Sun Fire™ B1600 刀片式系统机箱交换机管理指南

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

部件号 817-1895-10
2003 年 4 月，修订版 A

请将对本文档的意见发送到：docfeedback@sun.com

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版权所有。

Sun Microsystems, Inc. 拥有本文档所提到产品中使用的技术的知识产权。需要特别说明的是，这些知识产权可能包括 （但不限于） http://www.sun.com/patents 上列出的一项或多项美国专利，以及 Sun 在美国和其它国家/地区已申请到或正在申请的一项或多项专利。

本文档及其相关产品按照限制其使用、复制、分发和反编译的许可证进行分发。未经 Sun 及其许可证颁发机构 （如果有）的书面授权，不得以任何方式、任何形式复制本产品或本文档的任何部分。

第三方软件，包括字体技术，由 Sun 供应商提供许可和版权。

本产品的某些部分从 Berkeley BSD 系统派生而来，经 University of California 许可授权。 UNIX 是在美国和其它国家/地区注册的商标，经 X/Open Company, Ltd. 独家许可授权。

Sun、 Sun Microsystems、 Sun 徽标、 AnswerBook2、 docs.sun.com、 Sun Fire 和 Solaris 是 Sun Microsystems, Inc. 在美国和其它国家/地区的商标或注册商标。

所有 SPARC 商标都按许可证使用，是 SPARC International, Inc. 在美国和其它国家/地区的商标或注册商标。具有 SPARC 商标的产品都基于 Sun Microsystems Inc. 开发的体系结构。

OPEN LOOK 和 Sun™ 图形用户界面是 Sun Microsystems, Inc. 为其用户和许可证持有者开发的。 Sun 承认 Xerox 在为计算机行业研究和开发可视或图形用户界面方面所做出的先行努力。 Sun 以非独占方式从 Xerox 获得 Xerox 图形用户界面的许可证，该许可证也涵盖实施 OPEN LOOK GUI 且遵守 Sun 书面许可证协议的 Sun 的许可证持有人。

本资料按 “现有形式”提供，不承担明确或隐含的条件、陈述和保证，包括对特定目的的商业活动和适用性或非侵害性的任何隐含保证，除非这种不承担责任的声明是不合法的。

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版权所有。本产品受一项或多项美国专利保护；专利正在申请中。

本发行版本可能包含由第三方开发的材料。

Sun、Sun Microsystems、Sun 徽标、Java、Solaris、Sun Fire 和 100% Pure Java 徽标是 Sun Microsystems, Inc. 在美国和其它国家/地区的商标或注册商标。

所有 SPARC 商标都按许可证使用，是 SPARC International, Inc. 在美国和其它国家/地区的商标或注册商标。具有 SPARC 商标的产品都基于 Sun Microsystems Inc. 开发的体系结构。

本产品受美国出口控制法律管理和控制，而且可能受其它国家/地区的出口或进口法律管辖。核能、导弹、生化武器或核舰艇的最终使用或最终用户，无论是直接的还是间接的，都受到严格禁止。出口或转口到被美国禁运的国家/地区或上了美国出口黑名单的实体 （包括但不限于被拒绝的个人和明确指定的国家/地区名单），都受到严格的禁止。

任何备用或替换 CPU 的使用，仅限于遵守美国出口法律规定出口的产品的维修或一对一 CPU 替换。除非美国政府授权，否则严格禁止将 CPU 用于产品升级。

请
回收利用

Adobe PostScript

目录

序言　xv

1.　简介　1-1

1.1　概述　1-1

1.1.1　交换机体系结构　1-2

1.1.2　访问交换机管理应用程序的方法　1-2

1.2　硬件说明　1-3

1.2.1　以太网端口　1-3

1.2.1.1　上行链接端口　1-3

1.2.1.2　内部端口　1-3

1.2.2　状态指示灯　1-4

1.3　交换机的功能　1-5

1.4　默认设置　1-7

2.　初始配置　2-1

2.1　连接到交换机接口上　2-2

2.1.1　配置选项　2-2

2.1.1.1　通过内置的交换机接口配置交换机　2-2

2.2 启用 SNMP 管理权限 2-3

2.2.1 社区字符串 2-3

2.2.2 陷阱接收装置 2-4

3. 管理概述 3-1

3.1 使用 Web 界面 3-2

3.1.1 浏览 Web 浏览器界面 3-3

3.1.1.1 主页 3-3

3.1.1.2 配置选项 3-4

3.1.2 面板显示 3-4

3.1.3 主菜单 3-5

3.2 基本配置 3-7

3.2.1 显示系统信息 3-7

3.2.2 设置 IP 地址 3-10

3.2.2.1 手动配置 3-12

3.2.2.2 使用 DHCP/BOOTP 3-14

3.2.3 显示交换机软件版本 3-16

3.2.4 管理固件 3-18

3.2.4.1 从服务器下载系统软件 3-18

3.2.5 保存或恢复配置设置 3-21

3.2.5.1 从服务器下载配置设置 3-21

3.2.6 配置用户验证 3-23

3.2.7 配置 SNMP 3-27

3.2.7.1 配置对 SNMP 协议的访问 3-27

3.2.7.2 指定陷阱管理器和陷阱类型 3-28

3.3 配置全局网络协议 3-31

3.3.1 VLAN 配置 3-31

3.3.1.1 显示基本 VLAN 信息 3-33

3.3.1.2 启用或禁用 GVRP （全局设置） 3-36

3.3.1.3 配置 VLAN 3-37
3.3.1.4 向 VLAN 添加静态成员 3-39
3.3.2 多点传送配置 3-42
3.3.2.1 配置 IGMP 侦听参数 3-43
3.3.2.2 指定与多点传送路由器相连的接口 3-45
3.3.2.3 配置多点传送服务 3-48
3.3.3 广播风暴控制 （全局设置） 3-51
3.3.4 生成树算法配置 3-53
3.3.4.1 配置基本 STA 设置 3-53
3.3.4.2 配置高级 STA 设置 3-59
3.3.5 服务类别配置 3-60
3.3.5.1 设置接口的默认优先级 3-60
3.3.5.2 将 CoS 值映射到传出队列 3-62
3.3.5.3 设置通信类别的服务权级 3-65
3.3.5.4 将第 3/4 层优先级映射到 CoS 值 3-66
3.3.5.5 映射 IP 优先权 3-68
3.3.5.6 映射 DSCP 优先级 3-70
3.3.6 地址表设置 3-72
3.3.6.1 显示地址表 3-72
3.3.6.2 更改有效期 3-74
3.4 端口配置 3-75
3.4.1 显示连接状态 3-75
3.4.2 配置接口连接 3-79
3.4.3 端口聚合组配置 3-83
3.4.3.1 使用 LACP 动态配置聚合组 3-84
3.4.3.2 静态配置聚合组 3-87
3.4.4 配置接口的 VLAN 行为 3-89
3.4.5 配置静态地址 3-95

3.4.6 管理生成树算法的接口 3-98
3.4.6.1 显示 STA 的当前接口设置 3-98
3.4.6.2 配置 STA 的接口设置 3-102
3.4.6.3 检查接口的 STA 协议状态 3-105
3.4.7 过滤来自管理端口的通信 3-106
3.5 监视端口和管理通信 3-110
3.5.1 配置端口镜像 3-110
3.5.2 显示端口统计信息 3-112
3.5.3 显示 SNMP 统计信息 3-120
3.5.4 配置消息日志 3-124

4. 命令行参考 4-1
4.1 使用命令行界面 4-1
4.1.1 访问 CLI 4-1
4.1.1.1 控制台连接 4-1
4.1.1.2 Telnet 连接 4-2
4.1.2 输入命令 4-4
4.1.2.1 关键字和参数 4-4
4.1.2.2 最短缩写 4-4
4.1.2.3 命令完成 4-4
4.1.2.4 获取命令的帮助 4-4
4.1.2.5 显示命令 4-5
4.1.2.6 查找部分关键字 4-6
4.1.2.7 取消命令的效果 4-6
4.1.2.8 使用命令历史记录 4-6
4.1.2.9 了解命令模式 4-6
4.1.2.10 执行命令 4-7
4.1.2.11 配置命令 4-7
4.1.2.12 处理命令行 4-9

4.2 命令组 4-10
4.3 详细的命令说明 4-11
4.3.1 常规命令 4-11
4.3.1.1 enable 4-12
4.3.1.2 disable 4-13
4.3.1.3 configure 4-13
4.3.1.4 show history 4-14
4.3.1.5 reload 4-15
4.3.1.6 end 4-15
4.3.1.7 exit 4-16
4.3.1.8 quit 4-16
4.3.2 闪存 / 文件命令 4-17
4.3.2.1 copy 4-17
4.3.2.2 delete 4-20
4.3.2.3 dir 4-20
4.3.2.4 whichboot 4-22
4.3.2.5 boot system 4-23
4.3.3 系统管理命令 4-24
4.3.3.1 hostname 4-25
4.3.3.2 username 4-26
4.3.3.3 enable password 4-27
4.3.3.4 ip http port 4-28
4.3.3.5 ip http server 4-28
4.3.3.6 jumbo-frame 4-29
4.3.3.7 logging on 4-30
4.3.3.8 logging history 4-31
4.3.3.9 clear logging 4-32
4.3.3.10 show logging 4-33

4.3.3.11 show startup-config 4-34
4.3.3.12 show running-config 4-36
4.3.3.13 show system 4-38
4.3.3.14 show users 4-39
4.3.3.15 show version 4-40
4.3.4 验证命令 4-41
4.3.4.1 authentication login 4-42
4.3.4.2 radius-server host 4-43
4.3.4.3 radius-server port 4-43
4.3.4.4 radius-server key 4-44
4.3.4.5 radius-server retransmit 4-44
4.3.4.6 radius-server timeout 4-45
4.3.4.7 show radius-server 4-45
4.3.4.8 tacacs-server host 4-46
4.3.4.9 tacacs-server port 4-46
4.3.4.10 tacacs-server key 4-47
4.3.4.11 show tacacs-server 4-47
4.3.5 SNMP 命令 4-48
4.3.5.1 snmp-server community 4-48
4.3.5.2 snmp-server contact 4-49
4.3.5.3 snmp-server location 4-50
4.3.5.4 snmp-server host 4-50
4.3.5.5 snmp-server enable traps 4-51
4.3.5.6 show snmp 4-52
4.3.6 线路命令 4-54
4.3.6.1 line 4-55
4.3.6.2 login 4-56
4.3.6.3 password 4-57

4.3.6.4 exec-timeout 4-58
4.3.6.5 password-thresh 4-59
4.3.6.6 silent-time 4-60
4.3.6.7 show line 4-61
4.3.7 IP 命令 4-62
4.3.7.1 ip address 4-62
4.3.7.2 ip dhcp restart 4-64
4.3.7.3 ip dhcp client-identifier 4-65
4.3.7.4 ip default-gateway 4-66
4.3.7.5 show ip interface 4-66
4.3.7.6 show ip redirects 4-67
4.3.7.7 ping 4-67
4.3.7.8 ip filter 4-68
4.3.7.9 show ip filter 4-71
4.3.8 接口命令 4-73
4.3.8.1 interface 4-74
4.3.8.2 description 4-74
4.3.8.3 speed-duplex 4-75
4.3.8.4 negotiation 4-76
4.3.8.5 capabilities 4-77
4.3.8.6 flowcontrol 4-78
4.3.8.7 shutdown 4-80
4.3.8.8 switchport broadcast packet-rate 4-80
4.3.8.9 clear counters 4-81
4.3.8.10 show interfaces status 4-82
4.3.8.11 show interfaces counters 4-83
4.3.8.12 show interfaces switchport 4-85

4.3.9 地址表命令 4-86
4.3.9.1 mac-address-table static 4-87
4.3.9.2 clear mac-address-table dynamic 4-88
4.3.9.3 show mac-address-table 4-88
4.3.9.4 mac-address-table aging-time 4-89
4.3.9.5 show mac-address-table aging-time 4-90
4.3.10 端口安全性命令 4-90
4.3.10.1 port security 4-91
4.3.11 生成树命令 4-92
4.3.11.1 spanning-tree 4-92
4.3.11.2 spanning-tree mode 4-93
4.3.11.3 spanning-tree forward-time 4-94
4.3.11.4 spanning-tree hello-time 4-95
4.3.11.5 spanning-tree max-age 4-95
4.3.11.6 spanning-tree priority 4-96
4.3.11.7 spanning-tree pathcost method 4-97
4.3.11.8 spanning-tree transmission-limit 4-97
4.3.11.9 spanning-tree cost 4-98
4.3.11.10 spanning-tree port-priority 4-99
4.3.11.11 spanning-tree edge-port 4-100
4.3.11.12 spanning-tree protocol-migration 4-100
4.3.11.13 spanning-tree link-type 4-101
4.3.11.14 show spanning-tree 4-102
4.3.12 VLAN 命令 4-104
4.3.12.1 vlan database 4-105
4.3.12.2 vlan 4-105
4.3.12.3 interface vlan 4-106
4.3.12.4 switchport mode 4-107

4.3.12.5 switchport acceptable-frame-types 4-108
4.3.12.6 switchport ingress-filtering 4-108
4.3.12.7 switchport native vlan 4-109
4.3.12.8 switchport allowed vlan 4-110
4.3.12.9 switchport forbidden vlan 4-111
4.3.12.10 show vlan 4-112
4.3.13 GVRP 和网桥扩展命令 4-113
4.3.13.1 switchport gvrp 4-113
4.3.13.2 show gvrp configuration 4-114
4.3.13.3 garp timer 4-115
4.3.13.4 show garp timer 4-116
4.3.13.5 bridge-ext gvrp 4-117
4.3.13.6 show bridge-ext 4-117
4.3.14 IGMP 侦听命令 4-119
4.3.14.1 ip igmp snooping 4-120
4.3.14.2 ip igmp snooping vlan static 4-120
4.3.14.3 ip igmp snooping version 4-121
4.3.14.4 show ip igmp snooping 4-122
4.3.14.5 show mac-address-table multicast 4-122
4.3.14.6 ip igmp snooping querier 4-123
4.3.14.7 ip igmp snooping query-count 4-124
4.3.14.8 ip igmp snooping query-interval 4-125
4.3.14.9 ip igmp snooping query-max-response-time 4-125
4.3.14.10 ip igmp snooping router-port-expire-time 4-126
4.3.14.11 ip igmp snooping vlan mrouter 4-127
4.3.14.12 show ip igmp snooping mrouter 4-128

4.3.15 优先级命令 4-129
4.3.15.1 switchport priority default 4-130
4.3.15.2 queue bandwidth 4-131
4.3.15.3 queue cos-map 4-132
4.3.15.4 show queue bandwidth 4-133
4.3.15.5 show queue cos-map 4-134
4.3.15.6 map ip precedence （全局配置） 4-135
4.3.15.7 map ip precedence （接口配置） 4-135
4.3.15.8 map ip dscp （全局配置） 4-136
4.3.15.9 map ip dscp （接口配置） 4-137
4.3.15.10 show map ip precedence 4-138
4.3.15.11 show map ip dscp 4-139
4.3.16 镜像端口命令 4-140
4.3.16.1 port monitor 4-140
4.3.16.2 show port monitor 4-141
4.3.17 端口聚合命令 4-142
4.3.17.1 channel-group 4-143
4.3.17.2 lacp 4-144

A. 管理信息库 A-1

A.1 支持的 MIB A-1
A.2 支持的陷阱 A-3

B. 故障排除 B-1

B.1 诊断交换机指示灯 B-1
B.2 诊断端口连接 B-2
B.3 访问管理界面 B-2

B.4 使用系统日志 B-3
B.4.1 日志消息 B-4
B.5 错误消息 B-5
B.5.1 命令行错误检测 B-5
B.5.2 系统错误 B-5
B.5.3 命令行错误 B-6
B.5.4 Web 界面错误 B-8

C. 规格 C-1
C.1 交换机体系结构 C-1
C.2 管理功能 C-2
C.3 物理规格 C-2
C.4 电源 C-3
C.5 环境规格 C-3
C.6 标准 C-3

词汇表 词汇表 -1

索引 索引 -1

序言

通过这本 *《Sun Fire™ B1600 刀片式系统机箱交换机管理指南》*，您可以了解和使用位于系统机箱的 SSC （交换机和系统控制器）模块内的交换机。可以通过两个界面访问交换机：命令行界面和 Web 界面。本手册将介绍这两种界面。

本手册的读者对象是负责管理系统机箱的网络管理员。其前提是了解局域网运行的工作常识和熟悉网络协议。

在阅读本书之前

在开始配置交换机之前：

按照 *《Sun Fire™ B1600 刀片式系统机箱硬件安装指南》*和 *《Sun Fire™ B1600 刀片式系统机箱软件设置指南》*中的说明安装系统机箱。

本书的编排方式

第 1 章概述了交换机，其中包括管理选项、硬件功能、交换功能以及默认设置。

第 2 章介绍如何连接到交换机控制台和备选的 Web 界面。

第 3 章描述了交换机的所有主要功能，并介绍如何通过 Web 界面和控制台界面配置这些功能。另外，还提供了 SNMP 管理应用程序所使用的等效 MIB 变量的列表。

第 4 章详尽列出了所有控制台界面命令和参数。

附录 A 列出了此交换机支持的管理信息库 (MIB) 和陷阱。

附录 B 提供了基本的故障排除信息，其中包括如何识别系统指示灯和端口指示灯，如何解决无法访问管理界面的问题，以及如何使用系统日志。

附录 C 详细介绍了交换机各种功能的规格。

词汇表列出了术语、词组以及它们的定义。

索引为本手册中的所有重要主题提供了页面参考。

印刷惯例

字体	含义	示例
AaBbCc123	命令和文件的名称；计算机屏幕输出	显示系统文件。 使用 `dir` 列出所有文件。
AaBbCc123	您键入的内容 （与计算机屏幕输出相对比）	`>`**`enable`** `Password:`
AaBbCc123	书名、新词汇或术语、要强调的词语。用实际名称或值替换命令行变量。	请阅读 *《Sun Fire™ B1600 Installation and Maintenance Guide》*中的第 6 章。 这些被称为*类*选项。 要执行此操作，您*必须*是管理员。 要删除文件，请键入 `del` *filename*。

相关文档

应用	书名	部件号
安装	*Sun Fire™ B1600 刀片式系统机箱硬件安装指南*	817-1906
机箱软件设置	*Sun Fire™ B1600 刀片式系统机箱软件设置指南*	817-1890
机箱管理	*Sun Fire™ B1600 刀片式系统机箱管理指南*	817-1900

访问 Sun 联机文档

在下列网址中有大量的 Sun 系统文档：

`http://www.sun.com/products-n-solutions/hardware/docs`

在下列网址中有 Solaris 的文档全集以及许多其它文档：

`http://docs.sun.com`

订购 Sun 文档

Fatbrain.com 是 Internet 上的一家专业书店，备有精心选自 Sun Microsystems, Inc. 的产品文档。

有关文档清单及其订购方法，请按以下网址访问位于 Fatbrain.com 上的 Sun Documentation Center （Sun 文档中心）：

`http://www.fatbrain.com/documentation/sun`

Sun 欢迎您提出宝贵意见

Sun 愿意对其文档进行改进，并欢迎您提出意见和建议。请将您的意见和建议发送至：

`docfeedback@sun.com`

请在电子邮件的主题行中加入文档的部件号 (817-1895-10)。

第 I 部分　入门

本节概述了 Sun Fire™ B1600 刀片式系统机箱，并介绍了与网络交换机有关的一些基本概念。同时还介绍了访问管理界面所需的基本设置。

简介

初始配置

第 1 章

简介

Sun Fire™ B1600 刀片式系统机箱包含两个交换机和系统控制器 (SSC) 模块。 SSC 包含一个高性能的千兆位以太网交换机。该交换机上的 16 个内部全双工千兆位端口在机箱内提供了高性能的连接；同时，通过 8 个外部全双工千兆位端口与范围更广的网络相连。

1.1 概述

这些交换机为 Sun Fire™ B1600 刀片式系统机箱提供了千兆位以太网连接。如果其中一台交换机出现故障，操作不会中断，而在第二台交换机上继续运行。机箱中的所有组件（包括刀片、 SSC 和 PSU）均插入一块提供组件互连的通用中板上。

16 个服务器刀片中的每一个刀片均通过作为刀片主要输入 / 输出手段的千兆位以太网链接与每台交换机上的单个端口相连。每个 SSC 中的交换机均提供千兆位以太网结构，将所有刀片连接在一起，另外还通过 8 个外部链路与外部网络相连。同时，每个刀片还通过简单串行链接与每个 SSC 中的系统控制器 (SC) 相连。通过 SC，可以管理和监视机箱的组件。而且，还可以访问交换机的命令行界面，也可以访问机箱中所安装的每个服务器刀片的控制台。

1.1.1 交换机体系结构

交换机采用高速交换结构，可以在所有端口上以较低的时延同时传输多个数据包。它还采用存储转发技术，以最大程度地确保数据完整性。在这种模式下，必须先将完整的数据包接收到端口缓冲区中并检查其有效性，然后转发。这样可以防止将错误传播到整个网络上。

1.1.2 访问交换机管理应用程序的方法

交换机有一个配备了 RJ-45 插孔的串行控制台端口。通过该端口，可以对系统控制器进行现场管理访问。如果接通系统机箱的电源，则将显示系统控制器 (SC) 的界面。要访问交换机的命令行界面，请参阅第 2-2 页上的 “配置选项”，或参阅 *《Sun Fire B1600 刀片式系统机箱软件设置指南》*。

也可以使用 Telnet 连接通过 SSC 上的 100BASE-TX RJ-45 管理端口 (NETMGT) 直接访问此命令行界面。

也可以在网络上使用 Web 浏览器或 SNMP/RMON 软件将交换机连接到此端口，对它进行管理。

如果通过 Web 浏览器来进行连接，交换机将通过图形用户界面来提供 HTTP 管理访问。

经过适当配置且可以使用 SNMP 的管理应用程序可以显示由 SNMP 提供的信息。

1.2 硬件说明

交换机和系统控制器 (SSC) 包括交换机板、系统控制器 (SC)、冷却风扇以及中板和后面板连接器。 SC 提供对服务器机箱和交换机板的管理访问。它还控制系统指示灯，这些指示灯分别位于 Sun Fire™ B1600 刀片式系统机箱的正面和背面，且正面和背面的指示灯完全相同。

1.2.1 以太网端口

1.2.1.1 上行链接端口

8 个外部 RJ-45 端口支持对速度、双工模式以及流量控制进行自动协商 （符合 IEEE 802.3x）。每个端口均可在 10 Mbps、 100 Mbps 和 1000 Mbps 的速度下运行，而且均支持全双工和半双工模式，并控制数据流以防止缓冲区溢出。使用 5 类双绞线，可以将上行链接端口连接到 100 米 （328 英尺）内符合 IEEE 802.3ab 标准的其它 1000BASE-T 设备上。这些端口还可以自动执行 MDI/MDI-X 操作，因此可以使用直通电缆来进行所有连接。在配置界面中，上行链接端口的名称分别为 NETP0 - NETP7。

注：请注意，在使用自动协商功能时，如果挂接的设备也支持此功能，则会自动设置速度、传输模式以及流量控制。否则，需要针对每个连接手动配置上述各项。

注：必须为自动 MDI/MDI-X 管脚引线配置启用自动协商功能。

1.2.1.2 内部端口

交换机还提供了 16 个内部 1000BASE-X 千兆位以太网端口，用于连接机箱中的服务器刀片。这些端口固定采用 1000 Mbps 的速度和全双工模式。在配置界面中，这些内部端口的名称为 SNP0 - SNP15。

交换机还包括一个内部 10/100BASE-TX 端口 （称作 NETMGT）。它通过内部集线器连接到 SC 的网络端口和位于 SSC 前面板上的外部管理端口。

1.2.2 状态指示灯

交换机级指示灯位于 SSC 模块上。位于 SSC 后面板上的 1000BASE-T 上行链接端口和 10/100BASE-TX 管理端口还包括 “链接”指示灯和 “速度”指示灯。

图 1-1 SSC 外部面板

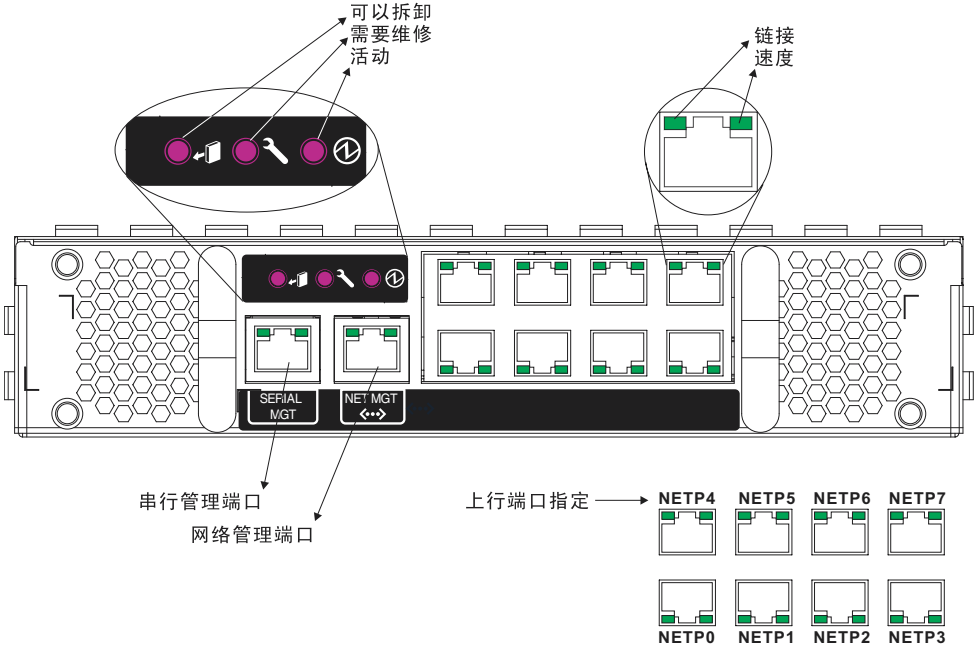


表 1-1 端口指示灯

指示灯	条件	状态
SSC		
活动	亮 （绿色）	SSC 正常工作。
需要维修	亮 （琥珀色）	SSC 需要维修。
可以拆卸	亮 （蓝色）	现在可以拆卸 SCC。
RJ-45 端口		
链路	亮 （绿色）	端口已经建立有效的网络连接。
速度	亮 （琥珀色）	链路以 1 Gbps 的速度运行。
	不亮	链路以低于 1 Gbps 的速度运行。

1.3 交换机的功能

交换机提供了各种可以增强性能的高级功能。多点传送过滤可以支持实时网络应用。基于端口和带标记的 VLAN 以及支持自动 GVRP VLAN 注册的功能，为通信提供了安全性，并可以有效地使用网络带宽。通过 QoS 优先级队列可以确保在整个网络上传输实时多媒体数据时延时最短。流量控制消除了由于端口饱和而导致的瓶颈所造成的数据包丢失。而广播风暴抑制可以防止广播通信风暴使整个网络瘫痪。以下简要介绍某些管理功能。

IEEE 802.1D 网桥 — 该交换机支持 IEEE 802.1D 透明桥接。地址表通过了解地址，然后根据这些信息过滤或转发通信，可以帮助进行数据交换。地址表最多支持 8000 个地址。

存储转发交换 — 交换机先将各帧存储到其内存中，然后将它们转发到其它端口。这样，就可以确保所有帧都符合标准的以太网大小，而且均已使用循环冗余检查 (CRC) 验证了它们的准确性。这样可以防止错误帧进入网络，浪费带宽。

为了避免在拥塞的端口上丢失帧，交换机为每个端口提供了 128 KB 的帧缓冲。此缓冲区可以对在拥塞网络上等待传输的数据包进行排队。

生成树协议 — 此交换机支持以下生成树协议：

生成树协议 （STP， IEEE 802.1D）— 此协议允许在一对 LAN 段之间建立两个或更多的冗余连接，从而提高容错水平。如果在网段之间有多条物理路径，本协议将选择单条路径，并禁用其它所有路径，以确保网络上的任何两个站之间只有一条路线。这样可以防止出现网络环路。但是，如果所选路径由于任何原因出现故障，则将激活另一条路径以保持连接。

快速生成树协议 （RSTP， IEEE 802.1w）— 本协议将网络拓扑结构变化的收敛时间降至大约较旧的 IEEE 802.1D STP 标准所需收敛时间的 10%。它旨在完全替代 STP，但是，如果运行较旧标准的交换机从所连接的设备上检测到 STP 协议消息，则仍可以通过自动将端口重新配置为兼容 STP 的模式，从而与这些交换机交互操作。

虚拟 LAN — 此交换机最多可支持 256 个 VLAN。虚拟 LAN 是多个网络节点的集合，共享同一个冲突域，而不考虑它们各自在网络中的物理位置或连接点。此交换机支持带标记的 VLAN （基于 IEEE 802.1Q 标准）。可以通过 GVRP 动态了解 VLAN 组的成员，也可以手动为特定的一组 VLAN 分配端口。这样，交换机就可以将通信限制到已分配了用户的 VLAN 组。通过将网络分割成多个 VLAN，您可以：

- 消除会严重降低平面网络性能的广播风暴。
- 通过为所有端口远程配置 VLAN 成员 （而不必手动更改网络连接），从而简化更改 / 移动节点时的网络管理工作。
- 通过将所有通信限制到源 VLAN （除已使用路由器或第 3 层交换机在单独的 VLAN 之间配置连接外），从而提供数据安全性。

端口镜像 — 交换机可以在不知不觉中将任何端口上的通信镜像到某个监视端口上。然后，可以将协议分析器或 RMON 探测器连接到此端口上，以执行通信分析和验证连接完整性。

端口聚合 — 端口可以组合成一个集合连接。使用 IEEE 802.3ad 链路聚合控制协议 (LACP) 可以手动设置或动态配置聚合组。附加端口可以大大增加通过所有连接的吞吐量，而且，如果聚合组中的某个端口出现故障，其它端口可以接管负荷，从而实现冗余功能。该交换机支持 6 个聚合组，并且每个聚合组可支持多达 4 个上行链接端口或两个下行链接端口。

端口安全性 — 端口安全性功能可防止未授权用户访问您的网络。通过它，每个端口都可以了解或分配已获得授权可以通过该端口访问网络的设备的 MAC 地址列表。该端口上收到的任何数据包都必须有一个源地址在授权列表中显示，否则会丢失该数据包。默认情况下，在所有端口上均禁用端口安全性功能，但可以按端口逐个启用该功能。

广播抑制 — 广播抑制可防止广播通信使整个网络瘫痪。如果某个端口启用了此功能，则通过该端口的广播通信的级别将受到限制。如果广播通信超过了预先定义的阈值，则它会受到抑制，直到回落到低于阈值的级别。

流量控制 — 流量控制可以降低拥塞期间的通信量，并可在端口缓冲区溢出时防止数据包丢失。该交换机支持基于 IEEE 802.3x 标准的流量控制。默认情况下，所有端口上均禁用流量控制。

通信优先级 — 此交换机提供服务质量 (QoS)，它根据所需的服务级别，使用四个优先级队列和加权轮询队列来确定每个数据包的优先级。它根据终端站应用程序的输入，使用 IEEE 802.1p 和 802.1Q 标记来区分传入通信的优先级。可以使用这些功能为对延迟敏感的数据和尽力而为的数据传输提供独立的优先级。

本交换机还支持多种用于区分第 3/4 层通信优先级的通用方法，以满足应用需要。通信的优先级可以根据 IP 帧的服务类型 (ToS) 八位字节中的优先位来确定。如果启用了这些服务，则交换机会将优先级映射为一个 “服务类别” 值，然后将通信发送到相应的输出队列。

地址过滤 — 本交换机为所有进入 CPU 端口且随后可能转发或路由到管理网络的通信提供了数据包过滤器。该数据包过滤器是基于规则 / 模式的，它建立了一组模式，如果数据包与该组模式相符，则将 “丢弃” 数据包；同时建立了另一组模式，如果与该组模式相符，则 “接受” 数据包。

多点传送交换 — 可以向交换机自身所在的 VLAN 分配特定的多点传送通信，以确保它不会干扰正常的网络通信；而且，可以通过为指定的 VLAN 设置所需的优先级来保证实时传送。本交换机使用 IGMP 侦听和 IGMP 来管理多点传送组注册。

1.4 默认设置

表 1-2 默认设置

功能	默认设置
系统设置	
Web Mgt.	启用
安全 Web Mgt.	禁用
BOOTP	启用
DHCP	启用
SNMP 社区	公用：只读 专用：读/写
SNMP 陷阱	验证陷阱：启用 链接建立断开事件：启用
用户名	admin （控制台、 Telnet、 Web） guest （控制台、 Telnet、 Web）
口令	登录 — 用户 admin，口令 “admin” 用户 guest，口令 “guest” 从 “普通执行” 变为 “特权执行”：“super”
串行端口	波特率：9600，数据位：8，停止位：1，奇偶校验：无
IP 设置	地址：0.0.0.0，子网掩码：255.0.0.0
端口状态	
端口速度	端口 SNP0-15：1000 Mbps 端口 NETP0-7：10/100/1000 Mbps，自动协商 端口 NETMGT：10/100 Mbps，自动协商
双工模式	端口 SNP0-15：全双工 端口 NETP0-7， NETMGT：半双工和全双工，自动协商
流量控制	禁用
端口优先级	入口优先级：0
端口安全性	禁用
生成树协议	启用，默认 RSTP （默认值：基于 IEEE 802.1w 的所有参数）
边缘端口 （快速转发）	默认情况下，对于 SNP0-15 启用，对于 NETP0-7 禁用
地址有效时间	300 秒

表 1-2 默认设置

功能	默认设置
虚拟 LAN	
GVRP	禁用
默认 VLAN	PVID 1（未标记的帧）
管理 VLAN	VLAN 2（用于管理端口）
标记	RX：所有帧， TX：未标记的帧
入口过滤	禁用
多点传送过滤	
IGMP 侦听	启用
ARP	启用
高速缓存超时	20 分钟

第 2 章

初始配置

有关对交换机执行初始配置的完整信息，请参阅 *《Sun Fire B1600 刀片式系统机箱软件设置指南》*。

本章包含以下各节：

- 第 2-2 页上的 “连接到交换机接口上”
- 第 2-3 页上的 “启用 SNMP 管理权限”

2.1 连接到交换机接口上

2.1.1 配置选项

为方便管理，交换机模块提供了一个命令行配置界面 (CLI)。要访问此程序，可先连接到交换机的 RJ-45 串行控制台端口，然后从系统控制器 (SC) 的命令提示符下登录到交换机的 CLI。具体情形如下，其中的 SSC*n* 表示 SSC0 或 SSC1。

```
sc>:console sscn/swt
Username:admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

注：如果您的管理网络中设置了 DHCP 服务器，即可使用 telnet 或 Web 方式与交换机建立连接。为确保交换机每次引导时都收到相同的地址 （并发出 DHCP 请求），需要在 DHCP 服务器上指定以下客户机标识符：SUNW,SWITCH_ID=*serial number of chassis*, 0 （表示 SSC0 中的交换机）或 SUNW,SWITCH_ID=*serial number of chassis*, 1 （表示 SSC1 中的交换机）。若要了解如何使网络做好安装系统机箱的准备，以及对交换机进行初始配置的所有步骤，请参阅 *《Sun Fire B1600 刀片式系统机箱软件设置指南》*。

2.1.1.1 通过内置的交换机接口配置交换机

控制台连接 — 通过在系统控制器的命令提示符下输入 “console ssc*n*/swt” 命令 （其中 n 表示 SSC0 或 SSC1），可访问交换机的命令行界面 (CLI)。

Telnet 连接 — 可借助 Telnet 连接通过管理网络远程连接到交换机的 CLI 上。

Web 接口 — 交换机中还包含一个内嵌的 HTTP Web 代理。可从管理网络中的任何一台计算机上通过标准的 Web 浏览器访问此代理。

SNMP 软件 — 交换机的管理代理基于 SNMP （简单网络管理协议，它对版本 1 和 2c 都提供支持）。此 SNMP 代理允许从管理网络中的任何系统利用管理软件 （例如 SunNet Manager）对交换机进行管理。

系统配置程序和 SNMP 代理所支持的管理功能有：

- 启用 / 禁用任何端口
- 为任何端口设置速度 / 双工模式
- 配置 SNMP 参数
- 在 VLAN 中添加端口
- 显示系统信息或统计信息
- 对交换机进行配置，使之加入生成树协议
- 下载系统固件

2.2 启用 SNMP 管理权限

可对交换机进行配置，使之能够接受发自 “简单网络管理协议”（SNMP v1 或 v2c）应用程序 （例如， SunNet Manager）的管理命令。可对交换机进行配置，使之响应 SNMP 请求和 / 或生成 SNMP 陷阱。

当 SNMP 管理站向交换机发出请求 （请求其返回信息或设置参数）后，交换机将提供所请求的数据或设置指定的参数。还可对交换机进行配置，使之 （在 SNMP 管理器未发出请求的情况下）通过陷阱消息向 SNMP 管理器发送信息，通知管理器发生了某些事件。

2.2.1 社区字符串

社区字符串用于控制对 SNMP 工作站的管理权限，还可用于授权 SNMP 工作站接收来自 SSC 的陷阱消息。因此，您需要给指定的用户或用户组分配社区字符串，并设置访问级别。

默认设置为：

- **public** — 提供只读权限。经授权的管理站只能检索 MIB 对象。
- **private** — 提供读写权限。经授权的管理站既能检索 MIB 对象，又能修改 MIB 对象。

注：如果您不打算使用 SNMP，则建议您将这两个默认的社区字符串都加以删除。如果没有社区字符串，则交换机的 SNMP 管理权限将被禁用。

要配置社区字符串，请完成以下步骤：

1. 在 “特权执行”级别的全局配置模式提示符下，键入 “snmp-server community *string mode*”，其中，“string”为社区访问字符串，而 “mode”则为 **rw** （读/写）或 **ro** （只读）。按 <Enter> 键。
2. 要删除现有的字符串，只需键入 “no snmp-server community *string*”，其中，“string”为要删除的社区访问字符串。按 <Enter> 键。

```
Console(config)#snmp-server community sun rw
Console(config)#no snmp-server community private
Console(config)#
```

2.2.2 陷阱接收装置

您还可指定 SNMP 工作站，用来接收发自 SSC 的陷阱。

要配置陷阱接收装置，请完成以下步骤：

1. **从 “全局配置”模式的提示符下，键入 “snmp-server host *host-address community-string*”，其中，“host-address”为陷阱接收装置的 IP 地址，而 “community-string”则为与该主机相关的字符串。**

   按 <Enter> 键。

2. **为使 SSC 能够发送 SNMP 通知，必须至少输入一个 snmp-server enable traps 命令。**

   键入 “snmp-server enable traps [*type*]”，其中，“type”为 authentication 或 link-up-down。按 <Enter> 键。

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

3. **按照 *《Sun Fire B1600 刀片式系统机箱软件设置指南》* 中的说明，对配置设置进行保存。**

第 II 部分 配置交换机

本节介绍交换机的基本功能，并提供了一些示例，用以说明如何通过 Web 浏览器或命令行界面来配置每种功能。

管理概述

命令行参考

第 3 章

管理概述

本章介绍如何执行基本的配置任务。

- 第 3-2 页上的第 3.1 节 “使用 Web 界面”
- 第 3-7 页上的第 3.2 节 “基本配置”
- 第 3-31 页上的第 3.3 节 “配置全局网络协议”
- 第 3-75 页上的第 3.4 节 “端口配置”
- 第 3-110 页上的第 3.5 节 “监视端口和管理通信”

3.1 使用 Web 界面

该交换机提供了一个嵌入式 HTTP Web 代理。使用 Web 浏览器，可以对交换机进行配置，并可查看统计信息以便监视网络活动。网络上任何使用标准 Web 浏览器（Internet Explorer 5.0 或更高版本，或 Netscape Navigator 6.2 或更高版本）的计算机均可访问此 Web 代理。

注：也可以使用命令行界面 (CLI)，通过与控制台端口之间的串行连接或通过 Telnet 来管理交换机。有关使用 CLI 的详细信息，请参阅第 4 章。

通过 Web 浏览器访问交换机之前，务必首先执行以下任务：

1. 使用带外 (out-of-band) 串行连接、 BOOTP 协议或 DHCP 协议，为交换机配置有效的 IP 地址、子网掩码和默认网关。（有关如何执行此操作的信息，请参阅 *《Sun Fire B1600 刀片式系统机箱软件设置指南》*。）
2. 使用带外 (out-of-band) 串行连接设置用户名和口令。控制访问 Web 代理的用户名和口令与板载配置程序中的用户名和口令相同。（有关如何执行此操作的信息，请参阅 *《Sun Fire B1600 刀片式系统机箱软件设置指南》*。）

注：如果管理站与此交换机之间的路径不经过任何使用生成树算法的设备，则可以将交换机端口设置为与管理站相连，以便使用快速转发功能来缩短交换机对通过 Web 界面所发出的管理命令的响应时间。（请参阅第 3-102 页上的 “Admin Edge Port”。）

---

3. 在输入了用户名和口令之后，您将可以访问系统配置程序。

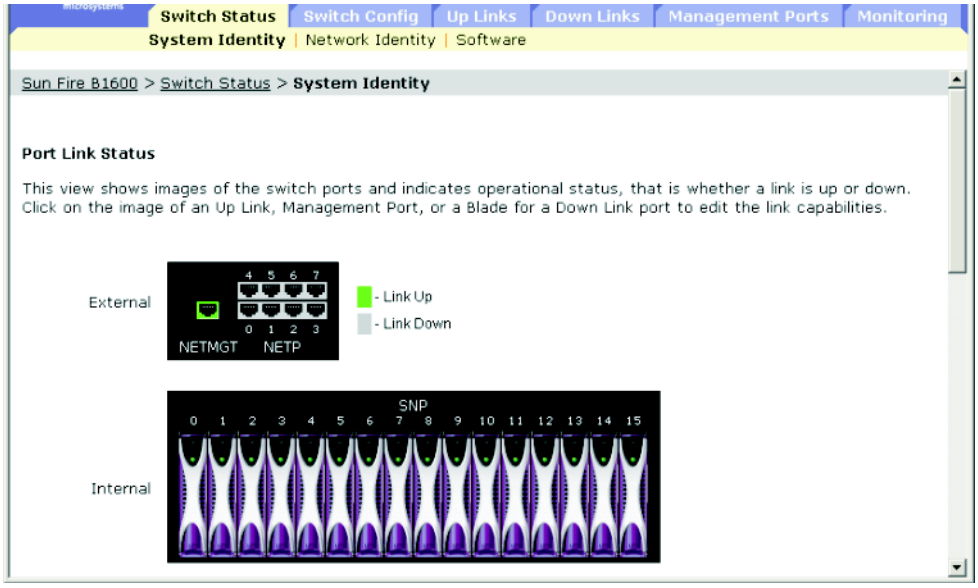
注：您可以三次尝试输入正确的口令；如果第三次尝试失败，当前连接将终止。

3.1.1 浏览 Web 浏览器界面

要访问 Web 浏览器界面，首先必须输入用户名和口令。管理员对所有配置参数和统计信息都具有读 / 写访问权限。管理员的默认用户名和口令均为 “admin”。

3.1.1.1 主页

当 Web 浏览器连接到交换机的 Web 代理时，将显示主页。从位于该页左侧的主菜单面板上选择 “Switch”。配置选项将显示在菜单选项卡中，相应的菜单项 （列在菜单选项卡下面一行中）显示在屏幕的顶部。菜单选项卡和下一级菜单项用于访问配置菜单以及显示配置参数和统计信息。



3.1.1.2 配置选项

可配置参数都有一个对话框或下拉列表。在页面上更改配置之后，请务必单击 “Save” 按钮来确认新设置。下表总结了 Web 页配置按钮。

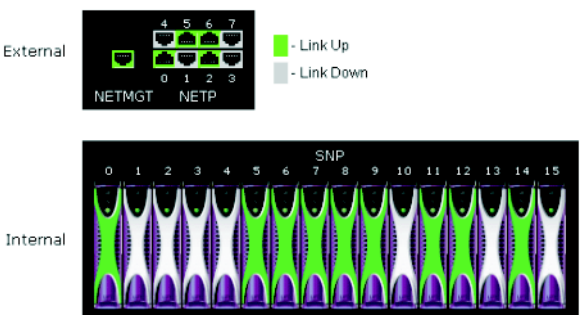
按钮	操作
Cancel	取消所指定的值并恢复当前值。
Reset	取消所指定的值并恢复当前值。
Save	为系统设置指定的值。

注：要确保屏幕正确刷新，请务必按照以下说明配置 Internet Explorer 5.x：在菜单 “工具 / Internet 选项 / 常规 / Internet 临时文件 / 设置” 中，“检查所存网页的较新版本” 一项的设置应该为 “每次访问此页时检查”。

注：如果使用 Internet Explorer 5.0，在更改配置之后，必须按浏览器的 “刷新” 按钮以手动刷新屏幕。

3.1.2 面板显示

Web 代理显示了交换机上行链接端口的图像，指示每条链接是建立还是断开。单击端口图像将打开 “端口配置” 页，如第 3-75 页所示。



3.1.3 主菜单

使用板载 Web 代理，可以定义系统参数，管理和控制交换机及其所有端口，也可以监视网络状况。下表简要说明了该程序中的可用选项。

菜单	说明	页码
Switch Setup	基本配置	3-7
System Identity	提供基本的系统说明，包括位置和联系人信息	3-7
Network Identity	为通过 DHCP、BOOTP 或手动配置来进行管理访问而设置 IP 地址	3-10
Software	显示固件版本；下载代码和配置设置	3-16
Switch Config	全局配置协议	3-31
Security	指定用户名和口令，以及指定通过 RADIUS 或 TACACS+ 进行的远程访问验证服务	3-23
Communication	设置 SNMP 社区访问字符串、陷阱管理器和要发出的陷阱类型	3-27
VLANs	显示基本的 VLAN 信息；启用 GVRP 多点传送协议；配置 VLAN	3-31
Static VLAN Port Membership	为 VLAN 添加静态成员	3-39
Broadcast & Multicast	设置广播风暴控制；配置多点传送协议，其中包括 IGMP 侦听、静态路由器端口信息以及多点传送服务	3-42
IGMP Parameters	启用多点传送过滤功能；为多点传送查询配置参数	3-43
Multicast Router Ports	指定与相邻的多点传送路由器 / 交换机相连的端口	3-45
Multicast Services	为特定接口分配多点传送服务	3-48
Broadcast Parameters	设置广播风暴阈值	3-51
Spanning Tree	配置生成树协议	3-53
Basic Configuration	配置全局生成树的设置	3-53
Advanced Configuration	配置 RSTP 的高级设置	3-59

菜单	说明	页码
Class of Service	配置服务类别	3-60
Basic Traffic Prioritisation	配置默认的 CoS 优先级，将 CoS 优先级映射到输出队列，以及配置加权轮询排队	3-60
Layer 3/4 Traffic Prioritisation	选择第 3/4 层优先级服务，将 IP 优先权标记映射为 CoS 值，以及将 DSCP 标记映射为 CoS 值	3-66
Address Tables	设置地址有效期；显示指定接口、 VLAN 或地址的条目；配置静态地址	3-72
Up Links	端口配置	3-75
Connection Status	显示端口连接状态	3-75
Connection Configuration	配置端口连接设置；启用广播风暴控制	3-79
Link Aggregation	将端口配置为通过 LACP 动态加入聚合组，或指定端口加入静态聚合组	3-83
VLANs	指定端口属性 （包括默认 PVID、交换机端口模式、入口过滤、 GVRP、 GARP 定时器）；配置静态 VLAN 成员	3-89
Static Addresses	显示或编辑地址表中的静态条目；启用 / 禁用了解永久条目的功能	3-95
Spanning Tree	配置全局生成树的端口设置	3-98
Spanning Tree Protocol	为全局生成树上的接口配置 STA 端口级设置	3-98
Down Links	端口配置	3-75
Connection Status	显示端口连接状态	3-75
Connection Configuration	配置端口连接设置；启用广播风暴控制	3-79
Link Aggregation	将端口配置为通过 LACP 动态加入聚合组，或指定端口加入静态聚合组	3-83
VLANs	指定端口属性 （包括默认 PVID、交换机端口模式、入口过滤、 GVRP、 GARP 定时器）；配置静态 VLAN 成员	3-89
Static Addresses	显示或编辑地址表中的静态条目；启用 / 禁用了解永久条目的功能	3-95
Spanning Tree	配置全局生成树的端口设置	3-98
Spanning Tree Protocol	为全局生成树上的接口配置 STA 端口级设置	3-98
Management Port	端口配置	3-75
Connection Status	显示端口连接状态	3-75
VLANs	指定端口属性 （包括默认 PVID、交换机端口模式、入口过滤、 GVRP、 GARP 定时器）；配置静态 VLAN 成员	3-89
Packet Filtering	过滤从上行链接端口进入管理端口的通信	3-106

菜单	说明	页码
Monitoring	交换机监视功能	3-110
Port Mirroring	设置用于镜像的源端口和目标端口	3-110
Port Statistics	显示有关端口通信的统计信息，包括有关接口组、Ethernetlike MIB 和 RMON MIB 的信息	3-112
SNMP Statistics	显示有关 SNMP 消息的统计信息	3-120
Logs	配置日志记录消息参数；显示存储在交换机内存中的消息	3-120

3.2 基本配置

3.2.1 显示系统信息

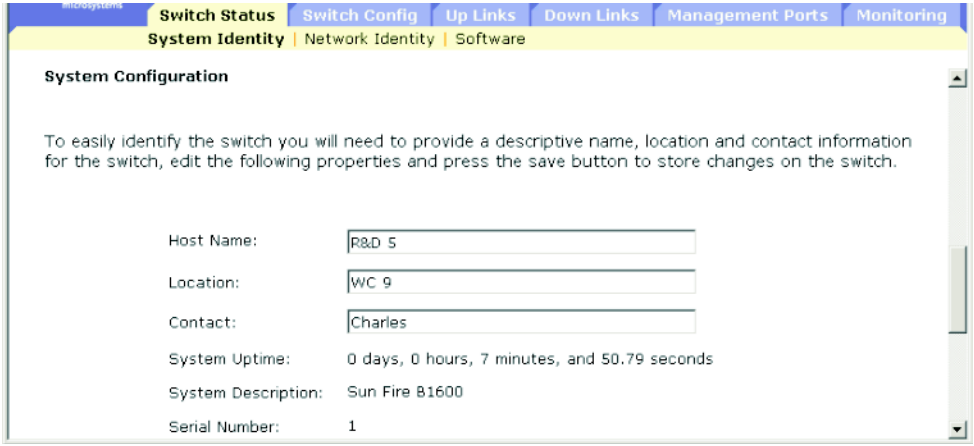
通过提供具有说明性的名称、地址和联系人信息，可以很容易地识别系统。

命令属性

- **Host Name** — 分配给交换机的名称。
- **Location** — 指定系统机箱的位置。
- **Contact** — 负责管理系统的管理员。
- **System Up Time** — 管理代理运行的时间长度。
- **System Description** — 制造商指定的系统硬件说明。
- **Serial Number**[1] — 主板的序列号。
- **System OID string**[2] — 交换机网络管理子系统的 MIB II 对象 ID。
- **MAC Address**[3] — 该交换机的物理层地址。
- **Web server**[2] — 显示是启用还是禁用通过 HTTP 进行管理访问。
- **Web server port**[2] — 显示 Web 界面使用的 TCP 端口号。
- **POST result**[2] — 显示加电自检的结果。

1: CLI：请参阅第 4-40 页上的 “show version”。
2: 仅适用于 CLI
3: Web：请参阅第 3-10 页上的 “设置 IP 地址”。

Web — 打开 “Switch Setup” => “System Identity”。指定主机名、位置和系统管理员的联系信息，然后单击 “Save Changes”。



CLI — 指定主机名、位置和联系人信息。

```
Console(config)#hostname R&D 5                                    4-25
Console(config)#snmp-server location WC 9                         4-50
Console(config)#snmp-server contact Bill                          4-49
Console#show system                                               4-38
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.674.10895.4
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
 System Name             : [NONE]
 System Location         : [NONE]
 System Contact          : [NONE]
 MAC address             : 00-00-e8-00-00-01
 Web server              : enable
 Web server port         : 80
 Web secure server       : enable
 Web secure server port  : 443
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
Switch Driver Initialization ........... PASS
------------------- DONE --------------------
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
System Name (Host Name)	MIB-II. system. sysName	读 / 写	字符串 （大小 (0-255)）	
System Location	MIB-II. system. sysLocation	读 / 写	字符串 （大小 (0-255)）	
System Contact	MIB-II. system. sysContact	读 / 写	字符串 （大小 (0-255)）	
System Up Time	MIB-II. system. sysUpTime	只读	计时时间 （厘秒）	
System Description	MIB-II. system. sysDescr	只读	字符串 （大小 (0-255)）	
System Object Identification	MIB-II. system. sysObjectID	只读	对象标识符	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	只读	物理地址	
HTTP State (Web Server)	sun... ipMgt. ipHttpState	读 / 写	enabled (1), disabled (2)	enabled
HTTP Port (Web Server Port)	sun... ipMgt. ipHttpPort	读 / 写	整数 (1-65535)	80
HTTPS State (Secure Server)	sun... ipMgt. ipHttpsState	读 / 写	enabled (1), disabled (2)	enabled
HTTPS Port (Secure Server Port)	sun... ipMgt. ipHttpsPort	读 / 写	整数 (1-65535)	443

3.2.2 设置 IP 地址

默认情况下，交换机使用 DHCP 搜索其 IP 地址、默认网关和子网掩码。

可以手动配置特定的 IP 地址，也可以指示设备从 BOOTP 或 DHCP 服务器获取 IP 地址。有效的 IP 地址由四个十进制数字 （0 到 255 之间）组成，各数字之间用句点分隔。如果与这种格式不同，软件将无法接受。

注：事实上，交换机的 IP 地址就是包含管理端口 (NETMGT) 的 VLAN 的 IP 地址。默认情况下，管理端口位于 VLAN 2 上。因此，在设置对交换机的网络访问时，是通过为 VLAN 2 分配 IP 地址实现的。只应为包含管理端口的 VLAN 指定 IP 地址。当您为任何 VLAN 分配 IP 地址时，将立刻禁用原始 IP 地址，且新的 IP 地址将立即生效。

命令属性

- **Current IP Address** — 允许进行管理访问的 VLAN 接口的当前地址。
- **MAC Address**[1] — 该交换机的物理层地址。
- **Management VLAN** — 只能通过该 VLAN 管理交换机。默认情况下，管理端口 (NETMGT) 已配置为该 VLAN （即 VLAN 2）的成员。不过，如果更改了管理 VLAN，则将无法对交换机进行管理访问，除非已将 NETMGT 端口配置为该新 VLAN 的成员。如果出现这种情况，必须使用控制台界面来将 NETMGT 端口添加到新配置的管理 VLAN 中。（请参阅第 4-110 页上的第 4.3.12.8 节 “switchport allowed vlan”。）

1: CLI：请参阅第 3-7 页上的 “显示系统信息”。

- **IP Address Mode** — 指定是通过手动配置 （静态）、动态主机配置协议 (DHCP) 还是通过引导协议 (BOOTP) 来启用 IP 功能。如果启用 DHCP/BOOTP，则在收到服务器的应答之前， IP 不会正常工作。交换机将定期广播请求，以请求 IP 配置设置。（DHCP/BOOTP 值可以包括 IP 地址、子网掩码和默认网关。）
  - **DHCP** — 动态主机配置协议
    - **Enable Client ID** — 在所有与 DHCP 服务器进行的通信中加入客户机标识符。
      - **Text/Hex** — 指示输入的客户机 ID 是文本字符串（1-15 个字符）还是十六进制值。具体采用哪种数据类型取决于 DHCP 服务器的要求。

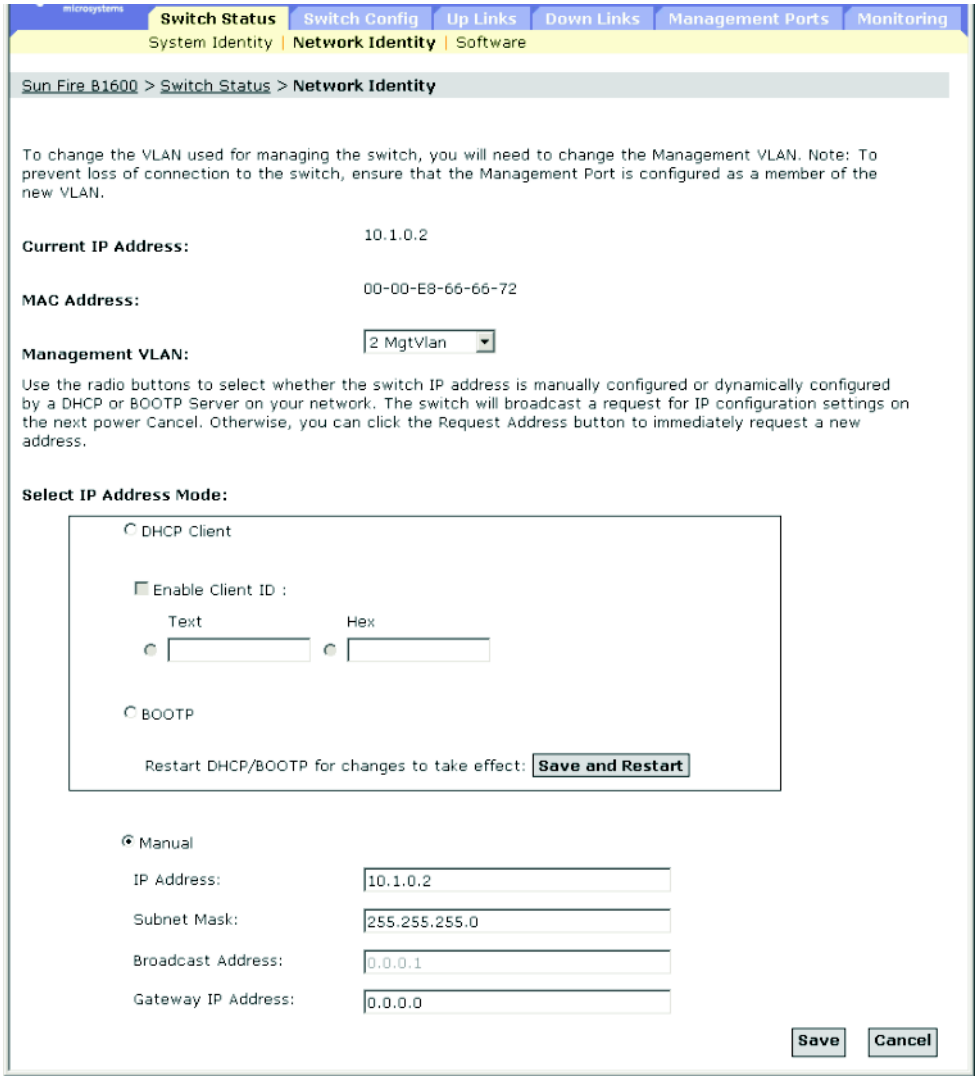
    注：在下次系统或交换机自身重新引导时， SC 将覆盖在此菜单中指定的客户机 ID。在下一个固件版本中，将删除 “Client ID” 字段。

  - **BOOTP** — 引导协议
- **Manual** — 将管理接口设置为指定值。
  - **IP Address** — 允许进行管理访问的VLAN接口的地址。有效的IP地址由四个数字（0 到 255 之间）组成，各数字之间用句点分隔。（默认值：0.0.0.0）
  - **Subnet Mask** — 该掩码标识用来路由到特定子网的主机地址位。（默认值：255.0.0.0）
  - **Broadcast Address**[2] — 在与 IP 地址相关的接口上发送数据报所使用的 IP 广播地址。该值适用于交换机所使用的子网和网络广播地址。（默认值：0.0.0.1）
  - **Gateway IP Address** — 本设备与管理站 （位于其它网段上）之间的网关路由器的 IP 地址。（默认值：0.0.0.0）

2: 仅适用于 Web

3.2.2.1 手动配置

Web — 打开 “Switch Setup” => “Network Identity”。选择管理接口，单击 “Manual” 单选按钮，指定 IP 地址、子网掩码和默认网关，然后单击 “Save”。



注： 如果显示错误消息，提示您输入的数据无效，则请检查是否正确指定了每个 IP 地址。

CLI — 指定管理接口、 IP 地址和默认网关。

```
Console#config
Console(config)#interface vlan 2                                    4-74
Console(config-if)#ip address 10.1.0.2 255.255.255.0                4-62
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                       4-66
Console(config)#
```

SNMP — 等效 MIB 变量。

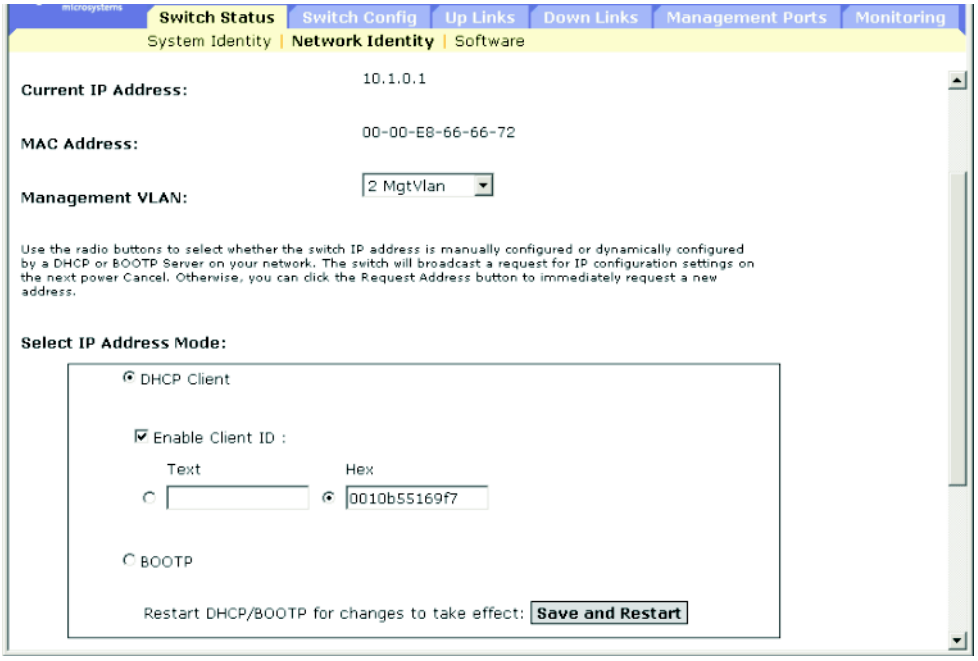
字段名	MIB 变量	访问权限	值范围	默认值
Management VLAN	sun... switchMgt. switchManagementVlan	读 / 写	整数 (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	读 / 写	user (1)，bootp (2)，dhcp (3)	user
IP Address Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntAddr	读 / 写	IP 地址	
Subnet Mask Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntNetMask	读 / 写	IP 地址	
Broadcast Address	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntBcastAddr	只读	整数 (0-1)	1
Default Gateway Configuration	sun... ipMgt. netDefaultGateway	读 / 写	IP 地址	

3.2.2.2 使用 DHCP/BOOTP

默认情况下，交换机使用 DHCP/BOOTP 服务来查找其 IP 配置信息。

Web — 打开 “Switch Setup” => “Network Identity”。指定管理接口，单击 “DHCP” 或 “BOOTP” 单选按钮。

默认情况下，机箱中的系统控制器向交换机提供客户机标识符。客户机标识符为 SUNW,SWITCH_ID= *机箱的序列号* ,0 或 SUNW,SWITCH_ID= *机箱的序列号* ,1 （具体值取决于是 SSC0 还是 SSC1 中的交换机）。您可以在 “Enable Client ID” 复选框中指定客户机标识符，但下次重置或引导系统控制器时，将覆盖该客户机标识符。建议您不要这样做。在将来的固件版本中，将删除 “Enable Client ID” 字段。



注：如果管理连接中断，请使用控制台连接并输入 “show ip interface” 来确定新的交换机地址。

注：下次重新引导系统控制器或交换机本身时， SC 将覆盖在本菜单中指定的客户机 ID。在下一个固件版本中，将删除 “Client ID” 字段。

CLI — 指定管理接口、将 IP 地址模式设置为 DHCP 或 BOOTP，然后输入“ip dhcp restart”命令。

```
Console#config
Console(config)#interface vlan 2                                    4-74
Console(config-if)#ip address dhcp                                  4-62
Console(config-if)#ip dhcp client-id hex 00-00-e8-66-65-72          4-65
Console(config-if)#end
Console#ip dhcp restart                                             4-64
Console#show ip interface                                           4-66
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
 and address mode: DHCP.
Console#
```

Renewing DHCP — DHCP 可以无限期或在特定期间内向客户机出租地址。如果该地址到期或交换机移到其它网段，则将无法对交换机进行管理访问。在这种情况下，可以重新引导交换机，或提交重新启动 DHCP 服务的客户机请求。

Web — 如果 DHCP 分配的地址无法正常使用，则无法通过 Web 界面来续用 IP 设置。如果当前地址仍然有效，则只能通过 Web 界面来重新启动 DHCP 服务。

CLI — 输入以下命令重新启动 DHCP 服务器。

```
Console#ip dhcp restart                                             4-64
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Management VLAN	sun... switchMgt. switchManagementVlan	读 / 写	整数 (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	读 / 写	user (1)，bootp (2)，dhcp (3)	dhcp
DHCP Client ID	sun... ipMgt. dhcpClientIfClientId	读 / 写	八位字节字符串（MAC 地址）	
DHCP Restart	sun... ipMgt. ipDhcpRestart	读 / 写	restart (1)，noRestart (2)	noRestart

3.2.3 显示交换机软件版本

命令属性

- **Loader Version** — 加载器代码的版本号。
- **Boot-ROM Version** — 引导代码的版本号。
- **Operation Code Version** — 运行时代码的版本号。
- **Unit ID*** — 活动交换机的 ID。（该值始终为 1。）

* 仅适用于 CLI。对于 Stiletto B1600 刀片式系统机箱中当前版本的交换机来说，“Unit Id”的值没有意义。

Web — 打开 “Switch Setup” => “Software”。

CLI — 使用以下命令显示版本信息。

```
Console#show version                                          4-40
Unit1
 Serial number           :1
 Service tag             :
 Hardware version        :R0B
 Number of ports         :25
 Main power status       :up
 Redundant power status  :not present
Agent(master)
 Unit id                 :1
 Loader version          :0.0.6.5
 Boot rom version        :0.0.7.3
 Operation code version  :1.0.0.1
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Switch Serial Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swSerialNumber	只读	显示字符串 （大小 (0..80)）	
Switch Hardware Version	SUN. switchMgt. switchInfoTable. switchInfoEntry. swHardwareVer	只读	显示字符串 （大小 (0..20)）	
Switch Port Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swPortNumber	只读	整数	25
Switch Unit Index	SUN. switchMgt. switchInfoTable. switchInfoEntry. swUnitIndex	不可访问	整数	1
Switch Loader Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swLoaderVer	只读	字符串 （大小 (0-20)）	
Switch Boot Rom Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swBootRomVer	只读	字符串 （大小 (0-20)）	
Switch Operation Code Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swOpCodeVer	只读	字符串 （大小 (0-20)）	

3.2.4 管理固件

可以将固件上载 TFTP 服务器上，也可以从 TFTP 服务器下载固件。通过将运行时代码保存在 TFTP 服务器上的文件中，在日后需要进行恢复操作时，可以将该文件下载到交换机上。也可以对交换机进行设置，使其在不覆盖以前版本固件的情况下使用新固件。

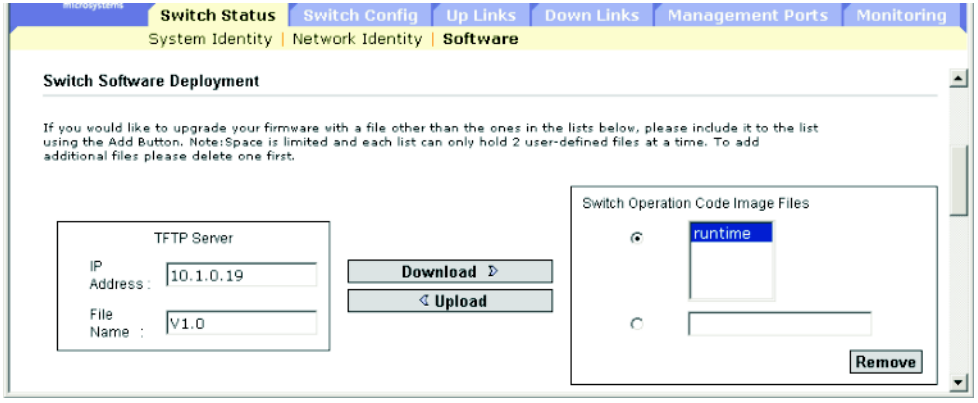
命令属性

- 目标文件名中不能包含斜杠（\ 或 /），文件名的首字母不能为点 (.)；在 TFTP 服务器上，文件名的最大长度为 127 个字符；而在交换机上，文件名的最大长度为 32 个字符。（有效字符为：A-Z、 a-z、 0-9、“.”、“-”、“_”）
- 在交换机的文件目录中，只可保存两份系统软件文件 （包含运行时固件）。该文件当前被指定为启动版本的副本是不能删除的。如果存在两份系统软件文件副本，则可以删除当前没有被指定为启动版本的那份副本并用新文件取代它，也可以使用其中一个现有文件名将新文件复制到该目录中。另外，可以删除当前启动文件中的启动指定，然后删除该文件，再将新版本的系统软件文件复制到该目录中，最后使该新文件成为指定的启动文件。

3.2.4.1 从服务器下载系统软件

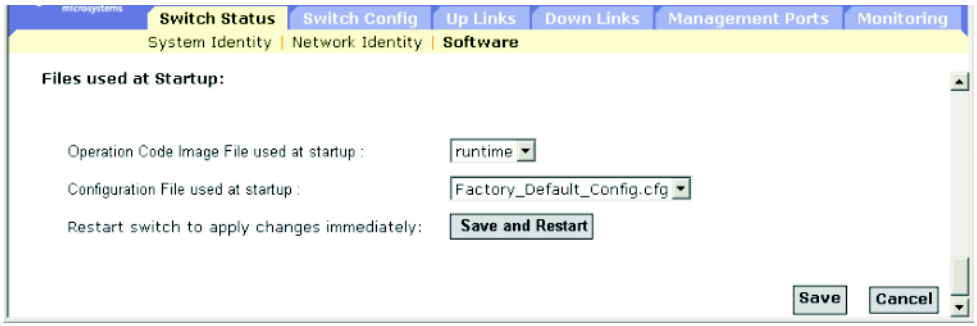
在下载运行时代码时，可以指定目标文件名来替换当前的映像，也可以先使用与当前运行时代码文件不同的名称下载文件，然后将新文件设置为启动文件。

Web — 打开 “Switch Status” => “Software”。输入 TFTP 服务器的 IP 地址，输入要下载的软件的文件名，选择交换机上要覆盖的文件或指定新文件名，然后单击 “Download”。



注：如果出现错误消息，提示您输入的数据无效，则您输入的 IP 地址或文件名可能不正确，或者您没有适当的用于执行 TFTP 传输的访问权限。另外，也可能是由于交换机内存不足所致。

如果要下载到新的目标文件，请从启动时使用的操作代码下拉框中选择文件，然后单击“Save”。要启动新固件，请单击“Save”和“Restart”，以重新引导系统。



CLI — 输入 TFTP 服务器的 IP 地址，选择“config”或“opcode”文件类型，然后输入源文件名和目标文件名，将新文件设置为系统启动文件，然后重新启动交换机。

```
Console#copy tftp file                                          4-17
TFTP server ip address: 10.1.0.99
Choose file type:
 1. config: 2. opcode: <1-2>: 2
Source file name: v10.bix
Destination file name: V10000
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#config
Console(config)#boot system opcode: V10000                      4-23
Console(config)#exit
Console#reload                                                  4-15
```

要启动新固件，必须输入“reload”命令来重新引导系统。

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围
Switch Operation Code Image Files	*未定义*		
TFTP Server IP Address	sun... tftpMgt. tftpServer	读 / 写	IP 地址
TFTP File Type	sun... tftpMgt. tftpFileType	读 / 写	opcode (1), config (2)

字段名	MIB 变量	访问权限	值范围
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	读/写	字符串 （大小 (0-127)）
TFTP Destination File Name	sun... tftpMgt. tftpDestFile	读/写	字符串 （大小 (0-127)）
TFTP Action	sun... tftpMgt. tftpAction	读/写	notDownloading (1)， downloadToPROM (2)， downloadToRAM (3) （*不支持*） upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	读/写	tftpSuccess (1)， tftpStatusUnknown (2)， tftpGeneralError (3)， tftpNoResponseFromServer (4)， tftpDownloadChecksumError (5)， tftpDownloadIncompatible Image(6)， tftpTftpFileNotFound(7)， tftpTftpAccessViolation(8)
Restart Operation Code File	sun... restartMgt. restartOpCodeFile	读/写	显示字符串 （大小 (0-127)）
Restart Action	sun... restartMgt. restartControl	读/写	running (1)， warmBoot (2)， coldBoot (3)

3.2.5 保存或恢复配置设置

可以将配置设置上载到 TFTP 服务器，也可以从 TFTP 服务器下载配置设置。日后，可以下载配置文件来恢复交换机的设置。

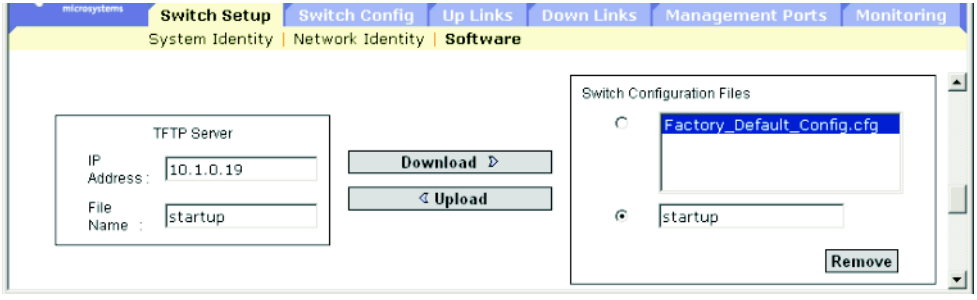
命令属性

- 目标文件名中不能包含斜杠（\ 或 /），文件名的首字母不能为点 (.)；在 TFTP 服务器上，文件名的最大长度为 127 个字符；而在交换机上，文件名的最大长度为 32 个字符。（有效字符为：A-Z、 a-z、 0-9、“.”、“-”、“_”）
- 用户定义的配置文件的最大数量受可用内存的限制。

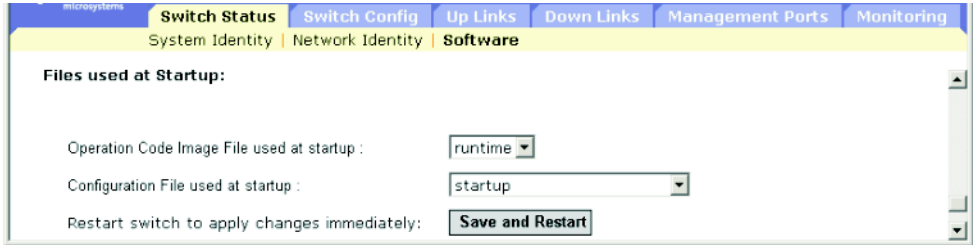
3.2.5.1 从服务器下载配置设置

可以用新文件名下载配置文件，然后将其设为启动文件；也可以将当前的启动配置文件指定为目标文件，以直接替代原来的文件。请注意，您可以将“Factory_Default_Config.cfg”文件复制到 TFTP 服务器上，但不能将其用作交换机上的目标文件。

Web — 打开 “Switch Setup” => “Software”。输入 TFTP 服务器的 IP 地址，输入要下载的文件的名称，选择交换机上要覆盖的文件或指定新文件名，然后单击“Download”。



如果您下载到新文件名下，请在下拉框中选择新文件名，然后按 “Save” 按钮。要使用新设置，请单击 “Save” 和 “Restart”，以重新引导系统。



CLI — 输入 TFTP 服务器的 IP 地址，在服务器上指定源文件，在交换机上设定启动文件名，然后重新启动交换机。

```
Console#copy tftp startup-config                                    4-17
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
System will be restarted, continue <y/n>?y
```

如果将启动配置文件下载到新文件名下，则可以在以后将该文件指定为启动文件，然后重新启动交换机。

```
Console#config
Console(config)#boot system config: startup-new                     4-23
Console(config)#exit
Console#reload                                                      4-15
System will be restarted, continue <y/n>?y
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围
TFTP Server IP Address	sun... tftpMgt. tftpServer	读 / 写	IP 地址
TFTP File Type	sun... tftpMgt. tftpFileType	读 / 写	opcode (1), config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	读 / 写	显示字符串 （大小 (0-127)）
TFTP Action	sun... tftpMgt. tftpAction	读 / 写	notDownloading (1), downloadToPROM (2), downloadToRAM (3), upload (4)

字段名	MIB 变量	访问权限	值范围
TFTP Status	sun... tftpMgt. tftpStatus	读 / 写	tftpSuccess (1)， tftpStatusUnknown (2)， tfttpGeneralError (3)， tftpNoResponseFromServer (4)， tftpDownloadChecksumError (5)， tftpDownloadIncompatibleImage(6)， tftpTftpFileNotFound(7)， tftpTftpAccessViolation(8)
Restart Configuration File	sun... restartMgt. restartConfigFile	读 / 写	显示字符串 （大小 (0-127)）
Restart Action	sun... restart.Mgt. restartControl	读 / 写	running (1)， warmBoot (2)， coldBoot (3)

3.2.6 配置用户验证

使用 “Security”菜单可以根据指定的用户名和口令限制用户进行管理访问。在配置对交换机的访问权限时，可以手动进行配置，也可以使用基于 RADIUS 或 TACACS+ 协议的远程访问验证服务器来进行配置。

访问类型有两种：“Normal”（普通访问）和 “Privileged”（特权访问）。普通访问级只能访问有限数量的命令，而特权访问级则可以访问所有命令。默认管理员帐号对管理板载代理的所有参数都具有写访问权限。因此，应尽早设定口令，并将其保存在安全的地方。

注：默认管理员的名称为 “admin”，口令为 “admin”。

命令用法

- 默认情况下，总是根据存储在本地交换机上的验证数据库来检查管理访问。如果使用远程验证服务器，则必须为每个指定的远程验证协议指定验证序列和相应的参数。
- 远程验证拨入用户服务 (RADIUS) 和终端访问控制器访问控制系统 (TACACS) 是登录验证协议，它们使用在中央服务器上运行的软件来控制对网络上可识别 RADIUS 或 TACACS 的设备的访问。验证服务器包含一个数据库，对于需要对交换机进行管理访问的每个用户或用户组，该数据库中包含了他们的用户名 / 口令对及相关的权限级别。

注：在 RADIUS 或 TACACS 服务器上设置权限级别时，请记住级别 0 允许对交换机进行 guest （即普通执行）访问。只有级别 15 才允许管理员 （即特权执行）访问。

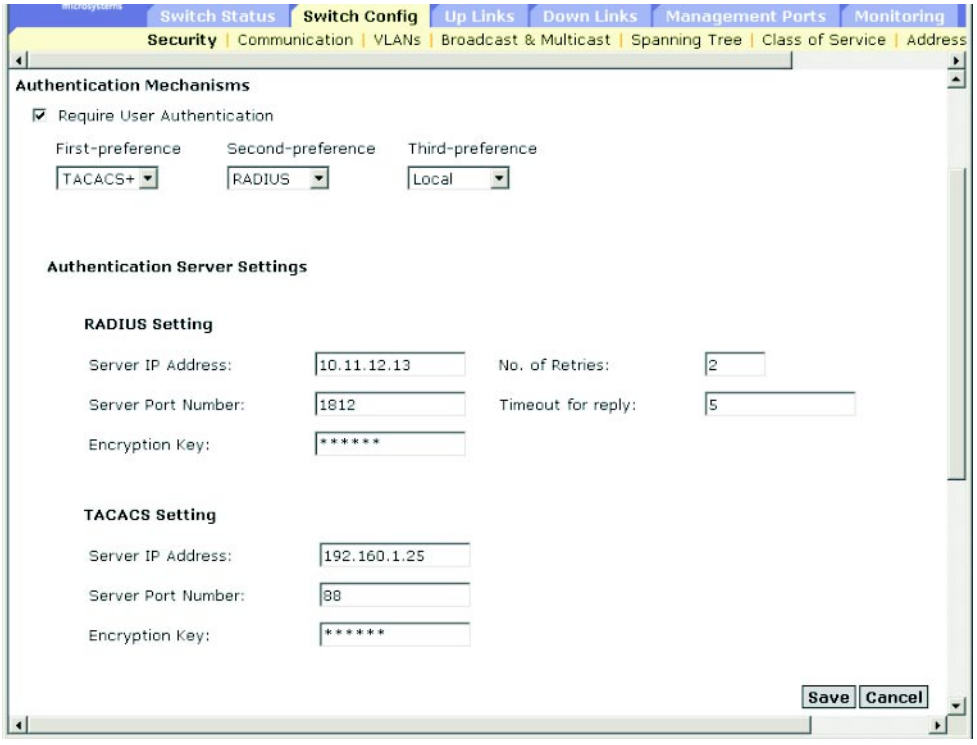
- RADIUS 使用 UDP，而 TACACS 使用 TCP。UDP 只提供尽力而为的传送，而 TCP 则提供面向连接的传输。同时，请注意， RADIUS 只对从客户机到服务器的访问请求数据包中的口令加密，而 TACACS 则对数据包的正文全部进行加密。
- RADIUS 和 TACACS 登录验证控制着通过控制台端口、Web 浏览器或 Telnet 进行的管理访问。这些权限选项必须在验证服务器上进行配置。
- RADIUS 和 TACACS 登录验证为每个用户名 / 口令对指定一个特定的权限级别。用户名、口令和权限级别必须在验证服务器上进行配置。
- 可以为任何用户指定一到三种验证方法，从而指示验证序列。例如，
  如果您选择 (1) RADIUS 和 (2) Local，则将首先验证 RADIUS 服务器上的用户名和口令。如果 RADIUS 服务器不可用，则检查本地用户名和口令。

命令属性

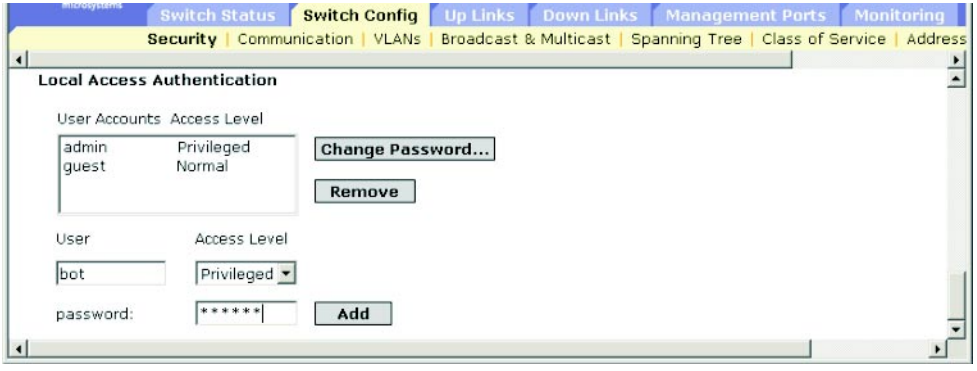
- **Authentication Mechanisms**
  - **Require User Authentication** — 指示是否需要验证。
  - **Preference** — 交换机将尝试根据指定的顺序来验证用户。
- **Authentication Server Settings**
  - **Server IP Address** — 验证服务器的地址。（默认值：10.1.0.1）
  - **Server Port Number** — 验证消息所使用的验证服务器的网络 (UDP) 端口。（范围为：1-65535 ；默认值：1812）
  - **Encryption Key** — 验证客户机登录访问所使用的加密密钥。不要在该字符串中使用空格。（最大长度：20 个字符）
  - **No. of Retries*** — 交换机通过验证服务器来验证登录访问的尝试次数。（范围为：1-30 ；默认值：2）
  - **Timeout for reply*** — 交换机在重新发送请求之前等待应答的秒数。（范围为：1-65535 ；默认值：5）
- **Local Access Authentication**
  - **User Account** — 用户的名称。
    （最大长度：8 个字符；最大用户数：5）
  - **Access Level** — 指定用户级别。
    （选项：“Normal”和 “Privileged”）
  - **Password** — 指定用户口令。
    （最大长度：8 个纯文本字符，区分大小写）

* 仅适用于 RADIUS 服务器验证。

Web — 打开 “Switch Config” => “Security”。要配置本地或远程验证首选项，请指定验证顺序 （一到三种方法），针对验证方法填写相应参数，然后单击 “Save”。



要配置本地访问的验证参数，请输入用户名、口令和访问级别，然后单击 “Add”。



CLI — 指定用户名和访问级别 （即， 0：普通访问； 15：特权访问），然后指定口令。接着，为 RADIUS 和 TACACS 远程客户机验证配置所需的设置。

```
Console(config)#username bob access-level 15                    4-26
Console(config)#username bob password smith
Console(config)#authentication login local tacacs radius        4-42
Console(config)#tacacs-server host 192.168.1.24                 4-46
Console(config)#tacacs-server port 181                          4-46
Console(config)#tacacs-server key green                         4-47
Console(config)#radius-server host 192.168.1.25                 4-43
Console(config)#radius-server port 181                          4-43
Console(config)#radius-server key white                         4-44
Console(config)#radius-server retransmit 5                      4-44
Console(config)#radius-server timeout 10                        4-45
Console(config)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
User Name	*未定义*			
Password	*未定义*			
Access Level	*未定义*			
Authentication Sequence	*未定义*			
RADIUS Server Address	sun... securityMgt.radiusMgt. radiusServerAddress	读 / 写	IP 地址	10.11.12.13
RADIUS Server Port Number	sun... securityMgt.radiusMgt. radiusServerPortNumber	读 / 写	整数 (1-65535)	1812
RADIUS Server Encryption Key	sun... securityMgt.radiusMgt. radiusServerKey	读 / 写 （读访问 总是返回 0）	字符串 （大小 (0-20)）	
RADIUS Server Retransmit	sun... securityMgt.radiusMgt. radiusServerRetransmit	读 / 写	整数 (1-65535)	2
RADIUS Server Timeout	sun... securityMgt.radiusMgt. radiusServerTimeout	读 / 写	整数 (1-65535) 秒	5
TACACS Server Address	sun... securityMgt.tacacsMgt. tacacsServerAddress	读 / 写	IP 地址	

字段名	MIB 变量	访问权限	值范围	默认值
TACACS Server Port Number	sun... securityMgt.tacacsMgt. tacacsServerPortNumber	读 / 写	整数 (1-65535)	
TACACS Server Encryption Key	sun... securityMgt.tacacsMgt. tacacsServerKey	读 / 写（读访问总是返回 0）	字符串（大小 (0-20)）	

3.2.7 配置 SNMP

SNMP （简单网络管理协议）是专门为管理网络上的设备或其它组件而设计的一种通信协议。通常使用 SNMP 来进行管理的设备包括交换机、路由器和主机。一般情况下是使用 SNMP 对这些设备进行配置，使它们能在网络环境中正常运行，同时对它们进行监视，以评估网络性能或检测潜在的问题。

交换机中有一个板载 SNMP 代理，它不间断地对交换机硬件的状态和通过交换机端口的通信进行监视。网络管理站可以使用软件 （如 SunNet Manager）来访问这些信息。对板载代理的访问权限是由社区字符串控制的。要与交换机通信，管理站首先必须提交有效的社区字符串以供验证。以下各节将介绍用于配置社区字符串和相关陷阱功能的选项。

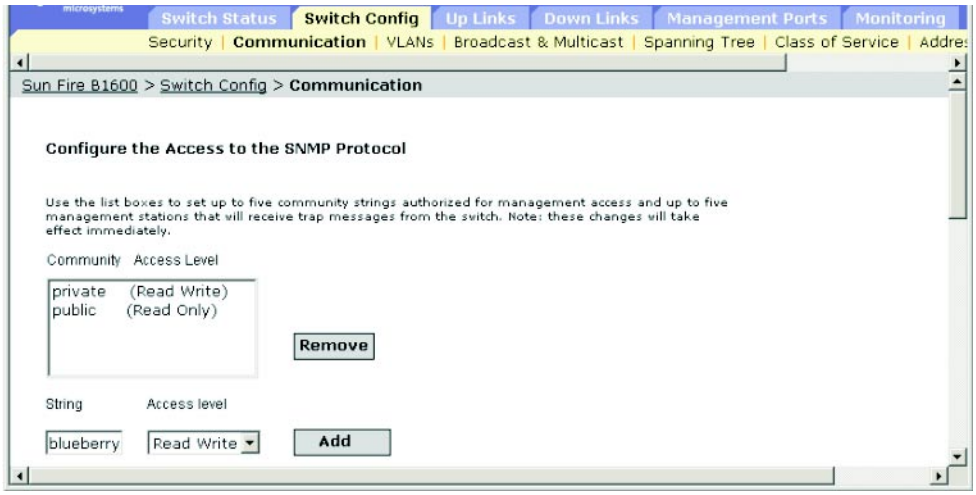
3.2.7.1 配置对 SNMP 协议的访问

最多可以配置五个社区字符串，经过验证后，它们可用于管理访问。出于安全原因，应该考虑删除默认字符串。

命令属性

- **Community** — 社区字符串的作用与口令相似，并且它允许对SNMP协议进行访问。默认字符串：“public”（只读访问）、“private”（读 / 写访问）
  - 范围：1-32 个字符，区分大小写
  - 默认值：“public”（只读访问）、“private”（读 / 写访问）
- **Access Level**
  - **Read Only** — 指定只读访问。经授权的管理站只能检索 MIB 对象。
  - **Read/Write** — 指定读 / 写访问。经授权的管理站既能检索 MIB 对象，又能修改 MIB 对象。

Web — 打开 “Switch Config” => “Communication”。根据需要添加新的社区字符串，从 “Access Level” 下拉列表中选择访问权限，然后单击 “Add”。



CLI — 以下示例添加具有读/写访问权限的字符串 “blueberry”。

```
Console(config)#snmp-server community blueberry rw              4-48
Console(config)#
```

SNMP — 等效 MIB 变量。

这些功能没有 MIB 变量。

3.2.7.2 指定陷阱管理器和陷阱类型

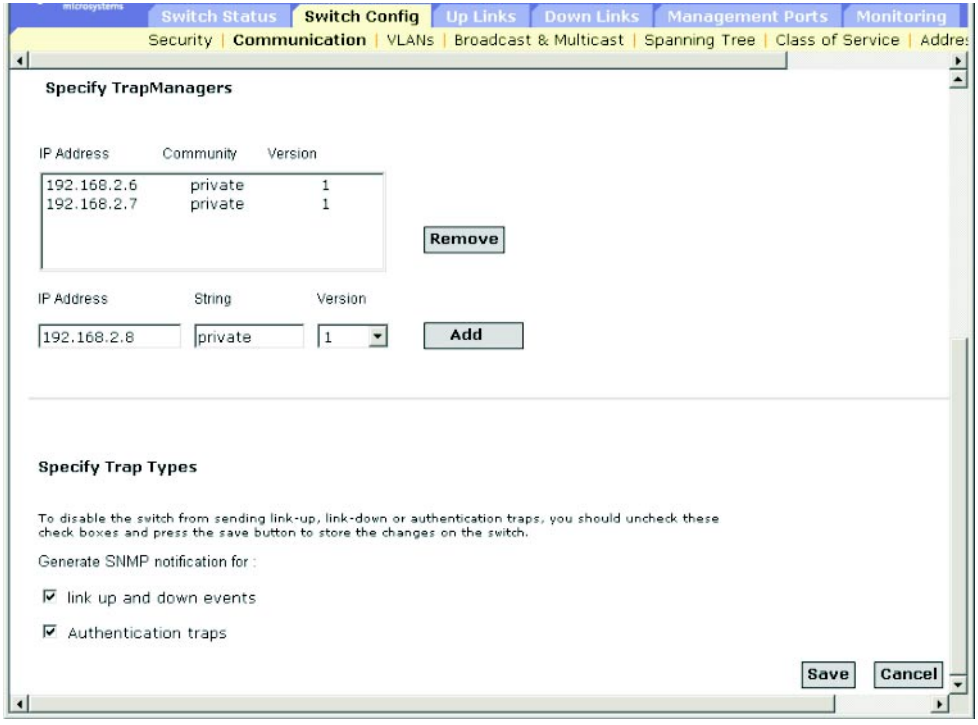
指示状态变化的陷阱是由交换机向指定的陷阱管理器发出的。您必须指定陷阱管理器，该交换机才会向管理站 （使用网络管理平台，如 SunNet Manager）报告重要事件。最多可以指定五个管理站来接收来自交换机的陷阱消息。该交换机所支持的陷阱列在第 A-3 页上的 “支持的陷阱” 中。

命令属性

- **IP Address** — 主机 （目标接收者）的 Internet 地址。（最大主机地址数：5 个陷阱目标 IP 地址条目）
- **Community** — 与口令相似的社区字符串，与通知操作一起发送。虽然可以在陷阱管理器表中设置该字符串，但建议您也要在 SNMP 协议表中定义该字符串。（最大长度：32 个字符）

- **Version** — 指示主机运行的是 SNMP 版本 1 还是版本 2c。
- **Generate SNMP notification for**
  - **Port link up and down events** — 当端口链接建立或中断时，发出陷阱消息。
  - **Authentication traps** — 在验证 SNMP 访问的过程中，只要提交了无效的社区字符串，就会发出陷阱消息。

Web — 打开 “Switch Setup” => “Communications”。为每个将接收这些消息的陷阱管理器填写 IP 地址和社区字符串，然后单击 “Add”。如果需要，请选中 “Port link up and link down events”或 “Authentication traps”复选框，然后单击 “Save”。



CLI — 本示例将添加一个陷阱管理器，并启用链接建立陷阱、链接断开陷阱以及验证陷阱。

```
Console(config)#snmp-server host 10.1.0.19 private version 1   4-50
Console(config)#snmp-server enable traps link-up-down          4-51
Console(config)#snmp-server enable traps authentication
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Trap Destination Address	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestAddress	无访问权限	IP 地址	
Trap Destination Community	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestCommunity	读 / 创建	字符串 （大小 (0-127)）	
Trap Destination Version	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	读 / 创建	version 1 (1)，version 2 (2)	
Trap Destination Status	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	读 / 创建	valid (1)，invalid (2)	
Enable Link-up-down Traps	MIB-II ifMIB.ifMIBObjects. ifXTable.ifXEntry. ifLinkUpDownTrapEnable	读 / 写	enabled (1)，disabled (2)	enabled

3.3 配置全局网络协议

本节介绍如何配置全局交换机设置，以便启用虚拟 LAN、多点传送服务、生成树算法，并根据特定的服务类别要求处理数据，以及显示地址表或设置静态地址。

3.3.1 VLAN 配置

在带有路由器的常规网络中，广播通信被分隔到不同的域中。交换机本质上不支持广播域。在处理如 IPX 或 NetBeui 等通信的大型网络中，这可能会导致广播风暴。通过使用符合 IEEE 802.1Q 的 VLAN，可以将任意一组网络节点组合到单独的广播域中，从而将广播通信限制在起源组内。这样做，还可以使网络环境更为安全和更干净。

IEEE 802.1Q VLAN 是一组端口，它们可以位于网络中的任何地方；但在进行通信时，它们就象处在同一个物理段上一样。

VLAN 有助于简化网络管理，因为它允许在不更改任何物理连接的情况下，将设备移到新的 VLAN 中。可以轻松地对 VLAN 进行组织，使其反映部门组 （如营销部门或研发部门）、应用组 （如电子邮件）或多点传送组 （多媒体应用，如视频会议）。

通过减少广播通信量，VLAN 可以提高网络效率，且不必更新 IP 地址或 IP 子网就可以进行网络更改。 VLAN 本身可以提供高级别的网络安全性，这是因为通信必须通过已配置的第 3 层链接才能到达其它 VLAN。

该交换机支持以下 VLAN 功能：

- 多达 255 个 VLAN （基于 IEEE 802.1Q 标准）
- 跨多台交换机的分布式 VLAN 了解功能 （这些交换机采用显式或隐式标记并使用 GVRP 协议）
- 端口重叠功能，允许一个端口参与到多个 VLAN 中
- 终端站可以属于多个 VLAN。
- 在可识别 VLAN 和不可识别 VLAN 的设备之间传递通信
- 优先级标记

将端口分配给 VLAN

在对交换机启用 VLAN 之前，首先必须将每个端口分配给该端口将参与的 VLAN 组。默认情况下，所有端口均作为未标记的端口分配给 VLAN 1。如果您希望某个端口承载一个或多个 VLAN 的通信，而且位于连接另一端的任何中间网络设备或主机均支持 VLAN，则将该端口作为带标记的端口添加到相应的一个或多个 VLAN 中。然后使用 GVRP，通过手动或动态方式，将承载该通信的路径上其它可识别 VLAN 的网络设备上的端口分配给相同的 （一个或多个） VLAN。然而，如果您希望该交换机上的端口参与一个或多个 VLAN，但位于连接另一端的所有中间网络设备和主机均不支持 VLAN，则应该将该端口作为未标记的端口添加到 VLAN 中。

注：标记为指向某个 VLAN 的帧可以通过可识别 VLAN 或不可识别 VLAN 的网络互连设备，但不能用于任何不支持 VLAN 标记的末端节点主机。

VLAN 分类 — 当交换机收到一帧时，它将按两种方式之一对其进行分类。如果该帧是未标记帧，交换机将其分配给相关的 VLAN （根据接收端口的 PVID）。但如果该帧是带标记帧，交换机将使用带标记的 VLAN ID 来标识该帧的端口广播域。

端口重叠 — 使用端口重叠功能，不同的 VLAN 组均可访问共享的网络资源，如文件服务器或打印机。请注意，如果 VLAN 不支持端口重叠功能，但仍需要进行通信，请使用第 3 层路由器或交换机将它们连接起来。

基于端口的 VLAN — 基于端口的 （静态） VLAN 是通过手动方式与特定端口联结在一起的。交换机的转发决定是根据目标 MAC 地址及其关联的端口做出的。因此，为了能够做出有效的转发或扩散决定，交换机在运行时必须了解 MAC 地址与其相关端口（进而与 VLAN）的关系。但是，如果启用 GVRP，这一过程可以完全自动实现。

自动 VLAN 注册 — GARP VLAN 注册协议 （GVRP）定义了一个系统，交换机根据该系统可以自动了解应将每个终端站分配给哪些 VLAN。如果终端站 （或其网络适配器）支持 IEEE 802.1Q VLAN 协议，则可以对其进行配置，使其向网络广播消息，以指示它要加入的 VLAN 组。当该交换机收到这些消息时，它自动将接收端口置于指定的 VLAN 中，然后将消息转发到所有其它端口上。当消息到达另一台支持 GVRP 的交换机时，它也会将接收端口置于指定的 VLAN 中，然后将消息传递到所有其它端口上。通过这种方式， VLAN 要求将传遍整个网络。这样，仅根据终端站的请求就可以自动配置与 GVRP 兼容的设备，以满足 VLAN 组的需要。

要在网络中实施 GVRP，首先应将主机设备添加到所需的 VLAN （使用操作系统或其它应用程序软件）中，以便可以将这些 VLAN 传播到网络上。无论是直接连接到这些主机的边缘交换机，还是网络中的核心交换机，都需要在这些设备之间的链接上启用 GVRP。（请参阅第 3-89 页上的 “配置接口的 VLAN 行为”。）还应该在网络中确定安全界线，并在终端站端口上禁用 GVRP （因为需要防止在这些端口上传播广告），或禁止端口加入受限的 VLAN 中。

注：如果主机设备不支持 GVRP，则必须为连接到这些设备的交换机端口配置静态 VLAN （如第 3-39 页上的 “向 VLAN 添加静态成员”中所述）。不过，您仍然需要在这些边缘交换机上启用 GVRP，对于网络上的核心交换机也是如此。

转发带标记帧 / 未标记帧

如果要为直接连接到单台交换机的设备创建一个小型的基于端口的 VLAN，您可以将端口指定给同一未标记的 VLAN。然而，要参与跨多台交换机的 VLAN 组，则需要为该组创建一个 VLAN，并在所有端口上启用标记。

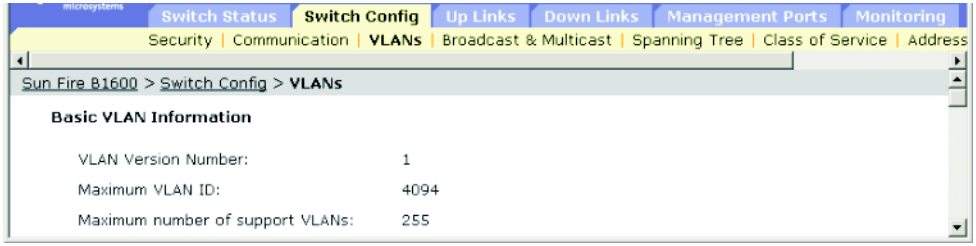
可以将端口分配给多个带标记或未标记的 VLAN。因此，交换机上的每个端口都可以传输带标记或未标记的帧。如果从该交换机沿着包含任何可识别 VLAN 设备的路径转发一帧，交换机中应该包含 VLAN 标记。当从该交换机沿着不含任何可识别 VLAN 设备 （包括目标主机）的路径转发一帧时，交换机首先必须去除 VLAN 标记才能转发该帧。当交换机收到带标记的帧时，它将该帧传输到帧标记所指示的 VLAN 上。然而，当该交换机从不可识别 VLAN 的设备上收到未标记帧时，它首先确定转发该帧的目标位置，然后加上一个反映入口端口默认 VID 的 VLAN 标记。

3.3.1.1 显示基本 VLAN 信息

命令属性

- **VLAN Version Number** — 此交换机根据 IEEE 802.1Q 标准规定所使用的 VLAN 版本。
- **Maximum VLAN ID** — 此交换机识别的最大 VLAN ID。
- **Maximum Number of Supported VLANs** — 可以在此交换机上配置的最大 VLAN 数量。

Web — 打开 “Switch Config” => “VLANs”。



CLI — 输入以下命令。

```
Console#show bridge-ext                                          4-117
 Max support vlan numbers: 32
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning:IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 Global GVRP status: Disabled
 GMRP: Disabled
Console#
```

SNMP — 等效 MIB 变量。

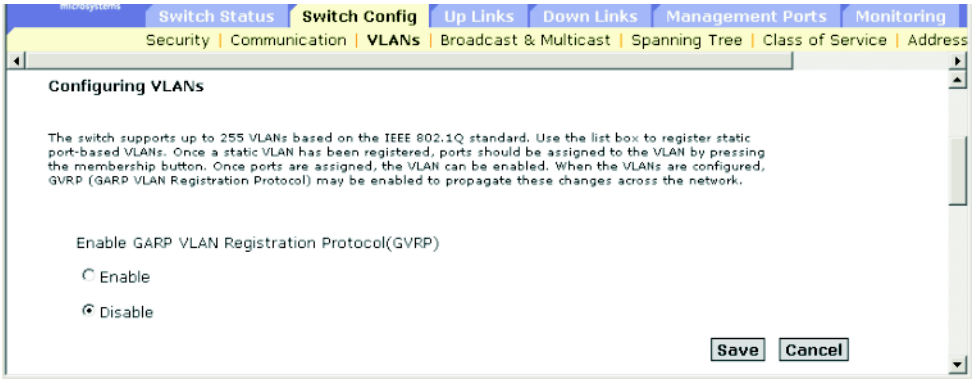
字段名	MIB 变量	访问权限	值范围	默认值
VLAN Version Number	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qVlanVersion-Number	只读	version1 (1)	version1
Maximum VLAN ID	MIB-II. dot1dBridge. BridgeMIB. BridgeMIBObjects. dot1qBase. dot1qMaxVlanId	只读	整数	4094
Maximum Number of Supported VLANs	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qMaxSupportedVlans	只读	整数	255

字段名	MIB 变量	访问权限	值范围	默认值
Device Capabilities	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dDeviceCapabilities	只读	位字符串 — ExtendedFiltering dot1dServices (0)， dot1dTrafficClasses (1)， StaticEntry dot1dIndividualPort (2)， dot1dIVLCapable (3)， dot1dSVLCapable (4)， dot1dHybridCapable (5)， dot1dConfigurablePvid dot1dTagging (6)， dot1dLocalVlanCapable (7)	2, 3, 6, 7
Traffic Classes Enabled	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dTrafficClasses-Enabled	读 / 写	true (1)， false (2)	true
GMRP Status	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dGmrpStatus	读 / 写	enabled (1)， disabled (2)	disabled
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	读 / 写	enabled (1)， disabled (2)	disabled

3.3.1.2 启用或禁用 GVRP （全局设置）

GARP VLAN 注册协议 (GVRP) 定义了各交换机之间交换 VLAN 信息的方式，以便实现在整个网络的所有端口上注册 VLAN 成员。 VLAN 是根据主机设备发出的加入消息来动态进行配置的，并在整个网络中传播。必须启用 GVRP，以便自动进行 VLAN 注册和支持延伸到本地交换机之外的 VLAN。

Web — 打开 “Switch Config” => “VLANs”。启用或禁用 GVRP，然后单击 “Save”。



CLI — 本示例为交换机启用 GVRP。

```
Console(config)#bridge-ext gvrp                    4-117
Console(config)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	读 / 写	enabled (1), disabled (2)	disabled

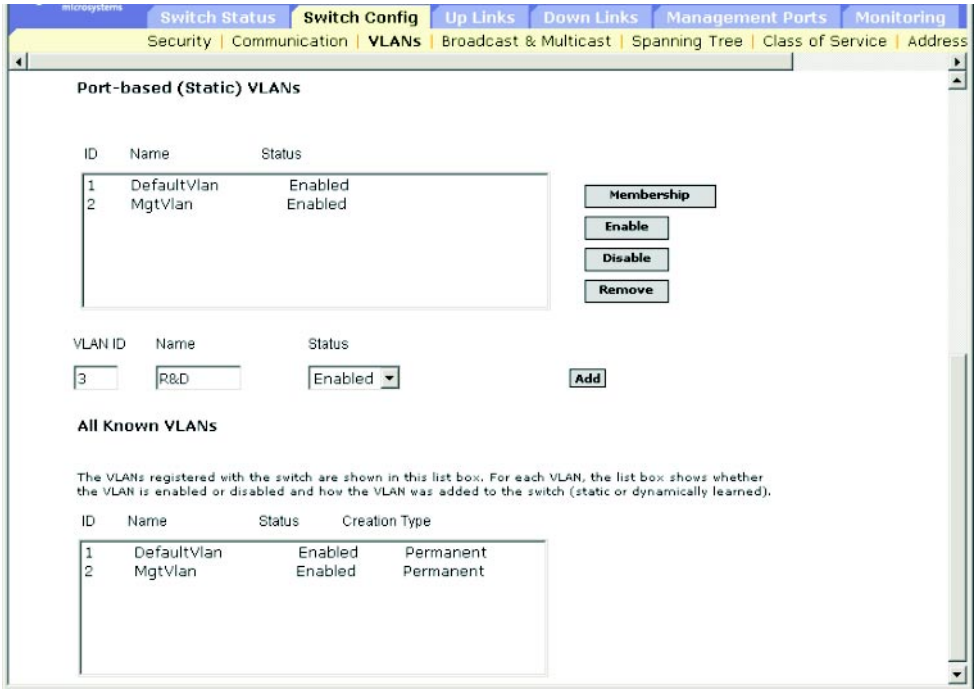
3.3.1.3 配置 VLAN

命令属性

- **ID** — 已配置的 VLAN 的 ID (1-4094)。
- **Name** — VLAN 的名称 （1 至 15 个字符）。
- **Status** — 显示是启用还是禁用此 VLAN。
  - **Enable** （活动 *）— VLAN 处在活动状态。
  - **Disable** （挂起 *）— VLAN 处于挂起状态，即不传递数据包。
- **Creation Type** — 显示将此 VLAN 添加到交换机的方式。
  - **Dynamic GVRP** （动态 *）：通过 GVRP 自动了解。
  - **Permanent** （静态 *）：添加为静态条目。
- **Ports/Channel groups*** — 显示 VLAN 接口成员。

* CLI 显示这些术语。

Web — 打开 “Switch Config” => “VLANs”。要创建新的 VLAN，请输入 VLAN ID 和名称，将状态设置为 “Enabled”或 “Disabled”，然后单击 “Add”。要修改现有的 VLAN，请选择一个或多个条目，然后单击 “Enable”、“Disable”或 “Remove”。要向 VLAN 添加接口，请选择条目并单击 “Membership”。（请参阅第 3-39 页上的 “向 VLAN 添加静态成员”。）



CLI — 本示例创建一个新的 VLAN，并显示所有 VLAN 信息。

```
Console(config)#vlan database                                                    4-105
Console(config-vlan)#vlan 3 name R&D media ethernet state active                 4-105
Console(config-vlan)#
Console#show vlan                                                                4-112
VLAN Type    Name              Status    Ports/Channel groups
---- ------- ----------------- --------- -----------------------------------------
   1  Static      DefaultVlan    Active     SNP0    SNP1    SNP2    SNP3    SNP4
                                            SNP5    SNP6    SNP7    SNP8    SNP9
                                           SNP10   SNP11   SNP12   SNP13   SNP14
                                           SNP15   NETP0   NETP1   NETP2   NETP3
                                           NETP4   NETP5   NETP6   NETP7
   2  Static          MgtVlan    Active  NETMGT
   3  Static              R&D    Active
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
VLAN ID	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanIndex	无访问权限	整数	1
VLAN Name	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	读 / 创建	八位字节字符串 （大小 (0-32)）	
VLAN Status	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic. RowStatus	读 / 创建	enable(1)， disable(2)	
VLAN Type	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	只读	其它 (1)， permanent(2)， dynamicGvrp(3)	

字段名	MIB 变量	访问权限	值范围	默认值
VLAN Ports	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCurrent- EgressPorts	只读	八位字节字符串 （端口列表）	

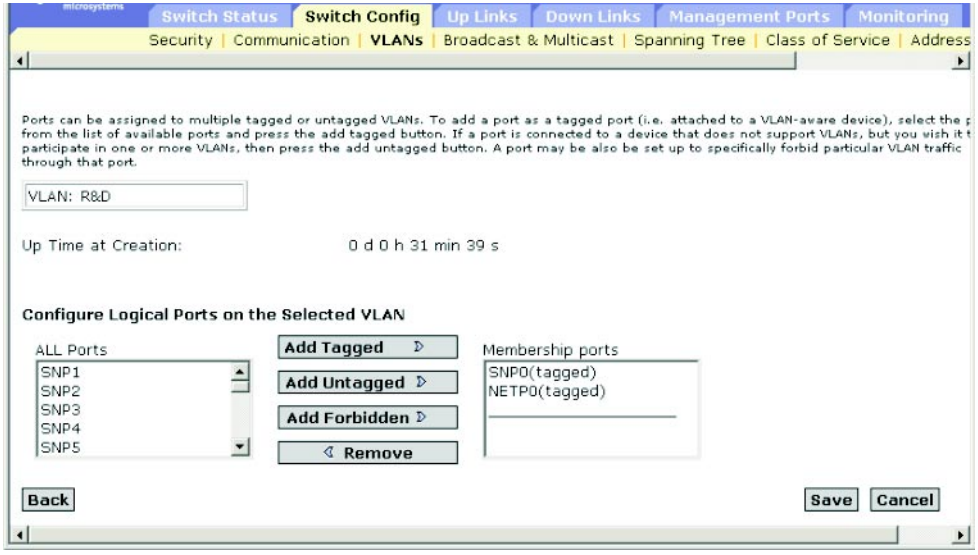
3.3.1.4 向 VLAN 添加静态成员

命令属性

- **Name** — VLAN 的名称。
- **Up Time at Creation** — 创建此 VLAN 的时间。
- **Status*** — 显示将此 VLAN 添加到交换机的方式。
  - **Dynamic**：通过 GVRP 自动了解。
  - **Static**：添加为静态条目。
- **All Ports** — 端口或聚合组标识符。
- **Membership Ports** — 作为带标记成员或未标记成员添加到选定 VLAN 中的接口，或禁止通过 GVRP 自动添加的接口。
- **Membership Type** — 通过突出显示所需接口并单击相应的 “Add”按钮来指定 VLAN 成员：
  - **Add Tagged**：接口是 VLAN 的成员。此 VLAN 上的端口所传输的所有数据包都将被标记，即携带一个标记，也就携带了 VLAN 或 CoS 信息。
  - **Add Untagged**：接口是 VLAN 的成员。该端口传输的所有数据包将不被标记，即不携带标记，因此也不携带 VLAN 信息或 CoS 信息。
  - **Add Forbidden**：禁止接口自动通过 GVRP 加入 VLAN。请参阅第 3-32 页上的 “自动 VLAN 注册”。
  - **Remove**：从该 VLAN 删除选定接口。

* 仅适用于 CLI。

Web — 打开 “Switch Config” => “VLANs”。突出显示静态列表中的某个 VLAN，然后单击 “Membership”。从端口成员页的 “All Ports” 列表 （即端口或聚合组）中选择一个接口，然后单击 “Add Tagged”、“Add Untagged” 或 “Add Forbidden” （即禁止通过 GVRP 添加此接口）。要删除接口，请从 “Membership Ports” 列表中选择相应的条目，然后单击 “Remove”。



CLI — 本示例添加若干个端口，然后显示 VLAN 成员。

```
Console(config)#interface ethernet NETP1                          4-74
Console(config-if)#switchport allowed vlan add 3 tagged           4-110
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#switchport allowed vlan add 3 untagged
Console(config-if)#exit
Console(config)#interface ethernet SNP13
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#end
Console#show vlan id 3
VLAN Type    Name              Status    Ports/Channel groups
---- ------- ---------------- --------- -------------------------
   3  Static              R&D    Active   NETP1   NETP2
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
VLAN ID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	索引	行	
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	读 / 创建	八位字节字符串 （大小 (0-32)）	
Up Time at Creation	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCreationTime	只读	计时时间 （厘秒）	
VLAN Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	只读	其它 (1)， permanent(2)， dynamicGvrp(3)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic-UntaggedPorts	读 / 创建	八位字节字符串 （端口列表）	

字段名	MIB 变量	访问权限	值范围	默认值
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden-EgressPorts	读 / 创建	八位字节字符串（端口列表）	
Port Trunk Index (Channel Groups)	sun... portMgt. portTable portEntry. portTrunkIndex	只读	整数	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic-RowStatus	读 / 创建	enable(1), disable(2)	

3.3.2 多点传送配置

多点传送用于支持实时应用程序，例如视频会议或流式音频。多点传送服务器不须与每台客户机建立单独的连接。它只是向网络广播其服务，任何想要接收多点传送服务的主机均应向其本地多点传送交换机 / 路由器注册。虽然这种方法可以减少多点传送服务器所需的网络开销，但必须在广播通信所通过的每一台多点传送交换机 / 路由器上仔细地截断这些通信，以确保它们只传递到已预订了此服务的主机。

此交换机使用 IGMP （因特网组管理协议）在所连接的主机中查询那些想要接收特定多点传送服务的主机。它可识别请求加入服务的主机所在的端口，并只将数据发送到这些端口。然后，此交换机将服务请求向上传播给任何相邻的多点传送交换机 / 路由器，以确保它将继续接收多点传送服务。此过程称为多点传送过滤。

IP 多点传送过滤的目的是为了优化交换网络的性能，以便多点传送数据包只转发到那些包含多点传送组主机或多点传送路由器 / 交换机的端口，而不会将通信扩散到子网 (VLAN) 中的所有端口上。

3.3.2.1 配置 IGMP 侦听参数

可以对交换机进行配置，使之以智能方式转发多点传送通信。根据 IGMP 查询和报告消息，交换机只将通信转发到那些请求多点传送通信的端口。这样，可以防止交换机将通信广播到所有端口，从而避免损坏网络性能。

命令用法

- **IGMP Snooping** — 此交换机可以被动地侦听在IP多点传送路由器/交换机和IP多点传送主机组之间传输的 IGMP 查询和报告数据包，以识别 IP 多点传送组成员。它只是监视通过它的 IGMP 数据包，提取组注册信息，并相应地配置多点传送过滤器。
- **IGMP Querier** — 路由器或启用多点传送的交换机可以定期询问其主机是否要接收多点传送通信。如果 LAN 上有多台路由器/交换机正在执行 IP 多点传送，则会选择其中一台设备作为 “查询器”，以承担查询 LAN 中的组成员的任务。然后，此设备将服务请求向上传播给任何上游的多点传送交换机/路由器，以确保它将继续接收多点传送服务。

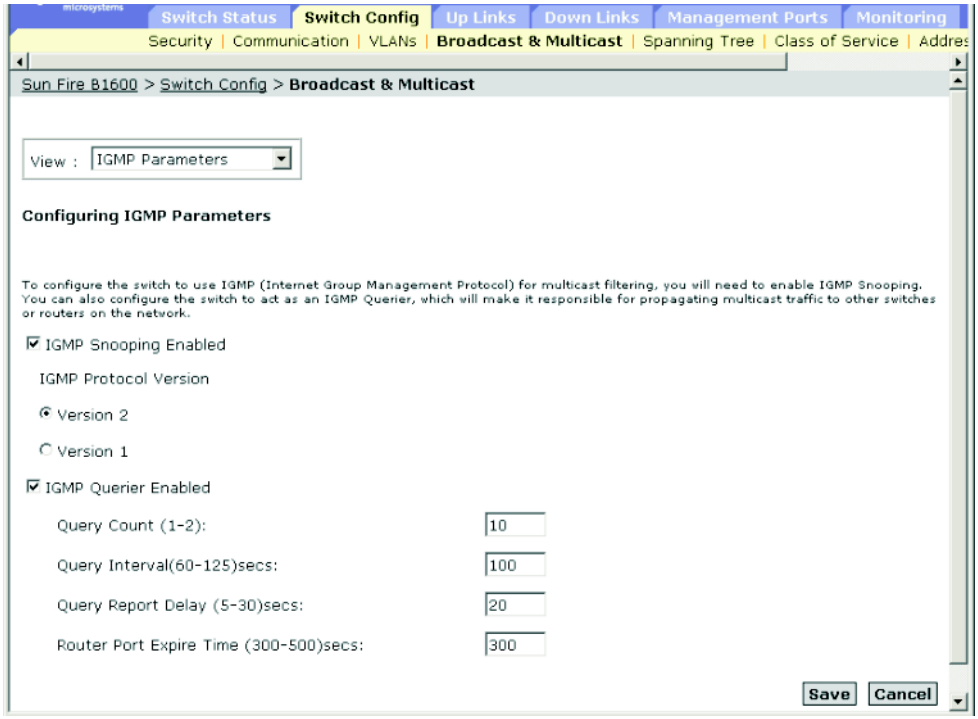
注：多点传送路由器使用此信息以及多点传送路由协议 （如 DVMRP）来支持因特网中的 IP 多点传送。

命令属性

- **IGMP Snooping** — 启用该属性后，交换机将监视网络通信，以确定哪些主机想要接收多点传送通信。（默认值：Disabled）
- **IGMP Protocol Version** — 设置协议版本，以便与网络中的其它设备兼容。（默认值：2 ；范围：1-2）
- **IGMP Querier** — 启用此属性后，交换机可以充当 “查询器”，负责询问各主机是否要接收多点传送通信。（默认值：Disabled）
  - **Query Count** — 设置在查询器采取措施从多点传送组中删除某客户机之前，已发出但没收到响应的最大查询数。（默认值：2 ；范围：2-10）
  - **Query Interval** — 设置交换机发送 IGMP 主机查询消息的频率。（默认值：125 秒；范围：60-125）
  - **Query Report Delay** — 设置交换机在接收有关某端口上的 IP 多点传送地址的 IGMP 报告之后，到交换机从该端口发出 IGMP 查询并从其列表中删除该条目之前的一段时间。（默认值：10 秒；范围：5-25）
  - **Router Port Expire Time** — 在前一个查询器停止查询之后，到交换机确定 （用于接收查询数据包的）接口已不再与查询器连接的等待时间。（默认值：300 秒；范围：300-500）

注：子网上的所有系统必须支持同一版本。某些属性仅对 IGMPv2 启用，包括 “IGMP Report Delay”和 “Router Port Expire Time”。

Web — 单击 “Switch Config” => “Broadcast & Multicast” => “IGMP Parameters”。根据需要调整 IGMP 设置，然后单击 “Save”。



CLI — 本示例修改多点传送过滤的设置，然后显示当前状态。

```
Console(config)#ip igmp snooping                              4-120
Console(config)#ip igmp snooping querier                      4-123
Console(config)#ip igmp snooping query-count 10               4-124
Console(config)#ip igmp snooping query-interval 100           4-125
Console(config)#ip igmp snooping query-max-response-time 20   4-125
Console(config)#ip igmp router-port-expire-time 300           4-126
Console(config)#ip igmp snooping version 2                    4-121
Console(config)#exit
Console#show ip igmp snooping                                 4-122
 Igmp Snooping Configuration
 ---------------------------------------------
 Service status           : Enabled
 Querier status           : Enabled
 Query count              : 10
 Query interval           : 100 sec
 Query max response time  : 20 sec
 Query time-out           : 300 sec
 IGMP snooping version    : Version 2
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Snooping Status	sun... igmpSnoopMgt. igmpSnoopStatus	读 / 写	enabled (1), disabled (2)	enabled
Snooping Querier	sun... igmpSnoopMgt. igmpSnoopQuerier	读 / 写	enabled (1), disabled (2)	enabled
Snooping Query Count	sun... igmpSnoopMgt. igmpSnoopQueryCount	读 / 写	整数 (2-10)	2
Snooping Query Interval	sun... igmpSnoopMgt. igmpSnoop-QueryInterval	读 / 写	整数 (60-125) 秒	125
Snooping Query Max Response Time	sun... igmpSnoopMgt. igmpSnoopQuery-MaxResponseTime	读 / 写	整数 (5-25) 秒	10
Snooping Router Port Expire Time	sun... igmpSnoopMgt. igmpSnoopRouterPort-ExpireTime	读 / 写	整数 (300-500) 秒	300
Snooping Version	sun... igmpSnoopMgt. igmpSnoopVersion	读 / 写	整数 (1-2)	2

3.3.2.2 指定与多点传送路由器相连的接口

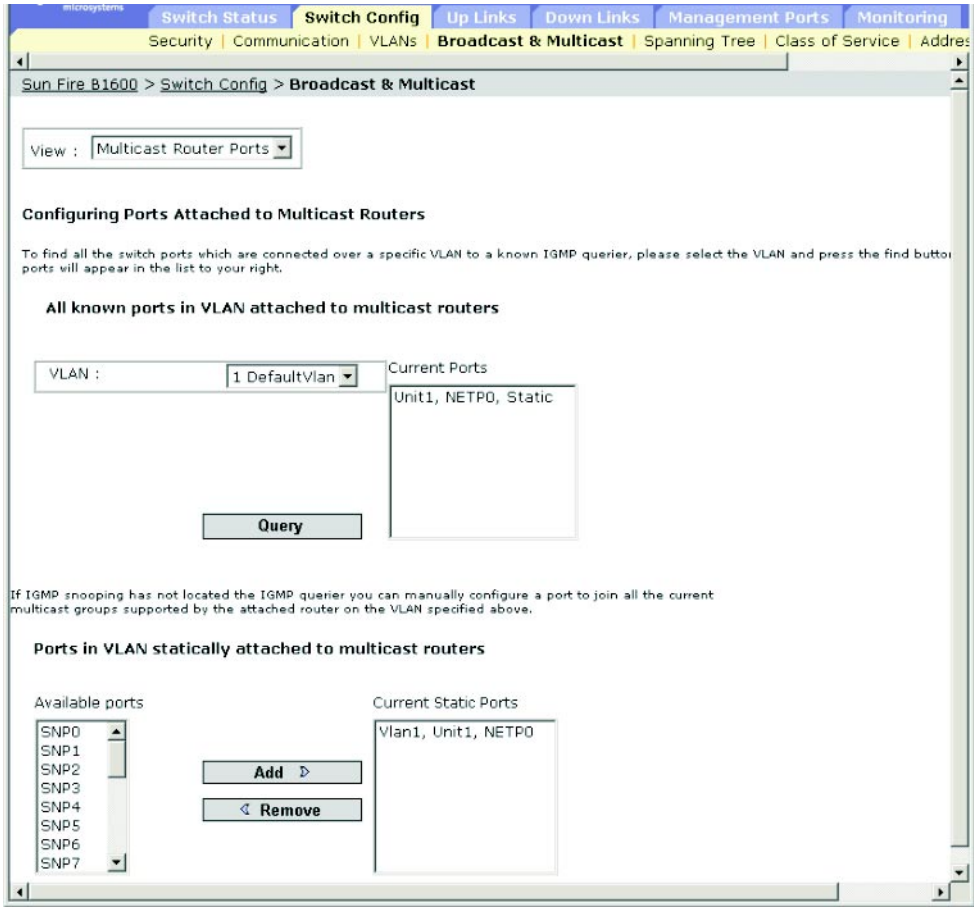
多点传送路由器使用从 IGMP 查询得到的信息以及多点传送路由协议 （如 DVMRP） 来支持在因特网中进行 IP 多点传送。这些路由器可以由交换机动态查找，也可以静态地分配给交换机上的端口。

根据网络连接的情况不同， IGMP 侦听可能始终无法找到 IGMP 查询器。因此，如果 IGMP 查询器是一个已知的多点传送路由器 / 交换机，而且它通过网络连接到交换机上的某个接口 （端口或聚合组），则可以手动配置该接口 （以及指定的 VLAN），使之加入所连接的路由器支持的当前所有多点传送组。这样，可以确保多点传送通信传递到交换机中的所有正确接口上。

命令属性

- VLAN 中所有与多点传送路由器相连的已知端口 —
  - **VLAN** — 选择此交换机上的 VLAN。
    （此下滚列表包括 VLAN ID 和名称。）
  - **Interface** — 显示与某个多点传送路由器相连的接口，以及分配是静态 (Static) 还是动态 (IGMP) 的。
- VLAN 中静态地与多点传送路由器相连的端口 —
  - **Available Ports** — 显示尚未分配给选定 VLAN 作为多点传送路由器端口的接口。
  - **Current Static Ports** — 显示已分配给选定 VLAN 作为多点传送路由器端口的接口。

Web — 单击 “Switch Config” => “Broadcast & Multicast” => “Multicast Router Ports”。选择一个 VLAN 并单击 “Query”，以显示该 VLAN 中所有与多点传送路由器相连的接口，或使用 “Add” / “Remove” 按钮静态地将接口连接到多点传送路由器。



CLI — 本示例将端口 NETP0 配置为 VLAN 1 中的多点传送路由器端口。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0  4-127
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                    4-128
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1              NETP0 Static
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围
Snooping Multicast Router Current VLAN	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. dot1qVlanIndex	索引	整数
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	读 / 创建	八位字节字符串（大小 (0-32)）
Snooping Multicast Router Current Ports	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. igmpSnoopRouterCurrentPorts	只读	八位字节字符串（端口列表）
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. dot1qVlanIndex	索引	整数
Snooping Multicast Router Static Ports	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticPorts	读 / 创建	八位字节字符串（端口列表）
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	读 / 创建	valid(1)，invalid(2)

3.3.2.3 配置多点传送服务

可以使用 IGMP 侦听和 IGMP 查询消息动态地配置多点传送过滤 （请参阅第 3-43 页上的 “配置 IGMP 侦听参数”）。对于某些需要更严格控制的应用程序，可能需要手动为特定接口分配多点传送服务。首先，将所有与参与主机相连的端口添加到一个共同的 VLAN 中，然后为该 VLAN 组分配多点传送服务。

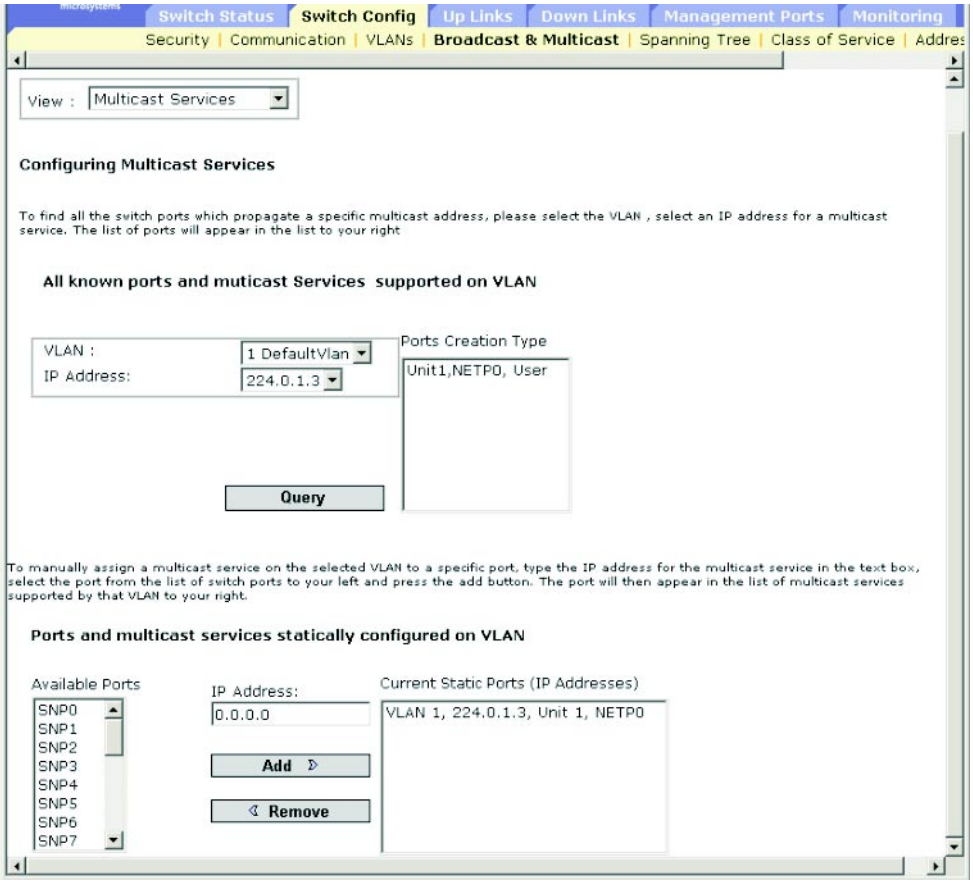
命令用法

- 静态多点传送地址绝对不会过期。
- 在为特定 VLAN 中的接口静态配置多点传送地址后，相应的通信只能转发至该 VLAN 中的端口。

命令属性

- VLAN 中支持的所有已知端口和多点传送服务 —
  - **VLAN** — 选择此交换机上的 VLAN。（此下滚列表包括 VLAN ID 和名称。）
  - **IP Address** — 特定多点传送服务的 IP 地址。
  - **Interface** — 显示与某个多点传送路由器相连的接口，以及分配是静态 (用户) 还是动态 (IGMP) 的。
- 在 VLAN 上静态配置的端口和多点传送服务 —
  - **IP Address** — 特定多点传送服务的 IP 地址。
  - **Available Ports** — 显示尚未分配给选定 VLAN 来支持特定多点传送服务的接口。
  - **Current Static Ports (IP Addresses)** — 显示已分配给选定VLAN以传播特定多点传送服务的接口。还显示分配给该接口的 IP 地址。

Web — 单击“Switch Config”=>“Broadcast & Multicast”=>“Multicast Support”。要显示传播特定多点传送服务的交换机接口，请从下滚列表中选择多点传送服务的 VLAN ID 和 IP 地址，然后单击“Query”。要手动为特定接口分配多点传送服务，请从下滚列表中选择 VLAN，在文本框中输入多点传送服务的 IP 地址，然后按“Add”。



注：如果显示错误消息，提示您输入的数据无效，则请检查是否正确指定了每个 IP 地址。

CLI — 本示例向端口 NETP0 分配多点传送地址，然后显示 VLAN 1 中支持的所有已知多点传送服务。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet NETP0  4-120
Console(config)#exit
Console#show mac-address-table multicast vlan 1                           4-122
 VLAN M'cast IP addr.Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12        NETP1    IGMP
    1       224.1.2.3        NETP0    USER
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. dot1qVlanIndex	索引	整数
Snooping Multicast Static IP Address	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticIPAddress	索引	IP 地址
Snooping Multicast Static Port List	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticPorts	读 / 创建	八位字节字符串（端口列表）
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	读 / 创建	valid(1), invalid(2)

3.3.3 广播风暴控制 （全局设置）

如果网络中的设备发生故障，或应用程序设计不完善或配置不正确，则可能会发生广播风暴。如果网络中的广播通信过多，则会严重降低性能或导致所有活动完全中止。

可以设置应用于每个端口的广播通信阈值，然后在所需的端口上启用广播风暴控制，以保护网络免受广播风暴损害。

这样，所有超过指定阈值的广播数据包均将被丢弃。

命令用法

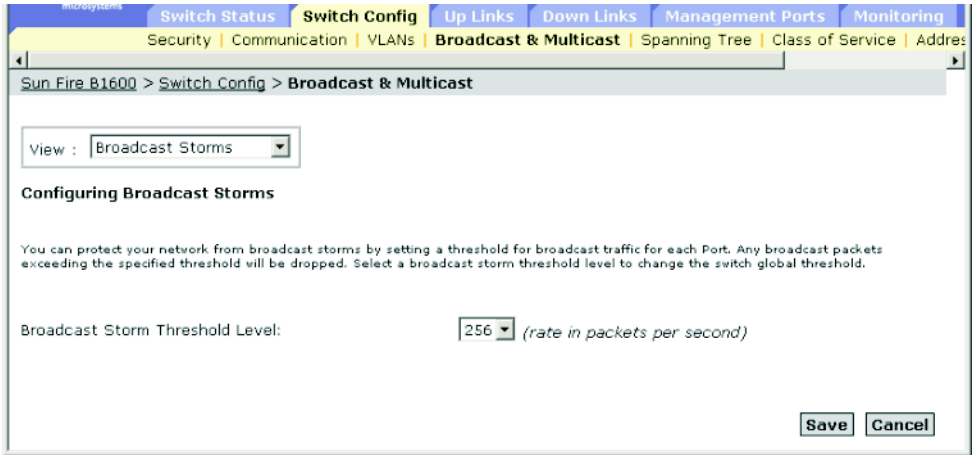
- 默认情况下启用广播风暴控制。
- 广播控制不会影响 IP 多点传送通信。

命令属性

- **Broadcast Storm Threshold Level*** — 每秒数据包量阈值。（范围：16、 64、 128、 256 ； 默认值：256）

* CLI 显示 “Broadcast Storm Limit”。

Web — 打开 “Switch Config” => “Broadcast & Multicast” => “Broadcast Parameters”。设置阈值级别，然后单击 “Save”。



CLI — 本示例显示将广播阈值设置为每秒 64 个数据包。

注：请注意， **switchport broadcast** 命令在指定接口上启用广播风暴控制，并设置交换机上每个接口的广播阈值。

```
Console(config)#interface ethernet NETP7                          4-74
Console(config-if)#switchport broadcast packet-rate 64            4-80
Console(config-if)#end
Console#show interfaces status ethernet NETP7                     4-82
Information of NETP7
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
 Configuration:
  Name: External RJ-45 connector NET7
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  Lacp: Disabled
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Broadcast Storm Packet Rate	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormPktRate	读/写	整数（16、64、128、256）	256
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	读/写	enabled (1)，disabled (2)	enabled

3.3.4 生成树算法配置

生成树算法 (STA) 可用于检测和禁用网络环路，并可用来提供交换机、网桥或路由器之间的备份链接。这样，交换机就可以与网络中的其它桥接设备 （即，与 STA 兼容的交换机、网桥或路由器）交互，以确保网络中任意两个工作站之间只存在一条路线，并提供备份链接 （以便在主链接出现故障时自动接管其功能）。

该交换机支持的生成树算法包括以下版本：

- STP — 生成树协议 (IEEE 802.1D)
- RSTP — 快速生成树协议 (IEEE 802.1w)

RSTP 是原有较慢的 STP 的一般替代协议。 RSTP 可以大大加快重新配置的速度 （即，约为 STP 所需时间的十分之一），因为它减少了活动端口开始了解地址之前的状态更改次数，且预定义了在节点或端口发生故障时使用的备用路线，并为重新配置时对树结构中的变化不敏感的端口保留了转发数据库。

3.3.4.1 配置基本 STA 设置

全局配置适用于整个交换机。

命令用法

- 快速生成树协议

  RSTP 通过监视传入的协议消息并动态调整 RSTP 节点所发送的协议消息类型，支持到 STP 节点或 RSTP 节点的连接。具体情况如下：

  - STP 模式 — 如果交换机在某端口的迁移延迟计时器到期之后收到一个 802.1D BPDU（即， STP BPDU），则交换机认为它所连接的是 802.1D 网桥，并开始只在该端口上使用 802.1D BPDU。
  - RSTP 模式 — 如果 RSTP 正在某端口使用 802.1D BPDU，并在迁移延迟到期后接收到一个 RSTP BPDU， RSTP 会重新启动迁移延迟计时器，并开始在该端口上使用 RSTP BPDU。

命令属性

全局设置的基本配置

可以配置以下全局属性：

- **Enable Spanning Tree** — 在此交换机上启用 / 禁用 STA。
- **Spanning Tree Protocol** — 指定此交换机上使用的生成树类型：
  - **STP**：生成树协议 （IEEE 802.1D ；即，如果选择此选项，交换机将使用设置为 STP 强制兼容模式的 RSTP）
  - **RSTP**：快速生成树 (IEEE 802.1w)

以下全局属性是固定的，不能更改：

- **Bridge ID** — 此设备的优先级和 MAC 地址。
- **Designated Root** — 生成树中此交换机已接受作为根设备的设备的优先级和MAC地址。
  - **Root Port** — 此交换机上离根设备最近的端口的编号。此交换机通过该端口与根设备通信。如果没有根端口，则此交换机已被接受作为生成树网络的根设备。
  - **Root Path Cost** — 此交换机上的根端口到根设备的路径成本。
  - **Root Hello Time** — 此设备传输配置消息的时间间隔 （以秒计）。
  - **Root Maximum Age** — 在试图重新配置之前，此设备在未接收到配置消息的情况下可以等待的最长时间 （以秒计）。所有设备端口 （指定端口除外）都应定期接收到配置消息。如果根端口在 STA 信息 （在最后一个配置消息中提供）之前过期，则将从与网络连接的设备端口中选择一个新的根端口。（在本节中，对 “端口”的引用表示 “接口”，它包括端口和聚合组。）
  - **Root Forward Delay** — 此设备在改变状态 （即，放弃 — 了解 — 转发）之前等待的最长时间 （以秒计）。这种延迟是必需的，因为每台设备在开始转发帧之前，都必须接收有关拓扑结构更改的信息。此外，每个端口也需要时间来侦听将会使其返回到放弃状态的冲突信息；否则，将可能出现暂时的数据环路。
  - **Root Hold Time** — 一个时间间隔（以秒计），在此期间，该节点不会传输 2 个以上的网桥配置协议数据单元。

根设备配置

可以配置以下全局属性：

- **Priority** — 网桥优先级用于选择根设备、根端口和指定端口。具有最高优先级的设备会变为 STA 根设备。不过，如果所有设备的优先级相同，那么具有最低 MAC 地址的设备将变为根设备。
  - 默认值：32768
  - 范围：0-61440，步进值为 4096
  - 选项：0；4096；8192；12288；16384；20480；24576；28672；32768；36864；40960； 45056； 49152； 53248； 57344； 61440
- **Hello Time** — 此设备传输配置消息的时间间隔 （以秒计）。
  - 默认值：2
  - 最小值：1
  - 最大值：10 或 [(Max. Message Age / 2) -1]；取其中较低者

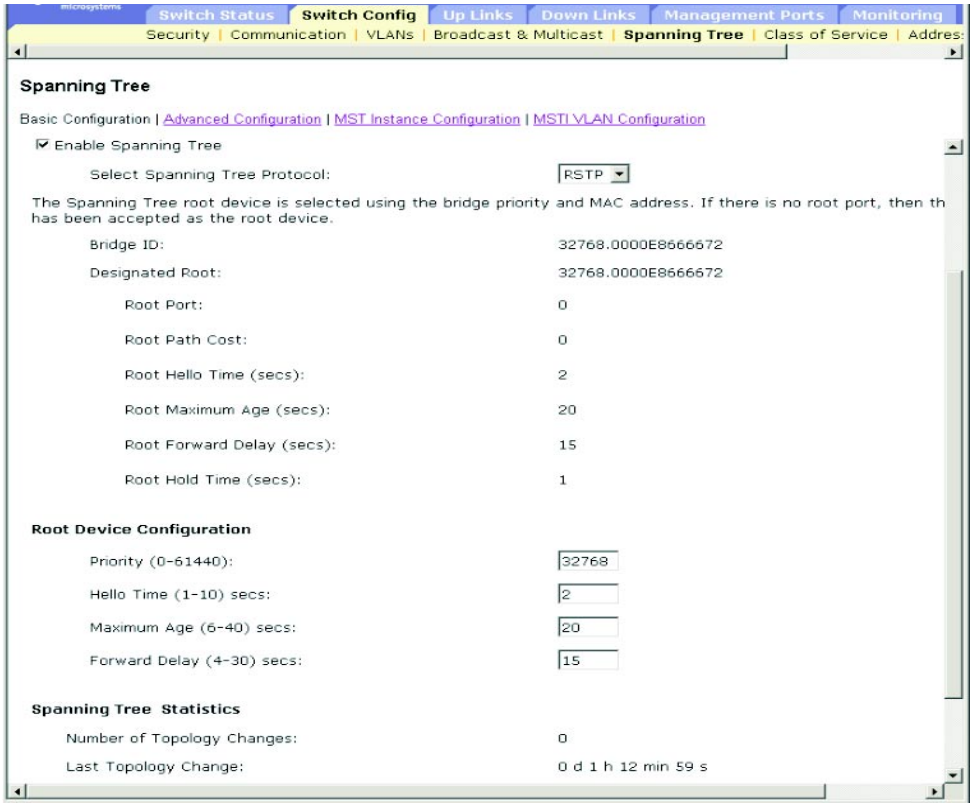
- **Maximum Age** — 在试图重新配置之前，此设备在未接收到配置消息的情况下可以等待的最长时间 （以秒计）。所有设备端口 （指定端口除外）都应定期接收到配置消息。任何在 STA 信息 （在所接收的最后一个配置消息中提供）之前过期的端口都会变为其所连接的 LAN 的指定端口。如果该端口是根端口，将会从当前连接到网络的各个设备端口中间选定一个新的根端口。（在本节中，对 “端口”的引用表示 “接口”，它包括端口和聚合组。）
  - 默认值：20
  - 最小值：6 或 [2 x (Hello Time + 1)] ；取其中较高者。
  - 最大值：40 或 [2 x (Forward Delay - 1)] ；取其中较低者
- **Forward Delay** — 此设备在改变状态（即，放弃 - 了解 - 转发）之前将等待的最长时间 （以秒计）。这种延迟是必需的，因为每台设备在开始转发帧之前，都必须接收有关拓扑结构更改的信息。此外，每个端口也需要时间来侦听将会使其返回到放弃状态的冲突信息；否则，将可能出现暂时的数据环路。
  - 默认值：15
  - 最小值：4 或 [(Max. Message Age / 2) +1] ；取其中较高者
  - 最大值：30

生成树统计信息

以下全局属性显示统计信息值，不能更改：

- **Number of Topology Changes** — 重新配置生成树的次数。
- **Last Topology Change** — 上次重新配置生成树的时间。

Web — 打开“Switch Config”=>“Spanning Tree”=>“Basic Configuration”。修改所需的属性，然后单击“Save”。



注：如果收到错误消息，说明您输入的数据无效，请检查您为“Priority”、“Hello Time”、“Maximum Age”以及“Forward Delay”指定的值是否在这些参数的指定范围内。

CLI — 此命令显示全局 STA 设置，其后是每个端口的设置。

```
Console#show spanning-tree                                          4-102
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode               :RSTP
 Spanning tree enable/disable     :enable
 Priority                         :32768
 Bridge Hello Time (sec.)         :2
 Bridge Max Age (sec.)            :20
 Bridge Forward Delay (sec.)      :15
 Root Hello Time (sec.)           :2
 Root Max Age (sec.)              :20
 Root Forward Delay (sec.)        :15
 Designated Root                  :32768.0000E8666672
 Current root port                :0
 Current root cost                :0
 Number of topology changes       :0
 Last topology changes time (sec.):9142
 Transmission limit               :3
 Path Cost Method                 :4308020
.
.
.
```

注：如果此设备未与网络相连，则当前根端口和当前根成本均显示为 0。

以下示例将生成树模式设置为 RSTP，启用生成树，然后设置指定的属性。

```
Console(config)#spanning-tree mode rst                              4-93
Console(config)#spanning-tree                                       4-92
Console(config)#spanning-tree priority 40000                        4-96
Console(config)#spanning-tree hello-time 5                          4-95
Console(config)#spanning-tree max-age 40                            4-95
Console(config)#spanning-tree forward-time 20                       4-94
Console(config)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
STA System Status	sun...staMgt. staSystemStatus	读/写	enabled (1), disabled (2)	enabled
STA Protocol Type	sun...staMgt. staProtocolType	读/写	stp (1), rstp (2),	rstp
Bridge ID	由网桥优先级与 MAC 地址组成。			
Designated Root	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-DesignatedRoot	只读	八位字节字符串	
Root Port	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootPort	只读	整数	
Root Cost	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootCost	只读	整数	
Hello Time	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-HelloTime	只读	整数	200 厘秒
Maximum Age	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgMaxAge	只读	整数	2000 厘秒
Forward Delay	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-ForwardDelay	只读	整数	1500 厘秒
Priority	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgPriority	读/写	整数 (0-61440)	32768
Bridge Hello Time	MIB-II. dot1dStp. dot1dStp-BridgeHelloTime	读/写	整数 (100-1000) 厘秒	200 厘秒

字段名	MIB 变量	访问权限	值范围	默认值
Bridge Maximum Age	MIB-II. dot1dStp. dot1dStpBridgeMaxAge	读 / 写	整数 (600-4000) 厘秒	2000 厘秒
Bridge Forward Delay	MIB-II. dot1dStp. dot1dStp-BridgeForwardDelay	读 / 写	整数 (400-3000) 厘秒	1500 厘秒
STA Configuration Changes	MIB-II. dot1dBridge.dot1dStp. dot1dStpTopChanges	只读	计数	
STA Last Topology Change	MIB-II. dot1dBridge.dot1dStp. dot1dStpTimeSince-TopologyChange	只读	整数	

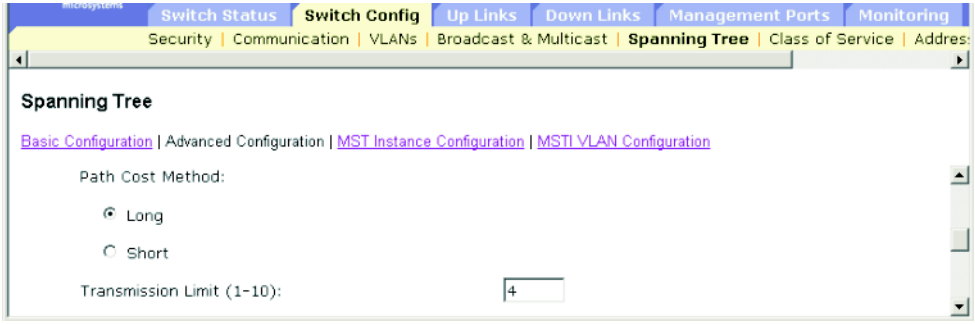
3.3.4.2 配置高级 STA 设置

本节介绍 RSTP 的高级设置。

命令属性

- **Path Cost Method** — 路径成本用来确定设备之间的最佳路径。路径成本方法用来确定可以分配给每个接口的值范围。
  - Long：指定基于 32 位的值，范围：1-200,000,000。
  - Short：指定基于 16 位的值，范围：1-65535。
- **Transmission Limit** — BPDU 的最大传输速率是通过设置传输两个连续的协议消息之间的最小时间间隔来指定的。（范围：1-10；默认值：3）

Web — 打开“Switch Config”=>“Spanning Tree”=>“Advanced Configuration”。修改所需的属性，然后单击“Save”。



注：如果收到错误消息，说明您输入的数据无效，请检查您指定的传输限制是否在指定范围内。

CLI — 本示例设置生成树路径成本方法和传输限制。

```
Console(config)#spanning-tree pathcost method long              4-97
Console(config)#spanning-tree transmission-limit 4              4-97
Console(config)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
RSTP Path Cost Method	sun... staMgt. staPathCostMethod	读/写	short (1), long (2)	long
RSTP Transmission Hold Count	sun.. staMgt. staTxHoldCount	读/写	整数 (1-10)	3

3.3.5 服务类别配置

通过服务类别 (CoS) 功能，可以指定当通信由于拥塞而进入交换机的缓冲区时，哪些数据包的优先级更高。此交换机为每个端口提供具有四种优先级队列的 CoS。端口的高优先级队列中的数据包将先于低优先级队列中的数据包发送。可以设置每个接口的默认优先级，并可配置帧优先级标记与交换机的优先级队列之间的映射关系。

3.3.5.1 设置接口的默认优先级

可以为交换机上的每个接口指定默认的端口优先级。所有未标记的数据包进入交换机时，均将使用指定的默认端口优先级进行标记，然后在输出端口进行排序，以进入相应的优先级队列。

命令用法

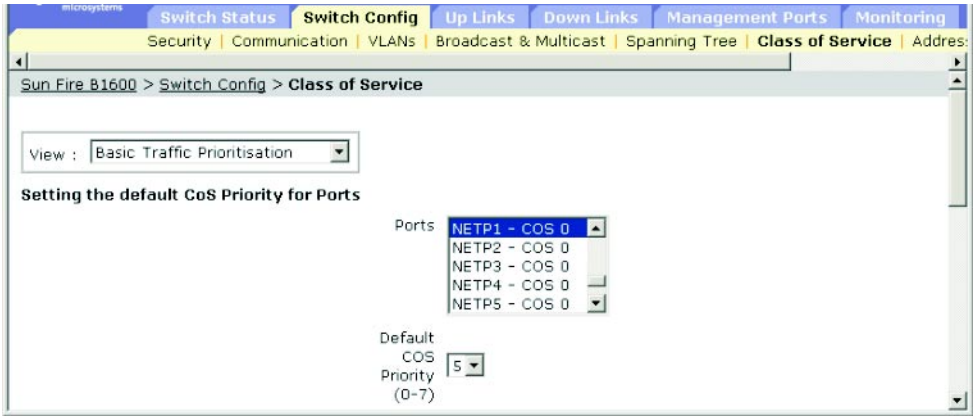
- 此交换机为每个端口提供四种优先级队列。它使用加权轮询来避免队列头部发生阻塞。
- 默认优先级适用于经设置应接收所有帧类型 （即接收带标记帧和未标记帧）的端口所接收的未标记帧。这种优先级不适用于 IEEE 802.1Q VLAN 带标记帧。如果传入帧是 IEEE 802.1Q VLAN 带标记帧，将使用 IEEE 802.1p 用户优先级位。
- 如果输出端口是相关 VLAN 的未标记成员，那么这些帧在发送之前将被去掉所有 VLAN 标记。

命令属性

- **Ports** — 接口（端口或聚合组）和分配的默认服务类别优先级。
- **Default COS Priority*** — 分配给在指定接口上所接收的未标记帧的优先级。（范围：0-7；默认值：0）

* CLI 将此信息显示为 “Priority for untagged traffic”。

Web — 打开 “Switch Config” => “Class of Service” => “Basic Traffic Prioritisation”。滚动到 “Setting the Default CoS Priority for Ports”。从 “Ports” 列表中选择一个接口，修改默认优先级，然后单击 “Save”。



CLI — 本示例为端口 NETP1 分配默认优先级 5。

```
Console(config)#interface ethernet NETP1                    4-74
Console(config-if)#switchport priority default 5            4-130
Console#show interfaces switchport ethernet NETP1           4-85
Information of NETP1
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 5
 Gvrp status: Enabled
 Allowed Vlan: 1(u),
 Forbidden Vlan:
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Port Default User Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dPortPriorityTable. dot1dPortPriorityEntry. dot1dPortDefault-UserPriority	读 / 写	整数 (0-7)	0

3.3.5.2 将 CoS 值映射到传出队列

此交换机使用每个端口的四个优先级队列及基于加权轮询的服务调度，以处理标记了服务类别 (CoS) 优先级的通信 （第 3-65 页）。IEEE 802.1p 中定义了多达 8 个单独的通信优先级。应按照 IEEE 802.1p 标准中的建议分配默认优先级，如下表所示。

	队列			
	0	**1**	**2**	**3**
优先级		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

下表中显示了 IEEE 802.1p 标准针对不同的网络应用程序建议使用的优先级。但是，可以通过任何对您自己的网络中的应用程序通信有利的方式，将优先级级别映射到交换机的输出队列。

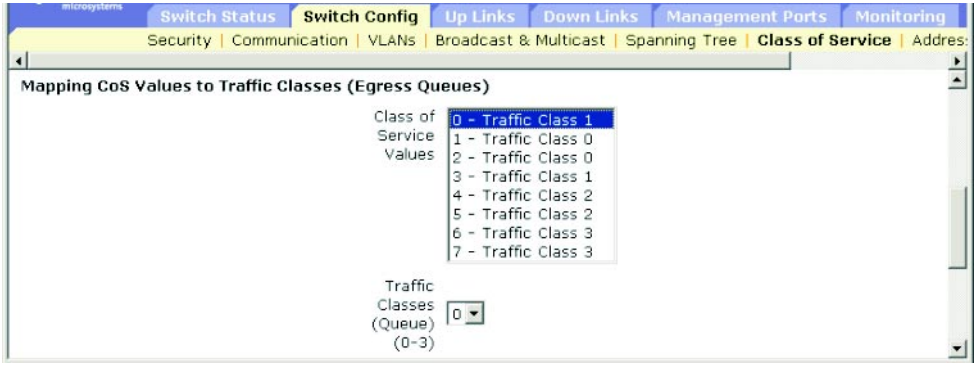
优先级	通信类型
1	后台
2	（备用）
0 （默认值）	尽力而为
3	卓有成效的努力
4	受控负载
5	视频，滞后和抖动时间低于 100 毫秒
6	语音，滞后和抖动时间低于 10 毫秒
7	网络控制

命令属性

- **Class of Service Values** — CoS 值。（范围：0-7； 7 是最高优先级）
- **Traffic Classes (Queue)*** — 输出队列缓冲区。（范围：0-3）

* CLI 显示队列 ID。

Web — 打开 “Switch Config” => “Class of Service” => “Basic Traffic Prioritisation”。滚动到 “Mapping CoS Values to Traffic Classes (Egress Queues)”。从 “Class of Service Values” 列表中选择优先级，从 “Traffic Classes” 下滚列表中选择输出队列，然后单击 “Save”。



CLI — 以下示例说明了如何将 CoS 值 0、1 和 2 映射到 CoS 优先级队列 0、将值 3 映射到 CoS 优先级队列 1、将值 4 和 5 映射到 CoS 优先级队列 2、将值 6 和 7 映射到 CoS 优先级队列 3。

```
Console(config)#interface ethernet NETP0                          4-74
Console(config)#queue cos-map 0 0 1 2                             4-132
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet NETP0                         4-134
Information of NETP0
 Queue ID  Class of service
 --------  ----------------
    0      0 1 2
    1      3
    2      4 5
    3      6 7
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Traffic Class Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClassPriority	不可访问	整数 (0-7)	
Traffic Class	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClass	读 / 写	整数 (0-7)	第 3-62 页

3.3.5.3 设置通信类别的服务权级

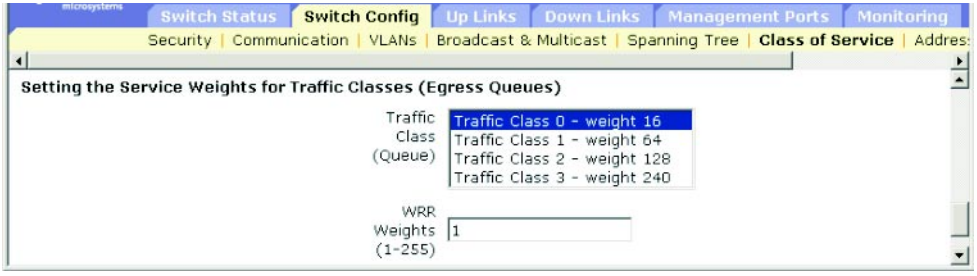
此交换机使用加权轮询 (WRR) 算法来确定其处理每个优先级队列的频率。如第 3-62 页上的 “将 CoS 值映射到传出队列”中所述，通信类别映射到为每个端口提供的 4 个传出队列之一。可以为其中的每一个队列分配权级 （进而为相应的通信优先级分配权级）。此权级设置轮询每个队列 （以提供服务）的频率，且随后会影响已分配特定优先级值的软件应用程序的响应时间。

命令属性

- **Traffic Class (Queue)*** — 显示每个通信类别的权级列表。
- **WRR Weights** — 为选定的通信类别设置新权级。（范围：1-255）

* CLI 显示队列 ID。

Web — 打开 “Switch Config” => “Class of Service” => “Basic Traffic Prioritisation”。滚动到 “Setting the Service Weights for Traffic Classes (Egress Queues)”。选择一种通信类别 （如，输出队列），输入一个权级，然后单击 “Save”。



CLI — 本示例说明如何将 WRR 权级 1、 4、 16 和 64 分配给 CoS 优先级队列 0、 1、 2 和 3。

```
Console(config)#queue bandwidth 1 4 16 64                    4-131
Console(config)#exit
Console#show queue bandwidth                                 4-133
 Queue ID Weight
 -------- ------
        0      1
        1      4
        2     16
        3     64
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
WRR Traffic Class (Queue ID)	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrTrafficClass	索引	整数 (0-7)	
WRR Weight	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrWeight	读 / 写	整数 (1-255)	对于队列 0：16 对于队列 1：64 对于队列 2：128 对于队列 3：240

3.3.5.4 将第 3/4 层优先级映射到 CoS 值

此交换机支持多种通用的确定第 3/4 层通信优先级的方法，可以满足应用程序的需求。可以使用服务类型 (ToS) 八位字节中的优先级位，在帧的 IP 标头中指定通信优先级。如果使用了优先级位，则在 ToS 字节中，可以将三位用于 IP 优先级，或将六位用于“差别化业务编码点 (DSCP)”服务。如果启用了这些服务，则交换机会将优先级映射为一个 “服务类别”值，然后将通信发送到相应的输出队列。

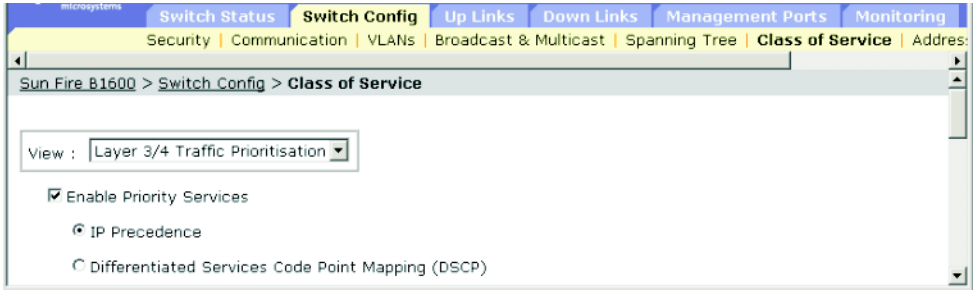
由于通信中可能包含不同的优先级信息，因此，此交换机采用以下方式将优先级值映射到输出队列：

- 优先级映射所采用的优先顺序是IP优先权或DSCP优先级，然后是默认端口优先级。
- 不能同时启用 IP 优先权和 DSCP 优先级。启用其中一种优先级类型会自动禁用另一种。

命令属性

- **Enable Priority Services** — 可以启用或禁用将第3/4层优先级映射到CoS值。（默认值：Disabled）
- **IP Precedence** — 使用 IP 优先权映射第 3/4 层优先级。
- **Differentiated Services Code Point Mapping (DSCP)** — 使用 DSCP 映射第 3/4 层优先级。

Web — 打开 “Switch Config” => “Class of Service” => “Layer 3/4 Traffic Prioritisation”。选中 “Enable Priority Services”，选择 “IP Precedence” 或 “DSCP”，然后单击 “Save”。



CLI — 本示例在交换机上启用 IP 优先权服务。

```
Console(config)#map ip precedence                    4-135
Console(config)#
```

要完全禁用第 3/4 层通信优先级划分，请使用下面的命令。

```
Console(config)#no map ip precedence                 4-135
Console(config)#no map ip dscp                       4-136
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
IP Precedence/ DSCP Status	sun... priorityMgt. prioIpPrecDscpStatus	读/写	disabled (1), precedence (2), dscp (3)	disabled

3.3.5.5 映射 IP 优先权

IPv4 标头中的服务类型 (ToS) 八位字节中包含三个优先权位，用于定义 8 种不同的优先级 （从用于网络控制数据包的最高优先级到用于常规通信的最低优先级）。默认的 IP 优先权值以一对一方式映射到服务类别值 （即，优先权值 0 映射到 CoS 值 0，以此类推）。位 6 和位 7 用于网络控制，其它各位对应于不同的应用类型。下表中定义了 ToS 位。

优先级	通信类型
7	网络控制
6	互连网络控制
5	严重
4	闪存覆盖
3	闪存
2	立即
1	优先级
0	常规

命令属性

- **IP Precedence** — 显示 IP 优先权到 CoS 的映射。
- **Class of Service Value** — 将 CoS 值映射到选定的 IP 优先权值。请注意，“0”表示低优先级，“7”表示高优先级。

Web — 打开 “Switch Config” => “Class of Service” => “Layer 3/4 Traffic Prioritisation”。滚动到 “Mapping IP Precedence to Class of Service Values”。从 “IP Precedence” 表中选择一个条目，在 “Class of Service Value” 字段中输入一个值，然后单击 “Save”。

CLI — 本示例将端口 SNP5* 上的 IP 优先权值 1 映射到 CoS 值 0，然后显示该端口的所有 IP 优先权设置。

```
Console(config)#interface ethernet SNP5                          4-74
Console(config-if)#map ip precedence 1 cos 0                     4-135
Console(config-if)#end
Console#show map ip precedence ethernet SNP5                     4-138
Precedence mapping status: disabled

 Port       Precedence COS
 ---------  ---------- ---
      SNP5           0   0
      SNP5           1   0
      SNP5           2   2
      SNP5           3   3
      SNP5           4   4
      SNP5           5   5
      SNP5           6   6
      SNP5           7   7
Console#
```

* 为 IP 优先权映射特定值是作为接口配置命令实现的，但所有更改都将应用于交换机上的所有接口。

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
IP Precedence Value	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecValue	不可访问	整数 (0-7)	
IP Precedence CoS	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecCos	读 / 写	整数 (0-7)	一对一映射

3.3.5.6 映射 DSCP 优先级

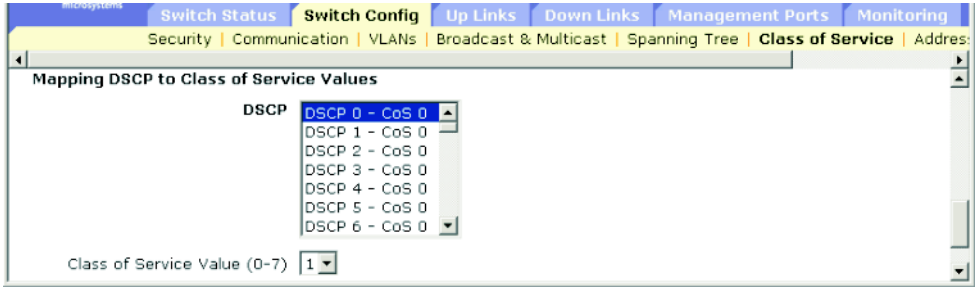
DSCP 长度为六位，最多允许编码 64 种不同的转发行为。 DSCP 取代 ToS 位，但它向后兼容三个优先权位，这样，非 DSCP 兼容和启用 ToS 的设备将不会与 DSCP 映射产生冲突。根据网络策略，可以为不同转发类型选择不同的通信类型。下表定义了 DSCP 默认值。请注意，下表中所有未指定的 DSCP 值均被映射到 CoS 值 0。

IP DSCP 值	CoS 值
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

命令属性

- **DSCP** — 显示 DSCP 优先级到 CoS 的映射。
- **Class of Service Value** — 将 CoS 值映射到选定的 DSCP 优先级值。请注意，“0”表示低优先级，“7”表示高优先级。

Web — 打开 “Switch Config” => “Class of Service” => “Layer 3/4 Traffic Prioritisation”。滚动到 “Mapping DSCP to Class of Service Values”。从 “DSCP” 表中选择一个条目，在 “Class of Service Value” 字段中输入一个值，然后单击 “Save”。



CLI — 本示例将端口 SNP5* 上的 DSCP 值 0 映射到 CoS 值 1，然后显示该端口的所有 DSCP 优先级设置。

```
Console(config)#interface ethernet SNP5                          4-74
Console(config-if)#map ip dscp 0 cos 1                           4-137
Console(config-if)#end
Console#show map ip dscp ethernet SNP5                           4-139
DSCP mapping status: disabled

 Port         DSCP COS
 ------------ ---- ---
        SNP1    0   1
        SNP1    1   0
        SNP1    2   0
        SNP1    3   0
.
.
.
        SNP1   61   0
        SNP1   62   0
        SNP1   63   0
Console#
```

* 为 IP DSCP 映射特定值是作为接口配置命令实施的，但所有更改将应用到交换机上的所有接口。

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
IP DSCP Value	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpValue	不可访问	整数 (0-63)	
IP DSCP CoS	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpCos	读 / 写	整数 (0-7)	第 3-70 页

3.3.6 地址表设置

交换机存储所有已知设备的地址。这些信息将用来在入站端口和出站端口之间直接路由通信。通过监视通信所了解到的所有地址均存储在动态地址表中。也可以手动配置绑定到特定端口的静态地址。

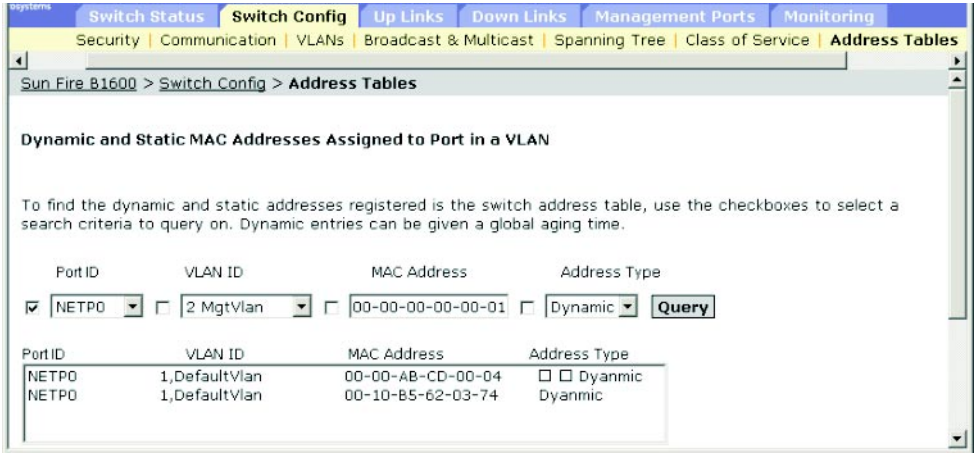
3.3.6.1 显示地址表

地址表包含 MAC 地址，它们是通过监视进入交换机的通信的源地址而动态了解到的。如果在数据库中找到了入站通信的目标地址，则以该地址为目标地址的数据包将直接转发到相关的端口。否则，通信将扩散到所有端口。地址表还包含绑定到特定端口上的静态 MAC 地址。（请参阅第 3-95 页上的 “配置静态地址”。）

命令属性

- **Port ID** （接口 *）— 端口或聚合组 （上行链接端口：NETP0-7 ； 下行链接端口：SNP0-15 ； 不能显示 NETMGT 的 MAC 地址表）。
- **VLAN ID** — VLAN 标识符 (1-4094)。
  （此字段包括 VLAN ID 和名称。）
- **MAC Address** — 与此接口关联的 MAC 地址。
- **Address Type** — 显示是动态了解地址还是静态配置地址。

Web — 打开 “Switch Config” => “Address Tables”。指定接口、 VLAN、 MAC 地址或地址类型 （即任意组合）作为搜索标准，然后单击 “Query”。



CLI — 本示例显示端口 NETP1 的地址表条目。

```
Console#show mac-address-table interface ethernet NETP1        4-88
 Interface   Mac Address       Vlan Type
 ----------- ----------------- ---- -----------------
       NETP0 00-20-9c-23-cd-61 1    Dynamic
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围
Interface	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbPort	只读	not learned (0)， 端口列表 (1-24)
MAC Address	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbAddress	只读	MAC 地址
VLAN	MIB-II. dot1dBridge.qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	不可访问	整数
Type	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbStatus	只读	其它 (1)， invalid (2)， learned (3)， self (4)， mgmt (5)

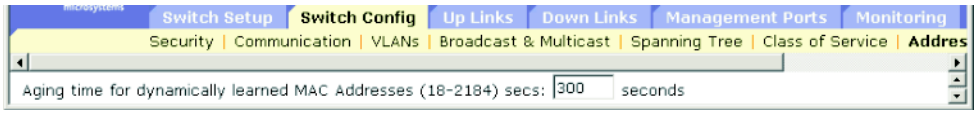
3.3.6.2 更改有效期

可以为动态地址表中的条目设置有效期。

命令属性

- **Aging Time** — 一段时间，在该时间之后丢弃已了解到的条目。（范围：18-2184 秒；默认值：300 秒）

Web — 单击“Switch Config”=>“Address Tables”。指定新的有效期，然后单击“Save”。



CLI — 本示例将有效期设置为 400 秒。

```
Console(config)#mac-address-table aging-time 400                    4-89
Console(config)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Aging Time	MIB-II dot1dBridge.dot1dTp. dot1dTpAgingTime	读 / 写	整数 (18-2184) 秒	300 秒

3.4 端口配置

本节包含下行链接端口、上行链接端口和管理端口的配置菜单。这些菜单中的大多数适用于所有端口类型。但是，管理端口仅支持几个基本菜单，且“Packet Filtering”（第 3-106 页）是专为管理端口提供的。

注：在以下菜单中使用的端口指定包括为上行链接端口指定的 NETP0-7、为下行链接端口指定的 SNP0-15，以及为管理端口指定的 NETMGT。

3.4.1 显示连接状态

可以使用端口状态页来显示当前连接状态，包括链接状态、速度 / 双工模式、流量控制、自动协商和广播风暴控制。

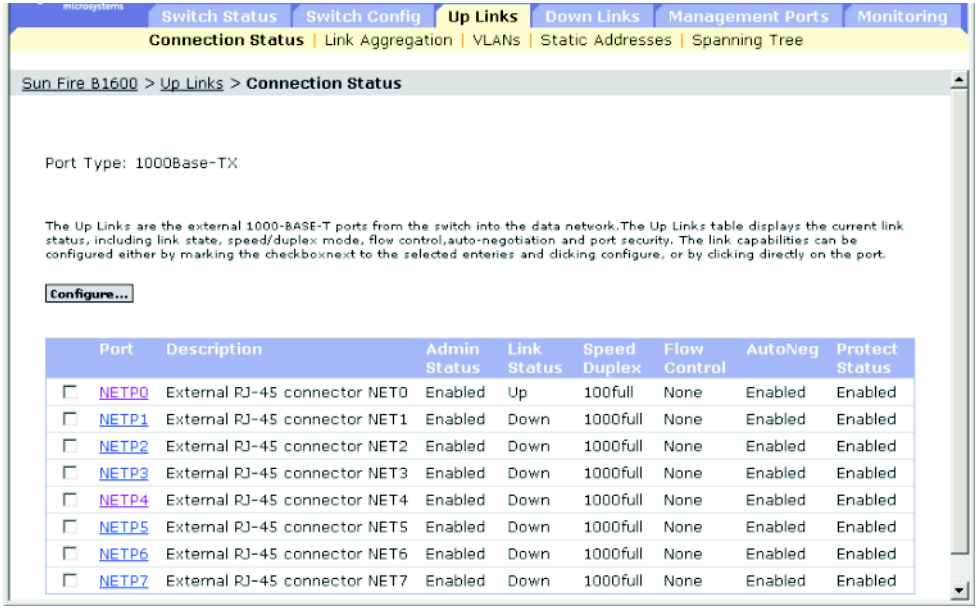
命令属性

- **Port Type** — 指示端口类型 （1000Base-SX、 1000Base-T 或 10/100Base-TX）。
- **Port** — 端口或聚合组 （上行链接端口：NETP0-7 ； 下行链接端口：SNP0-15 ； 管理端口：NETMGT）。
- **Description** — 接口标签。
- **Admin Status** — 显示接口处于启用还是禁用状态。
  Web — 显示 “Enabled”或 “Disabled”。
  CLI — 显示 “Port Admin”（建立或断开）。
- **Link Status** — 指明链接是建立还是断开。
- **Port Operation Status** — 提供有关端口状态的详细信息。
  仅限 CLI ； 仅当链接建立时才显示此项。
- **Speed/Duplex** — 显示当前的速度和双工模式。
- **Flow Control** — 显示流量控制为启用还是禁用。
  Web — IEEE 802.3x、反压或无。
  CLI — 启用或禁用。“Flow Type”显示 IEEE 802.3x、反压或无。
- **Auto-negotiation** — 显示自动协商为启用还是禁用。
- **Protect Status** — 显示是否在此接口上启用了广播风暴控制。要设置此阈值，请参阅第 3-51 页上的 “广播风暴控制 （全局设置）”。

- **MAC Address** — 此端口的物理层地址。
  仅限 CLI；要通过 Web 访问此项，请参阅第 3-10 页上的 “设置 IP 地址”。
- **Port Capabilities*** — 指定要在自动协商过程中公布的端口功能。支持以下功能。
  - **10half** — 支持 10 Mbps 半双工操作
  - **10full** — 支持 10 Mbps 全双工操作
  - **100half** — 支持 100 Mbps 半双工操作
  - **100full** — 支持 100 Mbps 全双工操作
  - **1000full** — 支持 1000 Mbps 全双工操作
  - **Sym** — 为流量控制发送并接收暂停帧
  - **FC** — 支持流量控制
- **LACP Status** — 显示是否在此端口上启用了链路聚合控制协议 (LACP)。（仅限 CLI）

* 要在 Web 上访问此项，请参阅第 3-79 页上的 “配置接口连接”。

Web — 单击 “Up Links” / “Down Links” / “Management Port” => “Status”。要配置一个或多个接口的连接，请单击所选条目旁边的复选框，然后单击 “Configure”。（请参阅第 3-79 页上的 “配置接口连接”。）



CLI — 本示例显示了端口 NETP7 的连接状态。

```
Console#show interfaces status ethernet NETP7                    4-82
Information of NETP7
 Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
 Configuration:
  Name: External RJ-45 connector NET7
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  Lacp: Disabled
 Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Port Type	sun... portMgt. portTable. portEntry. portType	只读	其它 (1), hundredBaseTX(2), hundredBaseFX(3), thousandBaseSX(4), thousandBaseLX(5), thousandBaseT(6), thousandBaseMiniGBIC(7) thousandBaseSFP(8)	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	只读	物理地址	
Port	sun... portMgt. portTable. portEntry	索引	整数 (1-25)	
Port Name	sun... portMgt. portTable. portEntry. portName	读/写	显示字符串 （大小 (0-64)）	

字段名	MIB 变量	访问权限	值范围	默认值
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	读/写	up (1), down (2), testing (3)	up
Link Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	只读	up (1), down (2-7),	
Operational Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	只读	up (1), down (2), testing (3), unknown (4), dormant (5), notPresent (6), lowerLayerDown (7)	
Port Speed Duplex Status	sun... portMgt. portTable.portEntry. portSpeedDpxStatus	只读	error(1), halfDuplex10(2), fullDuplex10(3), halfDuplex100(4), fullDuplex100(5), halfDuplex1000(6), fullDuplex1000(7)	
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	读/写	Bits{ portCap10half (0), portCap10full (1), portCap100half (2), portCap100full (3), portCap1000half (4), portCap1000full (5), reserved6-13 (6-13), portCapSym (14), portCapFlowCtrl (15)}	
Port Flow Control Status	sun... portMgt. portTable.portEntry. portFlowCtrlStatus	只读	error(1), backPressure(2), dot3xFlowControl(3), none(4)	none
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	读/写	enabled (1), disabled (2)	disabled

字段名	MIB 变量	访问权限	值范围	默认值
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	读 / 写	enabled (1), disabled (2)	enabled
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	读 / 写	enabled (1), disabled (2)	enabled

3.4.2 配置接口连接

可以使用 “Port Setup”页来启用 / 禁用接口、设置自动协商以及要公布的接口功能，也可以手动调整速度、双工模式和流量控制。

命令属性

- **Port/s** — 端口或聚合组 （上行链接：NETP0-7 ； 下行链接：SNP0-15）。
- **Port Description** — 允许为端口标上标签。（范围：1-64 个字符；
  默认值 — 上行链接：外部 RJ-45 连接器 NETn ； 下行链接：刀片插槽 n ； 管理端口：外部 RJ-45 连接器 NETMGT）
- **Administrative Status** — 允许手动禁用接口。可以禁用出现异常情况 （如冲突过多）的接口，并在问题解决后重新启用此接口。也可以出于安全性考虑禁用接口。
- **Negotiate Link Capabilities**[1] — 允许启用 / 禁用自动协商。启用自动协商后，需要指定要公布的功能。禁用自动协商后，可以强行设定速度、模式和流量控制的设置。支持以下功能。
  - **10half** — 支持 10 Mbps 半双工操作
  - **10full** — 支持 10 Mbps 全双工操作
  - **100half** — 支持 100 Mbps 半双工操作
  - **100full** — 支持 100 Mbps 全双工操作
  - **1000half** — 支持 1000 Mbps 半双工操作
  - **1000full** — 支持 1000 Mbps 全双工操作
  - **symmetric** （仅限千兆位）— 选中此项可以发送和接收暂停帧，清除此选项将自动协商非对称暂停帧的发送方和接收方。（交换机仅支持非对称暂停帧。）
  - **flowcontrol** — 支持流量控制
    当交换机缓冲区已满时，流量控制功能可以 “阻止”从终端站或直接连接到交换机的网段所发出的通信，从而避免帧丢失。启用此功能后，半双工操作将采用反压，全双工操作将采用 IEEE 802.3x。

注：Sun Fire B1600 刀片式系统机箱上的集成交换机中都包含两块链接在一起的交换机芯片。若要镜像某个端口上的通信，只能使用该端口所在交换机芯片上的其它端口才有可能实现。端口 NETP0、NETP1、NETP4、NETP5 以及 SNP8 到 SNP15 在同一交换机芯片上。端口 NETP、NETP3、NETP6、NETP7 以及 SNP0 到 SNP7 位于另一交换机芯片上。（如果您查看 SSC 的后面板，则将看到右侧的所有端口位于一块芯片上，而左侧的所有端口位于另一块芯片上。）

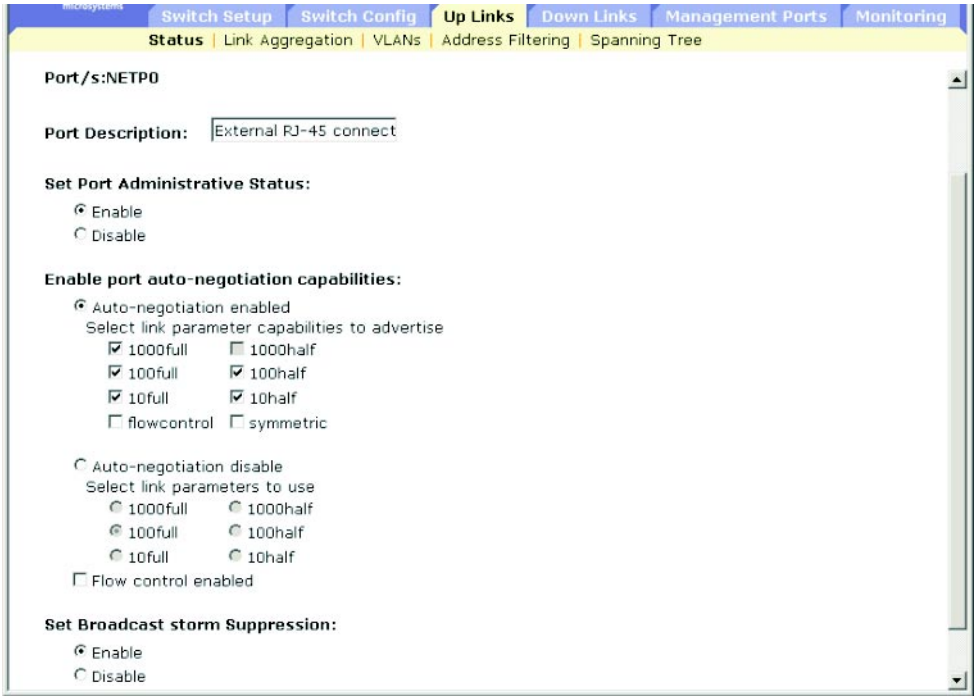
- **Speed/Duplex**[2] — 禁用自动协商后，可以手动配置端口速度和双工模式。

注：在禁用自动协商功能的情况下，只能将上行链接端口的速度设置为 10 Mbps 或 100 Mbps。要强制端口以 1 Gbps 全双工模式操作，则应启用自动协商功能，并且将该端口容量仅设置为 “1000full”。

- **Flow Control**[2] — 禁用自动协商后，需要启用或禁用流量控制。（请勿在连接到集线器的端口上使用流量控制，除非确实需要使用流量控制才能解决问题。否则，反压干扰信号可能削弱连接到集线器的网段的总体性能。）
- **Broadcast storm suppression** — 为选定端口启用广播风暴抑制。有关广播风暴控制的详细信息或设置广播阈值级别的信息，请参阅第 3-51 页上的 “广播风暴控制 （全局设置）”。

1. 不能在下行链接端口上禁用自动协商。这些端口固定采用 1000 Mbps 的速度和全双工模式。
2. 在可以配置或强制接口使用特定速度、双工模式或流量控制选项之前，必须在上行链接端口上禁用自动协商。

Web — 打开 “Up Links” / “Down Links” => “Status” 屏幕。选中要配置的接口的复选框，然后单击 “Configure”。根据需要修改接口设置，然后单击 “Save”。



CLI — 选择接口，然后输入所需的设置。

```
Console#Console(config)#interface ethernet NETP1                4-74
Console(config-if)#description RD SW#17                         4-74
Console(config-if)#shutdown                                     4-80
.
.
.
Console(config-if)#no shutdown
Console(config-if)#negotiation
Console(config-if)#capabilities 1000full                        4-77
Console(config-if)#capabilities 1000full                        4-77
Console(config-if)#capabilities flowcontrol
.
.
.
Console(config-if)#no negotiation                               4-76
Console(config-if)#speed-duplex 100half                         4-75
Console(config-if)#flowcontrol                                  4-78
Console(config-if)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Port Name	sun... portMgt. portTable.portEntry. portName	读 / 写	显示字符串 （大小 (0-64)）	第 3-79 页
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	读 / 写	up (1)， down (2)， testing (3)	up
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	读 / 写	enabled(1)， disabled(2)	enabled
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	读 / 写	Bits{ portCap10half (0), portCap10full (1), portCap100half (2), portCap100full (3), portCap1000half (4), portCap1000full (5), reserved6-13 (6-13), portCapSym (14), portCapFlowCtrl (15)}	
Port Speed Duplex Configuration	sun... portMgt. portTable.portEntry. portSpeedDpxCfg	读 / 写	reserved(1)， halfDuplex10(2)， fullDuplex10(3)， halfDuplex100(4)， fullDuplex100(5)， halfDuplex1000(6)， fullDuplex1000(7)	
Port Flow Control Configuration	sun... portMgt. portTable.portEntry. portFlowCtrlCfg	读 / 写	enabled(1)， disabled(2)， backPressure(3)， dot3xFlowControl(4)	

3.4.3 端口聚合组配置

可以在设备之间创建多个链接，然后将它们组合为一个虚拟的聚合链接。端口聚合组大大增加了其中存在瓶颈的网段的带宽，并为两台设备之间提供了容错链接。一次最多可以创建 6 个聚合组。

交换机同时支持静态聚合和动态链路聚合控制协议 (LACP)。通过 LACP 配置的端口将自动与另一台设备上通过 LACP 配置的端口协商一个聚合链接。可以将交换机上任意数量的上行链接端口配置为支持 LACP，只要这些端口未配置为静态聚合组的一部分。如果另一台设备上的端口也配置为支持 LACP，则交换机和此设备彼此将协商一个聚合链接。如果某个 LACP 聚合组包含的端口超过 4 个，则所有其它端口将处于备用模式。如果聚合组中的某个链接发生故障，则将自动激活某个备用端口来替换它。

命令用法

除了在聚合组中的每个端口之间平衡负载之外，附加端口还在聚合组中的某个端口出现故障时接管负载，从而提供冗余功能。但是，在设备之间建立任何物理连接之前，请使用 Web 界面或 CLI 来指定位于两端的设备的聚合组。使用端口聚合组时，请注意以下各事项：

- 在交换机之间连接相应的网线之前，请先完成对端口聚合组的配置，以免形成环路。
- 在交换机上最多可以创建 6 个聚合组，每个聚合组最多包括 4 个端口。
- 必须对各连接两端的端口进行配置，使之变为聚合组端口。
- 聚合组两端的端口必须采用相同的方式进行配置，包括通信模式 （即，速度、双工模式和流量控制）、 VLAN 分配和 CoS 设置。
- 如果目标交换机也已在连接端口上启用 LACP，则将自动激活聚合组。
- 对于与另一使用 LACP 的交换机组成的聚合组，将自动为其分配下一个可用的聚合组 ID。
- 如果连接到同一目标交换机的端口中有四个以上的端口启用了 LACP，则其它端口将进入备用模式，而且仅当活动链接出现故障后才会启用。
- 将同一聚合组中的所有端口移入 / 移出 VLAN，或将其添加到 VLAN 或从中删除时，必须将所有端口视为一个整体。
- 只能为完整的聚合组设定 STP、 VLAN 和 IGMP 设置。

3.4.3.1 使用 LACP 动态配置聚合组

Web — 单击 “Up Links” / “Down Links” => “Link Aggregation” 屏幕。在 “Link Aggregation” 表中找到所需的端口，然后单击 “Enable LACP” 或 “Disable LACP” 按钮。

注： 这些按钮操作会立即生效。为避免在网络中形成环路，请务必在连接端口之前启用 LACP，并在禁用 LACP 之前断开端口连接。请参阅第 3-83 页上的 “命令用法”。

CLI — 下面的示例在端口 NETP0 和 NETP1 上启用 LACP。仅将这些端口连接到另一台交换机上的两个启用 LACP 的聚合组端口，以形成一个聚合组。

```
Console(config)#interface ethernet NETP0                          4-74
Console(config-if)#lacp                                           4-144
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                     4-82
Information of Trunk 1
Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
 Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled

 Current status:
  Created by: Lacp
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1,
Console#
```

SNMP — 等效 MIB 变量。

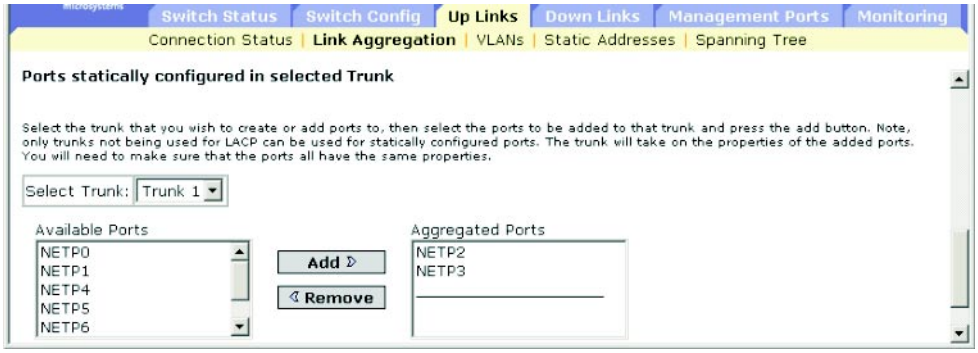
字段名	MIB 变量	访问权限	值范围	默认值
Trunk Maximum ID	sun... trunkMgt. trunkMaxId	只读	整数	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	只读	整数 (1-6)	
Trunk Index	sun... trunkMgt. trunkTable.trunkEntry. trunkIndex	索引	整数	
Trunk Ports	sun... trunkMgt. trunkTable.trunkEntry. trunkPorts	读 / 创建	八位字节字符串 （端口列表）	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	只读	static (1)， lacp (2)	
Trunk Status	sun... trunkMgt. trunkTable.trunkEntry. trunkStatus	读 / 创建	valid (1)， invalid (2)	
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	读 / 写	enabled (1) disabled (2)	

有关其它 CLI 变量的说明，请参阅第 3-75 页上的 “显示连接状态”

3.4.3.2 静态配置聚合组

Web — 单击 “Up Links” / “Down Links” => “Link Aggregation” 屏幕。从下拉列表中选择聚合组索引，选择所需的端口，然后单击 “Add” 或 “Remove”。

注：这些按钮操作会立即生效。为避免在网络中形成环路，请务必在连接端口之前通过配置界面来添加静态聚合组，并在去除静态聚合组之前通过配置界面断开端口连接。请参阅第 3-83 页上的 “命令用法”。



CLI — 本示例使用端口 NETP2 和 NETP3 创建聚合组 2。仅将这些端口连接到另一台交换机上的两个静态聚合组端口，以形成一个聚合组。

```
Console(config)#interface port-channel 2                    4-74
Console(config-if)#exit
Console(config)#interface ethernet NETP2                    4-74
Console(config-if)#channel-group 2                          4-143
Console(config-if)#exit
Console(config)#interface ethernet NETP3
Console(config-if)#channel-group 2
Console(config-if)#end
Console#show interfaces status port-channel 2               4-82
Information of Trunk 2
 Basic information:
  Port type: 1000t
  Mac address: 00-00-E8-66-66-83
 Configuration:
Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
```

```
 Current status:
  Created by: User
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP2, NETP3,
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Trunk Maximum ID	sun... trunkMgt.trunkMaxId	只读	整数	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	只读	整数 (1-6)	
Trunk Index	sun... trunkMgt.trunkTable. trunkEntry.trunkIndex	索引	整数	
Trunk Ports	sun... trunkMgt.trunkTable. trunkEntry.trunkPorts	读 / 创建	八位字节字符串（端口列表）	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	只读	static (1)，lacp (2)	
Trunk Status	sun... trunkMgt.trunkTable. trunkEntry.trunkStatus	读 / 创建	valid (1)，invalid (2)	

有关其它 CLI 变量的说明，请参阅第 3-75 页上的 “显示连接状态”。

3.4.4 配置接口的 VLAN 行为

可以配置特定接口的 VLAN 行为，包括默认的 VLAN 标识符 (PVID)、可接受的帧类型、入口过滤、 GVRP 状态以及 GARP 定时器。

命令用法

- **GVRP** — GARP VLAN 注册协议定义交换机之间交换 VLAN 信息的方式，以便在整个网络的所有端口上自动注册 VLAN 成员。
- **GARP** — GVRP 使用“组地址注册协议”来注册或取消注册桥接 LAN 中的客户端服务的客户端属性。 GARP 定时器的默认值独立于介质访问方法或数据速率。除非您进行 GVRP 注册 / 取消注册时遇到困难，否则不应更改这些值。

命令属性

- **Port** — 端口或聚合组 （上行链接：NETP0-7 ； 下行链接：SNP0-15 ； mgt：NETMGT）。
- **Default VLAN for Port (PVID)** — 分配给在接口上收到的未标记帧的 VLAN ID。（默认值 — 上 / 下行链接：1 ； NETMGT：2）

注：如果接口不是 VLAN 1 的成员，并且已将其 PVID 指定给此 VLAN，那么会自动将该接口作为未标记成员添加到 VLAN 1 中。对于所有其它 VLAN，必须先将某个接口配置成一个不带标记的成员，然后再将该接口的 PVID 指定到给该组。

- **Acceptable Frame Types** — 将接口设置为接受所有帧类型 （包括已标记帧或未标记帧），或只接受已标记帧。如果设置为接收所有类型的帧，那么所有接收到的未带标记的帧都将分配给默认 VLAN。（选项：all、 tagged ； 默认值：all）
- **Switch Port Mode** — 指定端口的 VLAN 成员关系模式。（默认值：Trunk）
  - **Trunk** — 将某端口指定为 VLAN 聚合组的一个端点。聚合组是指两台交换机之间的直接链接，因此端口发送的是标识源 VLAN 的标记帧。
  - **Hybrid** — 指定混合 VLAN 接口。此类端口可以发送带标记或不带标记的帧。

注：如果交换机端口模式设置为 **Trunk**，则属于端口的默认 VLAN （即，与 PVID 相关联）的帧在发送时将不进行标记，但所有其它帧将所分配的 VLAN ID 进行标记。

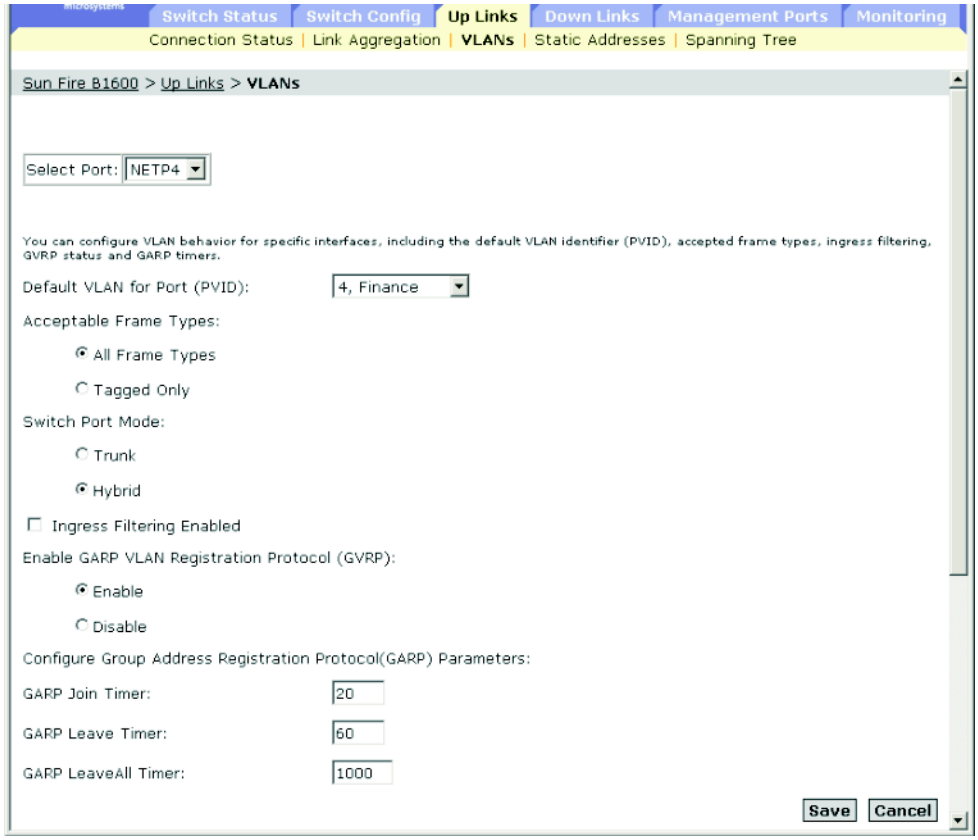
- **Ingress Filtering** — 如果启用了入口过滤，对于成员集中未包含此传入端口的各个 VLAN，该传入端口将丢弃传入它们的帧。（默认值：Disabled）

注：

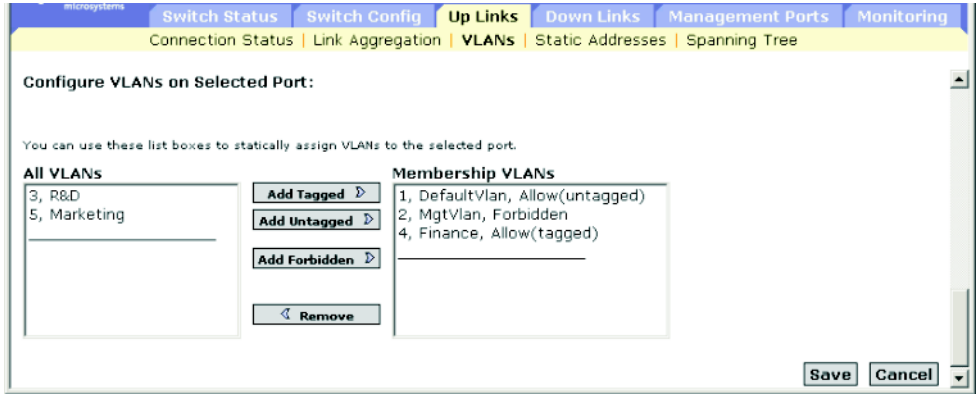
- 入口过滤措施只影响带标记的帧。
- 如果禁用了入口过滤，且标记与交换机已知的某个 VLAN （不包括那些已在此端口明确禁止的 VLAN）匹配，则接口将接受所有标记为指向该 VLAN 的帧。
- 如果启用了入口过滤，则对于成员集中未包含此传入端口的各个 VLAN，该接口将丢弃标记为指向它们的传入帧。
- 传入过滤不会影响独立于VLAN的BPDU帧，如GVRP或STP。但是，它们的确会影响与 VLAN 相关的 BPDU 帧，例如 GMRP。

- **GVRP** — 为接口启用 / 禁用 GVRP。在此设置生效之前，必须为交换机全局启用 GVRP （第 3-36 页）。如果禁用此设置，在此端口接收的所有 GVRP 数据包将被丢弃，并且将不会从其它端口传播 GVRP 注册。（默认值：Disabled）
- **GARP Join Timer** — 传输参与某个 VLAN 组的请求 / 查询的时间间隔。（范围：20-1000 厘秒；默认值：20 厘秒）
- **GARP Leave Timer** — 端口离开 VLAN 组之前等待的时间间隔。此时间应设置为加入时间的 2 倍以上。这样，就可以确保在发出 “Leave” 或 “LeaveAll” 消息以后，申请者可以在端口真正离开组之前重新加入。（范围：60-3000 厘秒；默认值：60 厘秒）
- **GARP LeaveAll Timer** — 为 VLAN 组参与者发出 “LeaveAll” 询问消息与端口离开组之间的时间间隔。此时间间隔应大大高于离开时间，以使重新加入组的节点所生成的通信量最少。（范围：500-18000 厘秒；默认值：1000 厘秒）
- **VLANs on Selected Port** — 静态地将端口分配给指定的 VLAN。
- **Membership Type** — 设置端口的静态 VLAN 成员关系。
  - **Tagged**：接口是VLAN的成员。此VLAN上的端口所传输的所有数据包都将被标记，即携带一个标记，也就携带了 VLAN 或 CoS 信息。
  - **Untagged**：接口是VLAN的成员。此VLAN上的端口传输的所有数据包将不被标记，即不携带标记，因此也不携带 VLAN 信息或 CoS 信息。
  - **Forbidden**：禁止接口自动通过 GVRP 加入 VLAN。请参阅第 3-32 页上的 “自动 VLAN 注册”。
  - **Remove**：从该 VLAN 删除选定接口。

Web — 打开 “Open Up Links” / “Down Links” / “Management Port” => “VLANs”。填写每个接口所需的设置，然后单击 “Save”。



滚动到 VLAN 成员表，配置选定接口所需的 VLAN。



CLI — 本示例将端口 NETP4 设置为只接受带标记帧，将 PVID 4 指定为本地 VLAN ID，启用 GVRP，设置 GARP 定时器，然后将交换机端口模式设置为混合。

```
Console(config)#interface ethernet NETP4                          4-74
Console(config-if)#switchport acceptable-frame-types tagged       4-108
Console(config-if)#no switchport ingress-filtering                4-108
Console(config-if)#switchport allowed vlan add 4 tagged           4-110
Console(config-if)#switchport native vlan 4                       4-109
Console(config-if)#switchport gvrp                                4-113
Console(config-if)#garp timer join 10                             4-115
Console(config-if)#garp timer leave 90                            4-115
Console(config-if)#garp timer leaveall 2000                       4-115
Console(config-if)#switchport mode hybrid                         4-107
Console(config-if)#switchport forbidden vlan add 3                4-111
Console(config-if)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Port PVID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPvid	读 / 写	整数 (1-4094)	1
Port Acceptable Frame Type	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortAcceptable-FrameTypes	读 / 写	admitAll (1)， admitOnlyVlan-Tagged (2)	admitAll
Port Mode	sun... vlanMgt. vlanPortTable. vlanPortEntry. vlanPortMode	读 / 写	hybrid (1)， dot1qTrunk (2)	hybrid

字段名	MIB 变量	访问权限	值范围	默认值
Port Ingress Filtering	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortIngressFiltering	读 / 写	true (1)， false (2)	false
Port GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortGVRPStatus	读 / 写	enabled (1)， disabled (2)	disabled
GARP Join Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpJoinTime	读 / 写	整数 (20-1000) 厘秒	20 厘秒
GARP Leave Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpLeaveTime	读 / 写	整数 (60-3000) 厘秒	60 厘秒
GARP Leave All Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarp-LeaveAllTime	读 / 写	整数 (500-18000) 厘秒	1000 厘秒

字段名	MIB 变量	访问权限	值范围	默认值
VLAN Static Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	读 / 创建	八位字节字符串 （大小 (0-32)）	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticRowStatus	读 / 创建	enable (1)， disable (2)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic-UntaggedPorts	读 / 创建	八位字节字符串 （端口列表）	
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden-EgressPorts	读 / 创建	八位字节字符串 （端口列表）	

3.4.5 配置静态地址

可以使用地址过滤来设置绑定到特定端口及 VLAN 的静态地址，或启用端口安全性功能来限制流向地址表（包括动态地址或静态地址）中当前所列条目的所有入站通信。

命令用法

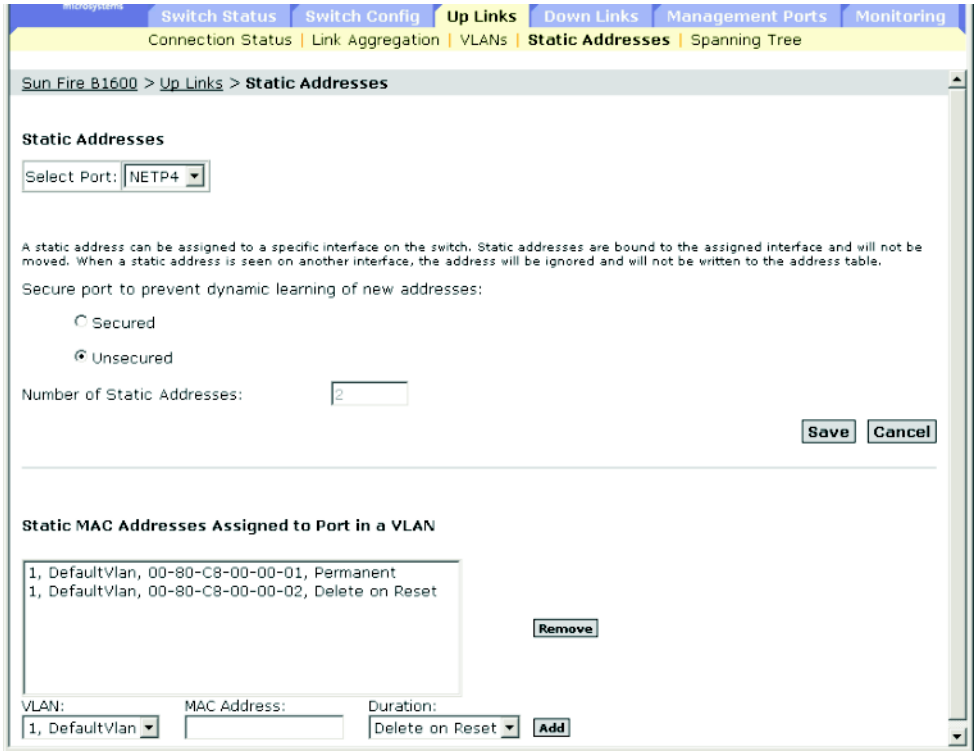
- **Setting Static Addresses** — 可以将静态地址分配给此交换机上的特定接口。如果当前绑定到某个接口的静态地址出现在另一个接口上，则看到此地址的新接口将不会接受来自该地址的数据，也不会向该地址传输数据，而且不会将该地址包括在其地址表中。
- **Configuring Port Security** — 如果启用端口安全性，交换机将停止动态了解指定端口上的新地址的功能。而只接受那些源地址已存储在动态地址表中的传入通信。要使用端口安全性，首先要允许交换机动态了解用于初始培训阶段的接口上所接收的 < 源 MAC 地址， VLAN> 对；然后再启用端口安全性，以停止了解地址的功能。务必将了解功能的启用时间设置得足够长，这样才能确保所有有效 VLAN 成员都已在选定接口上注册。
  要在以后添加新的 VLAN 成员，可以手动添加静态地址，或关闭端口安全性，以重新启用了解功能，而且时间足够新 VLAN 成员进行注册。然后可以根据需要再次禁用了解功能，以确保安全。

命令属性

- **Port** — 接口 （端口或聚合组）。
  （上行链接端口：NETP0-7 ；下行链接端口：SNP0-15）
- **Secure Port** — 启用或禁用端口安全性。（默认值：Disabled）
  安全端口具有以下限制：
  - 不能使用端口监视功能。
  - 不能是多 VLAN 接口。
  - 不能连接到网络互连设备。
  - 不能是聚合组端口。
- **Number of Static Addresses*** — 手动配置的地址的数量。
- **VLAN** — 所配置的 VLAN (1-4094) 的 ID 及其名称。
- **MAC Address** — 与此接口关联的 MAC 地址。
- **Duration** — 可以将地址设置为以下类型：
  - **Permanent** — 分配是永久性的，重置交换机后保持不变。
  - **Delete on Reset** — 地址分配持续到交换机重置时为止。

* 仅适用于 Web

Web — 打开 “Up Links”/ “Down Links” => “Address Filtering”。指定接口。选中 “Secure Port” 复选框以启用端口安全性。输入 VLAN、 MAC 地址及持续时间，然后单击 “Add”。



CLI — 本示例向静态地址表添加相同的项。

```
Console(config)#interface ethernet NETP4
Console(config-if)#port security                                    4-91
Console(config-if)exit
Console(config)#mac-address-table static 00-80-c8-00-00-01
  interface ethernet NETP4 vlan 1 permanent                         4-87
Console(config)#mac-address-table static 00-80-c8-00-00-02
  interface ethernet NETP4 vlan 1 delete-on-reset
Console(config)#exit
Console#show mac-address-table ethernet NETP4                       4-88
 Interface   Mac Address       Vlan Type
 ----------- ----------------- ---- -----------------
       NETP4 00-80-C8-00-00-01    1 Permanent
       NETP4 00-80-C8-00-00-02    1 Delete-on-reset
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Static Receive Port	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticReceivePort	读 / 写	整数	
Port Security Status	sun... securityMgt. portSecurityMgt portSecPortTable. portSecPortEntry. portSecPortStatus	读 / 写	enabled (1)， disabled (2)	disabled
Number of Static Addresses	*未定义*			
VLAN Index	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	索引	整数	
Static Addresses	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticAddress	读 / 写	MAC 地址	
Static Status	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticStatus	读 / 写	其它 (1)， invalid(2)， permanent(3)， deleteOnReset(4)， deleteOnTimeout(5)	permanent

3.4.6 管理生成树算法的接口

可以配置特定接口的 RSTP 属性，包括端口优先级、路径成本、链接类型和边缘端口。对于介质类型相同的端口，可以使用不同的优先级或路径成本来指定首选路径；并使用链接类型来指定点到点连接或共享介质连接；还可以使用边缘端口来指定连接的设备是否可以支持快速转发。

3.4.6.1 显示 STA 的当前接口设置

命令属性

- **Port** — 仅限端口；即，无聚合组或聚合组端口成员。（上行链接端口：NETP0-7 ；下行链接端口：SNP0-15）
- **STA Status** — 显示此端口在生成树中的当前状态：
  - **Discarding** — 端口接收 STA 配置消息，但不转发数据包。
  - **Learning** — 端口按由 “Forward Delay” 参数设置的时间间隔传送了配置消息，而没有收到不一致的信息。清除端口的地址表，端口开始了解地址。
  - **Forwarding** — 端口转发数据包，并继续了解地址。
- **Priority** — 定义此端口在生成树算法中使用的优先级。如果交换机上所有端口的路径成本都相同，则将具有最高优先级 （即值最低）的端口配置为生成树中的活动链接。这样，在生成树算法检测到网络环路时，优先级越高的端口被阻塞的可能性就越低。如果具有最高优先级的端口不止一个，则启用具有最低数字标识符的端口。
- **Path Cost** — STA 使用此参数来确定设备之间的最佳路径。因此，应为连接到较快介质的端口指定较低的值，为连接到较慢介质的端口指定较高的值。（应优先考虑路径成本，然后再考虑端口的优先级。）
- **Designated Cost** — 数据包从此端口传递到当前生成树配置中的根设备所需的成本。介质传输速度越慢，成本越高。
- **Designated Bridge** — 该端口必须通过某台设备进行通信才能到达生成树的根设备，此参数指定这台特定设备的优先级和 MAC 地址。
- **Designated Port** — 此交换机必须通过桥接设备才能与生成树的根设备进行通信，此参数即指定该桥接设备的优先级和端口号。

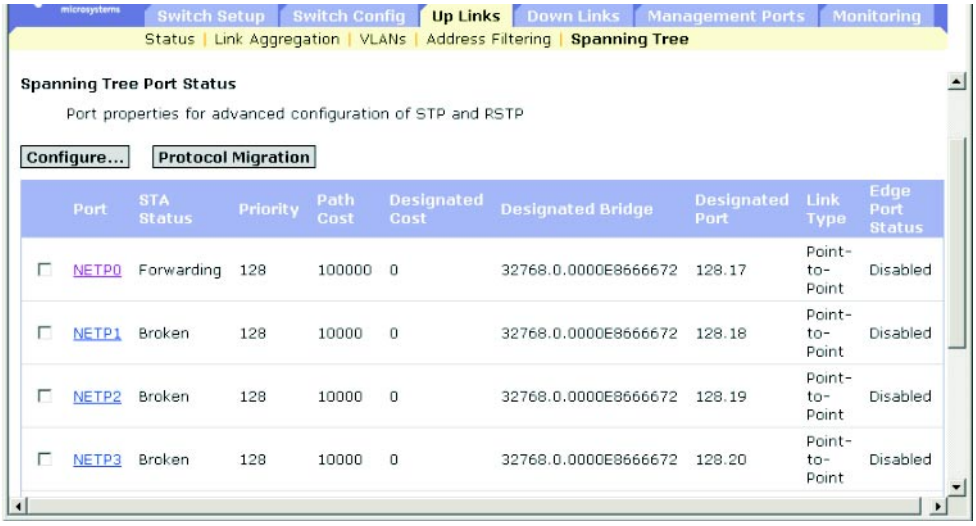
- **Link Type** （管理链接类型 *）— 连接到此接口的链接类型。
  - Point-to-Point — 只与一个其它网桥连接。
  - Shared — 连接到两个或多个网桥。
  - Auto — 交换机自动确定该接口是连接到点到点链接还是连接到共享介质。
- **Edge Port**（管理边缘端口 *）— 如果接口连接到位于桥接 LAN 末端的 LAN 网段或末端节点上，则可以启用此选项。由于末端节点**不会**产生转发环路，因此它们可以直达生成树转发状态。指定边缘端口的好处有四：第一，使各种设备 （如工作站或服务器）能更快地收敛；第二，保留了当前的转发数据库，从而减少了在重新配置事件过程中为重建地址表而需要的帧扩散量；第三，不会导致生成树在接口改变状态时启动重新配置操作；第四，解决了与 STA 相关的其它超时问题。不过，应谨记只能对连接到末端节点设备的端口启用 “边缘端口” 功能。

* CLI 显示此术语。

以下这些其它参数仅在 CLI 上显示：

- **Admin status** — 显示是否在此接口上启用了 STA。
- **Role** — 根据以下情况来分配角色：端口是否为将此网桥连接到根网桥 （即**根**端口）、通过网桥将 LAN 连接到根网桥 （即**指定**端口）的活动拓扑结构的一部分；端口是否为**替换**或**备份**端口 （此类端口可以在其它网桥、桥端口或 LAN 发生故障或被删除时提供连接）。如果端口在生成树中没有角色，则角色被设置为禁用 （即，**禁用**的端口）。
- **Designated root** — 生成树中此交换机已接受作为根设备的设备的优先级和 MAC 地址。
- **Forward transitions** — 此端口从 “了解” 状态转变为 “转发” 状态的次数。
- **Oper edge port** — 此参数被初始化为 “管理边缘端口” 的设置 （即， true 或 false），但如果收到 BPDU，将设置为 false。
- **Oper Link type** — 与此接口连接的 LAN 网段的运行时点到点状态。此参数通过手动配置或自动检测来确定 （请参阅 “管理链接类型” 的说明）。

Web — 单击“Up Links”/ “Down Links”=> “Spanning Tree”=> “Spanning Tree Protocol”。



CLI — 本示例显示端口 NETP4 的 STA 属性。

```
Console#show spanning-tree ethernet NETP4                    4-102
SNP0 information
---------------------------------------------------------------
 Admin status          : enable
 Role                  : designate
 State                 : forwarding
 Path cost             : 10000
 Priority              : 128
 Designated cost       : 10000
 Designated port       : 128.1
 Designated root       : 32768.00209C23C267
 Designated bridge     : 32768.0000E8666672
 Forward transitions   : 0
 Admin edge port       : disable
 Oper edge port        : disable
 Admin Link type       : point-to-point
 Oper Link type        : point-to-point
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry	索引	整数 (1-25)	
STA Port State	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortState	只读	discarding (1)， learning (2)， forwarding (3)	
STA Port Priority	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	读 / 写	整数 (0-240)	128
STA Port Path Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	读 / 写	整数 （long： 1-200,000,000； short：1-65,535）	第 3-102 页
STA Port Designated Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedCost	只读	整数	
STA Port Designated Bridge	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedBridge	只读	八位字节字符串	
STA Port Designated Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedPort	只读	八位字节字符串	
STA Port Admin Point to Point	sun...staMgt. staPortTable. staPortEntry. staPortAdminPointTo- Point	读 / 写	forceTrue(0) forceFalse (1) auto (2)，	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	读 / 写	true (1)， false (2)	false

字段名	MIB 变量	访问权限	值范围	默认值
STA Port Enable (Admin status)	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortEnable	读/写	enabled (1)，disabled (2)	enabled
STA Port Role	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPortRole	只读	disabled (1)，root (2)，designated (3)，alternate (4)，backup (5)	
STA Port Designated Root	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-DesignatedRoot	只读	八位字节字符串	
STA Port Forward Transitions	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-ForwardTransitions	只读	计数	

3.4.6.2 配置 STA 的接口设置

这些设置适用于当交换机设置为 STP 强制兼容模式 （第 3-53 页）和 RSTP 时所选择的接口。

命令属性

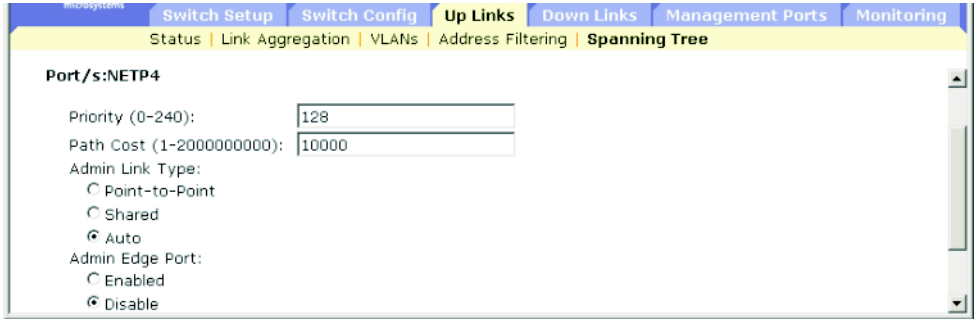
- **Priority** — 定义生成树算法 (STA) 中用于此端口的优先级。如果交换机上所有端口的路径成本都相同，则将具有最高优先级 （即，值最低）的端口配置为生成树中的活动链接。这样，如果 STA 检测到网络环路，优先级越高的端口被阻塞的可能性就越低。如果具有最高优先级的端口不止一个，则启用具有最低数字标识符的端口。
  - 默认值：128
  - 范围：0-240，步进值为 16
- **Path Cost** — STA 使用此参数来确定设备之间的最佳路径。因此，应为连接到较快介质的端口指定较低的值，为连接到较慢介质的端口指定较高的值。（应优先考虑路径成本，然后再考虑端口的优先级。）
  - 范围 —
    - 以太网：200,000-20,000,000
    - 快速以太网：20,000-2,000,000
    - 千兆位以太网：2,000-200,000

- 默认值 —
  - 以太网 — 半双工：2,000,000；全双工：1,000,000；聚合组：500,000
  - 快速以太网 — 半双工：200,000；全双工：100,000；聚合组：50,000
  - 千兆位以太网 — 全双工：10,000；聚合组：5,000

注：如果 “Path Cost Method”设置为 “short”（第 3-59 页），则最大路径成本为 65,535。

- **Admin Link Type** — 与此接口相连的链接类型。（默认值：Auto）
  - Point-to-Point — 只与一个其它网桥连接。
  - Shared — 连接到两个或多个网桥。
  - Auto — 交换机自动确定该接口是连接到点到点链接还是连接到共享介质。
- **Admin Edge Port** — 如果接口连接到位于桥接 LAN 末端的 LAN 网段或末端节点，则可以启用此选项。由于末端节点**不会**产生转发环路，因此它们可以直达生成树转发状态。指定边缘端口的好处有四：第一，使各种设备（如工作站或服务器）能更快地收敛；第二，保留了当前的转发数据库，从而减少了在重新配置事件过程中为重建地址表而需要的帧扩散量；第三，不会导致生成树在接口改变状态时启动重新配置操作；第四，解决了与 STA 相关的其它超时问题。不过，应谨记只能对连接到末端节点设备的端口启用 “边缘端口”功能。（默认值：NETP0-7：Disabled；SNP0-15：Enabled 并固定使用此设置）

Web — 单击 “Up Links”/ “Down Links” => “Spanning Tree” => “Spanning Tree Protocol”。要配置 STP (IEEE 802.1D) 的接口设置，请单击所需接口的复选框，并单击 “Configure”。然后修改所需的属性，并单击 “Save”。



CLI — 本示例设置端口 NETP5 的 STP 属性。

```
Console(config)# interface ethernet NETP5                    4-74
Console(config-if)#spanning-tree port-priority 128           4-99
Console(config-if)#spanning-tree cost 19                     4-98
Console(config-if)#spanning-tree link-type auto              4-101
Console(config-if)#no spanning-tree edge-port                4-100
```

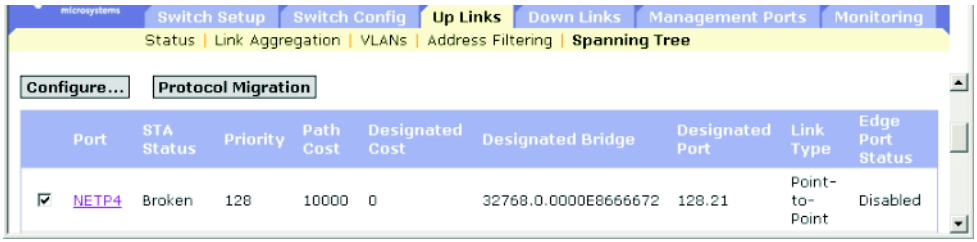
SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
STA Port Priority	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	读 / 写	整数 (0-240)	128
STA Port Path Cost	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	读 / 写	整数 （long：1-200,000,000； short：1-65,535）	第 3-102 页
STA Port Admin Link Type	sun...staMgt. staPortTable. staPortEntry. staPortAdmin-PointToPoint	读 / 写	forceTrue (0)， forceFalse (1)， auto (2)	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	读 / 写	true (1)， false (2)	false

3.4.6.3 检查接口的 STA 协议状态

只要交换机检测到 STP BPDU （包括配置 BPDU 或拓扑结构更改通知 BPDU），它就会自动将选定接口设置为强制的 STP 兼容模式。不过，也可以使用 “Protocol Migration”按钮手动重新检查要在选定接口上发送的相应 BPDU 格式 （RSTP 或 STP 兼容）。

Web — 单击 “Up Links”/ “Down Links” => “Spanning Tree” => “Spanning Tree Protocol”。选择所需的接口，然后单击 “Protocol Migration”按钮。



CLI — 本示例使用协议迁移命令来验证要在此接口上发送的生成树消息类型 （即 RSTP 或 STP 兼容）。

```
Console(config)interface ethernet NETP4
Console(config-if)#spanning-tree protocol-migration          4-100
Console(config-if)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
STA Port Protocol Migration	sun...staMgt. staPortTable. staPortEntry. staPortProtocolMigration	读/写	true (1), false (2)	true

3.4.7 过滤来自管理端口的通信

可以通过配置数据包过滤来阻止指定 IP 通信从下行链接端口到达内部管理端口 (NETMGT)。（请注意，绝对不允许从上行链接端口向管理端口传送通信。）

命令用法

- 根据系统的默认设置，禁止在内部管理端口与下行链接端口之间传送所有 IP 数据包。如果需要通过该管理端口访问服务器刀片，则必须设置一个过滤器，以允许在管理端口和下行链接端口之间传递指定的数据包。
- 根据系统的默认设置，禁止任何 IP 数据包从下行链接端口传递到管理端口 (NETMGT)。如果服务器刀片需要通过该管理端口 (NETMGT) 访问管理网络，则必须设置一个过滤器，以允许从下行链接端口向该管理端口传送特定帧。

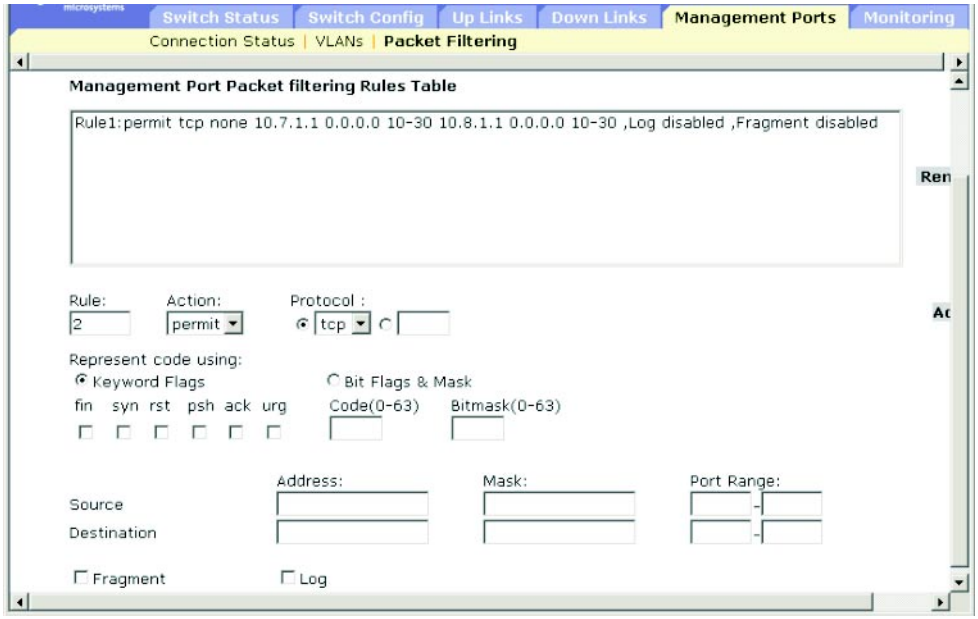
注：不允许在上行链接端口与该管理端口之间通信。

命令属性

- **Rule** — 在规则表中的指定位置插入一条过滤规则，从而使该表中位于插入位置或之后的所有现有模式均向下移动。规则编号不得大于该表中下一个可用编号。如果未指定规则编号，则会在规则表的末尾添加一个新模式。（范围：1-128）
- **Action** — 阻止或允许数据包从下行链接端口移到管理端口。（选项：permit，deny）
- **Protocol** — 选择一种协议 （TCP、 UDP、其它），或选择协议编号 (0-255)。
- **Keyword Flags**（代码序列）— 指示 TCP 标头第 14 个字节中的一个标记。可以指定一个代码序列 （即，如果选择，则为 “ON”；如果未选择，则为 “OFF”）。符号名称与相应的位包括以下各项：
  - **fin** (1) — 结束
  - **syn** (2) — 同步
  - **rst** (4) — 重置
  - **psh** (8) — 推
  - **ack** (16) — 确认
  - **urg** (32) — 紧急指针
- **Code** — 用于指定 TCP 标头第 14 个字节中的标记位的十进制数 （代表位字符串）。（范围：0-63）
- **Bitmask** — 适用于该代码的十进制数 （代表位掩码）。输入一个十进制数，其中所对应的二进制位 “1” 表示与一位匹配，“0” 表示忽略一位。可以指定以下位：32 (urg)、 16 (ack)、 8 (psh)、 4 (rst)、 2 (syn)、 1 (fin)
- **Source** — 帧的 TCP/UDP 源地址、子网掩码和端口范围。（端口范围：0-65535）
- **Destination** — 帧的 TCP/UDP 目标地址、子网掩码和端口范围。（端口范围：0-65535）

- **Fragment** — 规则使数据包仅与“分组片位”(MF) 位组匹配，或与大于零的分段偏移量匹配。如果未设置分段，规则将匹配分段数据包和未分段的数据包。
- **Log** — 在日志缓冲区中记录所有匹配的数据包。存储在日志缓冲区中的最大条目数为 64。如果缓冲区已满，它将绕回并覆盖时间最早的条目。请注意，日志存储在 RAM 中，因此，当交换机重置时，这些日志将丢失。

Web — 单击“Management Port”=>“Packet Filtering”。输入所需的规则，然后单击“Add”。本示例中的规则允许使用 TCP 端口 10-30 从源地址 10.7.1.1 向目标地址 10.8.1.1 传送 TCP 通信。



CLI — 本示例允许使用所有协议类型，并同时为源地址和目标地址使用一个空地址和网络掩码，以允许所有数据包通过此过滤器。有关示例的完整列表，请参阅第 4-68 页上的第 4.3.7.8 节 “ip filter”。

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0  4-68
Console(config)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
索引	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleIndex	无访问权限	整数 (1-128)	
Action	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleAction	读 / 创建	permit (1)， deny (2)	
Protocol	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleProtocol	读 / 创建	整数 （0-256 ； 256 表示可以采用任何协议）	
Source IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcIpAddr & pfuRuleSrcIpBitmask	读 / 创建	IP 地址	
Source IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcPortRange1 & pfuRuleSrcPortRange2	读 / 创建	整数 (1-65536)	
Destination IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstIpAddr & pfuRuleDstIpBitmask	读 / 创建	IP 地址	

字段名	MIB 变量	访问权限	值范围	默认值
Destination IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstPortRange1 & pfuRuleDstPortRange2	读 / 创建	整数 (1-65536)	
TCP Code	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCode	读 / 创建	整数 (0-63)	
TCP Code Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCodeBitmask	读 / 创建	整数 (0-63)	
Fragments	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleFragments	读 / 创建	enabled (1), disabled (2)	disabled
Log	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleLog	读 / 创建	enabled (1), disabled (2)	disabled

3.5 监视端口和管理通信

本节讨论交换机的监视功能，包括用来执行以下操作的功能：将通信镜像到监视端口以供分析、显示任意端口的详细网络统计信息，或显示有关通过管理端口的 SNMP 通信的主要统计信息。

注：Sun Fire B1600 刀片式系统机箱上的集成交换机中都包含两块链接在一起的交换机芯片。若要镜像某个端口上的通信，只能使用该端口所在交换机芯片上的其它端口才有可能实现。端口 NETP0、NETP1、NETP4、NETP5 以及 SNP8 到 SNP15 在同一交换机芯片上。端口 NETP、NETP3、NETP6、NETP7 以及 SNP0 到 SNP7 位于另一交换机芯片上。（如果您查看 SSC 的后面板，则将看到右侧的所有端口位于一块芯片上，而左侧的所有端口位于另一块芯片上。）

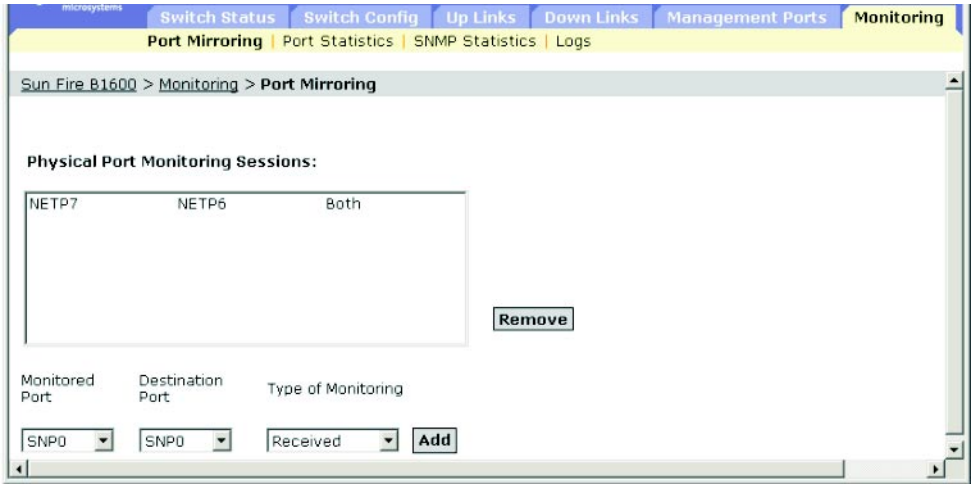
3.5.1 配置端口镜像

可将通信从任何源端口镜像到目标端口，以便进行实时分析。然后，可在目标端口上连接一个逻辑分析器或 RMON 探测器，并在完全不进行干预的情况下研究通过源端口的通信。

命令用法

- 镜像端口的速度应与源端口的速度相匹配或超过源端口的速度，否则，镜像端口就可能丢失通信。
- 在镜像端口通信时，目标端口与源端口必须位于同一个 VLAN 中。

Web — 打开“Monitoring”=>“Port Mirror”。指定源端口、要镜像的通信类型及监视端口，然后单击“Add”。



CLI — 使用 interface 命令选择镜像端口，然后使用 port monitor 命令指定源端口。请注意， CLI 下的默认镜像可同时用于接收和发送的数据包。

```
Console(config)#interface ethernet NETP7                    4-74
Console(config-if)#port monitor ethernet NETP6              4-140
Console(config-if)#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Mirror Source Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorSourcePort	不可访问	整数	
Mirror Destination Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorDestinationPort	不可访问	整数	
Mirror Type	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorType	读 / 创建	rx (1), tx (2), both (3)	both
Mirror Status	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorStatus	读 / 创建	valid (1), invalid (2)	

3.5.2 显示端口统计信息

可以通过 “接口组”和 “Ethernet-like MIB”来显示有关网络通信的标准统计信息，还可以显示基于 RMON MIB 的通信的详细信息。“Interfaces statistics”和 “Ethernet-like statistics”显示通过每个端口的通信所包含的错误。这些信息可用来确定交换机可能存在的问题 （如端口故障或不寻常的高负载）。通过 “RMON statistics”，可以访问大量的统计信息，包括通过每个端口的不同帧类型和大小的总数。显示的所有值均已自上一次系统重新引导后开始累计，并以每秒计数的形式显示。默认情况下，统计信息每 20 秒刷新一次。

注：RMON 组 2、 3 和 9 只能使用 SNMP 进行访问。

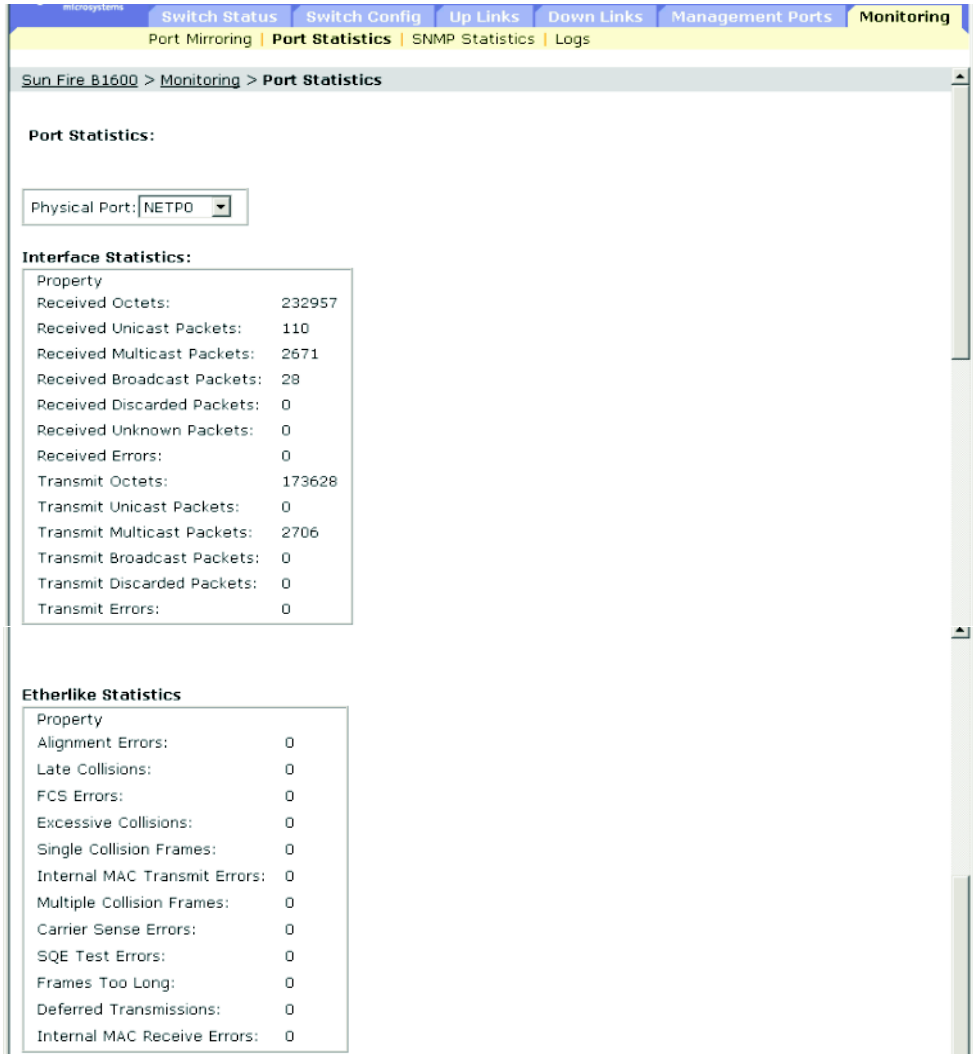
命令属性

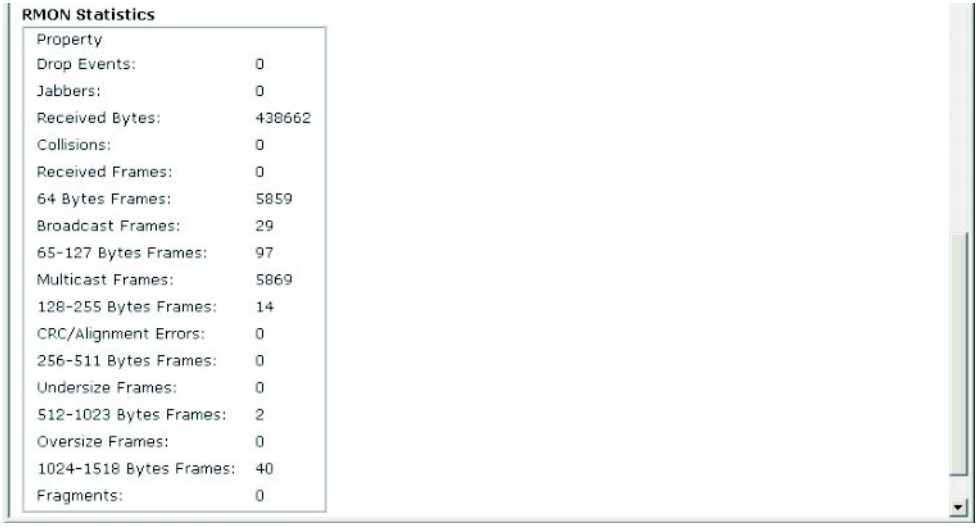
参数	说明
Interface Statistics	
Received Octets	该接口上收到的八位字节的总数，包括组帧字符。
Received Unicast Packets	向较高层协议传送的子网— 单点传送数据包的数量。
Received Multicast Packets	这一子层向更高 （子）层传送的数据包的数量，这些数据包的目标地址是该子层上的某个多点传送地址。
Received Broadcast Packets	这一子层向更高 （子）层传送的数据包的数量，这些数据包的目标地址为该子层上的某个广播地址。
Received Discarded Packets	选择丢弃的入站数据包的数量，即使没有检测到错误也丢弃这些数据包，目的是为了防止将它们传送到更高层协议。丢弃此类数据包的一种可能原因是为了释放缓冲区空间。
Received Unknown Packets	该接口收到但由于协议未知或不受支持而被丢弃的数据包数量。
Received Errors	其中包含错误而导致无法传送到更高层协议的入站数据包数量。
Transmit Octets	该接口上传出的八位字节的总数，包括组帧字符。
Transmit Unicast Packets	较高层协议请求传送到子网 - 单点传送地址的数据包总数，包括丢弃或未发送的那些数据包。
Transmit Multicast Packets	较高层协议请求传送到该子层上的某个多点传送地址的数据包总数，包括丢弃或未发送的那些数据包。

参数	说明
Transmit Broadcast Packets	较高层协议请求传送到该子层上的某个多点广播地址的数据包总数，包括丢弃或未发送的那些数据包。
Transmit Discarded Packets	选择要丢弃的出站数据包的数量，即使未检测到错误，也要丢弃这些数据包，目的是为了防止传送这些数据包。丢弃此类数据包的一种可能原因是为了释放缓冲区空间。
Transmit Errors	由于错误而导致无法传送的出站数据包的数量。
Etherlike Statistics	
Alignment Errors	调整错误 （错误同步的数据包）的数量。
Late Collisions	传送某个数据包时，在 512 位时间之后检测到冲突的次数。
FCS Errors	特定接口上收到的长度为八位字节的整数倍但未通过 FCS 校验的帧的数量。该计数不包括收到的带有 “frame-too-long”或“frame-too-short”错误的帧。
Excessive Collisions	由于冲突过多而导致在特定接口上传送失败的帧的计数。如果该接口以全双工模式运行，则该计数不会递增。
Single Collision Frames	传送只受一个冲突限制的已成功传送的帧的数量。
Internal MAC Transmit Errors	由于内部 MAC 子层传送错误而导致在特定接口上传送失败的帧的计数。
Multiple Collision Frames	传送受多个冲突限制的已成功传送的帧的计数。
Carrier Sense Errors	在试图传送帧时，缺乏或无法保证载波侦听条件的次数。
SQE Test Errors	特定接口的 PLS 子层生成 SQE TEST ERROR 消息的次数。
Frames Too Long	特定接口上收到的超过最大允许帧大小的帧的计数。
Deferred Transmissions	由于介质忙而导致在特定接口上的第一次传送尝试被延迟的帧的计数。
Internal MAC Receive Errors	由于内部 MAC 子层接收错误而导致在特定接口上接收失败的帧的计数。
RMON Statistics	
Drop Events	由于缺乏资源而导致丢失数据包的事件总数。
Jabbers	所收到的长度大于 1518 个八位字节 （不包括组帧位，但包括 FCS 八位字节）且带有 FCS 错误或调整错误的帧的总数。
Received Bytes	网络上所收到的数据的总字节数。此统计信息可作为以太网利用率的一个合理指标。

参数	说明
Collisions	此以太网网段上的冲突总数的最佳估计值。
Received Frames	收到的帧 （包括错误帧、广播帧和多点传送帧）的总数。
Broadcast Frames	所接收的定向到该广播地址的完好帧总数。请注意，该数量不包括多点传送数据包。
Multicast Frames	所接收的定向到此多点传送地址的完好帧总数。
CRC/Alignment Errors	CRC 错误/调整错误 （FCS 错误或调整错误）的数量。
Undersize Frames	所收到的长度小于 64 个八位字节 （不包括组帧位，但包括 FCS 八位字节），正常条件下应完好组帧的帧的总数。
Oversize Frames	所收到的长度大于 1518 个八位字节 （不包括组帧位，但包括 FCS 八位字节），正常条件下应完好组帧的帧的总数。
Fragments	所收到的长度小于 64 个八位字节 （不包括组帧位，但包括 FCS 八位字节）且带有 FCS 错误或调整错误的帧的总数。
64 Bytes Frames	所接收和传送的长度为 64 个八位字节 （不包括组帧位，但包括 FCS 八位字节）的帧 （包括错误数据包）的总数。
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	所接收和传送的八位字节数在指定范围内 （不包括组帧位，但包括 FCS 八位字节）的帧 （包括错误数据包）的总数。

Web — 单击 “Monitoring” => “Statistics”。选择所需的接口，然后单击 “Select”。您还可以使用位于页面底部的 “Refresh” 按钮来更新屏幕。





CLI — 本示例显示端口 SNP13 的统计信息。

```
Console#show interfaces counters ethernet SNP13                    4-83
Ethernet 13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unicast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input:v0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
 RMON stats:
  Drop events: 0, Octets:4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	范围
Interface Statistics			
In Octets	MIB-II. interfaces.ifNumber.ifTable.ifEntry.ifInOctets	只读	整数
In Unicast Packets	MIB-II. interfaces.ifNumber.ifTable.ifEntry. ifInUcastPkts	只读	整数
In Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInMulticastPkts	只读	整数
In Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInBroadcastPkts	只读	整数
In Discards	MIB-II. interfaces.ifTable.ifEntry.ifInDiscards	只读	整数
In Unknown Protocols	MIB-II. interfaces.ifTable.ifEntry.ifInUnknownProtos	只读	整数
In Errors	MIB-II. interfaces.ifTable.ifEntry.ifInErrors	只读	整数
Out Octets	MIB-II. interfaces.ifTable.ifEntry.ifOutOctets	只读	整数
Out Unicast Packets	MIB-II. interfaces.ifTable.ifEntry.ifOutUcastPkts	只读	整数
Out Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutMulticastPkts	只读	整数
Out Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutBroadcastPkts	只读	整数
Out Discards	MIB-II. interfaces.ifTable.ifEntry.ifOutDiscards	只读	整数
Out Errors	MIB-II. interfaces.ifTable.ifEntry.ifOutErrors	只读	整数

字段名	MIB 变量	访问权限	范围
Etherlike Statistics			
Alignment Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsAlignmentErrors	只读	整数
Late Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsLateCollisions	只读	整数
FCS Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFCSErrors	只读	整数
Excessive Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3Stats-ExcessiveCollisions	只读	整数
Single Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSingleCollisionFrames	只读	整数
Internal Mac Transmit Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacTransmitErrors	只读	整数
Multiple Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsMultipleCollisionFrames	只读	整数
Carrier Sense Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsCarrierSenseErrors	只读	整数
SQE Test Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSQETestErrors	只读	整数
Frames Too Long	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFrameTooLongs	只读	整数
Deferred Transmissions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsDeferredTransmissions	只读	整数
Internal MAC Receive Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacReceiveErrors	只读	整数

字段名	MIB 变量	访问权限	范围
RMON Statistics			
Drop Events	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsDropEvents	只读	整数
Jabbers	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsJabbers	只读	整数
Received Octets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsOctets	只读	整数
Collisions	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsCollisions	只读	整数
Received Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts	只读	整数
Broadcast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsBroadcastPkts	只读	整数
Multicast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsMulticastPkts	只读	整数
CRC/Alignment Errors	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsCRCAlignErrors	只读	整数
Undersize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsUndersizePkts	只读	整数
Oversize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsOversizePkts	只读	整数
Fragments	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsFragments	只读	整数
64 Bytes Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts64Octets	只读	整数
X-**Y** Byte Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts**X**to**Y**Octets	只读	整数

3.5.3 显示 SNMP 统计信息

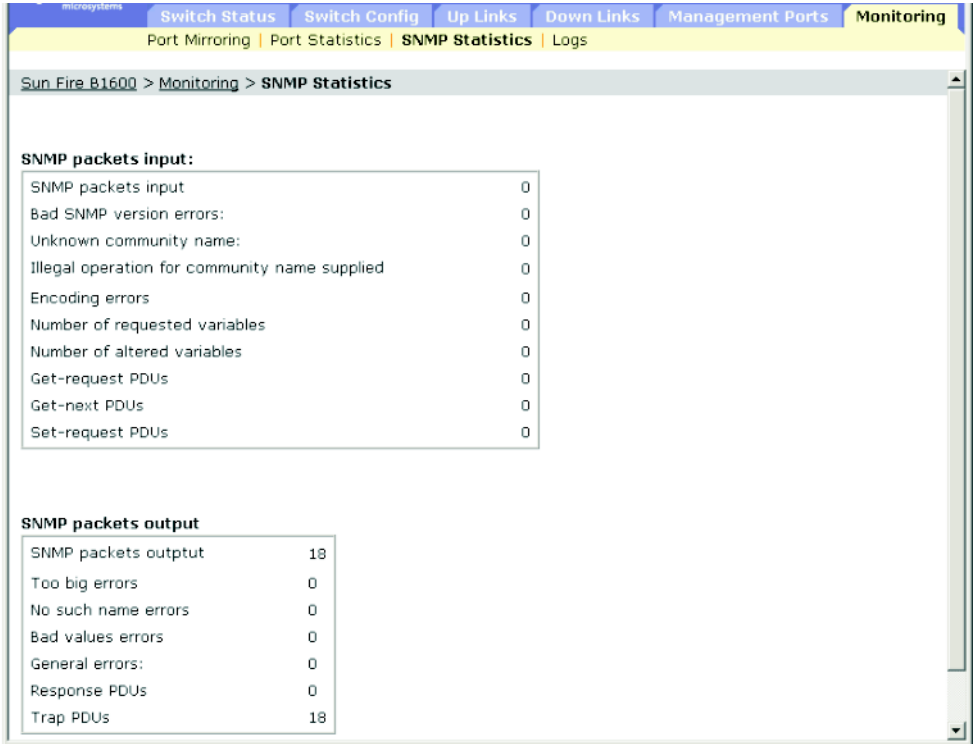
可以显示与通过管理端口的 SNMP 通信有关的主要统计信息。可以使用这些信息来调试 SNMP 错误，显示交换机处理的 SNMP 通信总量，以及显示通过 SNMP 对交换机进行的所有非法访问尝试。

命令属性

参数	说明
SNMP packets input	
SNMP packets input	通过传输服务发送给 SNMP 实体的消息总数。
Bad SNMP version errors	发送给 SNMP 协议实体且适合于不受支持的 SNMP 版本的 SNMP 消息总数。
Unknown community name	向 SNMP 协议实体 （该实体使用指定实体所不知的 SNMP 社区名称）发送的 SNMP 消息总数。
Illegal operation for community name supplied	向以下这种 SNMP 协议实体发送的 SNMP 消息总数：该 SNMP 协议实体代表一种 SNMP 操作，而在消息中指定的 SNMP 社区不允许执行这一操作。
Encoding errors	SNMP 协议实体在对收到的 SNMP 消息进行编码时，所遇到的 ASN.1 错误或 BER 错误的总数。
Number of requested variables	SNMP 协议实体由于收到有效的 SNMP Get-Request PDU 或 Get-Next PDU 而成功检索到的 MIB 对象的总数。
Number of altered variables	SNMP 协议实体由于收到有效的 SNMP Set-Request PDU 而成功修改的 MIB 对象的总数。
Get-request PDUs	SNMP 协议实体已接受和处理的 SNMP Get-Request PDU 的总数。
Get-next PDUs	SNMP 协议实体已接受和处理的 SNMP Get-Next PDU 的总数。
Set-request PDUs	SNMP 协议实体已接受和处理的 SNMP Set-Request PDU 的总数。

参数	说明
SNMP packets output	
SNMP packets output	从 SNMP 协议实体向传输服务传送的 SNMP 消息总数。
Too big errors	向错误状态为 “tooBig” 的 SNMP 协议实体发送的 SNMP PDU 的总数。
No such name errors	向错误状态为 “noSuchName” 的 SNMP 协议实体发送的 SNMP PDU 的总数。
Bad values errors	向错误状态为 “badValue” 的 SNMP 协议实体发送的 SNMP PDU 的总数。
General errors	向错误状态为 “genErr” 的 SNMP 协议实体发送的 SNMP PDU 的总数。
Response PDUs	SNMP 协议实体已生成的 SNMP Get-Response PDU 的总数。
Trap PDUs	SNMP 协议实体已生成的 SNMP Trap PDU 的总数。

Web — 单击 “Monitoring” => “SNMP Statistics”。您还可以使用位于页面底部的 “Refresh” 按钮来更新屏幕。



CLI — 本示例显示交换机的 SNMP 统计信息。

```
Console#show snmp                                                    4-52

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read/write
   2. public, and the privilege is read-only

11 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    8 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    1 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    3 Set-request PDUs
11 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    2 General errors
    3 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	范围
SNMP packets input			
In Packets	MIB-II.snmp.snmpInPkts	只读	整数
In Bad Versions	MIB-II.snmp.snmpInBadVersions	只读	整数
In Bad Community Names	MIB-II.snmp.snmpInBadCommunityNames	只读	整数
In Bad Community Uses	MIB-II.snmp.snmpInBadCommunityUses	只读	整数
In ASN Parse Errors	MIB-II.snmp.snmpInASNParseErrs	只读	整数
In Total Request Variables	MIB-II.snmp.snmpInTotalReqVars	只读	整数
In Total Set Variables	MIB-II.snmp.snmpInTotalSetVars	只读	整数
In Get Requests	MIB-II.snmp.snmpInGetRequests	只读	整数
In Get Nexts	MIB-II.snmp.snmpInGetNexts	只读	整数
In Set Requests	MIB-II.snmp.snmpInSetRequests	只读	整数
Silent Drops	MIB-II.snmp.snmpSilentDrops	只读	整数
Proxy Drops	MIB-II.snmp.snmpProxyDrops	只读	整数
SNMP packets output			
Out Packets	MIB-II.snmp.snmpOutPkts	只读	整数
Out Too Bigs	MIB-II.snmp.snmpOutTooBigs	只读	整数
Out No Such Names	MIB-II.snmp.snmpOutNoSuchNames	只读	整数
Out Bad Values	MIB-II.snmp.snmpOutBadValues	只读	整数
Out General Errors	MIB-II.snmp.snmpOutGenErrs	只读	整数
Out Get Responses	MIB-II.snmp.snmpOutGetResponses	只读	整数
Out Traps	MIB-II.snmp.snmpOutTraps	只读	整数

3.5.4 配置消息日志

可以根据严重性，限制保存到交换机内存中的系统日志消息。

命令属性

- **Enable Logging** — 启用将调试消息或错误消息记录到交换机内存中。（默认值：Disabled）
- **Logging Level** — 根据严重性，限制保存到交换机内存中的系统日志消息。请注意，所保存的消息包括所选的级别到 0 级。（范围：7-0 ；默认值 — 闪存：3-0，RAM：7-0）

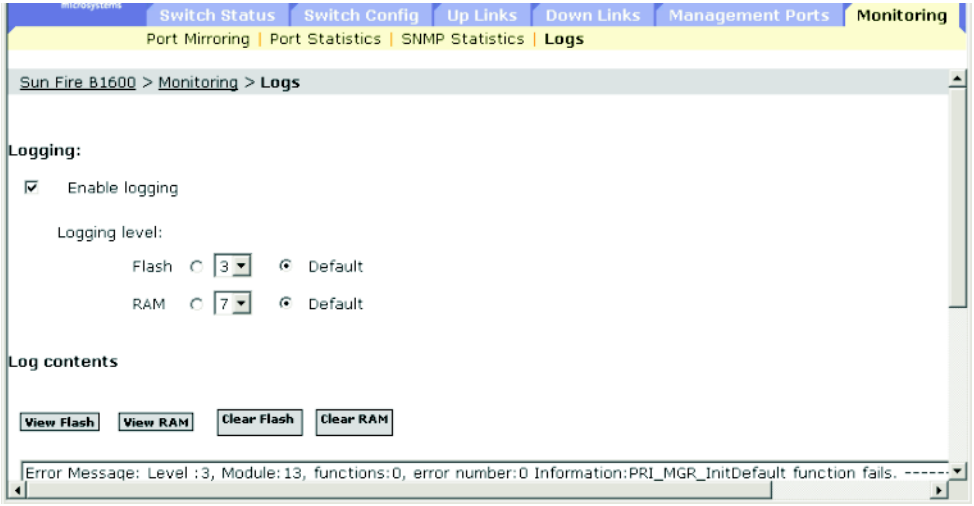
表 3-1 错误级别

级别参数	级别	说明
debugging	7	调试消息
informational	6	只供参考的消息 （即所有陷阱）
notifications	5	正常但比较重要的情况，如冷启动
warnings	4	警告情况 （如返回 false 值，异常返回）
errors	3	错误情况 （如无效输入、使用了默认值）
critical	2	严重情况 （如内存分配或可用内存不足错误 — 资源已耗尽）
alerts	1*	需要立即采取措施
emergencies	0*	系统无法使用

* 当前的固件版本尚无级别 0 或级别 1 的错误消息。

- **Log contents** — 包含允许您执行以下这些操作的按钮：列出闪存或 RAM 中存储的任何系统消息和事件消息；清除闪存 （即系统重新引导后仍会保留的非易失性内存）或 RAM （即系统重新引导后将丢失的随机存取内存）中的日志消息。

Web — 单击 “Monitoring” => “Logs”。选中 “Enable logging”，单击 “Flash” 或 “RAM”，选择要记录的消息级别 （即包括所选的级别到 0 级），然后单击 “Save Changes”。单击 “View Flash” 或 “View RAM” 可以更新所显示的消息。



CLI — 本示例启用日志记录，并将闪存中所记录的消息的级别设置为 3 （即 “errors”），然后显示闪存中所存储的日志消息。

```
Console(config)#logging on                                    4-30
Console(config)#logging history flash 3                       4-31
Console#show logging flash                                    4-33
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level:3, module:13, function:0, and event no.: 0
Console#
```

SNMP — 等效 MIB 变量。

字段名	MIB 变量	访问权限	值范围	默认值
Log Status	sun... sysLogMgt. sysLogStatus	读 / 写	enabled (1), disabled (2)	
History Flash Level	sun... sysLogMgt. sysLogStatus.sysLog.HistoryFlashLevel	读 / 写	整数 (0-7)	
History RAM Level	sun... sysLogMgt. sysLogStatus.sysLog.HistoryRAMLevel	读 / 写	整数 (0-7)	
日志消息	*未定义*。			

第 4 章

命令行参考

本章介绍如何使用命令行界面 (CLI)。

4.1 使用命令行界面

4.1.1 访问 CLI

当通过到服务器控制台端口的直接连接或通过 Telnet 连接访问交换机的管理界面时，可通过在提示符后输入命令关键字和参数来管理交换机。使用交换机的命令行界面 (CLI) 与在 UNIX 系统上输入命令非常类似。

4.1.1.1 控制台连接

要通过控制台端口访问交换机，可执行以下步骤：

1. 在控制台提示符后，输入用户名和口令。（默认的用户名是 “admin” 和 “guest”，它们对应的口令分别为 “admin” 和 “guest”。）输入 “admin” 用户名和口令后，CLI 将显示 “Console#” 提示符并进入特权访问模式 （即 “特权执行” 模式）。但当输入 “guest” 用户名和口令后， CLI 将显示 “Console>” 提示符并进入普通访问模式 （即 “普通执行” 模式）。
2. 输入必要的命令完成所需执行的任务。
3. 完成后，使用 “quit” 或 “exit” 命令退出会话。

通过控制台端口连接到系统之后，将显示如下登录屏幕：

```
User Access Verification

Username:admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

4.1.1.2 Telnet 连接

Telnet 以 IP 传输协议为基础运行。在这种环境下，您的管理站和以及您要通过网络进行管理的任何网络设备都必须有一个有效的 IP 地址。有效的 IP 地址由四组用句点分隔的数字组成，数字范围从 0 到 255。每个地址都由网络部分和主机部分组成。例如， IP 地址 10.1.0.1 就由网络部分 (10.1.0) 和主机部分 (1) 组成。

注：默认情况下，并没有为交换机分配 IP 地址。管理端口 (NETMGT) 分配给了 VLAN 2。不能将该端口分配给包含上行链接端口或下行链接端口的 VLAN。

要通过 Telnet 会话访问交换机，必须先为交换机设置 IP 地址；如果要通过其它 IP 子网管理交换机，则还需要设置默认网关。例如，

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

如果您的公司网络与办公室之外的另一个网络或者与 Internet 建立了连接，则需要申请一个已注册的 IP 地址。不过，如果您的网络连接的是一个孤立的网络，则可以使用符合您公司网络策略的任何 IP 地址。

在为交换机配置了 IP 地址之后，可通过执行以下步骤打开一个 Telnet 会话：

1. 如果位于远程主机，则输入 Telnet 命令以及您所要访问的设备的 IP 地址。
2. 出现提示符后，输入用户名和系统口令。对于具有 admin 权限的用户， CLI 将显示“Vty-0#”提示符，表明使用的是特权访问模式（即“特权执行”模式）；对于具有 guest 权限的用户，则显示“Vty-0>”提示符，表明使用的是普通访问模式（即“普通执行”模式）。
3. 输入必要的命令完成所需执行的任务。
4. 完成后，使用“quit”或“exit”命令退出会话。

输入 Telnet 命令后，将显示如下登录屏幕：

```
Username:admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

注：通过 Telnet 可以打开多达四个指向设备的会话。

4.1.2 输入命令

本节介绍如何输入 CLI 命令。

4.1.2.1 关键字和参数

CLI 命令是一系列关键字和参数。关键字标识命令，参数则指定配置参数。例如，在命令“show interfaces status ethernet SNP5”之中， **show interfaces** 和 **status** 是关键字，而 **ethernet** 是一个参数，指定了接口类型，参数 **SNP5** 则指定了端口。

可以按照如下方式输入命令：

- 要输入一条简单命令，输入命令关键字即可。
- 要输入多条命令，可按要求的顺序逐条输入命令。例如，要启用“特权执行”命令模式，并显示启动配置，可输入：

```
Console>enable
Console#show startup-config
```

- 要输入要求参数的命令，请在命令的关键字之后输入所需参数。例如，要设置管理员的口令，可输入：

```
Console(config)#username admin password 0 smith
```

4.1.2.2 最短缩写

CLI 将接受能够唯一标识出命令的最少字符数。例如，可输入 **logging h** 表示“logging history”命令。如果输入的命令不太明确，系统将提示进行进一步的输入。

4.1.2.3 命令完成

如果您按 Tab 键表示命令输入完毕，但 CLI 无法准确判断所输入的部分关键字的含义，那么它将会显示出关键字的其余字符供您确认。再次以“logging history”为例，如果在键入 **log** 之后再按 Tab 键，将使 CLI 显示出命令“**logging**”。

4.1.2.4 获取命令的帮助

输入 **help** 命令可以显示帮助系统的简短说明。通过使用“?”字符列出关键字或参数，也可以显示命令的语法。

4.1.2.5 显示命令

如果在命令提示符后输入 “?”，系统将显示当前命令类别 （普通执行或特权执行）或配置类别 （全局、接口、线路或 VLAN 数据库）的第一级关键字。也可以显示特定命令的有效关键字列表。例如，命令 “**show ?**”将列出一些可能使用的显示命令：

```
Console#show ?
  bridge-ext          Bridge extend information
  garp                Garp property
  gvrp                Show gvrp information of interface
  history             Information of history
  interfaces          Information of interfaces
  ip                  Ip
  line                TTY line information
  logging             Show the contents of logging buffers
  mac-address-table   Set configuration of the address table
  map                 Map priority
  port                Characteristics of the port
  queue               Information of priority queue
  radius-server       Radius server information
  running-config      The system configuration of running
  snmp                SNMP statistics
  spanning-tree       Specify spanning-tree
  startup-config      The system configuration of starting up
  system              Information of system
  tacacs-server       Login by tacacs server
  users               Display information about terminal lines
  version             System hardware and software status
  vlan                Switch VLAN Virtual Interface
Console#show
```

命令 “show interfaces ?”将显示以下信息：

```
Console>show interfaces ?
  counters    Information of interfaces counters
  status      Information of interfaces status
  switchport  Information of interfaces switchport
```

4.1.2.6 查找部分关键字

如果在输入部分关键字后再输入一个问号，则系统会显示匹配最初几个字母的备选关键字。（谨记，请勿在命令和问号之间留空格。）例如，“s?”将显示所有以 “s”开头的关键字。

```
Console#show s?
snmp            spanning-tree   startup-config  system
```

4.1.2.7 取消命令的效果

对于许多配置命令，可以输入前缀关键字 “**no**”来取消命令的效果或将配置重置为默认值。例如， **logging** 命令将把系统消息记录到主机服务器上。要禁用日志记录功能，可指定 **no logging** 命令。本指南介绍了所有适用命令的效果取消情况。

4.1.2.8 使用命令历史记录

CLI 对已输入的命令保留历史记录。按住向上箭头键，可以回滚查看命令的历史记录。历史记录列表中显示的所有命令都可以再次执行，或经过修改后再执行。

使用 **show history** 命令可以列出最近执行过的命令，该列表将更长。

4.1.2.9 了解命令模式

命令集被分为 “执行”和 “配置”两类。执行命令通常显示有关系统状态的信息，或清除统计信息计数器。配置命令则修改接口参数或启用某些交换功能。这两类又可细分为各种模式。可使用的命令因选定的模式而异。始终可以在提示符后输入问号 “?”，以让屏幕显示当前模式下可用命令的列表。下表显示了两种命令类别以及相关模式：

类别	模式
执行	普通
	特权
配置 *	全局
	接口
	线路
	VLAN 数据库

* 必须在 “特权执行”模式下才能访问所有的配置模式。

4.1.2.10 执行命令

使用用户名和口令“guest”打开交换机上的一个新控制台会话后，系统将进入“普通执行”命令模式（或 guest 模式），同时显示“Console>”命令提示符。在这种模式下可用的命令数量有限。要访问所有命令，只能通过“特权执行”命令模式（或 admin 模式）。要访问“特权执行”模式，必须使用用户名和口令“admin”打开一个新控制台会话。此时，系统将显示“Console#”命令提示符。也可以从“普通执行”模式进入“特权执行”模式，方法是输入 **enable** 命令，接着再输入特权级别口令“super”（请参阅第 4-27 页）。

要进入“特权执行”模式，请输入以下用户名和口令：

```
Username: admin
Password: [admin login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

4.1.2.11 配置命令

配置命令是用于修改交换机设置的特权级别命令。这些命令只修改正在运行的配置，当重新引导交换机时并不会保存这些配置。要将正在运行的配置存储在非易失性存储区中，可使用 **copy running-config startup-config** 命令。

配置命令分为以下几种模式：

- 全局配置 — 这些命令修改系统级配置，包括 **hostname** 和 **snmp-server community** 等命令。
- 接口配置 — 这些命令修改端口配置，如 **speed-duplex** 和 **negotiation** 等命令。

- 线路配置 — 这些命令修改控制台端口的配置以及 Telnet 配置，包括 **exec-timeout** 和 **silent-time** 等命令。
- VLAN 配置 — 包括用于创建 VLAN 组的命令。

要进入 “全局配置”模式，可在 “特权执行”模式下输入命令 **configure**。系统提示符将变为 “Console(config)#”，然后您就可以访问所有的 “全局配置”命令。

```
Console#configure
Console(config)#
```

要进入其它模式，可在配置提示符后键入以下命令之一。使用 **exit** 命令返回到 “配置”模式，或输入 **end** 命令返回到 “特权执行”模式。

模式	命令	提示符	参阅页码
接口模式	interface {ethernet *port* | port-channel *id* | vlan *id*}	Console(config-if)#	4-74
线路模式	line {console | vty}	Console(config-line)#	4-55
VLAN 模式	vlan database	Console(config-vlan)	4-105

例如，可以使用以下命令进入接口配置模式，然后再返回 “特权执行”模式。

```
Console(config)#interface ethernet SNP5
.
.
.
Console(config-if)#exit
Console(config)
```

4.1.2.12 处理命令行

命令不区分大小写。可以输入命令和参数的缩写形式，只要它们能与当前可用的其它命令或参数区分开来即可。输入部分命令后可按 Tab 键表示完成了命令的输入，或在输入部分命令后再输入字符 “?”，以显示可能匹配的命令列表。也可以将以下编辑按键用于命令行处理：

按键	功能
Ctrl-A	将光标移到命令行开始处。
Ctrl-B	将光标向左移动一个字符。
Ctrl-E	将光标移到命令行结尾。
Ctrl-F	将光标向右移动一个字符。
Ctrl-P	显示最后那条命令。
Ctrl-U	删除整行。
Ctrl-W	删除最后所键入的单词。
Delete 键或退格键	输入命令时擦除错误。

4.2 命令组

系统命令可细分为如下显示的几个功能组。

命令组	说明	页码
常规	一些基本命令，用于进入 “特权访问”模式、重新启动系统或退出 CLI	4-11
闪存 / 文件	管理代码映像或交换机配置文件	4-17
系统管理	控制系统日志、系统口令、用户名、浏览器管理选项和各种其它系统信息	4-24
验证	使用本地方法、 RADIUS 方法或 TACACS 方法配置对登录权限的验证	4-41
SNMP	激活验证故障陷阱；配置社区访问字符串和陷阱管理器	4-48
线路	设置串行端口和 Telnet 的连接选项，包括口令检查、线路口令和控制台超时时间	4-54
IP 命令	配置 IP 地址和网关以进行管理访问、显示默认网关或对指定设备进行 ping 操作	4-62
接口	配置所有以太网端口、聚合链接和 VLAN 的连接参数	4-73
地址表	配置地址表，以过滤指定地址、显示当前条目、清除地址表或设置有效时间	4-86
端口安全性	为端口的配置全地址	4-90
生成树	为交换机配置生成树设置	4-92
VLAN	配置 VLAN 设置，并定义 VLAN 组的端口成员资格	4-104
GVRP 和网桥扩展	配置允许 VLAN 自动了解的 GVRP 设置；显示网桥扩展 MIB 的配置	4-113
IGMP 侦听	配置 IGMP 多点传送过滤、查询器合格性、查询参数，并指定连接到多点传送路由器的端口	4-119
优先级	为不带标记的帧设置端口优先级、每个优先级队列的相对加权以及所启用队列的最大数量；还可为 IP 优先权和 DSCP 设置优先级	4-129
镜像端口	将数据镜像到另一个端口，以便在不影响数据传输或所镜像端口性能的情况下进行数据分析	4-140
端口聚合和 LACP	将多个端口静态地分入一个逻辑聚合组中；为端口聚合组配置 “链路聚合控制协议”	4-142

后面的表中所显示的访问模式由以下缩写词表示：

NE（普通执行）
PE（特权执行）
GC（全局配置）
IE（接口配置）
LC（线路配置）
VC（VLAN 数据库配置）

4.3 详细的命令说明

4.3.1 常规命令

命令	功能	模式	页码
enable	激活特权模式	NE	4-12
disable	从特权模式返回到普通模式	PE	4-13
configure	激活全局配置模式	PE	4-13
show history	显示命令历史记录缓冲区	NE、PE	4-14
reload	重新启动系统	PE	4-15
end	返回到“特权执行”模式	GC、IC、LC、VC	4-15
exit	返回到以前的配置模式，或退出 CLI	任何模式	4-16
quit	退出 CLI 会话	NE、PE	4-16
help	显示如何使用帮助	任何模式	NA
?	显示用于完成命令的选项（与上下文相关）	任何模式	NA

4.3.1.1 enable

使用此命令可以激活 “特权执行”模式。在 “特权执行”模式下，可使用更多的命令，而且某些命令还将显示更多的信息。请参阅第 4-6 页上的 “了解命令模式”。

语法

enable [*level*]

level — 登录到设备时所使用的权限级别。
设备有两种权限级别：0：普通执行， 15：特权执行。输入级别 15 可以访问 “特权执行”模式。

默认设置

级别 15

命令模式

普通执行

命令用法

- 如果要将命令模式从 “普通执行”改为 “特权执行”，则必须使用 “super”默认口令。（要设置此口令，请参阅第 4-27 页上的 **enable password** 命令。）
- 提示符结尾处附加了一个字符 “#”，表明系统处于 “特权访问”模式下。

示例

```
Console>enable
Password: [privileged level password]
Console#
```

相关命令

disable (4-13)
enable password (4-27)

4.3.1.2 disable

使用此命令可以从 “特权执行”模式返回到 “普通执行”模式。在普通访问模式下，只能显示有关交换机配置或以太网统计信息的基本信息。要获取对所有命令的访问权限，必须使用特权模式。请参阅第 4-6 页上的 “了解命令模式”。

默认设置

无

命令模式

特权执行

命令用法

提示符结尾处附加了一个 “>”字符，表明系统处于普通访问模式下。

示例

```
Console#disable
Console>
```

相关命令

enable (4-12)

4.3.1.3 configure

使用此命令可以激活 “全局配置”模式。必须进入此模式才能修改交换机上的任何设置。要想能够启用某些其它配置模式 （包括接口配置、线路配置或 VLAN 数据库配置），也必须进入 “全局配置”模式。请参阅第 4-6 页上的 “了解命令模式”。

默认设置

无

命令模式

特权执行

示例

```
Console#configure
Console(config)#
```

相关命令

end (4-15)

4.3.1.4 show history

使用此命令可以显示命令历史记录缓冲区中的内容。

默认设置

无

命令模式

普通执行、特权执行

命令用法

历史记录缓冲区的空间是固定的，只能存储 10 条执行命令和 10 条配置命令。

示例

在此例中， show history 命令列出了命令历史记录缓冲区中的内容：

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

当处于 “普通执行”模式或 “特权执行”模式下时， **!** 命令重复执行 “Execution” 命令历史记录缓冲区中的命令；当处于任何配置模式下时，该命令将重复执行 “Configuration”命令历史记录缓冲区中的命令。在此例中， **!2** 命令重复执行 “Execution”历史记录缓冲区中的第二条命令 (**config**)。

```
Console#!2
Console#config
Console(config)#
```

4.3.1.5 reload

使用此命令可以重新启动系统。

注：系统重新启动时，它始终会运行开电自检功能。系统还将保留 **copy running-config startup-config** 命令存储在非易失性存储区中的所有配置信息。

默认设置

无

命令模式

特权执行

命令用法

此命令将重置整个系统。

示例

以下示例说明如何重置交换机：

```
Console#reload
System will be restarted, continue <y/n>? y
```

4.3.1.6 end

使用此命令可以返回到 “特权执行”模式。

默认设置

无

命令模式

全局配置、接口配置、线路配置、 VLAN 数据库配置、路由器配置

示例

以下示例显示如何从 “接口配置”模式返回到 “特权执行”模式：

```
Console(config-if)#end
Console#
```

4.3.1.7 exit

使用此命令可以返回到以前的配置模式或退出配置程序。

默认设置

无

命令模式

任何模式

示例

以下示例说明如何从 “全局配置” 模式返回到 “特权执行” 模式，然后再退出 CLI 会话：

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

4.3.1.8 quit

使用此命令可以退出 CLI 会话。

默认设置

无

命令模式

普通执行、特权执行

命令用法

使用 **quit** 命令和 **exit** 命令都可以退出配置程序。

示例

以下示例说明如何退出 CLI 会话：

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

4.3.2 闪存 / 文件命令

这些命令用于管理系统代码文件或配置文件。

命令	功能	模式	页码
copy	自闪存或 TFTP 服务器中复制代码映像或交换机配置，或将代码映像或交换机配置复制到其中	PE	4-17
delete	删除文件或代码映像	PE	4-20
dir	显示闪存中的文件列表	PE	4-20
whichboot	显示所引导的文件	PE	4-22
boot system	指定用于启动系统的文件或映像	GC	4-23

4.3.2.1 copy

使用此命令可以在交换机的闪存和 TFTP 服务器之间移动 （上传 / 下载）代码映像或配置文件。将系统代码或配置设置保存到 TFTP 服务器上的某个文件之后，可以将该文件下载到交换机以便恢复系统操作。文件转移成功与否取决于 TFTP 服务器是否可供访问以及网络连接的质量。

语法

copy file {file | running-config | startup-config | tftp}
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config}
copy tftp https-certificate

- **file** — 关键字 （允许您从文件中进行复制或将内容复制到文件）。
- **running-config** — 关键字 （允许对当前运行的配置来回进行复制）。
- **startup-config** — 用于系统初始化的配置。
- **tftp** — 关键字 （允许对 TFTP 服务器中的内容来回进行复制）。
- **https-certificate** — 此选项用于指定公认的验证授权机构所提供的证书、私钥和口令。

默认设置

无

命令模式

特权执行

命令用法

- 系统会提示输入所需数据以完成 copy 命令。
- 目标配置文件名中不应包含斜杠（\ 或 /）；文件名的前导字符不应是句点 (.)；在 TFTP 服务器上该文件名的最大长度是 127 个字符，而在交换机上该文件名的最大长度是 32 个字符。（有效字符包括：A-Z、 a-z、 0-9、“.”、“-”、“_”）
- 由于闪存的空间有限，交换机只支持存储两个操作代码文件。
- 用户定义的配置文件最大数量取决于可用内存的大小。
- 可以从 “Factory_Default_Config.cfg” 中复制出厂默认配置文件，但不能将出厂默认配置文件复制到其中。
- 要更换启动配置，可以将 **startup-config** 当作目标。
- 引导 ROM 和加载器代码不能上传到 TFTP 服务器中，也不能从该服务器下载。如果要更改引导 ROM 或加载器代码，应由 Sun 服务工程师来执行。

示例

以下示例说明如何将配置设置上传到 TFTP 服务器的某个文件中：

```
Console#copy file tftp
Choose file type:
 1. config: 2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

以下示例说明如何将正在运行的配置复制到文件中。

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

以下示例说明如何下载配置文件：

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

以下示例说明如何在 TFTP 服务器上存储安全站点证书。然后，它重新引导交换机来激活该证书。

```
Console#copy tftp https-certificate

       TFTP server ip address: 10.1.0.19
       Source certificate file name: SS-certificate

       Source private file name: SS-private
       Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

4.3.2.2 delete

使用此命令可以删除文件或映像。

语法

delete *filename*

filename — 配置文件名或映像名称。

默认设置

无

命令模式

特权执行

命令用法

- 如果文件类型为引导 ROM，或者该文件用于启动系统，则不能删除该文件。
- 不能删除文件 “Factory_Default_Config.cfg”。

示例

以下示例说明如何从闪存中删除 test2.cfg 配置文件。

```
Console#delete test2.cfg
Console#
```

相关命令

dir (4-20)

4.3.2.3 dir

使用此命令可显示闪存中的文件列表。

语法

dir [**boot-rom** | **config** | **opcode** [**:***filename*]]

所显示的文件类型或映像类型包括：

- **boot-rom** — 引导 ROM
- **config** — 配置文件
- **opcode** — 运行时操作代码。
- *filename* — 要显示的文件名或映像名称。如果此文件已存在但有错误，则无法显示有关此文件的信息。

默认设置

无

命令模式

特权执行

命令用法

- 如果输入命令 **dir** 但不任何带参数，系统将显示所有文件。
- 文件信息显示如下：

表 4-1 文件信息

列标题	说明
file name	文件的名称。
file type	文件类型：引导 Rom、操作代码和配置文件。
startup	显示系统启动时是否使用此文件。
size	文件的长度 （按字节计）。

示例

以下示例说明如何显示所有文件信息：

```
Console#dir
                        file name      file type startup size (byte)
------------------------------- -------------- ------- -----------
                        diag_0060 Boot-Rom image       Y      111360
                        run_01642 Operation Code       N     1074304
                         run_0200 Operation Code       Y     1083008
      Factory_Default_Config.cfg    Config File       N        2574
                          startup    Config File       Y        2710
-----------------------------------------------------------------------
                                        Total free space:         0
Console#
```

4.3.2.4 whichboot

使用此命令可以显示当系统通电后会引导哪些文件。

默认设置

无

命令模式

特权执行

命令用法

有关对使用此命令后所显示的文件信息的说明，请参阅表 4-1。

示例

以下示例说明 **whichboot** 命令所显示的信息

```
Console#whichboot
        file name      file type startup size (byte)
----------------- -------------- ------- -----------
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

4.3.2.5 boot system

使用此命令可以指定用于启动系统的文件或映像。

语法

boot system {**boot-rom**| **config** | **opcode**}: *filename*

要设置为默认值的文件类型或映像类型包括：

- **boot-rom** — 引导 ROM
- **config** — 配置文件
- **opcode** — 运行时操作代码

要求使用冒号 (:)。

filename — 配置文件名或映像名称。

默认设置

无

命令模式

全局配置

命令用法

- 指定的文件类型之后要求使用冒号 (:)。
- 如果该文件有错，则不能将它设置为默认文件。

示例

```
Console(config)#boot system config:startup
Console(config)#
```

相关命令

dir (4-20)
whichboot (4-22)

4.3.3 系统管理命令

这些命令用于控制系统日志、口令、用户名、浏览器配置选项，以及显示或配置各种其它系统信息。

命令	功能	模式	页码
设备说明命令			
hostname	指定或修改设备的主机名	GC	4-25
用户访问命令			
username	登录时建立基于用户名的验证系统	GC	4-26
enable password	设置口令，用于控制对 “特权执行”级别的访问	GC	4-27
Web 服务器命令			
ip http port	指定 Web 浏览器接口所使用的端口	GC	4-28
ip http server	允许通过浏览器来监视或配置交换机	GC	4-28
超长帧命令			
jumbo-frame	启用对超长帧的支持	GC	4-29
事件记录命令			
logging on	控制对错误消息的记录	GC	4-30
logging history	根据严重程度来限制保存到交换机内存中的系统日志消息	GC	4-31
clear logging	清除日志记录缓冲区中的消息	PE	4-32
show logging	显示日志记录的状态	PE	4-33

命令	功能	模式	页码
系统状态命令			
show startup-config	显示用于启动系统的配置文件 （存储在闪存中）的内容	PE	4-34
show running-config	显示当前正在使用的配置数据	PE	4-36
show system	显示系统信息	NE、PE	4-38
show users	显示所有活动的控制台会话和 Telnet 会话，包括 Telnet 客户机的用户名、闲置时间和 IP 地址	NE、PE	4-39
show version	显示系统的版本信息	NE、PE	4-40

4.3.3.1 hostname

使用此命令可以指定或修改设备的主机名。使用此命令的 **no** 形式可以恢复默认主机名。

语法

hostname *name*
no hostname

name — 主机的名称。（最大长度：255 个字符）

默认设置

无

命令模式

全局配置

示例

```
Console(config)#hostname Server_Chassis_35
Console(config)#
```

4.3.3.2 username

使用此命令可以添加指定的用户、要求在登录时进行验证、指定或更改用户口令（或指定不需要使用口令），或指定或更改用户的访问级别。使用此命令的 **no** 形式可以删除用户名。

语法

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}
no username *name*

- *name* — 用户的名称。
  （最大长度：8 个字符；最大用户数：5）
- **access-level** *level* — 指定用户级别。
  设备有两个预定义的权限级别：**0**：普通执行； **15**：特权执行。（不使用级别 1-14。）
- **nopassword** — 用户登录不需要使用口令。
- {**0** | **7**} — 0 表示输入纯文本口令， 7 表示输入加密口令。
- **password** *password* — 用户的验证口令。
  （最大长度：纯文本口令为 8 个字符，加密口令为 32 个字符，且口令区分大小写）

默认设置

- 默认的访问级别是 “普通执行”。
- “普通执行”模式下的默认口令为 “guest”，而 “特权执行”模式下的默认口令为 “admin”。

用户名和口令的出厂默认值为：

表 4-2 默认的用户名和口令

用户名	访问级别	口令
guest	0	guest
admin	15	admin

命令模式

全局配置

命令用法

无须在命令行上指定加密口令。交换机进行系统引导时对内部使用了选项 7，从而使交换机能够读取存储在配置文件中的任何加密口令。

示例

以下示例说明如何为用户设置访问级别和口令。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

4.3.3.3 enable password

最初登录到系统之后，应该设置 “特权执行”级别的口令。谨记，应将口令放在安全的地方保管。使用此命令可以控制能否从 “普通执行”级别转到 “特权执行”级别。使用此命令的 **no** 形式可以重置默认口令。

语法

enable password [level *level*] {**0** | **7**} *password*
no enable password [level *level*]

- **level** *level* — 对于“特权执行”模式，使用的级别为 **15**。（不使用级别 0-14。）
- {**0** | **7**} — 0 表示输入纯文本口令， 7 表示输入加密口令。
- *password* — 此权限级别的口令。
  （最大长度：纯文本口令为 8 个字符，加密口令为 32 个字符，且口令区分大小写）

默认设置

- 默认值为级别 15。
- 默认口令为 “super”

命令模式

全局配置

命令用法

- 不能设置空口令。要使用 **enable** 命令将命令模式从 “普通执行”改为 “特权执行”，必须输入口令 （第 4-12 页）。
- 无须在命令行上指定加密口令。交换机进行系统引导时对内部使用了选项 7，从而使交换机能够读取存储在配置文件中的任何加密口令。

示例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

相关命令

enable (4-12)

4.3.3.4 ip http port

使用此命令可以指定 Web 浏览器接口所使用的 TCP 端口号。使用此命令的 **no** 形式可使用默认端口。

语法

ip http port *port-number*
no ip http port

port-number — 浏览器接口所要使用的 TCP 端口。（范围：1-65535）

默认设置

80

命令模式

全局配置

示例

```
Console(config)#ip http port 769
Console(config)#
```

相关命令

ip http server (4-28)

4.3.3.5 ip http server

如果使用此命令，则允许通过浏览器来监视或配置设备。使用此命令的 **no** 形式可禁用此功能。

语法

ip http server
no ip http server

默认设置

启用

命令模式

全局配置

示例

```
Console(config)#ip http server
Console(config)#
```

相关命令

ip http port (4-28)

4.3.3.6 jumbo-frame

使用此命令可启用对超长帧的支持。使用此命令的 **no** 形式可禁用它。

语法

jumbo-frame
no jumbo-frame

默认设置

禁用

命令模式

全局配置

命令用法

- 本交换机支持长达 9000 字节的超长帧，从而能够更有效地进行大型的连续数据传输 （即吞吐量更大）。与最大字节数仅达 1.5 KB 的标准以太网帧相比，使用超长帧可以显著降低处理各个数据包的协议封装字段时所需的开销。
- 要使用超长帧，源末端节点和目标末端节点 （如计算机或服务器）必须支持该功能。此外，当连接以全双工模式操作时，网络中处于两个末端节点之间的所有交换机都必须能够接受扩展的帧大小。对于半双工连接，冲突域中的所有设备都将需要支持超长帧。
- 通过启用超长帧，可将广播风暴控制的最大阈值限制为每秒传递 64 个数据包。（请参阅第 4-80 页上的 **switchport broadcast** 命令。）

示例

```
Console(config)#jumbo-frame
Console(config)#
```

4.3.3.7 logging on

使用此命令可以控制错误消息的记录情况。此命令会将调试消息或错误消息发送到交换机内存中。使用此命令的 **no** 形式可禁用记录进程。

语法

logging on
no logging on

默认设置

无

命令模式

全局配置

命令用法

记录进程控制着保存到交换机内存的错误消息。可以使用 **logging history** 命令来控制所存储的错误消息类型。

示例

```
Console(config)#logging on
Console(config)#
```

相关命令

logging history (4-31)
clear logging (4-32)

4.3.3.8 logging history

通过使用此命令，可根据严重程度来限制保存到交换机内存中的系统日志消息。使用此命令的 **no** 形式可将系统日志消息的记录级别返回到默认级别。

语法

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** — 存储在闪存 （即永久性内存）中的事件历史记录。
- **ram** — 存储在临时 RAM （即，其中的内容会在电源重置时被删除掉的存储器）中的事件历史记录。
- *level* — 0-7 （所保存的消息包括所选的级别到 0 级。）

表 4-3 错误级别

级别参数	级别	说明
debugging	7	调试消息
informational	6	仅仅是说明性消息
notifications	5	正常但比较重要的情况，如冷启动
warnings	4	警告情况 （如返回 false 值，异常返回）
errors	3	错误情况 （如无效输入、使用了默认值）
critical	2	严重情况 （如内存分配或可用内存不足错误 — 资源已耗尽）
alerts	1	需要立即采取措施
emergencies	0	系统无法使用

* 当前的固件版本尚无级别 0 或级别 1 的错误消息。

默认设置

闪存：错误 （级别 3 — 级别 0）
RAM：警告 （级别 7 — 级别 0）

命令模式

全局配置

命令用法

与 RAM 相比，为闪存指定的消息级别必须具有更高的优先级。即，为闪存指定的消息级别所对应的数字应更小。

示例

```
Console(config)#logging history ram 0
Console(config)#
```

4.3.3.9 clear logging

使用此命令可以清除日志缓冲区中的消息。

语法

clear logging [flash | ram]

- **flash** — 存储在闪存（即永久性内存）中的事件历史记录。
- **ram** — 存储在临时 RAM（即，其中的内容会在电源重置时被删除掉的存储器）中的事件历史记录。

默认设置

闪存和 RAM

命令模式

特权执行

示例

```
Console#clear logging
Console#
```

相关命令

show logging (4-33)

4.3.3.10 show logging

使用此命令可以显示当前的日志记录配置，以及存储在内存中的所有系统消息和事件消息。

语法

show logging {**flash** | **ram**}

- **flash** — 存储在闪存 （即永久性内存）中的事件历史记录。
- **ram** — 存储在临时 RAM （即，其中的内容会在电源重置时被删除掉的存储器）中的事件历史记录。

默认设置

无

命令模式

特权执行

命令用法

此命令将显示以下信息：

- `Syslog logging` — 是否已通过 **logging on** 命令启用系统日志记录功能。
- `History logging in FLASH/RAM` — 根据 **logging history** 命令而报告的消息级别。
- 存储在内存中的所有系统消息和事件消息。

示例

以下示例表明：系统日志记录功能已启用、闪存的消息级别为 “error”（即默认级别 3 - 级别 0）、 RAM 的消息级别为 “debugging”（即默认级别 7 - 级别 0）。该示例还列出了一个错误示例。

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1
   "PRI_MGR_InitDefault function fails."
   level: 3, module: 13, function: 0, and event no.: 0
Console#
```

相关命令

logging on (4-30)
logging history (4-31)

4.3.3.11 show startup-config

使用此命令可以显示用于启动系统且存储在非易失性存储区中的配置文件。

默认设置

无

命令模式

特权执行

命令用法

- 如果将此命令与 **show running-config** 命令结合使用，则可以将存储在运行的内存中的信息与存储在非易失性存储区中的信息进行比较。
- 此命令显示了对几个重要的命令模式的设置。每个模式组都用符号 “!” 隔开，并包括配置模式命令以及相应的命令。此命令将显示以下信息：
  - 系统说明 （主机名、位置、联系信息）
  - SNMP 社区字符串
  - 用户 （用户名、访问级别和加密口令）
  - VLAN 数据库 （VLAN ID、名称和状态）
  - 每个接口的 VLAN 配置设置
  - 管理 VLAN 的 IP 地址
  - 用户验证顺序，以及远程验证服务器地址和 UDP 端口
  - 已为控制台端口和 Telnet 配置的所有设置

示例

```
Console#show startup-config
building startup-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
```

```
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
 vlan 2 name MgtVlan media ethernet state active
!
!
spanning-tree mst-configuration
 name XSTP REGION 0
!
interface ethernet SNP0
 description Blade Slot 1
 flowcontrol
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 spanning-tree edge-port
 spanning-tree link-type auto
.
.
interface vlan 2
 ip address 0.0.0.0 255.0.0.0
!!
no bridge-ext gvrp!
!
authentication login local
tacacs-server host 0.0.0.0
tacacs-server port 0
!
line console
!
!
line vty
!
!
end
Console#
```

相关命令

show running-config (4-36)

4.3.3.12 show running-config

使用此命令可以显示当前正在使用的配置信息。

默认设置

无

命令模式

特权执行

命令用法

- 如果将此命令与 **show startup-config** 命令结合使用，则可以将存储在运行的内存中的信息与存储在非易失性存储区中的信息进行比较。
- 此命令显示了对几个重要的命令模式的设置。每个模式组都用符号 “!” 隔开，并包括配置模式命令以及相应的命令。此命令将显示以下信息：
  - 系统说明 （主机名、位置、联系信息）
  - SNMP 社区字符串
  - 用户 （用户名、访问级别和加密口令）
  - VLAN 数据库 （VLAN ID、名称和状态）
  - 每个接口的 VLAN 配置设置
  - 管理 VLAN 的 IP 地址
  - 用户验证顺序，以及远程验证服务器地址和 UDP 端口
  - 已为控制台端口和 Telnet 配置的所有设置

示例

```
Console#show running-config
building running-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
!
snmp-server community private rw
snmp-server community public ro
```

```
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
 vlan 2 name MgtVlan media ethernet state active
!
!
!
spanning-tree mst-configuration
!
interface ethernet SNP0
 description Blade Slot 0
 flowcontrol
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 spanning-tree edge-port
 spanning-tree link-type auto
.
.
interface vlan 2
 ip address 0.0.0.0 255.0.0.0
!
!
no bridge-ext gvrp
!
!
authentication login local
tacacs-server host 0.0.0.0
tacacs-server port 0
!
line console
!
line vty
!
!
end
Console#
```

相关命令

show startup-config (4-34)

4.3.3.13 show system

使用此命令可以显示系统信息。

默认设置

无

命令模式

普通执行、特权执行

命令用法

- 有关此命令显示的各个项目的说明，请参阅第 3-7 页上的 “显示系统信息”。
- POST 结果应该全部显示 “PASS”。如果有 POST 测试显示 “FAIL”，请与您的分销商联系以寻求帮助。

示例

```
Console#show system
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.42.2.24.1
System information
 System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
 System Name            : [NONE]
 System Location        : [NONE]
 System Contact         : [NONE]
 MAC address            : 00-00-e8-00-00-01
 Web server             : enable
 Web server port        : 80
 Web secure server      : enable
 Web secure server port : 443
 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
Switch Driver Initialization ........... PASS
------------------- DONE --------------------
Console#
```

4.3.3.14 show users

显示所有活动的控制台会话和 Telnet 会话，包括 Telnet 客户机的用户名、闲置时间和 IP 地址。

默认设置

无

命令模式

普通执行、特权执行

命令用法

用于执行本命令的会话用行 （即会话）索引编号旁边的 “*” 符号来标示。

示例

```
Console#show users
 Username accounts:
  Username Privilege
  -------- ---------
     admin        15
     guest         0

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
  1     vty 0    admin           0:04:37      10.1.0.19

Console#
```

4.3.3.15 show version

使用此命令可以显示系统的硬件信息和软件版本信息。

默认设置

无

命令模式

普通执行、特权执行

命令用法

有关各个软件项的详细信息，请参阅第 3-16 页上的 “显示交换机软件版本”。硬件项的含义如下：

- **Serial Number** — 主板的序列号。
- **Service Tag** — 不适用于本交换机。
- **Hardware Version** — 主板的硬件版本。
- **Number of Ports** — 交换机上的端口数量
- **Main Power Status** — 交换机的电源状态。
- **Redundant Power Status** — 不适用于本交换机。

示例

```
Console#show version
Unit1
 Serial number           :1
 Service tag             :
 Hardware version        :R0B
 Number of ports         :25
 Main power status       :up
 Redundant power status :not present
Agent(master)
 Unit id                 :1
 Loader version          :0.0.6.5
 Boot rom version        :0.0.7.3
 Operation code version :1.0.0.1
Console#
```

4.3.4 验证命令

您可以对交换机进行配置，令其使用本地验证方法、 RADIUS 验证方法或 TACACS 验证方法对登录系统进行管理访问的用户进行验证。

RADIUS 和 TACACS 都是登录验证协议，它们使用中央服务器上运行的软件来控制对网络上能识别 RADIUS 或 TACACS 的设备的访问权限。验证服务器中包含一个数据库，该数据库中包含多个用户名 / 口令对以及每个需要对交换机具有管理访问权限的用户或组的权限级别。

命令	功能	模式	页码
验证方法			
authentication login	定义登录验证方法和优先权	GC	4-42
RADIUS 客户机			
radius-server host	指定 RADIUS 服务器	GC	4-43
radius-server port	设置 RADIUS 服务器网络端口	GC	4-43
radius-server key	设置 RADIUS 加密密钥	GC	4-44
radius-server retransmit	设置重试次数	GC	4-44
radius-server timeout	设置两次发送验证请求之间的时间间隔	GC	4-45
show radius-server	显示当前的 RADIUS 设置	PE	4-45
TACACS 客户机			
tacacs-server host	指定 TACACS 服务器	GC	4-46
tacacs-server port	设置 TACACS 服务器网络端口	GC	4-46
tacacs-server key	设置 TACACS 加密密钥	GC	4-47
show tacacs-server	显示当前的 TACACS 设置	PE	4-47

4.3.4.1 authentication login

使用此命令可以定义登录验证方法和优先权。使用此命令的 **no** 形式可以恢复默认值。

语法

authentication login {**[local] [radius] [tacacs]**}
no authentication login

- **local** — 使用本地口令。
- **radius** — 使用 RADIUS 服务器口令。
- **tacacs** — 使用 TACACS 服务器口令。

可按任何顺序指定验证方法。

默认设置

无

命令模式

全局配置

命令用法

- RADIUS 使用 UDP，而 TACACS 使用 TCP。UDP 只注重发送方面的事项，而 TCP 则提供面向连接的传输。同时，请注意， RADIUS 只对从客户机到服务器的访问请求数据包中的口令加密，而 TACACS 则对数据包的正文全部进行加密。
- RADIUS 和 TACACS 登录验证可以控制是否允许通过控制台端口、Web 浏览器或 Telnet 进行管理。这些权限选项必须在验证服务器上进行配置。
- RADIUS 和 TACACS 登录验证为每个用户名 / 口令对分配一个特定的权限级别。用户名、口令和权限级别必须在验证服务器上进行配置。
- 可以在一条命令中指定两种或三种验证方法，用以说明验证顺序。例如，如果输入“**authentication login radius local**”，将首先验证 RADIUS 服务器上的用户名和口令。如果 RADIUS 服务器不可用，则检查本地用户名和口令。

示例

```
Console(config)#authentication login radius
Console(config)#
```

相关命令

username — 用于设置本地用户名和口令 (4-26)

4.3.4.2 radius-server host

使用此命令可以指定 RADIUS 服务器。使用此命令的 **no** 形式可以恢复默认值。

语法

radius-server host *host_ip_address*
no radius-server host

host_ip_address — 服务器的 IP 地址。

默认设置

10.11.12.13

命令模式

全局配置

示例

```
Console(config)#radius-server host 192.168.1.25
Console(config)#
```

4.3.4.3 radius-server port

使用此命令可以设置 RADIUS 服务器网络端口。使用此命令的 **no** 形式可以恢复默认值。

语法

radius-server port *port_number*
no radius-server port

port_number — 用于传输验证消息的 RADIUS 服务器 UDP 端口。（范围：1-65535）

默认设置

1812

命令模式

全局配置

示例

```
Console(config)#radius-server port 181
Console(config)#
```

4.3.4.4 radius-server key

使用此命令可以设置 RADIUS 加密密钥。使用此命令的 **no** 形式可以恢复默认值。

语法

radius-server key *key_string*
no radius-server key

key_string — 用于验证客户机的登录访问权限的加密密钥。请勿在该字符串中使用空格。（最大长度：20 个字符）

默认设置

无

命令模式

全局配置

示例

```
Console(config)#radius-server key green
Console(config)#
```

4.3.4.5 radius-server retransmit

使用此命令可以设置重试次数。使用此命令的 **no** 形式可以恢复默认值。

语法

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries — 交换机将尝试通过 RADIUS 服务器验证登录访问权限的次数。（范围：1-30）

默认设置

2

命令模式

全局配置

示例

```
Console(config)#radius-server retransmit 5
Console(config)#
```

4.3.4.6 radius-server timeout

使用此命令可以设置在两次向 RADIUS 服务器发送验证请求之间的时间间隔。使用此命令的 **no** 形式可以恢复默认值。

语法

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds — 交换机在重新发送请求之前等待响应的秒数。（范围：1-65535）

默认设置

5

命令模式

全局配置

示例

```
Console(config)#radius-server timeout 10
Console(config)#
```

4.3.4.7 show radius-server

使用此命令可以显示 RADIUS 服务器的当前设置。

默认设置

无

命令模式

特权执行

示例

```
Console#show radius-server
Remote radius server configuration:
 Server IP address: 10.11.12.13
 Communication key with radius server: green
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#
```

4.3.4.8 tacacs-server host

使用此命令可以指定 TACACS 服务器。使用此命令的 **no** 形式可以恢复默认值。

语法

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address — 服务器的 IP 地址。

默认设置

无

命令模式

全局配置

示例

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

4.3.4.9 tacacs-server port

使用此命令可以设置 TACACS 服务器网络端口。使用此命令的 **no** 形式可以恢复默认值。

语法

tacacs-server port *port_number*
no tacacs-server port

port_number — 用于传输验证消息的 TACACS 服务器 UDP 端口。（范围：1-65535）

默认设置

无

命令模式

全局配置

示例

```
Console(config)#tacacs-server port 181
Console(config)#
```

4.3.4.10 tacacs-server key

使用此命令可以设置 TACACS 加密密钥。使用此命令的 **no** 形式可以恢复默认值。

语法

tacacs-server key *key_string*
no tacacs-server key

key_string — 用于验证客户机的登录访问权限的加密密钥。请勿在该字符串中使用空格。（最大长度：20 个字符）

默认设置

无

命令模式

全局配置

示例

```
Console(config)#tacacs-server key green
Console(config)#
```

4.3.4.11 show tacacs-server

使用此命令可以显示 TACACS 服务器的当前设置。

默认设置

无

命令模式

特权执行

示例

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address: 10.11.12.13
 Communication key with tacacs server: green
 Server port number: 1824
Console#
```

4.3.5 SNMP 命令

这些命令可控制通过 SNMP 管理站对交换机所进行的访问，以及发送到陷阱管理器的错误类型。

命令	功能	模式	页码
snmp-server community	设置社区访问字符串 （以允许访问 SNMP 命令）	GC	4-48
snmp-server contact	设置系统联系人字符串	GC	4-49
snmp-server location	设置系统位置字符串	GC	4-50
snmp-server host	指定 SNMP 通知操作的收件人	GC	4-50
snmp-server enable traps	使设备可以发送 SNMP 陷阱或通知请求（即 SNMP 通知）	GC	4-51
show snmp	显示 SNMP 通信的状态	NE、PE	4-52

4.3.5.1 snmp-server community

使用此命令可以定义用于 “简单网络管理协议”的社区访问字符串。使用此命令的 **no** 形式可以删除指定的社区字符串。

语法

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* — 充当口令并确定是否允许访问 SNMP 协议的社区字符串。（最大长度：32 个字符；区分大小写；字符串最大数量：5）
- **ro** — 指定只读访问权限。经过授权的管理站只能检索 MIB 对象。
- **rw** — 指定读 / 写访问权限。经过授权的管理站既能检索 MIB 对象，又能修改 MIB 对象。

默认设置

- 公共 — 具有只读访问权限。
- 专用 — 具有读 / 写访问权限。

命令模式

全局配置

命令用法

您输入的第一条 **snmp-server community** 命令将启用 SNMP 的所有版本（SNMPv1 和 SNMPv2c）。**no snmp-server community** 命令禁用 SNMP 的所有版本。

示例

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

4.3.5.2 snmp-server contact

使用此命令可以设置系统联系人字符串。使用此命令的 **no** 形式可以删除系统联系人信息。

语法

snmp-server contact *string*
no snmp-server contact

string — 用于描述系统联系人信息的字符串。（最大长度：255 个字符）

默认设置

无

命令模式

全局配置

示例

```
Console(config)#snmp-server contact Paul
Console(config)#
```

相关命令

snmp-server location (4-50)

4.3.5.3 snmp-server location

使用此命令可以设置系统位置字符串。使用此命令的 **no** 形式可以删除系统位置字符串。

语法

snmp-server location *text*
no snmp-server location

text — 用于描述系统位置的字符串。（最大长度：255 个字符）

默认设置

无

命令模式

全局配置

示例

```
Console(config)#snmp-server location WC-19
Console(config)#
```

相关命令

snmp-server contact (4-49)

4.3.5.4 snmp-server host

使用此命令可以指定 “简单网络管理协议”通知操作的接收方。使用此命令的 **no** 形式可以删除指定的主机。

语法

snmp-server host *host-addr community-string* **version** *version-number*
no snmp-server host *host-addr*

- *host-addr* — 主机名或主机的 Internet 地址 （目标接收方）。（主机地址的最多数量：5 个陷阱目标 IP 地址条目）
- *community-string* — 随通知操作发送出的类似口令的社区字符串。尽管仅使用 **snmp-server host** 命令即可设置此字符串，但我们还是建议您在定义此字符串时先使用 **snmp-server host** 命令，然后再使用 **snmp-server community** 命令。（最大长度：32 个字符）
- *version-number* — {**1** | **2c**}
  指出主机运行的是 SNMP 版本 1 还是版本 2c。

默认设置

无

命令模式

全局配置

命令用法

如果不输入 **snmp-server host** 命令，则不会发送任何通知。为使交换机能够发送 SNMP 通知，必须至少输入一条 **snmp-server host** 命令。若要启用多台主机，必须为每台主机都单独发出一条 **snmp-server host** 命令。

snmp-server host 命令与 **snmp-server enable traps** 命令结合使用。使用 **snmp-server enable traps** 命令可以指定哪些 SNMP 通知应全局发送。要使主机能够接收通知，必须为该主机至少输入一条 **snmp-server enable traps** 命令和一条 **snmp-server host** 命令。

不过，有些通知类型无法通过 **snmp-server enable traps** 命令进行控制。例如，某些通知类型始终处于启用状态。

示例

```
Console(config)#snmp-server host 10.1.19.23 batman version 1
Console(config)#
```

相关命令

snmp-server enable traps (4-51)

4.3.5.5 snmp-server enable traps

使用此命令可以使本设备能够发送 “简单网络管理协议”陷阱或通知 （SNMP 通知）。使用此命令的 **no** 形式可以禁用 SNMP 通知。

语法

snmp-server enable traps [authentication | link-up-down]
no snmp-server enable traps [authentication | link-up-down]

- **authentication** — 用于发出验证失败陷阱的关键字。
- **link-up-down** — 用于发出链接建立陷阱或链接断开陷阱的关键字。

默认设置

发出验证陷阱、链接建立陷阱或链接断开陷阱。

命令模式

全局配置

命令用法

如果不输入 **snmp-server enable traps** 命令，则不会发出由此命令控制的任何通知。为使本设备能够发送 SNMP 通知，必须至少输入一个 **snmp-server enable traps** 命令。如果输入不带关键字的命令，则既会启用验证通知，又会启用链接建立通知或链接断开通知。如果输入带关键字的命令，则会只启用与该键字相关的通知类型。

snmp-server enable traps 命令与 **snmp-server host** 命令结合使用。使用 **snmp-server host** 命令可以指定用来 SNMP 通知的主机。为了发送通知，必须至少配置一条 **snmp-server host** 命令。

示例

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

相关命令

snmp-server host (4-50)

4.3.5.6 show snmp

使用此命令可以检查 SNMP 通信的状态。

默认设置

无

命令模式

普通执行、特权执行

命令用法

此命令可提供有关社区访问字符串的信息、 SNMP 输入协议数据单元和输出协议数据单元的计数器信息，并显示是否使用 **snmp-server enable traps** 命令启用了 SNMP 日志记录功能。

示例

```
Console#show snmp

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read/write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```

4.3.6 线路命令

如果将一台与 VT100 兼容的设备连接到服务器的串行端口，就可以访问内置的配置程序。这些命令用于设置串行端口或 Telnet （即虚拟终端）的通信参数。

注：串行接口的连接参数固定为 8 个数据位、 1 个停止位、无奇偶校验、速率为 9600 bps。

命令	功能	模式	页码
line	标识要进行配置的特定线路并启动线路配置模式	GC	4-55
login	启用登录时的口令检查功能	LC	4-56
password	指定线路的口令	LC	4-57
exec-timeout	设置在检测到用户输入之前命令解释程序将等待的时间间隔	LC	4-58
password-thresh	设置口令入侵阈值，该阈值对登录尝试的失败次数进行了限制	LC	4-59
silent-time*	设置一个时间量，即在登录尝试的失败次数超过 **password-thresh** 命令所设置的阈值后，无法对管理控制台进行访问的那一段时间	LC	4-60
show line	显示终端线路的参数	NE、PE	4-61

* 此命令仅适用于串行端口。

4.3.6.1 line

使用此命令可以标识要配置的特定线路，并处理随后的线路配置命令。

语法

line {**console** | **vty**}

- **console** — 控制台终端线路。
- **vty** — 用于访问远程控制台的虚拟终端 （即 Telnet）。

默认设置

无默认线路。

命令模式

全局配置

命令用法

Telnet 被当作是虚拟终端连接，因此将在诸如 **show users** 之类的屏幕显示中显示为“Vty”。

示例

要进入控制台线路模式，请输入以下命令：

```
Console(config)#line console
Console(config-line)#
```

相关命令

show line (4-61)
show users (4-39)

4.3.6.2 login

使用此命令可以在登录时启用口令检查功能。使用此命令的 **no** 形式可以禁用口令检查功能，并允许不输入口令即进行连接。

语法

login [local]
no login

local — 选择本地口令检查。验证以 **username** 命令所指定的用户名为基础。

默认设置

登录本地

命令模式

线路配置

命令用法

- 在登录时交换机本身提供了三种验证模式：
  - **login** 按 **password** 线路配置命令指定的单个全局口令来选择验证。使用此方法时，管理界面将在 “普通执行” (NE) 模式下启动。
  - **login local** 按 **username** 命令指定的用户名和口令（即默认设置）来选择验证。使用此方法时，管理界面将在 “普通执行” (NE) 模式或 “特权执行” (PE) 模式下启动，具体取决于用户的权限级别 （分别为 0 或 15）。
  - **no login** 选择不进行验证。使用此方法时，管理界面将在 “普通执行” (NE) 模式下启动。
- 此命令通过交换机本身控制登录验证。要为远程验证服务器配置用户名和口令，必须使用这些服务器上所安装的 RADIUS 或 TACACS 软件。

示例

```
Console(config-line)#login local
Console(config-line)#
```

相关命令

username (4-26)
password (4-57)

4.3.6.3 password

使用此命令可以指定线路的口令。使用此命令的 **no** 形式可以删除口令。

语法

password {**0** | **7**} *password*
no password

- {**0** | **7**} — 0 表示输入纯文本口令， 7 表示输入加密口令。
- *password* — 用于指定线路口令的字符串。（最大长度：纯文本口令为 8 个字符，加密口令为 32 个字符，且口令区分大小写）

默认设置

未指定口令。

命令模式

线路配置

命令用法

- 当在一条有口令保护的线路上启动连接时，系统将提示您输入口令。如果输入的口令正确，系统将会显示提示符。通过 **password-thresh** 命令，可以设置在系统终止线路连接并将终端返回到闲置状态之前，用户可以输入错误口令的次数。
- 无须在命令行上指定加密口令。交换机进行系统引导时对内部使用了选项 7，从而使交换机能够读取存储在配置文件中的任何加密口令。

示例

```
Console(config-line)#password 0 secret
Console(config-line)#
```

相关命令

login (4-56)
password-thresh (4-59)

4.3.6.4 exec-timeout

使用此命令可以设置系统在终止当前会话之前等待用户进行输入的时间间隔。使用此命令的 **no** 形式可以恢复默认值。

语法

exec-timeout [*seconds*]
no exec-timeout

seconds — 一个表示秒数的整数值。（范围：0 - 65535 秒； 0 表示无超时）

默认设置

CLI：无超时
Telnet：10 分钟

命令模式

线路配置

命令用法

- 如果在超时时间间隔内检测到用户输入，则会话将保持打开状态；否则会话将终止。
- 此命令适用于串行控制台连接和 Telnet 连接 （但不能为 Telnet 禁用超时）。

示例

要将超时值设置为 2 分钟，请输入以下命令：

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

4.3.6.5 password-thresh

使用此命令可以设置口令入侵阈值，用来限制登录尝试的失败次数。使用此命令的 **no** 形式可以删除阈值。

语法

password-thresh *threshold*
no password-thresh

threshold — 所允许的口令尝试次数。（范围：1-120 ； 0 表示无阈值）

默认设置

默认值为 3 次尝试。

命令模式

线路配置

命令用法

- 当达到控制台端口的登录尝试阈值后，系统界面会在指定的一段时间内不进行响应，之后才允许进行下次登录尝试。（使用 **silent-time** 命令可以设置无法响应的时间间隔）。如果达到了 Telnet 此方面的阈值， Telnet 登录界面将关闭。
- 此命令既适用于本地控制台连接，又适用于 Telnet 连接。

示例

要将口令阈值设置为 5 次尝试，请输入以下命令：

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

相关命令

silent-time (4-60)

4.3.6.6 silent-time

使用此命令可以设置一个时间量，即在登录尝试失败次数超过 **password-thresh** 命令所设置的阈值之后无法对管理控制台进行访问的那一段时间。使用此命令的 **no** 形式可以删除无响应的时间值。

语法

silent-time [*seconds*]
no silent-time

seconds — 禁止控制台做出响应的秒数。（范围：0-65535； 0 表示不设置无响应时间）

默认设置

默认值为不设置无响应时间。

命令模式

线路配置

示例

要将无响应时间设置为 60 秒，请输入以下命令：

```
Console(config-line)#silent-time 60
Console(config-line)#
```

相关命令

password-thresh (4-59)

4.3.6.7 show line

使用此命令可以显示终端线路的参数。

语法

show line [console | vty]

- **console** — 控制台终端线路。
- **vty** — 用于访问远程控制台的虚拟终端 （即 Telnet）。

默认设置

显示所有线路。

命令模式

普通执行、特权执行

示例

要显示所有线路的连接设置，请输入以下命令：

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 600
Console#
```

4.3.7 IP 命令

默认情况下，交换机使用 DHCP 搜索它的 IP 地址、默认网关和子网掩码。

可以手动配置一个特定的 IP 地址，也可指示设备从 BOOTP 服务器或 DHCP 服务器获取地址。有效的 IP 地址由四组用句点分隔的数字组成，数字范围从 0 到 255。任何不符合该格式的地址都无法为软件所接受。

命令	功能	模式	页码
IP 配置			
ip address	为此设备设置 IP 地址	IC	4-62
ip dhcp restart	提交 BOOTP 或 DCHP 客户机请求	PE	4-64
ip dhcp client-identifier	为交换机指定 DHCP 客户机标识符。请注意，每次启动系统控制器或交换机时，系统控制器都会为交换机指定客户机标识符。因此，我们建议您不要指定客户机标识符。	VC	4-65
ip default-gateway	定义默认网关，供带内管理站与本设备建立联系	GC	4-66
show ip interface	显示此设备的 IP 设置	PE	4-66
show ip redirects	显示已为此设备配置的默认网关	PE	4-67
ping	向网络上的另一个节点发送 ICMP 回应请求数据包	NE、PE	4-67
过滤 IP 数据包			
ip filter	阻止指定的 IP 数据包从其它交换机端口进入内部管理端口 (NETMGT)	GC	4-68
show ip filter	显示过滤规则或捕获的数据包	PE	4-71

4.3.7.1 ip address

使用此命令可为此设备设置 IP 地址。使用此命令的 **no** 形式可以恢复默认的 IP 地址。

语法

ip address {*ip-address netmask* | **bootp** | **dhcp**}
no ip address

- *ip-address* — IP 地址
- *netmask* — 相关 IP 子网的网络掩码。此掩码可标识用于路由到特定子网的主机地址位。
- **bootp** — 从 BOOTP 获取 IP 地址。
- **dhcp** — 从 DHCP 获取 IP 地址。

默认设置

默认设置为：dhcp

命令模式

接口配置 (VLAN)

命令用法

- 可以手动配置一个特定的IP地址，也可指示设备从BOOTP服务器或DHCP服务器获取地址。出厂默认设置为使用 DHCP。有效的 IP 地址由四组用句点分隔的数字组成，数字范围从 0 到 255。任何不符合该格式的地址都无法为配置程序所接受。
- 如果您选择了**bootp**或**dhcp**选项，将启用IP，但只在收到BOOTP或DHCP响应之后它才会起作用。此设备将定期广播请求，以了解其 IP 地址。（BOOTP 值和 DHCP 值可以包括 IP 地址、默认网关和子网掩码）。
- 通过输入 **ip dhcp restart** 命令或重新引导交换机，可以开始广播 BOOTP 请求或 DHCP 请求。

注：交换机的 IP 地址实际上就是包含管理端口 (NETMGT) 的那个 VLAN 的 IP 地址。默认情况下，管理端口位于 VLAN 2 上。因此，如果将某个 IP 地址分配给 VLAN 2，就将与交换机建立网络连接。只应给包含管理端口的那个 VLAN 分配 IP 地址。当您将一个 IP 地址分配给任意一个 VLAN 之后，该 VLAN 原来的 IP 地址将立即被禁用，而新的地址将立即生效。

示例

在以下示例中，将一个 IP 地址分配给了 VLAN 2 中的设备。

```
Console(config)#interface vlan 2
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

相关命令

ip dhcp restart (4-64)

4.3.7.2 ip dhcp restart

使用此命令可以启动 BOOTP 客户机请求或 DCHP 客户机请求。

默认设置

无

命令模式

特权执行

命令用法

- DHCP 要求服务器重新分配客户机最后所使用的地址 （如果可用）。
- 如果已将BOOTP服务器或DHCP服务器移至其它域，那么给客户机提供的IP地址中的网络部分应基于该新域。

示例

在以下示例中，将同一个地址再次分配给了设备。

```
Console(config)#interface vlan 2
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
 and address mode: DHCP.
Console#
```

相关命令

ip address (4-62)

4.3.7.3 ip dhcp client-identifier

使用此命令可为交换机指定 DCHP 客户机标识符。使用此命令的 **no** 形式可以删除此标识符。

注：下次重新引导系统或交换机自身时，客户机标识符将被系统控制器所覆盖。下一个固件版本将删除客户机标识符命令。

语法

ip dhcp client-identifier {**text** *text* | **hex** *hex*}
no ip dhcp client-identifier

- *text* — 文本字符串。（范围：1-15 个字符）
- *hex* — 十六进制值。

默认设置

只要 SSC 中的系统控制器重置交换机，该系统控制器就会提供 DHCP 客户机标识符。因此，我们建议您不要通过交换机命令行界面更改此值。有关系统机箱内的交换机和其它组件的 DHCP 客户机标识符的信息，请参阅 *《Sun Fire 1600 刀片式系统机箱软件设置指南》*。

命令模式

接口配置 (VLAN)

命令用法

- 通过此命令，可使与 DHCP 服务器的所有通信中都包含客户机标识符。所使用的数据类型将取决于您的 DHCP 服务器的要求。
- 通过此命令指定的客户机标识符将在系统控制器下次重新引导时被系统控制器所覆盖。

示例

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

相关命令

ip dhcp restart (4-64)

4.3.7.4 ip default-gateway

使用此命令可以在此设备和另一个网段上的管理站之间建立一条静态路由。使用此命令的 **no** 形式可以删除静态路由。

语法

ip default-gateway *gateway*
no ip default-gateway

gateway — 默认网关的 IP 地址

默认设置

未建立静态路由。

命令模式

全局配置

命令用法

如果管理站位于另一 IP 网段上，则必须定义网关。

示例

以下示例为此设备定义了默认网关：

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

相关命令

show ip redirects (4-67)

4.3.7.5 show ip interface

使用此命令可以显示 IP 接口的设置。

默认设置

所有接口

命令模式

特权执行

命令用法

只能给本交换机分配一个 IP 地址。该地址用于管理交换机。

示例

```
Console#show ip interface
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
 and address mode: User specified.
Console#
```

相关命令

show ip redirects (4-67)

4.3.7.6 show ip redirects

使用此命令可以显示为此设备配置的默认网关。

默认设置

无

命令模式

特权执行

示例

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

相关命令

ip default-gateway (4-66)

4.3.7.7 ping

使用此命令可以向网络中的另一个节点发送 ICMP 回应请求数据包。

语法

ping *host* [**count** *count*][**size** *size*]

- *host* — 主机的 IP 地址。
- *count* — 要发送的数据包数量。（范围：1-16，默认值：5）
- *size* — 数据包中的字节数。（范围：32-512，默认值：32）
  实际的数据包大小应该比指定的大小多 8 个字节，因为交换机添加了标题信息。

默认设置

此命令没有为主机指定默认值。

命令模式

普通执行、特权执行

命令用法

- 使用 ping 命令可以检查能否连接到网络中的另一个站点上。
- 下面列出了 ping 命令的部分结果：
  - 正常响应 — 正常响应将在 1 到 10 秒出现，具体情况取决于网络通信流量。
  - 目标不响应 — 如果主机不响应，则交换机将显示 “timeout”。
  - 无法连接到目标 — 目标的网关指出：目标无法进行连接。
  - 无法连接网络或主机 — 网关在路由表中没有相应的条目。
- 按 <Esc> 键可以停止执行 ping 命令。

示例

```
Console#ping 10.1.0.19
Type Ctrl-C to abort.
PING to 10.1.0.19, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time:0 ms
response time:0 ms
response time:10 ms
response time:10 ms
response time:10 ms
Ping statistics for 10.1.0.19:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 6 ms
Console#
```

4.3.7.8 ip filter

使用此命令可以阻止指定的 IP 数据包从下行连接端口进入内部管理端口。使用此命令的 **no** 形式可以删除过滤表中的规则。

语法

ip filter [*rule-number*] *action protocol* {*source source-bitmask*} {*destination destination-bitmask*} **[fragments] [log]**

不检查端口号。允许使用 **fragments** 选项。

ip filter [*rule-number*] *action protocol* {*source source-bitmask*} [*source-port-range*] {*destination destination-bitmask*} [*destination-port-range*] **[log]**

检查端口号；即，如果指定了 *source-port-range* 或 *destination-port-range*，则不允许使用 **fragments** 选项。

ip filter [*rule-number*] *action* **tcp** {*source source-bitmask*} [*source-port-range*] {*destination destination-bitmask*} [*destination-port-range*] [**code** {{*code code-bitmask*} | *code-keyword-seq*}] [**log**]

查看是否有 **tcp** 关键字。如果找到了该关键字，则允许使用 **code** 选项。

no ip filter {**all** |*rule-number*}

从过滤表中删除指定的规则编号。

- *rule-number* — 在过滤表中的指定位置插入一条过滤规则，从而使该表中位于插入位置或之后的所有现有模式都向下移动。规则编号不能大于该表中下一个可用的编号。如果未指定规则编号，会在该表的结尾处加上一种新模式。最大的规则编号为 128。
- *action* - {**deny** | **permit**}
  阻止或允许数据包在下行链接端口和管理端口 (NETMGT) 之间移动。
- *protocol* - {**any** | **tcp** | **udp** | *number*}
  指示任何协议：TCP、 UDP 或特定的协议编号 (0-255)。
- *source source-bitmask* — 帧的源地址和子网掩码。
- *source-port-range* - [*number* | *start_number-end_number*]
  TCP/UDP 源端口或端口范围。（范围：0-65535）
- *destination destination-bitmask* — 帧的目标地址和子网掩码。
- *destination-port-range* - [*number* | *start_number-end_number*]
  TCP/UDP 目标端口或端口范围。（范围：0-65535）
- **code**
  - *code* — 用于指定 TCP 标头中第 14 个字节的标记位的十进制数（代表位字符串）。（范围：0-63）
  - *code-bitmask* — 适用于该代码的十进制数 （代表位掩码）。输入一个十进制数，其中所对应的二进制位 “1” 表示匹配位，“0” 表示忽略位。可以指定以下位：
    - 1 (fin) — 完成
    - 2 (syn) — 同步
    - 4 (rst) — 重置
    - 8 (psh) — 推
    - 16 (ack) — 确认
    - 32 (urg) — 紧急指针
  - *code-keyword-seq* — 可以指定下列代码关键字，但必须按指定的顺序进行：**fin** | **syn** | **rst** | **psh** | **ack** | **urg**
    （如果指定代码关键字，则它必须是 ON，如果不指定，则必须是 OFF。）
- **fragments** — 规则使数据包仅与 “分组片位” (MF) 位组匹配，或是与大于零的分段偏移量匹配。如果没有设置 **fragment**，那么规则将匹配分段数据包和未分段的数据包。
- **log** — 在日志缓冲区中记录所有匹配的数据包。存储在日志缓冲区中的最大条目数为 64。如果缓冲区已满，它将绕回并覆盖时间最早的条目。请注意，日志存储在 RAM 中，因此，当交换机重置时，这些日志将丢失。

默认设置

无

命令模式

常规配置

命令用法

- 根据系统的默认设置，禁止任何 IP 数据包从下行链接端口传递到管理端口 (NETMGT)。如果您需要服务器刀片通过管理端口 (NETMGT) 访问管理网络，则必须设置一个过滤器，以允许特定的帧从下行链接端口传递到管理端口。请注意，绝对不允许从上行链接端口向管理端口通信。
- 分段指的是 MF（分组片位）= 1 或分段偏移量 > 0 的数据包。如果规则中没有关键字 **fragments**，那么规则会既检查分段数据包，又检查未分段的数据包。
- 指定了代码值和掩码后，逻辑为：如果 < 标头中的值 > & < 掩码 > == < 值 > & < 掩码 >，则数据包就可匹配。例如，通过下面显示的代码值和掩码，可使数据包与下列标记集匹配：
  - SYN 标记有效，使用 “代码 2 2”
  - SYN 和 ACK 都有效，使用 “代码 18 18”
  - SYN 有效但 ACK 无效，使用 “代码 2 18”

示例 — 地址过滤器

本例允许所有数据包通过过滤器，方法是允许使用任何协议类型，并对源地址和目标地址使用空地址和网络掩码。

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Console(config)#
```

这表示如果源地址在子网 10.7.1.x 之内，就将接受传入的所有数据包。例如，如果与该规则匹配，即规则 (10.7.1.1 & 255.255.255.0) 等于掩码地址 (10.7.1.2 & 255.255.255.0)，则让数据包通过。

```
Console(config)#ip filter permit any 10.7.1.1 255.255.255.0 0.0.0.0
   0.0.0.0
Console(config)#
```

示例 — 检查分段

本例阻止所有分段并将匹配的数据包记录到日志中。

```
Console(config)#ip filter deny any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   fragment log
Console(config)#
```

示例 — 检查代码值

本例阻止来自类别 C 地址 192.168.1.0 并设置了 SYN 的所有 TCP 数据包。

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
   0.0.0.0 code syn
Console(config)#
```

它还将阻止来自类别 C 地址 192.168.1.0 并设置了 SYN 的所有 TCP 数据包。

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
   0.0.0.0 code 2 2
Console(config)#
```

示例 — 检查端口号

本例允许在将目标端口设置为 80 的情况下，将来自类别 C 地址 192.168.1.0 的 TCP 数据包发送到任何位置。

```
Console(config)#ip filter permit tcp 192.168.1.0 255.255.255.0 0.0.0.0
   0.0.0.0 80
Console(config)#
```

本例删除符合以下条件的数据表：从源地址 10.7.1.1 到目标地址 10.8.1.1 ；源端口范围：30 - 46 ； 目标端口范围：100 - 2000。

```
Console(config)#ip filter deny tcp 10.7.1.1 255.255.255.255 30-46
   10.8.1.1 255.255.255.255 100-2000
Console(config)#
```

4.3.7.9 show ip filter

使用此命令可以显示 IP 过滤表中的所有规则。

语法

show ip filter [*rule-number* | **log**]

- *rule-number* — 显示 IP 过滤表中指定位置的过滤规则。范围：1-128
- **log** — 显示存储在日志缓冲区中的所有数据包。请注意，存储在日志缓冲区中的数据包必须符合过滤表中的规则。日志缓冲区中所能存储的最大条目数为 64。

如果未选择任何选项，则将显示日志缓冲区中的所有数据包。

默认设置

无

命令模式

特权执行

示例

本例中唯一指定的规则允许将子网 10.1.0.x 内的数据包在管理端口和下行链接端口之间传递。

```
Console#show ip filter
Ip filter:
 Rule:1, Action:permit, Protocol:any, Log:disable, Fragments:disable
 Source:10.1.0.0 255.255.255.0 any
 Destination:10.1.0.0 255.255.255.0 any
```

4.3.8 接口命令

这些命令用于显示或设置以太网端口、聚合链接或 VLAN 的通信参数。

命令	功能	模式	页码
interface	配置接口类型并进入接口配置模式	GC	4-74
description	为接口配置添加说明	IC	4-74
speed-duplex	在禁用自动协商功能的情况下配置指定接口的速度和双工操作	IC	4-75
negotiation	为指定接口启用自动协商功能	IC	4-76
capabilities	公布指定接口容量（以用于自动协商）	IC	4-77
flowcontrol	对指定接口启用流量控制	IC	4-78
shutdown	禁用接口	IC	4-80
switchport broadcast packet-rate	配置广播风暴控制阈值	IC	4-80
clear counters	清除接口的统计信息	PE	4-81
show interfaces status	显示指定接口的状态	NE、PE	4-82
show interfaces counters	显示指定接口的统计信息	NE、PE	4-83
show interfaces switchport	显示接口的管理状态和运行状态	NE、PE	4-85

4.3.8.1 interface

使用此命令可以配置接口类型并进入接口配置模式。

语法

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）
- **vlan** *vlan-id*（范围：1-4094）

默认设置

无

命令模式

全局配置

示例

要指定第一个上行链接端口，请输入以下命令：

```
Console(config)#interface ethernet NETP0
Console(config-if)#
```

4.3.8.2 description

使用此命令可以为接口添加说明。使用此命令的 **no** 形式可以删除说明。

语法

description *string*
no description

string — 备注或说明，可以帮助您记住此接口上所安装的设备。（范围：1-64 个字符）

默认设置

NETP0-7：外部 RJ-45 连接器 NET0-7
SNP0-15：刀片插槽 0-15
NETMGT：外部 RJ-45 连接器 NETMGT

命令模式

接口配置 （以太网、端口通道）

示例

以下示例为下行链接端口 SNP5 配置了说明。

```
Console(config)#interface ethernet SNP5
Console(config-if)#description RD-SW#3
Console(config-if)#
```

4.3.8.3 speed-duplex

在禁用自动协商功能的情况下，使用此命令可以配置指定接口的速度和双工模式。使用此命令的 **no** 形式可以恢复默认值。

语法

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **1000full** — 强制进行 1000 Mbps 全双工操作
- **100full** — 强制进行 100 Mbps 全双工操作
- **100half** — 强制进行 100 Mbps 半双工操作
- **10full** — 强制进行 10 Mbps 全双工操作
- **10half** — 强制进行 10 Mbps 半双工操作

默认设置

- 默认情况下启用自动协商功能。
- 在禁用自动协商功能的情况下，默认的速度、双工设置为：对于快速以太网端口为 100full，对于千兆位以太网端口为 1000full。

注：在禁用自动协商功能的情况下，只能将上行链接端口的速度设置为 10 Mbps 或 100 Mbps。要迫使端口以 1 Gbps 全双工模式操作，则应启用自动协商功能，并且将该端口容量仅设置为 “1000full”。

命令模式

接口配置 （以太网、端口通道）

命令用法

- 若要强行按 **speed-duplex** 命令中指定的速度和双工模式进行操作，可使用 **no negotiation** 命令对选定接口禁用自动协商功能。不过，请注意，不能对下行链接端口禁用自动协商功能。这些端口固定采用 1000 Mbps 的速度和全双工模式。
- 当使用 **negotiation** 命令启用自动协商功能时，最佳设置将由 **capabilities** 命令决定。如果要在启用了自动协商功能的情况下设置速度 / 双工模式，所需的模式必须在接口的容量列表中加以指定。

示例

以下示例将端口 NETP5 配置为 100 Mbps、半双工操作。

```
Console(config)#interface ethernet NETP5
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#
```

相关命令

negotiation (4-76)
capabilities (4-77)

4.3.8.4 negotiation

使用此命令可为指定接口启用自动协商功能。使用此命令的 **no** 形式可以禁用自动协商功能。

语法

negotiation
no negotiation

默认设置

启用

命令模式

接口配置 （以太网、端口通道）

命令用法

- 下行链接端口 SNP0-15 始终禁用自动协商功能。
- 启用自动协商功能后，交换机将根据 **capabilites** 命令协商链接的最佳设置。在禁用自动协商功能的情况下，必须使用 **speed-duplex** 命令和 **flowcontrol** 命令手动指定链接属性。
- 如果禁用自动协商功能，也将禁用上行链接端口的自动 MDI/MDI-X 管脚信号配置。

示例

以下示例对端口 SNP11 进行配置，使之使用自动协商功能。

```
Console(config)#interface ethernet SNP11
Console(config-if)#negotiation
Console(config-if)#
```

相关命令

capabilities (4-77)
speed-duplex (4-75)
flowcontrol (4-78)

4.3.8.5 capabilities

使用此命令可以在自动协商期间公布指定接口的端口容量。使用此命令的 **no** 形式与参数一起使用，可取消公布的容量；如果使用此命令的 **no** 形式但不带参数，则可以恢复默认值。

语法

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}
no port-capabilities [1000full | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric]**

- 1000full — 支持 1000 Mbps 全双工操作
- 100full — 支持 100 Mbps 全双工操作
- 100half — 支持 100 Mbps 半双工操作
- 10full — 支持 10 Mbps 全双工操作
- 10half — 支持 10 Mbps 半双工操作
- flowcontrol — 支持流量控制
- symmetric （仅限千兆位）— 如果指定此参数，端口将发送并接收暂停帧；如果不指定此参数，端口将自动协商以确定非对称暂停帧的发送方和接收方。（*当前的交换机 ASIC 只支持对称暂停帧。*）

默认设置

NETMGT：10half、 10full、 100half、 100full
NETP0-7：10half、 10full、 100half、 100full、 1000full、 flow control
SNP0-15：1000full

命令模式

接口配置 （以太网、端口通道）

命令用法

- SNP0-15 下行链接端口容量固定为 1000full。
- NETP0-7 上行链接端口容量包括 10half、 10full、 100half、 100full、 1000full、 flowcontrol 和 symmetric。使用 **negotiation** 命令启用自动协商功能后，交换机将根据 **capabilites** 命令协商链接的最佳设置。在禁用自动协商功能的情况下，必须使用 **speed-duplex** 命令和 **flowcontrol** 命令手动指定链接属性。
- NETMGT 端口容量固定为 10half、 10full、 100half、 100full。

示例

以下示例将端口 NETP5 的容量配置为 100half、 100full 和 flow control。

```
Console(config)#interface ethernet NETP5
Console(config-if)#no capabilities 10half
Console(config-if)#no capabilities 10hfull
Console(config-if)#no capabilities 1000full
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

相关命令

negotiation (4-76)
speed-duplex (4-75)
flowcontrol (4-78)

4.3.8.6 flowcontrol

使用此命令可以启用流量控制功能。使用此命令的 **no** 形式可禁用流量控制功能。

注：Sun Fire B1600 刀片式系统机箱上的集成交换机中都包含两块链接在一起的交换机芯片。若要镜像某个端口上的通信，只能使用该端口所在交换机芯片上的其它端口才有可能实现。端口 NETP0、NETP1、NETP4、NETP5 以及 SNP8 到 SNP15 在同一交换机芯片上。端口 NETP、NETP3、NETP6、NETP7 以及 SNP0 到 SNP7 位于另一交换机芯片上。（如果您查看 SSC 的后面板，则将看到右侧的所有端口位于一块芯片上，而左侧的所有端口位于另一块芯片上。）

语法

flowcontrol
no flowcontrol

默认设置

启用流量控制

命令模式

接口配置 （以太网、端口通道）

命令用法

- 当交换机缓冲区已满时，流量控制功能可以 “阻止”从终端站或直接连接到交换机的网段所发出的通信，从而避免帧丢失。启用流量控制后，将反压用于半双工操作、 IEEE 802.3x 用于全双工操作。
- 要强行打开或关闭流量控制功能（使用 **flowcontrol** 或 **no flowcontrol** 命令），可使用 **no negotiation** 命令禁用选定接口上的自动协商功能。
- 当使用 **negotiation** 命令启用自动协商功能时，最佳设置将由 **capabilities** 命令决定。要在启用自动协商功能的情况下启用流量控制，所有端口的容量列表中都必须包含 “flowcontrol”。
- 请勿在连接到集线器的端口上使用流量控制，除非确实需要使用流量控制才能解决问题。否则反压干扰信号可能会降低集线器所连网段的总体性能。

示例

以下示例在端口 NETP7 上启用流量控制功能。

```
Console(config)#interface ethernet NETP7
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

相关命令

negotiation (4-76)
capabilities (flowcontrol, symmetric) (4-77)

4.3.8.7 shutdown

使用此命令可以禁用接口。使用此命令的 **no** 形式可重新启动禁用的接口。

语法

shutdown
no shutdown

默认设置

所有接口都已启用。

命令模式

接口配置 （以太网、端口通道）

命令用法

此命令可用于禁用出现异常情况 （如冲突过多）的端口，并在问题得到解决后重新启用该端口。有时出于安全考虑，您可能也想禁用某个端口。

示例

以下示例禁用以太网端口 SNP5。

```
Console(config)#interface ethernet SNP5
Console(config-if)#shutdown
Console(config-if)#
```

4.3.8.8 switchport broadcast packet-rate

使用此命令可以配置广播风暴控制。使用此命令的 **no** 形式可以禁用广播风暴控制。

语法

switchport broadcast packet-rate *rate*
no switchport broadcast

rate — 速率的阈值级别；即每秒传递的数据包数。（范围：16、 64、 128、 256）

默认设置

为所有端口启用
每秒传递 256 个数据包

命令模式

接口配置 （以太网）

命令用法

- 如果广播通信量超过指定的阈值，则超出阈值的那些数据包将被删除。
- 此命令可以对选定接口启用或禁用广播风暴控制。不过，指定的阈值会应用于整个交换机。
- 下行链接端口 SNP0-15 会始终启用广播风暴控制。

示例

以下命令显示了如何将广播抑制配置为每秒传递 64 个数据包：

```
Console(config)#interface ethernet SNP5
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#
```

注：请注意， **switchport broadcast** 命令可对指定接口启用广播风暴控制，但它同时也会为交换机上的每个接口设置广播阈值。

4.3.8.9 clear counters

使用此命令可以清除接口的统计信息。

语法

clear counters *interface*

interface - **ethernet** *port-name*

port-name — 下行链接：SNP0-15 ； 上行链接：NETP0-7 ； mgt：NETMGT

默认设置

无

命令模式

特权执行

命令用法

统计信息只在电源重置时才会初始化。此命令将当前管理会话显示的统计信息的基值设置为零。不过，如果您注销之后再重新登录到管理界面，则显示的统计信息将显示自上次电源重置以来累计的所有值。

示例

以下示例清除了端口 SNP5 的统计信息。

```
Console#clear counters ethernet SNP5
Console#
```

4.3.8.10 show interfaces status

使用此命令可以显示接口的状态。

语法

show interfaces status [*interface*]

interface

- **ethernet** *port-name*

  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）
- **vlan** *vlan-id*（范围：1-4094）

默认设置

显示所有接口的状态。

命令模式

普通执行、特权执行

命令用法

如果未指定任何接口，将显示所有接口的信息。有关此命令所显示项目的说明，请参阅第 3-75 页上的“显示连接状态”。

示例

```
Console#show interfaces status ethernet SNP11
Information of SNP11
Basic information:
  Port type: 1000SX
  Mac address: 00-00-e8-00-00-0a
 Configuration:
  Name: Blade Slot 11
  Port admin status: Up
Speed-duplex: Auto
  Capabilities: 1000full,
Broadcast storm status: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control status: Enabled
  Lacp status: Disabled
 Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: Dot3X
Console#
```

4.3.8.11 show interfaces counters

使用此命令可以显示接口的统计信息。

语法

show interfaces counters [*interface*]

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

显示所有接口的计数器。

命令模式

普通执行、特权执行

命令用法

如果未指定任何接口，将显示所有接口的信息。有关此命令所显示项目的说明，请参阅第 3-112 页上的 “显示端口统计信息”。

示例

```
Console#show interfaces counters ethernet NETP7
NETP7:
 Iftable stats:
  Octets input: 19648, Octets output: 714944
  Unicast input: 0, Unicast output: 0
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 10524
  Broadcast input: 136, Broadcast output: 0
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
RMON stats:
  Drop events: 0, Octets: 734720, Packets: 10661
  Broadcast pkts: 136, Multi-cast pkts: 10525
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 9877, Packet size 65 to 127 octets: 93
  Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

4.3.8.12 show interfaces switchport

使用此命令可以显示高级的接口配置设置。

语法

show interfaces switchport [*interface*]

interface

- **ethernet** *port-name*

  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

显示所有接口。

命令模式

普通执行、特权执行

命令用法

如果未指定任何接口，将显示所有接口的信息。此命令所显示的项目包括：

- **广播阈值** — 显示是否已启用广播风暴抑制；如果已启用，还将显示阈值级别（第 4-80 页）。
- **Lacp 状态** — 显示是否已启用“链接聚合控制协议”（第 4-144 页）。
- **VLAN 成员模式** — 指出成员模式是“聚合组”还是“混合”（第 4-107 页）。
- **入口规则** — 显示是否已启用入口过滤（第 4-108 页）。
- **可接受的帧类型** — 显示可接受的 VLAN 帧是包括所有类型的帧还是只包括带标记的帧（第 4-108 页）。
- **本地 VLAN** — 指明默认的“端口 VLAN ID”（第 4-109 页）。
- **无标记通信的优先级** — 指明无标记帧的默认优先级（第 4-130 页）。
- **Gvrp 状态** — 显示是否已启用“GARP VLAN 注册协议（第 4-113 页）。
- **允许的 Vlan** — 显示此接口所加入的 VLAN，其中“(u)”表示无标记；“(t)”表示有标记（第 4-110 页）。
- **禁止的 Vlan** — 显示此接口无法通过 GVRP 动态加入的 VLAN（第 4-111 页）。

示例

此示例显示以太网端口 NETP7 的配置设置。

```
Console#show interfaces switchport ethernet NETP7
Information of NETP7
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Enabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Enabled
 Allowed Vlan: 1(u),
 Forbidden Vlan:    2,
Console#
```

4.3.9 地址表命令

这些命令用于配置地址表，使其用于过滤指定的地址、显示当前条目、清除地址表或设置地址表的有效期。

命令	功能	模式	页码
mac-address-table static	将静态地址映射为 VLAN 中的一个端口	GC	4-87
clear mac-address-table dynamic	从转发数据库中删除所有了解到的条目	PE	4-88
show mac-address-table	显示网桥转发数据库中的条目	PE	4-88
mac-address-table aging-time	设置地址表的有效期	GC	4-89
show mac-address-table aging-time	显示地址表的有效期	PE	4-90

4.3.9.1 mac-address-table static

使用此命令可以将静态地址映射到目标端口。使用此命令的 **no** 形式可以删除地址。

语法

mac-address-table static *mac-address* {**interface** *interface*} **vlan** *vlan-id* [*action*]
no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* — MAC 地址。
- *interface*
  - **ethernet** *port-name*
    port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
  - **port-channel** *channel-id*（范围：1-6）
- *vlan-id* - VLAN ID（范围：1-4094）
- *action* —
  - **permanent** — 地址分配是永久性分配。
  - **delete-on-reset** — 地址分配持续到交换机重置时为止。

默认设置

未定义任何静态地址。默认模式为 permanent。

命令模式

全局配置

命令用法

- 主机设备的静态地址可以分配给特定 VLAN 内的特定端口。使用此命令可以将静态地址添加到 MAC 地址表中。静态地址具有以下特征：
  - 当给定的接口链接断开时，静态地址不会从地址表中删除。
  - 静态地址与指定的接口绑定在一起，因此不会被移动。当在另一个接口上看到静态地址时，将忽略该地址，并且不会将它写入地址表。
  - 不能在一个端口上了解另一个端口上的静态地址，除非已使用此命令的 **no** 形式将该地址删除掉。

示例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
ethernet SNP1 vlan 1 delete-on-reset
Console(config)#
```

4.3.9.2 clear mac-address-table dynamic

使用此命令可以删除转发数据库中所有已了解到的条目，并清除所有静态配置条目或系统配置条目的发送计数和接收计数。

默认设置

无

命令模式

特权执行

示例

```
Console#clear mac-address-table dynamic
Console#
```

4.3.9.3 show mac-address-table

使用此命令可以查看网桥转发数据库的条目类别。

语法

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* — MAC 地址。
- *mask* — 地址中应该忽略的位。
- *interface*
  - **ethernet** *port-name*
    port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
  - **port-channel** *channel-id*（范围：1-6）
- *vlan-id* — VLAN ID（范围：1-4094）
- **sort** — 按照地址、VLAN 或接口进行排序。

默认设置

无

命令模式

特权执行

命令用法

MAC 地址表包含与每个接口相关的 MAC 地址。注意 “Type”（类型）字段可能包括以下类型：

- Learned — 动态地址条目
- Permanent — 静态条目
- Delete-on-reset — 将在系统重置时删除的静态条目

示例

```
Console#show mac-address-table
Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
     SNP11 00-10-b5-62-03-74    1 Learned
Console#
```

4.3.9.4 mac-address-table aging-time

使用此命令可以为地址表中的条目设置有效期。使用此命令的 **no** 形式可以恢复默认的有效期。

语法

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds — 时间以秒数表示 (18-2184)。

默认设置

300 秒

命令模式

全局配置

命令用法

通过设置有效期，可使动态了解到的转发信息过期。

示例

```
Console(config)#mac-address-table aging-time 300
Console(config)#
```

4.3.9.5 show mac-address-table aging-time

使用此命令可以显示地址表中条目的有效期。

默认设置

无

命令模式

特权执行

示例

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

4.3.10 端口安全性命令

这些命令可用于禁用了解功能或手动指定端口的安全地址。在初期培训阶段，您最好禁用端口安全性（即启用了解功能），以便注册选定端口上的当前所有 VLAN 成员。之后，再启用端口安全性，以确保端口将删除所有具有以下特点的传入帧：其源 MAC 地址未知或是从另一端口上了解到的。

命令	功能	模式	页码
port security	配置安全端口	IC	4-91
mac-address-table static	将静态地址映射为 VLAN 中的一个端口	GC	4-87
show mac-address-table	显示网桥转发数据库中的条目	PE	4-88

4.3.10.1 port security

使用此命令可以配置安全端口。使用此命令的 **no** 形式可以禁用端口安全性。

语法

port security
no port security

默认设置

所有端口安全性都已禁用。

命令模式

接口配置 （以太网）

命令用法

- 如果启用端口安全性，交换机将停止动态了解指定端口上的新地址。仅接受那些源地址已存储在动态地址表或静态地址表中的传入通信。
- 要使用端口安全性，首先要允许交换机动态了解用于初始培训阶段的端口上所接收的 < 源 MAC 地址， VLAN> 对，然后再启用端口安全性，以停止了解地址的操作。务必将了解功能的启用时间设置得足够长，这样才能确保所有有效 VLAN 成员都已在选定端口上注册。
- 要在以后添加新的 VLAN 成员，可以手动使用 **mac-address-table static** 命令添加安全地址，或关闭端口安全性，以重新启用了解功能，而且时间足够新 VLAN 成员进行注册。然后可以根据需要再次禁用了解功能，以确保安全。
- 安全端口具有以下限制：
  - 不能使用端口监视功能。
  - 不能是多 VLAN 端口。
  - 不能连接到网络互连设备。
  - 不能是聚合组端口。

示例

以下示例启用了端口 SNP5 上的端口安全性功能：

```
Console(config)#interface ethernet SNP5
Console(config-if)#port security
```

相关命令

mac-address-table static (4-87)
show mac-address-table (4-88)

4.3.11 生成树命令

本节介绍用于配置整个交换机的生成树算法 (STA) 的命令，以及用于配置选定接口的 STA 的命令。

命令	功能	模式	页码
spanning-tree	启用生成树协议	GC	4-92
spanning-tree mode	配置 STP 或 RSTP 模式	GC	4-93
spanning-tree forward-time	配置生成树网桥的转发时间	GC	4-94
spanning-tree hello-time	配置生成树网桥的问候时间	GC	4-95
spanning-tree max-age	配置生成树网桥的最长时限	GC	4-95
spanning-tree priority	配置生成树网桥的优先级	GC	4-96
spanning-tree path-cost method	配置 RSTP 的路径成本方法	GC	4-97
spanning-tree transmission-limit	配置 RSTP 的发送限制	GC	4-97
spanning-tree cost	配置接口的生成树路径成本	IC	4-98
spanning-tree port-priority	配置接口的生成树优先级	IC	4-99
spanning-tree edge-port	启用边缘端口的快速转发功能	IC	4-100
spanning-tree protocol-migration	重新检查有关的 BPDU 格式	PE	4-100
spanning-tree link-type	配置 RSTP 的链接类型	IC	4-101
show spanning-tree	显示生成树配置	PE	4-102

4.3.11.1 spanning-tree

使用此命令可以为交换机全局启用生成树算法。使用此命令的 **no** 形式可禁用它。

语法

spanning-tree
no spanning-tree

默认设置

启用生成树。

命令模式

全局配置

命令用法

生成树算法可用于检测和禁用网络环路，并提供交换机、网桥或路由器之间的备份链接。这样，交换机就可以与网络中的其它桥接设备（即，与 STA 兼容的交换机、网桥或路由器）交互，以确保网络中任意两个工作站之间只存在一条路线，并提供备份链接（以便在主链接出现故障时自动接管其功能）。

示例

以下示例将为此交换机启用生成树算法：

```
Console(config)#spanning-tree
Console(config)#
```

4.3.11.2 spanning-tree mode

使用此命令可以为此交换机选择生成树模式。使用此命令的 **no** 形式可以恢复默认值。

语法

spanning-tree mode {**stp** | **rstp**}
no spanning-tree mode

- **stp** — 生成树协议 (IEEE 802.1D)
- **rstp** — 快速生成树 (IEEE 802.1w)

默认设置

stp

命令模式

全局配置

命令用法

- 快速生成树协议

  RSTP 通过监视传入的协议消息并动态调整 RSTP 节点所发送的协议消息类型，支持到 STP 节点或 RSTP 节点的连接。具体情况如下：

  - STP模式 — 如果交换机在某端口的迁移延迟计时器到期之后接收到一个802.1D BPDU，则交换机将假设它所连接的是 802.1D 网桥并开始仅使用 802.1D BPDU。
  - RSTP 模式 — 如果 RSTP 正在某端口使用 802.1D BPDU，并在迁移延迟到期后接收到一个 RSTP BPDU， RSTP 会重新启动迁移延迟计时器，并开始在该端口上使用 RSTP BPDU。

示例

以下示例对交换机进行配置，使之使用快速生成树：

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

4.3.11.3 spanning-tree forward-time

使用此命令可以为交换机全局配置生成树网桥转发时间。使用此命令的 **no** 形式可以恢复默认值。

语法

spanning-tree forward-time *seconds*
no spanning-tree forward-time

seconds — 时间 （按秒计）。（范围：4-30 秒）
最小值取 4 或 [(max-age / 2) + 1] 这两者中的较大值。

默认设置

15 秒

命令模式

全局配置

命令用法

此命令设置根设备在改变状态 （即，放弃 - 了解 - 转发）之前将等待的最长时间（以秒计）。这种延迟是必需的，因为每台设备在开始转发帧之前，都必须接收有关拓扑结构更改的信息。此外，每个端口也需要时间来侦听将会使其返回到放弃状态的冲突信息；否则，将可能出现暂时的数据环路。

示例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

4.3.11.4 spanning-tree hello-time

使用此命令可以为交换机全局配置生成树网桥的问候时间。使用此命令的 **no** 形式可以恢复默认值。

语法

spanning-tree hello-time *time*
no spanning-tree hello-time

time — 时间 （按秒计）。（范围：1-10 秒）
最大值取 10 或 [(max-age / 2) -1] 这两者中的较小值。

默认设置

2 秒

命令模式

全局配置

命令用法

此命令设置根设备发送配置消息的时间间隔 （以秒计）。

示例

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

4.3.11.5 spanning-tree max-age

使用此命令可为此交换机全局配置生成树网桥的最长存在时间。使用此命令的 **no** 形式可以恢复默认值。

语法

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds — 时间 （按秒计）。（范围：6-40 秒）
最小值取 6 或 [2 x (hello-time + 1)] 这两者中的较大值。
最大值取 40 或 [2 x (forward-time - 1)] 这两者中的较小值。

默认设置

20 秒

命令模式

全局配置

命令用法

此命令设置设备在试图重新配置之前，如果未接收到配置消息可以等待的最长时间（以秒计）。所有设备端口（指定端口除外）都应定期接收到配置消息。任何在 STA 信息（在最后一个配置消息中提供）之前过期的端口都会变为其所连接的 LAN 的指定端口。如果该端口曾经是根端口，将会从当前连接到网络的各个设备端口中间选定一个新的根端口。

示例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

4.3.11.6 spanning-tree priority

使用此命令可为此交换机全局配置生成树优先级。使用此命令的 **no** 形式可以恢复默认值。

语法

spanning-tree priority *priority*
no spanning-tree priority

priority — 网桥的优先级。
（范围：0-61440，步进值为 4096；选项有： 0、 4096、 8192、 12288、 16384、 20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440）

默认设置

32768

命令模式

全局配置

命令用法

网桥优先级用于选择根设备、根端口和指定端口。具有最高优先级的设备会变为 STA 根设备。不过，如果所有设备的优先级相同，那么具有最低 MAC 地址的设备将变为根设备。

示例

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

4.3.11.7 spanning-tree pathcost method

使用此命令可以配置用于快速生成树的路径成本方法。使用 **no** 形式可以恢复默认值。

语法

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** — 指定基于 32 位的值，范围：从 1 到 200,000,000。
- **short** — 指定基于 16 位的值，范围：从 1 到 65535。

默认设置

短方法

命令模式

全局配置

命令用法

路径成本方法用于确定设备之间的最佳路径。因此，应为连接到较快介质的端口指定较低的值，为连接到较慢介质的端口指定较高的值。请注意，应优先考虑路径成本 （第 4-98 页），然后再考虑端口优先级 （第 4-99 页）。

示例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

4.3.11.8 spanning-tree transmission-limit

使用此命令可以配置发送连续的 RSTP BPDU 之间的最短时间间隔。使用 **no** 形式可以恢复默认值。

语法

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count — 发送的时间限制 （按秒计）。（范围：1-10）

默认设置

3

命令模式

全局配置

命令用法

此命令限制了 BPDU 的最高发送速率。

示例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

4.3.11.9 spanning-tree cost

使用此命令可以配置指定接口的生成树路径成本。使用 **no** 形式可以恢复默认值。

语法

spanning-tree cost *cost*
no spanning-tree cost

cost — 接口的路径成本。
（范围：1-200,000,000）
建议范围为 —

- 以太网：200,000-20,000,000
- 快速以太网：20,000-2,000,000
- 千兆位以太网：2,000-200,000

默认设置

- 以太网 — 半双工：2,000,000；全双工：1,000,000；聚合组：500,000
- 快速以太网 — 半双工：200,000；全双工：100,000；聚合组：50,000
- 千兆位以太网 — 全双工：10,000；聚合组：5,000

命令模式

接口配置 （以太网、端口通道）

命令用法

- 此命令供生成树算法用来确定设备之间的最佳路径。因此，应为连接到较快介质的接口指定较低的值，为连接到较慢介质的接口指定较高的值。
- 应优先考虑路径成本，然后再考虑接口的优先级。
- 如果生成树路径成本方法设置为 **short**，则路径成本的最大值为 65,535。

示例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

相关命令

spanning-tree port-priority (4-99)

4.3.11.10 spanning-tree port-priority

使用此命令可以配置指定接口的优先级。使用 **no** 形式可以恢复默认值。

语法

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority — 接口的优先级。（范围：0-240，其步进值为 16）

默认设置

128

命令模式

接口配置 （以太网、端口通道）

命令用法

- 此命令定义了在生成树算法中使用接口的优先级。如果交换机上所有接口的路径成本都相同，那么将把具有最高优先级 （即，值最低）的接口配置为生成树中的活动链接。
- 如果具有最高优先级的接口不止一个，则启用具有最低数字标识符的接口。

示例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

相关命令

spanning-tree cost (4-98)

4.3.11.11 spanning-tree edge-port

使用此命令可以将接口指定为边缘端口。使用 **no** 形式可以恢复默认值。

语法

spanning-tree edge-port
no spanning-tree edge-port

默认设置

NETP0-7， NETMGT：禁用
SNP0-15：启用 （在此设置中是固定的）

命令模式

接口配置 （以太网、端口通道）

命令用法

如果接口所连接的是位于桥接 LAN 末端的 LAN 网段或者是末端节点，则可以启用此选项。由于末端节点无法导致转发环路，因此它们可以直接进入生成树转发状态。指定边缘端口的好处有四：第一，使各种设备（如工作站或服务器）能更快地收敛；第二，保留了当前的转发数据库，从而减少了在重新配置事件过程中为重建地址表而需要的帧扩散量；第三，不会导致生成树在接口改变状态时启动重新配置操作；第四，解决了与 STA 相关的其它超时问题。不过，应谨记只能对连接到末端节点设备的端口启用“边缘端口”功能。

示例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

4.3.11.12 spanning-tree protocol-migration

使用此命令可以重新检查选定接口上要发送的 BPDU 格式是否合适。

语法

spanning-tree protocol-migration *interface*

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15 ； 上行链接：NETP0-7 ； mgt：NETMGT
- **port-channel** *channel-id* （范围：1-6）

命令模式

特权执行

命令用法

只要交换机检测到 STP BPDU （包括配置 BPDU 或拓扑结构更改通知 BPDU），它就会自动将选定接口设置为强制的 STP 兼容模式。不过，也可以随时使用 **spanning-tree protocol-migration** 命令手动重新检查选定接口上要发送的 BPDU 格式是否合适 （即， RSTP 或 STP 兼容）。

示例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

4.3.11.13 spanning-tree link-type

使用此命令可以配置快速生成树的链接类型。使用 **no** 形式可以恢复默认值。

语法

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** — 自动从双工模式设置得出。
- **point-to-point** — 点对点链接。
- **shared** — 共享介质。

默认设置

auto

命令模式

接口配置 （以太网、端口通道）

命令用法

- 如果接口只能连接到另外的一个网桥上，则指定点对点链接；如果接口能连接到两个或更多网桥，则可以指定共享链接。
- 如果选定了自动检测，交换机将从双工模式中得出链接类型。全双工接口被当作点对点链接，而半双工接口则被当作共享链接。
- RSTP 只在两个网桥之间的点对点链接中才起作用。如果将端口指定为共享链接，则会禁用 RSTP。

示例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

4.3.11.14 show spanning-tree

使用此命令可以显示生成树的配置。

语法

show spanning-tree [*interface*]

- *interface*
  - **ethernet** *port-name*
    port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
  - **port-channel** *channel-id*（范围：1-6）

默认设置

无

命令模式

特权执行

命令用法

- 使用不带参数的 **show spanning-tree** 命令可以显示交换机的生成树配置和生成树中每个接口的生成树配置。
- 使用 **show spanning-tree** *interface* 命令可以显示接口的生成树配置。
- 有关“网桥组信息”下显示的各个项目的说明，请参阅第 3-53 页上的“配置基本 STA 设置”。有关为特定接口显示的各个项目的说明，请参阅第 3-98 页上的“管理生成树算法的接口”。

示例

```
Console#show spanning-tree
Bridge-group information
---------------------------------------------------------
 Spanning tree mode                :RSTP
 Spanning tree enable/disable      :enable
 Priority                          :32768
 Bridge Hello Time (sec.)          :2
 Bridge Max Age (sec.)             :20
 Bridge Forward Delay (sec.)       :15
 Root Hello Time (sec.)            :2
 Root Max Age (sec.)               :20
 Root Forward Delay (sec.)         :15
 Designated Root                   :8.0000E8666672
 Current root port                 :0
 Current root cost                 :0
 Number of topology changes        :0
 Last topology changes time (sec.):1363
 Transmission limit                :3
 Path Cost Mothod                  :21
---------------------------------------------------------
SNP0 information
---------------------------------------------------------
 Admin status          : enable
 Role                  : designate
 State                 : forwarding
 Path cost             : 10000
 Priority              : 128
 Designated cost       : 0
 Designated port       : 8.1
 Designated root       : 8.0000E8666672
 Designated bridge     : 8.0000E8666672
 Forward transitions   : 0
 Admin edge port       : disable
 Oper edge port        : disable
 Admin Link type       : point-to-point
 Oper Link type        : point-to-point
.
.
.
Console#
```

4.3.12 VLAN 命令

VLAN 是指一组端口，它们可位于网络中的任意位置，但它们进行通信时却好像属于同一个物理网段。本节介绍一些命令，用于创建 VLAN 组、添加端口成员、指定如何使用 VLAN 标记以及为选定接口启用自动 VLAN 注册。

命令	功能	模式	页码
编辑 VLAN 组			
vlan database	进入 VLAN 数据库模式，以添加、更改和删除 VLAN	GC	4-105
vlan	配置 VLAN，包括 VID、名称和状态	VC	4-105
配置 VLAN 接口			
interface vlan	为指定 VLAN 而进入接口配置模式	GC	4-106
switchport mode	为接口配置 VLAN 成员模式	IC	4-107
switchport acceptable-frame-types	配置接口所要接受的帧类型	IC	4-108
swicthport ingress-filtering	在接口上启用入口过滤功能	IC	4-108
switchport native vlan	配置接口的 PVID （本地 VLAN）	IC	4-109
switchport allowed vlan	配置与接口关联的 VLAN	IC	4-110
switchport gvrp	为接口启用 GVRP	IC	4-113
switchport forbidden vlan	为接口配置禁用的 VLAN	IC	4-111
显示 VLAN 信息			
show vlan	显示 VLAN 信息	NE、PE	4-112
show interfaces status vlan	显示指定 VLAN 接口的状态	NE、PE	4-82
show interfaces switchport	显示接口的管理状态和运行状态	NE、PE	4-85

4.3.12.1 vlan database

使用此命令可以进入 VLAN 数据库模式。此模式下的所有命令将立即生效。

默认设置

无

命令模式

全局配置

命令用法

- 使用 VLAN 数据库命令模式可以添加、更改和删除 VLAN。完成配置更改后，可以通过输入 **show vlan** 命令来显示 VLAN 设置。
- 使用 **interface vlan** 命令模式可以定义端口成员模式，并向 VLAN 中添加端口或从中删除端口。这些命令的结果将写入运行配置文件。输入 **show running-config** 命令即可显示此文件。

示例

```
Console(config)#vlan database
Console(config-vlan)#
```

相关命令

show vlan (4-112)

4.3.12.2 vlan

使用此命令可以配置 VLAN。使用此命令的 **no** 形式可以恢复默认设置或删除 VLAN。

语法

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* — 已配置的 VLAN 的 ID。（范围：1-4094，无前导零）
- **name** — 位于 VLAN 名称之前的关键字。
  - vlan-name — ASCII 字符串，长度为 1 到 15 个字符。
- **media ethernet** — 以太网介质类型。
- **state** — 位于 VLAN 状态之前的关键字。
  - **active** — VLAN 可操作。
  - **suspend** — VLAN 挂起。 VLAN 挂起后，将不传递数据包。

默认设置

默认情况下只有 VLAN 1，并且处于活动状态。

命令模式

VLAN 数据库配置

命令用法

- **no vlan** *vlan-id* 可删除 VLAN。
- **no vlan** *vlan-id* **name** 可删除 VLAN 名称。
- **no vlan** *vlan-id* **state** 可让 VLAN 返回默认状态 （即活动状态）。
- VLAN 1 不能被挂起，但任何其它 VLAN 都可以被挂起。
- 在交换机上可以配置多达 255 个 VLAN。

示例

以下示例添加了一个 VLAN，它的 vlan-id 为 105，名称为 RD5。默认情况下，该 VLAN 处于活动状态。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

相关命令

show vlan (4-112)

4.3.12.3 interface vlan

使用此命令可以进入 VLAN 的接口配置模式，从而配置物理接口。

语法

interface vlan *vlan-id*

vlan-id — 已配置的 VLAN 的 ID。（范围：1-4094，无前导零）

默认设置

无

命令模式

全局配置

示例

以下示例说明如何将接口配置模式设置为 VLAN 1，然后为该 VLAN 指定一个 IP 地址：

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

相关命令

shutdown (4-80)

4.3.12.4 switchport mode

使用此命令可以配置端口的 VLAN 成员模式。使用 **no** 形式可以恢复默认值。

语法

switchport mode {**trunk** | **hybrid**}
no switchport mode

- **trunk** — 将端口指定为 VLAN 聚合组的端点。聚合组是指两台交换机之间的直接链接，因此端口发送的是标识源 VLAN 的标记帧。不过请注意，如果帧属于端口的默认 VLAN （即与 PVID 关联的 VLAN），则发送帧时将不对其进行标记。
- **hybrid** — 指定混合 VLAN 接口。此类端口可以发送带标记或不带标记的帧。

默认设置

所有端口都处于混合模式下，而且 PVID 均设置为 VLAN 1。

命令模式

接口配置 （以太网、端口通道）

示例

以下示例说明如何先为端口 SNP1 设置配置模式，然后将交换机端口模式设置为混合：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

4.3.12.5 switchport acceptable-frame-types

使用此命令可以配置端口所能接受的帧类型。使用 **no** 形式可以恢复默认值。

语法

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** — 端口接收所有类型的帧，不管带有标记还是不带标记。
- **tagged** — 端口只接收带标记的帧。

默认设置

所有帧类型

命令模式

接口配置 （以太网、端口通道）

命令用法

如果设置为接收所有类型的帧，那么所有接收到的未带标记的帧都将分配给默认 VLAN。

示例

以下示例显示如何对端口 SNP1 上的通信进行限制，使其仅接收带标记的帧：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

4.3.12.6 switchport ingress-filtering

使用此命令可以为接口启用入口过滤功能。使用 **no** 形式可以恢复默认值。

语法

switchport ingress-filtering
no switchport ingress-filtering

默认设置

禁用

命令模式

接口配置 （以太网、端口通道）

命令用法

- 入口过滤措施只影响带标记的帧。
- 如果禁用入口过滤功能，接口将接收任何带 VLAN 标记的帧，只要该标记与交换机所能识别的某个 VLAN （此端口上明确禁止的 VLAN 除外）匹配即可。
- 如果启用了入口过滤功能，但传入帧的 VLAN 标记所指向的 VLAN 中未包含此入口端口，则该传入帧将被丢弃。
- 入口过滤功能不会影响与 VLAN 无关的 BPDU 帧，如 GVRP 或 STP。不过，入口过滤功能确实会影响与 VLAN 相关的 BPDU 帧，如 GMRP。

示例

以下示例说明如何先将接口设置为端口 SNP1，然后再启用入口过滤功能：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

4.3.12.7 switchport native vlan

使用此命令可以配置接口的 PVID （即默认 VID）。使用 **no** 形式可以恢复默认值。

语法

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id — 接口的默认 VLAN ID。（范围：1-4094，无前导零）

默认设置

VLAN 1

命令模式

接口配置 （以太网、端口通道）

命令用法

- 如果接口不是 VLAN 1 的成员，并且您已将其 PVID 指定为此 VLAN，那么会自动将该接口作为不带标记的成员添加到 VLAN 1 中。对于所有其它 VLAN，必须先将某个接口配置成一个不带标记的成员，然后再将该接口的 PVID 指定到给该组。
- 如果将可接受的帧类型设置为 **all**，或将交换机端口模式设置为 **hybrid**，那么 PVID 将被插入进入入口端口的所有不带标记的帧中。

示例

以下示例显示如何将端口 SNP1 的 PVID 设置为 VLAN 3：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

4.3.12.8 switchport allowed vlan

使用此命令可以配置选定接口上的 VLAN 组。使用 **no** 形式可以恢复默认值。

语法

switchport allowed vlan {**add** *vlan* [**tagged** | **untagged**] | **remove** *vlan*}

- **add** *vlan* — 要添加的 VLAN 标识符。
- **remove** *vlan* — 要删除的 VLAN 标识符。

  请勿输入前导零。（范围：1-4094）

no switchport allowed vlan

注意：不能对 NETMGT 端口使用 **no switchport allowed vlan** 命令。（如果对 NETMGT 端口使用了此命令，交换机将显示错误消息。）要使管理端口恢复使用出厂默认 VLAN （即 VLAN 2），并将该管理端口从其已加入的所有其它 VLAN 中删除掉，请键入以下命令：

```
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 2
Console(config-if)#switchport native vlan 2
Console(config-if)#switchport allowed vlan remove <vlan id>
```

其中 *<vlan id>* 是除 VLAN 2 之外的、而且您已将 NETMGT 端口添加到其中的 VLAN 的编号。（对于其中仍包含 NETMGT 端口的每一个 VLAN （但 VLAN 2 除外），都重复执行最后那条命令。）

默认设置

- 默认情况下，所有端口 （NETMGT 除外）都将分配给 VLAN 1。
  默认情况下，将把 NETMGT 端口分配给 VLAN 2。
- 默认帧类型是不带标记的帧。

命令模式

接口配置 （以太网、端口通道）

命令用法

- 如果交换机端口模式设置为 **trunk**，那么只能将一个接口作为带标记的成员分配给 VLAN 组。
- 在交换机内，帧始终带有标记。将一个 VLAN 添加到某个接口时会使用带标记 / 不带标记的参数。该参数将指示交换机在将帧发送出去时是保留还是删除帧的标记。
- 如果所有中间网络设备以及连接另一端的主机都不支持 VLAN，那么该接口应作为不带标记的成员添加到这些 VLAN 中。否则，至多只需添加一个 VLAN （作为不带标记的成员），并且该 VLAN 应对应于该接口的本地 VLAN。
- 如果 VLAN 包括在某个接口的禁止列表上，但该 VLAN 又被手动添加到了该接口，那么该 VLAN 会自动从该接口的禁止列表中删除掉。

示例

以下示例说明了如何将 VLAN 1、 VLAN 2、 VLAN 5 和 VLAN 6 作为带标记的 VLAN 添加到端口 SNP1 的允许列表中：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport allowed vlan add 1 tagged
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 5 tagged
Console(config-if)#switchport allowed vlan add 6 tagged
Console(config-if)#
```

4.3.12.9 switchport forbidden vlan

使用此命令可以配置禁止的 VLAN。使用此命令的 **no** 形式可以删除遭禁 VLAN 的列表。

语法

switchport forbidden vlan {**add** *vlan* | **remove** *vlan*}
no switchport forbidden vlan

- **add** *vlan* — 要添加的 VLAN ID。
- **remove** *vlan* — 要删除的 VLAN ID。

  请勿输入前导零。（范围：1-4094）

默认设置

禁止列表中没有 VLAN。

命令模式

接口配置 （以太网、端口通道）

命令用法

- 此命令阻止通过 GVRP 将 VLAN 自动添加到指定的接口上。
- 如果某个 VLAN 已名列某个接口的允许 VLAN 组中，就不能将它添加到该接口的禁止 VLAN 组中。

示例

以下示例说明如何阻止将端口 SNP1 添加到 VLAN 3 中：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

4.3.12.10 show vlan

使用此命令可以显示 VLAN 信息。

语法

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** — 位于 VLAN ID 之前的关键字。
  - *vlan-id* — 已配置的 VLAN 的 ID。（范围：1-4094，无前导零）
- **name** — 位于 VLAN 名称之前的关键字。
  - *vlan-name* — ASCII 字符串，长度为 1 到 15 个字符。

默认设置

显示所有 VLAN。

命令模式

普通执行、特权执行

示例

以下示例说明如何显示 VLAN 1 的信息：

```
Console#show vlan id 1
VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ----------------------------------------
   1  Static      DefaultVlan    Active    SNP0    SNP1    SNP2    SNP3    SNP4
                                           SNP5    SNP6    SNP7    SNP8    SNP9
                                          SNP10   SNP11   SNP12   SNP13   SNP14
                                          SNP15   NETP0   NETP1   NETP2   NETP3
                                          NETP4   NETP5   NETP6   NETP7
   2  Static          MgtVlan    Active  NETMGT
Console#
```

4.3.13 GVRP 和网桥扩展命令

GARP VLAN 注册协议 (GVRP) 定义了交换机之间交换 VLAN 信息的方式，以便实现在整个网络的所有接口上自动注册 VLAN 成员。本节介绍如何为单个接口启用 GVRP、如何为交换机全局启用 GVRP，以及如何显示网桥扩展 MIB 的默认配置设置。

命令	功能	模式	页码
接口命令			
switchport gvrp	为接口启用 GVRP	IC	4-113
switchport forbidden vlan	为接口配置禁用的 VLAN	IC	4-111
show gvrp configuration	显示选定接口的 GVRP 配置	NE、PE	4-114
garp timer	为选定功能设置 GARP 计时器	IC	4-115
show garp timer	显示选定功能的 GARP 计时器	NE、PE	4-116
全局命令			
bridge-ext gvrp	为交换机全局启用 GVRP	GC	4-117
show bridge-ext	显示网桥扩展配置	PE	4-117

4.3.13.1 switchport gvrp

使用此命令可为端口启用 GVRP。使用此命令的 **no** 形式可禁用它。

语法

switchport gvrp
no switchport gvrp

默认设置

启用

命令模式

接口配置 （以太网、端口通道）

示例

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport gvrp
Console(config-if)#
```

4.3.13.2 show gvrp configuration

使用此命令可以显示是否已启用 GVRP。

语法

show gvrp configuration [*interface*]

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

既显示全局配置，又显示特定于接口的配置。

命令模式

普通执行、特权执行

示例

```
Console#show gvrp configuration
Whole system:
GVRP configuration: Enabled
SNP0:
 Gvrp configuration: Enabled
SNP1:
 Gvrp configuration: Enabled
.
.
.
```

4.3.13.3 garp timer

使用此命令可以设置 jion 计时器、 leave 计时器和 leaveall 计时器的值。使用此命令的 **no** 形式可以恢复计时器的默认值。

语法

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} — 要设置的计时器。
- *timer_value* — 计时器的值。
  范围：
  - join 计时器：20-1000 厘秒
  - leave 计时器：60-3000 厘秒
  - leaveall 计时器：500-18000 厘秒

默认设置

- join 计时器：20 厘秒
- leave 计时器：60 厘秒
- leaveall 计时器：1000 厘秒

命令模式

接口配置 （以太网、端口通道）

命令用法

- GVRP和GMRP使用组地址注册协议(GARP)来为桥接LAN内的客户机服务注册或取消注册客户机属性。 GARP 定时器的默认值独立于介质访问方法或数据速率。除非您在注册 / 取消注册 GMRP 或 GVRP 的过程中遇到困难，否则不应更改这些值。
- 计时器值应用于所有 VLAN 上所有端口的 GVRP。
- 计时器值必须满足以下条件：
  - leave >= (2 x join)
  - leaveall > leave

注：将连接到同一网络的所有 2 层设备上的 GVRP 计时器设置为相同的值。否则，GVRP 将无法成功运行。

示例

```
Console(config)#interface ethernet SNP1
Console(config-if)#garp timer join 100
Console(config-if)#
```

相关命令

show garp timer (4-116)

4.3.13.4 show garp timer

使用此命令可以显示选定接口的 GARP 计时器。

语法

show garp timer [*interface*]

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

显示所有 GARP 计时器。

命令模式

普通执行、特权执行

示例

```
Console#show garp timer ethernet SNP1
SNP1 GARP timer status:
 Join timer: 20 sec.
 Leave timer: 60 sec.
 Leaveall timer: 1000 sec.
Console#
```

相关命令

garp timer (4-115)

4.3.13.5 bridge-ext gvrp

使用此命令可为交换机全局启用 GVRP。使用此命令的 **no** 形式可禁用它。

语法

bridge-ext gvrp
no bridge-ext gvrp

默认设置

启用

命令模式

全局配置

命令用法

GVRP 定义了交换机之间互换 VLAN 信息的方式，以便实现在整个网络的所有端口上注册 VLAN 成员。应启用此功能，以便自动进行 VLAN 注册，并支持扩展到本地交换机之外的 VLAN。

示例

```
Console(config)#bridge-ext gvrp
Console(config)#
```

4.3.13.6 show bridge-ext

使用此命令可以显示网桥扩展命令的配置。

默认设置

无

命令模式

特权执行

命令用法

运行此命令后将显示一些项目，下面对这些项目的含义进行了解释：

- **Max support vlan numbers** — 此交换机根据 IEEE 802.1Q 标准的规定而使用的 VLAN 版本。
- **Max support vlan ID** — 此交换机识别的最大 VLAN ID。
- **Extended multicast filtering services** — 此交换机不支持过滤单个的多点传送地址 （根据 GMRP，即 GARP 多点传送注册协议）。
- **Static entry individual port** — 此交换机允许静态过滤单点传送地址和多点传送地址 （请参阅第 4-87 页和第 4-120 页）。
- **VLAN learning** — 此交换机使用“独立式 VLAN 了解”(Independent VLAN Learning, IVL) 模式，在这种模式下每个端口都维护各自的过滤数据库。
- **Configurable PVID tagging** — 此交换机允许您覆盖每个端口上的默认端口 VLAN ID （帧标记中使用的 PVID）和出口状态 （带 VLAN 标记或不带 VLAN 标记）（第 4-109 页）。
- **Local VLAN capable** — 此项指的是交换机为多个生成树提供的支持。目前，还不支持多个生成树。
- **Traffic classes** — 此交换机能够将用户优先级映射为多个通信类别 （第 4-132 页）。
- **Global GVRP status** — GARP VLAN 注册协议 (GVRP) 定义了交换机之间交换 VLAN 信息的方式，以便实现在整个网络的端口上注册必需的 VLAN 成员。应启用此功能，以便支持扩展到本地交换机之外的 VLAN 组 （第 4-117 页）。
- **GMRP** — GARP多点传送注册协议(GMRP)允许网络设备向多点传送组注册终端站。此交换机不支持 GMRP ；它通过因特网组管理协议 (IGMP) 来自动进行多点传送过滤。

示例

```
Console#show bridge-ext
 Max support vlan numbers: 255
 Max support vlan ID: 4094
 Extended multicast filtering services: No
 Static entry individual port: Yes
 VLAN learning: IVL
 Configurable PVID tagging: Yes
 Local VLAN capable: Yes
 Traffic classes: Enabled
 Global GVRP status: Enabled
 GMRP: Disabled
Console#
```

4.3.14 IGMP 侦听命令

此交换机使用 IGMP（因特网组管理协议）在所连接的主机中查询那些想接收特定多点传送服务的主机。它可识别请求服务的主机所在的端口，并只将数据发送到这些端口。然后，此交换机将服务请求向上传播给任何相邻的多点传送交换机/路由器，以确保它将继续接收多点传送服务。

命令	功能	模式	页码
基本的 IGMP 命令			
ip igmp snooping	启用 IGMP 侦听	GC	4-120
ip igmp snooping vlan static	将接口作为多点传送组的一个成员进行添加	GC	4-120
ip igmp snooping version	配置用于侦听的 IGMP 版本	GC	4-121
show ip igmp snooping	显示 IGMP 侦听配置	PE	4-122
show bridge multicast	显示 IGMP 侦听 MAC 多点传送列表	PE	4-122
IGMP 查询器命令			
ip igmp snooping querier	允许此设备充当 IGMP 侦听的查询器	GC	4-123
ip igmp snooping query-count	配置查询计数	GC	4-124
ip igmp snooping query-interval	配置查询时间间隔	GC	4-125
ip igmp snooping query-max-response-time	配置报告延迟时间	GC	4-125
ip igmp snooping router-port-expire-time	配置查询超时时间	GC	4-126
show ip igmp snooping	显示 IGMP 侦听配置	PE	4-122
多点传送路由器命令			
ip igmp snooping vlan mrouter	添加一个多点传送路由器端口	GC	4-127
show ip igmp snooping mrouter	显示多点传送路由器端口	PE	4-128

4.3.14.1 ip igmp snooping

使用此命令可以在此交换机上启用 IGMP 侦听功能。使用此命令的 **no** 形式可禁用它。

语法

ip igmp snooping
no ip igmp snooping

默认设置

禁用

命令模式

全局配置

示例

以下示例启用了 IGMP 侦听功能。

```
Console(config)#ip igmp snooping
Console(config)#
```

4.3.14.2 ip igmp snooping vlan static

使用此命令可以将端口添加到多点传送组中。使用此命令的 **no** 形式可以删除端口。

语法

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan vlan-id static *ip-address interface*

- *vlan-id* — VLAN ID（范围：1-4094）
- *ip-address* — 多点传送组的 IP 地址
- *interface*
  - **ethernet** *port-name*
    port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
  - **port-channel** *channel-id*（范围：1-6）

默认设置

无

命令模式

全局配置

示例

以下示例显示如何在端口上静态配置多点传送组：

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet SNP5
Console(config)#
```

4.3.14.3 ip igmp snooping version

使用此命令可以配置 IGMP 侦听版本。使用 **no** 形式可以恢复默认值。

语法

ip igmp snooping version {**1** | **2**}
no ip igmp snooping version

- **1** — IGMP 版本 1
- **2** — IGMP 版本 2

默认设置

IGMP 版本 2

命令模式

全局配置

命令用法

- 子网上的所有系统必须支持同一版本。如果您的网络上的旧设备只支持版本 1，则必须将此交换机配置为使用版本 1。
- 有些命令只能为IGMPv2启用，包括**ip igmp query-max-response-time**命令和**ip igmp query-timeout** 命令。

示例

以下示例将交换机配置为使用 IGMP 版本 1：

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

4.3.14.4 show ip igmp snooping

使用此命令可以显示 IGMP 侦听配置。

默认设置

无

命令模式

特权执行

命令用法

有关对所显示项目的说明，请参阅第 3-43 页上的 “配置 IGMP 侦听参数”。

示例

以下示例显示了当前的 IGMP 侦听配置：

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Query time-out: 300 sec
 IGMP snooping version: Version 2
Console#
```

4.3.14.5 show mac-address-table multicast

使用此命令可以显示已知的多点传送地址。

语法

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* — VLAN ID（1 到 4094）
- **user** — 只显示用户配置的多点传送条目。
- **igmp-snooping** — 只显示通过 IGMP 侦听了解到的条目。

默认设置

无

命令模式

特权执行

命令用法

显示的成员类型包括 IGMP 或 USER，具体情况取决于选定的选项。

示例

以下示例显示了通过 IGMP 侦听了解到的网桥组 1（VLAN 1）的多点传送条目：

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr.Member ports Type
 ---- --------------- ------------ -------
    1      224.0.0.12        NETP0    USER
    1       224.1.2.3        NETP1    IGMP
Console#
```

4.3.14.6 ip igmp snooping querier

使用此命令可以将交换机作为 IGMP 侦听查询器启用。使用此命令的 **no** 形式可禁用它。

语法

ip igmp snooping querier
no ip igmp snooping querier

默认设置

禁用

命令模式

全局配置

命令用法

如果启用此功能，选定的交换机将用作查询器。查询器负责询问主机是否想接收多点传送通信。

示例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

4.3.14.7 ip igmp snooping query-count

使用此命令可以配置查询计数。使用 **no** 形式可以恢复默认值。

语法

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count — 在查询器采取措施从多点传送组中删除客户机之前，它所发出但没收到响应的查询的最大数量。（范围：2-10）

默认设置

2 次

命令模式

全局配置

命令用法

查询计数定义了查询器在采取措施之前，将花多长时间等待多点传送客户机的响应。如果查询器已发送出了许多由该命令定义的查询，但客户机一直没有相应，则会启动一个倒计时器，该计时器的时间由 **ip igmp snooping query-max-response-time** 定义。如果倒计时结束，客户机依然没有做出响应，则会认为该客户机已离开多点传送组。

示例

以下示例显示了如何将查询计数配置为 10：

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

相关命令

ip igmp snooping query-max-response-time (4-125)

4.3.14.8 ip igmp snooping query-interval

使用此命令可以配置侦听查询的时间间隔。使用 **no** 形式可以恢复默认值。

语法

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds — 交换机发送 IGMP 主机查询消息的频率。（范围：60-125）

默认设置

125 秒

命令模式

全局配置

示例

以下示例说明了如何将查询时间间隔配置为 100 秒：

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

4.3.14.9 ip igmp snooping query-max-response-time

使用此命令可以配置侦听报告的延迟时间。使用此命令的 **no** 形式可以恢复默认值。

语法

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds — 在 IGMP 查询中公布的报告延迟时间。（范围：5-25）

默认设置

10 秒

命令模式

全局配置

命令用法

- 交换机必须使用 IGMPv2，然后此命令才能生效。
- 此命令定义了发出查询之后，预期要多长时间才能得到多点传送客户机的响应。如果查询器发出了由 **ip igmp snooping query-count** 定义的许多查询，但某个客户机一直没有响应，则会启动一个倒计时器，该倒计时器将使用此命令设置的初始秒数。如果倒计时结束，客户机依然没有做出响应，则会认为该客户机已离开多点传送组。

示例

以下示例说明了如何将最大响应时间配置为 20 秒：

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

相关命令

ip igmp snooping version (4-121)
ip igmp snooping query-max-response-time (4-125)

4.3.14.10 ip igmp snooping router-port-expire-time

使用此命令可以配置侦听查询的超时时间。使用此命令的 **no** 形式可以恢复默认值。

语法

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds — 在前一个查询器停止查询之后，交换机用于确信 （用于接收查询数据包的）接口已不再与该查询器之间存在连接的等待时间。（范围：300-500）

默认设置

300 秒

命令模式

全局配置

命令用法

交换机必须使用 IGMPv2，然后此命令才能生效。

示例

以下示例说明了如何将超时时间配置为 500 秒：

```
Console(config)#ip igmp snooping router-port-expire-time 500
Console(config)#
```

相关命令

ip igmp snooping version (4-121)

4.3.14.11 ip igmp snooping vlan mrouter

使用此命令可以静态配置多点传送路由器端口。使用此命令的 **no** 形式可以删除配置。

语法

ip igmp snooping vlan *vlan-id* **mrouter** *interface*
no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* — VLAN ID （范围：1-4094）
- *interface*
  - **ethernet** *port-name*

    port-name — 下行链接：SNP0-15 ； 上行链接：NETP0-7 ； mgt：NETMGT
  - **port-channel** *channel-id* （范围：1-6）

默认设置

没有配置静态多点传送路由器端口。

命令模式

全局配置

命令用法

根据网络连接的情况不同， IGMP 侦听可能始终无法找到 IGMP 查询器。因此，如果 IGMP 查询器是一个已知的多点传送路由器 / 交换机，而且它通过网络连接到您的交换机上某个接口 （端口或聚合组），则可以手动将该接口进行配置，使之加入当前所有的多点传送组。

示例

以下示例说明如何将端口 11 配置为 VLAN 1 中的一个多点传送路由器端口：

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0
Console(config)#
```

4.3.14.12 show ip igmp snooping mrouter

使用此命令可以显示有关静态配置的多点传送路由器端口和动态了解的多点传送路由器端口的信息。

语法

show ip igmp snooping mrouter [vlan *vlan-id***]**

vlan-id — VLAN ID（范围：1-4094）

默认设置

为已配置的所有 VLAN 显示多点传送路由器端口。

命令模式

特权执行

命令用法

所显示的多点传送路由器端口类型包括静态或动态两种。

示例

以下示例显示了连接到多点传送路由器的端口：

```
Console#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1               NETP5  Static
    2               NETP6  Dynamic
Console#
```

4.3.15 优先级命令

本节介绍的命令用于指定当数据通信由于发生拥塞被缓存于交换机之中时，哪些数据包的优先权更高。此交换机为每个端口提供具有四种优先级队列的 CoS。端口的高优先级队列中的数据包将先于低优先级队列中的数据包发送。可以设置每个接口的默认优先级、每个队列的相对加权，还可将帧优先级标记映射到交换机的优先级队列中。

命令	功能	模式	页码
2 层优先级命令			
switchport priority default	为传入的且未加标记的帧设置端口优先级	IC	4-130
queue bandwidth	为各优先级队列指定轮询加权	GC	4-131
queue cos map	为优先级队列指定服务类别值	IC	4-132
show queue bandwidth	显示指定给优先级队列的轮询加权	PE	4-133
show queue cos-map	显示服务类别映射	PE	4-134
show interfaces switchport	显示接口的管理状态和运行状态	PE	4-85
3 层和 4 层优先级命令			
map ip precedence	启用 IP 优先权服务类别映射	GC	4-135
map ip precedence	将 IP 优先权值映射为某个服务类别	IC	4-135
map ip dscp	启用 IP DSCP 服务类别映射	GC	4-136
map ip dscp	将 IP DSCP 值映射为某个服务类别	IC	4-137
show map ip precedence	显示 IP 优先权映射	PE	4-138
show map ip dscp	显示 IP DSCP 映射	PE	4-139

4.3.15.1 switchport priority default

使用此命令可为传入的且未带标记的帧设置优先级，或为连接到指定接口的设备所接收到的帧设置优先级。使用此命令的 **no** 形式可以恢复默认值。

语法

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id — 未标记的入口通信的优先级编号。优先级的范围为 0 到 7。数字 7 表示最高的优先级。

默认设置

未设置优先级，接口上收到的未带标记的帧的默认值为零。

命令模式

接口配置 （以太网、端口通道）

命令用法

- 用于优先级映射的优先权是IP优先权或IP DSCP，以及默认的交换机端口优先级。
- 默认优先级适用于经设置应接收所有帧类型 （即接收带标记的和未带标记的帧）的端口所接收的未带标记的帧。这种优先级不适用于 IEEE 802.1Q VLAN 带标记帧。如果传入帧是 IEEE 802.1Q VLAN 带标记帧，将使用 IEEE 802.1p 用户优先级位。
- 此交换机为每个端口提供四种优先级队列。已对此交换机进行配置，使之使用“加权轮询”。可使用 **queue bandwidth** 命令查看加权轮询。不带 VLAN 标记的入站帧会先用输入端口的默认入口用户优先级进行标记，然后才被放在输出端口的相应优先级队列中。所有传入端口的默认优先级为零。因此，所有未带优先级标记的入站帧都将被放入输出端口的队列 0 中。（请注意，如果输出端口是相关 VLAN 的未带标记的成员，那么这些帧在发送之前将被去掉所有 VLAN 标记。）

示例

以下示例显示了如何将端口 SNP3 的默认优先级设置为 5：

```
Console(config)#interface ethernet SNP3
Console (config-if)#switchport priority default 5
```

4.3.15.2 queue bandwidth

使用此命令可为四个服务类别 (CoS) 优先级队列指定 “加权轮询” (WRR) 权级。使用此命令的 **no** 形式可以恢复默认权级。

语法

queue bandwidth *weight1...weight4*
no queue bandwidth

weight1...weight4 — 队列 0 至队列 3 的权级比例决定了 WRR 调度程序所使用的权级。（范围：1-255）

默认设置

权级 16、 64、 128 和 240 分别分配给队列 0、 1、 2 和 3。

命令模式

全局配置

命令用法

WRR 通过定义调度权级，从而允许在传出端口进行带宽共享。

示例

以下示例说明了如何将 WRR 权级 1、3、5、7 指定给 CoS 优先级队列 0、1、2、3：

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

相关命令

show queue bandwidth (4-133)

4.3.15.3 queue cos-map

使用此命令可以将服务类别 (CoS) 值指定给 CoS 优先级队列。使用此命令的 **no** 形式可将 CoS 映射设置为默认值。

语法

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* — CoS 优先级队列的队列 ID。
  其范围从 0 到 3，其中 3 是级别最高的 CoS 优先级队列。
- *cos1 .. cosn* — 映射为队列 ID 的 CoS 值。它是一个数字列表，而且各数字之间用空格隔开。 CoS 值的范围是从 0 到 7，其中 7 的优先级最高。

默认设置

此交换机通过将四个优先级队列和加权轮询排队结合使用，从而为每个端口提供服务类别。 IEEE 802.1p 中定义了八个独立的通信类别。应按照 IEEE 802.1p 标准中的建议分配默认优先级，如下表所示。

	队列			
	0	**1**	**2**	**3**
优先级		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

命令模式

接口配置 （以太网、端口通道）

命令用法

在传入端口指定的 CoS 用于选择传出端口的 CoS 优先级。

示例

以下示例说明了如何将 CoS 值 0、 1 和 2 映射到 CoS 优先级队列 0、将值 3 映射到 CoS 优先级队列 1、将值 4 和 5 映射到 CoS 优先级队列 2、将值 6 和 7 映射到 CoS 优先级队列 3：

```
Console(config)#interface ethernet SNP1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

相关命令

show queue cos-map (4-134)

4.3.15.4 show queue bandwidth

使用此命令可以显示四个服务类别 (CoS) 优先级队列的加权轮询 (WRR) 带宽分配情况。

默认设置

无

命令模式

特权执行

示例

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
    0        16
    1        64
    2        128
    3        240
Console#
```

4.3.15.5 show queue cos-map

使用此命令可以显示服务类别优先级映射。

语法

show queue cos-map [*interface*]

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

无

命令模式

特权执行

示例

```
Console#show queue cos-map ethernet SNP11
Information of SNP11
 Queue ID Traffic class
 -------- -------------
    0     1 2
    1     0 3
    2     4 5
    3     6 7
Console#
```

4.3.15.6 map ip precedence （全局配置）

使用此命令可以启用 IP 优先权映射 （即， IP 服务类型）。使用此命令的 **no** 形式可以禁用 IP 优先权映射。

语法

map ip precedence
no map ip precedence

默认设置

启用

命令模式

全局配置

命令用法

- 用于优先级映射的优先权是IP优先权或IP DSCP，以及默认的交换机端口优先级。
- IP 优先权和 IP DSCP 不能同时启用。启用其中一个优先级类型将会自动禁用另一个优先级类型。

示例

以下示例说明如何全局启用 IP 优先权映射：

```
Console(config)#map ip precedence
Console(config)#
```

4.3.15.7 map ip precedence （接口配置）

使用此命令可以设置 IP 优先权的优先级 （即 IP 服务类别的优先级）。使用此命令的 **no** 形式可以恢复默认表。

语法

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* — 3 位的优先权值。（范围：0-7）
- *cos-value* — 服务类别值 （范围：0-7）

默认设置

一对一映射 （即，优先权值 0 映射到 CoS 值 0，依此类推）

命令模式

接口配置 （以太网、端口通道）

命令用法

- 用于优先级映射的优先权是IP优先权或IP DSCP，以及默认的交换机端口优先级。
- 根据一对一的原则以及IEEE 802.1p 标准中的建议，将IP优先权值映射到默认的服务类别值，然后再将其映射到队列默认值。
- IP 优先权特定值的映射会作为一条接口配置命令实施，但任何更改都会应用于交换机的所有接口。

示例

以下示例说明如何将 IP 优先权值 1 映射到 CoS 值 0：

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

4.3.15.8 map ip dscp （全局配置）

使用此命令可以启用 IP DSCP 映射 （即 “差别化业务编码点”映射）。使用此命令的 **no** 形式可以禁用 IP DSCP 映射。

语法

map ip dscp
no map ip dscp

默认设置

启用

命令模式

全局配置

命令用法

- 用于优先级映射的优先权是IP优先权或IP DSCP，以及默认的交换机端口优先级。
- IP 优先权和 IP DSCP 不能同时启用。启用其中一个优先级类型将会自动禁用另一个优先级类型。

示例

以下示例说明如何全局启用 IP DSCP 映射：

```
Console(config)#map ip dscp
Console(config)#
```

4.3.15.9 map ip dscp （接口配置）

使用此命令可以设置 IP DSCP 优先级 （即 “差别化业务编码点”优先级）。使用此命令的 **no** 形式可以恢复默认表。

语法

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* — 8 位的 DSCP 值。（范围：0-255）
- *cos-value* — 服务类别值 （范围：0-7）

默认设置

下表定义了 DSCP 默认值。请注意，所有未指定的 DSCP 值都将映射到 CoS 值 0。

IP DSCP 值	CoS 值
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

命令模式

接口配置 （以太网、端口通道）

命令用法

- 用于优先级映射的优先权是IP优先权或IP DSCP，以及默认的交换机端口优先级。
- 按照 IEEE 802.1p 标准中的建议，将 DSCP 优先级值映射到默认服务类别值，然后再将其映射到队列默认值。
- DSCP 特定值的映射会作为一条接口配置命令实施，但任何更改都会应用于交换机的所有接口。

示例

以下示例说明如何将 IP DSCP 值 1 映射到 CoS 值 0：

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

4.3.15.10 show map ip precedence

使用此命令可以显示 IP 优先权的优先级映射。

语法

show map ip precedence [*interface*]

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

无

命令模式

特权执行

示例

```
Console#show map ip precedence ethernet SNP5
Precedence mapping status:disabled

 Port          Precedence COS
 -----------   ---------- ---
        SNP5            0   0
        SNP5            1   1
        SNP5            2   2
        SNP5            3   3
        SNP5            4   4
        SNP5            5   5
        SNP5            6   6
        SNP5            7   7
Console#
```

相关命令

map ip precedence（全局配置）(4-135)
map ip precedence（接口配置）(4-135)

4.3.15.11 show map ip dscp

使用此命令可以显示 IP DSCP 的优先级映射。

语法

show map ip dscp [*interface*]

interface

- **ethernet** *port-name*
  port-name — 下行链接：SNP0-15；上行链接：NETP0-7；mgt：NETMGT
- **port-channel** *channel-id*（范围：1-6）

默认设置

无

命令模式

特权执行

示例

```
Console#show map ip dscp ethernet SNP1
DSCP mapping status:disabled

 Port         DSCP COS
 ------------ ---- ---
        SNP1     0   0
        SNP1     1   0
        SNP1     2   0
        SNP1     3   0
.
.
.
        SNP1    61   0
        SNP1    62   0
        SNP1    63   0
Console#
```

相关命令

map ip dscp（全局配置）(4-136)
map ip dscp（接口配置）(4-137)

4.3.16 镜像端口命令

本节说明如何将通信从源端口镜像到目标端口。

命令	功能	模式	页码
port monitor	配置镜像会话	IC	4-140
show port monitor	显示镜像端口的配置	PE	4-141

4.3.16.1 port monitor

使用此命令可以配置镜像会话。使用此命令的 **no** 形式可清除镜像会话。

注：Sun Fire B1600 刀片式系统机箱上的集成交换机中都包含两块链接在一起的交换机芯片。若要镜像某个端口上的通信，只能使用该端口所在交换机芯片上的其它端口才有可能实现。端口 NETP0、NETP1、NETP4、NETP5 以及 SNP8 到 SNP15 在同一交换机芯片上。端口 NETP、NETP3、NETP6、NETP7 以及 SNP0 到 SNP7 位于另一交换机芯片上。（如果您查看 SSC 的后面板，则将看到右侧的所有端口位于一块芯片上，而左侧的所有端口位于另一块芯片上。）

语法

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *port-name*
  port-name — 下行链接：SNP0-15 ； 上行链接：NETP0-7 ； mgt：NETMGT
  （此接口为源端口。）
- **rx** — 镜像所收到的数据包。
- **tx** — 镜像所发送的数据包。
- **both** — 镜像收到的和发送的数据包。

默认设置

未定义任何镜像会话。启用后，将对收到的和发送的数据包都默认进行镜像。

命令模式

接口配置 （以太网，目标端口）

命令用法

- 可将通信从源端口镜像到目标端口，以便进行实时分析。然后，可在目标端口上连接一个逻辑分析器或 RMON 探测器，并在完全不进行干预的情况下研究通过源端口的通信。
- 目标端口是通过指定以太网接口来设置的。

示例

以下示例对从端口 SNP6 至端口 NETP2 的所有数据包都进行镜像：

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6 both
Console(config-if)#
```

相关命令

show port monitor (4-141)

4.3.16.2 show port monitor

使用此命令可显示镜像信息。

语法

show port monitor [*interface*]

interface - **ethernet** *port-name*

port-name — 下行链接：SNP0-15 ； 上行链接：NETP0-7 ； mgt：NETMGT

（此接口为源端口。）

默认设置

显示所有会话

命令模式

特权执行

命令用法

此命令将显示当前所配置的源端口、目标端口和镜像模式 （即， RX、 TX、 RX/TX）。

示例

以下示例显示从端口 SNP6 至端口 NETP2 进行的镜像：

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):NETP2
 Source port(monitored port)  :SNP6
 Mode                         :RX/TX
Console#
```

相关命令

port monitor (4-140)

4.3.17 端口聚合命令

可将端口静态地纳入聚合链接 （即，聚合组），以增加网络连接的带宽或确保能从故障中恢复。或者，您也可使用 “链路聚合控制协议” (LACP) 在此交换机和另一网络设备之间自动协商聚合组链接。对于静态聚合组，交换机必须属于同一类型。而对于动态聚合组，交换机则只需符合 LACP 的要求即可。此交换机支持多达六个聚合组。例如，在全双工模式下，由两个 1000 Mbps 端口组成的聚合组可支持高达 4 Gbps 的总带宽。

命令	功能	模式	页码
手动配置命令			
interface port-channel	配置聚合组并进入聚合组的接口配置模式	GC	4-74
channel-group	在聚合组中添加端口	IC	4-143
动态配置命令			
lacp	为当前接口配置 LACP	IC	4-144
聚合组状态显示命令			
show interfaces status port-channel	显示聚合组信息	NE、PE	4-82

聚合组创建指南

- 在交换机之间连接相应的网线之前，请先完成对端口聚合组的配置，以免形成环路。
- 一个聚合组可包含多达四个上行链接端口或两个下行链接端口。
- 必须对各连接两端的端口进行配置，使之变为聚合组端口。
- 同一聚合组中的所有端口必须采用相同的方式进行配置，包括通信模式 （即，速度、双工模式和流量控制）、 VLAN 分配情况和 CoS 设置。
- 在通过指定的端口通道将同一聚合组中的所有端口移入 / 移出 VLAN 时，或将其添加到 VLAN 中或从中删除时，必须将所有端口当做一个整体来处理。
- 只能通过指定的端口通道对整个聚合组进行 STP、VLAN 和 IGMP 等方面的设置。

4.3.17.1 channel-group

使用此命令可将端口添加到静态聚合组中。使用此命令的 **no** 形式可从聚合组中删除端口。

语法

channel-group *channel-id*
no channel-group

channel-id — 聚合组索引 （范围：1-6）

默认设置

当前端口将添加到此聚合组中。

命令模式

接口配置 （以太网）

命令用法

- 配置静态聚合组时，只能对同一类型的交换机进行链接。
- 使用 **no channel-group** 可从聚合组中删除端口组。
- 使用 **no interfaces port-channel** 可从交换机中删除聚合组。

示例

以下示例先创建聚合组 1，然后再添加端口 NETP2：

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#channel-group 1
Console(config-if)#
```

4.3.17.2 lacp

使用此命令可为当前接口启用 802.3ad “链路聚合控制协议” (LACP)。使用此命令的 **no** 形式可禁用它。

语法

lacp
no lacp

默认设置

Enabled

命令模式

接口配置 （以太网）

命令用法

- 对于 LACP 聚合组两端的端口，必须通过强制模式或自动协商模式进行全双工配置。
- 对于使用 LACP 与另一交换机一起组成的聚合组，将自动为其分配下一个可用的端口通道 ID。
- 如果目标交换机也已在连接端口上启用 LACP，则将自动激活聚合组。
- 如果连接到同一目标交换机的端口中有四个以上的端口启用了 LACP，则其它端口将进入备用模式，而且仅当活动链接出现故障后才会启用。

示例

以下示例表明端口 NETP0-2 上启用了 LACP。由于链接另一端的端口上也启用了 LACP，因此， **show interfaces status port-channel 1** 命令表明聚合组 1 已建立。

```
Console(config)#interface ethernet NETP0
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port type: 1000t
  Mac address: 00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full
  Flow control status: Disabled
 Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex:1000full
  Flow control type:None
  Member Ports:NETP0, NETP1, NETP2,
Console#
```

第III部分 附录

本节介绍关于下列主题的附加信息。

管理信息库

故障排除

规格

附录 **A**

管理信息库

SNMP 管理站可以通过设置或读取在管理信息库 (MIB) 中指定的设备变量来配置和监控网络设备。本附录中列出了该交换机支持的主要 MIB 组。同时，请注意，在第 3 章“管理概述”中还列出了每种配置任务所使用的 MIB 变量。

A.1 支持的 MIB

下表中列出了各种标准 MIB。

RFC 编号	名称	支持的组
1213	MIB-II	• 系统组 • 接口组 • ip 组 • icmp 组 • tcp 组 • udp 组 • snmp 组
1493	Bridge MIB	• dot1dBase 组 • dot1dStp 组 • dot1dTp 组 • dot1dStatic 组
2863	Interfaces Evolution MIB	• ifXTable 组 • ifStackTable 组
2819	RMON MIB	• 统计信息组 • 历史记录组 • 警报组 • 事件组

RFC 编号	名称	支持的组
2618	RADIUS MIB	• radiusAuthClientMIB
2665	Etherlike MIB	• dot3StatsTable 组
2737	Entity MIB	• entityPhysical 组
2674	P-bridge	• dot1dExtBase 组 • dot1dPriority 组 • dot1dGarp 组
2674	Q-bridge	• dot1qBase 组 • dot1qTp 组 • dot1qStatic 组 • dot1qVlan

下面列出了 Sun 专有 Enterprise MIB。

名称	版本
CSSP.MIB	01.00.00

A.2 支持的陷阱

支持的 SNMP 陷阱包括以下各项：

RFC 编号	名称
RFC 1215 (SNMPv1)，RFC 1907 (SNMPv2c)	• coldStart • linkDown • linkUp • authenticationFailure
RFC 1493	• newRoot • topologyChange
RFC 2819	• risingAlarm • fallingAlarm

所支持的 Sun 专有 Enterprise 陷阱包括以下项：

RFC 编号	名称
CSSP.MIB	• swPowerStatusChangeTrap

附录 **B**

故障排除

如果在连接网络时遇到问题，请检查网络布线，以确保您怀疑有问题的设备正确连到网络上。然后，请参阅第 B-1 页上的 “诊断交换机指示灯”以验证交换机上的相应端口是否正常运行。

如果连接到管理界面时遇到问题，请参阅第 B-2 页上的 “访问管理界面”下的故障排除图表。

B.1 诊断交换机指示灯

如果某台设备已连接到交换机上的某个端口，但 “链路指示灯”不亮，请检查下列各项：

- 确保电缆已插入到交换机和相应的设备中。
- 验证所使用的电缆类型正确，且其长度未超过指定限制。
- 检查所挂接的设备上的适配器和电缆连接是否可能存在缺陷。如果需要，请替换有缺陷的适配器或电缆。

验证是否已正确安装了所有系统组件。如果任何网络布线出现异常，请在备用环境中对其进行测试 （必须确保备用环境中的其它所有组件工作正常）。

B.2 诊断端口连接

如果端口不工作，请检查下列各项：

- 电缆连接是否牢固，且电缆是否已连接到链路两端的正确端口上。
- 端口状态 (Admin) 是否已启用，是否启用了自动协商功能，或者链路两端的端口是否已配置为相同的速度和双工模式。有关详细信息，请参阅第 3-75 页上的 “端口配置”。

B.3 访问管理界面

使用 Telnet、 Web 浏览器或任何基于 SNMP 的网络管理软件，可以从所连接的网络中的任何位置访问交换机的管理界面。如果访问管理界面时遇到问题，请参阅下面显示的故障排除信息。

如果使用 Telnet、 Web 浏览器或 SNMP 软件无法进行连接，请检查下列各项：

- 确保服务器机箱已接通电源。
- 检查管理站和交换机之间的网络布线。
- 检查与交换机之间的网络连接正确有效，并确保要使用的端口未被禁用。请参阅第 3-75 页上的 “端口配置”。
- 如果管理站和服务器机箱之间只存在第 2 层交换机，应确保：
  - 已使用有效的 IP 地址和子网掩码配置交换机的管理 VLAN。
  - 管理站在管理 VLAN 所处的同一子网中具有一个 IP 地址。
  - 管理站所连接的交换机端口是管理 VLAN 的成员。
  - 连接网络中的中间交换机的端口是带标记的端口，同时也是管理 VLAN 的成员。
- 如果管理站和服务器机箱之间存在一个或多个第 3 层交换机，应确保：
  - 已使用有效的 IP 地址、子网掩码和默认网关配置交换机的管理 VLAN。
  - 管理站具有有效的 IP 地址、子网掩码和默认网关。
  - 管理站所连接的交换机端口是管理 VLAN 的成员。
  - 用来连接网络中的中间交换机和第 3 层交换机的端口是带标记的端口，同时也是管理 VLAN 的成员。
- 如果不能使用 Telnet 进行连接，则可能已经超出所允许的最大并发 Telnet 会话数。请稍后重试连接。

如果通过串行端口连接无法访问板载配置程序，请检查下列各项：

- 使用随 Sun Fire B1600 刀片式机箱一起提供的 DB-9 到 RJ-45 电缆，将您的终端或计算机连接到 SSC 模块上的串行端口。
- 确保已将终端仿真器程序设置为 VT100 兼容、8 个数据位、1 个停止位、无奇偶校验和 9600 bps。
- 检查空的调制解调器串行电缆是否与附录 B 中提供的管脚引线相符。

B.4 使用系统日志

如果出现故障，请参阅服务器机箱的其它手册，以确保所遇到的问题确实是由交换机引起的。如果问题看起来是由交换机引起的，请按照下述步骤操作。

1. 启用日志记录。
2. 设置所报告的错误消息，使之包含所有类别。
3. 指定将接收错误消息的 SNMP 主机。
4. 重复导致错误的命令序列或其它操作。
5. 列出导致故障的命令或情况。此外，还应列出所显示的全部错误消息。
6. 与客户服务人员联系。

示例

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 10.1.0.23
.
.
.
```

B.4.1 日志消息

下表中列出了此交换机生成的日志消息：

表 B-1 日志消息

消息	说明	级别 *
System coldStart notification	交换机冷引导。	5
System warmStart notification	交换机热引导。	5
Unit 1 Port YY link-up notification	端口链接建立。	6
Unit 1 Port YY link-down notification	端口链接断开。	6
Trunk 1 link-up notification	聚合组链接建立。	6
Trunk 1 link-down notification	聚合组链接断开。	6
VLAN XX link-up notification	VLAN 链接建立。	6
VLAN XX link-down notification	VLAN 链接断开。	6
Authentication failure notification	SNMP 访问验证失败。	6
STA root change notification	STA 根更改。	6
STA topology change notification	STA 拓扑发生变化。	6
RMON rising alarm notification	RMON 上升警报。	6
RMON falling alarm notification	RMON 下降警报。	6

Unit 1 Port YY 指装置 1，端口 YY（YY：1 到 25）。
VLAN XX 指某个 VLAN ID 值（XX：1 到 4094）。

* 系统日志消息级别（请参阅第 4-31 页上的“logging history”。）

B.5 错误消息

B.5.1 命令行错误检测

如果交换机检测到命令行中有无效输入，它会在检测到错误的位置下方显示一个“^”。例如，

```
Console#show interfaces statuss e 1/1
                                  ^
% Invalid input detected at '^' marker.
```

B.5.2 系统错误

下表中列出了此交换机生成的主要错误消息。要控制交换机发出的消息级别，请参阅第 4-31 页上的 “logging history”。

表 B-2 系统错误消息

消息	说明	级别 *
<module> create task fail.	指定的软件模块不能创建任务。	2
<module> task idle too long.	指定的软件模块保持空闲状态的时间太长。	2
Allocate <string> memory fail.	为指定的 <String> 分配内存失败。	2
Free <string> memory fail.	为指定的 <String> 释放内存失败。	2
<string> switch to default.	指定的值无效或不受支持；将使用默认值。（有关可接受的值的信息，请参阅联机帮助或本手册。）	3

module 指交换机软件模块 （例如， STA、 VLAN、 XFER、 TRAP 或 RMON）。
string 指的是为配置设置指定的值。

* 系统日志消息级别 （请参阅第 4-31 页上的 “logging history”。）

B.5.3 命令行错误

下表中列出了此交换机生成的命令行界面错误消息。请注意，这些消息未写入日志文件中。

表 B-3 命令行错误消息

消息	说明
Ambiguous command: <string>	命令含糊不清。
Clear dynamic address error.	无法清除动态地址。
CLI internal error - contact your local service provider.	CLI 命令内部错误。
Copy error.	复制操作失败。
Exec-timeout could not be disabled for vty session.	Telnet 会话不能禁用执行超时。
Factory default configuration file cannot be deleted.	不能删除出厂默认文件。
Factory default configuration file cannot be replaced.	不能替换出厂配置文件。
Failed to allocate resource.	资源不足。
Failed to get <string>	show 命令失败。
Failed to set <string>	配置命令失败。
Failed to write certificate file to flash.	证书文件存在错误，私钥文件出现错误 （如密码不正确），或私钥与证书公钥不匹配。
Incomplete command.	命令不完整。
Insufficient memory.	内存不足。
Insufficient memory to display or save running config.	没有足够的空间可用来搜集所有信息。
Invalid file name.	输入的的文件名无效。
Invalid input.	键盘输入错误。
Invalid input detected at '^' marker.	命令无效。
Invalid parameter.	Ping 参数错误。
Invalid parameter value/range.Type “?” to get more detail information.	采用了不允许的值或字符串长度。
Invalid TFTP server IP address.	TFTP IP 地址错误。
Not enough resources; please try later.	Ping 功能没有资源。
No such file.	系统没有该文件。

表 B-3 命令行错误消息 *（续）*

消息	说明
No such VLAN.	VLAN 不存在。
Port <port name> does not exist.	端口名不存在。
Port <port name> is an ethernet port.	端口为以太网端口。
Port <port name> is not present.	进入界面模式时端口不存在。
Port <port name> unknown.	端口为未知端口。
Session terminated.	CLI 退出当前会话。
Session timed out.	连接会话超时。
Startup file cannot be deleted.	不能删除启动文件。
This command for console only.	行模式 (vty) 不能使用控制台参数命令。
This command is only valid for adding a single port to a trunk.	使用此命令只能将一个端口添加到聚合组中。
This command is only valid for the name of a single port.	设置端口说明时，不接受多端口选择。
This command is not supported for management port in current release.	“no switchport allow vlan”命令不能用于管理端口。
Trunk ID:<trunk> is out of range.	不允许使用此聚合组 ID。
Trunk <trunk> does not exist.	聚合组不存在。
Trunk <trunk> is a normal trunk.	聚合组为普通聚合组。
Trunk with no members cannot be displayed.	无法配置或显示聚合组成员。
Type “show ?“ for a list of subcommands.	您只输入了 “show”命令。
Unknown error.	未知错误。
Unrecognized command.	命令无法识别。

<string> 指的是为命令指定的值。

B.5.4 Web 界面错误

下表中列出了此交换机生成的 Web 界面错误消息。请注意，这些消息未写入日志文件中。

表 B-4 Web 界面错误消息

菜单	消息	说明
Switch Setup		
System Identity	User privileges are not enough to perform this operation.	权限不足。
Network Identity	Current IP Address Mode is not DHCP or BOOTP.	重新启动 DHCP 时，交换机必须处于 DHCP 或 BOOTP 模式。
	Data is invalid.	一般错误。
	Set DHCP Client-ID error.	未能设置 DHCP 客户机 ID。
	User privileges are not enough to perform this operation.	权限不足。
Software	Data is invalid.	一般错误。
	Please input a destination file.	输入要下载或上载的目标文件名。
	Please input a source file.	输入要下载或上载的源文件名。
	Please input or select a destination file.	输入或选择要下载或上载的文件名。
	Please select a file.	选择要下载或上载的文件。
	System will be restarted...	系统将重新启动。
	User privileges are not enough to perform this operation.	权限不足。
Switch Config		
Security	Cannot add user.	用户名无效或已超出最大用户数。
	Cannot set password for user.	口令无效。
	Cannot set user privilege.	用户表存在问题。
	Cannot set user status.	用户表存在问题。
	User does not exist.	用户表存在问题。
Communication	Community String cannot contain spaces.	社区字符串不能包含空格。
	Community table is full or data is invalid.	公用表已满或数据无效。
	Data is invalid.	一般错误。

表 B-4 Web 界面错误消息 *（续）*

菜单	消息	说明
	Illegal SNMP trap IP address.	IP 地址格式非法。
	Please select a Community String.	选择要删除的社区字符串。
	Please type a Community String.	键入要添加的社区字符串。
	Trap Manager table is full or data is invalid.	陷阱管理器表已满或数据无效
	User privileges are not enough to perform this operation.	权限不足。
	You must specify an IP trap community string.	键入要添加的 IP 陷阱社区字符串。
Security	Authentication type doesn't exist.	本地、 TACACS 或 RADIUS 验证类型中有一种不受支持。
	Data is invalid	一般错误。
	Illegal IP address.	IP 地址格式非法。
	Number of Server Transmits is out of range.	RADIUS 重新发送次数超出范围。
	Password too long.	超出最大口令长度。
	Please input username.	输入一个用户名以添加新用户。
	Please select an user	选择一个用户以删除或更改口令。
	RADUIS KEY is invalid	RADIUS 加密密钥无效。
	Server Port Number is out of range.	RADIUS 端口号超出范围。
	Select a privilege level.	选择权限级别以添加用户。
	TACACS PORT is invalid	TACACS 端口无效。
	TACACS KEY is invalid	TACACS 密钥无效。
	Timeout is out of range.	RADIUS 超时超出范围。
	User privileges are not enough to perform this operation.	权限不足。
VLAN	Cannot create VLAN.	VLAN ID 无效或超出所支持的 VLAN 最大号码。
	Cannot set VLAN name.	VLAN 名称无效。
	Cannot set VLAN status.	不能禁用 VLAN 1，也不能禁用定义为管理端口的本地 VLAN (PVID) 的 VLAN。
	Cannot delete VLAN.	不能删除具有成员的 VLAN，也不能删除任何定义为接口的本地 VLAN(PVID) 的 VLAN。
	Data is invalid	一般错误。

表 B-4 Web 界面错误消息 *（续）*

菜单	消息	说明
	User privileges are not enough to perform this operation.	权限不足。
Membership	Data is invalid.	一般错误。
	User privileges are not enough to perform this operation.	权限不足。
Broadcast & Multicast		
Broadcast Parameters	Threshold is out of range.	超出最大广播风暴阈值级别。
	User privileges are not enough to perform this operation.	权限不足。
IGMP Parameters	Please enter a valid version.	输入有效版本。
	Query count is out of range.	查询计数超出范围。
	Query interval is out of range.	查询间隔超出范围。
	Query timeout is out of range.	查询超时超出范围。
	Report delay is out of range.	报告延迟超出范围。
	User privileges are not enough to perform this operation.	权限不足。
Multicast Router Ports	Data is invalid.	一般错误。
	Please select a port	选择要添加到多点传送路由器 （或要从中删除）的端口。
	User privileges are not enough to perform this operation.	权限不足。
Multicast Services	Data is invalid.	一般错误。
	Igmp group member is null.	从列表中选择 IGMP 组成员。
	Illegal IP address.	IP 地址格式非法。
	Select a port or trunk	选择端口以添加到 VLAN 上的静态端口 （或从中将其删除）。
	User privileges are not enough to perform this operation.	权限不足。
Spanning Tree		
Basic Configuration	Data is invalid.	一般错误。
	Priority is out of range.	优先级超出范围。
	User privileges are not enough to perform this operation.	权限不足。

表 B-4 Web 界面错误消息 *（续）*

菜单	消息	说明
Advanced Configuration	Data is invalid.	一般错误。
	User privileges are not enough to perform this operation.	权限不足。
Class of Service		
Basic Traffic Prioritisation	Cos Value is out of range.	CoS 值超出范围。
	Data is invalid.	一般错误。
	Priority is out of range.	优先级超出范围。
	Queue weight must be in a order of Q0<=Q1<=Q2<=Q3	队列权重无效。
	Traffic Class is out of range.	通信类别超出范围。
	User privileges are not enough to perform this operation.	权限不足。
Layer 3/4 Traffic Prioritisation	Cos Value is out of range.	CoS 值超出范围。
	Please select IP Precedence or DSCP mode	启用优先级服务时，请选择其中的一个选项。
	Traffic Class is out of range.	通信类别超出范围。
	User privileges are not enough to perform this operation.	权限不足。
Address Tables	Aging time is out of range.	超出最大地址有效时间。
	User privileges are not enough to perform this operation.	权限不足。
Up Links, Down Links		
Status	Cannot set port capabilities.	指定的端口的速度 / 双工模式不正确。
	Data is invalid.	一般错误。
	User privileges are not enough to perform this operation.	权限不足。
Link Aggregation	Cannot add trunk.The specified trunk is full or data is invalid.	指定的聚合组已满或数据无效。
	Cannot create trunk.	超出最大聚合组数。
	Cannot remove trunk.	聚合组表存在问题。
	Cannot remove trunk member.Data is invalid.	聚合组表存在问题。
	Cannot set trunk status.	不能对静态聚合组成员启用 LACP。
	Data is invalid.	一般错误。

表 B-4 Web 界面错误消息 *（续）*

菜单	消息	说明
	User privileges are not enough to perform this operation.	权限不足。
VLANs	Data is invalid.	一般错误。
	Please enter a valid PVID.	PVID 无效。请选择一个正确的 PVID。
	Please enter a valid timer.	计时器无效。请选择一个正确的计时器。
	Table is full or data is invalid.	表已满或数据无效。
	User privileges are not enough to perform this operation.	权限不足。
Address Filtering	Data is invalid.	一般错误。
	Please enter a valid MAC address.	MAC 地址无效。
	Please enter a valid VLAN ID.	VLAN ID 无效。
	Table is full or data is invalid.	表已满或数据无效。
	User privileges are not enough to perform this operation.	权限不足。
Spanning Tree	Data is invalid.	一般错误。
	User privileges are not enough to perform this operation.	权限不足。
Config	Path cost is out of range.	路径成本超出范围。
	Priority is out of range.	优先级超出范围。
Port	Path cost is out of range.	路径成本超出范围。
	Priority is out of range.	优先级超出范围。
	User privileges are not enough to perform this operation.	权限不足。
Management Ports		
VLANs	Data is invalid.	一般错误。
	Please enter a valid PVID.	PVID 无效。请选择一个正确的 PVID。
	Please enter a valid timer.	计时器无效。请选择一个正确的计时器。
	Table is full or data is invalid.	表已满或数据无效。
	User privileges are not enough to perform this operation.	权限不足。
Packet Filtering	User privileges are not enough to perform this operation.	权限不足。

表 B-4 Web 界面错误消息 *（续）*

菜单	消息	说明
Monitoring		
Port Mirroring	Data is invalid.	一般错误。
	User privileges are not enough to perform this operation.	权限不足。
Logs	Data is invalid.	一般错误。
	User privileges are not enough to perform this operation.	权限不足。

附录 **C**

规格

C.1 交换机体系结构

端口

交换机上行链接 — 8 1000BASE-T
中板 — 16 条千兆位串行下行链接 （用于服务器刀片）
管理通道 — 1 个 10/100BASE-TX， 1 个控制台端口 （串行 RJ-45）

网络接口

10/100/1000Base-T 端口 NETP0-7：
RJ-45 连接器，自动协商，自动 MDI/MDI-X
电缆连接：10BASE-T：100 欧姆， UTP 电缆； 3 类、 4 类、 5 类
100BASE-TX：100 欧姆， UTP 电缆； 5 类
1000BASE-T：100 欧姆， UTP 电缆； 5 类或 5e 类

缓冲区体系结构

上行链接端口和下行链接端口：1 MB 共享

总带宽

48 Gbps

交换数据库

32K MAC 地址条目

指示灯

SSC：活动的，需要维修，可以拆卸
以太网端口：链接/活动，速度

C.2 管理功能

带内管理

Telnet、基于 Web 的 HTTP、 SNMP

带外管理

通过 RJ-45 控制台端口传送 RS-232 信令

软件加载

带内 TFTP 或带外 XModem

MIB 支持

SNMP v1/v2 (RFC 1215, 1907)、 MIB II (RFC 2863)、 Bridge MIB (RFC 1493)、 Etherlike MIB (RFC 1643/2665)、RMON（RFC 2819 组 1、2、3、9）、IEEE 802.1Q VLAN (RFC 2674)、 IEEE 802.3ad LACP、专有 MIB

RMON 支持

组 1、 2、 3、 9（统计信息、历史记录、警报、事件）

其它功能

端口聚合组 （静态和 LACP）
端口镜像
端口安全性
RADIUS 认证客户端

C.3 物理规格

重量

2.08 千克 （4.59 磅）

体积

27.5 x 20.3 x 4.3 厘米 （10.8 x 8.0 x 1.7 英寸）

C.4 电源

工作电压

+12 伏直流

最大电流

5.2 A

功耗

最大 62 瓦特

散热量

最大每小时 211 BTU

C.5 环境规格

温度

工作时：5 至 45 摄氏度 （41 至 113 华氏度）
储运时：-40 至 70 摄氏度 （-40 至 158 华氏度）

湿度

工作时：10% 至 90% （无凝结）

C.6 标准

IEEE 802.3 Ethernet、 IEEE 802.3u Fast Ethernet、 IEEE 802.3ab Gigabit Ethernet
IEEE 802.1D 生成树协议和通信优先级，
IEEE 802.1w 快速重新配置 (STP)
IEEE 802.1p 优先级标记、 IEEE 802.1Q VLAN、 IEEE 802.3ac VLAN 标记，
IEEE 802.3x 全双工流量控制 (ISO/IEC 8802-3)
IEEE 802.3ad 链路聚合控制协议，
SNMP (RFC 1215， 1907)、 RMON (RFC 2819 组 1、 2、 3、 9)， MIB II (RFC 2863)，
Bridge MIB (RFC 1493)， Etherlike MIB (RFC 1643/2665)，
ARP (RFC 826)、 IGMP (RFC 1112)、 ICMP (RFC 792)

词汇表

1000BASE-T	用于通过两对 5 类、 5e 类 100 欧姆 UTP 电缆连接的千兆位以太网的 IEEE 802.3ab 规格。
1000BASE-X	用于任何基于 8B/10B 信令的 1000 Mbps 千兆位以太网的 IEEE 802.3 规格的缩写形式。
100BASE-TX	用于通过两对 5 类 UTP 电缆连接的 100 Mbps 快速以太网的 IEEE 802.3u 规格。
10BASE-T	用于通过两对 3 类、 4 类或 5 类 UTP 电缆连接的 10 Mbps 以太网的 IEEE 802.3 规格。
BOOTP	用于为连接到网络中的设备加载操作系统的引导协议。
CSMA/CD	载波侦听多路访问 / 冲突检测是以太网和快速以太网采用的通信方法。
GARP VLAN 注册协议 (GVRP)	为交换机交换 VLAN 信息定义一种方法，以便沿着生成树在端口上注册必要的 VLAN 成员，这样在每个交换机中定义的 VLAN 就可以在生成树网络上自动运行。
IEEE 802.1D	为 MAC 网桥操作指定一种通用方法，包括生成树协议。
IEEE 802.1p	在以太网网络中提供服务质量 (QoS) 的一种 IEEE 标准。该标准使用最多可定义八个通信等级的数据包标记，允许交换机基于标记的优先级值传输数据包。
IEEE 802.1Q	VLAN 标记 - 定义传递 VLAN 信息的以太网帧标记。它允许交换机将终端站分配到不同的虚拟 LAN，并为 VLAN 定义一种在交换网络中进行通信的标准方法。
IEEE 802.1w	快速生成树协议 (RSTP) 的 IEEE 标准，专门用于取代 IEEE 802.1D。 RSTP 可以大幅度提高拓扑结构变化的收敛速度。
IEEE 802.3	定义具有冲突检测功能的载波侦听多路访问 (CSMA/CD) 方法和物理层规格。
IEEE 802.3ab	为 1000BASE-T 快速以太网定义 CSMA/CD 访问方法和物理层规格。
IEEE 802.3ac	为 VLAN 标记定义帧扩展。

IEEE 802.3u 为 100BASE-TX 快速以太网定义 CSMA/CD 访问方法和物理层规格。

IEEE 802.3x 定义全双工链路上流量控制使用的以太网帧开始/停止请求和定时器。

IEEE 802.3z 为 1000BASE 千兆位以太网定义 CSMA/CD 访问方法和物理层规格。

IGMP 侦听 侦听在 IP 多点传送路由器和 IP 多点传送主机组之间传输的 IGMP 查询和 IGMP 报告数据包，以识别 IP 多点传送组成员。

IP 多点传送过滤 该交换机可以将多点传送流量传送到参与主机上的过程。

LAN 网段 独立的 LAN 或冲突域。

RJ-45 连接器 用于双绞线布线的连接器。

Telnet 为通过 TCP/IP 连接终端设备定义一种远程通信工具。

XModem 一种用于在设备之间传输文件的协议。数据以 128 字节块的形式进行分组并纠错。

冲突 通过电缆发送的数据包之间相互干扰的一种情况。这种干扰会使双方信号均无法理解。该情况仅适用于半双工连接。

冲突域 单个 CSMA/CD LAN 网段。

传输控制协议/因特网协议 (TCP/IP) 一组包含作为基本传输协议的 TCP 和作为网络层协议的 IP 的协议。

带宽 网络信号可以使用的最高频率与最低频率的差值。也与 “线速”一词同义，表示数据沿电缆传输的实际速度。

带宽利用率 收到的数据包占总带宽的百分比。

带内管理 从直接连接到网络上的工作站进行的网络管理。

带外管理 在未接入网络的工作站上进行的网络管理。

第 2 层 ISO 7 层数据通信协议中的数据链路层。该层与网络设备硬件接口直接相关，并基于 MAC 地址传送流量。

第 3 层 ISO 7 层数据通信协议中的网络层。该层为数据从一个开放系统移至另一个开放系统提供路由功能。

动态主机控制协议 (DHCP) 为向 TCP/IP 网络中的主机传送配置信息提供一个框架。 DHCP 以引导协议 (BOOTP) 为基础，增加了自动分配可重用网络地址的功能和其它配置选项。

端口镜像 将目标端口上的数据镜像到监视端口，从而通过逻辑分析器或 RMON 探测器进行故障排除的方法。使用该方法可以对目标端口上的数据进行无干扰研究。

端口聚合组 定义一种网络链路聚合和端口聚合方法，说明如何通过结合几个速度较低的物理链路来建立单个高速逻辑链路。

多点传送交换 交换机对传入的多点传送帧进行过滤，查找所连接主机没有注册的服务，或将它们转发给包含在指定多点传送 VLAN 组中所有端口的过程。

非屏蔽双绞线 (UTP) 由两条绝缘电线相互绞合而成的电缆，可以减少电子干扰；用于普通电话线中。

管理信息库 (MIB) Management Information Base （管理信息库）的缩写词。是一个数据库对象的集合，包含关于某一特定设备的信息。

简单网络管理协议 (SNMP) 因特网协议组中提供网络管理服务的应用协议。

交换端口 位于单独的冲突域或 LAN 网段中的端口。

介质访问控制 (MAC) 联网协议中约束对传输介质的访问的部分，有助于网络节点间的数据交换。

局域网 (LAN) 一组互连的计算机和支持设备。

快速以太网 一种基于以太网和 CSMA/CD 访问方法的 100 Mbps 网络通信系统。

链路段 连接一对中继器或连接一个中继器和一台 PC 的双绞线或光缆的长度。

链路聚合 请参阅 “端口聚合组”。

链路聚合控制协议 (LACP) 允许端口与另一设备上的 LACP 配置的端口自动协商聚合链路。

屏蔽双绞线 (STP) 外表覆盖旨在减少过多噪音干扰或辐射的铝箔或铜制屏蔽的双绞线。

千兆位以太网 一种基于以太网和 CSMA/CD 访问方法的 1000 Mbps 网络通信系统。

全双工 允许交换机和网卡同时收发信息的传输方法，可以有效地使该链路带宽增加一倍。

生成树协议 (STP) 一种检测网络中环路的技术。在复杂的网络系统或备份链接的网络系统中，经常会出现环路。生成树采用可用最短路径检测并导向数据，最大限度地提高网络性能和效率。

通用属性注册协议 (GARP) GARP 是一种终端站和交换机可以使用的协议，使用该协议可以在交换环境中注册和传播多点传送组成员信息，以便多点传送数据帧仅传播给交换 LAN 中包含已注册终端站的部分。以前称为组地址注册协议。

小型文件传输协议 (TFTP) 一种常用于软件下载的 TCP/IP 协议。

虚拟 LAN (VLAN) 虚拟 LAN 是多个网络节点的集合，共享同一个冲突域，而不考虑它们各自在网络中的物理位置或连接点。 VLAN 充当没有物理屏障的逻辑工作组，允许用户如同在同一 LAN 中那样共享信息和资源。

以太网 由 DEC、 Intel 和 Xerox 采用基带传输、CSMA/CD 访问、逻辑总线拓扑和同轴电缆开发并使其标准化的一种网络通信系统。后继的 IEEE 802.3 标准可以集成到 OSI 模型中，并通过在光纤光缆、同轴细缆和双绞线上使用的中继器和实施方案来扩展物理层和介质。

因特网信息控制协议 (ICMP) 通常在为了进行监视而发送回应消息 （例如， Ping）时使用。

因特网组管理协议 (IGMP) 主机可以在其本地路由器上注册多点传送服务的协议。如果某个指定的子网中有多个多点传送路由器，则其中一个路由器成为 “查询者”并承担跟踪组成员资格的责任。

远程监视 (RMON) RMON 提供全面的网络监视功能。通过该功能，没有必要再使用标准 SNMP 中的轮询功能，还可以设置在各种不同的流量状况下发出的警报，包括特定的错误类型。

远程认证拨入用户服务 (RADIUS) 一种使用中央服务器来控制对网络中符合 RADIUS 标准的设备访问的认证协议。可以通过这样的数据库对 RADIUS 服务器进行编程：该数据库具有多对用户名 / 口令，并且需要对此交换机进行管理访问的每个用户或组在该数据库中都具有相关的权限级别。

指示灯 用于监视设备或网络状况的发光二极管。

终端访问控制器访问控制系统 (TACACS) 一种使用中央服务器来控制对网络中符合 TACACS 标准的设备访问的认证协议。可以通过这样的数据库对 TACACS 服务器进行编程：该数据库具有多对用户名 / 口令，并且需要对此交换机进行管理访问的每个用户或组在该数据库中都具有相关的权限级别。

终端站 不用作网络互连的工作站、服务器或其它设备。

自动协商 一种信令方法，允许每个节点根据所连接节点的功能来选择最佳运行模式 （例如， 10 Mbps 半双工、 10 Mbps 全双工、 100 Mbps 半双工或 100 Mbps 全双工）。

组属性注册协议 *请参阅 “通用属性注册协议”。*

索引

英文

BOOTP， 3-14， 4-63
CLI， 4-1
CoS
  第 3/4 层优先级， 3-66， 4-129
  队列映射， 3-60， 4-132
  服务权级， 3-65， 4-131
  默认优先级， 3-60， 4-130
  配置， 3-60， 4-129
DHCP， 3-14， 4-63
  客户机标识符， 3-11， 4-65
DSCP， 3-70， 4-136
GARP， 3-89， 4-115
  设置定时器， 3-90
  设置计时器， 4-115
GARP VLAN 注册协议 *请参阅* GVRP
GVRP， 3-32， 3-89， 4-113
  接口配置， 3-90， 4-113
  全局设置， 3-36， 4-117
  说明， 3-32
IEEE 802.1D， 3-53， 4-93
IEEE 802.1w， 3-53， 4-93
IGMP， 3-42， 4-119
IP 地址
  BOOTP/DHCP 服务， 3-14， 4-62
  设置， 3-10， 4-62
  手动配置， 3-12， 4-62
IP 优先权， 3-68， 4-135
LACP， 3-83， 4-144
MIB， A-1
  支持的 MIB， A-1
PVID， 3-89， 4-109
  默认 ID， 3-89， 4-109
RADIUS， 3-23， 4-41
RSTP， 3-53， 4-93
  全局配置， 3-59， 4-93
  说明， 3-53
SC， 1-1， 1-3
SNMP， 2-2
  版本， 2-2， 3-29， 4-50
  配置， 3-27， 4-48
  启用陷阱， 3-28， 4-51
  社区字符串， 2-3， 3-27， 4-48
  陷阱，支持， A-3
  陷阱接收装置， 2-4， 3-28， 4-50
SSC， 1-xv， 1-1， 1-3
STA， 3-53， 4-92， 4-93
  边缘端口， 3-99， 3-103， 4-100
  接口设置， 3-98， 4-102
  链接类型， 3-99， 3-103， 4-101
  路径成本， 3-98， 3-102
  配置接口， 3-102， 4-92
  说明， 3-53
  协议迁移， 3-105， 4-100
  优先级， 3-98， 3-102， 4-99
STP， 3-53， 4-93
TACACS， 3-23， 4-41
Telnet， 4-2
VLAN， 3-31， 3-89， 4-104
  被禁止， 4-111

不带标记， 3-90， 4-110
成员端口， 3-90， 4-110
带标记， 4-110
禁止， 3-90
配置， 3-31， 4-104
说明， 3-31
已标记， 3-90
Web 界面， 3-2
菜单列表， 3-5
访问要求， 3-2
面板显示， 3-4
配置按钮， 3-4
主页， 3-3

B

边缘端口， STA， 3-99， 4-100

C

差别化业务编码点 *请参阅* DSCP
超长帧， 4-29
串行端口
配置， 4-54
错误消息， B-5
Web 界面， B-8
记录， 4-30
命令行错误， B-6
系统错误， B-5

D

登录
Web 界面， 3-3
登录验证， 3-23， 4-41
地址表， 3-72， 4-88
有效期， 3-74， 4-89
端口，配置， 3-75， 4-73
端口安全性， 3-95， 4-90
端口镜像， 3-110， 4-140
端口优先级，默认入口， 3-60， 4-130
多点传送
路由器， 3-45， 4-127
配置， 3-42， 4-119

F

服务类别 *请参阅* CoS
服务器刀片， 1-1， 1-3

G

故障排除， B-1
端口连接， B-2
管理界面， B-2
交换机指示灯， B-1
使用系统日志， B-3
固件，升级， 3-18， 4-17
固件版本，显示， 3-16， 4-40
管理
界面， Web， 3-2
界面，控制台， 4-1
管理端口， 1-3
管理端口，过滤通信， 3-106， 4-68
管理信息库 *请参阅* MIB
广播风暴
端口设置， 3-80， 4-80
阈值， 3-51， 4-80
规格， C-1
过滤通信，管理端口， 3-106， 4-68

J

记录，消息， 3-124， 4-30
加密口令， 4-26， 4-27， 4-57
简单网络管理协议 *请参阅* SNMP
交换机端口模式， 3-89， 4-107
交换机规格， C-1
交换机和系统控制器 *请参阅* SSC
静态地址，设置， 3-95， 4-87
镜像端口，配置， 3-110， 4-140
聚合组
LACP， 3-84， 4-144
动态， 3-84， 4-144
静态， 3-87， 4-142
配置， 3-83， 4-142

K

可接受的帧类型， 3-89， 4-108
控制台端口
  连接， 4-1
  配置， 4-54
口令， 4-26， 4-27， 4-57
口令，设置， 3-23， 4-41
快速生成树协议 *请参阅* RSTP

L

链接类型， STA， 3-99， 3-103， 4-101
链路聚合控制协议 *请参阅* LACP
路径成本， 3-98
路径成本， STA， 3-102， 4-97， 4-98
路径成本，方法， 3-59， 4-97

M

命令行界面 *请参阅* CLI

P

配置设置
  保存， 2-4
  保存或恢复， 3-21， 4-17

Q

启动配置文件，创建， 3-21， 4-18
启动文件
  设置， 3-18， 4-22
  显示， 3-18， 4-34

R

日志消息， B-4
入口过滤， 3-89， 4-108
软件版本，显示， 3-16， 4-40
软件下载， 3-18， 4-17

S

上行链接端口， 1-3
社区字符串， 2-3， 3-27， 4-48
生成树算法 *请参阅* STA
生成树协议 *请参阅* STP
升级软件， 3-18， 4-17

T

统计信息， SNMP， 3-120， 4-52
统计信息，交换机， 3-112， 4-83

X

系统日志， 3-124， 4-30， B-3
系统软件， 3-16， 4-17
  从服务器下载， 3-18， 4-17
  上传或下载， 4-17
  上载或下载， 3-18
下行链接端口， 1-3
下载软件， 3-18， 4-17
陷阱接收装置， 2-4， 3-28， 4-50
协议迁移， 3-105， 4-100

Y

因特网组管理协议 *请参阅* IGMP
用户名，设置， 3-23， 4-41
优先级， STA， 3-98， 3-102， 4-96
优先级，默认端口入口， 3-60， 4-130
有效期， 3-74， 4-89
远程验证拨入用户服务 *请参阅* RADIUS

Z

终端访问控制器访问控制系统 *请参阅* TACACS
主菜单， 3-5， 4-10
状态指示灯， 1-4
组地址注册协议 *请参阅* GARP