RDS800-C 工业级交换机

用户手册

2021 年 7 月 6 日

厦 门 人 达 科 技 有 限 公 司
Xiamen Renda Technology Co., Ltd
地址：厦门市集美区软件园三期 B 区 B10 栋 13 层
电话：0592-6158928
网址：www.renda-tech.com

图形界面格式约定

格式	意义
< >	尖括号中的文字表示为按钮名，如单击<修改>按钮
【】	引号中的文字表示为窗口名、菜单名，如打开【快速上网向导】页面
--	简单的操作步骤连接符，如依次打开[开始]--[控制面板]--[网络连接]
《》	书名号中的内容表示为文章中的章节名称，请查看下一章《4.2 基本设置》

各类标志的约定

本手册中我们采用了各种醒目的标志来表示在操作过程中需要特别注意的地方，这些标 志的意义如下：

格式	意义
	警告、注意：提醒操作过程中需要注意的事项
	说明、提示：对操作内容的描述进行必要的补充和说明，有助于您避免重复一个常见的错误。

手册图文参数约定

手册中配有插图、图片界面及相关参数，这些元素主要是为正确配置和使用产品提供参 考。实际产品的配置及使用可能会稍有差别，请根据实际情况配置产品。

目 录

1 产品简介

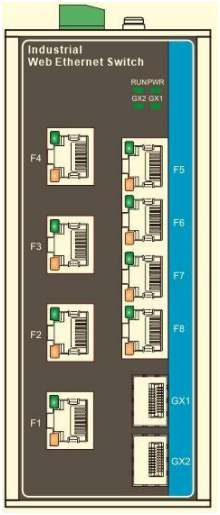
1.1 产品概述

RDS800-C交换机是安全型可网管交换机，含有2个千兆SFP光口，8个百兆电口，2个RS232接 口，是本公司为满足中小型企业高安全、高智能的接入网络研发设计的，也可用作小区、校 园等园区网络的二层可管理楼道接入交换机。完善的安全机制能够抵御层出不穷的网络恶意 攻击，将安全隐患拒之门外。强大的QOS功能，满足园区网多业务融合的需求，并批量实现网络资源灵活分配和调度，提高网络设备的业务扩展能力。本系列交换机既满足高性能接 入的需求，又提供了更全面的安全接入策略和更具易用性的网络管理维护，为用户提供了更 便捷、更安全、更可靠的解决方案。

1.2 产品外观

1.2.1 前面板说明

前面板：一个系统灯（RUN）、一个电源灯（PWR）、link/act 灯、一个 reset（RST）按钮、8 个 100M 电口和 2 个 1000M 光口，如下图所示：



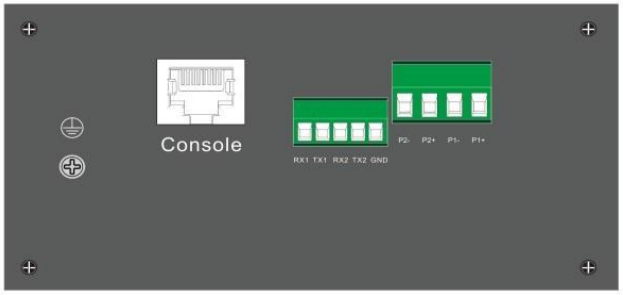
注意：管理 IP 地址为：**192.168.2.1**，子网掩码为：**255.255.255.0**，用户名为：**admin**， 密码为：**admin**。

1.2.2 指示灯说明

英文名称	颜色	状态	描述
SPEED	绿色	亮	端口 100Mbit/连接
		不亮	端口 10M 或端口未连接
ACT	黄色	闪	端口正常连接后指示灯状态为规律地闪烁
		亮	端口正常连接
		不亮	端口未连接
POWER	绿色	恒亮	指示灯恒亮表示设备已经正常启动
SYS	绿色	闪	系统正常启动后指示灯状态为规律地闪烁

1.2.3 上面板说明

上面板有电源插座，如下图所示：



2 安装前的准备

2.1 安全注意事项

为避免使用不当造成设备损坏及对人身的伤害，请遵从以下的注意事项：

- 在清洁设备前，应先将设备电源插头拔出。不要用湿润的布料擦拭设备，不要用液体清洗设备；
- 请不要将设备放在水边或潮湿的地方，并防止水或湿气进入设备机壳；
- 请不要将设备放在不稳定的箱子或桌子上，不慎跌落将会对设备造成严重损害；
- 应保持室内通风良好并保持设备通气孔畅通；
- 设备要在正确的电压下才能正常工作，请确认工作电压同设备所标示的电压相符。

2.2 检查安装场所

设备必须在室内使用，无论您将设备安装在机柜内还是直接放在工作台上，都需要保证以下条件：

- 确认设备的入风口及通风口处留有空间，以利于设备机箱的散热；
- 确认机柜和工作台自身有良好的通风散热系统；
- 确认机柜及工作台足够牢固，能够支撑设备及其安装附件的重量；
- 确认机柜及工作台的良好接地。

2.3 温/湿度要求

为保证设备正常工作和使用寿命，使用环境需维持一定的温度和湿度，如下表所示：

环境要求	工作温/湿度：-40℃～85℃，10%～90%，无冷凝
	存储温/湿度：-40℃～85℃，5%～95%，无冷凝

注意：若使用环境长期湿度过高，易造成绝缘材料绝缘不良甚至漏电，有时也易发生材料机械性能变化、金属部件锈蚀等现象；若相对湿度过低，绝缘垫片会干缩而引起紧固螺丝松动，同时在干燥的气候环境下，易产生静电，危害设备上的电路；温度过高则危害更大，　长期的高温将加速绝缘材料的老化过程，使设备的可靠性大大降低，严重影响其寿命。

2.4 抗干扰要求

设备在使用中可能受到来自系统外部的干扰，这些干扰通过电容耦合、电感耦合、电磁波辐 射、公共阻抗（包括接地系统）耦合和导线（电源线、信号线和输出线等）的传导方式对设 备产生影响。为此应注意：

- 交流供电系统为 TN 系统，交流电源插座应采用有保护地线（PE）的单相三线电源插座，使设备上滤波电路能有效的滤除电网干扰。
- 设备工作地点远离强功率无线电发射台、雷达发射台、高频大电流设备。
- 必要时采取电磁屏蔽的方法，如接口电缆采用屏蔽电缆。
- 接口电缆要求在室内走线，禁止户外走线，以防止因雷电产生的过电压、过电流将设备 信号口损坏。

2.5 安装场所要求

2.5.1 检查安装台

如果将设备安装在工作台，那么安装前需要保证以下条件：

- 确认安装台平稳、牢固，能够支撑本设备及其安装附件的重量。
- 确认安装台良好接地。

注意：设备表面不能压放过重的东西（最大承受重量4.5Kg），否则会造成设备损坏。

2.5.2 机柜安装要求

如果将设备安装在机柜内，请确认机柜符合下面的条件：

- 尽量把设备安装在敞开的机柜内。如果安装在密闭的机柜内，请确认机柜有良好的通风 散热系统；
- 确认机柜足够牢固，能够支撑本设备及其安装附件的重量；
- 确认机柜的尺寸适合本设备的安装。设备的左右侧面外应有一定的空间，以利于机箱的 散热；
- 为了便于散热和设备维护，建议机柜前后与墙面或其它设备的距离不应小于0.8 米，机房的净高不能小于3 米。

注意：本设备不随机提供安装工具，用户需要自己准备安装工具。

3 设备安装


注意：在机体的一个安装螺钉上封有本公司的防拆贴，当代理商对设备进行维护时，要求所维护设备的防拆贴完好，否则，由于擅自操作导致设备无法维护，将由用户本人负责。

3.1 交换机的安装流程

3.1.1 安装交换机到工作台

很多情况下，用户并不具备19英寸标准机柜，此时，人们经常用到的方法就是将设备放置在干净的工作台上，此种操作比较简单，操作中，只要注意如下事项即可：

- 保证工作台的平稳性与良好接地。
- 设备四周留出10cm以上的散热空间。
- 不要在设备上放置物品。

3.2 连接接口电缆

3.2.1 连 接 Console 口电缆

请按照下述步骤连接Console 口电缆：

1) 选定配置终端。

配置终端可以是标准的具有RS232串口的字符终端，也可以是一台普通的PC机，更常用的是后者。

2) 连接 Console 口电缆。

将Console口电缆带有RJ45连接器的一端连接到交换机的Console 口，将带有DB9（母）连接器的另一端连接到配置终端的串口。

3.2.2 连接以太网电缆

将以太网电缆一端连接到以太网电口，另一端连接到对端设备的以太网口。对于100M/1000M固定以太网电口，因支持MDI/MDI-X自适应，因此，当连接此接口到其它设备 时，使用标准网线或交叉网线均可。

上电后请检查以太网电口的指示灯状态。

4 配置准备和入门

本设备提供 Web 设置页面，本章将带领您了解设备的配置过程和熟悉 Web 设置页面。

4.1 设置准备

完成硬件安装后，在访问Web设置页面前，您需要确保管理计算机和网络满足一些基本要求。

4.1.1 计算机要求

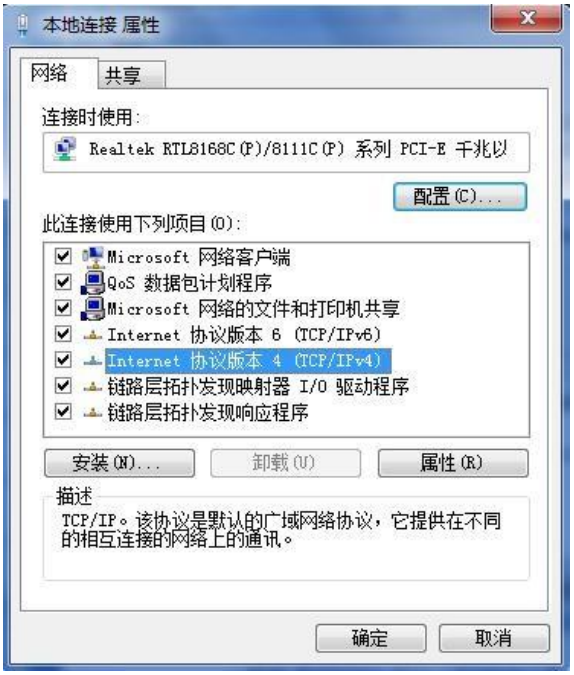
- 确认管理计算机已安装了以太网卡。
- 为了达到最佳的显示效果，推荐使用Microsoft IE浏览器（6.0或以上版本），显示器的分辨率为1024*768。

4.1.2 建立网络连接

说明：交换机管理 IP 地址为：192.168.2.1，子网掩码为：255.255.255.0，用户名为：admin，密码为：admin。

设备缺省配置时，操作步骤如下（以 Windows 7 系统为例）：

单击屏幕左下角<开始>按钮进入【开始】菜单栏，选择【控制面板】。点击【网络状态和 任务】图标，再双击【本地连接】图标，弹出【本地连接状态】窗口，如下图所示。
单击<属性>按钮，进入【本地连接属性】窗口，如图所示。



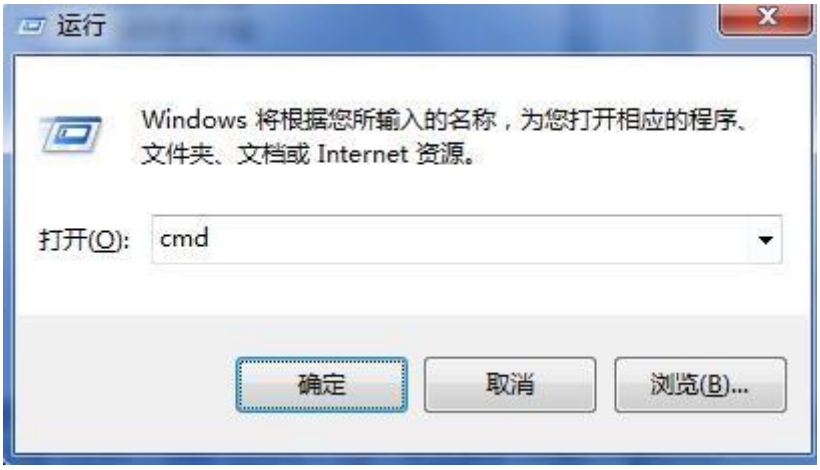
选中【Internet 协议版本4（TCP/IPv4）】，单击<属性>按钮，进入【Internet 协议（TCP/IP） 属性】窗口。选择【使用下面的IP 地址】单选按钮，输入IP 地址（在192.168.2.2～ 192.168.2.99和192.168.2.101～192.168.2.254中选择任意值）和子网掩码（255.255.255.0），确认后即可完成操作。

注意：

如果是进行本地配置，您需要将管理计算机的IP地址与设备的IP地址设置在同一子网中。

4.1.3 检查计算机和设备之间的网络是否连通

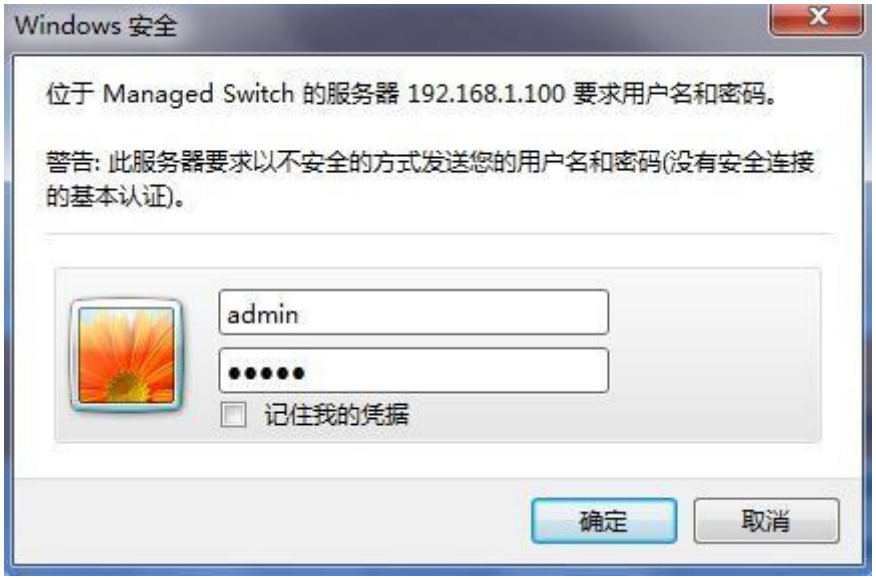
操作步骤如下：
单击屏幕左下角<开始>按钮进入【开始】菜单栏，选择【运行】，弹出如下图所示的对话框。



使用ping命令，输入“**ping 192.168.2.1**（缺省IP地址）”，单击<确定>按钮，如果在弹出的对话框中显示了如下图所示的回应，则表示网络连通；否则请检查网络连接。

4.2 登录交换机管理界面

运行 Web 浏览器，在地址栏中输入 IP 地址 **http://192.168.2.1** 按回车后
登录对话框，如下图所示，输入用户名和密码（首次登录时请输入缺省的用户名：**admin**，密码：**admin**），单击<确定>按钮或直接回车即可进入系统配置页面。



4.3 用户超时处理

当您长时间没有操作时，系统超时将注销本次登录，并返回到Web登录对话框，如需继续操作，请您重新登录。

5 WEB 界面简介

5.1 WEB 界面元素

交换机的WEB配置页面分为菜单栏、配置区两部分。单击菜单栏中的菜单项，进入到相应的配置页面，可以在配置区进行相应的配置并可查看设备状态或配置信息。如下图：

菜单栏：单击某个菜单项，用户即可进行相应的功能设置。
配置区：点击菜单栏某个菜单项，系统将在配置区显示相关配置界面，用户可在该界面进行相关功能设置。

5.2 错误提示功能

交换机的WEB管理界面提供了错误提示功能，即在参数设置错误或输入的格式不对时，系统会弹出错误提示对话框。如下图：

6 串口配置

6.1 串口设置

进入【串口设置】菜单栏，在串口设置页面中，可以启用/禁用串口、设置串口波特率、校验位、数据位、停止位设置，根据工作模式，选择 TCP server/TCP client/UDP connect 模式，远程 IP 等，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

7.接口管理

7.1 端口设置

进入【接口管理】--【端口设置】菜单栏，在端口设置页面中，可以启用/禁用端口、设置端口速率、启用/禁用流量控制，点击<修改>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
端口启用	选择启用/禁用该端口。
端口速率	设置该端口的端口速率，可设置为自动协商、1000M全双工、1000M半双工、10M全双工、10M半双工。
流量控制	选择启用/禁用流量控制功能。
端口范围	输入需要修改的端口号，可输入一个或一组端口，也可从下面的复选框中选择，端口的范围为 1~26.若设置一个端口，则在端口范围处输入对应的端口号；若设置一组端口，则可用“,”或“-”隔开。“,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如 1-8。

在【端口设置】页面中，可以查看到各端口的状态和配置信息。如下图：

☐	端口	端口标识	当前状态(speed/duplex)	设置状态		
				端口速率(speed/duplex)	流量控制	端口启用
☐	1	port1	未链接	Auto/Auto	禁用	启用
☐	2	port2	100M/Full	Auto/Auto	禁用	启用
☐	3	port3	未链接	Auto/Auto	禁用	启用
☐	4	port4	未链接	Auto/Auto	禁用	启用
☐	5	port5	未链接	Auto/Auto	禁用	启用
☐	6	port6	未链接	Auto/Auto	禁用	启用
☐	7	port7	未链接	Auto/Auto	禁用	启用
☐	8	port8	未链接	Auto/Auto	禁用	启用

界面项说明如下：

界面项	描述
端口	显示交换机各端口的序号。
端口标识	显示当前端口的标识。
当前状态	显示当前端口的连接速率。
端口速率	显示当前端口的端口速率。
流量控制	显示当前端口的流量控制功能状态。
端口启用	显示当前端口的状态。

7.1.1 端口设置示例

配置需求

开启端口 1-2、4-5，设置端口速率为“自动协商”，并启用流量控制功能。

配置步骤

【方法 1】

进入【接口管理】--【端口设置】菜单栏，选择启用端口，选择自动协商端口速率，选择启用流量控制，设置端口范围为“1-2,4-5”，点击<修改>按钮修改设置，设置完成后点击页面下方<保存>按钮保存配置。如下图：

【方法 2】

进入【接口管理】--【端口设置】菜单栏，勾选需要设置的端口号，选择启用端口，选择自动协商端口速率，选择启用流量控制，点击<修改>按钮完成配置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

端口启用	启用		
端口速率	100M	双工模式	自动协商
流量控制	禁用		
端口范围	2-3,5-6	修改	

	端口	端口标识	当前状态(speed/duplex)	设置状态		
				端口速率(speed/duplex)	流量控制	端口启用
☐	1	port1	未链接	100M/Auto	禁用	启用
☑	2	port2	100M/Full	100M/Auto	禁用	启用
☑	3	port3	未链接	100M/Auto	禁用	启用
☐	4	port4	未链接	Auto/Auto	禁用	启用
☑	5	port5	未链接	100M/Auto	禁用	启用
☑	6	port6	未链接	100M/Auto	禁用	启用
☐	7	port7	未链接	100M/Auto	禁用	启用
☐	8	port8	未链接	Auto/Auto	禁用	启用

7.2 风暴抑制

当主机系统响应一个在网上不断循环的报文分组或者试图响应一个没有应答的系统时 就会发生广播风暴。一般为了改变这种状态，请求或者响应分组源源不断地产生出来，常使 情况变得更糟。随着网络上分组数目的增加，拥塞会随之出现，从而降低网络的性能以至于 使之陷入瘫痪。 •

根据以上的原因，可以使用相应方法进行预防，但当产生风暴时，就需要通过在网络端 口上设置广播流量带宽比值或最大的广播包限值。假设在某端口上的广播限值为3000Kbps，当广播流量超过 3000Kbps 时，则会丢弃超出部分的广播包，这样就阻止了大量广播信息通过该端口扩散到整个网络，从而避免在广播域内发生广播风暴。

进入【接口管理】—【风暴抑制】菜单栏，在风暴抑制页面中，可以设置启用/禁用风暴抑制、广播数据包流量限制、多播数据包流量限制，设置完成后点击<保存>按钮完成配置。 如下图：

风暴抑制	◉ 启用 ○ 禁用	
端口范围	1-7	
广播抑制	6000	Kbps
多播抑制	6000	Kbps
单播抑制	6000	Kbps 配置

	端口	端口标识	广播抑制	组播抑制	单播抑制
☐	1	port1	6000Kbps	6000Kbps	6000Kbps
☐	2	port2	6000Kbps	6000Kbps	6000Kbps
☐	3	port3	6000Kbps	6000Kbps	6000Kbps
☐	4	port4	6000Kbps	6000Kbps	6000Kbps
☐	5	port5	6000Kbps	6000Kbps	6000Kbps
☐	6	port6	6000Kbps	6000Kbps	6000Kbps
☐	7	port7	6000Kbps	6000Kbps	6000Kbps
☐	8	port8	不受限制	不受限制	不受限制

界面项说明如下：

界面项	描述
风暴抑制	选择启用/禁用风暴抑制功能。 提示：以下参数设置仅在风暴抑制功能启用后方可设置。
端口范围	设定需要抑制风暴的端口及范围。例如：1-5
广播数据包流量限制	输入抑制的广播数据包流量限制，使广播数据包流量限制在合理的范围，从而有效地抑制广播风暴，避免网络拥塞，保证网络业务的正常运行。风暴抑制功能为启用时方可设置。范围：64-64000Kbps
多播数据包流量限制	输入抑制的多播数据包流量限制，使多播数据包流量限制在合理的范围，从而有效地抑制广播风暴，避免网络拥塞，保证网络业务的正常运行。风暴抑制功能为启用时方可设置。范围：64-64000Kbps
单播数据包流量限制	输入抑制的单播数据包流量限制，使单播数据包流量限制在合理的范围，从而有效地抑制广播风暴，避免网络拥塞，保证网络业务的正常运行。风暴抑制功能为启用时方可设置。范围：64-64000Kbps

7.3 带宽设置

进入【接口管理】--【带宽设置】菜单栏，在带宽设置页面中，可以限制各端口的出/入向带宽的速度，点击<配置>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
带宽设置	选择启用/禁用带宽设置功能。 提示：以下参数设置仅在带宽控制功能启用后方可设置。
端口范围	输入需要修改的端口号，可输入一个或一组端口，也可从下面的复选框中选择。若设置一个端口，则在端口范围处输入对应的端口号；若设置一组
	端口，则可用“,”或“-”隔开。 “,”用来设置一组不连续的端口，如 1,3,5。“-” 用来设置一组连续的端口，如1-8。
入口速度	设置的端口入口速度，千兆端口的速度范围可以设置为 64k~1000M；如果不限制入口速度请不要填写。
出口速度	设置的端口出口速度，千兆端口的速度范围可以设置为 64k~1000M；如果不限制出口速度请不要填写。

在【带宽设置】页面中，可以查看各端口的带宽限制信息。 界面项说明如下：

界面项	描述
端口	显示交换机各端口的序号。
端口标识	显示当前端口的标识。
入口速度	显示当前端口的入口速度。
出口速度	显示当前端口的出口速度。

7.3.1 带宽设置示例

配置需求

限制交换机上的所有端口的入口速率为 1Mbps，出口的速度为 512Kbps。

配置步骤

【方法 1】

进入【接口管理】--【带宽设置】菜单栏，选择启用带宽设置，设置端口范围为“1-8”，设置入口速度为“1024”，设置出口速度为“512”，点击<配置>按钮修改设置，再点击页面下方的<保存>按钮保存配置，使配置生效。如下图：

7.4 端口保护

端口保护就是在有些应用环境下，要求一台设备上的某些端口之间不能互相通讯。在这 种环境下，这些端口之间的通讯，不管是单播帧，还是广播帧，以及多播帧，都不能在保护 口之间进行转发。您可以通过将某些端口设置为保护口(Protected Port)来达到目的。当您将某些端口设为保护口之后，保护口之间互相无法通讯，保护口与非保护口之间可以正常通 讯。

当您将两个保护口设为一个镜像端口对时，镜像端口的源端口发送或接收的帧将按照镜 像端口的设置发到镜像端口的目的端口。因此您最好不要将镜像端口的目的端口设为保护 口。

设备支持将汇聚的端口设置为保护口，当您将汇聚组中的一个端口设置为保护口时，汇 聚组中的所有成员口都被设置为保护口。

进入【接口管理】—【端口保护】菜单栏，在端口保护设置页面中，可以启用/禁用端口保护 功能、设置端口为隔离口/普通端口，点击<配置>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
端口保护配置	选择启用/禁用端口保护功能。 提示：以下参数设置仅在端口保护功能启用后方可设置。
端口保护	设置端口为隔离端口或普通端口。隔离端口与隔离端口之间无法通信，隔离端口与普通端口之间可以正常通信。
端口范围	输入需要修改的端口号，可输入一个或一组端口，也可从下面的复选框中 选择。 若设置一个端口，则在端口范围处输入对应的端口号；若设置一组 端口，则可用“,”或“-”隔开。 “,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如1-8。

在【端口保护】页面中可查看到各端口保护信息。 界面

项说明如下：

界面项	描述
端口号	显示交换机各端口的序号。
端口标识	显示当前端口的标识。
端口保护	显示当前端口的端口保护状态

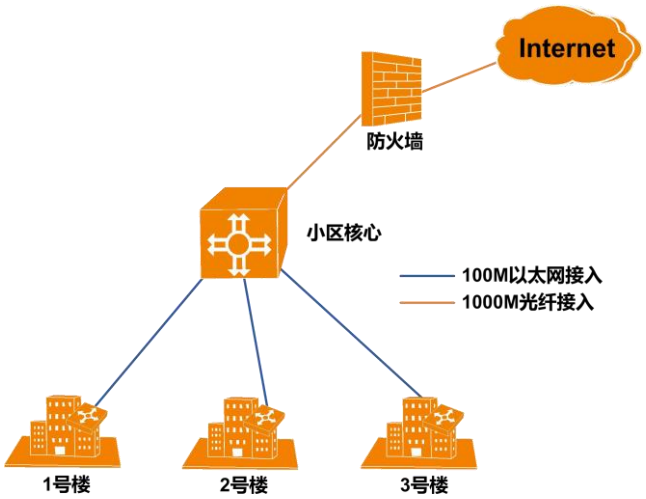
7.4.1 端口保护示例

配置需求

在一个小区环境中，所有的用户都在一个 VLAN 里面，但用户之间不能相互访问，只能和网关通讯访问互联网，此例中，本交换机放置在居民楼内，其中 1~6 口用于连接用户，其

它的端口用于上行的连接。

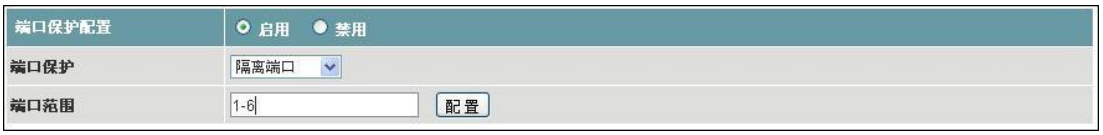
配置拓扑



配置步骤

【方法 1】

进入【接口管理】--【端口保护】菜单栏，选择启用端口保护功能，设置 1~6 号端口为隔离端口，即 1~6 号端口之间不能互相访问，点击<配置>按钮修改设置，再点击页面下方的< 保存>按钮保存配置，使配置生效。如下图：



7.5 回环检测

回环检测是通过在设备的端口上发送一种特殊的报文，并检测该报文是否能够从发送出去的端口送回来，来确定这个端口上是否存在环回情况。

进入【接口管理】--【回环检测】菜单栏，在回环检测页面中，可以启用/禁用回环检测功能、启用/禁用保护恢复功能、禁用端口环路时间，点击<修改>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
回环检测	选择启用/禁用回环检测功能。 提示：以下参数设置仅在回环检测功能启用后方可设置。
保护自动恢复	保护自动恢复就是在端口有环路进行保护后，在端口保护一段时间 后，端口可以恢复转发状态。 启用：在端口保护时间过后会自动恢复转发状态。 禁用：在端口保护后直到交换机重新启动后端口才恢复到转发状态。
禁用环路端口时间	关闭环路端口的时间是指当端口出现环路时关闭端口的时间，即保护端口时间，只有在“保护自动恢复”启用时，此参数有效。
端口范围	输入需要修改的端口号，可输入一个或一组端口，也可从下面的复选 框中选择。若设置一个端口，则在端口范围处输入对应的端口号；若 设置一组端口，则可用“,”或“-”隔开。 “,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如1-8。
端口回环检测	选择启用/禁用端口回环检测功能。

在【回环检测】页面中，可以查看各端口回环检测信息。

界面项说明如下：

界面项	描述
端口号	显示交换机各端口的序号。
端口标识	显示当前端口的标识。
回环检测	显示当前端口的回环检测启用状态。
回环检测状态	显示当前端口的回环检测状态。

7.6 MAC 地址表

MAC 地址表包含了用于端口之间报文转发的地址信息，MAC 地址表中分为 3 类地址：静态 MAC 地址，动态 MAC 地址和过滤 MAC 地址。

- 静态 MAC 地址：用户通过手动添加的 MAC 地址，不老化和不能被学习。
- 动态 MAC 地址：设备通过源 MAC 地址学习得来，有老化时间。
- 过滤 MAC 地址：通过用户手动添加的 MAC 地址，当设备接收到以过滤 MAC 地址为源地址的报文时会直接丢弃，过滤地址永远不会被老化。

进入【接口管理】--【MAC 地址表】菜单栏，在 MAC 地址表页面中，可以根据不同查询条件查询交换机的 MAC 地址表。如下图：

界面项说明如下：

界面项	描述
按物理端口查询	按物理端口查询，指定的物理端口范围为 1~26。可输入一个或一组端口。若设置一个端口，则在端口范围处输入对应的端口号； 若设置一组端口，则可用“,”或“-”隔开。 “,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如1-8。
按MAC地址类型查询	按MAC地址类型查询，可选择的类型有：静态MAC地址、动态MAC地址和过滤MAC地址。
查询	显示出你要查询的相关MAC信息。

在【MAC 地址表】页面中，可以查看查询到的 MAC 地址表信息。

界面项说明如下：

界面项	描述
序号	显示每条MAC地址排列的序号。
源地址	显示当前源MAC地址。
VLAN ID	显示对应的 VLAN ID 号。
类型	显示当前 MAC 地址的类型。
端口	显示对应的端口号。
处理方式	显示处理方式。

7.7 流量统计

设备的流量统计分为接收帧和发送帧，其中又包括了单播包、多播包、广播包和错误包。 进入【接口管理】—【流量统计】菜单栏，在该页面中，可以查看到单播包、多播包、广播包、错误包的接收和转发的数量统计。如下图：

端口	发送帧统计				接收帧统计			
端口号	单播包	多播包	广播包	错误包	单播包	多播包	广播包	错误包
1	0	0	0	0	0	0	0	0
2	317	62	0	0	230	0	150	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

8.VLAN 设置

VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。VLAN 是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。这一新兴技术主要应用于交换机之中。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分， 所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

8.1 端口 VLAN

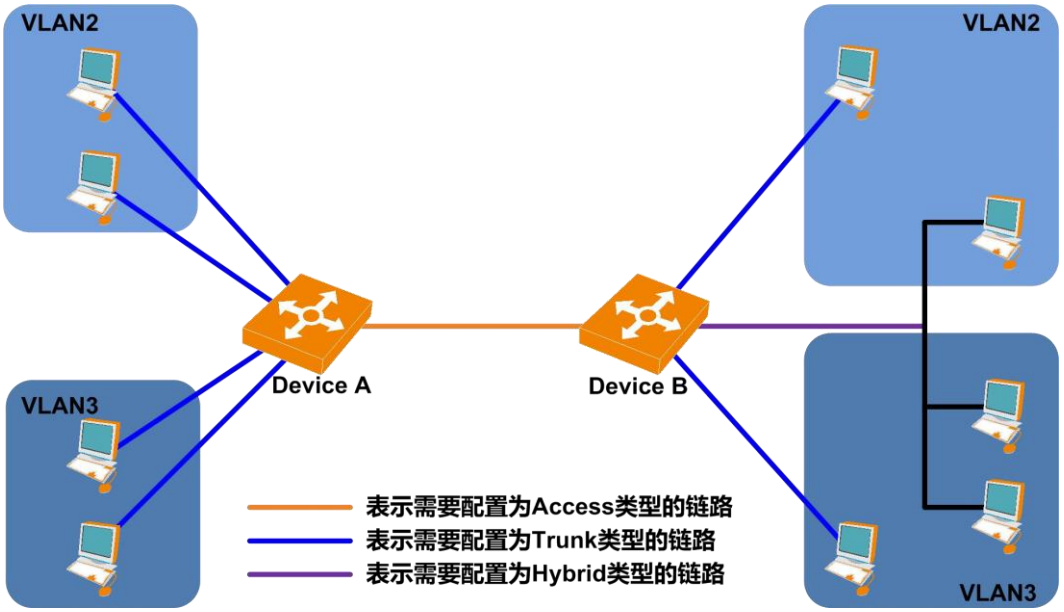
基于端口划分VLAN是VLAN最简单、最有效的划分方法。它按照设备端口来定义VLAN成员，将指定端口加入到指定VLAN中之后，端口就可以转发指定VLAN的报文。

根据端口在转发报文时对Tag标签的不同处理方式，可将端口的链路类型分为三种：

Access连接：端口发出去的报文不带tag标签。一般用于和不能识别VLAN tag的终端设备相连，或者不需要区分不同VLAN成员时使用。如下图所示，Device A和普通的PC相连， PC不能识别带VLAN tag的报文，所以需要将Device A和PC相连端口的链路类型设置为Access。

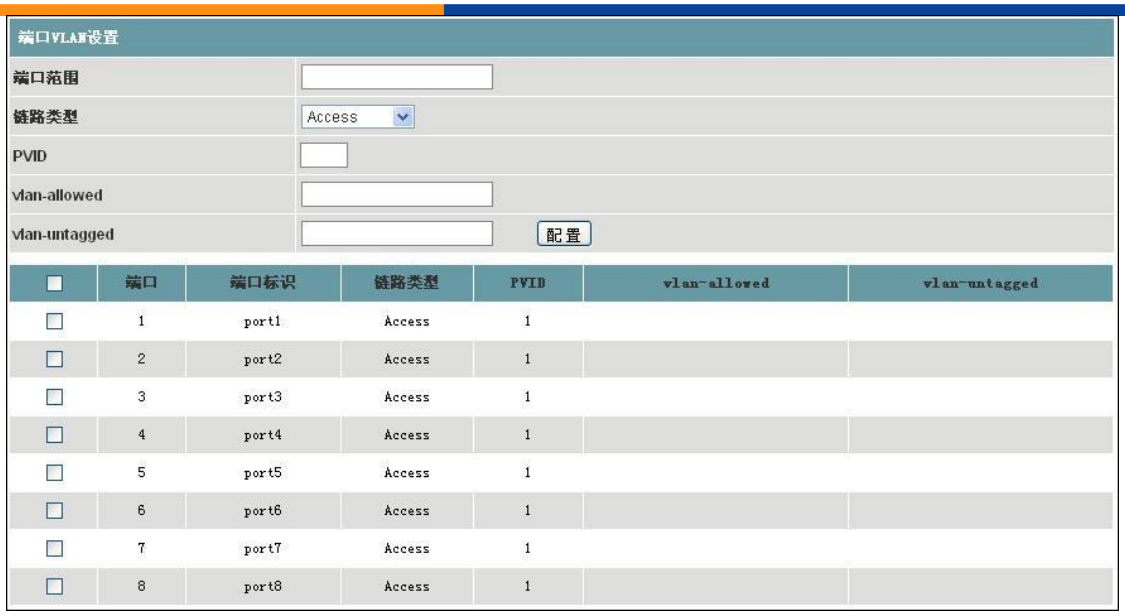
Trunk连接：端口发出去的报文，端口缺省VLAN内的报文不带tag，其它VLAN内的报文都必须带tag。通常用于网络传输设备之间的互连。如下图所示，Device A和Device B之间需要传输VLAN 2和VLAN 3的报文，所以，需要将Device A和Device B相连端口的链路类型设置为Trunk，并允许VLAN 2和VLAN 3通过。

Hybrid连接：端口发出去的报文可根据需要设置某些VLAN内的报文带tag，某些VLAN内的报文不带tag。通常用于相连的设备是否支持VLAN tag不确定的情况。如下图所示，DeviceB与一个小局域网相连，局域网中有些PC属于VLAN 2，有些PC属于VLAN 3，此时需要将Device B与该局域网相连端口的链路类型设置为Hybrid，并允许VLAN 2和VLAN 3的报文不带tag通过。



进入【VLAN 设置】--【端口 VLAN】菜单栏，在端口 VLAN 设置页面中，可以口设置链路的类型，端口范围，VLAN ID 等，点击<配置>按钮修改设置，设置完成后点击页面下方的

<保存>按钮保存配置。如下图：



界面项说明如下：

界面项	描述
端口VLAN	选择启用/禁用端口VLAN功能。 提示：以下参数设置仅在端口 VLAN 功能启用后方可设置。
端口范围	输入需要修改的端口号，可输入一个或一组端口，也可从下面的复选框 中选择。若设置一个端口，则在端口范围处输入对应的端口号；若设置 一组端口，则可用“,”或“-”隔开。 “,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如1-8。
链路类型	根据端口在转发报文时对 Tag 标签的不同处理方式，选择端口的链路类型，可选择 Access、Trunk 和 Hybrid。
PVID	输入端口需要加入的 VLAN ID 号。指定的 VLAN ID 范围为 1~4094。

在【端口 VLAN】页面中，可以查看各端口的配置信息。界面项说明如下：

界面项	描述
端口号	显示交换机各端口的序号。
端口标识	显示当前端口的标识。
链路类型	显示当前端口的链路类型。
PVID	显示当前端口对应的 PVID 号。

8.2QinQ 设置

进入【VLAN 设置】--【QinQ 设置】菜单栏，在 QinQ 设置页面中，可以设置 PVID 号，点击<配置>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项	描述
端口号	显示交换机各端口的序号。
TPID	表示VLAN Tag 的协议类型，设备可以根据TPID 值来识别报文中是否携带对应的VLAN Tag

8.3VLAN 转发表

VLAN 转发规则简介：

- 下面是定义的各种端口类型对各种数据帧的处理方法 ；

	Tagged 数据帧 IN	Tagged 数据帧 OUT	Untagged 数据帧 IN	Untagged 数据帧 OUT
Tagged 端口	原样接收	原样发送	按端口PVID 打Tag 标记	按 PVID 打 Tag 标记
Untagged 端口	丢弃	去掉Tag 标记	按端口PVID 打Tag 标记	原样发送

- 所谓的 Untagged Port 和 tagged Port 不是讲述物理端口的状态，而是将物理端口所拥有的某一个 VID 的状态，所以一个物理端口可以在某一个 VID 上是 Untagged Port，在另一个 VID 上是 tagged Port；
- 一个物理端口只能拥有一个 PVID，当一个物理端口拥有了一个 PVID 的时候，必定会拥有和 PVID 的 TAG 等同的 VID，而且在这个 VID 上，这个物理端口必定是 Untagged Port；
- PVID 的作用只是在交换机从外部接收到可以接收Untagged 数据帧的时候给数据帧添加 TAG 标记用的，在交换机内部转发数据的时候 PVID 不起任何作用；
- 拥有和 TAG 标记一致的 VID 的物理端口，不论是否在这个 VID 上是 Untagged Port 或tagged Port，都可以接受来自交换机内部的标记了这个 TAG 标记的 tagged数据帧；
- 拥有和 TAG 标记一致的 VID 的物理端口，只有在这个 VID 上是 tagged Port，才可以接受来自交换机外部的标记了这个 TAG 标记的 tagged 数据帧。

进入【VLAN 设置】--【VLAN 转发表】菜单栏，在 VLAN 转发表页面中设置 VLAN 转发设置规则，点击<配置>按钮添加设置，点击<编辑>按钮进行修改，点击<撤销>按钮删除设置， 设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
VID	输入需要设置的VLAN ID号。
VLAN名称	设置需要配置的VLAN名称。

在【VLAN 转发表】页面中，可以查看 VLAN 转发的配置信息。如下图：

界面项说明如下：

界面项	描述
编号	对应各VLAN转发规则的序号。
VID	显示当前VLAN转发规则的VID号。
VLAN名称	显示当前VLAN转发规则的VLAN的名称。
Tagged端口	显示当前打上标签的端口。
Untagged端口	显示当前未打上标签的端口。

9.QoS 管理

QoS（Quality of Service）即服务质量。对于网络业务，服务质量包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

网络资源总是有限的，只要存在抢夺网络资源的情况，就会出现服务质量的要求。服务质量是相对网络业务而言的，在保证某类业务的服务质量的同时，可能就是在损害其它业务的服务质量。例如，在网络总带宽固定的情况下，如果某类业务占用的带宽越多，那么其它业务能使用的带宽就越少，可能会影响其它业务的使用。因此，网络管理者需要根据各种业务的特点来对网络资源进行合理的规划和分配，从而使网络资源得到高效利用。

一旦网络可以区分电话通话和网上浏览，优先级处理就可以确保进行 Internet 上大型下载的同时不中断电话通话。为了确保准确的优先级处理，所有业务量都必须在网络骨干内进行识别。在工作站终端进行的数据优先级处理可能会因人为的差错或恶意的破坏而出现问题。黑客可以有意地将普通数据标注为高优先级，窃取重要商业应用的带宽，导致商业应用的失效。这种情况称为拒绝服务攻击。通过分析进入网络的所有业务量，可以检查安全攻击，并且在它们导致任何危害之前及时阻止。

在局域网交换机中，多种业务队列允许数据包优先级存在。较高优先级的业务可以在不受较低优先级业务的影响下通过交换机，减少对诸如话音或视频等对时间敏感业务的延迟事故。

为了提供优先级，交换机的每个端口必须有至少 2 个队列。虽然每个端口有更多队列

可以提供更为精细的优先级选择，但是在局域网环境中，每个端口需要 4 个以上队列的可能性不大。当每个数据包到达交换机时，都要根据其优先级别分配到适当的队列，然后该交换机再从每个队列转发数据包。该交换机通过其排队机制确定下一步要服务的队列。有以下 2 种排队方式。

严格优先队列(SPQ) 这是一种最简单的排队方式，它首先为最高优先级的队列进行服务，直到该队列为空，然后为下一个次高优先级队列服务，依此类推。这种方法的优势是高 优先级业务总是在低优先级业务之前处理。但是，低优先级业务有可能被高优先级业务完全阻塞。

加权循环(WRR) 这种方法为所有业务队列服务，并且将优先权分配给较高优先级队列。在大多数情况下，相对低优先级，WRR 将首先处理高优先级，但是当高优先级业务很多时， 较低优先级的业务并没有被完全阻塞。

9.1 QoS 设置

进入【QoS 管理】--【QoS 设置】菜单栏，在 QoS 设置页面中，可以启用/禁用 QoS 功能、设置 QoS 优先级、启用/禁用 802.1p QoS 功能和设置优先级，点击<配置>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
QoS设置	选择启用/禁用QoS功能。 提示：以下参数设置仅在 QoS 功能启用后方可设置。
QoS优先级队列	选择QoS控制数据传输的优先级，可选择绝对优先和相对优先。
802.1p QoS 设置	选择启用/禁用 802.1p QoS 功能。 提示：以下参数设置仅在 802.1p QoS 功能启用后方可设置。

802.1p 标识范围	配置 802.1p QoS 优先级范围，802.1p 定义了 8 个优先级，优先级范围为 0~7，最高优先级为 7。可输入一个或一组优先级。若设置一个优先级，则在802.1p 标识范围处输入对应的优先级；若设置一组优先级，则可用“,”或“-”隔开。 用来设置一组不连续的优先级，如 1,3,5。 “-”用来设置一组连续的优先级，如 1-4。
优先级	选择 802.1p QoS 优先级队列。

在【QoS 设置】页面中，可以查看到 802.1p QoS 的配置信息。界面项说明如下：

界面项	描述
802.1p标识	显示802.1p定义的优先级。
优先级	显示当前优先级所属的队列。

9.2 DSCP QoS

提示：只有在【QoS 设置】页面中，启用了 QoS 功能后，此功能项才可配置。

进入【QoS 管理】--【DSCP QoS】菜单栏，在 DSCP QoS 页面中，可以选择启用 DSCP 或禁用该功能、设置 DSCP 标识范围和 DSCP 优先级，点击<配置>按钮修改设置，设置DSCP 完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
DSCP QoS配置	选择DSCP功能进入到DSCP配置页面，选择<禁用>禁用该功能。 提示：以下参数设置仅在 DSCP 功能启用后方可设置。
DSCP 标识范围	输入需要配置的 DSCP 标识，可输入一个或一组标识。若设置一个标识，则在 DSCP 标识范围处输入对应的标识号；若设置一组标识，则可用“,”或“-”隔开。 “,”用来设置一组不连续的标识，如 1,3,5。“-”用来设置一组连续的标识，如1-6。 选择 DSCP 时可配置。
DSCP 优先级	配置 DSCP 优先级队列，选择 DSCP 时可配置。

在【DSCP QoS】页面中，可以查看到 DSCP QoS 的配置信息。界面项说明如下：

界面项	描述
DSCP标识	显示当前DSCP的标识。
优先级	显示当前 DSCP 标识所属的优先级队列。

10 网络管理

10.1 Trunking

Trunking（链路聚合）是将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，使用链路聚合服务的上层实体把同一聚合组内的多条物理链路视为一条逻辑链路。链路聚合可以实现出/入负荷在聚合组中各个成员端口之间分担，以增加带宽。同时，同一聚合组的各个成员端口之间彼此动态备份，提高了连接可靠性。

按照聚合方式的不同，链路聚合可以分为两种模式：

- 静态聚合模式
  静态聚合模式由用户手工配置，不允许系统自动添加或删除汇聚组中的端口。汇聚组中必须至少包含一个端口。当汇聚组只有一个端口时，只能通过删除汇聚组的方式将该端口从汇聚组中删除。

- 动态聚合模式
  动态聚合模式是一种系统自动创建或删除的汇聚，动态汇聚组内端口的添加和删除是 LACP 协议自动完成的。只有基本配置相同、速率和双工属性相同、连接到同一个设备、并且对端端口也满足以上条件时，才能被动态汇聚在一起。即使只有一个端口也可以创建动态汇聚，此时为单端口汇聚。动态汇聚中，端口的 LACP 协议处于开启状态。

在同一个汇聚组中，能进行出/入负荷分担的成员端口必须有相同的速率、 双工和基本配置。基本配置包括：

- STP 配置一致，包括：端口的 STP 开启/关闭、与端口相连的链路属性（如点对点或非点对点）、STP 优先级、STP 开销、STP 报文格式、是否开启环路保护和根保护、 是否为边缘端口等。
- QoS 配置一致，包括流量限速、优先级标记、802.1p 优先级、流重定向、流量统计等。

进入【网络管理】--【Trunking】菜单栏，在 Trunking 页面中，可以启用/禁用聚合功能、设置汇聚的协商参数，点击<添加>按钮添加设置，点击<修改>按钮修改设置，点击<删除> 按钮删除设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
Trunk配置	选择启用/禁用端口聚合功能。 提示：以下参数设置仅在端口聚合功能启用后方可设置。
聚合负载均衡模式	选择负载均衡的方式，可选择MAC源/目的地址、MAC源地址和MAC目的地址。
Trunk 名称	设置聚合组的名称，最多可以设置 6 个 Trunk 组。Trunk 名称最多填写 4个字符。
聚合模式	选择聚合的模式，可选择手工汇聚、静态 LACP 汇聚、动态 LACP 汇聚。
操作 key	设置操作 key，两端的操作 key 必须相同。取值范围为 1~65535。
端口范围	设置加入到汇聚组的端口号，每个 Trunk 组中最多有 8 个端口，每个端口只能属于一个 Trunk 组。

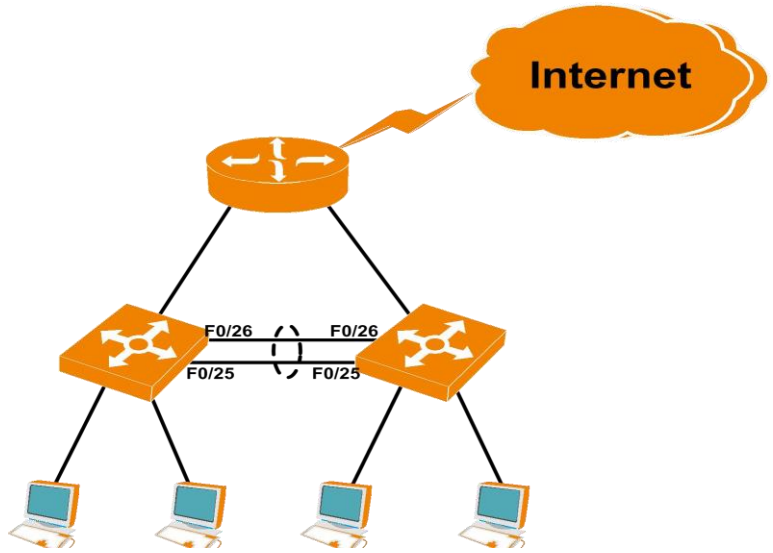
在【Trunking】页面中，可以查看端口聚合的配置信息。如下图：

界面项说明如下：

界面项	描述
编号	显示当前聚合组的序号。
Trunk名称	显示当前汇聚组的名称。
聚合模式	显示当前聚合组的聚合模式。
操作 key	显示当前聚合组的操作 key。
端口范围	显示所属当前聚合组的端口号。

10.1.1 端口汇聚配置示例

配置拓扑



配置步骤

进入【网络管理】--【Trunking】菜单栏，在 Trunking 配置页面中，首先启用端口汇聚功能， 设置汇聚组的名称，选择聚合负载模式为源地址，聚合模式为“动态 LACP 汇聚”，设置操作 key 为 12345，操作 key 两端必须一致，设置端口范围为“25-26”， 点击<添加>按钮添加设置，再点击<保存>按钮使配置生效。

10.2 端口镜像

端口镜像（port Mirroring)把交换机一个或多个端口（VLAN）的数据镜像到一个或多个端口的方法。

进入【网络管理】--【端口镜像】菜单栏，在端口镜像页面中，可以启用/禁用端口镜像功能、设置监控端口或镜像端口、设置监控的方式和采集数据的方式，点击<配置>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
端口镜像	选择启用/禁用端口镜像功能。 提示：以下参数设置仅在端口镜像功能启用后方可设置。
监控端口	设置监控端口，即将镜像端口的数据流copy或mirror一份，发送给连接 在监控端口上的流量分析仪。 提示：监控端口必须是唯一值，即不能是一组端口。
镜像端口范围	设置镜像端口的范围，该端口为受控端口，流往该端口的数据都会被copy 一份发送给监控端口。可输入一个或一组端口。若设置一个端口， 则在端口范围处输入对应的端口号；若设置一组端口，则可用“,”或“-”隔开。 “,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如 1-8。
集数据	选择端口监控数据的采集发式。可选择全部数据、进口数据和出口数据 3 种方式。 全部数据：监控镜像端口接收和发送的数据。 进口据：监控镜像端口接收的数据。 出口数据：监控镜像端口发送的数据。

在【端口镜像】页面中，可以查到端口镜像的配置信息。如下图：

界面项说明如下：

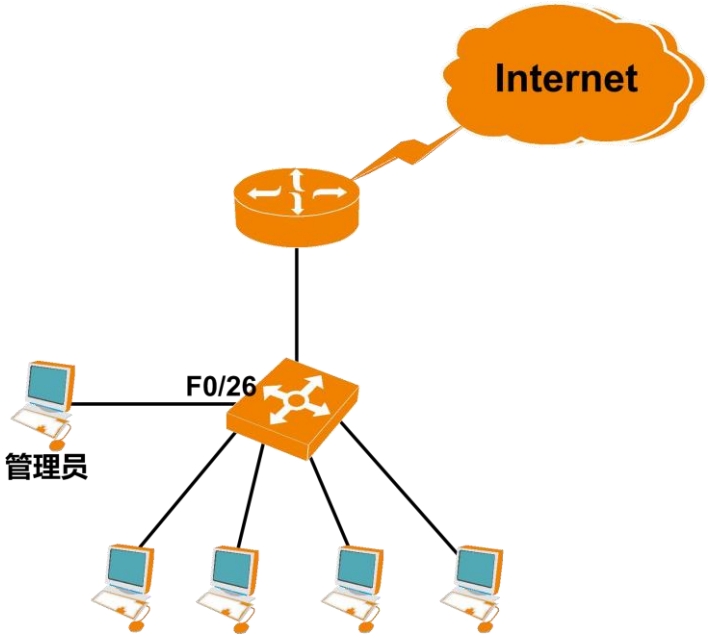
界面项	描述
监控端口	显示当前监控端口号。
镜像端口	显示当前镜像端口号。
采集数据	显示当前采集数据的方式。

10.2.1 端口镜像配置示例

配置需求

配置所有用户的数据流量都会被管理员监控。

配置拓扑



配置步骤

进入【网络管理】--【端口镜像】菜单栏，在端口镜像配置页面中，首先启用端口镜像功能，设置监控端口为“26”，设置镜像端口范围为“1-10”，选择采集数据的方式为“全部数据”，点击<配置>按钮修改配置，再点击<保存>按钮保存配置，使配置生效。如下图：

10.3 RSTP 生成树

RSTP (Rapid Spanning Tree Protocol)是快速生成树的英文缩写，提供和 STP 一样的功能。完全向下兼容 802.1D STP 协议。相对于 STP，最主要的特点是“快”，如果一个局域网内的网桥都支持 RSTP 协议，且管理员配置得当，一旦网络拓扑结构改变，而要重新生成拓扑树只需要不超过 1 秒的时间（传统 STP 约需 50 秒）。

进入【网络管理】-【RSTP 生成树】菜单栏，在 RSTP 生成树页面中，可以启用/禁用 RSTP 生成树功能、设置 RSTP 参数等，点击<修改>按钮修改设置，设置完成后点击页面下方的< 保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
RSTP配置	选择启用/禁用RSTP功能。 提示：以下参数设置仅在RSTP功能启用后方可设置。
设备优先级	设置设备的桥优先级，该优先级用来参加生成树选举时，决定那 台设备成为整个网络的根，担当起整个网络的转发工作，优先级 必须为4096的倍数，默认为32768，值越小优先级越高。 提示：建议将核心交换机的优先级的值设置的小一些，使 交换机在选举时成为根网桥，这样有利于整个网络的稳定。
消息发送的周期	配置交换机定时发送 BPDU 报文的时间间隔，缺省值为 2 秒。
消息最大生存期	配置 BPDU 报文消息生存的最长时间。缺省值为 20 秒。
端口状态迁移的延时	配置端口状态改变的时间延时。缺省值为 15 秒。
本网桥更新信息	显示当前网桥的相关信息。
路径开销	配置端口路径开销，端口路径开销的默认值与端口速率有关系， 一般是端口速率越高，端口路径花费越少。路径开销的范围0~200000000，0 表示为自动检测，1~200000000 路径开销值。
端口优先级	端口路径花费，必须是 16 的倍数。
点到点端口	配置端口 Point to Point 模式，当端口仅仅与一个桥连接时，则为点到点端口。“是”表示为点到点端口，“否”表示为不是点到点端口，“自动检测”表示为自动检测是否属于点到点端口。默 认为自动检测。
边缘端口	配置端口 Edge 模式，当端口不与任何桥连接时，称为边缘端口。 当设置端口是边缘端口后，端口又收到 BPDU，则端口自动转变为非边缘端口。

在【RSTP 生成树】页面中，可以查看到 RSTP 的配置信息。如下图：

	端口号	端口标识	路径开销	端口优先级	点到点端口	边缘端口
☐	1	port1	自动检测	128	自动检测	否
☐	2	port2	自动检测	128	自动检测	否
☐	3	port3	自动检测	128	自动检测	否
☐	4	port4	自动检测	128	自动检测	否
☐	5	port5	自动检测	128	自动检测	否
☐	6	port6	自动检测	128	自动检测	否
☐	7	port7	自动检测	128	自动检测	否
☐	8	port8	自动检测	128	自动检测	否

界面项说明如下：

界面项	描述
端口号	显示交换机各端口的序号。
端口标识	显示当前端口的标识。
路径开销	显示当前端口的路径开销。
端口优先级	显示当前端口的优先级
点到点端口	显示当前端口是否是点到点端口。
边缘端口	显示当前端口是否为边缘端口。

10.4 IGMP Snooping

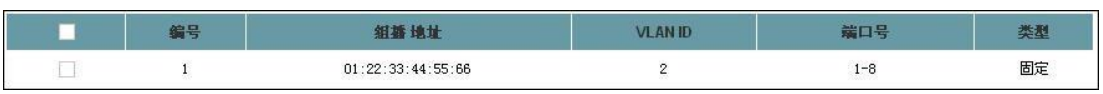
IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。交换机通过侦听主机向路由器的 IGMP 成员报告消息的方式，形成组成员和交换机接口的对应关系； 交换机根据该对应关系将收到组播数据包只转给具有组成员的接口。

进入【网络管理】--【IGMP Snooping】菜单栏，在 IGMP Snooping 页面中，可以启用/禁用 IGMP Snooping 功能、设置 IGMP Snooping 组播表等，点击<添加>按钮添加设置，点击<修改>按钮修改设置，点击<删除>按钮删除设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
IGMP snooping功能	选择启用/禁用IGMP Snooping功能。 提示：以下参数设置仅在 IGMP Snooping 功能启用后方可设置。
IGMP 查 询	开启/禁用IGMP查询功能。
IGMP 查询间隔	每隔多长时间查询存在的多播成员，60-1000 秒。
组成员生存时间	设备中已存在的多播成员从存在到收不到应答能存活的最长时间，120-5000 秒。
静态组播 MAC 地址	设置静态组播的 MAC 地址
VLAN ID（可选）	静态组播 MAC 地址的 VLAN ID 号
端口范围	静态组播MAC地址的端口号

在【IGMP Snooping】页面中，可以查看到 IGMP Snooping 的配置信息。如下图：



界面项说明如下：

界面项	描述
编号	显示当前静态组播地址的编号。
组播地址	显示当前的静态组播MAC地址。
VLAN ID	显示当前静态组播地址的 VLAN ID 号。
端口号	显示当前静态组播地址的端口号。

11 网络安全

11.1 端口安全认证

IEEE 802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网端口的一个普通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（port based network access control protocol）。“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。

进入【网络安全】--【端口安全认证】菜单栏，在端口安全认证页面中，可以启用/禁用端口 安全认证功能、设置端口安全认证参数等，点击<配置>按钮修改设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：

界面项说明如下：

界面项	描述
全局设置	选择启用/禁用端口安全认证功能。提示：以下参数设置仅在端口安全认证功能启用后方可设置。
定时更新认证	设置定时更新认证的周期时间，范围是60~40000000秒。
认证服务器设置	设置认证服务器的 IP 地址、端口号和共享密匙。共享密匙必须与认证服务器的共享密匙一致。
计费服务器设置（可选）	设置计费服务器的 IP 地址、端口号和共享密匙。共享密匙必须与计费服务器的共享密匙一致。
控制模式	设置 802.1X 在端口上进行接入控制的模式，可选的模式及其含义说明如下： 自动识别模式：指示端口初始状态为非授权状态；如果认证流程通过，则端口切换到授权状态。这也是最常见的情况。 强制授权模式：指示端口始终处于授权状态。 强制非授权模式：指示端口始终处于非授权状态。
端口控制方式	设置 802.1X 在端口上进行接入控制的方式。MAC Based：表示采用基于 MAC 方式。
最大用户数	设置认证的最大用户数，范围为 1~1024。
周期性重认证	设置是否在端口上启用周期性重认证定时器。
端口范围	设置要启用 802.1X 认证的端口，可输入一个或一组端口，也可从下面的复选框中选择。若设置一个端口，则在端口范围处输入对应的端口号；若设置一组端口，则可用“,”或“-”隔开。“,”用来设置一组不连续的端口，如 1,3,5。 “-”用来设置一组连续的端口，如 1-8。

在【端口安全认证】页面中，可以查看端口安全认证的配置信息。如下图：

	端口	端口标识	设置状态		
			控制模式	控制方式	最大用户数
	1	port1	强制授权模式	MAC Based	4096
	2	port2	强制授权模式	MAC Based	4096
	3	port3	强制授权模式	MAC Based	4096
	4	port4	强制授权模式	MAC Based	4096
	5	port5	强制授权模式	MAC Based	4096
	6	port6	强制授权模式	MAC Based	4096
	7	port7	强制授权模式	MAC Based	4096
	8	port8	强制授权模式	MAC Based	4096

界面项说明如下：

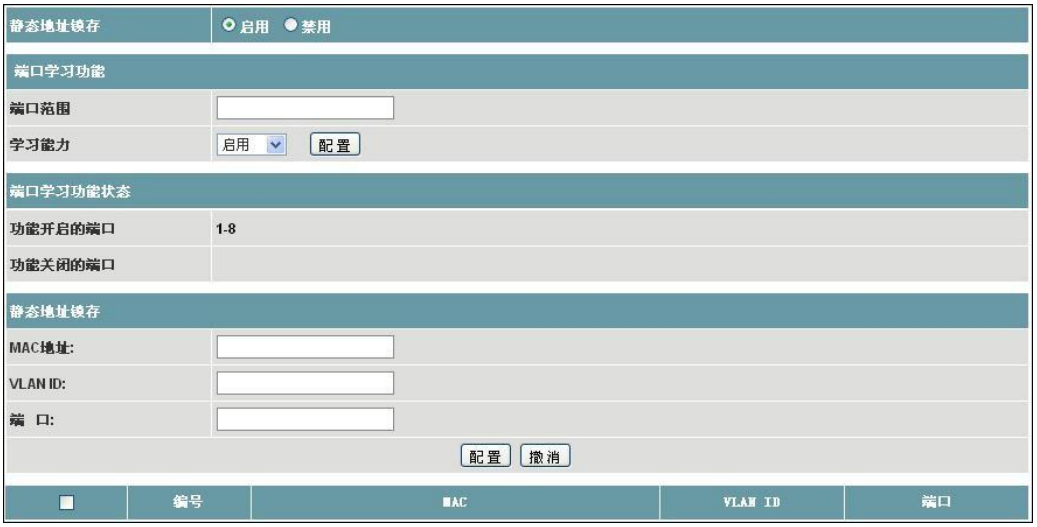
界面项	描述
端口	对应交换机各端口的序号。
端口标识	显示当前端口的标识。
控制模式	显示当前端口的控制模式。
控制方式	显示当前端口的控制方式。
最大用户数	显示当前端口的最大认证用户数。

11.2 静态地址锁存

静态 MAC 地址区别于一般的由学习得到的动态 MAC 地址。静态地址一旦被加入，该地址在删除之前将一直有效，不受最大老化时间的限制。静态地址表记录了端口的静态地址。静 态地址表中一个 MAC 地址对应一个端口，如果设置，则所有发给这个地址的数据只会转发给该端口。也成为 MAC 地址绑定。

静态 MAC 地址表旨在限制计算机的移动，凡是计算机的 MAC 和端口绑定的，此计算机移到其他端口是不能通信的，而别的计算机移到这个接口还是可以通讯的。而与这个相对应的 "端口安全"，端口安全旨在保护端口安全，端口只能在指定 MAC 与其连接的时候才转发数据，假定设置端口安全且与一个 MAC 绑定，那么这台 pc 接到其他端口上是可以的， 但是其他 pc 接到这个端口是不能通讯的。这个功能就是前面描述的"802.1x 认证"。

进入【网络安全】--【静态地址锁定】菜单栏，在静态地址锁存页面中，可以启用/禁用静态地址锁存、端口学习功能的端口范围、启用/禁用学习能力以及设置要锁定的 MAC 地址、VLAN ID 和端口号，点击<配置>按钮添加设置，点击<撤销>按钮删除设置，设置完成后点击页面下方的<保存>按钮保存配置。如下图：



界面项说明如下：

界面项	描述
静态地址锁存	选择启用/禁用静态地址锁存功能。 提示：以下参数设置仅在静态地址锁存功能启用后方可设置。
端口范围	需要进行设置的端口的范围。
学习能力	MAC地址的学习能力，可以选择禁用或者启用。
功能开启的端口	显示当前功能开启的端口号。
功能关闭的端口	显示当前功能关闭的端口号。
MAC地址	设置需要锁定的MAC地址。
VLAN ID	设置需要锁定的MAC地址所属VLAN
端口	设置需要锁定的端口号。

在静态锁存地址页面中，可以查看到锁定的 MAC 地址的相关信息，界面项说明如下：

界面项	描述
编号	显示当前静态地址锁定的序号。
MAC	显示当前锁定的MAC地址。
VLAN ID	显示当前锁定的VLAN ID。
端口	显示当前锁定的端口。

12 系统管理

12.1 IP 地址

IP 地址是分配给连接在 Internet 上的设备的一个 32 比特长度的地址。IP 地址由两个字段组成：网络号码字段（net-id）和主机号码字段（host-id）。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。为了方便 IP 地址的管理，IP 地址分成五类。如下所示：

网络类型　　地址范围　　用户可用的 IP 网络范围

A　0.0.0.0～127.255.255.255　　1.0.0.0～126.0.0.0

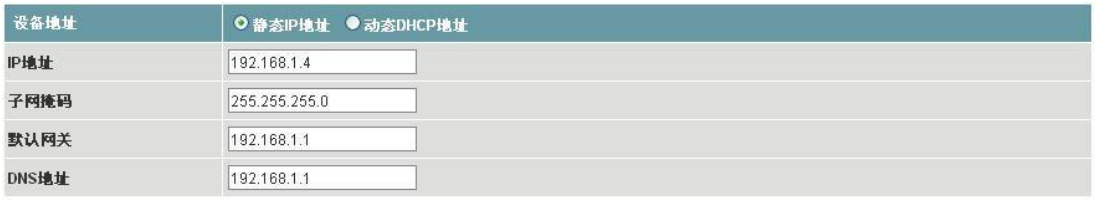
B　128.0.0.0～191.255.255.255　　128.0.0.0～191.254.0.0

C　192.0.0.0～223.255.255.255　　192.0.0.0～223.255.254.0 D
　　224.0.0.0～239.255.255.255　　无
E　240.0.0.0～247.255.255.255　　无

其中 A、B、C 类地址为单播（unicast）地址；D 类地址为组播（multicast）地址；E 类地址为保留地址，以备将来的特殊用途。目前大量使用中的 IP 地址属于 A、B、C 三类地址。IP 地址采用点分十进制方式记录。每个 IP 地址被表示为以小数点隔开的 4 个十进制整数， 每个整数对应一个字节，如 10.110.50.101。

进入【系统管理】--【IP 地址】菜单栏，在 IP 地址页面中，可以选择设置 IP 地址的方式和设置 IP 地址、子网掩码、默认网关、DNS，设置完成后点击页面下方的<保存>按钮保存配置。

如下图：



界面项说明如下：

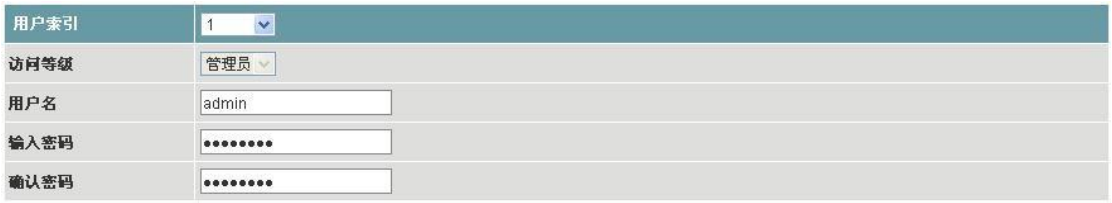
界面项	描述
设备地址	设置设备的IP地址，可以通过动态DHCP方式获取或手动设置IP地址。 提示：不建议使用DHCP配置，该设置可能会造成交换机无法获　取管理地址。
IP地址	设置设备的IP地址，选择为静态IP地址时可用。
子网掩码	设置设备 IP 地址的子网掩码，选择为静态 IP 地址时可用。
默认网关	设置设备的默认网关地址，选择为静态 IP 地址时可用。
DNS 地址	设置设备的 DNS 地址，选择为静态 IP 地址时可用。

在【IP 地址】页面中，可以查看当前设备的 IP 地址信息，界面项说明如下：

界面项	描述
编号	显示对应的设备地址的序号。
IP地址	显示设备的IP地址。
子网掩码	显示设备 IP 地址的子网掩码。
默认网关	显示设备的默认网关地址。
DNS 地址	显示设备的 DNS 地址。

12.2 用户密码

进入【系统管理】--【用户密码】菜单栏，在用户密码页面中，可以设置用户的权限、更改 用户密码等，设置完成后点击<保存>按钮保存配置。如下图：



界面项说明如下：

界面项	描述
用户索引	设置登录用户的用户编号。
访问等级	设置用户的访问等级，可选择管理员或客户。 管理员：可以对交换机进行所有操作。 客户：只能对交换机进行简单的配置。
用户名	设置登录用户的名称。
输入密码	设置登录用户的密码。
确认密码	再次输入登录用户的用户密码，必须保持与上次输入的密码相同。

12.3 SNMP 配置

SNMP是简单网络管理协议(Simple Network Management Protocol SNMP)的简称，是为了解决以下网络问题而产生的协议：

- 网络规模逐渐增大，网络设备的数量成级数增加，网络管理员很难及时监控所有设备的 状态、发现并修复故障。

- 网络设备可能来自不同的厂商，如果每个厂商都提供一套独立的管理接口 （比如命令行），将使网络管理变得越来越复杂。

SNMP主要有SNMP V1、SNMP V2c几种最常用的版本。

- SNMP V1

  SNMP V1是SNMP协议的最初版本，提供最小限度的网络管理功能。SNMP V1的SMI和MIB都比较简单，且存在较多安全缺陷。

  SNMPv1采用团体名认证。团体名的作用类似于密码，用来限制NMS对Agent的访问。 如果SNMP报文携带的团体名没有得到NMS/Agent的认可，该报文将被丢弃。

- SNMP V2c

  SNMP V2c也采用团体名认证。在兼容SNMP V1的同时又扩充了SNMP V1的功能：它提供了更多的操作类型（GetBulk操作等）；支持更多的数据类型（Counter32等）； 提供了更丰富的错误代码，能够更细致地区分错误。

进入【系统管理】-【SNMP 配置】菜单栏，在SNMP 设置页面中，可以启用/禁用 SNMP 功能、可以设置 SNMP 网关、版本、团体名等，点击<保存>按钮完成配置。如下图：

界面项说明如下：

界面项	描述
SNMP设置	选择启用/禁用SNMP功能。 提示：以下参数设置仅在SNMP功能启用后方可设置。
SNMP网关	SNMP Trap是SNMP的一部分，当被监控段出现特定事件，可能是性能问题，甚至是网络设备接口宕掉等，代理端会给管理站发告警事件。通过 告警事件，管理站可以通过定义好的方法来处理告警。SNMP网关地址即管理主机的IP地址。
SNMP 版本	选择使用的 SNMP 版本号。
只读团体名	设置只读团体名，用来限制 NMS 对 Agent 的访问，只能对设备信息进行查询。
读写团体名	设置设置读写团体名，用来限制 NMS 对 Agent 的访问，不仅能对设备进行查询，也能对设备进行配置。

12.4 日志输出

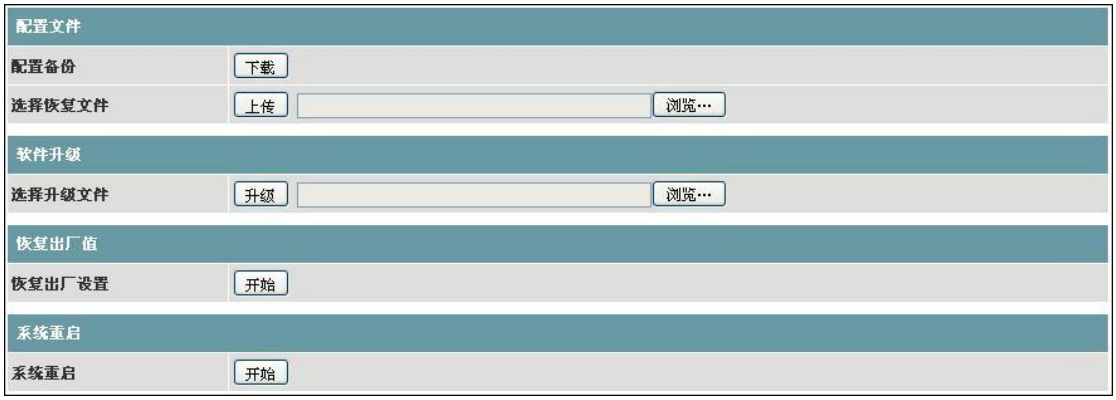
进入【系统管理】—【日志输出】菜单栏，在日志输出页面中，可以启用/禁用日志功能、可 以根据不同的日志类型查询日志，也可以点击<下载所有信息>按钮将日志导出或点击<删除 所有信息>按钮删除日志，点击<上一页>或<下一页>按钮，可以上翻或下翻日志信息。如下图：

界面项说明如下：

界面项	描述
日志记录	选择启用/禁用日志功能。  提示：以下参数设置仅在日志功能启用后方可设置。
显示类型	根据不同的日志类型查看日志，可选择全部信息、操作信息、网络信息和报警信息
信息处理	可选择日志的处理方式，可以导出日志或删除日志。
编号	显示当前日志的序号。
类型	显示当前日志的类型。
时间	显示当前日志产生的时间。
事件	显示日志的具体信息。

12.5 文件管理

进入【系统管理】--【文件管理】菜单栏，在文件管理页面中，可以导入/导出配置文件、升级软件、恢复出厂设置和重启设备。如下图：



界面项说明如下：

界面项	描述
配置备份	将配置以文件形式保存到计算机中，点击<下载>按钮将设备的配置文件导出。
选择恢复文件	将计算机中的配置文件还原到设备中，通过<浏览>按钮选择导出的配置文件，点击<上传>按钮完成配置文件的导入。
选择升级文件	使用升级文件对设备进行升级，通过<浏览>按钮选择最新的升级文件，点击<升级>按钮完成升级
恢复出厂设置	恢复设备的出厂设置值，点击<开始>按钮完成设置。
系统重启	重新启动交换机，点击<开始>按钮完成设置。

13 Console 界面设置

13.1 登录设备的 Console 界面

本可以通过 Console 线登录到设备的命令行配置界面，对设备进行相应的配置。具体配置步骤如下（以 Windows XP 操作系统为例）

1) 依次打开【开始】--【程序】--【附件】--【通讯】--【超级终端】（也可以在【开始】

--【运行】--【键入“hypertrm.exe”】）；

2） 在弹出的新建连接中输入名称并为连接选一个图标，配置完成后，单击<确定>按钮使其配置生效；

3） 选择使用的 COM 口；

4） 设置每秒位数为 115200；数据位为 8；奇偶校验为无；停止位为 1；数据流控制为无， 单击<确定>按钮使其生效；

5） 成功登录到设备的 Console 界面。