IntraSpection™ Personality Modules

AsantéFAST™ 100 Hub
AsantéFAST 100 TX Managed Hub

User's Manual

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

August 1997

Part Number 06-00341-00 Rev. A

Copyright Notice

TRADEMARKS Asanté Technologies, IntraSpection, and AsantéFAST are trademarks of Asanté Technologies, Inc. Oracle is a registered trademark of Oracle Corporation. Java is a trademark of Sun Microsystems, Inc. in the United States and other countries. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries. Netscape FastTrack Server is also a trademark of Netscape Communications Corporation, which may be registered in other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.All brand names and products are trademarks or registered trademarks of their respective holders.

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. Should you have any questions concerning this Agreement, or if you desire to contact Asanté Technologies for any reason, please contact your local Asanté Technologies subsidiary or sales office, or write:Asanté Technologies, In., 821 Fox Lane, San Jose, California 95131.

WARRANTY DISCLAIMERS Asanté Technologies, Inc. makes no other warranties, express, implied, or otherwise, regarding the AsantéFAST 100 Hub Personality Module or the AsantéFAST 100 TX Managed Hub 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

1

Introduction

IntraSpection Personality Modules

A Personality Module is a "plug-in" to the IntraSpection system that allows for expanded management of an SNMP 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 or Figure 1-2.

This manual provides information for two Personality Modules:

- ❑ The AsantéFAST 100 Hub Personality Module
- ❑ The AsantéFAST 100 TX Managed Hub Personality Module

AsantéFAST 100 Hub Personality Module

The AsantéFAST 100 Hub Personality Module allows for expanded management of an AsantéFAST 100 Hub — or stack of 100 Hubs — with an attached AsantéFAST 100 Management Module. See Figure 1-1.

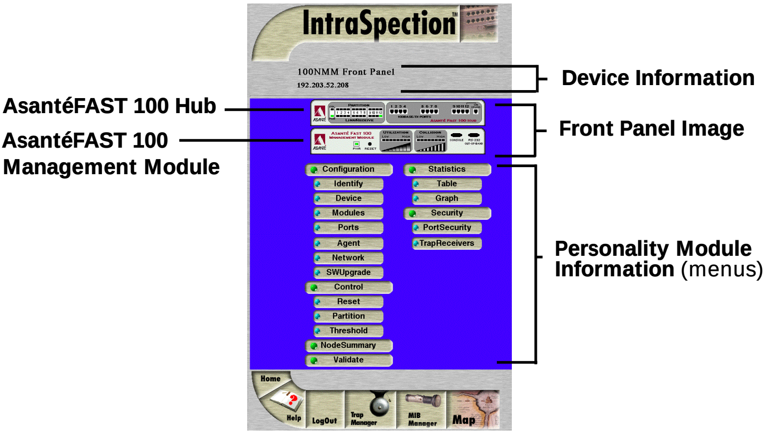


Figure 1-1 AsantéFAST 100 Hub Device Page

AsantéFAST 100 TX Managed Hub Personality Module

The AsantéFAST 100 TX Managed Hub Personality Module allows for expanded management of an AsantéFAST 100TX Managed Hub or a stack of 100 Hubs with an attached Managed Hub. See Figure 1-2.

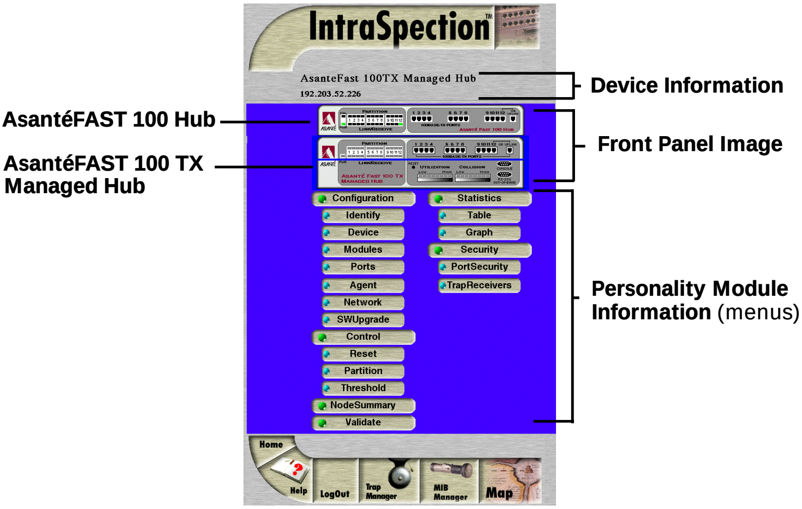


Figure 1-2 AsantéFAST 100 TX Managed Hub Device Page

Management Options

Both the AsantéFAST 100 Hub and the AsantéFAST 100 TX Managed Hub Personality Modules support the following management options:

- ❑ Device identification
- ❑ General device information
- ❑ Module information
- ❑ Port information
- ❑ SNMP agent information
- ❑ Network access configuration
- ❑ Software upgrades
- ❑ Device and group resets
- ❑ Group and port partitioning
- ❑ Alarm thresholds
- ❑ Node summary information
- ❑ Table statistics at the device/group/port levels
- ❑ Graph statistics at the device/group/port levels
- ❑ Port security
- ❑ Trap receiver management

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, 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 Java Script support such as Netscape Navigator® (version 3.0 required, 3.01 recommended) or Microsoft Internet Explorer™

Installation

The AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub are two separate Personality Modules; however, both are installed simultaneously from the same file.

See Chapter 2, “Installation” for instructions on installing the Personality Modules.

About This Manual

This manual is divided into the following chapters:

- ❑ Chapter 1,“Introduction,” describes IntraSpection Personality Modules.
- ❑ Chapter 2,“Installation” explains how to install the AsantéFAST 100 and AsantéFAST 100 TX Managed Hub Personality Modules.
- ❑ Chapter 3,“Management,” explains how to access and use a Personality Module’s Device Page and how to perform some basic management functions.
- ❑ Chapter 4,“Menus,” describes each management menu and its contents.

2

Installation

Installing a Personality Module

This chapter explains how to install the AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub Personality Modules.

Both Personality Modules are contained within the same installation file. When you install the file, you install both Personality Modules.

▲ **Important:** Before installing the Personality Modules, 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 **100NMM.exe** file.

4 Click **Yes** at the IntraSpection Personality Module Installation Confirmation dialog box.

The IntraSpection Personality Module information window appears.

5 Click **Finish** to continue.

The Personality Module files are decompressed.

The IntraSpection Personality Module Welcome dialog box appears.

6 Click **Next**.

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 100NMM.ipm file. See Figure 2-1.

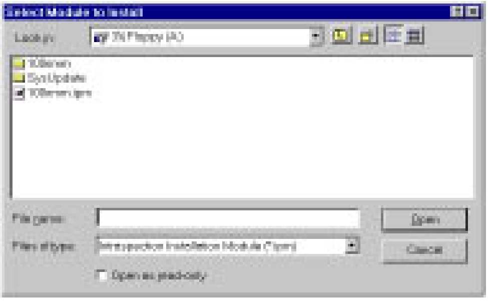


Figure 2-1 Select Module to Install window

10 Click once on the **100NMM.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**.

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

∆ ***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 a 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 an AsantéFAST 100 Hub stack, 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 AsantéFAST 100 Hub stack 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.

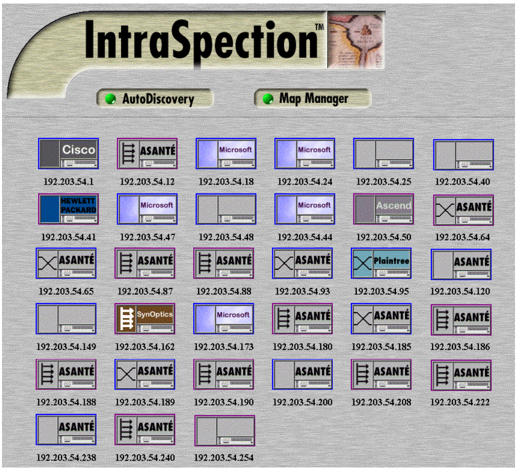


Figure 3-1 Discovered network map

6 Click once on the AsantéFAST 100 Hub or AsantéFAST 100 TX Managed Hub's icon**.**

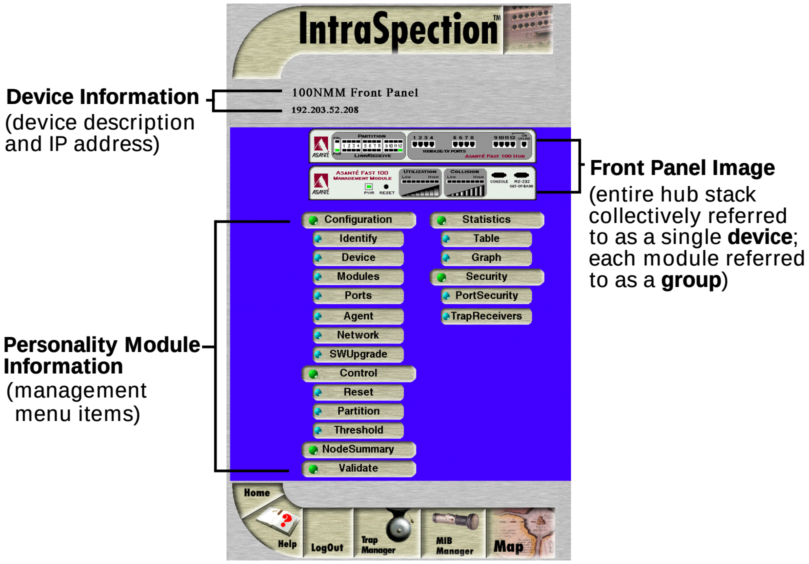
The Device Page for the selected hub appears (see Figure Figure 3-2 on page 3-3).

For information on the Device Page's components, see "Device Page Components" on page 3-2.

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

Device Page Components

A Personality Module's Device Page consists of several components, including device information, a front panel image, and management menu items. See Figure 3-2.



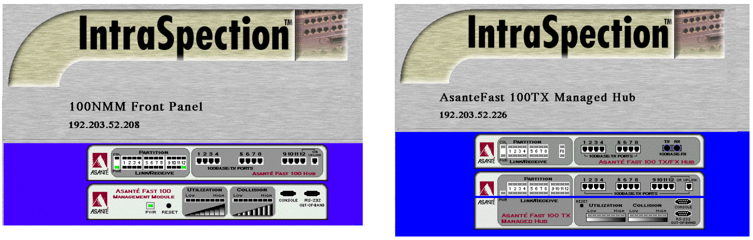
Device Information (device description and IP address)

Front Panel Image (entire hub stack collectively referred to as a single **device**; each module referred to as a **group**)

Personality Module Information (management menu items)

Figure 3-2 Device Page components

The Device Pages for the AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub Personality Modules are the same except for the device information and the front panel image. See Figure 3-3.



AsantéFAST 100 Hub Front Panel Image

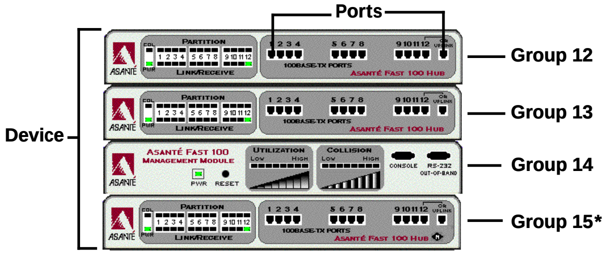
AsantéFAST 100 TX Managed Hub Front Panel Image

Figure 3-3 AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub Device Pages

Front Panel Image Components

The front panel image contains the following components (as illustrated in Figure 3-4):

- **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 modules; they display port activity.



*The bottom module is assigned Group 15, the next module up is assigned Group 14, etc.

Figure 3-4 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.

Group Numbering

For management purposes, each group within a device is assigned a number. The bottom module is always group 15, the next module up is group 14, etc.

▲ **Important:** The AsantéFAST 100 TX Managed Hub module contains two groups (the management module and the hub); therefore, it uses two group numbers (group 15 and group 14). See Figure 3-5.

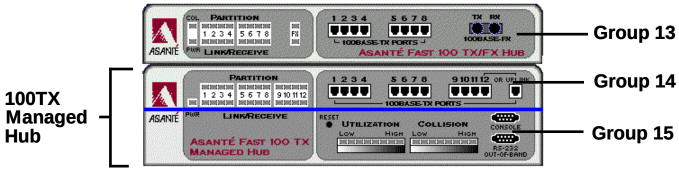


Figure 3-5 AsantéFAST 100 TX Managed Hub group numbering

Selecting the Device for Management

The AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub can be managed at different levels; that is, at the device, group, or port level.

For example, if a group is selected and you select the **Reset** menu, that group (module) will be reset. If the device is selected and you select **Reset**, the device (entire hub stack) will be reset.

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 AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub Device Pages provide access to the different management options supported by each 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; field cannot be edited.

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.

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 both Personality Modules. This section covers the following tasks:

Configuration Tasks

Management Task	Page
Setting community strings	page 3-8
Configuring network access parameters	page 3-10
Configuring device identification information	page 3-11

Management Tasks

Management Task	Page
Updating the Device Page	page 3-13
Viewing general device information	page 3-14
Viewing module information	page 3-15
Viewing SNMP agent Information	page 3-16
Enabling/disabling ports	page 3-17
Disabling a group	page 3-18
Partitioning a port	page 3-19
Resetting a group or device	page 3-20
Enabling traps	page 3-21
Managing trap receivers	page 3-22
Setting alarms	page 3-24
Viewing node summary information	page 3-27
Setting port security	page 3-28
Viewing statistics	page 3-30

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 an AsantéFAST 100 Hub stack's management module are manually set in the management module via the module's console port. In order to access the management module with IntraSpection, the community strings must be set in IntraSpection to match those set in the management module.

▲ **Important:** It is recommended that you set the community strings for an AsantéFAST 100 Hub stack in IntraSpection **before** you attempt to perform any network management functions.

This section describes how to set the community strings in IntraSpection to match those set in the management module.

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

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 3-6.

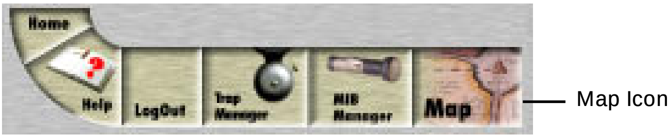


Figure 3-6 IntraSpection navigation bar

The most recently discovered map appears.

2 Click the **Map Manager** button.

The Map Manager Page appears, similar to Figure 3-7.

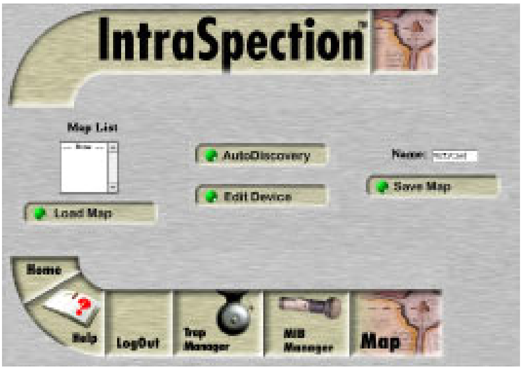


Figure 3-7 IntraSpection Map Manager Page

3 Click the **Edit Device** button.

The Map Configuration Table appears, similar to Figure 3-8.

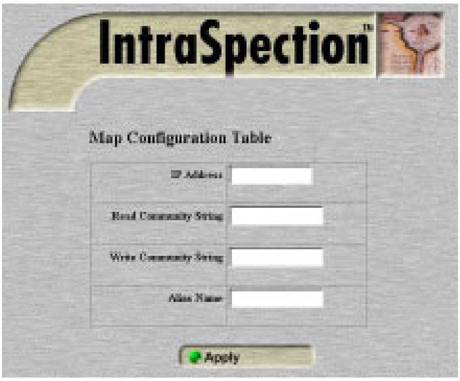


Figure 3-8 Map Configuration Table

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

5 Enter the management module's read community string in the **Read** field.

6 Enter the management module 's write community string in the **Write** field.

7 Click **Apply**.

The read and write community strings for the management module are configured.

Configuring Network Access Parameters

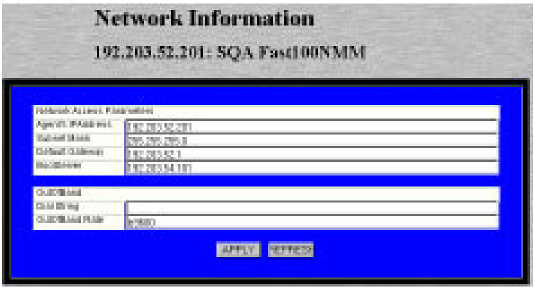
To configure and/or manage an AsantéFAST 100 Hub stack over the network or via out-of-band access, the hub stack's management module needs to be properly configured with network access parameters. These parameters are initially set-up in the management module via the module's console port; however, some can be modified using IntraSpection.

To configure network access parameters:

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

2 Click **Network**.

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



Network Information

192.203.52.201: SQA Fast100NMM

Network Access Parameters	
Agent IP Address	192.203.52.201
Subnet Mask	255.255.255.0
Default Gateway	192.203.52.1
[illegible]	192.203.54.181

OutOfBand	
Dial String	
OutOfBand Rate	9600

Figure 3-9 Network Information table

3 Click once in the field to be edited.

For a description of each field, see "Network" on page 4-9.

▲ **Important:** If you change the **IP address**, **subnet mask**, and/or **default gateway**, you must reset the stack's management module. See "Resetting a Group or Device" on page 3-20.

4 Type the new information.

5 Click **Apply.**

The network information is edited. Click **Refresh** to view updated information.

▲ **Important:** If you changed the IP address, you must rediscover the device on your network map using the AutoDiscovery feature. See "Accessing the Device Page" on page 3-1 for instructions.

Configuring Device Identification Information

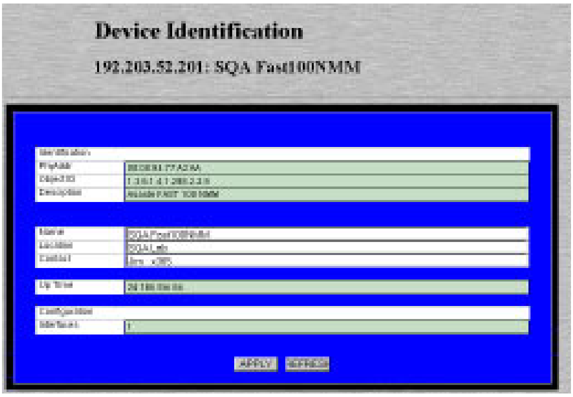
To help with hub identification, you can add certain hub details; such as, the hub stack's physical address, name, location, and contact information.

To configure device 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 3-10.



Device Identification

192.203.52.201: SQA Fast100NMM

Identification	
PhysAddr	[illegible]
ObjectID	[illegible]
Description	[illegible]
Name	SQA Fast100NMM
Location	SQA Lab
Contact	[illegible]
Up Time	[illegible]
Configuration	
Interfaces	1

Figure 3-10 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 or that contain drop-down menus 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 edited. Click **Refresh** to view updated information.

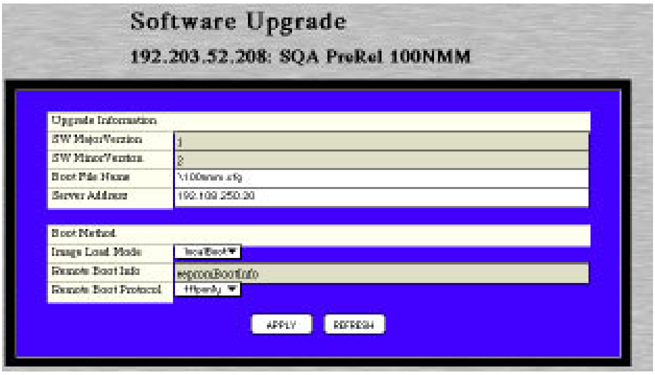
Performing a Software Upgrade

An AsantéFAST 100 Hub stack's software can be upgraded via IntraSpection.

To upgrade an AsantéFAST 100 Hub stack's software:

1 Click **Software**.

The Software Upgrade table appears, similar to Figure 3-11.



Software Upgrade

192.203.52.208: SQA PreRel 100NMM

Upgrade Information	
SW MajorVersion	1
SW MinorVersion	2
Boot File Name	\100nmm.cfg
Server Address	192.109.250.30

Boot Method	
Image Load Mode	localBoot
Remote Boot Info	eepromBootInfo
Remote Boot Protocol	tftpOnly

Figure 3-11 Software Upgrade table

2 Type the software's file name and network path in the **Boot File Name** field.

3 Type the server's IP address where the software file resides in the **Server Address** field.

4 Click **Apply**.

5 Reset the hub stack to initiate the downloading of the software. See "Resetting a Group or Device" on page 3-20.

Click **Refresh** to view updated information.

Updating the Device Page

The files for both Personality Modules 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's latest information.

To update the Personalty Module's Device Page:

1 Click **Validate**.

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

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

2 Click **AutoDiscovery** to rediscover the network map containing the devices.

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

Viewing General Device Information

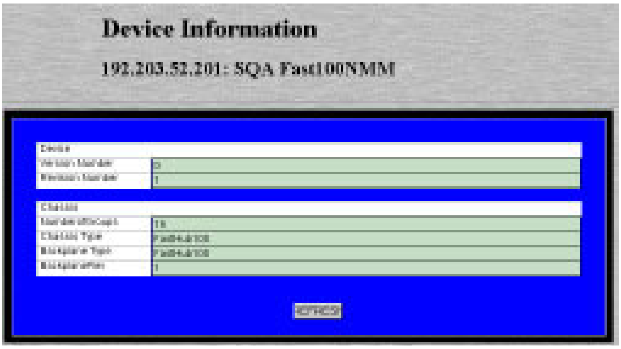
General device information includes items such as the management module's version and revision numbers, chassis type, backplane type, and backplane revision number.

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 3-12.



Device Information

192.203.52.201: SQA Fast100NMM

Device	
Version Number	0
Revision Number	1

Chassis	
Number ofGroups	16
Chassis Type	FastHub100
Backplane Type	FastHub100
BackplaneRev	1

Figure 3-12 Device Information table

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

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

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

Viewing Module Information

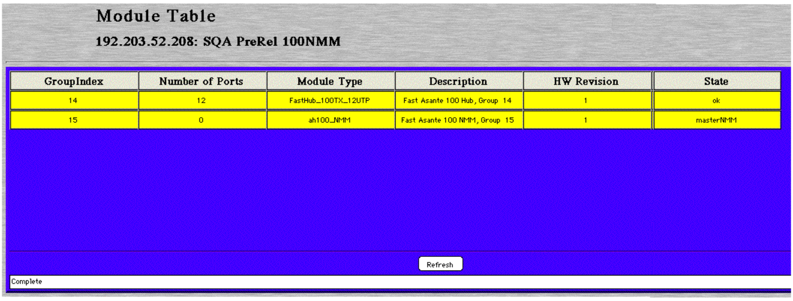
Module information includes information on each group within the device.

To view module information:

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

2 Click **Modules**.

The Module Table appears, similar to Figure 3-13.



Module Table

192.203.52.208: SQA PreRel 100NMM

GroupIndex	Number of Ports	Module Type	Description	HW Revision	State
14	12	FastHub_100TX_12UTP	Fast Asante 100 Hub, Group 14	1	ok
15	0	ah100_NMM	Fast Asante 100 NMM, Group 15	1	masterNMM

Figure 3-13 Modules Table

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

For a description of each field, see “Modules” on page 4-5.

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

Viewing SNMP Agent Information

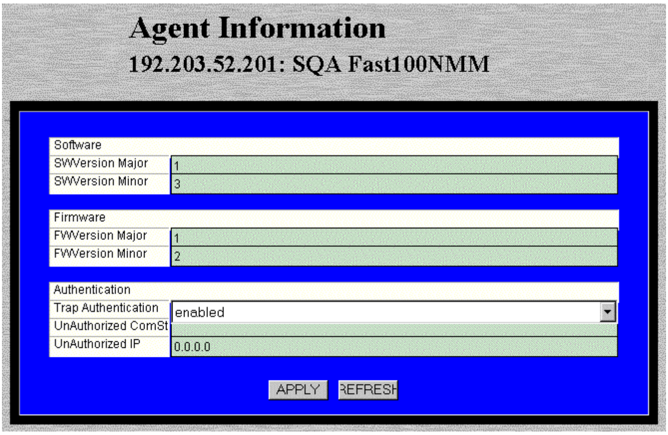
This menu allows you to view information on the management module's software agent. This information includes the module's agent type and mode, software and firmware version numbers, and trap authentication status.

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 3-14.



Agent Information

192.203.52.201: SQA Fast100NMM

Software	
SWVersion Major	1
SWVersion Minor	3
Firmware	
FWVersion Major	1
FWVersion Minor	2
Authentication	
Trap Authentication	enabled
UnAuthorized ComSt	
UnAuthorized IP	0.0.0.0

Figure 3-14 Agent Information table

For a description of each field, see "Agent" on page 4-8.

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

∆ ***Note:*** For information on using the Trap Authentication feature, see "Enabling Traps" on page 3-21.

Enabling/Disabling Ports

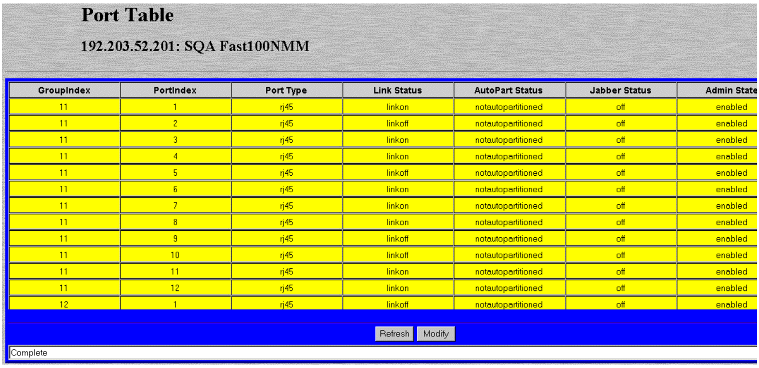
The enabling or disabling of a port is a manual operation that can be used to isolate network devices possibly causing problems on the network or to prevent unauthorized use of a port or station.

To enable or disable a port:

1 Click **Ports**.

You do not need to select any particular item on the front panel image.

The Port Table appears, similar to Figure 3-15.



Port Table

192.203.52.201: SQA Fast100NMM

GroupIndex	PortIndex	Port Type	Link Status	AutoPart Status	Jabber Status	Admin State
11	1	rj45	linkon	notautopartitioned	off	enabled
11	2	rj45	linkoff	notautopartitioned	off	enabled
11	3	rj45	linkon	notautopartitioned	off	enabled
11	4	rj45	linkon	notautopartitioned	off	enabled
11	5	rj45	linkoff	notautopartitioned	off	enabled
11	6	rj45	linkon	notautopartitioned	off	enabled
11	7	rj45	linkon	notautopartitioned	off	enabled
11	8	rj45	linkon	notautopartitioned	off	enabled
11	9	rj45	linkoff	notautopartitioned	off	enabled
11	10	rj45	linkoff	notautopartitioned	off	enabled
11	11	rj45	linkon	notautopartitioned	off	enabled
11	12	rj45	linkon	notautopartitioned	off	enabled
12	1	rj45	linkoff	notautopartitioned	off	enabled

Complete

Figure 3-15 Port Table

The Port Table displays the current status of each port on each group within the device. The table contains a scroll bar that is independent of the browser, which allows you to view information on all ports in the device.

2 Select the port to be enabled or disabled by clicking once on the port's row.

3 Click **Modify**.

The Modify Dialog box appears.

4 Open the **Admin State** drop-down menu and select **enable** (to enable the port) or **disable** (to disable the port).

5 Click **Apply**.

The port's state is modified.

Click **Refresh** to view updated information.

Disabling a Group

To disable a group:

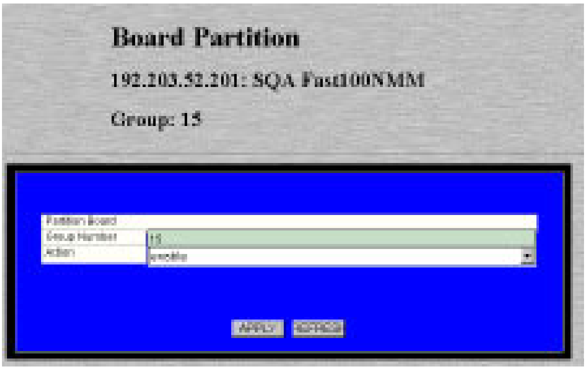
▲ **Important:** Group 15 (the bottom module within a stack) and the stack's management module CANNOT be disabled.

For more information on groups and group numbering, see "Group Numbering" on page 3-4.

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

2 Click **Partition**.

The Board Partition table appears for the selected group, similar to Figure 3-16.



Board Partition

192.203.52.201: SQA Fast100NMM

Group: 15

Partition Board	
Group Number	15
Action	enable

Figure 3-16 Board Partition table

3 Open the **Action** drop-down menu and select **disable**.

4 Click **Apply**.

The group is disabled.

Click **Refresh** to view updated information.

Partitioning a Port

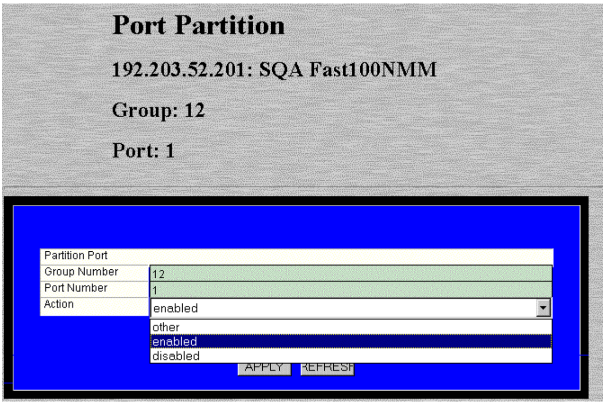
Port partitioning is an operation that is done **automatically** by the hub in certain circumstances to stop transmission on a port, if the port is enabled for automatic partitioning.

To enable or disable automatic partitioning:

1 Select the port to be partitioned (or group containing the port) by clicking on it once.

2 Click **Partition**.

The Port Partition table appears, similar to Figure 3-17.



Port Partition

192.203.52.201: SQA Fast100NMM

Group: 12

Port: 1

Partition Port	
Group Number	12
Port Number	1
Action	enabled

Figure 3-17 Port Partition table

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

4 Click **Apply**.

The port’s partitioning state is modified.

Click **Refresh** to view updated information.

Resetting a Group or Device

If you changed the IP address, subnet mask, and/or default gateway for a management module within a device, that management module needs to be reset.

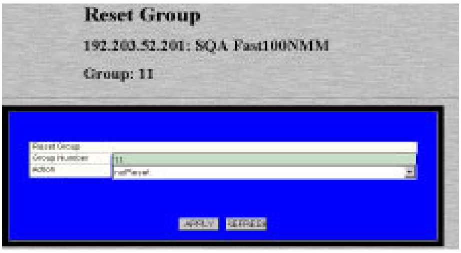
Resets can be performed at the device level (resets the entire stack) or at the group level (resets an individual hub or a management module).

To perform a reset:

1 To reset a group, click once on that group. To reset the device, do NOT select anything.

2 Click **Reset**.

Depending on what was selected (either a group or the device), the Reset Group or Reset Agent table appears, similar to Figure 3-18 and Figure 3-19.



Reset Group

192.203.52.201: SQA Fast100NMM

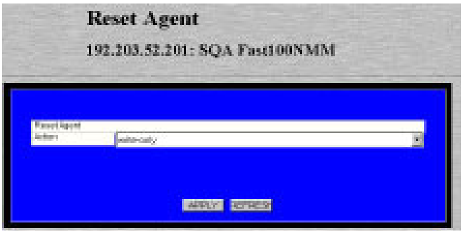
Group: 11

Reset Group

Group Number 11

Action noReset

Figure 3-18 Group Reset table



Reset Agent

192.203.52.201: SQA Fast100NMM

Reset Agent

Action write-only

Figure 3-19 Device Reset table

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

4 Click **Apply**.

The group or device is reset.

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

Enabling Traps

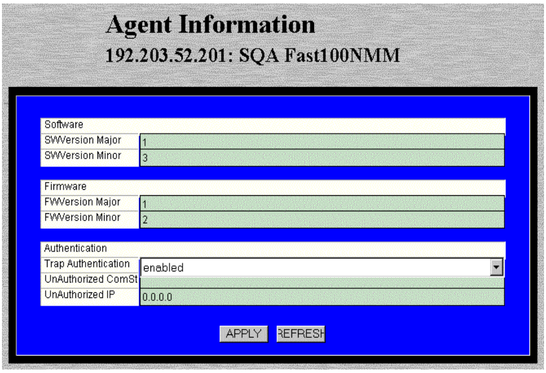
The Trap Authentication feature enables an AsantéFAST 100 Hub stack's management module to generate traps. Traps are generated when certain actions — such as an unauthorized IP address attempts to access a certain port — are violated.

To enable Trap Authentication:

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 3-20.



Agent Information

192.203.52.201: SQA Fast100NMM

Software	
SWVersion Major	1
SWVersion Minor	3
Firmware	
FWVersion Major	1
FWVersion Minor	2
Authentication	
Trap Authentication	enabled
UnAuthorized ComSt	
UnAuthorized IP	0.0.0.0

Figure 3-20 Agent Information table

3 Open the **Trap Authentication** drop-down menu and select **enabled**.

4 Click **Apply**.

The management module is configured to generate traps.

∆ ***Note:*** For information on determining when a trap occurs, see "Setting Alarms" on page 3-24 and "Setting Port Security" on page 3-28.

For information on determining which management stations can receive traps, see "Managing Trap Receivers" on page 3-22.

Click **Refresh** to view updated information.

Managing Trap Receivers

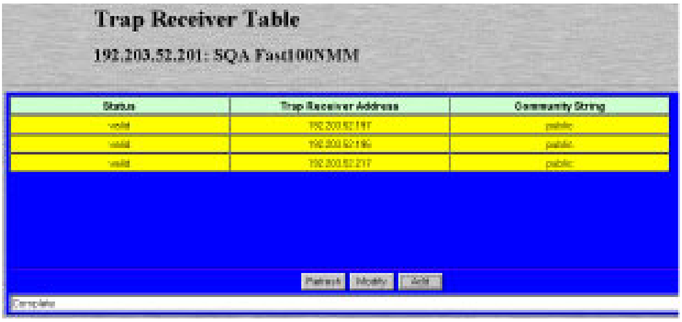
The Trap Receivers menu allows you to set which management stations on your network can receive traps. This section describes how to add and delete a trap receiver.

To add a trap receiver entry:

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

2 Click **Trap Receiver**.

The Trap Receiver Table appears, similar to Figure 3-21.



Trap Receiver Table

192.203.52.201: SQA Fast100NMM

Status	Trap Receiver Address	Community String
valid	192.203.52.197	public
valid	192.203.52.180	public
valid	192.203.52.217	public

Figure 3-21 Trap Receiver Table

3 Click **Add**.

The Add Dialog box appears.

4 Open the **Status** drop-down 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 for the management station in the **Community String** field.

7 Click **Apply**.

The entry for the management station is added and appears in the table. If it does not appear, click **Refresh**.

Deleting a Trap Receiver Entry

To delete a trap receiver entry:

1. Click once on the row containing the entry to be deleted.
2. Click **Modify**.

   The Modify Dialog box appears.
3. Open the **Status** drop-down menu and select **invalid**.
4. Click **Apply.**
5. Click **Refresh** in the Trap Receiver Table.

   The trap receiver is deleted.

Modifying a Trap Receiver Entry

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 3-22.

   The trap receiver entry's IP address is changed.

   Click **Refresh** to view updated information.

Setting Alarms

Alarm thresholds can help you locate problems or faults on the network. When you set a threshold for an activity on a hub, you instruct the hub to take a specific action when a value falls above or below the set threshold.

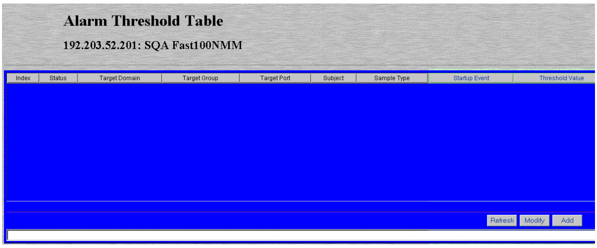
This section explains how to set, delete, and modify alarm thresholds.

To add an alarm:

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

2. Click **Threshold**.

   The Alarm Threshold Table appears, similar to Figure 3-22.



Alarm Threshold Table

192.203.52.201: SQA Fast100NMM

Index	Status	Target Domain	Target Group	Target Port	Subject	Sample Type	Startup Event	Threshold Value

Figure 3-22 Alarm Threshold Table

∆ ***Note:*** If there are no alarm thresholds set, the table is empty.

3. Click **Add** to add an entry.

   The Add Dialog box appears, similar to Figure 3-23.

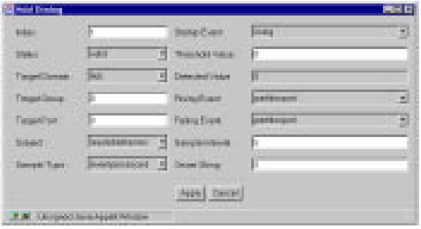


Figure 3-23 Add Alarm Threshold Dialog box

4. Complete each entry as outlined on page 3-25.

5. Click **Apply**.

   The alarm threshold is added. If it does not appear in the Alarm Threshold Table, click **Refresh**.

Field	Description	Action
Index	Displays the number of the alarm entry.	This field is read-only; it cannot be edited.
Status	The status of the alarm entry.	Select **valid** to add an alarm or **invalid** to delete the alarm.
Target Domain	The portion of the device for which the alarm is to be set.	Select **port**, **group**, or **segment0** (device) from the drop-down menu.
Target Group	The number of the group for which the alarm is to be set.	Only enter a group number if **group** was selected as the **Target Domain**.
Target Port	The number of the port for which the alarm is to be set.	Only enter a port number if **port** was selected as the **Target Domain**.
Subject	The counter to be polled for the alarm.	Select a counter from the drop-down menu. See “Subject” on page 4-14 for a description of each counter.
Sample Type	The unit of measure for the alarm.	This field cannot be edited; it is always set to **event-persecond**.
Startup Event	Determines when the alarm is to be triggered.	Select **rising**, **falling**, or **risingANDfalling** from the drop-down menu. See “Startup Event” on page 4-15 for a description of each event.
Threshold Value	The value that triggers the alarm.	Enter an integer.
Detected Value	Displays the last measurement made.	This field is read-only; it cannot be edited.
Rising Event	The response to occur for a triggered rising event.	Select a response from the drop-down menu. See “Rising Event” on page 4-15 for a description of each response.
Falling Event	The response to occur for a triggered falling event.	Select a response from the drop-down menu. See “Falling Event” on page 4-15 for a description of each response.

Field	Description	Action
Sampling Interval	The polling interval that determines how often to make the measurement.	Enter a number (in seconds). ***Note:*** The shorter the sampling interval, the more traffic on the network.
Owner String	The name of the person who defined the alarm entry.	Enter an eight-byte octet.

Deleting an Alarm

To delete an alarm:

1. Select the alarm entry to be deleted by clicking once on its row in the Alarm Threshold Table.
2. Click **Modify**.

   The Modify Dialog box appears.
3. Open the **Status** drop-down menu and select **invalid**.
4. Click **Apply**.

   The alarm is deleted. Click **Refresh** to view updated information.

Modifying an Alarm

To modify an alarm:

1. Select the alarm entry to be modified by clicking once on its row in the Alarm Threshold Table.
2. Click **Modify**.

   The Modify Dialog box appears.
3. Modify the parameters, as desired, following the guidelines on page 3-25.
4. Click **Apply**.

   The alarm is modified. Click **Refresh** to view updated information.

Viewing Node Summary Information

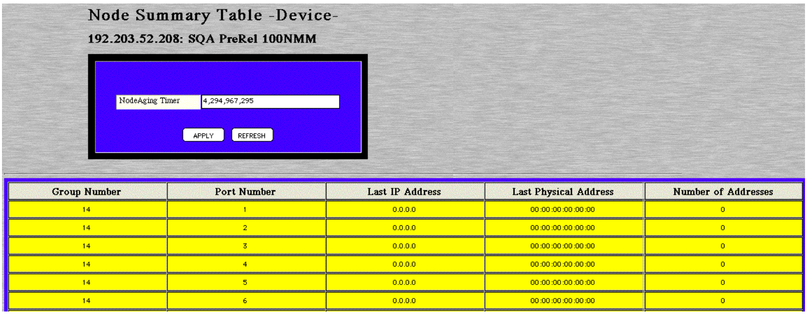
The Node Summary menu provides IP mapping information (a summary of node activity) for the device or a selected group. Each node address remains in the table for the amount of seconds specified in the Node Aging Timer.

To view node summary information:

1. To view node summary information for the device, do not select anything on the front panel image. To view information for a particular group, click once on a group.

2. Click **Node Summary**.

   The Node Summary table appears for the device or selected group, similar to Figure 3-24.



Node Summary Table -Device-

192.203.52.208: SQA PreRel 100NMM

NodeAging Timer: 4,294,967,295

Group Number	Port Number	Last IP Address	Last Physical Address	Number of Addresses
14	1	0.0.0.0	00:00:00:00:00:00	0
14	2	0.0.0.0	00:00:00:00:00:00	0
14	3	0.0.0.0	00:00:00:00:00:00	0
14	4	0.0.0.0	00:00:00:00:00:00	0
14	5	0.0.0.0	00:00:00:00:00:00	0
14	6	0.0.0.0	00:00:00:00:00:00	0

Figure 3-24 Node Summary Table

You can set the amount of time each entry remains in the table by typing the number of seconds in the Node Aging Timer field and clicking **Apply**.

❑ The default setting is **-1** (this value prevents the table from updating; the value "4,294,967,295" appears in the field).

❑ A value of **0** never deletes the entries in the table.

∆ ***Note:*** The information displayed in the Node Summary Table is read-only.

For a description of each field, see "Node Summary" on page 4-16.

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

Setting Port Security

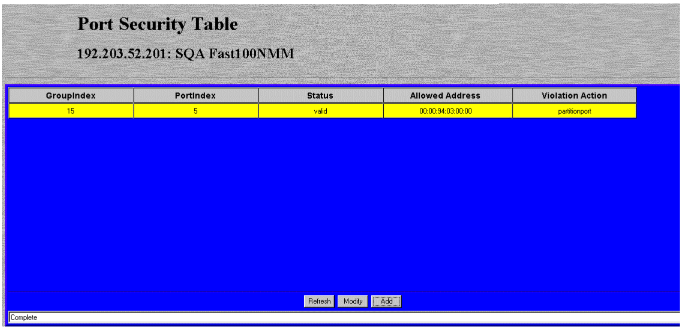
The Port Security menu allows network managers to control access to ports by specifying the physical addresses that are authorized to connect to the ports. If an unspecified physical address attempts to connect to a certain port, an action (such as automatic partitioning of the port, sending of a trap, etc) can be specified to occur.

To set port security:

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

2 Click **Port Security**.

The Port Security Table appears, similar to Figure 3-25.



Port Security Table

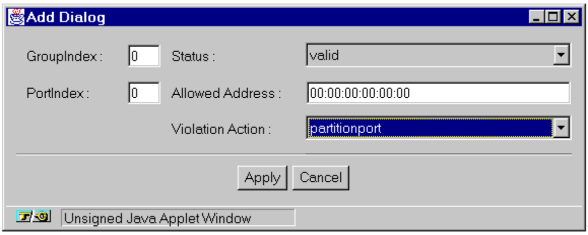
192.203.52.201: SQA Fast100NMM

GroupIndex	PortIndex	Status	Allowed Address	Violation Action
15	5	valid	00:00:94:03:00:00	partitionport

Figure 3-25 Port Security Table

3 Click the **Add** button.

The Add Dialog box appears, similar to Figure 3-26.



Add Dialog

GroupIndex : 0

PortIndex : 0

Status : valid

Allowed Address : 00:00:00:00:00:00

Violation Action : partitionport

Figure 3-26 Add Port Security Dialog box

4 Enter the number of the group for which port security information is to be set in the **GroupIndex** field.

5 Enter the number of the port for which port security information is to be set in the **PortIndex** field.

6 Open the **Status** drop-down menu and select **valid**.

7 Enter the physical (MAC) address that is allowed to use the selected port number in the **Allowed Address** field.

▲ **Important:** Enter the physical address in hexadecimal notation separated by colons. For example, 00:00:94:C5:15:F1.

8 Open the **Violation Action** drop-down menu and select the violation action to occur if an unauthorized MAC address attempts to access the port.

For a description of each violation action, see "Violation Action" on page 4-20.

9 Click **Apply**.

The port security information is configured.

Click **Refresh** to view updated information.

Viewing Statistics

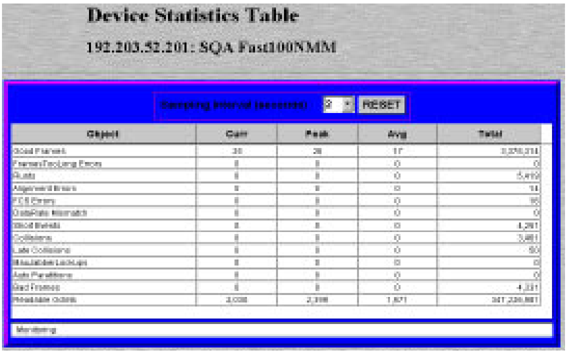
Statistics for an AsantéFAST 100 Hub stack can be viewed in two different formats: table or graph. Statistics collected include runts, alignment errors, late collisions, short events, good frames, and bad frames.

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 (entire hub stack), do NOT select anything.

2 Click **Table**.

Table statistics appear for the group, port, or device selected, similar to Figure 3-27.



Device Statistics Table

192.203.52.201: SQA Fast100NMM

Sampling Interval (seconds) 2 RESET

Object	Curr	Peak	Avg	Total
Good Frames	30	28	17	3,270,214
FramesTooLong Errors	0	0	0	0
Runts	0	0	0	5,412
Alignment Errors	0	0	0	14
FCS Errors	0	0	0	95
DataRate Mismatch	0	0	0	0
Short Events	0	0	0	4,281
Collisions	0	0	0	3,481
Late Collisions	0	0	0	50
[illegible] Lockups	0	0	0	0
Auto Partitions	0	0	0	0
Bad Frames	0	0	0	4,331
Readable Octets	3,008	2,398	1,871	347,226,881

Monitoring

Figure 3-27 Table Statistics

For a description of each object, see "Statistics" on page 4-17.

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

Statistics are automatically gathered 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 counters to zero.

Graph Statistics

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

2 Click **Graph**.

The Graph Statistics page appears for the group, port or device selected, similar to Figure 3-28.

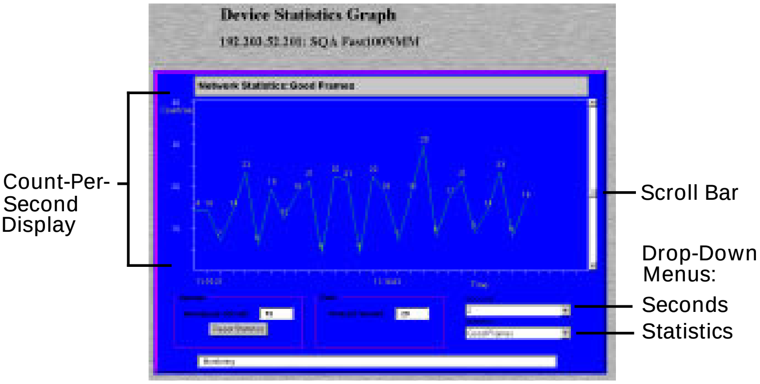


Figure 3-28 Graph Statistics page

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

For a description of each object, see "Statistics" on page 4-17.

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 counters to zero.

4

Menus

This chapter describes each management menu and its contents on the AsantéFAST 100 Hub and AsantéFAST 100 TX Managed Hub Personality Modules' Device Page.

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

Table 4-1 Device Page Menu Descriptions

Menu	Description
Configuration	Title for the submenus listed below it; this menu cannot be selected. See "Configuration" on page 4-3.
Identify	Allows you to view and configure device identification information. See "Identify" on page 4-3.
Device	Allows you to view general device information. See "Device" on page 4-4.
Modules	Allows you to view information on the device's group types. See "Modules" on page 4-5.
Ports	Allows you to view information for each port and enable and disable ports. See "Ports" on page 4-6.
Agent	Allows you to view information on the device's SNMP agent, such as software and firmware information, and allows you to enable and disable trap authentication. See "Agent" on page 4-8.
Network	Allows you to view and configure network access information for the device. See "Network" on page 4-9.
SWUpgrade	Allows you to determine the file name and server address for upgrading the switch's software. See "SWUpgrade" on page 4-10.

Menu	Description
Control	Title for the submenus listed below it; this menu cannot be selected. See "Control" on page 4-11.
Reset	Allows you to reset a group or device. See "Reset" on page 4-11.
Partition	Allows you to enable or disable a group and partition a port. See "Partition" on page 4-12.
Threshold	Allows you to set alarm thresholds for the device. See "Threshold" on page 4-13.
Node Summary	Allows you to view IP mapping information for the device or a group. See "Node Summary" on page 4-16.
Validate	Updates the Device Page with the latest information from the IntraSpection Application Server database. See "Validate" on page 4-17.
Statistics	Title for the submenus listed below it; this menu cannot be selected. See "Statistics" on page 4-17.
Table	Allows you to view real-time statistical data, in table format, on the device. See "Table" on page 4-17.
Graph	Allows you to view real-time statistical data, in graph format, on the device. See "Graph" on page 4-19.
Security	Title for the submenus listed below it; this menu cannot be selected. See "Security" on page 4-20.
Port Security	Allows you to control access to ports by determining which IP addresses are allowed to connect to certain ports. See "Port Security" on page 4-20.
Trap Receivers	Allows you to determine which management stations can receive traps from the device. See "Trap Receivers" on page 4-21.

Configuration

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

Identify

This menu provides read-only and configurable identification information for the device.

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

> ∆ ***Note:*** For instructions on using this menu, see "Configuring Device 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 to the device (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 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 this device.

Device

This menu provides read-only, general information on the device.

Table 4-3 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 4-3 Device Menu

Field	Description
Version Number	Read-only field; displays the current version number of the device.
Revision Number	Read-only field; displays the current revision number of the device.
Number of Groups	Read-only field; displays the number of groups the device contains.
Chassis Type	Read-only field; displays the device's chassis type. ***Note:*** This field always displays **FastHub100**.
Backplane Type	Read-only field; displays the device's backplane type. ***Note:*** This field always displays **FastHub100**.
Backplane Rev	Read-only field; displays the device's backplane revision number.

Modules

This menu provides read-only information on each group within the device.

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

∆ ***Note:*** For instructions on using this menu, see "Viewing Module Information" on page 3-15.

Table 4-4 Modules Menu

Field	Description
Group Index	Read-only field; displays the number of the selected group.
Number of Ports	Read-only field; displays the total number of ports in the group.
Module Type	Read-only field; displays the type of module of the selected group. For example, **FastHub100** or **Management Module**. ***Note:*** The table displays entries for groups 1 through 15; a module type of **empty** means that there is physically no group in that position in the device. See "Group Numbering" on page 3-3 for more information on groups and group numbering.
Description	Read-only field; displays a description of the group.
HW Revision Number	Read-only field; displays the hardware revision number of the device.
State	Read-only field; displays the state of the module. ❑ **OK** — the module is not a "master" module (it does not manage other devices within the stack) and is currently operating. ❑ **Fail** — a problem with the module's board has been detected. ❑ **Master NMM** — the module is a "master" module (it manages other devices in the stack). ❑ **Standby NMM —** the module is capable of being a "master" module.

Ports

This menu provides read-only and configurable information for each port on the device.

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

> Δ ***Note:*** For instructions on using this menu, see "Enabling/ Disabling Ports" on page 3-17 and "Partitioning a Port" on page 3-19.

Table 4-5 Ports Menu

Field	Description
Group Index	Read-only field; displays the number of the group to which the selected port belongs.
Port Index	Read-only field; displays the number of the port for which information is displayed.
Port Type	Read-only field; displays the type of connector on the port (for example, **RJ-45**).
Link Status	Read-only field; displays if a device is connected to the selected port. ❑ **linkon** — a device is properly connected to the selected port and is powered on. ❑ **linkoff** — a device is not connected to the port.
AutoPort Status	Configurable field; displays the automatic partitioning status of the selected port. ❑ **autopartitioned** — the port is configured for automatic partitioning. ❑ **noautopartitioned** — the port is not configured for automatic partitioning. See "Partitioning a Port" on page 3-19 for instructions.
Jabber Status	Read-only field; displays the status of the Jabber Detector (a device that helps prevent a node from transmitting constantly; for example, if the node is malfunctioning). ❑ **on** — jabber detector is on. ❑ **off** — jabber detector is off.

Field	Description
Admin Status	Configurable field; determines the state of the port. ❑ **enabled** — the port is enabled and can receive packets. ❑ **disabled** — the port is disabled and cannot receive packets. See “Enabling/Disabling Ports” on page 3-17 for instructions.

Agent

This menu provides read-only and configurable information for the device's SNMP agent.

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

∆ ***Note:*** For instructions on using this menu, see "Viewing SNMP Agent Information" on page 3-16.

Table 4-6 Agent Menu

Field	Description
SWVersion Major	Read-only field; displays the major software version number of the device's management module. ***Note:*** If the unit is running code version 1.2, the SWVersion Major number is 1.
SWVersion Minor	Read-only field; displays the minor software version number of the device's management module. ***Note:*** If the unit is running code version 1.2, the SWVersion Minor number is 2.
FWVersion Major	Read-only field; displays the major firmware version number of the device's management module. ***Note:*** If the unit is running code version 1.2, the FWVersion Major number is 1.
FWVersion Minor	Read-only field; displays the minor firmware version number of the device's management module. ***Note:*** If the unit is running code version 1.2, the FWVersion Major number is 2.
Trap Authentication	Configurable field; indicates if the device can send traps to the trap receiving stations. ❑ **enable** — the device can send traps. ❑ **diable** — the device cannot send traps. See "Enabling Traps" on page 3-21 for instructions.
Unauthorized Com Strin	Read-only field; displays the community string of the last network station that attempted to access the management module.
Unauthorized IP	Read-only field; 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 **Unauthorized Com Strin** field.)

Network

This menu provides configurable network access information for the device's management module. This information is needed to access the device across the network (in-band management).

Table 4-7 describes each field in the Network menu.

▲ **Important**: If you change the **IP address**, **subnet mask**, or **default gateway**, the management module needs to be reset in order for the changes to take effect. See "Resetting a Group or Device " on page 3-20 for instructions.

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

Table 4-7 Network Menu

Field	Description
Agent's IP Address	Configurable field; displays the IP address of the management module's SNMP agent.
Subnet Mask	Configurable field; displays the subnet address of the device. ***Note:*** A subnet mask, in the IP addressing scheme, is a group of selected bits whose values serve to identify a subnetwork. All members of the subnetwork share the mask value.
Default Gateway	Configurable field; displays the address of the default gateway to which the device belongs.
Boot Server	Configurable field; displays the IP address of the boot server that was used for booting the IP agent.
Dial 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**.

SWUpgrade

This menu provides read-only and configurable software upgrade and boot method information (the parameters used for downloading a new version of software) for the device.

Table 4-8 describes each field in the SWUpgrade menu.

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

Table 4-8 SWUpgrade Menu

Field	Description
SW Major Version	Read-only field; displays the major software version number of the device. ***Note:*** If the unit is running code version 1.2, the SW Major Version number is 1.
SW Minor Version	Read-only field; displays the minor software version number of the device. ***Note:*** If the unit is running code version 1.2, the SW Minor Version number is 2.
Boot File Name	Configurable field; sets the network path and name of the boot file for the device.
Server Address	Configurable field; sets the boot server's IP address.
Image Load Mode	Configurable field; determines the method for loading the software. ❑ **localBoot** — sets the device to boot from code stored in device (default setting). ❑ **netBoot** — sets the device to boot from a TFTP server on the network.
Remote Boot Info	Read-only field; indicates that the boot configuration parameters are originating from EEProm. ***Note:*** This field always displays **eepromBootInfo**
Remote Boot Protocol	Configurable field; determines the remote boot protocol used to load the software. ❑ **bootptftp** — sets the device to request an IP address from a BootP server and to load the software from a TFTP server. ❑ **tftponly** — sets the device to only load the software across the network (the device must already be configured with an IP address).

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 4-9 describes each field in the Reset menu.

> ∆ ***Note:*** For instructions on using this menu, see "Resetting a Group or Device" on page 3-20.

Table 4-9 Reset Menu

Field	Description
Device Level (Reset Agent)	
Reset Agent	Configurable field; resets the device. ❑ **reset** — resets the device . ❑ **not-reset** — does not reset the device.
Group Level (Reset Group)	
Group Number	Read-only field; displays the number of the group to be reset.
Action	Configurable field; resets the group. ❑ **reset** — resets the selected group. ❑ **not-reset** — does not reset the selected group.

Partition

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

Table 4-10 describes each field in the Partition menu.

▲ **Important:** Group 15 (the bottom module in the stack) and the stack's management module CANNOT be disabled.

For more information on groups and group numbering, see "Group Numbering" on page 3-4.

Δ ***Note:*** For instructions on using this menu, see "Disabling a Group" on page 3-18 and "Partitioning a Port" on page 3-19.

Table 4-10 Partition Menu

Field	Description
Group Level (Board Partition)	
Group Number	Read-only field; displays the number of the selected group to be disabled.
Action	Configurable field; disables or enables the group. ❑ **disable** — disables the selected group. ❑ **enable** — enables the selected group.
Port Level	
Group Number	Read-only field; displays the number of the group to which the selected port belongs.
Port Number	Read-only field; displays the number of the selected port.
Action	Configurable field; enables or disables automatic partitioning on the port. ❑ **enabled** — enables automatic partitioning on the selected port. ❑ **disable** — disables automatic partitioning on the selected port.

Threshold

This menu displays the current alarms that are set and allows alarms to be added or modified.

Alarms can help you locate problems or faults on the network. When you set an alarm threshold for an activity on a hub, you instruct the hub to take a specific action when the value falls above or below the set threshold.

Table 4-11 describes each field in the Threshold menu.

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

Table 4-11 Threshold Menu

Field	Description
Index	Read-only field; displays the number of the alarm entry. This field cannot be modified.
Status	Configurable field; displays the status of the entry in the table. ❑ **valid** — active entry. ❑ **invalid** — inactive entry (deletes the entry when selected).
Target Domain	Configurable field; determines the portion of the device for which alarms are being set. ❑ **port** — sets the alarm for a specific port; you must enter the port number in the **Target Port** field. ❑ **group** — sets the alarm for a specific group; you must enter the group number in the **Target Group** field. ❑ **segment0** — sets the alarm for the entire device.
Target Group	Configurable field; determines the group number for which to set the alarm. **Important:** This field only needs to be edited if the Target Domain is set to **group**.
Target Port	Configurable field; determines the port number for which to set the alarm. **Important:** This field only needs to be edited if the Target Domain is set to **port.**

Field	Description
Subject	Configurable field; determines the counter to be polled. ❑ **readableframes** — the total number of good or readable frames (frames without error). ❑ **frametoolong** — the number of frames that were longer than 1,518 bytes. ❑ **runts** — the number of frames that were shorter than 64 bytes. ❑ **alignmenterrors** — the number of frames that were an integral number of octets in length and did not pass the FCS check. ❑ **fcserrors** — the number of frames that failed Cyclic Redundancy Check (CRC). ❑ **dataratemismatch** — the number of errors where the incoming data rate is not within the tolerance level of 10Mhz (+ or - 0.01%). ❑ **shortevents** — the number of data bursts, where data is less than 10 bytes in length. ❑ **collisions** — the total number of collisions. ❑ **latecollisions** — the number of collisions that occurred after the 64-byte collision window. ❑ **autopartitions** — the number of times the port was automatically partitioned in response to 31 or more continuous collisions. ❑ **badframes** — the number of invalid frames (including toolong, runts, misaligned, or bad FCS).
Sample Type	Read-only field; sets a unit of measure for the alarm. ***Note:*** This field is always set to **eventpersecond** and cannot be modified.

Field	Description
Startup Event	Configurable field; determines when the alarm is to be triggered. ❑ **rising** — alarm is triggered when the event rate rises above the threshold. ❑ **falling** — alarm is triggered when the event rate falls below the threshold. ❑ **rising and falling** — alarm is triggered when the event rate rises above or falls below the threshold.
Threshold Value	Configurable field; sets the value that triggers the alarm.
Detected Value	Read-only field; displays the last measurement made.
Rising Event	Configurable field; displays the response to a triggered rising event. ❑ **partitionport** — partitions the target port. ❑ **sendtrap** — sends a trap to the receiving trap station. ❑ **partitionportANDsendtrap** — partitions the target port and sends a trap. ❑ **sendtrapANDrequestpage** — sends a trap and sends a page to the network administrator (if the trap receiving station is an AsantéView Management Station). ❑ **partitionportANDsendtrapANDrequestpage** — partitions the target port, sends a trap, and send a page to the network administrator (if the trap receiving station is an AsantéView Management Station).
Falling Event	Configurable field; displays the response to a triggered falling event. Options are the same as those for a rising event (see "Rising Event" above).
Sample Interval	Configurable field; sets (in seconds) the polling interval. ***Note:*** The shorter this time period, the more traffic on the network.
Owner String	Configurable field; displays the name of the person who defined the entry (eight-byte octect).

Node Summary

This menu provides IP mapping information (a summary of node activity on the device or a selected group).

Table 4-12 describes each field in the Node Summary menu.

> ∆ ***Note:*** For instructions on using this menu, see "Viewing Node Summary Information" on page 3-27.

Table 4-12 Node Summary Menu

Field	Description
NodeAgingTimer	Configurable field; specifies the amount of time (in seconds) to keep the node entry in the table. This value can be any number, including : ❑ **-1** — prevents the table from updating. When this value is entered in the Node Aging Timer field, the value "4,294,967,295" is displayed. ❑ **0** — entries are not deleted from the table The amount of time is rounded to the nearest minute.
Group Number	Read-only field; displays the number of the selected group.
Port Number	Read-only field; displays the number of the port on the group.
Last IP Address	Read-only field; displays the last known IP address that is associated with the port.
Last Physical Address	Read-only field; displays the last MAC address associated with the port.
Number of Addresses	Read-only field; displays the number of addresses received on the port.

Validate

This menu updates the Personality Module's Device Page with the latest information stored in the IntraSpection Application Server database.

For instructions on using this menu, see "Updating the Device Page" on page 3-13.

Statistics

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

Table

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

Table 4-13 describes each field in the Table menu.

> ∆ ***Note:*** For instructions on using this menu, see "Viewing Statistics" on page 3-30.

Table 4-13 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.
Objects	❏ **Good Frames** — the total number of good or readable frames (frames without error). ❏ **FramesTooLongErrors** — the number of frames that were longer than 1518 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. ❏ **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.

Field	Description
	❑ **Datarate Mismatch** — the number of errors where the incoming data rate is not within the tolerance level of 10Mhz (+ or - 0.01%). ❑ **Short Events** — the number of data bursts, where data is less than 10 bytes in length. ❑ **MauJabberLockups** — the number of times the hub repeater chip goes into a lockup state. ❑ **Auto Partitions** — the number of times the port was automatically partitioned in response to 31 or more continuous collisions. ❑ **Bad Frames** — the number of invalid frames (including toolong, runts, misaligned, or bad FCS). ❑ **Readable Octets** — the total number of octets received from valid frames.

Graph

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

Table 4-14 describes each field in the Graph menu.

Δ ***Note:*** For instructions on using this menu, see "Viewing Statistics" on page 3-30.

Table 4-14 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	Drop-down menu; determines the object for which statistics are gathered. ***Note:*** For a description of each object, see "Objects" on page 4-17.
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 graph.
Peak per second	Displays the largest number of occurrences since opening or resetting the screen.
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).
Objects	For a description of each object, see "Objects" on page 4-17.

Security

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

Port Security

This menu allows you to control access to ports by specifying the physical addresses that are allowed to connect to certain ports. If an unauthorized physical address attempts to connect to the restricted port, an action (such as partition the port, send a trap, etc) can occur.

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

> Δ ***Note:*** For instructions on using this menu, see “Setting Port Security” on page 3-28.

Table 4-15 Port Security Menu

Field	Description
Group Index	Read-only field; displays the number of the group selected.
Port Index	Read-only field; displays the number of the port on the group.
Status	Configurable field; determines the status of the entry. ❑ **valid** — entry is active. ❑ **invalid** — entry is inactive (deletes the entry).
Allowed Address	Configurable field; displays the physical address that is allowed to connect to the specified port.
Violation Action	Configurable field; the action to occur if the physical address does not match the Allowed Address. ❑ **partitionport** — partitions the target port. ❑ **sendtrap** — sends a trap to the receiving station. ❑ **partitionportANDsendtrap** — partitions the target port and sends a trap. ❑ **sendtrapANDrequestpage** — sends a trap and sends a page to the network administrator (if the trap receiving station is an AsantéView Management Station). ❑ **partitionportANDsendtrapANDrequestpage** — partitions the target port, sends a trap, and send a page to the network administrator .

Trap Receivers

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

Table 4-16 describes each field in the Trap Receivers menu.

∆ ***Note:*** For instructions on using this menu, see "Managing Trap Receivers" on page 3-22.

Table 4-16 Trap Receivers Menu

Field	Description
Status	Configurable field; displays the status of the trap receiving station's entry. ❑ **valid** — trap receiver entry is active. ❑ **invalid** — trap receiver entry is inactive (deletes the trap receiver's entry in the table when selected).
Trap Receiver Address	Configurable field; displays the IP address of the management station that can receive traps. To change or add an address, see "Managing Trap Receivers" on page 3-22.
Community String	Configurable field; displays the write community string of the receiving management station.

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