IntraSpection™ Personality Module

Bay Networks™ System 2000™ Ethernet Hubs Models 28xx

User's Manual

Asanté Technologies, Inc.
821 Fox Lane
San Jose, CA 95131
1.800.662.9686
www.asante.com

August 1997

Part Number 06-00372-00 Rev. A

SOFTWARE LICENSE AGREEMENT This is a legal agreement between you (either an individual or an entity) and Asanté Technologies, Inc. By opening the package(s) containing the software you are agreeing to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, promptly return the unopened software package(s) and the accompanying items including written materials and binders or other container(s) to the place you obtained them for a full refund.

1. GRANT OF LICENSE. Asanté Technologies grants to you the right to use one copy of the enclosed Asanté Technologies software program per serial number (the "SOFTWARE" is in "use" on a computer when it is loaded into temporary memory (i.e., RAM) or installed into permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. Installation on a network server for the sole purpose of distribution to one or more other computer(s) shall constitute "use" for which a separate license/serial number is required.

2. COPYRIGHT. The SOFTWARE is owned by Asanté Technologies or its suppliers and is protected by United States copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE like any other copyrighted material (e.g., a book or musical recording) except that you may either (a) make one copy of the SOFTWARE solely for backup or archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup or archival purposes. You may not copy the written materials accompanying the software.

3. OTHER RESTRICTIONS. You may not rent or lease the SOFTWARE, but you may transfer the SOFTWARE and accompanying written materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement. You may not reverse engineer, decompile, or disassemble the SOFTWARE. If the SOFTWARE is an update or has been updated, any transfer must include the most recent update and all prior versions.

LIMITED WARRANTY Asanté Technologies, Inc. warrants that the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt. Any implied warranties on the SOFTWARE are limited to ninety (90) days. Some states/countries do not allow limitations of duration of an implied warranty, so the above limitation may not apply to you.

CUSTOMER REMEDIES Asanté Technologies' and its suppliers' entire liability and your exclusive remedy shall be, at Asanté Technologies' option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet Asanté Technologies' Limited Warranty and which is returned to Asanté Technologies with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period. Outside the United States, these remedies are not available without proof of purchase from an authorized non-U.S. source.

NO OTHER WARRANTIES Asanté Technologies and its suppliers disclaim all other warranties, either express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, with regard to the SOFTWARE, the accompanying written materials, and any accompanying hardware. This limited warranty gives you specific legal rights. You may have others which vary from state to state or country to country.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES Asanté Technologies expressly disclaims all liability for any indirect or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interrupted, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this Asanté Technologies product, even if Asanté Technologies has been advised of the possibility of such damages. Any suit or legal action relating to this Agreement or Licensed Programs must be brought within one (1) year of the date the programs are purchased by the original licensee. Because some states/countries do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

LIMITATION OF LIABILITY The liability of Asanté Technologies, Inc. arising from this warranty and sale shall be limited to a refund of the purchase price. In no event shall Asanté Technologies, Inc. be liable for costs of procurement of substitute products or services, or for any lost profits, or for any consequential, incidental, direct or indirect damages, however caused and on any theory of liability, arising from this warranty and sale.

U.S. GOVERNMENT Restricted Rights The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the The Rights in Technical Data and Computer Software clause at DFARS 52.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software—Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Asanté Technologies, Inc., 821 Fox Lane, San Jose, California 95131. If you acquired this product in the United States, this Agreement is governed by the laws of the State of California.

WARRANTY DISCLAIMERS Asanté Technologies, Inc. makes no other warranties, express, implied, or otherwise, regarding the Bay Networks System 2000 Models 28x3 Personality Module, and specifically disclaims any warranty for merchantability or fitness for a particular purpose. The exclusion of implied warranties is not permitted in some states and the exclusions specified herein may not apply to you. This warranty provides you with specific legal rights. There may be other rights that you have which vary from state to state.

Table of Contents

Preface

About This Manual

This manual introduces the IntraSpection Personality Module for the following device(s):

- ❑ The Bay Networks System 2000 Ethernet Hubs (28xx Models)

The manual defines a Personality Module and explains how to install and use the Bay 28xx Personality Module.

> ▲ **Important:** For additional information on using IntraSpection, refer to the IntraSpection User's Manual.

Chapter Contents

This manual is divided into the following chapters:

- ❑ Chapter 1,"Introduction," defines an IntraSpection Personality Module and describes the components of the Bay 28xx Personality Module.
- ❑ Chapter 2,"Installation" explains how to install the Bay 28xx Personality Module.
- ❑ Chapter 3,"Management," explains how to access the Bay 28xx Personality Module's Device Page and how to perform some basic management functions.
- ❑ Chapter 4,"Menus," is a reference section that describes the Personality Module's management menus and their contents.

Document Conventions

This manual uses the following conventions to convey instructions and information:

- ❑ Commands and key words are in **boldface** font.

  - Δ ***Note:*** Noteworthy information, which contains helpful suggestions or references to other sections in the manual, is in this format.

  - ▲ **Important:** Significant information that calls attention to important features or instructions is in this format.

Audience

This manual uses terms and concepts associated with Ethernet networking and hubs; it is recommended that the user of this manual be familiar with the basics of local area networking and Ethernet hubs.

This manual also assumes familiarity with IntraSpection.

1

Introduction

IntraSpection Personality Modules

A Personality Module is a "plug-in" to the IntraSpection system that allows for expanded management of an SNMP (Simple Network Management Protocol) device by specifically addressing the device's proprietary information (the "Private MIB").

Management capabilities are accessed via the Personality Module's Device Page. See Figure 1-1.

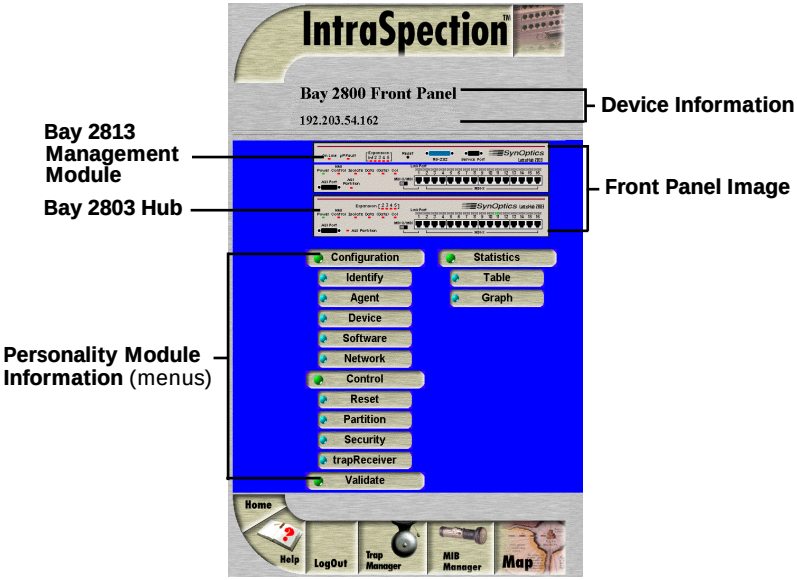

Figure 1-1 Bay 28xx Personalty Module's Device Page

For a description of the Device Page's components, see "Device Page Components" on page 3-3.

Bay 28xx Personality Module

The Bay 28x3 Personality Module allows for expanded management of any of the following models in the Bay Networks System 2000 Ethernet Hub family:

- ❑ **Model 2803** — Ethernet Hub with AUI Interconnect Port.
- ❑ **Model 2813** (Option 04 and Option 05) — Managed Ethernet Hub with AUI Interconnect Port and Advanced or Standard IP/IPX Management Agent.
- ❑ **Model 2813SA** — Managed Ethernet Hub with AUI Interconnect Port and Advanced Analyzer Management Agent.
- ❑ **Model 2814** (Option 04 and Option 05) — Managed Ethernet Hub with 10Base-FL Interconnect Port and Advanced or Standard IP/IPX Management Agent.
- ❑ **Model 2814SA** — Managed Ethernet Hub with 10Base-FL Interconnect Port and Advanced Analyzer Management Agent.

Management Options

The Bay 28xx Personality Module supports the following management options:

- ❑ Device identification information
- ❑ SNMP agent information
- ❑ General device information
- ❑ Software upgrades
- ❑ Network access configuration
- ❑ Device or group resets
- ❑ Group and port partitions
- ❑ Device, group, and port security
- ❑ Trap receiver management
- ❑ Device Page validation
- ❑ Table statistics at the device/group/port levels
- ❑ Graph statistics at the device/group/port levels

See Chapter 3,"Management," for information on performing some basic management functions. See Chapter 4 "Menus" for a complete description of each management option.

System Requirements

Server

- ❑ IntraSpection version 1.01.
- ❑ PC with 80486 or faster microprocessor.
- ❑ 48MB RAM.
- ❑ 100MB free disk space.
- ❑ Windows NT™ 3.51 or higher or Windows NT 4.0 (recommended).
- ❑ Web server that supports Common Gateway Interface (CGI) 1.1 (such as Netscape FastTrack Server™, Microsoft IIS, NCSA HTTP, etc.).
- ❑ Any database management system that supports ODBC (Open Database Connectivity), such as Microsoft Access™, Oracle™, or Microsoft SQL Server.

Client

- ❑ Any Windows™, Windows NT, Macintosh™ or UNIX® workstation.
- ❑ Any World Wide Web browser with Java™ and Javascript support such as Netscape Navigator® (version 3.0 required, 3.01 recommended) or Microsoft Internet Explorer™.

2

Installation

Installing a Personality Module

This chapter explains how to install the Bay 28xx Personality Module.

▲ **Important:** Before installing the Personality Module, make sure that IntraSpection (websuite.exe) is NOT running on the computer.

1. Insert the Personality Module CD into the computer where the IntraSpection Application Server is installed.
2. Open the CD to display its contents.
3. Double-click the **Bay.exe** file.
4. Click **Yes** at the "IntraSpection Personality Module for Bay Networks" dialog box.

   The "IntraSpection Personality Module for the Bay Networks" window appears.
5. Click **Finish** to continue.

   The Personality Module files are decompressed.

   The "IntraSpection Personality Module Welcome" dialog box appears.
6. Click **Next** to continue.

   The "Software License Agreement" window appears. Review the agreement carefully.
7. Click **Yes** to accept the agreement and continue with the installation; click **No** to exit the installation.

The "IntraSpection Personality Module Read Me" window appears. Review the information carefully.

8 Click **Next** to continue

The decompressed Personality Module files are installed onto your computer.

The "Decompression of the Source is Now Complete" dialog box appears.

9 Click **OK** to continue with the installation.

The "Select Module to Install" window appears, displaying the Bay.ipm file. See Figure 2-1.

Figure 2-1 Select Module to Install window

10 Click once on the **Bay.ipm** file.

11 Click **Open**.

The "Enter Product Serial Number" window appears.

12 Enter the serial number that came with your copy of the Personality Module.

The serial number is located on the inside cover of this User's Manual.

▲ **Important:** The serial number is case-sensitive; enter it exactly as shown.

13 Click **OK**.

The "IntraSpection Module Installation" window appears.

▲ **Important:** This window should be pointing to the directory that contains the IntraSpection (websuite.exe) program. If it is not, click **Browse** and locate that directory.

14 Click **OK**.

Δ ***Note:*** A "Select Database" window may appear. If it does, select **vendor.mdb**, then click **OK**.

Δ ***Note:*** A "Updating IntraSpection System Files" window may appear, if it does, click **OK**.

The installer program installs both Personality Modules into the IntraSpection Application Server.

Installation is complete when the "Installation Completed Successfully" dialog box appears.

15 Start the IntraSpection Application Server, following the guidelines below:

❑ Windows NT 3.51 users: double-click the **IntraSpection** icon (located in the Programs group).

❑ Windows NT 4.0 users: open the **Start** menu, select **Programs**, then **IntraSpection**.

For information on accessing the Personality Modules' Device Pages and performing some basic management functions, see Chapter 3, "Management."

3

Management

This chapter explains how to access and use the Bay 28xx Personality Module's Device Page. The Device Page provides access to the Personality Module's management options.

Accessing the Device Page

To access the Device Page for a Bay 28xx device, you must first create a map of the network.

1. Make sure the Personality Module is installed and the IntraSpection Application Server is running.
2. Access IntraSpection from any Java-enabled Web browser (requires logging into IntraSpection).

   ▲ **Important:** For help on accessing and logging into IntraSpection, refer to the IntraSpection User's Manual.
3. After you are logged into IntraSpection, click **Auto Discovery** on the IntraSpection Main Menu.

   The AutoDiscovery Page appears.
4. Complete each field on the AutoDiscovery Page, following the guidelines below:

   - ❑ Type the IP subnet address of the Bay 28xx device to be managed in the **Segment** field.

     (This is the subnet address of the stack's management module; the default setting for this field is the subnet address of the browser being used to access IntraSpection.)
   - ❑ Type the management module's community string in the **Community** field.

- ❑ Make sure the **Enterprise ID** field has a value of **all**.
- ❑ Type the lowest (beginning) IP address on your network in the **Low IP Address** field.
- ❑ Type the highest (last) IP address on your network in the **Hi IP Address** field.
- ❑ Select **New** in the **Discovery Mode** field to create a new map, or select **Append** to attach this map to the map that is stored in your system's buffer (if any).

5 Click **Apply**.

IntraSpection builds a map of your network. The map contains icons which represent each "discovered" SNMP device on the network. Figure 3-1 is an example map.

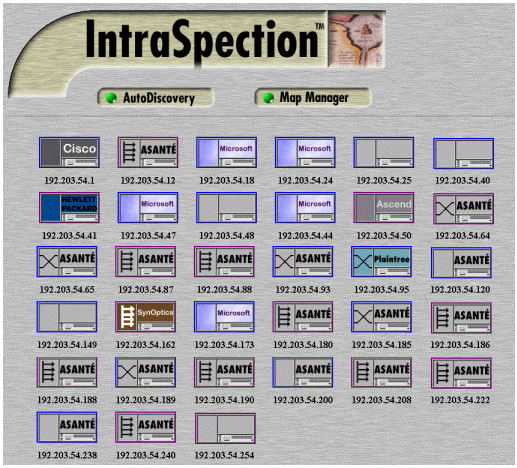

Figure 3-1 Discovered network map

6 Click once on the Bay 28xx device's icon.

▲ **Important:** The Bay 28xx's device icons are labeled "Synoptics."

The Device Page for the selected Bay 28xx device appears (see Figure 3-2 on page 3-3).

For information on the Device Page's components, see "Device Page Components" on page 3-3.

For information on performing basic management functions, see "Performing Basic Management Functions" on page 3-7.

Device Page Components

The Device Page consists of several components; including, device information, a front panel image, and management menu items. See Figure 3-2.

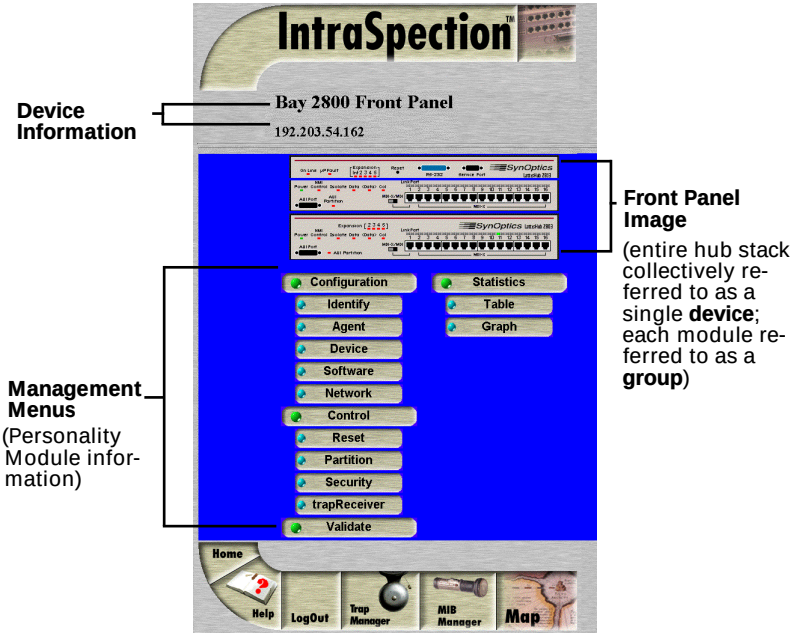

Figure 3-2 Device Page components

Device Information

The following device information is displayed at the top of the Device Page:

- ❑ A description of the device (i.e.,“Bay 2800 Front Panel”).
- ❑ The device’s IP address.

Front Panel Image Components

The front panel image contains the following components (as illustrated in Figure 3-3):

- ❑ **Device** — the entire stack of hubs and the attached management module.
- ❑ **Group** — each module within the device.
- ❑ **Port** — each port on each group.
- ❑ **Status LEDs** — real-time LEDs that represent the LEDs on the device. These LEDs indicate port activity.

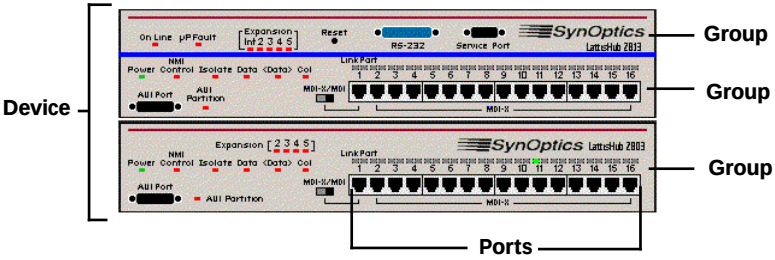

Figure 3-3 Front panel image components

▲ **Important:** Throughout this manual, the term **device** refers to the entire stack of hubs; the term **group** refers to an individual module; the term **port** refers to an individual port.

Selecting the Device for Management

A Bay 28xx device can be managed at different levels; that is, at the device, group, and/or port level.

For example, if a group is selected and you select the **Graph** menu, statistics for that group (single module) are displayed. If the device is selected and you select **Graph**, statistics for the device (entire hub stack) are displayed.

Selecting an Item

Target Item	Action
Device (entire hub stack)	Do not click anything on the front panel image.
Group (single module)	Click once on the group.
Port	Click once on the port.

Deselecting an Item

Target Item	Action
Device	Click once on a group or port.
Group	Click again on the selected group.
Port	Click again on the selected port.

Menu Components

The menus on the Device Page provide access to the different management options supported by the Bay 28xx Personality Module.

Tables

Some menus contain tables with information that is configurable directly on-screen from your Web browser while others contain information that is read-only.

The following tables describe how to recognize configurable and read-only information.

Configurable Information

Menu item	Action
Drop-down menu	Select from an available option.
White-colored fields	Type information.

Read-only Information

Menu item	Action
Green- or gray-colored fields	None; read-only field.

Table Columns

Table columns can be resized by placing the mouse pointer on a column title's left or right side (until a double arrow appears) and dragging the column to the left or to the right, as desired.

Buttons

Some menus contain buttons which allow you to edit/and or update the page.

The table below describes the different buttons that are available and their functions.

Button	Action
Apply	Applies any changes made to the device.
Refresh	Updates the page with the latest information.
Modify	Modifies a selected entry.
Add	Adds an entry into the table.

Performing Basic Management Functions

This section explains how to perform some basic management functions with a Bay 28xx Personality Module.

▲ **Important:** This section describes only how to configure and manage a Bay 28xx device via the functions available with its Personality Module. For additional information on configuring or managing a Bay 28xx device, refer to the device's User's Manual.

This section covers the following tasks:

Configuration Tasks

Management Tasks

Setting Community Strings

Community strings define access rights for reading and writing SNMP data objects for a device.

The community strings (read community and write community) for a Bay 28xx device are manually set in the management module via the module's console port. In order to manage the device with IntraSpection, the community strings must be set in IntraSpection to match those set in the device.

▲ **Important:** It is recommended that you set the community strings for a Bay 28xx device in IntraSpection **before** you attempt to perform any network management functions using the Personality Module

To set the community strings for a management module in IntraSpection:

▲ **Important:** You must know the device's community strings in order to enter them in IntraSpection. Refer to the Bay 28xx device's User's Manual for instructions on viewing the device's community strings.

1 On the Device Page, click the **map** icon on the IntraSpection navigation bar (located at the bottom of the screen), as shown in Figure 3-4.

Figure 3-4 IntraSpection navigation bar

The most recently discovered map appears.

2 Click the **Map Manager** button.

The Map Manager Page appears, similar to Figure 3-5.

Figure 3-5 IntraSpection Map Manager Page

3 Click the **Edit Device** button.

The Map Configuration Table appears, similar to Figure 3-6.

Figure 3-6 Map Configuration Table

4 Enter the device's IP address in the **IP Address** field.

5 Enter the device's read community string in the **Read Community String** field.

6 Enter the device's write community string in the **Write Community String** field.

7 Click **Apply**.

The read and write community strings for the device are configured.

Configuring Network Access Parameters

To configure and/or manage a Bay 28xx device over the network or via out-of-band access, the device needs to be properly configured with network access parameters. These parameters are initially set-up in the management module via the module's console port; however, some can be modified using IntraSpection.

To configure network access parameters:

1 Do not select any item on the front panel image. (This selects the entire hub stack.)

2 Click **Network**.

The Network Information table appears, similar to Figure 3-7.

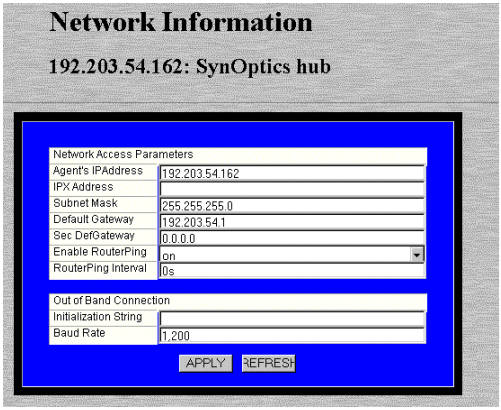

Figure 3-7 Network Information table

3 To configure in-band parameters, click once in a Network Access Parameters field.

To configure out-of-band parameters, click once in an Out-of-Band Connection field.

▲ **Important:** For a description of each field, see "Network" on page 4-8.

4 Type the new information or select an option from the drop-down menu.

5 Click **Apply.**

The network access parameters are configured. Click **Refresh** to view updated information.

Configuring Identification Information

To help with device identification, you can add certain details; such as, the device's physical address, name, location, and contact information.

To configure identification information:

1 Do not select any item on the Device Page's front panel image. (This selects the entire hub stack.)

2 Click **Identify**.

The Device Identification table appears, similar to Figure 3-8.

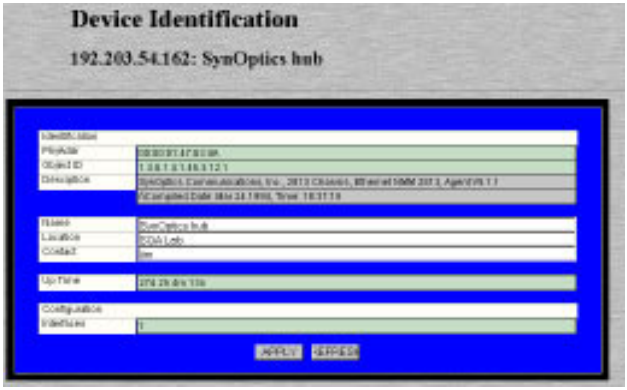

Figure 3-8 Device Identification table

3 Click once in the field to be edited.

For a description of each field, see "Identify" on page 4-3.

▲ **Important:** Only those fields that are colored white can be edited.

4 Type the new information.

▲ **Important:** A maximum of 254 characters (including spaces) is allowed.

5 Click **Apply.**

The identification information is configured.

Click **Refresh** to view updated information.

Performing a Software Upgrade

A Bay 28xx device's software can be upgraded via IntraSpection.

To upgrade a Bay 28xx device's software:

1. Click **Software**.

   The Software Information table appears, similar to Figure 3-9.

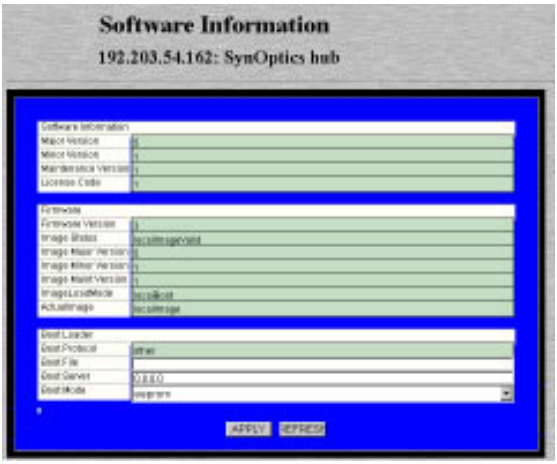

Figure 3-9 Sofware Information table

2. Type the software's file name and network path in the **Boot File** field.
3. Type the server's address where the software file resides in the **Boot Server** field.
4. Open the **Boot Mode** drop-down menu and select **net** (sets the device to load the file from a server on the network).
5. Click **Apply**.
6. Reset the device, following the instructions on page 3-16, to initiate downloading.

Updating the Device Page

The files for a Bay 28xx Personality Module are stored within the IntraSpection Application Server's database. Occasionally, these files should be updated from the Device Page to ensure that you are viewing the hub stack's latest information.

To update the Personality Module's Device Page:

1. Click **Validate**.

   The Device Page is updated with the latest information for the Personality Module.

   After the Device Page is updated, the IntraSpection Map Manager Page appears.

2. Click **AutoDiscovery** to rediscover the Device Page.

   ▲ **Important:** See "Accessing the Device Page" on page 3-1 for instructions on discovering devices with AutoDiscovery.

Viewing General Device Information

You can view information on a Bay 28xx device's hardware; such as, its EPROM size, chassis type, and system status.

To view general device information:

1 Do not select any item on the Device Page's front panel image. (This selects the entire hub stack.)

2 Click **Device**.

The Device Information table appears, similar to Figure 3-10.

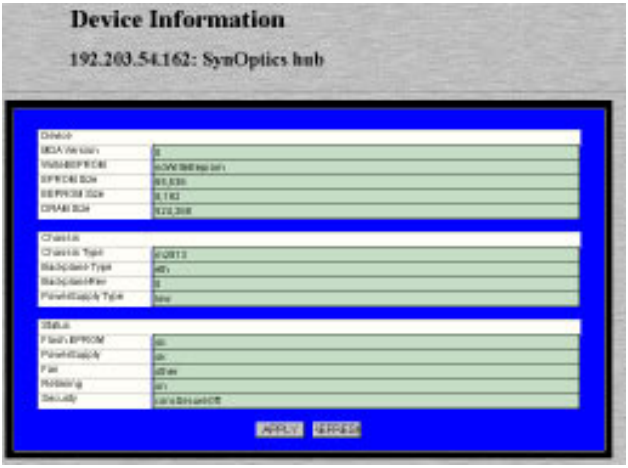

Figure 3-10 Device Information table

Δ ***Note:*** The information displayed on this page is read-only.

For a description of each field, see "Device" on page 4-5.

3 Click **Refresh** to view updated information.

Viewing SNMP Agent Information

You can view information on a Bay 28xx device's SNMP agent; including, the agent type and mode, MIB level, and software configuration load mode.

To view SNMP agent information:

1 Do not select any item on the Device Page's front panel image. (This selects the entire hub stack.)

2 Click **Agent**.

The Agent Information table appears, similar to Figure 3-11.

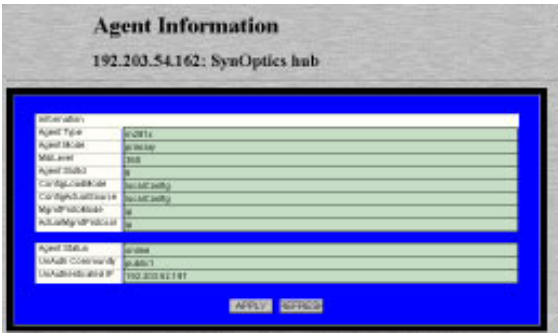

Figure 3-11 Agent Information table

Δ ***Note:*** The information displayed in this table is read-only.

For a description of each field, see "Agent" on page 4-4.

3 Click **Refresh** to view updated information.

Resetting a Group or Device

You can reset a Bay 28xx device (resets the entire stack) or a group (resets an individual hub or a management module).

To perform a reset:

1. To reset a group (an individual hub or a management module), click once on that group. To reset the device (the entire hub stack), do NOT select anything.
2. Click **Reset**.

   Depending on what was selected (either the device or a group), the Agent Control table or Group Reset table appears, similar to Figure 3-12 and Figure 3-13, respectively.

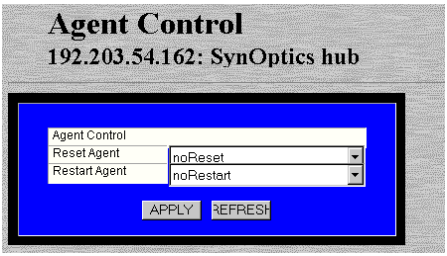

Figure 3-12 Agent Control table (Device Reset)

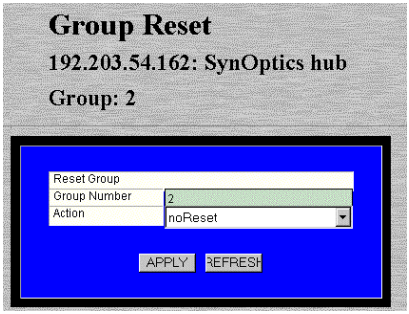

Figure 3-13 Group Reset table (Group Reset)

3. Open the **Action** drop-down menu and select **reset**.
4. Click **Apply**.

   The selected group or device is reset.

   ▲ **Important:** To abort the reset, click on the browser's back arrow to go back one page.

Disabling a Group

You can temporarily disable an individual group within a Bay 28xx device.

▲ **Important:** The device (entire hub stack) and the device's management module **cannot** be disabled.

To disable a group:

1. Select the group to be disabled on the Device Page's front panel image by clicking on it once.
2. Click **Partition**.

   The Group Partition table appears for the selected group, similar to Figure 3-14.

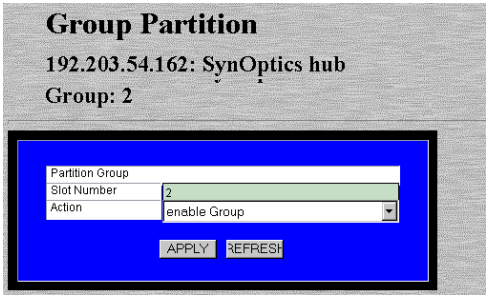

Figure 3-14 Group Partition table

3. Open the **Action** drop-down menu and select **partition indefinitely**.
4. Click **Apply**.

   The group is disabled. It remains disabled until you manually enable it.

Enabling a Group:

1. Select the group to be enabled by clicking on it once on the front panel image.
2. Click **Partition**.
3. Open the **Action** drop-down menu and select **enable**.
4. Click **Apply**.

   The group is enabled.

Partitioning a Port

Port partitioning is an operation that is done **automatically** by the hub in certain circumstances to stop transmission on a port, if the port is enabled for automatic partitioning.

To enable or disable automatic partitioning:

1. Select the port to be partitioned by clicking on it once.
2. Click **Partition**.

   The Port Partition table appears, similar to Figure 3-15.

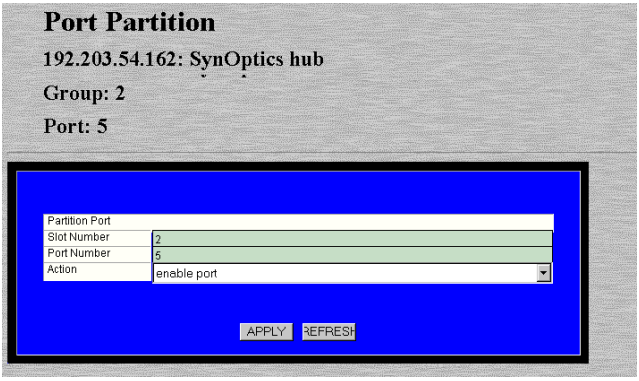

Figure 3-15 Port Partition table

3. Open the **Action** drop-down menu and select **enable port** (to enable automatic partitioning) or **disable port** (to disable automatic partitioning).
4. Click **Apply**.

   The port's partitioning state is modified.

   Click **Refresh** to view updated information.

Managing Trap Receivers

A Bay 28xx device can be set to generate traps. Traps are messages sent across the network to an SNMP network manager (such as IntraSpection). They alert you to faults or changes that occur to the device.

▲ **Important:** Refer to the Bay 28xx device's User's Manual for instructions on setting when traps occur.

This section describes how to add and delete trap receivers. Trap receivers are management stations designated to receive traps when they occur.

Adding a Trap Receiver

To add a trap receiver:

1. Do not select any item on the Device Page's front panel image. (This selects the entire device.)
2. Click **trapReceiver**.

   The Trap Receiver Table appears, similar to Figure 3-16.

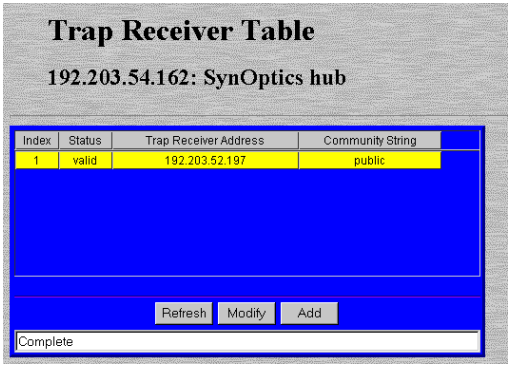

Figure 3-16 Trap Receiver Table

3. Click **Add**.

   The Add Dialog box appears.
4. Open the **Status** menu and select **valid**.
5. Type the IP address of the management station that is to receive traps in the **Trap Receiver Address** field.

   ▲ **Important:** Do not type an IP address of 0.0.0.0.

6 Type the community string of the management station in the **Community String** field.

7 Click **Apply**.

An entry for the management station appears in the table. If it does not appear, click **Refresh**.

Deleting a Trap Receiver

To delete a trap receiver entry:

1 Click once on the row containing the entry to be deleted in the Trap Receiver Table.

2 Click **Modify**.

The Modify Dialog box appears.

3 Open the **Status** drop-down menu and select **invalid**.

4 Click **Apply.**

You are returned to the Trap Receiver Table

5 Click **Refresh** in the Trap Receiver Table.

The trap receiver is deleted.

Modifying a Trap Receiver

To change the IP address of a trap receiver entry:

1 Delete the trap receiver entry, following the directions above.

2 Add a new trap receiver entry, following the instructions on page 3-19.

Setting Device, Group, and Port Security

You can restrict access to a Bay 28xx device, to one of its groups, or to one of its ports by turning on the device's Security feature.

Device Security

To set device security:

1 Do not select any item on the front panel image. (This selects the entire hub stack).

2 Click **Security**.

The Device Security table appears, similar to Figure 3-17.

Figure 3-17 Device Security table

3 Open the **Security Status** drop-down menu and select **ConcSecureOn**.

This sets security for the device; any node that is heard on the device, which is not allowed on this device, will cause the action specified in the **Sec Violation Action** menu.

4 Open the **Sec Violation Action** menu and select the action to occur if an unauthorized node attempts to access the device.

See "Security" on page 4-11 for a description of each violation action.

5 Click **Apply**.

Security for the device is configured.

Click **Refresh** to view updated information.

Group Security

To set group security:

1. Select the group for which security is to be set by clicking on it once on the front panel image.

2. Click **Security**.

   The Group Security table appears, similar to Figure 3-18.

Figure 3-18 Group Security table

3. Open the **Security Status** drop-down menu and select **On**.

   This sets security for the group; any node that is heard on the group, which is not allowed on this group, will cause the action specified in the **Sec Violation Action** menu.

4. Open the **Sec Violation Action** menu and select the action to occur if an unauthorized node attempts to access the group.

   See "Security" on page 4-11 for a description of each violation action.

5. Click **Apply**.

   Security for the group is configured.

   Click **Refresh** to view updated information.

Port Security

To set port security:

1. Select the port for which security is to be set by clicking on it once on the front panel image.

2. Click **Security**.

   The Port Security table appears, similar to Figure 3-19.

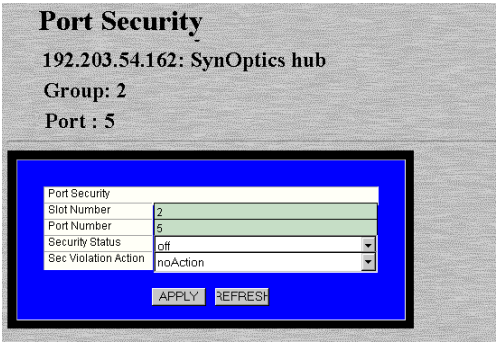

Figure 3-19 Port Security table

3. Open the **Security Status** drop-down menu and select **On**.

   This sets security for the port; any node that is heard on the port, which is not allowed on this port, will cause the action specified in the **Sec Violation Action** menu.

4. Open the **Sec Violation Action** menu and select the action to occur if an unauthorized node attempts to access the port.

   See "Security" on page 4-11 for a description of each violation action.

5. Click **Apply**.

   Security for the port is configured.

   Click **Refresh** to view updated information.

Viewing Statistics

Statistics for a Bay 28xx device can be viewed for the device, a selected group, or a selected port in two different formats: table or graph. Statistics collected include good frames, collisions, runts, and alignment errors.

Table Statistics

1 Select a group or a port for which statistics are to be gathered by clicking on it once. To view statistics for the device, do not select anything.

2 Click **Table**.

Table Statistics appear for the group, port, or device selected. Figure 3-20 displays statistics for a port.

Figure 3-20 Table Statistics page

For a description of each object, see "Statistics" on page 4-15.

3 Open the **Sampling Interval** drop-down menu and select the number of seconds to poll for statistics.

Statistics are automatically gathered at the set number of seconds in the following columns:

- ❑ **Curr** — (current) the number of occurrences each second.
- ❑ **Peak** — the largest number of occurrences since opening or resetting the screen.
- ❑ **Avg** — (average) the average number of occurrences since opening or resetting the screen.
- ❑ **Total** — the total number of occurrences since opening or resetting the screen.

4 Click **Reset** to reset the table's counters to zero.

Graph Statistics

1 Select a group or a port for which statistics are to be gathered by clicking on it once. To view statistics for the device, do not select anything.

2 Click **Graph**.

Graph Statistics appear for the group, port or device selected. Figure 3-21 displays statistics for a group.

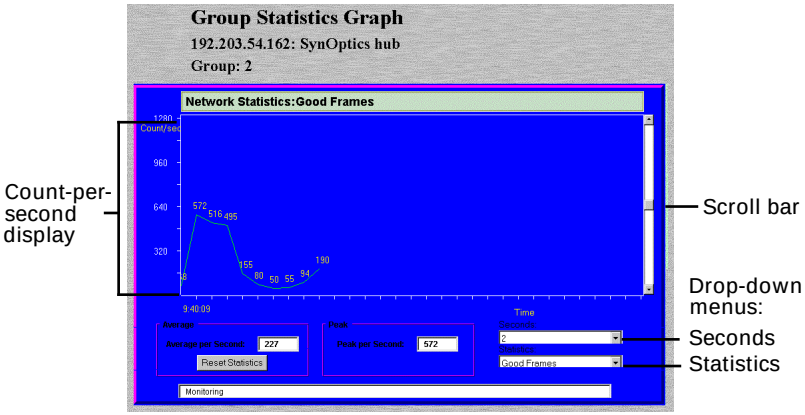

Figure 3-21 Graph Statistics page

3 Open the **Statistics** drop-down menu and select the object to be monitored.

For a description of each object, see "Statistics" on page 4-15.

4 Open the **Seconds** drop-down menu and select the number of seconds for which statistics are to be gathered.

5 Use the scroll button to change the graph's count-per-second display (scroll up to increase the count-per-second, scroll down to decrease it).

- ❑ **Average per Second** — the average number of occurrences since opening or resetting the screen.
- ❑ **Peak per Second** — the largest number of occurrences since opening or resetting the screen.

6 Click **Reset** to reset the graph's counters to zero.

4

Menus

This chapter describes each management menu and its contents on the Bay 28xx Personality Module's Device Page.

The table below provides a brief description of each menu; the sections that follow explain each menu in detail.

Table 4-1 Personality Module Menu Descriptions

Menu	Description
Configuration	Title for the submenus listed below it; this menu cannot be selected.
Identify	Allows you to configure device identification information. See "Identify" on page 4-3.
Agent	Allows you to view the device's SNMP agent information. See "Agent" on page 4-4.
Device	Allows you to view general device information. See "Device" on page 4-5.
Software	Allows you to determine the download filename, server address, and boot method for the device. See "Software" on page 4-6.
Network	Allows you to view and configure network access information (both in-band and out-of-band) for the device. See "Network" on page 4-8.
Control	Title for the submenus listed below it; this menu cannot be selected.
Reset	Allows you to reset the device or an individual group. See "Reset" on page 4-9.
Partition	Allows you to enable or disable a group or partition a port. See "Partition" on page 4-10.
Security	Allows you to enable security on the device, a group, or a port. See "Security" on page 4-11.

Menu	Description
Trap Receiver	Allows you to determine which management stations can receive traps from the device. See “Trap Receiver” on page 4-13.
Validate	Updates the Device Page with the latest information from the IntraSpection Application Server database. See “Validate” on page 4-14.
Statistics	Title for the submenus listed below it; this menu cannot be selected.
Table	Allows you to view real-time statistical data, in table format, on the device, a group, or a port. See “Table” on page 4-15.
Graph	Allows you to view real-time statistical data, in graph format, on the device, a group, or a port. See “Graph” on page 4-16.

Configuration

This menu is not a management option; it is a title for the sub-menus listed below it. This menu CANNOT be selected.

Identify

This menu allows you to view and configure identification information for the device.

Table 4-2 describes each field in the Identify menu.

Δ ***Note:*** For instructions on using this menu, see "Configuring Identification Information" on page 3-11.

Table 4-2 Identify Menu

Field	Description
Physical Address	Read-only field; displays the device's hardware address.
Object ID	Read-only field; displays the device's SNMP identifying number.
Description	Read-only field; displays a description of the device.
Name	Configurable field; assigns a name to the device. ***Note:*** A maximum of 254 characters (including spaces) is allowed.
Location	Configurable field; assigns a location (where the device is physically located). ***Note:*** A maximum of 254 characters (including spaces) is allowed.
Contact	Configurable field; assigns a name of the person responsible for the device. ***Note:*** A maximum of 254 characters (including spaces) is allowed.
Up Time	Read-only field; displays the amount of time (in days, hours, minutes, and seconds) the device has been operational since the last time it was off-line.
Interfaces	Read-only field; displays the number of network interfaces present on the device.

Agent

This menu displays read-only SNMP agent information for a Bay 28xx device.

Table 4-3 describes each field in the Agent menu.

Δ ***Note:*** For instructions on using this menu, see "Viewing SNMP Agent Information" on page 3-15.

Table 4-3 Agent Menu

Field	Description
Agent Type	Read-only; displays the agent's module type (such as **m281x**).
Agent Mode	Read-only; displays whether the management module is operating in primary (1) or secondary (2) mode. ***Note:*** A Bay 28x3 device can contain a secondary management module. This menu displays the mode of the active management module.
Mib Level	Read-only; displays the current release supported by the agent. ***Note:*** This field does not display periods within the release number; "3.60" displays as "360."
Agent Slotid	Read-only; displays the number of the group containing the agent.
ConfigLoadMode	Read-only; displays where the agent is receiving its code at start-up.
ConfigActualSource	Read-only; displays the configuration mode that was used at the last start-up.
MgmtProtolMode	Read-only; displays the configuration mode the agent will use at the next start-up.
AcutalMgmtProtocol	Read-only; displays the configuration mode the agent used at the last start-up.
Agent Status	Read-only; displays the status of the agent: on-line or off-line.
UnAuth Community	Read-only; displays the community string of the last network station with an unauthorized IP address that attempted to access the management module.
UnAuthenticatedIP	Read-only; displays the IP address of the last network station that attempted to access the device with an invalid community string. (The community string that was used is displayed in the **UnAuth Community** field.)

Device

This menu allows you to view general information on a Bay 28x3 device.

Table 4-4 describes each field in the Device menu.

Δ ***Note:*** For instructions on using this menu, see "Viewing General Device Information" on page 3-14.

Table 4-4 Device Menu

Field	Description
MDA Version	Read-only field; displays the device's current version number. ❑ **0** — Rev. A ❑ **1** — Rev. B ❑ **2** — Rev. C, etc.
WriteEEPROM	Read-only field; displays the device's write EEPROM status.
EPROM Size	Read-only field; displays the size (in bytes) of the device's EPROM.
EEPROM Size	Read-only field; displays the size (in bytes) of the device's EEPROM.
DRAM Size	Read-only field; displays the size (in bytes) of the device's DRAM.
Chassis Type	Read-only field; displays the device's chassis type. For example, **m2813**.
Backplane Type	Read-only field; displays the device's backplane type.
Backplane Rev	Read-only field; displays the device's backplane revision number.
PowerSupply Type	Read-only field; displays the device's power supply type. If the chassis has a redundant backplane, the agent returns **redundantCapable** (5).
Flash EPROM	Read-only field; displays the operational status of the flash device of the agent. ❑ **OK** — the flash device is operational. ❑ **Fail** — the flash device configuration on the board is not valid or the flash EEPROMs on the board have failed.
PowerSupply	Read-only field; displays the chassis' power supply status.
Fan	Read-only field; displays the status of the chassis' cooling fan.
Retiming	Read-only field; displays whether the device has retiming turned on or off.
Security	Read-only field; displays if the security features for the device are active or inactive.

Software

This menu allows you to view the agent's software and firmware information and set the download file name, server address, and boot method for the device.

Table 4-5 describes each field in the Software menu.

Δ ***Note:*** For instructions on using this menu, see "Performing a Software Upgrade" on page 3-12.

Table 4-5 Software Menu

Field	Description
Major Version	Read-only field; displays the agent's major software version number.
Minor Version	Read-only field; displays the agent's minor software version number.
Maintenance Version	Read-only field; displays the agent's maintenance version number.
License Code	Read-only field; displays the license code assigned to the agent.
Firmware Version	Read-only field; displays the agent's firmware version number.
Image Status	Read-only field; displays whether or not the agent has a valid local image on board.
Image Major Version	Read-only field; displays the major software version number of the locally stored image.
Image Minor Version	Read-only field; displays the minor software version number of the locally stored image.
Image Maint Version	Read-only field; displays the maintenance software version number of the locally stored image.
ImageLoadMode	Read-only field; displays the boot mode for loading image code. ❏ **remoteBoot** — from the network. ❏ **localBoot** — from the device (local) ❏ the device tries to load from network first and then falls back to **localBoot** if the network boot fails.
Actual Image	Read-only field; displays whether the agent loaded code from the network or used a local image.
Boot Protocol	Read-only field; displays the boot protocol used to load the module with its software.

Field	Description
Boot File	Configurable field; sets the name and network path of the boot file for the device.
Boot Server	Configurable field; sets the boot server's IP address.
Boot Mode	Configurable field; determines the method for loading the image file for the device. ❑ **eeprom** — sets the device to boot from code stored in device (default setting). ❑ **net** — sets the device to boot from a TFTP server on the network.

Network

This menu allows you to view and configure network access information (both in-band and out-of-band) for the device.

Table 4-6 describes each field in the Network menu.

Δ ***Note:*** For instructions on using this menu, see "Configuring Network Access Parameters" on page 3-10.

Table 4-6 Network Menu

Field	Description
Agent's IP Address	Configurable field; displays the IP address of the device's SNMP agent.
IPX Address	Configurable field; only displays an address if the device is using **IPX** or **IP and IPX**.
Subnet Mask	Configurable field; specifies the subnet address of the device.
Default Gateway	Configurable field; specifies the address of the default gateway to which the device is assigned.
Sec DefGateway	Configurable field; specifies a secondary gateway address (to be used if there is a problem with the default gateway's address).
Enable RouterPing	Configurable field; determines whether or not the agent will periodically send out pings to the default router. ❑ **On** — agent sends out pings to the default router. ❑ **Off** — agent does not send out pings to the default router.
RouterPing interval	Configurable field; determines the time interval that the agent uses to send out pings to the default router. ***Note:*** This value is in TimeTicks (hundredths of a second).
Initialization String	Configurable field; displays the initialization string used by the network management station to establish an out-of-band connection with the device.
Baud Rate	Configurable field; displays the baud rate for accessing the device via out-of-band management. The default is **9600**.

Control

This menu is not a management option; it is a title for the sub-menus listed below it. This menu cannot be selected.

Reset

This menu allows you to reset the device or a selected group within the device.

Table 4-7 and Table 4-8 describe each field in the Reset menu (for the device or a selected group).

Δ ***Note:*** For instructions on using this menu, see "Resetting a Group or Device" on page 3-16.

Table 4-7 Reset Menu (Device Level)

Field	Description
Reset Agent	Configurable field; resets the device. ❑ **noReset** — does not reset the device. ❑ **reset** — resets the device and performs a download and restart.
Restart Agent	Configurable field; restarts the device. ❑ **noRestart** — does not restart the device. ❑ **restart** — restarts the device. This initializes all the counters, re-reads the EEPROM data structure, and starts executing from the beginning of the code.

Table 4-8 Reset Menu (Group Level)

Field	Description
Group Number	Read-only field; displays the number of the selected group to be reset.
Action	Configurable field; resets the selected group's board. ❑ **noReset** — does not reset the group's board. ❑ **reset** — resets the group's board.

Partition

This menu allows you to disable or enable a group or configure a port for automatic partitioning.

Table 4-9 and Table 4-10 describe each field in the Partition menu (for a selected group or a port).

▲ **Important:** The stack's management module CANNOT be disabled.

Δ ***Note:*** For instructions on using this menu, see "Disabling a Group" on page 3-17 and "Partitioning a Port" on page 3-18.

Table 4-9 Partition Menu (Group Level)

Field	Description
Slot Number	Read-only field; displays the number of the selected group to be partitioned.
Action	Configurable field; indicates if the group's board is partitioned or enabled. ❑ **enable Group** — enables the selected group. ❑ **partition indefinitely** — partitions the selected group. The group remains partitioned until the **enable Group** option is selected.

Table 4-10 Partition Menu (Port Level)

Field	Description
Slot Number	Read-only field; displays the number of the selected group to be partitioned.
Port Number	Read-only field; displays the number of the selected port to be partitioned.
Action	Configurable field; indicated is the port is partitioned or enabled. ❑ **enable port** — enables the selected port. ❑ **partition indefinitely** — partitions the selected port. The port remains partitioned until the **enable port** option is selected.

Security

This menu allows you to enable security for the device, a group, or a port.

The security feature allows you to restrict access to the device, to a group, or to a port. Any node that is heard on the device/group/port, which is not allowed on the device/group/port (i.e., not in the **Auth Node Table** with the **slotIndex** equal to this board or **0** for all boards) causes the action specified in the **Violation Action** field.

Table 4-11, Table 4-12, and Table 4-13 describe each field in the Security menu (for the device, a group, or a port, respectively).

Δ ***Note:*** For instructions on using this menu, see "Setting Device, Group, and Port Security" on page 3-21.

Table 4-11 Security Menu (Device Level)

Field	Description
Security Status	Configurable field; determines the security status for the device. ❑ **concSecureOn** — security for the device is on and activated for every port. ❑ **portCheckOn** — security for a port is on. ❑ **slotCheckOn** — security for a group is on. ❑ **concSecureOff** — security is off for the device.
Sec Violation Action	Configurable field; determines the action to occur if an unauthorized node violation occurs. ❑ **no action** — no action occurs. ❑ **sendtrap** — sends a trap to the receiving trap station. ❑ **Partition** — partitions the target port. ❑ **sendTrapPartition** — sends a trap and partitions the target port.
Security Lock	Configurable field; determines the ability to set security. ❑ **locked** — agent refuses all requests to modify the security configuration. ❑ **notlocked** — requests to modify security configuration will be handled in the usual manner.

Table 4-12 Security Menu (Group Level)

Field	Description
Group Number	Read-only field; displays the number of the selected group.
Security Status	Configurable field; determines the security status for the group. ❑ **on** — any node that is heard on this group, which is not allowed on this group, will cause the action specified in the **Sec Violation Action** field. ❑ **off** — security is off for the group.
Sec Violation Action	Configurable field; determines the action to occur if an unauthorized node violation occurs on the group. ❑ **no action** — no action occurs. ❑ **sendtrap** — sends a trap to the receiving trap station. ❑ **partition** — partitions the target port. ❑ **sendTrapPartition** — sends a trap and partitions the target port.

Table 4-13 Security Menu (Port Level)

Field	Description
Slot Number	Read-only field; displays the number of the selected group.
Port Number	Read-only field; displays the number of the selected port.
Security Status	Configurable field; determines the security status for the port. ❑ **on** — any node that is heard on this port, which is not allowed on this port, will cause the action specified in the **Sec Violation Action** field. ❑ **off** — security for the port is off.
Sec Violation Action	Configurable field; determines the action to occur if an unauthorized node violation occurs on the port. ❑ **no action** — no action occurs. ❑ **sendtrap** — sends a trap to the receiving trap station. ❑ **partition** — partitions the target port. ❑ **sendTrapPartition** — sends a trap and partitions the target port.

Trap Receiver

This menu allows you to determine the management stations that will receive traps from the device.

Table 4-14 describes each field in the Trap Receiver menu.

Δ ***Note:*** For instructions on using this menu, see "Managing Trap Receivers" on page 3-19.

Table 4-14 Trap Receiver Menu

Field	Description
Index	Read-only field; displays the number of the table entry.
Status	Configurable field; displays the status of the trap receiving station. ❑ **valid** — trap receiving station is active. ❑ **invalid** — trap receiving station is inactive (deletes the trap receiving station).
Trap Receiver Address	Configurable field; sets the IP address of the management station that can receive traps. To change or add an address, see "Managing Trap Receivers" on page 3-19.
Community String	Configurable field; sets the write community string of the receiving management station.

Validate

This menu updates the Bay 28xx Personality Module with the latest information from the IntraSpection Application Server database. This menu only needs to be used when you want to ensure you are viewing the latest information on the Bay 28xx device.

When this option is selected, you are returned to the IntraSpection map page.

Δ ***Note:*** See "Updating the Device Page" on page 3-13 for instructions on using this menu.

Statistics

This menu is not a management option; it is a title for the sub-menus listed below it. This menu CANNOT be selected.

Table

This menu allows you to view real-time statistical information, in a table format, on the device, a selected group, or a selected port.

Table 4-15 describes each field in the Table menu.

Δ ***Note:*** For instructions on using this menu, see "Viewing Statistics" on page 3-24.

Table 4-15 Table Menu

Field	Description
Sampling Interval	Configurable field; allows you to set the amount of time (in seconds) that the device/group/port is polled for information.
Reset	Button; resets the counters to zero in the statistics table.
Object	Read-only fields; displays the objects for which statistics are gathered. ❑ **Good Frames** — the total number of good or readable frames (frames without error). ❑ **Multicast Frames** — the total number of frames that are simultaneously received and are directed to an active non-broadcast group address. This does not include frames received with a frame-too-long, runt, FCS, or alignment error. ❑ **Broadcast Frames** — the total number of frames that are successfully received and are directed to the broadcast group address. ❑ **Collisions** — the total number of collisions. ❑ **Frames TooLong Errors** — the number of frames that were longer than 1,518 bytes. ❑ **Runts** — the number of frames that were shorter than 64 bytes. ❑ **Alignment Errors** —the number of frames that were an integral number of octets in length and did not pass the FCS check. ❑ **Fragments** — the number of frames received that are less than the minimum permitted frame size and have a bad FCS or alignment error. ❑ **FCS Errors** — the number of frames that failed Cyclic Redundancy Check (CRC). ❑ **Late Collisions** — the number of collisions that occurred after the 64-byte collision window.

Graph

This menu allows you to view real-time statistical information, in a graph format, on the device, a selected group, or a selected port.

Table 4-16 describes each field in the Graph menu.

Δ ***Note:*** For instructions on using this menu, see "Viewing Statistics" on page 3-24.

Table 4-16 Graph Menu

Field	Description
Seconds	Drop-down menu; specifies the amount of time (in seconds) that the device/group/port is polled for information.
Statistics	Read-only fields; specifies the object for which statistics are to be gathered. ❑ **Good Frames** — the total number of good or readable frames (frames without error). ❑ **Multicast Frames** — the total number of frames that are simultaneously received and are directed to an active non-broadcast group address. This does not include frames received with a frame-too-long, runt, FCS, or alignment error. ❑ **Broadcast Frames** — the total number of frames that are successfully received and are directed to the broadcast group address. ❑ **Collisions** — the total number of collisions. ❑ **Frames TooLong Errors** — the number of frames that were longer than 1,518 bytes. ❑ **Runts** — the number of frames that were shorter than 64 bytes. ❑ **Alignment Errors** —the number of frames that were an integral number of octets in length and did not pass the FCS check. ❑ **Fragments** — the number of frames received that are less than the minimum permitted frame size and have a bad FCS or alignment error. ❑ **FCS Errors** — the number of frames that failed Cyclic Redundancy Check (CRC). ❑ **Late Collisions** — the number of collisions that occurred after the 64-byte collision window.
Average per second	Displays the average number of occurrences since opening or resetting the screen.
Reset Statistics	Button; resets the counters to zero in the statistics graph.
Peak per second	Displays the largest number of occurrences since opening or resetting the screen.

Field	Description
Count-per-second display	Displays the amount of counts per second displayed on the graph. ***Note:*** To control the count-per-second display, use the scroll bar on the right side of the graph (scroll up to increase the count-per-second; scroll down to decrease it).

A

Technical Support

Contacting Asanté Technical Support

To contact Asanté Technical Support:

Telephone	(800) 622-7464
Fax	(408) 432-6018
Fax-Back	(800) 741-8607 (408) 954-8607
Internet Mail	support@asante.com
World Wide Web	http://www.asante.com
Bulletin Board Service (BBS)	(408) 432-1416
ARA BBS (guest log in)	(408) 894-0765
AppleLink mail/BBS	ASANTE
FTP Archive	ftp.asante.com

Technical Support Hours

6:00 a.m. to 5:00 p.m. Pacific Standard Time USA, Monday - Friday.

.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R