FCC Compliance Statement

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the instructions provided with the equipment, may cause interference to radio and TV communication. The equipment has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If you suspect this equipment is causing interference, turn your Ethernet Switch on and off while your radio or TV is showing interference, if the interference disappears when you turn your Ethernet Switch off and reappears when you turn it back on, there is interference being caused by the Ethernet Switch.

You can try to correct the interference by one or more of the following measures:

1. Reorient the receiving radio or TV antenna where this may be done safely.
2. To the extent possible, relocate the radio, TV or other receiver away from the Switch.
3. Plug the Ethernet Switch into a different power outlet so that the Switch and the receiver are on different branch circuits.

If necessary, you should consult the place of purchase or an experienced radio/television technician for additional suggestions.

Caution: Do not use a RJ-11 (telephone) cable to connect your network equipment.

Important Safety Instructions

1. Read all of these instructions.
2. Save these instructions for later use.
3. Follow all warnings and instructions marked on the product.
4. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
5. Do not use this product near water.
6. Do not place this product on an unstable cart or stand. The product may fall, causing serious damage to the product.
7. The air vent should never be blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
8. This product should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
9. This product is equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug will only fit into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your outlet. Do not defeat the purpose of the grounding type plug.
10. Do not allow anything to rest on the power cord. Do not place this product where persons will walk on the cord.
11. If an extension cord is used with this product, make sure that the total ampere ratings on the products into the extension cord do not exceed the extension cord ampere rating. Also make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
12. Never push objects of any kind into this product through air ventilation slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
13. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to service personnel.

Table of Contents

Chapter 1 Introduction

Thank you for your purchase of The GSW-1600TXM 16 Port 10/100Mbps SNMP Switch. Through modular upgrades, the switch offers flexible port density and optional Gigabit Ethernet uplinks. It is also equipped with a MII slot in the rear of the chassis, which offers an alternative connection for users, such as 100BaseFX.

In addition to the traditional console and telnet interface, the Switch provides a user-friendly Web browser interface. With an on-board HTTP server and Java implementation, users can access the box with the use of popular browsers such as Netscape Navigator and Microsoft I.E. [1] The expandable 16-port Ethernet Switch also supports firmware upgrades using the TFTP protocol.

The following topics briefly describe the functional overview of this scalable 10/100/1000 Ethernet Switch:

- Features
- Front/Rear Panel Description
- LED Definitions
- Uplink Pushbutton
- Management

1.1 Features

- 16 10BaseT/100BaseTX auto-negotiation UTP ports
- Two expansion slots for added modular connectivity
- 1-Port 1000Base-SX fiber module support
- 4-Port 100Base-FX fiber module support
- 8 Port 10/BaseT/100BaseTX module support
- Back pressure flow control for half-duplex operation
- 802.3x flow control for full duplex operation
- 802.1Q based VLAN
- QoS through dual priority and support for 802.1p
- 12K-entry address cache
- Hardware assisted RMON statistic collection
- Port mirroring
- Extensive system LED and per port LEDs
- Console port (VT100)
- Telnet remote login
- Web-based management
- On-Board HTTP Server
- Network boot/software upload via TFTP
- MII expansion slot for manufacturer's available modules
- IGMP support with software upgrade
- SNMP based network management

[1] Netscape Navigator 4.0 and IE 4.01 or higher required

- MIB II (RFC1213)
- Ethernet interface MIB (RFC1643)
- Bridge MIB (RFC1493)
- Enterprise MIB
- 4-Group RMON (RFC 1757)

- Transparent Bridge (IEEE 802.1d)
  - Spanning tree protocol
  - Hardware assisted address learning
  - Auto aging
  - Static address entry

1.2 Front Panel Descriptions

The front panel (see Figure 1-1) contains all the Ethernet ports, expansion panels, and LEDs. There is one System LED, and three LEDs for each port on the front panel. Detailed definitions can be found in the next section.

Figure 1-1: Front Panel

1.3 Rear Panel Descriptions

Figure 1-2: Rear Panel

The rear panel (see Figure 1-2) contains an AC power receptacle, power switch, MII panel, and a console port. The MII shares a port at the switch fabric with Port 16. With a MII module plugged in, port 16 is disabled automatically.

1.4 LED Definitions

1.4.1 System LED

A LED is used to show the general operating status of the system.

- **System**:

Off	System is not powered up
Green	System is in operation
Yellow	System is in boot mode
Red	System fails during the initialization

The normal sequence after power-on or system reset is Green (Initialization success), then Yellow (booting up applications) and lastly Green again meaning the system is ready.

1.4.2 Port LEDs

There are three LEDs for each port. Their definitions are summarized as follows:

- **10/100Mbps**

Off	10Mbps (Default)
Solid Green	100Mbps

- **Full/Col**

Off	Half Duplex operation (Default)
Solid Green	Full Duplex operation
Blinking Amber	Collisions detected for Half Duplex operation.

- **Link/Act**

Off	Port is link down
Solid Green	Port is link up and no traffic
Blinking Green	Port is link up and with traffic

1.4.3 MII Module LED

There is a MII indicator LED near port 16. When a MII module is installed in the rear of the switch, the LED will light up and port 16 will be disabled.

- **100 Base-FX**

Off	No MII module installed
Solid Green	A MII module is installed (Port 16 will be disabled)

1.5 Uplink Pushbutton

There is a pushbutton near Port 1 on the front panel. The pushbutton provides a selective uplink capability. (Reference Appendix B: Networking Connection)

- **Uplink** When the pushbutton is pressed down, Port 1 provides a crossover connection to the networks

- **Normal** When the pushbutton is released, Port 1 provides a straight-through connection to the networks

1.6 Management

There are different methods by which a user can manage the Switch:

1.6.1 Web-Based Interface

Currently, users can configure the switch, monitor the LED panel, and display the statistics graphically with the Netscape Navigator browser version 4.0 or higher and Microsoft IE version 4.01 or higher. With Internet access, users can link directly to the local switch's home page. The Web-based interface is implemented using Java, which provides true interactive management. Detail description is in the WEB-BASED MANAGEMENT chapter.

1.6.2 Menu Driven Interface via Console or Telnet

Users can also access the switch in a more traditional way by connecting a PC or terminal to the serial console port or by Telnet across the network. The user interface is menu driven so users need not follow certain command syntax. The menus are organized in a manner similar to the web-based interface. Detail description is in the CONSOLE INTERFACE chapter.

1.6.3 SNMP Network Management Platforms

Since the switch supports SNMP, users can manage the Switch with an SNMP-compatible management station running platforms such as HP OpenView. It also supports a comprehensive set of MIB extensions along with MIB II, Ethernet MIB, the 802.1d bridge MIB, and the 4-group RMON.

SNMP v.1 is implemented. The SNMP agent decodes the incoming SNMP messages and responds to these requests with MIB objects that are stored in the database. For the statistics and counters of MIB Objects, the SNMP agent periodically (every 5 seconds) updates the MIB Objects.

1.6.4 MIBs

The system supports the following MIBs:

1. MIB II
2. Ethernet Interface MIB
3. Bridge MIB
4. 4 groups RMON
   - The Ethernet Statistics Group
   - The Ethernet History Group
   - The Alarm Group
   - The Event Group
5. Enterprise MIB
   - CommGroup : Allows users to configure the community database
   - HostGroup : Allows users to configure the hosts
   - MiscGroup : Allows users to configure miscellaneous items
   - SpanGroup : Allows users to configure the Spanning Tree
   - ConfigGroup : Allows users to configure the system

Chapter 2 Installation

This chapter provides the following information:

- Package Contents
- Installation
- Password Protection
- IP Assignment
- SNMP Host Access

2.1 Package Contents

The GSW-1600TXM 16 Port 10/100Mbps SNMP Switch package contains the following:

- User's Manual
- One AC Power Cord
- One null modem cable
- One 10/100/1000 Fast Ethernet Switch
- Four self-adhesive standoffs
- Two rackmount brackets and screws

If any of these items are missing, contact your dealer immediately.

2.2 Installation

Installation must be done using a RS232 connection to a computer. It is recommended that the switch be kept off the network until proper IP settings have been set. Install and setup the system in the following manner:

1. Mount switch in a rack or on a shelf system
2. Plug power cord into the back of unit
3. Attach the null modem cable between the RS232 port and a COM port on the PC
4. Setup a HyperTerminal (or equivalent terminal program) in the following manner:
   - Choose the appropriate COM port (COM1, COM2, etc)
   - Set the data rate to 9600 Baud
   - Set data format 8 data bits, 1 stop bit and no parity
   - Set flow control to NONE
   - In setting under Properties, choose VT100 for Emulation mode
   - **Select Terminal keys for Function, Arrow and Ctrl keys make sure the setting is for Terminal keys, NOT Windows keys**
5. Now that terminal is setup correctly, power on the switch (boot sequence will display in terminal)

2.3 Password Protection

If the password option is not turned on and set, ANYONE from the network can telnet into the unit and make changes to the configuration.

To set a password, from the Main menu:

1. Choose System Manager (when highlighted, hit enter to confirm your choice)
2. Choose General
3. Choose Password Administration
4. Now enter your password, hitting Enter when done
5. Enter the password again to confirm, hitting Enter when done
6. Press Ctrl-W to save

Note: If you enable password protection without setting your own password, the default password is "switch"

2.4 IP Assignment

IP address assignment:

1. From the Main Menu, choose System Manager (hitting enter to confirm your highlighted choice)
2. In the first field enter the proper IP address for this system (consult your network administrator)
3. Enter the address of the default gateway for the network to which the switch is attached
4. Finally enter the appropriate network mask for this network (again consult your network administrator)
5. Press Ctrl-W when done to save these changes
6. After making IP changes, the system needs to be reset. Press ESC twice to return to the Main Menu
7. Go to System Manager/General/System Administration
8. Select Reset (it will ask to confirm the reset)

2.5 SNMP Host Access

When the reset is complete the box should be seen on the network. If not, check the IP information again with your network administrator to ensure that all the data is correct. By default, any PC on the network can manage the switch via the Web Interface. However, if this is not desired, you may enable Host Authorization and then only hosts that are listed in the SNMP Host Table may access the box. To do so:

1. Choose System Manager from the Main Menu.
2. Next choose SNMP.
3. Enable Host Authorization by hitting space when the word "Host Authorization: Disable" is highlighted.
4. Then select Host Table.
5. Enter the host name and IP address. Repeat this for as many hosts as necessary. Enter 'WebInterface' for the community string. Hit space over 'Disabled' until the status shows 'Active'

6. When done entering hosts, press Ctrl-W to save this data.

For other management tasks, please refer to next two chapters.

Chapter 3 Web-Based Management

Web-Based Management allows Switch configuration changes to be made using an Internet Web browser. This interface also allows for system monitoring of the Switch.

This chapter contains the following:

- Configuration
- Features
- Web Pages
- System Manager
- General
- System Information
- Software Download
- Password Administration
- System Administration
- IP
- SNMP
- Bridge
- VLAN
- Mirroring
- RMON
- Port Manager
- VLAN Membership
- MIB Viewer

3.1 Configuration

The management function of this interface runs as an unsigned Java applet. As a result, your browser's security setting should be set as following:

- For Netscape 4 or later:
    1. Click on Edit
    2. Pick up Preferences item
    3. Select the Advanced category
    4. Make sure Enable Java is checked
    5. Make sure Enable JavaScript is checked
    6. Press OK
- For Internet Explorer 4:
    1. Click on View
    2. Pick up Internet Options
    3. Select the Security tab
    4. Set Zone to Local Intranet
    5. Click Add Sites, click Advanced and add the IP address of the switch to the zone
    6. Set the security level to Custom
    7. Press the Setting… button

8. Scroll down and set Java permissions to Custom
9. Press the Java Custom Settings button
10. Select the Edit Permissions tab
11. Set Run Unsigned Content to Enable
12. Press OK for all open dialog windows

- For Internet Explorer 5:
    1. Click on Tools
    2. Pick Internet Options
    3. Select the Security tab
    4. Select Local Intranet (click on the icon)
    5. Click on Sites, click Advanced and add the IP address of the switch to the zone
    6. Click on Custom Level
    7. Scroll down and set Java Permissions to Custom
    8. Press the Java Custom Settings button
    9. Select the Edit Permissions tab
    10. Set Run Unsigned Content to Enable
    11. Press OK for all open dialog windows

3.2 Features

There are features and characteristics of the web interface whose functionality and meanings are consistent throughout and worth mentioning.

- Easy to change folders for intuitive navigation
- Informational messages will print out at the bottom of the screens
- Error messages will be printed in red

Buttons featured are:

- Refresh: Pulls that screen's data from current values on the system
- Submit: Submits change request to system and refreshes screen data
- Add: Adds new entries to table information and refreshes screen data
- Remove: Removes selected entries from table and refreshes screen data

3.3 Web Pages

The arrangement of the Switch homepage consists of traditional web site hyperlinks for associated information and Java windows for system management.

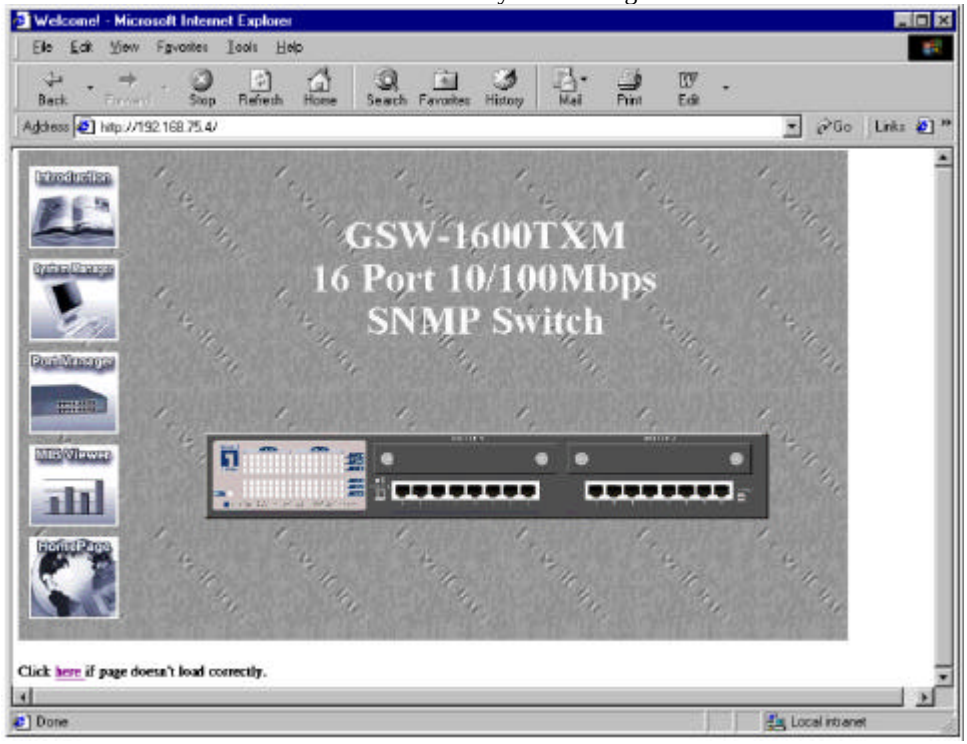


Figure 3-1: Web Interface front page

Upon connecting to the switch via a web browser (i.e. Netscape Navigator), a login screen will appear prompting for an administrator password. (Figure 3-2) The User Name will always be "root". Enter the password to access the switch's management mode. Once the password is entered correctly, the front page will appear (Figure 3-1). If the LEDs on the web page do not show up as green, the Java settings for the web browser is not set up correctly. Section 3.1 covers how to correctly setup Java for the web interface.

Figure 3-2 : Password Screen

After the password is entered you will see the main menu screen. (Figure 3-1)

Note: If password protection is enabled (using the console) without setting your own password, the default password is "switch".

There are five system icons that are available:

- Introduction
- System Manager
- Port Manager
- MIB Viewer
- Home Page

3.4 Introduction

The Introduction will explain the proper procedure for setting up the web interface. Make sure that the Java settings for your web browser have been setup correctly. If the Java is not set up correctly the web page will not work correctly.

3.5 System Manager

The system manager contains all system operations and general information. It is organized with several sub-folders:

- General — General system information and administration
- IP — IP parameters
- SNMP — Community table and host table management
- Bridge — Spanning tree and transparent bridging operations
- VLAN — VLAN configuration

- Mirroring Port Mirroring configuration
- RMON View Ethernet statistics, logs, and messages

3.5.1 General

Under the General folder, there are several sub-folders:

- System Information
- Software Download
- Password Administration
- System Administration

3.5.1.1 System Information

The System Information screen (see Figure 3-3) gives you helpful information about your system. The Media Access Control (MAC) address and the System Description are not configurable.

There are three fields that are site specific and can be modified by the system administrator:

- The local system name
- System administrator's name and contact information
- Physical location of the system

Notice that there are two buttons, Submit and Refresh, in the lower part of the window. The Refresh button is used for reloading values while the Submit button is for saving values to the Switch.

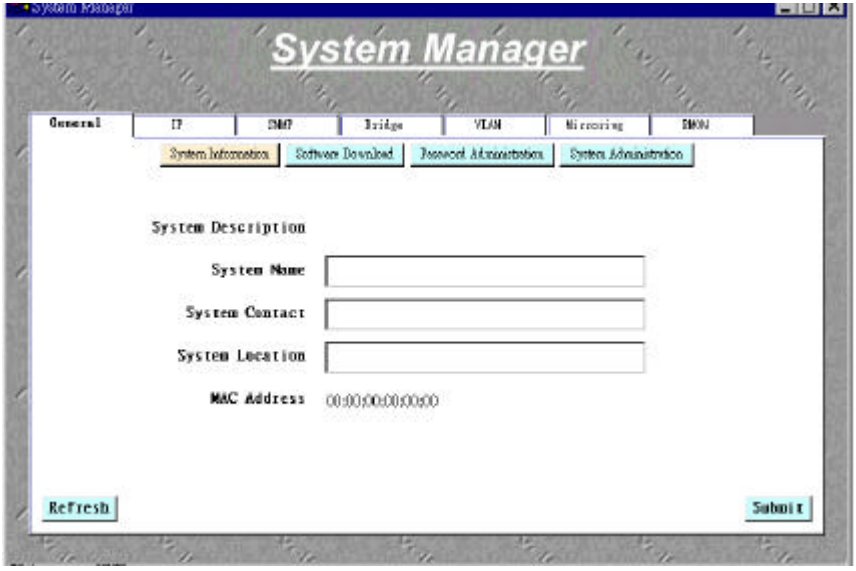


Figure 3-3: General: System Information

3.5.1.2 Software Download

In the Software Download screen (see Figure 34), the system can be configured to download and boot from a new image off the network. (Please refer to Chapter 5 when updating software)

- Click the arrow in the box at "Boot from" and click the Net option.
- Supply the IP address of the TFTP server and the full path and the filename of the image to be loaded from that server.
- Click the Submit button.
- Reset the switch by clicking on the System Administrator tab and clicking on Reset Switch. The image will load-up automatically after the switch reset.

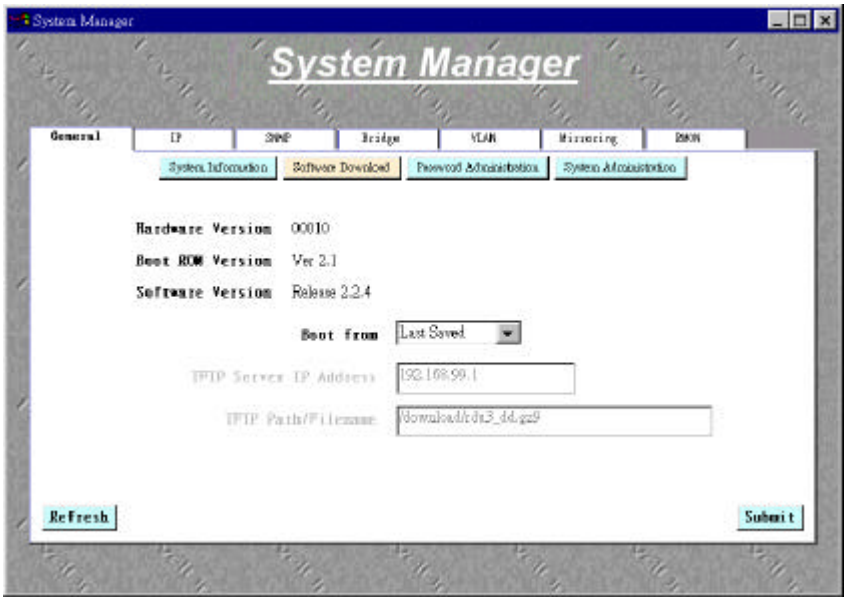


Figure 3-4: General: Software Download

3.5.1.3 Password Administration

The password entered is encrypted on the screen and will display as a sequence of asterisks (*).

- Type the new administrator password in the New password field
- Type the same password in the Verify field
- Click Submit to activate the new password

Note: Password protection is optional and can only be enabled through the console interface. If the password protection is enabled without setting your own password, the default password is "switch".

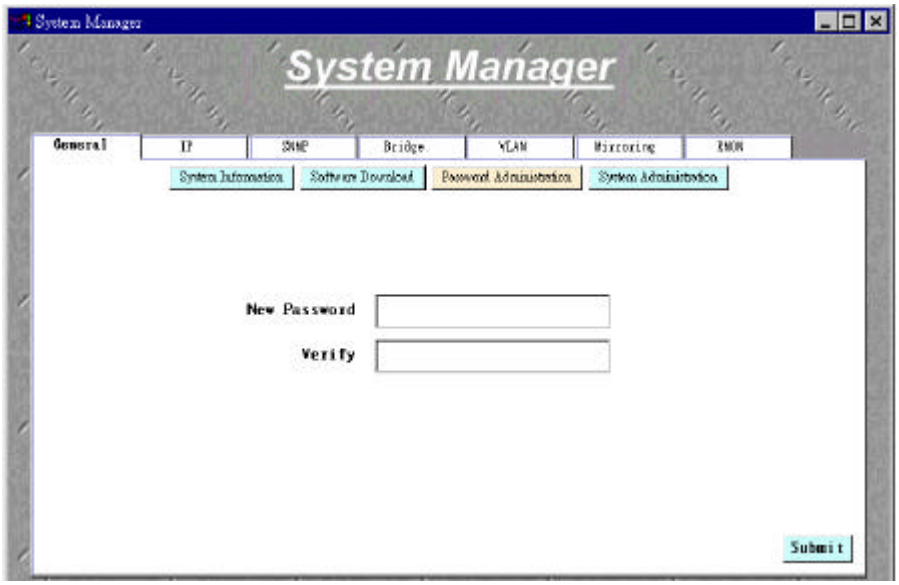


Figure 3-5: General: Password Administration

3.5.1.4 System Administration

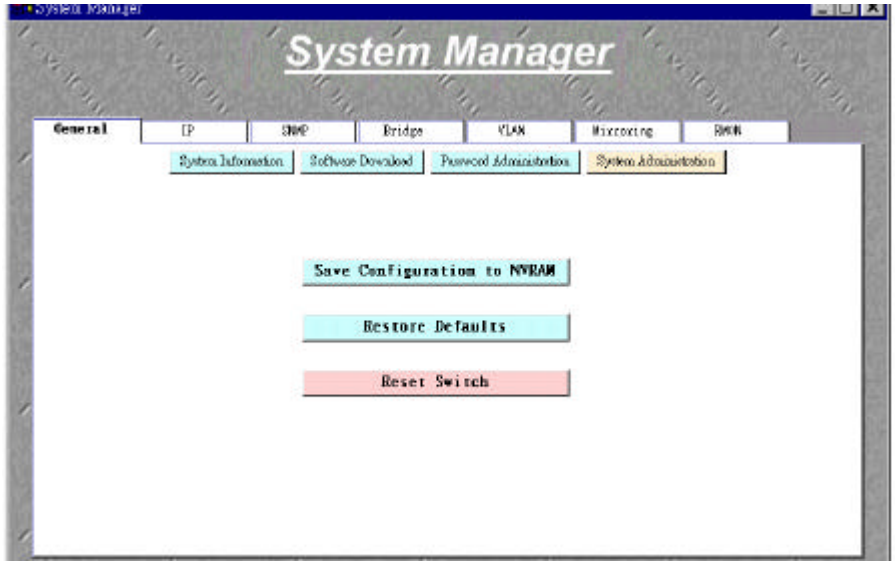


Figure 3-6: General: System Administration

After making any changes to the screens within the Web Interface, users must save the changed settings to NVRAM. This is done in the system administration screen (see Figure 3-6) in order for the new settings to remain after a system reboot.

Save Configuration to NVRAM

- Click on Save Configuration to NVRAM at this screen and a second screen will ask for verification of this action, to accept choose OK, otherwise click cancel.

Restore Defaults

- Click on Restore Defaults to reset switch parameters to their original default settings. In order for changes to occur, you must reset the switch. Note: network IP settings (i.e. IP address, Gateway Address, Network Mask) will not be affected by this command.

Reset Switch

- Click on the Reset Switch button and a second screen will ask for verification of this action, to accept choose OK, otherwise click cancel.

3.5.2 IP

There are three tunable parameters to be set by the system administrator (see Figure 3-7).

- Enter site-specific IP address, Gateway address and Net mask
- Click Submit to accept
- Save Configuration to NVRAM and reset the system to implement the changes (refer to General folder's System Administration)

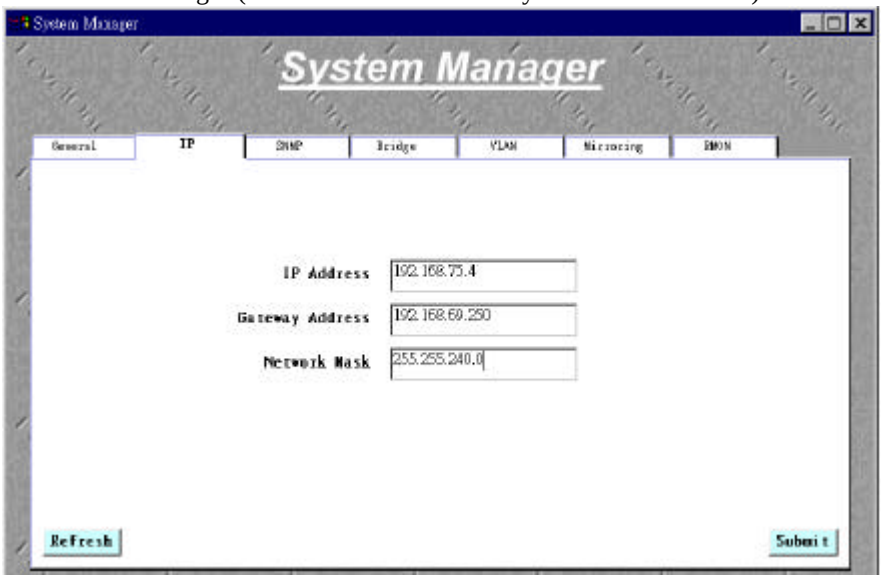


Figure 3-7: IP screen

3.5.3 SNMP

The SNMP folder contains the following sub-folders:

- SNMP Trap Configurations
- SNMP Host Table
- SNMP Community Table

3.5.3.1 SNMP Trap Configuration

The SNMP Trap Configuration (Figure 3-8) allows for the setup of authentication traps.

Authentication traps

- Enable The system will generate a SNMP trap upon a host authorization failure
- Disable The authentication traps will not be generated

All hosts in community strings with TRAP privileges will be notified when a trap condition occurs.

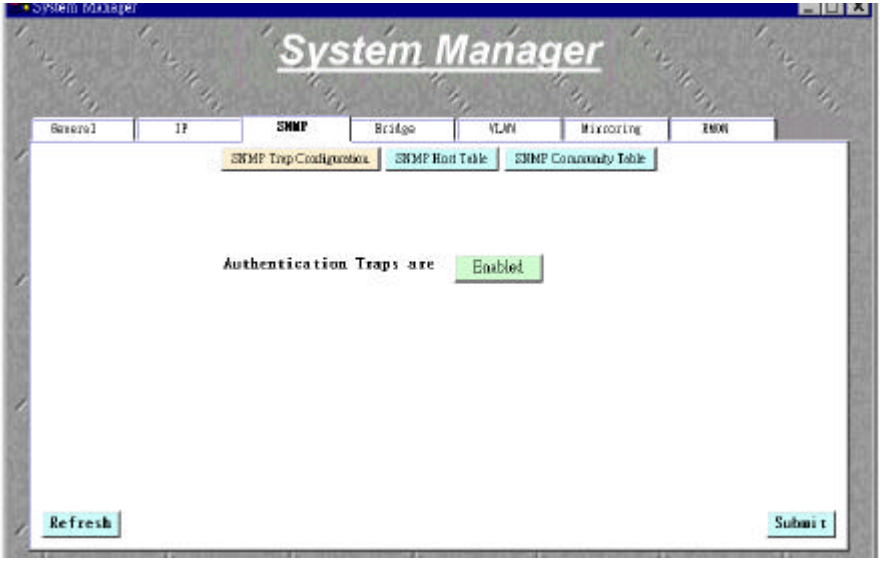


Figure 3-8: SNMP: SNMP Trap Configuration

3.5.3.2 SNMP Host Table

The SNMP Host Table screen (Figure 3-9) allows you to add and remove hosts from access rights that have been granted to community groups. The permissions GET, SET and TRAP are assigned to a community string (see next section SNMP Community Tables) and then these permissions are assigned to individual machines by adding those machines and their IP address to the appropriate community string. Host Authorization can be Enabled or Disabled.

Host Authorization

- Enable
- Disable

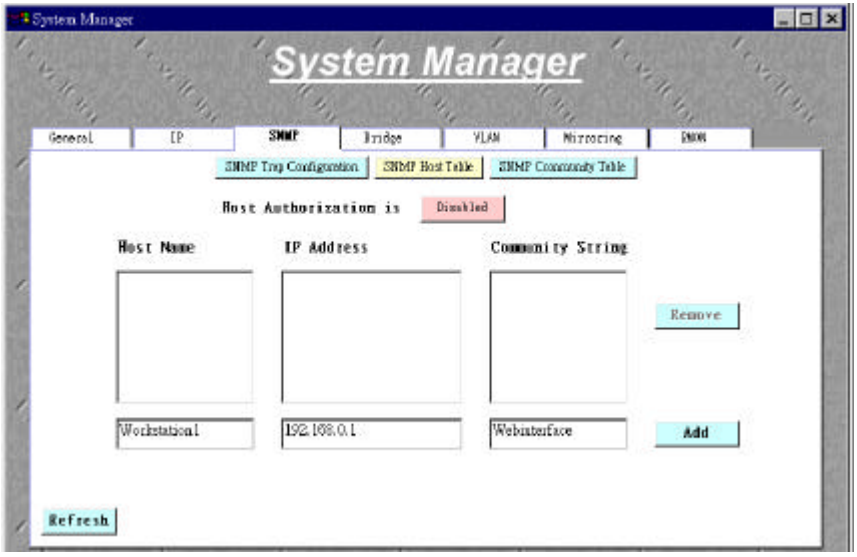


Figure 3-9: SNMP: SNMP Host Table

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

3.5.3.3 SNMP Community Table

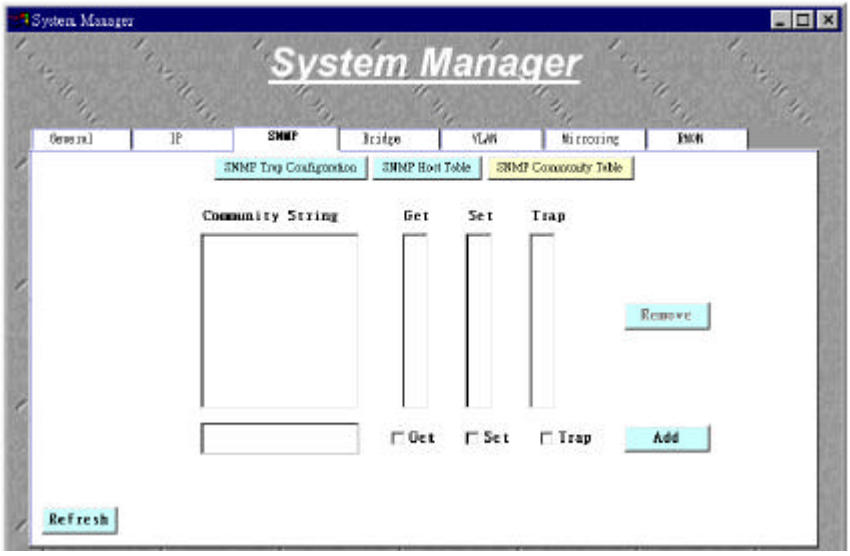


Figure 3-10: SNMP: SNMP Community Table

In the Community Table (see Figure 3-10) the administrator can create different community strings with customized access, by choosing combinations of GET, SET and TRAP rights. These community strings need to be set prior to setting host access, as the host table depends on the existence of the community strings.

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

3.5.4 Bridge

The Bridge folder of the System Manager has three sub-folders:

- Spanning Tree Configuration
- Static Bridge Table
- Bridge Aging

3.5.4.1 Spanning Tree Configuration

Spanning Tree can be enabled or disabled in this folder.
Enable: As shown in Figure 3-11, there are four other tunable parameters to be addressed.

- Hello Time — Interval between configuration messages sent by the spanning tree algorithm
- Max Age — Amount of time before a configuration message is discarded by the system
- Forward Delay — Amount of time system spends in "learning" and "listening" states
- Bridge Priority — Priority setting among other switches in the spanning tree

Disable: Disable spanning tree algorithm on the system.

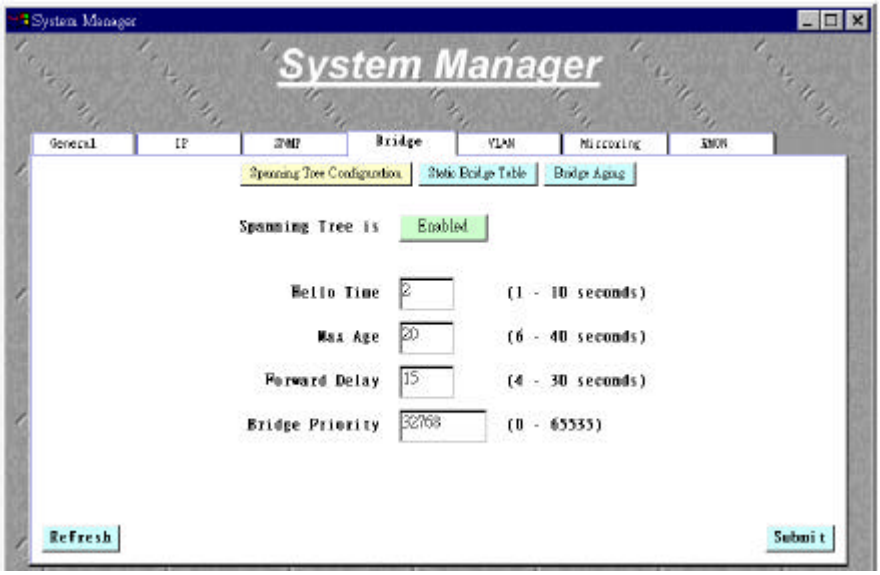


Figure 3-11: Bridge: Spanning Tree Configuration

- After entering the appropriate values you need and press Submit to set them on the system
- A notification screen will show up, click on OK to enable the new changes

3.5.4.2 Static Bridge Table

Any system, whose MAC address and the port number are listed in this screen, (see Figure 3-12) will not be purged from the system's forwarding table by the aging process.

Add a new entry

- Enter the MAC address and port in the appropriate boxes
- Click Add

Remove an exist entry

- Highlight that entry in the table, by clicking on the MAC address
- Choose Remove

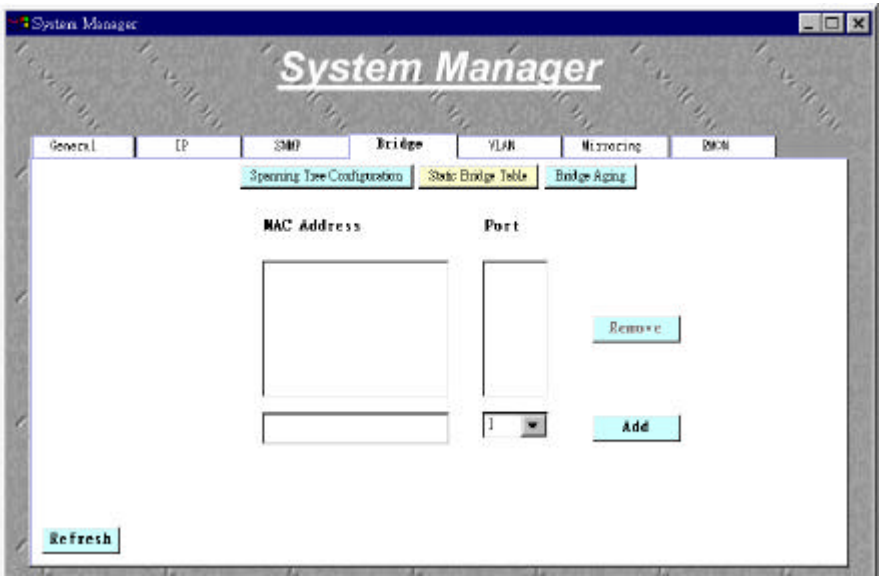


Figure 3-12: Bridge: Static Bridge Table

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

3.5.4.3 Bridge Aging

Aging Time is a variable that must be configured. Its purpose is to determine the amount of time an entry is held in the forwarding tables (Figure 3-13).

The default value is set to 300 seconds, (or 5 minutes).

- The administrator may change this value to any value between 10 and 824 seconds.
- After changing the value, click Submit

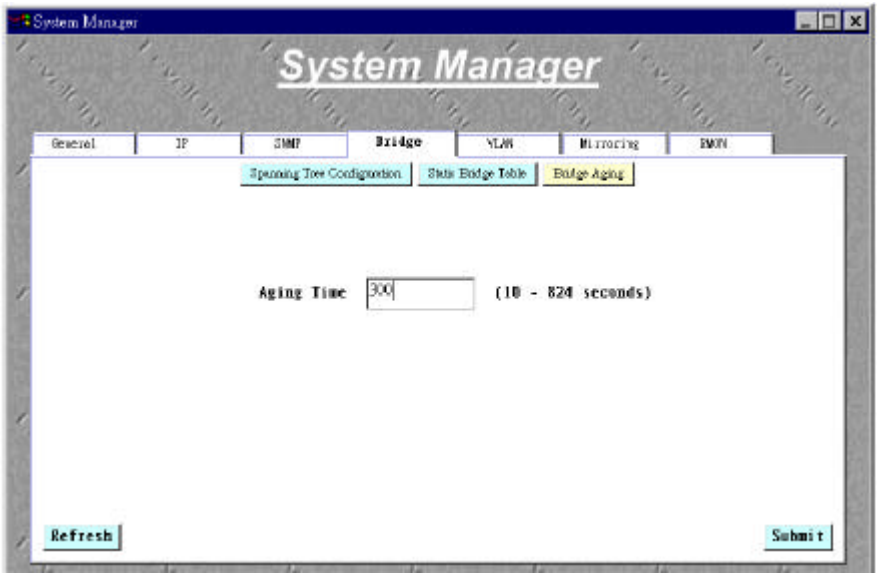


Figure 3-13: Bridge: Bridge Aging

3.5.5 802.1Q VLAN

The VLAN option within the System Manager allows users to define VLAN groups. The VLAN Administration button will allow you to create a new VLAN. The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches (Reference: Appendix A and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks).

Add VLAN Group

- Enter the VLAN Id and name in the appropriate boxes
- Click Add

Remove VLAN Group

- Highlight the group you want to remove
- Click on the Remove button

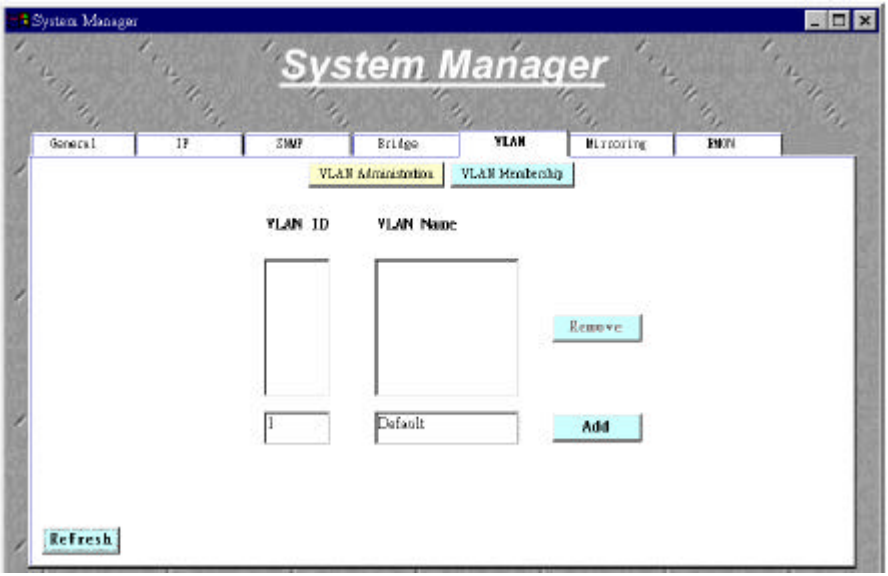


Figure 3-14: VLAN

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

Choose the VLAN Membership Option, and a window displaying all VLANs and ports will be called (see Figure 3-15).

Add VLAN Membership

- Click the box below the port number on the line of the VLAN so that a "T" (tagged) or "U" (untagged) appears.

Remove VLAN Membership

- Click the box again until a blank box appears. This will remove VLAN membership from the port.

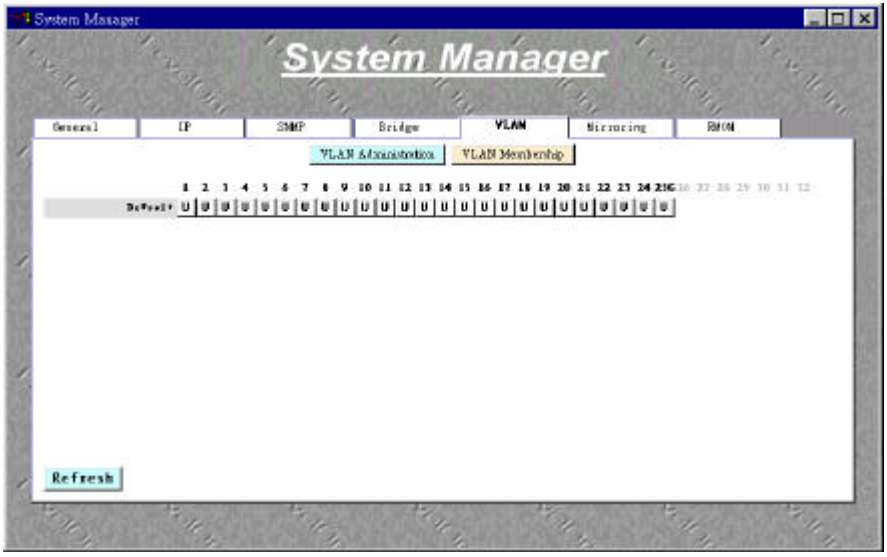


Figure 3-15: VLAN: VLAN Membership

3.5.6 Mirroring

Port mirroring is a feature to help in the debugging of a network. This web interface page, as seen in Figure 3-16, allows enabling or disabling of port mirroring and the setting of source and monitor ports (when enabled). The Monitor port will show a copy of every packet that arrives or leaves the source port.

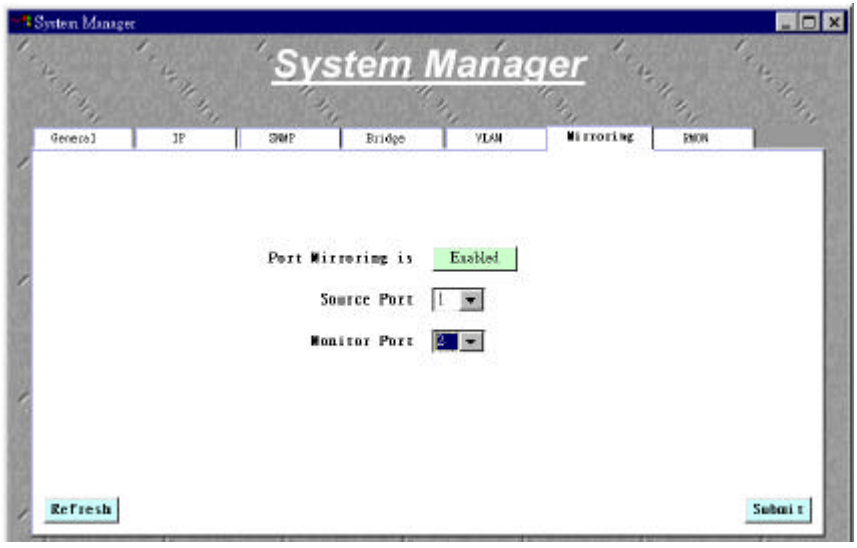


Figure 3-16: Mirroring

3.5.7 RMON

The remote monitoring (RMON) section of the System Manager is for configuring the monitoring parameters:

- Ethernet Statistics
- Ethernet History
- Alarm
- Event
- Log

3.5.7.1 Ethernet Statistics

Due to the fact that the RMON section of the System Manager is for configuration purposes only. This feature by default is always enabled.

3.5.7.2 Ethernet History

The Ethernet History tab (see Figure 3-17) sets the number of intervals between samples taken for a port. By default, there are no entries in the table. To add a new setting, choose a port, enter in the appropriate settings. Then, click Add to submit the request to the system. If the system could not handle the number of requested samples, then it will allow as many as possible and list the active number of samples in the Granted column. Any setup requests from this particular page will show the owner as 'WebInterface'.

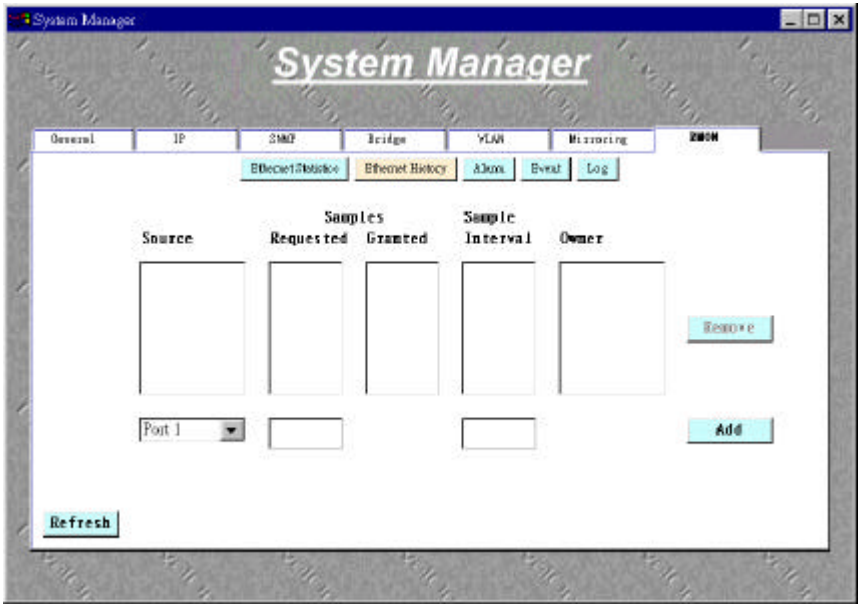


Figure 3-17: RMON: Ethernet History

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

3.5.7.3 Alarm

The Alarm folder under RMON is where conditions are set for an alarm that will trigger a pre-determined event (see next section on setting an event).

- Enter the interval (in seconds)
- Choose the type of statistic to check and port to monitor
- Choose a sample type and startup alarm
- Enter the threshold and event if needed
- Click Add

There are two sample types from which to choose: Delta and Absolute.

A Delta sample type

- Denotes a change in the statistic. The numeric value given for either the rising or falling threshold represents the difference between successive samples that trigger the event.

The Absolute type

- Defines the statistic actual value, so when a sample equals the rising or falling threshold, it will trigger an event.

In the example page below (Figure 3-18), the alarm can be explained as follows:

- Sample the Inbound Unicast Packets on Port 1 every 2 seconds
- If the value of the sample is greater than zero then trigger event ID 2

If the startup alarm type, Rising or Falling is chosen, then both thresholds and rising and falling event IDs need to be entered. Where if Rising or Falling are chosen independently then only the corresponding threshold and event id needs to be entered. At anytime, an alarm may be removed, simply highlight that alarm by clicking any one of the fields. Then click Remove.

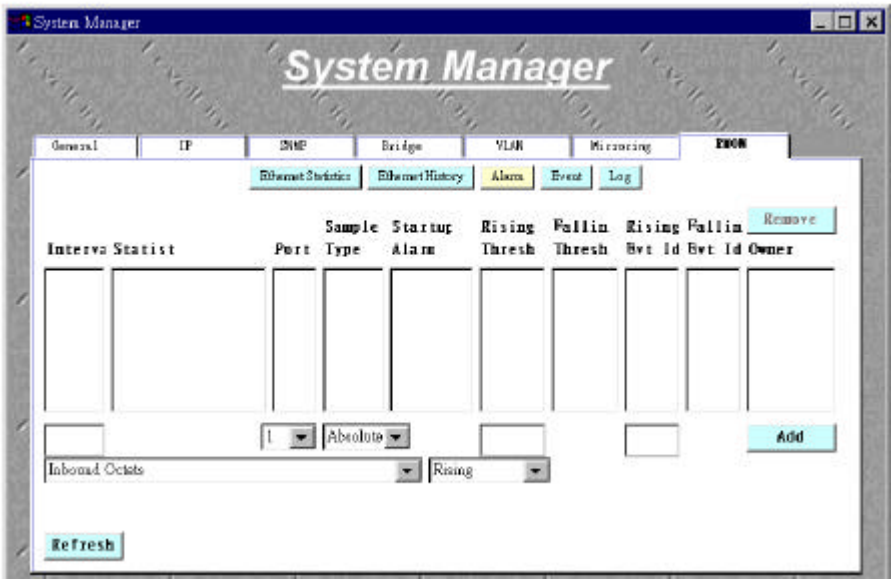


Figure 3-18: RMON: Alarm

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

3.5.7.4 Event

The event tells the system what to do when the conditions of the alarm are met. As seen in Figure 3-19, the event screen is quite clear.

Add an Event

- Enter a description of the event to be defined.
- Choose the type of action to be performed.
- A community string is also required, whether or not a Trap condition is set. If an invalid community string is entered, a message will appear at the bottom of the screen informing the user. (Refer to the SNMP Community Table section)
- After entering all appropriate data, click Add.

Remove an Event

- Click any field entry of that event and choose Remove.

There are four event actions that may be set; None, Log, SNMP Trap, and Log and Trap.

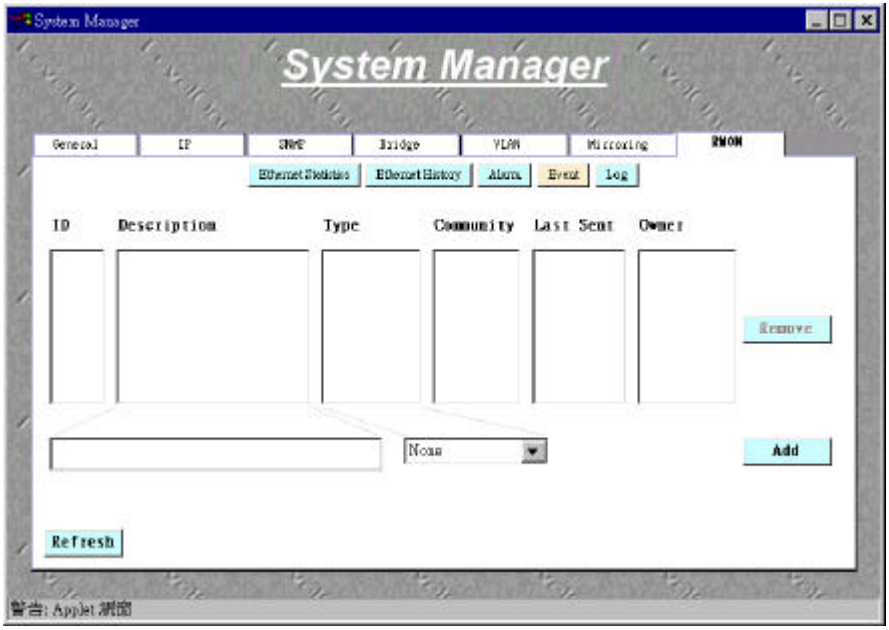


Figure 3-19: RMON: Event

Note: When the scroll bars start to appear due to a large number of entries, it may become necessary to click on an entry when viewing to ensure proper alignment of sub windows.

3.5.7.5 Log

If an event type defines logging as an action for an alarm, then the event will be entered in the table here (Figure 3-20). When an event is removed from the event table, all log entries corresponding to that event will be removed from this log table. This will only be evident with a Refresh of the logging output.

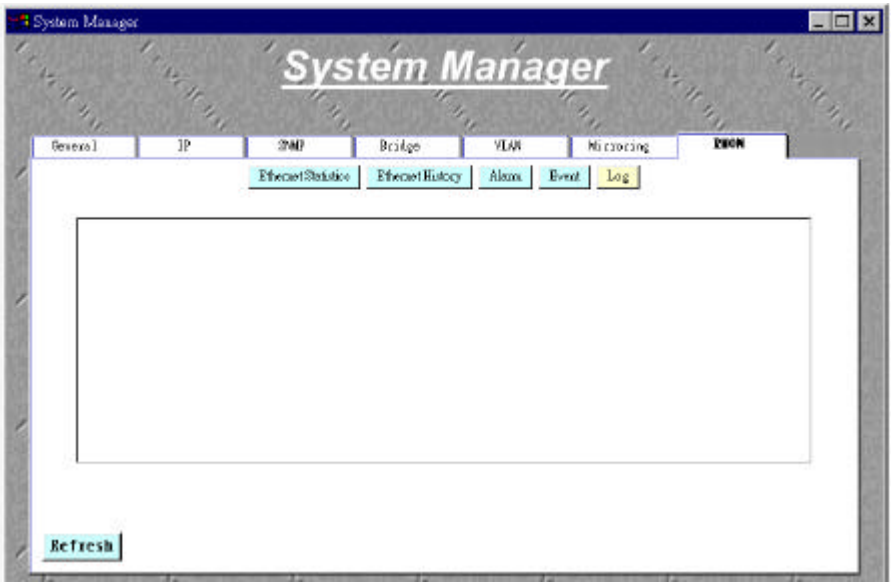


Figure 3-20: RMON: Log

3.6 Port Manager

Users can use the Port Manager folder to change the port related parameters and settings. In addition to the per port configuration, users can also program more then one port as a group to have the same configuration using the Group sub-folder. Under each sub-folder, these options are provided:

- All Ports
- Group Setup
- Port Configuration
- Spanning Tree Configuration
- VLAN Membership

3.6.1 All Ports

An overview of the port settings - The Administrator has the ability to change Admin Status, Data Rate, Duplex, Source Security, and Flow Control through this menu. It also describes the port state, current Data Rate and current Duplex.

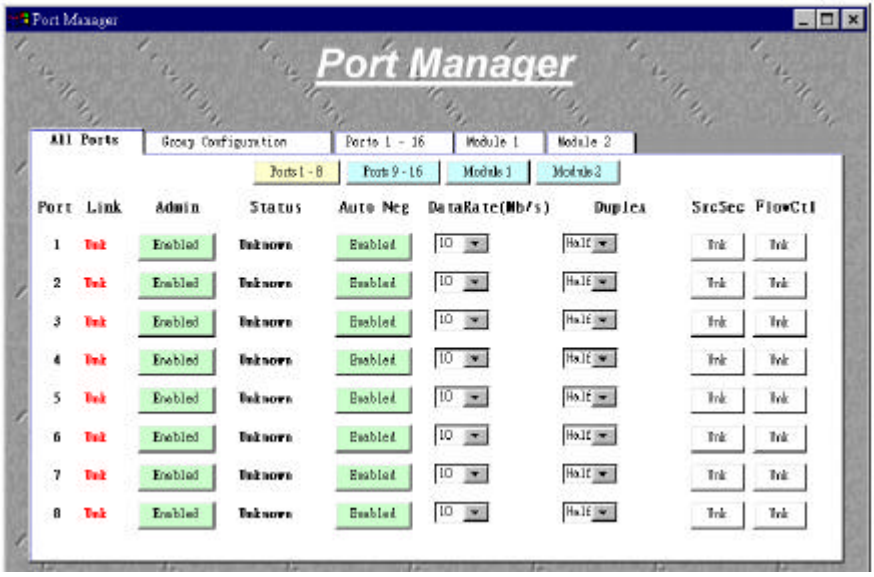


Figure 3-21: All Ports View

3.6.2 Group Setup

The benefit of Group Setup is the ability to setup link configurations, spanning tree configurations, and VLAN memberships for a group of ports at the same time. As shown in Figure 3-22, there are buttons for All Ports and No Ports, simply click to add all ports to the group or to clear up the ports that are associated with the group.

Add individual ports to the group

- Click the arrow of the port box and choose a port by highlighting it
- Click Add to add that port to the group

Remove a port from group

- Highlight the port from the group listing and choose Remove

These options exist in the Group sub-folder of the Port Manager.

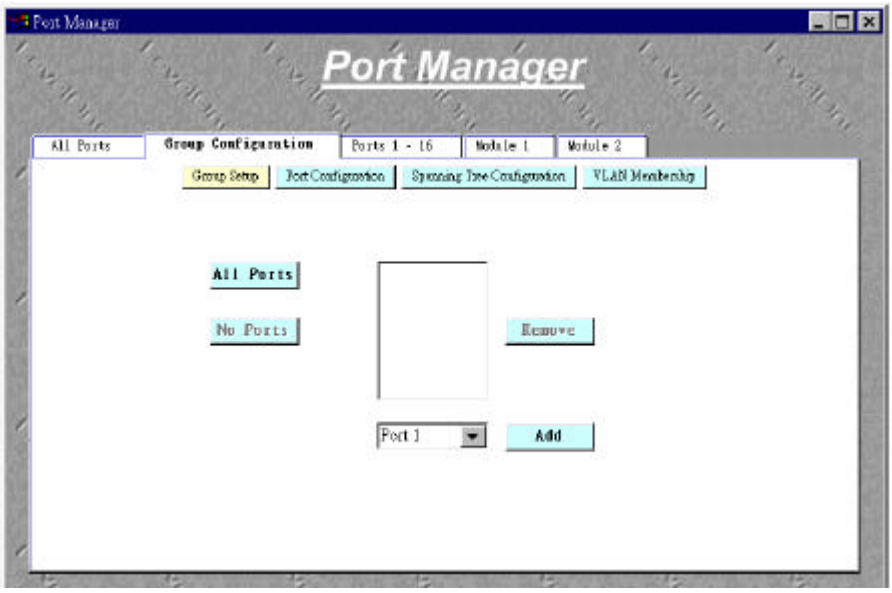


Figure 3-22: Group: Group Setup

3.6.3 Port Configuration

The Port Configuration screen is available in both the Group Setup and individual port pages. These pages allow for the manipulation of port link settings. There are three buttons that toggle between enabled and disabled states when chosen. These buttons are for:

- Admin status: Sets the port at Enable or Disable
- Source security: Turns security to the port on or off

- Flow Control: Used to stop the sender from sending data until the receiver can accept it

The link parameter settings

- Duplex: Sets the duplex rate as Full, Half, or Auto. Default setting is Auto
- Data Rate: Sets the data rate for each port by choosing Auto, 10, or 100 Megabit per second

When finished setting up the ports, choose Submit to activate the changes.
Note:
1) The one notable difference in the Group Port Configuration screen and the Group Port Configuration screen is the operational status.

2) On the ports 1-16 configuration screen it will state whether or not that port is Up or Down. The Up will be displayed in green while the Down is displayed in red. This informs the administrator whether or not the port is attached and active.

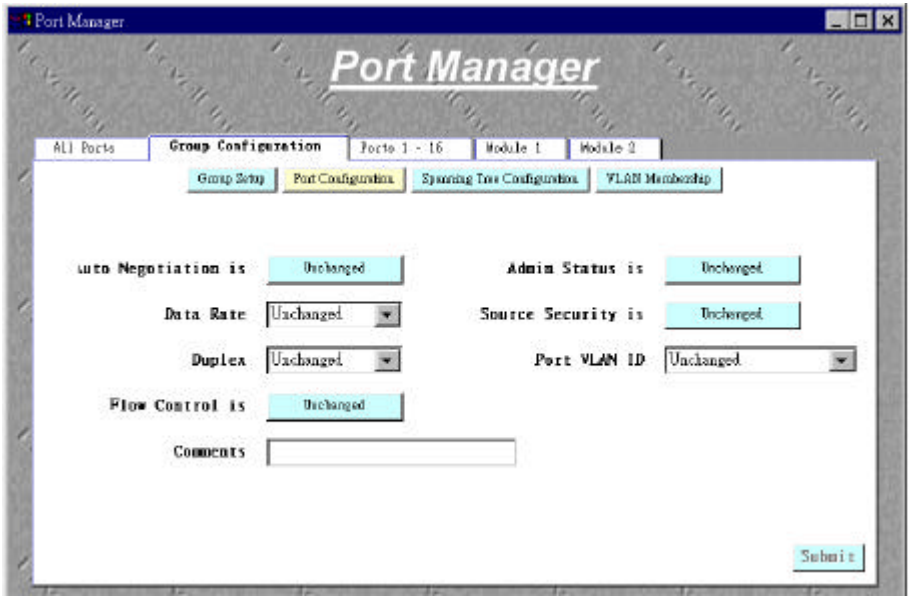


Figure 3-23a: Group: Port Configuration

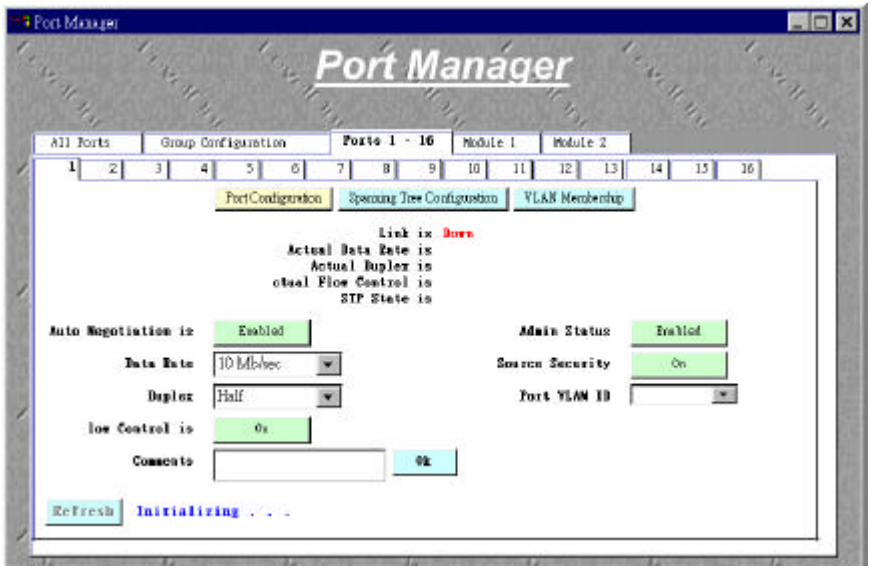


Figure 3-23b: Port #: Port Configuration

3.6.4 Spanning Tree Configuration

The spanning tree priority is a numeric value assigned to a port or group that determines the level of importance that this particular port or group holds in the bridge group. The lower the number the higher the importance. Similarly, the spanning tree cost is a variable that helps the system to determine which port to use in a group (refer Figure 3-24a, Figure 3-24b).

Note: The port or group with the lower cost will be chosen first by the system.

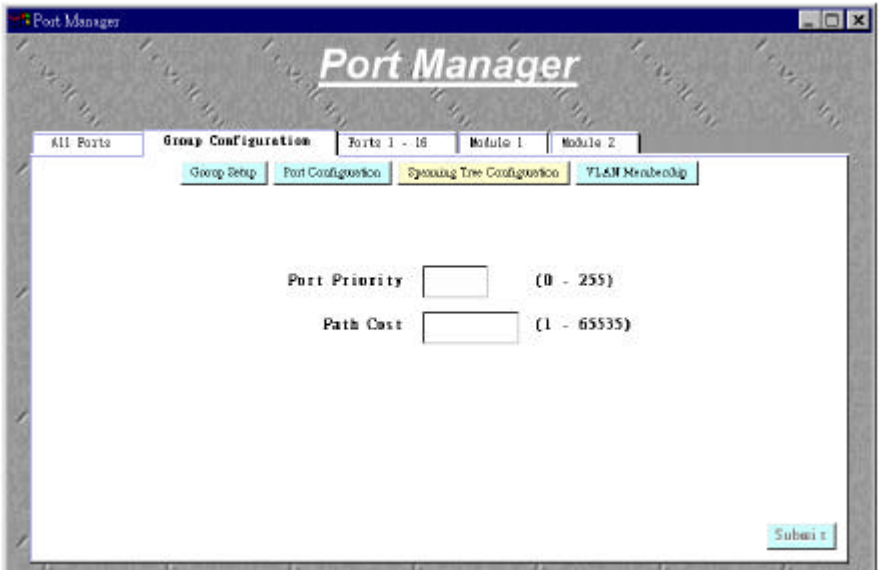


Figure 3-24a: Group: Spanning Tree Configuration

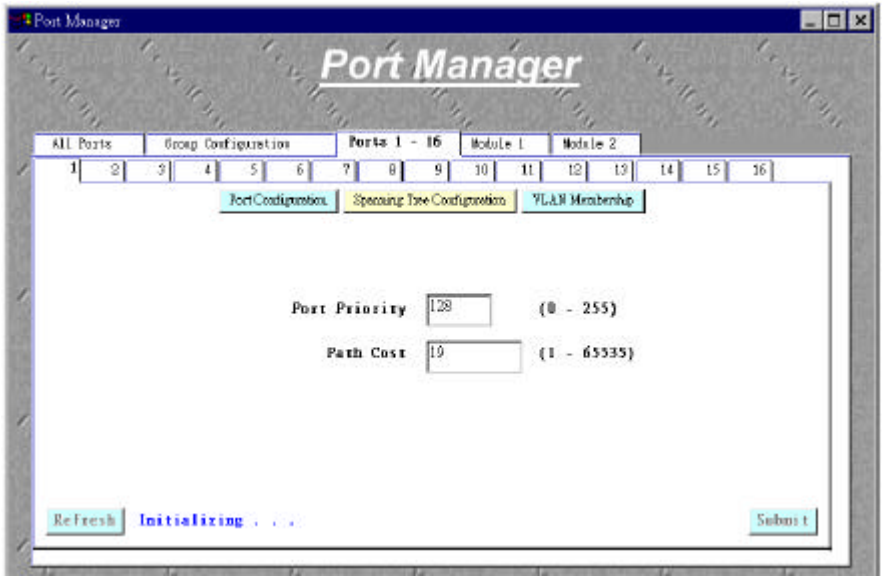


Figure 3-24b: Port #: Spanning Tree Configuration

3.6.5 VLAN Membership

Any VLAN that has been created from the System Manager will be displayed on the screen, as seen in Figures 2-25. Up to 16 VLANs with unique ID numbers and names can be added. VLAN ID numbers must be in the range of 1-4094.

Add a port or group to the VLAN

- Click on the box to configure VLAN membership. Settings can be changed from Untagged or Tagged.

Remove a port or group from the VLAN

- Click the box until it is blank and the VLAN membership for that port will be removed. To reflect the current system settings, click the Refresh button in the lower left.

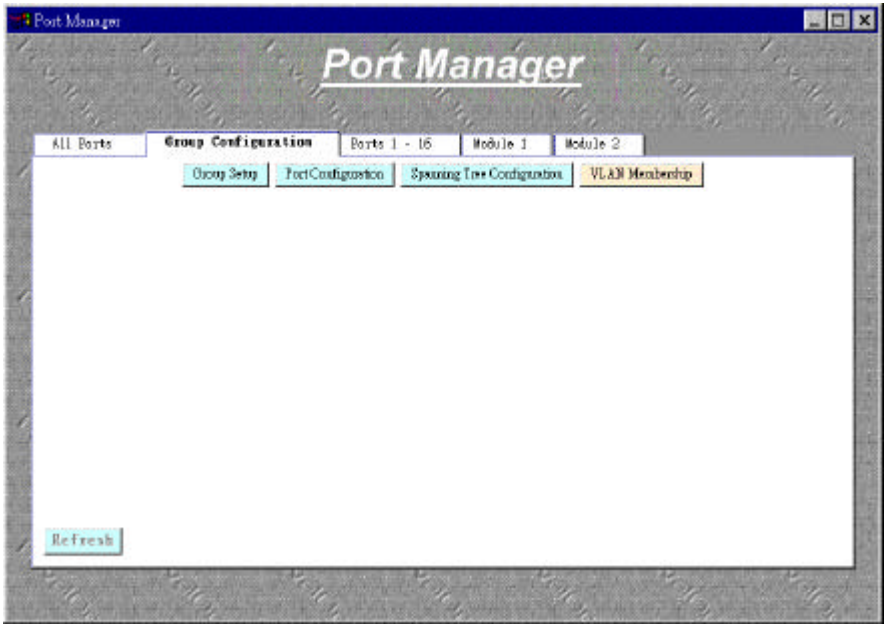


Figure 3-25a : Group VLAN Membership

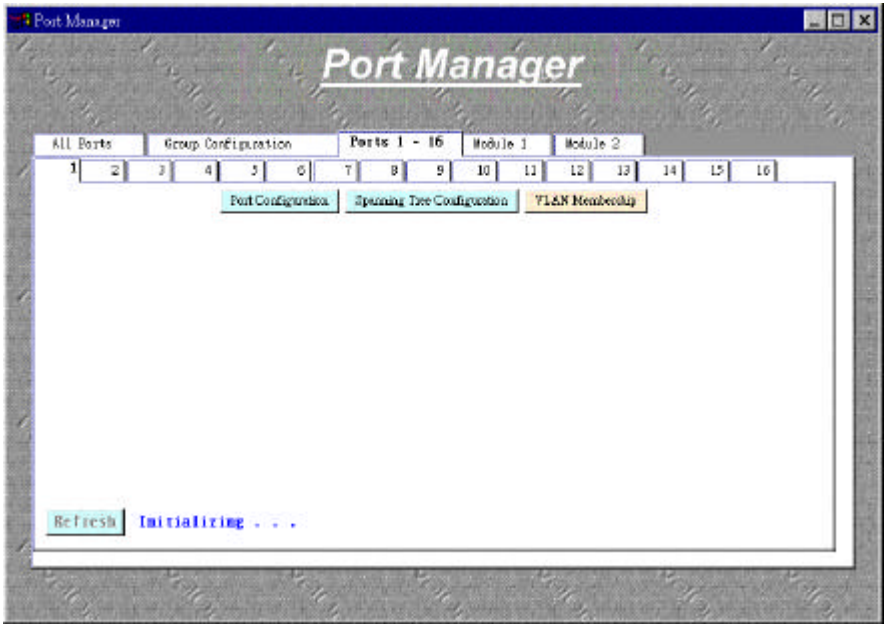


Figure 3-25b: Port #: VLAN Membership

3.7 MIB Viewer

The Management Information Base (or MIB) Viewer section of the Web Interface, allows the administrator to chart system data in different manners. There are three folders to this section:

- Comparison Chart
- Group Chart
- History Graph

3.7.1 Comparison Chart

For the Comparison Chart section (see Figure 3-26a), there are three parameters to set: Statistic, Refresh Rate, and Color. All charts have a maximum ceiling of 2^{31}-1. You can see the value of each bar or line in the chart by clicking on the bar.

- Statistic — The type of system data to be monitored
- Refresh Rate — The time interval between automatic refreshes
- Color — The color setting for the chart

When all of the variables are set, click Chart.

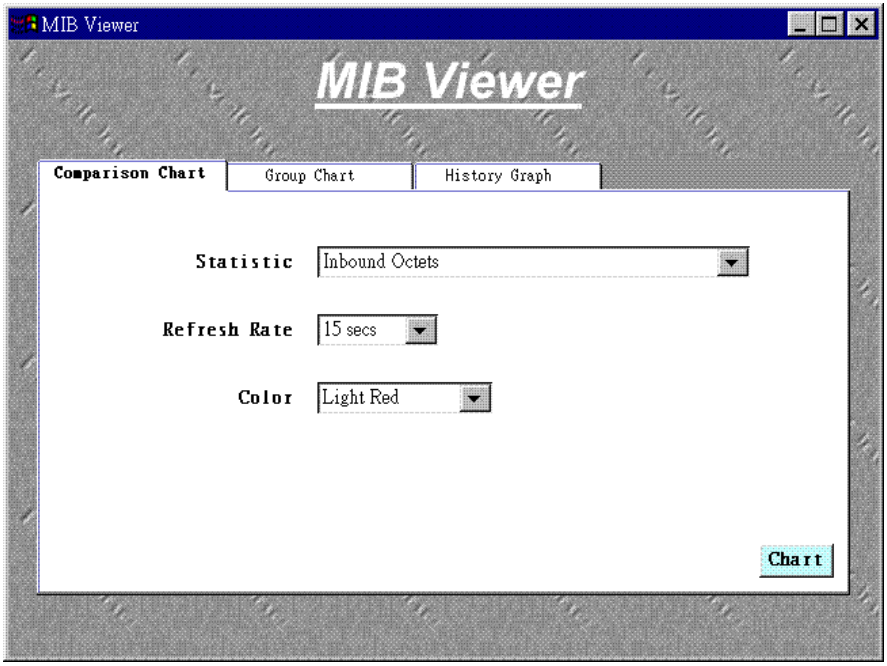


Figure 3-26a: Comparison Chart

The chart screen, seen below as Figure 2-26b, has a couple of options as well.

Reset

- To locally reset the data and start collecting new data.

Three options of the scale:

- Auto scale — Automatically choose an appropriate scale for data
- Manual scale — Requires user to enter the lower and upper values
- Full scale — Puts the maximum and minimum boundary value as the scale

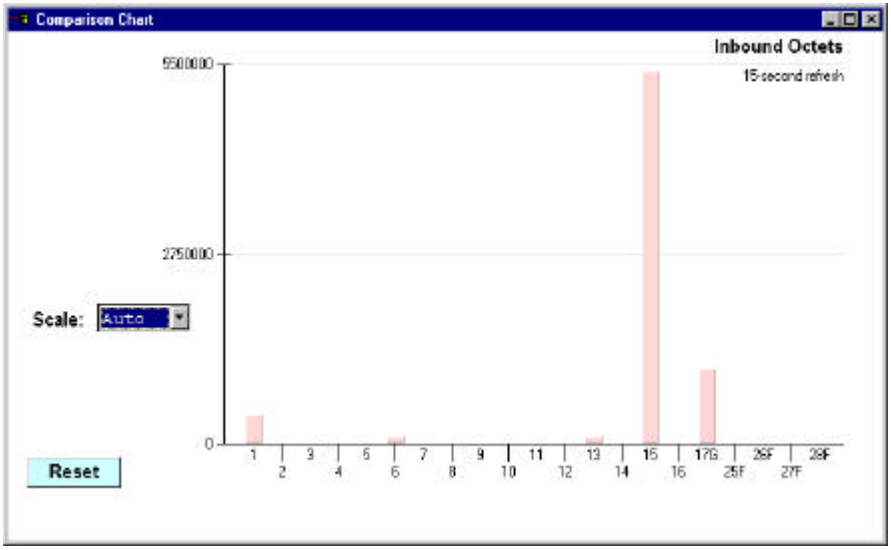


Figure 3-26b: Comparison Chart: Chart

3.7.2 Group Chart

View error statistics of a specific port (see Figure 3-27a):

- Click the arrow in the Group box and select a port to chart
- Select a Refresh Rate and a Color
- Click Chart to move to the graphical screen

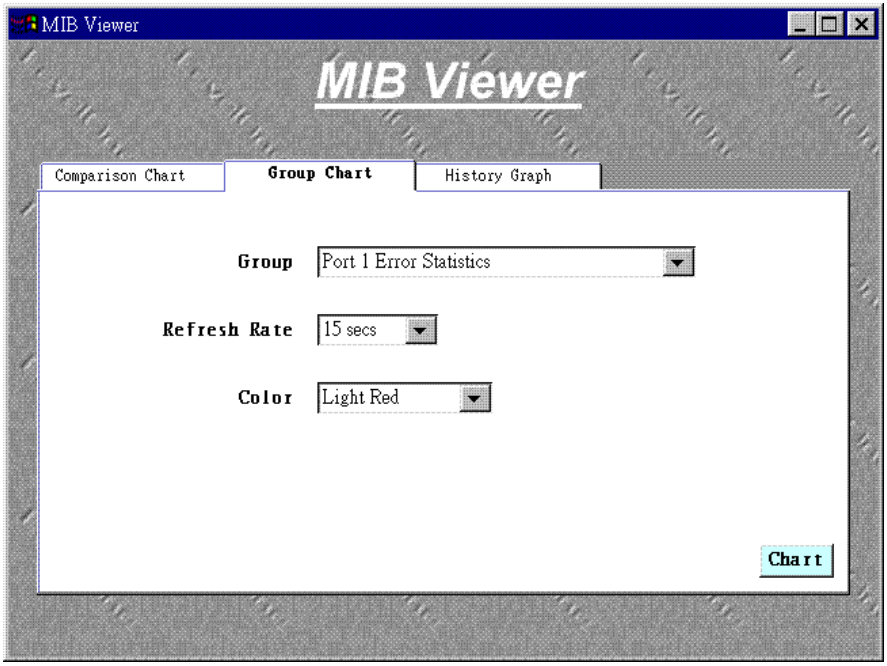


Figure 3-27a: Group Chart

There are twelve data transmit error types on this screen to choose from.

Scale setting

- As in the Comparison Chart, the scale can be set to Manual, Full, or Auto.

Get the exact value of the statistic

- Click the mouse button on any of the bars in the chart and a box with the exact value will appear.

Reset

- Click Reset to clear the chart and start plotting from new data, which is computed relative to when the reset button was pressed. This does not reset the statistics' values on the switch, just the local values.

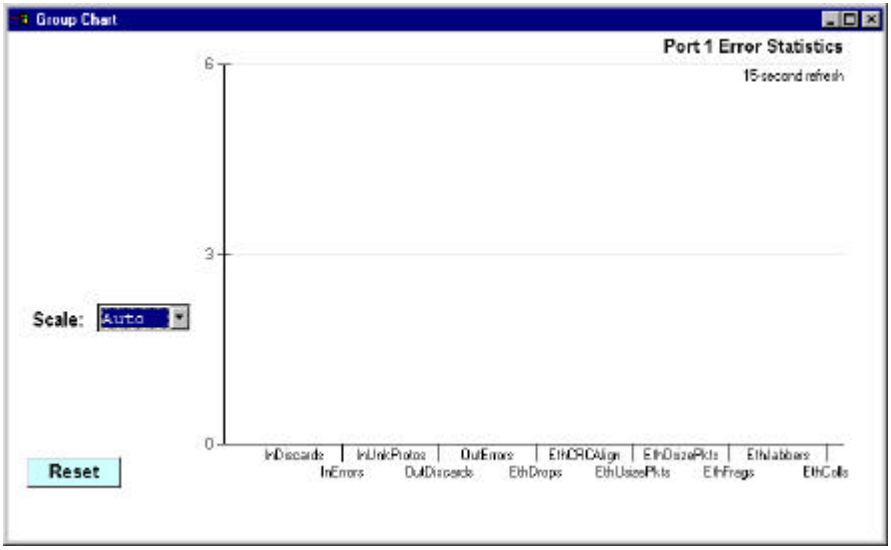


Figure 3-27b: Group Chart: Chart

3.7.3 History Graph

The history graph allows up to twelve colors to be chosen in order to plot any statistic for up to 10 ports.

Set up the information to graph

- Choose a statistic in the statistics box and highlighting an option
- Decide on a refresh rate from the times provided
- Select the ports to be viewed by choosing a port and color to represent
- Click Add
- Click the Graph button to proceed

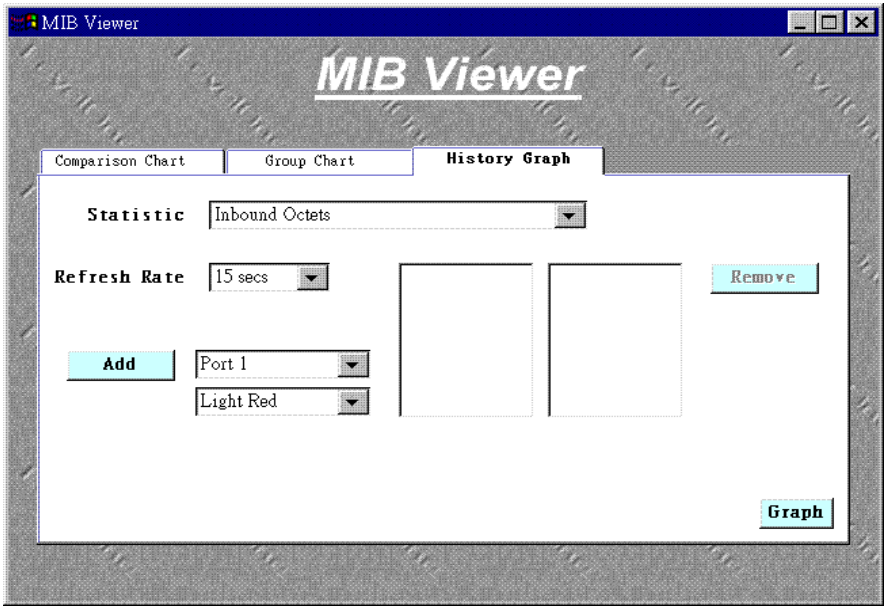


Figure 3-28a: History Graph

The graph page, as shown in Figure 3-28b, has all of the same options as the other chart screens. The scale can be set to Auto, Manual, or Full. The refresh button will remove old data from the screen and start a new graph. Clicking on the black data points will show the exact value of that point.

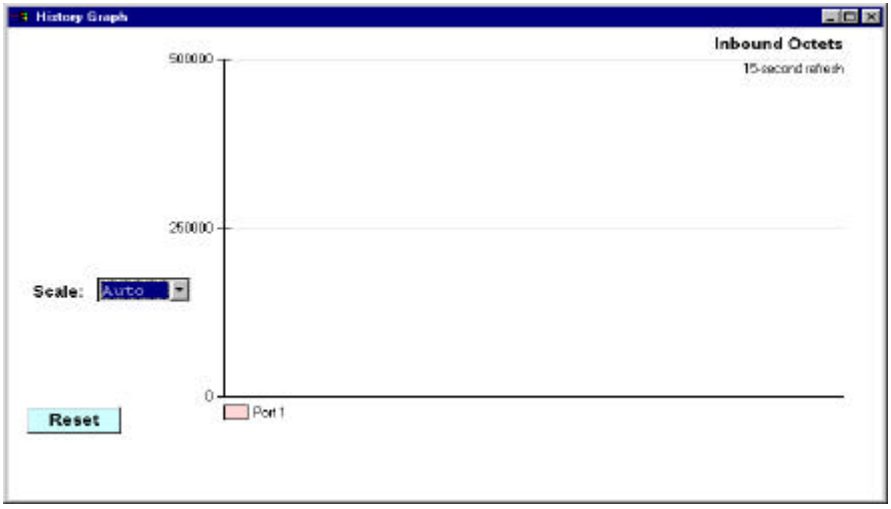
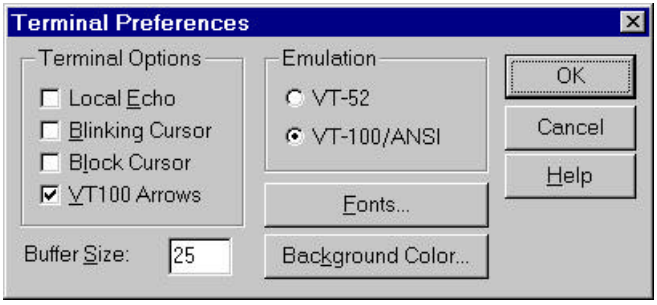


Figure 3-28b: History Graph: Graph

Chapter 4 Console Interface

The console, using VT100 terminal emulation, can be accessed from the RS232 serial port or a telnet connection. The switch offers password protection for this interface. All of the following examples of the Console's User Interface show a screen capture from a telnet session.



When attached to the User Interface via a Telnet Session, the following must be set in order to use the arrow keys: Under the terminal pull down menu choose Properties and make sure the VT100 Arrows option is turned on.

4.1 User Interface

The switch offers a menu-driven interface. The initial welcome screen, seen below in Figure 4-1, requires a password entry in order to proceed. If there is no password set on the system, the Main Menu will be displayed and access is granted immediately. By default, password protection is disabled. If enabled, the default password is "switch".

To enable password protection

- Choose System Manager from the Main Menu
- Choose General
- Select Password Administration
- Enter and verify new password

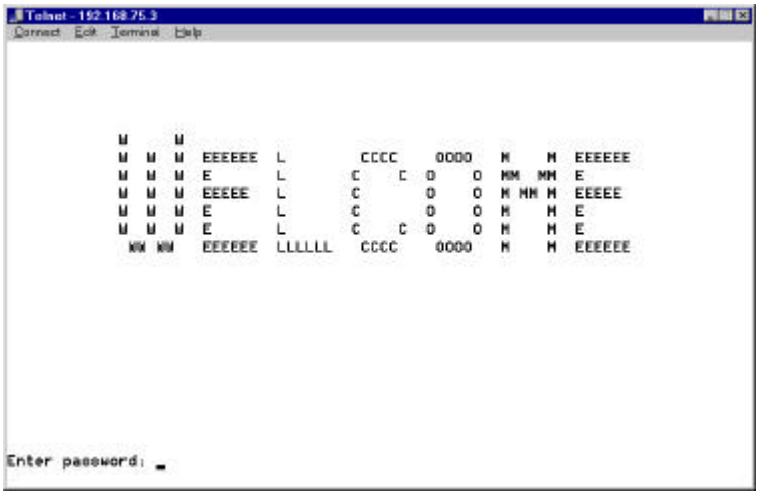


Figure 4-1 Initial Welcome screen of User Interface

4.2 Characteristics

There are several characteristics to the User Interface pages that are necessary to know before proceeding to use it. The arrow keys may be used to move within menus and sub-screens. At the bottom of every screen are some key commands available to the user for that particular screen, as well as some helpful information. The common key strokes and their definitions and intricacies are listed below:

ESC	Return to the previous menu or screen, or abort editing
Ctrl-L	Refresh the screen
Ctrl-D	Log off
Ctrl-W	Saves current configuration to NVRAM
Spacebar	Toggles between possible settings for a field
Enter	Select a menu item, edit a field, or accept a value after editing a field
Ctrl-X	Delete a table entry

4.3 Main Menu

The main menu displays all the sub-menus that are available. Striking Enter, at a highlighted option, will confirm the choice of the specified sub-menu. As shown in Figure 4-2, there are three menu items to choose from:

- System Manager
- Port Manager
- Statistics

To logout of the user interface, hit Ctrl-D at anytime during your telnet session. You will be brought back to the login screen.

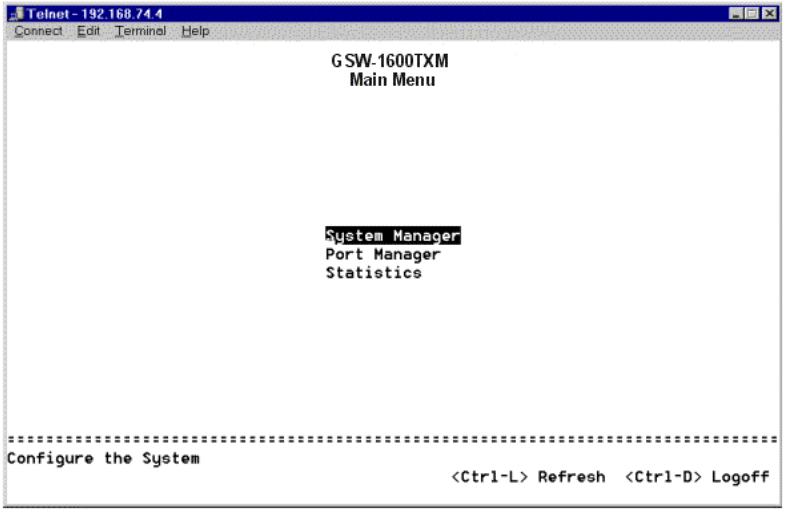


Figure 4-2: Main Menu

4.4 System Manager

This menu contains all the options needed to configure the switch to your network. Menu items are:

- General
- IP
- SNMP
- Bridge
- VLAN
- Mirroring

4.4.1 General

These parameters include the following:

- System Information — Includes system uptime, description, name, contact, location and MAC address
- Software Download — Manages the software version of the switch
- Password Administration — Manages the login password of the switch (For both console and web)
- System Administration — Saves the settings to NVRAM, resets the switch, and restores settings

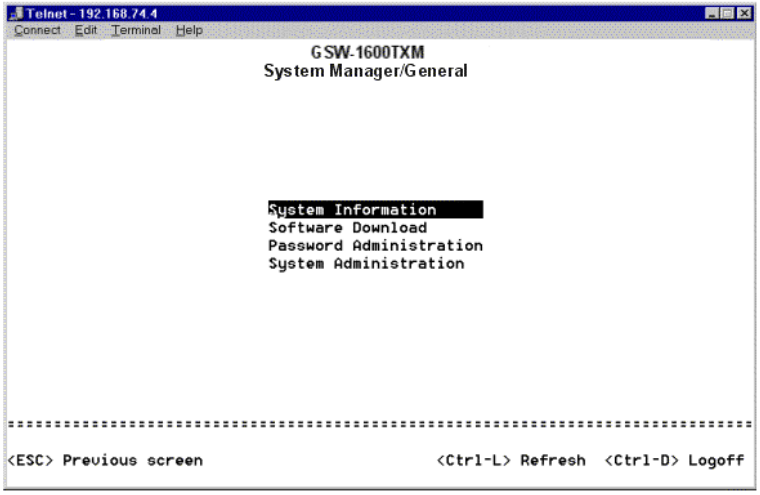


Figure 4-3: Main Menu: General

4.4.1.1 System Information

This screen displays the following:

- System Description
- System Name- user definable
- System Contact-user definable
- System Location-user definable
- MAC Address

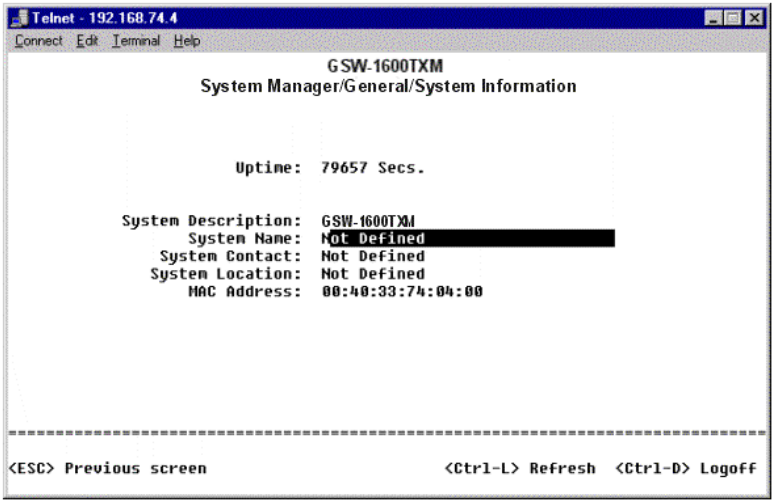


Figure 4-4 : System Information

4.4.1.2 Software Download

This screen (see Figure 4-5) allows users to select an image file and the location from where it can be downloaded using TFTP. There are three 'Boot from:' options: Net, Net & Save, and Last Saved. (Please refer to Chapter 5 when updating software)

Net option:
This option allows the user to try out a new image before upgrading. It requires a TFTP filename and a server IP address to retrieve the specified image from the given IP address.

The new image will not overwrite the one in the flash.

Net + Copy option
This option requires the same setup as the Net option, i.e. TFTP server and a new image. However, it copies the image to the flash directly and the system boots from the flash afterwards.

Last Saved option
This option will automatically show up after the 'Net + Copy' option is selected and the unit is reset.

Warning: The previous image in the flash will be lost when the procedure completes.

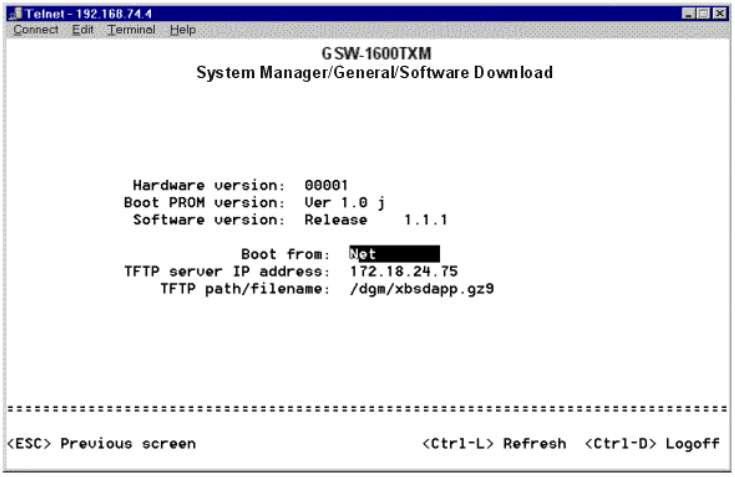


Figure 4-5: General: Software Download

4.4.1.3 Password Administration

This screen allows the user to change the password for both the Console and Web sessions. (Figure 4-6)
To use password protection, you must enable Password Protection.

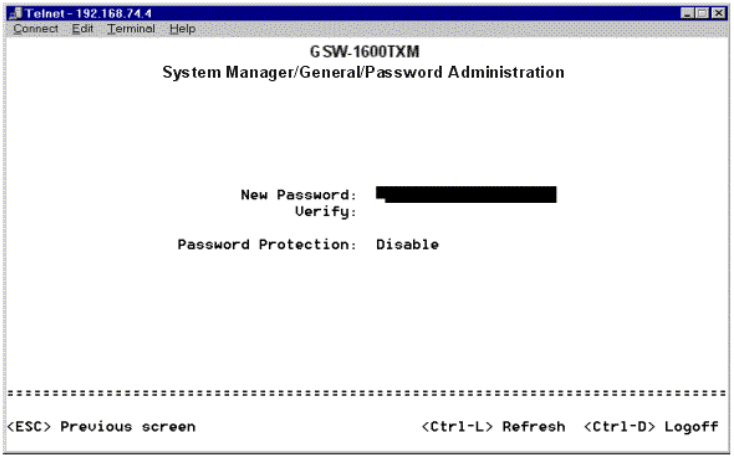


Figure 4-6: General: Password Administration

4.4.1.4 System Administration

- Save Configuration to NVRAM — Save all changed made in your session to NVRAM
- Restore Defaults — Restore original settings
- Reset Switch — Restart the switch

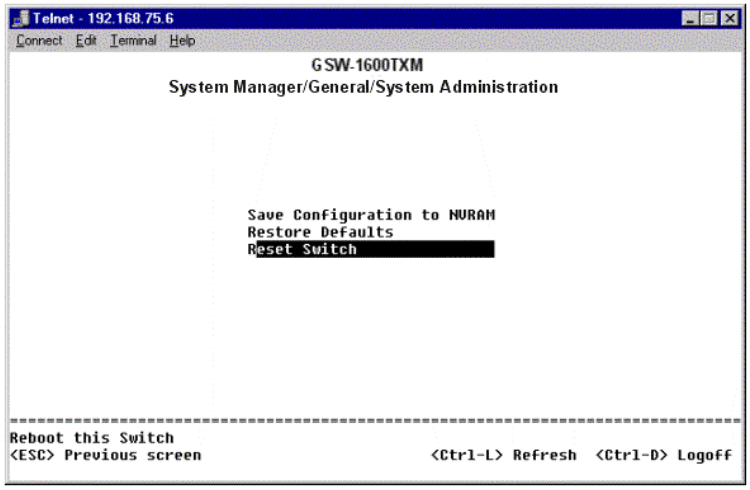


Figure 4-7: General: System Administration

4.4.2 IP

This menu manages the IP related information of the system.

- Enter a site specific IP address, Gateway Address, and Network Mask (or subnet mask). Consult your network administrator for the information.
- Press Ctrl-W to save any changes made.

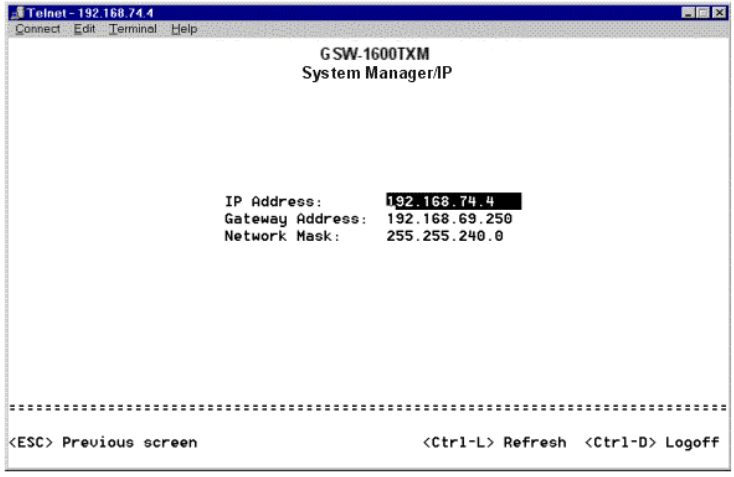


Figure 4-8: General: IP

4.4.3 SNMP

This sub-menu allows users to setup three sections as shown (Figure 4-9):

- Trap Configuration
- Community Table
- Host Authorization

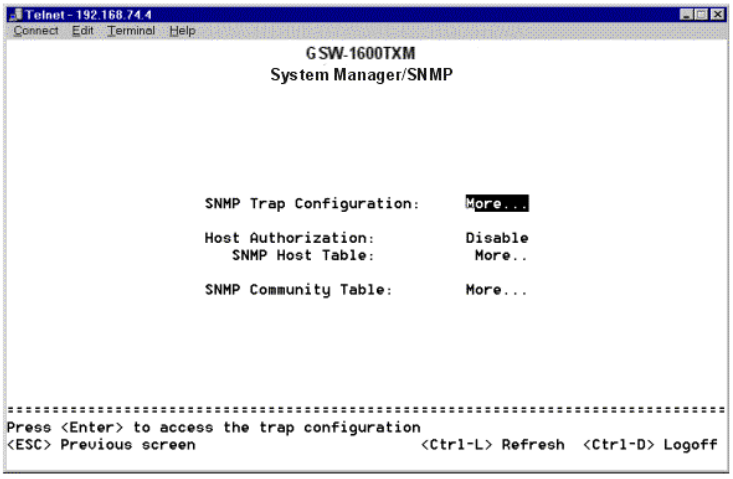


Figure 4-9: SNMP

4.4.3.1 SNMP Trap Configuration

Authentication Traps

When on, the system will generate an SNMP trap upon a host authorization failure. This failure occurs when a host tries to gain access to the system but the host's IP is not in the SNMP host table.

4.4.3.2 SNMP Host Table

The screen, shown in Figure 4-9, grants a host the access rights to the box.

Host Authorization must be enabled to use the host table. Host Authorization is used as a security feature to limit people who are not listed in the host table from accessing the switch.

If Host Authorization is enabled, the host must be added to this table, through the Console port connection in order for an end station to be access the switch via SNMP or the Web Interface.

Add host

- Enter the host name, IP address, and the community string. Press Enter after each entry to move to the next field.
- In the Status field, press the Spacebar until the desired Status is displayed.
- Press Ctrl-W to save all changes.

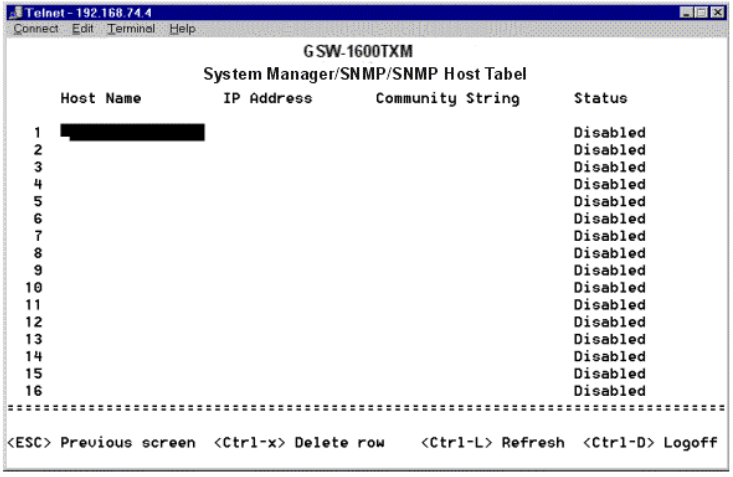


Figure 4-10: Main Menu: Configuration: SNMP Menu: Host Table

4.4.3.3 SNMP Community Table

The administrator can create up to eight different communities strings with combinations of GET, SET and TRAP privileges. These community strings need to be set prior to setting host access, as the host table depends on the existence of community strings. The public string has all the privileges by default.

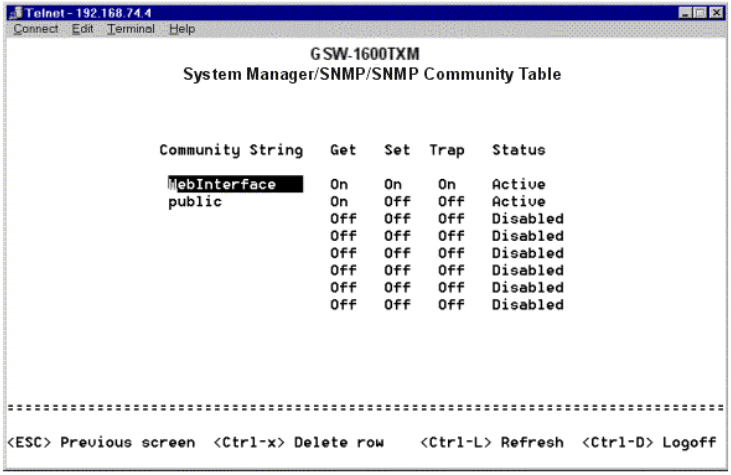


Figure 4-11: SNMP: SNMP Community Table

4.4.4 Bridge

There are several parameters to be set in the Bridge Configuration screen (see Figure 4-12):

- Spanning Tree Configuration
- Static Bridge Table
- Bridge Aging

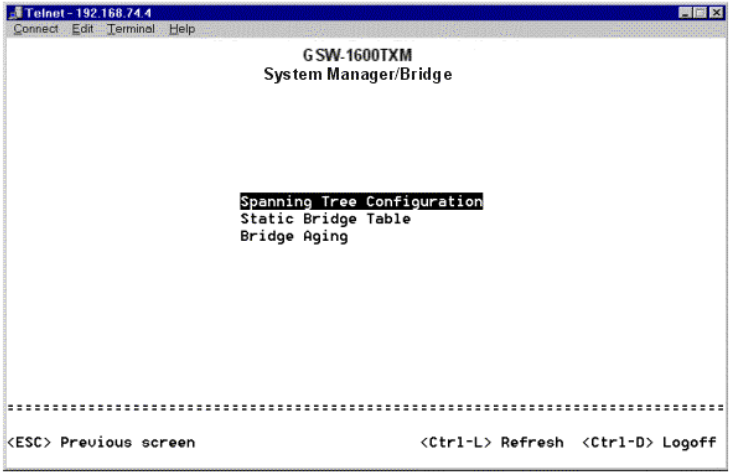


Figure 4-12: Bridge

4.4.4.1 Spanning Tree Configuration

If Spanning Tree is disabled the next four values are ignored. When enabled they do need to be set.

- Hello Time — Interval between configuration messages sent by the spanning tree algorithm
- Max Age — Amount of time before a configuration message is discarded by the system
- Forward Delay — Amount of time system spends in "learning" and "listening" states
- Bridge Priority — Priority setting among other switches in the spanning tree

4.4.4.2 Static Bridge Table

The Static Bridge Table, Figure 4-12, allows the administrator to specify Media Access Control (MAC) addresses for specific ports that will not be purged from the bridge table by the aging function.

Add an entry

- Type the MAC address under the first column, and hit Enter.
- Enter the port number, which is associated with the MAC address.

If all the information is correct, the new entry will appear in the list below, which is in order by port ID. Otherwise, an error message will be displayed and the cursor will return to the MAC Address field.

Remove an entry

- Tab down to the entry and press Ctrl-X. ESC will return to the previous menu.

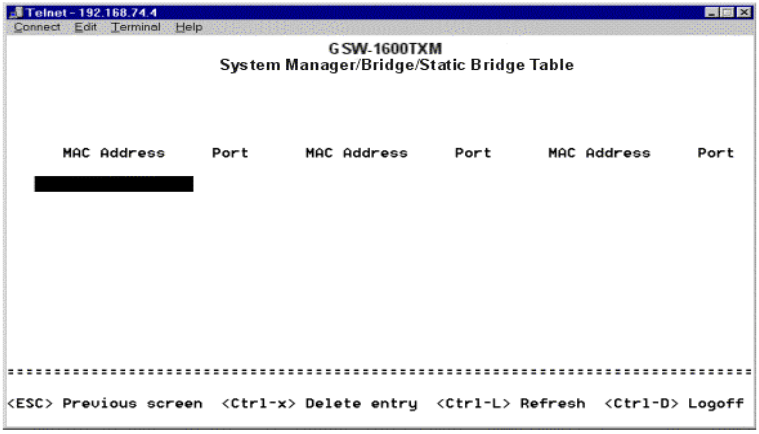


Figure 4-13: Bridge: Static Bridge Table

4.4.4.3 *Bridge Aging*

The aging time is the amount of time that an entry is kept in the bridge tables prior to being purged (or aged). The range (in parentheses) represents the minimum and the maximum values that the timer can be set.

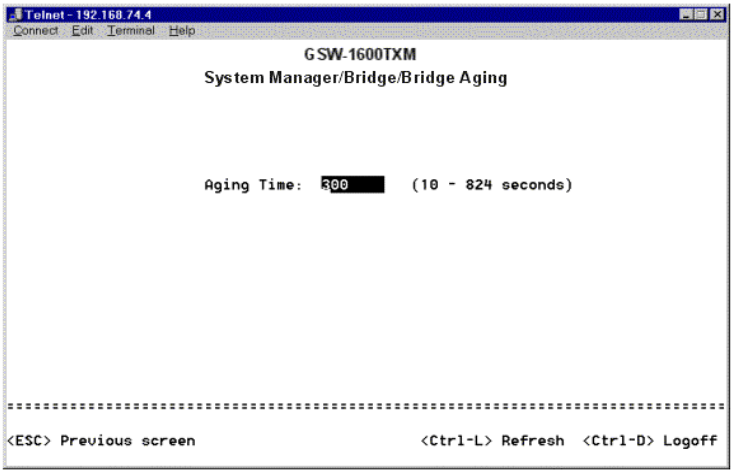


Figure 4-14: Bridge: Bridge Aging

4.4.5 *VLAN*

The VLAN settings are as follows:

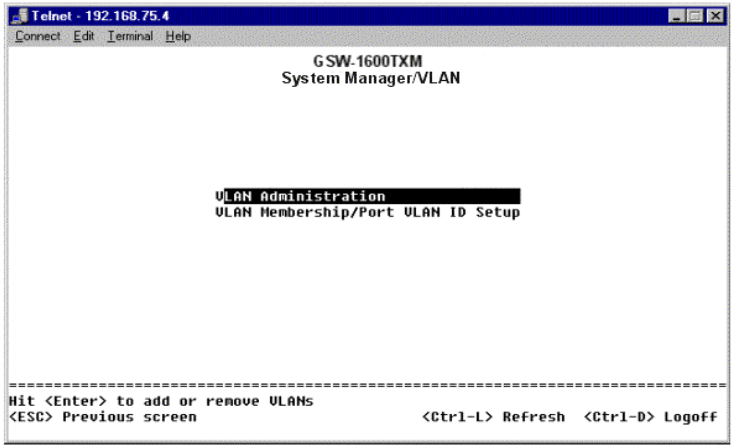


Figure 4-15: VLAN

4.4.5.1 VLAN Administration

Up to 16 VLANs with unique ID numbers and names can be added. VLAN ID numbers must be in the range of 1-4094.

Add a VLAN

- Type a unique numeric VLAN ID and hit Enter
- Type a unique VLAN name and hit Enter

Remove a port or an entire VLAN

- To remove an entire VLAN, just press Ctrl-X anywhere on that line

4.4.5.2 VLAN Membership/Port VLAN ID Setup

This matrix allows for real time management of up to 16 VLANs. To add a port to a VLAN, position the cursor in the desired matrix location and toggle the options with the SPACE bar.

Hitting 'Ctrl-V' in this page will toggle between the VLAN Membership and Port VLAN ID Setup page. A 'U' or 'T' will be displayed for each port assigned to the VLAN (see Figure 4-16a), where 'U' stands for untagged and 'T' for tagged. A '_' space indicates that the port is not a member of the particular VLAN. An 'X' in the Port VLAN ID Setup page will mark will PVID is set for each port (see Figure 4-16b). VLAN tagging is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches. (Reference: Appendix A and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks)

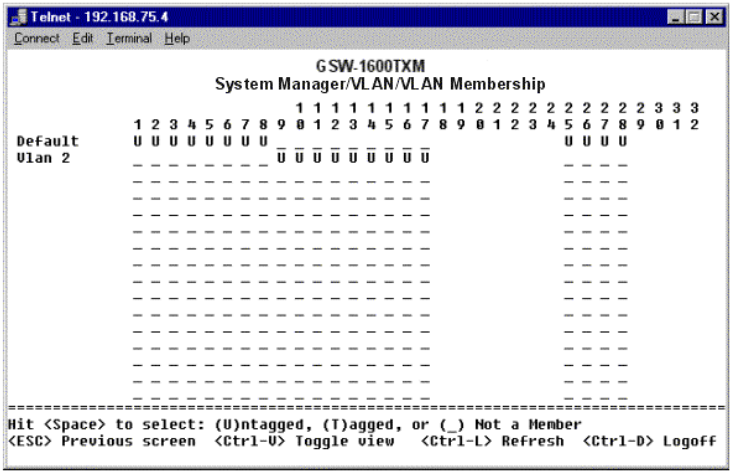


Figure 4-16a:VLAN Membership

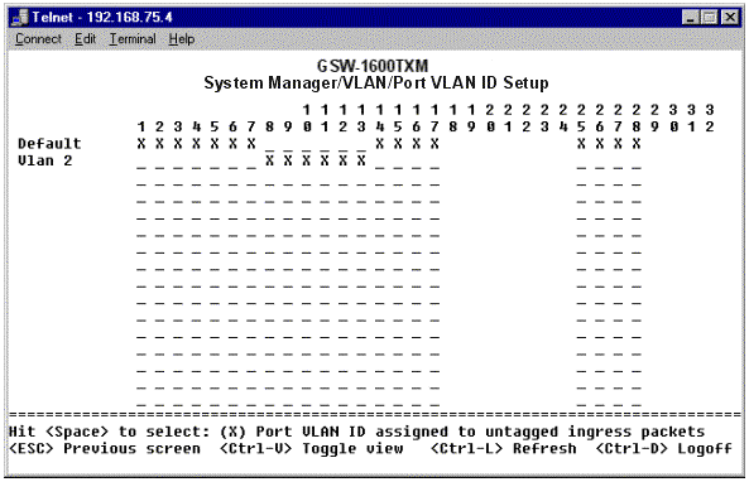


Figure 4-16b: Port VLAN ID Setup

4.4.6 Mirroring

This menu option allows users to enable the Port Mirroring capability (see Figure 4-17 and Section 3.11). Users need to specify both the Source and Monitor port. The Monitor port will show a copy of every packet that arrives and departs at the Source port.

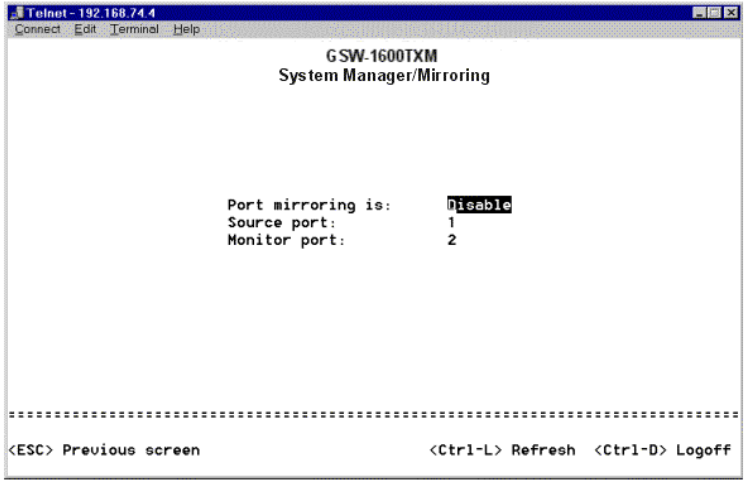


Figure 4-17: Port Mirroring

4.5 Port Manager

The Port Manager settings are as follows:

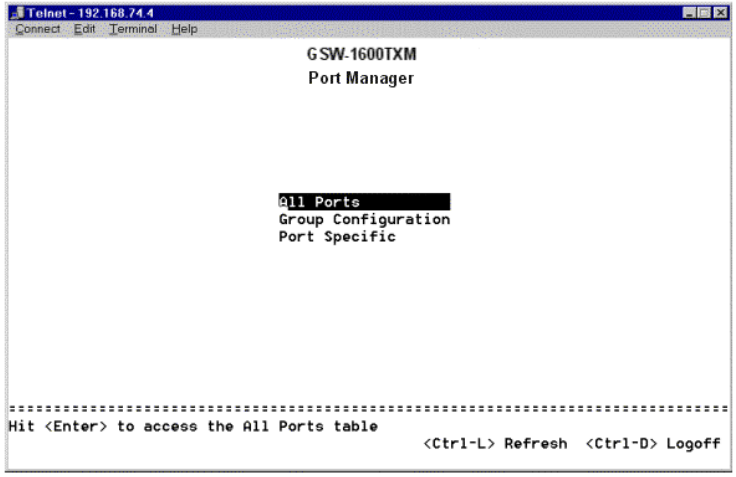


Figure 4-18: Port Manager

4.5.1 All Ports

Port Configuration, users can arrange the port characteristics related to link operations (see Figure 4-19). All of the parameters on this page are toggle settings. To switch or toggle between selections simply strike the space bar.

Admin Status field
Allows Administrator to Enable or Disable the port.

Speed field
The choices are 10Mbps, 100Mbps, and Auto (Auto-negotiate with the speed of the attached device).

Duplex field
Offers the choice of Full, Half, or Auto (will auto-detect the value of the attached device and set the port duplex accordingly).

Port Security field
When enabled, Port Security allows the administrator to specify which workstations on that port will be allowed to send packets into the switch. Only workstations, whose MAC address and switch port number are entered into the Static Bridge Table, will be allowed to send packets into the switch. (Note: The filtering occurs only for packets sent from the "Secured" ports to other ports. All packets sent from other ports to the "Secured" port will be sent without any filtering).

Flow Control
Flow control stops the sender from sending data until the receiver can accept it.

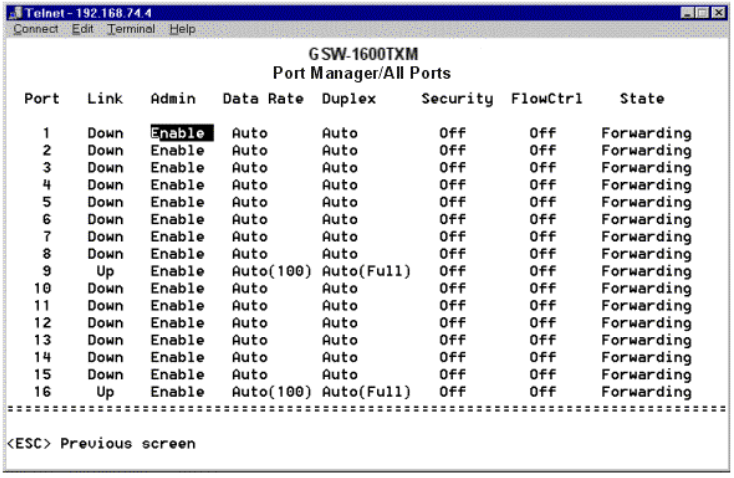


Figure 4-19: Port Manager: All Ports

4.5.2 Group Configuration

Group setup allows you to make identical changes to multiple ports at the same time. First setup up a group under the 'group setup' option, then changes can be made under 'Port Configuration', 'Spanning Tree Configuration', and 'VLAN Membership' menus.

Contains:

- Group Setup
- Port Configuration
- Spanning Tree Configuration
- VLAN Membership

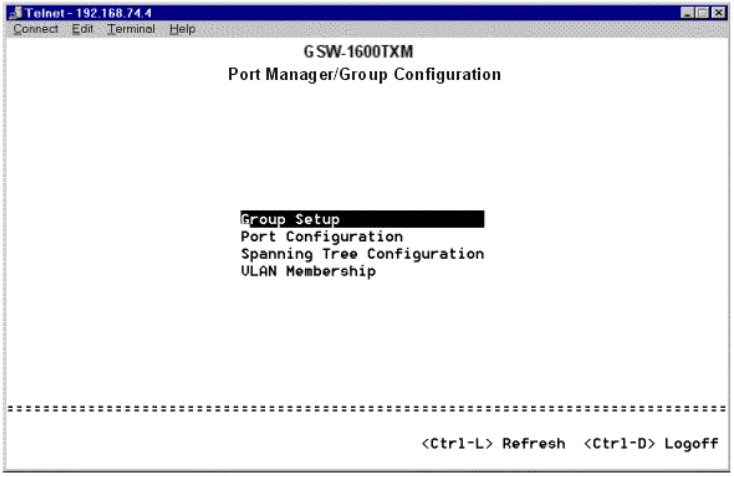


Figure 4-20: Port Manager: Group Configuration

4.5.2.1 Group Setup

There are three options for setting up the group.

- Specific Ports
- No Ports
- All Ports

Specific Ports:
Allows you to add or remove one port at a time.

No Ports:
Deletes all ports from the group.

All Ports:
Adds all ports to the group.

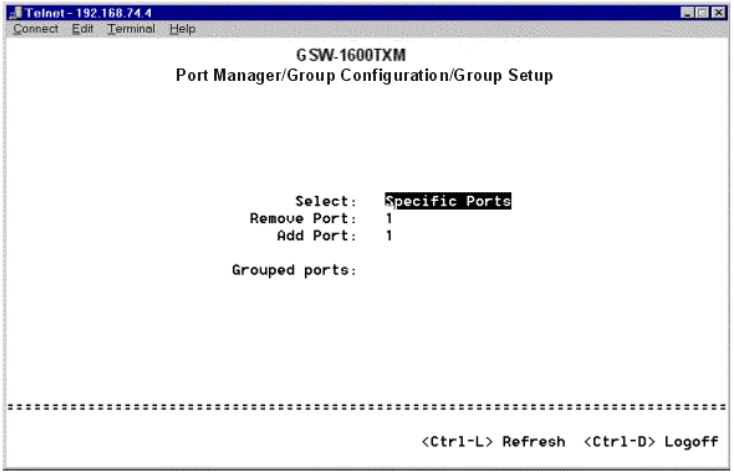


Figure 4-21: Group Setup

4.5.2.2 Port Configuration

The following parameters are accessible from this screen:

- Duplex
- Data rate
- Default VLAN
- Comments
- Admin Status
- Source Security
- Flow control

Please note that changes made in this screen will immediately change the setting for all the ports in the group.

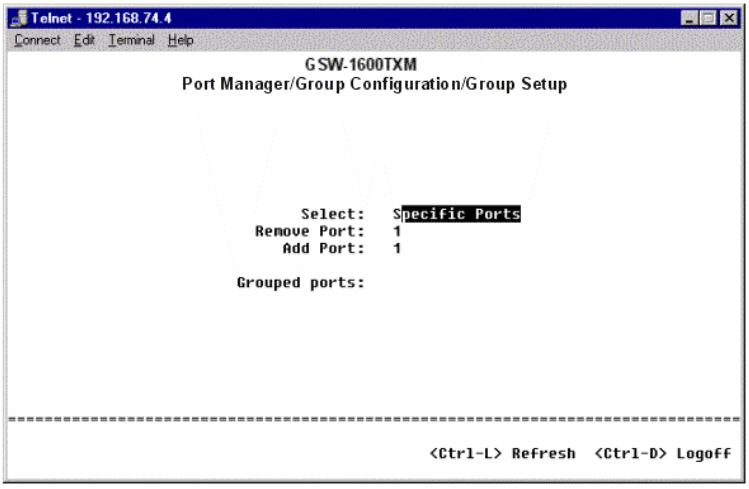


Figure 4-22: Port Configuration

4.5.2.3 *Spanning Tree Configuration*

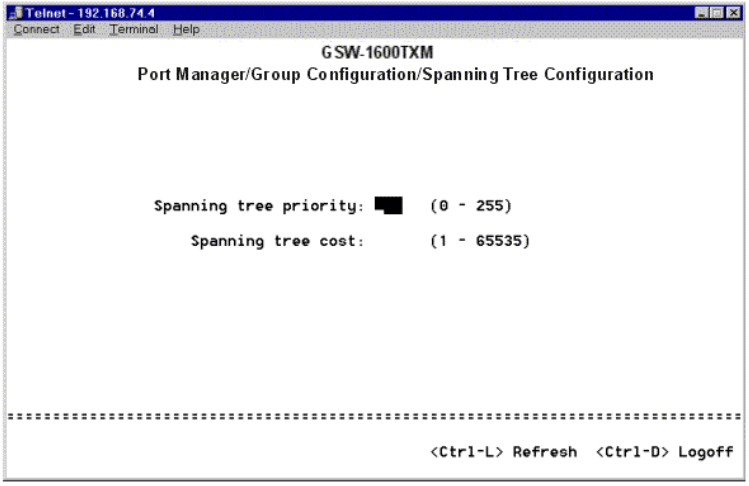


Figure 4-23: Spanning Tree Configuration

Changes to the Spanning Tree Priority and Cost can be made here. All ports in the group will be affected.

4.5.2.4 VLAN Membership

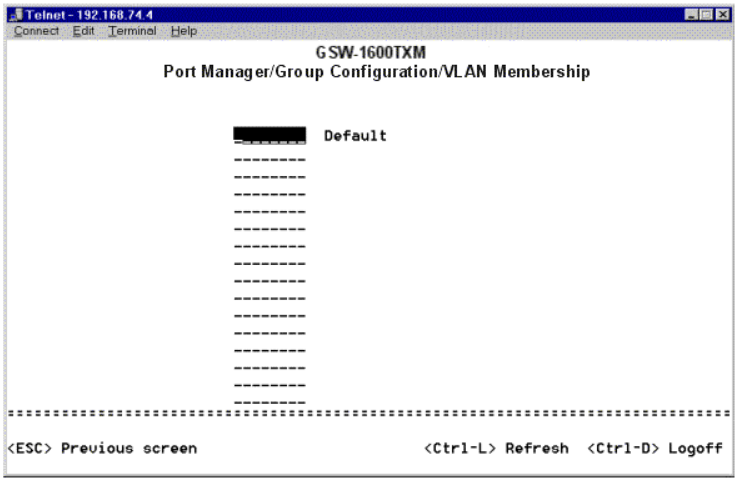


Figure 4-24: VLAN Membership

Hitting the SPACE bar will toggle the VLAN membership status for all ports in the group.

4.5.3 Port Specific

Contains:

- Port Configuration
- Spanning Tree Configuration
- VLAN Membership

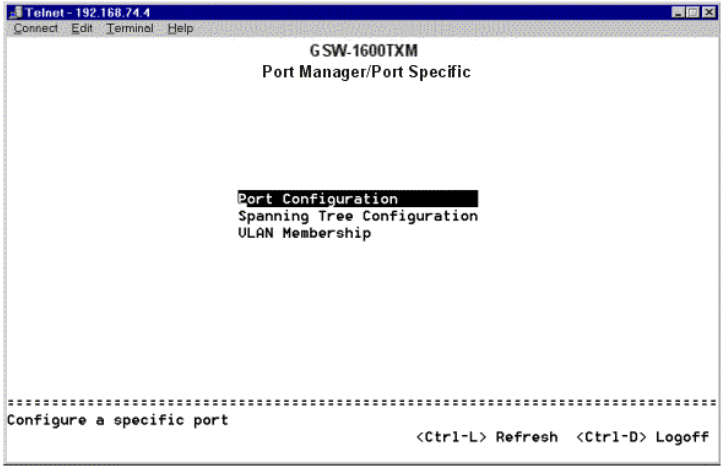


Figure 4-25: Port Specific

The options here are similar to those in the group configuration menus. The difference is that only the specified port will be changed.

4.5.3.1 *Port Configuration*

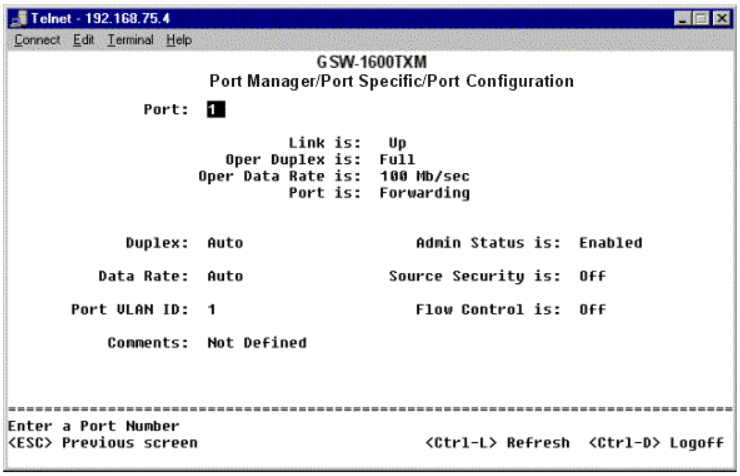


Figure 4-26: Port Configuration

The upper half of this screen shows the current status for the following parameters:

- Link Status
- Duplex
- Data Rate
- Port State

The lower half of the screen will allow you to make changes to the port settings.

4.5.3.2 Spanning Tree Configuration

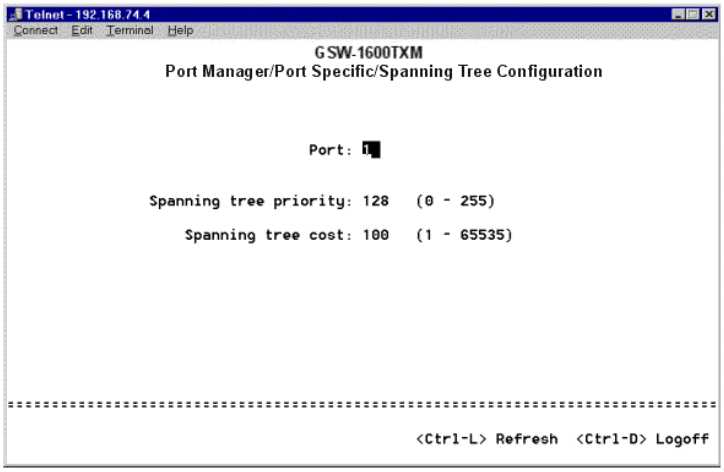


Figure 4-27: Spanning Tree Configuration

The Spanning Tree Priority and Cost can be set here for the specified port.

4.5.3.3 VLAN Membership

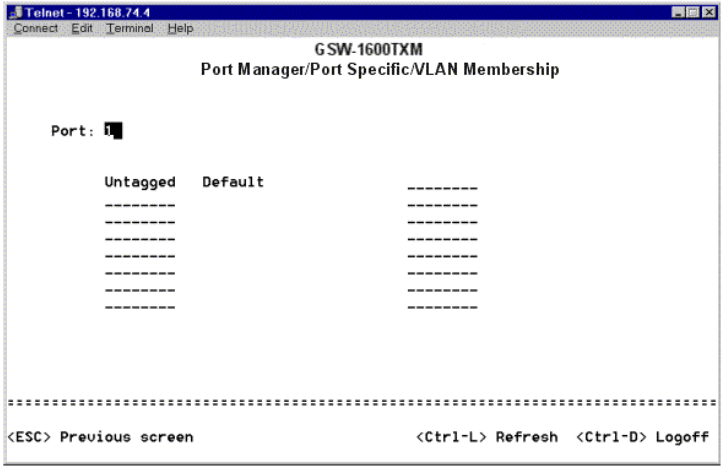


Figure 4-28: VLAN Membership

Hitting the SPACE bar will toggle the VLAN membership status for the specified port.

4.6 Statistics

There are two sections in this screen. The left-side Port-ID field allows users to choose a port to be observed. The central portion of the screen displays the basic statistics associated with the port, which is highlighted at the Port-ID field.

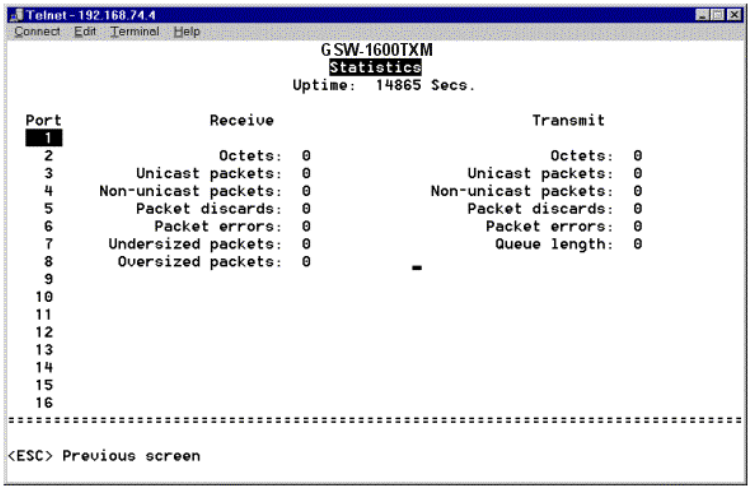


Figure 4-29: Statistics

Chapter 5 Software Upgrade Procedure

The application software is field upgradable. The upgrade procedure and the required equipment is described in the following section.

Note that once the system is up, it is controlled by an executing application image residing in the flash memory. No software upgrade is possible during this mode. The upgrade can only be done when the system is resetting. To initiate this sequence, the user must set the "boot mode" configuration parameter to "Boot from Net" during normal operation, and then perform a "reset". When the Boot-from-NET option is set, Bootstrap can start the system with an image residing on a TFTP server on the network. Be sure that the TFTP server residing on the network is accessible by the ADS-7000M. (Note: It is Highly recommended, though not necessary, to use a RS232 serial port connection to the switch during the software upgrading procedure. When using a Telnet Session or web interface alone, your connection to the switch will not be available until the switch has entered forwarding mode. This takes approximately three minutes. Once completed, the software version should be verified in the Software Download page. If the older version of the software has not been replaced, the unit was unable to reach the new software and booted from the old "flash" version)

The upgrade procedure is as follow:

1. Go to System Manager/General/Software Download (in the Web or Console Interface).
2. Set "Boot from Net" option during the normal operation.
3. Verify information such as the IP address for the TFTP Server, Gateway IP address, and the file name and its path of the new image, then perform "Submit" in the Web or "Ctrl-W" in the console interface. The bootstrap process allows for those items to be changed via the console.
4. Restart the system with "Boot from Net" set.
5. Bootstrap will retrieve the new image then pass control to it.
6. The system executes the new image.
   (Note that the previous image in the flash will not be replaced by the new image using this option. The image in the flash will be over-written if "Boot from Net and Saved" option is selected.)
7. If you decide to upgrade to the new image, go to Software Download again. Set "Boot from Net & Save" option, and perform "Submit" in the Web or "Ctrl-W" in the console interface.
8. Restart the system with "Boot from Net & Save" set.
9. The new image should over-write the old image in the Flash memory. Verify it by going to the Software Download screen and checking the Software Release information.

Note: It is recommended to perform the upgrade procedure from the Console Interface via RS232 serial port.

Appendix A: VLAN Description and Examples

Packets received by the switch will be treated in the following way with regard to the Switch's VLAN settings:

1) When an untagged packet enters a port, it will be automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting which is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in that port's respective Port Configuration page.

2) When a tagged packet enters a port, the tag for that packet will be unaffected by the default VLAN ID Setting.

3) The packet will now proceed to the VLAN specified by it's VLAN ID tag number.

4) If the port in which the packet entered does not have membership with the VLAN specified by the packets VLAN ID tag, the packet will be dropped. Port VLAN membership settings are changed in the VLAN Membership page.

5) If the port has membership to the VLAN specified by the packet's VLAN ID, the packet will be able to be sent to other ports with the same VLAN ID membership.

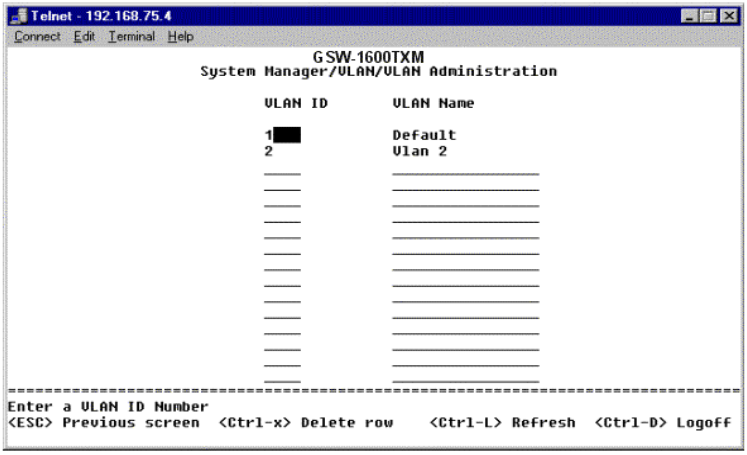
6) Packets leaving the switch will be either tagged or untagged depending on the setting specified for that port's membership properties.

7) A 'U' for a given port and VLAN will mean that packets leaving the switch from that port and VLAN will be Untagged. Inversely, a 'T' for a given port and VLAN will mean that packets leaving the switch from that port and VLAN will be tagged with the respective VLAN ID in which it participated in.

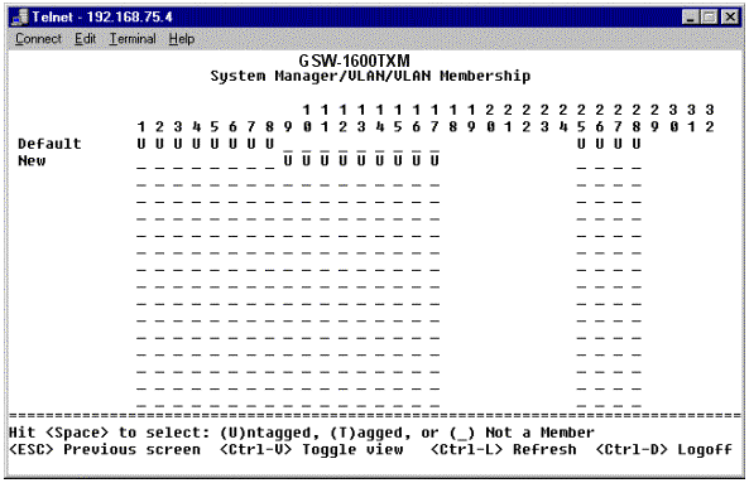
Two examples of for setting up VLANs will be given. Example 1 will step through a simple two group VLAN setup. Example 2 will step through a more elaborate setup illustrating all possible scenarios for a comprehensive understanding of tagged VLANs.

Example 1:

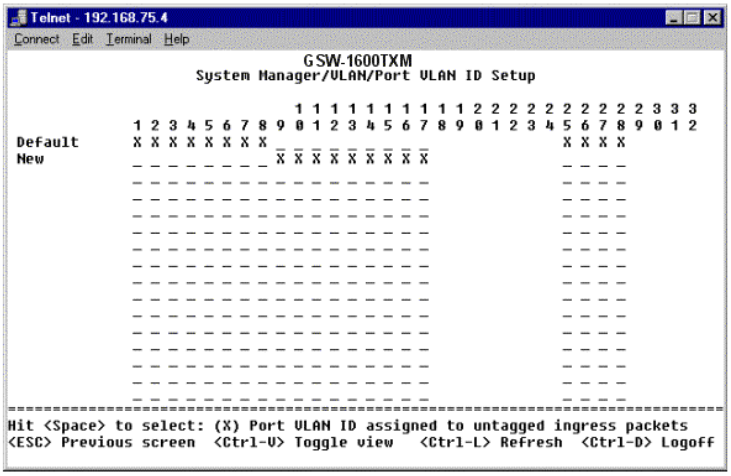
1) In the VLAN Administration page, add a new VLAN to the list, shown below as "New" with a VLAN ID value of 2.



2) In the VLAN Membership page, use the space bar to toggle matrix until, the desired ports are all members of the selected VLAN.

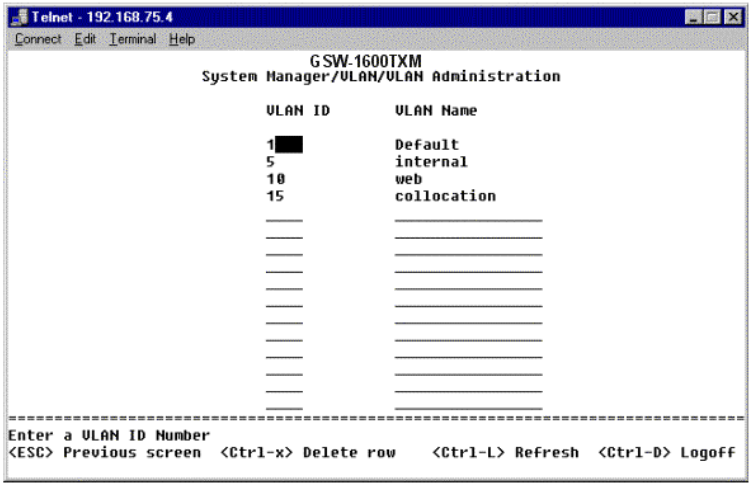


3) To allow untagged packets to participate in the ‘New’ VLAN, make sure to change the Port VLA N IDs for the relevent ports. To access the Port VLAN ID page hit ‘Ctrl-V’. Use the space bar to add an ‘X’ indicating which PVID is assigned to which port.

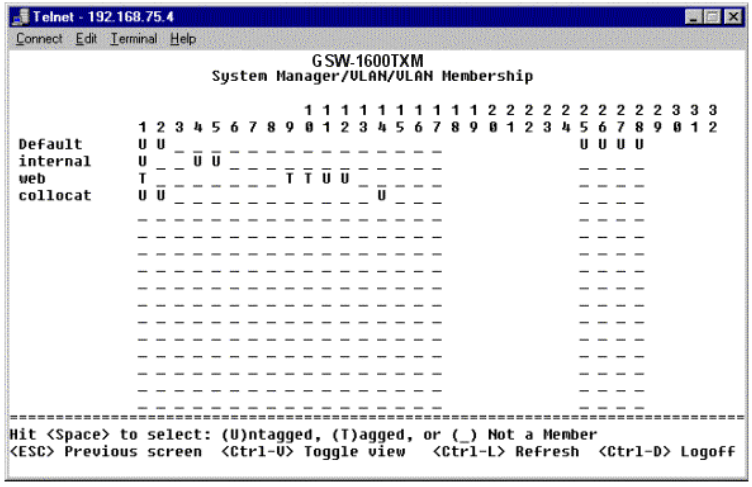


Example 2:

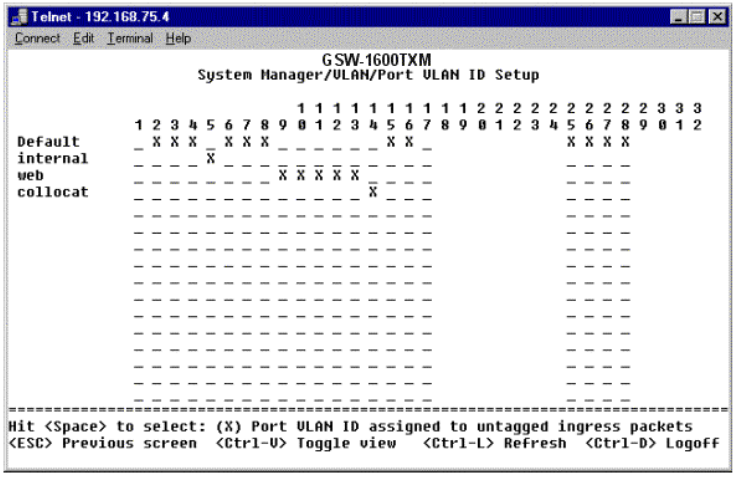
1) Setup the following VLANs:



2) Configure the VLAN membership has follows:



3) Setup the Port VLAN IDs as follows (note that port one PVID is set to 2. This must be done in the port specific page since there is no VLAN with ID 2):



The specific ports above have the following Port VLAN ID settings (The Port VLAN ID settings for each port are configured in their respective Port Configuration page or by hitting 'Ctrl-V' in the VLAN Membership page):

Port 01: 2	Port 05: 5	Port 09: 10	Port 13: 10
Port 02: 1	Port 06: 1	Port 10: 10	Port 14: 15
Port 03: 1	Port 07: 1	Port 11: 10	Port 15: 1
Port 04: 1	Port 08: 1	Port 12: 10	Port 16: 1

The following scenarios will produce results as described below:

1) If an untagged packet enters Port 4, the switch will tag it with a VLAN tag value of 1. Since Port 4 does not have membership with VLAN ID 1 (named "default"), the packet will be dropped.

2) If a tagged packet with a VLAN tag value 5 enters Port 4, the packet will have access to Ports 5 and 1. If the packet leaves Port 5 and/or 1, it will be stripped of its tag becoming an untagged packet as it leaves the switch.

3) If an untagged packet enters Port 1, the switch will tag it with a VLAN tag value of 2. It will then be dropped since Port 1 has no membership with VLAN ID 2.

4) If a tagged packet with a VLAN tag value 10 enters Port 2, it will have access to Ports: 1, 9, 10, 11, and 12. If the packets leave Ports 1, 9, or 10, they will be

tagged with a VLAN ID value of 10. If the packet leaves Ports 11 or 12, it will leave as an untagged packet.

5) If a tagged packet with a VLAN tag value 1 enters Port 9, it will be dropped since Port 9 does not have membership with VLAN ID 1.

Appendix B: Networking Connection

When attaching an end-station to the device, a standard straight-through CAT5 cable may be used, even when the end-station is attached via a patch panel. However, when attaching another switch or attaching workstations via hubs, a crossover cable will need to be used. Please see the following wire diagrams for examples of both cable types.

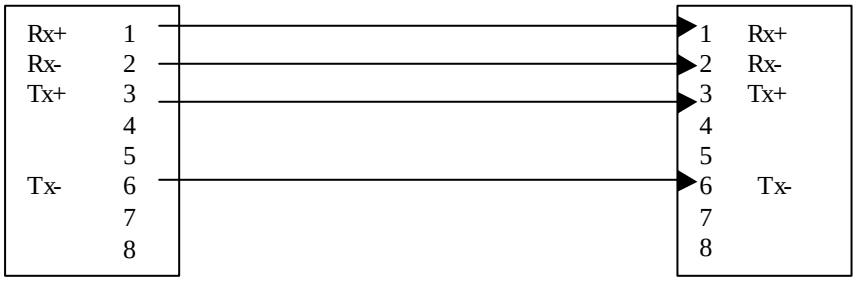


Figure A-1: Straight-Through Cable

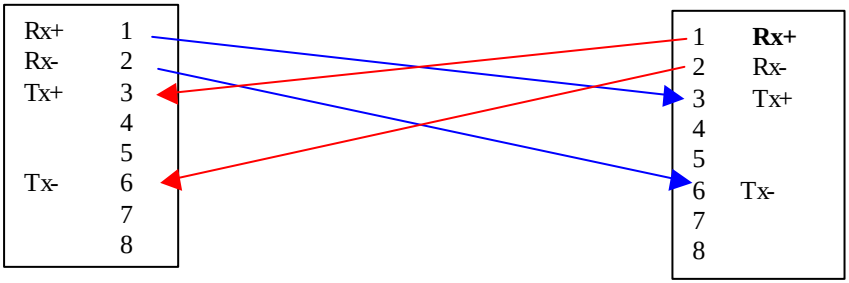


Figure A-2: Crossover Cable

Appendix C: Technical Specifications

Standard

IEEE802.3, IEEE802.3u, IEEE802.3z, IEEE802.1d

Interface

RJ-45 10/100M Ethernet Port	16
MII	1
RS232 Male connector	1
Slide-in Slot	2

Indicator

System LEDs	1
Port LEDs:	
100M/10M	1 per port
Full/Col	1 per port
Link/Act	1 per port

Power

Input	100-240VAC 50-60Hz

Environment

Temperature Operating	0º to 40ºC
Storage	-20º to 70ºC
Humility Operating	10 to 90 % RH
Storage	5 to 90 % RH

EMI

FCC Class A, CE Class A, VCCI, AS

Safety

UL, CSA, TUV

Dimensions

440mm x 258mm x 65mm