



10 口

网管型工业以太网交换机

用 户 手 册

发布时间：2017 年 7 月 25 日
版 本：V1.5.0

深圳市讯记科技有限公司
<http://www.comark.cn>

Copyright © 深圳市讯记科技有限公司 版权所有

本文档包含专有信息，受版权保护。未经深圳市讯记科技有限公司事先书面许可，不得以任何形式或电子、机械、磁学、光学、化学和人工等其它方式复制、传播、转录本文件的任何部分，也不得将任何部分储存于检索系统中或翻译成任何语言。

免责声明

深圳市讯记科技有限公司专利或专利权不作任何暗示或其它方式授权。深圳市讯记科技有限公司对本文档以及本文档中描述的产品不作任何暗示或其它方式的保证。本文档所提供的信息从发布之日起被认为是准确可靠的。 深圳市讯记科技有限公司不承担本文档中的任何错误之责任。 此外，深圳市讯记科技有限公司不承担任何本文档使用或本文档信息被滥用以及因使用本文档可能引起的任何专利侵权责任。 本文档的信息和在本文档中的产品规格可能会随时变更，恕不另行通知。

修订记录

日期	版本	描述
2014-03-15	1.1	首次发布。
2014-05-21	1.2	1.更新“5.16.3 设置 SNMP 陷阱”章节内容。 2.在“1 概述”中增加串口说明和面板图。 3.修改“2 访问交换机配置界面”中的 IP 地址为“192.168.1.253”。 4.增加“4.14 配置串口参数”和“5.15 配置串口参数”章节。
2015-02-10	1.3	增加 POE 功能
2016-04-27	1.4	增加串口 Modbus 功能
2017-07-25	1.5	CPU 升级

目 录

1. 概述.....	1-1
2. 访问交换机配置界面.....	2-1
2.1 通过 Console 访问	2-1
2.2 通过 Telnet 远程访问.....	2-4
2.3 通过 Web 浏览器访问.....	2-4
3. 功能特性.....	3-5
4. WEB 界面操作.....	4-6
4.1 查看系统信息	4-6
4.2 设置端口参数	4-7
4.3 设置端口镜像	4-8
4.4 创建端口隔离组.....	4-9
4.5 创建端口聚合组.....	4-10
4.6 管理虚拟局域网.....	4-11
4.6.1. 使能 802.1Q VLAN	4-13
4.6.2. 创建 802.1Q VLAN 组	4-13
4.6.3. 设置端口的 VLAN 属性.....	4-14
4.6.4. 使能 QinQ.....	4-15
4.7 设置服务质量	4-16
4.7.1. QoS.....	4-16
4.7.2. 设置 QoS 优先级协议.....	4-17
4.7.3. 设置 QoS 端口优先级.....	4-17
4.7.4. 设置调度机制	4-18
4.7.5. 设置发送队列	4-19
4.7.6. 设置 DSCP 队列映射	4-19
4.7.7. 设置 CoS 重映射	4-20
4.8 管理转发地址	4-20
4.8.1. 设置老化时间	4-21
4.8.2. 设置单播 MAC 地址.....	4-21
4.8.3. 设置多播 MAC 地址.....	4-22
4.8.4. 设置 IGMP Snooping.....	4-24
4.9 管理风暴抑制	4-26
4.10 查看数据统计	4-26
4.10.1. 查看端口数据	4-27
4.10.2. 查看 MAC 地址表.....	4-27
4.11 管理快速生成树.....	4-28
4.12 创建环网	4-32
4.12.1. 创建单环环网	4-33

4.12.2. 创建相交环环网	4-34
4.12.3. 创建相切环环网	4-36
4.13 管理 POE	4-38
4.14 配置串口参数	4-39
4.14.1. 服务器模式	4-44
4.14.2. 客户端模式	4-45
4.14.3. UDP 模式	4-47
4.14.4. Modbus TCP 模式	4-49
4.15 管理 SNMP	4-52
4.15.1. 创建 SNMP 团体名	4-54
4.15.2. 创建 SNMP 用户名	4-54
4.15.3. 设置 SNMP 陷阱	4-55
4.16 管理系统信息	4-56
4.16.1. 修改 IP 地址	4-56
4.16.2. 设置简单网络时间协议	4-56
4.16.3. 设置告警	4-58
4.16.4. 设置管理 VLAN	4-59
4.16.5. 查看系统日志	4-59
4.16.6. Ping 诊断	4-59
4.16.7. 修改帐户	4-60
4.16.8. 更新 Firmware	4-60
4.16.9. 下载或上传配置文件	4-61
4.17 保存配置	4-62
4.18 重启系统	4-62
4.19 退出系统	4-63
5. 命令行操作	5-63
5.1 常用命令	5-63
5.2 查看系统信息	5-66
5.3 设置端口参数	5-66
5.4 设置端口镜像	5-67
5.5 创建端口隔离组	5-69
5.6 创建端口聚合组	5-69
5.7 管理虚拟局域网	5-70
5.7.1. 使能 802.1Q VLAN	5-72
5.7.2. 设置 TPID	5-72
5.7.3. 创建 802.1Q VLAN 组	5-72
5.7.4. 设置端口的 VLAN 属性	5-73
5.7.5. 使能 QinQ	5-74
5.8 设置服务质量	5-74
5.8.1. QoS	5-75
5.8.2. 设置 QoS 优先级协议	5-75
5.8.3. 设置 QoS 端口优先级	5-75
5.8.4. 设置调度机制	5-76

5.8.5. 设置发送队列	5-76
5.8.6. 设置 DSCP 队列映射	5-77
5.8.7. 设置 CoS 重映射	5-78
5.9 管理转发地址	5-78
5.9.1. 设置老化时间	5-78
5.9.2. 设置单播 MAC 地址	5-79
5.9.3. 设置多播 MAC 地址	5-80
5.9.4. 设置 IGMP Snooping	5-80
5.10 管理风暴抑制	5-82
5.11 查看数据统计	5-83
5.11.1. 查看端口数据	5-83
5.11.2. 查看 MAC 地址表	5-84
5.12 管理快速生成树	5-85
5.13 创建讯记环网	5-89
5.13.1. 创建单环环网	5-90
5.13.2. 创建相交环环网	5-92
5.13.3. 创建相切环环网	5-94
5.14 管理 POE	5-96
5.15 配置串口参数	5-97
5.16 管理 SNMP	5-100
5.16.1. 创建 SNMP 团体名	5-102
5.16.2. 创建 SNMP 用户名	5-102
5.16.3. 设置 SNMP 陷阱	5-103
5.17 管理系统信息	5-104
5.17.1. 修改 IP 地址	5-104
5.17.2. 设置简单网络时间协议	5-104
5.17.3. 设置告警	5-105
5.17.4. 设置管理 VLAN	5-107
5.17.5. 查看系统日志	5-107
5.17.6. Ping 诊断	5-107
5.17.7. 修改帐户	5-108
5.17.8. 更新 Firmware	5-108
5.17.9. 下载或上传配置文件	5-109
5.18 保存配置	5-110
5.19 恢复出厂设置	5-110
5.20 重启系统	5-110
5.21 退出系统	5-110
6. 常见问题	6-110

1. 概述

感谢购买深圳讯记科技工业以太网交换机。通过阅读本份用户使用手册配置交换机能帮助您更好的应用于工业场合。

本手册分 4 部分介绍：

➤ 访问交换机界面方式

当您需要对交换机进行配置时，您可以通过 Console、Telnet 和 Web 浏览器三种方式访问或配置交换机。

➤ 功能特性

列表介绍本设备的各种配置、监控和管理功能。

➤ WEB 界面操作

本章介绍使用 Web 界面进行交换机配置的具体操作。

➤ 命令行操作

本章介绍使用命令行进行交换机配置的具体操作。

2. 访问交换机配置界面

当您需要对交换机进行配置时，您可以通过 Console、Telnet 和 Web 浏览器三种方式访问或配置交换机。

本设备的缺省 IP 地址配置如表 2-1 IP 地址配置所示，表格中 IP 地址只作为本手册配置参考数据，请根据现场实际的交换机 IP 地址进行设置。

表 2-1 IP 地址配置

值	值域
IP 地址	192.168.1.253
子网掩码	255.255.255.0
网关	192.168.1.1

目前 10 口网管型工业以太网交换机只提供一个用户，您可以根据具体情况修改交换机用户的密码。本设备的缺省用户配置如表 2-2 用户配置所示，表格中用户为只作为本手册配置参考数据，请根据现场实际的交换机用户进行设置。

表 2-2 用户配置

用户	密码	说明
admin	123	管理员用户，允许更改所有的交换机配置。

2.1 通过Console访问

当您不知道交换机的 IP 地址时，您可以用串口线将交换机上的 Console 口与 PC 机的 COM 口连接来访问交换机配置界面。

步骤1 启动超级终端。

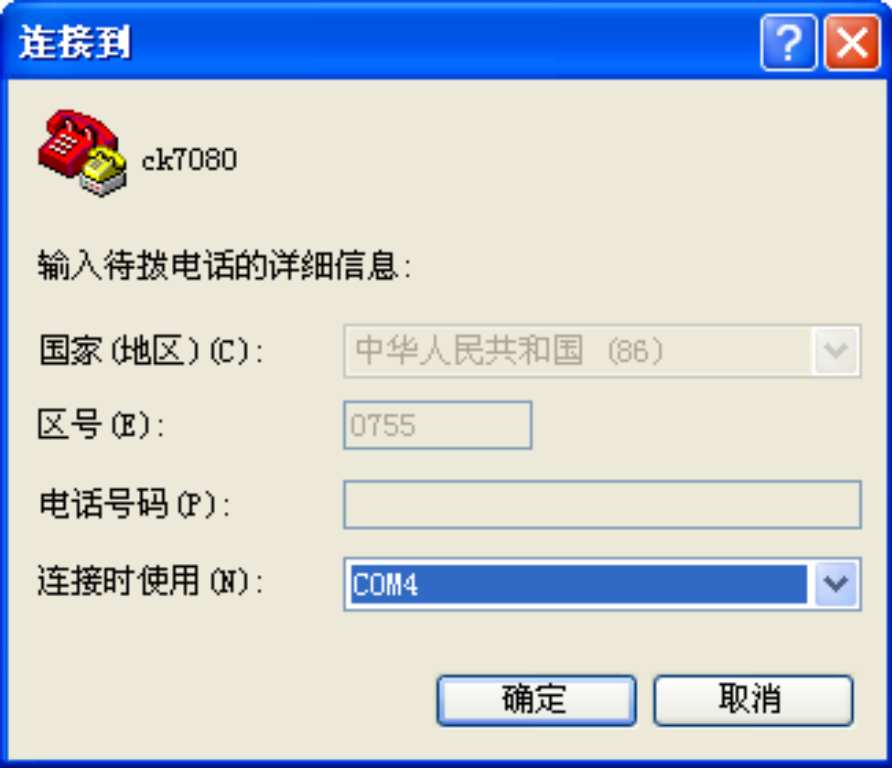
在 Windows 的开始菜单上选择“开始 < 程序 < 附件 < 通讯 < 超级终端”，Windows 系统启动超级终端。

步骤2 新建连接。

在“名称”中输入新建连接的名称，并选择图标，单击“确定”。



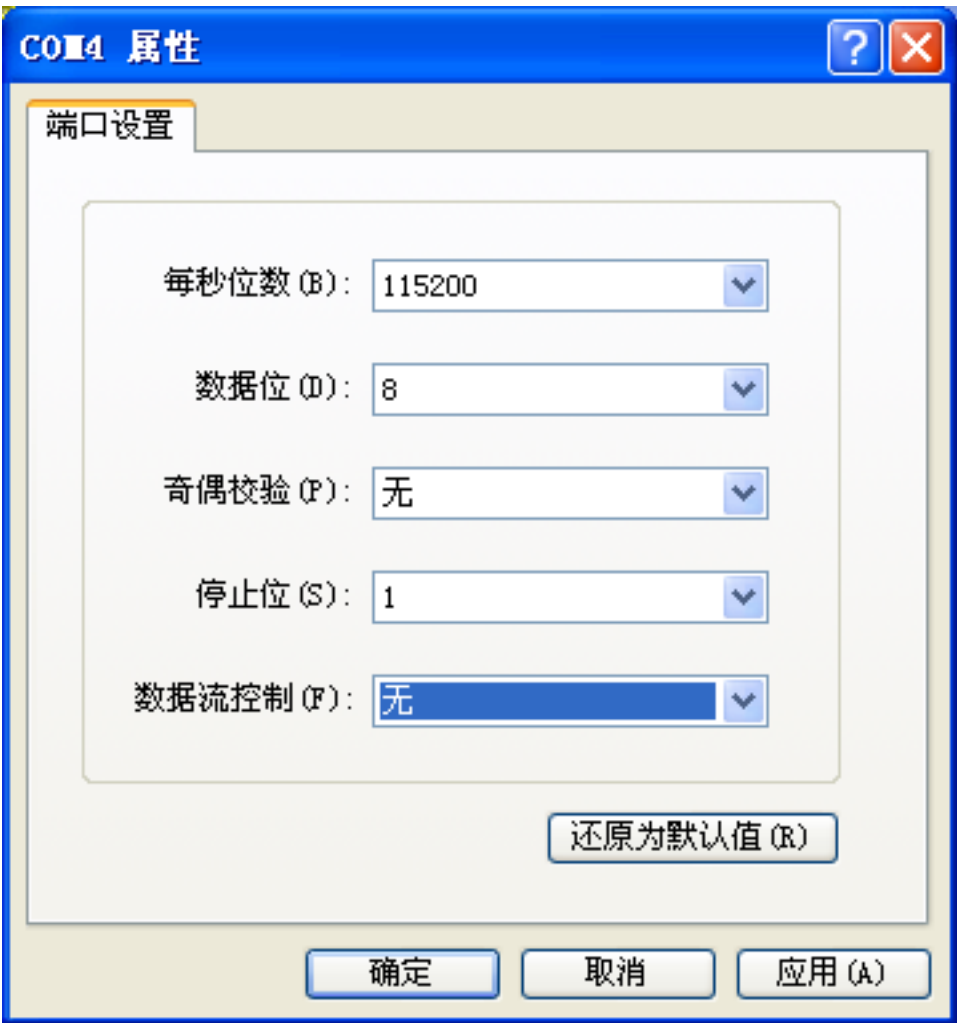
步骤3 设置连接使用的端口，单击“确定”。
请根据 PC（或配置终端）实际使用的端口在“连接时使用”下中选择，如选择“COM4”。



步骤4 在“端口属性”对话框中设置通信参数。

表 2-3 通信参数配置参考

值	值域
每秒位数（B）	115200
数据位（D）	8
奇偶校验（P）	无
停止位（S）	1
数据流控制（流量控制）（F）	无



步骤5 单击“确定”，表示进入命令行界面。

步骤6 输入用户名和密码。

用户名和密码请参见“表 2-2 用户配置”。

命令行界面提示登录成功，则可输入命令对交换机进行配置。如输入“show ipconfig”查看交换机的 IP 地址。



——结束

2.2 通过Telnet远程访问

当 PC 机和交换机属于同一个逻辑子网时，您可以使用 Telnet 远程访问交换机，并对其进行配置管理。在通过 Telnet 访问交换机之前，交换机机的以太网端口需连接到您的局域网，或者直接连接到您的 PC 机网口。

步骤1 在 Windows 的开始菜单上选择“开始 < 运行”。

Windows 系统弹出“运行”对话框。

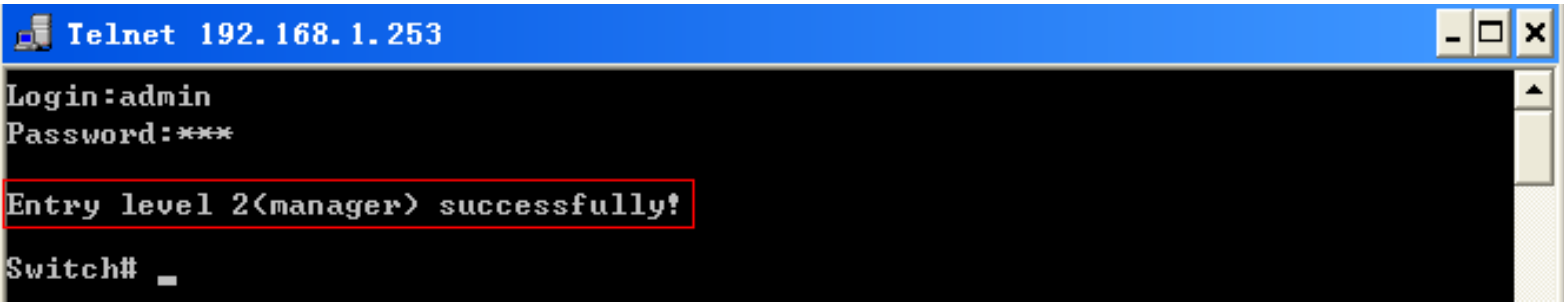
步骤2 在“运行”对话框中输入“telnet *IP 地址*”，如“telnet 192.168.1.253”。



步骤3 单击“确定”，进入命令行界面。

步骤4 输入用户名和密码，按“Enter”键。

用户名和密码请参见“表 2-2 用户配置”。命令行界面如下图所示，则远程登录交换机成功。



——结束

2.3 通过Web浏览器访问

Web 浏览器访问为交换机的访问和配置提供一种简便的方法。您可以使用 Internet Explorer(简称 IE 浏览器)这类标准的网页浏览器来访问交换机的 Web 配置界面。在通过 Web 浏览器访问交换机之前，交换机机的以太网端口需连接到您的局域网，或者直接连接到您的 PC 机网口。

步骤1 在 PC 上打开 IE 浏览器。

步骤2 在 IE 浏览器的地址栏中输入 IP 地址，如“http://192.168.1.253/index.htm”，按“Enter”键。

步骤3 在弹出的对话框中输入用户名和密码。



步骤4 单击“确定”，进入交换机 Web 配置界面。



——结束

3. 功能特性

简单介绍本设备的各种配置、监控和管理功能。

表 3-1 功能介绍

功能	说明
系统信息	查看设备的系统信息，如系统名称，MAC 地址等信息。
端口设置	设置端口的使能状态、自协商和流量控制等信息。
端口镜像	设置一个或多个端口的数据镜像到某一个端口来实现对网络的监控。
端口隔离组	创建一个或多个端口隔离组。端口隔离组内的端口相互隔离不可互相通信，端口隔离组外的端口可以互相通信。

端口聚合	创建端口聚合组，可实现两个交换机之间通过多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。
虚拟局域网	设置基于端口的 802.1Q VLAN 和 QinQ。
服务质量	设置 QoS、调度机制、发送队列、DSCP 映射和 CoS 重映射。
转发地址	设置交换机的老化时间、单播 MAC 地址、多播 MAC 地址和 IGMP Snooping。
风暴抑制	设置端口的流量类型和入口速度，以防止广播风暴。
数据统计	统计端口帧数据和 MAC 地址。
快速生成树	使能交换机快速生成树（RSTP）的功能，并配置 RSTP 桥信息和端口属性。
环网	设置和管理环网。
POE	设置端口 POE 属性
串口	设置和管理串口。 📖 说明：串口功能只对支持串口的机型可见。
SNMP 管理	设置 SNMP 账户和陷阱。
管理配置	设置设备 IP 地址、简单网络时间协议（SNTP）、系统告警，使能 VLAN 组，查看系统日志，进行 Ping 测试，添加、修改或删除新账户，通过 TFTP 服务器更新系统软件、备份配置文件和重载配置文件。
保存设置	保存您对设备系统所进行的设置。
重启系统	重启设备系统或恢复出厂设置。
退出系统	退出当前的登录。

4. Web界面操作

本章介绍使用 Web 界面进行交换机配置的具体操作。
通过 Web 浏览器的操作步骤请参见“[2.3 通过 Web 浏览器访问](#)”。
登录设备的 Web 界面后,您可以在界面右上方的菜单栏中更改您所需要的语言或联系技术支持工程师。

4.1 查看系统信息

系统信息即交换机的基本信息，主要包括系统名称、MAC 地址、硬件版本、软件版本和出厂编号等信息。当需要了解交换机的基本信息时，您可以通过在 web 界面左侧导航菜单中选择“系统信息”进入“系统信息”页面查看所需的信息。

系统信息	
系统信息	
系统名称	Optical Industrial Ethernet Switch
系统型号	Ck7080
硬件版本	VER 1.0.02
软件版本	V-3.1.198-(Jul 15 2017 16:05:53)
MAC 地址	00-a1-d3-88-13-68
出厂编号	
系统时间	1970年1月1日星期四 00:01:00
PC时间	2017年7月25日星期二 14:54:23
应用与更新时间至交换机	

4.2 设置端口参数

端口设置是对端口的访问状态、协商模式、速率/双工、流量控制和 MAC 地址学习的配置和管理。您可以根据实际情况设置端口的各种参数。

步骤1 在左侧导航中选择“端口设置”，进入端口参数设置页面。

端口设置

端口	状态	自协商	速率&双工	流控	出口速率(0=Disable)	MAC地址学习
FE1	Enabled	Auto	10M Half	Off	0 62~100000 kbps	Enabled

应用

端口状态

端口	状态	链路状态	自协商	配置的速率&双工	实际的速率&双工	流控	出口速率	MAC地址学习
FE1	Enabled	Down	Auto	-	-	Off	0	Enabled
FE2	Enabled	Down	Auto	-	-	Off	0	Enabled
FE3	Enabled	Down	Auto	-	-	Off	0	Enabled
FE4	Enabled	Down	Auto	-	-	Off	0	Enabled
FE5	Enabled	Down	Auto	-	-	Off	0	Enabled
FE6	Enabled	Down	Auto	-	-	Off	0	Enabled
FE7	Enabled	Down	Auto	-	-	Off	0	Enabled
FE8	Enabled	Up	Auto	-	100M Full	Off	0	Enabled

步骤2 选择某一端口，并设置该端口的参数。

表 4-1 端口设置参数

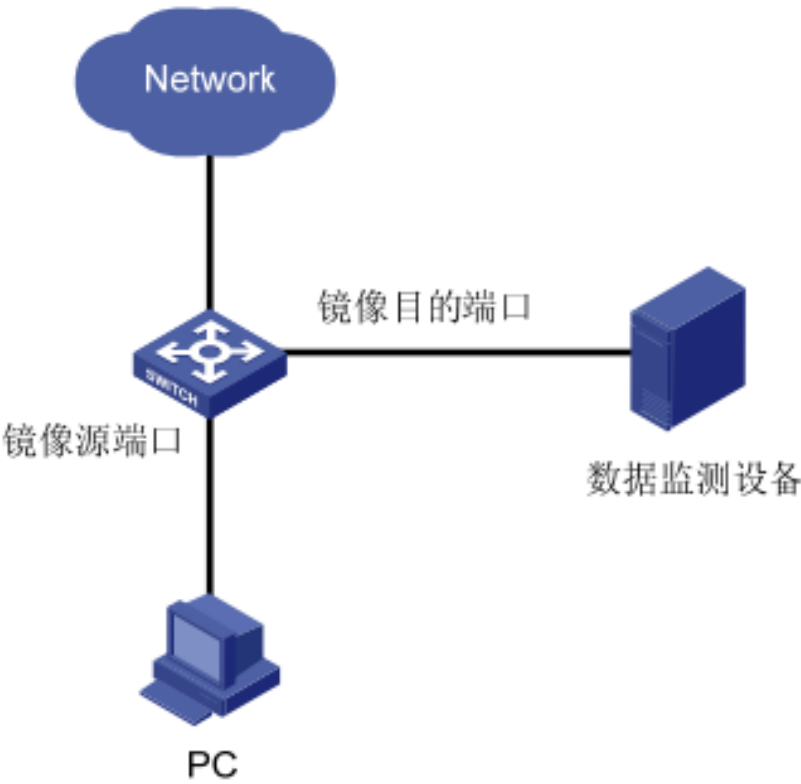
值	值域	描述
端口	如 FE1	选择需要设置的端口号。
状态	Enabled, Disabled 缺省值: Enabled	启用或禁用该端口。 Enabled: 表示启用端口。 Disabled: 表示禁用端口。当选择“Disabled”时，端口的“自协商”、“速率&双工”、“流控”和“MAC地址”均不可设置。
自协商	Auto, Force 缺省值: Auto	设置该端口的自协商状态。 Auto: 表示允许端口和所连接的设备之间按照IEEE802.3u 自动调节最佳的工作速率和工作模式。 Force: 表示强制限制端口的工作速率和工作模式，需手动在“速率&双工”中设置端口的工作速率和模式。
速率&双工	10M Half, 10M Full, 100M Half, 100M Full	设置该端口的工作速率和全/半双工模式。  说明: 只有把“自协商”设置为“Force”时，才可配置“速率&双工”。
流控	On, Off 缺省值: Off	启用或禁用该端口的流量控制功能。 流量控制用于防止在端口阻塞的情况下丢帧，这种方法是当发送或接收缓冲区开始溢出时通过将阻塞信号发送回源地址实现的。流量控制可以有效的防止由于网络中瞬间的大量数据对网络带来的冲击，保证用户网络高效而稳定的运行。

出口速率	百兆端口取值范围： 62~100000k bps 千兆端口取值范围： 62~250000k bps 缺省值：0	设置该端口的发送速率。交换机会自动将所设置的值转换为与之最接近的速率。 📖 说明：“0”时表示该端口无出口速率限制，发送数据在该端口上全速运行。由于交换机芯片内部的出口速率算法限制，千兆端口的出口速率最大取值为 250000kbps。
MAC 地址学习	Enabled, Disabled 缺省值：Enabled	启用或禁用该端口的 MAC 地址学习功能。 交换机是根据报文的目的 MAC 地址对报文进行转发的，因此交换机维护了一种记录 MAC 地址与端口对应关系的转发表来指导交换机进行转发，这个表称为 MAC 地址转发表。交换机将接收到的报文的源 MAC 地址以及接收端口记录到该表中，供后续报文转发使用，这个记录过程称为 MAC 地址的学习过程。

步骤3 单击“应用”，使所设置的端口口参数生效并在 “端口列表” 中显示。
——结束

4.3 设置端口镜像

端口镜像功能可以用来监视一个或多个端口的接收、发送或收发的数据，以便于在线调测和监控网络数据状态。其中被监视的端口称为镜像源端口，监视端口称为镜像目的端口。源端口和镜像目的端口必须位于同一台交换机上，镜像目的端口不能与源端口相同。端口镜像组网图如下图所示。您可以使用数据监测设备连接镜像目的端口接收所监控的数据进行网络数据分析或监控。



步骤1 在左侧导航中选择“端口镜像”，进入端口镜像设置页面。

端口镜像

端口镜像

目的端口

FE2

源端口	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2
不配置										
发送端口										
接收端口										
收发端口										

应用

步骤2 在“目的端口”中选择某一端口，如“FE2”。

步骤3 在源端口列表中选择需要监测的端口数据。

如，FE1 作为镜像目的端口，需要监测 FE2 的发送数据、FE3 的接收数据和 FE4 的收发数据，则端口镜像设置如下图所示。

端口镜像

端口镜像

目的端口

FE1

源端口	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2
不配置										
发送端口										
接收端口										
收发端口										

应用

步骤4 单击“应用”，使所设置的端口镜像进行生效。

——结束

4.4 创建端口隔离组

端口隔离组是采用端口隔离特性实现端口之间的隔离。将需要进行隔离的端口加入到一个隔离组中，可以实现隔离组内端口之间二层数据的隔离。端口隔离组功能提供了更安全、灵活的组网方案。

步骤1 在左侧导航中选择“端口隔离组”，进入端口隔离组设置页面。

端口隔离组

端口隔离组 1~16

组号

端口	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2
----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

创建

端口隔离组列表

组号	端口表	修改	删除
----	-----	----	----

步骤2 设置隔离组的组号，如设置“组号”为“1”。

说明：最多只能创建 16 个端口隔离组，“组号”的取值范围为 1~16。

步骤3 选择隔离组的成员端口。

如，需将 FE1、FE2 和 FE3 隔离，则选择 FE1、FE2 和 FE3。

端口隔离组

端口隔离组 1~16

组号

1

端口	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2
----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

创建

端口隔离组列表

组号	端口表	修改	删除
----	-----	----	----

步骤4 单击“创建”。
您所创建的隔离组在“端口隔离组列表”中显示。FE1、FE2 和 FE3 两两之间互不通信。

端口隔离组

端口隔离组 1~16

组号

端口

FE1

FE2

FE3

FE4

FE5

FE6

FX2

FX1

GE1

GE2

创建

端口隔离组列表

组号	端口表	修改	删除
1	FE1-FE2-FE3-	修改	删除

步骤5 （可选）在“端口隔离组列表”中，单击某一隔离组“修改”列的 “修改”，可以修改该组的成员端口。
步骤6 （可选）在“端口隔离组列表”中，单击某一隔离组“删除”列的 “删除”，可以删除该隔离组。
——结束

4.5 创建端口聚合组

端口聚合是将多个物理连接当作一个单一的逻辑连接来处理，如将 4 个 100M 的端口捆绑后成为一个高达 400M 的连接。它允许两个交换机之间通过多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。同一聚合组内端口的基本配置应保持一致。

步骤1 在左侧导航中选择“端口聚合”，进入端口聚合设置页面。

端口聚合

端口聚合

组号

T1

模式

manual

端口

FE1

FE2

FE3

FE4

FE5

FE6

FE7

FE8

创建

聚合列表

组号	模式	端口表	修改	删除
----	----	-----	----	----

步骤2 设置端口聚合的组号、模式和端口。
如设置组号为“T1”，模式为“manual”，端口聚合成员为 FE1、FE2。

表 4-2 端口聚合参数

值	值域	描述
组号	T1~T4	选择需要设置的端口聚合组号。
模式	manual	选择聚合组的汇聚模式。 manual: 手工聚合组，只能手工设置或删除。
端口	如 FE1	选择聚合组的成员端口。同一聚合组内端口的基本配置应保持一致。 手工或静态聚合组必须包含至少一个端口，当聚合组只有一个端口时，只能通过删除聚合组的方式将该端口从聚合组中删除。

步骤3 单击“创建”。
您所创建的隔离组在“聚合列表”中显示。

聚合列表

组号	模式	端口表	修改	删除
T1	manual	FE1-FE2-	修改	删除

步骤4（可选）在“聚合列表”中，单击某一聚合组“修改”列的“修改”，可以修改该组的成员端口。

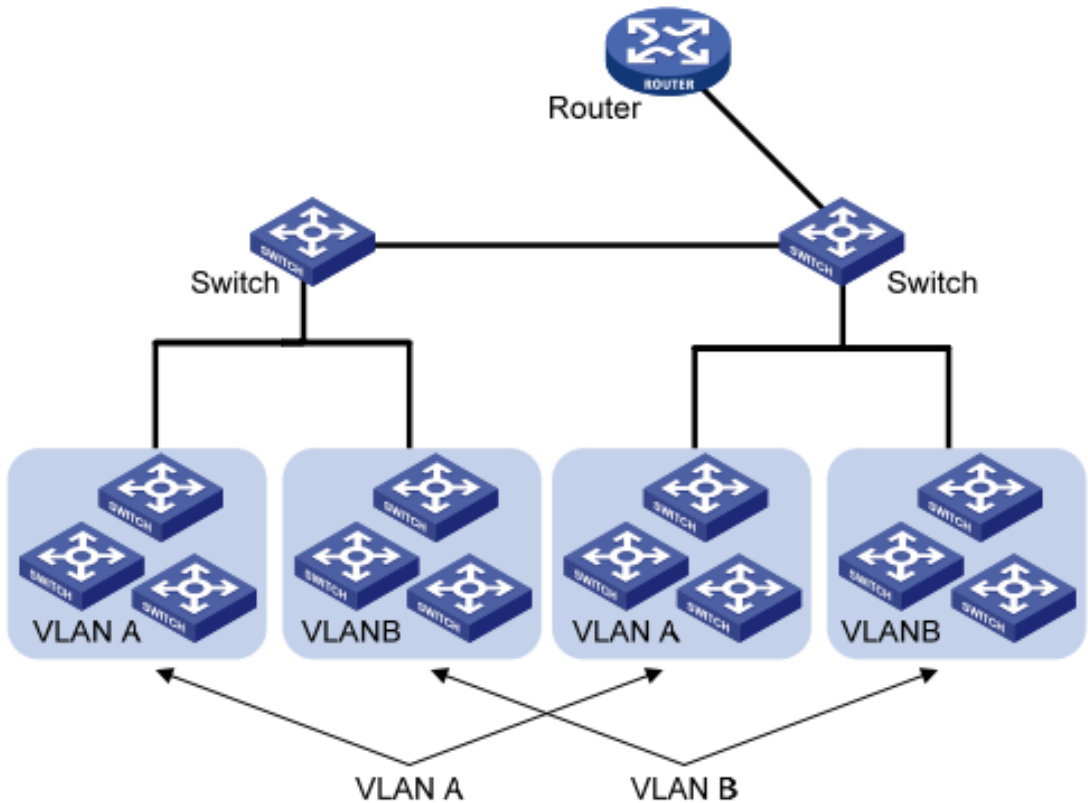
步骤5（可选）在“聚合列表”中，单击某一聚合组“删除”列的“删除”，可以删除该聚合组。

——结束

4.6 管理虚拟局域网

VLAN的概念

VLAN（Virtual Local Area Network，虚拟局域网）是一组逻辑上的设备和用户，这些设备和用户不受物理位置的限制，可以根据功能、部门及应用等因素设定为一个群组，使它们之间通信像在同一个物理分段中。处于不同 **VLAN** 内的主机之间通信必须通过路由器或三层交换机设备。



VLAN的优点

VLAN 的主要优点在于提供了一个网络分段系统，比传统网络具有更高的灵活性。使用 **VLAN** 的优点如下：

- 灵活创建虚拟工作组，使用 **VLAN** 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。
- 控制广播域的范围，局域网内的广播报文被限制在一个 **VLAN** 内，节省了带宽，提高了网络处理能力。
- 增强了 **LAN** 的安全性，由于报文在数据链路层被 **VLAN** 划分的广播域所隔离，因此各个 **VLAN** 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。

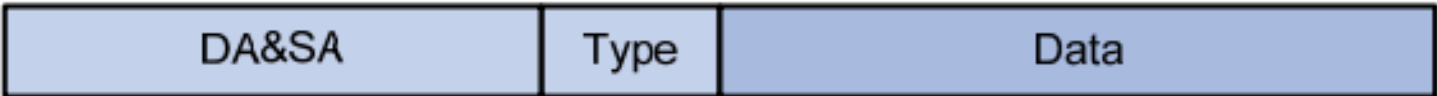
VLAN之间的通信

如果连接到一个 **VLAN** 中的设备要和另一个 **VLAN** 中的设备进行通信，需要安装连接双方 **VLAN** 的路由器或者第三层交换设备。只有当两边 **VLAN** 同时连接到路由器或者第三层交换设备后才能通信。

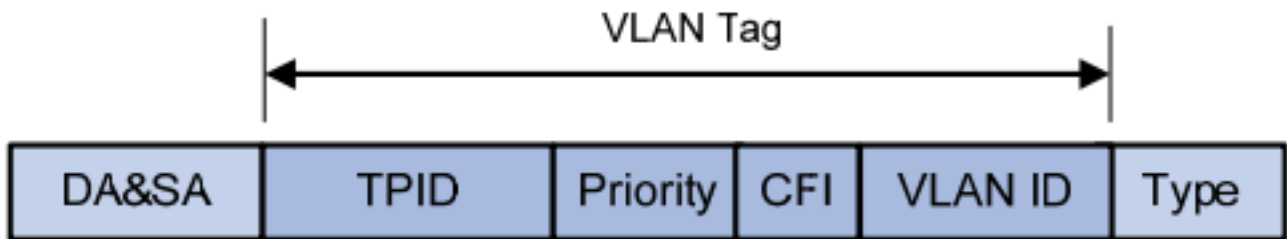
802.1Q VLAN

IEEE 802.1Q 协议，即 Virtual Bridged Local Area Networks 协议，主要规定 VLAN 的实现。802.1Q 协议为标识带有 VLAN 成员信息的以太网帧建立一种标准的方法。802.1Q VLAN 在报文中添加标识 VLAN 的字段，交换机在进行帧转发的同时判断 VLAN 是否匹配，从而确定其互通性。由于普通交换机工作在 OSI 模型的数据链路层，只能对报文的数据链路层封装进行识别。因此，如果添加识别字段，也需要添加到数据链路层封装中。

传统的以太网数据帧在目的 MAC 地址和源 MAC 地址之后封装的是上层协议的类型字段，如下图所示。



其中 DA 表示目的 MAC 地址，SA 表示源 MAC 地址，Type 表示报文所属协议类型。IEEE 802.1Q 协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。



VLAN Tag 包含以下四个字段：分别是 TPID(Tag Protocol Identifier, 标签协议标识符)、Priority、CFI (Canonical Format Indicator, 标准格式指示位) 和 VLAN ID。

- **TPID**: 标签协议标识符，Tag Protocol Identifie 的简称。用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。由于 TPID 字段在以太网报文中所处位置与不带 VLAN Tag 的报文中协议类型所处位置相同，为避免网络中转发和接收造成混乱，设备将不允许 TPID 配置为常用协议类型值。

常用以太网帧协议类型值协议类型对应取值如表 4-3 常用以太网帧协议类型值协议类型对应取值所示。

表 4-3 常用以太网帧协议类型值协议类型对应取值

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

- **Priority**: 定义用户优先级，包括 8 (0~7) 个优先级别。IEEE 802.1P 为 3bit 的用户优先级位定义了操作，0 的优先级最低，7 的优先级最高。
- **CFI**: 标识 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1bit。取值为 0 时，表示 MAC 地址以标准格式进行封装；取值为 1 时，表示以非标准格式封装。缺省取值为 0。
- **VLAN ID**: 简称 VID，对 VLAN 的识别字段，长度为 12 位。支持 4096VLAN 的识别取值范围为 0~4095。在 4096 可能的 VID 中，VID=0 用于识别帧优先级，4095 (FFF) 作为预留给值，所以 VLAN ID 的取值一般使用 1~4094。网络设备利用 VID 来识别报文所属的 VLAN，根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 值，来对报文进行处理。

4.6.1. 使能802.1Q VLAN

要使所划分的 VLAN 组生效，您必须使能 802.1Q VLAN 功能。

步骤1 在左侧导航中选择“虚拟局域网 < VLAN 全局”，进入 VLAN 全局设置页面。

VLAN全局

802.1Q VLAN

Disabled

VLAN TPID

0x8100

应用

步骤2 在“802.1Q VLAN”中选择“Enabled”。

表 4-4 VLAN 全局参数

值	值域	描述
802.1Q VLAN	Enabled, Disabled 缺省值: Disabled	启用或禁用 802.1Q VLAN。 Enable：表示启用 802.1Q VLAN。 Disabled：表示禁用 802.1Q VLAN。
VLAN TPID	取值范围为: 0x0001~0xffff 缺省值: 0x8100	设置 TPID 的值。 由于 TPID 字段在以太网报文中所处位置与不带 VLAN Tag 的报文中协议类型所处位置相同, 为避免网络中转发和接收造成混乱, 设备将不允许 TPID 配置为常用协议类型值。常用以太网帧协议类型值协议类型对应取值请参见“表 4-3 常用以太网帧协议类型值协议类型对应取值”。

步骤3 单击“应用”，使能 802.1Q VLAN 功能。

——结束

4.6.2. 创建802.1Q VLAN组

根据功能、部门及应用等因素可以创建不同的 VLAN 组，实现同一 VLAN 组内的主机可以互相通信， VLAN 组之间主机通信必须通过路由器或三层交换机设备。

步骤1 在左侧导航中选择“虚拟局域网 < 802.1Q VLAN”进入 VLAN 创建页面。

802.1Q VLAN

802.1Q 端口

802.1Q VLAN 配置

VID

端口

FE1FE2FE3FE4FE5FE6FX2FX1GE1GE2

模式

--- -- -- -- -- -- -- -- -- --

创建

*备注:UnTagged-此端口是VLAN成员,出去的帧无标记;Tagged-此端口是VLAN成员,出去的帧加标记; - - -此端口不是VLAN成员.

VLAN列表

VID	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2	修改	删除
1	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	修改	---

步骤2 设置 VLAN 组号和成员端口。

表 4-5 802.1Q VLAN 配置参数

值	值域	描述
VID	取值范围: 1~4094	设置所创建 VLAN 组的 ID。

模式	Untagged， Tagged， --- 缺省值： ---	设置所创建 VLAN 的成员端口和成员端口发送的帧是否带 VLAN 标识。一个端口可以同时属于多个 VLAN 组。 Untagged：表示设置该端口为 VLAN 组成员且发送的帧不带 VLAN 标识。 Tagged：表示设置该端口为 VLAN 组成员且发送的帧带有 VLAN 标识。 ---：表示设置该端口不属于 VLAN 组成员。
----	--------------------------------------	---

如，需要创建一个 ID 为 2 且成员端口为 FE1 和 FE2 的 VLAN 组，则设置“VID”为 2， FE1 和 FE2 的“模式”为“Tagged”或“Untagged”，如下图所示。

802.1Q VLAN

802.1Q 端口

802.1Q VLAN 配置

VID

2

端口	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2
模式	Untagged	Untagged	---	---	---	---	---	---	---	---

创建

*备注:UnTagged-此端口是VLAN成员,出去的帧无标记;Tagged-此端口是VLAN成员,出去的帧加标记; -- -此端口不是VLAN成员.

步骤3 单击“创建”。
您所创建的隔离组在“VLAN 列表”中显示。

802.1Q VLAN

802.1Q 端口

802.1Q VLAN 配置

VID

端口	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2
模式	---	---	---	---	---	---	---	---	---	---

创建

*备注:UnTagged-此端口是VLAN成员,出去的帧无标记;Tagged-此端口是VLAN成员,出去的帧加标记; -- -此端口不是VLAN成员.

VLAN列表

VID	FE1	FE2	FE3	FE4	FE5	FE6	FX2	FX1	GE1	GE2	修改	删除
1	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	修改	---
2	Untagged	Untagged	---	---	---	---	---	---	---	---	修改	删除

步骤4 （可选）在“VLAN 列表”中，单击某一 VLAN 组“修改”列的 “修改”，可以修改该 VLAN 组的成员端口。

步骤5 （可选）在“VLAN 列表”中，单击某一 VLAN 组“删除”列的 “删除”，可以删除该 VLAN 组。

说明：“VID”为“1”的 VLAN 组为系统缺省自带的 VLAN 组，每个端口都是该组的成员。该 VLAN 组支持修改该 VLAN 组的成员或端口模式，不可删除。

——结束

4.6.3. 设置端口的VLAN属性

当交换机端口接收到的报文不带有 VLAN Tag 时，交换机会自动为该报文分配一个 VID，这个 VID 就是端口缺省的 VLAN ID，简称 PVID。每个端口只能有一个端口 VLAN ID（PVID）。当不带标签的以太网数据包到达端口时，它将被打上 PVID VID 标签。您可以在“802.1Q 端口”中设置该 VLAN 成员端口的 PVID 和端口接收的帧类型。

步骤1 在左侧导航中选择“虚拟局域网 < 802.1Q VLAN”。

步骤2 单击“802.1Q 端口”页签，进入端口 VLAN 参数设置页面。

802.1Q VLAN

802.1Q 端口

端口	PVID (1~4094)	帧类型
FE1	1	Tag+Untag
应用		

Vlan 列表

端口	PVID	帧类型	端口	PVID	帧类型
FE1	1	Tag+Untag	FE2	1	Tag+Untag
FE3	1	Tag+Untag	FE4	1	Tag+Untag
FE5	1	Tag+Untag	FE6	1	Tag+Untag
FE7	1	Tag+Untag	FE8	1	Tag+Untag
GE1	1	Tag+Untag	GE2	1	Tag+Untag

步骤3 设置所需端口的 PVID 和帧类型。
如在[创建 802.1Q VLAN 组](#)中已创建“VID”为“2”的 VLAN 组，FE1 和 FE2 间互相通信且发送的报文不被其他端口获取，则需要把它们的 PVID 设置为“2”。

表 4-6 802.1Q 端口参数

值	值域	描述
端口	如 FE1	选择所需修改的端口。
PVID	取值范围： 1~4094 缺省值：1	设置基于端口缺省的 VLAN ID。
帧类型	Tag+Untag， Only_Tag 缺省值： Tag+Untag	设置该端口接收的帧类型。 Tag+Untag：表示设置该端口接收所有类型的帧。 Only_Tag：表示设置该端口只接收带有 VLAN 标识的帧。

步骤4 单击“应用”。
您所修改的端口属性在“VLAN 列表”中显示。

802.1Q VLAN

802.1Q 端口

端口	PVID (1~4094)	帧类型
FE1	2	Tag+Untag
应用		

Vlan 列表

端口	PVID	帧类型	端口	PVID	帧类型
FE1	2	Tag+Untag	FE2	2	Tag+Untag
FE3	1	Tag+Untag	FE4	1	Tag+Untag
FE5	1	Tag+Untag	FE6	1	Tag+Untag
FE7	1	Tag+Untag	FE8	1	Tag+Untag
GE1	1	Tag+Untag	GE2	1	Tag+Untag

——结束

4.6.4. 使能QinQ

QinQ 技术〔也称 StaCKed VLAN 或 Double VLAN〕，实现将用户私网 VLAN Tag 封装在公网 VLAN Tag 中，时报文带着两层 VLAN Tag 穿越运营商的骨干网络（公网）。不同用户网络的报文在公网传输时被完全分开，即使两个用户网络的 VLAN 范围存在重叠，在公网传输时也不会

产生混淆。基于端口的 QinQ 实现当该端口接收到报文，无论报文是否带有 VLAN Tag，交换机都会为该报文打上本端口缺省 VLAN 的 VLAN Tag。这样，如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是 untagged 的报文，该报文就成为带有端口缺省 VLAN Tag 的报文。您可以根据实际情况使能 QinQ 功能。

步骤1 在左侧导航中选择“虚拟局域网 < QinQ”，进入 QinQ 设置页面。

QinQ

端口	QinQ 使能
FE1	Disabled
应用	

QinQ 列表

端口	QinQ 状态	端口	QinQ 状态
FE1	Disabled	FE2	Disabled
FE3	Disabled	FE4	Disabled
FE5	Disabled	FE6	Disabled
FE7	Disabled	FE8	Disabled
GE1	Disabled	GE2	Disabled

步骤2 选择需要设置的端口并设置该端口的 QinQ 使能状态。

步骤3 单击“应用”，使所设置的端口 QinQ 生效并保存到 QinQ 列表中。

——结束

4.7 设置服务质量

QoS（Quality of Service，服务质量）是用来描述网络的服务质量和数据优先权的，可以解决网络延迟和阻塞等问题。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

4.7.1. QoS

QoS 是网络与用户之间以及网络上互相通信的用户之间关于信息传输与共享的质的约定，例如，传输延迟允许时间、最小传输画面失真度以及声像同步等，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

在互联网早期，各种数据都是平等的，网络带宽属于先来先得的自由抢占资源。随着互联网上数据类型的增加，对数据优先级需求也开始提出，比如对音频数据的实时性就要比视频数据高；而且付费用户希望自己的数据的发送优先权要高于免费用户。这些需求，促使了 QoS 的进一步研究和发展。

本设备提供了 QoS 优先级设置，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，减少对诸如语音或视频等对时间敏感业务的延迟。

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发送队列，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。

本设备提供以下两种调度机制：

- 严格优先级：该方式优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。
- 加权轮询（8:4:2:1）：该方式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，: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。

4.7.2. 设置QoS优先级协议

本设备为 QoS 优先级提供了 802.1P、Port_prio 和 DSCP 三种协议。在 QoS 全局中，您可以设置交换机 QoS 优先级所遵循的协议。

步骤1 在左侧导航中选择“质量服务 < QoS 配置”，进入 QoS 全局设置页面。

全局

QoS 端口配置

优先级选择

优先级

802.1P

应用

步骤2 在“优先级”中选择所需遵循的协议。

表 4-7 优先级协议

值	值域	描述
优先级	Port_Prio, 802.1P, DSCP 缺省值: 802.1P	选择所需遵循的协议。 Port_Prio: 基于端口的优先级，共 8 个优先级 0~7，0 优先级最低，7 优先级最高。您可以根据“4.7.3 设置 QoS 端口优先级”设置端口的优先级。 802.1P: 802.1P 是 IEEE 802.1Q（VLAN 标签技术）标准的扩充协议，它们协同工作。IEEE 802.1Q 标准定义了为以太网 MAC 帧添加的标签。VLAN 标签有两部分：VLAN ID（12 比特）和优先级(3 比特)。因此 802.1P 共 8 个优先级 0~7，0 优先级最低，7 优先级最高。802.1P 为二层交换机提供流量优先级，根据二层报文所携带的优先级在交换机内部进行 CoS（Class of Service）重映射，根据映射后的优先级进入队列发送。您可以根据“4.7.7 设置 CoS 重映射”设置本设备的 CoS 重映射。 DSCP: DSCP(Differentiated Services Code Point, 差分服务编码点) 使用 IP 报头中的 ToS 中的前 6 个比特来携带报文的分类信息，共有 64 个优先级 0~63，0 优先级最低，63 优先级最高。DSCP 使用 64 个值来对应用户定义的服务级别，可以让您确立更多的对网络流量的控制。您可以根据“4.7.6 设置 DSCP 队列映射”设置本设备内部的 DSCP 队列映射。

步骤3 单击“应用”，启用所选择的的协议。

——结束

4.7.3. 设置QoS端口优先级

本设备为每个端口提供 8 个优先级，即 0~7。其中，0 优先级最低，7 优先级最高。在使用“Port_Prio”优先级协议时，您可以根据实际使用情况设置端口优先级。

步骤1 在左侧导航中选择“质量服务 < QoS 配置”。

步骤2 单击“QoS 端口配置”页签，进入端口优先级设置页面。

全局

QoS 端口配置

端口

FE1

端口优先级

0

应用

端口优先级

端口	端口优先级	端口	端口优先级
FE1	0	FE2	0
FE3	0	FE4	0
FE5	0	FE6	0
FE7	0	FE8	0
GE1	0	GE2	0

步骤3 选择需要设置的端口并设置该端口的优先级。
如将端口 **FE1** 的优先级设置为 “3”。

步骤4 单击 “应用”，使所设置的参数生效并保存到端口优先级列表中。

全局

QoS 端口配置

端口

FE1

端口优先级

3

应用

端口优先级

端口	端口优先级	端口	端口优先级
FE1	3	FE2	0
FE3	0	FE4	0
FE5	0	FE6	0
FE7	0	FE8	0
GE1	0	GE2	0

——结束

4.7.4. 设置调度机制

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。本设备提供严格优先级和加权轮询（8:4:2:1）两种调度机制。您可以根据实际情况进行设置所需的调度机制。

步骤1 在左侧导航中选择 “质量服务 < 调度机制”，进入调度机制设置页面。

调度机制

调度模式

调度模式选择

严格优先级

应用

步骤2 在 “调度模式选择” 中选择所需遵循的协议。

表 4-8 优先级参数

值	值域	描述
调度模式选择	严格优先级， 加权轮询 (8:4:2:1) 缺省值：严格 优先级	选择所需遵循的协议。 严格优先级：按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样低优先级队列就不能发送任何帧，但是可以保证高优先级帧能够尽快发送。 加权轮询(8:4:2:1)：对于所有的业务流在排队等待调度的队列，根据每个队列配置的权值与所有的业务流在排队等待调度的队列的权值总和按照 8, 4, 2, 1 权值来分配带宽。这样就避免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。

步骤3 单击“应用”，启用所选择的的协议。
——结束

4.7.5. 设置发送队列

当缺省的 802.1p 优先级和本地优先级的映射关系不能满足需求时，您可以修改 802.1p 优先级到本地优先级的映射关系，从而实现 802.1p 优先级和发送队列之间映射关系的改变，将不同优先级的报文放入相应的发送队列进行调度。

步骤1 在左侧导航中选择“质量服务 < 发送队列”，进入发送队列设置页面。

发送队列

发送队列设置

优先级	0	1	2	3	4	5	6	7
发送队列	☒ Q0	☒ Q0	☐ Q0	☐ Q0	☐ Q0	☐ Q0	☐ Q0	☐ Q0
	☐ Q1	☐ Q1	☒ Q1	☒ Q1	☐ Q1	☐ Q1	☐ Q1	☐ Q1
	☐ Q2	☐ Q2	☐ Q2	☐ Q2	☒ Q2	☒ Q2	☐ Q2	☐ Q2
	☐ Q3	☐ Q3	☐ Q3	☐ Q3	☐ Q3	☐ Q3	☒ Q3	☒ Q3

应用

步骤2 根据实际情况选择优先级的所属发送队列。
本设备缺省的优先级与发送队列的映射关系如表 4-9 所示。

表 4-9 802.1P 优先级与发送队列缺省对应关系

802.1p 优先级	发送队列
0	Q0
1	Q0
2	Q1
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

步骤3 单击“应用”，保存所设置的优先级队列。
——结束

4.7.6. 设置DSCP队列映射

DSCP 在每个数据包 IP 头部的服务类别 TOS 标识字节中，利用已使用的 6 比特和未使用的 2 比特字节，通过编码值来区分优先级。DSCP 的取值范围为 0~63。您可以根据实际情况设置 DSCP 各个值所属的队列。

步骤1 在左侧导航中选择“质量服务 < DSCP 队列映射”，进入 DSCP 队列映射设置页面。

DSCP 队列映射

DSCP 队列映射设置

DSCP 队列映射	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
发送队列	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DSCP 队列映射	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发送队列	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
DSCP 队列映射	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
发送队列	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
DSCP 队列映射	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
发送队列	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

步骤2 设置需修改 DSCP 值的所属队列。
步骤3 单击“应用”，保存所设置的 DSCP 队列映射。
——结束

4.7.7. 设置CoS重映射

CoS 重映射是指各端口接收到携带有 802.1P 标识的数据包时根据本设备内部 CoS 值进行一一对应，重新赋一个 802.1P 值，将旧的 802.1P 标识信息丢失，按照映射后的 CoS 值分配到所属队列中进行发送。

步骤1 在左侧导航中选择“质量服务 < CoS 重映射”，进入 CoS 重映射设置页面。

CoS 重映射

CoS 重映射列表

端口	0	1	2	3	4	5	6	7	修改
FE1	0	1	2	3	4	5	6	7	修改
FE2	0	1	2	3	4	5	6	7	修改
FE3	0	1	2	3	4	5	6	7	修改
FE4	0	1	2	3	4	5	6	7	修改
FE5	0	1	2	3	4	5	6	7	修改
FE6	0	1	2	3	4	5	6	7	修改
FE7	0	1	2	3	4	5	6	7	修改
FE8	0	1	2	3	4	5	6	7	修改
GE1	0	1	2	3	4	5	6	7	修改
GE2	0	1	2	3	4	5	6	7	修改

步骤2 设置需修改端口的 CoS 重映射。
步骤3 单击“提交”，保存所设置的 CoS 重映射。
——结束

4.8 管理转发地址

以太网交换机在转发数据前必须知道它的每一个端口所连接的主机的 MAC 地址，构建出一个 MAC 地址表。当交换机从某个端口收到数据帧后，读取数据帧中封装的目的地 MAC 地址信息，然后查阅事先构建的 MAC 地址表，找出和目的地地址相对应的端口，从该端口把数据转发出去，其他端口则不受影响，这样避免了与其它端口上的数据发生碰撞。因此构建 MAC 地址表是交换机的首要工作。本设备提供配置静态单播地址、静态多播地址和 IGMP Snooping 的功能。

4.8.1. 设置老化时间

老化时间是一个影响交换机学习进程的参数。从一个地址记录加入地址表以后开始计时，如果在老化时间内各端口未收到源地址为该 MAC 地址的帧，那么，这些地址将从动态转发地址表中被删除。静态 MAC 地址表不受地址老化时间影响。

本设备老化时间的取值范围从 1~255 （*15）秒，缺省值为 20。老化时间过长，会导致交换机内的 mac 地址表超期，从而使交换机做出一些不正确的过滤/转发决定。老化时间过短，会造成地址表刷新太快，大量接收到的数据包的目的地址在 mac 地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这样大大地削弱了交换机的优点。

步骤1 在左侧导航中选择“转发地址 < 老化时间”，进入老化时间设置页面。

老化时间

Aging 使能

Enable

Aging Value

20

1-255(*15s)

应用

步骤2 在“Aging 使能”中选择“Enable”，启用老化时间。

步骤3 在“Aging Value”中设置 MAC 地址的老化时间。

表 4-10 老化时间参数

值	值域	描述
Aging 使能	Enable, Disable 缺省值： Enable	启用或禁用 MAC 地址老化时间。 Enable：表示启用 MAC 地址老化时间，老化时间超时后，动态 MAC 地址从 MAC 地址表中删除。 Disable：表示禁用 MAC 地址老化时间，动态 MAC 地址不会被删除。
aging value	取值范围： 1~255(*15 s) 缺省值：20	设置动态 MAC 地址的老化时间。只有在启用老化时间后才可以设置老化时间，“0”表示禁用老化时间。

步骤4 单击“应用”，使所设置的参数生效。

——结束

4.8.2. 设置单播MAC地址

单播是主机之间“一对一”的通讯模式，当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文从该表项中的转发出端口发送。单播 MAC 地址提供配置目的 MAC 地址与端口一一对应的功能，手动配置静态 MAC 地址表。配置某一端口与某一 MAC 地址对应后，目的地址为该 MAC 地址的报文只能从所对应的端口转发，而不进行广播。若使所配置的单播 MAC 地址表生效，您需是使能 VLAN，使能 VLAN 的具体步骤请参见“4.6.1 使能 802.1Q VLAN”。

步骤1 在左侧导航中选择“转发地址 < 单播 MAC 地址”，进入单播 MAC 地址设置页面。

单播MAC地址

转发地址表

VID	单播MAC地址[xx-xx-xx-xx-xx-xx]	端口	类型
1		FE1	静态

应用

*备注:如果想让这mac地址生效，你必须先使能VLAN.

MAC地址列表

VID	单播MAC地址	端口	类型	修改	删除
-----	---------	----	----	----	----

步骤2 设置单播 MAC 地址的 VID、MAC 地址和端口信息。

表 4-11 老化时间参数

值	值域	描述
VID	如 1	选择需要配置单播 MAC 地址的 VLAN ID。所选择的 VID 必须在 VLAN 列表中存在。
单播 MAC 地址	格式： XX-XX-XX-XX-X X-XX 如： 00-00-00-00-00-01	设置静态单播 MAC 地址。
端口	如 FE1	选择与单播 MAC 地址一一对应的端口。

步骤3 单击“应用”，保存所设置的 MAC 地址到单播 MAC 地址列表中。

单播MAC地址

转发地址表

VID	单播MAC地址[xx-xx-xx-xx-xx]	端口	类型
1		FE1	静态
应用			

“备注:如果想让这mac地址生效，你必须先使能VLAN.

MAC地址列表

VID	单播MAC地址	端口	类型	修改	删除
1	00-00-00-00-00-01	FE1	Static	修改	删除

步骤4 （可选）在“MAC 地址列表”中，单击某一单播 MAC 地址“修改”列的 “修改”，可以修改该单播 MAC 地址所对应的端口。

步骤5 （可选）在“MAC 地址列表”中，单击某一单播 MAC 地址“删除”列的 “删除”，可以删除该单播 MAC 地址的信息。

——结束

4.8.3. 设置多播MAC地址

多播是主机之间“一对多”的通讯模式，也就是目的 MAC 地址不是一个具体的接收者，而是一个成员不确定的组。若使所配置的多播 MAC 地址表生效，您需是使能 VLAN，使能 VLAN 的具体步骤请参见“4.6.1 使能 802.1Q VLAN”。

步骤1 在左侧导航中选择“转发地址 < 多播 MAC 地址”，进入多播 MAC 地址设置页面。

多播MAC地址

静态多播转发表

VID

1

多播MAC地址

[xx-xx-xx-xx-xx-xx]

端口

FE1

FE2

FE3

FE4

FE5

FE6

FE7

FE8

GE1

GE2

应用

*备注:如果想让这mac地址生效，你必须先使能VLAN.

MAC地址列表

VID	多播MAC地址	端口	修改	删除
-----	---------	----	----	----

步骤2 设置多播 MAC 地址的 VID、MAC 地址和成员端口。

表 4-12 老化时间参数

值	值域	描述
VID	如 1	选择需要配置多播 MAC 地址的 VLAN ID。所选择的 VID 必须在 VLAN 列表中存在。
多播 MAC 地址	格式： XX-XX-XX-XX-X X-XX 如： 01-00-00-00-00-00	设置静态多播 MAC 地址。
端口	如 FE1	选择与多播 MAC 地址对应的端口。可以同时选择多个端口。

步骤3 单击“应用”，保存所设置的 MAC 地址到多播 MAC 地址列表中。

多播MAC地址

静态多播转发表

VID

1

多播MAC地址

[xx-xx-xx-xx-xx-xx]

端口

FE1

FE2

FE3

FE4

FE5

FE6

FE7

FE8

GE1

GE2

应用

*备注:如果想让这mac地址生效，你必须先使能VLAN.

MAC地址列表

VID	多播MAC地址	端口	修改	删除
1	01-00-00-00-00-00	FE1-FE2-	修改	删除

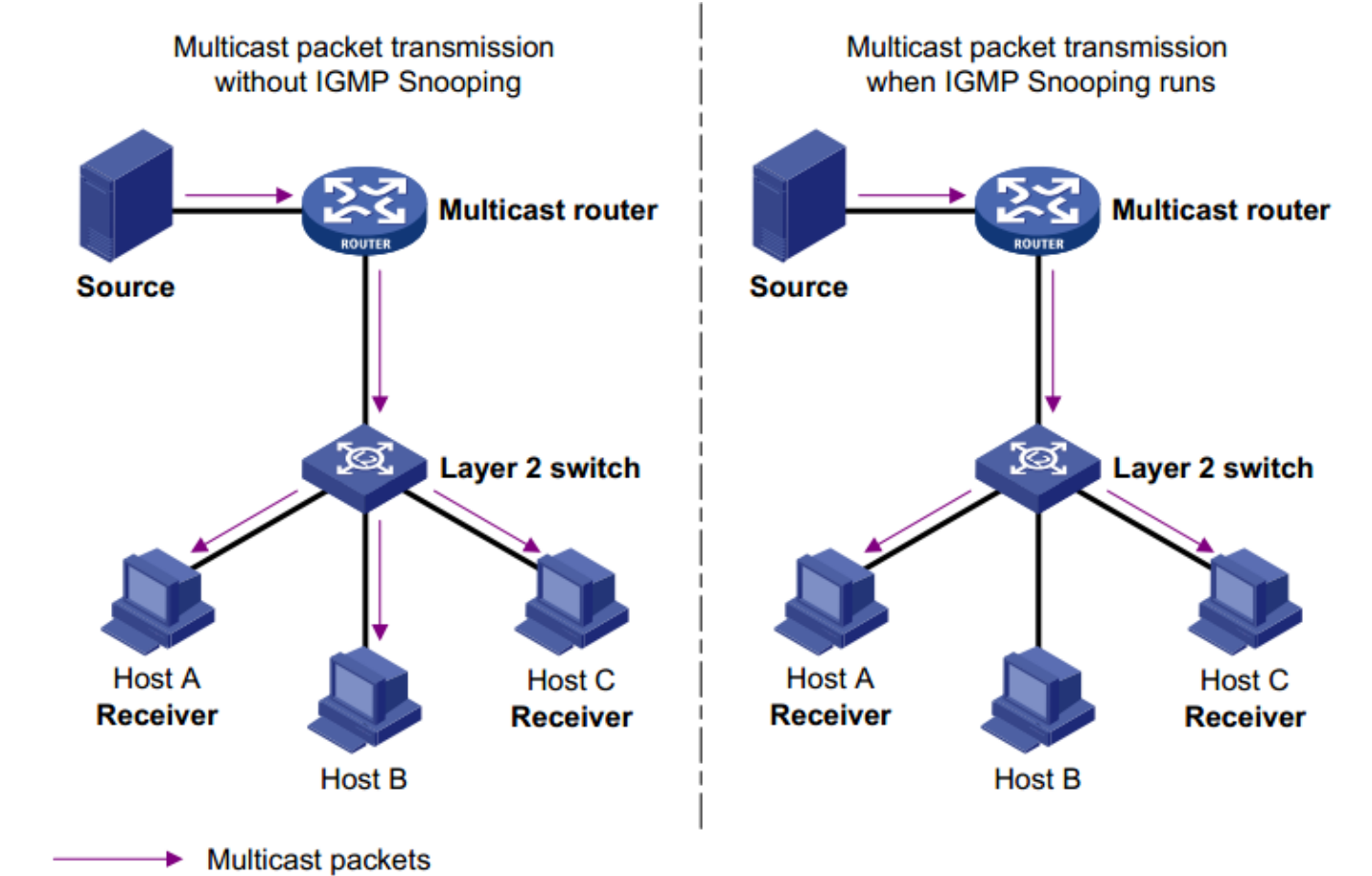
步骤4 （可选）在“MAC 地址列表”中，单击某一多播 MAC 地址“修改”列的 “修改”，可以修改该多播 MAC 地址所对应的成员端口。

步骤5 （可选）在“MAC 地址列表”中，单击某一多播 MAC 地址“删除”列的 “删除”，可以删除该多播 MAC 地址的信息。

——结束

4.8.4. 设置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。运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。如下图所示，当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。



- IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：
- 减少了二层网络中的广播报文，节约了网络带宽。
 - 增强了组播信息的安全性。
 - 为实现对每台主机的单独计费带来了方便。

步骤1 在左侧导航中选择“转发地址 < IGMP Snooping”，进入 IGMP Snooping 设置页面。

组播侦听

路由端口

组播杂项

IGMP Snooping

IGMP Snooping 使能

应用

Disabled

创建 Multicast VID

1

创建

删除

成员组列表

Multicast VID	IP	Memble Port
---------------	----	-------------

步骤2 使能 IGMP Snooping 并创建多播 VLAN。

1. 单击“组播侦听”页签。

表 4-13 组播侦听参数

值	值域	描述
IGMP Snooping 使能	Enabled, Disabled 缺省值: Disabled	启用或禁用 IGMP Snooping。 Enable: 表示启用 IGMP Snooping。 Disabled: 表示禁用 IGMP Snooping。

创建 Multicast VID	如 1	选择需要加入 IGMP Snooping 组播 VLAN 的 VLAN ID。所选择的 VID 必须在 VLAN 列表中存在。
------------------	-----	---

2. 在“IGMP Snooping 使能”中选择“Enabled”。
3. 单击“应用”，使能 IGMP Snooping。
4. 在“创建 Multicast VID”中选择需要加入多播 VLAN 组的 VID。
5. 单击“创建”，把所选的 VLAN 加入到 IGMP Snooping 的 Multicast VLAN 中。
6. （可选）选择需要删除的 Multicast VLAN，单击“删除”，可删除已该 Multicast VLAN。

步骤3 创建静态路由端口。

 说明：IGMP Snooping 启用后才能创建路由端口。

1. 单击“路由端口”页签。
2. 选择 Multicast VID 和路由端口。

表 4-14 路由端口参数

值	值域	描述
Multicast VID	如 1	选择在“组播侦听”中已创建的 Multicast VID。
路由端口	如 FE1	设置交换机上用于与路由器连接的端口。 路由端口即为交换机上与路由器连接的端口。

3. 单击“应用”，保存所创建的的路由端口到路由端口列表中。
- 设置组播侦听参数。

 说明：IGMP Snooping 启用后才能设置组播侦听参数。

1. 单击“组播杂项”页签。
2. 设置组播侦听的最大请求时间、路由端口老化时间和主机端口老化时间等参数。

表 4-15 组播侦听参数

值	值域	描述
最大请求时间	取值范围： 1~25 缺省值：10	设置主机收到 IGMP 查询报文后的最大响应时间。 超时后，交换机将该端口从组播组中删除。
路由端口老化时间	取值范围： 100~1000 缺省值：1000	设置路由端口从 IGMP Snooping 路由端口列表中删除的时间。 路由端口老化时间指交换机为每个路由端口都启动一个定时器，超过该时间则将路由端口从 IGMP Snooping 路由端口列表中删除。
主机端口老化时间	取值范围： 200~1000 缺省值：200	设置组播组成员端口从 IGMP Snooping 转发表中删除的时间。 主机端口老化时间指当一个端口加入某组播组时，交换机为该端口启动一个定时器，超过该时间则将该端口从 IGMP Snooping 转发表中删除。
IGMP 查询器	Enable, Disabled 缺省值： Disabled	启用或禁用 IGMP 查询器。 IGMP 查询器定期向本地网段内的所有主机与路由器发送 IGMP 通用查询报文，已查询该网段有哪些组播组的成员。
间隔时间	取值范围： 1~300 缺省值：100	设置 IGMP 查询器发送 IGMP 通用查询报文的时间间隔。

3. 单击“应用”，保存并使所设置的参数生效。

——结束

4.9 管理风暴抑制

当网络中有大量的广播/组播/单播流量通过以太网端口时，会在端口上产生流量风暴，可能导致网络的拥塞。在端口上配置了广播/组播/单播风暴抑制功能后，当端口上的广播/组播/单播流量超过所设置的抑制阈值时，系统会丢弃超出流量限制的报文，从而使端口的广播/组播/单播流量降低到限定范围内，保证网络业务的正常运行。您可以通过配置风暴控制，限制交换机上允许通过的广播/组播/单播流量的大小。

步骤1 在左侧导航中选择“风暴抑制”，进入风暴抑制设置页面。

风暴抑制

端口	流量类型	入口速度 (0=Disable)
FE1	None	0 62~100000 kbps

应用

Storm Limit List

端口	流量类型	入口速度	端口	流量类型	入口速度
FE1	None	0	FE2	None	0
FE3	None	0	FE4	None	0
FE5	None	0	FE6	None	0
FE7	None	0	FE8	None	0
GE1	None	0	GE2	None	0

步骤2 选择端口号，设置该端口所需抑制的流量类型和入口速度。

表 4-16 组播侦听参数

值	值域	描述
端口	如 FE1	选择需要设置风暴抑制的端口号。
流量类型	None, All ingress frames, Broad+Multi+uni, Broad+Multi, Broadcast 缺省值: None	设置该端口需要抑制的流量类型。 None: 表示禁用风暴抑制功能。 All ingress frames: 表示抑制通过端口的所有流量类型。 Broad+Multi+uni: 表示抑制通过端口的广播流量、多播流量和单播流量。 Broad+Multi: 表示抑制通过端口的广播流量和多播流量。 Broadcast: 表示抑制通过端口的广播流量。
入口速度 (0=Disable)	百兆端口取值范围: 62~100000k bps 千兆端口取值范围: 62~250000k bps 缺省值: 0	设置所抑制流量类型通过端口的速度。交换机会自动将所设置的值转换为与之最接近的速率。  说明: “0”时表示该端口无出口速率限制，发送数据在该端口上全速运行。由于交换机芯片内部的出口速率算法限制，千兆端口的出口速率最大取值为 250000kbps。

步骤3 单击“应用”，使所设置的参数生效并保存到风暴抑制列表中。

——结束

4.10 查看数据统计

为了能够直观的了解各端口的收发数据情况和交换机转发 MAC 地址表，本设备提供查看端口数据和 MAC 地址表功能。

4.10.1. 查看端口数据

“端口数据统计”显示每个端口的显示每个以太网端口的发送好报文数、发送坏报文数、接受好报文数、接受坏报文数和发送 FCS 错误报文数帧数等参数。

步骤1 在左侧导航中选择“数据统计 < 端口帧统计”，端口帧统计页面。

端口帧统计

数据包/端口	FE1	FE2	FE3	FE4	FE5	FE6	FE7	FE8	GE1	GE2
RxGood	0	0	0	0	0	0	0	2947	0	0
RxBad	0	0	0	0	0	0	0	0	0	0
TxFCSError	0	0	0	0	0	0	0	0	0	0
RxUnicasts	0	0	0	0	0	0	0	12	0	0
Deferred	0	0	0	0	0	0	0	0	0	0
RxBroadcasts	0	0	0	0	0	0	0	0	0	0
RxMulticasts	0	0	0	0	0	0	0	0	0	0
RT64	0	0	0	0	0	0	0	6	0	0
RT65~127	0	0	0	0	0	0	0	3	0	0
RT128~255	0	0	0	0	0	0	0	0	0	0
RT256~511	0	0	0	0	0	0	0	0	0	0
RT512~1023	0	0	0	0	0	0	0	3	0	0
RT1024~max	0	0	0	0	0	0	0	0	0	0
OutOctets	0	0	0	0	0	0	0	4523	0	0

步骤2 （可选）单击端口帧统计列表下方的 “重置”，可将端口帧统计列表中的数据清零。

端口帧统计

Single

TxPause	0	0	0	0	0	0	0	0	0	0
RxPause	0	0	0	0	0	0	0	0	0	0
Multiple	0	0	0	0	0	0	0	0	0	0
Undersize	0	0	0	0	0	0	0	0	0	0
Fragments	0	0	0	0	0	0	0	0	0	0
Oversize	0	0	0	0	0	0	0	0	0	0
Jabber	0	0	0	0	0	0	0	0	0	0
RxMACError	0	0	0	0	0	0	0	0	0	0
RxFCSError	0	0	0	0	0	0	0	0	0	0
RxDiscard	0	0	0	0	0	0	0	0	0	0
Late	0	0	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0	0	0
RxFilter	0	0	0	0	0	0	93	0	0	0
TxFilter	0	0	0	0	0	0	0	0	0	0

重置

——结束

4.10.2. 查看MAC地址表

MAC 地址表记录了交换机与其他相连的设备的 MAC 地址、端口号以及所属的 VLAN ID。在转发数据时，交换机根据报文中的目的 MAC 地址查询 MAC 地址表，快速定位出端口，从而减少广播。动态 MAC 地址为交换机端口通过 MAC 地址学习能力得来，超过老化时间将被删除；静态 MAC 地址为手工配置的 MAC 地址，不受老化时间影响。您可以通过在 web 界面左侧导航菜单中选择“数据统计 < MAC 地址表”进入“MAC 地址表”页面查看所需的信息。

MAC地址列表				
序号	VID	MAC 地址	端口	类型
1	1	00-16-ec-1a-f9-cd	FE7-	Dynamic
2	1	00-1e-90-9c-00-bb	FE7-	Dynamic
3	1	00-a1-d3-88-13-68	CPU	Static
4	1	00-e0-4c-28-10-87	FE7-	Dynamic
5	1	34-40-b5-8f-3c-3e	FE7-	Dynamic
6	1	9c-21-6a-3a-14-78	FE7-	Dynamic
7	1	b8-88-e3-eb-67-f4	FE7-	Dynamic
8	1	bc-5f-f4-c1-4a-6e	FE8-	Dynamic
9	1	d0-27-88-59-59-ff	FE7-	Dynamic
10	1	f0-de-f1-f8-91-3e	FE7-	Dynamic
11	1	ff-ff-ff-ff-ff-ff	FE1-FE2-FE3-FE4-FE5-FE6-FE7-FE8-GE1-GE2-CPU	Static

——结束

4.11 管理快速生成树

STP（Spanning Tree Protocol ）是生成树协议的英文缩写。STP 协议中定义了根桥（Root Bridge）、根端口（Root Port）、指定端口（Designated Port）、路径开销（Path Cost）等概念，用于通过构造一棵自然树的方法实现将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环，同时实现链路备份和路径最优化。

STP 采用 BPDU （Bridge Protocol Data Unit，桥协议数据单元）也称为配置消息，进行网桥之间的信息交流。 STP BDUP 是一种二层报文，目的 MAC 时多播地址 01-80-C2-00-00-00，所有支持 STP 协议的网桥都会接收并处理收到的 BPDU 报文。该报文的数据区里携带了用于生成树计算的所有有用信息。

根桥

树形的网络结构，必须要有树根，于是 STP 引入了根桥（Root Bridge）的概念。根桥在全网中只有一个，而且根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。网络收敛后，根桥会按照一定的时间间隔产生并向外发送配置 BPDU，其他的设备对该配置 BPDU 进行转发,从而保证拓扑的稳定.选举根桥的依据是网桥优先级和网桥MAC地址组合成的桥ID(Bridge ID)，桥 ID 最小的网桥将成为网络中的根桥。

根端口

所谓根端口，是指一个非根桥的设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。

指定桥与指定端口

指定桥与指定端口的含义，如表 4-17 指定桥与指定端口所示。

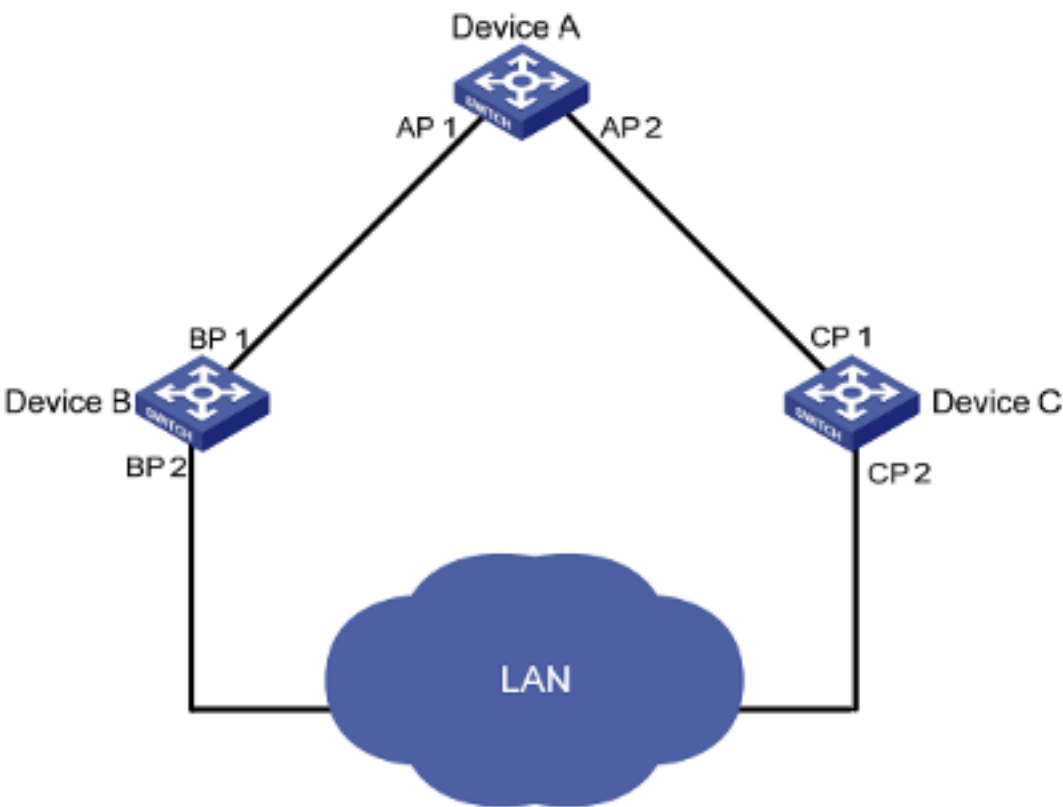
表 4-17 指定桥与指定端口

分类	指定桥	指定端口
对于一台设备而言	与交换机直接相连并且负责向交换机转发 BPDU 报文的设备。	指定桥向本机转发 BPDU 报文的端口。
对于一个局域网而言	负责向本网段转发 BPDU 报文的设备。	指定桥向本网段转发 BPDU 报文的端口。

指定桥与指定端口如下图所示，AP1 、AP2 、BP1 、BP2 、CP1 、CP2 分别表示设备 Device A、Device B、Device C 的端口。

- Device A 通过端口 AP1 向 Device B 转发配置消息，则 Device B 的指定桥就是 Device A，指定端口就是 Device A 的端口 AP1；
- 与局域网 LAN 相连的有两台设备：Device B 和 Device C，如果 Device B 负责向 LAN 转发

配置消息，则 LAN 的指定桥就是 Device B ，指定端口就是 Device B 的 BP2。



路径开销

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

快速生成树协议（Rapid Spanning Tree Protocol，简称 RSTP ）是从 STP 发展过来的，其实现基本思想一致，但它更进一步的处理了网络临时失去连通性的问题。RSTP 规定在某些情况下，处于 BloCKing 状态的端口不必经历 2 倍的 Forward Delay 时延而可以直接进入转发状态。如网络边缘端口（即直接与终端相连的端口），可以直接进入转发状态，不需要任何时延。或者是网桥旧的根端口已经进入 BloCKing 状态，并且新的根端口所连接的对端网桥的指定端口仍处于 Forwarding 状态，那么新的根端口可以立即进入 Forwarding 状态。即使是非边缘的指定端口，也可以通过与相连的网桥进行一次握手，等待对端网桥的赞同报文而快速进入 Forwarding 状态。

步骤1 在左侧导航中选择“快速生成树”，进入 RSTP 全局设置页面。

RSTP 全局		RSTP 桥	RSTP 端口属性
RSTP	Disabled		
Transmit Hold Count	6		
应用			

步骤2 使能 RSTP 协议并设置传输间隔。

1. 单击“RSTP 全局”页签。

表 4-18 RSTP 全局参数

值	值域	描述
RSTP	Enabled, Disabled 缺省值: Disabled	启用或禁用 RSTP 协议。 Enable: 表示启用 RSTP。 Disabled: 表示禁用 RSTP。

Transmit Hold Count	取值范围： 1~10 缺省值：6	设置 BPDU 的发送速率。 Transmit Hold Count 用来限制 BPDU 的发送速率，每发一个 BPDU，txCount+1，当发送 BPDU 的 txCount= Transmit Hold Count 时，延时发送 BPDU。
---------------------	------------------------	--

2. 在“RSTP”中选择“Enabled”。
3. 设置“Transmit Hold Count”的值。
4. 单击“应用”，使所设置的参数生效。

步骤3 设置网桥的参数。

 说明：RSTP 启用后才能设置网桥参数。

1. 单击“RSTP 桥”页签，进入 RSTP 网桥设置页面。
2. 设置网桥的优先级、最长老化时间和输出延迟时间。

表 4-19 RSTP 桥参数

值	值域	描述
优先级	取值范围： 0~65535s 缺省值： 32768	设置网桥的优先级。RSTP 会自动将所设置的值转换为与之最接近的 4096 的倍数。设置值越小，其优先级越高。 网桥优先级的大小决定了这个网桥是否能够被选择为整个交换网络的根网桥，通过配置较小的优先级可以指定某个网桥作为生成树的根。如果整个交换网络中所有网桥的优先级采用相同的值，则 MAC 地址最小的网桥将被选择为根网桥。
最长老化时间	取值范围： 6~40s 缺省值：20	设置 BPDU 的保存时间。 最长老化时间指网桥对 BPDU 信息保存的时间。如果超过最长老化时间，则对 BPDU 保存的信息失效，不能再用该 BPDU 计算根网桥、指定网桥和根端口等。 如果最大老化时间配置过小，生成树计算就会比较频繁，可能到时网络拥塞，误认为链路故障；配置过大，则可能不能及时发现链路故障，降到网络自适应能力，建议采用缺省值。
传输延迟时间	取值范围： 4~30s 缺省值：15	设置交换机状态迁移的延迟时间。 链路故障会引发网络重新进行生成树的计算。生成树的结构将发生相应的变化后，重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根端口和指定端口立刻就开始数据转发，则可能会造成暂时性的路径回环。为此，生成树协议采用了一种状态迁移的机制，根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 Forward Delay 延时后才能进入转发状态。这个延时保证了新的配置消息已经传遍整个网络。 交换机的 Forward Delay 特性与交换网络的网络直径有关，直径越大 Forward Delay 的时间就应该配置越长。如果 Forward Delay 配置过小，则可能会引入临时的冗余路径；如果 Forward Delay 配置过长，则可能导致网络较长时间不能回复。建议采用缺省值。

桥 ID	格式：优先级 -MAC 地址 不可设置	交换机自身的 ID。每台网桥都有一个网桥 ID。网桥 ID 由网桥优先级和网桥的 MAC 地址组成。网桥优先级是一个可配置的两字节字段，缺省值为 32768。网桥的 ID 值越低，越有可能成为根网桥。
根桥 ID	格式：优先级 -MAC 地址 不可设置	根桥的 ID。根网桥 ID 由根网桥优先级和根网桥的 MAC 地址组成。缺省情况下，根网桥优先级被配置为 32786。若网桥优先级相同，则使用较低 MAC 地址的网桥作为根网桥。
联络时间	如 2s 不可设置	BPDU 的发送间隔，缺省值为 2 秒。交换机每隔联络时间会向周围的交换机发送联络报文，以确认链路是否存在故障。 根桥定时向外发送配置 BPDU 报文，以维持现有生成树的稳定。如果在指定时间内交换机没有收到 BPDU 数据包，由于 BPDU 数据包超时，则生成树将被重新计算。当交换机成为根桥时，它将定时在联络时间所配置的时间间隔内发送 BPDU ，而其他非根桥交换机采用联络时间所指定的时间间隔。
根路径开销	如 2000 不可设置	此交换机到根桥的路径开销。因为网桥和网桥之间是以“接力”的形式来转发 BPDU 的，因此，通过将初始的路径开销加上每台网桥的端口优先级，来确定根网桥路径开销。

3. 单击“应用”，使所设置的参数生效。
- 步骤4 设置端口的参数。
-  说明：RSTP 启用后才能设置网桥参数。
1. 单击“RSTP 端口属性”页签，进入 RSTP 端口属性设置页面。
2. 设置端口的 McheCK、边缘端口配置和点对点等参数。

表 4-20 RSTP 端口属性参数

值	值域	描述
端口	如 FE1	选择需要设置参数的端口。
McheCK	Enabled, Disabled 缺省值： Enabled	启用或禁用端口的 McheCK 属性。 端口的 McheCK 属性用来检测运行在 STP 兼容模式下的端口是否可以转换到 RSTP 模式。通过设定 McheCK 可以检查与当前以太网端口相连的网段内是否还有运行 STP 协议的网桥存在。 如果在与当前以太网端口相连的网段内存在运行 STP 协议的网桥，RSTP 协议会将该端口的协议运行模式迁移到 STP 兼容模式。在网络比较稳定后，网段内运行 STP 协议的网桥被拆离，但 RSTP 协议仍然会运行在 STP 兼容模式下，通过设定 McheCK 变量可以迫使其迁移到 RSTP 模式下运行。 启用端口的 McheCK 功能之后，如果端口仍然运行在 STP 兼容模式，表示该端口所连接的网段存在 STP 网桥，否则该端口回到 RSTP 模式，表示该端口所连接的网段已经没有任何 STP 网桥。 Enabled：表示启用端口的 McheCK 功能。 Disabled：表示禁用端口的 McheCK 功能。

边缘端口配置	Auto, non-edge, edge 缺省值: Auto	设置端口是否可以作为边缘端口。 边缘端口指直接与终端用户相连的端口。边缘端口可以快速切换到转发状态，因为在边缘端口上，网络拓扑结构的变化不产生环路。通过把一个端口设置成边缘端口可以使其迅速切换到转发状态。 Auto: 表示 RSTP 协议自动检测端口为边缘端口或非边缘端口。 non-edge: 表示配置端口为非边缘端口。 edge: 表示配置端口为边缘端口。
点对点配置	Auto, shared, p2p 缺省值: Auto	设置端口是否与点对点链路相连。 端口只与一个网桥相连的链路是点对点链路，端口与多个网桥相连的链路是共享链路。链路类型对替换端口转换为根端口没有影响，指定端口快速迁移到转发状态只发生在点对点链路，除非是边缘端口。链路类型根据双工来判断，全双工为点对点链路，半双工为共享链路。 Auto: 表示 RSTP 协议自动检测与端口相连的链路类型。 shared: 表示配置端口与网桥相连的链路为共享链路。 p2p: 表示配置端口与网桥相连的链路为点对点链路。
路径开销	取值范围: 1~20000000 0 缺省值: 20000	设置该端口的路径开销。 以太网端口的路径开销与该端口的链路速率有关，链路速率越大，则应将参数配置得越小，RSTP 协议可以自动检测当前以太网端口的链路速率，并换算成相应的路径开销。配置以太网端口的路径开销会引起生成树重新计算。建议使用缺省值，让 RSTP 协议自己来计算当前以太网端口的路径开销。
优先级	取值范围: 0~240 缺省值: 128	设置端口的优先级。RSTP 会自动将所设置的值转换为与之最接近的 16 的倍数。 通过设定以太网端口的优先级可以指定特定的以太网端口包含在生成树内。配置的值越小，端口的优先级越高，该以太网端口就越有可能包含在生成树内。如果网桥所有的以太网端口采用相同的优先级，则以太网端口的优先级高低取决于该以太网端口的索引号。配置以太网端口的优先级会引起生成树重新计算。

3.单击“应用”，使所设置的参数生效。
——结束

4.12 创建环网

传统网络采用的是主干的方式，中间的任何一条连接线断掉，都至少会影响连接中的一个区域。这就给网络的安全性带来隐患。建立环网链路可以防止一处连接发生故障而影响整体网络。环网给数据通道提供了快速的故障恢复能力，其中最关键的就是小于 20ms 的保护倒换能力。在环中某一链路出故障时，传输交换机检测到链路故障会马上发送一个消息给主交换机，主交换机马上把被阻塞的端口解阻塞，迅速恢复数据的转发，环上的其他节点收到故障通告消息后，清空转发地址表；如果该节点有环上阻塞端口，则将该端口置为转发状态。故障恢复后，发现故障恢复的节点首先通过等待恢复时间来确认恢复，然后向环的两边通告故障恢复消息，并将与故障段相联的端口保持阻塞状态。

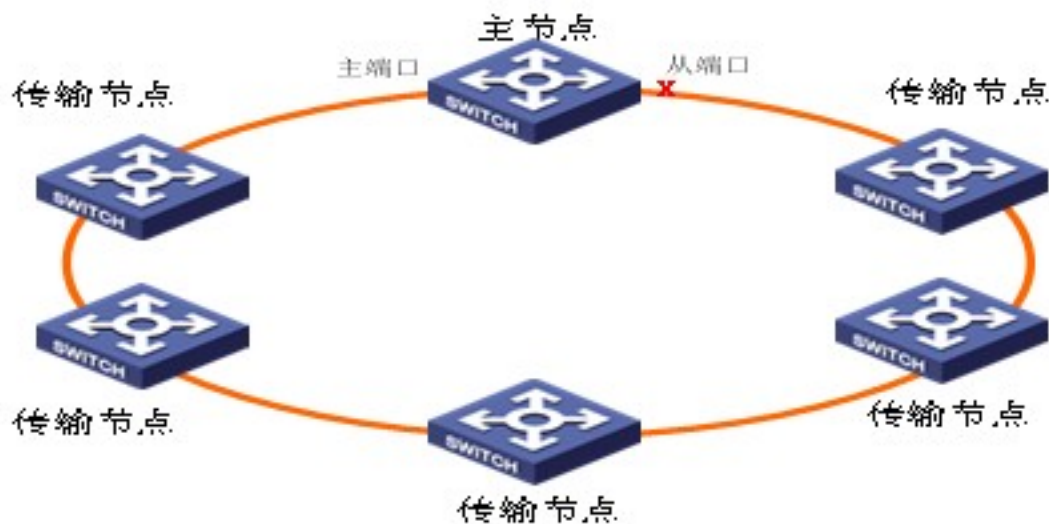
故障恢复后，发现故障恢复的节点首先通过等待恢复时间来确认恢复，然后向环的两边通告故障恢复消息，并将与故障段相联的端口保持阻塞状态。本设备提供单环、相交环和相切环三种环网模式。

主节点

主节点是环上的主要决策和控制节点。每个环上必须有一个主节点，而且只能有一个。主节点的环上端口分为主端口和从端口，环完整的情况下，通常阻断从端口。

传输节点

环上除主节点之外的其它节点都可以称为传输节点（边缘节点和辅助边缘节点实际上是特殊的传输节点）。一个环上可以有多个传输节点，如下图所示：



主端口和从端口

主节点和传输节点接入以太网环的两个端口中，一个为主端口，另一个为从端口，端口的角色由用户的配置决定。

主节点的主端口和从端口在功能上是有区别的。主节点从其主端口发送环路状态探测报文，如果能够从从端口收到该报文，说明本节点所在环网完整，因此需要阻塞从端口以防止数据环路；相反如果在规定时间内收不到探测报文，说明环网故障，此时需要放开从端口以保证环上所有节点的正常通信。传输节点的主端口和从端口在功能上没有区别。端口的角色同样由用户的配置决定。

4.12.1. 创建单环环网

介绍以太网单环环网的配置步骤。

如下图所示，SW1、SW2、SW3、SW4 在同一网络中，SW1 为主节点，SW2、SW3、SW4 为传输节点。

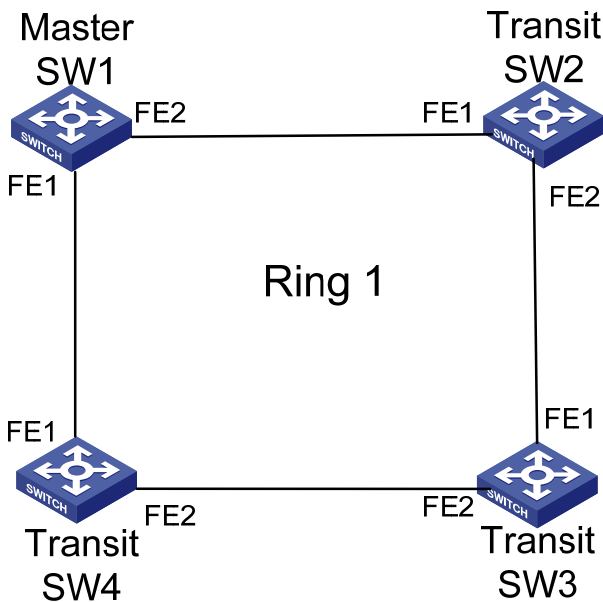


表 4-21 单环环网参数规划

交换机	环网 ID	节点模式	主端口	备用端口
SW1	1	Master	FE1	FE2
SW2	1	Transit	FE1	FE2
SW3	1	Transit	FE1	FE2
SW4	1	Transit	FE1	FE2

在物理连接各设备之前，需要先配置各设备的环网参数。

步骤1 登录 SW1，设置 SW1 的环网参数。

1. 登录 SW1 的 Web 配置页面，具体步骤请参见“2.3 通过 Web 浏览器访问”。
2. 在左侧导航中选择“讯记环网”，进入环网全局设置页面。
3. 在“讯记环网”中选择“Enable”。
4. 单击“应用”，使能环网功能。
5. 单击“讯记环网”页签，进入环网参数配置页面。
6. 参考“表 4-21 单环环网参数规划”，设置“讯记环网 ID”为“1”，节点模式为“Master”，“主端口”为“FE1”，“备用端口”为“FE2”。

全局

讯记环网

讯记环网 创建

讯记环网 ID	1
节点模式	Master
主端口	FE1
备用端口	FE2

创建

7. 单击“创建”，所设置的参数保存到环网列表中。

步骤2 登录 SW2，并设置 SW2 的环网参数。

1. 登录 SW2 的 Web 配置页面，具体步骤请参见“2.3 通过 Web 浏览器访问”。
2. 在左侧导航中选择“讯记环网”，进入环网全局设置页面。
3. 在“讯记环网”中选择“Enable”。
4. 单击“应用”，使能环网功能。
5. 单击“讯记环网”页签，进入环网参数配置页面。
6. 参考“表 4-21 单环环网参数规划”，设置“讯记环网 ID”为“1”，节点模式为“Transit”，“主端口”为“FE1”，“备用端口”为“FE2”。

全局

讯记环网

讯记环网 创建

讯记环网 ID	1
节点模式	Transit
主端口	FE1
备用端口	FE2

创建

7. 单击“创建”，所设置的参数保存到环网列表中。

步骤3 参考步骤 2，设置 SW3 和 SW4 的环网参数。

——结束

配置各交换机的环网参数后，请根据环网图正确连接各交换机。

4.12.2. 创建相交环环网

介绍以太网相交环环网的配置步骤。

如下图所示， SW1、SW2、SW3、SW4、SW5、SW6 组成 Ring1，SW1 为 Ring 1 主节点，SW5 为 Ring 3 的主节点。SW2、SW3、SW4、SW5、SW6、SW7 为 Ring 2 主节点，SW5 为 Ring 3 的主节点。

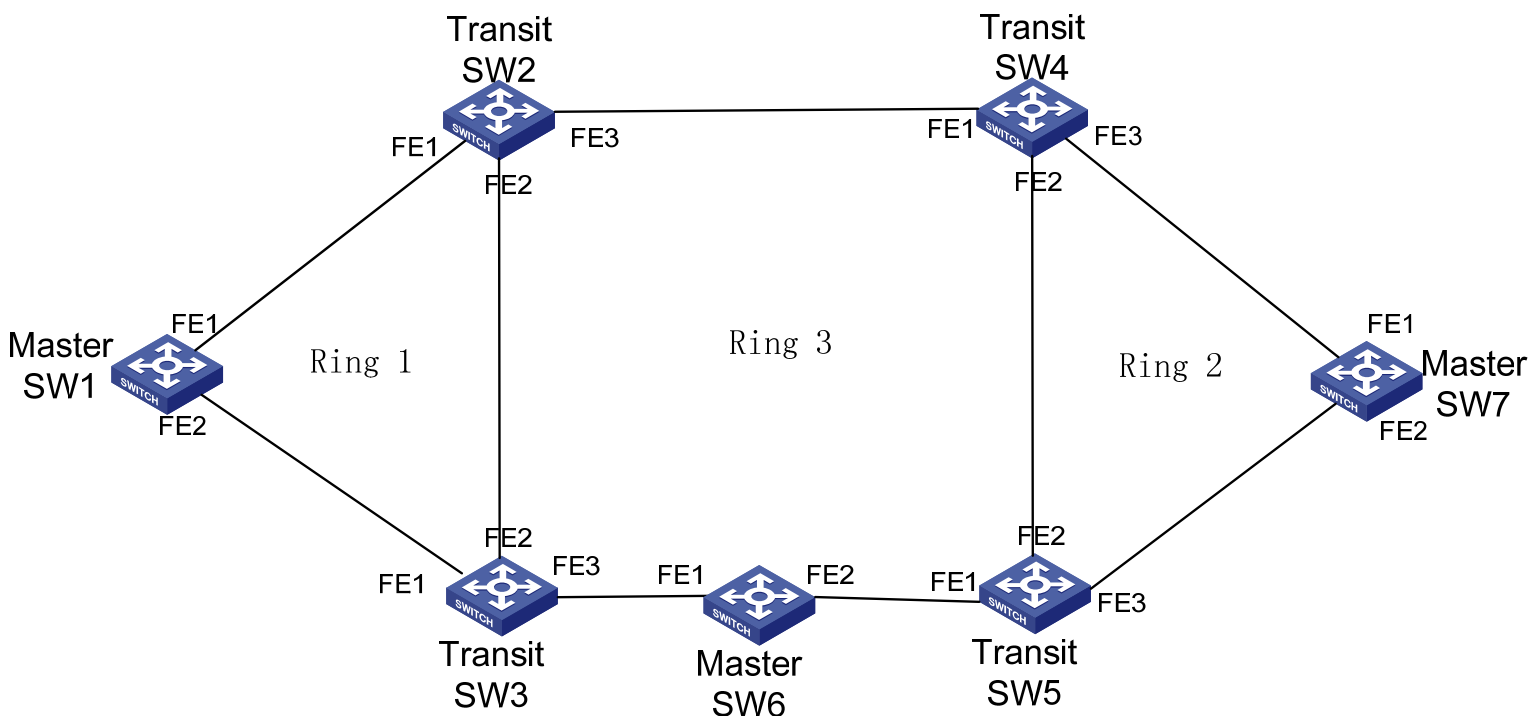


表 4-22 相交环网参数规划

交换机	环网 ID	节点模式	主端口	备用端口
SW1	1	Master	FE1	FE2
SW2	1	Transit	FE1	FE2
	3	Transit	FE3	FE2
SW3	1	Transit	FE1	FE2
	3	Transit	FE3	FE2
SW4	2	Transit	FE3	FE2
	3	Transit	FE1	FE2
SW5	2	Transit	FE3	FE2
	3	Transit	FE1	FE2
SW6	3	Master	FE1	FE2
SW7	2	Master	FE1	FE2

在物理连接各设备之前，需要先配置各设备的环网参数。

步骤1 登录 SW1，设置 SW1 的环网参数。

1. 登录 SW1 的 Web 配置页面，具体步骤请参见“2.3 通过 Web 浏览器访问”。
2. 在左侧导航中选择“讯记环网”，进入环网全局设置页面。
3. 在“讯记环网”中选择“Enable”。
4. 单击“应用”，使能环网功能。
5. 单击“讯记环网”页签，进入环网参数配置页面。
6. 参考“表 4-22 相交环网参数规划”，设置“讯记环网 ID”为“1”，节点模式为“Master”，“主端口”为“FE1”，“备用端口”为“FE2”。

全局

讯记环网

讯记环网 创建

讯记环网 ID

1

节点模式

Master

主端口

FE1

备用端口

FE2

创建

7. 单击“创建”，所设置的参数保存到环网列表中。

步骤2 参考步骤 1，分别设置 SW6 和 SW7 的环网参数。

步骤3 登录 SW2，并设置 SW2 的环网参数。

1. 登录 SW2 的 Web 配置页面，具体步骤请参见“2.3 通过 Web 浏览器访问”。

- 2. 在左侧导航中选择“讯记环网”，进入环网全局设置页面。
- 3. 在“讯记环网”中选择“Enable”。
- 4. 单击“应用”，使能环网功能。
- 5. 单击“讯记环网”页签，进入环网参数配置页面。
- 6. 参考“表 4-22 相交环环网参数规划”，设置“讯记环网 ID”为“1”，节点模式为“Transit”，“主端口”为“FE1”，“备用端口”为“FE2”。

全局

讯记环网

讯记环网 创建

讯记环网 ID	1
节点模式	Transit
主端口	FE1
备用端口	FE2

创建

- 7. 单击“创建”，所设置的参数保存到环网列表中。
- 8. 参考“表 4-22 相交环环网参数规划”，设置“讯记环网 ID”为“3”，节点模式为“Transit”，“主端口”为“FE3”，“备用端口”为“FE2”。

全局

讯记环网

讯记环网 创建

讯记环网 ID	3
节点模式	Transit
主端口	FE3
备用端口	FE2

创建

- 9. 单击“创建”，所设置的参数保存到环网列表中。
- 步骤4 参考步骤 3，分别设置 SW3、SW4、SW5 的环网参数。
- 结束
- 配置各交换机的环网参数后，请根据环网图正确连接各交换机。

4.12.3. 创建相切环环网

介绍以太网相切环环网的配置步骤。

如下图所示， SW1、SW2、SW3、SW4 在组成 Ring 1，SW1 为主节点。SW2、SW3、SW5、SW6 组成 Ring 2，SW6 为主节点。SW2、SW3 为 Ring 1 和 Ring 2 共用节点。

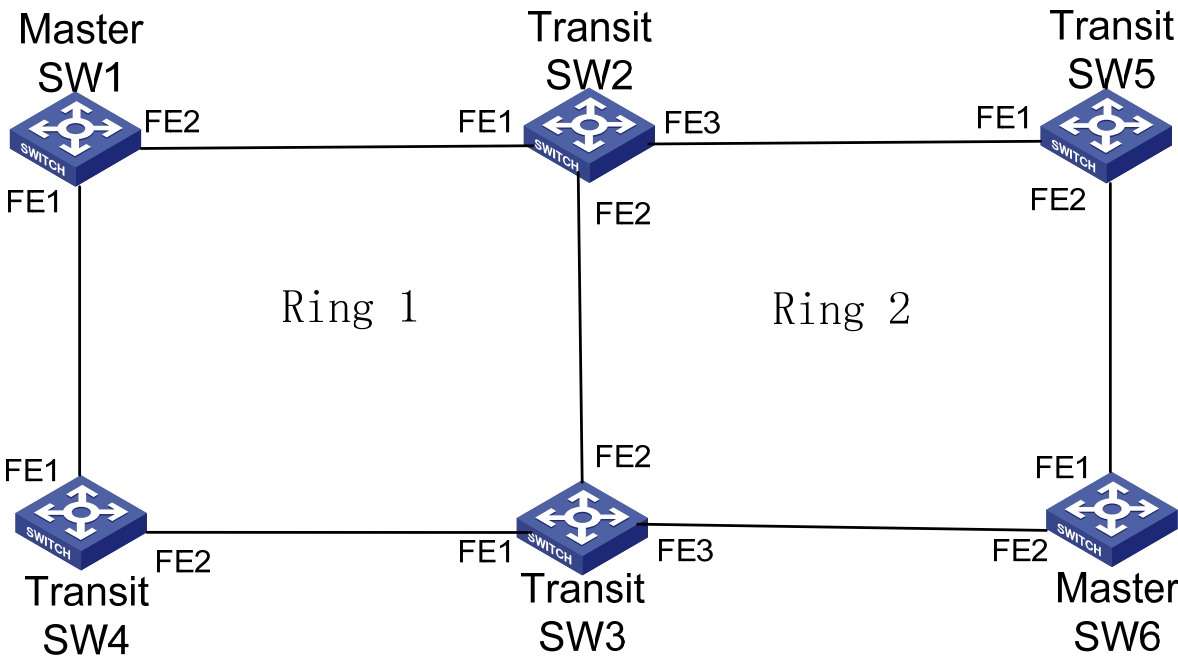


表 4-23 相切环环网参数规划

交换机	环网 ID	节点模式	主端口	备用端口
SW1	1	Master	FE1	FE2
SW2	1	Transit	FE1	FE2
	2	Transit	FE3	FE2
SW3	1	Transit	FE1	FE2
	2	Transit	FE2	FE3
SW4	1	Transit	FE1	FE2
SW5	2	Transit	FE1	FE2
SW6	2	Master	FE1	FE2

在物理连接各设备之前，需要先配置各设备的环网参数。

步骤1 登录 SW1，设置 SW1 的环网参数。

1. 登录 SW1 的 Web 配置页面，具体步骤请参见“2.3 通过 Web 浏览器访问”。

2. 在左侧导航中选择“讯记环网”，进入环网全局设置页面。

3. 在“讯记环网”中选择“Enable”。

4. 单击“应用”，使能环网功能。

5. 单击“讯记环网”页签，进入环网参数配置页面。

6. 参考“

7. 表 4-23”，设置“讯记环网 ID”为“1”，节点模式为“Master”，“主端口”为“FE1”，“备用端口”为“FE2”。

全局讯记环网

讯记环网 创建

讯记环网 ID

1

节点模式

Master

主端口

FE1

备用端口

FE2

创建

8. 单击“创建”，所设置的参数保存到环网列表中。

步骤2 参考步骤 1，设置 SW6 的环网参数。

步骤3 登录 SW2，并设置 SW2 的环网参数。

1. 登录 SW2 的 Web 配置页面，具体步骤请参见“2.3 通过 Web 浏览器访问”。

2. 在左侧导航中选择“讯记环网”，进入环网全局设置页面。

3. 在“讯记环网”中选择“Enable”。

4. 单击“应用”，使能环网功能。

5. 单击“讯记环网”页签，进入环网参数配置页面。

6. 参考“

7. 表 4-23”，设置“讯记环网 ID”为“1”，节点模式为“Transit”，“主端口”为“FE1”，“备用端口”为“FE2”。

全局讯记环网

讯记环网 创建

讯记环网 ID

1

节点模式

Transit

主端口

FE1

备用端口

FE2

创建

8. 单击“创建”，所设置的参数保存到环网列表中。

9. 参考“

10. 表 4-23 ”，设置“讯记环网 ID”为“2”，节点模式为“Transit”，“主端口”为“FE3”，“备用端口”为“FE2”。

全局

讯记环网

讯记环网 创建

讯记环网 ID	2
节点模式	Transit
主端口	FE3
备用端口	FE2

创建

11. 单击“创建”，所设置的参数保存到环网列表中。

步骤4 参考步骤 3，设置 SW3 环网参数。

步骤5 参考步骤 3 的 1-8，设置 SW4、SW5 的环网参数。

——结束

配置各交换机的环网参数后，请根据环网图正确连接各交换机。

4.13 管理POE

POE 工业以太网交换机提供管理 POE 功能，支持 8 个兼容 IEEE 802.3at/af 标准带 PoE 功能以太网口，可同时支持 8 个端口 15.4W 或 4 个端口 30W，总功率不能超过 120W。

步骤1 在左侧导航中选择“POE”，进入 POE 设置页面。默认情况开启 POE 功能。

•系统信息

•端口设置

•端口镜像

•端口隔离组

•端口聚合

+虚拟局域网

+服务质量

+转发地址

•风暴抑制

+数据统计

PoE 全局

PoE 端口

POE系统信息

POE设备开关	Enabled
POE设备输出总功率上限（瓦）	120W
POE设备输出电压上限（伏）	57.0[V]
POE设备输出电压下限（伏）	44.0[V]
POE设备接线输出模式	MODE B(4-5-7-8)

应用

步骤2 设置端口的参数。

表 4-24 端口设置参数

值	值域	描述
管理协议	802.3 af/at Auto Force 缺省值：802.3 af/at Auto	选择管理协议模式。 802.3 af/at Auto：不可修改功率上限值，默认 30。 Force：可修改功率上限值。
端口	如 FE1	选择需要设置的端口号。
开关	Enabled, Disabled 缺省值： Enabled	启用或禁用该端口。 Enabled：表示启用端口。 Disabled：表示禁用端口。
功率上限	取值范围： 0~30 缺省值： 30	设置该端口的功率上限。

优先级	Low High critical 缺省值： low	设置端口的优先级。 端口优先级的大小决定了这个端口满足设定功率情况。按照优先级从高到低的次序优先满足较高优先级功率情况，当优先级相同的时功率平均分配。
-----	--	--

步骤3 单击“应用”，使所设置的端口参数生效并在 “端口状态列表” 中显示。

——结束

4.14 配置串口参数

本设备提供串口服务器功能可将 RS-232/RS-422/RS-485 的数据通过 TCP Client、TCP Server 或者 UDP 模式实现串口数据的以太网转换与传输。您可以对串口的通信参数进行设置，如串口波特率、数据位、停止位、奇偶性、端口号等。对于两个进行通信的串口，这些参数必须匹配才能通信。串口功能只对带串口系列机型可见。

步骤1 在左侧导航中选择“串口”，进入串口设置页面。



步骤2 选择某一串口号，并设置该串口的参数。

表 4-25 端口设置参数

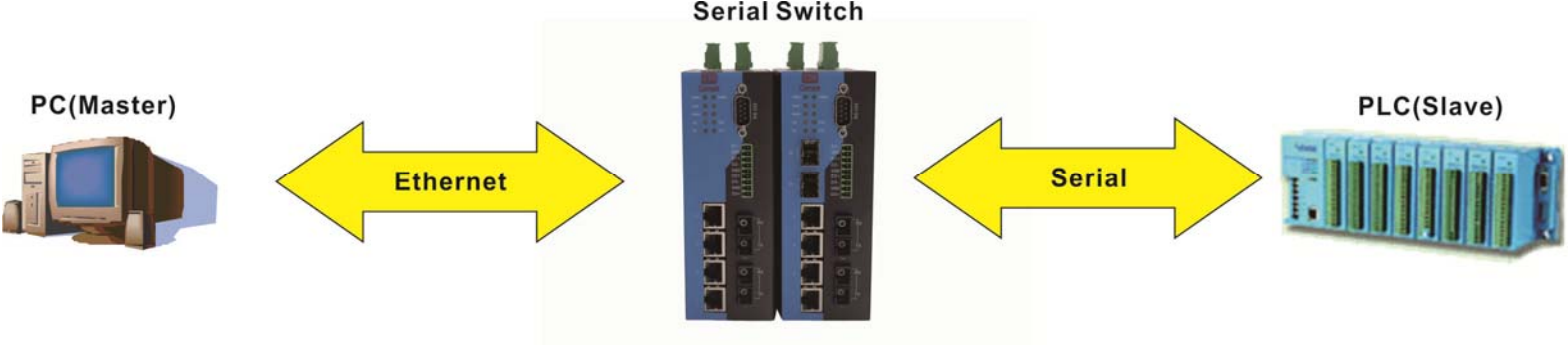
值	值域	描述
串口	1~4	选择需要设置的串口号。
波特率	110, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 缺省值：9600	设置该串口的波特率。 波特率表示每秒钟传送的数据位的格式，是一个衡量通信速度的参数。
数据位	5~8 缺省值：8	设置该串口的数据位。 数据位指每字节中实际数据所占的比特数，是衡量通信中实际数据位的参数。
停止位	1, 1.5, 2 缺省值：1	设置该串口的停止位。 停止位用于标识一个数据包数据结束。停止位不仅仅用于数据包的传输结束标志，还提供了计算机之间校正同步时钟的机会。用于停止位的位数越多，不同时钟同步的容忍程度越大。但是由于停止位占用了数据空间，过多的停止位将导致数据传输速度的下降。

奇偶性	even, mark, none, odd, space 缺省值: none	设置该串口的奇偶校验位。 奇偶校验用来判断接收的数据位有无错误。对于偶和奇校验，串口会设置校验位，用一个值确保传输的数据有偶个或者奇个逻辑高位。对于 1 和 0 校验，并不真正的检查数据，简单值位逻辑高或逻辑低校验，可以使接收设备能够知道一个位的状态，判断是否有噪声干扰了通信或者传输和接收数据是否不同步。 even: 奇校验，如果校验方式设置为“odd”，则发送数据中 1 的个数为奇数时，校验位为“0”；发送数据中 1 的个数为偶数时，校验位为“1”。 mark: 1 校验，如果校验方式设置为“mark”，校验位固定为“1”。 none: 无校验，在数据发送时，如果校验位设置为“none”，则不发送校验位，否则会发送一位校验位。 odd: 偶校验，如果校验方式设置为“odd”，则发送数据中 1 的个数为奇数时，校验位为“1”；发送数据中 1 的个数为偶数时，校验位为“0”。 sapce: 0 检验，如果校验方式设置为“space”，校验位固定为“0”。
模式	Disabled, Tcpclient, Tcpserver, Udp ModbusTCP(RTU) 缺省值: Disabled	设置该串口的数据到以太网的转换与传输的工作模式。 Tcpclient: 在此工作模式下，串口主动连接远端 IP 的目标端口。与 Tcpserver 成对使用。 Tcpserver: 在此工作模式下，串口监听客户端的连接。与 Tcpclient 成对使用。 Udp: UDP 协议没有建立连接，在使用 UDP 协议进行传输时，只向远端 IP 的目的端口收发数据。 ModbusTCP(RTU): 以太网对应的通信模式为 MODBUS TCP, 异步串行传输(RS-232-/422/485), 对应的通信模式是 MODBUS RTU。（本系列串口设备不支持 MODBUS ASCII 模式且串口不带隔离功能） Disabled: 关闭该串口。
本地端口	1~65535	设置该串口的本地端口号。
远程端口	1~65535	设置该串口通过以太网通讯的远端设备目的串口端口号。
IP 地址	XXX. XXX. XXX. XXX	设置该串口通过以太网通讯的远端设备 IP 地址。

步骤3 单击“应用”，使所设置的串口参数生效并在 “串口列表” 中显示。

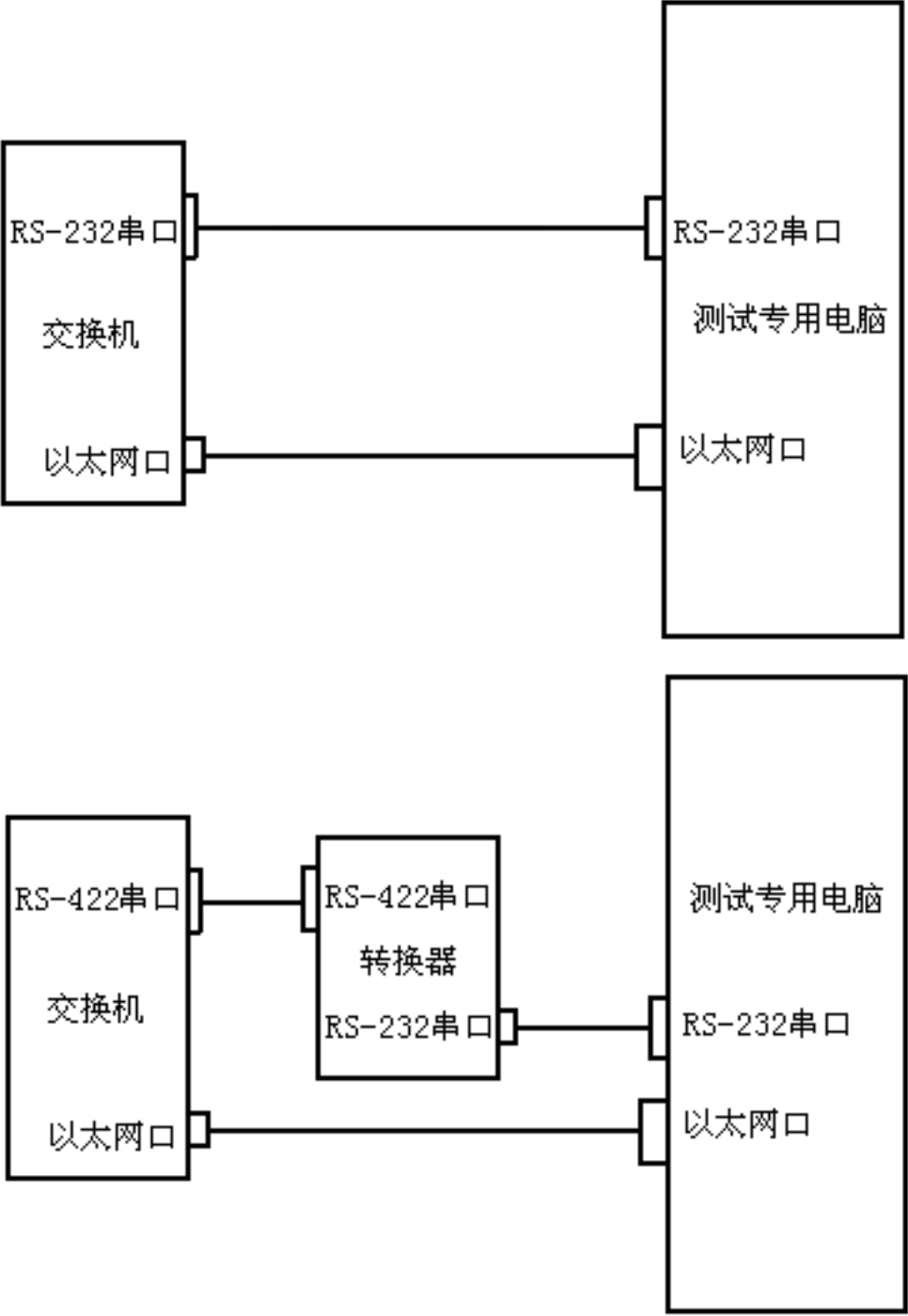
——结束

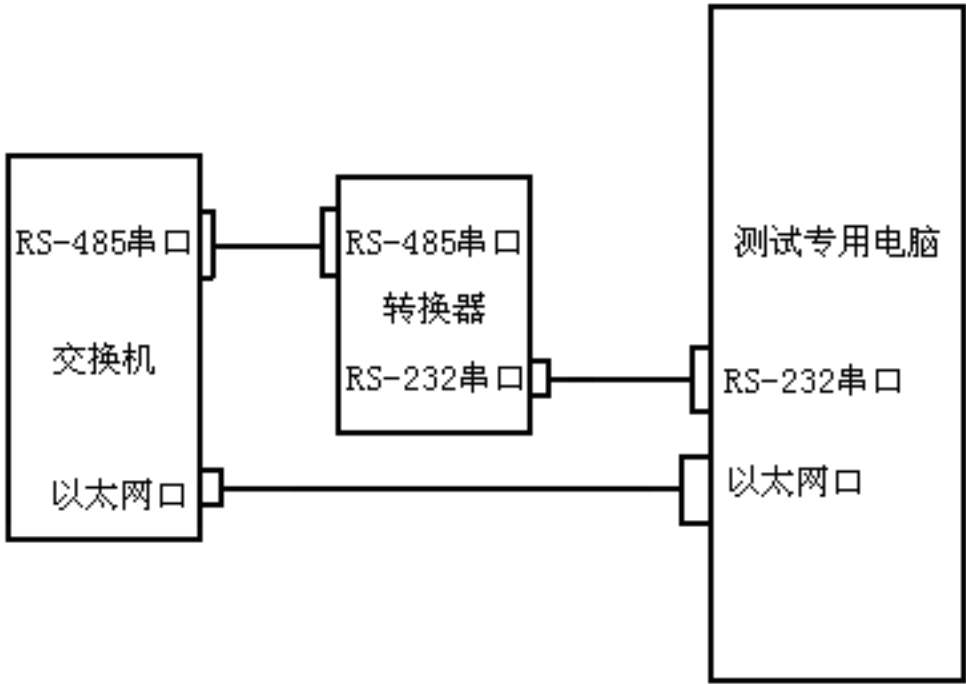
串口工作（应用于实际现场工作模式）
上位机 PC 电脑的网口连接本系列设备的以太网口，本系列设备的串口与下位机 PLC 的串口相连（RS-232/485/422），实现 TCP 转串行数据的传输。



串口工作（以模拟软件工作模式举例说明）

➤ 搭建简单配置环境：





说明： 电脑需要有串口，由于电脑都是 RS-232 串口如需使用 RS-485/422 串口需要 RS-485/422 转 RS-232 转换器。

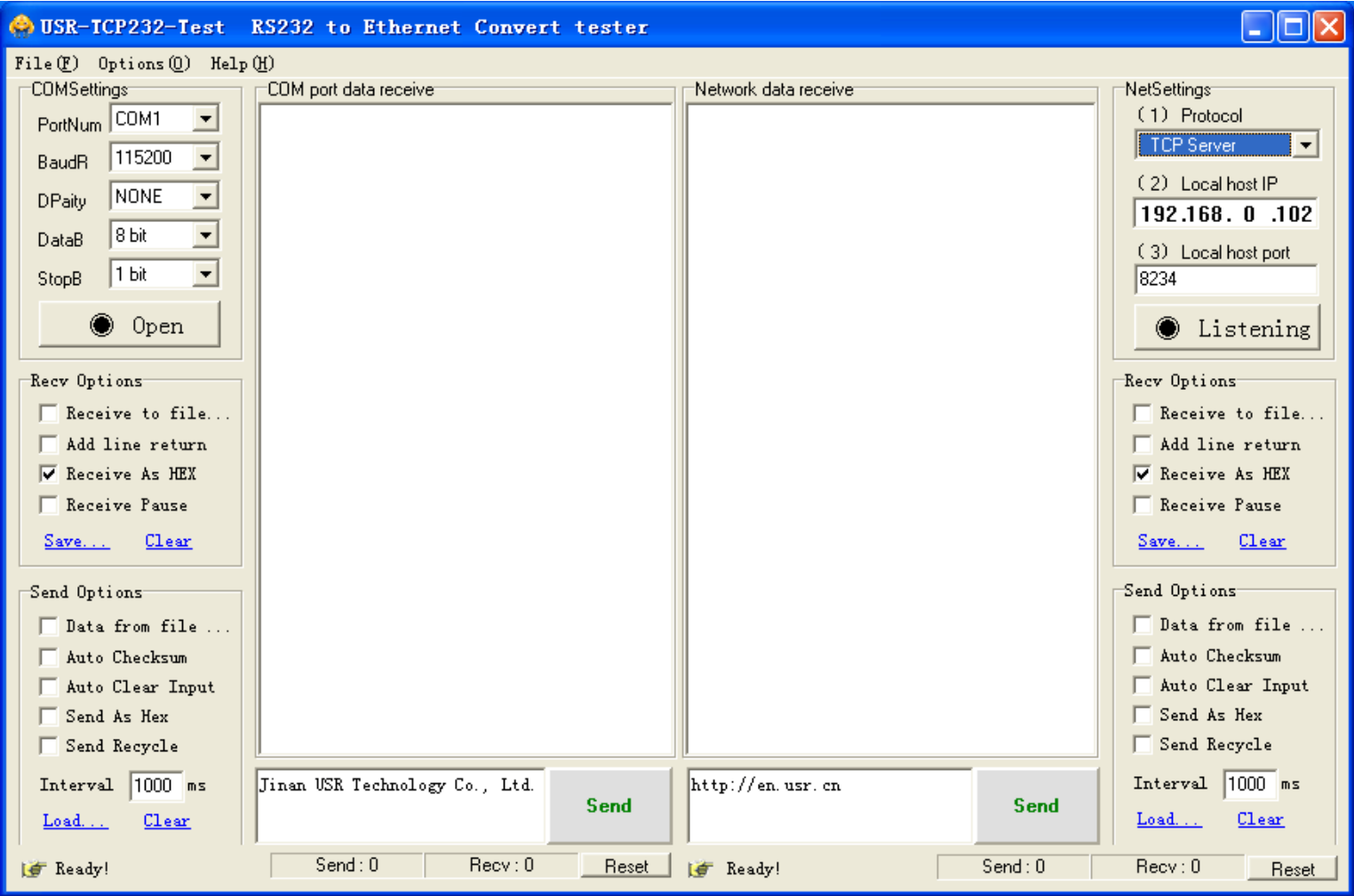
➤ 接线：

根据不同的串口接不同线序的线（RS-23 请使用双头 DB9 母头串口线；RS-485 接 2 根线 D+ 接 RS-485 转 RS-232 转换器的 R+, D-接转换器 R-; RS-422 接 4 根线 D+接 RS-422 转 RS-232 转换器的 T+/R+, D-接转换器 T-/R-）

➤ 电脑安装串口软件：



软件为 EXE 格式使用时直接双击即可，如下图所示。

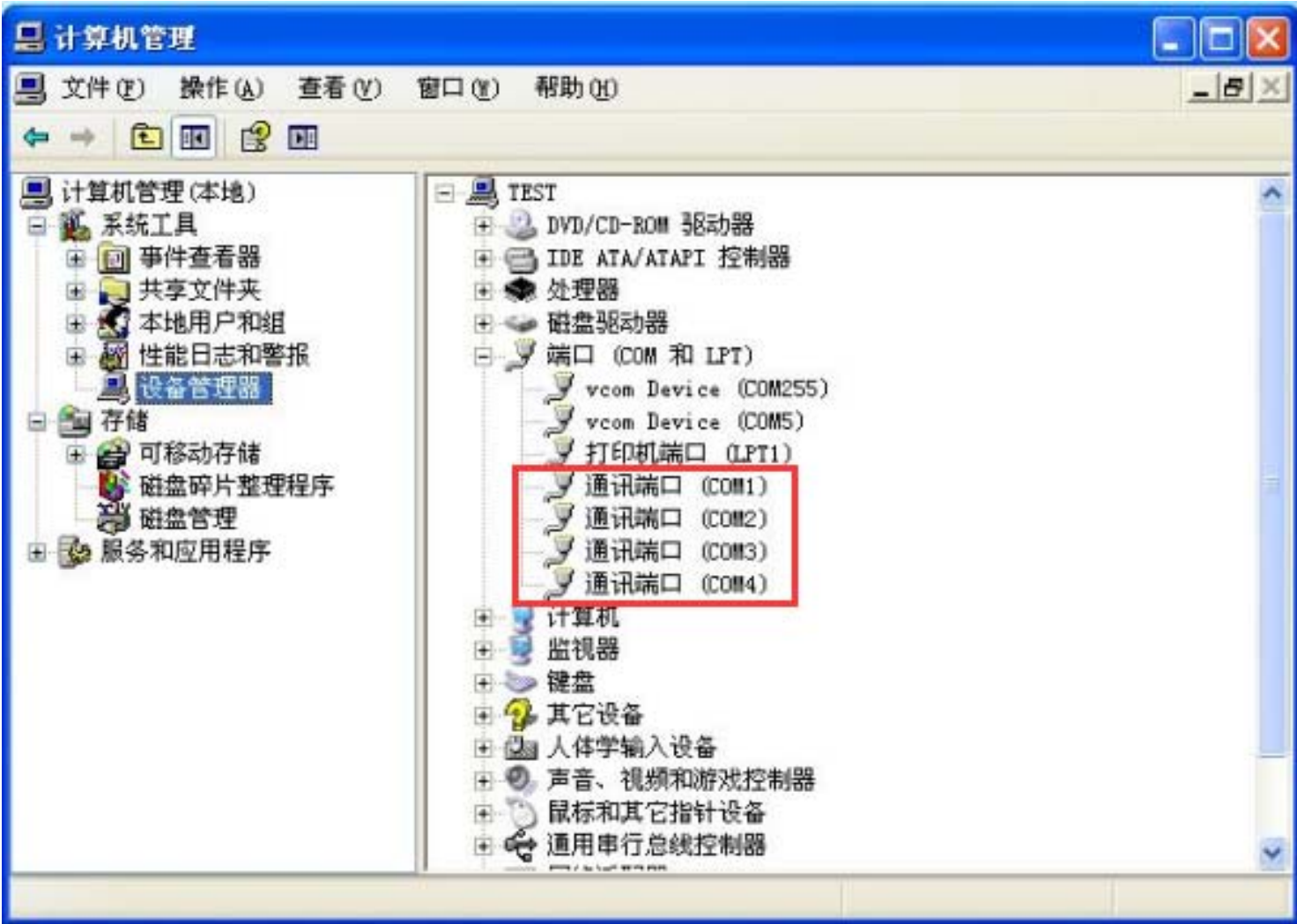


➤ 选择物理串口

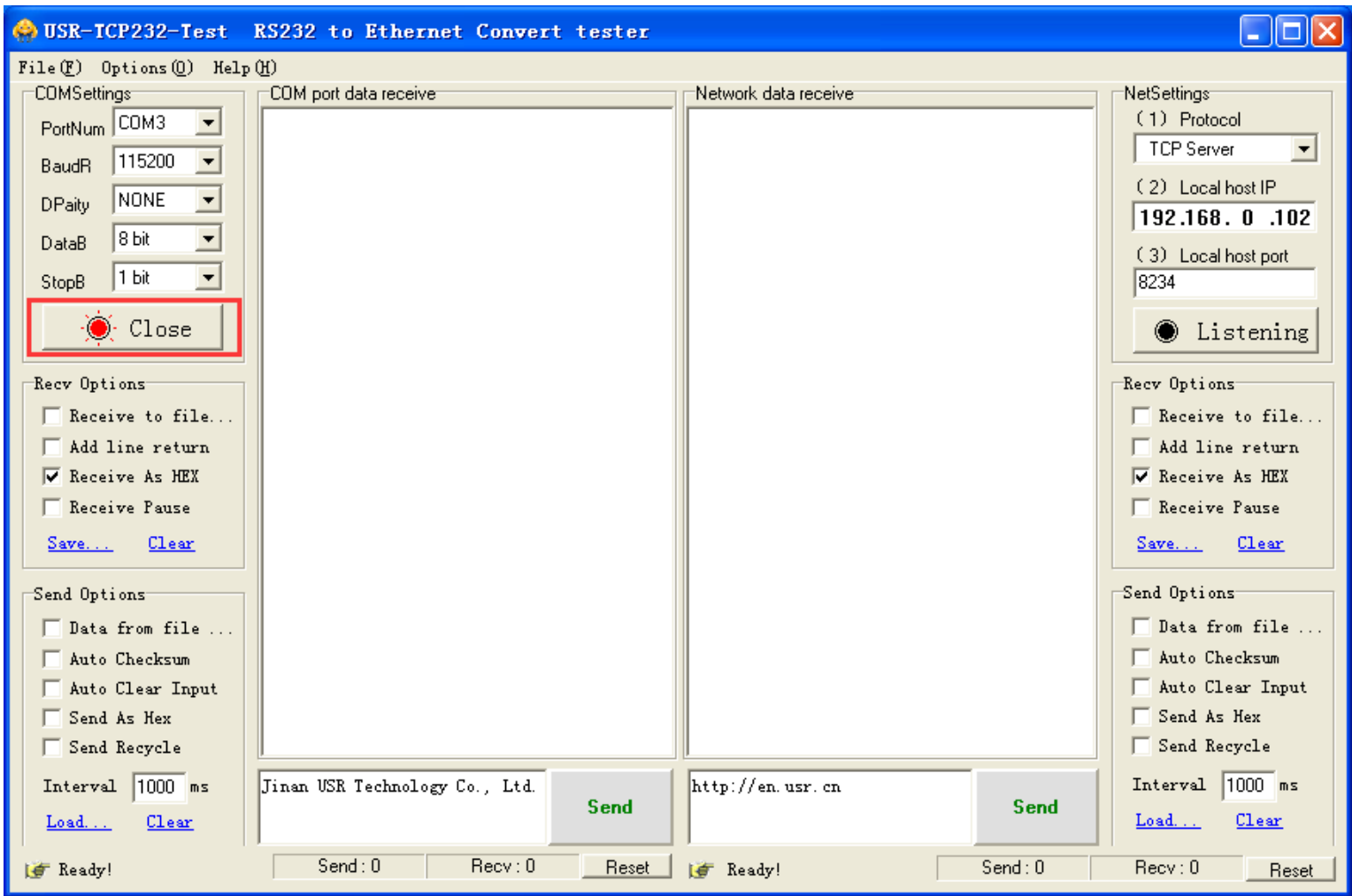
单机 “我的电脑” 管理出现如下图所示



单机设备管理器后再点击端口信息就会出现红色框框的电脑的串口信息



选择正确的串口号后单机打开串口出现如下状态



4.14.1. 服务器模式

配置服务器模式参数如下图所示：

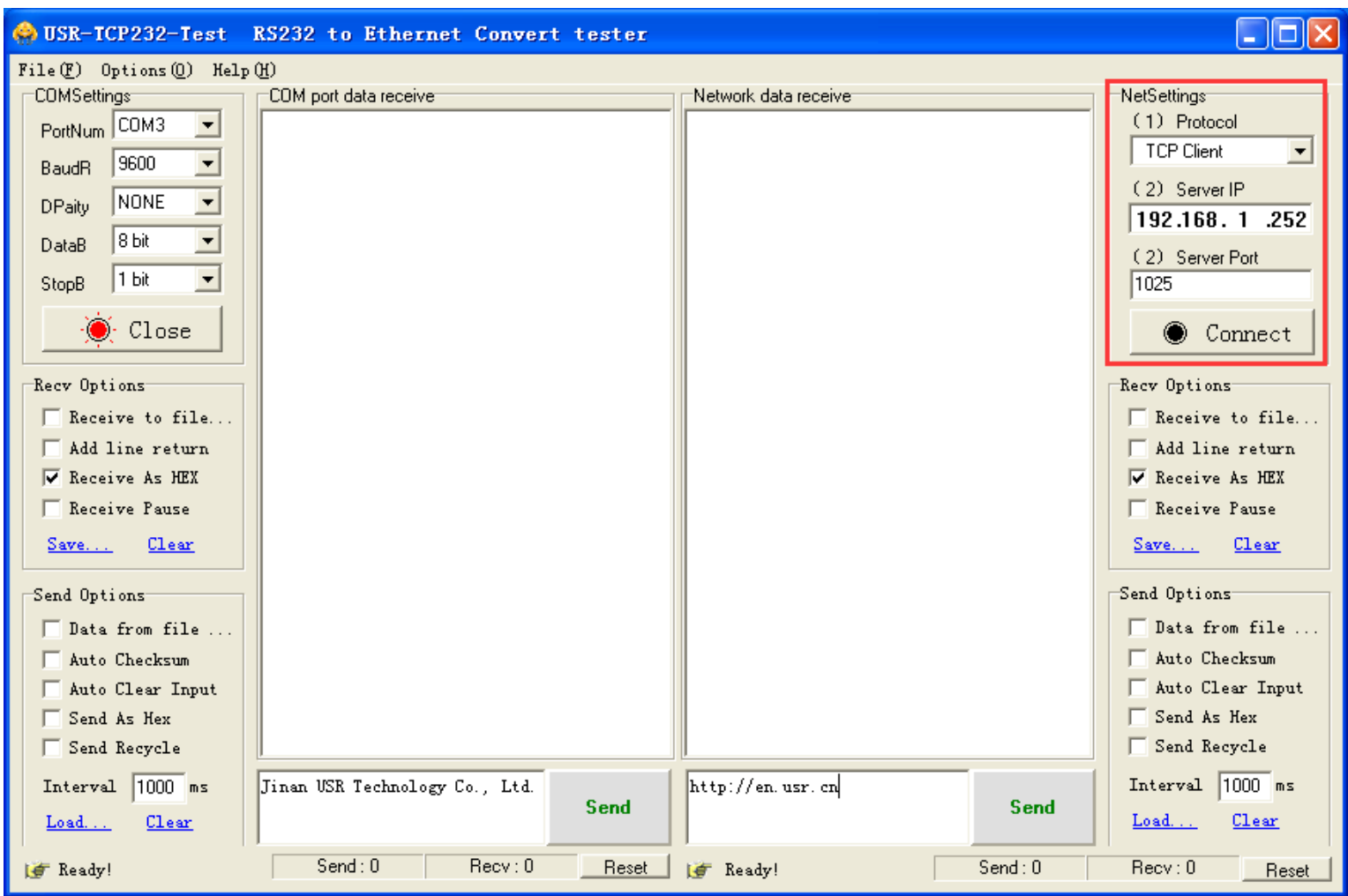
串口				
串口	波特率	数据位	停止位	奇偶性
1	9600	8	1	none
类型	模式	本地端口	远程端口	IP 地址
RS-232	Tcpserver	1025 1024~65535	30000 1024~65535	192.168.1.103
应用				

当设备作为服务器时只需要配置本地端口号即可

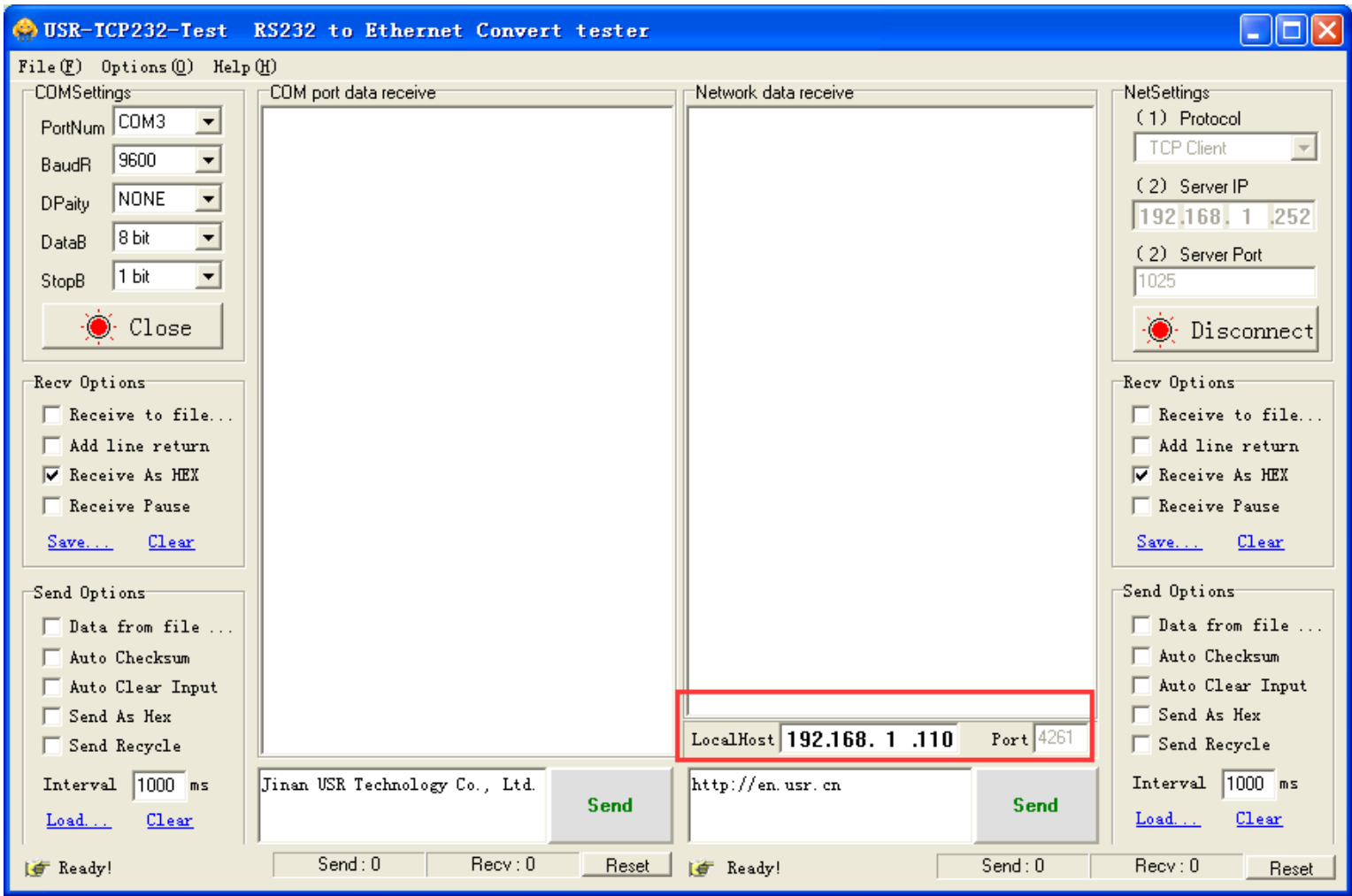
【本地端口】

设备作为服务器提供的能被其它 TCP/IP 结点连接的 TCP 端口

软件参数配置图如下：（PC 主动去连接设备所以协议选择 TCP Client ， IP 为设备 IP，端口号为设备本地端口号）



点击 Connect 出现下图红色框就可以正常通信了。



在发送区域上选择需要发送的数据包发送即可，如下图所示。



4.14.2. 客户端模式

配置客户端模式参数如下图所示：

串口	波特率	数据位	停止位	奇偶性
1	9600	8	1	none
类型	模式	本地端口	远程端口	IP 地址
RS-232	Tcpclient	1025 1024~65535	30000 1024~65535	192.168.1.110
应用				

作为 TCP Client 端时，设备主动去连接以太网上的 TCP/IP 的网络设备，如 PC。需要通过设置告诉设备在条件符合时，连接哪个网络地址和 TCP 端口号。建立 socket 后，设备将把从相应串口收到的数据通过 socket 传出，反之，从 socket 收到的数据会被送到相应串口。

与 TCP Client 有关设置选项：【远程端口】、【IP 地址】配置选项的含义解释如下：

【远程端口】

设备要连接的 TCP 端口号。

【IP 地址】

设备要连接的 IP 地址或域名地址，两者都可以对应 Internet 上的主机地址。

软件参数配置图如下：（设备主动去连接 PC 所以协议选择 TCP Server，IP 为 PC 的 IP，端口号为设备远程端口号）

USR-TCP232-Test RS232 to Ethernet Convert tester

File Options Help

COMSettings

PortNum COM3

BaudR 9600

DPaity NONE

DataB 8 bit

StopB 1 bit

Close

Recv Options

Receive to file...

Add line return

Receive As HEX

Receive Pause

Save... Clear

Send Options

Data from file ...

Auto Checksum

Auto Clear Input

Send As Hex

Send Recycle

Interval 1000 ms

Load... Clear

COM port data receive

Jinan USR Technology Co., Ltd.

Send

Send: 0 Recv: 0 Reset

Network data receive

http://en.usr.cn

Send

Send: 0 Recv: 0 Reset

NetSettings

(1) Protocol TCP Server

(2) Local host IP 192.168.1.110

(3) Local host port 30000

Listening

Recv Options

Receive to file...

Add line return

Receive As HEX

Receive Pause

Save... Clear

Send Options

Data from file ...

Auto Checksum

Auto Clear Input

Send As Hex

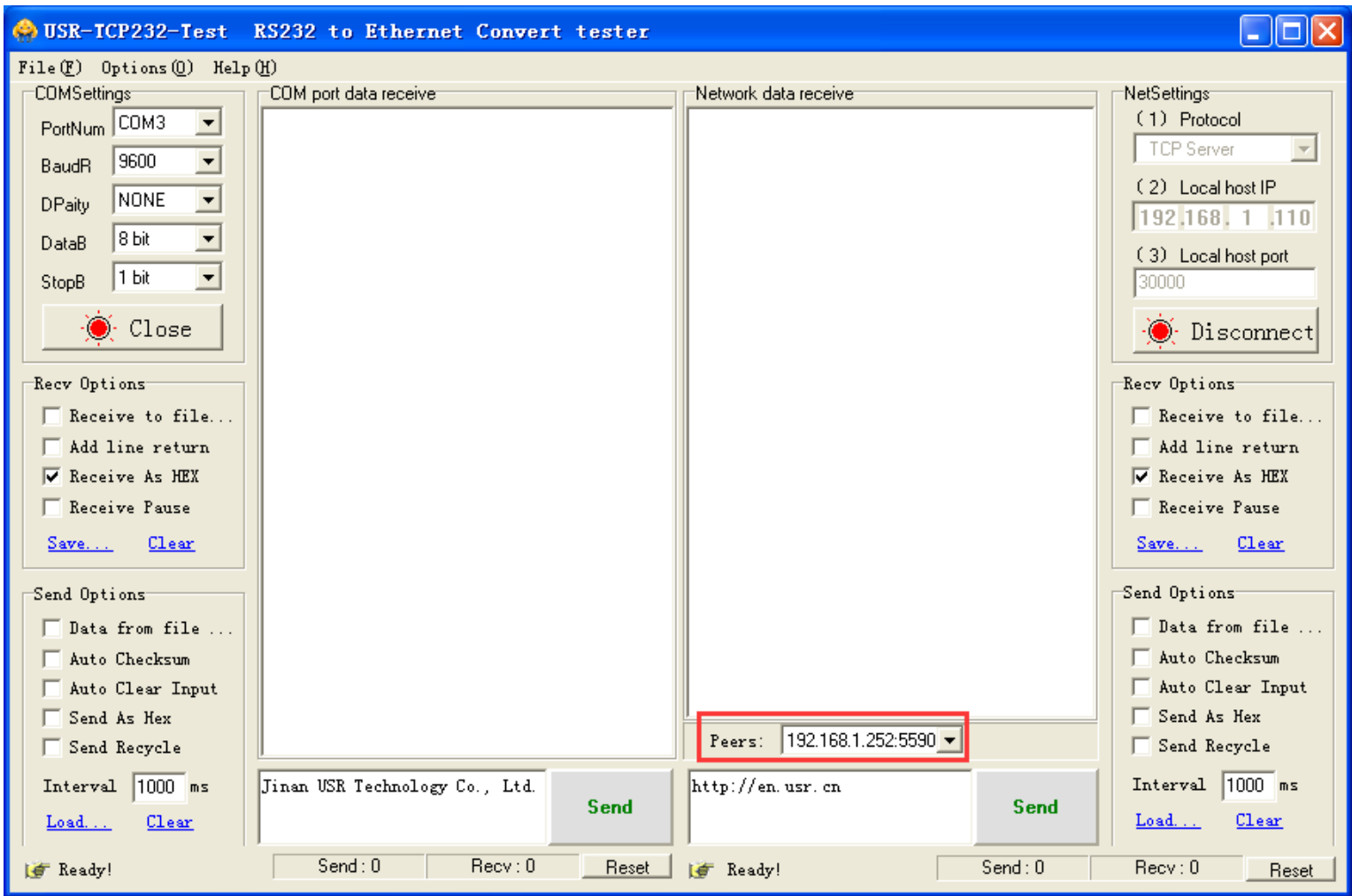
Send Recycle

Interval 1000 ms

Load... Clear

Ready! Ready!

点击 Listening 出现下图红色框就可以正常通信了。



在发送区域上选择需要发送的数据包发送即可，如下图所示。

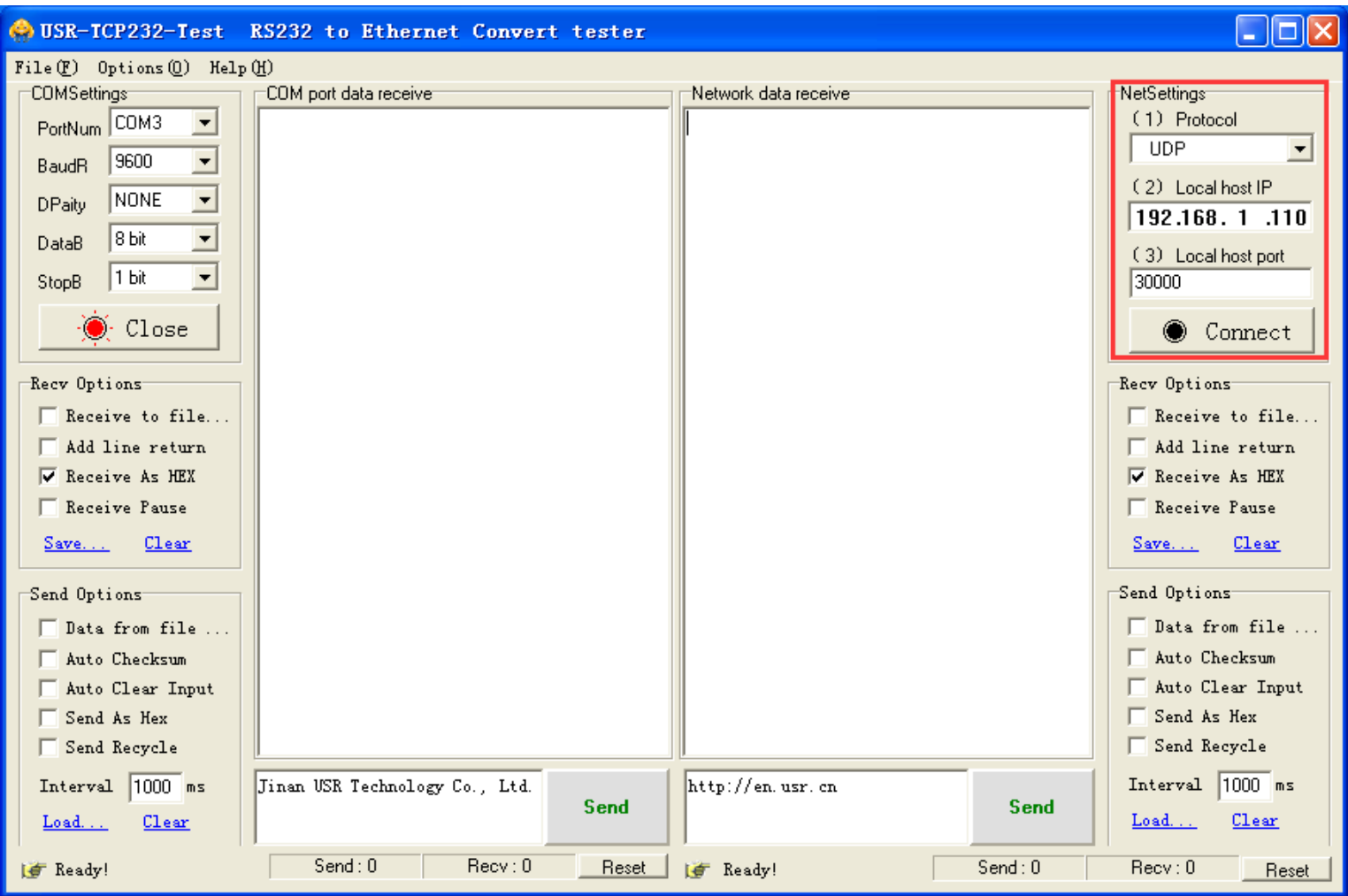


4.14.3. UDP模式

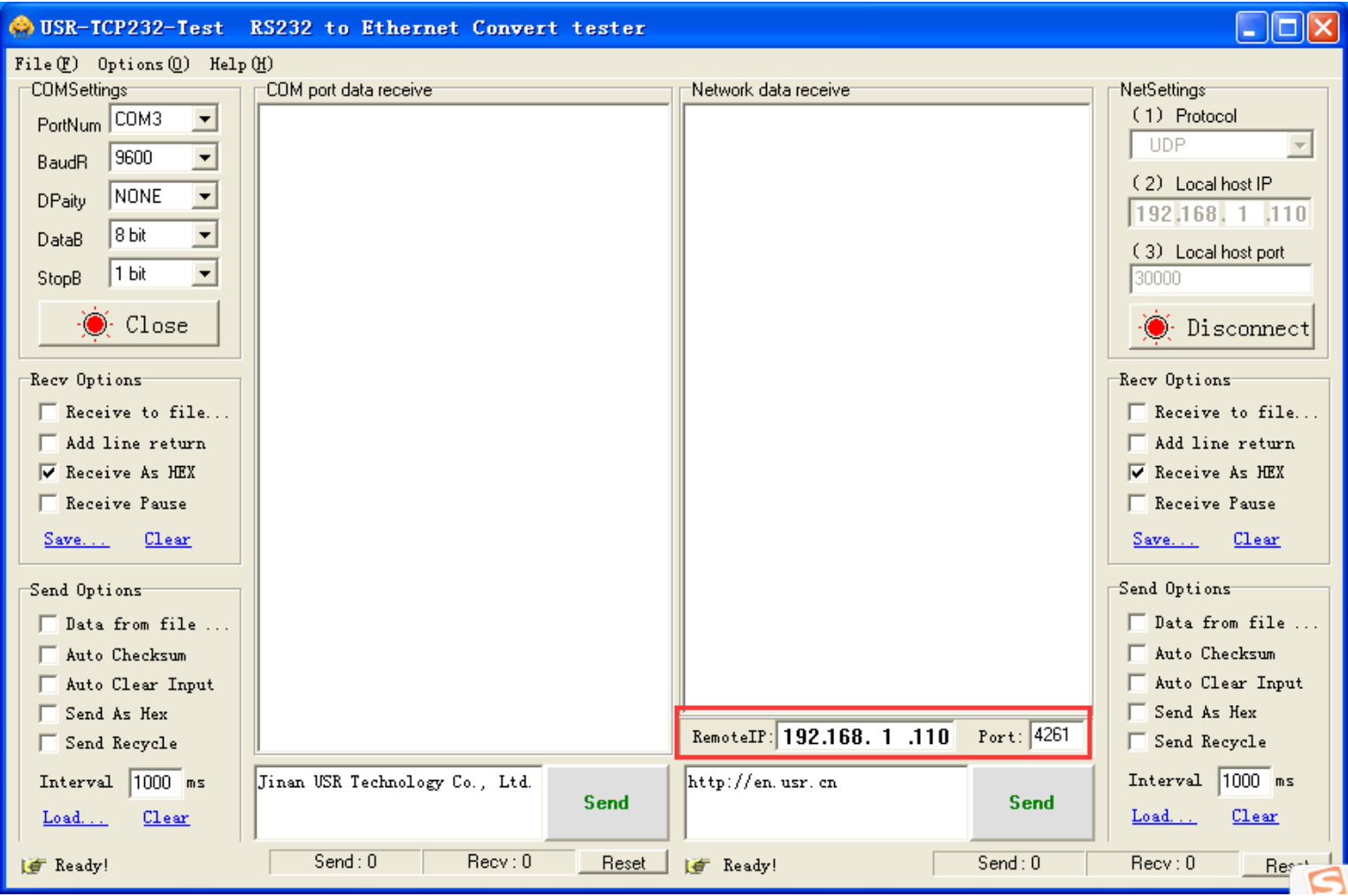
配置客户端模式参数如下图所示：

串口				
串口	波特率	数据位	停止位	奇偶性
1	9600	8	1	none
类型	模式	本地端口	远程端口	IP 地址
RS-232	Udp	1025 1024~65535	30000 1024~65535	192.168.1.110
应用				

在 UDP 工作模式下，设备既是 server 端，也是 client 端。与 udp 相关的配置选项有【本地端口】、【远程端口】和【IP 地址】。UDP 支持点对点方式，配置方式与 TCP 模式类似。软件参数配置图如下：（协议选择 UDP，IP 为 PC 的 IP，端口号为设备远程端口号）



点击 Connect 出现下图红色框就可以正常通信了。



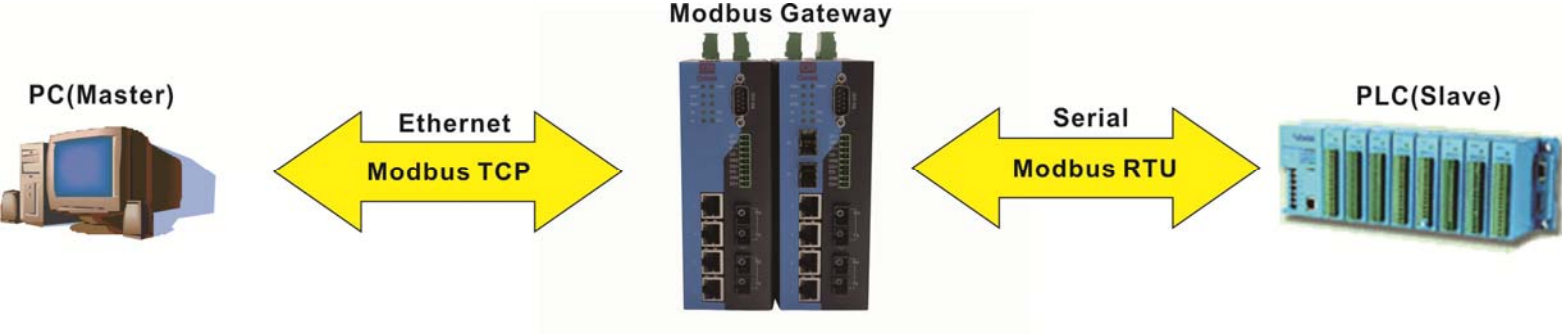
在发送区域上选择需要发送的数据包发送即可，如下图所示。



注意： RS-485 为半双工模式只能一个串口发送另一个串口只能接收数据；RS-232/422 为全双工模式可以同时双向发送。

4.14.4. Modbus TCP模式

Modbus 工作（应用于实际现场工作模式）
上位机 PC 电脑的网口连接本系列设备的以太网口，本系列设备的串口与下位机 PLC 的串口相连（RS-232/485/422），实现以太网链路上的 Modbus TCP 转串行链路上 Modbus RTU 的传输。（本系列串口设备不支持 MODBUS ASCII 模式且串口不带隔离功能）



以模拟软件工作模式举例说明
1、电脑安装 Modbus 测试软件（Modbus Poll 是上位机软件，Modbus Slave 是下位机软件，详细使用如下图所示）



2、Modbus 功能验证测试
配置交换机 WEB 串口参数
在 IE 浏览器上输入交换机默认 IP 192.168.1.253，点击串口配置页面配置串口参数：以串口 1 RS-232 为例配置如下图所示

串口	波特率	数据位	停止位	奇偶性
1	9600	8	1	none

类型	模式	本地端口	远程端口	IP 地址
RS-232	ModbusTcp(RTU)	1025	30000	192.168.1.253

应用

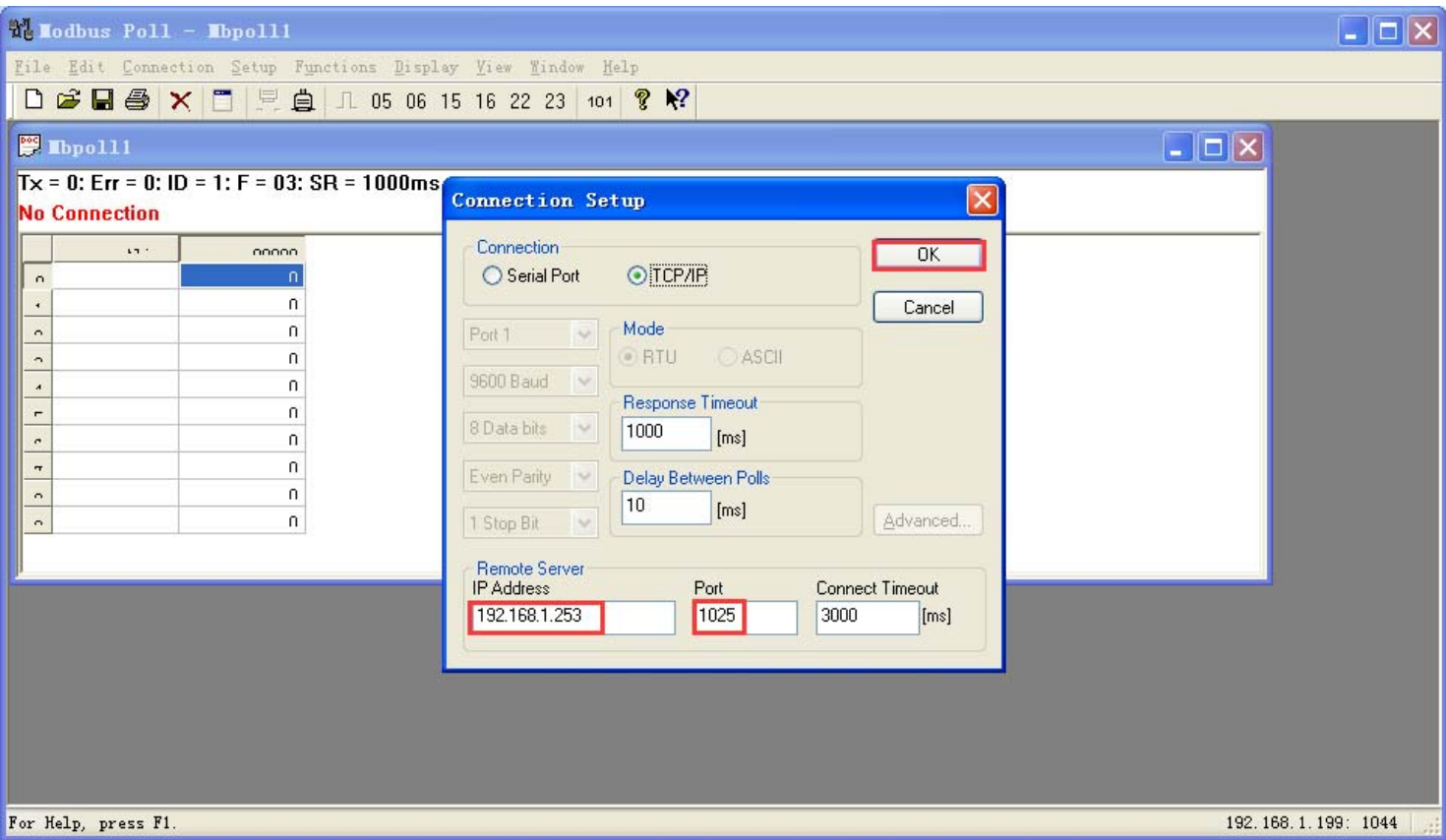
串口列表

串口	类型	波特率	数据位	停止位	奇偶性	模式	本地端口	远程端口	IP 地址
1	RS-232	9600	8	1	none	ModbusTcp (RTU)	1025	30000	192.168.1.253
2	RS-422	9600	8	1	none	ModbusTcp (RTU)	1026	30001	192.168.1.253
3	RS-485	9600	8	1	none	ModbusTcp (RTU)	1027	30002	192.168.1.253

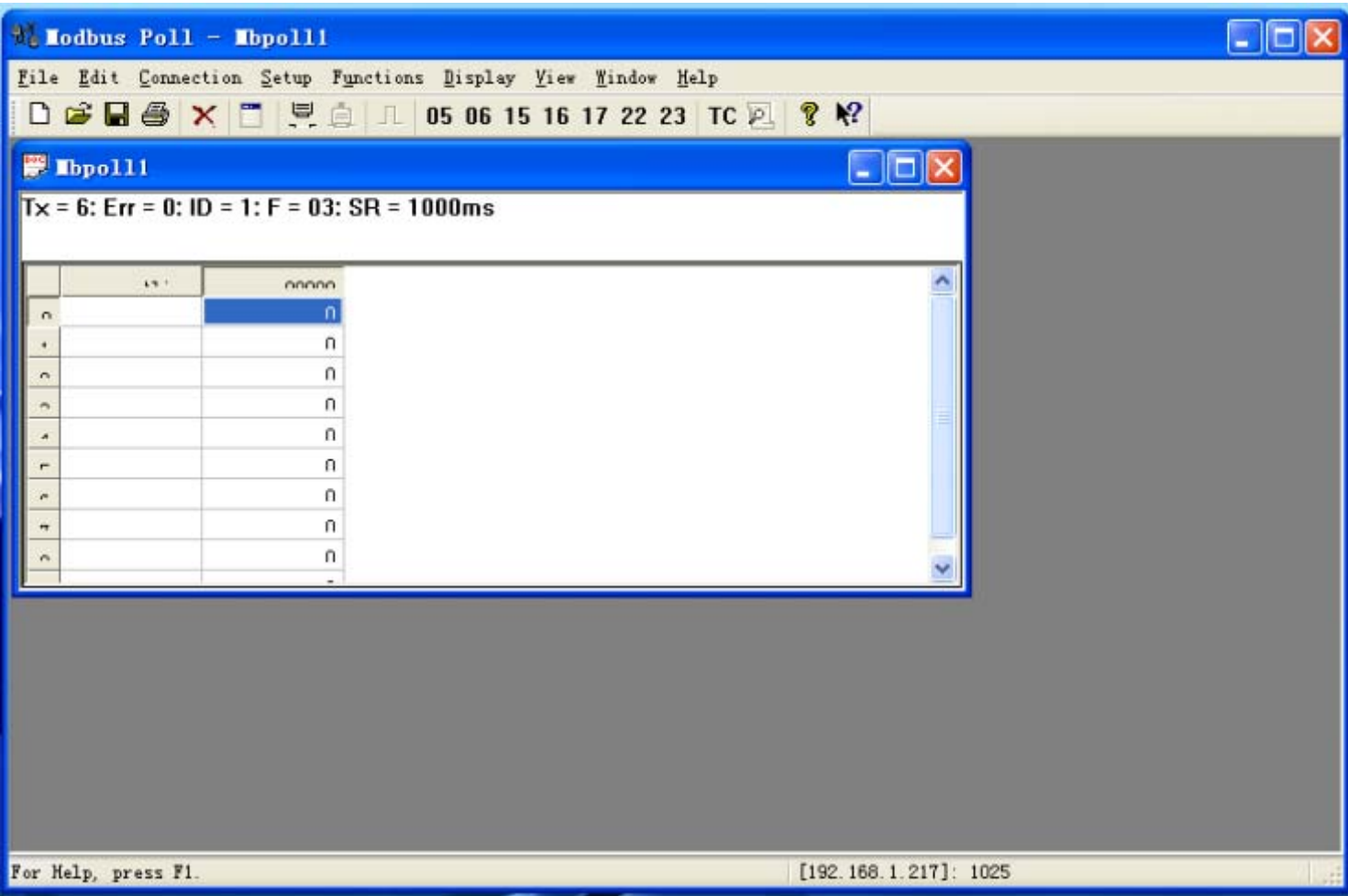
3、运行 Modbus 测试软件



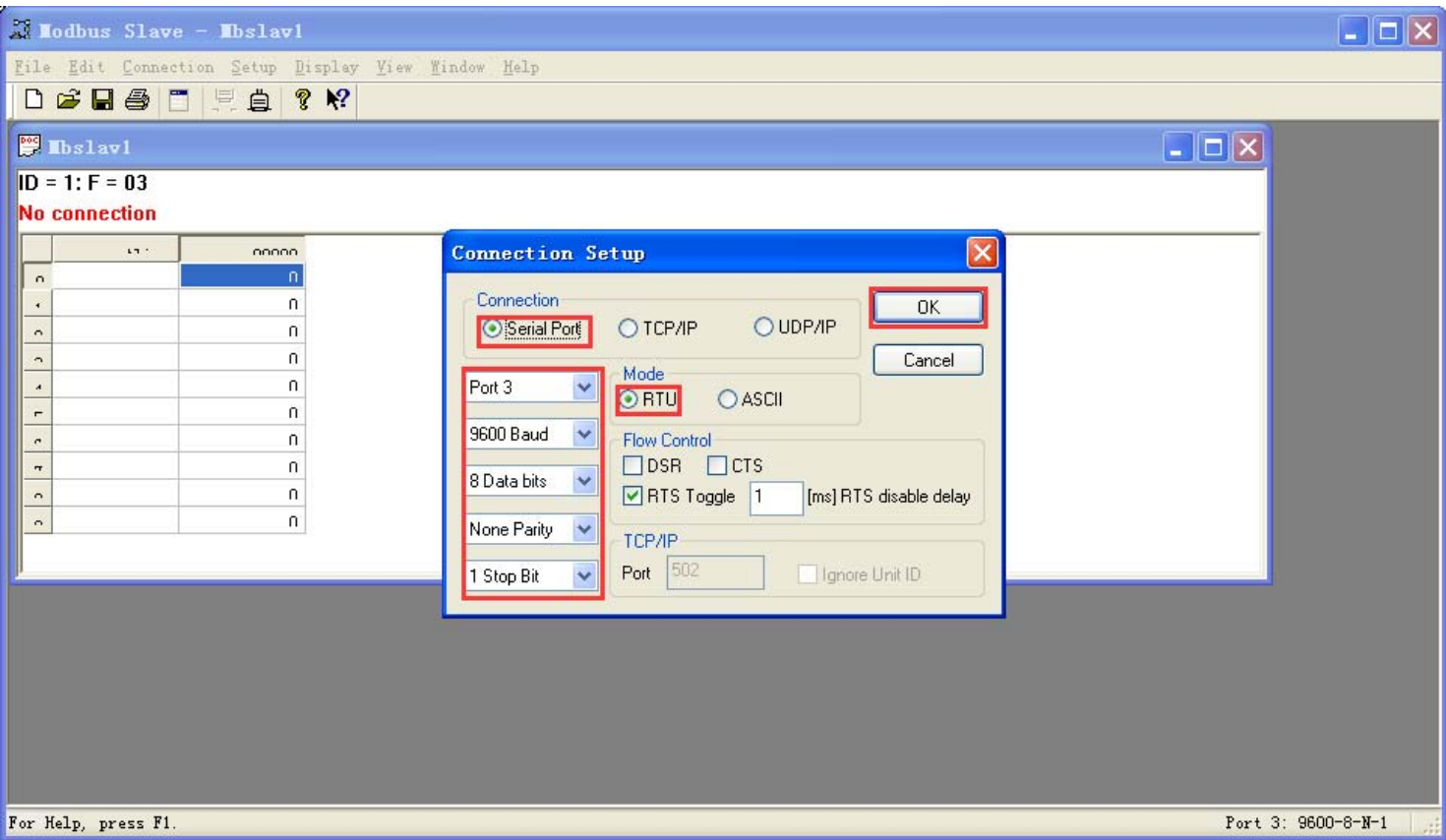
打开 Modbus Poll 软件进行配置，参数配置与 WEB 显示一致。
点击 Connection，选择 TCP/IP，IP Address 写交换机 IP 192.168.1.253，Port 写本地端口号 1025。



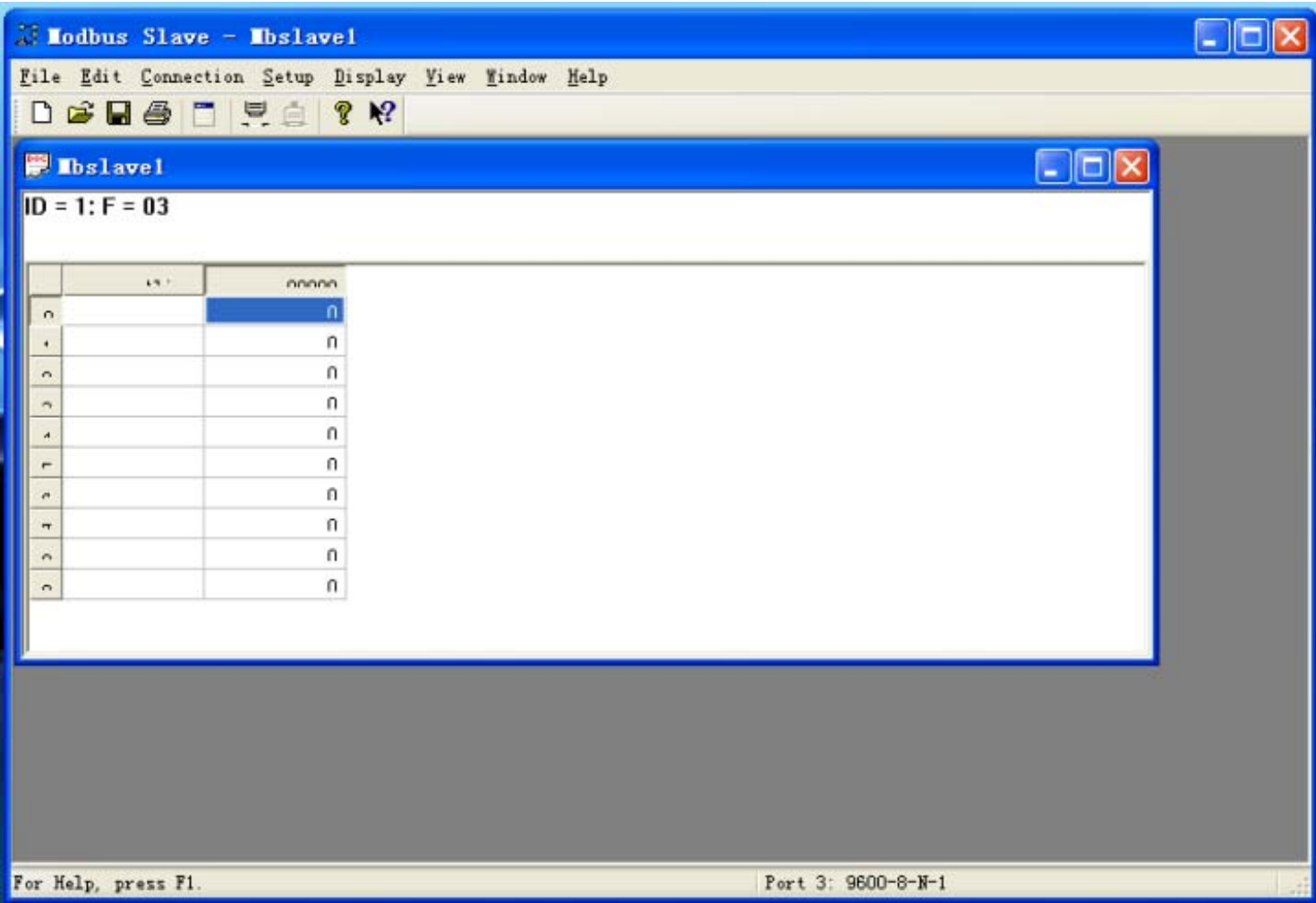
点击 OK 即连接上（红色字体 No Connection 会消失）



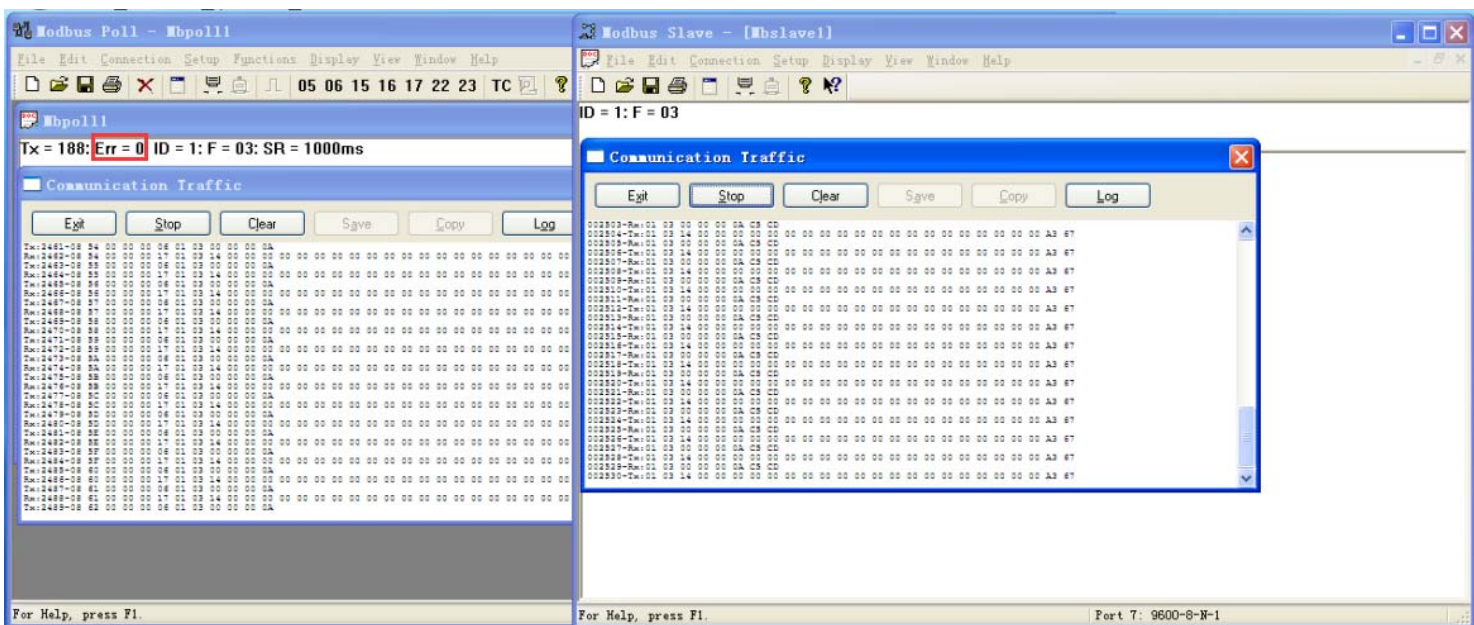
打开 Modbus Slave 软件进行配置，参数配置与 WEB 显示一致。
点击 Connection，选择 Serial Port，串口参数与 WEB 显示一致，选择 RTU 模式。



选择正确的通讯端口
点击 OK 即连接上（红色字体 No Connection 会消失）



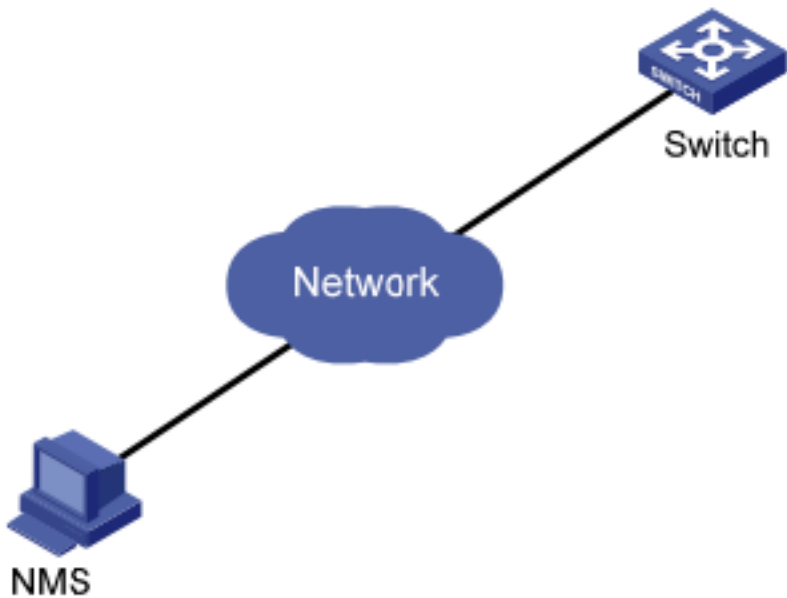
4、收发 Modbus 数据



错误为 0 即为测试正常通过。照此方法依次测试 RS-422/485 串口通讯。

4.15 管理SNMP

您可通过 NMS（Network Management Station，网管工作站）登录到交换机上，通过交换机上的 Agent 模块对交换机进行管理、配置，如下图所示。NMS 和 Agent 之间运行的协议为 SNMP（Simple Network Management Protocol，简单网络管理协议）。SNMP 是使用 TCP/IP 协议族对互联网上的设备进行管理的一个框架，它提供一组基本的操作来监视和维护互联网。



优势

- 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务分别与设备物理特性和下层的联网技术相对独立，从而实现对不同厂商设备的管理，特别适合在小型、快速和低成本的环境中使用。

网络元素

- NMS（Network Management Station，网络管理站）是运行 SNMP 客户端程序的工作站，能够提供非常友好的人机交互界面，方便网络管理员完成绝大多数的网络管理工作。
- Agent 是驻留在设备上的一个进程，负责接收、处理来自 NMS 的请求报文。在一些紧急情况下，如接口状态发生改变等，Agent 也会通知 NMS。

NMS 是 SNMP 网络的管理者，Agent 是 SNMP 网络的被管理者。NMS 和 Agent 之间通过 SNMP 协议来交互管理信息。

基本操作

- Get 操作：NMS 使用该操作查询 Agent 的一个或多个对象的值。
- Set 操作：NMS 使用该操作重新设置 Agent 数据库（MIB，Management Information Base）中的一个或多个对象的值。
- Trap 操作：Agent 使用该操作向 NMS 发送报警信息。
- Inform 操作：NMS 使用该操作向其他 NMS 发送报警信息。

协议版本

- SNMP v1 采用团体名（Community Name）认证。团体名用来定义 SNMP NMS 和 SNMP Agent 的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP NMS 对 SNMP Agent 的访问。
- 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 和 InformRequest），支持更多的数据类型（Counter64 等），提供了更丰富的错误代码，能够更细致地区分错误。
- SNMP v3 提供了基于用户的安全模型（USM，User-Based Security Model）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP NMS 和 SNMP Agent 之间的通信提供更高的安全性。

Agent 可以同时配置多个版本，与不同的 NMS 交互采用不同的版本交互。但是当 Agent 和某个 NMS 通信时，Agent 和该 NMS 上的 SNMP 版本配置必须相同（即都配置为 SNMP v1 或者都配置为 SNMP v2c 或者都配置为 SNMP v3），才能成功互访。

本设备支持 SNMP v1/v2c/v3。SNMP v1 和 SNMP v2c 使用一组字符串来进行认证，也就是说 SNMP 服务器可以访问所有对象，根据不同的字符串提供用户不同的权限。如 public 权限为只读，而 private 为读/写。SNMP V3 要求用户选择 MD5 或 SHA 中的一种认证方式，它是最安全的一种协议。您也可以通过数据加密来提升数据传输的安全级别。

表 4-26 SNMP V1/V2c/V3

协议版本	访问模式	认证类型	数据加密	说明
SNMP v1，v2c	Read Community	Community string	无	使用 Community string 匹配认证。
	Read /Write Community	Community string	无	使用 Community string 匹配认证。
SNMP v3	Read Community	基于 MD5 或 SHA 的认证	无	基于 MD5 或 SHA 算法的认证，认证要求为 9~15 位密码。
			数据密钥	基于 MD5 或 SHA 算法和数据密钥的的认证，认证和数据密钥要求为 9~15 位密码和密钥。
	Read /Write Community	基于 MD5 或 SHA 的认证	无	基于 MD5 或 SHA 算法的认证，认证要求为 9~15 位密码。
			数据密钥	基于 MD5 或 SHA 算法和数据密钥的的认证，认证和数据密钥要求为 9~15 位密码和密钥。

4.15.1. 创建SNMP团体名

SNMP 团体名是使用 SNMP v1, v2c 协议的认证，起到类似密码的作用，可以限制 SNMP NMS 对 SNMP Agent 的访问。

步骤1 在左侧导航中选择“SNMP 管理 < 帐户”，进入 SNMP 团体名设置页面。

SNMP 团体名

SNMP 用户

SNMP 版本

v1

团体名

public

访问模式

RO

应用

团体列表

SNMP 版本	团体名	访问模式	删除
---------	-----	------	----

步骤2 设置 SNMP 团体名的 SNMP 版本、团体名称和访问模式。

表 4-27 SNMP 团体名参数

值	值域	描述
SNMP 版本	v1, v2c 缺省值：v2c	选择团体名认证使用的 SNMP 协议。 v1：表示设置 v1 的团体名认证。 v2c：表示设置 v2c 的团体名认证。
团体名	取值范围： 3~16 个字符	设置 SNMP NMS 用于访问或设置 SNMP Agent 的认证字符串。
访问模式	RO, RW 缺省值：RW	设置 SNMP NMS 使用团体名来访问 SNMP Agent 的权限。 RO：只读模式，SNMP NMS 使用团体名只能读取 SNMP Agent 的数据，不能设置。缺省团体名为“public”。 RW：读写模式，SNMP NMS 使用团体名可以读取或设置 SNMP Agent 的数据。缺省团体名为“private”。

步骤3 单击“应用”，将所设置的团体名参数保存到团体列表中。

——结束

4.15.2. 创建SNMP用户名

USM（User-based Security Model）用户名使用 SNMP v3 协议封装，使用 MD5 或 SHA 和密钥加密，可以提高 SNMP NMS 和 SNMP Agent 之间通信的安全性。

步骤1 在左侧导航中选择“SNMP 管理 < 帐户”。

步骤2 单击“SNMP 用户名”页签，进入 USM 用户名设置页面。

SNMP 团体名

SNMP 用户

USM 用户

访问模式

SNMP V3 封装

授权算法

授权密码

私有算法

私有密码

RW

☐

MD5

Disabled

应用

用户列表

SNMP 版本	USM 用户	访问模式	删除
---------	--------	------	----

步骤3 设置 SNMP 用户名的用户名称、访问模式和 SNMP v3 封装等参数。

表 4-28 SNMP 用户名参数

值	值域	描述
---	----	----

USM 用户	取值范围： 3~16 个字符	设置 USM 用户名。
访问模式	RO，RW 缺省值：RW	设置 SNMP NMS 使用 USM 用户名来访问 SNMP Agent 的权限。 RO：只读模式，SNMP NMS 使用团体名只能读取 SNMP Agent 的数据，不能设置。 RW：读写模式，SNMP NMS 使用团体名可以读取或设置 SNMP Agent 的数据。
SNMP V3 封装	-	设置是否使用 SNMP V3 安全加密方式。如 SNMP V3 封装不被选择， 验证和加密都将无需执行。
授权算法	MD5，SHA 缺省值：MD5	选择验证所用的安全模式。 MD5：使用 MD5 算法作为验证模式。 SHA：使用 SHA 算法作为验证模式，比 MD5 更安全。
授权密码	取值范围： 9~15	设置授权算法的验证密码。
私有算法	Disabled， DES，AES 缺省值： Disabled	选择数据加密的安全模式。 Disabled：禁用数据加密。此时私有密码不可设置。 DES：使用 DES 数据加密模式。 AES：使用 AES 数据加密模式，比 DES 更安全。
私有密码	取值范围： 9~15	设置数据加密的验证秘密码。

步骤4 单击“应用”，将所设置的用户名参数保存到用户列表中。
——结束

4.15.3. 设置SNMP陷阱

SNMP 陷阱是指 SNMP Agent 在任何时候主动向 SNMP NMS 发送端口的 Linkup 和 Linkdown 情况。您可以根据实际情况设置 SNMP 陷阱的使能状态、发送陷阱的端口和接收告警信息的 SNMP NMS 所在服务器的 IP 地址。

步骤1 在左侧导航中选择“SNMP 管理 < SNMP 陷阱”，进入全局陷阱设置页面。

全局陷阱设置

增加陷阱主机IP

陷阱端口

全局陷阱设置

SNMP 陷阱

Disabled

应用

步骤2 使能 SNMP 陷阱。

1. 在“SNMP 陷阱”中选择“Enabled”。

全局陷阱设置

增加陷阱主机IP

陷阱端口

全局陷阱设置

SNMP 陷阱

Enabled

Disabled

Enabled

应用

2. 单击“应用”，使能 SNMP 陷阱。

步骤3 设置接收陷阱信息主机的 IP 地址。

1. 单击“增加陷阱主机 IP”页签，进入陷阱主机 IP 设置页面。

2. 在“主机 IP”中设置接收 SNMP 陷阱信息的主机 IP，如 192.168.1.100。

增加陷阱主机IP

主机 IP	192.168.1.100
应用	

3. 单击“应用”，所设置的 IP 地址保存到陷阱列表中。

步骤4 设置发送陷阱信息的端口。

说明：只有使能 SNMP 陷阱才能设置陷阱端口参数。

1. 单击“陷阱端口”页签，进入陷阱端口设置页面。

2. 选择所需设置的端口并设置该端口是否使能 SNMP 陷阱功能。

说明：交换机各端口缺省情况下均禁止 SNMP 陷阱功能。

3. 单击“应用”，使所设置的端口陷阱功能生效。

——结束

4.16 管理系统信息

系统管理提供了交换机基本信息的管理和维护功能，主要包括修改 IP、设置简单网络时间协议、设置告警、管理 VLAN、查看系统日志、Ping 诊断、TFTP 服务等。

4.16.1. 修改IP地址

交换机只支持静态 IP 地址，需手动设置指定的 IP 地址、子网掩码和网关。通过所设置的 IP 地址可以访问交换机的配置页面。设置新的 IP 地址后需重新登录。

步骤1 在左侧导航中选择“系统管理 < IP 配置”，进入 IP 配置页面。

步骤2 修改交换机的 IP 地址、子网掩码和网关，是交换机与访问交换机的主机在同一局域网。

IP 配置

IP 地址	192 . 168 . 1 . 171
子网掩码	255 . 255 . 255 . 0
网关	192 . 168 . 1 . 1
应用	

步骤3 单击“应用”，使所设置的 IP 地址生效并提示重新登录 Web 界面。

——结束

4.16.2. 设置简单网络时间协议

在大型的网络中，如果依靠管理员手工配置来修改网络中各台设备的系统时间，不但工作量巨大，而且也不能保证时间的精确性。NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，并提供较高的时间同步精度。

NTP 时间同步过程中需要进行复杂的时钟优选运算，时间同步速度较慢，并且占用较多的系统资源。SNTP（Simple NTP，简单 NTP）简化了 NTP 的时间同步算法，以牺牲时间精度为代价实现了时间的快速同步，并减少了占用的系统资源。在时间精度要求不高的情况下，可以使用 SNTP 来实现时间同步。

SNTP 既提供了客户端功能也提供服务器端功能。如果交换机作为 SNTP 服务器端，交换机作为 SNTP 服务器使用，其他交换机的时间可以同步到该交换机。设置该交换机系统时间年、月、日、时、分和秒，让其他交换机都同步到该交换机设置的时间。如果交换机作为 SNTP 客户端，可以通过 SNTP 服务器获取同步时间来设置该交换机的时间。

作为客户端

步骤1 在左侧导航中选择“系统管理 < 简单网络时间协议”，进入 SNTP 配置页面。

步骤2 在“SNTP 模式”中选择“Client”。

步骤3 设置服务器 IP 地址、响应时间和时区偏移等参数。

表 4-29 SNTP 客户端参数

值	值域	描述
服务器 IP 地址	格式 XXX.XXX.XXX.XXX 如 192.168.1.1	设置 SNTP 服务器的 IP 地址。
响应时间	取值范围： 1~59s 缺省值：0	设置从 SNTP 服务器上更新时间的频率。
时区偏移	取值范围： GMT -12:00~GMT 12:00 缺省值：GMT -12:00	设置格林威治标准时间（GMT）和本地时间的时差。
时分偏移	取值范围： 1~59min 缺省值：0	设置格林威治标准时间（GMT）和本地时间的分钟偏差。

SNTP 配置

SNTP 配置

SNTP 模式

Client

服务器IP 地址

192.168.1.1

xxx.xxx.xxx.xxx

响应时间 1~59(s)

5

时区偏移

GMT 8:00

时分偏移0~59(min)

0

年

2014

月

2

日

20

时

8

分

0

秒

0

应用

步骤4 单击“应用”，使所设置参数生效，所获取的时间在分别年、月、日、时、分、秒中显示。

作为服务器

步骤1 在左侧导航中选择“系统管理 < 简单网络时间协议”，进入 SNTP 配置页面。

步骤2 在“SNTP 模式”中选择“Service”。

步骤3 年、月、日和时、分、秒等参数。如时间为“2014-02-20 08:00:00”。

SNTP 配置

SNTP 配置

SNTP 模式

Service

服务器IP 地址

xxx.xxx.xxx.xxx

响应时间 1~59(s)

0

时区偏移

GMT -12:00

时分偏移0~59(min)

0

年

2014

月

2

日

20

时

8

分

0

秒

0

应用

步骤4 单击“应用”，使所设置参数生效。

——结束

4.16.3. 设置告警

本设备提供告警功能，提供继电器、电源、端口和环网的告警。

步骤1 在左侧导航中选择“系统管理 < 告警”，进入告警配置页面。

步骤2 在“告警”中选择“Enable”，使能全局告警。

 **说明：**使能全局告警后，才能设置继电器、电源、端口的告警。告警状态缺省值为“Disable”。

告警

系统告警

讯记环网告警

告警

Enabled

应用

系统告警

步骤1 单击“系统告警”页签，进入系统设置页面。

步骤2 设置继电器告警有效状态。

根据现场实际使用的报警设备状态设置交换机的“继电器告警有效状态”。

如交换机系统的“继电器告警有效状态”需与现场实际使用的报警设备的状态一致。如现场的报警设备状态为“常开”，则把“继电器告警有效状态”设置为“常开”。

告警

系统告警

讯记环网告警

继电器告警有效状态

常闭

继电器当前状态

闭合

步骤3 设置电源告警。

在“电源告警设置”区域中设置电源 1 或电源 2 的告警状态。

电源告警设置

电源号	告警设置	电源状态	电源号	告警设置	电源状态
1	☒禁用 ☐启用	故障	2	☒禁用 ☐启用	正常

步骤4 设置端口告警。

在“端口告警设置”区域中设置各端口的告警状态。

端口告警设置

电源号	告警设置	端口状态	电源号	告警设置	端口状态
FE1	☒禁用 ☐启用	连接	FE2	☒禁用 ☐启用	断开
FE3	☒禁用 ☐启用	断开	FE4	☒禁用 ☐启用	连接
FE5	☒禁用 ☐启用	断开	FE6	☒禁用 ☐启用	断开
FE7	☒禁用 ☐启用	断开	FE8	☒禁用 ☐启用	断开
GE1	☒禁用 ☐启用	断开	GE2	☒禁用 ☐启用	断开

应用

步骤5 单击“应用”，使所设置的告警参数生效。

环网告警

步骤1 单击“讯记环网告警”页签，进入环网告警设置页面。

告警

系统告警

讯记环网告警

讯记环网告警

RingID

1

告警使能

禁用

应用

告警列表

RingID	端口	类型	修改
1	ring-broken	禁用	修改
2	ring-broken	禁用	修改

步骤2 在“Ring ID”中选择需设置的环网 ID，并设置该环网告警的使能状态。

步骤3 单击“应用”，使所设置的告警参数生效。

——结束

4.16.4. 设置管理VLAN

管理 VLAN 是指用于登录交换机配置页面进行交换机管理和维护的 VLAN 组。该 VLAN 组必须存在 VLAN 列表中。

步骤1 在左侧导航中选择“系统管理 < 管理 VLAN”，进入设置管理 VLAN 页面。

管理VLAN

管理VLAN配置

VID

1

应用

步骤2 在“VID”中选择需要设置为管理 VLAN 的 VLAN ID。

步骤3 单击“应用”，使所设置的 VLAN 生效。

——结束

4.16.5. 查看系统日志

显示交换机系统的告警日志，您可以根据告警信息进行交换机维护。如果系统日志过多可单击“重置”清除系统日志。

系统日志

序号	告警 信息
----	-------

重置

4.16.6. Ping诊断

通过 Ping IP 地址可以检查交换机和某设备之间的连接情况。

步骤1 在左侧导航中选择“系统管理 < Ping 诊断”，进入 Ping 诊断页面。

Ping 诊断

Ping 诊断

Ping

应用

步骤2 设置需要诊断的 IP 地址，如 192.168.1.1。

步骤3 单击“应用”。

如果能 Ping 通，则提示 IP 地址有效；如果不能 Ping 通，则提示 IP 地址不能 Ping 通。

——结束

4.16.7. 修改帐户

本设备提供用户名的密码修改。您可以通过该功能修改当前用户名的密码。

步骤1 在左侧导航中选择“系统管理 < 帐户”，进入帐户修改页面。

帐户

修改帐户

用户名	
密码	
确认密码	
应用	

序号	用户名	访问模式	修改
1	admin	Admin	修改

步骤2 设置新用户名的密码。

 **说明：**用户名不可更改。

步骤3 单击“应用”，使所设置用户名替代当前的用户名，需重新登录。

——结束

4.16.8. 更新Firmware

TFTP（Trivial File Transfer Protocol，简单文件传输协议）使用方便，在连接过程中不需要认证控制，适用于客户端和服务端之间不需要复杂交互的环境。通过 TFTP 的升级固件功能您可以更新交换机软件。在升级交换机软件之前，请确保交换机与 TFTP 服务器正确连接。

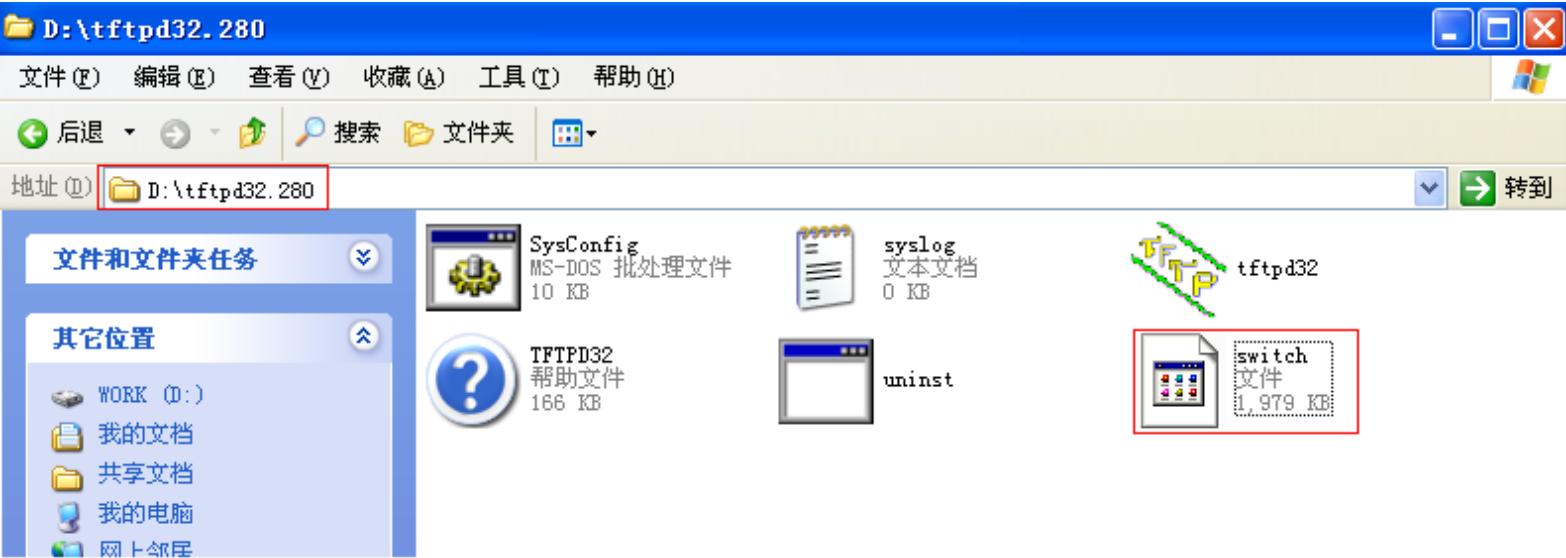
步骤1 打开附件中的“tftpd32.exe”。



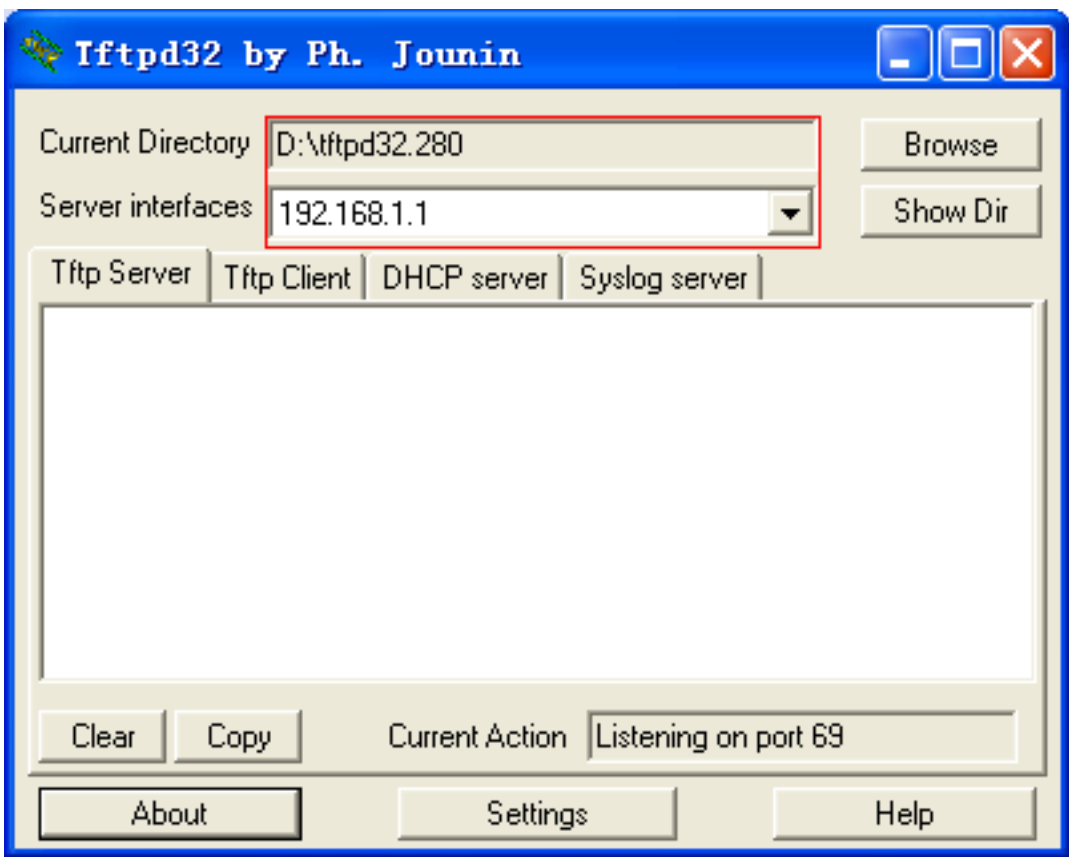
tftpd32.280.rar

步骤2 在 TFTP 中设置 TFTP 服务器的 IP 地址和 Firmware 存放路径。

如 TFTP 服务器的 IP 地址为“192.168.1.1”，固件“switch”存放在 TFTP 服务器的“D:\tftpd32.280”中。



在 TFTP 中设置如下图所示。



步骤3 在左侧导航中选择“系统管理 < TFTP 服务”，进入 TFTP 的升级固件页面。

步骤4 设置 TFTP 服务器的 IP 地址和升级软件的名称。



步骤5 单击“应用”，进行软件升级。

说明：升级可能需要几分钟，在升级过程中不可断开电源或进行其他设置。

步骤6 在“重启系统”中单击“重启不保存配置”，重启交换机使所升级的软件生效。

——结束

4.16.9. 下载或上传配置文件

TFTP（Trivial File Transfer Protocol，简单文件传输协议）使用方便，在连接过程中不需要认证控制，适用于客户端和服务端之间不需要复杂交互的环境。通过 TFTP 的配置文件功能您上传或下载的配置文件。在上传或下载配置文件之前，请确保交换机与 TFTP 服务器正确连接。

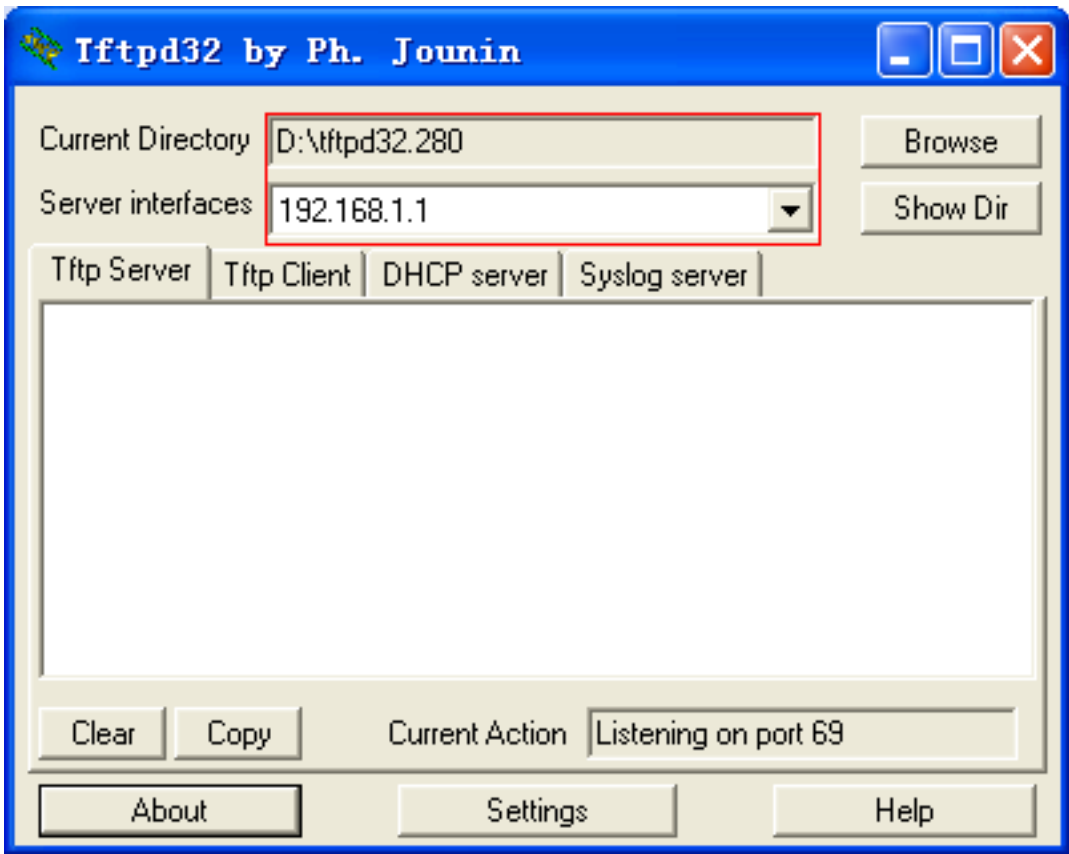
步骤1 打开附件中的“tftpd32.exe”。



tftpd32.280.rar

步骤2 在 TFTP 中设置 TFTP 服务器的 IP 地址和配置文件存放路径。

如 TFTP 服务器的 IP 地址为“192.168.1.1”，配置文件存放在 TFTP 服务器的“D:\tftpd32.280”中，则在 TFTP 中设置如下图所示。



步骤3 在左侧导航中选择“系统管理 < TFTP 服务”。

步骤4 单击“配置文件”页签，进入配置文件页面。



步骤5 设置 TFTP 服务器的 IP 地址。

步骤6 单击“下载”或者“上传”，下载配置文件到 TFTP 的指定路径中或上传配置文件到交换

机系统。文件放在  中。

——结束

4.17 保存配置

通过保存设置功能，您可以保存当前配置的数据，防止交换机断开电源或重启时数据丢失。

步骤1 在左侧导航中选择“保存配置”。

步骤2 单击“保存”。

步骤3 单击“确认”，保存当前配置的数据成功。

——结束

4.18 重启系统

您可以选择保存配置且重启、重启不保存配置或恢复出厂设置这三种模式来重启交换机系统。

步骤1 在左侧导航中选择“重启系统”。

步骤2 单击您所需要的重启模式。

如单击“保存配置且重启”，保存当前登录所配置的数据并重启交换机。

表 4-30 重启系统参数

值	值域	描述
保存配置且重启	-	保存当前用户所配置的数据并重启交换机。

重启不保存配置	-	不保存当前用户所配置的数据重启交换机。
恢复出厂设置	-	恢复交换机系统中的所有数据到出厂设置的数据。

——结束

4.19 退出系统

您可以通过“退出系统”功能，退出当前用户的登录。

步骤1 在左侧导航中选择“退出系统”。

步骤2 在弹出的对话框中单击“确定”，退出当前用户登录的 Web 界面。

——结束

5. 命令行操作

本章介绍使用命令行进行交换机配置的具体操作。

通过命令行的操作步骤请参见“[2.2 通过 Telnet 远程访问](#)”。命令行接口中内置有语法帮助。如果对某个命令的语法不太确定，请输入该命令中已知道的前面的部分，然后键入“?”或“空格加?”，命令行会提示已经输入的部分命令剩余部分的可能的命令清单。这样就可以根据提示的命令继续输入命令，直至提示命令为<cr>时，表示命令输入完毕，按回车就可以执行所键入的命令。

系统提供输入“tab”键补全命令的功能。也就是用户输入部分命令，然后输入“tab”键，系统自动检索匹配的命令如果检索到相应的命令，系统可以自动补齐。如果检索到多个命令，系统会显示可选择的命令。

系统对于输入的大小写进行区分，因此对于输入的命令和参数的大小写要严格一致，否则系统会提示错误。

命令中的斜体字代表需要设置的参数变量，可按实际使用情况修改。如 interface ethernet *fe1* 中的 *fe1* 可根据实际使用情况修改为其他端口。

5.1 常用命令

help命令

执行 help 命令显示系统当前路径下所能操作的命令。

如执行“interface ethernet *fe1*”进入端口 FE1 后，执行“help”命令显示 FE1 下可进行的操作。

```
SWITCH# interface ethernet fe1
SWITCH<fe1># help
cos                - configure port cos
duplex             - setting the mode of duplex
flow-control       - enable flow-control
learning           - enable to learn Mac Address on the current ethernet
                    port
line-rate          - rate limited setting
link-aggregation   - add current port to link-aggregation-group
mirroring-port     - configure the source port
monitor-port       - configure the destination port
priority           - configure interface Qos priority
qinq               - port double qinq disable|enable
quit               - exit this mode
shutdown           - force the interface to be down
speed              - setting the speed of interface
switchport         - configure the port
undo               - delete or clear some settings
Global command:
clear              - Clear the screen
exit               - Exit intermediate mode
help               - Show command help
show               - help string for show
SWITCH<fe1>#
```

show命令

show <功能参数>，显示该功能当前的配置信息。
如执行“show system-information”，显示系统信息。

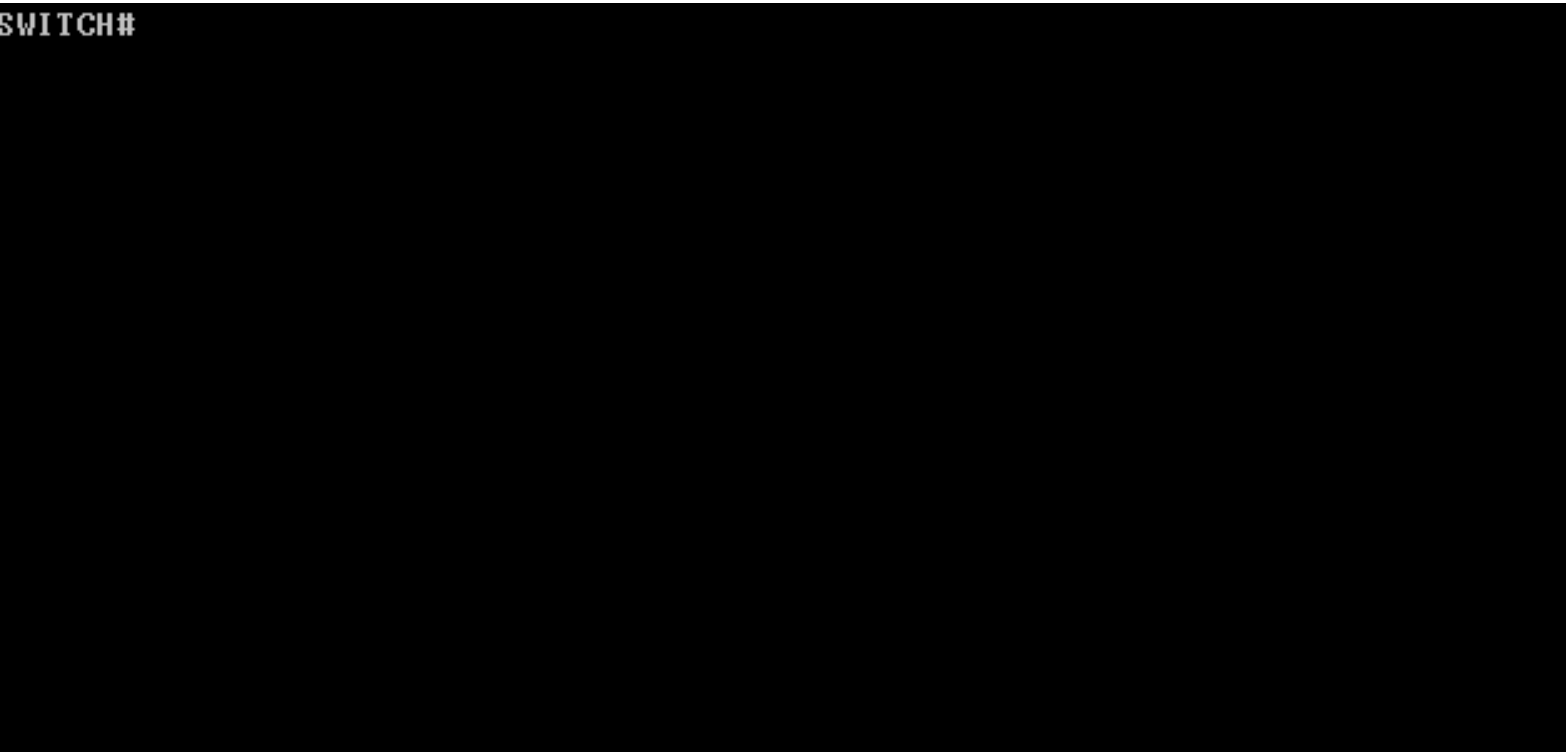
```
SWITCH# show system-information

System Name       : Optical Industrial Ethernet Switch
System Model      : Ck7080
Hardware Version  : VER 1.0.02
Firmware Version  : V-3.1.198-<Jul 15 2017 16:05:53>
MAC Address       : 00-a1-d3-88-13-68
System ID         :

SWITCH#
```

clear命令

执行 clear 命令清除当前命令行界面中的显示，即清屏作用。
如执行“clear”命令清屏。



undo命令

undo <功能参数>，显示该功能当前的配置信息。
如执行“undo vlan 2”，则删除 VID 为 2 的 VLAN 组。

save命令

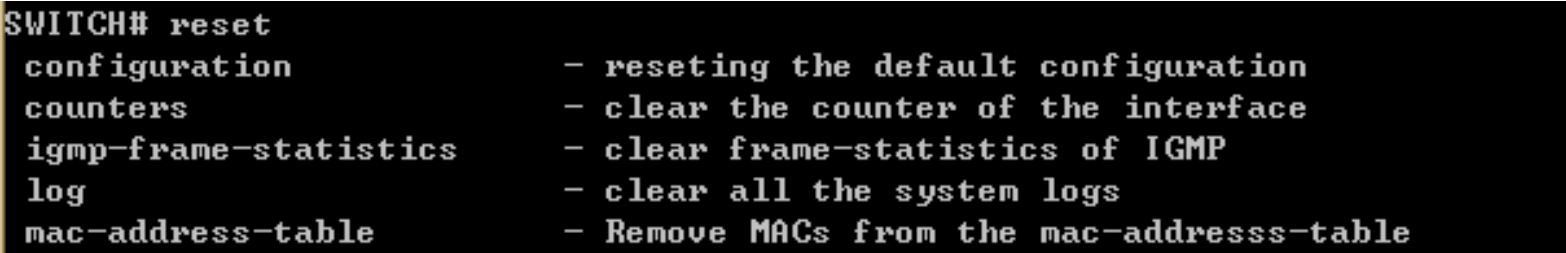
执行 save 命令用于保存当前的配置信息。

reboot命令

执行 reboot 命令用于重启设备。

reset命令

执行 reset 命令用于恢复设备的出厂设置和重置端口数据、系统日志、MAC 地址表等数据。
如执行“reset configuration”，恢复出厂设置。

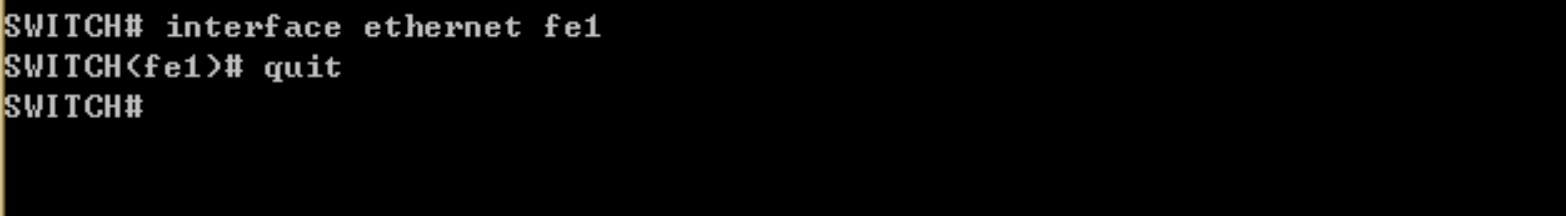


exit命令

执行 exit 命令用于退出当前登录。

quit命令

执行 quit 命令用于退出当前功能的操作。
如在端口 FE1 操作下执行“quit”，则退出 FE1 的操作。



5.2 查看系统信息

系统信息即交换机的基本信息，主要包括系统名称、MAC 地址、硬件版本、软件版本和出厂编号等信息。当需要了解交换机的基本信息时，您可以执行命令“show system-information”查看系统信息。

```
SWITCH# show system-information

System Name       : Optical Industrial Ethernet Switch
System Model      : Ck7080
Hardware Version  : VER 1.0.02
Firmware Version  : V-3.1.198-(Jul 15 2017 16:05:53)
MAC Address       : 00-a1-d3-88-13-68
System ID         :

SWITCH#
```

5.3 设置端口参数

端口设置是对端口的访问状态、协商模式、速率/双工、流量控制和 MAC 地址学习的配置和管理。您可以根据实际情况设置端口的各种参数。

如需要设置端口 FE1 的速率&双工为 100full，启用流控功能，限制出口速率为 10M，可以自主学习 MAC 地址，操作步骤如下：

步骤1 执行“interface ethernet fe1”，进入端口 FE1 的设置。

 **说明：**命令中的“fe1”为交换机的端口。可根据现场实际情况修改。

```
SWITCH# interface ethernet fe1
SWITCH<fe1>#
```

步骤2 执行“speed 100M”，设置 FE1 的速率为 100M。

 **说明：**“speed”命令下可选参数有 1000M、100M、10M 和 auto。其中 1000M、100M、10M 为强制模式，配置端口的速率，auto 为端口速率自适应模式。缺省状态为 auto。

```
SWITCH<fe1># show ethernet status-information

PORT      STATE  LINK  NEGO  SPEED  DUPLEX  FLOWCTRL  LEARN  EGRESS
-----
FE-1      enable down   Yes   --     --     off       Yes   disable
FE-2      enable down   Yes   --     --     off       Yes   disable
FE-3      enable down   Yes   --     --     off       Yes   disable
FE-4      enable up     Yes   100M   full   off       Yes   disable
FE-5      enable down   Yes   --     --     off       Yes   disable
FE-6      enable up     Yes   100M   full   off       Yes   disable
FE-7      enable down   Yes   --     --     off       Yes   disable
FE-8      enable down   Yes   --     --     off       Yes   disable
GE-1      enable down   No    --     --     off       Yes   disable
GE-2      enable down   No    --     --     off       Yes   disable

SWITCH<fe1># speed
1000M      - setting 1000M
100M       - setting 100M
10M        - setting 10M
auto       - setting the mode of speed to be auto
SWITCH<fe1># speed 100M
```

步骤3 执行“duplex full”，设置 FE1 的双工模式为 full。

 **说明：**“duplex”命令下可选参数有 full、half 和 auto。其中 full、half 为强制模式，配置端口的双工模式，auto 为自适应模式。缺省状态为 auto。

```
SWITCH<fe1># duplex
  auto          - setting auto mode
  full          - setting full mode
  half          - setting half mode
SWITCH<fe1># duplex full
```

步骤4 执行“flow-control”，启用 FE1 的流控功能。

```
SWITCH<fe1># flow-control
```

步骤5 执行“line-rare egress 10000”，设置 FE1 的出口速率为 10M。

说明：百兆端口的出口速率取值范围为 62~100000kbps，千兆端口的出口速率取值范围为 62~2500000kbps，交换机会自动将所设置的值转换为与之最接近的速率。由于交换机芯片内部的出口速率算法限制，千兆端口的出口速率最大取值为 250000kbps。

```
SWITCH<fe1># line-rate egress 10000
Egress rate has been set 10000 kbps on FE-1

SWITCH<fe1>#
```

步骤6 执行“learning”，开启 FE1 的 MAC 地址学习能力。

```
SWITCH<fe1># learning
```

步骤7 执行“show ethernet status-information”，可看到 FE1 的端口信息已设置成功。

```
SWITCH<fe1># show ethernet status-information
```

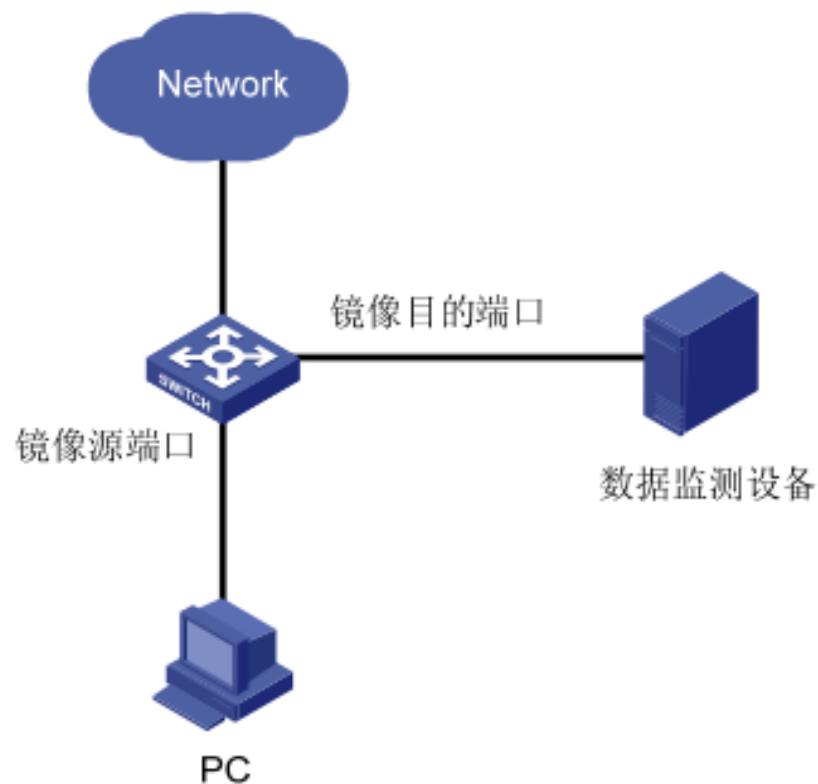
PORT	STATE	LINK	NEGO	SPEED	DUPLEX	FLOWCTRL	LEARN	EGRESS
FE-1	enable	down	No	--	--	on	Yes	10000kbps
FE-2	enable	down	Yes	--	--	off	Yes	disable
FE-3	enable	down	Yes	--	--	off	Yes	disable
FE-4	enable	up	Yes	100M	full	off	Yes	disable
FE-5	enable	down	Yes	--	--	off	Yes	disable
FE-6	enable	up	Yes	100M	full	off	Yes	disable
FE-7	enable	down	Yes	--	--	off	Yes	disable
FE-8	enable	down	Yes	--	--	off	Yes	disable
GE-1	enable	down	No	--	--	off	Yes	disable
GE-2	enable	down	No	--	--	off	Yes	disable

```
SWITCH<fe1>#
```

——结束

5.4 设置端口镜像

端口镜像功能可以用来监视一个或多个端口的接收、发送或收发的数据，以便于在线调测和监控网络数据状态。其中被监视的端口称为镜像源端口，监视端口称为镜像目的端口。源端口和镜像目的端口必须位于同一台交换机上，镜像目的端口不能与源端口相同。端口镜像组网图如下图所示。您可以使用数据监测设备连接镜像目的端口接收所监控的数据进行网络数据分析或监控。



如设置 FE1 作为镜像目的端口，需要监测 FE2 的发送数据、FE3 的接收数据和 FE4 的收发数据，操作步骤如下：

步骤1 设置 FE1 为监视口。

1. 执行 “interface ethernet fe1”，进入端口 FE1 的设置。
2. 执行 “monitor-port”，设置 FE1 为监视口。

```
SWITCH<fe1># mirroring-port _
```

3. 执行 “quit”，退出 FE1 设置。

步骤2 设置监测 FE2 的发送数据。

1. 执行 “interface ethernet fe2”，进入端口 FE2 的设置。
2. 执行 “mirroring-port egress”，监测 FE2 的发送数据。

📖 说明：“mirroring-port” 命令下的 both 表示监测收发数据，egress 表示监测发送数据，ingress 表示监测接收数据。

```
SWITCH<fe2># mirroring-port egress _
```

3. 执行 “quit”，退出 FE2 设置。

步骤3 设置监测 FE3 的接收数据。

1. 执行 “interface ethernet fe3”，进入端口 FE3 的设置。
2. 执行 “mirroring-port ingress”，监测 FE3 的发送数据。

📖 说明：“mirroring-port” 命令下的 both 表示监测收发数据，egress 表示监测发送数据，ingress 表示监测接收数据。

```
SWITCH# interface ethernet fe3
SWITCH<fe3># mirroring-port ingress
```

3. 执行 “quit”，退出 FE3 设置。

步骤4 设置监测 FE4 的收发数据。

1. 执行 “interface ethernet fe4”，进入端口 FE4 的设置。
2. 执行 “mirroring-port both”，监测 FE4 的收发数据。

📖 说明：“mirroring-port” 命令下的 both 表示监测收发数据，egress 表示监测发送数据，ingress 表示监测接收数据。

```
SWITCH<fe3># quit
SWITCH# interface ethernet fe4
SWITCH<fe4># mirroring-port both
```

3. 执行 “quit”，退出 FE4 设置。

步骤5 执行“show mirror”，可查看已设置的监视口和被监视口。

```
SWITCH<fe4># quit
SWITCH# show mirror
Monitor-port:
    FE-1
Mirroring-port:
    FE-2    egress
    FE-3    ingress
    FE-4    egress&ingress
```

——结束

5.5 创建端口隔离组

端口隔离组是采用端口隔离特性实现端口之间的隔离。将需要进行隔离的端口加入到一个隔离组中，可以实现隔离组内端口之间二层数据的隔离。端口隔离组功能提供了更安全、灵活的组网方案。

如需要把 FE1、FE2 和 FE3 之间的数据相互隔离，则可把 FE1、FE2 和 FE3 加入到一个隔离组中，实现 FE1、FE2 和 FE3 之间的数据独立，操作步骤如下：

步骤1 执行“port-isolate-group 1”，创建一个组号为 1 的隔离组。

 说明：端口隔离组号的取值范围为 1~16。

```
SWITCH# port-isolate-group 1_
```

步骤2 执行“interface ethernet fe1”，设置 FE1 为隔离组 1 的成员。

```
SWITCH# port-isolate-group 1
SWITCH<inter_prompt.isolate># interface ethernet fe1
```

步骤3 执行“interface ethernet fe2”，设置 FE2 为隔离组 1 的成员。

```
SWITCH<inter_prompt.isolate># interface ethernet fe2
```

步骤4 执行“show port-isolate-group”，可查看已设置的端口隔离组信息。

```
SWITCH<inter_prompt.isolate># show port-isolate-group
Isolate-Group-1<members>:
    FE-1
    FE-2
```

步骤5 执行“quit”，退出隔离组 1 的设置。

——结束

5.6 创建端口聚合组

端口聚合是将多个物理连接当作一个单一的逻辑连接来处理，如将 4 个 100M 的端口捆绑后成为一个高达 400M 的连接。它允许两个交换机之间通过多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。同一聚合组内的端口基本配置应保持一致。

如将 100M 全双工模式的 FE1 和 FE2 聚合，组成 200M 的连接，操作步骤如下：

步骤1 执行“link-aggregation group 1 mode manual”，创建一个组号为 1 的聚合组。

 说明：端口聚合组号的取值范围为 1~4；聚合模式有 manual 和 static 两种模式，此两种模式均只能手工设置或删除，不允许系统自动添加或删除，其中 static 为系统预留功能，暂不提供。

```
SWITCH# link-aggregation group 1 mode manual
```

步骤2 设置 FE1 为聚合组 1 的成员。

1. 执行“interface ethernet fe1”，进入端口 FE1 的设置。
2. 执行“link-aggregation group 1”，把 FE1 加入到聚合组 1 中。

```
SWITCH# interface ethernet fe1
SWITCH<fe1># link-aggregation group 1
```

- 3. 执行“quit”，退出 FE1 设置。
 - 步骤3 设置 FE2 为聚合组 1 的成员。
 - 1. 执行“interface ethernet fe2”，进入端口 FE2 的设置。
 - 2. 执行“link-aggregation group 1”，把 FE2 加入到聚合组 1 中。
- ```
SWITCH<fe2># link-aggregation group 1
```
- 3. 执行“quit”，退出 FE2 设置。
  - 步骤4 执行“show link-aggregation summary”，可查看已设置的端口聚合组信息。

```
SWITCH<fe2># quit
SWITCH# show link-aggregation summary
Port AggregationGroupID Type
FE-1 1 manual
FE-2 1 manual

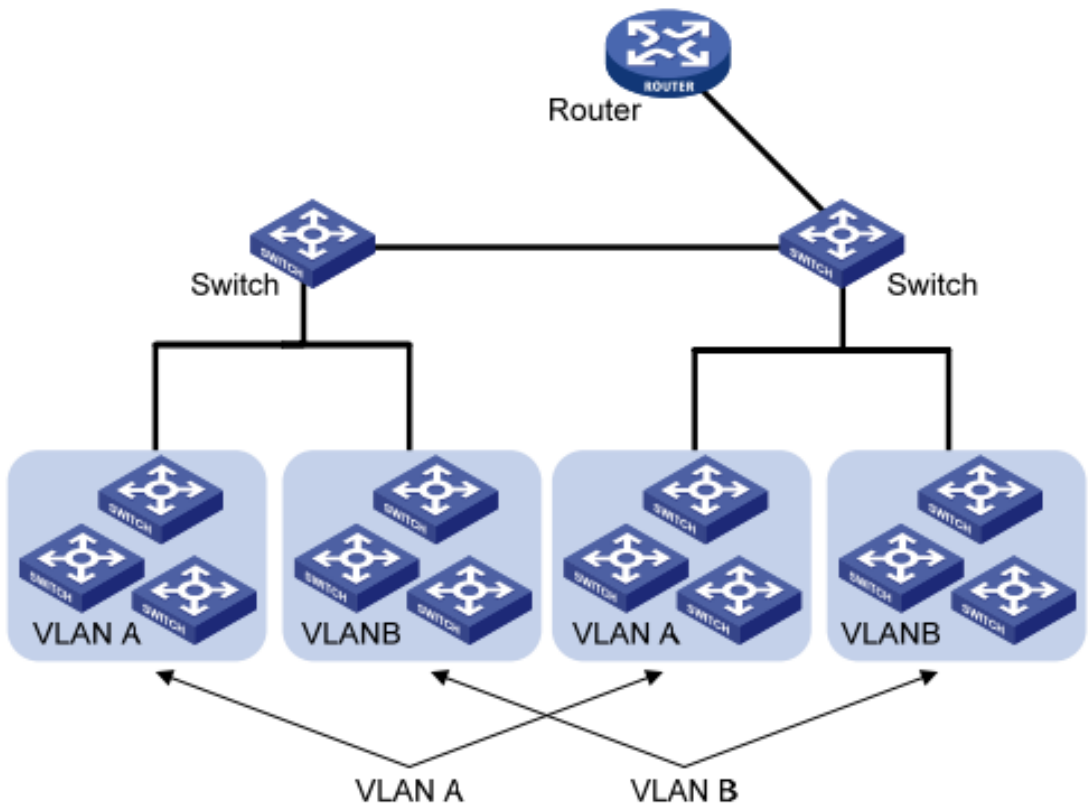
SWITCH#
```

——结束

## 5.7 管理虚拟局域网

### VLAN的概念

VLAN（Virtual Local Area Network，虚拟局域网）是一组逻辑上的设备和用户，这些设备和用户不受物理位置的限制，可以根据功能、部门及应用等因素设定为一个群组，使它们之间通信像在同一个物理分段中。处于不同 VLAN 内的主机之间通信必须通过路由器或三层交换机设备。



### VLAN的优点

- VLAN 的主要优点在于提供了一个网络分段系统，比传统网络具有更高的灵活性。使用 VLAN 的优点如下：
- 灵活创建虚拟工作组，使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。

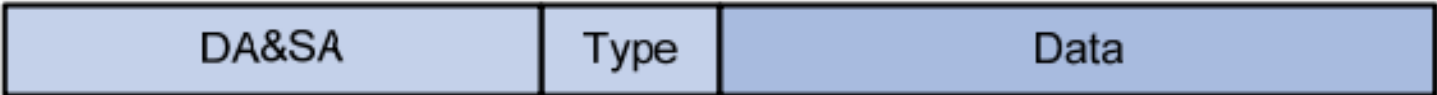
- 控制广播域的范围，局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强了 LAN 的安全性，由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。

VLAN之间的通信

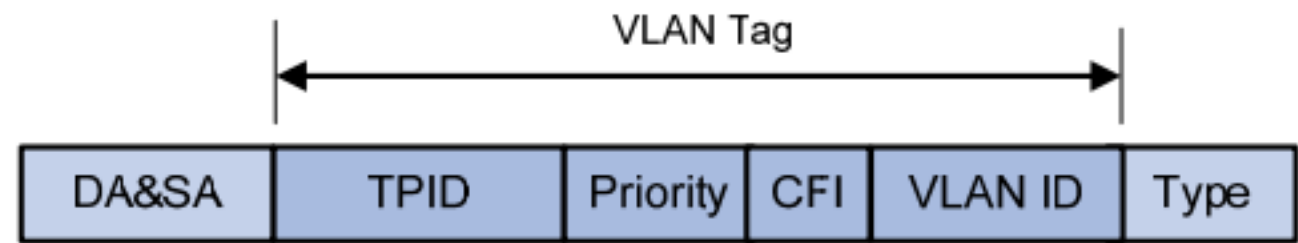
如果连接到一个 VLAN 中的设备要和另一个 VLAN 中的设备进行通信，需要安装连接双方 VLAN 的路由器或者第三层交换设备。只有当两边 VLAN 同时连接到路由器或者第三层交换设备后才能通信。

802.1Q VLAN

IEEE 802.1Q 协议，即 Virtual Bridged Local Area Networks 协议，主要规定 VLAN 的实现。802.1Q 协议为标识带有 VLAN 成员信息的以太网帧建立一种标准的方法。802.1Q VLAN 在报文中添加标识 VLAN 的字段，交换机在进行帧转发的同时判断 VLAN 是否匹配，从而确定其互通性。由于普通交换机工作在 OSI 模型的数据链路层，只能对报文的数据链路层封装进行识别。因此，如果添加识别字段，也需要添加到数据链路层封装中。传统的以太网数据帧在目的 MAC 地址和源 MAC 地址之后封装的是上层协议的类型字段，如下图所示。



其中 DA 表示目的 MAC 地址，SA 表示源 MAC 地址，Type 表示报文所属协议类型。IEEE 802.1Q 协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。



VLAN Tag 包含以下四个字段：分别是 TPID(Tag Protocol Identifier, 标签协议标识符)、Priority、CFI (Canonical Format Indicator, 标准格式指示位) 和 VLAN ID。

- TPID: 标签协议标识符，Tag Protocol Identifie 的简称。用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。由于 TPID 字段在以太网报文中所处位置与不带 VLAN Tag 的报文中协议类型所处位置相同，为避免网络中转发和接收造成混乱，设备将不允许 TPID 配置为常用协议类型值。

常用以太网帧协议类型值协议类型对应取值如表 5-1 常用以太网帧协议类型值协议类型对应取值所示。

表 5-1 常用以太网帧协议类型值协议类型对应取值

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

- Priority: 定义用户优先级，包括 8（0~7）个优先级别。IEEE 802.1P 为 3bit 的用户优先级

位定义了操作，0 的优先级最低，7 的优先级最高。

- CFI：标识 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1bit。取值为 0 时，表示 MAC 地址以标准格式进行封装；取值为 1 时，表示以非标准格式封装。缺省取值为 0。
- VLAN ID：简称 VID，对 VLAN 的识别字段，长度为 12 位。支持 4096VLAN 的识别取值范围为 0~4095。在 4096 可能的 VID 中，VID=0 用于识别帧优先级，4095（FFF）作为预留给值，所以 VLAN ID 的取值一般使用 1~4094。网络设备利用 VID 来识别报文所属的 VLAN，根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 值，来对报文进行处理。

### 5.7.1. 使能802.1Q VLAN

要使所划分的 VLAN 组生效，您必须使能 802.1Q VLAN 功能。

**步骤1** 执行“swmode vlan enable”，使能 VLAN。

📖 说明：vlan 的状态有 enable 和 disable 两种，缺省状态为 disable。

```
SWITCH# swmode vlan enable
```

**步骤2** 执行“show swmode vlan”，查看 VLAN 的使能状态。

```
SWITCH# show swmode vlan
802.1q VLAN: enable
SWITCH#
```

——结束

### 5.7.2. 设置TPID

TPID 标签协议标识符，Tag Protocol Identifie 的简称。用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。

**步骤1** 执行“tpid 8010”，修改 tpid 的值。

📖 说明：tpid 的取值范围为 0x0001~0xffff，缺省值为 0x8100。命令中“8010”可根据实际情况修改所需的值。

```
SWITCH# tpid 8100
```

**步骤2** 执行“show tpid”，查看所设置的 tpid。

```
SWITCH# show tpid
TPID : 0x8100
SWITCH#
```

——结束

### 5.7.3. 创建802.1Q VLAN组

根据功能、部门及应用等因素可以创建不同的 VLAN 组，实现同一 VLAN 组内的主机可以互相通信，VLAN 组之间主机通信必须通过路由器或三层交换机设备。

如创建一个 VID 为 2 的 VLAN 组，该 VLAN 组的成员端口为 FE1 和 FE2，FE1 和 FE2 的“模式”为“tagged”或“untagged”。操作步骤如下：

**步骤1** 执行“vlan 2”，创建 VID 为 2 的 VLAN 组。

📖 说明：VID 的取值范围为 1~4094。

```
SWITCH# vlan 2
SWITCH<vlan2>#
```

**步骤2** 执行“ethernet fe1 to fe2 untagged”，设置 FE1 和 FE2 为不带 VLAN 标识的成员。

📖 说明：“tagged”表示端口发送数据携带 VLAN 标识，“untagged”表示端口发送数据不携带 VLAN 标识。执行“undo ethernet fe1”可删除 VLAN 2 的成员端口 FE1。

```
SWITCH<vlan2># ethernet fe1 to fe2 untagged
```

步骤3 执行“show vlan 2”，可查看到所创建的 VLAN 2 信息。

```
SWITCH<vlan2># show vlan 2
Management VLAN: 1

vlan-2<members>:
 FE-1 ----- untagged
 FE-2 ----- untagged

SWITCH<vlan2>#
```

步骤4 执行“quit”，退出 VLAN 2 设置。  
——结束

### 5.7.4. 设置端口的VLAN属性

当交换机端口接收到的报文不带有 VLAN Tag 时，交换机会自动为该报文分配一个 VID，这个 VID 就是端口缺省的 VLAN ID，简称 PVID。每个端口只能有一个端口 VLAN ID（PVID）。当不带标签的以太网数据包到达端口时，它将被打上 PVID VID 标签。您可以设置该 VLAN 成员端口的 PVID 和端口接收的帧类型。

如在 [5.7.3 创建 802.1Q VLAN 组](#) 中已创建“VID”为“2”的 VLAN 组，设置 FE1 和 FE2 的 PVID 为“2”，接收数据类型为“all”或“only-tag”。操作步骤如下：

步骤1 设置端口 FE1 的 PVID 和帧类型。

1. 执行“interface ethernet fe1”，进入端口 FE1 的设置。
2. 执行“switchport pvid 2”，设置 FE1 的 PVID 为 2。

 说明：PVID 的取值范围为 1~4094。

```
SWITCH<fe1># switchport pvid 2
```

3. （可选）执行“switchport admit-frame only-tag”，设置 FE1 只接收带 VLAN 标识的数据。

 说明：only-tag 表示端口只接收携带 VLAN 标识的数据，all 表示端口接收所有的数据。缺省值为 all。

```
SWITCH<fe1># switchport admit-frame only-tag
```

4. 执行“quit”，退出 FE1 设置。

步骤2 设置端口 FE2 的 PVID 和帧类型。

1. 执行“interface ethernet fe2”，进入端口 FE2 的设置。
2. 执行“switchport pvid 2”，设置 FE1 的 PVID 为 2。

 说明：PVID 的取值范围为 1~4094。

```
SWITCH<fe2># switchport pvid 2
```

3. （可选）执行“switchport admit-frame only-tag”，设置 FE2 只接收带 VLAN 标识的数据。

 说明：only-tag 表示端口只接收携带 VLAN 标识的数据，all 表示端口接收所有的数据。缺省值为 all。

```
SWITCH<fe2># switchport admit-frame only-tag
```

4. 执行“quit”，退出 FE2 设置。

步骤3 执行“show vlan all”，可查看已设置的 PVID。

```
SWITCH# show vlan all
Management VLAN: 1
```

| PORT | QinQ    | PVID | Admit-frame |
|------|---------|------|-------------|
| FE-1 | disable | 2    | Only_Tag    |
| FE-2 | disable | 2    | Only_Tag    |
| FE-3 | disable | 1    | All         |
| FE-4 | disable | 1    | All         |
| FE-5 | disable | 1    | All         |
| FE-6 | disable | 1    | All         |
| FE-7 | disable | 1    | All         |
| FE-8 | disable | 1    | All         |
| GE-1 | disable | 1    | All         |
| GE-2 | disable | 1    | All         |

——结束

### 5.7.5. 使能QinQ

QinQ 技术（也称 StaCKed VLAN 或 Double VLAN），实现将用户私网 VLAN Tag 封装在公网 VLAN Tag 中，时报文带着两层 VLAN Tag 穿越运营商的骨干网络（公网）。不同用户网络的报文在公网传输时被完全分开，即时两个用户网络的 VLAN 范围存在重叠，在公网传输时也不会产生混淆。基于端口的 QinQ 实现当该端口接收到报文，无论报文是否带有 VLAN Tag，交换机都会为该报文打上本端口缺省 VLAN 的 VLAN Tag。这样，如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是 untagged 的报文，该报文就成为带有端口缺省 VLAN Tag 的报文。您可以根据实际情况使能 QinQ 功能。

如使能端口 FE1 的 QinQ 功能。操作步骤如下：

步骤1 执行“interface ethernet fe1”，进入端口 FE1 的设置。

步骤2 执行“qinq enable”，使能端口 FE1 的 QinQ 功能。

步骤3 执行“quit”，退出 FE1 设置。

步骤4 执行“show vlan all”，可查看端口的 QinQ 状态。

```
SWITCH# show vlan all
Management VLAN: 1
```

| PORT | QinQ    | PVID | Admit-frame |
|------|---------|------|-------------|
| FE-1 | enable  | 2    | Only_Tag    |
| FE-2 | disable | 2    | Only_Tag    |
| FE-3 | disable | 1    | All         |
| FE-4 | disable | 1    | All         |
| FE-5 | disable | 1    | All         |
| FE-6 | disable | 1    | All         |
| GE-1 | disable | 1    | All         |
| GE-2 | disable | 1    | All         |

——结束

## 5.8 设置服务质量

QoS（Quality of Service，服务质量）是用来描述网络的服务质量和数据优先权的，可以解决网络延迟和阻塞等问题。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

### 5.8.1. QoS

QoS 是网络与用户之间以及网络上互相通信的用户之间关于信息传输与共享的质的约定，例如，传输延迟允许时间、最小传输画面失真度以及声像同步等，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。在互联网早期，各种数据都是平等的，网络带宽属于先来先得的自由抢占资源。随着互联网上数据类型的增加，对数据优先级需求也开始提出，比如对音频数据的实时性就要比视频数据高；而且付费用户希望自己的数据的发送优先权要高于免费用户。这些需求，促使了 QoS 的进一步研究和发展。

本设备提供了 QoS 优先级设置，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，减少对诸如语音或视频等对时间敏感业务的延迟。

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发送队列，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。

本设备提供以下两种调度机制：

- 严格优先级：该方式优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。
- 加权轮询（8:4:2:1）：该方式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，：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。

### 5.8.2. 设置QoS优先级协议

本设备为 QoS 优先级提供了 802.1P、Port\_prio 和 DSCP 三种协议。在 QoS 全局中，您可以设置交换机 QoS 优先级所遵循的协议。

**步骤1** 执行“qos priority-trust cos”，设置 QoS 优先级所遵循的协议为 802.1P。

 **说明：**cos 表示 QoS 优先级遵循的协议为 802.1P，dscp 表示 QoS 优先级遵循的协议 DSCP，Port\_prio 协议对应的执行命令为“undo qos priority-trust”。QoS 优先级遵循的协议缺省值为 cos。

```
SWITCH# qos priority-trust cos
```

**步骤2** 执行“show qos priority-trust”，可查看到 QoS 优先级所遵循的协议。

```
SWITCH# show qos priority-trust
QoS Priority Trust Mode: 802.1p<COS>
```

——结束

### 5.8.3. 设置QoS端口优先级

本设备为每个端口提供 8 个优先级，即 0~7。其中，0 优先级最低，7 优先级最高。在使用“Port\_Prio”优先级协议时，您可以根据实际使用情况设置端口优先级。

如 QoS 优先级遵循 Port-prio 协议，将端口 FE1 的优先级设置为“3”。操作步骤如下：

**步骤1** 执行“undo qos priority-trust”，设置 QoS 优先级遵循 Port-prio 协议。

```
SWITCH# undo qos priority-trust
```

**步骤2** 执行“interface ethernet fe1”，进入端口 FE1 的设置。

**步骤3** 执行“priority 3”，设置端口 FE1 的优先级为 3。

 **说明：**端口的优先级取值范围为 0~7。其中，0 优先级最低，7 优先级。缺省值为 0。

```
SWITCH# interface ethernet fe1
SWITCH<fe1># priority 3
```

步骤4 执行“show qos interface priority”，查看 FE1 的端口优先级。

```
SWITCH<fe1># show qos interface priority
PORT PORT-BASED-PRIORITY

FE-1 3
FE-2 0
FE-3 0
FE-4 0
FE-5 0
FE-6 0
GE-1 0
GE-2 0
```

步骤5 执行“quit”，退出 FE1 设置。  
——结束

### 5.8.4. 设置调度机制

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。本设备提供严格优先级和加权轮询（8:4:2:1）两种调度机制。您可以根据实际情况进行设置所需的调度机制。

步骤1 执行“qos queue-scheduler sp”，设置调度机制为严格优先级。  
说明：sp 表示调度机制为严格优先级，wrr 表示调度机制为加权轮询（8:4:2:1）。

```
SWITCH# qos queue-scheduler sp
```

步骤2 执行“show qos queue-scheduler”，查看调度机制。

```
SWITCH# show qos queue-scheduler
Queue scheduling mode: SP
```

——结束

### 5.8.5. 设置发送队列

当缺省的 802.1p 优先级和本地优先级的映射关系不能满足需求时，您可以修改 802.1p 优先级到本地优先级的映射关系，从而实现 802.1p 优先级和发送队列之间映射关系的改变，将不同优先级的报文放入相应的发送队列进行调度。

如将优先级 0 所对应的队列由 0 修改为 1。操作步骤如下：

步骤1 执行“qos cos-local-precedence-map 1 0 1 1 2 2 3 3”，修改优先级 0 所对应的发送队列为 1。

说明：命令中的 1 0 1 1 2 2 3 3 依次是优先级 0~7 所对应的发送队列。

```
SWITCH# qos cos-local-precedence-map 1 0 1 1 2 2 3 3
```

本设备缺省的 802.1P 优先级与发送队列的映射关系如表 5-2 802.1p 优先级与发送队列缺省对应关系所示。

表 5-2 802.1p 优先级与发送队列缺省对应关系

| 802.1p 优先级 | 发送队列 |
|------------|------|
| 0          | 0    |
| 1          | 0    |
| 2          | 1    |
| 3          | 1    |
| 4          | 2    |
| 5          | 2    |
| 6          | 3    |
| 7          | 3    |

步骤2 执行“show qos cos-local-precedence-map”，查看优先级 0~7 对应的发送队列。

```
SWITCH# show qos cos-local-precedence-map
cos-local-precedence-map:
cos(802.1p) :0 1 2 3 4 5 6 7
queue :1 0 1 1 2 2 3 3

SWITCH#
```

——结束

### 5.8.6. 设置DSCP队列映射

DSCP 在每个数据包 IP 头部的服务类别 TOS 标识字节中，利用已使用的 6 比特和未使用的 2 比特字节，通过编码值来区分优先级。DSCP 的取值范围为 0~63。您可以根据实际情况设置 DSCP 各个值所属的队列。

如将优先级 0 所对应的队列由 0 修改为 1。操作步骤如下：

步骤1 执行“qos dscp-local-precedence-map 0:1”，修改优先级 0 所对应的发送队列为 1。

说明：命令中的 0 为优先级，1 为优先级所对应的发送队列。

```
SWITCH# qos dscp-local-precedence-map 0:1
```

本设备缺省的 DSCP 优先级与发送队列的映射关系如表 5-3 dscp 优先级与发送队列缺省对应关系所示。

表 5-3 dscp 优先级与发送队列缺省对应关系

| dscp 优先级 | 发送队列 |
|----------|------|
| 0~15     | 0    |
| 16~31    | 1    |
| 32~47    | 2    |
| 48~63    | 3    |

步骤2 执行“show qos dscp-local-precedence-map”，查看 DSCP 优先级对应的发送队列。

```
SWITCH# show qos dscp-local-precedence-map
dscp-local-precedence-map:
DSCP : 0 1 2 3 4 5 6 7
queue : 1 0 0 0 0 0 0 0
DSCP : 8 9 10 11 12 13 14 15
queue : 0 0 0 0 0 0 0 0
DSCP :16 17 18 19 20 21 22 23
queue : 1 1 1 1 1 1 1 1
DSCP :24 25 26 27 28 29 30 31
queue : 1 1 1 1 1 1 1 1
DSCP :32 33 34 35 36 37 38 39
queue : 2 2 2 2 2 2 2 2
DSCP :40 41 42 43 44 45 46 47
queue : 2 2 2 2 2 2 2 2
DSCP :48 49 50 51 52 53 54 55
queue : 3 3 3 3 3 3 3 3
DSCP :56 57 58 59 60 61 62 63
queue : 3 3 3 3 3 3 3 3
```

——结束

### 5.8.7. 设置CoS重映射

CoS 重映射是指各端口接收到携带有 802.1P 标识的数据包时根据本设备内部 CoS 值进行一一对应，重新赋一个 802.1P 值，将旧的 802.1P 标识信息丢失，按照映射后的 CoS 值分配到所属队列中进行发送。

如将端口 FE1 的优先级 0 所对应的 CoS 重映射为 1。操作步骤如下：

步骤1 执行“interface ethernet fe1”，进入端口 FE1 的设置。

步骤2 执行“cos remap-priority 0 1”，将端口 FE1 的优先级 0 对应 CoS 重映射改为 1。

```
SWITCH# interface ethernet fe1
SWITCH<fe1># cos remap-priority 0 1
SWITCH<fe1>#
```

本设备缺省的优先级与发送队列的映射关系如表 5-2 802.1p 优先级与发送队列缺省对应关系所示。

表 5-4 优先级与 cos 重映射的缺省关系

| 优先级 | cos 重映射 |
|-----|---------|
| 0   | 0       |
| 1   | 1       |
| 2   | 2       |
| 3   | 3       |
| 4   | 4       |
| 5   | 5       |
| 6   | 6       |
| 7   | 7       |

步骤3 执行“quit”，退出 FE1 设置。

步骤4 执行“show qos cos-port-remap”，可查看 CoS 重映射的值。

```
SWITCH<fe1># quit
SWITCH# show qos cos-port-remap
cos-local-precedence-remap:
default cos:0 1 2 3 4 5 6 7
Port No. :----- new cos -----
FE-1 :1 1 2 3 4 5 6 7
FE-2 :0 1 2 3 4 5 6 7
FE-3 :0 1 2 3 4 5 6 7
FE-4 :0 1 2 3 4 5 6 7
FE-5 :0 1 2 3 4 5 6 7
FE-6 :0 1 2 3 4 5 6 7
GE-1 :0 1 2 3 4 5 6 7
GE-2 :0 1 2 3 4 5 6 7

SWITCH#
```

——结束

## 5.9 管理转发地址

以太网交换机在转发数据前必须知道它的每一个端口所连接的主机的 MAC 地址，构建出一个 MAC 地址表。当交换机从某个端口收到数据帧后，读取数据帧中封装的目的地 MAC 地址信息，然后查阅事先构建的 MAC 地址表，找出和目的地地址相对应的端口，从该端口把数据转发出去，其他端口则不受影响，这样避免了与其它端口上的数据发生碰撞。因此构建 MAC 地址表是交换机的首要工作。本设备提供配置静态单播地址、静态多播地址和 IGMP Snooping 的功能。

### 5.9.1. 设置老化时间

老化时间是一个影响交换机学习进程的参数。从一个地址记录加入地址表以后开始计时，如果

在老化时间内各端口未收到源地址为该 MAC 地址的帧，那么，这些地址将从动态转发地址表中被删除。静态 MAC 地址表不受地址老化时间影响。

本设备老化时间的取值范围从 1~255（\*15）秒，缺省值为 20。老化时间过长，会导致交换机内的 mac 地址表超期，从而使交换机做出一些不正确的过滤/转发决定。老化时间过短，会造成地址表刷新太快，大量接收到的数据包的目的地址在 mac 地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这样大大地削弱了交换机的优点。

如将老化时间设置为 60 秒，则应该在交换机上设置老化时间的值为“4”。操作步骤如下：

**步骤1** 执行“mac-address-table timer aging 4”，将老化时间的值设置为 4。

 **说明：**老化时间取值范围为 1~255，老化时间的取值\*15s=实际的老化时间。如 4\*15s=60s，则实际老化时间为 60s。执行“mac-address-table timer no-aging”可以禁用老化时间，MAC 地址表不进行老化。

```
SWITCH# mac-address-table timer aging 4
SWITCH#
```

**步骤2** 执行“show mac-address-table aging-time”，可以查看老化时间。

```
SWITCH# show mac-address-table aging-time
MAC-ADDRESS-TABLE Aging-Timeout: 60 second(s)
SWITCH#
```

——结束

### 5.9.2. 设置单播MAC地址

单播是主机之间“一对一”的通讯模式，当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文从该表项中的转发出端口发送。单播 MAC 地址提供配置目的 MAC 地址与端口一一对应的功能，手动配置静态 MAC 地址表。配置某一端口与某一 MAC 地址对应后，目的地址为该 MAC 地址的报文只能从所对应的端口转发，而不进行广播。若使所配置的单播 MAC 地址表生效，您需是使能 VLAN，使能 VLAN 的具体步骤请参见“[5.7.1](#)

使能 802.1Q VLAN”。

如设置属于 VLAN 1 的端口 FE1 的单播地址为 00-00-00-00-00-01，操作步骤如下：

**步骤1** 执行“mac-address-table add 00-00-00-00-00-01 vlan 1 ethernet fe1”，将 VLAN 1 的端口 FE1 设置与 00-00-00-00-00-01 一一对应。

 **说明：**MAC 地址的输入格式为 xx-xx-xx-xx-xx-xx。设置的单播地址为静态 MAC 地址，不受老化时间影响。

```
SWITCH# mac-address-table add 00-00-00-00-00-01 vlan 1 ethernet fe1
SWITCH#
```

**步骤2** 执行“show mac-address-table l2-address”，可以查看 MAC 地址表。

```
SWITCH# show mac-address-table l2-address
```

| mac-address       | port | type    | vid |
|-------------------|------|---------|-----|
| 00-00-00-00-00-01 | FE-1 | static  | 1   |
| 00-71-c2-0b-a9-4f | FE-4 | dynamic | 1   |
| 00-a1-d3-81-14-65 | CPU  | static  | 1   |
| 00-a1-d3-88-13-61 | FE-4 | dynamic | 1   |
| 00-e0-4c-71-fc-0b | FE-4 | dynamic | 1   |
| 28-92-4a-1d-36-1f | FE-4 | dynamic | 1   |
| 34-40-b5-8f-3c-3e | FE-4 | dynamic | 1   |
| 38-59-f9-dc-48-9f | FE-4 | dynamic | 1   |
| 6c-59-40-4f-25-a5 | FE-4 | dynamic | 1   |
| 78-f2-9e-fa-5f-da | FE-4 | dynamic | 1   |
| 84-74-2a-5d-f3-e1 | FE-4 | dynamic | 1   |
| b8-ae-ed-2e-85-5d | FE-4 | dynamic | 1   |
| b8-f8-83-87-ad-81 | FE-4 | dynamic | 1   |
| d0-27-88-b4-17-f8 | FE-4 | dynamic | 1   |
| e4-d3-32-7e-c3-18 | FE-4 | dynamic | 1   |
| ec-a8-6b-d0-97-7d | FE-4 | dynamic | 1   |
| ff-ff-ff-ff-ff-ff | 7ff  | static  | 1   |

Total mac-address number: 17

步骤3（可选）执行“mac-address-table del 00-00-00-00-00-01 vlan 1”，可删除 00-00-00-00-00-01 对应的单播地址信息。  
——结束

### 5.9.3. 设置多播MAC地址

多播是主机之间“一对多”的通讯模式，也就是目的 MAC 地址不是一个具体的接收者，而是一个成员不确定的组。若使所配置的多播 MAC 地址表生效，您需是使能 VLAN，使能 VLAN 的具体步骤请参见“5.7.1

使能 802.1Q VLAN”。  
如将多播地址 01-00-5e-00-00-01 的成员端口设置为属于 VLAN 1 的端口 FE1、FE2、FE3，操作步骤如下：

步骤1 执行“mac-address-table add 01-00-5e-00-00-01 vlan 1 ethernet fe1”，将 VLAN 1 的端口 FE1 设置为 01-00-5e-00-00-01 的多播组成员。

说明：MAC 地址的输入格式为 xx-xx-xx-xx-xx-xx。设置的多播地址为静态 MAC 地址，不受老化时间影响。

```
SWITCH# mac-address-table add 01-00-5e-00-00-01 vlan 1 ethernet fe1
SWITCH#
```

步骤2 执行“mac-address-table add 01-00-5e-00-00-01 vlan 1 ethernet fe2”，将 VLAN 1 的端口 FE2 设置为 01-00-5e-00-00-01 的多播组成员。

步骤3 执行“mac-address-table add 01-00-5e-00-00-01 vlan 1 ethernet fe3”，将 VLAN 1 的端口 FE3 设置为 01-00-5e-00-00-01 的多播组成员。

步骤4 执行“show mac-address-table l2-address”，可以查看 MAC 地址表。

说明：MAC 地址表中，当一个 MAC 地址对应多个端口时采用十六进制表示。

```
SWITCH# show mac-address-table l2-address
```

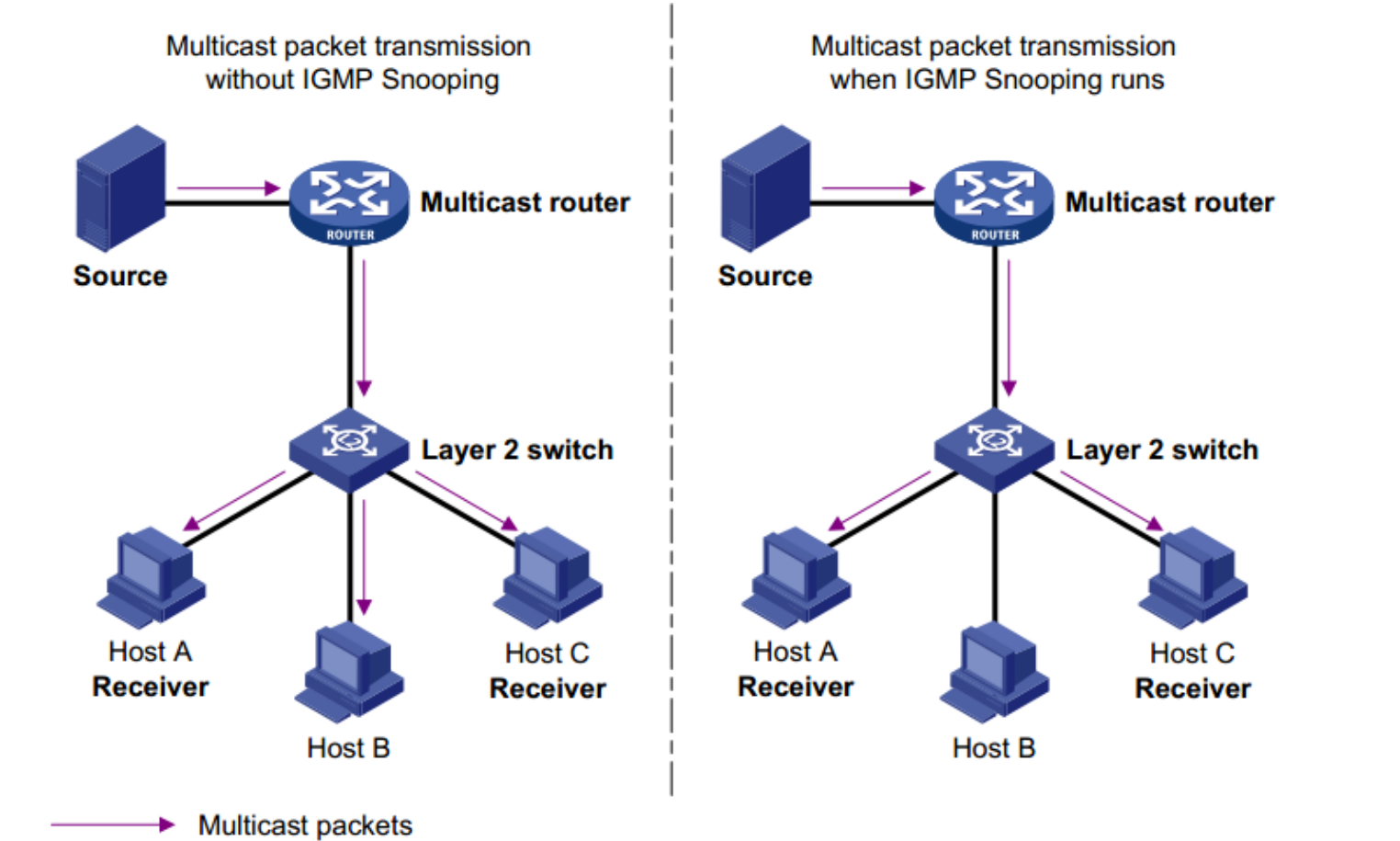
| mac-address       | port | type    | vid |
|-------------------|------|---------|-----|
| 00-00-00-00-00-01 | FE-1 | static  | 1   |
| 00-71-c2-0b-a9-4f | FE-4 | dynamic | 1   |
| 00-a1-d3-81-14-65 | CPU  | static  | 1   |
| 00-a1-d3-88-13-61 | FE-4 | dynamic | 1   |
| 00-e0-4c-71-fc-0b | FE-4 | dynamic | 1   |
| 01-00-5e-00-00-01 | FE-1 | static  | 1   |
| 1c-1b-0d-f8-ff-e3 | FE-4 | dynamic | 1   |
| 28-92-4a-1d-36-1f | FE-4 | dynamic | 1   |
| 34-40-b5-8f-3c-3e | FE-4 | dynamic | 1   |
| 38-59-f9-dc-48-9f | FE-4 | dynamic | 1   |
| 6c-59-40-4f-25-a5 | FE-4 | dynamic | 1   |
| 78-f2-9e-fa-5f-da | FE-4 | dynamic | 1   |
| b8-f8-83-87-ad-81 | FE-4 | dynamic | 1   |
| d0-27-88-b4-17-f8 | FE-4 | dynamic | 1   |
| e4-d3-32-7e-c3-18 | FE-4 | dynamic | 1   |
| ec-a8-6b-d0-97-7d | FE-4 | dynamic | 1   |
| ff-ff-ff-ff-ff-ff | 7ff  | static  | 1   |

Total mac-address number: 17  
SWITCH#

步骤5（可选）执行“mac-address-table del 01-00-5e-00-00-01 vlan 1”，可删除01-00-5e-00-00-01对应的多播地址信息。  
——结束

### 5.9.4. 设置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。运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。如下图所示，当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。



IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

- 减少了二层网络中的广播报文，节约了网络带宽。
- 增强了组播信息的安全性。
- 为实现对每台主机的单独计费带来了方便。

如 FE1、FE2、FE3 属于 VLAN 2，将 VLAN 2 加入到 ICMP Snooping 多播 VLAN 中，设置 FE3 为路由端口，使能 IGMP Snooping 功能并设置组播的参数。操作步骤如下：

步骤1 执行“igmp-snooping enable”，IGMPSnooping 功能。

📖 说明：IGMP Snooping 缺省状态为 disable。

```
SWITCH# igmp-snooping enable
SWITCH#
```

步骤2 执行“igmp-snooping multicast-vlan add 2”，把 VLAN 2 加入到 IGMP Snooping 多播 VLAN。

```
SWITCH# igmp-snooping multicast-vlan add 2
SWITCH#
```

步骤3 执行“igmp-snooping route-port add fe3 multicast-vlan 2”，创建静态路由端口为 FE3。

```
SWITCH# igmp-snooping route-port add fe3 multicast-vlan 2
```

步骤4 设置组播侦听参数。

表 5-5 组播侦听参数

| 值        | 值域                                      | 描述                                                                                                            |
|----------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------|
| 最大请求时间   | 取值范围：<br>1~25<br>缺省值：10                 | 设置主机收到 IGMP 查询报文后的最大响应时间。<br>超时后，交换机将该端口从组播组中删除。                                                              |
| 路由端口老化时间 | 取值范围：<br>100~1000<br>缺省值：1000           | 设置路由端口从 IGMP Snooping 路由端口列表中删除的时间。<br>路由端口老化时间指交换机为每个路由端口都启动一个定时器，超过该时间则将路由端口从 IGMP Snooping 路由端口列表中删除。      |
| 主机端口老化时间 | 取值范围：<br>200~1000<br>缺省值：200            | 设置组播组成员端口从 IGMP Snooping 转发表中删除的时间。<br>主机端口老化时间指当一个端口加入某组播组时，交换机为该端口启动一个定时器，超过该时间则将该端口从 IGMP Snooping 转发表中删除。 |
| IGMP 查询器 | Enable,<br>Disabled<br>缺省值：<br>Disabled | 启用或禁用 IGMP 查询器。<br>IGMP 查询器定期向本地网段内的所有主机与路由器发送 IGMP 通用查询报文，已查询该网段有哪些组播组的成员。                                   |
| 间隔时间     | 取值范围：<br>1~300<br>缺省值：100               | 设置 IGMP 查询器发送 IGMP 通用查询报文的时间间隔。                                                                               |

1. 执行“igmp-snooping query-proxy response-time 15”，设置最大请求时间为 15s。
  2. 执行“igmp-snooping route-port-aging-time 500”，设置路由端口老化时间为 500s。
  3. 执行“igmp-snooping member-port-aging-time 250”，设置主机端口老化时间为 250s。
  4. 执行“igmp-snooping query-proxy enable”，启用 IGMP 查询器。
- 📖 说明：IGMP 查询器缺省状态为 disable。
5. 执行“igmp-snooping query-proxy interval-time 50”，设置 IGMP 查询报文的间隔时间为 50s。

```
SWITCH# igmp-snooping query-proxy interval-time 50
SWITCH#
```

步骤5 执行“show igmp-snooping config”，查看 IGMP 的组播监听参数配置。

```
SWITCH# show igmp-snooping config
IGMP-Snooping State : enable
IGMP-Snooping Router-Port-Aging-Time: 500 seconds
IGMP-Snooping Member-Port-Aging-Time: 250 seconds
IGMP Query Proxy Mode : enable
IGMP Query Proxy Inteval Time : 50 seconds
IGMP Query Proxy Response Time : 15 seconds

Multicast Ulan List:
 vlan-2
```

——结束

### 5.10 管理风暴抑制

当网络中有大量的广播/组播/单播流量通过以太网端口时，会在端口上产生流量风暴，可能导致网络的拥塞。在端口上配置了广播/组播/单播风暴抑制功能后，当端口上的广播/组播/单播流量超过所设置的抑制阈值时，系统会丢弃超出流量限制的报文，从而使端口的广播/组播/单播流量降低到限定范围内，保证网络业务的正常运行。您可以通过配置风暴控制，限制交换机上允许通过的广播/组播/单播流量的大小。

如在端口 FE1 设置抑制广播帧的入口速率为 10M。操作步骤如下：

步骤1 执行“storm-control limite-mode 4 rate 10000 ethernet fe1”，设置在端口 FE1 抑制广播帧的入口速率为 10M。

说明：limite-mode 有四种类型：1 代表 All frame，抑制所有流量类型；2 代表 Broadcast&Multicast&Flooded-unicast，抑制广播&多播&单播流量类型；3 代表 Broadcast&Multicast，抑制广播&多播流量类型；4 代表 Broadcast，抑制广播流量类型。百兆端口取值范围：62~100000kbps，千兆端口取值范围：62~250000kbps，交换机会自动将所设置的值转换为与之最接近的速率。由于交换机芯片内部的出口速率算法限制，千兆端口的出口速率最大取值为 250000kbps。

```
SWITCH# storm-control limite-mode 4 rate 10000 ethernet fe1
Limit and count Broadcast. Setting 10000kbps on FE-1.
SWITCH#
```

步骤2 执行“show storm-control”，查看风暴抑制的信息。

```
SWITCH# show storm-control
Storm-Control:
 PORT STATUS TYPE RATE
 FE-1 enable 4 10000kbps
 FE-2 disable
 FE-3 disable
 FE-4 disable
 FE-5 disable
 FE-6 disable
 GE-1 disable
 GE-2 disable

note:
1---All ingress frames;
2---Broadcast&Multicast&flooded-unicast ingress frames;
3---Broadcast&Multicast ingress frames;
4---Broadcast ingress frames;
SWITCH#
```

——结束

### 5.11 查看数据统计

为了能够直观的了解各端口的收发数据情况和交换机转发 MAC 地址表，本设备提供查看端口

数据和 MAC 地址表功能。

### 5.11.1. 查看端口数据

端口数据显示每个端口的显示每个以太网端口的发送好报文数、发送坏报文数、接受好报文数、接受坏报文数和发送 FCS 错误报文数帧数等参数。当需要了解端口的数据时，您可以执行命令“show ethernet statistics”查看通过端口的各种数据。

```
SWITCH# show ethernet statistics
FE-1
 In Good Octets : 0
 In Bad Octets : 0
 In Broadcasts Frames : 0
 In Multicasts Frames : 0
 In Unicasts Frames : 0
 In Pause Frame : 0
 In MAC Received Error Frames : 0
 In FCS Error Frames : 0
 Undersize Frames : 0
 Fragments Frames : 0
 Oversize Frames : 0
 Jabber Frames : 0
 Out Octets : 0
 Out Broadcasts Frames : 0
 Out Multicasts Frames : 0
 Out Unicasts Frames : 0
 Out Pause Frames : 0
 Out FCS Error Frames : 0
 Deferred Frames : 0
 Excessive Frames : 0
 Single Collision Frames : 0
 Multiple Collision Frames : 0
 Late Frames : 0
 Collisions Frames : 0
```

### 5.11.2. 查看MAC地址表

MAC 地址表记录了交换机与其他相连的设备的 MAC 地址、端口号以及所属的 VLAN ID。在转发数据时，交换机根据报文中的目的 MAC 地址查询 MAC 地址表，快速定位出端口，从而减少广播。动态 MAC 地址为交换机端口通过 MAC 地址学习能力得来，超过老化时间将被删除；静态 MAC 地址为手工配置的 MAC 地址，不受老化时间影响。您可以执行命令“show mac-address-table l2-address”查看 MAC 地址表。

```
SWITCH# show mac-address-table l2-address
 mac-address port type vid
00-00-00-00-00-01 FE-1 static 1
00-71-c2-0b-a9-4f FE-4 dynamic 1
00-a1-d3-81-14-65 CPU static 1
00-a1-d3-88-13-61 FE-4 dynamic 1
01-00-5e-00-00-01 FE-1 static 1
1c-1b-0d-f8-ff-e3 FE-4 dynamic 1
28-92-4a-1d-36-1f FE-4 dynamic 1
34-40-b5-8f-3c-3e FE-4 dynamic 1
38-59-f9-dc-48-9f FE-4 dynamic 1
6c-59-40-4f-25-a5 FE-4 dynamic 1
78-f2-9e-fa-5f-da FE-4 dynamic 1
b8-f8-83-87-ad-81 FE-4 dynamic 1
d0-27-88-b4-17-f8 FE-4 dynamic 1
e4-d3-32-7e-c3-18 FE-4 dynamic 1
ec-a8-6b-d0-97-7d FE-4 dynamic 1
ff-ff-ff-ff-ff-ff 7ff static 1
Total mac-address number: 16
```

## 5.12 管理快速生成树

STP（Spanning Tree Protocol）是生成树协议的英文缩写。STP 协议中定义了根桥（Root Bridge）、根端口（Root Port）、指定端口（Designated Port）、路径开销（Path Cost）等概念，用于通过构造一棵自然树的方法实现将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环，同时实现链路备份和路径最优化。

STP 采用 BPDU（Bridge Protocol Data Unit，桥协议数据单元）也称为配置消息，进行网桥之间的信息交流。STP BDUP 是一种二层报文，目的 MAC 为多播地址 01-80-C2-00-00-00，所有支持 STP 协议的网桥都会接收并处理收到的 BPDU 报文。该报文的数据区里携带了用于生成树计算的所有有用信息。

### 根桥

树形的网络结构，必须要有树根，于是 STP 引入了根桥（Root Bridge）的概念。根桥在全网中只有一个，而且根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。网络收敛后，根桥会按照一定的时间间隔产生并向外发送配置 BPDU，其他的设备对该配置 BPDU 进行转发，从而保证拓扑的稳定。选举根桥的依据是网桥优先级和网桥 MAC 地址组合成的桥 ID（Bridge ID），桥 ID 最小的网桥将成为网络中的根桥。

### 根端口

所谓根端口，是指一个非根桥的设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口，根桥上没有根端口。

### 指定桥与指定端口

指定桥与指定端口的含义，如表 5-6 指定桥与指定端口所示。

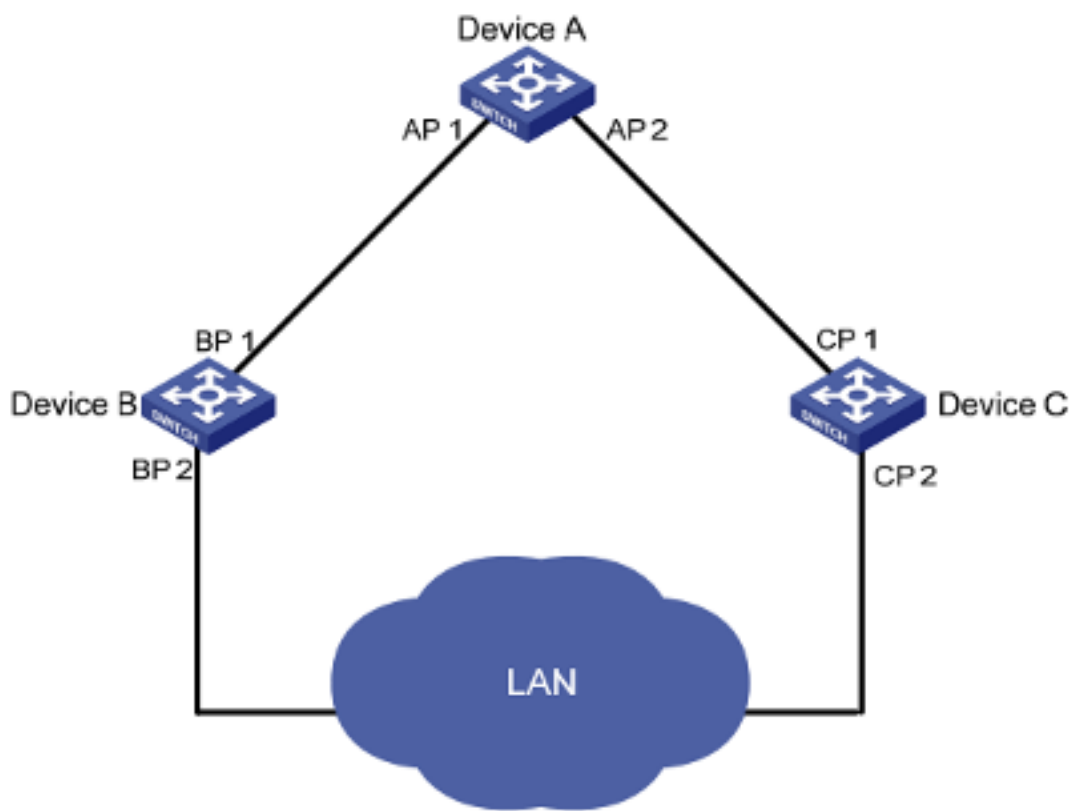
表 5-6 指定桥与指定端口

| 分类        | 指定桥                            | 指定端口                  |
|-----------|--------------------------------|-----------------------|
| 对于一台设备而言  | 与交换机直接相连并且负责向交换机转发 BPDU 报文的设备。 | 指定桥向本机转发 BPDU 报文的端口。  |
| 对于一个局域网而言 | 负责向本网段转发 BPDU 报文的设备。           | 指定桥向本网段转发 BPDU 报文的端口。 |

指定桥与指定端口如下图所示，AP1、AP2、BP1、BP2、CP1、CP2 分别表示设备 Device A、Device B、Device C 的端口。

● Device A 通过端口 AP1 向 Device B 转发配置消息，则 Device B 的指定桥就是 Device A，

指定端口就是 Device A 的端口 AP1；  
● 与局域网 LAN 相连的有两台设备：Device B 和 Device C，如果 Device B 负责向 LAN 转发配置消息，则 LAN 的指定桥就是 Device B，指定端口就是 Device B 的 BP2。



### 路径开销

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

快速生成树协议（Rapid Spanning Tree Protocol，简称 RSTP）是从 STP 发展过来的，其实现基本思想一致，但它更进一步的处理了网络临时失去连通性的问题。RSTP 规定在某些情况下，处于 BloCKing 状态的端口不必经历 2 倍的 Forward Delay 时延而可以直接进入转发状态。如网络边缘端口（即直接与终端相连的端口），可以直接进入转发状态，不需要任何时延。或者是网桥旧的根端口已经进入 BloCKing 状态，并且新的根端口所连接的对端网桥的指定端口仍处于 Forwarding 状态，那么新的根端口可以立即进入 Forwarding 状态。即使是非边缘的指定端口，也可以通过与相连的网桥进行一次握手，等待对端网桥的赞同报文而快速进入 Forwarding 状态。

步骤1 执行“rstp”，进入 RSTP 参数配置路径。

```

SWITCH# rstp
SWITCH(rstp)#
 bridge - configure bridge parameter
 disable - disable rstp
 enable - enable rstp
 ethernet - ethernet interface
 hold-count - set rstp transmit hold count
 quit - exit current mode
Global command:
 clear - Clear the screen
 exit - Exit intermediate mode
 help - Show command help
 show - help string for show
SWITCH(rstp)#

```

步骤2 执行“enable”，使能 RSTP 协议。

📖 说明：RSTP 缺省状态为 disable。

```

SWITCH(rstp)# enable

```

步骤3 执行“hold-count 6”，设置传输间隔为 6。

说明：传输间隔 (Transmit Hold Count) 用来限制 BPDU 的发送速率，每发一个 BPDU，txCount+1，Transmit Hold Count 的 txCount -1，当发送 BPDU 的 txCount= Transmit Hold Count 时，延时发送 BPDU。hold-count 的取值范围为 1~10，缺省值为 6。您可以根据实际使用情况修改。

步骤4 设置网桥的参数。

表 5-7 RSTP 桥参数

| 值      | 值域                                 | 描述                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 优先级    | 取值范围：<br>0~61440s<br>缺省值：<br>32768 | 设置网桥的优先级。RSTP 会自动将所设置的值转换为与之最接近的 4096 的倍数。设置值越小，其优先级越高。<br>网桥优先级的大小决定了这个网桥是否能够被选择为整个交换网络的根网桥，通过配置较小的优先级可以指定某个网桥作为生成树的根。如果整个交换网络中所有网桥的优先级采用相同的值，则 MAC 地址最小的网桥将被选择为根网桥。                                                                                                                                                                                                               |
| 最长老化时间 | 取值范围：<br>6~40s<br>缺省值： 20          | 设置 BPDU 的保存时间。<br>最长老化时间指网桥对 BPDU 信息保存的时间。如果超过最长老化时间，则对 BPDU 保存的信息失效，不能再用该 BPDU 计算根网桥、指定网桥和根端口等。<br>如果最大老化时间配置过小，生成树计算就会比较频繁，可能到时网络拥塞，误认为链路故障；配置过大，则可能不能及时发现链路故障，降到网络自适应能力，建议采用缺省值。                                                                                                                                                                                                 |
| 传输延迟时间 | 取值范围：<br>4~30s<br>缺省值： 15          | 设置交换机状态迁移的延迟时间。<br>链路故障会引发网络重新进行生成树的计算。生成树的结构将发生相应的变化后，重新计算得到的新配置消息无法立刻传遍整个网络。如果新选出的根端口和指定端口立刻就开始数据转发，则可能会造成暂时性的路径回环。为此，生成树协议采用了一种状态迁移的机制，根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 Forward Delay 延时后才能进入转发状态。这个延时保证了新的配置消息已经传遍整个网络。<br>交换机的 Forward Delay 特性与交换网络的网络直径有关，直径越大 Forward Delay 的时间就应该配置越长。如果 Forward Delay 配置过小，则可能会引入临时的冗余路径；如果 Forward Delay 配置过长，则可能导致网络较长时间不能恢复。建议采用缺省值。 |

- 1. 执行“bridge priority 32768”，设置网桥优先级为 32768。
- 2. 执行“bridge maxage 20”，设置最长老化时间为 20s。
- 3. 执行“bridge foward-delay 15”，设置传输延迟时间为 15s。

```
SWITCH(rstp)# bridge
foward-delay - set rstp forward delay
maxage - set rstp max age
priority - set rstp bridge priority
SWITCH(rstp)# bridge priority 32768
SWITCH(rstp)# bridge maxage 20
SWITCH(rstp)# bridge foward-delay 15
```

步骤5 （可选）设置端口的参数。

表 5-8 RSTP 端口属性参数

| 值      | 值域                                      | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 端口     | 如 FE1                                   | 需要设置参数的端口。                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| McheCK | enabled,<br>Disabled<br>缺省值:<br>Enabled | 启用或禁用端口的 McheCK 属性。<br>端口的 McheCK 属性用来检测运行在 STP 兼容模式下的端口是否可以转换到 RSTP 模式。通过设定 McheCK 可以检查与当前以太网端口相连的网段内是否还有运行 STP 协议的网桥存在。<br>如果在与当前以太网端口相连的网段内存在运行 STP 协议的网桥，RSTP 协议会将该端口的协议运行模式迁移到 STP 兼容模式。在网络比较稳定后，网段内运行 STP 协议的网桥被拆离，但 RSTP 协议仍然会运行在 STP 兼容模式下，通过设定 McheCK 变量可以迫使其迁移到 RSTP 模式下运行。<br>启用端口的 McheCK 功能之后，如果端口仍然运行在 STP 兼容模式，表示该端口所连接的网段存在 STP 网桥，否则该端口回到 RSTP 模式，表示该端口所连接的网段已经没有任何 STP 网桥。<br>Enabled: 表示启用端口的 McheCK 功能。<br>Disabled: 表示禁用端口的 McheCK 功能。 |
| 边缘端口配置 | auto,<br>non-edge,<br>edge<br>缺省值: auto | 设置端口是否可以作为边缘端口。<br>边缘端口指直接与终端用户相连的端口。边缘端口可以快速切换到转发状态，因为在边缘端口上，网络拓扑结构的变化不产生环路。通过把一个端口设置成边缘端口可以使其迅速切换到转发状态。<br>auto: 表示 RSTP 协议自动检测端口为边缘端口或非边缘端口。<br>non-edge: 表示配置端口为非边缘端口。<br>edge: 表示配置端口为边缘端口。                                                                                                                                                                                                                                                            |

|       |                                           |                                                                                                                                                                                                                                              |
|-------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 点对点配置 | auto, shared, p2p<br>缺省值: auto            | 设置端口是否与点对点链路相连。<br>端口只与一个网桥相连的链路是点对点链路，端口与多个网桥相连的链路是共享链路。链路类型对替换端口转换为根端口没有影响，指定端口快速迁移到转发状态只发生在点对点链路，除非是边缘端口。链路类型根据双工来判断，全双工为点对点链路，半双工为共享链路。<br>auto: 表示 RSTP 协议自动检测与端口相连的链路类型。<br>shared: 表示配置端口与网桥相连的链路为共享链路。<br>p2p: 表示配置端口与网桥相连的链路为点对点链路。 |
| 路径开销  | 取值范围:<br>1~20000000<br>0<br>缺省值:<br>20000 | 设置该端口的路径开销。<br>以太网端口的路径开销与该端口的链路速率有关，链路速率越大，则应将参数配置得越小，RSTP 协议可以自动检测当前以太网端口的链路速率，并换算成相应的路径开销。配置以太网端口的路径开销会引起生成树重新计算。建议使用缺省值，让 RSTP 协议自己来计算当前以太网端口的路径开销。                                                                                      |
| 优先级   | 取值范围:<br>0~240<br>缺省值: 128                | 设置端口的优先级。RSTP 会自动将所设置的值转换为与之最接近的 16 的倍数。<br>通过设定以太网端口的优先级可以指定特定的以太网端口包含在生成树内。配置的值越小，端口的优先级越高，该以太网端口就越有可能包含在生成树内。如果网桥所有的以太网端口采用相同的优先级，则以太网端口的优先级高低取决于该以太网端口的索引号。配置以太网端口的优先级会引起生成树重新计算。                                                        |

1. 执行“ethernet fe1 mcheCK”，使能端口 FE1 McheCK 功能。
2. 执行“ethernet fe1 edgecfg auto”，设置 RSTP 自动检测端口 FE1 是否为边缘端口。
3. 执行“ethernet fe1 p2pcfg auto”，设置 RSTP 自动检测与端口 FE1 相连的链路类型。
4. 执行“ethernet fe1 path-cost 20000”，设置端口 FE1 的路径开销为 20000。
5. 执行“ethernet fe1 priority 128”，设置端口 FE1 的优先级为 128。
- 步骤6 执行“show rstp”，查看 RSTP 的信息。

```
RSTP Bridge Status:
RSTP Setting :Enable
Bridge ID [PRI-MAC] :32768-00:a1:d3:88:13:68
Bridge Hello Time :2 sec
Bridge Max Age :20 sec
Bridge Forward Delay :15 sec
Transmit Hold Count :6
Root Bridge ID :32768-00:a1:d3:88:13:68
Root Path Cost :0

RSTP Port Status:
PID Mode Pri PathCost EdgeCfg OperEdge P2PCfg OperP2P State
1 RSTP 1 128 2000 Auto Non-Edge Auto Shared LinkDown
2 RSTP 0 128 1 Auto Non-Edge Auto Shared LinkDown
3 RSTP 0 128 20000 Auto Non-Edge Auto Shared LinkDown
4 RSTP 0 128 20000 Auto Non-Edge Auto Shared LinkDown
5 RSTP 0 128 20000 Auto Edge Auto P2P Forwarding
6 RSTP 0 128 20000 Auto Edge Auto P2P Forwarding
7 RSTP 0 128 20000 Auto Non-Edge Auto Shared LinkDown
8 RSTP 0 128 20000 Auto Non-Edge Auto Shared LinkDown
9 RSTP 0 128 20000 Auto Non-Edge Auto Shared LinkDown
10 RSTP 0 128 20000 Auto Non-Edge Auto Shared LinkDown
Total 10 RSTP ports dumped.
```

步骤7 执行“quit”，退出 RSTP 设置。  
——结束

### 5.13 创建讯记环网

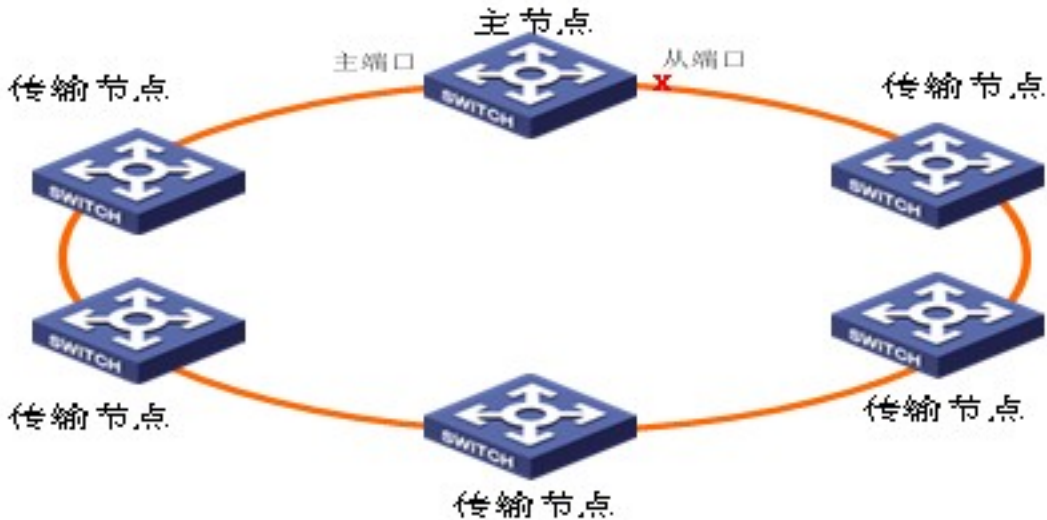
传统网络采用的是主干的方式，中间的任何一条连接线断掉，都至少会影响连接中的一个区域。这就给网络的安全性带来隐患。建立环网链路可以防止一处连接发生故障而影响整体网络。环网给数据通道提供了快速的故障恢复能力，其中最关键的就是小于 20ms 的保护倒换能力。在环中某一链路出故障时，传输交换机检测到链路故障会马上发送一个消息给主交换机，主交换机马上把被阻塞的端口解阻塞，迅速恢复数据的转发，环上的其他节点收到故障通告消息后，清空转发地址表；如果该节点有环上阻塞端口，则将该端口置为转发状态。故障恢复后，发现故障恢复的节点首先通过等待恢复时间来确认恢复，然后向环的两边通告故障恢复消息，并将与故障段相联的端口保持阻塞状态。故障恢复后，发现故障恢复的节点首先通过等待恢复时间来确认恢复，然后向环的两边通告故障恢复消息，并将与故障段相联的端口保持阻塞状态。本设备提供单环、相交环和相切环三种环网模式。

#### 主节点

主节点是环上的主要决策和控制节点。每个环上必须有一个主节点，而且只能有一个。主节点的环上端口分为主端口和从端口，环完整的情况下，通常阻断从端口。

#### 传输节点

环上除主节点之外的其它节点都可以称为传输节点（边缘节点和辅助边缘节点实际上是特殊的传输节点）。一个环上可以有多个传输节点，如下图所示：



#### 主端口和从端口

主节点和传输节点接入以太网环的两个端口中，一个为主端口，另一个为从端口，端口的角色由用户的配置决定。主节点的主端口和从端口在功能上是有区别的。主节点从其主端口发送环路状态探测报文，如果能够从从端口收到该报文，说明本节点所在环网完整，因此需要阻塞从端口以防止数据环路；相反如果在规定时间内收不到探测报文，说明环网故障，此时需要放开从端口以保证环上所有节点的正常通信。传输节点的主端口和从端口在功能上没有区别。端口的角色同样由用户的配置决定。

#### 5.13.1. 创建单环环网

介绍以太网单环环网的配置步骤。  
如下图所示， SW1、SW2、SW3、SW4 在同一网络中，SW1 为主节点，SW2、SW3、SW4 为传输节点。

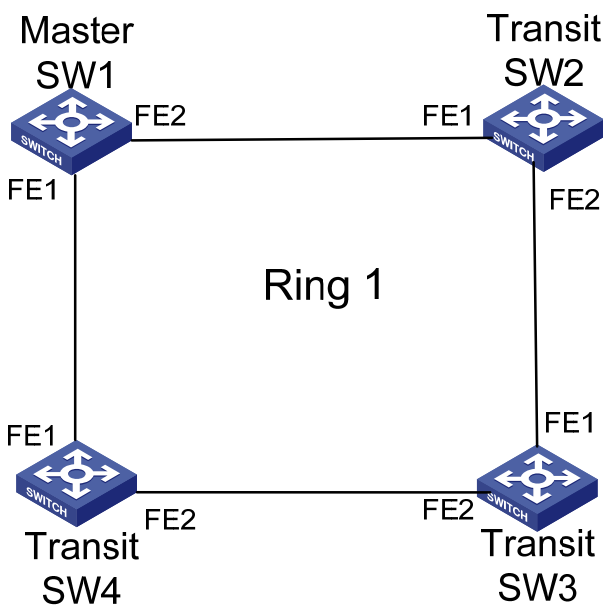


表 5-9 单环网参数规划

| 交换机 | 环网 ID | 节点模式    | 主端口 | 备用端口 |
|-----|-------|---------|-----|------|
| SW1 | 1     | Master  | FE1 | FE2  |
| SW2 | 1     | Transit | FE1 | FE2  |
| SW3 | 1     | Transit | FE1 | FE2  |
| SW4 | 1     | Transit | FE1 | FE2  |

在物理连接各设备之前，需要先配置各设备的环网参数。

步骤1 登录 SW1，设置 SW1 的环网参数。

- 1. 登录 SW1 的命令行配置页面，具体步骤请参见“2.2 通过 Telnet 远程访问”。
- 2. 执行“comark-ring enable”，使能 SW1 的环网功能。

说明：enable 代表使能环网，disable 代表禁用环网。缺省状态为 disable。

```
SWITCH# comark-ring enable
SWITCH#
```

3. 执行“comark-ring ring 1”，创建环网 1。

说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 1
SWITCH(ring-1)#
```

4. 执行“node master-node”，设置 SW1 为主节点。

```
SWITCH(ring-1)# node master-node
SWITCH(ring-1)#
```

5. 执行“primary-port fe1”，把 SW1 的端口 FE1 设置为主端口。

6. 执行“second-port fe2”，把 SW1 的端口 FE2 设置为备用端口。

```
SWITCH(ring-1)# primary-port fe1
SWITCH(ring-1)# second-port fe2
SWITCH(ring-1)#
```

7. 执行“show comark-ring”，查看环网信息。

```
SWITCH(ring-1)# show comark-ring
Ring and RSTP cannot be set at the same time:
===== Ring Status =====
Comark-Ring Setting :Enable
RingId | Node | FirstPort : State | SecondPort : State | Ring State
 1 master FE-01 :forward FE-02 : block ring-normal
SWITCH(ring-1)#
```

步骤2 登录 SW2，并设置 SW2 的环网参数。

- 1. 登录 SW2 的命令行配置页面，具体步骤请参见“2.2 通过 Telnet 远程访问”。

2. 执行“comark-ring enable”，使能 SW2 的环网功能。

说明：enable 代表使能环网，disable 代表禁用环网。缺省状态为 disable。

```
SWITCH# comark-ring enable
SWITCH#
```

3. 执行“comark-ring ring 1”，创建环网 1。

说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 1
SWITCH<ring-1>#
```

4. 执行“node transit-node”，设置 SW2 为主传输节点。

```
SWITCH<ring-1># node transit-node
SWITCH<ring-1>#
```

5. 执行“primary-port fe1”，把 SW2 的端口 FE1 设置为主端口。

6. 执行“second-port fe2”，把 SW2 的端口 FE2 设置为备用端口。

```
SWITCH<ring-1># primary-port fe1
SWITCH<ring-1># second-port fe2
SWITCH<ring-1>#
```

7. 执行“show comark-ring”，查看环网信息。

```
SWITCH<ring-1># show comark-ring
Ring and RSTP cannot be set at the same time:
===== Ring Status =====
Comark-Ring Setting :Enable
RingId | Node | FirstPort : State | SecondPort : State | Ring State
 1 | slave | FE-01 :forward| FE-02 :forward| ring-normal
SWITCH<ring-1>#
```

步骤3 参考步骤 2，设置 SW3 和 SW4 的环网参数。

——结束

配置各交换机的环网参数后，请根据环网图正确连接各交换机。

5.13.2. 创建相交环环网

介绍以太网相交环环网的配置步骤。

如下图所示， SW1、SW2、SW3、SW4、SW5、SW6 组成 Ring1，SW1 为 Ring 1 主节点，SW5 为 Ring 3 的主节点。SW2、SW3、SW4、SW5、SW6、SW7 为 Ring 2 主节点，SW5 为 Ring 3 的主节点。

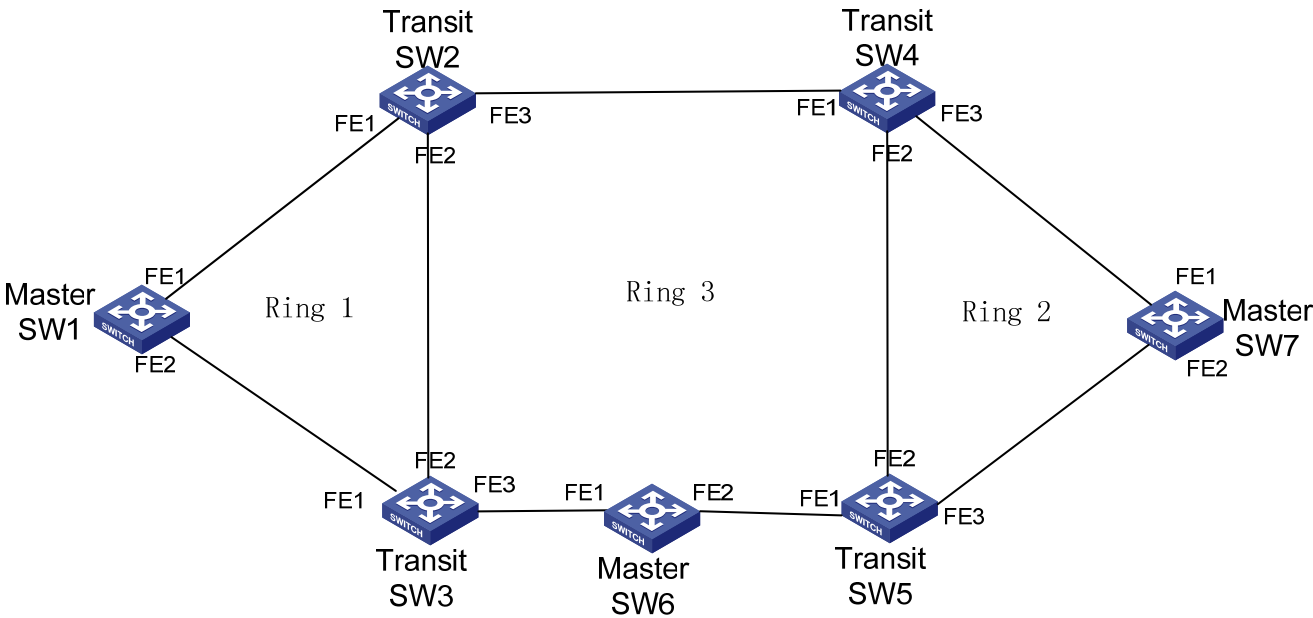


表 5-10 相交环环网参数规划

| 交换机 | 环网 ID | 节点模式    | 主端口 | 备用端口 |
|-----|-------|---------|-----|------|
| SW1 | 1     | Master  | FE1 | FE2  |
| SW2 | 1     | Transit | FE1 | FE2  |
|     | 3     | Transit | FE3 | FE2  |
| SW3 | 1     | Transit | FE1 | FE2  |
|     | 3     | Transit | FE3 | FE2  |
| SW4 | 2     | Transit | FE3 | FE2  |
|     | 3     | Transit | FE1 | FE2  |
| SW5 | 2     | Transit | FE3 | FE2  |
|     | 3     | Transit | FE1 | FE2  |
| SW6 | 3     | Master  | FE1 | FE2  |
| SW7 | 2     | Master  | FE1 | FE2  |

在物理连接各设备之前，需要先配置各设备的环网参数。

**步骤1** 登录 SW1，设置 SW1 的环网参数。

1. 登录 SW1 的命令行配置页面，具体步骤请参见“2.2 通过 Telnet 远程访问”。

2. 执行“comark-ring enable”，使能 SW1 的环网功能。

 说明：enable 代表使能环网，disable 代表禁用环网。缺省状态为 disable。

```
SWITCH# comark-ring enable
SWITCH#
```

3. 执行“comark-ring ring 1”，创建环网 1。

 说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 1
SWITCH(ring-1)#
```

4. 执行“node master-node”，设置 SW1 为主节点。

```
SWITCH(ring-1)# node master-node
SWITCH(ring-1)#
```

5. 执行“primary-port fe1”，把 SW1 的端口 FE1 设置为主端口。

6. 执行“second-port fe2”，把 SW1 的端口 FE2 设置为备用端口。

```
SWITCH(ring-1)# primary-port fe1
SWITCH(ring-1)# second-port fe2
SWITCH(ring-1)#
```

7. 执行“show comark-ring”，查看环网信息。

```
SWITCH(ring-1)# show comark-ring
Ring and RSTP cannot be set at the same time:
===== Ring Status =====
Comark-Ring Setting :Enable
 RingId | Node | FirstPort : State | SecondPort : State | Ring State
 1 | master | FE-01 :forward | FE-02 : block | ring-normal
SWITCH(ring-1)#
```

**步骤2** 参考步骤 1，分别设置 SW6 和 SW7 的环网参数。

**步骤3** 登录 SW2，并设置 SW2 的环网参数。

1. 登录 SW2 的命令行配置页面，具体步骤请参见“2.2 通过 Telnet 远程访问”。

2. 执行“comark-ring enable”，使能 SW2 的环网功能。

 说明：enable 代表使能环网，disable 代表禁用环网。缺省状态为 disable。

```
SWITCH# comark-ring enable
SWITCH#
```

3. 执行“comark-ring ring 1”，创建环网 1。

 说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 1
SWITCH<ring-1># _
```

4. 执行 “node transit-node”，设置 SW2 为主传输节点。

```
SWITCH<ring-1># node transit-node
SWITCH<ring-1>#
```

- 5. 执行 “primary-port fe1”，把 SW2 的端口 FE1 设置为环网 1 主端口。
- 6. 执行 “second-port fe2”，把 SW2 的端口 FE2 设置为环网 1 备用端口。

```
SWITCH<ring-1># primary-port fe1
SWITCH<ring-1># second-port fe2
SWITCH<ring-1>#
```

- 7. 执行 “quit”，退出环网 1 配置。
- 8. 执行 “comark-ring ring 3”，创建环网 3。

📖 说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 3
SWITCH<ring-3># _
```

9. 执行 “node transit-node”，设置 SW2 为主传输节点。

```
SWITCH<ring-3># node transit-node
SWITCH<ring-3># _
```

- 10. 执行 “primary-port fe3”，把 SW2 的端口 FE3 设置为环网 3 主端口。
- 11. 执行 “second-port fe2”，把 SW2 的端口 FE2 设置为环网 3 备用端口。

```
SWITCH<ring-3># primary-port fe3
SWITCH<ring-3># second-port fe2
SWITCH<ring-3>#
```

12. 执行 “show comark-ring”，查看环网信息。

```
SWITCH<ring-3># show comark-ring
Ring and RSTP cannot be set at the same time:
===== Ring Status =====
Comark-Ring Setting :Enable
RingId | Node | FirstPort : State | SecondPort : State | Ring State
 1 | slave | FE-01 :forward | FE-02 :forward | ring-normal
 3 | slave | FE-03 :forward | FE-02 :forward | ring-broken
SWITCH<ring-3>#
```

步骤4 参考步骤 3，分别设置 SW3、SW4、SW5 的环网参数。  
——结束  
配置各交换机的环网参数后，请根据环网图正确连接各交换机。

### 5.13.3. 创建相切环环网

介绍以太网相切环环网的配置步骤。  
如下图所示， SW1、SW2、SW3、SW4 在组成 Ring 1，SW1 为主节点。SW2、SW3、SW5、SW6 组成 Ring 2，SW6 为主节点。SW2、SW3 为 Ring 1 和 Ring 2 共用节点。

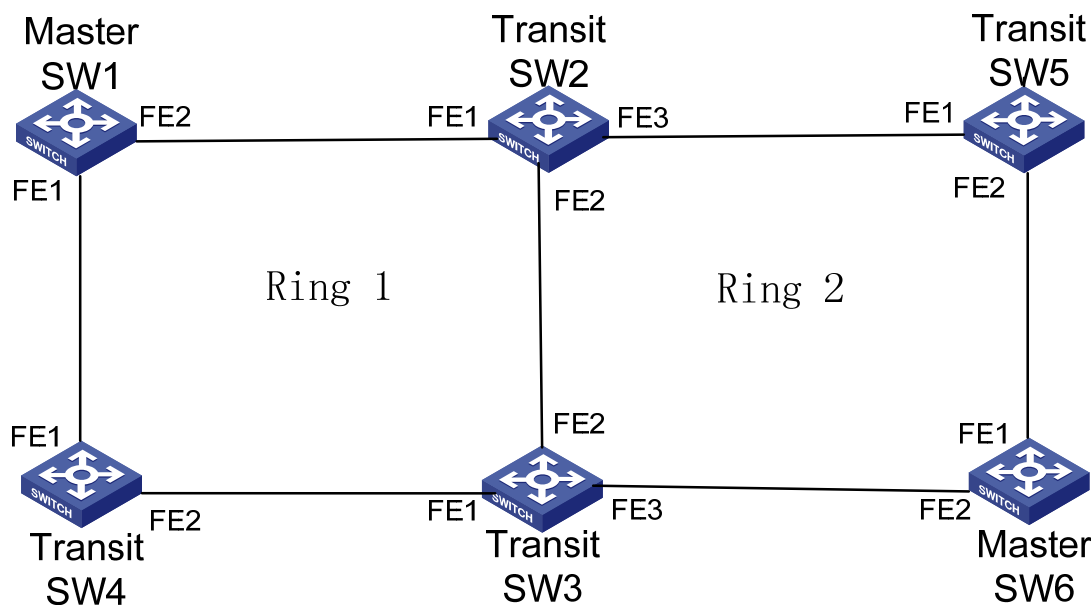


表 5-11 相切环网参数规划

| 交换机 | 环网 ID | 节点模式    | 主端口 | 备用端口 |
|-----|-------|---------|-----|------|
| SW1 | 1     | Master  | FE1 | FE2  |
| SW2 | 1     | Transit | FE1 | FE2  |
|     | 2     | Transit | FE3 | FE2  |
| SW3 | 1     | Transit | FE1 | FE2  |
|     | 2     | Transit | FE2 | FE3  |
| SW4 | 1     | Transit | FE1 | FE2  |
| SW5 | 2     | Transit | FE1 | FE2  |
| SW6 | 2     | Master  | FE1 | FE2  |

在物理连接各设备之前，需要先配置各设备的环网参数。

步骤1 登录 SW1，设置 SW1 的环网参数。

1. 登录 SW1 的命令行配置页面，具体步骤请参见“2.2 通过 Telnet 远程访问”。
2. 执行“comark-ring enable”，使能 SW1 的环网功能。

说明：enable 代表使能环网，disable 代表禁用环网。缺省状态为 disable。

```
SWITCH# comark-ring enable
SWITCH# _
```

3. 执行“comark-ring ring 1”，创建环网 1。

说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 1
SWITCH<ring-1># _
```

4. 执行“node master-node”，设置 SW1 为主节点。

```
SWITCH<ring-1># node master-node
SWITCH<ring-1># _
```

5. 执行“primary-port fe1”，把 SW1 的端口 FE1 设置为主端口。

6. 执行“second-port fe2”，把 SW1 的端口 FE2 设置为备用端口。

```
SWITCH<ring-1># primary-port fe1
SWITCH<ring-1># second-port fe2
SWITCH<ring-1>#
```

7. 执行“show comark-ring”，查看环网信息。

```
SWITCH<ring-1># show comark-ring
Ring and RSTP cannot be set at the same time:
===== Ring Status =====
Comark-Ring Setting :Enable
RingId | Node | FirstPort : State | SecondPort : State | Ring State
 1 | master | FE-01 :forward | FE-02 : block | ring-normal
SWITCH<ring-1>#
```

步骤2 参考步骤 1，分别设置 SW6 的环网参数。

步骤3 登录 SW2，并设置 SW2 的环网参数。

1. 登录 SW2 的命令行配置页面，具体步骤请参见“2.2 通过 Telnet 远程访问”。

2. 执行“comark-ring enable”，使能 SW2 的环网功能。

说明：enable 代表使能环网，disable 代表禁用环网。缺省状态为 disable。

```
SWITCH# comark-ring enable
SWITCH#
```

3. 执行“comark-ring ring 1”，创建环网 1。

说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 1
SWITCH<ring-1>#
```

4. 执行“node transit-node”，设置 SW2 为主传输节点。

```
SWITCH<ring-1># node transit-node
SWITCH<ring-1>#
```

5. 执行“primary-port fe1”，把 SW2 的端口 FE1 设置为环网 1 主端口。

6. 执行“second-port fe2”，把 SW2 的端口 FE2 设置为环网 1 备用端口。

```
SWITCH<ring-1># primary-port fe1
SWITCH<ring-1># second-port fe2
SWITCH<ring-1>#
```

7. 执行“quit”，退出环网 1 配置。

8. 执行“comark-ring ring 2”，创建环网 2。

说明：ring ID 的取值范围为 1~4094。

```
SWITCH# comark-ring ring 2
SWITCH<ring-2>#
```

9. 执行“node transit-node”，设置 SW2 为主传输节点。

```
SWITCH<ring-2># node transit-node
SWITCH<ring-2>#
```

10. 执行“primary-port fe3”，把 SW2 的端口 FE3 设置为环网 2 主端口。

11. 执行“second-port fe2”，把 SW2 的端口 FE2 设置为环网 2 备用端口。

```
SWITCH<ring-2># primary-port fe3
SWITCH<ring-2># second-port fe2
SWITCH<ring-2>#
```

12. 执行“show comark-ring”，查看环网信息。

```
SWITCH(ring-2)# show comark-ring
Ring and RSTP cannot be set at the same time:
===== Ring Status =====
Comark-Ring Setting :Enable
RingId : Node : FirstPort : State : SecondPort : State : Ring State
 1 slave FE-01 :forward FE-02 :forward ring-normal
 2 slave FE-03 :forward FE-02 :forward ring-broken
SWITCH(ring-2)#
```

步骤4 参考步骤 3，设置 SW3 环网参数。  
步骤5 参考步骤 3 的 1-7，设置 SW4、SW5 的环网参数。  
——结束  
配置各交换机的环网参数后，请根据环网图正确连接各交换机。

## 5.14 管理POE

POE 工业以太网交换机提供管理 POE 功能，支持 8 个兼容 IEEE 802.3at/af 标准带 PoE 功能以太网口，可同时支持 8 个端口 15.4W 或 4 个端口 30W，总功率不能超过 120W。

步骤1 执行“poe”，进入 poe 设置。

```
SWITCH# poe
ethernet - ethernet interface
globe_power - configure PoE globe_power
globe_threshold - configure PoE globe_threshold
log - configure PoE log
```

表 5-12 端口设置参数

| 值    | 值域                                                    | 描述                                                                  |
|------|-------------------------------------------------------|---------------------------------------------------------------------|
| 管理协议 | 802.3 af/at<br>Auto<br>Force<br>缺省值: 802.3 af/at Auto | 选择管理协议模式。<br>802.3 af/at Auto: 不可修改功率上限值，默认 30。<br>Force: 可修改功率上限值。 |
| 端口   | 如 FE1                                                 | 选择需要设置的端口号。                                                         |
| 开关   | Enabled,<br>Disabled<br>缺省值:<br>Enabled               | 启用或禁用该端口。<br>Enabled: 表示启用端口。<br>Disabled: 表示禁用端口。                  |
| 功率上限 | 取值范围:<br>0~30<br>缺省值:<br>30                           | 设置该端口的功率上限。                                                         |
| 优先级  | Low<br>High<br>critical<br>缺省值:<br>low                | 设置端口的优先级。<br>端口优先级的大小决定了这个端口满足设定功率情况。                               |

步骤2 执行“poe ethernet fe1 allocation 30”，设置端口 FE1 的功率上限为 30。  
说明: 命令中的“fe1”为交换机的端口。可根据现场实际情况修改。  
SWITCH# poe ethernet fe1 allocation 30  
步骤3 执行“poe ethernet fe1 autoneg auto”，设置端口 FE1 管理协议模式为“auto”。  
说明: 管理协议模式可根据实际情况进行设置。  
SWITCH# poe ethernet fe1 autoneg auto  
步骤4 执行“poe ethernet fe1 power enable”，设置端口 FE1 开关为“enable”。也可执行“poe globe-power enable”对所有端口进行开关设置。

 说明：开关可根据实际情况进行设置。

```
SWITCH# poe ethernet fe1 power enable
SWITCH# poe globle-power enable_
```

步骤5 执行“poe ethernet fe1 priority low”，设置端口 FE1 优先级为“low”。

 说明：优先级可根据实际情况进行设置。

```
SWITCH# poe ethernet fe1 priority low_
```

步骤6 执行“show poe”，查看端口 1 所设置的参数信息。

```
PoE Globe Status:
power output Setting :Enable
power threshold Setting :140
Max Voltage threshold :57.0
Min Voltage threshold :44.0
power output Setting :MODE B<4-5-7-8>
 PID Power Status Mode Allocation Priority Class Current Voltage Consumption
FE-1 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-2 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-3 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-4 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-5 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-6 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-7 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
FE-8 Enable On 802.3AT 30.0 low 6 0 0.0 0.0
```

——结束

## 5.15 配置串口参数

本设备提供串口服务器功能可将 RS-232/RS-422/RS-485 的数据通过 TCP Client、TCP Server 或者 UDP 模式实现串口数据的以太网转换与传输。您可以对串口的通信参数进行设置，如串口波特率、数据位、停止位、奇偶性、端口号等。对于两个进行通信的串口，这些参数必须匹配才能通信。串口功能只对带串口系列机型可见。

步骤1 执行“serial-server”，进入串口设置。

```
SWITCH# serial-server
SWITCH(serial-config)# _
```

步骤2 执行“serial-com port 1 baud-rate 9600”，设置串口 1 的波特率为“9600”。

 说明：串口和波特率可根据实际情况进行设置。

```
SWITCH(serial-config)#
quit - exit current mode
serial-com - configure the serial port settings
undo - restore the default setting
Global command:
clear - Clear the screen
exit - Exit intermediate mode
help - Show command help
show - help string for show
SWITCH(serial-config)# serial-com port 1 baud-rate 9600
```

表 5-13 端口设置参数

| 值  | 值域  | 描述          |
|----|-----|-------------|
| 串口 | 1~4 | 选择需要设置的串口号。 |

|      |                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 波特率  | 110, 300,<br>1200, 2400,<br>4800, 9600,<br>19200,<br>38400,<br>57600,<br>115200<br>缺省值: 9600 | 设置该串口的波特率。<br>波特率表示每秒钟传送的数据位的格式，是一个衡量通信速度的参数。                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 数据位  | 5~8<br>缺省值: 8                                                                                | 设置该串口的数据位。<br>数据位指每字节中实际数据所占的比特数，是衡量通信中实际数据位的参数。                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 停止位  | 1, 1.5, 2<br>缺省值: 1                                                                          | 设置该串口的停止位。<br>停止位用于标识一个数据包数据结束。停止位不仅仅用于数据包的传输结束标志，还提供了计算机之间校正同步时钟的机会。用于停止位的位数越多，不同时钟同步的容忍程度越大。但是由于停止位占用了数据空间，过多的停止位将导致数据传输速度的下降。                                                                                                                                                                                                                                                                                                                                   |
| 奇偶性  | even, mark,<br>none, odd,<br>space<br>缺省值: none                                              | 设置该串口的奇偶校验位。<br>奇偶校验用来判断接收的数据位有无错误。对于偶和奇校验，串口会设置校验位，用一个值确保传输的数据有偶个或者奇个逻辑高位。对于 1 和 0 校验，并不真正的检查数据，简单值位逻辑高或逻辑低校验，可以使接收设备能够知道一个位的状态，判断是否有噪声干扰了通信或者传输和接收数据是否不同步。<br>even: 奇校验，如果校验方式设置为“odd”，则发送数据中 1 的个数为奇数时，校验位为“0”；发送数据中 1 的个数为偶数时，校验位为“1”。<br>mark: 1 校验，如果校验方式设置为“mark”，校验位固定为“1”。<br>none: 无校验，在数据发送时，如果校验位设置为“none”，则不发送校验位，否则会发送一位校验位。<br>odd: 偶校验，如果校验方式设置为“odd”，则发送数据中 1 的个数为奇数时，校验位为“1”；发送数据中 1 的个数为偶数时，校验位为“0”。<br>sapce: 0 检验，如果校验方式设置为“space”，校验位固定为“0”。 |
| 模式   | Disabled,<br>Tcpclient,<br>Tcpserver,<br>Udp<br>缺省值:<br>Disabled                             | 设置该串口的数据到以太网的转换与传输的工作模式。<br>Tcpclient: 在此工作模式下，串口主动连接远端 IP 的目标端口。与 Tcpserver 成对使用。<br>Tcpserver: 在此工作模式下，串口监听客户端的连接。与 Tcpclient 成对使用。<br>Udp: UDP 协议没有建立连接，在使用 UDP 协议进行传输时，只向远端 IP 的目的端口收发数据。<br>Disabled: 关闭该串口。                                                                                                                                                                                                                                                  |
| 本地端口 | 1024~65535                                                                                   | 设置该串口的本地端口号。                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 远程端口 | 1024~65535                                                                                   | 设置该串口通过以太网通讯的远端设备目的串口端口号。                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|       |                       |                          |
|-------|-----------------------|--------------------------|
| IP 地址 | XXX. XXX. XXX.<br>XXX | 设置该串口通过以太网通讯的远端设备 IP 地址。 |
|-------|-----------------------|--------------------------|

步骤3 执行“serial-com port 1 data-bits 8”，设置串口 1 的数据位为“8”。

说明：串口和数据位可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 data-bits 8
```

步骤4 执行“serial-com port 1 stop-bits 1”，设置串口 1 的停止位为“1”。

说明：串口和停止位可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 stop-bits 1
```

步骤5 执行“serial-com port 1 parity none”，设置串口 1 的奇偶性为“none”。

说明：串口和奇偶性可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 parity none
```

步骤6 执行“serial-com port 1 work-mode udp”，设置串口 1 的模式为“udp”。

说明：串口和模式可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 work-mode udp
```

步骤7 执行“serial-com port 1 local-service-port 1025”，设置串口 1 的本地端口为“1025”。

说明：串口和本地端口可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 local-service-port 1025
```

步骤8 执行“serial-com port 1 peer ip-address 192.168.1.213”，设置串口 1 的目的 IP 地址为“30000”。

说明：串口和目的 IP 地址可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 peer ip-address 192.168.1.213
```

步骤9 执行“serial-com port 1 peer service-port 30000”，设置串口 1 的远端端口为“30000”。

说明：串口和远端端口可根据实际情况进行设置。

```
SWITCH(serial-config)# serial-com port 1 peer service-port 30000
```

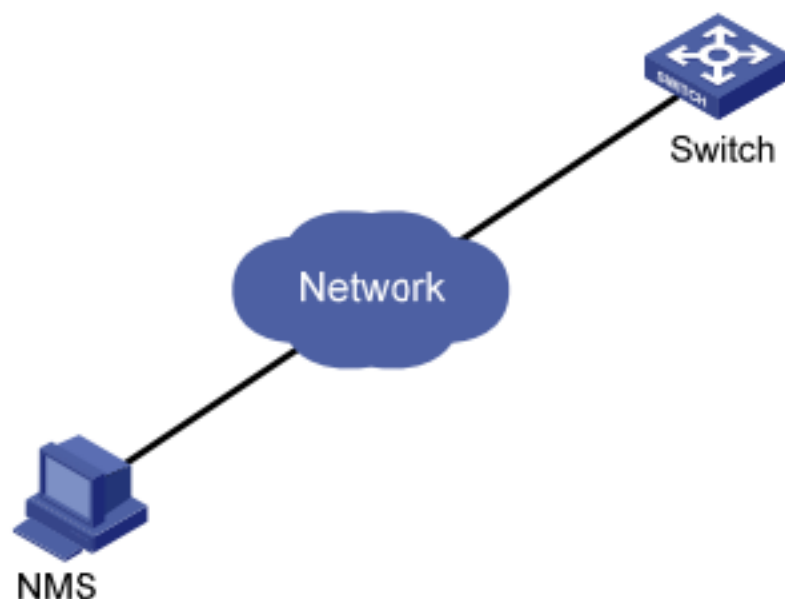
步骤10 执行“show serial-server serial-com port 1”，查看串口 1 所设置的参数信息。

```
SWITCH(serial-config)# show serial-server serial-com port 1
The information for Serial-Com Port-1
ser-type : RS232
Baud-rate : 9600 k
Stop-bits : 1.5<1>
Parity mode : n
Data-bits : 8
Work-mode : udp
Local -Port : 1025
Service-IP : 192.168.1.213
Service-Port : 30000
SWITCH(serial-config)#
```

——结束

## 5.16 管理SNMP

您可通过 NMS（Network Management Station，网管工作站）登录到交换机上，通过交换机上的 Agent 模块对交换机进行管理、配置，如下图所示。NMS 和 Agent 之间运行的协议为 SNMP（Simple Network Management Protocol，简单网络管理协议）。SNMP 是使用 TCP/IP 协议族对互联网上的设备进行管理的一个框架，它提供一组基本的操作来监视和维护互联网。



## 优势

- 自动化网络管理。网络管理员可以利用 **SNMP** 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。**SNMP** 只提供最基本的功能集，使得管理任务分别与被管设备的物理特性和下层的联网技术相对独立，从而实现对不同厂商设备的管理，特别适合在小型、快速和低成本的环境中使用。

## 网络元素

- **NMS**（Network Management Station，网络管理站）是运行 **SNMP** 客户端程序的工作站，能够提供非常友好的人机交互界面，方便网络管理员完成绝大多数的网络管理工作。
- **Agent** 是驻留在设备上的一个进程，负责接收、处理来自 **NMS** 的请求报文。在一些紧急情况下，如接口状态发生改变等，**Agent** 也会通知 **NMS**。

**NMS** 是 **SNMP** 网络的管理者，**Agent** 是 **SNMP** 网络的被管理者。**NMS** 和 **Agent** 之间通过 **SNMP** 协议来交互管理信息。

## 基本操作

- **Get** 操作：**NMS** 使用该操作查询 **Agent** 的一个或多个对象的值。
- **Set** 操作：**NMS** 使用该操作重新设置 **Agent** 数据库（**MIB**，Management Information Base）中的一个或多个对象的值。
- **Trap** 操作：**Agent** 使用该操作向 **NMS** 发送报警信息。
- **Inform** 操作：**NMS** 使用该操作向其他 **NMS** 发送报警信息。

## 协议版本

- **SNMP v1** 采用团体名（Community Name）认证。团体名用来定义 **SNMP NMS** 和 **SNMP Agent** 的关系。如果 **SNMP** 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 **SNMP NMS** 对 **SNMP Agent** 的访问。
- **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** 和 **InformRequest**），支持更多的数据类型（**Counter64** 等），提供了更丰富的错误代码，能够更细致地区分错误。
- **SNMP v3** 提供了基于用户的安全模型（**USM**，User-Based Security Model）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 **NMS** 和 **Agent** 之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 **SNMP NMS** 和 **SNMP Agent** 之间的通信提供更高的安全性。

**Agent** 可以同时配置多个版本，与不同的 **NMS** 交互采用不同的版本交互。但是当 **Agent** 和某个 **NMS** 通信时，**Agent** 和该 **NMS** 上的 **SNMP** 版本配置必须相同（即都配置为 **SNMP v1** 或者

都配置为 SNMP v2c 或者都配置为 SNMP v3），才能成功互访。  
本设备支持 SNMP v1/v2c/v3。SNMP v1 和 SNMP v2c 使用一组字符串来进行认证，也就是说 SNMP 服务器可以访问所有对象，根据不同的字符串提供用户不同的权限。如 public 权限为只读，而 private 为读/写。SNMP V3 要求用户选择 MD5 或 SHA 中的一种认证方式，它是最安全的一种协议。您也可以通过对数据加密来提升数据传输的安全级别。

表 5-14 SNMP V1/V2c/V3

| 协议版本         | 访问模式                  | 认证类型             | 数据加密 | 说明                                               |
|--------------|-----------------------|------------------|------|--------------------------------------------------|
| SNMP v1, v2c | Read Community        | Community string | 无    | 使用 Community string 匹配认证。                        |
|              | Read /Write Community | Community string | 无    | 使用 Community string 匹配认证。                        |
| SNMP v3      | Read Community        | 基于 MD5 或 SHA 的认证 | 无    | 基于 MD5 或 SHA 算法的认证，认证要求为 9~15 位密码。               |
|              |                       |                  | 数据密钥 | 基于 MD5 或 SHA 算法和数据密钥的的认证，认证和数据密钥要求为 9~15 位密码和密钥。 |
|              | Read /Write Community | 基于 MD5 或 SHA 的认证 | 无    | 基于 MD5 或 SHA 算法的认证，认证要求为 9~15 位密码。               |
|              |                       |                  | 数据密钥 | 基于 MD5 或 SHA 算法和数据密钥的的认证，认证和数据密钥要求为 9~15 位密码和密钥。 |

5.16.1. 创建SNMP团体名

SNMP 团体名是使用 SNMP v1, v2c 协议的认证，起到类似密码的作用，可以限制 SNMP NMS 对 SNMP Agent 的访问。

步骤1 执行 “snmp-server community”，进入 SNMP 团体名配置。

步骤2 设置 SNMP 团体名的 SNMP 版本、团体名称和访问模式。

表 5-15 SNMP 团体名参数

| 值       | 值域                | 描述                                                                                                                                                                            |
|---------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP 版本 | v1, v2c           | 选择团体名认证使用的 SNMP 协议。<br>v1: 表示设置 v1 的团体名认证。<br>v2c: 表示设置 v2c 的团体名认证。                                                                                                           |
| 团体名     | 取值范围：<br>3~16 个字符 | 设置 SNMP NMS 用于访问或设置 SNMP Agent 的认证字符串。                                                                                                                                        |
| 访问模式    | RO, RW            | 设置 SNMP NMS 使用团体名来访问 SNMP Agent 的权限。<br>RO: 只读模式，SNMP NMS 使用团体名只能读取 SNMP Agent 的数据，不能设置。缺省团体名为 “public” 。<br>RW: 读写模式，SNMP NMS 使用团体名可以读取或设置 SNMP Agent 的数据。缺省团体名为 “private” 。 |

如设置 SNMP 版本为 v2c，团体名为 admin，权限为 rw，则设置如下图所示。

```
SWITCH# snmp-server community
Version(v1 or v2c): v2c
Community(3-16chars): admin
Privilege(ro or rw): rw

Add snmp agent user successfully!
SWITCH#
```

——结束

### 5.16.2. 创建SNMP用户名

USM（User-based Security Model）用户名使用 SNMP v3 协议封装，使用 MD5 或 SHA 和密钥加密，可以提高 SNMP NMS 和 SNMP Agent 之间通信的安全性。

步骤1 执行“snmp-server user”，进入 SNMP 用户名配置。

步骤2 设置 SNMP 用户名的用户名称、访问模式和 SNMP v3 封装等参数。

表 5-16 SNMP 用户名参数

| 值          | 值域                | 描述                                                                                                                                            |
|------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| USM 用户     | 取值范围：<br>3~16 个字符 | 设置 USM 用户名。                                                                                                                                   |
| 访问模式       | RO, RW            | 设置 SNMP NMS 使用 USM 用户名来访问 SNMP Agent 的权限。<br>RO：只读模式，SNMP NMS 使用团体名只能读取 SNMP Agent 的数据，不能设置。<br>RW：读写模式，SNMP NMS 使用团体名可以读取或设置 SNMP Agent 的数据。 |
| SNMP V3 封装 | -                 | 设置是否使用 SNMP V3 安全加密方式。如 SNMP V3 封装不被选择， 验证和加密都将无需执行。                                                                                          |
| 授权算法       | NULL, MD5, SHA    | 选择验证所用的安全模式。<br>NULL：禁用安全模式。此时授权密码可不设置。<br>MD5：使用 MD5 算法作为验证模式。<br>SHA：使用 SHA 算法作为验证模式，比 MD5 更安全。                                             |
| 授权密码       | 取值范围：<br>9~15     | 设置授权算法的验证密码。                                                                                                                                  |
| 私有算法       | NULL, DES, AES    | 选择数据加密的安全模式。<br>NULL：禁用数据加密。此时私有密码不可设置。<br>DES：使用 DES 数据加密模式。<br>AES：使用 AES 数据加密模式，比 DES 更安全。                                                 |
| 私有密码       | 取值范围：<br>9~15     | 设置数据加密的验证秘密码。                                                                                                                                 |

如设置 SNMP 的用户名为 admin，权限为 rw，授权算法为 MD5，授权密码为 1234567890，私有算法为 DES，私有密码为 1234567890，则设置如下图所示。

```
UserName(3-16chars): admin
Popedom(ro or rw): rw
Auth-Alogrithm(MD5 or SHA or NULL): MD5
auth-password(9-15chars): 1234567890
Priv-Alogrithm(DES or AES or NULL): DES
priv-password(9-15chars): 1234567890_
```

——结束

5.16.3. 设置SNMP陷阱

SNMP 陷阱是指 SNMP Agent 在任何时候主动向 SNMP NMS 发送端口的 Linkup 和 Linkdown 情况。您可以根据实际情况设置 SNMP 陷阱的使能状态、发送陷阱的端口和接收告警信息的 SNMP NMS 所在服务器的 IP 地址。

步骤1 执行“snmp-server enable”，使能 SNMP 陷阱。

```
SWITCH# snmp-server enable
Enable global traps successfully!
```

步骤2 执行“snmp-server traps-host 192.168.1.100”，设置接收 SNMP 陷阱的主机为 192.168.1.100。

说明：接收 SNMP 陷阱信息的主机可以根据现场实际使用情况设置。

```
SWITCH# snmp-server traps-host 192.168.1.100
Add traps-host successfully!
```

步骤3 执行“snmp-server traps-port fe1 enable”，设置 FE1 为发送陷阱的端口。

说明：只有使能 SNMP 陷阱才能设置陷阱端口参数，交换机各端口缺省情况下均使能 SNMP 陷阱功能。

```
SWITCH# snmp-server traps-port fe1 enable
```

步骤4 执行“show snmp traps-status”，可以查看 SNMP 的陷阱信息。

```
SWITCH# show snmp traps-status
Global trap is enable.
interface status

ethernet-1 enable
ethernet-2 disable
ethernet-3 disable
ethernet-4 disable
ethernet-5 disable
ethernet-6 disable
ethernet-9 disable
ethernet-10 disable
```

——结束

5.17 管理系统信息

系统管理提供了交换机基本信息的管理和维护功能，主要包括修改 IP、设置简单网络时间协议、设置告警、管理 VLAN、查看系统日志、Ping 诊断、TFTP 服务等。

5.17.1. 修改IP地址

交换机只支持静态 IP 地址，需手动设置指定的 IP 地址、子网掩码和网关。通过所设置的 IP 地址可以访问交换机的配置页面。设置新的 IP 地址后需重新登录。

步骤1 执行“ipconfig ip IP 地址”，修改 IP 地址。

说明：IP 地址输入格式为 xxx.xxx.xxx.xxx，如 192.168.1.197。您可根据现场实际使用情况进行修改。

步骤2 输入“y”，按“Enter”键，确认修改 IP 地址。

```
SWITCH# ipconfig ip 192.168.1.197
Do you want to make the ip configuration efficient now? (y/n): y
```

步骤3 （可选）执行“ipconfig ip IP 地址 netmask 子网掩码 gateway 网关地址”，修改 IP 地址、子网掩码和网关地址。

说明：IP 地址、子网掩码和网关地址的输入格式均为 xxx.xxx.xxx.xxx，如 IP 地址为 192.168.1.197，子网掩码为 255.255.255.0，网关地址为 192.168.1.1。您可根据现场实际使用情况进行修改。

```
SWITCH# ipconfig ip 192.168.1.197 netmask 255.255.255.0 gateway 192.168.1.1
Do you want to make the ip configuration efficient now? <y/n>: y_
```

——结束

### 5.17.2. 设置简单网络时间协议

在大型的网络中，如果依靠管理员手工配置来修改网络中各台设备的系统时间，不但工作量巨大，而且也不能保证时间的精确性。**NTP**（**Network Time Protocol**，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，并提供较高的时间同步精度。

**NTP** 时间同步过程中需要进行复杂的时钟优选运算，时间同步速度较慢，并且占用较多的系统资源。**SNTP**（**Simple NTP**，简单 **NTP**）简化了 **NTP** 的时间同步算法，以牺牲时间精度为代价实现了时间的快速同步，并减少了占用的系统资源。在时间精度要求不高的情况下，可以使用 **SNTP** 来实现时间同步。

**SNTP** 既提供了客户端功能也提供服务器端功能。如果交换机作为 **SNTP** 服务器端，交换机作为 **SNTP** 服务器使用，其他交换机的时间可以同步到该交换机。设置该交换机系统时间年、月、日、时、分和秒，让其他交换机都同步到该交换机设置的时间。如果交换机作为 **SNTP** 客户端，可以通过 **SNTP** 服务器获取同步时间来设置该交换机的时间。

#### 作为客户端

**步骤1** 执行“**sntp-client server\_ip 192.168.1.1**”，设置 **SNTP** 服务器的 IP 地址。

```
SWITCH# sntp-client server_ip 192.168.1.1
```

**步骤2** 设置响应时间和时区偏移等参数。

表 5-17 **SNTP** 客户端参数

| 值         | 值域                                              | 描述                                                                   |
|-----------|-------------------------------------------------|----------------------------------------------------------------------|
| 服务器 IP 地址 | 格式<br>XXX.XXX.XXX.XX<br>如<br>192.168.1.1        | 设置 <b>SNTP</b> 服务器的 IP 地址。<br>执行命令：sntp-client server_ip 192.168.1.1 |
| 响应时间      | 取值范围：<br>1~59s<br>如 5                           | 设置从 <b>SNTP</b> 服务器上更新时间的频率。<br>执行命令：sntp-client inter 5             |
| 时区偏移      | 取值范围：<br>GMT -12:00~<br>GMT 12:00<br>如 GMT 8:00 | 设置格林威治标准时间（GMT）和本地时间的时差。<br>执行命令：sntp-client zone_offset GMT-8:00    |
| 时分偏移      | 取值范围：<br>1~59min<br>如 5                         | 设置格林威治标准时间（GMT）和本地时间的分钟偏差。<br>执行命令：sntp-client time_offset 5         |

```
SWITCH# sntp-client inter 5
SWITCH# sntp-client zone_offset GMT-8:00
SWITCH# sntp-client time_offset 5
SWITCH#
```

#### 作为服务器

**步骤1** 执行“**local-time date 26 month 2 year 2014**”，修改交换机的日、月、年。

 **说明：**date 的取值范围为 1~31，month 的取值范围为 1~12，year 的取值范围为 2009~3000。您可根据

现场实际使用情况进行修改。

```
SWITCH# local-time date 26 month 2 year 2014_
```

**步骤2** 执行“local-time hour 0 minute 0 second 0”，修改交换机的时、分、秒。

 **说明：**hour 的取值范围为 0~23，minute 的取值范围为 0~59，second 的取值范围为 0~59。您可根据现场实际使用情况进行修改。

```
SWITCH# local-time hour 0 minute 0 second 0_
```

——结束

### 5.17.3. 设置告警

本设备提供告警功能，提供继电器、电源、端口和环网的告警。

**步骤1** 执行“alarm enable”，使能全局告警。

 **说明：**使能全局告警后，才能设置继电器、电源、端口的告警。告警状态缺省值为 disable。

```
SWITCH# alarm
 disable - disable alarm
 enable - enable alarm
 ring - configure ring
 sysalarm - configure sysalarm
SWITCH# alarm enable_
```

#### 系统告警

**步骤2** 执行“alarm sysalarm outType on”，设置继电器告警有效状态为“常开”。

 **说明：**继电器告警有效状态分为“常开”和“常闭”两种状态。其中“常开”对应的命令是“alarm sysalarm outType on”，“常闭”对应的命令是“alarm sysalarm outType off”。您可以根据现场实际使用的报警设备状态选择交换机的“继电器告警有效状态”。继电器告警有效状态需与现场实际使用的报警设备的状态一致。如现场的报警设备状态为“常开”，则把继电器告警有效状态设置为“常开”。

```
SWITCH# alarm sysalarm outType on_
```

**步骤3** 执行“alarm sysalarm power 1 force enable”，启用电源 1 的告警状态。

 **说明：**交换机提供电源 1 和电源 2 两路电源输入，电源告警缺省状态为 disable。您可以根据现场实际情况设置电源的告警状态。

```
SWITCH# alarm sysalarm power 1 force enable_
```

**步骤4** 执行“alarm sysalarm ethernet fe1 force enable”，启用端口 FE1 的告警状态。

 **说明：**您可以根据现场实际情况设置端口的告警状态，端口告警缺省状态为 disable。

```
SWITCH# alarm sysalarm ethernet fe1 force enable_
```

#### 环网告警

**步骤5** 执行“alarm ring 1 force enable”，启用环网 1 的告警状态。

 **说明：**您可以根据现场实际情况设置端口环网的告警状态，环网告警缺省状态为 disable。

```
SWITCH# alarm ring 1 force enable_
```

**步骤6** 执行“show alarm”，查看告警的状态。

```
Alarm Status:
 Alarm Setting :Enable
 The relay outType :On
 The relay status :Open
Power Set status

Power1 enable Fault
Power2 disable Ok
Port Set status

FE-1 enable Down
FE-2 enable Down
FE-3 disable Down
FE-4 disable Down
FE-5 disable Up
FE-6 disable Down
FE-7 disable Down
FE-8 disable Down
GE-1 disable Down
GE-2 disable Down
Ring Set status

1 enable ring-broken
```

——结束

### 5.17.4. 设置管理VLAN

管理 VLAN 是指用于登录交换机配置页面进行交换机管理和维护的 VLAN 组。该 VLAN 组必须存在 VLAN 列表中。

**步骤1** 执行“management-vlan 1”，配置管理 VLAN。

 **说明：**VID 的取值范围为 1~4094。所配置的 VLAN 必须已创建。

```
SWITCH# management-vlan
<vid> - vlan ID 1-4094
SWITCH# management-vlan 1_
```

**步骤2** 执行“show vlan all”，可查看管理 VLAN 的信息。

```
SWITCH# show vlan all
Management VLAN: 1

PORT QinQ PVID Admit-frame

FE-1 disable 1 All
FE-2 disable 1 All
FE-3 disable 1 All
FE-4 disable 1 All
FE-5 disable 1 All
FE-6 disable 1 All
GE-1 disable 1 All
GE-2 disable 1 All

vlan-1(members):
 FE-1 ----- untagged
 FE-2 ----- untagged
 FE-3 ----- untagged
 FE-4 ----- untagged
 FE-5 ----- untagged
 FE-6 ----- untagged
 GE-1 ----- untagged
 GE-2 ----- untagged
```

——结束

### 5.17.5. 查看系统日志

显示交换机系统的告警日志，您可以根据告警信息进行交换机维护。执行“show log”可查看系统日志。

```
SWITCH# show log
```

### 5.17.6. Ping诊断

执行“ping IP 地址”，通过 Ping IP 地址可以检查交换机和某设备之间的连接情况。如 ping 192.168.1.1。

```
SWITCH# ping 192.168.1.1
```

### 5.17.7. 修改帐户

本设备提供用户名和密码修改。您可以通过该功能修改当前的用户名和密码。

步骤1 执行“user”，进入帐号修改。

步骤2 输入“y”，按“Enter”键，确认需要修改帐号。

```
SWITCH# user
Do you want to change the user?(y/n): y_
```

步骤3 输入旧密码。

步骤4 输入新用户名。

步骤5 输入两次新密码。

```
SWITCH# user
Do you want to change the user?(y/n): y
old password: ***
user : admin
password: ***
password(again): ***
Changing user successfully!
SWITCH#
```

——结束

5.17.8. 更新Firmware

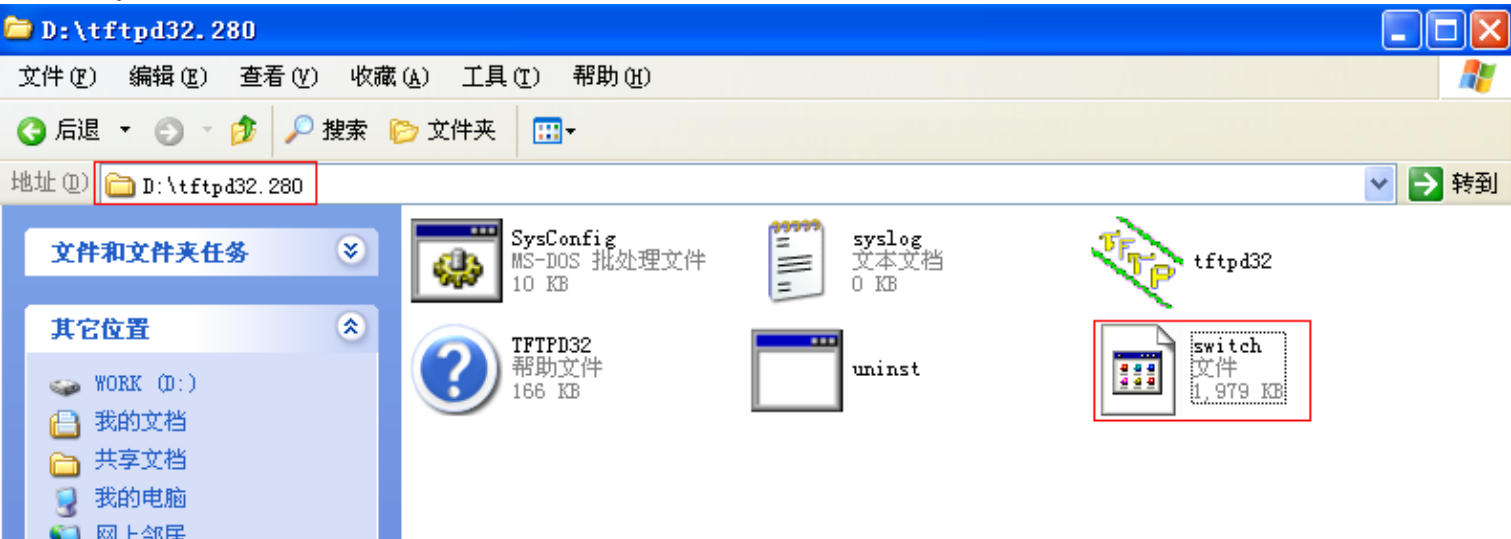
TFTP（Trivial File Transfer Protocol，简单文件传输协议）使用方便，在连接过程中不需要认证控制，适用于客户端和服务端之间不需要复杂交互的环境。通过 TFTP 的升级固件功能您可以更新交换机软件。在升级交换机软件之前，请确保交换机与 TFTP 服务器正确连接。

步骤1 打开附件中的“tftpd32.exe”。

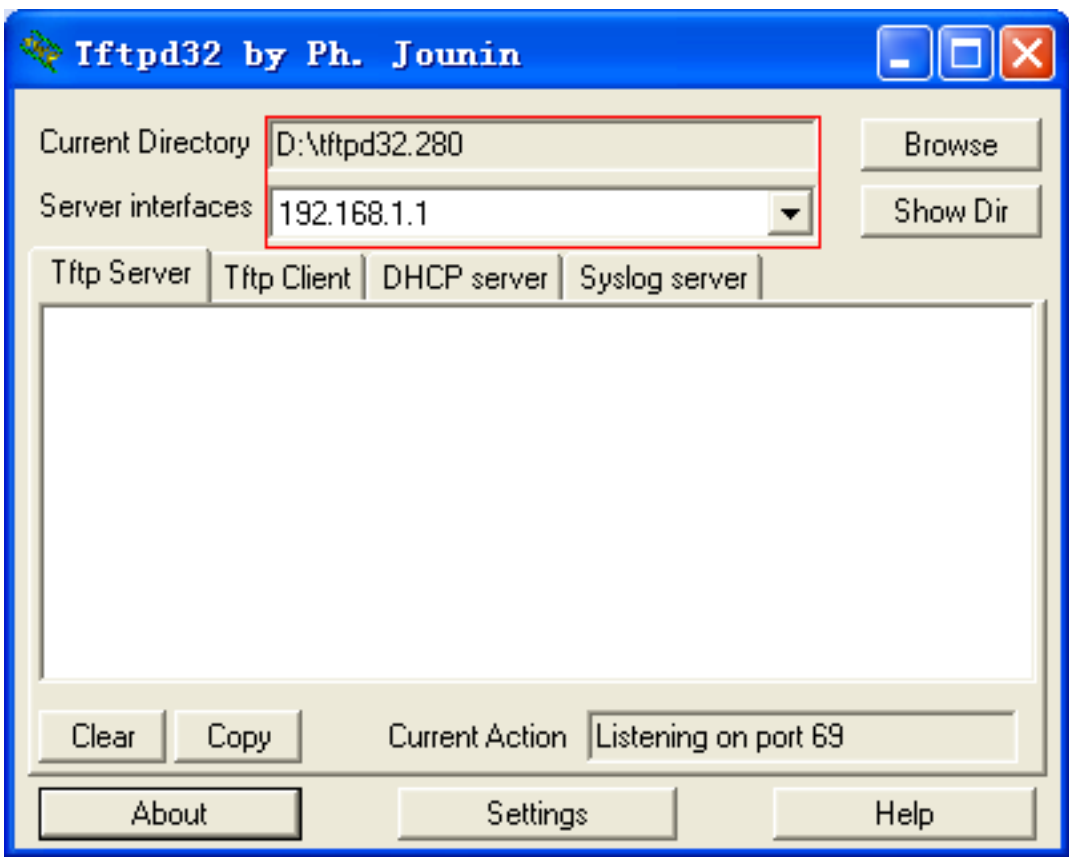


tftpd32.280.rar

步骤2 在 TFTP 中设置 TFTP 服务器的 IP 地址和 Firmware 存放路径。  
如 TFTP 服务器的 IP 地址为“192.168.1.1”，固件“comark”存放在 TFTP 服务器的“D:\tftpd32.280”中。



在 TFTP 中设置如下图所示。



**步骤3** 执行“`update firmware comark tftp-server 192.168.1.1`”，进行 Firmware 升级。

**说明：**升级可能需要几分钟，在升级过程中不可断开电源或进行其他设置。

```
SWITCH# update firmware comark tftp-server 192.168.1.1
```

**步骤4** 执行“`reboot`”，不保存配置重启交换机使所升级的软件生效。

——结束

## 5.17.9. 下载或上传配置文件

TFTP（Trivial File Transfer Protocol，简单文件传输协议）使用方便，在连接过程中不需要认证控制，适用于客户端和服务端之间不需要复杂交互的环境。通过 TFTP 的配置文件功能您上传或下载的配置文件。在上传或下载配置文件之前，请确保交换机与 TFTP 服务器正确连接。

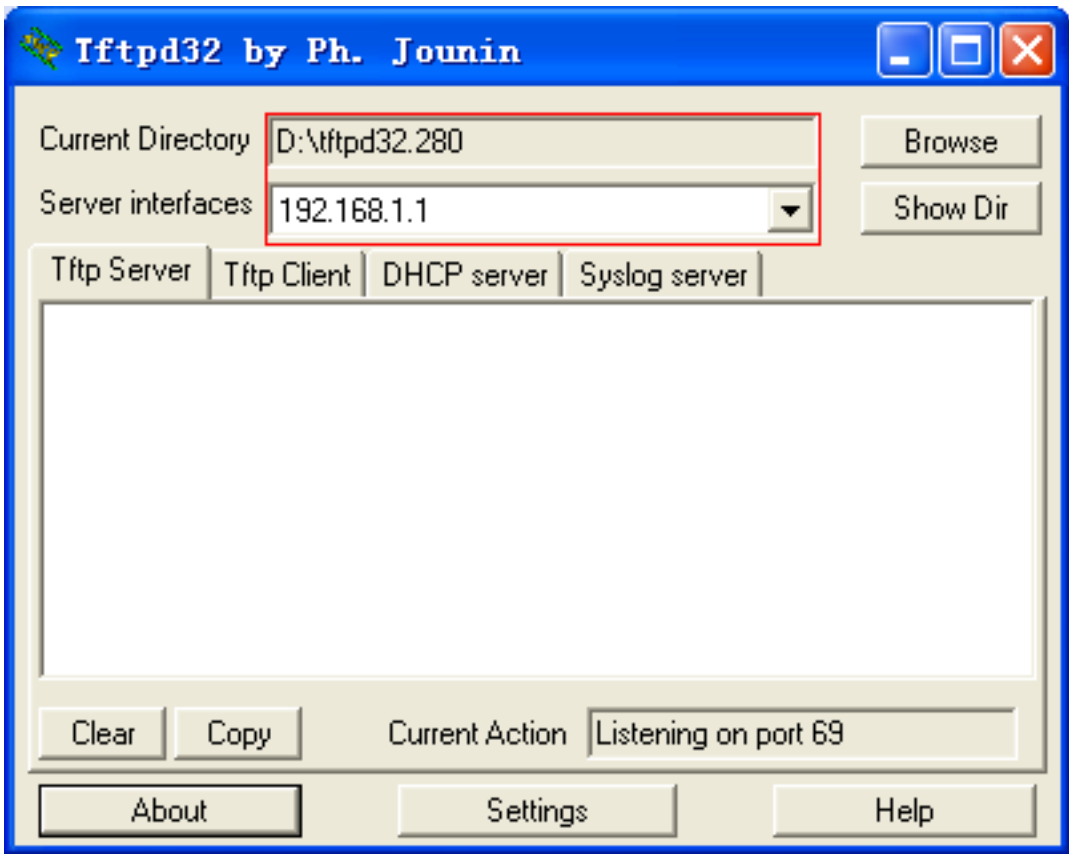
**步骤1** 打开附件中的“`tftpd32.exe`”。



tftpd32.280.rar

**步骤2** 在 TFTP 中设置 TFTP 服务器的 IP 地址和配置文件存放路径。

如 TFTP 服务器的 IP 地址为“`192.168.1.1`”，配置文件存放在 TFTP 服务器的“`D:\tftpd32.280`”中，则在 TFTP 中设置如下图所示。



步骤3 执行“tftp 192.168.1.1 get”或“tftp 192.168.1.1 put”，下载或上传交换机配置文件。

```
SWITCH# tftp 192.168.1.1 get _
SWITCH# tftp 192.168.1.1 put _
```

——结束

### 5.18 保存配置

您可以执行“save”保存当前配置的数据，防止交换机断开电源或重启时数据丢失。

```
SWITCH# save
Do you want to save the current switch configuration? (y/n): y_
```

### 5.19 恢复出厂设置

您可以执行“reset configuration”使交换机所有配置恢复到出厂时的配置。

```
SWITCH# reset configuration
Do you want to reset all the configuration? (y/n): y
```

### 5.20 重启系统

您可以执行“reboot”来选择是否保存当前配置再重启交换机系统。

```
SWITCH# reboot
Do you want to save the current configuration? (y/n): y_
```

### 5.21 退出系统

执行“exit”，可以退出当前用户的登录并关闭 telnet 连接窗口。

## 6. 常见问题

表 6-1 常见问题

| 问题          | 描述                         |
|-------------|----------------------------|
| 加电时所有指示灯均不亮 | 可能是电源连接错误或供电不正常，请检查电源线和插座。 |

|                         |                                                             |
|-------------------------|-------------------------------------------------------------|
| 网络能通，但传输速度变慢，有丢包现象      | 可能交换机与网络终端以太网口工作模式不匹配，请设置以太网口工作模式使其匹配或将其设为自适应工作模式。          |
| 正常工作一段时间后停止工作，而电源不正常,过热 | 请仔细检查以下两个方面：<br>1.检查电源是否有接触不良、电压过低或过高。<br>2.检查周围环境，通风孔是否畅通。 |
| 不能通过 Telnet 访问系统        | 可能是网络连接不正确，或 IP 地址不正确，请检查网络连接或通过串口访问系统，获取 IP 地址。            |