VERTICAL HORIZON
VH-2402S2 / VH-2402SM2
FAST ETHERNET SWITCH

Configuration Guide

9033820-03

ENTERASYS NETWORKS™

ELECTRICAL HAZARD: Only qualified personnel should perform installation procedures.

NOTICE

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810

Printed in Taiwan.

Order Number: 9033820-03 March 2004

TABLE OF CONTENTS

1. MANAGEMENT OVERVIEW

Configuration Options

IMPORTANT NOTICE: The information contained in this guide applies to both the VH-2402S2 and VH-2402S products.

IMPORTANT NOTICE: The VH-2402S2 (or VH-2402S) switch requires a VH-SMGMT2 Management Module to be installed with a minimum firmware version of 2.6.

For advanced management capability, the VH-SMGMT2 Vertical Horizon Management Module provides a menu-driven system configuration program. This program can be accessed by a direct connection to the serial port on the Management Module (out-of-band), or by a Telnet connection over the network (in-band).

The Management Module is based on SNMP (Simple Network Management Protocol). This SNMP agent permits a switch stack to be managed from any PC in the network using in-band management software.

The Management Module also includes an embedded HTTP Web agent. This Web agent can be accessed using a standard Web browser from any computer attached to the network. Refer to the Web Management Guide for more information.

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

- Enable/disable any port
- Set the communication mode for any port
- Configure SNMP parameters
- Select RMON options
- Display system information or statistics
- Configure the switch to join a Spanning Tree
- Download system firmware
- Restart the system

Backup Management Agent

Note the following points about master and backup management agents:

- The VH-SMGMT2 with software version 02.06.00.00 supports a stack master management agent and a backup management agent. The agent with the lower stack ID will be the master. Every 5 minutes the master agent downloads the entire configuration data to the backup agent. Any configuration changes made to the master agent will be synchronized incrementally with the backup agent as they occur.
- Up to a maximum of two Management Modules (one master and one back-up), may exist within a stackable configuration, which may consist of up to seven switches in a stack.
- The Management Modules (master or backup) cannot be “hot” inserted. The “hot” removal of the master or the backup Management Module will cause system instability and will require a manual reboot of the entire stack.
- The master management agent (version 02.06.00.00 or greater) will synchronize the system software with that of the backup management. This ensures that the backup agent always contains the same version of software as the master agent. The system software synchronization is performed as a background task, requiring 10 minutes for the master agent to download the software to the backup agent. The stack continues to operate while the backup agent reboots after loading the software code.
- Upon the failure or “hot” removal of the master Management Module within a stackable configuration, the following occurs:
  - A “Trap” is sent, a “Log event” is logged, the switch is re-booted and the backup Management Module takes over without loss of configuration settings.
  - The fail-over time of master management to that of the backup management in a medium-size stackable configuration is approximately 2 minutes. Consequently, network traffic is disrupted during the fail-over period.
  - The backup management’s “Backup Master” state changes to a “Master” state and the switch Unit IDs will also reflect the new change.
  - All ports will still be active and the switch will continue forwarding traffic in a normal operative manner.
  - If a Management Module were to be re-installed, the newly-installed Management Module would assume the role of “Master” agent with the incumbent one changing status to that of “Backup Master” agent.
  - If you need to replace a failed master Management Module, you can retain all configuration settings by moving the backup agent module to the location of the failed master agent. A new Management Module can then be installed in the location of former backup agent.

Closed-Loop Stack

The VH-2402S2 switches can be stacked together by installing optional Stacking Modules. The VH-STACK2 Stacking Module allows you to configure a closed-loop architecture that provides fault-tolerant operation of the stack. If a switch or stacking module fails, or if a stacking cable is disconnected, the entire stack will reboot and will subsequently resume normal operation and managment via the redundant stacking cable (closed loop). Also, any changes to the stack including powering down of a unit or the insertion of a unit will cause the stack to reboot.

NOTE: A VH-STACK2 Stacking Module must be installed with the master Management Module in Unit 1 only. If backup management is used in conjunction with the closed-loop feature, the backup Management Module must be installed in Unit 2.

NOTE: The stack will re-number itself if a unit in the closed-loop stack fails.

Required Connections

Console Port (Out-of-Band) Connections

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the Management Module. Use the null-modem cable provided with this package, or use a null-modem connection that is compatible with the console port pin assignments shown in Appendix A of the VH-2402S2 Hardware Installation Guide.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 19200 bps (for initial configuration). Also be sure to set flow control to “none.” (Refer to “Configuring the Serial Port” on page 21 for a complete description of configuration options.)

In-Band Connections

Prior to accessing the Management Module via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using an out-of-band connection or the BootP protocol.

Telnet Connection

After configuring the switch's IP parameters, you can use a Telnet connection to access the on-board configuration program from anywhere within the attached network.

Use the Network Configuration menu to specify the maximum number of simultaneous Telnet sessions that are supported by the system.

In-Band Network Connection

The on-board configuration program can be accessed using Telnet from any computer attached to the network. The switch and stack can also be managed by any computer using a Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above), or from a network comput using network management software.

2. VH-2402S2 USER INTERFACE

Overview

Access is gained to the console menus by connecting a terminal to the console port (with a direct cable connection), or using Telnet to access the Management Module over the network. These menus allow you to reconfigure the switch, as well as to monitor the status and performance of the switch or the attached stack. The menus have a layout similar to the sample Main Menu shown in Figure 2-1. The information is divided into the following parts:

- Menu Name (includes access privileges)
- Selectable Items
- Screen Prompt for menu selections and entry of field parameters, and Message Area for display of parameters or error messages.

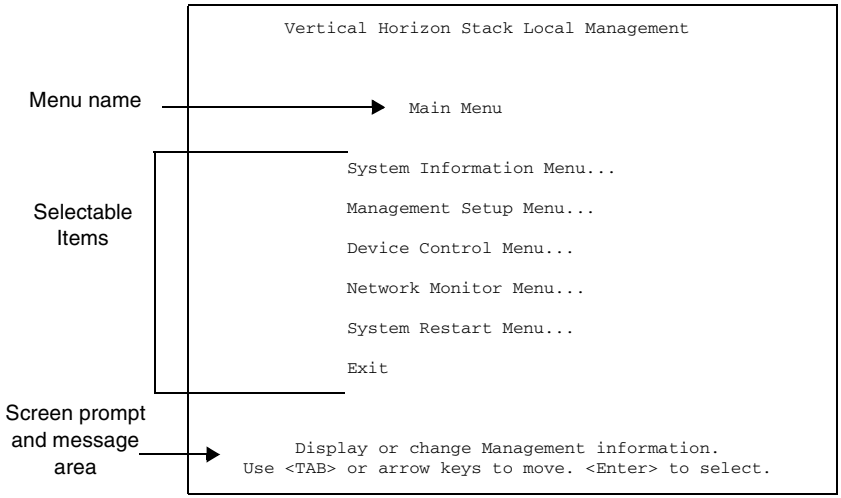

Figure 2-1. Sample Main Menu

User Access

Once a direct connection to the serial port or a Telnet connection is established, the login screen for the on-board configuration program appears. You may need to press Enter a few times to display the screen.

The default user names are “admin” and “guest,” with no passwords. The administrator has Read/Write access, which allows you to read and modify switch information. The guest has Read Only access to the management program, which allows you to view switch information, but not modify any operating parameters.

You should define a new administrator password, record it and put it in a safe place. From the Main Menu, select Management Setup Menu / Console Login Configuration, and enter a new password for the default administrator. Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

NOTE: A user is allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

To use the console menus, do the following:

1. Use the cursor keys to highlight the desired option.

   If the selected item is a submenu title, the submenu is displayed when you press the Enter key.

2. Follow the screen prompts to specify the parameter requested.

   If the selected item is a parameter, the system displays a prompt for you to enter a new value. If the value entered is invalid, a message displays, requesting you to enter a valid value.

Factory Defaults

Table 2-1 lists the default settings for switch configuration parameters. Each parameter can be changed via the console menus or Telnet.

Table 2-1. Factory Default Settings

Parameter	Default Value
Multicast Filtering	
GMRP	Disabled
IGMP Multicast Filtering	Disabled
Port Configuration	
Flow Control	Disabled
Speed and Duplex	Auto
Admin	Enabled
Broadcast Storm Control	Disabled - 200 pps
Port Priority	
Default Ingress User Priority	0
Spanning Tree Algorithm	
Active Aging Time	300
Bridge Priority	32768
Forward Delay	15
Hello Time	2
Max Age	20
Path Cost	4 - 1000Mbps ports 19 - 100Mbps ports 100 - 10Mbps ports
Port Priority	128
Spanning Tree Protocol	Enabled
Spanning Tree Fast Forwarding 10/100 Mbps ports	Enabled
System Configuration	
Management VLAN	All
BootP Enable	Disabled
Password	<none>
Screen Timeout	10 min
Send Authentication Fail Traps	Enabled
SNMP Community Name	public, private

Parameter	Default Value
Terminal Baud Rate	Auto
User Names	admin, guest
Virtual LANs	
Acceptable VLAN Frame Type	All
Configurable PVID Tagging	Yes
GVRP	Disabled
Untagged VLAN Group Assignment	1
VLAN Ingress Filtering	False
VLAN Learning	SVL

Main Menu

The Main Menu is the first screen seen after successfully logging into the system. Figure 2-2 shows the Main Menu and the accompanying table describes the Main Menu.

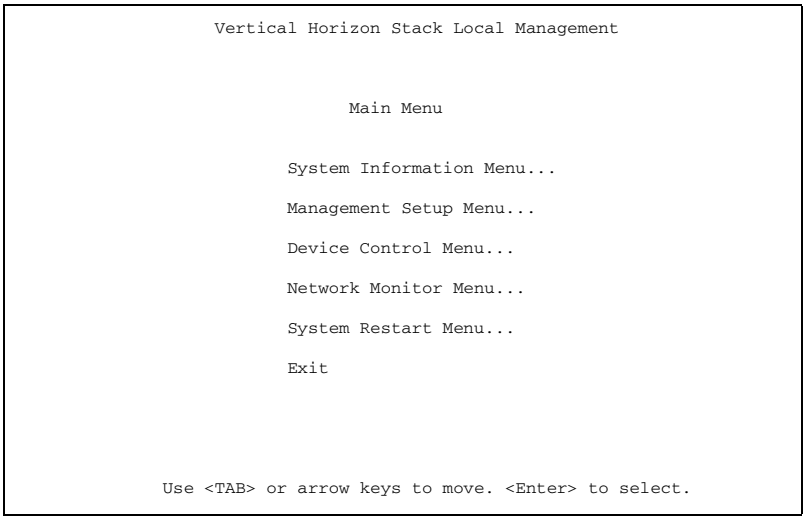

Figure 2-2. Main Menu

Selection	Description
System Information Menu	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the stack.
Stacking Information	Shows information on the closed-loop stacking status.
Management Setup Menu	
Network Configuration	Includes IP setup, Ping facility, HTTP (Web agent) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; and configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download Agent F/W	Downloads new version of firmware to update your system (in-band).
Configuration Save & Restore	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration.

Selection	Description
Management Configuration	Specifies if management access to the switch is available from all VLANs or restricted to one VLAN.
Device Control Menu	
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Port Information	Displays operational status, including link state, flow control method, and duplex mode.
Port Security Configuration	Allows you to enable and configure port security for the switch.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
Extented Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, GMRP multicast filtering, and VLAN extensions.
Spanning Tree Configuration	Enables Spanning Tree Algorithm; also sets parameters for hello time, maximum message age, switch priority, and forward delay; as well as port priority and path cost.
Spanning Tree Information	Displays full listing of parameters for the Spanning Tree Algorithm.
Mirror Port Configuration	Sets the source and target ports for mirroring.
BStorm Control Configuration	Allows you to enable broadcast storm control and set the packet-per-second threshold.
Global VLAN Configuration	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported, and allows you to enable/disable each VLAN.
Port Assignment VLAN Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and 802.1Q trunks.
Egress Ports VLAN Configuration	Configures VLAN groups via static assignments to individual ports or a range of ports, including setting ports as members and configuring them as untagged.
VLAN Forbidden Ports Configuration	Restricts individual ports or a range of ports from being dynamically added to a VLAN by the GVRP protocol.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members, or restricting ports from being dynamically added to a VLAN by the GVRP protocol.
802.1P Configuration	Configures default port priorities and queue assignments.
IGMP Configuration	Configures IGMP multicast filtering.
IGMP Member Port Configuration	Assigns ports that are attached to hosts who want to receive a specific multicast service.
Multicast Router Port Configuration	Displays the ports on the switch attached to a neighboring multicast router/switch for each VLAN ID.

Selection	Description
Network Monitor Menu	
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full address listing, as well as search and clear functions.
IP Multicast Registration Table	Displays all the multicast groups active on this switch, including multicast IP addresses and corresponding VLAN IDs.
Static Unicast Address Table Configuration	Used to manually configure host MAC addresses in the unicast table.
System Restart	Restarts system with options to use POST, or to retain factory defaults, IP settings, or user authentication settings.
Exit	Exits the configuration program.

System Information Menu

Use the System Information Menu to display a basic description of the switch, including contact information, and hardware/firmware versions.

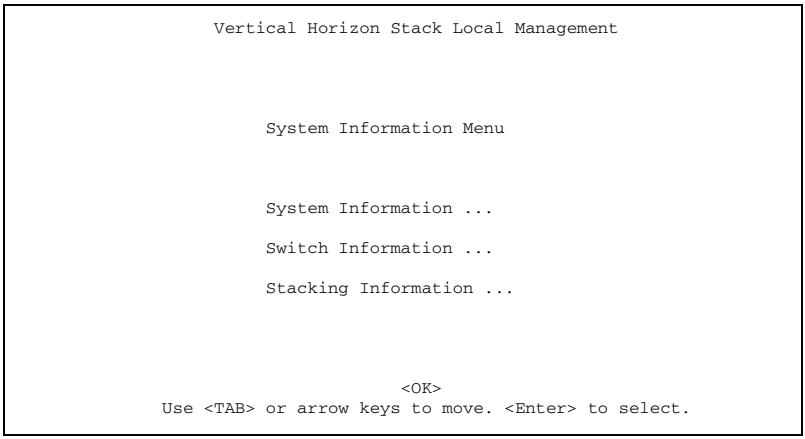

Figure 2-3. System Information Menu

Selection	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the stack.
Stacking Information	Shows the status of closed-loop stacking.

Displaying System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.

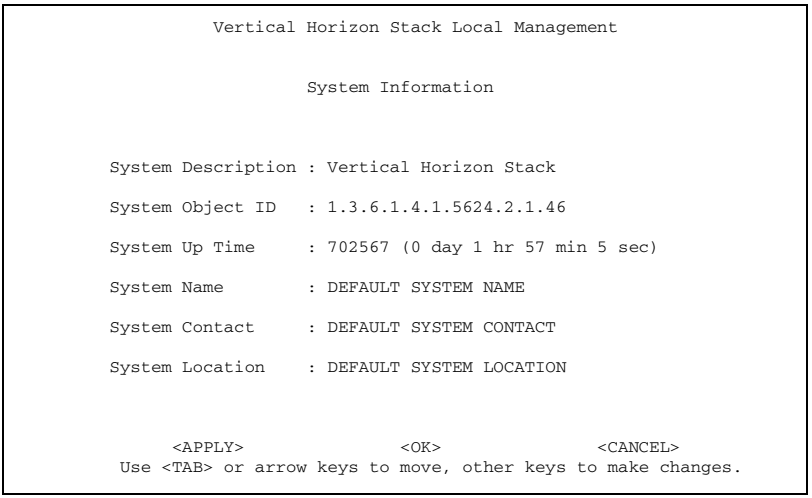

Figure 2-4. System Information

Parameter	Description
System Description	System hardware description.
System Object ID	MIB II object identifier for switch's network management subsystem.
System Up Time	Length of time the current management agent has been running. (Note that the first value is 1/100 seconds.)
System Name*	Name assigned to the switch system.
System Contact*	Contact person for the system.
System Location*	Specifies the area or location where the system resides.

*** Maximum string length is 255, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.**

Displaying Switch Version and Module Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board and agent module, as well as the power status and modules plugged into the system.

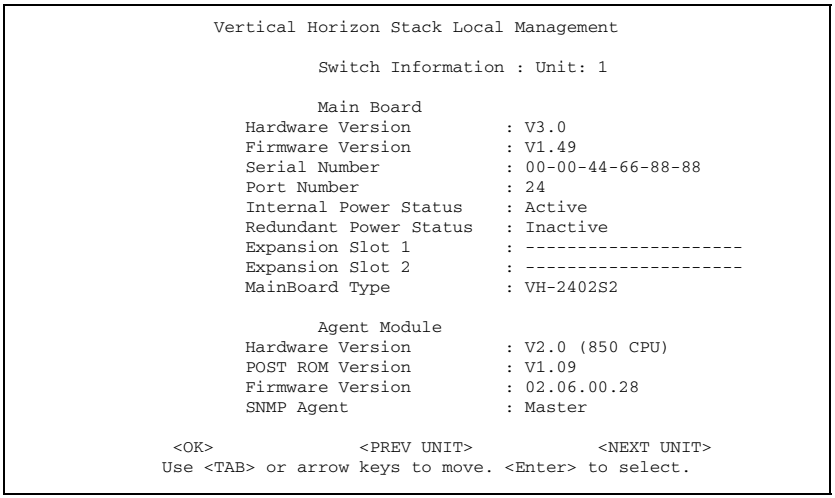

Figure 2-5. Switch Information

Parameter	Description
Main Board	
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	MAC address associated with the main board.
Port Number	Number of ports in this unit.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.
Expansion Slot 1	Shows module type if inserted (100Base-FX, 1000Base-SX, 1000Base-LX, 1000Base-T, or GBIC).
Expansion Slot 2.	Shows module type if inserted (100Base-FX, 1000Base-SX, 1000Base-LX, 1000Base-T, GBIC, or Stacking).
MainBoard Type	Indicates if the switch is a VH-2402S2 or VH-2402S.
Agent Module	
Hardware Version	Hardware version of the agent module.
POST ROM Version	Power-On Self-Test version number.
Firmware Version	Firmware version of the agent module.
SNMP Agent	Shows if this module is Master or Backup Master.

Displaying Stacking Information

Use the Stacking Information screen to display information about the state of a closed-loop switch stack.

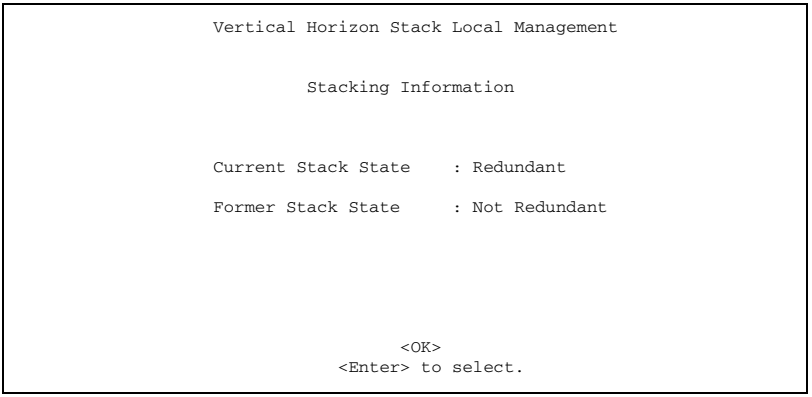

Figure 2-6. System Information

Parameter	Description
Current Stack State	Indicates the current state of a redundant closed-loop stacking.
Former Stack State	Indicates the last previous state of a redundant closed-loop stack.

Management Setup Menu

After initially logging onto the system, adjust the communication parameters for your console to ensure a reliable connection (Serial Port Configuration). Specify the IP addresses for the agent module (Network Configuration / IP Configuration), and then set the Administrator and User passwords (Console Login Configuration). Remember to record them in a safe place. Also set the community string which controls access to the on-board SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.

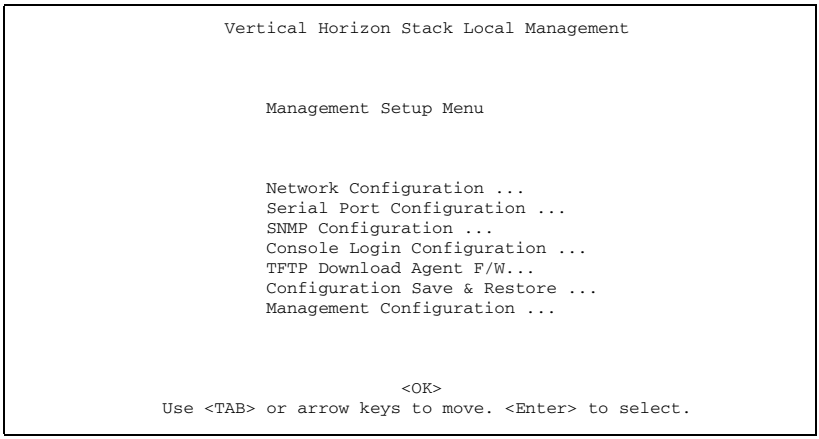

Figure 2-7. Management Setup Menu

Selection	Description
Network Configuration	Includes IP setup, Ping facility, HTTP (Web agent) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; and configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download Agent F/W	Downloads new version of firmware to update your Management Module system (in-band).
Configuration Save & Restore	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration.
Management Configuration	Specifies if management access to the switch is available from all VLANs or restricted to one VLAN.

Changing the Network Configuration

Use the Network Configuration menu to set the bootup option, configure the switch's Internet Protocol (IP) parameters, enable the on-board Web agent, or to set the number of concurrent Telnet sessions allowed. The screen shown below is described in the following table.

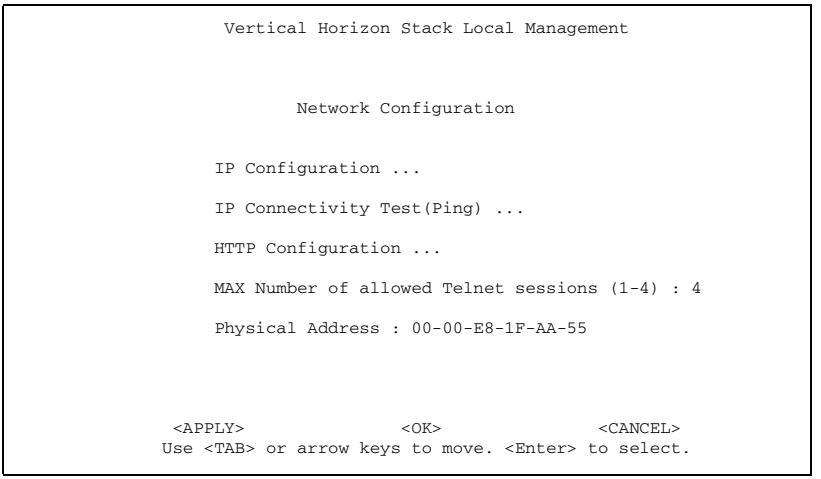

Figure 2-8. Network Configuration

Parameter	Description
IP Configuration	Screen used to set the bootup option, or configure the switch's IP parameters.
IP Connectivity Test	Screen used to test IP connectivity to a (Ping) specified device.
HTTP Configuration	Screen used to enable the Web Agent.
MAX Number of Allowed Telnet Sessions	The maximum number of Telnet sessions allowed to simultaneously access the agent module.
MAC Address	Physical address of the agent module.

IP Configuration

Use the IP Configuration screen to set the bootup option, or configure the switch's IP parameters. The screen shown below is described in the following table.

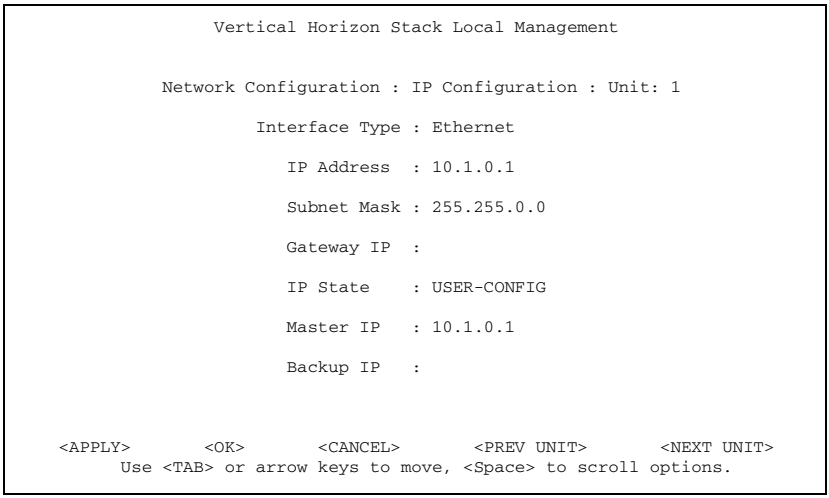

Figure 2-9. IP Configuration

Parameter	Default	Description
Interface Type	Ethernet	Indicates IP over Ethernet.
IP Address	10.1.0.1	IP address of the stack you are managing when accessing the agent module over the network. The agent module supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module (or running management software) must have an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.0.0	Subnet mask of the agent you have selected. This mask identifies the host address bits used for routing to specific subnets.
Default Gateway	0.0.0.0	Gateway used to pass trap messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.

Parameter	Default	Description
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, and subnet mask.)
Master IP		Shows the IP address of the switch in the stack operating as Master.
Backup IP		Shows the IP address of the switch in the stack operating as Backup Master.

IP Connectivity Test (Ping)

Use the IP Connectivity Test to see if another site on the Internet can be reached. The screen shown below is described in the following table.

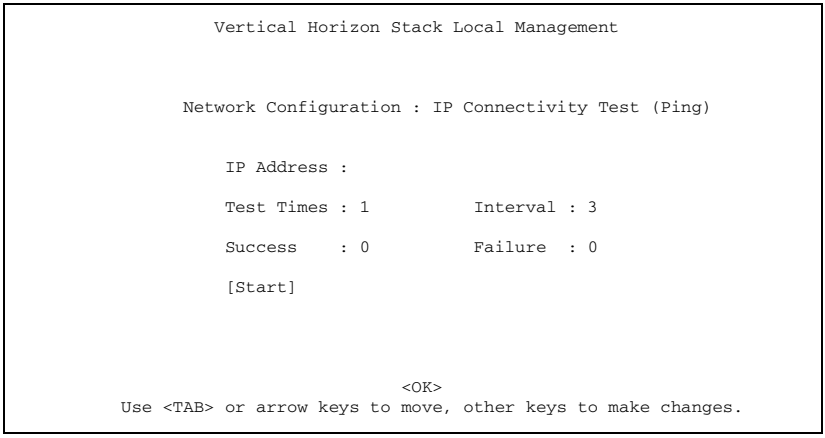

Figure 2-10. IP Connectivity Test

Parameter	Description
IP Address	IP address of the site you want to ping.
Test Times	The number of ICMP echo requests to send to the specified site. Range: 1~1000
Interval	The interval (in seconds) between pinging the specified site. Range: 1~10 seconds
Success/Failure	The number of times the specified site has responded or not to pinging.

HTTP Configuration

Use the HTTP Configuration screen to enable/disable the on-board Web agent, and to specify the TCP port that will provide HTTP service. The screen shown below is described in the following table.

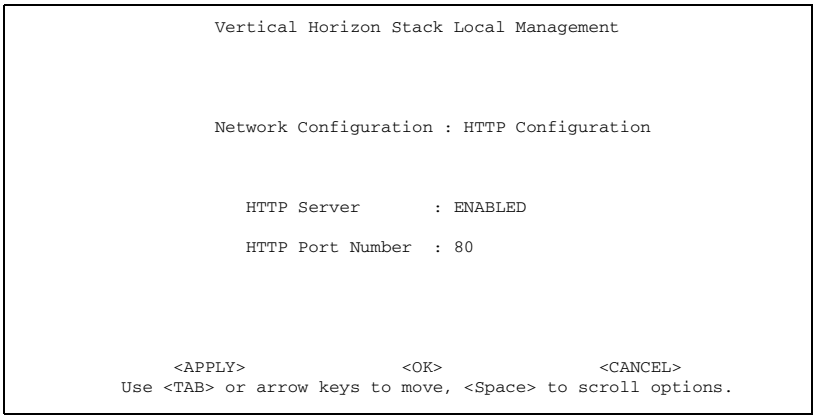

Figure 2-11. HTTP Configuration

Parameter	Description
HTTP Server	Enables/disables access to the on-board Web agent.
HTTP Port Number	Specifies the TCP port that will provide HTTP service. Range : 0~65535 Default : Port 80 (Telnet Port 23 is prohibited.)

Configuring the Serial Port

You can access the on-board configuration program by attaching a VT100 compatible device to the switch's serial port. (For more information on connecting to this port, see "Required Connections" on page 3.) The communication parameters for this port can be accessed from the Serial Port Configuration screen shown below and described in the following table.

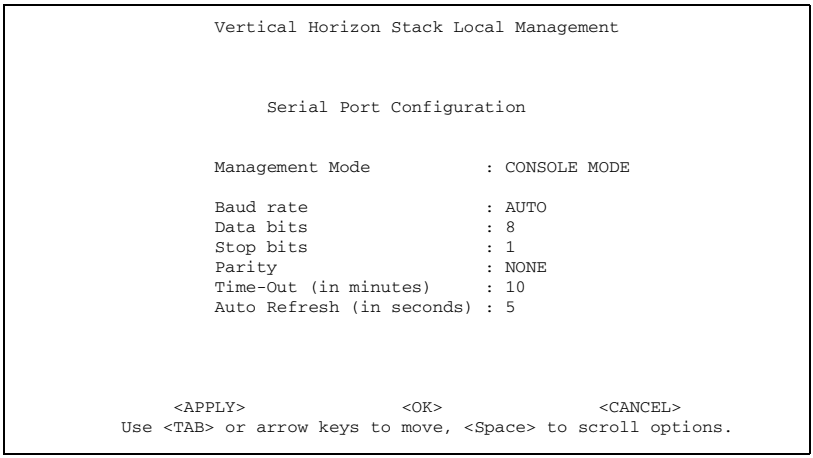

Figure 2-12. Serial Port Configuration

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the console port settings are for direct console connection.
Baud Rate	Auto	The rate at which data is sent between devices. Options : 2400, 4800, 9600, 19200 bps, and Auto detection
Databits	8 bits	Sets the databits of the RS-232 port. Options : 7, 8
Stopbits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	none	Sets the parity of the RS-232 port. Options : none/odd/even
Time-Out	10 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; 0: disabled
Auto Refresh	5 seconds	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 5-255 seconds; 0: disabled

Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS 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.

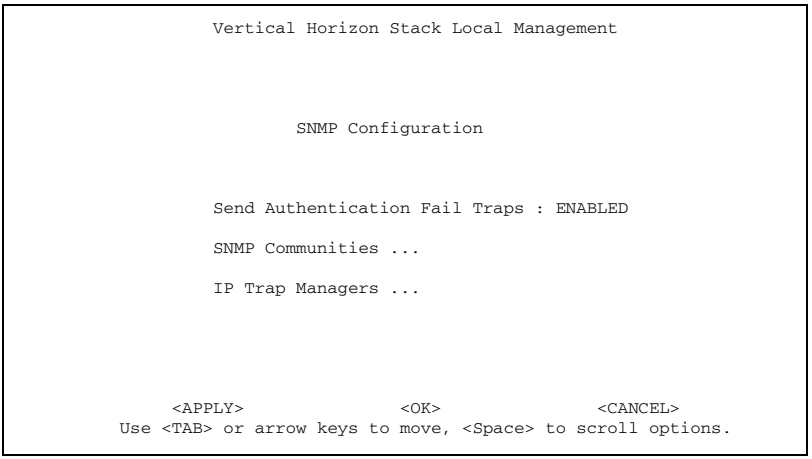

Figure 2-13. SNMP Configuration

Parameter	Description
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)
SNMP Communities	Assigns SNMP access based on specified strings.
IP Trap Managers	Specifies management stations that will receive authentication failure messages or other trap messages from the switch.

Configuring Community Names

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.

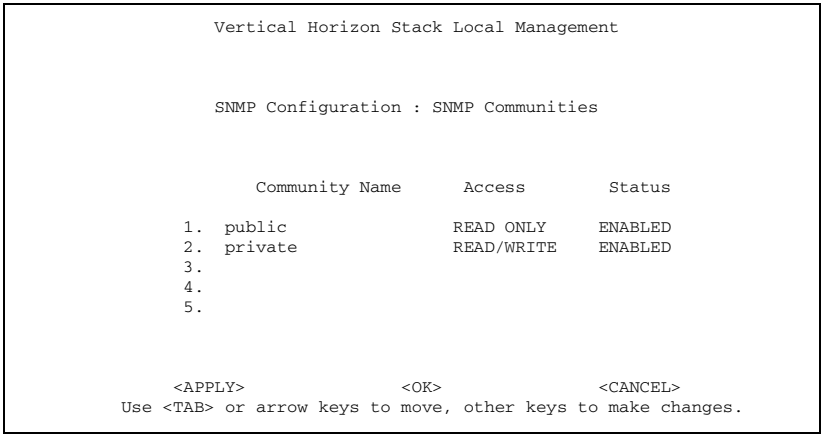

Figure 2-14. SNMP Communities

Parameter	Description
Community Name	A community entry authorized for management access. Maximum string length : 20 characters
Access	Management access is restricted to Read Only or Read/Write.
Status	Sets administrative status of entry to enabled or disabled.

Note: The default community strings are “public” with Read Only access, and “private” with Read/Write access.

Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

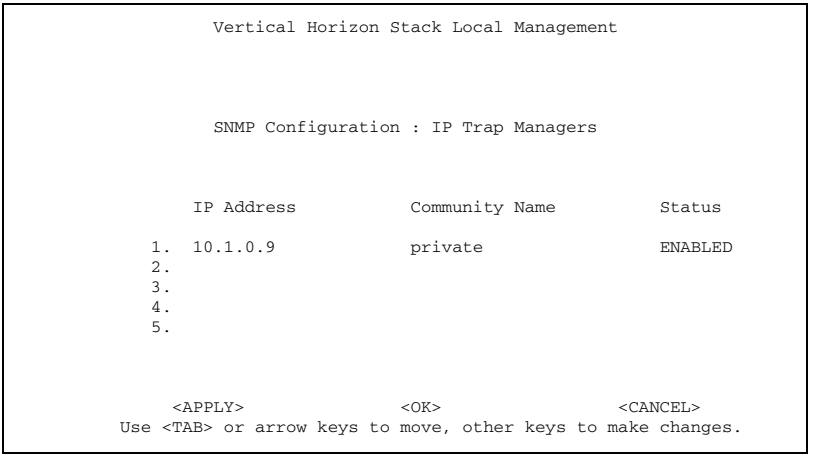

Figure 2-15. IP Trap Managers

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified for trap management access.
Status	Sets administrative status of selected entry to enabled or disabled. Can also delete the selected entry.

Console Login Configuration

Use the Management Setup: Console Login Configuration to restrict management access based on specified user names and passwords, or to set the invalid password threshold and timeout. There are only two user types defined, ADMIN (Administrator) and GUEST, but you can set up to five different user names and passwords. Only Administrators have write access for parameters governing the switch. You should therefore assign a user name and password to the default Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the System Configuration Program, contact Enterasys Networks Technical Support for assistance.) The parameters shown on this screen are indicated in the following figure and table.

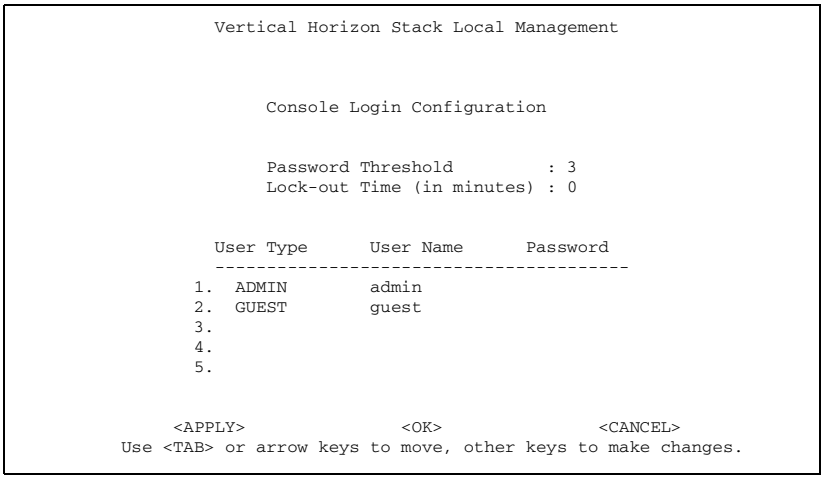

Figure 2-16. Console Login Configuration

Parameter	Default	Description
Password Threshold	3	Sets the password intrusion threshold which limits the number of failed logon attempts. Range : 0~65535
Lock-out Time	0	The time (in seconds) the management console will be disabled, due to an excessive number of failed logon attempts. Range : 0~65535
Admin*	name: admin password: null	Administrator has access privilege of Read/Write for all screens.
Guest*	name: guest password: null	Guest has access privilege of Read Only for all screens.

*** Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.**

Downloading System Software

Using TFTP Protocol to Download Over the Network

Use the TFTP Download menu to load software updates into the switch. The download file should be a VH-2402S2 file from Enterasys Networks; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

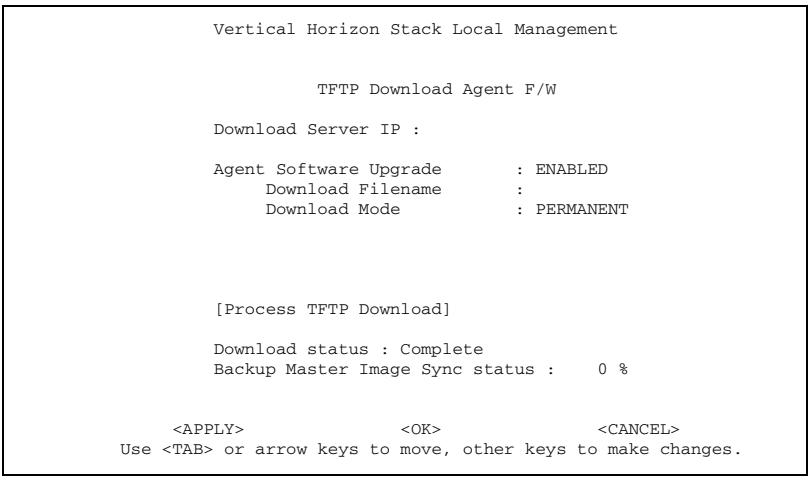

Figure 2-17. TFTP Download

Parameter	Description
Download Server IP	IP address of a TFTP server.
Agent Software Upgrade	Indicates that the switch is enabled for software upgrades.
Download Filename	The binary file to download to the agent module.
Download Mode	Indicates that the download is to permanent flash ROM.
[Process TFTP Download]	Issues a request to the TFTP server to download the specified file.
Download Status	Indicates if a download is “Complete” or “In Progress.”
Backup Master Image Sync status	Indicates the status of software synchronization with a backup management agent. The software synchronization function automatically copies new system software from the master to the backup agent. In a stack with a backup management agent installed, this process happens automatically after a TFTP download has completed.

Saving the System Configuration

Use the Configuration Save & Restore menu to save the switch configuration settings to a file on a TFTP server. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP server and the quality of the network connection. Parameters shown on this screen are indicated in the following figure and table.

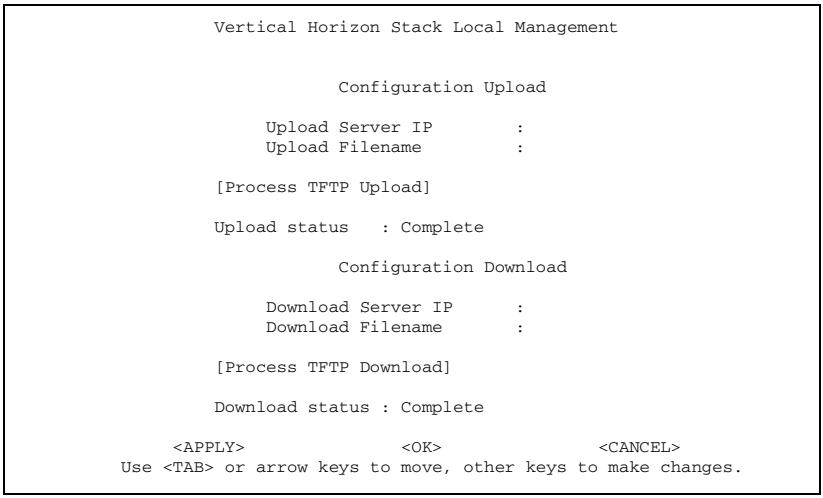

Figure 2-18. Configuration Save & Restore

Parameter	Description
Configuration Upload	
Upload Server IP	IP address of a TFTP server.
Upload Filename	The name of the file to contain the switch configuration settings.
[Process TFTP Upload]	Issues a request to upload the configuration settings to the specified file on the TFTP server.
Upload Status	Indicates if an upload is "Complete" or "In Progress."
Configuration Download	
Download Server IP	IP address of a TFTP server.
Download Filename	The name of the file that contains the switch configuration settings you wish to restore.
[Process TFTP Download]	Issues a request to the TFTP server to download the specified file.
Download Status	Indicates if a download is "Complete" or "In Progress."

Configuring Management Access

Use the Management Configuration menu to define which VLAN has management access to the switch. Parameters shown on this screen are indicated in the following figure and table.

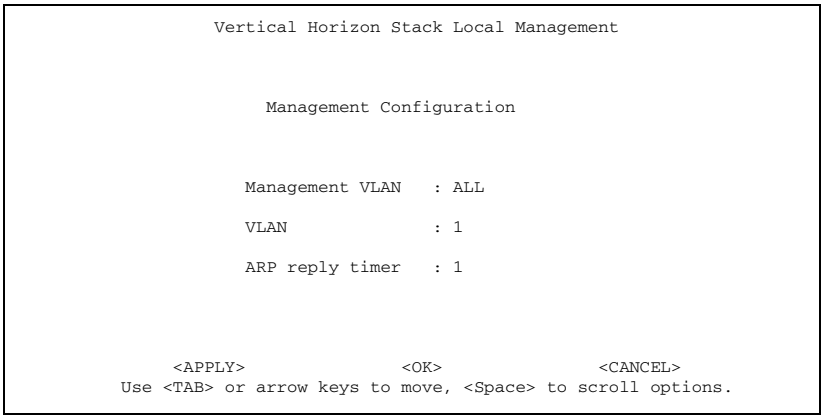

Figure 2-19. Management Configuration

Parameter	Default	Description
Management VLAN	All	Select ALL to give all VLANs access to switch management, or ONE to restrict access to a specified VLAN. If you select just one VLAN, you must specify its VLAN ID on the following line.
VLAN	1	Specifies the VLAN ID that has access to switch management.
ARP reply timer	1	Sets the interval time (in seconds) for sending ARP (Address Resolution Protocol) replies to other devices in the network. ARP is a protocol that allows network devices to identify the MAC address of a device that corresponds to a given IP address.

Configuring the Switch

The Device Control menu is used to control a broad range of functions, including port configuration, Spanning Tree support for redundant switches, port mirroring, multicast filtering, and Virtual LANs. Each of the setup screens provided by these configuration menus is described in the following sections.

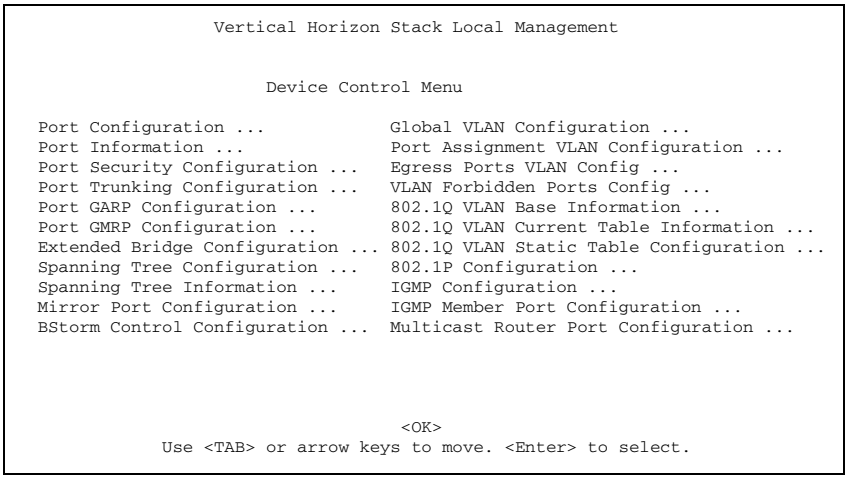

Figure 2-20. Device Control Menu

Selection	Description
Port Configuration	Sets communication parameters for ports.
Port Information	Displays current port settings and port status.
Port Security Configuration	Allows you to enable and configure port security for the switch.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
Port GARP Configuration*	Configures generic attribute settings used in the spanning tree protocol, VLAN registration, multicast filtering.
Port GMRP Configuration*	Configures GMRP multicast filtering.
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, and VLAN extensions.
Spanning Tree Configuration	Configures the switch, its ports and modules to participate in a local Spanning Tree.
Spanning Tree Information	Displays the current Spanning Tree configuration for the switch, its ports and modules.
Mirror Port Configuration	Sets the source and target ports for mirroring.
BStorm Control Configuration	Allows you to enable broadcast storm control and set the packet-per-second threshold.

Selection	Description
Global VLAN Configuration	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported, and allows you to enable/ disable each VLAN.
Port Assignment VLAN Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and 802.1Q trunks.
Egress Ports VLAN Configuration	Configures VLAN groups via static assignments to individual ports or a range of ports, including setting ports as members and configuring them as untagged.
VLAN Forbidden Ports Configuration	Restricts individual ports or a range of ports from being dynamically added to a VLAN by the GVRP* protocol.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members, or restricting ports from being dynamically added to a port by the GVRP* protocol.
802.1P Configuration	Configures default port priorities and queue assignments.
IGMP Configuration	Configures IGMP multicast filtering.
IGMP Member Port Configuration	Assigns ports that are attached to hosts who want to receive a specific multicast service.
Multicast Router Port Configuration	Displays the ports on the switch attached to a neighboring multicast router/switch for each VLAN ID.

*** Not implemented in the current firmware release.**

Configuring Port Parameters

Use the Port Configuration menus to set or display communication parameters for any port or module on the switch.

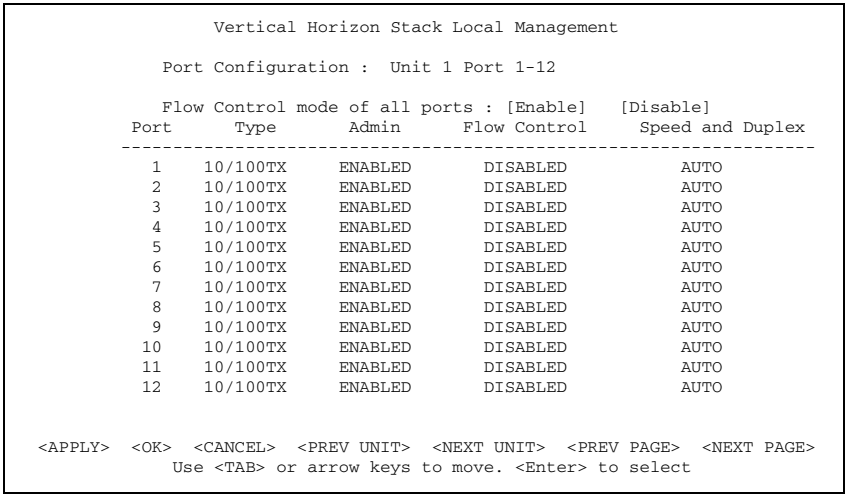

Figure 2-21. Port Configuration

Parameter	Default	Description
Type		Shows port type as: 10/100TX : 10Base-T / 100Base-TX 100FX : 100Base-FX 1000SX : 1000Base-SX 1000LX : 1000Base-LX 1000T : 1000Base-T GBIC : GBIC transceiver
Admin	ENABLED	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Flow Control	DISABLED	Used to enable or disable 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. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Speed and Duplex	AUTO	Used to set the current port speed, duplex mode, and auto-negotiation. (Auto-negotiation is not available for 100Base-FX ports.)

Viewing the Current Port Configuration

The Port Information screen displays the port type, status, link state, and flow control in use, as well as the communication speed and duplex mode. To change any of the port settings, use the Port Configuration menu. The parameters shown in the following figure and table are for the RJ-45 ports.

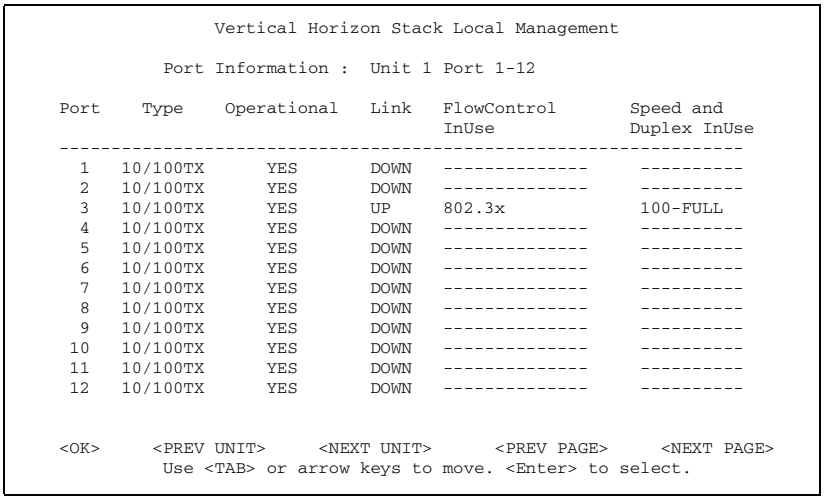

Figure 2-22. Port Information

Parameter	Description
Type	Shows port type as: 10/100TX : 10Base-T / 100Base-TX 100FX : 100Base-FX 1000SX : 1000Base-SX 1000LX : 1000Base-LX 1000T : 1000Base-T GBIC : GBIC transceiver
Operational	Shows if the port is functioning or not.
Link	Indicates if the port has a valid connection to an external device.
FlowControl InUse	Shows the flow control type in use. Flow control can eliminate frame loss by “blocking” traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Speed and Duplex InUse	Displays the current port speed and duplex mode used.

Port Security Configuration

Use the Port Security Configuration screen to enable and configure port security for the switch. Port Security allows you to configure each port with a list of MAC addresses of devices that are authorized to access the network through that port.

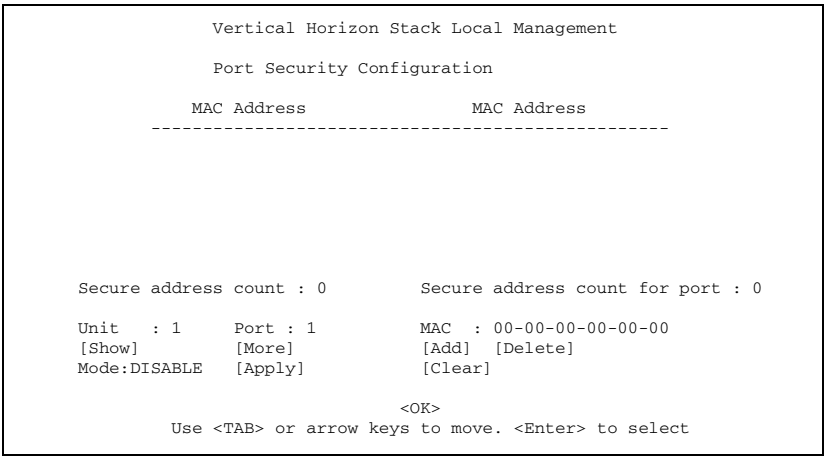

Figure 2-23. Port Security Configuration

Parameter	Description
MAC Address	A list of the authorized MAC addresses that can access the network through the specified port.
Secure address count	The total number of authorized MAC addresses configured.
Secure address count for port	The number of authorized MAC addresses configured for the specified port.
Unit	The stack unit ID.
Port	The port number on the unit.
[Show]	Displays authorized MAC addresses for the specified port.
[More]	Displays more MAC addresses for the port.
Mode	Port security can set to three states; Static, Disable, or Learning. When set to Static, the switch will drop packets from the port if the source MAC address does not match one of the addresses in the MAC Address list. If set to Learning, the switch will add the source MAC address of all packets received on the port to the authorized MAC Address list.
[Apply]	Applies a change of Mode to the port.
MAC	A specific MAC address to be added or deleted from the list.
[Add]	Adds a new MAC address to the current list.
[Delete]	Removes a MAC address from the current list.
[Clear]	Clears all the MAC addresses for the current port.

Configuring Port Trunks

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up five trunk connections (combining 2~4 ports into a fat pipe) between any two standalone switches, or up to 12 for an entire stack. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- The ports used in a trunk must all be of the same media type (RJ-45, 100Mbps fiber, or 1000Mbps fiber). The ports that can be assigned to the same trunk also have certain other restrictions (see the next page).
- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

You can use the Port Trunking Configuration screen set up port trunks as shown below:

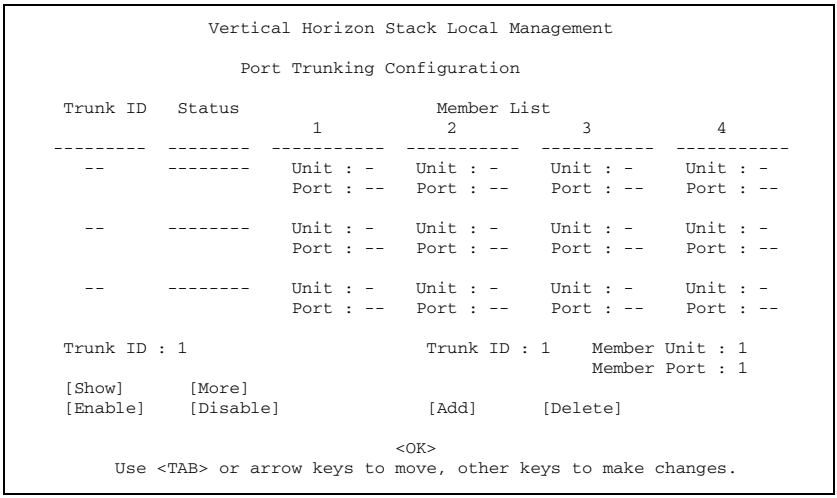

Figure 2-24. Port Trunking Configuration

Parameter	Description
Trunk ID	Configure up to five trunks per standalone switch, or up to 12 for an entire stack.
Unit	Specifies a switch unit in the stack (1~7).
Port	Select from 2~4 ports per trunk.
[Show]	Displays trunk settings, where the first trunk listed is specified by "Sorted by Trunk ID."
[More]	Scrolls through the list of configured trunks.
[Enable] [Disable]	Enables/disables the selected trunk.

The RJ-45 ports used for each trunk must all be on the same internal switch chip. The port groups permitted include:

Group 1	Group 2	Group 3
1,2,3,4, 13,14,15,16	5,6,7,8, 17,18,19,20	9,10,11,12, 21,22,23,24

Only two 100Mbps fiber ports can be configured as a trunk and these must be on the same module. 1000Base-SX/LX ports can be trunked together with any other like uplink ports in the stack.

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and Virtual LANs. To configure these extensions, use the Extended Bridge Configuration screen as shown below:

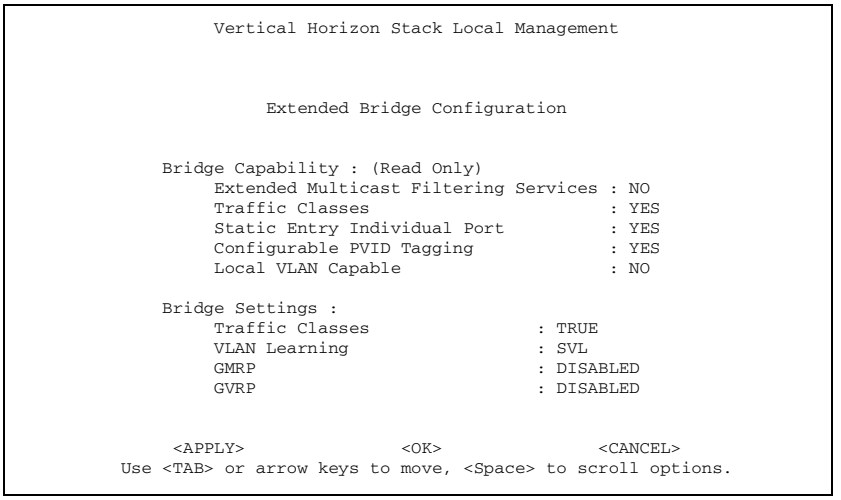

Figure 2-25. Extended Bridge Configuration

Parameter	Description
Bridge Capability	
Extended Multicast Filtering Services	Indicates that this switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Note that this function is not available for the current firmware release.
Traffic Classes	This switch provides mapping of user priorities to multiple traffic classes. (Refer to 802.1P Configuration.)
Static Entry Individual Port	This switch enables static filtering for unicast and multicast addresses. (Refer to Network Monitor Menu / Static Unicast Address Table Configuration and Static Multicast Address Table Configuration.)
Configurable PVID Tagging	This switch allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. (Refer to Port Assignment VLAN Configuration.)
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

Parameter	Description
Bridge Settings	
Traffic Class*	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by setting this parameter to False.
VLAN Learning	As default this switch uses Shared VLAN Learning (SVL), whereby all ports share one VLAN filtering database. However, you can set the switch to use Independent VLAN Learning (IVL), where each port maintains its own filtering database. Note that when you change from one method to the other, the switch will automatically reset and the current VLAN configuration will be lost..
GMRP*	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. (Note that GMRP is not implemented in the current firmware release.) The Internet Group Management Protocol (IGMP) is currently used by this switch to provide automatic multicast filtering.
GVRP*	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 VLANs groups which extend beyond the local switch.

*** Not implemented in the current firmware release.**

Using the Spanning Tree Algorithm

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. For a more detailed description of how to use this algorithm, refer to Appendix A, “Spanning Tree Concepts” on page 91.

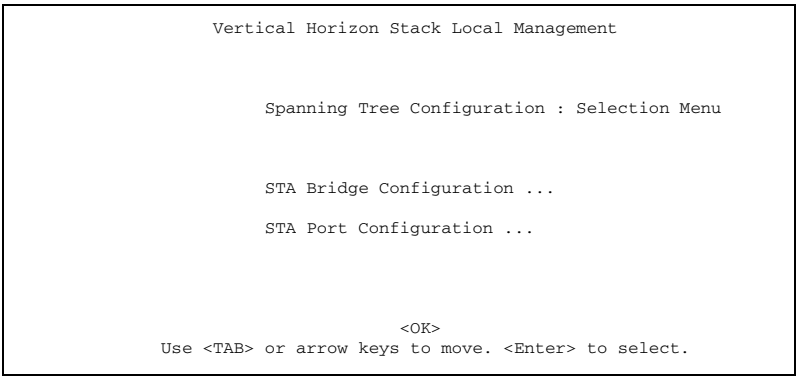

Figure 2-26. Spanning Tree Configuration

Configuring Bridge STA

The following figure and table describe Bridge STA configuration.

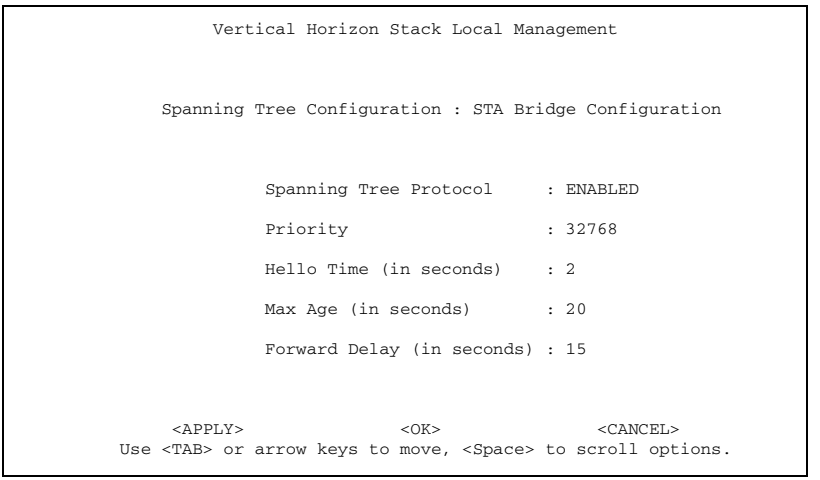

Figure 2-27. Bridge STA Configuration

Parameter	Default	Description
Spanning Tree Protocol	Enabled	Enable this parameter to participate in an STA compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message. The minimum value is1. The maximum value is the lower of 10 or [(Max. Message Age / 2) -1].
Max (Message) Age	20	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 is a root port, a new root port is selected from among the device ports attached to the network. 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 Delay - 1)].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening 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 blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

Configuring STA for Ports or Modules

The following figure and table describe STA configuration for ports or modules. (Note that the Spanning Tree Configuration screen for the expansion slots also indicates module type.)

```
                Vertical Horizon Stack Local Management

             Spanning Tree Port Configuration :  Unit 1 Port 1-12

             Fast forwarding on all ports :      [Enable]   [Disable]
              Port      Type       Priority    Cost    FastForwarding
              ------------------------------------------------------
                1      10/100TX      128         19      DISABLED
                2      10/100TX      128         19      DISABLED
                3      10/100TX      128         19      DISABLED
                4      10/100TX      128         19      DISABLED
                5      10/100TX      128         19      DISABLED
                6      10/100TX      128         19      DISABLED
                7      10/100TX      128         19      DISABLED
                8      10/100TX      128         19      DISABLED
                9      10/100TX      128         19      DISABLED
               10      10/100TX      128         19      DISABLED
               11      10/100TX      128         19      DISABLED
               12      10/100TX      128         19      DISABLED


<APPLY>  <OK>  <CANCEL>  <PREV UNIT>  <NEXT UNIT>  <PREV PAGE>  <NEXT PAGE>
             Use <TAB> or arrow keys to move. <Enter> to select
```

Figure 2-28. Spanning Tree Port Configuration

Parameter	Default	Description
Fast forwarding mode of all ports	ENABLED	Allows you to enable or disable fast forwarding for all ports on the switch.
Type		Shows 10/100TX, 100FX, 1000LX, 1000SX, 1000T, or GBIC port.
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm 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. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 1 - 65535.

Parameter	Default	Description
FastForwarding	ENABLED	This parameter is used to enable/disabled the Fast Spanning Tree mode for the port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding. FastForwarding enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, FastForwarding should only be enabled for ports that are connected to an end-node device.

Viewing the Current Spanning Tree Configuration

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port or module. To make any changes to the parameters for the Spanning Tree, use the Spanning Tree Configuration menu.

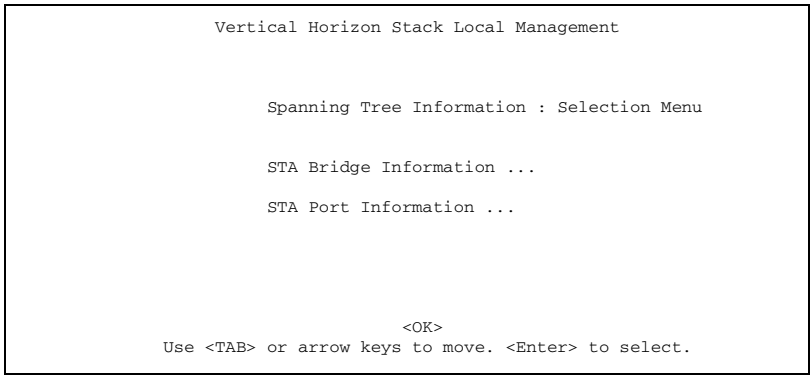

Figure 2-29. Spanning Tree Information

Displaying the Current Bridge STA

The parameters shown in the following figure and table describe the current Bridge STA Information.

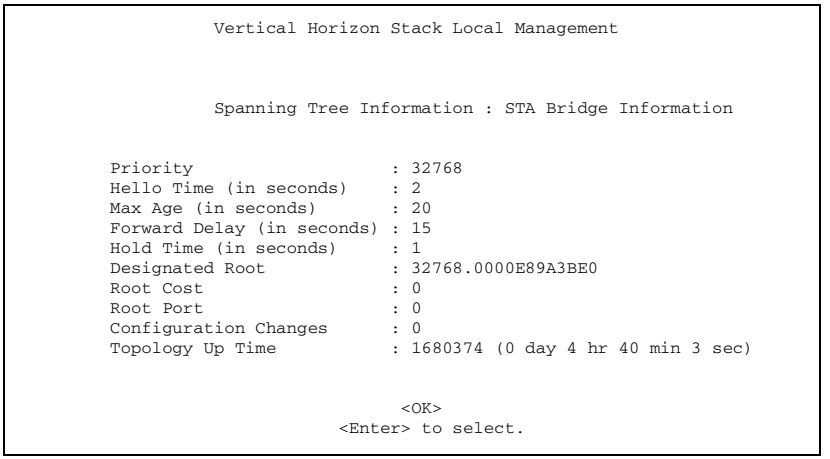

Figure 2-30. Bridge STA Information

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Configuration Changes	The number of times the spanning tree has been reconfigured.
Topology Up Time	The time since the spanning tree was last reconfigured.

Displaying the Current STA for Ports or Modules

The parameters shown in the following figure and table are for port or module STA Information (Port 1-12, Port 13-24, Port 25-32).

```
                Vertical Horizon Stack Local Management

            Spanning Tree Port Information :  Unit 1 Port 1-12

 Port    Type       Status       Designated     Designated      Designated
                                 Cost           Bridge          Port
-------------------------------------------------------------------------------
   1    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.1
   2    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.2
   3    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.3
   4    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.4
   5    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.5
   6    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.6
   7    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.7
   8    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.8
   9    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.8
  10    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.8
  11    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.8
  12    10/100TX   NO LINK           0     32768.0000E89A3BE0     128.8


  <OK>     <PREV UNIT>     <NEXT UNIT>      <PREV PAGE>     <NEXT PAGE>
           Use <TAB> or arrow keys to move. <Enter> to select.
```

Figure 2-31. Spanning Tree Port Information

Parameter	Description
Type	Shows port type as: 10/100TX : 10Base-T / 100Base-TX 100FX : 100Base-FX 1000SX : 1000Base-SX 1000LX : 100Base-LX 1000T : 1000Base-T GBIC : GBIC transceiver
Status	Displays the current state of this port within the spanning tree: No Link — There is no valid link on the port. Disabled — Port has been disabled by the user or has failed diagnostics. Blocking — Port receives STA configuration messages, but does not forward packets. Listening — Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. Learning — Has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding — The port forwards packets, and continues learning addresses.

Parameter	Description
	The rules defining port status are: • A port on a network segment with no other STA-compliant bridging device is always forwarding. • If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Designated Cost	The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
Designated Port (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

Using a Mirror Port for Analysis

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. When mirroring port traffic, note that the target port must be configured in the same VLAN and be operating at the same speed as the source port (see Configuring Virtual LANs on page 47). If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

You can use the Mirror Port Configuration screen to designate a single port pair for mirroring as shown below:

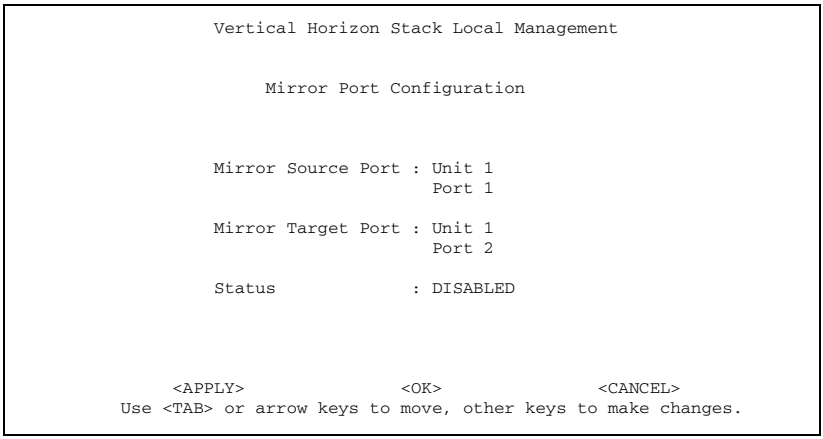

Figure 2-32. Mirror Port Configuration

Parameter	Description
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Port	The port that will duplicate or “mirror” all the traffic happening on the monitored port.
Status	Enables or disables the mirror function.

Configuring Broadcast Storm Control

Use the Broadcast Storm Control Configuration screen to enable broadcast storm control for all ports in the switch stack, as shown below:

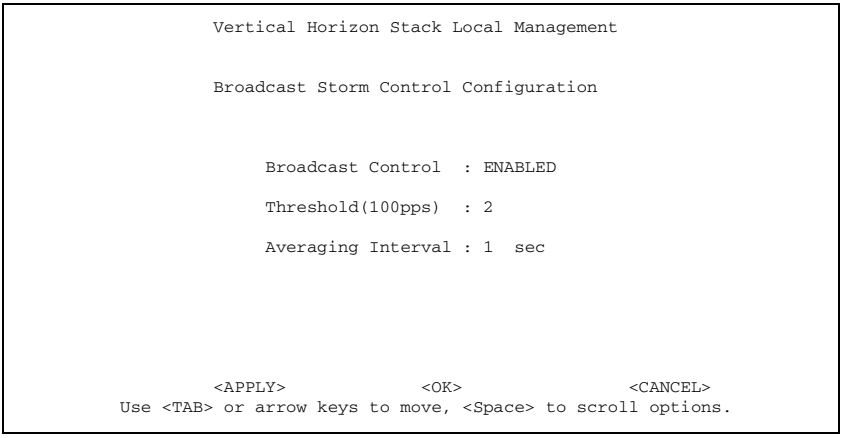

Figure 2-33. Broadcast Storm Control Configuration

Parameter	Description
Broadcast Control	Allows you to enable/disable broadcast storm control for all ports in the switch stack. When enabled, the switch stack will employ a broadcast-control mechanism if the packet-per-second threshold is exceeded. This mechanism drops all broadcast packets from the stack for the time period specified in the “Averaging Interval” field. (Default is Disabled.)
Threshold	The packet-per-second threshold for broadcast packets received on all ports in the switch stack. (Default is 200 pps.)
Averaging Interval	Specifies the time period for which broadcast packets will be dropped from the switch stack. Values can be 200 ms, 500 ms, 1, 5, or 10 seconds. (Default is 1 second.)

Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. 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 a lot of IPX and NetBEUI traffic. By using IEEE 802.1Q compliant VLANs and GARP VLAN Registration Protocol, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see Appendix B, “Virtual LANs (VLANs)” on page 97. The VLAN configuration screens are described in the following sections.

Global VLAN Configuration

Use the Global VLAN Configuration screen to create a new VLAN and enable/disable VLANs by specifying a VLAN ID and VLAN name. (Note that this is a global setting, you cannot configure VLAN port members from this screen). This screen also displays basic information on the VLAN support of the switch stack.

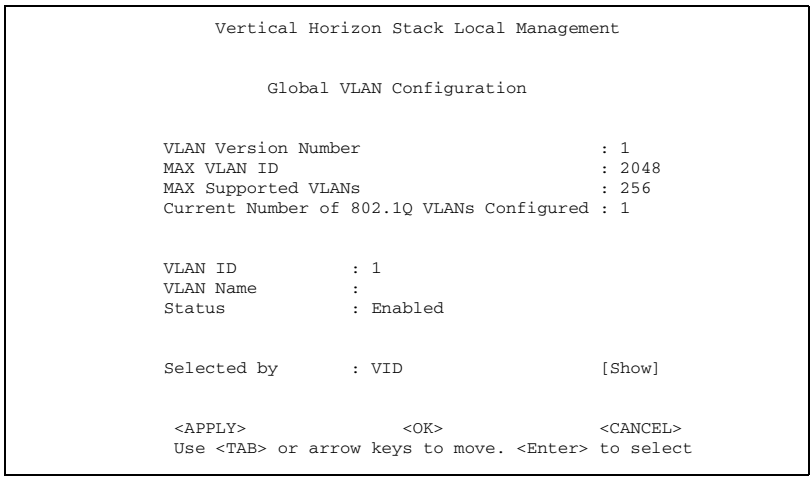

Figure 2-34. Global VLAN Configuration

Parameter	Description
VLAN Version Number	The VLAN version used by the switch stack as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by the switch stack.
MAX Supported VLANs	Maximum number of VLANs that can be configured for the switch stack.
Current Number of VLANs Configured	The number of VLANs currently configured in the switch stack.

Parameter	Description
VLAN ID	The ID for a new VLAN to be created, or the ID of an existing VLAN to be displayed.
VLAN Name	The name of a new VLAN to be created, or the name of an existing VLAN to be displayed.
Status	Allows a configured VLAN to be enabled or disabled. To create a new VLAN specified in the VLAN ID and VLAN Name fields, select “Create” and then use <APPLY>.
Slected by	Selects VLAN to display by VLAN ID or VLAN Name.
[Show]	Displays settings for the specified VLAN.

Port Assignment VLAN Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features.

```
                Vertical Horizon Stack Local Management

                     Port Assigment VLAN Configuration

                Unit  Port PVID  802.1Q Trunk  Ingress Filter
               ------------------------------------------------
                  1      1   2         NO           FALSE
                  1      2   1         NO           FALSE
                  1      3   1         NO           FALSE
                  1      4   1         NO           FALSE
                  1      5   1         NO           FALSE
                  1      6   1         NO           FALSE
                  1      7   1         NO           FALSE
                  1      8   1         NO           FALSE
                  1      9   1         NO           FALSE
                  1     10   1         NO           FALSE

Unit ID   : 1                    [Show]
Port ID   : 1                    [More]

          <APPLY>              <OK>              <CANCEL>
     Use <TAB> or arrow keys to move, <Space> to scroll options.
```

Figure 2-35. Port Assignment VLAN Configuration

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
802.1Q Trunk	Used to enable/disable the VLAN trunk status for the port. A VLAN Trunk link between two VLAN-aware switches will carry traffic from all VLANs, allowing VLAN tagged frames to maintain their VLAN ID across multiple switches. When enabled, a port joins all configured VLANs and the untagged port VLAN ID (PVID) is set to 4000, a reserved VLAN ID for trunk ports.
Ingress Filter*	If set to “True,” incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
[Show]	Displays settings for the specified stack unit and port.
[More]	Displays consecutively numbered stack units and ports.

*** This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.**

Egress Ports VLAN Configuration

Use this screen to modify the settings for an existing VLAN. You can add/delete port members for a VLAN from any unit in the stack. (Note that all ports can only belong to one untagged VLAN. This is set to VLAN 1 by default, but can be changed via the Port Assignment VLAN Configuration screen on page 48.)

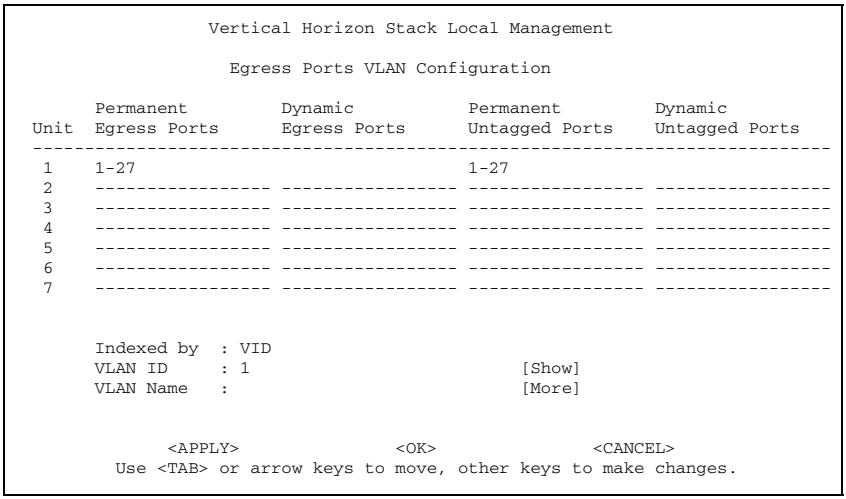

Figure 2-36. Egress Ports VLAN Configuration

Parameter	Description
Permanent Egress Ports	Enter the ports, or range of ports, to configured them as permanent (static) members of the displayed VLAN.
Dynamic Egress Ports	Shows the ports that have been added to the displayed VLAN group via GVRP*.
Permanent Untagged Ports	Enter the ports, or range of ports, to configured them as permanent (static) untagged members of the displayed VLAN.
Dynamic Untagged Ports	Shows the untagged ports that have been added to the displayed VLAN group via GVRP*.
Indexed by	Indicates if VLANs are displayed by ID or name.
VLAN ID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANs.

* Not implemented in the current firmware release.

VLAN Forbidden Ports Configuration

Use this screen to prevent a port from being automatically added to a VLAN via the GVRP protocol. (Note that GVRP is not implemented in the current firmware release.)

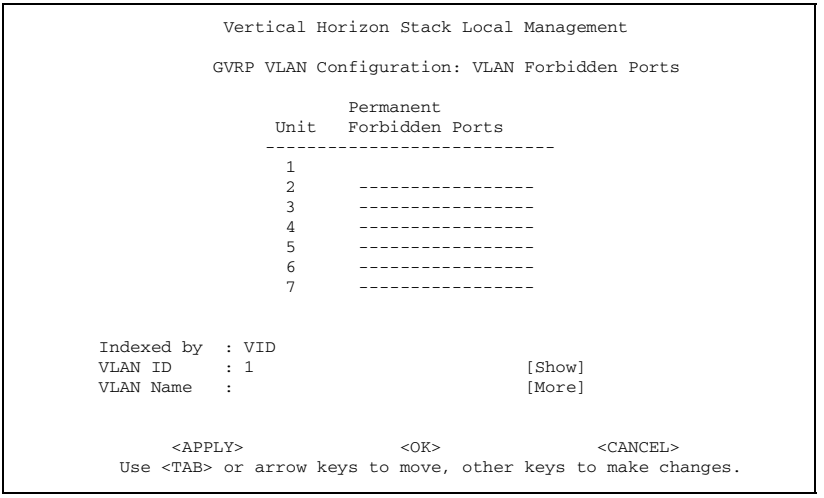

Figure 2-37. VLAN Forbidden Ports Configuration

Parameter	Description
Unit	Stack unit.
Permanent Forbidden Ports	A list of ports, or range of ports, on a stack unit that are not allowed to be automatically added to this VLAN via GVRP.
Indexed by	Indicates if VLANs are displayed by ID or name.
VLAN ID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANs.

802.1Q VLAN Base Information

The 802.1Q VLAN Base Information screen displays basic information on the VLAN type supported by this switch.

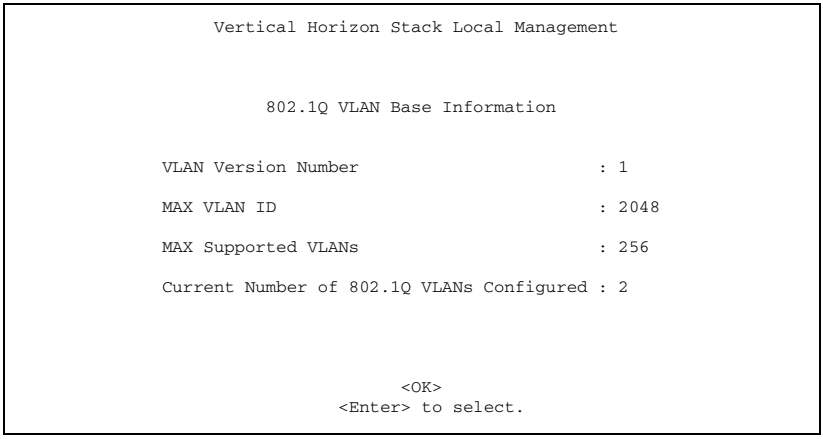

Figure 2-38. 802.1Q VLAN Base Information

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

802.1Q VLAN Current Table Information

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN (page 48). The current configuration is shown in the following figure.

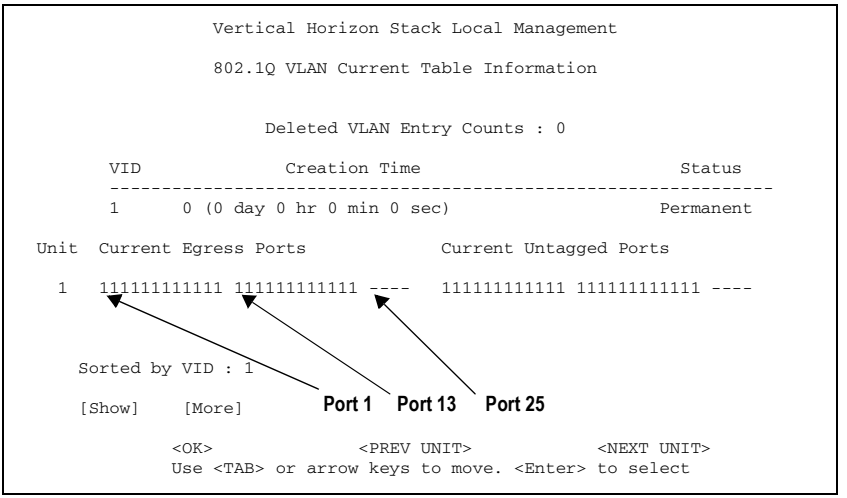

Figure 2-39. 802.1Q VLAN Current Table Information

Parameter	Description
Deleted VLAN Entry Counts	The number of times a VLAN entry has been deleted from this table.
VID	The ID for the VLAN currently displayed.
Creation Time	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch: Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Unit	Stack unit.
Current Egress Ports	Shows the ports which have been added to the displayed VLAN group, where “1” indicates that a port is a member and “0” that it is not.
Current Untagged Ports	If a port has been added to the displayed VLAN (see Current Egress Ports), its entry in this field will be “1” if the port is untagged or “0” if tagged.
[Show]	Displays the members for the VLAN indicated by the “Sorted by VID” field.
[More]	Displays any subsequent VLANs if configured.

802.1Q VLAN Static Table Configuration

Use this screen to create a new VLAN or modify the settings for an existing VLAN. You can add/delete port members for a VLAN from any unit in the stack, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Also, note that all ports can only belong to one untagged VLAN. This is set to VLAN 1 by default, but can be changed via the Port Assignment VLAN Configuration screen on page 48.)

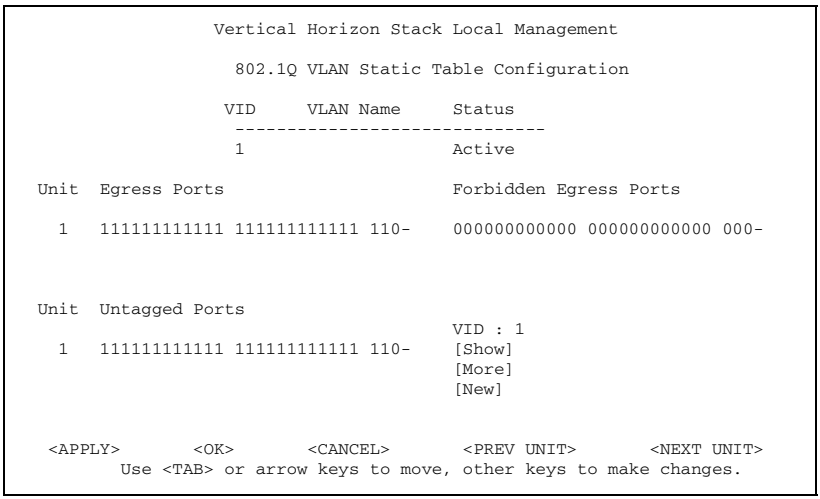

Figure 2-40. 802.1Q VLAN Static Table Configuration

Parameter	Description
VID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
Status	Sets the current editing status for this VLAN as: Not in Service, Destroy, or Active.
Unit	Stack unit.
Egress Ports	Set the entry for any port in this field to “1” to add it to the displayed VLAN, or “0” to remove it from the VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP.
Untagged Ports	Set the entry for any port in this field to “1” to add it to the displayed VLAN as an untagged port.
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANs.
[New]	Sets up the screen for configuring a new VLAN.

For example, the following screen displays settings for VLAN 2, which includes tagged ports 1-6, and forbidden port 12. (Note that the dashed lines show that there are no switch units in this system other than Unit 1.)

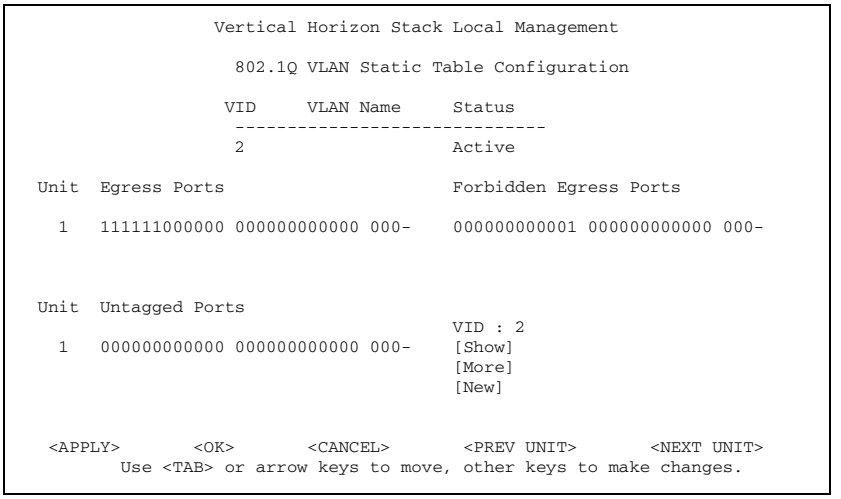

Figure 2-41. 802.1Q VLAN Static Table Configuration Example

Configuring Traffic Classes

IEEE 802.1p defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with strict priority queuing for each port. You can use the 802.1P Configuration menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections. Also, refer to Appendix C, “Class of Service” on page 101.

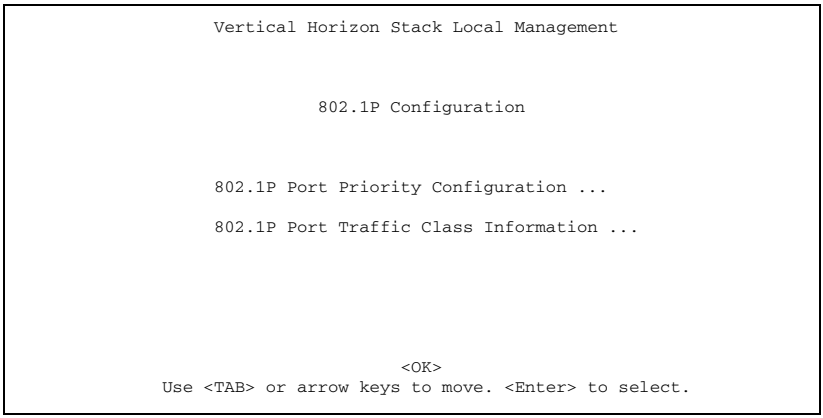

Figure 2-42. 802.1P Configuration

Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the 802.1P Port Priority Configuration menu to adjust default priority for any port as shown below:

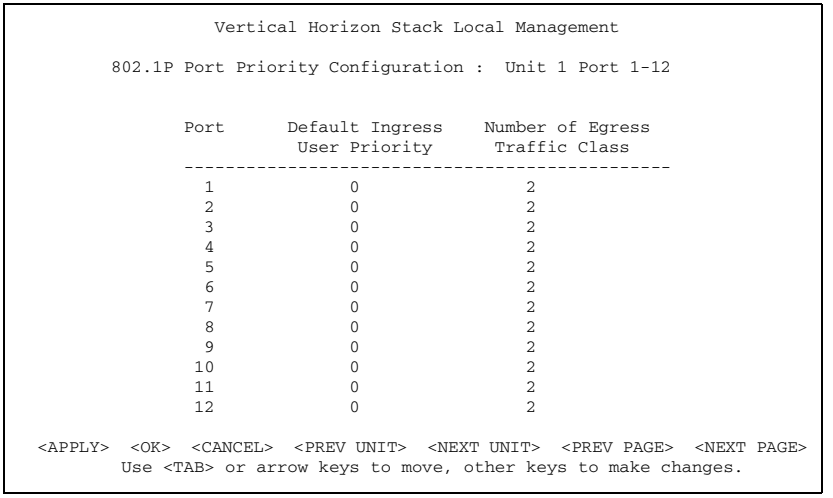

Figure 2-43. 802.1P Port Priority Configuration

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0~7, where 0~3 specifies the low priority queue and 4~7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

802.1P Port Traffic Class Information

This switch provides two priority levels with strict priority queuing for port egress. This means that any frames with a default or user priority from 0~3 are sent to the low priority queue “0” while those from 4~7 are sent to the high priority queue “1” as shown in the following screen:

```
                Vertical Horizon Stack Local Management

      802.1P Port Traffic Class Information :  Unit 1 Port 1-12

         Port                    User Priority

                0     1     2     3     4     5     6     7
         ------------------------------------------------------------
            1   0     0     0     0     1     1     1     1
            2   0     0     0     0     1     1     1     1
            3   0     0     0     0     1     1     1     1
            4   0     0     0     0     1     1     1     1
            5   0     0     0     0     1     1     1     1
            6   0     0     0     0     1     1     1     1
            7   0     0     0     0     1     1     1     1
            8   0     0     0     0     1     1     1     1
            9   0     0     0     0     1     1     1     1
           10   0     0     0     0     1     1     1     1
           11   0     0     0     0     1     1     1     1
           12   0     0     0     0     1     1     1     1

<OK>     <PREV UNIT>     <NEXT UNIT>      <PREV PAGE>     <NEXT PAGE>
          Use <TAB> or arrow keys to move. <Enter> to select.
```

Figure 2-44. 802.1P Port Traffic Class Information

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0~3 specify the low priority queue and 4~7 specify the high priority queue.

IGMP Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing 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 which want to receive the multicast 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 the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information, see “IGMP Snooping and IP Multicast Filtering” on page 103.)

Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast group. You can use the IGMP Configuration screen to configure multicast filtering shown below:

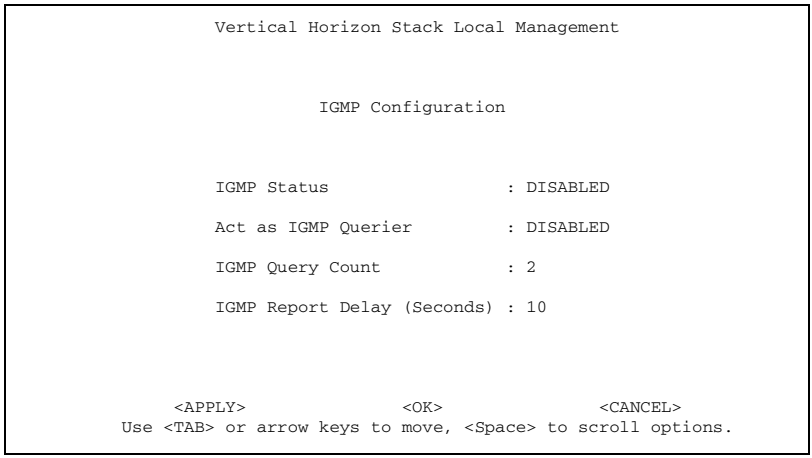

Figure 2-45. IGMP Configuration

Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
Act as IGMP Querier	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic.
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. (Range: 2 - 10.)
IGMP Report Delay	The time (in 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. (Range: 5 - 30.)

Note: The default values are indicated in the sample screen.

IGMP Member Port Configuration

You can use the IGMP Member Port Configuration screen to assign ports that are attached to hosts who want to receive a specific multicast service.

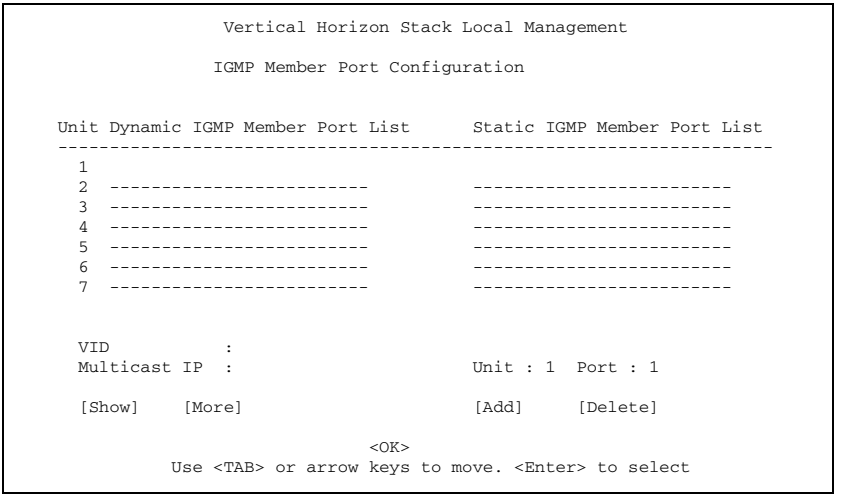

Figure 2-46. IGMP Member Port Configuration

Parameter	Description
Unit	The stack unit ID.
Dynamic IGMP Member Port List	A list of the switch ports that have been automatically configured as being attached to a IGMP host.
Static IGMP Member Port List	A list of the switch ports that have been manually configured as being attached to a IGMP host.
VID	The VLAN ID number used to sort the list.
Multicast IP	The IP address for a specific multicast service that is used to sort the list.
[Show]	Displays settings for the specified VLAN ID and stack unit.
[More]	Displays consecutively numbered stack units.
Unit/Port	Specifies a stack port to be added or deleted from the static member port list.
[Add]	Adds a new host port to the current list.
[Delete]	Removes a host port from the current list.

Multicast Router Port Configuration

You can use the Multicast Router Port Configuration screen to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

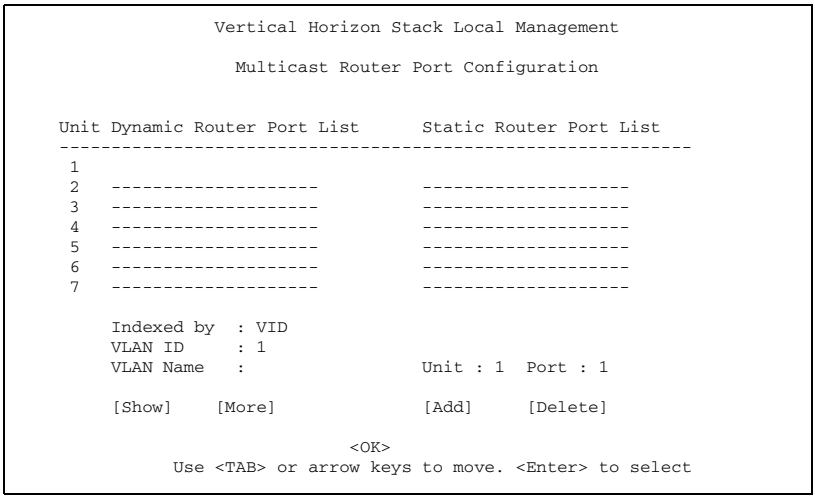

Figure 2-47. Multicast Router Port Configuration

Parameter	Description
Unit	The stack unit ID.
Dynamic Router Port List	The switch ports that have been automatically listed as being attached to a neighboring multicast router/switch.
Static Router Port List	The switch ports that have been manually listed as being attached to a neighboring multicast router/switch.
Indexed by	Indicates if the VLAN ID or VLAN Name is used to display the VLAN.
VLAN ID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
[Show]	Displays settings for the specified VLAN ID and stack unit.
[More]	Displays consecutively numbered stack units.
Unit/Port	Specifies a stack port to be added or deleted from the static router port list.
[Add]	Adds a new port to the current list.
[Delete]	Removes a port from the current list.

Monitoring the Switch

The Network Monitor Menu provides access to port statistics, RMON statistics, IP multicast addresses, and the static (unicast) address table. Each of the screens provided by these menus is described in the following sections.

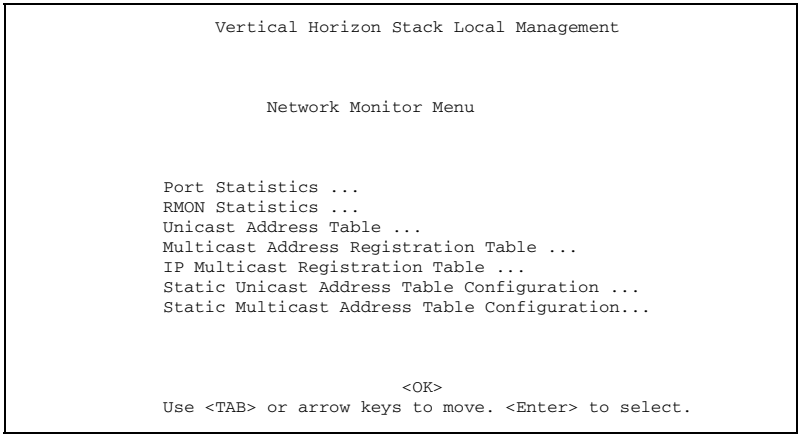

Figure 2-48. Network Monitor Menu

Parameter	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing of all unicast addresses stored in the switch, as well as sort, search and clear functions.
Multicast Address Registration Table	Displays the ports that belong to each GMRP Muticast group. (Not implemented in this firmware release.)
IP Multicast Registration Table	Displays the ports that belong to each IP Muticast group.
Static Unicast Address Table Configuration	Allows you to display or configure static unicast addresses.
Static Multicast Address Table Configuration	Allows you to display or configure static GMRP multicast addresses. (Not implemented in this firmware release.)

Displaying Port Statistics

Port Statistics display key statistics from the Ethernet-like MIB for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). The values displayed have been accumulated since the last system reboot.

Select the required stack unit, and port or module. The statistics displayed are indicated in the following figure and table.

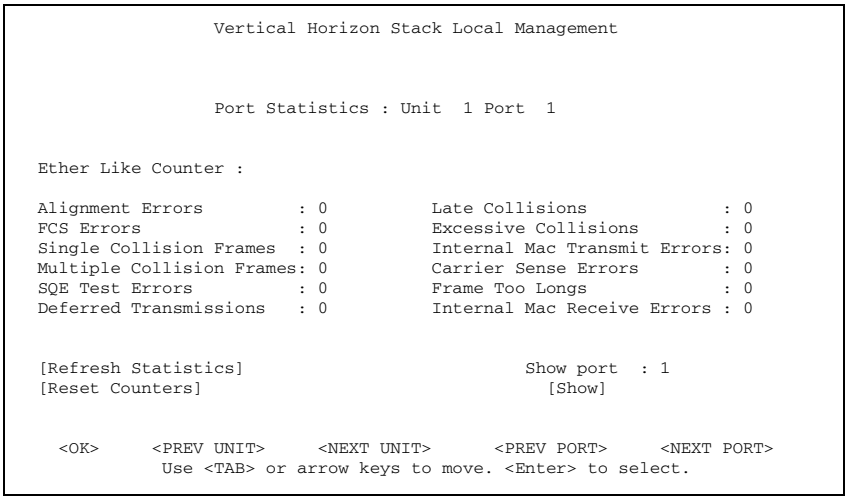

Figure 2-49. Port Statistics

Parameter	Description
Alignment Errors	For 10 Mbps ports, this counter records alignment errors (mis-synchronized data packets). For 100 Mbps ports, this counter records the sum of alignment errors and code errors (frames received with rxerror signal).
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.

Parameter	Description
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The number of frames for which reception failed due to an internal MAC sublayer receive error.

*** The reported values will always be zero because these statistics are not supported by the internal chip set.**

Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port or media module from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. Values displayed have been accumulated since the last system reboot.

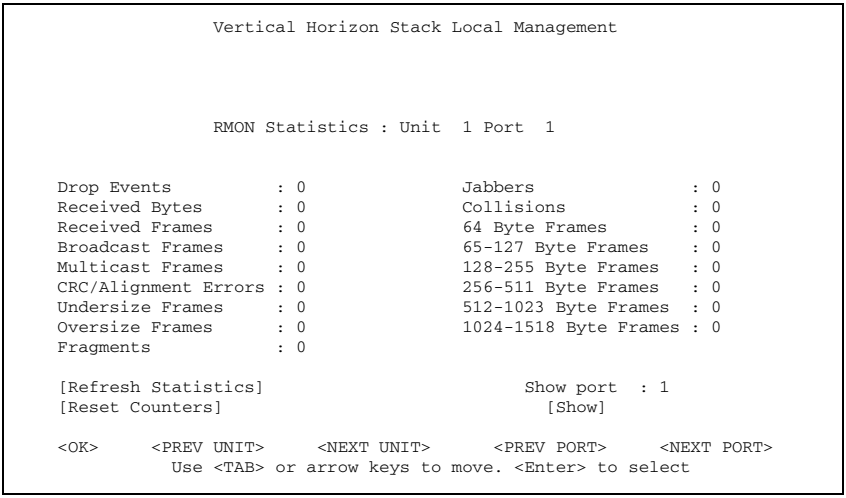

Figure 2-50. RMON Statistics

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
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	For 10Mbs ports, the counter records CRC/alignment errors (FCS or alignment errors). For 100Mbs ports, the counter records the sum of CRC/alignment errors and code errors (frame received with rxerror signal).
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.
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.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte 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	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Displaying the Unicast Address Table

The Address Table contains the MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN ID. You can search for a specific address, clear the entire address table, or information associated with a specific address, or set the aging time for deleting inactive entries.

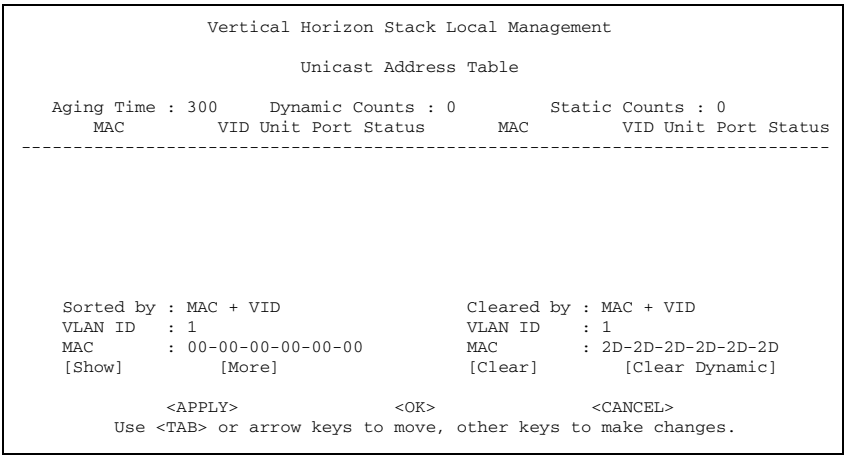

Figure 2-51. Unicast Address Table

Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 seconds; Default: 300 seconds
Dynamic Counts	The number of dynamically learned addresses in the table.
Static Counts	The number of static addresses in the table.
MAC	The MAC address of a node.
VID	The VLAN(s) associated with this address or port.
Unit	Switch unit in the stack (1~7).
Port	The port whose address table includes this MAC address.
Status	Indicates address status as: D: Dynamically learned, or P: Fixed permanently by SNMP network management software.
[Show]	Displays the address table based on specified VLAN ID, and sorted by primary key MAC or VID.
[More]	Scrolls through the entries in the address table.
[Clear]	Clears the specified MAC address.
[Clear Dynamic]	Clears all dynamically learned MAC addresses in the table.

Displaying the IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

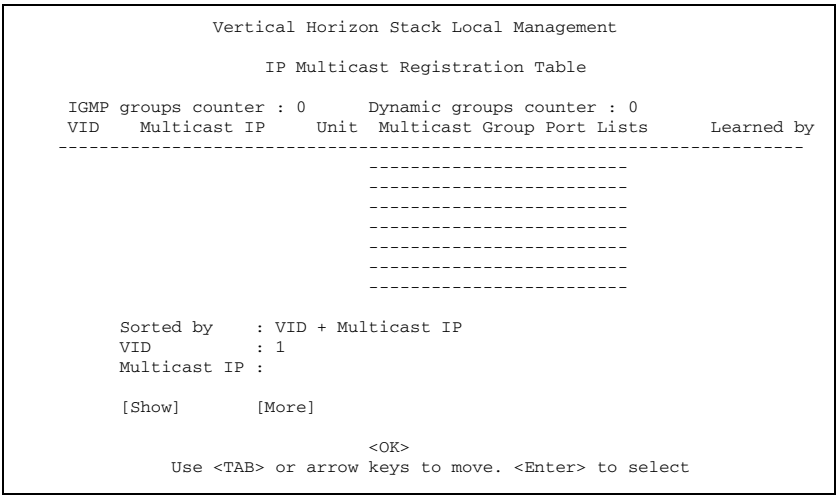

Figure 2-52. IP Multicast Registration Table

Parameter	Description
IGMP groups counter	The total number of multicast groups learned by IGMP.
Dynamic groups counter	The total number of multicast groups learned dynamically.
VID	VLAN ID assigned to this multicast group.
Multicast IP	IP address for specific multicast services.
Unit	Stack unit.
Multicast Group Port Lists	The switch ports registered for the indicated multicast service.
Learned by	Indicates if the ports were learned dynamically or via IGMP.
[Show]	Displays the address table sorted on VID and then Multicast IP.
[More]	Scrolls through the entries in the address table.

Configuring Static Unicast Addresses

Use the Static Unicast Address Table Configuration screen to manually configure host MAC addresses in the unicast table. You can use this screen to associate a MAC address with a specific VLAN ID and switch port as shown below.

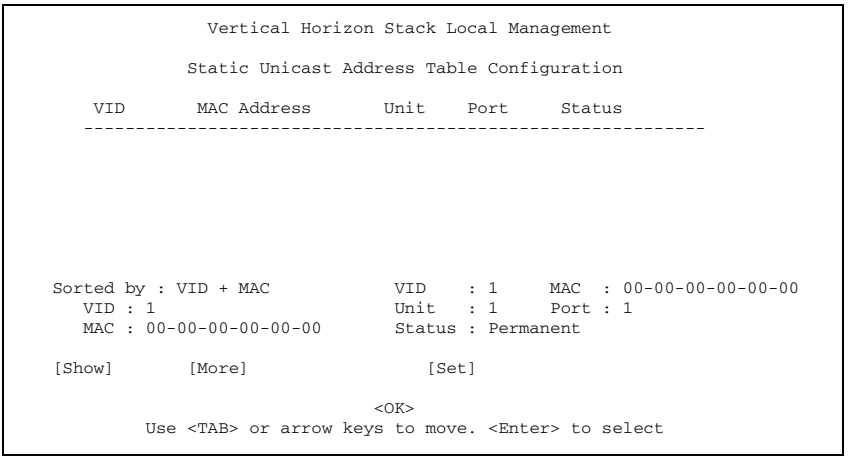

Figure 2-53. Static Unicast Address Table Configuration

Parameter	Description
VID	The VLAN group this port is assigned to.
MAC Address	The MAC address of a host device attached to this switch.
Unit	The switch unit the host device is attached to.
Port	The port the host device is attached to.
Status	The status for an entry can be set to: Permanent: This entry is currently in use and will remain so after the next reset of the switch. DeleteOnReset: This entry is currently in use and will remain so until the next reset. Invalid: Removes the corresponding entry. DeleteOnTimeOut: This entry is currently in use and will remain so until it is aged out. (Refer to Address Table Aging Time on page 66.) Other: This entry is currently in use but the conditions under which it will remain so differ from the preceding values.
[Show]	Displays the static address table sorted on VID as the primary key and MAC address as secondary key.
[More]	Scrolls through entries in the static address table.
[Set]	Adds the specified entry to the static address table, such as shown in the following example: VID : 1 MAC : 00-00-00-e8-34-22 Unit : 1 Port : 1 Status : Permanent

Resetting the System

Select the System Restart Menu under the Main Menu to reset the management agent. The reset screen includes options as shown in the following figure and table.

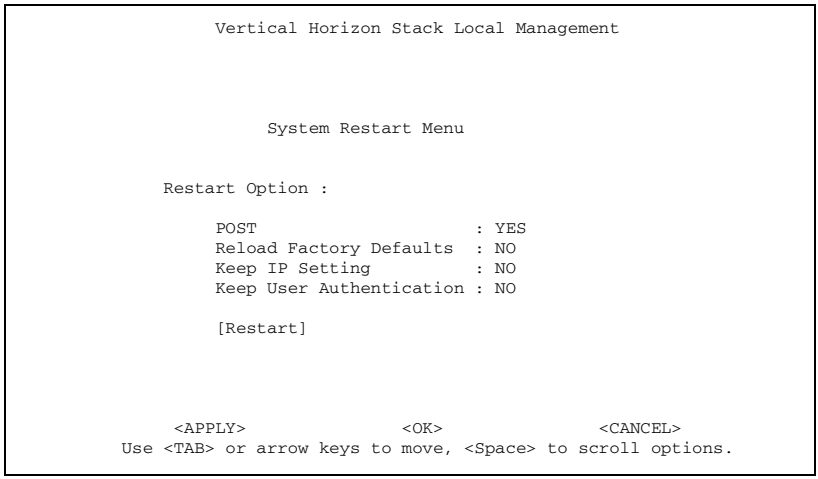

Figure 2-54. System Restart Menu

Parameter	Description
POST	Runs the Power-On Self-Test
Reload Factory Defaults	Reloads the factory defaults
Keep IP Setting	Retains the settings defined in the IP Configuration menu.
Keep User Authentication	Retains the user names and passwords defined in the Console Login Configuration menu.

Logging Off the System

Use the Exit command under the Main Menu to exit the configuration program and terminate communications with the switch for the current session.

3. CONFIGURING & MONITORING THE SWITCH

Common Tasks

The switch console menus allow you to modify default switch settings and configure a switch for network management. They also allow you to monitor switch performance and status. See Section 2, “VH-2402S2 User Interface,” for an overview of the menu hierarchy and a description of all menus. The following sections describe common tasks in setting up and operating the VH-2402S2 switch using the console menus.

To begin, set operating parameters and make sure the network connections are correct by performing these tasks:

- Setting password protection for the switch to prevent unauthorized access to console menus
- Assigning an IP address for the switch if you plan to manage the switch using SNMP, or if you use Telnet to access the switch
- Checking network configuration status and verifying that network connections are correct

After the switch is installed and operating, you may want to perform any of the following tasks:

- Connecting via Telnet for in-band access to the console menus
- Setting SNMP parameters for management access
- Viewing switch statistics to monitor and evaluate switch performance and traffic patterns on the network
- Configuring port mirroring
- Downloading a software upgrade
- Configuring Spanning Tree parameters
- Configuring VLANs
- Configuring Class of Service
- Configuring IGMP multicast filtering
- Configuring port operation (enable/disable, port speed, full/half duplex and flow control)
- Configuring port trunks
- Configuring broadcast storm control
- Configring the Unicast Address table
- Setting a default gateway
- Configuring BootP

Setting Password Protection

The VH-2402S2 switch is factory-configured with administrator access rights to the console menus set to READ/WRITE. This setting allows anyone to use the console menus to modify any operational parameter. To protect the configuration of a switch from unauthorized modification, you should set a password to protect access to the console menus.

To enter a password, do the following:

1. Select Management Setup Menu from the Main Menu and press [Enter].
2. Select Console Login Configuration and press [Enter].
3. For the “ADMIN” user type, enter a password containing up to 11 alphanumeric characters. Note that the password is not case sensitive.

By factory default, there is no password configured. This means that at the login: prompt, all you have to do is type “admin” for the username and press [Enter] to gain READ/ WRITE access to the console menus. When you configure the password parameter, the factory default setting is deactivated and the new password governs access to the console menus.

If you forget your password, contact your Enterasys Networks Support Representative.

You are automatically logged out from the console menus based on the Lock-out Time setting in the Console Login Configuration Menu. A setting of “0” permits the console menus to remain available indefinitely.

Assigning an IP Address

To assign an IP address to the switch, do the following:

1. Select Management Setup Menu from the Main menu.
2. Select Network Configuration and then IP Configuration.
3. Highlight the IP address field and enter the IP address. Press [Enter].

The IP address is now set. The subnet mask is automatically set to correspond to the class of the address entered. If a different mask is used on the network, higlight Subnet Mask and enter the appropriate mask.

Checking Network Configuration Status

To check connection status for the network, do the following:

1. Select Device Control Menu from the Main Menu.
2. Select Port Information and press [Enter].

   If a network cable is properly connected to a port, the Link for the port reads UP. If no cable is connected to the port, or if the cable or port is faulty, the Link for the port reads DOWN.
3. If you see a DOWN status for a connected port, plug the cable into another port on the switch or try another cable.

Connecting via Telnet

You can connect to the VH-2402S2 switch from a remote location using the Telnet application. This application allows you to establish in-band access to the console menus.

To connect to a VH-2402S2 switch via Telnet, do the following:

1. Assign an IP address using the Network Configuration Menu.
2. Set a password using the Console Login Configuration Menu.
3. Login to the VH-2402S2 switch via Telnet using the configured IP address and the password.

Setting SNMP Management Access

Access to the VH-2402S2 switch through SNMP is controlled by community names. The community names set for the switch must match those used by the SNMP management station for successful communication to occur. Access for community names can be set to READ/WRITE or READ ONLY access. The default “Public” community name allows READ ONLY access to the device via SNMP, whereas the default “Private” community name allows READ/WRITE access.

The VH-2402S2 switch can send SNMP messages called traps to SNMP management stations when an important event occurs with the switch. The switch allows up to five destinations to be configured for these trap messages to be sent.

To configure SNMP access for the switch, do the following:

1. Select Management Setup Menu from the Main Menu.
2. Select SNMP Configuration Menu.
3. Select SNMP Communities from the menu. Enter the desired community names (you are permitted to enter from one to 20 characters) and set access to READ/WRITE or READ ONLY.
4. Select IP Trap Managers from the SNMP Configuration Menu.
5. Enter appropriate IP addresses for the Trap destinations.
6. For each Trap destination entered, a corresponding access community name should be entered.

Viewing Switch Statistics

To view switch statistics, do the following:

1. Select Network Monitor Menu from the Main Menu.
2. Select Port Statistics. Then select the stack unit, and port to display the main statistical counts for the port.
3. Select RMON Statistics. Then select the stack unit, and port to display detailed statistical counts for the port.
4. On any of the statistics screens, select Reset Counters to clear (zero) the displayed statistical counts and Refresh Counters to refresh (update) the displayed statistical counts.

Configuring Port Mirroring

You can mirror the traffic being switched on any port for the purposes of network traffic analysis and connection assurance. When Port Mirroring is enabled, one port becomes a monitor port for any other port within the stack. Note that the source and target ports must be configured within the same VLAN and be operating at the same speed. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

To configure port mirroring, do the following:

1. Select Device Control Menu from the Main Menu.
2. Select Mirror Port Configuration.
3. For the Mirror Source Port, select the stack unit and port number.
4. For the Mirror Target Port, select the stack unit and port number.
5. Set the Status field to ENABLED.
6. Connect a traffic analyzer or RMON probe to the mirroring port.

Downloading a Software Upgrade

You can upgrade the operational software in the VH-2402S2 switch without physically opening the switch or being in the same location. The software storage sector in the flash memory of the Management Module is reprogrammable, allowing you to easily download software feature enhancements and problem fixes to the switch from a local or remote location.

Software can be downloaded to the VH-2402S2 switch in two ways:

- Via the serial port. This procedure is an out-of-band operation that copies the software through the Management Module's serial port. This operation takes approximately 10 minutes and requires minimal configuration.
- Via TFTP download. This procedure uses a TFTP server connected to the network and downloads the software using the TFTP protocol. A TFTP download is much faster than a serial download, requiring only a few seconds, and can be used to upgrade a switch that is not physically proximate. The disadvantage is that this method requires a TFTP server and additional setup.

You can also upload new software using the Web management interface. See the Web Management Guide for more information.

Downloading Via the Serial Port

A serial download is the easiest method to upgrade the VH-2402S2 switch software, requiring the least amount of equipment and configuration.

To download new software via the serial port, do the following:

1. With the console port connected, reset the switch by powering the switch off and then on.
2. After the power-on hardware and software tests are complete, the system initialization screen displays the following message:.

   ```
   (D)ownload System Image or (S)tart Application: [S]
   ```

3. Press “D” to download system firmware. The following message appears:

   ```
   Select the Firmware Type to Download (1)Runtime
   (2)POST (3)Mainboard [1]:
   ```

4. Select “1” to download the agent software. The following messages appear:

   ```
   Your Selection: Runtime Code

   Download code to FlashROM address 0x02880000

   Change Baud Rate to 115200 and Press <ENTER> to
   Download.
   ```

5. Change your baud rate to 115200 bps and press [Enter]. Send the file using the XMODEM protocol from your computer application (the procedure varies depending upon the application used).

   When the XMODEM procedure finishes, the following messages are displayed:

   ```
   XModem Download to DRAM buffer area 0x00200000: ...
   SUCCESS !

   Verifying image in DRAM download buffer
   0x00200000... SUCCESS !

   Update FlashROM Image at 0x02880000 ... SUCCESS !

   (D)ownload another Image or (S)tart Application:
   [S] s

   Change Baud Rate to 19200 and Press <ENTER>.
   ```

6. Press “S” to start the user interface, change your baud rate to back to 19200 bps and press [Enter]. The user interface logon screen will then appear.

Downloading Via TFTP

To perform a TFTP download, you must first configure the VH-2402S2 switch. This consists of setting an IP address, if this has not already been done, and entering the IP address of the TFTP server and the name of the upgrade file. To set the switch IP address, select the Management Setup Menu from the Main Menu screen, then select Network Configuration.

To download switch software via TFTP, do the following:

1. Select Download Server IP Address from the TFTP Download Menu.
2. Enter the TFTP server IP address and press [Enter].
3. Select Download Filename and enter the file name to be downloaded from the TFTP server.

For a TFTP download, the path to the file must be included its name. For example, if the upgrade file name is filename.bin and it resides in the directory /usr/tftp on the TFTP server, then you must enter the TFTP file name as: "/usr/tftp/filename.bin".

4. If necessary, configure the address of an IP gateway to reach the server from the switch using the Gateway IP field in the Network Configuration: IP Configuration menu.
5. Configure the TFTP server by copying the download file from the upgrade disk to an appropriate directory and starting the server.
6. Select Process TFTP Download and press [Enter].

   To verify that the TFTP download has been successfully completed, note the software version level displayed on the Switch Information screen accessible from the System Information Menu. This number should match the version number that appears on the upgrade disk.

Configuring Spanning Tree Parameters

The VH-2402S2 switch supports the IEEE 802.1D Spanning Tree Protocol. This protocol allows redundant connections to be created between LAN segments for purposes of fault tolerance. Two or more physical paths between different segments can be created through the switch, with the Spanning Tree Protocol choosing a single path at any given time and disabling all others.

If the chosen path fails for any reason, a disabled alternative is activated, thereby maintaining the connection. See Appendix A, “Spanning Tree Concepts” on page 91 for further information on using the Spanning Tree Protocol in a network.

Configuring Spanning Tree parameters from their default can cause serious deterioration of network performance.

To configure Spanning Tree Parameters, do the following:

1. Select the Device Control Menu from the Main Menu.
2. Select the Spanning Tree Configuration Menu and then STA Bridge Configuration.
3. Turn the switch Spanning Tree operation on or off by setting the Spanning Tree Protocol field to ENABLED/DISABLED.
4. Form the Spanning Tree Configuration Menu, select STA Port Configuration.

   The Spanning Tree Port Configuration Menu displays. Change the parameters that display in this menu as required.

Configuring VLANs

A virtual LAN (VLAN) is a group of devices on one or more LANs that are configured such that they can communicate as if they were attached to the same wire. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

The most fundamental benefit of VLAN technology is the ability to create workgroups based on function rather than on physical location or media. For further information, see Appendix B, “Virtual LANs (VLANs)” on page 97.

To configure VLANs, do the following:

1. Select the Device Control Menu from the Main Menu.
2. Select 802.1Q VLAN Static Table Configuration Menu.
3. In the VID and VLAN Name fields, enter an ID number (1-2048) and a symbolic alphanumeric name (up to 8 characters) to indentify the VLAN.
4. Set the Status field to Active and then select Apply to save the settings.
5. From the Device Control Menu, select Port Assignment VLAN Configuration.
6. For each VLAN port member, set the PVID to the VLAN ID.
7. Select Apply to save the settings and return the 802.1Q VLAN Static Table Configuration screen.
8. Under Forbidden Egress Ports for each stack unit, enter a “1” to prevent a port from being automatically added to this VLAN via GVRP.

   Note that you can enable or disable GVRP for the stack from the Extended Bridge Configuration screen on the Device Control Menu.
9. To configure other VLANs, select New and press [Enter].

Configuring Class of Service

You can configure Class of Service parameters using the 802.1P Port Priority Configuration screen. This screen permits you to configure two priority levels for traffic being forwarded through the switch. During periods of congestion, Class of Service settings ensure that traffic which has been assigned high priority is forwarded through the switch ahead of normal priority traffic. For further information, see Appendix C, “Class of Service” on page 101.”

To configure Class of Service, do the following:

1. Select Device Control Menu from the Main Menu.
2. Select 802.1P Configuration, then 802.1P Port Priority Configuration.

3. For each stack unit, set individual port priorities by entering 0-3 for the low priority queue or 4-7 for the high priority queue.

   Note that the default for all ingress ports is zero.

Configuring Port Operation

You can configure switch ports for operational parameters such as auto-negotiation, duplex mode, port speed and flow control. The 100Base-FX fiber ports always operate in full duplex mode and 100Mbps speed. Therefore, these two parameters, along with auto-negotiation, are not configurable on these fiber ports.

To configure port operation, do the following:

1. Select Device Control Menu from the Main Menu.
2. Select Port Configuration and press [Enter].
3. Select the stack unit and port number to configure.
4. In the Admin column, select ENABLED. You can also disable the port due to abnormal behavior or for security reasons.
5. In the Flow Control column, select ENABLED to enable flow control or DISABLED to disable it. When enabled, the switch uses back pressure for half duplex and IEEE 802.3x for full duplex. These flow control methods can also be set directly by selecting BACK_PRESSURE or 802.3X. Note that flow control should not be used of the port is connected to a hub.
6. In the Speed and Duplex column, select AUTO to enable Auto-negotiation for the port, or select 1000_FULL, 1000_HALF, 100_FULL, 100_HALF, 10_FULL, or 10_HALF.

If Auto-negotiation is not enabled, the duplex mode and port speed needs to be configured.

Configuring the Unicast Address Table

The Unicast Address Table allows you to designate forwarding treatment through the switch for specific MAC addresses, allowing you to maintain the efficiency and security of your network. You can search for a specific MAC address, clear the entire table, or information associated with a specific address, or set the Aging Time for deleteing inactive entries. The switch learns addresses dynamically from incoming packets and builds a table of these addresses along with their associated ports. There are two types of MAC addresses in the forwarding table:

- Dynamic MAC addresses, which are dynamically learned and removed by the switch based on a time period defined using the Aging Time option.
- Static MAC addresses, which are entered manually, stored in nonvolatile memory and automatically placed in the address table.

There are five types of status that can be configured for each address in the table:

- Permenant, which means that the MAC address is in use and will remain so after the next switch reset.
- Delete On Reset, which means that the MAC address is in use and will remain so until the next switch reset.
- Invalid, which will remove the entry.
- Delete On Time Out, which means that the MAC address is in use and will remain so until it is aged out.
- Other, which means that the MAC address is in use but the conditions under which it will remain so differ from the preceding values.

To configure the Unicast Address Table, do the following:

1. Select Network Monitor Menu from the Main Menu.
2. Select Unicast Address Table.
3. As desired, set the Aging Time for the table, or view, search or clear entries by MAC address or VLAN ID.

To configure a specific MAC address in the table, do the following:

1. From the Network Monitor Menu, select Static Unicast Address Table Configuration.
2. For the MAC address, specify the VLAN ID, switch port and the Status (Permanent, Delete On Reset, Invalid, Delete On Time Out, or Other).
3. Highlight the Set field and press [Enter].

Setting a Default Gateway

The default Gateway parameter defines the IP address of a router or other network device to which IP packets are to be sent if destined for a subnet outside of that which the switch is operating.

To set a default gateway, do the following:

1. Select Management Setup Menu from the Main Menu.
2. Select Network Configuration and then IP Configuration.
3. In the field Gateway IP,enter the IP address and press [Enter].

Configuring BootP

The BootP protocol allows you to automatically configure the switch's IP address information. Enabling this feature greatly speeds up device configuration, especially when a large number of devices are installed.

A BootP server must be operating on the network and be properly configured for this option to work. When this option is enabled, the switch tries to obtain an IP address from the BootP server.

To configure BootP, do the following:

1. Select Management Setup Menu from the Main Menu.
2. Select Network Configuration and then IP Configuration.
3. In the IP State field, select BOOTP-GET-IP.

   This selection toggles between BOOTP-GET-IP and USER-CONFIG (the default setting).

Configuring Port Security

The port security feature allows each port to learn, or be configured with, a list of up to 200 MAC addresses that are authorized to access the network through that port.

To configure the port security, do the following:

1. Select Device Control Menu from the Main Menu.
2. Select Port Security Configuration and press [Enter].
3. Select the stack unit and port number to configure.
4. Highlight the field Mode, then select LEARNING. Select [Apply] and press [Enter] to start the learning process. The switch will start to add the source MAC address of all packets received on the port to the authorized MAC address list

   Or, select the field MAC and manually enter an address. Highlight [Add] and press [Enter] to add this address to the authorized list.

5. Highlight the Mode field again, then select STATIC.

6. Select [Apply] and press [Enter].

The switch will now drop packets from the port if the source MAC address does not match one of the addresses in the authorized MAC address list.

Configuring Port Trunks

You can configure up to five port trunks on a standalone switch, or up to 12 for an entire stack. Each trunk can combine two, three, or four ports, creating an aggregate bandwidth of up to 4Gbps when grouping gigabit ports. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail.

To configure the port trunks, do the following:

1. Select the Device Control Menu from the Main Menu.

2. Select Port Trunking Configuration.

3. Enter a Trunk ID number from 1 to 12 to identify the trunk.

4. Select up to four ports to configure as one trunk. You can configure up to five trunks per switch unit. The ports used in a trunk must all be of the same media type (RJ-45, 100 Mbps fiber, or 1000 Mbps fiber). The ports that can be assigned to the same trunk also have certain other restrictions.

   The RJ-45 ports used for each trunk must all be on the same internal switch chip. The port groups permitted include:

Group 1	Group 2	Group 3
1,2,3,4, 13,14,15,16	5,6,7,8, 17,18,19,20	9,10,11,12, 21,22,23,24

   Only two 100Mbps fiber ports can be configured as a trunk and these must be on the same module. 1000Base-SX/LX ports can be trunked together with any other like uplink ports in the stack.

   Note that ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.

5. For each Trunk ID, select Enable to enable the trunk.

   Note that it is advisable to enable the trunk prior to connecting any cable between the switches to avoid creating a loop.

When using port trunks, remember that:

- Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.

- To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

Configuring Broadcast Storm Control

The VH-2402S2 switch supports a broadcast control mechanism that prevents a high level of broadcast traffic from overwhelming the network. When enabled for a switch stack, the system monitors the level of broadcast traffic that passes through all ports in the stack. If the broadcast traffic level rises above the specified packet-per-second threshold, the broadcast-control mechanism will be employed.

1. Select Device Control Menu from the Main Menu.
2. Select BStorm Control Configuration and press [Enter].
3. Highlight the Threshold field and enter the packet-per-second threshold at which broadcast control will be employed (default is 200 pps).
4. Highlight the Averaging Interval field and set the time period for which the control mechanism will be active (200 ms, 500 ms, 1, 5, or 10 seconds; default is 1 second).
5. Highlight the Broadcast Control field and select ENABLED.
6. Select <APPLY> and press [Enter].

The broadcast control mechanism drops all broadcast packets from the stack for the specified time period. The control mechanism will be continuously re-activated after each time period until the number of received broadcasts falls back below the packet-per-second threshold.

Saving and Restoring the Switch Configuration

After completing your switch configuration, you can save all the settings to a file on a TFTP server. This file can be later downloaded to the switch to restore the switch's settings.

To save a configuration file to a TFTP sever, do the following:

1. From the console interface Main Menu, select Management Setup Menu and then Configuration Save & Restore.
2. Select Upload Server IP Address under the section Configuration Upload.
3. Enter the TFTP server IP address and press [Enter].
4. Select Upload Filename and enter the file name to be uploaded to the TFTP server.
5. Select Process TFTP Upload and press [Enter].

To restore a switch configuration from a file on a TFTP server, do the following:

1. From the console interface Main Menu, select Management Setup Menu and then Configuration Save & Restore.
2. Select Download Server IP under the section Configuration Download.
3. Enter the TFTP server IP address and press [Enter].
4. Select Download Filename and enter the file name to be downloaded to the switch.

For a TFTP download, the path to the file must be included in its name. For example, if the configuration file name is filename.cfg and it resides in the directory /usr/tftp on the TFTP server, then you must enter the TFTP file name as: "/usr/tftp/filename.cfg."

5. Select Process TFTP Download and press [Enter].

4. SNMP MANAGEMENT

The SNMP Protocol

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for the purpose of managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, routers, and host computers. SNMP is typically used to configure these types of devices for proper operation in their network environment, as well as to monitor them to evaluate their performance and detect potential problems.

Managed entities supporting SNMP typically contain software, which runs locally on the device and is referred to as an agent. In Figure 4-1, software running on a VH-2402S2 switch functions as an agent, monitoring and controlling the functionality of the switch.

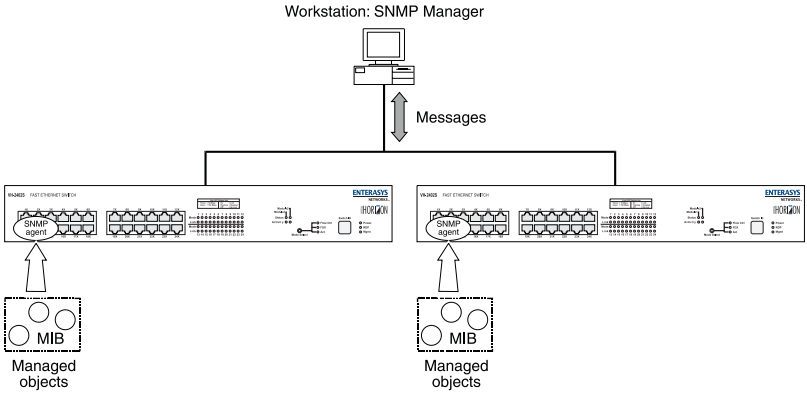

Figure 4-1. VH-2402S/VH-2402S2 Switches Managed by an SNMP Management Workstation

A defined set of variables, referred to as managed objects, is maintained by the agent and used to manage the device. These objects are defined in a Management Information Base (MIB) which allows for a standard presentation of the information controlled by the agent over the network.

The software used to access the information maintained by the SNMP agents across a network is referred to as the SNMP Manager, and typically runs on a workstation.

The SNMP manager software uses a MIB specification, equivalent to that which the agent maintains, to read and write objects controlled by the agent for purposes of configuring and monitoring the device. SNMP defines the format of the MIB specifications and the protocol used to access this information.

There are three main operations defined in SNMP:

- GET operations read information from the managed device, such as those used to obtain status or statistical data.
- SET operations change a functional parameter on the device, such as those used to configure Port Speed or to initiate a software download. GET and SET operations are initiated only by the manager software, and result in a response by the agent.
- TRAP operations allow the agent to send an unsolicited message to the manager. This operation is typically used as an alert of a potential problem or a change of status with the device. The Trap Destination parameter in the SNMP Configuration Menu is used to configure the IP addresses of the SNMP Manager to which switch trap messages are sent.

MIB Objects

A number of standard MIB specifications have been defined for managing network equipment. SNMP compliant devices typically support one or more standard MIBs defined by the Internet Engineering Task Force (IETF), in the form of Request for Comments (RFC) documents.

These MIBs provide a common method of managing devices, such as hubs and switches, and network interfaces, such as Ethernet and token ring. The primary standard MIB, referred to as MIB-II, provides an overall view of the managed agent and must be supported, at least in part, by all SNMP agents. In addition, proprietary MIB extensions are defined by commercial vendors for managing device-specific functions of their products.

The VH-2402S2 switch supports six standard MIBs:

- RFC 1213 - Management Information Base for Network Management of TCP/IP based Internets (MIB-II)
- RFC 1573 - Evolution of the Interfaces Group of MIB-II
- RFC 1643 - Definitions of Managed Objects for the Ethernet-like Interface Types (Ethernet-Like MIB)
- RFC 1493 - Definitions of Managed Objects for Bridges
- RFC 1757 - Remote Network Monitoring Management Information Base
- RFC 2674 - Extended Bridge Management Information Base

The VH-2402S2 switch also supports Enterasys Networks proprietary MIB extensions.

RFC 1213 (MIB-II)

RFC 1213 provides management of system-level parameters, including TCP/IP protocol-related statistics, IP addressing, and interface statistics for each switch port. MIB-II is the standard MIB defined by RFC 1213. All agent devices operating SNMP are required to support at least part of MIB-II.

This MIB reports information about the protocols and network interfaces supported on the agent itself, as well as other general information. The MIB is divided into a number of groups, each of which corresponds to a specific protocol or set of information. Some groups are defined in other RFC documents.

The groups specifically defined in RFC 1213 and supported by the VH-2402S2 switch system software are as follows:

- System – General information about the agent system
- Interfaces – Information about the network interfaces of the system
- Address Translation – Interface address information, both MAC level and network (IP) level
- IP – Statistics and information related to the IP protocol
- ICMP – Statistics and information related to the ICMP protocol
- TCP – Statistics and information related to the TCP protocol
- UDP – Statistics and information related to the UDP protocol
- Transmission – Statistics and information related to the physical network medium to which the system interfaces (e.g. Ethernet, token ring, etc.).
- SNMP – Statistics and information related to the SNMP protocol

RFC 1573 (Interfaces Evolution MIB)

RFC 1573 clarifies and extends the managed objects of the “Interfaces” group of MIB-II. This MIB takes account of the evolution in interface types and speeds employed in today’s networks.

RFC 1643 (Ethernet-Like MIB)

RFC 1643 provides management and monitoring for the Ethernet-specific aspects of each port on the switch. This is the Ethernet-specific statistics subgroup of the MIB-II Transmission group. This group provides a set of statistics related to Ethernet’s physical level operation. Specifically, error and collision-related statistics are presented.

RFC 1493 (Bridge MIB)

RFC 1493 is a group defined under MIB-II. This MIB deals with the operation of the system as an 802.1D-compliant bridge. Areas of functionality supported by this group include Spanning Tree and forwarding table information and configuration.

RFC 1757 (RMON MIB)

RFC 1757 is a group defined under MIB-II. This MIB provides management for the RMON aspects of the switch. The VH-2402S2 switch supports four of the nine groups of RMON defined for Ethernet networks on a per port basis.

RFC 2674 (Extended Bridge MIB)

This MIB includes the set of managed objects as defined in the RFC 2674 standard. This MIB provides management for traffic classes, multicast filtering, and VLAN aspects of the switch.

Enterasys Networks Proprietary MIB Extensions

Areas of switch functionality not covered by the standard RFC MIBs are specified in the Enterasys Networks private MIB. This MIB definition is specified separately from MIB-II. Areas covered in this MIB include various system, switch, and port level information.

Compiling MIB Extensions: Enterasys Networks Website

The MIBs supported by the VH-2402S2 switch must be compiled into the SNMP network management platform before the switch can be managed. The supported MIBs are available using the Enterasys Networks website at:

http://www.enterasys.com

The four standard MIB specifications listed above with which the VH-2402S2 switch is compliant are generally available with the SNMP management platform.

APPENDIX A. SPANNING TREE CONCEPTS

General

The IEEE 802.1D Spanning Tree Protocol resolves the problems of physical loops in a network by establishing one primary path between any two switches in a network. Any duplicate paths are barred from use and become standby or blocked paths until the original path fails, at which point they can be brought into service.

Spanning Tree Features

The VH-2402S2 switch meets the requirements of the Spanning Tree Protocol (STP) by performing the following functions:

- Creates a single spanning tree from any arrangement of switching or bridging elements.

The term "switch" is used as an equivalent to "bridge" in this document.

- Compensates automatically for the failure, removal, or addition of any device in an active data path.
- Achieves port changes in short time intervals, which establishes a stable active topology quickly with a minimum of network disturbance.
- Uses a minimum amount of communications bandwidth to accomplish the operation of the Spanning Tree Protocol.
- Reconfigures the active topology in a manner that is transparent to stations transmitting and receiving data packets.
- Manages the topology in a consistent and reproducible manner through the use of Spanning Tree Protocol parameters.

Spanning Tree Protocol in a Network

Figure A-1 illustrates the use of three VH-2402S2 switches to establish an effective Spanning Tree configuration. Switches A, B and C are connected together in a redundant topology (more than one path between two points). If the connection between A and B goes down, the link between A and C becomes active, thereby establishing a path between A and B through switch C. Additionally, if the connection between B and C goes down, the link between A and C becomes active, establishing a path between B and C through switch A.

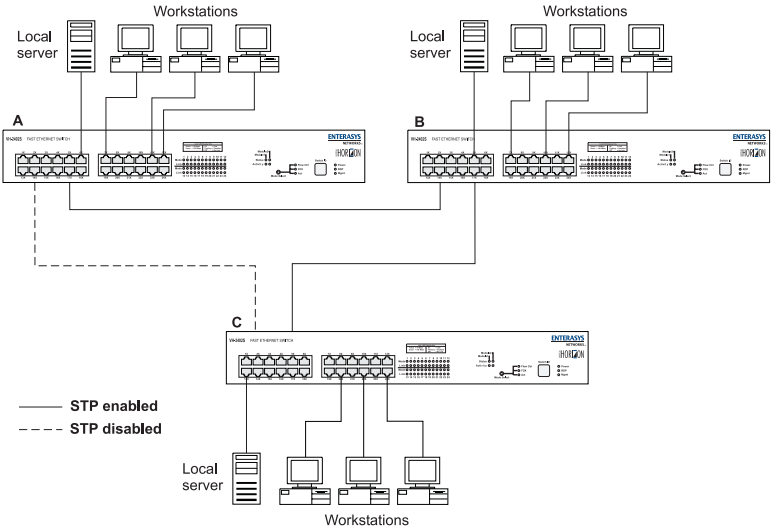

Figure A-1. Spanning Tree Using VH-2402S2 Switches

Spanning Tree Protocol Parameters

Several configuration parameters control the operation of the Spanning Tree Protocol. Table A-1 describes the parameters and lists the VH-2402S2 switch default settings for each parameter.

You can cause serious network performance degradation if you do not fully understand Spanning Tree concepts. Be sure to consult personnel experienced with this process prior to configuring Spanning Tree parameters.

Table A-1. Spanning Tree Protocol Defaults

Parameter	Description	Default Value
Bridge Group Address	Unique MAC group address, recognized by all bridges in the network.	
Bridge Identifier	Identifier for each bridge. This parameter consists of two parts: a 16-bit bridge priority and a 48-bit network adapter address. Ports are numbered in absolute numbers starting from 1 regardless of their bridge attachment. The network adapter address is the same address as the first port of the bridge.	32768 (bridge priority)
Port Identifier	Port Identifier Identifies each port of each bridge, with an incremental default value given for each port.	
	Port 1 -32768 Port 9 -32776 Port 17 -32784	
	Port 2 -32769 Port 10 -32777 Port 18 -32785	
	Port 3 -32770 Port 11 -32778 Port 19 -32786	
	Port 4 -32771 Port 12 -32779 Port 20 -32787	
	Port 5 -32772 Port 13 -32780 Port 21 -32788	
	Port 6 -32773 Port 14 -32781 Port 22 -32789	
	Port 7 -32774 Port 15 -32782 Port 23 -32790	
	Port 8 -32775 Port 16 -32783 Port 24 -32791	
Port Priority	Indicates the priority of a specific port in relation to other ports.	128
Cost Component of Each Port	The Spanning Tree Protocol calculates and ensures that an active topology generates minimal cost paths. A value of 100 is generally used for 10Mbps Ethernet networks, a value of 19 for 100Mbps Fast Ethernet, and a value of 4 for 1000Mbps Gigabit Ethernet.	19

For detailed information on the operation of the Spanning Tree Protocol, consult Section 4 of IEEE Standard 802.1D, ISO/IEC 10038:1993.

Spanning Tree Protocol Operation

When the Spanning Tree Protocol is enabled for the first time or when there is a change in the network topology, such as a failure or the addition or removal of a component, the Spanning Tree Protocol automatically sets up the active topology of the current network.

Communicating Between Bridges

Periodically, all devices running the Spanning Tree Protocol on a network transmit packets to each other “in care of” the Bridge Group Address which all bridges share. When a bridge receives a frame sent to the Bridge Group Address, the bridge’s Spanning Tree Protocol processes the packet. Application software and other LAN segments ignore the packet. Bridges communicate between each other in order to determine the Root Bridge.

Selecting a Root Bridge and Designated Bridges

During communication between bridges, one bridge is determined to have the lowest bridge identifier. This bridge becomes the Root Bridge.

After the Root Bridge has been selected, each LAN segment looks for the bridge that has the lowest cost relative to the Root Bridge. These bridges become Designated Bridges.

Selecting Designated Ports

Each Designated Bridge selects a Designated Port. This port is responsible for forwarding packets to the Root Bridge.

Handling Duplicate Paths

When the active topology of the network is determined, all packets between any two nodes in the network use only one path. Where a duplicate path exists, the non-designated port is put into a blocking state.

Remapping Network Topology

If there is a change in the network topology due to a failure or the removal or addition of any active components, the active topology also changes. This may trigger a change in the state of some blocked ports.

There are five (5) states that the ports can be in for spanning tree:

- Blocking: A port in this state does not participate in the transmission of frames, thus preventing duplication arising through multiple paths existing in the active topology of the bridged LAN.
- Listening: A port in this state is preparing to participate in the transmission of frames. The transmission of frames is temporarily disabled in order to prevent temporary loops, which may occur in a bridged LAN during the lifetime of this state as the active topology of the bridged LAN changes.
- Learning: A port in this state is preparing to participate in the transmission of frames.
- Forwarding: A port in this state is participating in the transmission of frames.
- Disabled: A port in this state does not participate in the transmission of frames or the operation of the spanning tree process.

APPENDIX B. VIRTUAL LANS (VLANS)

VLANs and Frame Tagging

The VH-2402S2 switch supports IEEE 802.1Q-compliant virtual LANs (VLANs). This capability provides a highly efficient architecture for establishing VLANs within a network and for controlling broadcast/ multicast traffic between workgroups. Central to this capability is an explicit frame tagging approach for carrying VLAN information between interconnected network devices.

With frame tagging, a four byte data tag field is appended to frames that cross the network. The tag identifies which VLAN the frame belongs to. The tag may be added to the frame by the end station itself or by a network device, such as a switch. In addition to VLAN information, the relative priority of the frame in the network can specified by the tag (see Appendix C, “Class of Service”).

VLANs provide greater network efficiency by reducing broadcast traffic, but also allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security, since traffic must pass through a Layer 3 switch or a router to reach a different VLAN.

The VH-2402S2 switch enables a switch to support the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GARP/GVRP protocol
- 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
- Two-level priority tagging
- Port trunking with VLANs

VH-2402S2 VLAN Configuration

VLAN operation on the VH-2402S2 switch is enabled by default. Therefore, all frames are transferred internally through a switch with a VLAN tag. This tag may already be on the frame entering the switch, or added to the frame by the switch. VLAN information already existing on frames entering the switch is automatically handled by the switch. The VH-2402S2 learns VLAN information from tagged frames and appropriately switches frames out the proper ports based on this information. The configuration of VLANs for frames entering the switch without tags must be made by the user of the switch. This configuration can be made either through the console interface or via SNMP.

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN groups it will participate in. By default all ports are assigned to VLAN 1 as untagged ports. You should add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and the device at the other end of the link also supports VLANs. Then assign the port at the other end of the link to the same VLANs. However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

Port-based VLANs are 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 and flooding decisions, the switch learns the relationship of the MAC address to its related port—and thus to the VLAN—at run-time.

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.
- 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 must connect them using a router or Layer 3 switch.

Forwarding Tagged/Untagged Frames

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port's default VID. The default PVID is VLAN 1, but this can be changed (see "Port Assignment VLAN Configuration" on page 48).

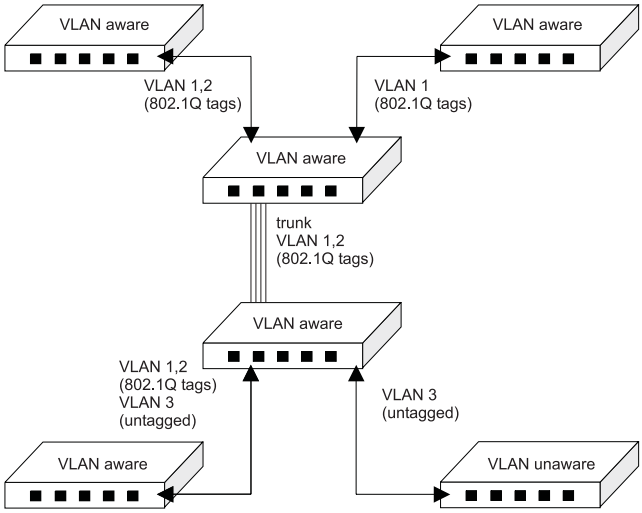

Figure B-1. Multi-Switch VLAN Configuration

Automatic VLAN Registration

GVRP defines a system whereby the switch can automatically learn the VLANs each endstation should be assigned to. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN standard, 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 endstation requests.

Forwarding Traffic with Unknown VLAN Tags

The VH-2402S2 switch only supports 256 VLANs with VLAN IDs ranging from 1 to 2048, but the IEEE 802.1Q VLAN standard allows for VLAN IDs from 1 to 4094. Therefore, if a switch is attached to endstations that issue VLAN registration requests, it will have to forward unknown VLAN tags. This traffic can only be propagated to the rest of the network if automatic VLAN registration is enabled on the switch.

APPENDIX C. CLASS OF SERVICE

Class of Service support on the VH-2402S2 switch allows you to assign mission-critical data a higher priority through a switch by delaying less critical traffic during periods of congestion. Higher priority traffic through a switch is serviced first before lower priority traffic. The Class of Service capability of the VH-2402S2 switch is implemented by a priority queuing mechanism. Class of Service is based on the IEEE 802.1p standard specification and allows you to define two priorities of traffic on each switch port:

- high
- normal

As traffic enters the switch, it is assigned to one of the two priority levels according to information located in the 802.1Q header tag of the frame (see Appendix B, “Virtual LANs”) or according to the incoming port number. Frames are then placed into one of two transmit queues on the outbound switch port based on their priority level. Frames on the high priority queue are transmitted first; when that queue empties, traffic on the normal priority queue is transmitted. When priority queuing is being used, each frame that passes through the switch contains a priority level in its header tag. The priority information may already exist in incoming frames, or be assigned by the switch. The determination of individual frame priority is based on the following rules:

1. Incoming tagged frames contain a priority level (range: 0-7)
2. Incoming non-tagged frames are assigned a preconfigured default priority level based on their incoming port (range: 0-7). The assignment of priority per port is done via management using the console interface or via SNMP. See “Configuring Traffic Classes” on page 55.
3. Priority levels of frames are compared against a preconfigured global priority threshold setting. Those frames with levels equal to or above the threshold are designated high priority traffic; those frames with levels below the threshold are designated normal priority traffic. The default setting for the threshold parameter is: 4 and above = High Priority, 3 and below = Normal Priority.

Properly configured, the Class of Service mechanism assures that during congestion, the highest priority data does not get delayed by normal priority traffic. The tagged header in the frame governs individual frame priority.

Figure C-1 shows priority queuing operating within a switch. Frames entering the switch through ports 1 and 4 are tagged as normal traffic and placed in a normal priority queue on the outbound port. Frames entering through ports 2 and 5 are tagged as high priority traffic and placed in a high priority queue on the outbound port. Priority queuing can be configured using the console interface or via SNMP.

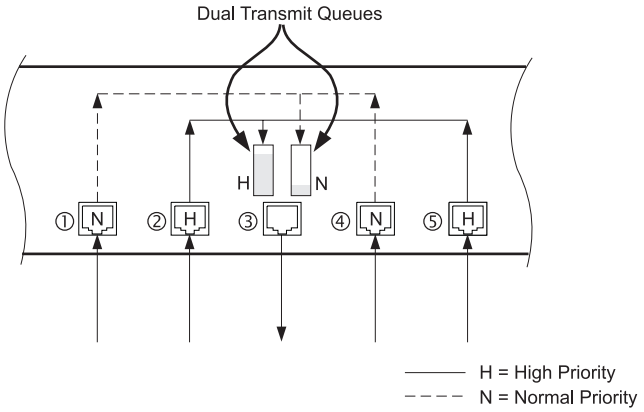

Figure C-1. Class of Service Example

APPENDIX D. IP MULTICAST FILTERING

IGMP Snooping and IP Multicast Filtering

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast router/switch. The protocol's mechanisms allow a host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

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 responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer-3, multicast routers use this information, along with a multicast routing protocol, to support IP multicasting across the Internet.

IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with forwarding multicast traffic from the local router/switch to group members on directly attached subnetwork or LAN segment.

The VH-2402S2 switch supports IP Multicast Filtering by:

- Passively snooping on the IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members, and
- Actively sending IGMP Query messages to solicit IP Multicast group members.

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

The VH-2402S2 switch, with IP multicast filtering capability, not only passively monitors IGMP Query and Report messages; it can also actively send IGMP Query messages to learn locations of multicast routers/switches and member hosts in multicast groups within each VLAN.

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, an external IP multicast router is needed if IP multicast packets have to be routed across different subnetworks.

INDEX

T

U

V

W

X