# *NetAtlas Enterprise 1.00*

*Element Management System*

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

Version 1.00
8/2005

ZyXEL

# Copyright

## 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

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

| METHOD | SUPPORT E-MAIL | TELEPHONE[A] | WEB SITE | REGULAR MAIL |
|---|---|---|---|---|
| LOCATION | SALES E-MAIL | FAX | FTP SITE | |
| **UNITED KINGDOM** | support@zyxel.co.uk | +44 (0) 1344 303044<br>08707 555779 (UK only) | 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) 1344 303034 | ftp.zyxel.co.uk | |

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

# Table of Contents

# List of Figures

# List of Tables

# Preface

Congratulations on your purchase of the NetAtlas Enterprise 1.00 Element Management System (EMS) for the ES-3124 Series.

**Note:** Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at 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 choices.
- 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 Element Management System for ES-3124 Series 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.
- ES-3124 User’s Guide or the ES-3124PWR User’s Guide

  Refer to the ES 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 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 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 Introducing the EMS

## 1.1 EMS Overview

The Element Management System (EMS) retrieves management information from switches using 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 switches in the NMS. The ES-3124 Series covers the ES-3124 and the ES-3124PWR.

### 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 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 IV, 1.6 GHz or above | Operating System: Windows 2000 (with service pack 1), Windows XP or Windows 2003 Server. |
| Memory (RAM): 1 GB or more | Database Program: MySQL 4.0.18 with ODBC 3.51.05 or later versions.<br>Please see www.mysql.com for details on MySQL. |
| Hard Disk free space: 20 GB | Castle Rock’s SNMPc 7.0 (Enterprise or Workgroup edition) |
| Screen Resolution: 1024x768 pixels | Ethernet Adaptor: 10/100 Mbps |

## 1.3 EMS Installation Overview

The following steps give an overview of what you need to do to install the EMS:

1 Install SNMPc

2 Install MySQL

3 Install the EMS software. Install the MySQL driver during the EMS installation.

4 Add custom MIB files in SNMPc

5 Locate device(s) that you want the EMS to manage

6 Configure the MySQL ODBC driver to connect to MySQL database.

### 1.3.1 Installing the EMS

Follow the steps below to install the EMS server on a computer.

1 Install SNMPc if it is not already installed. See the appendices for futher information.

2 Install MySQL. If it is already installed skip to step 11.

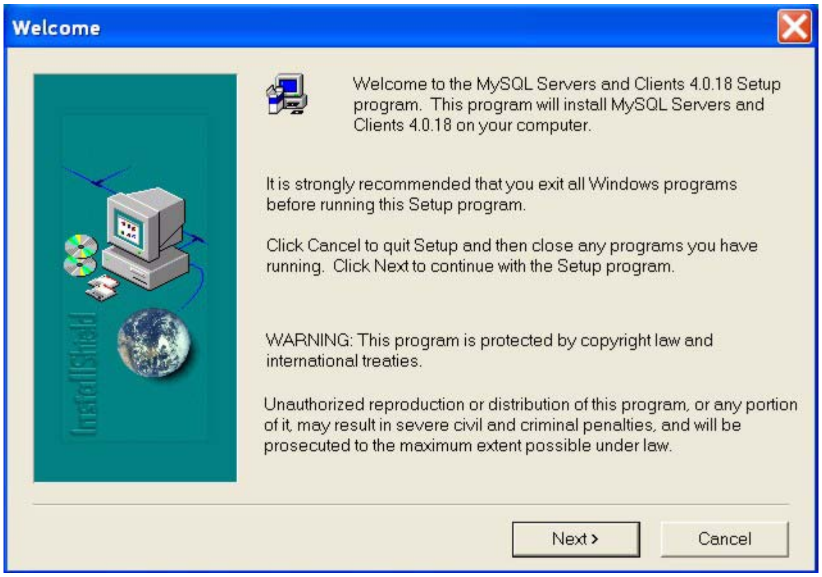
**Note:** You must install MySQL and the EMS on the same computer.

3 Find and **unzip the mysql-4.0.18-win** file on your CD.

4 Find and double-click the **setup.exe** file.

5 A **Welcome** screen displays. Click **Next** to continue.

**Figure 1** Installing MySQL: Welcome



Welcome to the MySQL Servers and Clients 4.0.18 Setup program. This program will install MySQL Servers and Clients 4.0.18 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

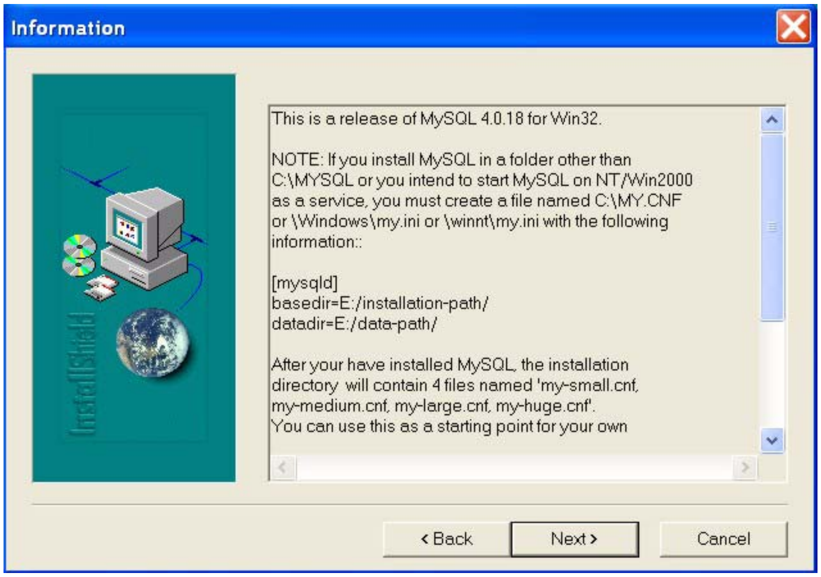
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

6 An **Information** screen displays. Click **Next** to continue.

**Figure 2** Installing MySQL: Information



This is a release of MySQL 4.0.18 for Win32.

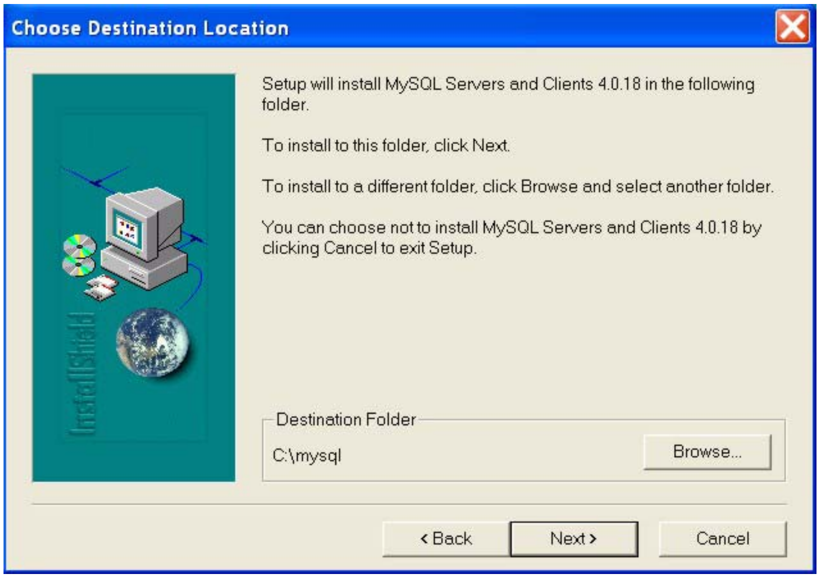
NOTE: If you install MySQL in a folder other than C:\MYSQL or you intend to start MySQL on NT/Win2000 as a service, you must create a file named C:\MY.CNF or \Windows\my.ini or \winnt\my.ini with the following information::

```
[mysqld]
basedir=E:/installation-path/
datadir=E:/data-path/
```

After your have installed MySQL, the installation directory will contain 4 files named 'my-small.cnf, my-medium.cnf, my-large.cnf, my-huge.cnf'.
You can use this as a starting point for your own

7 Click **Browse** if you want to install MySQL to a destination folder other than the destination shown.

**Figure 3** Installing MySQL: Choose Destination Location



Setup will install MySQL Servers and Clients 4.0.18 in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

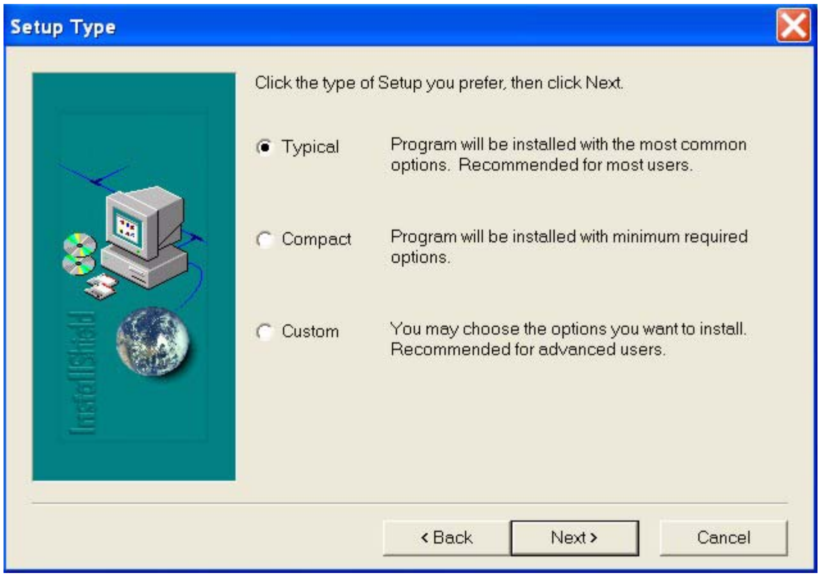
You can choose not to install MySQL Servers and Clients 4.0.18 by clicking Cancel to exit Setup.

Destination Folder

C:\mysql

8 You must select a setup type to install MySQL. Select **Typical** and click **Next** to continue.

**Figure 4** Installing MySQL: Setup Type



Click the type of Setup you prefer, then click Next.

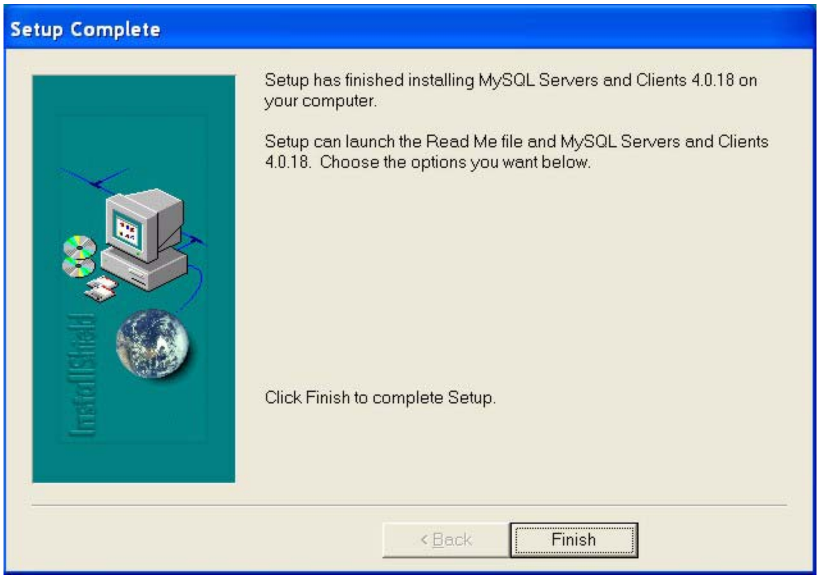
● Typical — Program will be installed with the most common options. Recommended for most users.

○ Compact — Program will be installed with minimum required options.

○ Custom — You may choose the options you want to install. Recommended for advanced users.

**9** Click **Finish** to complete the MySQL installation.

**Figure 5** Installing MySQL: Setup Complete



Setup has finished installing MySQL Servers and Clients 4.0.18 on your computer.

Setup can launch the Read Me file and MySQL Servers and Clients 4.0.18. Choose the options you want below.

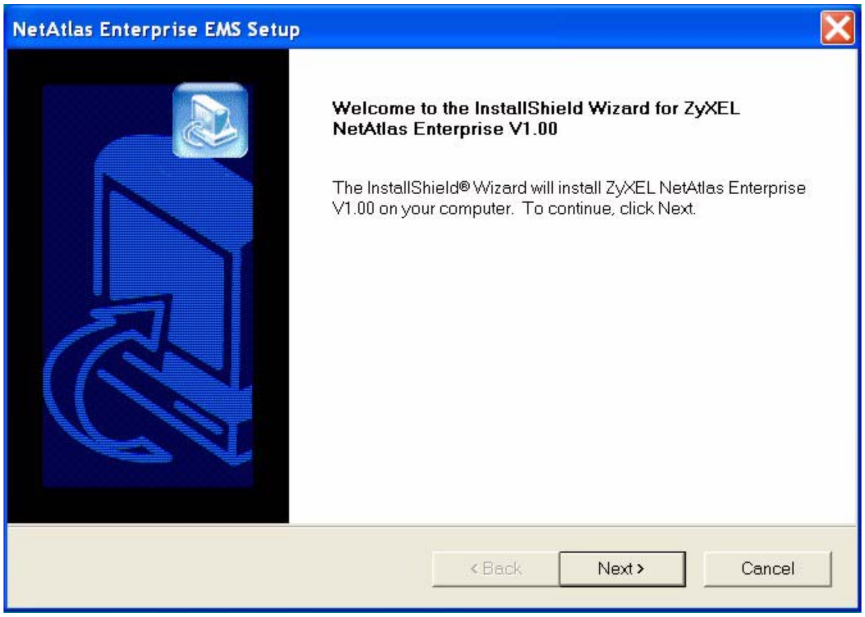
Click Finish to complete Setup.

**10** You must restart Windows to activate MySQL.

**11** Find and double-click **NetAtlasEnterprise_S100.exe** on your EMS CD.

**12** A **Welcome** screen displays. Click **Next** to continue.

**Figure 6** Installing EMS: Welcome



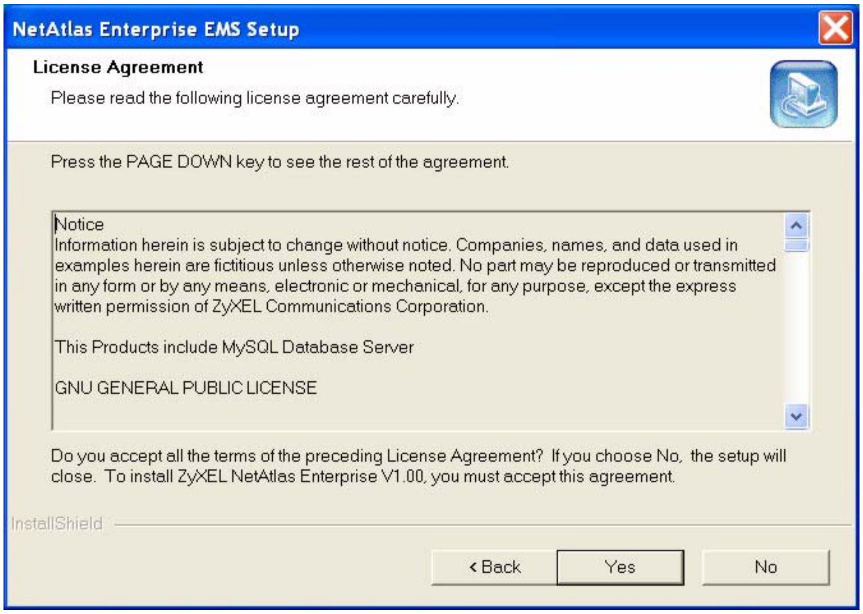
NetAtlas Enterprise EMS Setup

**Welcome to the InstallShield Wizard for ZyXEL NetAtlas Enterprise V1.00**

The InstallShield® Wizard will install ZyXEL NetAtlas Enterprise V1.00 on your computer. To continue, click Next.

**13** Read the license agreement. Click **Yes** to accept the agreement.

**Figure 7** Installing EMS: License Agreement



NetAtlas Enterprise EMS Setup

**License Agreement**

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

Notice
Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

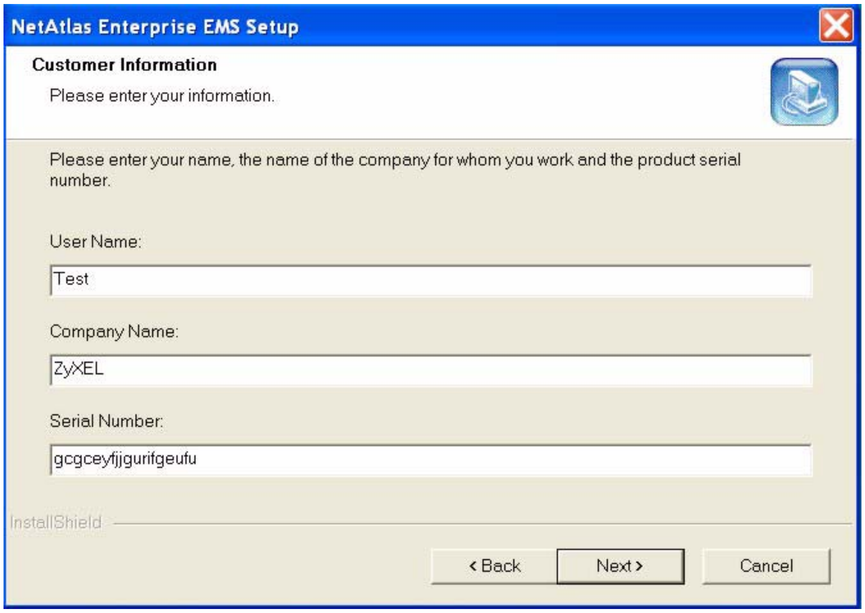
This Products include MySQL Database Server

GNU GENERAL PUBLIC LICENSE

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install ZyXEL NetAtlas Enterprise V1.00, you must accept this agreement.

**14** Type your name, company name and product serial number in the following screen. Click **Next** to continue.

**Figure 8** Installing EMS: Customer Information



NetAtlas Enterprise EMS Setup

Customer Information

Please enter your information.

Please enter your name, the name of the company for whom you work and the product serial number.

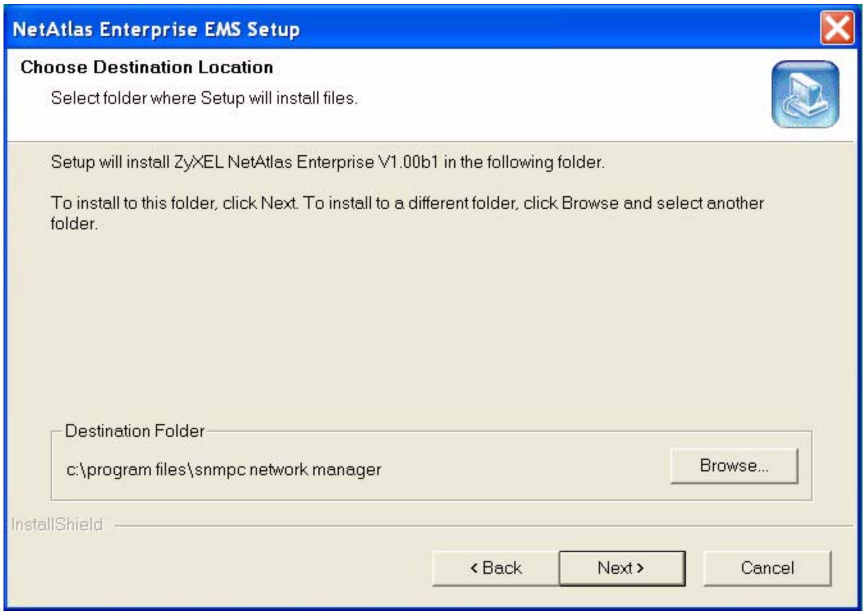
User Name: Test

Company Name: ZyXEL

Serial Number: gcgceyfjjgurifgeufu

**15** You must select the same directory where you installed SNMPc. Click **Browse** if it's different from the destination folder shown.

**Figure 9** Installing EMS: Choose Destination Location



NetAtlas Enterprise EMS Setup

Choose Destination Location

Select folder where Setup will install files.

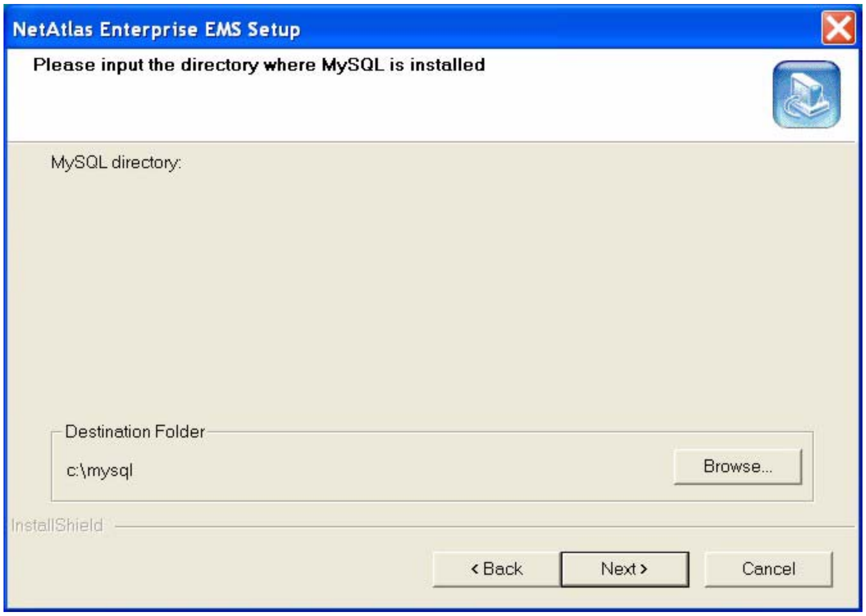
Setup will install ZyXEL NetAtlas Enterprise V1.00b1 in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder: c:\program files\snmpc network manager

**16** You must select the directory where you installed MySQL. Click **Browse** if you did not install MySQL database in the default folder shown. Click **Next**.

**Figure 10** Installing EMS: Specify MySQL Directory



NetAtlas Enterprise EMS Setup

Please input the directory where MySQL is installed

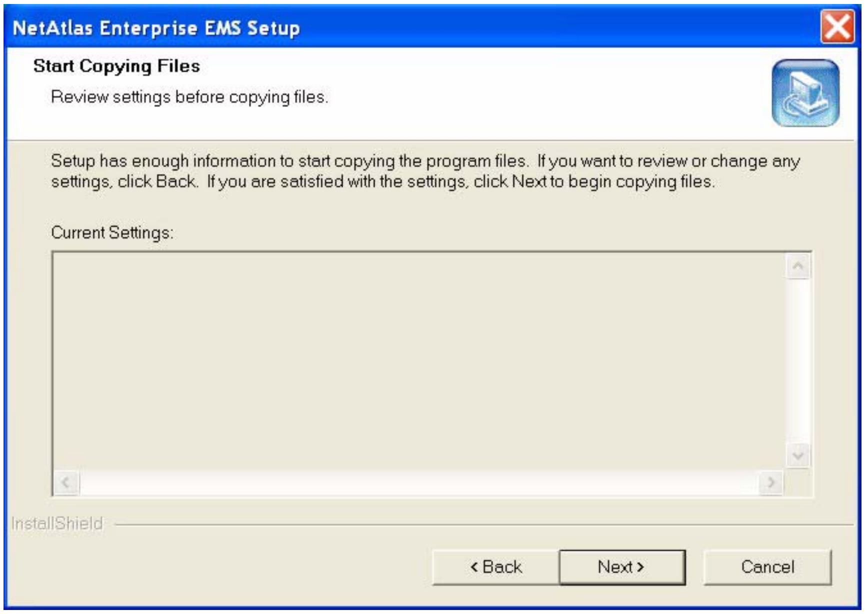
MySQL directory:

Destination Folder

c:\mysql

**17** In the next screen, click **Next** to begin the installation and start copying files.

**Figure 11** Installing EMS: Start Copying Files



NetAtlas Enterprise EMS Setup

Start Copying Files

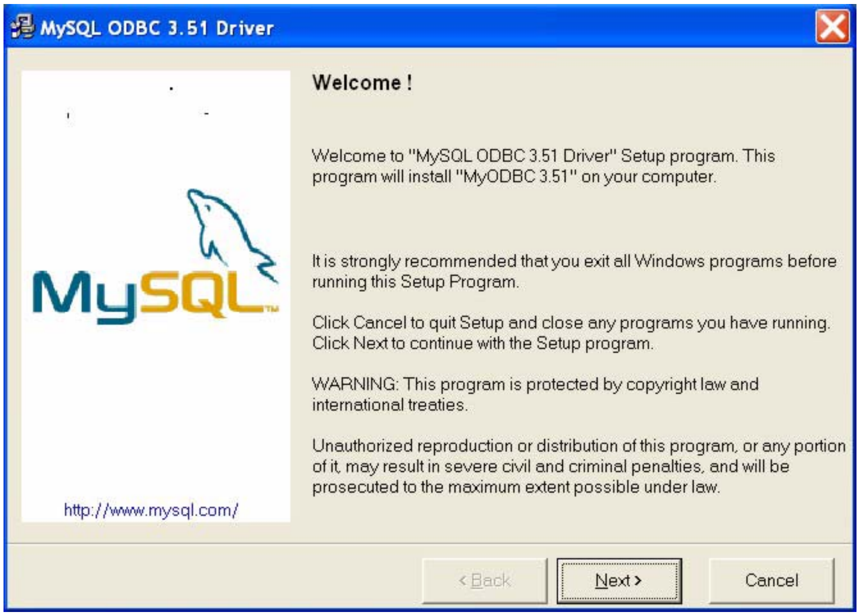
Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

**18** When a **Welcome** screen displays. Click **Next** to install the MySQL ODBC driver.

**Figure 12** Installing EMS: MySQL ODBC: Welcome



Welcome !

Welcome to "MySQL ODBC 3.51 Driver" Setup program. This program will install "MyODBC 3.51" on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup Program.

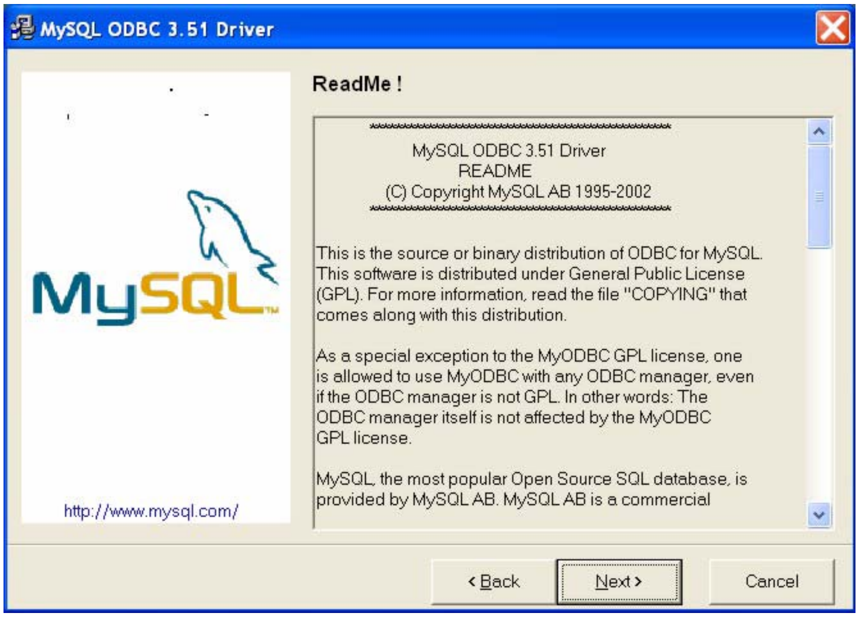
Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

**19** Read the license agreement. Click **Next** to accept the agreement.

**Figure 13** Installing EMS: MySQL ODBC: License Agreement



ReadMe !

```
        MySQL ODBC 3.51 Driver
               README
   (C) Copyright MySQL AB 1995-2002
```

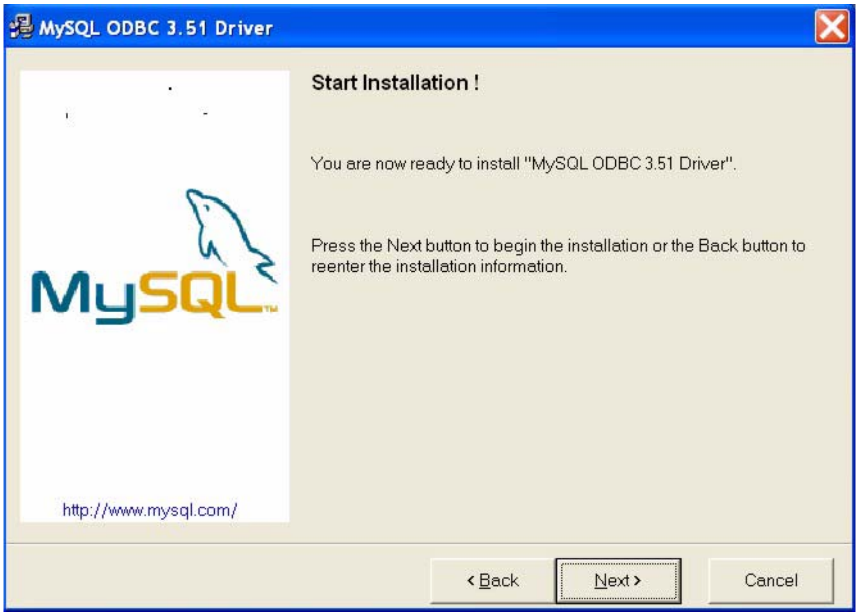
This is the source or binary distribution of ODBC for MySQL. This software is distributed under General Public License (GPL). For more information, read the file "COPYING" that comes along with this distribution.

As a special exception to the MyODBC GPL license, one is allowed to use MyODBC with any ODBC manager, even if the ODBC manager is not GPL. In other words: The ODBC manager itself is not affected by the MyODBC GPL license.

MySQL, the most popular Open Source SQL database, is provided by MySQL AB. MySQL AB is a commercial

**20** Click **Next** again to begin the MySQL ODBC driver installation.

**Figure 14** Installing EMS: MySQL ODBC: Start Installing



MySQL ODBC 3.51 Driver

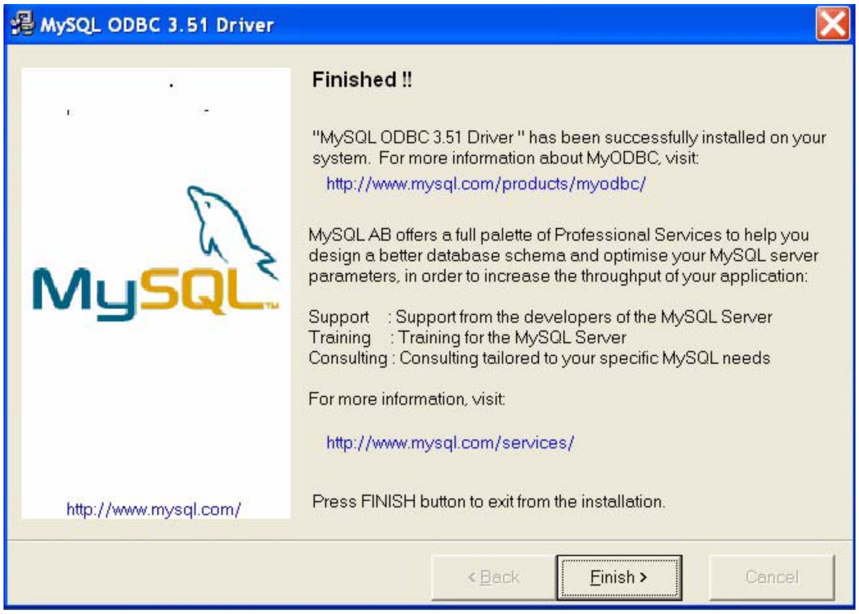
**Start Installation !**

You are now ready to install "MySQL ODBC 3.51 Driver".

Press the Next button to begin the installation or the Back button to reenter the installation information.

**21** Click **Finish** to complete the MySQL ODBC installation.

**Figure 15** Installing EMS: MySQL ODBC: Finish



MySQL ODBC 3.51 Driver

**Finished !!**

"MySQL ODBC 3.51 Driver " has been successfully installed on your system. For more information about MyODBC, visit:

http://www.mysql.com/products/myodbc/

MySQL AB offers a full palette of Professional Services to help you design a better database schema and optimise your MySQL server parameters, in order to increase the throughput of your application:

Support : Support from the developers of the MySQL Server
Training : Training for the MySQL Server
Consulting : Consulting tailored to your specific MySQL needs

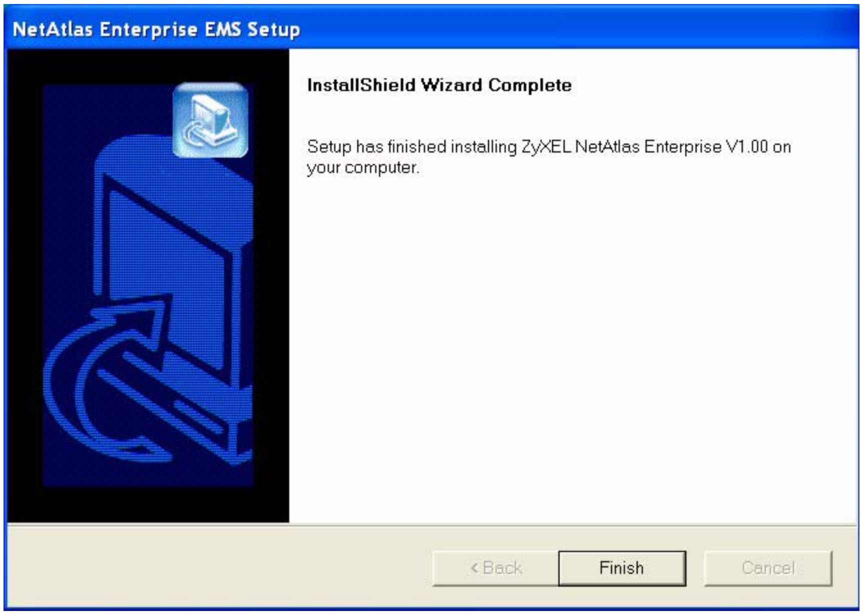
For more information, visit:

http://www.mysql.com/services/

Press FINISH button to exit from the installation.

**22** In the final screen of the EMS wizard, click **Finish** to complete the EMS installation.

**Figure 16** Installing EMS: Finish



NetAtlas Enterprise EMS Setup

InstallShield Wizard Complete

Setup has finished installing ZyXEL NetAtlas Enterprise V1.00 on your computer.

# 1.4 SNMPc Network Manager

Start the SNMPc Network Manager manually or have it start automatically each time you turn on your computer.

## 1.4.1 Manual SNMPc Startup

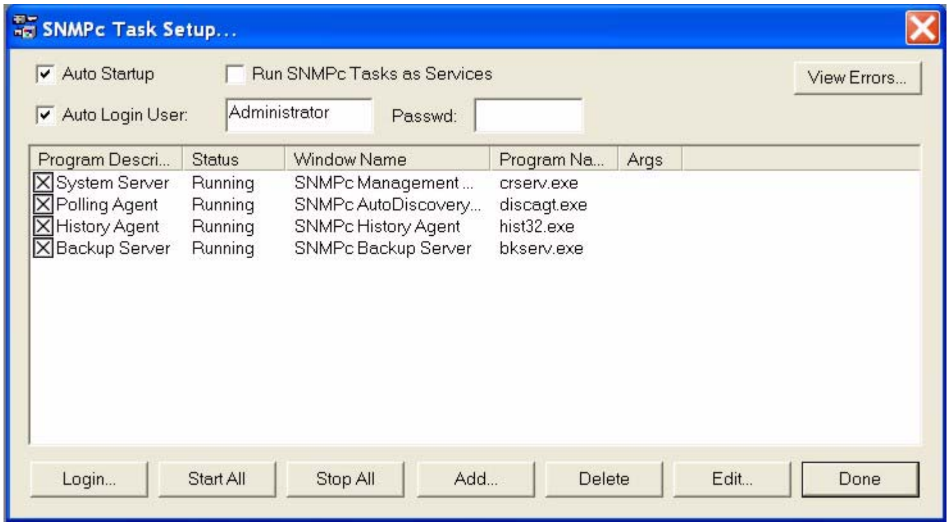
Manually starting SNMPc depends on your operating system. In Windows 2000, click **Start**, **Programs**, **SNMPc Network Manager**, **Startup System** to start the SNMPc Network Manager.

## 1.4.2 Automatic SNMPc Startup

To start SNMPc automatically each time you turn on your computer, first click **Config**, **System Startup**.

Then, select **Auto Startup** and finally click **OK**. Conversely, clear this checkbox if you do not wish SNMPc to automatically start each time you turn on your computer.

**Figure 17** SNMPc Task Setup



SNMPc Task Setup...

☑ Auto Startup  □ Run SNMPc Tasks as Services

☑ Auto Login User: Administrator  Passwd:

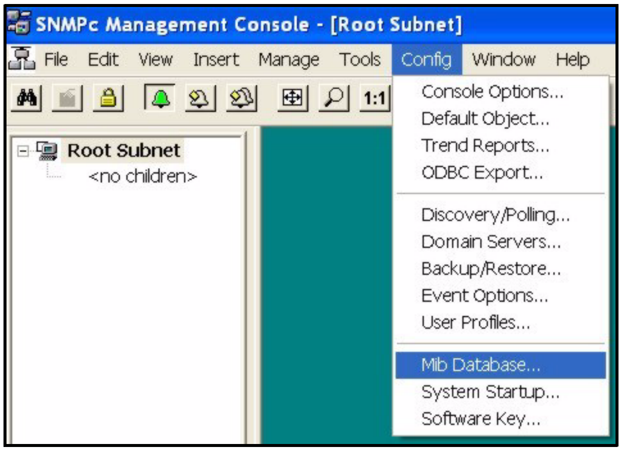
| Program Descri... | Status | Window Name | Program Na... | Args |
|---|---|---|---|---|
| ☒ System Server | Running | SNMPc Management ... | crserv.exe | |
| ☒ Polling Agent | Running | SNMPc AutoDiscovery... | discagt.exe | |
| ☒ History Agent | Running | SNMPc History Agent | hist32.exe | |
| ☒ Backup Server | Running | SNMPc Backup Server | bkserv.exe | |

## 1.5 Adding MIBs

The Management Information Base (MIB) is designed for holding management information on systems such as the MSC that the standard MIB does not include.

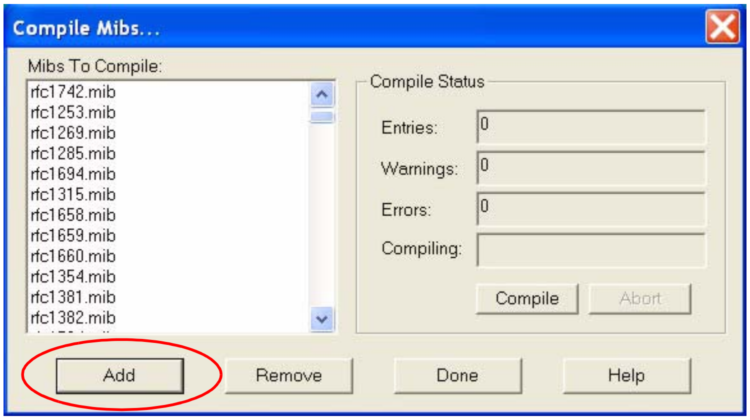
**1** From the SNMPc Network Manager main screen, click **Config**, **MIB Database**.

**Figure 18** Config: MIB Database



**2** Click **Add** in the **Compile Mibs** screen.

**Figure 19** Compile Mibs (First Screen)

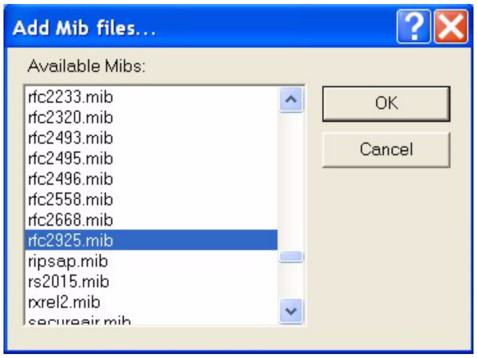


rfc1742.mib
rfc1253.mib
rfc1269.mib
rfc1285.mib
rfc1694.mib
rfc1315.mib
rfc1658.mib
rfc1659.mib
rfc1660.mib
rfc1354.mib
rfc1381.mib
rfc1382.mib

Entries: 0
Warnings: 0
Errors: 0
Compiling:

3 Scroll down the **Add Mibs** dialog box and select the MIB: **rfc2674.mib** (P-BRIDGE-MIB). Click **OK**.

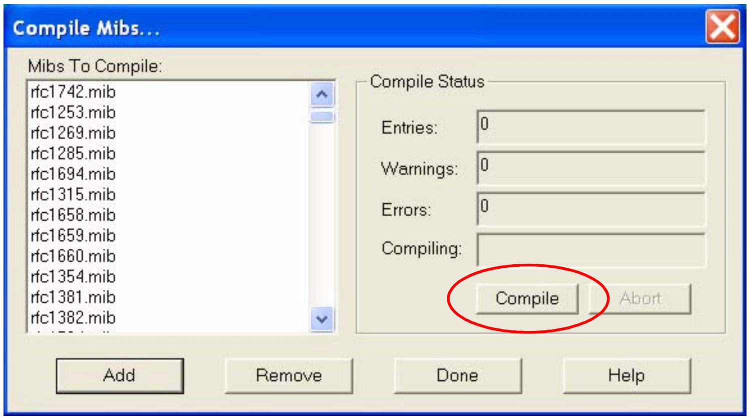
**Figure 20** Add Mib Files



rfc2233.mib
rfc2320.mib
rfc2493.mib
rfc2495.mib
rfc2496.mib
rfc2558.mib
rfc2668.mib
rfc2925.mib
ripsap.mib
rs2015.mib
rxrel2.mib
secureair.mib

4 Click **Compile** in the **Compile Mibs** screen.

**Figure 21** Compile Mibs (Second Screen)

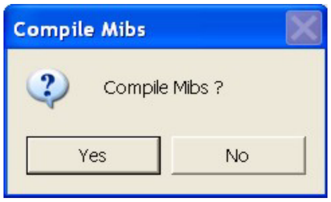


rfc1742.mib
rfc1253.mib
rfc1269.mib
rfc1285.mib
rfc1694.mib
rfc1315.mib
rfc1658.mib
rfc1659.mib
rfc1660.mib
rfc1354.mib
rfc1381.mib
rfc1382.mib

Entries: 0
Warnings: 0
Errors: 0
Compiling:

5 Click **Yes** when asked to confirm, then click **OK**.

**Figure 22** Compile Mibs



6 Repeat Steps 2 to 5 for the following;

- rfc2925.mib (DISMAN-PING-MIB)
- rfc3291.mib (INET-ADRESS-MIB)
- rfc3621.mib (POWER-ETHERNET-MIB)
- zyxel.mib
- zyxel-es3124.mib
- zyxel-es3124pwr.mib.

**Note:** You must add and compile the MIBs separately in the order specified.

7 Finally click **Done** in the **Compile Mibs** screen.

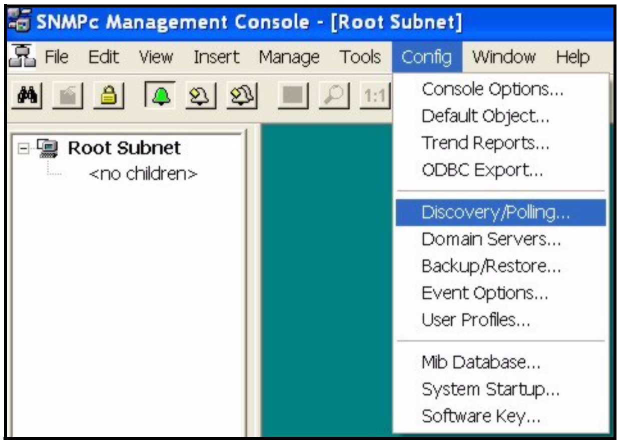
# 1.6 Finding your Switch

The SNMPc Network Manager can find new devices automatically using auto-discovery (enabled by default) or you will have to add device(s) manually.

## 1.6.1 Device Auto-Discovery

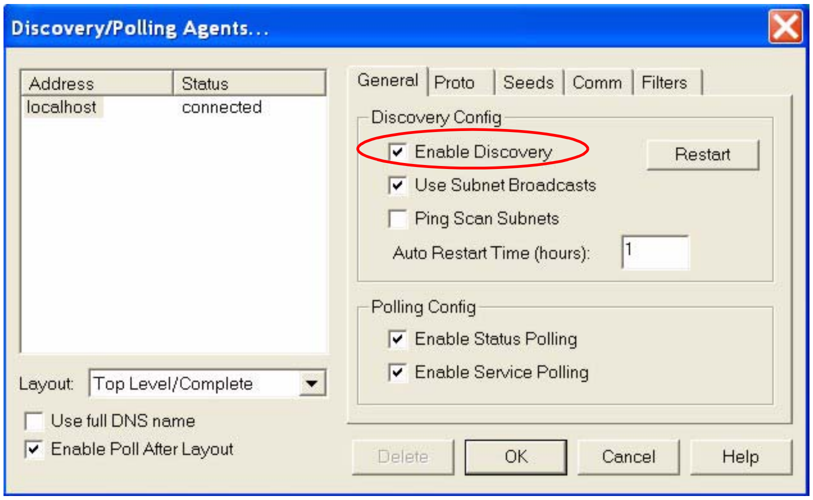
1 To enable auto-discovery and then find your device, click **Config**, **Discovery/Polling**.

**Figure 23** Config, Discovery Agents



2 Select the **Enable Discovery** check box and click **OK**.

**Figure 24** Discovery Agents Screen



Discovery/Polling Agents...

| Address | Status |
|---|---|
| localhost | connected |

Layout: Top Level/Complete

□ Use full DNS name

☑ Enable Poll After Layout

Discovery Config

☑ Enable Discovery

☑ Use Subnet Broadcasts

□ Ping Scan Subnets

Auto Restart Time (hours): 1

Polling Config

☑ Enable Status Polling

☑ Enable Service Polling

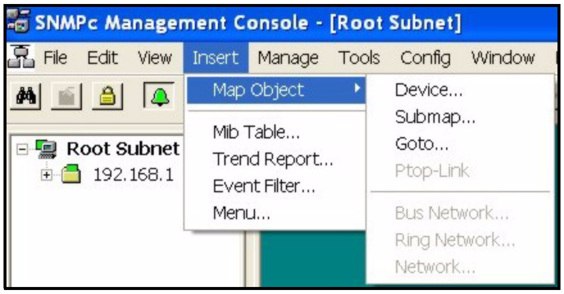
3 Find your device in the **Device List** panel. Double-click the device icon to access the EMS.

## 1.6.2 Add Device(s) Manually

If you have disabled auto-discovery, follow the steps below to add your device(s) manually.

1 Click **Insert**, **MAP Object**, **Device**.

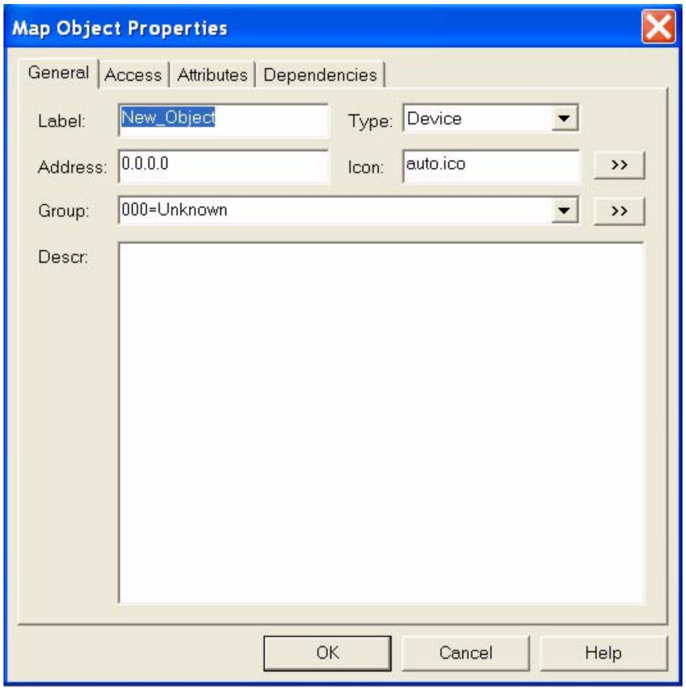
**Figure 25** Insert, MAP Object, Device



SNMPc Management Console - [Root Subnet]

2 Fill in the **MAP Object Properties** screen and then click **OK**.

**Figure 26** Map Object Properties: Generall



Label: New_Object

Type: Device

Address: 0.0.0.0

Icon: auto.ico

Group: 000=Unknown

**Table 2** Map Object Properties: General

| FIELD | DESCRIPTION |
|---|---|
| Label | Type a device name for identification purposes. If you do not configure this field, the default label is “New Object”. |
| Type | This field shows what type of device it is, for example a hub, workstation, router etc. This field displays **Device** for the switch. |
| Address | Type the IP address of the switch. |
| Icon | You may change the default icon by clicking **>>** and then choosing a different icon. |
| Group | This is the group number associated with this type of device. This field is optional. |
| Descr | Type a description of your device in this (optional) field. |

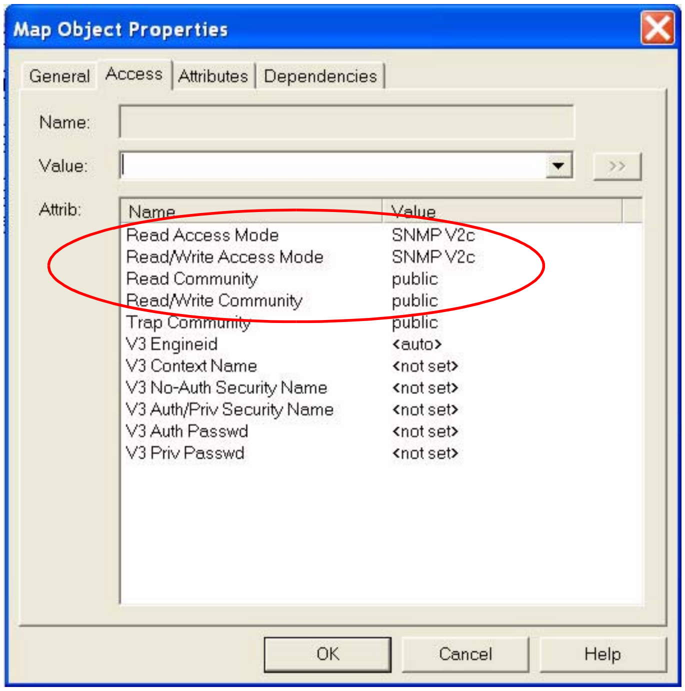
# 1.7 Using SNMP

Check that you are using SNMPv2c. If you are not using SNMPv2c, you must uninstall any previous versions and install SNMPv2c. Refer to *RFC 1901* for more information on SNMP Version 2c (SNMPv2c). Follow this procedure to use SNMPv2c.

**1** Right-click the **Device** icon and select **Properties**.

**2** Click the **Access** tab.

**Figure 27** Map Object Properties



Name:

Value:

Attrib:

| Name | Value |
|---|---|
| Read Access Mode | SNMP V2c |
| Read/Write Access Mode | SNMP V2c |
| Read Community | public |
| Read/Write Community | public |
| Trap Community | public |
| V3 Engineid | <auto> |
| V3 Context Name | <not set> |
| V3 No-Auth Security Name | <not set> |
| V3 Auth/Priv Security Name | <not set> |
| V3 Auth Passwd | <not set> |
| V3 Priv Passwd | <not set> |

3 Follow the instructions in the table below to set the specified fields in the **Map Object Properties** screen.

**Table 3** Required Map Object Properties

| FIELD | VALUE |
|---|---|
| Read Access Mode | "SNMPV2c" |
| Read/Write Access Mode | "SNMPV2c" |
| Read Community field | For initial configuration, "public" is the default for most devices. After initial configuration, you assign this field. |
| Read/Write Community field | For initial configuration, "public" is the default for most devices. After initial configuration, you assign this field. |

**Note:** For security purposes, we strongly recommend you change the **Read Community** and **Read Read/Write Community** defaults.

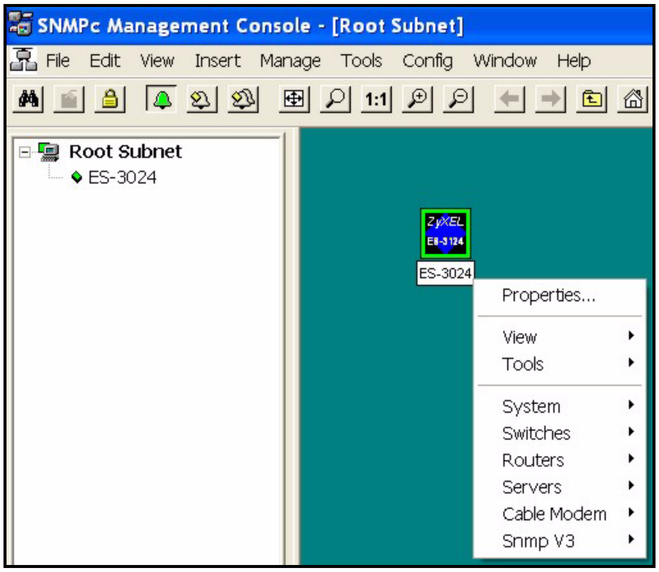
Write down this information in a secure place so you will not forget it later!

4 Click **OK**.

After the device has been found, the icon and label appear in the network manager view window.

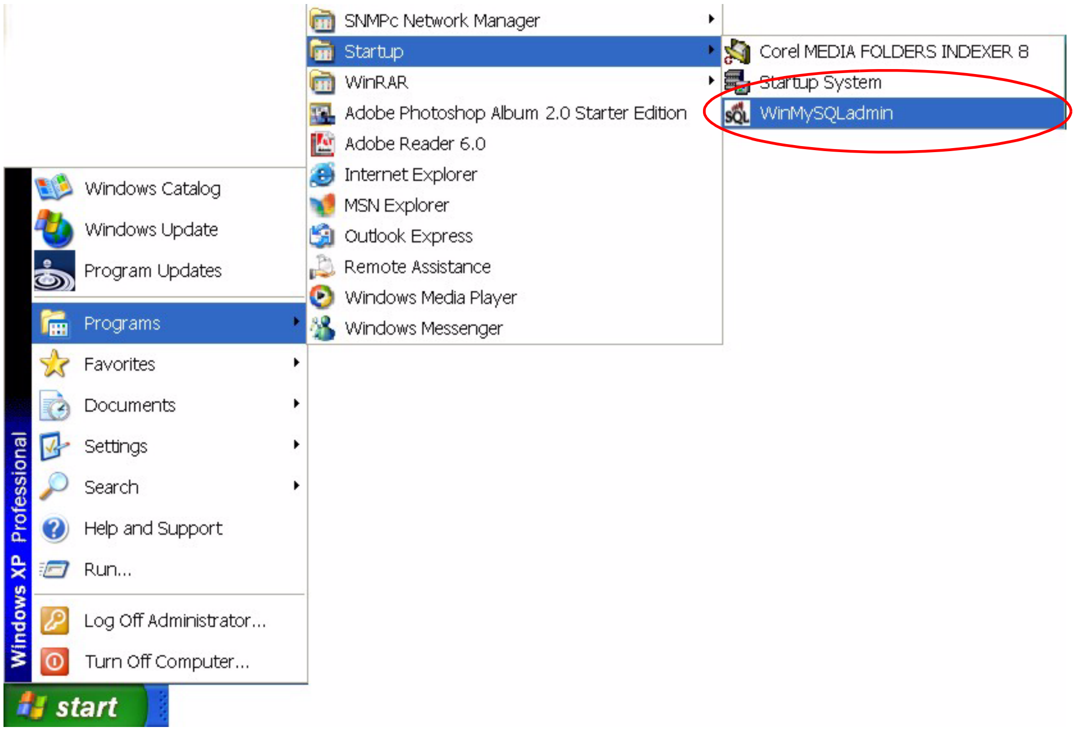
5 Right-click on the device icon to view a set of SMNPc network manager shortcuts. Click **Properties** to verify the information you entered in the previous step.

**Figure 28** Network Manager Shortcuts



**6** Make sure the MySQL database is running. You must restart windows after you install MySQL. MySQL should start automatically when you restart Windows. If it does not, click **start**, **Programs**, **Startup** and then click **WinMySQLadmin**.

**Figure 29** Startup MySQL



## 1.8 Configuring MySQL ODBC Driver

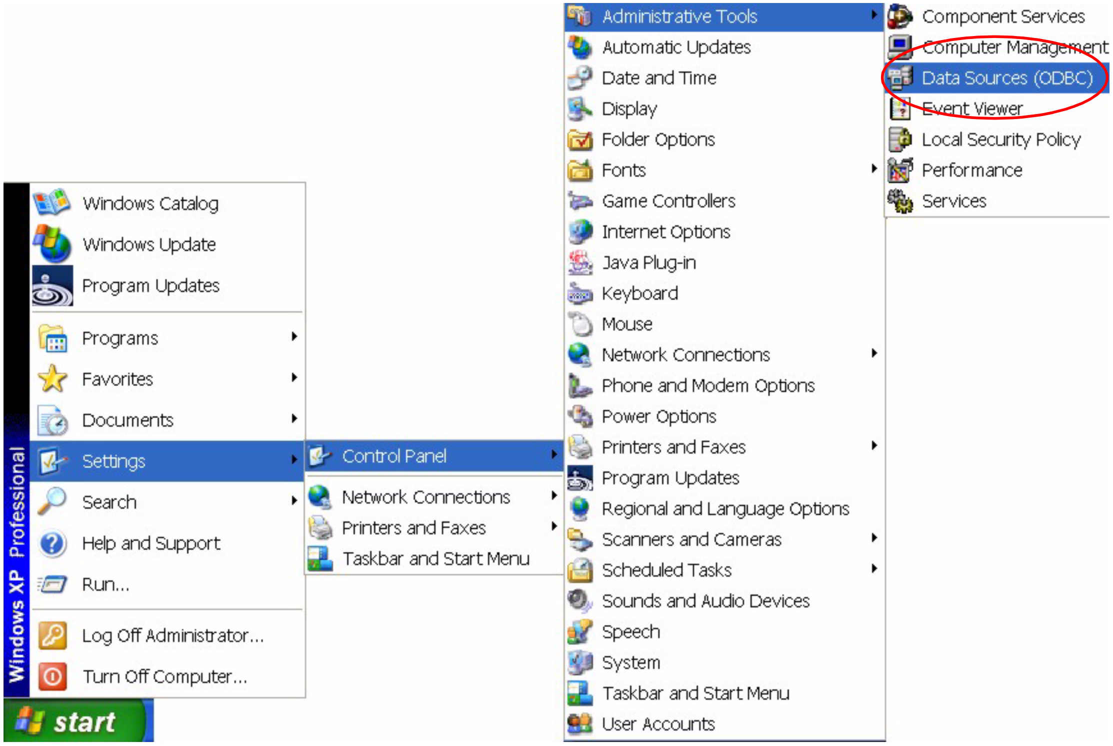
The MySQL driver should already be installed from the EMS installation. You must configure the MySQL ODBC driver for the EMS to connect to the MySQL database successfully.

Follow the steps below to configure the ODBC driver in Windows XP. Steps may be similar for Windows NT4.0.

Click **Start**, **Settings and Control Panel** to open the **Control Panel** screen. Double-click **Administrative Tools**.

1 Click **start**, **Settings**, **Control Panel**, **Administrative Tools** and click **Data Sources (ODBC)**.

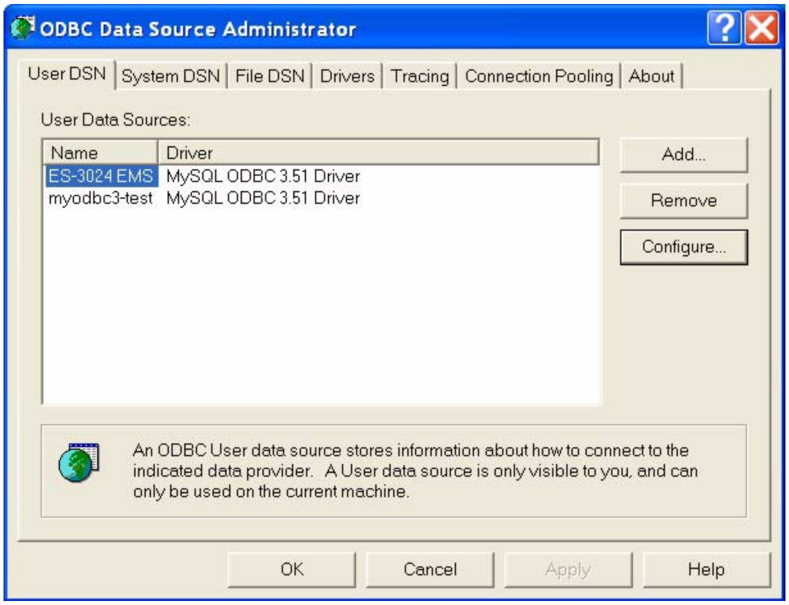
**Figure 30** Data Sources (ODBC)



**2** Click the **User DSN** tab and select the switch MySQL driver from the **User Data Sources** list.

**3** Click **Configure**.

**Figure 31** ODBC Data Source Administrator



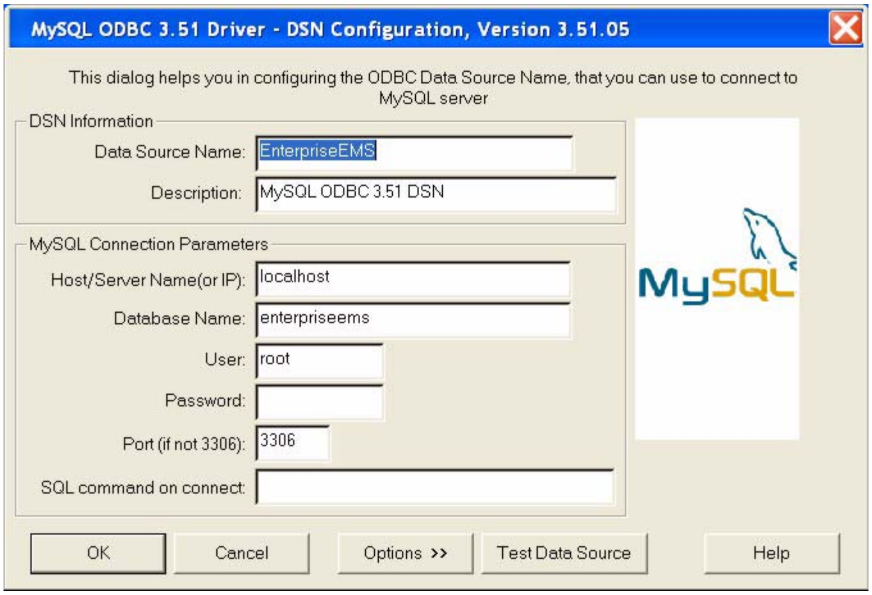
User Data Sources:

| Name | Driver |
|---|---|
| ES-3024 EMS | MySQL ODBC 3.51 Driver |
| myodbc3-test | MySQL ODBC 3.51 Driver |

An ODBC User data source stores information about how to connect to the indicated data provider. A User data source is only visible to you, and can only be used on the current machine.

**4** The MySQL ODBC DSN Configuration screen displays as shown next. Specify your MySQL database settings and click **OK**.

**Figure 32** MySQL: Connection Setup



MySQL ODBC 3.51 Driver - DSN Configuration, Version 3.51.05

This dialog helps you in configuring the ODBC Data Source Name, that you can use to connect to MySQL server

DSN Information

Data Source Name: EnterpriseEMS

Description: MySQL ODBC 3.51 DSN

MySQL Connection Parameters

Host/Server Name(or IP): localhost

Database Name: enterpriseems

User: root

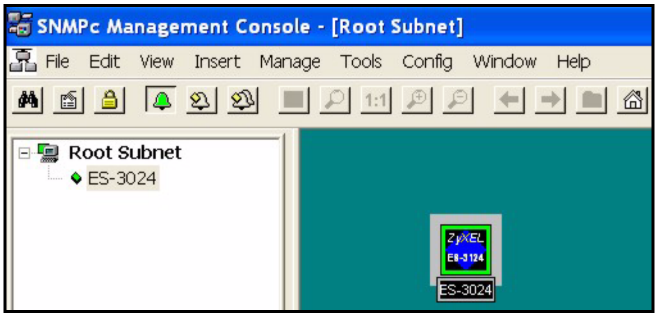
Password:

Port (if not 3306): 3306

SQL command on connect:

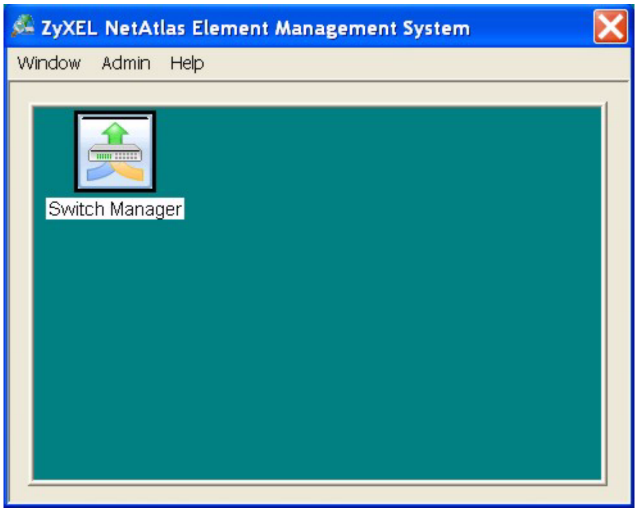
5 Double-click the switch icon to view the **Switch Manager**.

**Figure 33** Switch Device List Icon



6 Double-click the **Switch Manager** icon.

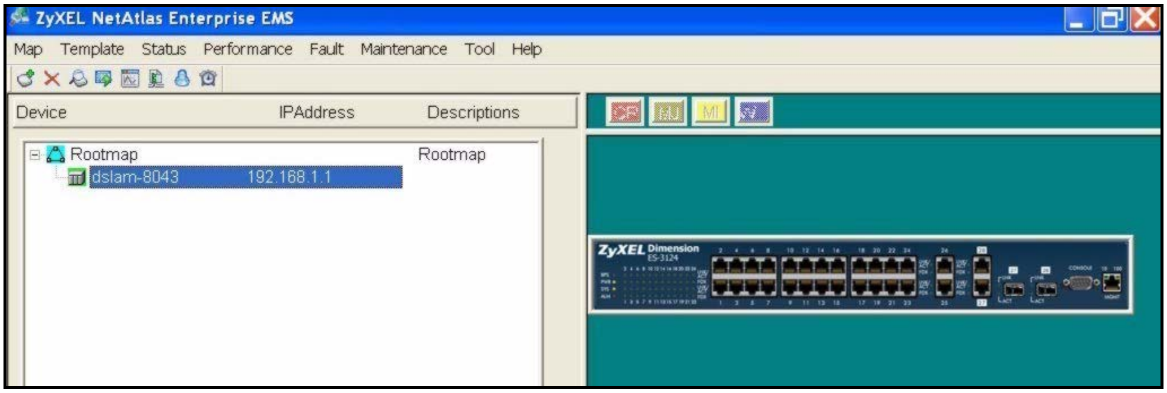
**Figure 34** Switch Manager



**Note:** For information on the **Window**, **Admin** and **Help** options in the **Switch Manager** screen, see Section 14.2 on page 140.

The EMS polls for all the available switch cards. 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 35** Switch Graphic Display



| Device | IPAddress | Descriptions |
|---|---|---|
| Rootmap | | Rootmap |
| dslam-8043 | 192.168.1.1 | |

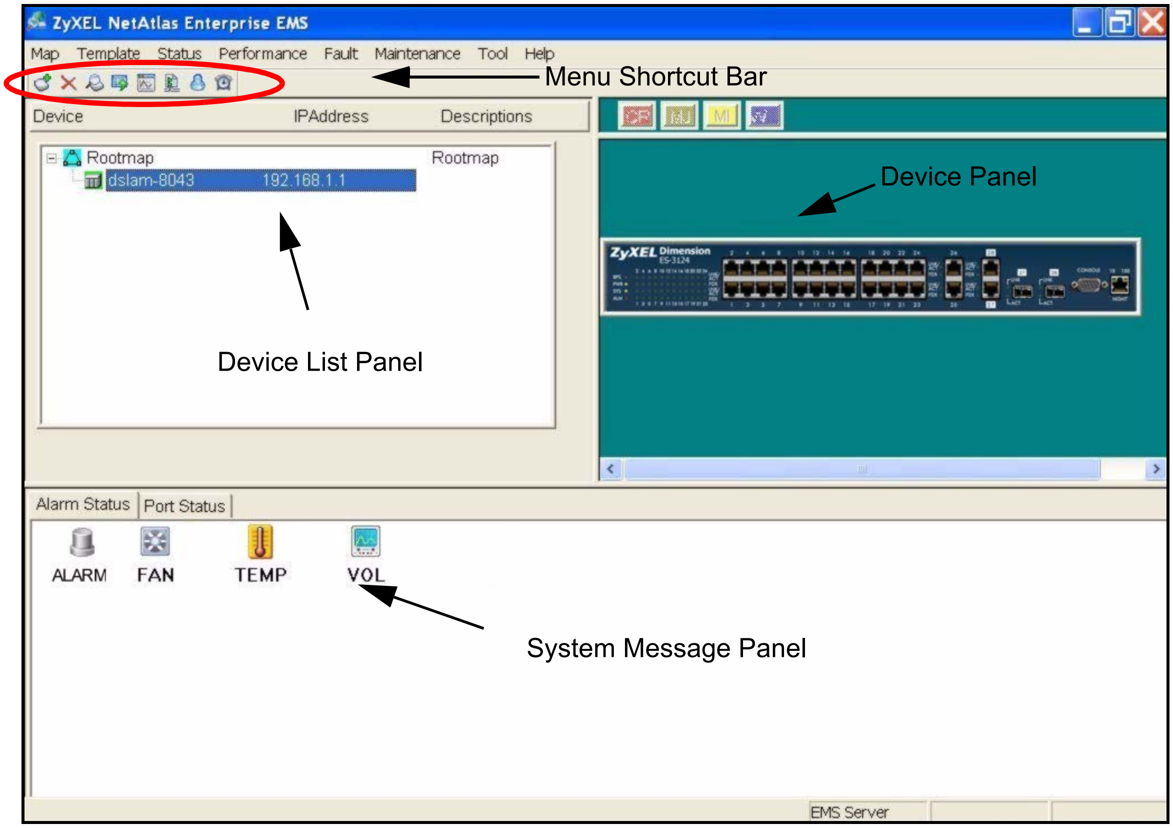
# CHAPTER 2 EMS Main Window

This chapter describes the EMS main window.

## 2.1 Introducing the EMS Main Window

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

**Figure 36** EMS Main Screen Overview



The following table describes the elements in the EMS screen.

**Table 4** EMS Main Screen Overview

| ELEMENT | FUNCTION |
|---|---|
| Menu Shortcut Bar | Use these buttons to execute common commands quickly. Hold the cursor over an icon to see a tool tip. |
| Device Panel | This is a graphical device display. Double-click on a switch to display the EMS GUI management window for the switch. |
| Device List Panel | View devices in a tree structure. The colors of the device icons indicate the real-time status of the represented devices. |
| System Message Panel | View the alarm status and port status of the selected switch. |

## 2.2 Device Icon Colors

The colors of the device icons (in the Device List Panel) indicate the real-time status of the represented devices. The following table describes the colors used.

**Table 5** 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. |

## 2.3 System Message Panel Alarm Status

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

**Table 6** System Message Panel Alarm Status

| PANEL ALARMS | ALARM OFF | ALARM ON |
|---|---|---|
| ALARM | The device fan, temperature or voltage alarm is off.j | The fan, temperature and voltage alarms are all on. A serious hardware problem exists. |
| FAN | The device fans are functioning properlyj | One or more of the device fans has a problem. |
| TEMP | 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 | 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 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 60 for hardware troubleshooting.

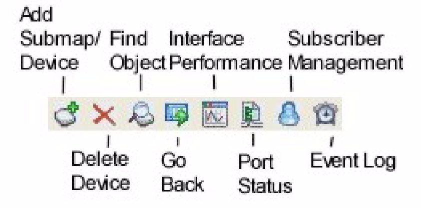
## 2.4 System Message Panel Port Status

Proceed to Section 5.4 on page 66 for information on the details displayed in this screen.

## 2.5 Menu Shortcut Buttons

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

**Figure 37** EMS Main Screen Shortcut Bar



## 2.6 EMS Main Menu Summary

This is a summary of the EMS menus in the main screen.

**Table 7** EMS Menu Summary

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

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

**Table 8** 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. |
| Template | |
| VLAN Template | This link takes you to a screen where you can pre-configure a template of settings for upload to multiple devices. |
| Status Screens | |
| 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 software 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. |
| 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. |
| 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 | |

**Table 8** EMS Navigation Panel Sub-link Descriptions (continued)

| DESCRIPTION | LABEL |
|---|---|
| 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. |

## 2.7 Common EMS Command Buttons

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

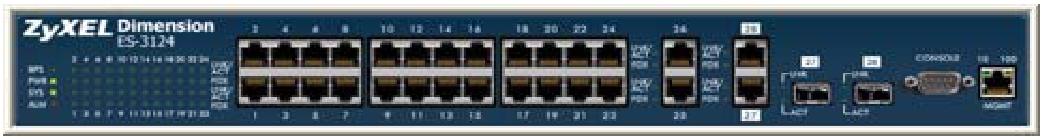
**Table 9** Common EMS Command Buttons

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save the changes back to the switch. |
| OK | Click **OK** to save your changes and close the screen. |
| Cancel | Click **Cancel** to discard all changes and close the screen. |
| Close | Click **Close** to close the screen. |

## 2.8 View the Switch

To display a selected switch, double-click the apporopriate 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 38** Switch View



## 2.9 Switch Information

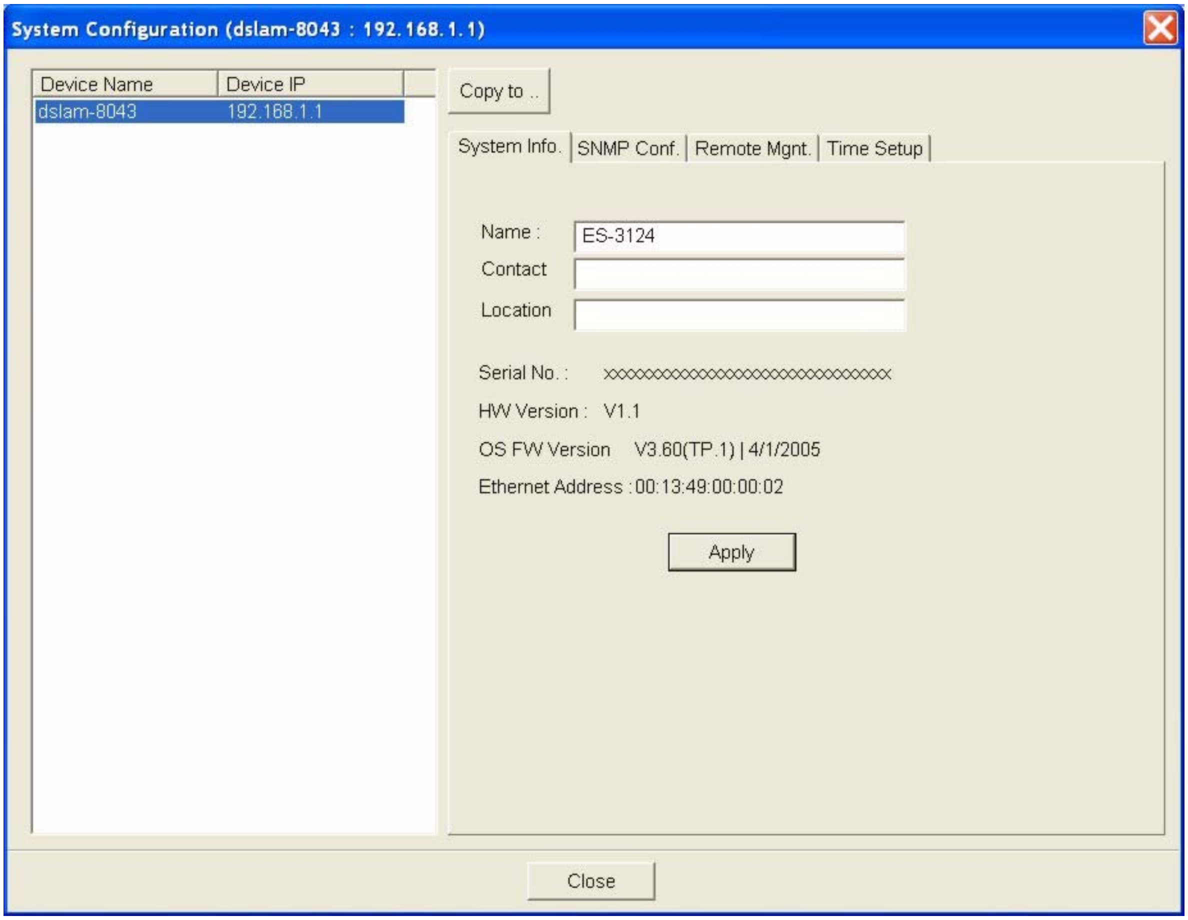
Follow the steps to display information on a switch.

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 39** Configuration: Switch System Configuration



| Device Name | Device IP |
|---|---|
| dslam-8043 | 192.168.1.1 |

Name : ES-3124

Contact

Location

Serial No. : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

HW Version : V1.1

OS FW Version V3.60(TP.1) | 4/1/2005

Ethernet Address : 00:13:49:00:00:02

The following table describes the labels in this screen.

**Table 10** Configuration: Switch System Configuration

| LABEL | DESCRIPTION |
|---|---|
| Device Name | This field displays the selected switch name. |
| Device IP | This field displays the selected switch IP address. |
| 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. |

**Table 10** Configuration: Switch System Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save the changes back to the switch. |
| Close | Click **Close** to close the screen. |

## 2.10 Configuration Save

You can save the current configuration of the switch(es).

**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.

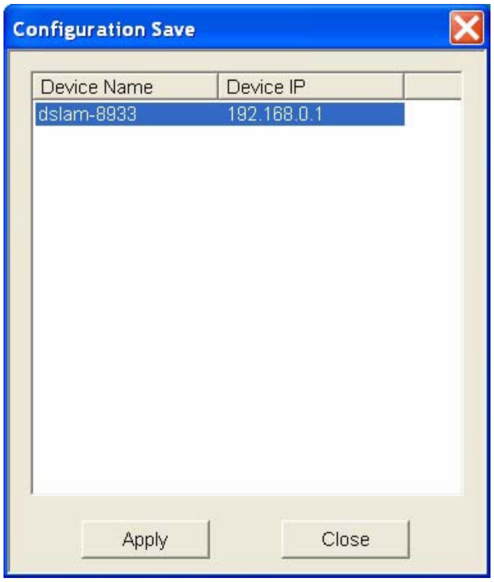
2 Click **Configuration Save**.

3 Choose a switch from the list located in the screen.

4 Click **Apply** to save the current configuration.

5 All settings configured on the EMS will be saved to the selected switch.

**Figure 40** Configuration: Save



| Device Name | Device IP |
|---|---|
| dslam-8933 | 192.168.0.1 |

# CHAPTER 3
# Managing Device Maps in EMS

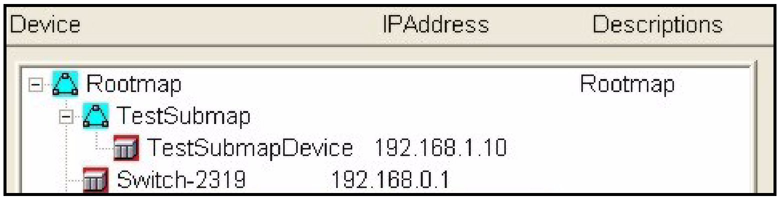
This chapter describes the Map menus you use to add, edit or delete device mappings in the EMS.

## 3.1 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.

In the following figure the “TestSubmap” folder and the “Switch-2319” are both mapped to the “Rootmap” folder. The “TestSubmap” is a submap folder that contains a mapped device “TestSubmapDevice”.

**Figure 41** Submaps and Device Mapping



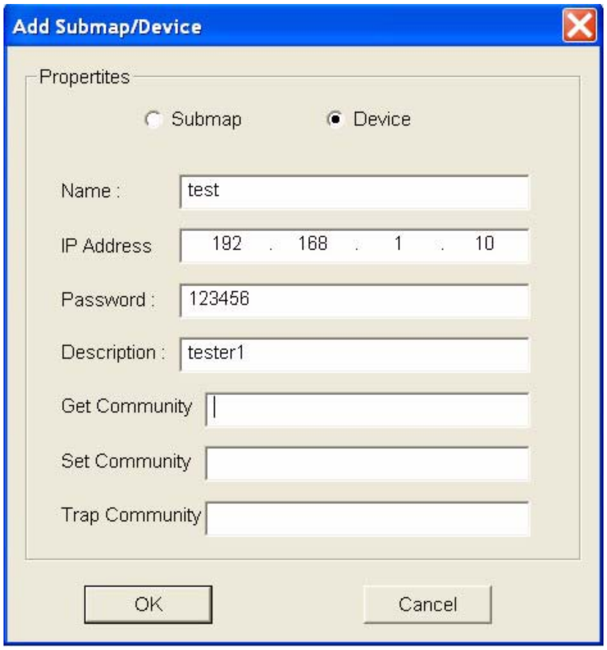
| Device | IPAddress | Descriptions |
|---|---|---|
| Rootmap | | Rootmap |
| TestSubmap | | |
| TestSubmapDevice | 192.168.1.10 | |
| Switch-2319 | 192.168.0.1 | |

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

### 3.1.1 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 42** Map: Add Submap/Device


Add Submap/Device

Propertites

○ Submap ● Device

Name : test

IP Address 192 . 168 . 1 . 10

Password : 123456

Description : tester1

Get Community

Set Community

Trap Community

The following table describes the labels in this screen.

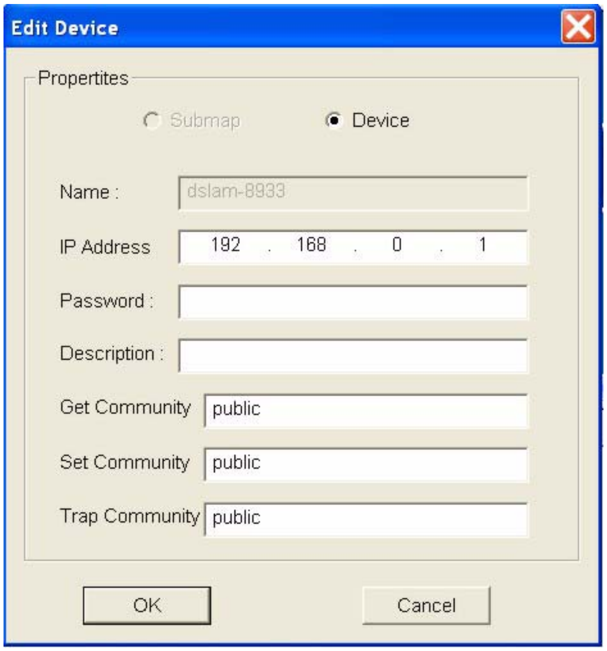
**Table 11** Map: Add Submap/Device

| LABEL | DESCRIPTION |
|---|---|
| Properties | Select the **Submap** or **Device** radio button to add a new submap or device icon to the Device List Panel.<br>If you select **Submap,** only the **Name** and **Description** fields display ; all other fields appear as read-only. |
| Name | Enter a descriptive name (up to 32 characters) for this node for identification purposes. |
| IP Address | Enter the IP address of the device. |
| Password | Enter a password (up to 32 characters). This password is used by the EMS administrator for device firmware upload. |
| Description | Enter a description (up to 32 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 **OK** to save the changes and close the screen. |
| Cancel | Click **Cancel** to discard the changes and close the screen. |

## 3.1.2 Edit a Node

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

**Figure 43** Map: Edit Node


Edit Device

Propertites

○ Submap ● Device

Name : dslam-8933

IP Address 192 . 168 . 0 . 1

Password :

Description :

Get Community public

Set Community public

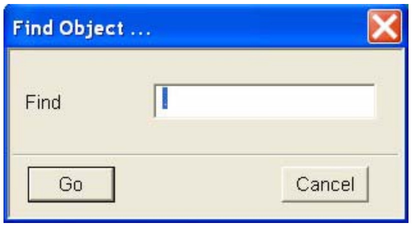
Trap Community public

Refer to Table 11 on page 53 for the field descriptions.

## 3.1.3 Find an Object

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

**Figure 44** Map: Find Object


Find Object ...

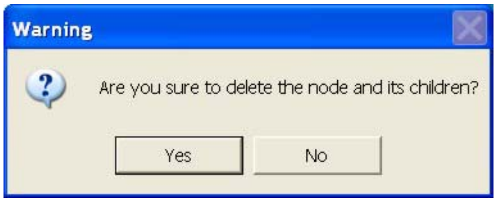
Find

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

## 3.1.4 Delete a Submap

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

**Figure 45** Map: Delete Warning



Warning

Are you sure to delete the node and its children?

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

### 3.1.5 Delete a Device

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

## 3.2 Exit

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

# CHAPTER 4
# VLAN Template

This chapter describes how to configure a VLAN template.

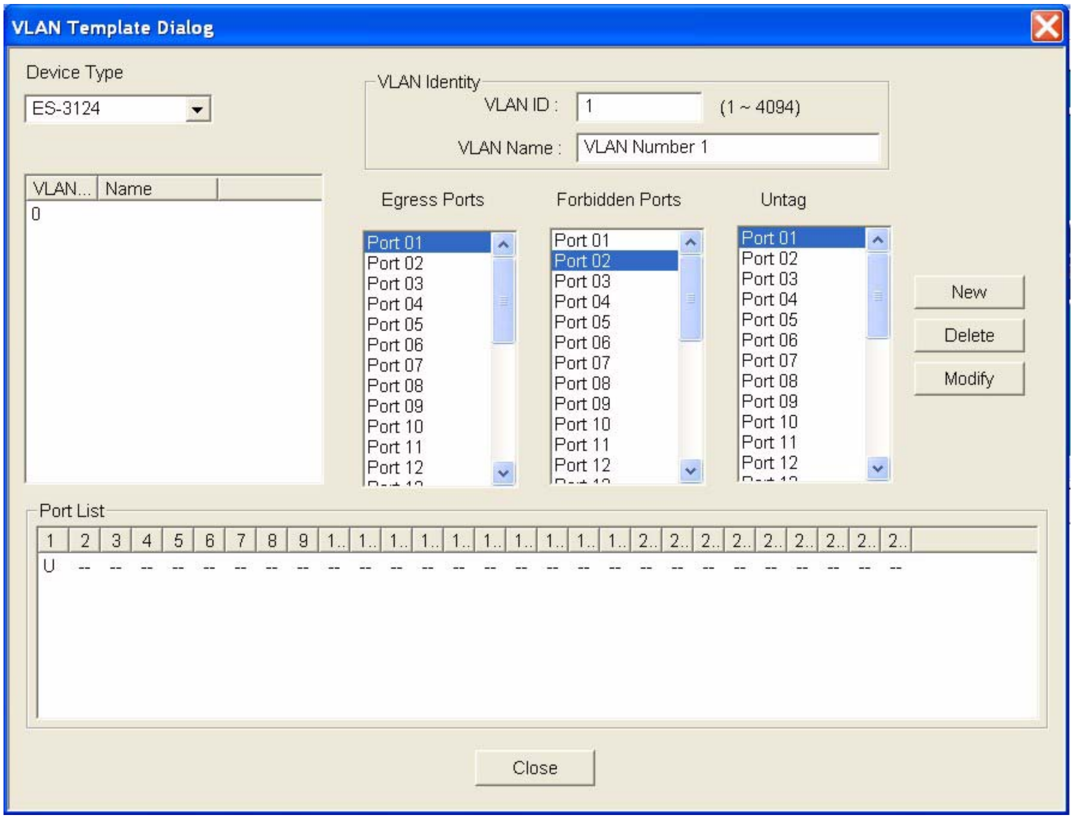
## 4.1 VLAN Template Overview

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.

### 4.1.1 Configuring a VLAN Template

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

**Figure 46** Template: VLAN



Device Type: ES-3124

VLAN ID : 1 (1 ~ 4094)

VLAN Name : VLAN Number 1

VLAN... 0

The following table describes the labels in this screen.

**Table 12** Template: VLAN

| LABEL | DESCRIPTION |
|---|---|
| Device Type | Select a device type 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 802.1Q VLAN.<br>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.<br>A forbidden port cannot be an egress or untagged port.<br>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.<br>An egress port can be untagged.<br>Select the ports which you want to be untagged ports from the list provided. |
| New | Click **New** to create a new VLAN. You must enter a **VLAN ID** and a **VLAN Name** to create a new **VLAN**. The new VLAN and name is displayed in the left-hand column in this screen. |

**Table 12** Template: VLAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Delete | Click on a VLAN in the left-hand column of this screen and then click the **Delete** button to remove it from the VLAN template. |
| Modify | Click on a VLAN in the left-hand column of this screen. Change the **VLAN Name** or change the configuration of the egress, forbidden and untagged ports. Click the **Modify** button to save the changes to the switch.<br>If you want to change the **VLAN ID** of a VLAN configuration, you can only delete the VLAN configuration or create a new VLAN configuration using a different **VLAN ID**. |
| Port List | Click on a port in the **Egress Ports** 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.<br>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 **Close** to close the screen. |

# CHAPTER 5
# Status

This chapter covers the hardware status, STP status, VLAN status, port status and 802.1d status screens.

## 5.1 Hardware Status

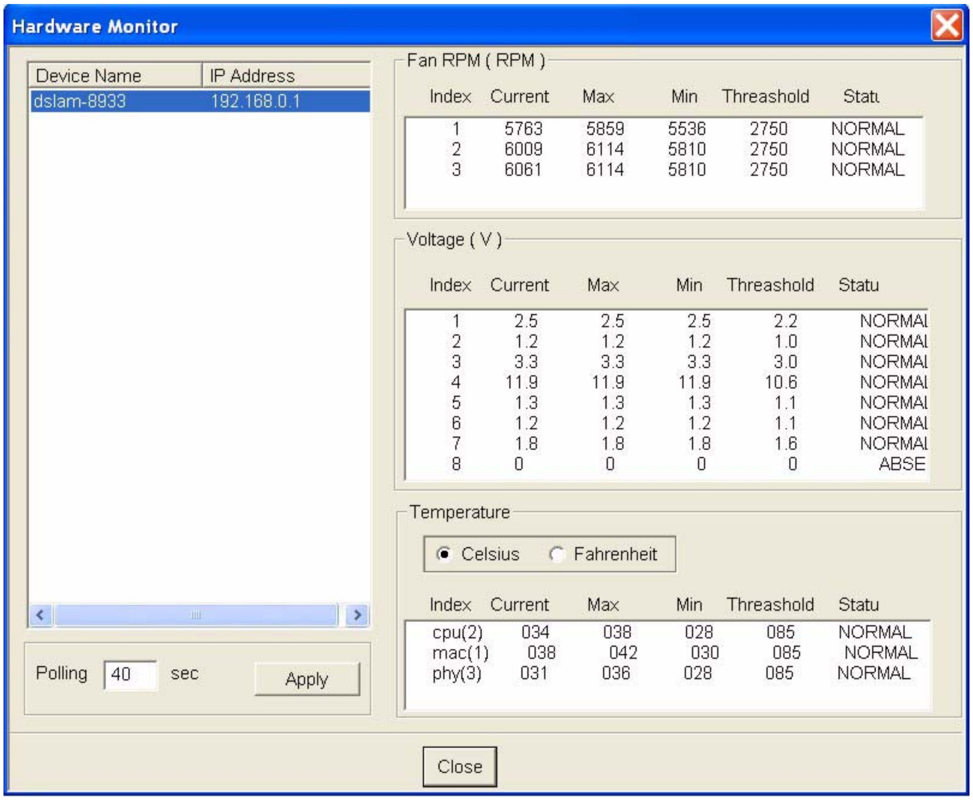
Follow the steps below to view fan speeds, voltage levels and temperatures of a switch.

1 To view the hardware status of a switch, click **Status** and then **Hardware Status**.

2 Choose a switch from the list located on the left-hand side of the screen as shown next.

It may take a few seconds to update the screen.

**Figure 47** Status: Hardware Status



Hardware Monitor

| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

Fan RPM ( RPM )

| Index | Current | Max | Min | Threashold | Statu |
|---|---|---|---|---|---|
| 1 | 5763 | 5859 | 5536 | 2750 | NORMAL |
| 2 | 6009 | 6114 | 5810 | 2750 | NORMAL |
| 3 | 6061 | 6114 | 5810 | 2750 | NORMAL |

Voltage ( V )

| Index | Current | Max | Min | Threashold | Statu |
|---|---|---|---|---|---|
| 1 | 2.5 | 2.5 | 2.5 | 2.2 | NORMAl |
| 2 | 1.2 | 1.2 | 1.2 | 1.0 | NORMAl |
| 3 | 3.3 | 3.3 | 3.3 | 3.0 | NORMAl |
| 4 | 11.9 | 11.9 | 11.9 | 10.6 | NORMAl |
| 5 | 1.3 | 1.3 | 1.3 | 1.1 | NORMAl |
| 6 | 1.2 | 1.2 | 1.2 | 1.1 | NORMAl |
| 7 | 1.8 | 1.8 | 1.8 | 1.6 | NORMAl |
| 8 | 0 | 0 | 0 | 0 | ABSE |

Temperature

● Celsius ○ Fahrenheit

| Index | Current | Max | Min | Threshold | Statu |
|---|---|---|---|---|---|
| cpu(2) | 034 | 038 | 028 | 085 | NORMAL |
| mac(1) | 038 | 042 | 030 | 085 | NORMAL |
| phy(3) | 031 | 036 | 028 | 085 | NORMAL |

Polling 40 sec

The following table describes the labels in this screen.

**Table 13** Status: Hardware Status

| LABEL | DESCRIPTION |
|---|---|
| Fan 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). "<41" is displayed for speeds too small to measure (under 2000 RPM). |
| Threshold | This field displays the minimum speed at which a normal fan should work. |
| Status | **NORMAL** indicates that this fan is functioning above the minimum speed. **ERROR** 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. |

**Table 13** Status: Hardware Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 | **NORMAL** indicates that the voltage is within an acceptable operating range at this point; otherwise **ERROR** is displayed. **ABSENT** 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 (Centigrade 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 **NORMAL** for temperatures below the threshold and **ERROR** 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 **Apply** button. |
| Close | Click **Close** to close the screen. |

# 5.2 STP Status

## 5.2.1 Introduction to 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.

### 5.2.1.1 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 14** 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 | 1to 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 15** 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. |

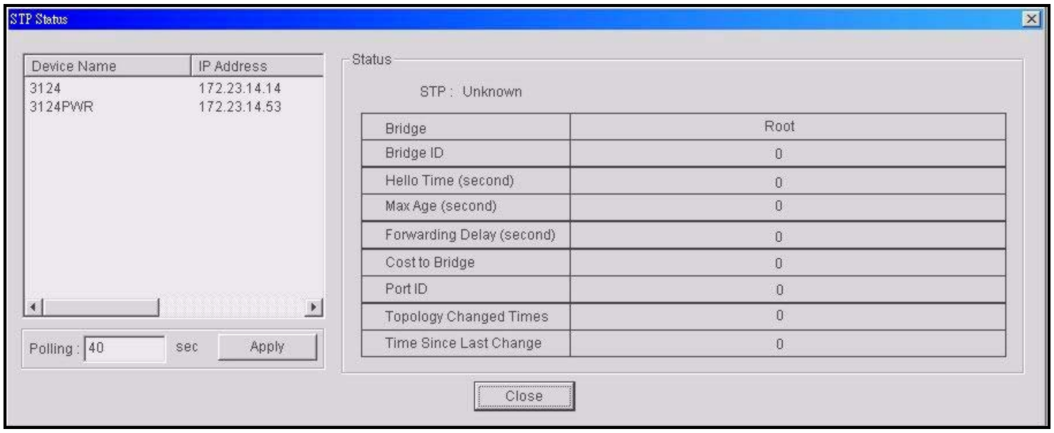
### 5.2.4 View STP Status

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

1 Click **Status** and then **STP Status**.

2 Choose a switch from the list located on the left-hand side of the screen.

**Figure 48** Status: STP Status



STP Status

| Device Name | IP Address |
|---|---|
| 3124 | 172.23.14.14 |
| 3124PWR | 172.23.14.53 |

Polling : 40 sec

Status

STP : Unknown

| Bridge | Root |
|---|---|
| Bridge ID | 0 |
| Hello Time (second) | 0 |
| Max Age (second) | 0 |
| Forwarding Delay (second) | 0 |
| Cost to Bridge | 0 |
| Port ID | 0 |
| Topology Changed Times | 0 |
| Time Since Last Change | 0 |

The following table describes the labels in this screen.

**Table 16** Status: STP Status

| LABEL | DESCRIPTION |
|---|---|
| STP | This field displays **Running** if STP is activated; otherwise, it displays **Unknown**. |
| Bridge | **Root** 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. |

**Table 16** Status: STP Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 **Apply** button. |
| Close | Click **Close** to close the screen. |

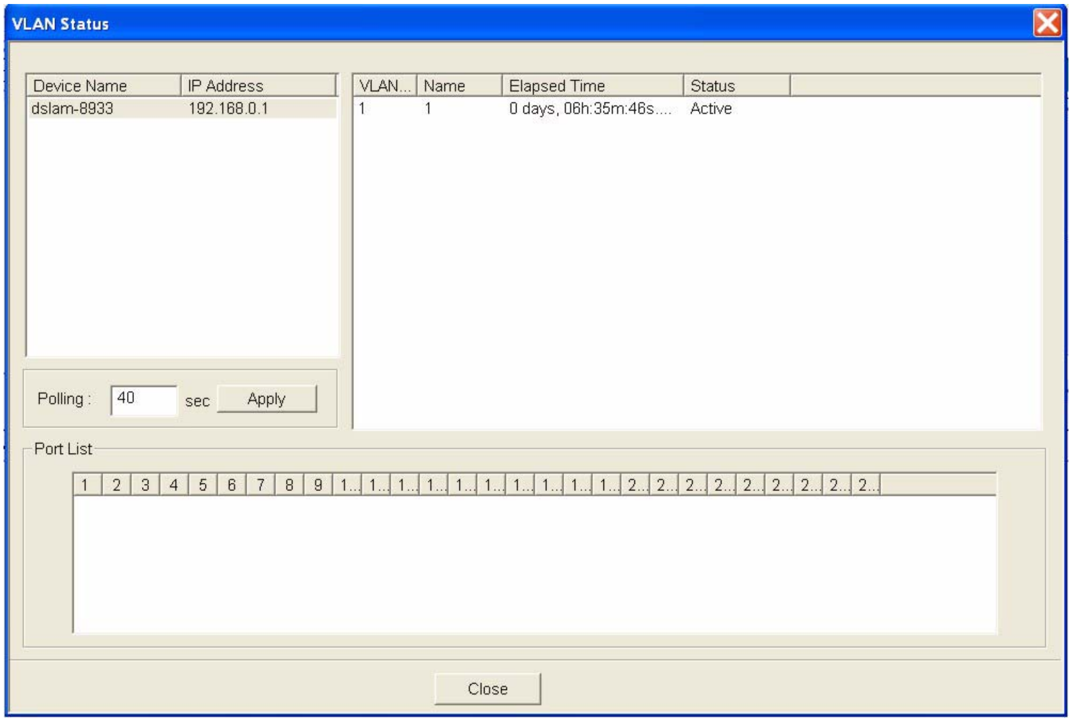
## 5.3 VLAN Status

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

1 Click **Status** and then **VLAN Status**.

2 Choose a switch from the list located on the left-hand side of the screen.

**Figure 49** Status: VLAN Status



| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

| VLAN... | Name | Elapsed Time | Status |
|---|---|---|---|
| 1 | 1 | 0 days, 06h:35m:46s.... | Active |

The following table describes the labels in this screen.

**Table 17** Status: VLAN Status

| | 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 **Active** if the VLAN is active and will remain so after the next reset of the device. This field displays **GVRP** 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 **Apply** button. |
| Close | Click **Close** to close the screen. |

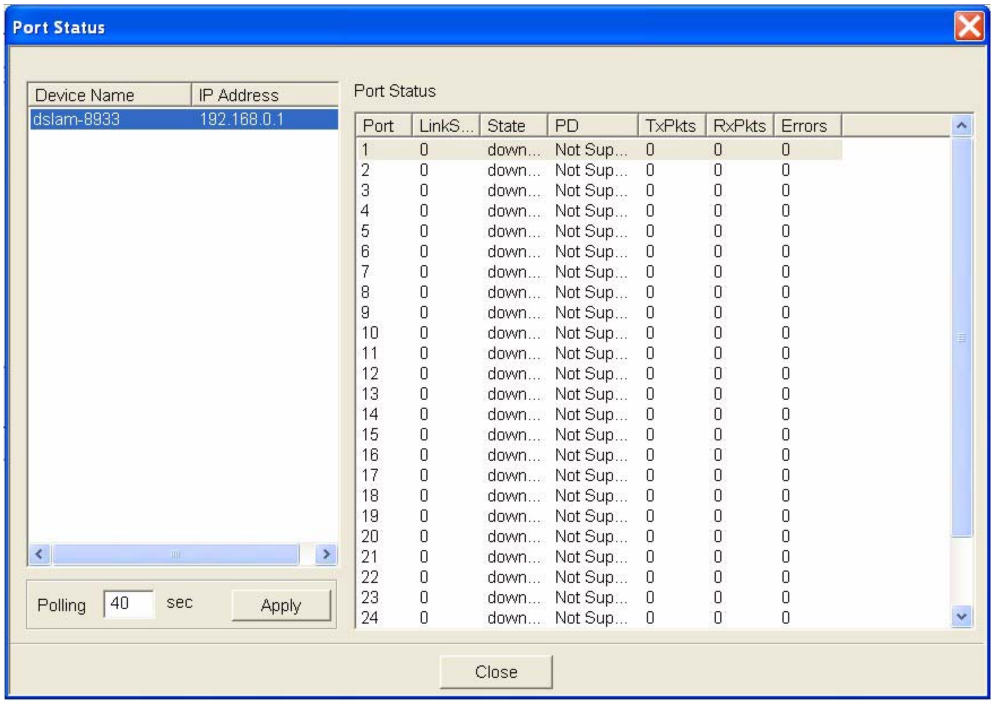
## 5.4 Port Status

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

1 Click **Status** 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 50** Status: Port Status



| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

Polling 40 sec

Port Status

| Port | LinkS... | State | PD | TxPkts | RxPkts | Errors |
|---|---|---|---|---|---|---|
| 1 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 2 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 3 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 4 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 5 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 6 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 7 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 8 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 9 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 10 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 11 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 12 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 13 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 14 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 15 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 16 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 17 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 18 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 19 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 20 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 21 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 22 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 23 | 0 | down... | Not Sup... | 0 | 0 | 0 |
| 24 | 0 | down... | Not Sup... | 0 | 0 | 0 |

The following table describes the labels in this screen.

**Table 18** Status: 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) and the duplex (F for full duplex or H for half). It also shows the cable type (Copper or Fiber) for the combo ports. |
| State | This field displays the STP state of the port. See the Spanning Tree Protocol chapter for details on STP port states. |
| PD | This field displays the power device (PD) module status on the switch. If **Not Supported** is displayed, the switch does not have a PD.<br>This field displays **On** if the switch has a PD and it is in use.<br>This field displays **Of** 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 **Apply** button. |
| Close | Click **Close** 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.

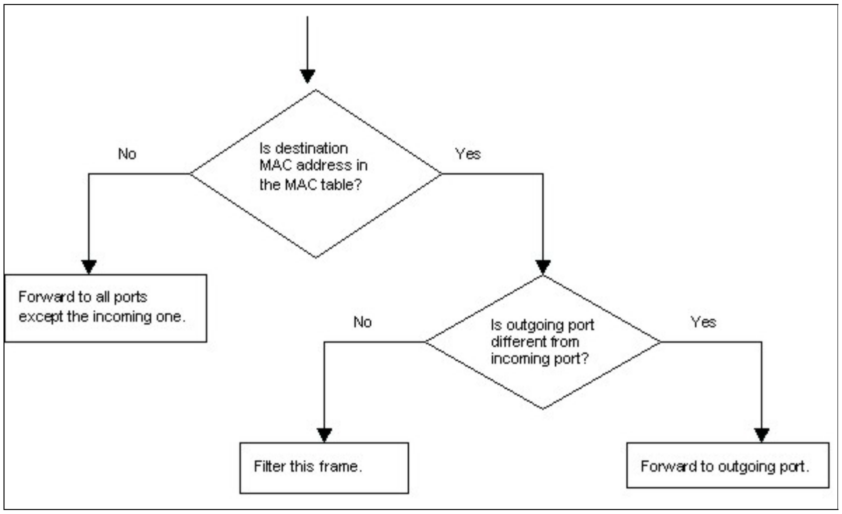
2 The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the Filtering Database.

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 51** MAC Table Flowchart


Is destination MAC address in the MAC table?
No
Yes
Forward to all ports except the incoming one.
Is outgoing port different from incoming port?
No
Yes
Filter this frame.
Forward to outgoing port.

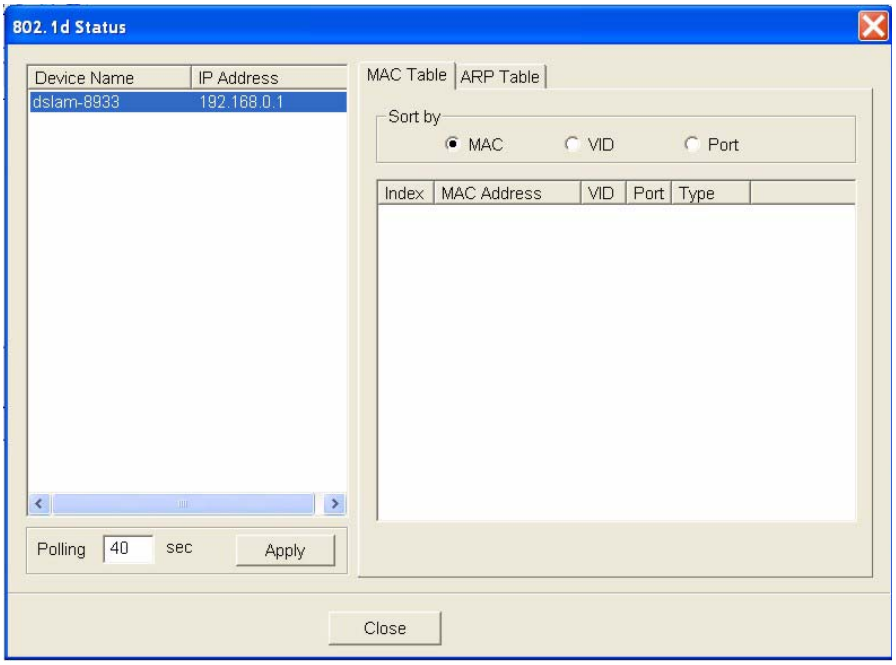
### 5.5.2 View the MAC Table

Follow the steps below to view the MAC table.

1 Click **Status** 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 52** Status: 802.1d: MAC Table



802.1d Status

| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

Sort by: ● MAC ○ VID ○ Port

| Index | MAC Address | VID | Port | Type |
|---|---|---|---|---|

Polling 40 sec

The following table describes the labels in this screen.

**Table 19** Status: 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. |
| Name | This field displays a descriptive name for this static MAC address forwarding rule. |
| 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 Static MAC Forwarding). |
| 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 **Apply** button. |
| Close | Click **Close** 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.

The ARP table can hold up to 16K entries.

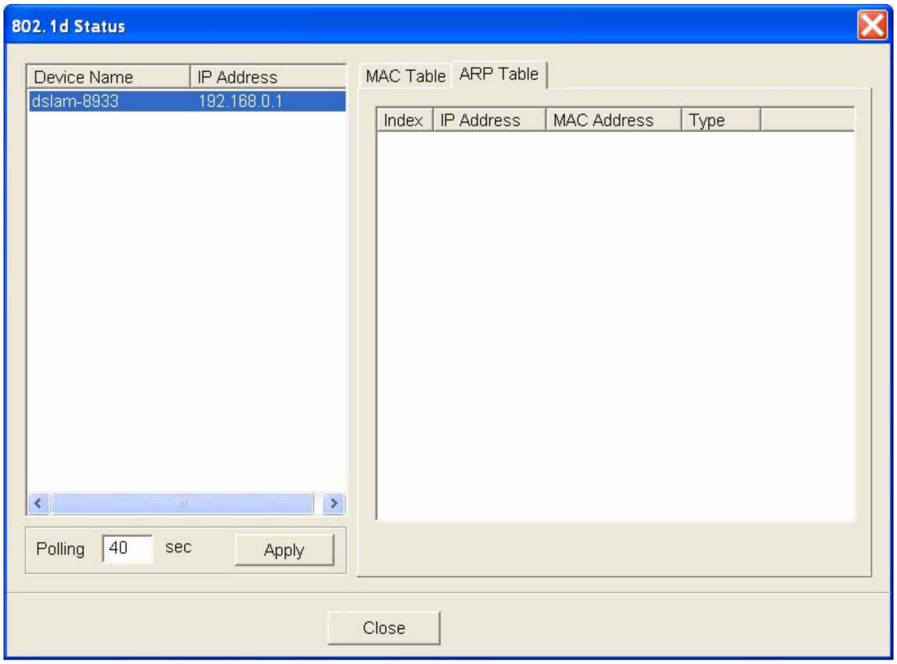
### 5.5.5 View the ARP Table

Follow the steps below to view the ARP table.

1 Click **Status** 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 53** Status: 802.1d: ARP Table



| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

| Index | IP Address | MAC Address | Type |
|---|---|---|---|

Polling 40 sec

The following table describes the labels in this screen.

**Table 20** Status: 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 Static MAC Forwarding). |
| 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 **Apply** button. |
| Close | Click **Close** to close the screen. |

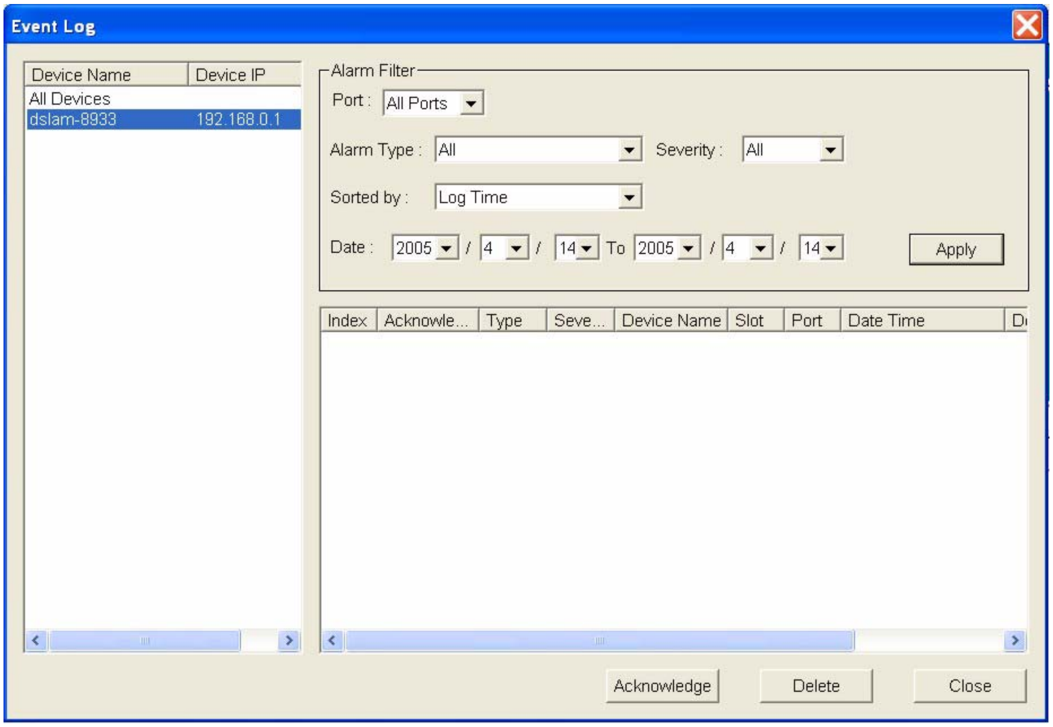
# CHAPTER 6 Fault Menus

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

## 6.1 Event Log

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

**Figure 54** Fault: Event Log


Event Log

| Device Name | Device IP |
|---|---|
| All Devices | |
| dslam-8933 | 192.168.0.1 |

Alarm Filter
Port : All Ports
Alarm Type : All
Severity : All
Sorted by : Log Time
Date : 2005 / 4 / 14 To 2005 / 4 / 14

The following table describes the labels in this screen.

**Table 21** 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 21** Fault: Event Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| Alarm Type | Select the type of logs from the drop-down list box. Choices are **All**, **Communication**, **QualityOfService**, **ProcessingError**, **Equipment** and **Environmental**.<br>Select **All** for system event logs generated by all alarm types.<br>Select **Communication** for transmission and signal logs.<br>Select **QualityOfService** for performance logs.<br>Select **Processing Error** for software and configuration problem logs.<br>Select **Equipment** for hardware-related logs.<br>Select **Environmental** for environmental logs.<br>See the appendix for a more detailed list of possible alarm causes. |
| Severity | 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:<br>• Critical - Red<br>• Major - Orange<br>• Minor - Yellow<br>• Warning - Blue<br>• Normal - Green |
| Sorted by | Select **Log Time** to sort event logs by the time at which they were generated or select **Device Name** to sort event logs by the device from which they were generated. |
| Date / To | Specify the time range to display the event logs. |
| Apply | Click **Apply** to display event logs generated within the specified time period. |
| Alarm | |
| Index | This field displays the index number of the event logs. |
| Acknowledge | 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. |
| Type | This field displays the type of the event log. |
| Severity | This field displays the severity of the event log. |
| Device Name | This field displays the name of the device on which the event log was generated. |
| Port | This field displays the port number on which the event log was generated. |
| Date Time | This field displays the date and time on which the event log was generated. |
| Description | This field displays some information about the event log. |
| Acknowledge | Click this button to acknowledge any selected log messages. |
| Delete | Click **Delete** to remove a log. |
| Close | Click **Close** to close this screen. |

## 6.2 Loopback Test

Follow the steps below to perform an internal loopback test.

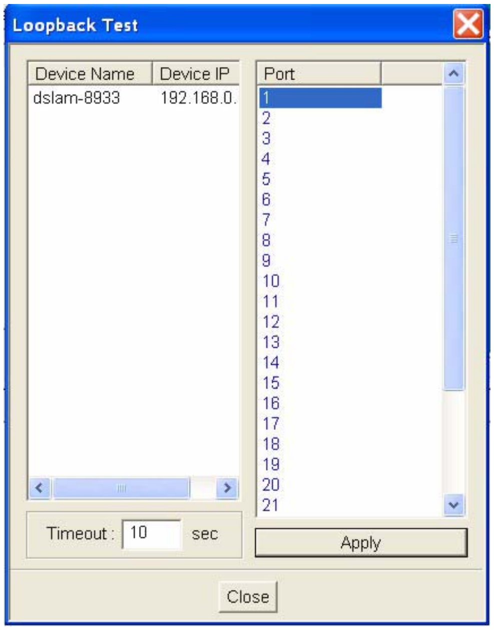
1 Click **Fault** and then **Loopback Test**.

**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** Click **Apply** to start the loopback test.

**Figure 55** Fault: Loopback Test



| Device Name | Device IP |
|---|---|
| dslam-8933 | 192.168.0. |

| Port |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 6 |
| 7 |
| 8 |
| 9 |
| 10 |
| 11 |
| 12 |
| 13 |
| 14 |
| 15 |
| 16 |
| 17 |
| 18 |
| 19 |
| 20 |
| 21 |

Timeout : 10 sec

# CHAPTER 7 Maintenance

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

## 7.1 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.

### 7.1.1 Procedure to Update Firmware

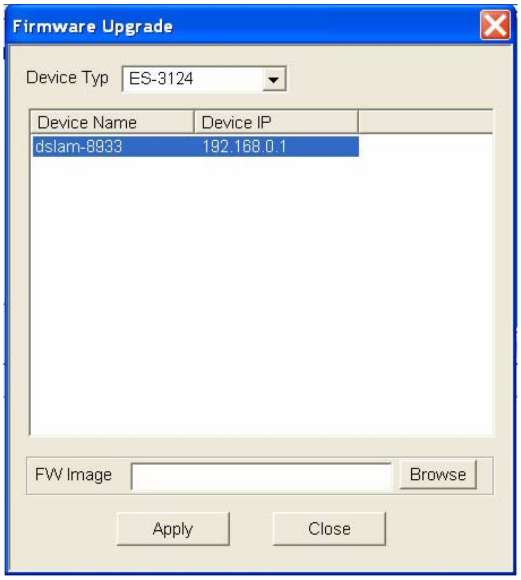
You can perform firmware upgrade on all switches of the same type simultaneously on the EMS. To update firmware, first download the latest firmware, then unzip and store it on your computer. You can use this EMS FTP client to connect to a selected switch.

**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 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 56** Maintenance: Firmware Upgrade



| Device Name | Device IP |
|---|---|
| dslam-8933 | 192.168.0.1 |

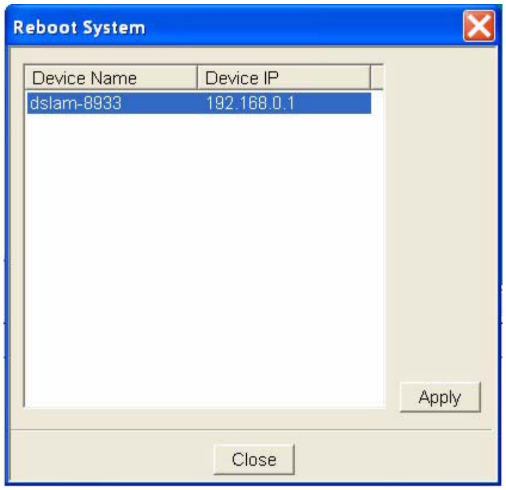
The switch(es) automatically restarts when the firmware upload is complete.

## 7.2 Device Reset

**Reboot System** allows you to restart a switch without physically turning the power off. Select a device from the list and click **Apply**.

Click **Apply** again and then wait for the switch to restart. This takes up to two minutes. This does not affect the switch's configuration.

**Figure 57** Maintenance: Device Reset



| Device Name | Device IP |
|---|---|
| dslam-8933 | 192.168.0.1 |

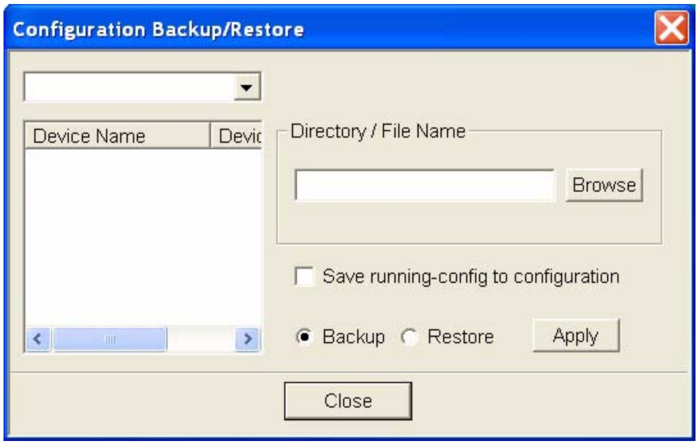
## 7.3 Network Element Configuration Backup and Restore

A Network Element is a piece of telecommunications equipment that provides support or services to the user.

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

1. Click **Maintenance** and then **NE (Network Element) Configuration Backup and Restore**.
2. Select a switch from the drop-down list box.
3. Type the path and file name of the file you wish to restore to the switch or backup to your computer in the **Directory / File Name** text box or click **Browse** to locate it.
4. Select the **Save configuration before backup?** text box to save the most recent switch configuration if you want to backup to your computer.
5. Click either the **Backup** or **Restore** radio button.
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 58** Maintenance: Configuration Backup/Restore



The following table describes the labels in this screen.

**Table 22** 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 **Directory / File Name** text box or click **Browse** to locate it. |
| Save running-config to configuration | Select the **Save running-config to configuration** text box to save the most recently updated configuration to a file specified in the **Directory/ File Name** field. |
| Backup | Click the **Backup** radio button to transfer the configuration file from your switch to a computer. |
| Restore | Click the **Restore** radio button to transfer the configuration file from your computer to a switch. |
| Apply | Click **Apply** to backup or restore the switch(es) configuration file. |
| Close | Click **Close** to close this screen. |

## 7.4 Load Factory Default

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

1 Click **Maintenance** and then **Load Factory Default**.

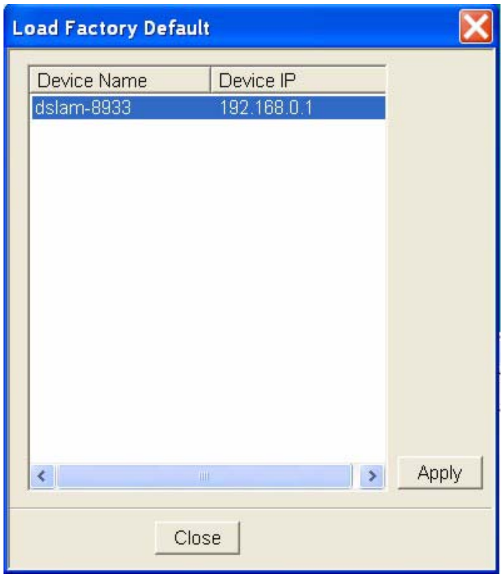
2 Select a switch from the list of devices shown.

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 59** Maintenance: Load factory Defaults

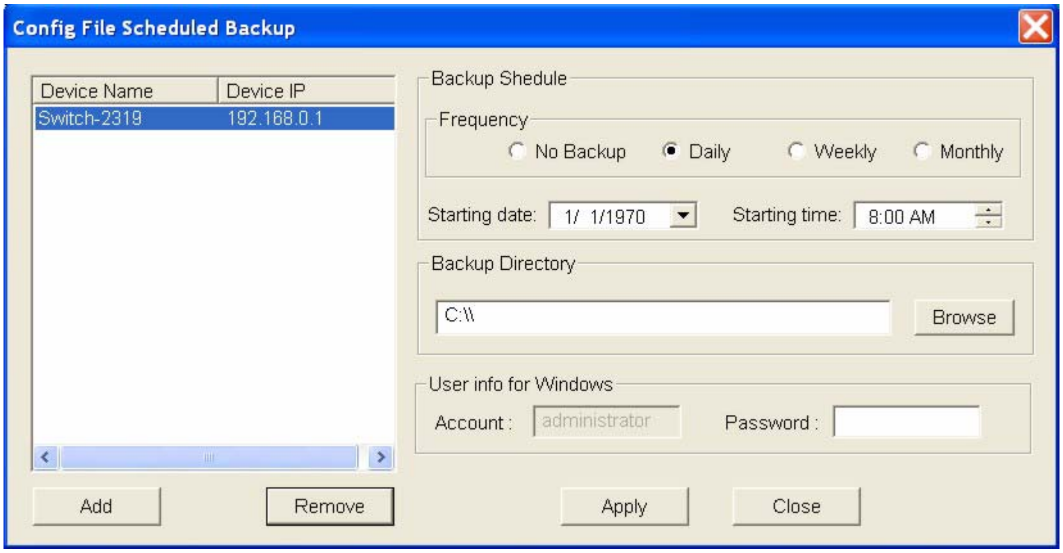


| Device Name | Device IP |
|---|---|
| dslam-8933 | 192.168.0.1 |

## 7.5 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 60** Maintenance: Scheduled NE Config Backup



Config File Scheduled Backup

| Device Name | Device IP |
|---|---|
| Switch-2319 | 192.168.0.1 |

Backup Shedule

Frequency: ○ No Backup ● Daily ○ Weekly ○ Monthly

Starting date: 1/ 1/1970

Starting time: 8:00 AM

Backup Directory: C:\\

User info for Windows

Account : administrator

Password :

The following table describes the labels in this screen.

**Table 23** Maintenance: Scheduled NE Config Backup

| LABEL | DESCRIPTION |
|---|---|
| Backup Schedule | |
| Frequency | Scheduled backups can be performed on a **Daily**, **Weekly** or **Monthly** basis. Select a radio button to schedule configuration backups starting at the date and time specifed below. The default setting is **No Backup**. |
| 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 **Backup Directory** text box or click **Browse** 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 **Account** above. |
| Add | Click the **Add** button to add a switch to the list of devices in the backup schedule. |
| Remove | Click the **Remove** button to remove a switch from the list of devices in the backup schedule. |
| Apply | Click **Apply** to save changes to the EMS. |
| Close | Click **Close** to close this screen. |

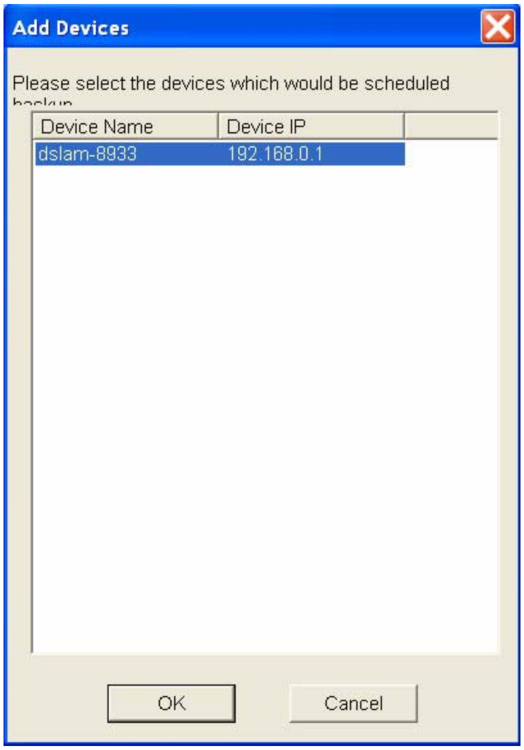
## 7.5.1 Scheduled Network Element Configuration Backup Add

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 61** Maintenance: Scheduled NE Config Backup Add



Please select the devices which would be scheduled backup

| Device Name | Device IP |
|---|---|
| dslam-8933 | 192.168.0.1 |

## 7.5.2 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 8 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.

## 8.1 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.

### 8.1.1 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.

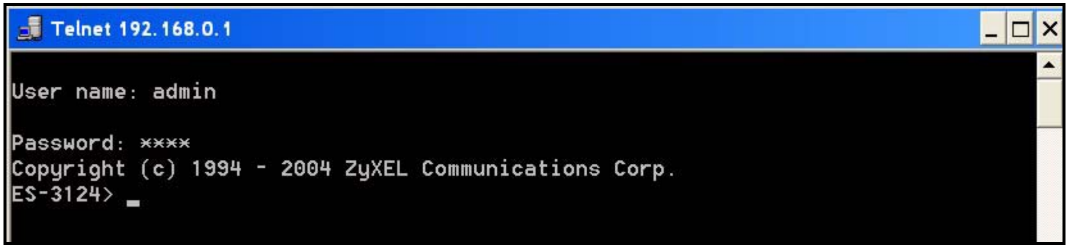
The administrator uses Telnet from a computer on a remote network to access the switch. You can use remote Telnet access as shown next.

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 62** Telnet



```
User name: admin

Password: ****
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ES-3124> _
```

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

### 8.1.2 Web Access

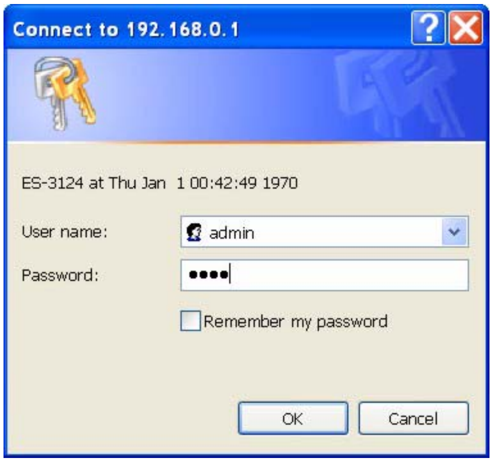
Configure the switch using the web configurator as shown.

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 63** Web Access



Connect to 192.168.0.1

ES-3124 at Thu Jan 1 00:42:49 1970

User name: admin

Password: ••••

☐ Remember my password

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

## 8.2 Ping

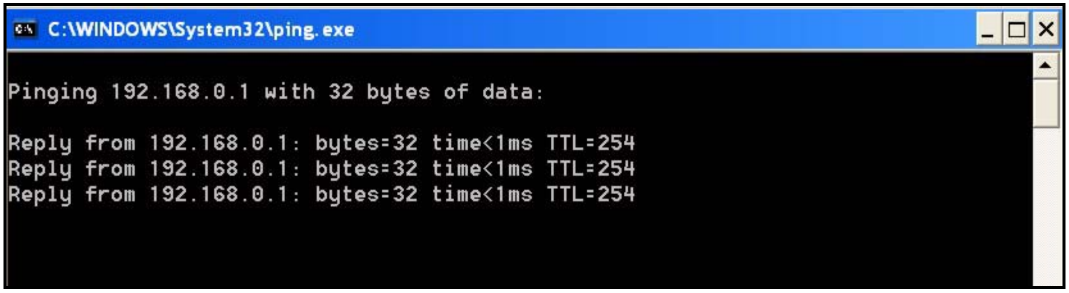
Ping the host to see if the links and TCP/IP protocol on both your computer and the switch is working. Follow the steps below:

1 Select a switch from the list of devices shown in the Device List Panel.

2 Click **Tool** and then **Ping** to have the switch ping the IP address of the selected device.

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

**Figure 64** Ping



C:\WINDOWS\System32\ping.exe

```
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=254
Reply from 192.168.0.1: bytes=32 time<1ms TTL=254
Reply from 192.168.0.1: bytes=32 time<1ms TTL=254
```

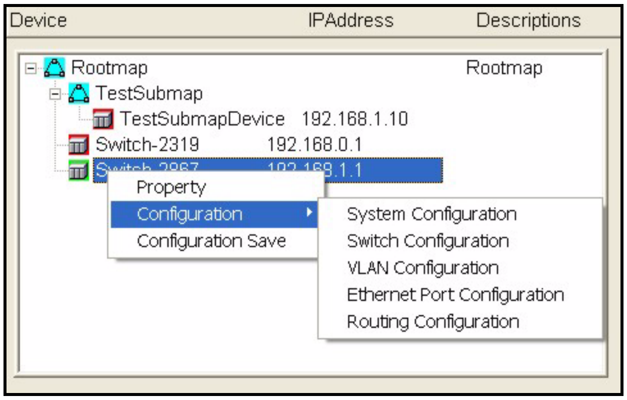
# CHAPTER 9
# Device Menu Overview

This chapter introduces the device configuration menus.

## 9.1 Device Menu Summary

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

**Figure 65** Device Panel List Menus



| Device | IPAddress | Descriptions |
|---|---|---|
| Rootmap | | Rootmap |
| TestSubmap | | |
| TestSubmapDevice | 192.168.1.10 | |
| Switch-2319 | 192.168.0.1 | |
| Switch-2867 | 192.168.1.1 | |

The following table shows the menus, sub menus and menu tab names.

**Table 24** Device Menu Summary

| MENU | SUBMENU | SUBMENU TABS |
|---|---|---|
| Property | Edit Device | |
| Configuration | System Configuration | System Info |
| | | SNMP Conf. |
| | | Remote Mgmt. |
| | | Time Setup |
| | Switch Configuration | Switch Setup |
| | | Priority Queue |
| | | STP Conf. |
| | | Link Aggregation |
| | | DHCP Relay |
| | | GARP Timer |
| | | RADIUS |
| | | MAC Forwarding |

**Table 24** Device Menu Summary

| MENU | SUBMENU | SUBMENU TABS |
|---|---|---|
| | | Filtering |
| | VLAN Configuration | |
| | Ethernet Port Configuration | Port Setup |
| | | Port VLAN |
| | | Port Link Aggregation |
| | | Port STP |
| | | Bandwidth Ctrl. |
| | | Broadcast Storm Ctrl. |
| | | Queue Method |
| | | Port 802.1x |
| | | Port Security |
| | | Port Mirroring |
| | | VLAN Stacking |
| | Routing Configuration | Static Route |
| Configuration Save | Configuration | |

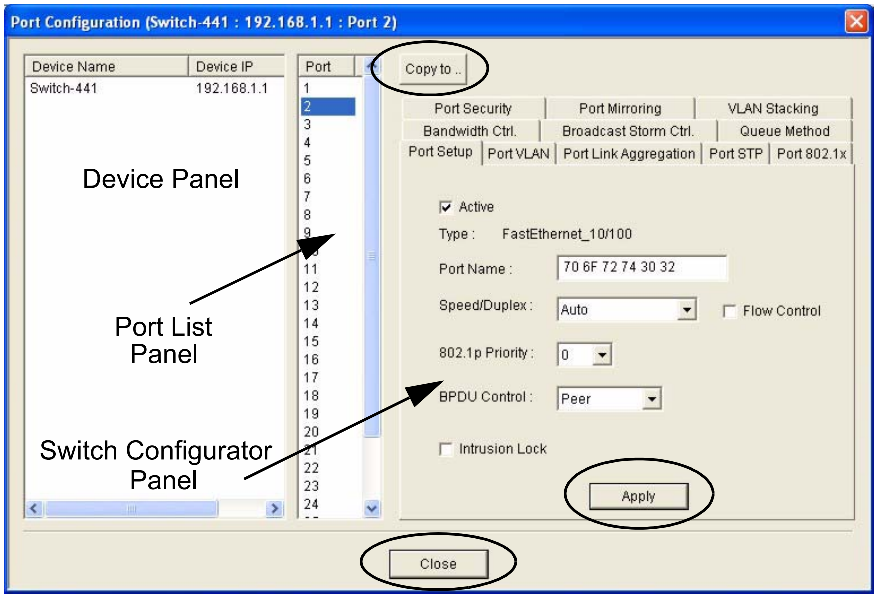
## 9.2 Property Configuration

See Section 3.1.2 on page 53 for information on the **Edit Device** screen.

## 9.3 Introducing the EMS 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 66** Configuration Window Panels



Port Configuration (Switch-441 : 192.168.1.1 : Port 2)

| Device Name | Device IP |
|---|---|
| Switch-441 | 192.168.1.1 |

☑ Active

Type : FastEthernet_10/100

Port Name : 70 6F 72 74 30 32

Speed/Duplex : Auto

☐ Flow Control

802.1p Priority : 0

BPDU Control : Peer

☐ Intrusion Lock

The following table describes the elements in this screen.

**Table 25** Configuration Window Panels

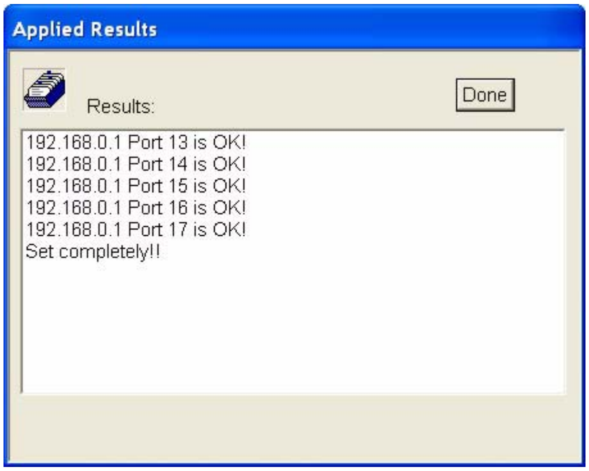
| LABEL | DESCRIPTION |
|---|---|
| Device Panel | This panel displays all active devices currently managed by the EMS. |
| Port List Panel | This field displays a list of switch ports. This list displays in the Ethernet Port Configuration screens only.<br>To make configuration changes to each port or 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. |
| Copy to.. | Click the **Copy to..** button to copy the configuration from the switch that you are currently configuring to one or more switches. Port configurations can also be copied to other device ports in the Ethernet Port Configuration screens. |
| Switch Configurator | Use this panel to make configuration changes to a device based on a port or multiple ports selected in the Port List Panel.<br>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. |
| Apply | Click **Apply** to save configuration changes to the switch. |
| Close | Click **Close** to close a configuration screen. If you close a screen without first clicking **Apply**, configuration changes will not be saved. |

## 9.3.1 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. Click **Apply** when you are satisfied with the configuration changes.

The following example screen displays.

**Figure 67** Applied Results



192.168.0.1 Port 13 is OK!
192.168.0.1 Port 14 is OK!
192.168.0.1 Port 15 is OK!
192.168.0.1 Port 16 is OK!
192.168.0.1 Port 17 is OK!
Set completely!!

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

## 9.3.2 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 Switch Configurator Panel.

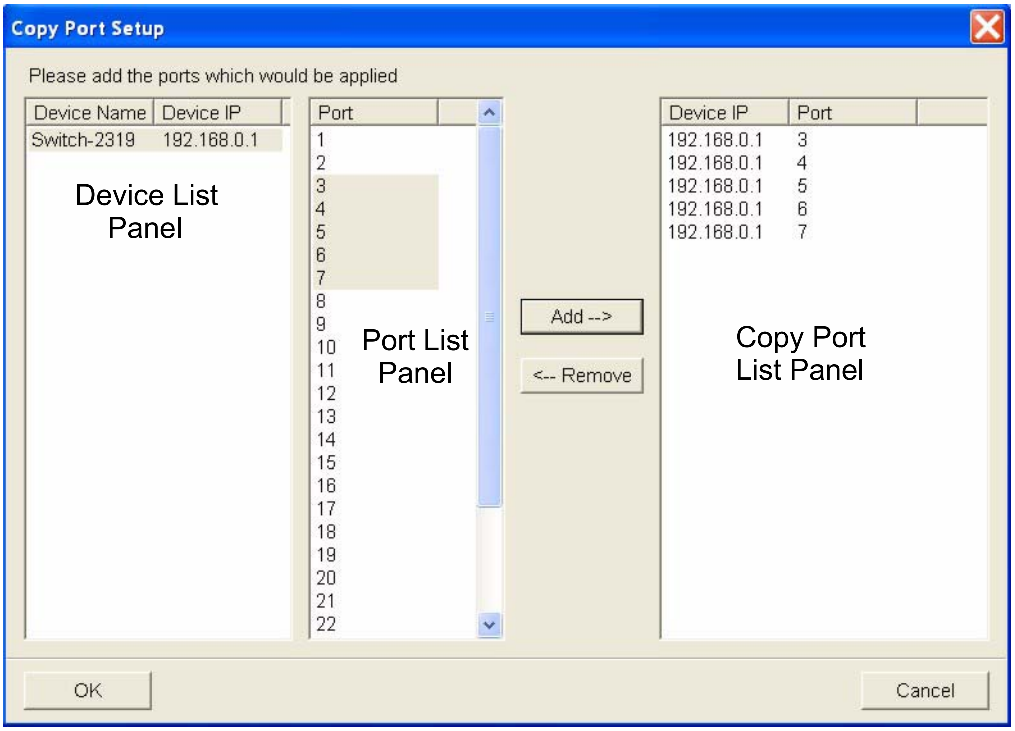
3 Select a port or multiple ports (by pressing the [CTRL] key and clicking at the same time) from the Port List Panel.

4 Make your configuration changes in the Switch Configurator Panel and click the **Apply** button.

5 Click the **Copy to..** button.

6 The following example screen displays.

**Figure 68** Copy Port Screen



Copy Port Setup

Please add the ports which would be applied

| Device Name | Device IP |
|---|---|
| Switch-2319 | 192.168.0.1 |

| Port |
|---|
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 6 |
| 7 |
| 8 |
| 9 |
| 10 |
| 11 |
| 12 |
| 13 |
| 14 |
| 15 |
| 16 |
| 17 |
| 18 |
| 19 |
| 20 |
| 21 |
| 22 |

| Device IP | Port |
|---|---|
| 192.168.0.1 | 3 |
| 192.168.0.1 | 4 |
| 192.168.0.1 | 5 |
| 192.168.0.1 | 6 |
| 192.168.0.1 | 7 |

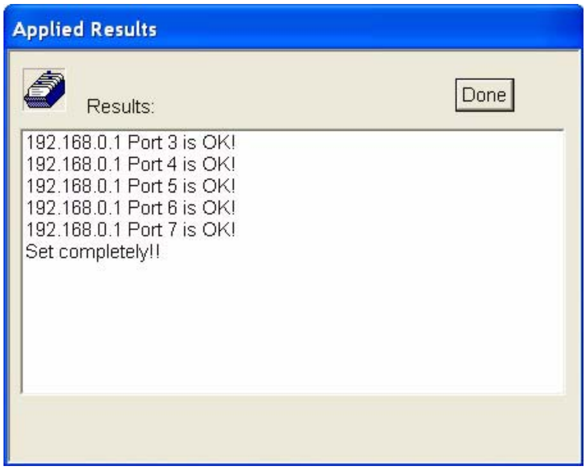
The following table describes the labels in this screen.

**Table 26** Copy Port Screen

| 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 **Add** to display the port(s) to which you want to copy from the switch you are currently configuring. |
| Remove | Click **Remove** 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 **OK** to copy the configuration from ycurrent switch to the device port(s) displayed in the Copy Port List Panel panel. |
| Cancel | Click **Cancel** to return to the previous screen. |

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

**Figure 69** Copy Successful



```
192.168.0.1 Port 3 is OK!
192.168.0.1 Port 4 is OK!
192.168.0.1 Port 5 is OK!
192.168.0.1 Port 6 is OK!
192.168.0.1 Port 7 is OK!
Set completely!!
```

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

# CHAPTER 10
# System Configuration

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

## 10.1 System Info

See Section 2.9 on page 48 for information about the switch.

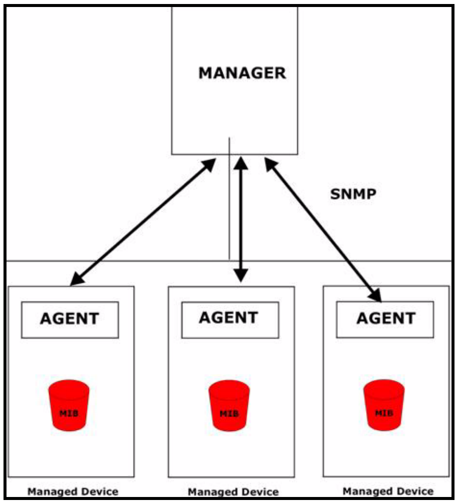
## 10.2 SNMP

This explains explains SNMP configuration.

### 10.2.1 About 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 70** 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 (the ES-3124). 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 27** 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.

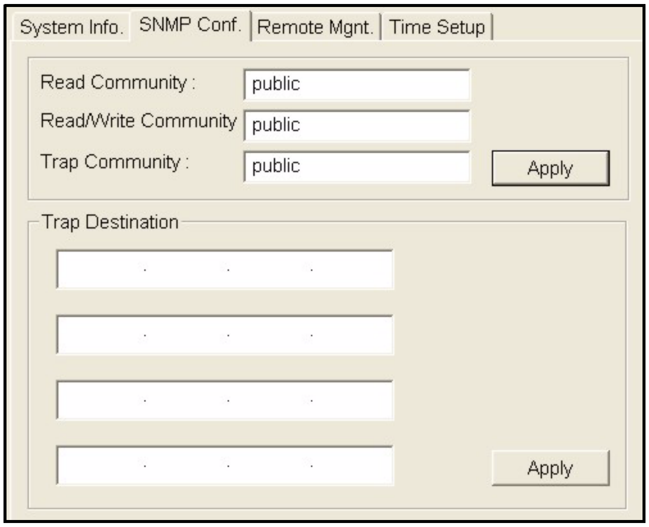
## 10.2.2 Configuring SNMP

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 71** Configuration: System Configuration: SNMP Conf.



Read Community : public

Read/Write Community public

Trap Community : public

The following table describes the labels in this screen.

**Table 28** Configuration: 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 **Apply** 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 **Apply** to save the trap destination changes back to the switch. |

# 10.3 Remote Management

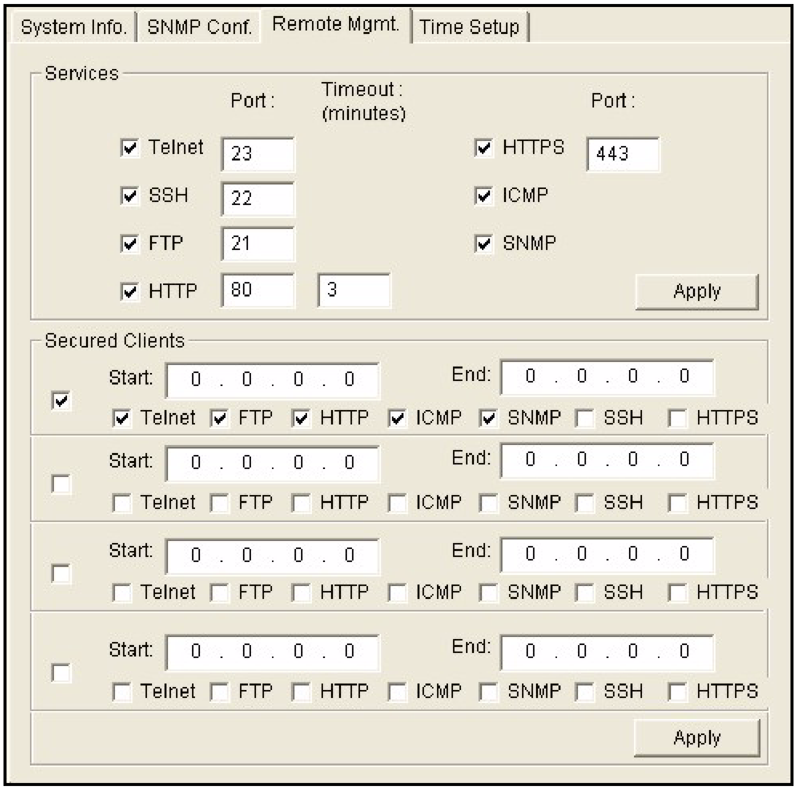
Remote management allows you to determine which services/protocols can access which device interface (if any) from which computers. You can customize the service port and the secured client IP address to enhance security and flexibility.

## 10.3.1 Configuring Remote Management

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 Mgnt**. tab.

**Figure 72** Configuration: System Configuration: Remote Management



Services

| | Port : | Timeout : (minutes) | | Port : |
|---|---|---|---|---|
| ☑ Telnet | 23 | | ☑ HTTPS | 443 |
| ☑ SSH | 22 | | ☑ ICMP | |
| ☑ FTP | 21 | | ☑ SNMP | |
| ☑ HTTP | 80 | 3 | | |

Secured Clients

| | Start: | End: | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0 | ☑ Telnet | ☑ FTP | ☑ HTTP | ☑ ICMP | ☑ SNMP | □ SSH | □ HTTPS |
| □ | 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0 | □ Telnet | □ FTP | □ HTTP | □ ICMP | □ SNMP | □ SSH | □ HTTPS |
| □ | 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0 | □ Telnet | □ FTP | □ HTTP | □ ICMP | □ SNMP | □ SSH | □ HTTPS |
| □ | 0 . 0 . 0 . 0 | 0 . 0 . 0 . 0 | □ Telnet | □ FTP | □ HTTP | □ ICMP | □ SNMP | □ SSH | □ HTTPS |

The following table describes the labels in this screen.

**Table 29** Configuration: 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 **Apply** 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 **End** 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 **Start** field. |

**Table 29** Configuration: System Configuration: Remote Management (continued)

| LABEL | DESCRIPTION |
|---|---|
| Telnet, FTP, HTTP, ICMP, SNMP, ICMP, SSH, HTTPS | Select the checkbox to allow the trusted computer(s) in the IP address range specified above to use this service to manage the switch. |
| Apply | Click **Apply** to save the changes back to the switch. |

# 10.4 Time Setup

The EMS 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 EMS. Use the **Time Setup** screen to update the time and date settings of the EMS. The real time is then displayed in the system messages.

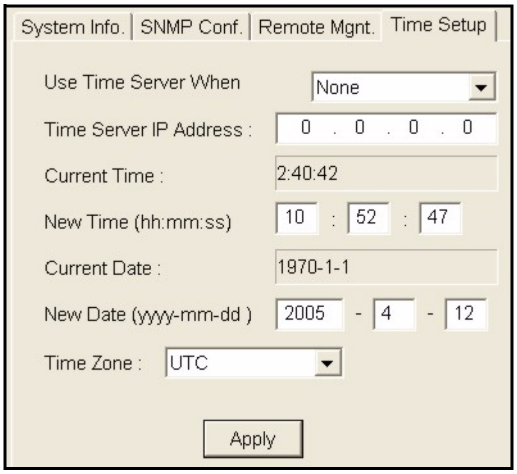
## 10.4.1 Configuring Time Setup

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 73** Configuration: System Configuration: Time Setup



Use Time Server When: None
Time Server IP Address : 0 . 0 . 0 . 0
Current Time : 2:40:42
New Time (hh:mm:ss) 10 : 52 : 47
Current Date : 1970-1-1
New Date (yyyy-mm-dd ) 2005 - 4 - 12
Time Zone : UTC

The following table describes the labels in this screen.

**Table 30** Configuration: System Configuration: Time Setup

| LABEL | DESCRIPTION |
|---|---|
| Use Time Server When | Select the time service protocol that your time server sends when you start the EMS. 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.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>**NTP (RFC-1305)** is similar to **Time (RFC-868)**.<br>**None** is the default; enter the time manually. |
| Time Server IP Address | Enter the IP address or domain name 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. |
| Time Zone | Select the time difference between your time zone and Universal Time Coordinate (UTC) formerly known as Greenwich Mean Time (GMT). |
| Apply | Click **Apply** to save the changes. |

# CHAPTER 11
# Switch Configuration

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

## 11.1 IGMP Snooping

IGMP (Internet Group Multicast Protocol) is a session-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.

A layer-2 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.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, group multicast traffic is only forwarded 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.

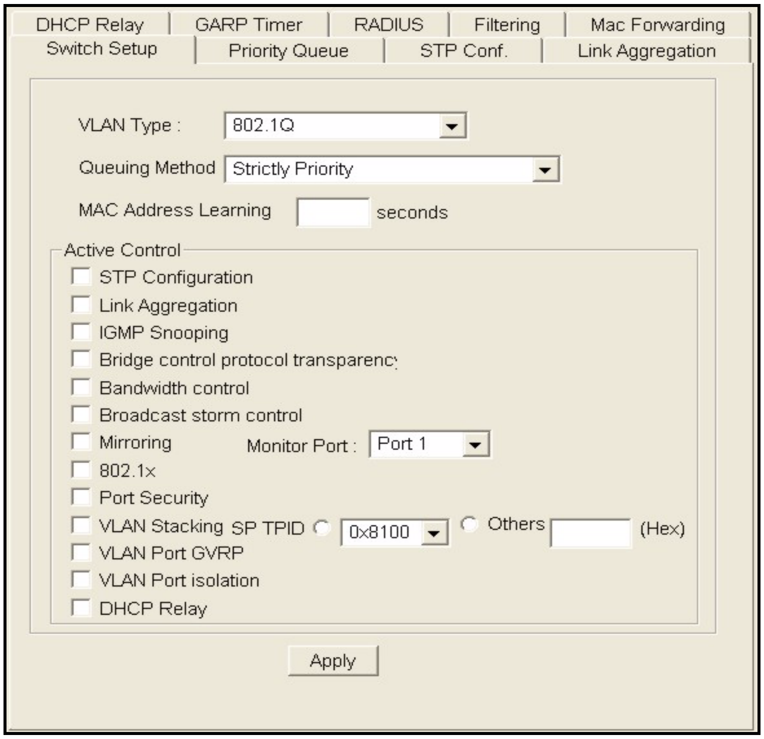
## 11.2 Switch Setup

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** and then the **Switch Setup** tab.

The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to Section 13.2 on page 126 for more information.

**Figure 74** Configuration: Switch Configuration: Switch Setup



VLAN Type : 802.1Q

Queuing Method: Strictly Priority

MAC Address Learning ____ seconds

Active Control

- □ STP Configuration
- □ Link Aggregation
- □ IGMP Snooping
- □ Bridge control protocol transparenc
- □ Bandwidth control
- □ Broadcast storm control
- □ Mirroring Monitor Port : Port 1
- □ 802.1x
- □ Port Security
- □ VLAN Stacking SP TPID ○ 0x8100 ○ Others ____ (Hex)
- □ VLAN Port GVRP
- □ VLAN Port isolation
- □ DHCP Relay

The following table describes the labels in this screen.

**Table 31** Configuration: Switch Configuration: Switch Setup

| LABEL | DESCRIPTION |
|---|---|
| VLAN Type | Choose **802.1Q** or **Port Based** from the drop-down list box. The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN Type or Port Based VLAN Type in this screen. See Section 13.2 on page 126 and the VLAN chapter for more information on VLANs. |
| Queuing Method | Select **Strictly Priority** or **Weighted Fair Scheduling** from the drop-down list box.<br>**Strictly Priority** services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest.<br>**Weighted Fair Scheduling** is used to guarantee each queue’s minimum bandwidth based on their bandwidth portion (weight). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. |
| MAC Address Learning | MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.<br>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). |
| Active Control | |
| STP Configuration | Select the check box to activate STP. |
| Link Aggregation | Select the check box to activate link aggregation. |

**Table 31** Configuration: Switch Configuration: Switch Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| IGMP Snooping | Select the check box to enable IGMP snooping. See Section 11.1 on page 98 for more information on IGMP snooping. |
| Bridge control protocol transparency | Select the check box to allow the switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the **Port Setup** screen. |
| 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. |
| 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 this drop-down list box. |
| 802.1x | Select the check box to activate 802.1x authentication. |
| Port Security | Select the check box to activate port security. |
| VLAN Stacking SP TPID | SP TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose **0x8100** or **0x9100** from the drop-down list box or select **Others** 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 **Others** text field. |
| VLAN Port 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. |
| Port Isolation | Port Isolation allows each port to communicate with the CPU port, uplink ports and stacking ports 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. |
| Apply | Click **Apply** to save your changes back to the switch. |

# 11.3 Priority Queue

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queue Method** screen to configure queuing algorithms for outgoing traffic.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

## 11.3.1 Strictly Priority

Strictly Priority (SP) services queues based on priority only. As traffic comes into the switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

## 11.3.2 Weighted Fair Scheduling

Weighted Fair Scheduling is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (portion) when there is traffic congestion. WFS is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on. Guaranteed bandwidth is calculated as follows:

$$\frac{\text{Queue Weight}}{\text{Total Queue Weight}} \quad \text{x Port Speed}$$

For example, using the default setting, Q0 on Port 1 gets a guaranteed bandwidth of:

$$\frac{1}{1+2+3+4+5+6+7+8} \quad \text{x 100 Mbps = 3 Mbps}$$

## 11.3.3 Configuring Priority Queue

Follow the steps below to configure priority queuing.

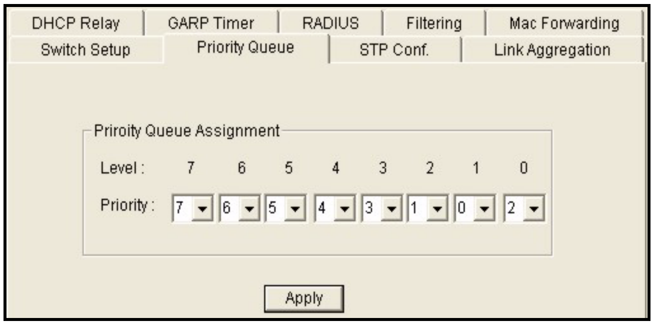
1 In the Device Panel list, select a device and then right-click.

2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select a **Queuing Method** from the drop-down list box and then click **Apply**.

4 Click the **Priority Queue** tab to display the following screen.

**Figure 75** Configuration: Switch Configuration: Priority Queue



Priroity Queue Assignment

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Level : | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Priority : | 7 | 6 | 5 | 4 | 3 | 1 | 0 | 2 |

The following table describes the labels in this screen.

**Table 32** Configuration: 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. The switch has 8 physical queues that you can map to the 8 priority levels. 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. See also Section 13.7 on page 131 for related information. |
| 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 **Apply** to save your changes back to the switch. |

## 11.4 STP Configuration

This section discribes STP and how to configure STP.

## 11.5 STP Overview

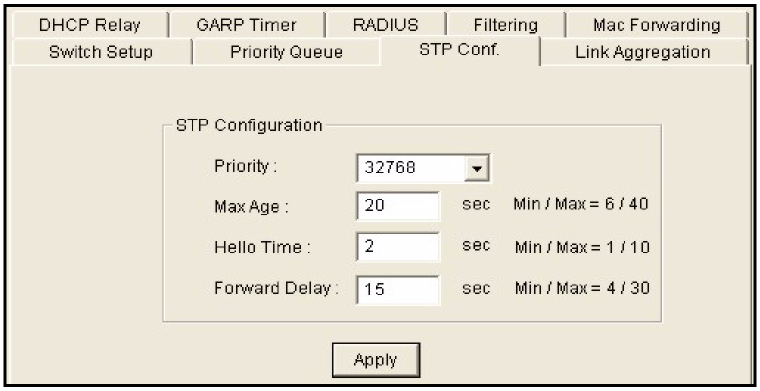
The switch supports STP. STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a device to interact with other STP-aware devices in your network to ensure that only one path exists between any two stations on the network.

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

### 11.5.1 Configuring STP Parameters

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 **STP Configuration** check box and then click **Apply**.
4. Click **Configuration**, **Switch Configuration** and then the **STP Conf.** tab to display the following screen.

**Figure 76** Configuration: Switch Configuration: STP Conf.



STP Configuration

Priority : 32768

Max Age : 20 sec Min / Max = 6 / 40

Hello Time : 2 sec Min / Max = 1 / 10

Forward Delay : 15 sec Min / Max = 4 / 30

The following table describes the labels in this screen.

**Table 33** Configuration: 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).<br>The lower the numeric value you assign, the higher the priority for this bridge.<br>**Priority** determines the root bridge, which in turn determines **Hello Time**, **Max Age** and **Forward Delay**. |
| 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). |

**Table 33** Configuration: Switch Configuration: STP Conf. (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 **Apply** to save your changes back to the switch. |

# 11.6 Link Aggregation

## 11.6.1 Introduction to 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.

## 11.6.2 Dynamic Link Aggregation

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

The switch supports the link aggregation IEEE802.3ad 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.

## 11.6.3 Link Aggregation ID

LACP aggregation ID consists of the following information:

**Table 34** 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 35** 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 |

## 11.6.4 Configuring Link Aggregation

1 In the Device Panel list, select a device and then right-click.

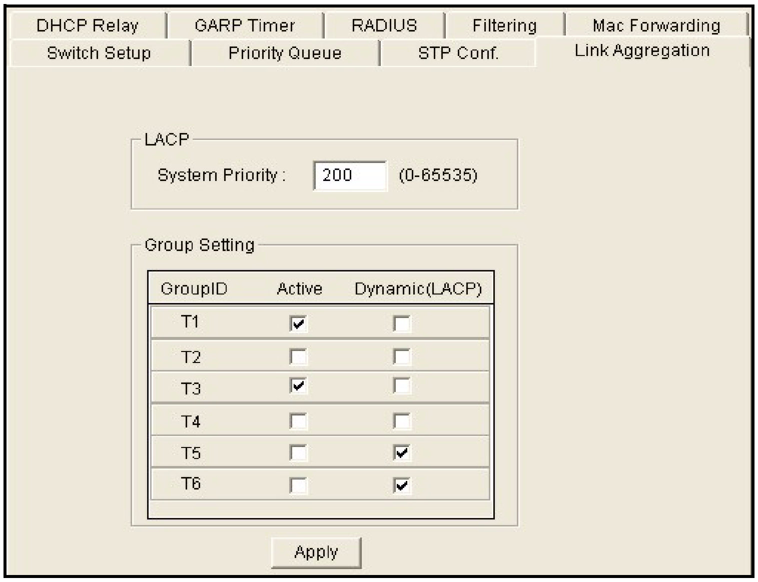
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **Link Aggregation** check box and then click **Apply**.

4 Click **Configuration**, **Switch Configuration** and then the **Link Aggregation** tab to display the following screen.

You can configure up to six link aggregation groups and each group can aggregate up to eight ports.

**Figure 77** Configuration: Switch Configuration: Link Aggregation



LACP

System Priority : 200 (0-65535)

Group Setting

| GroupID | Active | Dynamic(LACP) |
|---|---|---|
| T1 | ☑ | □ |
| T2 | □ | □ |
| T3 | ☑ | □ |
| T4 | □ | □ |
| T5 | □ | ☑ |
| T6 | □ | ☑ |

The following table describes the labels in this screen.

**Table 36** Configuration: Switch Configuration: Link Aggregation

| TABLE | DESCRIPTION |
|---|---|
| LACP | |
| System Priority | LACP system priority is a number between 0 and 65,355. 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 **Apply** to save your changes back to the switch. |

## 11.7 DHCP Relay

This section describes the DHCP relay and shows you how to configure the DHCP Relay screen.

### 11.7.1 Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a DHCP server. You can configure the switch to relay client TCP/IP configuration requests to a DHCP server and the server's responses back to the clients.

### 11.7.2 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)

### 11.7.3 Configuring DHCP Relay

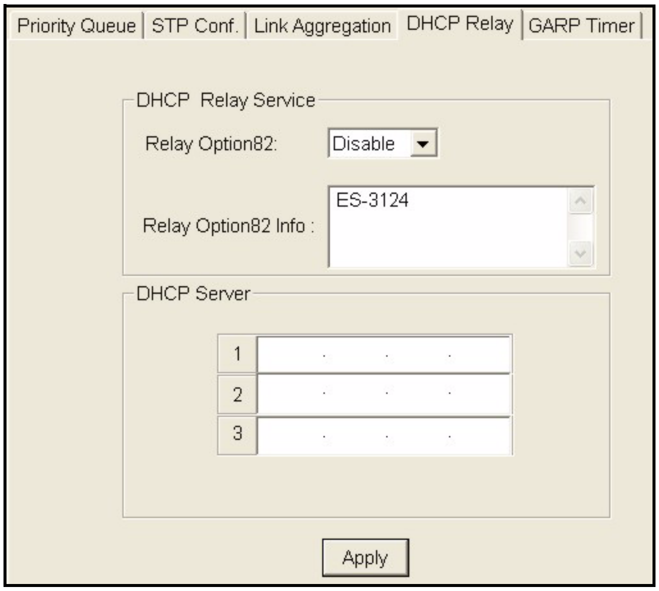
**1** In the Device Panel list, select a device and then right-click.

**2** Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

**3** Select the **DHCP Relay** check box and then click **Apply**.

**4** Click **Configuration**, **Switch Configuration** and then the **DHCP Relay** tab to display the following screen.

**Figure 78** Configuration: Switch Configuring: DHCP Relay



Relay Option82: Disable

Relay Option82 Info : ES-3124

The following table describes the labels in this screen.

**Table 37** Configuration: Switch Configuring: DHCP Relay

| TABLE | DESCRIPTION |
|---|---|
| DHCP Relay Service | Configure the fields below to set the DHCP relay settings. |
| Relay Option 82 | Enable DHCP relay info to have the switch add the originating slot and port numbers to client TCP/IP configuration requests that it relays to a DHCP server. |
| Relay Option82 Info | Use this field to specify up to 24 ASCII characters of additional information for the switch to add to the DHCP client TCP/IP configuration requests that it relays to a DHCP server. An example would be the casing number of the switch or the ISP’s name. |
| DHCP Server | This table displays the IP address(es) and status of the DHCP servers. You can configure up to three DHCP servers. |
| Apply | Click **Apply** to save the changes. |

## 11.8 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.

### 11.8.1 Configuring GARP Timer

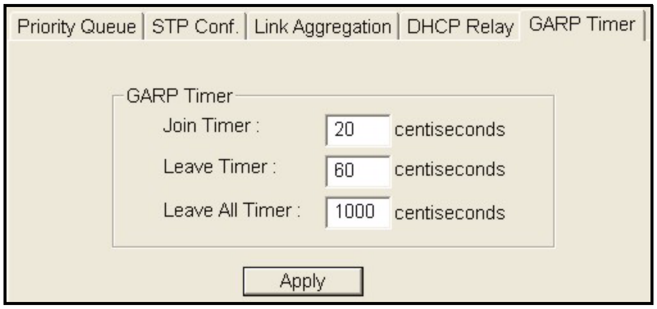
1 In the Device Panel list, select a device and then right-click.

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 79** Configuration: Switch Configuration: Garp Timer



Join Timer : 20 centiseconds

Leave Timer : 60 centiseconds

Leave All Timer : 1000 centiseconds

The following table describes the labels in this screen.

**Table 38** Configuration: Switch Configuration: Garp Timer

| LABEL | DESCRIPTION |
|---|---|
| Join Timer | **Join Timer** 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 | **Leave Timer** 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 **Join Timer**; the default is 60 centiseconds. |
| Leave All Timer | **Leave All Timer** 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 **Leave Timer**; the default is 100 centiseconds. |
| Apply | Click **Apply** to save your changes back to the switch. |

# 11.9 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.

## 11.9.1 Introduction to Authentication

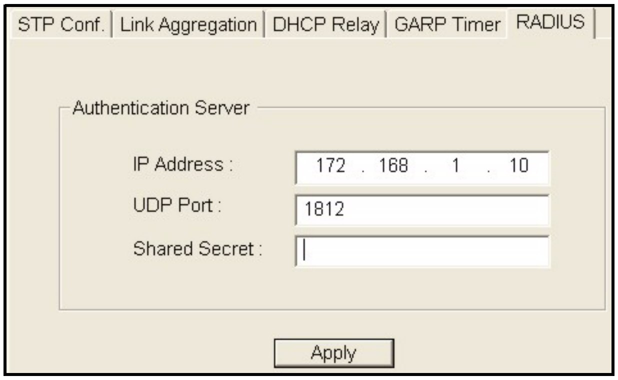
IEEE 802.1x is an extended authentication protocol  that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

## 11.9.2 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 80** Configuration: Switch Configuration: RADIUS



IP Address : 172 . 168 . 1 . 10

UDP Port : 1812

Shared Secret :

The following table describes the labels in this screen.

**Table 39** Configuration: 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. |

**Table 39** Configuration: Switch Configuration: RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Shared Secret | Specify a password (up to 31 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 **Apply** to save your changes back to the switch. |

## 11.10 MAC Forwarding

This chapter discusses MAC address forwarding.

### 11.10.1 Introduction to Static MAC Forward Setup

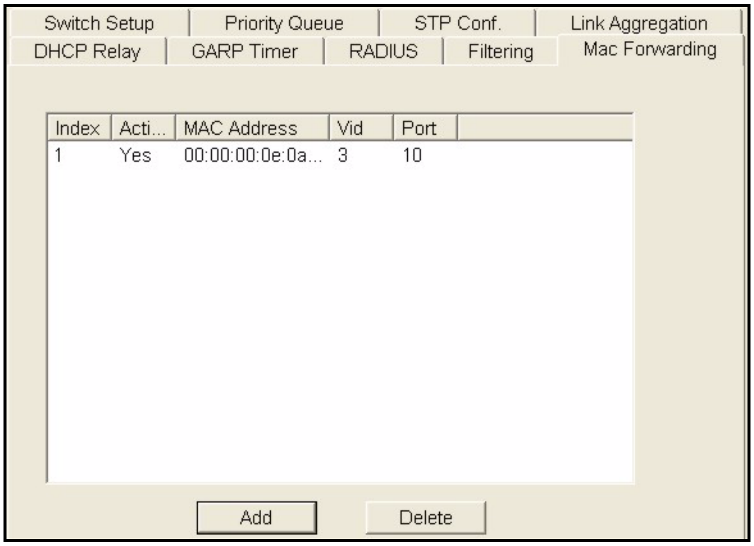
A static MAC address entry is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. Devices that match static MAC address rules on a port can only receive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

### 11.10.2 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 81** Configuration: Switch Configuration: MAC Forwarding



| Index | Acti... | MAC Address | Vid | Port |
|---|---|---|---|---|
| 1 | Yes | 00:00:00:0e:0a... | 3 | 10 |

The following table describes the labels in this screen.

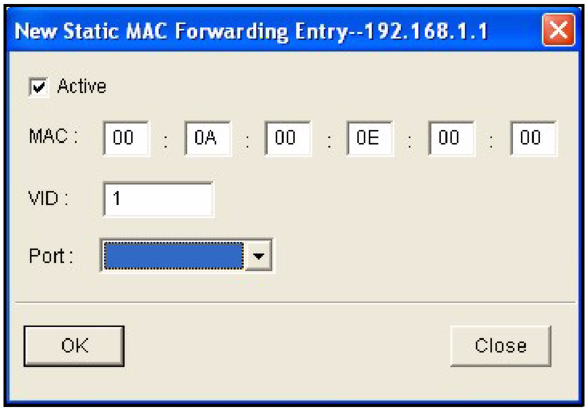
**Table 40** Configuration: Switch Configuration: MAC Forwarding

| 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 (**Yes**) or not (**No**). 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 **Add** 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 **Delete** button. |

### 11.10.2.1 Adding and Editing Static MAC Forwarding Rules

To add a new rule, click the **Add** button in the previous screen. To change the settings of a rule, select a rule and and click **Add** in the previous screen.

**Figure 82** Configuration: Switch Configuration: MAC Forwarding: Add



New Static MAC Forwarding Entry--192.168.1.1

☑ Active

MAC : 00 : 0A : 00 : 0E : 00 : 00

VID : 1

Port :

The following table describes the labels in this screen..

**Table 41** Configuration: 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 **OK** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen. |
| Close | Click **Close** to close the screen. |

# 11.11 Filtering

This chapter discusses MAC address port filtering.

## 11.11.1 Introduction to Filtering

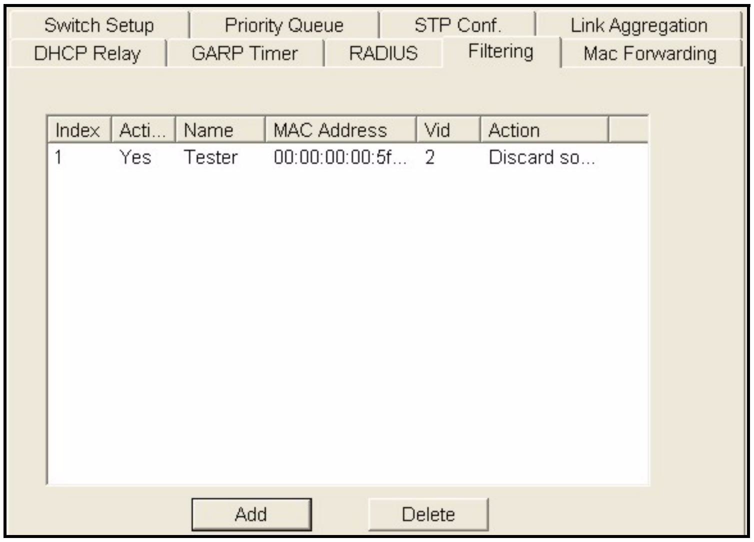
Filtering means sifting traffic going through the switch based on the source and/or destination MAC addresses and VLAN group (ID).

## 11.11.2 Configuring Filtering

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 83** Configuration: Switch Configuration: Filtering



| Index | Acti... | Name | MAC Address | Vid | Action |
|---|---|---|---|---|---|
| 1 | Yes | Tester | 00:00:00:00:5f... | 2 | Discard so... |

The following table describes the labels in the summary table.

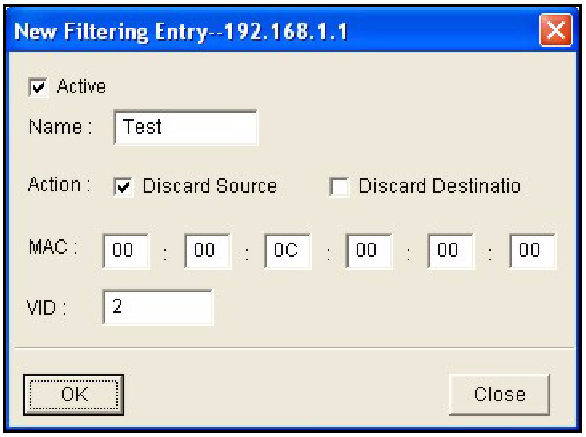
**Table 42** Configuration: Switch Configuration: Filtering

| LABEL | DESCRIPTION |
|---|---|
| Index | This field displays the index number of the rule. Click an index number to edit the rule. |
| Active | This field displays **Yes** when the rule is activated and **No** when is it deactivated. |
| Name | This field displays the descriptive name for this rule. This is for identification purpose only. |
| MAC Address | This field displays the MAC address with the VLAN identification number to which the MAC address belongs or a combination of the two. |
| VID | This field displays the VLAN identification number. |
| Action | This field displays the filtering action (**Discard both**, **Discard source** or **Discard dest.**). |
| Add | Click the **Add** button to create a filtering rule. |
| Delete | Select the rule(s) that you want to remove in the Filtering table and then click the **Delete** button. |

### 11.11.2.1 Adding and Editing Static Filtering Rules

To add a new rule, click a the **Add** button in the previous screen. To change the settings of a rule, select a rule and and click **Add** in the previous screen.

**Figure 84** Configuration: Switch Configuration: Filtering: Add



New Filtering Entry--192.168.1.1

☑ Active

Name : Test

Action : ☑ Discard Source ☐ Discard Destinatio

MAC : 00 : 00 : 0C : 00 : 00 : 00

VID : 2

The following table describes the labels in this screen..

**Table 43** Configuration: Switch Configuration: Filtering: 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. |
| Name | Type a descriptive name for this filter rule. This is for identification purpose only. |
| Action | Select **Discard Source** to drop frame from the source MAC address (specified in the MAC field). The switch can still send frames to the MAC address.<br>Select **Discard Destination** to drop frames to the destination MAC address (specified in the MAC address). The switch can still receive frames originating from the MAC address.<br>Select **Discard Source** and **Discard Destination** to block traffic to/from the MAC address specified in the MAC field. |
| 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. |
| OK | Click **OK** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen. |
| Close | Click **Close** to close the screen. |

# CHAPTER 12 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.

## 12.1 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.

## 12.2 Configuring 802.1Q VLAN

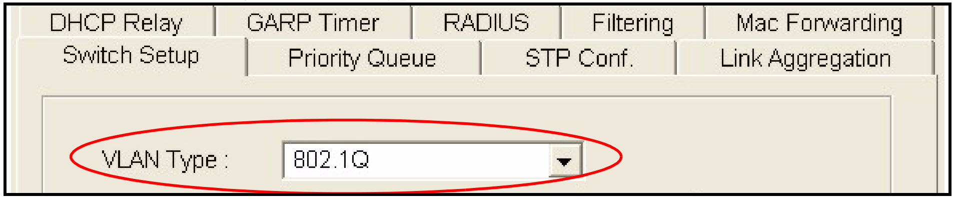
Follow the steps below to set the **802.1Q VLAN Type** on the switch.

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**.

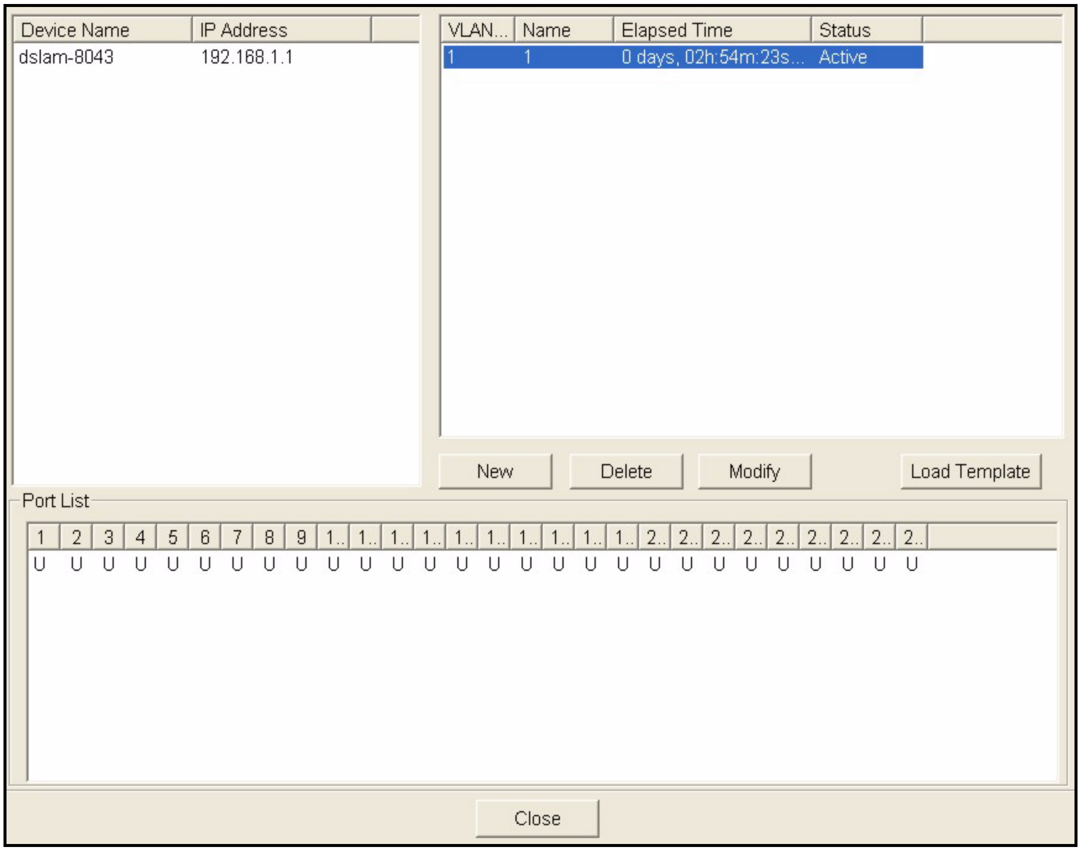
**Figure 85** Selecting a VLAN Type



VLAN Type : 802.1Q

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

**Figure 86** Configuration: VLAN Configuration: 802.1Q



| Device Name | IP Address |
|---|---|
| dslam-8043 | 192.168.1.1 |

| VLAN... | Name | Elapsed Time | Status |
|---|---|---|---|
| 1 | 1 | 0 days, 02h:54m:23s... | Active |

Port List

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |

The following table describes the labels in this screen.

**Table 44** Configuration: 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. |
| Elapsed Time | This field displays the time elapsed since the VLAN was created. |
| Status | This field displays **ACTIVE** if the VLAN is active and will remain so after the next reset of the device. This field is DynamicGVRP 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. |

**Table 44** Configuration: VLAN Configuration: 802.1Q (continued)

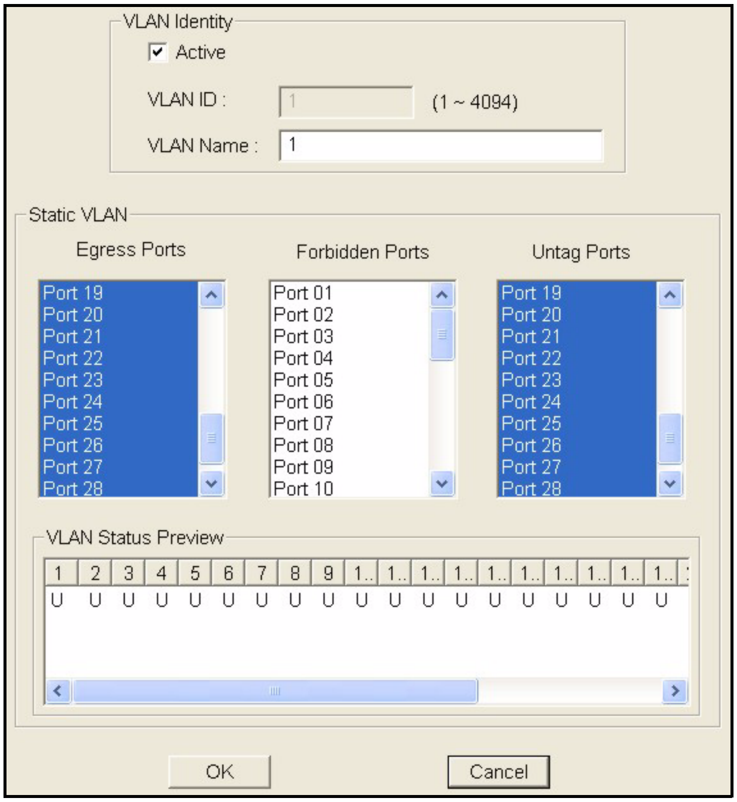
| LABEL | DESCRIPTION |
|---|---|
| New | Click **New** to create a new VLAN. You must enter a **VLAN ID** and a **VLAN Name** to create a new **VLAN**. The new VLAN and name is displayed in the left-hand column in this screen. |
| Delete | Click on a VLAN in the left-hand column of this screen and then click the **Delete** button to remove it from the VLAN template. |
| Modify | Click on a VLAN in the left-hand column of this screen. Change the **VLAN ID**, **VLAN Name** or change the configuration of the egress, forbidden and untagged ports. Click the **Modify** button to save the changes. |
| Load Template | Use a VLAN template to overwrite existing selected VLANs. Select one or more VLANs and click the **Load Template** button. See Section 4.1 on page 56 for more information. |
| Port List | Click on a port in the **Egress Ports** 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 the following table for the VLAN port type descriptions. |
| Close | Click **Close** to close the screen. |

## 12.2.1 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 87** Configuration: VLAN Configuration: 802.1Q: Modify



VLAN Identity

☑ Active

VLAN ID : 1 (1 ~ 4094)

VLAN Name : 1

Static VLAN

| Egress Ports | Forbidden Ports | Untag Ports |
|---|---|---|
| Port 19 | Port 01 | Port 19 |
| Port 20 | Port 02 | Port 20 |
| Port 21 | Port 03 | Port 21 |
| Port 22 | Port 04 | Port 22 |
| Port 23 | Port 05 | Port 23 |
| Port 24 | Port 06 | Port 24 |
| Port 25 | Port 07 | Port 25 |
| Port 26 | Port 08 | Port 26 |
| Port 27 | Port 09 | Port 27 |
| Port 28 | Port 10 | Port 28 |

VLAN Status Preview

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |

The following table describes the labels in this screen.

**Table 45** Configuration: VLAN Configuration: 802.1Q: Modify

| LABEL | DESCRIPTION |
|---|---|
| VLAN Identity | Select the **Active** checkbox 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 this if the subscriber's DSL modem or router supports 802.1Q 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 **Egress Ports** 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 the following table for the VLAN port type descriptions. |

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

For switches, an egress port cannot be untagged.

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

**Table 46** VLAN Port Type Descriptions

| LABEL | DESCRIPTION |
|---|---|
| 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 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. |

### 12.2.2 Removing a VLAN

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

## 12.3 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.

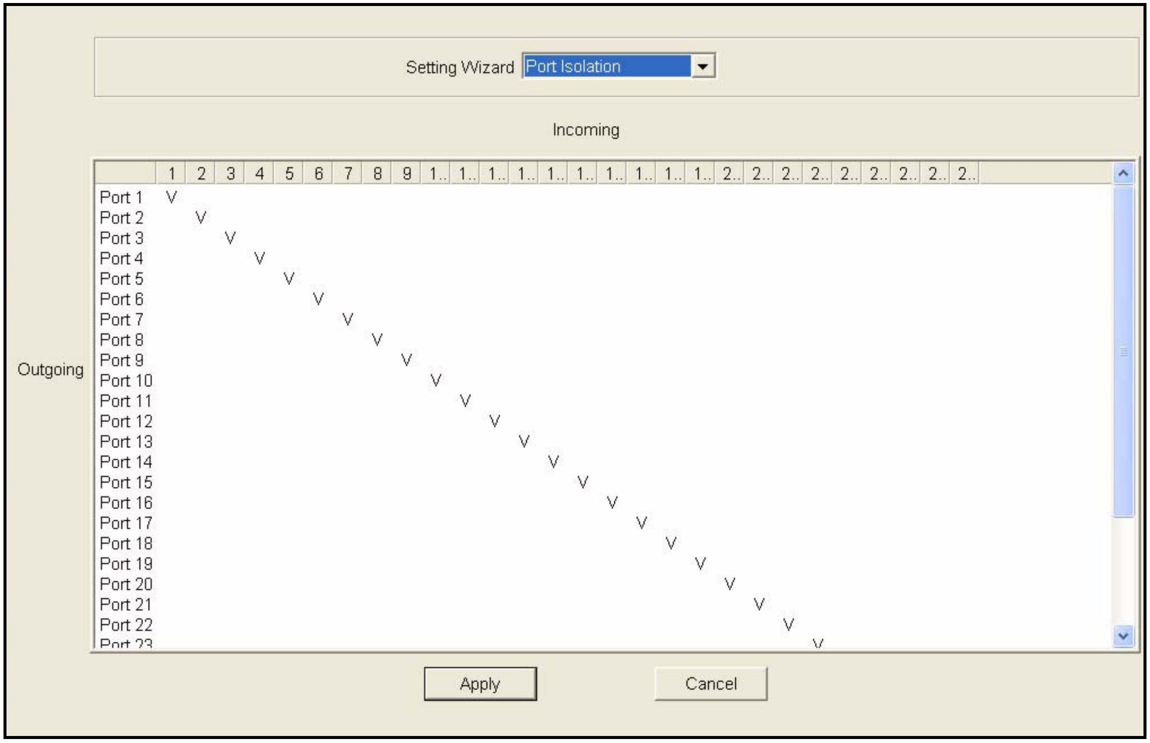
The port-based VLAN setup screen is shown next. The CPU management port forms a VLAN with all Ethernet ports.

### 12.3.1 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 88** Configuration: VLAN Configuration: Port Based



Setting Wizard: Port Isolation

Incoming

Outgoing

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 1.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. | 2.. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Port 1 | V | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Port 2 | | V | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Port 3 | | | V | | | | | | | | | | | | | | | | | | | | | | | | | |
| Port 4 | | | | V | | | | | | | | | | | | | | | | | | | | | | | | |
| Port 5 | | | | | V | | | | | | | | | | | | | | | | | | | | | | | |
| Port 6 | | | | | | V | | | | | | | | | | | | | | | | | | | | | | |
| Port 7 | | | | | | | V | | | | | | | | | | | | | | | | | | | | | |
| Port 8 | | | | | | | | V | | | | | | | | | | | | | | | | | | | | |
| Port 9 | | | | | | | | | V | | | | | | | | | | | | | | | | | | | |
| Port 10 | | | | | | | | | | V | | | | | | | | | | | | | | | | | | |
| Port 11 | | | | | | | | | | | V | | | | | | | | | | | | | | | | | |
| Port 12 | | | | | | | | | | | | V | | | | | | | | | | | | | | | | |
| Port 13 | | | | | | | | | | | | | V | | | | | | | | | | | | | | | |
| Port 14 | | | | | | | | | | | | | | V | | | | | | | | | | | | | | |
| Port 15 | | | | | | | | | | | | | | | V | | | | | | | | | | | | | |
| Port 16 | | | | | | | | | | | | | | | | V | | | | | | | | | | | | |
| Port 17 | | | | | | | | | | | | | | | | | V | | | | | | | | | | | |
| Port 18 | | | | | | | | | | | | | | | | | | V | | | | | | | | | | |
| Port 19 | | | | | | | | | | | | | | | | | | | V | | | | | | | | | |
| Port 20 | | | | | | | | | | | | | | | | | | | | V | | | | | | | | |
| Port 21 | | | | | | | | | | | | | | | | | | | | | V | | | | | | | |
| Port 22 | | | | | | | | | | | | | | | | | | | | | | V | | | | | | |
| Port 23 | | | | | | | | | | | | | | | | | | | | | | | V | | | | | |

The following table describes the labels in this screen.

**Table 47** Configuration: VLAN Configuration: Port Based

| LABEL | DESCRIPTION |
|---|---|
| Setting Wizard | Choose from **All connected** or **Port isolation**.<br>**All connected** 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.<br>**Port isolation** means that each port can only communicate with the **CPU** management port and cannot communicate with each other. All incoming ports are selected while only the **CPU** outgoing port is selected. This option is the most limiting but also the most secure.<br>After you make your selection, click **Apply** 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 Apply at the bottom of the screen. |
| Incoming | 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). **CPU** 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. |
| Outgoing | 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. **CPU** 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. |

**Table 47** Configuration: VLAN Configuration: Port Based (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save the changes, including the “wizard settings”. |
| Cancel | Click **Cancel** to start configuring the screen again. |

# CHAPTER 13 Ethernet Port Configuration

This chapter shows how to configure port setup, port VLAN, port link aggregation, port STP, bandwidth control, broadcast storm control, queuing method, port 802.1x, port security, port mirroring and VLAN stacking.

## 13.1 Port Setup

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

### 13.1.1 Configuring Port Setup

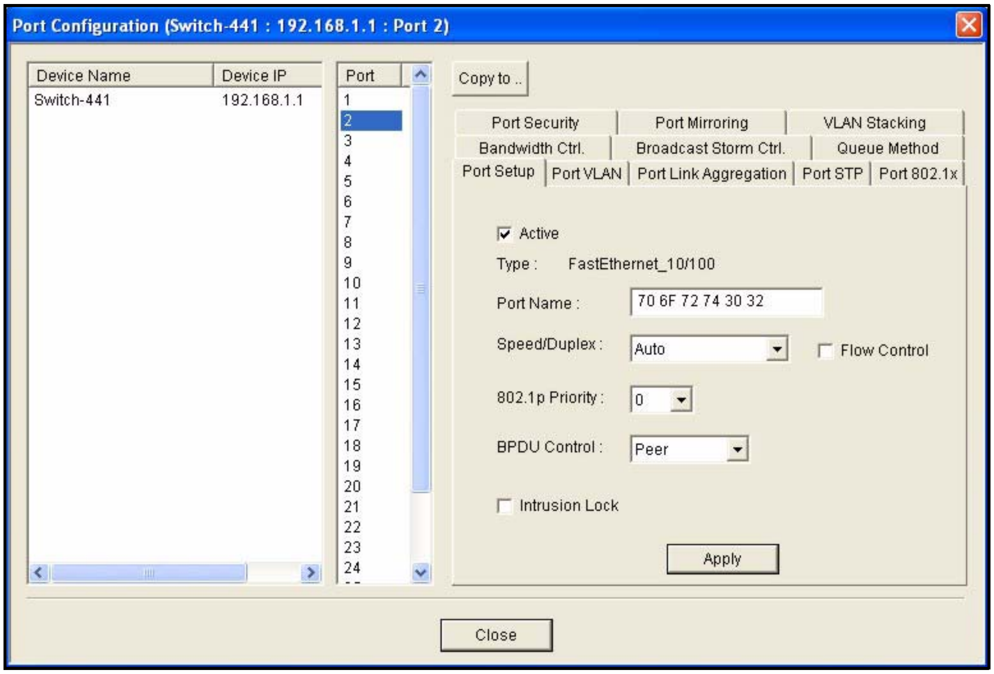
Follow the steps below to configure the **Port Setup** screen.

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 89** Configuration: Ethernet Port Configuration: Port Setup



Port Configuration (Switch-441 : 192.168.1.1 : Port 2)

| Device Name | Device IP |
|---|---|
| Switch-441 | 192.168.1.1 |

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

☑ Active

Type : FastEthernet_10/100

Port Name : 70 6F 72 74 30 32

Speed/Duplex : Auto

□ Flow Control

802.1p Priority : 0

BPDU Control : Peer

□ Intrusion Lock

The following table describes the fields in this screen.

**Table 48** Configuration: Ethernet Port Configuration: Port Setup

| LABEL | DESCRIPTION |
|---|---|
| Port | Select a port index number from the list of ports on the device you want to configure. |
| 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 10/100M for an Ethernet/Fast Ethernet connection and 100/1000M for Gigabit connections. |
| Port Name | This field displays the name of a selected port. |
| Speed/Duplex | Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **100M/Full Duplex** and **1000M/Full Duplex** (for Gigabit ports only).<br>Selecting **Auto** (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. |

**Table 48** Configuration: Ethernet Port Configuration: Port Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Flow Control | 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 IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.<br>IEEE802.3x 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 **Flow Control** to enable it. |
| 802.1p Priority | 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. |
| BPDU Control | Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first.<br>Select **Peer** to process any BPDU (Bridge Protocol Data Units) received on this port.<br>Select **Tunnel** to forward BPDUs received on this port.<br>Select **Discard** to drop any BPDU received on this port.<br>Select **Network** to process a BPDU with no VLAN tag and forward a tagged BPDU. |
| Intrusion Lock | Select the **Intrusion Lock** 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 unauthorised access such as hacking.<br>**Note:** You cannot access a port with intrusion locking enabled after a cable is disconnected and then reconnected. You must clear and re-select the **Intrusion Lock** check box to allow access to the port again. |
| Apply | Click **Apply** to save your changes back to the switch. |

## 13.2 Port VLAN

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

### 13.2.1 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.

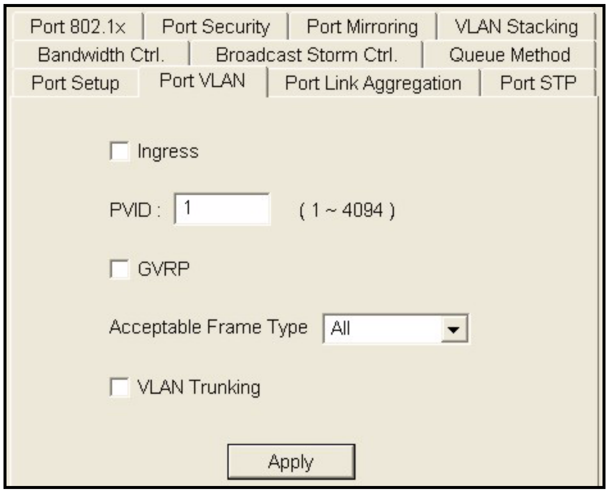
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **VLAN Port GVRP** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Port VLAN** tab.

**5** Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 90** Configuration: Ethernet Port Configuration: Port VLAN



□ Ingress

PVID : 1 ( 1 ~ 4094 )

□ GVRP

Acceptable Frame Type All

□ VLAN Trunking

The following table describes the fields in this screen.

**Table 49** Configuration: Ethernet Port Configuration: Port VLAN

| LABEL | DESCRIPTION |
|---|---|
| Port | Select a port index number from the list of ports on the device you want to configure. |
| Ingress | 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 802.1Q VLAN-unaware switch to an 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 **All** and **Tag Only**. Select **All** to accept all frames with untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames are dropped. |
| 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 **Apply** to save the changes back to the switch. |

## 13.3 Port Link Aggregation

Use the following screen to configure a port trunk group and set LACP timeout.

### 13.3.1 Configuring Port Link Aggregation

Follow the steps below to configure the **Port Link Aggregation** screen.

1 In the Device Panel list, select a device and then right-click.

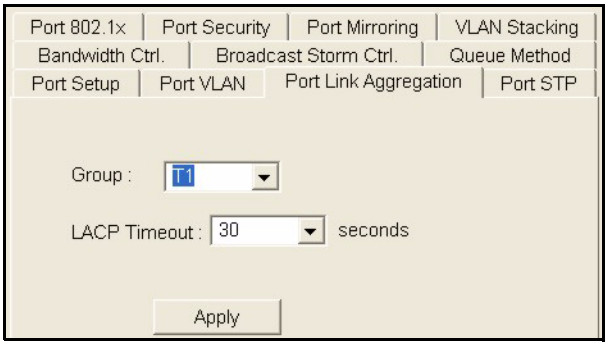
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **Link Aggregation** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Port Link Aggregation** tab.

5 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 91** Configuration: Ethernet Port Configuration: Port Link Aggregation



Group : T1

LACP Timeout : 30 seconds

The following table describes the fields in this screen.

**Table 50** Configuration: 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 **Apply** to save the changes back to the switch. |

## 13.4 Port STP

Use the following screen to configure STP for the selected ports.

### 13.4.1 Configuring Port STP

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

1 In the Device Panel list, right-click on a device.

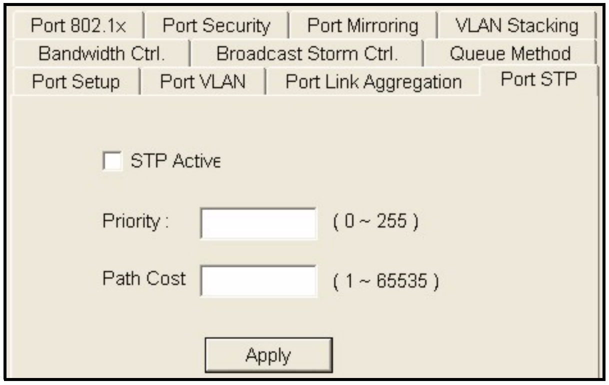
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **STP Configuration** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Port STP** tab.

5 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 92** Configuration: Ethernet Port Configuration: Port STP



□ STP Active

Priority : ( 0 ~ 255 )

Path Cost ( 1 ~ 65535 )

The following table describes the fields in this screen.

**Table 51** Configuration: 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 **Apply** to save the changes back to the switch. |

# 13.5 Bandwidth Control

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

## 13.5.1 Configuring Bandwidth Control

Follow the steps below to configure the **Bandwidth Control** screen.

1 In the Device Panel list, select a device and then right-click.

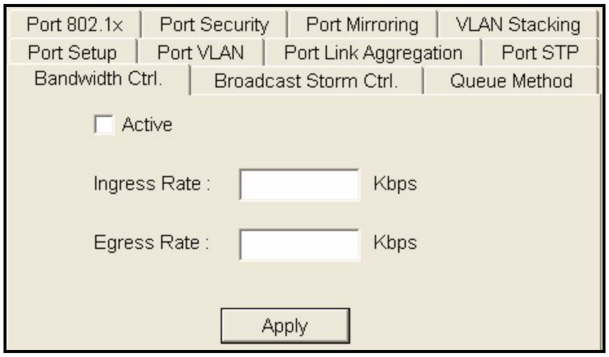
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **Bandwidth control** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Bandwidth Ctrl.** tab.

5 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 93** Configuration: Ethernet Port Configuration: Bandwidth Ctrl.



□ Active

Ingress Rate : Kbps

Egress Rate : Kbps

The following table describes the fields in this screen.

**Table 52** Configuration: Ethernet Port Configuration: Bandwidth Ctrl.

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to enable bandwidth control on the selected port(s).<br>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. |
| Apply | Click **Apply** to save the changes back to the switch. |

## 13.6 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. You can specify limits for each packet type on each port.

### 13.6.1 Configuring Broadcast Storm Control

Follow the steps below to configure the **Broadcast Storm Control** screen.

1 In the Device Panel list, select a device and then right-click.

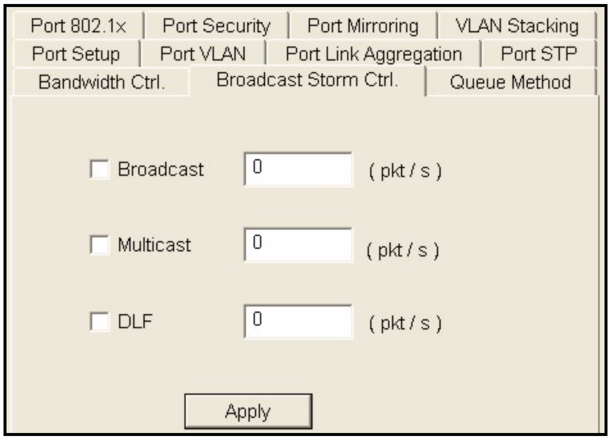
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **Broadcast storm control** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Broadcast Storm Ctrl.** tab.

5 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 94** Configuration: Ethernet Port Configuration: Broadcast Storm Ctrl.



☐ Broadcast 0 ( pkt / s )

☐ Multicast 0 ( pkt / s )

☐ DLF 0 ( pkt / s )

The following table describes the fields in this screen.

**Table 53** Configuration: Ethernet Port Configuration: Broadcast Storm Ctrl.

| LABEL | DESCRIPTION |
|---|---|
| Broadcast (pkt/s) | Select this option and specify how many broadcast packets the port receives per second. |
| Multicast (pkt/s) | Select this option and specify how many multicast packets the port receives per second. |
| DLF (pkt/s) | Select this option and specify how many destination lookup failure (DLF) packets the port receives per second. |
| Apply | Click **Apply** to save the changes back to the switch. |

## 13.7 Queue Method

Queuing is used to help solve performance degradation when there is network congestion. Use the following screen to configure queuing algorithms for outgoing traffic.

### 13.7.1 Configuring Queue Method

Follow the steps below to configure the **Queue Method** screen.

1 In the Device Panel list, select a device and then right-click.

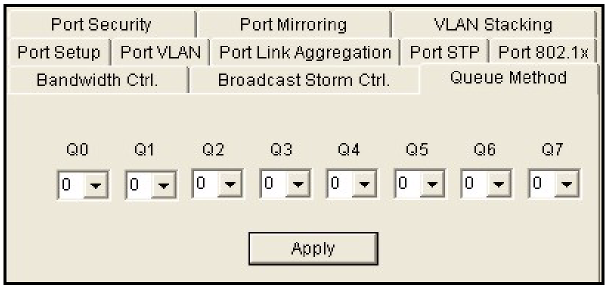
2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select a **Queuing Method** from the drop-down list box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Queue Method** tab.

5 Select the ports from the Port List Panel that you want to apply this configuration.

**Figure 95** Configuration: Ethernet Port Configuration: Queue Method



| Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The following table describes the fields in this screen.

**Table 54** Configuration: Ethernet Port Configuration: Queue Method

| LABEL | DESCRIPTION |
|---|---|
| Q0 ~ Q7 | Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest.Weighted Fair Scheduling is used to guarantee each queue’s minimum bandwidth based on their bandwidth portion (weight) (the number you select from the drop-down list box). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights.<br>Select a queue weight from the drop-down list box. |
| Apply | Click **Apply** to save the changes back to the switch. |

# 13.8 Port 802.1x

Use the following screen to configure reauthentication for selected ports.

## 13.8.1 Configuring Port 802.1x

Follow the steps below to configure the **Port 802.1x** screen.

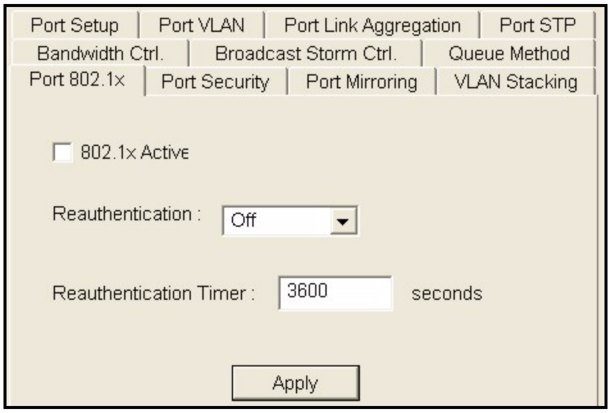
1 In the Device Panel list, select a device and then right-click.

2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **802.1x** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Port 802.1x** tab.

**Figure 96** Configuration: Ethernet Port Configuration: Port 802.1x



□ 802.1x Active

Reauthentication : Off

Reauthentication Timer : 3600 seconds

The following table describes the fields in this screen.

**Table 55** Configuration: Ethernet Port Configuration: Port 802.1x

| LABEL | DESCRIPTION |
|---|---|
| 802.1x Active | Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch before configuring it on each port. |
| Reauthentication | Select **On** 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 **Apply** to save the changes back to the switch. |

# 13.9 Port Security

## 13.9.1 About 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.

## 13.9.2 Configuring Port Security

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

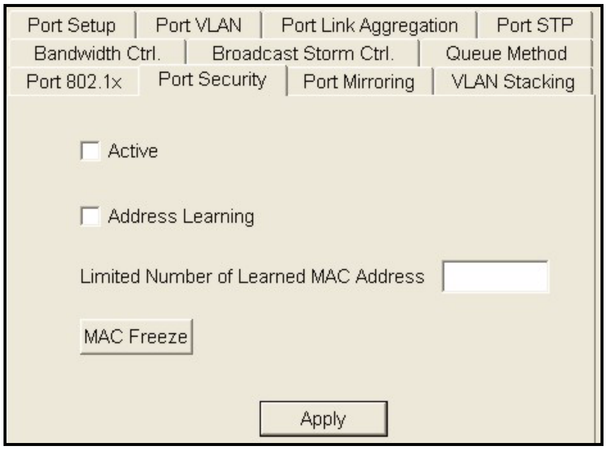
**1** In the Device Panel list, select a device and then right-click.

2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **Port Security** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Port Security** tab.

**Figure 97** Configuration: Ethernet Port Configuration: Port Security



□ Active

□ Address Learning

Limited Number of Learned MAC Address

The following table describes the fields in this screen.

**Table 56** Configuration: 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 Address Learning check box. |
| Limit 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 Switch Setup 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 **MAC Freeze** button to convert all current dynamic MAC addresses to static MAC addresses. When the **MAC Freeze** button is selected, the MAC **Address Learning** checkbox is cleared but port security becomes **Active**. |
| Apply | Click **Apply** to save the changes back to the switch. |

## 13.10 Port Mirroring

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.

### 13.10.1 Configuring Port Mirroring

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.

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

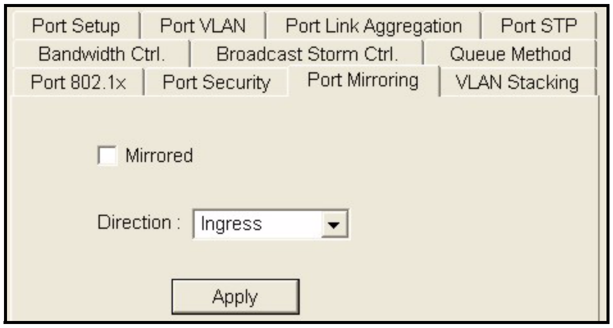
1 In the Device Panel list, select a device and then right-click.

2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **Mirroring** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **Port Mirroring** tab.

**Figure 98** Configuration: Ethernet Port Configuration: Port Mirroring



□ Mirrored

Direction : Ingress

The following table describes the fields in this screen.

**Table 57** Configuration: 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 Egress (outgoing), Ingress (incoming) or Both from the drop-down list box. |
| Apply | Click **Apply** to save the changes back to the switch. |

## 13.11 VLAN Stacking

### 13.11.1 Introduction to VLAN Stacking

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.

## 13.11.2 Configuring VLAN Stacking

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

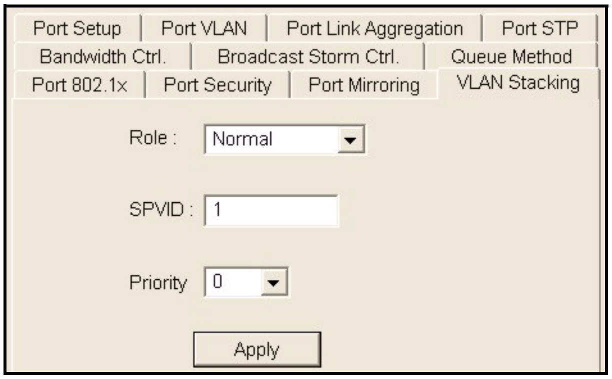
1 In the Device Panel list, select a device and then right-click.

2 Click **Configuration**, **Switch Configuration** and then the **Switch Setup** tab.

3 Select the **VLAN Stacking** check box and then click **Apply**.

4 Click **Configuration, Ethernet Port Configuration** and then the **VLAN Stacking** tab.

**Figure 99** Configuration: Ethernet Port Configuration: VLAN Stacking



Role : Normal

SPVID : 1

Priority 0

The following table describes the fields in this screen.

**Table 58** Configuration: Ethernet Port Configuration: VLAN Stacking

| TABLE | DESCRIPTION |
|---|---|
| Role | Select **Normal** to have the switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in SPVID and Priority are ignored.<br>Select **Access Port** to have the switch add the SP TPID tag to all incoming frames received on this port.<br>Select **Access Port** for ingress ports at the edge of the service provider's network.<br>Select **Tunnel Port** (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 | **SPVID** 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. |

**Table 58** Configuration: Ethernet Port Configuration: VLAN Stacking (continued)

| TABLE | DESCRIPTION |
|---|---|
| Priority | On the switch, configure priority level of inner IEEE 802.1Q tag in the Port Setup screen. "0" is the lowest priority level and "7" is the highest. |
| Apply | Click **Apply** to save the changes back to the switch. |

# CHAPTER 14 Routing Configuration

This chapter shows you how to configure the routing functions.

## 14.1 Static Route

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

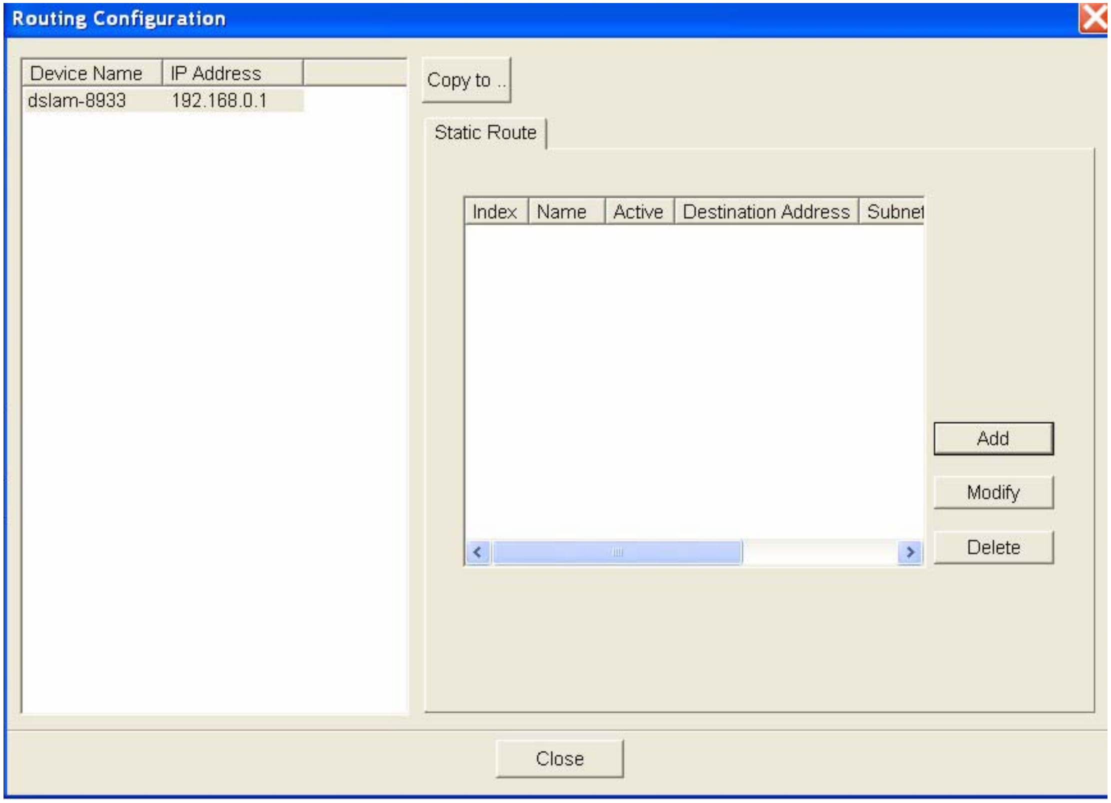
### 14.1.1 Configuring Static Routing

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** and then the tab.

**Figure 100** Configuration: Routing Configuration



Routing Configuration

| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

Static Route

| Index | Name | Active | Destination Address | Subnet |
|---|---|---|---|---|

The following table describes the labels in the summary table.

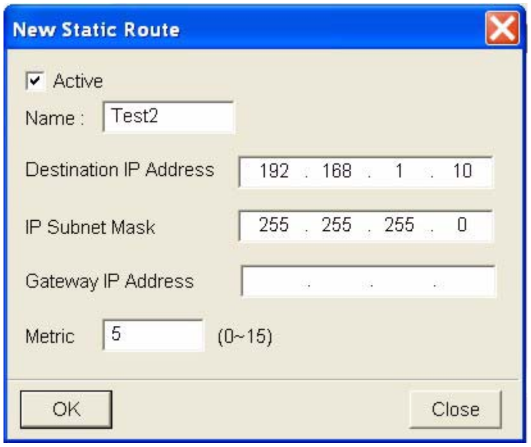
**Table 59** Configuration: Routing Configuration

| 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 purpose only. |
| Active | This field displays **Yes** when the static route is activated and **No** 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 **Add** button to create a new static route. |
| Modify | Select the rule(s) that you want to change and click the **Modify** button. |
| Delete | Check the rule(s) that you want to remove in the **Delete** column, and then click the **Delete** button. |

## 14.1.2 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 101** Configuration: Routing Configuration: Add or Modify



New Static Route

☑ Active

Name : Test2

Destination IP Address 192 . 168 . 1 . 10

IP Subnet Mask 255 . 255 . 255 . 0

Gateway IP Address . . .

Metric 5 (0~15)

The following table describes the labels in this screen.

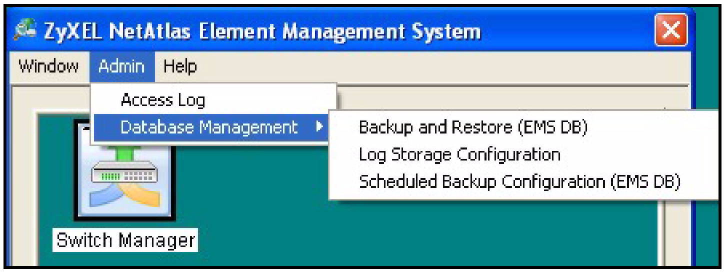
**Table 60** Configuration: Routing Configuration: Add or Modify

| 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 purpose only. |
| 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 **OK** to save the new rule to the switch. It then displays in the **Routing Configuration** screen. |
| Cancel | Click **Cancel** to close the screen. |

## 14.2 Switch Manager

In the **SNMPc Management Console** screen, double-click the switch icon to view the **Switch Manager**.

**Figure 102** Switch Manager Menus


ZyXEL NetAtlas Element Management System
Window
Admin
Help
Access Log
Database Management
Backup and Restore (EMS DB)
Log Storage Configuration
Scheduled Backup Configuration (EMS DB)
Switch Manager

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

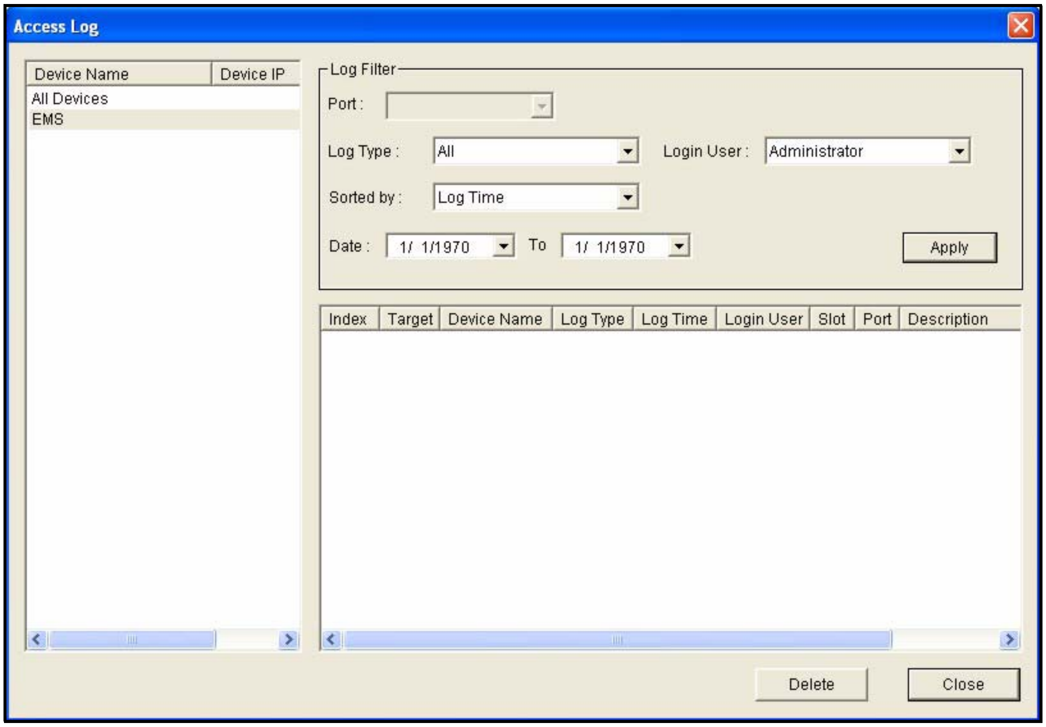
**Table 61** Switch Manager Menus Overview

| LABEL | MENU | SUB-MENU | DESCRIPTION |
|---|---|---|---|
| Window | Exit | | Select **Exit** to close the switch manager screen. |
| Admin | Access | | Use this screen to display filtered logs generated by a switch(es). |
| | Database Management | Backup and Restore (EMS DB) | Use this screen to backup or restore a switches configuration. |
| | | Log Storage Configuration | Use this screen to |
| | | Scheduled Backup Configuration (EMS DB) | |
| Help | On-line Help | | Select **On-line Help** to display an EMS help file. |

## 14.2.1 Access Log

Click **Admin** and then **Access Log** in the switch manager to display the following screen.

**Figure 103** Switch Manager: Admin: Access Log



The following table describes the fields in this screen.

**Table 62** Switch Manager: Admin: Access Log

| LABEL | DESCRIPTION |
|---|---|
| Log Filter | |
| Port | Select a port or **All Ports** 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 **All Users** to view logs for all access attempts to a switch via the EMS. Select **Administrator** to view only the EMS administrator access attempts. |
| Sorted by | Select **By Device Name** to sort the logs displayed in alphabetical order according to the names of the switch(es). Select **Log Time** 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 | Select **Apply** to save the above settings. |
| 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 EMS user that logged into the switch |
| Slot | This field is currently not supported. |

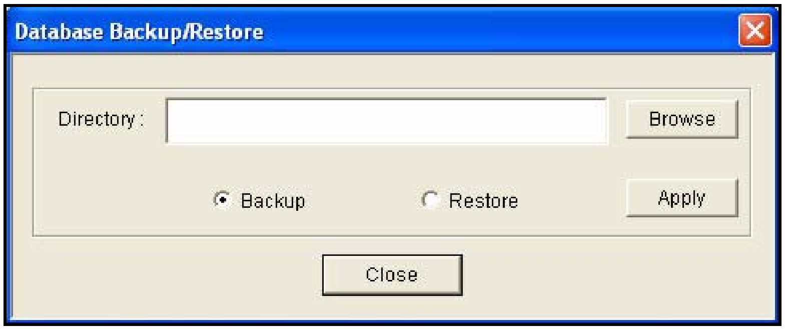
**Table 62** Switch Manager: Admin: Access Log

| LABEL | DESCRIPTION |
|---|---|
| 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 **Delete** to delete a select log from the list of log entries. |
| Close | Click **Close** to close this screen. |

## 14.2.2 Database Backup and Restore

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

**Figure 104** Switch Manager: Database Management: Backup/Restore



The following table describes the fields in this screen.

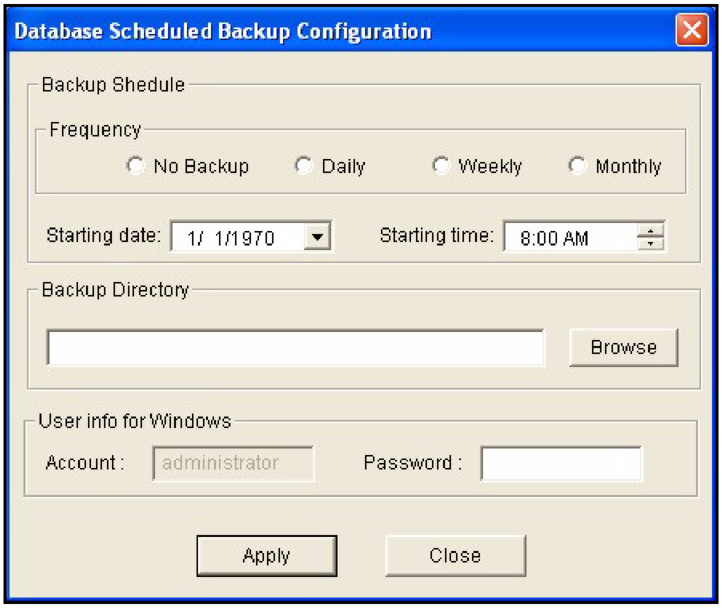
**Table 63** Switch Manager: Database Management: Backup/Restore

| LABEL | DESCRIPTION |
|---|---|
| Directory | Type the path and file name of the database (usually stored in MySQL) you wish to restore to the EMS or backup to your computer in the **Directory** text box or click **Browse** to locate it. |
| Backup | Click the **Backup** radio button to transfer the database file from the EMS to a computer. |
| Restore | Click the **Restore** radio button to transfer the database file from your computer to the EMS. |
| Apply | Click **Apply** to backup or restore the database file. |
| Close | Click **Close** to close the screen. |

## 14.2.3 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 105** Switch Manager: Database Management: Scheduled Backup



Starting date: 1/ 1/1970

Starting time: 8:00 AM

Account : administrator

The following table describes the fields in this screen.

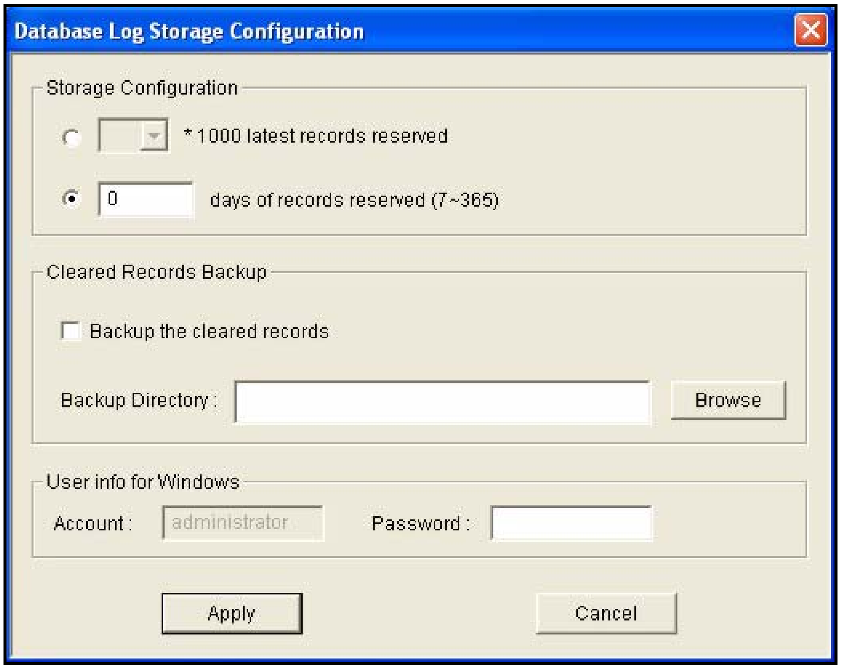
**Table 64** Switch Manager: Database Management: Scheduled Backup

| LABEL | DESCRIPTION |
|---|---|
| Backup Schedule | |
| Frequency | Scheduled backups can be performed on **Daily**, **Weekly** or **Monthly**. Select a radio button to schedule firmware backups starting from the date and time specifed below. The default setting is **No Backup**. |
| Starting date | Specify the starting date to begin firmware backup for the selected device(s). Select a date from the drop-down list box. |
| Starting time | Specify the starting time to begin firmware 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 firmware file you wish to backup to your computer in the **Backup Directory** text box or click **Browse** 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 **Account** above. |
| Apply | Click **Apply** to save changes to the EMS. |
| Close | Click **Close** to close the screen. |

## 14.2.4 Database Log Storage Configuration

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

**Figure 106** Switch Manager: Database Management: Log Storage



Database Log Storage Configuration

Storage Configuration

○ [ ] * 1000 latest records reserved

● 0 days of records reserved (7~365)

Cleared Records Backup

□ Backup the cleared records

Backup Directory :

User info for Windows

Account : administrator

Password :

The following table describes the fields in this screen.

**Table 65** Switch Manager: Database Management: Log Storage

| LABEL | DESCRIPTION |
|---|---|
| Storage Configuration | Configure the following fields to retain daily records.<br>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.<br>Or<br>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 checkbox and type the path and file name or click **Browse** 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 backup to your computer in the **Backup Directory** text box or click **Browse** 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 **Account** above. |
| Apply | Click **Apply** to save changes to the EMS. |
| Cancel | Click **Close** to close the screen. |

# CHAPTER 15
# Performance

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

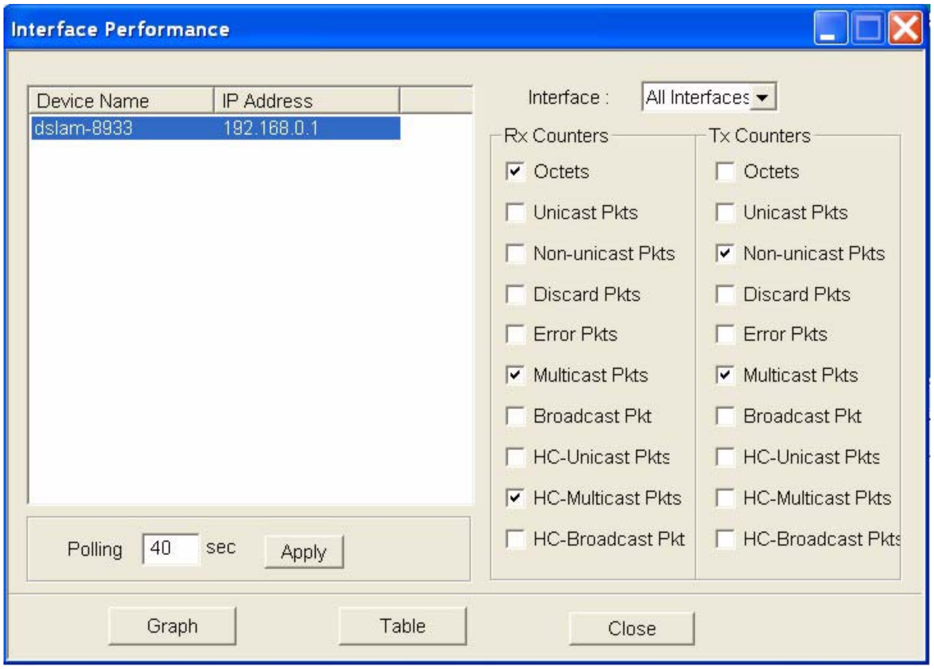
## 15.1 Interface

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

### 15.1.1 View Interface Performance

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

**Figure 107** Performance: Interface



| Device Name | IP Address |
|---|---|
| dslam-8933 | 192.168.0.1 |

Interface : All Interfaces

| Rx Counters | Tx Counters |
|---|---|
| ☑ Octets | □ Octets |
| □ Unicast Pkts | □ Unicast Pkts |
| □ Non-unicast Pkts | ☑ Non-unicast Pkts |
| □ Discard Pkts | □ Discard Pkts |
| □ Error Pkts | □ Error Pkts |
| ☑ Multicast Pkts | ☑ Multicast Pkts |
| □ Broadcast Pkt | □ Broadcast Pkt |
| □ HC-Unicast Pkts | □ HC-Unicast Pkts |
| ☑ HC-Multicast Pkts | □ HC-Multicast Pkts |
| □ HC-Broadcast Pkt | □ HC-Broadcast Pkts |

Polling 40 sec

The following table describes the labels in this screen.

**Table 66** 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. |
| 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 none-integer number of octets (alignment error). |

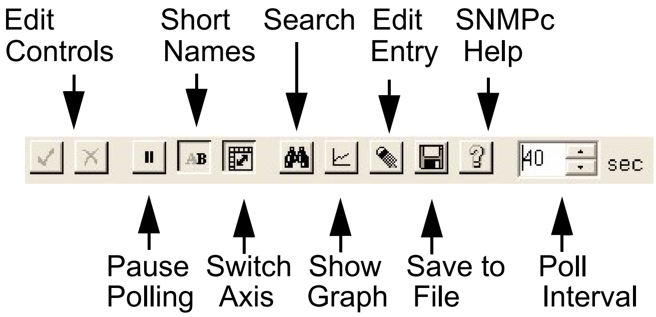
**Table 66** Performance: Interface (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 none-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 none-integer number of octets (alignment error). |
| Graph | Select the **Graph** button to create a graph based on the above selections. |
| Table | Select the **Table** button to create a table based on the above selections. |
| Close | Click **Close** to close the screen. |

## 15.2 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 108** Table Menu Bar Icons

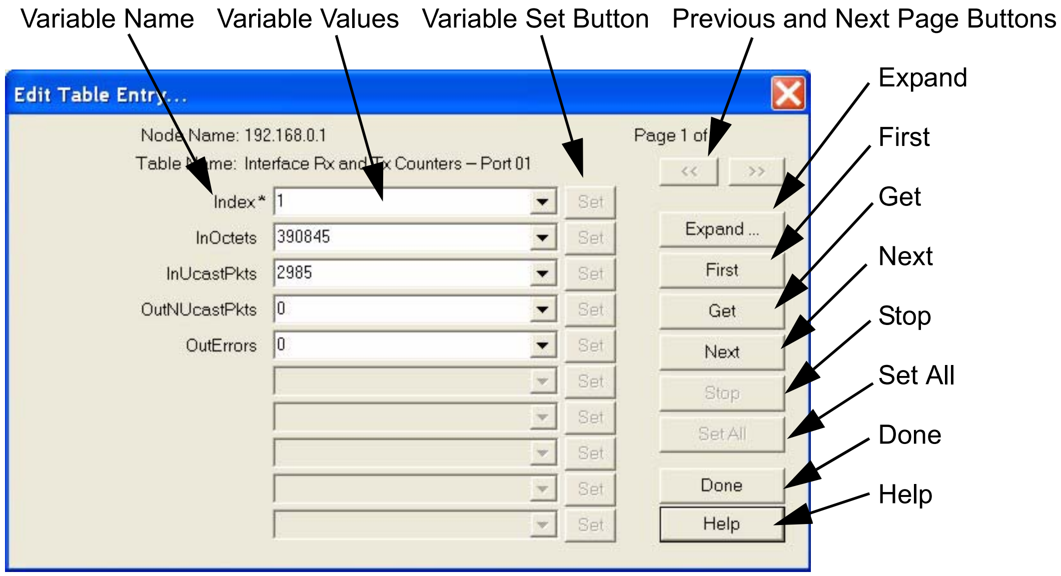


### 15.2.1 Editing a Table Entry

**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 109** Edit Table Entry



Node Name: 192.168.0.1

Table Name: Interface Rx and Tx Counters – Port 01

Page 1 of

Index* 1

InOctets 390845

InUcastPkts 2985

OutNUcastPkts 0

OutErrors 0

The following table describes the labels in this screen.

**Table 67** 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 **Set** button to perform an SNMP set on only one variable. Set buttons are grayed for variables that are read-only. |
| 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 **Expand** button to expand the view of the active variable value edit box. First click on the edit box, then select the **Expand** button. |
| First | Click the **First** 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 **Get** 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 **Get** button to refresh the variable values. |

**Table 67** Edit Table Entry (continued)

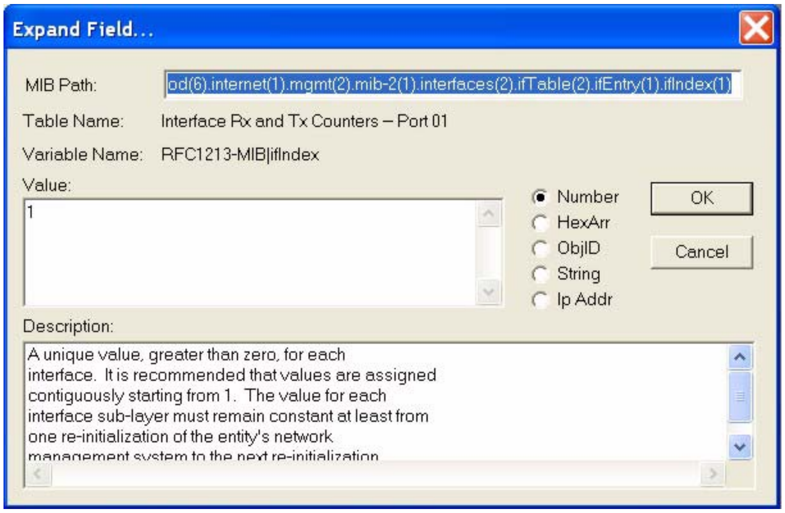
| COMMAND | DESCRIPTION |
|---|---|
| Next | Click the **Next** button to obtain the next entry of the table from the node, using an SNMP GetNext operation. The variable values are updated. If there are no more entries in the table, a message is displayed. You can specify a starting point for the GetNext 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 **Stop** 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 **Set** All 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.

## 15.2.2 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 110** Expand Field



MIB Path: od(6).internet(1).mgmt(2).mib-2(1).interfaces(2).ifTable(2).ifEntry(1).ifIndex(1)

Table Name: Interface Rx and Tx Counters – Port 01

Variable Name: RFC1213-MIB|ifIndex

Value:

1

● Number
○ HexArr
○ ObjID
○ String
○ Ip Addr

Description:

A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization

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.

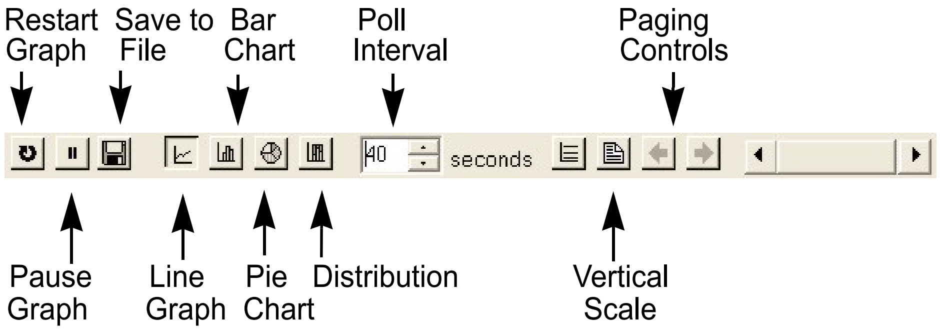
**Table 68** Variable Types

| 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. |

## 15.3 Graph Menu Bar Icons

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

**Figure 111** Graph Menu Bar



## 15.3.1 Graph Styles

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

**Table 69** 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. |

## 15.3.2 Chart Format Display Variable

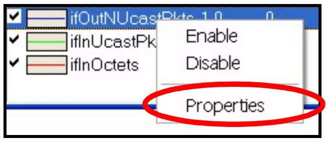
Choose which variables to display in chart format by doing one of the following:

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).

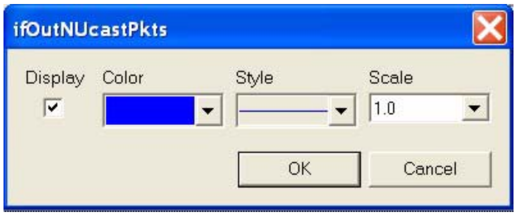
3 Right-click a variable's cell and select **Properties**.

**Figure 112** Cell Properties Select



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

**Figure 113** Chart Color Codes and Line Styles



ifOutNUcastPkts

| Display | Color | Style | Scale |
|---|---|---|---|
| ☑ | | | 1.0 |

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

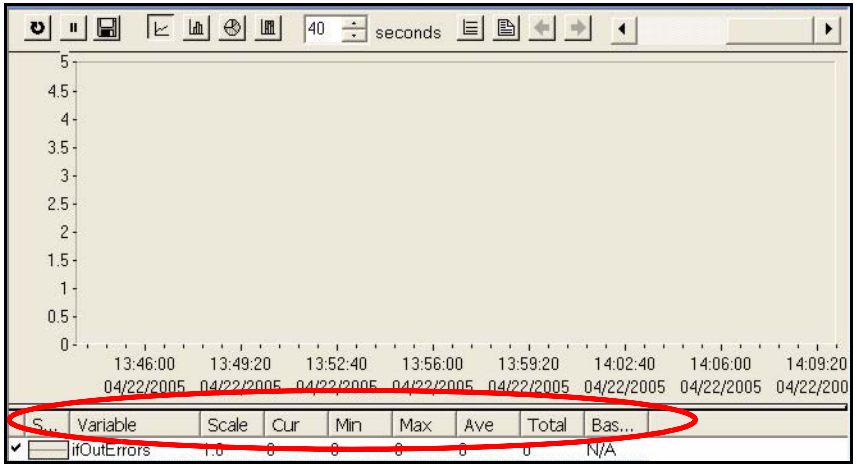
**Table 70** Edit Style Dialog Box

| 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. |

## 15.3.3 Graph Labels

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

**Figure 114** Graph Variables



| S... | Variable | Scale | Cur | Min | Max | Ave | Total | Bas... |
|---|---|---|---|---|---|---|---|---|
| ✓ | ifOutErrors | 1.0 | 0 | 0 | 0 | 0 | 0 | N/A |

The following table describes the labels in this screen.

**Table 71** 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. |

**Table 71** Graph Variables (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 16 Troubleshooting

This chapter covers potential problems and the corresponding remedies.

## 16.1 General Installation Problems

**Table 72** General Installation Problems

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| SNMPc, MySQL will not install properly | Make sure that the computer you want to install the SNMPc and MySQL has the correct hardware and Operating System (OS) specifications. See Section 1.2 on page 22 for a list of installation requirements.<br>Shutdown any services that are running which may affect the installation; for example, shutdown MySQL and SNMPc.<br>Remove any previous versions of MySQL and SNMP software from your computer.<br>Re-install MySQL and SNMPc in that order. |

## 16.2 EMS Installation Problems

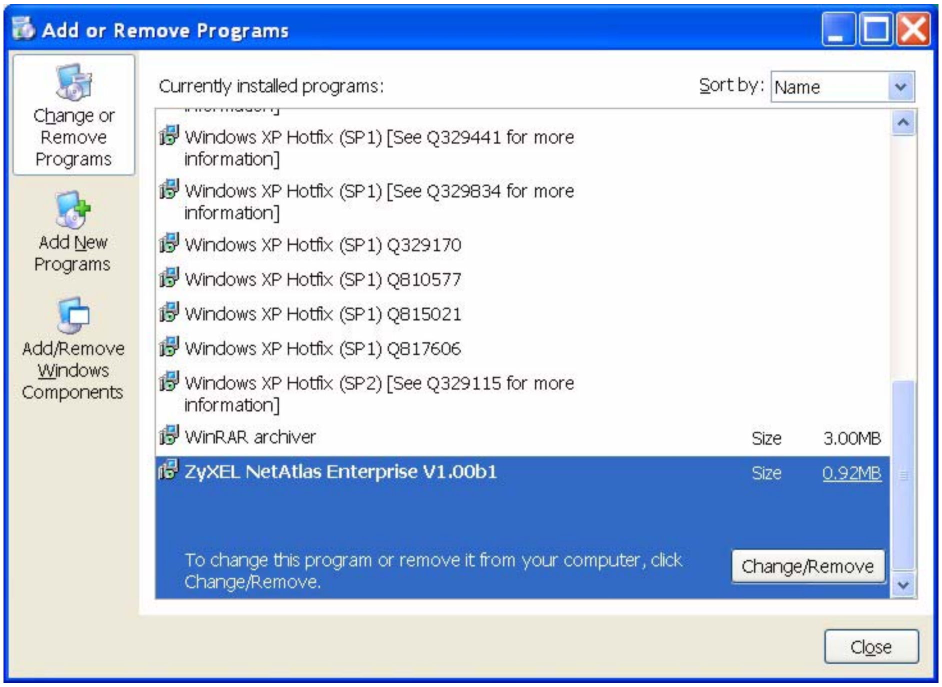
**Table 73** EMS Installation Problems

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| EMS will not install properly | Make sure that the computer you want to install the EMS has the correct hardware and Operating System (OS) specifications. See Section 1.2 on page 22 for a list of installation requirements.<br>Shutdown any services that are running which may affect the installation; for example, shutdown MySQL and SNMPc.<br>Remove any previous versions of the EMS software from your computer. See the Uninstalling the EMS section for information on how to do this.<br>If the problem still persists, try re-installing the EMS. |

## 16.3 Uninstalling the EMS

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

**Figure 115** EMS: Remove


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by:
Name
Windows XP Hotfix (SP1) [See Q329441 for more information]
Windows XP Hotfix (SP1) [See Q329834 for more information]
Windows XP Hotfix (SP1) Q329170
Windows XP Hotfix (SP1) Q810577
Windows XP Hotfix (SP1) Q815021
Windows XP Hotfix (SP1) Q817606
Windows XP Hotfix (SP2) [See Q329115 for more information]
WinRAR archiver
Size 3.00MB
ZyXEL NetAtlas Enterprise V1.00b1
Size 0.92MB
To change this program or remove it from your computer, click Change/Remove.
Change/Remove
Close

2 Select **ZyXEL NetAtlas Enterprise V1.00** 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.

## 16.4 Problems Finding a Device

**Table 74** Problems Accessing the EMS

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| In the SNMPc Management Console I cannot find my device | Check that you have compiled and added the MIB's correctly. See Section 1.5 on page 32 for information on adding MIB's. Make sure these instructions are followed exactly. The correct MIB's must be compiled in the correct order.<br>Check that you have enable auto-discovery; see Section 1.6 on page 34.<br>Check that the map object properties are correct for initial installation; see Section 1.7 on page 36. Make sure the IP address entered is the IP address of the switch you want to manage via the EMS.<br>Make sure that you restarted your computer after you installed MySQL.<br>Check that the MySQL driver is correctly configured; see Section 1.8 on page 39.<br>Make sure that MySQL is running.<br>Make sure that the computer you have installed the EMS on, is connected to the network where the switch is located.<br>Make sure your computer's Ethernet Card is working properly.<br>If the problem still persists, uninstall and re-install the EMS software. |

## 16.5 Problems Accessing the EMS

**Table 75** Problems Accessing the EMS

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| When I click the Switch Manager icon, I cannot access the EMS | Shutdown and restart both MySQL and the SNMPc manager.<br>The EMS may already be running. Check your Windows task bar. |

# 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 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.

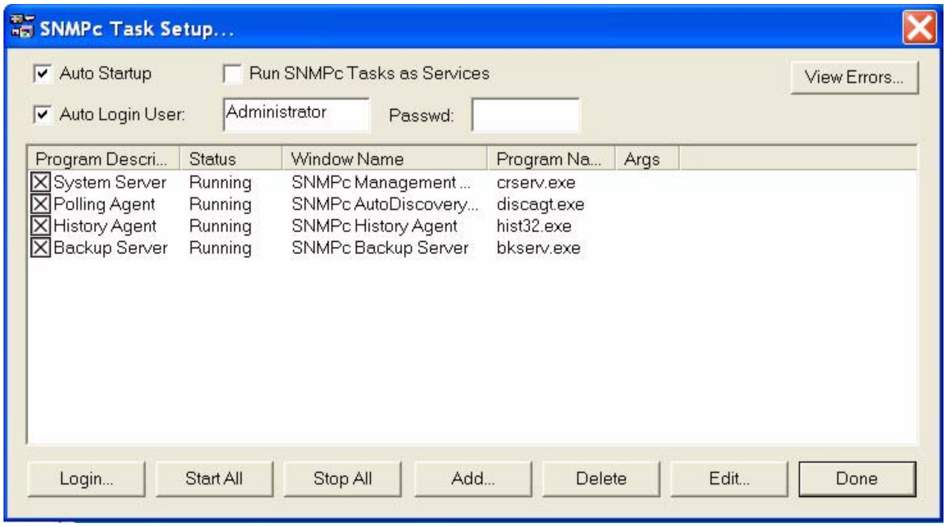
### Automatic Startup

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 116** Automatic Startup



☑ Auto Startup ☐ Run SNMPc Tasks as Services

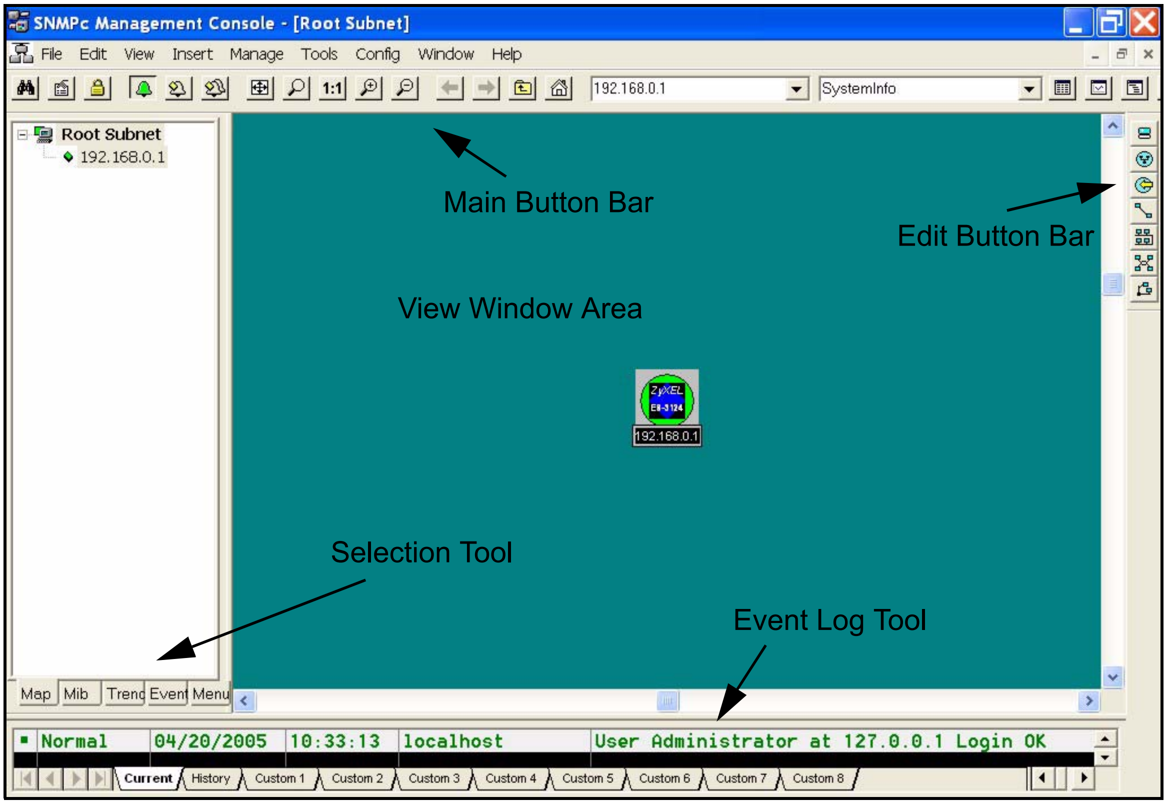
☑ Auto Login User: Administrator Passwd:

| Program Descri... | Status | Window Name | Program Na... | Args |
|---|---|---|---|---|
| ☒ System Server | Running | SNMPc Management ... | crserv.exe | |
| ☒ Polling Agent | Running | SNMPc AutoDiscovery... | discagt.exe | |
| ☒ History Agent | Running | SNMPc History Agent | hist32.exe | |
| ☒ Backup Server | Running | SNMPc Backup Server | bkserv.exe | |

## SNMPc Main Window

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

**Figure 117** SNMPc Main Windows



SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
192.168.0.1
SystemInfo
Root Subnet
192.168.0.1
Main Button Bar
Edit Button Bar
View Window Area
ZyXEL
ES-3124
192.168.0.1
Selection Tool
Event Log Tool
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8

```
Normal   04/20/2005   10:33:13   localhost   User Administrator at 127.0.0.1 Login OK
```

**Table 76** SNMPc Main Window

| ELEMENT | FUNCTION |
|---|---|
| Main Button Bar | Buttons and controls to execute common commands quickly. Hold the cursor over an icon to see a tool tip. |
| Edit Button Bar | Buttons to quickly insert map elements. Hold the cursor over an icon to see a tool tip. |
| Selection Tool | Tabbed control for selection of objects within different SNMPc functional modules. |
| Event Log Tool | Tabbed control for display of filtered event log entries. |
| 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 77** 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 press 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 118** SNMPc Main Button Bar Icons

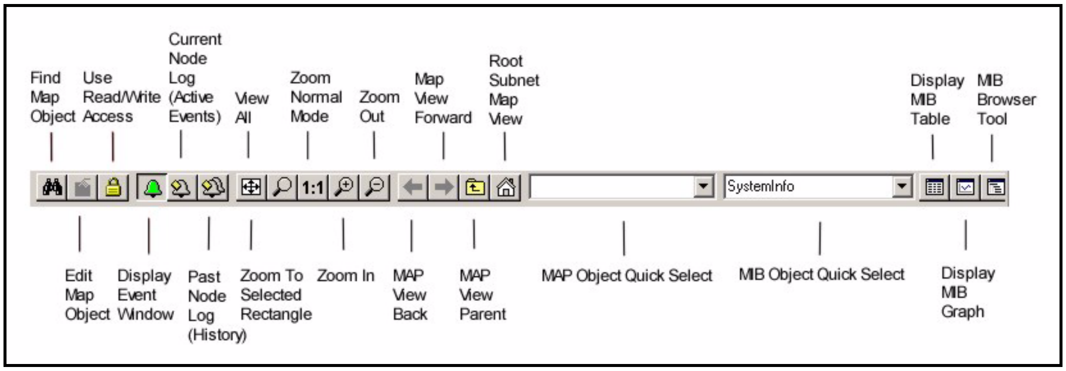
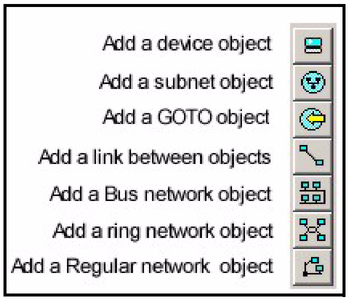


**Figure 119** SNMPc Edit Button Bar Icons


Add a device object
Add a subnet object
Add a GOTO object
Add a link between objects
Add a Bus network object
Add a ring network object
Add a Regular network object

**Note:** For more detailed information, please see www.castlerock.com.

# Appendix B
# Alarm Types and Causes

This appendix shows examples of probable alarm types and causes.

## Alarm Types and Causes Table

**Table 78** Alarm Types and Causes

| ALARM TYPE | PROBABLE CAUSES | |
|---|---|---|
| Communications | • Loss of signal<br>• Loss of frame<br>• Framing error<br>• Local node transmission error<br>• Remote node transmission error<br>• Call establishment error | • Degraded signal<br>• Communications subsystem failure<br>• Communications protocol error<br>• LAN error<br>• DTE-DCE interface error |
| Quality of service | • Response time excessive<br>• Queue size exceeded<br>• Bandwidth reduced<br>• Retransmission rate excessive | • Threshold crossed<br>• Performance degraded<br>• Congestion<br>• Resource at or nearing capacity |
| Processing error | • Storage capacity problem<br>• Version mismatch<br>• Corrupt data<br>• CPU cycles limit exceeded<br>• Software error<br>• Software program error | • Software program abnormally terminated<br>• File error<br>• Out of memory<br>• Underlying resource unavailable<br>• Application subsystem failure<br>• Configuration or customization error |
| Equipment | • Power problem<br>• Timing problem<br>• Processor problem<br>• Dataset or modem error<br>• Multiplexer problem<br>• Receiver failure<br>• Transmitter failure | • Receive failure<br>• Transmit failure<br>• Output device error<br>• Input device error<br>• I/O device error<br>• Equipment malfunction<br>• Adapter error |
| Environmental | • Temperature unacceptable<br>• Humidity unacceptable<br>• Heating/ventilation/cooling system problem<br>• Fire detected<br>• Flood detected<br>• Toxic leak detected | • Leak detected<br>• Pressure unacceptable<br>• Excessive vibration<br>• Material supply exhausted<br>• Pump failure<br>• Enclosure door open |

# Index