

# *NetAtlas Enterprise*

*Ethernet Switch Manager*

## ***User's Guide***

Version 1.01  
9/2005

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is lowercase and the "XEL" is uppercase.

# Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## **Disclaimer**

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## **Trademarks**

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Certifications

Go to [www.zyxel.com](http://www.zyxel.com)

- 1 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 2 Select the certification you wish to view from this page.

# Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

# ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

## Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

# Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
	SALES E-MAIL	FAX	FTP SITE	
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 8702 909090	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 8702 909091 0906 7370001(UK only)	ftp.zyxel.co.uk	

a. "+" is the (prefix) number you enter to make an international telephone call.

# Table of Contents

<b>Copyright .....</b>	<b>2</b>
<b>Federal Communications Commission (FCC) Interference Statement .....</b>	<b>3</b>
<b>Safety Warnings .....</b>	<b>4</b>
<b>ZyXEL Limited Warranty .....</b>	<b>5</b>
<b>Customer Support.....</b>	<b>6</b>
<b>Table of Contents .....</b>	<b>8</b>
<b>List of Figures .....</b>	<b>14</b>
<b>List of Tables .....</b>	<b>18</b>
<b>Preface .....</b>	<b>22</b>
<b>Chapter 1</b>	
<b>Introduction .....</b>	<b>24</b>
1.1 EMS Overview .....	24
1.1.1 SNMPc Network Manager .....	24
1.2 System Requirements .....	24
1.2.1 Device Firmware Versions Supported .....	25
1.3 EMS Installation .....	25
1.4 Accessing NetAtlas .....	25
<b>Chapter 2</b>	
<b>Switch Manager.....</b>	<b>28</b>
2.1 Switch Manager Overview .....	28
2.2 Access Log .....	29
2.3 Database Management .....	30
2.3.1 Filename Convention .....	30
2.3.2 Database Backup and Restore .....	30
2.3.3 Database Log Storage Configuration .....	31
2.3.4 Database Scheduled Backup Configuration .....	32
2.4 Accessing the EMS Main Screen .....	33
<b>Chapter 3</b>	
<b>EMS Main Window.....</b>	<b>36</b>
3.1 Introducing the EMS Main Window .....	36



3.2 Device Icon Colors .....	37
3.3 System Message Panel Alarm Status .....	37
3.4 System Message Panel Port Status .....	38
3.5 Menu Shortcut Buttons .....	38
3.6 EMS Main Menu Summary .....	39
3.7 Common EMS Command Buttons .....	41
3.8 View the Switch .....	41
3.9 Switch Information .....	41
3.10 Configuration Save .....	42
<b>Chapter 4</b>	
<b>Map .....</b>	<b>44</b>
4.1 Submap and Device Mapping .....	44
4.1.1 Adding a Submap or Device .....	44
4.1.2 Edit a Node .....	45
4.1.3 Find an Object .....	46
4.1.4 Delete a Submap .....	46
4.1.5 Delete a Device .....	47
4.2 Exit .....	47
<b>Chapter 5</b>	
<b>View .....</b>	<b>48</b>
5.1 Hardware Status .....	48
5.2 Spanning Tree Protocol (STP) .....	50
5.2.1 STP Terminology .....	50
5.2.2 How STP Works .....	50
5.2.3 STP Port States .....	51
5.2.4 STP Status .....	51
5.3 VLAN Status .....	52
5.4 Port Status .....	53
5.5 802.1D .....	55
5.5.1 802.1D: MAC Table .....	55
5.5.2 View the MAC Table .....	55
5.5.3 802.1D: ARP Table .....	57
5.5.4 How ARP Works .....	57
5.5.5 View the ARP Table .....	57
5.6 Multicast Status .....	58
<b>Chapter 6</b>	
<b>Template .....</b>	<b>60</b>
6.1 Template Overview .....	60
6.2 VLAN Template .....	60
6.3 IGMP Filter Template .....	61

6.3.1 IP Multicast Addresses .....	62
6.3.2 Configuring an IGMP Filter Template .....	62
6.3.3 New IGMP Filter Template Screen .....	63
6.4 Static Multicast Group Template .....	64
6.4.1 Multicast MAC Address .....	65
6.4.2 Static Multicast Group Template Screen .....	65
6.4.3 New Multicast Template Screen .....	67
<b>Chapter 7</b>	
<b>Provisioning .....</b>	<b>70</b>
7.1 Provisioning Overview .....	70
7.2 Applying an IGMP Filter Profile .....	70
7.3 Removing an IGMP Filter Profile .....	72
<b>Chapter 8</b>	
<b>Performance .....</b>	<b>74</b>
8.1 Interface Performance .....	74
8.2 Table Menu Bar Icons .....	75
8.2.1 Editing a Table Entry .....	76
8.2.2 Expand Dialog Box .....	77
8.3 Graph Menu Bar Icons .....	78
8.3.1 Graph Styles .....	79
8.3.2 Chart Format Display Variable .....	79
8.3.3 Graph Labels .....	80
<b>Chapter 9</b>	
<b>Fault.....</b>	<b>82</b>
9.1 Event Log .....	82
9.2 Loopback Test .....	83
<b>Chapter 10</b>	
<b>Maintenance .....</b>	<b>86</b>
10.1 Firmware Upgrade .....	86
10.1.1 Procedure to Update Firmware .....	86
10.2 Device Reset .....	87
10.3 Network Element Configuration Backup and Restore .....	88
10.4 Load Factory Default .....	89
10.5 Scheduled Network Element Configuration Backup .....	90
10.5.1 Scheduled Network Element Configuration Backup Add .....	91
10.5.2 Scheduled Network Element Configuration Backup Remove .....	92

<b>Chapter 11</b>	
<b>Tools</b> .....	<b>94</b>
11.1 Accessing the Switch .....	94
11.1.1 Telnet .....	94
11.1.2 Web Access .....	95
11.2 Ping .....	95
<b>Chapter 12</b>	
<b>Device Menu Overview</b> .....	<b>98</b>
12.1 Device Menu Summary .....	98
12.2 Property Configuration .....	98
12.3 Introducing the Device Configuration Window .....	98
12.3.1 Port List Multiple Port Configuration .....	99
12.3.2 The Copy to.. Button .....	100
<b>Chapter 13</b>	
<b>System Configuration</b> .....	<b>104</b>
13.1 System Info .....	104
13.2 SNMP .....	104
13.2.1 Configuring SNMP .....	105
13.3 Remote Management .....	106
13.4 Time Setup .....	108
<b>Chapter 14</b>	
<b>Switch Configuration</b> .....	<b>110</b>
14.1 Switch Setup .....	110
14.2 Priority Queue .....	113
14.3 STP Configuration .....	114
14.4 Link Aggregation .....	115
14.4.1 Dynamic Link Aggregation .....	116
14.4.2 Link Aggregation ID .....	116
14.4.3 Configuring Link Aggregation .....	117
14.4.4 DHCP Relay .....	117
14.4.5 DHCP Relay Agent Information .....	118
14.5 GARP Timer .....	119
14.6 RADIUS .....	120
14.6.1 Introduction to Authentication .....	120
14.6.2 Configuring RADIUS .....	120
14.7 Filtering .....	121
14.7.1 Creating a New Filter .....	122
14.8 MAC Forwarding .....	123
14.8.1 Configuring Static MAC Forwarding .....	123
14.9 Mirroring .....	125

14.10 DSCP .....	126
<b>Chapter 15</b>	
<b>VLAN .....</b>	<b>128</b>
15.1 Introduction to VLANs .....	128
15.2 Configuring 802.1Q VLAN .....	128
15.2.1 Modify an 802.1Q VLAN .....	130
15.2.2 Removing a VLAN .....	131
15.3 Introduction to Port-based VLANs .....	132
15.3.1 Configuring Port Based VLAN .....	132
<b>Chapter 16</b>	
<b>Ethernet Port Configuration .....</b>	<b>134</b>
16.1 Overview .....	134
16.2 Port Setup .....	134
16.3 Port VLAN .....	137
16.3.1 Configuring Port VLAN .....	137
16.4 Port Link Aggregation .....	138
16.5 Port STP .....	138
16.6 Bandwidth Control .....	139
16.7 Broadcast Storm Control .....	141
16.8 DiffServ .....	142
16.9 Port 802.1x .....	143
16.10 Port Security .....	144
16.10.1 Configuring Port Security .....	144
16.11 Port Mirroring .....	145
16.12 VLAN Stacking .....	146
16.13 Queue Method .....	147
<b>Chapter 17</b>	
<b>Routing Configuration .....</b>	<b>150</b>
17.1 Static Route .....	150
17.1.1 Configuring Static Routing .....	150
17.1.2 Add or Modify a Static Route .....	151
<b>Chapter 18</b>	
<b>Multicast Configuration .....</b>	<b>154</b>
18.1 Overview .....	154
18.1.1 IGMP Snooping .....	154
18.2 Multicast Setting .....	154
18.2.1 Changing the Port Multicast Settings .....	156
18.2.2 Applying a Multicast Template .....	156
18.2.3 Displaying IGMP Filter Profile .....	157

18.3 MVR .....	158
18.3.1 Types of MVR Ports .....	159
18.3.2 MVR Modes .....	159
18.3.3 Viewing MVR Settings .....	159
18.3.4 Creating a New Multicast VLAN .....	161
18.3.5 Creating a New MVR Group .....	162
<b>Chapter 19</b>	
<b>Troubleshooting .....</b>	<b>166</b>
19.1 Installation Problems .....	166
19.2 Problems Accessing the EMS .....	166
19.3 Uninstalling the EMS .....	166
19.4 Problems Finding a Device .....	167
<b>Appendix A</b>	
<b>SNMPc Network Manager .....</b>	<b>168</b>
Starting the SNMPc Network Manager .....	168
Manual Startup.....	168
Automatic Startup .....	168
SNMPc Main Window .....	169
Selection Tool .....	170
Event Log Tool.....	170
View Window Area.....	171
Main and Edit Button Bar Icons .....	171
<b>Appendix B</b>	
<b>Alarm Types and Causes .....</b>	<b>174</b>
<b>Index.....</b>	<b>176</b>

# List of Figures

Figure 1 SNMPc: Switch Device List Icon .....	25
Figure 2 NetAtlas Main Screen .....	26
Figure 3 EMS: Main Screen .....	26
Figure 4 Switch Manager .....	28
Figure 5 Switch Manager: Admin: Access Log .....	29
Figure 6 Switch Manager: Admin: Database Management: Backup/Restore .....	31
Figure 7 Switch Manager: Admin: Database Management: Log Storage .....	31
Figure 8 Switch Manager: Admin: Database Management: Scheduled Backup .....	32
Figure 9 EMS: Main Screen .....	34
Figure 10 EMS Main Screen Overview .....	36
Figure 11 EMS Main Screen Shortcut Bar .....	38
Figure 12 Switch View .....	41
Figure 13 Configuration: System Configuration: System Info .....	42
Figure 14 Configuration Save .....	43
Figure 15 Configuration Save: Result .....	43
Figure 16 Submaps and Device Mapping .....	44
Figure 17 Map: Add Submap/Device .....	45
Figure 18 Map: Edit Node .....	46
Figure 19 Map: Find Object .....	46
Figure 20 Map: Delete Warning .....	46
Figure 21 View: Hardware Status .....	48
Figure 22 View: STP Status .....	51
Figure 23 View: VLAN Status .....	53
Figure 24 View: Port Status .....	54
Figure 25 MAC Table Flowchart .....	55
Figure 26 View: 802.1d: MAC Table .....	56
Figure 27 View: 802.1d: ARP Table .....	58
Figure 28 View: Multicast Status .....	59
Figure 29 Template: VLAN .....	60
Figure 30 Template: IGMP Filter .....	62
Figure 31 Template: New IGMP Filter .....	63
Figure 32 Multicast MAC-IP Address Mapping Example .....	65
Figure 33 Template: Multicast .....	66
Figure 34 Template: New Multicast .....	67
Figure 35 Provisioning: IGMP Filter .....	71
Figure 36 Provisioning: IGMP Filter: Apply to Devices .....	71
Figure 37 Provisioning: IGMP Filter: Apply to Devices: Successful .....	72
Figure 38 Provisioning: IGMP Filter: Remove From Devices .....	72

Figure 39 Provisioning: IGMP Filter: Remove From Devices: Select Device .....	73
Figure 40 Provisioning: IGMP Filter: Remove From Devices: Successful .....	73
Figure 41 Performance: Interface .....	74
Figure 42 Table Menu Bar Icons .....	75
Figure 43 Edit Table Entry .....	76
Figure 44 Expand Field .....	78
Figure 45 Graph Menu Bar .....	79
Figure 46 Cell Properties Select .....	80
Figure 47 Chart Color Codes and Line Styles .....	80
Figure 48 Graph Variables .....	81
Figure 49 Fault: Event Log .....	82
Figure 50 Fault: Loopback Test .....	84
Figure 51 fault: Loopback: Result .....	84
Figure 52 Maintenance: Firmware Upgrade .....	87
Figure 53 Maintenance: Firmware Upgrade: Result .....	87
Figure 54 Maintenance: Device Reset .....	88
Figure 55 Maintenance: Device Reset: Result .....	88
Figure 56 Maintenance: Configuration Backup/Restore .....	89
Figure 57 Maintenance: Load Factory Defaults .....	90
Figure 58 Maintenance: Scheduled NE Config Backup .....	90
Figure 59 Maintenance: Scheduled NE Config Backup Add .....	92
Figure 60 Telnet .....	94
Figure 61 Web Access .....	95
Figure 62 Ping .....	96
Figure 63 Device Panel List Menus .....	98
Figure 64 Configuration Window .....	99
Figure 65 Configuration Window: Port List: Multiple Port Select .....	100
Figure 66 Applied Results .....	100
Figure 67 Copy Port Setup: Example .....	101
Figure 68 Copy Successful .....	102
Figure 69 SNMP Management Model .....	104
Figure 70 System Configuration: SNMP Conf. ....	106
Figure 71 System Configuration: Remote Management .....	107
Figure 72 System Configuration: Time Setup .....	108
Figure 73 Switch Configuration: Switch Setup (ES-2024A) .....	110
Figure 74 Switch Configuration: Switch Setup (GS-2024) .....	111
Figure 75 Switch Configuration: Switch Setup (ES-3124/ES-3124PWR) .....	111
Figure 76 Switch Configuration: Priority Queue .....	113
Figure 77 Switch Configuration: STP Conf. ....	115
Figure 78 Switch Configuration: Link Aggregation .....	117
Figure 79 Switch Configuration: DHCP Relay .....	118
Figure 80 Switch Configuration: GARP Timer .....	120
Figure 81 Switch Configuration: RADIUS .....	121

Figure 82 Switch Configuration: Filtering .....	122
Figure 83 Switch Configuration: Filtering: Add .....	122
Figure 84 Switch Configuration: MAC Forwarding .....	124
Figure 85 Switch Configuration: MAC Forwarding: Add .....	124
Figure 86 Switch Configuration: Mirroring (ES-2024) .....	125
Figure 87 Switch Configuration: Mirroring (GS-2024) .....	126
Figure 88 Switch Configuration: Mirroring (ES-3124/ES-3124PWR) .....	126
Figure 89 DiffServ: Differentiated Service Field .....	127
Figure 90 Switch Configuration: DSCP .....	127
Figure 91 Selecting a VLAN Type .....	129
Figure 92 VLAN Configuration: 802.1Q .....	129
Figure 93 VLAN Configuration: 802.1Q: Modify .....	130
Figure 94 VLAN Configuration: Port Based .....	132
Figure 95 Ethernet Port Configuration: Port Setup (ES-2024A) .....	134
Figure 96 Ethernet Port Configuration: Port Setup (GS-2024) .....	135
Figure 97 Ethernet Port Configuration: Port Setup (ES-3124/ES-3124PWR) .....	135
Figure 98 Ethernet Port Configuration: Port VLAN .....	137
Figure 99 Ethernet Port Configuration: Port Link Aggregation .....	138
Figure 100 Ethernet Port Configuration: Port STP .....	139
Figure 101 Ethernet Port Configuration: Bandwidth Ctrl. ....	140
Figure 102 Ethernet Port Configuration: Bandwidth Ctrl. (GS-2024) .....	140
Figure 103 Ethernet Port Configuration: Broadcast Storm Ctrl. (ES-2024A) .....	141
Figure 104 Ethernet Port Configuration: Broadcast Storm Ctrl. (GS-2024) .....	141
Figure 105 Ethernet Port Configuration: Broadcast Storm Ctrl. (ES-3124/ES-3124PWR) .....	141
Figure 106 Ethernet Port Configuration: DiffServ .....	143
Figure 107 Ethernet Port Configuration: Port 802.1x .....	143
Figure 108 Ethernet Port Configuration: Port Security .....	144
Figure 109 Ethernet Port Configuration: Port Security (GS-2024) .....	144
Figure 110 Ethernet Port Configuration: Port Mirroring .....	146
Figure 111 Ethernet Port Configuration: VLAN Stacking .....	147
Figure 112 Ethernet Port Configuration: Queue Method .....	148
Figure 113 Routing Configuration: Static Route .....	150
Figure 114 Routing Configuration: Static Route: Add or Modify .....	151
Figure 115 Multicast Configuration: Multicast Setting .....	155
Figure 116 Multicast Configuration: Multicast Setting: Modify .....	156
Figure 117 Multicast Configuration: Multicast Setting: Load Template .....	157
Figure 118 Multicast Configuration: Multicast Setting: View Profile .....	158
Figure 119 Multicast Configuration: MVR .....	160
Figure 120 Multicast Configuration: MVR: Add MVLAN .....	161
Figure 121 Multicast Configuration: MVR: Add MVLAN: Result .....	162
Figure 122 Multicast Configuration: MVR: Select MVLAN .....	162
Figure 123 Multicast Configuration: MVR: Add .....	163
Figure 124 Configuration: Multicast Configuration: MVR: Add MVR Group: Result .....	163



Figure 125 EMS: Remove .....	167
Figure 126 Automatic Startup .....	168
Figure 127 SNMPc Main Windows .....	169
Figure 128 SNMPc Main Button Bar Icons .....	171
Figure 129 SNMPc Edit Button Bar Icons .....	172

# List of Tables

Table 1 System Requirements .....	24
Table 2 Device Firmware Versions Supported .....	25
Table 3 Switch Manager Menus Overview .....	28
Table 4 Switch Manager: Admin: Access Log .....	29
Table 5 Switch Manager: Admin: Database Management: Backup/Restore .....	31
Table 6 Switch Manager: Admin: Database Management: Log Storage .....	32
Table 7 Switch Manager: Admin: Database Management: Scheduled Backup .....	33
Table 8 EMS Main Screen Overview .....	37
Table 9 Device Icon Colors .....	37
Table 10 System Message Panel Alarm Status .....	37
Table 11 EMS Menu Summary .....	39
Table 12 EMS Navigation Panel Sub-link Descriptions .....	39
Table 13 Common EMS Command Buttons .....	41
Table 14 Configuration: Switch System Configuration .....	42
Table 15 Map: Add Submap/Device .....	45
Table 16 Status: Hardware Status .....	49
Table 17 STP Path Costs .....	50
Table 18 STP Port States .....	51
Table 19 View: STP Status .....	52
Table 20 View: VLAN Status .....	53
Table 21 View: Port Status .....	54
Table 22 View: 802.1d: MAC Table .....	56
Table 23 View: 802.1d: ARP Table .....	58
Table 24 View: Multicast Status .....	59
Table 25 Template: VLAN .....	61
Table 26 Template: IGMP Filter .....	62
Table 27 Template: New IGMP Filter .....	64
Table 28 Template: Multicast .....	66
Table 29 Template: New Multicast .....	67
Table 30 Performance: Interface .....	74
Table 31 Edit Table Entry .....	76
Table 32 Variable Types .....	78
Table 33 Edit Table Entry .....	79
Table 34 Edit Style Dialog Box .....	80
Table 35 Graph Variables .....	81
Table 36 Fault: Event Log .....	82
Table 37 Maintenance: Configuration Backup/Restore .....	89
Table 38 Maintenance: Scheduled NE Config Backup .....	91

Table 39 Configuration Window .....	99
Table 40 Copy Port Setup .....	101
Table 41 SNMP Commands .....	105
Table 42 System Configuration: SNMP Conf. ....	106
Table 43 System Configuration: Remote Management .....	107
Table 44 System Configuration: Time Setup .....	108
Table 45 Switch Configuration: Switch Setup .....	112
Table 46 Switch Configuration: Priority Queue .....	114
Table 47 Switch Configuration: STP Conf. ....	115
Table 48 Aggregation ID Local Switch .....	116
Table 49 Aggregation ID Peer Switch .....	116
Table 50 Switch Configuration: Link Aggregation .....	117
Table 51 Switch Configuration: DHCP Relay .....	119
Table 52 Switch Configuration: GARP Timer .....	120
Table 53 Switch Configuration: RADIUS .....	121
Table 54 Switch Configuration: Filtering .....	122
Table 55 Switch Configuration: Filtering: Add .....	123
Table 56 Switch Configuration: MAC Forwarding .....	124
Table 57 Switch Configuration: MAC Forwarding: Add .....	125
Table 58 Switch Configuration: Mirroring .....	126
Table 59 Switch Configuration: DSCP .....	127
Table 60 VLAN Configuration: 802.1Q .....	129
Table 61 VLAN Configuration: 802.1Q: Modify .....	131
Table 62 VLAN Port Type Descriptions .....	131
Table 63 VLAN Configuration: Port Based .....	133
Table 64 Ethernet Port Configuration: Port Setup .....	135
Table 65 Ethernet Port Configuration: Port VLAN .....	137
Table 66 Ethernet Port Configuring: Port Link Aggregation .....	138
Table 67 Ethernet Port Configuration: Port STP .....	139
Table 68 Ethernet Port Configuration: Bandwidth Ctrl. ....	140
Table 69 Ethernet Port Configuration: Broadcast Storm Ctrl. ....	142
Table 70 Ethernet Port Configuration: Port 802.1x .....	143
Table 71 Ethernet Port Configuration: Port Security .....	145
Table 72 Ethernet Port Configuration: Port Mirroring .....	146
Table 73 Ethernet Port Configuration: VLAN Stacking .....	147
Table 74 Ethernet Port Configuration: Queue Method .....	148
Table 75 Routing Configuration: Static Route .....	151
Table 76 Routing Configuration: Static Route: Add or Modify .....	151
Table 77 Multicast Configuration: Multicast Setting .....	155
Table 78 Multicast Configuration: Multicast Setting: Modify .....	156
Table 79 Multicast Configuration: Multicast Setting: Load Template .....	157
Table 80 Multicast Configuration: Multicast Setting: View Profile .....	158
Table 81 Multicast Configuration: MVR .....	160

Table 82 General Installation Problems .....	166
Table 83 Problems Accessing the EMS .....	166
Table 84 Problems Accessing the EMS .....	167
Table 85 SNMPc Main Window .....	169
Table 86 Selection Tool .....	170
Table 87 Alarm Types and Causes .....	174



# Preface

Congratulations on your purchase of the NetAtlas Enterprise Ethernet Switch Manager for the ES-3124 series, ES-2024A, and GS-2024. The Ethernet Switch Manager is an Element Management System (EMS) that retrieves management information from switches using SNMP.

**Note:** Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

## About This User's Guide

This manual is designed to guide you through the configuration of your EMS for its applications.

## Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choice.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The NetAtlas Enterprise Ethernet Switch Manager may be referred to as “the EMS” in this User’s guide.
- The switches being managed by the EMS may be referred to as “the switch” in this User’s Guide.

## Related Documentation

- Supporting Disk  
Refer to the included CD for support documents.
- Switch User’s Guide  
Refer to your switch User’s Guide for directions on installation, connections, maintenance, hardware troubleshooting and safety warnings.
- ZyXEL Glossary and Web Site  
Please refer to [www.zyxel.com](http://www.zyxel.com) for an online glossary of networking terms and additional support documentation.

## **User Guide Feedback**

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

# CHAPTER 1

## Introduction

This chapter introduces and shows you how to access the EMS (Element Management System).

### 1.1 EMS Overview

The Element Management System (EMS) retrieves management information from switches using the SNMP protocol.

An EMS is composed of Network Elements (NE) that represent resources in a Network Management System (NMS). The network elements can represent a physical piece of equipment on the network, the components of a device on the network, or parts of the network itself. The EMS is designed to manage the ES-3124 series, ES-2024A and GS-2024 switches in the NMS. The ES-3124 series covers the ES-3124 and the ES-3124PWR.

EMS screens vary depending on your switch models. Screens for the ES-2024A will be shown unless otherwise specified.

#### 1.1.1 SNMPc Network Manager

SNMPc is network management software produced by Castle Rock.

You must have SNMPc properly installed before you can use the EMS; please refer to the appendices in this User's Guide; go to the Castle Rock web site at [www.castlerock.com](http://www.castlerock.com) or see your SNMPc user's guide.

### 1.2 System Requirements

These are the system requirements for the Windows version of the EMS.

**Table 1** System Requirements

HARDWARE	SOFTWARE
CPU: Intel Pentium 4, 1.6 GHz or above	Operating System using NTFS file system: Windows 2000 (with service pack 1), Windows XP or Windows Server 2003.
Memory (RAM): 1 GB or more	Database Program: PostgreSQL 8.0 or later versions.
Hard Disk free space: 20 GB or more	Castle Rock's SNMPc 6.09 (Enterprise or Workgroup edition)



**Table 1** System Requirements (continued)

HARDWARE	SOFTWARE
Screen Resolution: 1024x768 pixels	
Ethernet Adaptor: 10/100 Mbps	

## 1.2.1 Device Firmware Versions Supported<sup>1</sup>

The EMS supports the devices and device firmware versions as listed in the following table.

**Table 2** Device Firmware Versions Supported

DEVICE MODEL	FIRMWARE VERSION
ES-3124	360TP1C0 or later versions
ES-3124PWR	360TY1C0 or later versions
ES-2024A	360TX1C0 or later versions
GS-2024	360LT0C0 or later versions

## 1.3 EMS Installation

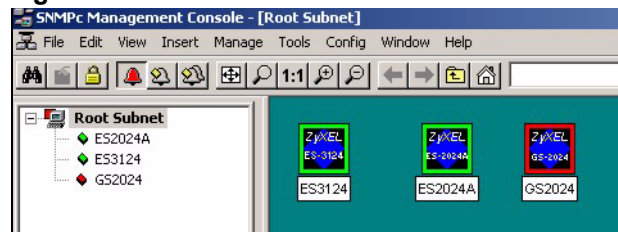
Refer to the Quick Start Guide for the EMS installation procedure.

## 1.4 Accessing NetAtlas

Follow the steps below to access NetAtlas.

- 1 In the SNMPc main screen, double-click the switch icon.

**Figure 1** SNMPc: Switch Device List Icon

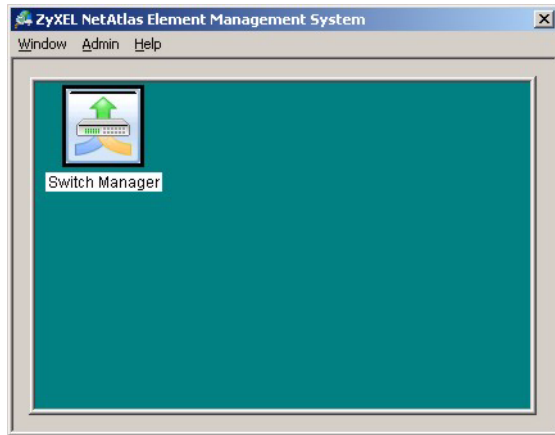


- 2 Click the **Switch Manager** icon to display the main EMS screen.

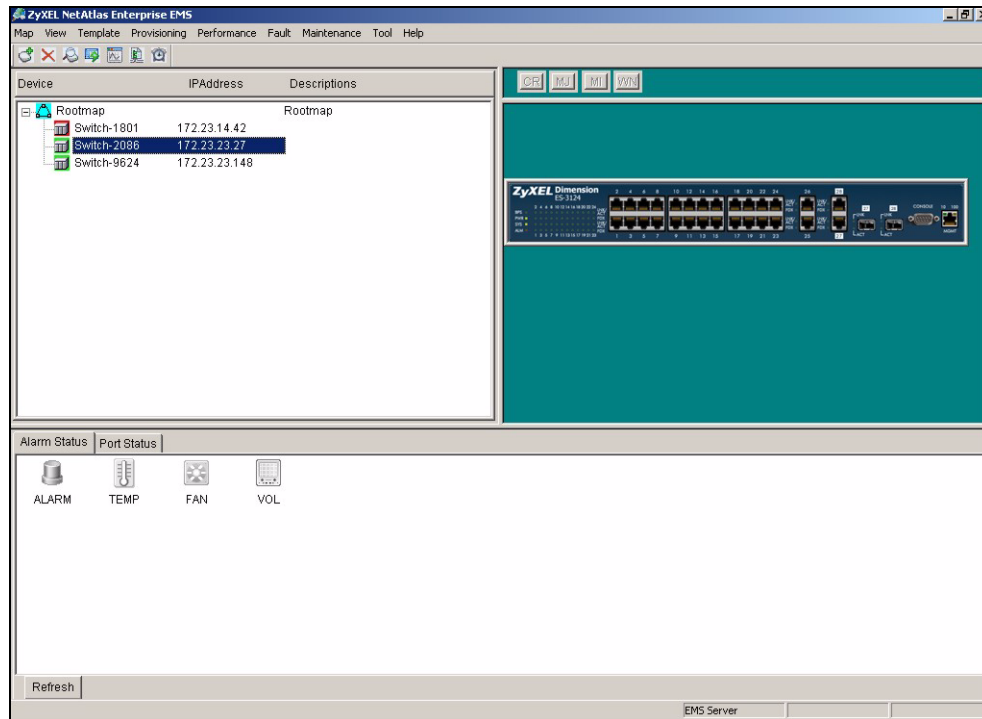
---

1. The list of devices and device firmware versions supported is accurate at the time of writing.

**Figure 2** NetAtlas Main Screen



**Figure 3** EMS: Main Screen





# CHAPTER 2

## Switch Manager

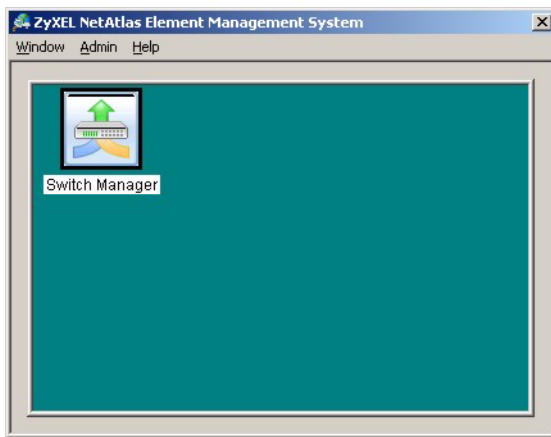
This chapter describes the Switch Manager screens.

### 2.1 Switch Manager Overview

Use the Switch Manager screens to view EMS and device logs and database management.

In SNMPc, double-click on a device icon to display the main Switch Manager screen as shown.

**Figure 4** Switch Manager



The following table describes the options in the switch manager screen.

**Table 3** Switch Manager Menus Overview

LABEL	MENU	SUB-MENU	DESCRIPTION
Window	Exit		Click <b>Exit</b> to close the switch manager screen.
Admin	Access Log		Use this screen to display logs.
	Database Management	Backup and Restore (EMS DB)	Use this screen to backup or restore a switch's configuration.
		Log Storage Configuration	Use this screen to enable logging and specify how many logs to store in the database.

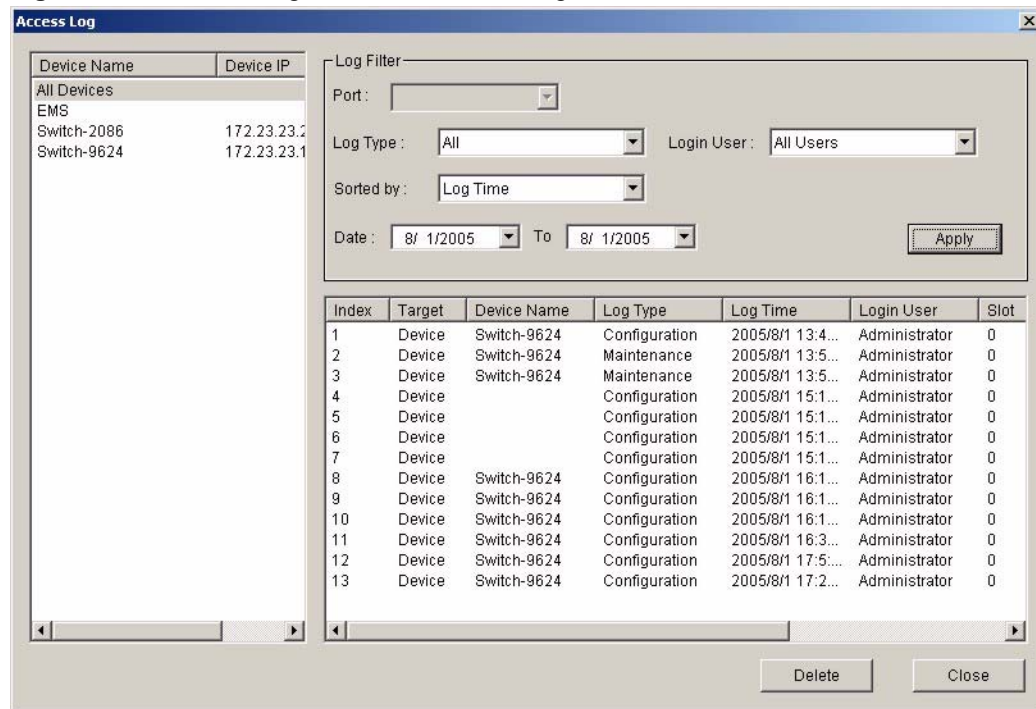
**Table 3** Switch Manager Menus Overview (continued)

LABEL	MENU	SUB-MENU	DESCRIPTION
		Scheduled Backup Configuration (EMS DB)	Use this screen to specify when to store logs in the database.
Help	On-line Help		Select <b>On-line Help</b> to display an EMS help file.

## 2.2 Access Log

To view access logs, click **Admin** and then **Access Log** in the **Switch Manager** screen.

**Figure 5** Switch Manager: Admin: Access Log



The following table describes the fields in this screen.

**Table 4** Switch Manager: Admin: Access Log

LABEL	DESCRIPTION
Log Filter	
Port	Select a port or <b>All Ports</b> for which you want to view switch login data via the EMS.
Log Type	Select the type of logs which you want to view for the selected switch and port(s).
Login User	Select <b>All Users</b> to view logs for all access attempts to a switch via the EMS. Select <b>Administrator</b> to view only the EMS administrator access attempts.

**Table 4** Switch Manager: Admin: Access Log (continued)

LABEL	DESCRIPTION
Sorted by	Select <b>By Device Name</b> to sort the logs displayed in alphabetical order according to the names of the switch(es). Select <b>Log Time</b> to sort the logs displayed according to the times received on the switch(es).
Date	Select a start date and end date from the list boxes to display logs for that period.
Apply	Click <b>Apply</b> to display logs with the criteria set above.
Index	This field displays the log number.
Target	This field displays a reason for the generated log.
Device Name	This field displays name of the switch that generated the log(s).
Log Type	This field displays the type of log the switch generated.
Log Time	This field displays the time a log was generated by a switch.
Login User	This field displays the EMS user that logged into the switch
Slot	This field is currently not supported.
Port	This field displays the selected switch port number on which the log was generated.
Description	This field displays further information about the log.
Delete	Click <b>Delete</b> to delete a selected log from the list of log entries.
Close	Click <b>Close</b> to close this screen.

## 2.3 Database Management

The EMS-related event and access logs information and various configuration settings are stored in the database. The database management features enable you to back up all logs and configurations and restore selected backed up files.

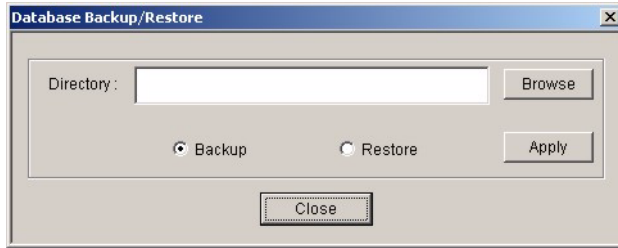
### 2.3.1 Filename Convention

The EMS follows a pre-defined naming convention for the backup data. The backup data is stored in plain text format with a “txt” filename extension. The general structure of the filename is <type>.txt (for example, AccessLog.txt).

### 2.3.2 Database Backup and Restore

Click **Admin, Database Management** and then **Backup/Restore** in the switch manager to display the following screen.

**Figure 6** Switch Manager: Admin: Database Management: Backup/Restore



The following table describes the fields in this screen.

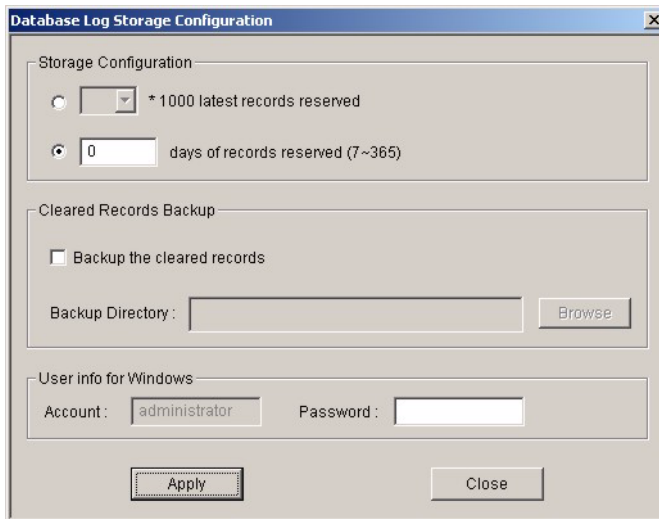
**Table 5** Switch Manager: Admin: Database Management: Backup/Restore

LABEL	DESCRIPTION
Directory	Specify the location you wish the EMS to restore from or back up to on your computer or click <b>Browse</b> to locate it.
Backup	Select <b>Backup</b> to transfer the database file from the EMS to the computer.
Restore	Select <b>Restore</b> to transfer the backed up files from your computer to the EMS.
Apply	Click <b>Apply</b> to backup or restore the database files.
Close	Click <b>Close</b> to close the screen.

### 2.3.3 Database Log Storage Configuration

Click **Admin, Database Management** and then **Log Storage Configuration** in the switch manager to display the following screen.

**Figure 7** Switch Manager: Admin: Database Management: Log Storage



The following table describes the fields in this screen.

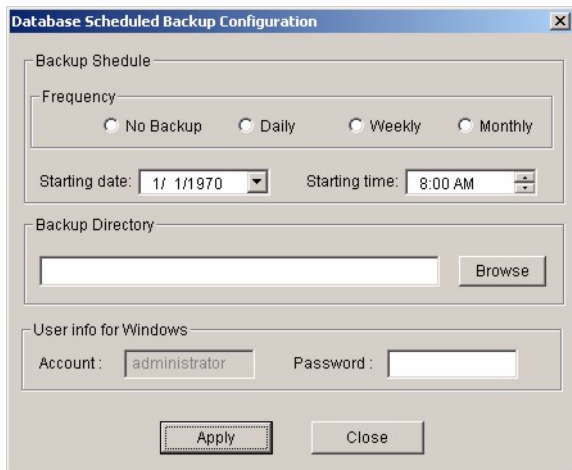
**Table 6** Switch Manager: Admin: Database Management: Log Storage

LABEL	DESCRIPTION
Storage Configuration	Configure the following fields to retain daily records. Select the first radio button and a number (in thousands) from the drop-down list box to retain that number of records. All records prior to these records are cleared every 24 hours. Or Select the second radio button and a number (from 7 to 365) in the field provided. All records up to the start of the period selected are cleared every 24 hours.
Cleared Records Backup	If you do not configure this section, all records (excluding the latest reserved records) will be cleared after 24 hours and therefore cannot be retrieved later.
Backup the cleared records	Select the check box and type the path and file name or click <b>Browse</b> to locate the folder you wish to save all records after 24 hours. The records are cleared but saved in the backup file.
Backup Directory	Type the path and file name of the record file you wish to back up to your computer in the <b>Backup Directory</b> text box or click <b>Browse</b> to locate it.
User info for Windows	
Account	This read-only field displays the Windows login account user.
Password	Enter a password in this field for the administrator <b>Account</b> above.
Apply	Click <b>Apply</b> to save changes to the EMS.
Close	Click <b>Close</b> to close the screen.

### 2.3.4 Database Scheduled Backup Configuration

Click **Admin, Database Management** and then **Backup and Restore (EMS DB)** in the switch manager to display the following screen.

**Figure 8** Switch Manager: Admin: Database Management: Scheduled Backup



The following table describes the fields in this screen.



**Table 7** Switch Manager: Admin: Database Management: Scheduled Backup

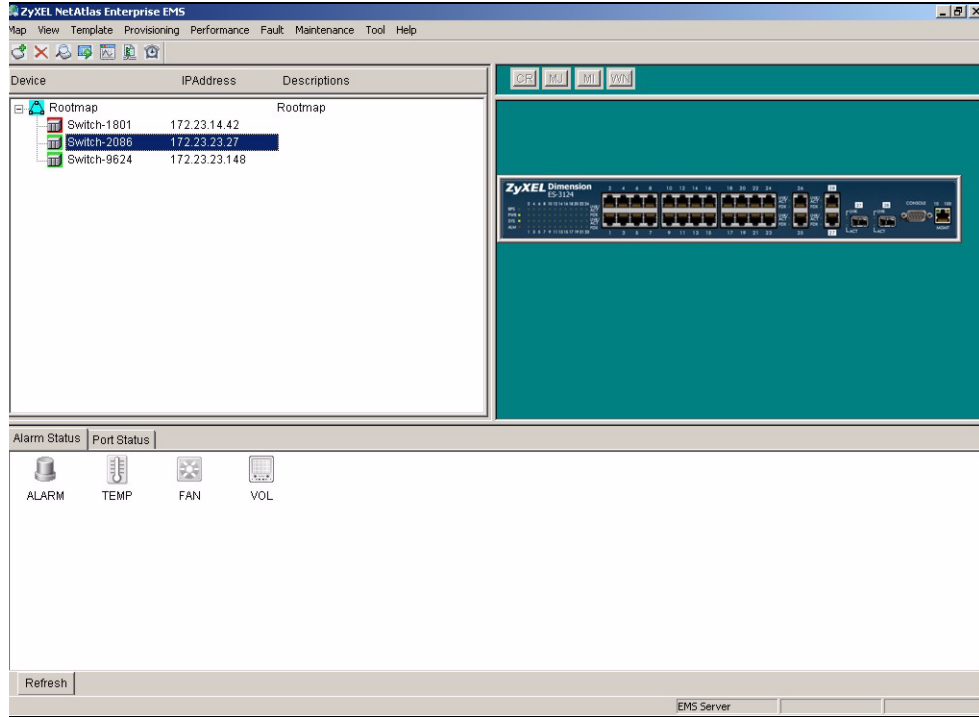
LABEL	DESCRIPTION
Backup Schedule	
Frequency	Scheduled backups can be performed <b>Daily</b> , <b>Weekly</b> or <b>Monthly</b> . Select a radio button to schedule database backups starting from the date and time specified below. The default setting is <b>No Backup</b> .
Starting date	Specify the starting date to begin database backup for the selected device(s). Select a date from the drop-down list box.
Starting time	Specify the starting time to begin database backup for the selected device(s). Select a time from the selection box or enter a time (hh:mm:ss AM/PM format).
Backup Directory	Type the path to which you wish to back up the database files on your computer in the <b>Backup Directory</b> text box or click <b>Browse</b> to locate it.
User info for Windows	
Account	This read-only field displays the Windows login account user.
Password	Enter a password in this field for the administrator <b>Account</b> above.
Apply	Click <b>Apply</b> to save changes to the EMS.
Close	Click <b>Close</b> to close the screen.

## 2.4 Accessing the EMS Main Screen

To display the EMS main screen, click on the device icon in the Switch Manager screen.

The EMS polls for all the available switches. Select a device icon to display a graphic of the switch in the Device Panel. You can only display one switch in the Device Panel at one time.

**Figure 9 EMS: Main Screen**





# CHAPTER 3

## EMS Main Window

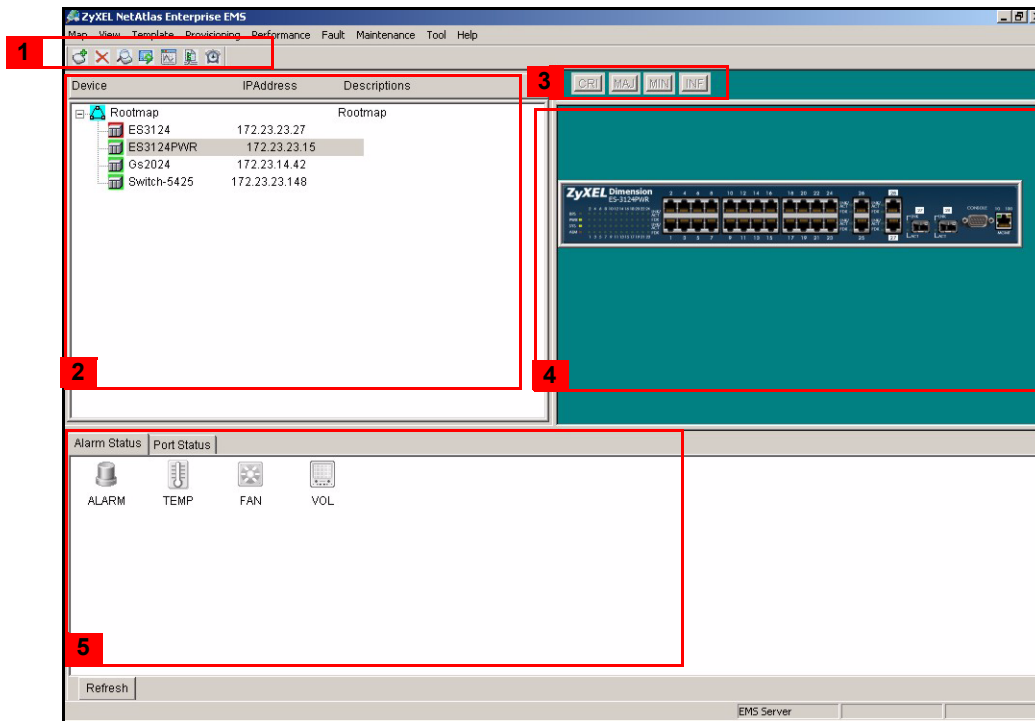
This chapter describes the EMS main window.

### 3.1 Introducing the EMS Main Window

After you have accessed the EMS, double-click the switch device icon in the Device List Panel to display the EMS main screen. The EMS retrieves device information from the switch (using SNMP protocol).

The EMS main screen varies depending on the selected switch model.

**Figure 10** EMS Main Screen Overview



The following table describes the elements in the EMS screen.

**Table 8** EMS Main Screen Overview

	ELEMENT	FUNCTION
1	Menu Shortcut Bar	Use these buttons to execute common commands quickly. Hold the cursor over an icon to see a tool tip.
2	Device List Panel	View devices in a tree structure. The colors of the device icons indicate the time status of the represented devices.
3	Alarm Severity Icons	These icons indicate the presence of any alarm/event logs. Click on an active icon to view the <b>Event Log</b> screen.
4	Device Panel	This is a graphical device display. Double-click on a switch to display the EMS GUI management window for the switch.
5	System Message Panel	View the alarm status <sup>a</sup> and port status of the selected switch.

a. Not available on all models at the time of writing.

### 3.2 Device Icon Colors

The colors of the device icons (in the Device List Panel) indicate the status of the represented devices stored in the database. To update the device status, double-click on a device icon. The following table describes the colors used.





**Table 9** Device Icon Colors

COLOR	DESCRIPTION
Green	The device is working and is responding to polling.
Red	There is no response from the device or the device is not turned on.





### 3.3 System Message Panel Alarm Status

The colors of the alarm icons (in the System Message Panel) indicate the real-time status of the current selected device. The following table describes the alarm states used.

**Table 10** System Message Panel Alarm Status

PANEL ALARMS	ALARM OFF	ALARM ON
ALARM	When this icon is gray out, the device fan, temperature or voltage alarm is off. 	The fan, temperature and voltage alarms are all on. A serious hardware problem exists. 
FAN	When this icon is gray out, the device fans are functioning properly. 	One or more of the device fans has a problem. 

**Table 10** System Message Panel Alarm Status (continued)

PANEL ALARMS	ALARM OFF	ALARM ON
TEMP	When this icon is gray out, temperatures at all sensor points in the switch are within the threshold temperature range. 	The temperature at a sensor point in the switch has risen above or below the threshold temperature range. 
VOL	When this icon is gray out, the power supply at all sensor points in the switch is within the tolerance range. 	The power supply at a sensor point in the switch has fallen out of the tolerance range. 

If an alarm turns on, click the **Port Status** tab in the System Message Panel or proceed to [Section 5.1 on page 48](#) for hardware troubleshooting.

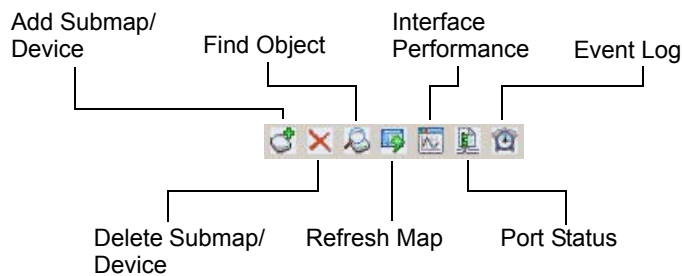
### 3.4 System Message Panel Port Status

Proceed to [Section 5.4 on page 53](#) for information on the details displayed in this screen.

### 3.5 Menu Shortcut Buttons

The following is a brief overview of the menu shortcut buttons.

**Figure 11** EMS Main Screen Shortcut Bar



### 3.6 EMS Main Menu Summary

This is a summary of the EMS menus in the main screen. Screens, screen labels and fields vary depending on your switch model.

**Table 11** EMS Menu Summary

MAP	VIEW	TEMPLATE	PROVISIONING	PERFORMANCE	FAULT	MAINTENANCE	TOOL	HELP
Add Submap /Device	Hardware Status	VLAN Template	IGMP Filtering Provisioning	Interface	Event Log	Firmware Upgrade	Telnet	About
Edit Node	STP Status	IGMP Filtering Profile Template			Loopback Test	Device Reset	Web Access	
Search Node	VLAN Status	Multicast Template				NE (Network Element) Configuration Backup and Restore	Ping	
Delete	Port Status					Load Factory Default		
Refresh	802.1d					Scheduled NE Config Backup		
Exit	Multicast Status							

The following table summarizes these sub-links in the navigation panel.

**Table 12** EMS Navigation Panel Sub-link Descriptions

DESCRIPTION	LABEL
MAP Screens	
Add Submap/Device	This link takes you to a screen where you can add a device or a submap folder to the EMS Device List Panel.
Edit Node	This link takes you to a screen where you can edit device properties.
Search Node	This link takes you to a screen where you can search for a device or a submap folder.
Delete	Click this link to delete a submap folder or devices within a folder.
Refresh	Click this link to update the screen with the most recently saved settings.
View	
Hardware Status	This link takes you to a screen where you can view the hardware status of a device.
STP Status	This link takes you to a screen where you can view the Spanning Tree Protocol (STP) status of a device.
VLAN Status	This link takes you to a screen where you can view the VLAN status of a device.
Port Status	This link takes you to a screen where you can view the port status of a device.

**Table 12** EMS Navigation Panel Sub-link Descriptions (continued)

DESCRIPTION	LABEL
802.1d	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs or view the MAC addresses – IP address resolution table.
Multicast Status	This link takes you to a screen where you can view the multicast traffic status of a device.
Template	
VLAN Template	This link takes you to a screen where you can pre-configure a VLAN template for upload to multiple devices.
IGMP Filtering Profile Template	This link takes you to screens where you can pre-configure an IGMP filter template for upload to multiple devices.
Multicast Template	This link takes you to a screen where you can configure a multicast template for upload to multiple devices.
Provisioning	
IGMP Filtering Provisioning	This link takes you to screens where you can apply IGMP filtering templates.
Performance	
Interface	This link takes you to a screen where you can configure interface performance graphs and tables.
Fault Screens	
Event Log	This link takes you to a screen where you can configure an alarm filter.
Loopback Test	This link takes you to a screen where you can perform a loopback test.
Maintenance	
Firmware Upgrade	This link takes you to a screen where you can perform a device firmware upgrade.
Device Reset	This link takes you to a screen where you can reset a device.
NE (Network Element) Configuration Backup and Restore	This link takes you to a screen where you can backup or restore configuration files.
Load Factory Default	This link takes you to a screen where you can load the factory default settings.
Scheduled NE Config Backup	This link takes you to a screen where you can schedule when you want to backup a device configuration file.
Tool Screens	
Telnet	This link takes you to a screen where you can access a device Telnet service.
Web Access	This link takes you to a screen where you can access a device Web configurator.
Ping	This link takes you to a screen where you can ping a device directly through the EMS.



### 3.7 Common EMS Command Buttons

The following table shows common command buttons found on most EMS screens.

**Table 13** Common EMS Command Buttons

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save the changes back to the switch.
OK	Click <b>OK</b> to save your changes and close the screen.
Cancel	Click <b>Cancel</b> to discard all changes and close the screen.
Close	Click <b>Close</b> to close the screen.

### 3.8 View the Switch

To display a selected switch, double-click the appropriate switch in the Device List Panel or on the switch icon in the Device Panel. You can only display one switch in the device Panel window at a time. Refer to the appropriate chapters or sections for the descriptions of each menu screen.

**Figure 12** Switch View

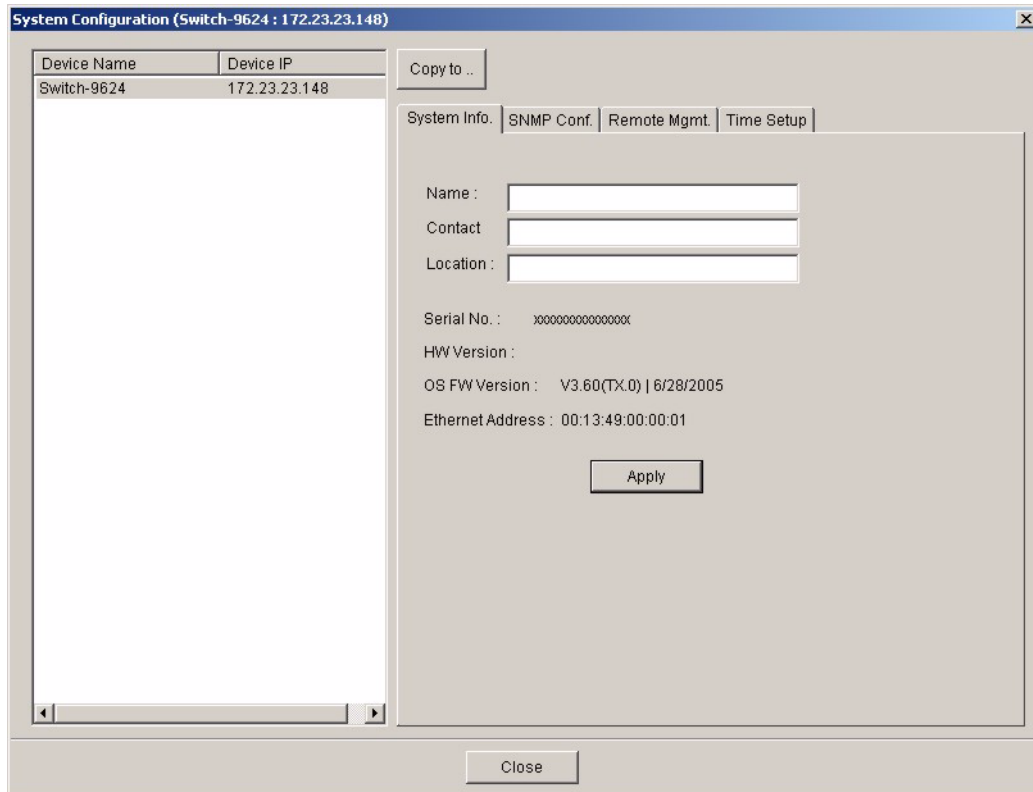


### 3.9 Switch Information

Follow the steps to display information on a switch.

- 1 Right-click on the switch icon in the Device List Panel.
- 2 Click **Configuration**, **System** and then **System Info**. The switch information window displays as shown next.
- 3 Choose a switch from the list located on the left-hand side of the screen.

**Figure 13** Configuration: System Configuration: System Info



The following table describes the labels in this screen.

**Table 14** Configuration: Switch System Configuration

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes. If you want to change the name, enter up to 32 printable characters; spaces are not allowed.
Contact	Enter the name (up to 32 characters) of the person in charge of the selected switch.
Location	Enter the geographic location (up to 32 characters) of the selected switch.
Serial No.	This field displays the serial number of the selected switch.
HW Version	This field displays the hardware version of the selected switch.
OS FW Version	This field displays the firmware version of the selected switch.
Ethernet Address	This field displays the switch Ethernet MAC address in six hexadecimal character pair format.
Apply	Click <b>Apply</b> to save the changes back to the switch.
Close	Click <b>Close</b> to close the screen.

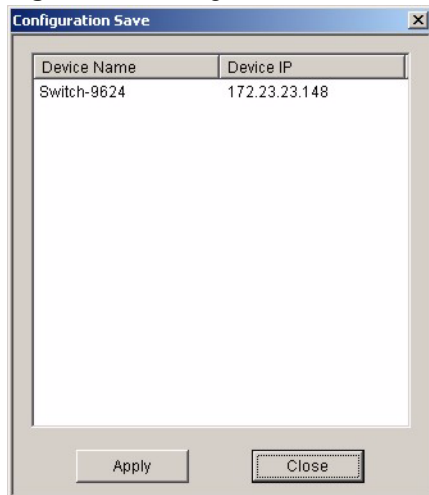
### 3.10 Configuration Save

You can save the current configuration in the EMS to the selected switch.

**Note:** Do NOT turn off the switch during the updating process, as it may corrupt the firmware and make your switch unusable.

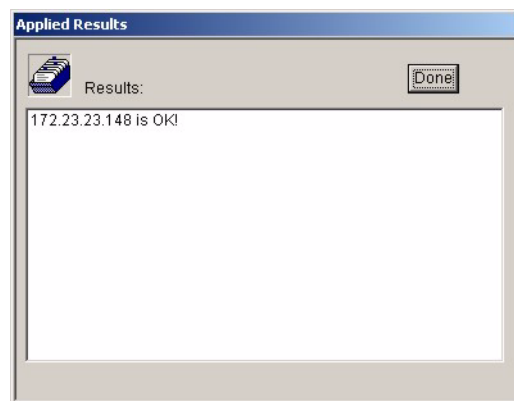
- 1 To save the current switch configuration, right-click on the switch icon in the Device List Panel.
- 2 Click **Configuration Save**.
- 3 Choose a switch from the list located in the screen.

**Figure 14** Configuration Save



- 4 Click **Apply** to save the current configuration. All settings configured on the EMS will be saved to the selected switch.
- 5 A screen displays showing the configuration save result. Click **Done** to close the screen.

**Figure 15** Configuration Save: Result



# CHAPTER 4

## Map

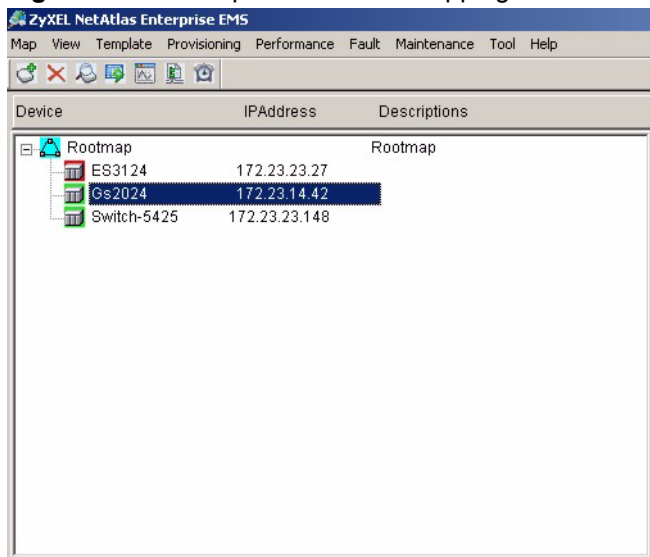
This chapter describes the Map screens you use to add, edit or delete device mappings in the EMS.

### 4.1 Submap and Device Mapping

The EMS mapping displays logical hierarchy for the switch in the EMS. When you first start the EMS, the default Root Map and an icon for your switch device are created in the Device List Panel automatically. Both devices and submaps (or folders) can be added below the rootmap. Devices can also be added to submap folders.

The following figure shows the “Rootmap” folder. “Switch-5425”, “Gs2024” and “ES3124” are mapped to the “Rootmap” folder.

**Figure 16** Submaps and Device Mapping



**Note:** You cannot create, edit or delete the Rootmap.

#### 4.1.1 Adding a Submap or Device

To add a new submap or a new device, select the Root Map or a submap icon in the Device List Panel. Click **Map** and **Add Submap/Device** to display the following screen.

**Figure 17** Map: Add Submap/Device



The following table describes the labels in this screen.

**Table 15** Map: Add Submap/Device

LABEL	DESCRIPTION
Properties	Select the <b>Submap</b> or <b>Device</b> radio button to add a new submap or device icon to the Device List Panel. If you select <b>Submap</b> , only the <b>Name</b> and <b>Description</b> fields display; all other fields appear as read-only.
Name	Enter a descriptive name (up to 30 characters) for this node for identification purposes.
IP Address	Enter the IP address of the device.
Password	Enter the administrative password (up to 30 characters) you use to log in to the switch. This password is used by the EMS administrator for device firmware upload.
Description	Enter a description (up to 30 characters) about the device.
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext-requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
OK	Click <b>OK</b> to save the changes and close the screen.
Cancel	Click <b>Cancel</b> to discard the changes and close the screen.

### 4.1.2 Edit a Node

Select a submap icon in the Device List Panel and then click **Map** and **Edit Node**.

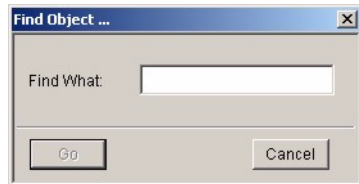
**Figure 18** Map: Edit Node

The screenshot shows a dialog box titled "Add Submap/Device". It has two radio buttons: "Submap" and "Device", with "Device" selected. Below the radio buttons are several text input fields: "Name" with the value "Test", "IP Address" with the value "172 . 23 . 23 . 27", "Password" (empty), "Description" (empty), "Get Community" with the value "public", "Set Community" with the value "public", and "Trap Community" with the value "public". At the bottom of the dialog are "OK" and "Cancel" buttons.

Refer to [Table 15 on page 45](#) for the field descriptions.

### 4.1.3 Find an Object

To find or locate a device (or node), click **Map** and then **Find Object**.

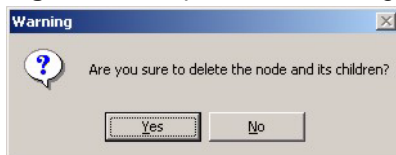
**Figure 19** Map: Find Object

The screenshot shows a dialog box titled "Find Object ...". It contains a text input field labeled "Find What:" which is currently empty. Below the input field are "Go" and "Cancel" buttons.

Enter a descriptive text (for example, the node name) in the **Find** field and click **OK** to start the search.

### 4.1.4 Delete a Submap

To delete a submap, select the submap icon in the Device List Panel and click **Map** and then **Delete**.

**Figure 20** Map: Delete Warning

The screenshot shows a dialog box titled "Warning". It features a question mark icon in a speech bubble and the text "Are you sure to delete the node and its children?". At the bottom are "Yes" and "No" buttons.

**Note:** If you delete a submap, all devices under a submap will be removed.

### 4.1.5 Delete a Device

To remove a device from the Device List Panel, select the device icon and click **Map** and then **Delete**.

## 4.2 Exit

Click **Map** and then **Exit** to close the EMS screen.

# CHAPTER 5

## View

This chapter describes the hardware status, STP status, VLAN status, port status and 802.1d status **View** screens.

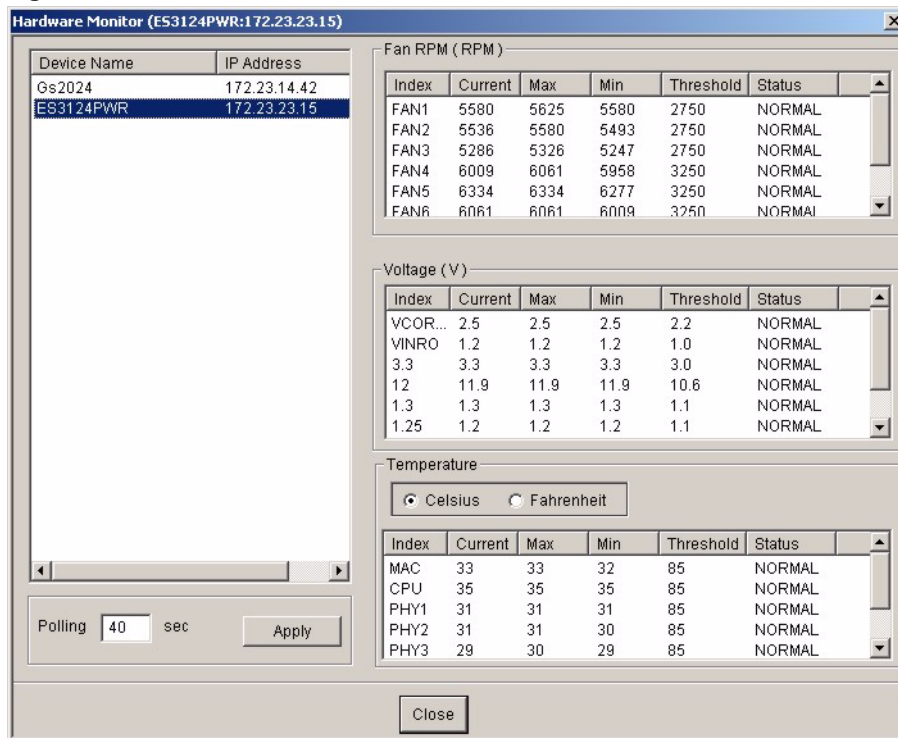
### 5.1 Hardware Status<sup>1</sup>

View fan speeds, voltage levels and temperatures of a selected switch in the **Hardware Monitor** screen.

Click **View** and then **Hardware Status** and select a switch from the device list located on the left-hand side of the screen. The device hardware status displays.

**Note:** It may take a few seconds to update the screen.

**Figure 21** View: Hardware Status



The following table describes the labels in this screen.

1. This features is not available for the ES-2024A at the time of writing.



**Table 16** Status: Hardware Status

LABEL	DESCRIPTION
Fan RPM (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Index	This field displays the fan number.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
Max	This field displays this fan's maximum speed recorded in Revolutions Per Minute (RPM).
Min	This field displays this fan's minimum speed recorded in Revolutions Per Minute (RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	<b>NORMAL</b> indicates that this fan is functioning above the minimum speed. <b>ERROR</b> indicates that this fan is functioning below the minimum speed.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Index	This field displays the first voltage sensor number.
Current	This is the current voltage reading in volts.
Max	This field displays the maximum voltage recorded at this sensor in volts.
Min	This field displays the minimum voltage recorded at this sensor in volts.
Threshold	This field displays the minimum voltage percentage at which the switch should work.
Status	<b>NORMAL</b> indicates that the voltage is within an acceptable operating range at this point; otherwise <b>ERROR</b> is displayed. <b>ABSENT</b> indicates that there is no power reading at a sensor(s).
Temperature	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (in degrees Celsius or or Fahrenheit).
Celsius	Select this option to display the temperature in degrees Centigrade.
Fahrenheit	Select this option to display the temperature in degrees Fahrenheit.
Index	This field displays the temperature sensor number.
Current Value	This shows the current temperature at this sensor.
Max	This field displays the maximum temperature recorded at this sensor.
Min	This field displays the minimum temperature recorded at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays <b>NORMAL</b> for temperatures below the threshold and <b>ERROR</b> for those above.
Polling	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking the <b>Apply</b> button.
Close	Click <b>Close</b> to close the screen.

## 5.2 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other STP-compliant switches in your network to ensure that only one route exists between any two stations on the network.

### 5.2.1 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

**Table 17** STP Path Costs

LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
4Mbps	250	100 to 1000	1 to 65535
10Mbps	100	50 to 600	1 to 65535
16Mbps	62	40 to 400	1 to 65535
100Mbps	19	10 to 60	1 to 65535
1Gbps	4	3 to 10	1 to 65535
10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

### 5.2.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

### 5.2.3 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

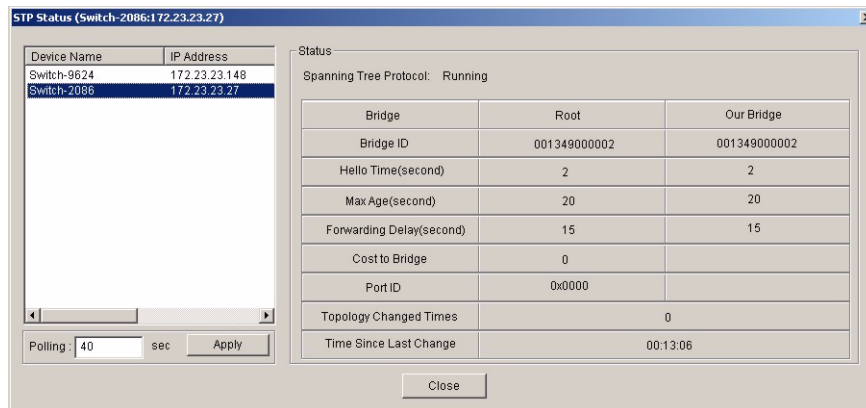
**Table 18** STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

### 5.2.4 STP Status

View current STP information in the **STP Status** screen. Click **Status** and then **STP Status**. Select a switch from the device list located on the left-hand side of the screen. The STP status displays in the table.

**Figure 22** View: STP Status



The following table describes the labels in this screen.

**Table 19** View: STP Status

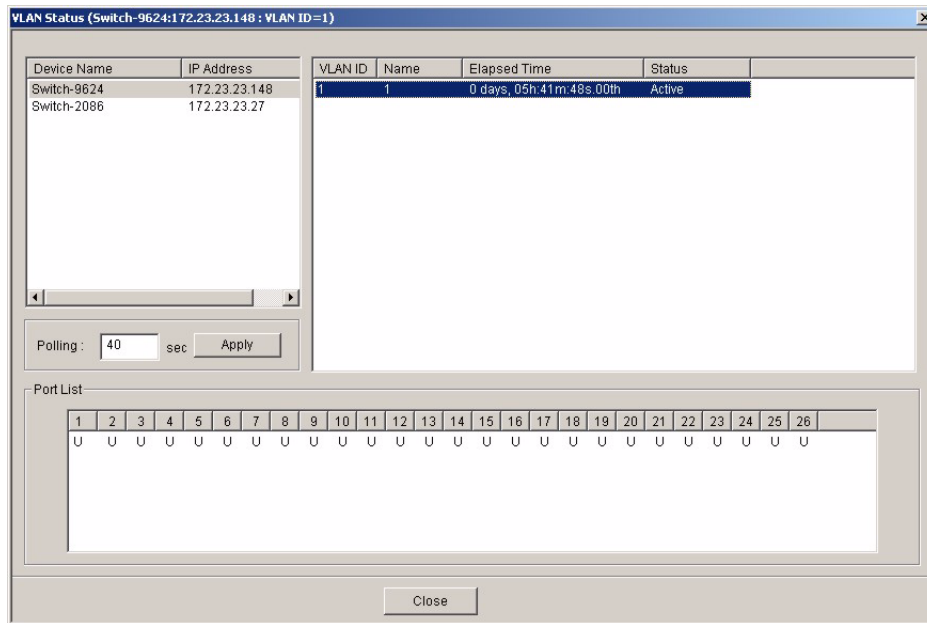
<b>LABEL</b>	<b>DESCRIPTION</b>
STP	This field displays <b>Running</b> if STP is activated; otherwise, it displays <b>Down</b> .
Bridge	<b>Root</b> refers to the base of the spanning tree (the root bridge).
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address.
Hello Time (second)	This is the time interval (in seconds) at which the root device transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the spanning tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Polling	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking the <b>Apply</b> button.
Close	Click <b>Close</b> to close the screen.

## 5.3 VLAN Status

Follow the steps below to view the VLAN status of a switch.

- 1** Click **View** and then **VLAN Status**.
- 2** Choose a switch from the list located on the left-hand side of the screen.

**Figure 23** View: VLAN Status



The following table describes the labels in this screen.

**Table 20** View: VLAN Status

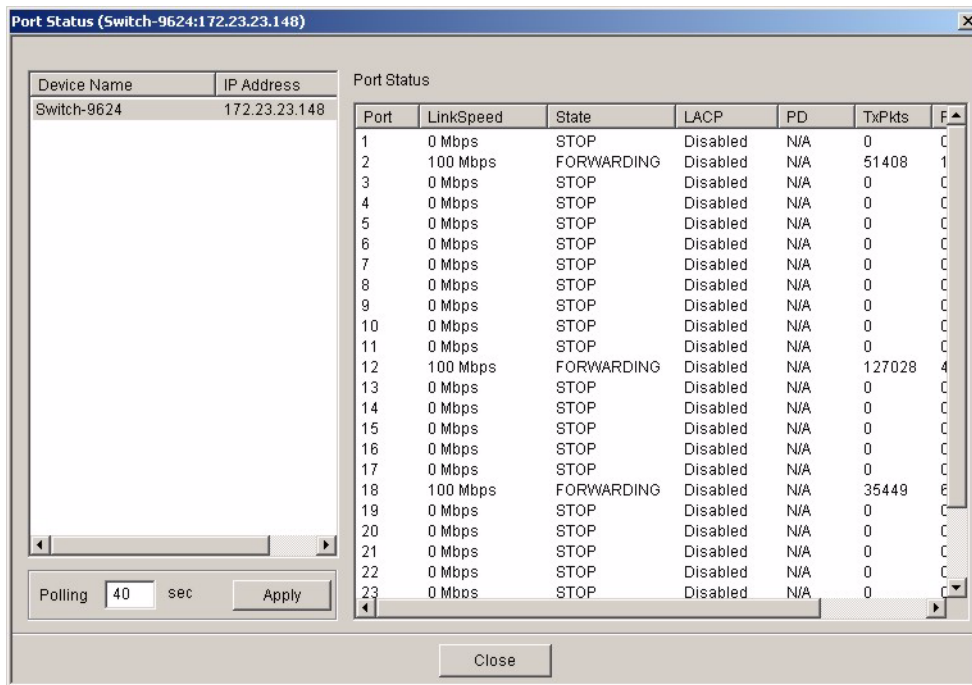
LABEL	DESCRIPTION
VLAN ID	This field displays the identification number of the VLAN.
Name	This field displays a unique number for identification purposes.
Elapsed Time	This field displays the time since the VLAN was created.
Status	This field displays <b>Active</b> if the VLAN is active and will remain so after the next reset of the device. This field displays <b>GVRP</b> if the VLAN is active and will remain so until removed by GVRP. This field is other if the VLAN is active, but is not permanent or created by GVRP.
Port List	This table displays all available ports that are participating in a VLAN. A tagged port is marked T while an untagged port is marked U.
Polling	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking the <b>Apply</b> button.
Close	Click <b>Close</b> to close the screen.

## 5.4 Port Status

Follow the steps below to view the port status of a switch.

- 1 Click **View** and then **Port Status** to display the following screen.
- 2 To view the port status of a switch choose a switch from the list located on the left-hand side of the screen.

**Figure 24** View: Port Status



The following table describes the labels in this screen.

**Table 21** View: Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Link Speed	This field displays the speed (either 10M for 10Mbps, 100M for 100Mbps or 1000M for 1000Mbps).
State	This field displays the STP state of the port. See the Spanning Tree Protocol chapter for details on STP port states.
LACP	This field displays whether LACP is activated.
PD	This field displays the power device (PD) module status on the switch. If <b>N/A</b> is displayed, the switch does not have a PD. This field displays <b>On</b> if the switch has a PD and it is in use. This field displays <b>Off</b> if the switch has a PD, but it is not in use.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Polling	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking the <b>Apply</b> button.
Close	Click <b>Close</b> to close the screen.

## 5.5 802.1D

Use the following screens to view a table of MAC address entries or to view a table of IP address mappings.

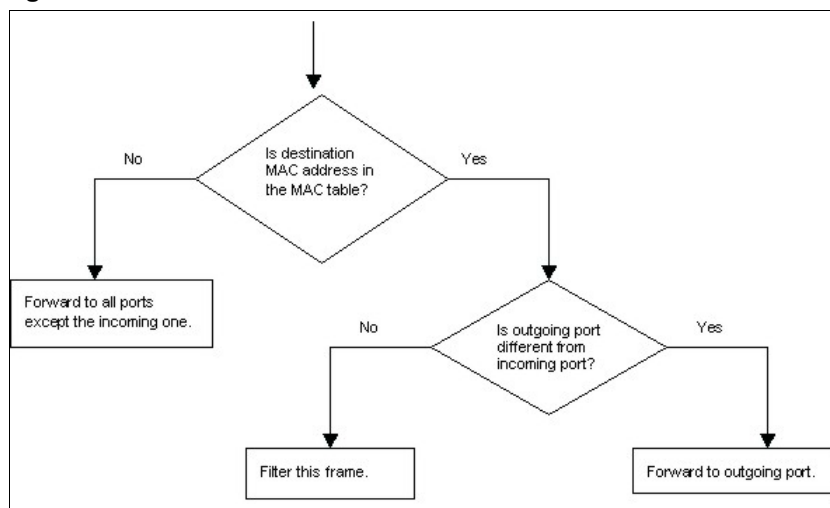
### 5.5.1 802.1D: MAC Table

The MAC table shows how frames are forwarded or filtered across the switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the switch) or static (manually entered in Static MAC Forwarding).

The switch uses the Filtering Database to determine how to forward frames. See the following figure.

- 1 The switch examines a received frame and learns the port on which this source MAC address came.
- 2 The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the Filtering Database.
  - If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
  - If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
  - If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

**Figure 25** MAC Table Flowchart

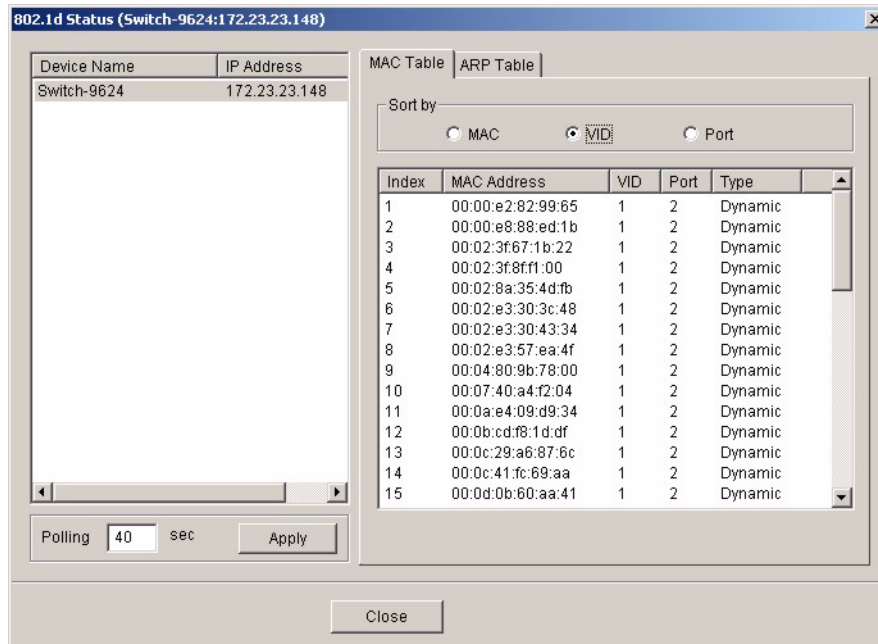


### 5.5.2 View the MAC Table

Follow the steps below to view the MAC table.

- 1 Click **View** and then **802.1d**.
- 2 To view the MAC table of a switch choose a switch from the list located on the left-hand side of the screen and click the **MAC Table** tab.

**Figure 26** View: 802.1d: MAC Table



The following table describes the labels in this screen.

**Table 22** View: 802.1d: MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in the <b>Static MAC Forwarding</b> screen).
Polling	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking the <b>Apply</b> button.
Close	Click <b>Close</b> to close the screen.



### 5.5.3 802.1D: ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

### 5.5.4 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

### 5.5.5 View the ARP Table

Follow the steps below to view the ARP table.

- 1 Click **View** and then **802.1d**.
- 2 To view the ARP table of a switch choose a switch from the list located on the left-hand side of the screen and click the **ARP Table** tab.

**Figure 27** View: 802.1d: ARP Table

Device Name	IP Address
Switch-9624	172.23.23.148

Index	IP Address	MAC Address	Type
1	0.0.0.0	00 0F FE 32 B4 12	dynamic
2	172.23.23.147	00 C0 9F 9B C9 72	dynamic
3	172.23.23.48	00 D0 59 CF BA EC	dynamic
4	172.23.23.109	00 0D 60 2C 36 84	dynamic
5	172.23.23.6	00 0C 41 FC 69 AA	dynamic
6	172.23.23.144	00 D0 59 CE E6 2E	dynamic
7	172.23.23.59	00 10 B5 AE 56 9B	dynamic
8	172.23.23.80	00 02 3F 8F F1 00	dynamic
9	172.23.23.53	00 C0 A8 FA E9 27	dynamic
10	172.23.23.3	00 50 8D 48 59 1F	dynamic
11	172.23.23.5	00 D0 59 B8 10 5D	dynamic
12	172.23.23.26	00 C0 9F 9B CB 04	dynamic
13	172.23.23.45	00 0F FE 0D 78 85	dynamic
14	172.23.23.62	00 0B CD F8 1D DF	dynamic
15	172.23.23.128	00 00 E8 88 ED 1B	dynamic
16	172.23.23.113	00 0D 60 CC 15 D8	dynamic
17	172.23.23.4	00 0A E4 09 D9 34	dynamic
18	172.23.23.110	00 C0 9F 9B C6 F6	dynamic
19	172.23.23.74	00 02 F3 30 3C 48	dynamic

The following table describes the labels in this screen.

**Table 23** View: 802.1d: ARP Table

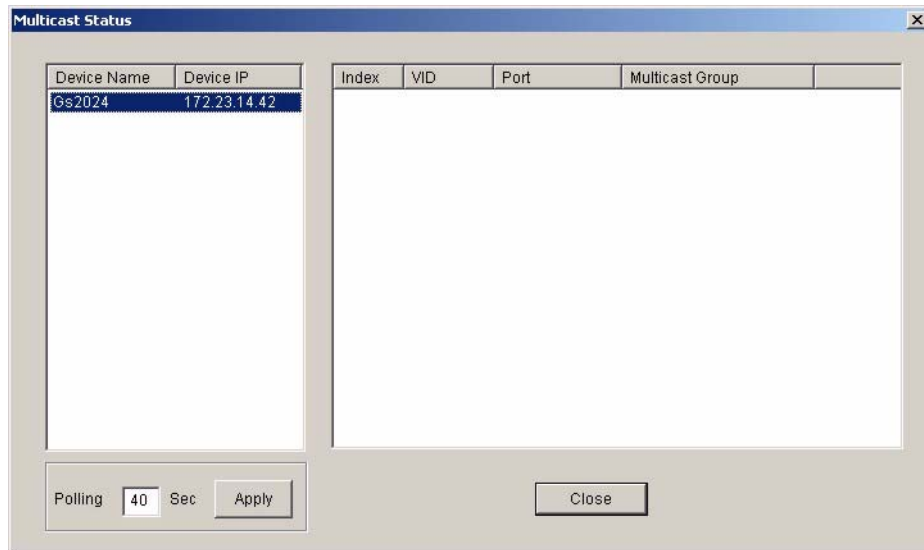
LABEL	DESCRIPTION
Index	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in the <b>Static MAC Forwarding</b> screen).
Polling	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking the <b>Apply</b> button.
Close	Click <b>Close</b> to close the screen.

## 5.6 Multicast Status

View the IGMP multicast group membership information in the **Multicast Status** screen.

Click **View** and **Multicast Status** to display the screen as shown. Select a switch model in the device list to display the multicast group membership information.

**Figure 28** View: Multicast Status



The following table describes the labels in this screen.

**Table 24** View: Multicast Status

LABEL	DESCRIPTION
Index	This field displays the index number.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number(s) that belongs to the multicast group.
Multicast Group	This field displays the multicast group address.

# CHAPTER 6

## Template

This chapter describes how to configure VLAN, IGMP filtering and multicast templates.

### 6.1 Template Overview

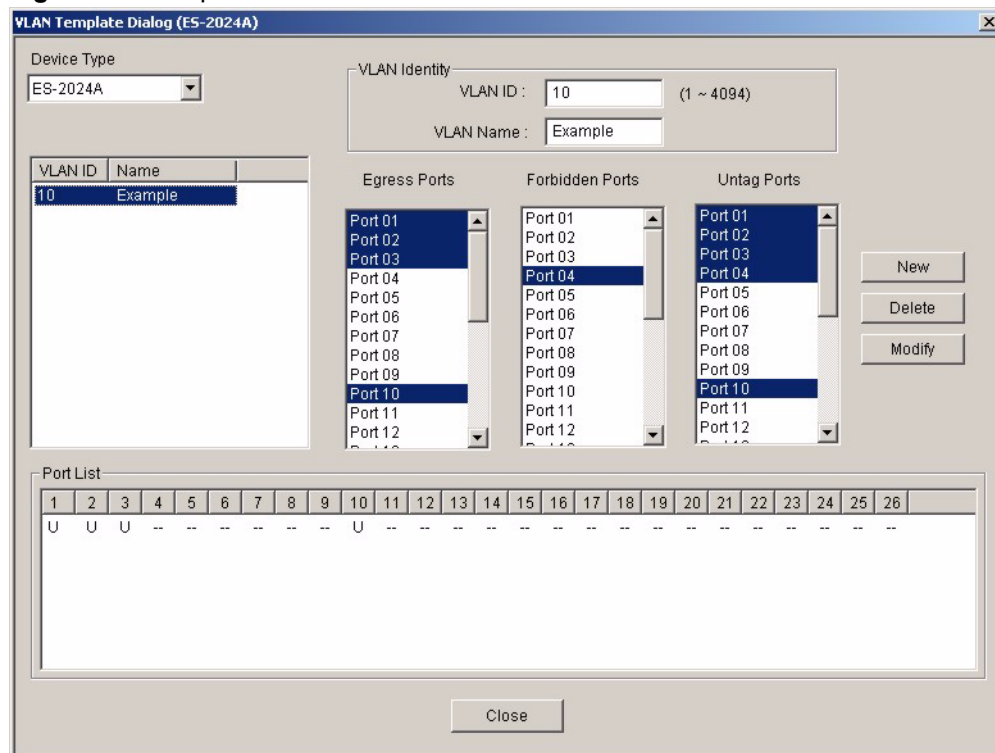
A template is a pre-configured set of configuration settings. Templates allow you to configure device VLANs efficiently. The template can then be uploaded to one or more devices thus removing the need to configure the VLAN settings for each device. See the VLAN Configuration chapter for more information on the template upload.

### 6.2 VLAN Template

Refer to [Section 15.1 on page 128](#) for more background information on VLAN.

Click **Template** and then click **VLAN** to display the screen as shown. Use this screen to configure, delete or view a VLAN template.

**Figure 29** Template: VLAN



The following table describes the labels in this screen.

**Table 25** Template: VLAN

LABEL	DESCRIPTION
Device Type	Select a device from the drop-down list box to view the device's VLAN configuration.
VLAN Identity	
VLAN ID	Enter a unique number to identify the VLAN.
VLAN Name	Enter a descriptive name for identification purposes.
Egress Ports	A port that is in the egress list in a VLAN. Only select this if the subscriber's DSL modem or router supports IEEE 802.1Q VLAN. Select the ports which you want to be egress ports from the list provided.
Forbidden Ports	A port that is blocked from joining a VLAN group. No frames are transmitted through this port. A forbidden port cannot be an egress port and cannot add tags to outgoing traffic. Select the ports which you want to be forbidden ports from the list provided.
Untag	A port that does not tag all outgoing frames transmitted. An egress port can be untagged. Select the ports which you want to be untagged ports from the list provided.
New	Click <b>New</b> to create a new VLAN. You must enter a <b>VLAN ID</b> and a <b>VLAN Name</b> to create a new <b>VLAN</b> . The new VLAN and name is displayed in the left-hand column in this screen.
Delete	Click on a VLAN in the left-hand column of this screen and then click the <b>Delete</b> button to remove it from the VLAN template.
Modify	Click on a VLAN in the left-hand column of this screen. Change the <b>VLAN Name</b> or change the configuration of the egress, forbidden and untagged ports. Click the <b>Modify</b> button to save the changes to the switch. If you want to change the <b>VLAN ID</b> of a VLAN configuration, you can only delete the VLAN configuration or create a new VLAN configuration using a different <b>VLAN ID</b> .
Port List	Click on a port in the <b>Egress Ports</b> list to add the selected port to the port list. If a port is not selected from any of the three port lists, then it is a normal tagged port. This fields displays all available ports that are participating in a VLAN. A tagged port is marked T while an untagged port is marked U.
Close	Click <b>Close</b> to close the screen.

### 6.3 IGMP Filter Template

Templates (also know as profiles) allow you to configure device IGMP filter settings efficiently. The template can then be uploaded to one or more devices thus removing the need to configure the IGMP filter settings for each device.

With the IGMP filter feature, you can limit the number of IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the device to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering template and associating the profile to a port.

IGMP filter templates allow you to control access to IGMP multicast groups. This allows you to have a service available to a specific IGMP multicast group. You can configure an IGMP filter template for an IGMP multicast group that has access to a service (like a SIP server for example).

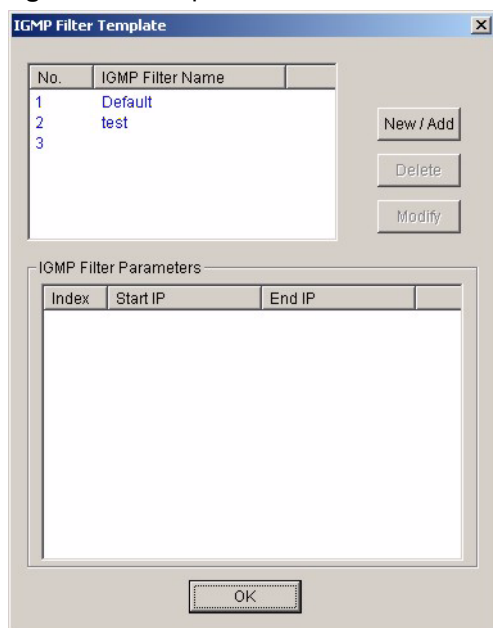
### 6.3.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

### 6.3.2 Configuring an IGMP Filter Template

Click **Template** and then click **IGMP Filtering Template** to display the screen as shown.

**Figure 30** Template: IGMP Filter



The following table describes the labels in this screen.

**Table 26** Template: IGMP Filter

LABEL	DESCRIPTION
No.	This field displays the index number.
IGMP Filter Name	This name identifies the IGMP filter profile.
New/Add	Click <b>New/Add</b> to create an IGMP filter profile.
Delete	Click <b>Delete</b> to remove one or more selected IGMP filter profiles.

**Table 26** Template: IGMP Filter (continued)

LABEL	DESCRIPTION
Modify	Click <b>Modify</b> to edit a selected IGMP filter profile.
IGMP Filter Parameters	This table displays the settings of the selected IGMP filter above.
Index	This is the number of the IGMP filter profile.
Start IP	This field displays the starting multicast IP address for a range of multicast IP addresses to which you want this IGMP filter profile to allow access.
End IP	This field displays the ending multicast IP address for a range of IP addresses to which you want this IGMP filter profile to allow access.
OK	Click <b>OK</b> to save your changes.

### 6.3.3 New IGMP Filter Template Screen

Click **New/Add** in the **IGMP Filtering Template** screen to display the screen as shown.

**Figure 31** Template: New IGMP Filter

The screenshot shows a dialog box titled "New IGMP Filter". At the top, there is a text input field for "IGMP Filter Name". Below it are two IP address input fields: "Start Address" and "End Address", both containing the value "224 . 0 . 0 . 0". To the right of these fields are two buttons: "Add" and "Clear". Below the input fields is a table titled "IGMP Filter Parameters" with three columns: "Index", "Start Address", and "End Address". The table is currently empty. At the bottom center of the dialog box is a "Close" button.

The following table describes the labels in this screen.

**Table 27** Template: New IGMP Filter

LABEL	DESCRIPTION
No.	This field displays the index number.
IGMP Filter Name	Type a name (up to 31 printable characters) to identify the IGMP filter profile.
New/Add	Click <b>New/Add</b> to create a new IGMP filter template.
Delete	Click <b>Delete</b> to remove the selected IGMP filter template.
Modify	Click <b>Modify</b> to change the settings of the selected IGMP filter template.
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses to which you want this IGMP filter profile to allow access.
End Address	Enter the ending multicast IP address for a range of IP addresses to which you want this IGMP filter profile to allow access. If you want to add a single multicast IP address, enter it in both the <b>Start IP</b> and <b>End IP</b> fields.
Index	This is the number of the IGMP filter profile. Double-click a profile's index number to edit the profile.
Start Address	This field displays the starting multicast IP address for a range of multicast IP addresses to which you want this IGMP filter profile to allow access.
End Address	This field displays the ending multicast IP address for a range of IP addresses to which you want this IGMP filter profile to allow access.
Close	Click <b>Close</b> to close this screen.

## 6.4 Static Multicast Group Template

Use the static multicast filter to allow incoming frames based on multicast MAC address(es) that you specify. This feature can be used in conjunction with IGMP snooping to allow multicast MAC address(es) that are not learned by IGMP snooping. Use the static multicast filter to pass routing protocols, such as RIP and OSPF.

A static multicast group template allows you to configure multicast filters efficiently. The template can then be uploaded to one or more devices thus removing the need to configure the static multicast filter settings for each device.

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

You can set the switch to forward multicast data to specific port(s). This is essential for sending multicast traffic to hosts that cannot report their membership with IGMP.



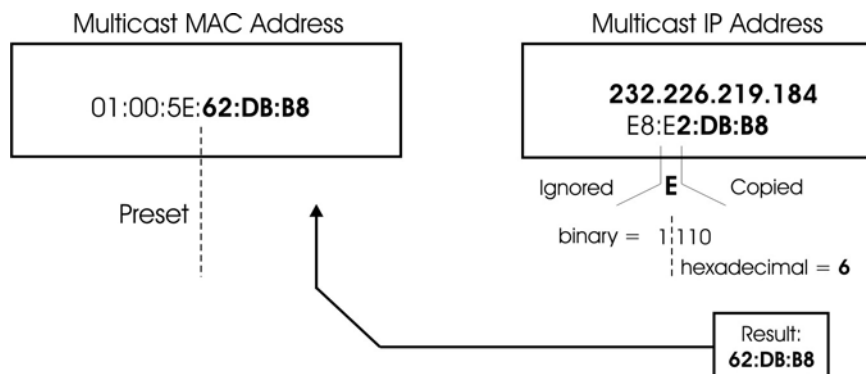
## 6.4.1 Multicast MAC Address

All Ethernet devices must have a unique MAC address to communicate with one another. Device such as routers and switches on the LAN keeps a table of MAC-IP address mappings. When a packet is received, the destination IP address is looked up in the address mapping table and the packet is forwarded to the intended Ethernet device. IP multicast packets are in the Class D group addresses, thus an IP multicast address does not correspond to a unique Ethernet device.

The IANA has reserved a range of address (01:00:5e:00:00:00 to 01:00:5e:7f:ff:ff in hexadecimal notation) for multicasting. This range gives 23 usable bits. The IP-MAC multicast address mapping is done by copying the lower-order 23-bit of a Class D address to the lower-order 23-bit of the MAC multicast address.

The following figure shows an example.

**Figure 32** Multicast MAC-IP Address Mapping Example

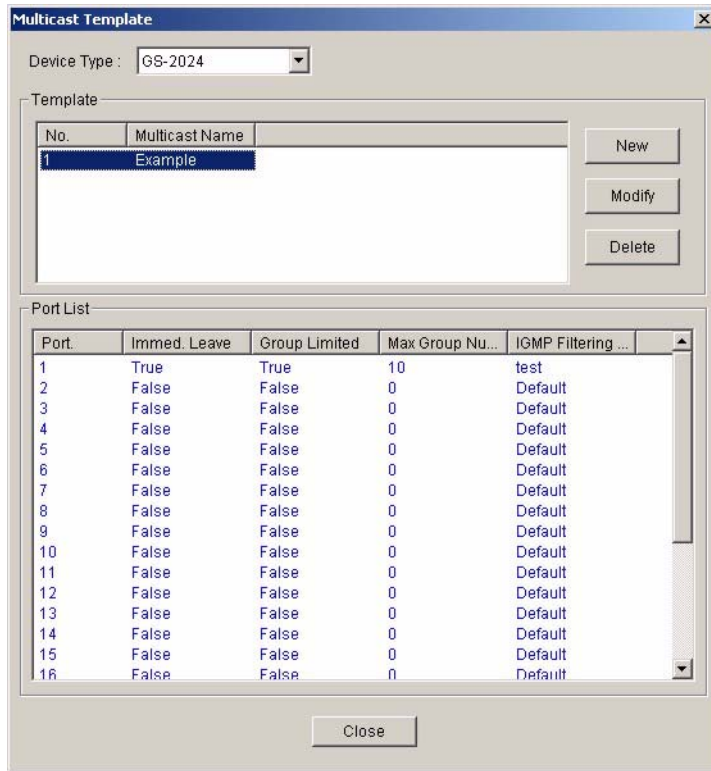


Since 32 Class D addresses are mapped to the same multicast MAC address, filtering (by checking the destination IP address) is recommended on the Ethernet devices to reduce excessive multicast packets.

## 6.4.2 Static Multicast Group Template Screen

Click **Template** and then click **Static Multicast Group Template** to display the screen as shown.

**Figure 33** Template: Multicast



The following table describes the labels in this screen.

**Table 28** Template: Multicast

LABEL	DESCRIPTION
Device Type	Select a device from the drop-down list box to view the device's VLAN configuration.
Template	
No.	This field displays the index number.
Multicast Name	This field displays the descriptive name for the multicast template.
New	Click <b>New</b> to create a new multicast template.
Modify	Click <b>Modify</b> to change the settings of the selected multicast template.
Delete	Click <b>Delete</b> to remove the selected multicast template.
Port List	
Port	This field displays the port number.
Immed. Leave	This field displays <b>True</b> when the switch is set to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. This field displays <b>False</b> when the feature is disabled.
Group Limit	This field shows whether the switch limit the number of multicast groups this port is allowed to join or not. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
Max. Group Number	This field displays the number of multicast groups this port is allowed to join.

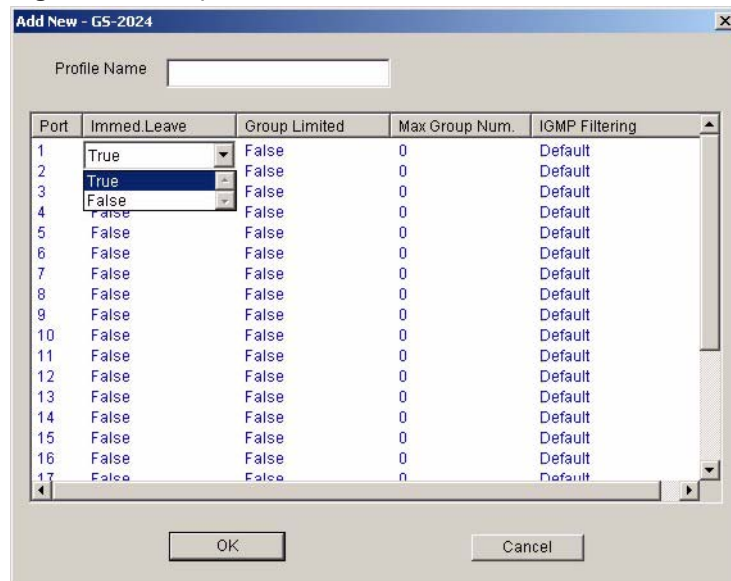
**Table 28** Template: Multicast (continued)

LABEL	DESCRIPTION
IGMP Filtering	This field displays the name of the IGMP filtering profile to use for this port.
Close	Click <b>Close</b> to close this screen.

### 6.4.3 New Multicast Template Screen

To create a new multicast template, click **New** in the **Multicast Template** screen. A screen displays as shown.

**Figure 34** Template: New Multicast



The following table describes the labels in this screen.

**Table 29** Template: New Multicast

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the new multicast template.
Port	This field displays the port number.
Immed. Leave	Specify whether the switch is to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select <b>True</b> from the drop-down list box to activate the immediate leave feature. Select <b>False</b> to disable this feature.
Group Limit	Select <b>True</b> to limit the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port. Select <b>False</b> to disable this feature.
Max. Group Number	Enter a number to limit the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filter	Select the name of the IGMP filtering profile to use for this port.

**Table 29** Template: New Multicast (continued)

LABEL	DESCRIPTION
OK	Click <b>OK</b> to save the settings and close this screen.
Cancel	Click <b>Cancel</b> to discard all changes and close this screen.



# CHAPTER 7

## Provisioning

This chapter shows you how to use the **Provisioning** screens to apply templates.

### 7.1 Provisioning Overview

After you have created an IGMP filter profile (or template) in the Template screens, you can use the Provisioning screens to apply or delete IGMP filter profiles to or from a device.

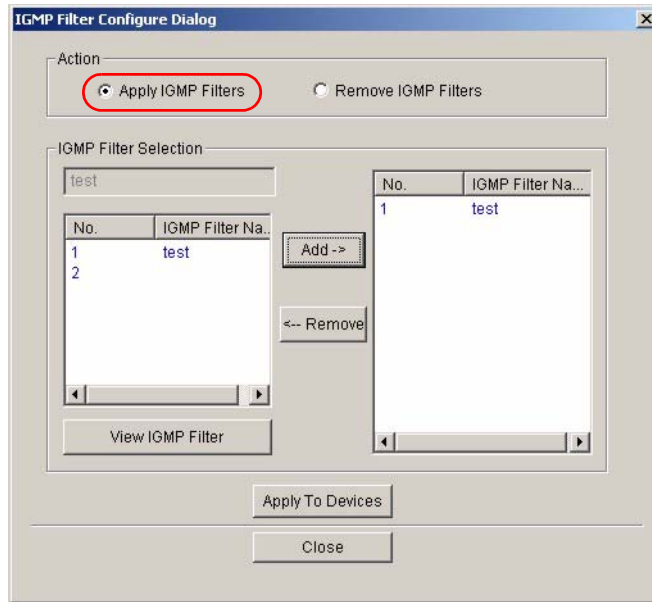
**Note:** You must first create IGMP filtering templates before you can apply them using the Provisioning screen. Refer to the chapter on creating templates for more information.

### 7.2 Applying an IGMP Filter Profile

Follow the steps below to apply an IGMP filter to a device.

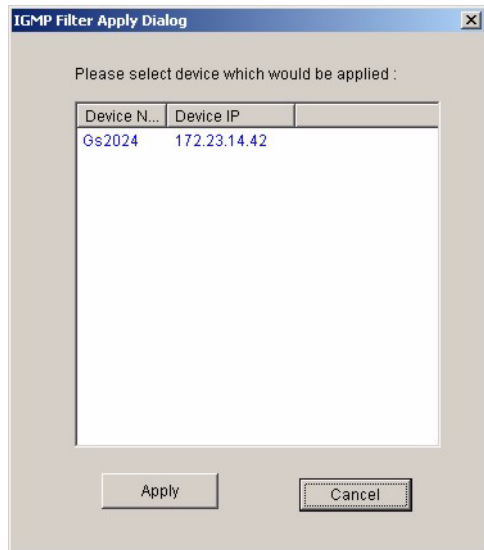
- 1** Click **Provisioning** and **IGMP Filter Provisioning** to display the screen as shown.
- 2** Select **Apply IGMP Filters** under **Action**.
- 3** Select a profile you want to use on the left and click **Add**. You can view the profile settings by clicking **View IGMP Filter**. Refer to the chapter on IGMP filter template settings for field descriptions.

**Figure 35** Provisioning: IGMP Filter



- 4 Click **Apply To Devices** to apply the selected IGMP filter profile(s).
- 5 A screen displays as shown. Select the device(s) to which you want to apply the IGMP filter(s). To select more than one device, press [SHIFT] or [CTRL] and select at the same time.

**Figure 36** Provisioning: IGMP Filter: Apply to Devices



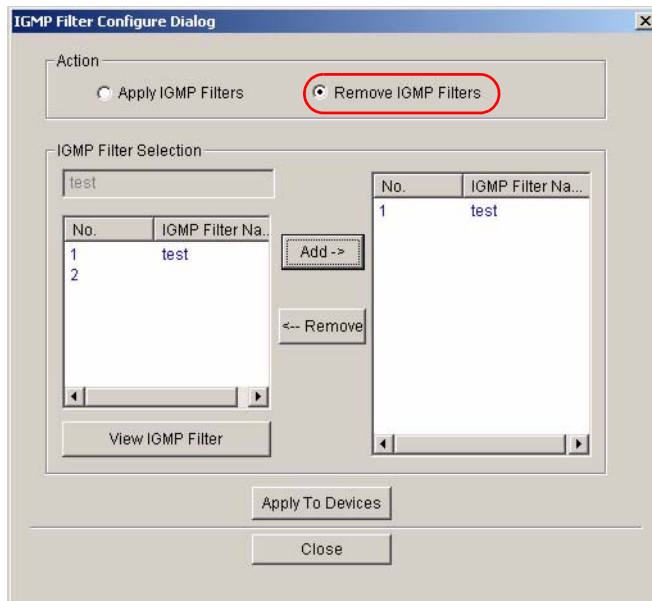
- 6 Click **Apply** to copy the IGMP filter profile settings to the selected device(s).
- 7 A screen displays showing the profile copy status. Click **OK** to close this screen.

**Figure 37** Provisioning: IGMP Filter: Apply to Devices: Successful

## 7.3 Removing an IGMP Filter Profile

Follow the steps below to remove an IGMP filter from a device.

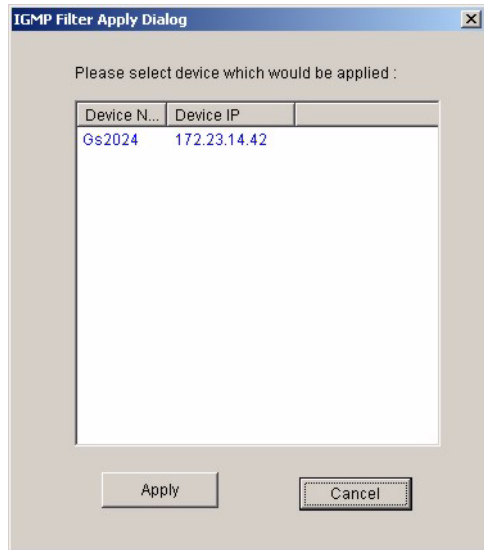
- 1 Click **Provisioning** and **IGMP Filter Provision** to display the screen as shown.
- 2 Select **Remove IGMP Filters** under **Action**.
- 3 Select a profile you want to remove and click **Add**. You can view the profile settings by clicking **View IGMP Filter**. Refer to the chapter on IGMP filter template settings for field

**Figure 38** Provisioning: IGMP Filter: Remove From Devices

- 4 Click **Apply To Devices**.
- 5 A screen displays as shown. Select the device(s) from which you want to remove the IGMP filter(s). To select more than one device, press [SHIFT] or [CTRL] and select at the same time.



**Figure 39** Provisioning: IGMP Filter: Remove From Devices: Select Device



- 6** Click **OK** to remove the IGMP filter profile settings from the selected device(s).
- 7** A **Result** screen displays showing the profile removal status. Click **Close** to close this screen.

**Figure 40** Provisioning: IGMP Filter: Remove From Devices: Successful



# CHAPTER 8

## Performance

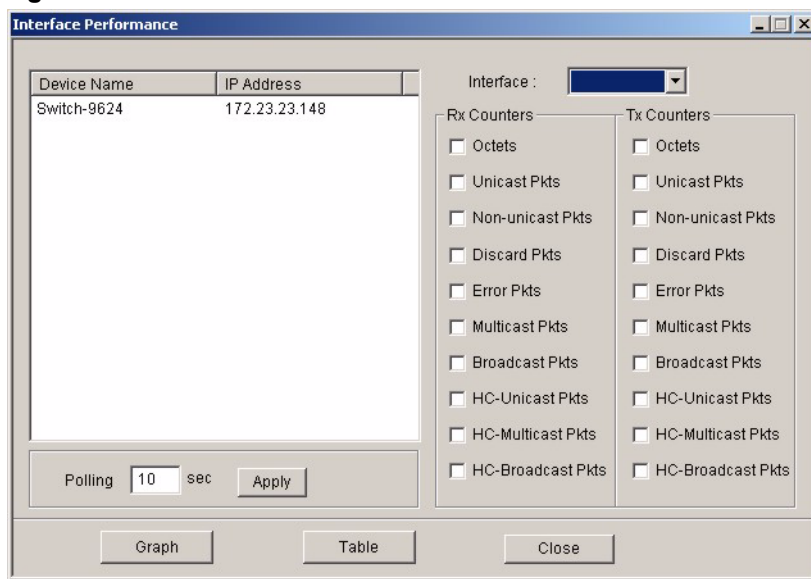
This chapter describes the interface performance screen, graph setup and table setup. View Ethernet history statistics for your switch network.

### 8.1 Interface Performance

This section shows you how to configure what you want to display in a performance table or graph.

Click **Performance** and then **Interface** in the EMS main menu.

**Figure 41** Performance: Interface



The following table describes the labels in this screen.

**Table 30** Performance: Interface

LABEL	DESCRIPTION
Interface	Select an interface (or port) from the drop-down list box.
Rx Counters	The following fields display the types of packet counters received on this interface.
Tx Counters	This following fields display the types of packet counters transmitted on this interface.
Octets	Select this option to show the total number of octets received or transmitted.
Unicast Pkts	Select this option to show the total number of good unicast packets received or transmitted that were dropped.

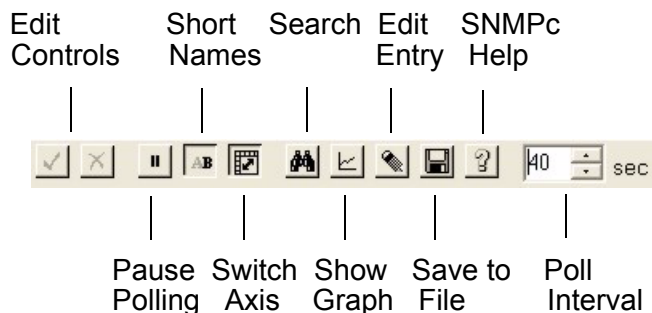
**Table 30** Performance: Interface (continued)

LABEL	DESCRIPTION
Non-unicast Pkts	Select this option to show the total number of good non-unicast packets received or transmitted that were dropped.
Discard Pkts	Select this option to show the total number of packets received or transmitted that were dropped.
Error Pkts	Select this option to show the total number of error packets received or transmitted.
Multicast Pkts	Select this option to show the total number of good multicast packets received or transmitted.
Broadcast Pkts	Select this option to show the total number of good broadcast packets received or transmitted.
HC-Unicast Pkts	Select this option to show the number of unicast packets (High Capacity (HC) 64 ~ 1518 octets long) dropped because they either had a bad Frame Check Sequence (FCS) or non-integer number of octets (alignment error).
HC-Multicast Pkts	Select this option to show the number of multicast packets (High Capacity (HC) 64 ~ 1518 octets long) dropped because they either had a bad Frame Check Sequence (FCS) or non-integer number of octets (alignment error).
HC-Broadcast Pkts	Select this option to show the number of broadcast packets (High Capacity (HC) 64 ~ 1518 octets long) dropped because they either had a bad Frame Check Sequence (FCS) or non-integer number of octets (alignment error).
Graph	Click the <b>Graph</b> button to create a graph based on the above selections.
Table	Click the <b>Table</b> button to create a table based on the above selections.
Close	Click <b>Close</b> to close the screen.

## 8.2 Table Menu Bar Icons


The following figure displays the table menu bar icons. These icons are common to all screens that display information in tabular format.

**Figure 42** Table Menu Bar Icons

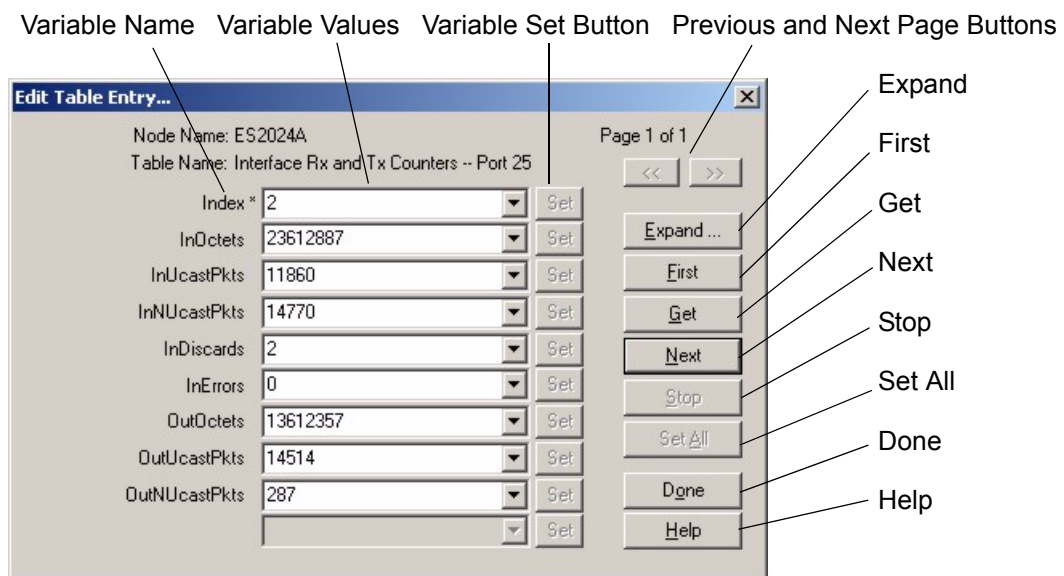


## 8.2.1 Editing a Table Entry

**Note:** You can edit a table entry in all screens that display information in tabular format.

In any tabulated screen display, click the **Edit** icon  in the menu bar icon to display the **Edit Table Entry** screen and edit any field in a table. There is a set of variable names, value and set button controls that operate on the fields of the selected table. There is also a set of function control buttons on the right. For tables that have more than ten entries, the **Edit Table Entry** screen supports multiple pages.

**Figure 43** Edit Table Entry



The following table describes the labels in this screen.

**Table 31** Edit Table Entry

COMMAND	DESCRIPTION
Variable Names	The first vertical column contains the variable names; these are the names of fields in the selected table. These names are set by SNMPc and cannot be changed. Some tables have variable names with an asterisk to the right of the name. These variables are used as indices into the table. All index variables must be specified to perform a Set operation.
Variable Values	The second vertical column contains the variable values in pull down list boxes. You can change the value by typing into the pull down edit box. If the variable has integer aliases defined in the MIB, you can select an alias by clicking on the down arrow and selecting an item from the drop down list. You must enter the variable value in the proper format. Use the expand button (see next section) to view the variable type.
Variable Set Button	Each variable value has a small Set button to the right. Click this <b>Set</b> button to perform an SNMP set on only one variable. Set buttons are grayed for variables that are read-only.

**Table 31** Edit Table Entry (continued)

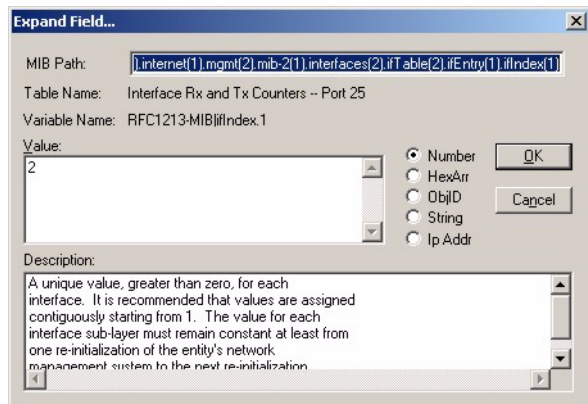
COMMAND	DESCRIPTION
Previous/Next Page Buttons	Each page shows up to ten variables. The page number and total number of pages are displayed in the top right corner. Use the >> button to move to the next page and click the << button to move to the previous page.
Expand	Click the <b>Expand</b> button to expand the view of the active variable value edit box. First click on the edit box, then select the <b>Expand</b> button.
First	Click the <b>First</b> button to obtain the first entry of the table from the node. The variable values will be updated. You do not need to enter index values - they will be ignored.
Get	Click the <b>Get</b> button to obtain the selected table entry. Enter all of the index values to select a table entry. If you have already displayed an entry, and perhaps modified the value boxes, you can Click the <b>Get</b> button to refresh the variable values.
Next	Click the <b>Next</b> button to obtain the next entry of the table from the node, using an SNMP GetNext operation. The variable values are updated. If there are no more entries in the table, a message is displayed. You can specify a starting point for the GetNext by entering index values. You do not need to enter all index values, but if you enter the Nth index value, you must also enter the 1st through (N-1)th index values.
Stop	Click the <b>Stop</b> button to abort the current SNMP operation. This button can be used to stop a command when a node is not responding and you don't want to wait for the timeout period.
Set All	Click the <b>Set All</b> button to set all writable variable values to the node. You must enter all of the index values (those with an asterisk to the right of the variable name) to select the table entry. If you do not know the proper index values, you can first find the entry you want to change by using the First and Get, Next buttons. Some nodes do not allow set operations to all variables that are defined as writable in the MIB. For these nodes, you will have to individually set table entry variables using the variable Set buttons.
Done	Click this button when you're done editing this dialog box.
Help	Click this button for online help.

**Note:** You can only use the variable Set button (via the EMS) to update system contact, system name, system location and the administrative status of each port.

## 8.2.2 Expand Dialog Box

In the **Edit Table Entry** screen click the **Expand** button to expand the view of the active variable value edit box. First click on the edit box, then click **Expand**.

**Figure 44** Expand Field



The **Expand** screen shows the variable value in a larger edit box, so you can more easily enter a long value. It also shows the variable type and a description from the MIB source file. Possible variable types are shown in the following table.

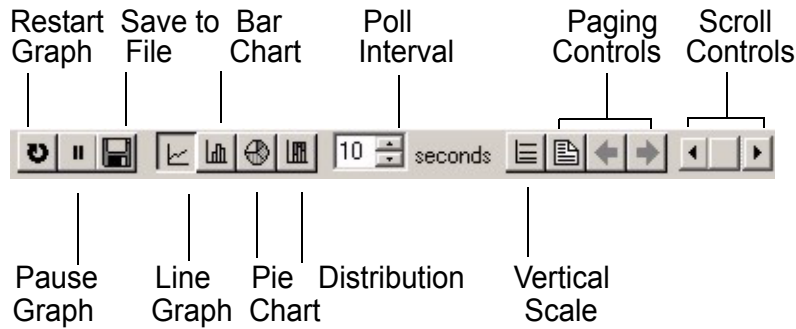
**Table 32** Variable Types

TYPE	DESCRIPTION
Number	This can be an INTEGER, COUNTER, GAUGE or Time Ticks. Data is normally represented as a decimal number. However, in cases where INTEGER aliases are defined in the MIB, an ASCII word will be displayed. For example, the value for ifOperStatus is displayed as UP or DOWN.
HexArr	OCTET PRIM TYPE. Data is formatted as a list of two digit hexadecimal numbers, representing one byte each, and separated by a single space, for example 22 3E 44 A1 10.
ObjID	OBJECT IDENTIFIER. Data is formatted in MIB dot format, optionally with a leading text identifier, for example sysObjectID.0 or 1.3.6.1.2.1.1.2.0.
String	This is OCTET PRIM TYPE with printable (ASCII string) data (DisplayString).
IP Addr	IP ADDRESS PRIM TYPE in dotted decimal notation, for example, 128.9.118.0.

### 8.3 Graph Menu Bar Icons

These graphical menu bar icons are common to all screens that display information in graphical format.

**Figure 45** Graph Menu Bar



### 8.3.1 Graph Styles

Use one of the style buttons to change the graph style to one of the following:

**Table 33** Edit Table Entry

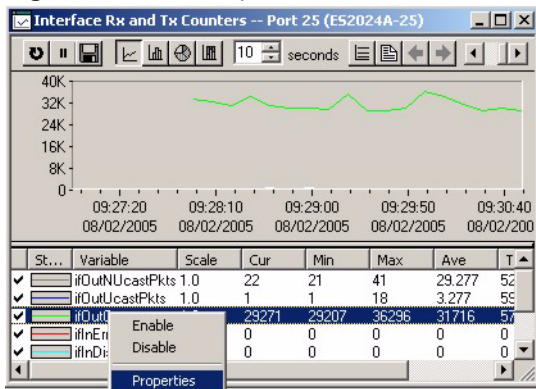
STYLE	DESCRIPTION
Line	Each variable is displayed as a line, with time as the horizontal axis. The vertical axis represents the size of each polled value for each poll interval.
Bar	The cumulative average value for each variable is displayed as a vertical bar.
Pie	All variables are displayed as relative sized portions of a pie diagram. The entire display represents a single poll interval.
Distribution	Each variable is displayed as a stacked vertical bar. Each segment of the bar represents the amount of time that the variable value is within a certain range (as a percent). The legend on the right side of the display shows the corresponding range for each color. The entire display represents a single poll interval.

### 8.3.2 Chart Format Display Variable

Choose which variables to display in chart format by doing one of the following:

- 1 Click a variable cell in a table and click the bar chart icon.
- 2 Display the chart menu and then deselect variables (all are displayed by default).
- 3 Right-click a variable's cell and select **Properties**.

**Figure 46** Cell Properties Select



4 A display properties dialog box opens. Select the **Display** check box.

**Figure 47** Chart Color Codes and Line Styles



You may also edit the color code and line style for a variable in the dialog box as described in the following table.

**Table 34** Edit Style Dialog Box

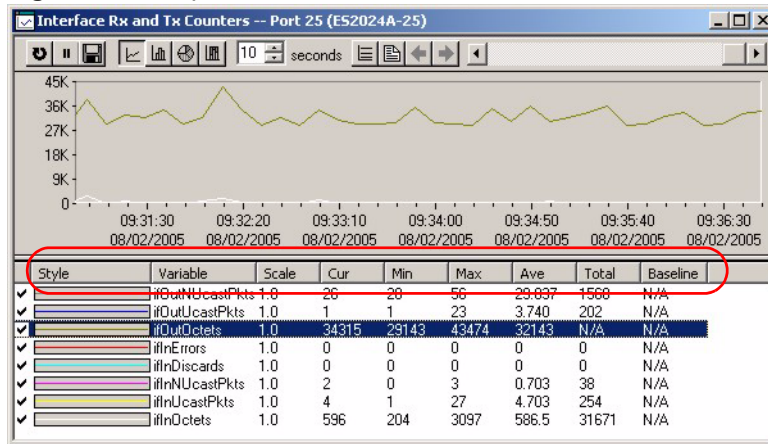
FIELD	DESCRIPTION
Display	Check Display to view information about this variable in chart format.
Color	Choose a color from this drop down list.
Style	Choose a line style from this drop down list.
Scale	Select the scaling multiplier from this drop down list. This factor is applied to each value in the line before it is displayed and can be used to keep all graph lines within a similar range of values. The range is from 0.0001 to 1000.0.

### 8.3.3 Graph Labels

In the **Interface** screen click the **Graph** button to display the following screen.



**Figure 48** Graph Variables



The following table describes the labels in this screen.

**Table 35** Graph Variables

LABEL	DESCRIPTION
Style	This is the line style discussed above.
Variable	This is the variable being represented by the line style discussed above.
Scale	This is the scaling multiplier.
Cur	This is the current value of the variable.
Min	This is the minimum value of the variable.
Max	This is the maximum value of the variable.
Ave	This is the average value of the variable.
Total	This is the total value of the variable.
Baseline	This is a measure of the typical variable behavior. After a learning period has transpired, SNMPc can automatically generate baseline alarms when variable values exceed the baseline.

# CHAPTER 9

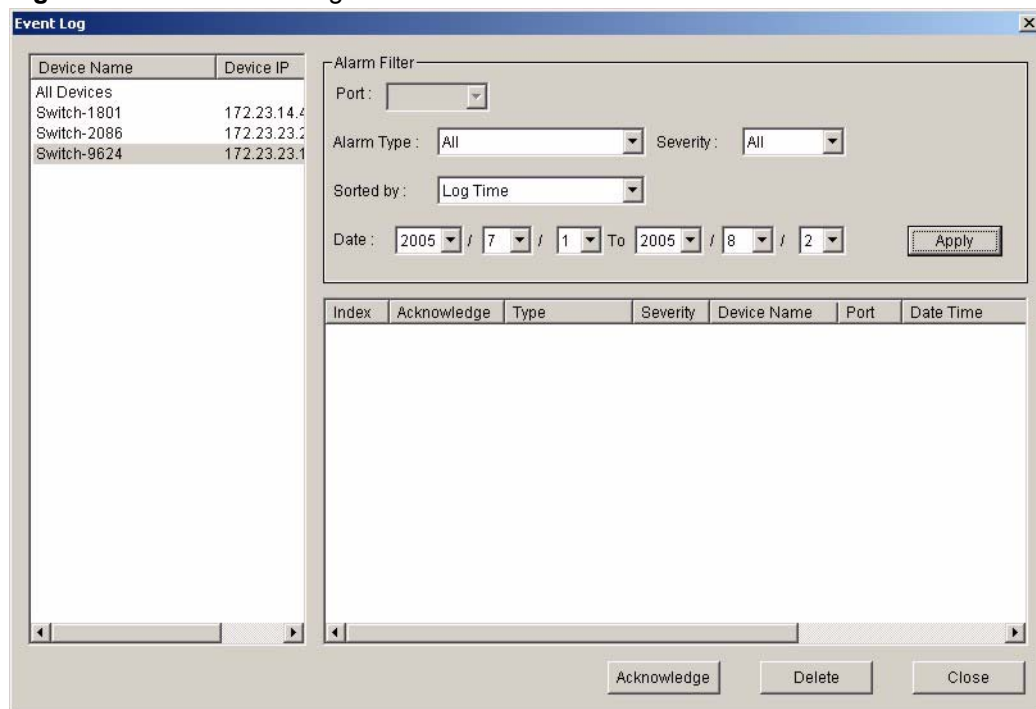
## Fault

This chapter describes the event logs and how to perform loopback tests using the Fault screens.

### 9.1 Event Log

To display system event logs click **Fault** and then **Event Log** to view the following screen.

**Figure 49** Fault: Event Log



The following table describes the labels in this screen.

**Table 36** Fault: Event Log

LABEL	DESCRIPTION
Alarm Filter	
Port	To display event logs of a port, select the port from the drop-down list box.

**Table 36** Fault: Event Log (continued)

LABEL	DESCRIPTION
Alarm Type	<p>Select the type of logs from the drop-down list box. Choices are <b>All</b>, <b>Communication</b>, <b>QualityOfService</b>, <b>ProcessingError</b>, <b>Equipment</b> and <b>Environmental</b>.</p> <p>Select <b>All</b> for system event logs generated by all alarm types.</p> <p>Select <b>Communication</b> for transmission and signal logs.</p> <p>Select <b>QualityOfService</b> for performance logs.</p> <p>Select <b>Processing Error</b> for software and configuration problem logs.</p> <p>Select <b>Equipment</b> for hardware-related logs.</p> <p>Select <b>Environmental</b> for environmental logs.</p> <p>See the appendix for a more detailed list of possible alarm causes.</p>
Severity	<p>Select the severity level of the logs you want to display from the drop-down list box. The choices and associated colors are as follows:</p> <ul style="list-style-type: none"> <li>• Critical - Red</li> <li>• Major - Orange</li> <li>• Minor - Yellow</li> <li>• Information - Blue</li> <li>• Normal - Green</li> </ul>
Sorted by	<p>Select <b>Log Time</b> to sort event logs by the time at which they were generated or select <b>Device Name</b> to sort event logs by the device from which they were generated.</p>
Date / To	<p>Specify the time range to display the event logs.</p>
Apply	<p>Click <b>Apply</b> to display event logs generated within the specified time period.</p>
Alarm	
Index	<p>This field displays the index number of the event logs.</p>
Acknowledge	<p>This field displays whether a log has been acknowledged so that EMS users will know when a log has been dealt with by an administrator.</p>
Type	<p>This field displays the type of the event log.</p>
Severity	<p>This field displays the severity of the event log.</p>
Device Name	<p>This field displays the name of the device on which the event log was generated.</p>
Port	<p>This field displays the port number on which the event log was generated.</p>
Date Time	<p>This field displays the date and time when the event log was generated.</p>
Description	<p>This field displays some information about the event log.</p>
Acknowledge	<p>Click <b>Acknowledge</b> to acknowledge any selected log messages.</p>
Delete	<p>Click <b>Delete</b> to remove the selected log.</p>
Close	<p>Click <b>Close</b> to close this screen.</p>

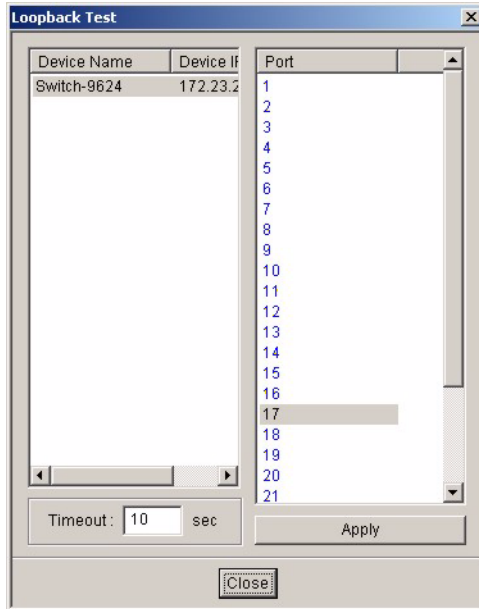
## 9.2 Loopback Test

Follow the steps below to perform an internal loopback test.

- 1 Click **Fault** and then **Loopback Test**.
- 2 Choose a switch from the list located on the left-hand side of the screen.

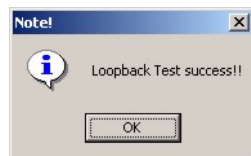
- 3 Choose a port from the list located on the right-hand side of the screen.
- 4 In the Timeout field, accept the default or specify a connection timeout period (in seconds).
- 5 Click **Apply** to start the loopback test.

**Figure 50** Fault: Loopback Test



- 6 A screen displays showing the test result. Click **OK** to close the screen.

**Figure 51** fault: Loopback: Result





# CHAPTER 10

## Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

### 10.1 Firmware Upgrade

You must be logged in with system administrator rights to use this function.

**Note:** Do NOT turn off the switch during the updating process, as it may corrupt the firmware and make the selected switch unusable.

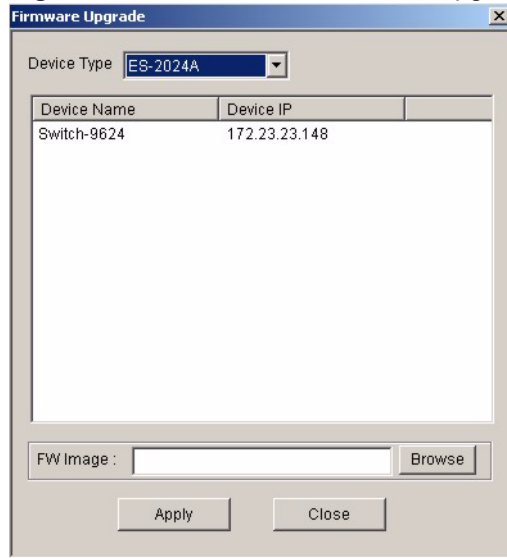
#### 10.1.1 Procedure to Update Firmware

You can perform firmware upgrade on all switches of the same type simultaneously on the EMS. To update firmware, first download the latest firmware, then unzip and store it on your computer. You can use this EMS FTP client to connect to a selected switch.

**Note:** Do NOT turn off the switch during the updating process, as it may corrupt the firmware and make your switch unusable.

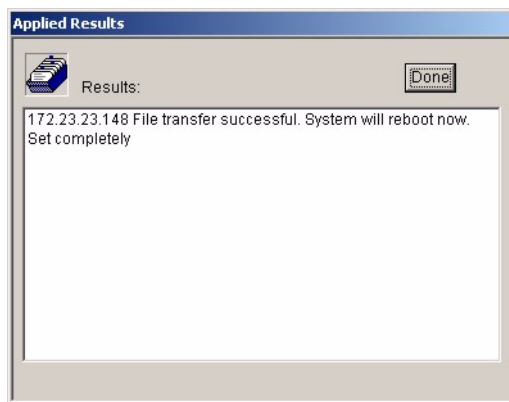
- 1 Click **Maintenance** and then **Firmware Upgrade**.
- 2 Select a device type from the **Device Type** drop-down list box.
- 3 The list displays the switches of the selected type. Select a switch or multiple switches on which you want to upgrade the firmware.
- 4 Type the path and file name of the firmware file you wish to upload to the switch in the **FW Image** text box or click **Browse** to locate it. After you have specified the file, click **Apply**.

**Figure 52** Maintenance: Firmware Upgrade



- 5 After the file transfer is complete, a screen displays showing the result. Click **Done** to close the screen. When the firmware upgrade process is complete, the switch(es) automatically restarts (the **SYS LED** blinks).

**Figure 53** Maintenance: Firmware Upgrade: Result

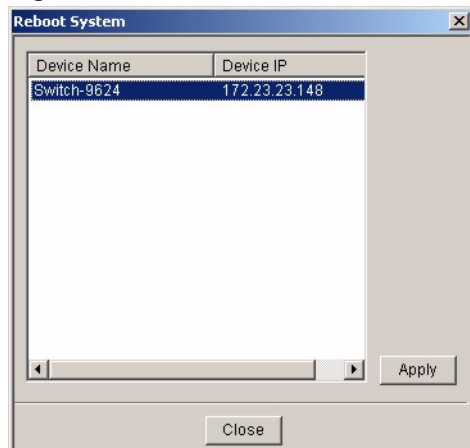


- 6 Wait until the switch(es) has finished rebooting before accessing it again. Check the firmware version on the switch to make sure that the firmware is updated successfully.

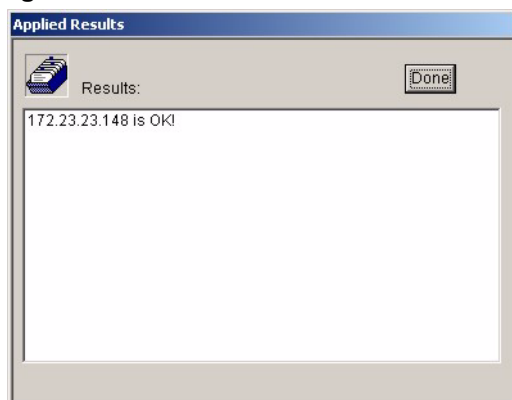
## 10.2 Device Reset

Use the **Reboot System** screen to restart a switch without physically turning the power off.

- 1 Click **Maintenance, Device Reset** to display the screen as shown.
- 2 Select a device from the list and click **Apply**.

**Figure 54** Maintenance: Device Reset

- 3 A screen displays. Click **Done**. The switch will restart. This takes up to two minutes. This does NOT affect the switch's configuration.

**Figure 55** Maintenance: Device Reset: Result

## 10.3 Network Element Configuration Backup and Restore

A Network Element (NE) is a network device that provides support or services to the user.

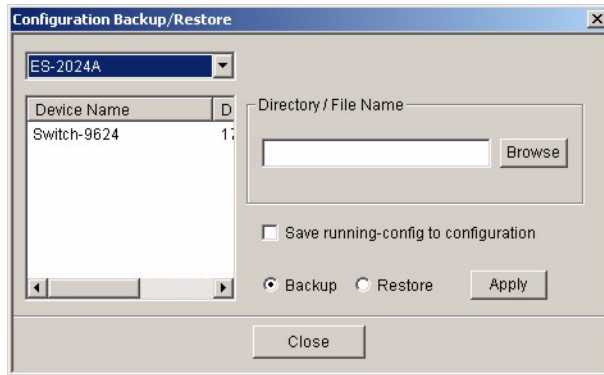
Follow the steps below to backup or restore a switch configuration file to your computer.

- 1 Click **Maintenance** and then **NE Configuration Backup and Restore**.
- 2 Select a device type from the drop-down list box and select a switch in the list box.
- 3 Under **Directory/File Name**, type the path and file name of the file you wish to restore to the switch or backup to your computer in the text box provided or click **Browse** to locate it.
- 4 Select the **Save running config to configuration** check box to save the current switch configuration if you want to back up to your computer.
- 5 Select **Backup** to save the configuration to your computer. Or select **Restore** to restore the configuration file back to the switch.



- 6 Click **Apply**.
- 7 If you chose **Restore**, the switch automatically restarts when the configuration file upload is complete.
- 8 Click **Close** to close this screen.

**Figure 56** Maintenance: Configuration Backup/Restore



The following table describes the labels in this screen.

**Table 37** Maintenance: Configuration Backup/Restore

LABEL	DESCRIPTION
Directory/File Name	Type the path and file name of the configuration file you wish to restore to the switch or backup to your computer in the <b>Directory / File Name</b> text box or click <b>Browse</b> to locate it.
Save running-config to configuration	Select the <b>Save running-config to configuration</b> text box to save the most recently updated configuration to a file specified in the <b>Directory/File Name</b> field.
Backup	Click the <b>Backup</b> radio button to transfer the configuration file from your switch to a computer.
Restore	Click the <b>Restore</b> radio button to transfer the configuration file from your computer to a switch.
Apply	Click <b>Apply</b> to backup or restore the switch(es) configuration file.
Close	Click <b>Close</b> to close this screen.

## 10.4 Load Factory Default

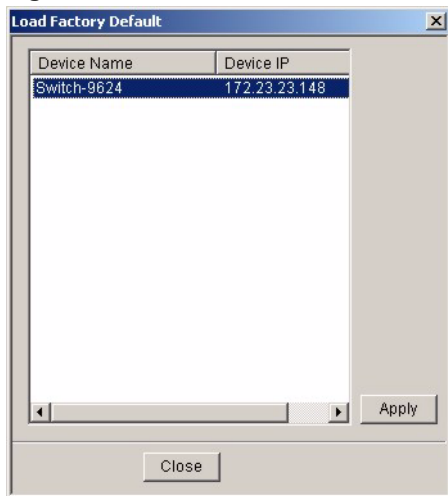
Follow the steps below to reset a switch configuration to the factory defaults.

- 1 Click **Maintenance** and then **Load Factory Default**.
- 2 Select a switch from the list of devices shown.
- 3 Click **Apply** to clear all configuration information and return the switch to the factory defaults.

This takes up to two minutes. If you want to access the switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address.

- 4 Click **Close** to close this screen.

**Figure 57** Maintenance: Load Factory Defaults



## 10.5 Scheduled Network Element Configuration Backup

Perform configuration backups according to a schedule. Set the frequency, time and date of the backup and the location where you want to backup the configuration file.

**Figure 58** Maintenance: Scheduled NE Config Backup



The following table describes the labels in this screen.

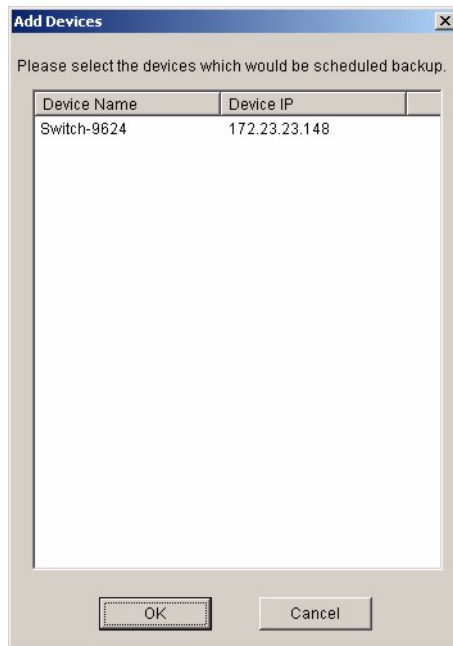
**Table 38** Maintenance: Scheduled NE Config Backup

LABEL	DESCRIPTION
Backup Schedule	
Frequency	Scheduled backups can be performed on a <b>Daily</b> , <b>Weekly</b> or <b>Monthly</b> basis. Select a radio button to schedule configuration backups starting at the date and time specified below. The default setting is <b>No Backup</b> .
Starting date	Specify the starting date to begin a configuration file backup for the selected device(s). Select a date from the drop-down list box.
Starting time	Specify the starting time to begin a configuration file backup for the selected device(s). Select a time from the selection box or enter a time (hh:mm:ss AM/PM format).
Backup Directory	Type the path and file name of the configuration file you wish to backup to your computer in the <b>Backup Directory</b> text box or click <b>Browse</b> to locate it.
User info for Windows	To perform scheduled backups, you need to specify your Windows administrator account information. This allows the EMS to add a scheduled task in Windows.
Account	This read-only field displays the Windows login account user.
Password	Enter a password in this field for the administrator <b>Account</b> above.
Add	Click the <b>Add</b> button to add a switch to the list of devices in the backup schedule.
Remove	Click the <b>Remove</b> button to remove a switch from the list of devices in the backup schedule.
Apply	Click <b>Apply</b> to save changes to the EMS.
Close	Click <b>Close</b> to close this screen.

### 10.5.1 Scheduled Network Element Configuration Backup Add

Follow the steps below to add a device to the list of devices in the **Scheduled NE Configuration Backup** screen.

- 1 Click the **Add** button in the **Scheduled NE Config Backup** screen.
- 2 Click the **OK** button.

**Figure 59** Maintenance: Scheduled NE Config Backup Add

## 10.5.2 Scheduled Network Element Configuration Backup Remove

To remove a device from the **Scheduled NE Configuration Backup** screen, click the **Remove** button in the **Scheduled NE Config Backup** screen.



# CHAPTER 11

## Tools

This chapter shows you how to access a switch via Telnet or web configurator directly through the EMS. You may need to do this to test the switch network connection for example.

### 11.1 Accessing the Switch

Access the switch remotely via Telnet or web browser.

**Note:** When you access a switch via Telnet or the web configurator, you CANNOT make any changes to that switch using the EMS.

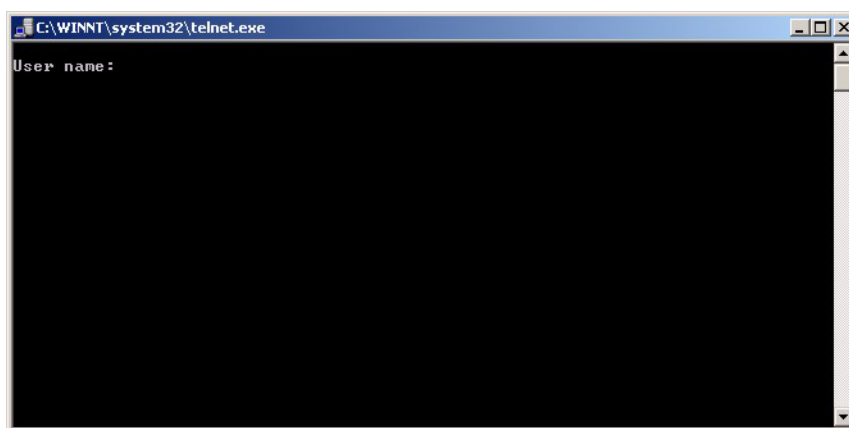
#### 11.1.1 Telnet

Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

The administrator uses Telnet from a computer on a remote network to access the switch. You can use remote Telnet access as shown next.

- 1 Select a switch from the list of devices shown in the Device List Panel.
- 2 Click **Tool** and then **Telnet** to open a console session for Telnet access to the switch.
- 3 Type the switch user name and password to access the switch command line prompt.

**Figure 60** Telnet



- 4 Refer to the switch User's Guide for information on the commands used in this screen.

## 11.1.2 Web Access

Configure the switch using the web configurator as shown.

- 1 Select a switch from the list of devices shown in the Device List Panel.
- 2 Click **Tool** and then **Web Access** to open the switch web configurator password screen. From here you can log in directly to the switch.
- 3 Type the switch **User name** and **Password** to access the web configurator.

**Figure 61** Web Access



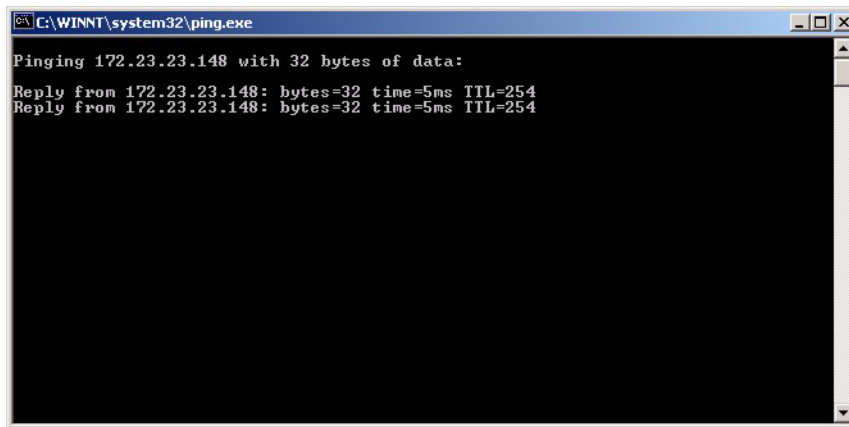
- 4 Refer to the switch User's Guide for information on the web configurator main screen.

## 11.2 Ping

Ping the host to see if the links and TCP/IP protocol on both your computer and the switch is working. Follow the steps below:

- 1 Select a switch from the list of devices shown in the Device List Panel.
- 2 Click **Tool** and then **Ping** to have the computer ping the IP address of the selected device.
- 3 The Command Prompt window automatically closes after the computer pings the selected switch three times.

**Note:** The device IP address varies according to whether the switch is connected to the EMS computer using an in-band or an out-of-band IP address.

**Figure 62** Ping

```
C:\WINNT\system32\ping.exe
Pinging 172.23.23.148 with 32 bytes of data:
Reply from 172.23.23.148: bytes=32 time=5ms TTL=254
Reply from 172.23.23.148: bytes=32 time=5ms TTL=254
```





# CHAPTER 12

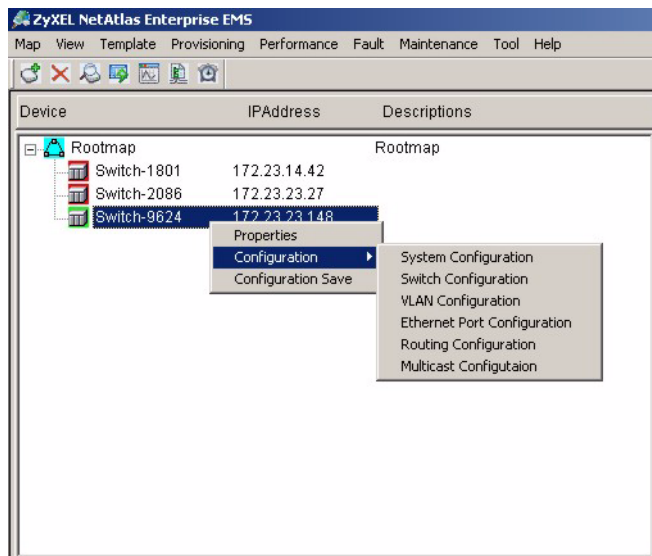
## Device Menu Overview

This chapter introduces the device configuration menus.

### 12.1 Device Menu Summary

To select a device configuration menu, right-click on a device in the Device List Panel.

**Figure 63** Device Panel List Menus



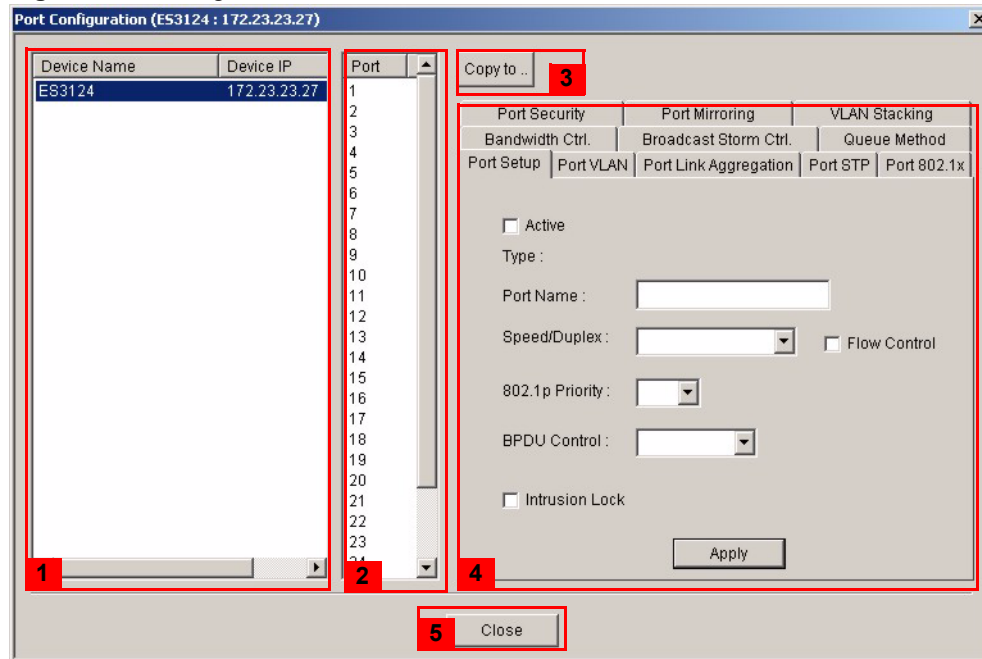
### 12.2 Property Configuration

See [Section 4.1.2 on page 45](#) for information on the **Edit Device** screen.

### 12.3 Introducing the Device Configuration Window

The following example screen displays the main features used to configure EMS-managed devices. See the individual screen selections for details on switch feature configuration.

**Figure 64** Configuration Window



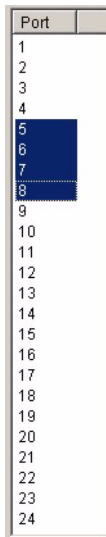
The following table describes the elements in this screen.

**Table 39** Configuration Window

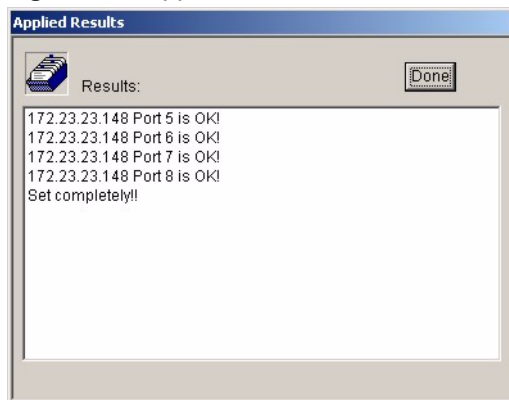
	LABEL	DESCRIPTION
1	Device Panel	This panel displays all active devices (of the same type) currently managed by the EMS.
2	Port List Panel	This field displays a list of switch ports. This list displays in the Ethernet Port Configuration screens only. To make configuration changes to each port or ports, select a port number or multiple port numbers (by pressing the [CTRL] key and clicking at the same time) in the Port List Panel.
3	Copy to..	Click the <b>Copy to..</b> button to copy the configuration from the switch that you are currently configuring to the port(s) on the same switch or other switch(es). Port configurations can also be copied to other device ports in the Ethernet Port Configuration screens.
4	Configuration Panel	Use this panel to make configuration changes to a device based on a port or multiple ports selected in the Port List Panel. If the screen does not have a Port List Panel, then use this panel to make configuration changes to a device selected in the Device Panel. Click <b>Apply</b> to save configuration changes.
5	Close	Click <b>Close</b> to close a configuration screen. If you close a screen without first clicking <b>Apply</b> , configuration changes will not be saved.

### 12.3.1 Port List Multiple Port Configuration

Configure more than one port at the same time by pressing the [CTRL] key and clicking at the same time in the Port List Panel.

**Figure 65** Configuration Window: Port List: Multiple Port Select

Click **Apply** when you are satisfied with the configuration changes. A screen displays showing the configuration result.

**Figure 66** Applied Results

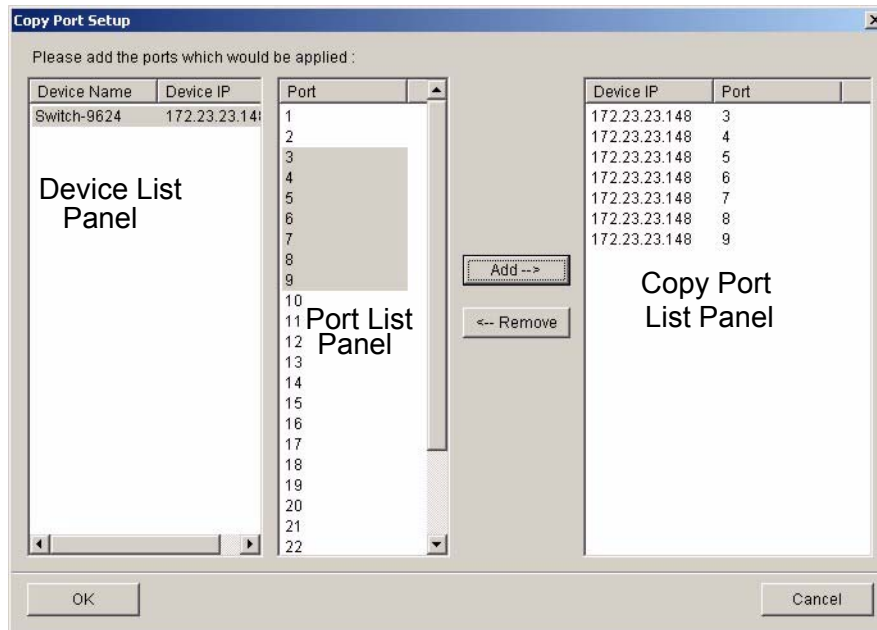
**4** Click **Done** to close the screen.

### 12.3.2 The Copy to.. Button

The **Copy to..** button allows you to copy the configuration from the switch you are currently configuring to one or more switches.

- 1** In the Device Panel list, select a device that you want configure.
- 2** Select a tab in the Configuration Panel.
- 3** Select a port or multiple ports (by pressing the [CTRL] key and clicking at the same time) from the Port List Panel.
- 4** Make your configuration changes in the Configuration Panel and click the **Apply** button.
- 5** Click the **Copy to..** button. The following screen displays.

**Figure 67** Copy Port Setup: Example

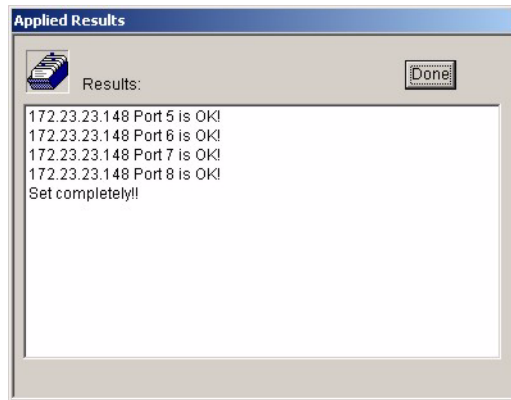


The following table describes this screen.

**Table 40** Copy Port Setup

LABEL	DESCRIPTION
Device List	Select a device to which you want to copy from the switch you are currently configuring.
Port List Panel	Select one port or multiple ports (by pressing the [CTRL] key and clicking at the same time) from the Port List Panel.
Add	Click <b>Add</b> to display the port(s) to which you want to copy from the switch you are currently configuring.
Remove	Click <b>Remove</b> to move a selected port(s) from the Copy Port List Panel list to the Port List Panel.
Copy Port List Panel	This panel displays the device port(s) to which you want to copy from the switch you are currently configuring.
OK	Click <b>OK</b> to copy the configuration from the current switch to the device port(s) displayed in the Copy Port List Panel.
Cancel	Click <b>Cancel</b> to return to the previous screen.

**6** Click **OK** to display the following screen.

**Figure 68** Copy Successful

**7** Click **Done** to close the screen.



# CHAPTER 13

## System Configuration

This chapter shows you how to view general system information, configure SNMP, remote management and time setup.

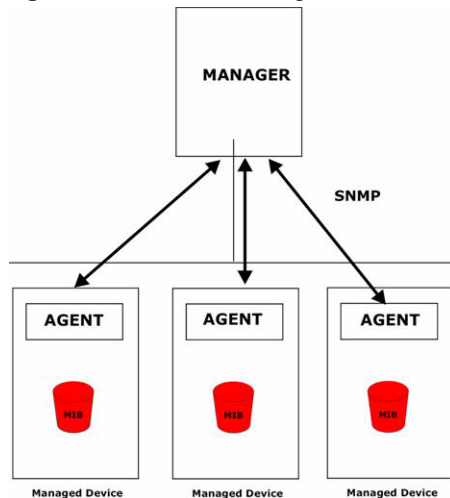
### 13.1 System Info

See [Section 3.9 on page 41](#) for information about the switch.

### 13.2 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the switch through the network via SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

**Figure 69** SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (your Ethernet switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.



The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

**Table 41** SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMP, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

See the switch User's Guide for a list of supported traps.

### 13.2.1 Configuring SNMP

Follow the steps below to configure SNMP.

- 1** In the Device Panel list, select a device and then right-click.
- 2** Click **Configuration**, **System Configuration** and then the **SNMP Conf.** tab.

**Figure 70** System Configuration: SNMP Conf.

The following table describes the labels in this screen.

**Table 42** System Configuration: SNMP Conf.

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click <b>Apply</b> to save the trap destination changes back to the switch.

## 13.3 Remote Management

Remote management allows you to determine which services/protocols can access which device interface (if any) from which computers. You can customize the service port and the secured client IP address to enhance security and flexibility.

Follow the steps below to configure remote management.

- 1** In the Device Panel list, select a device and then right-click.
- 2** Click **Configuration**, **System Configuration** and then the **Remote Mgmt.** tab.

**Figure 71** System Configuration: Remote Management

The following table describes the labels in this screen.

**Table 43** System Configuration: Remote Management

LABEL	DESCRIPTION
Services	This panel displays the services that you may use to remotely manage the switch. Select the check box(es) to allow remote management using the service(s).
Port	Enter the number of the server port to use with the corresponding service.
Apply	Click <b>Apply</b> to save the changes back to the switch.
Secured Clients	Select the check box(es) to enable the client set.
Start	To allow a range of computers to use Telnet, FTP, HTTP, ICMP, SSH or HTTPS services, enter the first IP address in the range here. The default value for a start and end address is 0.0.0.0, which means you don't care which host is trying to use a service (Telnet, FTP, HTTP, SNMP, ICMP, SSH or HTTPS). If you enter an IP address in this field, the switch will check if the client IP address matches the value here when a (Telnet, FTP, HTTP, SNMP, ICMP, SSH or HTTPS) session is up. If it does not match, the session is disconnected immediately.
End	To allow a range of computers to use Telnet, FTP, Web, SNMP or ICMP services, enter the <b>End</b> IP address in the range here. To allow a single computer to use Telnet, FTP, HTTP, SNMP, ICMP, SSH or HTTPS services, enter the same IP address here as in the <b>Start</b> field.
Telnet, FTP, HTTP, ICMP, SNMP, ICMP, SSH, HTTPS	Select the check box to allow the trusted computer(s) in the IP address range specified above to use this service to manage the switch.
Apply	Click <b>Apply</b> to save the changes back to the switch.
Close	Click <b>Close</b> to close the screen.

## 13.4 Time Setup

The switch keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you log in to the switch. Use the **Time Setup** screen to update the time and date settings in the EMS and then save the settings to the switch. The real time is then displayed in the system messages.

Follow the steps below to configure your system time.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, System Configuration** and then the **Time Setup** tab.

**Figure 72** System Configuration: Time Setup

The following table describes the labels in this screen.

**Table 44** System Configuration: Time Setup

LABEL	DESCRIPTION
Use Time Server When BootUp	Select the time service protocol that your time server sends when you start the switch. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. When you select the <b>Daytime (RFC 867)</b> format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. <b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. <b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b> . <b>None</b> is the default; enter the time manually.
Time Server IP Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date (yyyy:mm:dd)	Enter the new date in year, month and day format.

**Table 44** System Configuration: Time Setup (continued)

LABEL	DESCRIPTION
Time Zone	Select the time difference between your time zone and Universal Time Coordinate (UTC) formerly known as Greenwich Mean Time (GMT).
Apply	Click <b>Apply</b> to save the changes.

# CHAPTER 14

## Switch Configuration

This chapter shows how to configure priority queuing, STP, link aggregation, DHCP relay, GARP timer and RADIUS.

### 14.1 Switch Setup

Use the switch setup screen to set a VLAN type, a queuing method and enable or disable features in the **Active Control** panel.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Switch Configuration**. The **Switch Setup** screen displays. This screen varies depending on your switch models.

**Figure 73** Switch Configuration: Switch Setup (ES-2024A)

RADIUS	Filtering	MAC Forwarding	Mirroring	DSCP
Switch Setup	Priority Queue	STP Conf.	Link Aggregation	GARP Timer

VLAN Type :

MAC Address Aging Time :  seconds

Queuing Method  
Method :

Q0  Q1  Q2  Q3

Active Control

- STP Configuration
- Link Aggregation
- IGMP Snooping
- Bandwidth control
- Broadcast storm control
- Mirroring
- 802.1x
- Port Security
- GVRP
- 802.1q Ingress Check
- 802.1q Port Isolation
- DSCP

**Figure 74** Switch Configuration: Switch Setup (GS-2024)

RADIUS	MAC Forwarding	Mirroring	DSCP
Switch Setup	Priority Queue	STP Conf.	Link Aggregation
GARP Timer			

VLAN Type:

MAC Address Aging Time:  seconds

Queuing Method:

Q0:  Q1:  Q2:  Q3:

BroadCast Storm Control

Active:

Storm Control:

Packet Limit:

Active Control

- STP Configuration
- Link Aggregation
- Bandwidth control
- Mirroring
- 802.1x
- Port Security
- DSCP
- GVRP

**Figure 75** Switch Configuration: Switch Setup (ES-3124/ES-3124PWR)

GARP Timer	RADIUS	Filtering	Mac Forwarding	Mirroring
Switch Setup	Priority Queue	STP Conf.	Link Aggregation	DHCP Relay

VLAN Type:

Queuing Method:

MAC Address Aging Time:  seconds

Active Control

- STP Configuration
- Link Aggregation
- IGMP Snooping
- Bridge control protocol transparency
- Bandwidth control
- Broadcast storm control
- Mirroring
- 802.1x
- Port Security
- VLAN Stacking SP TPID:   Others  (Hex)
- GVRP
- 802.1q Port Isolation
- DHCP Relay

The following table describes the related labels in the screen.

**Table 45** Switch Configuration: Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose <b>802.1Q</b> or <b>Port Based</b> from the drop-down list box. The VLAN Setup screen changes depending on whether you choose <b>802.1Q</b> or <b>Port Based</b> VLAN type in this screen. See <a href="#">Section 16.3 on page 137</a> and the VLAN chapter for more information on VLANs.
MAC Address Aging Time	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active. Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
Queuing Method	Select a queuing method. Choices vary depending on your switch models. <b>Strict Priority Queuing (SPQ)</b> services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. The default queuing method is <b>Strictly Priority</b> . <b>Weighted Round Robin Scheduling (WRR)</b> services queues on a rotating basis based on their queue weight (the number you select from the drop-down list box for the corresponding queue). Queues with larger weights get more service than queues with smaller weights. <b>Weighted Fair Scheduling</b> is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the Weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights.
Broadcast Storm Control	These fields are not available on all switch models. Set the fields below to configure traffic storm control.
Active	Select <b>Active</b> to enable traffic storm control on the switch.
Storm Control	Specify the traffic type in this field. Select <b>Broadcast Only</b> , <b>Broadcast and multicast</b> , <b>Broadcast and unknown unicast</b> or <b>Broadcast, multicast and unknown unicast</b> from the drop-down list box.
Packet Limit	From the drop-down list box, select the number of packets (of the type chosen above) a port can receive per second.
Active Control	
STP Configuration	Select the check box to activate STP.
Link Aggregation	Select the check box to activate link aggregation.
IGMP Snooping	Select the check box to enable IGMP snooping.
Bridge control protocol transparency	Select the check box to enable bridge control protocol transparency.
Bandwidth control	Select the check box to activate bandwidth control.
Broadcast storm control	Select the check box to activate broadcast storm control.
Mirroring	Select the check box to activate port mirroring.
802.1x	Select the check box to activate IEEE 802.1x authentication.
Port Security	Select the check box to activate port security.



**Table 45** Switch Configuration: Switch Setup (continued)

LABEL	DESCRIPTION
VLAN Stacking	Select the check box to enable VLAN stacking. In the <b>SP TPID</b> drop-down list box, select a standard Ethernet type code to identify the frame and indicate whether the frame carries IEEE 802.1Q tag information. Or select <b>Others</b> and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the <b>Others</b> text field.
GVRP	Select the check box to permit VLANs groups beyond the local switch on this port. GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network.
802.1q Ingress Check	Select this check box to set the switch to discard incoming frames for VLANs that do not have this port as a member
802.1q Port Isolation	Port Isolation allows each port to communicate with the CPU port, uplink ports and stacking ports (if available) but not communicate with each other. This option is the most limiting but also the most secure.
DHCP Relay	Select the check box to enable DHCP relay.
DSCP	Select the check box to enable DSCP-IEEE 802.1q mapping.
Apply	Click <b>Apply</b> to save your changes back to the switch.

## 14.2 Priority Queue

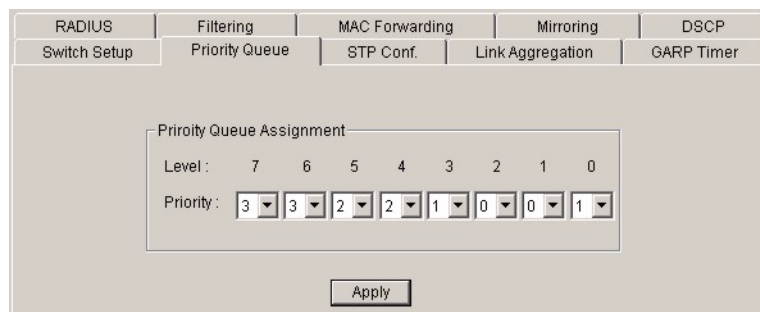
Queuing is used to help solve performance degradation when there is network congestion.

Configure queuing algorithms for outgoing traffic in the **Switch Setup** screen. Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

Follow the steps below to configure priority queuing.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration**, **Switch Configuration** and then click the **Priority Queue** tab to display the following screen.

**Figure 76** Switch Configuration: Priority Queue



The following table describes the labels in this screen.

**Table 46** Switch Configuration: Priority Queue

LABELS	DESCRIPTION
Priority Queue Assignment	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use these fields to configure the priority level-to-physical queue mapping. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.
Priority Level	The following descriptions are based on the traffic types defined in the IEEE 802.1D standard (which incorporates 802.1p). Select a level from the drop-down list box(es).
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click <b>Apply</b> to save your changes back to the switch.

## 14.3 STP Configuration

This section describes STP and how to configure STP.

The switch supports STP. STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a device to interact with other STP-aware devices in your network to ensure that only one path exists between any two stations on the network. Activate the STP feature in the **Switch Setup** screen.

Refer to the user's guide that comes with your switch for more information.

- 1 Right-click on a device in the Device Panel list.
- 2 Click **Configuration**, **Switch Configuration** and then the **STP Conf.** tab to display the following screen.

**Figure 77** Switch Configuration: STP Conf.

The following table describes the labels in this screen.

**Table 47** Switch Configuration: STP Conf.

LABEL	DESCRIPTION
Priority	Priority is used in determining the root device, root port and designated port. The device with the highest priority (lowest numeric value) becomes the RSTP root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. The allowed range is 0 to 65535 (32768 is the default). The lower the numeric value you assign, the higher the priority for this bridge. <b>Priority</b> determines the root bridge, which in turn determines <b>Hello Time</b> , <b>Max Age</b> and <b>Forward Delay</b> .
Max Age	This is the maximum time (in seconds) a device can wait without receiving a BPDU before attempting to reconfigure. All device ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The allowed range is 6 to 40 seconds (20 is the default).
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations (by all devices in RSTP or the root device in STP). The allowed range is 1 to 10 seconds (2 is the default).
Forward Delay	This is the maximum time (in seconds) a device will wait before changing states. This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds (15 is the default).
Apply	Click <b>Apply</b> to save your changes back to the switch.

## 14.4 Link Aggregation

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A link aggregation group is one logical link containing multiple ports.

The first port must be physically connected when forming a trunk group.

### 14.4.1 Dynamic Link Aggregation

This feature is not available on all models.

The switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The switch supports the link aggregation IEEE 802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention

Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

### 14.4.2 Link Aggregation ID

LACP aggregation ID consists of the following information:

**Table 48** Aggregation ID Local Switch

Local switch [(0000,00-00-00-00-00-00,0000,00,0000)]				
0000	00-00-00-00-00	0000	00	0000
System priority	MAC address	Key	Port Priority	Port Number

**Table 49** Aggregation ID Peer Switch

Peer switch [(0000,00-00-00-00-00-00,0000,00,0000)]				
0000	00-00-00-00-00	0000	00	0000
System priority	MAC address	Key	Port Priority	Port Number

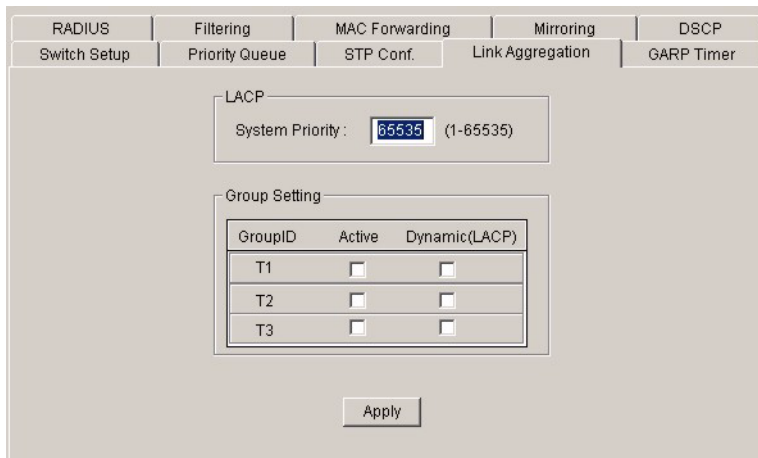
### 14.4.3 Configuring Link Aggregation

Activate link aggregation in the **Switch Setup** screen.

- 1 Right-click on a device in the Device Panel list.
- 2 Click **Configuration**, **Switch Configuration** and then the **Link Aggregation** tab to display the following screen.

**Note:** The number of link aggregation groups varies depending on your switch models.

**Figure 78** Switch Configuration: Link Aggregation



The following table describes the labels in this screen.

**Table 50** Switch Configuration: Link Aggregation

TABLE	DESCRIPTION
LACP	
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group Setting	
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports
Active	Select this option to activate a trunk group.
Dynamic (LACP)	Select this check box to enable LACP for a trunk.
Apply	Click <b>Apply</b> to save your changes.

### 14.4.4 DHCP Relay

This feature is not available on all switch models.

If there is an Ethernet device that performs the DHCP server function for your network, then you can configure the switch as a DHCP relay agent. When the switch receives a request from a computer on your network, it contacts the Ethernet device (the DHCP server) for the necessary IP information, and then relays the assigned information back to the computer.

## 14.4.5 DHCP Relay Agent Information

The switch can add information to client TCP/IP configuration requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the switch to add to the client TCP/IP configuration requests that it relays to the DHCP server. Please refer to RFC 3046 for more details.

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client TCP/IP configuration request frames that the switch relays to a DHCP server. The following lists the DHCP relay agent option 82 information that the switch sends to the DHCP server:

- Slot ID (1 byte)
- Port ID (1 byte)
- VLAN ID (2 bytes)
- System name (up to 32 bytes, this is optional)

Enable DHCP relay in the **Switch Setup** screen.

To configure DHCP relay, click **Configuration**, **Switch Configuration** and the **DHCP Relay** tab. A screen displays as shown.

**Figure 79** Switch Configuration: DHCP Relay

GARP Timer	RADIUS	Filtering	Mac Forwarding	Mirroring
Switch Setup	Priority Queue	STP Conf.	Link Aggregation	DHCP Relay

**DHCP Relay Service**

Relay Option82: Disable

Relay Option82 Info : ES-3124

**DHCP Server**

1	. . .
2	. . .
3	. . .

Apply

The following table describes the labels in this screen.

**Table 51** Switch Configuration: DHCP Relay

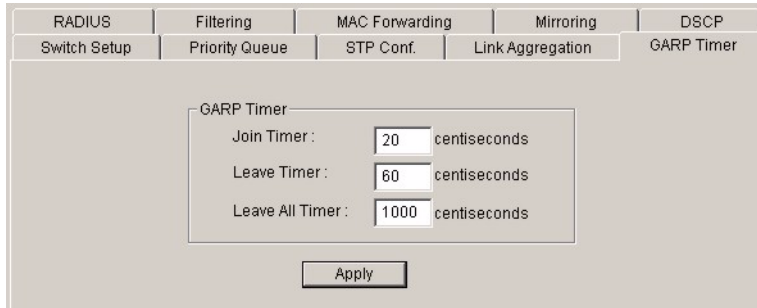
LABEL	DESCRIPTION
DHCP Relay Service	
Relay Option82	From the drop-down list box, select <b>Enable</b> to have the switch add information (slot number, port number and VLAN ID) to client TCP/IP configuration requests that it relays to a DHCP server. Otherwise, select <b>Disable</b> .
Information	This read-only field displays the system name you configure in the <b>System Info.</b> screen.
DHCP Server 1.. 3	Enter the IP address(es) of the DHCP server(s).
Apply	Click <b>Apply</b> to save the settings.

## 14.5 GARP Timer

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.

- 1** In the Device Panel list, select a device and then right-click.
- 2** Click **Configuration, Switch Configuration** and then the **Switch Setup** tab.
- 3** Select the **GARP Timer** check box and then click **Apply**.
- 4** Click **Configuration, Switch Configuration** and then the **GARP Timer** tab to display the following screen.

**Figure 80** Switch Configuration: GARP Timer



The following table describes the labels in this screen.

**Table 52** Switch Configuration: GARP Timer

LABEL	DESCRIPTION
Join Timer	<b>Join Timer</b> sets the duration of the join period timer for GVRP in milliseconds. Each port has a join period timer. The allowed join time range is between 10 and 6553 centiseconds; the default is 20 centiseconds. See the chapter on VLAN setup for more background information.
Leave Timer	<b>Leave Timer</b> sets the duration of the leave period timer for GVRP in milliseconds. Each port has a single leave period timer. Leave time must be at least two times larger than <b>Join Timer</b> ; the default is 60 centiseconds.
Leave All Timer	<b>Leave All Timer</b> sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than <b>Leave Timer</b> ; the default is 1000 centiseconds.
Apply	Click <b>Apply</b> to save your changes.

## 14.6 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

### 14.6.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

### 14.6.2 Configuring RADIUS

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration**, **Switch Configuration** and then the **RADIUS** tab to display the following screen.



**Figure 81** Switch Configuration: RADIUS

The following table describes the labels in this screen.

**Table 53** Switch Configuration: RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click <b>Apply</b> to save your changes.

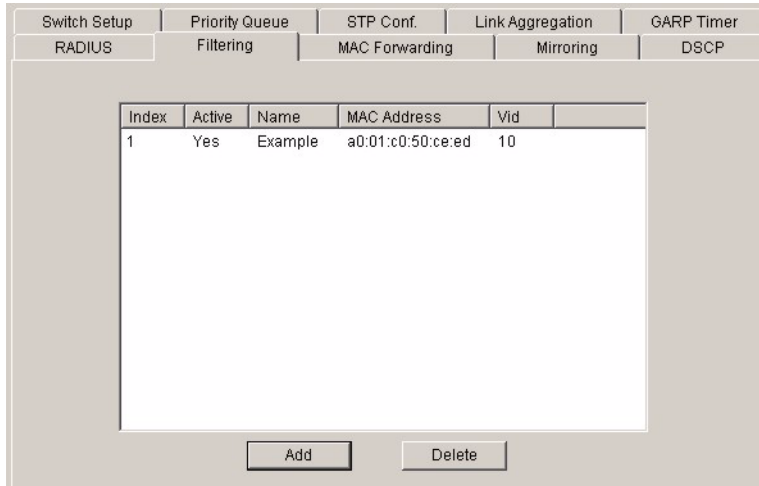
## 14.7 Filtering

This feature is not available on all switch models.

Port filtering means forwarding (not supported on all models) or discarding packets based on the MAC addresses and VLAN group.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration**, **Switch Configuration** and then the **Filtering** tab to display the following screen.

**Figure 82** Switch Configuration: Filtering



The following table describes the labels in this screen.

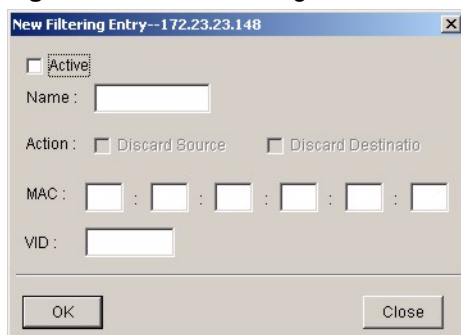
**Table 54** Switch Configuration: Filtering

LABEL	DESCRIPTION
Index	This field displays the index number.
Active	This field displays whether the filter is enabled (Yes) or not (No).
Name	This field displays the descriptive name for this filter.
MAC Address	This field displays the MAC address of a device whose traffic is forwarded or blocked.
VID	This field displays the ID of the VLAN group to which the MAC address belongs.
Add	Click <b>Add</b> to create a new filter.
Delete	Click <b>Delete</b> to remove the selected filter.

### 14.7.1 Creating a New Filter

To create a new filter, click **Add** in the **Filtering** screen. A configuration screen displays as shown.

**Figure 83** Switch Configuration: Filtering: Add



The following table describes the related labels in this screen.

**Table 55** Switch Configuration: Filtering: Add

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification purpose only.
Action	If the options are not applicable, packets that match the MAC address and VLAN ID specified will be discarded. Select <b>Discard source</b> to drop frame from the source MAC address (specified in the <b>MAC</b> field). The switch can still send frames to the MAC address. Select <b>Discard destination</b> to drop frames intended for the destination MAC address (specified in the <b>MAC</b> field). The switch can still receive frames originating from the MAC address. Select <b>Discard source</b> and <b>Discard destination</b> to block traffic to/from the MAC address specified in the <b>MAC</b> field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
OK	Click <b>OK</b> to save the changes and close this screen.
Close	Click <b>Close</b> to close this screen. All unsaved settings will be lost.

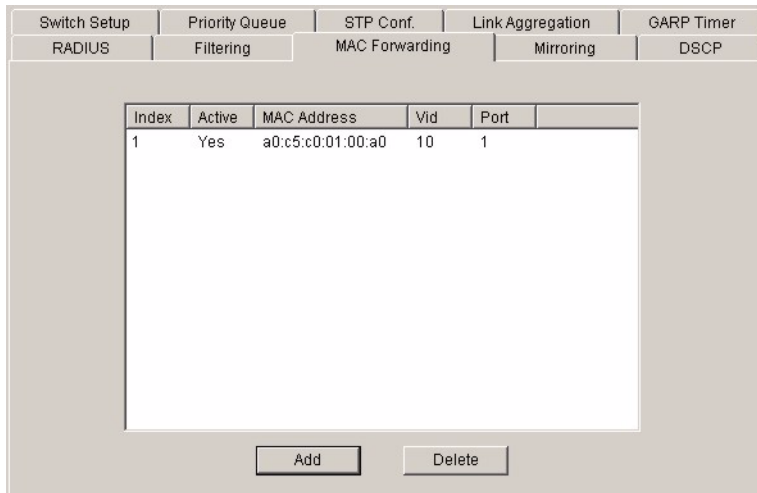
## 14.8 MAC Forwarding

A static MAC address entry is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. Devices that match static MAC address rules on a port can only receive traffic on that port and cannot receive traffic on other ports. This may reduce unicast flooding.

### 14.8.1 Configuring Static MAC Forwarding

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration**, **Switch Configuration** and then the **MAC Forwarding** tab to display the following screen.

**Figure 84** Switch Configuration: MAC Forwarding



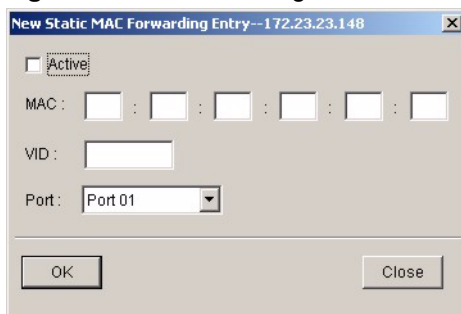
The following table describes the labels in this screen.

**Table 56** Switch Configuration: MAC Forwarding

LABEL	DESCRIPTION
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active ( <b>Yes</b> ) or not ( <b>No</b> ). You may temporarily deactivate a rule without deleting it.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN identification number.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Add	Click the <b>Add</b> button to create a MAC forwarding rule.
Delete	Select the rule(s) that you want to remove in the MAC Forwarding table and then click the <b>Delete</b> button.

- To add a new rule, click **Add** in the **MAC Forwarding** screen. A screen displays as shown. To change the settings of a rule, select a rule and click **Add** in the previous screen.

**Figure 85** Switch Configuration: MAC Forwarding: Add



The following table describes the labels in this screen.

**Table 57** Switch Configuration: MAC Forwarding: Add

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
MAC	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.
VID	Enter the VLAN group identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
OK	Click <b>OK</b> to save the settings.
Close	Click <b>Close</b> to close the screen. All unsaved settings will be lost.

## 14.9 Mirroring

Port mirroring allows you to copy a traffic flow to a mirror port (the port you copy the traffic to) in order that you can examine the traffic from the mirror port without interference.

Click **Configuration**, **Switch Configuration** and the **Mirroring** tab in the navigation panel to display the **Mirroring** screen. Use this screen to select a mirror port and specify the traffic flow to be copied to the mirror port.

**Figure 86** Switch Configuration: Mirroring (ES-2024)

**Figure 87** Switch Configuration: Mirroring (GS-2024)

**Figure 88** Switch Configuration: Mirroring (ES-3124/ES-3124PWR)

The following table describes the labels in this screen.

**Table 58** Switch Configuration: Mirroring

LABEL	DESCRIPTION
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select a port from the drop-down list box.
Mirrored Port	Select a port from the drop-down list box to mirror the traffic on a port.
Direction	This field is not available on all switch models. Select the traffic direction from the drop-down list box. Choices are <b>Ingress</b> (incoming) or <b>Egress</b> (outgoing).
Ingress	You can specify to copy all incoming traffic or traffic to/from a specified MAC address. Select <b>All</b> to copy all incoming traffic from the mirrored port(s). Select <b>Destination MAC</b> to copy incoming traffic to a specified MAC address on the mirrored port(s). Enter the destination MAC address in the fields provided. Select <b>Source MAC</b> to copy incoming traffic from a specified MAC address on the mirrored port(s). Enter the source MAC address in the fields provided.
Egress	You can specify to copy all outgoing traffic or traffic to/from a specified MAC address. Select <b>All</b> to copy all outgoing traffic from the mirrored port(s). Select <b>Destination MAC</b> to copy outgoing traffic to a specified MAC address on the mirrored port(s). Enter the destination MAC address in the fields provided. Select <b>Source MAC</b> to copy outgoing traffic from a specified MAC address on the mirrored port(s). Enter the source MAC address in the fields provided.
Apply	Click <b>Apply</b> to save the changes.

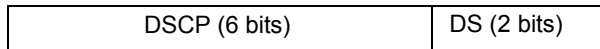
## 14.10 DSCP

This feature is not available on all models.

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 89** DiffServ: Differentiated Service Field

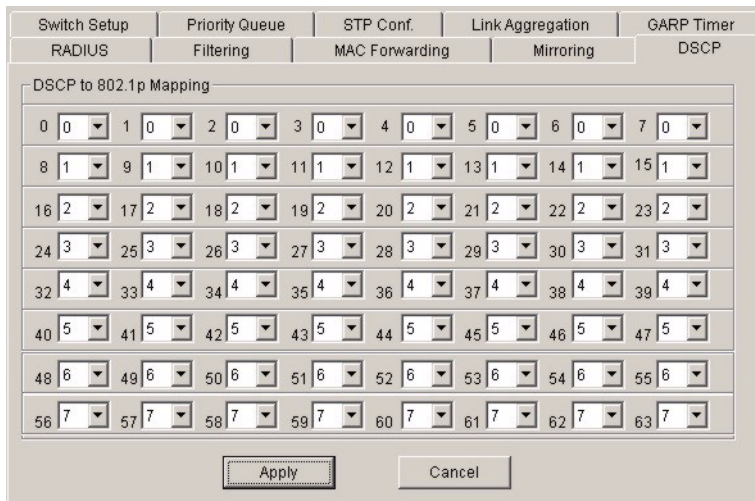


The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

You can configure the DSCP to IEEE 802.1p mapping to allow the switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

Click **Configuration**, **Switch Configuration** and the **DSCP** tab to display the screen as shown.

**Figure 90** Switch Configuration: DSCP



The following table describes the labels in this screen.

**Table 59** Switch Configuration: DSCP

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to discard all changes and start configuring the screen again.

# CHAPTER 15

## VLAN

This chapter describes how to view VLAN status, add and edit VLANs and how to use the VLAN template. The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen.

### 15.1 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that VLAN is unidirectional; it only governs outgoing traffic.

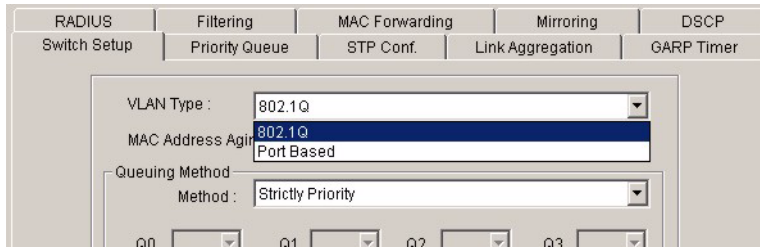
### 15.2 Configuring 802.1Q VLAN

Follow the steps below to set the **802.1Q VLAN Type** on the switch.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.
- 3 Select **802.1Q** as the **VLAN Type** and then click **Apply**.

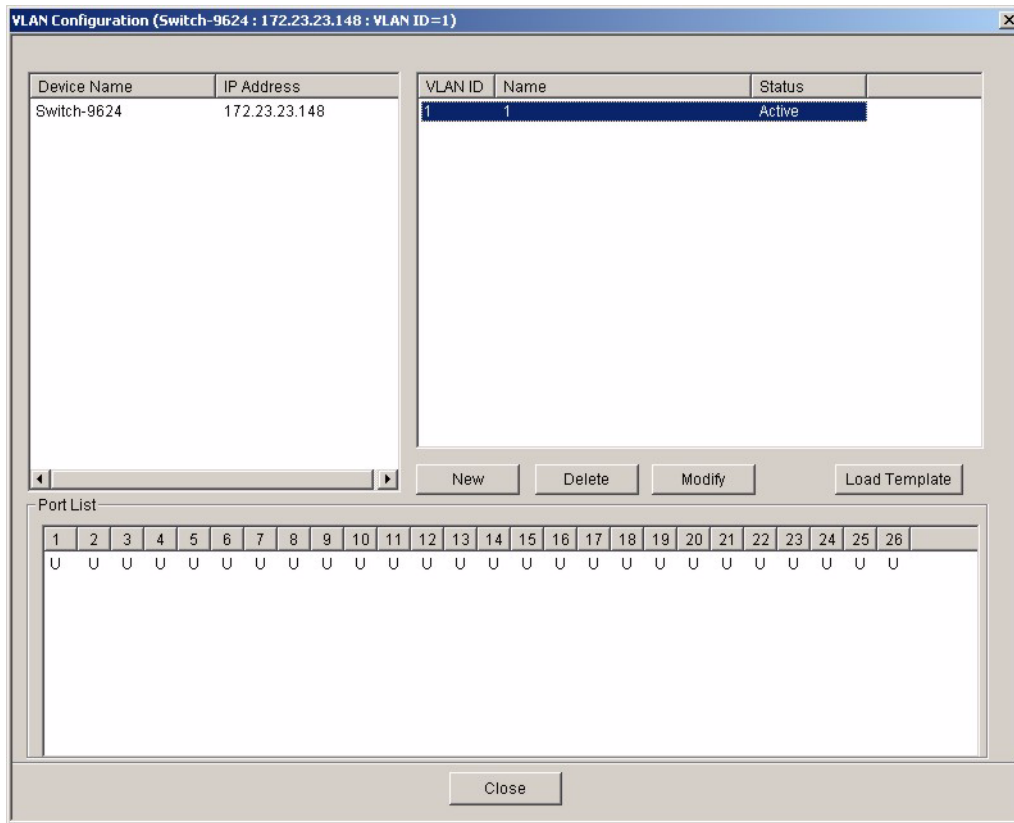


**Figure 91** Selecting a VLAN Type



**4** Click **Configuration** and then **VLAN Configuration** to display the screen as shown next.

**Figure 92** VLAN Configuration: 802.1Q



The following table describes the labels in this screen.

**Table 60** VLAN Configuration: 802.1Q

LABEL	DESCRIPTION
VLAN ID	This field displays the ID of the VLAN.
Name	This field displays the name of the VLAN.
Status	This field displays <b>ACTIVE</b> if the VLAN is active and will remain so after the next reset of the device. This field is <b>DynamicGVRP</b> if the VLAN is active and will remain so until removed by GVRP. This field is <b>OTHER</b> if the VLAN is active, but is not permanent or created by GVRP.

**Table 60** VLAN Configuration: 802.1Q (continued)

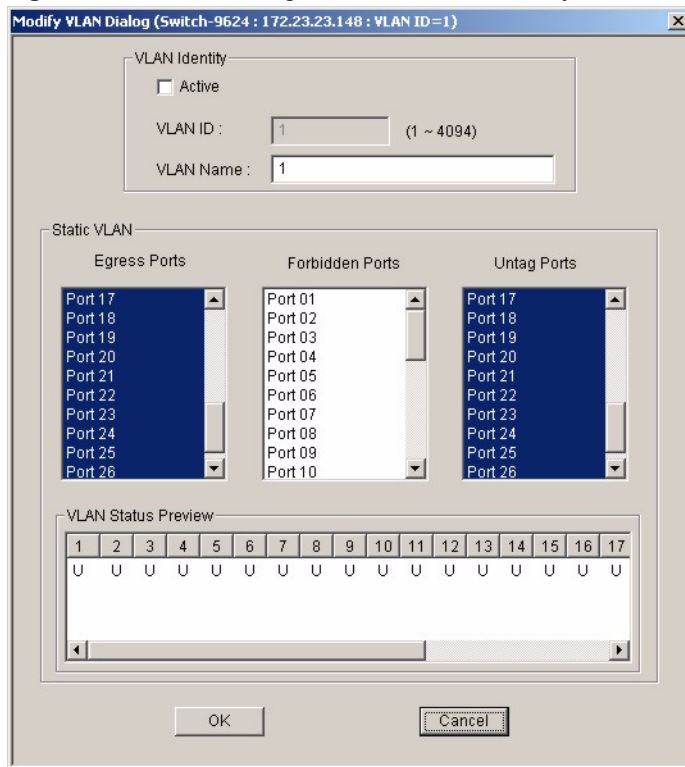
LABEL	DESCRIPTION
New	Click <b>New</b> to create a new VLAN. You must enter a <b>VLAN ID</b> and a <b>VLAN Name</b> to create a new <b>VLAN</b> . The new VLAN and name is displayed in the left-hand column in this screen.
Delete	Click on a VLAN in the left-hand column of this screen and then click the <b>Delete</b> button to remove it from the VLAN template.
Modify	Click on a VLAN in the left-hand column of this screen. Change the <b>VLAN ID</b> , <b>VLAN Name</b> or change the configuration of the egress, forbidden and untagged ports. Click the <b>Modify</b> button to save the changes.
Load Template	Use a VLAN template to overwrite existing selected VLANs. Select one or more VLANs and click the <b>Load Template</b> button. See <a href="#">Section 6.2 on page 60</a> for more information.
Port List	Click on a port in the <b>Egress Ports</b> list to add the selected port to the port list. If a port is not selected from any of the three port lists, then it is a normal tagged port. Refer to <a href="#">Table 61 on page 131</a> for the VLAN port type descriptions.
Close	Click <b>Close</b> to close the screen.

### 15.2.1 Modify an 802.1Q VLAN

Ports are assigned membership in a VLAN by associating a VLAN ID with the ports.

In the VLAN screen, click **New** or **Modify** to display the following screen.

**Figure 93** VLAN Configuration: 802.1Q: Modify



The following table describes the labels in this screen.

**Table 61** VLAN Configuration: 802.1Q: Modify

LABEL	DESCRIPTION
VLAN Identity	
Active	Select <b>Active</b> to enable this VLAN.
VLAN ID	This field displays a unique number to identify the VLAN.
VLAN Name	Enter a descriptive name for identification purposes.
Static VLAN	Click on a port in a list to add the selected port to the port list. If a port is not on any of the three port lists, then it is a normal tagged port. Refer to the following table for the VLAN port type descriptions.
Egress Ports	Select the port(s) to belong to this VLAN.
Forbidden Ports	This is a port that is blocked from joining a VLAN group. No frames are transmitted through this port.
Untagged Ports	This is a port that does not tag all outgoing frames transmitted.
VLAN Status Preview	Click on a port in the <b>Egress Ports</b> list to add the selected port to the VLAN Status Preview list. If a port is not selected from any of the three port lists, then it is a normal tagged port. Refer to <a href="#">Table 62 on page 131</a> for the VLAN port type descriptions.
OK	Click <b>OK</b> to save the changes and close this screen.
Cancel	Click <b>Cancel</b> to close this screen. All unsaved changes will be lost.

**Note:** A forbidden port cannot be an egress port or tagged.

The following table describes the labels in this screen for each VLAN port type.

**Table 62** VLAN Port Type Descriptions

LABEL	DESCRIPTION
Egress Ports	A port that is in the egress list in a VLAN. Only select this if the connected device supports IEEE 802.1Q VLAN.
Forbidden Ports	A port that is blocked from joining a VLAN group. No frames are transmitted through this port.
Untagged Ports	A port that does not tag all outgoing frames transmitted.
Normal Tagged Port	A port that joins a VLAN group using GVRP. Outgoing frames are tagged on this port.

## 15.2.2 Removing a VLAN

In the VLAN screen, select a VLAN and click **Delete**.

## 15.3 Introduction to Port-based VLANs

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.

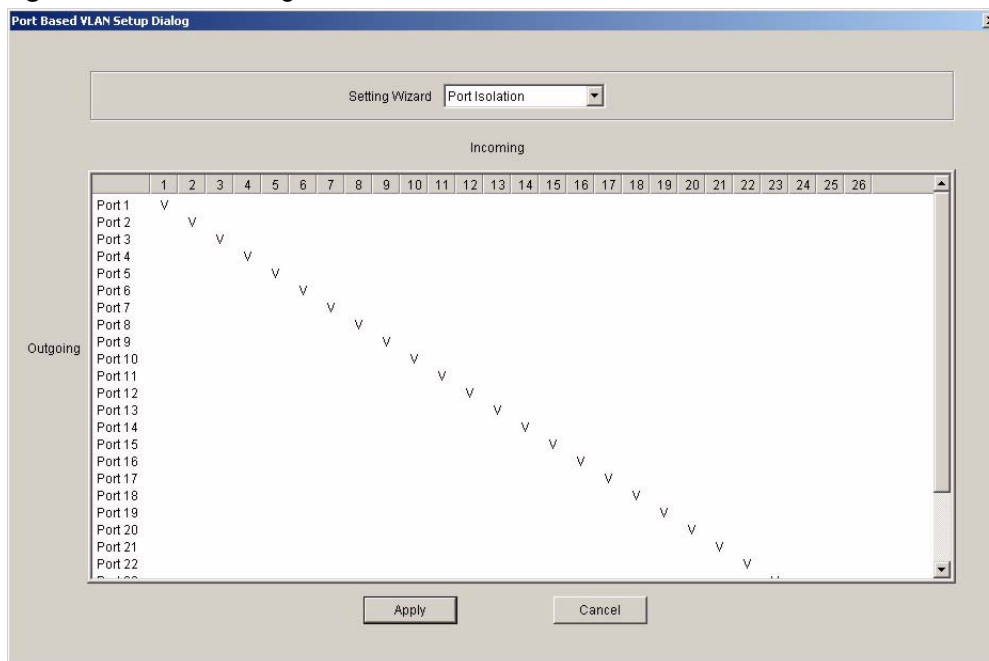
The port-based VLAN setup screen is shown next. The CPU management port forms a VLAN with all Ethernet ports.

### 15.3.1 Configuring Port Based VLAN

Follow the steps below to set the **Port Based VLAN Type** on the switch.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.
- 3 Select **Port Based** as the **VLAN Type** and then click **Apply**.
- 4 Click **Configuration** and then **VLAN Configuration** to display the screen as shown next.

**Figure 94** VLAN Configuration: Port Based



The following table describes the labels in this screen.

**Table 63** VLAN Configuration: Port Based

LABEL	DESCRIPTION
Setting Wizard	<p>Choose from <b>All connected</b> or <b>Port isolation</b>.</p> <p><b>All connected</b> means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure.</p> <p><b>Port isolation</b> means that each port can only communicate with the <b>CPU</b> management port and cannot communicate with each other. All incoming ports are selected while only the <b>CPU</b> outgoing port is selected. This option is the most limiting but also the most secure.</p> <p>After you make your selection, click <b>Apply</b> to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click <b>Apply</b> at the bottom of the screen.</p>
Incoming	<p>These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). <b>CPU</b> refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>
Outgoing	<p>These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. <b>CPU</b> refers to the switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.</p>
Apply	<p>Click <b>Apply</b> to save the changes, including the "wizard settings".</p>
Cancel	<p>Click <b>Cancel</b> to start configuring the screen again.</p>

# CHAPTER 16

## Ethernet Port Configuration

This chapter shows how to configure the Ethernet port settings.

### 16.1 Overview

Use the **Ethernet Port Configuration** screens to set port-related settings (such as port VLAN, STP and security, etc.).

Once you configure a feature on a port, you must enable that feature on the switch in the **Switch Setup** screen.

### 16.2 Port Setup

Use the **Port Setup** screen to activate and configure switch port parameters.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port** and then the **Port Setup** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 95** Ethernet Port Configuration: Port Setup (ES-2024A)

Port 802.1x	Port Security	Port Mirroring
Bandwidth Ctrl.	Broadcast Storm Ctrl.	Diffserv
Port Setup	Port VLAN	Port Link Aggregation
		Port STP

Active

Type : FastEthernet\_10/100

Port Name :

Speed/Duplex :   Flow Control

802.1p Priority :

Intrusion Lock

**Figure 96** Ethernet Port Configuration: Port Setup (GS-2024)

**Figure 97** Ethernet Port Configuration: Port Setup (ES-3124/ES-3124PWR)

The following table describes the fields in this screen.

**Table 64** Ethernet Port Configuration: Port Setup

LABEL	DESCRIPTION
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Type	This field displays <b>10/100M</b> for an Ethernet/Fast Ethernet connection or <b>100/1000M</b> for Gigabit connections.
Port Name	This field displays the name of a selected port.

**Table 64** Ethernet Port Configuration: Port Setup (continued)

LABEL	DESCRIPTION
Speed/Duplex	<p>Select the speed and the duplex mode of the Ethernet connection on this port. Choices are <b>Auto</b>, <b>10M/Half Duplex</b>, <b>10M/Full Duplex</b>, <b>100M/Half Duplex</b>, <b>100M/Full Duplex</b> and <b>1000M/Full Duplex</b> (for Gigabit/mini-GBIC ports only).</p> <p>Selecting <b>Auto</b> (auto-negotiation) makes one Ethernet port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, an Ethernet port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.</p>
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select <b>Flow Control</b> to enable it.</p>
802.1p Priority	<p>The switch uses this priority value for incoming frames without an IEEE 802.1p priority queue tag. The switch uses this priority value internally and does not add an IEEE 802.1p priority tag.</p>
Intrusion Lock	<p>Select the <b>Intrusion Lock</b> check box to enable this security feature on a selected port on the switch. If an Ethernet cable is disconnected from the port, intrusion locking prevents access once a cable is reconnected. This limits risk from unauthorized access such as hacking.</p> <p><b>Note:</b> You cannot access a port with intrusion locking enabled after a cable is disconnected and then reconnected. You must clear and re-select the <b>Intrusion Lock</b> check box to allow access to the port again.</p>
Jumbo Frame	<p>Jumbo frames are used to forward non-standard packet sizes on your network. These frames can deliver frames of up to 9216 bytes instead of standard Ethernet frames of 1522 bytes. Fewer packets are required for large data transfer, improving traffic throughput on the port.</p> <p>Select this option to allow a port to send and receive jumbo frames.</p> <p><b>Note:</b> The peer device must also support non-standard packet traffic.</p>
BPDU Control	<p>Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the <b>Switch Setup</b> screen first.</p> <p>Select <b>Peer</b> to process any BPDU (Bridge Protocol Data Units) received on this port.</p> <p>Select <b>Tunnel</b> to forward BPDUs received on this port.</p> <p>Select <b>Discard</b> to drop any BPDU received on this port.</p> <p>Select <b>Network</b> to process a BPDU with no VLAN tag and forward a tagged BPDU.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the switch.</p>



## 16.3 Port VLAN

Use the following screen to activate a port VLAN, GVRP and VLAN trunking.

### 16.3.1 Configuring Port VLAN

Follow the steps below to configure the **Port VLAN** screen.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Port VLAN** tab.
- 3 Select the ports from the Port List Panel to which you want to apply this configuration.

**Figure 98** Ethernet Port Configuration: Port VLAN

The following table describes the labels in this screen.

**Table 65** Ethernet Port Configuration: Port VLAN

LABEL	DESCRIPTION
Ingress	This feature is not supported on all models. If this check box is selected for a port, the device discards incoming frames for VLANs that do not include this port in its member set.
PVID	Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an IEEE 802.1Q VLAN-unaware switch to an IEEE 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the default ingress port's VLAN ID, the PVID. The default PVID is VLAN 1 for all ports, but this can be changed to any number between 1 and 4094.
GVRP	Select the check box to permit VLAN groups beyond the local switch on this port. GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are <b>All</b> and <b>Tag Only</b> . Select <b>All</b> to accept all frames with untagged or tagged frames on this port. This is the default setting. Select <b>Tag Only</b> to accept only tagged frames on this port. All untagged frames are dropped.

**Table 65** Ethernet Port Configuration: Port VLAN (continued)

LABEL	DESCRIPTION
VLAN Trunking	Enable VLAN trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
Apply	Click <b>Apply</b> to save the changes.

## 16.4 Port Link Aggregation

Use the **Port Link Aggregation** screen to configure a port trunk group and set LACP timeout.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Port Link Aggregation** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 99** Ethernet Port Configuration: Port Link Aggregation

The following table describes the fields in this screen.

**Table 66** Ethernet Port Configuring: Port Link Aggregation

LABEL	DESCRIPTION
Group	Select the trunk group to which a port belongs.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select from 1 second to 30 seconds.
Apply	Click <b>Apply</b> to save the changes.

## 16.5 Port STP

Use the **Port STP** screen to configure STP for the selected ports.

- 1 In the Device Panel list, right-click on a device.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Port STP** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 100** Ethernet Port Configuration: Port STP

The screenshot shows a configuration window for Port STP. At the top, there are several tabs: Port 802.1x, Port Security, Port Mirroring, Bandwidth Ctrl., Broadcast Storm Ctrl., Diffserv, Port Setup, Port VLAN, Port Link Aggregation, and Port STP. The 'Port STP' tab is active. Below the tabs, there is a checkbox labeled 'STP Active' which is currently unchecked. Below that, there are two input fields: 'Priority' with a value of 128 and a range of (0 ~ 255), and 'Path Cost' with a value of 4 and a range of (1 ~ 65535). At the bottom center, there is an 'Apply' button.

The following table describes the fields in this screen.

**Table 67** Ethernet Port Configuration: Port STP

LABEL	DESCRIPTION
STP Active	Select this check box to activate STP on this port.
Priority	Priority is used in determining the root device, root port and designated port. The device with the highest priority (lowest numeric value) becomes the STP root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. The allowed range is 0 to 255. The lower the numeric value you assign, the higher the priority for this device.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the link. The slower the media, the higher the cost (refer to the table on path cost in the section on STP).
Apply	Click <b>Apply</b> to save the changes back to the switch.

## 16.6 Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows on a port.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Bandwidth Ctrl.** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 101** Ethernet Port Configuration: Bandwidth Ctrl.

**Figure 102** Ethernet Port Configuration: Bandwidth Ctrl. (GS-2024)

The following table describes the labels in this screen.

**Table 68** Ethernet Port Configuration: Bandwidth Ctrl.

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the selected port(s). You may temporarily deactivate a rule without deleting it by clearing this check box.
Ingress Rate	Type the maximum bandwidth allowed in kilobits per second (Kbps) for traffic coming into this port.
Egress Rate	Type the maximum bandwidth allowed in kilobits per second (Kbps) for traffic going out of this port.
Scheme	Select <b>Drop</b> (default) from the drop-down list box to discard all incoming packets that are over the maximum allowable bandwidth on a port. A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. <b>Flow Control</b> is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select this option to enable flow control.
Apply	Click <b>Apply</b> to save the changes back to the switch.

## 16.7 Broadcast Storm Control

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Broadcast Storm Ctrl.** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 103** Ethernet Port Configuration: Broadcast Storm Ctrl. (ES-2024A)

The screenshot shows the configuration interface for Broadcast Storm Control on a switch. The 'Broadcast Storm Ctrl.' tab is selected. There is an 'Active' checkbox which is currently unchecked. Below it, the 'Rate' is set to '64' Kbps. An 'Apply' button is visible at the bottom.

**Figure 104** Ethernet Port Configuration: Broadcast Storm Ctrl. (GS-2024)

The screenshot shows the configuration interface for Broadcast Storm Control on a switch. The 'Broadcast Storm Ctrl.' tab is selected. There is an 'Active' checkbox which is currently unchecked. An 'Apply' button is visible at the bottom.

**Figure 105** Ethernet Port Configuration: Broadcast Storm Ctrl. (ES-3124/ES-3124PWR)

The screenshot shows the configuration interface for Broadcast Storm Control on a switch. The 'Broadcast Storm Ctrl.' tab is selected. There are three checkboxes: 'Broadcast', 'Multicast', and 'DLF'. Each checkbox is currently unchecked and has an empty input field next to it, followed by '( pkt / s )'. An 'Apply' button is visible at the bottom.

The following table describes the labels in this screen.

**Table 69** Ethernet Port Configuration: Broadcast Storm Ctrl.

LABEL	DESCRIPTION
Active	Select <b>Active</b> to enable broadcast storm control.  <b>Note:</b> For GS-2024, configure rate limiting settings in the <b>Switch Configuration: Switch Setup</b> screen. Refer to <a href="#">Section 14.1 on page 110</a> .
Rate	Specify the traffic a port receives in kilobits per second (Kbps). <ul style="list-style-type: none"> <li>• If you enter a number between 64 and 1728, the switch automatically rounds the number down to the nearest multiple of 64.</li> <li>• If you enter a number between 1729 and 1999, the rate is fixed at 1792.</li> <li>• If you enter a number between 2000 and 103999, the switch rounds the number down to the nearest multiple of 1000.</li> <li>• On a Gigabit Ethernet/ Mini-GBIC port, the switch rounds a number down to the nearest multiple of 8000 for a number between 104000 and 1000000.</li> </ul>
Broadcast	Select this option and specify how many broadcast packets the port receives per second.
Multicast	Select this option and specify how many multicast packets the port receives per second.
DLF	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click <b>Apply</b> to save the changes.

## 16.8 DiffServ

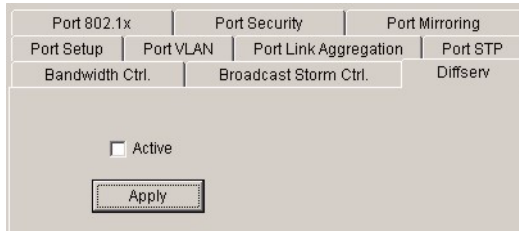
This feature is not available on all models.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Enable DiffServ in the **DiffServ** screen.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and the **DiffServ** tab.
- 3 Select **Active** to enable the DSCP-to-IEEE 802.1q mapping. Set the mapping in the **System Configuration: DSCP** screen. See [Section 14.10 on page 126](#).
- 4 Click **Apply** to save the changes.

**Figure 106** Ethernet Port Configuration: DiffServ

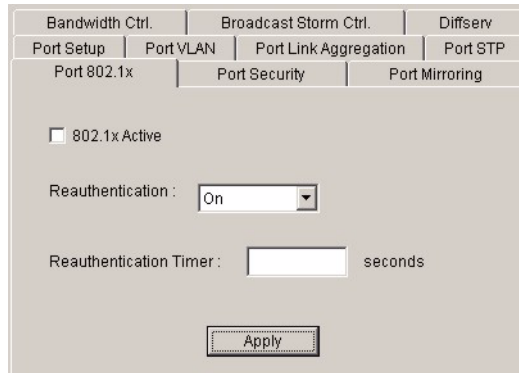


## 16.9 Port 802.1x

Use the **Port 802.1x** screen to configure reauthentication for selected ports.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Port 802.1x** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 107** Ethernet Port Configuration: Port 802.1x



The following table describes the fields in this screen.

**Table 70** Ethernet Port Configuration: Port 802.1x

LABEL	DESCRIPTION
802.1x Active	Select this check box to permit IEEE 802.1x authentication on this port. You must first allow IEEE 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Select <b>On</b> from the drop-down list box to periodically prompt a subscriber to re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click <b>Apply</b> to save the changes back to the switch.

## 16.10 Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable Port Security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

### 16.10.1 Configuring Port Security

Follow the steps below to configure the **Port Security** screen.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Port Security** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 108** Ethernet Port Configuration: Port Security

Bandwidth Ctrl.	Broadcast Storm Ctrl.	Diffserv
Port Setup	Port VLAN	Port Link Aggregation
Port 802.1x	Port Security	Port Mirroring

Active  
 Address Learning  
 Limited Number of Learned MAC Address :

**Figure 109** Ethernet Port Configuration: Port Security (GS-2024)

Port Setup	Port VLAN	Port Link Aggregation	Port STP
Port 802.1x	Port Security	Bandwidth Ctrl.	Broadcast Storm Ctrl.

Active



The following table describes the fields in this screen.

**Table 71** Ethernet Port Configuration: Port Security

TABLE	DESCRIPTION
Active	Select this check box to enable the port security feature on selected ports.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled. Select the <b>Address Learning</b> check box.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC-address aging out time can be set in the <b>Switch Setup</b> screen. The valid range is from 0 to 16K. 0 means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.
MAC Freeze	Use the <b>MAC Freeze</b> button to convert all current dynamic MAC addresses to static MAC addresses. When the <b>MAC Freeze</b> button is selected, the <b>MAC Address Learning</b> check box is cleared but port security becomes <b>Active</b> .
Apply	Click <b>Apply</b> to save the changes back to the switch.

## 16.11 Port Mirroring

This feature is not available on all models.

Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.

You must first select a monitor port. A monitor port is a port that copies the traffic of another port. After you select a monitor port, configure a mirroring rule in the related fields.

Select the monitor port and traffic direction in the **Switch Configuration: Mirroring** screen (refer to [Section 14.9 on page 125](#)).

Follow the steps below to configure the **Port Mirroring** screen.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Port Mirroring** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 110** Ethernet Port Configuration: Port Mirroring

The following table describes the fields in this screen.

**Table 72** Ethernet Port Configuration: Port Mirroring

LABEL	DESCRIPTION
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror. Select <b>Egress</b> (outgoing), <b>Ingress</b> (incoming) or <b>Both</b> from the drop-down list box.
Apply	Click <b>Apply</b> to save the changes back to the switch.

## 16.12 VLAN Stacking

This feature is not available on all models.

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

Follow the steps below to configure the **VLAN Stacking** screen.

- 1** In the Device Panel list, select a device and then right-click.
- 2** Click **Configuration, Ethernet Port Configuration** and then the **VLAN Stacking** tab.
- 3** Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 111** Ethernet Port Configuration: VLAN Stacking

The following table describes the fields in this screen.

**Table 73** Ethernet Port Configuration: VLAN Stacking

LABEL	DESCRIPTION
Role	Select <b>Normal</b> to have the switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in <b>SPVID</b> and <b>Priority</b> is ignored. Select <b>Access Port</b> to have the switch add the <b>SP TPID</b> tag to all incoming frames received on this port. Select <b>Access Port</b> for ingress ports at the edge of the service provider's network. Select <b>Tunnel Port</b> (available for Gigabit ports only) for egress ports at the edge of the service provider's network. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.
SPVID	<b>SPVID</b> is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See the chapter on VLANs for more background information on VLAN ID.
Priority	Select the priority level of the inner IEEE 802.1Q tag. "0" is the lowest priority level and "7" is the highest.
Apply	Click <b>Apply</b> to save the changes.

## 16.13 Queue Method

This feature is not available on all models.

Queuing is used to help solve performance degradation when there is network congestion. Use the **Switch Configuration: Switch Setup** screen to configure queuing algorithms for outgoing traffic.

Follow the steps below to configure queuing for each port.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Ethernet Port Configuration** and then the **Queue Method** tab.
- 3 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 112** Ethernet Port Configuration: Queue Method

The following table describes the fields in this screen.

**Table 74** Ethernet Port Configuration: Queue Method

LABEL	DESCRIPTION
Q0 - Q7	For <b>Weighted Fair Scheduling</b> , select the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. For Gigabit/ Mini-GBIC ports, if you select <b>0</b> for the queue weight, the switch uses <b>Strictly Priority</b> to service the queue.
Apply	Click <b>Apply</b> to save the changes.



# CHAPTER 17

## Routing Configuration

This chapter shows you how to configure the routing functions.

### 17.1 Static Route

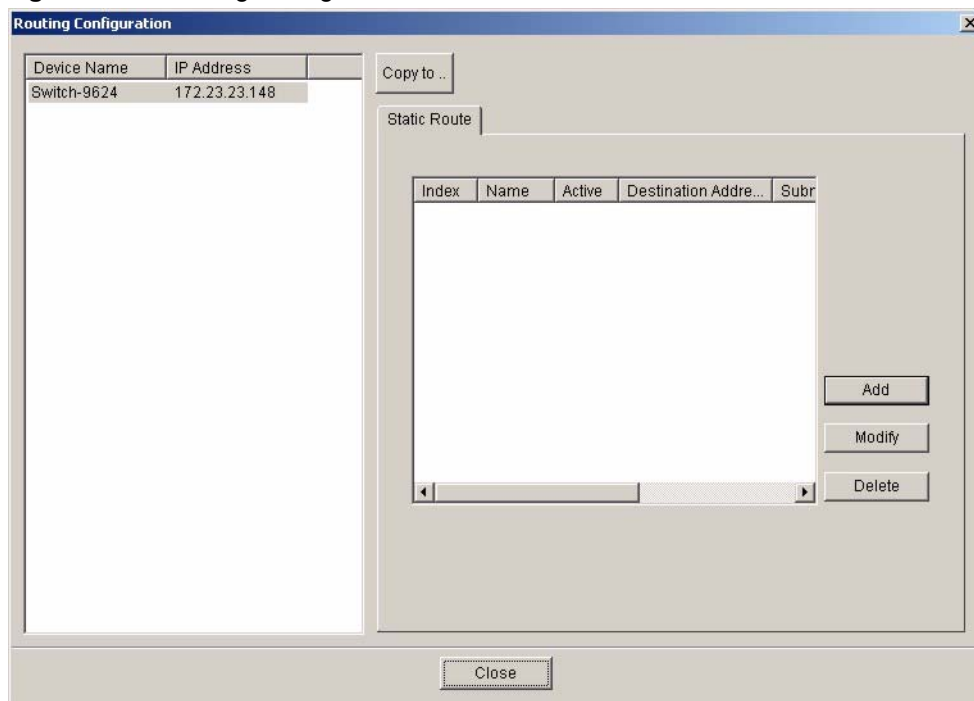
Static routes tell the switch how to forward IP traffic when you configure the TCP/IP parameters manually.

#### 17.1.1 Configuring Static Routing

Follow the steps below to view the **Routing Configuration** screen.

- 1 In the Device Panel list, select a device and then right-click.
- 2 Click **Configuration, Routing Configuration**.

**Figure 113** Routing Configuration: Static Route



The following table describes the labels in the summary table.

**Table 75** Routing Configuration: Static Route

LABEL	DESCRIPTION
Index	This field displays the index number of the route.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Active	This field displays <b>Yes</b> when the static route is activated and <b>No</b> when is it deactivated.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Add	Click the <b>Add</b> button to create a new static route.
Modify	Select the rule(s) that you want to change and click the <b>Modify</b> button.
Delete	Select the rule(s) that you want to remove in the <b>Delete</b> column, and then click the <b>Delete</b> button.

## 17.1.2 Add or Modify a Static Route

Click the **Add** button or select a static route and click the **Modify** button in the **Routing Configuration** screen to display the following screen.

**Figure 114** Routing Configuration: Static Route: Add or Modify

The following table describes the labels in this screen.

**Table 76** Routing Configuration: Static Route: Add or Modify

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name for this route. This is for identification purposes only.

**Table 76** Routing Configuration: Static Route: Add or Modify (continued)

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
OK	Click <b>OK</b> to save the new rule to the switch. It then displays in the <b>Routing Configuration</b> screen.
Cancel	Click <b>Cancel</b> to discard all changes and close the screen.





# CHAPTER 18

## Multicast Configuration

This chapter shows you how to configure multicast settings and MVR (Multicast VLAN Registration) groups. This feature is not available on all models.

### 18.1 Overview

Refer to [Section 6.3 on page 61](#) for more background information on IGMP and IP multicast addresses.

#### 18.1.1 IGMP Snooping

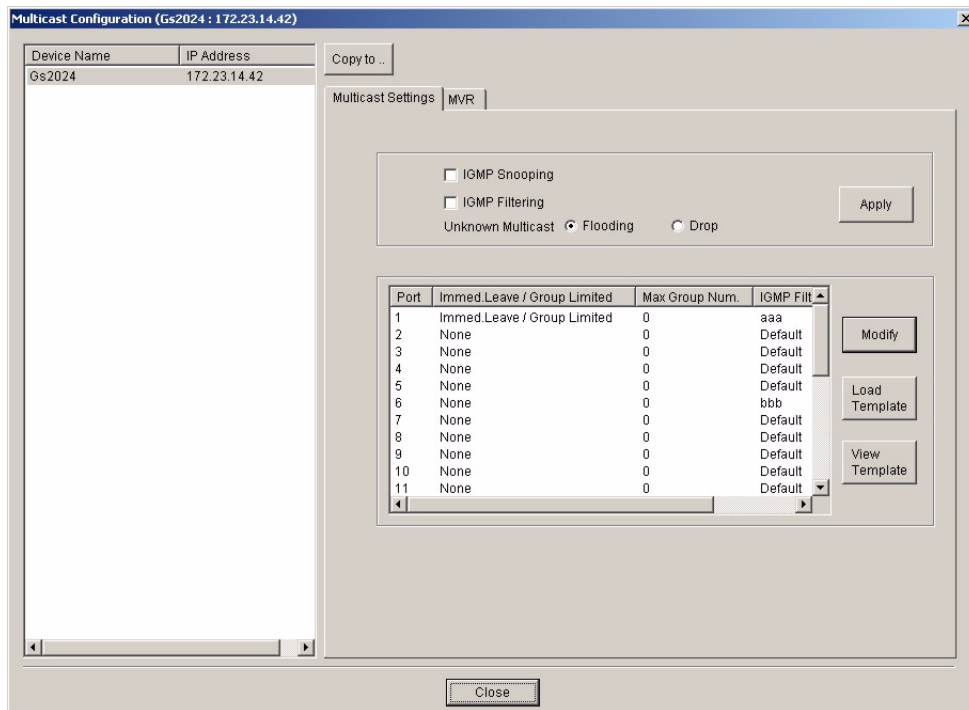
A switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the switch to learn multicast groups without you having to manually configure them.

The switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

### 18.2 Multicast Setting

To configure multicast settings, click **Configuration, Multicast Configuration**. The **Multicast Setting** screen displays.

**Figure 115** Multicast Configuration: Multicast Setting



The following table describes the labels in this screen.

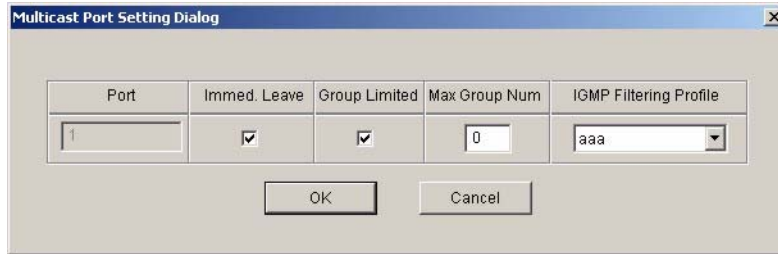
**Table 77** Multicast Configuration: Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Select <b>Active</b> to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group
IGMP Filtering	Select <b>Active</b> to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.
Unknown Multicast Frame	Specify the action to perform when the switch receives an unknown multicast frame. Select <b>Drop</b> to discard the frame(s). Select <b>Flooding</b> to send the frame(s) to all ports.
Port	This field displays the port number.
Immed. Leave/ Group Limited	This field displays whether the switch is set to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. This field also displays whether the port is set to join a limited number of groups.
Max Group Num.	This field displays number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	This field displays the name of the IGMP filtering profile this port uses. The default profile ( <b>Default</b> ) prohibits the port from joining any multicast group.
Modify	Click <b>Modify</b> to change the multicast settings of the selected port.
Load Template	Click <b>Load Template</b> to display a screen you use to select a multicast template.
View Template	Click <b>View Template</b> to display the settings of a selected multicast template.
Apply	Click <b>Apply</b> to save your changes back to the switch.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 18.2.1 Changing the Port Multicast Settings

To change the multicast settings of a port, select a port in the **Multicast Setting** screen and click **Modify**. A screen displays.

**Figure 116** Multicast Configuration: Multicast Setting: Modify



The following table describes the labels in this screen.

**Table 78** Multicast Configuration: Multicast Setting: Modify

LABEL	DESCRIPTION
Port	This field displays the port number.
Immed. Leave	Select this option to set the switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port. Enter <b>0</b> to allow a port to join any number of multicast groups.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise select <b>Default</b> to prohibit the port from joining any multicast group.
OK	Click <b>OK</b> to save your changes and close this screen.
Cancel	Click <b>Cancel</b> to discard all changes and close this screen.

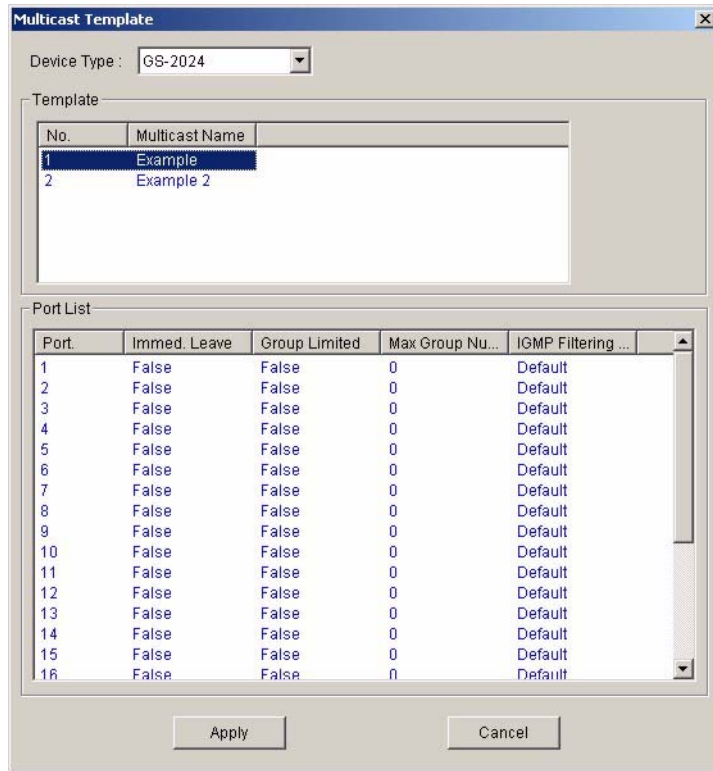
## 18.2.2 Applying a Multicast Template

After you create a multicast template using the Template screen, you can apply the template to the switch in the **Multicast Setting** screen.

**Note:** When you apply a multicast template, all custom port multicast settings will be erased.

In the **Multicast Setting** screen, select a device in the device list panel and click **Load Template**. A screen displays as shown.

**Figure 117** Multicast Configuration: Multicast Setting: Load Template



The following table describes the labels in this screen.

**Table 79** Multicast Configuration: Multicast Setting: Load Template

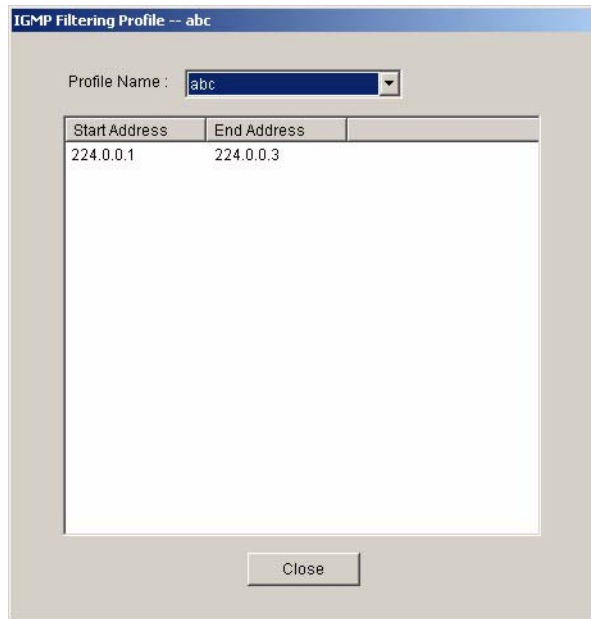
LABEL	DESCRIPTION
Device Type	Select a device type from the drop-down list box.
Template	
No.	This field displays the index number.
Multicast Name	This field displays the name of a multicast template you create using the <b>Template</b> screen.
PortList	This table displays the template settings. Refer to <a href="#">Figure 115 on page 155</a> for more information.
Apply	Click <b>Apply</b> to save the settings and close this screen.
Cancel	Click <b>Cancel</b> to discard the changes and close this screen.

### 18.2.3 Displaying IGMP Filter Profile

You can create IGMP filter templates in the **IGMP Filter Template** screen and apply IGMP filter templates in the **Multicast Template** screen.

In the **Multicast Setting** screen, select a port number and click **View Profile** to display IGMP filter profile settings.

**Figure 118** Multicast Configuration: Multicast Setting: View Profile



The following table describes the labels in this screen.

**Table 80** Multicast Configuration: Multicast Setting: View Profile

LABEL	DESCRIPTION
Profile Name	Select a profile name from the drop-down list box.
Start Address	This field displays the starting multicast IP address for a range of multicast IP addresses to which you want this IGMP filter profile to allow access.
End Address	This field displays the ending multicast IP address for a range of IP addresses to which you want this IGMP filter profile to allow access.
Close	Click <b>Close</b> to close this screen.

### 18.3 MVR

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across a service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

You must enable IGMP snooping to use MVR. However, MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

### 18.3.1 Types of MVR Ports

In MVR, a source port is a port on the switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

### 18.3.2 MVR Modes

You can set your switch to operate in either dynamic or compatible mode.

In dynamic mode, the switch sends IGMP leave and join reports through the source port(s) to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

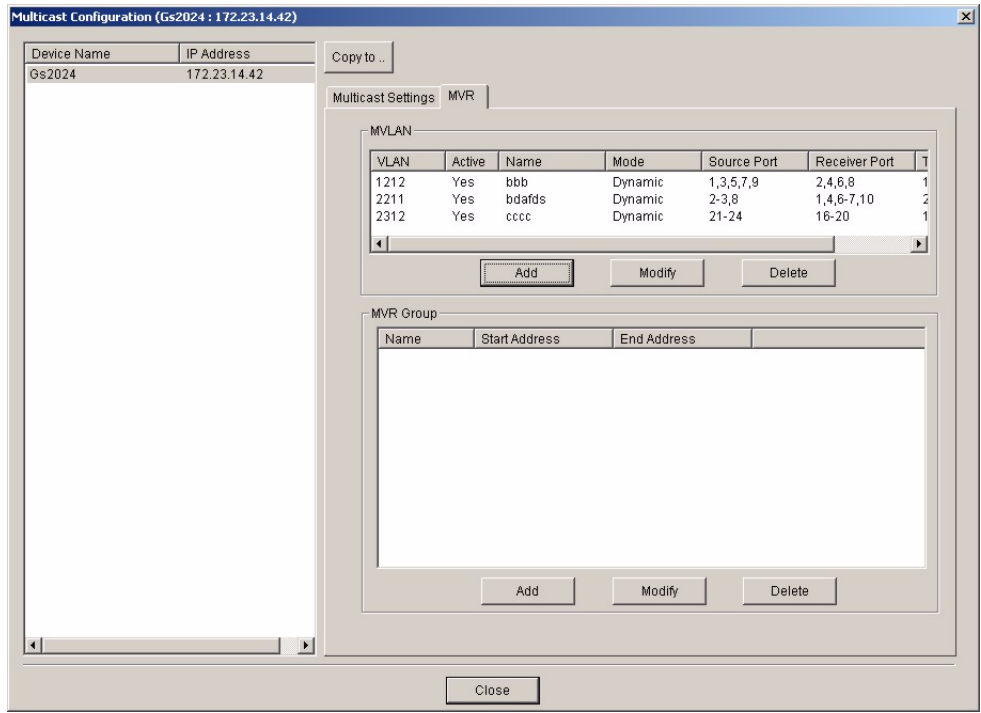
In compatible mode, the switch does not send any IGMP reports through the source port(s). In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

Refer to the user's guide that comes with your switch for more background information.

### 18.3.3 Viewing MVR Settings

Click **Configuration**, **Multicast Configuration** and click the **MVR** tab to display the screen as shown.

**Figure 119** Multicast Configuration: MVR



The following table describes the labels in this screen.

**Table 81** Multicast Configuration: MVR

LABEL	DESCRIPTION
MVLAN	This table displays the settings the multicast VLAN settings.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
Tagging Port	This field displays the port number(s) that adds the VLAN ID tag to all outgoing frames transmitted.
Add	Click <b>Add</b> to add a new entry.
Modify	Click <b>Modify</b> to change the settings of the selected MVLAN.
Delete	Click <b>Delete</b> to remove the selected MVLAN.
MVR Group	This table displays the MVR group settings.
Name	This field displays the descriptive name for this MVR group.
Start Address	This field displays the starting IP address of the MVR group.
End Address	This field displays the ending IP address of the MVR group.



**Table 81** Multicast Configuration: MVR (continued)

LABEL	DESCRIPTION
Add	Click <b>Add</b> to add a new entry.
Modify	Click <b>Modify</b> to change the settings of the selected MVR.
Delete	Click <b>Delete</b> to remove the selected MVR.

### 18.3.4 Creating a New Multicast VLAN

Follow the steps below to create a new multicast VLAN.

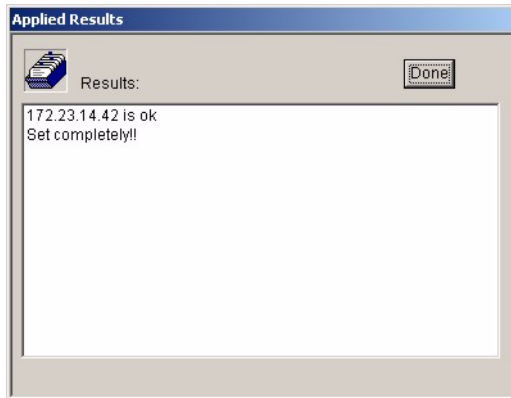
- 1 In the **MVR** screen, click **Add** under **MVLAN**. A screen displays as shown.

**Figure 120** Multicast Configuration: MVR: Add MVLAN

- 2 Select **Active** to enable this multicast VLAN setting.
- 3 In the **Name** field, enter a descriptive name (up to 32 ASCII characters) for identification purposes.
- 4 Specify a VLAN ID in the **Multicast VLAN ID** field. Enter a number between 1 and 4094.
- 5 In the **Mode** field, select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the switch not to send IGMP reports.
- 6 In the **Source Port** list box, select the MVR source port that sends and receives multicast traffic.
- 7 In the **Receiver Port** list box, select the port(s) that only receives multicast traffic.
- 8 In the **None** list box, select the port(s) not to participate in MVR. No MVR multicast traffic is sent or received on the port(s).
- 9 In the **Tagging** list box, select the port(s) to add the VLAN ID tag to all outgoing frames .
- 10 Click **OK** to save the settings and close this screen. Otherwise, click **Cancel** to discard the settings and close this screen.

11A screen displays showing the configuration result. Click **Done** to close the screen.

**Figure 121** Multicast Configuration: MVR: Add MVLAN: Result

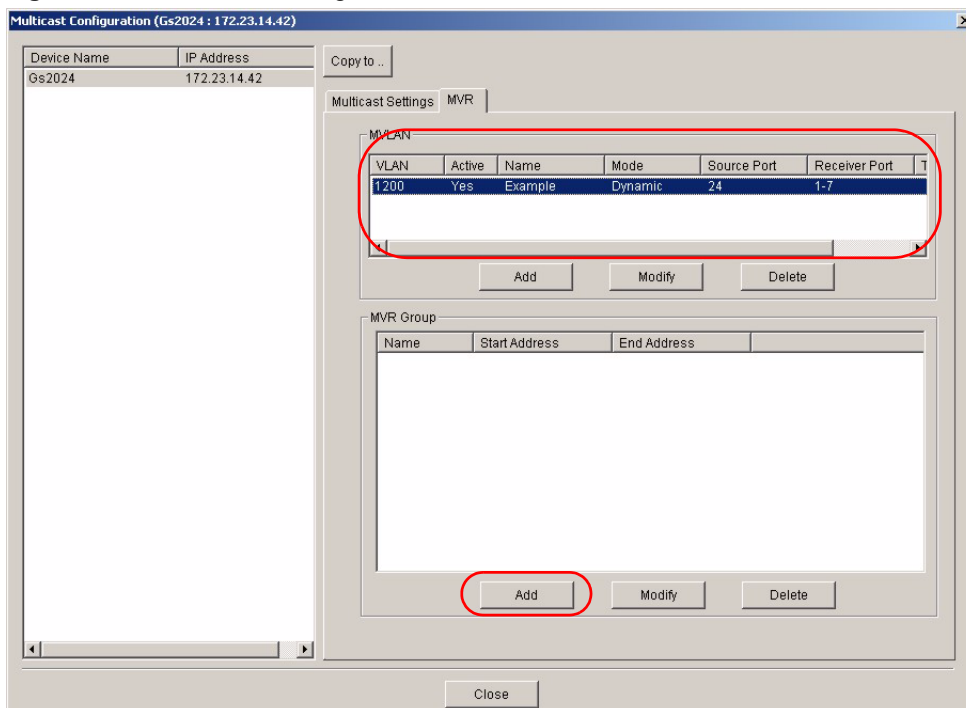


### 18.3.5 Creating a New MVR Group

Follow the steps below to create a new MVR group.

- 1 In the **MVR** screen, select one entry in the **MVLAN** list table.
- 2 Click **Add** under **MVR Group**.

**Figure 122** Multicast Configuration: MVR: Select MVLAN



- 3 A screen displays as shown. The **Multicast VLAN ID** field displays the VLAN ID to which this MVR group setting applies. In the **Name** field, enter a descriptive name for identification purposes.

**Figure 123** Multicast Configuration: MVR: Add

- 4** In the **Start Address** field, enter the starting IP multicast address of the multicast group in dotted decimal notation.
- 5** In the **End Address** field, enter the ending IP multicast address of the multicast group in dotted decimal notation.  
  
Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group.
- 6** Click **OK** to save the settings and close this screen. Otherwise, click **Cancel** to discard the settings and close this screen.
- 7** A screen displays showing the configuration result. Click **Done** to close the screen.

**Figure 124** Configuration: Multicast Configuration: MVR: Add MVR Group: Result





# CHAPTER 19

## Troubleshooting

This chapter covers potential problems and the corresponding remedies.

### 19.1 Installation Problems

**Table 82** General Installation Problems

PROBLEM	CORRECTIVE ACTION
The EMS or PostgreSQL will not install properly	<p>Make sure that the computer meets the minimum hardware and software requirements. See <a href="#">Section 1.2 on page 24</a> for more information.</p> <p>Close all programs before the installation.</p> <p>Remove any previous versions of the EMS software from your computer. See <a href="#">Section 19.3 on page 166</a> for information on how to do this.</p> <p>Re-install the EMS.</p>

### 19.2 Problems Accessing the EMS

**Table 83** Problems Accessing the EMS

PROBLEM	CORRECTIVE ACTION
When I click the Switch Manager icon, I cannot access the EMS	<p>Make sure the ODBC driver is configured properly to connect to the EMS database. Refer to the Quick Start Guide for more information.</p> <p>Shut down and restart both PostgreSQL and the SNMPc manager.</p> <p>EMS may already be running. Check your Windows task bar.</p>

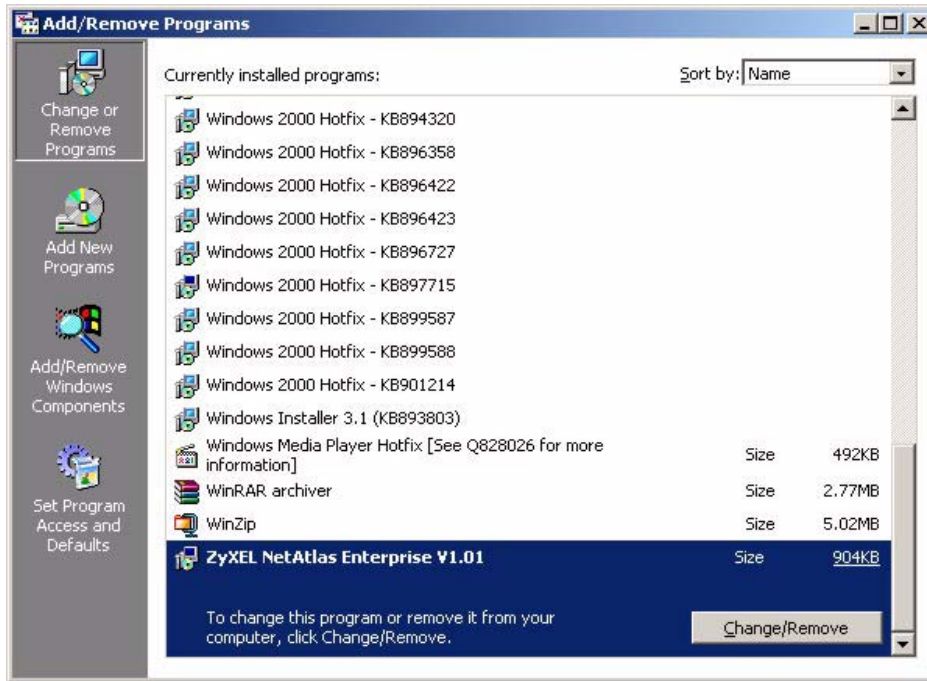
### 19.3 Uninstalling the EMS

When you install a new EMS version, the setup program automatically detects and uninstalls a previous EMS version.

Or you can manually uninstall the EMS. Follow the steps below.

- 1 Click **Start, settings, Control Panel, Add/Remove Programs**. The **Add or Remove Programs** dialog box opens.

**Figure 125 EMS: Remove**



- 2** Select **ZyXEL NetAtlas Enterprise V1.01** and then click **Change/Remove** (or **Add/Remove** depending on your version of Windows).
- 3** Click **Yes** when asked to confirm removal. The **Uninstall Shield** now runs.
- 4** Click **OK** when the uninstall has successfully completed. Restart the computer when prompted.

## 19.4 Problems Finding a Device

**Table 84** Problems Accessing the EMS

PROBLEM	CORRECTIVE ACTION
In the SNMPc Management Console I cannot find my device	<p>Check that you have compiled and added the MIBs correctly.</p> <p>Check that you have enabled auto-discovery.</p> <p>Check that the map object properties are correct for initial installation. Make sure the IP address entered is the IP address of the switch you want to manage via the EMS.</p> <p>Check that the ODBC driver is correctly configured.</p> <p>Make sure that PostgreSQL is running.</p> <p>Make sure that the computer you have installed the EMS on, is connected to the network where the switch is located.</p> <p>Make sure your computer's Ethernet card is working properly.</p> <p>If the problem still persists, uninstall and re-install the EMS software.</p>

# Appendix A

## SNMPc Network Manager

This appendix gives a brief overview of the SNMPc Network Manager.

### Starting the SNMPc Network Manager

You must have SNMPc properly installed before you can use the EMS; please refer to the Castle Rock web site at [www.castlerock.com](http://www.castlerock.com) or see your SNMPc user's guide.

You may start the SNMPc Network Manager manually or automatically each time you turn on your computer.

### Manual Startup

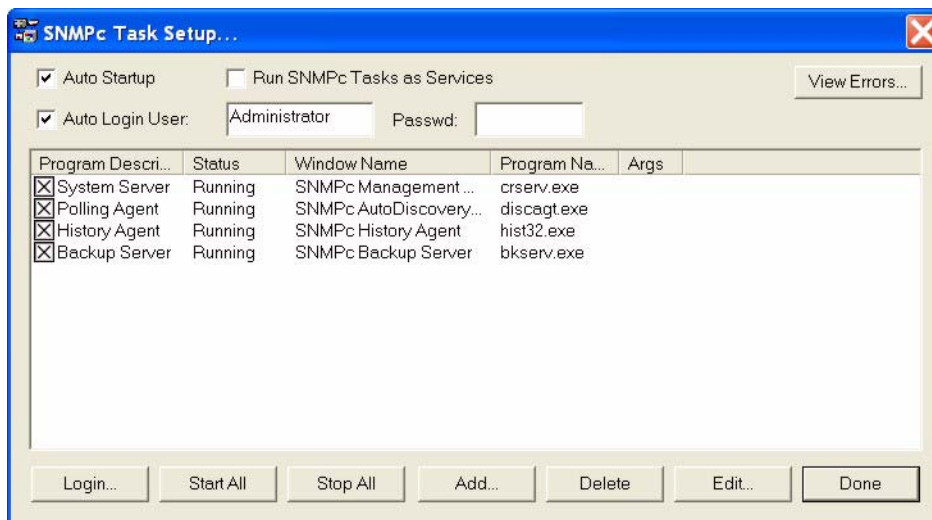
Click **Start, Programs, SNMPc, Startup System** to manually start the SNMPc network manager. This is the default location of the SNMPc network manager.

### Automatic Startup

To automatically start the SNMPc network manager each time you turn on your computer:

- 1 In SNMPc main window, click **Config, System Startup**.
- 2 Select the **Auto Startup** check box and click **Done**.

**Figure 126** Automatic Startup

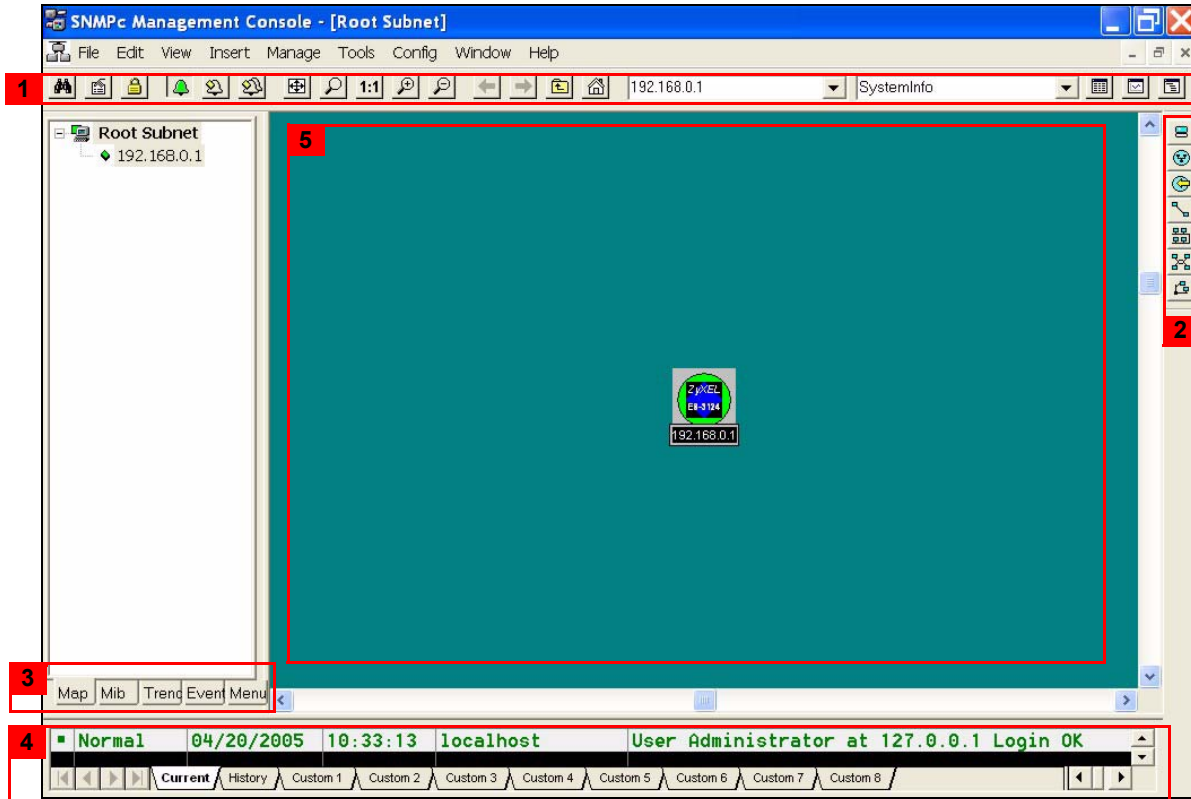




## SNMPc Main Window

The following figure and table show the elements of the SNMPc main window.

**Figure 127** SNMPc Main Windows



**Table 85** SNMPc Main Window

	ELEMENT	FUNCTION
1	Main Button Bar	Buttons and controls to execute common commands quickly. Hold the cursor over an icon to see a tool tip.
2	Edit Button Bar	Buttons to quickly insert map elements. Hold the cursor over an icon to see a tool tip.
3	Selection Tool	Tabbed control for selection of objects within different SNMPc functional modules.
4	Event Log Tool	Tabbed control for display of filtered event log entries.
5	View Window Area	Map View, Mib Tables and Mib Graph windows are shown here.

## Selection Tool

If you can't see the selection tool, click **View, Selection Tool** to display it. Use the selection tool to manipulate objects from one of several databases. Use the drag control at the right of the selection tool to change its size. Select one of the selection tool tabs to display a tree control for the database. Right-click on an icon inside a selection tree for database-specific commands.

**Table 86** Selection Tool

TAB	DESCRIPTION
Map	Map Object database, including devices and subnets.
Mib	Compiled SNMP Mibs, Custom Tables and Custom Mib Expressions.
Trend	Report profiles that define long-term polling procedures and scheduled reports.
Event	Event filters used to determine what happens when an event is received.
Menu	Custom menus that appear in the Manage, Tools and Help SNMPc menus.

## Event Log Tool

The event log tool displays different filtered views of the SNMPc event log. If you can't see the event log tool, click **View, Event Log Tool** to display it.

- Select the **Current** tab to show unacknowledged (current) events. These events have a colored box at the left side of the log entry. The color of map objects is determined by the highest priority unacknowledged event for that object.
- Select the **History** tab to show all events, including acknowledged and unacknowledged events.
- Select one of the **Custom** tabs and use the right-click **Filter View** menu to specify what events should be displayed for that tab.
- Double-click an event entry to display a **Map View** window with the corresponding device icon visible.
- To quickly view events for a particular device, first select the device and then use one of the **View Events** buttons (or the **View, Active Events** and **View, History Events** menus). This will show the device events in a separate window in the View Windows area.
- To remove one or more events, select the events and click the **Delete** key.
- To acknowledge (remove current status of) an event, right-click on an event entry and click **Acknowledge**.
- To completely clear the event log, click **File** and **Clear Events**.

## View Window Area

The View Window Area is the main interface for viewing the SNMPc map and command results. This area uses the Multi-Document-Interface (MDI) specification to display multiple windows at the same time. Click **Window** and select **Cascade**, **Tile Horizontally** or **Tile Vertically** to rearrange the windows in the View Window Area in a way that makes them all visible.

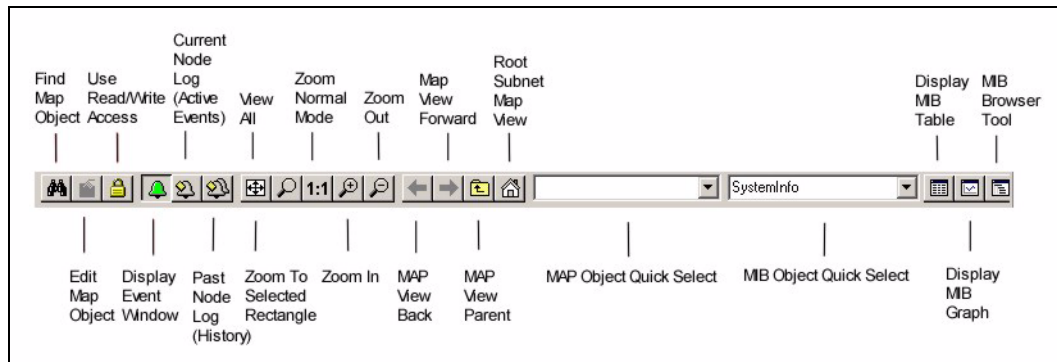
Windows in this area can be in one of several states:

- A **Maximized** window uses the entire area and hides any other windows behind it. If you close a maximized window, the next top-most window will still be displayed in the maximized state. You need to be careful when using maximized windows because it is easy to lose track of how many windows you have open and there is an upper limit. Use the Windows menu to see a list of windows. Click **Windows** and select either **Tile Horizontally** or **Tile Vertically** to view all windows at the same time.
- An **Overlapped** window does not take up the entire area. One window will be completely visible and other windows are partially hidden behind it. This is the most common situation for the View Window area because it lets you view maps, tables and graphs at the same time and quickly move between them. Click **Windows** and select **Cascade**.
- A **Minimized** window is displayed as a small title bar with window open/close buttons. Windows are not typically minimized within the View Window Area because, as with the maximized case, they can easily be lost behind other windows.

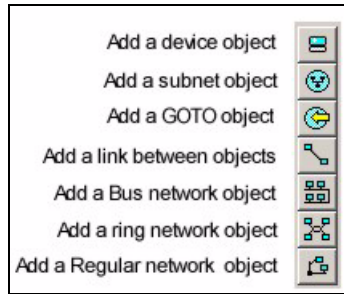
## Main and Edit Button Bar Icons

The following figure is a brief overview of the SNMPc main button and edit button bar icons.

**Figure 128** SNMPc Main Button Bar Icons



**Figure 129** SNMPc Edit Button Bar Icons



**Note:** For more detailed information, please see [www.castlerock.com](http://www.castlerock.com).



# Appendix B

## Alarm Types and Causes

This appendix shows examples of probable alarm types and causes.

**Table 87** Alarm Types and Causes

ALARM TYPE	PROBABLE CAUSES	
Communications	<ul style="list-style-type: none"> <li>• Loss of signal</li> <li>• Loss of frame</li> <li>• Framing error</li> <li>• Local node transmission error</li> <li>• Remote node transmission error</li> <li>• Call establishment error</li> </ul>	<ul style="list-style-type: none"> <li>• Degraded signal</li> <li>• Communications subsystem failure</li> <li>• Communications protocol error</li> <li>• LAN error</li> <li>• DTE-DCE interface error</li> </ul>
Quality of service	<ul style="list-style-type: none"> <li>• Response time excessive</li> <li>• Queue size exceeded</li> <li>• Bandwidth reduced</li> <li>• Retransmission rate excessive</li> </ul>	<ul style="list-style-type: none"> <li>• Threshold crossed</li> <li>• Performance degraded</li> <li>• Congestion</li> <li>• Resource at or nearing capacity</li> </ul>
Processing error	<ul style="list-style-type: none"> <li>• Storage capacity problem</li> <li>• Version mismatch</li> <li>• Corrupt data</li> <li>• CPU cycles limit exceeded</li> <li>• Software error</li> <li>• Software program error</li> </ul>	<ul style="list-style-type: none"> <li>• Software program abnormally terminated</li> <li>• File error</li> <li>• Out of memory</li> <li>• Underlying resource unavailable</li> <li>• Application subsystem failure</li> <li>• Configuration or customization error</li> </ul>
Equipment	<ul style="list-style-type: none"> <li>• Power problem</li> <li>• Timing problem</li> <li>• Processor problem</li> <li>• Dataset or modem error</li> <li>• Multiplexer problem</li> <li>• Receiver failure</li> <li>• Transmitter failure</li> </ul>	<ul style="list-style-type: none"> <li>• Receive failure</li> <li>• Transmit failure</li> <li>• Output device error</li> <li>• Input device error</li> <li>• I/O device error</li> <li>• Equipment malfunction</li> <li>• Adapter error</li> </ul>
Environmental	<ul style="list-style-type: none"> <li>• Temperature unacceptable</li> <li>• Humidity unacceptable</li> <li>• Heating/ventilation/cooling system problem</li> <li>• Fire detected</li> <li>• Flood detected</li> <li>• Toxic leak detected</li> </ul>	<ul style="list-style-type: none"> <li>• Leak detected</li> <li>• Pressure unacceptable</li> <li>• Excessive vibration</li> <li>• Material supply exhausted</li> <li>• Pump failure</li> <li>• Enclosure door open</li> </ul>



# Index

## Numerics

110V AC [4](#)  
230V AC [4](#)

## A

Abnormal Working Conditions [5](#)  
AC [4](#)  
Access EMS Troubleshooting [167](#)  
Accessories [4](#)  
Acts of God [5](#)  
Airflow [4](#)  
American Wire Gauge [4](#)  
Authority [3](#)  
AWG [4](#)

## B

Basement [4](#)

## C

Cables, Connecting [4](#)  
Certifications [3](#)  
Changes or Modifications [3](#)  
Charge [5](#)  
Circuit [3](#)  
Class B [3](#)  
Class of Service (CoS) [142](#)  
Communications [3](#)  
Compatible MVR mode [159](#)  
Compliance, FCC [3](#)  
Components [5](#)  
Condition [5](#)

Connecting Cables [4](#)  
Consequential Damages [5](#)  
Contact Information [6](#)  
Contacting Customer Support [6](#)  
Copyright [2](#)  
Correcting Interference [3](#)  
Corrosive Liquids [4](#)  
Covers [4](#)  
Customer Support [6](#)

## D

Damage [4](#)  
Dampness [4](#)  
Danger [4](#)  
Dealer [3](#)  
Defective [5](#)  
Denmark, Contact Information [6](#)  
DHCP  
    Relay agent [118](#)  
    Remote DHCP server [119](#)  
DiffServ  
    DS field [127](#)  
    DSCP [142](#)  
    PHB [127](#)  
Disclaimer [2](#)  
Discretion [5](#)  
DS (Differentiated Services) [127](#)  
DSCP  
    Service level [127](#)  
    What it does [127](#)  
DSCP (DiffServ Code Point) [142](#)  
Dust [4](#)  
Dynamic MVR mode [159](#)

## E

Electric Shock [4](#)  
Electrical Pipes [4](#)



Electrocution [4](#)  
Element Management System [24](#)  
Equal Value [5](#)  
Europe [4](#)  
Exposure [4](#)

## F

Failure [5](#)  
FCC [3](#)  
    Compliance [3](#)  
    Rules, Part 15 [3](#)  
Federal Communications Commission [3](#)  
Finland, Contact Information [6](#)  
Fitness [5](#)  
France, Contact Information [6](#)  
Functionally Equivalent [5](#)

## G

Gas Pipes [4](#)  
Germany, Contact Information [6](#)  
God, act of [5](#)

## H

Hardware [24](#)  
Harmful Interference [3](#)  
High Voltage Points [4](#)

## I

IGMP snooping [154](#), [158](#)  
Indirect Damages [5](#)  
Insurance [5](#)  
Interference [3](#)  
Interference Correction Measures [3](#)  
Interference Statement [3](#)

## L

Labor [5](#)  
LAN Setup [98](#)  
Legal Rights [5](#)  
Liability [2](#)  
License [2](#)  
Lightning [4](#)  
Liquids, Corrosive [4](#)

## M

Materials [5](#)  
Media-on-Demand (MoD) [158](#)  
Merchantability [5](#)  
Mirror port [125](#)  
Modifications [3](#)  
Multicast VLAN Registration (MVR) [158](#)  
MVR [158](#)  
MVR modes [159](#)  
MVR ports [159](#)

## N

Network Management System [24](#)  
New [5](#)  
NMS [24](#)  
North America [4](#)  
North America Contact Information [6](#)  
Norway, Contact Information [6](#)

## O

Opening [4](#)  
Operating Condition [5](#)  
Out-dated Warranty [5](#)  
Outlet [3](#)

## P

Parts [5](#)  
Patent [2](#)

Permission [2](#)  
PHB (Per-Hop Behavior) [127](#)  
Photocopying [2](#)  
Pipes [4](#)  
Pool [4](#)  
Port mirroring [125](#)  
    Mirror port [125](#)  
Postage Prepaid. [5](#)  
Power Adaptor [4](#)  
Power Cord [4](#)  
Power Outlet [4](#)  
Power Supply [4](#)  
Power Supply, repair [4](#)  
Product Model [6](#)  
Product Page [3](#)  
Product Serial Number [6](#)  
Products [5](#)  
Proof of Purchase [5](#)  
Proper Operating Condition [5](#)  
Purchase, Proof of [5](#)  
Purchaser [5](#)

## Q

Qualified Service Personnel [4](#)

## R

Radio Communications [3](#)  
Radio Frequency Energy [3](#)  
Radio Interference [3](#)  
Radio Reception [3](#)  
Radio Technician [3](#)  
Receiving Antenna [3](#)  
Registered [2](#)  
Registered Trademark [2](#)  
Regular Mail [6](#)  
Related Documentation [22](#)  
Relocate [3](#)  
Re-manufactured [5](#)  
Removing [4](#)  
Reorient [3](#)  
Repair [4, 5](#)  
Replace [5](#)  
Replacement [5](#)  
Reproduction [2](#)

Restore [5](#)  
Return Material Authorization (RMA) Number [5](#)  
Returned Products [5](#)  
Returns [5](#)  
Rights [2](#)  
Rights, Legal [5](#)  
Risk [4](#)  
RMA [5](#)

## S

Safety Warnings [4](#)  
Separation Between Equipment and Receiver [3](#)  
Serial Number [6](#)  
Service [4, 5](#)  
Service Personnel [4](#)  
Shipping [5](#)  
Shock, Electric [4](#)  
SNMPc Network Manager [24](#)  
Software [24](#)  
Spain, Contact Information [6](#)  
Supply Voltage [4](#)  
Support E-mail [6](#)  
Supporting Disk [22](#)  
Sweden, Contact Information [6](#)  
Swimming Pool [4](#)  
Switch Manager [26](#)  
Syntax Conventions [22](#)  
System [24](#)

## T

Tampering [5](#)  
Telecommunication Line Cord. [4](#)  
Telephone [6](#)  
Television Interference [3](#)  
Television Reception [3](#)  
Thunderstorm [4](#)  
Trademark [2](#)  
Trademark Owners [2](#)  
Trademarks [2](#)  
Translation [2](#)  
TV Technician [3](#)  
Type of Service (ToS) [127](#)

## U

Undesired Operations [3](#)

## V

Value [5](#)

Vendor [4](#)

Ventilation Slots [4](#)

Viewing Certifications [3](#)

Voltage Supply [4](#)

Voltage, High [4](#)

## W

Wall Mount [4](#)

Warnings [4](#)

Warranty [5](#)

Warranty Information [6](#)

Warranty Period [5](#)

Water [4](#)

Water Pipes [4](#)

Web Site [6](#)

Wet Basement [4](#)

Workmanship [5](#)

Worldwide Contact Information [6](#)

Written Permission [2](#)

## Z

Zero configuration Internet access [98](#)

ZyNOS [2](#)

ZyXEL Communications Corporation [2](#)

ZyXEL Home Page [3](#)

ZyXEL Limited Warranty

Note [5](#)

ZyXEL Network Operating System [2](#)