



UFS-2400NW

用户指导手册

©copyright 2005 by UCOM International InCo., Ltd. All rights reserved.

(第四版, 2005-12-01)

事先未征得友康国际股份有限公司（以下简称友康公司）的书面同意，任何人不得以任何方式拷贝或复制本文档中的任何内容。

友康公司不做与本文档相关的任何保证，不做商业性、质量或特定用途适用性的任何隐含保证。本文档中的信息随时可能变更，而不另行通知。友康公司保留对本出版物做修订而不通知任何个人或团体此类变更的权利。

产品设计：友康国际股份有限公司网络研究中心

地址：美国加州硅谷 2122Montere Hwy.,

TEL: 1-909-605-9900 FAX: 1-909-605-9901

中国区服务中心：

地址：深圳市福田区泰然工贸园劲松大厦 16D

邮编：518040

技术支持中心电话：(0755) 83890769/83890771

技术支持中心传真：(0755) 83891000

维修中心电话：(0755) 83890778

维修中心传真：(0755) 83891000

网址：<http://www.ucom.com.cn/>



是友康公司的商标。

目录

引言	5
1. 产品概述.....	6
1.1 端口特性.....	6
1.2 二层特性.....	6
1.3 管理特性.....	7
1.4 QOS 特性.....	7
2. 交换机的安装和使用	8
2.1 物品清单.....	8
2.2 安置方法.....	8
2.3 安置在桌面上的方法.....	8
2.4 上架的安装方法.....	8
2.5 加电.....	9
2.6 断电.....	9
2.7 注意事项.....	9
3. 交换机外观介绍.....	10
3.1 前面板.....	10
3.2 后面板.....	10
3.3 可选的扩展模块.....	11
3.3.1 100BASE-FX 模块.....	11
3.4 LED 指示灯.....	11
4. 交换机连接方法.....	11
4.1 连接到网络节点.....	11
4.2 连接到其他交换机或集线器.....	12
5. 交换机管理的概念	13

5.1	本地控制口管理	13
5.2	MAC 地址.....	13
5.3	管理信息库 (MIB)	13
5.4	包转发 (Packet Forwarding)	14
5.4.1	MAC 地址老化时间 (Aging Time)	14
5.4.2	过滤 (Filtering)	14
5.5	生成树协议 (Spanning Tree Protocol)	15
5.5.1	生成树的基本概念	15
5.5.2	生成树参数	16
5.5.3	创建 STP 拓扑结构	17
5.5.4	STP 端口状态	18
5.5.5	生成树举例	19
5.6	端口聚合(Port Aggregation)	20
5.7	虚拟局域网 VLAN.....	20
5.7.1	802.1Q VLAN	21
5.7.2	Port-Based VLAN	25
5.8	广播风暴 (Broadcast) 的管理.....	26
5.8.1	广播风暴 (Broadcast Storm)	26
5.8.2	分割广播域 (Segmenting Broadcast Domains)	26
5.8.3	减少广播风暴 (Eliminating Broadcast Storms)	26
6.	使用 CONSOLE 接口配置交换机.....	28
6.1	概括介绍	28
6.2	如何登录控制台界面	28
6.2.1	配置超级用户	29
6.2.2	配置交换机 IP 地址.....	31
6.3	CLI 命令使用说明	32
6.3.1	一些特殊键的使用	32
6.3.2	语法帮助	33
6.3.3	使用语法帮助补齐命令	33
6.3.4	命令帮助使用说明	33
6.3.5	常用命令	34
6.3.6	用户管理命令	40
6.3.7	配置交换机端口命令	41
6.3.8	虚拟局域网 (VLAN) 配置命令	47
6.3.9	生成树协议 STP 配置命令	53
6.3.10	认证设置	60
6.3.11	集群管理 (虚拟堆叠)	64
6.3.12	Garp 协议	71
6.3.13	端口聚合管理	76
6.3.14	简单网络管理 (SNMP)	76
6.3.15	MAC 地址绑定	82

6.3.16	MAC 地址过滤	83
6.3.17	日志功能	84
7.	基于 WEB 的网络管理	88
7.1	准备工作	88
7.2	WEB 管理界面配置说明	88
7.2.1	基本配置	89
7.2.2	高级配置（Advances Setup）	97

引言

UFS-2400NW 以太网交换机是新一代数据通信产品。该交换机以采用威盛高端交换芯片为核心，提供 10Mbps 、 100Mbps 的线速交换，支持 WEB,SNMP 等多种先进管理方式。

UFS-2400NW 的主要应用是为园区网建设提供支持二层交换的以太网交换机，或者配合特殊的软件（选件，支持认证和计费）用于宽带小区接入的以太网接入设备。

UFS-2400NW 支持 24 个 **100BASE-TX** 接口和最大 2 个 **100BASE-FX** 多模接口或 **100BASE-FX** 单模接口。

1. 产品概述

本章简要介绍了 UFS-2400NW 的交换功能和特性。

1.1 端口特性

- 24 个高性能的 10/100 Mbps 自适应端口
- 24 个端口都支持 10Mbps/ 100Mbps 速率和全双工/半双工模式的自动适应
- 在前面板上提供两个扩展插槽，可以扩展两个单口 100BASE-FX
- 提供 RS-232 控制端口(console port), 可以通过一台终端或者运行终端仿真程序的 PC 对交换机进行设置和管理

1.2 二层特性

- 6.4 Gbps 的交换背板
- 存储转发（Store and forward）的交换方式
- 在 10Mbps 和 100Mbps 连接下，支持全双工/半双工的工作模式。两个单口 100BASE-FX 只支持全双工的工作模式。
- 在全双工模式下，提供 IEEE 802.3x 流量控制功能（flow control）
- 在半双工模式下，提供背压流控功能（Back-pressure flow control）
- 每个端口提供极性的自动检测和纠正的功能
- 提供一个扩展插槽（支持双口模块）
- 接口模块种类：

100Base-FX 多模 传输距离 2km

100Base-FX 单模 传输距离 15km

- 在 10Mbps 速率下，可以达到 100% 的线速（wire-speed）的数据转发速率（14,880pps）
- 在 100Mbps 速率下，可以达到 100% 的线速（wire-speed）的数据转发速率（148,800 pps）
- 在 10Mbps 速率下，可以达到 100% 的线速（wire-speed）的数据过滤速率（14,880 pps）
- 在 100Mbps 速率下，可以达到 100% 的线速（wire-speed）的数据过滤速率（148,800 pps）
- 6 K 的 MAC 地址表，自动学习（automatic learning and aging）时间为 10 秒至 700 秒
- 支持广播风暴（Broadcast storm）控制，限制广播风暴
- 支持端口镜像（Port Mirroring），可以将任何一个端口（FE 或 GE）设置为镜像端口或监听端口，支持以下三种 Mirror 策略或他们的混合设置：

n 只镜像输入报文

n 只镜像输出报文

n 镜像所有报文

- 支持端口聚集（Port Trunking），最多支持 7 个聚集组（trunk group），每个组中最多

可以包含 4 个端口

- 支持 802.1D 生成树（Spanning Tree）
- 支持 VLAN 功能
 - n 802.1Q VLAN 和 PORT VLAN 可选
 - n 支持 GVRP VLAN 注册协议
 - n 支持 256 个 802.1Q 静态 VLAN 表项或 26 个 PORT VLAN 表项
 - n 支持 1-4094 VID 透传
- 支持 802.1p 优先级（Priority），提供 2 个优先队列

1.3 管理特性

- 提供 RS-232 控制端口（console port），用于通过一台终端或运行终端仿真程序的 PC 对交换机进行带外（out-of-band）网络管理
- 用闪存方式的软件升级设计，可以通过 TFTP 进行带内软件升级
- 支持通过 Console 接口进行访问
- 支持通过 TELNET 方式进行远程网管
- 支持远程 WEB 方式网管
- 支持 FTP/TFTP 方式的软件升级
- 提供口令(Password)安全设置

1.4 QOS特性

- 支持 IEEE802.1p 包优先级队列
- 具有 2 个输出优先级队列

2. 交换机的安装和使用

本章主要介绍 UFS-2400NW 的安装和使用方法。

2.1 物品清单

打开 UFS-2400NW 的包装箱，你将看到如下物品：

- ◆ UFS-2400NW 以太网交换机 一台
- ◆ 电源线 一根
- ◆ 用户手册光盘 一张
- ◆ 串口电缆 一根
- ◆ 安装螺钉 四只
- ◆ 黏性橡胶垫 四只
- ◆ 用户登记/保修卡 一本

如果发现上述物品有缺失或损坏，请立即与供货的销售商联系更换。

2.2 安置方法

请按照下述方法安置交换机：

- ◆ 放置交换机的表面（例如桌面）至少能够承受 3 千克的重量。
- ◆ 电源插座必须距离交换机 1.8 米之内。
- ◆ 确保电源线已可靠地插在电源插座上。
- ◆ 确保交换机周围留有足够的通风散热的空间，并且请不要将重物放置在交换机上。

2.3 安置在桌面上的方法

首先，将包装箱内的四个黏性橡胶垫粘贴到 UFS-2400NW 交换机背面的四个角落处，以使交换机与周围物体能够保留足够的通风空间。然后，将交换机放置于桌面上。

2.4 上架的安装方法

UFS-2400NW 交换机可以安装在标准的 19 寸机架内。首先，将包装箱内的上架的配件用螺丝安装在交换机的侧板上。然后，再用螺丝将交换机固定在 19 寸机架内

2.5 加电

UFS-2400NW 交换机的输入电压为110-240 V（50 - 60 Hz）交流电。交换机的电源开关位于交换机背面，紧邻电源插孔和系统散热风扇。在110V-240 V 允许输入电压范围内，UFS-2400NW 交换机能够自动检测输入的电源值，并适应输入电压，保持正常工作。

给 UFS-2400NW 交换机加电后，交换机前面板上的LED 状态指示灯将表现出如下状态：

- 所有 LED 指示灯将瞬间闪烁一下，这表示交换机的系统在进行复位。
- “power”指示灯在加电后将常亮，无闪烁。
- 当交换机在加载内置的程序进行自检时，“system”指示灯将闪烁。大约 5 秒钟之后，“system”指示灯将稳定地闪烁，表示交换机已经进入稳定工作状态。

2.6 断电

当供电出现问题时，为了防止对交换机造成损坏，请将电源线从交换机上拔下。当供电恢复时，再将交换机的电源线插上。

2.7 注意事项

在使用本装置时，为避免使用不当造成设备损坏及对人身伤害，请遵从以下注意事项：

- （1）使用前认真阅读本手册；
- （2）在清洁交换机前，应先将交换机电源头拔出，要用湿润的布料擦拭，不可用液体清洗；
- （3）请不要将交换机放在水边或潮湿的地方，并防止水和湿气进入交换机机壳；
- （4）请不要将交换机放在不稳定的桌子或箱子上，万一跌落，会造成严重损失；
- （5）应保持室内通风良好并保持交换机通气孔通畅；
- （6）UFS-2400NW 交换机要在正确的电压下才能正常工作，请确认工作电压与交换机所标示的电压相同；
- （7）为减少受电击的危险，在交换机工作时不要打开外壳，即使在不带电的情况下也不要自行打开。

3. 交换机外观介绍

本章主要介绍 UFS-2400NW 的前面板、后面板、可选扩展模块及其 LED 状态指示灯。

3.1 前面板

在 UFS-2400NW 的前面板上有 24 个 10/100 Mbps 自适应的以太网端口、2 个扩展插槽、1 个 RJ-45 控制接口和一些 LED 状态指示灯。



图 3-1 UFS-2400NW 的前面板示意

- 提供了一些 LED 状态指示灯，以便监视交换机的实时工作状态（详见下文中的“LED 指示灯说明”一节）。
- 提供 1 个 RJ-45 控制接口（console port），以便通过一台终端或者运行仿真终端程序的 PC 对交换机进行配置和管理。
- 在前面板的右侧有 2 个扩展插槽，可用于扩展两个单口的以太网模块，支持 100BASE-FX 千兆以太网模块。
- 24 个高性能的 10/100 Mbps 自适应的以太网端口，具有自动适应速率和全双工/半双工模式的能力
- 所有端口具有自识别能力，和其它交换设备相连或 PC 机相连时交叉双绞线或直通双绞线都可使用。

3.2 后面板

在 UFS-2400NW 的后面板上有一个三相的交流电源插口，支持的输入电压为 110-240V（50-60Hz）的交流电。

右侧有一些散热通风孔。是用于为交换机进行通风散热用的，以保证交换机能够正常工作。因此，请不要挡住这些散热装置，保证交换机的两侧留有 15 厘米左右的空间，以确保能够通风散热。

3.3 可选的扩展模块

UFS-2400NW 的所有可选扩展模块都需要单独购买，出厂配置中不包括这些可选的扩展模块。

3.3.1 100BASE-FX模块

- 有 100BASE-FX 单模和多模

3.4 LED指示灯

UFS-2400NW 的LED 状态指示灯包括“Power”、“System”、“BSF” 和“Link/Active”。下面介绍各指示灯的含义。

Power: 在交换机开机后，该灯将常亮（绿色），无闪烁。

System: 在交换机开机后，该灯将不断闪烁，表示程序运行。

BSF: 当交换机内由大量的广播报文时，该灯将不断闪烁，可通过6.3.7.7设置广播风暴控制。

Act/Link: 指示灯的上排为Speed灯，下排为Link/Active灯。当端口与所连接设备之间建立起正常的连接后，Link/Active指示灯将亮，表示已经link上，并且当端口正在收发数据时，此指示灯将闪烁(Activity-Act)；如果端口设置为100M时，Speed灯亮，如果为10M则灭。

4. 交换机连接方法

本章主要介绍 UFS-2400NW 交换机与网络之间的连接方法。

4.1 连接到网络节点

网络节点是指安装有 10Mbps、100Mbps 或 10/100Mbps 网卡的 PC 或服务器，以及路由器等网络设备。这些网络节点的接口都为 MDI-II 接口，它们需要与 MDI-X 类型的接口相连。

一个网络节点需要通过一根直通的 5 类或超 5 类非屏蔽/屏蔽双绞线与交换机连接起来。网络节点可以连接到 UFS-2400NW 交换机上的 24 个 RJ-45 端口或者扩展光模块上的任意一个端口上。交换机上的任何一个端口均可作为级联端口(uplink)，用于 UFS-2400NW 交换机与其他交换机或集线器级联时使用。



图 4-1交换机与网络节点间的连接方法

当 UFS-2400NW 交换机与网络节点之间建立起稳定的连接后，交换机上的LED 指示灯将出现如下显示状态：

1. Link指示灯亮，为绿色，表示已经link上。

4.2 连接到其他交换机或集线器

UFS-2400NW 交换机与其他交换机或集线器之间的连接方法有多种，既可以使用直通双绞线通过将交换机上任一端口与另一台交换机（或集线器）的级联（Uplink）端口（MDI-II）连接起来，或者使用交叉双绞线通过将交换机上任一端口与另一台交换机（或集线器）级联（Uplink）端口（MDI-II）连接起来，或者使用交叉双绞线/直通双绞线通过将交换机上任一端口与另一台交换机（或集线器）普通端口（MDI-X）连接起来，来实现交换机之间或交换机和集线器之间的级联。换句话说，只要与 UFS-2400NW 相连的交换机或集线器能识别的网线，UFS-2400NW 都可识别，不必区分交叉或直通。

一台 10BASE-TX/100BASE-TX 集线器或交换机可以使用 5 类或超 5 类非屏蔽/屏蔽双绞线与 UFS-2400NW 连接起来。如下图所示。



图 4-2与其他交换机或集线器之间的连接方法

5. 交换机管理的概念

本章主要介绍配置和管理交换机时将涉及到的一些概念和特性。

具体如何配置和管理交换机，实现这些概念和特性将在下一章中进行介绍。

5.1 本地控制口管理

本地控制口管理是指用一台终端或者一台运行终端仿真程序的PC 直接连接交换机的 RS-232 控制端口（console port），来对交换机进行配置和管理。这种管理方式为带外（Out-of-Band）管理方式，不需要借助网络进行通信，所以，即使网络运行不正常，也可以通过控制（console）接口对交换机进行配置和管理。

本地管理是通过终端连接操作交换机内置的控制台程序（console program），来对交换机进行管理的（详见第六章“使用Console接口配置交换机”）。

在 UFS-2400NW 交换机的内部有CPU、内存、flash等部件，其中，内存是用于存储数据的，flash用于存放配置数据、配置程序。这些部件使得交换机既可以通过控制端口（console port）进行管理和监视，也可以通过带内（in-band）网络进行管理和监视，不支持带外（out-of-band）管理。

5.2 MAC地址

交换机在出厂时还会被赋予一个唯一的MAC 地址。此MAC 地址不可以被改变，在交换机初始化界面中可以看到交换机的MAC 地址。

5.3 管理信息库（MIB）

所有管理信息和计数器都存贮于交换机内的管理信息库（Management Information Base，简称 MIB）。交换机一般使用标准的 MIB-II 管理信息库模块，因此，可以被任何基于 SNMP 的网管软件所读取。除了 MIB-II 之外，交换机还可以拥有私有的 MIB（proprietary enterprise MIB），作为补充的管理信息库。这些 MIB 也可以被网络管理系统中指定的 MIB 实体识别符（MIB Object-Identity，简称为 OID）所读取。MIB 值可以是只读的（read-only）或者可读写的（read-write）。

只读 MIB 可以是预置在交换机内部的常量（constant），也可以是随着交换机运行状态而不断变化的变量（variable）。例如，交换机的端口数量和端口的类型就是只读的常量，而统计所发生的错误的数量、或者每个端口接收并转发的数据量的计数器就是只读的变量。

可读写 MIB 通常是与用户定制（user-customized configurations）有关的变量。例如，

交换机的 IP 地址、生成树算法的参数，以及端口的状态等。

如果你使用第三方的 SNMP 管理软件来管理交换机，那么你可以要求交换机厂商提供其私有的 MIB（propriety enterprise MIB）。如果你所使用的软件提供浏览和修改 MIB 的功能，那么你可以得到 MIB 的数值并改变它们（如果该 MIB 的属性允许进行写操作的话）。但是，这是比较复杂的一件事情，因为你必须知道 MIB 的 OID，并且需要一一去读取它们。

5.4 包转发 (Packet Forwarding)

交换机具有学习网络的构成情况，并根据学习到的信息进行转发数据包的能力。由于交换机仅将数据包发送给目的地址，而不是发送给网段内的所有地址，所以可以有效地减少网段内的拥塞。例如，如果端口1 收到一个欲发送给连接在端口2 上的某个站点的数据包，那么，交换机只会将此数据包发送给端口2，而不会发给任何其它端口。这个过程就是学习网络拓扑结构的过程。

5.4.1 MAC地址老化时间 (Aging Time)

老化时间是一个影响交换机学习进程的参数。在老化时间内，如果地址未被使用，那么，这些地址将从动态转发地址表（由源MAC 地址、目的MAC 地址和它们相对应的交换机的端口号）中被删除。

老化时间的数值范围从10 秒~700 秒，缺省值为300 秒。过长的老化时间会导致交换机内的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。但是，如果老化时间过短，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。



注意：该老化时间必须是能被3整除的整数。

静态转发地址表（Static forwarding entries）不受老化时间的影响。

5.4.2 过滤 (Filtering)

交换机可以使用过滤数据库（filtering database）来划分网段，并控制网段间的数据通信。还可以过滤掉非法侵入的数据包。静态过滤地址表可以由 MAC 地址过滤方式实现。

交换机上的每个端口都对应一个碰撞域，交换机将过滤（即丢弃）那些目的地址与源地址相同的数据包，以避免本地数据包影响网络上的正常通信。

控制非法数据包的侵入是指交换机将丢弃任何一个发往或者来自过滤地址表中的 MAC 地址或 IP 地址表的数据包。

交换机将自动处理的一些过滤：

- 动态过滤（Dynamic filtering）：自动学习并更新 MAC 地址表。用以将本地的数据流限定在所属的网段内。

- 依据生成树协议进行的过滤（ **Filtering done by the Spanning Tree Protocol**）：可以根据拓扑结构进行过滤，确保没有网络环路生成。
- **VLAN 过滤**：从一个 VLAN（例如，VLAN 2）中的某个成员发往另外一个 VLAN（VLAN 3）的数据包将被过滤掉。

5.5 生成树协议（*Spanning Tree Protocol*）

IEEE 802.1D 生成树协议（Spanning Tree Protocol）允许网络上存在环路时，自动断开环路连接。当检测到交换机间存在多条连接时，将只启动最主要的一条连接，而将其他连接都阻塞掉，将这些连接变为备用连接。当主连接出现问题时，生成树协议将自动起用备用连接接替主连接的工作，不需要任何人工干预。一旦生成树协议被设置好并启动，将会自动建立主连接，并自动阻塞其余形成环路的连接。

这种网络自动重构的功能，使得网络上的用户能够最大限度地与网络保持正常的连接。但是，生成树算法较复杂，所以，建议最好在充分研究理解其之后，再更改其一些设置。请仔细阅读并理解下述内容之后，再去更改交换机上的生成树的默认设置。

UFS-2400NW 交换机上的生成树提供如下功能：

- 自动重建生成树，以补偿发生的连接故障，增加或删除生成树中的组成成员。
- 重构生成树，不需要任何人工干预。

5.5.1 生成树的基本概念

根桥（Root Bridge）：具有最小桥标志级数的（lowest Bridge Identifier）交换机是根桥（Root Bridge）。当然，你希望根桥是环路中所有交换机中最好的一台交换机，以保证能够提供最好的网络性能和可靠性。

桥标志级（Bridge Identifier）：桥标志级是桥的优先级和交换机的 MAC 地址的综合数值，其中桥的优先级是一个用户可以设定的参数。例如，“4 00 80 00 01 00 02”中的 4 是桥的优先级，“00 80 00 01 00 02”是桥的 MAC 地址。交换机的桥标志级数越低，则交换机的优先级越高，这样可以增加其成为根桥的可能性。

指定桥（TPESigned Bridge）：在每个网段中，到根桥的路径开销最低的（lowest Root Path Cost）桥将成为指定桥，数据包将通过它转发到网段。一旦所有的交换机具有相同的根路径开销（Root Path Cost），那么优先级最高的交换机才能被定为指定桥。

根路径开销（Root Path Cost）：从根到达一个桥的成本开销成为该桥的根路径开销。一台交换机的根路径开销的计算方法是将从根桥到达此网桥通路中沿途的端口路径开销数字相加。

桥的优先级（Bridge Priority）：是一个用户可以设定的参数，设定的值越小，优先级越高。

交换机具有较高的优先级，才能成为根桥。

根端口（Root Port）：每台交换机都有一个根端口，这个端口到根桥的开销路径最低。一旦多个端口具有相同的到根桥的路径开销，那么具有最低的端口标志级别的端口才能成为根端口。

指定端口（TPESignated Port）：将网段连接到其指定桥的单一非阻塞端口。

端口优先级（Port Priority）：数值越小，端口的优先级就越高，具有较高优先级的端口，才可能成为根端口。

路径开销（Path Cost）：这是一个可变的参数，它将随着生成树的设定值的变化而变化。依据 STA 的默认参数值，每个 1000Mbps 网段有一个指定的路径开销值为 4, 100Mbps 网段的路径开销为 19, 10Mbps 网段的路径开销值为 100。

5.5.2 生成树参数

用户可以根据需要修改生成树的参数，但建议最好使用出厂时的默认值设置。除非确实需要对出厂默认值进行变动时，再去改动默认值。用户可以改动的生成树参数有以下几个：

桥优先级（Bridge Priority）：数值范围从“0”到“65535”，0 的优先级最高。

呼叫时间（Bridge Hello Time）：数值范围从“1”秒到“10”秒，是指根桥向所有交换机发出 BPDU 数据单元包时的时间间隔，以告知其它交换机它是根桥。如果你的交换机还未是根桥时为其设置了呼叫时间，一旦你的交换机成为根桥，该呼叫时间就会派上用处。



注意：呼叫时间不能大于桥的老化时间，否则将出现错误信息。

最大的桥老化时间（Bridge Max.Age）：数值范围从“6”秒到“40”秒。如果在超出最大老化时间后，还没有收到根桥发出的 BPDU 数据包，那么在允许的情况下你的交换机将充当根桥向其它所有的交换机发送 BPDU 数据包。如果该交换机确实具有最小的桥标志级数，那么它将随之成为根桥。

桥转发时延（Bridge Forward Delay）：数值范围从“4”秒到“30”秒，是指交换机的端口从阻塞状态变为转发状态所用的监听时间。

端口优先级（Port Priority）：数值范围从“0”到“255”，数值越小，该端口就越可能成为根端口。

当用户欲变动生成树参数时，请一定记住下述公式：

最大的桥老化时间 $\leq 2 \times (\text{桥转发时延} - 1 \text{ 秒})$

即：Max.Age $\leq 2 \times (\text{Forward Delay} - 1)$

最大的桥老化时间 $\geq 2 \times (\text{呼叫时间} + 1 \text{ 秒})$

即：Max.Age $\geq 2 \times (\text{Hello Time} + 1)$

生成树参数	设置值	效果	备注
桥优先级 (Bridge Priority)	数值越小, 优先级越高	增加成为根桥的机会	如果交换机用于大型的工作组级的网络中, 那么, 尽量避免使用。
呼叫时间 (Hello Time)	1 – 10 秒	如果不是根桥, 那么, 没有任何影响。	不要大于最大老化时间 (Max. Age Time)。
最大老化时间 (Max. Age Time)	6 – 40 秒	如果没有收到 BPDU 数据包, 那么, 竞争成为根桥。	尽量不要选用较小的数值, 以免不断不必要地重设根桥。
转发时延 (Forward Delay)	4 – 30 秒	数值越高, 时延越长。	$\text{Max. Age} \bullet 2 \times (\text{Forward Delay} - 1)$ $\text{Max. Age} \bullet 2 \times (\text{Hello Time} + 1)$
端口级生成树参数 (Port Level STA parameters)			
Enable / Disable	Enable / Disable	Enable / disable	将某个端口设置为 Disable, 以隔离故障或者出于安全的目的。
端口优先级 (Port Priority)	数值越小, 优先级越高。	增加成为根端口的可能性。	

表格 5-1 生成树端口状态

5.5.3 创建STP拓扑结构

为了达到稳定的网络拓扑, 生成树将用到下述信息:

- 唯一的交换机标识符 (unique switch identifier)
- 交换机上的每个端口到根端口的路径开销 (path cost)
- 端口标识符 (port identifier)

生成树协议在交换机间进行通信时使用的是 BPDU (Bridge Protocol Data Units)。每个 BPDU 中包含如下信息:

当前根交换机 (root switch) 的唯一标识符。

从发送端口 (transmitting port) 到根 (root) 的路径开销 (path cost)。

发送端口 (transmitting port) 的端口标识符 (port identifier)。

交换机通过发送 BPDU 来进行通信并构建生成树拓扑, 连接到 LAN 的所有交换机都将接收 BPDU。交换机并不直接转发 BPDU, 但是接收 BPDU 的交换机会计算 BPDU, 如果网络拓扑发生改变, 就会发出一个 BPDU。

利用 BPDU 进行的交换机间的通信将导致如下结果:

一台交换机被选为根交换机 (root switch)

- 为每台交换机计算到根交换机最短的距离（shortest distance）
- 选出指定交换机（TPESignated switch），该交换机是最靠近根交换机（root switch）的交换机，数据包将通过该交换机转发给根交换机。
- 选出每台交换机上的一个端口，该端口是该交换机到根交换机的最佳路径。
- 选出生成树内的所有端口。

如果所有启动生成树协议的交换机都使用缺省的设置值，那么，具有最小 MAC 地址的交换机将成为根交换机（root switch）。通过提高交换机的优先级（数值越小），生成树协议可以将其强制选定为根交换机。

当生成树协议使用缺省参数值时，源站点和目的站点之间的路径未必是最理想的。例如，一个到某个端口的高速率的连接可能使得根端口发生改变，因其数值优于了当前的根端口。因为生成树追求的目标就是根端口应具有最快的连接。

5.5.4 STP端口状态

BPDU 在网络上传输是需要时间的，这种传播时延能导致拓扑改变，一个端口的状态从阻塞状态变为转发状态，从而产生短暂的环路。这样，其他端口在开始转发数据包之前，必须等待新的网络拓扑信息。转发时延（forward delay timer）被用于网络拓扑发生变化时，用以稳定网络拓扑。另外，STP 定义了一系列的状态，以确保网络拓扑发生变化后能够建立起新的稳定的网络拓扑。

交换机上的端口在启动 **STP** 协议后，存在的五种状态：

- 阻塞（Blocking） – 该端口被阻塞，不可以转发或接收数据包。
- 监听（Listening） – 该端口正在等待接收 BPDU 数据包，BPDU 可能告知该端口重新回到阻塞状态。
- 学习（Learning） – 该端口正在向其转发数据库中添加地址，但是，并不转发数据包。
- 转发（Forwarding） – 该端口正在转发数据包。
- 失效（Disabled） – 该端口只是相应网管消息，并且必须先转到阻塞状态。

端口可以转换的状态：

- 从初始化（交换机启动）到阻塞状态（blocking）
- 从阻塞状态（ blocking ）到监听（ listening ）或失效状态（disabled）
- 从监听状态（ listening ）到监听（ learning ）或失效状态（disabled）
- 从监听状态（listening）到转发（forwarding）或失效状态（disabled）
- 从转发状态（forwarding 到失效状态（disabled）
- 从失效状态（disabled）到阻塞状态（blocking）

当启动STP 后，网络上的每台交换机上的每个端口都将经历阻塞状态，然后，转换为监听状态或学习状态。如果STP 设置正确，那么，每个端口都将稳定地工作在转发或阻塞

状态。

任何数据包（除了BPDU 数据包之外）都不会被转发或接收，直至端口进入转发状态。

5.5.5 生成树举例

在一个环路中有三个桥（或三台交换机），如图5-1 所示。在此例中，如果不使用生成树技术，你可以预见到可能发生的一些网络故障。例如，如果桥A 向桥B 发出一个广播包，那么，桥B 将把此数据包广播给桥C，而桥C 又会将此数据包广播回给桥A。随后会一直将如此反复，广播包将会在这个环路中被循环往复地传递，从而导致严重的网络故障。

为了避免网络环路的发生，可以如图5-2 所示采用生成树（STP）来解决。生成树将阻断桥B 与桥C 之间的连接，以打破环路的形成。生成树算法将根据计算出来的各桥和端口之间的数值，来决定断开哪一条连接。现在，如果桥A 向桥C 发出一个广播包，那么，桥C 将在端口2处将此数据包丢弃，那么此广播将结束。

生成树的算法较复杂，所以，建议尽量不要改动其出厂默认设置值。生成树将自动任命根桥/根端口，并避免环路的形成。

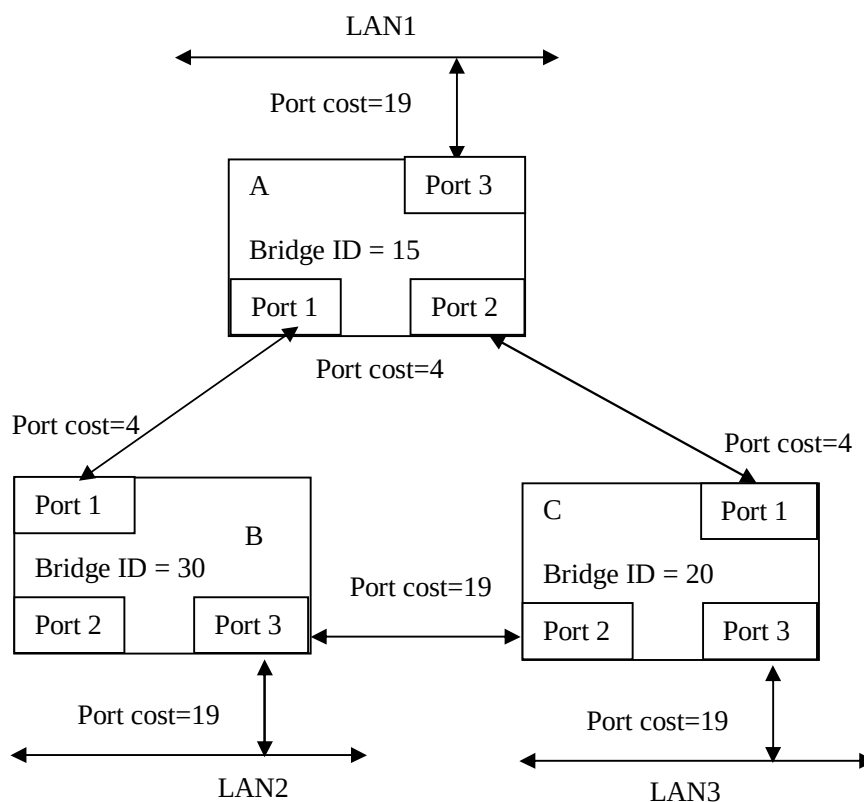


图 5-1 应用 STP 之前

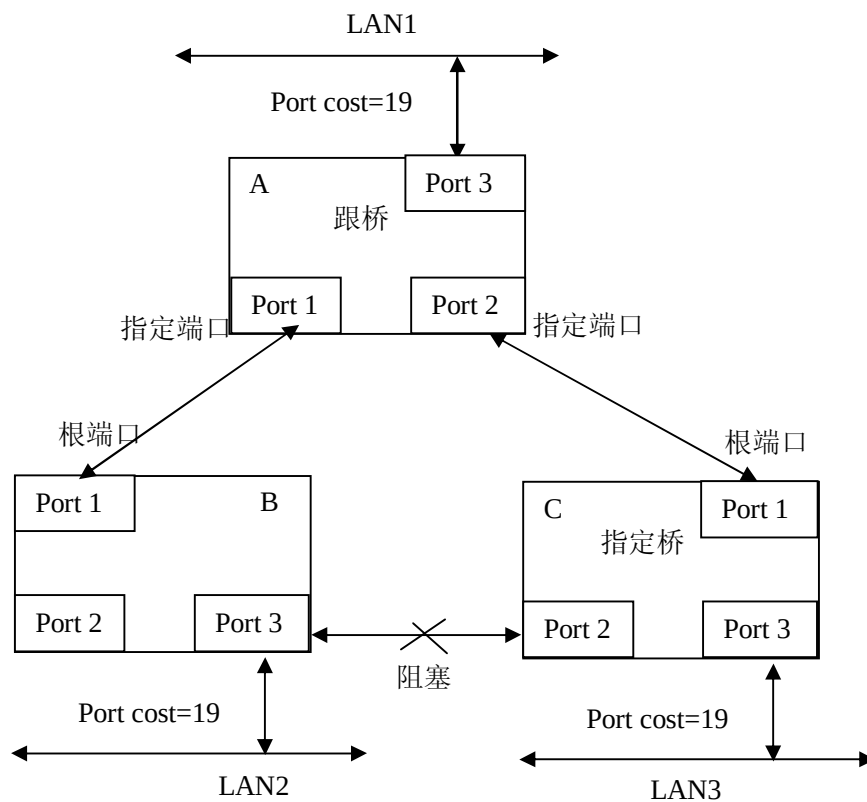


图 5-2 应用 STP 之后

5.6 端口聚合(Port Aggregation)

端口聚集通常被用于将多个端口聚集在一起，从而形成一个高带宽的数据传输通道。交换机将把端口聚集内的所有端口看作一个端口。在组成端口聚集的端口中，将有一个端口被指定为主端口（master port）。

由于干路中的所有成员需以相同的方式工作，所以，所有对主端口（master port）进行的设置，都将被同样作用到所有成员端口上。这样，当你需要对端口聚集中的端口进行设置时，可以仅对主端口进行设置即可。

UFS-2400NW 交换机上可以最多设置 7 个端口聚集组。

交换机将把端口聚集组中的所有端口看作一个端口，这样，聚集端口组将不会被生成树（STP）阻断。

5.7 虚拟局域网VLAN

虚拟局域网（Virtual Local Area Network，简写VLAN）是一种逻辑上的网络拓扑设置，而不是物理上的网络设计。VLAN 可以将网络逻辑地分割成数个不同的广播域，这样，数据包只能在VLAN 内进行转发。较有代表性的说明就是一个VLAN 就类似一个子网

(subnet)。VLAN 可以通过有效分割（保存带宽）的方式，提高网络的整体性能，并且可以提高数据传输的安全性。

VLAN 是将一些网络节点逻辑地组合在一起，而不是将其物理位置集中在一起。在一个 VLAN 中的网络节点可以随时相互通信，无论它们当时处在网络上的物理位置在何处。逻辑上来说，一个 VLAN 等于一个广播域，因为广播数据包只在 VLAN 内传播，不会传播到 VLAN 之外。

UFS-2400NW 支持 802.1Q VLAN 和 Port-Based VLAN。二者不能共存。

5.7.1 802.1Q VLAN

5.7.1.1 802.1Q VLAN 概念

UFS-2400NW 支持 IEEE 802.1Q VLAN，该 VLAN 涉及到以下概念：

- 加标记 (**Tagging**) - 将 802.1Q VLAN 信息添加到数据包的包头 (header) 中的动作。
- 去标记 (**Untagging**) - 将 802.1Q VLAN 信息从数据包的包头 (header) 中去掉的动作。
- 入端口 (**Ingress port**) - 交换机上的端口，数据包从该端口进入交换机，在此必须判断其 VLAN 属性。
- 出端口 (**Egress port**) - 交换机上的端口，数据包从该端口流出交换机，传送到其他交换机或网络节点站，在此必须确定数据包的标记 (tag) 属性。

VLAN 允许将网络分成数个网段，以减小广播域的范围。所有数据包（包括从未知源地址来的广播包、组播包和点播包）都只能在本地 VLAN 中进行传送。

VLAN 还可以为你的网络提供一定安全性。IEEE 802.1Q VLAN 只能在其 VLAN 成员端口范围内传送数据包。

任何一个端口都可以被设置 *tagging* 或 *untagging*。IEEE 802.1Q VLAN 的 *untagging* 特性使得无法识别 VLAN 标记 (tag) 信息的交换机也能与 UFS-2400NW 在一起工作。而 *tagging* 特性可以使 VLAN 信息在整个网络中传递。

IEEE 802.1Q VLAN 的主要特征如下：

- 通过过滤 (filtering) 分派数据包 (packet) 到 VLAN。
- 假设存在一个全局生成树 (a single global spanning tree)。
- 采用明确的一级 (one-level tagging) 加标记策略 (tagging scheme)

5.7.1.2 802.1Q VLAN 转发

- 进入规则 (Ingress rules) - 属于一个 VLAN 的接收到的数据帧 (received frame) 的分类规则。
- 端口间的转发规则 (Forwarding rules between ports) - 确定是过滤数据包还是转发数据包。

- 发出规则（Egress rules） – 确定数据包是加标记传送，还是去标记传送。

802.1Q Packet Forwarding

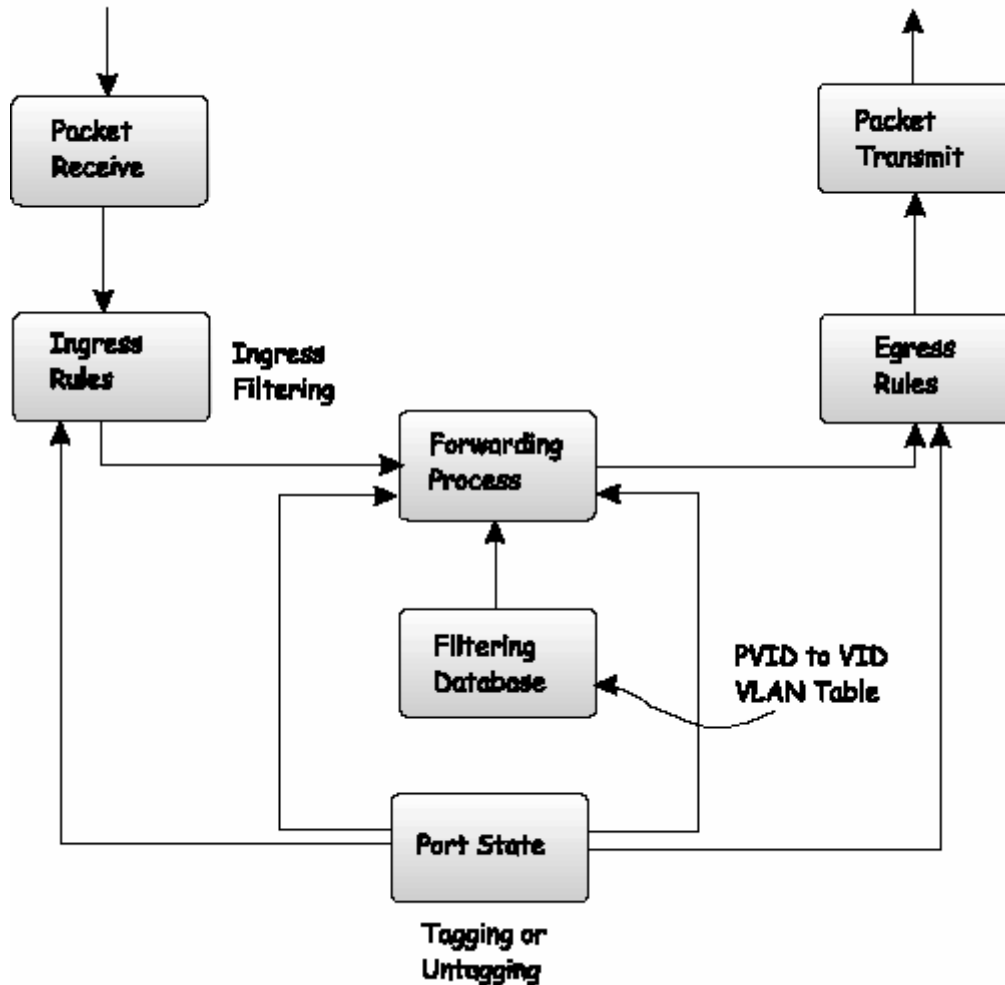


图 5—3 IEEE 802.1Q 数据包转发

5.7.1.3 802.1Q VLAN Tag

图5-4 示意出了802.1Q VLAN 标记(tag)的原理。在源MAC 地址的后面， 将插入4 个字节（octet） 的标记（tag）。当数据包的EtherType 字段为0x8100 时， 就表示数据包中携带有IEEE802.1Q/802.1p 标记（tag）。在标记（tag）中除了包含上述2 个字节（octet）之外， 还有3 个比特（bit）的优先级信息、1 个比特的CFI信息（Canonical Format Identifier， 用于压缩Token Ring 数据包， 以使其可以在以太网主干内传输）， 及12 比特的VLAN ID (VID)。3 个比特的优先级信息为802.1p 准备的， 而VID 是VLAN 的标识符（identifier）， 是为802.1Q 准备的， 因为VID 长度有12 个比特， 所以， 可以设置4094 个VLAN。

将标记（tag）插入到数据包的包头内后， 数据包将增长4 个字节（octet）。原来数据包中包含的信息都将保持不变将标记（tag）插入到数据包的包头内后， 数据包将增长4 个

字节（octet）。原来数据包中包含的信息都将保持不变。

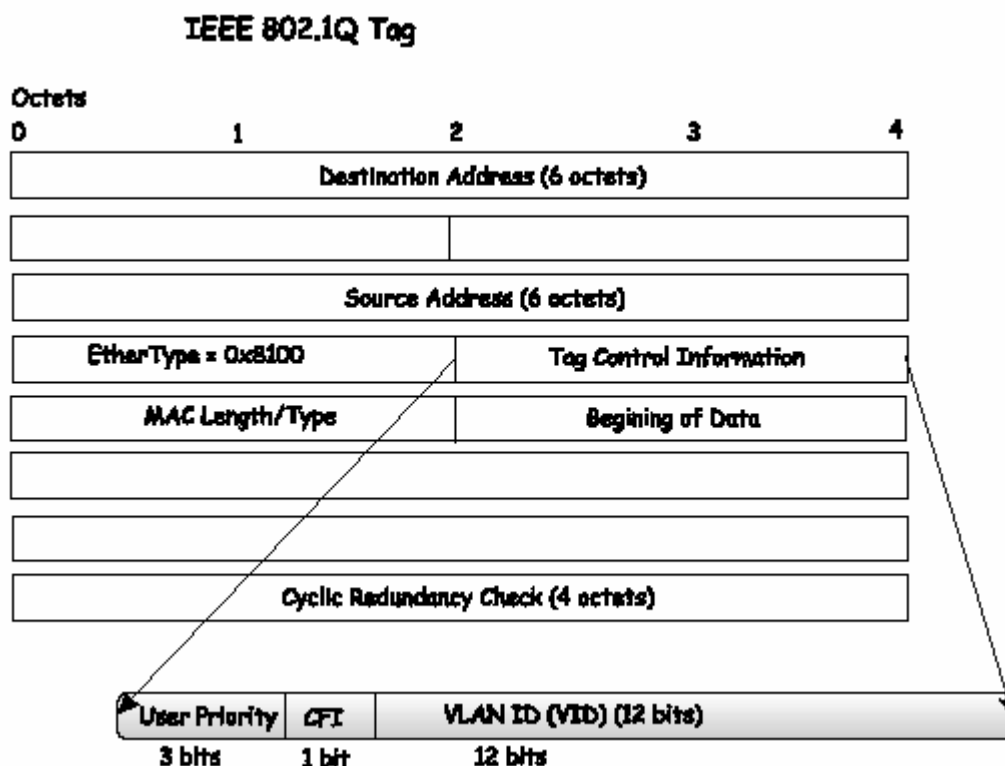


图 5-4 IEEE802.1Q 标记

EtherType 和 VLAN ID 插在源 MAC 地址（MAC source address）的后面，但是，位于原有的 EtherType/Length 或 Logical Link Control 之前。因现在数据包的长度比原来的略长，所以，CRC (Cyclic Redundancy Check) 必须重新计算。

5.7.1.4 端口 VID (Port Vlan ID)

被标记过的（即携带有 802.1Q VID 信息的）数据包将从一台具有 802.1Q 功能的设备传送到另一台具有 802.1Q 功能的设备，在传递期间 VLAN 信息保持不变。只要网络上的所有设备都支持 802.1Q，就可以使 802.1Q VLAN 可以延伸至整个网络。

但是，并不是网络上的所有设备都支持 802.1Q。这些不支持 802.1Q 的设备被称为是 *tag-unaware*，而支持 802.1Q 的设备称为是 *tagaware*。

在交换机内，不同的 PVID 意味着不同的 VLAN。



注意：在不存在路由器的情况下，两个 VLAN 之间是不能相互通信的。

交换机上的每个物理端口都有一个 PVID，同时 802.1Q 端口也会被赋予一个 PVID。如果交换机上未定义 VLAN，那么，所有端口都将属于一个缺省的 VLAN，其 PVID 都等于 1。这样，接收到的未加标记的（Untagged）数据包将被赋予接收端口的 PVID 值，是否转发的决定将依据该 PVID 进行确定。已携带有标记信息的（Tagged）数据包将根据其标记的 VID

信息来决定是否进行转发。已有标记的数据包也将被赋予一个PVID，但是，并不是根据此PVID 来决定是否转发该数据包，而是根据其VID 信息来进行判定。支持标记功能的交换机(Tag-aware switches) 必须具有能够建立交换机内各端口的PVID 与网络上的VID 之间关系表的能力。交换机将把数据包中的VID 与将传送该数据包的端口的VID 进行比较，如果两个VID 不同，那么，交换机将丢弃此数据包，不进行传送。由于针对未加标记的数据包存在着PVID，对加过标记的数据包存在着VID，所以，具有标记功能的交换机和不具有标记功能的交换机可以在同一个网络中共存。

交换机上的一个端口只可以有一个PVID，但是，可以有多个VID，（也就是说是一个端口可以属于多个VLAN）。交换机内有VLAN 表（VLAN table）可以用于存储VID 信息。
注: 802.1Q VLAN 需要创建一个包含所有端口的缺省VLAN，这将赋予所有端口的PVID = 1，并将PVID 对应出相应的VID。实际上，该缺省VLAN 是交换机的出厂设置之一，所有端口都将被初始化为PVID = 1。

因为网络上的有些设备不具有标记功能（tag-unaware），所以，在数据包被传送之前，具有标记功能的（tag-aware）设备上的端口必须做出决定将传送出去的数据包是否应加上一个标记（tag）。如果传送端口连接的是一台不支持标记功能的设备，那么，数据包就不必加上标记。反之，如果传送端口连接的是一台支持标记功能的设备，那么，数据包就必须加上标记。

5.7.1.5 加标记和去标记

802.1Q 交换机上的每个端口都将被设置为tagging 或untagging。具有tagging 功能的端口将把VID、优先级（priority）和其他VLAN 信息插入到所有流入和流出该端口的数据包的包头中。如果数据包事先已被标记过，那么，端口将不对数据包进行变更，这样，将保持其VLAN信息不变。这样，标记中的VLAN 信息将被其他802.1Q 设备所使用，以确定数据包是否应被转发。

具有untagging 功能的端口将把所有流入和流出该端口的数据包中的802.1Q tag 信息去掉。如果数据包中不含有802.1Q VLAN tag，那么，端口将不对数据包进行变更。这样，untagging 端口接收和转发的所有数据包中都将不带有802.1Q VLAN 信息。



注意: PVID 是仅限于交换机内部使用的。Untagging 功能是用将数据包从具有802.1Q功能的网络设备传递到不具有802.1Q 功能的网络设备的。

5.7.1.6 入过滤（Ingress Filtering）

入端口（ingress port）是交换机上的这样一个端口——数据包从该端口流入交换机，并且必须在该端口确定其VLAN 属性。如果端口的入站过滤（ingress filtering）被设置为生效（enabled），那么，交换机将检查数据包包头中的VLAN 信息（如果存在的话），并决定

是否转发该数据包。

如果数据包中包含VLAN 信息（即被加过标记），那么，入端口首先判定入端口本身是否是标记VLAN 的成员端口。如果不是，那么，该数据包将被丢弃，不进行传送。如果是成员端口，那么，交换机将进一步判定目的端口是否是标记VLAN 的成员端口。如果不是，那么，该数据包也将被丢弃；反之，该数据包将被转发到目的端口。

如果数据包中不包含VLAN 信息（即未被加过标记），那么，入端口将用其PVID 作为数据包的VID 为数据包加上标记（如果该端口是tagging port）。交换机随后判断目的端口是否与入端口属于同一个VLAN（即具有相同的VID），如果不是，那么，该数据包将被丢弃，不进行传送。反之，该数据包将被转发到目的端口。

这就是入站过滤（*ingress filtering*）。在入端口处就丢弃掉那些不在同一个VLAN 中的数据包，可以尽可能地保存带宽，减少后续的目的端口处理数据包的工作量。

5.7.2 Port-Based VLAN

5.7.2.1 Port-Based VLAN概念

基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法。这种划分 VLAN 的方法是根据以太网交换机的端口来划分，这实际上是某些交换端口的集合，用户只需管理和配置交换端口，而不用关心交换端口连接着什么设备。

5.7.2.2 Port-Based VLAN转发

基于端口的 VLAN 不关心交换端口连接着什么设备，也不关心收到的报文是 Tagged 或者是 Untagged。不同于 802.1Q VLAN，基于端口的 VLAN 不会对报文加上标记或者是去掉标记。

基于端口的 VLAN 是通过一个转发矩阵来实现转发控制的。这个矩阵的列是每个端口，行则是每个端口对应得转发列表。这样，报文到了一个端口，会先查这个端口的转发列表，再决定向那些端口转发。

所以，对于带标记的报文，转发之后标记不会改变；对于不带标记的报文，转发之后也不会带标记。

5.7.2.3 Port-Based VLAN使用

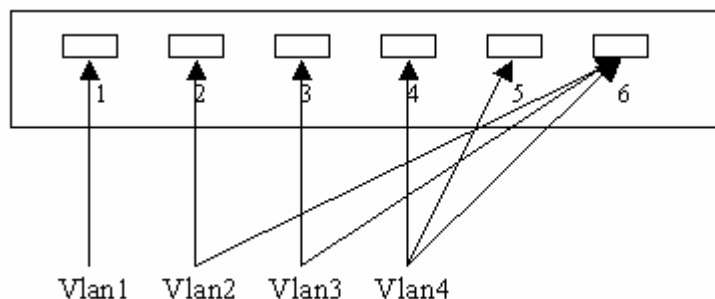


图 5—5 Port vlan 划分

如上图设置基于端口的 VLAN。

Port-Based VLAN 1: 包括成员端口 1, 该端口除了与交换机外, 不能和其它端口通讯

Port-Based VLAN 2: 包括成员端口 2 和 6, 端口 2 和 6 之间可以互相通讯

Port-Based VLAN 3: 包括成员端口 3 和 6, 端口 3 和 6 之间可以互相通讯

Port-Based VLAN 4: 包括成员端口 4, 5 和 6, 端口 4, 5 和 6 之间可以互相通讯

基于端口的 VLAN 划分有利于设置上连口, 且可以控制下连端口之间的互相通讯。如上图配置, 假如端口 6 是上连口, 则端口 2, 3, 4 和 5 都可以通过端口 6 上连, 而端口 2 和 3 之间互相不能访问; 端口 4 和 5 之间可以互相访问。



注意:

- 1) 在 Port-Based VLAN 下创建一个已经存在 VLAN 的成员端口的子集是没意义的, 端口转发仍会按照原 VLAN 转发;
- 2) 不属于任何 VLAN 的端口可以互相通讯。

5.8 广播风暴 (Broadcast) 的管理

广播 (Broadcast) 是指将数据包发送给局域网内所有连接的设备。广播对任何一个网络来说, 都是至关重要的。但是, 广播经常在网络中引起问题, 有时甚至导致整个网络崩溃。因此, 交换机必须提供多种功能用于管理网络中的广播数据包。

5.8.1 广播风暴 (Broadcast Storm)

广播风暴 (Broadcast storm) 是当今网络中常见的问题。通常, 当广播数据包在网络中大量传送, 或者在网络中循环传送时, 会引起网络性能明显地下降, 极限情况时将使网络整体瘫痪。引起广播风暴的原因有: 存在着网络环路、故障网卡、不良的线路连接, 或者一些产生广播的应用程序或协议等。

广播风暴的问题早就引起了网络管理员的关注, 并已经在使用传统的路由器来抑制广播风暴的出现。即使可能会在局部地区发生一些广播风暴, 也会竭尽全力将其限制在一定的区域内。但是, 借助 VLAN 的特点, 现在交换机拥有比路由器更好的抑制广播风暴的能力, 而且, 许多交换机还在每个端口内置了侦测和过滤广播包的功能, 以进一步控制广播风暴的发生。

5.8.2 分割广播域 (Segmenting Broadcast Domains)

VLAN 可以被用于分割广播域 (broadcast domain)。由于交换机在转发数据包时, 范围仅限于在属于同一个 VLAN 的成员间进行数据包传递, 这样, 网络的其他部分可以被有效地保护起来, 免于频繁地受广播风暴的影响。因此, 广播域被分割得越小, 广播风暴的影响也就越小。

5.8.3 减少广播风暴 (Eliminating Broadcast Storms)

一旦端口上的广播风暴发生的次数超出预先限定的上升阈值 (*rising threshold*) 时, 将

会丢弃广播包。

6. 使用console接口配置交换机

UFS-2400NW 交换机提供一个控制台管理界面（console management interface），使你可以通过其对交换机进行设置和控制管理。你可以利用一个终端设备（仿真终端也可以），或者利用TCP/IP 的TELNET功能，登录到控制台界面，以进行许多最基本的网络管理操作。本章内容就是向您介绍如何通过控制台界面来访问交换机，更改交换机的设置，以及监视交换机的运行状态的。

6.1 概括介绍

1. 确定网络如何最好的分段。这将在一个已有二层交换机的网络内运用 VLAN 功能。
2. 确定哪些网络资源必须在网段中共享。共享资源可能直接连接在二层交换机上，如果需要，应该确定静态路由到每个共享资源上。
3. 确定每个子网如何与广域网或 Internet 相连接。另外，静态路由应该确定相应的默认网关。
4. 确定安全设计。一些子网需要更多的安全性或应同其它子网进行隔离。这将使用到 IP 或 MAC 地址过滤。同样，一个或更多的 VLAN 在二层交换机上也可以不配置一个 IP 子网，在某些案例中，VLAN 的功能将类似一个二层 VLAN，另外将需要一个外部的路由器来连接整个网络。
5. 策略设计。一些子网将需要大量的组播带宽，策略就是一种机制，如在一个网络设备上改变正常的包转发方式，能够智能的分配带宽给急需的应用如视频、音频和大量数据等。
6. 确定冗余设计。计划冗余连接和网络重要资源路由能在一且链路或设备出现故障时产生挽救措施。UFS-2400NW 的 SpanningTree 功能可以用于冗余链路连接。

6.2 如何登录控制台界面

通过 Console 口进行管理时，必须用一根 RS-232C 电缆将一台兼容 VT-100 的终端或者一台运行终端仿真程序（如 Windows95/98/2000 操作系统中的超级终端）的 PC 机，连接到 UFS-2400NW 交换机前面板上的“Console”接口，然后，在终端上采用如下参数，就可以登录到控制台界面。

所需的设置参数如下：

Baud rate:	9,600
Data width:	8 bits
Parity:	none
Stop bits:	1

Flow Control : none

典型的和 Console 口的连接方法如下图所示：



图 6-1 与 Console 口的连接方法举例

在 Windows95/98/2000 下，执行“超级终端”的“Hypertrm.exe”，进行新建连接。在图标一栏中，选择电话图标->在“连接使用中”选择“直接连接到串口 1”或其他串口 -> 按“确认”键盘->在“端口设置”中选择波特率为“9600”、数据位为“8”、奇偶校验“无”、停止位为“1”、流量控制为“无”。进入“超级终端”界面后，按“ENTER”键，就可以进入控制台界面了。

此外，用户也可以利用 Telnet 来登录控制界面。一旦一个交换机已经被赋予一个 IP 地址后，你就可以利用 Telnet 命令（VT-100 兼容终端）通过网络来访问和控制交换机。实际上，用这两种方式登录到控制台界面后，所看到的和所操作的是一样的。但用户用 Telnet 登录控制台界面有两个前提：

前提一是在交换机的控制管理中必须有超级用户的存在，用户的优先级为 15 的用户为超级用户。第一次登录控制台界面添加用户和设置用户权限时必须依靠 Console 口进行登录。

前提二是必须为该交换机配置一个可行的 IP 地址。

6.2.1 配置超级用户

当用户第一次用 Console 口登录控制台界面时显示如图 6-2 所示：

该设备出厂时缺省用户名称是 **admin**，密码是 **password**。用户敲入相应的用户名和密码后就可以对交换机进行管理控制，即在“switch”的提示符下键入相应命令。



注意：登录交换机的口令是区分大小写的，“S”与“s”不同。

在这里只给出如何通过 Console 口进行添加用户和设置用户权限，具体操作如图 5-3 所示。

1. 用户在 Switch#下敲入“configure”命令。
2. 在 Switch(config)#下敲入“user”命令，会显示出两个对用户操作的命令：添加和删除；
3. 用户继续敲入“useradd tp”，则添加了一个用户名为“tp”的用户；
4. 用户在“password”提示下设置密码，在“enteragain”下确认密码；
5. 用户在“accesslevel”的提示下设置用户的权限，用户的权限有两个级别：管理员级别

(Administrator) (也叫超级用户)和普通用户级别 (Normal User), 将权限设置为 15 即表示该用户拥有管理员级别。

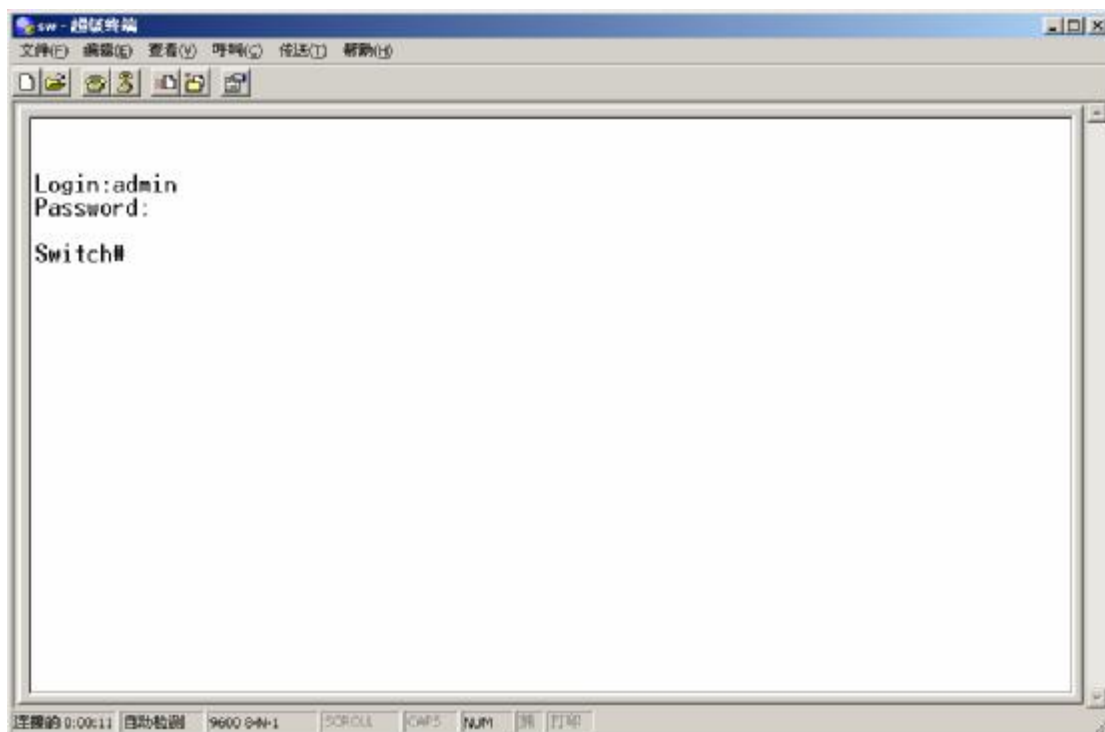


图 6-2 用 CONSOLE 口登录的初始界面

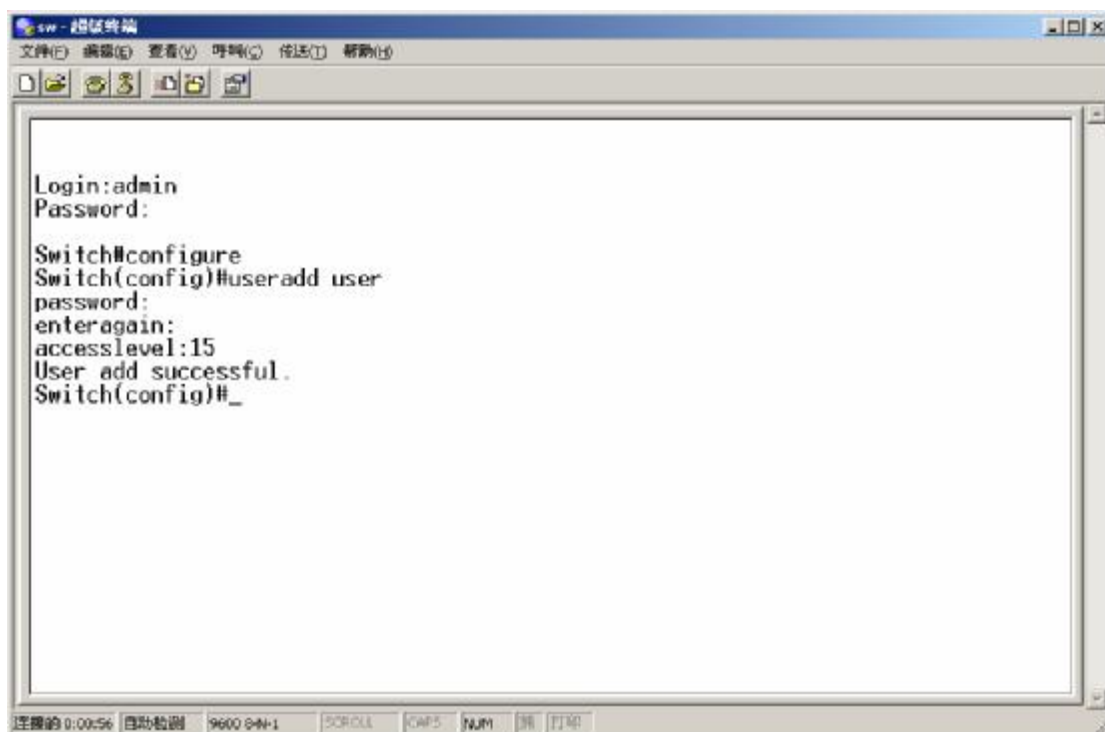


图 6-3 添加用户的界面

管理员级别的权限比普通用户级别的权限高，有一些菜单普通用户级别的用户就不允许访问或更改设置，普通用户也不能通过 Telnet 对控制台界面进行访问和控制。下表是关于普通用户权限和管理员权限的详细说明：

菜单 (menu)	管理员级 (Administrator)	普通用户级 (Normal User)
	权限	
更改配置	Read/Write	Yes, read only.
网络监测	Read/Write	Yes, read only.
一致性字符串和陷阱的设置 (Community Strings and Trap Stations)	Read/Write	Yes, read only.
升级固件 (Firmware) 和配置文件 (Configuration Files)	Read/Write	Yes, read only.
帐户管理 (User Accounts Management)		
创建/更改帐户	Read/Write	No
查看/删除帐户	Read/Write	No
系统利用	Read/Write	Yes, (Ping Test); 其余的 read only
恢复出厂默认设置	Read/Write	No
重启系统	Read/Write	No



注意：如果要使用 telnet 来进行远程管理交换机，首先要为交换机分配一个用于远程登录的用户，这样用户应当具有超级用户的权限。

6.2.2 配置交换机IP地址

由于 UFS-2400NW 不提供带外管理接口，在系统启动后必须通过 Console 口为交换机配置一个带内 IP 地址。有了该 IP 地址后，通过 Telnet 登录控制台界面或通过 Web 登录 Web 网络管理界面才能成为可能。

系统启动时配置了缺省的 VLAN 1，因为为交换机配置 IP 地址是第一步。

1. 用户在 Switch# 下敲入 "configure" 命令。
2. 在 Switch(config)# 下敲入 ip ?
3. 根据提示的帮助信息设定 ip, 一直到敲入 ? 后出现 <cr> 为止，这时敲回车设置命令完成。缺省的 vid 为 1，vid 的配置在[配置 vlan 命令](#)中有详细说明。

具体流程如图 6-4 所示：

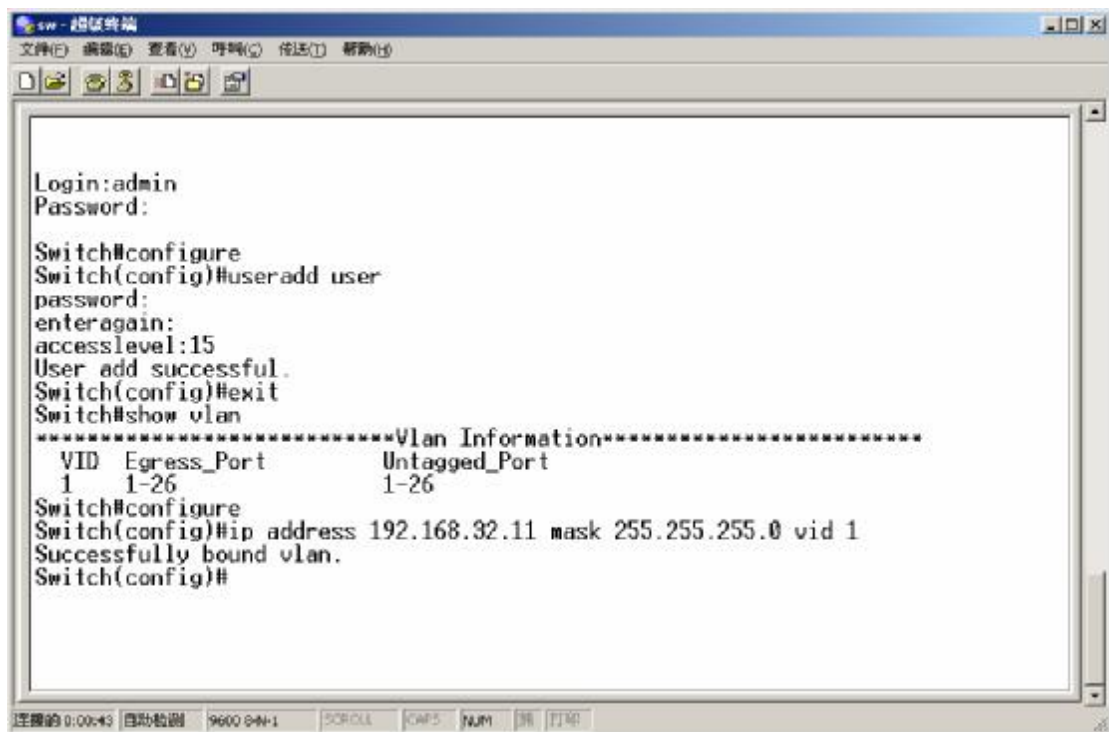


图 6-4 配置 IP 地址的界面

图中交换机的 IP 地址为 192.168.32.11，子网掩码为 255.255.255.0，vid 号为 1。此时只能设置一个交换机 IP 地址。你可以退出用 show ip address 来显示设置的结果。

下面就以 Telnet 命令登录控制台界面为例，详细介绍如何使用各种 CLI 命令。

6.3 CLI 命令使用说明

6.3.1 一些特殊键的使用

console 口支持下列的特殊键：

Tab 键：输入命令的前一部分后，键入 Tab 后可以显示出的整的命令。例如：

键入 sh 后按 Tab 键，则显示出 show 命令。

CTRL-n：向下翻滚命令的历史记录；

CTRL-p：向上翻滚命令的历史记录；

CTRL-b：把光标向左移动一格；

CTRL-f：把光标向右移动一格；

CTRL-d：删除光标上的一个字符；

CTRL-z：推出当前节点，等同于命令 exit；

向上方向键：向上翻滚命令的历史记录；

向下方向键：向下翻滚命令的历史记录；

当一屏幕显示不下时，可以分屏显示。当一屏幕显示不下时，会出现-more- 提示，这时空

格键使屏幕向上滚动一屏幕，回车键向上滚动一行。

6.3.2 语法帮助

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，表明命令输入完毕。按回车就可以执行所键入的命令。

【举例】

Switch#set po

在输入“set po”之后键入“?”，显示下面的内容：

port

提示完整的命令为 set port 。

如果是加入空格后再键入“?”，会显示下面的提示信息：

<String> <1-26/all> port list

提示下面的输入参数，在上面的例子中为端口列表或者选择全部的端口。

6.3.3 使用语法帮助补齐命令

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。

【举例】

Switch(config)#s

save spanning-tree

在上面的例子中，键入“s”后，使用“tab”键，因为有多条以“s”开头的命令，命令行会显示全部以“s”开头的命令。

如果在“s”后键入“p”，再使用“tab”键，这时候只检索到 spanning-tree 命令，系统会自动补齐。

Switch(config)#spanning-tree

6.3.4 命令帮助使用说明

在下面所有的命令行帮助信息中，对命令和参数进行了区分，在键入的例子中，用粗体字来表示命令，用一般字体表示参数。

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。

6.3.5 常用命令

6.3.5.1 help命令

用户使用 help 命令显示系统帮助信息。

【使用指南】 UFS-2400NW CLI 配置提供随时随地的在线帮助，用户可以随时键入“？”获取在线帮助。

【举例】

Switch#help

Help may be requested at any point in a command by entering a question mark '?'.

If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?').

Switch#

6.3.5.2 禁止命令disable

用户执行该命令设置当前用户的优先级为更低的优先级。

【命令格式】 disable <0-15>

【使用指南】该命令在根指示符下执行，降低当前用户权限为更低级别。目前情况下，级别 15 是管理员级别，取得该级别权限的用户，可以对交换机进行任何的操作，包括设置和设置信息的显示，以及对于用户的管理。低于 15 而高于 10 的级别可以使用“rcommand”命令，其它的设置命令都不可用。低于 10 的级别只能显示基本信息，不能进行任何的设置。如果要对交换机进行设置，需要使用“enable + 级别”命令来提高自己的级别。具体的使用方法参照下面关于 enable 命令的说明。

【参数说明】<0-15>为优先级编号，范围为 0-15，为可选参数，默认为 0。

【举例】

Switch# disable 0

Switch>

6.3.5.3 允许命令enable

用户执行该命令设置当前用户的优先级为更高优先级。

【命令格式】 enable <0-15>

【使用指南】该命令在根指示符下执行，升高当前用户权限为更高级别。如果设置优先级为

15，则可以变为管理员级用户，可以重新登录该 CLI 配置界面。

【参数说明】<0-15>为优先级编号，范围为 0-15，为可选参数，默认为 15。

【举例】

```
Switch# enable 15
```

```
Login:
```

```
Password:
```

```
Switch#
```

 注意：上述两个命令对于交换机默认的用户“admin”是不生效的，只有对添加的用户才生效。对于使用 telnet 来管理交换机的操作来说，必须要添加新的 15 级的用户，默认的超级用户是不能用于远程管理的。

6.3.5.4 arp 命令

用户执行该命令配置静态 ARP 表。ARP 表是一个三层地址对应表，它建立了一个 IP 地址和二层 MAC 地址的对应关系，如果表项是通过动态学习添加的，那么这个地址在一段时间内如果没有被应用就会老化掉；反之，如果是使用 ARP 命令添加的，这个表项永远不会被老化。

【命令格式】1. arp ip <A.B.C.D> mac-addr < HH:HH:HH:HH:HH:HH >

2. no arp ip <A.B.C.D>

3. no arp all

【使用指南】命令 1 添加一个 ARP 表项；

命令 2 删除一个 ARP 表项。

命令 3 删除所有的 ARP 表项。

【参数说明】<A.B.C.D>为点分十进制方式的 IP 地址。< HH:HH:HH:HH:HH:HH >表示 MAC 地址。

【举例】

```
Switch(config)#arp ip 192.168.32.100 mac-addr 00:20:34:e2:56:f4
```

```
Successfully add arp entry.
```

```
Switch(config)#
```

```
Switch(config)#no arp ip 192.168.32.100
```

```
Successfully delete arp entry.
```

```
Switch(config)#
```

```
Switch(config)#no arp all
```

```
Successfully clear all arp entries.
```

```
Switch(config)#
```

 注意：因为添加的地址用于直接和交换机通讯，所以要求添加的三层地址必须是交换机

直接可达的，也就是说这个 IP 地址必须和交换机中已经设定的 ip 地址在同一个网段。

6.3.5.5 **hostname**命令

用户使用 hostname 命令配置设备名称。

【命令格式】hostname <name>

【参数说明】<name> 为最大长度为 32 的字符串，用于表示设备名称。

【举例】

```
Switch<config>#hostname test-switch
Host name set to test-switch

Switch#show hostname
Host name is: test_switch

Switch#
```

6.3.5.6 保存配置命令**save**

用户执行该命令保存当前的所有配置。

【命令格式】save

【使用指南】该命令在 configure 配置路径下有效，无参数。

【举例】

```
Switch<config>#save
Save current configure to NVM is processing,Please wait...#####
#####OK.

Switch(config)#
```

6.3.5.7 复位命令**reset**

用户执行该命令用于重新启动设备。

【命令格式】reset

【使用指南】该命令必须在 configure 配置路径下才有效，用于系统热启动。

【举例】

```
Switch(config)#reset
Device resetted. Please connect again.
```

6.3.5.8 回复配置命令**resettodefaults**

用户执行该命令时，设备重新启动并且恢复到出厂时的配置。

【命令格式】resettodefaults

【使用指南】该命令必须在 configure 配置路径下才有效，用于系统热启动，并恢复出厂设置。

【举例】

```
Switch<config>#resettodefaults
```

Device reset to default. Please connect again.

6.3.5.9 终端设置

6.3.5.9.1 baud rate 命令

该命令用于设置 console 口的波特率。

【命令格式】 1. baud rate <2400|9600|19200|38400>

2. no baud

【使用指南】命令 1 设置 console 口波特率，命令 2 恢复 console 波特率的缺省值，缺省值为 38400。

【参数说明】<2400|9600|19200|38400>为要设定的 console 口波特率，取值为 2400，9600，19200，38400。

【举例】

```
Switch#configure
Switch(config)#terminal
Switch(con-term)# baud rate 9600
Baud rate is set to 9600
Switch(con-term)#no baud
```

6.3.5.9.2 length 命令

该命令用于设置 console 口的输出高度。

【命令格式】 1.length <20-40>

2.no length

【使用指南】命令 1 设置 console 口的输出高度，命令 2 恢复 console 输出高度的缺省值，缺省值为 25。

【参数说明】<20-40>为 console 口的高度值，取值范围为 20-40。

【举例】

```
Switch(con-term)#length 20
Terminal length is set to 20
Switch(con-term)#
Switch(con-term)#no length
Terminal length is set to 25
Switch(con-term)#
```

6.3.5.9.3 width 命令

该命令用于设置 console 口的输出宽度。

【命令格式】 1.width <60-80>

2.no width

【使用指南】 命令 1 设置 console 口的输出宽度，命令 2 恢复 console 输出宽度的缺省值，缺省值为 80。

【参数说明】 <60-80>为 console 口的宽度值，取值范围为 60-80。

【举例】

```
Switch(con-term)# width 70
```

```
Terminal width is set to 70
```

```
Switch(con-term)#
```

```
Switch(con-term)#no width
```

```
Terminal width is set to 80
```

```
Switch(con-term)#
```

可以用下面的命令显示端口设置的结果

```
Switch#show terminal
```

```
Terminal baud rate is 9600
```

```
Terminal width is 70
```

```
Terminal length is 20
```

```
Switch#
```

6.3.5.10 ping 命令

该命令等同于 Dos 下的 ping 命令。

【命令格式】 ping <A.B.C.D> [1-65535]

【参数说明】 <A.B.C.D>为点分十进制方式表示的目的 IP 地址；[1-65535]为 ping 报文的数目，该参数可选。

【举例】

```
Switch#ping 192.168.32.166 5
```

```
Sending 5, 56-byte ICMP Echos to 192.168.32.166, timeout is 5 seconds:
```

```
!!!!
```

```
5 packets received.
```

```
Switch#
```

6.3.5.11 配置 tftp server

用户在当前配置的提示符下键入“tftp ip <A.B.C.D>”，该命令用于配置 tftp server 的 IP 地址。

【命令格式】 tftp ip <A.B.C.D>

【使用指南】 tftp server 用于上传下载文件。

【参数说明】 <A.B.C.D>为 tftp server 的 IP 地址，以点分十进制表示。

【举例】

```
Switch(config)#tftp ip 10.1.1.8
Successfully set TFTP address.
Switch(config)#
```

6.3.5.12 download 命令

用户执行该命令进行软件的下载。使用前请先关闭防火墙。

【命令格式】 download filename <filename> <filetype>

【使用指南】 下载（更新）软件前，需要使用命令 tftp 配置 tftp server 的位置。



注意：要使用该命令，必须先配置交换机的一个 ip 地址。

【参数说明】 <filename>为要下载的文件名称，<filetype>为要下载的文件类型（这里支持 application，configuration 两种类型文件）

【举例】

```
Switch<config>#download filename switch.z application
Download file.Please wait#####OK.
```

6.3.5.13 upload 命令

用户执行该命令 upload 设备上运行的软件。使用前请先关闭防火墙。

【命令格式】 upload configfile <filename>

【使用指南】 下载（更新）软件前，需要使用命令 tftp 配置 tftp server 的位置。



注意：要使用该命令，必须先配置交换机的一个 ip 地址。

【参数说明】 <filename>为上传软件后软件的名称和位置（字符串形式）；

【举例】

```
Switch<config>#upload configfile "c:\switch\switch.cfg"
Switch<config>#
```

6.3.5.14 退出命令exit 、 Ctrl+z

从当前的节点退回到上一节点，如果当前是根结点，则退出当前会话。

【命令格式】 exit

【举例】

```
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

【命令格式】 Ctrl+z

【使用指南】 此命令直接从当前节点退到根节点

【举例】

```
Switch(config-if)#
```

```
Switch#
```

6.3.6 用户管理命令

6.3.6.1 添加用户命令

用户执行该命令进行添加用户操作。

【命令格式】 **useradd** <username>

【使用指南】用户输入“useradd”后，会执行“输入密码”、“确认新密码”、“访问级别”三步操作。为安全起见，这里输入的字符串都不回显。访问级别为 15 的是超级用户（管理员级别）。

【参数说明】<username>为用户名称，以字符串表达，可以输入的是 26 个英文字符的大小写或者数字的组合，不可以是其它字符或者不可显示的字符；访问级别的取值范围是 0—15。15 是最高级别。

【举例】

```
Switch<config>#useradd "user"
password:
enteragain:
accesslevel:15
User add successful
Switch<config>#
```

可以用下面的命令显示设置的结果。

```
Switch#show user
```

User name	Password	Access level	Property
user	user	15	0

```
Switch#
```



注意：如果要使一个低于 15 级别的新建用户可以登录到交换机，首先要保证已经建立了拥有 15 级权限的用户。如果只有默认的“admin”用户存在，不允许使用低于 15 级的用户登录交换机。

6.3.6.2 删除用户命令

用户执行该命令进行删除用户操作。

【命令格式】 **userdelete** <username>

【参数说明】<username>为用户名称，以“ ”字符串表达。

【举例】

```
Switch<config>#userdelete "user"
```

User delete successful

Switch<config>#

6.3.6.3 配置密码

用户执行该命令用于修改用户登录密码。

【命令格式】 password

【使用指南】用户输入“password”后，会执行“输入旧密码”、“输入新密码”、“确认新密码”三步操作。为安全起见，这里输入都不回显。

【举例】

```
Switch<config>#password
```

```
oldpassword:
```

```
newpassword:
```

```
enteragain:
```

```
Password change successful.
```

```
Switch<config>#
```

6.3.7 配置交换机端口命令

用户执行下述命令进行交换机物理端口的配置项。

【命令格式】 set port <portlist |all> +设置项

【使用指南】使用端口设置命令可以对交换机物理端口的一些属性进行设置，在上面的命令中包括了多个可能的设置项。

【参数说明】参数为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port ? <String>          <1-26/all> port list ...
```

6.3.7.1 端口禁用命令

用户执行该命令关闭指定的端口。使该端口不能进行正常的转发

【命令格式】 set port <1-26 |all> disable

【使用指南】<1-26 |all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port all disable
```

```
Successfully shutdown ports.
```

```
Switch#
```

6.3.7.2 端口使能命令

用户执行该命令使能指定的端口。

【命令格式】set port <1-26 |all> enable

【使用指南】<1-26 |all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port all enable
```

```
Successfully enable ports.
```

```
Switch#
```

6.3.7.3 端口速率、双工模式设置命令

用户执行该命令设置该物理端口速率的相关特性。

【命令格式】set port <1-26 |all> duplexspeed < autonegotiate|half-10|full-10|half-100|full-100>

【使用指南】对于端口速率和双工模式的配置和端口的自适应模式有关系。当交换机和另一台设备使用直通线相连时，用户改变相连端口的双工模式，导致该端口不能自动进行线序自识别，up-link 灯不再点亮。使用该命令将自适应模式禁止，则相连端口能够进行线序自识别，up-link 灯重新变亮。

【参数说明】<1-26 |all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。<autonegotiate|half-10|full-10|half-100|full-100>为指定端口速率，可以为 autonegotiate、half-10、full-10、half-100、full-100，分别代表端口自适应、半双工 10Mbps、全双工 10Mbps、半双工 100Mbps、全双工 100Mbps。对于本款交换机而言，1-24 端口支持 10/100M 自适应，所以这些端口的速率、双工模式的设置范围是 autonegotiate、half-10、full-10、half-100、full-100，对于端口 25-26，如果插入的模块是电口，参数的取值范围是上面的所有模式，如果是光口，只有 full-100 一种模式，进行其它的设置系统会提示错误。

【举例】

```
Switch#set port 20-24 duplexspeed full-100
```

```
Successfully set ports' duplex and speed.
```

```
Switch#
```

6.3.7.4 设定端口流量控制

6.3.7.4.1.1 打开端口流控

【命令格式】set port <1-26 |all> storm-weaken pause enable

【参数说明】<1-26 |all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port 9-10 storm-weaken pause enable
```

```
Successfully enable ports' pause.
```

Switch#

使用 show port storm-weaken 命令可以看到设置的结果。

Switch#show port storm-weaken

Port id	pause
1	disable
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable
9	disable
10	disable
11	disable
12	disable
13	disable
14	disable
15	disable
16	disable
17	disable
18	disable
19	disable
20	disable
21	disable
22	disable

-- More --

6.3.7.5 设置端口镜像命令

该命令集用于配置端口的镜像功能。系统支持多端口到一个端口的镜像，并可以分别设置镜像端口的发包和收包。

6.3.7.5.1 设置端口镜像命令

该命令用于设置指定端口为被镜像端口。

【命令格式】set mirror port <1-26>

【参数说明】<1-26>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-”

6”。

【举例】

```
Switch#set mirror port 3
```

```
set mirrored successful.
```

```
Switch#
```

6.3.7.5.2 选定监听端口命令

该命令用于设置端口镜像的监听端口，根据设定的监听模式，从该端口可以捕获被监听端口的报文。

【命令格式】 set mirror monitor <1-26>

【参数说明】 <1-26>为物理端口号，在 1—26 之间取值。

【举例】

```
Switch#set mirror monitor 2
```

```
Port mirror to port 2.
```

```
Switch#
```

6.3.7.5.3 设置端口镜像模式命令

该命令用于设置指定端口的镜像模式。

【命令格式】 set mirror mode <all|egress|ingress|none>

【参数说明】 <all|egress|ingress|none>为可选模式，all 表示镜像所有报文，egress 表示镜像出口报文，ingress 表示镜像入口报文，none 表示不镜像。

【举例】

```
Switch#set mirror mode egress
```

```
set mirror mode successful.
```

```
Switch#
```

6.3.7.5.4 显示端口镜像结果

可以使用 show port mirror 命令显示设置端口镜像的结果。

```
Switch#show port mirror
```

```
Mirror port:3.
```

```
MonitorPort:2.
```

```
Mirror mode: egress
```

```
Switch#
```

6.3.7.6 设置QOS命令

6.3.7.6.1 设置QOS命令

使用该命令改变端口的优先级，这个优先级包含在 vlan 的 tag 帧中。

控制优先级帧传输的基本规则如下：

- Ø 最高优先级队列中的帧最先发送。
- Ø 所有较高优先级队列为空时，再发送低优先级队列中底帧。

本设备具有 2 个优先级队列，当加上优先级底帧到达交换设备底时候，交换设备必须计算该帧属于那个优先级队列，它们之间有一个影射关系：

1	-->	0
2	-->	0
3	-->	0
4	-->	0
5	-->	1
6	-->	1
7	-->	1
8	-->	1

本设备支持 3 种优先级选择：high/low/802.1p。

high：不管该端口收到的报文 tag 帧中是什么优先级，一律按高优先级处理。

low：不管该端口收到的报文 tag 帧中是什么优先级，一律按低优先级处理。

802.1p：按照该端口收到的报文 tag 帧中的优先级处理。

【命令格式】set port <1-26|all> priority < high/low/802.1p >

【参数说明】<1-26|all>为交换机物理端口列表，输入的形式可以是“1—2”或者“1, 2, 4—6”，如果要设置全部的物理端口可以使用“all”参数项；< high/low/802.1p >为优先级的取值。

【举例】

```
Switch#set port 1-10 priority high
Successfully set 802.1p priority.
Switch#
```

6.3.7.6.2 显示QOS设置结果

可以使用 show port priority 命令来显示设置的结果。

```
Switch#show port priority
```

port	priority
1	802.1p
2	802.1p
3	802.1p
4	high
5	high
6	high
7	high
8	high
9	high
10	high
11	low
12	low
13	low
14	low
15	low
16	low
17	low
18	low
19	low
20	low
21	low
22	low
23	low
24	low
25	low
26	low

Switch#

6.3.7.7 设置广播风暴控制

该命令用于设置广播风暴控制，指定接收的广播帧的程度。

【命令格式】set broad-storm-control <off/tiny/low/medium>

【参数说明】<off/tiny/low/medium>为广播风暴控制的可选参数，选择其中一个，实现对应的广播风暴控制。

【举例】

```
Switch#set broad-storm-control low
set broadcast storm control successful.
Switch#
```

6.3.7.8 设置老化时间

该命令用于设置交换机 MAC 地址表的老化时间。

【命令格式】set agingtime <10-700>

【参数说明】Aging time 的设置范围从 10 到 700。



注意：请输入 3 的倍数，否则将设置最接近的 3 的倍数

【举例】

```
Switch#set agingtime 12
Switch#show agingtime
MAC address table agingtime is 12
Switch#set agingtime 19
Switch#show agingtime
MAC address table agingtime is 18
```

6.3.8 虚拟局域网（VLAN）配置命令

6.3.8.1 选择VLAN类型命令

该命令用于选择 VLAN 类型。

【命令格式】set vlantype <qvlan/pvlan>

【使用指南】命令用于选择 VLAN 类型。[] 内的配置项是可选的。

【参数说明】qvlan 表示 802.1Q VLAN，pvlan 表示 Port-Based VLAN。



注意：从一种 VLAN 类型切换到另一种 VLAN 类型，原 VLAN 下的配置会部分丢失。

802.1Q VLAN 切换到 Port-Based VLAN，以下配置会丢失，需重新配置，且在 Port-Based VLAN 下，Vid 必须选择 1：

- n IP 地址会被清除
- n Pvid 会被清除
- n Mac-bind 和 Mac-filter 会被清除
- n 如果 gvrp 在 802.1Q VLAN 是使能的，切换后 gvrp 会被禁止，且 gvrp 不可设置。

Port-Based VLAN 切换到 802.1Q VLAN，以下配置会丢失，需重新配置：

- n IP 地址会被清除
- n Pvid 会被清除
- n Mac-bind 和 Mac-filter 会被清除

【举例】

```
Switch#set vlantype pvlan
Successfully set vlan type.
Warning:
```

(1) Chang vlan mode will clear ip, pvid, mac-bind&mac-filter config.

Above-mentioned config will be cleaned & should be reconfigured!

(2) When Port-Based Vlan enabled:

-- Above-mentioned config should specify the vid to be No.1

-- GVRP will be disabled automatically

Switch#

6.3.8.2 802.1Q VLAN配置命令

在根提示符下键入“vlan”，进入vlan配置节点，对vlan数据库进行配置。

【命令格式】vlan

【举例】

Switch#**vlan**

Switch(vlan)#

6.3.8.2.1 802.1Q VLAN create 命令

该命令用于添加一个虚拟的 VLAN。

【命令格式】create <1-4094> [name <vlanname>] [taggedport <1-26/all>] [untaggedport <1-26/all>]

【使用指南】命令用于添加新的 VLAN。[]内的配置项是可选的。

【参数说明】<1-4094>为标识一个 vlan 的标识符 VID，该参数是必须的；<vlanname>是所配置 vlan 的名称，为一字符串，最好用“”括起来；[taggedport <1-26/all>]为带 tag 的端口范围，用“xx-xx”格式表示，“xx”表示端口号，也可以是一个单一的端口号；[untaggedport <1-26/all>]为不带 tag 的端口范围，用“xx-xx”格式表示，“xx”表示端口号，也可以是一个单一的端口号。

【举例】

Switch(vlan)#**create 2 name manager taggedport 6-9,15 untaggedport 16**

Successfully create a new VLAN.

Switch(vlan)#

6.3.8.2.2 802.1Q VLAN 忽略 VLAN 设置并退出命令

该命令放弃当前的 vlan 配置并且退出,和 exit 命令不同的是该命令不保存配置而未启用的 vlan 内容。

【命令格式】abort

【参数说明】无任何参数

【举例】

```
Switch(vlan)#abort
```

```
Switch#
```

6.3.8.2.3 802.1Q VLAN 应用 VLAN 设置命令

该命令把当前的 vlan 配置生效。

【命令格式】 **apply**

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#apply
```

```
Successfully apply vlan entries.
```

```
Switch(vlan)#
```

6.3.8.2.4 802.1Q VLAN 删除 VLAN 设置命令

该命令删除已经配置且正在工作的 vlan。删除没有生效的 vlan 系统会提示删除失败。（没有提示）

【命令格式】 **delete <1-4094>**

【参数说明】 <1-4094>为 vlan id。

【举例】

```
Switch(vlan)#delete 2
```

```
VLAN 2 was deleted.
```

```
Switch(vlan)#
```

6.3.8.2.5 802.1Q VLAN 应用 VLAN 设置并退出命令

该命令退出当前的 vlan 配置节点，并且使配置生效。

【命令格式】 **exit**

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#exit
```

```
Switch#
```

6.3.8.2.6 802.1Q VLAN 清空 VLAN 设置命令

该命令用于清空已设置但未生效 vlan 配置。

【命令格式】 **reset**

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#reset
Switch(vlan)#
```

6.3.8.2.7 802.1Q VLAN 配置 IP 命令

该命令用于设定交换机的 IP，配置 IP 的前提是已经配置成功 vlan。

- 【命令格式】**
1. ip address <A.B.C.D> mask <A.B.C.D> vid <1-4094>
 2. no ip address <A.B.C.D>
 3. show ip address

【使用指南】每个有效的 vlan 都用一个 VID 来标识，命令 2 取消 ip 的设定，参数为交换机的 IP 地址。命令 3 显示 Ip 地址。

【参数说明】address 后面的<A.B.C.D>为点分十进制方式的 IP 地址；mask 后面的<A.B.C.D>为 ip 地址对应的子网掩码，<1-4094>为 Vlan ID。

【举例】

```
Switch#config
Switch(config)#ip address 192.168.32.100 mask 255.255.255.0 vid 1
Successfully bound vlan.
Switch(config)#exit
Switch#show ip address
```

Ip Address	Mask	vid
192.168.32.100	255.255.255.0	1

```
Switch#config
Switch(config)#no ip address 192.168.32.100
The vlan bind has been released.
```

6.3.8.3 Port-Based VLAN配置命令

在根提示符下键入“pvlan”，进入 vlan 配置节点，对 vlan 数据库进行配置。

Port-Based VLAN 下支持 26 个 VLAN 表项，且在 Port-Based VLAN 下配置 IP，Mac-bind，Mac-filter 则 vid 参数必须为 1。



注意：Port-Based VLAN 下仅支持 26 个 VLAN 表项，且在 Port-Based VLAN 下配置 IP，Mac-bind，Mac-filter 都只能选择 Vid 为 1，否则有错误提示；还有在 Port-Based VLAN 下，Pvid 是没有意义的，不能设置 Pvid。

【命令格式】 pvlan

【举例】

```
Switch#pvlan
Switch(pvlan)#
```

6.3.8.3.1 Port-Based VLAN create 命令

该命令用于添加一个虚拟的 VLAN。

【命令格式】 create <1-26> [name <vlanname>] [memberport<1-26/all>]

【使用指南】 命令用于添加新的 VLAN。 []内的配置项是可选的。

【参数说明】 <1-26>为标识一个 vlan 的标识符 VID，该参数是必须的；<vlanname>是所配置 vlan 的名称，为一字符串，最好用 “ ” 括起来；[memberport<1-26/all>]为成员端口范围，用 “xx-xx” 格式表示，“xx” 表示端口号,也可以是一个单一的端口号；

【举例】

```
Switch(vlan)#create 2 name manager memberport 6-9,15
Successfully create a new VLAN.
Switch(vlan)#
```

6.3.8.3.2 Port-Based VLAN 忽略 VLAN 设置并退出命令

该命令放弃当前的 vlan 配置并且退出,和 exit 命令不同的是该命令不保存配置而未启用的 vlan 内容。

【命令格式】 abort

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#abort
Switch#
```

6.3.8.3.3 Port-Based VLAN 应用 VLAN 设置命令

该命令把当前的 vlan 配置生效。

【命令格式】 apply

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#apply
Successfully apply vlan entries.
Switch(vlan)#
```

6.3.8.3.4 Port-Based VLAN 删除 VLAN 设置命令

该命令删除已经配置且正在工作的 vlan。删除没有生效的 vlan 系统会提示删除失败。（没有提示）

【命令格式】 delete <1-26>

【参数说明】 <1-26>为 vlan id。

【举例】

```
Switch(vlan)#delete 2
VLAN 2 was deleted.
Switch(vlan)#
```

6.3.8.3.5 Port-Based VLAN 应用 VLAN 设置并退出命令

该命令退出当前的 vlan 配置节点，并且使配置生效。

【命令格式】 exit

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#exit
Switch#
```

6.3.8.3.6 Port-Based VLAN 清空 VLAN 设置命令

该命令用于清空已设置但未生效 vlan 配置。

【命令格式】 reset

【参数说明】 无任何参数

【举例】

```
Switch(vlan)#reset
Switch(vlan)#
```

6.3.8.3.7 Port-Based VLAN 配置 IP 命令

该命令用于设定交换机的 IP，配置 IP 的前提是已经配置成功 vlan。

【命令格式】 1. ip address <A.B.C.D> mask <A.B.C.D> vid <1>

2. no ip address <A.B.C.D>

3.show ip address

【使用指南】 每个有效的 vlan 都用一个 VID 来标识，命令 2 取消 ip 的设定，参数为交换机的 IP 地址。命令 3 显示 Ip 地址。

【参数说明】 address 后面的<A.B.C.D>为点分十进制方式的 IP 地址；mask 后面的<A.B.C.D>为 ip 地址对应的子网掩码，<1>为 Vlan ID。

【举例】

```
Switch#config
```

```
Switch(config)#ip address 192.168.32.100 mask 255.255.255.0 vid 1
```

Successfully bound vlan.

```
Switch(config)#exit
```

```
Switch#show ip address
```

Ip Address	Mask	vid
192.168.32.100	255.255.255.0	1

```
Switch#config
```

```
Switch(config)#no ip address 192.168.32.100
```

The vlan bind has been released.

6.3.9 生成树协议STP配置命令

生成树协议分为两部分来进行设置,包括基于主机的生成树协议设置和基于端口的生成树设置。

6.3.9.1 基于端口的生成树配置命令

用户执行该命令设置指定端口的 STP 属性。

6.3.9.1.1 使能基于端口的生成树协议命令

【命令格式】 set port <portlist|all> spanning-tree enable

【使用指南】该命令用于使能基于端口的生成树协议。参数为交换机物理端口列表,输入的形式可以是“1-2”或者“1, 2, 4-6”,如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port 1-10 spanning-tree enable
```

Successfully enable ports' stp protocol.

```
Switch#
```

6.3.9.1.2 禁止基于端口的生成树协议命令

【命令格式】 set port <portlist|all> spanning-tree disable

【使用指南】该命令用于禁止基于端口的生成树协议。参数为交换机物理端口列表,输入的形式可以是“1-2”或者“1, 2, 4-6”,如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port 1-10 spanning-tree disable
```

Successfully forbidden ports' stp protocol.

```
Switch#
```

6.3.9.1.3 设定端口路径开销命令

用户执行该命令设置该端口 STP 的端口路径开销。

【命令格式】 1. set port <portlist|all> spanning-tree cost <1-65535>

2. no set port <portlist|all> spanning-tree cost

【使用指南】命令 1 设置端口 STP 的端口路径开销，命令 2 恢复它的缺省值。默认情况下，每个 1000Mbps 网段有一个指定的路径开销值为 4，100Mbps 网段的路径开销为 19，10Mbps 网段的路径开销值为 100。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1，2，4-6”，如果要设置全部的物理端口可以使用“all”参数项。<1-65535>表示端口路径开销的数值。

【举例】

```
Switch#set port 1-10 spanning-tree cost 100
```

```
Successfully set ports' stp cost.
```

```
Switch#
```

可以用 show spanning-tree ethernet 命令显示设置的结果。

```
Switch#show spanning-tree ethernet
```

```
Designated root priority:8, address:80:00:00:0c:fe:00
```

```
Ethernet 1 is Forwarding.
```

```
Port path cost 100,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:1,path cost:0.
```

```
Ethernet 2 is Forwarding.
```

```
Port path cost 100,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:2,path cost:0.
```

```
Ethernet 3 is Forwarding.
```

```
Port path cost 100,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:3,path cost:0.
```

```
Ethernet 4 is Forwarding.
```

```
Port path cost 100,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:4,path cost:0.
```

```
Ethernet 5 is Forwarding.
```

```
Port path cost 100,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

Designated port:5,path cost:0.

Ethernet 6 is Forwarding.

Port path cost 100,Port priority 128.

-- More --

可以用下面的命令取消设置的结果。

Switch#**no set port 1-10 spanning-tree cost**

Successfully set port path cost to default.

Switch#

下面是取消后显示的结果：

Switch#**show spanning-tree ethernet**

Designated root priority:8, address:80:00:00:0c:fe:00

Ethernet 1 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:1,path cost:0.

Ethernet 2 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:2,path cost:0.

Ethernet 3 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:3,path cost:0.

Ethernet 4 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:4,path cost:0.

Ethernet 5 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:5,path cost:0.

Ethernet 6 is Forwarding.

Port path cost 19,Port priority 128.

-- More --

6.3.9.1.4 设定端口 STP 优先级命令

用户执行该命令设置指定端口的 STP 优先级。

【命令格式】 1. set port <portlist|all> spanning-tree port-priority <0-255>

2. no set port <portlist|all> spanning-tree port-priority

【使用指南】 命令 2 恢复它的缺省值。端口优先权可设置为从 0 到 255 中的一个数值。较小的数值表示端口有较大的可能性被选作为根端口。

【参数说明】 <portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。<0-255>表示端口生成树优先级数值大小。

【举例】

```
Switch#set port 1-3 spanning-tree port-priority 10
```

```
Successfully set ports' stp priority.
```

```
Switch#
```

可以使用 show spanning-tree interface 命令显示设置的结果。

```
Switch#show spanning-tree ethernet
```

```
Designated root priority:8, address:80:00:00:0c:fe:00
```

```
Ethernet 1 is Forwarding.
```

```
Port path cost 19,Port priority 10.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:4294937089,path cost:0.
```

```
Ethernet 2 is Forwarding.
```

```
Port path cost 19,Port priority 10.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:4294937090,path cost:0.
```

```
Ethernet 3 is Forwarding.
```

```
Port path cost 19,Port priority 10.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:4294937091,path cost:0.
```

```
Ethernet 4 is Forwarding.
```

```
Port path cost 19,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:4,path cost:0.
```

```
Ethernet 5 is Forwarding.
```

```
Port path cost 19,Port priority 128.
```

```
Designated bridge priority:8,address:80:00:00:0c:fe:00.
```

```
Designated port:5,path cost:0.
```

Ethernet 6 is Forwarding.

Port path cost 19,Port priority 128.

-- More --

对于上面的设置结果，可以用 no 命令取消。

Switch#**no set port 1-3 spanning-tree port-priority**

Successfully set port priority to default.

Switch#

可以看到进行取消操作后的结果：

Switch#**show spanning-tree ethernet**

Designated root priority:8, address:80:00:00:0c:fe:00

Ethernet 1 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:1,path cost:0.

Ethernet 2 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:2,path cost:0.

Ethernet 3 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:3,path cost:0.

Ethernet 4 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:4,path cost:0.

Ethernet 5 is Forwarding.

Port path cost 19,Port priority 128.

Designated bridge priority:8,address:80:00:00:0c:fe:00.

Designated port:5,path cost:0.

Ethernet 6 is Forwarding.

Port path cost 19,Port priority 128.

-- More --

6.3.9.2 基本STP设置命令

对于 STP 的基本设置包括：

- I 使能或者关闭 STP
- I 配置指定的 STP 参数

6.3.9.2.1 使能 STP

【命令格式】 spanning-tree enable

【使用指南】 该命令用于系统全局使能 STP,无参数。

【举例】

```
Switch(config)#spanning-tree enable
```

```
Successfully enable spanning tree protocol.
```

```
Switch(config)#
```

6.3.9.2.2 禁止 STP

【命令格式】 spanning-tree disable

【使用指南】 从系统全局禁止 STP 协议运行，无参数。

【举例】

```
Switch(config)#spanning-tree disable
```

```
Successfully disable spanning tree protocol.
```

```
Switch(config)#
```

6.3.9.2.3 设置 forward-time 命令

用户执行该命令用于设置 STP 的转发时间。

【命令格式】 1. spanning-tree forward-time <400-3000>

2. no spanning-tree forward-time

【使用指南】 该命令 1 能设置成 4 到 30 秒中的一个值。在从阻塞状态转换到转发状态时，这是任何交换机端口在侦听情况下所花费的时间。命令 2 恢复 forward time 的缺省值，缺省值为 15S。

【参数说明】 <400-3000>为转发延迟大小，单位为 1/100 秒。

【举例】

```
Switch(config)#spanning-tree forward-time 2400
```

```
Successfully set forward delay time.
```

```
Switch(config)#
```

```
Switch(config)# no spanning-tree forward-time
```

```
Successfully set forward delay time to default.
```

```
Switch(config)#
```

6.3.9.2.4 设置 hello-time 命令

设置当本交换机被选为根桥时发送BPDU 的时间间隔。

【命令格式】 1. spanning-tree hello-time <100-1000>

2. no spanning-tree hello-time

【使用指南】Hello Time 能被设置为从 1 到 10 秒中的一个值。这是根网桥发送两个通知其它交换机它是根网桥的 BPDU 包的发送时间间隔。命令 2 恢复 hello time 的缺省值，缺省值为 1S。

【参数说明】<100-1000>为呼叫时间大小，单位为 1/100 秒。

【举例】

```
Switch(config)#spanning-tree hello-time 500
```

```
Successfully set hello time.
```

```
Switch(config)#
```

```
Switch(config)#no spanning-tree hello-time
```

```
Successfully set hello time to default.
```

```
Switch(config)#
```

6.3.9.2.5 设置报 max-age 命令

设置BPDU 报文老化的最长时间间隔，收到超过这个时间的BPDU 报文，就直接丢弃。

【命令格式】 1. spanning-tree max-age <600-4000>

2. no spanning-tree max-age

【使用指南】Max. Age 能被设置为从 6 到 40 秒中的一个值。在 Max. Age 结束时，如果仍没有从根网桥接收到一个 BPDU，你的交换机将开始发送它自己的 BPDU 给其它所有交换机来确定成为根网桥。命令 2 恢复 max age 的缺省值，缺省值为 20S。

设置 STP max age。

【举例】

```
Switch(config)#spanning-tree max-age 3000
```

```
Successfully set max age.
```

```
Switch(config)#
```

```
Switch(config)#no spanning-tree max-age
```

```
Sucessfully set max age to default.
```

```
Switch(config)#
```

6.3.9.2.6 设置 priority 命令

用户执行该命令用于设置本交换机的优先级。

【命令格式】 1. spanning-tree priority <0-65535>

2. no spanning-tree priority

【使用指南】命令 1 为交换机设定的 Priority，能设置成 0 到 65535 中的一个数值。命令 2

恢复 STP priority 的缺省值，缺省值为 32768。

【参数说明】优先级数值。

【举例】

```
Switch(config)#spanning-tree priority 4000
```

Successfully set priority.

```
Switch(config)#
```

```
Switch(config)# no spanning-tree priority
```

Successfully set priority to default.

```
Switch(config)#
```

可以使用 show spanning-tree protocol 命令显示设置的结果。

```
Switch#show spanning-tree protocol
```

Spanning tree is executing the IEEE compatible Spanning Tree protocol.

Bridge Identifier has priority 32768, address 00:0c:fe:00:00:e1.

Configured hello time 100, max age 2000, forward delay 1500.

Current root has priority 0, address 05:dc:80:3e:38:24.

Root port is 0, cost of root path is 0.

Hold time: 1(s), topology change 9.

```
Switch#
```

6.3.10 认证设置

6.3.10.1 设置802.1x

关于 802.1x 的使能和禁止包括对于设备和端口的 802.1x 操作。

6.3.10.1.1 使能 802.1x

【命令格式】set dot1x enable

【使用指南】用户执行该命令从全局允许 802.1x 功能。

【举例】

```
Switch#set dot1x enable
```

802.1x protocol are enabled.

```
Switch#
```

6.3.10.1.2 禁止 802.1x

【命令格式】set dot1x disable

【使用指南】用户执行该命令从全局禁止 802.1x 功能。



注意：执行该命令后所有已经使能的端口的 802.1x 功能都会被禁止。

【举例】

```
Switch#set dot1x disable
```

802.1x protocol are disabled.

Switch#

6.3.10.1.3 使能端口的 802.1x

【命令格式】set port <portlist|all> dot1x enable

【使用指南】用户执行该命令来允许端口的 802.1x 功能。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。



注意：该命令执行的前提是全局 802.1x 功能必须被使能。如果全局 802.1x 功能是禁止态，该命令不能配置成功。

【举例】

```
Switch#set port all dot1x enable
```

Successfully enable ports' 802.1x functions.

Switch#

6.3.10.1.4 禁止端口的 802.1x

【命令格式】set port <portlist|all> dot1x disable

【使用指南】用户执行该命令来禁止端口的 802.1x 功能。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port all dot1x disable
```

Successfully forbidden ports' 802.1x functions.

Switch#

6.3.10.2 配置radius服务

使用 radius 认证服务包括两个方面的设置,即 radius 客户端配置和 radius 服务器端配置。在使用中,把 UFS-2400NW 作为客户端,所以在配置的时候,选取的客户端的 ip 地址只能是在交换机上配置的一个 ip 的地址。Radius 服务器可以有多个,是一个不同的 id 来进行标识。

6.3.10.2.1 配置 radius 客户端

6.3.10.2.1.1 配置 radius 客户端的 ip 地址

用户执行该命令对 radius client 的 IP 地址进行配置。

【命令格式】radius client ip <A.B.C.D>

【参数说明】<A.B.C.D>为点分十进制表示的 IP 地址。

【举例】

```
Switch(config)#radius client ip 192.168.32.11
Successfully set radius address.
Switch(config)#
```



注意：因为在 radius + 802.1x 的认证形式中，交换机起的是 radius 的客户端的作用，所以这里应该选择交换机的某个接口地址作为参数。

6.3.10.2.1.2 配置认证端口号

该命令设置 radius client 侧的接收认证报文的应用层端口号。

【命令格式】radius client port authen <1024-65535>

【使用指南】协议缺省值为 1812。

【参数说明】<1024-65535>为应用层端口号。

【举例】

```
Switch(config)#radius client port authen 1812
Successfully set radius account receive port.
Switch(config)#
```

6.3.10.2.1.3 配置计费端口号

该命令设置 radius client 侧的接收计费报文的应用层端口号。

【命令格式】radius port account <1024-65535>

【使用指南】协议缺省值为 1813。

【参数说明】<1024-65535>为应用层端口号

【举例】

```
Switch(config)#radius client port account 1813
Successfully set radius account receive port.
Switch(config)#
```

6.3.10.2.1.4 显示基本 RADIUS 基本配置命令

可以使用 show radius client 命令查看配置的结果

```
Switch# show radius client
RADIUS client IP address . . . . . : 192.168.32.11
RADIUS client authentication port. . . : 1812
RADIUS client account port . . . . . : 1813
Switch#
```

6.3.10.2.2 开启 *radius* 服务

【命令格式】radius server enable

【使用指南】该命令用于使能 radius 服务

【举例】

```
Switch(config)#radius server enable
Successfully enable radius server.
Switch(config)#
```

6.3.10.2.3 关闭 *radius* 服务

【命令格式】radius server disable

【使用指南】该命令用于禁止 radius 服务

【举例】

```
Switch(config)#radius server disable
Successfully disable radius server.
Switch(config)#
```

6.3.10.2.4 指定 *radius* 服务器

在当前配置提示符下键入“radius server”进入对 radius server 的相关信息进行配置。

【命令格式】

- 1.radius server id <1-6> ip <A.B.C.D> port <1024-65535> secret <key> retrans <1-5> interval <10-1000> type <authen,account,authen&account>
2. no radius server id <1-6>

【使用指南】命令 1 用于添加一个 radius server。”id”是 radius server 过程中必不可少的一项配置命令。命令 2 为删除一个 radius server，该命令的参数指明 radius server 的 ID 号。

【参数说明】<1-6>为 server 的 ID 号；<A.B.C.D>为点分十进制方式表示的 SERVER 的 IP 地址；<1024-65535>是 radius server 接收报文的应用层端口号，如果接收认证报文缺省端口号为 1812。如果接收计费报文缺省端口号为 1813；<key>为长度为 3-128 之间的字符串，用来标识 client 和 server 之间的共享密钥；<1-5>为用于配置 radius client 向 radius server 发送报文的最大重传次数，缺省值为 3；<10-1000>为 radius client 向 radius server 发送报文时，没收到 server 的响应而进行重传的最大时间间隔，缺省值为 10S，单位为秒；<authen,account,authen&account>是 server 接收报文的类型，目前 server 只支持两种类型：authentication，accounting。

【举例】

```
Switch(config)#radius server id 1 ip 192.168.32.100 port 1024 secret tp retrans 1 interval
```

100 type authen

Successfully configure a RADIUS server.

Switch(config)#



注意：必须保证 Radius Server 能够连通，并且连接端口为不需认证，因此在预置 1/2/3/4 口连接非认证设备，5/6/7/8 端口连接认证设备。非认证设备不需拨号就可以接入，而认证端口必须拨号。Radius server 所在主机连接在 1/2/3/4 端口之一，待认证主机接至 5/6/7/8 端口之一。

6.3.10.2.4.1 查看 server 配置命令

可以使用命令 show radius server 显示关于 radius server 的配置信息。

Switch#show radius server

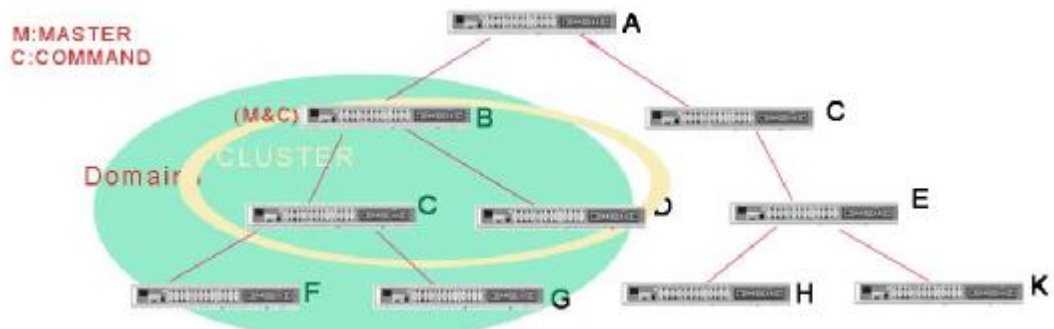
Radius server status: Enable

Id	IpAddress	Port	Times	Interval	Secret	Type
1	192.168.32.100	1	3	100	tp	authentication

Switch#

6.3.11 集群管理（虚拟堆叠）**6.3.11.1 设备发现协议**

设备发现协议配置，该协议也用于集群管理



如图所示，可以使用选定的命令设备来管理其它的设备。实现集群管理的操作步骤为：

- Ø 把要进行管理的设备和选定的命令设备进行正确的拓扑连接。
- Ø 使能所有设备的 ddp 协议。
- Ø 为管理的设备分配域名，只有同属于同一个域的设备才能完成管理功能。
- Ø 为要进行远程管理的设备创建一个有管理员操作权限的用户。
- Ø 把选定的 command 设备设为 ddp 的 master 设备。
- Ø 如果这时连接成功，可以在 command 设备上执行 show ddp neighbor 命令显示和该 command 设备处于同一域中的设备。

- Ø 对于可以被 ddp 发现的设备就可以通过 command 设备来进行管理。
- Ø 详细的配置介绍请参照《集群管理配置手册》

6.3.11.1.1 使能 ddp

用户执行该命令打开当前设备的 ddp 功能，使当前设备能够进行集群管理。

【命令格式】 ddp enable

【参数说明】 无

【举例】

```
Switch(config)#ddp enable  
DDP protocol are enabled  
Switch(config)#
```

6.3.11.1.2 禁止 ddp

用户执行该命令关闭当前设备的 ddp 功能，当前设备不再具有集群管理的特性。

【命令格式】 ddp disable

【参数说明】 无

【举例】

```
Switch(config)#ddp disable  
DDP protocol are disabled.  
Switch(config)#
```

6.3.11.1.3 配置 ddp 域名

设置当前设备的 ddp domain name。

【命令格式】 ddp domain-name <name>

【参数说明】 <name>为最大长度为 256 的字符串，用来表示 domain 的名称，最好用""括起来

【举例】

```
Switch(config)#ddp domain-name "domain1"  
DDP domain name set to domain1  
Switch(config)#
```

6.3.11.1.4 设置 ddp 命令设备

用户执行该命令设置当前设备为 ddp command 设备。

【命令格式】 ddp master

【参数说明】 无

【举例】

```
Switch(config)#ddp master
```

```
Switch(config)#
```

6.3.11.1.5 设置 ddp 监听设备

用户执行该命令改变命令设备的状态，设置当前设备为 ddp 监听设备。

【命令格式】 no ddp master

【参数说明】 无

【举例】

```
Switch(config)# no ddp master
```

```
Switch(config)#
```

6.3.11.1.6 显示 ddp 基本信息

用户执行该命令显示设备的 ddp 状态和参数。

【命令格式】 show ddp summary

【参数说明】 无

【举例】

```
Switch#show ddp summary
```

```
DDP protocol is enable.DDP domain name is: domain1.
```

```
Device status:Slave.
```

```
Switch#
```

6.3.11.1.7 显示 ddp 从设备

用户执行该命令显示 ddp 发现的其他设备。

【命令格式】 show ddp neighbor

【参数说明】 无

【举例】

```
Switch#show ddp neighbor
```

Device	Port	Mac Address	L3 Address	Cluster	Type	Time
sample	sy42949	00:0c:fe:00:00:e0	0.0.0.0	0	L3switch&agent	0

6.3.11.2 cluster 命令

6.3.11.2.1 使能命令设备

该命令设置当前的设备为 cluster 的命令设备。

【命令格式】 cluster enable <clustername>

【参数说明】 <clustername>为最大长度为 20 的字符串，用于表示这个集群的名称

【举例】

```
Switch(config)#cluster enable "manager"
Successfully set to a command device.
Switch(config)#
```

6.3.11.2.2 禁止命令设备

如果当前设备是 cluster 的命令设备，该命令把当前设备从命令状态转换到候选状态。

【命令格式】 cluster disable

【参数说明】 无

【举例】

```
Switch(config)#cluster disable
Successfully set to candidate status.
Switch(config)#
```

6.3.11.2.3 设置候选设备

该命令设置当前的设备状态由独立设备修改为 cluster 的候选设备。

【命令格式】 cluster candidate

【参数说明】 无

【举例】

```
Switch(config)#cluster candidate
Successfully set the device to candidate device.
Switch(config)#
```

6.3.11.2.4 禁止候选设备

如果当前设备是 cluster 的 member 设备，该命令把当前设备直接设置为候选设备，相当于静态设置。但是这个命令生效后，command 设备并不知晓这个 member 设备状态的改变，尽管它已经不再属于 cluster 了。这时候，如果使用命令设备依然把这个设备作为集群的成员设

备来管理，就会出错。因此，正常情况下，不要用这个命令来改变集群的 member 设备的状态。

【命令格式】 cluster change candidate

【参数说明】 无

【举例】

```
Switch(config)#cluster change candidate
```

```
Switch(config)#
```

6.3.11.2.5 设置独立设备状态

该命令设置当前的设备为 cluster 的独立设备，也就是此设备不可以被 command 设备添加到自己的 cluster 中。

【命令格式】 cluster independent

【参数说明】 无

【举例】

```
Switch(config)#cluster independent
```

```
Successfully set to independent.
```

```
Switch(config)#
```

6.3.11.2.6 添加/删除成员设备

如果当前设备是 cluster 的命令设备，该命令用于添加/删除 cluster 中的 member 设备。

【命令格式】 1.cluster add <devicename> username <name> password <password>

2. no cluster <devicename>

【使用指南】 如果当前设备是 cluster 的命令设备，命令 1 用于把其他当前状态是候选状态的设备添加到 cluster 中，命令 2 用于把其中的 member 设备从 cluster 中删除。

【参数说明】 <devicename>为对方设备的名称；<name>为该超级用户名，为一字符串；<password>为对方设备的一个超级用户的密码，为一个字符串。



注意：

1. 使用的用户名和口令参数必须存在，使用的设备名必须是用“show ddp neighbor”显示的设备名。
2. 在执行上述命令时，command 设备需要使用一个具有管理员权限的用户进行操作，而不能是系统默认的“admin”管理员帐户。

【举例】

```
Switch(config)#cluster add "devicename" username "slave" password "pass"
```

```
Successfully add a member.
```

```
Switch(config)#
```

6.3.11.2.7 改变成员状态

把当前设备直接设置为某个 cluster 的 member 设备，相当于静态设置。这个命令生效后，command 设备并不知晓这个 member 设备，但是 member 设备把设定的 command 设备当作自己的 command 设备。也就是说这时候不可以通过 command 设备来管理当前设备。目前该命令主要用于处理 member 设备的本地 member 状态丢失的情况。

【命令格式】cluster change member name <clustername> mac-addr <HH:HH:HH:HH:HH:HH>

【参数说明】<clustername>为最大长度为 256 的字符串，用于表示 cluster 的名称，<HH:HH:HH:HH:HH:HH>为 cluster 中命令设备的 MAC 地址。

【举例】

```
Switch(config)#cluster change member name "cluster1" mac-addr 00:02:e3:45:62:f5
Switch(config)#
```

6.3.11.2.8 show cluster summary

用户执行该命令显示当前设备的 cluster 状态和参数。

【命令格式】show cluster summary

【参数说明】无

【举例】

```
Switch#show cluster summary
Cluster name is:manager
Device is cluster Command status.
Switch#
```

6.3.11.2.9 show cluster member

如果当前设备是 cluster command 设备，此命令用于显示，当前所有的 member 成员。

【命令格式】show cluster member

【参数说明】无

【举例】

```
Switch#show cluster member
Cluster name is:manager
Device is cluster Command status.
Switch#
```

6.3.11.2.10 远程管理命令 rcommand

rcommand 命令用于实现设备的远程管理，需要两台以上的交换机，其功能类似于 telnet 网管方式。rcommand 是通过 ulink 协议进行传输，所以这里的 rcommand 命令有节省 IP 地址的优点。另外和 telnet 不同之处是 Telnet 需要客户端对收到的报文进行解释，而我们的 rcommand 命令的主要功能是透传，解释功能还是由 console 终端或者 Telnet 终端完成。



注意：在使用 rcommand 前要求进行控制和被控制的设备的 ddp 协议均被使能，并且把设备加入到同一个域中，同时把进行控制的设备设置为 ddp 命令设备。这样被控制设备作为进行控制的设备的从设备，可以使用显示从设备的命令进行显示，只有在显示结果中可以看到从设备，才可以成功执行 rcommand 命令。

【命令格式】rcommand <name>

【参数说明】<name>另一台交换机的设备名称，为一字符串。

【举例】

假设有下面两个设备。

设备名称	提示符	超级用户名	密码	举例
设备 A:	deviceA	tpA	tpA	图表 1
设备 B:	deviceB	tpB	tpB	图表 2

图表 1

```
deviceA#
deviceA# show user
```

User name	Password	Access level	Property
tpA	tpA	15	0

```
deviceB#
deviceB# show user
```

User name	Password	Access level	Property
tpB	tpB	15	0

图表 2

在设备 A 上执行命令 rcommand 命令后结果如下：

```
deviceA#
deviceA#rcommand deviceB
login: tpB
password:
deviceA#deviceB#show user
```

User name	Password	Access level	Property
tpB	tpB	15	0

deviceA#rcommand deviceB 提示符后面的命令是当前设备 B 上的命令，和在设备 B 上执行的命令完全相同。

6.3.12 Garp协议

6.3.12.1 设置join定时器

该命令用于设置 garp join timer 的值。

【命令格式】1 .set port <portlist|all> garp join-time<20-20000>

2. no set port <portlist|all>garp join-time

【使用指南】命令 1 用于设置 garp join timer 的值；命令 2 恢复 garp join timer 的缺省值，只需一个参数指明物理端口号即可，缺省值为 20ms。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；<20-20000>为该端口的 garp join timer 时间值，单位为 1/100 秒，取值范围为 20—20000。

【举例】

```
Switch#set port all garp join-time 200
Successfully set ports' garp join timer.
Switch#
Switch#no set port all garp join-time
Successfully set garp join time to default.
Switch#
```

6.3.12.2 leave命令

该命令用于设置 garp leave timer 的值。

【命令格式】1.set port <portlist|all> garp leave-time<60-20000>

2. no set port <portlist|all>garp leave-time

【使用指南】命令 1 用于设置 garp leave timer；命令 2 恢复 garp leave timer 的缺省值，只需一个参数指明物理端口号即可,缺省值为 60ms。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；<60-20000>为该端口的 garp leave timer 时间值，单位为 1/100 秒，取值范围为 60-20000。

【举例】

```
Switch#set port all garp leave-time 100
Successfully set ports' garp leave time.
Switch#
Switch#no set port all garp leave-time
Successfully set port garp leave time to default.
Switch#
```

6.3.12.3 leaveall 命令

该命令用于设置 garp leaveall timer 的值。

【命令格式】1.set port <portlist|all> garp leaveall-time<1000-1500>

2. no set port <portlist|all>garp leaveall-time

【使用指南】命令 1 用于设置 garp leaveall timer 的值；命令 2 恢复 garp leaveall timer 的缺省值，只需一个参数指明物理端口号即可，缺省值为 1000ms。

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；<1000-1500>为该端口的 garp leaveall timer 时间值，单位为 1/100 秒，取值范围为 1000-1500。

【举例】

```
Switch#set port all garp leaveall-time 1200
Successfully set port garp leaveall time.
Switch#
Switch#no set port all garp leaveall-time
Successfully set ports' garp leaveall time to default.
Switch#
```

可以用下面的命令显示 garp 设置的结果。也可以用 show garp all 命令显示所有设置的结果。

```
Switch#show garp port 10
Port  PortStatus  JoinTime(s)  LeaveTime(s)  LeaveAllTime(s)
10    disable      200          100           1200
Switch#
```

6.3.12.4 gvrp 命令

“gvrp”命令集完成对 GVRP 协议的使能和禁止功能。



注意：在 Port-Based VLAN 下，gvrp 是被禁止的，不能使能 gvrp，gvrp 只在 802.1Q VLAN 下有效。

6.3.12.4.1 禁止 gvrp 协议

该命令禁止 GVRP 协议。

【命令格式】 set gvrp disable

【参数说明】 无任何参数

【举例】

```
Switch#set gvrp disable
Successfully disable GVRP protocol.
Switch#
```

6.3.12.4.2 使能 gvrp 协议

该命令使能 GVRP 协议。

【命令格式】 set gvrp enable

【参数说明】 无任何参数

【举例】

```
Switch#set gvrp enable
Successfully enable GVRP protocol.
Switch#
```

6.3.12.4.3 基于端口的 gvrp

该命令用于设置指定端口的 GVRP 协议属性。

6.3.12.4.3.1 设置接收报文的类型

该命令设置端口的 gvrp 协议可以接收的报文类型。

【命令格式】 set port <portlist|all>gvrp acceptableframe <all|tag>

【参数说明】 <portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；<all|tag>为可接收的报文类型，目前支持两种类型：all, tag，最好用“”括起来。

【举例】

```
Switch#set port 5-10 gvrp acceptableframe tag
Successfully set gvrp port acceptable frame type.
Switch#
```

6.3.12.4.3.2 禁止端口的 gvrp

该命令禁止指定端口的 gvrp 功能。

【命令格式】 set port <portlist|all>gvrp disable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port 5-10 gvrp disable
Successfully forbidden ports' gvrp protocol.
Switch#
```

6.3.12.4.3.3 使能端口的 gvrp

该命令使能指定端口的 gvrp 功能。

【命令格式】set port <portlist|all>gvrp enable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项。

【举例】

```
Switch#set port 5-10 gvrp enable
Successfully enable ports' gvrp protocol.
Switch#
```

6.3.12.4.3.4 使能端口的 ingressfilter

该命令设置使能端口的 ingress filter 状态。当 filter 使能，端口只能接收所属 vlan（可以是一个 vlan 也可以是多个 vlan）内的报文；反之端口可以接收所有 vlan 的报文。

【命令格式】set port <portlist|all>gvrp ingressfilter enable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；

【举例】

```
Switch#set port 5-10 gvrp ingressfilter enable
Successfully enable gvrp ports' ingress filter.
Switch#
```

6.3.12.4.3.5 禁止端口的 ingressfilter

该命令设置使能端口的 ingress filter 状态。

【命令格式】set port <portlist|all>gvrp ingressfilter disable

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；

【举例】

```
Switch#set port 5-10 gvrp ingressfilter disable
Successfully disable gvrp ports' ingress filter.
Switch#
```

6.3.12.4.3.6 pvid 命令

该命令设置指定端口 pvid。

【命令格式】set port <portlist|all> gvrp pvid <1-4094>

【参数说明】<portlist|all>为交换机物理端口列表，输入的形式可以是“1-2”或者“1, 2, 4-6”，如果要设置全部的物理端口可以使用“all”参数项；<1-4094>为端口的 Vlan 标识 PVID,该参数为可选，默认情况下，端口的 vlan 标识为 1。



注意：

- a) 该命令仅在 802.1Q VLAN 下有效，在 Port-Based VLAN 下无效。
- b) vlan 标识必须是一个已经存在的 vlan 标识。如果命令行中使用的 vlan 标识不存在，设置就会不成功。
- c) 选择的端口列表中全部的端口必须处于同一个 vlan 中，否则设置不成功。

【举例】

```
Switch#set port 5-10 gvrp pvid 2
```

Successfully set ports' vlan id.

```
Switch#
```

可以用下面的命令显示 gvrp 设置的结果。

```
Switch#show gvrp port
```

Port	PortId	Acceptable Type	Filter	Status	Fail Regist	Last GVRP Pdu
1	1	admitAll	disable	enable	0	00:00:00:00:80:3f
2	1	admitAll	disable	enable	0	00:00:00:00:80:3f
3	1	admitAll	disable	enable	0	00:00:00:00:80:3f
4	1	admitAll	disable	enable	0	00:00:00:00:80:3f
5	2	admitTag	disable	disable	0	00:00:00:00:80:3f
6	2	admitTag	disable	disable	0	00:00:00:00:80:3f
7	2	admitTag	disable	disable	0	00:00:00:00:80:3f
8	2	admitTag	disable	disable	0	00:00:00:00:80:3f
9	2	admitTag	disable	disable	0	00:00:00:00:80:3f
10	2	admitTag	disable	disable	0	00:00:00:00:80:3f
11	1	admitAll	disable	enable	0	00:00:00:00:80:3f
12	1	admitAll	disable	enable	0	00:00:00:00:80:3f
13	1	admitAll	disable	enable	0	00:00:00:00:80:3f
14	1	admitAll	disable	enable	0	00:00:00:00:80:3f
15	1	admitAll	disable	enable	0	00:00:00:00:80:3f
16	1	admitAll	disable	enable	0	00:00:00:00:80:3f
17	1	admitAll	disable	enable	0	00:00:00:00:80:3f
18	1	admitAll	disable	enable	0	00:00:00:00:80:3f

19	1	admitAll	disable enable	0	00:00:00:00:80:3f
20	1	admitAll	disable enable	0	00:00:00:00:80:3f
21	1	admitAll	disable enable	0	00:00:00:00:80:3f
22	1	admitAll	disable enable	0	00:00:00:00:80:3f

-- More --

6.3.13 端口聚合管理

6.3.13.1 静态链路聚合

该命令设置静态端口聚合组

【命令格式】set trunk static port <1-26> to <1-26>

【使用指南】在静态链路聚合设置成功之后，负荷分担真正起作用的前提条件是被绑定的所有端口都已链接上，缺一不可，否则聚合不起作用

【参数说明】port 后面的<1-26>为要聚合的物理端口号；to 后面的<1-26>为要聚合到的端口号。

【举例】

```
Switch#set trunk static port 2 to 1
bind port 2 to port 1 .
Switch#
```

6.3.14 简单网络管理（SNMP）

SNMP（Simple Network Management Protocol，简单网络管理协议）它为网络管理系统提供了底层网络管理的框架。**SNMP**的设计原则是简单性和扩展性。简单性是通过信息类型限制、请求响应或协议而取得。扩展性是通过将管理信息模型与协议、被管理对象的详细规定（**MIB**）分离而实现的。它的设计目标是使管理信息能在网络任意两点间传送，使网络管理员可以在网络中的任何节点检索信息，修改配制，查找故障，诊断故障，规划流量及生成报告。它采用轮询机制，提供最基本的功能集。

本节将介绍 **SNMP** 功能的有关配置。

6.3.14.1 设置community 及访问权限

SNMP采用**community**(共同体)的认证方案，每个**SNMP**报文中都有一个称为**community** 的字符串，作为**NMS**（网管站）和**Agent**(代理)通讯的口令。如果收到的**SNMP**报文的**community**同设备认可的**community**不符，该报文将会被丢弃。同时不同的**community**还具有不同的访问权限。只读的共同体只能对设备信息进行查询，而可读写的共同体除此之外还能对设备进行配置。

【命令格式】

1. snmp-server community <name> access <ro/rw>
2. no snmp-server community <name>

【参数说明】<name>为共同体的名称，可由 26 个英文字母和阿拉伯数字组成，最多包含 20 个字符；access <ro/rw>表示其共同体访问的权限，ro/rw 分别为 read only 和 read write 的缩写，即为只读和读写。

【使用指南】命令 1 是创建命令，命令 2 用于删除。系统有一默认共同体 “public”。

【举例】

```
Switch(config)#snmp-server community am access rw
Successfully set SNMP server community.
switch(config)#no snmp-server community am
Successfully delete community entry.
switch(config)#
管理员可以通过 show snmp-server community 来显示配置信息
Switch#show snmp-server community
*****SNMP Community*****
*          ro=ReadOnly          rw=ReadWrite          *
*****
NAME                                ACCESS_LEVEL
public                              rw
am                                  rw
Switch#
```

6.3.14.2 创建SNMP Agent联系人

SysContact是MIB-II中的一个管理变量，用来标识被管设备的管理员的姓名及联系方式等信息，在网络出现故障时，可依据此值同设备管理人员取得联系。

【命令格式】snmp-server contact <name>

【参数说明】<name>为管理员的姓名，可由 26 个英文字母和阿拉伯数字组成，最多包含 255 个字符。默认值为 “sample sysContact factory default”。

【举例】

```
Switch(config)#snmp-server contact tom
Successfully set snmp server contact.
Switch(config)#
```

可通过show switch命令显示信息。

6.3.14.3 创建SNMP Agent地址信息

SysLocation也是MIB-II 中的一个管理变量，用来标识被管设备所处的实际位置。

【命令格式】snmp-server location <name>

【参数说明】<name>为所处的实际位置，可由26个英文字母和阿拉伯数字组成，最多包含255

个字符。默认值为“**sample sysContact factory default**”。

【举例】

```
Switch(config)#snmp-server location center
```

Successfully set snmp server system location.

```
Switch(config)#
```

可通过 **show switch** 命令显示信息。

6.3.14.4 SNMP Trap

6.3.14.4.1 创建修改

【命令格式】

```
snmp-server target name <name> params [ip <A.B.C.D> |version<v1/v2c> |retry<0-255> |
timeout<0-4294967295>]
```

【参数说明】<name>可以由 26 个英文字母和阿拉伯数字组成，最多可以包含 32 个字符；ip <A.B.C.D>表示的是 SNMP trap 应该发往的 PC 机的 IP 地址，默认为 0.0.0.0；version<v1/v2c>表示的是 SNMP 报文的版本 v1、v2c，缺省版本为 v1；retry<0-255>表示的是交换机发送 trap 报文而没有得到响应后传送的次数，范围为 0-255，缺省值为 3 次；timeout<0-4294967295>表示的是交换机发送 SNMP trap 报文的没有得到响应的超时时间，单位为秒，缺省值为 1500 秒。

【使用指南】此命令可用于创建一个 SNMP trap 报文的发送给 PC 机时的一些设定，[]内的参数为可选参数，但是必须输入其中一个参数作为创建内容，也必须填写一个参数作为修改。



注意：当修改时，必须先使 trap 状态设为 notInService，即使用 **snmp-server disable trap name <name>**命令。

【举例】

```
Switch(config)#snmp-server target name abcd params ip 192.168.32.108 version v2c
```

Successfully configure target entry.

```
Switch(config)#
```

用户可以使用 show snmp-server information 命令来显示配置

```
Switch#show snmp-server information
```

```
*****SNMPCONFIGURE INFORMATION*****
*      L=linkupdown   A=auth-fail   T=topochange   NOT=notInService      *
*****
Name           IpAddress      Version   Trap   Status  Retry  Timeout
abcd           192.168.32.108  V2c      L A T  NOT    3      1500
Switch#
```

6.3.14.4.2 设置 SNMP trap 类型

本款交换机的 SNMP 支持对三种类型的 trap 报文的接收，一是认证失败（authentication fail），一是链接情况（link up or down），一是拓扑改变（topology change）。

【命令格式】snmp-server trap name <name> type [auth-fail|linkupdown|topochange]

【参数说明】<name>为创建 **target** 时所写的名称，可由 26 个英文字母和阿拉伯数字组成，最多包含 32 个字符。[] 内为可选参数，不输入表示全部包括，输入任何一种表示只接收此类 **trap** 报文。

【使用指南】此命令是在创建后设定的接收的 trap 类型，所以请在创建后，设置此命令。然后再使能 trap。

【举例】

```
Switch(config)#snmp-server trap name abcd type
```

Successfully configure SNMP trap.

```
Switch(config)#
```

用户可以使用 show snmp-server information 命令来显示配置

```
Switch#show snmp-server information
```

```
*****SNMPCONFIGURE INFORMATION*****
*          L=linkupdown   A=auth-fail   T=topochange   NOT=notInService          *
*****
Name                IpAddress          Version   Trap   Status  Retry  Timeout
abcd                192.168.32.108      V2c      L A T  NOT    3     1500
Switch#
```

6.3.14.4.3 使能 SNMP trap

【命令格式】snmp-server enable trap name <name>

【参数说明】<name>为创建 **target** 时所写的名称，可由 26 个英文字母和阿拉伯数字组成，最多包含 32 个字符。

【使用指南】此命令是使 trap 设置成功的必然命令。

【举例】

```
Switch(config)#snmp-server enable trap name abcd
```

Successfully enable SNMP trap.

```
Switch(config)#
```

用户可以使用 show snmp-server information 命令来显示配置

```
Switch#show snmp-server information
```

```
*****SNMPCONFIGURE INFORMSTION*****
*          L=linkupdown   A=auth-fail   T=topochange   NOT=notInService          *
*****
```

Name	IpAddress	Version	Trap	Status	Retry	Timeout
abcd	192.168.32.108	V2c	L A T	Active	3	1500

Switch#

6.3.14.4.4 禁止 SNMP trap

【命令格式】 snmp-server disable trap name <name>

【参数说明】<name>为创建target时所写的名称，可由26个英文字母和阿拉伯数字组成，最多包含32个字符。

【使用指南】此命令是使 trap 设置处于不服务（not in service）状态，此状态将不向目的 PC 机发送 trap 报文，而且预对 trap 的设置进行修改时必须使用此命令才可以进行修改。

【举例】

Switch(config)#snmp-server disable trap name abcd

Successfully disable SNMP trap.

Switch(config)#

用户可以使用 show snmp-server information 命令来显示配置

Switch#show snmp-server information

*****SNMPCONFIGURE INFORMATION*****

* L=linkupdown A=auth-fail T=topochange NOT=notInService *

Name	IpAddress	Version	Trap	Status	Retry	Timeout
abcd	192.168.32.108	V2c	L A T	NOT	3	1500

Switch#

6.3.14.4.5 删除 SNMP trap

【命令格式】 no snmp-server target name <name>

【参数说明】<name>为创建target时所写的名称，可由26个英文字母和阿拉伯数字组成，最多包含32个字符。

【使用指南】此命令是使 trap 设置全部删除。

【举例】

Switch(config)#no snmp-server target name abcd

Successfully delete SNMP trap.

Switch(config)#

用户可以使用 show snmp-server information 命令来显示配置

6.3.14.4.6 设置 SNMP trap 举例

I 创建

创建一个名为 center 的 SNMP trap 并使其工作使能。假设将向 IP 地址为 192.168.32.108 的 PC 机发送 V1 的 trap 报文，而且只发送链接状态（link up or down）和拓扑改变（topology change）的 trap 报文，重传次数为四次，超时时间为 1000 秒。具体命令如下：

```
Switch(config)#snmp-server target name center params ip 192.168.32.108 version v1 retry
4 timeout 1000
```

Successfully configure target entry.

```
Switch(config)#snmp-server trap name center type linkupdown topochange
```

Successfully configure SNMP trap.

```
Switch(config)#snmp-server enable trap name center
```

Successfully enable SNMP trap.

```
Switch#show snmp-server information
```

```
*****SNMP CONFIGURE INFORMATION*****
*      L=linkupdown   A=auth-fail   T=topochange   NOT=notInService      *
*****
Name                IpAddress          Version  Trap   Status  Retry  Timeout
center              192.168.32.108    V1      T.L    Active  4      1000
Switch#
```

I 修改

修改一个名为 center 的 SNMP trap 并使其工作使能。假设将向 IP 地址为 192.168.32.108 的 PC 机发送 V2c 的 trap 报文，而且只发送链接状态（link up or down）的 trap 报文，重传次数仍为四次，超时时间也为 1000 秒。具体命令如下：

```
Switch(config)#snmp-server disable trap name center
```

Successfully disable SNMP trap.

```
Switch(config)#snmp-server target name center params version v2c
```

Successfully configure target entry.

```
Switch(config)#snmp-server trap name center type linkupdown
```

Successfully configure SNMP trap.

```
Switch(config)#snmp-server enable trap name center
```

Successfully enable SNMP trap.

```
Switch#show snmp-server information
```

```
*****SNMP CONFIGURE INFORMATION*****
*      L=linkupdown   A=auth-fail   T=topochange   NOT=notInService      *
*****
Name                IpAddress          Version  Trap   Status  Retry  Timeout
center              192.168.32.108    V2c     L      Active  3      1500
```

Switch#

I 删除

删除一个名为 center 的 SNMP trap。

```
Switch(config)#no snmp-server target name center
```

Successfully delete SNMP trap.

```
Switch(config)#
```

6.3.15 MAC地址绑定

UFS-2400NW MAC 地址绑定，是将 MAC 地址和 Vlan ID、端口绑定。对于拥有符合条件的 MAC 地址的报文才可以转发。



注意：

- 1) 如果某个端口已经使能 802.1x，该端口可以同时进行 MAC 地址的绑定；但如果在该端口已经和 MAC 地址绑定的情况下禁止该端口的 802.1x，则操作失败，必须先解除绑定，才能禁止该端口的 802.1x。一般来讲，将某个 MAC 和某个端口绑定后，就不需要进行 802.1x 的认证。
- 2) 在 Port-Based VLAN 下，Mac 绑定的 vlan 参数只能选择 1，否则有错误提示。

6.3.15.1 创建与删除

【命令格式】

1. mac-bind mac<HH:HH:HH:HH:HH:HH>vlan<1-4094>port<1-26>
2. no mac-bind mac<HH:HH:HH:HH:HH:HH>vlan<1-4094>

【参数说明】<HH:HH:HH:HH:HH:HH>为绑定的MAC地址，<1-4094>为vlan的ID号，<1-26>为端口号。

【使用指南】命令 1 是用于创建的，命令 2 用于删除。

【举例】

```
Switch(config)#mac-bind mac 01:02:03:04:06:06 vlan 3 port 19
```

Successfully create MAC bind.

```
Switch(config)#no mac-bind mac 01:02:03:04:06:06 vlan 3
```

Successfully delete MAC bind.

```
Switch(config)#
```

用户可以使用 show mac-bind 命令来显示配置

6.3.15.2 显示配置信息

【命令格式】show mac-bind

【参数说明】此命令无参数。

【举例】

Switch#show mac-bind

*****Mac Bind Table*****

MacAddress	Vlan	Port
01:02:03:04:05:06	1	16
01:02:03:04:06:06	2	18
01:02:03:04:06:06	3	19

Switch#

6.3.16 MAC地址过滤

UFS-2400NW MAC 地址过滤，是将要过滤的 MAC 地址和 Vlan ID 绑定。对于拥有符合条件的 MAC 地址的报文将不转发。



注意：在 Port-Based VLAN 下，Mac 过滤的 vlan 参数只能选择 1，否则有错误提示。

6.3.16.1 创建与删除

【命令格式】

1. mac-filter mac<HH:HH:HH:HH:HH:HH>vlan<1-4094>
2. no mac-filter mac<HH:HH:HH:HH:HH:HH>vlan<1-4094>

【参数说明】<HH:HH:HH:HH:HH:HH>为过滤的MAC地址，<1-4094>为vlan的ID号

【使用指南】命令 1 是用于创建的，命令 2 用于删除。

【举例】

Switch(config)#mac-filter mac 01:02:03:04:05:06 vlan 1

Successfully create MAC filter.

Switch(config)#no mac-filter mac 01:02:03:04:05:06 vlan 1

Successfully delete MAC filter.

Switch(config)#

用户可以使用 show mac-filter 命令来显示配置

6.3.16.2 显示配置信息

【命令格式】show mac-filter

【参数说明】此命令无参数。

【举例】

Switch#show mac-filter

*****Mac Filter Table*****

MacAddress	Vlan
01:02:03:04:05:06	1

01:02:03:04:05:06 2

01:02:03:04:06:06 3

Switch#

6.3.17 日志功能

6.3.17.1 日志格式介绍

1. 错误消息的格式

系统日志的消息格式和**4.3 BSD UNIX**保持一致，系统错误消息格式如下：

%TIME-FACILITY-SEVERITY-MNEMONIC:Message Text

% 表示消息的开始；

TIME 为交换机产生消息的时间

FACILITY 指出错误消息涉及的设备名。该值可以是协议、硬件设备或者系统软件模块。

SEVERITY表示了消息的等级，它是一个范围在**0**到**7**之间的数字。数字的值越小，严重程度越高。

MNEMONIC唯一标识错误消息的单值代码。该代码通常可以暗示错误的类型。

Message Text 它是错误消息的简短描述，其中包括涉及的路由器硬件和软件信息。

下面是一些错误消息的示例。

%08: 01: 02-DUAL-3-SIA:

Route 171.155.148.192/26 stuck-in-active state in IP-EIGP 211. Cleaning up

%09:01:02-LANCE-3-OWNERR: Unit 0, buffer ownership error



注意：并不是所有的消息都涉及到故障或者问题的状况。某些消息显示的是状态方面的信息。

例如，以下消息仅表明**ISDN BRI 0**接口与特定的远端数据连接。

%09:021:02-ISDN-6-CONNECT: Interface BRI0 is now connected to 95551212

2. 类型的属性和分级

日志的属性，它如表一所示：

日志种类	说明
auth	登陆记录
App	应用程序
Ip	Ip 内核消息
L2	L2 协议

Mroute	组播模块
Nms	网络管理模块
Osal	操作系统内核消息
Qos	服务质量模块消息
Route	单播路由模块消息
Security	安全模块消息
Vovi	Voip 模块消息
local0 - 7	其它内部使用

表格 6-1 日志属性

3. 日志的等级

表二日志的等级程度:

訊息程度	說明
debug	调试消息 —— 7
info	提示性的消息 —— 6
notice	正常的，可能需要注意的消息 —— 5
warning	警告消息 —— 4
err	错误消息 —— 3
crit	重要消息 —— 2
alert	需要马上采取行动的消息 —— 1
emerg	系统不可以使用消息 —— 0

表格 6-2 日志消息级别

6.3.17.2 启动日志功能

通过本命令将启动日志功能。

【命令格式】 logging on

【参数说明】 此命令无参数。

【举例】

Switch(config)# logging on

Switch(config)#

6.3.17.3 关闭日志功能

通过本命令将关闭日志功能。

【命令格式】no logging on

【参数说明】此命令无参数。

【举例】

```
Switch(config)# no logging on
```

```
Switch(config)#
```

6.3.17.4 设置向缓存区输出日志信息

【命令格式】logging buffered <0-7>

【参数说明】<0-7>与表格 6-3 所示的日志消息级别相对应。

【举例】

```
Switch(config)# logging buffered 3
```

```
Switch(config)#
```

6.3.17.5 取消向缓存区输出日志信息

【命令格式】no logging buffered

【参数说明】此命令无参数。

【举例】

```
Switch(config)# no logging buffered
```

```
Switch(config)#
```

6.3.17.6 设置向控制台输出日志信息

【命令格式】logging console <0-7>

【参数说明】<0-7>与表格 6-4 所示的日志消息级别相对应。

【举例】

```
Switch(config)# logging console 2
```

```
Switch(config)#
```

6.3.17.7 取消向控制台输出日志信息

【命令格式】no logging console

【参数说明】此命令无参数。

【举例】

```
Switch(config)# no logging console
```

```
Switch(config)#
```

6.3.17.8 显示日志信息

【命令格式】 show logging

【参数说明】 此命令无参数。

【举例】

Switch#**show logging**

Syslog logging: enabled

Console logging: enabled ,level error

Buffer logging: enabled ,level critical

Switch#

7. 基于WEB的网络管理

交换机还提供了一个内置的基于 WEB 方式的网络管理系统，用户可以位于网络的任何地方通过标准的浏览器（Microsoft Internet Explorer 4.x 及以上）来管理交换机，由于浏览器的版本不同，你看到的访问界面可能与下文中的图示不太相同。如果要到达一个好的显示效果，需要把显示器的分辨率调整为 1026×768。

7.1 准备工作

首先，需要在你的计算机上安装好浏览器软件（Microsoft Internet Explorer 4.x 及以上），安装方法详见浏览器自己的安装说明。

其次，需要配置交换机的 IP 地址，可以在控制台界面中手动设置。见 6.2.2 [配置交换机 IP 地址](#)。

7.2 WEB 管理界面配置说明

运行浏览器，在浏览器的 URL 地址栏中输入交换机的 IP 地址，就可以通过 WEB 访问交换机。假设交换机的 IP 地址为：192.168.32.11，则在 URL 中输入 **http://192.168.32.11**，然后点击 Enter 键，即可进入 WEB 管理界面。

初次进入视窗管理界面，会出现用户名和密码对话框。输入登录名“admin”，密码“password”，即可进入管理主画面，并可看见设备的前面板图标。

所有可操作菜单皆罗列于视窗的左侧，用户可通过直接点击相应功能项，进入下层菜单。

绝大多数设置画面都具有接受设置 **apply** 及 **save** 选项。“接受设置”表示修改参数并刷新界面，“save”表示存储参数。

 **注意：**点击 **apply** 只对当前设置生效，如需将设置存储于 NVRAM，则需 **save** 功能使之生效。

初次进入视窗管理界面时的界面如下图所示：

该页面显示交换机的基本配置信息：包括交换机的设备类型描述，交换机的 MAC 地址（不可改变），IP 地址，子网掩码，缺省网关 IP 地址，交换机的位置描述及其它二层协议的使能、禁止开关。以后会详细介绍该各项配置。

Switch Information	
Display information about the switch's hardware and software	
MAC Address	00:0c:fe:0a:0e:0d
IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Software Version	1.21
Name	sample sysName factory default
Location	factory default
Contact	factory default
Traffic Classes	enable ▾
GVRP	disable ▾

图 7-1 WEB 管理初始界面

7.2.1 基本配置

展开左侧的“Base Setup”，会下拉出配置信息的各个表项，点击相应的表项，即可对相应信息进行配置或产生相应操作。

7.2.1.1 交换机信息 (Switch Information)

点击配置页面左侧的“Switch Information”，会打开图 7-1 所示的初始界面，显示该交换机的基本配置信息。

7.2.1.2 交换机基本信息配置(Basic Switch Setup)

点击配置页面左侧的“Basic Switch Setup”，打开图 7-2 所示的配置界面，显示目前的配置信息及可以对该交换机进行新的配置的文本框。内容包括：

IP address: 交换机的 IP 地址

Default Gateway: 缺省网关的 IP 地址

VLAN Name: 缺省 VLAN1 的名称

Link Aggregation: 链路聚合的使能禁止开关

STP: STP 协议的使能禁止开关

Name: 用户指定的交换机名，对应于 SNMP MIB II 中的 system.sysName 变量；

Location: 用户定义的交换机所在的位置描述，对应于 SNMP MIB II 中 system.sysLocation 变量；

Contact: 系统维护的联系人，对应于 SNMP MIB II 中的 sysContact 变量。

Basic Switch Setup

Configure the switch's IP address and contact information

Current Switch IP Settings	
Default Gateway	0.0.0.0
VLAN Name	default

New Switch IP Settings	
Default Gateway	0.0.0.0
VLAN Name	default

STP	disable
-----	--------------------------------------

Name	sample sysName factory default
Location	factory default
Contact	factory default

图 7-2 Basic Switch Setup 界面

7.2.1.3 配置串口属性(Serial Port Setting)

点击配置页面左侧的“Serial Port Setting”，会打开图 7-3 所示的串口属性配置界面，本页面完成对串口属性的配置，包括波特率、数据位、奇偶校验、停止位等属性。

Serial Port Settings	
Configure the switch's serial port that is used for terminal sessions	

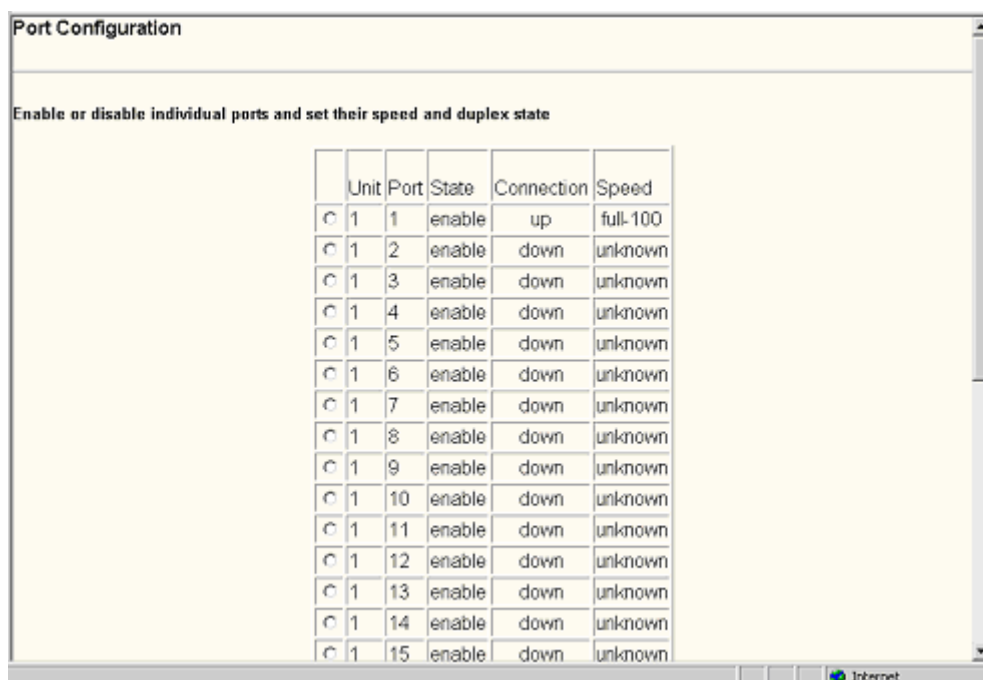
Console Settings	
Baud Rate	9600
Data Bits	8
Parity Bits	None
Stop Bits	1

图 7-3 Serial Port Setting 界面

7.2.1.4 端口配置 (Port Configuration)

点击配置页面左侧的“Port Configuration”，会进入图 7-4 所示的端口信息显示界面，该界面列出了全部 26 个端口的状态、连接状态及端口速率等信息。选择某个端口后点击“Edit”按钮会弹出图 7-5 所示的对话框，利用该对话框可以对该端口进行设置了，可按如下步骤进行：

1. 在“State”中，Enable 或 Disable 该端口，如果用户选择“Disable”，那么连接在该端口的设备将不能使用交换机，并且在 MAC 地址表老化后，交换机会将该设备的 MAC 地址从地址表中清除掉。但是，如果该设备的 MAC 地址在静态地址表中，则不会被老化清除。
2. 在“Set Speed”中，可以设置端口的工作速率和双工模式，可选值有：autonegotiate（自适应）、half-10（10Mbps 半双工）、full-10（10Mbps 全双工）、half-100（100Mbps 半双工）、full-100（100Mbps 全双工）。
3. 对话框中还可以看出该端口的实际速率、类型、STP 状态等。



	Unit	Port	State	Connection	Speed
☐	1	1	enable	up	full-100
☐	1	2	enable	down	unknown
☐	1	3	enable	down	unknown
☐	1	4	enable	down	unknown
☐	1	5	enable	down	unknown
☐	1	6	enable	down	unknown
☐	1	7	enable	down	unknown
☐	1	8	enable	down	unknown
☐	1	9	enable	down	unknown
☐	1	10	enable	down	unknown
☐	1	11	enable	down	unknown
☐	1	12	enable	down	unknown
☐	1	13	enable	down	unknown
☐	1	14	enable	down	unknown
☐	1	15	enable	down	unknown

图 7-4 端口信息

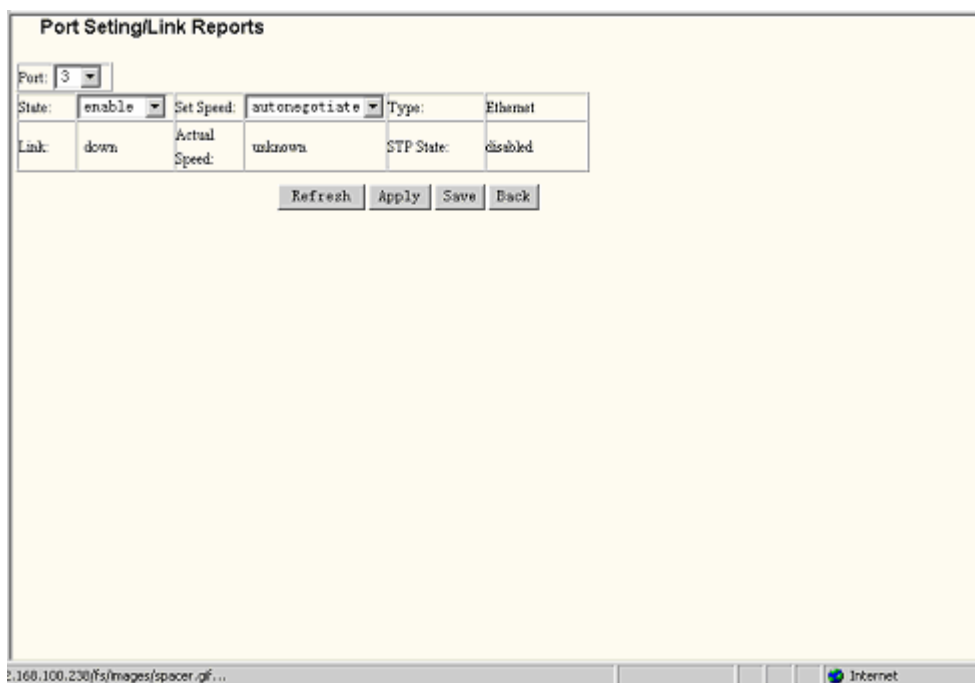


图 7-5 端口配置

7.2.1.5 工具配置 (Switch Utilities)

点击配置页面左侧的“Switch Utilities”，并按图 7-6 配置页面左侧展开，点击第一个“Download or Upload”，会显示如图所示配置页面。

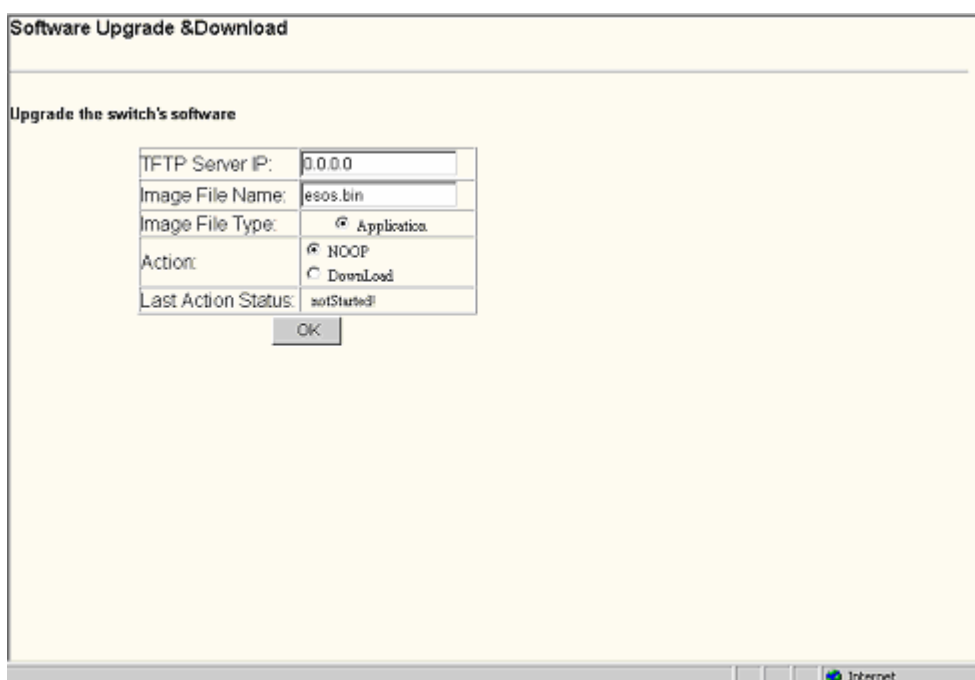


图 7-6 download or upload application file

界面中各项的含义说明如下：

- ◆ TFTP Server IP: 软件所在的 TFTP 服务器的 IP 地址；

- ◆ image File Name: TFTP 服务器上的镜像文件所在的路径和文件名;
- ◆ image File Type: 上传或下载的镜像文件类型, 包括两种类型: 应用文件和配置文件;
- ◆ action: 软件升级的动作, 支持三种操作: 不动作、download、upload;
- ◆ Last action status: 最后一个动作完成后的结果, 无论成功与否。

点击第二个“Download or Upload”, 除了 **image File Type** 有所变动外, 其它操作同图 7-6 所示完全相同。

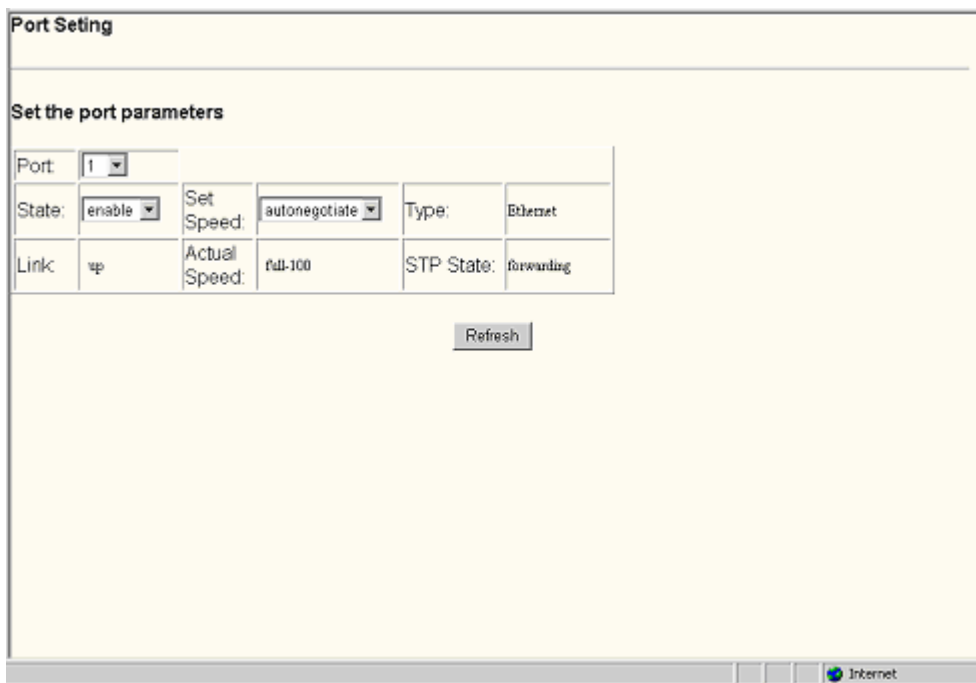
 **注意:** 在使用上面的命令进行上传或者下载的时候, 必须把网线连接到交换机的端口 1 上。

7.2.1.6 网络监视信息 (Networks Monitor)

点击配置页面左侧的“Networks Monitor”路径下的“Statistims”, 会看到端口的统计信息列表。

7.2.1.6.1 端口利用率 (Port Utilization)

点击“Port Utilization”, 会进入如图 7-7 所示界面。



Port:	1				
State:	enable	Set Speed:	autonegotiate	Type:	Ethernet
Link:	up	Actual Speed:	full-100	STP State:	forwarding

Refresh

图 7-7 Port Utilization

该界面同 7-5 的界面的部分功能相同, 可以对选定的某个端口进行配置, 包括端口状态、端口速率和双工模式及端口类型等。

7.2.1.6.2 端口收发报文统计 (Port Packet Analysis)

点击“Port Packet Analysis”，会进入如图 7-8 所示界面。该界面显示了某端口所处理的出错数据包的统计信息，包括：

RxPkts: 该端口收到的报文总数；

TxPkts: 该端口发出的报文总数；

Port Link Reports

Analysis the port's incoming/outgoing octets and packets

Port:	1	
Analysis		
Rx Pkts	45417	Tx Pkts 23548

图 7-8 Port Packet Analysis

7.2.1.6.3 VLAN 状态 (VLAN Status)

在配置页面左侧“Status”菜单下，点击“VLAN Status”，进入 GVRP 状态表，该表显示了目前的 VLAN 配置，包括：

VID: VLAN 标识符；

Status: 状态，静止态；

Create Time: 创建时间，日一小时一分一秒；

Current Egress Ports: 目前的输出端口，M 表示该端口为 VLAN 的成员；

Current Untagged Ports: 目前的 Untagged 端口，U 表示该端口为 Untagged 端口。

Current VLAN Configuration

Unit: 1

(-None, M=Member, U=Unagged)

VID	1																									
FID	1																									
Status	Static																									
Create Time	0-Days 0-Hours 0-Minutes 0-Seconds																									
Current Egress Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
Current Untagged Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Refresh

Next

Prev

图 7-9 VLAN STATUS

7.2.1.7 修改密码设置 (Password Changed)

在页面左侧的主菜单，选择“Password Changed”，将出现如下图所示界面：

Password Modification

New Password

RetypeNewPassword

Apply

Save

图 7-10 Password Change

7.2.1.8 存贮改变 (Save Change)

在页面左侧的主菜单，选择“Save Change”，将出现如下图所示界面：

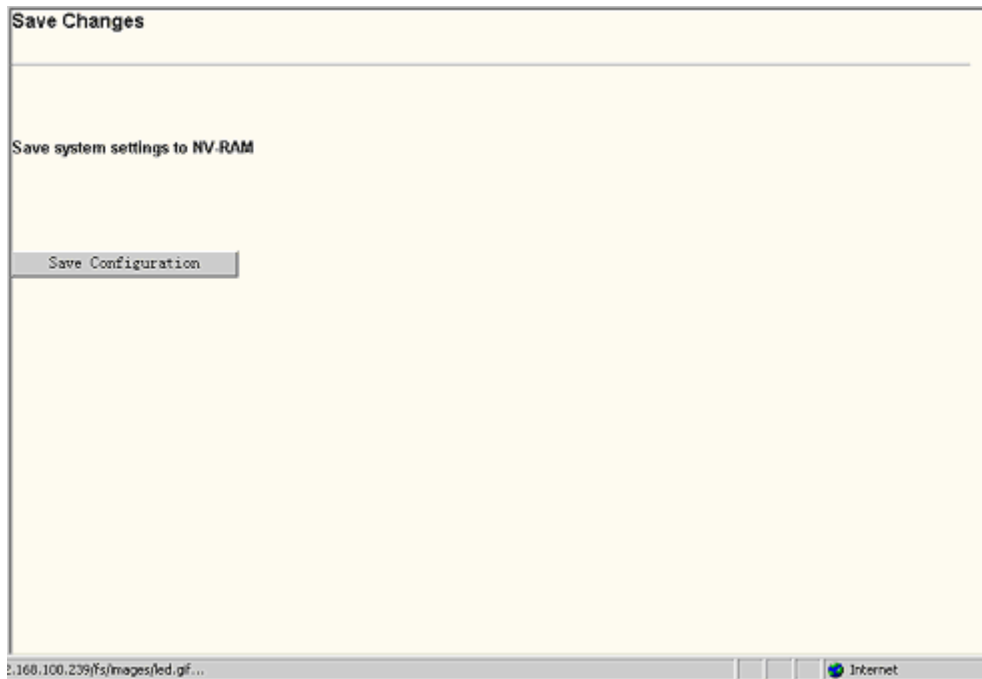


图 7-11 Save Changes

如果想将当前所有更改的设置值保存到交换机的闪存（flash memory），那么，按 Save Configuration 即可。一旦设置值存入 NV-RAM 中，它们将成为交换机的默认设置。

7.2.1.9 重启系统（Restart System）

在页面左侧的主菜单，选择“Restart System”，可以根据用户选择重新启动交换机。

通过下拉菜单也可以选择“reset”，实现热启动

通过下拉菜单也可以选择“reset factory default”，恢复出厂默认设置。在执行“reset factory default”之前，请务必确定是否需要进行此操作。一旦执行了此操作，那么交换机所有存贮在 NV-RAM 内的设置（包括 TCP/IP 协议设置、SNMP 参数、端口上所有功能的设置、以及安全设置等）都将被删除，恢复为出厂时的缺省值。

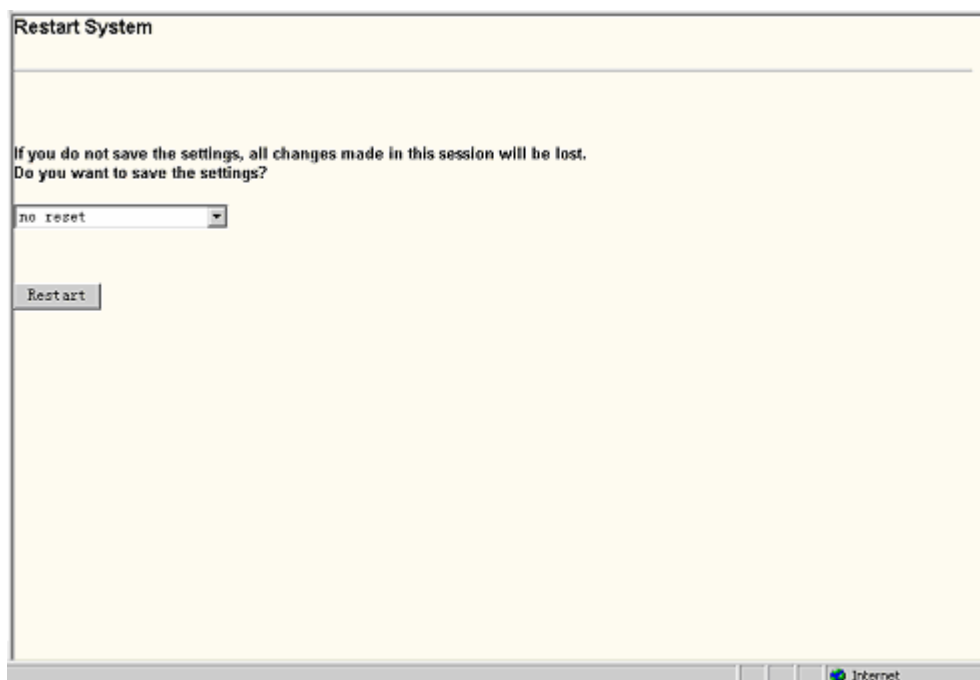


图 7-12 System Restart

7.2.2 高级配置 (Advances Setup)

7.2.2.1 生成树配置 (Spanning Tree)

UFS-2400NW 交换机支持 IEEE802.1D 生成树协议，允许用户创建备份路径，以保证网络的高可用连接性。有关生成树协议的详细内容，请参阅本手册的 5.7 节。

7.2.2.1.1 交换机生成树配置 (STP Switch Settings)

如果想配置交换机的生成树功能，请在图 7-14 所示的各项中填入相应的参数，然后按 Apply 按钮。

STP Switch Settings

Configure the switch's global STP settings.
STP must be enabled on the switch before it can be enabled on a particular port.

STP Designated Root	8000 00 0C FE 01:17:60
Priority	32768
Hello Time (1/100 Second)	200
Forward Delay (1/100 Second)	1500
Max Age (1/100 Second)	2000
Root Port	0
Root Cost	0
Topology Changes	0
Aging Time (Second)	300

Refresh Apply Save

Internet

图 7-13 STP Switch Settings

界面中各项含义说明如下：

STP Designated Root: STP 指定的根桥的 MAC 地址；

Priority: 为交换机设定的 Priority，能设置成 0 到 65535 中的一个数值。0 代表最高优先权。这个数值将在网络交换机间的选举过程中使用来决定那一个交换机是根交换机。一个低交换机表明高优先权，并且这个交换机被选为根交换机的可能性也较高。

Hello Time: Hello Time 能被设置为从 1 到 10 秒中的一个值。这是根网桥发送两个通知其它交换机它是根网桥的 BPDU 包的发送时间间隔。如果你为你的交换机设置了一个 Hello Time，并且它不是根网桥，设置 Hello Time 将在你的交换机成为根网桥时被使用。

 **注意：** Hello Time 不能比 Max. Age 长。另外，将要产生一个配置错误。

Forward Delay: Forward Delay 能设置成 4 到 30 秒中的一个值。在从阻塞状态转换到转发状态时，这是任何交换机端口在侦听情况下所花费的时间。

Max Age: Max. Age 能被设置为从 6 到 40 秒中的一个值。在 Max. Age 结束时，如果仍没有从根网桥接收到一个 BPDU，你的交换机将开始发送它自己的 BPDU 给其它所有交换机来确定成为根网桥。如果证实你的交换机有最低网桥标识符，它将成为根网桥。

 **注意：** 当设置上面的参数时，应遵守如下公式：

$$\text{Max. Age} < 2 \times (\text{Forward Delay} - 1 \text{ second})$$

$$\text{Max. Age} > 2 \times (\text{Hello Time} + 1 \text{ second})$$

Root Port: 根端口，每台交换机都有一个根端口，这个端口到根桥的开销路径最低。

Root Cost: 该交换机到根桥的路径开销。

Aging Time: MAC地址表的老化时间，老化时间的数值范围从10 秒~1,000,000 秒，缺省值为300 秒。该老化时间必须是能被3整除的整数。



注意：界面上除Priority 、 Aging Time的所有值的配置单位为1/100秒。

7.2.2.1.2 端口生成树配置（STP Port Settings）

端口生成树配置界面如图 7-15 所示，在相应的窗口中输入欲设置的值，然后按 Apply。

STP Port Settings

Configure STP for individual ports.

Unit: 1 Port: 1

Bridge Port	Enable	Path Cost	Priority	Fwd Transitions	State
1	enable	19	128	1	forwarding
1	enable	19	128	1	forwarding
2	enable	10	128	1	disabled
3	enable	10	128	1	disabled
4	enable	10	128	1	disabled
5	enable	10	128	1	disabled
6	enable	10	128	1	disabled
7	enable	10	128	1	disabled
8	enable	10	128	1	disabled
9	enable	10	128	1	disabled
10	enable	10	128	1	disabled
11	enable	10	128	1	disabled
12	enable	10	128	1	disabled
13	enable	10	128	1	disabled

图 7-14 STP Port Settings

界面中各项含义说明如下：

Bridge Port: 显示该交换机所有的物理端口号；

Enable: 使能或禁止该端口的 STP 功能；

Path Cost: 路径开销，它是一个可变的参数，可以根据生成树算法的指标进行修改。每个 10Mbps、100Mbps 和 1000Mbps 网段的路径开销值为 100、19 和 4。

Priority: 口优先权可设置为从0 到255 中的一个数值。较小的数值表示端口有较大的可能性被选作为根端口。

Fwd Transitions: 该端口从学习态到转发态的转变次数；

State: 该端口的STP状态（阻塞、侦听、学习、转发态等）。

7.2.2.1.3 广播风暴过滤控制

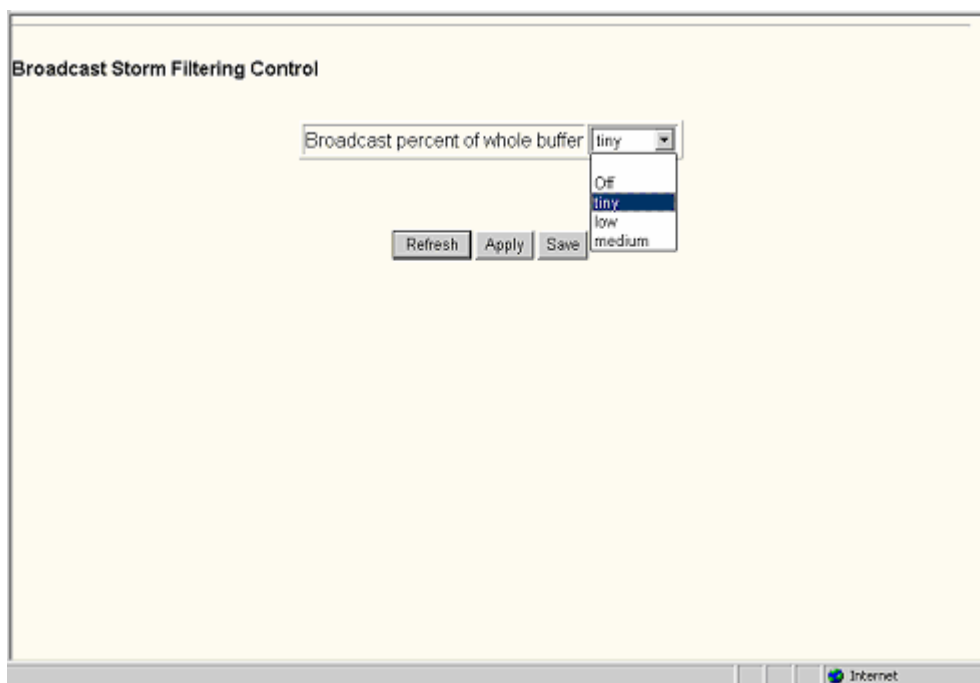


图 7-15 Broadcast Storm Filtering Control

该配置界面用于广播风暴过滤控制，可以选择的控制程度在上面列出。

7.2.2.1.4 MAC 地址绑定

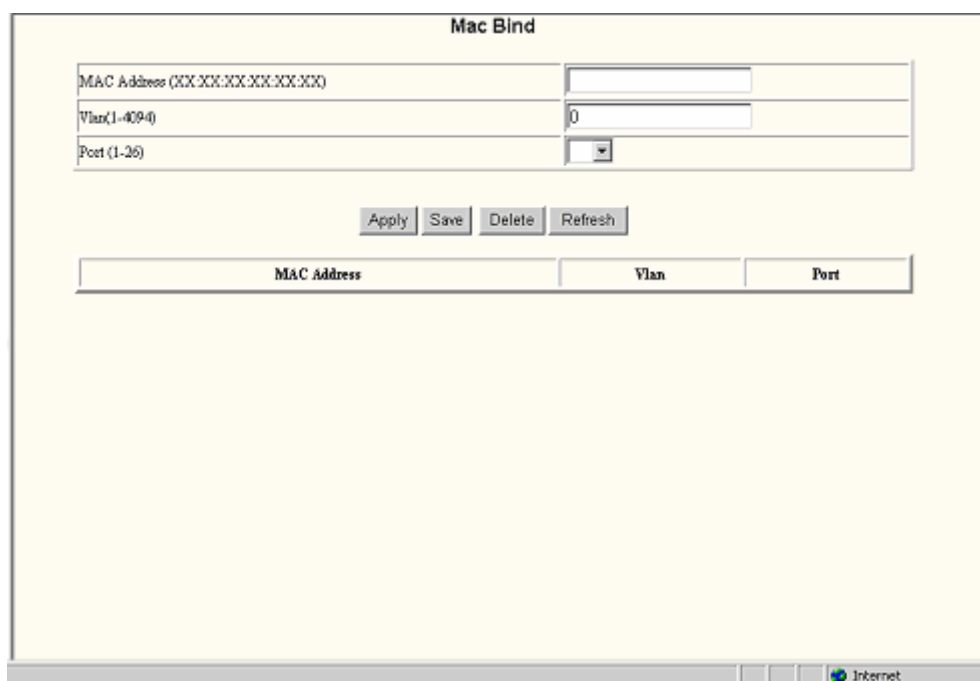
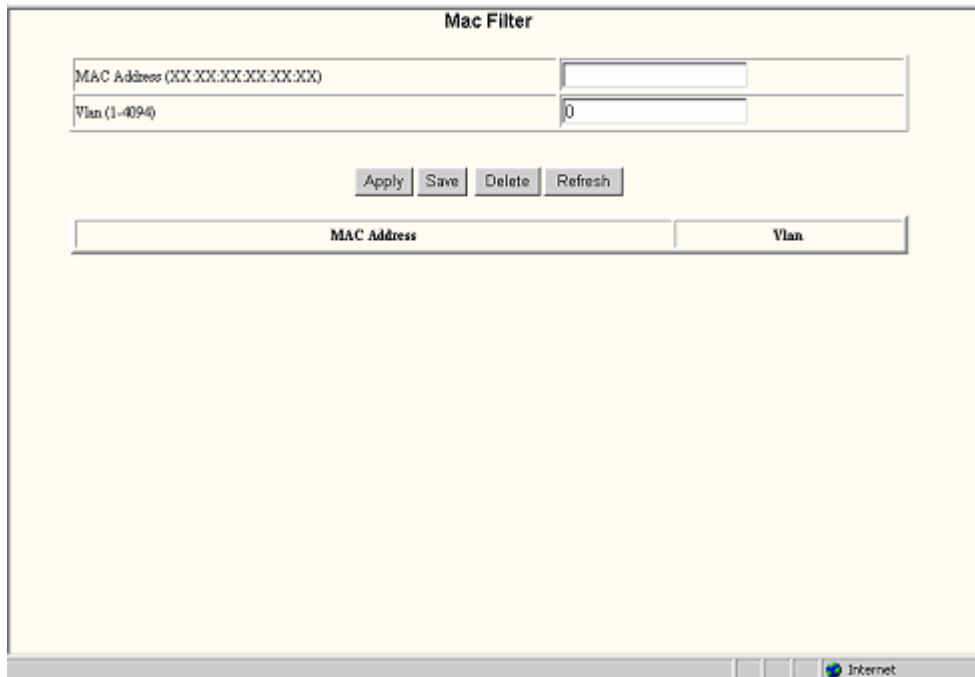


图 7-18 MAC 地址绑定

该配置界面用于地址绑定，是将 MAC 地址和 Vlan ID、端口绑定。符合条件的 MAC 地址的报文才可以转发。

 注意：必须先创建 VLAN 再进行 MAC 地址绑定，在 Port-Based VLAN 下 vlan 只能选择 1。

7.2.2.1.5 MAC 地址过滤



The image shows a web-based configuration interface titled "Mac Filter". It contains two input fields: "MAC Address (XX:XX:XX:XX:XX:XX)" and "Vlan (1-4094)". Below these fields are four buttons: "Apply", "Save", "Delete", and "Refresh". At the bottom, there is a table with two columns: "MAC Address" and "Vlan". The table is currently empty. The interface has a light yellow background and a grey border.

图 7-19 MAC 地址过滤

该配置界面用于 MAC 地址过滤，是将 MAC 地址和 Vlan ID 绑定。符合条件的 MAC 地址的报文将被过滤。

 注意：必须先创建 VLAN 再进行 MAC 地址绑定。该绑定和 802.1x 的端口使能有冲突，在配置过程中，如果某个端口已经使能 802.1x，该端口可以同时进行 MAC 地址的绑定；但如果在该端口已经和 MAC 地址绑定的情况下禁止该端口的 802.1x，则操作失败，必须先解除绑定，才能禁止该端口的 802.1x。一般来讲，将某个 MAC 和某个端口绑定后，就不需要进行 802.1x 的认证。

7.2.2.2 QOS配置 (Configure QOS)

在配置界面左侧的主菜单中点击“QOS default priority”，则进入基于端口的优先级配置界面。

Priority Based on Port

Select priority based on port or disable priority based on per port basis.

Unit: 1 Port: 1

Bridge Port	Priority
1	802-1p
1	802-1p
2	802-1p
3	802-1p
4	802-1p
5	802-1p
6	802-1p
7	802-1p
8	802-1p
9	802-1p
10	802-1p
11	802-1p

图 7-20 QoS default priority

该页面可以配置每个端口的 QoS 优先级，进而提供和识别 **QoS** 专用的包优先级。可以通过 **2 层 VLAN** 的优先标签来给数据包定义优先级别，并根据优先级进行数据包转发或丢弃，从而保证了服务质量。该优先级的设置遵循 **802.1p** 标准。

7.2.2.3 端口镜像配置 (Mirroring Configuration)

UFS-2400NW 交换机允许用户将某个或某几个端口收发的所有数据包复制一份到另外一个端口，以使用户能够将一台监视设备（如 Sniffer 或 RMON Probe）连接到镜像端口上，来查看通过前一个或几个端口的所有数据包的详细情况。

选择配置界面左侧主菜单的“Mirroring Configuration”，将出现图 7-21 所示的界面。下面对各项分别进行介绍：

Mirror Mode: 提供源端口的镜像操作模式，该模式提供四种选择：none、ingress、egress、all。none 表示该端口不进行镜像操作；ingress 表示只对该端口的输入报文进行源端口镜像；egress 表示只对该端口的输出报文进行源端口镜像；all 表示对该端口的所有报文（包括输入和输出）进行源端口镜像。

Mirror to Port: 用于选择镜像的目的端口，用户可以在该端口上连接监视或故障排除的设备，这样就可以监视源端口上发生的所有情况。

Mirroed Port: 用于选择镜像的源端口，该端口的数据包可以被复制到目的端口。



注意：不能将一个高速端口镜像到一个低速端口上。例如，如果将一个 100Mbps 端口镜像到一个 10Mbps 端口，会造成吞吐量承受能力的问题。因此，源端口速率应和目的端口速率相同，或者更低，而且目的端口不能是端口干路（Trunk Group）的成员。

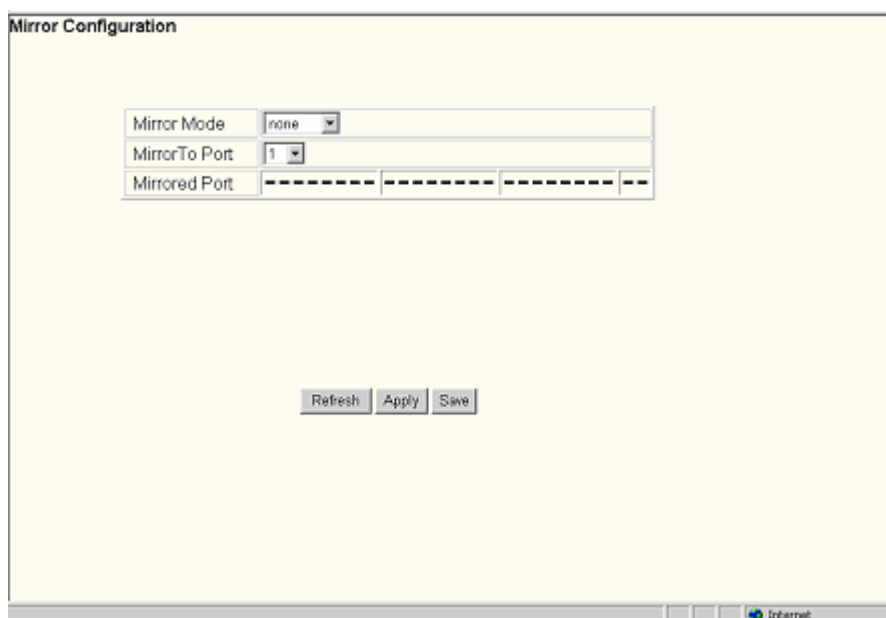


图 7-21 Mirroring configuration Control

7.2.2.4 VLAN配置 (VLAN Configuration)

点击配置界面左侧主菜单中的“VLAN Configuration”，会下拉出四项配置。

7.2.2.4.1 VLAN Config 配置

VLAN Config配置如下图所示，通过下拉菜单选择VLAN类型。

Vlan mode Switch & GVRP Enable/Disable

VLAN mode Prompt:
 (1)Chang VLAN mode will clear ip,pvid ,mac-bind&mac-filter config.
 Above-mentioned config will be cleaned & should be reconfigured!!!
 (2)When Port-Based Vlan enabled
 -- Above-mentioned config should specify the vid to be No.1;
 -- GVRP will be disabled automatically.

GVRP Prompt:
 GVRP could work with 802.1Q Vlan only, if Port-Based Vlan enabled,the GVRP will be disabled automatically.
 When GVRP Enabled,ports will be able to join VLANs dynamically.
 When GVRP disabled,only statically configured ports can be membered.

VLAN mode 802.1Q
 GVRP enable disable

Refresh Apply Save

图 7-22 VLAN Config

7.2.2.4.2 Port-Based VLAN 配置(Port-Based VLAN)

Static VLAN Configuration

Unit: 1

(- =None, M=Member)

VID	Name	1	8	9	16	17	24	25
		-	-	-	-	-	-	-

0001 Default

Refresh

Apply

Save

Delete

图 7-23 Port-Based VLAN Configuration

交换机保留了一个VLAN，VID = 1，称之为DEFAULT_VLAN。出厂时缺省设置将交换机的所有端口都分配至DEFAULT_VLAN。

上图所示为 Port Q VLAN 配置界面，在该界面上可以配置哪几个端口归属于哪个VLAN，不同的 VLAN 用不同的 VID 标识。在 VID 的文本框中输入有效的 ID 号，还可以为该 VLAN 命名。

在对某个端口进行选择时，会出现“-”、“M”两种符号，每个符号代表一定的意义：
- (None)：表示该端口将被禁止成为静态VLAN 的成员，但允许该端口动态地加入任何VLAN。
M (Member)：指端口作为VLAN 中的一个的成员。

同时当当前的VLAN类型和配置的页面不符的时候，页面就会变暗，不能设置。

7.2.2.4.3 802.1Q VLAN 配置 (802.1Q VLAN)

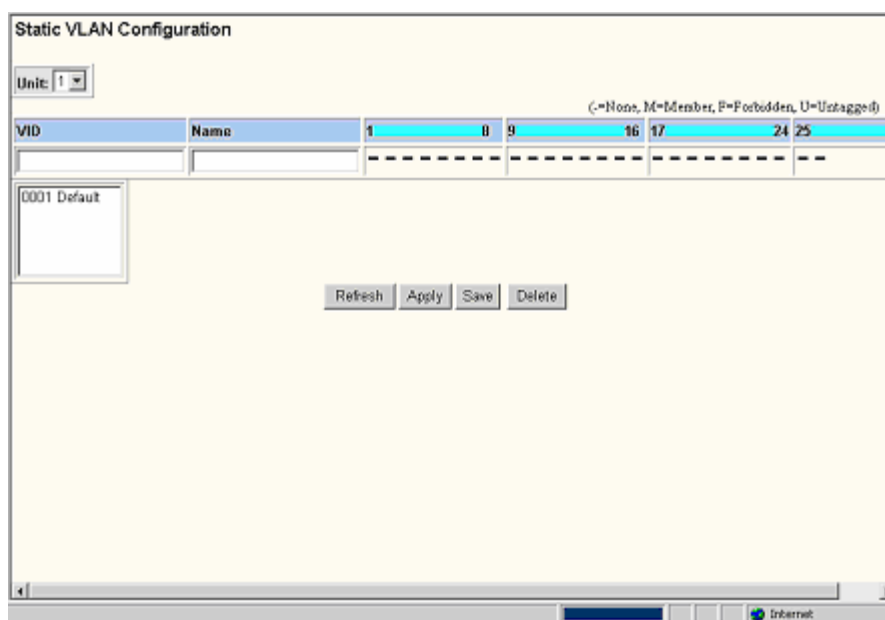


图 7-23 802.1Q VLAN Configuration

交换机保留了一个VLAN，VID = 1，称之为DEFAULT_VLAN。出厂时缺省设置将交换机的所有端口都分配至DEFAULT_VLAN。

上图所示为 802.1Q VLAN 配置界面，在该界面上可以配置哪几个端口归属于哪个VLAN，不同的VLAN用不同的VID标识。在VID的文本框中输入有效的ID号，还可以为该VLAN命名。

在对某个端口进行选择时，会出现“—”、“M”、“U”四种符号，每个符号代表一定的意义：

— (None)：表示该端口将被禁止成为静态VLAN的成员，但允许该端口动态地加入任何VLAN。

M (Member)：指端口作为VLAN中的一个带标记的成员。当一个不带标记的包传输时，包头被改变为包含32位标记的PVID。当一个带标记包存在时，包头将不改变。

U (Untagged)：指端口作为一个不带tag标记的VLAN端口。当一个untagged包通过此端口传输时，此包头保持不便。当一个tagged包在端口中存在时，此包也将变为一个不带tag标记的包。

7.2.2.4.4 IEEE802.1Q 端口设置 (IEEE802.1Q Port Settings)

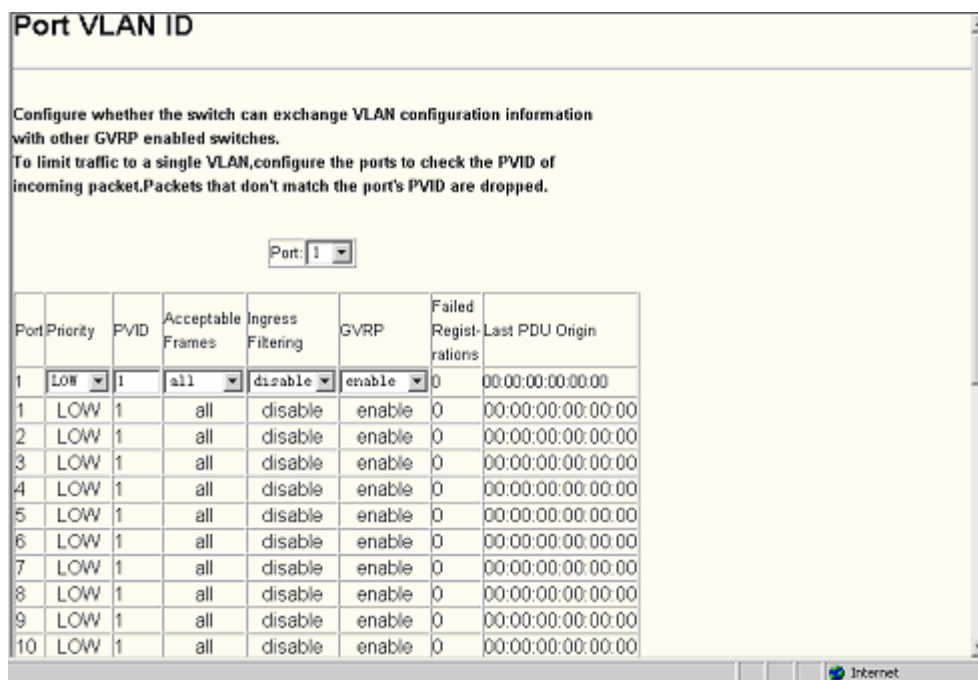


图 7-24 802.1Q Port Settings

一个802.1Q VLAN 端口配置界面如上图所示，各项说明如下：

PVID - PVID 定义了交换机将向哪一个VLAN 转发数据包，以及什么时候数据包会需要转发到另一台交换机的端口上，或者网络中的某个地方。另外，用户也可以定义某个端口同时属于多个VLAN (VIDs)，使得它可以接收网络中多个VLAN 的数据包。PVID 和VID 这两个变量用于控制端口发送和接收VLAN 数据流的能力，而两者之间的区别在于后者还允许信息可以在多个VLAN 间共享。

Ingress Filtering - 如果入端口的Ingress Filtering 功能被设置为disable 时，那么，交换机将检查每一个流经该端口的数据包，以决定流经的数据包是否是其所属VLAN 中的成员。然后，做出如下两个动作中的一个：如果该端口所属的VLAN 与数据包中所标记的VLAN 不是同一个，那么，该数据包将被丢弃，反之，将被转发。而如果入端口的Ingress Filtering 功能被设置为enable时，那么，交换机将以通常的方式处理所有流经该端口的数据包。

GVRP - VLAN 组注册协议 - 将允许端口动态加入一个VLAN 组。

Priority: 设置该端口的优先级，同图7-20 QOS的设置是一样的。

7.2.2.5 链路聚合配置 (Link Aggregation)

点击配置界面左侧主菜单中的“Link Aggregation”，进行链路聚合配置。

链路聚合是由几个端口组合在一起组成的，而且它还可作为一个单一连接来使用，并提供若干单一连接带宽。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干

网络的服务器或服务器群。

注意：UFS-2400NW 允许建立最多7 个链路聚合组，每组包括最多4 个连接（端口）。集合的所有在组中的端口必须是同一个VLAN 中的成员。而且，连接端口必须都是相同速率的，并且都可以配置为全双工。链路聚合策略为目的MAC、源MAC和源端口。

组中的最小编号端口的配置变成对集合组中所有端口的配置。这个端口被称做组的基础端口，并且包括VLAN 配置的所有配置选项能应用在基础端口被应用的整个链路聚合组中。负载平衡自动的应用到在集合组中的连接，并且组中的连接失败引起网络通信量被导向组中的保持端口。

注意：生成树协议在交换机层把一个链路聚合像一个单一连接来对待。在端口层，STP 将使用基础端口的端口参数来计算端口代价和决定链路聚合组的状态。如果在交换机上配置两个多余的链路聚合组，STP 将阻塞一个组，并且STP 以同样的方式阻塞一个有多余连接的单一端口。

7.2.2.5.1 显示干路组（Trunk Show Table）

Show Trunk Table

This table can show the trunk that configure by static or LACP.

Trunk Group	1	9	17	25
1	M-----			
2	-M-----			
3	--M-----			
4	---M-----			
5	----M-----			
6	-----M-----			
7	-----M-----			
8	-----M-----			
9	-----M-----			
10	-----M-----			
11	-----M-----			
12	-----M-----			
13	-----M-----			
14	-----M-----			
15	-----M-----			
16	-----M-----			
17	-----M-----			
18	-----M-----			
19	-----M-----			

图 7-25 Show Trunk Table

该配置界面显示当前静态 Trunk 的聚合状态

7.2.2.5.2 配置静态干路（Trunk Static Table）

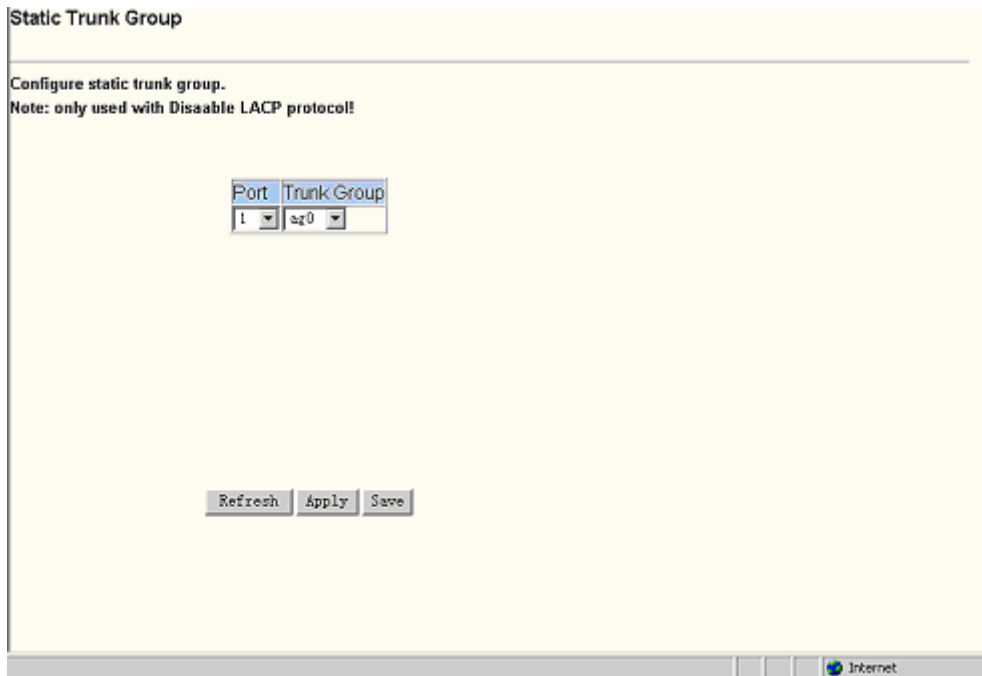


图 7-26 Static Trunk Group

该界面用于配置静态 Trunk，在“port”下拉菜单中用户可以选择要聚合的物理端口号，“Trunk Group”下拉菜单中用户选择聚合的组标识。

 **注意：**最多支持 7 个聚集组（trunk group），每个组中最多可以包含 4 个端口。选择同一组标识则为同一组。

7.2.2.6 认证配置（Authentication）

UFS-2400NW 提供 802.1x 认证方法。WEB 管理界面左侧的“Authentication”菜单下有两个配置子菜单，分别是 Radius、802.1x 的配置。

7.2.2.6.1 Radius（配置）（Radius Configuration）

点击“Radius Configuration”菜单，会显示如下配置页面：

Radius Server and client Settings

Configure radius server and client for your switch.

Radius Server Status:

Radius Client Account Receive Port:

Radius Client IP Address:

Radius Client Authen Receive Port:

Entry	server index	server type	transmit interval	max transmit times	destination IP address	receive port	secret
new	0		0	0		0	

Apply Save Delete Refresh

图 7-27 Radius Server and client Settings

该页面完成对 Radius server 和 Radius client 的配置，各项说明如下：

Radius Client Account Receive Port: Radius Client 侧计费报文接收端口号，协议缺省配置为 1813；

Radius Client IP Address: Radius Client 侧的 IP 地址，一般为交换机某个接口的 IP 地址；

Radius Client Authen Receive Port: Radius Client 侧认证报文接收端口号，协议缺省配置为 1812；

Radius Client Encrpy Method: Radius Client 侧密码加密算法，目前支持两种加密算法：CHAP 和 PAP。

表格形式的设置方式用于配置 Radius server，系统支持可以配置多个 Radius Server，最大支持 6 个 Radius Server。

server index: Radius Server 的索引，为 0-5 的数字；

server type: Radius Server 的类型，支持二种 Server 类型，认证 Authentication、计费 Accounting。

transmit interval: Radius client 向 Radius Server 发送请求报文后，在收到 Radius Server 响应前决定重发请求报文的时间间隔，缺省值为 10s。

max transmit times: Radius client 向 Radius Server 发送重传报文的最多重复次数，缺省值为 3。

EStination IP address: Radius Server 的 IP 地址；

receive port: Radius Server 接收 radius 报文的端口号，协议缺省的认证请求报文接收端口号为 1812，协议缺省的计费请求报文接收端口号为 1813；

secret: 长度为 3-256 的字符串，作为 Radius Server 和 Radius Client 间的共享密钥。

7.2.2.6.2 802.1x 配置 (Dot1x Configuration)

802.1x 配置界面如下图 7-28 所示：

Port	Enable
1	disable
1	disable
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

图 7-28 802.1x configuration

Dot1x enable or disable: 是否启动 802.1x 认证方式的总的开关：使能或禁止；

针对每个端口号也设置了一个使能禁止开关，目的是用户可灵活控制认证形式：有些端口需要进行认证才能访问 Internet，有些端口不需要通过认证直接可以上网。

注意： 端口进行认证使能的前提是 802.1x 全局系统已经使能；如果关闭全局 802.1x 功能，各端口的使能配置会自动关闭。如果该端口已经进行 MAC 地址绑定，则不能关闭该端口的 802.1x 功能，必须先解除绑定。

如果用户发现了本产品的任何错误，或者用户有任何意见和建议，请发送给我们。

Web: <http://www.ucom.com.cn>

E-mail: support@ucom.com.cn

Tel: 0755-83890769 / 83890771 / 83891188

Fax: 0755-83891000

公司地址: 深圳市福田区泰然工贸园劲松大厦 16D