Sun Fire™ B1600 Blade System Chassis Switch Administration Guide

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

Part No. 817-2576-10
June 2003, Revision A

Send comments about this document to: docfeedback@sun.com

Contents

Preface

This *Sun Fire B1600 Blade System Chassis Switch Administration Guide* provides information that enables you to understand and use the switch inside the Switch and System Controller (SSC) module in the system chassis. There are two interfaces to the switch: a command-line interface and a web interface. This manual describes both.

The manual is intended for network administrators who are responsible for managing the *system chassis*. The manual assumes a working knowledge of local area network operations and familiarity with networking protocols.

Before You Read This Book

Before you start configuring the switch:

Install your system chassis by following the instructions in the Sun Fire B1600 Blade System Chassis Hardware Installation Guide and the Sun Fire B1600 Blade System Chassis Software Setup Guide.

How This Book Is Organized

Chapter 1 provides an overview of the switch, including management options, hardware features, switching features, and default settings.

Chapter 2 describes how to connect to the switch console and to the alternative web interface.

Chapter 3 describes all of the key switch features and shows you how to configure these features through both the web interface and the console interface. It also provides a list of comparable MIB variables used by SNMP management applications.

Chapter 4 provides a detailed listing of all the console interface commands and parameters.

Appendix A lists the Management Information Bases (MIB) and traps supported by this switch.

Appendix B provides basic troubleshooting information, including how to interpret the system and port LEDs, how to solve problems that might prevent you from accessing the management interface, and how to use the system logs.

Appendix C provides detailed specifications of the switch's features.

The Glossary is a list of words and phrases and their definitions.

The Index provides page references to all of the key topics discussed in this manual.

Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc123`	The names of commands and files; on-screen computer output	Display system files. Use `dir` to list all files.
`AaBbCc123`	What you type, when contrasted with on-screen computer output	`>`**`enable`** `Password:`
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *Sun Fire B1600 Installation and Maintenance Guide*. These are called *class* options. You *must* be an administrator to do this. To delete a file, type `del` *filename*.

Related Documentation

Application	Title	Part Number
Installation	*Sun Fire B1600 Blade System Chassis Hardware Installation Guide*	816-7614
Chassis Software Setup	*Sun Fire B1600 Blade System Chassis Software Setup Guide*	816-3361
Chassis Administration	*Sun Fire B1600 Blade System Chassis Administration Guide*	816-4765

Accessing Sun Documentation

You can view, print, or purchase a broad selection of Sun documentation, including localized versions, at:

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

Contacting Sun Technical Support

If you have technical questions about this product that are not answered in this document, go to:

`http://www.sun.com/service/contacting`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

`http://www.sun.com/hwdocs/feedback`

Please include the title and part number of your document with your feedback:

Sun Fire B1600 Blade System Chassis Switch Administration Guide, part number 816-3365-01

CHAPTER 1

Introduction

The Sun Fire B1600 blade system chassis includes two (Switch and System Controller (SSC) modules. The SSC includes a high-performance Gigabit Ethernet switch. The 16 internal full-duplex Gigabit ports on this switch provide high-capacity connectivity within the chassis, while the eight external full-duplex Gigabit ports connect to the wider network.

This chapter contains the following sections:

1.1 Overview

The switches provide Gigabit Ethernet connectivity for the Sun Fire B1600 blade system chassis. If a fault develops in one switch, operation continues without interruption on the second. All components in the chassis—blades, SSCs and power supply units (PSUs)—plug into a common midplane which provides all interconnection between the components.

Each of the 16 server blades is connected to a single port on each switch by a Gigabit Ethernet link that provides the blade's principal means of I/O. The switch within each SSC provides the Gigabit Ethernet fabric that connects all the blades together, in addition to eight external links for connection to the network. Each blade is also connected to the *System Controller* (SC) within each SSC by a simple serial link. The SC enables you to manage and monitor the components of the chassis. It also gives you access to the switch's command-line interface, and to the console for each server blade installed in the chassis.

1.1.1 Switch Architecture

The switch employs a high-speed switching fabric that enables simultaneous transport of multiple packets at low latency on all ports. The switch also uses store-and-forward technology to ensure maximum data integrity. In this mode, the entire packet must be received into a port buffer and checked for validity before being forwarded, preventing errors from propagating throughout the network.

1.1.2 Ways of Accessing the Switch Management Application

There is a serial console port implemented with an RJ-45 jack that provides on-site management access to the SC. When you apply power to the system chassis, the interface for the SC is displayed. To access the command-line interface for the switch, see "Configuration Options" on page 2-2 or refer to the *Sun Fire B1600 Blade System Chassis Software Setup Guide*.

This command-line interface can also be accessed directly using telnet through the 100BASE-TX RJ-45 management port (NETMGT) on the SSC.

The switch can also be managed by connecting to this port over the network with a Web browser or SNMP/RMON software.

When you connect through a web browser the switch provides HTTP management access with a graphical user interface.

The information provided by SNMP can be displayed by an appropriately configured management application that is able to use SNMP.

1.2 Description of Hardware

The SSC includes the switch board, the SC, cooling fans, as well as midplane and rear panel connectors. The SC provides management access to the server chassis and switch board. The SC also drives the system indicators, duplicate copies of which are located on the front and rear of the Sun Fire B1600 blade system chassis.

1.2.1 Ethernet Ports

1.2.1.1 Up-link Ports

Eight external RJ-45 ports support IEEE 802.3x auto-negotiation of speed, duplex mode, and flow control. Each port can operate at 10 Mbit/sec, 100 Mbit/sec, and 1000 Mbit/sec, full- and half-duplex, and control the data stream to prevent buffers from overflowing. The up-link ports can be connected to other IEEE 802.3ab 1000BASE-T compliant devices up to 100 m (328 ft.) away using Category 5 twisted-pair cable. These ports also feature automatic MDI/MDI-X operation, so you can use straight-through cables for all connections. The up-link ports are named NETP0 to NETP7 in the configuration interface.

Note – When using auto-negotiation, the speed, transmission mode, and flow control can be automatically set if this feature is also supported by the connected device. Otherwise, these settings can be manually configured for any connection.

Note – Autonegotiation must be enabled for automatic MDI/MDI-X pinout configuration.

1.2.1.2 Internal Ports

The switch also includes 16 internal 1000BASE-X Gigabit Ethernet ports that connect to the blades in the chassis. These ports are fixed at 1000 Mbit/sec, full duplex. The internal ports are named SNP0 to SNP15 in the configuration interface.

The switch also includes an internal 10/100BASE-TX port called NETMGT, which is connected to the SC's network port and to the external management port on the SSC's front panel through an internal hub.

1.2.2 Status LEDs

Switch level indicators are located on the SSC module. The 1000BASE-T up-link ports and the 10/100BASE-TX management port located on the rear panel of the SSC also include indicators for both Link and Speed.

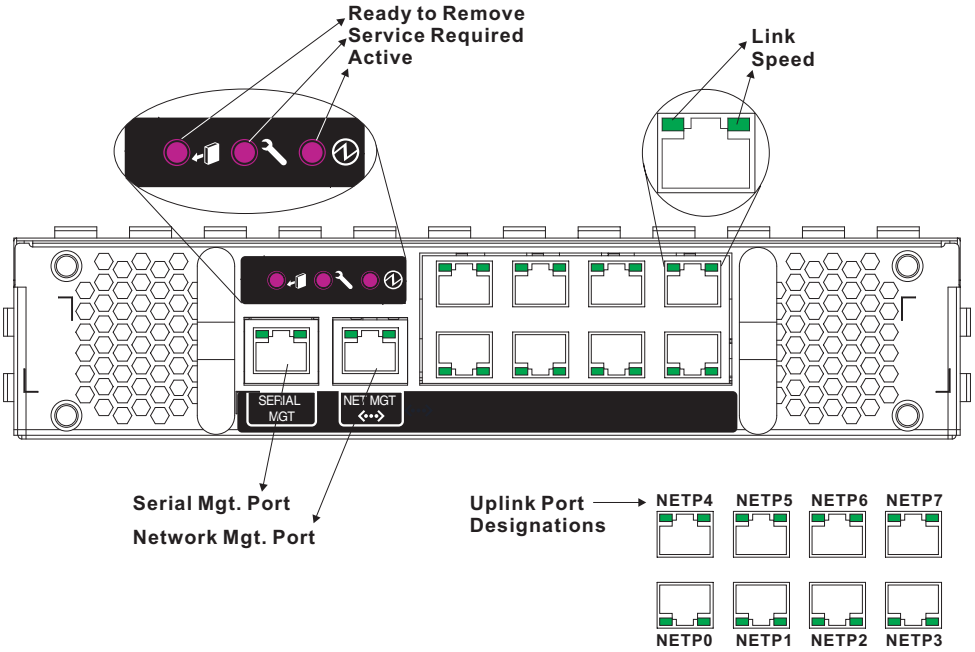


FIGURE 1-1 SSC Exterior Panel

TABLE 1-1 Port LEDs

LED	Condition	Status
SSC		
Active	On (Green)	The SSC is functioning normally.
Service Required	On (Amber)	The SSC requires service.
Ready to Remove	On (Blue)	The SSC can now be removed.
RJ-45 Ports		
Link	On (Green)	Port has established a valid network connection.
Speed	On (Amber)	Link is operating at 1 Gbps.
	Off	Link is operating at less than 1 Gbps.

1.3 Features of the Switch

The switch provides a wide range of advanced performance-enhancing features. Multicast filtering provides support for real-time network applications. Port-based and tagged virtual local area networks (VLANs), plus support for automatic GARP VLAN Registration Protocol (GVRP) provides traffic security and efficient use of network bandwidth. Quality of Service (QoS) priority queueing ensures the minimum delay for moving real-time multi-media data across the network. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. And broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Some of the management features are briefly described in this section.

- IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses and then filtering or forwarding traffic based on this information. The address table supports up to 8000 addresses.
- Store-and-Forward Switching – The switch copies each frame into its memory before forwarding it to another port to ensure that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

  To avoid dropping frames on congested ports, the switch provides 128 Kbytes of frame buffering per port. This buffer can queue packets awaiting transmission on congested networks.
- Spanning Tree Protocol – The switch supports these spanning tree protocols:
  - Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol chooses a single path and disables all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path fails for any reason, an alternate path will be activated to maintain the connection.
  - Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from connected devices.
- Virtual LANs – The switch supports up to 256 VLANs. A virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical locations or connection points in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups

can be dynamically learned through GVRP or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms, which severely degrade performance in a flat network.
- Simplify network management for node changes and moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection has been configured between separate VLANs using a router or Layer 3 switch.

- Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then connect a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.
- Link aggregation – Ports can be combined into an aggregate link. Aggregate links can be manually set up or dynamically configured using IEEE 802.3ad Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk fails. The switch supports six aggregated links, with up to four up-link ports per aggregated link or up to two down-link ports per aggregated link.
- Port Security – Port security prevents unauthorized users from accessing your network. It enables each port to learn, or be assigned, a list of MAC addresses for devices authorized to access the network through that port. Any packet received on the port must have a source address that appears in the authorized list, otherwise it will be dropped. Port security is disabled on all ports by default, but can be enabled on a per-port basis.
- Broadcast Suppression – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it is throttled until the level falls back beneath the threshold.
- Flow Control – Flow control reduces traffic during periods of congestion and prevent packets from being dropped when port buffers overflow. The switch supports flow control based on the IEEE 802.3x standard. By default, flow control is disabled on all ports.
- Traffic Priority – This switch provides Quality of Service (QoS) by prioritizing each packet based on the required level of service, using four priority queues with Weighted Round Robin queuing. The switch uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic is then sent to the corresponding output queue.

- Address Filtering – This switch provides a packet filter for all traffic entering the CPU port and potentially forwarded or routed to the management network. The packet filter is rule/pattern-based and constitutes a set of patterns that when matched DROPS the packet, and a further set of patterns that when matched ACCEPTS the packet.
- Multicast Switching – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and IGMP to manage multicast group registration.

1.4 Switch Default Settings

TABLE 1-2 Switch Default Settings

Function	Default
System Settings	
• Web Mgt.	Enabled
• Secure Web Mgt.	Disabled
• BOOTP	Enabled
• DHCP	Enabled
• SNMP Communities	`public`: Read Only `private`: Read/Write
• SNMP Traps	Authentication traps: enabled Link up down events: enabled
• User Name	`admin` (for console, Telnet, Web) `guest` (for console, Telnet, Web)
• Password	logon - user `admin`, password `admin` user `guest`, password `guest` Change from Normal Exec to Privileged Exec: `super`
Serial Port	Baud rate: 9600, Data bits: 8, Stop bits: 1, Parity: none
IP Settings	Address: 0.0.0.0, Subnet mask: 255.0.0.0
Port Status	
• Port Speed	Port SNP0-15: 1000 Mbps Port NETP0-7: 10/100/1000 Mbps, auto-negotiated Port NETMGT: 10/100 Mbps, auto-negotiated
• Duplex Mode	Port SNP0-15: full Port NETP0-7, NETMGT: half- and full-duplex, auto-negotiated
• Flow Control	Disabled
Port Priority	Ingress priority: 0
Port Security	Disabled
Spanning Tree Protocol	Enabled, Default RSTP (Defaults: All parameters based on IEEE 802.1w)

TABLE 1-2 Switch Default Settings *(Continued)*

Function	Default
• Edge Port (Fast Forwarding)	Enabled by default for SNP0-15, disabled for NETP0-7
Address Aging	300 seconds
Virtual LANs	
• GVRP	Disabled
• Default VLAN	PVID 1 (for untagged frames)
• Management VLAN	VLAN 2 (for the management port)
• Tagging	RX: All frames, TX: Untagged frames
• Ingress Filtering	Disabled
Multicast Filtering	
• IGMP Snooping	Enabled
ARP	Enabled
• Cache Timeout	20 minutes

CHAPTER 2

Initial Configuration

For full information about performing the initial configuration of the switch, refer to the *Sun Fire B1600 Blade System Chassis Software Setup Guide*.

This chapter contains the following sections:

2.1 Connecting to the Switch Interface

2.1.1 Configuration Options

For management access, the switch module provides a command-line configuration interface (CLI). This program can be accessed by first connecting to the RJ-45 serial console port on the switch, and then logging into the switch's CLI from the System Controller's (SC) command prompt as shown below, where SSC*n* indicates either SSC0 or 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#
```

Note – You can use a telnet or a web connection to the switch provided that you have set up a DHCP server on your management network. To ensure that the switch receives the same address each time it boots (and makes a DHCP request), you need to specify the following client identifier on your DHCP server: SUNW,SWITCH_ID=*serial number of chassis*, 0 (for the switch in SSC0) or SUNW,SWITCH_ID=*serial number of chassis*, 1 (for the switch in SSC1). For information about preparing the network to receive the system chassis, and about all procedures for performing the initial configuration of the switch, refer to the *Sun Fire B1600 Blade System Chassis Software Setup Guide*.

2.1.1.1 Configuring the Switch Through the Built-in Switch Interfaces

Console Connection – You can access the switch's CLI by typing **`console sscn/swt`** at the System Controller command prompt, where *n* is either 0 or 1 depending on whether the switch whose console you want to access is in SSC0 or SSC1.

Telnet Connection – You can connect to the switch's CLI remotely by a Telnet connection over the management network.

Web Interface – The switch also includes an embedded HTTP Web agent. This agent can be accessed using a standard Web browser from any computer on the management network.

SNMP Software – The switch's management agent is based on Simple Network Management Protocol (SNMP), supporting versions 1, 2c, and 3. This SNMP agent enables the switch to be managed from any system in the management network using management software, such as Solstice Domain Manager™ software.

The system configuration program and the SNMP agent support management functions such as:

- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure SNMP parameters
- Add ports to network VLANs
- Display system information or statistics
- Configure the switch to join a Spanning Tree
- Download system firmware

2.2 Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP v1, v2c or v3) applications such as Soltice Domain Manager. You can configure the switch to respond to SNMP requests and/or generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

2.2.1 Community Strings

Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages from the SSC. You therefore need to assign community strings to specified users or user groups and set the access levels.

The default strings are:

- `public` – With read-only access. Authorized management stations are only able to retrieve MIB objects.
- `private` – With read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note – If you do not intend to utilize SNMP, delete both of the default community strings. When there are no community strings, SNMP management access to the switch is disabled.

To configure a community string:

1. **From the Privileged Exec level global configuration mode prompt, type `snmp-server community` *string mode*, where *string* is the community access string and *mode* is `rw` (read/write) or `ro` (read only). Press Enter.**
2. **To remove an existing string, type `no snmp-server community` *string*, where *string* is the community access string to remove. Press Enter.**

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

2.2.2 Trap Receivers

You can also specify SNMP stations that are to receive traps from the SSC.

To configure a trap receiver:

1. **From the Global Configuration mode prompt, type `snmp-server host` *host-address community-string*, where *host-address* is the IP address for the trap receiver and *community-string* is the string associated with that host. Press Enter.**
2. **To configure the SSC to send SNMP notifications, you must enter at least one `snmp-server enable traps` command.**

   Type **`snmp-server enable traps`** *type*, where *type* is either `authentication` or `link-up-down`. Press Enter.

```
Console(config)#snmp-server host 10.1.0.9 sun
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

3. **Save the configuration settings by following the instructions in the** *Sun Fire B1600 Blade System Chassis Software Setup Guide***.**

CHAPTER 3

General Management of the Switch

This chapter describes how to perform basic configuration tasks and includes the following sections:

3.1 Using the Web Interface

The Sun Fire B1600 blade system chassis switch provides an embedded HTTP web agent. Using a web browser, you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above or Netscape Navigator 6.2 or above).

Note – You can also use the command-line interface (CLI) to manage the switch over a serial connection to the console port or though Telnet. For more information about using the CLI, see Chapter 4, "Command-Line Reference."

To access the switch from a web browser, perform the following tasks:

1. **Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol.**

   For information on how to do this, refer to the *Sun Fire B1600 Blade System Chassis Software Setup Guide*.

2. **Set a user name and password using an out-of-band serial connection.**

   Access to the web agent is controlled by the same user names and passwords as the command-line interface. (For information on how to do this, refer to the *Sun Fire B1600 Blade System Chassis Software Setup Guide*.)

   Note – If the path between your management station and the switch does not pass through any device that uses the Spanning Tree Algorithm, you can set the switch port connected to your management station to use fast forwarding to improve the switch's response time to management commands issued through the web interface. (See "Admin Edge Port" on page 3-129.)

   ---

3. **Type the IP address of the switch into the address bar of your web browser.**

   A login dialog box opens.

4. **Type a user name and password in the appropriate text fields.**

5. **Click OK.**

   If the user name and password are accepted, the System Identity page (home page) opens and you have access to switch configuration.

   Note – You are allowed three attempts to enter the correct password. After the third failed attempt, the current connection is terminated.

3.1.1 Navigating the Web Browser Interface

To access the web-browser interface, you must first enter a user name and password. The administrator has read/write access to all configuration parameters and statistics. The default administrator user name and password is `admin`.

3.1.1.1 Home Page

When your web browser connects with the switch's web agent, the home page is displayed. The configuration options are displayed in the menu tabs and corresponding menu items (listed in the row beneath the menu tabs) at the top of the page. The menu tabs and subordinate menu items are used to access the configuration menus and display configuration parameters and statistics.

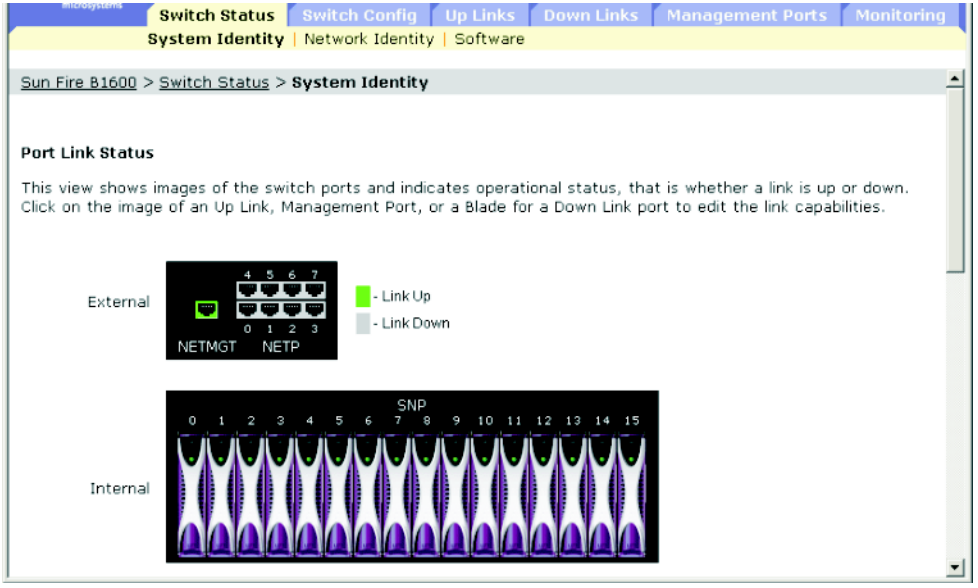


FIGURE 3-1 Web GUI Home Page

3.1.1.2 Configuration Options

Configurable parameters have a text field or a menu. Once a configuration change has been made on a page, click the Save button to confirm the new setting. The following table summarizes the web page configuration buttons.

TABLE 3-1 Web Page Configuration Buttons

Button	Action
Cancel	Cancels specified values and restores current values.
Reset	Cancels specified values and restores current values.
Save	Sets specified values to the system.

Note – To ensure proper screen refresh, confirm that Internet Explorer 5.x is configured as follows: From the Tools menu, choose Internet Options ⇒ General ⇒ Temporary Internet Files ⇒ Settings and set "Check for newer versions of stored pages" to "Every visit to the page."

Note – When using Internet Explorer 5.0, you might have to click the web browser's refresh button to manually refresh the screen after making configuration changes.

3.1.2 Panel Display

The web agent displays an image of the switch's up-link ports, indicating whether each link is active. Clicking on the image of a port opens the Port Configuration page, which is described in Section 3.4, "Port Configuration" on page 3-96.

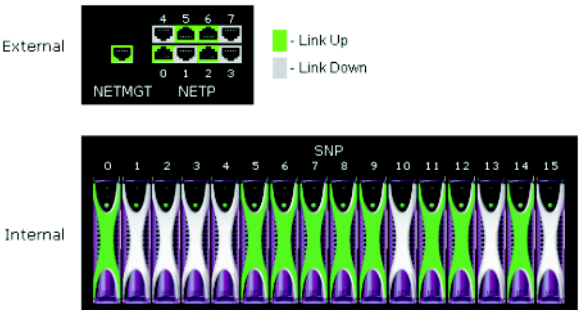


FIGURE 3-2 Image of the Switch's Active Uplinks and Downlinks

3.1.3 Main Menu

Using the on-board web agent, you can define system parameters, manage and control the switch and all its ports, and monitor network conditions. The following table briefly describes the selections available from this program.

TABLE 3-2 Summary of Tasks You Can Perform Using the Web Agent

Menu	Subordinate Menu	Description	See Page
Switch Setup		Basic configuration	3-8
	System Identity	Provides basic system description, including location and contact information	3-8
	Network Identity	Sets the IP address for management access using DHCP, BOOTP, or manual configuration	3-12
	Software	Manage switch firmware code and configuration files	3-18
Switch Config		Global configuration protocols	3-39
	Security	Assigns user names and passwords, as well as remote access authentication service using RADIUS or TACACS+	3-28
	Communication	Sets the SNMP community access strings, trap managers, and type of traps to issue	3-34
	VLANs	Displays basic VLAN information; enables GVRP multicast protocol; configures VLANs	3-39
	• Static VLAN Port Membership	Adds static members to VLANs	3-50
	Broadcast & Multicast	Sets broadcast storm control; configures multicast protocols including IGMP Snooping, static router port information, and multicast services	3-54
	• IGMP Parameters	Enables multicast filtering; configures parameters for multicast query	3-55
	• Multicast Router Ports	Assigns ports that are connected to a neighboring multicast router/switch	3-59
	• Multicast Services	Assigns a multicast service to a specific interface	3-64
	• Broadcast Parameters	Sets the broadcast storm threshold	3-67
	Spanning Tree	Configures the Spanning Tree Protocol	3-70
	• Basic Configuration	Configures settings for the global spanning tree	3-70
	• Advanced Configuration	Configures advanced settings for RSTP	3-76

TABLE 3-2 Summary of Tasks You Can Perform Using the Web Agent *(Continued)*

Menu	Subordinate Menu	Description	See Page
	Class of Service	Configures Class of Service	3-78
	• Basic Traffic Prioritisation	Configures default CoS priorities, maps CoS priorities to output queues, and configures Weighted Round Robin queueing	3-78
	• Layer 3/4 Traffic Prioritisation	Selects layer 3/4 priority service, maps IP precedence tags to CoS values, and maps DSCP tags to CoS values	3-85
	Address Tables	Sets address aging; displays entries for the specified interface, VLAN or address; configures static addresses	3-92
Up Links		Port configuration	3-96
	Connection Status	Displays port connection status	3-96
	• Connection Configuration	Configures port connection settings; enables broadcast storm control	3-102
	Link Aggregation	Configures ports to dynamically join aggregated links using LACP, or specifies ports to group into static aggregated links	3-107
	VLANs	Specifies port attributes (including default PVID, switchport mode, ingress filtering, GVRP, GARP timers; configures static VLAN members	3-114
	Static Addresses	Displays or edits static entries in the Address Table; enables and disables learning of permanent entries	3-121
	Spanning Tree	Configures port settings for the global spanning tree	3-125
	• Spanning Tree Protocol	Configures STP port-level settings for interface(s) on the global spanning tree	3-125
Down Links		Port configuration	3-96
	Connection Status	Displays port connection status	3-96
	• Connection Configuration	Configures port connection settings; enables broadcast storm control	3-102
	Link Aggregation	Configures ports to dynamically join aggregated links using LACP, or specifies ports to group into static aggregated links	3-107
	VLANs	Specifies port attributes (including default PVID, switchport mode, ingress filtering, GVRP, GARP timers; configures static VLAN members	3-114

TABLE 3-2 Summary of Tasks You Can Perform Using the Web Agent *(Continued)*

Menu	Subordinate Menu	Description	See Page
	Static Addresses	Displays or edits static entries in the Address Table; enables and disables learning of permanent entries	3-121
	Spanning Tree	Configures port settings for the global spanning tree	3-125
	• Spanning Tree Protocol	Configures STP port-level settings for interface(s) on the global spanning tree	3-125
Management Port		Port configuration	3-96
	Connection Status	Displays port connection status	3-96
	VLANs	Specifies port attributes (including default PVID, switchport mode, ingress filtering, GVRP, GARP timers; configures static VLAN members	3-114
	Packet Filtering	Filters traffic entering the management port from the up-link ports	3-134
Monitoring		Switch monitoring functions	3-139
	Port Mirroring	Sets the source and target ports for mirroring	3-139
	Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB	3-141
	SNMP Statistics	Displays statistics on SNMP messages	3-152
	Logs	Configures logging message parameters; displays messages stored in switch memory	3-152

3.2 Basic Configuration

3.2.1 Displaying System Information

You can identify the system by providing a descriptive name, location, and contact information.

When displaying system information using the web interface or CLI, the following parameters are displayed or can be configured:

- Host Name – The name assigned to the switch.
- Location – The system chassis location.
- Contact – The administrator responsible for the system.
- System Up Time – The length of time the management agent has been up.
- System Description – The system hardware description assigned by the manufacturer.
- Serial Number[1] – The serial number of the main board.
- System OID string[2] – The MIB II object ID for switch's network management subsystem.
- MAC Address[3] – The physical layer address for the switch.
- Web server[2] – The operational status of web (HTTP) management access on the switch.
- Web server port[2] – The TCP port number used by the web interface.
- POST result[2] – The results of the switch power-on self-test.

3.2.1.1 Web Interface: Displaying and Specifying Identification Details

1. **Open the Switch Setup ⇒ System Identity window.**
2. **Specify the host name, location, and contact information for the system administrator.**
3. **Click Save.**

---

1. CLI: See "show version" on page 4-44
2. CLI only
3. Web: See "Setting the IP Address" on page 3-12

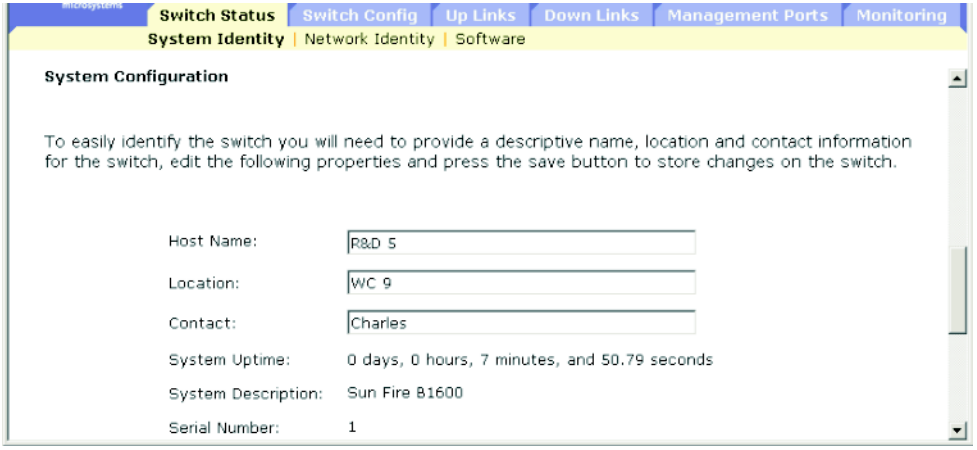


FIGURE 3-3 Switch Setup ⇒ System Identity Window

3.2.1.2 Command-line Interface: Displaying and Specifying Identification Details

```
Console(config)#hostname R&D 5
Console(config)#snmp-server location WC 9
Console(config)#snmp-server contact Charles
Console#show system
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#
```

FIGURE 3-4 CLI Commands for Specifying Host Name, Location, and Contact Information.

3.2.1.3 MIB Variables: Identification Details

TABLE 3-3 SNMP MIB variables Corresponding to the Switch Setup ⇒ System Identity Window

Field Name	MIB Variable	Access	Value Range	Default Value
System Name (Host Name)	`MIB-II. system. sysName`	Read/write	String (size(0-255))	
System Location	`MIB-II. system. sysLocation`	Read/write	String (size(0-255))	
System Contact	`MIB-II. system. sysContact`	Read/write	String (size(0-255))	
System Up Time	`MIB-II. system. sysUpTime`	Read only	Timeticks (in centiseconds)	
System Description	`MIB-II. system. sysDescr`	Read only	String (size(0-255))	
System Object Identification	`MIB-II. system. sysObjectID`	Read only	Object identifier	
MAC Address	`MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress`	Read only	Physical address	
HTTP State (Web Server)	`sun... ipMgt. ipHttpState`	Read/write	enabled (1), disabled (2)	enabled
HTTP Port (Web Server Port)	`sun... ipMgt. ipHttpPort`	Read/write	Integer (1-65535)	80
HTTPS State (Secure Server)	`sun... ipMgt. ipHttpsState`	Read/write	enabled (1), disabled (2)	enabled
HTTPS Port (Secure Server Port)	`sun... ipMgt. ipHttpsPort`	Read/write	Integer (1-65535)	443

3.2.2 Setting the IP Address

By default, the switch searches for its IP address, default gateway, and netmask using DHCP.

You can manually configure a specific IP address or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Any other format will not be accepted by the software.

Note – The IP address of the switch is in fact the IP address of the VLAN containing the management port (NETMGT). By default, the management port is on VLAN 2. Therefore, by assigning an IP address to VLAN 2 you set up network access to the switch. Only the VLAN containing the management port should be assigned an IP address. If you assign an IP address to any other VLAN, the original IP address is immediately disabled and the new address takes immediate effect.

When setting the switch IP configuration using the web interface or CLI, the following parameters are displayed or can be configured:

- Current IP Address – The current address of the VLAN interface that is allowed management access.
- MAC Address[4] – The physical layer address for this switch.
- Management VLAN – The VLAN through which you can manage the switch. By default, the management port (NETMGT) is configured as a member of this VLAN (that is, VLAN 2). However, if you change the Management VLAN, you will lose management access to the switch unless the NETMGT port has already been configured as a member of the new VLAN. If this occurs, you will have to use the console interface to add the NETMGT port to the newly configured Management VLAN. (See Section 4.3.12.8, “switchport allowed vlan” on page -127.)
- IP Address Mode – The method through which IP functionality is enabled. The options are manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests are broadcast periodically by the switch for IP configuration settings. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
  - DHCP – Dynamic Host Configuration Protocol

    Enable Client ID – Includes a client identifier in all communications with the DHCP server.

---

4. CLI: See “Displaying System Information” on page 3-8.

Text / Hex – Indicates whether the client ID has been entered as a text string (1-15 characters) or as a hexidecimal value. The data type used will depend on the requirements of your DHCP server.

Note – The Client ID specified in this menu will be overwritten by the SC the next time the system, or the switch itself, is rebooted. The Client ID field will be removed from the next firmware release.

  - BOOTP – Boot Protocol
- Manual – The IP parameters are set to specified values.
  - IP Address – The address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, and separated by periods. The default is 0.0.0.0.
  - Subnet Mask – The mask that identifies the host address bits used for routing to specific subnets. The default is 255.0.0.0.
  - Broadcast Address[5] – The IP broadcast address used for sending datagrams on the interface associated with the IP address. This value applies to both the subnet and network broadcast addresses used by the switch. The default is 0.0.0.1.
  - Gateway IP Address – The IP address of the gateway router between this device and management stations that exist on other network segments. The default is 0.0.0.0.

3.2.2.1 Manual Configuration

Web Interface: Specifying the Management VLAN and IP Details

1. **Open Switch Setup ⇒ Network Identity.**
2. **Select the management VLAN interface.**
3. **Select the Manual IP Address Mode.**
4. **Specify the IP address, subnet mask, and default gateway.**
5. **Click Save.**

---

5. Web only

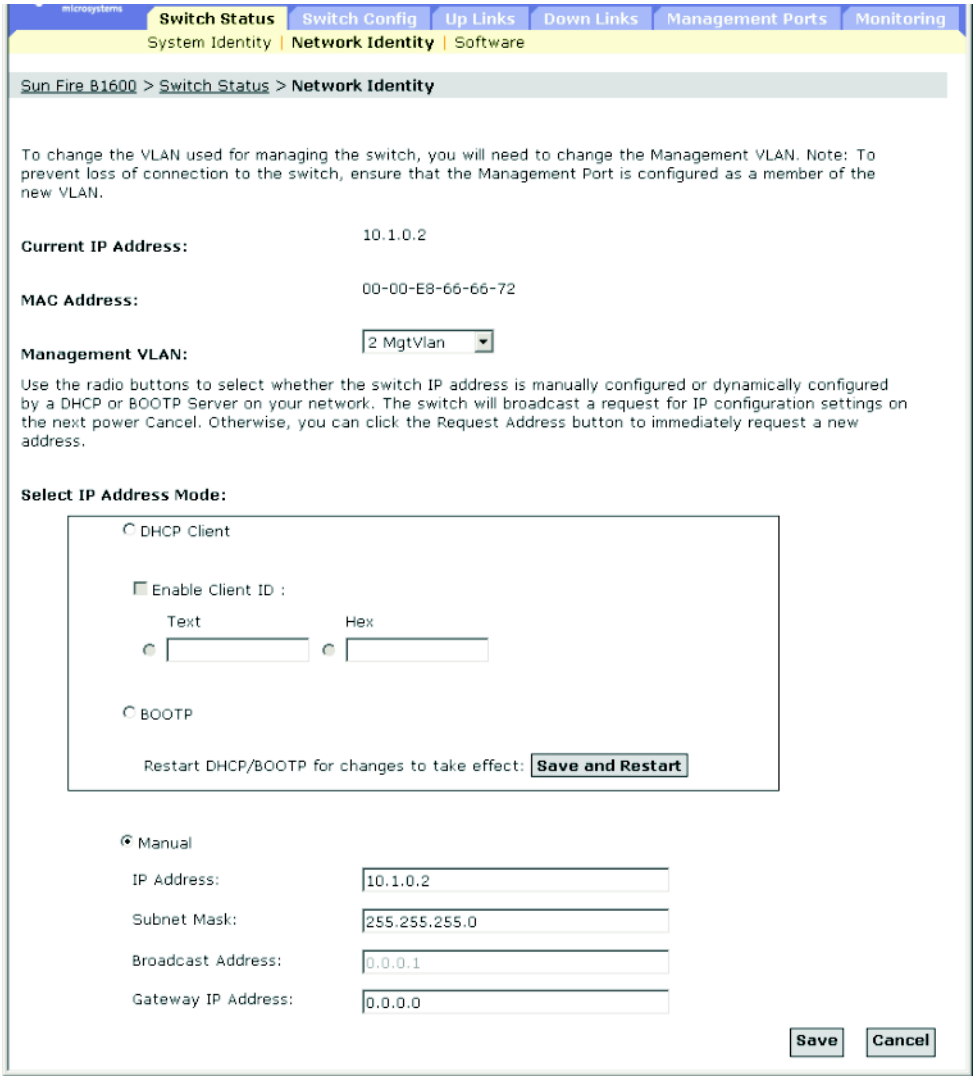


FIGURE 3-5 Open Switch Setup ⇒ Network Identity Window

Note – If you receive an error message saying that the data you have entered is invalid, confirm that you have specified each of the IP addresses correctly.

Command-line Interface: Specifying the Management VLAN and IP Details

- **Specify the management interface, IP address, and default gateway:**

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

MIB Variables: Specifying the Management VLAN and IP Details

TABLE 3-4 MIB Variables for Specifying the Management VLAND and IP Details

Field Name	MIB Variable	Access	Value Range	Default Value
Management VLAN	sun... switchMgt. switchManagementVlan	Read/write	Integer (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry . vlanAddressMethod	Read/write	user (1), bootp (2), dhcp (3)	user
IP Address Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntAddr	Read/write	IP address	
Subnet Mask Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntNetMask	Read/write	IP address	
Broadcast Address	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntBcastAddr	Read only	Integer (0-1)	1
Default Gateway Configuration	sun... ipMgt. netDefaultGateway	Read/write	IP address	

3.2.2.2 Using DHCP/BOOTP

By default, the switch uses DHCP/BOOTP services to find its IP configuration information.

Web Interface: Using Dynamic IP Configuration Services

1. **Open Switch Setup ⇒ Network Identity.**
2. **Specify the management VLAN interface.**
3. **Specify the IP Address Mode by selecting DHCP or BOOTP.**

   By default, the System Controller in the chassis provides a client identifier to the switch. The client identifier is SUNW,SWITCH_ID=*serial number of chassis*,0 or SUNW,SWITCH_ID=*serial number of chassis*,1 (depending on whether the switch is in SSC0 or SSC1). You can specify a client identifier in the Enable Client ID checkbox, but it will be overwritten the next time the System Controller resets or boots. Do not do this. The Enable Client ID field will be removed from future versions of the firmware.

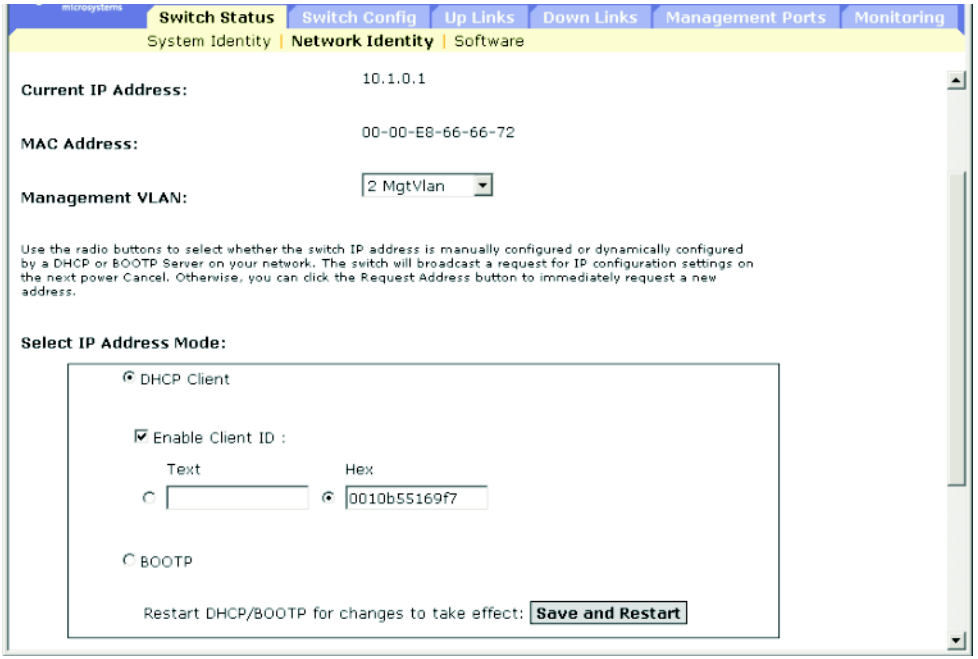


FIGURE 3-6 Open Switch Setup ⇒ Network Identity Window (Showing DHCP/BOOTP Radio Buttons)

If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings through the web interface. You can only restart the DHCP service through the web interface if the current address is still valid.

Note – If you lose your management connection, use a console connection and the `show ip interface` command to determine the new switch address.

Note – The Client ID specified in this menu will be overwritten by the SC the next time the System Controller, or the switch itself, is rebooted. The Client ID field will be removed from the next firmware release.

Command-line Interface: Using Dynamic IP Configuration Services

1. **Specify the management interface.**
2. **Set the IP address mode to** `DHCP` **or** `BOOTP`**.**
3. **Issue the** `ip dhcp restart` **command.**

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

DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service.

Type the following command to restart DHCP service:

```
Console#ip dhcp restart
```

MIB variables: Using Dynamic IP Configuration Services

TABLE 3-5 MIB Variables Associated With Dynamic IP Configuration Services

Field Name	MIB Variable	Access	Value Range	Default Value
Management VLAN	`sun... switchMgt. switchManagementVlan`	Read/write	Integer (1-4094)	1
IP Address Mode	`sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod`	Read/write	user (1), bootp (2), dhcp (3)	dchp
DHCP Client ID	`sun... ipMgt. dhcpClientIfClientId`	Read/write	Octet string (MAC address)	
DHCP Restart	`sun... ipMgt. ipDhcpRestart`	Read/write	restart (1), noRestart (2)	noRestart

3.2.3 Displaying Switch Software Versions

When displaying switch software versions using the web interface or CLI, the following parameters are displayed:

- Loader Version – The version number of the loader code.
- Boot-ROM Version – The version number of the boot code.
- Operation Code Version – The version number of the runtime code.
- Unit ID[6] – The ID of the active switch. (This value will always be 1.)

3.2.3.1 Web Interface: Displaying Switch Software Version Information

- **Open Switch Status ⇒ Software.**

6. CLI only. The value of Unit ID has no significance in the current version of the switch in the Sun Fire B1600 blade system chassis.

FIGURE 3-7 Open Switch Setup ⇒ Software Window (showing version information)

3.2.3.2 Comand-line Interface: Displaying Switch Software Version Information

Use the following command to display version information:

```
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#
```

3.2.3.3 MIB Variables Associated With Software Version Information

TABLE 3-6 MIB Versions Associated With Software Version Information

Field Name	MIB Variable	Access	Value Range	Default Value
Switch Serial Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swSerialNumber	Read only	Display string (size (0..80))	
Switch Hardware Version	SUN. switchMgt. switchInfoTable. switchInfoEntry. swHardwareVer	Read only	Display string (size (0..20))	
Switch Port Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swPortNumber	Read only	Integer	25
Switch Unit Index	SUN. switchMgt. switchInfoTable. switchInfoEntry. swUnitIndex	Not-accessible	Integer	1
Switch Loader Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swLoaderVer	Read only	String (size (0-20))	
Switch Boot Rom Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swBootRomVer	Read only	String (size (0-20))	
Switch Operation Code Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swOpCodeVer	Read only	String (size (0-20))	

3.2.4 Managing Firmware

You can upload and download firmware to and from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version.

When downloading software files, note the following points:

- The destination file name should not contain slashes (\ or /).
- The leading character of the file name should not be a period (.).
- The maximum length for file names on the TFTP server is 127 characters.
- The maximum length for file names on the switch is 32 characters.
- Valid characters are A-Z, a-z, 0-9, ".", "-", and "_".
- Only two copies of the System Software file (containing the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted. If there are two copies of the System Software file present, you can delete the one that is not currently designated as the startup version and replace it with a new file, or you can copy a new one into the directory using one of the existing file names. Alternatively you can remove the startup designation from the current startup file, delete that file, copy a new version of the System Software file into the directory, and finally make the new file the designated startup file.

3.2.4.1 Downloading Switch Firmware From a Server

When downloading runtime code, you can specify the destination file name to overwrite the current image, or first download the file to a different file name and then set the new file as the startup file.

Web Interface: Downloading Switch Firmware

1. **Open the Switch Status ⇒ Software window.**
2. **Type the IP address of the TFTP server.**
3. **Type the file name of the software to download, select a file on the switch to overwrite, or specify a new file name.**
4. **Click Download.**

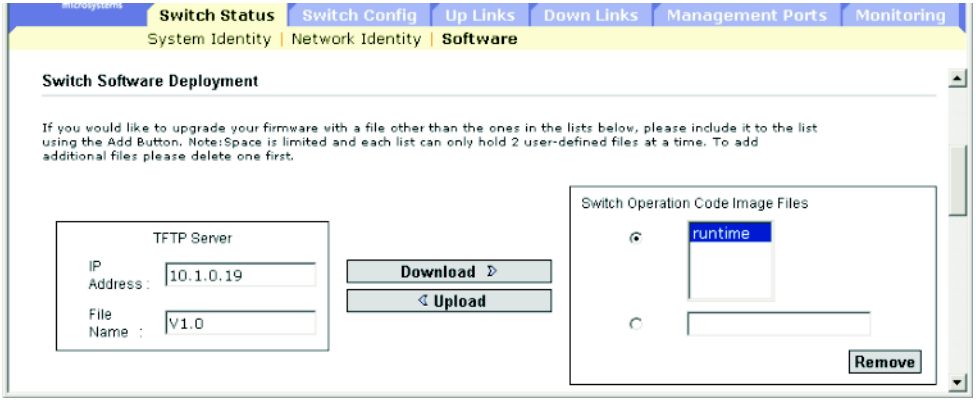


FIGURE 3-8 **The Switch Status ⇒ Software Window (for downloading firmware)**

Note – If you receive an error message saying that the data you have entered is invalid, you might have typed an incorrect IP address or an incorrect file name, or you not might have the correct access permissions for TFTP transfer. Alternatively, it is possible that there is not enough memory available on the switch.

If you download to a new destination file, select the new file from the pull-down menu for the operation code used at startup and click Save. To start the new firmware, reboot the system by clicking Save and Restart.

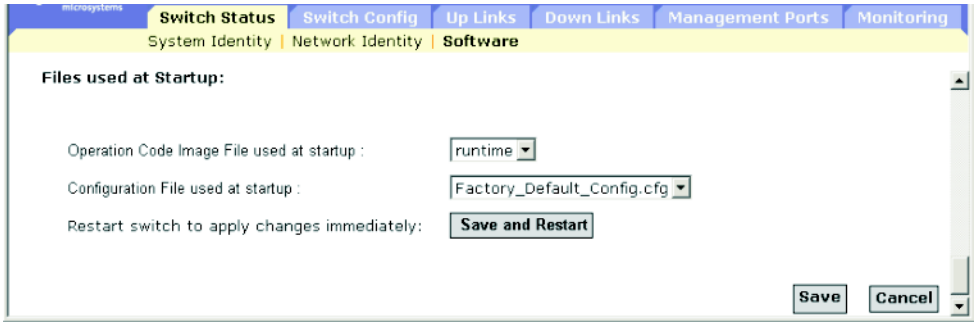


FIGURE 3-9 The Switch Status ⇒ Software Window (at the End of the Download Process)

Command-line Interface: Dowloading Switch Firmware

1. **Type the IP address of the TFTP server.**
2. **Select** `config` **or** `opcode` **file type.**

3. **Type the source and destination file names.**
4. **Set the new file to start up the system.**
5. **Restart the switch.**

```
Console#copy tftp file
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
Console(config)#exit
Console#reload
```

To start new firmware, use the `reload` command to reboot the system.

MIB Variables Associated With Downloading Firmware

TABLE 3-7 MIB Variables Associated With Downloading Firmware

Field Name	MIB Variable	Access	Value Range
Switch Operation Code Image Files	*Not defined*		
TFTP Server IP Address	`sun... tftpMgt. tftpServer`	Read/write	IP address
TFTP File Type	`sun... tftpMgt. tftpFileType`	Read/write	opcode (1), config (2)
TFTP Source File Name	`sun... tftpMgt. tftpSrcFile`	Read/write	String (size (0-127))

TABLE 3-7 MIB Variables Associated With Downloading Firmware *(Continued)*

Field Name	MIB Variable	Access	Value Range
TFTP Destination File Name	`sun... tftpMgt. tftpDestFile`	Read/write	String (size (0-127))
TFTP Action	`sun... tftpMgt. tftpAction`	Read/write	notDownloading (1), downloadToPROM (2), downloadToRAM (3) (*not supported)* upload (4)
TFTP Status	`sun... tftpMgt. tftpStatus`	Read/write	tftpSuccess (1), tftpStatusUnknown (2), tftpGeneralError (3), tftpNoResponseFromServer (4), tftpDownloadChecksumError (5), tftpDownloadIncompatible Image(6), tftpTftpFileNotFound(7), tftpTftpAccessViolation(8)
Restart Operation Code File	`sun... restartMgt. restartOpCodeFile`	Read/write	Display String (Size (0-127))
Restart Action	`sun... restartMgt. restartControl`	Read/write	running (1), warmBoot (2), coldBoot (3)

3.2.5 Saving or Restoring Configuration Settings

You can upload and download configuration settings to and from a TFTP server. The configuration file can later be downloaded to restore the switch's settings.

When downloading configuration files, note the following points:

- The destination file name should not contain slashes (\ or /).
- The leading character of the file name should not be a period (.).
- The maximum length for file names on the TFTP server is 127 characters.
- The maximum length for file names on the switch is 32 characters.
- Valid characters are A-Z, a-z, 0-9, ".", "-", and "_".
- The maximum number of user-defined configuration files is limited by available memory.

3.2.5.1 Downloading Configuration Settings From a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to overwrite it. Note that `Factory_Default_Config.cfg` can be copied to the TFTP server but cannot be used as the destination on the switch (it cannot be overwritten).

Web Interface: Downloading a File of Configuration Settings

1. **Open the Switch Setup ⇒ Software window.**
2. **Type the IP address of the TFTP server.**
3. **Type the name of the file to download, select a file on the switch to overwrite, or specify a new file name.**
4. **Click Download.**

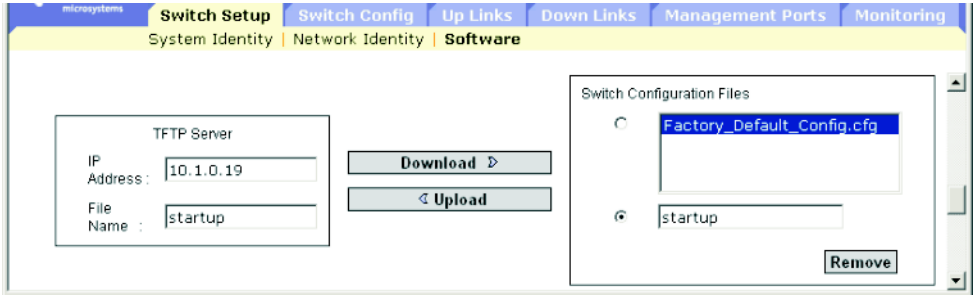


FIGURE 3-10 The Switch Setup ⇒ Software Window (for downloading a configuration file)

If you download to a new file name, select the new file from the pull-down menu and click Save. To use the new settings, reboot the system by clicking Save and Restart.

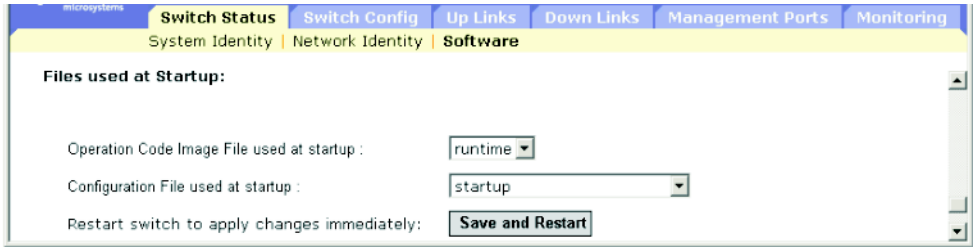


FIGURE 3-11 The Switch Setup ⇒ Software Window (enabling you to specify the operation code and configuration file to use at startup)

Command-line Interface: Downloading a File of Configuration Settings

1. **Type the IP address of the TFTP server.**
2. **Specify the source file on the server.**
3. **Set the startup file on the switch.**

4. **Restart the switch.**

```
Console#copy tftp startup-config
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
```

If you download the startup configuration file under a new file name, you can set this file as the startup file at a later time, and then restart the switch.

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

MIB Variables Associated With Downloading Configuration Settings

TABLE 3-8 MIB Variables Associated With Downloading Configuration Settings

Field Name	MIB Variable	Access	Value Range
TFTP Server IP Address	sun... tftpMgt. tftpServer	Read/write	IP address
TFTP File Type	sun... tftpMgt. tftpFileType	Read/write	opcode (1), config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	Read/write	Display string (size (0-127))
TFTP Action	sun... tftpMgt. tftpAction	Read/write	notDownloading (1), downloadToPROM (2), downloadToRAM (3), upload (4)

TABLE 3-8 MIB Variables Associated With Downloading Configuration Settings

Field Name	MIB Variable	Access	Value Range
TFTP Status	`sun... tftpMgt. tftpStatus`	Read/write	tftpSuccess (1), tftpStatusUnknown (2), tfttpGeneralError (3), tftpNoResponseFromServer (4), tftpDownloadChecksumError (5), tftpDownloadIncompatibleImage (6), tftpTftpFileNotFound(7), tftpTftpAccessViolation(8)
Restart Configuration File	`sun... restartMgt. restartConfigFile`	Read/write	Display string (size (0-127))
Restart Action	`sun... restart.Mgt. restartControl`	Read/write	running (1), warmBoot (2), coldBoot (3)

3.2.6 Configuring User Authentication

Use the Security menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.

There are two access types: Normal and Privileged. Normal level only provides access to a limited number of commands, while Privileged level provides access to all commands. The default administrator account has write access for all of the parameters governing the switch. You should therefore assign a password as soon as possible and store it in a safe place.

Note – The default administrator user name is `admin` with the password `admin`.

Note the following points about configuring user authentication:

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for each remote authentication protocol specified.
- Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to

RADIUS-aware or TACACS+-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to a switch.

Note – When setting up privilege levels on a RADIUS or TACACS+ server, remember that level 0 allows guest (Normal Exec) access to the switch. Only level 15 allows administrator (Privileged Exec) access.

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication controls management access through the console port, Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify one to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS and (2) Local, the user name and password on the RADIUS server are verified first. If the RADIUS server is not available, then the local user name and password are checked.

When configuring user authentication using the web interface or CLI, the following parameters are displayed or can be configured:

- Authentication Mechanisms
  - Require User Authentication – The operating status of user authentication.
  - Preference – The switch attempts to authenticate the user based on the specified sequence.
- Authentication Server Settings
  - Server IP Address – The address of the authentication server. The default is: 10.1.0.1.
  - Server Port Number – The UDP or TCP network port (between 1 and 65,535) of the authentication server used for authentication messages. The default is 1812.
  - Encryption Key – The password (between 1 and 20 characters) used to authenticate logon access for the client. Do not use blank spaces in the string.
  - No. of Retries[7] – The number of times (between 1 and 30) the switch tries to authenticate logon access through the authentication server. The default is 2.

---

7. Applies only to RADIUS server authentication.

- Timeout for reply[8] – Number of seconds (between 1 and 65,535) the switch waits for a reply before resending a request. The default is 5.

- Local Access Authentication
  - User Account – The name (between 1 and 8 characters) of the user. The maximum number of users is 5.
  - Access Level – The user level. Specify Normal or Privileged.
  - Password – The user password. A plain text string of between 1 and 8 characters that is case sensitive.

3.2.6.1 Web Interface: Configuring User Authentication

1. **Open the Switch Config ⇒ Security window.**
2. **Specify the authentication sequence by selecting local or remote methods for each of the three preferences.**
3. **Type parameter values for the specified authentication methods.**
4. **Click Save.**

8. Applies only to RADIUS server authentication.

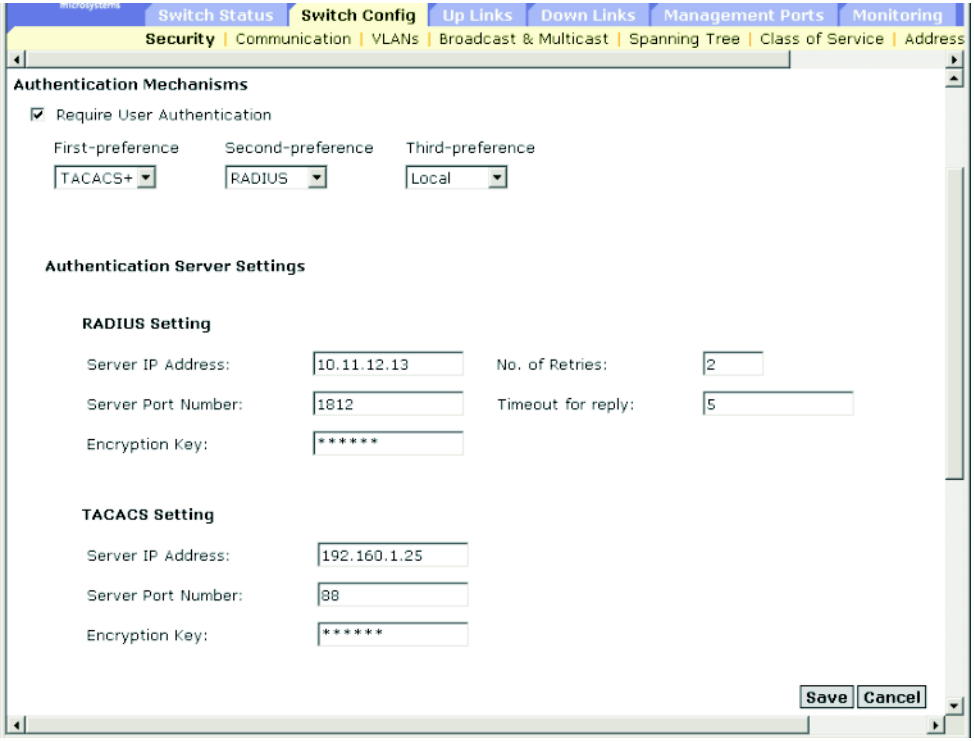


FIGURE 3-12 The Switch Config ⇒ Security Window for Use With Authentication Servers

To configure authentication parameters for local access:

1. **Type a user name.**
2. **Select an access level,** `Normal` **or** `Privileged`**.**
3. **Type a password.**
4. **Click Add.**

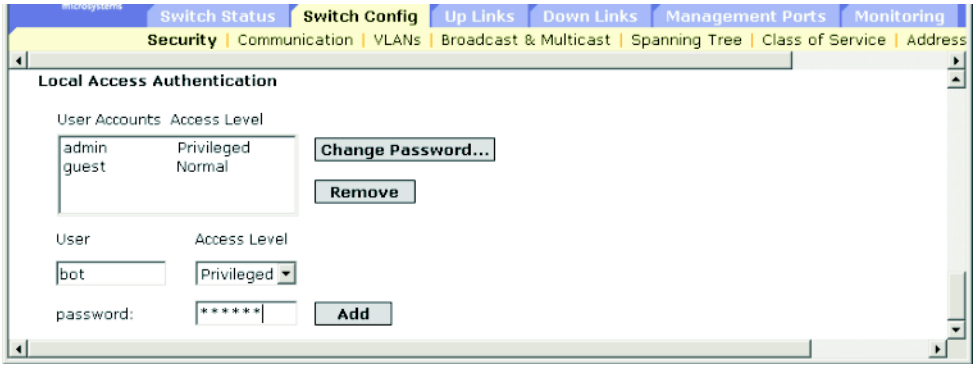


FIGURE 3-13 The Switch Config ⇒ Security Window Showing Locally Stored Logins

3.2.6.2 Command-line Interface: Configuring User Authentication

1. **Assign a user name and access level. Type `0` for Normal access and `15` for Privileged access.**
2. **Specify the password.**
3. **Configure the required settings for RADIUS and TACACS+ remote client authentication.**

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#authentication login local tacacs radius
Console(config)#tacacs-server host 192.168.1.24
Console(config)#tacacs-server port 181
Console(config)#tacacs-server key green
Console(config)#radius-server host 192.168.1.25
Console(config)#radius-server port 181
Console(config)#radius-server key white
Console(config)#radius-server retransmit 5
Console(config)#radius-server timeout 10
Console(config)#
```

3.2.6.3 MIB variables Associated With User Authentication

TABLE 3-9 MIB Variables Associated With User Authentication

Field Name	MIB Variable	Access	Value Range	Default Value
User Name	*Not Defined*			
Password	*Not Defined*			
Access Level	*Not Defined*			
Authentication Sequence	*Not Defined*			
RADIUS Server Address	`sun... securityMgt.radiusMgt. radiusServerAddress`	Read/write	IP address	10.11.12 .13
RADIUS Server Port Number	`sun... securityMgt.radiusMgt. radiusServerPortNumber`	Read/write	Integer (1-65535)	1812
RADIUS Server Encryption Key	`sun... securityMgt.radiusMgt. radiusServerKey`	Read/write (Read always returns 0)	String (size (0-20))	
RADIUS Server Retransmit	`sun... securityMgt.radiusMgt. radiusServerRetransmit`	Read/write	Integer (1-65535)	2
RADIUS Server Timeout	`sun... securityMgt.radiusMgt. radiusServerTimeout`	Read/write	Integer (1-65535) seconds	5
TACACS Server Address	`sun... securityMgt.tacacsMgt. tacacsServerAddress`	Read/write	IP address	
TACACS Server Port Number	`sun... securityMgt.tacacsMgt. tacacsServerPortNumber`	Read/write	Integer (1-65535)	
TACACS Server Encryption Key	`sun... securityMgt.tacacsMgt. tacacsServerKey`	Read/write (Read always returns 0)	String (size (0-20))	

3.2.7 Configuring SNMP

The Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices or other elements on a network.

Equipment commonly managed with SNMP includes switches, routers, and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

The blade system chassis switch includes an on-board SNMP agent that continuously monitors the status of its hardware and the traffic passing through its ports. A network management station can access this information using software such as Solstice Domain Manager. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

3.2.7.1 Configuring SNMP Access

You can configure up to five community strings authorized for management access. For security reasons, consider removing the default strings.

When configuring SNMP community strings using the web interface or CLI, the following parameters can be configured:

- Community – A password (between 1 and 32 characters, which is case sensitive) that permits access to the SNMP protocol. The default community strings are `public` (read-only access) and `private` (read/write access)
- Access Level
  - Read Only – Read-only access. Authorized management stations are able to only retrieve MIB objects.
  - Read/Write – Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Web Interface: Adding and Removing Community Strings

1. **Open the Switch Config ⇒ Communication window.**
2. **Type the new community string in the String text field.**
3. **Select the access rights from the Access Level pull-down menu.**
4. **Click Add.**

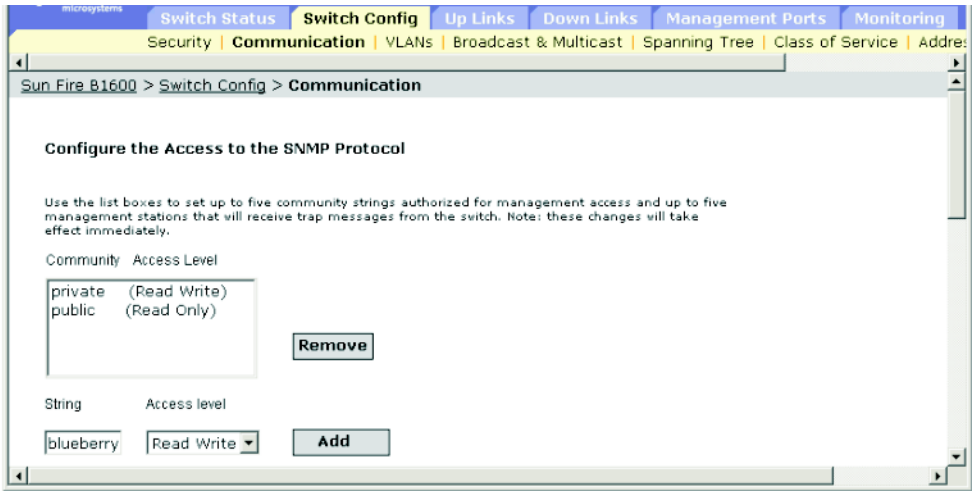


FIGURE 3-14 The Switch Config ⇒ Communication Window for Adding and Removing Community Strings

Command-line Interface: Adding and Removing Community Strings

The following example adds the string `blueberry` with read/write access.

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

MIB Variables Associated With Community Strings

Note – There are no MIB variables for these functions.

3.2.7.2 Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as Soltice Domain Manager). You can specify up to five management stations that will receive trap messages from the switch. The traps supported by this switch are listed under "Supported Traps" on page A-3.

When configuring SNMP trap managers using the web interface or CLI, the following parameters can be configured:

- IP Address – The Internet address of the host (the targeted recipient). The maximum number of host IP addresses is 5.
- Community – The password-like string (between 1 and 32 characters) sent with the notification operation. Although you can set this string in the Trap Managers table, it is recommended to define this string in the SNMP Protocol table as well.
- Version – The SNMP version (1 or version 2c) that the host is running.
- Generate SNMP notification for
  - Port link up and down events – Whenever a port link is established or broken.
  - Authentication traps – Whenever an invalid community string is submitted during the SNMP access authentication process.

Web Interface: Specifying Trap Management Stations

1. **Open the Switch Setup ⇒ Communications window.**
2. **Type the IP address and community string for each Trap Manager to receive messages.**
3. **Click Add.**
4. **Select Port link up and link down events or Authentication traps if required.**
5. **Click Save.**

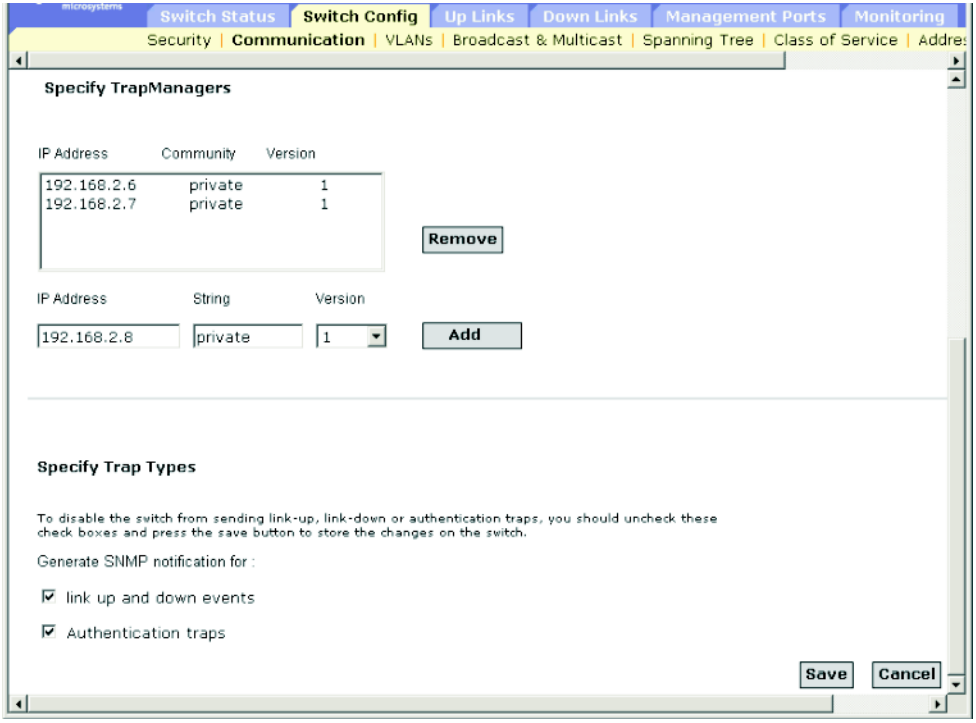


FIGURE 3-15 The Switch Config ⇒ Communication Window Listing the Stations That Receive Traps From the Switch

Command-line Interface: Specifying Trap Management Stations

This example adds a trap manager and enables link-up-down and authentication traps.

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

MIB Variables Associated With Trap Management

TABLE 3-10 MIB Variables Associated With Trap Management

Field Name	MIB Variable	Access	Value Range	Default Value
Trap Destination Address	`sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestAddress`	No access	IP address	
Trap Destination Community	`sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestCommunity`	Read/create	String (size (0-127))	
Trap Destination Version	`sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus`	Read/create	version 1 (1), version 2 (2)	
Trap Destination Status	`sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus`	Read/create	valid (1), invalid (2)	
Enable Link-up-down Traps	`MIB-II ifMIB.ifMIBObjects. ifXTable.ifXEntry. ifLinkUpDownTrapEnable`	Read/write	enabled (1), disabled (2)	enabled

3.3 Configuring Global Network Protocols

This section describes how to configure global switch settings for virtual LANs, multicast service, Spanning Tree Algorithm, handling data based on specific class-of-service requirements, and displaying the address table or setting static addresses.

3.3.1 VLAN Configuration

In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q-compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and efficient network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic and enable you to make network changes without having physically change network connections. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer-3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of

the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note – VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but should not be used for any end-node host that does not support VLAN tagging.

Note these points about assigning ports to VLANs:

- VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.
- Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by using a Layer-3 router or switch.
- Port-based VLANs – Port-based (or static) VLANs are manually tied to specific ports. The switch's forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding or flooding decisions, the switch must learn the relationship of the MAC address to its related port—and thus to the VLAN—at run-time. However, when GVRP is enabled, this process can be fully automatic.
- Automatic VLAN Registration – GARP VLAN Registration Protocol (GVRP) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on end-station requests.

  To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. (See "Configuring VLAN Behavior for Interfaces" on

page 3-114.) You should also determine security boundaries in the network and disable GVRP on end-station ports where you need to prevent advertisements from being propagated, or forbid ports from joining restricted VLANs.

Note – If you have host devices that do not support GVRP, you must configure static VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs" on page 3-50). But you still need to enable GVRP on these edge switches, as well as on the core switches in the network.

- If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you need to create a VLAN for that group and enable tagging on all ports.

  Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

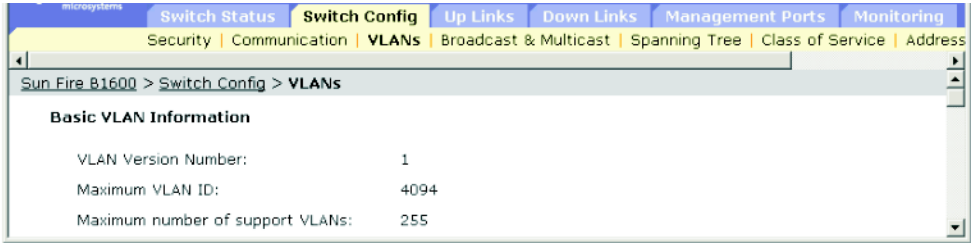
3.3.1.1 Displaying Basic VLAN Information

When displaying basic VLAN information using the web interface or CLI, the following parameters are displayed:

- VLAN Version Number – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- Maximum VLAN ID – The maximum VLAN ID recognized by this switch.
- Maximum Number of Supported VLANs – The maximum number of VLANs that can be configured on this switch.

Web Interface: Displaying Basic VLAN Information

- **Open the Switch Config ⇒ VLANs window.**



Command-line Interface: Displaying Basic VLAN Information

- **Type the following command:**

```
Console#show bridge-ext
 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#
```

MIB Variables Associated With Basic VLAN Information

TABLE 3-11 MIB Variables Associated With Basic VLAN Information

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN Version Number	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects . dot1qBase. dot1qVlanVersion-Number	Read only	version1 (1)	version1
Maximum VLAN ID	MIB-II. dot1dBridge. BridgeMIB. BridgeMIBObjects. dot1qBase. dot1qMaxVlanId	Read only	Integer	4094
Maximum Number of Supported VLANs	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects . dot1qBase. dot1qMaxSupportedV lans	Read only	Integer	255
Device Capabilities	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects . dot1dExtBase. dot1dDeviceCapabi lities	Read only	Bit String – ExtendedFiltering dot1dServices (0), dot1dTrafficClasses (1), StaticEntry dot1dIndividualPort (2), dot1dIVLCapable (3), dot1dSVLCapable (4), dot1dHybridCapable (5), dot1dConfigurablePvi d dot1dTagging (6), dot1dLocalVlanCapable (7)	2, 3, 6, 7

TABLE 3-11 MIB Variables Associated With Basic VLAN Information *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
Traffic Classes Enabled	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dTrafficClasses-Enabled	Read/ write	true (1), false (2)	true
GMRP Status	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dGmrpStatus	Read/ write	enabled (1), disabled (2)	disabled
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	Read/ write	enabled (1), disabled (2)	disabled

3.3.1.2 Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Web Interface: Enabling or Disabling GVRP (Global Setting)

1. **Open Switch Config ⇒ VLANs.**
2. **Select Enable or Disable.**
3. **Click Save.**

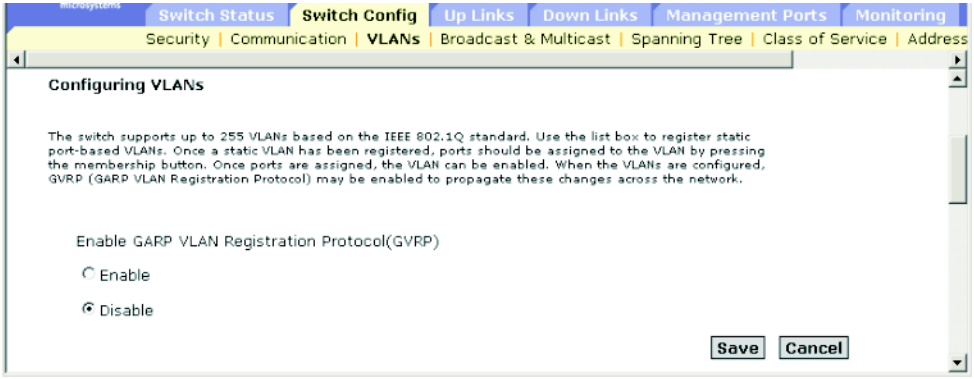


FIGURE 3-16 The Switch Config ⇒ VLANs Window (showing radio buttons for enabling GVRP)

Command-line Interface: Enabling GVRP

Th following sample command enables GVRP for the switch:

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

MIB Variables Associated With GVRP

TABLE 3-12 MIB Variables Associated With GVRP

Field Name	MIB Variable	Access	Value Range	Default Value
GVRP Status	`MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects . dot1qBase. dot1qGvrpStatus`	Read/write	enabled (1), disabled (2)	disabled

3.3.1.3 Configuring VLANs

When configuring VLANs using the web interface or CLI, the following parameters are displayed or can be configured:

- ID – The ID of configured VLAN (1 to 4094).
- Name – The name of the VLAN (1 to 15 characters).
- Status – The current operational state of the VLAN.
  - Enable (Active[9]) – The VLAN is active.
  - Disable (Suspend[9]) – The VLAN is suspended; that is, it does not pass packets.
- Creation Type – The method by which the VLAN was added to the switch.
  - Dynamic GVRP (Dynamic[9]): Automatically learned through GVRP.
  - Permanent (Static[9]): Manually configured as a static entry.
- Ports / Channel groups[9] – The interfaces that are members of the VLAN.

Web Interface: Configuring VLANs

To create a new VLAN, follow these steps:

1. **Open Switch Config ⇒ VLANs.**
2. **Type the new VLAN ID and name.**
3. **Set the status to Enabled or Disabled.**
4. **Click Add.**

To modify existing VLANs:

1. **Select one or more entries.**

9. CLI displays these terms.

2. **Click Enable, Disable or Remove.**

To add interfaces to a VLAN:

1. **Select an entry.**
2. **Click Membership.**

(See "Adding Static Members to VLANs" on page 3-50.)

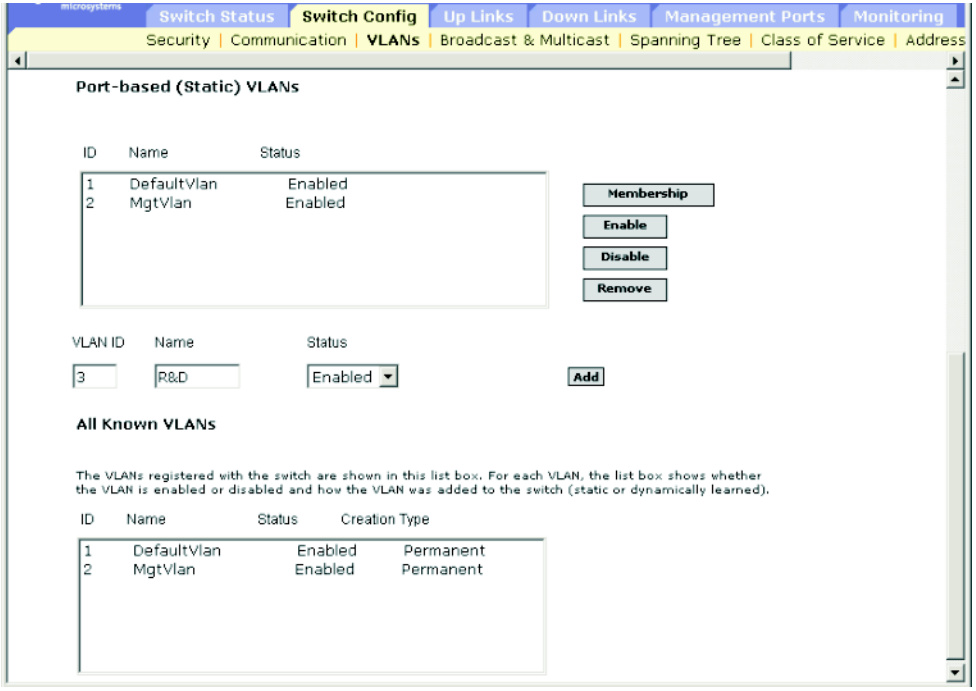


FIGURE 3-17 The Switch Config ⇒ VLANs Window With the Default VLAN Configuration Displayed

Command-line Interface: VLAN Configuration

The following sample commands create a new VLAN and display all VLAN information:

```
Console(config)#vlan database
Console(config-vlan)#vlan 3 name R&D media ethernet state active
Console(config-vlan)#
Console#show vlan
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#
```

MIB Variables Associated With VLAN Configuration

TABLE 3-13 MIB Variables Associated With VLAN Configuration

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN ID	`MIB-II.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qVlanCurrentTable.dot1qVlanCurrentEntry.dot1qVlanIndex`	No access	Integer	1
VLAN Name	`MIB-II.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qVlanStaticTable.dot1qVlanStaticEntry.dot1qVlanStaticName`	Read/ create	Octet string (size (0-32))	
VLAN Status	`MIB-II.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qVlanStaticTable.dot1qVlanStaticEntry.dot1qVlanStatic.RowStatus`	Read/ create	enable(1), disable(2)	

TABLE 3-13 MIB Variables Associated With VLAN Configuration *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN Type	`MIB-II.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qVlanCurrentTable.dot1qVlanCurrentEntry.dot1qVlanStatus`	Read only	other(1), permanent(2), dynamicGvrp(3)	
VLAN Ports	`MIB-II.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qVlanCurrentTable.dot1qVlanCurrentEntry.dot1qVlanCurrent-EgressPorts`	Read only	Octet string (port list)	

3.3.1.4 Adding Static Members to VLANs

When adding static members to VLANs using the web interface or CLI, the following parameters are displayed or can be configured:

- Name – The name of the VLAN.
- Up Time at Creation – The time the VLAN was created.
- Status[10] – The method by which the VLAN was added to the switch.
  - Dynamic: Automatically learned through GVRP.
  - Static: Manually configured as a static entry.
- All Ports – The port or port-channel identifier.
- Membership Ports – The interfaces added to the selected VLAN as tagged or untagged, or restricted from being automatically added through GVRP.
- Membership Type – Specify VLAN membership by highlighting the required interface, and clicking the appropriate Add button:

10.CLI only.

- Add Tagged: The interface is a member of the VLAN. All packets transmitted by the port on this VLAN will be tagged, that is, carry a tag and therefore carry VLAN or COS information.
- Add Untagged: The interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or COS information.
- Add Forbidden: The interface is forbidden from automatically joining the VLAN through GVRP. See "Automatic VLAN Registration" on page 3-40.
- Remove: Removes the selected interface from the VLAN.

Web Interface: Adding Ports Manually to a VLAN

To add an interface to a VLAN:

1. **Open Switch Config ⇒ VLANs.**
2. **Highlight a VLAN in the static list, and click Membership.**
3. **From the port membership page, select an interface from the All Ports list (port or port-channel).**
4. **Click Add Tagged, Add Untagged, or Add Forbidden (to prevent this interface from being added through GVRP).**

To remove an interface from a VLAN:

1. **Select an entry from the Membership Ports list.**
2. **Click Remove.**

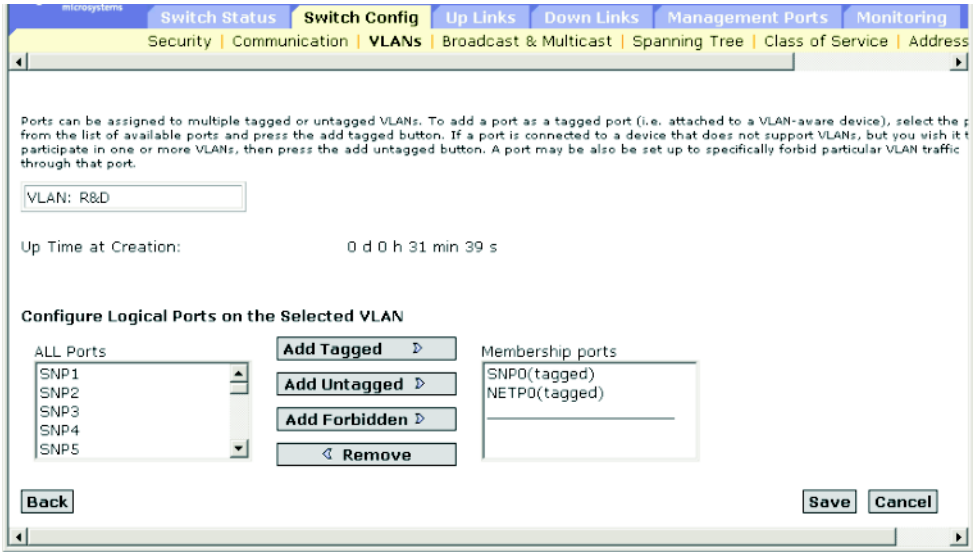


FIGURE 3-18 The Switch Config ⇒ VLANs Window

Command-line Interface: Adding Ports Manually to a VLAN

The following example adds two ports to VLAN 3 (named R&D), forbids server blade port SNP13 from joining the VLAN dynamically (using GVRP), and finally displays the VLAN's membership:

```
Console(config)#interface ethernet NETP1
Console(config-if)#switchport allowed vlan add 3 tagged
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#
```

MIB Variables Associated With Adding Ports to a VLAN

TABLE 3-14 MIB Variables Associated With Adding Ports to a VLAN

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN ID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	Index	Row	
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Read/create	Octet string (size (0-32))	
Up Time at Creation	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCreationTime	Read only	Timeticks (in centiseconds)	
VLAN Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	Read only	other(1), permanent(2), dynamicGvrp(3)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic- UntaggedPorts	Read/create	Octet string (port list)	

TABLE 3-14 MIB Variables Associated With Adding Ports to a VLAN *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden- EgressPorts	Read/create	Octet string (port list)	
Port Trunk Index (Channel Groups)	sun... portMgt. portTable portEntry. portTrunkIndex	Read only	Integer	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic- RowStatus	Read/create	enable(1), disable(2)	

3.3.2 Multicast Configuration

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network and any hosts that want to receive the multicast service register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts that subscribed to the service.

The blade system chassis switch uses the Internet Group Management Protocol (IGMP) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. This procedure is called *multicast filtering*.

The purpose of IP multicast filtering is to optimize a switched network's performance, so that multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

3.3.2.1 Configuring IGMP Snooping Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Note the following points about IGMP snooping:

- IGMP Snooping – The switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly.
- IGMP Querier – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note – Multicast routers use this information, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet.

When configuring IGMP snooping through the web interface or CLI, the following parameters are displayed or can be configured:

- IGMP Snooping – The operating status of IGMP. When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. The default is Disabled.
- IGMP Protocol Version – The protocol version. Specify 1 or 2 for compatibility with other devices on the network. The default is 2.
- IGMP Querier – The operating status of IGMP querier. When enabled, the switch can serve as the querier, which is responsible for asking hosts if they want to receive multicast traffic. The default is Disabled.
  - Query Count – The maximum number of queries issued (between 2 and 10) for which there has been no response before the querier takes action to drop a client from the multicast group. The default is 2.

- Query Interval – The frequency (between 60 and 125 seconds) at which the switch sends IGMP host-query messages. The default is 125 seconds.
- Query Report Delay – The time (between 5 and 25 seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. The default is 10 seconds.
- Router Port Expire Time – The time (between 300 and 500 seconds) the switch waits after the previous querier stops querying before it determines that the interface (which had been receiving query packets) is no longer attached to a querier. The default is 300 seconds.

Note – All systems on the subnet must support the same version.
Some attributes are only enabled for IGMPv2, including IGMP Report Delay and Router Port Expire Time.

Web Interface: Configuring IGMP Snooping Parameters

1. **Open Switch Config ⇒ Broadcast & Multicast ⇒ IGMP Parameters.**
2. **Adjust the IGMP settings as required.**
3. **Click Save.**

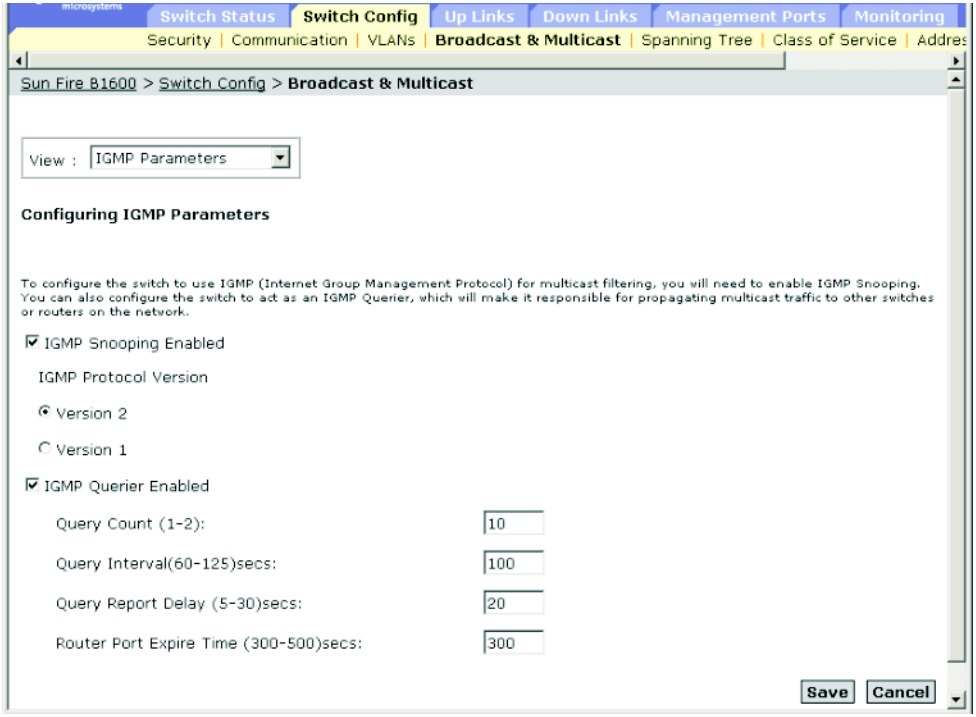


FIGURE 3-19 The Switch Config ⇒ Broadcast & Multicast Window

Command-line Interface: Configuring IGMP Snooping Parameters

This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping
Console(config)#ip igmp snooping querier
Console(config)#ip igmp snooping query-count 10
Console(config)#ip igmp snooping query-interval 100
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#ip igmp router-port-expire-time 300
Console(config)#ip igmp snooping version 2
Console(config)#exit
Console#show ip igmp snooping
 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#
```

MIB Variables Associated With IGMP Parameters

TABLE 3-15 MIB Variables Associated With IGMP Parameters

Field Name	MIB Variable	Access	Value Range	Default Value
Snooping Status	`sun... igmpSnoopMgt. igmpSnoopStatus`	Read/write	enabled (1), disabled (2)	enabled
Snooping Querier	`sun... igmpSnoopMgt. igmpSnoopQuerier`	Read/write	enabled (1), disabled (2)	enabled
Snooping Query Count	`sun... igmpSnoopMgt. igmpSnoopQueryCount`	Read/write	Integer (2-10)	2
Snooping Query Interval	`sun... igmpSnoopMgt. igmpSnoop- QueryInterval`	Read/write	Integer (60-125) seconds	125
Snooping Query Max Response Time	`sun... igmpSnoopMgt. igmpSnoopQuery- MaxResponseTime`	Read/write	Integer (5-25) seconds	10
Snooping Router Port Expire Time	`sun... igmpSnoopMgt. igmpSnoopRouterPort -ExpireTime`	Read/write	Integer (300-500) seconds	300
Snooping Version	`sun... igmpSnoopMgt. igmpSnoopVersion`	Read/write	Integer (1-2)	2

3.3.2.2 Specifying Interfaces Connected to Multicast Routers

Multicast routers use the information obtained from IGMP Query, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or aggregated link) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the connected router. This can ensure that multicast traffic is passed on to all the appropriate interfaces within the switch.

When specifying interfaces connected to multicast routers through the web interface or CLI, the following parameters are displayed or can be configured:

- All known ports in VLAN connected to multicast routers:
  - VLAN – The VLAN on the switch.
    (The pull-down menu includes the VLAN ID and name.)
  - Interface – The interfaces connected to a multicast router and the whether the assignment was static (Static) or dynamic (IGMP).
- Ports in the VLAN statically connected to multicast routers:
  - Available Ports – The interfaces that have not been assigned to the selected VLAN as multicast router ports.
  - Current Static Ports – The interfaces that have already been assigned to the selected VLAN as multicast router ports.

Web Interface: Specifying Interfaces Connected to Multicast Routers

1. **Open Switch Config ⇒ Broadcast & Multicas ⇒ Multicast Router Ports.**
2. **Select a VLAN.**
3. **Click Query to display all the interfaces in the VLAN that are connected to multicast routers.**
4. **From the Available Ports, select an interface that is connected to a multicast router**
5. **Click Add.**
6. **From Current Static Ports, select an interface that is no longer connected to a multicast router.**
7. **Click Remove.**

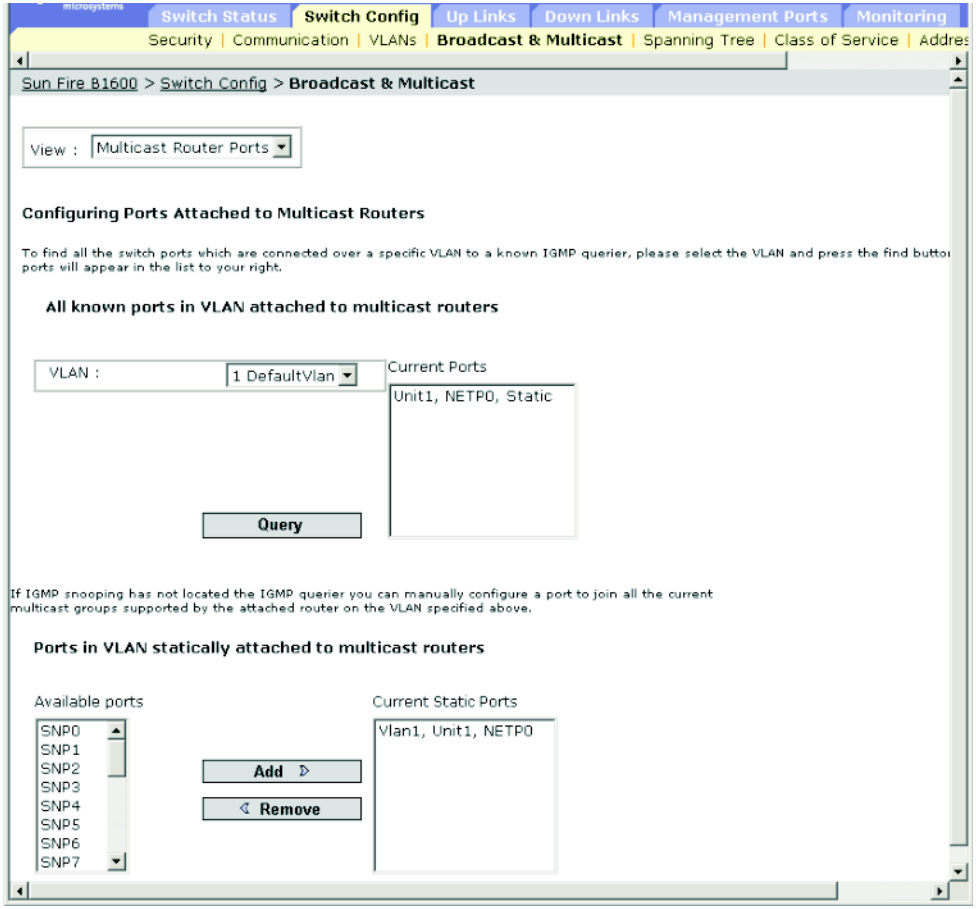


FIGURE 3-20 The Switch Config ⇒ Broadcast & Multicast Window (Multicast Router Ports selected)

Command-line Interface: Specifying Interfaces Connected to Multicast Routers

The following example configures port NETP0 as a multicast router port within VLAN 1 and then displays a confirmation of this configuration:

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

MIB Variables Associated With Interfaces Connected to Multicast Routers

TABLE 3-16 MIB Variables Associated With Interfaces Connected to Multicast Routers

Field Name	MIB Variable	Access	Value Range
Snooping Multicast Router Current VLAN	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. dot1qVlanIndex	Index	Integer
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Read/create	Octet string (size (0-32))
Snooping Multicast Router Current Ports	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. igmpSnoopRouterCurrentPorts	Read only	Octet string (port list)
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. dot1qVlanIndex	Index	Integer

TABLE 3-16 MIB Variables Associated With Interfaces Connected to Multicast Routers

Field Name	MIB Variable	Access	Value Range
Snooping Multicast Router Static Ports	`sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticPorts`	Read/create	Octet string (port list)
Snooping Multicast Router Static Status	`sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus`	Read/create	valid(1), invalid(2)

3.3.2.3 Configuring Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in "Configuring IGMP Snooping Parameters" on page 3-55. For certain applications that require tighter control, you might need to manually assign a multicast service to a specific interface. First add all the ports connected to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Note the following points about configuring multicast services:

- Static multicast addresses are never aged out.
- When a multicast address is statically assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports in that VLAN.

When configuring multicast services through the web interface or CLI, the following parameters are displayed or can be configured:

- All known ports and Multicast Services supported on VLAN:
  - VLAN – The VLAN on the switch.
    (The pull-down menu includes the VLAN ID and name.)
  - IP Address – The IP address for a specific multicast service.
  - Interface – The interfaces that are connected to multicast routers and whether the assignment was static (User) or dynamic (IGMP).
- Ports and Multicast Services statically configured on VLAN:
  - IP Address – The IP address for a specific multicast service.
  - Available Ports – The interfaces that have not been assigned to the selected VLAN to support a specific multicast service.
  - Current Static Ports (IP Addresses) – The interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service. Includes the IP address assigned to the interface.

Web Interface: Configuring Multicast Services

- **Open Switch Config ⇒ Broadcast & Multicast ⇒ Multicast Support.**

To display the switch interfaces that propagate a specific multicast service:

1. **Select the VLAN ID and the IP address for a multicast service from the pull-down menus.**
2. **Click Query.**

To manually assign a multicast service to a specific interface:

1. **Select the VLAN from the pull-down menu.**

2. **Type the IP address for the multicast service in the text field.**

3. **Click Add.**

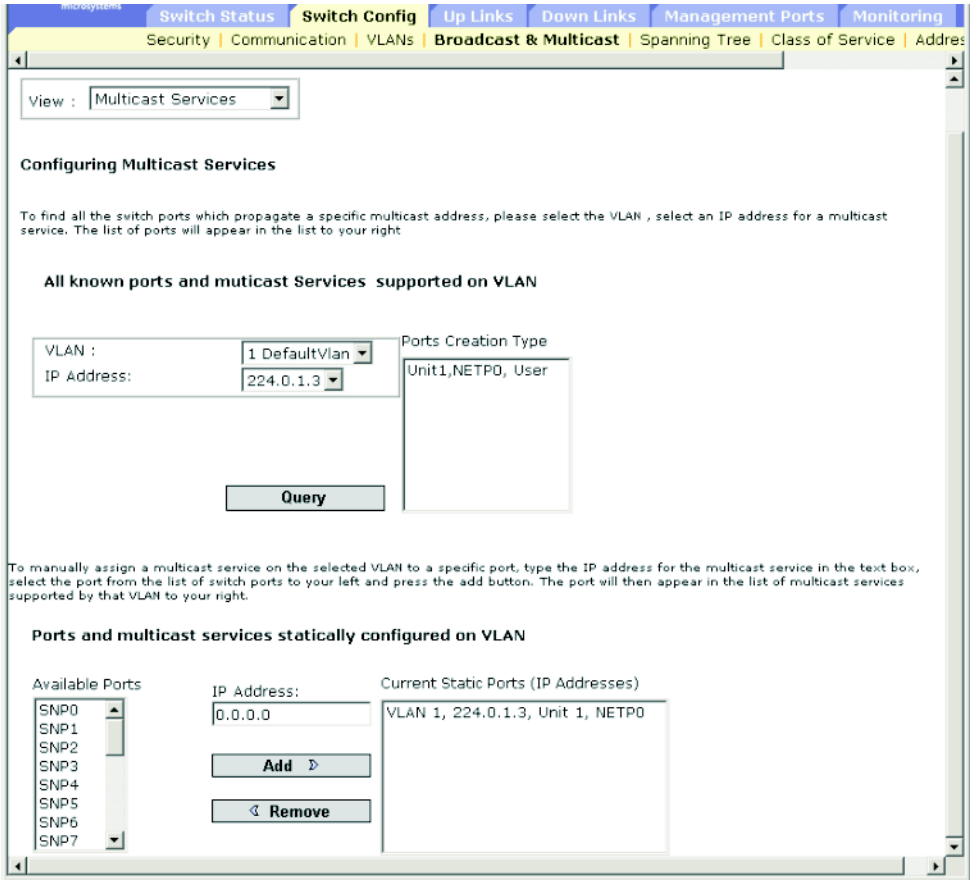


FIGURE 3-21 The Switch Config ⇒ Broadcast & Multicast Window (Multicast Services selected)

Note – If you receive an error message saying that the data you have entered is invalid, check that you have specified each of the IP addresses correctly.

Command-line Interface: Configuring Multicast Services

The following example assigns a multicast address to port NETP0 and then displays all the known multicast services supported on VLAN 1.

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

MIB Variables Associated With Configuring Multicast Servcies

TABLE 3-17 MIB Variables Associated With Configuring Multicast Services

Field Name	MIB Variable	Access	Value Range
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. dot1qVlanIndex	Index	Integer
Snooping Multicast Static IP Address	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticIPAddress	Index	IP address
Snooping Multicast Static Port List	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticPorts	Read/create	Octet string (port list)
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	Read/create	valid(1), invalid(2)

3.3.3 Broadcast Storm Control (Global Setting)

Broadcast storms can occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to a complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic that applies to every port and then enabling broadcast storm control on the required ports.

Any broadcast packets exceeding the specified threshold are dropped.

Note the following points about broadcast storm control:

- Broadcast storm control is enabled by default.
- Broadcast control does not affect IP multicast traffic.

When configuring broadcast storm control through the web interface or CLI, the following parameter can be configured:

- Broadcast Storm Threshold Level[11] – The threshold in packets per second. Specify 16, 64, 128, or 256 packets per second. The default is 256.

3.3.3.1 Web Interface: Using Broadcast Storm Control

1. **Open Switch Config ⇒ Broadcast & Multicast ⇒ Broadcast Parameters.**
2. **Select the threshold level.**
3. **Click Save.**

11.CLI shows "Broadcast Storm Limit."

FIGURE 3-22 The Switch Config ⇒ Broadcast & Multicast Window (Broadcast Storms selected)

3.3.3.2 Command-line Interface: Using Broadcast Storm Control

The following example shows how to set the broadcast threshold to 64 packets per second.

Note – Note that the `switchport broadcast` command enables broadcast storm control on the *specified* interface and sets the broadcast threshold for *every* interface on the switch.

```
Console(config)#interface ethernet NETP7
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#end
Console#show interfaces status ethernet NETP7
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: 64 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#
```

MIB Variables Associated With Broadcast Storm Control

TABLE 3-18 MIB Variables Associated With Broadcast Storm Control

Field Name	MIB Variable	Access	Value Range	Default Value
Broadcast Storm Packet Rate	`sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormPktRate`	Read/write	Integer (16, 64, 128, 256)	256
Broadcast Storm Status	`sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus`	Read/write	enabled (1), disabled (2)	enabled

3.3.4 Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link fails.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)

RSTP is a general replacement for the slower, legacy STP. RSTP achieves must faster reconfiguration (around one tenth of the time required by STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

3.3.4.1 Configuring Basic STA Settings

Global settings apply to the entire switch.

Note the following points about basic STA settings:

- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits:

  - STP Mode – If the switch receives an 802.1D BPDU (STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

When configuring basic STA settings through the web interface or CLI, the following global parameters can be configured:

- Enable Spanning Tree – The current operational status of STA on the switch.
- Spanning Tree Protocol – The type of spanning tree used on the switch:
  - STP: Spanning Tree Protocol (IEEE 802.1D). When this option is selected, the switch will use RSTP set to STP forced-compatibility mode.
  - RSTP: Rapid Spanning Tree Protocol (IEEE 802.1w).

The following global STA paramters are fixed and cannot be changed:

- Bridge ID – The priority and MAC address of the switch.
- Designated Root – The priority and MAC address of the device in the spanning tree that the switch has accepted as the root device.
  - Root Port – The number of the port on the switch that is closest to the root. The switch communicates with the root device through this port. If there is no root port, then the switch has been accepted as the root device of the spanning tree network.
  - Root Path Cost – The path cost from the root port on the switch to the root device.
  - Root Hello Time – The interval (in seconds) after which the current root device transmits a configuration BPDU frame.
  - Root Maximum Age – The maximum time (in seconds) the switch can wait without receiving a configuration message before attempting to reconfigure. All switch ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the switch ports connected to the network. (References to "ports" in this section means "interfaces," which includes both ports and aggregated links.)
  - Root Forward Delay – The maximum time (in seconds) the switch waits before changing states (for example, from discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Root Hold Time – The interval (in seconds) during which no more than two configuration BPDUs shall be transmitted by the switch.

The following root device global parameters can be configured:

- Priority – The bridge priority that is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device (0=highest, 61440=lowest). However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

  Specify a value from 0 to 61,440 in steps of 4096. The possible options are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default is 32,768.

- Hello Time – The interval (in seconds) after which the switch transmits a configuration BPDU frame when it becomes the root device.

  Specify a value from 1 to the lower of 10 or [(Max. Message Age / 2) -1]. The default is 2 seconds.

- Maximum Age – The maximum time (in seconds) the switch can wait without receiving a configuration message before attempting to reconfigure. All switch ports (except for designated ports) receive configuration messages at regular intervals. Any port that ages out the STA information provided in the last configuration message it received becomes the designated port for the connected LAN. If it is a root port, a new root port is selected from among the switch ports connected to the network. (References to "ports" in this section mean "interfaces," which include both ports and trunks.)

  Specify a value from the higher of 6 or [2 x (Hello Time + 1)] to the lower of 40 or [2 x (Forward Delay - 1)]. The default is 20 seconds.

- Forward Delay – The maximum time (in seconds) the switch waits before changing states (for example, from discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

  Specify a value from the higher of 4 or [(Max. Message Age / 2) + 1] to 30 seconds. The default is 15 seconds.

The following global parameters are statistical values and cannot be changed:

- Number of Topology Changes – The number of times the spanning tree has been reconfigured.
- Last Topology Change – The time since the spanning tree was last reconfigured.

Web Interface: Configuring Basic STA Settings

1. **Open Switch Config ⇒ Spanning Tree ⇒ Basic Configuration.**
2. **Modify the required parameters.**
3. **Click Save.**

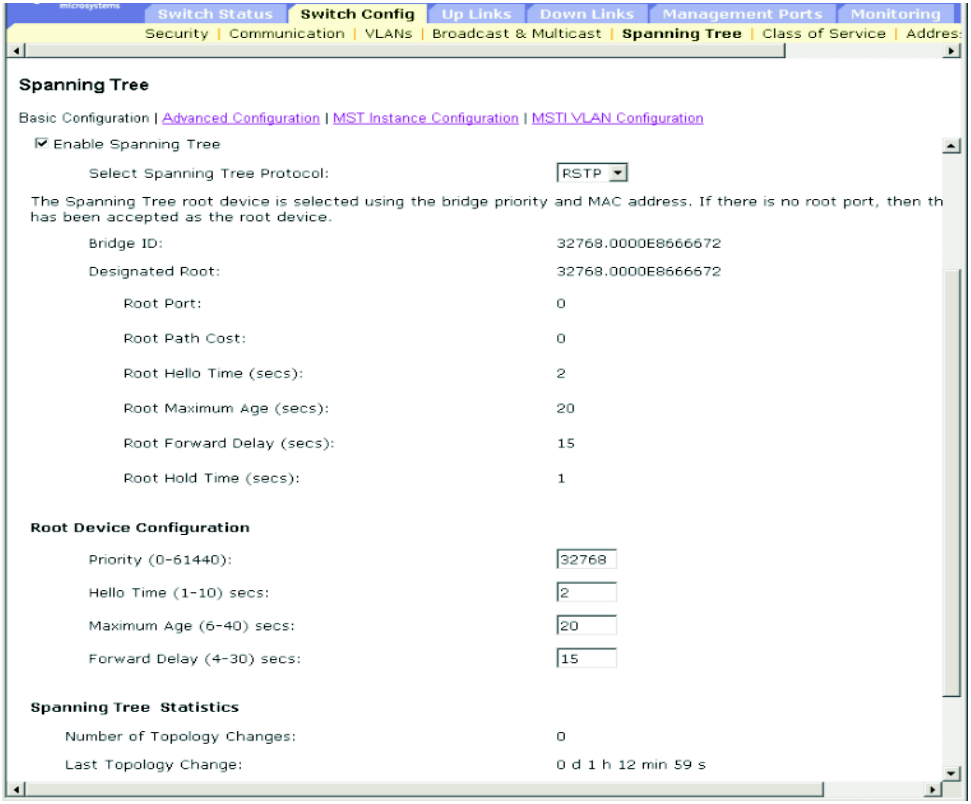


FIGURE 3-23 The Switch Config ⇒ Spanning Tree ⇒ Basic Configuration Window

---

Note – If you receive an error saying that the data you have entered is invalid, check that the values you have given for Priority, Hello Time, Maximum Age, and Forward Delay are within the specified ranges for these parameters.

Command-line Interface: Configuring Basic STA Settings

The following command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree
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
.
.
.
```

Note – The current root port and current root cost display zero when the switch is not connected to the network.

The following example sets the spanning tree mode to RSTP, enables the spanning tree, and then sets the indicated attributes.

```
Console(config)#spanning-tree mode rst
Console(config)#spanning-tree
Console(config)#spanning-tree priority 40000
Console(config)#spanning-tree hello-time 5
Console(config)#spanning-tree max-age 40
Console(config)#spanning-tree forward-time 20
Console(config)#
```

MIB Variables Associated With Basic STA Settings

TABLE 3-19 MIB Variables Associated With Basic STA Settings

Field Name	MIB Variable	Access	Value Range	Default Value
STA System Status	sun...staMgt. staSystemStatus	Read/write	enabled (1), disabled (2)	enabled
STA Protocol Type	sun...staMgt. staProtocolType	Read/write	stp (1), rstp (2),	rstp
Bridge ID	Consists of bridge priority plus MAC address.			
Designated Root	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-DesignatedRoot	Read only	Octet string	
Root Port	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootPort	Read only	Integer	
Root Cost	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootCost	Read only	Integer	
Hello Time	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-HelloTime	Read only	Integer	200 centiseconds
Maximum Age	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgMaxAge	Read only	Integer	2000 centiseconds
Forward Delay	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg-ForwardDelay	Read only	Integer	1500 centiseconds
Priority	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgPriority	Read/write	Integer (0-61440)	32768
Bridge Hello Time	MIB-II. dot1dStp. dot1dStp-BridgeHelloTime	Read/write	Integer (100-1000) centiseconds	200 centiseconds

TABLE 3-19 MIB Variables Associated With Basic STA Settings *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
Bridge Maximum Age	`MIB-II. dot1dStp. dot1dStpBridgeMaxAge`	Read/write	Integer (600-4000) centiseconds	2000 centiseconds
Bridge Forward Delay	`MIB-II. dot1dStp. dot1dStp-BridgeForwardDelay`	Read/write	Integer (400-3000) centiseconds	1500 centiseconds
STA Configuration Changes	`MIB-II. dot1dBridge.dot1dStp. dot1dStpTopChanges`	Read only	Counter	
STA Last Topology Change	`MIB-II. dot1dBridge.dot1dStp. dot1dStpTimeSince-TopologyChange`	Read only	Integer	

3.3.4.2 Configuring Advanced STA Settings

This section describes advanced settings for RSTP.

When configuring RSTP settings through the web interface or CLI, the following parameters can be configured:

- Path Cost Method – The setting that defines the range of values that can be assigned as the path cost of each interface. The path cost is used to determine the best path between devices in the spanning tree.
  - Long: Specifies 32-bit based values that range from 1 to 200,000,000.
  - Short: Specifies 16-bit based values that range from 1 to 65,535.
- Transmission Limit – An RSTP parameter (between 1 and 10) that defines the rate at which each bridge in the spanning tree transmits BPDUs to its neighbours to inform them that the configured ports are still linked. The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. The default is 3.

Web Interface: Configuring Advanced STA Settings

1. **Open Switch Config ⇒ Spanning Tree ⇒ Advanced Configuration.**
2. **Modify the required parameters.**
3. **Click Save.**

FIGURE 3-24 The Switch Config ⇒ Spanning Tree ⇒ Advanced Configuration Window

---

Note – If you receive an error saying that the data you have entered is invalid, check that you have specified a transmission limit within the specified range.

Command-line Interface: Configuring Advanced STA Settings

This example sets the spanning tree path cost method and transmission limit.

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

MIB variables Associated With Advanced STA Settings

TABLE 3-20 MIB Variables Associated With Advanced STA Settings

Field Name	MIB Variable	Access	Value Range	Default Value
RSTP Path Cost Method	`sun... staMgt. staPathCostMethod`	Read/write	short (1), long (2)	long
RSTP Transmission Hold Count	`sun.. staMgt. staTxHoldCount`	Read/write	Integer (1-10)	3

3.3.5 Class of Service Configuration

Class of Service (COS) enables you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. The switch supports COS with four priority queues for each port. Data packets in a port's high-priority queue are transmitted before those in the low-priority queues. You can set the default priority for each interface and configure the mapping of frame priority tags to the switch's priority queues.

3.3.5.1 Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority and then sorted into the appropriate priority queue at the output port.

Note the following points about setting the default priority for interfaces:

- The switch provides four priority queues for each port and uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (that is, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

When setting the default priority for interfaces through the web interface or CLI, the following parameters can be configured:

- Ports – The interface (port or link) and assigned default class-of-service priority.
- Default COS Priority[12] – The priority (between 0 and 7) that is assigned to untagged frames received on the specified interface. The default is 0.

Web Interface: Configuring Class of Service

1. **Open Switch Config ⇒ Class of Service ⇒ Basic Traffic Prioritisation.**
2. **Scroll to Setting the Default CoS Priority for Ports.**
3. **Select an interface from the Ports list.**
4. **Select the default priority.**
5. **Click Save.**

12.CLI displays this information as "Priority for untagged traffic."

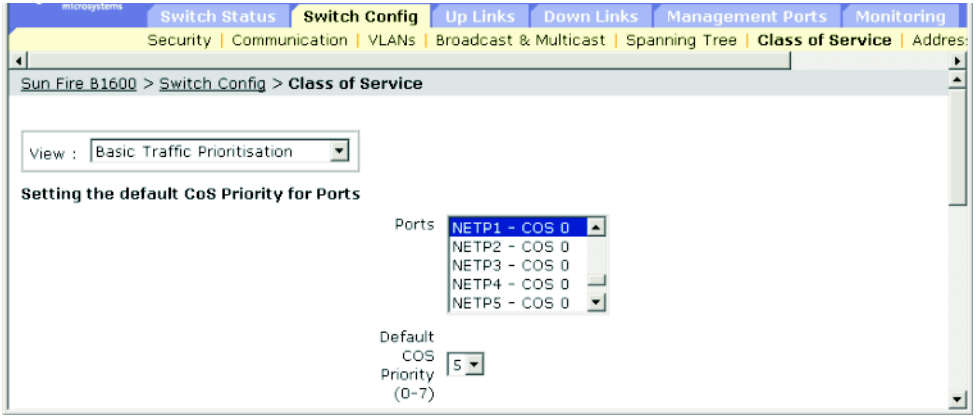


FIGURE 3-25 The Switch Config ⇒ Class of Service

Command-line Interface: Configuring Class of Service

This example assigns a default priority of 5 to port NETP1.

```
Console(config)#interface ethernet NETP1
Console(config-if)#switchport priority default 5
Console#show interfaces switchport ethernet NETP1
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#
```

MIB Variables Associated With Class of Service

TABLE 3-21 MIB Variables Associated With Class of Service

Field Name	MIB Variable	Access	Value Range	Default Value
Port Default User Priority	`MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dPortPriorityTable. dot1dPortPriorityEntry. dot1dPortDefault-UserPriority`	Read/write	Integer (0-7)	0

3.3.5.2 Mapping COS Values to Egress Queues

This switch processes Class of Service (COS) priority tagged traffic by using four priority queues for each port, with service schedules based on Weighted Round Robin (page 3-84). Up to eight separate traffic priorities are defined in the IEEE 802.1p standard. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

TABLE 3-22 IEEE 802.1p Default Priority Recommendations

	Queue			
Priority	**0**	**1**	**2**	**3**
0		•		
1	•			
2	•			
3		•		
4			•	
5			•	
6				•
7				•

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

TABLE 3-23 IEEE 802.1p Traffic Types

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

When mapping COS queues to port egress queues through the web interface or CLI, the following parameters can be configured:

- Class of Service Values – The COS value. Specify a value between 0 and 7, where 7 is the highest priority.
- Traffic Classes (Queue)[13] – The output queue buffer. Specify 0, 1, 2, or 3.

Web Interface: Mapping COS Values to Traffic Classes

1. **Open Switch Config ⇒ Class of Service ⇒ Basic Traffic Prioritisation.**
2. **Scroll to Mapping CoS Values to Traffic Classes (Egress Queues).**
3. **Select a priority from the Class of Service Values list.**
4. **Select an output queue from the Traffic Classes menu.**
5. **Click Save.**

13.CLI shows Queue ID.

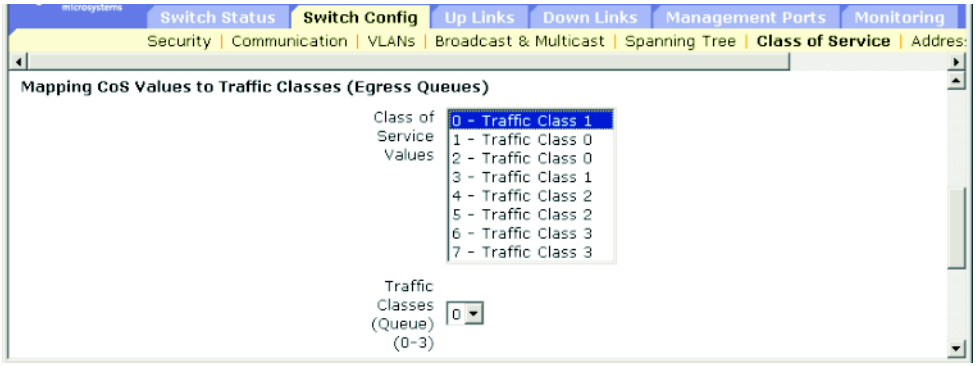


FIGURE 3-26 The Switch Config ⇒ Class of Service Window for Mapping COS Values to Traffic Classes

Command-line Interface: Mapping COS Values to Traffic Classes

The following example shows how to map COS values 0, 1 and 2 to COS priority queue 0, value 3 to COS priority queue 1, values 4 and 5 to COS priority queue 2, and values 6 and 7 to COS priority queue 3:

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

MIB Variables Associated With Mapping COS Values to Traffic Queues

TABLE 3-24 MIB Variables Associated With Mapping COS Values to Traffic Queues

Field Name	MIB Variable	Access	Value Range	Default Value

Traffic Class Priority	`MIB-II.`
	`dot1dBridge.`
	`pBridgeMIB.`
	`pBridgeMIBObjects.`
	`dot1dPriority.`
	`dot1dTrafficClassTable.`
	`dot1dTrafficClassEntry.`
	`dot1dTrafficClassPriority`
		Not-accessible	Integer (0-7)	

Traffic Class	`MIB-II.`
	`dot1dBridge.`
	`pBridgeMIB.`
	`pBridgeMIBObjects.`
	`dot1dPriority.`
	`dot1dTrafficClassTable.`
	`dot1dTrafficClassEntry.`
	`dot1dTrafficClass`
		Read/write	Integer (0-7)	page 3-80

3.3.5.3 Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in "Mapping COS Values to Egress Queues" on page 3-80, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service and subsequently affects the response time for software applications assigned a specific priority value.

When setting the weight for traffic classes through the web interface or CLI, the following parameters can be configured:

- Traffic Class (Queue)[14] – A list of weights for each traffic class.
- WRR Weights – The weight (between 1 and 255) for the selected traffic class.

Web Interace: Setting the Service Weight for Traffic Classes

1. **Open Switch Config ⇒ Class of Service ⇒ Basic Traffic Prioritisation.**
2. **Scroll to Setting the Service Weights for Traffic Classes (Egress Queues).**
3. **Select a traffic class (output queue).**
4. **Type a value in the WRR Weights text field.**
5. **Click Save.**

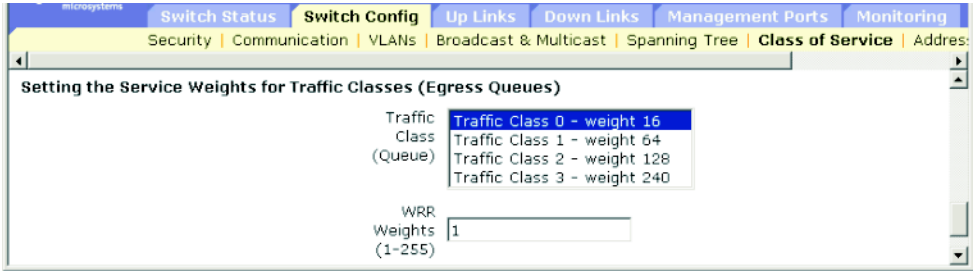


FIGURE 3-27 The Switch Config ⇒ Class of Service Window for Setting Service Weights for Traffic Queues

14.CLI shows Queue ID.

Command-line Interface: Setting the Service Weight for Traffic Classes

The following example shows how to assign WRR weights of 1, 4, 16, and 64 to the COS priority queues 0, 1, 2 and 3.

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

MIB Variables: Setting the Service Weight for Traffic Classes

TABLE 3-25 Setting the Service Weight for Traffic Classes

Field Name	MIB Variable	Access	Value Range	Default Value
WRR Traffic Class (Queue ID)	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrTrafficClass	Index	Integer (0-7)	
WRR Weight	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrWeight	Read/write	Integer (1-255)	For queue 0: 16 For queue 1: 64 For queue 2: 128 For queue 3: 240

3.3.5.4 Mapping Layer 3/4 Priorities to COS Values

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types automatically disables the other.

When mapping layer 3/4 priorities to COS values through the web interface or CLI, the following parameters can be configured:

- Enable Priority Services – The current operating status for mapping for layer 3/4 priorities to COS values. The default is disabled.
- IP Precedence – IP Precedence mapping.
- Differentiated Services Code Point Mapping (DSCP) – DSCP mapping.

Web Interface: Enabling Priority Services

1. **Open Switch Config ⇒ Class of Service ⇒ Layer 3/4 Traffic Prioritisation.**
2. **Select Enable Priority Services,**
3. **Select IP Precedence or DSCP.**
4. **Click Save.**

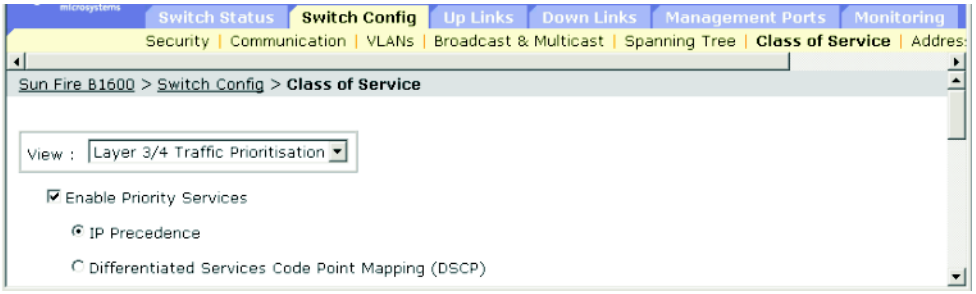


FIGURE 3-28 The Switch Config ⇒ Class of Service Window for Enabling Priority Services

Command-line Interface: Enabling Priority Services

The following example enables IP Precedence service on the switch:

```
Console(config)#map ip precedence
Console(config)#
```

To disable layer 3/4 traffic prioritization completely, use the following commands:

```
Console(config)#no map ip precedence
Console(config)#no map ip dscp
```

MIB Variables Associated With Traffic Prioritisation

TABLE 3-26 MIB Variables Associated With Traffic Prioritization

Field Name	MIB Variable	Access	Value Range	Default Value
IP Precedence/ DSCP Status	`sun... priorityMgt. prioIpPrecDscpStatus`	Read/write	disabled (1), precedence (2), dscp (3)	disabled

3.3.5.5 Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (Precedence value 0 maps to COS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table:

TABLE 3-27 ToS Octet Traffic Types

Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

When mapping IP Precedence values to COS values through the web interface or CLI, the following parameters can be configured:

- IP Precedence – The current IP Precedence to COS map.

- Class of Service Value – The COS value that is mapped to the selected IP Precedence value. Note that “0” represents low priority and “7” represents high priority.

Web Interface: Mapping IP Precedence

1. **Open Switch Config ⇒ Class of Service ⇒ Layer 3/4 Traffic Prioritisation.**
2. **Scroll to Mapping IP Precedence to Class of Service Values.**
3. **Select an entry from the IP Precedence table.**
4. **Select a value from the Class of Service Value menu.**
5. **Click Save.**

FIGURE 3-29 The Switch Config ⇒ Class of Service Window for Mapping IP Precedence

Command-line Interface: Mapping IP Precedence

The following example maps IP Precedence value 1 to COS value 0 on port SNP5[15], and then displays all the IP Precedence settings for that port.

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#end
Console#show map ip precedence ethernet SNP5
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#
```

MIB Variables Associated With Mapping IP Precedence

TABLE 3-28 MIB Variables Associated With Mapping IP Precedence

Field Name	MIB Variable	Access	Value Range	Default Value
IP Precedence Value	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecValue	Not-accessible	Integer (0-7)	
IP Precedence CoS	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecCos	Read/write	Integer (0-7)	one-to-one mapping

15.Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

3.3.5.6 Mapping DSCP Priority

The DSCP is six bits wide, enabling coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified in the following table are mapped to COS value 0.

TABLE 3-29 Default DSCP to COS Mapping

IP DSCP Value	COS Value
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

When mapping DSCP values to COS values through the web interface or CLI, the following parameters can be configured:

- DSCP – The current DSCP Priority to COS map.
- Class of Service Value – The COS value that is mapped to the selected DSCP Priority value. Note that "0" represents low priority and "7" represents high priority.

Web Interface: Mapping DSCP Priority

1. **Open Switch Config ⇒ Class of Service ⇒ Layer 3/4 Traffic Prioritisation.**
2. **Scroll to Mapping DSCP to Class of Service Values.**
3. **Select an entry from the DSCP table.**
4. **Select a value from the Class of Service Value menu.**
5. **Click Save.**

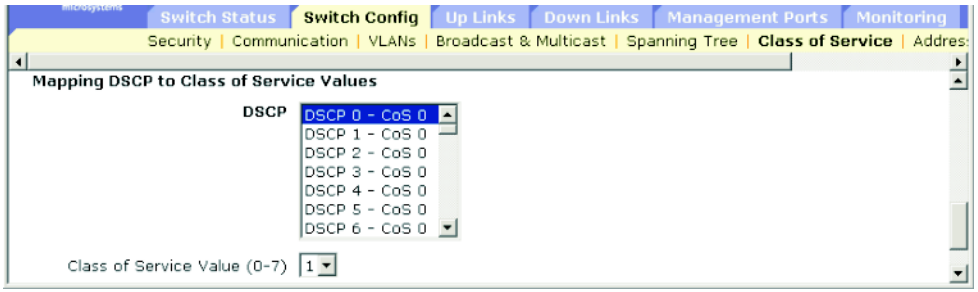


FIGURE 3-30 The Switch Config ⇒ Class of Service Window for Mapping DSCP to COS Values

Command-line Interface: Mapping DSCP Priority

The following example maps DSCP value 0 to COS value 1 on port SNP5[16], and then displays all the DSCP Priority settings for that port.

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip dscp 0 cos 1
Console(config-if)#end
Console#show map ip dscp ethernet SNP5
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#
```

16.Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

MIB Variables Associated With Mapping DSCP to CoS Values

TABLE 0-1 MIB Variables Associated With Mapping DSCP to COS Values

Field Name	MIB Variable	Access	Value Range	Default Value
IP DSCP Value	`sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpValue`	Not-accessible	Integer (0-63)	
IP DSCP CoS	`sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpCos`	Read/write	Integer (0-7)	page 3-90

3.3.6 Address Table Settings

Switches store the addresses for all known devices. This information is used to route traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

3.3.6.1 Displaying the Address Table

The Address Table contains the MAC addresses dynamically learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports. The Address Table also includes static MAC addresses that are tied to a specific port. (See "Configuring Static Addresses" on page 3-121.)

When viewing the Address Table through the web interface or CLI, the following parameters are displayed:

- Port ID (Interface[17]) – The port or aggregated link. Up-link ports NETP0 to NETP7 or down-link ports SNP0 to SNP15. You cannot display the MAC address table for NETMGT.
- VLAN ID – The VLAN identifier (between 1 and 4094). (This field includes the VLAN ID and name.)
- MAC Address – The MAC address associated with this interface.

17.CLI displays `Interface`.

- Address Type – Whether an address was learned or statically configured.

Web Interface: Viewing the Address Tables

1. **Open Switch Config ⇒ Address Tables.**
2. **Specify an interface, VLAN, MAC address, or address type (any combination) for the search criteria.**
3. **Click Query.**

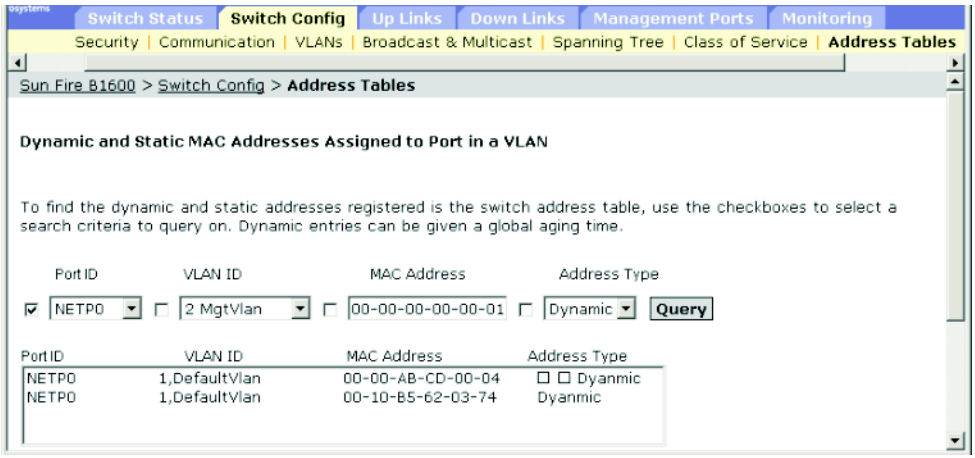


FIGURE 3-31 The Switch Config ⇒ Address Tables Window

Command-line Interface: Viewing the Address Tables

This example displays the address table entries for port NETP1.

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

MIB Variables Associated With the Address Tables

TABLE 3-30 MIB Variables Associated With the Address Tables

Field Name	MIB Variable	Access	Value Range

Interface	`MIB-II.`
	`dot1dBridge.dot1dTp.`
	`dot1dTpFdbTable.dot1dTpFdbEntry.`
	`dot1dTpFdbPort`
		Read only	not learned (0), Port list (1-24)

MAC Address	`MIB-II.`
	`dot1dBridge.dot1dTp.`
	`dot1dTpFdbTable.dot1dTpFdbEntry.`
	`dot1dTpFdbAddress`
		Read only	MAC address

VLAN	`MIB-II.`
	`dot1dBridge.qBridgeMIB.`
	`qBridgeMIBObjects.`
	`dot1qVlan.`
	`dot1qVlanStaticTable.`
	`dot1qVlanStaticEntry.`
	`dot1qVlanIndex`
		Not accessible	Integer

Type	`MIB-II.`
	`dot1dBridge.dot1dTp.`
	`dot1dTpFdbTable.dot1dTpFdbEntry.`
	`dot1dTpFdbStatus`
		Read only	other (1), invalid (2), learned (3), self (4), mgmt (5)

3.3.6.2 Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

When setting the address table aging time, the following parameter can be configured:

- Aging Time – The time (between 18 and 2184 seconds) after which a learned entry is discarded. The default is 300 seconds.

Web Interface: Changing the Aging Time

1. **Open Switch Config ⇒ Address Tables.**
2. **Type the new aging time in the text field.**
3. **Click Save.**

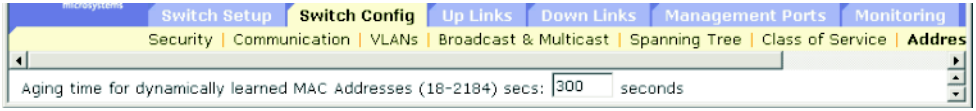


FIGURE 3-32 The Switch Config ⇒ Address Tables Window (showing aging time option)

Command-line Interface: Changing the Aging Time

This example sets the aging time to 400 seconds.

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

MIB Variables Associated With Aging Time

TABLE 3-31 MIB Variables Associated With Aging Time

Field Name	MIB Variable	Access	Value Range	Default Value
Aging Time	MIB-II dot1dBridge.dot1dTp. dot1dTpAgingTime	Read/write	Integer (18-2184) seconds	300 seconds

3.4 Port Configuration

This section includes configuration menus for the down-link ports, up-link ports, and management port. Most of these menus apply to all port types. However, the management port only supports a few basic menus, and Packet Filtering (page 3-134) is only provided for the management port.

Note – The port designations used in the following menus include NETP0 to NETP7 for up-link ports, SNP0 to SNP15 for down-link ports, and NETMGT for the management port.

3.4.1 Displaying Connection Status

You can use the port Status page to display the current connection status, including link state, speed/duplex mode, flow control, auto-negotiation, and broadcast storm control.

When viewing the status of port connections through the web interface or CLI, the following parameters are displayed:

- Port Type – The port type (1000BASE-SX, 1000BASE-T or 10/100BASE-TX).
- Port – The port or aggregated link. (Up-link ports NETP0 to NETP7, down-link ports SNP0 to SNP15, or the management port NETMGT.)
- Description – The interface label.
- Admin Status – The configured state of the interface:
  - Web - Either Enabled or Disabled.
  - CLI - (Port Admin) Either up or down.
- Link Status – The state of the connection. Either Up or Down.
- Port Operation Status[18] – The state of the connection. Either Up or Down. (Displayed only when the link is up.)
- Speed/Duplex – Shows the current speed and duplex mode.
- Flow Control – The configured state of flow control:
  - Web - Either IEEE 802.3x, Back-Pressure or None.
  - CLI - Either Enabled or Disabled. Flow Type shows IEEE 802.3x, Back-Pressure or None.

18.CLI only.

- Auto-negotiation – The configured state of auto-negotiation. Either enabled or disabled.
- Protect Status – The configured state of broadcast storm control on the interface. To set the threshold value, see "Broadcast Storm Control (Global Setting)" on page 3-67.
- MAC Address[19] – The physical layer address of the port.
- Port Capabilities[20] – The capabilities that are advertised for a port during auto-negotiation. The following capabilities are supported:
  - 10half – 10 Mbit/sec half-duplex operation
  - 10full – 10 Mbit/sec full-duplex operation
  - 100half – 100 Mbit/sec half-duplex operation
  - 100full – 100 Mbit/sec full-duplex operation
  - 1000full – 1000 Mbit/sec full-duplex operation
  - Sym – The transmitting and receiving of pause frames for flow control
  - FC – Flow control
- LACP Status[21] – The configured state of Link Aggregation Control Protocol (LACP) on the port.

Web Interface: Displaying Connection Status for the Ports

To display port status information and configure connections for one or more interfaces:

1. **Open Up Links / Down Links / Management Port ⇒ Status.**
2. **Select the check box next to the interface to configure.**
3. **Click Configure.**

   See "Configuring Interface Connections" on page 3-102.

19.CLI only. To display this parameter through the Web interface, see "Setting the IP Address" on page 3-12.

20.CLI only. To display this parameter through the Web interface, see "Configuring Interface Connections" on page 3-102.

21.CLI only.

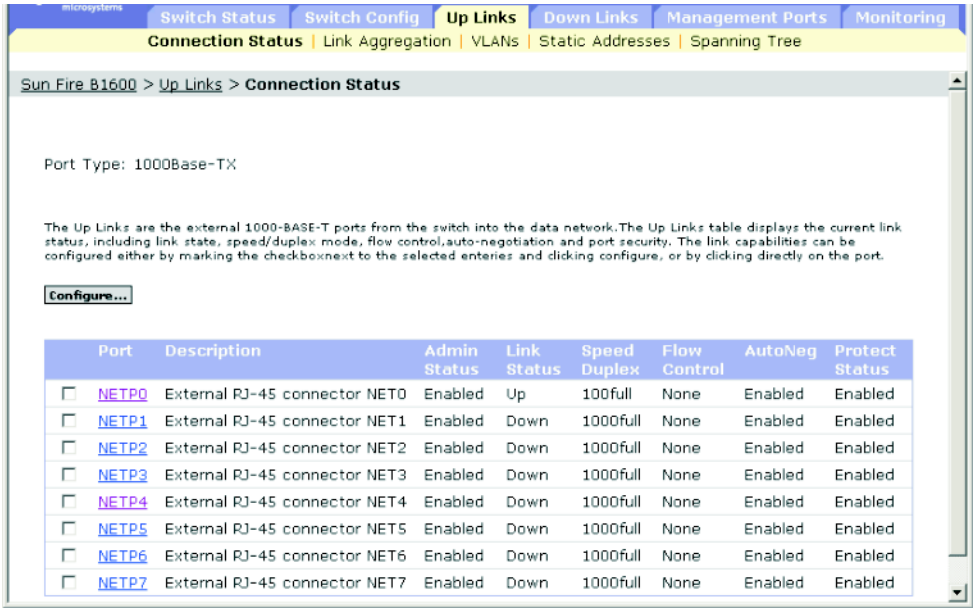


FIGURE 3-33 The Up Links ⇒ Connections Status Window

Command-line Interface: Displaying the Connection Status of a Port

This example shows the connection status for Port NETP7.

```
Console#show interfaces status ethernet NETP7
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#
```

MIB Variables Associated With the Connection Status of Ports

TABLE 3-32 MIB Variables Associated With the Connection Status of Ports

Field Name	MIB Variable	Access	Value Range	Default Value
Port Type	`sun... portMgt. portTable. portEntry. portType`	Read only	other(1), hundredBaseTX(2), hundredBaseFX(3), thousandBaseSX(4), thousandBaseLX(5), thousandBaseT(6), thousandBaseMiniGBIC(7) thousandBaseSFP(8)	
MAC Address	`MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress`	Read only	Physical address	
Port	`sun... portMgt. portTable. portEntry`	Index	Integer (1-25)	
Port Name	`sun... portMgt. portTable. portEntry. portName`	Read/ write	Display string (size (0-64))	
Administrative Status	`MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus`	Read/ write	up (1), down (2), testing (3)	up
Link Status	`MIB-II. interfaces. ifTable.ifEntry. ifOperStatus`	Read only	up (1), down (2-7),	
Operational Status	`MIB-II. interfaces. ifTable.ifEntry. ifOperStatus`	Read 0nly	up (1), down (2), testing (3), unknown (4), dormant (5), notPresent (6), lowerLayerDown (7)	

TABLE 3-32 MIB Variables Associated With the Connection Status of Ports *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
Port Speed Duplex Status	sun... portMgt. portTable.portEntry . portSpeedDpxStatus	Read only	error(1), halfDuplex10(2), fullDuplex10(3), halfDuplex100(4), fullDuplex100(5), halfDuplex1000(6), fullDuplex1000(7)	
Port Capabilities	sun... portMgt. portTable.portEntry . portCapabilities	Read/ write	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	Read only	error(1), backPressure(2), dot3xFlowControl(3), none(4)	none
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	Read/ write	enabled (1), disabled (2)	disabled
Port Auto-negotiation	sun... portMgt. portTable.portEntry . portAutonegotiation	Read/ write	enabled (1), disabled (2)	enabled
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	Read/ write	enabled (1), disabled (2)	enabled

3.4.2 Configuring Interface Connections

You can use the Port Setup page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

When configuring interface connections through the web interface or CLI, the following parameters are displayed or can be configured:

- Port/s – The port or aggregate link (up links NETP0 to NETP7, and down links SNP0 to SNP15).
- Port Description – The label (between 1 and 64 characters) of the interface. The default for up-link ports is External RJ-45 connector NETn. The default for down-link ports is Blade Slot n. The default for the management port is External RJ-45 connector NETMGT.
- Administrative Status – The configured state of the interface. You can disable an interface due to abnormal behavior (for example, excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- Negotiate Link Capabilities[22] – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported:
  - 10half – 10 Mbit/sec half-duplex operation
  - 10full – 10 Mbit/sec full-duplex operation
  - 100half – 100 Mbit/sec half-duplex operation
  - 100full – 100 Mbit/sec full-duplex operation
  - 1000half – 1000 Mbit/sec half-duplex operation
  - 1000full – 1000 Mbit/sec full-duplex operation
  - symmetric (Gigabit only) – The capability to transmit and receive pause frames. When disabled, the sender and receiver auto-negotiate for asymmetric pause frames. (The switch only supports symmetric pause frames.)
  - flowcontrol – Flow control

    Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.

22. Auto-negotiation cannot be disabled on the down-link ports. These ports are fixed at 1000 Mbit/sec, full duplex.

Note – The integrated switches on the Sun Fire B1600 blade system chassis are each composed of two switch chips linked together. It is only possible to enable flow control between two ports that are on the same switch chip. The ports NETP0, NETP1, NETP4, NETP5, and SNP8 through SNP15 are on one switch chip. The ports NETP2, NETP3, NETP6, NETP7, and SNP0 through SNP7 are on the other. (If you look at the rear panel of the SSC, all the ports on the right are on one chip, and all the ports on the left are on the other.)

- Speed/Duplex[23] – The port speed and duplex mode. When auto-negotiation is disabled, you can manually configure the port speed and duplex mode.

Note – When auto-negotiation is disabled, you can only set the up-link ports to 10 Mbit/sec or 100 Mbit/sec. To force a port to operate at 1 Gbit/sec full duplex, enable auto-negotiation, and set the port capabilities to "1000full" only.

- Flow Control[23] – When auto-negotiation is disabled, you need to enable or disable flow control. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment connected to the hub.)
- Broadcast storm suppression – The state of broadcast storm control on the interface. For more information on broadcast storm control or information on setting the broadcast threshold level, refer to "Broadcast Storm Control (Global Setting)" on page 3-67.

3.4.2.1 Web Interface: Configuring Interface Connections

1. **Open the Up Links / Down Links ⇒ Status window.**
2. **Se;ect the interfaces you want to configure.**
3. **Click Configure.**
4. **Modify the required interface settings.**
5. **Click Save.**

23. Auto-negotiation must be disabled on the up-link ports before you can configure or force the interface to use a specific speed, duplex mode, or flow control option.

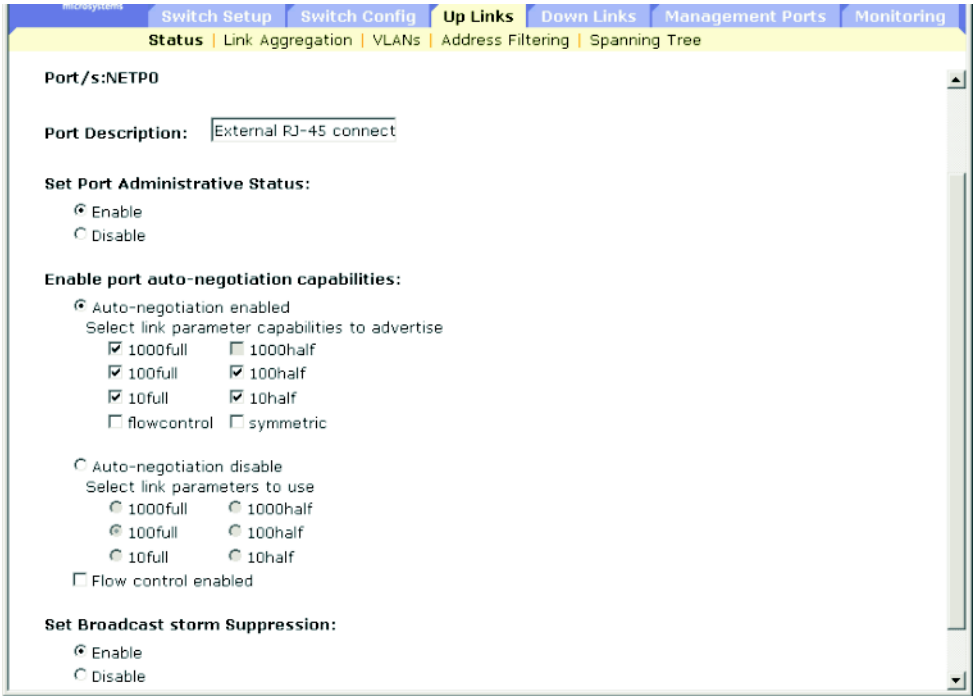


FIGURE 3-34 The Up Links ⇒ Status Window (showing attribues of NETP0)

3.4.2.2 Command-line Interface: Configuring Interface Connections

Select the interface, and then enter the required settings.

```
Console#Console(config)#interface ethernet NETP1
Console(config-if)#description RD SW#17
Console(config-if)#shutdown
.
.
.
Console(config-if)#no shutdown
Console(config-if)#negotiation
Console(config-if)#capabilities 1000full
Console(config-if)#capabilities 1000full
Console(config-if)#capabilities flowcontrol
.
.
.
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#flowcontrol
Console(config-if)#
```

3.4.2.3 MIB Variables Inspecting or Configuring Interface Connections

TABLE 3-33 MIB Variables for Interface Connections

Field Name	MIB Variable	Access	Value Range	Default Value
Port Name	sun... portMgt. portTable.portEntry. portName	Read/write	Display String ((Size (0-64))	page 3-102
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	Read/write	up (1), down (2), testing (3)	up
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	Read/write	enabled(1), disabled(2)	enabled

TABLE 3-33 MIB Variables for Interface Connections *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
Port Capabilities	`sun... portMgt. portTable.portEntry. portCapabilities`	Read/write	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`	Read/write	reserved(1), halfDuplex10(2), fullDuplex10(3), halfDuplex100(4), fullDuplex100(5), halfDuplex1000(6), fullDuplex1000(7)	
Port Flow Control Configuration	`sun... portMgt. portTable.portEntry. portFlowCtrlCfg`	Read/write	enabled(1), disabled(2), backPressure(3), dot3xFlowControl(4)	

3.4.3 Configuring Aggregated Links

You can create multiple links between devices that work as one virtual, aggregate link. An aggregated link offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to six aggregated links at a time.

The switch supports both static aggregated links and dynamic Link Aggregation Control Protocol (LACP). LACP configured ports will automatically negotiate a link with LACP-configured ports on another device. You can configure any number of the up-link ports on the switch as LACP, as long as they are not already configured as part of a static link. If ports on another device are also configured as LACP, the switch and the other device will negotiate an aggregated link between them. If an LACP link consists of more than four ports, all other ports will be placed in a standby mode. If one link in the aggregated link fails, one of the standby ports will automatically be activated to replace it.

Besides balancing the load across each port in the aggregated link, the additional ports provide redundancy by taking over the load if a port in the aggregated link fails. However, before making any physical connections between devices, use the web interface or CLI to specify the aggregated link on the devices at both ends.

When using aggregated links, take note of the following points:

- Finish configuring aggregated links before you connect the corresponding network cables between switches, to avoid creating a loop.
- You can create up to six aggregated links on the switch, with up to four ports per aggregated link.
- The ports at both ends of a connection must be configured as aggregated links (in some device interfaces, the word “trunk” might be used to refer to an aggregated link).
- The ports at both ends of an aggregated link must be configured in an identical manner, including communication mode (speed, duplex mode and flow control), VLAN assignments, and COS settings.
- If the target switch has also enabled LACP on the connected ports, the aggregated link will be activated automatically.
- An aggregated link formed with another switch using LACP will automatically be assigned the next available port-channel number.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All the ports in an aggregated link have to be treated as a whole when moved from or to, or when added to or deleted from, a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire aggregated link.

3.4.3.1 Dynamically Configuring an Aggregated Link with LACP

Web Interface: Dynamic Aggregated Links (LACP)

1. **Click Up Links/Down Links ⇒ Link Aggregation.**
2. **Locate the required port in the Link Aggregation table.**
3. **Click Enable LACP or Disable LACP.**

Note – The action buttons take immediate effect. To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.

FIGURE 3-35 The Uplink ⇒ Link Aggregation Window

Command-line Interface: Dynamic Aggregated Links (LACP)

The following example enables LACP for ports NETP0 and NETP1. These ports can be connected to two LACP-enabled ports on another switch to form an aggregated link.

```
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)#end
Console#show interfaces status port-channel 1
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#
```

MIB Variables Associated With Dynamic Aggregated Links

TABLE 3-34 MIB Variables Associated With Dynamic Aggregated Links

Field Name*	MIB Variable	Access	Value Range	Default Value
Trunk Maximum ID	`sun... trunkMgt. trunkMaxId`	Read only	Integer	6
Trunk Valid Number	`sun... trunkMgt. trunkValidNumber`	Read only	Integer (1-6)	
Trunk Index	`sun... trunkMgt. trunkTable.trunkEntry. trunkIndex`	Index	Integer	
Trunk Ports	`sun... trunkMgt. trunkTable.trunkEntry. trunkPorts`	Read/create	Octet string (port list)	
Trunk Creation	`sun... trunkMgt. trunkTable.trunkEntry. trunkCreation`	Read only	static (1), lacp (2)	
Trunk Status	`sun... trunkMgt. trunkTable.trunkEntry. trunkStatus`	Read/create	valid (1), invalid (2)	
LACP Port Status	`sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus`	Read/write	enabled (1) disabled (2)	

* For a description of other CLI variables, see "Displaying Connection Status" on page 3-96

3.4.3.2 Statically Configuring an Aggregated Link

Web Interface: Statically Configuring an Aggregated Link

1. **Click Up Links / Down Links ⇒ Link Aggregation.**
2. **Select a trunk from the Select Trunk menu.**
3. **Select the required port.**
4. **Click Add or Remove.**

Note – The action buttons take immediate effect. To avoid creating a loop in the network, be sure you add a static aggregated link using the configuration interface before connecting the ports, and also disconnect the ports before removing a static aggregated link using the configuration interface.

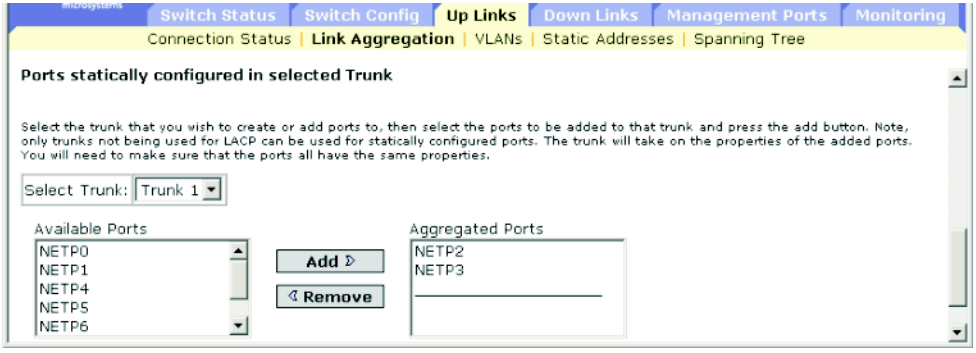


FIGURE 3-36 The Up Links ⇒ Link Aggregation Window

Command-line Interface: Statically Configuring an Aggregated Link

This example creates port-channel 2 using ports NETP2 and NETP3. These ports can be connected to two ports on another switch to form an aggregated link.

```
Console(config)#interface port-channel 2
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#channel-group 2
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
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#
```

MIB Variables Associated With Static Aggregated Links

TABLE 3-35 MIB Variables Associated With Static Aggregated Links

Field Name*	MIB Variable	Access	Value Range	Default Value
Trunk Maximum ID	`sun... trunkMgt.trunkMaxId`	Read only	Integer	6
Trunk Valid Number	`sun... trunkMgt. trunkValidNumber`	Read only	Integer (1-6)	
Trunk Index	`sun... trunkMgt.trunkTable. trunkEntry.trunkIndex`	Index	Integer	
Trunk Ports	`sun... trunkMgt.trunkTable. trunkEntry.trunkPorts`	Read/create	Octet string (port list)	
Trunk Creation	`sun... trunkMgt. trunkTable.trunkEntry. trunkCreation`	Read only	static (1), lacp (2)	
Trunk Status	`sun... trunkMgt.trunkTable. trunkEntry.trunkStatus`	Read/create	valid (1), invalid (2)	

* For a description of other CLI variables, see "Displaying Connection Status" on page 3-96

3.4.4 Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including default VLAN identifier (PVID), accepted frame types, ingress filtering, GARP VLAN Registration Protocol (GVRP) status, and Group Address Registration Protocol (GARP) timers.

Note the following points about GVRP and GARP:

- GVRP – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- GARP – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

When configuring VLAN behavior for interfaces through the web interface or CLI, the following parameters are displayed or can be configured:

- Port – The port or trunk (up links NETP0 to NETP7, down links SNP0 to SNP15, or the management port NETMGT).
- Default VLAN for Port (PVID) – The VLAN ID assigned to untagged frames received on an interface. The default for up/down links is 1 and for NETMGT it is 2.

Note – If an interface is not a member of VLAN 1 and you assign its PVID to VLAN 1, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- Acceptable Frame Types – The interface can accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. Specify all or tagged. The default is all.
- Switch Port Mode – The VLAN membership mode for a port. The default is Trunk.
  - Trunk – The port is an end point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN.
  - Hybrid – A hybrid VLAN interface. The port can transmit tagged or untagged frames.
- Ingress Filtering – If ingress filtering is enabled, incoming frames for VLANs that do not include this ingress port in their member set are discarded at the ingress port. The default is disabled.

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled, the interface accepts any VLAN-tagged frame if the tag matches a VLAN known on the switch (except for those VLANs explicitly forbidden on the port).
- If ingress filtering is enabled, the interface discards incoming frames tagged for VLANs that do not include the ingress port in their member set.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- GVRP – The configured state of GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (page 3-45.) When disabled, any GVRP packets received on this port are discarded and no GVRP registrations are propagated from other ports. The default is disabled.
- GARP Join Timer – The interval (between 20 and 1000 centiseconds) between transmitting requests/queries to participate in a VLAN group. The default is 20 centiseconds.
- GARP Leave Timer – The interval (between 60 and 3000 centiseconds) a port waits before leaving a VLAN group. Set this time to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. The default is 60 centiseconds.
- GARP LeaveAll Timer – The interval (between 500 and 18,000 centiseconds) between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. The default is 1000 centiseconds.
- VLANs on Selected Port – The port is statically assigned to the specified VLAN.
- Membership Type – The port's static VLAN membership type.
  - Tagged: The interface is a member of the VLAN. All packets transmitted by the port on this VLAN are tagged, that is, carry a tag and therefore carry VLAN or COS information.
  - Untagged: The interface is a member of the VLAN. All packets transmitted by the port on this VLAN are untagged, that is, do not carry a tag and therefore do not carry VLAN or COS information.
  - Forbidden: The interface is forbidden from automatically joining the VLAN through GVRP. See "Automatic VLAN Registration" on page 3-40.
  - Remove: The selected interface is removed from the VLAN.

3.4.4.1 Web Interface: Configuring VLAN Behavior for Interfaces

1. **Open Up Links / Down Links / Management Port ⇒ VLANs.**

2. **Modify the required settings for each interface.**

3. **Click Save.**

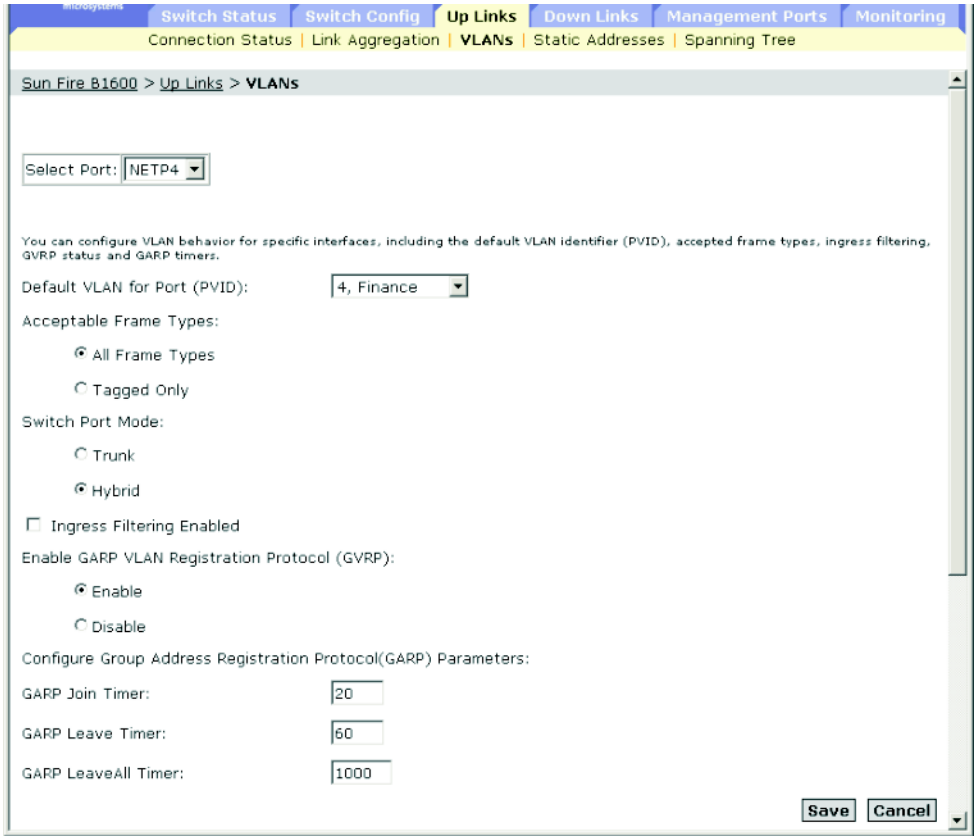


FIGURE 3-37 The Up Links ⇒ VLANs Window

Scroll down to the VLAN membership table, and configure the VLANs required for the selected interface.

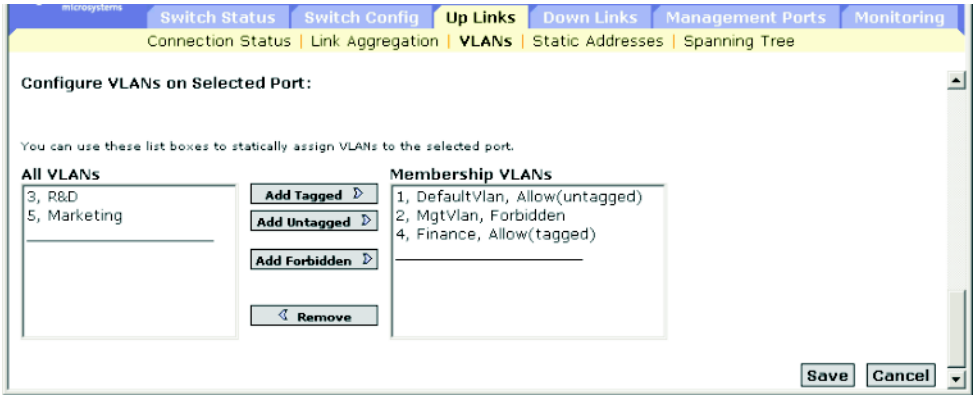


FIGURE 3-38 The Up Links ⇒ VLANs Window (cont'd)

3.4.4.2 Command-line Interface: Configuring VLAN Behavior for Interfaces

This example sets port NETP4 to accept only tagged frames, assigns PVID 4 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to `hybrid`.

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

3.4.4.3 MIB Variables Associated With VLAN Behavior of Interfaces

TABLE 3-36 MIB Variables Associated With VLAN Behavior of Interfaces

Field Name	MIB Variable	Access	Value Range	Default Value

Port PVID	`MIB-II.`
	`dot1dBridge.`
	`qBridgeMIB.`
	`qBridgeMIBObjects.`
	`dot1qVlan.`
	`dot1qPortVlanTable`
	`.`
	`dot1qPortVlanEntry`
	`.`
	`dot1qPvid`
		Read/write	Integer (1-4094)	1

Port Acceptable Frame Type	`MIB-II.`
	`dot1dBridge.`
	`qBridgeMIB.`
	`qBridgeMIBObjects.`
	`dot1qVlan.`
	`dot1qPortVlanTable`
	`.`
	`dot1qPortVlanEntry`
	`.`
	`dot1qPortAcceptabl`
	`e-FrameTypes`
		Read/write	admitAll (1),
			admitOnlyVlan
			-Tagged (2)
				admitAll

Port Mode	`sun...`
	`vlanMgt.`
	`vlanPortTable.`
	`vlanPortEntry.`
	`vlanPortMode`
		Read/write	hybrid (1),
			dot1qTrunk (2)
				hybrid

Port Ingress Filtering	`MIB-II.`
	`dot1dBridge.`
	`qBridgeMIB.`
	`qBridgeMIBObjects.`
	`dot1qVlan.`
	`dot1qPortVlanTable`
	`.`
	`dot1qPortVlanEntry`
	`.`
	`dot1qPortIngressFi`
	`ltering`
		Read/write	true (1),
			false (2)
				false

TABLE 3-36 MIB Variables Associated With VLAN Behavior of Interfaces *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
Port GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable . dot1qPortVlanEntry . dot1qPortGVRPStatus	Read/write	enabled (1), disabled (2)	disabled
GARP Join Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable . dot1dPortGarpEntry . dot1dPortGarpJoinTime	Read/write	Integer (20-1000) centiseconds	20 centiseconds
GARP Leave Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable . dot1dPortGarpEntry . dot1dPortGarpLeaveTime	Read/write	Integer (60-3000) centiseconds	60 centiseconds
GARP Leave All Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable . dot1dPortGarpEntry . dot1dPortGarp-LeaveAllTime	Read/write	Integer (500-18000) centiseconds	1000 centiseconds

TABLE 3-36 MIB Variables Associated With VLAN Behavior of Interfaces *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN Static Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	Read/ create	Octet string (size (0-32))	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticRowStatus	Read/ create	enable (1), disable (2)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic-UntaggedPorts	Read/ create	Octet string (port list)	
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden-EgressPorts	Read/ create	Octet string (port list)	

3.4.5 Configuring Static Addresses

You can use address filtering to set static addresses that are bound to a specific port and VLAN, or to enable port security that restricts all inbound traffic to the entries currently listed in the address table (including either dynamic or static addresses).

Note the following points about static addresses and port security:

- Setting Static Addresses – A static address can be assigned to a specific interface on the switch. When a static address that is currently bound to an interface, is seen on another interface, the new interface that sees it does not accept or transmit data from or for that address and does not include the address in its address table.
- Configuring Port Security – If you enable port security, the switch stops dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic address table are accepted. To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on an interface for an initial training period, and then enable port security to stop address learning. Enable the learning function long enough to ensure that all valid VLAN members are registered on the selected interface.

  To add new VLAN members at a later time, you can manually add static addresses, or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

When configuring static addresses and port security through the web interface or CLI, the following parameters are displayed or can be configured:

- Port – The interface (port or trunk). Up-link ports NETP0 to NETP7 or down-link ports SNP0 to SNP15.
- Secure Port – The configured state of port security. The default is disabled.

  A secure port has the following restrictions:

  - It cannot use port monitoring.
  - It cannot be a multi-VLAN interface.
  - It cannot be connected to a network interconnection device.
  - It cannot be a member of an aggregated link.
- Number of Static Addresses[24] – The number of manually configured addresses.
- VLAN – The ID of the configured VLAN (1-4094) and its name.
- MAC Address – The MAC address associated with the interface.

24.Web only.

- Duration – The address can be set to the following type:
  - Permanent – The assignment is permanent, and restored after the switch is reset.
  - Delete on Reset – The assignment lasts until the switch is reset.

3.4.5.1 Web Interface: Configuring Static Addresses

1. **Open Up Links / Down Links ⇒ Address Filtering.**
2. **Select the interface.**
3. **Select Secure Port to enable port security.**
4. **Select VLAN, MAC address, and duration.**
5. **Click Add.**

FIGURE 3-39 The Up Links ⇒ Static Addresses Window

3.4.5.2 Command-line Interface: Configuring Static Addresses

This example adds the same items to the static address table:

```
Console(config)#interface ethernet NETP4
Console(config-if)#port security
Console(config-if)exit
Console(config)#mac-address-table static 00-80-c8-00-00-01
  interface ethernet NETP4 vlan 1 permanent
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
 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#
```

3.4.5.3 MIB Variables Associated With Static Addresses

TABLE 3-37 MIB Variables Associated With Static Addresses

Field Name	MIB Variable	Access	Value Range	Default Value
Static Receive Port	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticReceivePort	Read/write	Integer	
Port Security Status	sun... securityMgt. portSecurityMgt portSecPortTable. portSecPortEntry. portSecPortStatus	Read/write	enabled (1), disabled (2)	disabled
Number of Static Addresses	*Not Defined*			

TABLE 3-37 MIB Variables Associated With Static Addresses *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
VLAN Index	`MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects . dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex`	Index	Integer	
Static Address	`MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticAddress`	Read/write	MAC address	
Static Status	`MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticStatus`	Read/write	other(1), invalid(2), permanent(3), deleteOnReset(4), deleteOnTimeout (5)	permanent

3.4.6 Managing Interfaces for Spanning Tree Algorithm

You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You can use a different priority or path cost for ports of same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the connected device can support fast forwarding.

3.4.6.1 Displaying the Current Interface Settings for STA

When viewing STA interface settings through the web interface or CLI, the following parameters are displayed:

- Port – The interface (ports only, no aggregated links or members of aggregated links). Up-link ports NETP0 to NETP7 or down-link ports SNP0 to SNP15.
- STA Status – The current state of the port within the Spanning Tree:
  - Discarding – The port receives STA configuration messages, but does not forward packets.
  - Learning – The port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. The port address table is cleared and the port begins learning addresses.
  - Forwarding – The port forwards packets and continues learning addresses.
- Priority – The priority used for the port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (lowest value) is configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier is enabled.
- Path Cost – This parameter is used by the STA to determine the best path between devices. Therefore, assign lower values to ports attached to faster media and higher values to ports with slower media. (Path cost takes precedence over port priority.)
- Designated Cost – The cost for a packet to travel from the port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- Designated Bridge – The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- Designated Port – The priority and number of the port on the designated bridging device through which the switch must communicate with the root of the Spanning Tree.

- Link Type (Admin Link type[25]) – The link type connected to the interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is connected to a point-to-point link or to shared media.
- Edge Port (Admin Edge Port[25]) – You can enable this option if an interface is connected to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, enable Edge Port only for ports connected to an end-node device.

These additional parameters are only displayed for the CLI:

- Admin status – Shows if STA has been enabled on this interface.
- Role – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (root port), connecting a LAN through the bridge to the root bridge (designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (disabled port) if a port has no role within the spanning tree.
- Designated root – The priority and MAC address of the device in the Spanning Tree that the switch has accepted as the root device.
- Forward transitions – The number of times the port has transitioned from the Learning state to the Forwarding state.
- Oper edge port – This parameter is initialized to the setting for Admin Edge Port (that is, true or false), but will be set to false if a BPDU is received.
- Oper Link type – The operational point-to-point status of the LAN segment connected to the interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type.

Web Interface: Displaying the Current Interface Settings for STA

- **Open Up Links / Down Links => Spanning Tree => Spanning Tree Protocol.**

25.The CLI displays this term.

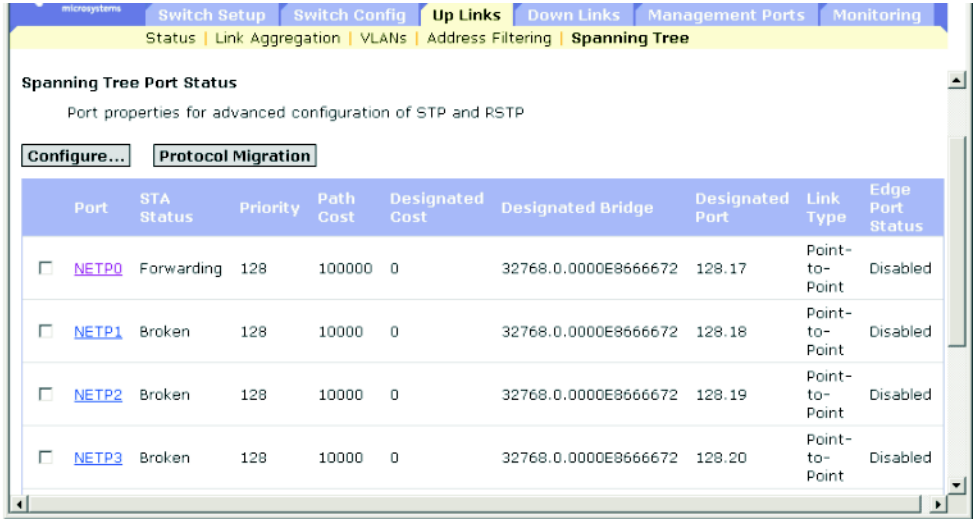


FIGURE 3-40 The Up Links ⇒ Spanning Tree Window

Command-line Interface: Displaying the Current Interface Settings for STA

This example shows the STA attributes for port NETP4:

```
Console#show spanning-tree ethernet NETP4
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#
```

MIB Variables Associated With a Port's STA Settings

TABLE 3-38 MIB Variables Associated With a Port's STA Settings

Field Name	MIB Variable	Access	Value Range	Default Value
Port	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry`	Index	Interger (1-25)	
STA Port State	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortState`	Read only	discarding (1), learning (2), forwarding (3)	
STA Port Priority	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority`	Read/write	Integer (0-240)	128
STA Port Path Cost	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost`	Read/write	Integer (long: 1-200,000,000; short: 1-65,535)	page 3-129
STA Port Designated Cost	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedCost`	Read only	Integer	
STA Port Designated Bridge	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedBridge`	Read only	Octet string	
STA Port Designated Port	`sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedPort`	Read only	Octet string	
STA Port Admin Point to Point	`sun...staMgt. staPortTable. staPortEntry. staPortAdminPointTo- Point`	Read/write	forceTrue(0) forceFalse (1) auto (2),	auto
STA Port Admin Edge Port	`sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort`	Read/write	true (1), false (2)	false

TABLE 3-38 MIB Variables Associated With a Port's STA Settings *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
STA Port Enable (Admin status)	`sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortEnable`	Read/write	enabled (1), disabled (2)	enabled
STA Port Role	`sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPortRole`	Read only	disabled (1), root (2), designated (3), alternate (4), backup (5)	
STA Port Designated Root	`sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-DesignatedRoot`	Read only	Octet string	
STA Port Forward Transitions	`sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort-ForwardTransitions`	Read only	Counter	

3.4.6.2 Configuring Interface Settings for STA

These settings apply to the selected interface(s) when the switch is set to STP forced compatibility mode (page 3-70) and RSTP.

When configuring STA interface settings through the web interface or CLI, the following parameters can be configured:

- Priority – The priority (between 0 and 240 in steps of 16) used for the port in the Spanning Tree Algorithm (STA). If the path cost for all ports on a switch is the same, the port with the highest priority (lowest value) is configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the STA is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier is enabled. The default is 128.
- Path Cost – This parameter is used by the STA to determine the best path between devices. Therefore, assign lower values to ports connected to faster media and higher values to ports connected to slower media. (Path cost takes precedence over port priority.)
  - The range of values for Ethernet connections is between 200,000 and 20,000,000, for Fast Ethernet 20,000 to 2,000,000, and Gigabit Ethernet 2000 to 200,000.

- The default values for Ethernet connections are 2,000,000 (half duplex), 1,000,000 (full duplex), and 500,000 (aggregated link). The default values for Fast Ethernet connections are 200,000 (half duplex), 100,000 (full duplex), and 50,000 (aggregated link). The default values for Gigabit Ethernet connections are 10,000 (full duplex) and 5000 (aggregated link).

Note – When the Path Cost Method is set to short (page 3-76), the maximum path cost is 65,535.

- Admin Link Type – The link type attached to the interface. The default is Auto.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is connected to a point-to-point link or to shared media.
- Admin Edge Port – You can enable this option if an interface is connected to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, enable Edge Port only for ports connected to an end-node device. The default for NETP0 to NETP7 is disabled. The default for SNP0 to SNP15 is enabled and fixed at this setting.

Web Interface: Configuring STA Settings for a Port

To configure interface settings for STP (IEEE 802.1D):

1. **Open Up Links / Down Links ⇒ Spanning Tree ⇒ Spanning Tree Protocol.**
2. **Select the required interfaces.**
3. **Click Configure.**
4. **Modify the required attributes.**
5. **Click Save.**

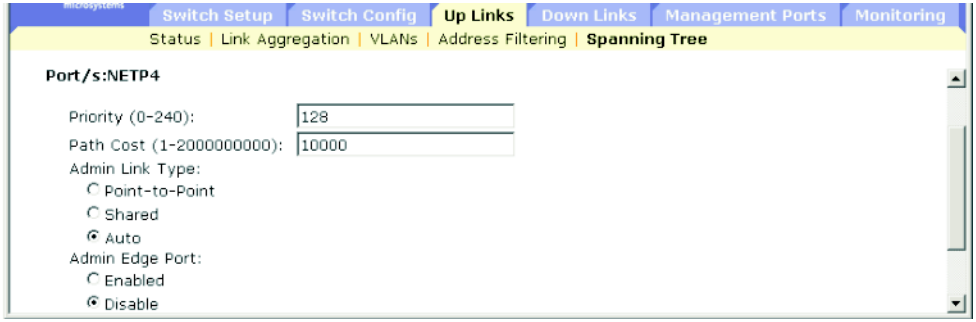


FIGURE 3-41 The Up Links ⇒ Spanning Tree Window for NETP4

Command-line Interface: Configuring STA Settings for a Port

This example sets STP attributes for port NETP5.

```
Console(config)#interface ethernet NETP5
Console(config-if)#spanning-tree port-priority 128
Console(config-if)#spanning-tree cost 19
Console(config-if)#spanning-tree link-type auto
Console(config-if)#no spanning-tree edge-port
```

MIB Variables for Configuring a Port's STA Settings

TABLE 3-39 MIB Variables for Configuring a Port's STA Settings

Field Name	MIB Variable	Access	Value Range	Default Value
STA Port Priority	`sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority`	Read/write	Integer (0-240)	128
STA Port Path Cost	`sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost`	Read/write	Integer (long: 1-200,000,000; short: 1-65,535)	page 3-129
STA Port Admin Link Type	`sun...staMgt. staPortTable. staPortEntry. staPortAdmin-PointToPoint`	Read/write	forceTrue (0), forceFalse (1), auto (2)	auto
STA Port Admin Edge Port	`sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort`	Read/write	true (1), false (2)	false

3.4.6.3 Checking the STA Protocol Status for Interfaces

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it automatically sets the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces.

Web Interface: Checking the STA Protocol Status for Interfaces

1. **Open Up Links / Down Links ⇒ Spanning Tree ⇒ Spanning Tree Protocol.**
2. **Select the required interfaces.**
3. **Click Protocol Migration.**

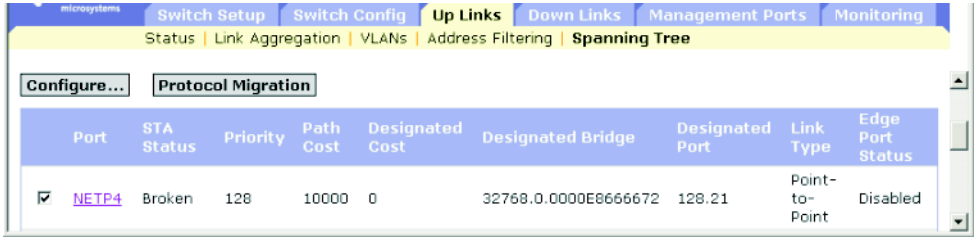


FIGURE 3-42 The Up Links ⇒ Spanning Tree Window (showing STA status)

Command-line Interface: Checking the STA Protocol Status for an Interface

This example uses the protocol migration command to verify the spanning tree message type (RSTP or STP-compatible) to send on this interface.

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

MIB Variables Associated With a Port's STA Status

TABLE 3-40 MIB Variables Associated With a Port's STA Status

Field Name	MIB Variable	Access	Value Range	Default Value
STA Port Protocol Migration	sun...staMgt. staPortTable. staPortEntry. staPortProtocolMigration	Read/write	true (1), false (2)	true

3.4.7 Filtering Traffic From the Down Link Ports to the Management Port

You can configure the packet filtering to prevent specified IP traffic from reaching the internal management port (NETMGT) from the down-link ports.

Note – Traffic is not allowed between up-link ports and the management port.

The system default is to stop all IP packets from passing from the down-link ports to the management port (NETMGT). If you need the blades to access the management network through the management port (NETMGT), you must set a filter to permit specific frames to pass from the down-link ports to the management port.

When configuring filtering for the management port through the web interface or CLI, the following parameters can be configured:

- Rule – The rule number (between 1 and 128). A filter rule can be inserted at the specified position in the table, pushing any existing patterns at or below that location down in the table. A rule number cannot exceed the next available number in the table. If the rule number is not specified, a new pattern is appended to the end of the rule table.
- Action – The control that blocks or allows packets passing from the down-link ports into the management port. Select permit or deny.
- Protocol – The protocol (either TCP, UDP, or Any), or protocol number (between 0 and 255).
- Keyword Flags (Code Sequence) – A flag in byte 14 of the TCP header. You can specify a sequence of codes (ON if selected and OFF if not selected). The symbolic name and corresponding bit include these items:
  - fin (1) – Finish
  - syn (2) – Synchronize
  - rst (4) – Reset
  - psh (8) – Push
  - ack (16) – Acknowledgement
  - urg (32) – Urgent pointer
- Code – The decimal number (between 0 and 63) representing a bit string that specifies flag bits in byte 14 of the TCP header.
- Bitmask – The decimal number representing a bit mask that is applied to the code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. Specify 32 (urg), 16 (ack), 8 (psh), 4 (rst), 2 (syn), or 1 (fin).

- Source – The frame's TCP/UDP source address, netmask, and port range (between 0 and 65,535).
- Destination – The frame's TCP/UDP destination address, netmask, and port range (between 0 and 65,535).
- Fragment – The rule will only match packets with the More Fragments (MF) bit set or with a fragment offset greater than zero. If fragment is not set, the rule will match both fragments and non-fragmented packets.
- Log – Logs any matching packets in the log buffer. The maximum number of entries stored in the log buffer is 64. When the buffer fills, it will wrap around and overwrite the oldest entries. Note that the log is stored in RAM and is lost when the switch is reset.

3.4.7.1 Web Interface: Filtering Traffic to the Management Port

1. **Open Management Port ⇒ Packet Filtering.**
2. **Specify the required rules.**
3. **Click Add.**

The rule in the following example permits TCP traffic from source address 10.7.1.1 to destination address 10.8.1.1, using TCP ports 10 to 30.

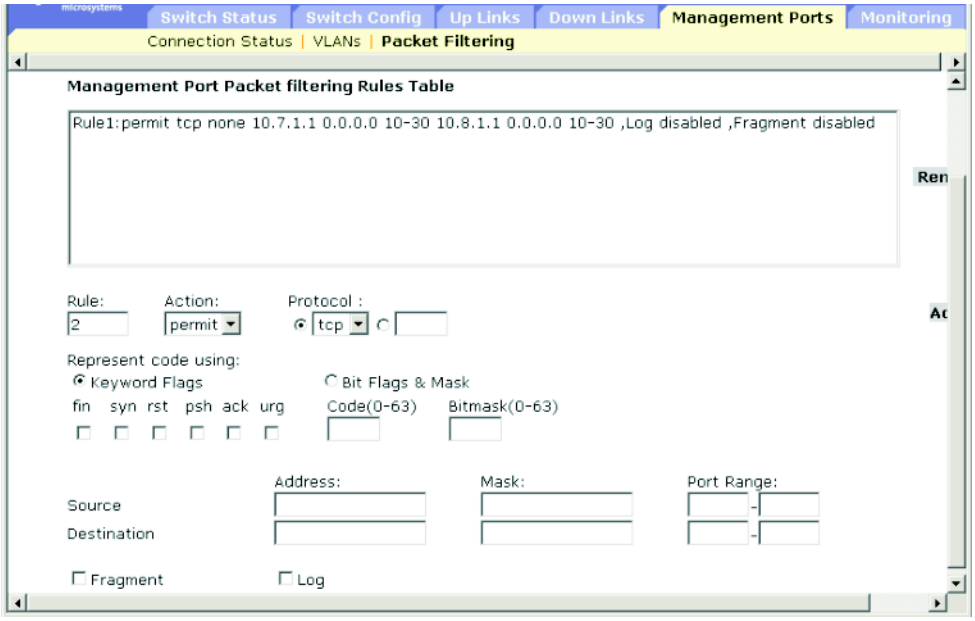


FIGURE 3-43 The Management Ports ⇒ Packet Filtering Window

3.4.7.2 Command-line Interface: Filtering Traffic to the Management Port

The following example allows all packets to pass through the filter by permitting any protocol type, and using a null address and network mask for both the source address and destination address. For a full list of examples, refer to Section 4.3.7.8, "ip filter" on page 4-77.

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

3.4.7.3 MIB Variables Associated With Filtering Traffic to the Management Port

TABLE 3-41 MIB Variables Associated With Filtering Traffic to the Management Port

Field Name	MIB Variable	Access	Value Range	Default Value
Index	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleIndex	No access	Integer (1-128)	
Action	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleAction	Read/create	permit (1), deny (2)	
Protocol	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleProtocol	Read/create	Integer (0-256; 256 means any protocol)	
Source IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcIpAddr & pfuRuleSrcIpBitmask	Read/create	IP address	
Source IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcPortRange1 & pfuRuleSrcPortRange2	Read/create	Integer (1-65536)	
Destination IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstIpAddr & pfuRuleDstIpBitmask	Read/create	IP address	

TABLE 3-41 MIB Variables Associated With Filtering Traffic to the Management Port *(Continued)*

Field Name	MIB Variable	Access	Value Range	Default Value
Destination IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstPortRange1 & pfuRuleDstPortRange2	Read/create	Integer (1-65536)	
TCP Code	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCode	Read/create	Integer (0-63)	
TCP Code Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCodeBitmask	Read/create	Integer (0-63)	
Fragments	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleFragments	Read/create	enabled (1), disabled (2)	disabled
Log	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleLog	Read/create	enabled (1), disabled (2)	disabled

3.5 Monitoring Port and Management Traffic

This section describes switch monitoring functions, including those used to mirror traffic to a monitor port for analysis, display detailed network statistics for any port, or display key statistics on SNMP traffic passing through the management port.

Note – The integrated switches on the Sun Fire B1600 blade system chassis are each composed of two switch chips linked together. It is only possible to mirror the traffic on one port by using another port that is on the same switch chip. The ports NETP0, NETP1, NETP4, NETP5, and SNP8 through SNP15 are on one switch chip. The ports NETP2, NETP3, NETP6, NETP7, and SNP0 through SNP7 are on the other. (If you look at the rear panel of the SSC, all the ports on the right are on one chip, and all the ports on the left are on the other.)

3.5.1 Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Note the following points about port mirroring:

- The monitor port speed must match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

3.5.1.1 Web Interface: Configuring Port Mirroring

1. **Open Monitoring ⇒ Port Mirror.**
2. **Select the source port.**
3. **Select the monitor port.**
4. **Select the traffic type to be mirrored.**
5. **Click Add.**

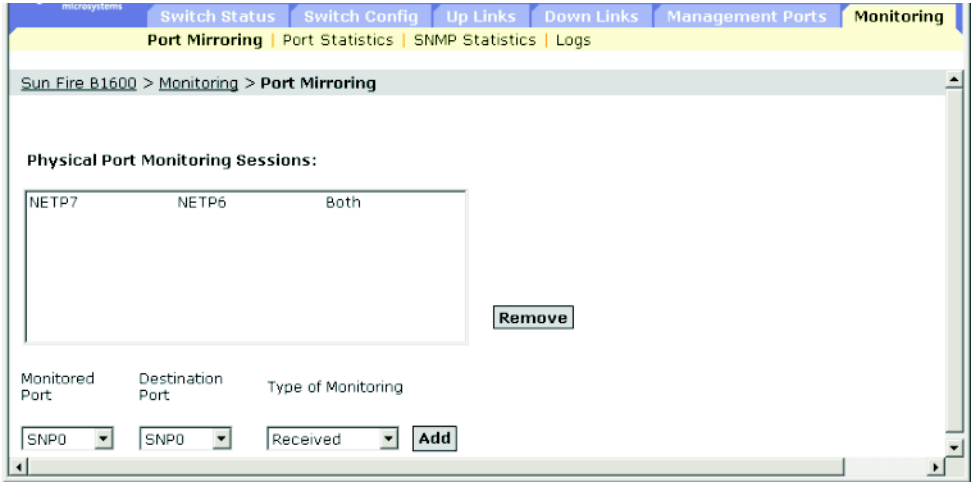


FIGURE 3-44 The Monitoring ⇒ Port Mirroring Window

3.5.1.2 Command-line Interface: Configuring Port Mirroring

Use the `interface` command to select the monitor port, then use the `port monitor` command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

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

3.5.1.3 MIB Variables Associated With Port Mirroring

TABLE 3-42 MIB Variables Associated With Port Mirroring

Field Name	MIB Variable	Access	Value Range	Default Value
Mirror Source Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorSourcePort	Not accessible	Integer	
Mirror Destination Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorDestinationPort	Not accessible	Integer	
Mirror Type	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorType	Read/create	rx (1), tx (2), both (3)	both
Mirror Status	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorStatus	Read/create	valid (1), invalid (2)	

3.5.2 Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 20 seconds by default.

Note – RMON groups 2, 3 and 9 can only be accessed using SNMP.

TABLE 3-43 Traffic Statistics

Statistic	Description
Interface Statistics	
• Received Octets	The total number of octets received on the interface, including framing characters.
• Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
• Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
• Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
• Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
• Received Unknown Packets	The number of packets received through the interface which were discarded because of an unknown or unsupported protocol.
• Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
• Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
• Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
• Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
• Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

TABLE 3-43 Traffic Statistics *(Continued)*

Statistic	Description
• Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
• Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Ether-like Statistics	
• Alignment Errors	The number of alignment errors (missynchronized data packets).
• Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
• FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
• Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
• Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
• Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
• Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
• Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
• SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
• Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
• Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
• Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.

TABLE 3-43 Traffic Statistics *(Continued)*

Statistic	Description
RMON Statistics	
• Drop Events	The total number of events in which packets were dropped due to lack of resources.
• Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
• Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
• Collisions	The best estimate of the total number of collisions on this Ethernet segment.
• Received Frames	The total number of frames (bad, broadcast and multicast) received.
• Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
• Multicast Frames	The total number of good frames received that were directed to this multicast address.
• CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
• Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
• Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
• Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
• 64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
• 65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

3.5.2.1 Web Interface: Viewing Port Statistics

1. **Open Monitoring ⇒ Statistics.**
2. **Select the required interface.**
3. **Click Select.**

   You can also use the Refresh button at the bottom of the page to update the screen.

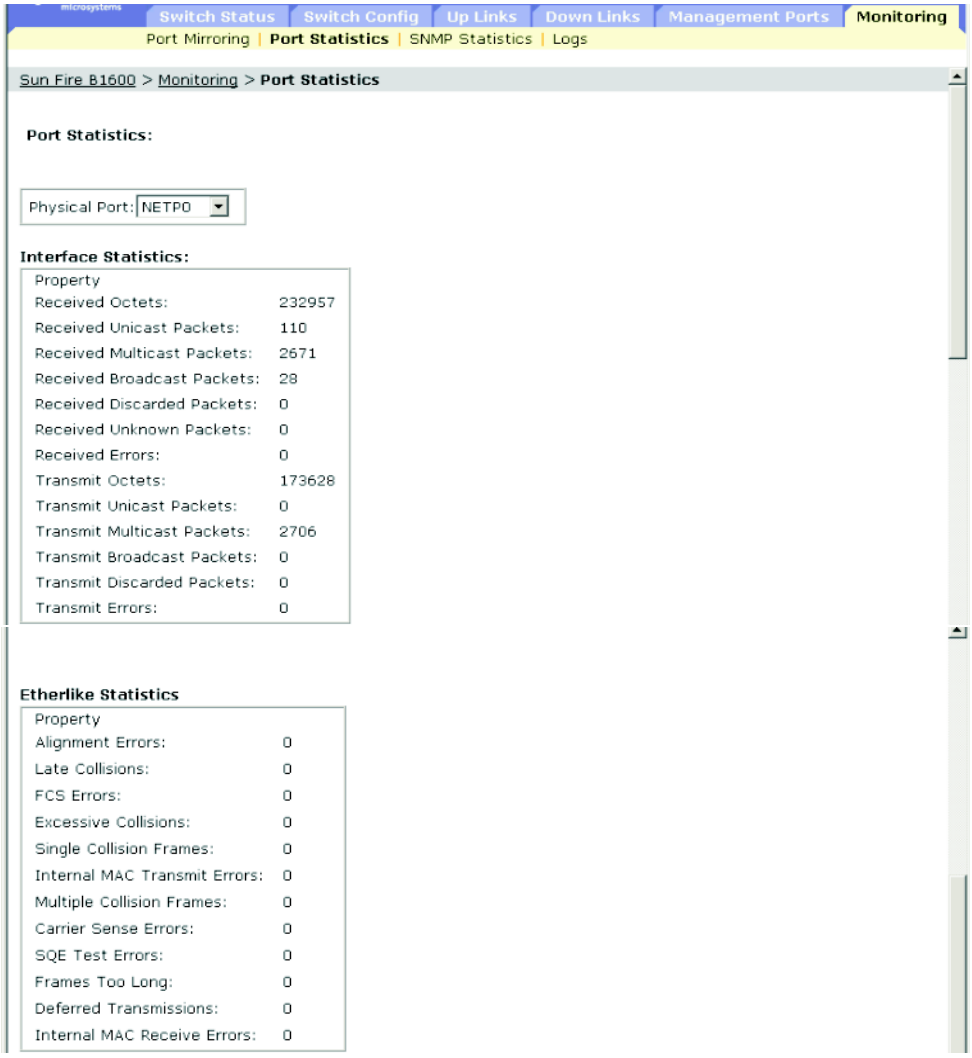


FIGURE 3-45 The Monitoring ⇒ Port Statistics window

Scroll down the page to view RMON statistics.

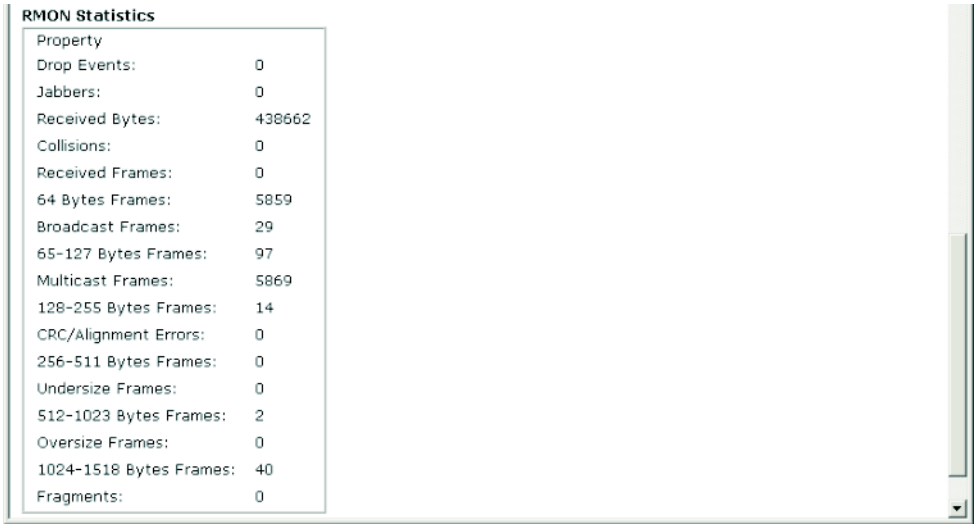


FIGURE 3-46 The Monitoring ⇒ Port Statistics Window Showing RMON Statistics

3.5.2.2 Command-line Interface: Viewing Port Statistics

This example shows statistics for port SNP13.

```
Console#show interfaces counters ethernet SNP13
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: 0, 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#
```

3.5.2.3 MIB Variables Associated With Port Statistics

TABLE 3-44 MIB Variables Associated With Port Statistics

Field Name	MIB Variable	Access	Range
Interface Statistics			
• In Octets	MIB-II. interfaces.ifNumber.ifTable.ifEntry.ifInOctets	Read only	Integer
• In Unicast Packets	MIB-II. interfaces.ifNumber.ifTable.ifEntry. ifInUcastPkts	Read only	Integer
• In Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInMulticastPkts	Read only	Integer
• In Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInBroadcastPkts	Read only	Integer
• In Discards	MIB-II. interfaces.ifTable.ifEntry.ifInDiscards	Read only	Integer
• In Unknown Protocols	MIB-II. interfaces.ifTable.ifEntry.ifInUnknownProtos	Read only	Integer
• In Errors	MIB-II. interfaces.ifTable.ifEntry.ifInErrors	Read only	Integer
• Out Octets	MIB-II. interfaces.ifTable.ifEntry.ifOutOctets	Read only	Integer
• Out Unicast Packets	MIB-II. interfaces.ifTable.ifEntry.ifOutUcastPkts	Read only	Integer
• Out Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutMulticastPkts	Read only	Integer
• Out Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutBroadcastPkts	Read only	Integer

TABLE 3-44 MIB Variables Associated With Port Statistics *(Continued)*

Field Name	MIB Variable	Access	Range
• Out Discards	MIB-II. interfaces.ifTable.ifEntry.ifOutDiscards	Read only	Integer
• Out Errors	MIB-II. interfaces.ifTable.ifEntry.ifOutErrors	Read only	Integer
Ether-like Statistics			
• Alignment Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsAlignmentErrors	Read only	Integer
• Late Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsLateCollisions	Read only	Integer
• FCS Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFCSErrors	Read only	Integer
• Excessive Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3Stats-ExcessiveCollisions	Read only	Integer
• Single Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSingleCollisionFrames	Read only	Integer
• Internal Mac Transmit Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacTransmitErrors	Read only	Integer
• Multiple Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsMultipleCollisionFrames	Read only	Integer
• Carrier Sense Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsCarrierSenseErrors	Read only	Integer

TABLE 3-44 MIB Variables Associated With Port Statistics *(Continued)*

Field Name	MIB Variable	Access	Range
• SQE Test Errors	`MIB-II.transmission.dot3StatsTable.dot3StatsEntry.dot3StatsSQETestErrors`	Read Only	Integer
• Frames Too Long	`MIB-II.transmission.dot3StatsTable.dot3StatsEntry.dot3StatsFrameTooLongs`	Read only	Integer
• Deferred Transmissions	`MIB-II.transmission.dot3StatsTable.dot3StatsEntry.dot3StatsDeferredTransmissions`	Read only	Integer
• Internal MAC Receive Errors	`MIB-II.transmission.dot3StatsTable.dot3StatsEntry.dot3StatsInternalMacReceiveErrors`	Read only	Integer
RMON Statistics			
• Drop Events	`MIB-II.rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsDropEvents`	Read only	Integer
• Jabbers	`MIB-II.rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsJabbers`	Read only	Integer
• Received Octets	`MIB-II.rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsOctets`	Read only	Integer
• Collisions	`MIB-II.rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsCollisions`	Read only	Integer
• Received Packets	`MIB-II.rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsPkts`	Read only	Integer
• Broadcast Packets	`MIB-II.rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsBroadcastPkts`	Read only	Integer

TABLE 3-44 MIB Variables Associated With Port Statistics *(Continued)*

Field Name	MIB Variable	Access	Range
• Multicast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsMulticastPkts	Read only	Integer
• CRC/Alignment Errors	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsCRCAlignErrors	Read only	Integer
• Undersize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsUndersizePkts	Read only	Integer
• Oversize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsOversizePkts	Read only	Integer
• Fragments	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsFragments	Read only	Integer
• 64 Bytes Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsPkts64Octets	Read only	Integer
• X-Y Byte Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry.etherStatsPktsXtoYOctets	Read only	Integer

3.5.3 Showing SNMP Statistics

You can display key statistics on SNMP traffic crossing the management port. This information can be used to debug SNMP errors, or to display the overall amount of SNMP traffic processed by the switch, as well as any illegal attempts to access the switch through SNMP.

TABLE 3-45 SNMP Traffic Statistics

Statistic	Description
SNMP packets input	
• SNMP packets input	The total number of messages delivered to the SNMP entity from the transport service.
• Bad SNMP version errors	The total number of SNMP messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
• Unknown community name	The total number of SNMP messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.
• Illegal operation for community name supplied	The total number of SNMP messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
• Encoding errors	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.
• Number of requested variables	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
• Number of altered variables	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
• Get-request PDUs	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
• Get-next PDUs	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.
• Set-request PDUs	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.

TABLE 3-45 SNMP Traffic Statistics *(Continued)*

Statistic	Description
SNMP packets output	
• SNMP packets output	The total number of SNMP messages which were passed from the SNMP protocol entity to the transport service.
• Too big errors	The total number of SNMP PDUs delivered to the SNMP protocol entity for which the error-status is “tooBig.”
• No such name errors	The total number of SNMP PDUs delivered to the SNMP protocol entity for which the error-status is “noSuchName.”
• Bad values errors	The total number of SNMP PDUs delivered to the SNMP protocol entity for which the error-status is “badValue.”
• General errors	The total number of SNMP PDUs delivered to the SNMP protocol entity for which the error-status is “genErr.”
• Response PDUs	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.
• Trap PDUs	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.

3.5.3.1 Web Interface: Viewing SNMP Statistics

- **Open Monitoring ⇒ SNMP Statistics.**

  You can also use the Refresh button at the bottom of the page to update the screen.

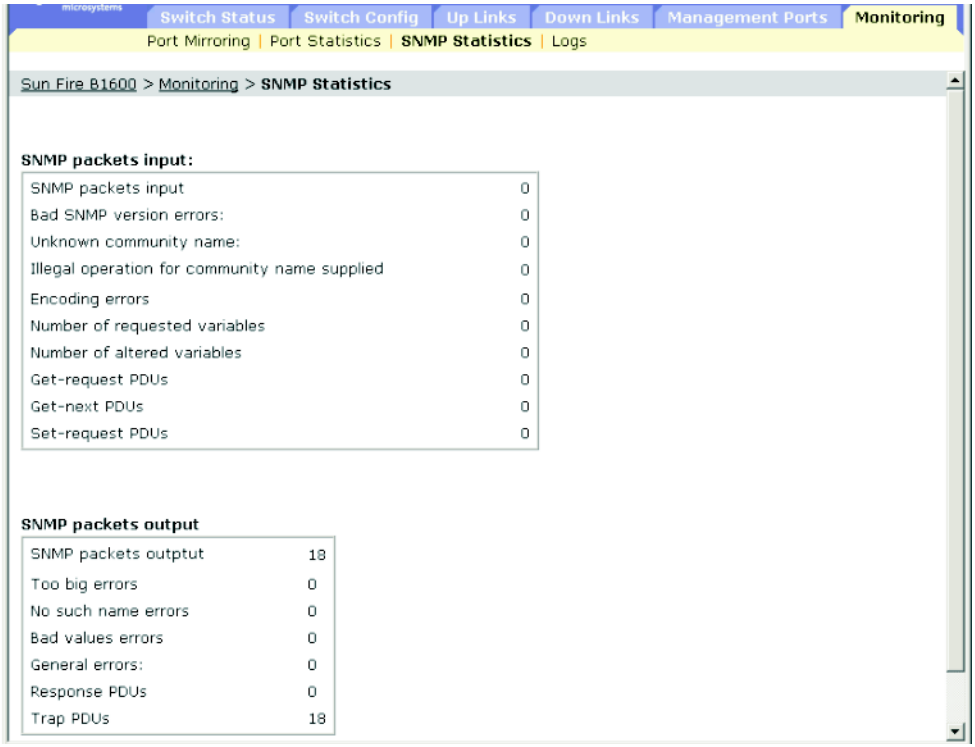


FIGURE 3-47 The Monitoring SNMP Statistics Window

3.5.3.2 Command-line Interface: Viewing SNMP Statistics

This example shows SNMP statistics for the switch.

```
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

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#
```

3.5.3.3 MIB Variables Associated With SNMP Statistics

TABLE 3-46 MIB Variables Associated With SNMP Statistics

Field Name	MIB Variable	Access	Range
SNMP packets input			
In Packets	MIB-II.snmp.snmpInPkts	Read only	Integer
In Bad Versions	MIB-II.snmp.snmpInBadVersions	Read only	Integer
In Bad Community Names	MIB-II.snmp.snmpInBadCommunityNames	Read only	Integer
In Bad Community Uses	MIB-II.snmp.snmpInBadCommunityUses	Read only	Integer
In ASN Parse Errors	MIB-II.snmp.snmpInASNParseErrs	Read only	Integer
In Total Request Variables	MIB-II.snmp.snmpInTotalReqVars	Read only	Integer
In Total Set Variables	MIB-II.snmp.snmpInTotalSetVars	Read only	Integer
In Get Requests	MIB-II.snmp.snmpInGetRequests	Read only	Integer
In Get Nexts	MIB-II.snmp.snmpInGetNexts	Read only	Integer
In Set Requests	MIB-II.snmp.snmpInSetRequests	Read only	Integer
Silent Drops	MIB-II.snmp.snmpSilentDrops	Read only	Integer
Proxy Drops	MIB-II.snmp.snmpProxyDrops	Read only	Integer
SNMP packets output			
Out Packets	MIB-II.snmp.snmpOutPkts	Read only	Integer
Out Too Bigs	MIB-II.snmp.snmpOutTooBigs	Read only	Integer
Out No Such Names	MIB-II.snmp.snmpOutNoSuchNames	Read only	Integer
Out Bad Values	MIB-II.snmp.snmpOutBadValues	Read only	Integer
Out General Errors	MIB-II.snmp.snmpOutGenErrs	Read only	Integer
Out Get Responses	MIB-II.snmp.snmpOutGetResponses	Read only	Integer
Out Traps	MIB-II.snmp.snmpOutTraps	Read only	Integer

3.5.4 Configuring Message Logs

You can limit system log messages saved to switch memory based on severity.

When configuring message logs through the web interface or CLI, the following parameters can be displayed or configured:

- Enable Logging – The status of logging of debug or error messages to switch memory. The default is disabled.
- Logging Level – The error level (between 0 and 7) of system log messages saved to switch memory based on severity. Note that the messages saved include the selected level down to level 0. The defaults are level 3 to 0 for Flash memory and level 7 to 0 for RAM.

TABLE 3-47 Error Levels

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only (that is, all traps)
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (for example, return false, unexpected return)
errors	3	Error conditions (for example, invalid input, default used)
critical	2	Critical conditions (for example, memory allocation, or free memory error - resource exhausted)
alerts	1*	Immediate action needed
emergencies	0*	System unusable

* There are no Level 0 or Level 1 error messages for the current firmware release.

- Log contents – The buttons that allow you to list any system and event messages stored in Flash or RAM, as well as to clear the log messages in Flash memory (non-volatile memory retained after system reboot) or RAM (random access memory lost after system reboot).

3.5.4.1 Web Interface: Configuring Message Logs

1. **Open Monitoring ⇒ Logs.**
2. **Select Enable logging.**
3. **Click Flash or RAM.**
4. **Select the message level to log (includes selected level down to level 0).**
5. **Click Save Changes.**
6. **Click View Flash or View RAM to update the displayed messages.**

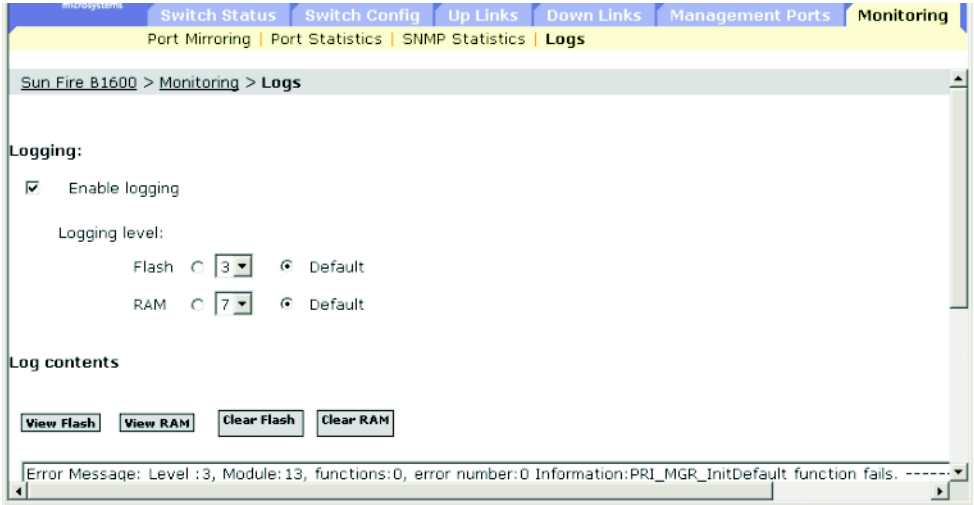


FIGURE 3-48 The Monitoring ⇒ Logs Window

3.5.4.2 Command-line Interface: Configuring Message Logs

This example enables logging, sets the recorded messages for Flash memory to level 3 (that is “errors”), and then shows the log messages stored in Flash.

```
Console(config)#logging on
Console(config)#logging history flash 3
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#
```

3.5.4.3 MIB Variables Associated With Message Logs

TABLE 3-48 MIB Variables Associated With Message Logs

Field Name	MIB Variable	Access	Value Range	Default Value
Log Status	`sun... sysLogMgt. sysLogStatus`	Read/write	enabled (1), disabled (2)	
History Flash Level	`sun... sysLogMgt. sysLogStatus.sysLog .HistoryFlashLevel`	Read/write	Integer (0-7)	
History RAM Level	`sun... sysLogMgt. sysLogStatus.sysLog .HistoryRAMLevel`	Read/write	Integer (0-7)	
Log Messages	*Not Defined.*			

CHAPTER 4

Command-Line Reference

This chapter describes how to use the command-line interface (CLI) and includes the following sections:

4.1 Using the Command-Line Interface

4.1.1 Accessing the CLI

When accessing the management interface for the switch over a direct connection to the switch's console port, or through a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

4.1.1.1 Console Connection

To access the switch through the console port, perform these steps:

1. **At the console prompt, type the user name and password.**

   The default user names are `admin` and `guest` with corresponding passwords of `admin` and `guest`. When the administrator user name and password is entered, the CLI displays the `Console#` prompt and enters privileged access mode (Privileged Exec). But when the guest user name and password is entered, the CLI displays the `Console>` prompt and enters normal access mode (Normal Exec).

2. **Type the necessary commands to complete your desired tasks.**

3. **When finished, exit the session with the `quit` or `exit` command.**

   After connecting to the system through the console port, the login screen displays:

```
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 Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note – The IP address for the switch is unassigned by default. The management port (NETMGT) is assigned to VLAN 2. This port cannot be assigned to a VLAN that contains up-link or down-link ports.

To access the switch through a Telnet session, you must first set the IP address for the switch, and set the default gateway if you are managing the switch from a different IP subnet. For example:

```
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
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that comforms with your site's network policy.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. **From the remote host, enter the Telnet command and the IP address of the device you want to access.**
2. **At the prompt, type the user name and system password.**

   The CLI displays the `Vty-0#` prompt for the administrator to show that you are using privileged access mode (Privileged Exec), or `Vty-0>` for the guest to show that you are using normal access mode (Normal Exec).
3. **Type the necessary commands to complete your desired tasks.**
4. **When finished, exit the session with the `quit` or `exit` command.**

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

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

Vty-0#
```

Note – You can open up to four sessions to the switch through Telnet.

4.1.2 Entering Commands

This section describes how to enter CLI commands.

4.1.2.1 Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command `show interfaces status ethernet SNP5`, `show interfaces` and `status` are keywords, `ethernet` is an argument that specifies the interface type, and `SNP5` specifies the port.

You can enter commands as follows:

- To enter a simple command, type the command keyword.
- To enter multiple commands, type each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, type:

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

- To enter commands that require parameters, type the required parameters after the command keyword. For example, to set a password for the administrator, type:

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

4.1.2.2 Minimum Abbreviation

The CLI accepts a minimum number of characters that uniquely identify a command. For example, the command `logging history` can be entered as `logging h`. If an entry is ambiguous, the system prompts for further input.

4.1.2.3 Command Completion

If you terminate input with a Tab key, the CLI prints the remaining characters of a partial keyword up to the point of ambiguity. In the `logging history` example, typing `log` followed by a tab results in printing the command up to `logging`.

4.1.2.4 Getting Help on Commands

You can display a brief description of the help system by entering the `help` command. You can also display command syntax by using the `?` character to list keywords or parameters.

4.1.2.5 Showing Commands

If you type a `?` at the command prompt, the system displays the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, Interface, Line, or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command `show ?` displays a list of possible show commands:

```
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
```

The command `show interfaces ?` displays the following information:

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

4.1.2.6 Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example `s?` shows all the keywords starting with "s."

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

4.1.2.7 Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword `no` to cancel the effect of a command or reset the configuration to the default value. For example, the `logging` command logs system messages to a host server. To disable logging, specify the `no logging` command. This guide describes the negation effect for all applicable commands.

4.1.2.8 Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the `show history` command displays a longer list of recently executed commands.

4.1.2.9 Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always type a question

mark ? at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

TABLE 4-1 Command Modes

Class	Mode
Exec	Normal
	Privileged
Configuration*	Global
	Interface
	Line
	VLAN Database

* You must be in Privileged Exec mode to access any of the configuration modes.

4.1.2.10 Exec Commands

When you open a new console session on the switch with the user name and password `guest`, the system enters the Normal Exec command mode (or guest mode), displaying the `Console>` command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password `admin`. The system now displays the `Console#` command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by typing the `enable` command, followed by the privileged level password `super`.

To enter Privileged Exec mode, type the following user names and passwords:

```
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 Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the `copy running-config startup-config` command.

The configuration commands are organized into these modes:

- Global Configuration – These commands modify the system level configuration, and include commands such as `hostname` and `snmp-server community`.
- Interface Configuration – These commands modify the port configuration such as `speed-duplex` and `negotiation`.
- Line Configuration – These commands modify the console port and Telnet configuration, and include command such as `exec-timeout` and `silent-time`.
- VLAN Configuration – Includes the command to create VLAN groups.

To enter the Global Configuration mode, type the command `configure` in Privileged Exec mode. The system prompt changes to `Console(config)#`, which gives you access privilege to all Global Configuration commands.

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

To enter the other modes, at the configuration prompt type one of the following commands. Use the `exit` command to return to Configuration mode or the `end` command to return to Privileged Exec mode.

TABLE 4-2 Configuration Modes

Mode	Command	Prompt	See Page
Interface	`interface` {`ethernet` *port* | `port-channel` *id* | `vlan` *id*}	`Console(config-if)#`	4-83
Line	`line` {`console` | `vty`}	`Console(config-line)#`	4-62
VLAN	`vlan database`	`Console(config-vlan)`	4-121

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode.

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

4.1.2.12 Command-Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the `?` character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

TABLE 4-3 CLI Editing Keystrokes

Keystrokes	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-P	Shows the last command.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Delete key or backspace key	Erases a mistake when typing a command.

4.2 Command Groups

The system commands can be broken down into the functional groups shown below.

TABLE 4-4 Command Groups

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	4-13
Flash/File	Manages code image or switch configuration files	4-20
System Management	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	4-27
Authentication	Configures authentication for logon access using local, RADIUS, or TACACS methods	4-45
SNMP	Activates authentication failure traps; configures community access strings, and trap managers	4-54
Line	Sets connection options for the serial port and Telnet, including password checking, line password, and console time-out	4-62
IP	Configures the IP address and gateway for management access, displays the default gateway, or pings a specified device	4-69
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	4-83
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time	4-98
Port Security	Configures secure addresses for a port	4-103
Spanning Tree	Configures Spanning Tree settings for the switch	4-105
VLAN	Configures VLAN settings, and defines port membership for VLAN groups	4-120
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	4-131
IGMP Snooping	Configures IGMP multicast filtering, querier eligibility, query parameters, and specifies ports attached to a multicast router	4-138

TABLE 4-4 Command Groups *(Continued)*

Command Group	Description	Page
Priority	Sets port priority for untagged frames, relative weight for each priority queue, and the maximum number of queues enabled; also sets priority for IP precedence and DSCP	4-150
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	4-164
Link Aggregation and LACP	Statically groups multiple ports into an aggregated link; configures Link Aggregation Control Protocol for aggregated links	4-166

The access mode shown in the following tables is indicated by these abbreviations:

- NE (Normal Exec)
- PE (Privileged Exec)
- GC (Global Configuration)
- IE (Interface Configuration)
- LC (Line Configuration
- VC (VLAN Database Configuration)

4.3 Detailed Command Description

4.3.1 General Commands

TABLE 0-2

Command	Function	Mode	Page
`enable`	Activates privileged mode	NE	4-13
`disable`	Returns to normal mode from privileged mode	PE	4-14
`configure`	Activates global configuration mode	PE	4-15
`reload`	Restarts the system	PE	4-17
`end`	Returns to Privileged Exec mode	GC, IC, LC, VC	4-18
`exit`	Returns to the previous configuration mode, or exits the CLI	any	4-19
`quit`	Exits a CLI session	NE, PE	4-19
`help`	Shows how to use help	any	NA
`?`	Shows options for command completion (context sensitive)	any	NA

4.3.1.1 enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 4-7.

Syntax

`enable` [*level*]

level - Privilege level to log in to the device.

The device has two privilege levels: 0: Normal Exec, 15: Privileged Exec. Type level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- `super` is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the `enable password` command on page 4-30.)
- The # character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

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

Related Commands

`disable` (4-14)

`enable password` (4-30)

4.3.1.2 disable

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 4-7.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The > character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

`enable` (4-13)

4.3.1.3 configure

Use this command to activate Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See "Understanding Command Modes" on page 4-7.

Default Setting

None

Command Mode

Privileged Exec

Example

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

Related Commands

`end` (4-18)

4.3.1.4 show history

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
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#
```

The `!` command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the `!2` command repeats the second command in the Execution history buffer (`config`).

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

4.3.1.5 reload

Use this command to restart the system.

Note – When the system is restarted, it always runs the Power-On Self-Test. It also retains all configuration information stored in non-volatile memory by the `copy running-config startup-config` command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

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

4.3.1.6 end

Use this command to return to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, Router Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

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

4.3.1.7 exit

Use this command to return to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

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

Press ENTER to start session

User Access Verification

Username:
```

4.3.1.8 quit

Use this command to exit the CLI session.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The `quit` and `exit` commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

4.3.2 Flash/File Commands

These commands are used to manage the system code or configuration files.

Command	Function	Mode	Page
`copy`	Copies a code image or a switch configuration to or from Flash memory or a TFTP server	PE	4-20
`delete`	Deletes a file or code image	PE	4-22
`dir`	Displays a list of files in Flash memory	PE	4-23
`whichboot`	Displays the files booted	PE	4-25
`boot system`	Specifies the file or image used to start up the system	GC	4-26

4.3.2.1 copy

Use this command to move (upload/download) a code image or configuration file between the switch's Flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

```
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` – Keyword that allows you to copy to/from a file.
- `running-config` – Keyword that allows you to copy to/from the current running configuration.
- `startup-config` – The configuration used for system initialization.
- `tftp` – Keyword that allows you to copy to/from a TFTP server.
- `https-certificate` – This option allows you to specify a certificate, private key, and password from a recognised certification authority.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the `copy` command.
- The destination configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 32 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use `Factory_Default_Config.cfg` as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you can use `startup-config` as the destination.
- The Boot ROM and Loader code cannot be uploaded or downloaded from the TFTP server. Changing the Boot ROM or Loader code requires a Sun Service Engineer.

Example

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
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#
```

The following example shows how to copy the running configuration to a file.

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

Console#
```

The following example shows how to download a configuration file:

```
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#
```

4.3.2.2 delete

Use this command to delete a file or image.

Syntax

`delete` *filename*

filename – Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is boot-ROM or is used for system startup, then this file cannot be deleted.
- The file `Factory_Default_Config.cfg` cannot be deleted.

Example

This example shows how to delete the test2.cfg configuration file from Flash memory.

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

Related Commands

`dir` (4-23)

4.3.2.3 dir

Use this command to display a list of files in Flash memory.

Syntax

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

The type of file or image to display includes:

- `boot-rom` – Boot ROM
- `config` – Configuration file
- `opcode` – Run-time operation code.
- *filename* – Name of the file to display. If this file exists but contains errors, information on the file cannot be displayed.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command `dir` without any parameters, the system displays all files.
- File information is shown below:

TABLE 4-5 File Information

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
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

Use this command to display which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See TABLE 4-5 on for a description of the file information displayed by this command.

Example

This example shows the information displayed by the `whichboot` command

```
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

Use this command to specify the file or image used to start up the system.

Syntax

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

The type of file or image to set as a default includes:

- `boot-rom` – Boot ROM
- `config` – Configuration file
- `opcode` – Run-time operation code
- The colon (:) is required.
- *filename* – Name of the configuration file or image name.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

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

Related Commands

dir (4-23)

whichboot (4-25)

4.3.3 System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

TABLE 4-6 System Management Commands

Command	Function	Mode	Page
Device Description Command			
hostname	Specifies or modifies the host name for the device	GC	4-28
User Access Commands			
enable password	Sets a password to control access to the Privileged Exec level	GC	4-30
Web Server Commands			
ip http port	Specifies the port to be used by the Web browser interface	GC	4-31
ip http server	Allows the switch to be monitored or configured from a browser	GC	4-32
Jumbo Frame Command			
jumbo-frame	Enables support for jumbo frames	GC	4-33
Event Logging Commands			
logging on	Controls logging of error messages	GC	4-34
logging history	Limits syslog messages saved to switch memory based on severity	GC	4-35
clear logging	Clears messages from the logging buffer	PE	4-36
show logging	Displays the state of logging	PE	4-37

TABLE 4-6 System Management Commands *(Continued)*

Command	Function	Mode	Page
System Status Commands			
`show startup-config`	Displays the contents of the configuration file (stored in Flash memory) that is used to start up the system	PE	4-38
`show running-config`	Displays the configuration data currently in use	PE	4-40
`show system`	Displays system information	NE, PE	4-42
`show users`	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	4-44
`show version`	Displays version information for the system	NE, PE	4-44

4.3.3.1 hostname

Use this command to specify or modify the host name for this device. Use the `no` form to restore the default host name.

Syntax

`hostname` *name*

`no hostname`

name – The name of this host. The maximum length is 255 characters.

Default Setting

None

Command Mode

Global Configuration

Example

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

4.3.3.2 username

Use this command to add named users, require authentication at login, specify or change a user's password (or specify that no password is required), or specify or change a user's access level. Use the `no` form to remove a user name.

Syntax

`username` *name* {`access-level` *level* | `nopassword` | `password` {`0` | `7`} *password*}

`no username` *name*

- *name* – The name of the user.

  (Maximum length: 8 characters; maximum number of users: 5)

- access-level *level* – Specifies the user level.

  The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. (Levels 1-14 are not used.)

- nopassword – No password is required for this user to log in.

  {`0` | `7`} – `0` means input plain password, `7` means input encrypted password.

- password *password* – The authentication password for the user.

  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The default passwords are `guest` in Normal Exec mode, and `admin` in Privileged Exec mode.

  Factory defaults for the user names and passwords are:

TABLE 4-7 Default User Names and Passwords

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

There is no need to specify encrypted passwords on the command line. The option 7 is used internally by the switch at system bootup time to enable the switch to read any encrypted passwords stored in the configuration file.

Example

This example shows how the set the access level and password for a user.

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

4.3.3.3 enable password

After initially logging onto the system, first set the Privileged Exec password. Remember to record it in a safe place. Use this command to control access to the Privileged Exec level from the Normal Exec level. Use the `no` form to reset the default password.

Syntax

`enable password` [`level` *level*] {`0` | `7`} *password*

`no enable password` [`level` *level*]

- `level` *level* – Level 15 for Privileged Exec. (Levels 0 to 14 are not used.)

  {0 | 7} – 0 means input plain password, 7 means input encrypted password.

- *password* – password for this privilege level.

  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is `super`

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You have to enter a password to change the command mode from Normal Exec to Privileged Exec with the `enable` command (page 4-13).
- There is no need to specify encrypted passwords on the command line. The option 7 is used internally by the switch at system bootup time to enable the switch to read any encrypted passwords stored in the configuration file.

Example

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

Related Commands

`enable` (4-13)

4.3.3.4 ip http port

Use this command to specify the TCP port number used by the Web browser interface. Use the `no` form to use the default port.

Syntax

`ip http port` *port-number*

`no ip http port`

port-number – The TCP port to be used by the browser interface. (Range: 1 to 65,535)

Default Setting

80

Command Mode

Global Configuration

Example

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

Related Commands

`ip http server` (4-32)

4.3.3.5 ip http server

Use this command to allow the switch to be monitored or configured from a browser. Use the `no` form to disable this function.

Syntax

`ip http server`

`no ip http server`

Default Setting

Enabled

Command Mode

Global Configuration

Example

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

Related Commands

`ip http port` (4-31)

4.3.3.6 jumbo frame

Use this command to enable support for jumbo frames. Use the `no` form to disable it.

Syntax

`jumbo frame`

`no jumbo frame`

Default Setting

disabled

Command Mode

Global Configuration

Command Usage

- The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9000 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

- Enabling jumbo frames limits the maximum threshold for broadcast storm control to 64 packets per second. (See the `switchport broadcast` command on page 4-91.)

Example

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

4.3.3.7 logging on

Use this command to control logging of error messages. This command sends debug or error messages to switch memory. The `no` form disables the logging process.

Syntax

`logging on`

`no logging on`

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory. You can use the `logging history` command to control the type of error messages that are stored.

Example

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

Related Commands

`logging history` (4-35)

`clear logging` (4-36)

4.3.3.8 logging history

Use this command to limit syslog messages saved to switch memory based on severity. The `no` form returns the logging of syslog messages to the default level.

Syntax

`logging history` {`flash` | `ram`} *level*

`no logging history` {`flash` | `ram`}

- `flash` – The event history stored in Flash memory (permanent memory).
- `ram` – The event history stored in temporary RAM (memory flushed on power reset).
- *level* – 0 to 7 (Messages saved include the selected level down to level 0.)

TABLE 4-8 Error Levels

Level Argument	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (for example, return false, unexpected return)
errors	3	Error conditions (for example, invalid input, default used)
critical	2	Critical conditions (for example, memory allocation, or free memory error - resource exhausted)
alerts*	1	Immediate action needed
emergencies*	0	System unusable

* There are no Level 0 or Level 1 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 to 0)

RAM: warnings (level 7 to 0)

Command Mode

Global Configuration

Command Usage

The message level specified for Flash memory must be a higher priority (numerically lower) than that specified for RAM.

Example

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

4.3.3.9 clear logging

Use this command to clear messages from the log buffer.

Syntax

`clear logging` [`flash` | `ram`]

- `flash` – The event history stored in Flash memory (permanent memory).
- `ram` – The event history stored in temporary RAM (memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

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

Related Commands

`show logging` (4-37)

4.3.3.10 show logging

Use this command to display the current logging configuration, along with any system and event messages stored in memory.

Syntax

`show logging {flash | ram}`

- `flash` – Event history stored in Flash memory (permanent memory).
- `ram` – Event history stored in temporary RAM (memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command shows the following information:

- Syslog logging – Whether or not system logging has been enabled using the `logging on` command.
- History logging in FLASH/RAM – The message level(s) that are reported based on the `logging history` command.
- Any system and event messages stored in memory.

Example

The following example shows that system logging is enabled, the message level for Flash memory is `errors` (default level 3 to 0), the message level for RAM is `debugging` (default level 7 to 0), and lists one sample error.

```
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#
```

Related Commands

`logging on` (4-34)

`logging history` (4-35)

4.3.3.11 show startup-config

Use this command to display the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the `show running-config` command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by `!` symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

  System description (host name, location, contact information)

  SNMP community strings

  Users (names, access levels, and encrypted passwords)

  VLAN database (VLAN ID, name and state)

  VLAN configuration settings for each interface

  IP address of the management VLAN

  User authentication sequence, along with remote authentication server address and UDP port

  Any configured settings for the console port and Telnet

Example

```
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#
```

Related Commands

`show running-config` (4-40)

4.3.3.12 show running-config

Use this command to display the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the `show startup-config` command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by `!` symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:

  System description (host name, location, contact information)

  SNMP community strings

  Users (names, access levels, and encrypted passwords)

  VLAN database (VLAN ID, name and state)

  VLAN configuration settings for each interface

  IP address of the management VLAN

  User authentication sequence, along with remote authentication server address and UDP port

  Any configured settings for the console port and Telnet

Example

```
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#
```

Related Commands

`show startup-config` (4-38)

4.3.3.13 show system

Use this command to display system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to "Displaying System Information" on page 3-8.
- The POST results should all display PASS. If any POST test indicates FAIL, contact your distributor for assistance.

Example

```
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

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a * symbol next to the Line (session) index number.

Example

```
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

Use this command to display hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See "Displaying Switch Software Versions" on page 3-18 for detailed information about the software items. The meaning of hardware items are as follows:

- Serial Number – The serial number of the main board.
- Service Tag – Not applicable for this switch.
- Hardware Version – The hardware version of the main board.
- Number of Ports – The number of ports on the switch
- Main Power Status – The power status for the switch.
- Redundant Power Status – Not applicable for this switch.

Example

```
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 Authentication Commands

You can configure the switch to authenticate users logging into the system for management access using local, RADIUS, or TACACS authentication methods.

RADIUS and TACACS are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name and password pairs with associated privilege levels for each user that requires management access to a switch.

TABLE 4-9 Authentication Commands

Command	Function	Mode	Page
Authentication Method			
`authentication login`	Defines logon authentication method and precedence	GC	4-46
RADIUS Client			
`radius-server host`	Specifies the RADIUS server	GC	4-48
`radius-server port`	Sets the RADIUS server network port	GC	4-48
`radius-server key`	Sets the RADIUS encryption key	GC	4-49
`radius-server retransmit`	Sets the number of retries	GC	4-50
`radius-server timeout`	Sets the interval between sending authentication requests	GC	4-50
`show radius-server`	Shows the current RADIUS settings	PE	4-51
TACACS Client			
`tacacs-server host`	Specifies the TACACS server	GC	4-52
`tacacs-server port`	Sets the TACACS server network port	GC	4-52
`tacacs-server key`	Sets the TACACS encryption key	GC	4-53
`show tacacs-server`	Shows the current TACACS settings	PE	4-54

4.3.4.1 authentication login

Use this command to define the login authentication method and precedence. Use the `no` form to restore the default.

Syntax

`authentication login` {[`local`] [`radius`] [`tacacs`]}

`no authentication login`

- `local` – Use local password.
- `radius` – Use RADIUS server password.
- `tacacs` – Use TACACS server password.

Authentication methods may be specified in any order.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS encrypts the entire body of the packet.
- RADIUS and TACACS logon authentication can control management access through the console port, a Web browser, or Telnet. These access options must be configured on the authentication server.
- RADIUS and TACACS logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify two or three authentication methods in a single command to indicate the authentication sequence. For example, if you enter `authentication login radius local`, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then the local user name and password is checked.

Example

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

Related Commands

`username` – for setting the local user name and password (4-29)

4.3.4.2 radius-server host

Use this command to specify the RADIUS server. Use the `no` form to restore the default.

Syntax

`radius-server host` *host_ip_address*

`no radius-server host`

host_ip_address – The IP address of the server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

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

4.3.4.3 radius-server port

Use this command to set the RADIUS server network port. Use the `no` form to restore the default.

Syntax

`radius-server port` *port_number*

`no radius-server port`

port_number – RADIUS server UDP port (between 1 and 65,535) used for authentication messages.

Default Setting

1812

Command Mode

Global Configuration

Example

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

4.3.4.4 radius-server key

Use this command to set the RADIUS encryption key. Use the `no` form to restore the default.

Syntax

`radius-server key` *key_string*

`no radius-server key`

key_string – The encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. The maximum length is 20 characters.

Default Setting

None

Command Mode

Global Configuration

Example

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

4.3.4.5 radius-server retransmit

Use this command to set the number of retries. Use the `no` form to restore the default.

Syntax

`radius-server retransmit` *number_of_retries*

`no radius-server retransmit`

number_of_retries – The number of times (between 1 and 30) the switch tries to authenticate logon access through the RADIUS server.

Default Setting

2

Command Mode

Global Configuration

Example

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

4.3.4.6 radius-server timeout

Use this command to set the interval between transmitting authentication requests to the RADIUS server. Use the `no` form to restore the default.

Syntax

`radius-server timeout` *number_of_seconds*

`no radius-server timeout`

number_of_seconds – The number of seconds (between 1 and 65,535) the switch waits for a reply before resending a request.

Default Setting

5

Command Mode

Global Configuration

Example

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

4.3.4.7 show radius-server

Use this command to display the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
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

Use this command to specify the TACACS server. Use the `no` form to restore the default.

Syntax

`tacacs-server host` *host_ip_address*

`no tacacs-server host`

host_ip_address – IP address of server.

Default Setting

None

Command Mode

Global Configuration

Example

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

4.3.4.9 tacacs-server port

Use this command to set the TACACS server network port. Use the `no` form to restore the default.

Syntax

`tacacs-server port` *port_number*

`no tacacs-server port`

port_number - TACACS server UDP port (between 1 and 65,535) used for authentication messages.

Default Setting

None

Command Mode

Global Configuration

Example

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

4.3.4.10 tacacs-server key

Use this command to set the TACACS encryption key. Use the **no** form to restore the default.

Syntax

`tacacs-server key` *key_string*

`no tacacs-server key`

key_string – The encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. The maximum length is 20 characters.

Default Setting

None

Command Mode

Global Configuration

Example

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

4.3.4.11 show tacacs-server

Use this command to display the current settings for the TACACS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
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 Commands

Controls access to this switch from SNMP management stations, as well as the error types sent to trap managers.

TABLE 4-10 SNMP Commands

Command	Function	Mode	Page
`snmp-server community`	Sets the community access string to permit access to SNMP commands	GC	4-55
`snmp-server contact`	Sets the system contact string	GC	4-56
`snmp-server location`	Sets the system location string	GC	4-57

TABLE 4-10 SNMP Commands

Command	Function	Mode	Page
`snmp-server host`	Specifies the recipient of an SNMP notification operation	GC	4-57
`snmp-server enable traps`	Enables the device to send SNMP traps (SNMP notifications)	GC	4-59
`show snmp`	Displays the status of SNMP communications	NE, PE	4-60

4.3.5.1 snmp-server community

Use this command to define the community access string for the Simple Network Management Protocol. Use the `no` form to remove the specified community string.

Syntax

`snmp-server community` *string* [`ro`|`rw`]

`no snmp-server community` *string*

- *string* – Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; maximum number of strings: 5)
- `ro` – Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- `rw` – Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- `public` - with read-only access.
- `private` - with read/write access.

Command Mode

Global Configuration

Command Usage

The first `snmp-server community` command you enter enables all versions of SNMP (SNMP v1 and SNMP v2c). The `no snmp-server community` command disables all versions of SNMP.

Example

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

4.3.5.2 snmp-server contact

Use this command to set the system contact string. Use the `no` form to remove the system contact information.

Syntax

`snmp-server contact` *string*

`no snmp-server contact`

string – The string that describes the system contact information.

(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

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

Related Commands

`snmp-server location` (4-57)

4.3.5.3 snmp-server location

Use this command to set the system location string. Use the `no` form to remove the location string.

Syntax

`snmp-server location` *text*

`no snmp-server location`

text – String that describes the system location.

(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

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

Related Commands

`snmp-server contact` (4-56)

4.3.5.4 snmp-server host

Use this command to specify the recipient of a Simple Network Management Protocol notification operation. Use the `no` form to remove the specified host.

Syntax

`snmp-server host` *host-addr community-string* `version` *version-number*

`no snmp-server host` *host-addr*

- *host-addr* – Name or Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- *community-string* – Password-like community string sent with the notification operation. Though you can set this string using the `snmp-server host` command by itself, we recommend you define this string using the `snmp-server community` command prior to using the `snmp-server host` command. (Maximum length: 32 characters)
- *version-number* – {`1` | `2c`}
- Indicates if the host is running SNMP version 1 or version 2c.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- If you do not enter an `snmp-server host` command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one `snmp-server host` command. In order to enable multiple hosts, you must issue a separate `snmp-server host` command for each host.
- The `snmp-server host` command is used in conjunction with the `snmp-server enable traps` command. Use the `snmp-server enable traps` command to specify which SNMP notifications are sent globally. For a host to receive notifications, you must enter at least one `snmp-server enable traps` command and the `snmp-server host` command for that host.
- Some notification types cannot be controlled with the `snmp-server enable traps` command. For example, some notification types are always enabled.

Example

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

Related Commands

`snmp-server enable traps` (4-59)

4.3.5.5 snmp-server enable traps

Use this command to enable the switch to send Simple Network Management Protocol traps (SNMP notifications). Use the `no` form to disable SNMP notifications.

Syntax

`snmp-server enable traps` [`authentication` | `link-up-down`]

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

- `authentication` – The keyword to issue authentication failure traps.
- `link-up-down` – The keyword to issue link-up or link-down traps.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an `snmp-server enable traps` command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one `snmp-server enable traps` command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The `snmp-server enable traps` command is used in conjunction with the `snmp-server host` command. Use the `snmp-server host` command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one `snmp-server host` command.

Example

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

Related Commands

`snmp-server host` (4-57)

4.3.5.6 show snmp

Use this command to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the `snmp-server enable traps` command.

Example

```
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 Line Commands

You can access the on-board configuration program by attaching a VT100 compatible device to the switch's serial port. These commands are used to set communication parameters for the serial port or Telnet (a virtual terminal).

Note – The connection parameters for the serial interface are fixed at 8 data bits, 1 stop bit, no parity, and 9600 bps.

TABLE 4-11 Line Commands

Command	Function	Mode	Page
`line`	Identifies a specific line for configuration and starts the line configuration mode	GC	4-62
`login`	Enables password checking at login	LC	4-63
`password`	Specifies a password on a line	LC	4-64
`exec-timeout`	Sets the interval that the command interpreter waits until user input is detected	LC	4-66
`password-thresh`	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	4-66
`silent-time`*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the `password-thresh` command	LC	4-67
`show line`	Displays a terminal line's parameters	NE, PE	4-68

* This command only applies to the serial port.

4.3.6.1 line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

`line {console | vty}`

- `console` – The console terminal line.
- `vty` – A virtual terminal for remote console access (Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as `Vty` in screen displays such as `show users`.

Example

To enter console line mode, enter the following command:

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

Related Commands

`show line` (4-68)

`show users` (4-44)

4.3.6.2 login

Use this command to enable password checking at login. Use the `no` form to disable password checking and allow connections without a password.

Syntax

`login` [`local`]

`no login`

`local` – Selects local password checking. Authentication is based on the user name specified with the `username` command.

Default Setting

`login local`

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:

  `login` selects authentication by a single global password as specified by the `password` line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.

  `login local` selects authentication using the user name and password specified by the `username` command (the default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).

  `no login` selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication through the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

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

Related Commands

username (4-29)

password (4-64)

4.3.6.3 password

Use this command to specify the password for a line. Use the `no` form to remove the password.

Syntax

`password {0 | 7} password`

`no password`

- `{0 | 7}` - 0 means input plain password, 7 means input encrypted password.
- *password* - Character string that specifies the line password.

  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the `password-thresh` command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- There is no need to specify encrypted passwords on the command line. The option 7 is used internally by the switch at system bootup time to enable the switch to read any encrypted passwords stored in the configuration file.

Example

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

Related Commands

`login` (4-63)

`password-thresh` (4-66)

4.3.6.4 exec-timeout

Use this command to set the interval that the system waits for user input before terminating the current session. Use the `no` form to restore the default.

Syntax

`exec-timeout` [*seconds*]

`no exec-timeout`

seconds - Integer that specifies the number of seconds. (Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout

Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the serial console and Telnet connections (but you cannot disable the timeout for Telnet).

Example

To set the timeout to two minutes, enter this command:

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

4.3.6.5 password-thresh

Use this command to set the password intrusion threshold that limits the number of failed login attempts. Use the `no` form to remove the threshold value.

Syntax

`password-thresh` *threshold*

`no password-thresh`

threshold – The number of allowed password attempts. (Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the login attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next login attempt. (Use the `silent-time` command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.
- This command applies to both the local console and Telnet connections.

Example

To set the password threshold to five attempts, enter this command:

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

Related Commands

`silent-time` (4-67)

4.3.6.6 silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful login attempts exceeds the threshold set by the `password-thresh` command. Use the `no` form to remove the silent time value.

Syntax

`silent-time` [*seconds*]

`no silent-time`

seconds – The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration

Example

To set the silent time to 60 seconds, enter this command:

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

Related Commands

`password-thresh` (4-66)

4.3.6.7 show line

Use this command to display the terminal line's parameters.

Syntax

`show line` [`console` | `vty`]

- `console` – The console terminal line.
- `vty` – A virtual terminal for remote console access (Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show the connection settings for all lines, enter this command:

```
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 Commands

By default, the switch searches for its IP address, default gateway, and netmask using DHCP.

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the software.

TABLE 4-12 IP Commands

Command	Function	Mode	Page
IP Configuration			
`ip address`	Sets the IP address for this device	IC	4-70
`ip dhcp restart`	Submits a BOOTP or DCHP client request	PE	4-71

TABLE 4-12 IP Commands

Command	Function	Mode	Page
`ip dhcp client-identifier`	Specifies the DHCP client identifier for the switch. Note that the System Controller assigns the client identifier for the switch each time either it or the switch boots. Therefore we do not recommend you specify a client identifier.	VC	4-72
`ip default-gateway`	Defines the default gateway through which an in-band management station can reach this device	GC	4-74
`show ip interface`	Displays the IP settings for this device	PE	4-75
`show ip redirects`	Displays the default gateway configured for this device	PE	4-75
`ping`	Sends ICMP echo request packets to another node on the network	NE, PE	4-76
IP Packet Filtering			
`ip filter`	Blocks specified IP packets from entering the internal management port (NETMGT) from other switch ports	GC	4-77
`show ip filter`	Displays filter rules or captured packets	PE	4-81

4.3.7.1 ip address

Use this command to set the IP address for this device. Use the `no` form to restore the default IP address.

Syntax

`ip address` {*ip-address netmask* | `bootp` | `dhcp`}

`no ip address`

- *ip-address* – The IP address
- *netmask* – The network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- `bootp` – Obtains an IP address using BOOTP.
- `dhcp` – Obtains an IP address using DHCP.

Default Setting

The default setting is: `dhcp`

Command Mode

Interface Configuration (VLAN)

Command Usage

- You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. The factory default is to use DHCP. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Any other format will not be accepted by the software.
- If you select the `bootp` or `dhcp` option, IP is enabled but does not function until a BOOTP or DHCP reply is received. Requests are broadcast periodically by the switch in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- You can start broadcasting BOOTP or DHCP requests by entering an `ip dhcp restart` command, or by rebooting the switch.

Note – The IP address of the switch is in fact the IP address of the VLAN containing the management port (NETMGT). By default, the management port is on VLAN 2. Therefore, by assigning an IP address to VLAN 2 you set up network access to the switch. Only the VLAN containing the management port should be assigned an IP address. If you assign an IP address to any other VLAN, the original IP address is immediately disabled and the new address takes immediate effect.

Example

In the following example, the device is assigned an address in VLAN 2.

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

Related Commands

`ip dhcp restart` (4-71)

4.3.7.2 ip dhcp restart

Use this command to initiate a BOOTP or DCHP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server is moved to a different domain, the network portion of the address provided to the client is based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
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#
```

Related Commands

`ip address` (4-70)

4.3.7.3 ip dhcp client-identifier

You can use this command to specify the DCHP client identifier for the switch. Use the `no` form to remove this identifier.

Note – The client identifier is overwritten by the SC the next time the system, or the switch itself, is rebooted. The client-identifier command will be removed from the next firmware release.

Syntax

`ip dhcp client-identifier` {`text` *text* | `hex` *hex*}

`no ip dhcp client-identifier`

- *text* – A text string. (Range: 1-15 characters)
- *hex* – The hexidecimal value.

Default Setting

The DHCP client identifier is supplied by the System Controller in the SSC whenever the System Controller resets the switch. Therefore, do not change this value from the switch command-line interface. For information about the DHCP client identifier for the switch and the other components of the system chassis, refer to the *Sun Fire 1600 Blade System Chassis Software Setup Guide*.

Command Mode

Interface Configuration (VLAN)

Command Usage

- This command is used to include a client identifier in all communications with the DHCP server. The data type used will depend on the requirements of your DHCP server.
- The client identifier specified in this command is overwritten by the System Controller the next time the System Controller is rebooted.

Example.

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

Related Commands

`ip dhcp restart` (4-71)

4.3.7.4 ip default-gateway

Use this command to a establish a static route between the switch and management stations that exist on another network segment. Use the `no` form to remove the static route.

Syntax

`ip default-gateway` *gateway*

`no ip default-gateway`

gateway – The IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

A gateway must be defined if the management station is located in a different IP segment.

Example

The following example defines a default gateway for this device:

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

Related Commands

`show ip redirects` (4-75)

4.3.7.5 show ip interface

Use this command to display the settings of an IP interface.

Default Setting

All interfaces

Command Mode

Privileged Exec

Command Usage

This switch can only be assigned one IP address. This address is used for managing the switch.

Example

```
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#
```

Related Commands

`show ip redirects` (4-75)

4.3.7.6 show ip redirects

Use this command to show the default gateway configured for the switch.

Default Setting

None

Command Mode

Privileged Exec

Example

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

Related Commands

`ip default-gateway` (4-74)

4.3.7.7 ping

Use this command to send ICMP echo request packets to another node on the network.

Syntax

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

- *host* – The IP address of the host.
- *count* – The number of packets to send. (Range: 1-16, default: 5)
- *size* – The number of bytes in a packet. (Range: 32-512, default: 32)

  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

Default Setting

This command has no default for the host.

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the ping command:

  Normal response – The normal response occurs in one to ten seconds, depending on network traffic.

  Destination does not respond – If the host does not respond, the switch displays `timeout`.

  Destination unreachable – The gateway for this destination indicates that the destination is unreachable.

  Network or host unreachable – The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

Example

```
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

Use this command to block specified IP packets from reaching the internal management port from the down-link ports. Use the `no` form to remove a rule from the filter table.

Syntax

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

The port number is not checked. The `fragments` option is allowed.

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

The port number is checked; that is, if either *source-port-range* or *destination-port-range* is specified, the `fragments` option is not allowed.

`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`]

Checks for `tcp` keyword. If found, the `code` option is allowed.

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

Deletes the specified rule number from the filter table.

- *rule-number* – Inserts a filter rule at the specified position in the table, pushing any existing patterns at or below that location down in the table. A rule-number cannot exceed the next available number in the table. If the rule-number is not specified, a new pattern is appended to the end of the rule table. The maximum number of rules is 128.
- *action* – {`deny` | `permit`}

  Blocks or allows packets moving between the down-link ports and the management port (NETMGT).
- *protocol* – {`any` | `tcp` | `udp` | number}

  Indicates any protocol, TCP, UDP, or a specific protocol number (0 to 255).
- *source source-bitmask* – The frame's source address and netmask.
- *source-port-range* – [number | start_number-end_number]

  TCP/UDP source port or port range. (Range: 0 to 65,535)
- *destination destination-bitmask* – The frame's destination address and netmask.
- *destination-port-range* – [number | start_number-end_number]

  TCP/UDP destination port or port range. (Range: 0-65535)
- `code`

  code – A decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

  code-bitmask – A decimal number (representing a bit mask) that is applied to the code. Type a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

1 (fin) – Finish
2 (syn) – Synchronize
4 (rst) – Reset
8 (psh) – Push
16 (ack) – Acknowledgement
32 (urg) – Urgent pointer

code-keyword-seq – The following code keywords can be specified, but must follow the indicated sequence: `fin | syn | rst | psh | ack | urg`

(The code keyword must be ON if specified and OFF if not specified.)

- `fragments` – The rule only matches packets with the More Fragments (MF) bit set or with a fragment offset greater than zero. If fragment is not set, the rule matches both fragment and non-fragment packets.
- `log` – Logs any matching packets in the log buffer. The maximum number of entries stored in the log buffer is 64. When the buffer fills, it wraps around and overwrites the oldest entries. Note that the log is stored in RAM and is lost when the switch is reset.

Default Setting

None

Command Mode

General Configuration

Command Usage

- The system default is to stop all IP packets from passing from the down-link ports to the management port (NETMGT). If you need the blades to access the management network through the management port (NETMGT), you must set a filter to permit specific frames to pass from the down-link ports through the management port. Note that traffic is never allowed to pass from the up-link ports to the management port.
- A fragment is a packet where MF (more fragments) = 1 or Fragment Offset > 0. If the `fragments` keyword is absent in a rule, then both fragments and non-fragmented packets will be checked by the rule.
- When specifying a code value and mask, the logic is that a packet matches if <value in header> & <mask> == <value> & <mask>. For example, use the code value and mask shown below to catch packets with the following flags set:

SYN flag valid, use `code 2 2`
Both SYN and ACK valid, use `code 18 18`
SYN valid and ACK invalid, use `code 2 18`

Example – Address filters

This example allows all packets to pass through the filter by permitting any protocol type, and using a null address and network mask for both the source address and destination address.

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

This accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; that is, the rule (10.7.1.1 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

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

Example – Checking for fragments

This example blocks all fragments and logs the matching packets in the log.

```
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)#
```

Example – Checking for code values

This blocks all TCP packets from class C addresses 192.168.1.0 with SYN set.

```
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)#
```

This also blocks all TCP packets from class C addresses 192.168.1.0 with SYN set.

```
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)#
```

Example – Checking for port numbers

This example allows TCP packets from class C addresses 192.168.1.0 to anywhere when set for destination port 80.

```
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)#
```

This example drops any TCP packets from source 10.7.1.1 to destination 10.8.1.1, with the source port between 30 - 46 and the destination port between 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

Use this command to display all rules in the IP filter table.

Syntax

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

- *rule-number* – Display a filter rule at the specified position in the table. Range: 1-128
- `log` – Display all packets stored in the log buffer. Note that packets stored in this buffer must match the rules in the filter table. The maximum number of entries stored in the log buffer is 64.

  If no options are selected, all packets in the log buffer are displayed.

Default Setting

None

Command Mode

Privileged Exec

Example

In this example, the only specified rule permits packets within the subnet 10.1.0.x to pass between the management port and the down-link ports.

```
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 Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

TABLE 4-13 Interface Commands

Command	Function	Mode	Page
`interface`	Configures an interface type and enters interface configuration mode	GC	4-83
`description`	Adds a description to an interface configuration	IC	4-84
`speed-duplex`	Configures the speed and duplex operation of a given interface when auto-negotiation is disabled	IC	4-85
`negotiation`	Enables auto-negotiation of a given interface	IC	4-86
`capabilities`	Advertises the capabilities of a given interface for use in auto-negotiation	IC	4-87
`flowcontrol`	Enables flow control on a given interface	IC	4-89
`shutdown`	Disables an interface	IC	4-91
`switchport broadcast packet-rate`	Configures the broadcast storm control threshold	IC	4-91
`clear counters`	Clears statistics on an interface	PE	4-93
`show interfaces status`	Displays status for the specified interface	NE, PE	4-93
`show interfaces counters`	Displays statistics for the specified interface	NE, PE	4-95
`show interfaces switchport`	Displays the administrative and operational status of an interface	NE, PE	4-96

4.3.8.1 interface

Use this command to configure an interface type and enter interface configuration mode.

Syntax

`interface` *interface*

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

interface

- `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT
- `port-channel` *channel-id* (Range: 1 to 6)
- `vlan` *vlan-id* (Range: 1 to 4094)

Default Setting

None

Command Mode

Global Configuration

Example

To specify the first up-link port, enter the following command:

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

4.3.8.2 description

Use this command to add a description to an interface. Use the `no` form to remove the description.

Syntax

`description` *string*

`no description`

string – A comment or a description to help you remember what is attached to the interface. (Range: 1 to 64 characters)

Default Setting

NETP0-7: External RJ-45 connector NET0-7

SNP0-15: Blade Slot 0-15

NETMGT: External RJ-45 connector NETMGT

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following example configures a description for down-link port SNP5.

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

4.3.8.3 speed-duplex

Use this command to configure the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the `no` form to restore the default.

Syntax

`speed-duplex` {`1000full` | `100full` | `100half` | `10full` | `10half`}

`no speed-duplex`

- `1000full` – Forces 1000 Mbit/sec full-duplex operation
- `100full` – Forces 100 Mbit/sec full-duplex operation
- `100half` – Forces 100 Mbit/sec half-duplex operation
- `10full` – Forces 10 Mbit/sec full-duplex operation
- `10half` – Forces 10 Mbit/sec half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is `100full`. for Fast Ethernet ports and `1000full` for Gigabit Ethernet ports.

Note – When auto-negotiation is disabled, you can only set the up-link ports to 10 Mbit/sec or 100 Mbit/sec. To force a port to operate at 1 Gbit/sec full duplex, enable auto-negotiation, and set the port capabilities to `1000full` only.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- To force operation to the speed and duplex mode specified in a `speed-duplex` command, use the `no negotiation` command to disable auto-negotiation on the selected interface. However, note that auto-negotiation cannot be disabled on the down-link ports. These ports are fixed at 1000 Mbit/sec, full duplex.
- When using the `negotiation` command to enable auto-negotiation, the optimal settings will be determined by the `capabilities` command. To set the speed or duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port NETP5 to 100 Mbit/sec, half-duplex operation.

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

Related Commands

`negotiation` (4-86)

`capabilities` (4-87)

4.3.8.4 negotiation

Use this command to enable auto-negotiation for a given interface. Use the `no` form to disable auto-negotiation.

Syntax

`negotiation`

`no negotiation`

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Down-link ports SNP0-15 are fixed with auto-negotiation disabled.
- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the `capabilites` command. When auto-negotiation is disabled, you must manually specify the link attributes with the `speed-duplex` and `flowcontrol` commands.
- If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the up-link ports. This means that you may have to use a cross-over cable to connect two switches. However, an alternative is to leave auto-negotiation enabled (this is the default setting) but reduce the subset of permitted modes to the single mode that you want to use.

Example

The following example configures port SNP11 to use auto-negotiation.

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

Related Commands

`capabilities` (4-87)

`speed-duplex` (4-85)

`flowcontrol` (4-89)

4.3.8.5 capabilities

Use this command to advertise the port capabilities of a given interface during auto-negotiation. Use the `no` form with parameters to remove an advertised capability, or the `no` form without parameters to restore the default values.

Syntax

`capabilities` {`1000full` | `100full` | `100half` | `10full` | `10half` | `flowcontrol` | `symmetric`}

`no port-capabilities` [`1000full` | `100full` | `100half` | `10full` | `10half` | `flowcontrol` | `symmetric`]

- `1000full` – Supports 1000 Mbit/sec full-duplex operation
- `100full` – Supports 100 Mbit/sec full-duplex operation
- `100half` – Supports 100 Mbit/sec half-duplex operation
- `10full` – Supports 10 Mbit/sec full-duplex operation
- `10half` – Supports 10 Mbit/sec half-duplex operation
- `flowcontrol` – Supports flow control
- `symmetric` (Gigabit only) – When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch ASIC only supports symmetric pause frames.)

Default Setting

NETMGT: `10half`, `10full`, `100half`, `100full`

NETP0-7: `10half`, `10full`, `100half`, `100full`, `1000full`, `flowcontrol`

SNP0-15: `1000full`

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- SNP0-15 down-link port capabilities are fixed at `1000full`.
- NETP0-7 up-link port capabilities include `10half`, `10full`, `100half`, `100full`, `1000full`, `flowcontrol` and `symmetric`. When auto-negotiation is enabled with the `negotiation` command, the switch negotiates the best settings for a link based on the `capabilites` command. When auto-negotiation is disabled, you must manually specify the link attributes with the `speed-duplex` and `flowcontrol` commands.
- NETMGT port capabilities are fixed at `10half`, `10full`, `100half`, `100full`.

Example

The following example configures port NETP5 capabilities to `100half`, `100full` and `flowcontrol`.

```
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)#
```

Related Commands

`negotiation` (4-86)

`speed-duplex` (4-85)

`flowcontrol` (4-89)

4.3.8.6 flowcontrol

Use this command to enable flow control. Use the `no` form to disable flow control.

Note – The integrated switches in the Sun Fire B1600 blade system chassis are each composed of two switch chips linked together. It is only possible to enable flow control between two ports on the same switch chip. The ports NETP0, NETP1, NETP4, NETP5, and SNP8 through SNP15 are on one switch chip. The ports NETP2, NETP3, NETP6, NETP7, and SNP0 through SNP7 are on the other. (If you look at the rear panel of the SSC, all the ports on the right are on one chip, and all the ports on the left are on the other.)

Syntax

`flowcontrol`

`no flowcontrol`

Default Setting

Flow control enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation.
- To force flow control on or off (with the `flowcontrol` or `no flowcontrol` command), use the `no negotiation` command to disable auto-negotiation on the selected interface.
- When using the `negotiation` command to enable auto-negotiation, the optimal settings will be determined by the `capabilities` command. To enable flow control under auto-negotiation, `flowcontrol` must be included in the `capabilities` list for any port.
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port NETP7.

```
Console(config)#interface ethernet NETP7
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

`negotiation` (4-86)

`capabilities` (flowcontrol, symmetric) (4-87)

4.3.8.7 shutdown

Use this command to disable an interface. To restart a disabled interface, use the no form.

Syntax

```
shutdown
no shutdown
```

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (for example, excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables Ethernet port SNP5.

```
Console(config)#interface ethernet SNP5
Console(config-if)#shutdown
Console(config-if)#
```

4.3.8.8 switchport broadcast packet-rate

Use this command to configure broadcast storm control. Use the no form to disable broadcast storm control.

Syntax

`switchport broadcast packet-rate` *rate*

`no switchport broadcast`

rate – The threshold level in packets per second. (Range: 16, 64, 128, 256)

Default Setting

Enabled for all ports

256 packets per second

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to the entire switch.
- Down-link ports SNP0-15 are fixed with broadcast storm control enabled.

Example

The following shows how to configure broadcast suppression at 64 packets per second:

```
Console(config)#interface ethernet SNP5
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#
```

Note – The `switchport broadcast` command enables broadcast storm control on the specified interface, but it sets the broadcast threshold for every interface on the switch.

4.3.8.9 clear counters

Use this command to clear statistics on an interface.

Syntax

`clear counters` *interface*

interface – `ethernet` *port-name*

port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port SNP5.

```
Console#clear counters ethernet SNP5
Console#
```

4.3.8.10 show interfaces status

Use this command to display the status for an interface.

Syntax

`show interfaces status` [*interface*]

interface

- `ethernet` *port-name*
- *port-name* – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT
- `port-channel` *channel-id* (Range: 1-6)
- `vlan` *vlan-id* (Range: 1-4094)

Default Setting

Shows status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status" on page 3-96.

Example

```
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

Use this command to display statistics for an interface.

Syntax

`show interfaces counters` [*interface*]

interface

- `ethernet` *port-name*

  port-name - down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

Shows counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port Statistics" on page 3-141.

Example

```
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

Use this command to display advanced interface configuration settings.

Syntax

`show interfaces switchport` [*interface*]

interface

- `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. The items displayed by this command include:

- Broadcast threshold – Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 4-91).
- Lacp status – Shows if Link Aggregation Control Protocol has been enabled or disabled (page 4-168).
- VLAN membership mode – Indicates membership mode as Trunk or Hybrid (page 4-123).
- Ingress rule – Shows if ingress filtering is enabled or disabled (page 4-125).
- Acceptable frame type – Shows if acceptable VLAN frames include all types or tagged frames only (page 4-124).
- Native VLAN – Indicates the default Port VLAN ID (page 4-126).
- Priority for untagged traffic – Indicates the default priority for untagged frames (page 4-151).
- Gvrp status – Shows if GARP VLAN Registration Protocol is enabled or disabled (page 4-132).
- Allowed Vlan – Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 4-127).
- Forbidden Vlan – Shows the VLANs this interface can not dynamically join through GVRP (page 4-129).

Example

This example shows the configuration setting for Ethernet port NETP7.

```
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 Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

TABLE 4-14 Address Table Commands

Command	Function	Mode	Page
`mac-address-table static`	Maps a static address to a port in a VLAN	GC	4-99
`clear mac-address-table dynamic`	Removes any learned entries from the forwarding database	PE	4-100
`show mac-address-table`	Displays entries in the bridge-forwarding database	PE	4-100
`mac-address-table aging-time`	Sets the aging time of the address table	GC	4-101
`show mac-address-table aging-time`	Shows the aging time for the address table	PE	4-102

4.3.9.1 mac-address-table static

Use this command to map a static address to a destination port. Use the `no` form to remove an address.

Syntax

`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 address.
- *interface*

  `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

  `port-channel` *channel-id* (Range: 1-6)
- *vlan-id* – VLAN ID (Range: 1-4094)
- *action*

  `permanent` – Assignment is permanent.

  `delete-on-reset` – Assignment lasts until switch is reset.

Default Setting

No static addresses are defined. The default mode is permanent.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses are not removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and are not moved. When a static address is seen on another interface, the address is ignored and is not written to the address table.

- A static address cannot be learned on another port until the address is removed with the `no` form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
interface ethernet SNP1 vlan 1 delete-on-reset
Console(config)#
```

4.3.9.2 clear mac-address-table dynamic

Use this command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

4.3.9.3 show mac-address-table

Use this command to view classes of entries in the bridge-forwarding database.

Syntax

`show mac-address-table` [`address` *mac-address* [*mask*]] [`interface` *interface*] [`vlan` *vlan-id*] [`sort` {`address` | `vlan` | `interface`}]

- *mac-address* – MAC address.

- *mask* – Bits to ignore in the address.
- *interface*

  `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

  `port-channel` *channel-id* (Range: 1-6)
- *vlan-id* – VLAN ID (Range: 1-4094)
- `sort` – Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The MAC Address Table contains the MAC addresses associated with each interface. Note that the `Type` field may include the following types:

- Learned – dynamic address entries
- Permanent – static entry
- Delete-on-reset – static entry to be deleted when system is reset

Example

```
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

Use this command to set the aging time for entries in the address table. Use the `no` form to restore the default aging time.

Syntax

`mac-address-table aging-time` *seconds*

`no mac-address-table aging-time`

seconds – The time is the number of seconds (18 to 2184).

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 300
Console(config)#
```

4.3.9.5 show mac-address-table aging-time

Use this command to show the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

4.3.10 Port Security Commands

These commands can be used to disable the learning function or manually specify secure addresses for a port. You might want to leave port security off for an initial training period (enable the learning function) to register all the current VLAN members on the selected port, and then enable port security to ensure that the port drops any incoming frames with a source MAC address that is unknown or has been previously learned from another port.

TABLE 4-15 Port Security Commands

Command	Function	Mode	Page
`port security`	Configures a secure port	IC	4-103
`mac-address-table static`	Maps a static address to a port in a VLAN	GC	4-99
`show mac-address-table`	Displays entries in the bridge-forwarding database	PE	4-100

4.3.10.1 port security

Use this command to configure a secure port. Use the `no` form to disable port security.

Syntax

`port security`

`no port security`

Default Setting

All port security is disabled.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If you enable port security, the switch stops dynamically learning new addresses on the specified port. Only incoming traffic with source addresses already stored in the dynamic or static address table are accepted.
- To use port security, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port.
- To add new VLAN members at a later time, you can manually add secure addresses with the `mac-address-table static` command, or turn off port security to reenable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.
- A secure port has the following restrictions:

  Cannot use port monitoring.

  Cannot be a multi-VLAN port.

  Cannot be connected to a network interconnection device.

  Cannot be a trunk port.

Example

The following example enables port security of port SNP5:

```
Console(config)#interface ethernet SNP5
Console(config-if)#port security
```

Related Commands

`mac-address-table static` (4-99)

`show mac-address-table` (4-100)

4.3.11 Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) for the overall switch, and commands that configure STA for the selected interface.

TABLE 4-16 Spanning Tree Commands

Command	Function	Mode	Page
`spanning-tree`	Enables the spanning tree protocol	GC	4-105
`spanning-tree mode`	Configures STP or RSTP mode	GC	4-106
`spanning-tree forward-time`	Configures the spanning tree bridge forward time	GC	4-107
`spanning-tree hello-time`	Configures the spanning tree bridge hello time	GC	4-108
`spanning-tree max-age`	Configures the spanning tree bridge maximum age	GC	4-109
`spanning-tree priority`	Configures the spanning tree bridge priority	GC	4-110
`spanning-tree path-cost method`	Configures the path cost method for RSTP	GC	4-111
`spanning-tree transmission-limit`	Configures the transmission limit for RSTP	GC	4-112
`spanning-tree cost`	Configures the spanning tree path cost of an interface	IC	4-112
`spanning-tree port-priority`	Configures the spanning tree priority of an interface	IC	4-114
`spanning-tree edge-port`	Enables fast forwarding for edge ports	IC	4-115
`spanning-tree protocol-migration`	Re-checks the appropriate BPDU format	PE	4-116
`spanning-tree link-type`	Configures the link type for RSTP	IC	4-117
`show spanning-tree`	Shows the spanning tree configuration	PE	4-118

4.3.11.1 spanning-tree

Use this command to enable the spanning tree algorithm globally for this switch. Use the `no` form to disable it.

Syntax

`spanning-tree`

`no spanning-tree`

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

The following example enables the spanning tree algorithm for this switch:

```
Console(config)#spanning-tree
Console(config)#
```

4.3.11.2 spanning-tree mode

Use this command to select the spanning tree mode for this switch. Use the `no` form to restore the default.

Syntax

`spanning-tree mode {stp | rstp}`

`no spanning-tree mode`

- `stp` – Spanning Tree Protocol (IEEE 802.1D)

- `rstp` – Rapid Spanning Tree Protocol (IEEE 802.1w)

Default Setting

`rstp`

Command Mode

Global Configuration

Command Usage

- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

4.3.11.3 spanning-tree forward-time

Use this command to configure the spanning tree bridge forward time globally for this switch. Use the `no` form to restore the default.

Syntax

`spanning-tree forward-time` *seconds*

`no spanning-tree forward-time`

seconds – The time in seconds. (Range: 4-30 seconds)

The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (that is, discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

4.3.11.4 spanning-tree hello-time

Use this command to configure the spanning tree bridge hello time globally for this switch. Use the `no` form to restore the default.

Syntax

`spanning-tree hello-time` *time*

`no spanning-tree hello-time`

time – Time in seconds. (Range: 1-10 seconds)

The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

4.3.11.5 spanning-tree max-age

Use this command to configure the spanning tree bridge maximum age globally for this switch. Use the `no` form to restore the default.

Syntax

`spanning-tree max-age` *seconds*

`no spanning-tree max-age`

seconds – The time in seconds. (Range: 6-40 seconds)

The minimum value is the higher of 6 or [2 x (hello-time + 1)].

The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it was a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

4.3.11.6 spanning-tree priority

Use this command to configure the spanning tree priority globally for this switch. Use the `no` form to restore the default.

Syntax

`spanning-tree priority` *priority*

`no spanning-tree priority`

priority – Priority of the bridge (0=highest, 61440=lowest).

(Range – 0 to 61,440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device (0=highest, 61440=lowest). However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

4.3.11.7 spanning-tree pathcost method

Use this command to configure the path cost method used for Rapid Spanning Tree. Use the `no` form to restore the default.

Syntax

`spanning-tree pathcost method {long | short}`

`no spanning-tree pathcost method`

- `long` – Specifies 32-bit based values that range from 1-200,000,000.
- `short` – Specifies 16-bit based values that range from 1-65535.

Default Setting

short method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 4-112) takes precedence over port priority (page 4-114).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

4.3.11.8 spanning-tree transmission-limit

Use this command to configure the minimum interval between the transmission of consecutive RSTP BPDUs. Use the no form to restore the default.

Syntax

`spanning-tree transmission-limit` *count*

`no spanning-tree transmission-limit`

count – The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

4.3.11.9 spanning-tree cost

Use this command to configure the spanning tree path cost for the specified interface. Use the no form to restore the default.

Syntax

`spanning-tree cost` *cost*

`no spanning-tree cost`

cost – The path cost for the interface.

(Range – 1-200,000,000) The recommended range is -

Ethernet: 200,000-20,000,000

Fast Ethernet: 20,000-2,000,000

Gigabit Ethernet: 2,000-200,000

Default Setting

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Path cost takes precedence over interface priority.
- When the spanning-tree pathcost method is set to `short`, the maximum value for path cost is 65,535.

Example

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

Related Commands

`spanning-tree port-priority` (4-114)

4.3.11.10 spanning-tree port-priority

Use this command to configure the priority for the specified interface. Use the `no` form to restore the default.

Syntax

`spanning-tree port-priority` *priority*

`no spanning-tree port-priority`

priority – The priority for an interface. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the spanning-tree algorithm. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) is configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

Related Commands

`spanning-tree cost` (4-112)

4.3.11.11 spanning-tree edge-port

Use this command to specify an interface as an edge port. Use the `no` form to restore the default.

Syntax

```
spanning-tree edge-port
no spanning-tree edge-port
```

Default Setting

NETP0-7, NETMGT: Disabled

SNP0-15: Enabled (fixed at this setting)

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

You can enable this option if an interface is attached to a LAN segment that is at the end of bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

Example

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

4.3.11.12 spanning-tree protocol-migration

Use this command to re-check the appropriate BPDU format to send on the selected interface.

Syntax

`spanning-tree protocol-migration` *interface*

interface

- `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the `spanning-tree protocol-migration` command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (RSTP or STP-compatible).

Example

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

4.3.11.13 spanning-tree link-type

Use this command to configure the link type for Rapid Spanning Tree. Use the `no` form to restore the default.

Syntax

`spanning-tree link-type {auto | point-to-point | shared}`

`no spanning-tree link-type`

- `auto` – Automatically derived from the duplex mode setting.
- `point-to-point` – Point-to-point link.
- `shared` – Shared medium.

Default Setting

`auto`

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden.

Example

```
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

Use this command to show the configuration for the spanning tree.

Syntax

`show spanning-tree` [*interface*]

interface

- `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the `show spanning-tree` command with no parameters to display the spanning tree configuration for the switch and for every interface in the tree.
- Use the `show spanning-tree` *interface* command to display the spanning tree configuration for an interface.
- For a description of the items displayed under `Spanning tree information`, see "Configuring Basic STA Settings" on page 3-70. For a description of the items displayed for specific interfaces, see "Managing Interfaces for Spanning Tree Algorithm" on page 3-125.

Example

```
Console#show spanning-tree
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                  :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 Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

TABLE 4-17 VLAN Commands

Command	Function	Mode	Page
Edit VLAN Groups			
`vlan database`	Enters VLAN database mode to add, change, and delete VLANs	GC	4-121
`vlan`	Configures a VLAN, including VID, name and state	VC	4-121
Configure VLAN Interfaces			
`interface vlan`	Enters interface configuration mode for a specified VLAN	GC	4-123
`switchport mode`	Configures VLAN membership mode for an interface	IC	4-123
`switchport acceptable-frame-types`	Configures frame types to be accepted by an interface	IC	4-124
`swicthport ingress-filtering`	Enables ingress filtering on an interface	IC	4-125
`switchport native vlan`	Configures the PVID (native VLAN) of an interface	IC	4-126
`switchport allowed vlan`	Configures the VLANs associated with an interface	IC	4-127
`switchport gvrp`	Enables GVRP for an interface	IC	4-132
`switchport forbidden vlan`	Configures forbidden VLANs for an interface	IC	4-129
Display VLAN Information			
`show vlan`	Shows VLAN information	NE, PE	4-130
`show interfaces status vlan`	Displays status for the specified VLAN interface	NE, PE	4-93
`show interfaces switchport`	Displays the administrative and operational status of an interface	NE, PE	4-96

4.3.12.1 vlan database

Use this command to enter VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the `show vlan` command.
- Use the `interface vlan` command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the `show running-config` command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

`show vlan` (4-130)

4.3.12.2 vlan

Use this command to configure a VLAN. Use the `no` form to restore the default settings or delete a VLAN.

Syntax

`vlan` *vlan-id* [`name` *vlan-name*] `media ethernet` [`state` {`active` | `suspend`}]

`no vlan` *vlan-id* [`name` | `state`]

- *vlan-id* – ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- `name` – Keyword to be followed by the VLAN name.

  vlan-name – ASCII string from 1 to 15 characters.
- `media ethernet` – Ethernet media type.
- `state` – Keyword to be followed by the VLAN state.
- `active` – VLAN is operational.
- `suspend` – VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- `no vlan` *vlan-id* deletes the VLAN.
- `no vlan` *vlan-id* `name` removes the VLAN name.
- `no vlan` *vlan-id* `state` returns the VLAN to the default state (active).
- VLAN 1 cannot be suspended, but any other VLAN can be suspended.
- You can configure up to 255 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

`show vlan` (4-130)

4.3.12.3 interface vlan

Use this command to enter interface configuration mode for VLANs, and configure a physical interface.

Syntax

`interface vlan` *vlan-id*

vlan-id – The ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

`shutdown` (4-91)

4.3.12.4 switchport mode

Use this command to configure the VLAN membership mode for a port. Use the `no` form to restore the default.

Syntax

`switchport mode {trunk | hybrid}`

`no switchport mode`

- `trunk` – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (associated with the PVID) are sent untagged.
- `hybrid` – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port SNP1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

4.3.12.5 switchport acceptable-frame-types

Use this command to configure the acceptable frame types for a port. Use the `no` form to restore the default.

Syntax

`switchport acceptable-frame-types {all | tagged}`

`no switchport acceptable-frame-types`

- `all` – The port accepts all frames, tagged or untagged.
- `tagged` – The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on SNP1 to tagged frames:

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

4.3.12.6 switchport ingress-filtering

Use this command to enable ingress filtering for an interface. Use the `no` form to restore the default.

Syntax

`switchport ingress-filtering`

`no switchport ingress-filtering`

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled, the interface accepts any VLAN-tagged frame if the tag matches a VLAN known to the switch (except for VLANs explicitly forbidden on this port).
- If ingress filtering is enabled, incoming frames tagged for VLANs that do not include this ingress port in their member set are discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port SNP1 and then enable ingress filtering:

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

4.3.12.7 switchport native vlan

Use this command to configure the PVID (default VID) for an interface. Use the `no` form to restore the default.

Syntax

`switchport native vlan` *vlan-id*

`no switchport native vlan`

vlan-id – The default VLAN ID for an interface. (Range: 1-4094, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to `all` or switchport mode is set to `hybrid`, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port SNP1 to VLAN 3:

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

4.3.12.8 switchport allowed vlan

Use this command to configure VLAN groups on the selected interface. Use the `no` form to restore the default.

Syntax

`switchport allowed vlan` {`add` *vlan* [`tagged` | `untagged`] | `remove` *vlan*}

`no switchport allowed vlan`

- `add` *vlan* – VLAN identifier to add.
- `remove` *vlan* – VLAN identifier to remove.

  Do not enter leading zeros. (Range: 1-4094)

Note – You cannot use the `no switchport allowed vlan` command on the NETMGT port. (If you do, the switch will display an error message.)

To restore the management port to its factory-default VLAN (VLAN 2) and remove it from any other VLANs you have added it to, type the following commands:

```
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
```

where *vlan id* is the number of a VLAN other than VLAN 2 to which you have added NETMGT. (Repeat the last command for every VLAN other than VLAN 2 for which NETMGT is still a member.)

Default Setting

- All ports (except NETMGT) are assigned to VLAN 1 by default.
- NETMGT is assigned to VLAN 2 by default..
- The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If switchport mode is set to `trunk`, then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The `tagged` or `untagged` parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port SNP1:

```
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

Use this command to configure forbidden VLANs. Use the `no` form to remove the list of forbidden VLANs.

Syntax

`switchport forbidden vlan` {`add` *vlan* | `remove` *vlan*}

`no switchport forbidden vlan`

- `add` *vlan* – VLAN ID to add.
- `remove` *vlan* – VLAN ID to remove.

  Do not enter leading zeroes. (Range: 1-4094)

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface through GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port SNP1 from being added to VLAN 3:

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

4.3.12.10 show vlan

Use this command to show VLAN information.

Syntax

`show vlan` [`id` *vlan-id* | `name` *vlan-name*]

- `id` – Keyword to be followed by the VLAN ID.

  vlan-id – ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

- `name` – Keyword to be followed by the VLAN name.

  vlan-name – ASCII string from 1 to 15 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1:

```
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 and Bridge Extension Commands

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

TABLE 4-18 GVRP and Bridge Extension Commands

Command	Function	Mode	Page
Interface Commands			
`switchport gvrp`	Enables GVRP for an interface	IC	4-132
`switchport forbidden vlan`	Configures forbidden VLANs for an interface	IC	4-129
`show gvrp configuration`	Displays GVRP configuration for selected interface	NE, PE	4-132
`garp timer`	Sets the GARP timer for the selected function	IC	4-133
`show garp timer`	Shows the GARP timer for the selected function	NE, PE	4-135
Global Commands			
`bridge-ext gvrp`	Enables GVRP globally for the switch	GC	4-135
`show bridge-ext`	Shows bridge extension configuration	PE	4-136

4.3.13.1 switchport gvrp

Use this command to enable GVRP for a port. Use the `no` form to disable it.

Syntax

```
switchport gvrp
no switchport gvrp
```

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport gvrp
Console(config-if)#
```

4.3.13.2 show gvrp configuration

Use this command to show if GVRP is enabled or disabled.

Syntax

`show gvrp configuration` [*interface*]

interface

- `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration
Whole system:
GVRP configuration: Enabled
SNP0:
 Gvrp configuration: Enabled
SNP1:
 Gvrp configuration: Enabled
.
.
.
```

4.3.13.3 garp timer

Use this command to set the values for the join, leave and leaveall timers. Use the `no` form to restore the timers' default values.

Syntax

`garp timer` {`join` | `leave` | `leaveall`} *timer_value*

`no garp timer` {`join` | `leave` | `leaveall`}

- {`join` | `leave` | `leaveall`} - The timer to set.
- *timer_value* - Value of timer.

  Range:

  `join`: 20-1000 centiseconds

  `leave`: 60-3000 centiseconds

  `leaveall`: 500-18000 centiseconds

Default Setting

- `join`: 20 centiseconds
- `leave`: 60 centiseconds
- `leaveall`: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol (GARP) is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:

  leave >= (2 x join)

  leaveall > leave

Note – Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP will not operate successfully.

Example

```
Console(config)#interface ethernet SNP1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

`show garp timer` (4-135)

4.3.13.4 show garp timer

Use this command to show the GARP timers for the selected interface.

Syntax

`show garp timer` [*interface*]

interface

- `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet SNP1
SNP1 GARP timer status:
 Join timer: 20 sec.
 Leave timer: 60 sec.
 Leaveall timer: 1000 sec.
Console#
```

Related Commands

`garp timer` (4-133)

4.3.13.5 bridge-ext gvrp

Use this command to enable GVRP globally for the switch. Use the `no` form to disable it.

Syntax

```
bridge-ext gvrp
no bridge-ext gvrp
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

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

4.3.13.6 show bridge-ext

Use this command to show the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The meanings of items displayed by this command are as follows:

- Max support vlan numbers – The VLAN version used by the switch as specified in the IEEE 802.1Q standard.
- Max support vlan ID – Maximum VLAN ID recognized by the switch.
- Extended multicast filtering services – The switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- Static entry individual port – The switch allows static filtering for unicast and multicast addresses (page 4-99 and 4-140).
- VLAN learning – The switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- Configurable PVID tagging – The switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port (page 4-126).
- Local VLAN capable – This item refers to the support provided by the switch for Multiple Spanning Tree. At present, Multiple Spanning Tree is not supported.
- Traffic classes – The switch provides mapping of user priorities to multiple traffic classes (page 4-153).
- Global GVRP status – GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLAN groups which extend beyond the local switch (page 4-135).
- GMRP – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Example

```
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 Snooping Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it continues to receive the multicast service.

TABLE 4-19 IGMP Snooping Commands

Command	Function	Mode	Page
Basic IGMP Commands			
`ip igmp snooping`	Enables IGMP snooping	GC	4-139
`ip igmp snooping vlan static`	Adds an interface as a member of a multicast group	GC	4-140
`ip igmp snooping version`	Configures the IGMP version for snooping	GC	4-141
`show ip igmp snooping`	Shows the IGMP snooping configuration	PE	4-142
`show bridge multicast`	Shows the IGMP snooping MAC multicast list	PE	4-143
IGMP Querier Commands			
`ip igmp snooping querier`	Allows this device to act as the querier for IGMP snooping	GC	4-144
`ip igmp snooping query-count`	Configures the query count	GC	4-144

TABLE 4-19 IGMP Snooping Commands *(Continued)*

Command	Function	Mode	Page
`ip igmp snooping query-interval`	Configures the query interval	GC	4-145
`ip igmp snooping query-max-response-time`	Configures the report delay	GC	4-146
`ip igmp snooping router-port-expire-time`	Configures the query timeout	GC	4-147
`show ip igmp snooping`	Shows the IGMP snooping configuration	PE	4-142
Multicast Router Commands			
`ip igmp snooping vlan mrouter`	Adds a multicast router port	GC	4-148
`show ip igmp snooping mrouter`	Shows multicast router ports	PE	4-149

4.3.14.1 ip igmp snooping

Use this command to enable IGMP snooping on this switch. Use the `no` form to disable it.

Syntax

```
ip igmp snooping
no ip igmp snooping
```

Default Setting

Disabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

4.3.14.2 ip igmp snooping vlan static

Use this command to add a port to a multicast group. Use the `no` form to remove the port.

Syntax

`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 (Range: 1-4094)
- *ip-address* - IP address for multicast group
- *interface*

  `ethernet` *port-name*

  port-name - down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

  `port-channel` *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Global Configuration

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet SNP5
Console(config)#
```

4.3.14.3 ip igmp snooping version

Use this command to configure the IGMP snooping version. Use the `no` form to restore the default.

Syntax

`ip igmp snooping version {1 | 2}`

`no ip igmp snooping version`

- `1` – IGMP Version 1
- `2` – IGMP Version 2

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
- Some commands are only enabled for IGMPv2, including `ip igmp query-max-response-time` and `ip igmp query-timeout`.

Example

The following configures the switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

4.3.14.4 show ip igmp snooping

Use this command to show the IGMP snooping configuration.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See "Configuring IGMP Snooping Parameters" on page 3-55 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
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

Use this command to show known multicast addresses.

Syntax

`show mac-address-table multicast` [`vlan` *vlan-id*] [`user` | `igmp-snooping`]

- *vlan-id* – VLAN ID (1 to 4094)
- `user` – Display only the user-configured multicast entries.
- `igmp-snooping` – Display only entries learned through IGMP snooping.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include `IGMP` or `USER`, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for bridge group 1, VLAN 1:

```
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

Use this command to enable the switch as an IGMP snooping querier. Use the `no` form to disable it.

Syntax

`ip igmp snooping querier`

`no ip igmp snooping querier`

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

4.3.14.7 ip igmp snooping query-count

Use this command to configure the query count. Use the `no` form to restore the default.

Syntax

`ip igmp snooping query-count` *count*

`no ip igmp snooping query-count`

count - The maximum number of queries issued for which there has been no response before the querier takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by `ip igmp snooping query-max-response-time`. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

`ip igmp snooping query-max-response-time` (4-146)

4.3.14.8 ip igmp snooping query-interval

Use this command to configure the snooping query interval. Use the `no` form to restore the default.

Syntax

`ip igmp snooping query-interval` *seconds*

`no ip igmp snooping query-interval`

seconds – The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

4.3.14.9 ip igmp snooping query-max-response-time

Use this command to configure the snooping report delay. Use the `no` form of this command to restore the default.

Syntax

`ip igmp snooping query-max-response-time` *seconds*

`no ip igmp snooping query-max-response-time`

seconds – The report delay advertised in IGMP queries. (Range: 5-25)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the `ip igmp snooping query-count`, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time
20
Console(config)#
```

Related Commands

`ip igmp snooping version` (4-141)

`ip igmp snooping query-max-response-time` (4-146)

4.3.14.10 ip igmp snooping router-port-expire-time

Use this command to configure the snooping query-timeout. Use the `no` form of this command to restore the default.

Syntax

`ip igmp snooping router-port-expire-time` *seconds*

`no ip igmp snooping router-port-expire-time`

seconds – The time the switch waits after the previous querier stops querying before it considers the interface (which had been receiving query packets) to no longer be attached to a querier. (Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the timeout to 500 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 500
Console(config)#
```

Related Commands

`ip igmp snooping version` (4-141)

4.3.14.11 ip igmp snooping vlan mrouter

Use this command to statically configure a multicast router port. Use the `no` form to remove the configuration.

Syntax

`ip igmp snooping vlan` *vlan-id* `mrouter` *interface*

`no ip igmp snooping vlan` *vlan-id* `mrouter` *interface*

- *vlan-id* – VLAN ID (Range: 1-4094)
- *interface*

  `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

  `port-channel` *channel-id* (Range: 1-6)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0
Console(config)#
```

4.3.14.12 show ip igmp snooping mrouter

Use this command to display information on statically configured and dynamically learned multicast router ports.

Syntax

`show ip igmp snooping mrouter` [`vlan` *vlan-id*]

vlan-id – VLAN ID (Range: 1-4094)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include `Static` or `Dynamic`.

Example

The following shows the ports attached to multicast routers:

```
Console#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1               NETP5  Static
    2               NETP6  Dynamic
Console#
```

4.3.15 Priority Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports COS with four priority queues for each port. Data packets in a port's high-priority queue are transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

TABLE 4-20 Priority Commands

Command	Function	Mode	Page
Layer 2 Priority Commands			
`switchport priority default`	Sets a port priority for incoming untagged frames	IC	4-151
`queue bandwidth`	Assigns round-robin weights to the priority queues	GC	4-152
`queue cos map`	Assigns class-of-service values to the priority queues	IC	4-153
`show queue bandwidth`	Shows round-robin weights assigned to the priority queues	PE	4-155
`show queue cos-map`	Shows the class-of-service map	PE	4-156

TABLE 4-20 Priority Commands *(Continued)*

Command	Function	Mode	Page
`show interfaces switchport`	Displays the administrative and operational status of an interface	PE	4-96
Layer 3 and 4 Priority Commands			
`map ip precedence`	Enables IP precedence class-of-service mapping	GC	4-157
`map ip precedence`	Maps IP precedence value to a class of service	IC	4-158
`map ip dscp`	Enables IP DSCP class-of-service mapping	GC	4-159
`map ip dscp`	Maps IP DSCP value to a class of service	IC	4-160
`show map ip precedence`	Shows the IP precedence map	PE	4-161
`show map ip dscp`	Shows the IP DSCP map	PE	4-162

4.3.15.1 switchport priority default

Use this command to set a priority for incoming untagged frames, or the priority of frames received by the device connected to the specified interface. Use the `no` form to restore the default value.

Syntax

`switchport priority default` *default-priority-id*

`no switchport priority default`

default-priority-id – The priority number for untagged ingress traffic.

The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits are used.
- This switch provides four priority queues for each port. It is configured to use Weighted Round Robin, which can viewed with the `queue bandwidth` command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags are placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port SNP3 to 5:

```
Console(config)#interface ethernet SNP3
Console (config-if)#switchport priority default 5
```

4.3.15.2 queue bandwidth

Use this command to assign weighted round-robin (WRR) weights to the four class-of-service (COS) priority queues. Use the `no` form to restore the default weights.

Syntax

`queue bandwidth` *weight1...weight4*

`no queue bandwidth`

weight1...weight4 – The ratio of weights for queues 0 to 3 determines the weights used by the WRR scheduler. (Range: 1-255)

Default Setting

Weights 16, 64, 128 and 240 are assigned to queue 0, 1, 2 and 3 respectively.

Command Mode

Global Configuration

Command Usage

WRR allows bandwidth sharing at the egress port by defining scheduling weights.

Example

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the COS priority queues 0, 1, 2 and 3:

```
Console(config)#queue bandwidth 1 3 5 7
Console(config)#
```

Related Commands

`show queue bandwidth` (4-155)

4.3.15.3 queue cos-map

Use this command to assign class-of-service (COS) values to the COS priority queues. Use the `no` form to set the COS map to the default values.

Syntax

`queue cos-map` *queue_id* [*cos1 ... cosn*]

`no queue cos-map`

- *queue_id* – The queue id of the CoS priority queue.

  Ranges are 0 to 3, where 3 is the highest CoS priority queue.

- *cos1 .. cosn* – The CoS values that are mapped to the queue id. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using four priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

TABLE 4-21 IEEE 802.1p Default Priority Recommendations

	Queue			
Priority	**0**	**1**	**2**	**3**
0		•		
1	•			
2	•			
3		•		
4			•	
5			•	
6				•
7				•

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

COS assigned at the ingress port is used to select a COS priority at the egress port.

Example

The following example shows how to map COS values 0, 1 and 2 to COS priority queue 0, value 3 to COS priority queue 1, values 4 and 5 to COS priority queue 2, and values 6 and 7 to COS priority queue 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)#
```

Related Commands

`show queue cos-map` (4-156)

4.3.15.4 show queue bandwidth

Use this command to display the weighted round-robin (WRR) bandwidth allocation for the four class-of-service (COS) priority queues.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
    0        16
    1        64
    2        128
    3        240
Console#
```

4.3.15.5 show queue cos-map

Use this command to show the class-of-service priority map.

Syntax

`show queue cos-map` [*interface*]

interface

- `ethernet` *port-name*

  port-name - down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
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 (Global Configuration)

Use this command to enable IP precedence mapping (IP Type of Service). Use the no form to disable IP precedence mapping.

Syntax

```
map ip precedence
no map ip precedence
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types automatically disables the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

4.3.15.7 map ip precedence (Interface Configuration)

Use this command to set IP precedence priority (IP Type of Service priority). Use the `no` form to restore the default table.

Syntax

`map ip precedence` *ip-precedence-value* `cos` *cos-value*

`no map ip precedence`

precedence-value – 3-bit precedence value. (Range: 0-7)

cos-value – Class-of-Service value (Range: 0-7)

Default Setting

One-to-one mapping (Precedence value 0 maps to COS value 0, and so forth)

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults.
- Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes apply to all interfaces on the switch.

Example

The following example shows how to map IP precedence value 1 to COS value 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 (Global Configuration)

Use this command to enable IP DSCP mapping (Differentiated Services Code Point mapping). Use the no form to disable IP DSCP mapping.

Syntax

```
map ip dscp
no map ip dscp
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types automatically disables the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

4.3.15.9 map ip dscp (Interface Configuration)

Use this command to set IP DSCP priority (Differentiated Services Code Point priority). Use the `no` form to restore the default table.

Syntax

`map ip dscp` *dscp-value* `cos` *cos-value*

`no map ip dscp`

- *dscp-value* – 8-bit DSCP value. (Range: 0-255)
- *cos-value* – Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to COS value 0.

TABLE 4-22 Default DSCP to COS Mapping

IP DSCP Value	COS Value
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

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Precedence or IP DSCP, and default switchport priority.

- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then mapped to the queue defaults.
- Mapping specific values for DSCP is implemented as an interface configuration command, but any changes apply to all interfaces on the switch.

Example

The following example shows how to map IP DSCP value 1 to COS value 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

Use this command to show the IP precedence priority map.

Syntax

`show map ip precedence` [*interface*]

interface

- `ethernet` *port-name*

  port-name - down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
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#
```

Related Commands

`map ip precedence (Global Configuration)` (4-157)

`map ip precedence (Interface Configuration)` (4-158)

4.3.15.11 show map ip dscp

Use this command to show the IP DSCP priority map.

Syntax

`show map ip dscp` [*interface*]

interface

- `ethernet` *port-name*

  port-name - down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

- `port-channel` *channel-id* (Range: 1-6)

Default Setting

None

Command Mode

Privileged Exec

Example

```
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#
```

Related Commands

map ip dscp (Global Configuration) (4-159)

map ip dscp (Interface Configuration) (4-160)

4.3.16 Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

TABLE 4-23 Mirror Port Commands

Command	Function	Mode	Page
`port monitor`	Configures a mirror session	IC	4-164
`show port monitor`	Shows the configuration for a mirror port	PE	4-165

4.3.16.1 port monitor

Use this command to configure a mirror session. Use the `no` form to clear a mirror session.

It is only possible to monitor one port on the switch at a time.

Note – The integrated switches on the Sun Fire B1600 blade system chassis are each composed of two switch chips linked together. It is only possible to mirror the traffic on one port by using another port that is on the same switch chip. The ports NETP0, NETP1, NETP4, NETP5, and SNP8 through SNP15 are on one switch chip. The ports NETP2, NETP3, NETP6, NETP7, and SNP0 through SNP7 are on the other. (If you look at the rear panel of the SSC, all the ports on the right are on one chip, and all the ports on the left are on the other.)

Syntax

`port monitor` *interface* [`rx | tx | both`]

`no port monitor` *interface*

- *interface* – `ethernet` *port-name*

  port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT
- `rx` – Mirror received packets.
- `tx` – Mirror transmitted packets.
- `both` – Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from a source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.

Example

The following example mirrors all packets from port SNP6 to port NETP2:

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6 both
Console(config-if)#
```

Related Commands

`show port monitor` (4-165)

4.3.16.2 show port monitor

Use this command to display mirror information.

Syntax

`show port monitor` [*interface*]

interface – `ethernet` *port-name*

port-name – down link: SNP0-15; up link: NETP0-7; mgt: NETMGT

Default Setting

Shows all sessions

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (RX, TX, RX/TX).

Example

The following shows mirroring configured from port SNP6 to port NETP2:

```
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#
```

Related Commands

`port monitor` (4-164)

4.3.17 Link Aggregation Commands

Ports can be statically grouped into an aggregated link to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to negotiate a dynamic aggregated link between this switch and another network device. For static aggregated links, the switches connected to must be of the same type. But for dynamic aggregated links, the switches simply have to comply with LACP. This switch supports up to six

aggregated links. For example, an aggregated link consisting of two 1000 Mbit/sec ports can support an aggregate bandwidth of 4 Gbit/sec when operating at full duplex.

TABLE 4-24 Link Aggregation Commands

Command	Function	Mode	Page
Manual Configuration Commands			
`interface port-channel`	Configures an aggregated link and enters interface configuration mode for the aggregated link	GC	4-83
`channel-group`	Adds a port to an aggregated link	IC	4-167
Dynamic Configuration Command			
`lacp`	Configures LACP for the current interface	IC	4-168
Aggregated link Status Display Command			
`show interfaces status port-channel`	Shows information about a particular aggregated link.	NE, PE	4-93

Guidelines for Creating Aggregated Links

- Finish configuring aggregated links before you connect the corresponding network cables between switches to avoid creating a loop.
- An aggregated link can contain up to four up-link ports or up to two down-link ports.
- The ports at both ends of a connection must be configured as aggregated link ports.
- All ports in an aggregated link must be configured in an identical manner, including communication mode (that is, speed, duplex mode and flow control), VLAN assignments, and COS settings.
- All the ports in an aggregated link have to be treated as a whole when moved from or to, or added or deleted from a VLAN through the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire aggregated link through the specified port-channel.

4.3.17.1 channel-group

Use this command to add a port to a static aggregated link. Use the `no` form to remove a port from a static aggregated link.

Syntax

`channel-group` *channel-id*

`no channel-group`

channel-id – The port-channel index (Range: 1-6)

Default Setting

The current port will be added to this aggregated link.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static aggregated links, you can only link switches of the same type.
- Use `no channel-group` to remove a port group from an aggregated link.
- Use `no interfaces port-channel` to remove an aggregated link from the switch.

Example

The following example creates aggregated link 1 and then adds port 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

Use this command to enable 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the `no` form to disable it.

Syntax

```
lacp
no lacp
```

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an aggregated link must be configured for full duplex, either by forced mode or auto-negotiation.
- An aggregated link formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the aggregated link will be activated automatically.
- If more than four ports attached to the same target switch have LACP enabled, the additional ports are placed in standby mode, and are only enabled if one of the active links fails.

Example

The following shows LACP enabled on ports NETP0 to NETP2. Because LACP has also been enabled on the ports at the other end of the links, the `show interfaces status port-channel 1` command shows that port-channel 1 has been established.

```
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#
```

APPENDIX **A**

Management Information Base

An SNMP management station can configure and monitor network devices by setting or reading device variables specified in the Management Information Base (MIB). The key MIB groups supported by the switch are listed in this appendix. Also, note that specific MIB variables used for each configuration task are listed in Chapter 3, "General Management of the Switch."

This appendix contains the following sections:

A.1 Supported MIBs

The standard MIBs are listed in the following table.

TABLE A-1 Supported MIBs

RFC No.	Title	Supported Groups
1213	MIB-II	• system group • interfaces group • ip group • icmp group • tcp group • udp group • snmp group
1493	Bridge MIB	• dot1dBase group • dot1dStp group • dot1dTp group • dot1dStatic group
2863	Interfaces Evolution MIB	• ifXTable group • ifStackTable group
2819	RMON MIB	• statistics group • history group • alarm group • event group
2618	RADIUS MIB	• radiusAuthClientMIB
2665	Etherlike MIB	• dot3StatsTable group
2737	Entity MIB	• entityPhysical group
2674	P-bridge	• dot1dExtBase group • dot1dPriority group • dot1dGarp group
2674	Q-bridge	• dot1qBase group • dot1qTp group • dot1qStatic group • dot1qVlan

The Sun private enterprise MIB is listed below.

TABLE A-2 Sun Private Enterprise MIB

Title	Version
CSSP.MIB	01.00.00

A.2 Supported Traps

SNMP traps supported include the following items:

TABLE A-3 SNMP Traps

RFC No.	Title
RFC 1215 (SNMPv1), RFC 1907 (SNMPv2c)	• coldStart • linkDown • linkUp • authenticationFailure
RFC 1493	• newRoot • topologyChange
RFC 2819	• risingAlarm • fallingAlarm

Sun private enterprise traps supported include the following item:

TABLE A-4 Sun Private Enterprise Traps

RFC No.	Title
CSSP.MIB	• swPowerStatusChangeTrap

APPENDIX **B**

Troubleshooting

If you are having problems connecting to the network, check your network cabling to ensure that the device in question is properly connected to the network. Then see "Diagnosing Switch Indicators" on page B-2 to verify that the corresponding port on the switch is functioning properly.

If you are having problems connecting to the management interface, see the troubleshooting chart under "Accessing the Management Interface" on page B-2.

This appendix contains the following sections:

B.1 Diagnosing Switch Indicators

If you have a connected a device to a port on the switch, but the Link LED is off, then check the following items:

- Be sure the cable is plugged into both the switch and corresponding device.
- Verify that the proper cable type is used and its length does not exceed specified limits.
- Check the adapter on the connected device and cable connections for possible defects. Replace the defective adapter or cable if necessary.

Verify that all system components have been properly installed. If any network cabling appears to be malfunctioning, test it in an alternate environment where you are sure that all the other components are functioning properly.

B.2 Diagnosing Port Connections

If a port does not work, check the following:

- The cable connections are secure and the cables are connected to the correct ports at both ends of the link.
- The port status (Admin) is enabled, and the auto-negotiation feature is enabled, or the ports at both ends of the link are configured to the same speed and duplex mode. See "Port Configuration" on page 3-96 for more information.

B.3 Accessing the Management Interface

You can access the management interface for the switch from anywhere within the connected network using Telnet, a Web browser, or any SNMP-based network management software. If you are having trouble accessing the management interface, see the troubleshooting information displayed below.

If you cannot connect using Telnet, a Web browser, or SNMP software, check the following:

- Be sure the system chassis is powered up.
- Check the network cabling between the management station and the switch.

- Check that you have a valid network connection to the switch and that the port you are using has not been disabled. See "Port Configuration" on page 3-96.
- If there are only Layer 2 switches between the management station and system chassis, make sure that:
  - The switch's management VLAN is configured with a valid IP address and subnet mask.
  - The management station has an IP address in the same subnet as the management VLAN.
  - The management station is connected to a switch port that is a member of the management VLAN.
  - The ports connecting intermediate switches in the network are tagged ports and are a member of the management VLAN.
- If there are one or more Layer 3 switches between the management station and system chassis, make sure that:
  - The switch's management VLAN is configured with a valid IP address, subnet mask, and default gateway.
  - The management station has valid IP address, subnet mask, and default gateway.
  - The management station is connected to a switch port that is a member of the management VLAN.
  - The ports connecting intermediate switches and the Layer 3 switch(es) in the network are tagged ports and are a member of the management VLAN.
- If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet sessions permitted. Try connecting again at a later time.

If you cannot access the command-line interface through a serial port connection, check the following:

- Use the DB-9-to-RJ-45 cable supplied with the Sun Fire B1600 blade system chassis to connect your terminal or computer to the serial port on the SSC module.
- Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps.

B.4 Using System Logs

If a fault does occur, refer to the other manuals for the system chassis to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. **Enable logging.**
2. **Set the error messages reported to include all categories.**
3. **Designate the SNMP host that is to receive the error messages.**
4. **Repeat the sequence of commands or other actions that lead up to the error.**
5. **Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.**
6. **Contact customer service.**

Example

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 10.1.0.23
.
.
.
```

B.4.1 Log Messages

Log messages generated by this switch are listed in the following table:

TABLE B-1 Log Messages

Message	Description	Level[3]
System coldStart notification	Switch cold boot	5
System warmStart notification	Switch warm boot	5
Unit 1 Port YY[1] link-up notification	Port link up	6
Unit 1 Port YY link-down notification	Port link down	6
Trunk 1 link-up notification	Aggregated link up	6

TABLE B-1 Log Messages

Message	Description	Level[3]
Trunk 1 link-down notification	Aggregated link down	6
VLAN XX[2] link-up notification	VLAN link up	6
VLAN XX link-down notification	VLAN link down	6
Authentication failure notification	SNMP access authentication failure	6
STA root change notification	STA root change	6
STA topology change notification	STA topology change	6
RMON rising alarm notification	RMON rising alarm	6
RMON falling alarm notification	RMON falling alarm	6

1 Indicates unit 1, port YY (YY: 1 to 25).

2 Indicates a VLAN ID value (XX: 1 to 4094).

3 Syslog message level (See "logging history" on page 4-35.)

B.5 Error Messages

B.5.1 Command-Line Error Detection

If the switch detects invalid input in the command line, it displays a ^ beneath the location where the error was detected. For example:

```
Console#show interfaces statuss e 1/1
                                  ^
% Invalid input detected at '^' marker.
```

B.5.2 System Errors

The key error messages generated by the switch are listed in the following table. To control the message levels issued by the switch, see "logging history" on page 4-35.

TABLE B-2 System Error Messages

Message	Description	Level[3]
module[1] create task fail.	Specified software module cannot create the task.	2
module task idle too long.	Specified software module stayed in idle state too long.	2
Allocate *string*[2] memory fail.	Allocate memory failed for specified *String*.	2
Free *string* memory fail.	Free memory failed for specified *String*.	2
string switch to default.	Specified value is invalid or not supported; the default value will be used. (Please refer to the on-line help or this manual for information on acceptable values.)	3

1 Indicates the switch software module (for example, STA, VLAN, XFER, TRAP, or RMON).

2 Indicates the value specified for a configuration setting.

3 The syslog message level. (See "logging history" on page 4-35.)

B.5.3 Command Line Errors

The error messages generated by the switch for the command-line interface are listed in the following table. Note that these messages are not written to the log file.

TABLE B-3 Command Line Error Messages

Message	Description
`Ambiguous command:` *string*[1]	Ambiguous command.
`Clear dynamic address error.`	Cannot clear dynamic address.
`CLI internal error - contact your local service provider.`	CLI command internal error.
`Copy error.`	Copy failed.
`Exec-timeout could not be disabled for vty session.`	Telnet session cannot disable exec-timeout.
`Factory default configuration file cannot be deleted.`	Factory default file cannot be deleted.
`Factory default configuration file cannot be replaced.`	Factory configuration file cannot be replaced.
`Failed to allocate resource.`	Not enough resources.

TABLE B-3 Command Line Error Messages *(Continued)*

Message	Description
`Failed to get` *string*	Show command failed.
`Failed to set` *string*	Configuration command failed.
`Failed to write certificate file to flash.`	Certificate file has an error, private key file error (such as incorrect pass phrase), or private key does not match the certificate public key.
`Incomplete command.`	Incomplete command.
`Insufficient memory.`	Not enough memory.
`Insufficient memory to display or save running config.`	Not enough space to collect all information.
`Invalid file name.`	Invalid filename input.
`Invalid input.`	Wrong keyboard input.
`Invalid input detected at '^' marker.`	Invalid command.
`Invalid parameter.`	Ping parameter is wrong.
`Invalid parameter value/range. Type "?" to get more detail information.`	Value or character string length is not allowed.
`Invalid TFTP server IP address.`	TFTP IP address error.
`Not enough resources; please try later.`	Ping function has no resources.
`No such file.`	System does not have the file.
`No such VLAN.`	VLAN does not exist.
`Port` *port name* `does not exist.`	The port name does not exist.
`Port` *port name* `is an ethernet port.`	Port is an Ethernet port.
`Port` *port name* `is not present.`	The port is not present when entering interface mode.
`Port` *port name* `unknown.`	Port is an unknown port.
`Session terminated.`	CLI exited the current session.
`Session timed out.`	Connect session timed out.
`Startup file cannot be deleted.`	Startup file cannot be deleted.

TABLE B-3 Command Line Error Messages *(Continued)*

Message	Description
`This command for console only.`	Line mode (vty) can not use console parameter commands.
`This command is only valid for adding a single port to a an aggregated link.`	Only one port can be added to an aggregated link with this command.
`This command is only valid for the name of a single port.`	When setting the port description, multi-port selection is not accepted.
`This command is not supported for management port in current release.`	The “no switchport allow vlan” command cannot be used for the management port.
`Trunk ID: `*`trunk`*` is out of range.`	Trunk id is not allowed.
`Trunk `*`trunk`*` does not exist.`	This trunk does not exist.
`Trunk `*`trunk`*` is a normal trunk.`	This trunk is a normal trunk.
`Trunk with no members cannot be displayed.`	Trunk member cannot be configured or displayed.
`Type "show ?" for a list of subcommands.`	You only input the “show” command.
`Unknown error.`	Unknown error.
`Unrecognized command.`	Unrecognized command.

1 Indicates the value specified for a command.

B.5.4 Web Interface Errors

The error messages generated by this switch for the Web interface are listed in the following table. Note that these messages are not written to the log file.

TABLE B-4 Web Interface Error Messages

Menu	Message	Description
Switch Setup		
System Identity	User privileges are not enough to perform this operation.	Privileges insufficient.
Network Identity	Current IP Address Mode is not DHCP or BOOTP.	When restarting DHCP, the switch must be in DHCP or BOOTP mode.
	Data is invalid.	General error.
	Set DHCP Client-ID error.	Failed to set DHCP client ID.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Software	Data is invalid.	General error.
	Please input a destination file.	Input a destination file name to download or upload.
	Please input a source file.	Input a source file name to download or upload
	Please input or select a destination file.	Input or select a file name for downloading or uploading.
	Please select a file.	Select a file to download or upload.
	System will be restarted...	System will be restarted.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Switch Config		
Security	Cannot add user.	User name is invalid or maximum number of users has been exceeded.
	Cannot set password for user.	Password is invalid.
	Cannot set user privilege.	There is a problem with the user table.
	Cannot set user status.	There is a problem with the user table.
	User does not exist.	There is a problem with the user table.
Communication	Community String cannot contain spaces.	Community string cannot contain spaces.
	Community table is full or data is invalid.	Community table is full or data is invalid.

TABLE B-4 Web Interface Error Messages *(Continued)*

Menu	Message	Description
	Data is invalid.	General error.
	Illegal SNMP trap IP address.	Illegal IP address format.
	Please select a Community String.	Select a community string to remove.
	Please type a Community String.	Type a community string to add.
	Trap Manager table is full or data is invalid.	Trap Manager table is full or data is invalid
	User privileges are not enough to perform this operation.	Privileges insufficient.
	You must specify an IP trap community string.	Type an IP trap community string to add.
Security	Authentication type doesn't exist.	One of Local, TACACS or RADIUS authentication type is not supported.
	Data is invalid	General error.
	Illegal IP address.	IP address format is illegal.
	Number of Server Transmits is out of range.	RADIUS retransmits number is out of range.
	Password too long.	Maximum password length exceeded.
	Please input username.	Input a user name to add a new user.
	Please select an user	Select a user to remove or change password.
	RADUIS KEY is invalid	RADIUS encryption key is invalid.
	Server Port Number is out of range.	RADIUS port number is out of range.
	Select a privilege level.	Select privilege level to add a user.
	TACACS PORT is invalid	TACACS port is invalid.
	TACACS KEY is invalid	TACACS key is invalid.
	Timeout is out of range.	RADIUS timeout is out of range.
	User privileges are not enough to perform this operation.	Privileges insufficient.
VLAN	Cannot create VLAN.	VLAN ID invalid, or maximum number of supported VLANs has been exceeded.
	Cannot set VLAN name.	VLAN name invalid.
	Cannot set VLAN status.	Cannot disable VLAN 1 or the VLAN defined as the native VLAN (PVID) for the mangement port.
	Cannot delete VLAN.	Cannot delete VLANs with members or any VLAN defined as the native VLAN (PVID) for an interface.

TABLE B-4 Web Interface Error Messages *(Continued)*

Menu	Message	Description
	Data is invalid	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Membership	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Broadcast & Multicast		
Broadcast Parameters	Threshold is out of range.	Maximum broadcast storm threshold level exceeded.
	User privileges are not enough to perform this operation.	Privileges insufficient.
IGMP Parameters	Please enter a valid version.	Enter a valid version.
	Query count is out of range.	Query count is out of range
	Query interval is out of range.	Query interval is out of range.
	Query timeout is out of range.	Query timeout is out of range.
	Report delay is out of range.	Report delay is out of range.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Multicast Router Ports	Data is invalid.	General error.
	Please select a port	Select ports to add(remove) to(from) multicast router.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Multicast Services	Data is invalid.	General error.
	Igmp group member is null.	Select IGMP group member from list.
	Illegal IP address.	IP address format is illegal.
	Select a port or aggregated link	Select ports to add(remove) to(from) static ports on VLAN.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Spanning Tree		
Basic Configuration	Data is invalid.	General error.
	Priority is out of range.	Priority is out of range.
	User privileges are not enough to perform this operation.	Privileges insufficient.

TABLE B-4 Web Interface Error Messages *(Continued)*

Menu	Message	Description
Advanced Configuration	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Class of Service		
Basic Traffic Prioritisation	Cos Value is out of range.	CoS Value is out of range.
	Data is invalid.	General error.
	Priority is out of range.	Priority is out of range.
	Queue weight must be in a order of Q0<=Q1<=Q2<=Q3	Invalid Queue weight.
	Traffic Class is out of range.	Traffic Class is out of range.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Layer 3/4 Traffic Prioritisation	Cos Value is out of range.	CoS Value is out of range.
	Please select IP Precedence or DSCP mode	Select one of these options when priority service is enabled.
	Traffic Class is out of range.	Traffic Class is out of range.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Address Tables	Aging time is out of range.	Maximum address aging time exceeded.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Up Links, Down Links		
Status	Cannot set port capabilities.	Incorrect speed/duplex mode for specified port.
	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Link Aggregation	Cannot add aggregated link. The specified aggregated link is full or data is invalid.	The specified aggregated link is full or data is invalid.
	Cannot create aggregated link.	Maximum number of aggregated links has been exceeded.
	Cannot remove aggregated link.	There is a problem with the aggregated link table.
	Cannot remove member of aggregated link. Data is invalid.	There is a problem with the aggregated link table.

TABLE B-4 Web Interface Error Messages *(Continued)*

Menu	Message	Description
	Cannot set aggregated link status.	Cannot enable LACP for a static member of an aggregated link.
	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
VLANs	Data is invalid.	General error.
	Please enter a valid PVID.	PVID is invalid. Select a correct one.
	Please enter a valid timer.	Timer is invalid. Select a correct one.
	Table is full or data is invalid.	Table is full or data is invalid.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Address Filtering	Data is invalid.	General error.
	Please enter a valid MAC address.	Invalid MAC address.
	Please enter a valid VLAN ID.	VLAN ID is invalid.
	Table is full or data is invalid.	Table is full or data is invalid.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Spanning Tree	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Config	Path cost is out of range.	Path cost is out of range.
	Priority is out of range.	Priority is out of range.
Port	Path cost is out of range.	Path cost is out of range.
	Priority is out of range.	Priority is out of range.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Management Ports		
VLANs	Data is invalid.	General error.
	Please enter a valid PVID.	PVID is invalid. Select a correct one.
	Please enter a valid timer.	Timer is invalid. Select a correct one.
	Table is full or data is invalid.	Table is full or data is invalid.
	User privileges are not enough to perform this operation.	Privileges insufficient.

TABLE B-4 Web Interface Error Messages *(Continued)*

Menu	Message	Description
Packet Filtering	User privileges are not enough to perform this operation.	Privileges insufficient.
Monitoring		
Port Mirroring	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.
Logs	Data is invalid.	General error.
	User privileges are not enough to perform this operation.	Privileges insufficient.

APPENDIX **C**

Specifications

This appendix contains the following sections:

C.1 Switch Architecture

TABLE C-1 Switch Architecture

Item	Specifications
Ports	• Network up links - 8 1000BASE-T • Midplane - 16 Gigabit serialized down links (for server Blades) • Management channel - 1 10/100BASE-TX, 1 console port (serial RJ-45)
Network Interface	• 10/100/1000Base-T Ports NETP0-7: RJ-45 connector, auto-negotiation, auto MDI/MDI-X • Cabling: 10BASE-T: 100-ohm, UTP cable; Categories 3, 4, 5 100BASE-TX: 100-ohm, UTP cable; Category 5 1000BASE-T: 100-ohm, UTP cable; Category 5 or 5e
Buffer Architecture	Up-link and down-link ports: 1 Mbyte shared
Aggregate Bandwidth	48 Gbps
Switching Database	32K MAC address entries
LEDs	• SSC: Active, Service Required, Ready to Remove • Ethernet Ports: Link/Active, Speed

C.2 Management Features

TABLE C-2 Management Features

Item	Specifications
In-Band Management	Telnet, Web-based HTTP, or SNMP
Out-of-Band Management	RS-232 signaling over RJ-45 console port
Software Loading	TFTP in-band or XModem out-of-band
MIB Support	• SNMP v1/v2 (RFC 1215, 1907) • MIB II (RFC 2863) • Bridge MIB (RFC 1493) • Etherlike MIB (RFC 1643/2665) • RMON (RFC 2819 groups 1,2,3,9) • IEEE 802.1Q VLAN (RFC 2674) • IEEE 802.3ad LACP, private MIB
RMON Support	Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)
Additional Features	• Aggregated links (Static and LACP) • Port Mirroring • Port Security • RADIUS Authentication Client

C.3 Physical

TABLE C-3 Physical Specifications

Item	Specifications
Weight	2.08 kg (4.59 lbs)
Size	27.5 x 20.3 x 4.3 cm (10.8 x 8.0 x 1.7 in.)

C.4 Power

TABLE C-4 Power Specifications

Item	Specifications
Operating Voltage	+12 VDC
Maximum Current	5.2 A
Power Consumption	62 Watts maximum
Heat Dissipation	211 BTU/hr maximum

C.5 Environmental

TABLE C-5 Environmental Specifications

Item	Specifications
Temperature	• Operating: 5 to 45 ˚C (41 to 113 ˚F) • Storage: -40 to 70 ˚C (-40 to 158 ˚F)
Humidity	Operating: 10% to 90% (non-condensing)

C.6 Standards

TABLE C-6 Supported Standards

Standard	Description
IEEE 802.3	Ethernet
IEEE 802.3u	Fast Ethernet
IEEE 802.3ab	Gigabit Ethernet
IEEE 802.1D	Spanning Tree Protocol and traffic priorities
IEEE 802.1w	Rapid Reconfiguration (STP)
IEEE 802.1p	Priority tags
IEEE 802.1Q	VLANs
IEEE 802.3ac	VLAN tagging

TABLE C-6 Supported Standards *(Continued)*

Standard	Description
IEEE 802.3x	full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ad	Link Aggregation Control Protocol
RFC 1215, 1907	SNMP
RFC 2819	RMON (groups 1,2,3,9)
RFC 2863	MIB II
RFC 1493	Bridge MIB
RFC 1643, 2665	Etherlike MIB
RFC 826	ARP
RFC 1112	IGMP
RFC 792	ICMP

Glossary

10BASE-T	IEEE 802.3 specification for 10 Mbit/sec Ethernet over two pairs of Category 3, 4, or 5 UTP cable.
100BASE-TX	IEEE 802.3u specification for 100 Mbit/sec Fast Ethernet over two pairs of Category 5 UTP cable.
1000BASE-T	IEEE 802.3ab specification for Gigabit Ethernet over two pairs of Category 5, 5e 100-ohm UTP cable.
1000BASE-X	IEEE 802.3 shorthand term for any 1000 Mbit/sec Gigabit Ethernet based on 8B/10B signaling.
Bandwidth	The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.
Bandwidth Utilization	The historical percentage of packets received as compared to total bandwidth.
BOOTP	Boot protocol used to load the operating system for devices connected to the network.
Auto-negotiation	Signalling method allowing each node to select its optimum operational mode (for example, 10, 100, or 100 Mbit/sec and half or full duplex) based on the capabilities of the node to which it is connected.
Collision	A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible. This only applies to half-duplex connections.
Collision Domain	Single CSMA/CD LAN segment.
CSMA/CD	Carrier Sense Multiple Access/Collision Detect is the communication method employed by Ethernet and Fast Ethernet.

Dynamic Host Control Protocol (DHCP) — Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

End Station — A workstation, server, or other device that does not act as a network interconnection.

Ethernet — A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

Fast Ethernet — A 100 Mbit/sec network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex — Transmission method that allows switch and network card to transmit and receive concurrently, effectively doubling the bandwidth of that link.

GARP VLAN Registration Protocol (GVRP) — Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP) — GARP is a protocol that can be used by end stations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered end stations. Formerly called Group Address Registration Protocol.

Gigabit Ethernet — A 1000 Mbit/sec network communication system based on Ethernet and the CSMA/CD access method.

Group Attribute Registration Protocol — *See Generic Attribute Registration Protocol.*

IEEE 802.1D — Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q — VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign end stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p — An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1w	An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which is designed to supersede IEEE 802.1D. RSTP provides considerably faster convergence for topology changes.
IEEE 802.3	Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
IEEE 802.3ab	Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Fast Ethernet.
IEEE 802.3ac	Defines frame extensions for VLAN tagging.
IEEE 802.3u	Defines CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet.
IEEE 802.3x	Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.
IEEE 802.3z	Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet.
IGMP Snooping	Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.
Internet Control Message Protocol (ICMP)	Commonly used to send echo messages (Ping) for monitoring purposes.
Internet Group Management Protocol (IGMP)	A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the "querier" and assumes responsibility for keeping track of group membership.
In-Band Management	Management of the network from a station attached directly to the network.
IP Multicast Filtering	A process whereby this switch can pass multicast traffic along to participating hosts.
LAN Segment	Separate LAN or collision domain.
LED	Light emitting diode used for monitoring a device or network condition.
Link Segment	Length of twisted-pair or fiber cable joining a pair of repeaters or a repeater and a PC.
Local Area Network (LAN)	A group of interconnected computer and support devices.

Layer 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation Defines a network link aggregation method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Link Aggregation Control Protocol (LACP) Allows ports to automatically negotiate an aggregated link with LACP-configured ports on another device.

Media Access Control (MAC) A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

Management Information Base (MIB) An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

Multicast Switching A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Out-of-Band Management Management of the network from a station not attached to the network.

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Remote Monitoring (RMON) RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Remote Authentication Dial-in User Service (RADIUS) An authentication protocol that uses a central server to control access to RADIUS-compliant devices on the network. A RADIUS server can be programmed with a database of multiple user name/password pairs and associated privilege levels for each user or group that requires management access to this switch.

RJ-45 Connector A connector for twisted-pair wiring.

Shielded Twisted Pair (STP) **Cable** — Twisted-pair wire covered with an external aluminum-foil or woven copper shield designed to reduce excessive noise pick up or radiation.

Simple Network Management Protocol (SNMP) — The application protocol in the Internet suite of protocols which offers network management services.

Spanning Tree Protocol (STP) — A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Switched Ports — Ports that are on separate collision domains or LAN segments.

Terminal Access Controller Access Control System (TACACS) — An authentication protocol that uses a central server to control access to TACACS-compliant devices on the network. A TACACS server can be programmed with a database of multiple user name/password pairs and associated privilege levels for each user or group that requires management access to this switch.

Telnet — Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Transmission Control Protocol/Internet Protocol (TCP/IP) — Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP) — A TCP/IP protocol commonly used for software downloads.

Unshielded Twisted Pair (UTP) **Cable** — Cable composed of two insulated wires twisted together to reduce electrical interference; used in common telephone cord.

Virtual LAN (VLAN) — A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XModem — A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index

T

U

V

W