密钥。
认证端口：	服务器采用的认证端口号。
计费端口：	服务器采用的计费端口号。
重传次数：	超时后的最大重传次数。
超时时长：	最大等待时间。

- **服务器列表**

查看和修改服务器参数。

12.8.6 TACACS+配置

本页面可以配置 TACACS+（增强的终端接入控制系统）。

进入页面的方法：网络安全>>AAA>>TACACS+配置

图 12-31 TACACS+配置

条目介绍：

- **服务器配置**

  服务器 IP： 输入服务器的 IP 地址。

  超时时长： 允许的最大超时时间。

  加密密钥： 输入交换机和服务器共享的加密密钥。

  端口： TACACS+服务器采用的 TCP 端口号。

- **服务器列表**

查看和修改服务器参数。

注意：

- 只有同时开启全局和端口的 802.1X 特性后，才能使 802.1X 认证功能生效。
- LAG 端口不能启用 802.1X 功能。如果端口启动了 802.1X，则不能配置该端口加入聚合组。
- 认证服务器连接的端口请勿开启 802.1X 特性，且服务器配置参数必须与认证服务器软件的参数一致。

配置步骤：

步骤	操作	说明
1	搭建认证服务器	必选操作。搭建完成后，请在服务器中记录局域网接入用户的信息并设置相应的用户名和密码以备认证。
2	安装客户端软件	必选操作。请在接入计算机中安装光盘中的 802.1X 客户端软件，更多信息请参阅与软件在同一目录中的软件指南。
3	设置 802.1X 全局参数	必选操作。默认情况下，交换机 802.1X 全局功能未开启，请在**网络安全>>802.1X 认证>>全局配置**页面中设置全局参数。

4	设置认证服务器参数	必选操作。请自行搭建认证服务器，并在**网络安全>>AAA>>RADIUS 配置**页面中设置服务器参数。
5	设置各端口 802.1X 功能参数	必选操作。请在**网络安全>>802.1X 认证>>端口配置**页面中根据实际网络情况设置交换机各端口的 802.1X 功能参数。

回目录

第13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 14-1 所示。

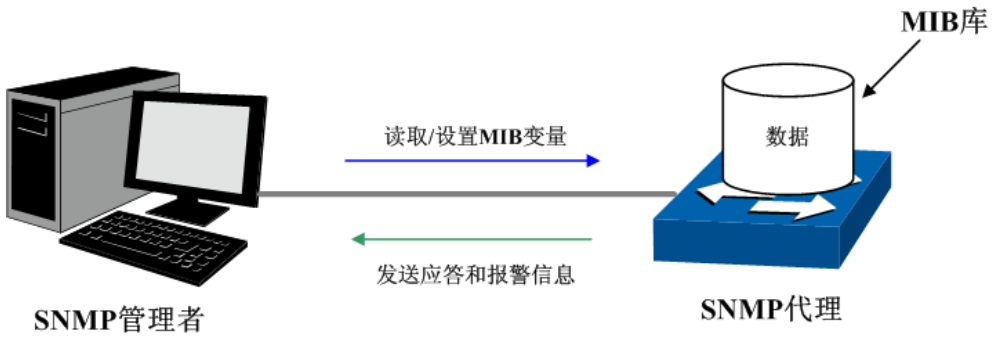


图 13-1 SNMP 网元关系图

➢ 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 14-2 所示。图中，B 的 OID 为{1.2.1.1}，A 的 OID 为{1.2.1.1.5}。

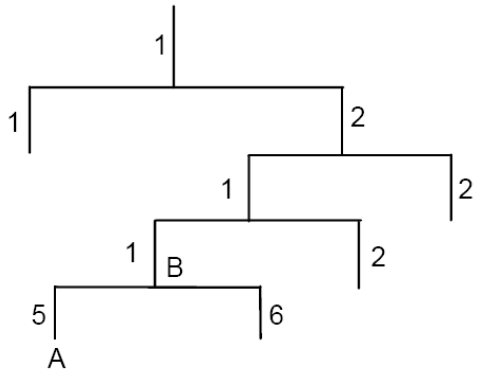


图 13-2 MIB 树结构

- **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。

13.1 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。

13.1.1 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

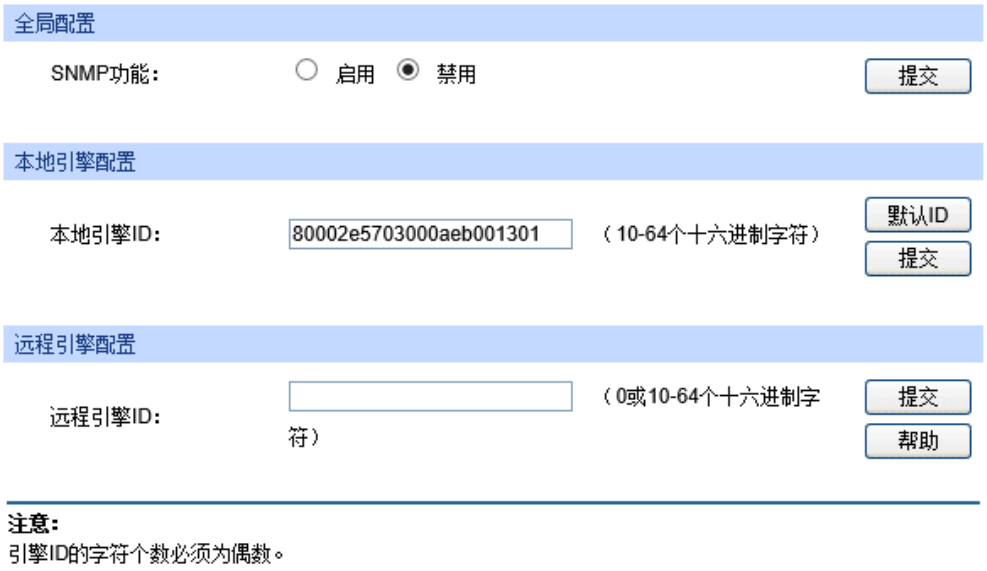


图 13-3 全局配置

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。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。

13.1.2 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

图 13-4 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）。

13.1.3 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

图 13-5 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。

13.1.4 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

图 13-6 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。

13.1.5 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

图 13-7 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：

- 若使用 SNMPv3 版本

步骤	操作	说明
1	启用 SNMP 全局功能	必选操作。在 **SNMP>>SNMP 配置>>全局配置**页面，启用交换机的 SNMP 功能。

步骤	操作	说明
2	创建视图	可选操作。在 **SNMP>>SNMP 配置>>视图管理**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 **SNMP>>SNMP 配置>>组管理**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 **SNMP>>SNMP 配置>>用户管理**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。

- 若使用 SNMPv1 版本或 SNMPv2c 版本

<table>
<tr><th>步骤</th><th colspan="3">操作</th><th>说明</th></tr>
<tr><td>1</td><td colspan="3">启用 SNMP 全局功能。</td><td>必选操作。在 SNMP>>SNMP 配置>>全局配置页面，启用交换机的 SNMP 功能。</td></tr>
<tr><td>2</td><td colspan="3">创建视图</td><td>可选操作。在 SNMP>>SNMP 配置>>视图管理页面，创建管理对象的视图。默认视图名为 viewDefault，OID 为 1。</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">配置访问权限</td><td>直接设置</td><td>创建团体</td><td rowspan="3">二者必选其一。
• 直接设置是在 SNMP>>SNMP 配置>>团体管理页面，以 SNMPv1 和 v2c 版本的团体名进行设置。
• 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。</td></tr>
<tr><td rowspan="2">间接设置</td><td>创建 SNMP 组</td></tr>
<tr><td>创建 SNMP 组内的用户</td></tr>
</table>

13.2 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

图 13-8 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。

IP 地址类型： 选择 IP 地址类型。

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。

IP 地址类型： 显示 IP 地址类型。

UDP 端口： 显示管理主机上启用供通知过程使用的 UDP 端口。

团体名/用户名： 显示管理软件的团体名/用户名。

安全模型： 显示用户的安全模式。

安全级别： 显示 SNMP v3 的用户的安全级别。

通知类型： 显示使用的通知报文的类型。

重传： 显示收到 Inform 报文回应报文的超时时间。

超时： 显示 Inform 报文的重传次数。

操作： 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。

13.3 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，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、冲突帧以及以下长度的数据包：64、65~127、128~255、256~511、512~1023 和 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**统计组**、**历史组**、**事件组**和**警报组**四个配置页面。

13.3.1 统计组

本页用来配置 RMON 的统计组。

进入页面的方法：SNMP>>RMON>>统计组

图 13-9 统计组

条目介绍：

- **统计组配置**

  ID 号： 填写统计条目的 ID 号，大小范围为 1-65535。

  端口： 填写或者选择被统计的以太网端口。

  创建者： 填写创建这一条目的用户名。

  状态： 选择是否启用所选采样条目。

- **统计条目列表**

可以在这里查看已存在的统计组条目的配置信息。

13.3.2 历史组

本页用来配置 RMON 的历史组。

进入页面的方法：SNMP>>RMON>>历史组

图 13-10 历史组

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。
最大采样数目：	显示当前历史控制表项所能够保存的采样数据条目的最大数目。范围为 1-130，默认值为 10。
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。

13.3.3 事件组

本页用来配置 RMON 的事件组。

进入页面的方法：SNMP>>RMON>>事件组

事件配置

选择	序号	用户名	描述	类型	创建者	状态
☐				无		禁用
☐	1	public		无	monitor	禁用
☐	2	public		无	monitor	禁用
☐	3	public		无	monitor	禁用
☐	4	public		无	monitor	禁用
☐	5	public		无	monitor	禁用
☐	6	public		无	monitor	禁用
☐	7	public		无	monitor	禁用
☐	8	public		无	monitor	禁用
☐	9	public		无	monitor	禁用
☐	10	public		无	monitor	禁用
☐	11	public		无	monitor	禁用
☐	12	public		无	monitor	禁用

提交 帮助

图 13-11 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。

13.3.4 警报组

本页用来配置 RMON 的警报组。

进入页面的方法：SNMP>>RMON>>警报组

图 13-12 警报配置

条目介绍：

- **警报配置**

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。

统计条目： 选择对警报变量进行采样的统计条目。

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直接与阈值进行比较。
- 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14章 LLDP

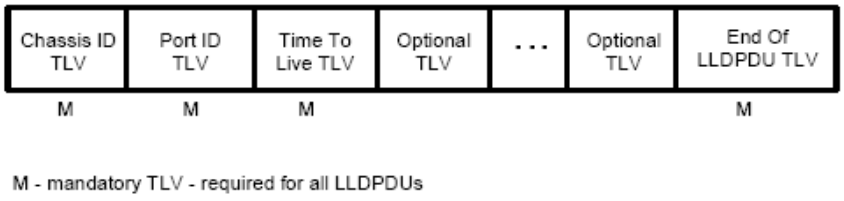
链路层发现协议 LLDP（Link Layer Discovery Protocol）是一个二层协议，在符合 IEEE802 标准的局域网络中，允许网络设备周期性地向邻居设备通告自己的设备信息。LLDP 根据 IEEE802.1AB 标准把设备的标识、性能和配置等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给邻居设备，邻居设备收到这些信息后将其以标准的 MIB（Management Information Base，管理信息库）形式保存起来。网络管理系统可以通过管理协议 SNMP（Simple Network Management Protocol，简单网络管理协议）获取到这些信息，以查询及判断链路的通信状况。

为了描述网络的物理拓扑和拓扑中的相关系统，IETF（Internet Engineering Task Force, 互联网工程任务组）组织提出了标准 MIB，一些公司也提出了私有 MIB。但是，IEEE 802 局域网站点并没有统一的标准来传输 MIB 信息。LLDP 解决了这一问题。LLDP 协议允许不同厂商的网络设备协同工作，运行 LLDP 协议的设备能够自动检测并学习邻居设备的信息。LLDP 还可以使运行不同网络层协议的系统互相学习对方的设备信息。

SNMP 应用可以利用 LLDP 获取的信息，进行网络故障排除，从而提高网络的稳定性，维持正确的网络拓扑。

➢ LLDPDU

每一个 LLDPDU 携带四个必须的 TLV 以及一个或者多个可选的 TLV。如下图所示，Chassis ID TLV, Port ID TLV, TTL TLV 和 End TLV 是每个 LLDPDU 所必须携带的四个 TLV。可选的 TLV 是由网络管理系统决定的，它们提供了关于本地 LLDP 设备的详细信息。



LLDPDU 的最大长度由特定的传输速率和协议所允许的最大报文长度决定。就 IEEE 802.3 MAC 协议来说，LLDPDU 的最大长度是不带 TAG 的基本 MAC 帧的最大长度，即 1500 字节。

➢ LLDP 工作机制

1) LLDP 的工作模式

每个端口都可以分别配置 LLDPDU 的接收和发送功能，这样端口可以配置四种工作模式：

- 发送接收：既发送也接收 LLDPDU。
- 只接收：只对接收到的 LLDPDU 进行处理，而不向外发送 LLDPDU。
- 只发送：只向外发送 LLDPDU，而不对接收到的 LLDPDU 进行处理。
- 禁用：既不向外发送 LLDPDU，也不对接收到的 LLDPDU 进行处理。

2) LLDPDU 的传输机制

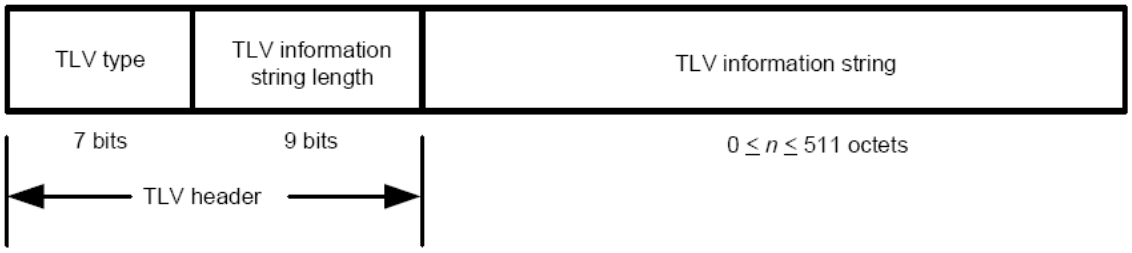
- 当端口工作在发送接收模式或者只发送模式时，设备会周期性地向邻居设备发送 LLDPDU 以通告自己的信息。
- 当本地设备发生变化时，设备会发送变化通告。当本地设备在短时间内频繁变化时，为避免设备连续地发送 LLDPDU 而导致网络阻塞，NMS（Network Management System，网络管理系统）将会设定一个报文发送时延，以确保 LLDPDU 的发送有一个固定的最小时间差。
- 当端口的工作模式由禁用或者只接收模式切换为发送接收模式或者只发送模式时，该设备的快速启动机制将被激活，报文的发送间隔变为 1s，快速发出一些 LLDPDU 之后，设备恢复正常的发送周期。

3) LLDPDU 的接收机制

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

➢ TLV

TLV 是 LLDPDU 的基本组成单位，是 Type/Length/Value 的简称，即类型/长度/值。基本 TLV 的格式如下图所示：



每个 TLV 的类型都是不一样的，根据 TLV 的类型可以判断 TLV 中的信息类型。

下表是目前定义的各种 TLV 的详细信息。

TLV 类型	TLV 名称	说明	是否必须携带
0	End of LLDPDU	标识 LLDPDU 结束。任何在 End Of LLDPDU TLV 之后的信息将被丢弃。	是
1	Chassis ID	标识连接设备的 Chassis ID	是
2	端口 ID	标识发送端口的 ID 信息	是
3	Time To Live	本地设备信息在邻居设备上的老化时间	是
4	端口描述	用以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述	否
5	系统名称	用以向邻居发布本地设备的系统名称	否

TLV 类型	TLV 名称	说明	是否必须携带
6	系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述	否
7	系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息	否
8	管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理	否
127	组织定义	允许不同的组织、软件和设备生产商定义向邻居设备发送信息的 TLV	否

TLV 一般分为两类，基本 TLV 和组织定义的 TLV。

1) 基本 TLV

基本 TLV 是实现 LLDP 协议必不可少的，它们包含网络管理的基本信息。

2) 组织定义的 TLV

不同的组织定义了许多不同的 TLV。端口 VLAN ID、协议 VLAN ID、VLAN 名称以及协议标识 TLV 都是 IEEE 802.1 定义的，MAC/PHY 配置/状态、供电能力、链路聚合以及最大帧长度 TLV 则是由 IEEE 802.3 定义的。

注意:

要获取更多关于 TLV 的详细信息，请参考 IEEE 802.1AB 标准。

TP-LINK 交换机中所支持的可携带 TLV 如下表所示：

端口描述	用以向邻居发布本端口的 IEEE 802 局域网工作站规定的端口描述。
系统能力	用以向邻居发布本地设备支持的功能和这些功能是否允许的信息。
系统描述	用以向邻居发布本地设备包含系统硬件、软件版本等系统信息的描述。
系统名称	用以向邻居发布本地设备的系统名称。
管理地址	用以向邻居发布本地设备的管理地址，网络管理协议可以通过该地址对本地设备进行管理。
端口 VLAN ID	用以向邻居发布本端口所处 802.1Q VLAN 的 ID。
协议 VLAN ID	用以向邻居发布本端口所处协议 VLAN 的 ID。
VLAN 名称	用以向邻居发布本端口所处 VLAN 被指派的名称。
链路聚合	用以向邻居发布本端口当前的链路聚合信息，包括本端口是否具有链路聚合能力、是否处于聚合状态以及处于链路聚合状态时的端口 ID。

MAC/PHY 配置/状态	用以向邻居发布本端口的端口属性，包括端口支持的速率双工、当前工作的速率双工以及是手工设置还是自动协商而得到的速率双工。
最大帧长度	用以向邻居发布本端口的 MAC 和 PHY 支持的最大帧长度。
供电能力	用以向邻居发布本端口的基本供电信息。

表 15-1 TP-LINK 交换机中所支持的可携带 TLV

LLDP 模块主要用来配置交换机的 LLDP 功能，包括**基本配置**、**设备信息**、**设备统计**和 **LLDP-MED** 四个部分。

14.1 基本配置

本功能包括**全局配置**和**端口配置**两个功能配置页面。

14.1.1 全局配置

配置交换机的 LLDP 功能，首先需要在本页配置交换机 LLDP 的全局功能和相关参数。

进入页面的方法：LLDP>>基本配置>>全局配置

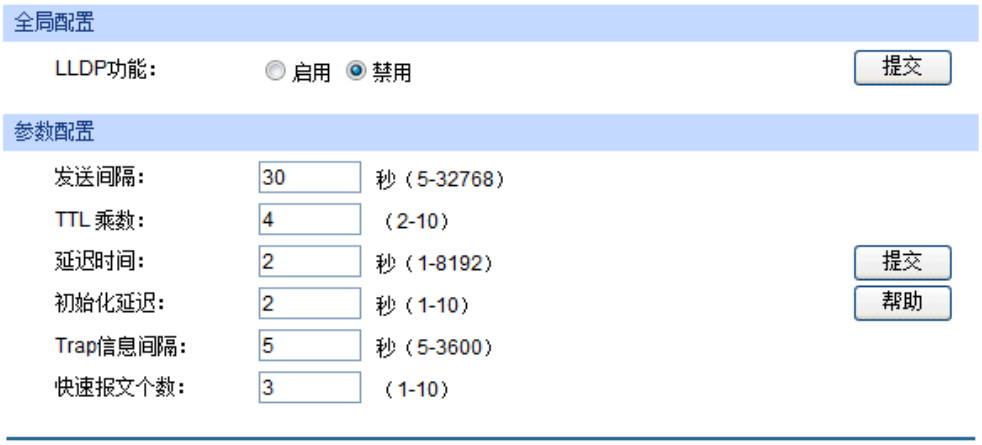


图 15-1 全局配置

条目介绍：

- **全局配置**

  LLDP 功能: 选择是否启用 LLDP。

- **参数配置**

  发送间隔: 配置本地设备向邻居设备发送 LLDPDU 的时间间隔。

  TTL 乘数: TTL 乘数用以控制本地设备发送的 LLDPDU 中 TTL 字段的值，TTL 即为本地信息在邻居设备上的存活时间。TTL=TTL 乘数*发送间隔。

延迟时间: 配置本地设备向邻居设备发送 LLDPDU 的延迟时间。当本地配置发生变化时，将延迟指定时间再发送 LLDPDU 通知邻居设备，从而可以避免由于本地配置频繁变化而导致 LLDPDU 的频繁发送。

初始化延迟: 当端口 LLDP 工作模式改变时，将延迟一段时间再进行初始化，以避免端口 LLDP 工作模式频繁改变导致端口不断执行初始化。

Trap 信息间隔: 配置本地设备向网管系统发送 Trap 信息的发送时间间隔。通过调整该时间间隔，可以避免由于邻居信息频繁变化而导致 Trap 信息的频繁发送。

快速报文个数: 当端口 LLDP 工作模式从禁用（或只接收）切换为发送接收（或只发送）时，为了让其它设备尽快发现本设备，将启用快速发送机制，即将 LLDP 报文的发送周期缩短为 1 秒，并连续发送指定数量的 LLDPDU 后再恢复为正常的发送周期。

14.1.2 端口配置

在本页可以配置所有端口的 LLDP 参数。

进入页面的方法：LLDP>>基本配置>>端口配置

图 15-2 端口配置

条目介绍：

- **端口配置**

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。
端口状态:	选择端口的 LLDP 工作状态： ● 发送接收：既发送也接收 LLDPDU。 ● 只接收：只对接收到的 LLDPDU 进行处理，而不向外发送 LLDPDU。 ● 只发送：只向外发送 LLDPDU，而不对接收到的 LLDPDU 进行处理。 ● 禁用：既不向外发送 LLDPDU，也不对接收到的 LLDPDU 进行处理。
SNMP 通知:	配置本端口是否启用 SNMP 通知。启用此功能时，如果发生 trap 事件，本地设备将会通知 SNMP 服务器。
TLV 字段:	配置发送的 LLDPDU 中包含的 TLV 类型。

14.2 设备信息

本功能包括**本地信息**和**邻居信息**两个配置页面。

14.2.1 本地信息

在本页可以查看各端口的配置参数及系统参数。

进入页面的方法：LLDP>>设备信息>>本地信息

图 15-3 本地信息

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。

- **本地信息**

点击端口可以查看端口的 LLDP 信息。

14.2.2 邻居信息

在本页可查看邻居设备的信息。

进入页面的方法：LLDP>>设备信息>>邻居信息

图 15-4 邻居信息

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。

- **邻居信息**

点击端口可以查看端口邻居的 LLDP 信息。

14.3 设备统计

在本页可以查看本地设备 LLDP 相关统计信息。

进入页面的方法：LLDP>>设备统计>>统计信息

图 15-5 统计信息

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。

- **全局统计**

  更新时间： 显示此统计数据的更新时间。

  邻居总数： 显示最新更新时本地设备的邻居数目。

  删除总数： 显示本地设备上删除的邻居数目。

  丢弃总数： 显示本地设备上丢弃的邻居数目。

  超时总数： 显示本地设备上超时的邻居数目。

- **详细统计**

  端口： 显示本地端口号。

  发送报文： 显示本端口已经发送的 LLDPDU 数量。

接收报文：	显示本端口已经接收到的 LLDPDU 数量。
丢弃报文：	显示本端口丢弃的 LLDPDU 数量。
错误报文：	显示本端口接收的错误 LLDPDU 数量。
超时邻居：	显示此端口连接的邻居设备中超时邻居的数目。
丢弃 TLV：	显示本端口接收 LLDPDU 时，丢弃的 TLV 数量。
未知 TLV：	显示本端口接收的 LLDPDU 中包含的未知 TLV 的数量。

14.4 LLDP-MED

LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery，用于媒体终端发现的链路层发现协议）是 LLDP 协议的一个扩展，它仅适用于 LLDP-MED 规定的网络连接设备和终端设备之间的交互。

LLDP-MED 包括**基本配置**、**端口配置**、**本地信息**和**邻居信息**四个页面。

14.4.1 全局配置

在本页可以配置本地设备的 LLDP-MED 参数。

进入页面的方法：LLDP>> LLDP-MED >>全局配置

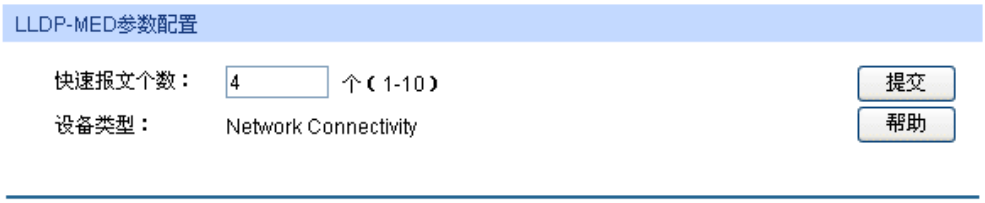


图 15-6 全局配置

条目介绍：

- **LLDP-MED 参数配置**

快速报文个数：	当 LLDP-MED 的快速发送机制启动时，会连续发送指定个数的包含 LLDP-MED 信息的 LLDPDU。
设备类型：	LLDP-MED 规定了两种设备类型，分别是网络连接设备（Network Connectivity Device）和终端设备（Endpoint Device），其中终端设备又可以分为 I、II 和 III 型共三种。交换机是一种网络连接设备。

14.4.2 端口配置

在本页可以配置所有端口的 LLDP-MED 状态和 TLV。

进入页面的方法：LLDP >> LLDP-MED >> 端口配置

图 15-7 端口配置

条目介绍：

- **LLDP-MED 端口配置**

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。

LLDP-MED 状态： 启用/禁用端口的 LLDP-MED 功能。

- 启用：启用端口的 LLDP-MED 功能，同时端口的 LLDP 状态会被设置为发送接收。
- 禁用：禁用端口的 LLDP-MED 功能。

TLV 字段： 选择发送的 LLDPDU 中包含的 LLDP-MED 的 TLV 信息。

点击<详细>按键即可进入如下页面，在本页可以配置端口发送的 LLDPDU 中包含的可选 LLDP-MED 的 TLV。

图 15-8 TLV 字段

条目介绍：

- **TLV 字段**

网络策略： 网络策略 TLV 允许网络连接设备和终端设备发布本端口的 VLAN 配置与二层和三层属性。

设备地址： 设备地址 TLV 提供了向相邻设备发布本地设备物理地址信息的能力。可以在**设备地址参数**中配置设备端口的详细地址。如果没有配置**设备地址参数**而又包含了设备地址 TLV，那么将会使用一个默认的地址信息。

扩展供电能力： 扩展供电能力 TLV 允许 LLDP-MED 连接设备和终端设备之间交互详细的供电信息，例如供电优先级、供电状态等

资产信息： 资产信息中包含七种基本的资产信息 TLV，分别为硬件版本 TLV、固件版本 TLV、软件版本 TLV、序列号 TLV、制造厂商名称 TLV、模块名称 TLV 和资产跟踪 ID TLV。

- **设备地址参数**

紧急号码： 紧急号码是紧急呼叫服务使用的号码，用以呼叫 CAMA 或者 PSAP，字符长度介于 10 到 25 之间。

设备地址： 普通地址使用 IETF 规定的地址信息格式。

- 类型：描述本地设备充当的设备角色，当前有三种选择：DHCP 服务器，switch 和 LLDP-MED 终端。
- 国家代码：ISO 3166 规定的代表国家的两个字符的代码，例如 CN、US 等。
- 语言、省/州等：普通地址的详细信息。

14.4.3 本地信息

在本页可以查看所有端口的 LLDP-MED 配置信息。

进入页面的方法：LLDP>> LLDP-MED >>本地信息

图 15-9 本地信息

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。

- **本地信息**

点击端口可以查看端口的 LLDP-MED 信息。

14.4.4 邻居信息

在本页可以查看所有端口邻居的 LLDP-MED 信息。

进入页面的方法：LLDP>> LLDP-MED >>邻居信息

图 15-10 邻居信息

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。

- **LLDP-MED 邻居信息**

点击端口可以查看端口邻居的 LLDP-MED 信息。

回目录

第15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。

15.1　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。

15.1.1 CPU 监控

进入页面的方法：系统维护>>运行状态>>CPU 监控

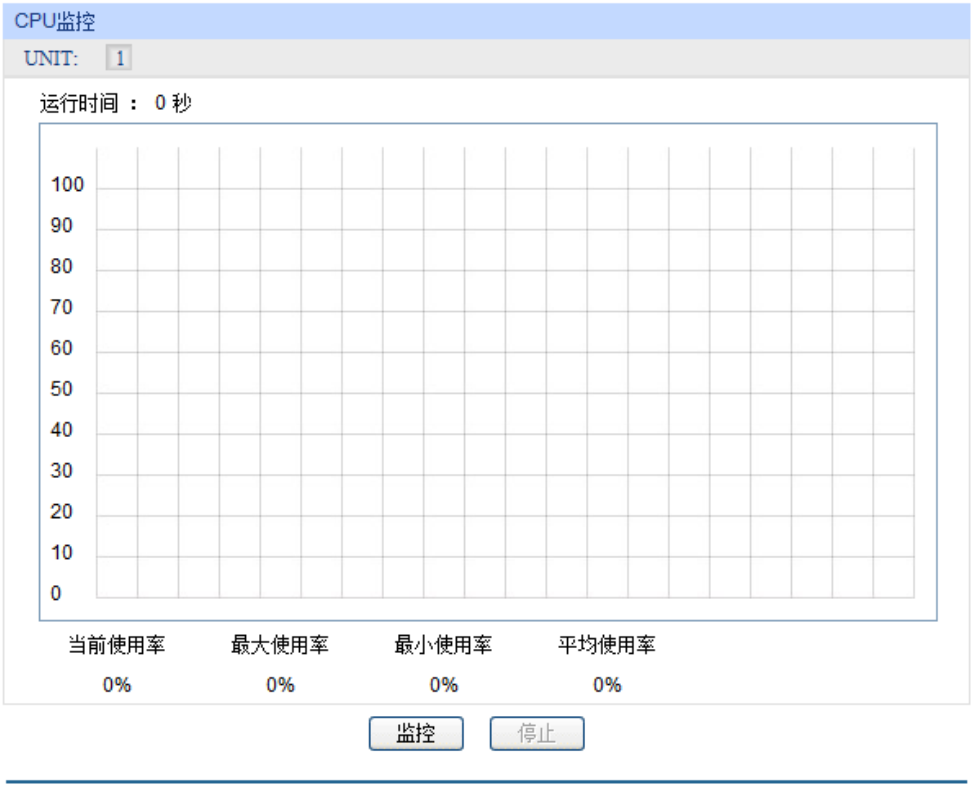


图 15-1 CPU 监控

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。

15.1.2 内存监控

进入页面的方法：系统维护>>运行状态>>内存监控

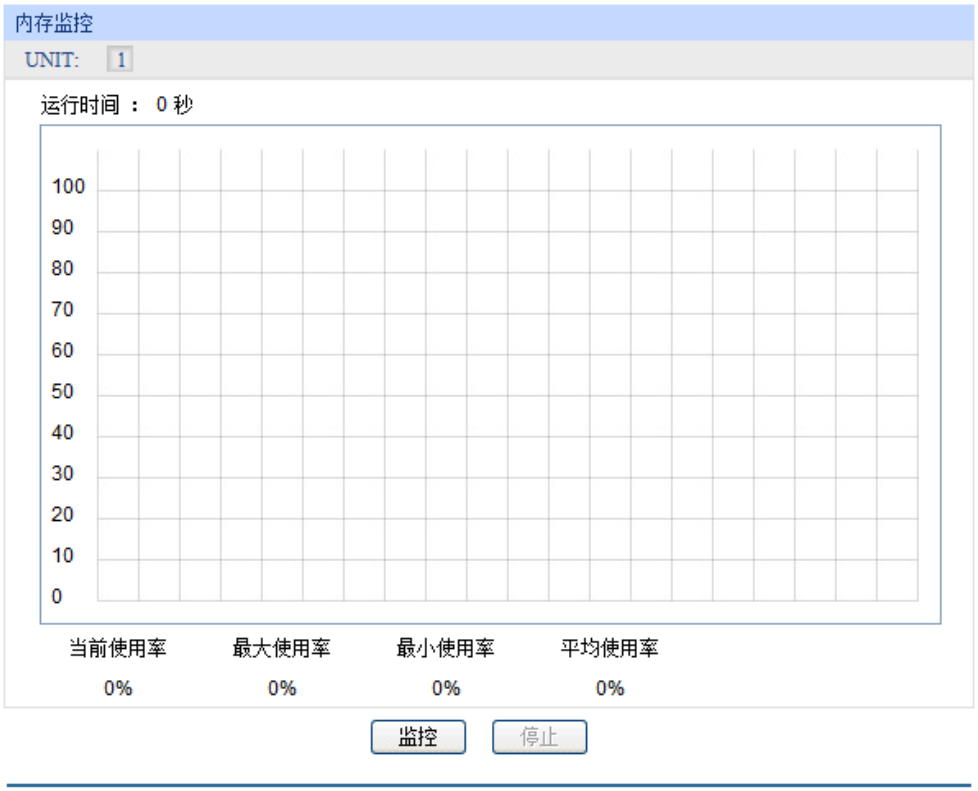


图 15-2 内存监控

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。

15.2 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 16-1 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
debugging	7	调试过程产生的信息

表 16-1 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。

15.2.1 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

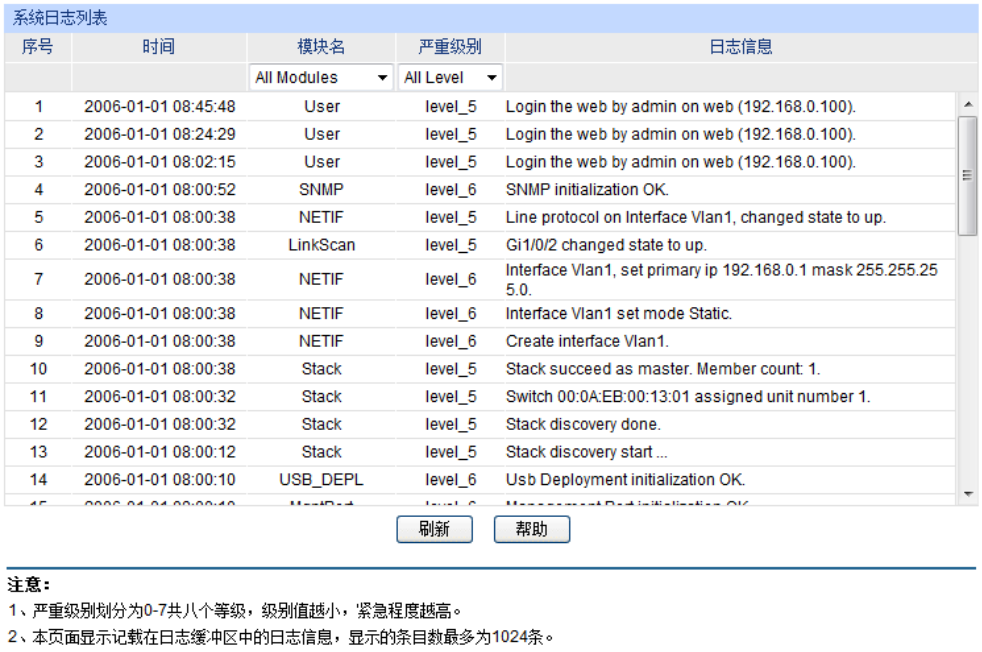


图 15-3 日志列表

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。

15.2.2 本地日志

本地日志是指保存在本设备上的系统日志信息。本地日志有两个输出方向，即可以保存到两个不同地方：日志缓冲区和日志文件。

进入页面的方法：系统维护>>系统日志>>本地日志

图 15-4 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。

输出方向： 显示日志输出方向。

- 日志缓冲区：日志缓冲区是用于保存系统日志的一块内存区域。缓冲区中的信息在“日志列表”页面上进行显示，在断电重启后这些信息将会丢失。
- 日志文件：日志文件是 Flash 里的一块存储区域。日志文件的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： 选择启用或禁用该输出方向。

同步频率： 日志信息写入日志文件的时间间隔。

15.2.3 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

图 15-5 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。

15.2.4 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，以获取跟错误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

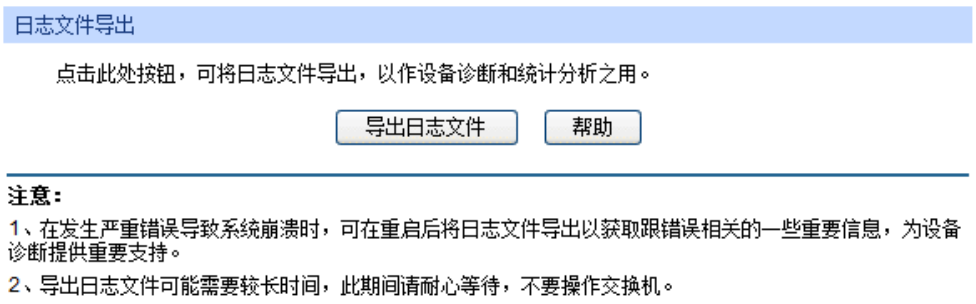


图 15-6 日志导出

条目介绍：

- **日志文件导出**

  导出日志文件： 点击此按键导出日志文件中的日志信息。

15.3 系统诊断

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

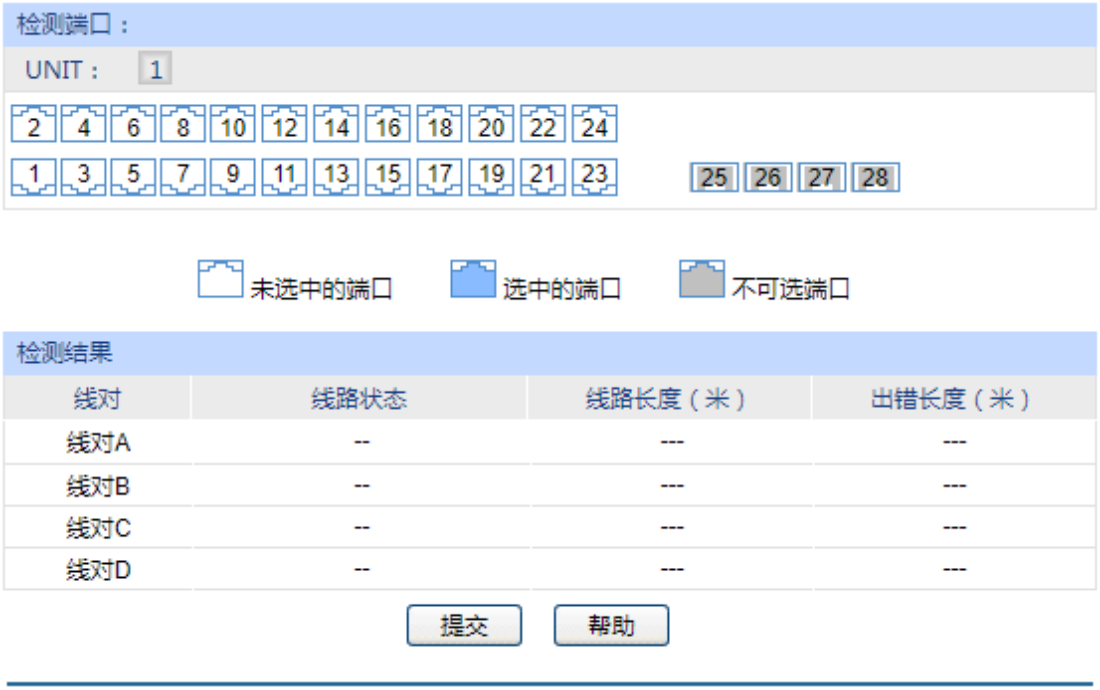


图 15-7 线缆检测

条目介绍：

- **检测端口**

  选择要进行线缆检测的端口。

- **检测结果**

  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：

- 对同一个端口前后两次诊断，请间隔 3 秒以上。
- 当电缆对端未连接时，诊断结果会较为准确。
- 这里的长度是指线缆绕对的长度，不是线缆表皮的长度，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。

15.4 网络诊断

本交换机提供了 Ping 检测和 Tracert 检测功能。

15.4.1 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

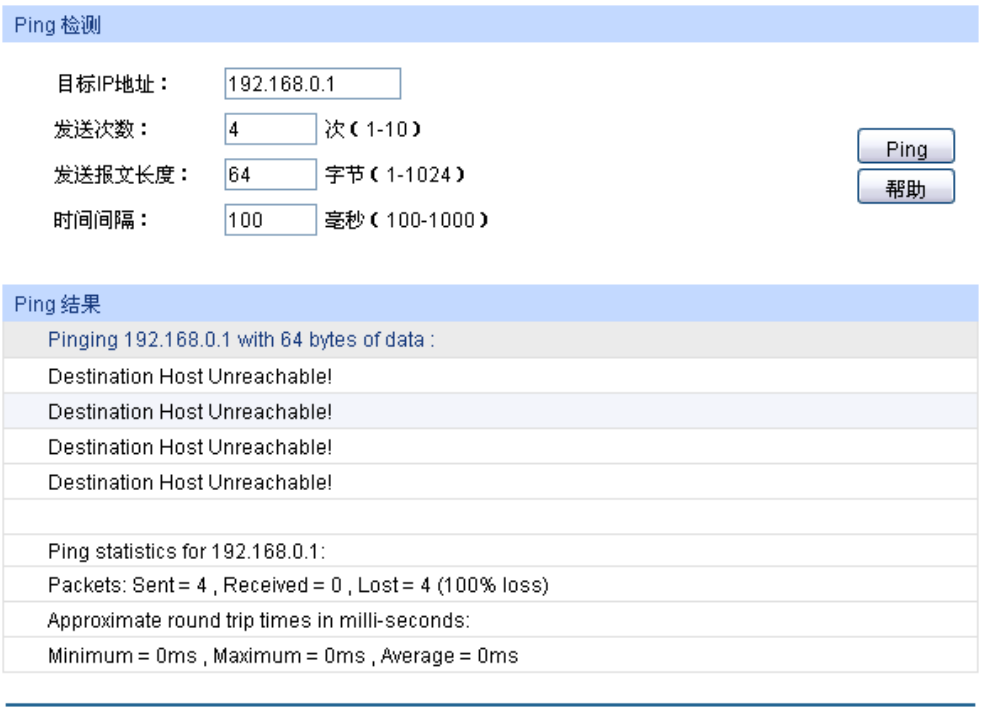


图 15-8 Ping 检测

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。支持 IPv4 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：	交换机发送检测包后，在此时间间隔内如果没有收到回复，则重新发送检测包，直到所发送的检测包达到所设置的发送次数。建议使用缺省值。

15.4.2 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

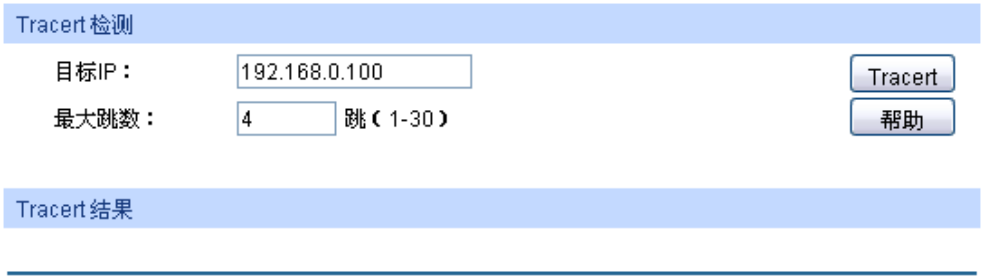


图 15-9 Tracert 检测

条目介绍：

- **Tracert 检测**

目标 IP： 填写目的设备的 IP 地址。支持 IPv4 地址。

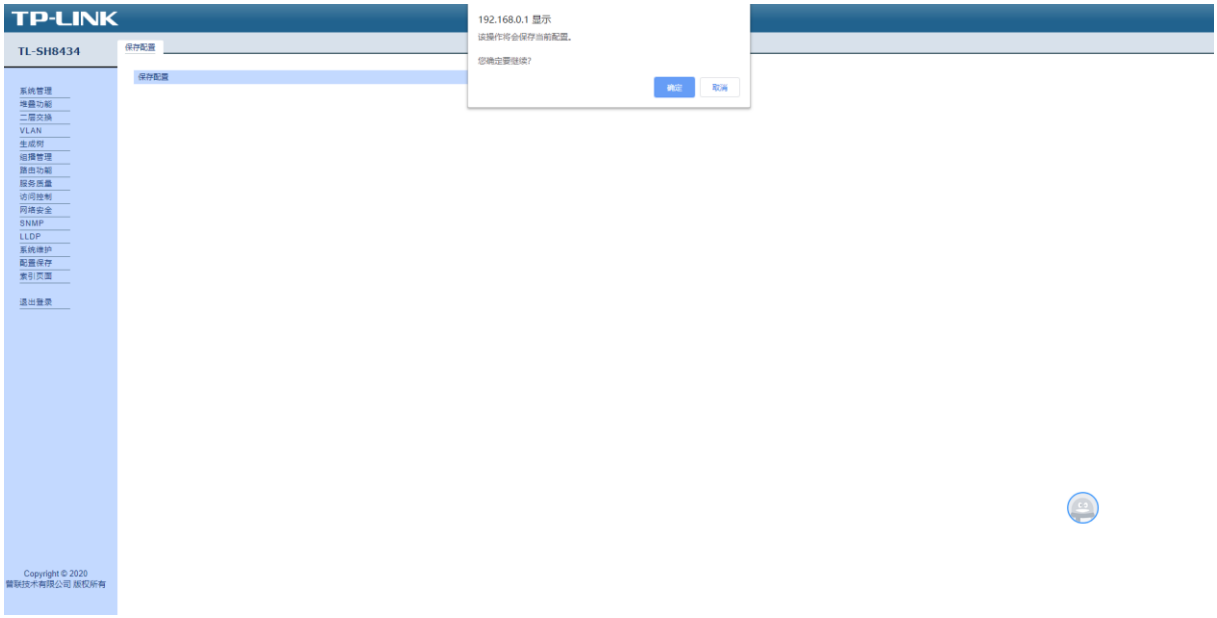
最大跳数： 填写测试报文发送的最大跳数。

第16章　配置保存

当交换机配置完成后，请注意保存当前配置，避免当出现断电等突发情况时，配置数据丢失。

进入页面的方法：配置保存

点击确定，保存当前配置。



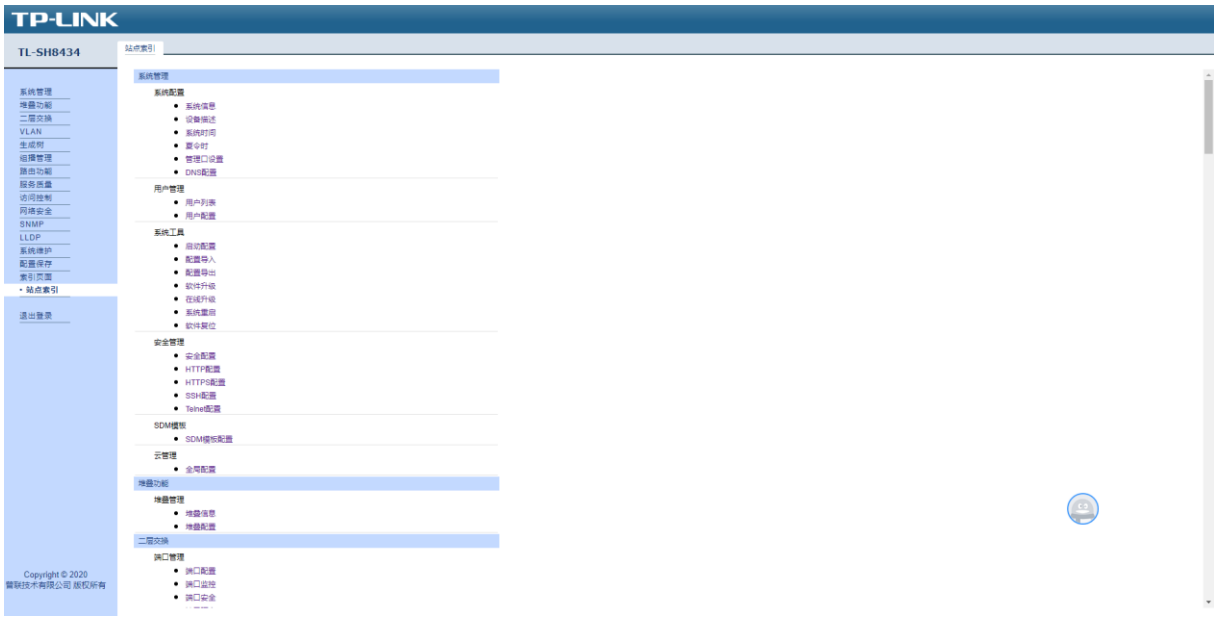
回目录

第17章　索引页面

通过站点索引部分，可快速进入各功能设置页面。

进入页面的方法：站点索引

点击所需进入的功能设置页面。



回目录

第18章　软件系统维护

在本交换机中，可以通过FTP功能加载软件。FTP（File Transfer Protocol，文件传输协议）在TCP/IP协议族中属于应用层协议，主要用于在远端服务器和本地主机之间传输文件，是IP网络上传输文件的通用协议。当交换机软件出故障导致无法正常启动时，也可以采用FTP功能重新加载软件。

18.1　硬件连接图

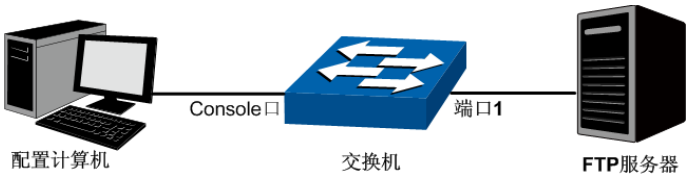


图 17-1　利用 FTP 加载软件连接图

1. FTP 服务器通过端口 1 连接到交换机。
2. 配置计算机通过 Console 口与交换机连接。配置计算机和 FTP 服务器可以是同一台主机。
3. 将交换机软件存储在 FTP 服务器的共享目录下，并记录相应用户名、密码以及交换机软件名称，以便后续使用。

18.2　配置超级终端

完成硬件连接后，为保证计算机能够正常通过交换机 Console 口进行本地登录，需在计算机上运行终端仿真程序，以便管理交换机。

1. 打开计算机的终端仿真程序（如 Hyperterminal 程序），配置如下参数：
   - 波特率：38400bps
   - 数据位：8 位
   - 奇偶校验：无
   - 停止位：1 位
   - 数据流控制：无

2. 在主窗口中输入回车键，可以看到“TL-SG5428>”的提示符，说明已成功登录交换机。

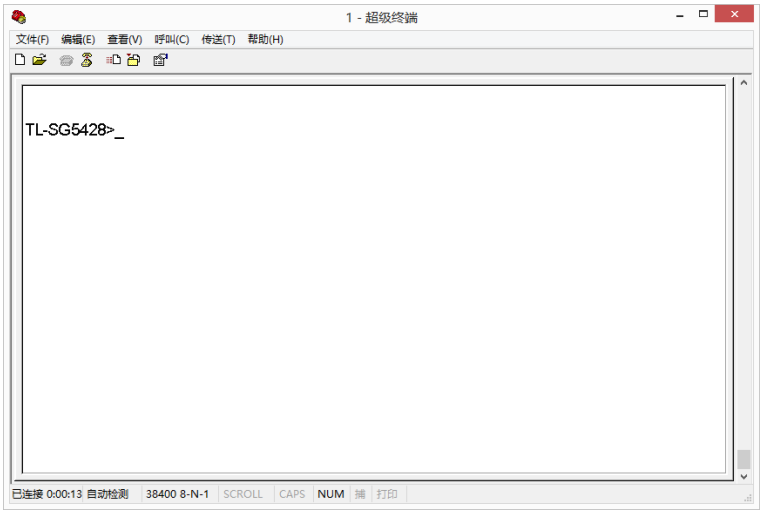


图 17-2 命令行主窗口

说明：

若计算机使用 Windows XP 系统，可在**开始>所有程序>附件>通讯>终端仿真程序**，打开终端仿真程序，配置如上所需参数，也可登录交换机。

18.3 bootUtil 菜单下加载软件

利用 FTP 功能加载软件需要进入交换机的 bootUtil 菜单。请按照下面提示步骤进行操作：

1. 将配置计算机的串口连接到交换机的 Console 口，并打开配置成功的超级终端。FTP 服务器连接到交换机端口 1。

2. 将交换机断电重启，当在超级终端界面中看到提示信息 Press CTRL-B to enter the bootUtil 时，同时按下 Ctrl 按键和 b 字母按键进入 bootUtil 菜单，如图 17-3 所示。

```
*********************************************
*         TP-LINK  BOOTUTIL(v1.0.0)         *
*********************************************
Copyright (c) 2015 TP-LINK Tech. Co., Ltd
Create Date: Oct 20 2015 10:02:35

help                    - print this list
reboot                  - reboot the system
ifconfig                - config the interface
ftp                     - config the remote host ip,the user name,user password
and the image file name
upgrade                 - upgrade the firmware
start                   - start the system
reset                   - reset the system to the factory config.
```

图 17-3 bootUtil 菜单

由于该提示信息显示时间较短，可以在交换机上电后一直按住 Ctrl 按键和 b 字母按键不放，直到进入 bootUtil 菜单。

3. 进入 bootUtil 菜单后，首先配置交换机的 IP 参数，命令格式为：

ifconfig ip xxx.xxx.xxx.xxx **mask** 255.255.255.0 **gateway** xxx.xxx.xxx.xxx。

此处设置交换机的 IP 地址为 10.10.70.22，掩码为 255.255.255.0，网关设置为 10.10.70.1。详细命令如下所示。输入命令后按回车键。

[TP-LINK] : *ifconfig ip 10.10.70.22 mask 255.255.255.0 gateway 10.10.70.1*

4. 然后配置存放升级软件的 FTP 服务器的参数，以方便交换机从 FTP 服务器上下载软件。命令格式为：**ftp host** xxx.xxx.xxx.xxx **user** xxxxx **pwd** xxxxx **file** xxxxxx.bin。

   此处以下面的 FTP 服务器参数为例：IP 地址为 10.10.70.146，登录 FTP 服务器的用户名和密码分别为 123，交换机的升级软件名称为 up.bin。详细命令如下所示。输入命令后按回车键。

   [TP-LINK] : *ftp host 10.10.70.146 user 123 pwd 123 file up.bin*

5. 最后输入 upgrade 命令后按回车键开始升级。等待片刻，超级终端会显示提示信息：You can only use the port 1 to upgrade，如下所示。请通过交换机的端口 1 连接的 FTP 服务器，若 FTP 没有连接到端口 1 将无法加载软件。请将 FTP 服务器通过端口 1 与交换机连接并重复上述操作。

   [TP-LINK] : *upgrade*

   You can only use the port 1 to upgrade.

6. 当超级终端弹出提示信息：Are you sure to upgrade the firmware[Y/N]: 时，输入 Y 开始升级，输入 N 退出升级。如下所示。图中的#字符表示正在升级，升级结束后将弹出[TP-LINK]命令提示符。

   Are you sure to upgrade the firmware[Y/N]:y

   ##

   ##

   [TP-LINK] :

7. 完成第 6 步后，请将交换机断电重启，则可以通过 CLI 命令管理交换机，如下图所示。

   [TP-LINK] :

   Press CTRL-B to enter the bootUtil

   Starting...

   TL-SG5428>

8. 当忘记了登录交换机的用户名和密码时，可在第 2 步进入交换机 bootUtil 菜单后输入 reset 命令来软件复位，复位后恢复到出厂默认设置，登录交换机的用户名和密码均为 admin。

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
A		回首页
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		回首页
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
C		回首页
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
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
D		回首页
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
E		回首页
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
F		回首页
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
G		回首页
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
H		回首页
-	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
I		回首页
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

英文缩写	英文全称	中文全称
J		回首页
-	Jumbo Frame	超长帧
L		回首页
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
M		回首页
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
N		回首页
NMS	Network Management Station	网络管理站
NTP	Network Time Protocol	网络时间协议
-	NTP Server	网络时间服务器
O		回首页
OID	Object Identifier	对象标识符
OSI	Open Systems Interconnection	开放系统互连
OUI	Organizationally Unique Identifier	全球统一标识符
P		回首页
-	Packet	数据包
PAP	Password Authentication Protocol	密码认证协议
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
-	Port	端口
PPP	Point-to-Point Protocol	点到点协议
PQ	Priority Queuing	优先队列

英文缩写	英文全称	中文全称
Q		回首页
QoS	Quality of Service	服务质量
-	Query	查询
R		回首页
RADIUS	Remote Authentication Dial in User Service	远程认证拨号用户服务
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
S		回首页
-	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
T		回首页
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
TTL	Time to Live	生存时间
-	Trap	陷阱
U		回首页
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
V		回首页
VACM	View-based Access Control Model	基于视图的访问控制模型

英文缩写	英文全称	中文全称
VLAN	Virtual Local Area Network	虚拟局域网
VOS	Virtual Operate System	虚拟操作系统
W		回首页
WAN	Wide Area Network	广域网
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
技术标准	IEEE 802.3:以太网介质访问控制（MAC）协议 IEEE 802.3i:10BASE-T 以太网 IEEE 802.3u:100BASE-TX 快速以太网 IEEE 802.3u:100BASE-FX 快速以太网（光纤） IEEE 802.3ab:1000BASE-T 千兆以太网 IEEE 802.3z:1000BASE-X 千兆以太网（光纤） IEEE 802.3ad:执行链路聚合的标准方法 IEEE 802.3x:流量控制 IEEE 802.1p:有关流量优先级的 LAN 第二层 Qos/Cos 协议（组播过滤功能） IEEE 802.1q:VLAN 网桥操作 IEEE 802.1x:基于端口的网络访问控制，身份验证 IEEE 802.1d:STP 生成树 IEEE 802.1s:MSTP 生成树 IEEE 802.1w:RSTP 生成树
PoE 供电标准①	IEEE 802.3af:通过以太网数据线对或设备来实现以太网设备供电 IEEE 802.3at:通过以太网数据线对或设备来实现以太网设备大功率供电
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:2 对 3 类(Cat3)或以上 UTP/STP（<=100m） 100BASE-TX:2 对 5 类(Cat5)或以上 UTP/STP（<=100m） 100BASE-FX:62.5μm/50μm 的 MMF（<=2000m） 1000BASE-T:4 对超 5 类（Cat5e)或以上 UTP/STP（<=100m） 1000BASE-SX：62.5μm/50μm 的 MMF（2m～550m） 1000BASE-LX：62.5μm/50μm 的 MMF（2m～550m）或 10μm 的 SMF（2m～5000m）
传输方式	存储转发
MAC 地址学习	自动更新
包转发速率	10BASE-T:14881pps/端口 100BASE-TX:148810pps/端口 100BASE-FX:148810pps/端口 1000BASE-T:1488095pps/端口 1000BASE-X:1488095pps/端口
交流输入	PoE 交换机：220V~ 50Hz 非 PoE 交换机：100-240V~ 50/60Hz

参数项	参数内容
工作温度	0℃~40℃
存储温度	-40℃~70℃
工作湿度	10%~90% RH 无凝结
存储湿度	5%~90% RH 无凝结
背板带宽	TL-SG5452：104Gbps TL-SG5428：56Gbps TL-SG5828F：56Gbps TL-SG5820F：40Gbps TL-SG5218：36Gbps TL-SG5210：20Gbps TL-SG5428PE: 56Gbps TL-SG5226PE：52Gbps TL-SG5226P：52Gbps TL-SG5218PE：36Gbps TL-SG5210PE：20Gbps TL-SL5452-Combo：17.6Gbps TL-SL5428-Combo：12.8Gbps TL-SL5218-Combo：7.2Gbps TL-SL5210：5.6Gbps

说明:

① 仅 TL-SG5428PE/TL-SG5226PE/TL-SG5226P/TL-SG5218PE/TL-SG5210PE 支持 PoE 供电标准。

回目录