

TP-LINK®

24FE+4GE 二层全网管交换机

TL-SL5428

用户手册

REV2.4.1
1910040614

声明

Copyright © 2016 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，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	1
1.1	目标读者	1
1.2	本书约定	1
1.3	章节安排	1
第 2 章	产品介绍	5
2.1	产品简介	5
2.2	产品外观	5
2.2.1	前面板	5
2.2.2	后面板	6
第 3 章	配置指南	7
3.1	登录 Web 页面	7
3.2	Web 页面简介	8
3.3	Web 配置注意事项	9
第 4 章	系统管理	10
4.1	系统配置	10
4.1.1	系统信息	10
4.1.2	设备描述	12
4.1.3	系统时间	12
4.1.4	夏令时	14
4.1.5	管理 IP	15
4.1.6	IPv6 管理 IP	16
4.2	用户管理	24
4.2.1	用户列表	24
4.2.2	用户配置	24
4.3	系统工具	25
4.3.1	配置导入	25
4.3.2	配置导出	26
4.3.3	软件升级	26
4.3.4	系统重启	27
4.3.5	软件复位	27

4.4	安全管理	27
4.4.1	安全配置	28
4.4.2	SSL 配置	29
4.4.3	SSH 配置	30
第 5 章	二层交换	37
5.1	端口管理	37
5.1.1	端口配置	37
5.1.2	端口监控	38
5.1.3	端口安全	39
5.1.4	端口隔离	41
5.1.5	环路监测	42
5.2	汇聚管理	43
5.2.1	汇聚列表	44
5.2.2	手动配置	45
5.2.3	LACP 配置	46
5.3	流量统计	48
5.3.1	流量概览	48
5.3.2	详细统计	49
5.4	地址表管理	50
5.4.1	地址表显示	51
5.4.2	静态地址表	52
5.4.3	动态地址表	53
5.4.4	过滤地址表	55
第 6 章	VLAN	57
6.1	802.1Q VLAN	57
6.1.1	VLAN 配置	59
6.1.2	端口配置	61
6.2	MAC VLAN	62
6.2.1	MAC VLAN	63
6.2.2	端口使能	64
6.3	协议 VLAN	64
6.3.1	协议配置	65

6.3.2	协议模板	66
6.3.3	端口使能	67
6.4	VLAN VPN	67
6.4.1	VPN 配置	69
6.4.2	VLAN 映射	69
6.4.3	端口使能	70
6.5	Private VLAN	71
6.5.1	PVLAN 配置	74
6.5.2	端口配置	75
6.6	GVRP	76
6.7	802.1Q VLAN 功能的组网应用	79
6.8	MAC VLAN 功能的组网应用	81
6.9	协议 VLAN 功能的组网应用	82
6.10	Private VLAN 功能的组网应用	84
第 7 章	生成树	86
7.1	基本配置	92
7.1.1	基本配置	92
7.1.2	生成树信息	93
7.2	端口配置	94
7.3	MSTP 实例	95
7.3.1	域配置	96
7.3.2	实例配置	96
7.3.3	实例端口	97
7.4	安全配置	99
7.4.1	端口保护	99
7.4.2	TC 保护	101
7.5	STP 功能的组网应用	101
第 8 章	以太网 OAM	106
8.1	基本配置	110
8.1.1	基本配置	110
8.1.2	Discovery 信息	111
8.2	链路监控	113

8.3	远端故障指示	114
8.4	远端环回	114
8.5	统计信息	115
8.5.1	统计信息	115
8.5.2	事件日志	116
8.6	DLDP	117
8.7	DLDP 功能的组网应用	120
第 9 章	DHCP	123
9.1	DHCP 中继	123
第 10 章	组播管理	127
10.1	IGMP 侦听	131
10.1.1	基本配置	132
10.1.2	VLAN 参数	133
10.1.3	端口参数	134
10.1.4	过滤地址	135
10.1.5	组播 VLAN	136
10.1.6	静态地址表	139
10.1.7	报文统计	141
10.1.8	查询器	142
10.1.9	IGMP 认证	143
10.2	MLD 侦听	144
10.2.1	基本配置	146
10.2.2	VLAN 配置	147
10.2.3	过滤配置	149
10.2.4	端口参数	150
10.2.5	静态组播组	150
10.2.6	查询器	151
10.2.7	MLD 报文统计	152
10.3	组播地址表	153
10.3.1	IPv4 组播表	153
10.3.2	IPv6 组播表	154
第 11 章	服务质量	156

11.1	QoS 配置.....	156
11.1.1	端口配置.....	159
11.1.2	DSCP 映射.....	160
11.1.3	802.1P /CoS 映射.....	162
11.1.4	队列调度模式.....	163
11.2	流量管理.....	163
11.2.1	带宽控制.....	163
11.2.2	风暴抑制.....	165
11.3	语音 VLAN.....	166
11.3.1	全局配置.....	168
11.3.2	端口配置.....	168
11.3.3	OUI 配置.....	170
第 12 章	访问控制.....	172
12.1	时间段配置.....	172
12.1.1	时间段列表.....	172
12.1.2	新建时间段.....	173
12.1.3	节假日定义.....	174
12.2	ACL 配置.....	174
12.2.1	ACL 列表.....	174
12.2.2	新建 ACL.....	175
12.2.3	MAC ACL.....	176
12.2.4	标准 IP ACL.....	177
12.2.5	扩展 IP ACL.....	177
12.2.6	组合字段 ACL.....	179
12.3	Policy 配置.....	180
12.3.1	Policy 列表.....	180
12.3.2	新建 Policy.....	181
12.3.3	配置 Policy.....	181
12.4	绑定配置.....	182
12.4.1	绑定列表.....	183
12.4.2	端口绑定.....	183
12.4.3	VLAN 绑定.....	184
12.5	访问控制功能组网应用.....	185

第 13 章 网络安全	188
13.1 四元绑定	188
13.1.1 绑定列表	188
13.1.2 手动绑定	190
13.1.3 扫描绑定	191
13.2 DHCP 侦听.....	193
13.2.1 DHCP 侦听	193
13.2.2 Option 82.....	197
13.3 ARP 防护	198
13.3.1 防 ARP 欺骗	201
13.3.2 防 ARP 攻击	202
13.3.3 报文统计	203
13.4 IP 源防护	204
13.5 DoS 防护.....	205
13.5.1 DoS 防护	206
13.5.2 攻击检测	208
13.6 802.1X 认证	208
13.6.1 全局配置	212
13.6.2 端口配置	213
13.7 AAA.....	215
13.7.1 全局配置	216
13.7.2 使能管理员权限	216
13.7.3 RADIUS 配置.....	216
13.7.4 TACACS+配置.....	217
13.7.5 服务器组配置	218
13.7.6 认证列表	219
13.7.7 应用认证设置	221
13.7.8 Dot1x 列表配置.....	221
13.7.9 默认设置	222
13.8 PPPoE 配置	223
第 14 章 SNMP	226
14.1 SNMP 配置	227

14.1.1	全局配置	228
14.1.2	视图管理	228
14.1.3	组管理	229
14.1.4	用户管理	231
14.1.5	团体管理	232
14.2	通知管理	234
14.2.1	通知管理	234
14.2.2	上报配置	236
14.3	RMON	238
14.3.1	历史采样	238
14.3.2	事件配置	239
14.3.3	警报管理	240
第 15 章	LLDP	242
15.1	基本配置	244
15.1.1	基本配置	245
15.1.2	端口配置	246
15.2	设备信息	247
15.2.1	本地信息	247
15.2.2	邻居信息	248
15.3	设备统计	249
第 16 章	集群管理	251
16.1	拓扑发现	252
16.1.1	邻居信息	252
16.1.2	配置显示	253
16.1.3	全局配置	254
16.2	拓扑收集	255
16.2.1	设备列表	255
16.2.2	配置显示	257
16.2.3	全局配置	258
16.3	集群管理	259
16.3.1	配置显示	259
16.3.2	集群配置	262

16.3.3	成员管理	264
16.3.4	拓扑图	265
16.4	集群管理功能组网应用	267
第 17 章	系统维护	269
17.1	运行状态	269
17.1.1	CPU 监控	269
17.1.2	内存监控	270
17.2	系统日志	270
17.2.1	日志列表	271
17.2.2	本地日志	272
17.2.3	远程日志	272
17.2.4	日志导出	273
17.3	系统诊断	274
17.3.1	线缆检测	274
17.4	网络诊断	275
17.4.1	Ping 检测	275
17.4.2	Tracert 检测	276
第 18 章	软件系统维护	277
18.1	硬件连接图	277
18.2	配置终端仿真软件	277
18.3	bootUtil 菜单下加载软件	278
附录 A	术语表	280
附录 B	技术参数规格	285

第1章 用户手册简介

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

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 所提到的“交换机”、“本产品”等名词，如无特别说明，系指 TL-SL5428 24FE+4GE 二层全网管交换机，下面简称为 TL-SL5428。
- 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	帮助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 TL-SL5428 的 Web 页面，并简要介绍页面特点。

章节	章节说明
第4章 系统管理	<p>本模块主要用于配置交换机的系统属性，主要介绍了：</p> <ul style="list-style-type: none"> ● 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：安全管理：针对不同的登录方式，增强用户管理交换机的安全性。包括安全配置、SSL 配置和 SSH 配置。
第5章 二层交换	<p>本模块主要用于配置交换机的基本功能，主要介绍了：</p> <ul style="list-style-type: none"> ● 端口管理：配置交换机端口的基本属性包括端口配置、端口监控、端口安全、端口隔离和环路监测。 ● 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	<p>VLAN 主要用于隔离广播域，通过划分虚拟工作中来简化网络管理，主要介绍了：</p> <ul style="list-style-type: none"> ● 802.1Q VLAN：划分基于端口的 VLAN，也是 MAC VLAN 和协议 VLAN 的基础。 ● MAC VLAN：在不改变原 802.1Q VLAN 配置的情况下划分 MAC VLAN。 ● 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 信息来达到配置 VLAN 的目的，并传播 VLAN 信息到其它交换机中，简化配置 VLAN 时的操作。
第7章 生成树	<p>生成树主要用于在局域网中消除环路。本模块主要用于配置交换机的生成树功能，主要介绍了：</p> <ul style="list-style-type: none"> ● 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 以太网 OAM	<p>本模块主要用于配置交换机的以太网 OAM 功能，主要介绍了：</p> <ul style="list-style-type: none"> ● 基本配置：开启以太网 OAM 功能，配置 OAM 模式并查看连接状态。 ● 链路监控：配置以太网 OAM 链路时间参数并选择是否启用事件通知。 ● 远端故障指示：配置端口是否启用远端故障信息通知。 ● 远端环回：选择开始或停止远端环回功能；选择忽略或者处理收到的远端环回请求。 ● 统计信息：查看详细的以太网 OAM 流量统计信息和事件日志信息。 ● DLDP：配置 DLDP 功能，允许交换机监控链路的物理配置及检测是否存在单向链路。
第 9 章 DHCP	<p>本模块用于配置 DHCP 中继功能，使不同子网内的 DHCP 客户端可以共用 DHCP 服务器。</p>
第 10 章 组播管理	<p>本模块主要用于配置交换机的组播管理功能，主要介绍了：</p> <ul style="list-style-type: none"> ● IGMP 侦听：配置 IGMP 侦听功能。 ● MLD 侦听：配置 MLD 侦听功能。 ● 组播地址表：配置 IPv4 和 IPv6 组播地址表。
第 11 章 服务质量	<p>本模块主要为网络中某些特殊应用程序提供保障，主要介绍了：</p> <ul style="list-style-type: none"> ● 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 12 章 访问控制	<p>本模块通过配置对报文的匹配规则和处理操作来实现对数据包的过滤功能，有效防止非法用户对网络的访问，节约网络资源，主要介绍了：</p> <ul style="list-style-type: none"> ● 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。
第 13 章 网络安全	<p>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：</p> <ul style="list-style-type: none"> ● 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：对局域网中的 IP 数据包进行过滤。 ● 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。 ● AAA：配置 AAA 功能用于防止设备被未经授权的用户操作。 ● PPPoE 配置：配置 PPPoE 电路 ID 插入功能用于支持在以太网接口中的认证、授权和计费（AAA）接入请求。

章节	章节说明
第 14 章 SNMP	<p>SNMP 提供了一个管理框架来监控和维护互联网设备。本模块主要用于配置交换机的 SNMP 功能，主要介绍了：</p> <ul style="list-style-type: none"> ● 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	<p>本模块用于配置 LLDP 功能，为 SNMP 提供部分信息，简化机器故障排除的过程，主要介绍了：</p> <ul style="list-style-type: none"> ● 基本配置：配置 LLDP 的参数。 ● 设备信息：查看本地设备以及邻居设备的 LLDP 信息。 ● 设备统计：查看本地设备的 LLDP 相关统计信息。
第 16 章 集群管理	<p>集群管理的主要目的是解决大量分散的网络设备的集中管理问题。模块主要用于配置交换机的集群管理功能，主要介绍了：</p> <ul style="list-style-type: none"> ● 拓扑发现：配置拓扑发现功能。用于获取与其直接相连的邻居交换机的信息。 ● 拓扑收集：配置拓扑收集功能。用于命令交换机收集网络的拓扑信息。 ● 集群管理：配置集群管理功能。用于建立和维护集群。
第 17 章 系统维护	<p>系统维护模块将管理交换机的常用系统工具组合在一起，主要介绍了：</p> <ul style="list-style-type: none"> ● 运行状态：对交换机内存和CPU进行监控。 ● 系统日志：查看在交换机上配置参数。 ● 系统诊断：检测与交换机连接的线缆及对端设备的可用性。 ● 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 18 章 软件系统维护	<p>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。</p>
附录 A 术语表	<p>整理用户手册中出现的术语。</p>
附录 B 技术参数规格	<p>技术参数规格表。</p>

[回目录](#)

第2章 产品介绍

2.1 产品简介

TL-SL5428 交换机是一款由普联技术有限公司自主设计和开发的，为构建高安全、高性能网络需求而专门设计的新一代二层全网管交换机，具有完备的安全策略、完善的 QoS 策略、丰富的 VLAN 特性、支持 IPV6 功能、易管理维护等特点。系统采用全新的软硬件平台，在安全接入策略、多业务支持、易管理和维护等方面为用户提供了全新的技术特性和解决方案，是理想的办公网、校园网的汇聚、接入层交换机以及中小企业、分支机构的核心交换机。

2.2 产品外观

2.2.1 前面板

本交换机的前面板由 24 个 10/100M 端口、4 个 1000M 端口、4 个 SFP 口、1 个 Console 口和指示灯组成，如图 2-1 所示。

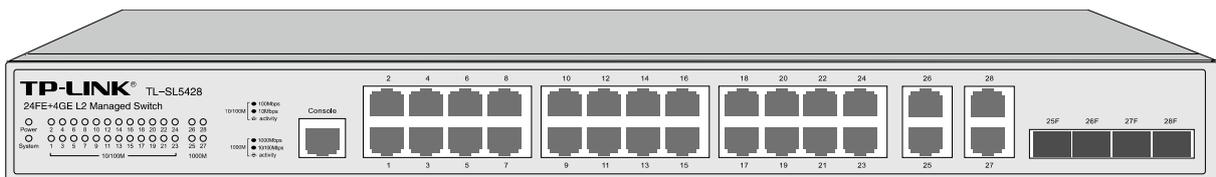


图 2-1 前面板

➤ 1 个 Console 端口

Console 端口位于面板的左边，用于和计算机或其他终端的串口相连，可以通过 Console 口登录并管理交换机。

➤ 24 个 10/100Mbps 自适应 RJ45 端口

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

➤ 4 个 10/100/1000Mbps 自适应 RJ45 端口

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

➤ 4 个 SFP 端口

SFP 模块卡扩展槽位于千兆 RJ45 端口的右边，同与其 Combo 共享的千兆 RJ45 端口共用指示灯，其中 25F-28F 分别于与端口 25-28 共用。

➤ 指示灯

指示灯，包括 Power, System, 10/100M, 1000M 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	
		闪烁	系统供电异常	
		熄灭	系统未通电或供电异常	
System	系统指示灯	常亮/熄灭	系统出现异常	
		闪烁	系统正常工作	
10/100M	端口指示灯	常亮	绿色	端口工作在百兆模式但没有数据传输
			黄色	端口工作在十兆模式但没有数据传输
		闪烁	端口正在传输数据	
1000M	端口指示灯	常亮	绿色	端口工作在千兆模式但没有数据传输
			黄色	端口工作在十兆或百兆模式但没有数据传输
		闪烁	端口正在传输数据	

2.2.2 后面板

交换机后面板由电源接口和防雷接地柱组成，如图 2-2 所示：

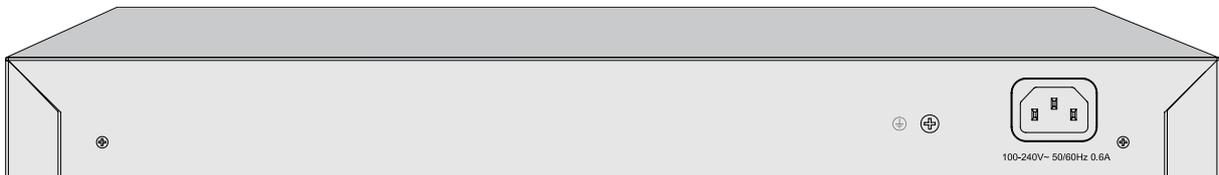


图 2-2 后面板

➤ 电源接口

位于后面板右侧，接入电源需为 100-240V~ 50/60Hz 0.6A 的交流电源。

➤ 防雷接地柱

位于电源接口左侧，请使用导线接地，以防雷击。



注意：

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

[回目录](#)

第3章 配置指南

3.1 登录 Web 页面

第一次登录时，请确认以下几点：

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

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



交换机登录页面如图 3-1 所示。



图 3-1 登录页面

在此页面输入交换机管理帐号的用户名和密码，出厂默认值均为 admin。

成功登录后可以看到交换机的系统信息，如图 3-2 所示。

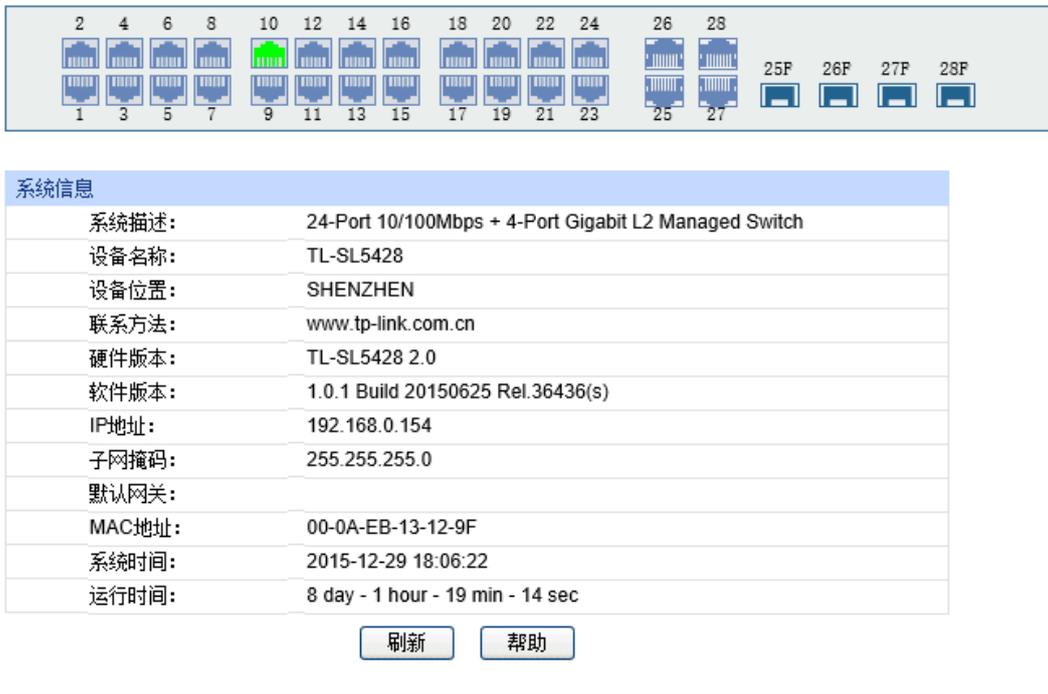


图 3-2 系统信息

3.2 Web 页面简介

交换机典型的 Web 页面如图 3-3 所示。



图 3-3 典型 Web 页面

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

3.3 Web 配置注意事项

➤ 索引页面

本交换机功能全面，基本覆盖了当前网络中用户的主流需求。通过一级菜单项**索引页面**，可以快速查询并定位至相应的功能页面。

➤ 配置保存

配置交换机后，点击<提交>按钮当前配置立即生效，但断电重启后配置参数将失效；若需要当前配置在交换机重启后依旧生效，则需要点击功能菜单栏底部的<配置保存>按钮保存配置参数。建议每次配置完成后均进行配置保存动作，或者在交换机断电或重启前完成该动作。

[回目录](#)

第4章 系统管理

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

4.1 系统配置

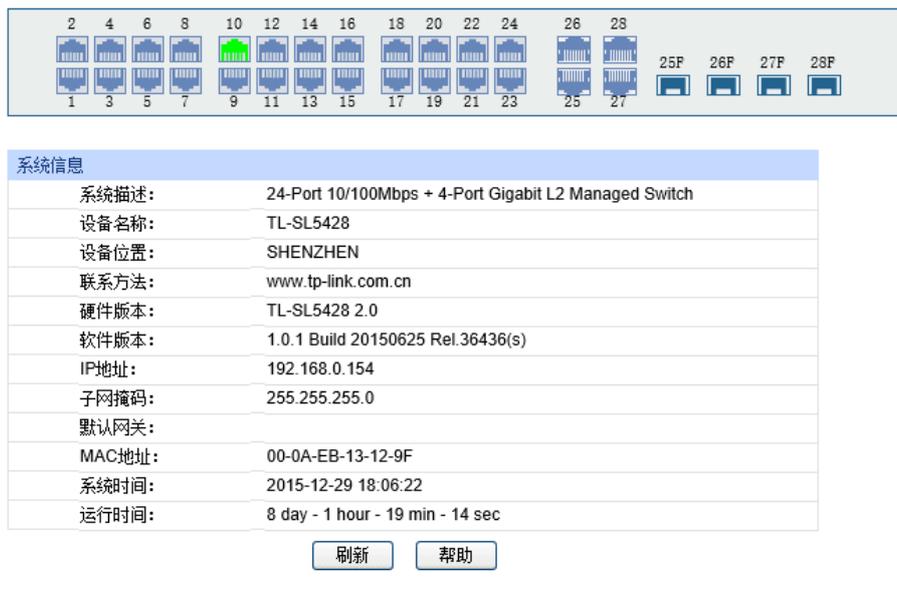
系统配置用于配置交换机的基本属性，本功能包括系统信息、设备描述、系统时间、夏令时、管理IP和IPv6管理IP六个配置页面。

4.1.1 系统信息

本页面用来查看本交换机的系统信息和端口连接信息。

端口状态界面指示了本交换机的 24 个 10/100Mbps RJ45 端口、4 个 10/100/1000Mbps RJ45 端口以及 4 个 SFP 扩展模块槽的工作状态，其中端口 1-24 是 10/100Mbps RJ45 端口，端口 25~28 是 10/100/1000Mbps RJ45 端口，端口 25F~28F 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



系统信息	
系统描述:	24-Port 10/100Mbps + 4-Port Gigabit L2 Managed Switch
设备名称:	TL-SL5428
设备位置:	SHENZHEN
联系方法:	www.tp-link.com.cn
硬件版本:	TL-SL5428 2.0
软件版本:	1.0.1 Build 20150625 Rel.36436(s)
IP地址:	192.168.0.154
子网掩码:	255.255.255.0
默认网关:	
MAC地址:	00-0A-EB-13-12-9F
系统时间:	2015-12-29 18:06:22
运行时间:	8 day - 1 hour - 19 min - 14 sec

图 4-1 系统信息

条目介绍：

➤ 端口状态



100M 端口未接入设备。



100M 端口工作速率为 100Mbps。



100M 端口工作速率为 10Mbps。



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 100 Mbps /10Mbps。



SFP 端口未接入设备。



SFP 端口工作速率为 1000Mbps。



SFP 端口工作速率为 100Mbps。

当鼠标移到某端口上时，会显示该端口的详细信息，如下图所示。

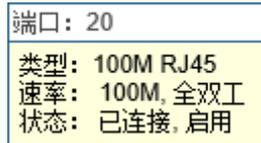


图 4-2 端口信息

条目介绍：

➤ 端口信息

- 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及传输模式。
- 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，可以帮助及时了解各端口的流量概况，便于监控网络流量和分析网络异常。如下图所示。

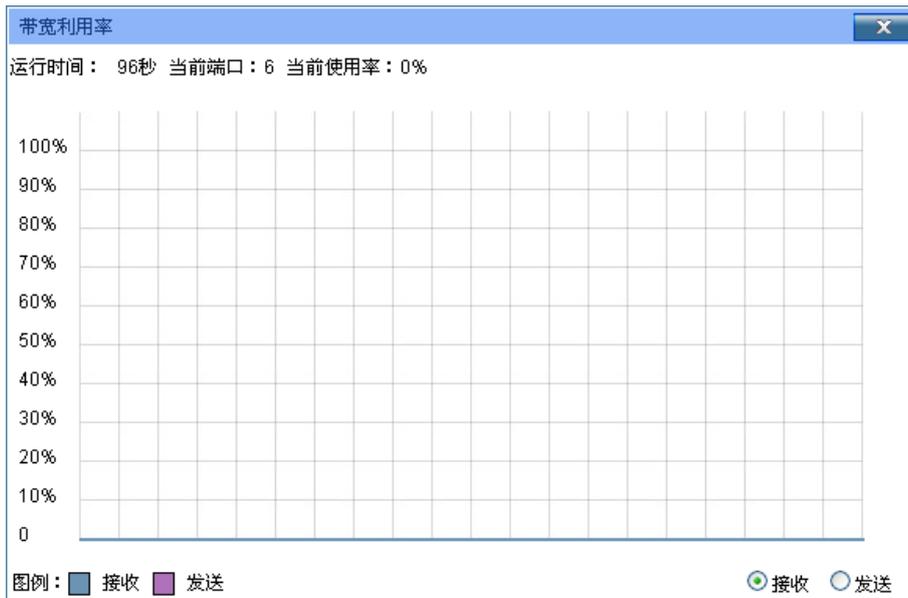


图 4-3 带宽利用率

条目介绍:

➤ 带宽利用率

接收

点击后，显示此端口接收数据的带宽利用率。

发送

点击后，显示此端口发送数据的带宽利用率。

4.1.2 设备描述

本页面用来配置交换机的描述信息，包括设备名称、设备位置、联系方法。

进入页面的方法：系统管理>>系统配置>>设备描述

设备描述

设备名称：

设备位置：

联系方法：

提交

注意：
设备名称、设备位置和联系方法最长可输入32个字符。

图 4-4 设备描述

条目介绍:

➤ 设备描述

设备名称:

填写交换机的名称。

设备位置:

填写交换机的位置信息。

联系方法:

填写联系方法。

4.1.3 系统时间

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

进入页面的方法：系统管理>>系统配置>>系统时间

时间信息

当前系统时间： 2006-01-02 02:04:58 星期一
当前时间来源： 手动配置时间

时间配置

手动配置时间

日期： 2006 01 02
时间： 02 04 58

从NTP服务器获取时间

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

首选NTP服务器： 133.100.9.2
备选NTP服务器： 139.78.100.163
更新周期： 12 小时

获取管理PC时间

提交
刷新
帮助

图 4-5 系统时间

条目介绍：

➤ 时间信息

当前系统时间： 显示交换机当前的日期、时间。

当前时间来源： 显示交换机当前系统时间的来源。

➤ 时间配置

手动配置时间： 勾选后，手动配置日期、时间。

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

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

获取管理PC时间： 勾选后，将管理主机的时间配置为交换机的系统时间。



注意：

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

4.1.4 夏令时

本页面用来配置交换机的夏令时。

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：

选择是否启用夏令时功能。

预定义模式：

选择一个预先定义好的夏令时配置。

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

循环模式：

配置夏令时功能。在这一模式下做的配置可以循环使用。

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

日期模式：

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

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



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 管理 IP

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

- “静态 IP”获取方式

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

- “DHCP”获取方式

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

- “BOOTP”获取方式

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

本页面用来配置交换机的管理 IP 地址。

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

The screenshot shows a web form titled "IP配置". It contains the following fields and options:

- MAC地址: 00-00-54-28-00-04
- 获取方式: 静态IP DHCP BOOTP
- 管理VLAN: (VLAN ID 1-4094)
- IP地址:
- 子网掩码:
- 默认网关:

On the right side of the form, there are two buttons: "提交" (Submit) and "帮助" (Help).

注意：

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

图 4-7 管理 IP

条目介绍：

➤ **IP 配置**

MAC 地址： 显示交换机的物理地址。

获取方式： 选择交换机网络参数的获取方式。

- 静态 IP：手动填写交换机的 IP 地址、子网掩码和默认网关。
- DHCP：从网络中的 DHCP 服务器获取交换机的网络参数。
- BOOTP：从网络中的 BOOTP 服务器获取交换机的网络参数。

- 管理 VLAN:** 配置交换机的管理 VLAN，只有连接到管理 VLAN 成员端口的计算机才可以通过 Web、telnet、SSL 或 SSH 等方式来管理交换机。当通过 Web 页面等方式来配置交换机的管理 VLAN 后，可能无法再对交换机进行配置管理，这时请将管理计算机连接的交换机端口切换到管理 VLAN 的成员端口以便获得管理交换机的权限。
- IP 地址:** 填写交换机的管理 IP 地址。该 IP 地址出厂默认值为 192.168.0.1，可以根据需要改变它。
- 子网掩码:** 填写本交换机的子网掩码。
- 默认网关:** 填写本交换机的默认网关。

**注意:**

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

4.1.6 IPv6 管理 IP

IPv6 (Internet Protocol Version 6, 因特网协议版本 6), 也被称为 IPng (IP Next Generation, 下一代因特网), 是 IETF (Internet Engineering Task Force, Internet 工程任务组) 制定的一套规范, 为 IPv4 (Internet Protocol Version 4, 因特网协议版本 4) 的升级版本。相比于 IPv4, IPv6 的 IP 地址长度从 32 比特增加到 128 比特, 极大地解决了 IPv4 的地址紧缺问题。

➤ IPv6 特点

IPv6 主要具有以下优点:

1. 充足的地址空间: IPv6 的源地址与目的地址长度都是 128 比特 (16 字节)。可以提供超过 3.4×10^{38} 种可能的地址空间, 完全可以满足多层次的地址划分需求, 及公有网络和机构内部私有网络的地址分配。
2. 简化的报文头格式: 通过将 IPv4 报文头中的某些字段裁减或移入到扩展报文头, 减小了 IPv6 基本报文头的长度, 从而简化了转发设备对 IPv6 报文的处理, 提高了转发效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍, 但 IPv6 基本报文头的长度只有 40 字节, 是 IPv4 报文头长度 (不包括选项字段) 的两倍。
3. 灵活的扩展报文头: IPv6 取消了 IPv4 报文头中的选项字段, 并引入了多种扩展报文头, 在提高处理效率的同时还大大增强了 IPv6 的灵活性, 为 IP 协议提供了良好的扩展能力。IPv4 报文头中的选项字段最多只有 40 字节, 而 IPv6 扩展报文头的大小只受到 IPv6 报文大小的限制。
4. 内置安全性: IPv6 将 IPSec 作为它的标准扩展头, 可以提供端到端的安全特性。这一特性也为解决网络安全问题提供了标准, 并提高了不同 IPv6 应用之间的互操作性。
5. 地址自动配置: 为简化主机配置, IPv6 支持有状态和无状态地址配置。

- 有状态地址配置：主机从服务器（如 DHCP 服务器）获取 IPv6 地址及相关信息。
- 无状态地址配置：主机根据自己的链路层地址及路由器发布的前缀信息自动配置 IPv6 地址及相关信息。

另外，主机也可根据自己的链路层地址及默认前缀（FE80::/64）生成链路本地地址，从而与本地链路上的其他主机进行通信。

6. 增强的邻居发现机制：IPv6的邻居发现协议是通过一组ICMPv6（Internet Control Message Protocol Version 6，Internet控制消息协议版本6）消息实现的，管理同一链路上邻居节点之间的信息交互。其代替了ARP（Address Resolution Protocol，地址解析协议）、ICMPv4（Internet Control Message Protocol Version 4，Internet控制消息协议版本4）的路由器发现和ICMPv4重定向消息，并提供了一系列其他功能。

➤ IPv6 地址简介

1. IPv6地址格式

IPv6 地址被表示为以冒号（:）分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，组和组之间用冒号隔开，每组的 16 比特用 4 个十六进制数来表示，字母不区分大小写，例如 2001:0000:130F:0000:0000:09C0:876A:130B。

为简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导0可以省略，即上述地址可写为2001:0:130F:0:0:9C0:876A:130B。
- 如果地址中包含连续两个或多个均为0的组，可以用双冒号（::）来代替，即上述地址可写为2001:0:130F::9C0:876A:130B。

如果地址中包含多个连续均为 0 的组时，双冒号一般用在连续均为 0 的组组数最多的部分。在 IPv6 地址中，双冒号只能出现一次，否则当设备将省略格式的 IPv6 地址恢复成 128 比特时，无法判断双冒号表示多少组 0。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号，接口标识相当于 IPv4 地址中的主机号。

地址前缀表示方式为：IPv6 地址/前缀长度。其中，“IPv6 地址”是前面所列出的任一形式，而“前缀长度”是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。

2. IPv6地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：在单个节点上，用来唯一标识一个接口。发送到单播地址的数据报文将被传送给此地址标识的接口。
- 组播地址：用来标识一组接口，通常这组接口属于不同的节点，类似于IPv4的组播地址。发送到组播地址的数据报文将被传送给此地址标识的所有接口。IPv6中没有广播地址，其功能是通过组播地址实现的。

- 任播地址：用来标识一组接口，通常这组接口属于不同的节点。发送到任播地址的数据报文将被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

IPv6 地址类型是由地址前面几位，即格式前缀指定的。下表列出地址类型与格式前缀的对应关系。

地址类型		格式前缀（二进制）	IPv6 前缀标识
单播地址	未指定地址	00...0（128 比特）	::/128
	回环地址	00...1（128 比特）	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址（当前已分配）	001	2xxx::/4 或 3xxx::/4
	保留类型（在未来被分配）	其他格式	
组播地址		11111111	FF00::/8
任播地址		任播地址从单播地址空间中进行分配，使用单播地址的格式。	

表 4-1 地址类型与格式前缀的对应关系

3. IPv6单播地址简介

IPv6单播地址用于在单个节点上，唯一标识一个接口，一般由子网前缀和接口标识两部分组成。

- 子网前缀：由IANA（The Internet Assigned Numbers Authority，互联网数字分配机构）、ISP（Internet Service Provider，互联网服务提供商）和各组织分配。
- 接口标识：用于标识链路上的一个接口，在链路上具有唯一性。

接口标识有多种构造方法，除组播地址外，格式前缀从001到111的IPv6地址的接口标识要求64位长，并构成EUI-64格式。

不同接口类型的EUI-64格式的接口标识的构造方法不同，其中，所有IEEE 802类型接口（例如，以太网接口、VLAN接口）的接口标识构造方法如下：

IEEE EUI-64格式的接口标识是从接口的MAC地址（链路层地址）变化而来的。IPv6地址中的接口标识是64位，而接口MAC地址是48位，因此需要在MAC地址的中间位置（从高位开始的第24位后）插入十六进制数FFFE（111111111111110）。为了确保这个从MAC地址得到的接口标识是唯一的，还要将U/L位（Universal/Local位，通用/本地位，即从高位开始的第7位）设置为“1”。最后得到的这组数则为EUI-64格式的接口标识。

以 MAC 地址 0012:0B0A:2D51 为例介绍构造 IEEE EUI-64 格式的接口标识的过程：将 FFFE 插入 MAC 地址的中间位置得到 0012:0BFF:FE0A:2D51；将 U/L 位设置为 1 得到 0212:0BFF:FE0A:2D51，即为 EUI-64 格式的接口标识。

从表 4-1 可知，IPv6 单播地址包括多种类型，以下介绍最常见的两种：全球单播地址和链路本地地址。

全球单播地址

全球单播地址是 IPv6 单播地址，全球唯一且路由可达。

全球单播地址以二进制 001（2000::/3）开头，由全局路由前缀、子网号和 EUI-64 格式的接口标识组成。全局路由前缀由 IANA 和 ISP 分配。子网号一般用于组织或企业内部进行子网划分。下图显示了全球单播地址的结构。

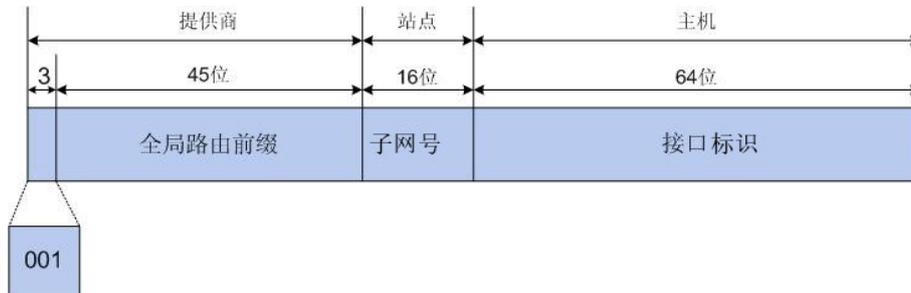


图 4-8 全球单播地址格式

链路本地地址

链路本地地址是 IPv6 单播地址，由链路本地前缀 FE80::/10（1111 1110 10）和 EUI-64 格式的接口标识构成，可以在任何接口上自动配置而成。下图显示了链路本地地址的结构。

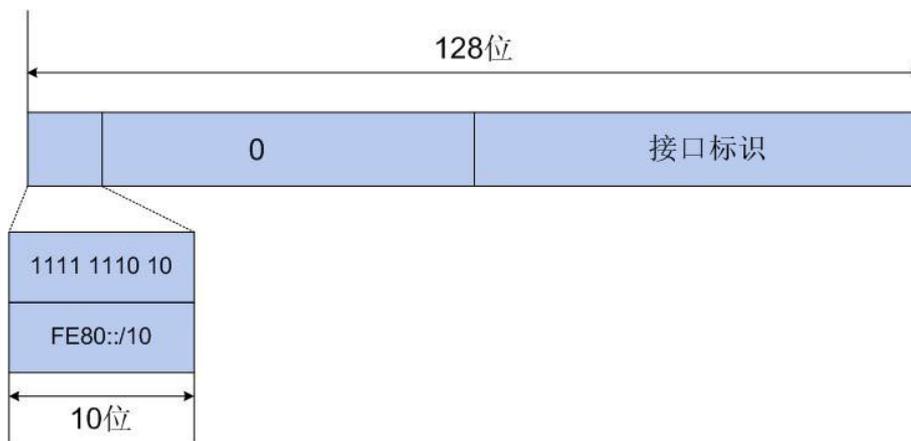


图 4-9 链路本地地址格式

链路本地地址用于邻居发现协议和无状态自动配置过程。由于接口标识的唯一性，链路本地地址在链路范围内也具有唯一性，在本地链路上的节点可以使用链路本地地址进行通信。IPv6 设备不会将使用链路本地地址作为源或目的地址的数据包转发到其他链路上。



说明：

可以为每个接口配置多个 IPv6 地址，但只能有一个链路本地地址。

➤ IPv6 邻居发现协议

IPv6 邻居发现协议（Neighbor Discovery Protocol, NDP）使用 ICMPv6 消息和请求节点的多播地址来获取同一链路上邻居节点的链路层地址，验证邻居的可达性，并跟踪相邻设备。

1. 邻居请求消息和邻居通告消息

邻居请求消息 NS(Neighbor Solicitation)是类型为 135 的 ICMPv6 消息，邻居通告消息 NA(Neighbor Advertisement)是类型为 136 的 ICMPv6 消息。

邻居请求消息 NS 可用于获取邻居的链路层地址、验证邻居是否可达及进行重复地址检测。

邻居通告消息 NA 的主要作用是对 NS 消息进行响应。另外，当本地链路上的节点的链路层地址变更时，节点会主动发送 NA 消息，向邻居节点通告本节点的变化信息。

获取邻居的链路层地址

当一个节点需要获取同一链路上另一个节点的链路本地地址时，可以通过邻居请求消息 NS 和邻居通告消息 NA 实现。实现过程如下：

- 节点A以组播方式发送NS消息。NS消息的源地址是节点A的接口IPv6地址，目的地址是节点B的被请求节点组播地址，消息内容中包含了节点A的链路层地址。
- 节点B收到NS消息后，判断报文的地址是否为自己的IPv6地址对应的被请求节点组播地址。如果是，则节点B可以学习到节点A的链路层地址，并以单播方式返回NA消息，其中包含了节点的链路层地址。
- 节点A从收到的NA消息中就可获取到节点B的链路层地址。

验证邻居是否可达

在获取到邻居节点的链路层地址后，可以通过邻居请求消息 NS 和邻居通告消息 NA 验证邻居节点的可达性。验证过程如下：

- 节点发送NS消息，其中目的地址是邻居节点的IPv6地址。
- 如果收到邻居节点的确认报文，则认为邻居可达；否则，认为邻居不可达。

重复地址检测

在无状态自动配置过程中，给接口分配 IPv6 地址之前，需要经过重复地址检测（Duplicate Address Detection），验证该地址的唯一性。

通过邻居请求消息 NS 和邻居通告消息 NA 可以实现重复地址检测功能。检测过程如下：

- 节点A发送NS消息，NS消息的源地址是未指定地址::，目的地址是待检测的IPv6地址对应的被请求节点组播地址，消息内容中包含了待检测的IPv6地址。
- 如果节点B已经使用这个IPv6地址，则会返回NA消息。其中包含了节点的IPv6地址。
- 节点A收到节点B发来的NA消息，就知道该IPv6地址已被使用。反之，在一定时间内，节点A未收到节点B发来的NA消息，则说明该地址未被使用，节点A就可使用此IPv6地址。

每一个 IPv6 单播地址（全局或本地链接）都需要对其在链路上的唯一性进行验证。但只有链路本地地址被验证过唯一性之后，才能对其他 IPv6 地址进行重复地址检测。

2. 路由器请求消息和路由器通告消息

路由器请求消息 RS(Router Solicitation)是类型为 133 的 ICMPv6 消息，路由器通告消息 RA(Router Advertisement) 是类型为 134 的 ICMPv6 消息。

在没有抑制 RA 消息发布的情况下，IPv6 路由器会周期性地发布 RA 消息。RA 消息通常包括以下信息：

- 一个或多个 IPv6 前缀，本地链路上的节点能使用这些前缀来自动配置它们的 IPv6 地址。

- 每个前缀的生存周期。
- 标识所支持的自动配置类型（无状态或者有状态）。
- 默认路由器信息（发送该通告消息的设备是否作为默认路由器，如果是，该设备作为默认路由器的时间，单位为秒）。
- 给主机的附加信息，如跳数限制和主机在发送数据包时可使用的最大传输单元（MTU）等。

当路由器收到主机发来的 RS 消息时，也会回复给该主机 RA 消息，来帮助主机迅速进行自动配置而不必等待路由器的周期性 RA 消息。

主机通过监听 RA 消息发现和选择默认设备。

地址无状态自动配置是指，节点根据收到的 RA 消息中的地址前缀和其他配置参数，自动配置其接口的 IPv6 地址和其他信息。

3. 邻居重定向消息

邻居重定向消息（Neighbor Redirect）是类型为 137 的 ICMPv6 消息。

当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定条件时，缺省网关会向源主机发送 ICMPv6 重定向消息，通知主机选择更好的下一跳进行后续报文的发送。

设备在满足下列条件时会发送对主机重定向的 ICMPv6 重定向报文：

- 接收和转发数据报文的接口是同一接口。
- 被选择的路由本身没有被 ICMPv6 重定向报文创建或修改过。
- 被选择的路由不是缺省路由。
- 被转发的 IPv6 数据报文中不包含路由扩展头。

本页面用来配置交换机的 IPv6 管理 IP 地址。

进入页面的方法：系统管理>>系统配置>>IPv6 管理 IP

IPv6全局配置

IPv6功能: 启用 禁用 提交

IPv6链路本地地址配置

链路本地地址配置方式: 手动 自动

IPv6链路本地地址: (格式: 地址) 提交

链路本地地址状态: 正常

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 提交

通过DHCPv6获取全球地址

启用DHCPv6获取全球地址 提交

手动添加IPv6全球地址

配置方式: EUI-64 非EUI-64

IPv6全球地址: (格式: 地址或前缀/前缀长度) 提交

系统当前IPv6全球地址列表

选择	IPv6全球地址	前缀长度	地址类型	首选时间/有效时间	状态
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>			

删除
修改
帮助

图 4-10 IPv6 管理 IP

条目介绍:

➤ **IPv6 全局配置**

IPv6 功能: 选择是否启用交换机的 IPv6 功能。

➤ **IPv6 链路本地地址配置**

链路本地地址配置方式: 可以根据需要选择链路本地地址配置方式。

- 手动: 手动填写链路本地地址。
- 自动: 系统自动生成一个链路本地地址。

IPv6 链路本地地址: 当选择“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: 一般状态。
 - 试探: 新配置的链路本地地址可能为此状态。
 - 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:** 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:** 当选择“EUI-64”方式配置全球地址时, 在此输入地址前缀。
当选择“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:** 可以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。
- 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。
 - 手动: 表示对应地址是用户手动配置的。
- 首选时间/有效时间:** 显示全球地址的首选时间和有效时间。
- 状态:** 显示全球地址的状态。
- 正常: 一般状态。
 - 试探: 新配置的全局地址可能为此状态。
 - 重复: 表明对应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。

4.2 用户管理

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

本功能包括用户列表和用户配置两个配置页面。

4.2.1 用户列表

可以在本页查看到当前交换机存在的全部用户。

进入页面的方法：系统管理>>用户管理>>用户列表

用户列表		
序号	用户名	类型
1	admin	管理员

图 4-11 用户列表

4.2.2 用户配置

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

进入页面的方法：系统管理>>用户管理>>用户配置

用户信息				
用户名：	<input type="text"/>			
用户类型：	<input type="text" value="受限用户"/>	<input type="button" value="添加"/>		
密码：	<input type="text"/>			<input type="button" value="清除"/>
确认密码：	<input type="text"/>			

用户列表				
选择	序号	用户名	类型	操作
<input type="checkbox"/>	1	admin	管理员	编辑

注意：

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

图 4-12 用户配置

条目介绍：

➤ 用户信息

用户名： 填写登录 Web 页面的用户名。

- 用户类型：** 选择该用户名的用户类型。
- 管理员：可以编辑、修改和查看交换机各个功能的配置。
 - 受限用户：仅可以查看交换机各个功能的配置情况。
- 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、状态：** 显示当前用户的序号、用户名、用户类型和用户状态。
- 操作：** 点击对应条目的<编辑>按键，可以修改该条目的用户信息。修改完毕后点击<修改>按键，修改内容生效。但是不允许修改当前登录用户自身的用户类型和状态。

4.3 系统工具

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

4.3.1 配置导入

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

进入页面的方法：**系统管理>>系统工具>>配置导入**

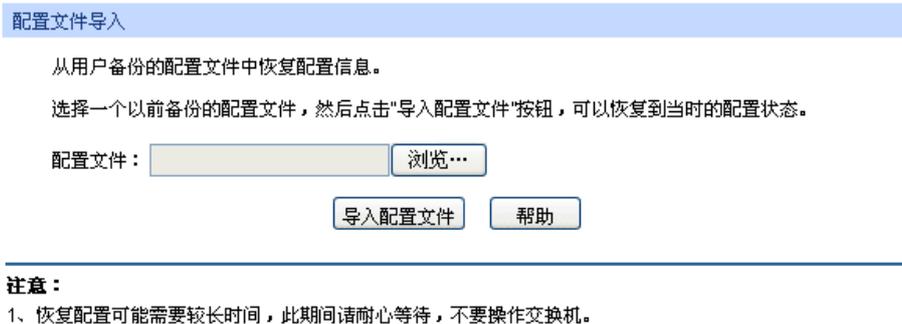


图 4-13 配置导入

条目介绍：

➤ **配置文件导入**

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

 **注意：**

- 恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

- 导入配置文件的过程不能关闭交换机电源，否则将导致交换机损坏而无法使用。
- 导入配置文件后，交换机中原有的配置信息将会丢失。如果导入的配置文件有误，可能会导致交换机无法被管理。

4.3.2 配置导出

配置导出功能是将交换机当前的配置信息打包成文件保存到 PC 中，方便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

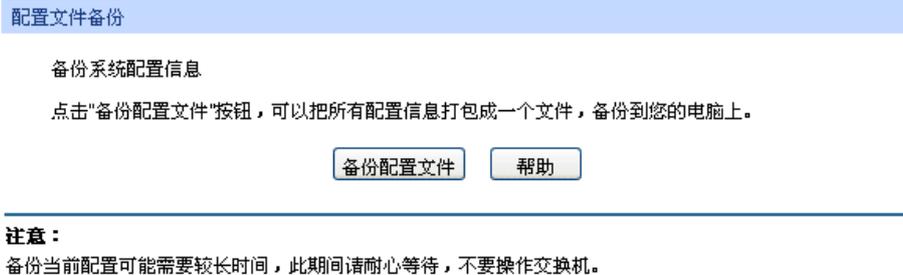


图 4-14 配置导出

条目介绍：

> 配置文件备份

备份配置文件： 以文件形式保存设置。建议升级前进行备份。



注意：

备份当前配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

4.3.3 软件升级

本交换机可以通过 Web 方式升级系统文件，系统升级后将获得更完善的功能，请在网站 <http://www.tp-link.com.cn> 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 4-15 软件升级

 **注意：**

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

4.3.4 系统重启

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

进入页面的方法：**系统管理>>系统工具>>系统重启**

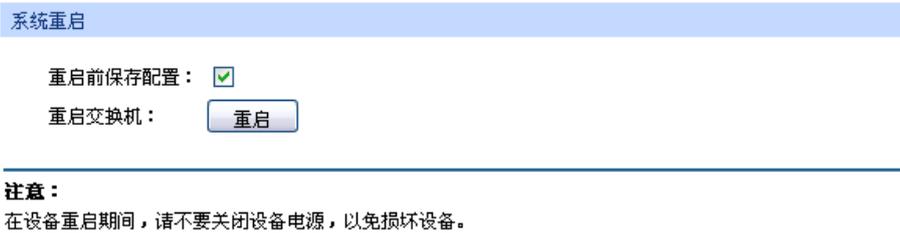


图 4-16 系统重启

 **注意：**

在设备重启期间，请不要关闭设备电源，以免损坏设备。

4.3.5 软件复位

通过软件复位，可以将交换机恢复为出厂设置状态，所有配置数据将被清除。

进入页面的方法：**系统管理>>系统工具>>软件复位**



图 4-17 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**、**SSL 配置**、**SSH 配置**三个配置页面。

4.4.1 安全配置

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

进入页面的方法：系统管理>>安全管理>>安全配置

身份限制

限制类型： ▾

选择序号	IP地址	掩码
<input type="checkbox"/> 1	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> 2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> 3	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> 4	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> 5	<input type="text"/>	<input type="text"/>

MAC地址：

端口号：

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

超时配置

超时时间： 分钟（5-30）

管理人数限制

人数限制功能： 启用 禁用

管理员人数： 名（1-16）

受限用户人数： 名（0-15）

图 4-18 安全配置

条目介绍：

➤ 身份限制

限制类型：

选择限制用户身份的类型。

- 基于 IP：用来限制访问交换机 Web 页面的用户的 IP 网段。
- 基于 MAC：用来限制访问交换机 Web 页面的用户的主机 MAC 地址。
- 基于端口：用来限制访问交换机 Web 页面的交换机端口号。

- IP 地址、掩码:** 选择“基于 IP”时才能进行配置。只允许指定 IP 网段的用户才可以通过 Web 页面访问交换机。
- MAC 地址:** 选择“基于 MAC”时才能进行配置。只允许指定 MAC 地址的用户才可以通过 Web 页面访问交换机。
- 端口号:** 选择“基于端口”时才能进行配置。只允许指定端口上的用户才可以通过 Web 页面访问交换机。
- **超时配置**
- 超时时间:** 如果在超时时间之内没有对交换机管理页面进行操作，系统会自动退出管理页面，若要再次进行管理请重新登录。默认为 10 分钟。
- **管理人数限制**
- 人数限制功能:** 选择是否启用人数限制功能。
- 管理员人数:** 填写可同时登录交换机 Web 页面的管理员总数。
- 受限用户人数:** 填写可同时登录交换机 Web 页面的受限用户总数。

4.4.2 SSL 配置

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

SSL 协议提供的服务主要有:

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

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

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

交换机也支持通过 IPv6 地址连接 HTTPS, 若为交换机设置了一个 IPv6 地址, 如 3001::1, 则可以通过 [https://\[3001::1\]](https://[3001::1]) 登录交换机的 Web 页面。

进入页面的方法：系统管理>>安全管理>>SSL 配置

注意：

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

图 4-19 SSL 证书管理

条目介绍：

➤ **SSL 证书管理**

SSL 功能： 选择是否启用交换机的 SSL 功能。

➤ **证书导入**

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

➤ **密钥导入**

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



注意：

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

4.4.3 SSH 配置

SSH (Secure Shell, 安全外壳) 是由 IETF (Internet Engineering Task Force, 因特网工程任务组) 所制定，建立在应用层和传输层基础上的安全协议。SSH 加密连接所提供的功能类似于一个 telnet 连接，但是传统的 telnet 远程管理方式在本质上是不安全的，因为它在网络上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 and 加密算法，协商一致后，由客户端向服务器端发起请求

登录的认证请求，认证通过后双方即可进行信息的交互。本交换机支持 SSH 服务器功能，可以使用 SSH 客户端软件通过 SSH 连接方式登录交换机。

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

进入页面的方法：**系统管理>>安全管理>>SSH 配置**

全局配置

SSH功能： 启用 禁用

Protocol V1： 启用 禁用

Protocol V2： 启用 禁用

静默时长： 秒（1-120）

最大连接数： （1-5）

密钥导入

选择你要导入交换机的密钥。

密钥类型：

密钥文件：

注意：

1、导入密钥可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 4-20 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。默认为 120 秒。
- 最大连接数：** 填写 SSH 同时可允许的最大连接数，连接数若满，将无法再建立新的连接。默认为 5。

➤ **密钥导入**

- 密钥类型：** 选择所要导入的密钥类型。本机支持 SSH-1 RSA,SSH-2 RSA 和 SSH-2 DSA 三种类型的密钥。
- 密钥文件：** 选择要导入的密钥文件。
- 导入密钥：** 点击此按键，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。

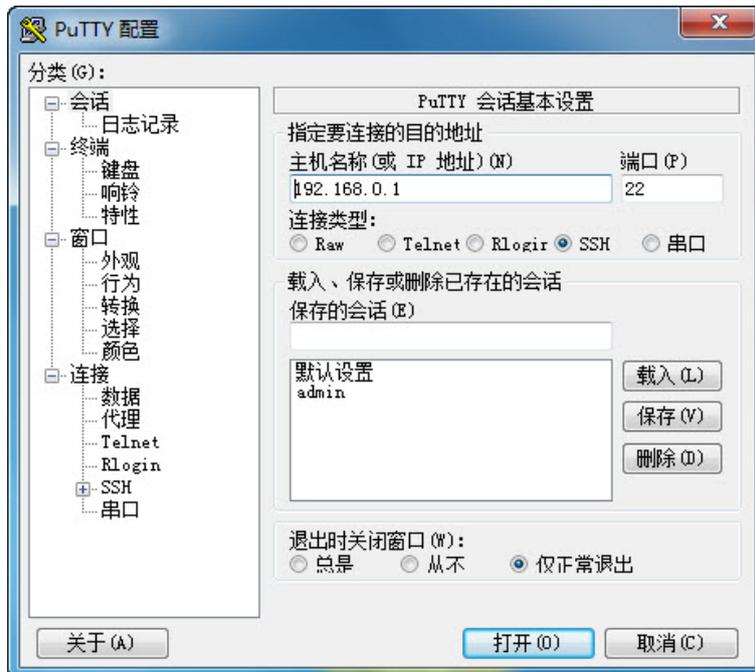
组网应用 1:

➤ 组网需求

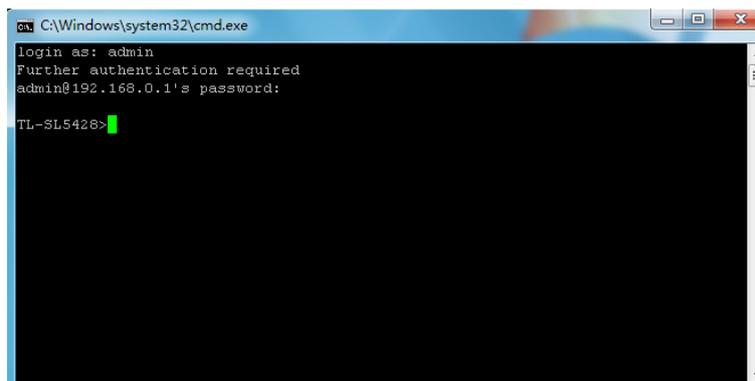
1. 使用 SSH 功能的“密码认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

➤ 配置步骤

1. 打开软件，登录 PuTTY 的主界面。在“主机名称”处填写交换机的 IP 地址；“端口”保持默认的 22；“连接类型”处选择 SSH 的接入方式。如下图所示。



2. 点击<打开>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。



注意:

完成上述配置步骤后，PuTTY 客户端显示“TL-SL5428>”表明已经成功登录交换机，并处在用户模式下。若要通过 SSH 进入特权模式管理交换机，需要先设置进入特权模式的密码。对于出厂设置下的交换机，请先使用串口线连接主机及交换机的 Console 口，在终端仿真程序上设置该密码。详细步骤请参考《命令行手册》中的 1.1.2 配置特权模式密码。

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。

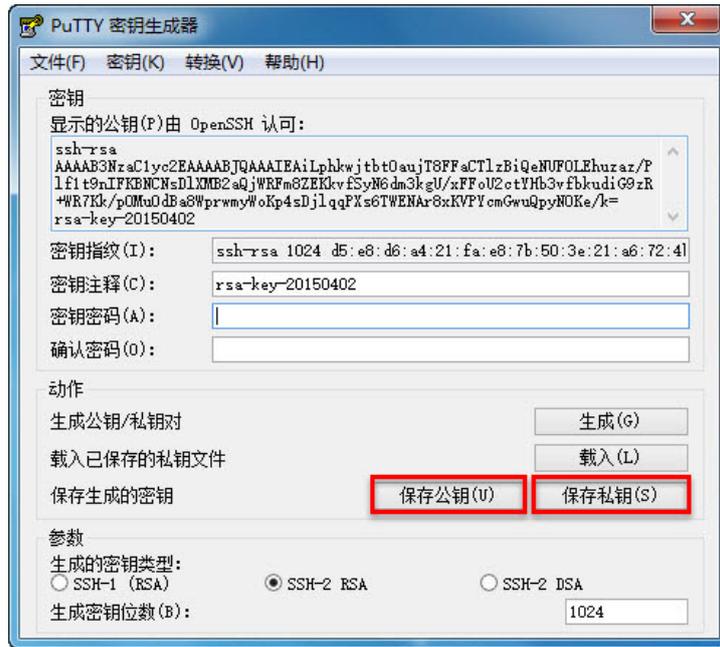
➤ 配置步骤

1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。

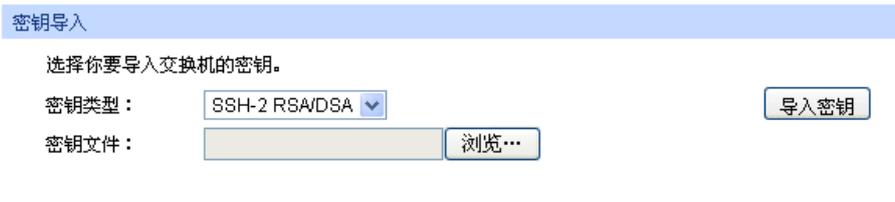
**注意:**

- 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。



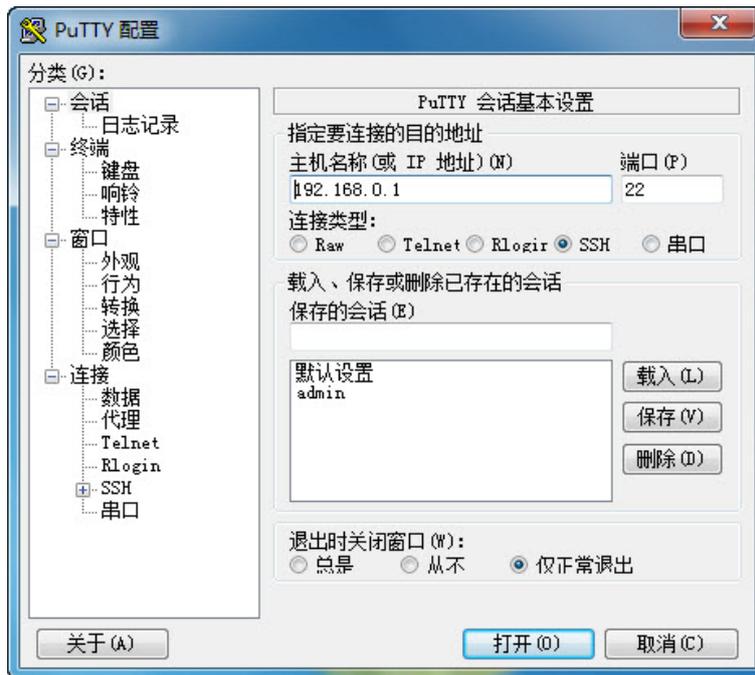
3. 在交换机配置页面上，将保存至主机上的公钥文件导入交换机中。



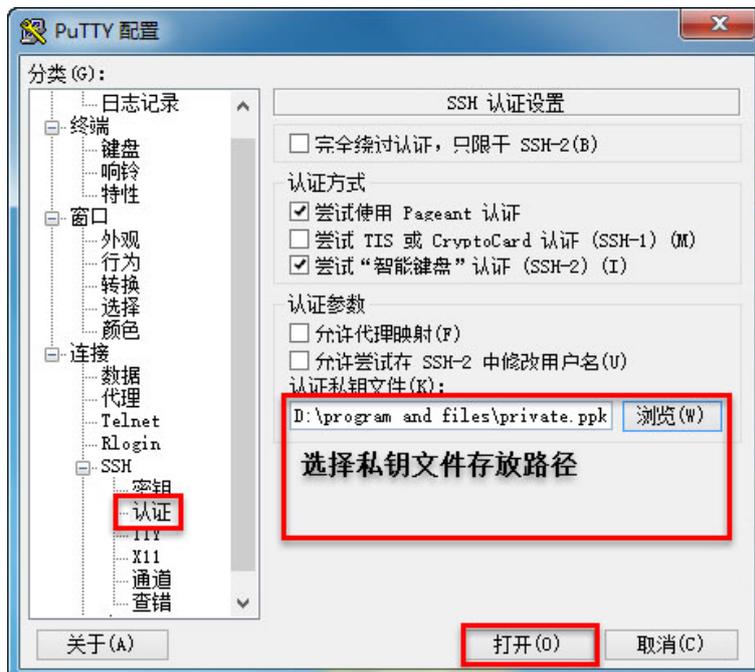
注意:

- 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。

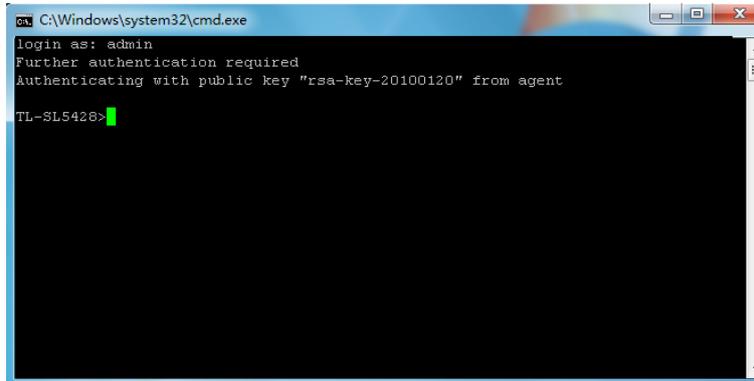
4. 打开 PuTTY 的主界面，输入 IP 地址并选择连接类型为 SSH，如下图所示。



5. 点击左边的目录栏进入 SSH 目录下的认证菜单，将私钥文件导入至 SSH 客户端软件中，再点击<打开>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。



```
C:\Windows\system32\cmd.exe
login as: admin
Further authentication required
Authenticating with public key "rsa-key-20100120" from agent
TL-SL5428>
```

注意：

完成上述配置步骤后，Putty 客户端显示“TL-SL5428>”表明已经成功登录交换机，并处在用户模式下。若要通过 SSH 进入特权模式管理交换机，需要先设置进入特权模式的密码。对于出厂设置下的交换机，请先使用串口线连接主机及交换机的 Console 口，在终端仿真程序上设置该密码。详细步骤请参考《命令行手册》中的 **1.1.2 配置特权模式密码**。

[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功能配置页面。

5.1.1 端口配置

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

端口基本参数将会直接影响端口的工作方式，请结合实际情况进行配置。

进入页面的方法：二层交换>>端口管理>>端口配置

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

注意：
端口描述1-16个字符。

图 5-1 端口配置

条目介绍：

➤ 端口配置

- 端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：** 勾选端口配置端口参数，可多选。
- 端口：** 显示交换机的端口号。
- 描述：** 填写端口的描述信息，便于区分各个端口的用途。

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

**注意:**

- 端口状态配置为禁用则不能通过该端口管理交换机，请将要进行管理的端口配置为启用状态。
- 从属于同一个汇聚组的所有成员端口的相应参数配置应该保持一致。

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

监控端口配置

选择监控端口：

被监控端口配置

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

图 5-2 端口监控

条目介绍:

➤ **监控端口配置**

选择监控端口: 选择物理端口作为监控端口，可在此端口连接数据检测设备，当选择“禁用”选项时将禁止端口监控。

➤ **被监控端口配置**

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: 勾选端口配置为被监控端口，可多选。

端口: 显示交换机的端口号。

入口监控: 对被监控端口收到的数据进行监控，复制到监控端口。

出口监控: 对被监控端口发出的数据进行监控，复制到监控端口。

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



注意:

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

5.1.3 端口安全

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

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

进入页面的方法：二层交换>>端口管理>>端口安全

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

注意：

最大学习地址数的范围为0-64。

图 5-3 端口安全

条目介绍：

➤ 端口安全

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



注意：

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

端口隔离配置

初始端口： 结束端口：

转发端口：

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

端口隔离列表

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

图 5-4 端口隔离

条目介绍：

➤ 端口隔离配置

初始/结束端口： 选择指定端口，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。

➤ 端口隔离列表

端口： 显示交换机的端口号。

转发端口： 显示可转发的端口列表。

5.1.5 环路监测

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

进入页面的方法：二层交换>>端口管理>>环路监测

全局配置

环路监测功能： 启用 禁用

环路监测间隔： 秒（1-1000）

自动恢复时间： 倍监测间隔（1-100） 提交

页面自动刷新： 启用 禁用

自动刷新间隔： 秒（3-100）

端口配置

端口 选择

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

提交
手动恢复
帮助

注意：

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

图 5-5 环路检测

条目介绍：

➤ 全局配置

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

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

**注意:**

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

5.2 汇聚管理

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

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

- 开启**GVRP、802.1Q VLAN、语音VLAN、生成树、QoS配置、DHCP侦听及端口配置**（速率、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。
- 开启**端口安全、端口监控、MAC地址过滤、静态MAC地址绑定、半双工及802.1X认证**功能的端口，不能加入汇聚组。
- 开启**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带宽为8000Mbps。
- LAG的流量会根据选路算法均衡分配到各个成员端口中。当LAG中的一个或几个端口连接断开的时候, 这些端口的流量会转移到LAG中其它链接正常的端口中, 具备链路冗余备份功能。

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

5.2.1 汇聚列表

在本页可以查看到交换机当前的全部汇聚组。

进入页面的方法: 二层交换>>汇聚管理>>汇聚列表

全局配置

选路算法: 源目的MAC地址 提交

汇聚列表

选择	组号	描述	成员	操作
<input type="checkbox"/>	LAG1	Static LAG	3, 4, 5, 6	编辑 查看

全选
删除
帮助

注意:

- 1、LACP动态创建的汇聚组不能被手动删除。

图 5-6 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。

详细信息	
组号描述：	LAG3
汇聚类型：	手动设置
端口状态：	启用
速率双工：	Auto
端口流控：	启用
入口带宽(bps)：	---
出口带宽(bps)：	---
广播包抑制(pps)：	---
多播包抑制(pps)：	---
UL包抑制(pps)：	---
Qos优先级：	cos0
加入的VLAN：	1

[返回](#)

图 5-7 汇聚组状态

5.2.2 手动配置

可以在本页对汇聚组进行手动配置，手动配置的汇聚端口的 LACP 状态为禁用。

进入页面的方法：二层交换>>汇聚管理>>手动配置

汇聚组配置

选择组号： ▼

该组描述：

成员端口

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

注意：

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

图 5-8 手动配置

条目介绍：

➤ **全局配置**

选择组号： 选择汇聚组的序号，组号格式为 LAG*。

该组描述： 汇聚组的描述信息，便于区分各个汇聚组的用途。手动配置的汇聚组不可更改描述。

➤ 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。

可以在本页配置交换机的 LACP 功能。

进入页面的方法：二层交换>>汇聚管理>>LACP 配置

全局配置

系统优先级: (0 - 65535) 提交

LACP 配置

选择

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

提交 帮助

注意:

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

图 5-9 LACP 配置

条目介绍:

➤ 全局配置

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

➤ LACP 配置

端口选择: 点击<选择>按键,可根据所输端口号,快速选择相应端口。

选择: 勾选端口配置端口 LACP 功能,可多选。

端口: 显示交换机的端口号。

管理 Key: 处于同一汇聚组的成员,需配置相同的管理 Key。

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

模式: 选择相应端口的LACP模式。

状态: 选择相应端口是否启用 LACP 功能。

LAG: 显示端口当前所属的汇聚组。

5.3 流量统计

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

5.3.1 流量概览

流量概览用来显示交换机各端口的流量信息，便于监控网络流量和分析网络异常。

进入页面的方法：**二层交换>>流量统计>>流量概览**

自动刷新

自动刷新： 启用 禁用

刷新周期： 秒 (3-300) 提交

流量概览

端口
选择

端口	接收数据包数	发送数据包数	接收字节数	发送字节数	信息查询
1	0	0	0	0	详细信息
2	0	0	0	0	详细信息
3	0	0	0	0	详细信息
4	0	0	0	0	详细信息
5	0	0	0	0	详细信息
6	0	0	0	0	详细信息
7	0	0	0	0	详细信息
8	0	0	0	0	详细信息
9	0	0	0	0	详细信息
10	0	0	0	0	详细信息
11	0	0	0	0	详细信息
12	0	0	0	0	详细信息

刷新
清空
帮助

图 5-10 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

自动刷新

自动刷新： 启用 禁用

刷新周期： 秒（3-300）

详细统计

端口

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

图 5-11 详细统计

条目介绍：

➤ 自动刷新

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。

➤ 详细统计

端口： 输入所要查看流量信息的交换机端口号。

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）。

Alignment 错误包： 端口接收的长度为 64-2044 字节（带 vlan-tag 则为 2048 字节）的校验和错误且字节数不对齐的数据帧（Alignment Error）及校验和错误且字节数对齐的数据帧（CRC Error）。

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）。
大于 1023 字节包:	端口接收的长度大于 1023 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 **MAC** 地址将报文输出到相应的端口。地址表包含了端口间报文转发的地址信息，是交换机实现报文快速转发的基础。地址表中的表项可以通过自动学习和手动绑定两种方式进行更新和维护，多数地址表条目都是通过自动学习功能来创建和维护的，而对于某些相对固定的连接来说，手动绑定可以提高交换机的效率，通过 **MAC** 地址过滤功能可以使交换机对不期望转发的数据帧进行过滤，从而提升了网络安全性。

地址表的分类及特点如下表所示：

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

本功能包括**地址表显示**、**静态地址表**、**动态地址表**和**过滤地址表**四个配置页面。

5.4.1 地址表显示

在本页可以查看到交换机地址表的全部信息。

进入页面的方法：二层交换>>地址表管理>>地址表显示

显示配置

MAC地址：（格式为：00-00-00-00-00-01）

VLAN ID：（1-4094）

端口：

地址类型： 全部 静态 动态 过滤

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

当前地址总数：58

注意：
默认显示条上限为100条，请点击显示按钮获取完整的地址表信息。

图 5-12 地址表显示

条目介绍：

➤ 显示配置

MAC 地址：填写欲查找条目需包含的 MAC 地址信息。

VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。

端口：选择欲查找条目需包含的交换机端口。

地址类型：选择欲查找条目需包含的地址类型信息。

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

➤ 地址表

MAC 地址：显示交换机学习到的 MAC 地址。

VLAN ID：显示 MAC 地址条目对应的 VLAN ID。

- 端口：**显示 MAC 地址条目对应的交换机端口。
- 地址类型：**显示 MAC 地址的类型。
- 老化状态：**显示 MAC 地址的老化状态。

5.4.2 静态地址表

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

进入页面的方法：二层交换>>地址表管理>>静态地址表

新建条目

MAC地址： (格式为：00-00-00-00-00-01)

VLAN ID： (1-4094) 添加

端口：

查找条目

查找选项： 查找

静态地址表

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
<input type="checkbox"/>			端口 1		

提交
删除
帮助

当前地址总数：0

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

图 5-13 静态地址表

条目介绍：

> 新建条目

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

> 查找条目

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

➤ 静态地址表

- 选择:** 勾选条目进行删除或修改该条目对应的交换机端口号，可多选。
- MAC 地址:** 显示静态绑定的 MAC 地址。
- VLAN ID:** 显示 MAC 地址条目对应的 VLAN ID。
- 端口:** 显示 MAC 地址条目对应的交换机端口。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和老化来不断更新其动态地址表。

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

在本页可以配置交换机的动态地址表功能。

进入页面的方法：二层交换>>地址表管理>>动态地址表

老化配置

自动老化： 启用 禁用

老化时间： 秒（10-630秒，默认为300秒）

查找条目

查找选项：

动态地址表

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

当前地址总数： 1

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

图 5-14 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： 填写需要的地址老化时间。默认为 300 秒。

➤ 查找条目

查找选项： 选择动态地址表的显示规则，可以帮助快速查找到所需的条目。

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

➤ 动态地址表

选择： 勾选动态地址条目进行删除或将该条目绑定为静态地址，可多选。

MAC 地址： 显示动态绑定的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

绑定： 将动态绑定的地址条目转化为静态绑定。

**说明：**

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

5.4.4 过滤地址表

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

进入页面的方法：二层交换>>地址表管理>>过滤地址表

新建条目

MAC地址： (格式为：00-00-00-00-00-01)

VLAN ID： (1-4094) 添加

查找条目

查找选项：全部 查找

过滤地址表

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
全选 删除 帮助					

当前地址总数：0

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

图 5-15 过滤地址表

条目介绍：

➤ **新建条目**

MAC 地址：填写过滤的 MAC 地址。

VLAN ID：填写 MAC 地址条目对应的 VLAN ID。

➤ **查找条目**

查找选项：选择过滤地址表的显示规则，可以帮助快速查找到所需的条目。

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

➤ **静态地址表**

选择：勾选过滤地址条目进行删除，可多选。

MAC 地址：显示过滤的 MAC 地址。

VLAN ID:	显示 MAC 地址条目对应的 VLAN ID。
端口号:	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、性能显著下降甚至使网络不可用等问题。通过交换机实现 LAN 互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network）技术，这种技术可以把一个 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文被限制在一个 VLAN 内。同一个 VLAN 内的主机通过传统的以太网通信方式进行报文的交互，而不同 VLAN 内的主机之间则需要通过路由器或三层交换机等网络层设备进行通信。如图 6-1 所示。

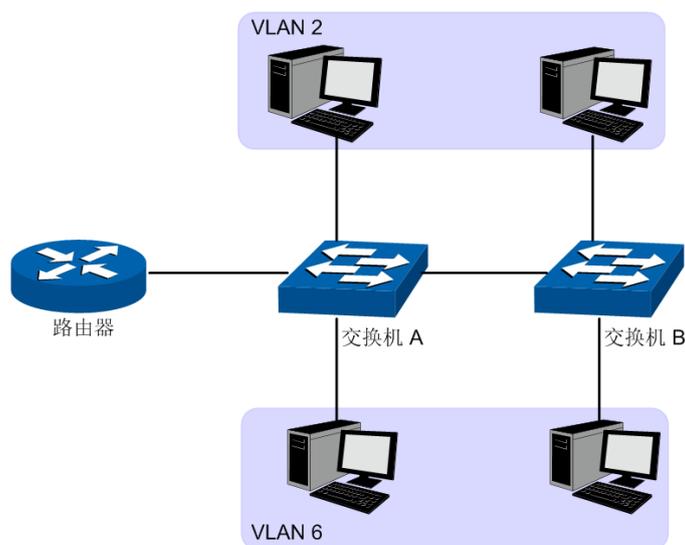


图 6-1 VLAN 示意图

VLAN 的优点如下：

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

VLAN 的划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一个交换机上，也可以跨越交换机。本交换机支持的 VLAN 划分方式包括 802.1Q VLAN、MAC VLAN 和协议 VLAN 三种。MAC VLAN 和协议 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，如图 6-2 所示。VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。

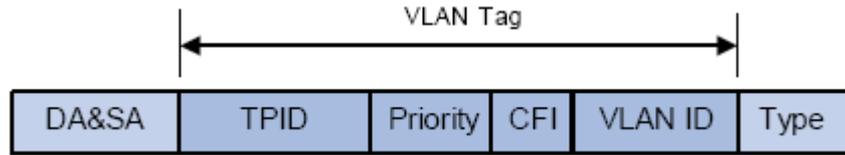


图 6-2 VLAN Tag 组成字段

- 1) **TPID**: 用来表示本数据帧是带有 VLAN Tag 的数据。该字段长度为 16bit。协议规定的缺省取值为 0x8100。
- 2) **Priority**: 用来表示数据包的传输优先级。
- 3) **CFI**: 以太网交换机中，CFI 总被设置为 0。由于兼容特性，CFI 常用于以太网类网络和令牌环类网络之间，如果在以太网端口接收的帧 CFI 设置为 1，表示该帧不进行转发，这是因为以太网端口是一个无标签端口。
- 4) **VLAN ID**: 用来标识该报文所属 VLAN 的编号。该字段长度为 12bit，取值范围为 0~4095。由于 0 和 4095 是保留值，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，当接收到的数据包不携带 VLAN Tag 时，交换机会为该数据包封装带有接收端口缺省 VLAN ID 的 VLAN Tag，将数据包在接收端口的缺省 VLAN 中进行传输。

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

➤ 端口的三种链路类型

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 类型端口的出口规则为 TAG，能够保证转发各种 VLAN 的数据包时不改变其携带的 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缺省 VLAN 内广播。

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

端口类型	对接收报文的处理		发送报文时的处理
	报文不带 Tag	报文带 Tag	
Access	接收报文，并为报文添加缺省的 VLAN Tag 即输入端口的 PVID。	当 VID=端口 PVID,接收报文。 当 VID≠端口 PVID,丢弃报文。	去掉 Tag 后，发送报文。
Trunk		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。	保持原有 Tag 发送报文。
General			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。

表 6-1 端口类型与 VLAN 数据处理关系

IEEE 802.1Q VLAN 功能包括 **VLAN 配置**、**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，所有端口的缺省 VLAN 均为 VLAN1，只有属于 VLAN1 的端口才能访问交换机 Web 页面。VLAN1 无法编辑和删除。

条目介绍：

➤ **端口配置**

- VLAN ID 选择:** 点击<选择>按键，可根据所输 VLAN ID，快速查找 VLAN 条目。
- 选择:** 勾选条目进行删除，可多选。
- VLAN ID:** 显示 VLAN ID。
- 名称:** 显示 VLAN 的描述信息。

端口成员： 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。
- 查看：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。

VLAN配置

VLAN ID: (2 - 4094) VID检查

VLAN 描述: (1-16个字符)

选择端口成员

端口 选择

选择	端口	链路类型	出口规则	LAG
<input type="checkbox"/>	1	ACCESS	UNTAG	---
<input type="checkbox"/>	2	ACCESS	UNTAG	---
<input type="checkbox"/>	3	ACCESS	UNTAG	---
<input type="checkbox"/>	4	ACCESS	UNTAG	---
<input type="checkbox"/>	5	ACCESS	UNTAG	---
<input type="checkbox"/>	6	ACCESS	UNTAG	---
<input type="checkbox"/>	7	ACCESS	UNTAG	---
<input type="checkbox"/>	8	GENERAL	UNTAG ▼	---
<input type="checkbox"/>	9	ACCESS	UNTAG	---
<input type="checkbox"/>	10	ACCESS	UNTAG	---
<input type="checkbox"/>	11	ACCESS	UNTAG	---
<input type="checkbox"/>	12	ACCESS	UNTAG	---
<input type="checkbox"/>	13	ACCESS	UNTAG	---
<input type="checkbox"/>	14	ACCESS	UNTAG	---

提交
全选
返回
帮助

注意：

端口的链路类型可以在“端口配置”标签页下修改。

图 6-4 创建或编辑 802.1Q VLAN

条目介绍：

➤ **VLAN 配置**

VLAN ID： 填写 VLAN ID。

VLAN 描述： 填写 VLAN 的描述信息，以便区分各个 VLAN 的用途。

VID 检查 点击<VID 检查>按键，检查所填的 VLAN ID 是否有效。

➤ **选择端口成员**

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： 勾选端口配置属于 VLAN 的端口成员，可多选也可不选。

端口： 显示交换机的端口号。

链路类型： 显示相应端口的端口类型，本项可在**端口配置**页面中进行设置。

出口规则: 选择 VLAN 端口成员的出口规则。默认为 UNTAG。

- TAG: 输出的数据帧带有 tag 信息。
- UNTAG: 输出的数据帧不带 tag 信息。

LAG: 显示端口当前所属的汇聚组。

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**

选择	端口	端口类型	PVID	LAG	所属VLAN
<input type="checkbox"/>		ACCESS			VLAN ID查询
<input type="checkbox"/>	1	ACCESS	1	---	查询
<input type="checkbox"/>	2	ACCESS	1	---	查询
<input type="checkbox"/>	3	ACCESS	1	---	查询
<input type="checkbox"/>	4	ACCESS	1	---	查询
<input type="checkbox"/>	5	ACCESS	1	---	查询
<input type="checkbox"/>	6	ACCESS	1	---	查询
<input type="checkbox"/>	7	ACCESS	1	---	查询
<input type="checkbox"/>	8	GENERAL	1	---	查询
<input type="checkbox"/>	9	ACCESS	5	---	查询
<input type="checkbox"/>	10	ACCESS	1	---	查询
<input type="checkbox"/>	11	ACCESS	1	---	查询
<input type="checkbox"/>	12	ACCESS	1	---	查询
<input type="checkbox"/>	13	ACCESS	1	---	查询
<input type="checkbox"/>	14	ACCESS	1	---	查询

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。

端口7加入的VLAN		
VLAN ID	VLAN名称	从该VLAN移除
1	Default VLAN	移除

VLAN ID

注意：

端口7加入VLAN的数目：1

图 6-6 查看端口所属 VLAN

条目介绍：

> 端口加入的 VLAN

- VLAN ID 查找:** 点击<查找>按键，可根据所输 VLAN ID，快速查找端口所属的 VLAN 条目。
- VLAN ID:** 显示 VLAN ID。
- VLAN 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。

6.2 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。
3. 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。

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**

The screenshot shows the 'MAC VLAN配置' (MAC VLAN Configuration) and 'MAC VLAN列表' (MAC VLAN List) sections. The configuration section includes input fields for MAC address (format: 00-00-00-00-00-01), MAC description (1-8 characters), and VLAN ID (1-4094), with '添加' (Add) and '清空' (Clear) buttons. The list section shows a search box for MAC address and a '选择' (Select) button. Below the table, it indicates '当前MAC VLAN列表为空' (Current MAC VLAN list is empty) and has '全选' (Select All), '删除' (Delete), and '帮助' (Help) buttons.

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。只有在配置了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**

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

图 6-8 开启 MAC VLAN 使能端口

勾选端口启用MAC VLAN功能，默认情况下所有端口MAC VLAN功能均已关闭。

MAC 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 页面结合实际网络结构设置端口链路类型。
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	创建 MAC VLAN	必选操作。在 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。

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

协议类型	对应取值
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 端口类型与 VLAN 数据处理关系。

6.3.1 协议配置

在协议配置页面中，可以创建协议 VLAN 并查看当前已创建的协议 VLAN。

进入页面的方法：**VLAN>>协议 VLAN>>协议配置**

协议 VLAN 配置

协议类型： 添加

VLAN ID： (1-4094) 清空

协议 VLAN 列表

选择	协议类型	以太网协议类型	VLAN ID	操作
当前协议 VLAN 列表为空				

图 6-9 创建并查看协议 VLAN

条目介绍：

➤ 协议 VLAN 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 VLAN 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。
- 以太网协议类型：** 显示该协议 VLAN 的以太网协议类型值。
- VLAN ID：** 显示该协议对应的 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。

6.3.2 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**

协议模板配置

协议类型： (1-8个字符)

以太网协议类型： (4位十六进制数)

协议模板列表

选择	序号	协议类型	以太网协议类型
<input type="checkbox"/>	1	IP	0800
<input type="checkbox"/>	2	ARP	0806
<input type="checkbox"/>	3	RARP	8035
<input type="checkbox"/>	4	IPX	8137
<input type="checkbox"/>	5	AT	809B

图 6-10 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值。



注意：

当协议模板与 VLAN 绑定后，将无法删除协议模板。

6.3.3 端口使能

端口使能用来开启端口的协议VLAN功能。只有在配置了协议VLAN并使能端口，才能正式启用协议VLAN功能。

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

图 6-11 开启协议 VLAN 使能端口

勾选端口启用协议VLAN功能，默认情况下所有端口协议VLAN功能均已关闭。

协议 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 页面结合实际网络结构设置端口链路类型。
2	创建 VLAN	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 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	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。
4	选择支持协议 VLAN 的端口	必选操作。在 VLAN>>协议 VLAN>>端口使能 页面选择支持协议 VLAN 的端口。
5	创建协议 VLAN	必选操作。在 VLAN>>协议 VLAN>>协议配置 页面中选择协议类型并输入 VLAN ID 来创建 VLAN。
6	编辑/查看 VLAN	可选操作。在 VLAN>>协议 VLAN>>协议配置 页面点击<编辑>按钮对相应的 VLAN 进行编辑。
7	删除 VLAN	可选操作。在 协议配置 页面勾选相应的 VLAN 条目, 点击<删除>按钮进行删除。

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，需要配置 SP VLAN，然后再配置相应的 VLAN 映射，使用户的私网报文能够按照 VLAN 映射条目插入外层 Tag 或者修改 Tag，顺利穿越骨干网络到达目的地。

1. 当启用 VLAN-VPN 功能时，将同时启用 VLAN 映射功能。启用 VLAN-VPN 功能后，若端口收到 Tag 报文，交换机会根据 VLAN 映射表条目给报文封装外层 VLAN Tag，然后通过上联端口在骨干网络中传输双 Tag 报文；如果端口接收报文不带 Tag，将按照其它 VLAN 方式进行处理。
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. 若不启用 VPN 模式，仅在端口使能页面使能端口，则只开启 VLAN 映射功能。当使能端口接收到 Tag 报文时，将根据 VLAN 映射表对报文中的 Tag 字段进行映射，映射到 SP VLAN 中。该功能使运营商的网络构架更为灵活，在连接接入层设备的端口上可以根据 VLAN Tag 对不同的终端用户进行分类，并在 SP VLAN 中进行传输，提供不同的网络服务。
4. 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

协议类型	对应取值
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**、**VLAN 映射**和**端口使能**三个配置页面。

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，交换机将根据 VLAN 映射表条目对收到的 tag 数据包插入外层 tag。

进入页面的方法：**VLAN>>VLAN VPN>>VPN 配置**

VPN全局配置

VPN模式： 启用 禁用

全局TPID： (4位十六进制整数)

VPN上联端口

<input type="checkbox"/> 1(LAG1)	<input type="checkbox"/> 2(LAG1)	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6
<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11(LAG7)	<input type="checkbox"/> 12
<input type="checkbox"/> 13(LAG7)	<input type="checkbox"/> 14	<input type="checkbox"/> 15(LAG7)	<input type="checkbox"/> 16	<input type="checkbox"/> 17(LAG7)	<input type="checkbox"/> 18
<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28		

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

勾选端口设置为 VPN 上联端口，请将连接到骨干网络的端口设置为上联端口。



注意：

启用 VPN 模式后，请在 VLAN 映射功能页面创建 VLAN 映射条目。

6.4.2 VLAN 映射

VLAN 映射功能可以将报文的 VLAN TAG 按照 VLAN 映射条目替换成 SP VLAN 的 VLAN TAG，然后在 SP VLAN 范围中转发报文。如果启用 VPN 模式，则按照 VLAN 映射条目对 TAG 报文插入外层 TAG，然后新的 VLAN 中转发报文。

进入页面的方法：**VLAN>>VLAN VPN>>VLAN 映射**

图 6-13 创建 VLAN 映射条目

条目介绍:

➤ **VLAN 映射配置**

C VLAN:

Customer VLAN（用户 VLAN）。本交换机中收到 TAG 报文时，对接收报文所属的 VLAN 称为 C VLAN。

SP VLAN:

Service Provider VLAN（服务商 VLAN）。在骨干网络中，用户可以使用公网 VLAN 为不同的 C VLAN 提供服务，本交换机中将公网 VLAN 称为 SP VLAN。

描述:

填写 VLAN 映射条目的附加描述信息，可留空。

➤ **VLAN 映射列表**

C VLAN 选择:

点击<选择>按键，可根据所输的 C VLAN 快速查找 VLAN 映射条目。

选择:

勾选条目进行删除，可多选。

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。

6.4.3 端口使能

端口使能用来开启端口的VLAN映射功能。只有在配置了VLAN映射后并使能端口，才能正式启用VLAN映射功能。

图 6-14 开启 VLAN 映射使能端口

勾选端口启用VLAN映射功能，默认情况下关闭所有端口的VLAN映射功能。



注意:

启用 VPN 模式时无需配置端口使能。当未启用 VPN 模式时，端口使能对 VLAN 映射功能生效。

VLAN VPN 配置步骤:

步骤	操作	说明
1	启用 VPN 模式	必选操作。在 VLAN>>VLAN VPN>>VPN 配置 功能页面启用 VPN 模式功能。
2	设置全局 TPID	可选操作。在 VLAN>>VLAN VPN>>VPN 配置 功能页面，根据上联端口的对端设备属性设置全局 TPID 值。
3	设置上联端口	必选操作。在 VLAN>>VLAN VPN>>VPN 配置 功能页面启用 VPN 上联端口，请将连接到骨干网络的端口设置为上联端口。
4	创建 VLAN 映射条目	必选操作。在 VLAN>>VLAN VPN>>VLAN 映射 功能页面中根据实际应用情况设置 VLAN 映射条目。
5	创建 SP VLAN	可选操作。在 VLAN>>802.1Q VLAN 功能中创建 SP VLAN，创建 VLAN 步骤请参考 802.1Q VLAN 。

VLAN 映射功能配置步骤:

步骤	操作	说明
1	创建 VLAN 映射条目	必选操作。在 VLAN>>VLAN VPN>>VLAN 映射 功能页面中根据实际应用情况设置 VLAN 映射条目。
2	设置 VLAN 映射使能端口	必选操作。在 VLAN>>VLAN VPN>>端口使能 功能页面中选择启用 VLAN 映射功能的端口。
3	创建 SP VLAN	可选操作。在 VLAN>>802.1Q VLAN 功能中创建 SP VLAN，创建 VLAN 步骤请参考 802.1Q VLAN 。

6.5 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,解决了上次设备 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,要求对各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 6-15示。

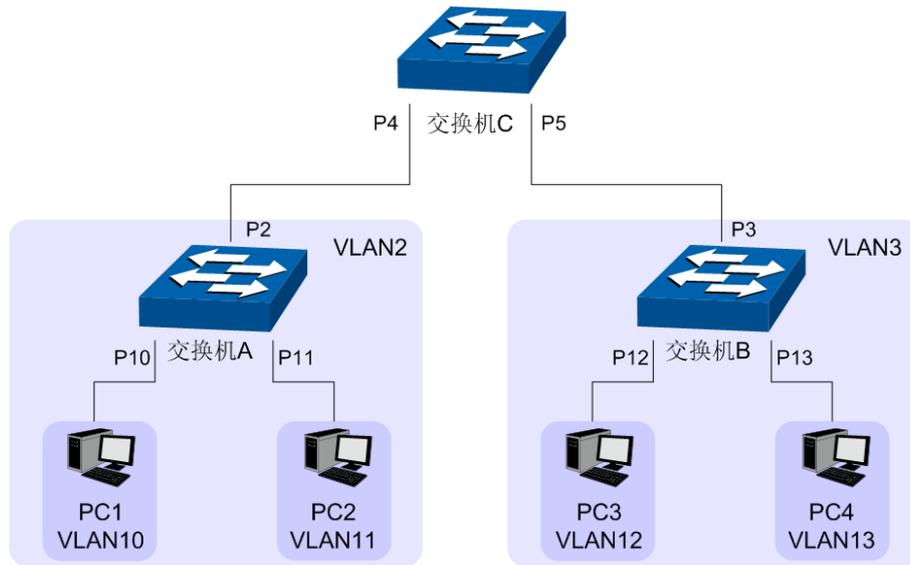


图 6-15 Private VLAN网络模型

如图所示，交换机A和交换机B分别运用Private VLAN功能，建立Secondary VLAN将各PC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。

Private VLAN功能主要有如下有点：

- （1） 解决上层设备 VLAN 资源短缺的问题。
- （2） 通过 MAC 地址复制技术，将 Secondary VLAN 与 Primary VLAN 中学习到的 MAC 地址自动复制到对方 VLAN 中，可有效抑制各 VLAN 中广播通信，从而节约带宽资源，增强网络安全性。

➤ 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，从而用户之间相互隔离。

根据 VLAN 特性，Primary VLAN 和 Secondary VLAN 之间也相互隔离，为了使数据在本层设备上能够正常转发，需要进一步制定严谨的端口数据处理规则以及 MAC 地址复制规则。在 Private VLAN 中有两种端口类型，Promiscuous 和 Host，详细定义和作用如下。

Promiscuous: 上行端口，和上层设备相连，负责和上层设备通信。所有添加到 Private VLAN 中的 Promiscuous 端口，将同步到 Primary VLAN 和 Secondary VLAN 中成为 VLAN 成员端口。为了向上层设备屏蔽 Secondary VLAN 的信息，Promiscuous 端口的出口规则默认为 UNTAG，可修改。当 Promiscuous 端口用于设备间的级联时，就需要把端口出口规则改为 tag。Promiscuous 端口只能作为一个 Primary VLAN 的上行端口，其 PVID 为 Primary VLAN ID，学习到的 MAC 地址将复制到其关联的所有 Secondary VLAN 中。

Host: 下行端口, 和下层设备相连, 负责和下行设备通信。所有添加到 Private VLAN 中的 Host 端口, 将同步到 Primary VLAN 和 Secondary VLAN 中成为 VLAN 成员端口。为了向下层设备屏蔽 Primary VLAN 的信息, Host 端口的出口规则为 UNTAG。Host 端口只能加入一个 Secondary VLAN, 其 PVID 为 Secondary VLAN ID, 学习到的 MAC 地址将复制到关联的 Primary VLAN 中。

如图 6-15 所示, 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 VLAN 10, 下面格式同此处) 和 Private VLAN 2/11。
- (2) 交换机 A 的端口 10 和端口 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 2 作为 Promiscuous 类型端口连接上层设备, 通过 Primary VLAN 2 向上层设备屏蔽本交换机上的 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 10 和端口 11 同时成为 Primary VLAN 2 的成员端口, 端口出口规则为 UNTAG, 端口 PVID 为各自所属的 Secondary VLAN; 端口 2 连接上层设备, 同时也同步到 Secondary VLAN 中成为 VLAN 成员端口, 出口规则为 UNTAG, PVID 为 Primary VLAN ID。
- (4) 交换机 A 内部执行 MAC 地址复制机制, 解决了传统 VLAN 中常见的广播问题, 以下两个表格是 MAC 地址复制前后的地址表内容。

序号	目的 MAC	VLAN	出端口
1	PC1	10	10
2	PC2	11	11
3	交换机 C	2	2

表 6-4 MAC 地址复制前的地址表

序号	目的 MAC	VLAN	出端口
1	PC1	10	10
2	PC1	2	10
3	PC2	11	11
4	PC2	2	11
5	交换机 C	2	2
6	交换机 C	10	2
7	交换机 C	11	2

表 6-5 MAC 地址复制后的地址表

由上表可知, 在 Primary VLAN 和 Secondary VLAN 中学习到的 MAC 地址相互复制, 大量消除了 VLAN 中因目的 MAC 地址未知而产生的广播问题。

本功能配置简单, 包括 **PVLAN 配置**和**端口配置**两个配置页面。

6.5.1 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**

The screenshot displays the PVLAN configuration interface. It is divided into three main sections:

- Private VLAN 创建 (Private VLAN Creation):** Contains two input fields: 'Primary VLAN:' with a range constraint '(2-4094)' and 'Secondary VLAN:' with a format constraint '(格式:2,4-5,8)'. A '添加' (Add) button is located to the right.
- 查找条目 (Search Items):** Features a '查找选项:' (Search Options) dropdown menu set to '全部' (All), a search input field, and a '查找' (Search) button.
- Private VLAN 列表 (Private VLAN List):** A table with the following structure:

选择	Primary VLAN	Secondary VLAN	端口成员
<input type="checkbox"/>			
<input type="checkbox"/>	2	10	

 Below the table are '删除' (Delete) and '帮助' (Help) buttons.

At the bottom of the interface, it shows '当前Private VLAN总数:1' (Current Private VLAN total: 1) and a '注意:' (Note) section stating: '为避免响应时间过长，建议每次创建Private VLAN数少于10个。' (To avoid long response times, it is recommended to create fewer than 10 Private VLANs at a time.)

图 6-16 PVLAN 配置

条目介绍:

➤ Private VLAN 创建

Primary VLAN: 填写 Primary VLAN ID。一个 Primary VLAN 可以和多个 Secondary VLAN 关联组成多个 Private VLAN。

Secondary VLAN: 填写 Secondary VLAN ID。一个 Secondary VLAN 中只能和一个 Primary VLAN 关联，即加入一个 Private VLAN。

➤ 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。

端口成员: 显示 Private VLAN 的成员端口。当在 Private VLAN 列表区中修改 Private VLAN 参数时，其原有的成员端口参数将失效，请重新配置。



注意:

在创建 Private VLAN 时, 交换机可能会产生大量的地址复制, 为了避免交换机响应时间过长, 建议每次创建的 Private VLAN 数少于 10 个。

6.5.2 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**

端口配置

端口: ▼

端口类型: ▼ 添加

Primary VLAN: (2-4094) 帮助

Secondary VLAN: (2-4094)

Private VLAN 端口列表		
端口号	端口类型	操作
3	Promiscuous	移除
8	Host	移除

图 6-17 端口配置

条目介绍:

➤ 端口配置

端口: 选择需配置的端口号。

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:

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他 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，根据端口的对端设备属性将端口添加到 Private VLAN 中。

6.6 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。当该定时器超时时，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，当该定时器超时时，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 6-18 配置 GVRP



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。

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**

端口选择: 点击<选择>按键，可根据所输端口号快速查找相应条目。

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:

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:

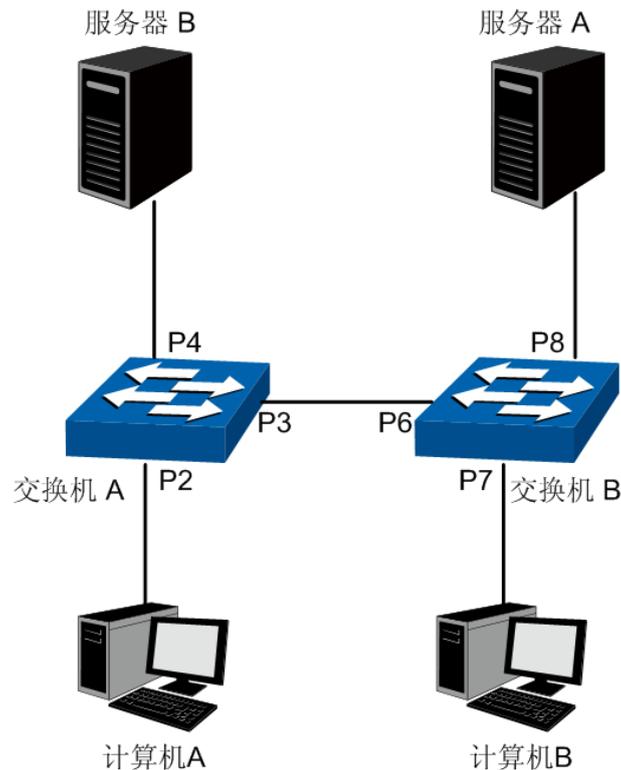
步骤	操作	说明
1	设置端口类型	必选操作。在 VLAN>>802.1Q VLAN>>端口配置 页面将端口类型设置为 TRUNK。
2	启用 GVRP 功能	必选操作。在 VLAN>>GVRP>>GVRP 配置 页面启用 GVRP 功能。
3	配置端口的注册模式以及各定时器时长。	必选操作。在 VLAN>>GVRP>>GVRP 配置 页面中根据实际情况设置端口的参数并启用端口。

6.7 802.1Q 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>按钮创建 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>按钮创建 VLAN，VLAN ID 为 20，并包含的端口 3 和端口 4。

● 配置交换机 B:

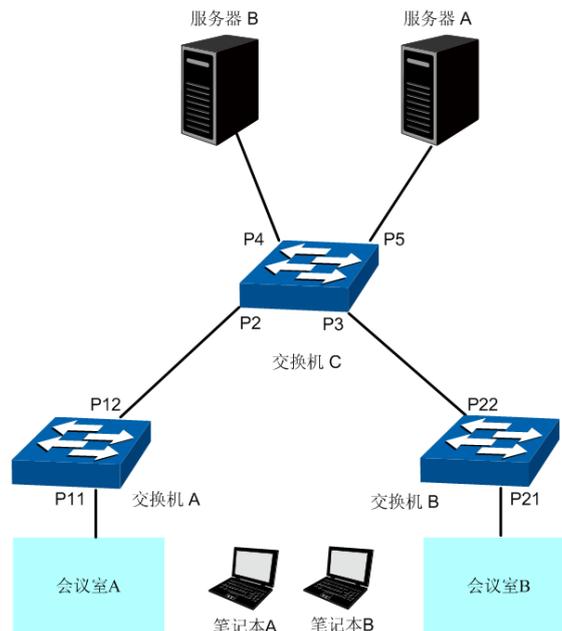
步骤	操作	说明
1	设置端口类型	必选操作。在 VLAN>>802.1Q VLAN>>端口配置 页面设置端口 7 的类型为 ACCESS；设置端口 6 的类型为 TRUNK；端口 8 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN，VLAN ID 为 10，并包含的端口 6 和端口 8。
3	创建 VLAN20	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN，VLAN ID 为 20，并包含的端口 6 和端口 7。

6.8 MAC VLAN 功能的组网应用

组网需求

- 交换机 A 和交换机 B 分别连接到两个会议室，会议室为各部门共用；
- 笔记本 A 和笔记本 B 为会议室专用电脑，分别属于不同部门；
- 两个部门分别属于 VLAN10 和 VLAN20。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部门的服务器，即服务器 A 和服务器 B；
- 笔记本 A 和笔记本 B 的 MAC 地址分别为 00-19-56-8A-4C-71、00-19-56-82-3B-70。

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 11 的端口类型为 GENERAL，端口 12 的端口类型为 TRUNK。
2	创建 VLAN10	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN，VLAN ID 为 10，包含的端口 11 和端口 12，端口 11 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN，VLAN ID 为 20，包含的端口 11 和端口 12，端口 11 的出口规则设置为 Untag。
4	设置 MAC VLAN 10	在 VLAN>>MAC VLAN 页面创建 MAC VLAN10，关联的 MAC 地址为 00-19-56-8A-4C-71。

步骤	操作	说明
5	设置 MAC VLAN 20	在 VLAN>>MAC VLAN 页面创建 MAC VLAN20, 关联的 MAC 地址为 00-19-56-82-3B-70。

- 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 21 的端口类型为 GENERAL, 端口 22 的端口类型为 TRUNK。
2	创建 VLAN10	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN, VLAN ID 为 10, 包含的端口 21 和端口 22, 端口 21 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN, VLAN ID 为 20, 包含的端口 21 和端口 22, 端口 21 的出口规则设置为 Untag。
4	设置 MAC VLAN 10	在 VLAN>>MAC VLAN 页面创建 MAC VLAN10, 关联的 MAC 地址为 00-19-56-8A-4C-71。
5	设置 MAC VLAN 20	在 VLAN>>MAC VLAN 页面创建 MAC VLAN20, 关联的 MAC 地址为 00-19-56-82-3B-70。

- 配置交换机 C:

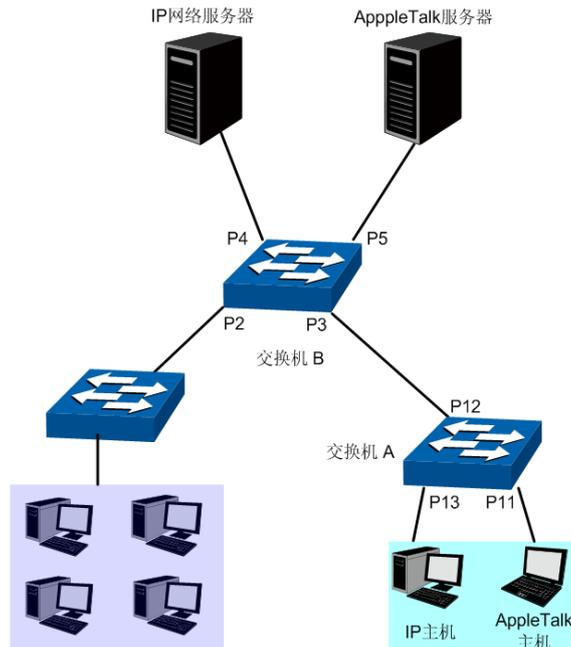
步骤	操作	说明
1	设置端口类型	必选操作。在 VLAN>>802.1Q VLAN>>端口配置 页面设置端口 2 和端口 3 的端口类型为 GENERAL, 端口 4 和端口 5 的端口类型为 ACCESS。
2	创建 VLAN10	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN, VLAN ID 为 10, 包含的端口 2、端口 3 和端口 5。
3	创建 VLAN20	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN, VLAN ID 为 20, 包含的端口 2、端口 3 和端口 4。

6.9 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 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



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 11 和端口 13 的端口类型为 ACCESS，端口 12 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>按钮创建 VLAN，VLAN ID 为 10，包含的端口 12 和端口 13，端口 12 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN，VLAN ID 为 20，包含的端口 11 和端口 12，端口 12 的出口规则设置为 Untag。

● 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 4 和端口 5 的端口类型为 ACCESS，端口 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>按钮创建 VLAN，VLAN ID 为 10，包含的端口 3 和端口 4，端口 3 的出口规则设置为 Tag。
3	创建 VLAN20	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 VLAN，VLAN ID 为 20，包含的端口 3 和端口 5，端口 3 的出口规则设置为 Tag。

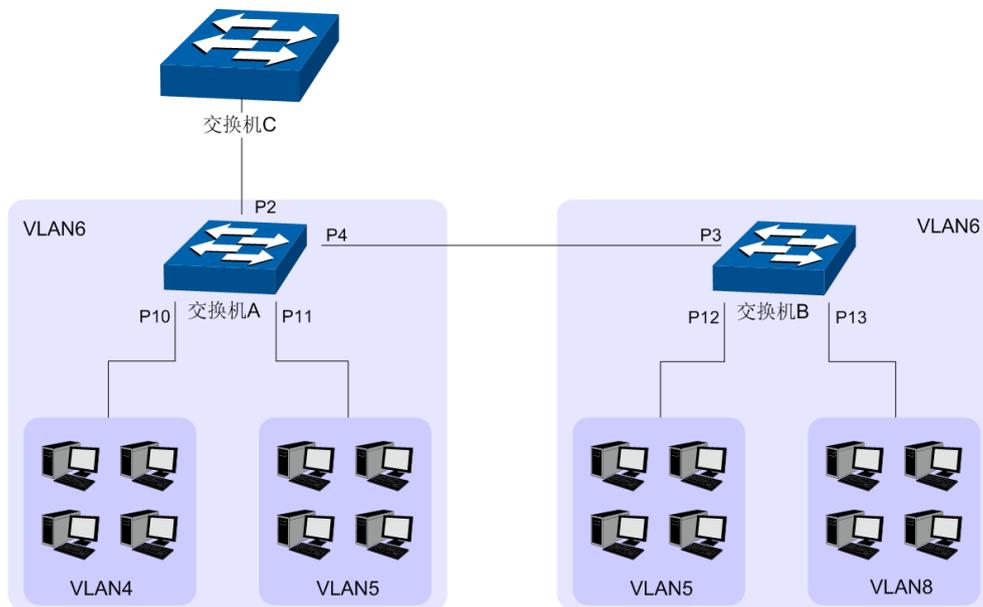
步骤	操作	说明
4	创建协议模板	必选操作。此处请根据实际情况在 VLAN>>协议 VLAN>>协议模板 页面配置协议模板。例如 IP 网络数据包以 Ethernet II 类型封装，Ether Type 字段为 0800；AppleTalk 网络数据包以 SNAP 类型封装，PID 字段为 809B。
5	设置协议 VLAN 10	在 VLAN>>协议 VLAN>>协议组列表 页面中点击<新建>按键来创建协议 VLAN10，关联 IP 协议，并勾选成员端口 3。
6	设置协议 VLAN 20	在 VLAN>>协议 VLAN>>协议组列表 页面中点击<新建>按键来创建协议 VLAN20，关联 AppleTalk 协议，并勾选成员端口 3。

6.10 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



图中的“P 数字”表示交换机的端口号。

配置步骤

- 配置交换机 A:

步骤	操作	说明
1	创建 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。

步骤	操作	说明
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 10 的端口类型为 Host 并添加到 Private VLAN 6/4 中；配置端口 11 的端口类型为 Host 并添加到 Private VLAN 6/5 中；配置端口 2 和端口 4 的端口类型为 Promiscuous 并添加到 Private VLAN 6/4 中。
3	配置端口出口规则	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面，编辑各 VLAN 端口的出口规则，P4 作为交换机之间的级联，要求在 Private VLAN 中的出口规则为 Tag。

- 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 12 的端口类型为 Host 并添加到 Private VLAN 6/5 中；配置端口 13 的端口类型为 Host 并添加到 Private VLAN 6/8 中；配置端口 3 的端口类型为 Promiscuous 并添加到 Private VLAN 6/5 中。
3	配置端口出口规则	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面，编辑各 VLAN 端口的出口规则，P3 作为交换机之间的级联，要求在 Private VLAN 中的出口规则为 Tag。

[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，由两字节的优先级和 6 字节 MAC 地址构成

Root path cost: 根路径开销

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

Port ID: 端口 ID，标识发出 BPDU 的端口

Message age: BPDU 生存时间

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

Hello time: 根桥发送 BPDU 的周期

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

➤ STP 的基本概念

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

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

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

根路径开销 (Root Path Cost): 一台交换机的根路径开销是根端口的路径开销与数据包经过的所有交换机的根路径开销之和。根桥的根路径开销是零。

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

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

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

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

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

生成树基本概念的组网示意图如图 7-1 所示。交换机 A、B、C 三者顺次相连，经 STP 计算过后，交换机 A 被选为根桥，端口 2 和端口 6 之间的线路被阻塞。

- 桥：交换机 A 为整个网络的根桥；交换机 B 是交换机 C 的指定桥。
- 端口：端口 3 和端口 5 分别为交换机 B 和交换机 C 的根端口；端口 1 和端口 4 分别为交换机 A 和交换机 B 的指定端口；端口 6 为交换机 C 的阻塞端口。

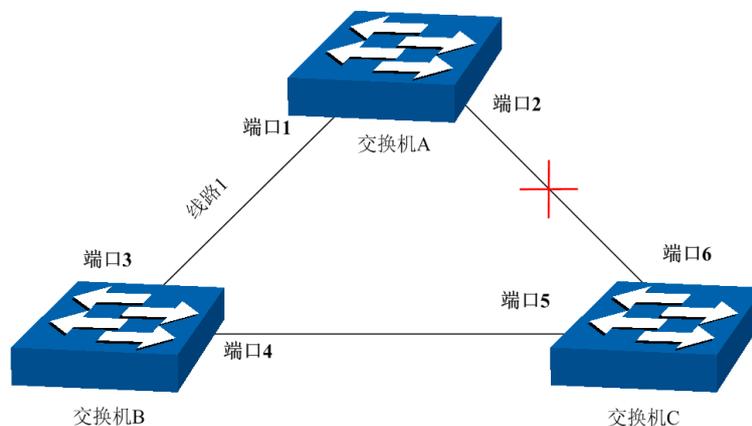


图 7-1 生成树基本概念组网图

➤ STP 定时器

联络时间 (Hello Time):

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

老化时间 (Max. Age):

数值范围从 6 秒到 40 秒。如果在超出老化时间之后，还没有收到根桥发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。

传输时延 (Forward Delay):

数值范围从 4 秒到 30 秒。是指交换机的端口状态迁移所用的时间。

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

➤ STP 模式的 BPDU 的优先级比较原则

假定有两条 BPDU X 和 Y，则：

如果 X 的根桥 ID 小于 Y 的根桥 ID，则 X 优于 Y；

如果 X 和 Y 的根桥 ID 相同，但 X 的根路径开销小于 Y，则 X 优于 Y；

如果 X 和 Y 的根桥 ID 和根路径开销相同，但 X 的桥 ID 小于 Y，则 X 优于 Y；

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

➤ STP 的计算过程

- 初始状态

每台交换机在初始时会生成以自己为根桥的 BPDU，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

- 最优 BPDU 的选择

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

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

表 7-1 最优 BPDU 的选择

- 根桥的选择

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

- 根端口、指定端口的选择

根端口、指定端口的选择过程如下表所述：

步骤	内容
1	非根桥交换机将接收到最优 BPDU 的那个端口指定为根端口。

步骤	内容
2	交换机根据根端口的 BPDUs 和根端口的路径开销,为其它端口计算一个端口 BPDUs: <ul style="list-style-type: none"> 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 BPDUs 和需要确定端口角色的端口上的 BPDUs 进行比较,并根据比较结果进行不同的处理: <ul style="list-style-type: none"> 如果计算出来的 BPDUs 优,则设备就将该端口定为指定端口,端口上的 BPDUs 被计算出来的 BPDUs 替换,并周期性向外发送。 如果端口上的 BPDUs 优,则设备不更新该端口 BPDUs 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 BPDUs 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, 它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, 它既可以快速收敛, 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。

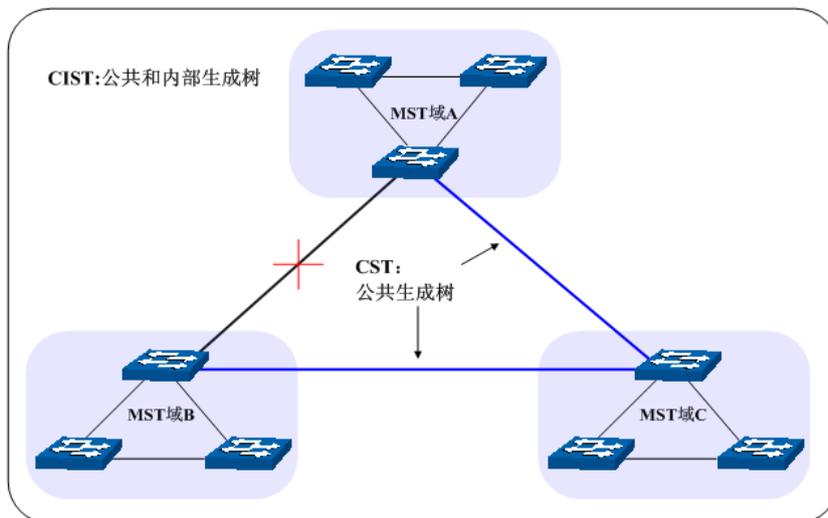


图 7-2 MSTP 基本概念组网图

➤ 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。

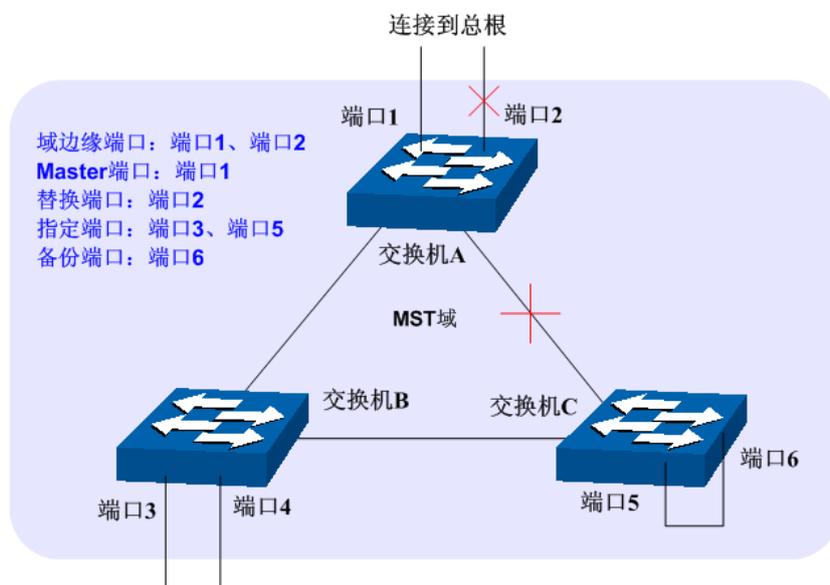


图 7-3 端口角色示意图

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

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

进入页面的方法：**生成树>>基本配置>>基本配置**

全局配置

生成树功能： 启用 禁用

生成树模式：

参数配置

CIST优先级： (0 - 61440, 4096为间隔)

联络时间： 秒 (1-10)

老化时间： 秒 (6-40)

传输时延： 秒 (4-30)

流量限制： pps (1-20)

最大跳数： 跳 (1-40)

图 7-4 基本配置

条目介绍：

➤ 全局配置

生成树功能： 选择是否启用交换机的生成树功能。

生成树模式： 选择交换机的生成树模式。

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

➤ 参数配置

CIST 优先级： 填写交换机的 CIST 优先级。CIST 优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。值越小，表示优先级越高。默认为 32768，且必须是 4096 的倍数。

联络时间： 填写交换机发送协议报文的周期，用于检测链路是否存在故障。并且， $2 \times (\text{联络时间} + 1) \leq \text{老化时间}$ 。默认为 2 秒。

老化时间： 填写协议报文在交换机中能够保存的最大生存期。默认为 20 秒。

- 传输时延：** 在网络拓扑改变后，交换机的端口状态迁移的延时时间。并且， $2 \times (\text{传输时延} - 1) \geq \text{老化时间}$ 。默认为 15 秒。
- 流量限制：** 填写在每个联络时间内，端口最多能够发送的协议报文的速度。默认为 5pps。
- 最大跳数：** 填写协议报文被转发的最大跳数，限制生成树的规模，默认 20 跳。

**注意：**

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

7.1.2 生成树信息

本页用来查看交换机生成树功能的相关参数。

进入页面的方法：[生成树](#)>>[基本配置](#)>>[生成树信息](#)

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

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

图 7-5 基本信息

7.2 端口配置

本页用来配置交换机端口的 CIST 参数。

进入页面的方法：生成树>>端口配置

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

注意：

将路径开销设置为0，即可根据端口连接速率自动设置路径开销。

图 7-6 端口配置

条目介绍：

> 端口配置

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

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

**注意:**

- 对于直接与终端相连的端口，请将该端口设置为边缘端口，同时启动 BPDU 保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。
- 对于属于汇聚组的端口，所有端口都可以被配置成与点对点链路相连。
- 当端口被设置为与点对点链路相连，则该端口所在的所有生成树实例均被设置为与点对点链路相连。如果端口实际物理链路不是点对点链路，而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。可以按需要将 VLAN 分配至不同的实例，每个实例就是一个“VLAN 组”，不受其它实例和公共生成树的影响。

进入页面的方法：生成树>>MSTP 实例>>实例配置

选择	实例ID	状态	优先级	VLAN ID	操作
<input type="checkbox"/>					
<input type="checkbox"/>	1	禁用	32768		删除映射
<input type="checkbox"/>	2	禁用	32768		删除映射
<input type="checkbox"/>	3	禁用	32768		删除映射
<input type="checkbox"/>	4	禁用	32768		删除映射
<input type="checkbox"/>	5	禁用	32768		删除映射
<input type="checkbox"/>	6	禁用	32768		删除映射
<input type="checkbox"/>	7	禁用	32768		删除映射
<input type="checkbox"/>	8	禁用	32768		删除映射
	CIST	启用	32768	1-4094,	

注意：

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

图 7-8 实例配置

条目介绍:

➤ **实例配置**

- 实例 ID 选择:** 点击<选择>按键, 可根据所输 ID 号, 快速选择相应实例。
- 选择:** 勾选条目配置实例状态及优先级, 可多选。
- 实例 ID:** 显示交换机的实例 ID 号。
- 状态:** 显示是否启用了相应实例。
- 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。

➤ **VLAN-实例映射**

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



注意:

当 GVRP 和 MSTP 同时启用时, GVRP 报文将沿着生成树实例 CIST 进行传播。因此如果希望通过 GVRP 在网络中发布某个 VLAN, 则需在配置 MSTP 的“VLAN-实例映射”时保证把这个 VLAN 映射到 CIST 上。关于 GVRP 的相关介绍请参见 [6.5 GVRP](#)。

7.3.3 实例端口

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

进入页面的方法：生成树>>MSTP 实例>>实例端口

实例端口配置

实例ID 端口

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

注意：

将路径开销设置为0，即可根据端口连接速率自动设置路径开销。

图 7-9 实例端口

条目介绍：

➤ 实例端口配置

- 实例 ID：** 选择需要配置端口属性的实例 ID。
- 端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：** 勾选端口配置端口的优先级和路径开销，可多选。
- 端口：** 显示交换机的端口号。
- 优先级：** 在对应实例 ID 中，确定与该端口连接的端口是否会被选为根端口的重要依据。默认为 128，范围 0-240，且为 16 的倍数。
- 路径开销：** 在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。
- 端口角色：** 显示端口在生成树实例中担任的角色。
- 端口状态：** 显示端口所处的工作状态。
- LAG：** 显示端口当前所属的汇聚组。



注意：

同一端口在不同的生成树实例中的端口状态可以不同。

安全树功能全局配置步骤：

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

7.4 安全配置

通过配置设备的保护功能，来防止生成树网络中的设备遭受各种形式的恶意攻击。本功能包括端口保护和 TC 保护两个配置页面。

7.4.1 端口保护

> 环路保护：

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

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

> 根桥保护：

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

为了防止这种情况发生，MSTP 提供根桥保护功能：对于启用了根桥保护功能的端口，它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相应的保护功能。

进入页面的方法：生成树>>安全配置>>端口保护

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

图 7-10 端口保护

条目介绍:

➤ 端口保护

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

7.4.2 TC 保护

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

进入页面的方法: 生成树>>安全配置>>TC 保护

TC保护

TC保护阈值: 数据包 (1 - 100)

TC保护周期: 秒 (1 - 10)

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。

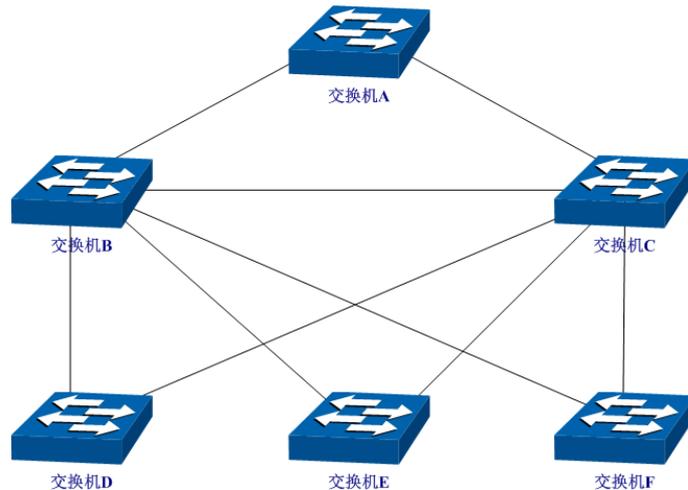
7.5 STP 功能的组网应用

➤ 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。
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。

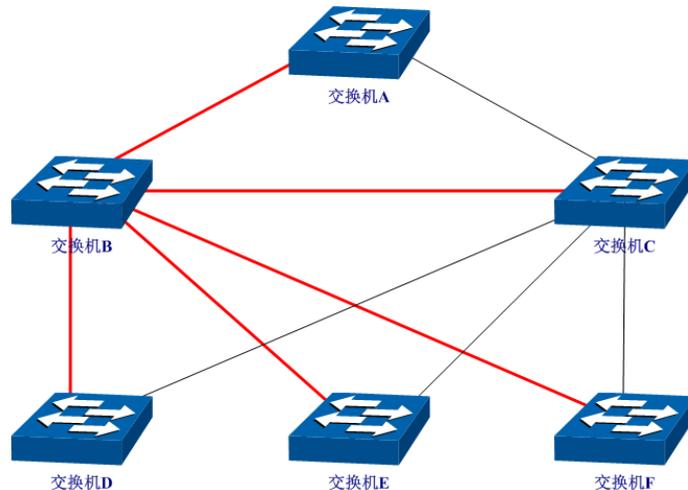
- 配置交换机 C

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。

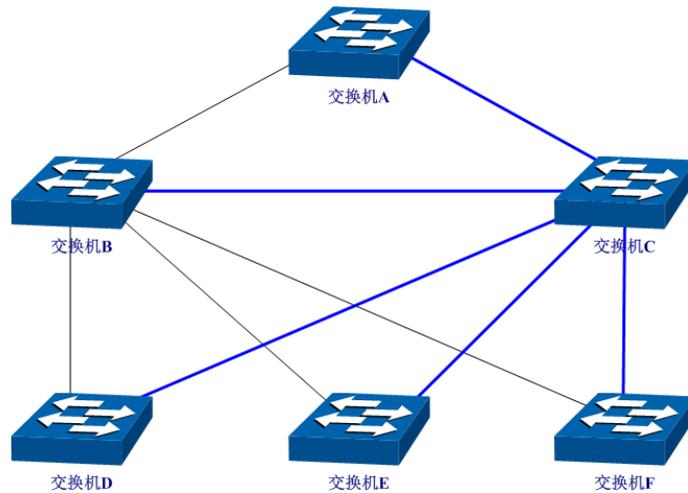
● 配置交换机 D

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。
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 以太网 OAM

➤ OAM 概述

以太网最初为局域网而设计，由于局域网规模较小，且本身已经具备较高的可靠性和稳定性，所以以太网在设计之初并未建立管理维护的机制。而近年来，随着千兆、万兆以太网技术的相继应用，网络运营商、设备制造商和标准化组织致力于将以太网技术向城域网和广域网推进。和局域网相比，城域网和广域网在链路长度和网络规模上都在迅速扩大。因此，缺乏有效的管理维护机制已成为以太网技术在城域网和广域网中应用的严重障碍。基于这种情况，在以太网上实现 OAM（Operations, Administration and Maintenance，操作、管理和维护）机制已成为必然的发展趋势。

以太网 OAM 是一种监控网络故障的工具，用于监控和解决以太网接入“最后一公里”中常见的链路问题。用户通过在两个点到点连接的设备上启用以太网 OAM 功能，可以监控这两台设备之间的链路状态，并及时上报链路故障信息，使得网络管理员能够更有效地管理网络，保障网络的稳定运行。

以太网 OAM 能够有效提高以太网的管理和维护能力。其功能包括：

1. 链路性能监测：对链路的各种性能进行监测，包括对丢包、时延和抖动等的衡量，以及对各类流量的统计。
2. 故障侦测和告警：通过发送检测报文来探测链路的连通性，当链路出现故障时及时通知网络管理员。
3. 环路测试：通过非 OAMPDU 报文的环回来检测链路故障。

➤ 以太网 OAM 协议报文

以太网 OAM 工作在数据链路层，其协议报文被称为 OAMPDU（OAM Protocol Data Units，OAM 协议数据单元）。OAMPDU 报文共有六种，常用的主要有这几种类型：Information OAMPDU（信息 OAMPDU）、Event Notification OAMPDU（事件通知 OAMPDU）和 Loopback Control OAMPDU（环回控制 OAMPDU）。

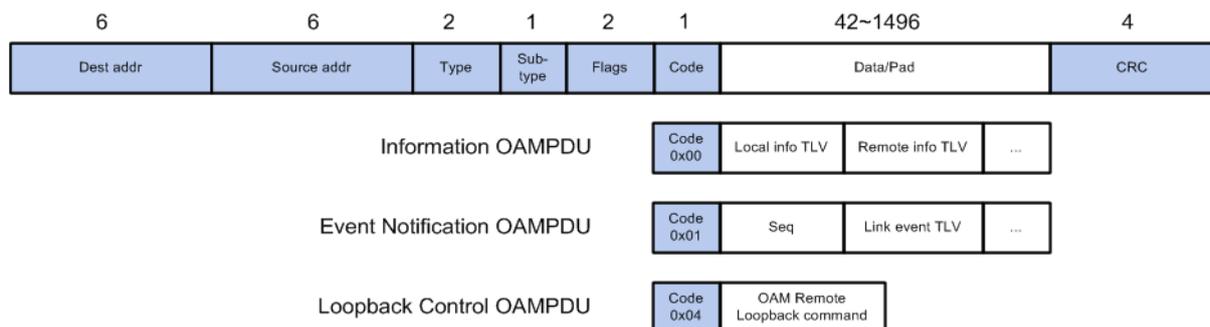


图 8-1 OAMPDU 报文

OAMPDU 是标准长度的以太网报文，长度为 64-1518 个字节且不带 tag。图 8-1 所示是几种常见的 OAMPDU 的报文格式，各重要字段的含义如下表所示。

字段	含义
Dest addr	OAMPDU 报文的目的地 MAC 地址，为慢速协议组播地址：0x0180-C200-0002。

字段	含义
Source addr	OAMPDU 报文的源 MAC 地址，为发送端口的 MAC 地址。
Type	协议类型，值为0x8809。
Subtype	协议子类型，值为 0x03。
Flags	Flag 域，包含了以太网 OAM 实体的状态信息。
Code	OAMPDU 报文的类型。Information OAMPDU、Event Notification OAMPDU 和 Loopback Control OAMPDU 在该字段的值分别为：0x00、0x01 和 0x04。

表 8-1 OAMPDU 报文字段

常用的三种 OAMPDU 报文如下表所示：

报文类型	中文含义	作用
Information OAMPDU	信息 OAMPDU 报文	用于将 OAM 实体的状态信息（包括本地信息、远端信息和自定义信息）发给远端 OAM 实体，以维持以太网 OAM 连接。
Event Notification OAMPDU	事件通知 OAMPDU 报文	一般用于链路监控，对连接本端和远端 OAM 实体的链路上所发生的故障进行告警。
Loopback Control OAMPDU	环回控制 OAMPDU 报文	主要用于远端环回控制，即控制远端设备的 OAM 环回状态。该报文中带有使能或关闭环回功能的信息，远端设备可根据该信息开启或关闭远端环回功能。

表 8-2 OAMPDU 报文类型

➤ OAM 功能

根据 IEEE 802.3 标准的第 57 章规定，OAM 功能包括：建立连接，链路监控，远端故障指示，远端环回。

▪ 建立连接

以太网 OAM 连接的建立过程被称为 Discovery 阶段。在该阶段，本端 OAM 实体和远端 OAM 实体通过 Information OAMPDU 报文建立起稳定的连接。

以太网 OAM 有两种连接模式：主动模式和被动模式。以太网 OAM 连接只能由主动模式的 OAM 实体发起，而被动模式的 OAM 实体只能等待并响应远端 OAM 实体的连接请求。互连的 OAM 实体通过 Information OAMPDU 报文相互通报各自的 OAM 配置信息和本地节点是否支持 OAM 来确定是否可以建立 OAM 连接。只有当两端 OAM 实体对环回功能，链路监控和链路事件等配置信息检查通过后，OAM 连接才能够建立。

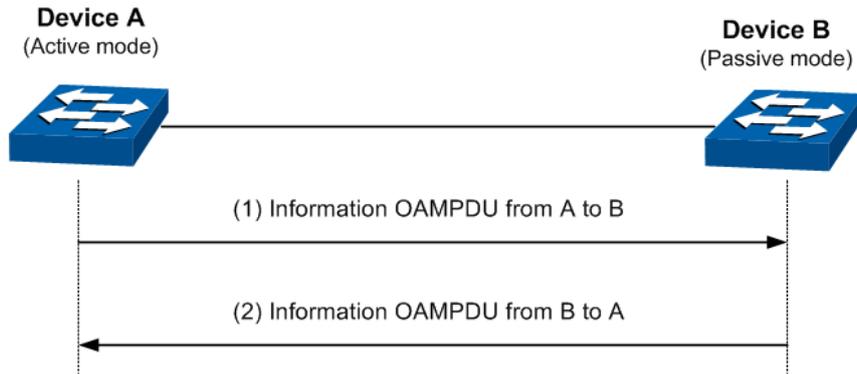


图 8-2 OAM 发现过程

主动模式和被动模式的区别如下表所示：

处理能力	主动模式	被动模式
初始化以太网 OAM Discovery 阶段	可以	不可以
对以太网 OAM Discovery 阶段初始化过程响应	可以	可以
发送 Information OAMPDU 报文	可以	可以
发送 Event Notification OAMPDU 报文	可以	可以
发送不带 TLV 的 Information OAMPDU 报文	可以	可以
发送 Loopback Control OAMPDU 报文	可以	不可以
响应 Loopback Control OAMPDU 报文	可以（需远端也为主动模式）	可以
发送自定义 OAMPDU 报文	可以	可以

表 8-3 主动模式和被动模式区别

OAM 建立连接后，两端的 OAM 实体会周期性地发送 Information OAMPDU 报文来检测连接是否正常。若一端 OAM 实体超过 5 秒未收到远端实体发送的 Information OAMPDU 报文，则视为 OAM 连接中断。

▪ 链路监控

链路监控用于检测和发现各种环境下的链路错误。当一端 OAM 实体监控到一般链路事件时，将向其远端发送 Event Notification OAMPDU 报文以进行通报。这样，管理员可以通过观察日志信息动态地了解链路状态，对相应的错误进行及时处理。一般链路事件如下表所示。

事件类型	描述
错误信号周期事件（Symbol Period Error）	单位时间内的错误信号数量超过定义的阈值
错误帧事件（Frame Error）	单位时间内的错误帧数量超过定义的阈值

事件类型	描述
错误帧周期事件 (Frame Period Error)	指定数目的接收帧中错误帧数量超过定义的阈值
错误帧秒数事件 (Frame Seconds Error)	指定时间内出现错误帧的秒数超过了定义的阈值

表 8-4 一般链路事件

▪ 远端故障检测

以太网的故障检测非常困难，特别是在网络物理通信仍然正常而网络性能缓慢下降的情况下。当设备发生故障或不可用导致流量中断时，故障端 OAM 实体会通过 Information OAMPDU 报文中的 Flag 域将故障信息通知给远端 OAM 实体。故障情况有以下几种：

- 链路故障：远端链路信号丢失。此情况下 Information OAMPDU 报文每秒发送一次。
- 致命故障：不可预知状态发生，如电源中断。此情况下 Information OAMPDU 报文不间断发送。
- 紧急事件：不能确定的紧急事件发生。此情况下 Information OAMPDU 报文不间断发送。

▪ 远端环回

远端环回功能可以用于检测链路质量和定位链路故障。以太网 OAM 连接建立后，主动模式 OAM 实体可以通过向远端 OAM 实体发送带有使能信息的环回控制 OAMPDU 报文，使远端 OAM 实体进入远端环回状态。

远端环回功能开启后，主动模式 OAM 实体向远端发送远端环回请求，在远端环回模式下，远端实体会将接收到的除 OAMPDU 以外的报文按原路发回给主动模式 OAM 实体。网络管理人员可以通过返回报文测试链路的延时、抖动和帧丢失等性能。

远端环回的测试过程如下图所示：

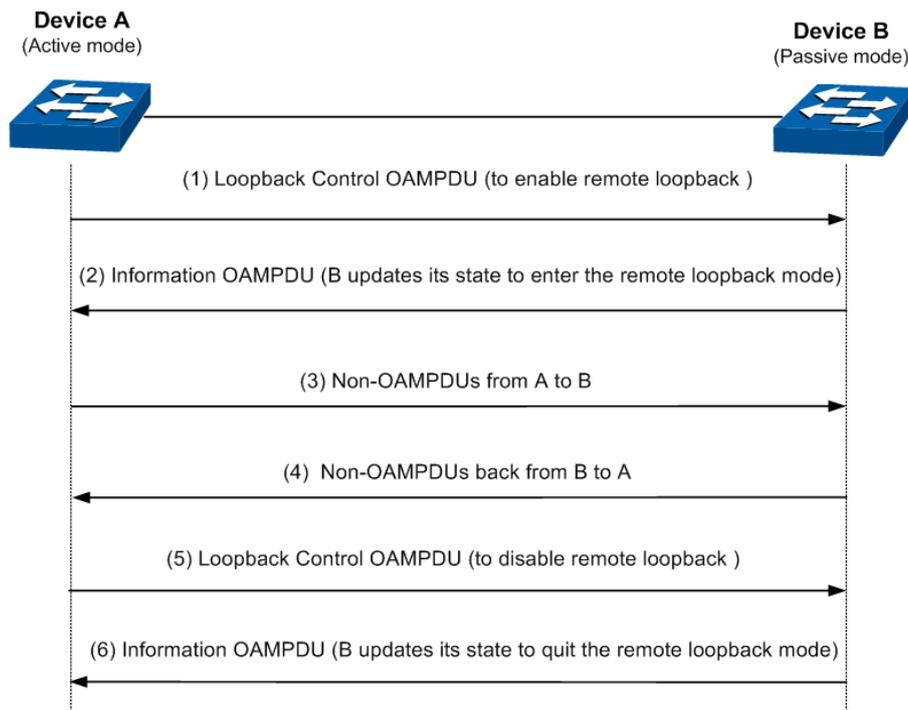


图 8-3 远端环回

8.1 基本配置

基本配置页面功能包括开启交换机特定端口的 OAM 功能和设置 OAM 模式。在 Discovery 信息页面可查看连接状态。

8.1.1 基本配置

进入页面的方法：以太网 OAM>>基本配置>>基本配置

基本配置			
选择	端口	模式	状态
<input type="checkbox"/>		<input type="text" value=""/> ▾	<input type="text" value=""/> ▾
<input type="checkbox"/>	1	主动	禁用
<input type="checkbox"/>	2	主动	禁用
<input type="checkbox"/>	3	主动	禁用
<input type="checkbox"/>	4	主动	禁用
<input type="checkbox"/>	5	主动	禁用
<input type="checkbox"/>	6	主动	禁用
<input type="checkbox"/>	7	主动	禁用
<input type="checkbox"/>	8	主动	禁用
<input type="checkbox"/>	9	主动	禁用
<input type="checkbox"/>	10	主动	禁用
<input type="checkbox"/>	11	主动	禁用
<input type="checkbox"/>	12	主动	禁用
<input type="checkbox"/>	13	主动	禁用
<input type="checkbox"/>	14	主动	禁用
<input type="checkbox"/>	15	主动	禁用

注意:

1、同处于被动模式下的两个OAM实体之间无法建立以太网OAM连接。

图 8-4 基本配置

条目介绍:

> 基本配置

- 端口选择:** 输入端口号后点击<选择>按钮,可以快速选择相应的端口。
- 选择:** 勾选端口进行配置,可多选。
- 端口:** 显示交换机的端口号。
- 模式:** 选择以太网 OAM 工作模式。
- 状态:** 选择是否启用以太网 OAM 功能。



注意:

同处于被动模式下的两个 OAM 实体之间无法建立以太网 OAM 连接。

8.1.2 Discovery 信息

进入页面的方法：以太网 OAM>>基本配置>>Discovery 信息

Discovery信息	
端口 <input type="text" value="1"/> <input type="button" value="选择"/>	
本端	
OAM	禁用
模式	主动
以太网OAM报文最大长度	1518 字节
远端环回	支持
单向链路	不支持
链路监控	支持
MIB变量获取	不支持
报文版本	0
运行状态	Disable
环回状态	No Loopback
远端	
模式	---
MAC地址	---
制造商 (OUI)	---
以太网OAM报文最大长度	---
远端环回	---
单向链路	---
链路监控	---
MIB变量获取	---
报文版本	---
制造商信息	---
<input type="button" value="刷新"/>	

图 8-5 Discovery 信息

条目介绍：

> 本端

- OAM:** 显示选定端口的 OAM 功能是否开启。
- 模式:** 显示选定端口的 OAM 模式。
- 以太网 OAM 报文最大长度:** 显示以太网 OAMPDU 报文的最大长度。
- 远端环回:** 显示本端是否支持远端环回功能。
- 单向链路:** 显示本端是否支持单项链路操作。
部分设备支持单向 OAM 操作，当链路单方向工作异常时，这些设备通过发送 OAMPDU 报文通知远端设备。

链路监控:	显示本端是否支持链路监控功能。
MIB 变量获取:	显示是否支持 MIB 变量获取。
报文版本:	显示报文版本。
运行状态:	显示运行状态。 <ul style="list-style-type: none"> ● Disable: 该端口未启用 OAM 功能。 ● LinkFault: 检测到链路故障且在发送通报该链路事件的 OAMPDU 报文。 ● PassiveWait: 端口处于被动模式且在等待确认远端设备是否支持 OAM。 ● ActiveSendLocal: 端口处于主动模式且在发送本端信息。 ● SendLocalAndRemote: 本端端口已发现远端设备, 但仍未对远端设备响应。 ● SendLocalAndRemoteOK: 本端实体已接受远端 OAM 实体的连接请求。 ● PeeringLocallyRejected: 本端实体拒绝了远端 OAM 实体的连接请求。 ● PeeringRemotelyRejected: 远端实体拒绝了本端 OAM 实体的连接请求。 ● NonOperHalfDuplex: 由于以太网 OAM 功能在设计上并不支持在半双工端口上完全正常工作。该值指示此端口启用了 OAM 功能, 但端口处于半双工状态。
环回状态:	显示环回状态。 <ul style="list-style-type: none"> ● No Loopback: 本端和远端 OAM 实体都未处于环回模式。 ● Local Loopback: 本端 OAM 实体处于环回模式。 ● Remote Loopback: 远端 OAM 实体处于环回模式。
➤ 远端	
模式:	显示远端实体的 OAM 模式。
MAC 地址:	显示远端实体的 MAC 地址。
制造商 (OUI):	显示远端实体的制造商 OUI。 OUI 地址是由 IEEE 分配给设备供应商的唯一标识符。
以太网 OAM 报文最大长度:	显示以太网 OAM 报文最大长度。
远端环回:	显示远端实体是否支持远端环回功能。
单向链路:	显示远端实体是否支持单项链路操作。
链路监控:	显示远端实体是否支持链路监控功能。
MIB 变量获取:	显示远端实体是否支持 MIB 变量获取。
报文版本:	显示 OAMPDU 报文的 TLV 版本。
制造商信息:	显示远端实体的制造商信息。

8.2 链路监控

在链路监控页面可以配置包括阈值和探测周期的 OAM 链路事件参数，也可选择是否启用链路事件通知。

进入页面的方法：以太网 OAM>>链路监控>>链路监控

选择	端口	检测阈值 (错误信号)	检测窗口 (100毫秒)	通知
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1	1	10	启用
<input type="checkbox"/>	2	1	10	启用
<input type="checkbox"/>	3	1	10	启用
<input type="checkbox"/>	4	1	10	启用
<input type="checkbox"/>	5	1	10	启用
<input type="checkbox"/>	6	1	10	启用
<input type="checkbox"/>	7	1	10	启用
<input type="checkbox"/>	8	1	10	启用
<input type="checkbox"/>	9	1	10	启用
<input type="checkbox"/>	10	1	10	启用
<input type="checkbox"/>	11	1	10	启用
<input type="checkbox"/>	12	1	10	启用
<input type="checkbox"/>	13	1	10	启用
<input type="checkbox"/>	14	1	10	启用
<input type="checkbox"/>	15	1	10	启用

图 8-6 链路监控配置

条目介绍：

➤ 链路监控配置

链路事件：

选择要进行监控的链路事件。

链路事件包括：信号周期错误，帧错误，帧周期错误和帧秒数错误。详情见[一般链路事件](#)。

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：

勾选端口进行配置，可多选。

端口：

显示交换机的端口号。

检测阈值：

输入触发链路事件的检测阈值。

- 对于错误信号周期事件，其值为设定时间内最多可以出现的错误信号数量。
- 对于错误帧事件，其值为100ms内最多可以出现的错误帧数量。
- 对于错误帧周期事件，其值为指定帧数的时间内最多可以出现的错误帧数
- 对于错误帧秒数事件，其值为设定时间内最多可以出现错误帧的秒数。

- 检测窗口:** 输入链路事件的检测窗口。
- 对于错误帧周期事件，窗口指定为接收到的帧数目。
 - 对于其他链路事件，窗口指定为一段时间间隔。

通知: 选择是否启用事件通知。

8.3 远端故障指示

在本配置页面，可以选择是否启用致命故障通知和紧急事件通知。

进入页面的方法：以太网 OAM>>远端故障指示>>远端故障指示

选择	端口	致命故障通知	紧急事件通知
<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	1	启用	启用
<input type="checkbox"/>	2	启用	启用
<input type="checkbox"/>	3	启用	启用
<input type="checkbox"/>	4	启用	启用
<input type="checkbox"/>	5	启用	启用
<input type="checkbox"/>	6	启用	启用
<input type="checkbox"/>	7	启用	启用
<input type="checkbox"/>	8	启用	启用
<input type="checkbox"/>	9	启用	启用
<input type="checkbox"/>	10	启用	启用
<input type="checkbox"/>	11	启用	启用
<input type="checkbox"/>	12	启用	启用
<input type="checkbox"/>	13	启用	启用
<input type="checkbox"/>	14	启用	启用
<input type="checkbox"/>	15	启用	启用

图 8-7 远端故障指示

条目介绍:

> 远端故障指示配置

- 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:** 勾选端口进行配置，可多选。
- 端口:** 显示交换机的端口号
- 致命故障通知:** 选择是否启用致命故障通知。
- 紧急事件通知:** 选择是否启用紧急事件通知。

8.4 远端环回

如果本端开启了 OAM 主动模式并建立了 OAM 连接，在本配置页面可以选择启用远端环回功能，也可选择忽略或处理收到的远端环回请求。

进入页面的方法：以太网 OAM>>远端环回>>远端环回

远端环回配置

端口

选择	端口	收到远端环回请求	远端环回
<input type="checkbox"/>		<input type="text"/> ▼	<input type="text"/> ▼
<input type="checkbox"/>	1	忽略	---
<input type="checkbox"/>	2	忽略	---
<input type="checkbox"/>	3	忽略	---
<input type="checkbox"/>	4	忽略	---
<input type="checkbox"/>	5	忽略	---
<input type="checkbox"/>	6	忽略	---
<input type="checkbox"/>	7	忽略	---
<input type="checkbox"/>	8	忽略	---
<input type="checkbox"/>	9	忽略	---
<input type="checkbox"/>	10	忽略	---
<input type="checkbox"/>	11	忽略	---
<input type="checkbox"/>	12	忽略	---
<input type="checkbox"/>	13	忽略	---
<input type="checkbox"/>	14	忽略	---
<input type="checkbox"/>	15	忽略	---

注意:

- 1、只有在以太网OAM连接建立完成后才能进行远端环回操作。
- 2、远端环回主要用于测试单条链路，汇聚端口并不支持该功能。

图 8-8 远端环回配置

条目介绍:

➤ 远端故障指示配置

- 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:** 勾选端口进行配置，可多选。
- 端口:** 显示交换机的端口号
- 收到远端环回请求:** 选择忽略或者处理收到的远端环回请求。
- 远端环回:** 选择开始或者停止远端环回功能。

8.5 统计信息

统计信息用于显示指定端口的以太网 OAM 的详细流量统计信息和事件日志信息。

8.5.1 统计信息

本配置页面显示了指定端口的以太网 OAM 的详细流量统计信息。点击<刷新>或设备重启后，统计信息会清零并重新开始统计。

进入页面的方法：以太网 OAM>>统计信息>>统计信息

统计信息		
	发送	接收
信息 OAMPDU	0	0
Unique 事件通知 OAMPDU	0	0
Duplicate 事件通知 OAMPDU	0	0
MIB 变量请求 OAMPDU	0	0
MIB 变量回应 OAMPDU	0	0
环回控制 OAMPDU	0	0
组织自定义 OAMPDU	0	0
未支持 OAMPDU	0	0
OAM 导致的帧丢失	0	0

端口

图 8-9 统计信息

条目介绍：

➤ 统计信息

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。
发送：	显示发送 OAMPDU 报文的数目。
接收：	显示接收 OAMPDU 报文的数目。
信息 OAMPDU：	显示接收、发送信息 OAMPDU 报文的数目。
Unique 事件通知 OAMPDU：	显示接收、发送 Unique 事件通知 OAMPDU 报文的数目。
Duplicate 事件通知 OAMPDU：	显示接收、发送 Duplicate 事件通知 OAMPDU 报文的数目。
MIB 变量请求 OAMPDU	显示接收、发送 MIB 变量请求 OAMPDU 报文的数目。
MIB 变量回应 OAMPDU	显示接收、发送 MIB 变量回应 OAMPDU 的数目。
环回控制 OAMPDU	显示接收、发送环回控制 OAMPDU 报文的数目。
组织自定义 OAMPDU	显示接收、发送组织自定义 OAMPDU 报文的数目。
未支持 OAMPDU	显示接收、发送未支持 OAMPDU 报文的数目。
OAM 导致的帧丢失	显示由于 OAM 子层内部发送错误导致帧丢失的数目。

8.5.2 事件日志

本配置页面显示了指定端口的以太网 OAM 的事件日志统计信息。点击<刷新>或设备重启后，统计信息会清零并重新开始统计。

进入页面的方法：以太网 OAM>>统计信息>>事件日志

事件日志统计信息		
	端口 <input type="text" value="1"/> <input type="button" value="选择"/>	
	本端	远端
错误信号周期事件	0	0
错误帧事件	0	0
错误帧周期事件	0	0
错误帧秒数事件	0	0
致命故障	0	0
紧急事件	0	0

事件日志列表						
类型	位置	时间	检测值	检测窗口	检测阈值	累计错误数目
<input type="button" value="刷新"/> <input type="button" value="清空"/> <input type="button" value="帮助"/>						

图 8-10 事件日志

条目介绍：

➤ 事件日志统计信息

- 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。
- 本端：** 显示发生在本端的链路事件数目。
- 远端：** 显示发生在远端的链路事件数目。
- 错误信号周期事件：** 显示发生在本端、远端的错误信号周期事件数目。
- 错误帧事件：** 显示发生在本端、远端的错误帧事件数目。
- 错误帧周期事件：** 显示发生在本端、远端的错误帧周期事件数目。
- 错误帧秒数事件：** 显示发生在本端、远端的错误帧秒数事件数目。
- 致命故障：** 显示发生在本端、远端的致命故障数目。

➤ 事件日志列表

- 类型：** 显示链路事件的类型。
- 位置：** 显示链路事件发生的位置。
- 时间：** 显示链路事件发生的时间。
- 检测值：** 显示在检测窗口期间检测到的错误数目。
- 检测窗口：** 显示链路事件的检测窗口。
- 检测阈值：** 显示链路事件的检测阈值。
- 累计错误数目：** 显示自从 OAM 子层重置之后累计检测到的错误数目。

8.6 DLDP

DLDP(Device Link Detection Protocol, 设备链路检测协议)是一个链路层协议，可以用来监控光纤或双绞线的链路状态，并检测设备之间是否存在单向链路。当两个设备之间存在了单向链路时，本端设备可以通过链路层收到对端设备发送的报文，但对端设备不能收到本端设备的报文。单向链路会引发一系列问题，如生成树拓扑环路等。一旦设备检测到单向链路，DLDP 可以根据用户配置，

自动关闭或通知用户手动关闭相关端口，以防止网络问题的发生。

➤ **DLDP 处理机制**

1. DLDP 状态

DLDP 协议定义了六种链路状态，如下表所示：

状态	说明
Initial (初始)	DLDP 未使能。
Inactive (非活动)	DLDP 已使能，但链路状态为 down
Active (活动)	这种状态是暂时的，它表明： 1. DLDP 已使能且链路 up。 2. 邻居表项为空。
Advertisement (通告)	该状态表明未发现单向链路，包括下面两种情况： 1. 与所有邻居建立了双向连通。 2. DLDP 处于 Active 状态超过 5 秒。
Probe (探测)	收到一个未知邻居的报文后进入的状态，此时将发送探测报文检测链路是否为单向链路。
Disable (单通)	该状态表明检测到单向链路。

表 8-5 DLDP 协议状态

2. DLDP 工作流程

DLDP 一般的工作流程如下图所示：

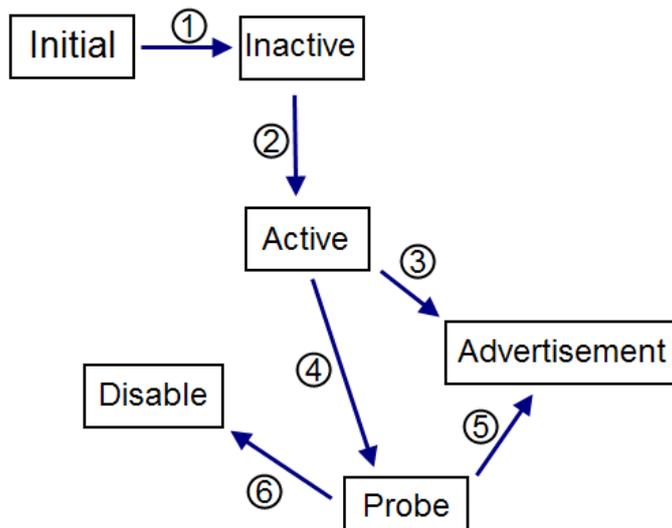


图 8-11 DLDP 流程

DLDP 流程如下所示

①：当 DLDP 在 down 状态链路下使能，DLDP 状态将跳转到 Inactive。

②：当已使能的 DLDP 链路为 up，DLDP 状态将跳转到 Active。该状态下本端设备将会向远端设备发送带有 RSY 标记的 Advertisement 报文。

③：若设备在 5 秒内未收到任何 DLDP 报文，DLDP 状态将跳转到 Advertisement。

④：设备收到未知邻居报文后，DLDP 状态将由 Active 跳转到 Probe，并发送一些探测报文以检测链路状态。

⑤：若设备接收到远端设备的 Echo 报文，它们之间的链路状态将被标记为是双向的，DLDP 状态也将由 Probe 跳转到 Advertisement。处于 Advertisement 的设备将发送 Advertisement 报文。

⑥：若设备在设定的周期内未收到 Echo 报文，链路状态将被标记为是单向的，DLDP 状态也将由 Probe 跳转到 Disable。端口将会根据用户设置自动关闭或由用户手动关闭。

典型的双向链路检测流程为 ②→④→⑤，典型的单向链路检测流程为 ②→④→⑥。

在 DLDP 页面，可以设置 DLDP 状态并配置通告间隔、端口关闭模式、网页刷新状态和网页自动刷新间隔等功能。

进入页面的方法：以太网 OAM>>DLDP>>DLDP

全局配置

DLDP状态: 启用 禁用

通告间隔: 秒 (1-30)

关闭模式:

网页刷新状态: 启用 禁用

网页自动刷新间隔: 秒 (1-100)

端口配置

端口

选择	端口	DLDP状态	协议状态	链路状态	邻居状态
<input type="checkbox"/>		<input type="text" value="禁用"/>			
<input type="checkbox"/>	1	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	2	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	3	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	4	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	5	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	6	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	7	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	8	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	9	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	10	禁用	Initial	Link-Down	N/A

注意:

- 1、一个使能了DLDP的端口不能检测对端未使能DLDP端口的链路状态。
- 2、确保链路两边端口是相同的功能配置。

图 8-12 DLDP 配置

条目介绍:

➤ 全局配置

DLDP 状态: 开启或禁用 DLDP 全局功能。

- 通告间隔:** 设置 1-30 秒的通告间隔，默认为 5 秒。
- 关闭模式:** DLDP 采取自动模式或手动模式关闭检测到的单向链路，默认使用自动模式。
- **自动:** 在该模式下，DLDP 会生成日志和触发信息，并自动关闭检测到的单向链路，DLDP 状态也将跳转到 **Disable**。
 - **手动:** 在该模式下，DLDP 只生成日志和触发信息，并由用户手动关闭检测到的单向链路。
- 网页刷新模式:** 启用或禁用网页自动刷新。
- 网页自动刷新闻隔:** 设置网页自动刷新闻隔为 1 到 100 秒之间，默认为 5 秒。

➤ 端口配置

- 端口选择:** 点击选择按钮来快速选择输入的指定端口号。
- 选择:** 选择需要配置 DLDP 的端口号，可多选。
- 端口:** 交换机端口列表。
- DLDP 状态:** 启用或禁用 DLDP。
- 协议状态:** 显示端口的 DLDP 配置。
- 链路状态** 显示端口的链路状态。
- 邻居状态** 显示端口的邻居状态。

➤ 配置步骤

步骤	操作	说明
1	开启全局 DLDP 状态	必选操作。进入以太网 OAM>>DLDP>>DLDP 页面，开启 DLDP 状态。
2	开启相应端口的 DLDP 状态	必选操作。进入以太网 OAM>>DLDP>>DLDP 页面，开启相应端口的 DLDP 状态。
3	设置关闭模式	可选操作。进入以太网 OAM>>DLDP>>DLDP 页面，设置关闭模式为自动或手动。
4	重置 DLDP 状态	可选操作。进入以太网 OAM>>DLDP>>DLDP 页面，选择相应或全部端口，点击<重置>按键，重置 DLDP 状态。

8.7 DLDP 功能的组网应用

➤ 组网需求

- 设备 A 和设备 B 通过两对光纤交叉互连，如图所示。
- 单向链路须一检测到就立即关闭，且被 DLDP 关闭的端口须在光纤正确连接后重新开启。

➤ 组网图

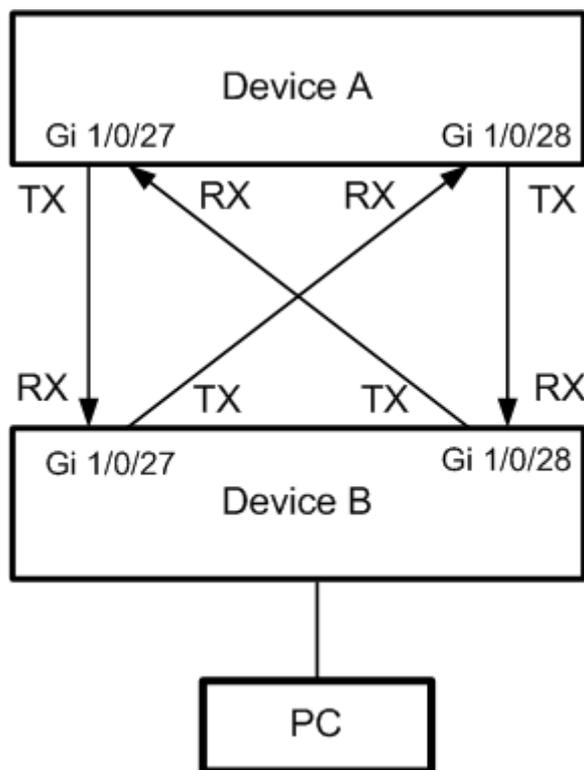


图 8-13 DLDP 应用举例

➤ 配置步骤

步骤	操作	说明
1	开启全局 DLDP 状态	必选操作。进入以太网 OAM>>DLDP>>DLDP 页面，全局启用设备 A 和设备 B 的 DLDP 状态。
2	开启相应端口的 DLDP 状态	必选操作。进入以太网 OAM>>DLDP>>DLDP 页面，设置设备 A、设备 B 的 1/0/27 端口和 1/0/28 端口的 DLDP 状态为“启用”。
3	设置关闭模式	必选操作。可选进入以太网 OAM>>DLDP>>DLDP 页面，设置设备 A 和设备 B 的关闭模式为“自动”。
4	重置 DLDP 状态	必选操作。进入以太网 OAM>>DLDP>>DLDP 页面，选中端口 1/0/27 和端口 1/0/28，点击<重置>按键以重置这两个端口的 DLDP 状态。

端口 1/0/27 和端口 1/0/28 的 DLDP 信息如下图所示：

全局配置

DLDP状态: 启用 禁用

通告间隔: 秒 (1-30)

关闭模式:

网页刷新状态: 启用 禁用

网页自动刷新间隔: 秒 (1-100)

端口配置

端口

选择	端口	DLDP状态	协议状态	链路状态	邻居状态
<input type="checkbox"/>		<input type="text" value="禁用"/>			
<input type="checkbox"/>	19	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	20	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	21	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	22	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	23	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	24	禁用	Initial	Link-Up	N/A
<input type="checkbox"/>	25	禁用	Initial	Link-Down	N/A
<input type="checkbox"/>	26	禁用	Initial	Link-Down	N/A
<input checked="" type="checkbox"/>	27	启用	Disable	Link-Down	Unidirectional
<input checked="" type="checkbox"/>	28	启用	Disable	Link-Down	Unidirectional

注意：

- 1、一个使能了DLDP的端口不能检测对端未使能DLDP端口的链路状态。
- 2、确保链路两边端口是相同的功能配置。

当四个端口正确连接后,选中端口 1/0/27 和端口 1/0/28 并点击<重置>按键,将其状态从 Disable 恢复正常。

[回目录](#)

第9章 DHCP

9.1 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中继的实现

下图为我司交换机TL-SL5428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。

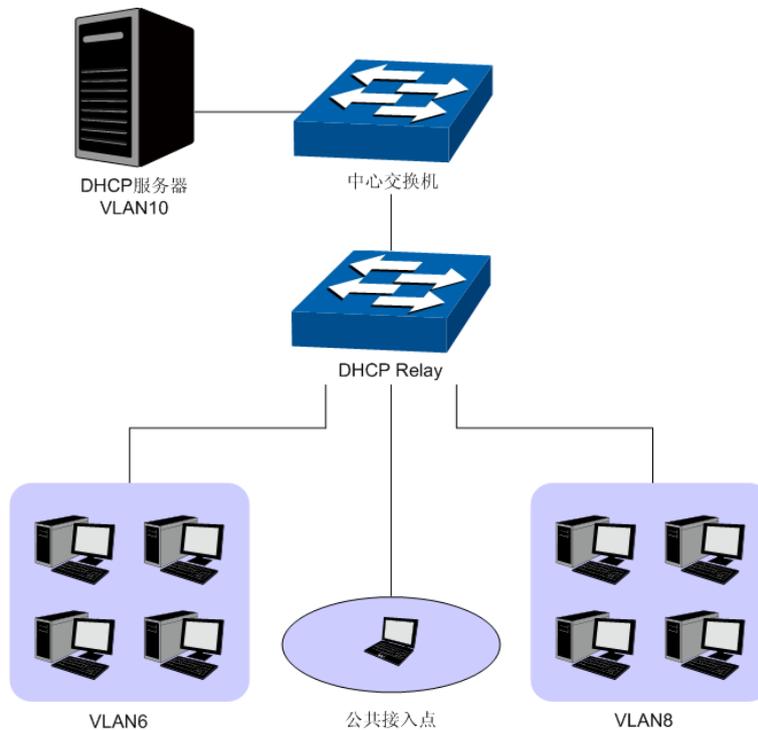


图 9-1 DHCP 中继典型拓扑图

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TL-SL5428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Option 82，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。

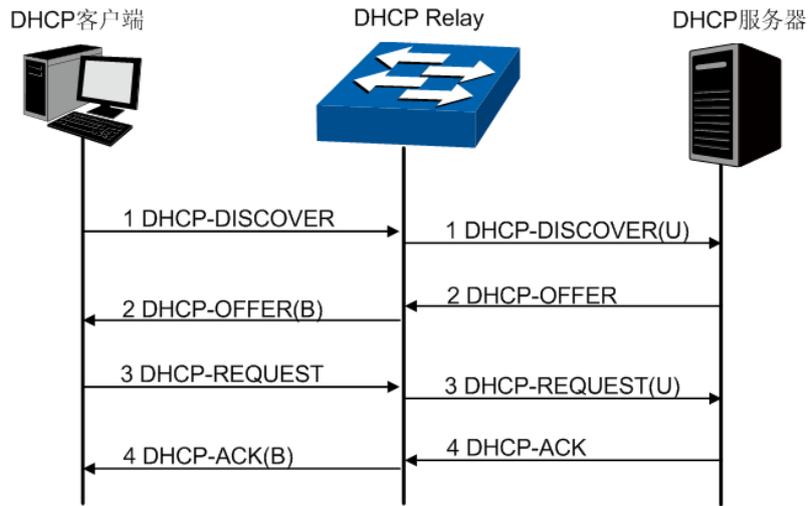


图 9-2 报文交互过程图片

➤ **DHCP Relay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Option 82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。

option82	Length(1)		
sub-option1(1)	Length(1)	VLAN(2)	Port(2)
sub-option2(1)	Length(1)	Hardware address(6)	

图 9-3 Option 82 字段格式

**注意:**

Option 82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中继功能可以在**DHCP中继**配置页面进行相关功能配置。

在DHCP中继页面中，可以启用DHCP中继功能，同时需要指定DHCP服务器来提供IP分配服务，还可以根据网络需要配置Option 82选项来辅助IP地址分配。

进入页面的方法：**DHCP>>DHCP中继>>DHCP中继**

全局配置

DHCP中继: 开启 关闭

Option 82设置

Option 82支持: 开启 关闭

已有Option 82字段: 保留 替换 丢弃

自定义选项内容:

电路ID子选项:

远程ID子选项:

添加DHCP服务器

IP地址: (格式: 192.168.0.1)

服务器名称: (最大16个字符)

DHCP服务器列表

选择	ID	IP地址	名称
<input type="button" value="全选"/> <input type="button" value="删除"/>			

注意:

1. 所有配置只会在DHCP中继功能开启后生效；
2. DHCP中继和DHCP侦听功能不能同时开启。

图 9-4 DHCP 中继

条目介绍:

➤ **全局配置**

DHCP中继: 选择是否启用DHCP中继功能。

➤ **Option 82设置**

Option 82支持: 选择是否启用Option 82字段。默认关闭。

原有Option 82字段处理:

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。

自定义支持:

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

Circuit ID:

设置自定义的Circuit ID值。

Remote ID:

设置自定义的Remote ID值。

➤ **添加DHCP服务器**

IP地址:

填写DHCP服务器的IP地址。

服务器名称:

填写对应的DHCP服务器的名称。

➤ **DHCP服务器列表**

选择:

勾选DHCP服务器条目进行删除，可多选。

ID:

显示DHCP服务器的ID。

IP地址:

显示DHCP中继服务器的IP地址。

名称:

显示DHCP服务器的名称。

**注意:**

- DHCP服务器功能和DHCP中继功能不能同时启用。
- DHCP侦听功能和DHCP中继功能不能同时启用。

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 DHCP>>DHCP中继>>DHCP中继功能 页面中启用DHCP中继功能。
2	配置Option 82选项。	可选操作。在 DHCP>>DHCP中继>>DHCP中继功能 页面中配置Option 82选项参数。
3	配置DHCP Server。	必选操作。在 DHCP>>DHCP中继>>DHCP中继功能 页面中配置DHCP服务器来提供IP分配服务。

[回目录](#)

第10章 组播管理

➤ 组播概述

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

当前，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（multicast）应运而生，它实现了网络中单点到多点的高效数据传送，能够节约大量网络带宽，降低网络负载。组播传输信息的方式如图 10-1 所示。

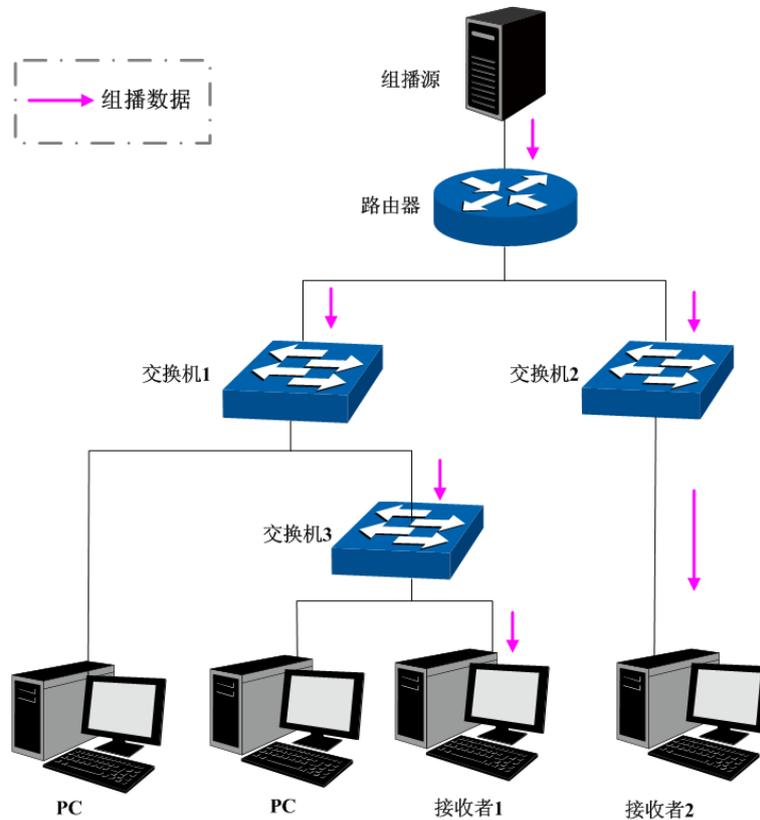


图 10-1 组播传输信息的方式

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。

➤ IPv4 组播地址

1. IPv4 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 10-1 特殊的组播 IP 地址段

2. IPv4 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 10-2 所示:

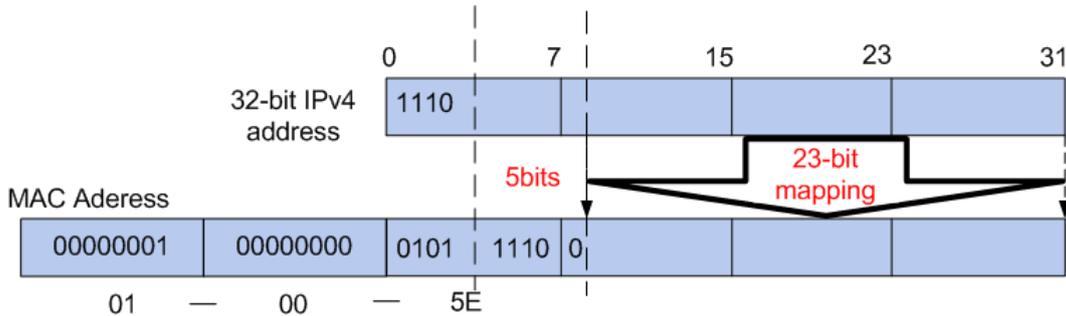


图 10-2 IPv4 组播 MAC 地址和组播 IP 地址的对应关系

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。

➤ IPv6 组播地址

1. IPv6 组播 IP 地址

IPv6 组播 IP 地址是一组接口的标识，有固定前缀 FF00::/8，IPv6 组播 IP 地址的格式如下图所示：

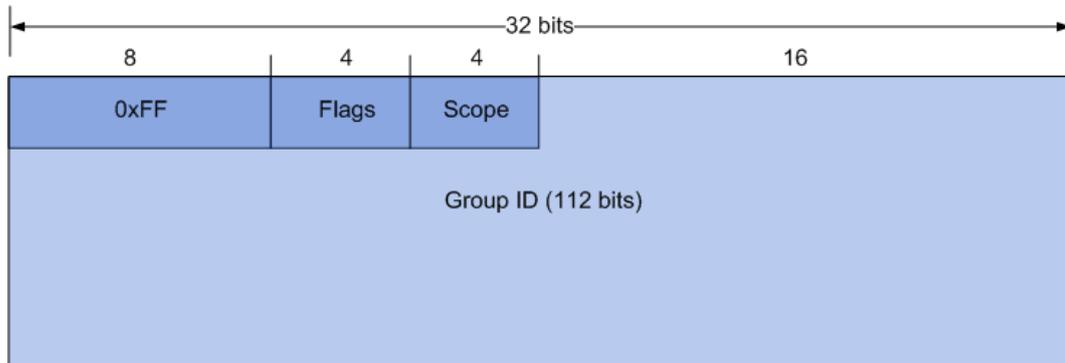


图 10-3 IPv6 组播 IP 地址格式

各字段含义如下：

- 0xFF：8比特，标识此地址为IPv6组播IP地址。
- Flags：4比特，结构如下所示。



- (1) 最高位是保留位，必须为 0。
 - (2) R 位：取 0 表示非内嵌 RP 的组播地址；取 1 则表示内嵌 RP 的组播地址，此时 P、T 位也必须取 1。具体定义和用途请参见 RFC3956。
 - (3) P 位：取 0 表示非基于单播前缀的组播地址；取 1 则表示基于单播前缀的组播地址，此时 T 位也必须取 1。具体定义和用途请参见 RFC3306。
 - (4) T 位：表示此地址的存活周期。取 0 表示由 IANA 永久分配的组播地址；取 1 表示非永久分配的组播地址。
- Scope：4比特，标识该组播组的应用范围，如下表所示。

取值	含义
0、3、F	保留（reserved）
1	接口本地范围（interface-local scope）
2	链路本地范围（link-local scope）
4	管理本地范围（admin-local scope）
5	站点本地范围（site-local scope）
6、7、9~D	未分配（unassigned）
8	机构本地范围（organization-local scope）

取值	含义
E	全局范围 (global scope)

表 10-2 Scope 取值含义

- **Group ID: 112**比特, 组播组标识号。用来在由Scope字段所指定的范围内唯一标识组播组。Flags字段的T位决定该标识是永久分配的还是临时的。

下表列出预留的 IPv6 组播 IP 地址:

取值	含义
FF01::1	节点本地范围所有节点组播地址
FF02::1	链路本地范围所有节点组播地址
FF01::2	节点本地范围所有路由器组播地址
FF02::2	链路本地范围所有路由器组播地址
FF05::2	站点本地范围所有路由器组播地址
FF0X::	X 取值范围从 0 到 F。这些是被保留的组播地址, 不能分配给任何组播组。

表 10-3 预留的 IPv6 组播 IP 地址列表

还有一类组播 IP 地址叫做被请求节点 (Solicited-node) 组播地址, 它对应于一个 IPv6 单播或任播地址, 主要用于获取同一链路上邻居节点的链路层地址以及进行重复地址检测。每个 IPv6 节点都必须加入到它的单播或任播地址所对应的被请求节点组播组中。

被请求节点组播地址的格式为: FF02:0:0:0:0:1:FFXX:XXXX。其中, FF02:0:0:0:0:1:FF 为 104 位固定前缀, XX:XXXX 为对应的单播或任播 IPv6 地址的低 24 位。

2. IPv6 组播 MAC 地址

IPv6 组播 MAC 地址的高 16 位为 0X3333, 标识 IPv6 组播组, 低 32 位为 IPv6 组播 IP 地址的低 32 位。下面是 IPv6 组播 IP 地址 FF1E::0101:130B 和其 IPv6 组播 MAC 地址映射对应关系示意图。

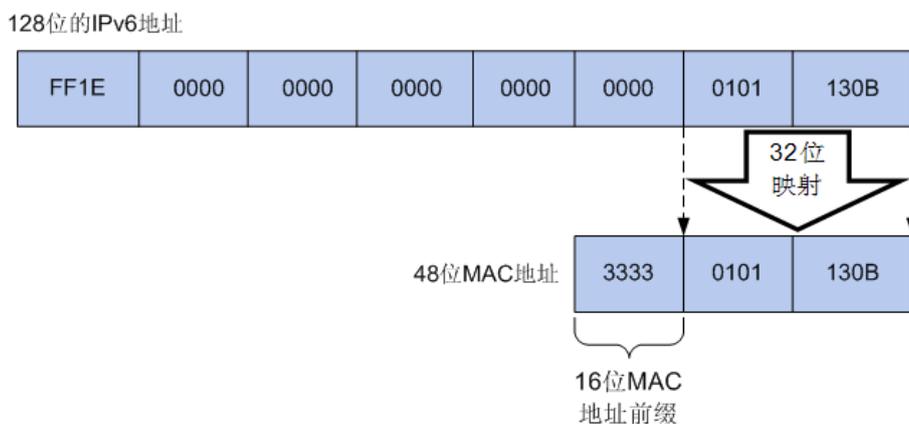


图 10-4 IPv6 组播 IP 地址和 MAC 地址映射关系示意图

➤ 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 10-5 所示。

VLAN ID	组播 IP	端口
---------	-------	----

图 10-5 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。

➤ MLD 侦听

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。

组播管理模块主要用于配置交换机的组播管理功能，包括 IGMP 侦听、MLD 侦听以及组播地址表三个部分。

10.1 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次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**、**VLAN 参数**、**端口参数**、**过滤地址**、**组播 VLAN**、**静态地址表**、**报文统计**、**查询器**和**IGMP 认证**九个配置页面。

10.1.1 基本配置

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

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

进入页面的方法：组播管理>>IGMP 侦听>>基本配置

基本配置

IGMP侦听： 启用 禁用

未知组播报文： 通过 丢弃

IGMP侦听信息

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

注意：
基本配置、端口参数、VLAN参数同时启用，IGMP侦听才能启用。

图 10-6 基本配置

条目介绍：

> 端口配置

- IGMP 侦听：** 选择是否启用交换机的 IGMP 侦听功能。
- 未知组播报文：** 选择交换机对未知组播报文的处理方法。

> IGMP 侦听信息

- 描述：** 显示 IGMP 侦听的配置项。
- 成员：** 显示对应配置项的成员。

10.1.2 VLAN 参数

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

进入页面的方法：组播管理>>IGMP 侦听>>VLAN 参数

VLAN参数

VLAN ID: (1-4094)

路由器端口时间: 秒 (60-600, 推荐: 300)

成员端口时间: 秒 (60-600, 推荐: 260)

离开滞后时间: 秒 (1-30, 推荐: 1)

禁用路由器端口: (格式为: 1-3,6,8)

静态路由器端口: (格式为: 1-3,6,8)

VLAN列表

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

注意：
当组播VLAN功能启用时，此处配置将失效。

图 10-7 VLAN 参数

条目介绍:

➤ VLAN 参数

- VLAN ID:** 填写启用 IGMP 侦听功能的 VLAN ID。
- 路由器端口时间:** 在所设时间内, 如果交换机没有从路由器端口接收到查询报文, 就认为该路由器端口失效。推荐 300 秒。
- 成员端口时间:** 在所设时间内, 如果交换机没从成员端口接收到报告报文, 就认为该成员端口失效。推荐 260 秒。
- 离开滞后时间:** 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐 1 秒。
- 禁用路由器端口** 选择禁止被配置成路由器端口的端口。
- 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

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



注意:

当“组播 VLAN”功能启用时, 本页的配置将失效。

配置步骤:

步骤	操作	说明
1	启用 IGMP 侦听功能	必选操作。在 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	配置 VLAN 的组播参数	可选操作。在 组播管理>>IGMP 侦听>>VLAN 参数 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。

10.1.3 端口参数

本页用来配置交换机端口的 IGMP 侦听属性。

进入页面的方法：组播管理>>IGMP 侦听>>端口参数

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

提交 帮助

注意：

- 1、此处的过滤设置对静态组播IP不生效。
- 2、一个端口最多只能绑定15个过滤地址ID，请使用如下的输入格式：1，5，8。

图 10-8 端口参数

条目介绍：

➤ 端口配置

- 端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：** 勾选条目配置端口的 IGMP 侦听功能，可多选。
- 端口：** 显示交换机的端口号。
- IGMP 侦听：** 选择该端口是否启用 IGMP 侦听功能。
- 快速离开：** 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。
- 过滤：** 选择是否启用端口组播过滤功能。
- 动作模式：** 选择当组播地址属于过滤地址范围时，交换机对数据包的处理方式。
- 允许：只有组播地址属于过滤地址范围时，才处理组播报文。
 - 拒绝：只处理组播地址不在过滤地址范围内的组播报文。
- 绑定过滤地址 (ID)：** 配置该端口需要绑定的过滤地址 ID 号。
- 最多加入组播组：** 通过限制端口最多加入组播组数目，来避免某些端口占据过多带宽。
- LAG：** 显示端口当前所属的汇聚组。



注意：

- 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。

10.1.4 过滤地址

本页用来配置需要过滤的组播地址段。

进入页面的方法：组播管理>> IGMP 侦听>>过滤地址

新建条目

过滤地址ID： (1-30)

起始组播IP： (格式为：225.0.0.1)

结束组播IP： (格式为：225.0.0.1)

过滤地址表

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

当前过滤地址总数：0

图 10-9 过滤地址

条目介绍：

➤ **新建条目**

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

➤ **过滤地址表**

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

10.1.5 组播 VLAN

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

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

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

进入页面的方法：组播管理>>IGMP 侦听>>组播 VLAN

组播VLAN	
组播VLAN:	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
VLAN ID:	<input type="text"/> (2-4094)
路由器端口时间:	<input type="text"/> 秒 (60-600, 推荐300秒)
成员端口时间:	<input type="text"/> 秒 (60-600, 推荐260秒)
离开滞后时间:	<input type="text"/> 秒 (1-30, 推荐1秒)
静态路由端口:	<input type="text"/> (格式为: 1-3,6,8)
源IP替换:	<input type="text"/> (格式为: 192.168.0.1)

注意:

- 1、创建了组播VLAN后，所有的IGMP报文都在组播VLAN内处理。
- 2、必须在VLAN配置页面完成端口的相关VLAN属性配置，组播VLAN才能正常运行。
- 3、当设置源IP替换值为0.0.0.0时，源IP替换机制不生效。

图 10-10 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，如果交换机没从成员端口接收到报告报文，就认为该成员端口失效。推荐 260 秒。
- 离开滞后时间:** 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐 1 秒。
- 静态路由端口:** 填写静态配置的路由器端口，多用于拓扑稳定的网络中。
- 源 IP 替换** 在组播 VLAN 内收到的用户 IGMP request 报文将根据此源 IP 进行替换。



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。
- 建立了组播 VLAN 后，所有的 IGMP 报文只在组播 VLAN 内处理。

配置步骤:

步骤	操作	说明
1	启用 IGMP 侦听功能	必选操作。在 组播管理>>IGMP 侦听>>基本配置 、 端口参数 页面，启用交换机的 IGMP 侦听功能和端口的 IGMP 侦听功能。
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。 <ul style="list-style-type: none"> 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。

➤ 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。

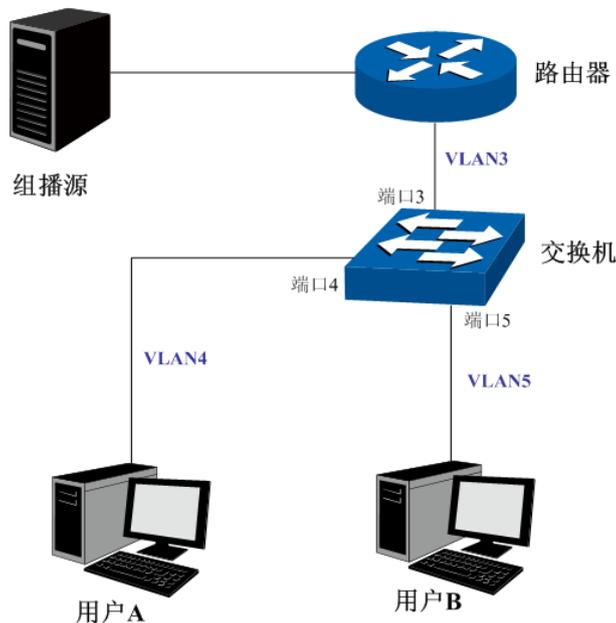
交换机：端口 3 与路由器相连，且通过 VLAN3 转发数据；端口 4 与用户 A 相连，且通过 VLAN4 转发数据；端口 5 与用户 B 相连，且通过 VLAN5 转发数据。

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 IGMP 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。

10.1.6 静态地址表

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

进入页面的方法：**组播管理>>IGMP 侦听>>静态地址表**

新建条目

组播 IP : (格式为：225.0.0.1)

VLAN ID : (1-4094)

转发端口 : (格式为：1-3,6,8) 添加

查找条目

查找选项: 全部 查找

静态组播IP表

选择	组播IP	VLAN ID	转发端口
全选 删除 帮助			

当前静态组播IP总数：0

图 10-11 静态地址表

条目介绍:

➤ **新建条目**

组播 IP: 填写静态绑定的组播 IP 地址。

VLAN ID: 填写组播 IP 对应的 VLAN ID。

转发端口: 填写组播 IP 的转发端口。

➤ **查找条目**

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

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

➤ **静态组播 IP 表**

选择: 勾选条目进行删除，可多选。

组播 IP: 显示绑定的组播 IP 地址。

VLAN ID: 显示组播组对应的 VLAN ID。

转发端口: 显示组播组的转发端口。

10.1.7 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**

自动刷新

自动刷新： 启用 禁用

刷新周期： 秒（3-300） 提交

IGMP报文统计

端口 选择

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

刷新
清空
帮助

图 10-12 报文统计

条目介绍：

➤ **自动刷新**

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为 5 秒。

➤ **IGMP 报文统计**

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

端口： 显示交换机的端口号。

查询报文数： 显示端口接收到的查询报文的数目。

报告报文(V1)： 显示端口接收到的 IGMPv1 报告报文的数目。

报告报文(V2)： 显示端口接收到的 IGMPv2 报告报文的数目。

报告报文(V3)： 显示端口接收到的 IGMPv3 报告报文的数目。

离开报文： 显示端口接收到的离开报文的数目。

错误报文： 显示端口接收到的错误报文的数目。

141

10.1.8 查询器

在运行了 IGMP 的组播网络中，会有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，这样的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。本交换机提供 IGMP 查询器功能，可以解决此问题，通过使用 IGMP 查询器功能，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。

在本页可以配置 IGMP 查询器相关参数。

进入页面的方法：**组播管理>>IGMP 侦听>>查询器**

查询器参数配置

VLAN ID: (1-4094)

通用组查询间隔: 秒 (1-300)

最大响应时间: 秒 (1-25)

通用组源IP: (格式为: 192.168.0.1)

特定组查询间隔: 秒 (1-5)

特定组查询次数: (1-5)

特定组源IP: (格式为: 192.168.0.1)

查询器列表

选择	VLAN ID	通用组查询间隔	最大响应时间	通用组源IP	特定组查询间隔	特定组查询次数	特定组源IP
<input type="checkbox"/>	<input type="text"/>						

注意:

- 1、一个VLAN只能添加一个查询器。
- 2、启用查询器会影响查询路由器的选举。

图 10-13 IGMP 查询器

条目介绍:

➤ 查询器参数配置

- VLAN ID:** 设置启用 IGMP 查询器的 VLAN ID。
- 通用组查询间隔:** 设置 IGMP 查询器发送通用组查询报文的查询间隔，IGMP 查询器将根据该值定期向指定 VLAN ID 发送通用组查询报文。
- 最大响应时间:** 设置报告报文的响应时间，发送通用组查询报文后，若在此段时间内没有收到报告报文，则认为该端口下无组播组成员。
- 通用组源 IP:** 设置 IGMP 查询器发送通用组查询报文的源 IP 地址，地址不能设置为组播 IP 地址和广播 IP 地址。
- 特定组查询间隔:** 该参数用于设置 IGMP 查询器发送特定组查询报文的查询间隔。在收到离开报文后，IGMP 查询器将根据该值定期向接收到离开报文的端口发送特定组查询报文。

特定组查询次数: 该参数用于设置 IGMP 查询器发送特定组查询报文的查询次数。在收到离开报文后, IGMP 查询器将向接收到离开报文的端口发送特定组查询报文, 如果在达到指定发送次数之前就收到报告报文, 则接收端口仍为该组播组成员端口, 同时停止特定组查询报文的发送; 如果特定组查询报文发送次数达到指定发送次数, 且没有收到报告报文, 则将该端口从组播组转发端口中删除。

特定组源 IP: 该参数用于设置 IGMP 查询器发送特定组查询报文的源 IP 地址, 地址不能设置为组播 IP 地址和广播 IP 地址。

➤ 查询器列表

VLAN ID 选择: 点击<选择>按键, 可根据所输 VLAN ID, 快速查找查询器条目。

选择: 勾选条目配置查询器参数, 可多选。

VLAN ID: 显示 VLAN ID。

通用组查询间隔: 显示查询器的通用组查询间隔。

最大响应时间: 显示查询器的最大响应时间。

通用组源 IP: 显示查询器的通用组源 IP。

特定组查询间隔: 显示查询器的特定组查询间隔。

特定组查询次数: 显示查询器的特定组查询次数。

特定组源 IP: 显示查询器的特定组源 IP。

10.1.9 IGMP 认证

IGAP (Internet Group membership Authentication Protocol, IGMP 认证协议) 是组播认证协议, 开启该认证可以使得端口接收到需要通过用户名及密码认证的组播组资源。

在本页面可以开启或关闭端口的 IGMP 认证。

进入页面的方法：组播管理>>IGMP 侦听>>IGMP 认证

选择	端口	IGMP认证	LAG
<input type="checkbox"/>		禁用	
<input type="checkbox"/>	1	禁用	---
<input type="checkbox"/>	2	禁用	---
<input type="checkbox"/>	3	禁用	---
<input type="checkbox"/>	4	禁用	---
<input type="checkbox"/>	5	禁用	---
<input type="checkbox"/>	6	禁用	---
<input type="checkbox"/>	7	禁用	---
<input type="checkbox"/>	8	禁用	---
<input type="checkbox"/>	9	禁用	---
<input type="checkbox"/>	10	禁用	---
<input type="checkbox"/>	11	禁用	---
<input type="checkbox"/>	12	禁用	---

图 10-14 端口参数

条目介绍：

➤ **IGMP 认证**

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选条目配置端口的 IGMP 认证功能，可多选。

端口： 显示交换机的端口号。

IGMP 认证： 选择该端口是否启用 IGMP 认证功能。

LAG： 显示端口当前所属的汇聚组。

10.2 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。

本功能包括基本配置、VLAN 配置、过滤配置、端口参数、静态组播组、查询器和 MLD 报文统计七个配置页面。

10.2.1 基本配置

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

进入页面的方法：组播管理>>MLD 侦听>>基本配置

基本配置	
MLD 侦听：	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
Report 报文抑制：	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
未知组播报文：	<input checked="" type="radio"/> 通过 <input type="radio"/> 丢弃
路由器端口时间：	<input type="text" value="260"/> 秒 (1-1000)
成员端口时间：	<input type="text" value="260"/> 秒 (200-1000)
特定组查询间隔：	<input type="text" value="1"/> 秒 (1-5)
特定组查询次数：	<input type="text" value="2"/> (1-7)
组播 VLAN：	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用
组播 VLAN ID：	<input type="text" value="1"/> (1-4094)

注意：

- 1、配置未知组播报文丢弃时，IGMP Snooping 中的未知组播报文丢弃功能同时生效。
- 2、当 VLAN 配置页面中有与组播 VLAN ID 对应的 VLAN 时，组播 VLAN 功能将生效。

图 10-15 基本配置

条目介绍：

> 基本配置

MLD 侦听：

选择是否启用交换机的 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。

未知组播报文：

选择交换机对未知组播报文的处理方法。

配置未知组播报文为“丢弃”时，IGMP 侦听中的未知组播报文丢弃功能同时生效。

- 路由器端口时间:** 输入全局路由器端口时间，如果在路由器端口老化时间内路由器端口没有收到任何查询报文，则该路由器端口将老化。
若在 [10.2.2 VLAN 配置](#) 界面配置了路由器端口时间，将覆盖这里的全局配置。
- 成员端口时间:** 输入全局成员端口时间，如果在成员端口老化时间内成员端口没有收到任何报告报文，则该成员端口将老化。
若在 [10.2.2 VLAN 配置](#) 界面配置了成员端口时间，将覆盖这里的全局配置。
- 特定组查询间隔:** 输入特定组查询间隔，当某个组播组内没有成员端口时，将以特定组查询间隔为间隔时间发送特定组查询报文，以此判断是否还有成员要加入该组播组。
- 特定组查询次数:** 输入特定组查询次数，当某个组播组内没有成员端口时，将发送特定组查询次数的特定组查询报文，以此判断是否还有成员要加入该组播组。
- 组播 VLAN:** 选择是否启用组播 VLAN 功能，当组播 VLAN 启用，则所有组播数据报文都在组播 VLAN 内转发。
- 组播 VLAN ID:** 输入组播 VLAN ID。

组播 VLAN 配置步骤:

步骤	操作	说明
1	设置 VLAN	必选操作。在 6.1 802.1Q VLAN 页面创建 VLAN，并添加相应端口。
2	使能 MLD 侦听	必选操作。在 组播管理>>MLD 侦听>>基本配置 页面“启用” MLD 侦听 条目功能。
3	在 VLAN 中使能 MLD 侦听	必选操作。进入 组播管理>>MLD 侦听>>VLAN 配置 页面，设置 VLAN ID 参数为步骤 1 中创建的 VLAN。
4	使能组播 VLAN	必选操作。在 组播管理>>MLD 侦听>>基本配置 页面，“启用” 组播 VLAN 条目功能，并设置 组播 VLAN ID 参数为步骤 1 中创建的 VLAN。 使能组播 VLAN 后 10.2.2 VLAN 配置 页面中的配置将全部失效。

10.2.2 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 侦听参数。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](#)

当前配置的VLAN总数: 0

注意:

- 1、当全局MLD Snooping启用且对应的VLAN创建时，MLD中VLAN参数的设置生效。
- 2、当设置VLAN中的路由器端口时间和成员端口时间时，这些值将代替全局配置的相应时间值生效。
- 3、当未设置老化时间（设为默认的0秒），全局配置的老化时间将生效。

图 10-16 VLAN 配置

条目介绍:

➤ VLAN 参数

VLAN ID:

填写启用 MLD 侦听功能的 VLAN ID。

当 [10.2.1 基本配置](#) 页面 **MLD 侦听** 条目功能被设置为“启用”，且在 [第 6 章 VLAN](#) 中创建了 VLAN，则此处相应 VLAN 设置的 MLD 侦听参数才会生效。

路由器端口时间:

输入该 VLAN 的路由器端口时间。它将代替 [10.2.1 基本配置](#) 页面设置的路由器端口时间生效。

成员端口时间:

输入该 VLAN 的成员端口时间。它将代替 [10.2.1 基本配置](#) 页面设置的成员端口时间生效。

快速离开:

启用或者禁用该 VLAN 内的端口快速离开功能。

若启用该功能，则当组播组内的成员端口收到 MLD 离开报文时将马上删除，不会发送通用组查询判断组播组内是否还存在成员端口。即若某个端口开启快速离开功能，只要此端口下同一个 IPv6 组播组中有一个成员离开，其他成员都将无法接收 IPv6 组播报文。因此，建议仅在 VLAN 的每个端口只有一个成员时开启快速离开功能。

禁用路由器端口

输入 VLAN 内的禁用路由器端口，禁用路由器端口不能被配置为路由器端口。

静态路由器端口:

输入静态配置的路由器端口，多用于拓扑稳定的网络中。

➤ VLAN 列表

VLAN ID 选择:

点击<选择>按键，可根据所输 VLAN ID，快速查找 VLAN 条目。

选择:

勾选条目配置 VLAN 参数，可多选。

VLAN ID:

显示 VLAN ID。

路由器端口时间:

显示 VLAN 的路由器端口时间。

成员端口时间:

显示 VLAN 的成员端口时间。

- 快速离开：** 显示 VLAN 的端口快速离开功能。
- 禁用路由器端口** 显示 VLAN 内的禁用路由器端口。
- 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。

10.2.3 过滤配置

当交换机收到 MLD 报告报文时，各个端口将根据其绑定的过滤地址 ID 号来决定该端口能否加入特定的组播组。如果要加入的组播组未被过滤，该端口将被加入到特定组播组的转发端口列表中，否则交换机将丢弃 MLD 报告报文。通过组播过滤功能，可以限制用户能够加入的组播组。

进入页面的方法：**组播管理>>MLD 侦听>>过滤配置**

图 10-17 过滤配置

条目介绍：

> 过滤配置

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

> 过滤地址表

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



说明：

最多可设置 30 条过滤条目。

10.2.4 端口参数

可以在本页配置端口的 MLD 侦听功能。

进入页面的方法：**组播管理>>MLD 侦听>>端口参数**

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

注意：

- 1、此处的过滤设置对静态组播IP不生效。
- 2、一个端口最多只能绑定15个过滤地址ID，请使用如下的输入格式：1，5，8。
- 3、如果设置的最大加入组播组数目比当前端口学习到的组播组数目小，多出的组播表项将被删除。

图 10-18 端口参数

条目介绍：

▶ 端口参数

- 端口选择：** 点击<选择>按键，可根据所输端口号，快速选择相应端口。
- 选择：** 勾选条目配置端口的 MLD 侦听功能，可多选。
- 端口：** 显示交换机的端口号。
- 过滤：** 选择是否启用端口组播过滤功能。
- 过滤模式：** 选择当组播地址属于过滤地址范围时，交换机对数据包的处理方式。
- 允许：只有组播地址属于过滤地址范围时，才处理组播报文。
 - 拒绝：只处理组播地址不在过滤地址范围内的组播报文。
- 绑定过滤地址（ID）：** 配置该端口需要绑定的过滤地址 ID 号。一个端口最多只能绑定 15 个过滤地址 ID。输入格式为 1,5,8。
- 最多加入组播组：** 通过限制端口最多加入组播组数目，来避免某些端口占据过多带宽。范围为 0-256。
- LAG：** 显示端口当前所属的汇聚组。



说明：

如果设置的最大加入组播组数目比当前端口学习到的组播组数目小，多出的组播表项将被删除。

10.2.5 静态组播组

可以在本页配置组播的静态地址表，在此配置的组播组不是通过 MLD 侦听学习到的，不受动态组播组及组播过滤的影响。

进入页面的方法：组播管理>>MLD 侦听>>静态组播组

静态组播组配置

VLAN ID: (1-4094)

组播 IP: (格式为: FF03::C2D5:2313)

转发端口: (格式为: 1-3,6,8)

静态组播 IP 表

VLAN ID

选择	VLAN ID	组播 IP	转发端口
<input type="checkbox"/>			<input type="text"/>

当前静态组播 IP 总数: 0

图 10-19 静态组播组

条目介绍：

➤ 静态组播组配置

VLAN ID: 填写组播 IP 对应的 VLAN ID。

组播 IP: 填写静态绑定的组播 IP 地址。

转发端口: 填写组播 IP 的转发端口。

➤ 静态组播 IP 表

VLAN ID 选择: 点击<选择>按键，可根据所输 VLAN ID，快速查找静态组播 IP 条目。

选择: 勾选条目进行修改，可多选。

VLAN ID: 显示组播组对应的 VLAN ID。

组播 IP: 显示绑定的组播 IP 地址。

转发端口: 显示组播组的转发端口。

10.2.6 查询器

MLD 查询器在二层网络中充当路由器的作用，它能够定时发送查询报文，使二层设备能够在数据链路层建立并维护组播转发表项。

进入页面的方法：组播管理>>MLD 侦听>>查询器

查询器参数配置

VLAN ID: (1-4094)

最大响应时间: 10 秒 (1-25)

通用组查询间隔: 25 秒 (2-300)

通用组源 IP: FE80::02FF:FFFF:FE00:0001 (格式为: FE80::ABEC:12EA)

查询器列表

VLAN ID

选择	VLAN ID	最大响应时间	通用组查询间隔	通用组源 IP
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>

当前查询器总数: 0

图 10-20 查询器

条目介绍:

➤ 查询器参数配置

- VLAN ID:** 该参数用于设置启用 MLD 侦听查询器的 VLAN ID。
- 最大响应时间:** 该参数用于设置报告报文的响应时间，发送通用组查询报文后，若在此段时间内没有收到报告报文，则认为该端口下无组播组成员。
- 通用组查询间隔:** 该参数用于设置 MLD 侦听查询器发送通用组查询报文的查询间隔，MLD 侦听查询器将根据该值定期向指定 VLAN 发送通用组查询报文。
- 通用组源 IP:** 该参数用于设置 MLD 侦听查询器发送通用组查询报文的源 IP 地址，地址不能设置为组播 IP 地址和广播 IP 地址。

➤ 查询器列表

- VLAN ID 选择:** 点击<选择>按键，可根据所输 VLAN ID，快速查找查询器条目。
- 选择:** 勾选条目配置查询器参数，可多选。
- VLAN ID:** 显示 VLAN ID。
- 最大响应时间:** 显示查询器的最大响应时间。
- 通用组查询间隔:** 显示查询器的通用组查询间隔。
- 通用组源 IP:** 显示查询器的通用组源 IP。

10.2.7 MLD 报文统计

可以在本页查看交换机各端口的 IPv6 组播报文流量信息，便于监控网络中的 MLD 报文。

进入页面的方法：组播管理>>MLD 侦听>>MLD 报文统计

自动刷新

自动刷新： 启用 禁用

刷新周期： 秒 (3-300) 提交

MLD报文统计						
端口	收到的MLD查询 报文	收到的MLD报告 报文 (v1)	收到的MLD报告 报文 (v2)	收到的MLD离开 报文	发送的MLD特定 组查询报文	错误报文
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

刷新
清空
帮助

图 10-21 MLD 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。

➤ MLD 报文统计

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

端口： 显示交换机的端口号。

收到的 MLD 查询报文： 显示端口接收到的 MLD 查询报文数目。

收到的 MLD 报告报文 (v1)： 显示端口接收到的 MLDv1 报告报文数目。

收到的 MLD 报告报文 (v2)： 显示端口接收到的 MLDv2 报告报文数目。

收到的 MLD 离开报文： 显示端口接收到的 MLD 离开报文数目。

发送的 MLD 特定组查询报文： 显示端口发送的 MLD 特定组查询报文数目。

错误报文： 显示端口收到的 MLD 错误报文数目。

10.3 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 组播表**和 **IPv6 组播表**两个配置页面。

10.3.1 IPv4 组播表

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 组播表**

显示设置

组播IP： (格式为：225.0.0.1)

VLAN ID： (1-4094)

端口：

地址类型： 全部 静态 动态

组播IP表

组播IP	VLAN ID	转发端口	地址类型
<input type="button" value="刷新"/> <input type="button" value="帮助"/>			

当前组播IP总数：0

图 10-22 IPv4 组播表

条目介绍：

➤ 显示设置

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

➤ 组播 IP 表

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

10.3.2 IPv6 组播表

显示交换机中学习到的 IPv6 组播组。

进入页面的方法：组播管理>>组播地址表>>IPv6 组播表

显示设置

组播 IP： (格式为：FF03::AD45:3444)

VLAN ID： (1-4094)

端口：

地址类型： 全部 静态 动态

提交

组播IP表

组播IP	VLAN ID	转发端口	地址类型
刷新 帮助			

当前组播IP总数： 0

图 10-23 IPv6 组播表

条目介绍：

➤ 显示设置

- 组播 IP：** 选择欲查找条目需包含的组播 IP 地址信息。
- VLAN ID：** 选择欲查找条目需包含的 VLAN ID 信息。
- 端口：** 选择欲查找条目需包含的端口号。

地址类型: 选择欲查找条目需包含的地址类型信息。

- 全部: 显示全部组播地址表条目。
- 静态: 显示静态组播地址表条目。
- 动态: 显示动态组播地址表条目。

➤ **组播 IP 表**

组播 IP: 显示组播 IP 地址。

VLAN ID: 显示组播组对应的 VLAN ID。

转发端口: 显示组播组的转发端口。

地址类型: 显示组播 IP 的类型。



说明:

IPv4 组播表和 IPv6 组播表条目数的总和不得超过 256。

[回目录](#)

第11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。

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

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

➤ QoS 工作原理

本交换机通过在入口阶段对数据流进行分类，然后在出口阶段将不同类型的数据流映射到不同优先级的队列，最后依据调度模式来决定不同优先级队列的数据包被转发的方式，从而实现了 QoS 功能。

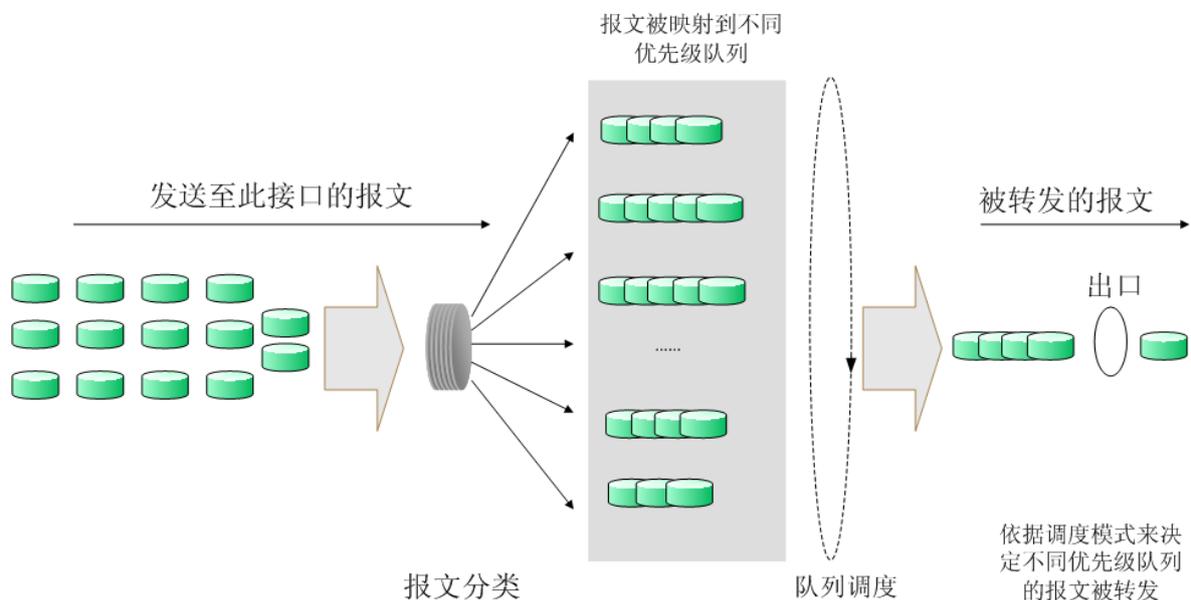


图 11-1 QoS 工作原理

- 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

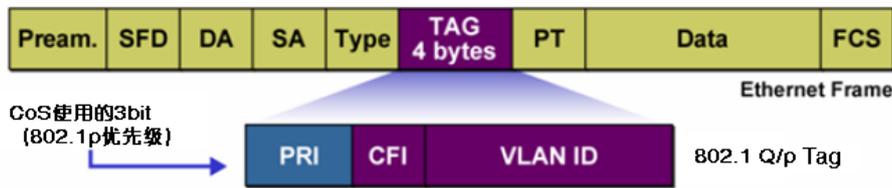


图 11-2 802.1Q 的帧格式

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

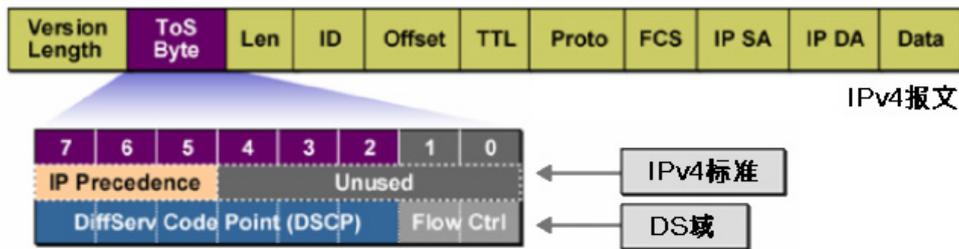


图 11-3 IP 报文

如图所示，IP 报文头部的 ToS（Type of Service，服务类型）字段共有 8bit，可以表征不同优先级特征的报文，前 3 个 bit 表示的是 IP 的优先级，取值范围是 0~7。RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域。其中 DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前 6 个 bit（0~5bit）表示，取值范围为 0~63，后 2 个 bit（6、7bit）是保留位。通过交换机的配置页面，可以配置不同的 DS 字段对应不同的优先级，交换机发送 IP 包时，会根据 IP 包的 DS 域决定发送的优先级。对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

⚠ 注意:

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

➤ 调度模式

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

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

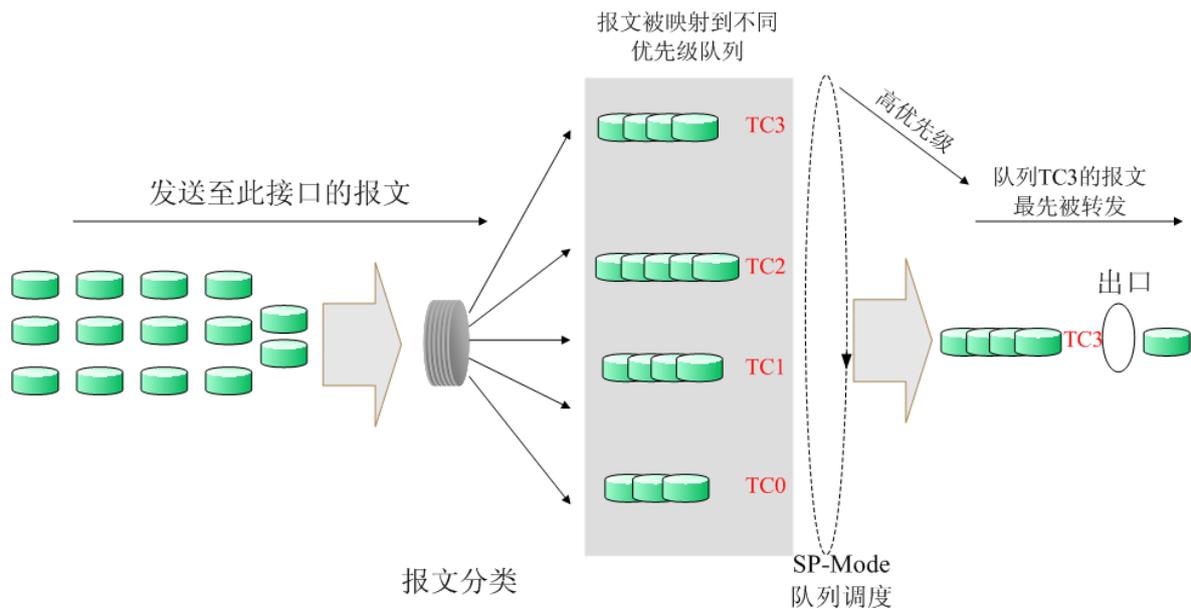


图 11-4 严格优先级模式

2. **WRR-Mode: WRR 优先级模式。** WRR 模式的调度算法是在队列之间按权重比值进行轮流调度，以保证每个队列都得到一定的服务时间，加权值表示获取资源的比重。WRR 队列避免了采用 SP 调度时低优先级中的报文可能长时间得不到服务的缺点，并且虽然多个队列调度是轮询进行的，但是对每个队列不是固定的分配服务时间，如果队列为空则马上更换下一个队列调度，这样可以充分利用带宽资源。TC0-TC3 的默认权重比是 1:2:4:8。

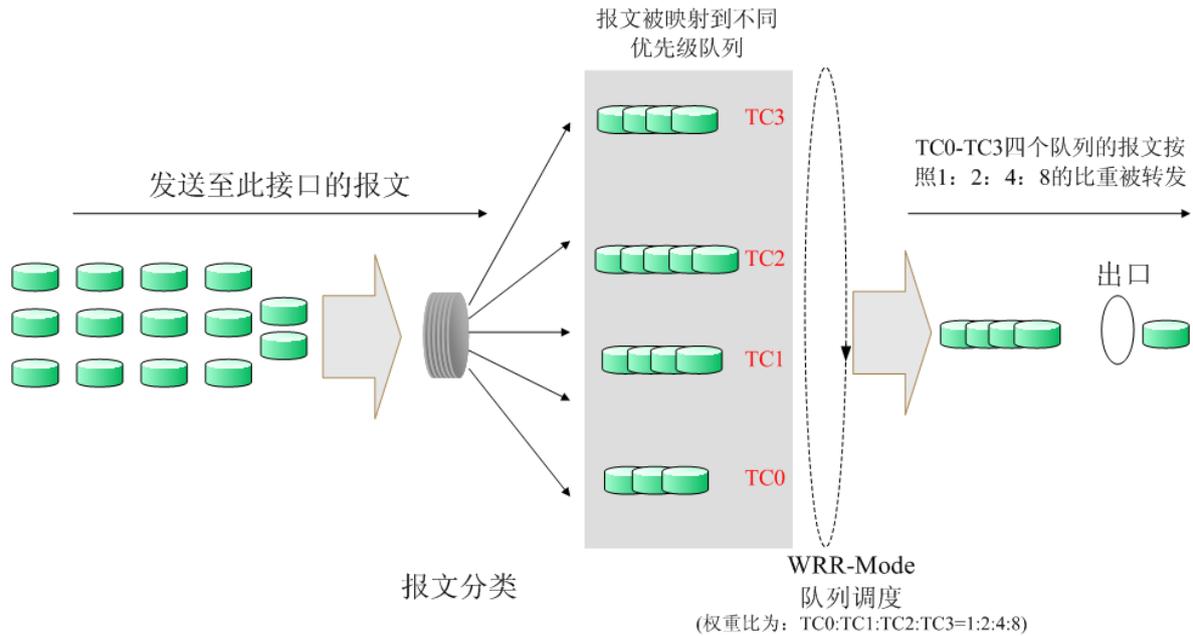


图 11-5 WRR 优先级模式

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

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

11.1.1 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

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

注意：

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

图 11-6 端口配置

条目介绍：

➤ 端口优先级配置

- 选择：** 勾选端口配置端口优先级，可多选。
- 端口：** 显示交换机的物理端口。
- 优先级：** 配置端口的所属优先级等级。
- LAG：** 显示当前端口所属的 LAG 组。



注意：

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

配置步骤：

步骤	操作	说明
1	进入页面	
2	选择端口进行配置	勾选所需端口，可多选。
3	选择端口的优先级	可选操作，可选择 CoS 0-CoS 7。
4	配置 802.1P/CoS 优先级	必选操作。进入 802.1P/CoS 映射 页面配置 802.1P/CoS 优先级。
5	选择调度模式	必选操作。进入 队列调度模式 页面选择调度模式。

11.1.2 DSCP 映射

在 DSCP 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 字段的重新定义，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。

优先级配置

DSCP优先级： 启用 禁用 提交

优先级等级

DSCP： 优先级等级：

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

提交
帮助

注意：
优先级等级TC0、TC1...TC3中，数字越大，表示优先级越高。

图 11-7 DSCP 优先级

条目介绍：

➤ **优先级配置**

DSCP 优先级： 选择是否启用 DSCP 优先级。

➤ **优先级等级**

DSCP： 根据 IP 包的 DS 域决定的优先级。优先级级别从 0 到 63。

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

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

配置步骤：

步骤	操作	说明
1	进入页面	
2	启用 DSCP 优先级模式	必选操作。缺省状态下，DSCP 功能为禁用。
3	将 DSCP 优先级对应至优先级等级队列	必选操作。选择 DSCP 优先级的同时选择相应的优先级等级队列。
4	选择调度模式	必选操作。进入 队列调度模式 页面选择调度模式。

11.1.3 802.1P /CoS 映射

在802.1P/CoS配置页面中，可以进行802.1P/CoS优先级的配置。802.1P对802.1Q tag中的Pri字段进行了定义，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；否则应用基于端口的优先级。

进入页面的方法：服务质量>>QoS 配置>>802.1P/CoS 映射

802.1P优先级配置

802.1P优先级： 启用 禁用 提交

tag与CoS到出口队列映射配置

Tag-id/CoS-id: 队列TC-id:

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

提交 帮助

注意：

队列TC-id TC0、TC1...TC3中，数字越大，表示优先级越高。

图 11-8 802.1P 优先级

条目介绍：

➤ **802.1P 优先级配置**

802.1P 优先级： 选择是否启用 802.1P 优先级。

➤ **tag 与 CoS 到出口队列映射配置**

Tag-id/CoS-id： IEEE802.1P 协议里规定的 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...TC3 表示。



注意：

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

配置步骤：

步骤	操作	说明
1	进入页面	
2	启用 802.1P 优先级模式	必选操作。缺省状态下，802.1P 功能为禁用。
3	将 802.1P 优先级对应至优先级等级队列	必选操作。选择 802.1P 优先级的同时选择相应的优先级等级队列。
4	选择调度模式	必选操作。进入 队列调度模式 页面选择调度模式。

11.1.4 队列调度模式

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

进入页面的方法：**服务质量>>QoS 配置>>队列调度模式**



图 11-9 调度模式

条目介绍：

> 调度模式配置

- SP-Mode:** 严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。
- WRR-Mode:** 加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。TC0 到 TC3 的权重比值是 1: 2: 4: 8。
- SP+WRR-Mode:** SP+WRR 模式，这种队列调度模式是前两种模式的混合。在此模式下，交换机提供了两个调度组，分别是 SP 组和 WRR 组。其中 SP 组和 WRR 组之间遵循的是严格优先级调度规则，而 WRR 组内部队列遵循的是 WRR 调度模式。
在该调度模式下 TC3 属于 SP 组；TC0、TC1、TC2 属于 WRR 组，权重比是 1: 2: 4。这样在调度的时候首先是 TC3 按照 SP 的调度模式独自占用带宽，然后是 WRR 组的成员 TC0、TC1、TC2 按照权重比 1: 2: 4 的比例占用带宽。
- 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。

11.2 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。

11.2.1 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

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

注意:

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

图 11-10 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(Kbps): 配置端口接收数据时的带宽，可选择下拉列表中提供的带宽，也可选择“手动输入”或“禁用”选项。若选择“手动输入”选项，则系统将会自动选择与填写的数值最相近的 **64Kbps** 的整数倍值作为入口带宽的输入值；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(Kbps): 配置端口转发数据时的带宽，可选择下拉列表中提供的带宽，也可选择“手动输入”或“禁用”选项。若选择“手动输入”选项，则系统将会自动选择与所填写的数值最相近的 **64Kbps** 整数倍值作为出口带宽的输入值；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。
- 在一个或多个端口上启用出口带宽限制时，建议将各端口的流量控制禁用，以保证交换机的正常工作。

11.2.2 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**

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

注意：
风暴抑制和入口带宽限制不能同时开启。

图 11-11 风暴抑制

条目介绍：

> 风暴抑制

端口选择： 点击<选择>按键，可根据所输端口号，快速选中相应端口。

选择： 勾选端口以配置风暴抑制参数，可多选也可不选。

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

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

UL 包抑制(bps):

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

LAG:

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

**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。

11.3 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 11-1 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 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。
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 11-2 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 11-3 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。

11.3.1 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 11-12 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。

11.3.2 端口配置

在启用语音 VLAN 功能之前，需要在端口配置页面中配置各端口的功能参数。

进入页面的方法：服务质量>>语音 VLAN>>端口配置

端口配置

端口

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

注意：

任何一个端口不能同时属于“语音VLAN”和“私有VLAN”。

图 11-13 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。

11.3.3 OUI 配置

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

进入页面的方法：**服务质量>>语音 VLAN>>OUI 配置**

新建条目

OUI地址： (格式为：00-00-00-00-00-01)

OUI掩码： (默认为：FF-FF-FF-00-00-00) 添加

OUI描述： (1-16个字符)

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

全选
删除
帮助

图 11-14 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 11-2 设置语音设备连接端口的端口类型。

步骤	操作	说明
2	创建 VLAN	必选操作。在 VLAN>>802.1Q VLAN>>VLAN 配置 页面中点击<新建>按钮创建 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12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。

12.1 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。

12.1.1 时间段列表

在时间段列表页面，可以查看和编辑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
<input type="checkbox"/>	1	HN	18:00-24:00	---	---	---	周期&绝对	编辑 查看
<input type="checkbox"/>	2	CC	20:00-24:00	---	---	---	周期	编辑 查看

图 12-1 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。

12.1.2 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

The screenshot shows the '新建时间段' configuration interface. It includes the following elements:

- 时间段定义 (Time Period Definition):**
 - 时间段名称: [Text Input Field]
 - 假日
 - 绝对时间: 起始日期: [2000] / [01] / [01] 结束日期: [2000] / [01] / [01]
 - 周期: 星期一 星期二 星期三 星期四 星期五 星期六 星期日
- 时间片段 (Time Fragment):**
 - 起始时间: [00] : [00]
 - 结束时间: [24] : [00]
 - [添加] button
- 时间片段列表 (Time Fragment List):**

序号	起始时间	结束时间	操作
[提交] [帮助]			

图 12-2 创建时间段

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。

12.1.3 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 12-3 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。

12.2 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 **组合字段 ACL** 六个配置页面。

12.2.1 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

选择	序号	RuleID	源MAC地址	目的MAC地址	VLAN ID	时间段名称	操作
<input type="checkbox"/>	1	1	00-19-66-80-54-36	---	---	---	编辑 查看 上移 下移
<input type="checkbox"/>	2	2	---	00-19-66-80-54-36	---	---	编辑 查看 上移 下移

图 12-4 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。

> **规则列表**

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

12.2.2 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 12-5 创建 ACL

条目介绍：

> **创建 ACL**

ACL ID: 配置 ACL ID。

规则排序: 配置该 ACL 内部的规则如何排序。默认为用户配置。

用户配置：按照用户配置规则的先后顺序进行规则匹配。

12.2.3 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

MAC ACL

访问控制列表ID：MAC访问控制列表

规则ID：

安全操作：允许

源MAC： 地址掩码：

目的MAC： 地址掩码：

VLAN ID：

以太网类型：（4位十六进制数）

用户优先级：无限制

时间段：无限制

提交 帮助

图 12-6 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。

12.2.4 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 12-7 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。
- 分片报文：** 选择此规则是否对分片报文生效。当选择支持分片报文时，此规则对所有分片报文进行处理，而最后一块报文总是允许转发。
- 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。

12.2.5 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 12-8 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：** 选择此规则是否对分片报文生效。当选择支持分片报文时，此规则对所有分片报文进行处理，而最后一块报文总是允许转发。
- 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。
- 选择 ICMP：** 当 IP 协议选择 ICMP 时，此处配置预定义的 ICMP 类型和代码。
- ICMP 类型：** 配置自定义的 ICMP 名称。
- ICMP 代码：** 配置自定义的 ICMP 代码。
- 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。

12.2.6 组合字段 ACL

组合字段 ACL 根据数据包的 MAC 地址，IP 地址以及其他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>>组合字段 ACL

图 12-9 为扩展 IP ACL 添加规则

条目介绍：

> 组合字段 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。
- 分片报文:** 选择此规则是否对分片报文生效。当选择支持分片报文时，此规则对所有分片报文进行处理，而最后一块报文总是允许转发。
- 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。

12.3 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**、**配置 Policy** 三个配置页面。

12.3.1 Policy 列表

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

进入页面的方法：**访问控制>>Policy 配置>>Policy 列表**



图 12-10 查看 Policy 列表

条目介绍：

> Policy 显示

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

➤ **Action 列表**

- 选择:** 选择动作条目进行删除。
- 序号:** 显示动作条目的序号。
- ACL ID:** 显示此 Policy 中包含的 ACL。
- 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。

12.3.2 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



创建Policy

Policy名称:

提交

帮助

图 12-11 创建 Policy

条目介绍:

➤ **创建 Policy**

- Policy 名称:** 填写 Policy 的名称。

12.3.3 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

Policy设置：

选择Policy：选择Policy名称

选择ACL：选择ACL

流镜像

镜像端口：Port 1

流监管

超额速率： Kbps(1-1000000)

超速处理：不处理

端口重定向

指定出口端口：所有端口

指定VID：

QoS重标记

DSCP：无限制

本地优先级：默认

提交 帮助

图 12-12 为 Policy 添加 ACL 并设置动作

条目介绍：

➤ Policy 设置

- 选择 Policy：** 选择 Policy 的名称。
- 选择 ACL：** 选择 ACL 作为 Policy 作用的对象。
- 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。
- 超额速率：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 规则的数据包指定转发端口。
 - 指定 VID：将匹配了相应 ACL 规则的数据包指定转发 VLAN。
- 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。

12.4 绑定配置

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

绑定配置功能包括绑定列表、端口绑定、VLAN 绑定三个配置页面。

12.4.1 绑定列表

在此页面中可以查看已进行端口/VLAN 绑定的 Policy 条目。

进入页面的方法：访问控制>>绑定配置>>绑定列表



图 12-13 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： 请根据需要进行选择参考已绑定的条目类别。

> Policy 绑定列表

选择： 选择绑定条目进行删除。

序号： 显示绑定条目的序号。

Policy 名称： 显示绑定的 Policy 名称。

绑定接口： 显示与相应 Policy 绑定的端口号或 VID。

方向： 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

12.4.2 端口绑定

在此页面中可以将 Policy 与端口进行绑定。

进入页面的方法：访问控制>>绑定配置>>端口绑定



图 12-14 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。

12.4.3 VLAN 绑定

在此页面中可以将 Policy 与 VLAN 进行绑定。

进入页面的方法：访问控制>>绑定配置>>VLAN 绑定

VLAN绑定配置

Policy名称： 添加

VLAN ID： (格式为：2-10,100) 帮助

VLAN绑定列表

序号	Policy名称	VLAN ID	方向

图 12-15 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 三个标签页中配置 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>>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。

12.5 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00-46-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

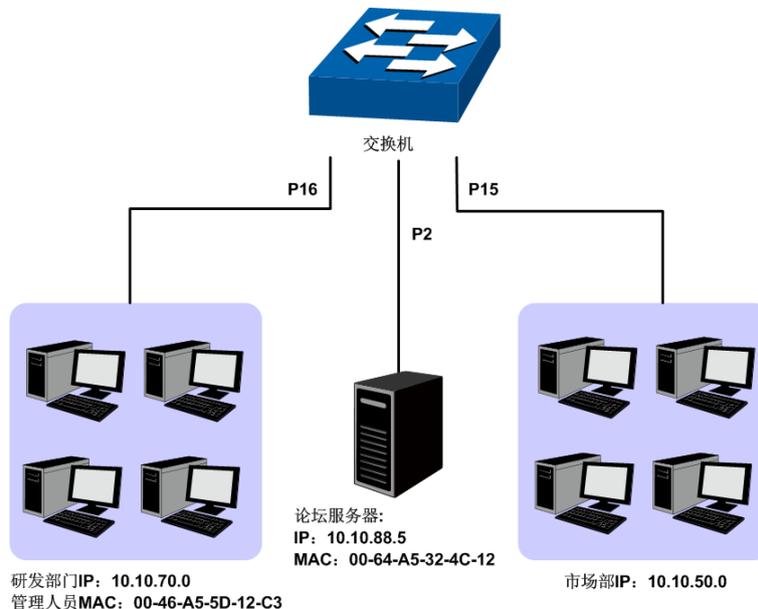


图 12-16 访问控制功能组网举例

➤ 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	<p>在访问控制>>ACL配置>>新建ACL页面，创建ACL 11。</p> <p>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。</p> <p>在访问控制>>Policy配置>>新建Policy页面，创建Policy，名称定为manager。</p> <p>在访问控制>>Policy配置>>配置Policy页面，将ACL 11应用到Policy manager。</p> <p>在访问控制>>绑定配置>>端口绑定页面，选择Policy manager与端口16绑定。</p>
3	需求2、4配置	<p>在访问控制>>ACL配置>>新建ACL页面，创建ACL 100。</p> <p>在访问控制>>ACL配置>>标准IP ACL页面，选择ACL 100，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。</p> <p>在访问控制>>ACL配置>>标准IP ACL页面，选择ACL 100，创建规则3，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。</p> <p>在访问控制>>ACL配置>>标准IP ACL页面，选择ACL 100，创建规则4，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。</p> <p>在访问控制>>Policy配置>>新建Policy页面，创建Policy，名称定为limit1。</p> <p>在访问控制>>Policy配置>>配置Policy页面，将ACL 100应用到Policy limit1。</p> <p>在访问控制>>绑定配置>>端口绑定页面，选择Policy limit1与端口16绑定。</p>

步骤	操作	说明
4	需求3、4配置	<p>在访问控制>>ACL配置>>新建ACL页面，创建ACL 101。</p> <p>在访问控制>>ACL配置>>标准IP ACL页面，选择ACL 101，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10.10.70.0，掩码为255.255.255.255；时间段选择无限制。</p> <p>在访问控制>>ACL配置>>标准IP ACL页面，选择ACL 101，创建规则6，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255.255.255.0；时间段选择work_time。</p> <p>在访问控制>>Policy配置>>新建Policy页面，创建Policy，名称定为limit2。</p> <p>在访问控制>>Policy配置>>配置Policy页面，将ACL 101应用到Policy limit2。</p> <p>在访问控制>>绑定配置>>端口绑定页面，选择Policy limit2与端口15绑定。</p>

[回目录](#)

第13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、AAA 和 PPPoE 配置八个部分，请根据实际需要进行配置。

13.1 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 防护和 IP 源防护，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。

13.1.1 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

选择	主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	来源	冲突
<input type="checkbox"/>								

当前条目总数: 0

注意:

- 1、冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。
- 2、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。

图 13-1 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。

➤ 四元绑定表

主机名/IP 地址/MAC 地址选择: 点击<选择>按键, 可根据主机名/IP 地址/MAC 地址快速查找四元绑定条目。

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描述名称。

IP 地址: 显示主机 IP 地址。

MAC 地址: 显示并编辑此条目主机的 MAC 地址。

VLAN ID: 显示并编辑此条目的 VLAN ID。

端口: 显示并编辑此条目主机连接的交换机端口。

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。

13.1.2 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**

手动绑定

主机名：（长度限制为20字符）

IP地址：（格式为：192.168.0.1）

MAC地址：（格式为：00-00-00-00-00-01）

VLAN ID：（1-4094）

端口：

防护范围：

手动绑定条目

选择	主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	冲突

当前条目总数：0

注意：

- 1、冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。
- 2、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。

图 13-2 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。
- 端口：** 输入主机连接的交换机端口。
- 防护范围：** 选择此条目支持的防护范围。
- 绑定：** 点击此按钮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。

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。

13.1.3 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 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：

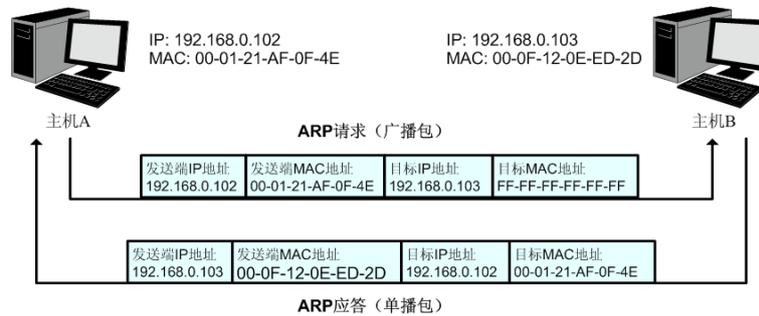


图 13-3 ARP 地址解析图

- 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

当前条目总数：0

注意：

- 1、VLAN ID选项适用于扫描存在跨交换机VLAN的网络拓扑
- 2、VLAN ID选项用于指定ARP扫描所使用的报文所带的VLAN Tag，且不受交换机VLAN配置的限制
- 3、当VLAN ID为空时交换机会使用不带VLAN Tag的数据包进行扫描

图 13-4 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>按钮将对局域网计算机进行扫描。

➤ **扫描结果**

选择： 勾选条目进行绑定或删除。

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。

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。

13.2 DHCP 侦听

13.2.1 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:

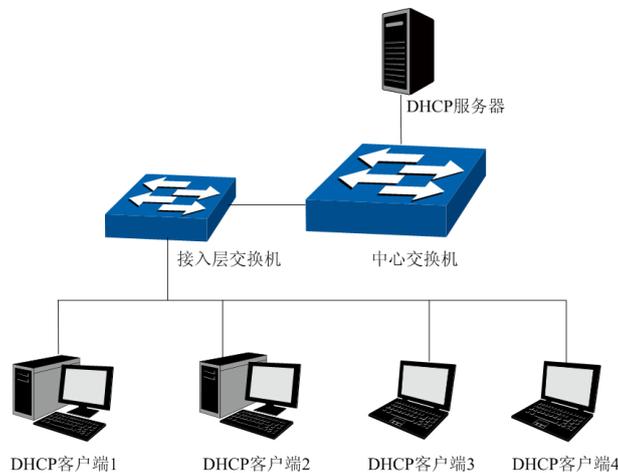


图 13-5 DHCP 网络典型应用

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:

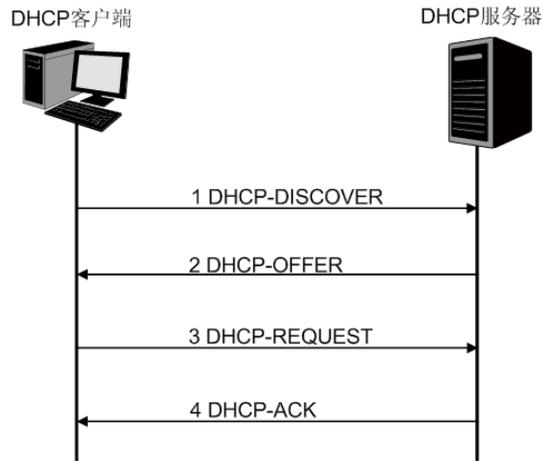


图 13-6 动态获取 IP 地址的过程

- 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。

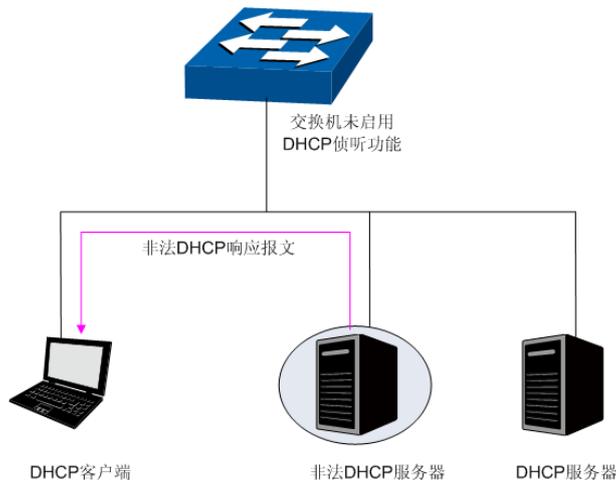


图 13-7 DHCP 服务欺骗攻击

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、IP 源防护等安全功能配合使用；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。

进入页面的方法：网络安全>> DHCP 侦听>> DHCP 侦听

DHCP侦听配置

DHCP侦听： 启用 禁用

全局流量控制： pps

Decline保护阈值： pps

Decline保护流量限制： pps

端口配置

端口

选择	端口	授信端口	MAC验证	流量控制	Decline侦听	LAG
<input type="checkbox"/>		<input type="text" value="禁用"/>	<input type="text" value="禁用"/>	<input type="text" value="禁用"/>	<input type="text" value="禁用"/>	
<input type="checkbox"/>	1	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	2	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	3	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	4	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	5	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	6	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	7	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	8	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	9	启用	禁用	禁用	禁用	---
<input type="checkbox"/>	10	启用	禁用	禁用	禁用	---

图 13-8 DHCP 侦听

 **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。

条目介绍：

➤ **DHCP 侦听配置**

- DHCP 侦听：** 选择是否启用 DHCP 侦听功能。默认未启用。
- 全局流量控制：** 填写交换机每秒允许转发的 DHCP 消息的数目，超出的部分将被丢弃。
- Decline 保护阈值：** 选择触发特定端口 Decline 保护所需的 Decline 报文最小流量。
- Decline 保护流量限制：** 如果端口 Decline 消息流量超出阈值，则将相应端口的端口流量限制设置为该值。

➤ **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端口。

- 选择:** 勾选端口配置端口参数，可多选。
- 端口:** 显示交换机的端口号。
- 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。

13.2.2 Option 82

进入页面的方法：网络安全>> DHCP 侦听>>Option 82

Option 82配置

初始端口: 结束端口:

Option 82功能: 启用 禁用

已有Option 82字段:

自定义选项内容:

电路ID子选项:

远程ID子选项:

Option 82 配置列表

端口号	Option 82功能	操作策略	电路ID子选项	远程ID子选项	LAG
1	禁用	保持	--	--	--
2	禁用	保持	--	--	--
3	禁用	保持	--	--	--
4	禁用	保持	--	--	--
5	禁用	保持	--	--	--
6	禁用	保持	--	--	--
7	禁用	保持	--	--	--
8	禁用	保持	--	--	--
9	禁用	保持	--	--	--
10	禁用	保持	--	--	--
11	禁用	保持	--	--	--
12	禁用	保持	--	--	--
13	禁用	保持	--	--	--
14	禁用	保持	--	--	--
15	禁用	保持	--	--	--

图 13-9 Option 82 配置

➤ Option 82 配置

- 初始端口:** 选择要配置 Option 82 功能的初始端口。
- 结束端口:** 选择要配置 Option 82 功能的结束端口。

- Option 82 功能:** 选择是否启用 Option 82 字段。默认未启用。
- 已有 Option 82 字段:** 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 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。

➤ Option 82 配置列表

显示端口的 Option 82 配置情况。

13.3 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 13-10 所示。

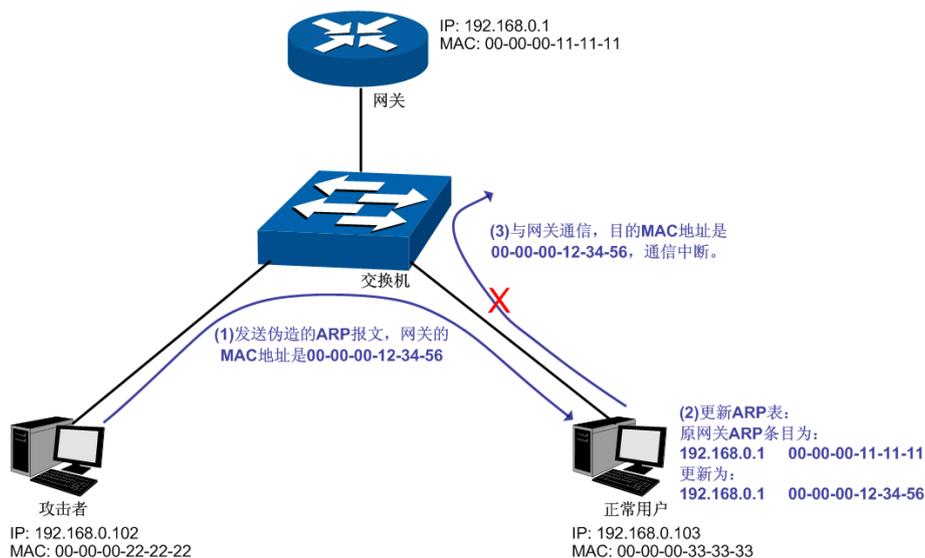


图 13-10 ARP 攻击-网关仿冒示意图

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 13-11 所示。

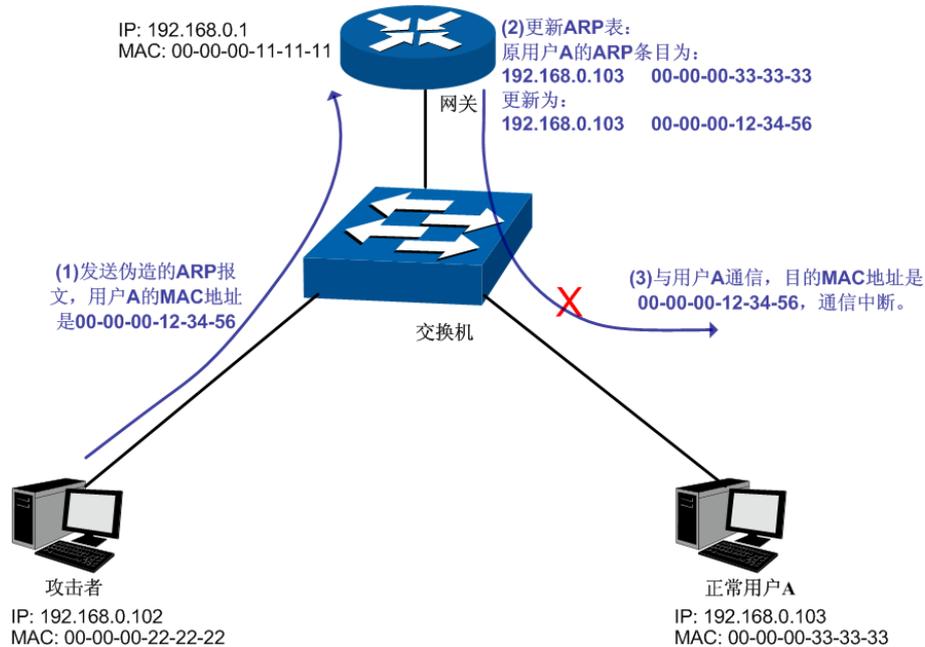


图 13-11 ARP 攻击-欺骗网关示意图

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 13-12 所示。

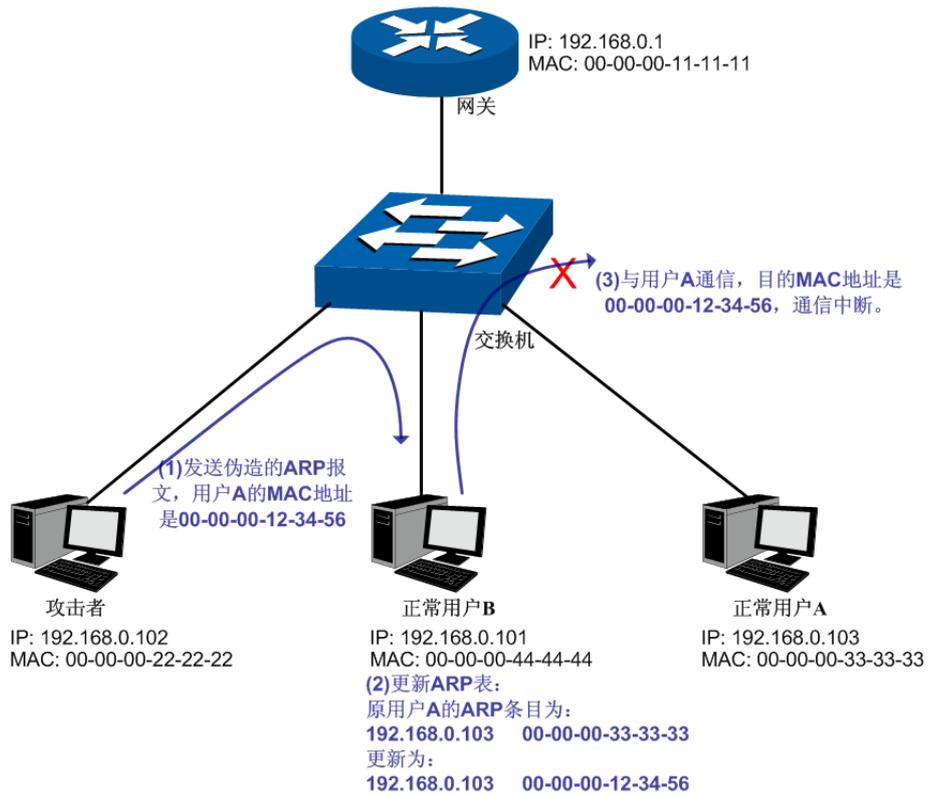


图 13-12 ARP 攻击-欺骗普通用户示意图

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 13-13 所示。

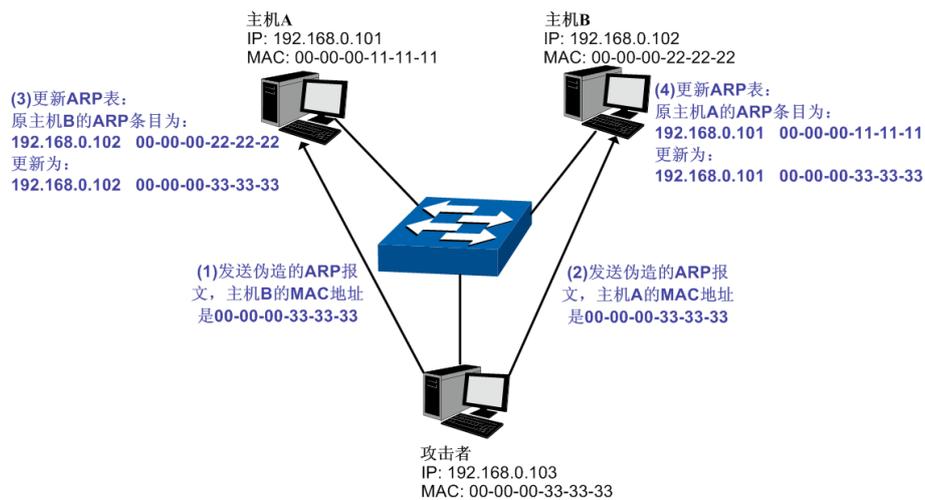


图 13-13 中间人攻击

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。

13.3.1 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

防ARP欺骗

防ARP欺骗： 启用 禁用

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

注意：

建议将上联端口和LAG端口设置为信任端口。

图 13-14 防 ARP 欺骗

条目介绍:

➤ **防 ARP 欺骗**

防 ARP 欺骗: 选择启用并单击<提交>按键即可启用防 ARP 欺骗功能。

➤ **信任端口**

信任端口: 勾选无须启用防 ARP 欺骗功能的信任端口。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

配置步骤:

步骤	操作	说明
1	绑定四元信息条目	必选操作。在 四元绑定 功能中将接入用户的四元信息进行绑定，手动绑定、扫描绑定和 DHCP 侦听方式均可进行绑定
2	对四元信息条目启用防护	必选操作。在 网络安全>>四元绑定>>绑定列表 页面中对相应的四元条目启用防护。
3	设置信任端口	必选操作。在 网络安全>>ARP 防护>>防 ARP 欺骗 页面中设置信任端口，上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。
4	启用防 ARP 欺骗	必选操作。在 网络安全>>ARP 防护>>防 ARP 欺骗 页面中启用防 ARP 欺骗功能。

13.3.2 防 ARP 攻击

防 ARP 攻击功能对交换机的各端口处理的合法 ARP 数据包设定阈值，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

防ARP攻击配置

端口

选择	端口	保护功能	速率(10-100)pps	当前速率pps	状态	LAG	操作
<input type="checkbox"/>		禁用 <input type="button" value="v"/>	<input type="text"/>				
<input type="checkbox"/>	1	禁用	15	---	---	---	---
<input type="checkbox"/>	2	禁用	15	1	---	---	---
<input type="checkbox"/>	3	禁用	15	---	---	---	---
<input type="checkbox"/>	4	禁用	15	---	---	---	---
<input type="checkbox"/>	5	禁用	15	---	---	---	---
<input type="checkbox"/>	6	禁用	15	---	---	---	---
<input type="checkbox"/>	7	禁用	15	---	---	---	---
<input type="checkbox"/>	8	禁用	15	---	---	---	---
<input type="checkbox"/>	9	禁用	15	---	---	---	---
<input type="checkbox"/>	10	禁用	15	---	---	---	---
<input type="checkbox"/>	11	禁用	15	---	---	---	---
<input type="checkbox"/>	12	禁用	15	---	---	---	---
<input type="checkbox"/>	13	禁用	15	---	---	---	---
<input type="checkbox"/>	14	禁用	15	---	---	---	---
<input type="checkbox"/>	15	禁用	15	---	---	---	---
<input type="checkbox"/>	16	禁用	15	---	---	---	---

注意：

建议LAG端口不要开启防ARP攻击功能。

图 13-15 防 ARP 攻击

条目介绍：

➤ 防 ARP 攻击配置

- 端口选择：** 点击<选择>按键，可根据所输端口号快速选择端口。
- 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。
- 防护功能：** 选择是否启用防 ARP 攻击功能。
- 速率：** 填写端口每秒允许接收的 ARP 数据包个数。
- 当前速率：** 显示端口当前收到的 ARP 数据包速率。
- 状态：** 显示端口当前防 ARP 攻击状态。
- LAG：** 显示端口当前所属的汇聚组。
- 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。



注意：

建议 LAG 端口不要开启防 ARP 攻击功能。

13.3.3 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

自动刷新

自动刷新： 启用 禁用

刷新周期： 秒 (3-300)

非法ARP报文统计

端口	信任端口	非法ARP报文	端口	信任端口	非法ARP报文
1	否	---	2	否	---
3	否	---	4	否	---
5	否	---	6	否	---
7	否	---	8	否	---
9	否	---	10	否	---
11	否	---	12	否	---
13	否	---	14	否	---
15	否	---	16	否	---
17	否	---	18	否	---
19	否	---	20	否	---
21	否	---	22	否	---
23	否	---	24	否	---

图 13-16 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。

➤ 非法 ARP 报文统计

端口： 显示交换机的端口号。

信任端口： 显示端口是否是 ARP 信任端口。

非法 ARP 报文： 显示端口收到的非法 ARP 数据包数量。

13.4 IP 源防护

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 IP 源防护功能中则利用在交换机中绑定的四元信息对 IP 包进行检查，过滤不符合四元绑定表的 IP 报文，只处理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

选择	端口	防护类型	LAG
<input type="checkbox"/>		禁用	
<input type="checkbox"/>	1	禁用	---
<input type="checkbox"/>	2	禁用	---
<input type="checkbox"/>	3	禁用	---
<input type="checkbox"/>	4	禁用	---
<input type="checkbox"/>	5	禁用	---
<input type="checkbox"/>	6	禁用	---
<input type="checkbox"/>	7	禁用	---
<input type="checkbox"/>	8	禁用	---
<input type="checkbox"/>	9	禁用	---
<input type="checkbox"/>	10	禁用	---
<input type="checkbox"/>	11	禁用	---
<input type="checkbox"/>	12	禁用	---

注意：

LAG端口不能启用IP源防护功能。

图 13-17 IP 源防护

条目介绍：

➤ **IP 源防护配置**

端口选择： 点击<选择>按键，可根据所输端口号快速选择端口。

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：** 只处理源 IP 地址和端口符合四元绑定信息的数据包。
- **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。

13.5 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。
Smurf Attack	通过冒充某主机向一个子网的广播地址发 ICMP 请求数据包，收到这一请求的主机都回应请求，向被攻击主机发包，使该主机受到攻击。
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 Attack	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。
Ping of Death	当 ICMP 重复请求报文的 IP 报文头中“Fragment Offset”和“Total Length”字段长度总和大于 65535 字节时，可能会引发 Ping of Death 攻击。因为包括 IP 报头在内的 IPv4 报文长度不能超过 65535 个字节，所以很多计算机系统不能合适地处理这种恶意的 ICMP 重复请求报文。因此，当主机收到这类报文时有可能会死机或自动重启。

表 13-1 本交换机支持的 DoS 防护种类

13.5.1 DoS 防护

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

全局配置

DoS攻击防护: 启用 禁用

Ping限速: ▼

SYN限速: ▼

攻击防护列表

选择	防护类型	攻击次数统计
<input type="checkbox"/>	Land Attack	---
<input type="checkbox"/>	Scan SYNFIN	---
<input type="checkbox"/>	Xmascan	---
<input type="checkbox"/>	NULL Scan	---
<input type="checkbox"/>	SYN sPort less 1024	---
<input type="checkbox"/>	Blat Attack	---
<input type="checkbox"/>	Ping Flooding	---
<input type="checkbox"/>	SYN/SYN-ACK Flooding	---
<input type="checkbox"/>	winNuke Attack	---
<input type="checkbox"/>	Smurf Attack	---
<input type="checkbox"/>	Ping Of Death	---

图 13-18 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。

Ping 限速： 启用了 Ping Flooding 攻击防护后，可在此设置局域网中 ping 数据包的转发速度。

SYN 限速： 启用了 SYN/SYN-ACK Flooding 攻击防护后，可在此设置局域网中 SYN/SYN-ACK 数据包的转发速度。

➤ 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。

攻击次数统计： 显示交换机受到的相应攻击类型的攻击总次数。

13.5.2 攻击检测

在此页面中可以检测交换机受到 DoS 攻击的实时信息。

进入页面的方法：[网络安全](#)>>[DoS 防护](#)>>[攻击检测](#)

检测结果		
端口	攻击类型	已检测攻击次数

图 13-19 攻击检测

条目介绍：

➤ 检测时间

检测时间：配置检测攻击时的检测时间长度，检测类型不包括泛洪攻击。

检测：点击<检测>按钮开始检测，交换机采用轮询方式检测受到的各种 DoS 攻击实时情况。

➤ 检测结果

端口：显示交换机端口号。

攻击类型：显示攻击类型名称。

已检测攻击次数：显示在上一检测时间内受到的实时攻击次数。



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。

13.6 802.1X 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。

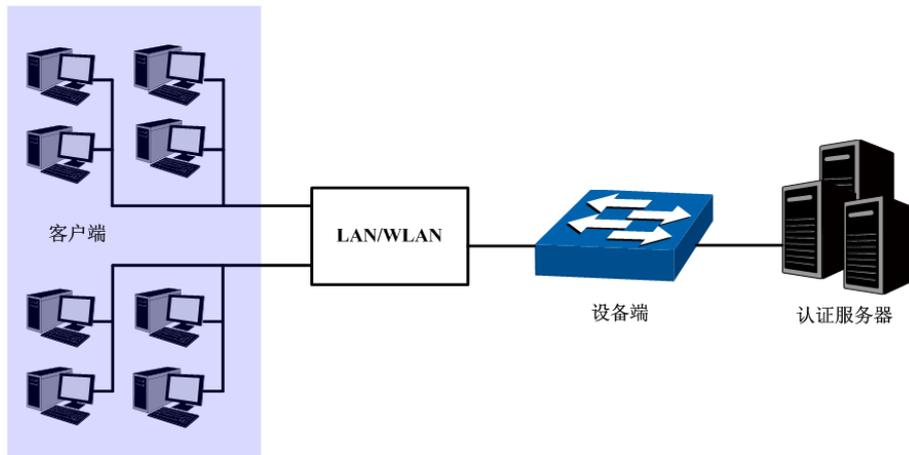


图 13-20 802.1X 认证的体系结构

- 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。

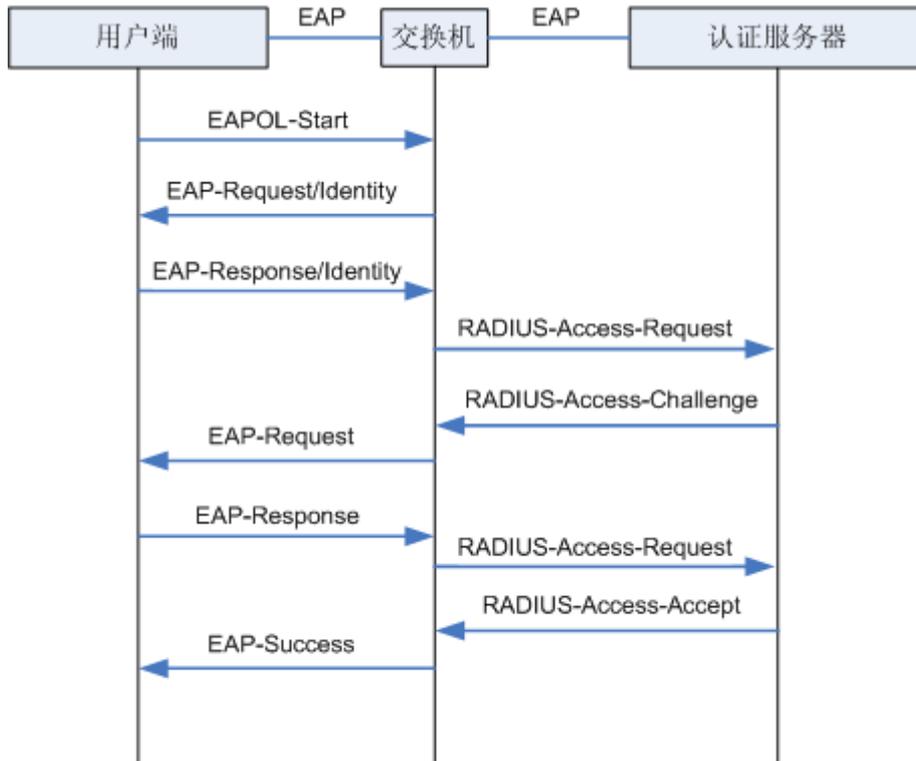


图 13-21 EAP-MD5 认证过程

- 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控。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。

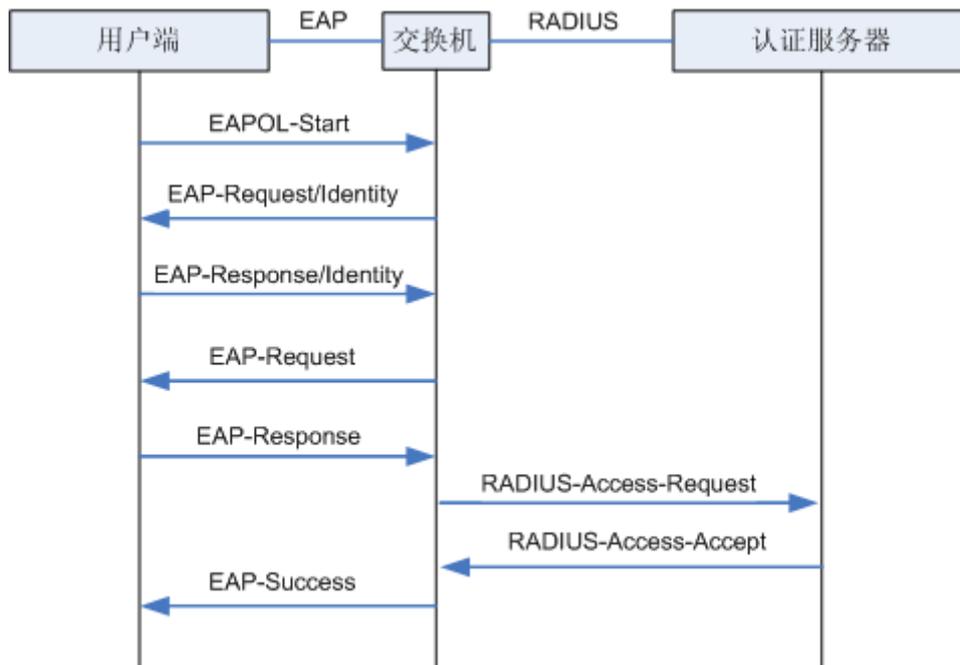


图 13-22 PAP 认证过程

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、端口配置两个配置页面。

13.6.1 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](#)

全局配置

802.1X功能： 启用 禁用

认证方法： 提交

Guest VLAN： 启用 禁用

Guest VLAN ID： (2-4094)

认证参数配置

静默： 启用 禁用

静默时长： 秒 (1-999)

重复发送次数： 次 (1-9) 提交

客户端响应超时： 秒 (1-9) 帮助

服务器响应超时： 秒 (1-9)

图 13-23 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。

认证方法: 选择 802.1X 认证方法。

- **EAP-MD5:** 交换机与认证服务器之间运行 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。

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。

➤ **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。

服务器响应超时: 填写交换机等待服务器响应的最大等待时间。若交换机在设定时间内没有收到服务器的回复，则重发报文。

13.6.2 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](#)

选择	端口	状态	Guest VLAN	控制模式	控制类型	授权状态	LAG
<input type="checkbox"/>		禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	1	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	2	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	3	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	4	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	5	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	6	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	7	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	8	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	9	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	10	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	11	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	12	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	13	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	14	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	15	禁用	禁用	自动	基于MAC	已授权	---
<input type="checkbox"/>	16	禁用	禁用	自动	基于MAC	已授权	---

注意:
LAG端口不能启用802.1X功能。

图 13-24 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查找相应条目。
- 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。

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, 安装过程见“802.1X 客户端软件使用说明”。
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。
5	全局开启 AAA 功能	必选操作。默认情况下, 交换机 AAA 全局功能未开启, 请在 网络安全>>AAA>>全局配置 页面中开启 AAA 功能。
6	设置 RADIUS 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。
7	设置 RADIUS 认证服务器组	可选操作。若需搭建多个 RADIUS 服务器对用户进行 802.1X 认证, 可先在步骤 6 中设置各个认证服务器参数, 并在 网络安全>>AAA>>服务器组 页面中创建一个 RADIUS 服务器组, 将已创建的 RADIUS 服务器加入到该服务器组中。

8	设置认证列表	可选操作。在 网络安全>>AAA>>认证列表 页面中, 选择 Login 认证方法列表, 并设置用于 802.1X 认证方法。认证方法可以选择内置的 RADIUS 服务器组, 也可选择自定义的 RADIUS 服务器组。
---	--------	--

 **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。

13.7 AAA

> 概述

AAA (Authentication, Authorization and Accounting, 认证, 授权, 计费) 用于在用户登录交换机或获取管理权限时对用户进行认证。

用户需输入用户名和密码进行登录和管理权限认证, 认证过程可以在交换机本地进行, 也可以在远程认证服务器 RADIUS/TACACS+ 上进行。进行交换机本地认证的用户名和密码可以在 [4.2 用户管理](#) 中进行设置。

> 应用模块

AAA 认证可应用于以下几种登录方式: Console, Telnet, SSH 和 HTTP。

> 认证列表

认证列表列出了对接入用户的认证方法及认证顺序。本交换机支持两种认证方法列表: Login 认证方法列表和 Enable 认证方法列表。Login 认证方法列表用于登录交换机的用户进行认证, Enable 认证方法列表用于将当前登录用户的权限从 guest 提升到 admin 从而使用户获得管理权限。

管理员可以在方法列表中自行设置不同认证方法的认证顺序。交换机将按照认证方法列表的顺序来对用户进行认证, 即首先按照第一种认证方法进行认证, 若未得到响应, 则使用下一种认证方法进行认证.....依此类推, 直到通过某种认证方法成功地实现通信或所有认证服务器没有响应。若在认证过程中认证失败, 则意味着安全服务器或交换机拒绝了用户的访问请求, 认证停止且不再尝试使用其他认证方法进行认证。

> 802.1X 认证

802.1x 认证采用 RADIUS 协议来提供详细的计费信息和灵活的认证管理。Dot1x 列表中定义了 802.1x 认证的服务器组。

> RADIUS/TACACS+ 配置

用户可以为交换机和服务器之间的连接设置 RADIUS/TACACS+ 服务器。

> 服务器组

用户可以将多个运行相同安全协议 (RADIUS 或 TACACS+) 的服务器定义成为一个服务器组, 并可以在服务器组列表中设置这些服务器的认证顺序。当用户尝试访问交换机时, 交换机会首先向

列表中第一个服务器发出认证请求，若未得到响应，则会向列表中下一个服务器进行请求……依此类推，直到有服务器对该认证请求发出响应。

交换机有 RADIUS 和 TACACS+两个内置服务器群组，不可删除。用户自定义的 RADIUS/TACACS+服务器将会自动加入这两个服务器群组。

13.7.1 全局配置

在该页面可以选择全局开启或关闭 AAA 功能。

进入页面的方法：网络安全 >> AAA >> 全局配置



图 13-25 AAA 全局配置

> 配置步骤:

选择开启，点击<提交>以全局开启 AAA 功能。

13.7.2 使能管理员权限

在本页面可以将当前登录用户的权限从 guest 提升到 admin 从而使用户获得管理权限。认证密码可以在 RADIUS/TACACS+服务器、自定义服务器或交换机本地进行认证。

进入页面的方法：网络安全 >> AAA >> 全局配置



图 13-26 使能管理员权限

> 配置步骤:

输入设置用户模式切换到管理员模式的管理密码，并点击<提交>按钮，当前登录的用户权限将由 guest 提升到 admin。只有 admin 用户可以进行接下来的 AAA 设置。



注意:

若管理密码要在本地进行确认，需事先在交换机设置该管理密码。详细信息请参考 CLI 手册中的 enable password 命令。

13.7.3 RADIUS 配置

本页面可以配置运行 RADIUS 安全协议的认证服务器。

进入页面的方法：网络安全 >> AAA >> RADIUS 配置

服务器配置

服务器IP: (格式: 192.168.0.1)

加密密钥:

认证端口: (1-65535)

计费端口: (1-65535) 添加

重传次数: (1-3)

超时: sec (1-9)

服务器列表

选择	服务器IP	加密密钥	认证端口	计费端口	重传次数	超时
<input type="checkbox"/>	<input type="text"/>					

提交
删除
帮助

图 13-27 RADIUS 配置

> 配置步骤

在服务器配置下配置 RADIUS 服务器的 IP 地址和其他相关参数，在服务器列表下可以查看、编辑或删除已配置好的 RADIUS 服务器。

> 条目解释:

- 服务器 IP:** 输入 RADIUS 服务器的 IP 地址。
- 加密密钥:** 输入交换机和服务器共享的加密密钥。
- 认证端口:** RADIUS 服务器采用的认证端口号。
- 计费端口:** RADIUS 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:** 交换机等待服务器响应的最大等待时间。

13.7.4 TACACS+配置

本页面可以配置运行 TACACS+安全协议的认证服务器。

进入页面的方法：网络安全 >> AAA >> TACACS+配置

服务器配置

服务器IP: (格式: 192.168.0.2)

超时: s (1-9)

加密密钥:

端口: (1-65535) 添加

服务器列表

选择	服务器IP	超时	加密密钥	端口
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

提交
删除
帮助

图 13-28 TACACS+配置

➤ **配置步骤:**

在**服务器配置**下配置 TACACS+服务器的 IP 地址和其他相关参数，在**服务器列表**下可以查看、编辑或删除已配置好的 TACACS+服务器。

➤ **条目解释:**

- 服务器 IP:** 输入 TACACS+服务器的 IP 地址。
超时: 交换机等待服务器响应的最大等待时间。
加密密钥: 输入交换机你和服务器共享的加密密钥。
端口: TACACS+服务器采用的认证端口号。

13.7.5 服务器组配置

本页面可以将运行相同安全协议的认证服务器设为认证服务器组。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。服务器组中服务器将按条目添加的顺序对用户进行认证。

进入页面的方法：**网络安全 >> AAA >> 服务器组**

添加服务器组

服务器组:

服务器类型: RADIUS ▼ 添加

服务器组列表

选择	服务器组	服务器类型	操作
<input type="checkbox"/>			
<input type="checkbox"/>	radius	RADIUS	编辑
<input type="checkbox"/>	tacacs	TACACS+	编辑

删除
帮助

图 13-29 创建新的服务器组

添加服务器IP

服务器组: auth 添加

服务器类型: RADIUS ▼ 返回

服务器IP: 10.10.10.10 ▼

服务器列表

选择	Server Ip
<input type="checkbox"/>	

删除
帮助

图 13-30 添加服务器到服务器组

➤ **配置步骤**

- 1) 输入新服务器组名并选择服务器类型，点击**添加**，创建服务器组。（图 13-30）
- 2) 在**服务器组列表**中，选择新建的服务器组并点击**编辑**，即可编辑相应的服务器组。（图 13-30）
- 3) 选择在之前已创建的服务器IP，点击**添加**，将该服务器添加到服务器组中。（图 13-31）

➤ **条目解释：**

服务器组：	服务器组名称
服务器类型：	服务器组类型。可以为 RADIUS 或 TACACS+。
服务器 IP：	选择之前已配置好的服务器 IP。



注意：

1. 内置的 radius 服务器组和 tacacs 服务器组不可被编辑或删除。
2. 每个服务器组最多可以包含 16 个服务器。

13.7.6 认证列表

在为某个特定应用配置 AAA 认证之前，需要先定义一个认证方法列表。认证方法列表中定义了对用户的认证方法和认证方法的认证顺序。

交换机先采用列表中第一种方法对用户进行验证，若未得到响应，将选择方法列表中的下一种方法.....照此一致持续下去，直到列表中某种认证方法成功完成了对用户的验证。如果遍历方法列表而仍未得到认证响应，则认证失败。如在认证过程中，某种方法拒绝了用户访问，则认证过程结束，且不再尝试其他的认证方法。

例如，若用户定义了一个认证登录方法列表为 tacacs-radius-local，交换机将向 TACACS+服务器组中的第一个 TACACS+服务器发出认证请求。如果未得到响应，交换机将向第二个 TACACS+服务器发出认证请求.....依此类推，直到有服务器响应。若 TACACS+服务器组中所有服务器都未响应，则交换机会向 RADIUS 服务器组发出认证请求。若在 RADIUS 服务器列表中仍未完成认证，则交换机将会对用户进行本地认证。这种方法可以为用户认证建立一个备份机制。

进入页面的方法：网络安全 >> AAA >> 认证列表

添加方法列表

方法列表名:

列表类型: Login ▼

方法一: -- ▼

方法二: -- ▼

方法三: -- ▼

方法四: -- ▼

Login认证方法列表

选择	方法列表	方法一	方法二	方法三	方法四
<input type="checkbox"/>		-- ▼	-- ▼	-- ▼	-- ▼
<input type="checkbox"/>	default	local	--	--	--

Enable认证方法列表

选择	方法列表	方法一	方法二	方法三	方法四
<input type="checkbox"/>		-- ▼	-- ▼	-- ▼	-- ▼
<input type="checkbox"/>	default	none	--	--	--

图 13-31 认证列表

➤ 配置步骤

- 1) 输入方法列表名称。
- 2) 定义列表类型为Login或Enable。
- 3) 设置认证方法的优先级。可以选择radius, tacacs, local或用户自定义的服务器组。

在 **Login 认证方法列表**和 **Enable 认证方法列表**下可以查看或删除已配置的认证方法优先级列表。

➤ 条目解释：

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。

Login: Login 认证方法列表。

Enable: Enable 认证方法列表。

方法一、二、三、四 按顺序添加认证列表中认证方法。交换机将按照列表中认证方法的顺序对用户进行认证，若某一认证方法未响应，则将尝试使用下一种认证方法进行认证。

local: 使用本地认证。

none: 不需要认证。

radius: 使用所有配置好的 RADIUS 服务器进行认证。

tacacs: 使用所有配置好的 TACACS+服务器进行认证。

组名: 使用选择的服务器组来进行认证。



提示:

若要在远程 RADIUS 服务器上验证 Enable password，交换机将会发送默认认证用户名“\$enable\$”。

13.7.7 应用认证设置

用户可以设置 console, telnet, ssh 和 http 这几种接入方式的认证方法列表。

进入页面的方法：网络安全 >> AAA >> 全局配置

应用认证设置			
选择	模块	Login列表	Enable列表
<input type="checkbox"/>		default ▾	default ▾
<input type="checkbox"/>	console	default	default
<input type="checkbox"/>	telnet	default	default
<input type="checkbox"/>	ssh	default	default
<input type="checkbox"/>	http	default	default

图 13-32 应用认证设置

> 配置步骤

- 1) 选择应用模块。
- 2) 在Login列表下拉菜单中配置用户在登录交换机时的认证方法列表。
- 3) 在Enable列表下拉菜单中配置用户在获取管理员权限时的认证方法列表。

> 条目解释:

- 模块:** 应用模块的名称。
- Login 列表:** 选择应用采用的 Login 认证方法列表。
- Enable 列表:** 选择应用采用的 Enable 认证方法列表。

13.7.8 Dot1x 列表配置

本页面用于设置 802.1x 认证、计费 and IGMP 认证的 RADIUS 服务器组。

进入页面的方法：网络安全 >> AAA >> Dot1x 列表

Dot1x认证方法列表		
选择	方法列表	方法一
<input type="checkbox"/>		radius
<input type="checkbox"/>	default	radius

提交

Dot1x计费方法列表		
选择	方法列表	方法一
<input type="checkbox"/>		radius
<input type="checkbox"/>	default	radius

提交 帮助

图 13-33 Dot1x 列表

➤ 配置 802.1x认证、计费步骤

- 1) 全局配置 802.1x功能并配置和客户端相连的端口。详细配置见 [13.6 802.1X认证](#)。
- 2) 在Dot1x认证方法列表中配置 802.1x认证的RADIUS服务器组。
- 3) 在Dot1x计费方法列表中配置 802.1 计费的RADIUS服务器组。

➤ 配置IGMP认证步骤

- 4) 开启端口的IGMP认证功能。详细配置见 [10.1.9 IGMP认证](#)。
- 5) 在Dot1x认证方法列表中配置IGMP认证的RADIUS服务器组。

13.7.9 默认设置

➤ 默认设置

条目	默认设置
AAA 功能	禁用
Enable password	未定义
RADIUS 服务器	<ul style="list-style-type: none"> ● 认证端口：1812 ● 计费端口：1813 ● 重发次数：2 ● 响应超时：5 秒
TACACA+服务器	<ul style="list-style-type: none"> ● 通信端口：49 ● 响应超时：5 秒
服务器组	默认服务器组：radius 和 tacacs。 所有的 RADIUS 服务器都默认加入 radius 服务器组。 所有的 TACACA+服务器都默认加入 tacacs 服务器组。
Login 认证方法列表	方法一默认为 local ， 默认的登录用户名和密码均为 admin。

条目	默认设置
Enable 认证方法列表	列表为空，表示在无需密码的情况下可以提升用户权限为管理员权限。
应用认证设置	访问方式 console/telnet/ssh/http 都默认采用 Login 列表和 Enable 列表。
802.1X 认证服务器和计费服务器	802.1x 认证、计费和 IGMP 认证都采用 radius 服务器组

13.8 PPPoE 配置

➤ PPPoE 电路 ID 概述

在 ATM 网络中，BRAS(Broadband Remote Access Server, 宽带远程接入服务器)需要通过 DSL (Digital Subscriber Line, 数字用户线) 获取认证和计费过程的唯一信息。PPPoE 电路 ID 插入功能在 DSLAM(Digital Subscriber Line Multiplexer, 数字用户线路接入复用器)中起到替代功能。DSLAM 可以为 PPPoE discovery 报文插入一个 PPPoE Vendor-Specific 标签，这个标签包含了一个唯一线路标识。BRAS 收到打上标签的报文后，提取报文的 Circuit-Id 域，用以在 RADIUS 接入和计费请求中作为 NAS-Port-Id 属性发送给远程的 AAA 服务器。

PPPoE 电路 ID 插入功能提供了添加 Circuit-Id 标签的方法，该标签作为其中一个标识符用于在以太网的认证、授权和计费 (AAA) 接入请求中。启用该功能时，如果接收到的 PPPoE 发现阶段的 PADI(PPPoE Active Discovery Initiation, PPPoE 主动发现初始报文)或 PADR (PPPoE Active Discovery Request, PPPoE 主动发现请求报文)不包含电路 ID 标签，系统将为报文插入 Circuit-Id 标签；如果接收到的 PPPoE 发现阶段的 PADO (PPPoE Active Discovery Offer, PPPoE 主动发现提议报文)或 PADS (PPPoE Active Discovery Session-confirmation, PPPoE 主动发现停止报文)报文包含 Circuit-Id 标签，系统将会移除报文中的 Circuit-Id 标签。

➤ PPPoE 电路 ID 工作流程

PPPoE 电路 ID 工作流程如下图所示：

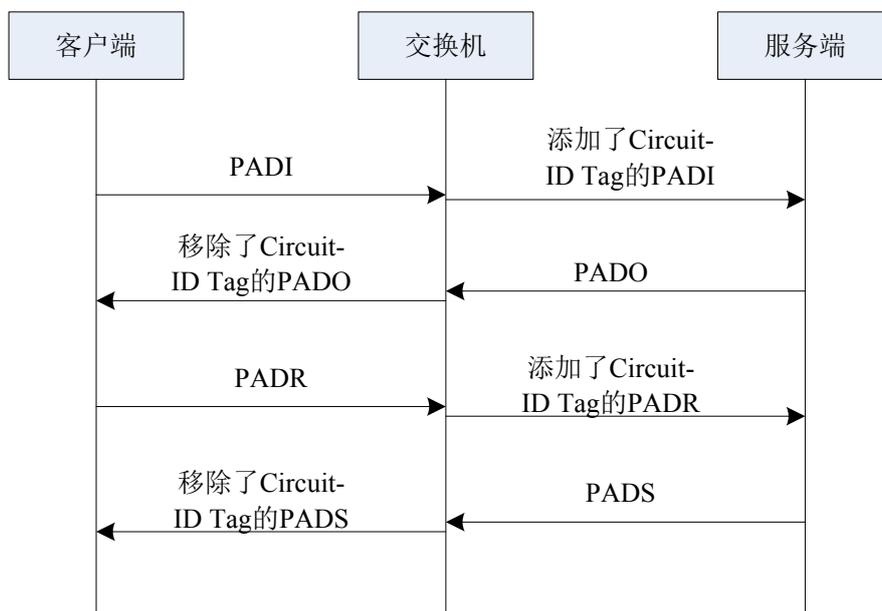


图 13-34 PPPoE Discovery 流程

1. 用户终端发起 PPPoE 请求，发送 PADI 报文；
2. 交换机接收到 PADI 报文并为其添加一个唯一的 Circuit-Id 标签；
3. 交换机转发添加了 Circuit-Id 标签的报文给服务端；
4. 服务端收到添加了 Circuit-Id 标签的 PADI 报文，给用户返回 PADO 报文；
5. 交换机收到 PADO 报文，送 CPU 处理，如果 PADO 报文中的包含有 Circuit-Id 标签，则移除该标签；
6. 交换机转发不含 Circuit-Id 标签的 PADO 报文；
7. 终端按正常流程发送 PADR 报文；
8. 交换机收到 PADR 报文，送 CPU 处理，添加 Circuit-Id 标签；然后转发；
9. 服务端接收到添加了 Circuit-Id 标签的 PADR 报文，为其分配一个 PPP Session ID（服务端把 Circuit-Id 标签提取出来，作为 NAS-Port-ID 的组成部分发送到 RADIUS/PPPoE server）；
10. 服务端返回 PADS 报文；
11. 交换机收到服务端返回的 PADS 报文，送 CPU 处理，如果 PADS 报文中包含有 Circuit-ID tag，则移除该标签，然后转发给客户端。

在 **PPPoE 电路 ID** 页面，可以选择全局开启 PPPoE 电路 ID 功能和开启特定交换机端口的 PPPoE 电路 ID 功能。

进入页面的方法：**网络安全>>PPPoE 配置>>PPPoE 电路 ID**

全局配置

PPPoE电路ID插入: 启用 禁用 提交

端口配置

端口 选择

选择	端口	端口状态	电路ID类型	UDF值
<input type="checkbox"/>		禁用 <input type="button" value="v"/>	IP <input type="button" value="v"/>	<input style="width: 100%;" type="text"/>
<input type="checkbox"/>	1	禁用	IP	---
<input type="checkbox"/>	2	禁用	IP	---
<input type="checkbox"/>	3	禁用	IP	---
<input type="checkbox"/>	4	禁用	IP	---
<input type="checkbox"/>	5	禁用	IP	---
<input type="checkbox"/>	6	禁用	IP	---
<input type="checkbox"/>	7	禁用	IP	---
<input type="checkbox"/>	8	禁用	IP	---
<input type="checkbox"/>	9	禁用	IP	---
<input type="checkbox"/>	10	禁用	IP	---

提交
帮助

图 13-35 PPPoE 电路 ID

条目介绍:

➤ 全局配置

PPPoE 电路 ID 插入: 选择是否启用 PPPoE 电路 ID 插入功能。

➤ 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相应条目。

选择: 勾选端口, 配置端口的 PPPoE 电路 ID 插入功能参数, 可多选。

端口: 显示交换机端口号。

端口状态: 选择是否开启端口的 PPPoE 电路 ID 插入功能。

电路 ID 类型: 选择端口的电路 ID 类型。

- **IP:** 设备 IP 地址将被用于电路 ID 标签的构成内容。这是默认选项。
- **MAC:** 设备 MAC 地址将被用于电路 ID 标签的构成内容。
- **UDF:** 用户自定义的不超过 32 个字符的字符串将被用于电路 ID 标签的构成内容。

UDF 值: 用户自定义的一串不超过 32 个字符的字符串。

[回目录](#)

第14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。

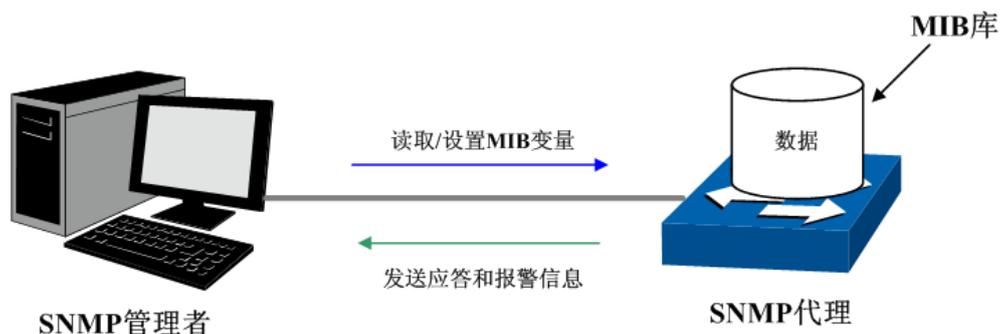


图 14-1 SNMP 网元关系图

➤ 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}。

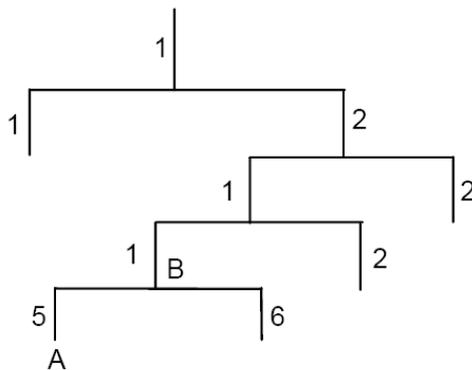


图 14-2 MIB 树结构

➤ 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。

14.1 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。

14.1.1 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**

The image shows a web-based configuration interface for SNMP. It is divided into three sections:

- 全局配置 (Global Configuration):** Contains a radio button for 'SNMP功能' (SNMP Function) with '禁用' (Disabled) selected. A '提交' (Submit) button is to the right.
- 本地引擎配置 (Local Engine Configuration):** Contains a text input for '本地引擎ID' (Local Engine ID) with the value '80002e57030077c66e2d8f'. A '默认ID...' (Default ID...) button is to the right. Below the input is a '提交' (Submit) button.
- 远程引擎配置 (Remote Engine Configuration):** Contains an empty text input for '远程引擎ID' (Remote Engine ID). To the right are '提交' (Submit) and '帮助' (Help) buttons.

注意：
引擎ID的字符个数必须为偶数。

图 14-3 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。

14.1.2 视图管理

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

进入页面的方法：**SNMP>>SNMP 配置>>视图管理**

新建视图

视图名称： (1-16个字符)

MIB子树OID： (1-61个字符) 添加

视图类型： 包括 排除

视图列表

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

全选
删除
帮助

图 14-4 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）。

14.1.3 组管理

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

进入页面的方法：**SNMP>>SNMP 配置>>组管理**

组配置

组名： (1-16个字符)

安全模式：

安全级别：

只读视图：

只写视图：

通知视图：

组列表

选择	组名	安全模式	安全级别	只读视图	只写视图	通知视图	操作
<input type="checkbox"/>							

注意：
一个组必须具备一个只读视图，默认只读视图为viewDefault。

图 14-5 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。若想要进行读写操作, 则需要同时在“只读视图”中添加。

通知视图：选择通知视图, 管理软件可以接收到所选视图发送的异常警报信息。

➤ **组列表**

选择：勾选条目进行删除, 可多选。

组名：显示 SNMP 组的组名。

安全模式：显示组的安全模式。

安全级别：显示组的安全级别。

只读视图：显示组中具有只读权限的视图名称。

只写视图：显示组中具有只写权限的视图名称。

通知视图： 显示组中具有通知权限的视图名称。

操作： 点击对应条目的<编辑>按键，可以修改该条目的视图。修改完毕后点击<修改>按键，修改内容生效。



注意：

一个组必须具备一个只读视图，默认只读视图为 viewDefault。

14.1.4 用户管理

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

进入页面的方法：**SNMP>>SNMP 配置>>用户管理**

用户配置

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

用户列表

选择	用户名	用户类型	组名	安全模式	安全级别	认证模式	加密模式	操作

注意：

用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

图 14-6 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。

14.1.5 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**

注意：

团体的默认MIB视图为viewDefault。

图 14-7 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

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。
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	配置访问权限	直接设置 创建团体	二者必选其一。 <ul style="list-style-type: none"> ● 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。
间接设置 创建 SNMP 组			
间接设置 创建 SNMP 组内的用户			

14.2 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，在 SNMP v2c 和 SNMP v3 中均可以使用。

14.2.1 通知管理

本页用来配置 SNMP 的通知管理功能。

进入页面的方法：**SNMP>>通知管理>>通知管理**

新建条目

IP地址类型:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6						
目的IP地址:	<input type="text"/>	UDP端口:	<input type="text" value="162"/>				
团体名/用户名:	<input type="text"/>						<input type="button" value="添加"/>
安全模式:	<input type="text" value="v1"/>	安全级别:	<input type="text" value="不认证不加密"/>	<input type="button" value="清空"/>			
通知类型:	<input type="text" value="Trap"/>						
重传:	<input type="text"/>	(1-255)					
超时:	<input type="text"/>	秒 (1-3600)					

目的主机列表

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

图 14-8 通知管理

条目介绍:

➤ 新建条目

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

➤ 目的主机列表

- 选择:** 勾选条目进行删除，可多选。
- IP 地址类型:** 选择 IP 地址类型。
- 目的 IP 地址:** 显示管理主机的 IP 地址。

- UDP 端口:** 显示管理主机上启用供通知过程使用的 UDP 端口。
- 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 的用户的的安全级别。
- 通知类型:** 显示使用的通知报文的类型。
- 超时:** 显示 Inform 报文的重传次数。
- 重传:** 显示收到 Inform 报文回应报文的超时时间。
- 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。

14.2.2 上报配置

交换机通过 SNMP 向管理软件上报消息，在这里可以对要上报的事项进行配置。

进入页面的方法：**SNMP>>通知管理>>上报配置**

全局上报配置

<input checked="" type="checkbox"/> SNMP认证	<input checked="" type="checkbox"/> 冷启动	<input checked="" type="checkbox"/> 热启动
<input checked="" type="checkbox"/> 链路状态	<input type="checkbox"/> CPU使用率	<input type="checkbox"/> 内存使用率
<input type="checkbox"/> Flash操作	<input type="checkbox"/> VLAN操作	<input type="checkbox"/> IP变化
<input type="checkbox"/> 风暴抑制	<input type="checkbox"/> 带宽控制	<input type="checkbox"/> LLDP
<input type="checkbox"/> 地址表变化	<input type="checkbox"/> 环路监测	<input type="checkbox"/> 生成树
<input type="checkbox"/> 端口访问控制	<input type="checkbox"/> 四元绑定	<input type="checkbox"/> IP冲突
<input type="checkbox"/> DHCP过滤		

端口上报配置

端口

选择	端口	链路状态
<input type="checkbox"/>		禁用 <input type="button" value="v"/>
<input type="checkbox"/>	1	启用
<input type="checkbox"/>	2	启用
<input type="checkbox"/>	3	启用
<input type="checkbox"/>	4	启用
<input type="checkbox"/>	5	启用
<input type="checkbox"/>	6	启用
<input type="checkbox"/>	7	启用
<input type="checkbox"/>	8	启用
<input type="checkbox"/>	9	启用
<input type="checkbox"/>	10	启用
<input type="checkbox"/>	11	启用
<input type="checkbox"/>	12	启用

图 14-9 通知管理

条目介绍:

➤ 全局上报配置

SNMP 认证:	SNMP 认证失败。
冷启动:	交换机进行了重新启动。
热启动:	SNMP 功能进行了重新使能。
链路状态:	端口的启动/禁用状态发生了变化。
CPU 使用率:	CPU 使用率超过了 80%。
内存使用率:	内存使用率超过了 80%。
Flash 操作:	对 Flash 进行了操作。
VLAN 操作:	创建或者删除了 VLAN。
IP 变化:	交换机 IP 发生了变化。
风暴抑制:	违反了带宽控制规则。
带宽控制:	违反了带宽控制规则。
LLDP:	LLDP 的状态发生了变化。
地址表变化:	MAC 地址表有变化。
环路监测:	环路监测的状态发生了变化。
生成树:	STP 协议的状态发生了变化。
端口访问控制:	违反了端口访问控制的规则。
四元绑定:	违反了四元绑定的规则。
IP 冲突:	有别的主机使用了与本交换机相同的 IP。
DHCP 过滤:	在不允许的端口收到了 DHCP 报文。

➤ 端口上报配置

端口选择:	点击【选择】按键，可根据所输端口号快速查找相应条目。
选择:	勾选端口，配置端口上报功能参数，可多选。
端口:	显示交换机的端口号。
链路状态:	选择端口是否允许上报链路状态信息。

14.3 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, 从而有效的监控网络。	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	监控报警变量在指定端口的统计值。	丢弃数据包、丢弃字节、数据包发送、广播数据包、组播数据包、CRC 错误帧、过小 (或超大) 的数据报文、冲突帧以及各种长度的数据包, 包括 64、65~127、128~255、256~511、512~1023 以及 1024~10240 字节。
警报组	定期对指定的警报变量进行监控, 一旦计数器超过阈值则触发警报。	警报变量、样例类型、时间间隔、阈值上限、阈值下限、警报触发方式。

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

14.3.1 历史采样

本页用来配置 RMON 的历史组。

进入页面的方法：**SNMP>>RMON>>历史采样**

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

图 14-10 历史采样

条目介绍：

➤ 历史采样控制

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

14.3.2 事件配置

本页用来配置 RMON 的事件组。

进入页面的方法：**SNMP>>RMON>>事件配置**

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

图 14-11 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。

14.3.3 警报管理

本页用来配置 RMON 的统计组和警报组。

进入页面的方法: **SNMP>>RMON>>警报管理**

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

图 14-12 警报配置

条目介绍:

➤ 事件配置

- 选择:** 勾选条目配置警报属性。
- 序号:** 显示警报条目的序号。
- 计数器:** 选择警报变量。
- 端口:** 选择进行警报监视的端口号。
- 样例类型:** 为警报变量选择取样的方法,再将取样的值与阈值进行比较。

- 绝对值：在一个取样周期结束时将取样结果与阈值进行比较。
 - 增量：将现在值减去上一次取样值之后的增量与阈值进行比较。
- 上升阈值：** 填写触发警报的上升阈值。默认为 100。
- 上升事件：** 选择触发上升阈值警报的事件的序号。
- 下降阈值：** 填写触发警报的下降阈值。默认为 100。
- 下降事件：** 选择触发下降阈值警报的事件的序号。
- 启动警报：** 选择警报触发的方式。
- 上升：只在触发上升阈值后触发警报。
 - 下降：只在触发下降阈值后触发警报。
 - 全部：触发上升和下降阈值均触发警报。
- 时间间隔：** 填写警报的时间间隔。默认为 1800 秒。
- 创建者：** 填写创建该警报条目的实体。
- 状态：** 选择是否启用所选警报条目。

**注意：**

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

[回目录](#)

第15章 LLDP

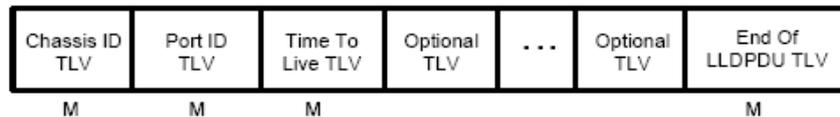
链路层发现协议 LLDP (Link Layer Discovery Protocol) 是一个二层协议, 在符合 IEEE802 标准的局域网中, 允许网络设备周期性地向邻居设备通告自己的设备信息。LLDP 根据 IEEE802.1AB 标准把设备的标识、性能和配置等信息组织成不同的 TLV (Type/Length/Value, 类型/长度/值), 并封装在 LLDPU (Link Layer Discovery Protocol Data Unit, 链路层发现协议数据单元) 中发布给邻居设备, 邻居设备收到这些信息后将其以标准的 MIB (Management Information Base, 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。

➤ LLDPU

每一个 LLDPU 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 LLDPU 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。



M - mandatory TLV - required for all LLDPU

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

2) LLDPU 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 LLDPU 以通告自己的信息。

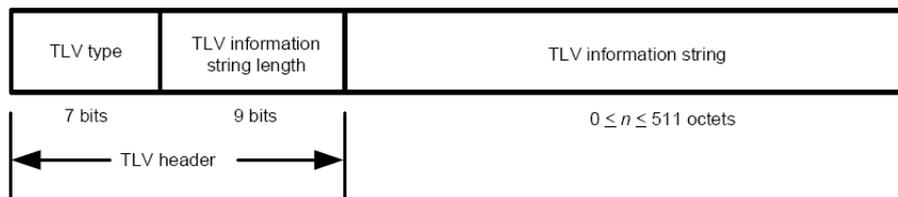
- 当本地设备发生变化时，设备会发送变化通告。当本地设备在短时间内频繁变化时，为避免设备连续地发送 LLDPDU 而导致网络阻塞，NMS（Network Management System，网络管理系统）将会设定一个报文发送时延，以确保 LLDPDU 的发送有一个固定的最小时间差。
- 当端口的工作模式由禁用或者只接收模式切换为发送接收模式或者只发送模式时，该设备的快速启动机制将被激活，报文的发送间隔变为 1s，快速发出一些 LLDPDU 之后，设备恢复正常的发送周期。

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
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 IEE 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**和**设备统计**三个部分。

15.1 基本配置

本功能包括**基本配置**和**端口配置**两个功能配置页面。

15.1.1 基本配置

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>>基本配置**

The screenshot shows a web-based configuration interface for LLDP. It is divided into two main sections: '全局配置' (Global Configuration) and '参数配置' (Parameter Configuration). In the '全局配置' section, there is a radio button for 'LLDP功能' (LLDP Function) with '禁用' (Disabled) selected and '启用' (Enabled) unselected, and a '提交' (Submit) button. The '参数配置' section contains several input fields with their respective units and ranges: '发送间隔' (Send Interval) set to 30 seconds (range 5-32768), 'TTL乘数' (TTL Multiplier) set to 4 (range 2-10), '发送延迟时间' (Send Delay Time) set to 2 seconds (range 1-8192), '初始化延迟时间' (Initialization Delay Time) set to 3 seconds (range 1-10), 'Trap信息间隔' (Trap Information Interval) set to 5 seconds (range 5-3600), and '快速报文个数' (Fast Packet Count) set to 3 (range 1-10). There are '提交' (Submit) and '帮助' (Help) buttons at the bottom right of the parameter configuration section.

图 15-1 基本配置

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。默认为 30 秒。

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。默认值为 4。

发送延迟时间: 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。默认值为 2 秒。

初始化延迟时间: 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。默认值为 3 秒。

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。默认值为 5 秒。

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。默认值为 3 个。

15.1.2 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**

选择	端口	端口状态	SNMP通知	TLV字段
<input type="checkbox"/>		禁用	禁用	
<input type="checkbox"/>	1	发送接收	禁用	详细信息
<input type="checkbox"/>	2	发送接收	禁用	详细信息
<input type="checkbox"/>	3	发送接收	禁用	详细信息
<input type="checkbox"/>	4	发送接收	禁用	详细信息
<input type="checkbox"/>	5	发送接收	禁用	详细信息
<input type="checkbox"/>	6	发送接收	禁用	详细信息
<input type="checkbox"/>	7	发送接收	禁用	详细信息
<input type="checkbox"/>	8	发送接收	禁用	详细信息
<input type="checkbox"/>	9	发送接收	禁用	详细信息
<input type="checkbox"/>	10	发送接收	禁用	详细信息
<input type="checkbox"/>	11	发送接收	禁用	详细信息
<input type="checkbox"/>	12	发送接收	禁用	详细信息
<input type="checkbox"/>	13	发送接收	禁用	详细信息
<input type="checkbox"/>	14	发送接收	禁用	详细信息

图 15-2 端口配置

条目介绍:

➤ **LLDP 端口配置**

端口选择:

点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择:

勾选端口配置端口参数，可多选。

端口:

显示交换机的端口号。

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。

详细信息: 点击此按键，将显示 TLV 字段详细信息。

15.2 设备信息

本功能包括本地信息和邻居信息两个配置页面。

15.2.1 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**

自动刷新

自动刷新: 启用 禁用 提交

刷新周期: 秒 (3-300)

本地信息

端口 选择

本地端口:	1
Chassis ID 类型:	Reserved
Chassis ID:	
Port ID 类型:	Reserved
Port ID:	
TTL:	0
端口描述:	
系统名称:	
系统描述:	
系统能力:	
系统使能:	
管理地址:	0.0.0.0

刷新
帮助

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。默认为 30 秒。

➤ **本地信息**

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。

本地端口: 显示本地端口号。

Chassis ID 类型:	显示 Chassis ID 的类型，默认为 MAC 地址。
Chassis ID:	显示本地设备的 Chassis ID 值。
Port ID 类型:	显示本端口的 ID 类型。
Port ID:	显示本端口的端口 ID 值。
TTL:	显示从本端口发送出去的 LLDPDU 中包含的 TLV 中的 TTL 值。
端口描述:	显示本端口的端口描述信息。
系统名称:	显示本地设备的系统名称。
系统描述:	显示本地设备的系统描述信息。
系统能力:	显示本地设备支持的功能。
系统使能:	显示本地设备已经使能的功能。
管理地址:	显示本地设备的管理地址信息。

15.2.2 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。

刷新速度: 填写自动刷新的时间周期。默认为 30 秒。

➤ 邻居设备信息

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。

本地端口: 显示本地端口号。

- 系统名称:** 显示邻居的系统名称。
- Chassis ID:** 显示邻居设备的 Chassis ID 值。
- 系统描述:** 显示邻居的系统描述信息。
- 邻居端口:** 显示连接到本地端口的邻居端口号。
- 详细信息:** 点击此按钮可以查看更详细的邻居信息。

15.3 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**

自动刷新

自动刷新： 启用 禁用

刷新周期： 秒 (3-300) 提交

全局统计信息

更新时间	创建邻居数量	删除邻居数量	丢弃邻居数量	老化邻居数量
00:00:00:00	0	0	0	0

端口统计信息

端口 选择

端口	发送报文	接收报文	丢弃报文	错误报文	老化邻居	丢弃TLV	未知TLV
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0

刷新
清空
帮助

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。默认为 30 秒。

➤ 全局统计信息

更新时间:	显示此统计数据的更新时间。
创建邻居数量:	显示最新更新时本地设备已经创建的邻居数量。
删除邻居数量:	显示最新更新时本地设备已经删除的邻居数量。
丢弃邻居数量:	显示最新更新时本地设备已经丢弃的邻居数量。
老化邻居数量:	显示最新更新时本地设备上已经老化的邻居数量。

➤ 端口统计信息

端口选择:	点击<选择>按键, 可根据所输端口号, 快速选择相应端口。
端口:	显示本地端口号。
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。
老化邻居:	显示本端口连接的邻居设备中老化邻居的数量。
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。

[回目录](#)

第16章 集群管理

随着网络技术的发展，网络的规模越来越大，网络设备的数量越来越多，所以网络管理也就越来越烦琐。数量众多的设备需要分配不同的网络地址，每台管理设备均需要单独配置之后才能够满足应用的需要，以上这些造成管理人员很大的压力。

集群管理可以很好地解决上述问题。集群是可以当作单一设备来管理的一组网络设备的集合，集群管理的主要目的是解决大量分散的网络设备的集中管理问题。网络管理者通过集群中的一个交换机就可以实现对集群中其他交换机的管理和维护；其中执行管理功能的交换机是命令交换机，其他被管理的交换机是成员交换机，命令交换机和成员交换机组成了一个“集群”。典型组网应用如图 16-1 所示。

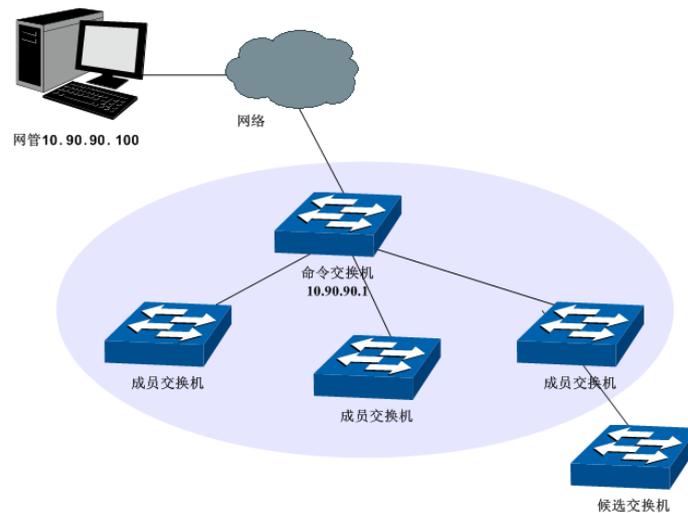


图 16-1 集群典型应用组网图

► 集群角色

由于各个交换机在集群中所处的地位和功能的不同，形成了不同的角色，可以配置交换机在集群中的角色。集群的角色有三种：

命令交换机：在集群中，唯一的可以配置和管理整个集群的交换机。命令交换机通过收集 NDP（Neighbor Discovery Protocol，邻居发现协议）和 NTDP（Neighbor Topology Discovery Protocol，邻居拓扑发现协议）信息来发现和确定候选交换机。

成员交换机：集群中被管理的交换机。

候选交换机：具有加入集群能力，但还没有加入任何集群的交换机。

独立交换机：未启用集群功能的交换机。

各种集群角色可以按一定的规则进行转换：

- 用户在交换机上创建集群的同时，将当前交换机指定为命令交换机。
- 命令交换机通过收集相关信息，发现和确定候选交换机。
- 候选交换机加入集群后，成为成员交换机。
- 集群内的成员交换机被删除后将恢复为候选交换机。
- 命令交换机只有在删除集群时才能恢复为候选交换机。

➤ 集群工作原理

集群通过 NDP、NTDP、CMP（Cluster Management Protocol，集群管理协议）三个协议，对集群内部的交换机进行配置和管理。

集群的过程分为拓扑发现、拓扑收集和集群的建立维护，具体工作过程如下：

- 拓扑发现：所有交换机通过 NDP 来获取邻居交换机的信息。
- 拓扑收集：命令交换机通过 NTDP 来收集网络内指定跳数范围内的交换机信息以及各个交换机的连接信息，并从收集到的拓扑信息中确定集群的候选交换机。
- 集群建立维护：命令交换机根据 NTDP 收集到的候选设备信息完成将候选交换机加入集群、成员交换机离开集群等集群管理操作。

集群管理模块主要用于配置交换机的集群管理功能，包括**拓扑发现**、**拓扑收集**以及**集群管理**三个部分。

16.1 拓扑发现

集群中的交换机使用 NDP 来获取与其直接相连的邻居交换机的信息。交换机周期性地向邻居发送 NDP 报文，同时也会接收但不转发邻居交换机发送的 NDP 报文。NDP 报文中包含 NDP 信息（包括本交换机的名称、MAC 地址、软件版本等信息）等。

交换机会存储和维护一个邻居信息表，邻居信息表里包含每个邻居交换机的 NDP 信息表项。如果交换机收到新邻居的 NDP 信息，则会在邻居信息表新增一个表项；如果从邻居交换机收到的 NDP 信息与旧的信息不同，则更新邻居信息表中的数据，如果相同，则只更新老化时间，如果超过老化时间还没有收到邻居发送的 NDP 信息，将自动删除相应的邻居表项。

本功能包括**邻居信息**、**配置显示**和**全局配置**三个配置页面。

16.1.1 邻居信息

在本页可以查看交换机的 NDP 邻居信息表。

进入页面的方法：**集群管理>>拓扑发现>>邻居信息**



图 16-2 邻居信息

条目介绍：

➤ 邻居查找

查找选项： 选择欲查找条目需包含的信息。

➤ 邻居信息

本地端口： 显示本交换机的端口号。

远程端口：	显示与相应端口相连的邻居交换机的端口号。
设备名称：	显示邻居交换机的名称。
设备 MAC：	显示邻居交换机的 MAC 地址。
软件版本：	显示邻居交换机的软件版本。
老化时间：	显示邻居交换机发送的 NDP 报文在本交换机上的剩余时间。

16.1.2 配置显示

在本页可以查看交换机的 NDP 配置信息。

进入页面的方法：[集群管理](#)>>[拓扑发现](#)>>[配置显示](#)

全局配置

NDP状态：	启用
老化定时器：	180秒
Hello定时器：	60秒

端口状态						
端口	NDP状态	发送NDP包数	接收NDP包数	错误NDP包数	邻居数	详细信息
1	启用	0	0	0	0	详细信息
2	启用	0	0	0	0	详细信息
3	启用	0	0	0	0	详细信息
4	启用	0	0	0	0	详细信息
5	启用	0	0	0	0	详细信息
6	启用	0	0	0	0	详细信息
7	启用	0	0	0	0	详细信息
8	启用	0	0	0	0	详细信息
9	启用	0	0	0	0	详细信息
10	启用	0	0	0	0	详细信息
11	启用	0	0	0	0	详细信息
12	启用	0	0	0	0	详细信息

刷新
帮助

图 16-3 配置显示

条目介绍：

➤ 全局配置

NDP 状态：	显示本交换机的全局 NDP 状态。
老化定时器：	显示本交换机发送的 NDP 报文在邻居交换机上的老化时间。
Hello 定时器：	显示本交换机 NDP 报文发送的间隔时间。

➤ 端口状态

- 端口：** 显示交换机的端口号。
- NDP 状态：** 显示当前端口的 NDP 状态。
- 发送 NDP 包数：** 显示端口当前发送的 NDP 数据包数。
- 接收 NDP 包数：** 显示端口当前接收的 NDP 数据包数。
- 错误 NDP 包数：** 显示端口当前接收到的错误 NDP 数据包数。
- 邻居数：** 显示端口所连接的邻居交换机数。
- 详细信息：** 点击此按钮，将显示该端口的收集到的邻居信息。

16.1.3 全局配置

在本页可以配置交换机的 NDP 功能。

进入页面的方法：集群管理>>拓扑发现>>全局配置

全局配置

NDP状态： 启用 禁用

老化定时器： 秒（5-255，默认为180）

Hello定时器： 秒（5-254，默认为60）

端口状态

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

图 16-4 全局配置

条目介绍:

➤ 全局配置

- NDP 状态:** 选择是否启用全局 NDP 功能。
- 老化定时器:** 填写本交换机发送的 NDP 报文在接收设备上的老化时间。默认为 180 秒。
- Hello 定时器:** 填写本交换机 NDP 报文发送的时间间隔。默认为 60 秒。

➤ 端口状态

- 选择:** 勾选端口配置端口 NDP 状态。
- 端口:** 显示交换机的端口号。
- NDP 状态:** 显示端口当前的 NDP 状态。
- 启用:** 点击后启用所选端口的 NDP 功能。
- 禁用:** 点击后禁用所选端口的 NDP 功能。



注意:

- 必须在全局配置和端口状态中同时启用 NDP 状态，NDP 功能才能正常运行。
- 老化定时器时间要大于 Hello 定时器时间，否则将引起 NDP 端口邻居信息表的不稳定。

16.2 拓扑收集

NTDP 用于命令交换机收集整个网络指定跳数的拓扑信息。NTDP 根据 NDP 邻居信息表发送和转发 NTDP 拓扑收集请求，收集指定跳数内的网络中每个交换机的 NDP 信息及其连接信息。命令交换机可以定时在网络内进行拓扑收集，也可以随时在命令交换机上手动启用拓扑收集。

命令交换机发送拓扑收集请求报文后，大量交换机会同时收到拓扑收集请求并同时发送拓扑收集响应报文，如此以来可能造成网络拥塞和命令交换机负担过重。为了避免上述现象的产生，设计了两个时间参数来控制拓扑收集请求报文扩散速度：

- 请求跳数延迟时间：交换机收到拓扑收集请求，会等待该时间段之后，才开始在第一个启用 NTDP 的端口转发该拓扑收集请求报文。
- 端口跳数延迟时间：在同一个交换机上，除第一个端口外，每个启用 NTDP 功能的端口在前一个端口发送拓扑收集请求报文后，都会等待该时间段，再进行拓扑收集请求报文的转发。

本功能包括**设备列表**、**配置显示**和**全局配置**三个配置页面。

16.2.1 设备列表

在此处可以查看 NTDP 收集到的设备信息。同时，无论集群是否建立，都可以在本页随时手动收集 NTDP 信息，从而更有效地对设备进行实时管理与监控。

进入页面的方法：集群管理>>拓扑收集>>设备列表

设备信息列表					
设备类型	设备MAC	集群名	角色	跳数	邻居信息
TL-SL5428 1.0	00-9B-BD-01-3C-DD	name1	命令交换机	0	详细信息

图 16-5 设备列表

条目介绍：

➤ 设备信息列表

- 设备类型：** 显示 NTDP 所收集到的设备信息。
- 设备 MAC：** 显示该设备的 MAC 地址。
- 集群名：** 显示该设备的集群名称。
- 角色：** 显示该设备在集群中的角色。
- 命令交换机：配置并管理集群的交换机。
 - 成员交换机：在集群中被管理的交换机。
 - 候选交换机：能够成为集群成员但是还未加入集群的交换机。
 - 独立交换机：未启用集群功能的交换机。
- 跳数：** 显示该设备距离本交换机的跳数。
- 邻居信息：** 点击<详细信息>，可以查看该设备的详细信息及其邻居信息表。

点击<详细信息>按键后，可以看到 NTDP 收集到的该设备的详细信息。

当前设备信息				
设备名称：	name1_0.TL-SL5428			
MAC：	00-9B-BD-01-3C-DD			
跳数：	0			
设备类型：	TL-SL5428 1.0			
IP地址：	192.168.0.1			
软件版本：	2.1.8 Build 20131031 Rel.35865			
集群信息：	集群name1的命令交换机			

邻居信息				
本地端口	远程端口	设备MAC	速度(Mbit/s)	双工
<input type="button" value="返回"/>				

图 16-6 当前设备信息

16.2.2 配置显示

在本页可以查看交换机的 NTDP 配置信息。

进入页面的方法：[集群管理](#)>>[拓扑收集](#)>>[配置显示](#)

全局配置			
NTDP状态：	启用		
拓扑收集间隔时间：	1分钟		
拓扑收集跳数：	3跳		
请求跳数延迟时间：	200毫秒		
端口跳数延迟时间：	20毫秒		

端口状态			
端口	NTDP状态	端口	NTDP状态
1	启用	2	启用
3	启用	4	启用
5	启用	6	启用
7	启用	8	启用
9	启用	10	启用
11	启用	12	启用
13	启用	14	启用
15	启用	16	启用
17	启用	18	启用
19	启用	20	启用
21	启用	22	启用
23	启用	24	启用
25	启用	26	启用
27	启用	28	启用

图 16-7 配置显示

条目介绍：

➤ 全局配置

- NTDP 状态：** 显示本交换机的全局 NTDP 状态。
- 拓扑收集间隔时间：** 显示本交换机拓扑信息收集的周期。
- 拓扑收集跳数：** 显示本交换机拓扑收集的范围。
- 请求跳数延迟时间：** 显示本交换机在收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。
- 端口跳数延迟时间：** 显示本交换机在相邻端口转发拓扑请求报文的延时时间。

➤ 端口状态

- 端口：** 显示交换机的端口号。
- NTDP 状态：** 显示当前端口的 NTDP 状态。

16.2.3 全局配置

在本页可以配置交换机的 NTDP 功能。

进入页面的方法：[集群管理](#)>>[拓扑发现](#)>>[全局配置](#)

全局配置

NTDP状态： 启用 禁用

拓扑收集间隔时间： 分钟（1-60，默认为1）

拓扑收集跳数： 跳（1-16，默认为3） 提交

请求跳数延迟时间： 毫秒（1-1000，默认为200）

端口跳数延迟时间： 毫秒（1-100，默认为20）

端口状态

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

全选
启用
禁用
帮助

图 16-8 全局配置

条目介绍：

➤ 全局配置

- NTDP 状态：** 选择是否启用全局 NTDP 功能。
- 拓扑收集间隔时间：** 填写本交换机拓扑信息收集的周期。默认为 1 分钟。
- 拓扑收集跳数：** 填写本交换机拓扑收集的范围。默认为 3 跳。
- 请求跳数延迟时间：** 填写本交换机在收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。默认为 200 毫秒。
- 端口跳数延迟时间：** 填写本交换机在相邻端口转发拓扑请求报文的延时时间。默认为 20 毫秒。

➤ 端口状态

- 选择：** 勾选端口配置端口 NTDP 状态。

- 端口：** 显示交换机的端口号。
- NTDP 状态：** 显示端口当前的 NTDP 状态。
- 启用：** 点击后启用所选端口的 NTDP 功能。
- 禁用：** 点击后禁用所选端口的 NTDP 功能。

**注意：**

必须在全局配置和端口状态中同时启用 NTDP 状态，NTDP 功能才能正常运行。

16.3 集群管理

命令交换机通过 NDP 和 NTDP 协议发现和确定候选交换机，并将候选交换机自动加入集群，也可以通过手动配置将候选交换机加入到集群中。候选交换机成功加入集群后，将获得由命令交换机为它分配的私有 IP 地址。可以在命令交换机上直接访问成员交换机的 Web 页面，对成员交换机进行管理。

本功能包括**配置显示**、**集群配置**、**成员管理**和**拓扑图**四个配置页面。

16.3.1 配置显示

在本页可以查看到当前集群的状态。

进入页面的方法：**集群管理>>集群管理>>配置显示**

- 当前交换机为候选交换机时，可以看到：

全局配置

集群状态： 启用

集群角色： 候选交换机

刷新

帮助

图 16-9 候选交换机的配置显示

条目介绍：

➤ 全局配置

集群状态： 显示当前交换机的集群状态。

集群角色： 显示交换机在集群中的角色。

- 当前交换机为命令交换机时，可以看到：



图 16-10 命令交换机的配置显示

条目介绍：

➤ 全局配置

集群状态： 显示当前交换机的集群状态。

集群角色： 显示交换机在集群中的角色。

集群名： 显示交换机当前的集群名称。

➤ 集群设置

集群地址池、掩码： 显示集群中成员交换机的私有 IP 地址范围。

保持时间： 显示集群信息在命令交换机中保存的时间。

时间间隔： 显示本交换机与成员交换机握手报文的时间间隔。

TFTP 服务器： 显示 TFTP 服务器的 IP 地址。

➤ 成员信息

设备名称： 显示成员交换机的名称。

设备 MAC： 显示成员交换机的 MAC 地址。

IP 地址： 显示成员交换机在集群中的 IP 地址。

状态： 显示成员交换机的连通性。

角色： 显示交换机当前的集群角色。

加入集群时间： 显示成员交换机加入集群的时间。

跳数： 显示成员交换机距离命令交换机的跳数。

- 当前交换机为成员交换机时，可以看到：



图 16-11 成员交换机的配置显示

条目介绍：

➤ 全局配置

- 集群状态：** 显示当前交换机的集群状态。
- 集群角色：** 显示交换机在集群中的角色。
- 集群名：** 显示交换机当前的集群名称。
- 命令交换机 MAC：** 显示命令交换机的 MAC 地址。

- 当前交换机为独立交换机时，可以看到：



图 16-12 独立交换机的配置显示

条目介绍：

➤ 全局配置

- 集群状态：** 显示当前交换机的集群状态。
- 集群角色：** 显示交换机在集群中的角色。

16.3.2 集群配置

在本页可以配置交换机的集群状态。

进入页面的方法：**集群管理>>集群管理>>集群配置**

- 当前交换机为候选交换机时，可以看到：

当前角色

集群角色： 候选交换机

角色转换

集群角色转换： 独立交换机 命令交换机

集群名： (1-16个字符)

集群地址池： 掩码：

图 16-13 候选交换机的集群配置

条目介绍：

➤ 当前角色

集群角色： 显示交换机在集群中的角色。

➤ 角色转换

独立交换机： 将交换机的集群角色转换为独立交换机。

命令交换机： 将交换机的集群角色转换为命令交换机。之后，还需要配置集群的基本属性：

- 集群名：配置交换机当前的集群名称。
- 集群地址池、掩码：配置集群中成员交换机的私有 IP 地址范围。

- 当前交换机为命令交换机时，可以看到：

当前角色

集群角色： 命令交换机

角色转换

集群角色转换： 候选交换机

集群配置

保持时间： 秒 (1-255)

时间间隔： 秒 (1-255)

TFTP 服务器：

图 16-14 命令交换机的集群配置

条目介绍：

➤ 当前角色

集群角色： 显示交换机在集群中的角色。

➤ 角色转换

候选交换机： 将交换机的集群角色转换为候选交换机。

➤ 集群配置

保持时间： 填写集群信息在命令交换机中保存的时间。

时间间隔： 填写命令交换机与成员交换机握手报文的时间间隔。

TFTP 服务器： 填写 TFTP 服务器的 IP 地址。

- 当前交换机为成员交换机时，可以看到：

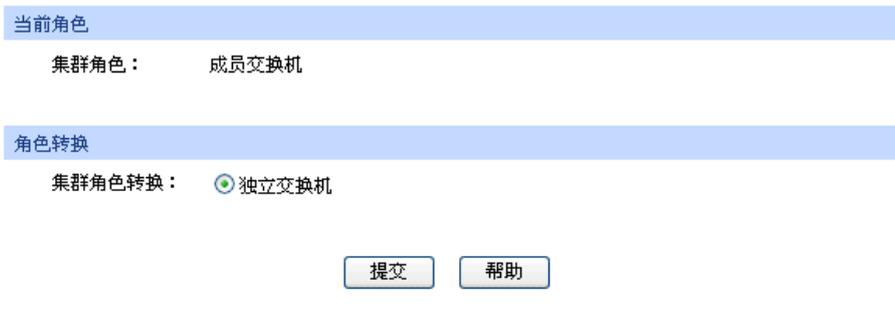


图 16-15 成员交换机的集群配置

条目介绍：

➤ 当前角色

集群角色： 显示交换机在集群中的角色。

➤ 角色转换

独立交换机： 将交换机的集群角色转换为独立交换机。

- 当前交换机为独立交换机时，可以看到：

图 16-16 独立交换机的集群配置

条目介绍：

➤ 当前角色

集群角色： 显示交换机在集群中的角色。

➤ 角色转换

候选交换机： 将交换机的集群角色转换为候选交换机。

16.3.3 成员管理

当交换机为集群中的命令交换机时，可以在命令交换机上手动指定要加入集群的候选交换机，也可以手动删除集群中指定的成员交换机，同时也可以在本页对成员交换机进行配置管理。

进入页面的方法：**集群管理>>集群管理>>成员管理**

选择	设备名称	设备MAC	IP地址	状态	角色	加入集群时间	跳数
<input checked="" type="checkbox"/>	WD_1.TL-SL5428	00-3C-95-1D-DF-1F	192.168.0.2	在线	成员交换机	0:00:41	1

图 16-17 成员管理

条目介绍：

➤ 手动成员加入

成员 MAC： 填写候选交换机的 MAC 地址。

➤ 成员信息

选择： 勾选条目进行管理或删除操作。

设备名称： 显示成员交换机的名称。

设备 MAC:	显示成员交换机的 MAC 地址。
IP 地址:	显示成员交换机在集群中的 IP 地址。
状态:	显示成员交换机的连通性。
角色:	显示交换机当前的集群角色。
加入集群时间:	显示成员交换机加入集群的时间。
跳数:	显示成员交换机距离本交换机的跳数。
管理:	勾选条目后点击此按键，进入相应的成员交换机的 Web 页面。

16.3.4 拓扑图

在本页可以看到集群的整个拓扑结构图，也可以点击节点交换机直接进入相应的管理页面，从而对该交换机进行配置管理。同时双击拓扑图上的各个节点交换机，可以看到该交换机的详细信息。

进入页面的方法：**集群管理>>集群管理>>拓扑图**

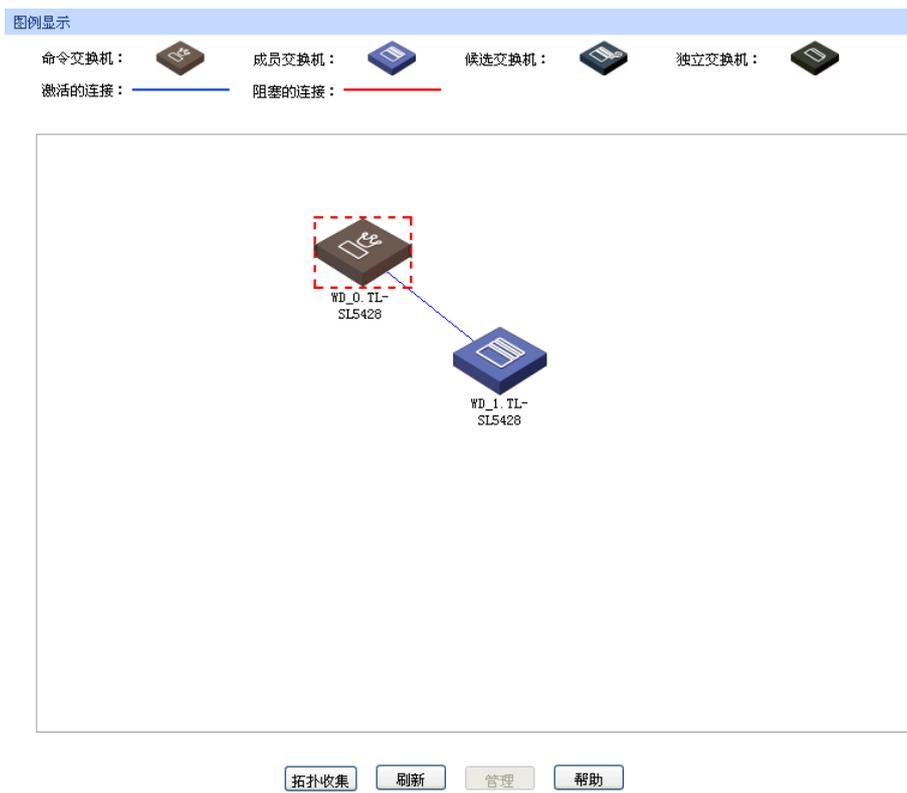


图 16-18 拓扑图

条目介绍:

➤ **图例显示**

拓扑收集: 点击此按键后将集群内的拓扑信息以拓扑图的形式展现出来。

管理： 如果当前设备为集群中的命令交换机，并且选中的设备为此集群中的成员交换机，那么点击此按键，将进入相应交换机的管理页面。

集群管理功能全局配置步骤：

在配置集群之前，首先需要明确集群内各交换机的角色及功能，做好集群的规划工作。

➤ 若此交换机为命令交换机。

步骤	操作	说明
1	启用系统和端口的 NDP 功能，并配置 NDP 参数	可选操作。在 集群管理>>拓扑发现>>全局配置 页面，启用交换机的 NDP 功能。
2	启用系统和端口的 NTDP 功能，并配置 NTDP 参数	可选操作。在 集群管理>>拓扑收集>>全局配置 页面，启用交换机的 NTDP 功能。
3	建立集群，并配置集群参数	可选操作。在 集群管理>>集群管理>>集群配置 页面，建立集群并配置集群参数。
4	管理集群设备	可选操作。 在 集群管理>>集群管理>>成员管理 页面，选择成员交换机，点击<管理>按键，即可进入该成员交换机的 Web 页面进行管理。 也可在 集群管理>>集群管理>>拓扑图 页面，双击交换机图标，可以查看该交换机的详细信息；单击交换机的图标，点击<管理>按键，即可进入该成员交换机的 Web 页面进行管理。

➤ 若此交换机为成员交换机。

步骤	操作	说明
1	启用系统和端口的 NDP 功能	可选操作。在 集群管理>>拓扑发现>>全局配置 页面，启用交换机的 NDP 功能。
2	启用系统和端口的 NTDP 功能	可选操作。在 集群管理>>拓扑收集>>全局配置 页面，启用交换机的 NTDP 功能。
3	手动收集拓扑信息	可选操作。 在 集群管理>>拓扑收集>>设备列表 页面，点击<拓扑收集>按键，手动收集拓扑信息。 也可在 集群管理>>集群管理>>拓扑图 页面，点击<拓扑收集>按键，手动收集拓扑信息。
4	查询集群中其它交换机的详细信息	在 集群管理>>集群管理>>拓扑图 页面，双击交换机图标，可以查看该交换机的详细信息。

16.4 集群管理功能组网应用

➤ 组网需求

三台交换机构成一个集群，其中：一台为命令交换机（以我司交换机 TL-SL5428 为例）、其它交换机为成员交换机（以我司交换机 TL-SL3428 为例）。网管通过命令交换机来管理整个集群。

- 命令交换机的端口 1 与外网连接，端口 2、端口 3 分别与成员交换机 1、成员交换机 2 连接。
- 集群地址池：175.128.0.1；掩码：255.255.255.0。

➤ 组网图

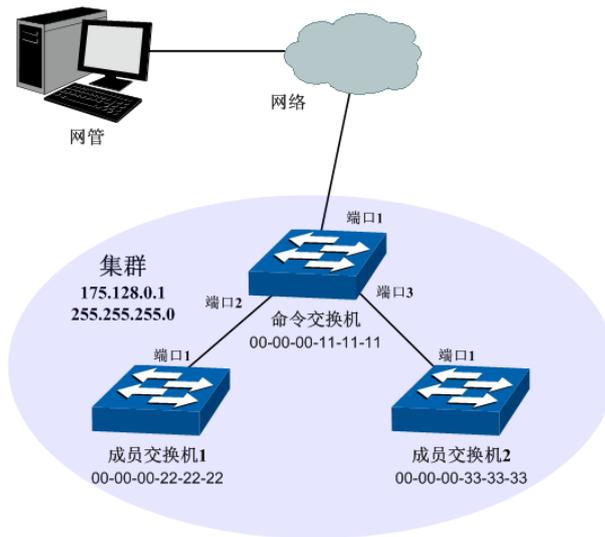


图 16-19 集群管理组网图

➤ 配置步骤

- 配置成员交换机

步骤	操作	说明
1	启用系统和端口 1 的 NDP 功能	在 集群管理>>拓扑发现>>全局配置 页面，启用交换机的 NDP 功能。
2	启用系统和端口 1 的 NTDP 功能	在 集群管理>>拓扑收集>>全局配置 页面，启用交换机的 NTDP 功能。

- 配置命令交换机

步骤	操作	说明
1	启用系统和端口 1、2、3 的 NDP 功能	在 集群管理>>拓扑发现>>全局配置 页面，启用交换机的 NDP 功能。
2	启用系统和端口 1、2、3 的 NTDP 功能	在 集群管理>>拓扑收集>>全局配置 页面，启用交换机的 NTDP 功能。

步骤	操作	说明
3	建立集群，并配置集群参数	在 集群管理>>集群管理>>集群配置 页面，配置集群角色为命令交换机，并填写集群信息。 集群地址池：175.128.0.1 掩码：255.255.255.0
4	配置成员交换机	在 集群管理>>集群管理>>成员管理 页面，选择成员交换机，点击<管理>按键，进入该交换机的 Web 页面。 也可在 集群管理>>集群管理>>拓扑图 页面，双击交换机图标，可以查看该交换机的详细信息；单击交换机图标，点击<管理>按键，可以进入该交换机的 Web 页面。

[回目录](#)

第17章 系统维护

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

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

17.1 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。

17.1.1 CPU 监控

进入页面的方法：系统维护>>运行状态>>CPU 监控

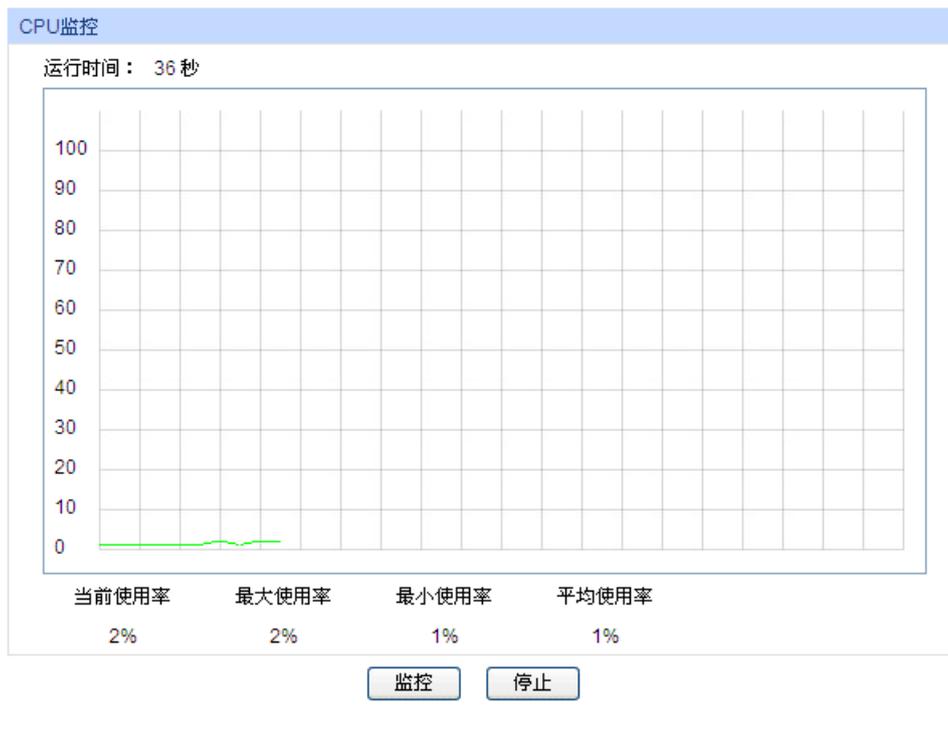


图 17-1 CPU 监控

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。

17.1.2 内存监控

进入页面的方法：系统维护>>运行状态>>内存监控

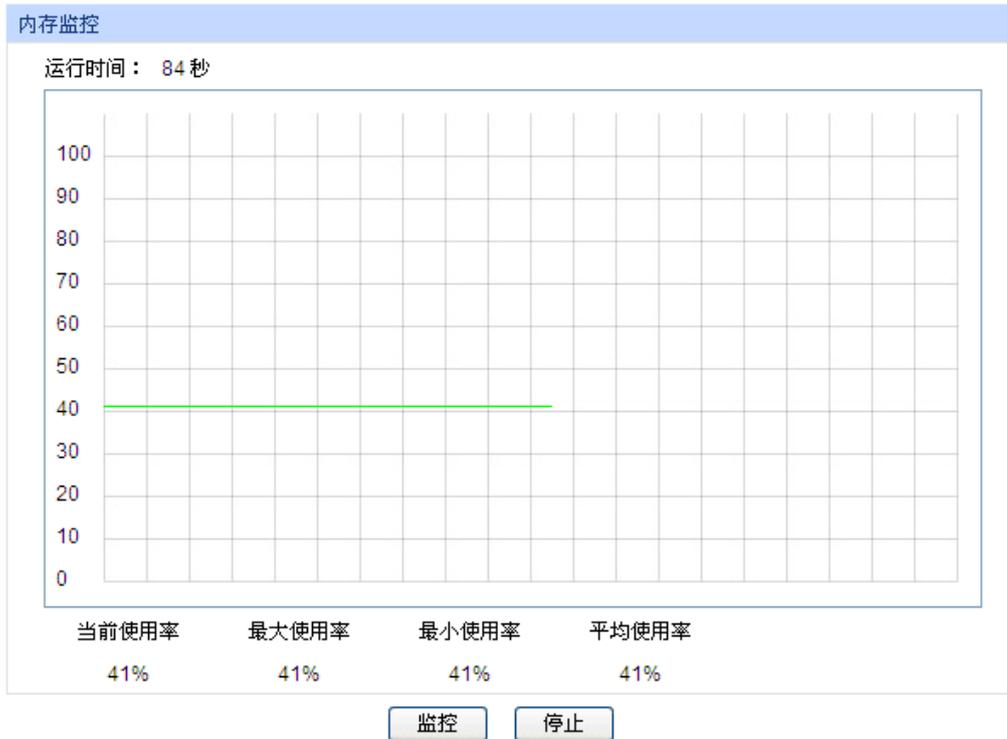


图 17-2 内存监控

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。

17.2 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 17-1 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 17-1 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。

17.2.1 日志列表

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

进入页面的方法：系统维护>>系统日志>>日志列表

系统日志列表				
序号	时间	模块名	严重级别	日志信息
		所有模块 ▾	所有级别 ▾	
1	2006-01-06 08:40:05	User	level_3	User admin login the web by admin on web (192.168.0.200).
2	2006-01-06 07:16:53	User	level_3	User admin login the web by admin on web (192.168.0.200).
3	2006-01-06 05:44:46	User	level_3	User admin login the web by admin on web (192.168.0.200).
4	2006-01-06 05:24:56	User	level_3	User admin login the web by admin on web (192.168.0.200).
5	2006-01-06 02:35:35	User	level_3	User admin login the web by admin on web (192.168.0.200).
6	2006-01-06 02:01:38	User	level_3	User admin login the web by admin on web (192.168.0.200).
7	2006-01-06 01:33:00	User	level_3	User admin login the web by admin on web (192.168.0.200).
8	2006-01-06 01:12:47	User	level_3	User admin login the web by admin on web (192.168.0.200).
9	2006-01-06 01:00:32	User	level_3	User admin login the web by admin on web (192.168.0.200).
10	2006-01-05 07:53:56	User	level_3	Logout the CLI by admin on vty0 (192.168.0.200).
11	2006-01-05 07:47:14	User	level_3	Login the CLI by admin on vty0 (192.168.0.200).
12	2006-01-05 07:38:18	User	level_3	User admin login the web by admin on web (192.168.0.200).
13	2006-01-05 06:00:15	User	level_3	User admin login the web by admin on web (192.168.0.200).
14	2006-01-03 07:53:01	User	level_3	User admin login the web by admin on web (192.168.0.200).
15	2006-01-03 07:44:20	User	level_3	Logout the CLI by admin on vty0 (192.168.0.200).
16	2006-01-03 07:38:20	VLAN	level_6	Added port 2 to VLAN 2 by admin on vty0 (192.168.0.200).
17	2006-01-03 07:35:48	User	level_3	Login the CLI by admin on vty0 (192.168.0.200).
18	2006-01-03 07:32:07	User	level_3	Logout the CLI by admin on vty0 (192.168.0.200).

注意：

- 1、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。
- 2、本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为511条。

图 17-3 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 511 条。

17.2.2 本地日志

本地日志是指保存在本交换机上的所有系统日志信息。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**

本地日志配置			
选择	输出方向	严重级别	状态
<input type="checkbox"/>		<input type="text" value=""/> ▾	<input type="text" value=""/> ▾
<input type="checkbox"/>	日志缓冲区	level_6	启用
<input type="checkbox"/>	日志文件	level_2	禁用

注意：

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

图 17-4 本地日志

条目介绍：

➤ **系统日志列表**

- 选择：** 勾选相应的日志记录位置进行配置。
- 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记录。
- 状态：** 启用/禁用保存到该位置的日志功能。

17.2.3 远程日志

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

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

进入页面的方法：系统维护>>系统日志>>远程日志

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

注意：

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

图 17-5 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。

17.2.4 日志导出

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

进入页面的方法：系统维护>>系统日志>>日志导出

日志文件导出

点击此处按钮，可将日志文件导出，以作设备诊断和统计分析之用。

注意：

导出日志文件可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 17-6 日志导出

条目介绍：

➤ 日志文件导出

导出日志文件： 点击此按钮导出日志文件中的日志信息。

17.3 系统诊断

本交换机提供了线缆检测功能。

17.3.1 线缆检测

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

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

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

注意：

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

图 17-7 线缆检测

条目介绍：

➤ 线缆检测

检测端口： 选择要进行线缆检测的端口。

线对： 显示线对序号。

线路状态： 检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。

- 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。
- 短路：线路金属内芯互相接触，导致短路。
- 阻抗失配：网线质量问题。

线路长度： 若线路为正常状态，显示该线缆的长度范围。

出错长度： 若线路为短路、开路或阻抗失配状态，则显示该线缆的出错长度。

注意：

- 这里的长度是指线缆绕对的长度，不是线缆表皮的长度，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。

17.4 网络诊断

本交换机提供了 Ping 检测和 Tracert 检测功能。

17.4.1 Ping 检测

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

Ping 检测过程如下：

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

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

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

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

图 17-8 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 和 IPv6 地址。

发送次数： 填写 Ping 检测时发送的检测包次数。建议使用缺省值。

发送报文长度： 填写 Ping 检测时发送的检测包长度。建议使用缺省值。

时间间隔： 发送 ICMP 请求报文的时间间隔。

17.4.2 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 17-9 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 和 IPv6 地址。

最大跳数： 填写测试报文发送的最大跳数。

延时时间： 填写等待报文回复的时间。

[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

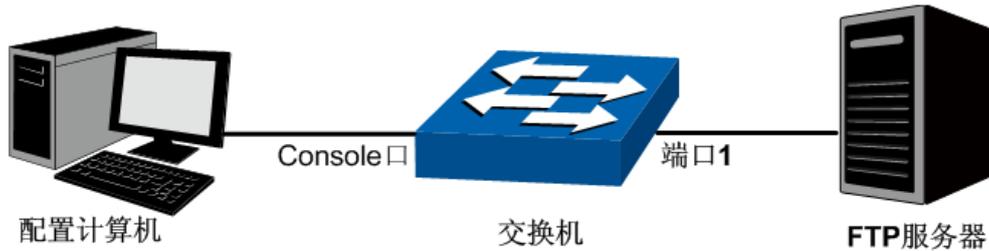


图 18-1 利用 FTP 加载软件连接图

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 配置终端仿真软件

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-SL5428>”的提示符，说明已成功登录交换机。

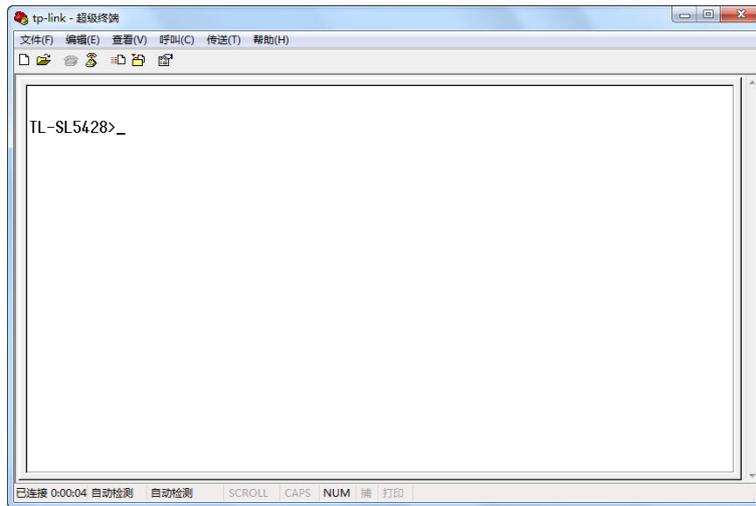


图 18-2 命令行主窗口



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，并打开配置成功的终端仿真程序。FTP 服务器连接到交换机端口 1。
2. 将交换机断电重启，当在终端仿真程序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 18-3 所示。

```

*****
*          TP-LINK  BOOTUTIL(v1.0.0)          *
*****
Copyright (c) 2011 TP-LINK Tech. Co., Ltd
Create Date: May 17 2011 16:40:15

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 18-3 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。详细命令如下图所示。输入命令后按回车键。

```
[TL-SL5428] : 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 tl_sl5428_up.bin。详细命令如下图所示。输入命令后按回车键。

```
[TL-SL5428] : ftp host 10.10.70.146 user 123 pwd 123 file tl_sl5428_up.bin
```

5. 最后输入 upgrade 命令后按回车键开始升级。等待片刻，终端仿真程序会显示提示信息：**You can only use the port 1 to upgrade**，如下图所示。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。

```
[TL-SL5428] : upgrade
You can only use the port 1 to upgrade.
```

6. 当终端仿真程序弹出提示信息：**Are you sure to upgrade the firmware[Y/N]:** 时，输入 Y 开始升级，输入 N 退出升级。如下图所示。图中的#字符表示正在升级，升级结束后将弹出[TL-SL5428]命令提示符。

```
Are you sure to upgrade the firmware [Y/N]: y
#####
#####
#####
#####
[TL-SL5428]:
```

7. 完成第 6 步后，输入 start 命令启动交换机，如下图所示。出现图示界面后输入用户名和密码（缺省均为“admin”）即可登录交换机的 CLI 命令窗口，可以通过 CLI 命令管理交换机。

```
[TL-SL5428]: start
Start . . . . .
◀
***** User Access Login *****
User:
```

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		
AAA	Authentication, Authorization and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
-	Auto-Negotiation	自协商
B 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
CMP	Cluster Management Protocol	集群管理协议
CRC	Cyclic Redundancy Check	循环冗余校验
CoS	Class of Service	服务等级
CSMA/CD	Carrier Sense Multiple Access/Collision Detect	载波侦听多路访问/冲突检测
CST	Common Spanning Tree	公共生成树
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
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
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
J 回首页		
-	Jumbo Frame	超长帧

英文缩写	英文全称	中文全称
L 回首页		
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元
LAG	Link Aggregated Group	链路聚合组
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
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		
NAPT	Network Address Port Translation	网络地址端口转换
NAT	Net Address Translation	网络地址转换
NDP	Neighbor Discovery Protocol	邻居发现协议
NMS	Network Management Station	网络管理站
NPDU	Network Protocol Data Unit	网络协议数据单元
NTDP	Neighbor Topology Discovery Protocol	邻居拓扑发现协议
NTP	Network Time Protocol	网络时间协议
-	NTP Server	网络时间服务器
O 回首页		
OID	Object Identifier	对象标识符
OSI	Open Systems Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
OUI	Organizationally Unique Identifier	全球统一标识符
P 回首页		
P2P	Point To Point	点到点
-	Packet	数据包
PAP	Password Authentication Protocol	密码认证协议

英文缩写	英文全称	中文全称
PCB	Printed Circuit Board	印制电路板
PDU	Protocol Data Unit	协议数据单元
PING	Packet Internet Groper	Internet 包探测器
PoE	Power over Ethernet	以太网供电
-	Port	端口
PPP	Point-to-Point Protocol	点到点协议
PPTP	Point to Point Tunneling Protocol	点对点隧道协议
PQ	Priority Queuing	优先队列
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
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Monitoring	远程网络监视
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
-	Router	路由器
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
TRIP	Trigger RIP	触发路由信息协议

英文缩写	英文全称	中文全称
TTL	Time to Live	生存时间
-	Trap	陷阱
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
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
WLAN	wireless local area network	无线局域网
WRR	Weighted Round Robin Queuing	加权轮询队列
WWW	World Wide Web	万维网

[回目录](#)

附录 B 技术参数规格

参数项	参数内容
支持的标准和协议	IEEE 802.3 10Base-T 以太网 IEEE 802.3u 100Base-TX 快速以太网 IEEE 802.3ab 1000Base-T 千兆以太网 IEEE 802.3z 千兆以太网(光纤) ANSI/IEEE 802.3 N-Way 自动协商 IEEE 802.3x 流量控制 IEEE 802.1p 优先级 IEEE 802.1q VLAN 桥操作 IEEE 802.1X 基于端口的访问认证 CSMA/CD Ethernet
数据传输速率	以太网 10Mbps 半双工, 20Mbps 全双工 快速以太网 100Mbps 半双工, 200Mbps 全双工 千兆以太网 2000Mbps 全双工
网络介质	10Base-T: 3 类或以上 UTP/STP(≤100m) 100Base-TX: 5 类或以上 UTP/STP(≤100m) 1000Base-T: 4 对超 5 类(Cat5e)或以上 UTP/STP(≤100m)
指示灯	Power、System、10/100M 指示灯、1000M 指示灯
传输方式	存储转发
背板带宽	6.4Gbps
MAC 地址学习	自动更新, 支持 8K 地址空间
包转发速率	10Base-T: 14881pps/端口 100Base-TX: 148810pps/端口 1000Base-T: 1488095pps/端口
交流输入	100-240V~ 50/60Hz
工作温度	0℃~40℃
存储温度	-40℃~70℃
工作湿度	10%~90% (RH 无凝结)
存储湿度	5%~90% (RH 无凝结)

[回目录](#)