

主要功能配置实例

3/5/6/7/8系列企业级交换机

声明

Copyright © 2021 普联技术有限公司

版权所有,保留所有权利

未经普联技术有限公司明确书面许可,任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容,且不得以营利为目的进行任何方式(电子、影印、录制等)的传播。

TP-LINK[®]为普联技术有限公司注册商标。本手册提及的所有商标,由各自所有人拥有。本手册所提到的产品规格和资讯仅供参考,如有内容更新,恕不另行通知。除非有特殊约定,本手册仅作为使用指导,所作陈述均不构成任何形式的担保。

目录

第1	章	前	言	1
	1.1	目	标读者	1
	1.2	本	书约定	1
	1.3	适	用机型	2
第2	章	设	备管理	3
	2.1	Ξ	层网管交换机管理方法介绍	3
		2.1.1	通过业务接口管理交换机	3
		2.1.2	通过 Console 接口管理交换机	7
		2.1.3	通过 Management 接口管理交换机1	0
		2.1.4	管理安全1	11
	2.2	=	层网管交换机管理方法介绍	6
		2.2.1	通过业务接口管理交换机1	6
Ť		2.2.2	通过 Console 接口管理交换机2	20
		2.2.3	♥ 管理安全2	23
	2.3	简	单 WEB 网管交换机管理方法介绍2	28
		2.3.1	简单 WEB 管理交换机介绍 2	28
		2.3.2	WEB 管理 2	28

	2.3.3	TP-LINK Web 网管交换机客户端应用程序管理	30
2.4	各种	交换机硬件拨码开关介绍	34
	2.4.1	硬件拨码开关介绍	34
	2.4.2	1 系列交换机	34
	2.4.3	1 系列 POE 交换机	34
	2.4.4	2 系列非云管理机型	36
	2.4.5	2系列云管理机型	36
	2.4.6	工业级交换机	37
2.5	各种	交换机复位方法介绍	40
	2.5.1	2 系列交换机	40
	2.5.2	3/5/6/7/8 系列交换机	41
第3章	交换i	段置	44
3.1	交换	机端口监控配置指南	44
	3.1.1	应用介绍	44
	3.1.2	▼ 需求介绍	44
	3.1.3	设置方法	45
	3.1.4	配置注意事项	47
3.2	交换体	机端口隔离配置指南	48

	3.2.1	应用介绍	48
	3.2.2	需求介绍	48
	3.2.3	设置方法	49
3.3	交换	机端口安全配置指南	52
	3.3.1	应用介绍	52
	3.3.2	需求介绍	52
	3.3.3	设置方法	52
3.4	交换	机端口汇聚配置指南	54
	3.4.1	应用介绍	54
	3.4.2	需求介绍	54
	3.4.3	设置方法	54
	3.4.4	配置注意事项	57
3.5	交换	机地址表管理功能使用指南	59
•	3.5.1	交换机地址表介绍	59
	3.5.2	▶ 地址表显示	59
	3.5.3	静态地址表	60
	3.5.4	动态地址表	61
	3.5.5	过滤地址表	. 62

第4章	堆叠	功能	64
4.1	交换	机堆叠配置指导	64
	4.1.1	应用介绍	64
	4.1.2	需求介绍	64
	4.1.3	设置方法	65
	4.1.4	配置注意事项	70
第5章	VLA	Ν	71
5.1	交换	机 802.1Q VLAN 配置指南	71
	5.1.1	应用介绍	71
	5.1.2	需求介绍	71
	5.1.3	设置方法	72
5.2	МАС	VLAN 配置指南	75
	5.2.1	应用介绍	75
*	5.2.2	需求介绍	75
	5.2.3	· 设置方法	76
	5.2.4	配置注意事项	79
5.3	语音	VLAN 典型配置指导	80
	5.3.1	应用介绍	80

	5.3.2	需求介绍	80
	5.3.3	设置方法	81
	5.3.4	配置注意事项	88
第6章	生成	树	90
6.1	交换	机生成树功能配置指南	90
	6.1.1	应用介绍	90
	6.1.2	需求介绍	
	6.1.3	设置方法	91
	6.1.4	配置注意事项	97
第7章	组播	管理	98
7.1			00
	交换	机多网段 IGMP 侦听配置指南	
	交换 7.1.1	机多网段 IGMP 侦听配置指南 应用介绍	
	交换 ⁴ 7.1.1 7.1.2	机多网段 IGMP 侦听配置指南 应用介绍 需求介绍	
	交换 7.1.1 7.1.2 7.1.3	机多网段 IGMP 侦听配置指南 应用介绍 需求介绍 设置方法	
第8章	交换: 7.1.1 7.1.2 7.1.3 路由:	机多网段 IGMP 侦听配置指南 应用介绍 需求介绍 设置方法	
第8章 8.1	交换 7.1.1 7.1.2 7.1.3 路由 交换	机多网段 IGMP 侦听配置指南	
第8章 8.1	交换: 7.1.1 7.1.2 7.1.3 路由: 交换: 8.1.1	机多网段 IGMP 侦听配置指南	

	8.1.3	设置方法		 	107
8.2	三	层网管交换机策略	路路由配置指导	 	108
	8.2.1	应用介绍		 	108
	8.2.2	需求介绍		 	109
	8.2.3	设置方法		 	111
第9章	服	务质量			122
9.1	交	奂机带宽控制配 置	置指南		122
	9.1.1	应用介绍			122
	9.1.2	需求介绍		 	122
	9.1.3	设置方法		 	123
9.2	交	换机风暴抑制配置	置指南	 	124
	9.2.1	应用介绍		 	124
	9.2.2	需求介绍		 	124
	9.2.3	设置方法		 	125
第 10 章	i 访	问控制		 	126
10.	1 交	奂机访问控制设置	置指南	 	126
	10.1.1	应用介绍		 	126
	10.1.2	需求介绍		 	126

	10.	1.3	设置方法	127
第 11	章	网络	安全	132
1	1.1	交换	① DHCP 侦听配置设置指南	132
	11.	1.1	应用介绍	132
	11.	1.2	需求介绍	132
	11.	1.3	设置方法	133
1	1.2	交换	机四元绑定、ARP 防护、IP 源防护设置指南	135
	11.	2.1	应用介绍	135
	11.	2.2	需求介绍	135
	11.	2.3	设置方法	136
第12	章	802.1	IX	140
1	2.1	交换构	玑 802.1X 认证功能配置指南	140
	12.	1.1	应用介绍	140
	12.	1.2	需求介绍	140
	12.	1.3	设置方法	141
第13	章	工业组	及特性	147
1	3.1	ERP	S 单环环网配置指南	147
	13.	1.1	应用介绍	147

	13.1.2	需求介绍	147
	13.1.3	设置方法	148
13.	2 TP-	RING 单环环网配置指南	158
	13.2.1	应用介绍	158
	13.2.2	需求介绍	158
	13.2.3	设置方法	159
第14章	i įć	3功能	169
14.	1 三厚	层网管交换机连云配置指南	169
	14.1.1	应用介绍	169
	14.1.2	需求介绍	169
	14.1.3	设置方法	169
14.	2 二层	层 Web 网管交换机连云配置指南	173
	14.2.1	应用介绍	173
	14.2.2	需求介绍	173
	14.2.3	▼ ひ置方法	173

第1章 前言

本手册旨在帮助您正确使用 TP-LINK 企业级交换机。内容包含配置交换机各种功能的的实例和详细说明。请在操作前仔细阅读本手册。

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,

- 用 >> 符号表示配置界面的进入顺序。默认为一级菜单 >> 二级菜单 >> 标签页,
 其中,部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字或图形,表示 Web 界面的按钮名称,如<确定>或<
 新端>。
- 正文中出现的""双引号标记文字,表示 Web 界面出现的除按钮外名词,如"ARP 绑定"
 界面。

本手册中使用的特殊图标说明如下:

图标	含义
@	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 适用机型

本手册适用于 TP-LINK 3/5/6/7/8 系列企业级交换机,部分功能仅特定型号支持,以产品 实际页面为准。

2

第2章 设备管理

2.1 三层网管交换机管理方法介绍

2.1.1 通过业务接口管理交换机

三层网管交换机可以通过业务口直接管理交换机,通过业务口可以使用 HTTP、HTTPS、

Telnet、SSH、SNMP 管理交换机。

业务口默认管理 IP: 192.168.0.1

业务口默认管理用户名: admin

业务口默认管理密码: admin

本章介绍交换机在出厂情况下,电脑如何通过业务口使用 HTTP、HTTPS、Telnet、SSH 管理交换机。

电脑连接方式

将电脑的网线连接到交换机的业务接口上,如下图所示:



第一、HTTP、HTTPS 管理

1、在电脑上打开浏览器,输入 http://192.168.0.1 或者 https://192.168.0.1 (浏览器 建议使用 Chrome、Firefox、Edge 或 IE9 以上的浏览器)。

🖷 🖅 🗖 192.168.0.1	× + ~		-	-		×
\leftrightarrow \rightarrow \circlearrowright \Uparrow	⊙ 192.168.0.1/	☆	5⁄≡	h	Ŀ	
	TP-LINK [®]					
	用户名:					
	登录 清除 Copyright © 2017 普班技术有限公司					
	版权所有					2

2、输入正确的用户名和密码。

テ注意:

- 如果使用 HTTPS 管理,浏览器会提示安全风险,在浏览器中点击"详细信息"—"继续转到网页"即可。(不同浏览器提示可能会略有不同)
- 如果输入正确用户名和密码之后,管理页面显示不全,可能是由于浏览器缓存原因造成,此时按 Ctrl+F5刷新页面即可。

第二、Telnet 管理

1、电脑上安装 Telnet 客户端软件(比如:Tera Term、SecureCRT 等,本章节以 Tera Term 为例),在 Telnet 客户端软件上新建连接,选择 Telnet 协议,主机 IP 192.168.0.1,端口号 23。

Tera Term: New o	connection	×
⊚ ТСР<u>/</u>I Р	Hos <u>t</u> : 192.168.0 ✓ Hist <u>o</u> ry Service: ● Telnet ○ <u>S</u> SH ○ Other	TCP port#: 23 SSH version: SSH2 ~ Protocol: UNSPEC ~
⊖ S <u>e</u> rial	Po <u>r</u> t: COM1: 通 OK Cance	! [COM1] ✓

2、输入正确的用户名和密码。



第三、SSH 管理

SSH 管理功能在交换机上默认情况下是禁用的,需要先使用其他管理方式进入交换机开启 该功能才可以进行 SSH 管理。

1、电脑登录交换机的 Web 页面,"系统管理"-"安全管理"-"SSH 配置", 启用 SSH 功能。

安全配置 HTTP配置	HTTPS配置 SSH配置 Telnet配置	
全局配置		
SSH功能:	◉ 启用 ◎ 禁用	
Protocol V1:	● 启用 ◎ 禁用	田立
Protocol V2:	● 启用 ○ 禁用	報助
静默时长:	120 秒 (1-120)	
最大连接数:	5 (1-5)	
加密算法		
AES128-CBC	AES192-CBC 🗹 AES256-CBC	
Blowfish-CBC	Cast128-CBC 🗹 3DES-CBC	提交
数据完整性算法		
MMAC-SHA1	MMAC-MD5	提交
密钥导入		
选择你要导入交换	们的密钥。	
密钥类型:	SSH-2 RSA/DSA V	导入密钥
密钥文件:	选择文件未选择任何文件	
 1.守へ密钥り能需要較も 2.导入配置文件后,交換 	、叩问,	钥文件有误,SSH会转
用密码认证的方式登陆。		

2、电脑上安装 SSH 客户端软件(比如:Tera Term、SecureCRT 等,本章节以 Tera

Term 为例),在 SSH 客户端软件上新建连接,选择 SSH 协议,主机 IP 192.168.0.1,

端口号 22。

Tera Term: New co	onnection		×
● TCP/ <u>I</u> P	Hos <u>t</u> : <mark>192.168.0.</mark> ☑ Hist <u>o</u> ry Service: ○ Te <u>I</u> net	TCP port#: 22 SSH version: SSH2 Protocol: UNSPEC	>
⊖ S <u>e</u> rial	Po <u>r</u> t: COM1: 通信	言端□ (COM1)	\sim
	OK Cancel	<u>H</u> elp	

3、输入正确的用户名和密码。

SSH Authentication				_	×
Logging in to 192.168	.0.1				
Authentication require	ed.				
User <u>n</u> ame:	admin				
Passphrase:	•••••				
	Remember passw	vord in <u>m</u> emory			
	Forward agent				
OUse plain passw	ord to log in				
O Use <u>R</u> SA/DSA/E	CDSA/ED25519 key t	to log in Priva	te <u>k</u> ey file:		
O Use rhosts to log	g in (SSH1)	Local <u>u</u> ser	name;		
	Host private k	æy <u>fi</u> le:			
🔿 Use keyboard-įr	nteractive to log in				
O Use Pageant to	log in				
	ОК		Disconnect		

第四、SNMP 管理

可以参考《SNMP 基础设置方法介绍》。

2.1.2 通过 Console 接口管理交换机

三层网管交换机可以通过 Console 接口进行管理,交换机出厂配置下,使用 Console 管理 交换机不需要用户名和密码。

电脑连接方式

方式一:使用串口线进行连接(所有三层网管交换机均支持这种方式),串口接电脑, RJ45 接口接交换机的 Console 接口。



方式二:使用标准 USB 转 Micro USB 线连接 (部分交换机支持这种方式),标准 USB 接电

脑, Micro USB 接交换机。

Port	1-28 0 1000Mb	ps Nops	Port	25F-4	285	10	DOMES	× 1	Port 29-	32 0 10Gbps	Manager
	Le activity					• ac	wity			Les activity	
											4.44
1000	PWR	4	•	12	16	20	24	28	32		
	ອາຮ	э		11	15	19	23	27	31		
	Master	2		10	14	18	22	26	30		
	RPS		5		13		21	25	29	-	Const

Console 接口管理

- 1、安装驱动
- 1) 如果电脑自带串口接口,不需要安装驱动;
- 2) 如果使用 USB 转串口线, 电脑上需要安装 USB 转串口线的驱动;
- 3) 如果使用 USB 转 Micro USB 线连接, 需要安装"TP-LINK Micro USB 串口驱动程序"。

2、电脑上安装串口通信客户端软件(比如: Tera Term、SerureCRT等,本章节以 Tera Term 为例),在串口通信客户端软件上新建连接,选择 Serial,以及对应的通信端口(不同电脑 的通信端口会不一样)。

Tera Term: New co	onnection		×
○ ТСР/<u>І</u>Р	Hos <u>t</u> : 192.168.0.1 ✓ Hist <u>o</u> ry Service: ○ Te <u>I</u> net ◎ <u>S</u> SH ○ Other	TCP <u>p</u> ort#; 22 SSH ⊻ersion: SSH2 Proto <u>c</u> ol: UNSPEC	~
• Serial	Po <u>r</u> t: COM1: 通信 OK Cancel	端□ (COM1) <u>H</u> elp	~

3、Serial Port 相关设置中设置波特率: 38400bps、数据位: 8bit、奇偶校验: none、停

止位:	1bit、	数据流控制:	none.
-----	-------	--------	-------

Tera Term: Serial port	setup		×					
<u>P</u> ort:	COM1	\sim	ОК					
Sp <u>e</u> ed:	38400	~						
<u>D</u> ata:	8 bit	\sim	Cancel					
P <u>a</u> rity:	none	\sim						
<u>S</u> top bits:	1 bit	\sim	<u>H</u> elp					
Elow control:	none	\sim						
Transmit delay 0 msec/ <u>c</u> har 0 msec/ <u>l</u> ine								

4、登录成功之后,直接在窗口中输入管理 CLI 命令即可。

M	COM1	- Tera	Term VT			_	×
<u>F</u> ile	<u>E</u> dit	<u>S</u> etup	C <u>o</u> ntrol	<u>W</u> indow	<u>H</u> elp		
							^
TL-SG5	452>						
TL-SG5	452>						
TL-SG5	452>en						
TL-SG5	452 # con	f					
TL-SG5	452(con	fig)#					
							~

2.1.3 通过 Management 接口管理交换机

三层网管交换机可以通过 Management 接口管理。(部分交换机不支持该接口)

电脑连接方式

将电脑的网线连接到交换机的 Management 接口上。

Port 1-28	bps Mbps	Port	25F~	285 [10 ect	00Mbj Ivity	pis I	Part 29-3	2 = 10Gbps 2 = 1Gbps = activity	Manage
PWR			12	16	20	24	28	32		1
515	3	7	11	15	19	23	27	31		
Master	2		10	14	18	22	26	30	-	1. I
RPS	1	5	9	13	17	21	25	29	-	Conse

 1、通过其他管理方式,设置 Management 接口的 IP 地址,以 Web 管理为例在"系统管理"
 -"系统设置"-"管理口设置"中设置 Management 接口的 IP 地址。(部分交换机该管理口默 认 IP 为 192.168.1.1)

系统信息 设备描述	系统时间 夏令时	管理口设置	
端口配置			
自动协商:	🖲 开启 🔍 关闭		
速率:	100M •		(建父)
双工:	全双工 🔻		帮助
IP配置			
IP地址:	192.168.1.1	(格式: 192.168.1.1)	
子网掩码:	255.255.255.0	(格式: 255.255.255.0)	JÆX.
管理口状态			
接口名称:	Meth0/0/1		
连接状态:	未连接		
速率信息:	未知		

2、通过 Management 接口,可以使用 HTTP、HTTPS、Telnet、SSH 等方式管理交换机,

具体操作方法与电脑通过业务口连接交换机操作方法一致。

2.1.4 管理安全

交换机中用户分为4个级别,在实际应用过程中根据需求创建用户:

- 管理员:可以设置和修改所有功能,包括创建和修改用户。
- 操作员:可以设置和修改大部分功能,但不能创建和修改用户。(具体不可设置的功能
 参见用户手册和命令行手册)
- 高级用户:不可备份和导入配置、不可创建和修改用户,可以设置和修改交换机大部分
 功能。(具体不可设置的功能参见用户手册和命令行手册)
- 普通用户: 仅可以查看交换机各个功能的配置情况。

1、web 配置举例

在交换机的"系统管理-用户管理-用户配置"界面,设置不同权限的管理员账号。

用户列表用户配置			
用户信息			
用户名:			
用户类型:	普通用户 🗸		添加
密码:			清除
确认密码:			
用户列表			
选择 序号	用户名	用户类型	操作
□ 1	admin	管理员	编辑
2	caozuo	操作员	编辑
□ 3	gaoji	高级用户	编辑
4	putong	普通用户	编辑
	全选	删除 帮助	

2、CLI 配置

需求: 交换机中创建一个管理员, 用户名 test 密码 test1234567。

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)# user name test privilege admin password test1234567

注意:如果忘记用户名和密码,可以通过 Console 口管理交换机,通过 CLI 创建一个管理 员账户,重新管理交换机。

3、创建特权模式密码

通过 CLI 管理, 在特权模式下, 用户可以设置交换机的所有功能, 网络管理员可以根据网络安全需要启用 CLI 特权模式密码。

CLI 配置举例:

需求: 交换机中创建特权密码 test1234567

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#enable password test1234567

注意:如果忘记了特权密码,希望进入特权模式,交换机就只能复位了。

4、设置 Console 口登录用户名密码认证

如果希望增强交换机 Console 接口管理的安全性,则需要启用交换机的 AAA 认证,通过

AAA 功能给 Console 接口增加用户名和密码。

Web 配置举例:

步骤一:网络安全-AAA-全局配置,启用AAA功能。

全局配調	置 方法列表	Dot1x配置 服务器组 RADIUS配置	TACACS+
全層	局配置		
	AAA:	● 启用 ○ 禁用	提交
使自	管理员权限		
0.0			
	使能密码:		提交
AA	A配置列表		
选拔	♀ 模块	登录方法列表	认证方法列表
)	default 🔻	default 🔻
	console	default	default
	telnet	default	default
	ssh	default	default
	http	default	default
		全洗 桿衣	基明

步骤二:网络安全-AAA-方法列表,查看"登录方法",默认已经添加了 local 的认证方式,

无需额外设置。

添加方法列表					
方法列表名	:				
列表类型:	登录 ~				
方法一:	~				沃加
方法二:	~				10K/JH
方法三:	~				
方法四:	~				
容录方法列表					
选择	方法列表	方法一	方法二	方法三	方法四
		~	~	~	- ~
	default	local			
		全选 提	交删除		
认证方法列表					
选择	方法列表	方法一	方法二	方法三	方法四
		~	~	- ~	~
	default	local			
		全选 提交	删除 帮助	1	

CLI 配置举例:

"登录方法列表"出厂设置默认已经设置好了, CLI 中只要启用 AAA 认证即可。

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#aaa enable

注意:如果启用了 AAA 认证,又忘记了密码,交换机就只能复位了。

5、终端权限管理

交换机可以针对 IP、MAC 和端口来限制管理交换机的用户属性。

Web 配置举例:

需求:限制只有192.168.0.0/24网段的用户才能管理交换机。

系统管理-安全管理-安全配置 选择限制类型、接入方式,以及允许访问交换机用户的 IP 地址。

身份限制	
限制类型:	基于IP ▼
接入方式:	🗆 SNMP 🗹 Telnet 🗹 SSH 🗹 HTTP 🔲 HTTPS 🗌 Ping 🗌 All
IP地址:	192.168.0.0 掩码: 255.255.255.0
MAC地址:	(格式: 00-00-00-00-01)
	提交帮助

CLI 配置举例:

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#user access-control ip-based 192.168.0.0 255.255.255.0 telnet

ssh http

2.2 二层网管交换机管理方法介绍

2.2.1 通过业务接口管理交换机

二层网管交换机可以通过业务口直接管理交换机,通过业务口可以使用 HTTP、HTTPS、

Telnet、SSH、SNMP 管理交换机。

业务口默认管理 IP: 192.168.0.1

业务口默认管理用户名: admin

业务口默认管理密码: admin

本章介绍交换机在出厂情况下,电脑如何通过业务口使用 HTTP、HTTPS、Telnet、SSH 管理交换机。

电脑连接方式

将电脑的网线连接到交换机的业务接口上,如下图所示:



第一、HTTP、HTTPS 管理

1、在电脑上打开浏览器,输入 http://192.168.0.1 或者 https://192.168.0.1 (浏览器 建议使用 Chrome、Firefox、Edge 或 IE9 以上的浏览器)。

🖥 🗲 🗖 192.168.0.1	× + ~		-	-		×
\leftrightarrow \rightarrow \circlearrowright $\widehat{\omega}$	① 192.168.0.1/	□ ☆	r∕≡	h	Ŕ	
	TP-LINK [®]					
	用户名:					
	85.04 :					1
	登录 清除					
	Copyright © 2017 普联技术有限公司					
	版权所有					
	~		_		-	

1、输入正确的用户名和密码。

Ctrl+F5 刷新页面即可。

đ	• 注意:
•	如果使用 HTTPS 管理,浏览器会提示安全风险,在浏览器中点击"详细信息"—"继续转到网页"即可。(不同浏览器提示可能会略有不同)
•	如果输入正确用户名和密码之后,管理页面显示不全,可能是由于浏览器缓存原因造成,此时按

第二、Telnet 管理

1、电脑上安装 Telnet 客户端软件(比如: Tera Term、SecureCRT 等,本章节以 Tera Term 为例),在 Telnet 客户端软件上新建连接,选择 Telnet 协议,主机 IP

192.168.0.1, 端口号 23。

Tera Term: New o	connection	×
● TCP <u>/I</u> P	Hos <u>t</u> : 192.168.0.1	~
	✓ History Service: ● Telnet	TCP port#: 23
	⊖ <u>s</u> sh	SSH version: SSH2 \sim
	○ Other	Proto <u>c</u> ol: UNSPEC ~
⊖ S <u>e</u> rial	Po <u>r</u> t: COM1: 通信	試告口 (COM1) ── ──
	OK Cancel	Help

2、输入正确的用户名和密码。



第三、SSH 管理

SSH 管理功能在交换机上默认情况下是禁用的,需要先使用其他管理方式进入交换机开启 该功能才可以进行 SSH 管理。

1、电脑登录交换机的 Web 页面,"系统管理"-"安全管理"-"SSH 配置", 启用 SSH 功能。

安全配置 HTTP配置	HTTPS配置 SSH配置 Telnet配置	
全局配置		
SSH功能:	◉ 启用 ◎ 禁用	
Protocol V1:	● 启用 ◎ 禁用	- 捍亦
Protocol V2:	● 启用 ○ 禁用	帮助
静默时长:	120 秒 (1-120)	
最大连接数:	5 (1-5)	
加密算法		
AES128-CB	C 🖉 AES192-CBC 🖉 AES256-CBC	~ 提示]
Blowfish-CB	C 🗹 Cast128-CBC 🗹 3DES-CBC	
数据完整性算法		
MMAC-SHA	1 🗹 HMAC-MD5	提交
密钥导入		
选择你要导入交换	机的密钥。	
密钥类型:	SSH-2 RSA/DSA V	导入密钥
密钥文件:	选择文件未选择任何文件	
1.每个密钥可能需要数 2.导入配置文件后,交打 用密码认证的方式登陆	云印间, 匹期间请耐心等待,不要操作交换机。 换机中此用户原有的同类型密钥将会被覆盖。如果您导入的; 。	密钥文件有误,SSH会转

2、电脑上安装 SSH 客户端软件(比如:Tera Term、SecureCRT 等,本章节以 Tera Term 为例),在 SSH 客户端软件上新建连接,选择 SSH 协议,主机 IP 192.168.0.1,端 口号 22。

Tera Term: New c	onnection	×
. тср <u>∥</u> р	Hos <u>t</u> : <mark>192.168.0.1</mark> ☑ Hist <u>o</u> ry Service: ○ Te <u>I</u> net	✓ TCP port#: 22 SSH version: SSH2 ∨ Protocol: UNSPEC ∨
○ S <u>e</u> rial	Po <u>r</u> t: COM1: 通信 OK Cancel	端□ (COM1) ∨ <u>H</u> elp

3、输入正确的用户名和密码。

SSH Authentication				_	×
Logging in to 192.168	.0.1				
Authentication require	ed.				
User <u>n</u> ame:	admin				
Passphrase:	•••••				
	Remember passw	vord in <u>m</u> emory			
	Forward agent				
OUse plain passw	ord to log in				
O Use <u>R</u> SA/DSA/E	CDSA/ED25519 key t	to log in Priva	te <u>k</u> ey file:		
O Use rhosts to log	g in (SSH1)	Local <u>u</u> ser	name;		
	Host private k	æy <u>fi</u> le:			
🔿 Use keyboard-įr	nteractive to log in				
O Use Pageant to	log in				
	ОК		Disconnect		

第四、SNMP 管理

可以参考《SNMP 基础设置方法介绍-。

2.2.2 通过 Console 接口管理交换机

三层网管交换机可以通过 Console 接口进行管理,交换机出厂配置下,使用 Console 管理 交换机不需要用户名和密码。

电脑连接方式

方式一:使用串口线进行连接(所有三层网管交换机均支持这种方式),串口接电脑, RJ45 接口接交换机的 Console 接口。



方式二:使用标准 USB 转 Micro USB 线连接 (部分交换机支持这种方式),标准 USB 接电脑, Micro USB 接交换机。

Port 1-20	1000Mb	ipis Nopis	Port	25F-	28F [10 • act	00Mb) Ivily	76	Part 29-	32 9 1Gbps s activity	Manag
	PWR			12	16	20	24	28	32		
	ราร	э		11	15	19	23	27	31		
	Master	2		10	14	10	22	28	30		14.
	RPS		5	9	13		21	25	29	*	Con

Console 接口管理

- 1、安装驱动
 - 1) 如果电脑自带串口接口,不需要安装驱动;
 - 2) 如果使用 USB 转串口线, 电脑上需要安装 USB 转串口线的驱动;

2、电脑上安装串口通信客户端软件(比如: Tera Term、SerureCRT等,本章节以 Tera Term 为例),在串口通信客户端软件上新建连接,选择 Serial,以及对应的通信端口(不同电脑 的通信端口会不一样)。

Tera Term: New co	onnection		×
○ TCP <u>/I</u> P	Hos <u>t</u> : 192.168.0.1		~
	✓ History		
	Service: O Telnet	TCP <u>p</u> ort#; 22	
	⊚ <u>s</u> sh	SSH ⊻ersion: SSH2	\sim
	⊖ Other	Proto <u>c</u> ol: UNSPEC	~
• Serial	Po <u>r</u> t: COM1: 通信	端口 (COM1)	~
	OK Cancel	<u>H</u> elp	

3、Serial Port 相关设置中设置波特率: 38400bps、数据位: 8bit、奇偶校验: none、停

止位:	1bit、	数据流控制:	none.
-----	-------	--------	-------

Tera Term: Serial port se	tup		×
Port:	COM1	\sim	ОК
Sp <u>e</u> ed:	38400	~	
<u>D</u> ata:	8 bit	\sim	Cancel
P <u>a</u> rity:	none	\sim	
<u>S</u> top bits:	1 bit	\sim	<u>H</u> elp
<u>F</u> low control:	none	\sim	
Transmit delay 0 msec <u>k</u>	char O	ms	ec/ <u>l</u> ine

4、登录成功之后, 直接在窗口中输入管理 CLI 命令即可。

VT	COM1	- Tera 1	Term VT			_	×
<u>F</u> ile	<u>E</u> dit	<u>S</u> etup	C <u>o</u> ntrol	<u>W</u> indow	<u>H</u> elp		
							^
N-865	452>						
N-865	452>						
TL-SG5	452>en						
NL-865	452#cont	f					
TL-SG5	452(cont	fig)#					
							~

2.2.3 管理安全

交换机中用户分为4个级别,在实际应用过程中根据需求创建用户:

- 管理员:可以设置和修改所有功能,包括创建和修改用户。
- 操作员:可以设置和修改大部分功能,但不能创建和修改用户。(具体不可设置的功能
 参见用户手册和命令行手册)
- 高级用户:不可备份和导入配置、不可创建和修改用户,可以设置和修改交换机大部分
 功能。(具体不可设置的功能参见用户手册和命令行手册)
- 普通用户: 仅可以查看交换机各个功能的配置情况。
- 1、web 配置举例

在交换机的"系统管理-用户管理-用户配置"界面,设置不同权限的管理员账号。

用	户列表	用户配置			
	用户信息	ļ			
	用户	名:			
	用户	类型:	普通用户 🗸		添加
密码:					清除
	确认密码:				
	用户列表				
	选择	序号	用户名	用户类型	操作
		1	admin	管理员	编辑
		2	caozuo	操作员	编辑
		3	gaoji	高级用户	编辑
		4	putong	普通用户	编辑
			全选	删除 帮助	

2、CLI 配置

需求: 交换机中创建一个管理员, 用户名 test 密码 test1234567。

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)# user name test privilege admin password test1234567

注意:如果忘记用户名和密码,可以通过 Console 口管理交换机,通过 CLI 创建一个管理 员账户,重新管理交换机。

3、创建特权模式密码

通过 CLI 管理, 在特权模式下, 用户可以设置交换机的所有功能, 网络管理员可以根据网络 安全需要启用 CLI 特权模式密码。

CLI 配置举例:

需求: 交换机中创建特权密码 test1234567

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#enable password test1234567

注意:如果忘记了特权密码,希望进入特权模式,交换机就只能复位了。

4、设置 Console 口登录用户名密码认证

如果希望增强交换机 Console 接口管理的安全性,则需要启用交换机的 AAA 认证,通过

AAA 功能给 Console 接口增加用户名和密码。

Web 配置举例:

步骤一:网络安全-AAA-全局配置,启用 AAA 功能。

全	局配置	方法列表	Dot1x配置	服务器组	RADIUS配置	TACACS+		
	全局配置							
					_			
	AAA		• 唐	明 🗌 禁用				提交
	使能管理	员权限						
	使能	密码:						提交
	A A A #199	지는						
	AAA配查列表							
	选择	模块		登录方法列表 认证方法		认证方法列表		
				default 🔻			default 🔻	
		console		default			default	
		telnet		default			default	
		ssh		default			default	
		http		default			default	
				全选	提交	帮助		

步骤二:网络安全-AAA-方法列表,查看"登录方法",默认已经添加了 local 的认证方式,

无需额外设置。

添加方法列表								
方法列表名	:							
列表类型:	登录 ~							
方法一:	~				沃加			
方法二:	~				TONJH			
方法三:	~							
方法四:	~							
兴己子计划主								
豆灰力法列农								
选择	方法列表	方法一	方法二	方法三	方法四			
		~	V	~	~			
	default	local						
全选 提交 删除								
认证方法列表								
选择	方法列表	方法一	方法二	方法三	方法四			
		~	~	~	~			
	default	local						
全选 提交 删除 帮助								

CLI 配置举例:

"登录方法列表"出厂设置默认已经设置好了, CLI 中只要启用 AAA 认证即可。

- TL-SH7428>enable
- TL-SH7428#configure
- TL-SH7428(config)#aaa enable

注意:

1、如果启用了 AAA 认证,又忘记了密码,交换机就只能复位了。

2、早期软件版本的交换机不支持 AAA 认证,需要通过在 Console 接口中使用 line 命令配

置 Console 接口的登录密码,具体配置过程如下:

TL-SG3210>enable

TL-SG3210#configure
TL-SG3210(config)#line console 0

TL-SG3210(config-line)#login local

5、终端权限管理

交换机可以针对 IP、MAC 和端口来限制管理交换机的用户属性。

Web 配置举例:

需求:限制只有 192.168.0.0/24 网段的用户才能管理交换机。

系统管理-安全管理-安全配置选择限制类型、接入方式,以及允许访问交换机用户的 IP 地址。

身份限制	
限制类型:	基于IP ▼
接入方式:	🔲 SNMP 🗹 Telnet 🗹 SSH 🗹 HTTP 🔲 HTTPS 🔲 Ping 🔲 All
IP地址:	192.168.0.0 掩码: 255.255.255.0
MAC地址:	(格式: 00-00-00-00-01)
	提交 帮助

CLI 配置举例:

TL-SH7428>enable

TL-SH7428#configure

TL-SH7428(config)#user access-control ip-based 192.168.0.0 255.255.255.0 telnet

ssh http

2.3 简单 WEB 网管交换机管理方法介绍

2.3.1 简单 WEB 管理交换机介绍

简单 Web 网管交换机是 TP-LINK2 系列简单网管交换机,目前已经全系升级成云交换系列,本篇文章针对以前老机型的设备管理方式进行介绍,老版本的 2 系列简单 WEB 网管交换机可以通过 Web 界面和 TP-LINK Web 网管交换机客户端进行管理。

2.3.2 WEB 管理

1、将交换机的模式开关拨动到"Web 管理"模式,使用网线将电脑网口与交换机的任意接口

相连。



2、将电脑的IP地址设置成与交换机同一网段,出厂状态下,交换机默认IP是192.168.0.1。

Internet 协议版本 4 (TCP/IPv4) 属性		×
常规		
如果网络支持此功能,则可以获取自动排 络系统管理员处获得适当的 IP 设置。	旨派的 IP 设置。否则,你需要从网	
○ 自动获得 IP 地址(<u>O</u>)		
— () 使用下面的 IP 地址(<u>S</u>):		
IP 地址(<u>l</u>):	192.168.0.20	
子网掩码(<u>U</u>):	255 . 255 . 255 . 0	
默认网关(<u>D</u>):		
○ 自动获得 DNS 服务器地址(B)		
● 使用下面的 DNS 服务器地址(E):		
首选 DNS 服务器(P):		
备用 DNS 服务器(<u>A</u>):	· · ·	
□退出时验证设置(L)	高级(⊻)	
	确定取消	

3、在电脑上打开浏览器, 输入 192.168.0.1, 即可正常管理交换机。

192.168.0.1/Logout.htm × +	– 🗆 X
← → C ① 不安全 192.168.0.1/Logout.htm	• 🛠 😝 🖸
TP-LINK [®]	
用户名: 密码: 登录 清除 Copyright © 2018 普联技术有限公司	
版权所有	

注意:如果输入正确用户名和密码之后,管理页面显示不全,可能是由于浏览器缓存原因 造成,此时按 Ctrl+F5 刷新页面即可。

2.3.3 TP-LINK Web 网管交换机客户端应用程序管理

1、设置电脑上安装"TP-LINK Web 网管交换机客户端应用程序"(下载地址:

https://service.tp-link.com.cn/detail_download_5553.html)。

- 2、设置电脑网口与交换机的任意接口相连。
- 3、运行"TP-LINK Web 网管交换机客户端应用程序",点击"刷新"按钮。

TP-LIN	<`					– • ×
交换机列表						
产品型号	设备描述	MAC地址	IP地址	主机IP地址	IP设置	登录
TL-SG2218	TL-SG2218	78-44-FD-7A-01-97	192.168.0.1	192.168.1.20	*	1
帮助					刷亲	fí

4、如果交换机 IP 与主机 IP 不在同一个网段,点击 IP 设置,将交换机 IP 修改为与主机 IP

在同一网段。(需要知道交换机正确的用户名和密码才能修改)

— 3/5/6/7/8 系列企业级交换机 —

TP-LIN	K.					- = x
交换机列表						
卒品型号	设备描述	MAC地址	IP地址	主机IP地址	IP设置	登录
TL-SG2218	TL-SG2218	78-44-FD-7A-01-97	192.168.0.1	192.168.1.20	*	1
帮助					刷新	

	IP设置			
T		MAC地址: 硬件版本: 软件版本:	78-44-FD-7A-01-97 TL-SG2218 1.0 1.0.0 Build 20180522 Rel.57913	
	-	设备描述:	TL-SG2218	
	ſ	IP地址:	祭用 192.168.1.1]
	L	子网掩码:	255.255.255.0	
		默认网关:	0.0.0	
		用户名 :	admin	
		密码:		
		应用	取消	

5、点击"登录",输入正确的用户名和密码,即可管理交换机。

— 3/5/6/7/8 系列企业级交换机 —

交換机列表 IP地址 主机IP地址 I	UD 11 BB	
产品型号 设备描述 MAC地址 IP地址 主机IP地址 I	(D)1 P	
	IP设置	登录
TL-SG2218 TL-SG2218 78-44-FD-7A-01-97 192.168.1.1 192.168.1.20	*	1
tent	Pil àr	
帮助	刷新	

TP-LIN	K.					
交换机列表						
产品型号	设备描述	MAC地址	IP地址	主机IP地址	IP设置	登录
TL-SG2218	TL-SG2218	78-44-FD-7A-01-97	192.168.1.1	192.168.1.20	*	1
		TP-LI 1 admin 6 记住用户名和密码 登录				
非 助					刷穿	Б

32

TP-LINK								TL-3	- □ 5G221	x 8 1.0
系统管理	二层交换	监控	VLAN	服务质量	帮助			保存	A	返回
➤ 系统信息	系统(言息								
• IP设置	设备描述	<u>*</u> :	TL-S	G2218						
• 用户设置	MAC地址	ut:	78-4	4-FD-7A-01-97						
• 备份与还原	IP地址: 子网墙码	1.	192. 255	168.1.1 255.255.0						
。又公垂白	默认网头	÷:	0.0.0).0						
* 永筑里启	软件版本	Σ:	1.0.0) Build 2018052	2 Rel.57913					
 系统恢复 	硬件版本	Σ:	TL-S	G2218 1.0						
• 系统升级	设备描述	<u>*</u> :	TL-	SG2218		应用				
	注意: 说	设备描述长;	度不能超过3	2个字符。						

2.4 各种交换机硬件拨码开关介绍

2.4.1 硬件拨码开关介绍

TP-LINK 不同型号的交换机拥有不同的拨码开关,因此可选择的工作模式不一样,适用的场 景也不一样,这篇文章主要介绍目前所有的交换机的硬件拨码开关及一些使用说明。

2.4.2 1 系列交换机

Г		-	Link/Act	No. of the second second
1	3	5	7 9 11 13 15 17 19 21 23	
				5045 0 M
2	4	6	8 10 12 14 16 18 20 22 24	WANRE
				标准交换————————————————————————————————————

标准交换:所有端口自由通信,适用于普通数据传输环境;

VLAN 隔离:端口与端口之间相互隔离,只能与上联口通信,适用于连接无线 AP 的使用场景,抑制网络风暴,提升网络性能。适合用在一些酒店、宿舍、无线覆盖,这种终端只需要上网不需要相互访问的场景中;

网络克隆:所有端口的 IEEE802.3x 流控功能关闭,适合用在一些使用广播或组播传输数据的环境中,如:学校视频教学、网吧网络克隆等。

2.4.3 1 系列 POE 交换机

模式组合 1



VLAN 隔离: 端口与端口之间相互隔离, 只能与上联口通信, 适用于连接无线 AP 的使用场景, 抑制网络风暴, 提升网络性能。适合用在一些酒店、宿舍、无线覆盖, 这种终端只需要上网不需要相互访问的场景中;

视频监控:通过调整交换机中的缓存资源,优化视频传输效率,减少监控网络中卡顿和马赛 克现象,适合用在一些视频监控应用场景;

标准交换:所有端口自由通信,适用于普通数据传输环境;

模式组合 2



标准交换:所有端口自由通信,适用于普通数据传输环境;

1~4 延长 (10Mbps): 1~4号 PoE 端口通过降低协商速率,实现更远距离 (200~300m) 的数据传输,适合用在一些网线较长的视频监控应用场景。

2.4.4 2 系列非云管理机型



VLAN 隔离:端口与端口之间相互隔离,只能与上联口通信,适用于连接无线 AP 的使用场景,抑制网络风暴,提升网络性能。适合用在一些酒店、宿舍、无线覆盖,这种终端只需要上网不需要相互访问的场景中;

Web 管理: 交换机支持本地 Web 管理,支持配置端口参数,支持设置端口速率,支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置;

标准交换:所有端口自由通信,适用于普通数据传输环境。



2.4.5 2 系列云管理机型

VLAN 隔离:端口与端口之间相互隔离,只能与上联口通信,适用于连接无线 AP 的使用场景,抑制网络风暴,提升网络性能。适合用在一些酒店、宿舍、无线覆盖,这种终端只需要上网不需要相互访问的场景中;

云管理: 交换机支持本地 Web 管理,支持配置端口参数,支持设置端口速率,支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置;同时交换机也支持云管理功 能,可以通过商云 APP 或者商用网络云平台进程远程管理。 标准交换:所有端口自由通信,适用于普通数据传输环境;

2.4.6 工业级交换机

类型 1



VLAN:开启/关闭端口与端口之间相互隔离,只能与上联口通信;

BSP:开启/关闭广播风暴保护功能;

以上两种功能都是用在工业场景,使用者根据实际需求决定是否开启。

类型 2



WEB:交换机支持本地 Web 管理,支持配置端口参数,支持设置端口速率,支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置;部分最新硬件版本(3.0 及以 上)的工业级交换机也支持云管理功能,可以通过商云 APP 或者商用网络云平台进程远程 管理。

BSP:开启/关闭广播风暴保护功能;

DIP 拨码开关 (P1-P10):开启/关闭对应端口中断报警功能,开启后端口如果断开且也通过 FAULT 接线端子接入了报警器的情况下,设备会输出报警信息给报警器产生报警;

类型 3



WEB:交换机支持本地 Web 管理,支持配置端口参数,支持设置端口速率,支持 802.1Q VLAN、MTU VLAN、端口 VLAN 等功能的配置;部分最新硬件版本(3.0 及以 上)的工业级交换机也支持云管理功能,可以通过商云 APP 或者商用网络云平台进程远程 管理。

BSP:开启/关闭广播风暴保护功能;

DIP 拨码开关 (P1-P10): 开启/关闭对应端口中断报警功能, 开启后端口如果断开旦也 通过 FAULT 接线端子接入了报警器的情况下, 设备会输出报警信息给报警器产生报警; ERPS: 环网开关, 默认关闭, 需要在 WEB 模式下才能开启, 开启后, 交换机开启 ERPS 的主环功能, 并使能 RPL 开关;

RPL:默认关闭,开启后,配置端口1为RPL口。

2.5 各种交换机复位方法介绍

2.5.1 2 系列交换机

1、Web 管理界面复位方法

登录交换机管理页面"系统管理"-"系统工具"-"系统恢复",点击"复位"按钮即可。

系统恢复	
	恢复到出厂设置并重启系统。
	复位
注意: 系统恢复后4	5.地配置将会丢失,所有配置将会恢复成默认配置。

2、硬件复位方法

2.1、非云管理交换机



模式开关由 Web 管理拨至标准交换,再快速(2s内)拨回 Web 管理。

2.2、云管理交换机

模式开关由云管理拨至标准交换,再快速 (2s内)拨回云管理。



2.5.2 3/5/6/7/8 系列交换机

1、Web 管理界面复位方法

登录交换机管理页面"系统管理"-"系统工具"-"软件复位",点击"复位"按钮即可。

TP-LINK [®]	
TL-SH7428	启动配置 配置导入 配置导出 软件升级 系统重启 软件复位
系統管理 · 系統管理 · 所戶管理 · 系统管理 · SDM模板 · 安全管理 · SDM模板 · 建叠功能 · 二层交换 VLAN 生成树 组播管功能 服务质量 访问控制	\$\$ <br< th=""></br<>

- 2、Console 接口复位方法
- 2.1、Console 接口未设置登录密码
- 1、电脑连接交换机的 Console 接口,具体连接和设置方法参见"二层网管交换机的管理方

法"或"三层网管交换机的管理方法"。

2、使用 reset 命令对交换机进行复位.

复位命令举例:

TL-SH7428>enable

TL-SH7428#reset

System software reset, are you sure? (Y/N):y

2.2、Console 接口设置了登录密码

1、电脑连接交换机的 Console 接口,具体连接和设置方法参见"二层网管交换机的管理方

法"或"三层网管交换机的管理方法"。

2、对设备重新上电的过程中,当串口界面中出现"Hit any key to stop autoboot"提示的

时候,按任意键,出现如下界面:



3、选择2,选择复位交换机。



4、如果交换机使用的比较早期的软件版本,在启动时,当串口界面中出现"Press CTRL-B

to enter the bootUtil"及时按下 Ctrl+B, 在出现的界面中选择 reset。

Press CTRL-B to enter the	bootUtil
	IF-LIMA DUUIUIL(VI.U.U)
Conversion in the	(-) 9046 TD TWW TL P- +J
Copyright Costs D	(C) 2010 IFFLIMK IECN. CO., LTO Han May 17 2016 17-54.47
create Da	te: nar 17 2010 17:54:47
heln	- print this list
reboot	- reboot the sustem
ifconfig	- config the interface
fto	- config the remote host in the user name user password
and the image file name	
upgrade	– upgrade the firнµare
start	– start the sustem
reset	– reset the system to the factory config.
[TP-LINK]: ^	
[TP-LINK]:	
[TP-LINK]: ^	
[TP-LINK]: reset	

第3章 交换设置

3.1 交换机端口监控配置指南

3.1.1 应用介绍

端口监控是一种数据包获取技术,可以实现将一个或几个端口(被监控端口)的数据包复制 到一个特定的端口(监控端口),通过对收集到的数据包进行分析,可以达到网络监控或排 除网络故障的目的。

3.1.2 需求介绍

网络中有一台安装了数据包分析软件的主机连接在交换机的 3 号端口, 需要对网络中电脑的上网行为进行监控。示意网络拓扑如下:



3.1.3 设置方法

1、在"二层交换->端口管理->端口监控"中,点击编辑,如下如所示。

	께니패꾼	端口安全 端口	隔离环路监测	
监控组列表	Ę			
监控组	监控端口	监控方式	被监控端口	操作
		仅入口监控		
1		仅出口监控		编辑 清空
		出入口监控		
			帮助	
	监控组列录 监控组 1	協控组列表 监控组 1	協控组列表 监控端口 监控方式 1 仅入口监控 1 仅出口监控 出入口监控	協控組列表 協控方式 被监控端口 监控组 监控方式 被监控端口 1 仅入口监控 1 仅出口监控 出入口监控 部助

选择监控端口3的,并点击提交;在被监控端口中选择需要被监控的端口5.6口,入口出口

均选择启用,点击提交,如下图所示。

- 3/5/6/7/8 系列企业级交换机 -

端口配置 端口监控	端口安全 端口隔离	环路监测	
监控端□			
监控端口:	1/0/3 (格式:	1/0/1) 提交	1
			1
UNIT: 1			
2 4 6 8	10 12 14 16 18 20 22	24	
1 3 5 7	9 11 13 15 17 19 21	23 25 26 27 28	
	🗋 未选中的端口 🛛 📄 🖞	选中的端口 📄 不可选端口	
被监控端□			
UNIT: 1 L	AGS		
选择端口	入口监控	出口监控	LAG
	~	~	
1/0/1	禁用	禁用	^
1/0/2	禁用	禁用	
1/0/3	禁用	禁用	
1/0/4	禁用	禁用	
1/0/5	启用	启用	
1/0/6	启用	启用	
1/0/7	祭用	第用 林田	
1/0/8	宗用	一 宗用 林田	
1/0/10		示巾 	
1/0/11	—————————————————————————————————————		
1/0/12	禁用	禁用	+
	全选 提交	返回 帮助	

2、提交后可以看到被监控端口状态列表:

端	口配置	端口监控	端口安全 端口	隔离 环路监测	
	监控组列制	麦			
	监控组	监控端口	监控方式	被监控端口	操作
			仅入口监控		
	1	1/0/3	仅出口监控		编辑 清空
			出入口监控	1/0/5-6	
				帮助	

至此已完成设置,注意保存配置以免掉电导致配置丢失。

3.1.4 配置注意事项

设置过多被监控端口可能造成网络不稳定,网络中流量较大时不建议一次性设置过多被监控端口。

47

3.2 交换机端口隔离配置指南

3.2.1 应用介绍

端口隔离功能可以限制一个端口到另外一组端口的数据转发。这种限制数据转发的方式和通过 VLAN 进行限制的方式很相似,但是限制性更强。通过设置端口隔离可以在物理上隔绝开两个端口通讯,一般适用于一些对广播流量比较敏感的场所,通过设置端口隔离来隔绝广播域。

3.2.2 需求介绍

某购物商场进行无线覆盖组网,使用双频 AP 搭配 AC 的组网方案,为了隔离 AP 和 AP 之间的通讯,减少广播流量的干扰,增强无线的运行稳定性,采用在接入交换机上进行端口隔离的设置,使 AP 只能和上联的 AC 通讯,相互之前不能通讯,网络拓扑如下:



3.2.3 设置方法

在"二层交换->端口管理->端口隔离"中,点击编辑,选择对应端口的转发端口,本次举例设置 2-28 端口的转发端口为1端口;因为1口是上联口,1端口的转发端口为所有端口,如下如所示。

1、设置 2-28 端口只转发到 1 端口:

- 3/5/6/7/8 系列企业级交换机 -

端口配置 端口监控 端口安全 端口隔离 环路监测
端口隔离配置
端口:
UNIT: 1 LAGS
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28
全选
转发端口:
UNIT: 1 LAGS
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28
全选 清空 提交 返回
🔁 未选中的端口

2、设置1端口可以转发1-28端口:

端口配置 端口监控 端口安全 端口隔离 环路监测
端口隔离配置
端口:
UNIT: 1 LAGS
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28
結労端口・
UNIT: 1 LAGS
2 4 6 8 10 12 14 16 18 20 22 24
1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28
全选 清空 提交 返回
🔁 未选中的端口 📄 选中的端口 💼 不可选端口

设置完端口和转发端口的关系,点击提交,可以看到如下的端口转发列表:

端口配置 端[二监控 端口安全	端口隔离	环路监测	
端口隔离列表				
UNIT:	1 LAGS			
端口	LAG		转发端口	
1/0/1			1/0/1-28	<u>^</u>
1/0/2			1/0/1	
1/0/3			1/0/1	
1/0/4			1/0/1	
1/0/5			1/0/1	
1/0/6			1/0/1	
1/0/7			1/0/1	
1/0/8			1/0/1	
1/0/9			1/0/1	
1/0/10			1/0/1	
1/0/11			1/0/1	-
		编辑	帮助	

至此已完成设置, 2-28 口上的 AP 只能和 1 口接的 AC 设备通讯, AP 相互之间不能通

讯。另外请注意保存配置以免掉电导致配置丢失。

3.3 交换机端口安全配置指南

3.3.1 应用介绍

一些网络场景下需要通过限制端口的最大学习 MAC 数目,来防范 MAC 地址攻击和控制端 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,保证安全性,通常将静态地址表+端口安全结合起来使用。

3.3.2 需求介绍

某公司管理员要求交换机的端口 1 只能是静态地址表中 1 个 MAC 对应的设备可以上网, 不在静态地址表中的设备则无法上网,那么设置端口安全功能针对端口 1 设置最大学习地 址数为 0.,并且在静态地址表中添加允许上网的这个设备的 MAC。

3.3.3 设置方法

1、在交换机 web 界面"二层交换-> 端口管理-> 端口安全", 设置端口安全, 端口 1 最 大学习地址数为 0: - 3/5/6/7/8 系列企业级交换机 -

TL-SG5210PE	端口配置	端口监控	端口安全 端口	隔离环路监测	1	
	端口安全	È				
系统管理	UNIT:	1				
二层交换	选择	端口	最大学习地址数	已学习地址数	学习模式	状态
・端口管理					× ×	× I
・ 汇聚管理		1/0/1	0	0	永久	启用
• 流量统计		1/0/2	1024	0		
 ・地址表管理 		1/0/3	1024	0 12	直 端」最大	、字习地业数为0
VLAN		1/0/4	1024	0	动态	禁用
生成树		1/0/5	1024	0	动态	禁用
组播管理		1/0/6	1024	0	动态	禁用
路由功能		1/0/7	1024	0	动态	禁用
服务质量		1/0/8	1024	0	动态	禁用
PoE		1/0/9	1024	0	动态	禁用
访问控制		1/0/10	1024	0	动态	禁用
网络安全				「担か」	15Bh	
SNMP			主应	LEX:	++++4/J	
LLDP	×+					
系统维护	注意:	14-11 #665.7*6				
配置保存	·	ARALEX ROYOR	町750-1024。			

2、针对端口1做静态地址绑定,绑定允许上网的设备。

TL-SG5210PE	地址表显示 静态地址表 动态地址表 过滤地址表	
系统管理	MAC地址: 30-EA-07-0D-0B-CC (格式为: 00-00-00-00-01)	
二层交换	VI AN ID: (1-4094)	添加
 ・端口管理 ・ 二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、	·····································	10-15
・汇聚管理	靖山:	
・流量统计	UNIT: 1 LAGS	
 ・地址表管理 		
VLAN		
生成树		
组播管理	绑定端口1	
路由功能		
服务质量		
PoE		
访问控制	查找选项:	查找
网络安全		
SNMP	静态地址表	
LLDP	UNIT: 1	
系统维护	选择 MAC地址 VLAN ID 端口 地址类型 等	8化状态
配置保存		
索引页面	□ 80-EA-07-0D-0B-CC 1 1/0/1 配置静态地址	不老化
退出登录		
	いいに、「当前1920小1940年第日数」「 添加后显示列表	
	新队亚尔印苏日数工作值为100余,消从古草找按钮获取元釜印的址衣后息。	

进行如上设置后,则只有 MAC 为 80-EA-07-0D-0B-CC 的设备接在端口 1 的 VLAN1 下能

上网,其他设备接到端口1则无法上网。

3.4 交换机端口汇聚配置指南

3.4.1 应用介绍

端口汇聚功能是将交换机的多个物理端口汇聚在一起形成一个逻辑上的物理端口,同一汇聚 组内的多条链路则可视为一条逻辑链路。端口汇聚主要有两个作用:带宽叠加、链路备份。

3.4.2 需求介绍

某企业中有两个部门,每个部门有两个办公点,每个办公点的两个部门各有一个接入交换机, 不同办公点之间通过核心交换机进行连接,现在需要核心交换机之间的链路进行汇聚,同时 不同部门需设置不同 VLAN。本文以 TL-SG5428PE 为例介绍如何在(3/5/6/7/8)系列交 换机设置端口汇聚以及在 VLAN 设置时如何使用该功能。网络拓扑如下:



3.4.3 设置方法

1、静态聚合设置方法

在"二层交换->汇聚管理->手动配置"中,下拉选择 LAG 组号如 LAG1,选择需要进行汇聚 的端口如 23-24 号端口,点击提交。 - 3/5/6/7/8 系列企业级交换机 -

TL-SG5428PE	汇聚列表 手动配置 LACP配置
系统管理 二层交换 • 端口管理	汇聚组配置 汇聚组号: 工聚组描述:
 ・	成员端口 UNIT: 1 2 4 6 8 10 12 14 16 18 20 22 24 26 28 1 3 5 7 9 11 13 15 17 19 21 23 25 27 清空 提交 解助

2、动态聚合设置方法

在"二层交换->汇聚管理->LACP 配置"中,选择需要进行汇聚的端口,输入管理 Key (即 LAG 组号 1-8),状态下拉选择开启,点击提交。

TL-SG5428PE	汇聚列表 月	F动配置	LACP配置					
Contractor and	全局配置							
系统管理	系统优势	先级:	32768	(0-65535)			提交	
二层交换								
・端口管理	LACP配置							
 ・ : 聚管理 	UNIT :	1						
• 流量统计	选择	端口	管理Key	端口优先级(0-65535)	模式	状态	LAG	
• 地址表管理			8			启用 ~		
VLAN		1/0/14	0	32768	被动	禁用		~
生成树		1/0/15	0	32768	被动	禁用		
组播管理		1/0/16	0	32768	被动	禁用	· · · · ·	
路由功能		1/0/17	0	32768	被动	禁用		
服务质量		1/0/18	0	32768	被动	禁用		
PoE		1/0/19	0	32768	被动	禁用		
访问控制		1/0/20	0	32768	被动	禁用	-	
网络安全		1/0/21	0	32768	被动	禁用		۰.
SNMP		1/0/22	0	32768	被动	禁用		1
LLDP		1/0/23	0	32768	被动	禁用	LAG 1	1
系统维护		1/0/24	0	32768	被动	禁用	LAG 1	1
配置保存		1/0/25	0	32768	被动	並用		
索引页面		1/0/26	0	32768	被动			
		1/0/27	0	32768	被动	並用		
退出登录		1/0/28	0	32768	被动	並用		~
						3013		
				全选 提交 帮	助			
	×.							
	注意:		田冲积中安生产场风目	建议中国生命物情能				
			37321住中广生) 浦风嶺 9666号20月14日中1	 ・ 建以后用注意内引起。 				
	2、口砼////////////////////////////////////	明心LAG	且的成页」而日元法后用L					

3、 VLAN 设置时如何使用汇聚端口

多个端口进行汇聚后在逻辑上是一个端口,进行 VLAN 设置时与普通端口类似,只是需要 注意手动选择 LAGS 列表。具体设置方法如下:

1、设置端口类型为 TRUNK。在"VLAN->802.1Q VLAN->端口配置"中,在 VLAN 端口配

置的 UNIT 列表中选中 LAGS,将端口 LAG1 的端口类型配置为 TRUNK,点击提交。

rl-SG5428PE	VLAN配置 端口配	置			
系统管理	VLAN端口配置 UNIT: 1L	AGS			
二层交换 VLAN	选择 端口	端口类型 TRUNK V	PVID	LAG	所属VLAN
802.1Q VLAN	LAG1	ACCESS	1		查询
MAC VLAN 协议VLAN VLAN VPN	LAG8	ACCESS 全选	1 【提交】[查询

2、划分 VLAN:在"VLAN->802.1Q VLAN->VLAN 配置"中,分别创建 VLAN10、VLAN20 选择对应的端口,注意汇聚端口需设置为 Tagged,在 Tagged 端口的 UNIT 列表中选择 LAGS,再选择对应的汇聚端口,点击提交。如下图 LAG1 口为 Tagged,9-16 口为 Untagged。

VLAN配置端口配置	
VLAN信息	
VLAN ID :	10 (1 - 4094)
VLAN 名称:	产品部 (1-16个字符)
Untagged 端口	
UNIT : 1 LAGS	
2 4 6 8 10	12 14 16 18 20 22 24 26 28
	11 13 15 17 19 21 23 25 27
	全选 清空
Tagged 端口	
UNIT : 1 LAGS	
12345	6 7 8
	全选 清空 提交 帮助
E	🗋 未选中的端口 🛛 🕋 选中的端口 💭 不可选端口

3、VLAN20的设置重复第2步即可。添加完成后, VLAN 列表如下:

VLAN	配置列表			
选择	VLAN_ID	名称	成员	操作
112	1	System-VLAN	1/0/1-8,1/0/25-28,LAG1,LAG8	编辑 详细
	10	产品部	1/0/1-2,1/0/9-16,LAG1	编辑 详细
	20	研发部	1/0/1-2,1/0/17-24,LAG1	编辑 详细

至此已完成设置,注意保存配置以免掉电导致配置丢失。

3.4.4 配置注意事项

属于同一个汇聚组中的成员端口必须有一致的配置,这些配置主要包括 STP、QoS、
 VLAN、端口属性、MAC 地址学习等。如果需要配置汇聚组,建议在优先配置汇聚组
 后,再配置汇聚组的其它功能。如果两台设备之间做端口汇聚,两者必须都支持端口汇
 聚,否则可能会导致环路。

- 开启 802.1Q VLAN、语音 VLAN、生成树、QoS 配置、DHCP 侦听及端口配置 (速 率、流控)功能的端口,若属于汇聚组成员,则他们的配置需保持一致。
- 开启端口安全、端口监控、MAC 地址过滤、静态 MAC 地址绑定、半双工及 802.1X
 认证功能的端口,不能加入汇聚组。
- 开启 ARP 防护、DoS 防护功能的端口,建议不要将其加入汇聚组。
- 链路聚合分为静态聚合和动态聚合,实际应用中使用其中一种即可,我司产品推荐使用
 静态聚合的方式。

3.5 交换机地址表管理功能使用指南

3.5.1 交换机地址表介绍

TP-LINK 3/5/6/7/8 系列交换机都带有地址表管理功能,交换机的地址表管理功能是管理 交换机所学习到 MAC 的集中展示的地方,通过交换机的地址表管理功能,可以优化网络流 量或者保障络安全。交换机的地址表管理功能主要分以下几个功能模块,现分别简介下各个 模块的功能和应用场景。

3.5.2 地址表显示

该地址表包含了端口间报文转发的地址信息,是交换机实现二层报文快速转发的基础。可以 在本页查看到交换机地址表的全部信息。

查询选项					
□ MAC地址:		(格式为: 00	-00-00-00-00-01)		
□ VLAN ID: 〔1-4094〕					
端口: 查询板块,可以查询到交换机新学习和记录到的所有的地址信息,					
UNIT: 1 LAGS 包括动态地址,手动配置的静态地址和过滤地址。					
2 4 6 8 10 1	2 14 16 18 20	22 24			
1 3 5 7 9 1	1 13 15 17 19	21 23 25	26 27 28		
P					
	大洗中形[[清]	选中的/扁口			
地址表显示					
地址表显示 UNIT: 1					
地址表显示 UNIT: 1 MAC地址	VLAN ID	端口	地址类型	老化状态	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44	VLAN ID 100	端口 1/0/23	地址类型 配置静态地址	老化状态 不老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77	VLAN ID 100 1	端口 1/0/23	地址类型 配置静态地址 过滤地址	老化状态 不老化 不老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F	VLAN ID 100 1 100	端口 1/0/23 1/0/20	地址类型 配置静态地址 过滤地址 动态地址	老化状态 不老化 不老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF	VLAN ID 100 1 100 100	端口 1/0/23 1/0/20 1/0/20	地址类型 配置静态地址 过滤地址 动态地址 动态地址	老化状态 不老化 不老化 正在老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF F4-2A-7D-6C-BE-12	VLAN ID 100 1 100 100 100 1	端口 1/0/23 1/0/20 1/0/20 1/0/25	地址类型 配置静态地址 过滤地址 动态地址 动态地址 动态地址	老化状态 不老化 不老化 正在老化 正在老化 正在老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF F4-2A-7D-6C-BE-12 F4-2A-7D-82-7A-26	VLAN ID 100 1 100 100 100 1 1	端口 1/0/23 1/0/20 1/0/20 1/0/25 1/0/2	地址类型 配置静态地址 过滤地址 动态地址 动态地址 动态地址 动态地址	老化状态 不老化 不老化 正在老化 正在老化 正在老化 正在老化 正在老化 正在老化 正在老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF F4-2A-7D-6C-BE-12 F4-2A-7D-6C-BE-12 F4-2A-7D-82-7A-26 F4-2A-7D-82-7A-26	VLAN ID 100 1 100 100 1 1 1 1 100	端口 1/0/23 1/0/20 1/0/20 1/0/25 1/0/2 1/0/18	地址类型 配置静态地址 过滤地址 动态地址 动态地址 动态地址 动态地址 动态地址	老化状态 不老化 不老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF F4-2A-7D-6C-BE-12 F4-2A-7D-6C-BE-12 F4-2A-7D-82-7A-26 F4-2A-7D-82-7A-26 F4-2A-7D-82-7A-26 F4-2A-7D-82-7A-26	VLAN ID 100 1 100 100 1 1 100 1 1 100 1	端口 1/0/23 1/0/20 1/0/20 1/0/25 1/0/2 1/0/18 1/0/4	地址类型 配置静态地址 过滤地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址	老化状态 不老化 不老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF F4-2A-7D-6C-BE-12 F4-2A-7D-6C-BE-12 F4-2A-7D-82-7A-26 F4-2A-7D-82-7A-26 F4-2A-7D-80-7E-BD F8-8C-21-25-83-94 F8-8C-21-A4-4D-63	VLAN ID 100 1 100 100 1 1 100 1 100 1 100	端口 1/0/23 1/0/20 1/0/25 1/0/2 1/0/18 1/0/4 1/0/20	地址类型 配置静态地址 过滤地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态	老化状态 不老化 不老化 正在老化 正在老化	
地址表显示 UNIT: 1 MAC地址 00-11-22-33-55-44 00-22-33-55-88-77 6E-D4-50-A6-6F-9F D2-86-99-70-73-BF F4-2A-7D-6C-BE-12 F4-2A-7D-6C-BE-12 F4-2A-7D-B2-7A-26 F4-2A-7D-B2-7A-26 F4-2A-7D-E0-7E-BD F8-8C-21-A4-4D-63	VLAN ID 100 1 100 100 1 1 100 1 100 1 100 1 100	端口 1/0/23 1/0/20 1/0/20 1/0/25 1/0/2 1/0/18 1/0/4 1/0/20	地址类型 配置静态地址 过滤地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址 动态地址	老化状态 不老化 不老化 正在老化	

3.5.3 静态地址表

静态地址由用户手工添加和删除,不受最大老化时间的限制。对于网络拓扑相对固定的使用环境来说,使用静态地址绑定可以提高交换机的转发效率,减少网络中的广播流量。

地址表显示 静态地址表 动态地	此表 过滤地址表		
新建条目			
MAC地址:	(格式为: 00	-00-00-00-01)	
VLAN ID:	(1-4094)		添加
端口:		王动添加静本地加	1. 素栏 雪亜同时添加
UNIT: 1 LAGS		MAC地址, VLAN	NID, 端口的对应关系
2 4 6 8 10 12 14	16 18 20 22 24		
1 3 5 7 9 11 13	15 17 19 21 23 25 2	6 27 28	
1 未送	中的端口 🌕 选中的端口	一 不可选端口	
查找条月			
查找洗项: 全部	· · · · · · · · · · · · · · · · · · ·		查找
静态地址表 MA VLA	ン地址 N ID 土地	烟毒洗咖的基大地北丰	
UNIT: 1 端口		这条体加口的形态和出现	
选择 MAC地址	VLAN ID	地址类型	老化状态
	100 1/0/22	副帶格大地也	エキル
00-11-22-33-35-44	100 1/0/23		1-2112
	全选 提交 删除	*	
		展示所有或者搜索条件下的	
所有UNIT地址条目总数: 1			
注意: 野江目天的冬日粉上阳店头400条 ···	主占土本将达纽兹取合教的协业主信间	3	
新小业小时东口数上附值为100余,1	月尽山里找按钮获取元罡的地址发情题	5°°	

3.5.4 动态地址表

动态地址是交换机通过自动学习获取的 MAC 地址。交换机通过自动学习新的地址和自动老

.

化掉不再使用的地址来不断更新其动态地址表。

自动 老化	老化: 素化: 素(1) 新日日: 300 	調 〇 禁用	秒(10-630秒,默认	人为: 300秒)	提交
查找条目	1		配置交换机自动学	学习到的地址表的老化	时间
查找	选项: 全部	~			查找
动太地加	-=				
UNIT:	1				
选择	MAC地址	VLAN ID	端口	地址类型	老化状态
0	6E-D4-50-A6-6F-9F	100	1/0/20	动态地址	正在老化
	F4-2A-7D-B2-7A-26	1	1/0/2	动态地址	正在老化
	F4-2A-7D-E0-7E-BD	100	1/0/18	动态地址	正在老化
	F8-8C-21-25-83-94	1	1/0/4	动态地址	正在老化
	F8-8C-21-A4-4D-63	100	1/0/20	动态地址	正在老化
		全选 册	JI除	帮助	
UNIT: 1 所有UNIT	显示的地址条目数: 5 「地址条目总数: 5	展示交换机	所学习到所有的动态 "	地址表信息,并且可以 ま中	儿在这个表格中选择条 目

3.5.5 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,即此处是配置交换机的 MAC 地址转发黑名单,此列表中的 MAC 数据包到了交换机,交换机会选择丢弃。过滤地 址不会被老化,只能手工进行配置和删除。
啦表显示	静态地址表	动态地址表	过滤地址表				
新建条目							
MAC	地址:			(格式为: 0	0-00-00-00-00	-01)	
VLAN	ID:			(1-4094)			添加
查找条目		新建地址表	条目,该条目可	J以不选择端L	1号,交换机	匹配到此条目	目后的数据包将会丢弃。
查找说	选项:		~				重找
过滤地址	表						
选择	MAC地址		VLAN ID	词词	tt.	地类型	老化状态
	00-22-33-55-8	38-77	1		ì	İ滤地址	不老化
			全选	删除	帮助	展示所有通	过手动配置的黑名单条目
地址条目总	总数: 1						
地址条目总 注意:	总数: 1						
地址条目总 注意: 默认显示的	总数: 1 均条目数上限值为	100条,请点击	查找按钮获取完	整的地址表信息	1.		

第4章 堆叠功能

4.1 交换机堆叠配置指导

4.1.1 应用介绍

堆叠 (Stack) 是指将多台设备通过专用的堆叠口连接起来, 堆叠系统由多台成员设备组成, 主交换机 (Master) 设备负责堆叠系统的运行、管理和维护, 其他成员设备在处理业务的同 时可作为主交换机的备份。一旦主交换机设备故障, 系统会迅速自动选举新的主交换机, 以 保证业务不中断, 从而实现了设备的 1: N 备份。进行必要的配置后, 所有设备虚拟化成一 台"分布式设备"。使用堆叠技术可以实现多台设备的协同工作和统一管理, 对外表现就像 一台设备一样。

4.1.2 需求介绍

某大型网络为了保障网络运行的稳定性,并且增加转发带宽使用三台 TL-SH8434 交换机进行堆叠组网,设备堆叠后要求达到以下网络需求:

1、强大的网络扩展能力, 堆叠增加交换机的背板带宽, 增加端口数量;

2、堆叠后设备统一成一台设备,统一配置;

3、增加设备的冗余备份能力,保障网络的稳定性。



4.1.3 设置方法

第一步、堆叠前准备

准备三台出厂状态下的 TL-SH8434 交换机,三根 1 米万兆 SFP+电缆 TL-TC532-1 用于连接交换机的堆叠口。

第二步、堆叠口的配置

TL-SH8434 有 6 个端口可以配置成堆叠端口, 其中 4 个万兆 SFP+和 2 个 QSFP+端口, 如图:



1、分别登录 3 台设备的 web 界面,在"堆叠功能—堆叠管理—堆叠配置"界面设置堆叠

口,	\Box ,	将选中的堆叠口状态设置成启用,	本次选择将交换机的 29.30 口设置成堆叠口。
----	----------	-----------------	--------------------------

堆叠端口	配置			
UNIT :	4 5 6			
选择	堆叠口	堆叠口组	堆叠功能	状态
			¥	
	4/0/29	0	启用	OK
	4/0/30	0	・	OK
	4/0/31	1	禁用	Ethernet
	4/0/32	1	禁用	Ethernet
	4/0/33	2	禁用	Ethernet
	4/0/34	2	禁用	Ethernet
		全选	提交帮助	

2、在进行物理连线之前分别配置三台交换机:

(1) 设置堆叠名称:在"堆叠功能—堆叠管理—堆叠配置"页面设置堆叠名称 (可选操作);

(2) 设置堆叠口:在"堆叠功能—堆叠管理—堆叠配置"页面中将堆叠口状态设置为启用(必选操作);

(3)配置堆叠编号:在"堆叠功能—堆叠管理—堆叠成员配置"页面中分别设置三台交换机的堆叠编号为4、5、6。(可选操作)

备注:每台设备独立配置,配置之后请记得保存配置。

3、将三台交换机分别设置后保存配置后断电,然后按照链式或者环式的连接方式进行物理接线。

4、物理连接后,给设备上电,堆叠开始形成,堆叠后只有作为主交换机的"Master"指示灯 会亮。



	Port 1~28	● 1000Mbps ● 10/100Mb - 巻 activity	; ps	Port 2	5F~28	8F [4	● 100 5- acti)0Mbp ivity	5	Port 29	~32 → 32 → 10Gbps → activity	s Management	
		PWR			12	16	20	24	28	32		-	
-		SYS					19	23	27	31		The second second	
-		Master				14	18	22	26	30	. [
		RPS			9	13		21	25	29	÷¢	Console	1
	_												
	Port 1~28	[● 1000Mbp ● 10/100M - ⇔ activity	is bps	Port 2	5F~28	8⊨[.,	● 100 5- acti	0Mbp vity	' ^s F	Port 29-	32 → 10Gbps → 1Gbps → activity	Management	2
		PWR					20	24	28	32			
		SYS								31			
		Master				14			26	30			
		RPS						21	25	29	*	Console	1
	Port 1-3	28 1000Mt 10/100/ & activity PWR SYS Master RPS	Mbps Mbps Mi 3 2 1	Port aste 7 6 5	25F~2 12 11 10 9	18F [16 15 14 13	100 55 act 20 19 18 17	24 23 22 21	28 27 26 25	20rt 29~ 32 31 30 29	32 • 10Gbps • 1Gbps * activity	Management	

堆叠系统形成后,用户可以通过任意成员设备的端口登陆堆叠系统。堆叠后的配置分为全局 配置和端口配置,涉及到端口相关的配置会在相应的界面显示不同 Unit,通过选择不同 Unit 来配置不同交换机的端口。

堆叠信息展示:

館息	堆叠配置	≝ `						
	-							
堆聲信	思							
	堆叠排	石扑		Ring				
	堆叠М	/IAC		80-8F	-1D-0F-3B	-78		
成员信	良							
成员号	新成员号	角色	M	AC地址	优先级	版本	机型	状态
4	4	Member	54-75-9	95-ED-90-07	3	2.1.1	TL-SH8434	Ready
5	5	Master	80-8F-1	1D-0F-3B-78	12	2.1.1	TL-SH8434	Ready
6	6	Member	80-8F-1	1D-0F-3B-90	10	2.1.1	TL-SH8434	Ready
堆叠口	信息							
UNIT	: 45	5 6						
堆	遷口	堆叠	口组	状态			邻居	
4/	/0/29	0		OK			5	
4/	/0/30	0		OK			6	
4/	/0/31	1		Ethernet	t		None	
4/	/0/32	1		Ethernet	t		None	
4/	/0/33	2		Ethernet	t		None	
4/	/0/34	2		Ethernet	t		None	
				刷新	帮助]		

4.1.4 配置注意事项

- 堆叠的设备型号和软件版本要求一样;堆叠后全局配置会沿用 Master 设备的配置。
- 如果设备不是在出厂状态下配置,堆叠形成后哪个设备是 Master,就会沿用这个设备 的所有配置。
- 堆叠配置是无法通过复位交换机消除的,需要手动关闭堆叠口和其它堆叠功能。
- 设备对应端口启用了堆叠功能后无法再用作业务口配置。

第5章 VLAN

5.1 交换机 802.1Q VLAN 配置指南

5.1.1 应用介绍

802.1Q VLAN 可以实现局域网内二层网络的隔离以及跨交换机的 VLAN 互访, 在中大型网络中为了隔离广播域, 设置 802.1Q VLAN 是一个非常有效且方便的办法, 这样既能保证用户带宽, 也能降低设备因为处理局域网广播所带来的性能损耗。

5.1.2 需求介绍

802.1Q VLAN 可以实现局域网内二层网络的隔离以及跨交换机的 VLAN 互访,本文以 TL-SG5428PE 为例介绍 (5/6/7/8) 系列交换机设置 IEEE 802.1Q VLAN 的方法。

实例:同一个公司的同一个部门有多个不同的办公地点(比如在不同的楼层),各办公点有 各自的交换机,级联形成同一个局域网,要求不同部门划分 VLAN。网络拓扑如下:



5.1.3 设置方法

以交换机一为例,端口1接路由器,端口2接交换机二端口1。

1、确定端口类型:将端口 1-2,5-12 设置为 GENERAL。在"VLAN->802.1Q VLAN->端 口配置"中,勾选对应端口进行设置,注意 5-8 需将 PVID 设置为 10,9-12 需将 PVID 设置 为 20。

VLAN	端口配置				
UNIT	: 1	LAGS			
选择	端口	端口类型	PVID	LAG	所属VLAN
		GENERAL V			
	1/0/1	ACCESS	1		查询 个
	1/0/2	ACCESS	1		查询
	1/0/1 1/0/2	GENERAL V ACCESS ACCESS	1 1		查询 查询

端口配置				
[: 1	LAGS			
端口	端口类型	PVID	LAG	所属VLAN
	GENERAL \sim	10		
1/0/1	GENERAL	1		查询 个
1/0/2	GENERAL	1		查询
1/0/3	ACCESS	1		查询
1/0/4	ACCESS	1		查询
1/0/5	ACCESS	1		查询
1/0/6	ACCESS	1		查询
1/0/7	ACCESS	1		查询
1/0/8	ACCESS	1		查询
	端口配置 : 1 端口 1/0/1 1/0/2 1/0/3 1/0/4 1/0/5 1/0/6 1/0/7 1/0/8	端口配置 端口配置 端口 端口 端口 端口 端口 端口 愛型 GENERAL 1/0/1 GENERAL 1/0/2 GENERAL 1/0/3 ACCESS 1/0/4 ACCESS 1/0/5 ACCESS 1/0/6 ACCESS 1/0/7 ACCESS 1/0/7 ACCESS 1/0/8 ACCESS	端口配置 端口 端口类型 PVID GENERAL ✓ 10 1/0/1 GENERAL 1 1/0/2 GENERAL 1 1/0/3 ACCESS 1 1/0/4 ACCESS 1 1/0/5 ACCESS 1 1/0/6 ACCESS 1 1/0/7 ACCESS 1 1/0/8 ACCESS 1	端口配置 : 1 LAGS 端口 ※型 PVID LAG GENERAL 10 1/0/1 GENERAL 1 1/0/2 GENERAL 1 1/0/3 ACCESS 1 1/0/4 ACCESS 1 1/0/5 ACCESS 1 1/0/6 ACCESS 1 1/0/7 ACCESS 1 1/0/8 ACCESS 1

VLAN	端口配置				
UNIT	: 1	LAGS			
选择	端口	端口类型	PVID	LAG	所属VLAN
		GENERAL 🗸	20		
	1/0/1	GENERAL	1		査询 ヘ
	1/0/2	GENERAL	1		查询
	1/0/3	ACCESS	1		查询
	1/0/4	ACCESS	1		查询
	1/0/5	GENERAL	10		查询
	1/0/6	GENERAL	10		查询
	1/0/7	GENERAL	10		查询
	1/0/8	GENERAL	10		查询
	1/0/9	ACCESS	1		查询
	1/0/10	ACCESS	1		查询
	1/0/11	ACCESS	1		查询
	1/0/12	ACCESS	1		查询

设置完后的端口配置列表:

VLAN	端口配置				
UNIT	: 1	LAGS			
选择	端口	端口类型	PVID	LAG	所属VLAN
		~			
	1/0/1	GENERAL	1		査询 ヘ
	1/0/2	GENERAL	1		查询
	1/0/3	ACCESS	1		查询
	1/0/4	ACCESS	1		查询
	1/0/5	GENERAL	10		查询
	1/0/6	GENERAL	10		查询
	1/0/7	GENERAL	10		查询
	1/0/8	GENERAL	10		查询
	1/0/9	GENERAL	20		查询
	1/0/10	GENERAL	20		查询
	1/0/11	GENERAL	20		查询
	1/0/12	GENERAL	20		查询

VLAN 的划分:在"VLAN->802.1Q VLAN->VLAN 配置"中,分别创建 VLAN10、
 VLAN20 将产品部划分为 VLAN 10,选择对应的端口,注意需将级联口包含进去,如下图
 端口 2 为 Tagged,端口 1 和端口 5-8 为 Untagged。VLAN20 重复上述步骤即可。

VLAN信息
VLAN ID : 10 (1 - 4094)
VLAN 名称: 产品部 (1-16个字符)
Untagged 端口
UNIT : 1 LAGS
2 4 6 8 10 12 14 16 18 20 22 24 26 28 1 3 5 7 9 11 13 15 17 19 21 23 25 27
全选 清空
Tagged 端口
UNIT : 1 LAGS
2 4 6 8 10 12 14 16 18 20 22 24 26 28
1 3 5 7 9 11 13 15 17 19 21 23 25 27
全选 清空 提交 帮助

添加完成后, VLAN 列表如下:

VLAN	配置列表			
选择	VLAN_ID	名称	成员	操作
	1	System-VLAN	1/0/1-28	编辑 详细
	10	产品部	1/0/1-2,1/0/5-8	编辑 详细
	20	研发部	1/0/1-2,1/0/9-12	编辑 详细

交换机二设置是一样的,只是级联口此时只有一个端口1,与交换机一的端口2配置相同。

至此已完成交换机中 802.1Q VLAN 的设置,注意保存配置以免掉电导致配置丢失。

5.2 MAC VLAN 配置指南

5.2.1 应用介绍

MAC VLAN 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 VL AN 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 VL AN 的成员端口即可,而不必改变 VLAN 成员 的配置。

MAC VLAN 能够实现灵活的接入控制,同一终端通过不同端口接入设备时,设备会给终端 分配相同的 VLAN;而不同终端通过同一端口接入设备时,设备可以给不同终端分配不同 的 VLAN。

5.2.2 需求介绍

某公司有两个部门,为了通信安全设置了 VLAN 隔离。由于人员流动较大,公司在会议室 提供了临时的办公场所,即员工可以通过临时办公场所接入公司网络,但要求接入后只能划 分到自己部门所在的 VLAN,拓扑如下:



5.2.3 设置方法

1、在"VLAN 管理"—"802.1QVLAN"—"端口配置",将需求端口均设置为"GENERAL",点 击提交,这里我们示例设置 1-8 口,并修改 1-4 的 PVID 为 10,5-8 的 PVID 为 20,如下 图所示: — 3/5/6/7/8 系列企业级交换机 —

SK的管理 UNIT: LAGS 二层交換 第二 第二
XK管理 二层交换 UNIT: LAGS 选择 演□ PVID LAG 所属VLAN · MAC VLAN · · 查询 · · 802.1Q VLAN · · · · 查询 · · MAC VLAN ·
系統管理 UNIT: 1 LAGS ご层交換 端口 端口类型 PVID LAG 所属VLAN · MAC VLAN ·
二层交换 洗子 端口 端口美型 PVID LAG 所属VLAN ·
VLAN ·
• 802.1Q VLAN □ 1/0/1 GENERAL 10 査询 * • MAC VLAN □ 1/0/2 GENERAL 10 查询 * • が以VLAN □ 1/0/3 GENERAL 10 查询 * • VLAN VPN □ 1/0/3 GENERAL 10 查询 * • VLAN VPN □ 1/0/4 GENERAL 10 查询 * • Private VLAN □ 1/0/5 GENERAL 20 查询 * 4료成树 □ 1/0/7 GENERAL 20 查询 * 1/0/8 GENERAL 20 查询 *
· MAC VLAN □ 1/0/2 GENERAL 10 査询 · 协议VLAN □ 1/0/3 GENERAL 10 查询 · VLAN VPN □ 1/0/4 GENERAL 10 查询 · GVRP □ 1/0/5 GENERAL 20 查询 · Private VLAN □ 1/0/6 GENERAL 20 查询 · MGE 1/0/7 GENERAL 20 查询 · J1/0/8 GENERAL 20 查询 · MABB □ 1/0/7 GENERAL 20 查询 · MBAB □ 1/0/7 GENERAL 20 查询 · MABB □ 1/0/7 GENERAL 20 查询 · MABB □ 1/0/9 ACCESS 1 查询 · MABB □ 1/0/10 ACCESS 1 查询 · MID □ 1/0/12 ACCESS 1 查询
・ 协议VLAN □ 1/0/3 GENERAL 10 査询 ・ VLAN VPN □ 1/0/4 GENERAL 10 查询 • GVRP □ 1/0/5 GENERAL 20 查询 • Private VLAN □ 1/0/6 GENERAL 20 查询 组漏管理 □ 1/0/7 GENERAL 20 查询 路由功能 □ 1/0/8 GENERAL 20 查询 服务质量 □ 1/0/10 ACCESS 1 查询 □ 1/0/10 ACCESS 1 查询 □ 1/0/11 ACCESS 1 查询 □ 1/0/12 ACCESS 1 查询
· VLAN VPN □ 1/0/4 GENERAL 10 査询 · GVRP □ 1/0/5 GENERAL 20 查询 · Private VLAN □ 1/0/6 GENERAL 20 查询 生成树 □ 1/0/7 GENERAL 20 查询 組漏管理 □ 1/0/7 GENERAL 20 查询 路由功能 □ 1/0/9 ACCESS 1 查询 BK务质量 □ 1/0/10 ACCESS 1 查询 □ 1/0/11 ACCESS 1 查询 □ 1/0/12 ACCESS 1 查询
· OVRP 1/0/5 GENERAL 20 查询 · Private VLAN 1/0/6 GENERAL 20 查询 生成树 1/0/7 GENERAL 20 查询 組漏管理 1/0/7 GENERAL 20 查询 路由功能 1/0/7 GENERAL 20 查询 图4365 1 查询 1 查询 POE 1/0/10 ACCESS 1 查询 1/0/11 ACCESS 1 查询
• Private VLAN □ 1/0/6 GENERAL 20 查询 生成树 □ 1/0/7 GENERAL 20 查询 組攝管理 □ 1/0/8 GENERAL 20 查询 路由功能 □ 1/0/9 ACCESS 1 查询 BK务质量 □ 1/0/10 ACCESS 1 查询 □ 1/0/11 ACCESS 1 查询 □ 1/0/12 ACCESS 1 查询
生成树 □ 1/0/7 GENERAL 20 査询 組漏管理 □ 1/0/8 GENERAL 20 查询 踏由功能 □ 1/0/9 ACCESS 1 查询 服务质量 □ 1/0/10 ACCESS 1 查询 POE □ 1/0/11 ACCESS 1 查询 访问控制 □ 1/0/12 ACCESS 1 查询
狙攝管理 路由功能 服务质量 POE 访问控制 1/0/10 ACCESS 1 查询 □ 1/0/10 ACCESS 1 查询 □ 1/0/11 ACCESS 1 查询 □ 1/0/11 ACCESS 1 查询
路田切崩 1/0/9 ACCESS 1 查询 服务质量 1/0/10 ACCESS 1 查询 PoE 1/0/11 ACCESS 1 查询 访问控制 1/0/12 ACCESS 1 查询
服务质量 1/0/10 ACCESS 1 查询 PoE 1/0/11 ACCESS 1 查询 访问控制 1/0/12 ACCESS 1 查询
PoE 1/0/11 ACCESS 1 查询 访问控制 1/0/12 ACCESS 1 查询
· 访问控制 □ 1/0/12 ACCESS 1 查询
Mag E A
<u>网络安王</u> 1/0/13 ACCESS 1 査询
SNMP 1/0/14 ACCESS 1 查询
LLDP 1/0/15 ACCESS 1 查询 ·
退出登录

2、在"VLAN 管理"—"802.1QVLAN"—"VLAN 配置",设置部门所在的 VLAN,将 1-8 口

均设置在 vlan10 和 vlan20 里面,出口规则皆为 untag 如下图所示:

2014 VL		VLAN配置列表 洗择 VLAN ID 名称 成品 操作				
	1	System-VLAN	1/0/1-28	编辑 详细		
	10	vlan10	1/0/1-8	编辑 详细		
	20	vlan20	1/0/1-8	编辑 详细		

3、在"路由设置"—"接口"配置里面给不同的 VLAN 绑定 IP,如下图所示:

	修改注目	
系统管理 	接口D: Vian20	
VLAN 生成树	IP地址模式: ○ Norle ● Static ○ DHCP ○ BOOTP IP地址: 192.168.20.1 格式: 192.168.0.1) 修改	
组播管理 路由功能	子网接码: 255.255.255.0 (音式: 255.255.0) 返回	
 ・接口 ・路由表 	1日 2 (可选、1-16字符)	
•静态路由		

4、在"路由设置"—"DHCP 服务器"里面开启 DHCP 功能,启用即可,并添加地址池,注

意网关和 DNS 也添加,如下图所示:

TL-SG5428PE	DHCP服务器 地址池设置	静态绑定 绑	定表				
	DHCP服务器地址池	-					
系统管理	地址池名称:	bumenA	(长度为1-8)			
二层交换	网络里。	102 169 10 0	(おまざみ・1	, 02.169.0.01			
VLAN	M:45.	192.100.10.0	(16,0,0,0,0)	32.100.0.0)			
生成树	推码:	255.255.255.0	(稽式方:2	55.255.255.	0)		
	起始地址:	192.168.10.2	(格式为: 1	92.168.0.0)			
路田切能 · 培口	结束地址:	192.168.10.254	(格式为: 1	92.168.0.0)			
・ 協由表	租期:	120	(1-2880分)	钟, 默认为12	20分钟)		
静态崩击	默认网关:		(可洗参数,	格式为: 19	2.168.0.1)		提交
 DHCP服务器 			(司法会数	格式 10	2 169 0 1)		取消
・DHCP中继	DING/00/95 Birt		(1)20000,	1000/01:10	2.108.0.1)		
・代理ARP	Netbios服务器:		(可选参数,	格式为: 19	2.168.0.1)		
• ARP	Netbios节点类型:		✓ (可选参数,	可选项: b/	p/m/h/空)		
· KIF 服务质量	下一服务器地址:		(可选参数,	格式为: 19	2.168.0.1)		
PoE	客户端域名:		(可选参数,	长度0-255)			
	启动文件名:		(可洗参数,	长度0-128)			
	in the second se		(1)200	10000 1207			
SNMP	地址池列表						
LLDP	洗坯 夕穀	网络早	培和	細胞	把始地址	结审地业	<u> 提作</u>
系统维护	bumenA	192.168.10.0	255.255.255.0	120	192.168.10.2	192.168.10.254	编辑 查看
配置保存	bumenB	192.168.20.0	255.255.255.0	120	192.168.20.2	192.168.20.254	编辑 查看
索引页面			全选	删除	帮助		
退出登录							
	注意: 当DHCP服务器功能启用时	,此处配置才生效。					

5、在"VLAN"—"MAC VLAN"里面,设置 MAC VLAN,如下图所示:

TL-SG5428PE	MAC VLAN 端口使能			
	MAC VLAN配置			
系统管理	MAC地址: 8c-8	9-a5-65-b8-9a (<mark>格式为:00</mark>	0-00-00-00-00-01)	
二层交换 VLAN	MAC描述:	(1-8个字符)		修改
• 802.1Q VLAN	VLAN ID: 10	(1-4094)		有工
MAC VLAN				
• 协议VLAN	MAC VLAN列表			
VLAN VPN	选择 MAC地址	MAC描述	VLAN ID	操作
• GVRP	8c-89-a5-65-b8-9a	N/A	10	编辑
• Private VLAN 生成树		全选 删除 帮	助	
组播管理	当前MAC \/I AN首数,1			
路由功能				
服务质量				
PoF				

6、设置端口使能,我们这里设置了1-8口,所以开启1-8口的端口使能,如下图所示:

TL-SG5428PE	MAC VLAN 端口使能
	端口使能
系统管理	UNIT: 1 LAGS
二层交换	2 4 6 8 10 12 14 16 18 20 22 24 26 28
• 802 10 VLAN	1 3 5 7 9 11 13 15 17 19 21 23 25 27
MAC VLAN	全洗
・协议VLAN	
VLAN VPN	
• GVRP	
Private VLAN	
生成树	

以上, MAC VLAN 配置完成! 该终端接入任意的 1-8 口都属于 VLAN10。

5.2.4 配置注意事项

輸入该 MAC VLAN 对应的 VLAN ID 时,此 VLAN 必须是输入端口所在的 802.1Q
 VLAN。

5.3 语音 VLAN 典型配置指导

5.3.1 应用介绍

具有语音 VLAN 功能的设备将通过 OUI 地址来匹配进入端口的报文中的源 MAC 地址字 段,源 MAC 地址符合系统设置(预先在交换机上面配置了这个 OUI 地址表)的语音设备 OUI 地址(提供语音 IP 电话的厂商的 OUI 标识是唯一的,可以事先查询到)的报文被认为 是语音数据流,被划分到语音 VLAN 中传输,并自动下发优先级规则,提高语音流的优先级,保证通话质量。

5.3.2 需求介绍

某公司需要实现语音电话和网络混合组网的需求,且语音电话需要专门在一个 VLAN 中传输。需求如下:

需求 1:

(1) 配置 VLAN 2 为语音 VLAN,只允许语音报文通过。

(2) IP Phone 类型为 Untagged, 接入端口是 General 类型端口 1。

(3) 电脑和 IP 电话串联接入交换机,端口 1 工作在自动模式,如果它们在 30 分钟内没有 收到语音流,就将相应的语音 VLAN 老化。

(4) 端口 1 允许 OUI 地址是 0011-2233-0000、掩码是 ffff-ffff-0000 的语音报文通过, 描述字符为 test。



需求 2:

- (1) 配置 VLAN 2 为语音 VLAN,只允许语音报文通过。
- (2) IP Phone 类型为 Untagged, 接入端口是 General 类型端口 1。
- (3) 端口1只接入了语音电话,工作在手动模式。
- (4) 端口 1 允许 OUI 地址是 0011-2233-0000、掩码是 ffff-ffff-0000 的语音报文通过, 描述字符为 test。



5.3.3 设置方法

针对需求 1—使用自动模式

第一步、配置接语音电话的口为 general 口, 并创建 VLAN 2

1、"VLAN"-"802.1Q VLAN"-"端口配置",设置接语音电话的口为 general 口, PVID 保 持之前的业务设置不改变 (不影响端口 1 的其他业务数据):

TL-SG5210PE	VLAN配置	端口配置			
	操作成功。				
	VLAN端口]配置			
系统管理	UNIT:	1 LAGS			
二层交换	选择	端口 端口类型	PVID	LAG	所属VLAN
VLAN			✓		
• 802.1Q VLAN		I/0/1 GENERA	L 1		查询
 MAC VLAN 	0 1	I/0/2 ACCESS	1		查询
•协议VLAN	0 1	I/0/3 ACCESS	1		查询
VLAN VPN	0 1	I/0/4 ACCESS	1		查询
• GVRP	0 1	I/0/5 ACCESS	1		查询
Private VLAN	0 1	I/0/6 ACCESS	1		查询
生成树	0 1	I/0/7 ACCESS	1		查询
	0 1	I/0/8 ACCESS	1		查询
路田切能	1	I/0/9 ACCESS	1		查询
	1/	/0/10 ACCESS	1		查询
POE		C	△洪 坦六	期由	
访问控制 		L	土地 征义	נאו מד	
网络安全					

2、新建 VLAN 2 为语音 VLAN,可以不包含端口(自动模式下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):

VLAN配置端口配置	
VLAN信息	
VLAN ID:	2 (2 - 4094)
VLAN 名称:	语音VLAN (1-16个字符)
Untagged 端口	
UNIT: 1 LA	GS
1 2 3 4	5 6 7 8 9 10
	全选 清空
Tagged 端口	
UNIT: 1 LA	GS
1 2 3 4	5 6 7 8 9 10
	全选 清空 提交 帮助
	🖳 未选中的端口 🛛 💼 选中的端口 💭 不可选端口

第二步、配置全局语音 VLAN 功能。

在"服务质量"-"语音 VLAN", 全局配置中启用全局语音 VLAN 功能, 配置语音 VLAN 为 VLAN 2, 老化时间为 30min:

全	局配	置端口配置	OUI配置		
-	소	局配要			
	-	语音VLAN:	● 启用 ○ 禁用	_	
		VLAN ID:	2	(2 - 4094)	桿森
		老化时间:	30] 分钟(1-43200,默认1440)	帮助
		语音优先级:	6 🗸	_	



语音优先级分为 0~7 共 8 档, 默认优先级为 6, 且数字越大, 优先级越高。

第三步、配置端口 1 的语音 VLAN 功能。

全	局配置	端口配置	OUI配置			
	端口配	置				
	UNIT	: 1 LA	IGS		_	
	选择	端口	成员模式	安全模式	成员状态	LAG
			自动 🗸	禁用▼		
		1/0/1	自动	禁用	退出	
	U	1/0/2	自动	禁用	退出	
		1/0/3	自动	禁用	退出	
		1/0/4	自动	禁用	退出	
		1/0/5	自动	禁用	退出	
		1/0/6	自动	禁用	退出	
		1/0/7	自动	禁用	退出	
		1/0/8	自动	禁用	退出	
		1/0/9	自动	禁用	退出	
		1/0/10	自动	禁用	退出	
			全道	き 提交 帮	助	

配置端口1的语音 VLAN 功能,设置端口1为自动模式,安全模式禁用。

说明:

 安全模式代表设置端口转发数据包的模式,其中禁用代表端口转发所有数据包,启用代表端口只 转发语音数据包。

第四步、配置语音 VLAN 能识别的 OUI 地址。

系统已经预设了一些常见厂商的 OUI 地址,如果没有自己厂商的则可以通过掩码与运算将 设备的地址添加进去。

全局配置	端口配置 OU	配置				
新建条	:目					
OL	川地址:	00-11-2	2-33-00-00	(格式为:	: 00-00-00-00-00-01)	
οι	川掩码:	FF-FF-			添加	
0	旧構成・	foet		(1.16个)	* (立)	
00	/1) 两方1	liest		(1-10]-	-10 <i>)</i>	
OUI列	表		添加OUI地址			
选择	OUI地址		OUI掩码		OUI描述	
	00-01-e3-00-0	00-00	ff-ff-ff-00-00-00)	Siemens Pho	ne
	00-03-6b-00-0	00-00	ff-ff-ff-00-00-00)	Cisco Phon	e
	00-04-0d-00-0	00-00	ff-ff-ff-00-00-00)	Avaya Phon	е
	00-60-b9-00-0	00-00	ff-ff-ff-00-00-00)	Philips Phor	ie
	00-d0-1e-00-0	00-00	ff-ff-ff-00-00-00)	Pingtel Phor	ie
	00-e0-75-00-0	00-00	ff-ff-ff-00-00-00)	PolyCom Pho	one
	00-e0-bb-00-0	00-00	ff-ff-ff-00-00-00)	3Com Phon	e
			è选	帮助		

至此,自动模式下的语音 VLAN 配置成功,1 口下符合 OUI 配置的语音设备接入后交换机 自动将语音电话数据在 VLAN 2 中传输。

针对需求 2—使用手动模式

第一步、配置接语音电话的口为 general 口,并创建 VLAN 2

1、"VLAN"-"802.1Q VLAN"-"端口配置",设置接语音电话的口为 general 口, PVID 设置为 2:

VL	AN配置	端口西	記畫			
	操作成	功。				
	VLAN就	問配置				
	UNIT:	: 1 l	LAGS			
	选择	端口	端口类型	PVID	LAG	所属VLAN
			~			
		1/0/1	GENERAL	2		查询
		1/0/2	ACCESS	1		查询
		1/0/3	ACCESS	1		查询
		1/0/4	ACCESS	1		查询
		1/0/5	ACCESS	1		查询
		1/0/6	ACCESS	1		查询
		1/0/7	ACCESS	1		查询
		1/0/8	ACCESS	1		查询
		1/0/9	ACCESS	1		查询
		1/0/10	ACCESS	1		查询
			全选	提交	帮助	

2、新建 VLAN 2 为语音 VLAN,包含端口 1,出口规则为 untag:

VLAN		
_		
V	/LAN信息	
	VLAN ID:	2 (1 - 4094)
	VLAN 名称:	语音VLAN (1-16个字符)
	Untagged 端口	
	UNIT: 1 LAGS	
	12345	6 7 8 9 10
		全选 清空
	Tagged 端囗	
	UNIT: 1 LAGS	
	1 2 3 4 5	6 7 8 9 10
		全选 清空 提交 帮助
	Ľ	🗋 未选中的端口 👘 选中的端口 👘 不可选端口
_		

第二步、配置全局语音 VLAN 功能。

在"服务质量"-"语音 VLAN", 全局配置中启用全局语音 VLAN 功能, 配置语音 VLAN 为

VLAN 2,老化时间为可以保持默认:

全局配	置 端口配置	OUI配置		
全	局配置			
	语音VLAN:	◉启用 ○禁用	_	
	VLAN ID:	2	(2 - 4094)	坦六
	老化时间:	30] 分钟(1-43200,默认1440)	<u>徒父</u> 帮助
	语音优先级:	6 🗸	_	
(P	说明:			

语音优先级分为 0~7 共 8 档, 默认优先级为 6, 且数字越大, 优先级越高。

第三步、配置端口 1 语音 VLAN 功能。

配置端口1的语音 VLAN 功能,设置端口1为手动模式,安全模式根据自己需求选择:

端口配	 王 王 王 王 王				
UNIT	: 1 LA	GS			
选择	端口	成员模式	安全模式	成员状态	LAG
		~	~		
	1/0/1	手动	禁用	加入	
	1/0/2	自动	禁用	退出	
	1/0/3	自动	禁用	退出	
	1/0/4	自动	禁用	退出	
	1/0/5	自动	禁用	退出	
	1/0/6	自动	禁用	退出	
	1/0/7	自动	禁用	退出	
	1/0/8	自动	禁用	退出	
	1/0/9	自动	禁用	退出	
	1/0/10	自动	禁用	退出	
		全道	提交	帮助	

吮먯.

 安全模式代表设置端口转发数据包的模式,其中禁用代表端口转发所有数据包,启用代表端口只 转发语音数据包。

第四步、配置语音 VLAN 的 OUI 地址。

系统已经预设了一些常见厂商的 OUI 地址,如果没有自己厂商的则可以通过掩码与运算将

设备地址添加进去。

新建条目			
OUI地	助止: 00-1	-22-33-00-00	(格式为: 00-00-00-00-01)
OUI掩码: FF		F-FF-FF-00-00 🗸	(默认为:FF-FF-FF-00-00-00) 添加
OUI描	述: test		(1-16个字符)
OUI列表		添加OUI地址	
选择	OUI地址	OUI掩码	OUI描述
	00-01-e3-00-00-00	ff-ff-ff-00-00-00	0 Siemens Phone
	00-03-6b-00-00-00	ff-ff-ff-00-00-00	0 Cisco Phone
	00-04-0d-00-00-00	ff-ff-ff-00-00-00	0 Avaya Phone
	00-60-b9-00-00-00	ff-ff-ff-00-00-00	0 Philips Phone
	00-d0-1e-00-00-00	ff-ff-ff-00-00-00	0 Pingtel Phone
	00-e0-75-00-00-00	ff-ff-ff-00-00-00	0 PolyCom Phone
	00-e0-bb-00-00-00	ff-ff-ff-00-00-00	0 3Com Phone
	ſ		±₽BH

至此,手动模式下的语音 VLAN 配置成功,手动将1口加入在语音 VLAN 2中。

5.3.4 配置注意事项

- IP 电话的工作原理:与其他网络设备一样, IP 电话也需要 IP 地址才能在网络中正常通信。IP 电话获取 IP 地址的方式有两种:通过 DHCP 自动获取和通过用户手工配置,可以参考 IP 电话的使用说明书。
- 一般情况下: IP 电话在自动获取 IP 地址时, IP 电话还可以向 DHCP 服务器同时请求
 Voice VLAN 信息,如果 DHCP 服务器返回了 Voice VLAN 信息, IP 电话就可以直接

发送携带有 Voice VLAN Tag 的语音流 (简称 tagged 语音流);如果 DHCP 服务器没 有返回 Voice VLAN 信息, IP 电话就只能发送不带 VLAN Tag 的语音流(简称 untagged 语音流)。同样,在用户在 IP 电话上手工设置 IP 地址时,也可以设置或不设置 Voice VLAN 信息, IP 电话会根据用户的配置发出 tagged/untagged 语音流。

- 语音 VLAN 中的端口可工作在语音 VLAN 的自动模式或手动模式,在不同的工作模式 下端口加入语音 VLAN 的方式不同。
- 自动模式:当用户 IP 电话启动时,所发出的报文经支持语音 VLAN 的设备时,设备通过识别该报文的源 MAC 地址,匹配设备上所配置的 OUI 地址,OUI 地址匹配成功后,设备自动将该语音报文的输入端口添加到语音 VLAN,并下发策略,将语音报文的优先级修改为设备上所配置的语音 VLAN 中语音流的优先级,并使用老化机制对语音 VLAN 内的端口进行维护。在老化时间内,系统没有从输入端口收到任何语音报文时,系统将把该端口从语音 VLAN 中删除。
- 手动模式:手动模式下,端口加入语音 VLAN 或从语音 VLAN 中删除的过程由管理员 手动进行配置。用户 IP 电话通讯过程中,设备通过识别报文的源 MAC 地址,匹配设 备上所配置的 OUI 地址,OUI 地址匹配成功后,下发策略,将语音报文的优先级修改 为设备上所配置的语音 VLAN 中语音流的优先级。
- 自动模式适用于 PC--IP 电话串联接入端口,可以同时传输语音数据和普通业务数据的 组网方式。
- 手工模式适用于 IP 电话单独接入交换机,端口仅传输语音报文的组网方式,这种组网的方式可以使该端口专用于传输语音数据,避免业务数据对语音数据传输的影响。

第6章 生成树

6.1 交换机生成树功能配置指南

6.1.1 应用介绍

生成树 STP(Spanning Tree Protocal)主要用于在局域网中消除链路层物理环路,并在 链路故障时自动激活备份链路恢复网络。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。



(1) 通过阻断冗余链路消除网络中存在的路径回环;

(2) 当前路径发生故障时,激活冗余备份链路,恢复网络连通性。

生成树协议分为三种,普通生成树 STP(Spanning Tree Protocal)、快速生成树 RSTP (Rapid Spanning Tree Protocal)以及多生成树 MSTP(Multiple Spanning Tree Protocal),可以根据需要选用,满足多种使用环境需求。下面介绍 TP-LINK 交换机生成 树功能的设置方法。 STP 和 RSTP 功能的设置方法是相同的。RSTP 相比于 STP 来说收敛速度更快,且兼容 STP 协议,所以一般推荐使用 RSTP 协议。

6.1.2 需求介绍

1、客户公司内部网络,5台TP-LINK管理型交换机搭建STP或者RSTP环形网络,实现链路故障备份的功能。5台交换机环形连接,所有交换机之间的连接用端口为1、2号端口。如下图所示:



2、客户公司内部网络,如下图所示拓扑结构,整个网络中设置了6个VLAN 101-106, 需要实现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。采用MSTP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。



6.1.3 设置方法

STP/RSTP 设置方法

1、修改交换机的 IP 地址不冲突: TP-LINK 的交换机默认管理 IP 地址均是 192.168.0.1,

为了防止地址冲突,首先建议修改为不冲突的 IP 地址。以 TL-SG5428 为例,打开"路由功能"—"接口"页面,点击"编辑"修改。

TL-SG5428	接口设置	
	创建接口	
系统管理 二层交换	接口ID: VLAN (1-4094)	
VLAN 生成树	IP地址模式: ⑧ None 〇 Static 〇 DHCP 〇 BOOTP	
组播管理	IP地址: (格式: 192.168.0.1)	创建
路由功能	子网掩码: (格式: 255.255.255.0)	
・接口	管理状态: 开启 🖌	
• 路田表		
• 静态路由	12日日4月~ (1955-1-10-71年)	
 DHCP服务器 		
・DHCP中继	接口列表	
 代理ARP 	选择 接口ID 模式 IP地址 子网掩码 接口名称 状态	操作
• ARP	□ Vlan1 Static 192.168.0.1 255.255.255.0 Up 編編 編	辑IPv6 详细
• RIP 服务质量	全选 删除 帮助	

2、交换机开启 STP 或者 RSTP 全局配置开关:打开菜单"生成树"—"基本配置"页面,生成

TL-SG5428	基本配置 生成树信息		
系统管理 二层交换	全局配置 生成树功能 :	● 启用 ○ 禁用	提交
VLAN 生成树 ・基本配置	生成树模式 : 参数配置	STP V STP RSTP MSTP	
 ・ 端山配置 ・ MSTP实例 ・ 安全配置 	CIST优先级 : 联络时间 :		
	老化时间 :	20 秒 (6-40)	提交
	传输时处 : 流量限制 :	15 秒 (4-30) 5 pps (1-20)	帮助
SNMP LLDP	最大跳数 :	20	

树功能选择"启用",生成树模式选择"STP 或者 RSTP",点击"提交"。

3、交换机级联端口启用生成树功能:打开菜单"生成树"—"端口配置"页面,选择交换机级联的端口(本例中是端口1和2),状态选择"启用",点击"提交"。

端口配置	Ē												
端口	<u>第口配置</u>												
U	NIT : 🗌	LAGS											
选择	ない ひょうし ひょうしん ひょうしん ほうしん しょうしん しょうしょう いまい ひょうしん しょうしん しょうしょう いまい しょうしょう いまい しょうしょう いまい しょうしょう いまい しょう いまい しょうしょう いまい しょうしょう しょうしょう いまい しょう いまい しょう いまい しょう いまい しょう いまい いまい いまい しょう いょう いまい しょう いまい しょう いまい しょう いまい いまい しょう いまい しょう いまい いまい しょう いまい しょう い い いょう い いょう い い い い いょう い い い い い い	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	端口工作模式	端口角色	端口状态	LAG	
)	启用 ✔				~	~	~					
	1/0/1	林田	128	自动	自动	禁用	自动					4	
	1/0/2	一定用	128	自动	自动	禁用	自动						
	1/0/3	泉川	128	自动	自动	禁用	自动						
	1/0/4	禁用	128	自动	自动	禁用	自动						
C	1/0/5	禁用	128	自动	自动	禁用	自动						
	1/0/6	禁用	128	自动	自动	禁用	自动						
	1/0/7	禁用	128	自动	自动	禁用	自动						
	1/0/8	禁用	128	自动	自动	禁用	自动						
	1/0/9	禁用	128	自动	自动	禁用	自动						
	1/0/10	禁用	128	自动	自动	禁用	自动						
	1/0/11	禁用	128	自动	自动	禁用	自动						
	1/0/12	禁用	128	目动	目动	禁用	目动						
	1/0/13	祭用 ##四	128	日初	目初	第用 ##用	目初						
	1/0/14	第用 禁用	128	日初	日初	二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	日初						
	1/0/15	漂用	120	日初	브페	奈用							
					全选	提交	刷新 帮	助					

一台交换机设置完成,相同的方法,依次设置其他的交换机。完成 STP/RSTP 功能的设置之后,进行线路连接即可。

MSTP 设置方法

本例中假定 IP、VLAN 等相关的设置已经完成,仅关注生成树的设置。

1、所有交换机开启 MSTP 全局配置开关:打开菜单"生成树"—"基本配置"页面,生成树功 能选择"启用",生成树模式选择"MSTP",点击"提交"。

TL-SG5428	基本配置生成树信息		
	全局配置		
系统管理			
二层交换	生成树功能:	● 启用 ○ 禁用	提交
VLAN	生成树模式 :	STP 🗸	
生成树		STP	
・基本配置	参数配置	MSTP	
• 端口配置	0107倍件/(3)。		
 MSTP实例 	CISH/LFt 2	32768 (0-61440,4096方间隔)	
• 安全配置	联络时间 :	2 秒(1-10)	
组播管理	来 少时间,	20 ÷h (c 40)	
路由功能	-ESTORULATION -	20	提交
服务质量	传输时延 :	15 秒 (4-30)	帮助
访问控制	流量限制 :	5 pps (1-20)	
网络安全	100000 (C.193		
SNMP	最大跳数 :	20 跳(1-40)	
LLDP			

2、所有交换机级联端口启用生成树功能:打开菜单"生成树"—"端口配置"页面,选择交换机 之间级联的端口编号。状态选择"启用",点击"提交"。

端口	配置													
ŷ	满口配 <u>置</u>													
	UNIT: 1 LAGS													
6	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	端口工作模式	端口角色	端口状态	LAG	6
- 1			启用 ✔				~	~	~					
- 1	 Image: A second s	1/0/1		128	自动	自动	禁用	自动						-
- 1	✓	1/0/2	祭用	128	自动	自动	禁用	自动						
_ F	0	1/0/3	汞用	128	自动	自动	禁用	自动						
		1/0/4	禁用	128	自动	自动	禁用	自动						
		1/0/5	禁用	128	自动	自动	禁用	自动						
		1/0/6	禁用	128	自动	自动	禁用	自动						
		1/0/7	禁用	128	自动	自动	禁用	自动						
		1/0/8	禁用	128	自动	自动	禁用	自动						
		1/0/9	禁用	128	自动	自动	禁用	自动						
		1/0/10	禁用	128	自动	自动	禁用	自动						
		1/0/11	禁用	128	自动	自动	禁用	自动						
		1/0/12	禁用	128	自动	自动	禁用	自动						
		1/0/13	禁用	128	自动	自动	禁用	自动						
		1/0/14	禁用	128	自动	自动	禁用	自动						
		1/0/15	禁用	128	自动	自动	禁用	自动						-
						全选	提交	刷新 帮助						

3、所有交换机配置相同的 MST 域的域名(任意域名)和修订级别(默认即可):打开菜单 "生成树"—"MSTP 实例"—"域配置"页面,所有交换机设置相同的域名(本例中为"TEST") 和修订级别(本例中为默认的"0"),点击"提交"。

TL-SG5428	域配置 实例配置 实例端口
	域配置
系统管理	協欠 · TEST
<u>一层交换</u> VLAN	修订级别: 0 (0.65535) 提交
生成树	#助
・基本配置	
・端口配置	
 MSTP实例 	
• 安全配置	

4、所有交换机配置 MST 域的 VLAN-实例映射,将 VLAN 101、103、105 映射到实例 1, 将 VLAN 102、104、106 映射到实例 2:打开菜单"生成树"—"MSTP 实例"—"实例配置"页 面,实例 ID 设置"1",VLAN ID 设置"101,103,105",点击"添加",将 VLAN 101、103、 105 映射到实例 1。相同设置方法将 VLAN 102、104、106 映射到实例 2。所有交换机相 同的设置。 - 3/5/6/7/8 系列企业级交换机 -

TL-SG5428	域配置	实例配置	实例端口			
	VLAN	-实例映射				
系统管理 二层交换	实	例ID:	1		(0-8,0代表CIST)	添加
VLAN	V	LAN ID :	101,10	03,105	(1-4094,格式:1,	3,4-7,11-30) 删除
生成树						
・基本配置	实例商	置				
・端口配置	选择	实例ID	状态	优先级	VLAN ID	
・MSTP实例						
 安全配置 		CIST	启用	32768	1-4094,	显示全部映射 清除全部映射
组播管理		1	禁用	32768		显示全部映射 清除全部映射
路由功能		2	禁用	32768		显示全部映射 清除全部映射
服务质量		3	禁用	32768		显示全部映射 清除全部映射
访问控制		4	禁用	32768		显示全部映射 清除全部映射
网络安全		5	禁用	32768		显示全部映射 清除全部映射
SNMP		6	禁用	32768		显示全部映射 清除全部映射
LLDP		7	禁用	32768		显示全部映射 清除全部映射
系统维护		8	禁用	32768		显示全部映射 清除全部映射
配置保存 					提交帮助	

5、添加完毕如下图所示。

实例配	置				
选择	实例ID	状态	优先级	VLAN ID	
	CIST	启用	32768	1-100,107-4094,	显示全部映射 清除全部映射
	1	启用	32768	101,103,105,	显示全部映射 清除全部映射
	2	启用	32768	102,104,106,	显示全部映射 清除全部映射
	3	禁用	32768		显示全部映射 清除全部映射
	4	禁用	32768		显示全部映射 清除全部映射
	5	禁用	32768		显示全部映射 清除全部映射
	6	禁用	32768		显示全部映射 清除全部映射
	7	禁用	32768		显示全部映射 清除全部映射
	8	禁用	32768		显示全部映射 清除全部映射
				提交帮助	

6、将交换机 B 配置为实例 1 的根桥, 且是实例 2 的指定桥: 打开交换机 B 的配置页面, 打 开菜单"生成树"—"MSTP 实例"—"实例配置"页面,选择实例"1",并将优先级设置为"0", 点 击"提交"。

TL-SG5428	域配置实例配置	实例端口		
	VLAN-实例映射			
系统管理 二层交换 VI AN	实例ID : VI AN ID :		(0-8,0代表CIST) (1-4094、格式:13	添加
生成树 • 基本配置	实例配置			
• 端口配置	选择 实例ID	状态优先级	VLAN ID	
 MSTP契例 ・安全配置 	CIST	月 32768	1-100,107-4094,	显示全部映射 清除全部映射
组播管理 路由功能	✓ 12	启用 32768 启用 32768	101,103,105, 102,104,106,	显示全部映射 清除全部映射 显示全部映射 清除全部映射
	3	禁用 32768		显示全部映射 清除全部映射
	5	禁用 32768 禁用 32768		显示全部映射 清除全部映射 显示全部映射 清除全部映射
SNMP LLDP	6	禁用 32768 禁用 32768		显示全部映射 清除全部映射 显示全部映射 清除全部映射
系统维护	8	禁用 32768		显示全部映射 清除全部映射
<u>一回旦休行</u> 			提交帮助	

7、然后选择实例"2",并将优先级设置为"4096",点击"提交"。设置完毕如下图所示。

实例配置									
选择	实例ID	状态	优先级	VLAN ID					
	CIST	启用	32768	1-100,107-4094,	显示全部映射 清除全部映射				
	1	启用	0	101,103,105,	显示全部映射 清除全部映射				
	2	启用	4096	102,104,106,	显示全部映射 清除全部映射				
	3	禁用	32768		显示全部映射 清除全部映射				
	4	禁用	32768		显示全部映射 清除全部映射				
	5	禁用	32768		显示全部映射 清除全部映射				
	6	禁用	32768		显示全部映射 清除全部映射				
	7	禁用	32768		显示全部映射 清除全部映射				
	8	禁用	32768		显示全部映射 清除全部映射				
				提交帮助					

8、将交换机 C 配置为实例 2 的根桥, 且是实例 1 的指定桥: 打开交换机 C 的配置页面, 打 开菜单"生成树"—"MSTP 实例"—"实例配置"页面,选择实例"1",并将优先级设置为"4096", 点击"提交"。然后选择实例"2",并将优先级设置为"0", 点击"提交"。设置完毕如下图所示。

实例配置								
选择	实例ID	状态	优先级	VLAN ID				
	CIST	启用	32768	1-100,107-4094,	显示全部映射 清除全部映射			
	1	启用	4096	101,103,105,	显示全部映射 清除全部映射			
	2	启用	0	102,104,106,	显示全部映射 清除全部映射			
	3	禁用	32768		显示全部映射 清除全部映射			
	4	禁用	32768		显示全部映射 清除全部映射			
	5	禁用	32768		显示全部映射 清除全部映射			
	6	禁用	32768		显示全部映射 清除全部映射			
	7	禁用	32768		显示全部映射 清除全部映射			
	8	禁用	32768		显示全部映射 清除全部映射			
				提交帮助				

9、MSTP 的所有设置完成,实现的效果:实例1 (VLAN101、103、105),连通的链路如 左边红色所示,实例2 (VLAN102、104、106),连通的链路如右边蓝色所示。



至此, 生成树功能的基本设置方法就介绍完了。

6.1.4 配置注意事项

设置时每台交换机单独连接设置,每次设置一台交换机。设置完成后再进行线路连接。
 部和分部路由器都处于联网状态,且至少有一端出口是公网 IP 地址

第7章 组播管理

7.1 交换机多网段 IGMP 侦听配置指南

7.1.1 应用介绍

在很多网络环境中需要用到组播来传递数据,由于交换机默认转发本 VLAN 中的组播报文, 所以不加以限制的话,会造成交换机被占用过多资源、端口几乎全部用来转发组播数据,带 宽浪费严重。为了合理的转发组播数据,节省资源,提高终端的上网体验,可以通过设置 IGMP 侦听并选择丢弃未知组播报文来解决。设置之后该端口只有加入到这个组播组中,才 会收到组播数据,不加入的话该组播组的组播报文被该端口认定为未知组播报文,并进行丢 弃,这样这个端口是不会收到组播数据的。这样设置能有效节约带宽和交换机的性能,同时 也方便对组播成员进行管理,合理的设置组播业务。

7.1.2 需求介绍

某企业通过三层交换机划分了 3 个业务 VLAN,分别是 VLAN 10.20.30,这三个业务部门都 需要收到来自公司组播服务器的组播业务数据,但是为了节约交换机资源需要设置 IGMP 侦 听来控制哪些需要端口需要转发这份数据,网络拓扑如下:


7.1.3 设置方法

第一步、划分业务 VLAN 10.20.30,组播数据使用的 VLAN 40。

划分 VLAN 时需要将需要组播业务的端口设置为 general 口,便于之后的 VLAN 设置,同 时保证该端口既可以运行普通业务也可以转发组播数据。

在"VLAN-802.1Q VLAN-VLAN 配置"界面,划分对应端口到对应业务 VLAN 下,本拓扑 下出口规则为 untag:

TI-SH6428	VLAN配置 端口配置			
	VLAN配置列表			
系统管理	选择 VLAN ID	名称	成员	操作
堆叠功能	1	System-VLAN	1/0/1-28	编辑 详细
二层交换	10	业务1	1/0/1-4	编辑 详细
VLAN	20	业务2	1/0/5-8	编辑 详细
• 802.1Q VLAN	30	业务3	1/0/9-12	编辑 详细
 MAC VLAN 		会法	新建 删除 帮助	
•协议VLAN		土地	291 XE 002 POA TO PUJ	

其余的接口, DHCP, 以及静态路由配置可以参考:【配置实例】三层交换机企业应用配置实例。

第二步、新建组播服务器和需要用到组播数据端口所在的 VLAN 。

新建一个 VLAN40 用于在该 VLAN 传输组播数据,保证组播数据只会在该 VLAN 中转发, 不会影响的其他的 VLAN 和端口,节约交换机的资源,提高带宽利用率。

在"VLAN-802.1Q VLAN-VLAN 配置"界面,将需要用到组播业务的端口添加到该 VLAN中,端口带不带 tag 视具体网络环境而定,成员端口的类型不会影响到正常的组播转发,本次设置选择 untagged 接口,新建组播 VLAN 40 包含 1-13 端口,且皆为 untag,13 端口接组播服务器,PVID 设置为 40 :

TL-SH6428	VLAN配置 端口配置
	VLAN信息
系统管理	VLAN ID: 40 (2 - 4094)
堆叠功能	
二层交换	VLAN 名称:
VLAN	Untagged 端口
• 802.1Q VLAN	UNIT: 1 LAGS
MAC VLAN	
• 顶设 V LAN	
• GVRP	
Private VLAN	全选 清空
生成树	Taggod 详目
组播管理	
路由功能	
服务质量	2 4 6 8 10 12 14 16 18 20 22 24
访问控制	1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28
网络安全	全洗
SNMP	
LLDP	
系统维护	

第三步、设置端口的 PVID

对于组播 VLAN 所在的端口,组播源端口 (本例是 13 号端口)即发送组播数据的端口,其 PVID 要设置成组播 VLAN 的 ID (本例是 VLAN40),保证组播数据进来的时候是在组播 VLAN 中的; 而其他成员端口 1-12 端口, 即需要接收组播数据的端口, PVID 仍为之前所 在 VLAN 的 ID, 也就是说这些端口原有的配置和业务不会受到影响。在"VLAN-802.1Q VLAN-端口配置界面",配置 1-13 口为 general 口,并设置对应端口的的 PVID 为对应的 VLAN ID, 如下:

TL-SH6428	VLAN配置端口配	<u> </u>			
	VLAN端口配置				
系统管理	UNIT: 1 LA	\GS			
堆叠功能	选择 端口	端口类型	PVID	LAG	所属VLAN
二层交换		~			
VLAN	1/0/1	GENERAL	10		查询
• 802.1Q VLAN	1/0/2	GENERAL	10		
 MAC VLAN 	1/0/3	GENERAL	10		
•协议VLAN	1/0/4	GENERAL	10		查询
 VLAN VPN 	1/0/5	GENERAL	20		查询
• GVRP	1/0/6	GENERAL	20		查询
Private VLAN	1/0/7	GENERAL	20		
生成树	1/0/8	GENERAL	20		查询
	1/0/9	GENERAL	30		
	1/0/10	GENERAL	30		
	1/0/11	GENERAL	30		查询
	1/0/12	GENERAL	30		
网络安全	1/0/13	GENERAL	40		查询
SNMP	1/0/14	ACCESS	1		查询
LLDP	1/0/15	ACCESS	1		查询
系统维护		A.)#		±504	
配置保存		至远	(建文	邗即	

第四步、开启 IGMP 侦听

在组播管理中, 启用全局 IGMP 侦听, 在 IGMP 全局配置中, 选择丢弃未知组播报文, 其

余选项默认。

TL-SH6428	基本配置 端口配置 VLAN	配置 组播VLAN 查	词器配置 Profile配置	Profile绑定 报文统计
系统管理	全局配置 IGMP侦听:	● 启用 ○ 禁用	1	
	未知组播报文:	 ○ 抗抗 ○ 素抗 ○ 转发 ● 丢弃 		
生成树 组播管理	Report报文抑制: 路由器端口时间:	○ 启用 ● 禁用 300	秒 (60-600, 推荐300利	没
 IGMP侦听 MLD侦听 	成员端口时间: 最后监听成员查询问隔·	260	● 秒 (60-600, 推荐260秒 ● 秒 (1-5)	▷)
• 组播地址表路由功能	最后监听成员查询次数:	2	(1-5)	
服务质量 访问控制	IGMP侦听信息 描述		成品	
网络安全 SNMP			1470544	
LLDP 系统维护		刷新	帮助	

注: IGMP 侦听和 MLD 侦听需要同时启用。

第五步、设置 IGMP 侦听的端口和组播 VLAN

在"组播管理-IGMP 侦听-端口配置"中, 需要用到组播功能的端口 1-12 口启用 IGMP 侦听,

同时启用快速离开功能(在有多个组播组的环境下使用),之后点击提交。

TL-SH6428	基本配置	端口配置	VLAN配置	组播VLAN	查询器配置	Profile配置	Profile绑定	报文统计
	操作成功	功。						
	端口配證	野田						
系统管理	UNIT:	1 LAG	s					
堆叠功能	选择	端口号	IGMP	侦听	快速离开功) 危	LAG	
二层交换				~	~	1		
VLAN		1/0/1	启月	Ð	启用			<u>^</u>
生成树		1/0/2	启月	Ħ	启用			
组播管理		1/0/3	启月	Ð	启用			
• IGMP侦听		1/0/4	启月	ŧ	启用			
• MLD 仮听		1/0/5	启月	Ħ	启用			
		1/0/6	启月	Ħ	启用			
		1/0/7	启月	Ð	启用			
加方应里 		1/0/8	启月	Ħ	启用			
		1/0/9	启月	Ð	启用			
		1/0/10	启月	Ð	启用			
		1/0/11	启月	Ð	启用			
		1/0/12	启月	ŧ	启用			
系统班伊 ————————————————————————————————————		1/0/13	禁用	Ð	禁用			
		1/0/14	禁用	ŧ	禁用			
<u>赤川火回</u>		1/0/15	禁用	Ħ	禁用			-
退出登录				全选	提交帮	助		

然后在"组播管理-IGMP 侦听-组播 VLAN"一栏中,启用组播 VLAN40,路由器端口时间和成员端口时间根据需要填写,一般选择推荐值。静态路由器端口也就是发送组播数据的端口,

选中端口 13, 之后点提交。

TL-SH6428	基本配置 端口配置 VLAN配置 组描VLAN 查询器配置 Profile配置 Profile绑定 报文统计
	组播VLAN
系统管理	组擢VIAN·
	VLAN ID: [40 [2-4094] [2-4094]
	路由器端口时间: 0 秒 (0, 60-600, 推荐300秒) 帮助
	成员端口时间: 0 秒 (0, 60-600, 推荐260秒)
• IGMP侦听	动态路由器端口
◆ MLD侦听	UNIT: 1 LAGS
• 组播地址表	2 4 6 8 10 12 14 16 18 20 22 24
路由功能	1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28
服务质量	
	静态路由器端口
	UNIT: 1 LAGS
	2 4 6 8 10 12 14 16 18 20 22 24
系统维护	1 3 5 7 9 11 13 5 17 19 21 23 25 26 27 28
索引页面	
	🔤 未选中的端口
退出登录	

第六步、组播 VLAN 测试

设置好组播 VLAN 和 IGMP 侦听后,服务器通过交换机的 13 端口开始发送组播数据,接 收端电脑连接交换机的 1-12 端口,由于未知组播报文丢弃,此时是收不到组播报文的。当 接收端电脑发送加入该组播组的声明之后,该 13 口的组播源发送的组播组数据不再被认为 是未知组播报文,故可以被接收端电脑收到。

第七步、组播静态地址表的设置

对于某些特定的场所来说,接收端即组播成员端口下终端不支持标准的组播协议,是不会发出加入这个组播的通告的。由于设置了未知组播报文丢弃,所以该成员端口是不会收到未通告过的组播报文的。此时,为了保证该成员端口也能接收到组播数据,可以设置静态组播地址表。



在"组播管理-组播地址表-IPv4静态组播地址表"中,填写需要加入的组播 IP 和组播 VLAN,

转发端口选择无法发送通告报文的端口8,之后点击添加。

TI-SH6428	IPv4组播地址表	IPv4静态组播地址表	IPv6组播地址表	IPv6静态组播地址表	
	新建条目				
系统管理	组播IP:	224.1.1.	1	(格式为: 225.0.0.1)	
堆叠功能	VLAN ID:	40]	(1-4094)	
	转发端口:			1	添加
	LINIT:	1 1465			
14.100 · · · · · · · · · · · · · · · · · ·	ESTERT.				
• IGMP侦听		5 7 9 11 13 1	5 17 19 21 23	25 26 27 28	
• MLD侦听	<u>bidbid</u>	<u>Cablabiabiabiabia</u>		25 20 21 20	
• 组播地址表			全选	清空	
路田切能 		273			
		——————————————————————————————————————	选中的端口	选中的端口 不可选端口	
SNMP	显示设置				
LLDP	显示设置	全部	~		查找
系统维护					
	静念祖備表	行揺り		*#427#	1
索引 <u>负</u> 面	辺洋	油油IP	VLAN ID	转反)而L 2 5 中	1
退出登录			7211		
			全选 册	除 帮助	

这时在组播地址表中便会生成一条静态的地址表,默认将组播地址为224.1.1.1的组播报文 转发到8端口。

IPv4组播地址表 IP	v4静态组播地址表	IPv6组播地址表	IPv6静态组播地址表		
显示设置					
显示设置	全部	~			查找
组播IP表					
组播IP	VLAN IE)		转发端口	
224.1.1.1	40		1	/0/8,1/0/13	
		刷新	帮助		

此时,不需要接收端发送组播通告报文,一样可以接收到组播数据。

以上即可完成组播 VLAN 和 IGMP 侦听的设置满足用户的使用需求,配置完成后记得保存

配置。

第8章 路由功能

8.1 交换机 DHCP 中继配置指南

8.1.1 应用介绍

在大型的网络中,可能会存在多个子网。DHCP 客户端通过网络广播消息获得 DHCP 服务器的响应后得到 IP 地址。但广播消息是不能跨越子网的。因此,如果 DHCP 客户端和服务器在不同的子网内,客户端还能不能向服务器申请 IP 地址呢?这就需要用到 DHCP 中继功能。DHCP 中继功能,承担不同子网间 DHCP 客户端和服务器的通信任务。

8.1.2 需求介绍

某企业使用三层交换机划分多个子网,同时装有一台专用的 DHCP 服务器。三层交换机上 不配置 DHCP 服务器,各个子网都由专用的 DHCP 服务器分配 IP 地址。



8.1.3 设置方法

登录到三层交换机的管理界面,点击"路由功能-DHCP中继-全局配置",启用交换机的DHCP

中继功能,如下图:

TI -SH6428	全局配置 DHCP服务器
	操作成功。
	全局配置
系统管理	
堆叠功能	
二层交换	Option 82配置
VLAN	Option 82支持: 〇 启用 🖲 禁用
生成树	已存在Option 82处理: 保留 🗸
组播管理	Option 82自定义:
路由功能	
• 接凵 	
*	远柱IU于选坝:
* 閉心哈田 • 敗中陆討主	提交帮助
 策略路由 	
 DHCP服务器 	
• DHCP中继	电路ID和远程ID只允许汉字、英文字母、数字、空格和一些特殊字符-@//并且长度不超过64个字符(1个中
・代理ARP	又按2个字符计算)。
• ARP	
• RIP	
。	
• Option 82 配	置需要根据实际需求确认是否开启。Option 82 一般在 802.1X 认证等应用中会
使用到。	

点击"路由功能>DHCP 中继>DHCP 服务器",添加 DHCP 服务器地址,如下图:

TL-SH6428	全局配置 DHCP服务器	
	添加DHCP服务器地址	填写需要通过服务器分配地址的VLAN 信息
系统管理 	接口ID:	VLAN ~ 30 (1-4094)
二层交换 VI AN	服务器地址:	192.168.0.10 (格式: 192.168.2.1) 1首写DHCP服条器ID批批
生成树	DHCP服务器列表	
	选择 接口ID	服务器地址
路由功能	VLAN10	192.168.0.10
• 接口	VLAN20	192.168.0.10
 路由表 	VLAN30	192.168.0.10
 静态路由 路由映射表 		全选 删除 帮助

这样,就可以实现三层交换机的不同子网都通过专用的 DHCP 服务器分配 IP 地址。

8.2 三层网管交换机策略路由配置指导

8.2.1 应用介绍

交换机的策略路由 (PBR: Policy-Based Routing) 提供了一种比基于目的地址进行路由转发更加灵活的数据包路由转发机制。

策略路由可以根据 IP/IPv6 报文源地址、目的地址、端口、报文长度等内容灵活地进行路 由选择,优先级比普通的路由高,这样就可以按照管理员的意志针对部分感兴趣的流量重新 定义报文的转发路径,满足一些特殊场景下的需求。



8.2.2 需求介绍

某公网络出口分为外网和专网,需要通过交换机的策略路由实现不同部门访问不同网络。

需求介绍:

(1) 研发部、财务部、销售部分别划分成不同网段;

(2)研发部门、财务部和销售部门之间不能互访;

(3)研发和财务部门不能访问外网,但可以访问公司内网;销售部门既可以访问外网,也可以访问公司内网。

需求分析:

(1) 交换机对接两台路由可以通过设置交换机路由口对接不同的出口路由;

(2) 不同部门不能够互访可以通过设置 ACL 规则来实现;

(3) 针对这种不同网段访问不同资源需要从不同出口路由转发的情况,可以使用核心三层交换机的策略路由功能,通过 ACL 条目匹配交换机中的数据流,针对数据流指定路由下一跳的 IP 地址,从而实现不同数据流从不同出口转发。

拓扑如下:



8.2.3 设置方法

第一步、研发部、财务部、销售部分别划分为不同网段

交换机按照常规给三个部门规划好 VLAN, 接口地址, DHCP 地址池, 这里就不再详细描

述,具体配置结果如图:

VL	AN配置	端口配置			
ŀ	VLAN	記置列表			
	选择	VLAN ID	名称	成员	操作
		1	System-VLAN	6/0/13-22,6/0/25-32	编辑 详细
		10	研发部	6/0/1-4	编辑 详细
		20	财务部	6/0/5-8	编辑 详细
		30	销售部	6/0/9-12	编辑 详细
		1000	INTERNAL-VLAN	6/0/23	编辑 详细
		1001	INTERNAL-VLAN	6/0/24	编辑 详细
			全选	新建 删除 帮助	

接口列表							
选择	接口ID	模式	IP地址	子网掩码	接口名称	状态	操作
	Gi6/0/24	Static	192.168.111.2	255.255.255.0	对接外网路由器的接口IP	Up	编辑 编辑IPv6 详细
	Gi6/0/23	Static	192.168.100.2	255.255.255.0	对接内网路由的接口IP	Up	编辑 编辑IPv6 详细
	Vlan30	Static	192.168.30.1	255.255.255.0	销售部接口	Up	编辑 编辑IPv6 详细
	Vlan20	Static	192.168.20.1	255.255.255.0	财务部接口	Down	编辑 编辑IPv6 详细
	Vlan10	Static	192.168.10.1	255.255.255.0	研发部接口	Up	编辑 编辑IPv6 详细
	Vlan1	Static	192.168.0.1	255.255.255.0		Up	编辑 编辑IPv6 详细
			4	送 删除	帮助		

地址池》	列表						
选择	名称	网络号	掩码	租期	起始地址	结束地址	操作
	研发部	192.168.10.0	255.255.255.0	120	192.168.10.10	192.168.10.250	编辑 查看
	财务部	192.168.20.0	255.255.255.0	120	192.168.20.10	192.168.20.250	编辑 查看
	销售部	192.168.30.0	255.255.255.0	120	192.168.30.10	192.168.30.250	编辑 查看
			全选	删除	帮助		

第二步、研发部门、财务部和销售部门之间不能互访

通过 ACL 实现双向禁止访问, 配置 ACL 并绑定对应接口后如图:

- 3/5/6/7/8 系列企业级交换机 -

ACL列表	新建AC	CL MAC A	ACL 标准IP ACL	扩展IP ACL IPv	6 ACL		
ACL	眎						
Ĕ	5择ACL:		ACL 610 ~]			
A	CL类型:		标准IP ACL				
Ħ	则排序:		用户配置		~ > 그 교구 소 1		
+0.00				阻止研友证	川川川分り	和玥告部	_
光则	一 夜	Rula ID	海口地中	日約10	ահերի	时间的夕文	
	د-تد/ 1	1	192 168 10 0	192 168	нонц 3 20 0		
	2	2	192.168.10.0	192.168	3.30.0		
					全洗	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
ACL列表	新建AC	CL MAC A	ACL 标准IP ACL	扩展IP ACL IPv6	ACL		
ACU	=_						
ACL			101.000	1			
1	☆持拿ACL:		ACL 620				
· /	ACL类型:		标准IP ACL				
, ,	观则排序:		用户配置	止财务访问	研发和销	售部	
规则	列表						
选择	序号	Rule ID	源IP地址	目的IPt	也址	时间段名字	
	1	3	192.168.20.0	192.168	.10.0		
	2	4	192.168.20.0	192.168	.30.0		
					全选	删除 帮助]
			A				
ACL列表	新建AG	CL MAC A	ACL 标准IP ACL	扩展IP ACL IPv	6 ACL		
-							
ACL	显示						
ì	选择ACL:		ACL 630 🗸]			
A	(CL类型:		标准IP ACL				
ŧ	则排序:		用户配置	阳止绌佳动	心方问研	发和财务或	
规回应	列表				- וערדידנא או		1
选择	序号	Rule ID	源IP地址	目的IP	地址	时间段名字	
	1	5	192.168.30.0	192.168	3.10.0		
	2	6	192.168.30.0	192.168	3.20.0		
					全选	删除 帮助	
	_						

第三步、设置策略路由控制不同部门的外网权限

1、配置路由接口

配置交换机的路由口地址,对接不同出口路由器,在交换机 Web 界面:"路由功能"—"接口" —"接口 ID"--"路由口",配置 23 端口对接内网路由的接口 IP 和 24 端口对接外网路由器的 接口 IP:

接口设置						
د						
的建设山	_					
接口ID: 路(±□ ~					
UNIT: 6						
2 4 6 8 10	0 12 14 16	18 20 22 24	26 28	30 32		
1 3 5 7 9	11 13 15	17 19 21 23	25 27	29 31		
			-			创建
IP地址模式: 〇	None 🖲 Stat		BOOTP			- Bitter
IP地址:		(格式: 192.16	8.0. 1)			
子网掩码:		(格式: 255.25	5.255.0)			
管理状态: 开启	∃ ~					
接口名称:		(可选。1-16字符	夺)			
		_				
接口列表						
选择 接口ID	模式	IP地址	子网掩码	接口名称	状态	操作
Gi6/0/24	Static	192.168.111.2	255.255.255.0	对接外网路由器的接口IP	Up	编辑 编辑IPv6 详细
Gi6/0/23	Static	192.168.100.2	255.255.255.0	对接内网路由的接口IP	Up	编辑 编辑IPv6 详细
Vlan30	Static	192.168.30.1	255.255.255.0	销售部接口	Up	编辑 编辑IPv6 详细
Vlan20	Static	192.168.20.1	255.255.255.0	财务部接口	Down	编辑 编辑IPv6 详细
Vlan10	Static	192.168.10.1	255.255.255.0	研发部接口	Up	编辑 编辑IPv6 详细
Vian1	Static	192.168.0.1	255.255.255.0		Up	编辑 编辑IPv6 详细
		全	选 删除	帮助		

2、配置标准 IP ACL

配置标准 IP ACL 列表,指定数据流量,在交换机 Web 界面:"访问控制"—"ACL 配置"— "新建 ACL"--"标准 IP ACL",创建标准 IP ACL 条目(此条目的目的是指定策略路由的源目 的 IP):

本次举例研发部访问公司内网的数据流创建方法。

ACL列表 新建ACL MAC	ACL 标准IP ACL 扩展IP ACL IPv6 ACL
标准IP ACL	
访问控制列表ID:	ACL 510
规则ID: 安全操作:	10 (0-1999) 分 在
☑ 源IP:	
☑ 目的IP:	10.10.10.0 地址撞码: 255.255.255.0
HJIPJE2:	□研发部访问公司内网的数据流

最终创建的几条数据流条目如图:

— 3/5/6/7/8 系列企业级交换机 —

ACL列表新建A	CL MAC ACL	标准IP ACL 扩展	展IP ACL IPv6 ACL		
101 B-					
ACL显示	ACI	510			
ACL举型:	「たし」	P ACL			
规则排序:	用户面				
					_
规则列表 选择 序号	Rule ID	渡IP 地址	目的旧地址	时间的夕字	
	10	192.168.10.0	10.10.10.0		
研約	发访问内网的	的数据流	É	と选 删除 帮助	b
ACI 列表 新建A		标准IPACI扩展		1	
ACL显示					
选择ACL:	ACL	. 520 🗸			
ACL类型:	标准	PACL			
规则排序:	用户	配置			
规则列表					
选择序号	Rule ID	源IP地址	目的IP地址	时间段名字	
	20	192.168.20.0	10.10.10.0		
财多	务访问内网的	り数据流	1		
ACL列表新建AC	CL MAC ACL	标准IP ACL 扩展	副P ACL IPv6 ACL		
ACL列表 新建AC	CL MAC ACL	标准IP ACL 扩展	뢰P ACL IPv6 ACL		
ACL列表 新建AC	CL MAC ACL	标曲P ACL 扩展	뢰P ACL IPv6 ACL		
ACL列表 新建AC ACL显示 选择ACL: ACL类型:	CL MAC ACL ACL 标曲F	标曲P ACL 扩展 530 マ	뢴P ACL IPv6 ACL		
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序:	CL MAC ACL ACL 标泪F 用户酉	标曲P ACL 扩展 530 V P ACL	ਫ਼IP ACL IPv6 ACL		
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序:	CL MAC ACL ACL 标准IF 用户面	标曲P ACL 扩展 530 v P ACL 2音	뢵IP ACL IPv6 ACL		
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 选择 序号	CL MAC ACL ACL 标准IF 用户面	标准IP ACL 扩展 530 V P ACL 语	≷IP ACL IPv6 ACL	时间段名字]
ACL列表 新建AC ACL显示 选择ACL: 选择ACL: ACL类型: 规则排序: 规则列表 选择 序号 1	CL MAC ACL ACL 标准IF 用户面 Rule ID 30	标准IP ACL 扩展 530 ▼ P ACL C置 源IP地址 192.168.30.0	副P ACL IPv6 ACL 目的IP地址 10.10.10.0	时间段名字 	
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 选择 序号 □ 1 详售	CL MAC ACL ACL 标測F 用户面 Rule ID 30 到内网的数	标准IP ACL 扩展 530 ▼ P ACL 彊 源IP地址 192.168.30.0 据流	IP ACL IPv6 ACL 目的IP地址 10.10.10.0	时间段名字 	
ACL列表 新建ACL ACL显示 选择ACL: 法择ACL: ACL类型: 规则排序: 规则排序: 规则列表 选择 序号 □ 1 销售	CL MAC ACL ACL 标准F 用户面 Rule ID 30 到内网的数	标曲P ACL 扩展 530 ▼ P ACL C置 源IP地址 192.168.30.0 据流	뢰P ACL IPv6 ACL 目的IP地址 10.10.10.0	时间段名字 注选 删除 報日	
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 选择 序号 口 1 详售	CL MAC ACL ACL 标卸F 用户面 Rule ID 30 到内网的数	标曲PACL 扩展 530 ▼ PACL 彊 192.168.30.0 据流	립면 ACL IPv6 ACL 目的IP地址 10.10.10.0	时间段名字 注选 删除 報訊	D
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 选择 序号 □ 1 销售	CL MAC ACL ACL 标曲F 用户面 30 到内网的数 CL MAC ACL	标曲P ACL 扩展 530 ▼ P ACL 遭 第IP地址 192.168.30.0 据流 标准IP ACL 扩展	剧P ACL IPv6 ACL 目的IP地址 10.10.10.0 属IP ACL IPv6 ACL	时间段名字 注选 删除 種目	
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 选择 序号 口 1 详任 ACL列表 新建A	CL MAC ACL ACL 标單F 用户面 30 到内网的数 CL MAC ACL	标曲P ACL 扩展 530 ▼ ACL 置 第四地址 192.168.30.0 据流 标曲P ACL 扩展	립P ACL IPv6 ACL 目的IP地址 10.10.10.0	时间段名字 2选 删除 報用	
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 近译 序号 口 1 销售	CL MAC ACL ACL 标准F 用户面 30 到内网的数 CL MAC ACL	标准IP ACL 扩展 530 ▼ P ACL 语 192.168.30.0 据流 标准IP ACL 扩展	IPv6 ACL IPv6 ACL 目的IP地址 10.10.10.0 로	时间段名字 注选 删除 報用	
ACL列表 新建ACL ACL显示 选择ACL: ACL类型: 规则列表 选择 序号 1 计首售 ACL列表 ACL列表 新建ACL ACL列表 新建ACL ACL列表 新建ACL	CL MAC ACL ACL 标曲F 用户面 30 到内网的数 CL MAC ACL ACL 标准	标准IP ACL 扩展 530 ▼ P ACL 语 192.168.30.0 据流 标准IP ACL 扩展 531 ▼ P ACL	립P ACL IPv6 ACL 目的IP地址 10.10.10.0	时间段名字 2选 删除 帮用	
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 近择 序号 □ 1 销售 ACL列表 ACL列表 新建AC ACL见示 选择ACL: ACL显示 选择ACL: ACL显示 选择ACL: ACL显示 选择ACL: 和CL类型: 规则排序:	CL MAC ACL ACL 标准F 用户面 30 到内网的数 CL MAC ACL ACL 标准I 用户面	标准IP ACL 扩展 530 ▼ P ACL 理 源IP地址 192.168.30.0 据流 标准IP ACL 扩展 531 ▼ P ACL 配置	립마 ACL IPv6 ACL 目的IP地址 10.10.10.0 로	时间段名字 注选 删除 帮用	
ACL列表 新建ACL ACL显示 选择ACL: 成上菜型: 规则列表 选择 序号 □ 1 销售 ACL列表 新建ACL ACL列表 新建ACL ACL列表 新建ACL ACL显示 法择ACL: ACL显示 法择ACL: 和U則排序: 規则則排序:	CL MAC ACL ACL 标單F 用户面 30 到内网的数 CL MAC ACL 反面 原理 用户面 和户面	标准IP ACL 扩展 530 ▼ P ACL 留 192.168.30.0 据流 标准IP ACL 扩展 531 ▼ P ACL 配置	립PACL IPv6ACL 目的IP地址 10.10.10.0 ((로IPACL IPv6ACL	时间段名字 2选 删除 架相	
ACL列表 新建ACL ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 原号 □ 1 销售 ACL列表 ACL列表 新建ACL ACL列表 新建ACL ACLL 法 ACL列表 新建ACL ACL显示 法择ACL: ACL 東原号 近择 序号	CL MAC ACL ACL 标准IF 用户面 30 到内网的数 CL MAC ACL ACL 标准II 用户面 30 Rule ID 属CL	标准IP ACL 扩展 530 ▼ P ACL 遭 第IP地址 192.168.30.0 据流 标准IP ACL 扩展 531 ▼ P ACL 配置 源IP地址	로IP ACL IPv6 ACL 目的IP地址 10.10.10.0 로IP ACL IPv6 ACL	时间段名字 	
ACL列表 新建AC ACL显示 选择ACL: ACL类型: 规则排序: 规则列表 序号 □ 1 销售 ACL列表 新建AC ACL列表 新建AC ACL列表 新建AC ACL列表 新建AC ACL显示 法择ACL: ACL显示 选择ACL: 加则排序: 规则排序: 规则列表 选择 选择 序号 □ 1	CL MAC ACL ACL 标曲F 用户面 30 到内网的数 CL MAC ACL CL MAC ACL ACL 标曲 用户配 用户配	标准IP ACL 扩展 530 ▼ P ACL 理 源IP地址 192.168.30.0 据流 标准IP ACL 扩展 531 ▼ P ACL 配置	程PACL IPv6ACL 目的IP地址 10.10.10.0 展IPACL IPv6ACL 目的IP地址 0.0.0.0	时间段名字 送选 删除 帮用	

3、创建路由器映射表

指定策略路由的条目名称,后续用此条目绑定对应的 VLAN 接口,使能接口,在交换机 Web 界面:"路由功能"—"路由映射表"—"创建路由映射表",此处创建三条路由映射表分 别为:研发到内网,财务到内网和销售到内网和外网三条条目:

创建路由映射表	配置路由映射表 规则列表
创建路由映射	表
名称: 序列号: 操作:	研发到内网 10 0-65535 (默认:10) 允许
	创建和助
创建路由映射表	配置路由映射表 规则列表
创建路由映射	表
名称:	财务到内网
序列号:	20 0-65535 (默认:10)
序列号: 操作:	20 0-65535 (默认:10) 允许 v

创建路由映射表	配置路由映射表	规则列表		
创建路由映射	表			
名称:	销售	到内网和外网		
序列号:	30		0-65535	(默认:10)
操作:	允许	Ŧ ~		
		创建	帮助	

创建路由映射表	配置路由映射表	规则列表				
						_
创建路由映射	表					
名称:	销售	到内网和外网]			
序列号:	31		0-65535	(默认:10)		
操作:	允许	-	\sim			
		创建	帮助]		

4、配置路由映射表,针对数据流配置交换机的转发操作,在交换机 Web 界面:"路由功能"—"路由映射表"—"创建路由映射表,配置路由映射表",创建路由映射表名称 --路由映射表匹配数据流 --针对匹配的数据流执行的转发操作:

本次列举销售部访问内网和外网数据流匹配操作。

内网:

创建	路由映射表	配置路由映射表 规则列表
1	创建路由映射潮	
	名称:	创建映射表名称
	序列号:	30 🔽 🔽 创建映射表序列号
	配置:	匹配IP ACL 530 (500-2499)
创建	路由映射表	配置路由映射表 规则列表
1	创建路由映射表	長規则
	名称:	销售到内网和外网 🗸
	序列号:	30 将匹配的数据流执行下一跳到内网路由
	配置:	设置下一跳 192.168.100.1 (格式为: 192.168.0.1)
		提交 帮助

说明:

- 交换机"设置下一跳"代表这条条目的优先级比系统直连路由高,即:VLAN 间互访数据也会匹配
 策略路由条目而不是匹配直连路由条目。
- 交换机"设置缺省下一跳"代表这条条目的优先级比系统直连路由低,即:VLAN 间互访数据会匹优先匹配直连路由。

外网:

8 8	建路由映射表	<u>配置路由映射表</u> 规则列表
_		
	创建路由映射表	规则
	名称:	销售到内网和外网
	序列号:	31 内网序列号30,外网序列号31,数字越小优先级越高
	配置:	匹配IP ACL 531 (500-2499)
		提交 帮助 匹配销售访问外网的数据流
创建	建路由映射表	配置路由映射表 规则列表
创建	即由映射表	配置路由映射表 规则列表 · · · · · · · · · · · · · · · · · · ·
创建	^{建路由映射表} 创建路由映射表	配置路由映射表 规则列表
创建	踏由映射表 创建路由映射表 名称:	配置路由映射表 规则 期間 销售到内网和外网 ∨
创强	踏由映射表 创建路由映射表 名称: 序列号:	配置路由映射表 規则列表 規则 期告目内网和外网 ▼ 31 ▼
创建	 路由映射表 创建路由映射表 名称: 序列号: 配置: 	配置路由映射表 规则列表 规则 销售到内网和外网 ∨ 31 ∨ 设置下一跳 ↓ 192.168.111.1 (格式为: 192.168.0.1)
ئ اھ	路由映射表 创建路由映射表 名称: 序列号: 配置:	配置路由映射表 规则列表 规则 销售到内网和外网 ◇ 31 ◇ 设置下一跳 192.168.111.1 (楷式为: 192.168.0.1) 提交 帮助 执行销售访问外网下一跳到外网路由器

() 说明:

- 交换机"设置下一跳"代表这条条目的优先级比系统直连路由高,即:VLAN 间互访数据也会匹配
 策略路由条目而不是匹配直连路由条目。
- 交换机"设置缺省下一跳"代表这条条目的优先级比系统直连路由低,即:VLAN 间互访数据会匹优先匹配直连路由。
- 在做数据流匹配的时候,一个路由映射表名称可以匹配多个数据流,通过序列号区分,且序列号 越小优先级越高。

最终创建的几条路由映射表规则条目如下:

- 3/5/6/7/8 系列企业级交换机 -

创建路由映射表 配置路由映	射表 规则列表	
路由映射表		
名称:	研发到内网	删除
语句		
序列号:	10 🗸	删除
操作类型:	允许 🗸	修改
规则列表	指定研发访问内网的数据	下一跳为内网路由器的地址
选择 序号	匹配/设置	数值
0	匹配IP ACL	510
1	设置下一跳	192.168.100.1
	全选 删除 帮助	
创建路由映射表 配置路由映	討表 规则列表	
路由映射表		
名称:	财务到内网 🗸	删除
连句		
店到日.	20	mira
序列号:	20 V	
"嘿"作笑望: 	财务访问内	网的数据流下一跳地址为内网路由器地址
规则列表		
选择 序号	匹配/设置	数值
		520
		192.108.100.1
	全选 删除 帮助	
创建路由映射表 配置路由映	村表 规则列表	
路由映射表		
名称:	销售到内网和外网 🗸	删除
治 句		
序列号:	30 「序列号: 30	
操作类型:	│ 允许	的数据下一跳为内网路由器
规则列表	A DECKST OF STORE	
选择 序号	匹配设置	数值
0	匹配IP ACL	530
	设置下一跳	192.168.100.1
	全选 删除 帮助	
L		

创建路由映射表	配置路由映射	表规则列表				
路由映射表						
名称:		销售到内网和外的	X] ~			删除
语句						
序列号:		31	▶ 序列	号: 31		删除
操作类型:		允许	▼ 销售i	方问外网的	数据流下一	修改 跳为外网路由
规则列表						
选择	序号		匹配/设置			数值
	0		匹配IP ACL			531
	1		设置下一跳		192.1	168.111.1
		全选	删除	帮助		

5、配置策略路由

将配置好的路由映射表规则绑定到对应的 VLAN 接口, 在交换机 Web 界面:"路由功能"

策	略路由配置		
	策略路由表	表	
	选择	接口ID	路由映射表名称
		Gi6/0/24	
		Gi6/0/23	
		Vlan30	销售到内网和外网
		Vlan20	财务到内网
		Vlan10	研发到内网
		Vlan1	将对应的路由映射表规则绑定到对应的VLAN接口 修改 删除 帮助

—"策略路由"—"策略路由配置":



一个接口只能绑定一条路由映射表名称,但可以通过一个路由映射表中的序列号区分不同的数据 流和动作。

6、配置内网和外网路由器

配置内网路由的 NAPT 条目和静态路由条目,保证数据正常转发。

内网路由器 NAPT 规则:

- 3/5/6/7/8 系列企业级交换机 -

NAPT规	NAPT规则列表									
						🕂 新增 🍸 删除				
	序号	规则名称	出接口	源地址范围	状态	设置				
	1	NAT_LAN_WAN1	WAN1	192.168.100.0/24	已启用					
	2	NAT_LAN_WAN2	WAN2	192.168.100.0/24	已启用					
	3	yanfa	WAN2	192.168.10.0/24	已启用ぐ	2 🕯				
	4	cxaiwu	WAN2	192.168.20.0/24	已启用	2				
	5	xiaoshou	WAN2	192.168.30.0/24	已启用	2				

内网路由器回程路由规则:

静态路	各由									•
									¢	新增 👕 删
	序号	规则名称	目的地址	子网掩码	下一跳	出接口	Metric	可达性	状态	设置
	1	yanfa	192.168.10.0	255.255.255.0	192.168.100.2	LAN	0	可达	已启用 오	2
	2	caiwu	192.168.20.0	255.255.255.0	192.168.100.2	LAN	0	可达	已启用📀	2
	2	viaoshou	192,168,30,0	255,255,255.0	192.168.100.2	LAN	0	不可达	已启用	

配置外网路由的 NAPT 条目和静态路由条目,保证数据正常转发。

外网路由器 NAPT 规则:

NAPT	—对—	NAT 虚拟服务器 ,	ALG服务 NAT-DMZ				
NAPT规则列表							
							🕂 新増 🗧 删除
	序号	规则名称	出接口	源地址范围	状态	备注	设置
	1	NAT_LAN_WAN1	WAN1	192.168.111.0/24	已启用		
	2	NAT_LAN_WAN2	WAN2	192.168.111.0/24	已启用		
	3	xiaoshou	WAN1	192.168.30.0/24	已启用😣	销售部	A 🖻
	4	xiaoshou2	WAN2	192.168.30.0/24	已启用😣	销售部	🤌 💼

外网路由器回程路由规则:

	策略	路由	静态路由	IPv6静态路由 系统	充路由						
١.											
	静态路由										
							🔮 启用 🏾	🗴 禁用	🕂 新増 🌘	🛢 删除 (傻 搜索	🛓 🝳 全局搜索
		序号	规则名称	目的地址	子网掩码	下一跳	出接口	Metric	可达性	状态	设置
		1	销售部回程路由	192.168.30.0	255.255.255.0	192.168.111.2	LAN	0	可达	已启用😣	A 🗇
								共1条	,每页: 10	0 ∨ <mark>条</mark> 当前:	1/1页, 1~1条 < 1 >





至此,以上需求便可以通过配置交换机的策略路由功能全部实现。

第9章 服务质量

9.1 交换机带宽控制配置指南

9.1.1 应用介绍

交换机的带宽控制功能可以控制每个端口的出入口速率,在使用有限带宽的情况下,保证每 个终端都能正常使用应用,不会因为某个端口流量过大导致其他终端无法上网的情况。

9.1.2 需求介绍

某出租屋的管理人员发现经常有租户在使用电脑下载大量视频数据,在下载数据时导致其他 用户无法使用网络,因此管理人员通过设置接入交换机的端口带宽控制功能控制每个端口的 出入口速率,保障所有用户的上网使用,示意网络拓扑如下:



9.1.3 设置方法

在"服务质量->流量管理->带宽控制"中,设置所有下联终端端口的出入口速率为 5Mbps, 上联口 24 口不限制,注意单位为 Kbps,如下如所示。

带	宽控制	风暴抑制			
	带宽控制	J			
	UNIT:	1 LAC	GS		
	选择	端口	入口带宽 (Kbps)	出口带宽 (Kbps)	LAG
		1/0/1	4992	4992	^
		1/0/2	4992	4992	
		1/0/3	4992	4992	
		1/0/4	4992	4992	
		1/0/5	4992	4992	
		1/0/6	4992	4992	
		1/0/7	4992	4992	
		1/0/8	4992	4992	
		1/0/9	4992	4992	
		1/0/10	4992	4992	
		1/0/11	4992	4992	
		1/0/12	4992	4992	•
			全选 提	交帮助	

说明:

同一个端口的入口带宽限制和风暴抑制不能同时开启;且端口限制数值必须为 64 的整数倍,输入其他数值后设备会自动匹配最近的一个值。

这样就可以限制除上联端口外的其他端口的进出口速率约为 5 Mbps, 保障了整个网络中终端都可以正常使用网络。

9.2 交换机风暴抑制配置指南

9.2.1 应用介绍

交换机的风暴抑制功能允许交换机在网络中过滤广播、多播和 UL 包。如果三种数据包的传输速率超过了设置的带宽,则会自动丢弃数据包以避免网络广播风暴,保障网络的运行稳定性,这种应用一般在无线网络的场景较多。

9.2.2 需求介绍

某企业使用一台3系列交换机作为接入层设备,为了保障网络(尤其是无线网络)运行的稳定性,需要对真个网络拓扑中的广播包流量有所控制,因此需要在交换机上设置端口的最大接受广播速率,如果端口的接受广播速率超过此值,则丢弃多余广播包,保障网络稳定性。示意网络拓扑如下:



9.2.3 设置方法

在"服务质量->流量管理->风暴抑制"中,设置所有终端端口的广播接受速率为 200Kbps(一

般情况下无线场景接 AP 的千兆端口建议值),如下如所示:

带	宽控制	风暴抑制									
	风暴抑制	IJ									
	UNIT:	1 LAG	S								
	选择	端口	PPS模式	广播包抑制单位	广播包抑制	组播包抑制单位	组播包抑制	UL包抑制单位	UL包抑制	LAG	
			~	~		~		~			
		1/0/1	禁用	kbps	192	kbps		kbps			-
		1/0/2	禁用	kbps	192	kbps		kbps			
		1/0/3	禁用	kbps	192	kbps		kbps			
		1/0/4	禁用	kbps	192	kbps		kbps			
		1/0/5	禁用	kbps	192	kbps		kbps			
		1/0/6	禁用	kbps	192	kbps		kbps			
		1/0/7	禁用	kbps	192	kbps		kbps			
		1/0/8	禁用	kbps	192	kbps		kbps			
		1/0/9	禁用	kbps	192	kbps		kbps			
		1/0/10	禁用	kbps	192	kbps		kbps			
		1/0/11	禁用	kbps	192	kbps		kbps			
		1/0/12	禁用	kbps	192	kbps		kbps			-
					全选	提交 帮助	Ъ				

说明:

- 同一个端口的入口带宽限制和风暴抑制不能同时开启;且端口限制数值必须为 64 的整数倍,输入其他数值后设备会自动匹配最近的一个值。
- PPS 模式:交换机统计数据包不按照字节统计,而是按照每秒多少个广播包数量统计;默认情况下 PPS 模式是禁用的状态,启用后,单位只能为 PPS,不能为 kbps 或 ratio。
- 交换机界面还有一个统计单位为 ratio,单位含义为比率,使用此单位时取值范围只能在 0-100
 范围内,含义为广播包占比端口总数据包的比例。

这样就可以限制端口的最高广播接受速率,保障了整个网络运行稳定性。

第10章 访问控制

10.1 交换机访问控制设置指南

10.1.1 应用介绍

在交换机中主要通过 ACL 来控制访问权限,由于交换机默认规则是转发所有数据,ACL 控制是逐条匹配的,通过访问控制可以根据需求限制什么可以访问,什么不可以访问,交换机 支持 MAC ACL ,标准 IP ACL ,扩展 IP ACL,控制非常灵活多变。

10.1.2 需求介绍

某企业划分了多网段,需要设置访问权限保障网络的安全性,本例使用其中的标准 IP ACL 进行配置,其余的 MAC ACL 等原理类似。示意网络拓扑如下:



需求

产品部:禁止访问研发部网络。

研发部:只允许访问服务器,禁止访问其余网络。

员工无线网络:禁止访问产品部、研发部、服务器网络。

访客网络:禁止访问产品部、研发部、员工无线网络、服务器网络。

10.1.3 设置方法

以研发部为例,具体设置如下:

首先需要新建一个 ACL ID,标准 IP ACL 的 ID 号范围是 500-1499,本例使用 520。在"访问控制->ACL 配置->新建 ACL"中,输入 520,点击创建即可。

ACL列表	新建ACL	MAC ACL	标准IP ACL	扩展IPACL
新建AC	L		_	
AC	LID:	520		0-499 MAC访问控制列表
				500-1499 标准IP访问控制列表
				1500-2499 扩展IP访问控制列表
规则	则顺序:	用户配	罟	
			创建	帮助

再根据需求创建 ACL 规则。在"访问控制->ACL 配置->标准 IP ACL"中,下拉选择创建的 ACL 520,输入规则 ID 21,安全操作选择允许,源 IP 为研发部 IP,目的 IP 为服务器 IP。 如下图所示,完成后点击提交。

- 3/5/6/7/8 系列企业级交换机 -

 ACL列表 新建ACL	MAC ACL 标准IP ACL 扩展IP ACL
标准IP ACL	
访问控制列表ID:	ACL 520
规则ID:	21 (0-1999)
安全操作:	允许 ~
☑ 濵IP:	192.168.20.0 地址掩码: 255.255.255.0 (格式为: 192.168.0.1)
✓ 目的IP:	192.168.253,0 × 地址掩码: 255.255.255.0
时间段:	无限制 🗸
	提交 帮助

禁止访问其余网络的规则如下所示:

标准IP ACL				
访问控制列表ID:	ACL 520	\sim		
规则ID:	22	(0-1999)		
安全操作:	丢弃 🗸 🗸			
☑ 濵IP:	192.168.20.0	地址掩码:	255.255.255.0	× (格式为: 192.168.0.1)
✓ 目的IP:	0.0.0.0	地址掩码:	0.0.0	
时间段:	无限制 >			

完成后 ACL 520 列表如下图所示:

ACL显	示					
选择ACL:			ACL 520 🗸			
ACL类型:			标准IPACL			
规!	则排序:		用户配置			
规则列	表					
选择	序号	Rule ID	源IP地址	目的IP地址	时间段名字	操作
	1	21	192.168.20.0	192.168.253.0		编辑 宣 上移 下移
	2	22	192.168.20.0	0.0.0.0		编辑 宣呑 上移 下移

最后绑定至相应 VLAN 中。在"访问控制->ACL 绑定配置->VLAN 绑定"中,下拉选择 ACL

520, 输入 VLAN ID 号 20, 点击添加。如下图所示:

绑定列表 端口绑定	VLAN绑定		
VLAN绑定配置			
ACL ID :	520	\sim	添加
VLAN ID :	20	 × (格式为: 1)	帮助

其余网络重复上述三个步骤即可,注意每个网络都需要创建一个 ACL ID 号以进行 VLAN 的

绑定。

其余网络创建后的 ACL 列表如下:

ACL显	示						
选	译ACL:	: ACL 510 🗸					
ACL类型: 标准IP ACL							
规	则排序:		用户配置				
规则列表							
选择	序号	Rule ID	源IP地址	目的IP地址	时间段名字	操作	
	1	11	192.168.10.0	192.168.20.0		编辑 宣吾 上移 下移	

ACL显	示									
选择ACL:			ACL 530 🗸							
ACL类型:			标准IPACL							
规则排序:			用户配置							
规则列	表									
选择	序号	Rule ID	源IP地址	目的IP地址	时间段名字	操作				
	1	31	192.168.30.0	192.168.10.0		编辑 宣看 上移 下移				
	2	32	192.168.30.0	192.168.20.0		编辑 宣看 上移 下移				
	3	33	192.168.30.0	192.168.253.0		编辑 宣看 上移 下移				

ACL 540 🗸						
标准IPACL						
操作						
看 上移 下移						
香 上移 下移						
看 上移 下移						
看 上移 下移						

以上通过设置交换机的访问控制功能实现了企业各部门的访问控制需求,如需要更具体的需求可以通过设置 MAC ACL 或者扩展 IP ACL 进行控制。其中 MAC ACL 根据数据包的源MAC 地址、目的 MAC 地址、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。

ACL列表	新建ACL MAG	CACL 标准IP AC	L 扩展	割P ACL	IPv6 ACL	
MAC ACL						
访问控	潮列表ID:	MAC访问控制列表	•			
规则ID):			(0-999)		
安全操	(作:	允许	~			
口源	MAC:			地址	止掩码:	
	的MAC:			地均	止掩码:	
🗆 v	LAN ID:			支持	控制二层以大	大网类型
	太网类型:			(4位十六进	制数)	
用户优	计先级:	无限制	~	•		
时间段	<u>}</u> :	无限制	~			
				提交	帮助)

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。

例:

1、新建 ACL ID, ID 范围 1500-2499。

ACL列表	所建ACL	MAC ACL	标准IP ACL	扩展IP ACL	
新建ACL					
ACL ID	:	1500			0-499 MAC访问控制列表
					500-1499 标准IP访问控制列表
					1500-2499 扩展IP访问控制列表
规则顺	字:	用户配	置		
			创建	帮助	

2、新建一条扩展 IP 条目:在时间 1 时间段丢弃源 IP 为 192.168.100.0/24, 源端口为 600,

IP 优先级 DSCP 字段字段为 1 的 TCP 数据包。

ACL列表 新建ACL M	IAC ACL 标准IP ACL 扩展IP ACL								
扩展IP ACL									
访问控制列表ID: 规则ID: 安全操作:	ACL 1500 V 10 (0-1999) 丢弃 V 源IP段192.168.100.0/24								
☑ 源IP:	地址掩 192.168.100.0 码: (格式为: 192.168.0.1)								
 目的IP: 	地址掩 码:								
IP 协议: · 源端미号:	6 TCP ✓ 600 TCP协议的源端□为600								
🗌 目的端口号:	IP报文代表报文优先级的字段								
DSCP: IP ToS:	1 ✓ 无限制 ✓ IP Pre: 无限制 ✓								
时间段:	时间段: 时间1 ✓ 在某个时间段内								
提交 帮助									

可以根据需要填写更具体的源目的 IP, 源目的端口, 以及对应的协议 (ICMP, UDP, TCP 等)

2、条目创建成功后,将对应 ID=1500 的条目绑定到端口或者 VLAN 接口上即可生效,此

处同标准 IP ACL 设置。

第11章 网络安全

11.1 交换机 DHCP 侦听配置设置指南

11.1.1 应用介绍

DHCP 主要作用是集中分配和管理 IP 地址,通常我们是通过路由器或三层网管交换机充当 DHCP 服务器的角色,但如果网络中有其他能够分配 DHCP 的非法服务器,也会给客户端 分配不正确的 IP,导致终端无法上网,网络结构紊乱。而开启"DHCP 侦听"功能,添加授信 端口,可以让终端和服务器只能从授信端口接收发送 DHCP Offer 报文,从而能正确的进行 网络通信。

11.1.2 需求介绍

某企业通过 3 系列交换机作为接入层使用,为了保证网络的运行稳定性,使终端只能从规定的 DHCP 服务器获取 IP 地址,不能从非法的 DHCP 获取地址,示意网络拓扑如下:



11.1.3 设置方法

在"网络安全->DHCP 侦听->全局配置"中, 启用 DHCP 侦听功能,并选择生效的 VLAN, 本例只有 VLAN 1 因此选择 VLAN 1,如果有其他 VLAN 需要开启侦听功能,也需要输入 对应的 VLAN ID,如下如所示。

全局配置 端口配置 0	otion 82配置
DHCP侦听配置	
DHCP侦听:	● 启用 ○ 禁用
VLAN ID:	
VLAN配置显示:	(1-4094, 形式: 1,3,4-7,11-30) 1
	提交帮助

在"网络安全->DHCP 侦听->端口配置"中设置连接合法路由器的端口为信任端口,本例设

置连接路由器的上联口1口为信任端口,其余为非信任端口,其余设置本例选择默认。

- 3/5/6/7/8 系列企业级交换机 -

全局配置 端口配置 Option 82配置										
DHCP侦听端口配置										
UNIT: 1 LAGS										
选择	端口	授信端口	MAC验证	流量控制	Decline侦听	LAG				
		~	~	5 🗸	~					
	1/0/1	启用	启用	禁用	禁用		-			
	1/0/2	禁用	启用	禁用	禁用					
	1/0/3	禁用	启用	禁用	禁用					
	1/0/4	禁用	启用	禁用	禁用					
	1/0/5	禁用	启用	禁用	禁用					
	1/0/6	禁用	启用	禁用	禁用					
	1/0/7	禁用	启用	禁用	禁用					
	1/0/8	禁用	启用	禁用	禁用					
	1/0/9	禁用	启用	禁用	禁用					
	1/0/10	禁用	启用	禁用	禁用					
	1/0/11	禁用	启用	禁用	禁用					
	1/0/12	禁用	启用	禁用	禁用					
	1/0/13	禁用	启用	禁用	禁用					
	1/0/14	禁用	启用	禁用	禁用					
	1/0/15	禁用	启用	禁用	禁用		-			
			全选 打	是交 帮助						
					1					

这样交换机上所接入的终端就只能从 1 口上联的设备获取地址, 不会从其余端口的非法

DHCP 服务器获取地址,保障了网络的安全性。
11.2 交换机四元绑定、ARP 防护、IP 源防护设置指南

11.2.1 应用介绍

四元绑定功能可以将局域网中计算机的 IP 地址、MAC 地址、VLAN 和端口进行绑定, ARP 防护功能以及 IP 源防护功能将使用四元绑定条目对数据包进行过滤, 在使用了四元绑定条目后可以启用 ARP 防护, IP 源防护来进行网络保护, 使只能是绑定条目中的设备才能通过交换机。

11.2.2 需求介绍

某企业通过 3 系列交换机作为接入层使用,为了保证网络的运行稳定性和安全性,需要开启 每个业务 VLAN 下的 ARP 防护和 IP 源防护功能,保证只有固定终端在固定端口才能正常 通过交换机转发数据,避免了非法的 ARP 攻击,示意网络拓扑如下:



11.2.3 设置方法

在"网络安全->四元绑定->扫描绑定"中,通过 ARP 扫描扫描当前所有正常接入交换机的终端设备,三个 VLAN 需要扫描三次,每次扫描出的结果选择防护范围为全部防护,并点击提交提交到绑定列表,如下如所示:

绑定列表 手动绑定 扫描绑定							
ARP扫描							
起始IP地址: 192 结束IP地址: 192 VLAN ID: 10	.168.10.1 .168.10.254 (1-4094)						扫描
扫描结果							
UNIT: 1							
选择主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	来源	冲突
					全部防护 🖌 🗸		
	192.168.10.20	8c-dc-d4-3f-2a-27	10	1/0/2	不防护	ARP扫描	
	全选	提交删除	刷	新	帮助		

最终通过扫描出来的四元绑定列表如下:

列表 手	动绑定 扫描绑定							
搜索条目								
来源:	全部来源	~						搜索
IP:								选择
继定列表								
LINIT.	4							
UNIT.	1							
选择	主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	来源	冲突
选择	主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	来源	冲突
选择	上 主机名 	IP地址 192.168.10.20	MAC地址 8c-dc-d4-3f-2a-27	VLAN ID 10	端口 1/0/2	防护范围 全部防护	来源 ARP扫描	冲突
	主机名	IP地址 192.168.10.20 192.168.30.10	MAC地址 8c-dc-d4-3f-2a-27 f8-8c-21-34-f1-dd	VLAN ID 10 30	端口 1/0/2 1/0/10	防护范围	来源 ARP扫描 ARP扫描	冲突
	□□ 主机名 	IP地址 192.168.10.20 192.168.30.10 192.168.20.20	MAC地址 8c-dc-d4-3f-2a-27 f8-8c-21-34-f1-dd f4-2a-7d-93-06-fb	VLAN ID 10 30 20	端口 1/0/2 1/0/10 1/0/6	防护范围 全部防护 全部防护 全部防护	来源 ARP扫描 ARP扫描 ARP扫描	冲突
	上 主机名 	IP地址 192.168.10.20 192.168.30.10 192.168.20.20 192.168.111.1	MAC地址 8c-dc-d4-3f-2a-27 f8-8c-21-34-f1-dd f4-2a-7d-93-06-fb f8-8c-21-25-83-94	VLAN ID 10 30 20 1	端口 1/0/2 1/0/10 1/0/6 1/0/24	防护范围 全部防护 全部防护 全部防护 全部防护 全部防护 全部防护	来源 ARP扫描 ARP扫描 ARP扫描 ARP扫描	冲突
	主机名	IP地址 192.168.10.20 192.168.30.10 192.168.20.20 192.168.111.1 192.168.111.6	MAC地址 8c-dc-d4-3f-2a-27 f8-8c-21-34-f1-dd f4-2a-7d-93-06-わ f8-8c-21-25-83-94 6c-62-6d-fa-49-49	VLAN ID 10 30 20 1 1	端口 1/0/2 1/0/10 1/0/6 1/0/24 1/0/22	防护范围	来源 ARP扫描 ARP扫描 ARP扫描 ARP扫描 ARP扫描	·····································
送择 □ □ □ □ □ □ □ □	主机名 2	IP地址 192.168.10.20 192.168.30.10 192.168.20.20 192.168.111.1 192.168.111.5 192.168.111.254	MAC地址 8c-dc-d4-3f-2a-27 f8-8c-21-34-f1-dd f4-2a-7d-93-06-ゆ f8-8c-21-25-83-94 6c-62-6d-fa-49-49 1 c-1b-0d-c9-b8-07	VLAN ID 10 30 20 1 1 1 1	端口 1/0/2 1/0/10 1/0/6 1/0/24 1/0/22 1/0/27	防护范围 全部防护 全部防护 全部防护 全部防护 全部防护 全部防护 全部防护	来源 ARP扫描 ARP扫描 ARP扫描 ARP扫描 ARP扫描 ARP扫描 手工添加	· 冲突

此时光有绑定列表还不能实现需求,需要在"网络安全->ARP 防护->防 ARP 欺骗"中启用源 MAC 验证,目的 MAC 验证,IP 验证,并使能对应的 VLAN,然后点击提交: 3/5/6/7/8 系列企业级交换机

防ARP欺骗 防ARP攻击	报文统计		
防ARP欺骗			
源MAC验证:	● 启用 ○ 禁用	1	
目的MAC验证:	● 启用 ○ 禁用	1	
IP验证:	● 启用 ○ 禁用	1	
使能 VLAN			
VLAN ID: Logging:	1 0 禁用 ✔	(1-4094)	启用
VLAN 配置			
选择 VLAN ID	状态	Log 状态	
	~	~	
1	启用	禁用	
10	启用	禁用	
20	启用	禁用	
30	启用	禁用	
	全选	提交帮助	

☞ 说明:

- 源 MAC 验证:当此功能开启后,ARP 防护功能会检查 ARP 报文的源 MAC 是否等于发送 MAC,如果不等则将报文丢弃,本处的发送 MAC 是四元绑定条目中对应端口的所对应的 MAC。
- 目的 MAC 验证:当此功能开启后,ARP 防护功能会检查 ARP 回复报文的目的 MAC 是否等于目标 MAC,如果不等则将报文丢,本处目标 MAC 是指这个端口所对应四元绑定条目中的MAC。
- IP 验证:当此功能开启后,ARP 防护功能会检查报文的 IP 合法性,如果 IP 字段不合法则将报 文丢弃。
- 交换机会根据四元绑定条目来匹配对应端口的 ARP 报文中的源 MAC 或者目的 MAC 是否是端口 已经绑定的 MAC,如果不是则选择丢弃。

如果用户对网络中的 ARP 报文的数量也需要控制,可以在"网络安全->ARP 防护->防 ARP 攻击"中设置端口的 ARP 报文的速率,单位 PPS,当端口收到的 ARP 报文速率高于设定值 后,该端口将会断开,需要手动在界面恢复,因此设置值需要根据实际网络中有用 ARP 的数量来定。

方ARP欺骗	防ARP攻击	报文统计					
防ARP攻击	去配置						
UNIT:	1						
选择	端口	信任	速率 (0 1-300)pp	s 限速周期(1-15)s	状态	操作	
		~					
	1/0/1	禁用	50	1			
	1/0/2	禁用	50	1			
	1/0/3	禁用	50	1			
	1/0/4	禁用	50	1			
	1/0/5	禁用	50	1			
	1/0/6	禁用	50	1			
	1/0/7	禁用	50	1			
	1/0/8	禁用	50	1			
	1/0/9	禁用	50	1			
	1/0/10	禁用	50	1			
	1/0/11	禁用	50	1			
	1/0/12	禁用	50	1			
	1/0/13	禁用	50	1			
	1/0/14	禁用	50	1			
	1/0/15	启用	15	1			•
			全选 提交	刷新 帮	助		

() 注意:

- 交换机上联口可以启用信任,这个口将放行所有的 ARP 报文,不会对数量有限制。
- 防 ARP 攻击功能需要启用对应 VLAN 才能生效,因此也需要根据四元绑定条目来匹配,如果和
 对应端口的四元绑定条目不匹配,交换机将会丢弃报文。

同时在"网络安全->ARP 防护->IP 源防护"中启用需要设置的端口 IP 源防护功能, 防护类型 选择 SIP+MAC 的方式, 上联端口 24 口一般不要启用, 因为外网回复的数据包源 IP 可能 没在四元绑定条目内导致无法上网:

UNIT:	1				
选择	端口	防护类型		LAG	
			~		
	1/0/14	SIP+MAC			
	1/0/15	SIP+MAC			
	1/0/16	SIP+MAC			
	1/0/17	SIP+MAC			
	1/0/18	SIP+MAC			
	1/0/19	SIP+MAC			
	1/0/20	SIP+MAC			
	1/0/21	SIP+MAC			
	1/0/22	SIP+MAC			
	1/0/23	SIP+MAC			
	1/0/24	禁用			
	1/0/25	SIP+MAC			
	1/0/26	SIP+MAC			
	1/0/27	SIP+MAC			
	1/0/28	SIP+MAC			-
		全选 提交	帮助		

以上即可完成只有对应终端接入到对应端口且使用对应 IP 才能上网, 保证了企业网络的安

全性。

第12章 802.1X

12.1 交换机 802.1X 认证功能配置指南

12.1.1 应用介绍

802.1X 协议作为局域网端口的接入控制机制在以太网中被广泛应用,主要解决以太网内认证和安全方面的问题。 802.1X 协议是一种基于端口的网络接入控制协议,"基于端口的网络接入控制"是指在局域网接入设备的端口这一级,对所接入的用户设备进行认证和控制。 连接在端口上的用户设备如果能通过认证,就可以访问局域网中的资源;如果不能通过认证,则无法访问局域网中的资源。

12.1.2 需求介绍

某公司为了保证数据接入的安全性,使用交换机做 802.1X 认证,只有通过登陆网络管理员 分配的员工账号才有权接入网络使用网络资源,拓扑结构如下:



图中以 TL-SG5428 做为中心交换机, 802.1X 认证服务器接在 TL-SG5428 上。所有终端 都需要通过认证之后才能访问服务器资源或者网络资源。下面将介绍实现局域网中每台设备 通过交换机的 802.1X 功能搭配 Radius 服务器实现认证接入的配置过程。

12.1.3 设置方法

第一步、搭建 Radius 认证服务器

本文以试用版的 WinRadius 做为认证服务端。(也可以在 Windows Server 上搭建 Radius 认证服务器。有关服务器的搭建方法请在网上参考相关资料)。

1、启用 Winradius,用管理员身份运行,并在"设置—数据库—自动配置 ODBC",配置数据库,数据库配置成功后再重启软件。

3/5/6/7/8 系列企业级交换机

1 20143397616851928 20143397616851928 20143397616851928 20143397616851928 1 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 20143397616851928 20143397616851928 20143397616851928 20143397616851928 3 20143397616851928 20143397616851928 20143397616851928 20143397616851928 3 20143397616851928 20143397616851928 20143397616851928 20143397616851928 3 20143397616851928 20143397616851928 20143397616851928 20143397616851928 3 20143397616851928 20143397616851928 20143397616851928 20143397616851928 3 20143397616851928 20143397616851928 20143397616851928 20143397616851928 2 2<	S WinRadius - 无标题		– 🗆 X
ID 初週 消息 1 2021年3月7日16月51923秒 加酸酸小加酸酸小和adus 以使供注意操作生改. 2 2021年3月7日16月51923秒 始建 ODSC 成功. 清整新启动 WinRadius 以使供注意操作生改. () 自力能置 ODBC () 自力能置 Statistics () 自力能置 ODBC () 自力 N 特 刷新 () 回口 () 回日 () 回日 <th></th> <th></th> <th></th>			
1 2021年3月7日105159239 加速販売加速学売 2 2021年3月7日105519239 他種 ODBC 成功, 清重新信助 WinRadius 以便知注意地听生法。 「資在 控制面積/ ODBC 中设置 FADIUS 数据库: 新型電池振星 WinFladius.mdb. 約 0000 系统 中、 加速和注意数据度活动加速的 0000 系统 中、 加速和注意、如果需要 username/password, 清输入 YourdduchametUd yourSename: FHP形号表名: 1 四日 天主, 加果需要 username/password, 清输入 YourdduckametUd yourSename: FHP形号表名: 1 町の方 1 町の方 1 町の方 1 町の方 1 町の方 1 「日方配置 0008C 1 1008C 1 日本 1 日	」		17
2 2021年3月7日16月5155230 創催 ODBC 成功, 書重新編録 WinRadius 以便完定建操作主次. ODBC 役 従 译在 控制面積 ODBC 中沿 面 和配置 ODBC 小 沿面 正 目 引起置 ODBC 一 目 引起置 A The Table T	1 2021年3月7日16时51分0秒 加载账户数据失败。		
Cobe dag (2 2021年3月7日16时51分23秒 创建 ODBC 成功,请重新启动 WinRadi	us 以便使这些操作生效。	
議在"控制面積/OBC" 中、 留計型目標 一 自动配置 ODBC ODBC名: WinRadius 注意:如果需要 username/password, 请输入 'YourOdecNameLidi-yourdsemame: P 由少urPassword'。 用户账号表名: bbogs VoIP记录表名: bbogs VoIP记录表名: bbogs WoIP记录表名: bbogs WoIP记录表名: bvoIP 每隔 0 分钟刷新一次用户信息 该数据库支持 dynaset 确定 取消		ODBC 设置 X	
就達		講在 空気画版 ODBC 中设置 FADUS 数据率、 株在型数据是本 WnEnd Fuen TV通过点 中 1 個技程把该数据库添加到您的 ODBC系统 ODBC名: WnRadius 注意、如果需要 username/password,请输入 'YourOdbcMancUld-yourDssword,请输入 'YourOdbcMancUld-yourDssword', 用 户账号表名: bUsers 计 赞记录表名: bUsers 计 赞记录表名: bUsers 计 赞记录表名: bUsers 计 赞记录表名: bUsers 计 赞记录表名: bUsers 过 惯 Users 过 惯 Users 过 赞 Users 工 赞 Users 过 赞 Users 工 赞 Users Users 工 赞 Users 工 赞 敬 Users 工 赞 敬 版 取 通	
	84134		
	94,78		数子 ///

2、软件重启成功后,配置服务器参数

认证服务器上的配置:

- 服务器 IP 地址: 192.168.111.250 (服务器 IP 需要保证与交换机 VLAN1 的接口 IP 是 可以相互通讯的,本例按照和 VLAN 1 同网段 IP 举例)
- 认证端口: 1812
- 计费端口: 1813
- 密钥: fae
- 服务器上设置用户账号密码:员工 1/123456

S WinRadius - 无标题		- 🗆 ×
操作 日志 高级 设置 查看 帮助		
D<	 	
教練 参 WinRadius - 无标题		×
操作 日志 高级 设置 查看 帮助		
1 2021年3月7日16時57分240 2 2021年3月7日16時57分240 3 2021年3月7日16時57分240 4 2021年3月7日16時57分240 4 2021年3月7日16時58份1110	Passer/報告 (以正知口)1912.1 計畫與口为1913. 新聞为fae). Winfaduli 医器種BatE機構成。(以正如口)1912.1 計畫與口为1913. 新聞为fae). (Winfaduli ETEN等 MAS 8) request 演員. 如果没有, 書位置 MAS 配置. 第四時号 第二章 第二章 第二章 第二章 第二章<	
1		
就達		

第二步、配置 TL-SG5428 的 802.1X 功能

1、802.1X 配置。在交换机的"网络安全—802.1X 认证—全局配置"界面, 启用 802.1X 全局配置功能, 认证模式选择 EAP, 其余参数本次配置选择默认。

全局配置端口配置		
操作成功。		
全局配置		
802.1X功能: 认证模式: 握手检测:	 ● 启用 ○ 禁用 EAP ✓ ● 启用 ○ 禁用 	坦六
Guest VLAN : Guest VLAN ID : 计费功能:	 ○ 启用 ● 禁用 (2-4094) ○ 启用 ● 禁用 	LEX.
认证参数配置		
静默:	○ 启用 • 禁用	
静默时长:	秒 (1-999)	捍亦
重复发送次数:	3 次 (1-9)	帮助
客户端响应招时:	6 秒 (1-9)	

2、在交换机的"网络安全—802.1X 认证—端口配置"界面,配置对应端口的 802.1X 功能。

全	局配置	端口酉	躍						
	端口配	置							
	UNIT	: 1	LAGS						
	选择	端口	状态	Guest VLAN	控制模式	控制类型	授权状态	LAG	
			~	~	~	×			
		1/0/14	启用	禁用	自动	基于MAC	已授权		*
		1/0/15	启用	禁用	自动	基于MAC	已授权		
		1/0/16	启用	禁用	自动	基于MAC	已授权		
		1/0/17	启用	禁用	自动	基于MAC	已授权		
		1/0/18	启用	禁用	自动	基于MAC	已授权		
		1/0/19	启用	禁用	自动	基于MAC	已授权		
		1/0/20	启用	禁用	自动	基于MAC	已授权		
		1/0/21	启用	禁用	自动	基于MAC	已授权		-11
		1/0/22	启用	禁用	自动	基于MAC	已授权		-11
		1/0/23	启用	禁用	自动	基于MAC	已授权		-8
	<u> </u>	1/0/24	启用	禁用	自动	基于MAC	已授权		-81
	<u> </u>	1/0/25	启用	禁用	自动	基于MAC	已授权		-81
	<u> </u>	1/0/26	启用	禁用	自动	基于MAC	已授权		-11
		1/0/27	<u> </u>	禁用	自动	基于MAC	已授权		- 11
	U	1/0/28	禁用	禁用	自动	基于MAC	已授权		∇
				全选	刷新 提交	帮助			

- ③ 说明:
- 不启用 TL-SG5428 级联端口(28 端口)的 802.1X 认证,使认证服务器在任何时候都能通过该端
 口接入网络以便认证客户端。

3/5/6/7/8 系列企业级交换机

- 配置其它需要认证的端口。(TL-SG5428 可同时支持基于 MAC 和 Port 的认证,这里均采用基于 MAC 的认证方式)。
- 如果端口的"状态"处于禁用,则该端口下的设备不需要进行认证,始终处于接入网络的状态。
- 控制类型中,"基于 MAC"意为着该端口下的所有设备必需单独进行认证,认证通过后才能接入
 网络;"基于 Port"意味着该端口下只要有一台设备认证通过,其它设备不再需要认证也能接入网络。
- 2、AAA 配置。在交换机的"网络安全—AAA—全局配置"界面,配置交换机的 AAA 认证功

能,全局配置 AAA 功能启用,以便对接 Radius 服务器。

全	局配置	方法列表	Dot1x配置	服务器组	RADIUS配置	TACACS+	
-	全局配置	三					
	AAA	A:	• 启	用 〇 禁用			提交

在交换机的"网络安全—AAA—RADIUS 配置"界面,配置交换机所对接的 Radius 服务器信

息。

全局配置	方法列表	Dot1x配置	服务器组	RADIUS配置	TACACS+			
服务器画	置							
服务	;器IP:	192.1	68.111.250	(格式:192.	168.0.1			
共享	密钥: 端口:	fae 1812		(1-65535)				
计费	端口:	1813		(1-65535)				添加
重传 超时	疢数: 时长:	2		(1-3) 秒(1-9)				
服务器列	康							
选择	服务器IP		共享密	钥	认证端口] 计费端口	重传次数	超时时长
				表格为空				
			全选	提交	删除	野助		

3、802.1X 认证客户端配置。本次以 WIN 10 电脑为例,在电脑上安装 TP-LINK 802.1X_V2.1 版客户端应用程序,配置参数默认,电脑接入交换机的端口客户端软件输入用户名账号和密 码:员工 1/123456,选择对应连接交换机的网卡,电脑通过认证即可使用网络资源。

	🐇 TP-LINK 80)2.1X 认证客户端	-	×	
		IP-LIN	IK		
	田白夕	局 工1			
	,元/ ·白· 索 孤·	******		_	
		│			
	语言:	中文		•	
	网卡:	Realtek PCIe GBE Fa	amily Controller		
	法按(0)	居此(1)	温山の		
L					
\$ WinRadius - 无标题 操作日志 诺级 设置 查看 帮助					- 🗆 X
□ ○ ○ □ 时间 1 2021年3月7日16时59分26秒 日 2021年3月7日16时59分26秒 日 2021年3月7日16日59分26秒 日 2021年3月7日16日5959分26秒 日 2021年3月7日16日5959500 日 2021年3月7日16日595950 日 2021年3月7日16日59500 日 2021年3月7日16日59500 日 2021年3月7日16日59500 日 2021年3月7日16日59500 日 2021年3月7日16日59500 日 2021年3月7日16日59500 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月7日16日5000 日 2021年3月71000 日 2021年3月71000000000000000000000000000000000000	\$ @ ? 就1个账号				
2 2021年3月7日16時59分26秒 WinRa 3 2021年3月7日16時59分26秒 WinRa 4 2021年3月7日17时27分50秒 用户债 5 2021年3月7日17时27分51秒 用户债	drus 服务器已经止侧局动,(以止诱口方 dius 正在等待 NAS 的 request 消息。数 工1)认证继续 工1)认证通过 连接状态	51812, 计费强山为1813, 密钥为18e)。 如果没有,请检查 NAS 配置。 ————————————————————————————————————			
	连接 状态:	已连接上			
	<mark>持续时间:</mark> 一活动	收到 意法			
	数据包:	17 2 断开(D) 关闭(X)			
就清					数字 //
④ 说明:					

至此 802.1X 认证接入实现完成,局域网中所有电脑需要通过认证后才能访问局域网,从而 实现了网络的安全接入。

第13章 工业级特性

13.1 ERPS 单环环网配置指南

13.1.1 应用介绍

工业环境的交换机需要保证运行的稳定性,即便出现一台设备故障 可以通过其它设备替代 运转,而且要求切换快速无延迟。工业级的 ERPS 环网即可满足这种使用场景,比一般的生 成树协议切换更快速,能做到业务的无中断切换。ERPS 环网正常工作时,RPL 端口阻塞所 在链路,防止网络环路;当环网中某条链路出现异常断开时,异常节点会发包通知 RPL Owner 节点,于是 RPL 端口放开,使所在链路恢复正常通信,保障整个网络通信不中断。 一个环网中,有且仅有一个 RPL Owner 节点。

13.1.2 需求介绍

某工业环境使用交换机组环网,保障任何一台交换机故障都不会影响业务的转发,使用 ERPS 组环网拓扑如下:



13.1.3 设置方法

1、通过拨码开关快速配置(以 TL-SG2210R 工业级为例)

TL-SG2210R 工业级交换机机身有 DIP 拨码开关,涉及到 ERPS 环网配置的有以下三个开关:

WEB:默认关闭,开启后,交换机开启 WEB 管理功能,只有开启 WEB 管理开关,才能使用 ERPS 环网功能。

ERPS:默认关闭,开启后,交换机开启 ERPS 的主环功能,并使能 RPL 开关。

RPL: 默认关闭, 开启后, 配置端口 1 为 RPL 端口。



那么对于这样一个环网拓扑:



只需做如下操作:

(1) 交换机 A 将 WEB 开关、ERPS 开关和 RPL 开关都拨到 ON;

- (2) 交换机 B、C 将 WEB 开关和 ERPS 开关拨到 ON。
- (3) 将三台交换机的端口 1、2 按照拓扑连接起来。

需要注意的是,使用拨码开关来配置环网时,只能使用端口 1、2 来组建环网,且只能配置端口 1为 RPL Owner 端口。如果需要使用其他的端口来组建环网,比如使用光口来组建光 纤环网,那么就必须采用 WEB 页面配置的方法。

2、WEB页面配置

使用 WEB 页面配置时,可以任意指定所用端口,拓扑示意如下:



角色分类: 交换机 A 为 RPL Owner 节点, 交换机 B、C 为普通节点。

交换机 A 配置

(1) 启用交换机的 802.1Q VLAN 功能

依次点击 < VLAN > → < 802.1Q VLAN >,将"802.1Q VLAN 使能"选择为开启,如下图所示:

	TP-LINK°			
TL-SG2210R <u>工业级</u>	802.1Q VLAN设置 帮助			
系统管理 系统工具 二层交换		802.1Q VLAN使能: 关闭 开启 关闭	×	应用
				新増 编辑 删除
VLAN	VLAN VLAN	VLAN描述	Tagged端口	Untagged跳□
MTU VLAN				
・端口VLAN				
• 802.1Q VLAN				
* 802.10 PVID @				
ERPS				
海山西南				
退工型來				
点击<应用>危	5,页面显示如下图	图所示:		

点击 < 应用 > 后,页面显示如下图所示:

	TP-LINK°			
TL-SG2210R <u>工业级</u>	802.1Q VLAN设置 帮助			
系统工具		802.1Q VLAN使能:	*	应用
二层交换				
<u> </u>				新増 編輯 剷除
VLAN	VLAN VLAN	VLAN描述	Tagged)第日	Untagged)编□
MTU VLAN	1	Default		1-10
・鎊□VLAN				
- 802.1Q VLAN				
- 802.1Q PVID设置				
ERPS				
退出登录				

(2) 配置环网保护实例

依次点击<ERPS>→<ERPS 实例>,勾选一个实例,然后点击<设置>,如下图所示:

	TP-LINK [®]	
TL-SG2210R <u>工业级</u>	ERPS实例配置 ^{影动}	
系统工具 二层交换 监控	● (二) (二) (二) (二) (二) (二) (二) (二)	VLANID
VLAN ERPS ·ERPS配置	3 4 5 6	
・ERPS実制 退出整束	7 8	a.

点击<设置>后,填写需要保护的 VLAN,要同时包含数据 VLAN 和协议 VLAN,此处数据

VLAN 为 1, 预设协议 VLAN 为 2, 如下图所示:

	TP-LINI	<°			
TL-8G2210R <u>工业级</u>	ERPS实例配置 ^{设置} 海除	Rh .			
系统工具 二层交换	 一 实例ID ▼ 1 	实例配置		×	
监控 VLAN	2	成例D: 1 VLAN ID: 1-2	(1-8) (1-4094,格式1,4-7)		
ERPS · ERPS配置	□ 4 □ 5 □ 6			确认	
·ERPS实例	7 8				
退出登录					

点击<确认>后,页面显示如下图所示:

-	TP-LINK [®]		
TL-SG2210R工业级 系统管理	ERP S 实例 配置 ^{帮助} 设置 滴除		
<u>新统工具</u>	一 实例ID	VLAN ID	
二层交换	1	1-2	
[[2]]	2	200	
VLAN	□ 3 □ 4		
ERPS	5		
・ERPS配置	6		
. EUL 35603	7		
通出登录	8		

这里,就完成了保护实例的配置,需要注意的是,设置的 VLAN ID 范围,需要包含所有数据 VLAN 和协议 VLAN,比如数据通信用到了 VLAN 1-5, TP 环的协议 VLAN 设置为 10, 那么这里 VLAN ID 范围可以设置为 1-10。协议 VLAN 在 ERPS 环配置中会用到。

(3) 配置 ERPS 环

环配置:

依次点击<ERPS>→<ERPS 配置>,然后点击<创建>,如下图所示:

	TP-LINK [®]
TL-SG2210R工业级 系统管理 系统工具 二层交换 监控	环列表 幣物 注意: 以下设置時号版ERPS版研并关先效: 1. 已配置环、 2. 开启MTU VLAN、 3. 开启第ロVLAN(除VLAN(除VLAN(以外))。 按證 傳過 第ロ 勤除 恢复
VLAN ERPS	□ 获号 环绕型 角色 协议VLAN 版本 回切 左跳口 左跳口转发状态 石湖口 右跳口转发状态 状态
- ERPS配置 - ERPS实例 退出整荣	

点击<创建>后,配置"环号"、"协议 VLAN"、"保护实例",如下图所示:

	TP-LINK°				
TL-SG2210R工业级	环列表 帮助				
系统管理	注意:				
系统工具	以下设置将导致ERPS拨码开关失效: 1 PPP型				
二层交换	2. 开启MT 外配置			×	
监控	3、开启调: 环号:	1	(1-8)	环号这里设置为1	(注口) #69e (行知
VLAN	一 环号 描述:		(0-16个字符)		
ERPS	版本:	V2 ×			
·ERPS配置	环类型:	主环			
・ERPS实例	回切:	开启 👻			
	协议VLAN:	2	(1-4094)	协议VLAN不与数据VLAN冲突	即可,这里设置为2
退出登录	保护实例:	1 *		填写前面设置过的保护实例编	号,这里设置为1
	通知环:	~			
	周期 :		(1-600秒)		
	國值:		(1-255)		
	WTR定时器:	5	(1-12分钟)		
	Guard定时器 :	200	(1-200厘秒)		
	Hold定时器:	0	(0-100分秒)		
				浙认	

点击<确认>后,页面显示如下图所示:

	TP-LI	NK [.]									
TL-SG2210R <u>工业级</u> 系统管理 系统工具 二层交换	环列表 構成 注意: 以下设置将导致 1、已配置环。 2、开启MTUN	t DERPS拨码开关失效: /LAN,									
监控	3、 升启调口V	LAN并配置VLAN(除VLAN	11281).				(1) (1)		辑 第日	創除	恢复
VLAN	□ 环号	环模型 角色	协议VLAN	版本	回切	左端口	左端口转发状态	右端口	右端口转发状态	状态	
ERPS	1	主环 Normal	2	V2	开启	断开	转发	断开	转发	PENDING	
- ERPS获例 退出登录											

左右端口配置:

点击上图中红框标出的<端口>,进入左右端口配置,将端口7设置为 RPL Owner,将端口

8 设置为 Normal,如下图所示:

	TP-LINK [®]		
TL-SG2210R工业线 系统管理 原始工具 二层交換 这些 VLAN ERPS ·ERPS監護 ·ERPS素例 退出要求	研究者 新助 1: 以下の回路局券数ERPS版用并关先效: 1: 已起至床。 2: 开始ITU VLAN. 3: 开始原因VLAN+相互型VLAN (BM/LAN 152)+ 図 环号 环境型 角色 図 1 主环 Normal	株口配置 > 环号:1 芝油:2 28月 第二:7 角色:8 第二:8 角色:10000 御録:2 ※ ※	

点击<确认>,则完成了左右端口配置。

到这里,就完成了对交换机 A 的配置。

交换机 B.C 配置

交换机 B、C 与交换机 A 的唯一区别就是, B 和 C 不需要设置 RPL Owner。也就是说, 除了最后的左右端口配置, A、B、C 的其他所有配置都相同。

那么同样的, 交换机 B、C 也需要做如下配置:

A. 启用交换机的 802.1Q VLAN 功能

同交换机 A

B. 配置环网保护实例

同交换机 A

C. 配置 ERPS 环

环配置:

同交换机 A

左右端口配置:

左右端口的角色均选择为 Normal 即可,如下图所示:

3/5/6/7/8 系列企业级交换机

	TP-LINK [®]
TL-SG2210R工业级	环列表 帮助
系统管理	注意:
系统工具	以下设置将导致ERPS拨码开关先效: 1. 已配置环。
二层交换	2. TRIMTU VLAN, VALUE X
监控	3、 开始例LIVLAN(REVLAN (REVLAN 10.09 环号:1 的鍵 編編 第日 影除 佐族
VLAN	◎ 环号 环类型 角色 左端口: ◎ 启用 口转发状态 右端口 右端口转发状态 状态
ERPS	図 1 主环 Normal 第日:7 断开 经序 PROTECTION
·ERPS配置	角色: Normal
・ERPS实例	020 : ···· ··· ··· ··· ··· ··· ··· ··· ···
100.01.070.000	右調曰: 図启用 将端口7、8均设置为Normal
退出登录	P#□: 8
	角色: Normal ~
	明時:
	- 1496 J

到这里就完成了对交换机 B、C 的配置。

配置完成后,将三台交换机按照设定的端口两两连接起来,就组建好了一个环网。这种单环 网络在实际应用中最为常见,配置起来也比较简单,对于具有 N 个节点的单环网络,只需 配置 1 个 RPL Owner 节点和 N-1 个普通节点即可。

13.2 TP-RING 单环环网配置指南

13.2.1 应用介绍

TL-SG5412 工业级新增了 TP-RING 功能,受到客户的广泛关注。TP-RING 是 TP-LINK 研 发的环网协议,支持单环、多环组网,支持快速环网(故障自愈时间<20ms),在实现链路 冗余备份的同时,有效避免网络环路、广播风暴等现象,保护工作数据,提高网络可靠性。 正常工作时,RPL 端口阻塞所在链路,防止网络环路;当环网中某条链路出现异常断开时, 异常节点会发包通知 RPL Owner 节点,于是 RPL 端口放开,使所在链路恢复正常通信,保 障整个网络通信不中断。一个环网中,有且仅有一个 RPL Owner 节点

13.2.2 需求介绍

某工业环境使用交换机组环网,保障任何一台交换机故障都不会影响业务的转发,使用 ERPS 组环网拓扑如下:



13.2.3 设置方法

1、通过拨码开关快速配置(以TL-SG5412工业级为例)

TL-SG5412 工业级交换机有两个拨码开关:

TP-RING:默认关闭,开启后,交换机开启 TP-RING 的主环功能,并使能 RPL 开关。

RPL:默认关闭,开启后,配置端口1为RPL端口。

3/5/6/7/8 系列企业级交换机

POWER INPUTS: 12V/24V/48V		3 8 6 1	•
	5 FAULT V2+ PWR2 V2-	OFF ON	TP-RING RPL

那么对于这样一个环网拓扑:



只需做如下操作:

- (1) 交换机 A 将 TP-RING 开关和 RPL 开关都拨到 ON;
- (2) 交换机 B、C 将 TP-RING 开关拨到 ON。
- (3) 将三台交换机的端口 1、2 按照拓扑连接起来。

需要注意的是,使用拨码开关来配置环网时,只能使用端口 1、2 来组建环网,且只能配置端口 1为 RPL Owner 端口。如果需要使用其他的端口来组建环网,比如使用光口来组建光 纤环网,那么就必须采用 WEB 页面配置的方法。

2、WEB页面配置

使用 WEB 页面配置时,可以任意指定所用端口,拓扑示意如下:



角色分类: 交换机 A 为 RPL Owner 节点, 交换机 B、C 为普通节点。

3/5/6/7/8 系列企业级交换机

交换机 A 配置

(1) 配置相应端口类型为 TRUNK

依次点击 < VLAN > → < 802.1Q VLAN > → < 端口配置 > ,选中 7、8两个端口,选择端口类型为 TRUNK,如下图所示:

TP-LINK						
			700			
TL-SG5412 <u>工业级</u>		》 第二日	011			
	-					
	VLAN	满口配置				
系统管理	UNI	: 1	LAGS			
二层交换	选择	端口	端口类型	PVID	LAG	所属VLAN
VLAN			TRUNK 🗸			
• 802.1Q VLAN		1/0/1		1		查询
MAC VLAN		1/0/2	ACCESS	1		查询
•协议VLAN		1/0/3	TRUNK	1		查询
VLAN VPN		1/0/4	GENERAL	1		查询
• GVRP		1/0/5	ACCESS	1		查询
Private VLAN		1/0/6	ACCESS	1		查询
生成树		1/0/7	ACCESS	1		查询
1P5本		1/0/8	ACCESS	1		查询
古容츎配宣		1/0/9	ACCESS	1		查询
时间同步		1/0/10	ACCESS	1		查询
		1/0/11	ACCESS	1		查询
路由功能		1/0/12	ACCESS	1		查询
服务质量					≠s.Bh	
访问控制			主应	iteX	THE AU	
网络安全						
SNMP						
LLDP						
系统维护						
配置保存						
索引页面						
退出登录						

点击<提交>后,页面显示如下图所示:

- 3/5/6/7/8 系列企业级交换机 -

IP-LINK						
The second State	VI AN 配置	端口配	8			
1L-SG5412 <u>工业政</u>	操作成	功.				
	VLAN					
系统管理	UNIT	: 1 L	AGS			
	选择	端口	端口类型	PVID	LAG	所属VLAN
VLAN			~			
• 802.1Q VLAN		1/0/1	ACCESS	1		查询
MAC VLAN		1/0/2	ACCESS	1		查询
•协议VLAN		1/0/3	ACCESS	1		查询
VLAN VPN OVPP		1/0/4	ACCESS	1		查询
GVRP Private VLAN		1/0/5	ACCESS	1		查询
		1/0/6	ACCESS	1		查询
тръ		1/0/7	TRUNK	1		查询
		1/0/8	TRUNK	1		查询
时间同步		1/0/9	ACCESS	1		查询
		1/0/10	ACCESS	1		查询
		1/0/11	ACCESS	1		查询
服务质量		1/0/12	ACCESS	1		查询
			全选	提交	帮助	
SNMP						
LLDP						
系统维护						
配置保存						
索引页面						
退出登录						

(2) 配置环网保护实例

依次点击<生成树>→<MSTP 实例>→<实例配置>,设置实例 ID,本例设置为 1,设置 需要保护的 VLAN 范围,本例设置为 1-20,如下图所示:

TP-LINK							
TL-SG5412	域配置	实例配置	实例端口				
		rth /pint of					
マゴムナ ANK III	VLAIN	头的脉制					
	实	例ID:	1		(0-8,0代表CIST)		添加
VIAN	v	AN ID :	1-20)	(1-4094, 格式: 1.3.4-7	11-30)	删除
生成树							
 基本配置 	实例面	置					
・端口配置	选择	实例ID	状态	优先级	VLAN ID		
・MSTP实例							
・安全配置		CIST	禁用	32768	1-4094,	显示全部映射	清除全部映射
TP环		1	禁用	32768		显示全部映射	清除全部映射
告答器配置		2	禁用	32768		显示全部映射	清除全部映射
时间同步		3	禁用	32768		显示全部映射	清除全部映射
组播管理		4	禁用	32768		显示全部映射	清除全部映射
路由功能		5	禁用	32768		显示全部映射	清除全部映射
服务质量		6	禁用	32768		显示全部映射	清除全部映射
访问控制		7	禁用	32768		显示全部映射	清除全部映射
网络安全		8	禁用	32768		显示全部映射	清除全部映射
SNMP					提交帮助		
LLDP	_						
系効理护 ————————————————————————————————————	注意:						
	当有VL	AN ID映射到	某个实例时	(CIST除外),	,这个实例会自动启用。		
很出登录							

点击<添加>后,页面显示如下图所示:

TP-LINK							
	1-027100						
T-SG5412 工业级	域配置	买例配置	实例病日				
		rin Inina Aak					
and the auto TBI	VLAN	头例跌別					
系统官理	实	例ID:			(0-8,0代表CIST)		添加
	V	AN ID :			(1-4094、格式:134-	7 11-30)	删除
生成树					(14034, 1020, 1,3,4	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	and a
 基本配置 	实例直	置					
・端口配置	选择	实例ID	状态	优先级	VLAN ID		
 MSTP実例 							
 安全配置 		CIST	禁用	32768	21-4094,	显示全部映射	清除全部映射
TP环		1	启用	32768	1-20,	显示全部映射	清除全部映射
告警器配置		2	禁用	32768		显示全部映射	清除全部映射
时间同步		3	禁用	32768		显示全部映射	清除全部映射
组播管理		4	禁用	32768		显示全部映射	1 清除全部映射
路田切能		5	禁用	32768		显示全部映射	1 清除全部映射
版务质基		6	禁用	32768		显示全部映射	1 清除全部映射
			禁用	32768		显示全部映射	1 清除全部映射
SNMP		8	禁用	32708		显示主部映象	「」清除主部映射
					提交帮助		
 配置保存	注意:						
索引页面	当有VL	.AN ID映射到	某个实例时	(CIST除外),	这个实例会自动启用。		
退出登录							

这里,就完成了保护实例的配置,需要注意的是,设置的 VLAN ID 范围,需要包含所有数据 VLAN 和协议 VLAN,比如数据通信用到了 VLAN 1-5, TP 环的协议 VLAN 设置为 10, 那么这里 VLAN ID 范围可以设置为 1-10。协议 VLAN 在 TP 环配置中会讲到。

(3) 配置 ERPS 环

环配置:

依次点击<TP 环>→<环配置>→<全局配置>,如下图所示:

配置好红框标出的项目,其他参数留空或者保持默认即可。

TP-LINK					
TL-SG5412	全局配置				
	环配置				
系统管理	环号:	1 (1-8) 环号	这里设置为1	
二层交换	描述:				
VLAN the children	版本:	V2 ~			
王成149 TP环	环举型:	主环			
 环配置 	回切:	王启			
告警器配置	1997. (赤沢)/L AN -	10 (1-4094) +++		而
时间同步		(
组播管理	保护实例:	1 (1-3,4) 填写	前面创建的保护实例编号,	
路由功能	通知环:	(1-3,4)		清除
服务质量	周期:	(1-600秒)		
访问控制 	阈值:	(1-255)		
	虑通道:	关闭			
	WTR 完时器·	(1-12分钟)		
系统维护	0		1 000 (751)		
配置保存	Gualozen) as:	(1-200/里代》)		
索引页面	Hold 定时器:	(0-100分秒)		
	环列表				
退出登录	法终 环岛 环光刑	66 协议 · 新本 回切	医海道 左端日		据 /元
		VLAN NKAA LAND	主投 4次	1002	Jake 1 (*
			夜情/分全。	(to 5)	
		全边	割除	帮助	
	注意:				
	请先在生成树-MSTP页面配	置保护实例的对应VLAN范围。			

点击<创建>后,如下图所示:

点击<创建>后,	如下图所示:		>
TP-LINK [®]			
TL-SG5412	全局配置		
	环配置		
系统管理	环号:	(1-8)	
二层交换	描述:		
	版本:	V2 v	
TP环	环类型:	主环 🗸	
・环配置	回切:	开启	
告警器配置	协议VLAN:	(1-4094)	
町旧同步 	保护实例:	(1-3,4)	创建
	通知环:	(1-3,4)	清除
服务质量	周期:	(1-600秒)	
访问控制	诫值:	(1-255)	
网络安全 	店通道:	关闭	
LLDP	WTR定时器:	(1-12分钟)	
	Guard定时器:	(1-200厘秒)	
配置保存	Hold 完时器:	(0-100分钟)	
索引页面	Hold XENJER.		
退出登录	环列表		
	选择 环号 环类型	加议 版本 回切 広通道 左端口 右端口 状态	操作
	□ 1 主环	NORMAL 10 2 开启 关闭 PENDING	编辑 端口 恢复
		全选 删除 帮助	
	注意:		
	请先在生成树-MSTP页面面	置保护实例的对应VLAN范围。	

左右端口配置:

点击下图中红框标出的<端口>:

- 3/5/6/7/8 系列企业级交换机 -

TP-LINK [®]			
TL-SG5412	全局配置		
	环配置		
系统管理	环号:	(1-8)	
	描述:		
VLAN 在成树	版本:	V2 🗸	
	环类型:	主环	
・环配置	回切:	开启 🗸	
告警器配置	协议VLAN:	(1-4094)	
时间同步	(R·拉克)例。	(1.3.4)	
组播管理		(1-3,4)	
路田切能	1世大山北下:	(1-3,4)	「清除」
加方贝里 	周期:	(1-600秒)	
	阈值:	(1-255)	
SNMP	虚通道:	关闭	
LLDP	WTR定时器:	(1-12分钟)	
系统维护	Guard定时器:	(1-200厘秒)	
配置保存	Hold 定时器:	(0-100分秒)	
索引页面	TOTO ALCOUNT	(0.003(5))	
退中禁患	环列表		
	选择 环号 环类型	角色 が议版本 回切 虚通道 左端口 右端口 状	态 操作
	□ 1 主环	NORMAL 10 2 开启 关闭 PEN	DING 编辑 端口 恢复
		全选 删除 帮助	
	注意:		
	请先在生成树-MSTP页面	配置保护实例的对应VLAN范围。	

进入左右端口配置,将端口7配置为RPL Owner,如下图所示:

TP-LINK [®]	
TL-SG5412 <u>工业级</u>	全局配置
	续口配置:
系统管理	环号: 1
	☑ 左端口
	[第日: 1/0/7
	曲· BPL Owner · · · · · · · · · · · · · · · · · · ·
 环配置 	
告警器配置	
时间同步	
组播管理	端口: 1/0/8 端口8配置为Normal
路由功能	角色: Vormal V
服务质量	倒换: 🗸
近回控制 网络中全	
SNMP	提交」 返回
LLDP	
系统维护	
配置保存	
索引页面	
退出登录	

点击<提交>,则完成了左右端口配置。

到这里,就完成了对交换机 A 的配置,别忘了点击 < 配置保存 >。

交换机 B.C 配置

交换机 B、C 与交换机 A 的唯一区别就是, B 和 C 不需要设置 RPL Owner。也就是说, 除 了最后的左右端口配置, A、B、C 的其他所有配置都相同。

那么同样的, 交换机 B、C 也需要做如下配置:

(1) 配置相应端口为 TRUNK

同交换机 A

(2) 配置环网保护实例

同交换机 A

- (3) 配置 TP 环
- 1) 环配置:

同交换机 A

2) 左右端口配置:

左右端口的角色均选择为 Normal 即可。

3/5/6/7/8 系列企业级交换机

TP-LINK [®]	
TL-SG5412 工业级 系统管理 二层交换 VLAN 生成树 TP环 • 环配置 音響翻配置 时间同步	全局配置
は 描書 語曲功能 服务质量 访问控制 网络安全 SNMP LDP 系统維护 系统維护 配置保存	端□: 1/0/8 角色: Normal 例换:
<u>素引页面</u> 退出登录	

到这里就完成了对交换机 B、C 的配置。

配置完成后,将三台交换机按照设定的端口两两连接起来,就组建好了一个环网。这种单环 网络在实际应用中最为常见,配置起来也比较简单,对于具有 N 个节点的单环网络,只需 配置 1 个 RPL Owner 节点和 N-1 个普通节点即可。

第14章 其它功能

14.1 三层网管交换机连云配置指南

14.1.1 应用介绍

TP-LINK 全新推出的三层网管交换机都支持连接 TP-LINK 商用网络云平台,通过将设备上云,用户可以在云平台上针对交换机做一些远程操作,减少运维成本,非常方便。目前具体支持的机型可见链接:<u>https://www.tp-link.com.cn/act-smbcloud-devices2</u>

本文介绍三层网管交换机连接商云的配置方法。

14.1.2 需求介绍

某公司三层网管交换机需要连接商用网络云平台,通过云平台管理。

14.1.3 设置方法

在交换机界面,点击"路由功能"-"接口",配置交换机设备 VLAN1(管理 VLAN,即对接前端路由器的 VLAN)的接口 IP 地址,使接口 IP 地址和前端路由器地址在同一个网段:

- 3/5/6/7/8 系列企业级交换机 -

TP-LINK [®]		
TL-SG5210PE	接口设置	
系统管理 二层交换 VLAN 生成网 组播管理 路由功能 • 投口 • 路由表	修改接口 接口ID: Vlan1 IP地址模式: ○ None ⑥ Static ○ DHCP ○ BOOTP IP地址: 192.168.111.210 IP地址: 192.168.111.210 子网獲码: 1255.255.255.0 管理状态: 开启 ▼ 接口名称: (佰式: 116字符)	修改 返回
・静态路由 ・DHCP服务器 ・DHCP中继 ・代理ARP ・ARP	创建第二IP IP地址: (格式: 192.168.0.1) 子网掩码: (格式: 255.255.255.0)	创建
・RIP 服务质量 PoE 访问控制 网络安全 SNMP	第二IP列表 子网掩码 选择 IP地址 子网掩码 表指为空。 全选 删除 返回 報助	

点击"系统配置"-"DNS 配置",确认设备的 DNS 服务器地址填写正确,交换机默认填写了两

条 DNS 地址:

TP-LINK °	
TL-SG5210PE	系统信息 设备描述 系统时间 夏令时 DNS配置
	服务器配置
系统管理 • 系统配置	服务器IP地址: (格式: 192.168.0.10) 添加
 ・用户管理 ・系体工具 	
・ <u>永</u> 筑 上兵 ・ 安全管理	选择 IP地址
• <u>云管理</u> 二层交换	
VLAN 生成树	
14.4.4.5 14.4.4.5.2.5.1.5.1.5.1.5.1.5.1.5.1.5.1.5.1.5.1	
路由功能 服务质量	DNS服务器条目数: 2

点击"系统管理"-"云管理", 启用交换机的云管理功能, 并选择 TP-LINK 商云管理:

TP-LINK [®]		
TL-SG5210PE	全局配置	
	全局配置	
系统管理	全局开关	
 系統配置 用户管理 	● 启用	
・系统工具		保存配置
・安全管理		导入配置 浏览 未洗择文件。
 · 云管理 	- 194713	
		□ 恢复工/
		提交 帮助
点击"路由功能"-"静态路由",配置一条全 0 的静态路由下一跳指向前端路由器 LAN 接口:

TP-LINK [®]		
TL-SG5210PE	IPv4静态路由条目 IPv6静态路由条目	
	静态路由配置	
系统管理 	目的地址: (格式: 10.10.10.0)	
VLAN	子网掩码: (格式: 255.255.255.0)	
生成树	下一跳地址: (格式: 192.168.0.2)	
组播管理 	管理距离: (可选。范围: 1-255)	
• 接口	趋大败山久日	
・路由表		
• 静态路由		
• DHCP服务器	0.0.0 0.0.0 192.168.111.1 1 0	
・DHCP中継 ・代理ARP	▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
• RIP		

点击"系统维护"-"网络诊断"-"Ping 检测",检查设备是否可以正常联网,一般 Ping DNS 服

务器:

TP-LINK°	
TL-SG5210PE	Ping 检测 Tracert 检测
系统管理 二层交换 VLAN 生成树 组播管理 路由功能 服务质量	Ping 检测 目标IP地址: 114.114.114 发送次数: 4 次 (1-10) 发送报文长度: 64 字节 (1-1500) 时间间隔: 1000 室秒 (100-1000)
PoE 访问控制 网络安全 SNMP LLDP 系统维护	Ping 结果 Pinging 114.114.114.114.ith 64 bytes of data : Reply from 114.114.114.114.ith 64 bytes = 64 time=40ms TTL=67 Reply from 114.114.114.114.ith bytes=64 time=40ms TTL=87 Reply from 114.114.114.114.ith bytes=64 time=40ms TTL=90 Reply from 114.114.114.114.ith bytes=64 time=30ms TTL=62
・系統日志 ・系統诊断 ・网络诊断 配置保存 素引页面	Ping statistics for : Packets: Sent = 4 , Received = 4 , Lost = 0 (0% loss): Approximate round trip times in milli-seconds: Minimum = 30ms , Maximum = 40ms , Average = 37ms

登陆 TP-LINK 商用网络云平台: <u>https://smbcloud.tp-link.com.cn/</u>,登陆 TP-LINK ID 账 号,点击"设备列表"-"添加设备",设备上云后即可在列表中看到并且可以远程管理:

添加设备		>
请确认项目中的设备都已接入互联网,再添加设 设备包括路由器、交换机、网桥、AC和FAT AP(FIT AP无	备。 	
* MAC地站	54-A7-03	
设备名称	TL-SG5210PE	┛交换机MAC
 请輸入设备石 (网桥设备用户: 失败)。 	E本地web管理界面中的用户各和密码,在添加设备时用于验证 名统一输入admin,并确保各设备不存在IP冲突情况,以避免连云	
* 用户名	admin	
* 密码	•••••	交换机的登录名和密码
分组	测试 ~	
		重添加 添加

至此,设备已经可以正常上云,点击远程管理即可管理设备。

设备信息	网络设备射	濒信息	网桥设备射频	信息								
≡ 内容	删除设备	修改分组	重启 升级	LED设置	导出设备信息	刷新				Q	筛选 丶	•
设备名称 ↓	设备分组	设备类型↓	工作模式 ♭	设备状态↓	设备型号↓	IP地址 ↓	MAC地址 🖡	LED状态	关联设备	▶ 操作		
TL-SG3452	测试	L2交换机		 在线 	TL-SG3452	192.168.111.250	64-6E-97			远程管理	重启	升级
TL-SG5210PE	测试	L3交换机		●在线	TL-SG5210PE	192.168.111.210	54-A7-03.			远程管理	重启	升级

14.2 二层 Web 网管交换机连云配置指南

14.2.1 应用介绍

TP-LINK 新出的 3 系列交换机都支持连接 TP-LINK 商用网络云平台,通过将设备上云,用 户可以在云平台上针对交换机做一些远程操作,减少运维成本,非常方便。目前具体支持的 机型可见链接: https://www.tp-link.com.cn/act-smbcloud-devices2

本文介绍3系列交换机连接商云的配置方法。

14.2.2 需求介绍

某公司二层网管交换机需要连接商用网络云平台,通过云平台管理。

14.2.3 设置方法

在交换机界面,点击"系统配置"-"管理 IP",配置交换机设备的 IP 地址和默认网关:

TP-LINK °				
TL-SG3452	系统信息 设备描述	系统时间 夏令时	管理IP 管理IPv6 DNS配置	
	管理VLAN			
 系统管理 ・系统配置 ・用户管理 ・系统工具 ・安全管理 ・云管理 二层交換 VLAN 	管理VLAN: [IP地址模式: IP地址: [子网掩码: [默认网关: [1 DHCP Static DHCP 192.168.111.250 255.255.255.0 192.168.111.1	(VLAN ID: 1-4094) ○ BOOTP 添加设备管理1 ^{98.168.0.1)} (指式: 255.255.255.0) 添加设备的网关地址	移改
生成树 组播管理	注意: IP地址的变更可能	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	网般。

点击"系统配置"-"DNS 配置", 确认设备的 DNS 服务器地址填写正确, 交换机默认填写了两条 DNS 地址:

- 3/5/6/7/8 系列企业级交换机 -

TP-LINK [®]											
TL-SG3452	系统信息	设备描述	系统时间	夏令时	管理IP	管理IPv6	DNS配置				
	服务器配置	2									
系统管理											
・系统配置	服务器	剖P地址:			(格式:	192.168.0.10))				添加
・用户管理		-						_			
 系统工具 	服务蓄杀日	3									
· 安全管理	选择					IP均	也址				
 云管理 											
						8.8	.8.8				
VLAN						114.114	.114.114				
生成树					全洗	删除	製助				
组播管理								默	认已有自	匀DNS月	B 务器地址
服务质量	DNS服务器	<u>冬日数:</u> 2									
访问控制											

点击"系统管理"-"云管理", 启用交换机的云管理功能, 并选择 TP-LINK 商云管理:

TP-LINK°		
TL-SG3452	全局配置	
	全局配置	
系统管理 • 系统配置	云管理:	
 ・用户管理 		保存配置
 系統工具 安全管理 	云类型:	TP-LINK商用网络云平台 🗸 🛛 导入配置 浏览… 未选择文件。
 、 云管理 		
二层交换		提交 帮助
生成例 	注意	
	1、开启云管理可能会	☆使部分配置被修改,建议在开启前将配置导出。
	2、导入配置后会覆盖	显当前启动配置文件,交换机将重启以使之生效。 The shakes manager and the shakes and
	3、设置软件恢复出)	后,交换机配置将恢复成出厂默认状态,所有用户配置数据将丢失,交换机将重启以使之生效。 5.4 JUN ATTERA 2. 天中工艺大
SNMP	4、云官埋相天配重4	>会囚刀配宣守人里后而更成。

点击"系统维护"-"网络诊断"-"Ping 检测",检查设备是否可以正常联网,一般 Ping DNS 服

务器:

TP-LINK [®]		
TL-SG3452	Ping 检测 Tracert 检测	
	Ping 检测	
系统管理 	目标P地址: 114.114.114	
VLAN	发送次数: 4 次 (1-10)	Ping
生成树	发送报文长度: 64 字节 (1-1500)	帮助
组播管理 	时间间隔: 1000 室秒 (100-1000)	
网络安全	Ping 结果	
SNMP	Pinging 114.114.114.114 with 64 bytes of data :	
LLDP	Reply from 114.114.114.114 : bytes=64 time=80ms TTL=86	
系统维护	Reply from 114.114.114.114 : bytes=64 time=50ms TTL=91	
・运行状态	Reply from 114.114.114.114 : bytes=64 time=50ms TTL=70	
・系统日志	Reply from 114.114.114.114 : bytes=64 time=60ms TTL=89	
 系統诊断 		
 网络诊断 	Ping statistics for :	
	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss):	
索引页面	Approximate round trip times in milli-seconds:	
海山委員	Minimum = 50ms , Maximum = 80ms , Average = 60ms	
返出豆求		

登陆 TP-LINK 商用网络云平台: https://smbcloud.tp-link.com.cn/,登陆 TP-LINK ID 账

号,点击"设备列表"-"添加设备",设备上云后即可在列表中看到并且可以远程管理:

添加设备					×
清确认项目中的设备都已接入互联网,再 设备包括路由器、交换机、网桥、AC和FAT AP(添加设备。 FIT AP无需手动	<mark>查看支持机型</mark> 动添加,添加完AC后,系统·	会自动识别并添加关联的FI	T AP)	
* M	AC地址 64-	-6E-97-	交换机的MAC		
ž	诸名称 TL-	-SG3452			
• 请辑 (网桥· 失败),	俞入设备在本地W 设备用户名统一。	web管理界面中的用户名和。 -输入admin,并确保各设备	密码,在添加设备时用于验 不存在IP冲突情况,以避免	证 B连云	
	用户名 adr	min			
	* 密码 🛛 🐽	•••		ø	登陆交换机的用户名和
	分组测试	đ		~	密码
				批重	添加 添加

至此,设备已经可以正常上云,点击远程管理即可管理设备。

设备列表		
📙 路由器: 0 ● 运行正常	━ 交換机:1 • 运行正常	添加设备
所有设备	设备信息 网络设备别频信息 网桥设备别频信息	
设备分组 /		
٩	■ 内容 副除设备 修改分组 重启 升级 LED设置 导出设备信息 刷新 名称,型号,IP,MAC	Q 筛选 >
▶ 测试	设备名称 / 设备分组 设备类型 / 工作模式 / 设备状态 / 设备型号 / IP地址 / MAC地址 / LED状态 关联设备 / 推	曩作
	TL-SG3452 测试 L2交换机 ●在线 TL-SG3452 192.168.111.250 64-6E-97 注	远程管理 重启 升级 纵
	共计1条 第1/1页 已选:0 1090页 ∨ K < 1 > ×	前往第页