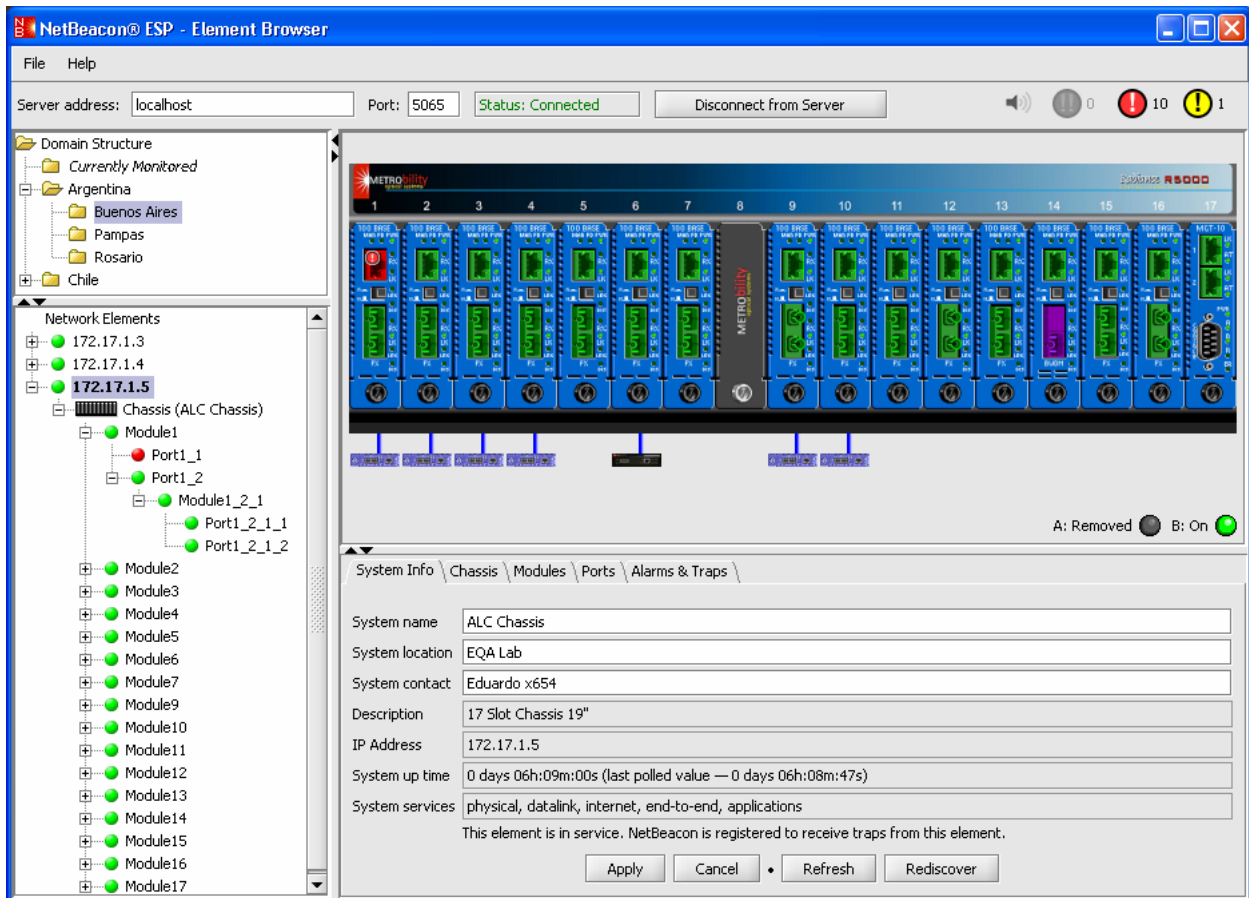


# NetBeacon<sup>®</sup> Ethernet Services Provisioning Software Installation and User's Guide



Version 1.0

© 2006 Metrobility Optical Systems, Inc. All Rights Reserved. Printed in USA.

This publication is protected by the copyright laws of the United States and other countries, with all rights reserved. No part of this publication may be reproduced, stored in a retrieval system, translated, transcribed, or transmitted, in any form, or by any means, manual, electric, electronic, electromagnetic, mechanical, chemical, optical or otherwise, without prior explicit written permission of Metrobility Optical Systems, Inc.

The information contained in this publication is accurate as of its publication date; such information is subject to change without notice. Metrobility Optical Systems, Inc. is not responsible for any inadvertent errors.

### Third-Party Copyright and Trademark Notification

Parts of NetBeacon include industry standard components, packages, or products, and are copyrighted by their respective owners. Individual files in these components, packages, or products may contain additional copyright or trademark notices, and certain relevant portions are provided herein.

#### JAAS Modules Version 1.0.3

Copyright © 2001-2003: Andy Armstrong, [andy@tagish.com](mailto:andy@tagish.com)

**Description:** A number of JAAS modules that allow authentication against JDBC connected databases, text files and perhaps most usefully, Windows NT Domains.

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

<http://www.gnu.org/copyleft/lesser.html>

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place – Suite 330, Boston, MA 02111-1307, USA.

**Source:** <http://free.tagish.net/jaas/>

Metrobility Optical Systems, Metrobility, Lancast, AutoTwister, MicroChassis, NetBeacon, and "twister" are registered trademarks; the Metrobility Optical Systems logo, the Lancast logo, WebBeacon and "redundant twister" are trademarks of Metrobility Optical Systems, Inc. Java, Sun, Sun Microsystems, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.

Radiance and "redundant twister" technologies are patents of Metrobility Optical Systems, Inc. (U.S. Patent Nos. 6,741,566 and 6,058,479)

# Contents

---

<b>CONTENTS</b>	<b>III</b>
ABOUT THIS GUIDE .....	VII
DOCUMENT CONVENTIONS .....	VII
RELATED DOCUMENTS .....	VII
USING THE MOUSE .....	IX
TECHNICAL SUPPORT .....	IX
<b>CHAPTER 1. GETTING STARTED</b>	<b>1</b>
WHAT IS NETBEACON? .....	1
What is an Element? .....	1
How Does NetBeacon Communicate with Network Elements? .....	2
FEATURES AND BENEFITS .....	4
SYSTEM REQUIREMENTS .....	4
NETBEACON CD CONTENTS .....	5
INSTALLING THE NETBEACON SOFTWARE .....	5
UNINSTALLING THE NETBEACON SOFTWARE .....	9
WHAT'S NEXT? .....	10
<b>CHAPTER 2. NETBEACON BASICS</b>	<b>13</b>
STARTING NETBEACON .....	13
Viewing the NetBeacon Element Manager and Database Properties .....	13
Opening the Element Manager Configuration Window .....	14
Opening the Database Configuration Window .....	15
Opening the NetBeacon Element Browser Window .....	16
EXITING NETBEACON .....	17
Closing the NetBeacon Element Browser Window .....	17
Closing the NetBeacon Element Manager Admin Tool or the Database Admin Tool Windows .....	18
Stopping the NetBeacon Element Manager Service or the NetBeacon Database Service .....	18
CHECKING NETBEACON VERSION NUMBERS .....	19
Element Browser Version Number .....	19
Database Service and Database Service Admin Tool Version Numbers .....	19
Element Manager Service and Element Manager Admin Tool Version Numbers .....	20
<b>CHAPTER 3. ELEMENT MANAGER AND DATABASE CONFIGURATION</b>	<b>21</b>
LEARNING ABOUT THE NETBEACON CONFIGURATION WINDOW .....	22
ADDING AND REMOVING ELEMENTS .....	23
Adding a New Element .....	23
Adding Multiple Elements .....	24
Deleting an Element .....	26
Editing Element Settings .....	26
CONFIGURING SNMP SETTINGS .....	28
SNMPv1 or SNMPv2 .....	28
SNMPv3 .....	29
DOWNLOADING SOFTWARE TO AN ELEMENT .....	30
DEFINING THE DOMAIN STRUCTURE ORGANIZATION .....	32
Creating New Network Domains .....	32
Assigning Elements to a Domain .....	33
Deleting a Domain or Element .....	34
Undoing Changes .....	34

Editing the Name .....	35
Creating a Placeholder.....	35
CONFIGURING USER LOG-IN AUTHENTICATION .....	36
No Authentication.....	37
Basic Log-in .....	37
Creating Passwords for Basic Log-in Users .....	37
Adding Basic Log-in Users .....	38
Changing a Basic User's Password .....	39
Deleting a Basic User .....	39
Platform Log-in .....	40
RADIUS Log-in .....	40
CREATING AND AUTHORIZING USER ACCOUNTS.....	41
Creating Groups and Adding Users.....	41
Deleting Users or Groups .....	43
Renaming Users or Groups.....	44
Assigning Permissions.....	44
SPECIFYING NETWORK PARAMETERS.....	47
Sending a Test E-mail Message.....	49
CONFIGURING THE DATABASE .....	50
Creating a Database File.....	53
Viewing Historical Security Information .....	55
Running a Custom Security Query .....	56
Filtering the Database Tables .....	57
SENDING E-MAIL NOTIFICATIONS.....	58
Configuring E-Mail Recipients.....	58
Customizing Alarms for Recipients.....	59
ENTERING THE NETBEACON LICENSE .....	62
Requesting a NetBeacon License Key.....	63
Entering the NetBeacon License .....	63
SEEKING METROBILITY SUPPORT.....	63
<b>CHAPTER 4. LEARNING ABOUT THE NETBEACON ELEMENT BROWSER WINDOW</b> .....	<b>65</b>
RESIZING THE WINDOWS AND DIALOG BOXES.....	65
MENU BAR .....	66
File Menu.....	66
Help Menu .....	66
Shortcut Keys .....	67
SERVER CONNECTION BAR.....	67
ALARM INDICATORS.....	67
DOMAIN STRUCTURE.....	68
NETWORK ELEMENTS.....	69
Expanding and Collapsing the Network Elements List .....	69
CHASSIS VIEW.....	71
Power Supply Status.....	72
Remote Devices.....	72
Chassis in Stack.....	73
Discovery Status Bar .....	73
INFORMATION TABS .....	73
<b>CHAPTER 5. MANAGING THE ELEMENTS</b> .....	<b>75</b>
CONNECTING TO AN ELEMENT .....	75
DISPLAYING SYSTEM INFORMATION .....	76
MONITORING THE CHASSIS .....	77
Resizing Table Columns.....	78
Displaying Chassis Information .....	78

Displaying Temperature and Power Supply Information .....	79
Resetting the Chassis .....	80
<b>CHAPTER 6. CONFIGURING THE MODULES</b> .....	<b>81</b>
DISPLAYING MODULE INFORMATION .....	81
OPENING THE MODULE CONFIGURATION DIALOG BOX .....	83
Opening the Port Configuration Dialog Box .....	84
Module Configuration Dialog Box Button Options.....	84
Changing a Module Name and Asset ID .....	85
Resetting a Module.....	85
APPLYING LINK LOSS CARRY FORWARD .....	85
Applying Copper Loss Carry Forward .....	86
MAKING MODULE CONFIGURATIONS .....	86
Setting the Data Rate for a Multi-Rate Line Card .....	87
Setting the Transparency Mode on the R141, R111-13-B, or R11-15-B Line Card.....	87
MANAGING THE ACCESS LINE CARD.....	88
Applying Write Protection on an Access Line Card.....	88
LLCF Warning .....	89
Displaying Sensor Information for an Access Line Card or Access ONU .....	89
CONFIGURING THE REDUNDANT INTERFACE LINE CARD .....	90
Dynamic Recovery Mode.....	91
Applying SONAR .....	92
Select A/B Mode .....	93
CONFIGURING THE 10/100 MBPS LINE CARD .....	93
Link Loss Carry Forward and Flow Control .....	93
Backpressure (Half-Duplex Flow Control).....	94
Auto-Recovery .....	94
MANAGING THE CHASSIS STACKING LINE CARD .....	95
Port Duplex, Full-Duplex Flow Control, and Half-Duplex Flow Control.....	95
CONFIGURING THE MANAGEMENT MODULE .....	96
Displaying Management Module Information.....	96
Configuring Trap Destinations .....	97
Adding a New Trap Destination.....	98
Reconfiguring a Trap Destination.....	98
Deleting a Trap Destination.....	99
Filtering the Trap Control Options .....	99
Configuring the Access Control List .....	101
Configuring Management Module Network Settings.....	103
Viewing Management Card Sensors.....	103
CONFIGURING THE SERVICES LINE CARD.....	104
Viewing Remote Services Lines.....	104
Changing Network and Management Settings .....	107
Configuring Logical Services Loopback .....	109
Upgrading the Firmware.....	109
Viewing Temperature and Voltage Measurements.....	112
Setting SNMP Trap Destinations.....	113
Configuring the ARP Table.....	114
Assigning User VLANs.....	115
Prioritizing Traffic Classes .....	117
Precedence.....	117
CONFIGURING THE RS960 .....	119
<b>CHAPTER 7. CONFIGURING THE PORTS</b> .....	<b>121</b>
DISPLAYING PORT DETAILS .....	121
OPENING THE PORT CONFIGURATION DIALOG BOX .....	122

Displaying Serial Port Information.....	123
APPLYING LINK LOSS RETURN.....	124
SETTING THE SPEED ON THE R141 LINE CARD.....	125
CONFIGURING THE 10/100MBPS PORTS .....	126
CONFIGURING THE R133 PORTS .....	127
CONFIGURING THE R153 PORTS .....	129
CONFIGURING THE R380 PORTS .....	130
CONFIGURING THE ACCESS LINE CARD PORTS .....	131
Displaying Port Statistics.....	132
Viewing Data Graphs .....	133
Provisioning Bandwidth .....	133
CONFIGURING THE SERVICES LINE CARD PORTS.....	134
Displaying SFP Sensor Readings and Hardware Parameters .....	136
OAM Options (Standalone NIDs Only) .....	137
Defining the Access and Trunk Ports .....	137
Applying a Rate Limit on the R821 .....	137
Setting the Default Port Priority .....	138
Configuring Layer 2 Control Protocols .....	138
OAM Controls and Loopback .....	139
OAM Events.....	141
OAM Statistics .....	143
Copper Line Quality (CLQ) Testing.....	143
MANAGING THE RS960 PORTS .....	143
CONFIGURING THE T1/E1 PORTS.....	144
Selecting the Line Code and Line Buildout.....	145
Setting BERT 511, Remote Loopback, and Far End Fault.....	145
T1/E1 Indicators .....	146
CONFIGURING THE T3/E3 PORTS.....	146
Setting the T3 Line Buildout .....	147
<b>CHAPTER 8. MONITORING TRAPS AND ALARMS</b> .....	<b>149</b>
VIEWING ALARMS AND TRAPS .....	149
Understanding the Trap Legend .....	150
Acknowledging Alarms and Traps .....	151
Removing Alarm and Trap Messages.....	151
FILTERING TRAPS AND ALARMS.....	152
VIEWING HISTORICAL DATA .....	153
Running a Standard Query.....	153
Sorting the Alarms Database .....	153
Specifying Time Periods .....	153
Filtering Alarm Database Fields.....	154
Running a Custom Query .....	155
<b>APPENDIX A. DOWNLOAD ERROR MESSAGES</b> .....	<b>157</b>
<b>APPENDIX B. FREQUENTLY ASKED QUESTIONS</b> .....	<b>159</b>
<b>APPENDIX C. ABBREVIATIONS AND ACRONYMS</b> .....	<b>161</b>
<b>APPENDIX D. NETBEACON WARRANTY STATEMENT</b> .....	<b>163</b>
<b>APPENDIX E. STANDARDS COMPLIANCE</b> .....	<b>165</b>

## About this Guide

The *NetBeacon® Ethernet Services Provisioning Software Installation and User's Guide* provides network managers and system administrators with information about how to configure and manage any Metrobility® chassis-based system and related cards by using the NetBeacon software.

The reader of this document should be knowledgeable about network devices, device configuration, network management, and Windows environments. The user is assumed to be a network administrator with an understanding of network operations.

## Document Conventions

The following conventions are used in this guide.

<b>Bold</b>	Indicates a menu option that you choose, a command that you type, or a command button that you click.
<i>Italics</i>	Indicates a variable for which you provide a value or the title of a document.
Courier	Indicates a message, directory, or filename.
<u>Underline</u>	Indicates a hyperlink. Hyperlinks provide cross-references to other information that is helpful when performing a task.
SMALL CAPS	Indicates a key on the keyboard that you press. For example: Press the SHIFT key.
<b>Tip</b>	Information that is helpful when performing some activity.
<b>Important</b>	Information that is critical to your understanding of how the product works.

## Related Documents

The following documents are additional resources that provide useful information regarding the Radiance or Lancast® devices and cards, including installation and configuration guidelines. All Metrobility manuals can be found on our website, [www.metrobility.com](http://www.metrobility.com).

*Intelligent 7500 Chassis ~ Installation and User Guide*  
*Radiance R5000 Central Service Platform ~ Installation and User Guide*  
*Radiance R1000 Premise Service Platform ~ Installation and User Guide*  
*Radiance R400 Premise Service Platform ~ Installation and User Guide*  
*Radiance DIN Rail Mounted Chassis ~ Installation and User Guide*

Provides detailed chassis and power supply installation instructions and specifications.

*Radiance 10Mbps Single Interface Line Cards ~ Installation and User Guide*  
*Radiance 100Mbps Single Interface Line Cards ~ Installation and User Guide*  
*Radiance 10 and 100 Mbps Single Interface Line Cards ~ Installation and User Guide*

Contains installation instructions, specifications, and switch settings for the 10 and 100Mbps cards, including the feature-rich R133 line cards.

*Radiance 100Mbps Redundant Interface Line Cards ~ Installation & User Guide*  
*Radiance 1000Mbps Redundant Interface Line Cards ~ Installation & User Guide*

Provides details on how to install, configure, and operate the 10Mbps, 100Mbps, or 1000Mbps line protection and restoration (LPR) interface line cards.

*Radiance 10/100Mbps Interface Line Cards ~ Installation & User Guide*

Contains information on the installation, configuration, network specifications, and operation of the 10/100Mbps cards.

*Radiance Gigabit Single Interface Line Cards ~ Installation & User Guide*  
*Radiance SONET Single Interface Line Cards ~ Installation & User Guide*  
*Radiance 1Gbps Interface Line Cards with SFP Optics ~ Installation & User Guide*

Provides installation and operational guidelines for the 1000Mbps, OC-3/STM-1 and OC-12/STM-4 cards.

*Radiance Access Line Cards ~ Installation & User Guide*

Provides details on how to install, configure, and operate the 100Mbps access line cards. Also includes technical specifications.

*Radiance 10/100Mbps Access Optical Network Unit ~ Installation & User Guide*

Provides details on how to install, configure, operate and monitor the 10/100Mbps access optical network unit. Also includes troubleshooting information and technical specifications.

*Radiance T1/E1 Single Interface Line Cards ~ Installation & User Guide*  
*Radiance T3/E3 Single Interface Line Cards ~ Installation & User Guide*

Contains information on the installation, configuration, technical specifications, and operation of the TDM line cards.

*Multi-Rate Line Card ~ Installation & User Guide*

Provides details on how to install, configure, and operate the multi-rate line card.

*Radiance Chassis Stacking Line Card ~ Installation & User Guide*

Provides information on the installation, operation and management of the 10/100Mbps TX four-port chassis stacking line card. Also includes an example of how to configure a stack of four chassis using the card.

*Command Line Interface ~ Reference Guide*

Contains a complete list of the console commands to configure and manage any Metrobility device, as well as instructions on how to set up the management card.



Contains installation instructions, a description of the device's features and management system, and a list of console commands to configure and manage the services line card.

## **Using the Mouse**

Always use the left mouse button when instructed to "click" a command button or choose a menu option, unless you are instructed to "right-click." If you have reversed the functions of the left and right buttons, use the alternate button when following these procedures. See your platform documentation for further instructions on using your mouse.

## **Technical Support**

Before contacting Technical Support, please make sure you have the following information:

- NetBeacon software version number
- Java Runtime Environment (JRE) version number
- Version of software on the management card
- Version of software on any services line card(s)
- Management station hardware specifications (RAM, operating system, and CPU)

Refer to [Checking NetBeacon Version Number](#).

Notify Metrobility Technical Support via e-mail by contacting **techsupport@metrobility.com** or by calling 1.877.526.2278, from 8 AM to 7 PM (EST). You can also fax Metrobility Optical Systems, Inc. at 1.603.594.2887.



# Chapter 1. Getting Started

---

## What is NetBeacon?

The NetBeacon Ethernet Services Provisioning software is a real-time network element management application that helps network administrators configure and monitor any manageable Metrobility device or chassis-based system, perform diagnostics, provision services, and access its database. NetBeacon ensures network security with user authentication and authorization along with data encryption. NetBeacon runs under Microsoft® Windows® XP and consists of three key components:

- Element Manager
- Element Browser
- Database

All three components may be installed together on a single standalone server, or each component may be installed separately on individual systems.

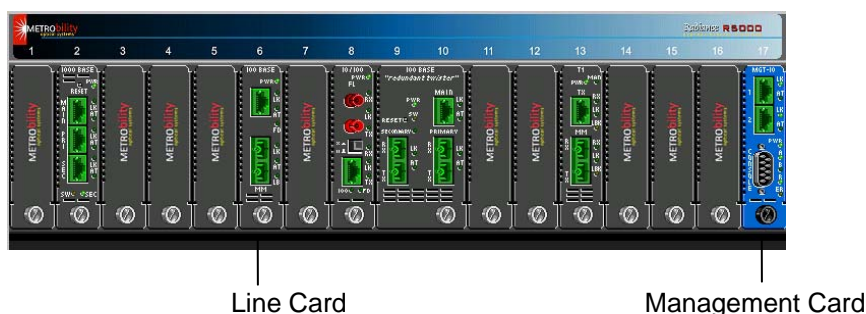
The Element Manager (EM) and Database are “headless” applications, which run as Windows Services and start automatically at boot time. Both require a client application (i.e., EM Admin Tool or Database Service Admin Tool) for management and control. The EM and EM Admin Tool may be installed on different machines, however, the Database and its admin tool cannot be separated and are installed as a bundled set.

The Element Browser is Metrobility’s innovative, Java-based graphical user interface (GUI) that simulates the appearance and functions of each network element in real time. The Element Browser graphically shows all link connections, environmental conditions, alarms, and port activity and status at a glance.

### *What is an Element?*

A Metrobility element is any manageable Radiance or Lancast device with an IP address. An element may be a Radiance RS960 Ethernet Services Provisioning Platform, a Radiance services line card in a chassis, or any chassis managed by an R502-M management card. The following is an example of a 17-slot Radiance R5000 chassis containing several cards.

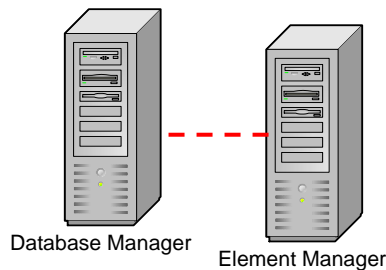
### Radiance R5000 Chassis



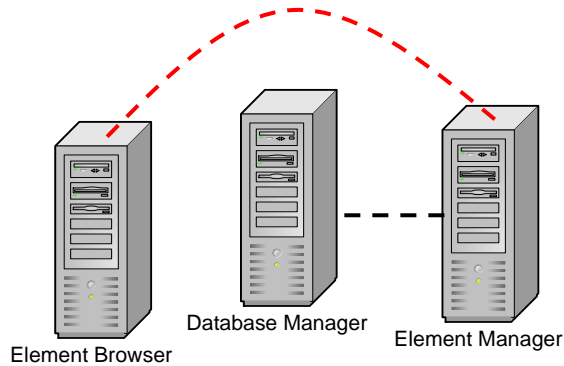
Metrobility provides a wide range of electrical-to-optical connectivity, access, and wavelength multiplexing products. Interface line cards translate information that enables the integration of differing network segments (e.g., from copper to fiber, singlemode to multimode, or Ethernet to Fast Ethernet). Modules are the replaceable cards installed into the chassis. Services line cards, access line cards, and access optical network units integrate extensive troubleshooting and remote management tools to deliver the highest level of control and management. Metrobility CWDM models provide wavelength multiplexing to achieve maximum network flexibility and scalability.

### ***How Does NetBeacon Communicate with Network Elements?***

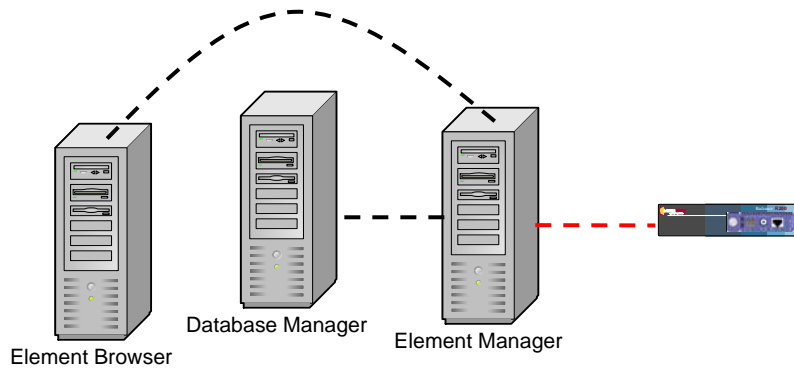
Once the NetBeacon Element Manager and Database Manager services are started, the first step in the process is establishing communications between the two services. When NetBeacon is first installed, a network administrator uses the EM and Database admin tools to enter a list of network elements along with a list of users who will have varying degrees of access to those elements.



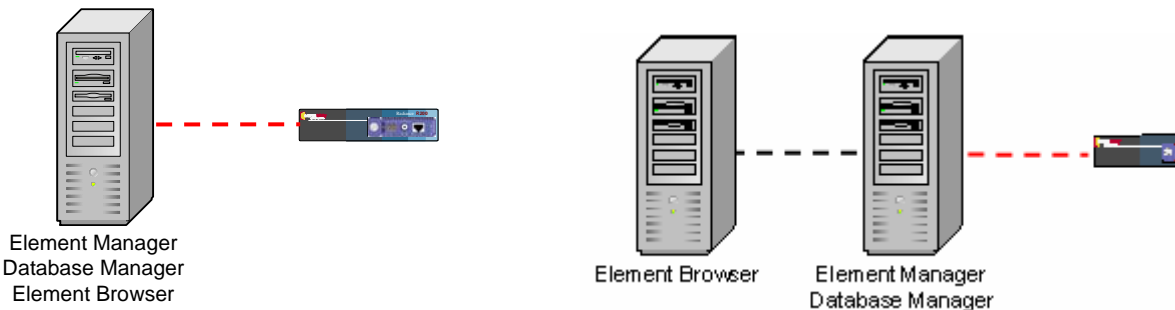
Through the NetBeacon Element Browser application, a user authenticates himself with the Element Manager and asks for permission to monitor one or more network elements.



If the request is approved, the Element Manager will seek the desired network element(s) and begin monitoring the element(s) for the user. Using the Element Browser, the user can manage, test, and/or monitor the network element(s). The NetBeacon Element Browser interface is tailored to match the access privileges of the user. The user is only allowed to view and manage those elements for which he has permission.



The Element Manager, Database Manager, and Element Browser can reside on three separate platforms, as shown in the example above, or they can reside on a single platform, as shown below, left. The Element Browser could also be on a separate machine while the Element Manager and Database Manager reside together on the same platform, as shown below, right. Multiple Element Browsers can be connected simultaneously to the same Element Manager and Database.



The R502-M management card provides the interface between the system hardware (chassis and cards) and NetBeacon. Connected through the backplane to the line cards in the chassis, the management card reports on the status and configuration of individual boards. Users can view this information and modify the device configuration through NetBeacon, if they have been given authority to do so. The management card, together with NetBeacon, provides the network administrator or any authorized user with the information necessary to maintain network uptime and achieve efficient operation.

NetBeacon also supports direct communication with an RS960 or a services line card using the device's unique IP address. In this manner, both devices serve as User Network Interfaces (UNIs) or Network Interface Devices (NIDs) with full management and monitoring access at the customer site.

Through Metrobility's patented Radiance technology, NetBeacon provides remote management of the access line card and access optical network unit without the need for an additional IP addresses at the remote site. Similarly, NetBeacon provides remote management of the services line card and RS960 using the new IEEE 802.3ah protocol. Remote site management can include non-intrusive remote loopback, bandwidth provisioning, optical power monitoring, quality of line information (RMON Group 1 statistics), and hardware "health" information (temperature and voltage).

## Features and Benefits

NetBeacon provides an efficient, user-friendly way to configure and manage all of the devices installed on a single network or on a series of networks. You can use NetBeacon as an alternative to the command line interface typically used to configure and operate network devices. NetBeacon provides an accurate display of each chassis and its cards, along with real-time status information on their operation. Management and operational tasks include the following:

- [Configuring User Log-in Authentication](#)
- [Creating and Authorizing User Accounts](#)
- [Displaying Port Details](#)
- [Monitoring the Chassis](#)
- [Downloading Software to an Element](#)
- [Displaying Temperature and Power Supply Information](#)
- [Sending E-Mail Notifications](#)
- [Configuring the Database](#)
- [Configuring Trap Destinations](#)

## System Requirements

Your management hardware must meet the minimum requirements provided in the following table. For optimal operation, the hardware should satisfy the recommended requirements.

NetBeacon Component	Minimum Hardware Requirements	Recommended Hardware Requirements	Supported Operating System
Full (all components on a single platform)	3 GHz processor, 1 GB RAM, 80 GB disk, 1024x768 screen resolution	3+ GHz processor, 1+ GB RAM, 80+ GB disk, 1024x768 screen resolution	Windows XP Professional
Element Manager	2 GHz processor, 512 MB RAM, 60 GB disk	3 GHz processor, 1 GB RAM, 80 GB disk	Windows XP Professional
Database Manager	2 GHz processor, 512 MB RAM, 60 GB disk	3 GHz processor, 1 GB RAM, 80 GB disk	Windows XP Professional
Element Browser	2 GHz processor, 512 MB RAM, 60 GB disk, 1024x768 screen resolution	2 GHz processor, 512 MB RAM, 60 GB disk, 1024x768 screen resolution	Windows XP Professional

Each NetBeacon component may be installed on a separate machine with the requirements listed above.

The Element Manager can register up to ten Element Browser clients.

Additional software may include Adobe Acrobat Reader for online viewing of this guide.

## NetBeacon CD Contents

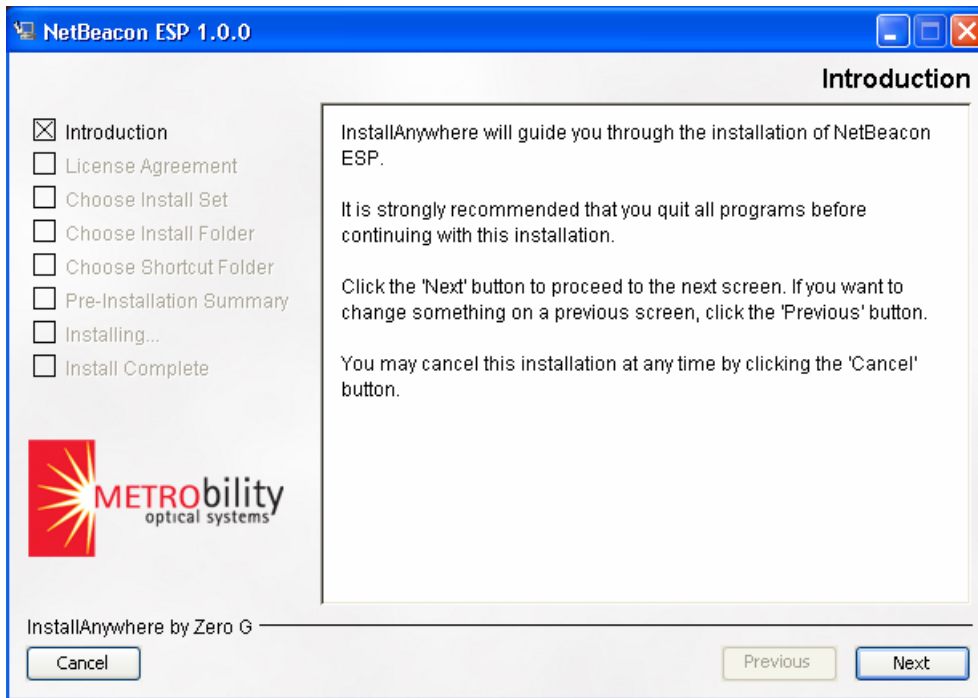
The NetBeacon CD contains the following six folders.

Folder	Contents
NetBeacon	The NetBeacon application files and Release Notes.
Firmware	Latest management card firmware (including boot code), and Release Notes.
Manuals	The documentation for installing and configuring various modules and this guide in Adobe Acrobat portable document format (PDF). Refer to the Utilities folder for the latest version of the Adobe Acrobat Reader.  For a complete list of documents available for reference, see <a href="#">Related Documents</a> .
MIBs	Management Information Base (MIB) for use with other network management software. MIB file load order.
Licenses	Metrobility and related third-party license agreements.
Utilities	The latest version of Adobe Acrobat Reader.


## Installing the NetBeacon Software

To install NetBeacon, do the following:

1. Log on to an Administrator account.
2. Exit any applications you have running.
3. Insert the compact disc into your CD-ROM drive. The installer begins automatically.
4. After InstallAnywhere completes preparing for the installation, the NetBeacon ESP Introduction window appears.

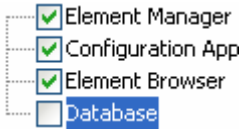


There are three buttons along the bottom of the window. Do one of the following:

- Click **Next** to continue.
  - Click **Cancel** at any time to quit the installation. If you click Cancel, a dialog box will appear asking you if you really want to quit or resume with the installation. Click **Quit** to end the process.
  - Click **Previous** to go back to the previous panel.
5. The software license agreement terms appear next. Read the agreement, click **I accept the terms of the License Agreement**, and then click **Next**.
6. Select one of the six options for installing the NetBeacon software by clicking on the  icon. Click **Next** to continue.

Installation Option	Description
Full	Installs all of the NetBeacon components (Element Manager, Admin Tool, Element Browser, Database). This is the default setting.
Element Manager	Installs a resident host service that provides the following: <ul style="list-style-type: none"> <li>• Management of SNMP elements</li> <li>• Server for Element Browsers</li> <li>• Client to Database</li> </ul>



Installation Option	Description
Database	Installs a resident host service for providing persistent storage with an SQL database. Also installs the Database Service Admin Tool.
Configuration App	Installs the administrative configuration tool for the Element Manager. This tool enables configuration of local and network-based NetBeacon components.
Element Browser	Installs the graphical user interface for configuring and displaying elements being served by the Element Manager.
Custom	<p>Allows you to customize your NetBeacon installation. After clicking <b>Next</b>, check the components you want to install, as shown in the example below. Click <b>Next</b> to continue.</p> 

- The next panel displays the default directory where the software will be installed. You may change this destination or accept the location as shown.

The default installation directory is `C:\Program Files\NetBeacon ESP`.

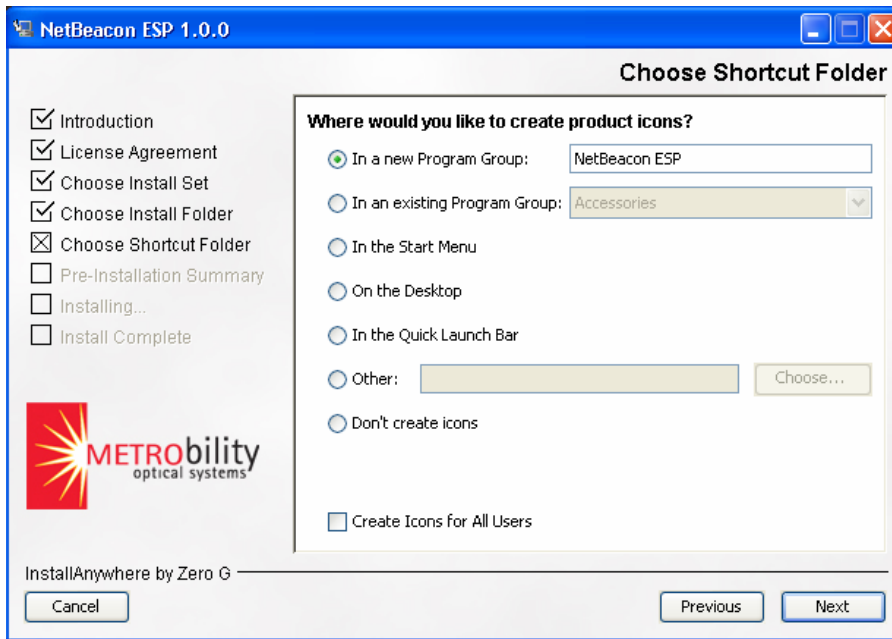
To use the default location, click **Next**.

To change the destination, do one of the following:

- Type the *name* of the directory and then click **Next**.
- Click **Choose**, go to the desired folder using the Select a Directory dialog box, click **Select**, and then click **Next**.

Click **Restore Default Folder** if you make a mistake and want to return to the default location.

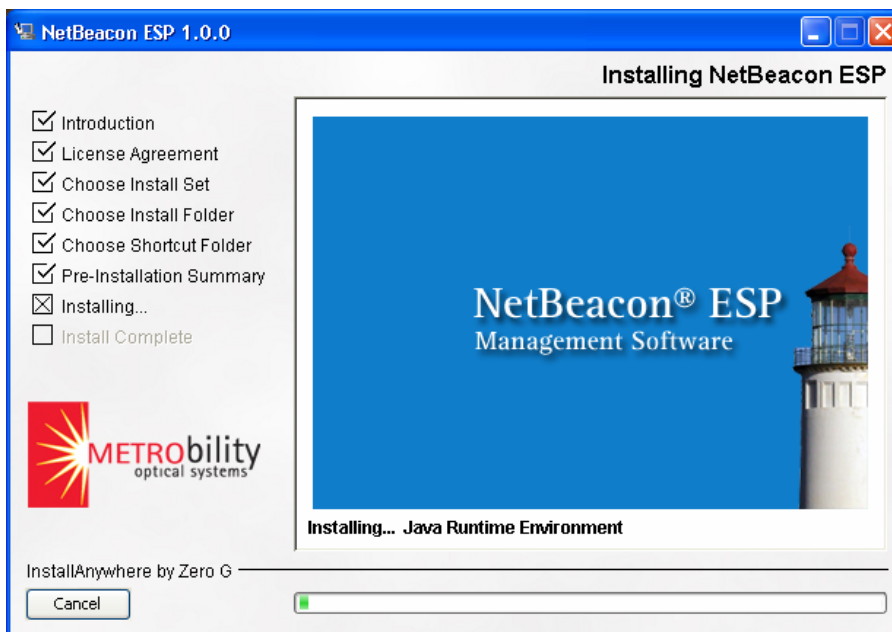
- Choose the location where you want NetBeacon shortcut icons to be created. If you do NOT want any shortcut icons, select the last option. For the first three locations, you may also select the **Create Icons for All Users** check box if you want to make NetBeacon accessible to others.



Click **Next** to continue.

9. Review the summary of installation options you have configured. If you see an error, click **Previous** to go back and make corrections. If everything is satisfactory, click **Install** to begin the installation process.

10. The installer panel displays the status of the installation.



When the installation is complete, click **Done**. If you chose to create NetBeacon icons, the shortcuts are now available.

## Uninstalling the NetBeacon Software

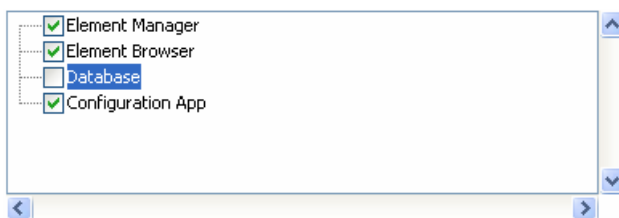
This procedure describes how to uninstall the NetBeacon software. It will remove the features and components downloaded by the installer. It will not remove the database folder(s).

**Important:** Before uninstalling NetBeacon, you must first shut down all NetBeacon applications.

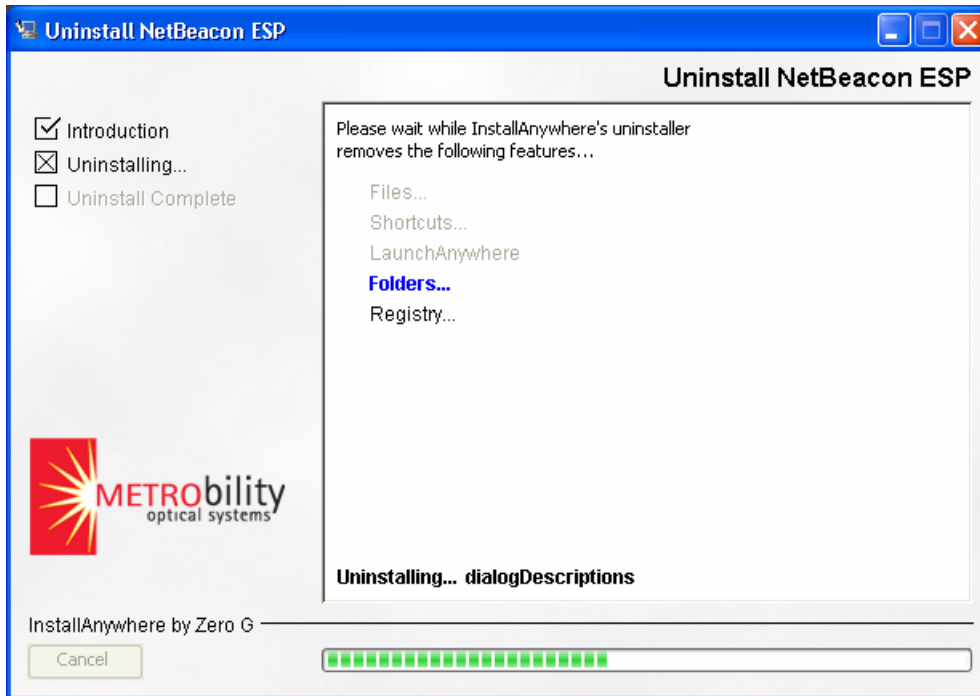
To uninstall NetBeacon, do the following:

1. Click **Start** and then choose **All Programs**.
2. From the Programs list, select **NetBeacon ESP**.
3. From the directory list, choose **Uninstall NetBeacon ESP**. The Uninstall NetBeacon ESP window appears.
4. Click **Next** to begin.
5. Choose one of the two uninstall options by clicking on the blue icon:
  - **Complete Uninstall** removes all NetBeacon software that was downloaded by the installer. Files and folders created after the installation will not be deleted. This is the default option.
  - **Uninstall Specific Features** allows you want to remove only specific components of NetBeacon. Click **Next**. The next panel lists all NetBeacon components that are installed. Clear the check box(es) for the component(s) you want removed.

In the example below, the Database component will be uninstalled, while the Element Manager, Element Browser, and Configuration Application will remain unaffected.



6. Click **Next** to begin the removal process.



7. After the NetBeacon files are successfully uninstalled, click **Done**.
8. The Complete Uninstall procedure does not remove all files. For example, any database files that were created are not deleted. If you reinstall NetBeacon, these files may be used again.

To remove the remaining files and folders, delete them manually using an Explorer window. If you installed NetBeacon in a different directory, any remaining files will reside in that directory.

## What's Next?

Now that you have installed NetBeacon successfully, you are ready to begin.

[Chapter 2. NetBeacon Basics](#) provides an overview of how to open and close the three NetBeacon windows for the Element Manager Admin Tool, Database Admin Tool, and Element Browser. Read Chapter 2 to learn about how to start and stop the NetBeacon services, as well as locate the NetBeacon version numbers.

[Chapter 3. Element Manager and Database Configuration](#) describes how to configure both the Element Manager and the Database. It explains how to add network elements and organize them into domains for management by NetBeacon. This chapter includes detailed instructions on how to establish user accounts and passwords, apply permissions to groups and individual users, and how to customize the database.

[Chapter 4. Learning about the NetBeacon Element Browser Window](#) describes the views and features available through the NetBeacon graphical user interface (GUI).

[Chapter 5. Managing the Elements](#) provides information on connecting to an element, displaying system information, and monitoring the chassis.

[Chapter 6. Configuring the Modules](#) contains detailed instructions to view statistical information and configure the various types of line cards, including the management module.

[Chapter 7. Configuring the Ports](#) explains how to configure and monitor settings related to the ports, including SFP optics with digital diagnostics.

[Chapter 8. Monitoring Traps and Alarms](#) describes the alarms and SNMP trap messages, and how to filter the information to meet your viewing preferences.



## Chapter 2. NetBeacon Basics

---

Chapter 2 provides useful information for network administrators who are just beginning to use the NetBeacon software. This chapter provides information on the following topics:

- [Starting NetBeacon](#)
- [Exiting NetBeacon](#)
- [Checking NetBeacon Version Numbers](#)

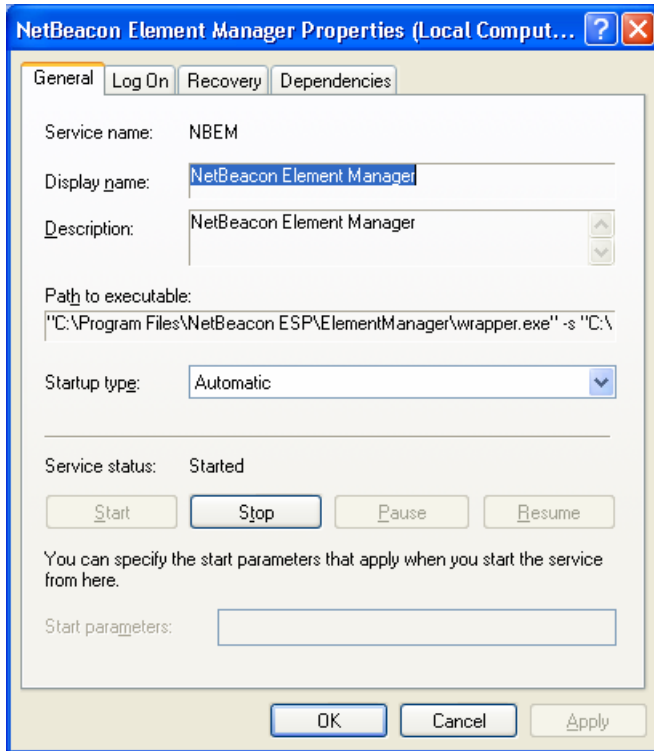
### Starting NetBeacon

The NetBeacon Element Manager and NetBeacon Database are Windows services that start automatically at boot time. To run the services effectively, you must first configure them through their client applications: the EM Admin Tool and the Database Service Admin Tool. Through the admin tool applications, you will customize the software to your particular network requirements by creating user and group accounts, selecting the authentication method, setting security parameters, defining the domain structure, creating logs, and choosing database options. After the Element Manager and Database are configured, you can run the NetBeacon Element Browser to begin monitoring and managing network devices.

#### *Viewing the NetBeacon Element Manager and Database Properties*

The NetBeacon Element Manager and Database are Windows services that are begun automatically at startup. To view the NetBeacon Element Manager or NetBeacon Database properties, do the following:

1. Click **Start** and then choose **Control Panel**.
2. From the Control Panel directory, select **Administrative Tools**.
3. From the Administrative Tools directory, select the shortcut to **Services**.
4. In the Services list, double-click **NetBeacon Database** or **NetBeacon Element Manager**. The dialog box for each service provides four tabs labeled General, Log On, Recovery, and Dependencies.
5. Click on any of the tabs to view the properties currently configured for the NetBeacon Database or the NetBeacon Element Manager.



### ***Opening the Element Manager Configuration Window***

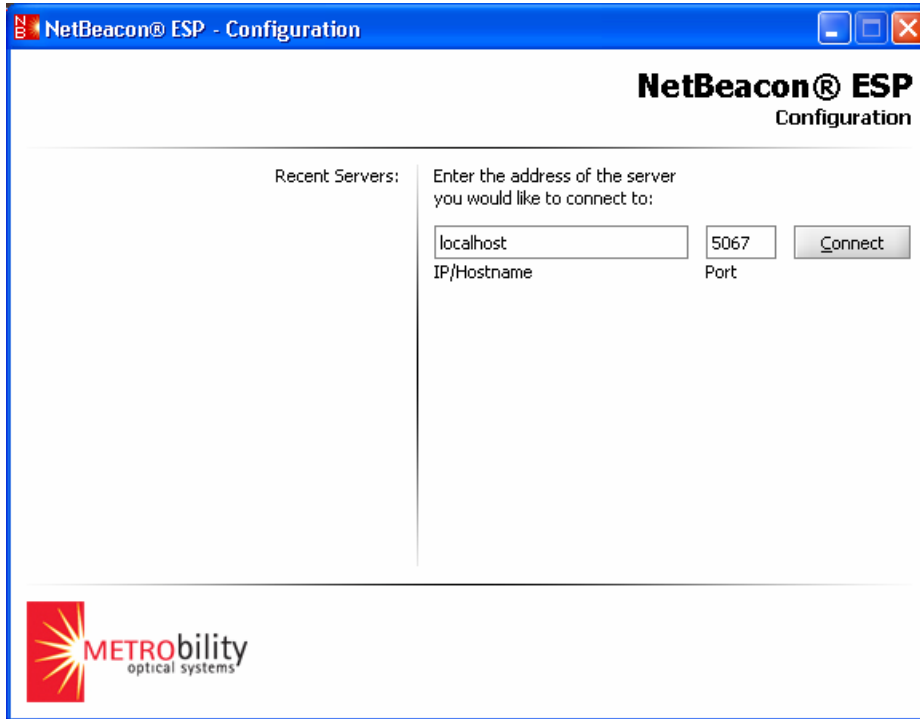
To start the NetBeacon Element Manager service configuration application, do the following:

1. Click **Start** and then choose **All Programs**.
2. From the Programs list, select **NetBeacon ESP**.
3. From the NetBeacon ESP directory, choose the **EM Configuration** application.

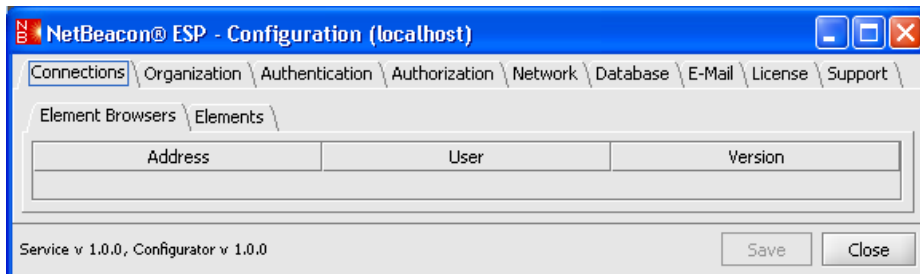
**Tip:** If you chose to add shortcut icons to the desktop, quick launch bar, or another location during the installation, you will use those icons instead of going through the Programs directory.

4. The log-in window appears. In the IP/Hostname text box, type the *IP address* or *DNS name* of the server where the Element Manager resides, or if the Element Manager is installed on your local machine, type **localhost** in the text box.
5. In the Port text box, type the port *number* (between 0 and 65535) on which the Element Manager service will listen for connections from the EM Admin Tool application. The default is port 5067.





6. Click **Connect**. After a few seconds, the NetBeacon Configuration window appears.



NOTE: The window in the above example has been resized.

Detailed information describing how to use the NetBeacon Element Manager Admin Tool is provided in [Chapter 3. Element Manager and Database Configuration](#).

### *Opening the Database Configuration Window*

To start the NetBeacon Database service configuration application, do the following:

1. Click **Start** and then choose **All Programs**.
2. From the Programs list, select **NetBeacon ESP**.
3. From the NetBeacon ESP directory, choose the **DB Configuration** application.

4. In the IP/Hostname text box, type the *IP address* or *DNS name* of the server where the Element Manager resides, or if the Element Manager is installed on your local machine, type **localhost** in the text box.
5. In the Port text box, type the port *number* (between 0 and 65535) on which the Element Manager service will listen for connections from the Database Configuration application. The default is port 5069.
6. Click **Connect**. After a few seconds, the Database Configuration window appears.

**NetBeacon ESP - Database Configuration**

**Client**

Bind to Address: 127.0.0.1    Username: netbeacon

Port: 1527    Password:

**Service Startup**

Log File:  append  overwrite

Log (dis)Connections

**Configuration Access**

Contact Port: 5069    Session Port: 5070

Auth Mode:  None  RADIUS  Platform

**Platform**

Default Domain:

**RADIUS**

Hostname:    Port: 1812

Secret:

Derby v 10.1.1.0  
Service v 1.0.0.48, Configurator v 1.0.0.48

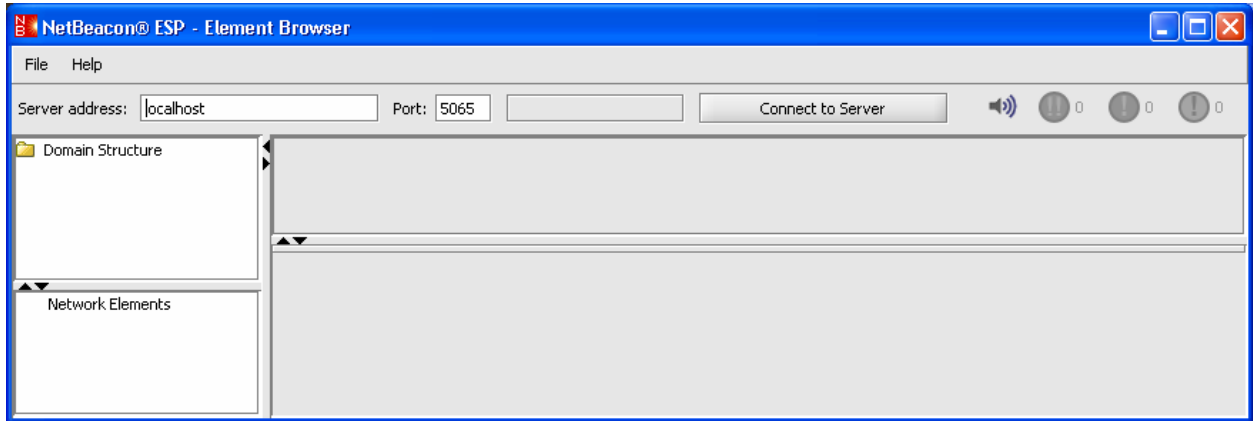
Apply    Reset    Close

Detailed information describing how to set up the Database Configuration is provided in [Configuring the Database](#).

### ***Opening the NetBeacon Element Browser Window***

To start the NetBeacon Element Browser application, do the following:

1. Click **Start** and then choose **All Programs**.
2. From the Programs list, select **NetBeacon ESP**.
3. From the NetBeacon ESP directory, choose the **Element Browser** application. The NetBeacon Element Browser window appears.



**Tip:** If you chose to add shortcuts to the desktop, quick launch bar (shown below), or any other location during the installation, you will use them to start the browser or admin tool applications instead of going through the Programs directory.



For information describing the functions and views available through this window, refer to [Chapter 4. Learning about the NetBeacon Element Browser Window](#).



## Exiting NetBeacon

The NetBeacon Element Manager and Database are headless server applications. Under most circumstances, stopping these services is not recommended. The Element Browser window may be opened and closed, but the two services should be kept operating to continue monitoring devices and performing tasks for other clients. Admin tool applications may also be closed after use.

**Important:** Stopping the NetBeacon EM service will shut down all NetBeacon operations to all clients. Stopping the NetBeacon EM is NOT recommended.

### *Closing the NetBeacon Element Browser Window*

To exit the NetBeacon Element Browser application, do one of the following:




- Click  in the upper right-hand corner of the Element Browser window.
- Right-click the NetBeacon Element Browser button  on the task bar, and then choose **Close**.
- Press the shortcut keys ALT+F4.
- From the File menu, choose **Close**.

- From the File menu, choose **Exit**, and when the confirmation message appears, click **Yes**.
- From the File menu, choose **Close All Connected to Server**, and when the confirmation message appears, click **Yes**.

**Tip:** When you close your NetBeacon Element Browser window, your display settings are saved as part of your user profile. For example, if you resized the window or any of the panels, the next time you open the NetBeacon Element Browser, the window will appear with the settings that were last used.

### *Closing the NetBeacon Element Manager Admin Tool or the Database Admin Tool Windows*

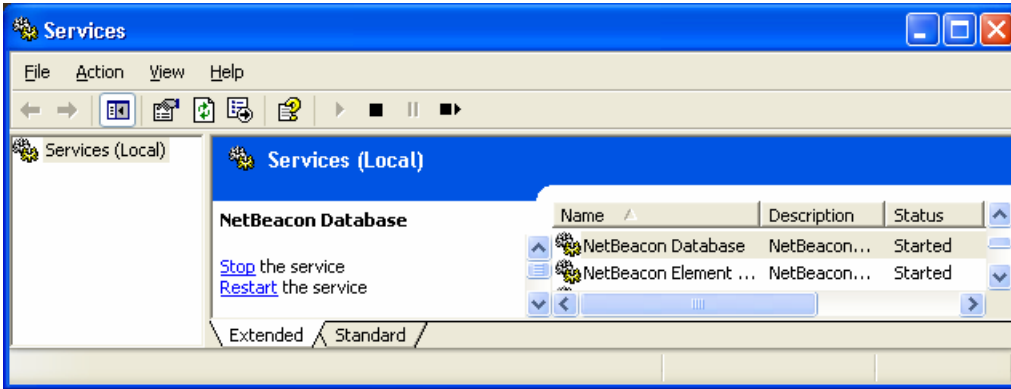
To shut down either of the admin tool applications, do one of the following:

- Click  in the upper right-hand corner of the Configuration window.
- In the Configuration window, click **Close**.
- Right-click the NetBeacon® ESP Database Configuration  button or the NetBeacon® ESP Configuration  button on the task bar, and then choose **Close**.
- Press the shortcut keys ALT+F4.

### *Stopping the NetBeacon Element Manager Service or the NetBeacon Database Service*

To stop running the NetBeacon Element Manager or Database service, do the following:

1. Close all open client applications such as the Element Browser. All applications must be closed before you stop either of the services.
2. Click **Start** and then choose **Control Panel**.
3. From the Control Panel directory, select **Administrative Tools**.
4. From the Administrative Tools directory, select the shortcut to **Services**.
5. Do one of the following:
  - From the Services list, click **NetBeacon Database** or **NetBeacon Element Manager**. Click **Stop** to end the service.



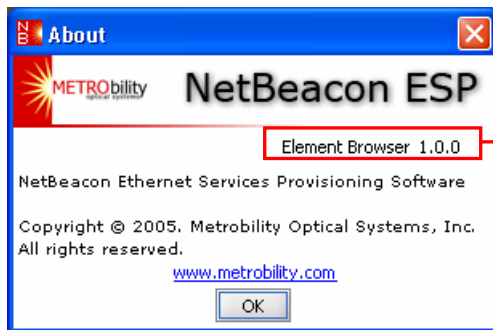
- From the Services list, right-click **NetBeacon Database** or **NetBeacon Element Manager**, and then choose **Stop**.
- From the Services list, double-click **NetBeacon Database** or **NetBeacon Element Manager**. Click the **General** tab, if it is not already selected. Under Service status, click the **Stop** button.

## Checking NetBeacon Version Numbers

If you have a problem using NetBeacon, you will need to know the version number of your NetBeacon software components before contacting technical support. To check the firmware version on the management card, see [Displaying Management Module Information](#).

### *Element Browser Version Number*

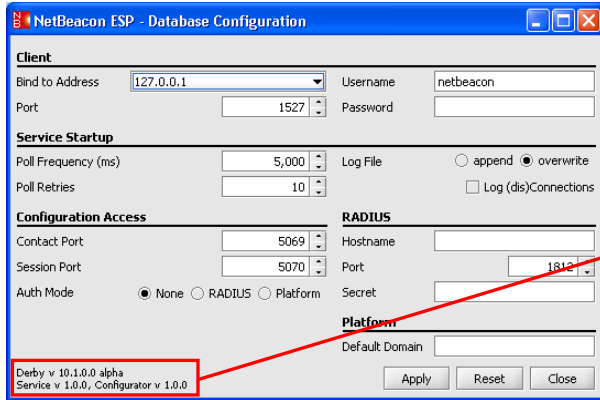
Open the Element Browser window. From the Help menu, choose **About**. The new window shows the software version of the Element Browser. From the About window, you can click on [www.metrobility.com](http://www.metrobility.com) to connect to Metrobility's website.



Element Browser version number

### *Database Service and Database Service Admin Tool Version Numbers*

Open the Database Configuration window. The version numbers for the NetBeacon Database Service and Admin Tool (Configurator), as well as the Apache Derby database, are printed in the lower left corner.

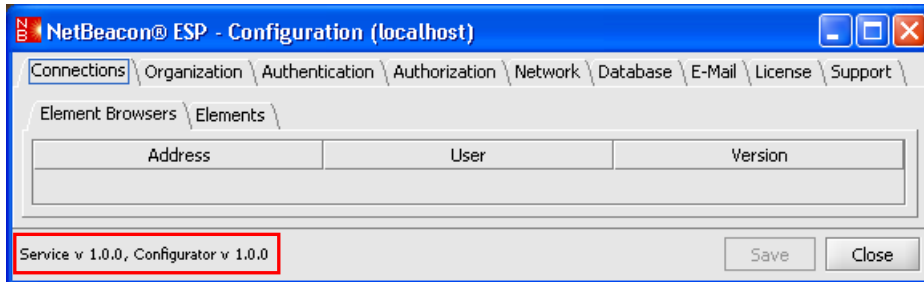


Apache Derby database version number

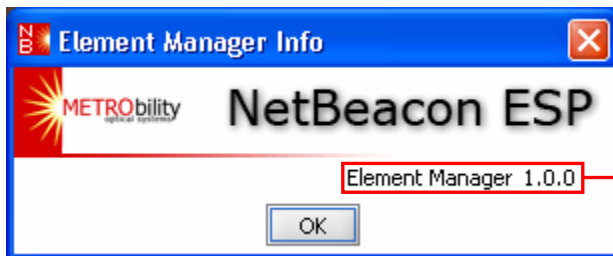
NetBeacon Database Service and Database Admin Tool version numbers

### *Element Manager Service and Element Manager Admin Tool Version Numbers*

Open the NetBeacon Configuration window. The Element Manager Service and Admin Tool (Configurator) version numbers are printed in small text at the lower left corner of the window.



Alternatively, you can view the Element Manager version number from the Element Browser window, if the browser is connected to the Element Manager. From the Help menu, choose **Element Manager Info**. The new window shows the software version of the Element Manager.



Element Manager version number

## Chapter 3. Element Manager and Database Configuration

---

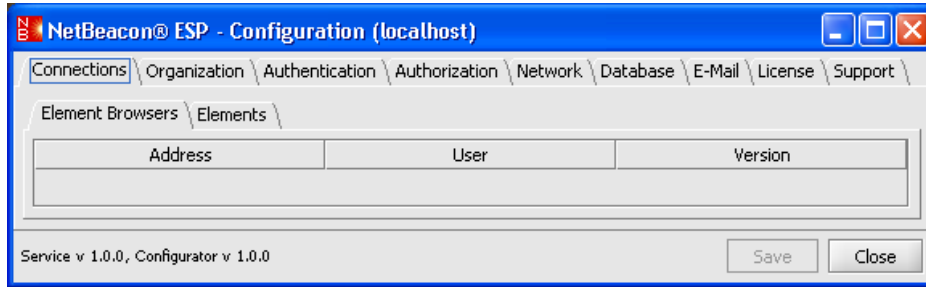
Before you begin monitoring network elements, you must first configure the NetBeacon Element Manager through the admin tool application. Chapter 3 describes the NetBeacon Configuration window and provides the steps necessary to add each device you want to manage, create a domain structure, organize user groups, create user accounts, and set up security parameters. This chapter also describes how to configure the NetBeacon Database using the Database Service Admin Tool application. The following topics are covered in this chapter:

- [Learning about the NetBeacon Configuration Window](#)
- [Adding and Removing Elements](#)
- [Configuring SNMP Settings](#)
- [Downloading Software to an Element](#)
- [Defining the Domain Structure Organization](#)
- [Configuring User Log-in Authentication](#)
- [Creating and Authorizing User Accounts](#)
- [Specifying Network Parameters](#)
- [Configuring the Database](#)
- [Sending E-Mail Notifications](#)
- [To prevent users from](#) receiving numerous repetitive e-mail messages at very high rates, NetBeacon includes automatic e-mail flood suppression. After an alarm for which an e-mail should be generated occurs, NetBeacon waits up to 30 seconds for subsequent alarms for the same element and e-mail address. All subsequent alarms are bundled into one combined e-mail message.

Once an alarm e-mail has been sent, NetBeacon will not send an alarm to the same user regarding the same element until five minutes have passed, at which time the user will receive an e-mail message containing all alarms for the last five minutes for the given element, if any alarms for that element have occurred.

- Entering the NetBeacon License
- [Seeking Metrobility Support](#)

## Learning about the NetBeacon Configuration Window



The NetBeacon Configuration window is comprised of nine tabs. Metrobility recommends configuring the software by going through the tabs from left to right. The functions and settings configured under each tab are described in detail in this chapter and summarized in the table below.

Tab Name	Description
Connections	View information for all Element Browsers currently connected to the Element Manager, add or remove elements you want to manage through NetBeacon, and update the firmware on a management card or services line card.
Organization	Create the domain structure by adding elements to named containers.
Authentication	Select the authentication method required to access the Element Manager and configure security parameters such as user names and passwords.
Authorization	Create groups and assign users to them with applied read or write privileges. Privileges may also be denied.
Network	Specify the network contact and session ports, along with the interface to which they are bound, for both the Element Browser and the EM Admin Tool. Enable or disable the built-in TFTP server, enter information to connect to an e-mail server, and specify encryption parameters.
Database	Choose tables to include in a named database.
E-Mail	Customize NetBeacon to send automatic e-mail notifications to one or more recipients when certain events occur.
License	Request, view, or enter NetBeacon license information.
Support	Link to Metrobility's customer support website and reference materials.

The NetBeacon Configuration window provides two buttons, Save and Close, located in the lower right corner.

Button Name	Description
Save	Save all modifications that have been entered, including those under tabs that are not currently visible.



Button Name	Description
Close	Close the NetBeacon Configuration window and shut down the Admin Tool application without saving any of your changes.

**Important:** You must click the **Save** button before you close the NetBeacon Configuration window to keep any changes you have made. If you do not click **Save**, all modifications will be lost.

## Adding and Removing Elements

### *Adding a New Element*

For each element you want to manage via NetBeacon, do the following:

1. Start the NetBeacon EM Admin Tool and connect to the server where the Element Manager resides. The NetBeacon Configuration window appears.
2. Click the **Connections** tab, if it is not currently selected. Under the Connections tab are two additional tabs labeled Elements Browsers and Elements.

When a NetBeacon Element Browser connects to the Element Manager, the Browser's IP address, the name of its associated user, and the Browser's software version are recorded and listed under the Element Browsers tab. If this is the first time you are using the Admin Tool, or if no devices are connected to the Element Manager, the list will be empty.

3. Click the **Elements** tab.
4. Click the **Add** button. The Add Element dialog box appears.

5. In the Address text box, type the *IP address* or *DNS name* of the element you want to add.

6. Go to the section [Configuring SNMP Settings](#) for instructions on how to configure the SNMP access information.
7. If the element you are adding is a services line card, type the *administrative community string* in the **Admin** text box to enable access to the element's SNMP community strings, FTP download username and password, trap manager, and trap e-mail setup. The default administrative community string is admin. This field is applicable only when NetBeacon is communicating directly with a services line card.
8. If you want the element to send traps and alarms to NetBeacon Element Browsers, select the check box for **Mark this element as in service**. If the check box is not selected, alarms will not be reported. This feature may be useful if an element must be taken off-line temporarily for maintenance, as it will prevent the element from sending unnecessary alarms.

**Tip:** Metrobility recommends NOT marking elements as in service until all configuration changes have been made.

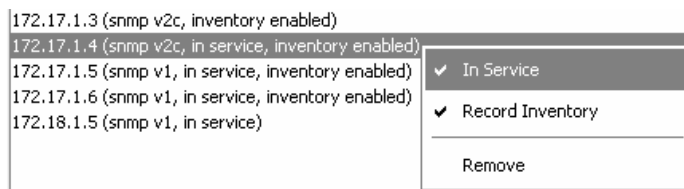
9. If the database is enabled and you want NetBeacon to store hardware information about the element into the database for inventory purposes, select the check box for **Record inventory for this element**.

10. Click **OK**. The element appears in blue text under the Elements tab. Blue indicates that the information has not been saved. The element's SNMP version appears in parentheses. If the element is in service or if inventory recording is enabled, they also will be noted in the parentheses.

**Tip:** As an alternative to clicking OK, you can press the shortcut keys ALT+O. To cancel and close the dialog box, you can click **Cancel** or press ALT+C.

11. Click **Save**.

**Tip:** Once an element has been added, you can right-click on it to change the service and inventory settings, as shown below. You may also delete an element from the list by choosing **Remove** from this pop-up menu.

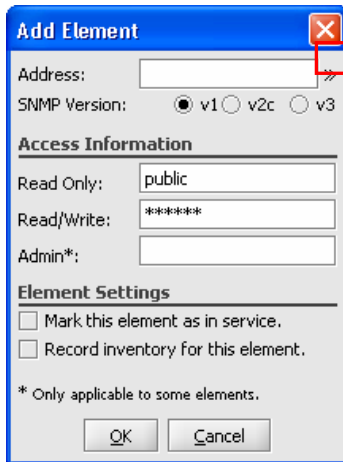


### ***Adding Multiple Elements***

Instead of repeatedly entering each network element individually, you can use an option that allows you to generate multiple elements simultaneously. You can enter multiple DNS names or a set of similar IP addresses.

1. Under the Elements tab, click **Add**.

2. When the Add Element dialog box appears, click the right-pointing double angle bracket (») located at the end of the Address text box.



Click here to enter multiple elements.

3. In the Address text box, do one of the following:

- Type an asterisk (\*) to enter a series of DNS names. If the names all have a common prefix or suffix, it may be entered along with the asterisk (e.g., \*@metroblity). The prefix or suffix will be added to each name.
- Type the *IP address* with an asterisk in the part that you do not want repeated. For example, you can type 196.168.1.\*, if you want the first three numbers repeated, but not the fourth. Partial numbers are acceptable. For example, you also can type 196.168.1.2\*, if you want the first three numbers repeated and the fourth number to always begin with 2 (e.g., 196.168.1.21, 196.168.1.22, 196.168.1.23, 196.168.1.24).

**Tip:** Click the question mark (?) to open a ToolTip that explains how to configure multiple elements. The ToolTip remains open until you click on it.

4. Select the check box that says **Generate multiple elements**.




5. Do one of the following:

- For multiple IP addresses: type the *first number* in the series in the Start text box, the *last number* in the series in the End text box, and the *increments* between the first and last numbers in the Step text box. Any number between 0 and 254 may be entered into the three text boxes. For example, if you enter the numbers 20, 35, and 5, along with an address of 196.198.1.\*, NetBeacon will generate the following IP addresses: 196.198.1.20, 196.198.1.25, 196.198.1.30, and 196.198.1.35.

Start: 20 End: 35 Step: 5

- To enter a series of DNS names, click the left-pointing double angle bracket («) located at the end of the Step text box. In the List text box that appears, type the DNS names of each element you want to add, separating each element name with a comma. Valid characters are letters (a-z, A-Z), numbers (0-9), and hyphens (-);

spaces are not permitted.

Address:    
 Generate multiple elements   
List:  

6. Go to [Configuring SNMP Settings](#) for instructions on how to change the SNMP settings.
7. Refer to Steps 7-11 in [Adding a New Element](#), to configure the element settings. The settings will be applied to all the newly generated elements.

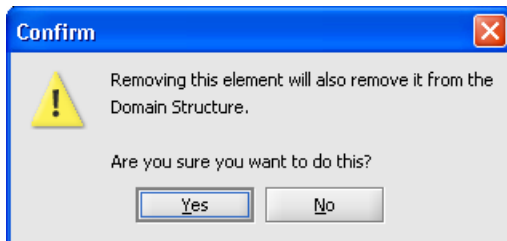
### *Deleting an Element*

To remove one or more elements, do the following:

1. Select the **Connections** tab in the NetBeacon Configuration window.
2. Click the **Elements** tab.
3. Click on the IP address or DNS name of the element(s) you want to delete and click the **Remove** button.

**Tip:** To select multiple elements, hold down the CTRL key, and click on each element you want to remove. To select multiple element in a series, select the first element, hold down the SHIFT key, and click on the last element you want to delete.

4. If an element has already been assigned to a domain, the following confirmation dialog box appears.



Click **Yes** to remove the element.

5. Click **Save**.

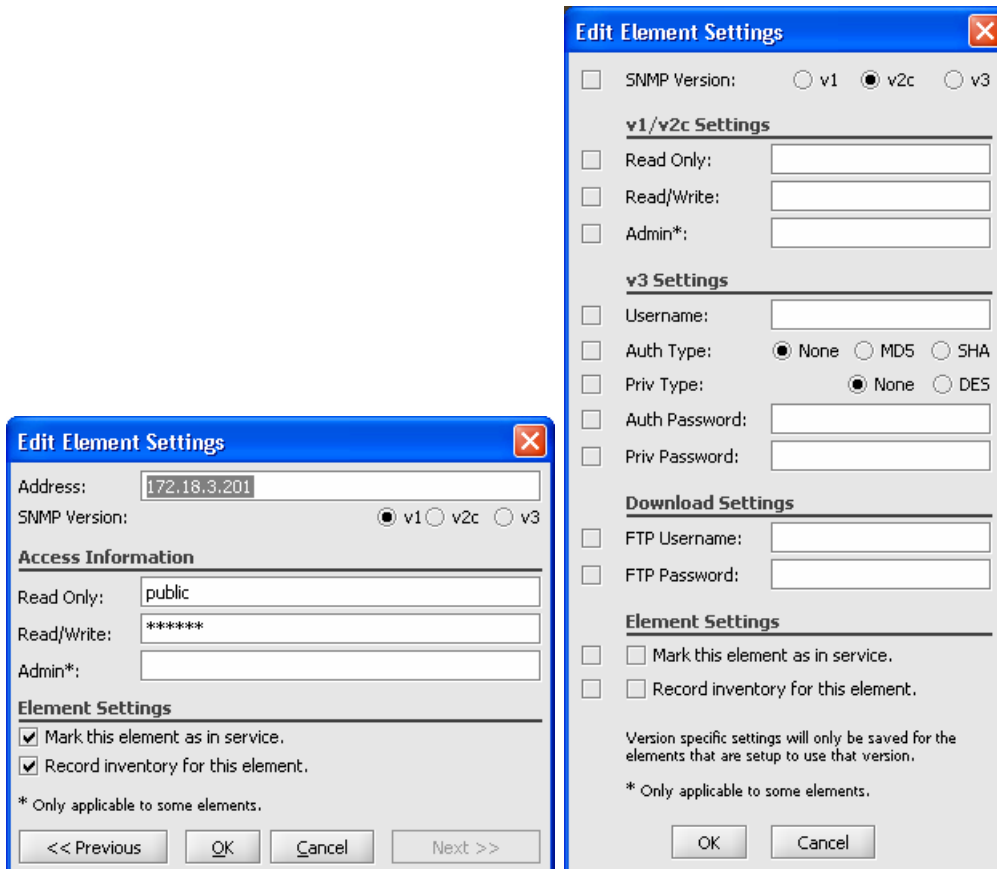
### *Editing Element Settings*

To change any of the settings for one or more elements, do the following:

1. Open the NetBeacon Configuration window and select the **Connections** tab.
2. Click the **Elements** tab.
3. Click on the element(s) you want to modify.

- Click the **View/Edit SNMP Settings** button. The Edit Element Settings dialog box appears. If one element is selected, the dialog on the left appears. If two or more elements are selected, the dialog on the right appears.

**Tip:** If you want to edit the setting for a single element, simply double-click on the element to open the Edit Element Settings dialog box.



- Change the desired settings as described in Steps 5-11 in [Adding a New Element](#). To change the SNMP configuration, refer to [Configuring SNMP Settings](#).

When changing SNMP settings for multiple elements, note the following points:

- If the SNMP Version is changed, it will be applied to all selected elements.
- If the selected elements are configured for different SNMP versions, changing the v1/v2c Settings will only apply to elements that are already configured for SNMPv1 or SNMPv2c. Changing the v3 Settings will only apply to elements that are already configured for SNMPv3.
- The Admin text box is only applicable to services line cards communicating directly with NetBeacon using the card's IP address.

- If one or both of the options under Element Settings are changed, they will be applied to all selected elements.
  - To specify that the elements are in service, both check boxes must be selected. To specify that the elements are not in service, select only the left check box.
  - To record inventory for the selected elements, both check boxes must be selected. If you do not want to record inventory for the elements, select only the left check box.
  - If a check box in the far left is not selected, the setting associated with the check box will not be altered when you click OK.
6. If you are editing for a single element, you may click **Previous** or **Next** to view and/or modify parameters for the previous or next element in the Elements list. Modified elements will appear in blue text as you go up or down the list.
  7. Click **OK**.
  8. Click **Save**.

## Configuring SNMP Settings

Through the NetBeacon EM Admin Tool, you can configure SNMPv1/v2 community strings as well as SNMPv3 security for accessing network elements. If you want to connect to a Radiance services line card, or are unable to establish the initial connection to hardware which has been configured outside of NetBeacon, or encounter problems involving multiple clients accessing the same element when community strings are changed, follow the procedure below to ensure proper SNMP device access.

In the Add Element or Edit Element Settings dialog box, select the version (**v1**, **v2**, or **v3**) of the element's SNMP agent. Validation depends on which version is selected.

### *SNMPv1 or SNMPv2*

When SNMPv1 or v2c is selected, two text boxes appear under the Access Information heading in the Add Element dialog box. The third text box, Admin, is only applicable to services line cards.

SNMP Version:  v1  v2c  v3

**Access Information**

Read Only:

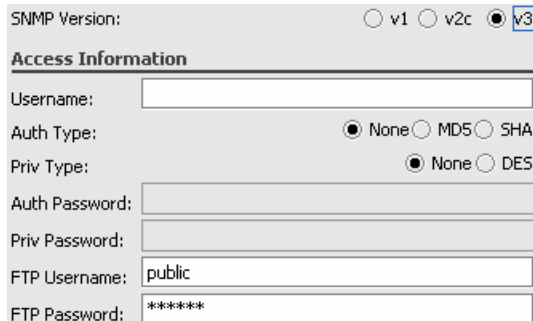
Read/Write:

1. In the Read Only community string text box, type a unique *string* authorizing SNMP read access to the device. The default string is public.

- In the Read/Write community string text box, type a unique *string* authorizing SNMP write access to the device. The default string is public.
- Click **OK**.
- Click **Save**.

### SNMPv3

If SNMPv3 is selected, additional fields will become available, as shown below.



SNMP Version:  v1  v2c  v3

**Access Information**

Username:

Auth Type:  None  MD5  SHA

Priv Type:  None  DES

Auth Password:

Priv Password:

FTP Username:

FTP Password:

- In the Username text box, type the *user name* which has access to the element.

Use the following table to determine which fields are required for SNMPv3 devices based on their levels of security.

SNMPv3 Security Level	Authentication Password	Encryption Algorithm	Privacy Password
No Authentication, No Privacy			
Authentication, No Privacy	X	X	
Authentication, Privacy	X	X	X

- Select the algorithm, **MD5** or **SHA**, that will be used to validate the authentication process. Both options require an authentication password. If authentication is not required, select **None** (default).

**Important:** The services line card only supports MD5 authentication. SHA is not applicable to Metrobility devices.

- Specify the use of data encryption by selecting **None** or **DES**. By default, the data is not encrypted. DES requires a privacy password.
- If you have specified an authentication type, type the user's authentication *password* in the Auth Password text box.
- If the SNMPv3 device requires encryption (i.e., DES is selected), type the *password* in the Priv Password text box.

6. If the SNMPv3 device is an R502-M management card that uses FTP for transferring firmware files, type the *user name* and the user's *password* in the FTP Username and FTP Password text boxes. The default strings are public and public.
7. Click **OK**.
8. Click **Save**.

## Downloading Software to an Element

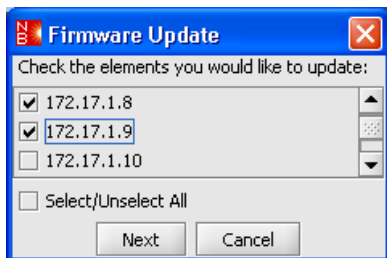
The firmware installed on Metrobility's management card and services line cards can easily be updated to the latest code. For a management card, the image software (`corepm.biz`) and boot code (`boot.bin`) are replaceable. When new software is downloaded onto a management card, it overrides the older version. You may update one or both files.

For a services line card, its operating system (OS), FPGA code, and bootloader files are replaceable. Unlike the management card which stores only one version of its software, the services line card holds two versions of the OS and FPGA. Once the software is downloaded, you can select which version to activate. If you download a new bootloader, it will overwrite the existing code.

The NetBeacon CD contains a directory called Firmware. This directory contains the management card software, including Release Notes.

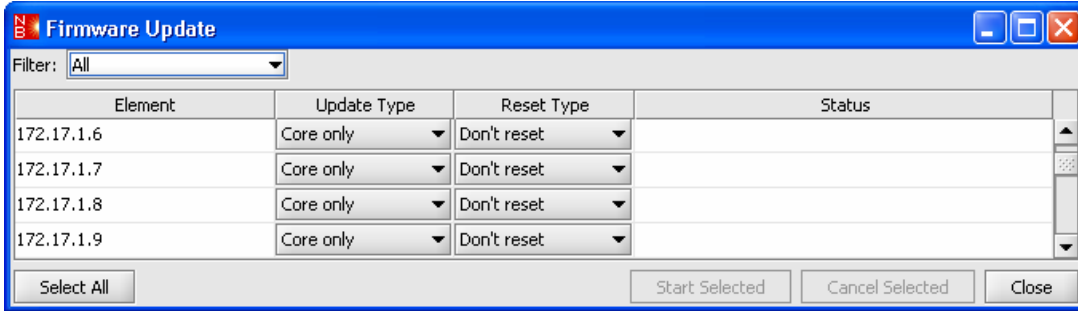
This section describes how to configure download parameters and monitor the software transfer progress.

1. In the NetBeacon Configuration window, click the **Connections** tab.
2. Click the **Elements** tab.
3. Click the **Firmware Update** button. The Firmware Update dialog box appears with a list of all elements you have added.



4. Check each element you want to update, or check **Select/Unselect All**.
5. Click **Next** to continue.
6. All elements you selected are displayed in the Firmware Update table.





**Tip:** Use the Filter drop-down menu to specify the card(s) you want displayed in the table.

Filter Option	Description
All	Display all management cards and services line cards.
R50x managed elements	Display all R50x management cards.
Services Line Cards	Display all services line cards.

7. Choose the type of software you want to update from the options listed under the Update Type column. For a management card, choose one of the following options:

- **Core only:** Replace only the image file, corepm.biz.
- **Core and boot:** Replace both the boot and core files.

For a services line card, choose one of the following options:

- **OS:** Download the new operating system software into the inactive location.
- **FPGA:** Download the new FPGA code into the inactive location.
- **OS and FPGA:** Download both the OS and FPGA into the inactive location for each.
- **Bootloader:** Update the boot code.

8. For a management card, click in the Reset Type column to specify whether or not to reset the card after downloading the new software. For a services card, choose one of the following options under the Reset Type column:

- **No set or reset:** keep the current OS or FPGA active and do not reset the card. The newly downloaded firmware will be inactive.
- **Set and reset:** activate the new OS or FPGA after downloading, and reset the card.
- **Set, no reset:** after downloading, do not reset the card, however, prepare the new OS or FPGA so that when the card is reset, the new software is activated.

9. Select each element you want to upgrade. Click **Select All** to upgrade all elements in the table.
10. Click **Start Selected** to begin downloading. The software transfer progress is displayed in the Status column of the table.

Status
Boot: 1.3.8, CorePM: 1.3.8
85% - Good

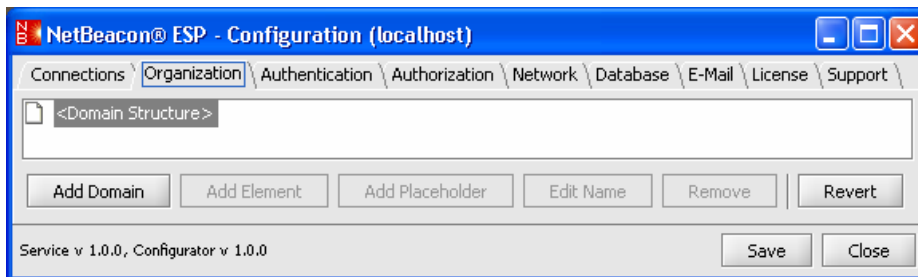
11. To stop the downloading process, select the element and click **Cancel Selected**.

## Defining the Domain Structure Organization

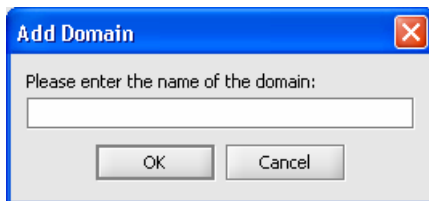
After adding all the elements you want to manage, you now must organize the elements into a hierarchical structure consisting of domains. There must be at least one domain in which the elements can be a member. Each element can only belong to one domain.

### Creating New Network Domains

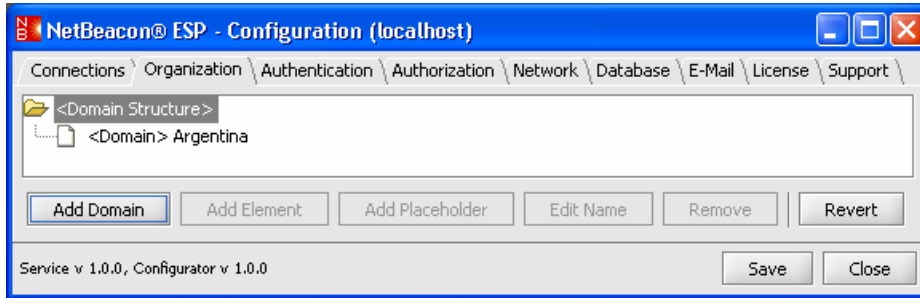
1. Click the **Organization** tab in the NetBeacon Configuration window.



2. Select the domain into which you want to add a new domain. If this is the first time you are adding a domain, the only existing domain to select is the default Domain Structure.
3. Click **Add Domain**. The Add Domain dialog box appears.



4. Type the *name* of the domain in the text box.
5. Click **OK**. A new domain appears under Domain Structure.

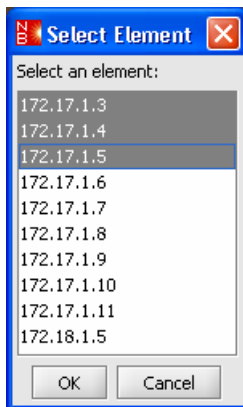


6. Click **Save**.
7. To add another domain, repeat the steps above. In the example shown in Step 5, you can add another domain under `Domain Structure` or under `Argentina`.

### *Assigning Elements to a Domain*

Once you have created your domain structure, you are ready to assign elements to the individual domains. Each element can only be a member of one domain, but a domain can have multiple elements.

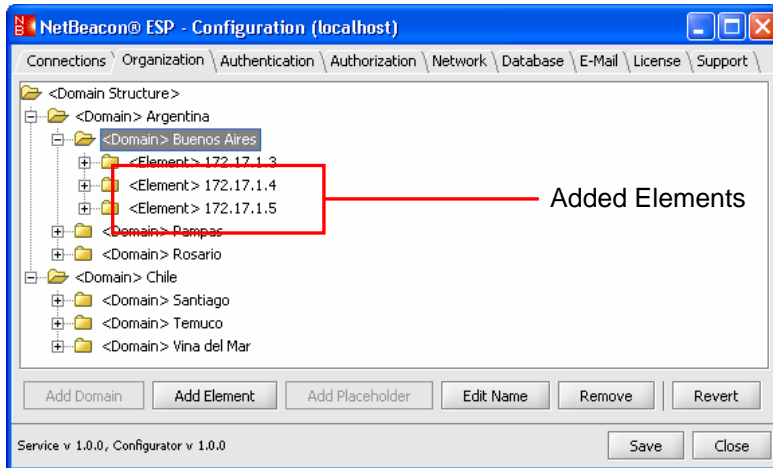
1. Select the domain into which you want to add an element.
2. Click the **Add Element** button. The list of elements you entered earlier now appears in the `Select Element` dialog box.







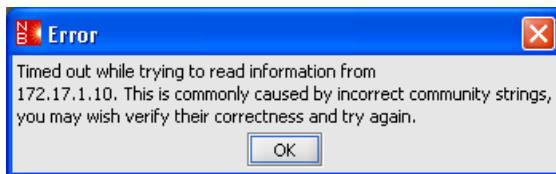
3. Choose the element(s) you want to put into the domain you have selected.

**Tip:** To select multiple elements, hold down the `CTRL` key, and click on each element you want to include. To select more than one element in a series, select the first element, hold down the `SHIFT` key, and click on the last element you want to include.

4. Click **OK**. The element(s) are added to the domain.



When elements are added to a domain, the domain's icon changes from  to . As elements are discovered, their icons also change from  to . If NetBeacon fails to discover an element, the following error message appears. Make sure the element's SNMP version and community strings are entered correctly.



5. Click **Save**.

### *Deleting a Domain or Element*

1. Under the **Organization** tab in the NetBeacon Configuration window, select the element you want to delete from a domain.

Or:

Select the domain you want to delete. If you delete a domain, everything in that domain will be removed, including other sub-domains and their elements. The only domain you cannot delete is the top level Domain Structure.

2. Click **Remove**. The element or group no longer appears in the Domain Structure.
3. Click **Save**.

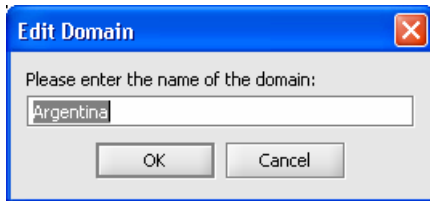
### *Undoing Changes*

NetBeacon provides an option to undo any Domain Structure changes you have made but not yet saved. This option will restore the Domain Structure back to its last saved version. To undo changes, click **Revert**.

## *Editing the Name*

The name of any domain can be modified. Element names cannot be changed.

1. Click the **Organization** tab in the NetBeacon Configuration window.
2. Select the domain you want to rename.
3. Click **Edit Name**. The Edit Domain dialog box appears.



4. In the text box, type the new *name* you want to apply.
5. Click **OK**.
6. Click **Save**.

## *Creating a Placeholder*

NetBeacon includes a feature that allows you to set up an off-line domain structure. For example, if you are configuring the network for a new building and want to set up devices before users arrive, you can use the placeholder feature. You may assign users and permissions to the placeholders, which will be activated as soon as the actual component is enabled. A placeholder can represent a stack, chassis, module, or port.

1. Click the **Organization** tab in the NetBeacon Configuration window.
2. Do one of the following:
  - Select the element into which you want to add a stack placeholder. Note that you cannot select elements that have already been discovered.
  - Select the stack into which you want to add a chassis placeholder.
  - Select the chassis into which you want to add a module placeholder.
  - Select the module into which you want to a port placeholder.
3. Click **Add Placeholder**. A new stack, chassis, module, or port appears in the display panel.
4. Repeat Steps 2 and 3 for each placeholder you want add.
5. Click **Save**.

## Configuring User Log-in Authentication

By default NetBeacon does not provide any authentication for individual users, however, through the NetBeacon EM Admin Tool, you can apply one of three log-in security modes: basic, Windows, or RADIUS. The authentication described in this section applies to users who attempt to connect to the NetBeacon EM Admin Tool or Element Browser.

When the authentication mode is changed to basic, platform, or RADIUS, all users are denied access to all elements by default. Under any of these modes, users must be given permission to read and/or write.

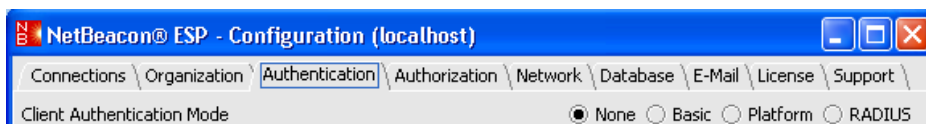
**IMPORTANT:** When the client authentication mode is set to basic, platform, or RADIUS, at least one user must be listed in the NetBeacon Administrators group in the Authorization tab. If you do not have a user in the group, all users will be locked out of NetBeacon.

The NetBeacon log-in security modes are described below:

- **None:** This is the default setting. NetBeacon requires no authentication. Users are connected automatically without having to enter a user name or password.
- **Basic:** When configured for basic log-in, NetBeacon maintains a database of user names and passwords that you set up.
- **Platform:** When configured for Platform login authorization, NetBeacon validates users via a specified Windows domain server.
- **RADIUS:** The NetBeacon Element Manager is configured as a RADIUS client. The RADIUS user name and password must be entered to log on to the NetBeacon EM Admin Tool or Element Browser.

To configure user log-in authentication, do the following:

1. Click the **Authentication** tab in the NetBeacon Configuration window.
2. Configure the Basic, Platform, or RADIUS parameters by selecting one of the tabs and filling out the information (see below).
3. Select one of the four Client Authentication Modes to activate one of the modes. Simply filling in the information in the tabbed section will not activate the mode; the corresponding radio button must also be selected.



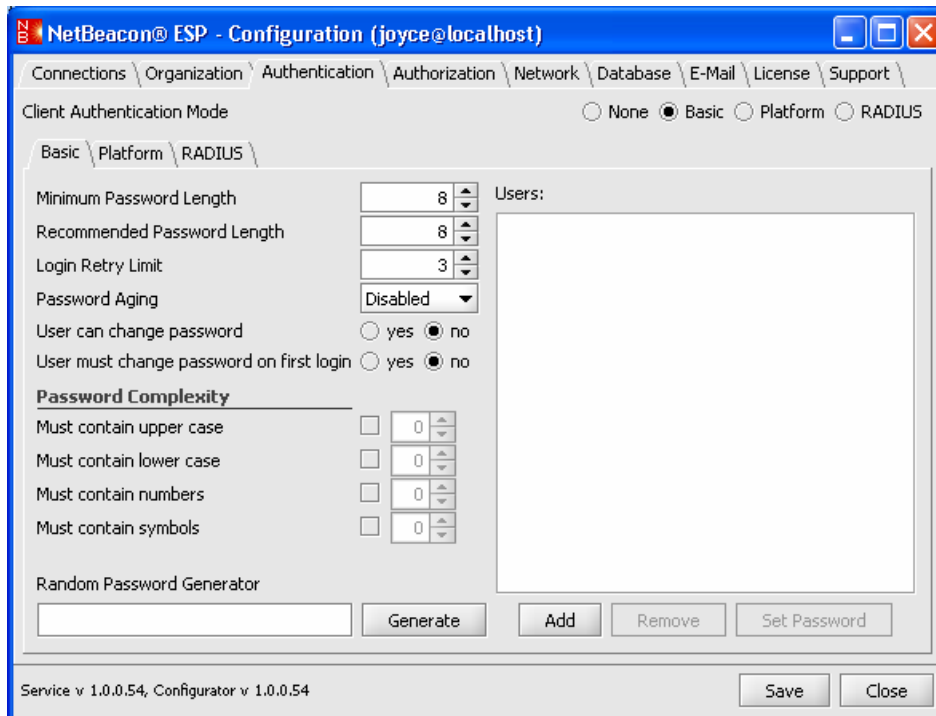
4. Click **Save**. The changes will take effect the next time a user tries to connect to the Element Manager through the NetBeacon Element Browser or Admin Tool application.

## No Authentication

This is the default setting. If you want users to have immediate access to NetBeacon, without entering a user name or password, choose **None** for the Client Authentication Mode.

## Basic Log-in

The second option enables basic log-in authentication (i.e., a user name and corresponding password).



Click the **Basic** tab.

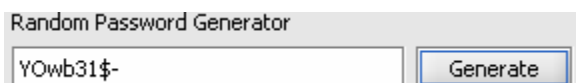
### Creating Passwords for Basic Log-in Users

The NetBeacon EM Admin Tool allows you to specify various password characteristics for all basic log-in users.

Password Feature	Description
Minimum Password Length	Specify the minimum number of characters allowed for user passwords. The range is 1-256. The default is 8 characters.
Recommended Password Length	Specify the number of characters user passwords should contain. The range is 0-256. The default is 8 characters.
Login Retry Limit	Specify the maximum number of times the user will be allowed to enter an incorrect password for logging on to the NetBeacon EM Admin Tool or

Password Feature	Description
	Element Browser. The range is 0-100. The default is 3.
Password Aging	Choose the maximum length of time passwords will be valid. The default is 0, which means no expiration. Other options are 30, 60, 90, and 120 days.
User can change password	Indicate whether or not users will be allowed to change their own passwords. The default is no.
User must change password on first login	Indicate whether or not users are required to change their default passwords the first time they log in. The default is no.
Must contain upper case	Enable the check box and select a value between 0 and 64 to specify the minimum number of upper case letters each password must contain. The default is disabled and 0.
Must contain lower case	Enable the check box and select a value between 0 and 64 to specify the minimum number of lower case letters each password must contain. The default is disabled and 0.
Must contain numbers	Enable the check box and select a value between 0 and 64 to specify the minimum number of numerals each password must contain. The default is disabled and 0.
Must contain symbols	Enable the check box and select a value between 0 and 64 to specify the minimum number of symbols each password must contain. The default is disabled and 0.

When assigning passwords to users, you can use the Random Password Generator to create passwords that satisfy all your criteria. After configuring the password characteristics, click **Generate**. The resulting password, which appears in the Random Password Generator text box, is now available for you to use.



After changing any password parameters, you must click **Save**. You will not be able to add users if you do not save first.

### Adding Basic Log-in Users

1. Click **Add**. The following dialog box appears.





2. In the Username text box, type the *user name* for new user.
3. In the Password text box, type the user's *password*, or copy it from the Random Password Generator.
4. In the Verify Password text box, retype the *password* you entered in the previous step.
5. Click **OK**.
6. Repeat Steps 1-5 for each user you want to add.
7. Click **Save**.

### **Changing a Basic User's Password**

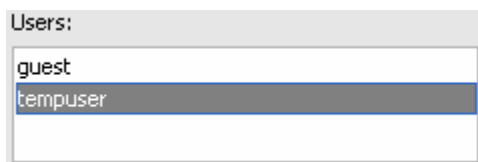
1. Click the **Basic** tab.
2. Select the user whose password you want to change.
3. Click **Set Password**.
4. Type the user's new *password* in the first text box.



5. Re-type the new password to verify that it is entered correctly.
6. Click **OK**.
7. Click **Save**.

### **Deleting a Basic User**

1. From the list of users under the **Basic** tab, select the user you want to delete.



2. Click **Remove**.
3. Click **Save**.

## ***Platform Log-in***

If this option is enabled, the user will be prompted to enter the same user name, password, and domain name that are used to access the system under Windows XP.

1. Click the **Platform** tab.



Basic \ Platform \ RADIUS \

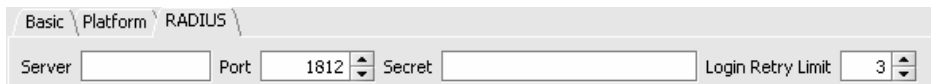
Default Domain

2. In the text box, type the name of the Windows *domain* that includes the users who should have access to the NetBeacon Element Manager.
3. Click **Save**.

## ***RADIUS Log-in***

The last option enables log-in authentication with a RADIUS server. The NetBeacon Element Manager is configured as a RADIUS client. To configure for RADIUS log-in, do the following:

1. Click the **RADIUS** tab.

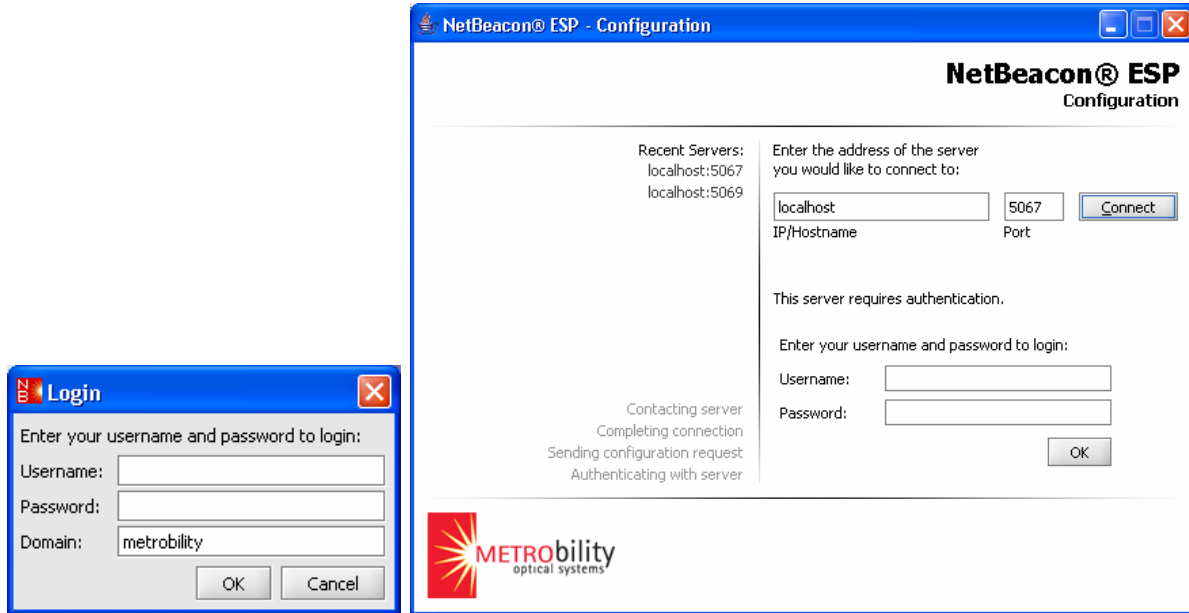


Basic \ Platform \ RADIUS \

Server  Port  Secret  Login Retry Limit

2. In the Server textbox, enter the *IP address* or *DNS name* of the RADIUS server.
3. Next, type the *port number* on which the RADIUS server is configured to communicate with NetBeacon. The valid range is 0 through 65535. The default is 1812.
4. In the Secret text box, type the *shared secret* associated with the RADIUS server.
5. To specify the maximum number of attempts to send a request to a RADIUS server without receiving a response, type the *number* in the Login Retry Limit text box. The range is 0 to 100. The default is 3 retries.
6. Click **Save**.

If you change the authentication mode to basic, Windows, or RADIUS, the next time a user attempts to connect to the NetBeacon Element Manager via the NetBeacon Admin Tool or the Element Browser, a login prompt, similar to the ones shown below, will appear. The smaller window appears when opening the NetBeacon Element Browser.



To connect successfully to the Element Manager, the user will have to enter a valid user name, domain name (Windows only), and password.

## Creating and Authorizing User Accounts

By default all users have full access to every manageable element. However, if you have enabled basic, platform, or RADIUS authentication under the Authentication tab, all users are denied access to elements by default. In order to create a secure network environment, you must give individual users read or write permission to various network elements, modules, or ports. You may also choose to deny them access to certain elements or components of an element. You can also enable or disable users from accessing the NetBeacon EM Admin Tool.

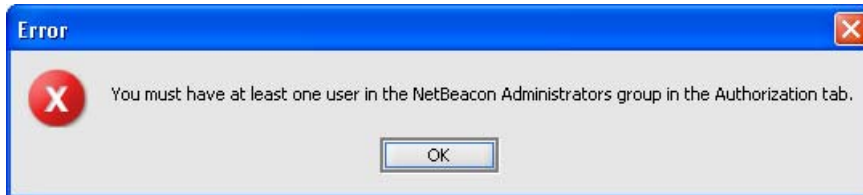
Each user must be unique, and may belong to only one group. Permissions may be applied to an individual user or to an entire group of users. To authorize user accounts, you must first create the user group structure. Once that is done, you can apply permissions to access the NetBeacon EM Admin Tool as well as the various network elements.

### *Creating Groups and Adding Users*

1. Click the **Authorization** tab in the NetBeacon Configuration window. The left panel displays your users and groups. The people icon (👤) represents a group of one or more users. The person icon (👤) represents a single user. The right panel displays items to which you can apply permissions. Under the `Permissions` folder are two folders labeled `Configuration` and `Domain Structure`. `Configuration` contains all the tabs available in the NetBeacon EM Admin Tool. `Domain Structure` contains the network element structure that was set up under the Organization tab.

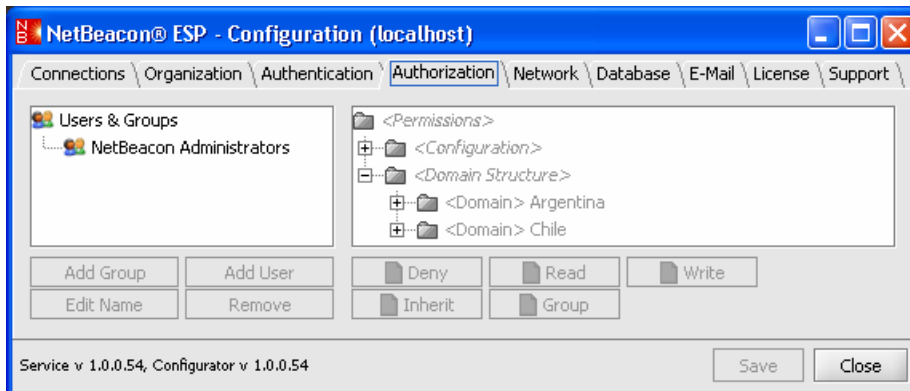
If this the first time you are creating user groups, the only item in the left panel will be the default groups labeled `Users & Groups` and under it the `NetBeacon Administrators`.

The default NetBeacon Administrators group has write access to all of NetBeacon (i.e., the entire `Configuration` and `Domain Structure`). You cannot change the name of the NetBeacon Administrators group or add other groups to it, however, you may add users to the group. If you have enabled basic, platform, or RADIUS authentication, at least one user must be assigned to the NetBeacon Administrators group. If you try to save without at least one user assigned to the NetBeacon Administrators group, the following error message will appear.

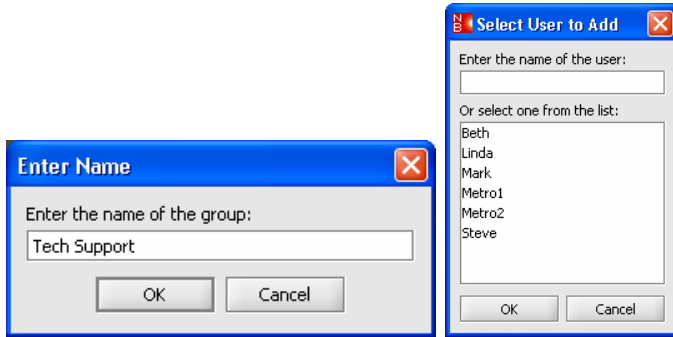


**IMPORTANT:** When the client authentication mode is set to basic, platform, or RADIUS, at least one user must be listed in the NetBeacon Administrators group. If you do not have a user in the group, all users will be locked out of NetBeacon.

When creating the user groups, you may want to organize users by their level of accessibility to network elements. For example, you could set up groups for network administrators with full access to all elements as well as the Admin Tool application; technicians with access to certain elements and read-only access to some tabs in the Admin Tool; and users with restricted access to only one element, module, or port and no access to the Admin Tool.



2. Select the group into which you want to add a new group or user. The NetBeacon EM Admin Tool uses a hierarchical structure, and you can only add new users or groups to an existing group, excluding the NetBeacon Administrators group, to which you can only add users.
3. Click **Add Group** or **Add User**. The Enter Name dialog box or the Select User to Add dialog box appears.

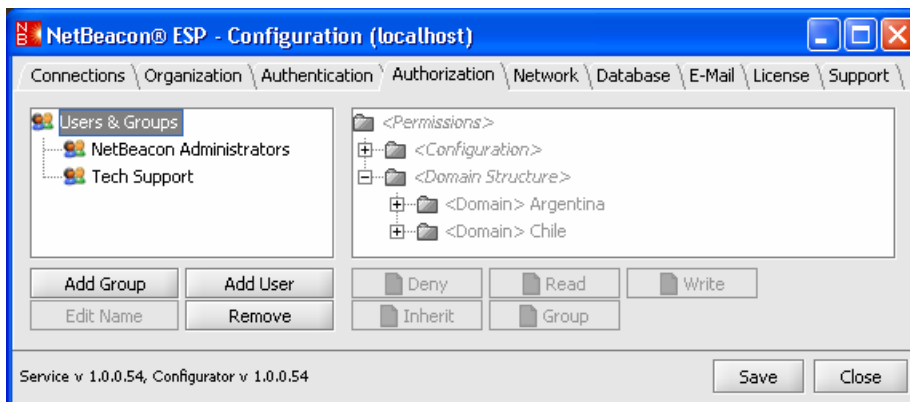


4. Type the *name* of the group or user in the text box. If you entered a list of user names under the Authentication tab, those names will appear in the bottom half of the Select User to Add dialog box and you may select one.

**Important:** User and group names must be unique.

**Tip:** Under Basic authentication mode, user names entered in this section must match the user names configured under the Authentication tab. Names are case-sensitive. Under Platform authentication mode, user names must include the domain. For example, you must enter the name as **user33@domain** instead of **user33**.

5. Click **OK**. The new group or user appears in the left panel under the selected group.



6. Repeat Steps 2 through 5 to create more groups or to add more users to a group.
7. Click **Save**.

### *Deleting Users or Groups*

1. Click the **Authorization** tab in the NetBeacon Configuration window.
2. In the left panel, select the group or user you want to delete. If you select a group, all users and subgroups within it will also be deleted.
3. Click **Remove**.

4. Click **Save**.

To delete all groups and any users associated with the groups, select **User & Groups** in the left panel, and click **Remove**. When the confirmation dialog box appears, click **Yes**.

### ***Renaming Users or Groups***

1. Click the **Authorization** tab in the NetBeacon Configuration window.
2. In the left panel, select the group or user you want to rename.
3. Click **Edit Name**.
4. In the text box, type the new user or group *name* you want to apply. Note that group and user names must be unique.
5. Click **OK**.
6. Click **Save**.

### ***Assigning Permissions***

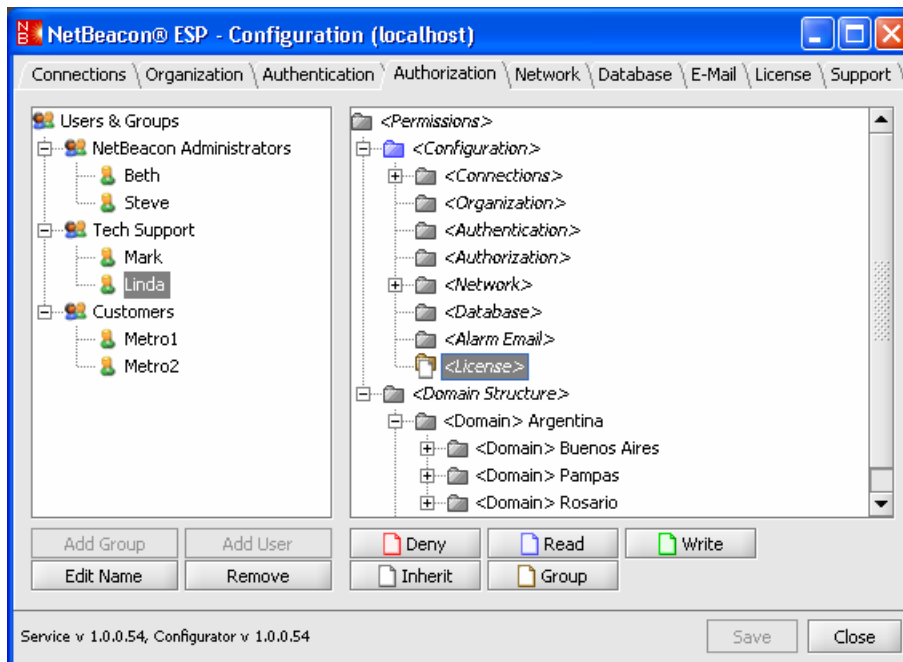
Once you have set up the user group structure, you are ready to assign permissions to individual users or to a group of users. Permissions are assigned by applying a color-coded label that indicates the access privilege. You may apply permissions to the NetBeacon EM Admin Tool and any of its tabs. You also may apply permissions to any element that has been added under the Organization tab. Additionally, you may apply permissions down to the port level for an element.

In the `Domain Structure`, each node may have only one label assigned to it for an individual user. That is, User A cannot have both Deny and Read access to Element X; it must be one or the other. However, an element may have different labels for different users. For example, User A may have Read access to Element X, while User B has Write access to Element X. The same rule applies to each node in the Configuration hierarchy.

A user's or group's permission may be one of the following options: deny, read, write, inherit, or group. Permissions are inherited from the top down. By default, users have full access to all elements and all Configuration tab fields when the authentication mode is set to None. When the authentication is set to basic, platform, or RADIUS, users in the NetBeacon Administrators group have full access to all elements and all Configuration tab fields, but users in all other groups are denied access to all elements and all Configuration tab fields, by default. Permissions may be overwritten. The permission options are described below.

- Deny: User is unable to view the selected component(s).
- Read: User may view characteristics for the selected component(s), but cannot change settings.
- Write: User has full access to the selected component(s) and can change software settings as well as view all settings.

- **Inherit:** Access to the selected component(s) is determined by the parent's access setting. The parent is the node one level above the component in the Permissions hierarchy. This is the default setting. For example, if the Browsers tab has Inherit permission, then its permission will depend on the permission of the Connections tab. So, if the Connections tab has Read permission, then the Browsers tab will also have Read permission.
- **Group:** Access to the selected component(s) is determined by the permission assigned to the group in which the user is a member. For example, if the License tab has Group permission for the user named Linda, who is a member of the group "Tech Support," then Linda's access to the License tab will depend on the permission of the Tech Support group. If the Tech Support group has Read permission for the License tab, then Linda will have Read permission.



1. Click the **Authorization** tab in the NetBeacon Configuration window.
2. From the left panel, choose the user or group to which you want to give permission to access one or more items in the right panel.
 

**Tip:** To select more than one user or group, hold down the CTRL key, and click on each individual or group you want to include. To select more than one user or group in a series, select the first user or group, hold down the SHIFT key, and click on the last user or group you want to include.
3. In the right panel, select Permissions, Configuration, Domain Structure, or any node(s) for which you want to specify permissions for the selected user(s) or group(s).
4. Click one of the five authorization buttons: **Deny**, **Read**, **Write**, **Inherit**, or **Group**. The privilege setting will be applied to the element or element node and everything below it.

The folder or file icon color changes to the option you selected. By default, all elements provide full read/write access to all users and groups.

Button Name	Description
Deny	Access to the selected component is denied. For example, if the component is a module, the module will appear as a blank slot in the chassis.
Read	The user or group is allowed to view settings for the component, but configuration changes are not allowed.
Write	The user or group is given full access to the selected component. Settings may be viewed and modified through the NetBeacon Element Browser.
Inherit	Access to the selected component is determined by the privilege of the parent's access setting. For example, if a module in Chassis A is given the Inherit status, access to the module will be the same as the user's access to Chassis A. This is the default setting.
Group	Access to the selected component is determined by the permission assigned to the group in which the user is a member. For example, if User A is a member of Group X , which has Read permission on Configuration, User A's access to the NetBeacon EM Admin Tool will also be Read.

- Repeat Steps 2-4 to apply permissions for any other users and groups.
- To change a group or user's access level, select the group/user and the node(s) you want to modify under the Permissions folder. Click **Deny**, **Read**, **Write**, **Inherit**, or **Group**. The folder or file icon color changes according to the new permission.

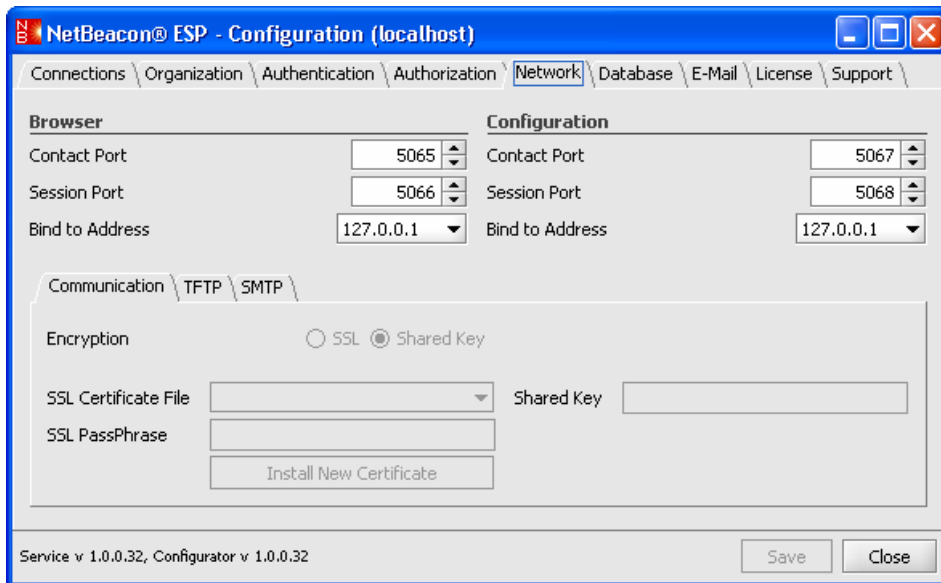
If you applied the permission to a group, all of its users and subgroups will now have the same permission.

- Click **Save**.



## Specifying Network Parameters

1. Click the **Network** tab in the NetBeacon Configuration window.



2. Specify the Element Browser communication characteristics.

- In the Contact Port text box, type the port *number* (between 0 and 65535) on which the Element Manager will listen for connections from the Element Browser application. The default is port 5065. The contact port is where two connecting components determine the session parameters such as the security mode, the session port number, etc. Once the session parameters are determined, all communications occur on the session port.
- In the Session Port text box, enter the port *number* (between 0 and 65535) on which the Element Manager and the Element Browser will exchange data. The default is port 5066.

**Important:** Make sure your firewall settings will allow NetBeacon to communicate through the contact and session ports you have specified.

- From the drop-down list choose the address to which the Element Manger server binds itself. By default, it binds to localhost, 127.0.0.1. When the default address is used, only Element Browsers on the local machine are given access to the Element Manager. To allow other Browser applications on the network to access the Element Manager, use the IP address option.

3. Specify the Element Manager Admin Tool communication characteristics.

- In the Contact Port text box, type the port *number* (between 0 and 65535) on which the Element Manager service will listen for connections from the Admin Tool application. The default is port 5067.

- In the Session Port text box, enter the port *number* (between 0 and 65535) on which the EM service and the Browser application will exchange data. The default is port 5068.
  - From the drop-down list choose the address to which the Element Manger server binds itself. By default, it binds to localhost, 127.0.0.1. When the default address is used, only Admin Tool applications on the local machine are given access to the Element Manager. To allow other Admin Tool applications on the network to access the Element Manager, use the IP address option.
4. To specify the security parameters for communications between the Element Manager and its client application:
- Select the **Communication** tab.
  - Select the encryption mode: **SSL** (Secure Sockets Layer) or **Shared Key**. The default is Shared Key.
  - If Shared Key encryption is selected, in the Shared Key text box, type the *key* that will be used by both the Element Manager and the client.
  - If SSL encryption is selected, choose a certificate from the SSL Certificate File drop-down menu. Type the new certificate's *password* in the SSL PassPhrase text box. Click **Install New Certificate**.
5. NetBeacon provides an internal TFTP server for providing firmware updates. To configure NetBeacon's TFTP server settings, do the following:
- Select the **TFTP** tab.

The screenshot shows a configuration window with three tabs: 'Communication', 'TFTP', and 'SMTP'. The 'TFTP' tab is selected. Inside the window, there are several settings:

- 'Enable Embedded Server': A radio button is selected for 'yes', and 'no' is unselected.
- 'Bind Address': A dropdown menu showing '172.18.1.44'.
- 'Alternate Server Address': A text box containing '172.18.1.44'.
- 'Port': A spinner box showing '69'.

- To enable NetBeacon as a TFTP server, select **yes**. From the Bind Address drop-down list, select one of the options. The default is 127.0.0.1 (localhost).
  - To specify an external TFTP server, select **no** for Enable Embedded Server. Type the external TFTP server's *IP address* in the Alternate Server Address text box. The default is 127.0.0.1 (localhost).
  - To specify the port on which the TFTP server will listen, enter the *port number* in the Port text box. The default is 69.
6. To configure the SMTP e-mail server settings for sending alarm notifications, do the following:
- Select the **SMTP** tab.

Communication \ TFTP \ SMTP \

From Address: NetBeacon@metroability.com    Authentication: none

Hostname: metroemailserver    Username: [ ]

Port: 25    Password: [ ]

Send Test E-mail

- In the From Address text box, enter the *e-mail address* of the sender of NetBeacon e-mail notices. Note that some e-mail servers require a valid e-mail address in this field.
- In the Hostname text box, enter the *IP address* or *DNS name* of the SMTP server.
- In the Port field, type the *port number* (between 0 and 65535) to which the SMTP server is connected. The default is 25.
- From the Authentication drop-down list, select the type of security required by your e-mail server. The available options are:
  - none: no authentication, no security
  - basic: authentication via username and password, no security
  - TLS: authentication via username and password, and transmission over a secure socket
- If basic or TLS authentication is selected, the last two fields will be specified. In the text boxes, enter the *user name* and *password* of a valid user of the e-mail server.

7. Click **Save**.

### *Sending a Test E-mail Message*

To verify your e-mail server settings, NetBeacon provides an option to send a sample e-mail message to an individual. Click **Send Test E-mail**. The following dialog box appears.

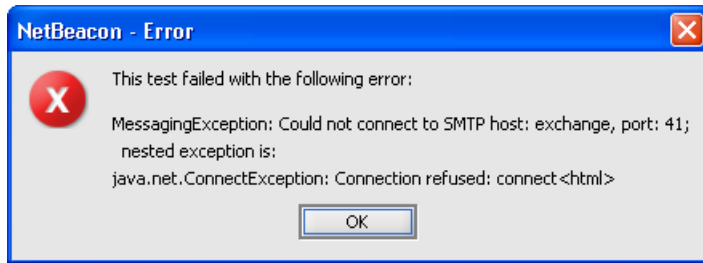
NetBeacon - E-mail Test

Please enter an e-mail address where the test e-mail will be sent.

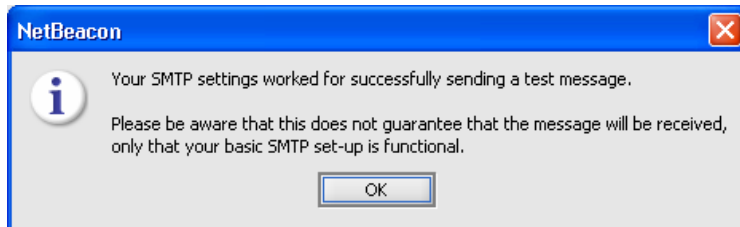
[ ]

OK    Cancel

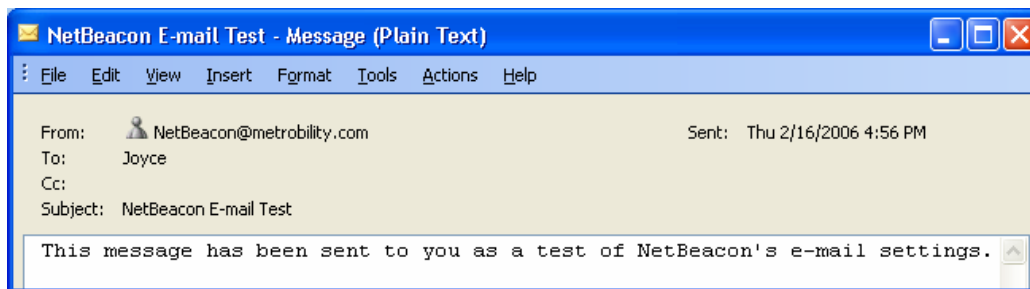
In the text box, type the *e-mail address* of the person who should receive the test message, then click **OK**. If your settings are set up incorrectly, an error message will appear.



If there are no problems with any of the settings, the following dialog box will appear.



The recipient will get an e-mail message, as shown below:



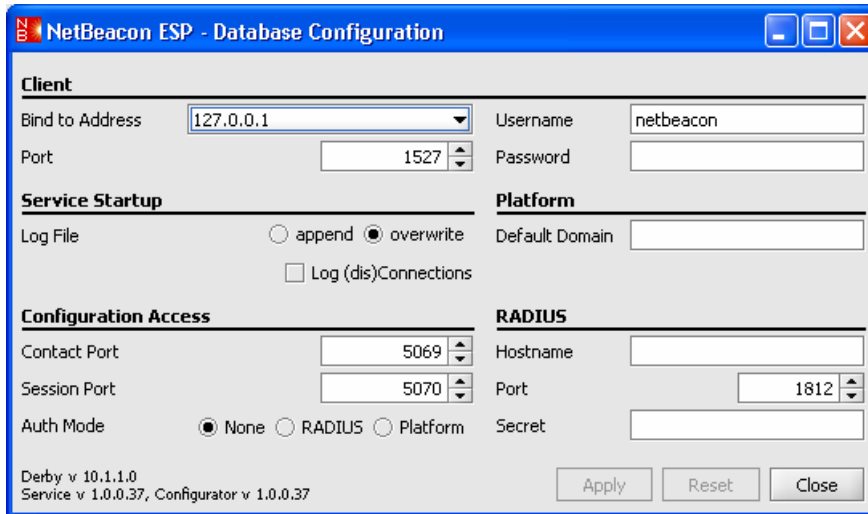
## Configuring the Database

**Important:** This section is only applicable if you have installed the Database component of NetBeacon.

With the Database service installed, NetBeacon provides several options that determine how and when data is logged for an element. The Database Service Admin Tool, an independent client application, allows you to set up the initial configuration to enable proper communication. After the initial setup, all database communications will be through the Element Manager Admin Tool or the Element Browser.

This section describes how to set up database management.

1. Open the Database Configuration window.



The following table lists the information shown in this window, along with a brief description of each field.

Name	Description
<b>Client</b>	The Database Service Admin Tool is a client application to the NetBeacon Database service.
Bind to Address	Address to which the Database server binds itself. By default, it binds to localhost, 127.0.0.1.
Port	Port number on which the Database server accepts connections. The default is 1527. Note that the Client Port number must differ from the Configuration Access Contact Port and Session Port numbers.
Username	User name that the client application uses to authenticate itself to the NetBeacon Database service. The default user name is netbeacon.
Password	Password that the client application uses to authenticate itself to the Database service. The password is encrypted and the field always appears blank. The default password is netbeacon.
<b>Service Startup</b>	Start-up characteristics of the Database service.
Log File	Select <b>overwrite</b> to start a new file, which will log all Database activity. Select <b>append</b> to add onto the existing file without destroying any previous data. By default, the file is overwritten whenever the Database Admin Tool is run.
Log (dis)Connections	Indicates whether or not all connections and disconnections to the Database are being logged in a file called <code>derby.log</code> .
<b>Configuration Access</b>	Communication and security parameters of the Database service.

Name	Description
Contact Port	Port on which the Database service listens for connections from the Database client application. The default is port 5069. Note that this port number must differ from the Client Port number and the Configuration Access Session Port number.
Session Port	Port on which the Database service transfers data to the Database client application. The default is port 5070. Note that this port number must differ from the Client Port number and the Configuration Access Contact Port number.
Auth Mode	Authentication mode used to verify the database client application with the database service. By default, no authentication is used. The Database service supports RADIUS and Platform authentication, but not basic (i.e., a list of user names and passwords).
<b>Platform</b>	Log-in characteristic when platform (i.e., Windows XP) authentication is specified.
Default Domain	Name of the Windows XP domain that includes users who should have access to the NetBeacon Database.
<b>RADIUS</b>	Log-in characteristics when RADIUS authentication is specified.
Hostname	IP address or DNS name of the RADIUS server.
Port	Port number on which the RADIUS server is configured to communicate with NetBeacon. The range is 0 through 65535; default is 1812.
Secret	Shared secret associated with the RADIUS server.

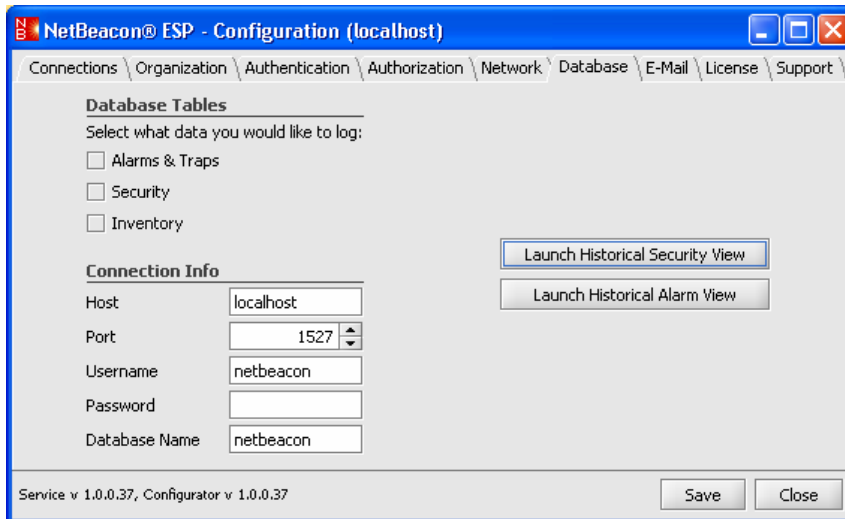
- In the Bind to Address text box, choose the address to which the Database server should bind itself. By default, it binds to the local host, 127.0.0.1. When the default address is used, only the Element Manager and Database Service Admin Tool applications on the local machine are given access to the Database service. Select the system's IP address if you want other users on the network to be able to access the Database service.
- In the Port text box, type the port *number* (between 0 and 65535) on which the Database server should listen for connections. The default is 1527.
- In the Username text box, type the *user name* that the client application should use to authenticate itself to the Database service. The default user name is netbeacon.
- Type the *password* that the client application should use to authenticate itself to the Database service, in the Password text box. The password is encrypted and the field always appears blank, except when you are typing the password. The default password is netbeacon.
- Specify how you want the Log File written. Select **append** to add onto the existing file. Select **overwrite** if you want to create a new file or override an existing file called `derby.log`, which will log all Database activity. The default setting is overwrite.

7. Select the Log (dis)Connections check box if you want to record all connections and disconnections to the Database. The connections and disconnections will be logged in a file called `derby.log`.
8. In the Contact Port text box, type the port *number* (between 0 and 65535) on which the Database service will listen for connections from the Database Service Admin Tool. The default is port 5069.
9. In the Session Port text box, enter the port *number* on which the Database service will transfer information to the Database client application. The default is port 5070, and the acceptable range is between 0 and 65535. You may want to modify the session port if you are using a firewall.
10. Specify the authentication mode: **None**, **RADIUS**, or **Platform**. The default is none, no authentication.
11. If you specified Platform in Step 10, enter the Windows XP *domain name* in the Default Domain text box.
12. If you specified RADIUS in Step 10, enter the RADIUS settings:
  - Type the *IP address* or *DNS name* of the RADIUS server in the Hostname text box.
  - Type the *port number* which the RADIUS server is configured to communicate with NetBeacon. The range is 0 through 65535; default is 1812.
  - Type the *password* associated with the RADIUS server in the Secret text box.
13. Click **Apply** to save your change(s), click **Reset** to restore all modifications to their original values, or click **Close** to exit the Database Service Admin Tool application without saving your change(s).

### ***Creating a Database File***

To create a named database which contains information from tables you select, do the following:

1. Open the NetBeacon Configuration window and select the **Database** tab.



## 2. NetBeacon provides three types of database tables:

- **Alarms & Traps:** The Alarms & Traps table is a record of all SNMP trap notifications, related alarms, and events. This database logs the date and time the event occurred and its severity. If the alarm was acknowledged, it includes the date and time it was acknowledged, along with the user who acknowledged it. If the alarm was resolved, the date and time of resolution is included. The DNS name or IP address of the element where the event occurred and a description of the alarm are also included in the database.
- **Security:** This database table logs the date and time of each user connection and disconnection, the user's name and address, the application to which the user connected, and the version of the user's software. The table also includes the number of login failures that occurred, if any.
- **Inventory:** This table contains the date and time when the information was first recorded, the serial number and model of the element, the date the element was manufactured, its location, type, description, name, and additional element-specific information. The table also includes whether or not an element is in service.

Click in the check box for the table(s) you want to include in the database.

3. In the Host text box, enter the *IP address* or *DNS name* of the Database server. The default is localhost.
4. In the Port text box, enter the *port number* on which the Database server accepts connections. The default is 1527.
5. In the Username text box, type the *user name* that the Element Manager should use to authenticate itself to the Database server. The default user name is netbeacon.
6. In the Password text box, type the *password* that the Element Manager should use to authenticate itself to the Database server. The password is encrypted and the field



always appears blank, except when you are typing the password. The default password is netbeacon.

7. In the Database Name text box, type the *name* to apply to the of database file. The default name is netbeacon.
8. Click **Save**.

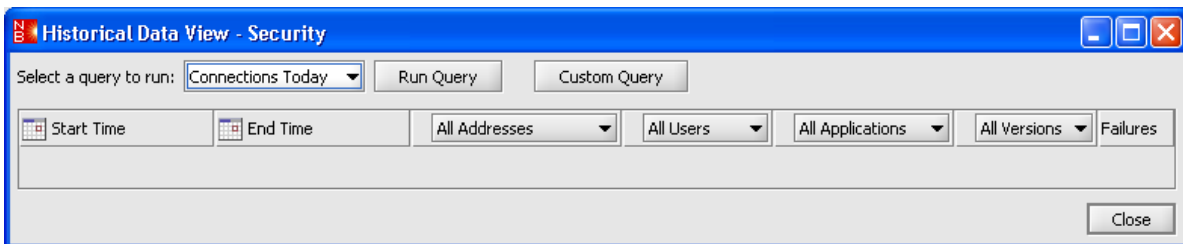
There are two additional buttons that will allow you to view the Security table and the Alarms & Traps database table. The Alarms & Traps database is described in [Viewing Historical Data](#).

### Viewing Historical Security Information

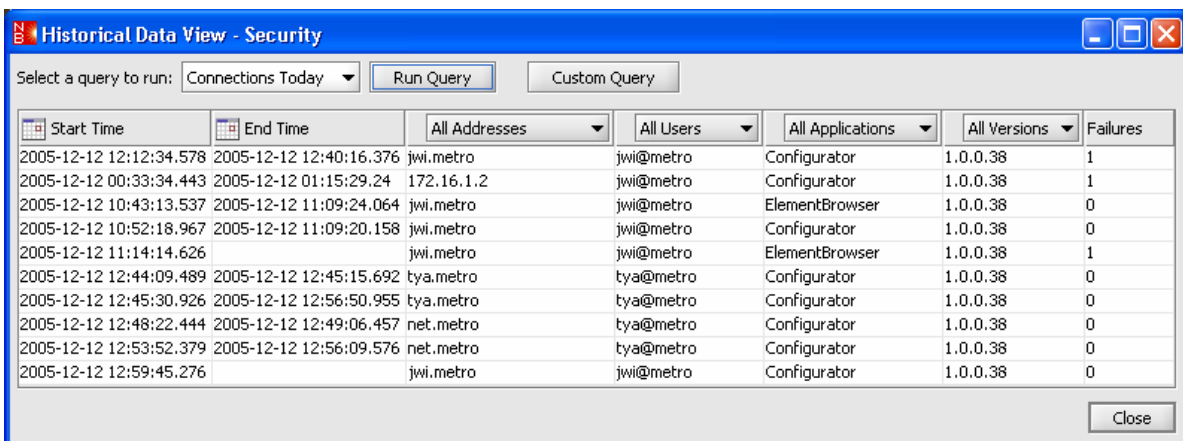
NetBeacon provides an option to view historical information regarding security by running a standard SQL query or a customized query.

To run a standard SQL query to view the security database table, do the following:

1. Click **Launch Historical Security View**.



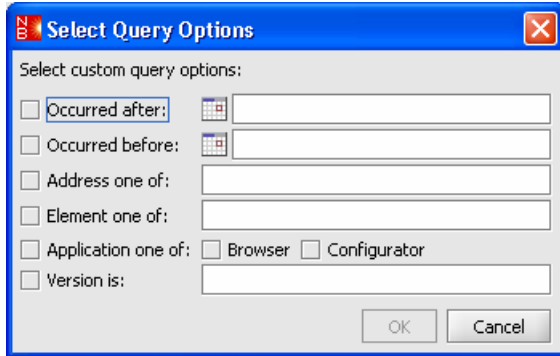
2. From the 'Select a query to run' drop-down list, select **Connections Today** if you want to see all login for the current date, or select **Current Connections** if you want to see all login information that are currently active.
3. Click **Run Query**. The security database table appears in the window, as shown in the example below.




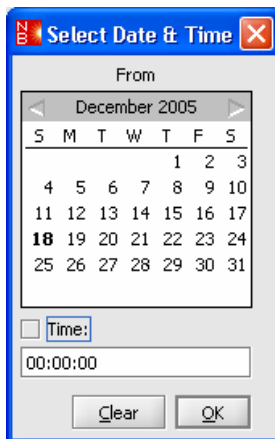
## Running a Custom Security Query

To run a customized SQL query in which you specify more detailed information about the security settings, do the following:

1. In the Historical Data View window, click **Custom Query**. The Select Query Options dialog box appears.



2. For each text box with a calendar icon , click on the icon to select a date and time to specify the start and end of the period when the login connections occurred. If dates are not specified, the query will include all dates. In the Select Date & Time dialog box, the current date is shown in bold text. Use the forward and reverse arrows to change the month displayed.



Do any of the following:

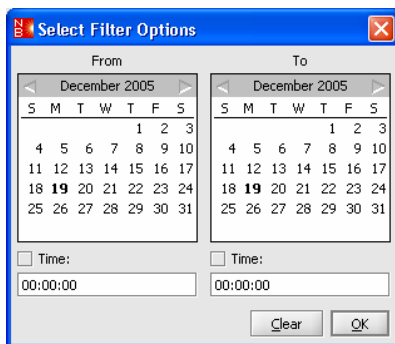
- Click on a *date* to select it. The selection will be underlined.
- To specify a time, select the Time check box and enter the *start time* or *stop time*. This is optional.
- If you make a mistake, click **Clear** to reset the settings.
- Click **OK** when the date and time are properly configured. The date and the time will appear in the text box in the Select Query Options dialog box.

3. In the 'Address one of' text box, type the *DNS name* or *IP address* of each element you want to include in the query. Separate each entry with a comma. If this text box is empty, the query will include login connections to all elements.
4. In the 'User one of' text box, type the *user name(s)* of the people who logged in. Separate each user name with a comma. If this text box is empty, the query will include connections by all users.
5. To include only the NetBeacon Element Browser in the query, check **Browser**. To include only the NetBeacon Element Manager Admin Tool, check **Configurator**. If no applications are checked, the query will include both applications.
6. In the Version text box, type the *version number* of the NetBeacon application. If this text box is empty, the query will include all versions.
7. Click **OK**. The customized information appears in the Historical Data View window.

### Filtering the Database Tables

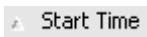
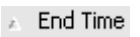
After running the SQL query, you can modify and filter the information that is displayed by using the buttons at the top of each column.

1. To filter the start and end times, click on the calendar icon .



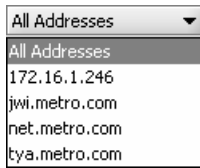
The current date is shown in bold text. Click a *date* to select it. The selection will be underlined. Check the Time check box, and enter the *start time* and *stop time*. Click **Clear** if make a mistake and want to reset the settings. When the date and time are properly set, click **OK**.

2. Click **Start Time** or **End Time** to view the entries in chronological order or reverse chronological. A little arrowhead that points up or down indicates the order.

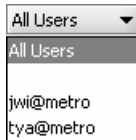
 **Start Time**  **End Time** = chronological order

 **Start Time**  **End Time** = reverse chronological order

3. To view logins related to one address, select it from the address drop-down list.



4. To view logins by a specific user, select the username from the drop-down list.



5. To view entries for only the Element Browser or the Admin Tool, select it from the Applications drop-down list.
6. If multiple versions of NetBeacon are included in the table, you can filter them using the Versions drop-down list.

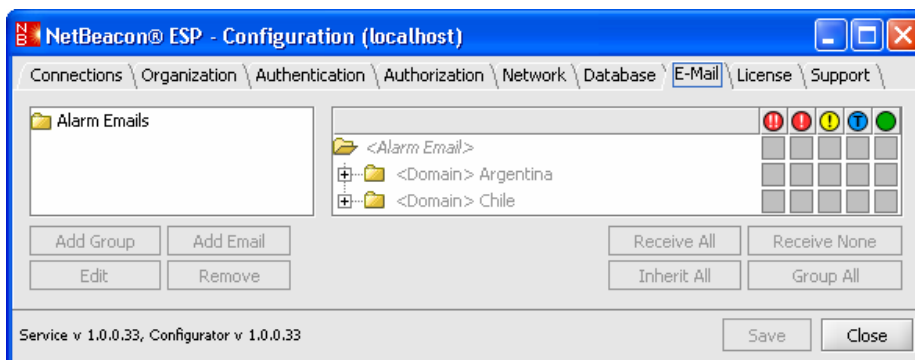
## Sending E-Mail Notifications

You can customize NetBeacon to send automatic e-mail notifications to one or more recipients when certain events occur.

### *Configuring E-Mail Recipients*

To create a list of e-mail recipients, do the following:

1. Click the **E-Mail** tab.



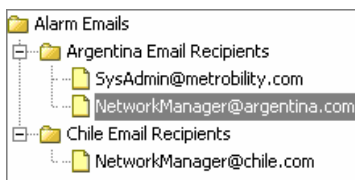
2. In the left panel, select **Alarm Emails**.
3. If you want to organize your recipients into one or more groups, follow the steps below. Note that it is not necessary to place e-mail recipients into groups.
  - Click **Add Group**.
  - Type the *name* of the group in the text box.

- Click **OK**
4. To enter the e-mail address of the recipient of alarm notifications, follow the steps:
    - Select the group into which the recipient is a member. (Optional)
    - Click **Add Email**.
    - In the text box, type the recipient's *e-mail address*.
    - Click **OK**.
  5. To change the name of a group, or to change an e-mail address, select the group or address, click **Edit**, enter the new name or new e-mail address, and click **OK**.
  6. To delete a group of e-mail recipients or an individual recipient, select the unwanted group or e-mail address from the left panel, and click **Remove**. To delete all groups and users, select **Alarm Emails**, click **Remove**, and then click **Yes** when the confirmation dialog appears.
  7. Click **Save**.

### *Customizing Alarms for Recipients*

By default, all alarms are disabled. To customize the types of alarms and traps that a group or individual will or will not receive, do the following:

1. From the left panel, select the group(s) or individual(s) who will be receiving e-mail.



2. The right panel displays Alarm Email folder, which is the domain structure that you configured under the Organization tab. Here, you will select the domain, element, chassis, module, or port from which you want the e-mail recipient to receive trap or alarm notifications.

The following table describes the alarm icons shown in this panel. The icons are displayed in order of decreasing severity from left to right.

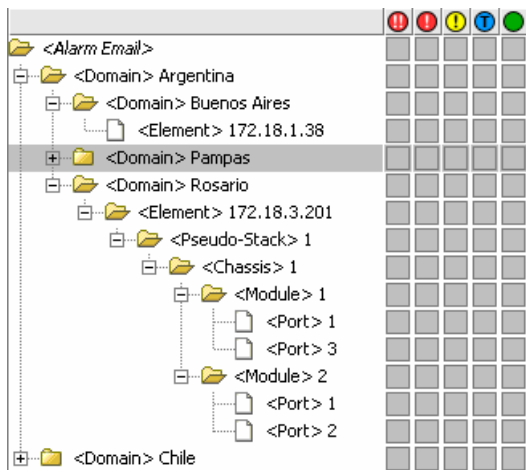
Icon	Name	Description
	Critical Alarm	Critical alarms require immediate attention. They include conditions such as loss of communication with an element.
	Major Alarm	Major alarms are serious conditions that may indicate some type of failure or that may result in network disruption. Major alarms are sent under conditions such as when the power supply goes above or below the acceptable voltage

Icon	Name	Description
		range, or when a module is removed from or inserted into a chassis.
!	Minor Alarm	Minor alarms do not require urgent attention, but should be checked before a more serious problem occurs. An example of a minor alarm is a loss of link on a redundant port.
T	Trap	An SNMP trap. Some traps can be raised to an alarm. For example, if link is down and it remains down for 2.5 seconds, the link down trap becomes an alarm. Some traps can indicate the resolution of an alarm. For example, if link is up and remains up for 10 seconds after the link up trap occurs, the alarm will be resolved. Some traps are simply informative.
●	Report	An informational message that requires no action. Usually indicates an alarm condition has been resolved. To resolve most alarms, the entity must remain in the resolved state for at least 10 seconds.

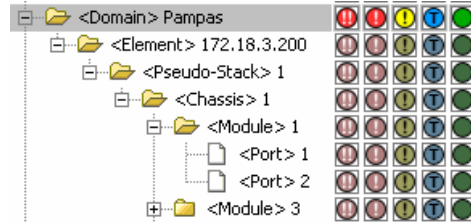
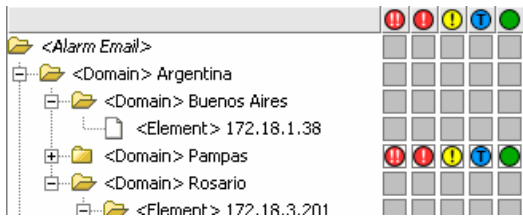
**Tip:** NetBeacon provides a ToolTip, such as the one shown below, for each check box to explain the current setting.

Minor alarms are NOT being received for this object.

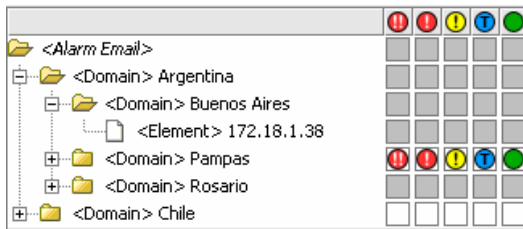
In the right panel, select the domain(s) or element(s) from which the selected recipient should get alarm notifications. You can also choose any node within the element down to the port level. By default, all alarms are inherited (gray). This means that if Major Alarms are enabled for a domain, then Major Alarms for all elements, chassis, modules, and ports within that domain will also be enabled.



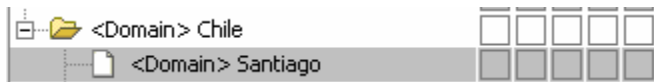
- Click **Receive All** to allow all alarms from the selected node to be sent to the recipient. The gray check boxes now display color-coded icons for the node. In the following example, the Pampas domain was the selected node. The recipient will receive all minor, major, and critical alarms as well as all traps and reports from everything within the Pampas domain. Expand the view under the Pampas and you can see that each node below it is now enabled. The icons are a lighter shade than the Pampas color, indicating that they are inherited from the parent.



4. Select a node and click **Receive None** to prevent sending any messages from the node to the recipient. The check boxes appear white, as shown in the following example in which the Chile domain was the selected node.

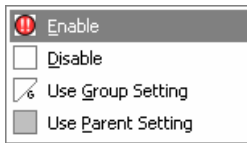


5. Select a node and click **Inherit All** to enable e-mail alarms and traps based on the setting of the parent node. Example: The parent node is domain Chile and the selected node is the domain Santiago. If Chile is configured to send no alarms to the recipient, Santiago will not send any alarms too. If Chile is configured to send only Minor Alarms, Santiago will also send only Minor Alarms to the recipient.



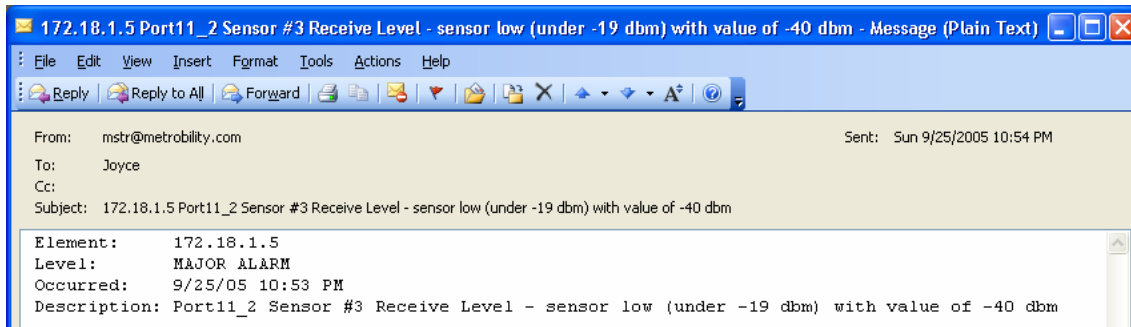
6. Select a node and click **Group All** to enable/disable e-mail alarms based on the recipient's group setting. That is, if the group in which the recipient is a member receives no alarms from the selected node, the recipient will also receive no alarms from that node.
7. In addition to enabling/disabling all or no alarms and traps for a selected node, you can configure a single alarm or trap. To change an individual alarm/trap setting, do one of the following:

- Click on the icon or check box until the desired setting is achieved.
- Point the cursor at the icon or check box, then right-click on the mouse. When the pop-up box appears, select one of the options:
  - Enable** – sends the alarm/trap to the recipient.
  - Disable** – does not send any alarm e-mails to the recipient.
  - Use Group Setting** – e-mail notification depends on the setting of the group in which the recipient is a member. For example, if the trap/alarm is disabled for the group, the recipient will not receive any e-mail.
  - Use Parent Setting** – e-mail notification depends on the setting of the node's parent. If the node's parent is enabled to send the trap/alarm to the recipient, the recipient will also receive alarms/traps from the node.



8. Click **Save**.

Below is an example of an e-mail notice sent by NetBeacon.



The following table describes the information included in each e-mail alarm notice.

Name	Description
Element	The IP address or DNS name of the element where the alarm occurred.
Level	The severity of the alarm: minor, major, or critical.
Occurred	The date and time when the alarm was recorded by the system monitoring elements.
Description	A description of the alarm.

To prevent users from receiving numerous repetitive e-mail messages at very high rates, NetBeacon includes automatic e-mail flood suppression. After an alarm for which an e-mail should be generated occurs, NetBeacon waits up to 30 seconds for subsequent alarms for the same element and e-mail address. All subsequent alarms are bundled into one combined e-mail message.

Once an alarm e-mail has been sent, NetBeacon will not send an alarm to the same user regarding the same element until five minutes have passed, at which time the user will receive an e-mail message containing all alarms for the last five minutes for the given element, if any alarms for that element have occurred.

## Entering the NetBeacon License

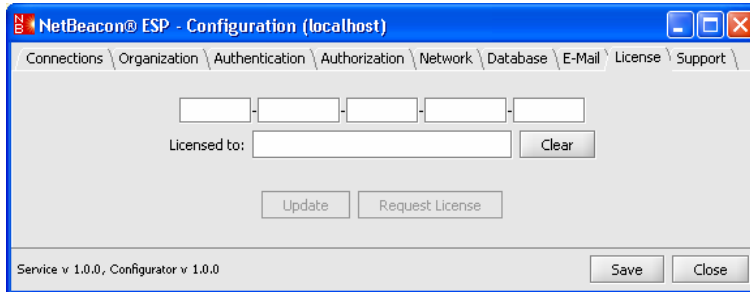
To use NetBeacon, you must register your software by contacting Metrobility to obtain a license key code.



**Important:** You will be unable to connect any Element Browsers to the Element Manager if a valid license is not entered.

### ***Requesting a NetBeacon License Key***

1. Click the **License** tab in the NetBeacon Configuration window.



2. Click **Request License**.

### ***Entering the NetBeacon License***

After you receive your license key, follow the steps below to register your software.

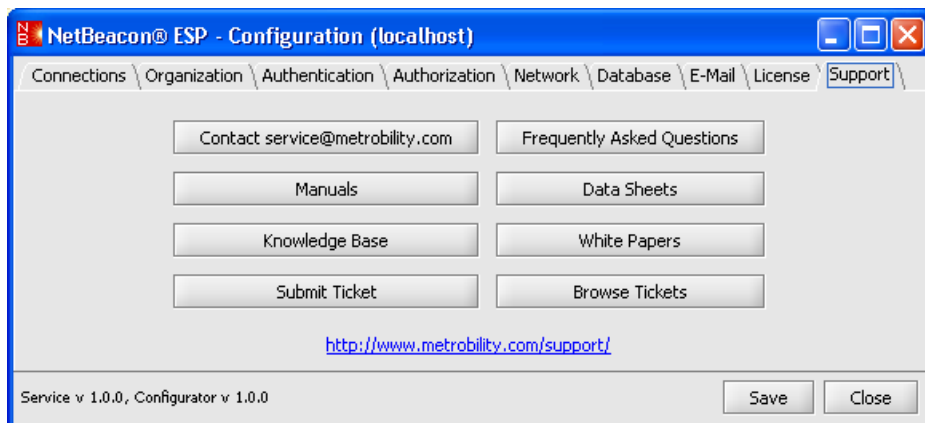
1. Click the **License** tab in the NetBeacon Configuration window.
2. In the set of five text boxes, enter your *license key code*.

**Tip:** You may copy the code from the e-mail you received from Metrobility and paste it into the first text box. The license will fill all five text boxes.

3. Enter a *name* in the Licensed to textbox. (Optional)
4. Click **Clear** if you make an error and want to empty all text boxes.
5. Click **Save**.

## **Seeking Metrobility Support**

Metrobility maintains an interactive, user-friendly, and up-to-date website to assist you in locating technical information, solving problems, or answering questions. If you want more information or help regarding any Metrobility product, click the **Support** tab in the NetBeacon Configuration window. Under the tab, you will find several buttons and a link.

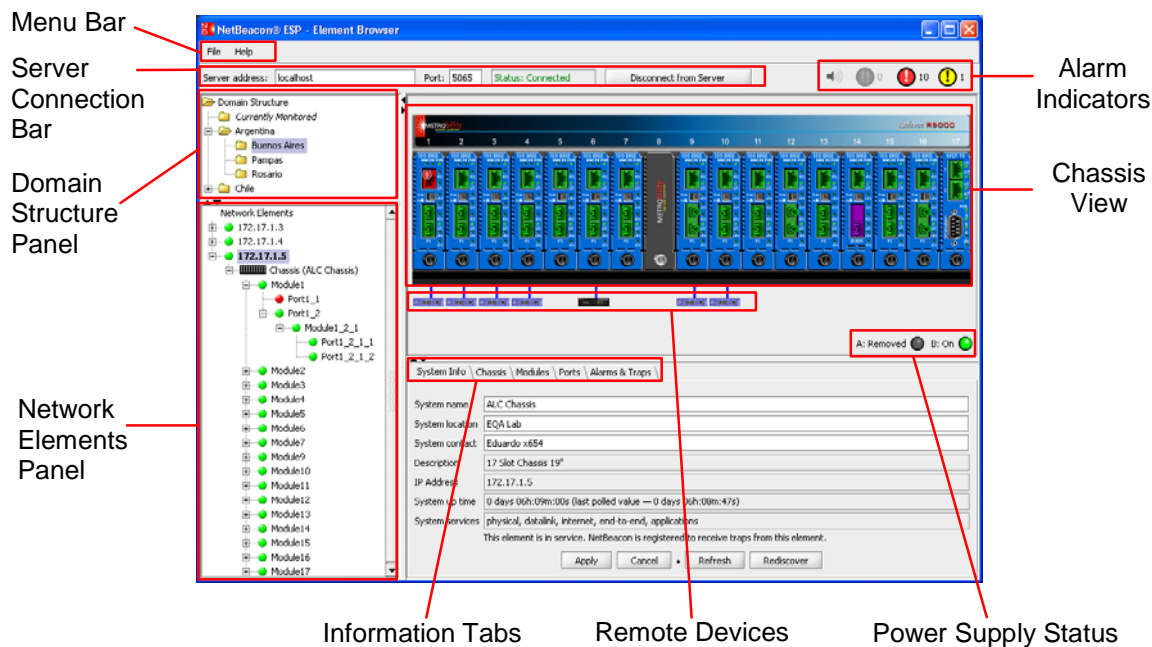


Click any of the buttons or hyperlink for support.

Button or Link	Description
Contact service@metroability.com	Send an e-mail to a Metrobility customer service representative.
Manuals	Download the most recent version of our hardware or software user guides.
Knowledge Base	Search our knowledge database for various product solutions.
Submit Ticket	Report a problem or ask a question to someone in our technical support or customer service department.
Frequently Asked Questions	Download documents from our technical reference library.
Data Sheets	Download data sheets for any Metrobility product.
White Papers	Download our latest white papers.
Browse Tickets	View the status of your trouble ticket, create a new ticket, or respond to an existing one.
<a href="http://www.metroability.com/support/">http://www.metroability.com/support/</a>	Go to Metrobility's Support Helpdesk and choose any of the topics.

## Chapter 4. Learning about the NetBeacon Element Browser Window

The NetBeacon Element Browser window is comprised of four panels. The upper left panel displays the Domain Structure managed by the NetBeacon Element Manager. When you select a domain from this panel, its elements are displayed below in the Network Elements panel. The upper right panel graphically shows the device selected from the Network Elements panel. The lower right panel uses a set of tabs which provide detailed information about the selected element. In addition to the visual displays, the Element Browser includes an audible alarm indicator to alert a network administrator about certain alarm condition.



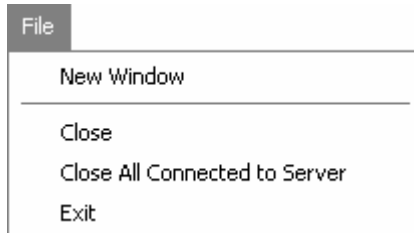
### Resizing the Windows and Dialog Boxes

You can minimize, maximize, resize, and position most of NetBeacon's windows and dialog boxes. Each dialog box also appears as an item in the taskbar. In the NetBeacon Element Browser and Configuration windows, you can resize any of the panels and table columns to enlarge or reduce the viewing area by clicking on the dividers between the panels and dragging them to the desired position. You may also move table columns to the left or right by clicking in column heading and dragging the entire column to the new position. Use the scroll bars to move either vertically or horizontally across a panel.

## Menu Bar

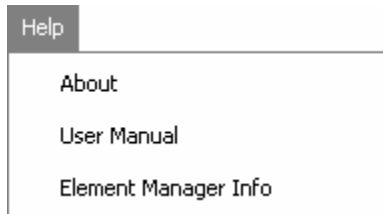
There are two drop-down menus, which you access from the menu bar. This section describes each menu option.

### *File Menu*



Option	Use this option to:
New Window	Open a new, empty NetBeacon Element Browser window.
Close	Close the selected NetBeacon Element Browser window. Other Element Browser windows will remain open.
Close All Connected to Server	Close all Element Browser windows (opened via File>New) connected to the specified Element Manager server. If there are any Element Browser windows connected to other servers, those windows will remain open.
Exit	Close all Element Browser windows (opened via File>New) connected to all Element Manager servers. Element Browser windows opened through other means will remain open.

### *Help Menu*



Option	Use this option to:
About	Display the software version number of the NetBeacon Element Browser application. (See <a href="#">Checking the NetBeacon Version Number.</a> )
User Manual	Display this user's guide in PDF format. You must have the Adobe Acrobat Reader installed to view this guide.
Element Manager Info	Display the version number of the NetBeacon Element Manager. (See <a href="#">Checking the NetBeacon Version Number.</a> )

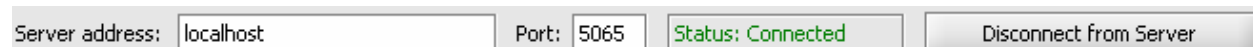
## Shortcut Keys

The following table lists the shortcut keys supported by the NetBeacon Element Browser.

Option	Shortcut Keys
Exit NetBeacon Element Browser	ALT+F4
Cut	CTRL+X
Copy	CTRL+C
Paste	CTRL+V

## Server Connection Bar

The server connection bar displays the IP address or DNS name of the NetBeacon Element Manager and the port number through which communications are occurring. The status of the connection to the Element Manager is also displayed. Depending on the current status, the button on the far right, gives you the option to connect to or disconnect from the server.



## Alarm Indicators

Whenever alarm conditions occur on any of the elements you are monitoring, even those that are not currently in view, NetBeacon alerts you audibly with a beeping sound. Three types of alarm severities are reported by different sounds – the more severe the alarm is, the faster and higher in pitch its tone will be. There is also an option to mute audio alarms.



Click to activate or mute audio alarms. The image is dimmed when sounds are muted.



Indicates the number of critical alarms recorded by NetBeacon. Flashing icon indicates at least one critical alarm has not been either acknowledged or resolved. This example indicates there is one critical alarm.



Indicates the number of major alarms recorded by NetBeacon. Flashing icon indicates at least one major alarm has not been either acknowledged or resolved. This example indicates 55 major alarms.



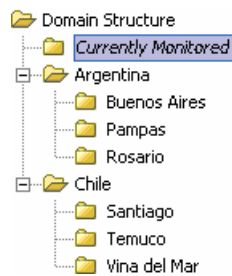
Indicate the number of minor alarms recorded by NetBeacon. Flashing icon indicates at least one minor alarm has not been either acknowledged or resolved. This example indicates 7 minor alarms

In addition to audible alerts, NetBeacon provides several visual alarm indicators. The alarm icons in the upper left corner change from gray to red or yellow and begin flashing as soon

as an alarm condition occurs. In the chassis view, a color-coded alarm icon flashes in the upper left corner of the chassis, module, port, or front-facing power supply, where the event occurred. Alarms are not displayed on remote units or rear-facing power supplies. Additionally, the name of the domain in the Domain Structure panel, up to the highest level domain, flashes in red text. In the Network Elements panel, the IP address or DNS name of the element also flashes in red text. Each node of the tree, down to the actual port or module which recorded the problem, also flashes in red. Icons remain flashing until they are acknowledged or resolved. To view a listing of all recorded alarm and trap events, click the **Alarms & Traps** tab. Double-clicking on an alarm icon in the chassis view automatically opens the Alarms & Traps tab, if it is not already active, and the alarm is highlighted. Refer to [Chapter 8. Monitoring Traps and Alarms](#) for further information.

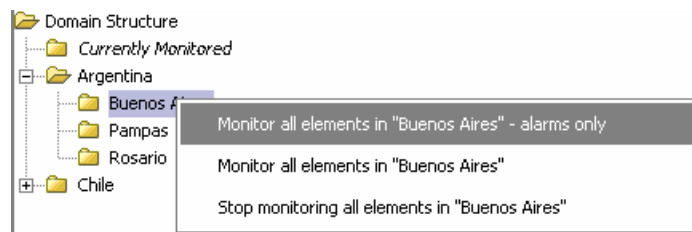
## Domain Structure

When you configured the NetBeacon Element Manager, you added each element you want to manage into a hierarchical structure. In the NetBeacon Element Browser, the Domain Structure panel displays that hierarchy. When you select a domain from this panel, all the elements within it are displayed in the Network Elements panel located directly below. In the example shown below, if *Argentina* is selected, all the elements in the *Buenos Aires*, *Pampas*, and *Rosario* directories will be displayed in the Network Elements panel. If *Buenos Aires* is selected, only the elements in the *Buenos Aires* directory will be shown in the Network Elements panel.



Within the Domain Structure is one named *Currently Monitored*. This domain contains a list of the all network elements that have been selected for monitoring by the Element Browser thus far. The list grows continuously as you select elements from the various domains.

You can right click on any domain to open a pop-up menu that allows you to monitor or stop monitoring all elements in that domain. There is also an option to monitor the domain's elements for alarm conditions only. Click on the menu option to select it.

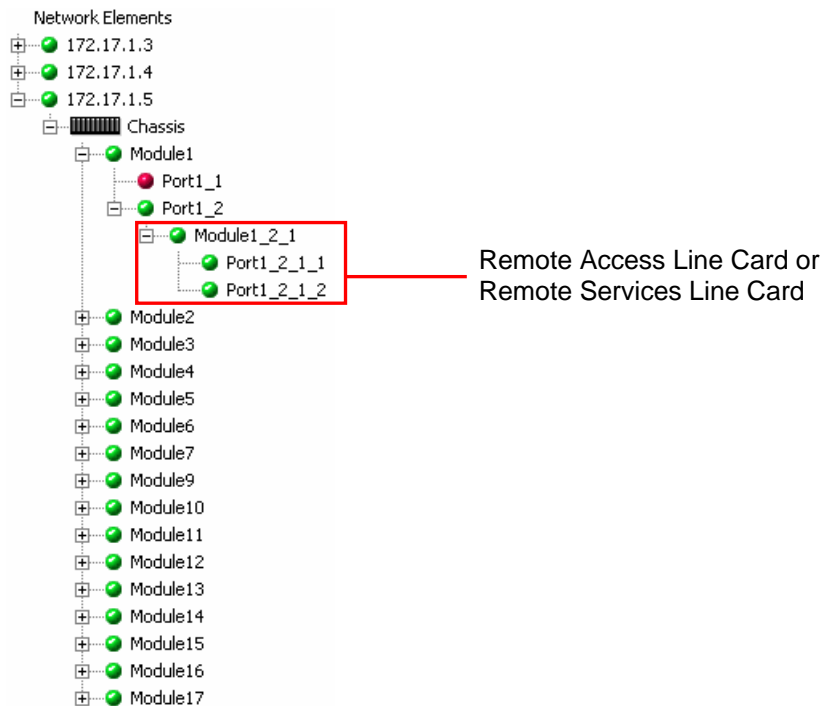




## Network Elements

When a folder in the Domain Structure is selected, its contents are displayed in the Network Elements panel. The element you select from the Network Elements list is presented graphically in the chassis view, and the information tabs below the image contain details related to the element. The selected element is highlighted.

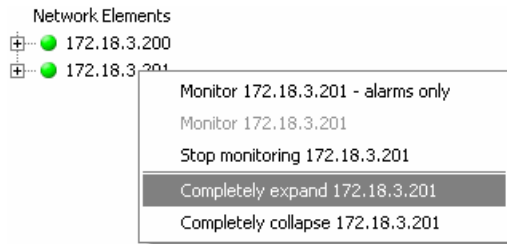
### *Expanding and Collapsing the Network Elements List*

You can expand the list of network elements so that the modules and ports associated with those elements are displayed. The expanded list will include any remote access or services line cards that are part of the element. If the element consists of a stack of two or more chassis, you will be able to see each chassis, its modules, ports, and remote units.



Click  or  to collapse or expand a particular node in the tree. To see all of an element's components, do the following:

- Select the element from the Network Elements panel.
- Right click to open the pop-up menu.
- Select **Completely expand** as shown below.







- Select **Completely collapse** to minimize the view.







The Network Elements pop-up menu options are described in the following table.

Menu Option	Description
Monitor – alarms only	Unmanage the element, but allow NetBeacon to receive and report traps and alarms.
Stop monitoring	Unmanage the element.
Monitor	Fully manage the element.
Completely expand	Display all nodes for the element in the Network Elements panel, including remote units connected to any of the ports.
Completely collapse	Minimize the view displayed in the Network Elements panel. Only the IP address or DNS name will be shown if this option is selected.

The Element Browser uses colored bullets to represent the status of the elements, modules, and ports. When you expand the Network Elements list, a chassis icon appears. To monitor the port status on a device in the Network Elements list, expand the view to the port level.

-  A green bullet can indicate any of the following:
  - Element is being managed by the NetBeacon.
  - The module has passed diagnostics and is functioning.
  - Port link is up.
-  A red bullet can indicate any of the following:
  - NetBeacon is unable to reach the element or has lost communications with the device.
  - The module has failed diagnostics.
  - Port link is down.
-  A blue bullet indicates the port has been administratively disabled, or NetBeacon is only monitoring the element for alarms and traps.
-  A purple bullet indicates the port is administratively disabled and the port has a fault, such as no link or Far End Fault.



-  An orange bullet indicates a signal has been detected on the port, but a link could not be established (e.g., there is a speed mismatch).
-  A yellow bullet indicates a Far End Fault condition has occurred on the port.
-  A white bullet indicates the element is available, but it is not selected.
-  A gray bullet indicates link status is unknown or not applicable to the port (e.g., it is a serial port).
-  A flashing bullet indicates that the NetBeacon is attempting to reach the element. The alternating colors will vary, depending on its current status.
-  A Metrobility device (e.g., chassis, services line card).

## Chassis View

NetBeacon provides a dynamic graphical display of the selected element, showing the complete front view of the device. Each line card is accurately displayed with all ports, switches, labels, and LEDs included. Blank panels and line cards are shown in black except for the following which are blue: R502-M management cards, access line cards, and services line cards. Ports are displayed in various colors depending on the port state or if a specific condition has occurred.



Green indicates an active link on the port.



Red indicates no link is detected.



Blue indicates the port is administratively disabled.



Purple indicates the port is administratively disabled and the port has a fault, such as no link or Far End Fault. The port could be administratively disabled to prevent errors from being reported.



Yellow means a Far End Fault condition has occurred.

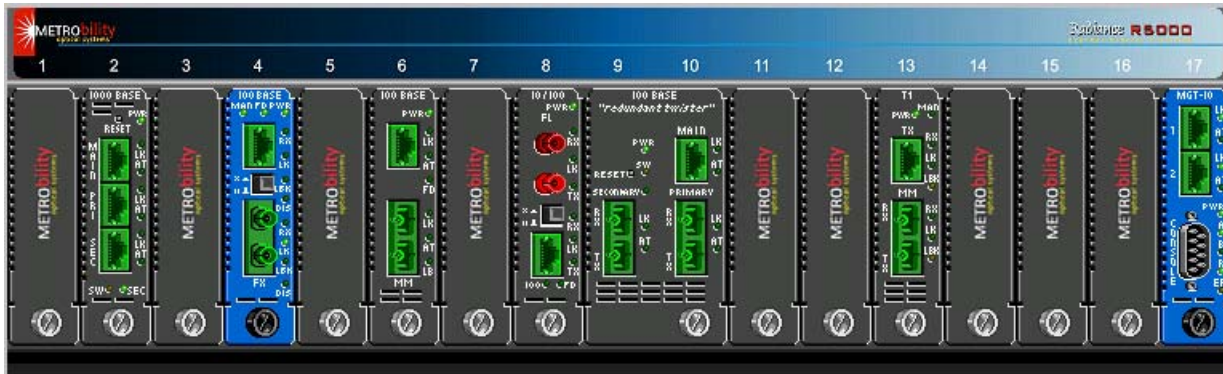


Orange means a signal is detected, but it is not locked.  
(Link down, line up.)



A gray port indicates link status is not applicable to the port (i.e., it is a serial port) or the port is in an unknown state (this may occur at startup).

The LEDs, which are green or amber when lit, are shown in their actual states which may be off, on, or blinking. The following illustration shows an example of a 17-slot chassis with a management card, several line cards, and blank panels.



### Power Supply Status

Below the chassis image, the status of the power supply modules is provided in a graphical format as shown in the following example. This feature is especially useful for chassis with power supplies located in the rear. The power supply status may be On, Off, or Removed.



Power Supply A: On  Power Supply B: On 

Power Supply Status Indicators

### Remote Devices

Remote devices connected to an access line card or services line card are shown below the card to which they are physically connected. Remote management is achieved through Metroblity's patented Radiance technology or the IEEE 802.3ah protocol.



Remote Devices

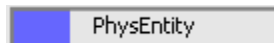
## Chassis in Stack

When the selected element consists of a two or more stacked chassis, only one chassis is shown at a time. Below the chassis image, a number is shown for each chassis in the stack. For example, if there were three chassis, the numbers 1 through 3 will appear. The chassis number of the device currently in view appears in blue. Click **Previous** or **Next** to view other chassis in the stack.



## Discovery Status Bar

Each time NetBeacon connects a new element, the discovery progress is displayed in a status bar located in the lower left corner of the chassis view. As the discovery proceeds, the blue area increases to show the actual progress. The name of the last SNMP table that NetBeacon successfully reads is printed in the status bar. Discovery usually takes less than a minute, however, sometimes it can take several minutes.



## Information Tabs

NetBeacon organizes information about the network elements through the use of tabs. Each tab contains different information relevant to the selected element. The tabs displayed will vary, depending on the element selected. For example, a stand-alone services line card does not include the Chassis and Modules tabs, however, it does include additional tabs that are not available to other line cards.

You cannot change any shaded (grayed) field information; this information is for display only. You can edit field information with a white background (e.g., system name or location).

Tabs	Description
System Info	System information about the selected device, including the name of the device, its physical location, a contact name, its description, its IP address, system uptime and services.
Chassis	Basic information about each device in the selected stack, including the location in the stack, the device name, part number, asset identifier, and description. A single chassis is treated as a stack of one.
Modules	Information about the replaceable cards, including the management card, installed in the chassis. Includes each card's location, name, type, asset identification, and a brief description.
Ports	General port information including location, name, type, link status, and speed.

<b>Tabs</b>	<b>Description</b>
Alarms & Traps	Alarm messages and SNMP traps that relate to the configuration or status change of a device, module, or port. Alarm information includes the element on which the alarm occurred, a description of the alarm, the start and end times, and acknowledgement indicator. Through the NetBeacon EM Admin Tool, you can filter or forward these messages via e-mail to a network manager.

The following information tabs are only applicable to stand-alone services line cards and Ethernet services provisioning platforms.

<b>Tabs</b>	<b>Description</b>
Module Information	Hardware information about the device, as well as its part number and serial number.
Network	Network configuration information, including the element's IP address, MAC address, network mask, gateway, SNMP community strings, DHCP parameters, management VLAN, and loopback timeout period. On some devices, this tab also includes Logical Services Loopback configuration parameters and other switch settings.
Firmware	Information related to the element's embedded software (FPGA, OS). Also includes information about the server from which new firmware can be downloaded.
Trap Manager/ARP /VLAN	SNMP trap destinations table, Address Resolution Protocol (ARP) table, and user VLAN information. Also provides the ability to add, delete, or edit entries. (This tab is only applicable to the 10/100 Mbps services line card.)
Traffic Management	Traffic classification information for choosing the prioritization method or assigning queues. Only applicable to the 10/100 Mbps services line card.
Sensors	Temperature and voltage regulator gauges. For the Ethernet services provisioning platform, fan gauges are also included.

## Chapter 5. Managing the Elements

---

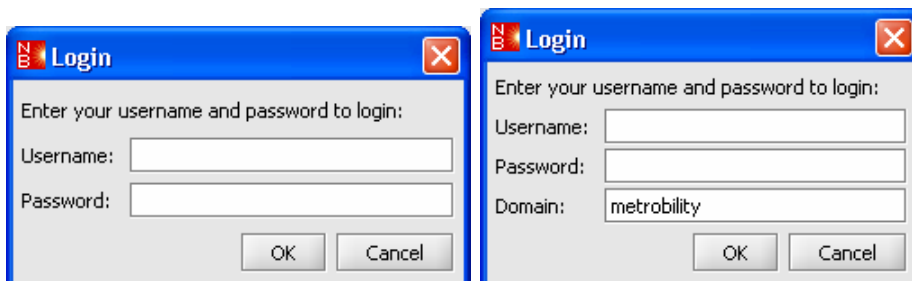
This section describes the NetBeacon management features and how to use them to monitor the elements in your network. The topics covered in Chapter 5 include the following:

- [Connecting to an Element](#)
- [Displaying System Information](#)
- [Monitoring the Chassis](#)

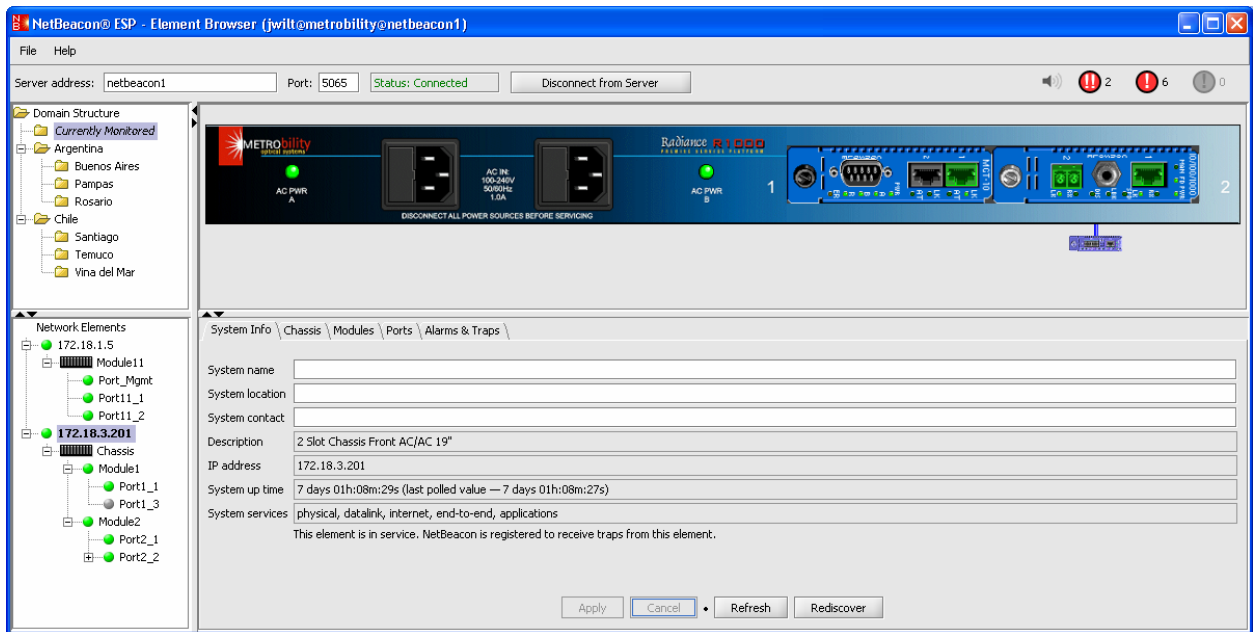
**Important:** You cannot change any information that is shaded (grayed); this information is for display purposes only.

### Connecting to an Element

1. Open the NetBeacon Element Browser window.
2. In the Server address text box, type the *IP address* or *DNS name* of the NetBeacon Element Manager service.
3. In the port text box, type the *port number* through which communications should occur.
4. Click **Connect to Server**.
5. In the Login window, enter your *user name* and *password*. If necessary, enter your Windows XP *domain name*.



6. Expand the Domain Structure in the upper left panel and select the domain name that contains the element to which you want to connect. The selected domain's elements appear in the Network Elements panel.
7. From the Network Elements panel, choose the element. The selected element appears in the chassis view, and the information tabs are filled.



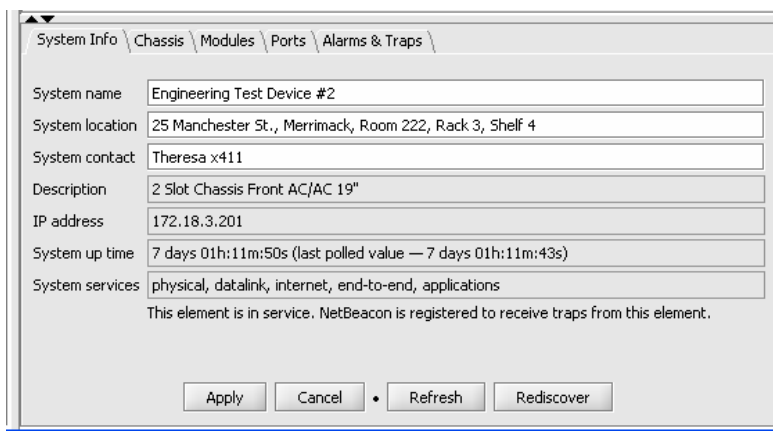
## Displaying System Information

The System Information tab displays information about the selected element, including the system name, location, contact, description, IP address, uptime, and services.

The only information you can change are the system name, its physical location, and the name of a contact person.

To view information about an element, do the following:

1. From the Network Elements list, select the element you want to view.
2. Click the **System Info** tab.
3. In the white text boxes, enter the device *name*, *location*, and *contact*, if you want to add or edit this information.



Do one of the following:

- Click **Apply** to confirm any changes.
- Click **Cancel** to discard your changes and return to the last saved settings.
- Click **Refresh** to update all system information the server has cached regarding the selected element.
- Click **Rediscover** to repoll the element and receive new SNMP data. When the confirmation dialog box appears, click **Yes** to proceed. As NetBeacon reads the SNMP data tables, a status bar located below the chassis displays the discovery progress.

The following table lists the information shown under this tab, along with a brief description of each field.

Name	Description
System name	Name of the element.
System location	Physical location of the element.
System contact	Person or group to contact regarding the element.
Description	A description of the element.
IP address	The IP address of the element.
System up time	The length of time that the system has been running since it was last reset.
System services	The system-level services available on the element. Below this field are two statements indicating whether the element is in service, and if NetBeacon is registered to receive traps from it.
Status line (not labeled)	Located just below the table, this line of text indicates whether or not an element is in service, and whether or not NetBeacon is registered with the element for traps.

## Monitoring the Chassis

The Chassis tab displays information about all the chassis in a stack configuration, as shown in the example below. For an element that is not part of a stack, only a single chassis is listed in the table.

System Info \ Chassis \ Modules \ Ports \ Alarms & Traps				
Location	Name (Alias)	Part Number	Asset ID	Description
Chassis 1	Chassis1	R5000-17H5		17 Slot Chassis 19"
Chassis 3	Chassis3	R5000-17H5		17 Slot Chassis 19"

The following table lists the Chassis tab fields, along with a brief description of each field.

Name	Description
Location	Chassis number in the stack.
Name (Alias)	The name of the chassis. If a user assigned a name to the chassis, this alias will be shown in parentheses.
Part Number	The part number assigned to the chassis for identification purposes.
Asset ID	User-defined asset tracking identifier.
Description	Details on the type of chassis.

### *Resizing Table Columns*

You may resize any of the table columns in the NetBeacon Element Browser. To enlarge or reduce the width of a column, place the cursor on one of the column dividers in the table heading, click and hold down the mouse button on the divider, and drag it to the desired position. You may also move table columns to the left or right by clicking in the column heading and dragging the entire column to the new position. If the table is too long or wide, use the scroll bars to move either vertically or horizontally across a table too see its entire contents.

### *Displaying Chassis Information*

To display chassis information, do the following:

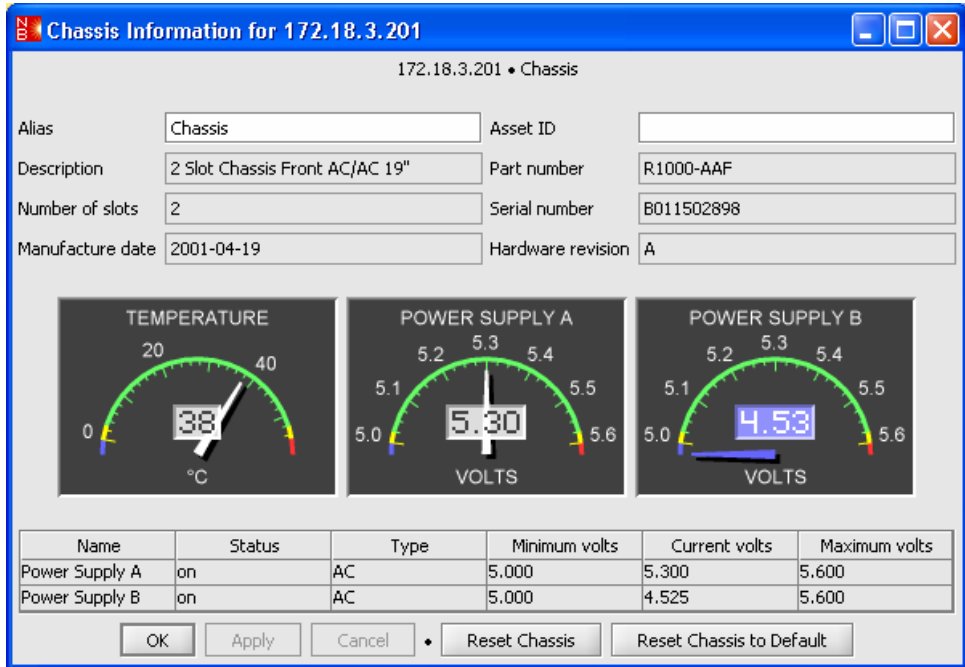
1. From the Network Elements panel, select the element.
2. Click the **Chassis** tab.
3. From the Chassis table, select a chassis by double-clicking on it. Alternatively, you can double-click on the chassis in the image panel.

The Chassis Information dialog box appears. The top half of the dialog box displays information relating to the chassis hardware and is described in the following table.

Name	Description
Alias	The default or user-defined name of the chassis.
Asset ID	User-defined asset tracking identifier.
Description	Details on the type of chassis in which the modules are installed (for example, number of slots and type).
Part number	The part number assigned to the chassis for identification purposes.



Name	Description
Number of slots	The number of slots the chassis contains: e.g., 2, 12 or 17.
Serial number	The serial number assigned to the chassis for identification purposes.
Manufacture date	The date the chassis was manufactured.
Hardware revision	The version of the chassis backplane.



4. To change the alias or to enter an asset identifier for the chassis, type them in the white text boxes.
5. Do one of the following:
  - Click **OK** to apply any changes and close the dialog box.
  - Click **Apply** to confirm any changes and keep the dialog box open.
  - Click **Cancel** to discard your changes and close the dialog box.

### *Displaying Temperature and Power Supply Information*

The bottom half of the Chassis Information dialog box displays environmental information, including the temperature of the chassis, the voltage supplied by each power supply, and the operating status of each power supply. Voltage and temperature information are displayed using both a graphical and textual format.

The table below describes the color coding used on the gauges.

Color	Description
Green	Normal operating range.
Yellow	Warning: above or below the recommended operating range.
Blue	Danger: voltage/temperature is too low.
Red	Danger: voltage/temperature is too high.

The following table describes the power supply information fields.

Name	Description
Power Supply A or B	A device may have one or two power supplies, denoted Unit A (on the left) and Unit B (on the right).
Status	Operational status of the power supply, either ON or OFF.
Type	Type of power supply: AC or DC.
Minimum volts	A predefined value representing the minimum voltage that the power supply should provide.
Current volts	The current voltage output by the power supply.
Maximum volts	A predefined value representing the maximum voltage that the power supply should provide.

### ***Resetting the Chassis***

NetBeacon provides two ways to reset a chassis:

- Click **Reset Chassis** to reset the management module in the chassis, as well as each module installed in the chassis, and any remote units connected to those modules.

When the confirmation dialog appears, click **Yes** to reset the chassis.

- Click **Reset Chassis to Default** to reset the chassis to its factory default settings.

## Chapter 6. Configuring the Modules

---

Through the NetBeacon Element Browser, users can monitor and configure any of the modules they have permission to manage. In addition to overriding hardware switch settings, users can enable advanced functions such as Switch On No Activity Received (SONAR) on the redundant interface line card and Backpressure (half-duplex flow control) on the 10/100Mbps line card.

This chapter includes the following topics:

- [Displaying Module Information](#)
- [Opening the Module Configuration Dialog Box](#)
- [Applying Link Loss Carry Forward](#)
- [Making Module Configurations](#)
- [Managing the Access Line Card](#)
- [Configuring the Redundant Interface Line Card](#)
- [Configuring the 10/100 Mbps Line Card](#)
- [Managing the Chassis Stacking Line Card](#)
- [Configuring the Management Module](#)
- [Configuring the Services Line Card](#)
- [Configuring the RS960](#)

### Displaying Module Information

The Modules tab displays information about the modules (e.g., management card or services line card) installed in the selected element, along with any remote modules. If the element is a stack of two or more chassis, all modules in the entire stack are included.

Information includes the location, name, type, part number, asset identifier, a brief description, and the uptime of each module.

1. Click the **Modules** tab to display the module information table.

System Info \ Chassis \ Modules \ Ports \ Alarms & Traps \						
Location	Name (Alias)	Type	Part Number	Asset ID	Description	Up Time
Slot 2	Module2	Interface	7131-13-75	Metro 012763	100M SC SM 1550nm Ex-Long Haul	day 006 04h:37m:32s
Slot 3	Module3	Redundant Interface	7711-11-75	050929175019	10M TP to Redundant TP	day 006 04h:37m:33s
Slot 4	Module4	MultiRate	R380-55		MultiRate Optical Transponder	day 006 04h:37m:33s
Slot 5	Module5	Stacking	R104-11	050929175021	10/100 Four Port Switch	day 006 04h:37m:34s
Slot 6	Module6	Transparent	R141-14	050929175022	10+100M TX to FX SM/SC	day 006 04h:37m:34s
Slot 7	Module7	Access	R231-14		100M TX to FX SM/SC S/IP	day 006 04h:37m:35s
Slot 7, Port 2, Remote 1	Module7_2_1	Access	R231-14		100M TX to FX SM/SC S/IP	day 006 04h:37m:34s
Slot 8	Module8	Rate Adapter	R621-11	a	10/100M TX to 10/100M TX	day 006 04h:37m:36s
Slot 9/10	Module10	Redundant Interface	R732-14		100M TX-Dual FX SM/SC SONAR	day 006 04h:37m:36s
Slot 11	Module11	Services	R851-15		1G TX to FX SLC	day 001 04h:55m:34s
Slot 11, Port 2, Remote 1	Module11_2_1	Services	R851-15		1G TX to FX SLC	day 000 05h:13m:50s
Slot 12	Module12	Gigabit Interface v3	R153-55		1G FX to FX	day 006 04h:37m:38s
Slot 13	Module13	Interface	7131-54-75		100M FX(MM ST) to FX(SM SC)	day 006 04h:37m:38s
Slot 15	Module15	Auto Interface v3	R643-13		10/100 TX to 100M FX MM/SC	day 006 04h:37m:38s
Slot 16	Module16	Stacking	R104-11		Four Port Switch	day 006 04h:37m:38s
Slot 17	Module17	Management	R502-M		Management Module Dual Port	day 006 04h:37m:40s

The following table lists the information shown under the Modules tab, along with a brief description of each field.

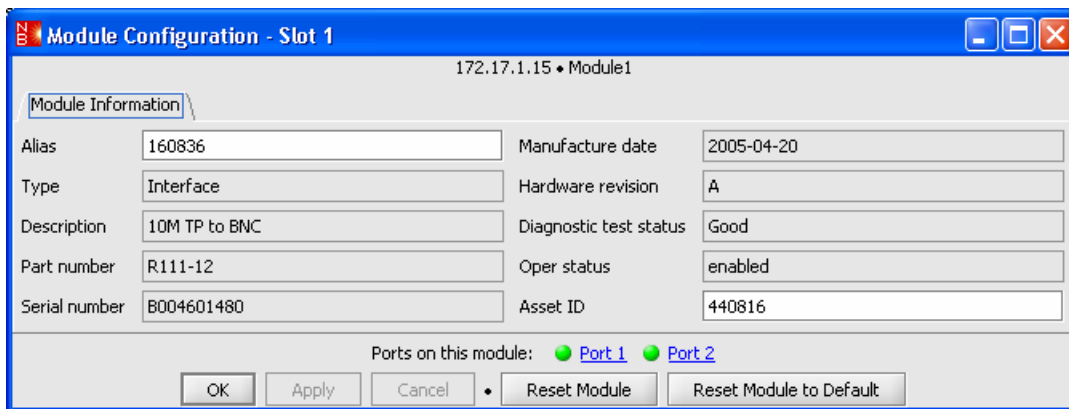
Name	Description				
Location	<p>The slot where the module is installed.</p> <p>For a remote access or services line card, the local module's port to which it is connected and the remote card number are also included. In the example shown above, a remote access line card is connected to port 2 of the module in slot 7.</p> <p>If the element is a stack of two or more chassis, the chassis number in the stack is also included, as shown below.</p> <table border="1" data-bbox="453 1161 654 1276"> <thead> <tr> <th>Location</th> </tr> </thead> <tbody> <tr> <td>Chassis 1, Slot 1</td> </tr> <tr> <td>Chassis 1, Slot 2</td> </tr> <tr> <td>Chassis 1, Slot 3</td> </tr> </tbody> </table>	Location	Chassis 1, Slot 1	Chassis 1, Slot 2	Chassis 1, Slot 3
Location					
Chassis 1, Slot 1					
Chassis 1, Slot 2					
Chassis 1, Slot 3					
Name (Alias)	The default or user-assigned name for the module. The name assigned by the user is shown in parentheses.				
Type	The type of module – a management card, an access line card, an interface line card, a services line card, etc.				
Part Number	The part number assigned to the module for identification purposes.				
Asset ID	User-defined asset tracking identifier.				
Description	Details on the module's specifications.				
Up Time	Length of time that the module has been up since it was last reset.				

## Opening the Module Configuration Dialog Box

To open the Module Configuration dialog box, do one of the following:

- In the chassis view, double-click anywhere on the image of the desired module, except on its ports.
- Under the Modules tab, double-click anywhere in the row of the desired module.
- In the Network Elements panel, right-click on the desired module and select **Show configuration dialog** from the pop-up menu.

The Module Configuration dialog box displays hardware information specific to the module you selected. The dialog box may contain more than one tab.



The following table describes the fields shown for all modules under the Module Information tab in this dialog box. For most modules, this is the only tab provided.

Name	Description
Alias	Default or user-defined name of the module.
Type	The type of module installed in the slot. For example, an access line card or a management card.
Description	Details on the module's specifications.
Part number	The part number assigned to the module for identification purposes.
Serial number	The serial number assigned to the module for identification purposes.
Manufacture date	The date the module was manufactured.
Hardware revision	The version of the module's circuit board.
Diagnostic test status	The results of the diagnostics test of the module.

Name	Description
Oper status	Operational status of the module, either Enabled or Disabled.
Asset ID	User-defined asset tracking identifier.

The following table describes additional read-only fields shown with certain modules under the Module Information tab.

NOTE: Not all fields are applicable to every module.

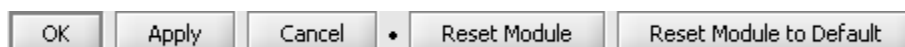
Name	Description
FPGA revision	Version number of the module's Field-Programmable Gate Array code.
PIC revision	Version number of the module's microcontroller firmware.
CPLD revision	Version number of the module's Complex Programmable Logic Device.


### *Opening the Port Configuration Dialog Box*

To open the Port Configuration dialog box for the ports on the selected module, click on any of the blue hyperlinks.

Ports on this module:  [Port 1](#)  [Port 2](#)

### *Module Configuration Dialog Box Button Options*



All Module Configuration dialog boxes provide five buttons, shown above. For a services line card, an additional reset button  is provided. The button functions are described in the following table.

Name	Description
OK	Save any changes that were entered and close the Module Configuration dialog box.
Apply	Save any changes that were entered and keep the dialog box open.
Cancel	Discard any changes that were entered and close the dialog box.
Reset Module	Reset the selected module.
Reset Module to Default	Reset the selected module to its factory default settings.
Hard Reset Module	Force a register reset on the services line card. Use this option only if a regular reset is ineffective.

**Tip:** For simplicity, this manual instructs you to click **OK** after making changes, although you may also click **Apply**.

### ***Changing a Module Name and Asset ID***

1. Open the Module Configuration dialog box.
2. In the Alias text box, type the *name*<sup>1</sup> you want to assign to the module.
3. In the Asset ID text box, type the *asset tracking identifier*<sup>2</sup> to assign to the module.
4. Click **OK**.

### ***Resetting a Module***

To reset a module, do the following:

1. Open the Module Configuration dialog for the module you want to reset. At bottom of the dialog box, there are two reset buttons.
2. Click **Reset Module** if you want to reset the module; or click **Reset Module to Default** if you want to reset the module to its factory default settings.
3. When the confirmation dialog box appears, click **Yes**.

### **Applying Link Loss Carry Forward**

In addition to changing the name and asset ID, you can enable or disable Link Loss Carry Forward (LLCF) on the many of the modules.

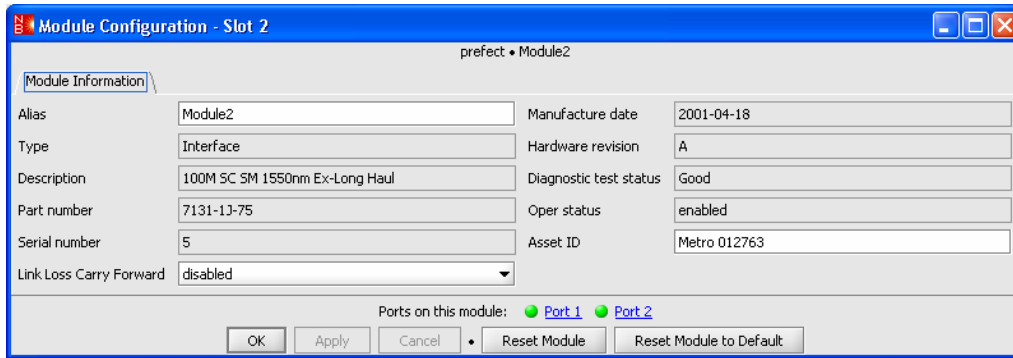
When LLCF is enabled, if one port loses link, the module will not transmit a link pulse from the other port.

1. Open the Module Configuration dialog box by double-clicking on the module in the chassis view or on a row in the Modules table.
2. From the Link Loss Carry Forward drop-down list, select **enabled** or **disabled**. LLCF is disabled by default.

---

<sup>1</sup> There is a limit of 32 characters for the module name. Do not use the following characters: . ; & = : " < > .

<sup>2</sup> There is a limit of 32 characters for the asset ID. Do not use the following characters: . ; & = : " < > .



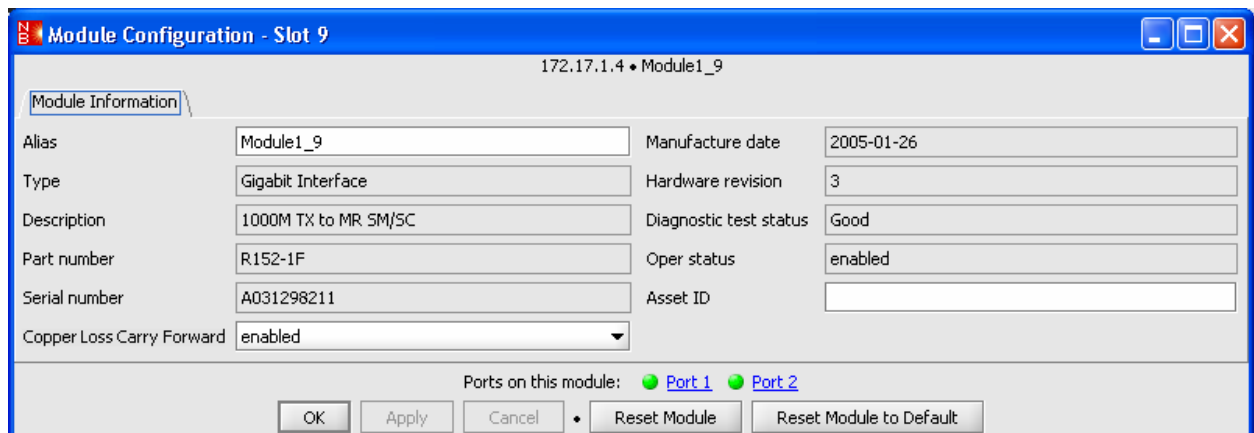
3. Click **OK**.

### *Applying Copper Loss Carry Forward*

Copper Loss Carry Forward (CLCF) is only applicable to the 1000Mbps TX-FX line cards. CLCF is disabled by default.

When CLCF is enabled, the fiber port's transmitter shuts down if the copper port stops receiving link pulses. To apply CLCF, do the following:

1. Open the Module Configuration dialog box for the 1000Mbps TX-FX line card to configure.
2. From the Copper Loss Carry Forward drop-down list, select **enabled**.
3. Click **OK**.



## **Making Module Configurations**

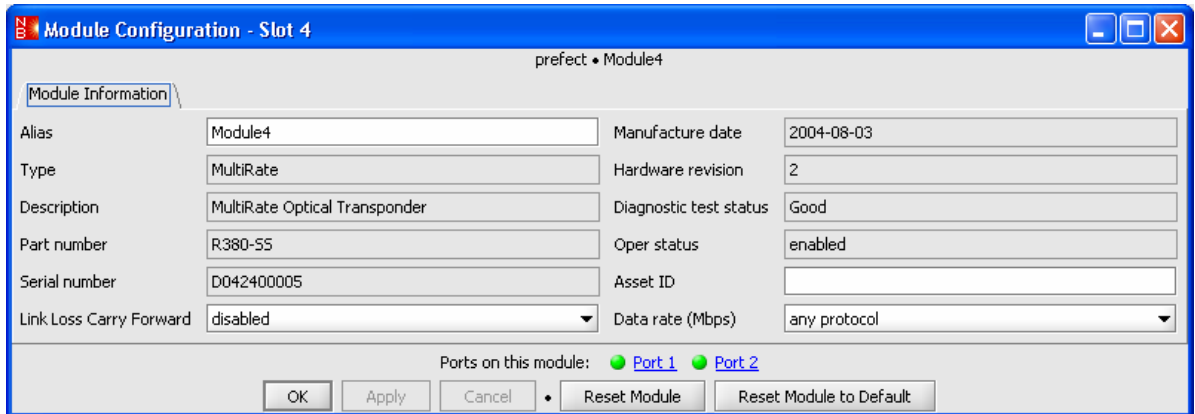
This section describes how to configure unique functions associated with various types of modules.



## Setting the Data Rate for a Multi-Rate Line Card

The multi-rate line card provides a transparent interface for multimode, singlemode, bidirectional wavelength division multiplexing (BWDM), and coarse wavelength division multiplexing (CWDM) connections across a wide range of protocols with data rates ranging from 44.736 to 2666.057 Mbps.

1. In the chassis view, double-click on the multi-rate line card you want to configure. The Module Configuration dialog box appears.



2. Select one of the speed settings provided in the Data rate drop-down list. The values are given in megabits per second (Mbps).

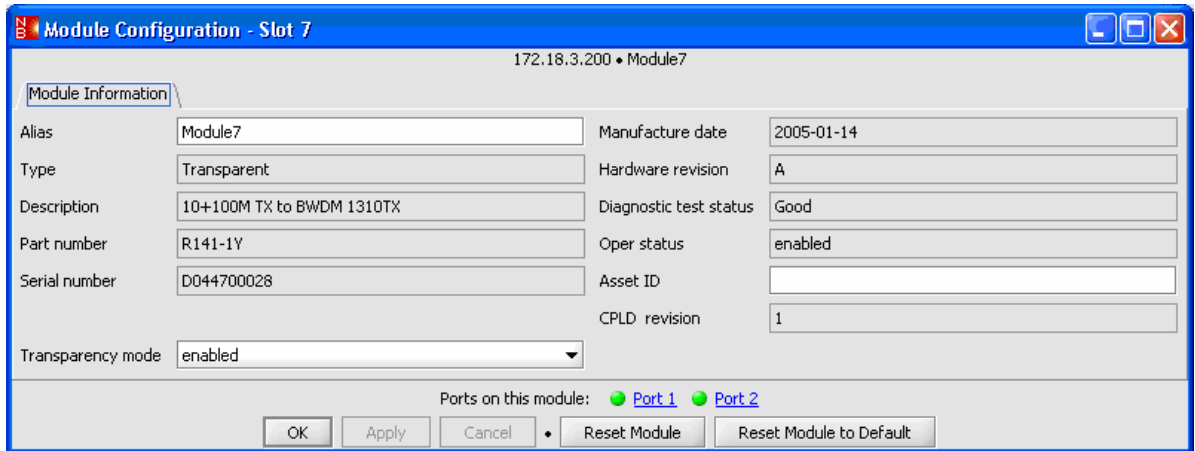
Select **any protocol** if you want the multi-rate line card to be protocol transparent. This is the default setting, and it allows the card to bypass its clock and data recovery circuit.

Select **auto detect** if you want the multi-rate line card to automatically determine which data rate to use on both ports. In this mode, the speed is determined by the data rate of the first active device the multi-rate line card detects through one of its ports.

3. Click **OK**.

## Setting the Transparency Mode on the R141, R111-13-B, or R11-15-B Line Card

1. In the chassis view or in the Modules table, double-click on the R141, R111-13-B, or R11-15-B line card. The Module Configuration dialog box appears. The dialog provides the standard module information, with one addition—the Complex Programmable Logic Device (CPLD) revision number or letter.



2. Set the Transparency mode to **enabled** or **disabled**.

When the Transparency mode is enabled, the line card becomes completely transparent to the end devices connected to the card's two ports. This allows the end devices to negotiate which speed and duplex they will use for data transfer. (For the R111-13-B and R111-15-B, only the duplex mode is negotiated, because the card only supports one speed, 10Mbps.) An advantage of having the Transparency mode enabled is that it allows both end devices to become aware of any link failure that may occur between them.

When the Transparency mode is disabled on the R141, the speed is determined by the DIP switch setting or by the speed setting that is configured through software (refer to [Setting the Speed on the R141 Line Card](#)).

When the Transparency mode is disabled on the R111-13-B or R111-15-B, you must manually set the speed and duplex on both end devices to the same setting. That is, both end devices must be set to 10Mbps full-duplex, or both devices must be set to 10Mbps half-duplex.

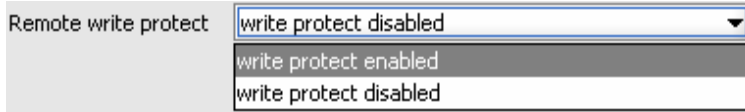
3. Click **OK**.

## Managing the Access Line Card

### *Applying Write Protection on an Access Line Card*

By default, the access line card is not write-protected. To prevent a remote access line card from making changes to a locally managed card, do the following:

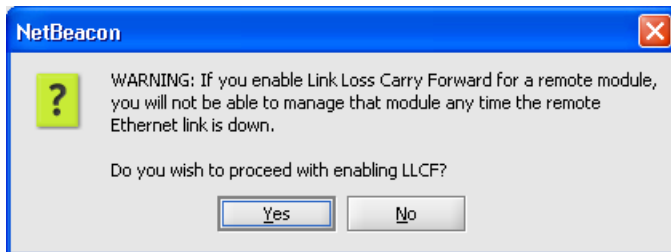
1. Double-click the local access line card in the chassis view to open the Module Configuration dialog box. Write protection is not applicable to remote devices.
2. The access line's Module Configuration dialog box contains two tabs. Click the **Module Information** tab.
3. Select **write protect enabled** from the Remote write protect drop-down list.



4. Click **OK**.

### ***LLCF Warning***

Link Loss Carry Forward can be enabled and disabled on both the local and remote access line cards. However, be aware that if you do enable LLCF on the remote card and its Ethernet link goes down, you will lose the ability to manage that card. If you attempt to enable LLCF on a remote access line card, a warning message will appear:

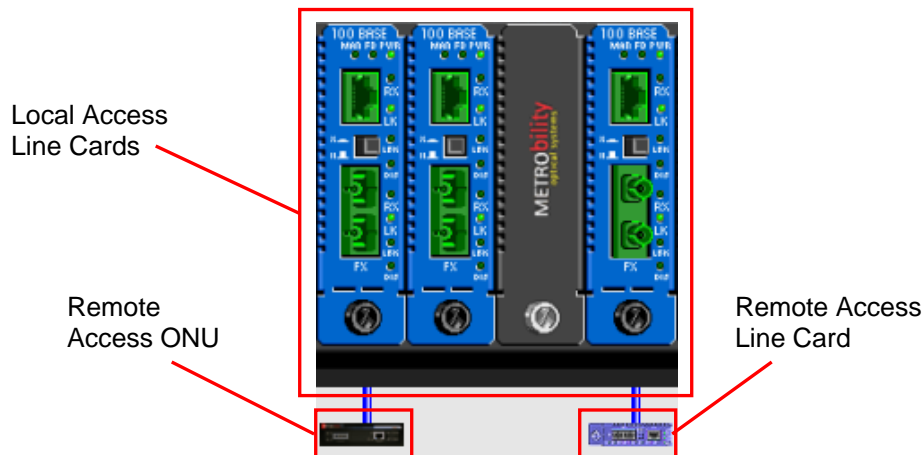


Enabling LLCF on a remote access line is NOT recommended.

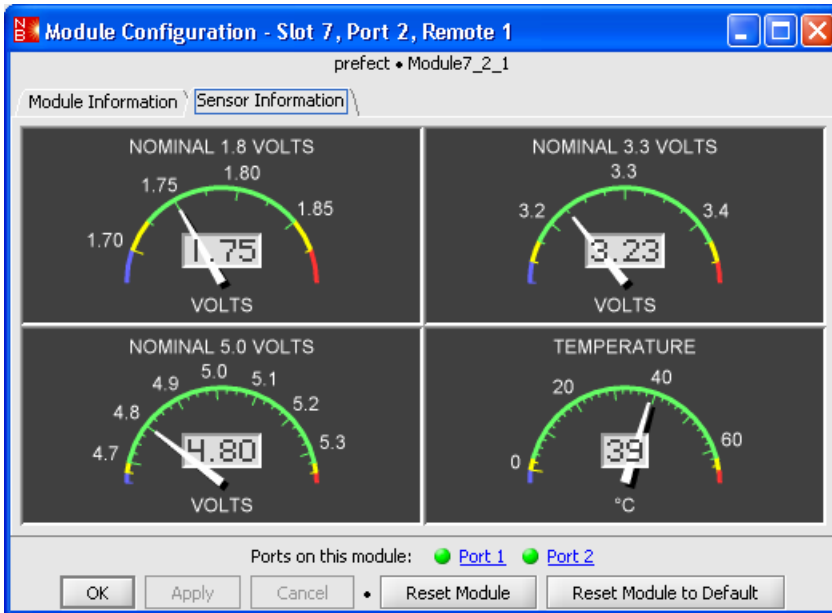
### ***Displaying Sensor Information for an Access Line Card or Access ONU***

The access line card and the access optical network unit (ONU), which can be connected remotely, contain a temperature sensor and two or three internal voltage regulators. To view information about the regulators and sensor, do the following:

1. Open the Module Configuration dialog box for the local or remote access line card or remote access ONU.



2. Click the **Sensor Information** tab. The access line card voltage and temperature gauges appear.



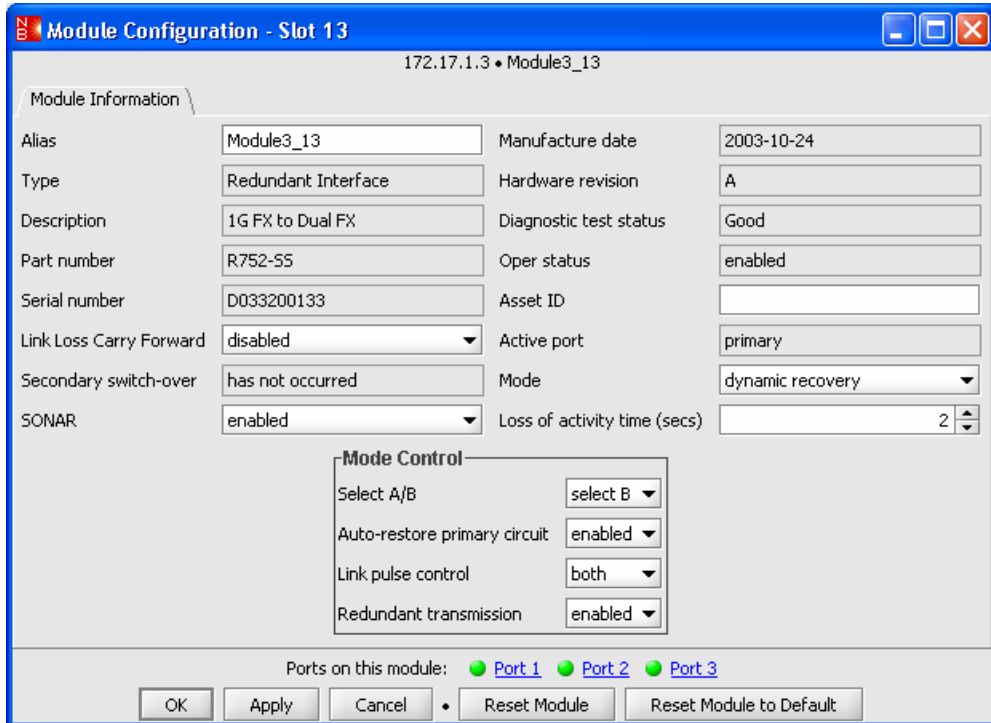
The table below describes the color coding used on the gauges.

Color	Description
Green	Normal operating range.
Yellow	Warning: above or below the recommended operating range.
Blue	Danger: voltage/temperature is too low.
Red	Danger: voltage/temperature is too high.

## Configuring the Redundant Interface Line Card

To configure a redundant interface line card, do the following:

1. In the chassis view or Modules table, double-click the redundant module to configure. The Module Configuration dialog box for a redundant line card appears.



The dialog box displays the Mode and Mode Control settings for the selected module and active port. You can override the DIP switches on the board by changing these settings.

2. Select the Mode option: **dynamic recovery** or **select AB**.

### ***Dynamic Recovery Mode***

When dynamic recovery mode is active, both links are directed to the same network. Only the primary link is active unless (1) a failure occurs, in which case the secondary link assumes primary control, or (2) redundant transmission mode is enabled.

If you select the auto restore option, then the primary link will be reactivated as soon as it is restored. Otherwise, the secondary port remains active if its link does not fail.

Use dynamic recovery when you want to ensure continuous network connectivity and secure uninterrupted user access in the event of a link failure.

Dynamic Recovery Mode:	Select A/B: This setting is not applicable in dynamic recovery mode.
	Auto-restore primary circuit: <ul style="list-style-type: none"> <li>enabled – reverts the active port back to the primary port when the primary link is reestablished.</li> <li>disabled – keeps the secondary port as the active port even if the primary link is reestablished.</li> </ul>
	Link pulse control: <ul style="list-style-type: none"> <li>both – sends idle signals on both the primary and secondary ports.</li> <li>active - sends idle signals on the active port only.</li> </ul>
	Redundant transmission: <ul style="list-style-type: none"> <li>enabled – sends data on both the primary and secondary ports simultaneously.</li> <li>disabled – sends data on the active port only.</li> </ul>

**Tip:** You must enable link pulse control to enable redundant transmission.

### *Applying SONAR*

For redundant interface line cards with Switch On No Activity Received (SONAR), an additional parameter appears in the top half of the Module Configuration dialog box. SONAR affects the module's response to a loss of activity (LOA) for two seconds on the active port. (NOTE: For some models, the LOA period is configurable.) SONAR is applicable only in dynamic recovery mode with link pulse control enabled.

The other switch settings do not affect SONAR operation. However, SONAR will override the auto-restore primary circuit setting. If both these settings are enabled, the active port will not automatically revert back to the primary port (after switching to the secondary port) if the primary port has link but no data activity. Data activity on the primary port must also be detected during the LOA period before the active port reverts back to the primary port.

To enable SONAR, do the following:

1. In the redundant interface line card's Module Configuration dialog box, choose **enabled** from the SONAR drop-down list.
2. Set the Mode to **dynamic recovery**.
3. Make sure that link pulse control is set to **both**.
4. For a gigabit redundant interface line card, the loss of activity period can be set anywhere from 1 to 31 seconds. If the active port remains idle for the specified time, the card will verify activity on the secondary port, and switch to the secondary port if traffic is detected there.

Loss of activity time (secs)

5. Click **OK**.

## Select A/B Mode

When Select A/B mode is active, each link on the redundant interface line card operates independently and is directed to a different network. Only one link (primary or secondary) is active at any given time.

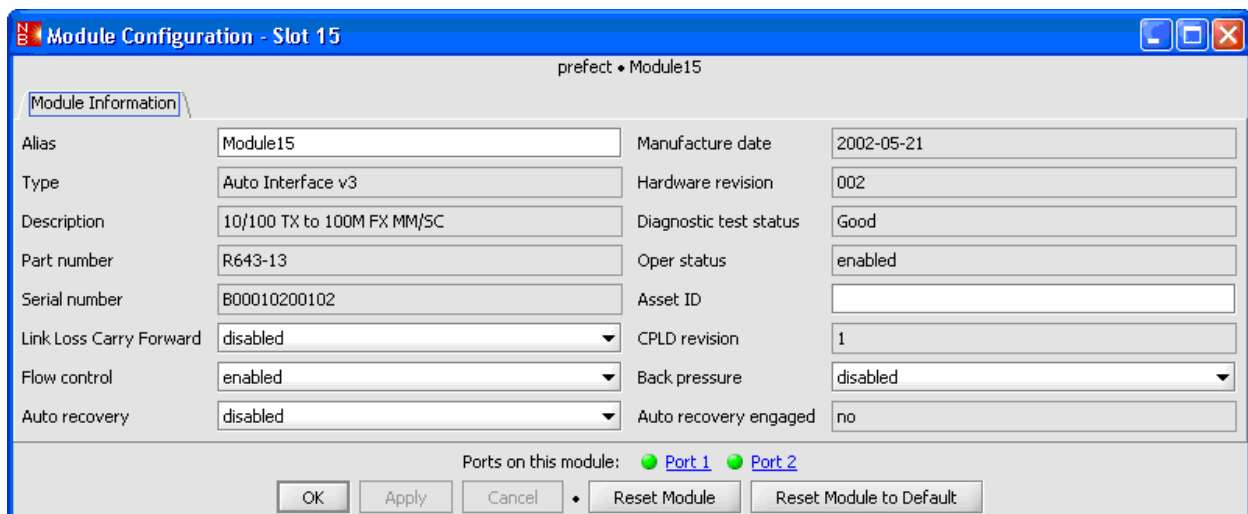
Use the Select A/B mode to redirect traffic from one network to another in less critical points in your network where full redundancy is not required.

Select A/B: select A – enables the primary port.  
select B – enables the secondary port.

## Configuring the 10/100 Mbps Line Card

The 10/100Mbps interface line card (AutoTwister) is a rate adapter that connects 10Mbps devices to 100Mbps devices, copper-based networks to fiber-based networks, and full-duplex systems to half-duplex systems. Depending on your model, various features are available for this card.

In the chassis view or Modules table, double-click the module to configure. The Module Configuration dialog box for a 10/100Mbps line card appears.



Module Configuration - Slot 15

perfect • Module15

Module Information

Alias	Module15	Manufacture date	2002-05-21
Type	Auto Interface v3	Hardware revision	002
Description	10/100 TX to 100M FX MM/SC	Diagnostic test status	Good
Part number	R643-13	Oper status	enabled
Serial number	B00010200102	Asset ID	
Link Loss Carry Forward	disabled	CPLD revision	1
Flow control	enabled	Back pressure	disabled
Auto recovery	disabled	Auto recovery engaged	no

Ports on this module: ● Port 1 ● Port 2

OK Apply Cancel • Reset Module Reset Module to Default

### Link Loss Carry Forward and Flow Control

1. For a 10/100Mbps line card with LLCF functionality, you can select **enabled** or **disabled** from the drop-down list. The default is LLCF disabled.
2. On some models an additional feature, flow control, is provided. If you enable flow control, the 10/100Mbps line card will issue a PAUSE frame when there is no buffer space available for incoming packets. Select **enabled** or **disabled** from the drop-down list. This setting is enabled by default.
3. Click **OK**.

### ***Backpressure (Half-Duplex Flow Control)***

1. Backpressure is only applicable to ports operating at half duplex. When backpressure is activated, the 10/100Mbps card generates a jamming pattern to force a collision on a port when the module cannot allocate a buffer for the port's incoming packets. Enabling backpressure activates it on both ports of the module. Backpressure is ignored in full duplex because collisions are not generated in this mode. Select **enabled** or **disabled** from the drop-down list. Backpressure is disabled by default.
2. Click **OK**.

### ***Auto-Recovery***

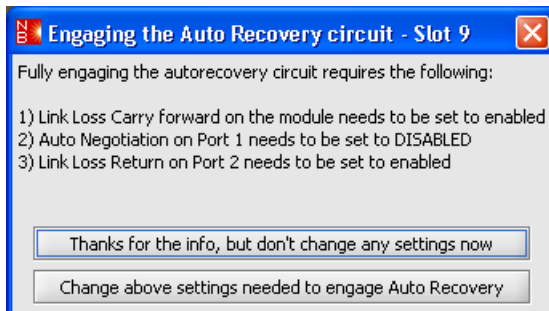
The R643 10/100Mbps line cards include the auto-recovery feature to assist in troubleshooting remote connections. Auto-recovery allows the card to restart its fiber connection after a link loss event.

Auto-recovery is enabled only when all of the following conditions are met:

- Link Loss Carry Forward is enabled.
- Link Loss Return is enabled.
- Auto-negotiation is disabled.
- Auto-recovery is enabled.

If any of the above settings are not set properly, NetBeacon provides you an option to enable auto-recovery by making all the necessary configuration changes in one easy step.

1. In the Module Configuration dialog box, set auto-recovery to **enabled**. If any of the first three settings listed above are incorrect, the following dialog box appears. The dialog lists each configuration change required to activate auto-recovery.



2. Click **Change above settings needed to engage Auto Recovery**. NetBeacon automatically reconfigures the all the settings it identified in the dialog box, along with the auto-recovery setting. It is not necessary to click Apply or OK unless you made other changes in the Module Configuration dialog box. After approximately 30 seconds, the auto-recovery engaged status box should say, "yes."

Auto recovery engaged | yes



## Managing the Chassis Stacking Line Card

The chassis stacking line card is a 10/100Mbps four-port switch that can be used to stack up to four Metrobility chassis. The Module Configuration dialog box for this card provides the standard module information, with four additional fields—the Complex Programmable Logic Device (CPLD) revision number or letter and three functional settings which are described in the next section. The Module Configuration dialog box for a chassis stacking line card is shown below.

The screenshot shows a window titled "Module Configuration - Slot 16" with a sub-header "prefect • Module16". The "Module Information" tab is active. The form contains the following fields and values:

Alias	Module16	Manufacture date	2003-03-19
Type	Stacking	Hardware revision	2
Description	Four Port Switch	Diagnostic test status	Good
Part number	R104-11	Oper status	enabled
Serial number	A120300012	Asset ID	
		CPLD revision	36
Port duplex	half	FD flow control	disabled
HD flow control	disabled		

At the bottom, it shows "Ports on this module:" with four green status indicators for Port 1, Port 2, Port 3, and Port 4. Buttons for "OK", "Apply", "Cancel", "Reset Module", and "Reset Module to Default" are located at the bottom of the dialog.

### *Port Duplex, Full-Duplex Flow Control, and Half-Duplex Flow Control*

1. The port duplex setting determines the duplex mode on all ports that have auto-negotiation disabled. Select **full** or **half** from the drop-down list.

If auto-negotiation is enabled on a port, the port will ignore the port duplex setting. Instead, the duplex mode will be determined through the auto-negotiation process.

2. Full-duplex (FD) flow control is provided as a means of avoiding packet loss during times of network congestion. This setting can only be changed through software control and is enabled by default. With FD flow control enabled, the chassis stacking line card will issue a PAUSE frame if there is no buffer space available for incoming packets. Select **enabled** or **disabled** from the drop-down list.
3. Half-duplex (HD) flow control is only applicable to ports operating at half duplex. When HD flow control is activated, the 10/100Mbps card generates a jamming pattern to force a collision on a port when the card cannot allocate a buffer for the port's incoming packets. Activating HD flow control enables it on all ports. HD flow control is ignored in full duplex because collisions are not generated in this mode.

Select **disabled** or **enabled** from the HD flow control drop-down list.

4. Click **OK**.

## Configuring the Management Module

The management card is located in slot 12 of a 12-slot chassis, slot 17 of a 17-slot chassis, or either slot of a two-slot chassis.

### Displaying Management Module Information

To display management card details, do the following:

1. Open the Module Configuration dialog box for the management card.
2. Select the **Module Information** tab.

The screenshot shows a window titled "Module Configuration - Slot 17" with a sub-header "perfect • Module17". The "Module Information" tab is selected, showing a grid of fields for configuration. The fields include: Alias (Module17), Type (Management), Description (Management Module Dual Port), Part number (R502-M), Serial number (B04250027), Boot image name (boot.bin), Core image name (corepm.biz), RAM memory size (32768K), NVRAM memory size (8K), Manufacture date (2004-06-22), Hardware revision (1), Diagnostic test status (Good), Oper status (enabled), Asset ID (empty), Boot image revision (3.8.0.0(May 13 2005)), and Core image revision (3.8.0.0(May 13 2005)). Below the grid, there are radio buttons for "Ports on this module": Port 1 (selected), Port 2 (selected), and Port 3 (unselected). At the bottom, there are buttons for "OK", "Apply", "Cancel", "Reset Module", and "Reset Module to Default".

In addition to the ten parameters shown for every module under the Module Information tab, the management module includes the following fields described in the table below.

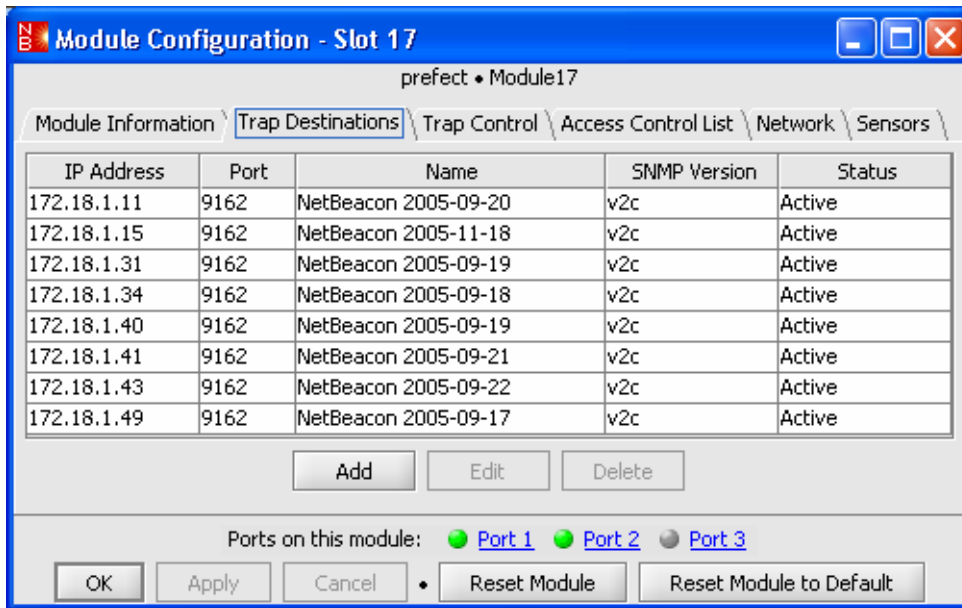
Name	Description
Boot image name	File name of the boot image.
Boot image revision	Version number of the boot image, and the date it was created.
Core image name	File name of the core image.
Core image revision	Version number of the core image, and the date it was created.
RAM memory size	The amount of volatile RAM on the card.
Flash memory size	The amount of non-volatile flash memory on the card.
NVRAM memory size	The amount of non-volatile memory on the card. This memory is backed up by battery.

## Configuring Trap Destinations

Through NetBeacon, you can configure multiple management stations to monitor traps. NetBeacon tries to register itself with each device's trap destination table, but it may not succeed due to insufficient access (read-only access), or because the device's trap manager table is full. Some devices such as the services line card and RS960 only have four slots for up to four entries in their tables. No trap managers are removed until you delete them.

To display the list of trap destinations configured for the selected element, do the following:

1. Open the Module Configuration dialog box for the management card.
2. Select the **Trap Destinations** tab.



The following table lists the Trap Destinations information shown above, along with a brief description of each field.

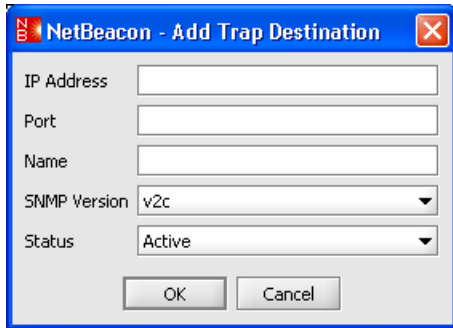
Name	Description
IP Address	IP address of the workstation where trap notices are sent.
Port	The User Datagram Protocol (UDP) port number.
Name	Name assigned to the trap destination.
SNMP Version	The traps' SNMP version: v1 or v2c.
Status	Indicates whether the trap destination is active or not in service. When active, traps are sent to the manager. When not in service, traps are logged but not sent.

## Adding a New Trap Destination

To add a new trap destination, do the following:

1. Click **Add**.

The Add Trap Destination dialog box appears.



2. In the IP Address text box, type the *IP address* of the destination server or device to which traps will be sent.
3. In the Port text box, type the trap destination's *UDP port number*. The default number is 9162. Port 162 is the standard SNMP trap port.
4. In the Name text box, type a *name* for the new trap destination.
5. Select **v1** or **v2c** from the drop-down list to set the SNMP version that will be used to send trap messages.
6. Select **Active** or **Not in service** from the Status drop-down list. Traps are sent to the trap destination if you select Active. Traps are recorded but not sent, if you choose Not in service.

**Important:** Make sure your trap destination workstations are configured to receive trap notices.

7. Click **OK** to update the trap destinations table.

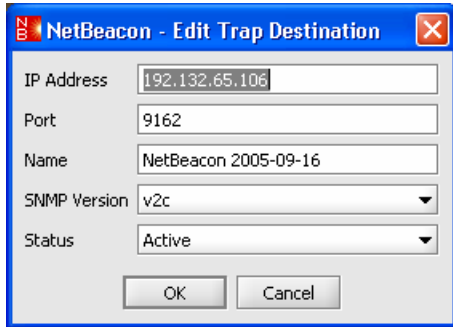
## Reconfiguring a Trap Destination

After you have configured your trap destinations, you can change any of the fields.

To change trap management information, do the following:

1. From the Trap Destinations table, select the trap destination you want to modify.
2. Click **Edit**.

The following Edit Trap Manager Destination dialog box appears.



3. Do any of the following:
  - In the IP Address text box, type the new *IP address* of the destination server or device to which traps will be sent.
  - In the Port text box, type the trap destination's new *UDP port number*.
  - In the Name text box, type the new *name* of the trap manager.
  - Select **v1** or **v2c** from the SNMP Version drop-down list.
  - Select **Active** or **Not in service** from the Status drop-down list.
4. Click **OK** to update the Trap Destination table.

### **Deleting a Trap Destination**

To remove one or more trap destinations, do the following:

1. From the Trap Destinations table, select the row(s) of the destination(s) you want to remove.

**Tip:** To select more than one, hold down the CTRL key and select all the trap destinations you want to remove.

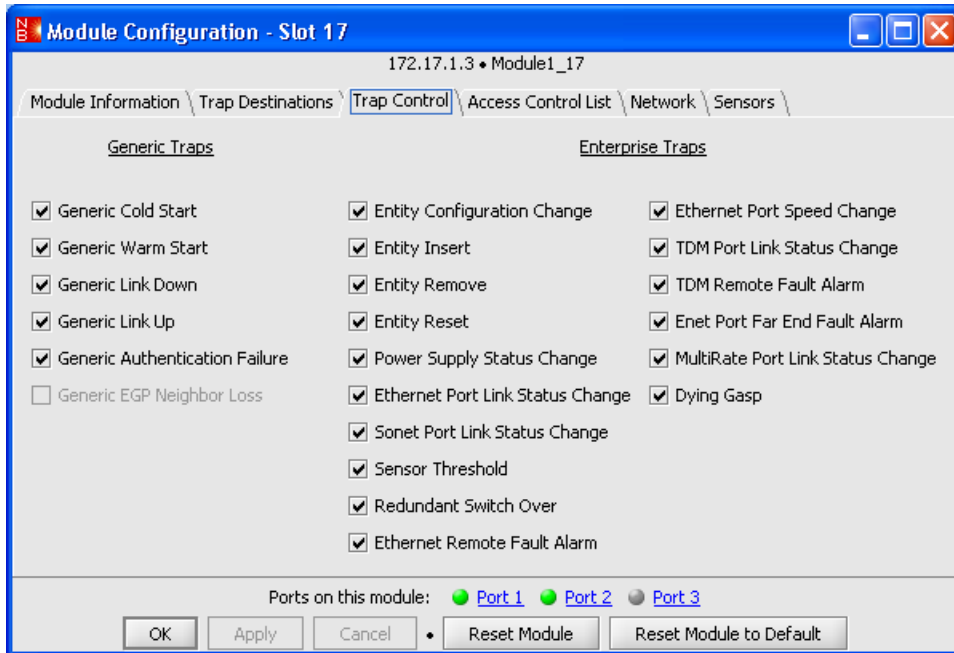
2. Click **Delete**.
3. Click **OK**.

### **Filtering the Trap Control Options**

NetBeacon has two categories of traps: Generic Traps and Enterprise Traps. Initially, all traps, excluding Generic EGP Neighbor Loss, are enabled. Each trap can be individually disabled to suit your network monitoring preferences.

To display the trap legend, do the following:

1. Open the Module Configuration dialog box for the element's management card.
2. Select the **Trap Control** tab.



The following table lists all the traps and describes the conditions that trigger them when enabled. Traps that are enabled are recorded in the Alarms log.

Name	Trap Event
Generic Cold Start	The management card is reset.
Generic Warm Start	The occurrence of a software error that caused a spontaneous reset.
Generic Link Down	A port loses link. (The port is not specified.)
Generic Link Up	A port detects link. (The port is not specified.)
Generic Authentication Failure	Invalid SNMP community string is used.
Generic EGP Neighbor Loss	Not Applicable.
Entity Configuration Change	A power supply or card is removed from or added to a chassis, or a chassis is removed from or added to a stack.
Entity Insert	A power supply or card is installed in a chassis, or a chassis is added to a stack.
Entity Remove	A power supply or card is removed from a chassis, or a chassis is removed from a stack.
Entity Reset	A chassis or card is reset.
Power Supply Status Change	Power supply status changes from ON to OFF or vice versa.

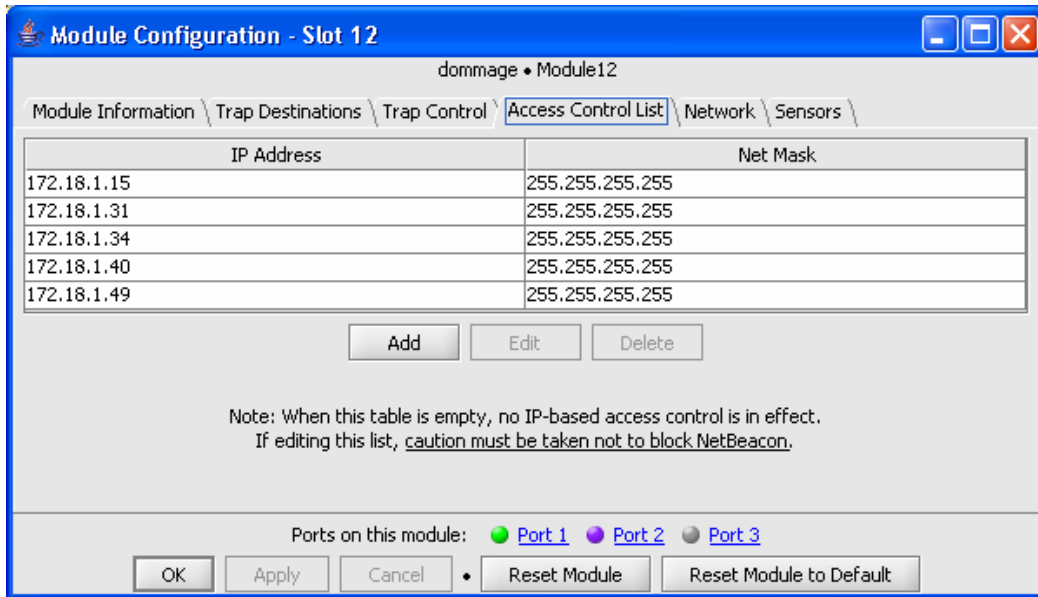
Name	Trap Event
Ethernet Port Link Status Change	The presence of link on an Ethernet port is lost or detected.
Sonet Port Link Status Change	The presence of link on a SONET port is lost or detected.
Sensor Threshold	The temperature or voltage exceeds the limits on a management card, services line card, or access line card; or the fiber optic power level is exceeded on an access line card or any line card with SFP optics that support diagnostics.
Redundant Switch Over	The active port changes from the primary to the secondary port on a redundant interface line card.
Ethernet Remote Fault Alarm	A remote card's Ethernet fiber port loses its receive link.
Ethernet Port Speed Change	The speed on an Ethernet port is changed.
TDM Port Link Status Change	The presence of link on a TDM port is lost or detected.
TDM Remote Fault Alarm	A remote TDM card's fiber port loses its receive link.
Enet Port Far End Fault Alarm	A remote R133 card's fiber port receiver fails to detect link.
MultiRate Port Link Status Change	The presence of link on a multi-rate port is lost or detected.
Dying Gasp	The power level in the peer device falls below its minimum operating value.

3. Check to enable a trap, or uncheck to disable a trap.
4. Click **OK**.

### ***Configuring the Access Control List***

By default, IP-based access control is disabled (i.e., the Access Control List is empty). When adding items to the Access Control List, make sure the system where the NetBeacon Element Manager resides is added to the list first, otherwise you will not be able to manage the element through NetBeacon. Only systems included in the Access Control List will have access to the element. To add, remove, or change an entry into the Access Control List for the selected element, do the following:

1. Open the Module Configuration dialog box for the element's management card.
2. Select the **Access Control List** tab.



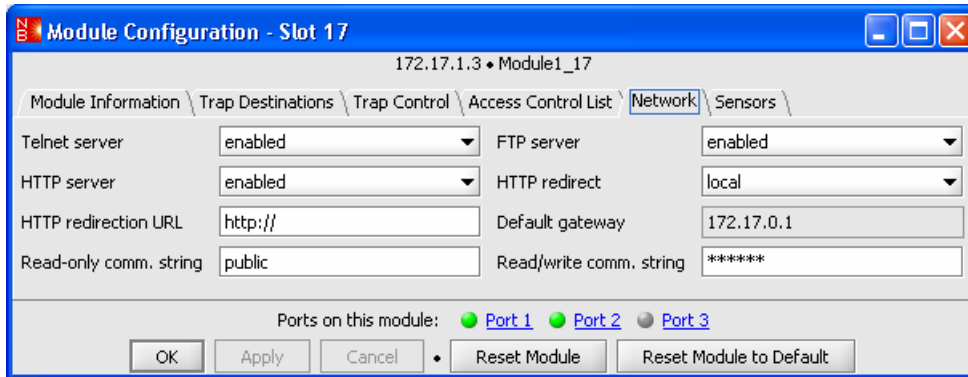
3. To add an entry, do the following:
  - Click **Add**. The Add Address to ACL dialog box appears.
  - In the IP Address text box, type the *IP address* of the system which should have access to the element.
  - In the Net Mask text box, type the system's netmask. The default is 255.255.255.255.
  - Click **OK**. The new entry is added to the table.
4. To change an entry's IP address or netmask, do the following:
  - Double-click the entry in the Access Control List. The Edit ACL Entry dialog appears. Alternatively, you can select the entry and click **Edit**.
  - In the IP Address text box, type the new *IP address*.
  - In the Net Mask text box, type the system's new netmask.
  - Click **OK**.
5. To remove an entry from the Access Control List, do the following:
  - Select the entry you want to remove and click **Delete**. The element is eliminated from the table.
  - Click **OK**.



## Configuring Management Module Network Settings

To configure the network settings on the management card, do the following:

1. Open the Module Configuration dialog box for the management card.
2. Select the **Network** tab.

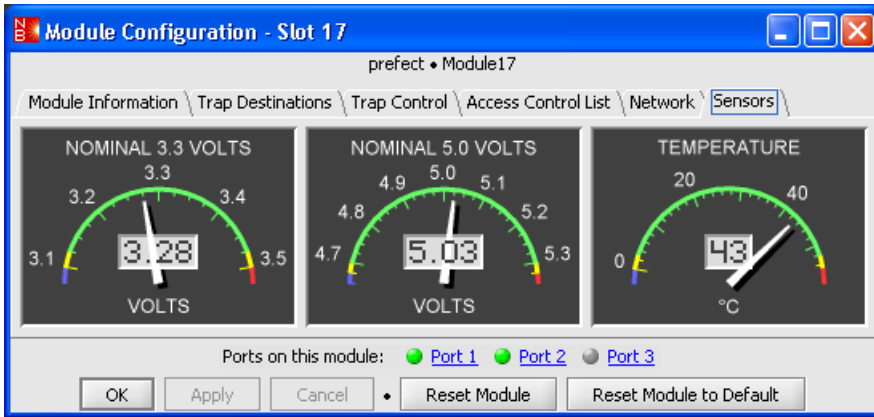


3. Set the Telnet server to **enabled** or **disabled**.
4. Set the FTP server to **enabled** or **disabled**.
5. Set the HTTP server to **enabled** or **disabled**.
6. Set HTTP redirect to **local** to set the Web server so it points to the local system, or set it to **redirected** to redirect it to another IP address or URL.
7. In the HTTP redirection URL text box, type the *IP address* or *URL* where the Web server will go, if the Web server is redirected away from the local system.
8. The default gateway is provided for display purposes only. It cannot be changed.
9. In the read-only community string text box, type the *SNMP community string* for read-only access to the element. The default is public.
10. In the read/write community string text box, type the *SNMP community string* for read-write access to the element. The default is public.
11. Click **OK**.

## Viewing Management Card Sensors

To display gauges for the management module's internal voltage supplies and temperature sensor, do the following:

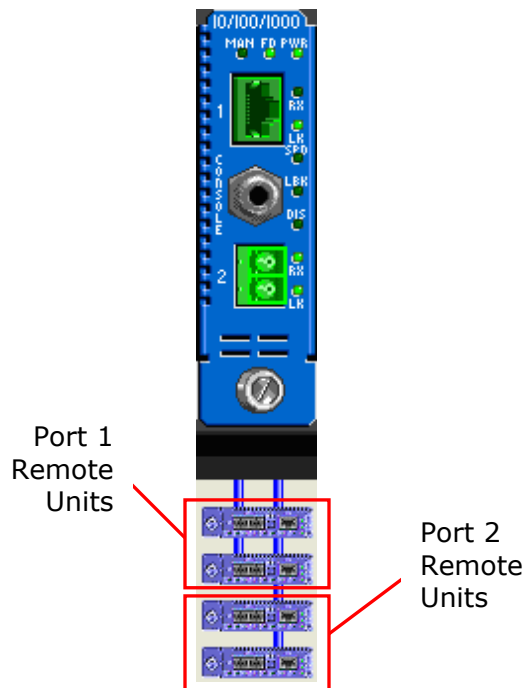
1. Open the Module Configuration dialog box for the management card.
2. Select the **Sensors** tab.



## Configuring the Services Line Card

### *Viewing Remote Services Lines*

In the chassis view, remote services line cards appear below the card to which they are connected. Up to two remote cards are supported per port. When remote cards are connected to both ports, the remote units off Port 1 are shown above the units off Port 2. Port 1 remote units are displayed with a blue line drawn toward the left side of the remote card. Remote units connected to Port 2 are shown below all remote units connected to Port 1. Port 2 remote units are shown with a blue line drawn toward the right side, as illustrated in the following example.



NetBeacon supports three configurations of the Radiance services line card:

- A standalone Network Interface Device (NID) with its own IP address. NetBeacon communicates directly with the SNMP agent on the services line card.
- A book-ended configuration with one services line card in a managed chassis and another card in a remote location. The cards may be connected through either port. Using IEEE 802.3ah, NetBeacon and the R502-M management card provide proxy management of the remote services line card without the need for a second IP address.
- A daisy chain configuration with one services line card in a managed chassis, a second card connected to first card, and a third card connected to the second. Each local port can support up to two remote units. Using IEEE 802.3ah, NetBeacon and the R502-M management card provide proxy management capabilities to all the remote services line cards without using additional IP addresses.

1. In the chassis view, double-click the services line card.

The services line card's Module Configuration dialog box contains four tabs: Module Information, Network, Firmware, and Sensors. When a services line card is managed directly as a standalone NID using its own IP address, there is no Module Configuration dialog box associated with it. Instead, the lower right panel displays additional tabs such as Network, Firmware, and Sensors.

2. Click on a tab to perform the tasks listed below.

### **Network**

- Assign a new IP address, network mask, and/or default gateway.
- Reconfigure the processing mode for end-station ICMP messages.
- Set the SNMP community string for any of the three access profiles (read-only, read-write, or admin).
- Enable or disable DHCP client operation.
- Specify the maximum number of attempts to acquire an IP address through DHCP before reverting to the valid IP address.
- Enable or disable the card's management Layer 3 capability to receive and transmit IP packets. (Not applicable to standalone NIDs.)
- Change the management VLAN ID number.
- Specify the timeout period which takes the unit out of loopback mode.

The following are only applicable to the 10/100Mbps standalone NID.

- Configure Logical Services Loopback (LSL).
- Specify the LSL multicast address.

- View the LSL unicast address.
- View the total number of LSL packets that have been looped.
- Set the switch forwarding mode: transparent or IEEE 802.1Q.
- Enable or disable Q-in-Q operation.

### **Firmware**

- View the FPGA and OS version stored in the primary and secondary locations.
- Change the active image of the operating system or FPGA.
- Specify the parameters that will be used for downloading firmware.
- Download firmware onto the services line card.
- View the status of the upgrade process.

### **Sensors**

- View the current readings on the services line card's four voltage supply sensors.
- View the current temperature of the circuit board.

The following tabs only appear in the lower right panel of the NetBeacon main window when the services line card is managed directly as a standalone NID.

### **Trap Manager/ARP/VLAN**

- Add an entry to the SNMP Trap Manager table.
- Change a trap manager's IP address, UDP port number, SNMP community string, SNMP version number, or the SNMPv3 security name.
- Remove one or more trap managers.
- Add an entry to the ARP (Address Resolution Protocol) table.
- Change an ARP entry's IP address, MAC address, or its dynamic/static setting.
- Remove one or more ARP entries.
- Specify the user VLAN ID number(s) on both ports.
- Remove one or more user VLANs.

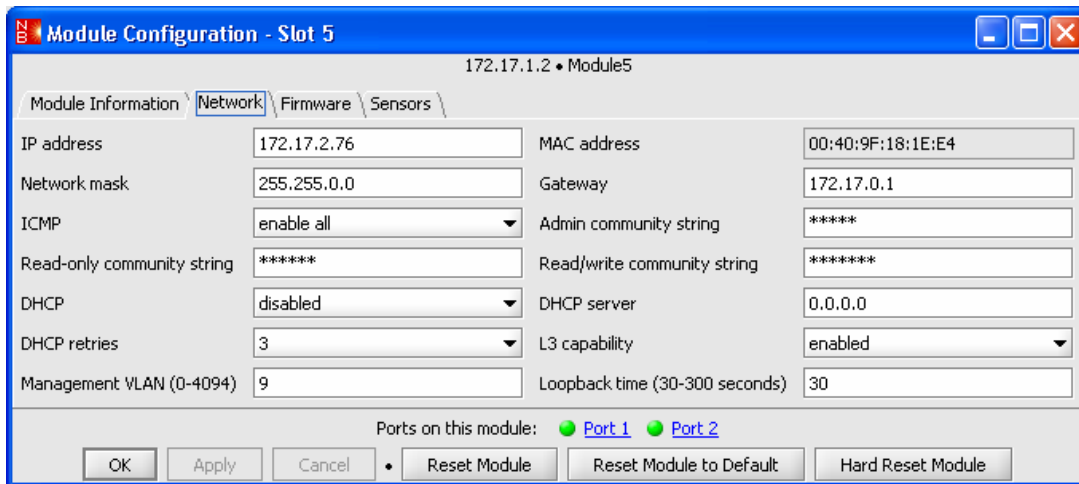
### **Traffic Management**

(Only applicable to the standalone 10/100Mbps services line card NID.)

- Specify the traffic classification mode (DSCP or P-bits) that will take precedence in determining the priority of data when both modes are enabled.
- Enable or disable DSCP or P-bits mode.
- Select the DSCP model to use when DSCP mode is enabled.
- Select the P-bits model to use when P-bits mode is enabled.
- Specify the queues to which DSCP or P-bits will be mapped using a free form option.
- Change any of the traffic prioritization settings.

### Changing Network and Management Settings

In the services line card Module Configuration dialog box, click the **Network** tab.



Name	Description
IP address	IP address of the services line card.
MAC address	MAC address of the services line card.
Network mask	The services line card's network prefix, or mask.
Gateway	The services line card's default route.
ICMP	The operational mode for processing ICMP messages. The options are to enable or disable all messages or to only enable unicast ICMP messages.
Admin community string	A text string that provides a community user with full read-write access to all objects.
Read-only community string	A text string that provides a community user with read-only access to non-privileged objects.

Name	Description
Read/write community string	A text string that provides a community user with read-write access to non-privileged objects.
DHCP	Operational mode of the DHCP client.
DHCP server	IP address of the current DHCP server.
DHCP retries	Number of address acquisition attempts before reverting to using the last known valid IP address. The range is 1 to 5.
L3 capability	Choose <b>enabled</b> to allow all Layer 3 IP packets destined for the card's management port to be received and to allow the management port to transmit IP packets. Choose <b>disabled</b> to prevent the reception and transmission of all Layer 3 IP packets to/from the management port.  NOTE: This parameter is only available for services line cards in a chassis managed by an R502-M management card. It is not applicable to standalone NIDs.
Management VLAN	The management VLAN identifier (VID). The range of valid IDs is 0 to 4094. To disable management VLAN, set the VID to 0.
Loopback time	Maximum number of seconds to remain in loopback mode. The timeout period can be set from 30 to 300 seconds. To enable loopback, open the Port Configuration dialog box for a port by double-clicking on it in the chassis view, and set Loopback to <b>enabled</b> .  NOTE: For the R851 GigE services line card, loopback cannot be set on Port 1.

The following fields are only applicable to the 10/100Mbps services line card standalone NID under direct management.

Logical Services Loopback (LSL) State	disabled	LSL Unicast Address	00:40:9F:18:1F:78
LSL Multicast Address	00:00:00:00:00:00	LSL Total Packets	0
Switch State	802.1Q	Q-in-Q	disabled

Name	Description
Logical Services Loopback (LSL) State	Identifies the state of LSL: disabled, enabled for unicast only, enabled for multicast only, or enabled for both multicast and unicast. When enabled, only frames with the specified MAC address(es) are looped.
LSL Unicast Address	The unicast MAC address to be used by LSL.
LSL Multicast Address	The configurable multicast MAC address to be used by LSL.
LSL Total Packets	Total number of unicast and multicast packets that have been looped.

Name	Description
Switch State	Select the forwarding mode. In transparent mode, tagged and untagged frames are forwarded without modification. In 802.1Q mode, the R821 complies with IEEE 802.1Q VLAN bridge forwarding aspects.
Q-in-Q	Enable or disable Q-in-Q operation. When enabled, untagged frames are tagged with the PVID as they egress out the trunk port, and tagged frames are double tagged with the PVID as the outer tag. When disabled, double-tagging is not applied.

### Configuring Logical Services Loopback

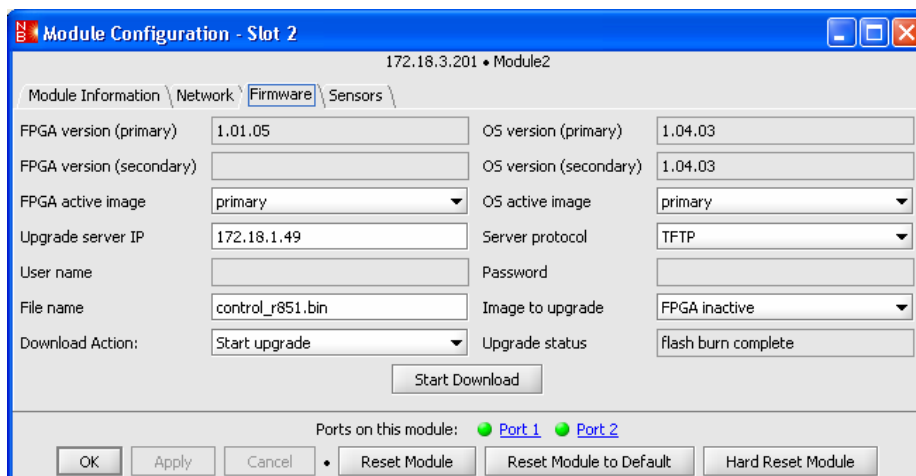
- To configure LSL, select one of the options from the Logical Services Loopback (LSL) State drop-down list.
  - disabled** – disables Logical Services Loopback.
  - all** – enables LSL and all frames that match the specified unicast or multicast MAC addresses will be looped.
  - unicast** – enables LSL and all frames that match the factory-assigned unicast MAC address will be looped.
  - multicast** – enables LSL and all frames that match the user-defined multicast MAC address will be looped.
- In the LSL Multicast Address text box, type the *multicast MAC address* to be used by LSL.

**Important:** The first two bits of the multicast address must be set to **1**. That is, the Global/Local (G/L) bit and the multicast bit must be set to 1.

- Click **Apply**.

### Upgrading the Firmware

- To upgrade or to display the current status of the embedded software on the card, click the **Firmware** tab.



Name	Description
FPGA version (primary)	Version number of the primary FPGA embedded software.
FPGA version (secondary)	Version number of the secondary FPGA embedded software
FPGA active image	Indicates which of the two FPGA images, primary or secondary, is active.
OS version (primary)	Version number of the primary operating system software.
OS version (secondary)	Version number of the secondary operating system software.
OS active image	Indicates which of the two OS images, primary or secondary, is active.
Upgrade server IP	IP address of the host server used to download new firmware onto the card.
Server protocol	Specifies whether the host server will use FTP or TFTP to transfer the firmware. NOTE: Currently, NetBeacon only supports TFTP.
User name	The login user name. Only applicable to FTP.
Password	The password associated with the login user name. Only applicable to FTP.
File name	Name of the file to download.
Image to upgrade	Specifies which of the images will be replaced by the new firmware, where it will be stored, and the reset option, if applicable.
Download action	Specifies downloading options between the services line card, the management card, and any remote cards connected to the local services line card.  NOTE: This parameter is only available for services line cards in a chassis managed by an R502-M management card. It is not applicable to standalone NIDs.
Upgrade status	Displays the progress of downloading the firmware.
Start Download	Activates the download process.

2. To change the active FPGA or OS image, select **primary** or **secondary**.
3. In the upgrade server IP text box, type the *IP address* of the host server from which to download the firmware.



4. Select the protocol (**FTP** or **TFTP**) to use when downloading the firmware from the host server. NOTE: Currently, the services line card firmware only supports downloading via TFTP.
5. If you selected FTP, enter the login *user name* and *password* in the next two text boxes. These fields are not applicable to TFTP.
6. In the file name text box, type the *name* of the file you want to download.
7. From the list of images to upgrade, select an option that specifies where to download the new firmware and if any additional actions should be performed. The following table describes the actions associated with each option.

Name	Description
OS primary or FPGA primary	Downloads new firmware into the primary OS or FPGA location.
OS secondary or FPGA secondary	Downloads new firmware into the secondary OS or FPGA location.
OS inactive or FPGA inactive	Downloads new firmware into the inactive OS or FPGA location.
OS w/set or FPGA w/set	Downloads new firmware into the inactive OS or FPGA location, and sets the new location as active. No change occurs until the next reset, when the new software will be activated.
OS w/reset or FPGA w/reset	Downloads new firmware into the inactive OS or FPGA location, sets the new location as active, and immediately resets the card. The new firmware is activated.
OS w/set to default or FPGA w/set to default	Downloads new firmware into the inactive OS or FPGA location, sets the new location as active, and immediately resets the card to its factory default settings. The new firmware will be activated only if it is downloaded to the default location (primary).
config primary image	Downloads a new configuration script file into the primary location.
config secondary image	Downloads a new configuration script file into the secondary location.
boot loader	Overwrites the existing boot loader code.

8. For a standalone NID, go to the next step.

If the R502-M is serving as the proxy-manager for the services line card, select one of the options provided in "After applying settings" drop-down list.

Name	Description
Start upgrade	Starts downloading the file directly onto the services line card.

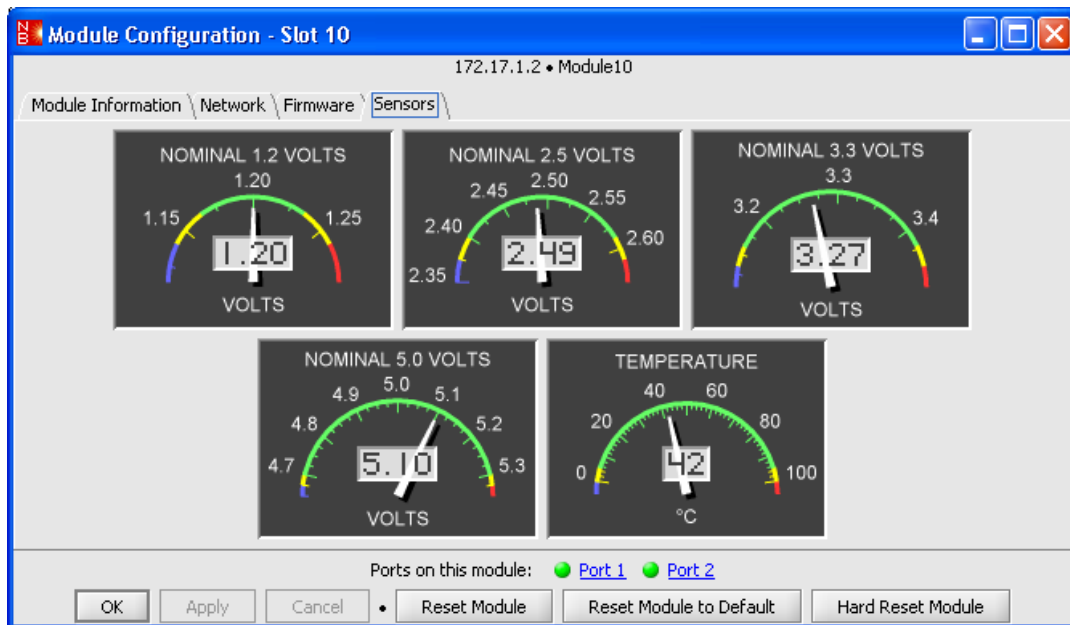
Name	Description
Start proxy upgrade after TFTP transfer	Downloads the file via TFTP to the R502, then transfers the file from the R502-M to the services line card through the chassis backplane.
Start proxy upgrade, no TFTP transfer	Starts downloading the file from the R502-M to the services line card through the chassis backplane.
Start proxy chained upgrade after TFTP transfer	Downloads the file via TFTP to the R502, transfers the file from the R502-M to the services line card through the chassis backplane, and then upgrades all remote cards connected to the services line card.
Start proxy chained upgrade, no TFTP transfer	Starts downloading the file from the R502-M to the services line card through the chassis backplane, and then upgrades all remote cards connected to the services line card.

9. Click **Apply**.

10. To begin downloading the firmware, click **Start Download**. You can monitor the progress through the Upgrade status field.

NOTE: If the services line card is communicating directly with NetBeacon, and not through a management card, the Admin text box in the Element Settings dialog box in the NetBeacon EM Admin Tool must contain the correct SNMP administrative access string. If the field is missing or incorrect, an SNMP timeout error message will appear about a one minute after you click the Start Download button.

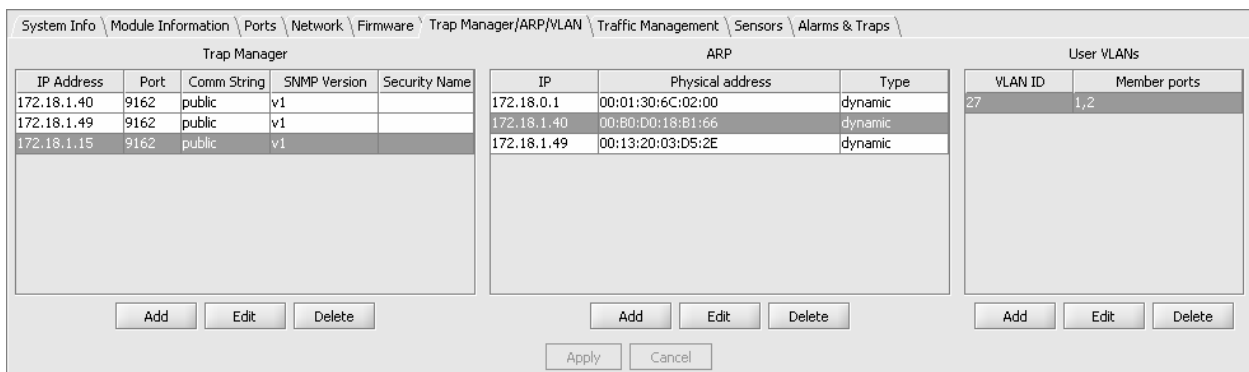
### Viewing Temperature and Voltage Measurements



To view the various environmental monitors available on the services line card, click the **Sensors** tab. The dialog box displays the temperature of the board along with the current readings for its 1.2, 2.5, 3.3 and 5.0-volt supplies. The 5.0-volt supply is the input power source for the services line card. The other supplies are used to power various components on the circuit board. Each monitor has a warning threshold and an alarm threshold to indicate when the level is too high or low. To prevent a potential problem, a trap can be set so an alarm is sent to the network manager if any threshold is crossed.

### Setting SNMP Trap Destinations

This option is only available for a standalone NID. Click the **Trap Manager/ARP/VLAN** tab. The services line card supports up to four SNMP trap destination hosts.



1. Under the Trap Manager section, click **Add** to create a trap destination entry.



2. In the IP Address text box, type the *IP address* of the destination server or device where SNMP traps will be sent.
3. In the Port text box, type the trap manager's *UDP port number*. The default number is 9162. Port 162 is the standard SNMP trap port.
4. In the Comm String text box, type the *SNMP community string* denoting the receive profile on the trap destination host. The default is public.

5. Select **v1**, **v2**, or **v3** from the drop-down list to set the SNMP version that will be used to send trap messages. The default is version 2.
6. In the Security Name text box, type the user name for SNMPv3 traps. This field is required only if you specified v3 in the previous step.
7. Click **OK**.
8. After a trap destination has been added to the table, you can change any of the fields by clicking the **Edit** button. Click **OK**.
9. To remove one or more trap destination entries, select it/them from the table and then click **Delete**.
10. Click **Apply**.

### *Configuring the ARP Table*

This option is only available for a standalone NID. Click the **Trap Manager/ARP/VLAN** tab.

ARP		
IP	Physical address	Type
172.18.0.1	00:01:30:6C:02:00	dynamic
172.18.1.40	00:80:D0:18:B1:66	dynamic
172.18.1.49	00:13:20:03:D5:2E	dynamic

1. Click **Add** to configure a new entry for the Address Resolution Protocol (ARP) table, which maps IP addresses to hardware MAC addresses.

NetBeacon - Add ARP Entry

IP:

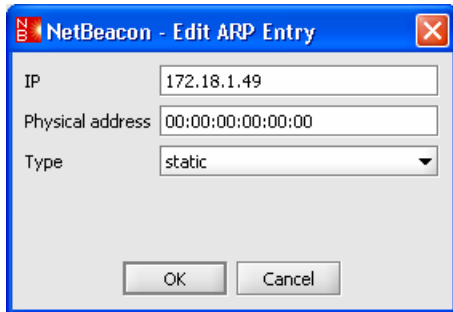
Physical address:

Type:

OK Cancel

2. In the two text boxes, type the *IP address* and *MAC address* for a device.
3. Set the ARP entry type to **dynamic** or **static**. Dynamic entries are automatically removed through aging; static entries are never deleted until they are removed.

4. Click **OK**.
5. The services line card supports up to five ARP entries, including up to four static entries. Repeat Steps 1 through 4 above to configure additional entries.
6. After an ARP entry is configured, you can make changes by clicking the **Edit** button.



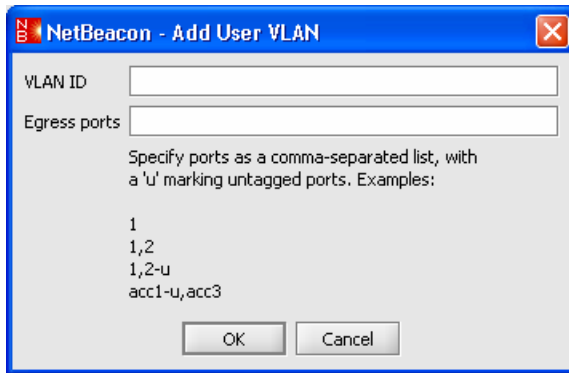
7. Change the any of the settings, as described in steps 2 and 3.
8. Click **OK**.
9. To remove an ARP entry, select it from the table and then click **Delete**.
10. Click **Apply**.

### *Assigning User VLANs*

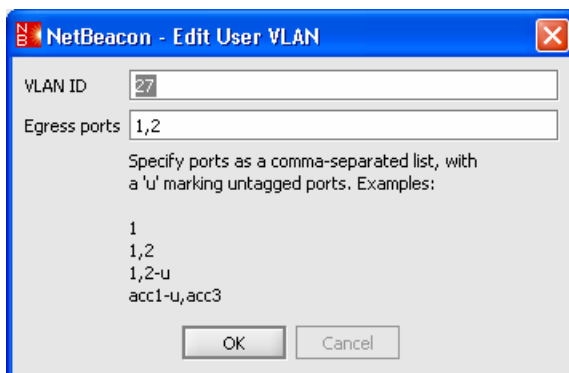
This option is only available for a standalone NID. Click the **Trap Manager/ARP/VLAN** tab.

VLAN ID	Member ports
26	1,2
27	1,2

1. Click **Add** to configure a user VLAN.



2. In the VLAN ID text box, type the *user VLAN ID number* you want to assign. The number must be in the range 1 to 4094. The user VLAN ID must be different from any previously provisioned management VLAN ID number.
3. In the egress ports text box, type **1,2** to apply the user VLAN to both ports. (For two-port devices such as the R851 and R821, user VLANs are only effective when both ports are members.) For multi-port devices such as the RS960, you must include the port type (e.g., 'net2' for network port 2, or 'acc3' for access port 3). To remove the specified user VLAN tag from frames that egress the access port, add '-u' next to the port number (e.g., **1-u, 2**). Untagging is not allowed on the trunk port on the services line cards. Untagging is only applicable in IEEE 802.1Q mode.
4. Click **OK**.
5. The services line card supports up to 16 user VLANs. Repeat Steps 1 through 4 above to configure additional user VLANs.
6. Once a user VLAN is created, you can change the VLAN ID number by clicking the **Edit** button. Note that although the egress ports can be changed, both Port 1 and Port 2 must be identified with each user VLAN for proper operation. Click **OK**.



7. To remove a user VLAN, select the entry from the table and then click **Delete**.
8. Click **Apply**.

## Prioritizing Traffic Classes

This option is only available for a standalone R821 NID. The R821 supports Class of Service (CoS) with four priority queues (0 low, 3 high). CoS allows you to assign mission-critical data to a higher priority, so they are processed before less critical traffic during times of network congestion. The four CoS queues determine the priority for transmitting data. Queues are based on any of the following classifications:

- Priority bits (P-bits) in the VLAN header
- DSCP/TOS (differentiated services code point / type of service) bits in the header of IP frames
- Default port priority bits

### Precedence

By default, both P-bits and DSCP classifications are disabled, and only default port priority is used to determine the queue for each incoming frame. The default port priority state is always enabled, however the other two classifications may be enabled/disabled independently.

All traffic prioritization settings are configured through the Traffic Management tab, except the default port priority binary bits setting, which is configured under the Port Configuration Details dialog box.

To configure traffic prioritization, do the following:

1. Click the **Traffic Management** tab.

The screenshot shows the 'Traffic Management' configuration page. At the top, there are navigation tabs: System Info, Module Information, Ports, Network, Firmware, Trap Manager/ARP/VLAN, Traffic Management (selected), Sensors, and Alarms & Traps. Below the tabs, there are several configuration options:

- Precedence:** A dropdown menu set to 'DSCP'.
- DSCP state:** A dropdown menu set to 'enabled'.
- DSCP model:** A dropdown menu set to 'class'.
- P-bits state:** A dropdown menu set to 'enabled'.
- P-bits model:** A dropdown menu set to '802.1D'.

Below these settings are two tables. The left table is for DSCP bits and the right table is for P-bits. Both tables have columns for the classification bits and the corresponding Queue number.

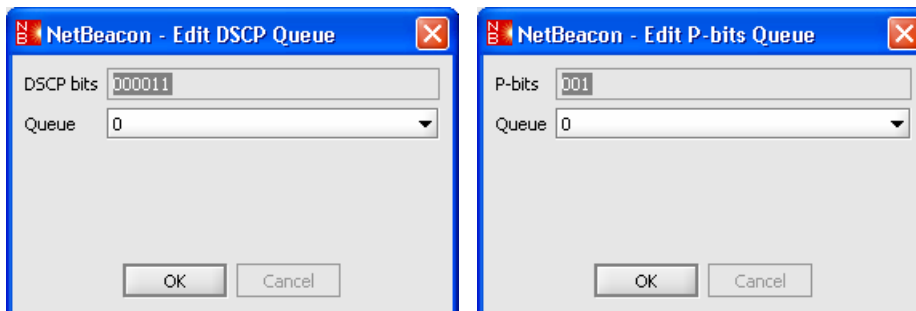
DSCP bits	Queue
000000	2
000001	0
000010	0
000011	0
000100	0
000101	0
000110	0
000111	0
001000	0

P-bits	Queue
000	1
001	0
010	0
011	1
100	2
101	2
110	3
111	3

At the bottom of the configuration area, there are 'Edit' buttons for each table, and 'Apply' and 'Cancel' buttons at the very bottom.

2. To specify which classification (DSCP or p-bits) will take precedence when both are enabled, select **DSCP** or **P-bits** from the Precedence drop-down list.

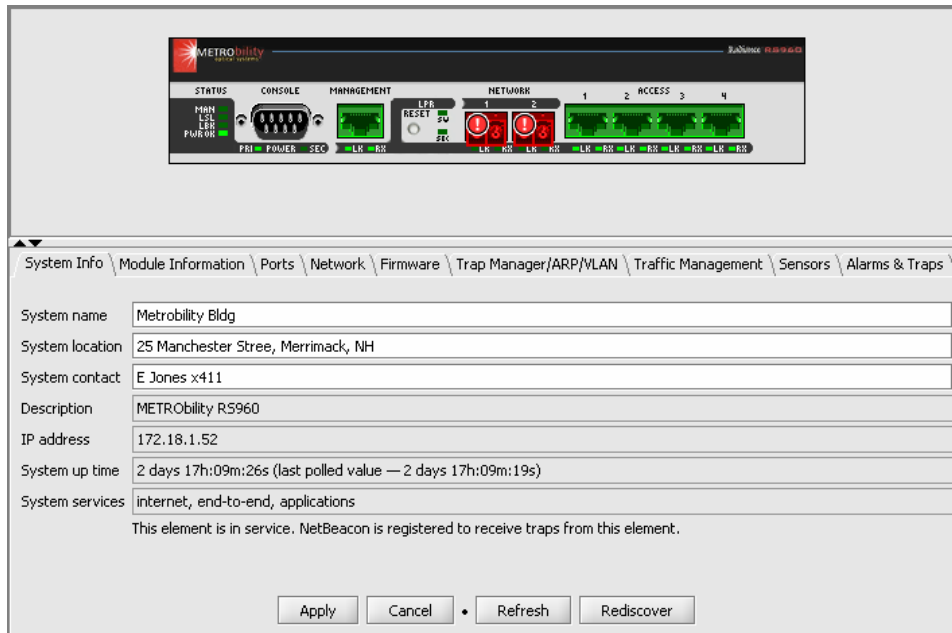
3. Select **enabled** or **disabled** from the DSCP state and/or P-bits state drop-down list(s) to activate classification based DSCP and/or P-bits.
4. If you want to use DSCP classification to determine traffic prioritization, select a policy model to use from the DSCP model drop-down list. The first four options support a pre-determined DSCP bit value to queue mapping which appears in the table when you click **Apply**.
5. If you want to use P-bits classification, select **802.1D** or **provider bridge** from the P-bits model drop-down list. Both options support a P-bits to queue mapping which appears in the table when you click **Apply**.
6. To customize the DSCP or P-bits to queue mapping, select the **free form** option from the model list. When free form is chosen, the queue for any table entry may be modified. To make a change, click **Edit**. The Edit DSCP or P-bits Queue dialog box appears. Select a queue from the drop-down list, then click **OK**.



7. Click **Apply**.

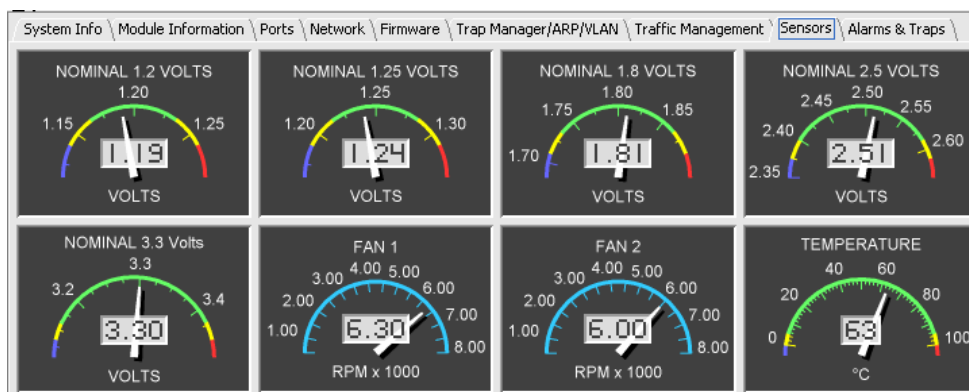


## Configuring the RS960



The RS960, shown above, is a standalone Ethernet services provisioning platform with two network ports and four access ports. It supports the Metro Ethernet Forum (MEF) services model with four domains, one Ethernet virtual connection (EVC) per user network interface (UNI), and four UNIs. NetBeacon currently does not support MEF configurations. The RS960 is designed to deliver services (voice, video, data) over virtual Ethernet in the Metro Ethernet Network (MEN).

The RS960 provides the same tabs that appear for standalone services line card NID. The only differences are that the RS960 does not support user VLANs (they may be configured through NetBeacon, but they have no effect); ports are identified as Management, Network, or Access; and NetBeacon does not support traffic management for the RS960. The RS960 also includes additional gauges under the Sensors tab, as shown below. The two fan gauges display the primary and secondary fans' rotational speed in revolutions per minute.





## Chapter 7. Configuring the Ports

Many features such Link Loss Return and RMON statistics are only applicable on a port basis. This chapter describes all the port functions available on the various modules and devices.

The Ports tab displays information about the ports on the selected element. If the element is a stack of two or more chassis, the ports on all chassis in the stack will be displayed.

### Displaying Port Details

Click the **Ports** tab to display the Ports table. The information in this table is for display purposes only and cannot be changed.

Location	Name (Alias)	Type	Link Status	Speed (Mbps)	Up Time
Slot 1, Port 1	Port1_1	e1000Base-LX	link up	1000	day 000 00h:00m:00s
Slot 1, Port 2	Port1_2	e1000Base SM 1310/1550	link up	1000	day 000 00h:00m:00s
Slot 3, Port 1	Port3_1	T3	link up	44.736	day 000 00h:00m:00s
Slot 3, Port 2	Port3_2	T3-F-SM	link up	44.736	day 009 02h:35m:32s
Slot 4, Port 1	Port4_1 (Metrobility ENG)	E1	link down	2.048	day 000 00h:00m:00s
Slot 4, Port 2	Port4_2	E1-F-SM	link down	2.048	day 000 00h:00m:00s
Slot 5, Port 1	Port5_1	e10Base-T	link up	10	day 000 00h:00m:00s
Slot 5, Port 2	Port5_2	e10Base-FL MM	link up	10	day 000 00h:00m:00s
Slot 6, Port 1	Port6_1	e10Base-T	link up	10	day 000 00h:00m:00s
Slot 6, Port 2	Port6_2	e10Base-FL SM	link up	10	day 000 00h:00m:00s
Slot 7, Port 1	Port7_1	e10/100Base-TX	link up	10	day 000 00h:00m:00s
Slot 7, Port 2	Port7_2	e10/100Base-F 1310/1550	link up	10	day 000 00h:00m:00s
Slot 8, Port 1	Port8_1	e10/100Base-TX	link up	10	day 000 00h:00m:00s
Slot 8, Port 2	Port8_2	e10/100Base-F 1550/1310	link up	10	day 000 00h:00m:00s








● Link down  
 ● Signal, no link  
 ● Far-end fault  
 ● Link up  
 ● Disabled  
 ● Disabled, no link  
 ● N/A

The following table lists the information shown under the Ports tab, along with a brief description of each field.

Name	Description
Location	Slot number in the chassis and port number on the card. For ports in a stack: chassis number in the stack, slot in the chassis, and port on the card. For a remote access or services line card, the remote card and port numbers are also included.
Name (Alias)	Default name or user-assigned alias of the port. The alias is in parentheses.
Type	The port's media type.
Link Status	Indicates whether or not link is detected on the port.

Name	Description
Speed (Mbps)	Speed in megabits per second (Mbps). For a serial port, the speed is displayed in bits per second.
Up Time	Length of time the port has been up since it was last reset.

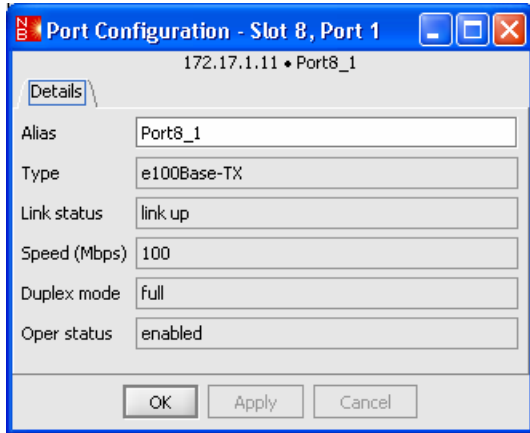
The Ports table uses the same colored bullets to represent the status of the ports as those used in the Network Elements panel. The ports in the chassis view also match the colors in the table.

	A red bullet indicates the port link is down.
	An orange bullet indicates a signal has been detected on the port, but a link could not be established (e.g., there is a speed mismatch).
	A yellow bullet indicates a Far End Fault condition has occurred on the port.
	A green bullet indicates the port link is up.
	A blue bullet indicates the port has been administratively disabled.
	A purple bullet indicates the port is administratively disabled and it has a fault, such as no link or Far End Fault.
	A gray bullet indicates link status is unknown or not applicable to the port (e.g., it is a serial port).

## Opening the Port Configuration Dialog Box

You can view additional port information through the Ports Configuration dialog box. For some cards, such as the redundant interface line card, the only information you can change in the dialog box is the port name. This section describes the Port Configuration details.

1. Open the Port Configuration dialog box by doing one of the following:
  - Under the Ports tab, select a port by double-clicking it.
  - Double-click the port in the chassis view.
  - In the Network Elements panel, right-click on the desired port and select **Show configuration dialog** from the pop-up menu.
  - At the bottom of the Module Configuration dialog box, click on the blue hyperlink for the port information you want to view.



The first four fields in the Port Configuration dialog are identical to those in the Ports table. The duplex mode indicates whether the port is in full or half duplex. The oper status gives the port's operational status, either enabled or disabled.

2. In the Alias text box, type the *name*<sup>3</sup> to assign to the port.
3. Do one of the following:
  - Click **OK** to save the change and close the dialog box.
  - Click **Apply** to save the change and keep the dialog box open.
  - Click **Cancel** to close the dialog box without saving any of the changes.

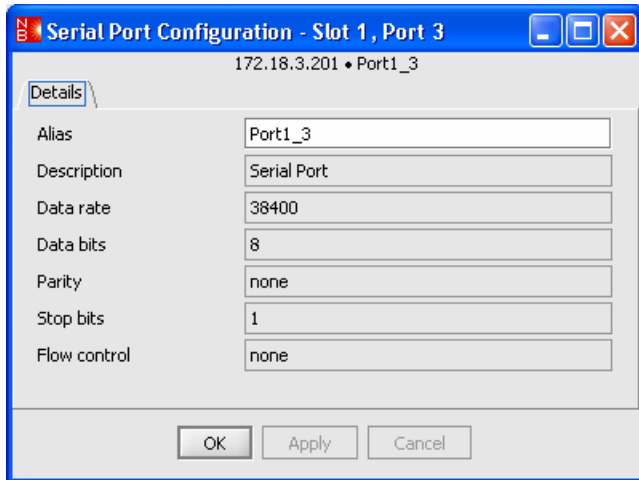
**Tip:** For simplicity, this manual instructs you to click **OK** after making configuration changes, however, you may also click **Apply**.

### ***Displaying Serial Port Information***

To view information about the serial port on the management card, double-click on the port in the chassis view or on the row in the Ports table. The Serial Port Configuration dialog appears. The only field you can change is the alias.

---

<sup>3</sup> There is a limit of 32 characters for the port name. Do not use the following characters: . ; & = : " < > .



Name	Description
Alias	Default name or user-assigned alias of the port. The alias is in parentheses.
Description	The type of port.
Data rate	Baud rate of the serial port.
Data bits	The number of data bits.
Parity	Metrobility serial ports have no parity.
Stop bits	The number of stop bits.
Flow control	Metrobility serial ports do not support flow control.

## Applying Link Loss Return

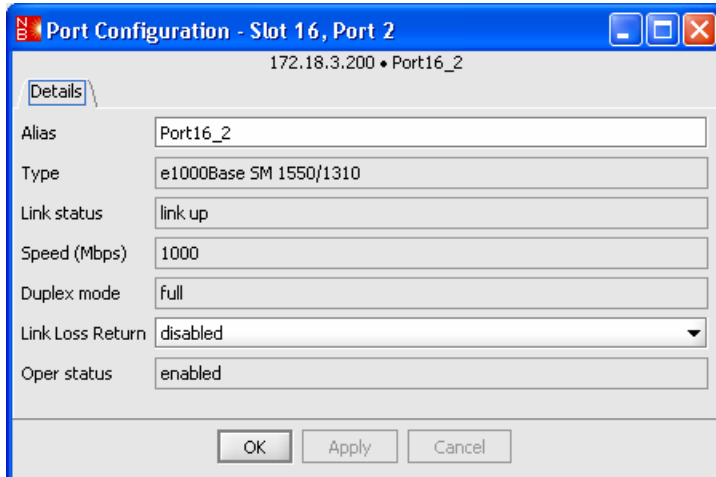
In addition to the name, you can enable or disable Link Loss Return<sup>4</sup> (LLR) on any fiber port with this feature. LLR typically is used in conjunction with Link Loss Carry Forward (LLCF). When a lost link signal is returned to an unmanaged card, the lost link must then be carried forward to a managed device for trap generation.

When LLR is enabled, the port's transmitter will shut down if its receiver fails to detect a valid receive link. LLR should only be enabled on one end of a link and is typically enabled on the unmanaged or remote device.

To apply LLR, do the following:

1. Open the Port Configuration dialog box for a fiber port that supports this feature.

<sup>4</sup> For additional information, refer to "Link Loss Return" in the user guide for the card you are configuring.



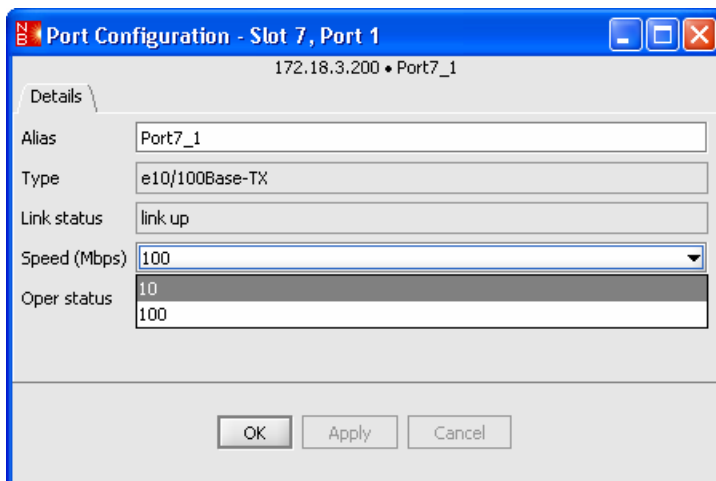
2. Choose **enabled** from the Link Loss Return drop-down list.
3. Click **OK**.

## Setting the Speed on the R141 Line Card

The ports on the R141 line card run at either 10 Mbps or 100 Mbps. Both ports are set to the same speed, which is configured through the copper port (Port 1).

To set the speed on the R141, do the following:

1. Open the Port Configuration dialog box for Port 1 of the R141.



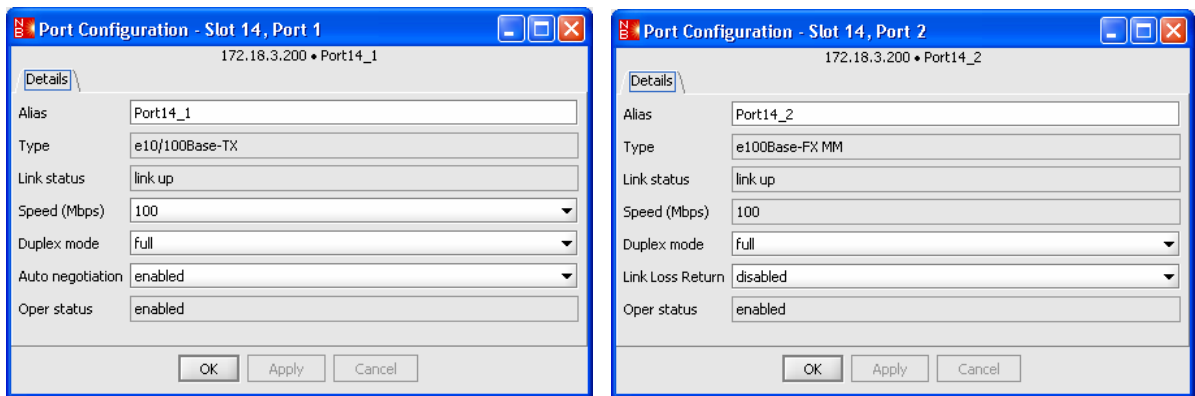
2. Choose **10** or **100** from the Speed (Mbps) drop-down list.
3. Click **OK**.

## Configuring the 10/100Mbps Ports

Depending on the type of 10/100Mbps interface line card (AutoTwister) installed, there are two or three port settings that can be configured through NetBeacon. These include auto-negotiation, duplex, speed, and Link Loss Return. The duplex mode can be changed on any 10/100Mbps port. For a copper port, speed and auto-negotiation can also be changed. For a fiber port, Link Loss Return can be enabled or disabled.

To configure the 10/100Mbps ports, do the following:

1. Double-click the port to configure in either the chassis view or the Ports folder.
2. The Port Configuration dialog box appears. The dialog box for a copper port is shown on the left. The dialog box for a fiber port is shown on the right.



Select the port settings from the drop-down lists. Changing these settings will override the DIP switches<sup>5</sup> on the 10/100Mbps line card.

For a copper port, do any of the following:

- Set Speed (Mbps) to **10** or **100**.
- Set Duplex mode to **half** or **full**.
- Set Auto-negotiation to **disabled** or **enabled**.

For a fiber port, do any of the following:

- Set Duplex mode to **half** or **full**.
- Set Link Loss Return to **disabled** or **enabled**.

3. Click **OK**.

---

<sup>5</sup> Refer to the *Intelligent 7500 10/100 AutoTwister Module Installation and User Guide* or the *Radiance 10/100Mbps Interface Line Cards Installation and User Guide*, Step 2 "Set the Switches," for additional information.

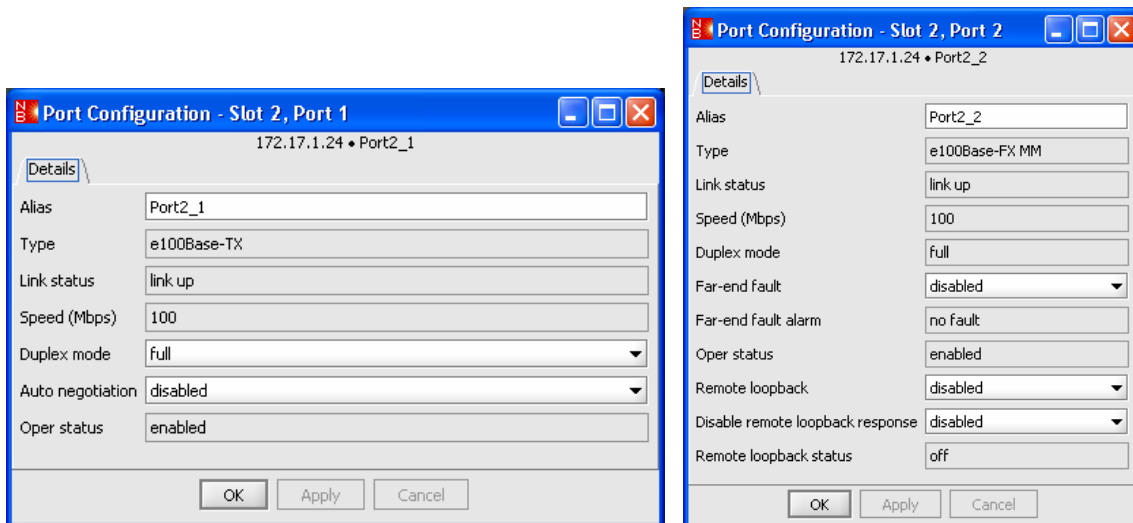


## Configuring the R133 Ports

The 100Mbps TX-FX R133 ports include additional functions that are not available on other single interface line cards. These functions include Far End Fault notification, auto-negotiation, duplex selection, and remote loopback testing.

To configure the R133 ports, do the following:

1. Double-click the port to configure in either the chassis view or the Ports folder.
2. The Port Configuration dialog box appears. The dialog box for a copper port is shown on the left. The dialog box for a fiber port is on the right.



Select the port settings from the drop-down lists.

For a copper port, do any of the following:

- Set Duplex mode to **half** or **full**.
- Set Auto-negotiation to **disabled** or **enabled**.

If auto-negotiation is disabled, the duplex setting will determine the mode at which the port operates. When auto-negotiation is enabled, the copper port will advertise full duplex capability if the duplex mode is set to full. The copper port will advertise half duplex capability if the duplex mode is set to half.

For a fiber port, do any of the following:

- Set Far End Fault (FEF) to **disabled** or **enabled**. When FEF is enabled, the loss of inbound link pulses on the port generates an alarm which is sent out the port's transmitter. FEF also enables the port to read the FEF alarm. To function properly, the FEF setting must be the same on both the local and remote R133 line cards.

- Set Remote loopback to **disabled** or **enabled**. During remote loopback, the R133 card generates a test pattern that is sent to the remote unit, which then returns the test pattern back to the R133 card. The card reads the returned data and verifies proper transmission. To run the remote fiber loopback test, enable Remote loopback and make sure the loopback response setting on the remote unit is also enabled. (If the remote unit is a 100Mbps Delta Class "twister", be sure that its DSLB DIP switch is OFF.)
- Set 'Disable remote loopback response' to **disabled** or **enabled**. This setting determines the response of the fiber port to requests to enter remote loopback. If the setting is enabled, the port will ignore all remote loopback requests. If the setting is disabled, the port will permit remote loopback to occur. That is, it will return the test data back to the sending device.
- View the Remote loopback status box to see if the port is in remote loopback mode.

Changing these settings will override the DIP switches<sup>6</sup> on the R133 line card.

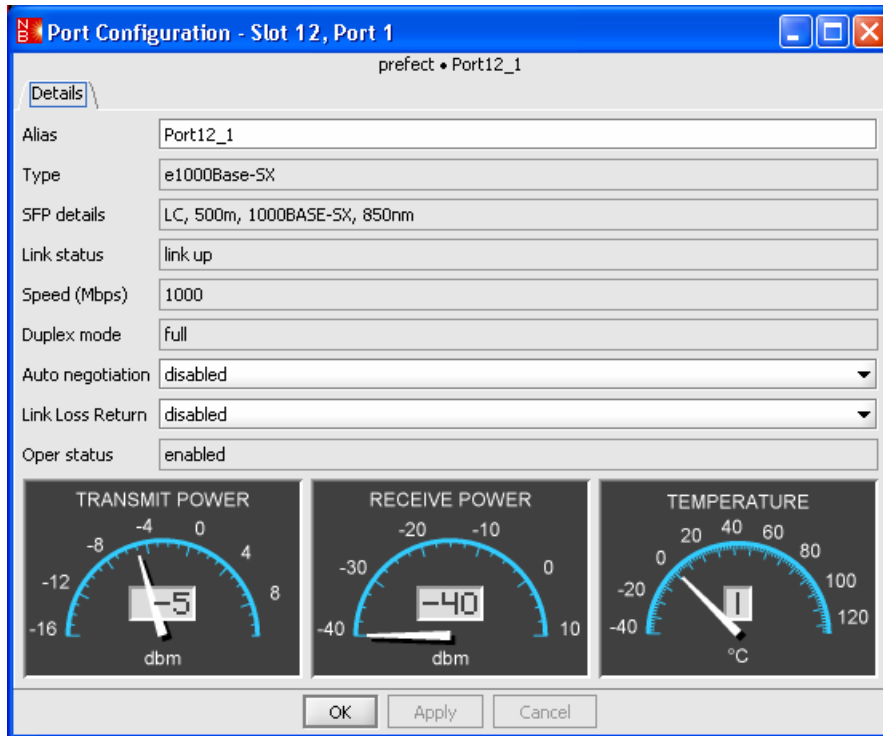
3. Click **OK**.

---

<sup>6</sup> Refer to the *Radiance 100Mbps Single Interface Line Cards Installation and User Guide*, Step 2 "Set the Switches," for additional information.

## Configuring the R153 Ports

The R153 is a 1000Mbps line card with small form-factor pluggable (SFP) optics. Double-click on the fiber port to view the port's optical receive and transmit laser levels, along with its internal temperature reading. Note that the laser levels and temperature are supported only when SFP transceivers with diagnostics are installed.



The Port Configuration dialog box for the R153 (and other cards that use SFP optics) includes a field called 'SFP details.'

SFP details LC, 500m, 1000BASE-SX, 850nm

The SFP field provides the following information about the SFP optic:

- Type of connector (e.g., LC or SC)
- Maximum distance supported in meters or kilometers
- Ethernet media designation
- Wavelength in nanometers

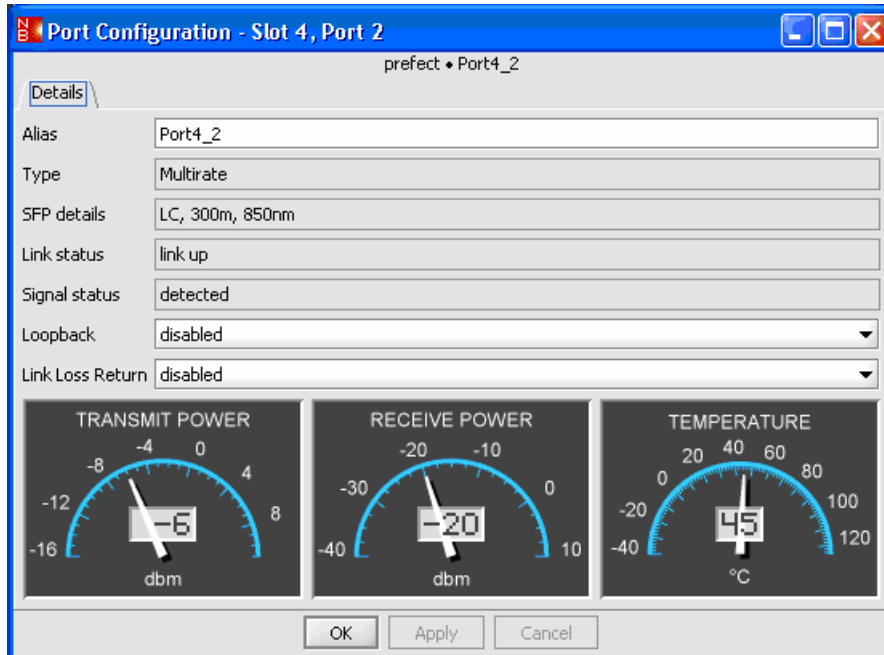
The fiber port(s) on the R153 can be configured to support Auto-negotiation and Link Loss Return. (The copper port on the R153-1S is not configurable.)

1. Select **enabled** or **disabled** from the Auto-negotiation drop-down list.

2. Select **enabled** or **disabled** from the Link Loss Return drop-down list.
3. Click **OK**.

## Configuring the R380 Ports

The R380 is a multi-rate line card with two small form-factor pluggable (SFP) optics. Double-click on either port to view the optical receive and transmit laser levels, along with SFP optic's temperature reading.



The Port Configuration dialog box for the R380 includes the SFP details field, which provides information about the type of connector on the optic, the maximum distance supported by the optic in meters or kilometers, and the optic's wavelength in nanometers.

SFP details LC, 300m, 850nm

Both ports on the R380 can be configured to enable/disable Link Loss Return and Loopback.

1. Select **enabled** or **disabled** from the Link Loss Return drop-down list.
2. Select **enabled** or **disabled** from the Loopback drop-down list. When loopback is enabled, the port's transmitter is connected to its receiver, thus returning incoming data back to the sender. Loopback may be enabled independently on each port. Port loopback does not time out automatically; once it is enabled, the card stays in loopback mode until the setting is changed.
3. Click **OK**.

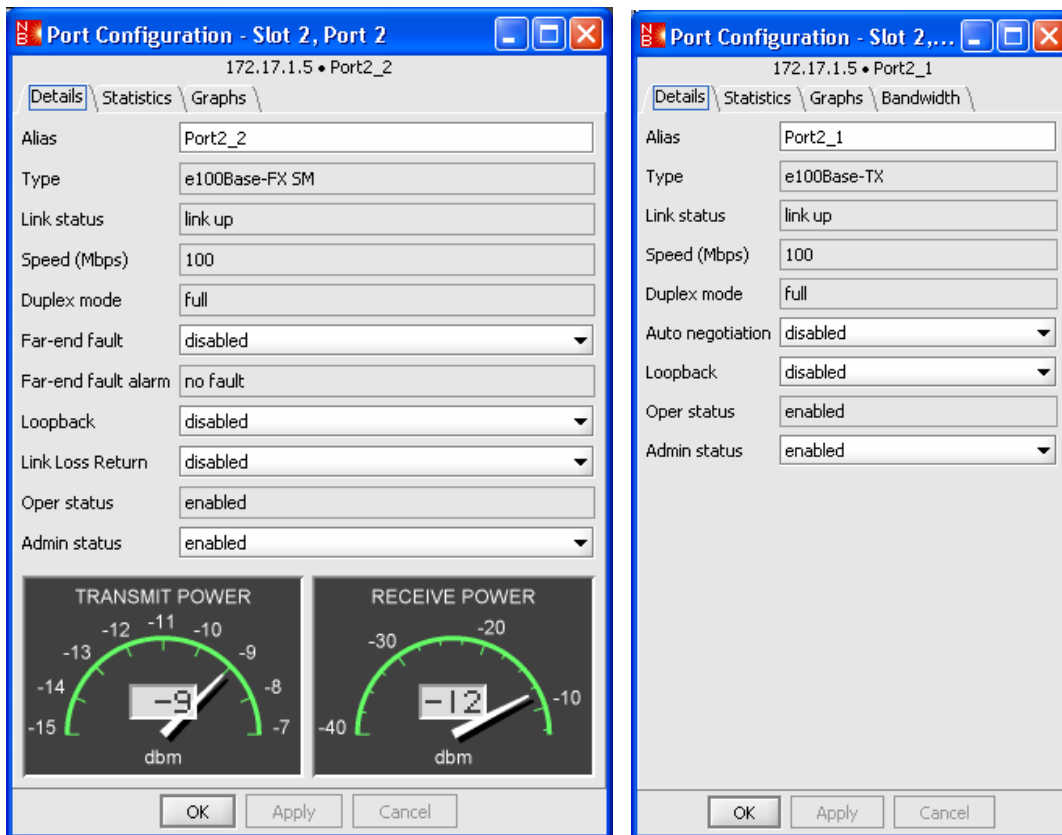
## Configuring the Access Line Card Ports

Using NetBeacon and Metrobility's patented Radiance technology, you can override the hardware switches on a locally managed or remote access line card and modify their internal default settings. You also can view each access line card's RMON port statistics and display data as graphs.

To change the settings on a local or remote access line card, do the following:

1. Double-click the port to configure in either the chassis view or the Ports folder.

The Port Configuration dialog box for a fiber port (left) or a copper port (right) appears.



2. For a fiber port, you can configure the following settings: Far End Fault, Loopback, Link Loss Return, and administrative status. For a copper port, you can configure Auto-negotiation, Loopback (locally managed card only), and administrative status.<sup>7</sup>

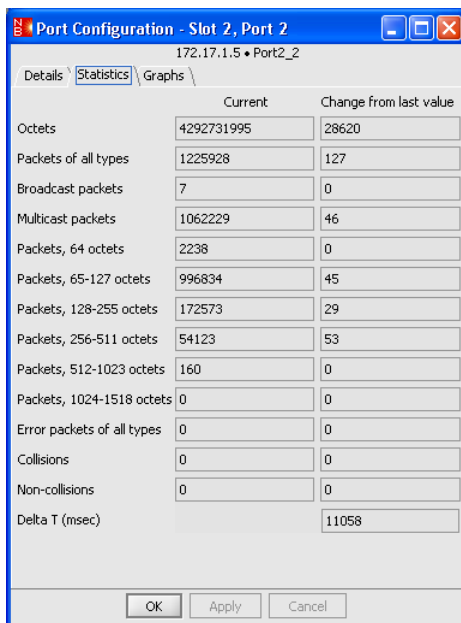
To change any these port settings, select **enabled** or **disabled** from the drop-down list, and then click **OK**.

<sup>7</sup> Refer to the *Radiance Access Line Cards - Installation and User Guide*, "Software Settings," for additional information.

Name	Description
Admin status	When enabled, the port sends and receives data, including management packets. When disabled, data is neither sent to nor received from the port. However, the port continues to accept, process, and transmit management packets.
Auto-negotiation	When enabled, the copper port advertises full/half duplex capability. Speed is not auto-negotiated and set to 100Mbps. When disabled, the copper port is set to full duplex.
Far End Fault (FEF)	When FEF is enabled on a remote line card and it loses its receive fiber link, the card sends an unsolicited alarm to the locally managed card. When disabled, the remote card does not send an alarm if it loses its receive fiber link.
Link Loss Return (LLR)	When LLR is enabled, loss of the port's receive link disables its transmit link. When disabled, the port continually transmits an idle signal.
Loopback	When disabled, the port sends data to the receiver. When enabled, the port returns its incoming data back to the sender, while continuing to receive and send management packets. Management packets are not looped back to the sender. Loopback can only be applied to one port at a time because enabling loopback on one port disables the opposite port. Not applicable to the remote copper port.

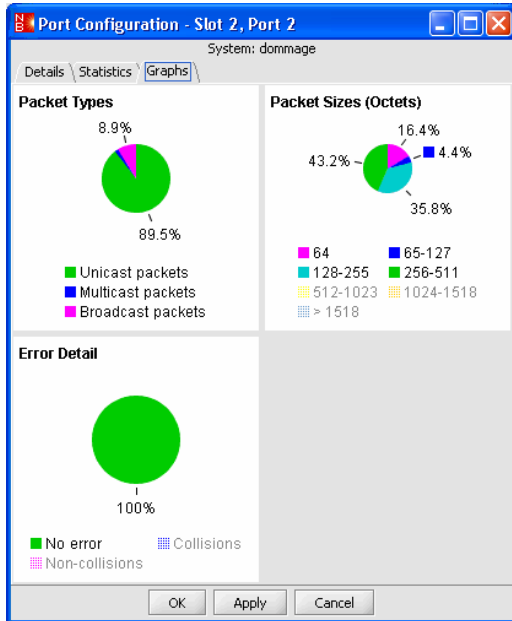
### Displaying Port Statistics

To view the port's RMON statistics, click the **Statistics** tab on the Port Configuration dialog box. The current totals and the changes since the last printed values are displayed. Changes are the difference between the current totals and the totals from the previous sampling. The time between samplings is displayed in milliseconds in the Delta T field.



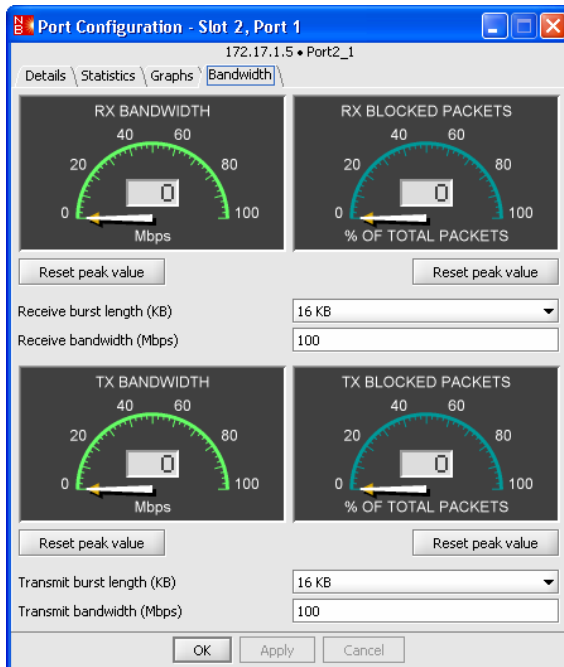
## Viewing Data Graphs

To view pie charts showing the various packet types received, the sizes of those packets, and the types of error packets received, click the **Graphs** tab.



## Provisioning Bandwidth

1. To configure the bandwidth settings for the access line card, select the copper port and click the **Bandwidth** tab. (This tab is not available for the fiber port.)



The top half displays information relating to the ingress bandwidth, and the bottom half displays information relating to the egress bandwidth.

The yellow arrowheads point to the highest levels attained in each gauge. Click **Reset peak value** to reset the pointer.

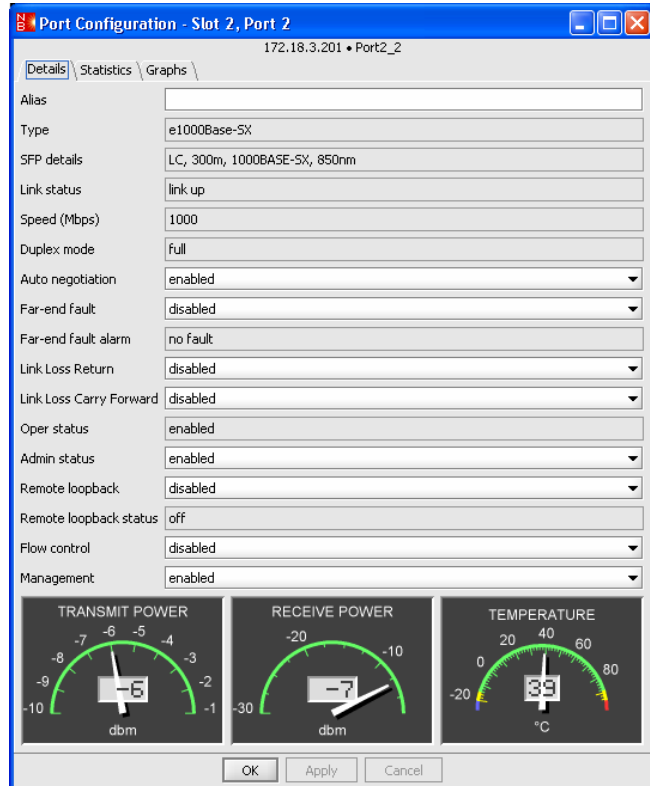
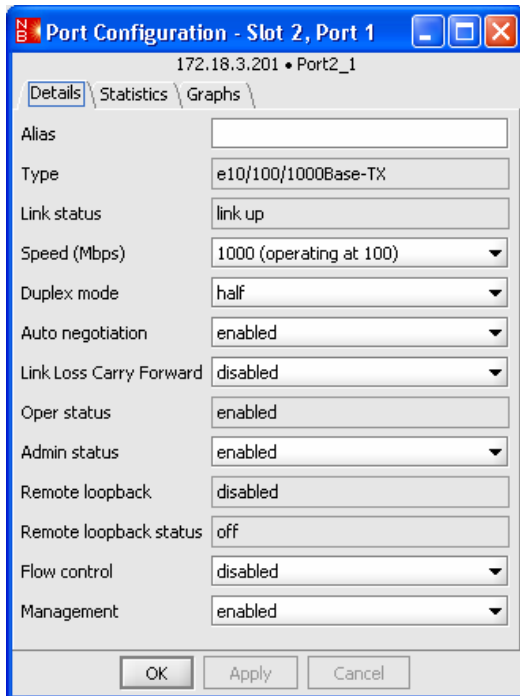
Note that the gauges do NOT use the same units. The bandwidth gauges on the left display data in megabits per second (Mbps), while the blocked packet gauges on the right display the percentage of the total packets which were blocked and then dropped. Click the **Statistics** tab to see further details about the information shown in the gauges.

2. To configure the bandwidth settings, do the following:
  - Set the maximum burst size by selecting one of the following options from the Receive or Transmit burst length drop-down list:  
  
16 KB, 32 KB, 64 KB, 128 KB, or 256 KB.  
  
This determines the maximum data burst size permitted in that direction. The access line card provides full access to the channel bandwidth until the burst threshold is reached.
  - Set the Receive or Transmit bandwidth by typing a number between 1 and 100. This sets the maximum amount of data that can be carried over the network in megabits per second (Mbps).
  - Click **OK**.

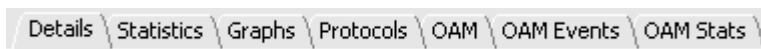
## Configuring the Services Line Card Ports

1. Double-click the port to configure in either the chassis view or the Ports folder.
2. The Port Configuration dialog box appears. The dialog boxes for a copper port (left) and a fiber port (right) are shown below. Note that not all SFP transceivers provide laser and temperature readings.

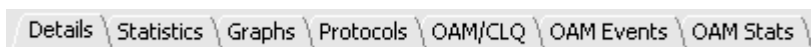




The Port Configuration dialog box for a standalone services line card NID includes an additional Protocols tab and several OAM tabs:



For the copper port on the R821, the OAM tab includes CLQ (copper line quality) information:



Refer to [OAM Options \(Standalone NIDs Only\)](#) for more information.

3. To assign a new name to the port, type a *name* in the Alias text box.
4. On the copper port, set the speed to **10**, **100**, or **1000** Mbps. On a standalone NID, there is an addition option, **auto negotiate**, which enables the port to negotiate operational speed with its link partner. Selecting the auto-negotiate option overwrites the Auto-negotiation setting. The fiber port speed is fixed and not configurable.
5. Set the duplex mode to **full** or **half**. (Only applicable to the copper port when auto-negotiation is disabled.)
6. The remaining options allow you to enable or disable various functions. To change any these port settings, select **enabled** or **disabled** from the drop-down list.

Name	Description
Auto-negotiation	<p>When enabled on a 10/100/1000BASE-T port, the port advertises 1000Mbps full-duplex capability to its link partner. When enabled on a 10/100BASE-T port, the port advertises 100Mbps full-duplex capability.</p> <p>When disabled on the fiber port of the R851, the fiber port is set to 1000Mbps full duplex. When disabled on the copper port, the speed and duplex are determined by the port's speed and duplex mode settings.</p>
Admin status	Administratively enable or disable a port. When a port is disabled, no traffic passes through the port and the link appears down.
Link Loss Return (LLR)	When LLR is enabled on a fiber port, loss of the port's receive link disables its transmit link. When disabled, the port continually transmits an idle signal. Not applicable to copper ports.
Link Loss Carry Forward (LLCF)	When LLCF is enabled on a port, loss of link on the port prevents the opposite port from transmitting idle signals. For example, if LLCF is enabled on Port 1 and it loses link, Port 2 will stop transmitting idle signals. When LLCF is disabled on a port, loss of link on the port has no effect on the opposite port's transmission of idle signals.
Flow control	When enabled, PAUSE frames are used on full-duplex ports, and collisions are forced on half-duplex ports.
Loopback	<p>When enabled, the port returns its incoming data back to the sender, while continuing to receive and send management packets. Management packets are not looped back to the sender. For normal operation, loopback must be disabled.</p> <p><b>Tip:</b> The services line card allows you to set the loopback timeout period. Refer to <a href="#">Changing Network and Management Settings</a>.</p>
Far End Fault (FEF)	When FEF is enabled on a remote line card and it loses its receive fiber link, the remote card sends an unsolicited alarm to the locally managed card. When disabled, the remote card does not send an alarm if it loses its receive fiber link. When a port receives a FEF alarm, the information is displayed in the Far End Fault alarm field. FEF is only applicable to fiber ports.
Management	Enable or disable management access over the port.
Rate limiting	Activate or cancel rate limiting. Disable rate limiting to allow traffic to flow at full line rate. When rate limiting is enabled, the maximum data rate is set to the value specified by the rate option. This command is only applicable to ports on the R821.

7. Click **OK**.

### ***Displaying SFP Sensor Readings and Hardware Parameters***

Each fiber port with an SFP transceiver installed in it provides accurate digital diagnostic information. The Port Configuration dialog box provides three sensor gauges that display the

port's optical receive and transmit laser levels, along with its internal temperature. Each sensor has a warning threshold and an alarm threshold to indicate when the level is too high or too low. To warn the network manager of a potential problem, a trap can be set so notification will be sent if any threshold is crossed.

The SFP details field provides the following hardware information about the pluggable optics:

- Type of connector: LC or SC
- Maximum distance supported in meters or kilometers
- Ethernet media designation
- Wavelength in nanometers

The services line card provides RMON statistics and pie charts similar to those for the access line card. Refer to [Displaying Port Statistics](#) and [Viewing Data Graphs](#).

### ***OAM Options (Standalone NIDs Only)***

As a standalone NID, the services line card includes support on each port for numerous IEEE 802.3ah operations, administration, and maintenance (OAM) options including OAM loopback, events, and statistics. These options are accessible by clicking the OAM tabs in the Port Configuration dialog.

### **Defining the Access and Trunk Ports**

Specify if the port should be designated as the trunk port or the access port by selecting **trunk** or **access** from the Access/trunk mode drop-down list. Typically Port 2 is the trunk port, which is connected to the service provider's network, and Port 1 is the access port, which is connected to the customer.

### **Applying a Rate Limit on the R821**

For the R821 only, enable or disable rate limiting. Disable rate limiting to allow traffic to flow at full line rate. Enable rate limiting to set the maximum data rate to the value specified in the rate limit (admin).

Type the ingress (inbound) traffic rate limit in Kbps. The following rates are available: **128, 256, 512, 1000, 2000, 4000, 8000, 100000**. The rate limit (oper) text box displays the operational rate limit.

Rate limiting	<input type="text" value="enabled"/>
Rate limit (admin)	<input type="text" value="100000"/>
Rate limit (oper)	<input type="text" value="100000"/>

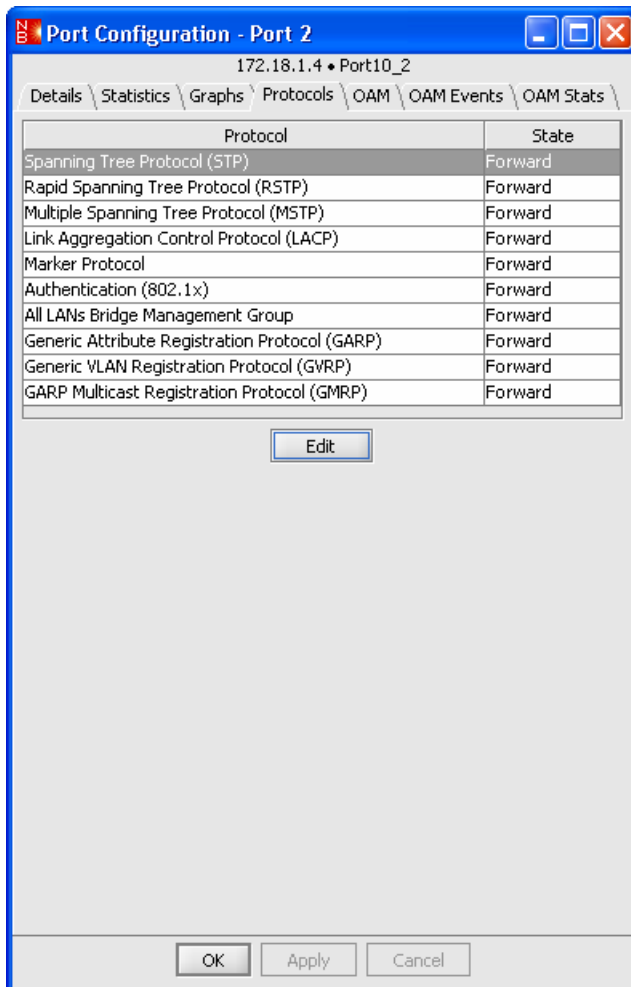
## Setting the Default Port Priority

For the R821, you can set the priority bits on a port to any value from 0 to 7. The bits are mapped to a queue depending on which p-bit mode is enabled, either provider bridge or 802.1D. To set the default port priority, select a value from the default port priority drop-down list.

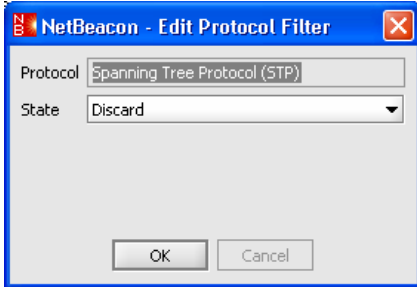
## Configuring Layer 2 Control Protocols

By default all Layer 2 control protocols are forwarded. To change the disposition for a protocol on a port, do the following:

1. In the Port Configuration dialog box, click the **Protocols** tab.



2. Select the protocol you want to change.
3. Click **Edit**. The Edit Protocol Filter dialog appears.



4. From the State drop-down list, select one of the options:
  - **Forward** – forward the specified protocol, based on forwarding rules and policies.
  - **Discard** – discard (filter) the specified protocol.
  - **Process** – accept the specified protocol for end-station processing.
5. Click **OK**. The change appears in the Protocols table.
6. Click **OK**.

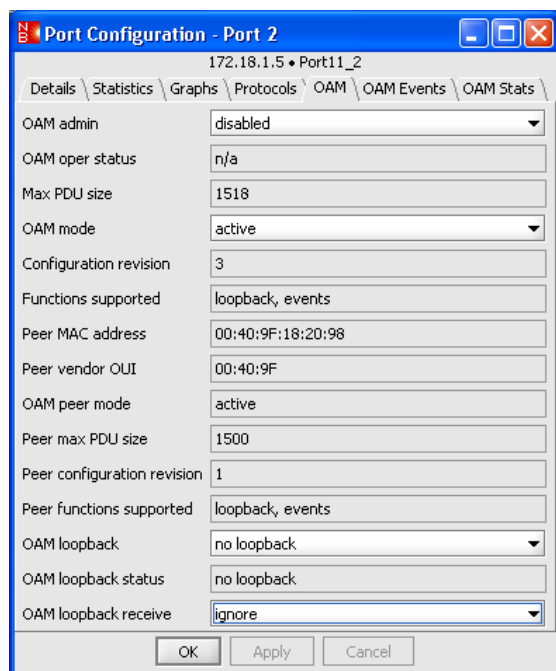
### OAM Controls and Loopback

The following table describes the fields under the **OAM** tab.

Name	Description
OAM admin	Set the port's administrative OAM mode to <b>enabled</b> or <b>disabled</b> .
OAM oper status	Identifies the OAM capability between the port and its peer. <ul style="list-style-type: none"> <li>• disabled—OAM is disabled administratively on the port.</li> <li>• link fault—the port has detected a fault and is transmitting OAMPDUs with a link fault indication.</li> <li>• passive wait—the port is in passive OAM mode and is waiting to see if its peer supports OAM.</li> <li>• active send local—the port is in active OAM mode and is trying to discover whether its peer has OAM capability, but has neither accepted nor rejected the peer's configuration yet.</li> <li>• send local and remote—the port has discovered its peer, but has yet to accept or reject the peer's configuration.</li> <li>• send local and remote OK—the port has accepted OAM peering with its peer.</li> <li>• OAM peering locally rejected—the port has rejected OAM peering.</li> <li>• OAM peering remotely rejected—the port's peer has rejected OAM peering.</li> <li>• operational—both the port and its peer have accepted peering.</li> </ul>
Max PDU size	Largest OAMPDU (in bytes) that the port supports. The port exchanges maximum OAMPDU sizes with its peer, and both ports negotiate to use the smaller of the two maximum sizes between them.
OAM mode	Mode of OAM operation for the port. <ul style="list-style-type: none"> <li>• passive—the port waits for its peer to initiate OAM actions; the port cannot initiate actions itself.</li> <li>• active—the port can initiate monitoring activities with its peer.</li> </ul>

Name	Description
Configuration revision	Revision number of the port as reflected in the latest OAMPDU it sent. The configuration revision is used to indicate changes that have occurred which might require its peer to re-evaluate whether peering is allowed.
Functions supported	OAM functions supported by the port. One or more of the following functions may be supported: unidirectional, loopback, events, variable.
Peer MAC address	MAC address of the port's peer. The MAC address is derived from the most recently received OAMPDU.
Peer vendor OUI	Peer's Organizational Unique Identifier (OUI), which can be used for identifying the peer's vendor.
OAM peer mode	<p>Mode of OAM operation for the peer.</p> <ul style="list-style-type: none"> <li>• active—the peer can initiate monitoring activities with the local port.</li> <li>• passive—peer waits for the local port to initiate OAM actions.</li> <li>• unknown—the peer status is inactive.</li> </ul>
Peer max PDU size	Largest OAMPDU (in bytes) that the peer supports. The peer exchanges maximum OAMPDU sizes with the local port, and both ports negotiate to use the smaller of the two maximum sizes between them.
Peer configuration revision	Configuration revision of the remote port as reflected in the latest OAMPDU sent by the remote port. The configuration revision is used to indicate configuration changes that have occurred which might require the local port to re-evaluate whether peering is allowed.
Peer functions supported	OAM functions supported by the peer. One or more of the following functions may be supported: unidirectional, loopback, events, variable.
OAM loopback	<p>Select <b>start loopback</b> to initiate remote loopback with the remote port. Starting remote loopback causes the port to send a loopback OAMPDU (with the loopback enable flags set) to the remote port.</p> <p>Select <b>stop loopback</b> to terminate remote loopback. Ending remote loopback causes the port to send a loopback OAMPDU (with the loopback enable flags cleared) to the remote port.</p> <p><b>no loopback</b> has no effect.</p>
OAM loopback status	<p>Indicates the loopback state of the port.</p> <ul style="list-style-type: none"> <li>• no loopback—normal operation with no loopback in progress.</li> <li>• initiating loopback—the local device has sent a loopback request to the remote unit and is waiting for a response.</li> <li>• remote loopback—the remote unit has responded to the local device and indicated that it is in loopback mode.</li> <li>• terminating loopback—the local device is in the process of ending the remote loopback.</li> <li>• local loopback—the remote unit has put the local device in loopback mode.</li> <li>• unknown—the local and remote parsers and multiplexers are in an unexpected state.</li> </ul>

Name	Description
OAM loopback receive	Select <b>process</b> or <b>ignore</b> to process or drop incoming requests for loopback when the port receives them.



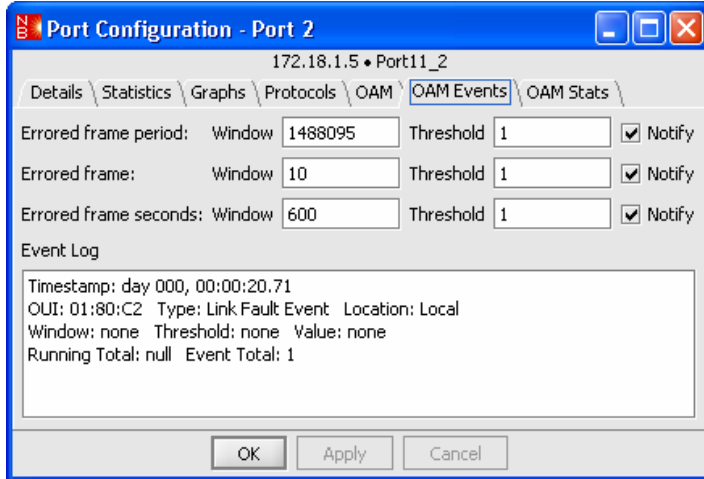
## OAM Events

Click the **OAM Events** tab to configure OAM event notification and to view the event log. The service line card supports the following Ethernet OAM events:

- Errored frame period: generated when the number of frame errors exceeds a threshold within a given window defined by a number of frames. For example, 5 frames out of 1,000,000 had errors. Acceptable values for the Window are 148,809 to 89,285,714.
- Errored frame: generated when the number of frame errors exceeds a threshold within a given window defined by a period of time. For example, 1 frame in 10 seconds had errors. The value displayed in the errored frame window represents the number of tenths of a second. For example, 5 = 0.5 second, 10 = 1 second, 200 = 20 seconds, etc. Acceptable values for the Window are 10 to 600, which represent 1 to 60 seconds.
- Errored frame seconds: generated when the number of errored frame seconds exceeds a threshold within a given time period. For example, 5 errored frame seconds within the last 60 seconds. An errored frame second is defined as a 1 second interval which had one or more frame errors. The value displayed in the errored frame seconds window represents the number of tenths of a second. For example, 600 = 60 seconds. Acceptable values for the Window are 100 to 9,000,

which represent 10 to 900 seconds. Acceptable values for the Threshold are 1 to 900 errored frame seconds.

Select the **Notify** check box at the end of each event to enable notification to the port's OAM peer that the OAM event has been triggered.



The Event Log parameters are described in the following table.

Name	Description
Timestamp	The services line card's system uptime value when the event occurred.
OUI	The Organizational Unique Identifier. Excluding event TLVs that are unique to an organization, all IEEE 802.3 events use the OUI of 01:80:C2. Organizations that define their own event notification TLVs include their OUI in the TLV which gets reflected here.
Type	The type of event that generated the entry into the Event Log. When the OUI is 01:80:C2, the following event types are defined: Errored Symbol Event, Errored Frame Period Event, Errored Frame Event, Errored Frame Seconds Event, Link Fault Event, Dying Gasp Event, and Critical Link Event. The first four types are threshold crossing events which are generated when a metric exceeds a given value within a specified window. The other types are not threshold crossing events.
Location	Indicates whether the event occurred locally, or was received from the OAM peer via Ethernet OAM.
Window	For a threshold crossing event, the period over which the value was measured for the event (e.g.: 5, when 11 occurrences happened in 5 seconds while the threshold was 10).
Threshold	For a threshold crossing event, the limit that was crossed for the event to be logged (e.g.: 10, when 11 occurrences happened in 5 seconds while the threshold was 10).



Name	Description
Value	For a threshold crossing event, this indicates the number of occurrences within the given window that generated the event (e.g.: 11, when 11 occurrences happened in 5 seconds while the threshold was 10).
Running Total	The total number of times this occurrence has happened since the last reset (e.g.: 987, when 987 frame errors resulted in 18 frame error threshold crossing events since the last reset).
Event Total	The total number of times one or more of these occurrences resulted in an event since the last reset (e.g.: 18, when 987 frame errors resulted in 18 frame error threshold crossing events since the last reset).

### OAM Statistics

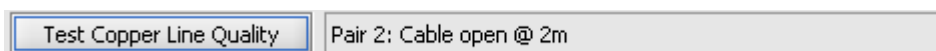
Click the **OAM Stats** tab to view the complete list of OAM statistics for the port. These statistics include the number of OAMPDUs transmitted and received as well as the number of frames dropped by the OAM multiplexer. The OAMPDU types include information, unique and duplicate event notifications, loopback controls PDUs, variable requests and responses, organization specific PDUs, and unsupported codes.

### Copper Line Quality (CLQ) Testing

The R821 NID includes a built-in cable tester that can check the copper cable for faults (open circuit, short circuit, or impedance mismatch) and estimate the distance to the fault. The accuracy of the distance measurement is +/- 2 meters.

**Important:** The CLQ test interrupts normal communication through the copper port. This is especially important if the R821 is being managed through the copper port.

1. Click the **OAM/CLQ** tab in the Port Configuration dialog box for Port 1 of the R821.
2. Near the bottom of the dialog box, click the **Test Copper Line Quality** button. The test takes a few seconds to complete. While the test is running, the display may show a message that says: -- testing --. If the test concludes quickly, the test message will not appear.
3. When the test is complete, the message will indicate that the CLQ test passed, or it will identify the fault and specify the distance to the problem from the R821.



### Managing the RS960 Ports

The RS960 provides three types of ports, which perform specific tasks. These ports are the Ethernet management port for out-of-band management access, the two fiber optic network ports for connecting to a service provider's network, and the four access ports that are the user network interfaces (UNIs) in an MEF configuration. The RS960 port configuration dialog

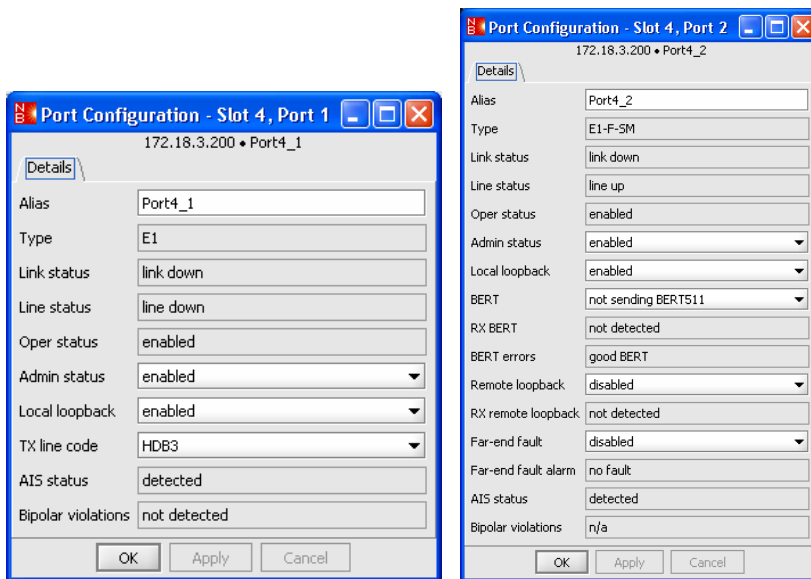
boxes are similar to the services line card NID dialogs and include OAM support. The differences are highlighted below:

- Loopback is not applicable to the RS960's management port.
- The RS960 does not support Link Loss Carry Forward, which is only applicable to two-port devices.
- Access/trunk mode is not applicable to the RS960. The network ports are always the trunk ports and the access ports are always the access ports.
- Ingress rate limiting on the access and network ports on the RS960 can be set to any value from 1 to 1000 Mbps. On the services line cards, only certain rates are available for rate limiting.
- The RS960 does not support copper line testing on its copper ports.

## Configuring the T1/E1 Ports

To configure a port on the T1/E1 card, do the following:

1. Double-click the port to configure in either the chassis view or the Ports folder.
2. The Port Configuration dialog box appears. The dialog boxes for an E1 copper port (left) and an E1 fiber port (right) are shown below.



3. In the Alias textbox, type the *name*<sup>8</sup> to assign to the port.

<sup>8</sup> There is a limit of 32 characters for the port name. Do not use the following characters: . ; & = : " < > .

1. To enable or disable the port, select **enabled** or **disabled** from the admin status drop-down list. Disabling a port has no effect on the incoming data, however, outgoing data from the port will be dropped and AIS will be sent.
2. Set local loopback according to the following:

For normal operation, set local loopback to **disabled**.

If you want the inbound data on the copper or fiber line to be regenerated and sent back to the sending device, set local loopback to **enabled**. Local loopback may be enabled on both ports at the same time.

3. Click **OK**.

### *Selecting the Line Code and Line Buildout*

1. To set the line code or line buildout on a T1/E1 line card, double-click on its copper port.
2. From the TX line code drop-down list, select **B8ZS** or **AMI** for a T1 card, or select **HDB3** or **AMI** for an E1 card.
3. To set the line buildout for a T1 card, select one of the options from the line buildout drop-down menu. The line buildout determines the shape of the transmitter's output pulse. Line buildout is not applicable to E1 cards.
4. Click **OK**.

### *Setting BERT 511, Remote Loopback, and Far End Fault*

1. To configure BERT 511, remote loopback, or Far End Fault (FEF) for the T1/E1 line card, double-click on its fiber port.
2. Set BERT to **sending BERT511** if you want the fiber transmitter to send a test sequence on the data channel to the remote unit. The remote unit can be either another line card or a standalone. Set BERT to **not sending BERT511** for normal operation.

**Important:** To test the fiber connection between two T1/E1 line cards, both BERT and remote Loopback must be enabled individually. The two functions are set automatically through the DIP switch, BR.

3. Set remote loopback to **enabled** to force the data on the fiber line to loop back at the remote end. Only the data bits will be looped, not the management bits. Set remote loopback to **disabled** for normal operation.
4. Set Far End Fault (FEF) to **enabled** to send an unsolicited alarm via the fiber management channel if it loses its carrier or receives AIS. Set Far End Fault to **disabled** if you don't want the remote card to receive an alarm. FEF is enabled by default.
5. Click **OK**.

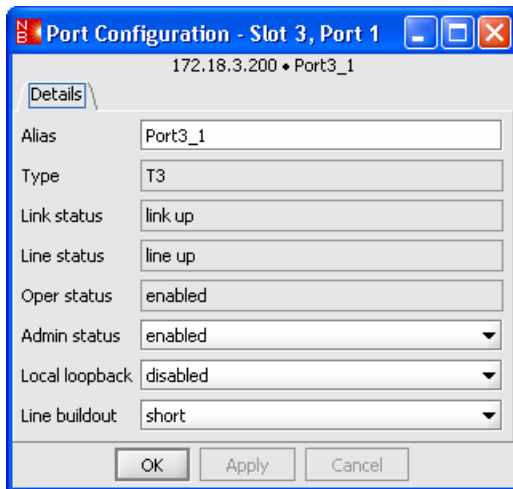
## T1/E1 Indicators

The following table describes the alarm and status indication fields provided in the T1/E1 Port Configuration dialog boxes.

Name	Description
Link status	Indicates if the port is detecting link.
Line status	Indicates if the port is receiving a carrier line signal.
Oper status	Operational status of the port, either enabled or disabled.
RX BERT	Indicates if the port is receiving BERT 511 patterns.
BERT errors	Indicates if the BERT sequence it received had any errors.
RX remote loopback	Indicates if the port is receiving a request for temporary loopback.
Far End Fault alarm	Indicates if the port has received a Far End Fault alarm from the remote device.
AIS Status	Indicates if AIS was detected on the port.
Bipolar violations	Indicates if any bipolar violations were detected on the port.

## Configuring the T3/E3 Ports

1. Open the Port Configuration dialog box. The dialog for a T3 copper port is shown below.



2. In the Alias text box, type the *name*<sup>9</sup> to assign to the port.

<sup>9</sup> There is a limit of 32 characters for the port name. Do not use the following characters: . ; & = : " < > .

3. To enable or disable the port, select **enabled** or **disabled** from the admin status drop-down list. Disabling a port stops the flow of data to and from that port. If the copper port is disabled, no signals will be sent from the coaxial transmitter, and an unframed all-ones pattern will be transmitted over the fiber line to the remote line card. If the fiber port is disabled, no signals will be sent from the fiber transmitter, and an unframed all-ones pattern will be passed from the copper port. Once a port is disabled, the only way to enable it again is through software.

NOTE: An all-ones pattern indicates an alarm indication signal (AIS) for the E3 line cards only. For T3 cards, the all-ones pattern is simply transmitted to the remote device; it does NOT indicate AIS.

4. Set local Loopback to the following:

For normal operation, set local loopback to **disabled**.

The T3/E3 line card provides independent copper and fiber loopback modes. To set either the copper port or the fiber port into loopback, set Local Loopback to **enabled**. When local loopback is enabled, incoming data is both transmitted to the remote device and returned to the sending device. Copper and fiber loopback cannot be enabled at the same time.

5. Click **OK**.

### ***Setting the T3 Line Buildout***

For a T3 line card, an additional option is provided to set the line buildout on the copper port. Line buildout is not applicable to E3 cards.

1. Open the Port Configuration dialog box the copper port on a T3 line card.
2. Set the line buildout to **short** if your coaxial cable length is less than 255 feet. If the cable is between 255 and 1200 feet, set the line buildout to **long**.
3. Click **OK**.



## Chapter 8. Monitoring Traps and Alarms

The NetBeacon Element Browser provides both audible and visual alarm indicators. Three distinct sounds representing different levels of alarms audibly notify a network administrator that a problem has occurred. Flashing alarm icons on the chassis image and flashing red text in the Domain Structure and Network Elements panels visually alert the administrator to an alarm.

The Alarms & Traps tab displays a color-coded message whenever certain events occur in any of the elements being monitored. Alarms are more severe than traps, which are mainly informational. NetBeacon reports three types of alarm severities: minor, major, and critical.

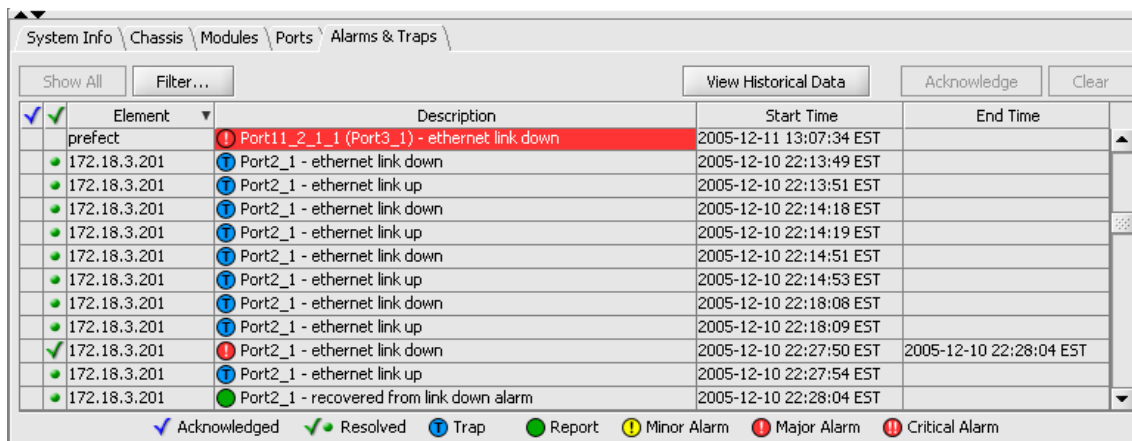
NetBeacon provides numerous traps and alarms, including notification of configuration and status changes or problems with a power supply, chassis, module, or port. By default, all traps and alarms for all monitored elements that are in service are reported. However, there is an option to filter the information by alarm severity, domain, element, resolution, or acknowledgement. The types of traps reported can also be filtered at their original source by checking or unchecking items in the R502-M management module Trap Control table (refer to [Filtering the Trap Control Options](#)).

**Important:** When recording events, the time reported is the time from the NetBeacon Element Manager, not the local PC time. If an element is not in service, some alarms will be recorded as traps, not alarms.

For information about the alarm indicators in the upper right corner of the Element Browser window, refer to [Alarm Indicators](#).

### Viewing Alarms and Traps

To display all alarm and trap notifications received by NetBeacon, click the **Alarms & Traps** tab. The table, which can be scrolled vertically, displays each message with a colored icon indicating its severity.





The screenshot shows the 'Alarms & Traps' window with a table of events. The table has columns for 'Element', 'Description', 'Start Time', and 'End Time'. The first row is highlighted in red, indicating a Major Alarm. The legend at the bottom identifies the icons used for Acknowledged, Resolved, Trap, Report, Minor Alarm, Major Alarm, and Critical Alarm.

Element	Description	Start Time	End Time
✓ prefect	Port11_2_1_1 (Port3_1) - ethernet link down	2005-12-11 13:07:34 EST	
172.18.3.201	Port2_1 - ethernet link down	2005-12-10 22:13:49 EST	
172.18.3.201	Port2_1 - ethernet link up	2005-12-10 22:13:51 EST	
172.18.3.201	Port2_1 - ethernet link down	2005-12-10 22:14:18 EST	
172.18.3.201	Port2_1 - ethernet link up	2005-12-10 22:14:19 EST	
172.18.3.201	Port2_1 - ethernet link down	2005-12-10 22:14:51 EST	
172.18.3.201	Port2_1 - ethernet link up	2005-12-10 22:14:53 EST	
172.18.3.201	Port2_1 - ethernet link down	2005-12-10 22:18:08 EST	
172.18.3.201	Port2_1 - ethernet link up	2005-12-10 22:18:09 EST	
172.18.3.201	Port2_1 - ethernet link down	2005-12-10 22:27:50 EST	2005-12-10 22:28:04 EST
172.18.3.201	Port2_1 - ethernet link up	2005-12-10 22:27:54 EST	
172.18.3.201	Port2_1 - recovered from link down alarm	2005-12-10 22:28:04 EST	







Legend: ✓ Acknowledged, ✓ Resolved, ⚙ Trap, 🟢 Report, 🟡 Minor Alarm, 🔴 Major Alarm, 🔴 Critical Alarm

The following table describes the fields shown in this table.


Heading	Description
	A blue check mark indicates that the message has been acknowledged by a user.
	A green check mark indicates that the condition has been resolved. For example, a down link is now up. A green dot indicates that the alert is informational only, and no further action is required. A green dot message may result in the resolution of an existing alarm condition. Some types of alarms, such as the insertion or removal of a module, become resolved simply by acknowledging them.
Element	The IP address or DNS name of the element where the alert was generated.
Description	A brief description of the alarm or trap.
Start Time	The date and time when the event occurred.
End Time	The date and time when the problem was resolved.

### *Understanding the Trap Legend*

Below the Alarms and Traps table is a legend briefly describing all the icons displayed in the Element Browser.

Icon	Name	Description
	Acknowledged	Refer to descriptions in the preceding table.
	Resolved	
	Trap	<p>An SNMP trap message. For example, when the link is up after it had been down.</p> <p>A trap can signify the start of an alarm as well as the end of an alarm. A trap that starts an alarm typically turns into an alarm. For example, a link down event occurs and is reported as a trap, but after 2.5 seconds, if the link does not go up, the same item in the trap/alarm list is <u>raised</u> to an alarm status.</p>
	Report	An informational message that requires no action. Usually indicates an alarm condition has been resolved. To resolve most alarms, the entity must remain in the resolved state for at least 10 seconds.
	Minor Alarm	Minor alarms do not require urgent attention because there are back-up solutions for them, however, they should be checked before a more serious problem occurs. An example of a minor alarm is a loss of link on a redundant port, which has another redundant port as its back-up. Another example is a loss of power in a device with dual power supplies.
	Major Alarm	Major alarms are serious conditions that may indicate some type of failure or that may result in network disruption. There are no back-up solutions for major alarms. Major alarms are sent under conditions such as when the



Icon	Name	Description
		power supply goes above or below the acceptable voltage range, or when a module is removed from or inserted into a chassis. Loss of link on a non-redundant port, and loss of power in a device with only one power supply are two more examples of major alarms.
	Critical Alarm	Critical alarms require immediate attention. They include conditions such as loss of communication with an element.

Whenever new alarms are added to the Alarms and Traps table, they are highlighted in red or yellow, depending on their severity. Traps and reports are not highlighted. When an alarm condition is acknowledged by a user or the underlying problem is resolved, the highlighting disappears.

Double-clicking on an alarm in the Alarms and Traps table changes the chassis image to the element where the alarm occurred, if the element was not in view.

Double-clicking on an alarm icon in the chassis view automatically opens the Alarms & Traps tab, if it was not active, and the alarm is highlighted.

### *Acknowledging Alarms and Traps*

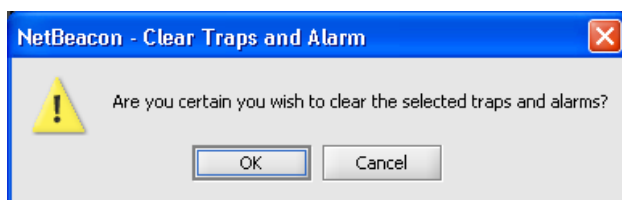
One or more messages may be acknowledged by selecting the message(s) and clicking **Acknowledge**. Acknowledged messages have a blue check mark in the first column of the table. Acknowledged alarms are not highlighted and the corresponding icon on the chassis view stops flashing. When all alarms of a particular severity are acknowledged or resolved, the icon (located in the upper right corner of the browser window) representing the severity stops flashing.

To undo an acknowledgement, select the message, hold down the SHIFT key and click **Acknowledge**. The blue check mark is removed, and if the message is an alarm, the yellow or red highlighting reappears.

### *Removing Alarm and Trap Messages*

To permanently remove one or more messages from the Alarms and Traps table, do the following:

1. Select the message(s) you want to delete.
2. Click **Clear**. The following confirmation dialog box appears.



3. Click **OK**. The message is removed from the table. If alarms were removed, the tallies in the upper right corner are updated with the new lower totals.

## Filtering Traps and Alarms

By default, all alarms and traps for all currently monitored elements are reported in the Alarms and Traps table. The information shown can be filtered based on domain, element, severity, or status. This section describes how to configure parameters to display.

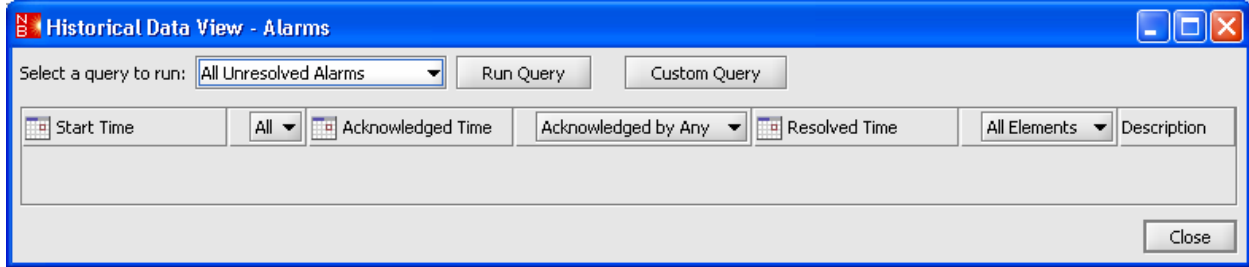
1. From the Alarms and Traps table, click **Filter**. The following dialog appears.



2. Select an option for showing alarms, reports, and traps.
3. By default, messages of all severities are enabled (checked). Under Severity, uncheck any type of alarms, traps, or reports you do not want displayed.
4. By default, both acknowledged and resolved messages are displayed in the table.
  - Select **Yes** to display only acknowledged or resolved messages.
  - Select **No** to display only messages that are not acknowledged or resolved.
  - Select **Either** to display both acknowledged/resolved and unacknowledged/unresolved messages.
5. Click **OK**.
6. Click the **Show All** button to restore the Alarms and Traps table to the default state in which all traps, alarms, and reports for all monitored elements are displayed.

## Viewing Historical Data

NetBeacon provides an option to view historical information regarding the alarms by running an SQL query. Under the Alarms & Traps tab, click **View Historical Data**.



### Running a Standard Query

To run a standard SQL query, select one of the options from the 'Select a query to run' drop-down list, then click **Run Query**. The alarms database table appears, as shown below.


The screenshot shows the 'Historical Data View - Alarms' window with the results of a query displayed in a table. The table has the same columns as the previous screenshot. The data is sorted by start time in descending order. The first row is '2005-12-12 12:33:09.161' with a red alarm icon and description 'Communication with element has failed'. The second row is '2005-12-12 12:37:05.529' with a green icon and description 'Communication with element has been r...'. The following rows are '2005-12-12 12:28:00.725', '2005-12-12 12:28:00.733', '2005-12-12 12:28:00.736', '2005-12-12 12:28:00.758', '2005-12-12 12:28:00.76', and '2005-12-12 12:28:00.773', all with yellow icons and descriptions of 'PortX\_Y\_Z - ethernet link down'. The final three rows are from '2005-12-11 12:39:31.824', '2005-12-11 12:39:31.825', and '2005-12-11 12:39:33.911', all with red icons and descriptions of 'PortX\_Y\_Z - ethernet link down', with 'Acknowledged by Any' set to 'jwi@metro' and 'Resolved Time' set to 'prefect'. A 'Close' button is at the bottom right.

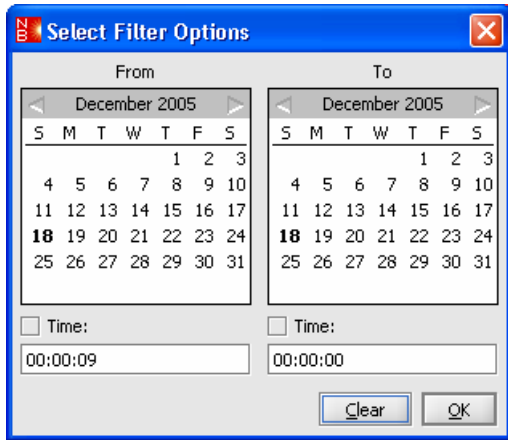
Start Time	All	Acknowledged Time	Acknowledged by Any	Resolved Time	All Elements	Description
2005-12-12 12:33:09.161	🔴				172.17.1.3	Communication with element has failed
2005-12-12 12:37:05.529	🟢				172.17.1.3	Communication with element has been r...
2005-12-12 12:28:00.725	🟡				172.17.1.3	Port1_2_3 - ethernet link down
2005-12-12 12:28:00.733	🟡				172.17.1.3	Port1_6_3 - ethernet link down
2005-12-12 12:28:00.736	🟡				172.17.1.3	Port1_7_3 - ethernet link down
2005-12-12 12:28:00.758	🟡				172.17.1.3	Port3_3_3 - ethernet link down
2005-12-12 12:28:00.76	🟡				172.17.1.3	Port3_4_3 - ethernet link down
2005-12-12 12:28:00.773	🟡				172.17.1.3	Port3_13_3 - ethernet link down
2005-12-11 12:39:31.824	🔴		jwi@metro		prefect	Port2_1 - ethernet link down
2005-12-11 12:39:31.825	🔴		jwi@metro		prefect	Port2_2 - ethernet link down
2005-12-11 12:39:33.911	🔴		jwi@metro		prefect	Port10_1 - ethernet link down
2005-12-11 12:39:33.911	🔴		jwi@metro		prefect	Port10_2 - ethernet link down

### Sorting the Alarms Database

NetBeacon allows you to sort the data shown in the alarms database by listing them in chronological order or reverse chronological order. Click on the text of any column heading with a calendar icon. An up or down arrowhead appears. An upward pointing arrowhead lists the data in chronological order. (The most recent alarm is at the bottom of the list.) A downward pointing arrow head lists the data in reverse chronological order with the most recent alarm at the top. The alarms can be sorted chronologically for acknowledgement time and resolution time as well as start time.

### Specifying Time Periods

The results from the SQL query can be modified by using the calendars and drop-down lists provided in the column headers of the database table. To filter the start and end dates for when the alarms occurred, were acknowledged or were resolved, click on the calendar icon .



Select a date and time to specify the start and end of the period. If dates are not specified, all dates will be included. The current date is shown in bold text. Use the forward and reverse arrows to change the month displayed.

Do any of the following:

- Click on a date to select it. The selection will be underlined.
- To specify a time, select the Time check box and enter the start or stop time. This is optional.
- If you make a mistake, click **Clear** to reset the settings.
- Click **OK** when the date and time are properly configured.

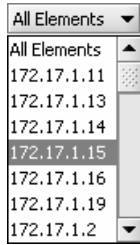
### Filtering Alarm Database Fields

The database table can also be modified to include only one type of alarm instead of all alarms. From the All drop-down list, select one of the alarm icons, as shown in the following example.



To view alarms acknowledged by a specific user, instead of any user, select the user's name from the Acknowledged by Any drop-down list.

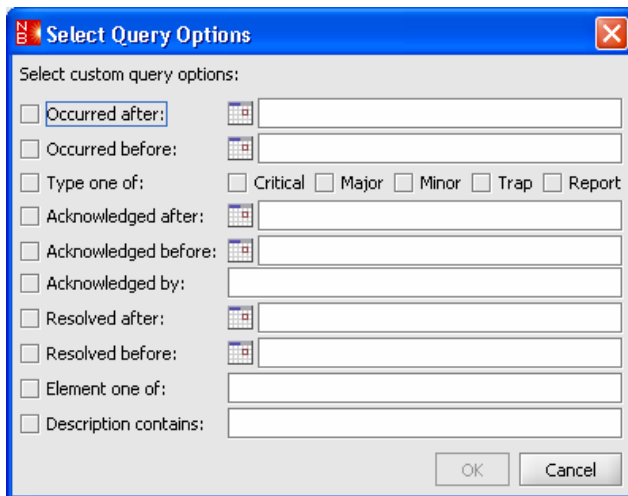
To view elements alarms that occurred on a specific element, instead of all elements, select the element's IP address or DNS name from the All Elements drop-down list.




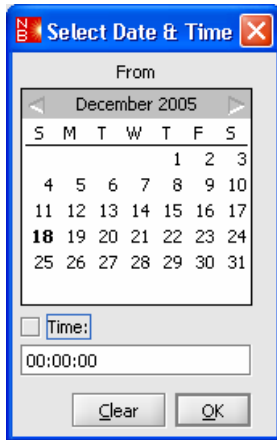
## Running a Custom Query

To run a customized SQL query in which you specify more detailed information about the alarms before you run the query, do the following:

1. In the Historical Data View window, click **Custom Query**. The Select Query Options dialog box appears.



2. For each text box with a calendar icon , click on the icon to select a date and time to specify the start and end of the period when the alarms occurred, were acknowledged, or were resolved. If dates are not specified, the query will include all dates. In the Select Date & Time dialog box, the current date is shown in bold text. Use the forward and reverse arrows to change the month displayed.



Do any of the following:

- Click on a date to select it. The selection will be underlined.
  - To specify a time, select the Time check box and enter the start or stop time. This is optional.
  - If you make a mistake, click **Clear** to reset the settings.
  - Click **OK** when the date and time are properly configured. The date and the time, if it was specified, appear in the text box in the Select Query Options dialog box.
3. To specify one or more alarm types, check **Critical, Major, Minor, Trap, or Report**. If no alarms are checked, the query will include all alarms.
  4. In the 'Acknowledged by' text box, type the *user name(s)* of the people who acknowledged the alarms. Separate each user name with a comma. If this text box is empty, the query will include alarms acknowledged by any user.
  5. In the 'Element one of' text box, type the *DNS name* or *IP address* of each element you want to include in the query. Separate each entry with a comma. If this text box is empty, the query will include alarms that occurred on any element.
  6. In the last text box, type the any *description* of the alarm. If this text box is empty, the query will include alarms with any description.
  7. Click **OK**. A customized view of the alarms database table appears. You can use the filters provided at the top of each column to further restrict or sort the information displayed.

## Appendix A. Download Error Messages

---

While attempting to download new software, you may receive an error message. The following table lists some common errors with solutions to help you correct them. Contact Metrobility's technical support if you are unable to resolve a problem.

Error	Solution
Alert: FTP failure during transfer	Do not ignore this message. Try downloading the software again, or manually reload the files through your local console.
Alert: telnet copyboot failed	Manually issue a copyboot command via telnet or console, or contact Metrobility technical support.
Copyboot failure	Contact Metrobility technical support.
Device not available	Check your network connections.
Failed to initiate copyboot	Manually issue a copyboot command via telnet or console.
Failed to reset	Select <b>Reset Chassis</b> in the Stack folder.
FTP failed – couldn't establish connection	Check your network connections.
FTP failed – unknown host	Check your network connections.
FTP failed to initiate copyboot	Start copyboot manually according to directions in the <i>Command Line Interface Reference Guide</i> .
FTP login failure – user known; login failed or login incorrect.	Enter the user name and password you have set for the device.
Skipped – complete update required	Choose <b>Complete update</b> from the Embedded Software Download dialog box.





## Appendix B. Frequently Asked Questions

---

**Q: When the Element Manager Admin Tool is started, is there any authentication between the Element Manager service and the admin tool application?**

A: Yes, the admin tool uses the same authentication as the Element Browser. It authenticates the same users, passwords, etc., that are used for the Element Browser. By default, no authentication is required.

**Q: Can I upgrade to NetBeacon ESP 1.0 from NetBeacon 3.8?**

A: No. The NetBeacon ESP administration differs so vastly from earlier versions of NetBeacon that no set-up information from any previous version is preserved.

**Q: What is the minimum version of WebBeacon, which is the OS on the R502 management card, that is compatible with NetBeacon ESP 1.0?**

A: 3.8.

**Q: What is the maximum number of elements supported by NetBeacon?**

A: NetBeacon supports up to 150 elements (R502 management cards managing interface line cards and some access line cards). If the elements include services line cards and Ethernet provisioning platforms, and if they are chained with multiple remotes, the total number of elements will diminish.

**Q: Where is the admin tool and Element Browser authentication information stored?**

A: It is stored in the file `security.xml` in the Element Manager's settings directory.

**Q: If the log-in information is lost, forgotten, or corrupted, is there a way to recover?**

A: Yes, the file `security.xml` can be edited directly, and forgotten or corrupted passwords can be changed.

**Q: What is the minimum screen resolution for viewing the Element Browser?**

A: Metrobility recommends a minimum screen resolution of 1024 by 768 pixels.

**Q: What is the difference between a line card and a module?**

A: There is no difference between the two. They are simply two terms for the same thing.

**Q: What is an element?**

A: An element is any network device with an IP address. Below are a few examples of elements:

- R851 or R821 services line card in an R200 chassis.
- RS960 Ethernet services provisioning platform.
- R5000 chassis with an R502 management card.
- R1000 chassis with an R502 management card.

## Appendix C. Abbreviations and Acronyms

---

AIS	Alarm Indication Signal
AMI	Alternate Mark Inversion
ARP	Address Resolution Protocol
B8ZS	Bit Eight Zero Substitution
BERT	Bit Error Rate Test
BWDM	Bidirectional Wavelength Division Multiplexing
CLCF	Copper Loss Carry Forward
CLQ	Copper Line Quality
CPLD	Complex Programmable Logic Device
CWDM	Coarse Wavelength Division Multiplexing
dB	Decibel
dBm	Decibel relative to 1 mW of power (0 dBm equals 1 mW)
DHCP	Dynamic Host Configuration Protocol
DIP	Dual In-line Package
DNS	Domain Name System
DRM	Dynamic Recovery Mode
DSLB	Disable Loopback
ESP	Ethernet Services Provisioning
FD	Full Duplex
FEF	Far End Fault
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
G/L	Global/Local
GUI	Graphical User Interface
HDB3	High-Density Bipolar Three Zeroes
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
KB	Kilobyte
Km	Kilometer
L2	Layer 2
L3	Layer 3
LLCF	Link Loss Carry Forward
LLR	Link Loss Return
LOA	Loss of Activity
LPC	Link Pulse Control
LPR	Line Protection and Restoration
LSL	Logical Services Loopback
MAC	Media Access Control
Mbps	Megabits per second
MDI	Media Dependent Interface
MIB	Management Information Base
MM	Multimode
Ms	Millisecond
mV	Millivolt

N/A	Not Applicable
NID	Network Interface Device
Nm	Nanometer
OAM	Operation, Administration, and Maintenance
OAMPDU	Operation, Administration, and Maintenance Protocol Data Unit
OID	Object Identifier
ONU	Optical Network Unit
OS	Operating System
OUI	Organizational Unique Identifier
PDF	Portable Document Format
PDU	Protocol Data Unit
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Monitoring
RX	Receive
SFP	Small Form-factor Pluggable optical transceiver
SM	Singlemode
SNMP	Simple Network Management Protocol
SONAR	Switch On No Activity Received
SQL	Structured Query Language
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TX	Transmit
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VID	VLAN Identifier
VLAN	Virtual Local Area Network

## **Appendix D. NetBeacon Warranty Statement**

---

Metrobility Optical Systems, Inc. warrants that a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and b) any Support Services provided by Metrobility shall be substantially as described in applicable written materials provided to you by Metrobility, and Metrobility support engineers will make commercially reasonable efforts to solve any problem issues. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you. To the extent allowed by applicable law, implied warranties on the SOFTWARE PRODUCT, if any, are limited to ninety (90) days.

SUPPORTED VERSIONS. Metrobility supports only the current released version and the most recent previous minor version of the SOFTWARE PRODUCT.

CUSTOMER REMEDIES. Metrobility and its suppliers' entire liability and your exclusive remedy shall be repair or replacement of the SOFTWARE PRODUCT that does not meet Metrobility's limited warranty and which is returned to Metrobility with proof of purchase. This limited warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by Metrobility are available without proof of purchase from an authorized international source.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, Metrobility and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-failure to provide support services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

LIMITATION OF LIABILITY. To the maximum extent permitted by applicable law, in no event shall Metrobility or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitations, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of failure to provide support services, even if Metrobility has been advised of the possibility of such damage. In any case, Metrobility's entire liability shall be limited to the amount actually paid by you for the SOFTWARE PRODUCT. Metrobility's entire liability regarding support services shall be governed by the terms of that agreement. Because some states and jurisdictions do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

## **Software Maintenance and Support Agreement**

Metrobility Optical Systems, Inc. offers an optional one-year software maintenance and support plan. The plan includes free electronic mail and telephone technical support, along with all minor and maintenance releases for this version of the software for a period of one year.

To purchase the agreement, contact your reseller or the Metrobility Sales Department.

## Appendix E. Standards Compliance

---

NetBeacon complies with the following standards:

- RFC 768 — UDP
- RFC 791 — IP
- RFC 792 — ICMP
- RFC 793 — TCP
- RFC 826 — ARP
- RFC 854 — Telnet
- RFC 950 — Internet Standard Subnetting Procedure
- RFC 959 — FTP
- RFC 1570 — SNMPv1
- RFC 1213 — MIB-II
- RFC 1350 — TFTP
- RFC 3416 — SNMPv2
- RFC 2131 — DHCP
- RFC 2819 — RMON Group 1
- RFC 3273 — RMON High Capacity Networks

NetBeacon complies with following updated standards:

- RFC 950 — updates ICMP RFC 792
- RFC 1349 — updates IP RFC 791
- RFC 1782 — updates TFTP RFC 1350
- RFC 1783 — updates TFTP RFC 1350
- RFC 1784 — updates TFTP RFC 1350
- RFC 1785 — updates TFTP RFC 1350
- RFC 3168 — updates TCP RFC 793
- RFC 2228 — updates FTP RFC 959
- RFC 2347 — updates TFTP RFC 1350
- RFC 2348 — updates TFTP RFC 1350
- RFC 2349 — updates TFTP RFC 1350
- RFC 2640 — updates FTP RFC 959
- RFC 2773 — updates FTP RFC 959
- RFC 2011 — updates MIB-II RFC 1213
- RFC 2012 — updates MIB-II RFC 1213
- RFC 2013 — updates MIB-II RFC 1213
- RFC 3396 — updates DHCP RFC 2131

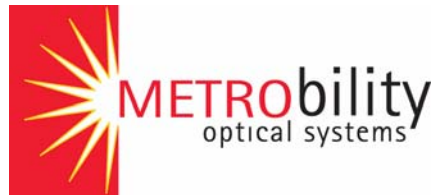
This product shall be handled, stored and disposed of in accordance with all governing and applicable safety and environmental regulatory requirements.

**Product Manuals**

The most recent version of this manual is available online at  
<http://www.metrobility.com/support/manuals.htm>

**Product Registration**

To register your product, go to  
<http://www.metrobility.com/support/registration.asp>



25 Manchester Street, Merrimack, NH 03054 USA  
1.603.880.1833 FAX: 1.603.594.2887  
[www.metrobility.com](http://www.metrobility.com)

5660-000101 A  
2/06

---