HIRSCHMANN
Rheinmetall Elektronik

HIWAY WEBBASED NETWORK MANAGEMENT FOR

FES-24TP PLUS AND GES-24TP/2SX

USER GUIDE

Version 03/99

Richard Hirschmann GmbH&Co.
Stuttgarter Str. 45-51
D-72654 Neckartenzlingen
(07127) 14 1538

Hirschmann worldwide:

Richard Hirschmann GmbH & Co.
Stuttgarter Straße 45-51
D-72654 Neckartenzlingen
Tel ++49-7127-14-1527
Fax ++49-7127-14-1542
email: n-hi-line@nt.hirschmann.de
Internet: www.hirschmann.de

Richard Hirschmann GmbH & Co.
Oberer Paspelweg 6-8
A-6830 Rankweil-Brederis
Tel ++43-5522-3070
Fax ++43-5522-307555
A-1230 Wien
Tel ++43-1-6174646
Fax ++43-1-6174646
email: cherz@nt.hirschmann.de

Hirschmann España S.A.
Calle Traspaderne, 29
Barrio del Aeropuerto
Edificio Barajas 1,2 Planta
E-28042 Madrid
Tel ++34-1-7461730
Fax ++34-1-7461735
email: hirschmann.fuente@mad.servicom.es

Richard Hirschmann
Electronics UK Ltd.
St. Martins Way
St. Martins Business Centre
GB-Bedford MK42 OLF
Tel ++44-1234-345999
Fax ++44-1234-352222
email: richardhirschmann@compuserve.com

Richard Hirschmann
Electronica Nederland B.V.
Postbus 92
NL-1380 AB Weesp
Tel ++31-294-462500
Fax ++31-294-480639
email: nwt@hirschmann.nl

Richard Hirschmann
Electronique S.A.
24, rue du Fer à Cheval, Z.I.
F-95200 Sarcelles
Tel ++33-1-39330280
Fax ++33-1-39905968
email: yfave@hirschmann.fr

Hirschmann - Hungária Kft.
Rokolya u. 1-13
H-1131 Budapest
Tel. ++36-1-1494199
Fax. ++36-1-1298453

Richard Hirschmann
of America, Inc.
30 Hook Mountain Road - Unit 201
USA-Pine Brook, N. J. 07058
Tel ++1-973-8301470
Fax ++1-973-8302000
email: sschueler@hirschmann-usa.com

Hirschmann Electronics
(Asia Pacific) Pte. Ltd.
3, Howard Road - Tat Hong
Industrial Building #04-00
SGP-Singapore 369578
Tel ++65-382-2055
Fax ++65-382-2755
email: hirschmann.ap@pacific.net.sg

TABLE OF CONTENTS

1. OVERVIEW

HiWay Webbased Network Management Application Description

This user guide describes the Hirschmann HiWay Webbased Network Management application, a web browser-based utility which allows you to configure and manage Hirschmann FES/GES family switches remotely. There is no software to install as web management capability is built into each switch.

The Hirschmann HiWay Webbased Network Management application provides a graphical, real time representation of an FES/GES family switch front panel. This graphic, along with additionally defined areas of the browser interface, allow you to interactively configure the switch, monitor its status, and view statistical information.

The HiWay Webbased Network Management application provides a simple, intuitive method for managing FES/GES family switches. The switches can also be managed via serial console, Telnet, or SNMP.

Features

- Switch configuration and monitoring from any Java-enabled browser
- Easy to navigate menuing system
- Detailed parameter descriptions using Help button
- Statistical analysis using tables, graphs and charts
- Switch operating status using front panel area LEDs and color indications
- Extensive Alarm configuration capability

System Requirements

The requirements for running the HiWay Webbased Network Management application are relatively simple. You will need a Java-enabled, frames-capable web browser and a TCP/IP network connection to the switch, whether over a local network, a remote private network, or over the Internet.

When connecting over the Internet, the integrity of your connection will have an impact on the speed and performance of tasks. If your connection is subject to prohibitive periods of network congestion, or experiences high packet loss, you may need to consider a different Internet service provider.

In addition, the HiWay Webbased Network Management application uses SNMP for some of its communications with the switch. This may cause problems when the application is run across some Internet firewalls, which may be configured to disallow SNMP access.

Conventions

This guide uses the following user input conventions:

- When you read "Select," use the mouse to either select the link identified by a hand icon, or select the identified button or area.
- When you read "Enter", type in the text and select the button identified in the procedure.

2. USING WEB-BASED MANAGEMENT

Setting Up Web Management

Before running web-based management, some basic configuration of the switch may need to be performed. The following information at a minimum must be configured or known for each switch to be managed:

- IP Address
- SNMP Public Community Name
- Web Management Enable

In addition, several other parameters may need to be configured or known to properly communicate with the switch or allow full management capability. These include:

- SNMP Private Community Name
- Default Gateway
- Trap Destination and Community Name

Configuration of these items may be made from the User Interface, which is accessible via either the serial console or Telnet. Refer to the Installation and User Guide that came with your system for more information about setting up either of these connections to the switch. The following subsections describe the required configuration.

Setting an IP Address

The switch IP address must be set before it can be managed with HiWay Webbased Network Management application. The switch IP address may be automatically set using the BootP or DHCP protocols, in which case the actual address assigned to the switch must be known. Refer to the Installation and User Guide.

The IP address may alternatively be set manually as follows:

1. Select System Configuration Menu from the Main Menu of the User Interface.
2. Select IP Address from the menu and enter the IP address. Press Enter.

   The IP address is now programmed. The subnet mask is set to automatically correspond to the class of the address entered. If a different mask is used on the network:
3. Select Subnet Mask from the menu and enter the appropriate mask. Press Enter.

Setting Community Names

Community names are used by the SNMP protocol as a means of user authentication when managing network devices. The HiWay Webbased Network Management application uses the same community names as SNMP to provide a level of security similar to passwords for access to its browser interface. The SNMP Public Community Name allows read-only (monitoring) access to the switch. The SNMP Private Community Name allows read/write (monitoring and configuring) access to the switch.

1. Select System Configuration Menu from the Main Menu of the User Interface.
2. Select SNMP Configuration Menu.
3. Select SNMP Public Community Name from the menu and enter the community. Press Enter.
4. Select SNMP Private Community Name from the menu and enter the community. 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. This parameter must be set if you are attempting to manage the switch using the HiWay Webbased Network Management application from a remote network or across the Internet.

1. Select System Configuration Menu from the Main Menu of the User Interface.
2. Select Default Gateway from the menu and enter the router IP address. Press Enter.

Setting Trap Destinations

If you wish to record SNMP traps, or events, generated by the switch, you must configure Trap Destinations. A trap destination is the IP address of the system being used to manage the device, in this case the IP address of the computer system on which the HiWay Webbased Network Management application is being run.

1. Select System Configuration Menu from the Main Menu of the User Interface.
2. Select SNMP Configuration Menu.
3. Select a Trap Destination entry from the menu and enter the community name. Press Enter.
4. Select the corresponding Community Name entry from the menu and enter the community name. Press Enter.

Setting Web Management Enable

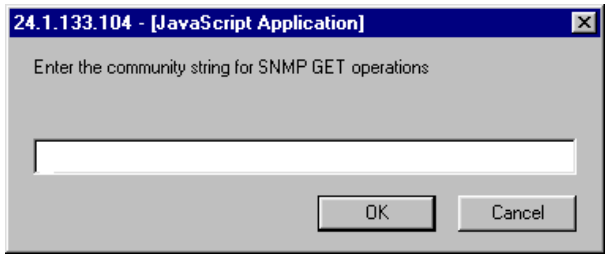
The Web Management Enable parameter is used to enable or disable the ability to manage the switch with web management. Web Management Enable must be set to Yes before the HiWay Webbased Network Management application can be used to manage the switch. If it is desired to disallow web management of the switch, this parameter should be set to No.

1. Select System Configuration Menu from the Main Menu of the User Interface.
2. Select Web Management Enable to toggle between Yes and No.

Starting & Stopping HiWay Webbased Network Management

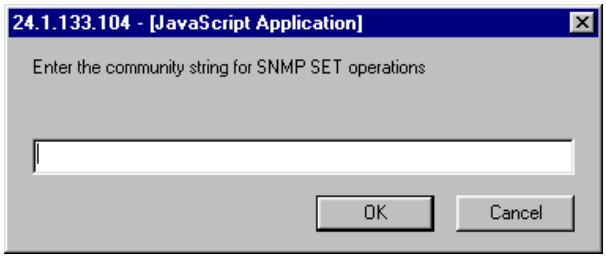
Do the following to use the HiWay Webbased Network Management application:

1. Start a Java-enabled web browser from any machine with network access to the switch.
2. Enter the IP address for the switch you want to manage in the URL field of the browser.
3. Two screens will appear in sequence, prompting you to enter two SNMP community names. These community names correspond to the values entered previously in the Setting Up Web Management section. One or both of the values may be entered, depending on the level of access to the switch being allowed. The following screen is the first to appear:



4. Enter the SNMP public community name previously configured for the switch in this field, then select OK.

   The following screen then appears:



5. Enter the SNMP private community name previously configured for the switch in this field, then select OK.

   This entry allows read/write access to the switch. If this value is not entered, and the SNMP public community name is, read-only access to the switch will be established.

   The full application will now launch. A four-frame page will display with the product graphic located in the upper right hand frame.

6. To stop the HiWay Webbased Network Management application, close the web browser application.

HiWay Webbased Network Management User Interface

The HiWay Webbased Network Management user interface provides access to various switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor system status.

Areas of the User Interface

Figure 2-1 shows the HiWay Webbased Network Management user interface. The user interface is divided into four distinct areas as described in Table 2-1.

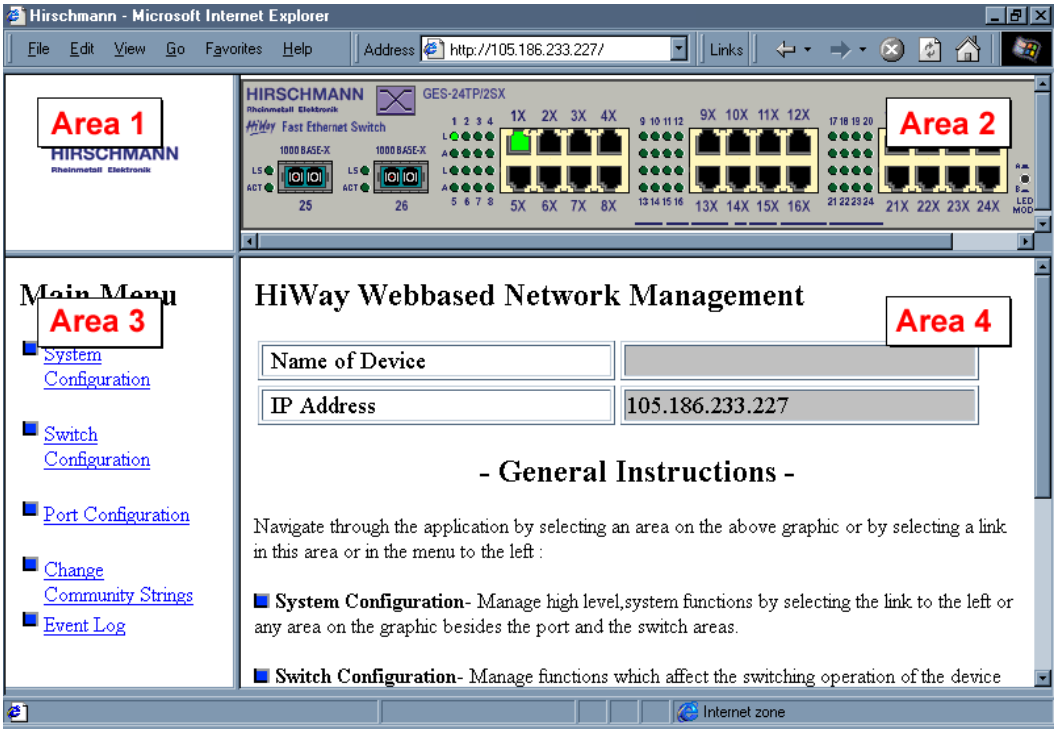


Figure 2-1. HiWay Webbased Network Management User Interface

Table 2-1. Areas of the User Interface

Area	Function
1	Displays the Hirschmann logo. Selecting this area takes you directly to the Hirschmann web site.
2	Presents a graphical near real-time image of the switch front panel. Various areas of the graphic can be selected for performing management functions (see Table 2-2 for details).
3	Displays a list of links allowing you to go to the associated menu or screen by selecting the item. You can use the "Home" selection to return to the top level of the screen hierarchy.
4	Presents switch information based on your selection, as well as links to other associated selections.

Table 2-2 describes configuration and system information functions available in Area 2.

Table 2-2. Area 2 Functions

Function	Description
System Configuration	Allows you to go directly to the System Configuration Menu by selecting any area not identified by another specific function in this table (such as the gray background).
Switch Configuration	Allows you to go directly to the Switch Configuration Menu by selecting the purple "X" symbol located in the upper left hand corner.
Port Configuration	Allows you to go directly to the Port Configuration Menu by selecting inside the individual port, or on the numeric port designation.
Link LEDs	Link LED on: A light green color indicates a valid connection (link up) on the associated port. Link LED off: A dark green color indicates no link (link down) on the associated port.
Port Status	A light green color inside the port icon indicates that the port is linked. An amber color inside the port icon indicates that the port is disabled. A black color inside the port icon indicates that the port is neither linked nor disabled.
Console port	Allows you to launch a Telnet session by selecting the console port graphic.

The Activity, Power, and Test LEDs, and the LED Mode button on the Area 2 graphic are non-functional.

Navigating the System

The HiWay Webbased Network Management application contains navigation tools to assist you in moving around the interface. A "Back" arrow appears on some screens in Area 4, and is used to return to return to the previous screen.

Using Help

General HiWay Webbased Network Management help guidelines are available from the Home page in Area 4. For detailed help descriptions for individual pages, select the "Help" icon represented by a question mark.

3. CONFIGURING & MONITORING THE SWITCH

This section, arranged by topic, describes how to perform common monitoring and configuration tasks on an FES/GES family switch using the HiWay Webbased Network Management application. After you have properly configured the switch, and started the application, you can perform any of the tasks described in the following sections.

Screen Hierarchy

This chapter is arranged following the structure shown in Area 4 of the HiWay Webbased Network Management application. Figure 3-1 shows the Screen Hierarchy.

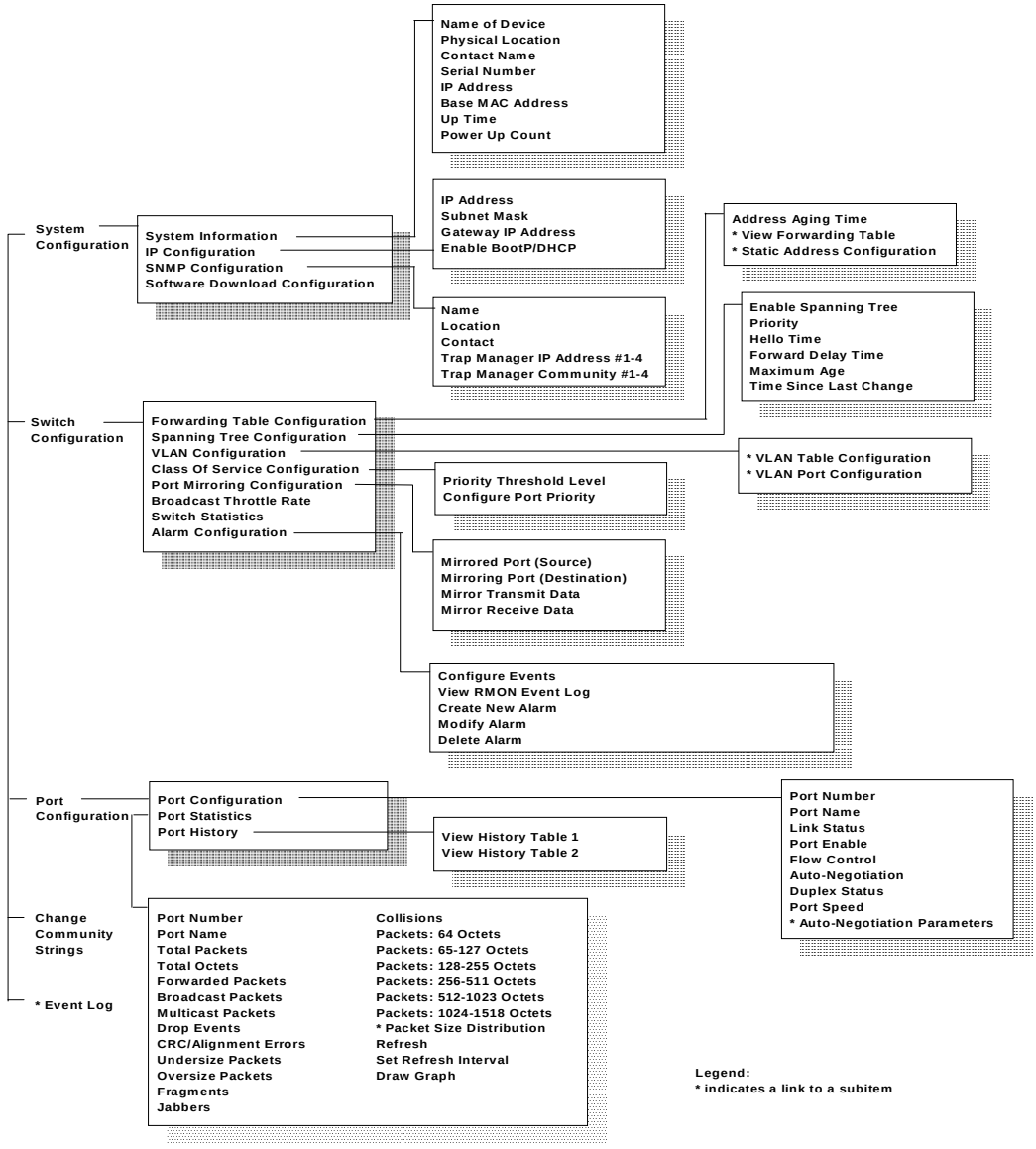


Figure 3-1. HiWay Webbased Network Management Screen Hierarchy

System Configuration

The following configuration options are available by selecting the System Configuration link from the HiWay Webbased Network Management application home page in Area 3, or by selecting a blank area on the switch graphic front panel in Area 2. These configuration options affect the overall configuration and management settings of the switch.

System Information

The System Information screen displays a summary list of switch configuration information. This screen is read-only. When you select System Information, the parameters appear as shown in Table 3-1.

Table 3-1. System Information Fields

Parameter	Description and Configuration Information
Name of Device	An administratively-assigned name for the switch. This setting is changed using the Name option in the SNMP Configuration screen.
Physical Location	The physical location of the switch (e.g., `telephone closet, 3rd floor'). This setting is changed using the Location option in the SNMP Configuration screen.
Contact Name	The textual identification of the contact person for this switch, together with information on how to contact this person. This setting is changed using the Contact option in the SNMP Configuration screen.
Serial Number	The serial number of the switch.
Software version	The version of software currently running on the switch.
IP Address	The IP Address of the switch. This setting is changed using the IP Address option in the IP Address configuration screen.
Base MAC Address	The MAC address used by the switch when it must be referred to in a unique fashion. It is the numerically smallest MAC address of all ports on the switch.
Up Time	Amount of time that has elapsed since the switch was last powered up or reset.
Power Up Count	The total number of times the switch has powered up since it was shipped from the factory.

IP Configuration

The IP Configuration screen allows the configuration of several switch IP protocol-related parameters. Make the appropriate changes, then select Apply to save changes to the configuration. To configure IP parameters:

1. Select IP Configuration.

   Fields for IP Address, Subnet Mask, Gateway IP Address and Enable BootP/DHCP appear.

2. You can enter the switch IP address in the IP Address field.

3. You can enter the switch subnet mask in the Subnet Mask field.

4. You can enter the switch gateway IP Address in the Gateway IP Address field.

5. Select either "enable" or "disable" in the Enable BootP/DHCP field.

6. Select Apply to save changes to the configuration.

SNMP Configuration

The SNMP Configuration screen allows the configuration of several SNMP related parameters of the switch. The Trap Manager entries on this screen are the same as the Trap Destination parameters described in Chapter 2 in the section Setting Up Web Management. A Trap Manager entry must be configured using the IP address of the workstation running the HiWay Webbased Network Management application in order for it to be able to receive SNMP traps. The traps themselves can be viewed in the Event Log, described below.

1. Select SNMP Configuration.

   Fields for Name, Location, Contact, Trap Manager IP Addresses #1 through #4, and Trap Manager Communities #1 through #4 appear.

2. You can enter a unique name for the device in the Name field, the location of the device in the Location field, and the name of a system contact in the Contact field.

3. Select one or more trap manager entries from the menu and enter the appropriate IP addresses.

4. For each trap manager entered, a corresponding community name should be entered.

5. Select Apply to save changes to the configuration.

Software Download Configuration

This procedure allows you to download a software upgrade to the software storage sector in the flash memory of the switch. The procedure uses a TFTP server connected to the network and downloads the software using the TFTP protocol. A TFTP server must be configured and

running on a network for this procedure to work properly. See the Installation and User Guide that came with your switch for more detailed information. To perform a software download:

1. Select Software Download Configuration.
2. Enter the TFTP Server IP Address.
3. Enter the Download File Name. Path information must be included in the file name.
4. Select Start Software Download.
5. Select the Start Download button.

   During the download process, communication with the switch via the HiWay Webbased Network Management application will be lost.
6. After starting the download process, close the HiWay Webbased Network Management application, then restart the application after a few minutes to reestablish connection with the switch.
7. Go to the System Information screen to verify that the software version shown matches that of the upgrade.

Switch Configuration

The following configuration options are available by selecting the Switch Configuration link from the HiWay Webbased Network Management application home page in Area 3.

Or, you can use go to the Switch Configuration link by selecting the "X" symbol within Area 2.

These configuration options affect the actual switching of data through the switch.

Forwarding Table Configuration

The Forwarding Table Configuration screen allows you to designate forwarding treatment through the switch for specific MAC addresses, enabling you to maintain the efficiency and security of your network. Refer to the Installation and User Guide for more detailed information. To configure the forwarding table:

1. Select Forwarding Table Configuration.

   The first field that displays is the Address Aging Time field. The address aging represents the timeout period in seconds for aging out dynamically learned address forwarding information. The 802.1D-1990 standard recommended default is 300 seconds.
2. Enter the desired address aging time in the field.
3. Select Apply.
4. Select View Forwarding Table.

The View Forwarding Table appears. You can select the "?" icon for a description of the parameters in the table.

a. Select the Refresh button to refresh the table information.

b. Select the Set Refresh Interval button to change the refresh intervals. The Set time interval default setting is 5 seconds.

c. Enter the new Set time interval and select OK.

5. Select Static Address Configuration.

The Static Address Configuration screen appears.

a. Select the Add New Address button to add a new address.

The Add New Static Address window appears.

1) Enter the New MAC Address.

2) Set the address disposition (Discard or Forward)

3) Enter the port number and select Apply.

b. Select the Modify Address button to modify an existing address row.

The Static Address Configuration window appears.

1) Select the Select button in the row you want to modify.

2) Select the Modify Address button.

3) The Modify Static Address window appears.

4) Enter the port number and select Apply.

c. Select the Delete Address button to delete an existing address row.

1) Select the Select button in the row you want to delete.

2) Select the Apply button.

Spanning Tree Configuration

The Spanning Tree Protocol allows redundant connections to be created between LAN segments for purposes of fault tolerance. To configure Spanning Tree parameters:

1. Select Spanning Tree Configuration.

The Spanning Tree Configuration window appears.

2. Select either "on" or "off" in the Enable Spanning Tree field to enable Spanning Tree operation on the switch, then select Apply.

3. Change any of the settings on the screen and select Apply.

If you enter an invalid value in any of the fields, the switch will ignore the value and return to the previous valid setting.

VLAN Configuration

A virtual LAN (VLAN) is a group of network devices on one or more network segments configured such that they can communicate as if they are on the same LAN. Refer to the Installation and User Guide for more detailed information on VLANs.

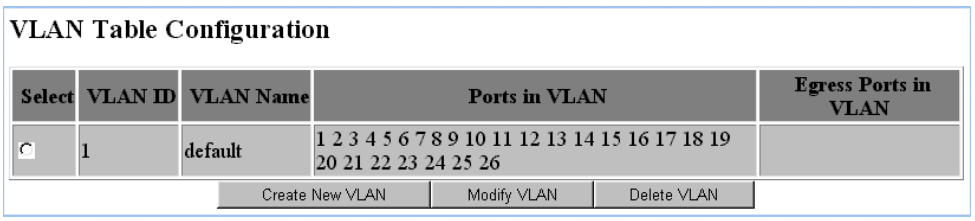
To configure VLAN parameters:

1. Select VLAN Configuration.

2. Select either "enable" or "disable" in the Enable VLANs field to enable or disable VLAN operation on the switch, then select Apply.

3. Select VLAN Table Configuration.

The VLAN Table Configuration window appears.

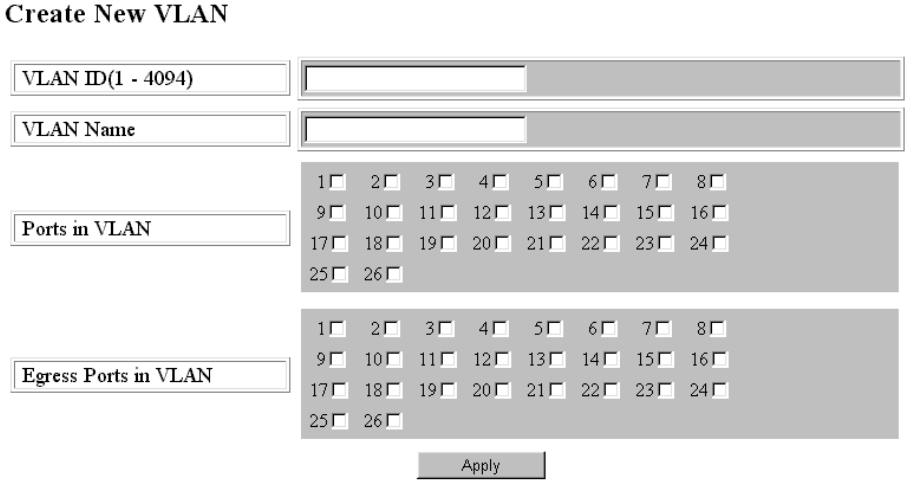


This table displays a list of VLANs configured on the switch. By default, there is one VLAN containing all ports on the switch.

4. To create a new VLAN:

a. Select the Create New VLAN button.

The Create New VLAN window appears.



b. Enter the ID for the new VLAN. It must be a new ID not already configured on the switch. Valid values are 1-4094.

c. Enter a VLAN name.

d. Select the ports in the new VLAN.

e. Select the egress ports in the new VLAN.

f. Select Apply.

The VLAN Table Configuration appears with the newly created VLAN listed.

5. To modify an existing VLAN:

a. select the Select button in row you want to modify.

b. Select the Modify VLAN button.

The Modify VLAN window appears.

c. Modify the settings and select Apply.

6. To delete an existing VLAN:

a. Select the Select button in the row you want to delete.

b. Select Delete.

7. To configure VLANs on a per-port basis:

a. Select VLAN Port Configuration.

The VLAN Port Configuration window appears.

Select	Port Number	Port Name	VLAN ID	VLAN Port Type
○	1		2	access
○	2		2	access
○	3		2	access
○	4		1	access
○	5		1	access
○	6		1	access
○	7		1	access
○	8		1	access
○	9		1	access
○	10		1	access
○	11		1	access
○	12		1	access

b. Select the Select button in the row you want to modify.

c. Select the Modify Port VLAN button.

The Modify Port VLAN window appears.

d. Enter a new VLAN ID for the port if you wish to change it.

e. Select either "access" or "hybrid" in the VLAN Port Type field and select Apply.

The modifications now appear in the VLAN Port Configuration window.

Class of Service Configuration

The Class of Service Configuration menu permits you to configure priority levels to traffic being forwarded through the switch. Refer to the Installation and User Guide fro more detailed information on Class of Service.

1. Select Class of Service Configuration.

2. Select either "enable" or "disable" in the Enable Class of Service field and select Apply. This setting enables or disables Class of Service operation for the switch.

3. To configure the priority threshold level, select a number between 0 and 7 in the Priority Threshold field and select Apply.

4. To configure port priority, select Configure Port Priority.

The Port Priority Configuration window appears.

Select	Port Number	Port Name	Priority Level
○	1		0
○	2		0
○	3		0
○	4		0
○	5		0
○	6		0
○	7		0
○	8		0
○	9		0
○	10		0
○	11		0
○	12		0

5. Select the Select button in the row you want to configure.

6. Select the Modify Port Priority button.

The Modify Port Priority window appears.

7. Select a number between 0 and 7 in the Priority Level field and select Apply.

The modifications now appear in the Port Priority Configuration window.

Port Mirroring Configuration

When Port Mirroring is enabled, one 10/100 port in each group of eight becomes a monitor port for any one of the other ports within the group.

1. Select Port Mirroring Configuration.
2. Select either "enable" or "disable" in the Enable Port Mirroring field. Selecting "enable" activates port mirroring between the Mirrored Port and the Mirroring Port.
3. Enter the port number of the Mirrored Port (Source).
4. Enter the port number of the Mirroring Port (Destination).
5. Select either "enable" or "disable" in the Mirror Transmit Data field. Selecting "enable" activates the mirroring of data transmitted out of the mirrored port.
6. Select either "enable" or "disable" in the Mirror Receive Data field. Selecting "enable" activates the mirroring of data received by the mirrored port.

Either Mirror Transmit Data or Mirror Receive Data can be enabled at one time. Enabling one of these options automatically disables the other option.

7. Select Apply to confirm your settings.

Broadcast Throttle Rate

The Broadcast Throttle Rate of the switch allows for the control of broadcast storms. The value of this variable sets a per second rate (valid range is 100-500,000). To configure the broadcast cutoff rate, do the following:

1. Select Switch Configuration from the Main Menu.
2. Enter the Broadcast Throttle Rate and select Apply.

Switch Statistics

To view overall switch-level statistical parameters in real-time, do the following:

1. Select Switch Statistics
   The Switch Statistics window appears.

Total Packets	42551
Total Octets	9470943
Total Forwarded Packets	1
Total Filtered Packets	983038
Total Errors	2
Total Collisions	2

2. Select the Refresh button to manually refresh switch statistics.
3. Select the Set Refresh Interval button to set the time interval for automatic refresh of switch statistics, and select the OK button.

Alarm Configuration

The switch alarm and event capabilities are part of the RMON functionality of the product. An alarm is a configuration setting that is made to monitor thresholds of statistical parameters on the switch. When a statistical threshold is reached, the alarm is triggered. When an alarm is triggered, a configured event, or action, associated with the alarm is executed. An executed event may be configured to either log the occurrence locally on the switch in the RMON Event Log, send an SNMP trap message to a remote network management station, or do both.

When configuring switch alarms and events, it must be first determined what statistical information would be the most useful to monitor. Setting an alarm on the number of octets seen on a specific port, for example, would allow you to be alerted when the network utilization of a specific port exceeds a certain value. Setting an alarm on the number of a certain type of error packets seen on a specific port would allow you to be alerted of a potential network hardware problem.

Alarm and event configuration is accomplished by first selecting the Alarm Configuration link on the Switch Configuration screen. Start the configuration by first setting up one or more events, then set up the specific alarms.

Configure Events

1. Select Configure Events

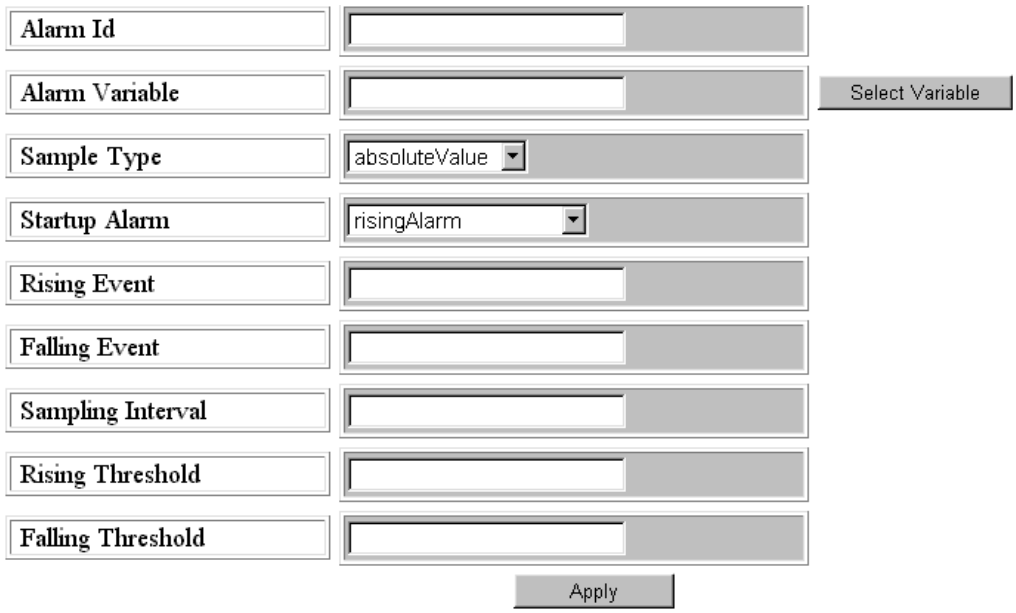
   The Event Configuration screen appears. This screen displays a table of all currently configured events on the switch. Each event is identified by a unique Event ID. From this screen you have the following options: Create New Event, Modify Event, or Delete Event.
2. To create a new event:
   - **a**. Select the Create New Event button.
   - **b**. Enter a unique Event ID. Valid values are between 1 and 65535. Select an Event ID that does not already appear in the table.
   - **c**. Select one of the four values in the Type field. Selecting "none" will cause no action to be taken when the event is triggered. Selecting "log" will cause an RMON log entry to be made. Selecting "snmp-trap" will cause an SNMP trap to be sent. Finally, selecting "log-and-trap" will cause both a log entry to be made and an SNMP trap to be sent.
   - **d**. Enter an appropriate SNMP community in the Community field if an SNMP trap is to be sent when the event is triggered. This SNMP community must match the community set for the network management station to which the trap is to be sent.
   - **e**. Select the Apply button.

3. To modify an event:
   a. Select the Select button for the event you want to modify.
   b. Select the Modify Event button.
   c. Change the settings as desired.
   d. Select the Apply button.
4. To delete an event:
   a. Select the Select button for the event you want to delete.
   b. Select the Delete Event button.

Create New Alarm

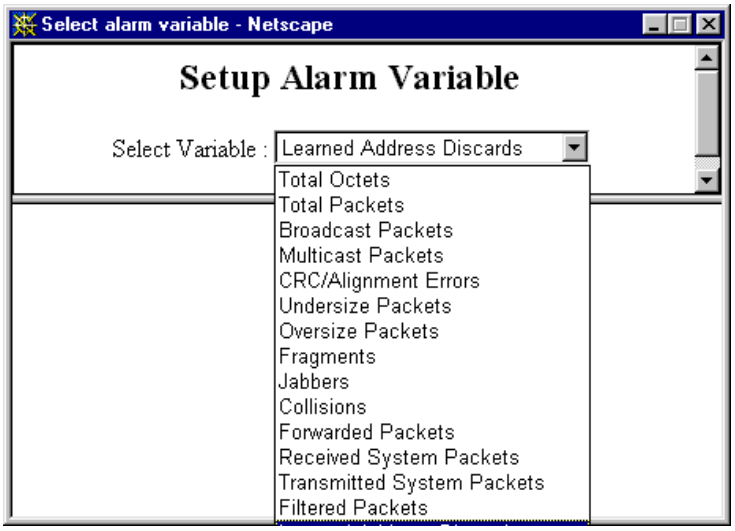
1. Select the Create New Alarm button.

   The Create New Alarm window appears.

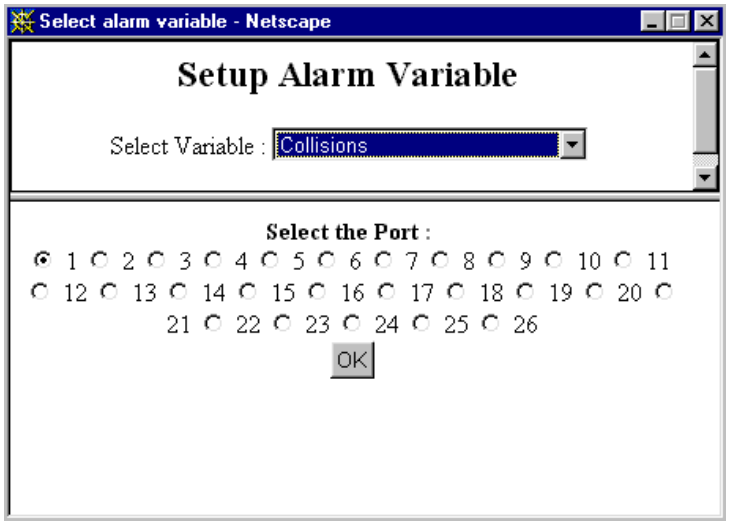


2. Select the "?" button for more detailed definitions of each of the parameters contained in this window.
3. Enter a unique Alarm ID. Valid values are between 1 and 65535. Select an Alarm ID that does not already appear in the table.
4. Select the Select Variable button to select the switch statistic to monitor. The Setup Alarm Variable window appears.

5. Select the drop down menu to display the available variables.



6. Highlight a variable. In this instance, "Collisions" was selected. The following window appears.



7. Select the specific port on which you want to monitor the specific variable selected and select OK.

Note that the selected variable is now represented as an Object Identifier (OID) string in the Alarm Variable field of the Create New Alarm window.

8. Select a value in the Sample Type field. If you select "deltaValue", the alarm monitors the difference between two samples of the statistic. If you select "absoluteValue", the alarm monitors the absolute value of the statistic.

9. Select a value in the Startup Alarm field. If you select "risingAlarm", the alarm will trigger the first time if the first sample is equal to or greater than Rising Threshold. If you select "fallingAlarm", the alarm will trigger the first time if the first sample is equal to or less than Falling Threshold. If you select "risingOrFallingAlarm", the alarm will trigger the first time if either of the first two cases occurs.

10. Enter an Event ID in the Rising Event field. This event will be executed when the statistic sample is equal to or greater than the Rising Threshold. The event should already be configured.

11. Enter an Event ID in the Falling Event field. This event will be executed when the statistic sample is equal to or less than the Falling Threshold. The event should already be configured.

12. Enter a time value in seconds in the Sampling Interval field. This value determines how frequently the alarm will monitor the value of the statistic and determine if a threshold has been reached.

13. Enter a value in the Rising Threshold field. This is the value that the statistic sample is compared with each interval to determine if the alarm threshold has been reached in the rising direction (equal to or greater than). This is either a difference or an absolute value, depending on the Sample type parameter.

14. Enter a value in the Falling Threshold field. This is the value that the statistic sample is compared with each interval to determine if the alarm threshold has been reached in the falling direction (equal to or less than). This is either a difference or an absolute value, depending on the Sample type parameter.

15. Select the Apply button. The newly configured alarm appears in the Alarm Configuration Table.

Modify Alarm

1. Select the Select button for the alarm you want to modify.

2. Select the Modify Alarm button.

3. Modify settings in any of the fields.

4. Select Apply.

Delete Alarm

1. Select the Select button for the alarm you want to delete.

2. Select the Delete button.

View RMON Event Log

The RMON Event Log is a historical table of triggered alarms stored locally on the switch. This table can be viewed whenever desired.

1. Select View RMON Event Log

   The RMON Event Log screen appears.

2. Select the Refresh button to manually refresh the RMON Event Log.

3. Select the Set Refresh Interval button to set the time interval for automatic refresh of the RMON Event Log, and select OK.

   There must be an existing RMON log entry in order to apply the Refresh and Set Refresh Interval settings.

Port Configuration

You can configure 10/100 ports for operational parameters such as auto-negotiation, duplex mode, port speed and flow control. On Gigabit Ethernet ports, flow control and auto-negotiation can be configured, but duplex mode and port speed cannot. The Hirschmann FES/GES family Gigabit Ethernet ports always operate in full duplex mode and at a 1Gbps speed.

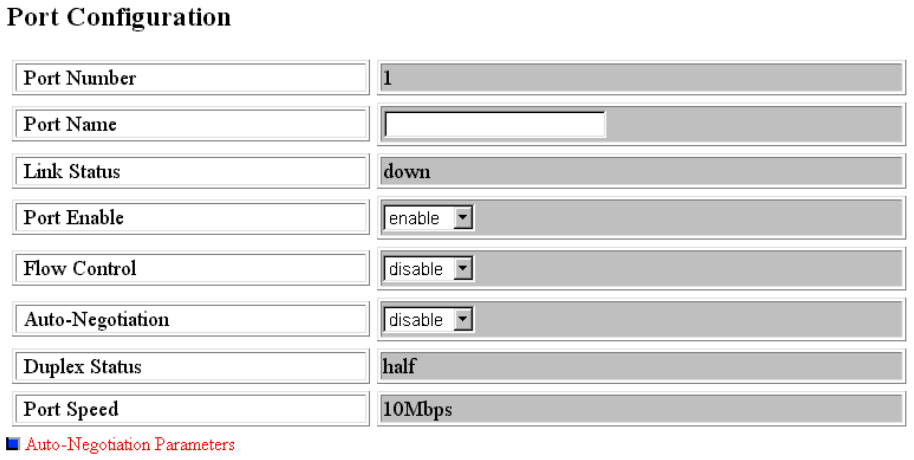
You can select a specific port to configure in one of two ways, either by selecting the port from the Port Table or by selecting the port from the switch graphic in Area 2.

1. To configure a specific port, do one of the following:

   a. Select the Port Configuration link in Area 3 from the home page. Then, select the "Configure" link in the Configure Port column for the specific port to be configured. Make desired changes and select Apply, or

   b. Select the individual port from the switch graphic.

   The Port Configuration screen appears. Port Number 1 is selected in this example.



2. Enter a Port Name.

3. Select either "enable" or "disable" in the Port Enable field.

4. Select either "enable" or "disable" in the Flow Control field.

5. Select either "enable" or "disable" Auto-Negotiation field. Auto-Negotiation must be set to "disable" in order for the Auto-Negotiation Parameters option to appear.

   The following fields are displayed, but cannot be configured in the table: Link status (up or down), Duplex Status (half or full), Port speed (10Mbps, 100Mbps or 1Gbps).

Auto-Negotiation Parameters

When Auto-Negotiation on the Port Configuration screen is set to "enable", the Duplex Status and Port Speed variables cannot be manually configured, and the "Auto-Negotiation Parameters" link does not appear. If you set Auto-Negotiation to "disable", the "Auto-Negotiation Parameters" link appears.

1. From the Port Configuration screen, set Auto-Negotiation to "disable", and then select Apply.

2. Select Auto-Negotiation Parameters.

   The Auto-Negotation Parameters screen appears.

3. Select either "half" or "full" in the Duplex Status field.

4. Select either "10Mbps" or "100Mbps" in the Port Speed field.

5. Select Apply if settings have changed.

Port Statistics

The Port Statistics screen allows you to display statistics for each port on the switch. Statistics are displayed in tabular form. These statistics can be refreshed, and the Refresh interval can be changed.

1. To view port statistics for a specific port, do one of the following:

   a. Select the Port Configuration link from the home page, select the Configure button for the specific port to be viewed (Area 4), and then select the Port Statistics link, or

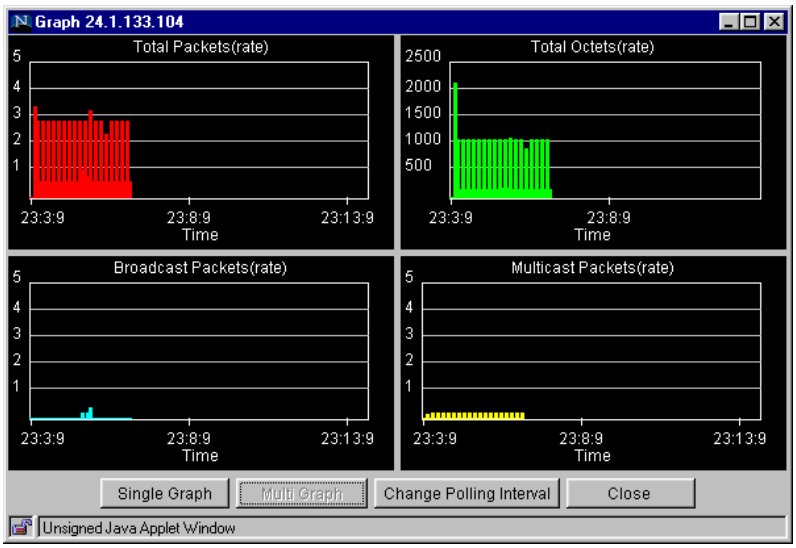
   b. Select the specific port to be viewed (Area 2), and then select the Port Statistics link.

   Any of the statistical parameters presented in the Port Statistics screen can be graphed in real time. Multiple graphs can be opened simultaneously for a comprehensive view of critical parameters.

2. Select a specific port for which to graph statistics.

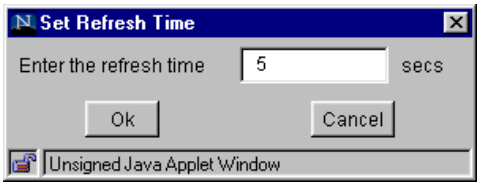
3. Select the statistics(s) to graph by selecting the corresponding "Enable Graphing" checkbox. The following example shows graph results when selecting "Total Packets", "Total Octets", Broadcast Packets", and "Multicast Packets".

4. Select Draw Graph to draw the graph. The following screen shows the results.



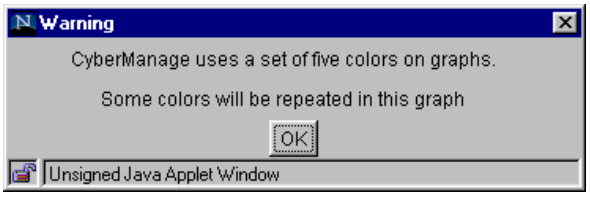
You can use the Single Graph or Multi Graph buttons to change the display. The lapsed time is displayed in the horizontal plane and value of the sample is displayed in the vertical plane.

5. Select the Change Polling Interval button to change the polling interval. The Set Refresh Time window appears.

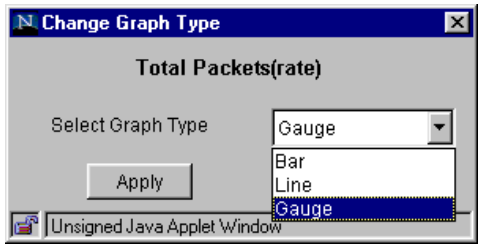


6. Select OK if you change the value, select Cancel to cancel.

If you elect to display more than five parameters in your graph, the following message appears:



7. Any graph can be displayed either as a bar, line or gauge graph. To change graph type, select anywhere in the parameter window and the following configurable window appears:

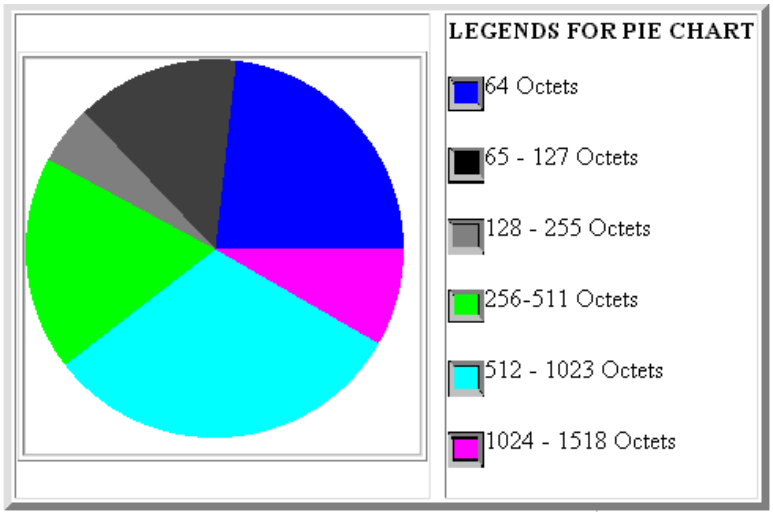


The settings take affect when you select Apply.

8. The Packet Size Distribution selection allows you to view a pie chart representing the distribution of packets by octet length range for an individual port.

a. Select the port you want to view and select Packet Size Distribution from the Port Statistics screen.

The Packet Size Distribution screen appears.



b. Select the Refresh button to manually refresh the Packet Size Distribution statistics.

c. Select the Set Refresh Interval button to set the time interval for automatic refresh of the Packet Size Distribution statistics.

Port History

Port History allows you to view historical port statistics information. Samples of port statistics data are collected by the switch at specific intervals. Two sets of data are collected, each at a different, configurable sampling rate. By default, one table shows statistics for each port taken at an interval of every 30 seconds, while the other table default interval is every 30 minutes.

1. Select Port History from the Port Configuration Menu

A listing of the two history tables appears.

2. Select View History Table 1 or 2.

3. Enter a new sampling interval if you wish to change the current setting, then select Apply. Entering a new sampling interval will clear all the data in the current table.

4. Select View Statistics to view the port statistics in a table format.

5. Select Graph Parameters

The Setup Graphing History Table appears.

6. Make a selection from the Select the Variable to Graph drop-down menu and select OK.

The History Graph for the selected parameter appears. A History Graph does not appear if values for this parameter are currently all zeroes.

Event Log

The Event Log option allows you to view, in real time, events occurring with the switch. The events are reported to the HiWay Webbased Network Management application through SNMP traps sent from the switch. The HiWay Webbased Network Management application must be configured to receive these traps as described in Setting up Web Management in Section 2. Once configured, the Event Log will display these events as they are received from the switch.

1. Select Event Log from the Main menu.

When you start the Event Log, the Current Events screen displays, showing a list of the most recent events on the switch. Table 3-2 defines the Event Log fields.

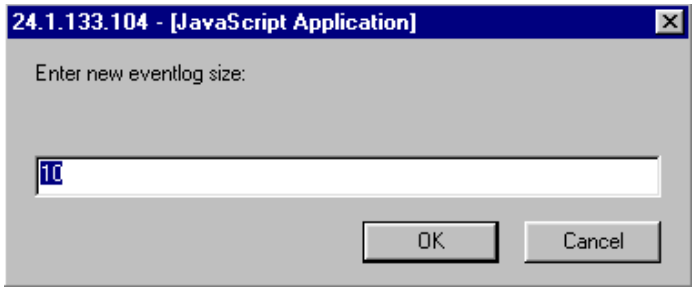
Table 3-2. Event Log Fields

Parameter	Event Description
Generic Type	Cold start: system powers up
	Link down: link goes down
	Link up: link goes up
	Authentication failure: attempted SNMP security breach (community name mismatch)
	Enterprise specific: prompts Specific Type field to display the specific trap type.
Specific Type	Traps defined by other MIBs and individual vendors.
Up Time (minutes)	The number of minutes the switch has been operational since the last power cycle or reset.
Description	Brief description of the event.

2. Select the Open History Eventlog button to display a list of all the events that have occurred since the Event Log was first opened.

   The History Event Log appears.

3. Select the Set Current Eventlog Size button to enter the number of events that can displayed at once on the Current Events screen. The following window appears:



4. Enter the new eventlog size and select OK.
5. The Reset Current Eventlog button clears the events from the Current Events Log.

APPENDIX A. TROUBLESHOOTING

This appendix describes problems potentially encountered when using the HiWay Webbased Network Management application and presents suggested solutions for correcting these problems.

Troubleshooting

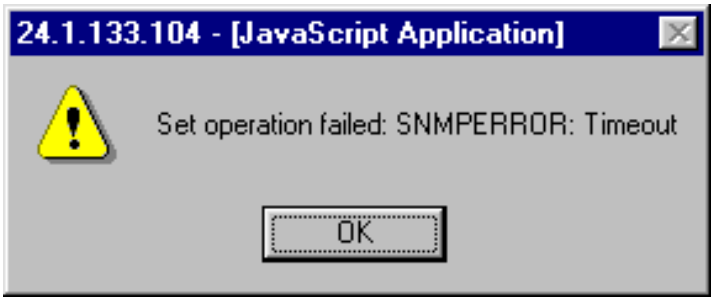
Cannot Connect to the Switch

If you attempt to connect to the switch and the main window does not appear, make sure that the correct IP address is entered in the URL field of the browser.

- Check the network connections of both your workstation and the switch.
- Try to Ping the IP address to see if it's indeed reachable.
- Set the IP gateway if necessary.
- Make sure the correct community names are entered.
- Make sure the Web Management Enable parameter is set to "Yes".

System is Disconnected from the Switch

If your workstation is disconnected from the switch during an active session, you may see the following messages:



or, "Device is not responding to SNMP queries".

- Reconnect the workstation to the switch. You may need to re-enter your latest changes, but the user interface should become available again for use.
- If the user interface does not become available after reconnecting, close the HiWay Webbased Network Management application window and start a new session.

Cannot Change Switch Settings

The "Set operation failed" popup window may also display if you attempt to change a setting on the switch, but have only entered an SNMP GET community, not a SET community (i.e., you are in read-only mode). Make sure you are in the read-write mode by entering a SET community using the Change Community Strings option.

Frequently Asked Questions

Can I Open More Than One Window for Same Switch?

Yes. You can start multiple browser sessions with the switch at once.

Will Network Congestion Prevent Use of Network Manager?

It could. If there is significant network delay after a configuration command is issued, the system could time out. In addition, excessive delays when gathering switch statistics could interfere with the accuracy of performance statistics.

How Do I Confirm a Successful Software Download?

After the download is complete, go to the System Information screen to verify that the software version running on the switch is the same as the software just upgraded. If the version has not been upgraded, retry the procedure.

INDEX

R

S

T

U

V

W