



IntraCore™ 3500 Series

Gigabit Ethernet Switches

User's Manual

Quick Start Guide

Follow these steps to install your IntraCore switch:

1. Open the box and check the contents. See *Chapter 1.1 Package Contents* for a complete list of the items included with your IntraCore switch.
2. Install the switch in an equipment or wall rack, or prepare it for desktop placement.
3. Connect the power cord to the unit and to an appropriate power source.
4. Connect network devices to the switch.
5. Refer to Chapters 3-5 to configure the IntraCore for configuration and management capabilities.

For more information on installing the switch, please refer to *Chapter 2 Installation and Setup*.



IC3524, IC3524-2T and IC3524-2G Models



IC3548-2GT

IntraCore 3500 Series
Gigabit Ethernet Switches
User's Manual

Asanté Technologies, Inc.
821 Fox Lane
San Jose, CA 95131
USA

SALES

800-662-9686 Home/Office Solutions
800-303-9121 Enterprise Solutions
408-435-8388

TECHNICAL SUPPORT

801-566-8991: Worldwide
801-303-3787: FAX
www.asante.com
support@asante.com

Copyright © 2002 Asanté Technologies, Inc. All rights reserved. No part of this document, or any associated artwork, product design, or design concept may be copied or reproduced in whole or in part by any means without the express written consent of Asanté Technologies, Inc. Asanté is a registered trademark and the Asanté logo, IntraCore, IntraCare and AsantéCare are trademarks of Asanté Technologies, Inc. All other brand names or product names are trademarks or registered trademarks of their respective holders. All features and specifications are subject to change without prior notice.

Rev. A

Table of Contents

Quick Start Guide	2
Chapter 1. Introduction	6
1.1 Package Contents	6
1.2 LEDs	7
1.3 Front and Back Panel Descriptions	9
1.4 Management and Configuration	10
Chapter 2. Hardware Installation and Setup	12
2.1 Installation Overview	12
2.2 Installation into an Equipment Rack	13
2.3 GBIC Interfaces	14
2.4 Installing Optional Hardware Modules	15
2.5 Connecting Power	15
2.6 Connecting to the Network	16
2.7 Setup	17
2.8 Changing the Password	18
2.9 IP Assignment	19
2.10 SNMP Management	19
2.11 Using the Stacking Feature	20
Chapter 3. Configuration	22
3.1 General Information	23
3.2 Configuration Menu	23
3.3 System Administration Configuration	24
3.4 System IP Configuration	25
3.5 Bootstrap Configuration	25
3.6 SNMP Configuration	26
3.7 Port Configuration	28
3.8 Advanced Port Configuration	31
3.9 Unicast Forwarding Database Configuration	33
3.10 Security Management	35
3.11 VLAN Management	35
3.12 IP Multicast Traffic Management	35
3.13 Port Mirroring Configuration	35
3.14 File Up/Downloading Configuration	36
3.15 System Reset Configuration	38
3.16 System Log	39
3.17 User Interface Configuration	40
3.18 System Utility	42
3.19 Viewing Statistics	43
Chapter 4. Advanced Management	44
4.1 Spanning Tree Protocol	44
4.2 SNMP and RMON Management	46
4.3 Security Management	46
4.4 VLAN Management	50
4.5 IP Multicast Traffic Management	55
Chapter 5. Web-Based Management	58
5.1 Front Panel Button	59
5.2 Genl Info (General Information) Button	59
5.3 Statistics Button	60
5.4 Port Config (Port Configuration) Button	61
5.5 Span Tree (Spanning Tree) Button	62
5.6 SNMP Button	63
5.7 Addr (Address) Table Button	63
5.8 VLAN Button	64
5.9 Security Button	68

5.10 Duplicate IP Button	69
Chapter 6. SNMP Management	70
6.1 SNMP Management Operations	70
6.2 The SNMP Protocol	70
6.3 Community Name and Security	71
6.4 The MIB Tree	71
Chapter 7. Switching Concepts	73
7.1 VLANs	73
7.2 Spanning Tree Protocol	74
7.3 Full Duplex, Flow Control and Auto-negotiation	75
Appendix A. Troubleshooting	77
Appendix B. Features and Specifications	78
B.1 Features	78
B.2 Specifications	78
Appendix C. FCC Compliance and Warranty Statements	80
Appendix D. Console Port Pin Outs	82
Appendix E. Online Warranty Registration	83
Appendix F. BootP Configuration	84

Chapter 1. Introduction

Thank you for purchasing the Asanté IntraCore 3500 Series Gigabit switch. The IntraCore 3500 series include 24- and 48-port 10/100 managed switches with a variety of hardware and software options.

The IntraCore 3524 is a 24-port 10/100 managed switch with several optional hardware modules. Hardware expansion slots (two Type IC35) can accept a wide range of Gigabit and 10/100 Mbps media modules:

- 10/100/1000BaseT
- 1000BaseX GBIC
- 1000BaseSX
- 100BaseMMFX
- 100BaseSMFX

The IntraCore 3548-2GT is a 48-port 10/100 managed switch with integrated 10/100/1000BaseT Gigabit Ethernet ports and 1000BaseX GBIC expansion ports.

See the table below for a description of the 3500 series models that are available.

Model	10/100 Ports	Optional Media Modules	Description
IC 3524 Base	24	Two IC35 slots available	Managed 24-port 10/100 switch; base
IC 3524-2G	24	Two 1000BaseX GBIC slots	Integrated 1000BaseX GBIC slots
IC 3524-2T	24	Two 10/100/1000 BaseT ports	Integrated copper Gigabit ports
IC 3548-2GT	48		Managed 48-port 10/100 switch with two integrated GBIC slots or two integrated 10/100/1000BaseT Gigabit Ethernet ports

Table 1-1 3500 Models

The system can operate as a stand-alone network or be used in combination with other IntraCore series switches in the backbone.

1.1 Package Contents

The following items are included in your package:

- Switch
- AC power cord
- Rack mount brackets with screws
- Rubber feet
- Reference Guide
- Getting Started Guide
- User's Manual (this document, on CD-ROM)
- IntraCore 3500 CD-ROM

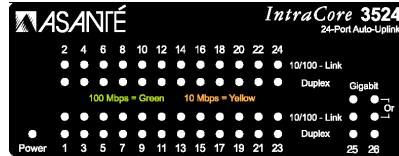
Contact your dealer immediately if any of these items are missing.

1.2 LEDs

The system's LED display allows you to monitor the status of your switch. Refer to the sections below for LED information specific to your switch's model.

1.2.1 IC3524 Models

The IntraCore 3524 model switches have two LED indicators for each of the 24 10/100 ports, and three LED indicators for both of the optional Gigabit ports. See Tables 1-2 and 1-3 below for a complete LED description.



Port #	LED	Color	Description
N/A	Power/System	Green	Power is on
		Off	Power is off
1-24(10/100)	10/100 Link	Solid Green	A valid 100 Mbps link has been established
		Solid Amber	A valid 10Mbps has been established
		Off	No link has been established
1-24(10/100)	Duplex	Solid Green	Full Duplex
		Solid Amber	Half Duplex

Table 1-2 IC3524 Models-- Ports 1-24

Port #	LED	Color	Description
25, 26	Gigabit (speed)	Solid Green	A valid 1000Mbps link has been established
		Off	No link has been established, or link is at 10/100Mbps rate
25, 26	10/100 Link	Solid Green	A valid 100Mbps link has been established
		Solid Amber	A valid 10Mbps link has been established
		Off	No 10/100 link has been established
25, 26	Duplex	Solid Green	Full Duplex
		Solid Amber	Half Duplex

Table 1-3 IC3524 Models--Ports 25 & 26

1.2.2 IC3548-2GT

The IntraCore 3548-2GT switch has two LED status indicators for each of the 48 10/100 ports and the 2 Gigabit ports. Using the Mode button on the lower left of the front panel allows the user to convert between Link/Activity status and Duplex status displays. See the tables below for more information on the LED functions of the 3548.



Port #	LED	Color	Description
N/A	Power/System	Green	Power is on
		Off	Power is off
1-48(10/100)	Link/Activity	Solid Green	A valid 100 Mbps link has been established
		Blinking Green	Data transfer at 100Mbps
		Solid Amber	A valid 10Mbps has been established
		Blinking Amber	Data transfer at 10Mbps
		Off	No link has been established
1-48(10/100)	Duplex	Solid Green	Full Duplex
		Solid Amber	Half-Duplex
		Blinking Amber	The switch is operating in half-duplex
		Off	No full-duplex link has been established, or no collisions are occurring on the port when operating at half-duplex

Table 1-4 IC3548 Model--Ports 1-48

Port #	LED	Color	Description
Gigabit Ports #49, 50	Link/Activity	Solid Green	A valid 1000Mbps link has been established
		Blinking Green	Data transfer at 1000Mbps
		Solid Amber	A 10/100Mbps link has been established
		Blinking Amber	Data transfer at 10/100Mbps
		Off	No Gigabit link has been established
Gigabit Ports #49, 50	Duplex	Solid Green	Full Duplex
		Solid Amber	Half Duplex
		Blinking Amber	The switch is operating in half-duplex
		Off	No full-duplex link has been established, or no collisions are occurring on the port when operating at half-duplex

Table 1-5 IC3548 Model—Ports 49 & 50

1.3 Front and Back Panel Descriptions

Refer to the following sections for detailed descriptions of the front and back panels of the IntraCore 3500 series switches.

1.3.1 IC3524 Models

From left to right, the front panel contains the following: Power and port LEDs; 24 10/100 ports; 2 optional module slots; and a console port.



The switch is field upgradeable for use with 100BaseFX, 1000BaseSX, 1000BaseX GBIC or 10/100/1000BaseT modules.



The back panel (not shown) has only the AC socket.

1.3.2 IC3548-2GT

From the left to the right, the 3548 switch's front panel contains the power LED and 2 exchanging LEDs; a push button *display mode converter*; 48 10/100 ports, each with its own indicator light; and 2 Gigabit ports (capable of using either the GBIC expansion ports [for fiber and copper GBICs] **OR** the 10/100/1000BaseT Gigabit Ethernet ports), each with its own indicator light.



From left to right, the back panel (shown below) contains: a console port; a 12V DC jack for an external power supply (IC35-RPS12, US part number 99-00777-01, sold separately); an AC socket (for primary power) and a power switch.



1.4 Management and Configuration

There are three different methods by which a user can manage the switch: web, console/telnet, or with SNMP software. You may prefer using a web browser to be able to configure the switch from any local or remote computer, via the network, or you may wish to use a console for out-of-band management. SNMP is an advanced management application, and is mostly automatic, giving you the information without having to go through an interface step by step (**Note:** The switch is shipped with BootP support. See Appendix F for more information on setting up BootP).

Method	Type	Description
Console	Out-of-Band Management	Local connection to the switch via the console port
Telnet	In-Band Management	Remote connection over the network to the switch via the telnet session
HTTP Server	In-Band Management	Remote connection over the network to the switch via a Web browser
SNMP-Based Network Management Software	In-Band Management	Remote connection over the network to the switch via any SNMP-based network management application

Table 1-4 Out-of-Band and In-Band Management

1.4.1 Console Interface

Users can access the switch in a more traditional way by connecting a PC or terminal to the console port or by telnet across the network. The menus are organized in a manner similar to the web-based interface. A detailed description can be found in *Chapter 3 Configuration*. Users must use a console connection to form a stack (multiple units sharing one IP address). The stacking feature is available on the IC3524 models, versions 1.1 or higher. See *Chapter 2.11 Using the Stacking Feature* for more details.

1.4.2 Web-Based Interface

With Internet access, users can link directly to the local switch's home page. Users can configure the switch, monitor the LED panel, and display statistics graphically. A detailed description can be found in *Chapter 5. Web-Based Interface*.

1.4.3 SNMP Management

Since the switch supports SNMP, users can manage the switch with an SNMP-compatible management station running platforms such as HP OpenView. It also supports a comprehensive set of MIB extensions along with MIB II, Ethernet MIB, the 802.1D bridge MIB, and 4 groups of RMON. Please see Chapter 3, or *Chapter 6. SNMP Management* for more information.

Chapter 2. Hardware Installation and Setup

The following guidelines will help you to easily install the switch, and to ensure that it has the proper power supply and environment.

2.1 Installation Overview

Follow these steps to install your IntraCore switch:

1. Open the box and check the contents. See *Chapter 1.1 Package Contents* for a complete list of the items included with your IntraCore switch.
2. Install the switch in an equipment or wall rack, or prepare it for desktop placement.
3. Connect the power cord to the unit and to an appropriate power source.
4. Connect network devices to the switch.



See the sections below for more detailed installation instructions.

2.1.1 Safety Overview

The following information provides safety guidelines to ensure your safety and to protect the switch from damage.



Note: This information is intended as a guideline, and may not include every possible hazard to which you may be exposed. Use caution when installing this switch.

- Only trained and qualified personnel should be allowed to install or replace this equipment.
- Always use caution when lifting heavy equipment
- Keep the unit clean
- Keep tools and components off the floor and away from foot traffic
- Avoid wearing rings or chains (or other jewelry) that could get caught in the switch. Metal objects can heat up and cause serious injury to persons and damage to the equipment. Avoid wearing loose clothing (i.e. ties or loose sleeves) when working around the switch

When working with electricity, follow these guidelines:

- Disconnect all external cables before installing or removing the cover
- Do not work alone when working with electricity
- Always check that the cord has been disconnected from the outlet before performing hardware configuration
- Do not tamper with the equipment. Doing so could void your warranty
- Examine your work area for potential hazards (i.e. wet floors, ungrounded cables, etc.)

2.1.2 Recommended Installation Tools

You will need the following tools and equipment (not included) to install the switch into an equipment rack:

- Flat head screwdriver
- Phillips head screwdriver
- Antistatic mat or foam



2.1.3 Power Requirements

The electrical outlet should be located near the switch and be easily accessible. It must also be properly grounded.

Make sure the power source adheres to the following guidelines:

- Power: Auto Switching 110/240 VAC
- Frequency range: 50/60 Hz
- Maximum Input AC Current: 1.0A at 115 VAC full load

2.1.4 Environmental Requirements

The switch must be installed in a clean, dry, dust-free area with adequate air circulation to maintain the following environmental limits:

- Operating Temperature: 0° to 40° C (32° to 104° F)
- Storage Temperature: -20° to 70° C (-4° to 158° F)
- Relative Humidity: 10% to 90% non-condensing
- Storage Relative Humidity: 10% to 95% non-condensing

Avoid direct sunlight, heat sources, or areas with high levels of electromagnetic interference.

2.1.5 Cooling and Airflow

The IntraCore 3500 series switches use internal fans for air-cooling. Do not restrict airflow by covering or obstructing air vents on the sides of the switch.

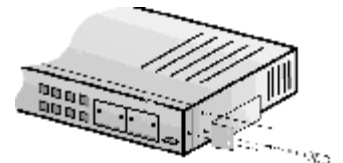


2.2 Installation into an Equipment Rack

To install the unit in an equipment rack, use the following procedure:

Important! Before continuing, disconnect all cables from the unit.

1. Place the switch on a flat, stable surface.
2. Locate a rack-mounting bracket (supplied) and place it over the mounting holes on one side of the unit.
3. Use the screws (supplied) to secure the bracket (with a Phillips screwdriver).
4. Repeat the two previous steps on the other side of the unit.
5. Place the switch in the equipment rack.
6. Secure the switch by securing its mounting brackets onto the equipment rack with the appropriate screws (supplied).



Important! Make sure the unit is supported until all the mounting screws for each bracket are secured to the equipment rack. Failure to do so could cause the unit to fall, which may result in personal injury or damage to the unit.

2.2.1 Equipment Rack Guidelines

Use the following guidelines to ensure that the switch will fit safely within the equipment rack:

- Size: 17.25 x 10.0 x 1.8 inches (423 x 245 x 39 mm)
- Ventilation: Ensure that the rack is installed in a room where the temperature remains below 40° C (104° F). Be sure that there are no obstructions, such as other equipment or cables, blocking airflow to or from the vents of the switch
- Clearance: In addition to providing clearance for ventilation, ensure that there is adequate clearance for servicing the switch from the front

2.3 GBIC Interfaces

The GBIC Interface is the industry standard for Gigabit Ethernet Interfaces. Some of the benefits of GBIC include reducing the components needed in your “spares” inventory, a wide variety of manufacturers with cross-vendor compatibility and competitive prices.

Instructions for installing, removing, and maintaining GBIC modules are provided in following sections.



Model	Part Number	Standard	Media
GBIC 1000SX	99-00549-01	1000BaseSX	Multi-mode fiber
GBIC 1000LX	99-00550-01	1000BaseLX	Single mode fiber
GBIC 1000T	99-00673-01	1000BaseT	Category 5 UTP copper
GBIC 1000TP	99-00647-07	1000BaseT	Category 5 UTP copper

Table 2-1 GBIC Modules by Asanté

2.3.1 Installing a GBIC

GBICs are hot swappable. This means that they can be inserted and removed while the unit is powered on. However, you should allow 40 – 60 seconds for the switch to recognize the module when it has been installed while the unit is on.

1. Wearing an ESD (electro-static discharge) wrist strap, remove the GBIC module from its protective packaging.
2. Verify that the GBIC is the correct type for your network (see the table above).
3. Grip the sides of the GBIC with your thumb and forefinger, then insert the GBIC into the slot on the face of the switch.
4. Slide the GBIC into the slot until you hear or feel a click. The click indicates that the GBIC is locked into the slot.
5. *GBIC 1000SX and GBIC 1000LX modules:* Remove the rubber plugs from the end of the GBIC module. Save them for future use.
6. Attach the appropriate cable.

Note: After installing a GBIC 1000T module, the link LED will light even before a valid cable has been connected. This is a normal condition for most 1000BaseT GBIC modules.

2.3.2 Removing a GBIC

Caution: GBIC 1000T modules run hot under normal operating conditions. When it has been removed from the system, place it on a heat resistant surface and allow the module to cool before handling.

Note: Unnecessary removals/insertions of a GBIC module will lead to premature failure of the GBIC. The rated duty cycle for a GBIC module is 100 to 500 removals/insertions.

Follow the steps below to remove a GBIC interface from a Gigabit Ethernet module:

1. Disconnect the cable from the GBIC module.
2. Release the GBIC from the slot by simultaneously squeezing the locking tabs on both sides of the GBIC.
3. Slide the GBIC out of the slot.
4. *GBIC 1000SX and GBIC 1000LX modules:* Install the rubber plugs in the GBIC optical bores, and place the GBIC in protective packaging.

2.3.3 GBIC Care and Handling

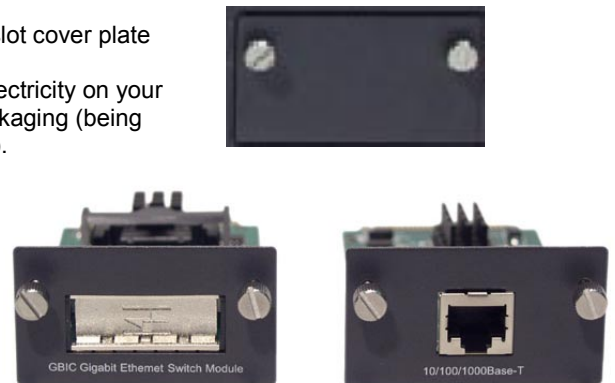
Follow these GBIC maintenance guidelines:

- GBICs are static-sensitive. To prevent ESD damage, follow your normal board and component handling procedures. Wear an ESD wrist strap
- GBIC 1000SX and GBIC 1000LX modules are very sensitive to dust and contaminants. When they are not connected to a fiber-optic cable, install the rubber plugs in the optical bores
- The ferrules of the optical connectors may pick up debris that can obstruct the optical bore. Use an alcohol swab or equivalent to clean the ferrules of the optical connector

2.4 Installing Optional Hardware Modules

Follow the steps below to install your media modules (10/100/1000BaseT, 1000BaseX GBIC, 1000BaseSX or 100BaseFX):

1. Using a flat-head screwdriver (not included), remove the slot cover plate from the switch.
2. Touch a grounded, metal object to discharge any static electricity on your body, and then remove the module from its protective packaging (being careful not to touch any board components or connectors).
3. Slide the module firmly into the module slot until it has clicked into place. The module's faceplate should be flush with the front panel of the switch.
4. Replace the screws to secure the module, being careful not to over-tighten the screws.
5. Connect network cables to the module port.
6. Restore power to the switch if necessary, or reset the switch.



2.5 Connecting Power

Use the following procedure to connect power to the switch:

Important: Carefully review the power requirements (Chapter 2.1.3) before connecting power to the switch.

1. Plug one end of the supplied power cord into the power connector on the back of the unit.
2. Plug the other end into a grounded AC outlet.
3. Turn on the switch's power. The Power LED will begin its initialization process.

The front panel LEDs blink and the Power LED illuminates when it has initialized. The switch is ready for connection to the network.

Important: If the power does not come on, check the next section to ensure you are using the correct cabling.

2.6 Connecting to the Network

The switch may be connected to an Ethernet network with the unit powered on or off. Use the following procedure to make your network connections:

1. Connect your network devices to the switch, following the cable guidelines outlined below.
2. After the unit is connected to the network, it can be configured for management capabilities (see the following chapters for information on configuration).

2.6.1 10/100BaseT Ports Cabling Procedures

The 10/100 ports on the IntraCore 3500 series allow for the connection of 10BaseT or 100BaseTX network devices. The ports are compatible with IEEE 802.3 and 802.3u standards.

Important: The switch must be located within 100 meters of its attached 10BaseT or 100BaseTX devices.

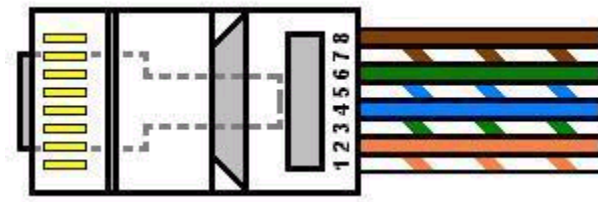
Use the following guidelines to determine the cabling requirements for your network devices:

- Connecting to Network Station: Category 5 UTP (Unshielded Twisted-Pair) straight-through cable (100 meters maximum) with RJ-45 connectors
- Connecting to Repeater/Hub/Switch's Uplink port: Category 5, UTP straight-through cable (100 meters maximum) with RJ-45 connectors



Note: There aren't specific uplink ports on these switches. All 10/100 ports on these switches are auto-sensing MDI/MDI-X. This advanced feature means that the 10/100 ports will automatically determine whether the device at the other end of the link is a hub, switch or workstation, and adjust its signals accordingly.

Although 10/100BaseT requires only pins 1, 2, 3 and 6, Asanté strongly recommends cables with all 8 wires connected as shown in Table 2-1 below.



1000BaseT requires that all four pairs (8 wires) be connected correctly, using Category 5 or better Unshielded Twisted Pair (UTP) cable (to a distance of 100 meters). Table 2-1 shows the correct pairing of all eight wires.

Pin Number	Pair Number & Wire Colors
1	2 White/Orange
2	2 Orange/White
3	3 White/ Green
4	1 Blue/White
5	1 White/Blue
6	3 Green/White
7	4 White/Brown
8	4 Brown/White

Table 2-2 Pin Numbers and Wire Colors

2.6.2 Gigabit Ethernet Ports Cabling Procedures

Cabling requirements for the optional hardware modules depend on the type module that has been installed. Use the following guidelines to determine the cabling requirements for your modules:

- 1000BaseSX GBIC: Cables with SC-type fiber connectors; 62.5-micron multimode fiber (MMF) media up to 275 meters (902 feet) long, or 50-micron MMF media up to 550 meters (1805 feet) long
- 1000BaseLX GBIC: Cables with SC-type fiber connectors; 10-micron single mode fiber media up to 5 kilometers (3.1 miles) long
- 1000BaseLX Long Haul GBIC: Cables with SC-type fiber connectors; 10-micron single mode fiber media up to 100 kilometers (62 miles) long
- 1000BaseT: Category 5 or better Unshielded Twisted Pair (UTP) cable to a distance of 100 meters (328.1 feet)

2.7 Setup

The following sections describe the steps for setting up the switch for basic configuration, and putting into place basic security measures (setting up password protection, changing from the default IP address and configuring the SNMP host table).

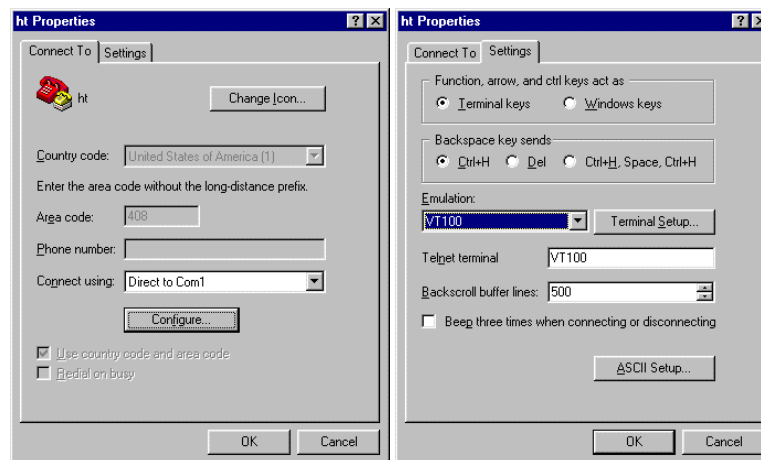
In order to configure the switch, you will need to connect to it through a console (out-of-band management), through your web browser, or through a telnet session.

2.7.1 Connecting to a Console

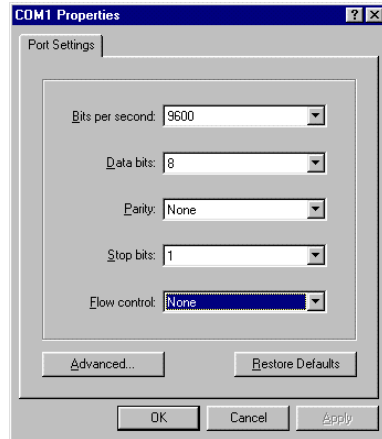
When attaching a workstation to the device, a standard straight-through CAT5 cable may be used, even when the workstation is attached via a patch panel. No crossover cable is needed with the MDX/MDI ports. It is recommended that the switch be kept off the network until proper IP settings have been set.

To connect the switch to a console or computer, setup the system in the following manner:

1. Plug power cord into the back of unit.
2. Attach a straight-through serial cable between the RS232 port and a COM port on the PC.
3. Setup a HyperTerminal (or equivalent terminal program) in the following manner:
 - Open the HyperTerminal program, and from it's file menu, right click on **Properties**
 - Under the **Connect To** tab, choose the appropriate COM port (COM1, COM2, etc)



- Under the Settings tab, choose VT100 for Emulation mode
- Select Terminal keys for Function, Arrow and Ctrl keys. Be sure the setting is for Terminal keys, NOT Windows keys
- Back under the **Connect To** tab, press the **Configuration** button



- Set the data rate to 9600 Baud
- Set data format 8 data bits, 1 stop bit and no parity
- Set flow control to NONE

Now that terminal is setup correctly, power on the switch (boot sequence will display in terminal).

2.7.2 Connecting Via the Web Browser

To connect to the switch via your web browser, you must first have configured your computer's IP address to be on the same IP address subnet as the switch (The switch's default IP is **192.168.0.1**). For more information on how to configure your TCP/IP settings, please refer to your computer manufacturer's user's manual.

You may now launch your web browser and enter the switch's default IP address into the address field. The Introduction page will appear, and you may proceed through the pages to configure each variable. See *Chapter 5. Web-Based Interface* for more information on configuring the switch via your web browser.

2.7.3 Connecting Via Telnet

To connect to the switch via a telnet session, you must first have configured your computer's IP address to be on the same IP address subnet as the switch (192.168.0.X). For more information on how to configure your TCP/IP settings, please refer to your computer manufacturer's user's manual.

You may now run a telnet session to configure and manage your switch. The **Enter Password** screen will appear. Enter the default password to access the Main Menu, and proceed to select the variables that you wish to configure. See *Chapter 3. Configuration* for more information on configuring the switch via telnet.

2.8 Changing the Password

The default password (which is **Asante**, and is case sensitive), may allow immediate access to ANYONE on the network. To protect your switch from unauthorized changes to the configuration, you must change the administrator's password. It can only be changed through the console or telnet interfaces.

To change the administrator's password, follow these steps:

1. Establish a telnet session, and type **Asante** at the password prompt.
2. Press **Enter** to proceed.
3. Type **c** to access the Configuration menu.
4. Type **u** to access the User Interface Configuration sub-menu.
5. Type **p** to select *Change Administrator's Password*.
6. Type the current password (Asante) and press **Enter**.
7. Type the new password and press **Enter**.
8. Re-type the new password to confirm your entry, and press **Enter**.

2.9 IP Assignment

To change the IP address of the switch from the default setting:

1. Access the System IP Configuration menu by typing **i** in the Configuration menu.
2. Type the command letter of the option you want to change.
3. Type the new address at the prompt.

To cancel a change, type **ctrl-c** at the command prompt.

4. Press **Enter**. The IP setting change for the switch takes effect.
5. Type **q** to quit and return to the Configuration menu.

When the reset is complete the switch should be seen on your network. If not, check the IP information again to ensure that all the data is correct.

2.10 SNMP Management

The SNMP Configuration Menu allows you to configure the unit's read and write community strings, and to enable or disable authentication traps. This menu also allows you to specify which of your network management stations will receive traps from the switch.

The **n** option in the Configuration Menu displays the SNMP (Simple Network Management Protocol) Configuration Menu, as shown below.

```
IntraCore SNMP Configuration Menu

SNMP Read Community: public
SNMP Write Community: private
Trap Authentication: Disabled

SNMP Trap Receivers:
  IP Address      Community
  1. xxx.xxx.xxx.xxx    public
  2. <empty>          <empty>
  3. <empty>          <empty>
  4. <empty>          <empty>

<Cmd>    <Description>
r        Set SNMP Read Community
w        Set SNMP Write Community
t        Toggle Trap Authentication Enable/Disable
a        Add/Update SNMP Trap Receiver
d        Delete SNMP Trap Receiver
q        Return to previous menu

Command>
```

Important! Be sure to change the SNMP community strings in order to prevent unauthorized access to management information. See Chapter 3 for details.

Also, see *Chapter 6. SNMP Management* for more detailed information on the SNMP protocol.

2.11 Using the Stacking Feature (IC3524 only)

The IC3524 firmware v.1.1 (or later) offers a stacking feature that allows the user to stack up to eight units, all sharing one IP address of the master switch (unit #1). This is an efficient and cost-effective way to add ports as needed. The following lists the characteristics of stacking that the user needs to be aware of:

- Uses any physical media supported by the switch: copper or fiber, Fast Ethernet or Gigabit Ethernet, or the special stacking kit shown below (sold separately)



IC35-SKT Stacking Kit
P/N 99-00710-01

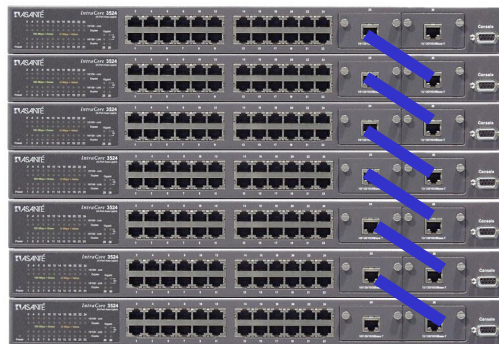
- All stacked units are managed through connection to the master switch, via console, telnet or web interfaces

Note: While the user may manage the stack via console, telnet or web interface, the initial formation of the stack may only be done by connection to a console.

- The switches need no extra software, but they must all have the 1.1 firmware installed (see Chapter 3.14 for firmware upgrade instructions)

Follow the steps below to install (build) a stack:

1. Physically stack the units, in an equipment rack, or on a flat, stable surface (Asanté recommends that the stack is formed from the bottom up for ease of adding additional units).
2. Units are connected via the Gigabit ports (see section 2.4 for instructions on installing the optional modules). Starting with the first unit in the stack (the bottom unit, in the photo below), connect the Ethernet cable or stacking cable from Gigabit port #26 to the Gigabit port #25 of the next unit and continue the connections to the last unit in the stack. The result is a stack with $n \times 24$ 10/100 ports and 2 Gigabit ports, where n is the number of units in the stack (up to eight).



3. For stacking operation, the stacking feature must first be enabled on each unit (by default, stacking is disabled). Establish a console connection to the first unit. Type **k** in the Configuration Menu to access the Stack Management menu. Type **t** to toggle the switch from “disabled” to “enabled”. Repeat for all remaining units.

IntraCore 3524 Configuration Menu

```
<Cmd>    <Description>
a        System Administration Configuration
i        System IP Configuration
b        Bootstrap Configuration
n        SNMP Configuration
p        Port Configuration
s        Spanning Tree Configuration
d        Unicast Forwarding Database Configuration
t        Security Management
v        VLAN Management
c        IP Multicast Traffic Management
m        Port Mirroring Configuration
f        File Up/Downloading Configuration
k        Stack management
r        System Reset Options
l        System Log
u        User Interface Configuration
y        System Utility
q        Return to previous menu
```

Command>

IntraCore 3524 Stack Management Configuration Menu

```
Stacking : ENABLED
Stacking Operation (1 of 8)
Stack IP  : xxx.xxx.xxx.xxx
Stack MAC : 00:00:94:CC:C7:6D

<Cmd>    <Description>
s        Stacking Multiple Modules
d        Stand Alone Operation
t        Toggle Stacking Enable/Disable
q        Return to previous menu
```

Command>

4. After all units have had stacking enabled, connect the console to the first unit (the Master unit).
5. Power cycle the whole stack, or, if the units are to be powered up separately, power the Master last.
6. Go to the Master's Stack Management menu and type **s** to begin the automatic formation of the stack.
7. After the stack is formed, configuration and operation of the stack can begin (see *Chapter 3 Configuration* and *Chapter 4 Advanced Configuration* for more details).

Chapter 3. Configuration

This chapter describes the log in procedure and configuration of the switch via the console or telnet interfaces. For information on configuring the switch via your web browser, see *Chapter 5. Web-Based Management*.

Note: The screens shown are of IC3524 firmware version 1.1. Earlier firmware may have slightly different screens, but will not effect the basic configuration instructions. The user interface of the IC3548-2GT may also vary, but should not effect the basic configuration instructions.

Logging In

When you connect to the Local Management Interface, the “Enter Password” prompt appears. Enter your password, and then press **Enter**. The Main Menu appears.

Important! The default password is **Asante**. The password is case-sensitive; enter it exactly as shown.

After logging in, the Main Menu appears, as shown below.

```
=====
IntraCore 3524 Remote Management System Version 1.10
Compiled Date: Dec 05 2001 13:53:58
Asante Technologies, Inc.
Copyright (c) 2001 Asante Technologies, Inc.
=====

Main Menu

<Cmd>    <Description>
g        General Information
c        Configuration
s        Statistics
q        Close Connection

Command>
```

From the Main Menu, you can access three submenus:

- General Information
- Configuration
- Statistics

If you are using Telnet, a fourth option for closing the connection is available as well.

Accessing a Submenu

To access a submenu, type the command letter that corresponds with the option you need to use. For example, type **g** for General Information.

Note: When configuring certain options on multiple IC3524 units (stacked switches), the System Unit Map screen may appear, like the one below. Type the number of the unit to be configured and press **Enter**.

```
System Unit Map
=====
```

Please select one of the following slots

Slot	Description (Unit Type)
1	IntraCore 3524 Unit
2	IntraCore 3524 Unit
3	IntraCore 3524 Unit
4	IntraCore 3524 Unit
5	IntraCore 3524 Unit
6	IntraCore 3524 Unit
7	IntraCore 3524 Unit
8	IntraCore 3524 Unit

```
Enter Unit Number (1 - 8) >
```

Exiting a Submenu

To exit a submenu, type **q**.

To exit a command line without changing the configuration setting (e.g., the “Set Password” option in the User Interface Configuration Menu), press **ctrl-c**.

3.1 General Information

The General Information Screen displays the current operating information of the switch, such as its name, IP address, and boot information.

To view General Information, type **g** from the Main Menu. A screen similar to that below appears.

```
IntraCore 3524 General Information Menu

System up for: 001day(s), 17hr(s), 27min(s), 54sec(s)
Software Version
  Bank 1 Image Version/Date: 1.10/Dec 05 2001 13:54:06
  Bank 2 Image Version/Date: 1.10/Dec 05 2001 13:54:06 (Running)
System Information
  PROM Image Version/Date: 1.03D/Oct 06 2001 15:29:58
  DRAM Size: 16.0MB      Flash Size: 2.0MB
  Config NVRAM Size: 64KB      Console Baud Rate: 9600 bps
Administration Information
  System Name: Test Stack
  System Location:
  System Contact:
System MAC Address, IP Address, Subnet Mask and Router
  MAC Address: 00:00:94:CC:C7:6D
  IP Address: xxx.xxx.xxx.xxx
  Subnet Mask: 255.255.255.0
  Router: 0.0.0.0
Bootstrap Configuration
  Boot Load Mode: LOCAL

Press any key to continue...
```

Note: The information displayed on this screen is read-only.

To exit the General Information Screen, press any key on your keyboard.

3.2 Configuration Menu

The Configuration Menu allows you to manage and configure switch and each of its ports.

To access the Configuration Menu, type **c** from the Main Menu. The Configuration Menu appears, as shown below (from a telnet session):

```

IntraCore 3524 Configuration Menu

<Cmd>    <Description>
 a       System Administration Configuration
 i       System IP Configuration
 b       Bootstrap Configuration
 n       SNMP Configuration
 p       Port Configuration
 s       Spanning Tree Configuration
 d       Unicast Forwarding Database Configuration
 t       Security Management
 v       VLAN Management
 c       IP Multicast Traffic Management
 m       Port Mirroring Configuration
 f       File Up/Downloading Configuration
 r       System Reset Options
 l       System Log
 u       User Interface Configuration
 y       System Utility
 q       Return to previous menu

Command>

```

Accessing a Submenu

To access a submenu, type the command letter that corresponds with the configuration option you need to use. For example, type **a** to access the System Administration Configuration Menu.

Note: When configuring certain options on multiple units (stacked switches), the System Unit Map screen may appear. Type the number of the unit to be configured and press **Enter**.

Most of the configuration options are described in detail in the rest of this chapter. The more advanced options are discussed in *Chapter 4. Advanced Management*.

3.3 System Administration Configuration

The System Administration Configuration Menu displays and allows you to change the name of the switch, its location, and the contact information.

```

IntraCore 3524 System Admin. Configuration Menu

Description: Asante Technologies, Inc. IntraCore 3524 Version: FW(1.10)
Object ID:   1.3.6.1.4.1.298.2.2.27
Name:        Test Stack
Location:
Contact:

<Cmd>    <Description>
 n       Set System Name
 l       Set System Location
 c       Set System Contact Information
 q       Return to previous menu

Command>

```

Changing System Administration Info

To change the name, location, or contact information for the switch, use the following procedure:

1. Open the System Administration Configuration Menu by typing **a** in the Configuration Menu.
2. Type the command letter (**n**, **l** or **c**) of the item to be changed in the System Administration Configuration Menu.
3. At the prompt, type the information you want to change.

Note: Each parameter is limited to 64 characters, including spaces.

To cancel a selected option, press **ctrl-c** at the command prompt.

4. Press **Enter**. The system administration information changes take effect.
5. Type **q** to quit and return to the Configuration Menu.

3.4 System IP Configuration

The System IP Configuration Menu displays and allows you to change the information needed to access the switch over the network via in-band management.

```
IntraCore 3524 System IP Configuration Menu

System MAC Address:    00:00:xx:xx:xx:xx
System IP Address:    000.000.000.000
System Subnet Mask:   255.255.255.0
System Default Router: 0.0.0.0

<Cmd>    <Description>
  i       Set IP Address
  m       Set Subnet Mask
  r       Set Default Router
  q       Return to previous menu

Command>
```

Important! By default, each address is set to 0.0.0.0.

Changing System IP Information

To change the IP address, subnet mask, or default router of the switch, use the following procedure:

1. Open the System IP Configuration Menu by typing **i** in the Configuration Menu.
2. Type the command letter (**i**, **m** or **r**) of the option you want to change.
3. Type the new address at the prompt.

Important! Follow the format: *number.number.number.number*

To cancel a change, press **ctrl-c** at the command prompt.

4. Press **Enter**. The IP setting change for the switch takes effect.
5. Type **q** to quit and return to the Configuration Menu.

3.5 Bootstrap Configuration

The Bootstrap Configuration Menu displays (and allows you to change) the bootstrap parameters used for loading the software for the switch at startup, and for downloading a new version of software when one is issued.

To access the Bootstrap Configuration Menu, type **b** in the Configuration Menu. If the Load Mode is set to *Local*, a screen similar to that below will appear.

```

IntraCore 3524 Bootstrap Configuration Menu

Bank 1 Image Version/Date: 1.10/Dec 5 2001 13:54:06
Bank 2 Image Version/Date: 1.00I/Dec 5 2001 13:54:06 (Running)

Load Mode:      Local
Boot Bank:      2

<Cmd>      <Description>
r          Set Load Mode to REMOTE
a          Toggle Boot Bank
o          Commence Bootstrap Sequence
q          Return to previous menu

Command>

```

When the switch is powered on, it loads its software via one of two methods: locally (via its internal flash memory, which is the default setting) or remotely over the network. You can change the bootstrap configuration from this menu. See *Appendix F. BootP Configuration* for more information.

3.6 SNMP Configuration

The SNMP Configuration Menu allows you to configure the unit's read and write community strings, and to enable or disable authentication traps. This menu also allows you to specify which of your network management stations will receive traps from the switch.

The **n** option in the Configuration Menu displays the SNMP (Simple Network Management Protocol) Configuration Menu, as shown below.

```

IntraCore 3524 SNMP Configuration Menu

SNMP Read Community: public
SNMP Write Community: private
Trap Authentication: Enabled

SNMP Trap Receivers:
  IP Address      Community
1. xxx.xxx.xxx.xxx public
2. <empty>      <empty>
3. <empty>      <empty>
4. <empty>      <empty>

<Cmd>      <Description>
r          Set SNMP Read Community
w          Set SNMP Write Community
t          Toggle Trap Authentication Enable/Disable
a          Add/Update SNMP Trap Receiver
d          Delete SNMP Trap Receiver
q          Return to previous menu

Command>

```

For further details on using SNMP and RMON for remote management of your network, see *Chapter 6. SNMP Management*.

3.6.1 Changing Community Strings

Important! Be sure to change the SNMP community strings in order to prevent unauthorized access to management information.

To change the switch's community strings, use the following procedure:

1. Open the SNMP Configuration Menu by typing **n** in the Configuration Menu.
2. To change the read community string, type **r**. To change the write community string, type **w**.
3. At the prompt, type a new community string.

For a description of read and write community strings, see the table below:

Settings	Description
SNMP Read Community	The string that defines access rights for reading SNMP data objects. The default is public .
SNMP Write Community	The string that defines access rights for writing SNMP data objects. The default is private .
Trap Authentication	The status of the SNMP agent for authentication trap generation. The default is disabled .
SNMP Trap Receivers	The IP addresses of the network management stations that can receive traps from the switch. Normally, these addresses are the same as your network management software systems' IP addresses. Important! A maximum of four trap receivers is allowed.

To cancel a selected option, press **ctrl-c** at the command prompt.

4. Press **Enter**. The new string takes effect.
5. Type **q** to quit and return to the Configuration Menu.

3.6.2 Enabling Authentication Traps

The switch can be set to generate authentication traps. Authentication traps are messages sent across the network to an SNMP network management station. They alert you when someone attempts to read or change data without the proper community string.

To set the switch to generate traps, use the following procedure:

1. Open the SNMP Configuration Menu by typing **n** in the Configuration Menu.
2. To toggle trap authentication to *Enabled*, type **t**.

To cancel the change, press **ctrl-c** at the command prompt.

3. Press **Enter**. The new setting takes effect.
4. Type **q** to quit and return to the Configuration Menu.

3.6.3 Adding or Updating a Trap Receiver

Trap receivers are network management stations designated to receive traps from the switch.

Important! The maximum number of trap receivers that can be set is four.

To add or update a trap receiver entry, use the following procedure:

1. Open the SNMP Configuration Menu by typing **n** in the Configuration Menu.
2. Type **a** to *Add/Update Trap Receiver*. An IP prompt appears.
3. Type the new or updated IP address of the network management station you want to receive traps. Press **Enter**.

To cancel an entry, press **ctrl-c** at the command prompt.

4. Type the trap receiver's community string when prompted for it, then press **Enter** again.

The trap receiver entry is added or updated. Type **q** to return to the Configuration Menu.

3.6.4 Deleting a Trap Receiver

Use the following procedure to delete a trap receiver you have previously designated:

1. Open the SNMP Configuration Menu by typing **n** in the Configuration Menu.
2. Type **d** to *Delete a Trap Receiver*. A prompt for the entry of the trap receiver appears.
3. Enter the number of the entry you want to delete (1,2,3, or 4) and press **Enter**.

The trap receiver is deleted from the SNMP Trap Receivers list.

For further details on using SNMP, see *Chapter 6 SNMP Management*.

3.7 Port Configuration

The Port Configuration Menu allows you to manually configure each port of the switch for port speed, duplex, and auto-negotiation. It also provides an overview of the entire system's port operating status.

To access the Port Configuration Menu, type **p** in the Configuration Menu. A System Unit Map screen appears. Type the unit number you wish to configure and press **Enter**.

```

System Unit Map
=====

Please select one of the following slots

Slot      Description (Unit Type)
-----
1         IntraCore 3524 Unit
2         IntraCore 3524 Unit
3         <none>
4         <none>
5         <none>
6         <none>
7         <none>
8         <none>

Enter Unit Number (1 - 8) >

```

The Basic Port Configuration Menu appears.

```

IntraCore 3524 Basic Port Configuration Menu      Unit Type: [IntraCore 3524 Unit]
Unit: [1]          Port: [01]
Operating Status:  -----  -K
Auto Negotiation:  *****  **
Speed/Duplex:      hhhhhhhh  hhhhhhhh  hhhhhhhh  GG

Port Status:  Enabled          Link Status: Down
Auto-Nego:    Enabled[ABCD]    Link Speed:  N/A

<Cmd>    <Description>
h        Help for Legends
t        Toggle Port Status Enable/Disable
a        Toggle Auto-Negotiation/Manual
l        Toggle 10M/100M bps Link Speed
d        Toggle Half/Full Duplex
r        Restart Auto-Negotiation
v        Advanced Port Configuration
g        Global Port Configuration
q        Return to previous menu

Command>
Select U)nit  Nex)t unit  Prev) unit  S)elect port N)ext port P)rev port

```

To see legends explaining the symbols used for both the Basic and Global Port Configuration Menu settings, type **h**. A screen appears, as shown below.

```
Legends for port status:
    X - Absent
    - - Link down
    D - Disabled by Mgmt Action
    d - Disabled by Security Violation
    B - Blocking
    S - Listening
    R - Learning
    + - Forwarding
    M - Mirror Port
Legends for Enable/Disable State:
    - - Disabled
    * - Enabled
Legends for Auto-Negotiation Advertisement:
    A - 100Base-TX full duplex mode
    B - 100Base-TX half duplex mode
    C - 10Base-T full duplex mode
    D - 10Base-T half duplex mode

Legends for port speed & duplex:
    f - 10 Mbps & full duplex
    F - 100 Mbps & full duplex
    h - 10 Mbps & half duplex
    H - 100 Mbps & half duplex
    G - 1 Gbps & full duplex

Legends for port priority:
(The range is from 0 to 7)
    0 - priority 0 (lowest)
    1 - priority 1
    2 - priority 2
    3 - priority 3
    4 - priority 4
    5 - priority 5
    6 - priority 6
    7 - priority 7 (highest)

Press any key to continue...
```

3.7.1 Enabling or Disabling a Port

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

Note: A manual operation such as this can be performed only when auto-negotiation is set to manual mode. See “Configuring a Port Manually” below.

To enable or disable a port, use the following procedure:

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. To select the port you want to enable or disable, type **s**, **n**, or **p** in the Basic Port Configuration Menu.
4. To toggle the port’s connection to either enabled or disabled status, type **t**.
5. To configure ports on another unit in the stack, type **u** to select the unit.

The port’s status is changed immediately, and it is reflected in the Port Configuration Menu’s Port Status indication and the Operating Status symbol for the port.

Important! Be careful not to disable the port to which the configuration computer is connected. This will disconnect the computer from the switch and prevent further configuration of the switch. Likewise, be cautious about disabling uplink ports on the switch.

3.7.2 Configuring Auto-Negotiation

Auto-negotiation is a feature of the Fast Ethernet standard that enables two devices on a common segment to communicate their transmission speed capabilities. This feature allows the devices to determine and use their highest common speed and best communication parameters.

Important! By default, all of the ports are set to Auto-Negotiation.

To set a port to manual-setting mode, or to re-enable auto-negotiation, use the following procedure:

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. To select the port for which you want to set the auto-negotiation mode, in the Basic Port Configuration Menu, type **s**, **n**, or **p**.

4. To toggle the port's auto-negotiation mode to *Enabled* or to return it to *Manual*, type **a**.
5. To configure auto-negotiation on another unit in the stack, type **u** to select the unit.

The Auto Negotiation status changes immediately, and is displayed on the Auto-Negotiation line near the top of the Port Configuration Menu.

Important! If you change the port's status from *Manual* to *Enabled* you must type **r** to restart auto-negotiation.

3.7.3 Configuring a Port Manually

If you have changed the Auto Negotiation status of a port to Manual, as described in the previous section, you can toggle the link speed from 10Mbps to 100Mbps and back, and toggle the port from half to full duplex and back.

Toggling Port Link Speed

Use the following procedure to toggle the port's link speed:

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. To select the port for which you want to set the link speed, type **s**, **n** or **p** in the Basic Port Configuration Menu.
4. To toggle the port's link speed, type **l**.
5. To configure port link speed on another unit in the stack, type **u** to select the unit.

The link speed is changed immediately, and the change is reflected in the Link Speed line near the top of the Port Configuration Menu.

Toggling Half to Full Duplex

Half duplex mode allows transmission in two directions on the same channel, but only in one direction at a time. Full duplex mode allows transmission in two directions on the same channel at the same time.

Important! To use full duplex mode, the device to which the port is connected must support and be configured for duplex mode.

Use the following procedure to change the duplex mode setting for a port that is in Manual status:

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. To select the port for which you want to set the duplex mode, type **s**, **n** or **p** in the Basic Port Configuration Menu.
4. To toggle the port's duplex mode, type **d**.
5. To configure duplex mode on another unit in the stack, type **u** to select the unit.

The duplex mode is changed immediately, and the change is reflected in the Link Speed/Duplex line near the top of the Port Configuration Menu.

Configuring 1000BaseX Ports

Because 1000BaseX ports are always in full duplex mode, the only configuration option for 1000BaseX ports is enabling and disabling the port.

3.8 Advanced Port Configuration

The Advanced Port Configuration Menu allows you to control the port broadcast and multicast rate, to enable or disable 802.3x flow control, and to set the default priority of the port.

To access the Advanced Port Configuration Menu, type **v** in the Port Configuration Menu. The Advanced Port Configuration Menu appears, as shown below.

```
IntraCore 3524 Advanced Port Configuration Menu      Unit Type: [IntraCore 3524 Unit]
Unit: [1]          Port:  [01]
Operating Status:  -----  -----  -----  -K
Flow Ctrl:        -----  -----  -----  --
Class Of Service:  *****  *****  *****  **
Priority:          00000000  00000000  00000000  00

Flow Control: Disabled
IEEE 802.1p Traffic Class Of Service: Enabled
Port Default Priority: 0

<Cmd>    <Description>
h        Help for Legends
f        Toggle Flow Control Enable/Disable
c        Toggle Traffic Class Of Service (COS) Enable/Disable
i        Set Port Default Priority
q        Return to previous menu

Command>
Select U)nit Nex)t unit  Prev) unit  S)elect port N)ext port P)rev port
```

The following subsections explain the configuration options in the Advanced Port Configuration Menu.

3.8.1 Enabling or Disabling 802.3x Flow Control

Use the following procedure to control traffic and avoid congestion, such as when there is a shortage of buffer resources for the port. Flow control is accomplished by means of standard PAUSE control frames for each port, independent of all others. Before you can enable flow control for a port, that port must be configured to operate in Full Duplex mode.

If you enable flow control on a port, and that port runs short of buffer resources, the port will transmit PAUSE frames. When it receives them, the link partner obeys these PAUSE frames. When the low-resource situation is relieved, the port sends out PAUSE frames with zero time values. This ends the pause state that was imposed on the end-station.

To enable flow control, take the following steps.

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. Type **v** in the Basic Port Configuration Menu to open the Advanced Port Configuration Menu.
4. To select the port for which you want to enable or disable flow control, type **s**, **n** or **p**.
5. To toggle flow control for the selected port, type **f**.
6. To configure flow control on another unit in the stack, type **u** to select the unit.

In the Advanced Port Configuration Menu, the Flow Control symbol for the selected port reflects its change in state, as does the 802.3x Flow Control setting.

Important! When using this method of flow control, the link partner must be configured to recognize PAUSE frames.

3.8.2 Setting Port Class of Service

To set a port's class of service, take the following steps.

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.

3. Type **v** to access the Advanced Port Configuration Menu.
4. To select the port for which you want to enable or disable class of service, type **s**, **n** or **p**.
5. To toggle traffic class of service for the selected port, type **c**.
6. To configure class of service on another unit in the stack, type **u** to select the unit.

In the Advanced Port Configuration Menu, the Traffic Class of Service symbol for the selected port reflects its change in state.

3.8.3 Setting Port Default Priority

This priority setting determines the order in which the port forwards packets. Each port is associated with a traffic class: zero (0) is the lowest, and the default priority level. Seven (7) is the highest priority level. Use the following procedure to set the priority for a port:

1. Access the Port Configuration Menu by typing **p** in the Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. Type **v** to access the Advanced Port Configuration Menu.
4. Use **s**, **n** or **p** to select the port for which you want to set the default priority.
5. Type **i** to set the priority for the selected port.
6. Enter the priority, from 0 to 7, and press **Enter**.
7. To port priority on another unit in the stack, type **u** to select the unit.

The new default priority is shown on the Advanced Port Configuration Menu.

3.8.4 Global Port Configuration

The Global Port Configuration Menu allows you to simultaneously change the configuration information for all ports in a unit.

To change the port configuration for all ports in a unit, use the following procedure:

1. From the Configuration Menu, type **p** to access the Port Configuration Menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**.
3. From the Basic Port Configuration Menu, type **g**. The Global Port Configuration Menu appears, as shown in below.

```
IntraCore 3524 Global Port Configuration Menu      Unit Type: [IntraCore 3524 Unit]

Unit: [1]
Operating Status:  -----  -----  -----  -K
Auto Negotiation:  *****  *****  *****  **
Speed/Duplex:      hhhhhhhh  hhhhhhhh  hhhhhhhh  GG
Flow Ctrl:         -----  -----  -----  --
Class Of Service:  *****  *****  *****  **
Priority:           00000000  00000000  00000000  00

<Cmd>      <Description>
h          Help for Legends
t          Select Global Port Status Enable/Disable
a          Select Global Auto-Negotiation Enable/Disable
l          Select Global 10/100 Mbps Link Speed
d          Select Global Half/Full Duplex
f          Toggle Global Flow Control Enable/Disable
c          Toggle Global Class Of Service (COS) Enable/Disable
i          Set Global Port Default Priority
q          Return to previous menu

Command>
Select M)odule Nex)t unit   Prev) unit
```

Follow the procedures above for port configuration and advanced port configuration.

3.9 Unicast Forwarding Database Configuration

The Unicast Forwarding Database Configuration Menu allows you to view and search for addresses in the MAC Forwarding Table on the switch. It also provides options for displaying MAC addresses and IP/MAC binding by individual port or by VLAN.

The MAC Forwarding Table is a table of node addresses that the switch automatically builds by “learning.” It performs this task by monitoring the packets that pass through the switch, checking the source and destination addresses, and then recording the source address information in the table.

The switch uses the information in this table to decide whether a frame should be forwarded to a particular destination port or “flooded” to all ports other than the received port. Each entry consists of three parts: the MAC address of the device, the port number on which it was received, and the VLAN number.

Note: The MAC address table can hold a maximum of 8,192 entries.

When you type **d** in the Configuration Menu, the Unicast Forwarding Database Configuration Menu appears, as shown below.

```
IntraCore 3524 Unicast Forwarding Database Configuration Menu

Age-out Time:      300 sec.
MAC Address Count: 13
IP Address Count:  10

<Cmd>      <Description>
 a         Display All Forwarding Database With/Without IP
 p         Display Forwarding Database By Port With/Without IP
 v         Display Forwarding Database By VLAN With/Without IP
 m         Search for MAC Address
 i         Search for IP Address
 t         Set Age-Out Time
 q         Return to previous menu

Command>
```

3.9.1 Displaying the Forwarding Database

Use the following procedure to view the Unicast Forwarding Database table.

1. Open the Unicast Forwarding Database Configuration Menu by typing **d** in the Configuration Menu.
2. Type **a**, **p** or **v**, depending on the range of MAC addresses you want to view.

Type **a** to display the MAC addresses learned on all ports on the switch.

Type **p** to specify a unit and port (you will see the MAC addresses for that port only).

Type **v** to specify a VLAN (you will see the MAC addresses for the member ports of that VLAN only).

3. At the prompt that appears, type **y** to see IP addresses in the display or type **n** to see the display without IP addresses, then press **Enter**. The selected display appears.

Below is an example of the Unicast Forwarding Database table for all ports, without the IP displayed.

The **Type** field refers to the type of MAC address. The Type setting may be:

- **S** — static (set by management, and will *not* age out)
- **D** — dynamic (learned by the switch; will be aged out)
- **M** — multiple (associated with multiple IP addresses, as in the case of a router)
- **I** — Self (the MAC address of the switch)

Unit	Port	Type	MAC Address	PVID
1	17	D	00:00:94:00:00:10	0001
1	17	D	00:00:94:75:2B:D0	0001
1	17	D	00:00:94:93:21:38	0001
1	17	D	00:00:94:B4:7E:34	0001
1	17	D	00:00:94:C6:51:07	0001
1	17	D	00:00:94:C6:FC:43	0001
1	17	D	00:00:94:CB:5F:0E	0001
1	17	D	00:00:94:CC:C4:E5	0001
-	--	I	00:00:94:CC:C5:36	--
1	17	D	00:00:94:CC:C7:37	0001
1	17	D	00:0A:27:89:94:A4	0001
1	17	D	00:10:A4:B0:41:F9	0001
1	17	D	00:30:65:E7:17:8C	0001
1	17	D	00:40:33:E3:0A:83	0001
1	17	D	00:40:F4:29:A2:D5	0001
1	17	D	00:80:AD:B6:91:F9	0001
1	17	D	00:A0:24:9A:1E:4E	0001
1	17	D	00:C0:02:55:13:67	0001
1	17	D	00:E0:52:01:44:46	0001

Quit Next Page

3.9.2 Searching for a MAC Address

The Unicast Forwarding Database can be searched by MAC address or by IP address. To search for a specific MAC or IP address, use the following procedure:

1. Access the Unicast Forwarding Database Configuration Menu by typing **d** in the Configuration Menu.
2. Type **m** to search for a MAC address.
Type **i** to search for an IP address.
3. Type the MAC or IP address at the prompt.
4. Press **Enter**.

If the address is located, it is displayed, with its associated information. If the address is not located, a message appears, stating this.

The Search Summary screen tells the location of the MAC or IP address, the unit, port, and the domain name. Configuration information, such as the type, age, and priority are also displayed.

3.9.3 Setting the MAC Address Age-Out Time

This option sets the Age-Out Time for the MAC Forwarding Table.

The Age-Out Time is the number of seconds that addresses remain in the table after being learned by the switch. The default is 300 seconds.

Use the following procedure to set the MAC address Age-Out Time.

1. Access the Unicast Forwarding Database Configuration Menu by typing **d** in the Configuration Menu.
2. Type **t** to set the MAC Address *Age-Out Time*.
3. Enter the new Age-Out time (in seconds) at the prompt.
4. Press **Enter**.

The MAC Address Age-Out Time is changed and is displayed at the top of the Unicast Forwarding Database Configuration Menu.

3.10 Security Management

See *Chapter 4 Advanced Management*.

3.11 VLAN Management

See *Chapter 4 Advanced Management*.

3.12 IP Multicast Traffic Management

See *Chapter 4 Advanced Management*.

3.13 Port Mirroring Configuration

Port mirroring allows you to configure the switch to copy all traffic associated with one port (the Monitor Port) to a Mirror Port on the switch. You can connect the Mirror Port to a network analyzer or RMON probe for packet analysis. You can configure the Monitor Port to send either transmitted or received traffic to the Mirror Port.

```
IntraCore 3524 Port Mirroring Configuration Menu      Unit Type: [IntraCore 3524 Unit]
Unit: 01 Port: 01

System Port Mirroring Status: [Disabled]
Monitor Port: [N/A]
Port Traffic Monitor Type: [Port Receive Data]

<Cmd>      <Description>
s          Set Monitor Port
t          Toggle System Port Mirroring Enable/Disable
e          Toggle Port Monitor Type Receive/Transmit Data
q          Return to previous menu

Command>
Select U)nit Nex)t unit  Prev) unit  S)elect port N)ext port P)rev port
```

3.13.1 Enabling or Disabling System Port Mirroring

To enable or disable port mirroring, use the following procedure:

1. Type **m** in the Configuration menu to display the Port Mirroring Configuration menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**, or select another unit by typing **u** in the command line.
3. Type **t** to toggle System Port Mirroring.

The change is reflected immediately in the settings shown at the top of the Port Mirroring Configuration menu.

Note: If System Port Mirroring is enabled, then the Mirror Port setting shows Port 13 as Mirror Port by default. You can specify any other *10/100 port* to be a Monitor Port.

3.13.2 Specifying Port Traffic Monitor Type

To specify whether to monitor port receive traffic or port send traffic, System Port Mirroring must be enabled. After enabling port mirroring, use the following procedure to specify the Port Traffic Monitor Type:

1. Type **m** in the Configuration menu to display the Port Mirroring Configuration menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**, or select another unit by typing **u** in the command line.
3. Type **e** to toggle Port Monitor type.

The change is reflected immediately in the settings shown at the top of the Port Mirroring Configuration menu.

3.13.3 Setting the Monitor Port

To specify which port to monitor, use the following procedure:

1. Type **m** in the Configuration menu to display the Port Mirroring Configuration menu.
2. If necessary, select which unit to be configured on the System Unit Map and press **Enter**, or select another unit by typing **u** in the command line.
3. Type **s** and then enter the port number of the port you want to specify.

The change is reflected immediately in the settings shown at the top of the Port Mirroring Configuration menu.

3.14 File Up/Downloading Configuration

The Image File Downloading Configuration Menu allows you to upgrade your IntraCore 3524 system easily, using either TFTP or X/Y/Z modem protocol.

Type **f** in the Configuration Menu to access the Image File Downloading Configuration Menu, as shown below.

```
IntraCore 3524 File Downloading Configuration Menu

<Cmd>      <Description>
t          TFTP File Up/Downloading Configuration
x          X/Y/ZMODEM File Downloading Configuration
q          Return to previous menu

Command>
```

From the Image File Downloading Configuration Menu, select the downloading protocol. Type **t** to download the image file via TFTP or type **x** to download using the X/Y/Z modem protocol. The two subsections that follow describe downloading by each of the two protocols.

When Asanté issues a new version of software for the switch, you can obtain it from the Asanté World Wide Web site or by contacting Asanté Technical Support.

3.14.1 Image Downloading through TFTP

To download a new image file in-band through TFTP, type **t** in the Image File Downloading Configuration Menu.

```
IntraCore 3524 TFTP File Downloading Menu

Bank 1 Image Version/Date:  1.10/Dec 05 2001 13:54:06
Bank 2 Image Version/Date:  1.10/Dec 05 2001 13:54:06 (Running)

File Type:          Image
Server IP:          xxx.xxx.xxx.xxx
File Name:          3524110a.ima
Retry Count:        5
Destination Bank:   1

<Cmd>      <Description>
s          Set Server IP Address
f          Set File Name
d          Download Image File to Destination Bank
b          Download and Reboot from the Image File
r          Set Retry Count
a          Toggle Destination Bank
q          Return to previous menu

Command>
```

Performing a Software Upgrade at Runtime

The software image file must be downloaded from a server on your network that is running a TFTP server application.

Important! Make sure the switch is configured with an IP address. For details, see “Changing System IP Information” earlier in this chapter.

To upgrade the switch software via TFTP, use the following procedure:

1. Access the TFTP Image File Downloading Configuration Menu by typing **t** in the Image File Downloading Configuration Menu.
2. Type **s** to set the image server IP address.
3. At the prompt, enter the IP address of the server containing the image file, then press **Enter**.
4. Type **f** to set the image file name.
5. At the prompt, enter the image file's name and path, then press **Enter**.
6. Type **r** to set the *retry* count.
7. At the prompt, enter the number of attempts the switch will make to download the image file, then press **Enter**.
8. Select the Destination Image Bank by using typing **a**. In a typical situation, you will want to select the Bank on which the software is not currently running.
9. To download the image file to the destination bank, type **d**. This option allows you to change the boot bank at a later time or to use the System Reset Configuration to schedule a reset, at which time the new software will be run.

OR

To download the image file and reset the switch, type **b**. This option immediately boots the switch with the new version of software.

10. Type **q** to return to the Image File Downloading Menu.

3.14.2 Serial Downloading Configuration

The X/Y/ZModem Image File Downloading Menu lets you download a new software image file for the switch without interrupting the current operation.

To download a new image through the switch's serial (console) port, type **x** in the Image File Downloading Configuration Menu. The X/Y/ZModem Image File Downloading Menu appears, similar to the screen shown below.

```
IntraCore 3524 X/Y/ZMODEM File Downloading Menu

Bank 1 Image Version/Date: 1.10/Dec 05 2001 13:54:06
Bank 2 Image Version/Date: 1.10/Dec 05 2001 13:54:06 (Running)

Download Protocol:      ZMODEM
Current Baud Rate:     9600 bps
Destination Bank:      1

<Cmd>    <Description>
x        Set download protocol to XMODEM
y        Set download protocol to YMODEM
z        Set download protocol to ZMODEM
c        Change Baud Rate Setting
d        Download file to Destination Bank
b        Download and Reboot from the Image File
a        Toggle Destination Bank
q        Return to previous menu

Command>
```

Performing a Software Upgrade

Use the following procedure to upgrade the switch's software through its serial (console) port:

1. In the Image File Download Configuration Menu, type **x** to access the X/Y/Z Modem Image File Downloading Menu.
2. Type **x**, **y** or **z** to select the corresponding modem protocol.

Note: For information about these protocols, see the manual for your communications software.

3. Type **c** to select the console baud rate. The Baud Rate Setting Menu appears. The maximum baud rate currently supported is 57,600 bps.
4. Select one of the options in the above screen to select the required baud rate, and confirm it by typing **y**.

Note: The baud rate default for console management is 9600 bps; in most cases the default will match the rate for the connected terminal. If you change the baud rate for the console port, the screen will display garbled data unless the connected terminal is set to the same rate.

5. Type **a** to select the Destination Bank.
6. To download the image file, use any serial communications software such as Procomm Plus, HyperTerminal, ZTerm, etc. For file transfer instructions, follow the instruction manual of the serial communications software.

Note: The terminal on which the serial communications software is running must have the same baud rate as switch's console. The connection from the terminal to the switch console port must be an RS232C straight-through cable.

7. Type **d** to download to the selected destination bank or **b** to download and reset.
8. After performing a successful download, type **q** to return to the previous menu.

3.15 System Reset Configuration

The System Reset Configuration Menu allows you to reset the switch by performing a "warm" reboot. It also allows you to schedule a reset up to 24 hours in advance.

```
IntraCore 3524 System Reset Configuration Menu

Bank 1 Image Version/Date: 1.10/Dec 05 2001 13:54:06
Bank 2 Image Version/Date: 1.10/Dec 05 2001 13:54:06 (Running)

Reset Status:      Stop
Reset Type:        Normal
Reset Countdown: 1 sec.

Load Mode:        Local
Boot Bank:        2

<Cmd>    <Description>
s        Schedule Reset Time
c        Cancel Reset
r        Reset Switch
a        Toggle Boot Bank
d        Reset Switch to Factory Default
i        Reset Switch to Factory Default except IP and Bootstrap
q        Return to previous menu

Command>
```

3.15.1 Resetting the Switch

To reset the switch, use the following procedure:

1. Open the System Reset Menu by typing **r** in the Configuration Menu.

2. Type **r**, **d** or **i**. Typing **r** resets the switch to its current configuration. Typing **d** resets switch to the factory default. Typing **i** resets the switch to the factory default, but without affecting its IP and Bootstrap configuration.
3. Type **y** to confirm the reset or type **n** to cancel the reset.

Note: During the scheduled reset operation, you can see the reset countdown decrement by refreshing the screen.

3.15.2 Scheduling a System Reset

You can schedule the switch to automatically perform a reset from one second up to 24 hours (86,400 seconds) in advance.

To schedule a reset, use the following procedure:

1. Open the System Reset Menu by typing **r** in the Configuration Menu.
2. Type **s** to schedule a reset time (within the specified range).
3. Enter the number of seconds the switch will wait before it automatically resets.

Important! The maximum number of seconds that can be entered is 86,400 (24 hours).

4. Press **Enter**. The switch will reset automatically after the number of seconds you specified.

3.16 System Log

The switch's system log records and displays any major system events on the switch, such as fatal errors, plugging in or removing a module, etc.

To view the system log, use the following procedure:

1. Type **l** in the Configuration Menu. The System Log Menu appears, as shown below.

```
IntraCore 3524 System Log Menu
<Cmd>    <Description>
  l       Display System Log
  c       Clear System Log
  q       Return to previous menu
Command>
```

2. Type **I** in the System Log Menu to display the current system log.

The system log displays any major system events that have occurred on the switch. If no major events have occurred, "System up" messages are displayed.

```
IntraCore 3524 System Log Summary
=====
No.   D: H: M: S   Event
  1. 000:00:00:00 Reset NVDB sections to factory default
  2. 000:00:32:25 Spanning Tree Task Disabled
  3. 000:00:05:05 1-unit Software Stack Is Up and Running!
  4. 000:00:06:11 1-unit Software Stack Is Up and Running!
  5. 000:00:07:24 1-unit Software Stack Is Up and Running!
  6. 000:00:23:25 2-unit Software Stack Is Up and Running!
  7. 004:17:30:33 2-unit Software Stack is out of service!-Specast
  8. 004:17:50:02 2-unit Software Stack is back running!-Specast
  9. 004:19:09:08 REDO fail:ifnCFGSetPortStatus in the unit 1
 10. 004:19:26:35 REDO fail:ifnCFGSetPortStatus in the unit 1
 11. 004:19:27:15 1-unit Software Stack Is Up and Running!
 12. 004:19:30:35 2-unit Software Stack Is Up and Running!
 13. 004:20:17:47 1-unit Software Stack Is Up and Running!
 14. 004:20:26:40 2-unit Software Stack Is Up and Running!
 15. 000:00:00:30 2-unit Software Stack Is Up and Running!
 16. 000:00:06:21 Spanning Tree Task Enabled
 17. 000:00:14:38 1-unit Software Stack Is Up and Running!
 18. 000:01:50:58 2-unit Software Stack Is Up and Running!
 19. 000:00:01:06 2-unit Software Stack Is Up and Running!
 20. 000:00:01:06 2-unit Software Stack Is Up and Running!
Quit Next Page
```

Note: The system log holds a maximum of 64 entries.

3. Type **n** to display the next page of System Log information, or type **q** to quit.

3.16.1 Clearing the System Log

Use the following procedure to clear all entries from the current System Log:

1. Open the System Log Menu by typing **I** in the Configuration Menu.
2. Type **c** to clear the current System Log.

New entries will begin to accrue as events occur.

3.17 User Interface Configuration

The User Interface Configuration Menu lets you set the idle time-out periods for both the console and telnet user interfaces, change the password used for logging in to the Local Management Interface, and enable or disable the Web server.

To display the User Interface Configuration Menu, as shown below, type **u** in the Configuration Menu.

```
IntraCore 3524 User Interface Configuration Menu

Console UI Idle Time Out: Console UI idle time-out feature is disabled
Telnet UI Idle Time Out: 5 Min. HTTP Server Status: ENABLED

Telnet Sessions Status: Access Hosts:
Session Status Source IP
1 Active xxx.xxx.xxx.xxx 1. <empty>
2 Inactive <none> 2. <empty>
3 Inactive <none> 3. <empty>
4 Inactive <none> 4. <empty>

<Cmd> <Description>
c Set Console UI Time Out
t Set Telnet UI Time Out
p Change Administrator Password
a Add Access host
d Delete Access host
o Toggle to Enable/Disable HTTP Server
q Return to previous menu

Command>
```

3.17.1 Setting Console Idle Time-out Period

Use the following procedure to set the console idle time-out:

1. Type **c** in the User Interface Configuration Menu.

A prompt for the number of minutes is displayed.

2. Enter the desired idle time-out in minutes.

Note: The default time-out is 5 minutes. Range for time-out is 0-60 minutes (0 indicates no time-out). To exit without making any changes, press **ctrl-c**.

3. Press **Enter**.

The new Console UI Idle Time Out is reflected in the User Interface Configuration Menu.

3.17.2 Setting Telnet Idle Time-out Period

Use the following procedure to change the Telnet Time-out.

1. Type **t** in the User Interface Configuration Menu.

A prompt for the number of minutes is displayed.

2. Enter the desired idle time-out in minutes.

Note: The default time-out is 5 minutes. Range for time-out is 1-60.

To exit without changes, press **ctrl-c**.

3. Press **Enter**.

The new Telnet UI Idle Time Out is reflected in the User Interface Configuration Menu. After you have configured the desired time-outs, type **q** to return to the previous menu.

3.17.3 Changing the Password

Use this option to change the password that the user must enter when they log in.

Important! The factory default password is **Asante**. The password is case-sensitive.

To change the current Local Management Interface or Web-based Interface password, use the following procedure:

1. Type **p** in the User Interface Configuration Menu.
2. Type the password you have been using at the prompt.
3. Type a new password at the “Enter Current Password” prompt.

Important! The password is case-sensitive. The password can be up to a maximum of 20 characters in length. The password characters can be any ASCII code.

4. Press **Enter**.
5. Type the new password again at the confirmation password prompt.

To cancel the change in password, type **ctrl-c**.

6. Press **Enter**.

The password change takes effect.

7. Type **q** to return to the Configuration Menu.

You will now need to enter the new password each time you log in to the Configuration Menu.

3.17.4 Enabling or Disabling the Web Server

The current HTTP Server Status is shown in the User Interface Configuration.

Important! For security, the web server is disabled by default.

To toggle the status of the HTTP server, type **o** in the User Interface Configuration Menu.

3.18 System Utility

Type **y** on the Configuration Menu to access the Ping Utility Menu. Type **p** to enter the IP address you wish to Ping.

```
IntraCore 3524 Ping Utility Menu
```

```
<Cmd>    <Description>
  p       PING Utility
  q       Return to previous menu
```

```
Command>
```

3.19 Viewing Statistics

Viewing statistics on a regular basis allows you to evaluate your network's performance. You can view current statistics for the switch on a per-port basis and can change your view of those statistics and the counters displayed in it. To view statistics use the following procedure:

1. Type **s** in the Main Menu. Select a unit from the System Unit Map screen, and press **Enter**. The Port Statistics Counters screen is displayed, as shown below.

```

IntraCore 3524 Port Statistics Counters                               Unit: 1  Port: 1
Elapsed Time Since Up:      001:18:21:39

<Counter Name>  <Total>    <Avg./s>  <Counter Name>  <Total>    <Avg./s>
Total RX Pkts   0           0          Total RX Bytes   0           0
Good Broadcast  0           0          Good Multicast   0           0
Total TX Pkts   0           0          Total TX Bytes   0           0
TX Unicast      0           0          TX Non-unicast   0           0
Dropped Pkts    0           0          Undersize Pkts   0           0
Oversize Pkts   0           0          CRCAlign Errors  0           0
Fragments       0           0          FCS Errors       0           0
Collisions      0           0          Late Events      0           0
64-Byte Pkts    0           0          65-127 Pkts     0           0
128-255 Pkts   0           0          256-511 Pkts    0           0
512-1023 Pkts  0           0          1024-1518 Pkts  0           0
<Cmd>  <Description>  <Cmd>  <Description>  <Cmd>  <Description>
r      since reset    x      next Unit      n      next port
t      stop refresh   v      prev Unit      p      prev port
q      quit           i      select Unit    s      select port

Command>

```

2. Use the **s** command to select a port for which you want to see the counters, or use **n** and **p** to find the port.
3. Type **t** to stop the periodic updating of the counters, so you can record what they are at that time.
4. Type **r** to see a display of the same counters, but accrued since the last reset of the counters.
5. Type **r** in the "since reset" screen to reset the statistics counters so you can see them accrue again from zero.
6. Type **x**, **v** or **i** to view another unit's statistics.
7. Type **q** to quit either statistics screen and return to the Main Menu.

Chapter 4. Advanced Management

This chapter deals with the advanced management of the switch, via the console mode or telnet connection. See *Chapter 5. Web-Based Management* for information on managing the switch through your web browser.

The following sections describe these advanced topics for management of the IntraCore 3524:

- Spanning Tree Protocol
- SNMP and RMON Management
- Security Management
- VLAN Management
- Multicast Management

4.1 Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a part of the IEEE 802.1D standard that provides for redundancy in a bridged LAN by allowing multiple links between points in the LAN.

Without the use of STP, multiple links in a bridged network will result in bridging loops, which can generate excess broadcast traffic that can bring down an entire network. See *Chapter 7. Switching Concepts* for a more detailed explanation.

4.1.1 Enabling and Disabling STP

The switch is shipped with Spanning Tree enabled on all ports by default. To enable or disable STP on your switch, use the following procedure:

1. Type **c** to open the Configuration Menu.
2. Open the Spanning Tree Configuration Menu by typing **s** in the Configuration Menu.
3. Type **t** to toggle STP to enabled or disabled.

When you disable STP, you are prompted to confirm the change. The STP status is changed. The status is displayed near the top of the Spanning Tree Configuration Menu.

4.1.2 Configuring Spanning Tree Parameters

Important! You should attempt to set these parameters only if you have experience with the 802.1D specification.

To view the Spanning Tree Configuration Menu, as shown below, type **s** in the Configuration Menu.

IntraCore 3524 Spanning Tree Configuration Menu

```
STP Status:      Enabled
Bridge ID:       8000 00:00:94:CC:C7:37
Designated Root: 4000 00:00:94:AA:64:31
Root Port:      Unit: 2      Port: 1
Root Path Cost: 100
Addr Ageout Time: 300

Hello Time:      3 Sec.      Bridge Hello Time: 2 Sec.
Maximum Age:     20 Sec.     Bridge Maximum Age: 20 Sec.
Forward Delay:   15 Sec.     Bridge Forward Delay: 15 Sec.
```

```
<Cmd>    <Description>
t        Toggle STP Enable/Disable
i        Set Bridge Priority
h        Set Bridge Hello Time
a        Set Bridge Maximum Age
d        Set Bridge Forward Delay
p        Spanning Tree Port Configuration
q        Return to previous menu
```

Command>

4.1.3 Spanning Tree Port Configuration

To set the Port Priority and Port Path Cost values for STP, access the Spanning Tree Port Configuration Menu shown below by typing **p** in the Spanning Tree Configuration Menu.

IntraCore 3524 Spanning Tree Port Configuration Menu Unit: [1] Port: [01]

```
Port Speed:      10 Mbps
Port Status:     Enabled
Port State:      Forwarding
Port MAC Address: 00:00:94:CC:C7:6D
Port Priority:    0x80
Port Path Cost:  100
```

```
<Cmd>    <Description>
i        Set Port Priority
c        Set Port Path Cost
q        Return to previous menu
o        Display Stacking port cost (debug menu)
```

Command>

Select U)nit Nex)t unit Prev) unit S)elect port N)ext port P)rev port

Setting Port Priority and Path Cost

Use the following procedure to set the STP Port Priority and Path Cost values:

1. Access the Spanning Tree Port Configuration Menu by typing **p** in the Spanning Tree Configuration Menu.
2. Use the **s**, **n** and **p** commands to select the port you want to configure.
3. Type **i** to set the Port Priority.

Type **c** to set the Port Path Cost.

4. Enter a value for the setting you are making. See Chapter 7 for more information.
5. Press **Enter**.

The new Port Priority or Port Path Cost is displayed in the Spanning Tree Port Configuration Menu.

4.2 SNMP and RMON Management

The Simple Network Management Protocol (SNMP) may be used to manage the IntraCore 3524. The SNMP agent supports database objects that are defined in the following management information bases (MIBs):

- MIB II (RFC 1213)
- Bridge MIB (RFC 1493)
- RMON (RFC 1757) 4 groups - Ethernet Statistics, Ethernet History, Alarm, and Events (See next section for details)
- Private Asanté 3524 MIB

Any SNMP-based network management application can be used to manage the switch. For information on management of switches, refer to your SNMP software manual. Also, see *Chapter 6. SNMP Management* for more information on SNMP protocol.

For details on console-based SNMP settings, see “SNMP Configuration” in Chapter 3.

RMON Management

Remote Network Monitoring (RMON) allows the network manager to gather data on the network’s traffic for future retrieval. RMON is an Internet Standard defined in RFC1757.

Using RMON, a network monitor (also called a probe) listens to traffic on the network and gathers statistics that may be retrieved later by a network management station using SNMP, as described in the previous section.

The four groups of RMON that are supported by the switch are described in *Chapter 6. SNMP Management*.

The IntraCore 3524 switches provide control of the RMON groups only through SNMP. For information on controlling RMON groups, please refer to the documentation for your SNMP management application.

4.3 Security Management

To access the Security Management Menu, type **t** in the Configuration Menu. A screen similar to that below will appear.

```
IntraCore 3524 Security Management Menu

Duplicated-IP Monitoring Status : Enable
Duplicated-IP Trap Status       : Enable
Station Movement Trap Status    : Disable

<Cmd>    <Description>
p        Port Security Configuration
d        Toggle Duplicated-IP Detection Enable/Disable
i        Toggle Duplicated-IP Trap Enable/Disable
l        Display Duplicated-IP List
s        Toggle Station Movement Trap Enable/Disable
r        Reset All Security Configuration to Factory Default
q        Return to previous menu

Command>
```

Important! For any traps (alerts) to be sent, you must designate one or more devices as trap receivers. See “SNMP Configuration” in Chapter 3.

4.3.1 Duplicated IP Detection and Trap

The duplicated IP detection and duplicated IP trap security measures allow you to monitor the use of a single IP address by two stations.

If you enable duplicated IP detection, the switch starts monitoring the broadcast Address Resolution Protocol (ARP) traffic from all of its ports, to detect duplicated IP address conditions. When duplicate IP

addresses are used on the system, the MAC addresses of both stations and the ports they accessed are logged.

If you enable both duplicated IP detection and duplicated IP trap, the designated trap receiver gets an alert each time a duplicated IP address is used on the system. In order to send duplicated IP traps, duplicated IP detection must be enabled.

By default, duplicated IP detection and trapping are enabled.

Enabling and Disabling Duplicated IP Detection

To enable or disable detection of duplicated IP addresses:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **d** to toggle duplicated IP detection.

Enabling and Disabling Duplicated IP Trap

To enable the sending of a trap when a duplicated IP is detected, you must first enable duplicated IP detection. See the previous subsection, "Enabling and Disabling Duplicated IP Detection."

To enable or disable the sending of a trap when a duplicated IP is detected:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **i** to toggle duplicated IP trap.

Viewing a List of Duplicated IP Addresses

To view a list of duplicated IP addresses that have been detected at the switch:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **l** to display the duplicated IP list. A screen appears, similar to the following screen.

```
+-----+-----+-----+-----+
| IP Address | Owner MAC | P | Spoofer MAC | P |
+-----+-----+-----+-----+
xxx.xxx.xxx.xxx 00:00:94:CC:C5:36 1 00:00:94:CC:C7:37 17
xxx.xxx.xxx.xxx 00:00:94:CC:C5:36 1 00:00:94:CC:C7:37 17
xxx.xxx.xxx.xxx 00:00:94:CC:C5:36 1 00:00:94:CC:C7:37 17
End of Summary, Quit
```

4.3.2 Enabling and Disabling Station Movement Trap

The station movement trap security measure ensures that when any end station is moved from one switch port to another, an alert is sent to the designated trap receiver. Station movement is detected when a station's MAC address (already learned by the switch) appears on a different switch port. The station movement trap includes the station's MAC address and IP address (if available) and the switch's port numbers.

By default, station movement trap is disabled.

To enable or disable detection of the movement of a station on the switch:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **s** to toggle the station movement trap.

4.3.3 Configuring Port Security

To access the Port Security Configuration Menu, type **t** in the Configuration Menu to access the Security Management Menu, then type **p** to access the Port Security Configuration Menu. A screen similar to the following will appear:

```
IntraCore 3524 Port Security Configuration Menu      Unit Type: [24-100TX/RJ45]
Unit: 01 Port: 01

Unit Port Security Info:
[+: Port Security Enabled, -: No Port Security, !: Port Disabled By Security]
Port Security Status:  [01]----- [09]----- [17]----- [25]--XXXXXX

Port Security Type:  <none>
Port New Node Detect Trap Status:  [Disabled]
Port Intruder Detect Trap Status:  [Enabled]
Port Trusted MAC Address:  [<none>]

<Cmd>      <Description>
u          Set/Clear Port Security
t          Toggle Port Security Trap Enable/Disable
i          Insert/Modify Port Trusted MAC Address
d          Display Port Intruder Nodes
h          Port Security Help
q          Return to previous menu

Command>
Select U)nit      Nex)t unit      Prev) unit      S)elect port N)ext port P)rev port
```

Configuring Port New Node Detection Trap

The port new node detection trap security measure (also called “port security trap”) ensures that when any new device is connected to the secured port, an alert will be sent to the designated trap receiver. The new device is detected when it is connected to the switch and its MAC address is recognized as one not present in the current address table. The information shown in the alert is the new node’s MAC address and IP address (if available) and the port to which they are connected.

Once a device has been connected and has generated traffic on the network, the trap will not be re-sent. If the switch ages out the MAC address of a connected device from its forwarding database, new traffic from that device will result in a new node trap being sent. The default age-out time is 300 seconds. You may reduce the number of traps sent by lengthening the age-out time, as explained in “Setting the MAC Address Age-Out Time” in Chapter 3.

By default, New Node detection is disabled.

To enable or disable detection of a new node on the system, you must first set the security level on a port or group of ports to 1. Then, if it is not already enabled, you must enable New Node detection.

To set security level 1 on a port:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **p** to access the Port Security Configuration Menu.
3. Select **u** to Set/Clear port security.
4. Type **s** to set security.
5. Type the numbers of the ports for which you want to set the security. You can specify a single port, a series of port numbers separated by commas, a range of ports shown with a hyphen, or a combination of ranges and single ports. For example, type 1-8, 14 to specify ports one through eight, and port fourteen. See Help for more information.
6. Type **l** for Port Security Level 1.

To enable New Node detection:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **p** to access the Port Security Configuration Menu, as shown in Figure 4-5.
3. Type **t** to choose *Toggle Port Security Trap*.
4. Type **l** to toggle the new node trap (if it is not already enabled).

Configuring Port Lock and Intruder Lock

The port intruder security measure allows you to create a port-trusted MAC address that is the only station with full rights to direct traffic to the port. Attempts to send traffic to the port from other stations are regarded as security intrusions, and can be disallowed. The security measure may be enabled as a port lock (security level 2) or an intruder lock (security level 3).

Note: The three security levels are mutually exclusive; a port can have security level 1, level 2, or level 3, but never a combination of security levels.

To configure security level 2 or 3, you must specify the port-trusted MAC address. You can either specify the address directly, or direct the system to trust the address of the first station that addresses the port. By trusting the first station to address the port, you can configure port security before you know which system will ultimately use that port.

When security level 2 (port lock) is enabled and an intruder attempts to direct traffic to the port, the port is immediately disabled. The port is then re-enabled only by clearing the security level by management.

When security level 3 (intruder lock) is enabled and an intruder attempts to direct traffic to the port, the switch locks out the intruder's MAC address; the port will not accept any traffic from that station. The intruder's address is then re-enabled only by clearing the security level by management.

Important! If you set security level 2 or 3, you should also set the Intruder Trap. If you do not set this trap, you will not receive notification that the port has been disabled. See "Setting the Intruder Trap" section below.

By default, security levels 2 and 3 are both disabled.

Configuring Security Level 2 or Level 3

To set security level 2 (port lock) or level 3 (intruder lock) on a port:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **p** to access the Port Security Configuration Menu.
3. Use the commands at the bottom of the menu to navigate to the unit and port needed.
4. Select **u** to Set/Clear port security.
5. Type **s** to set security.
6. Type **2** to select Port Security with Port Lock, or **3** to select Port Security with Intruder Lock.
7. Type **1** to have the system trust the first station that addresses this port, or type **2** to enter a specific port-trusted MAC address. If you type **2**, you are prompted to enter an address where the values are hexadecimal and separated by colons, as follows: xx:xx:xx:xx:xx:xx

Setting the Intruder Trap

If you set security level 2 or 3, you should also ensure the Intruder Trap is set. Enabling this trap directs the system to send an alert to the designated trap receiver when an intruder tries to access the port. To set the intruder trap:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **p** to access the Port Security Configuration Menu.
3. Type **t** to choose Toggle Port Security Trap.
4. Type **2** to toggle the new node trap (if it is not already enabled).

Inserting/Modifying a Port Trusted MAC Address

When you set port security level 2 or 3 for a port, you specify the port-trusted MAC address. You can change that address for a port without completing all the steps to set the port security.

To add or change the port-trusted MAC address:

1. From the Configuration Menu, type **t** to access the Security Management Menu.
2. Type **p** to access the Port Security Configuration Menu.
3. Type **i**, and then follow the instructions on the screen.

Resetting Security to Defaults

To reset the security measures on the switch to the factory defaults, access the Security Management Menu by typing **t** in the Configuration Menu. Then type **r** to reset all of the security configurations to the factory-set defaults. These defaults and their meanings are discussed in the sections on each security measure, earlier in this chapter.

4.4 VLAN Management

A *virtual* LAN, or VLAN, is a logical grouping that allows stations to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of a network. The IntraCore 3524 supports port-based VLANs, in compliance with the IEEE 802.1Q standard. The following sections describe how to configure and manage VLANs on the switch. For more information on VLANs, see *Chapter 7. Switching Concepts*.

4.4.1 VLAN Specifications for the IntraCore 3500 Series

The switch supports the following features of the IEEE 802.1Q standard:

- Port-based VLAN management
- Up to 64 manually-configurable VLANs
- Default VLAN
- VLAN creation and deletion
- VLAN port member addition and deletion
- VLAN untagged set addition and deletion
- Configurable VID range: 2 to 4094
- Port VID configurable range: 1 to 4094
- Port ingress filtering
- Port admit frame type
- Independent VLAN learning (IVL)
- Shared VLAN learning (SVL)
- GVRP for dynamic VLAN learning (to be supported; later versions)
- Single STP (Spanning Tree Protocol) spanning multiple VLANs
- SNMP-based VLAN management

Other VLAN Features of the switch

- VLAN management security
- VLAN MAC address insertion and removal
- Console UI management of VLANs
- Web interface management of VLANs

The management operations allowed are:

- Creation
- Deletion
- Name configuration
- VID change configuration
- Adding and deleting port members

- Adding and deleting untagged sets
- Sharing and unsharing VLANs
- Inserting and removing MAC addresses
- Toggling management access

To access the VLAN Management Menu, type **v** in the Configuration Menu. A screen similar to the following will appear:

```

IntraCore 3524 VLAN Management Menu

VLAN Version:          1          VLAN Type:          Port Based
Max. Supported VLAN ID: 4094      Max. Supported VLANs: 64
Number of VLANs Configured: 1      Number of Active VLANs: 1

<Cmd>  <Description>
v      VLAN Group Static Configuration
p      VLAN Port Attribute Configuration
d      Display VLAN Groups Summary
a      Display Port VLAN Attribute Summary
r      Reset VLAN Configuration to Factory Default
q      Return to previous menu

Command>

```

4.4.2 Configuring Static VLAN Groups

To access the VLAN Group Static Configuration Menu, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **v** again to access the VLAN Group Static Configuration Menu. A screen similar to the following appears:

```

IntraCore 3524 VLAN Group Static Configuration Menu   VID: [0002]

Name: test2                      Created By: Mgmt
Mgm Access: Enable                Status: Active
Unit   Port List  1      8  9   16 17   24 25   32
=====
1      -----  -----  -----  -----  -----  -KXXXXXX  +: static
2      -----  -----  -----  -----  -----  KKXXXXXX  d: dynamic
3      -----  -----  -----  -----  -----  KKXXXXXX  -: Not Member
4      -----  -----  -----  -----  -----  KKXXXXXX  K: Stacking
5      -----  -----  -----  -----  -----  KKXXXXXX
6      -----  -----  -----  -----  -----  KKXXXXXX
7      -----  -----  -----  -----  -----  KKXXXXXX
8      -----  -----  -----  -----  -----  KXXXXXXX

<Cmd>  <Description>          <Cmd>  <Description>
c      Create VLAN           r      Remove VLAN
e      Set VLAN Name        t      Toggle Mgmt Access
m      Move ports to this VLAN  d      Delete Port Members
o      Overlap Ports To This Vlan  f      Display Vlan-Grp Information
l      Toggle To Vlan-prt Config Menu

Command>
S)elect VID   N)ext VLAN   P)rev VLAN   H)elp   Q)uit

```

Navigate to the VLAN that you want to configure by typing a command (**s**, **n** or **p**) as shown at the bottom of the screen. With the Select command, you select a VLAN by its VLAN ID (VID); you can type the VID of an existing VLAN, or the VID of a VLAN you will create.

Creating a VLAN

Follow the steps below to create a new VLAN:

1. Type **c** from the VLAN Group Static Configuration Menu.
2. Type **s** to select the VLAN, and then enter the VLAN ID (VID) that you decided to use. You will notice that the VID for an unused VLAN is 0000.
3. Press **Enter**.
4. Type **e** to set the VLAN name (up to 32 characters) and press **Enter**.
5. Type **m** to select the ports you wish to assign the VLAN.

To make more than one assignment, separate each one with a comma. For example, 8,11 specifies ports 8 and 11. To specify a range of ports, use a hyphen. For example, 1-3, 8, 11 specifies ports 1, 2, 3, 8, and 11. See Help for more information about specifying units and ports.

Removing a VLAN

To remove the VLAN, from the VLAN Group Static Configuration Menu, type **r**.

Enabling and Disabling Management Access

The IntraCore 3524 supports configurable management access for VLANs. By default, management access is enabled, and all devices connected to the switch in a VLAN can communicate with the switch management agent.

Important! You can disable management access for a VLAN. If security is a concern for members of a particular VLAN, disabling management access for that VLAN will prevent any member of that VLAN from attempting to change the switch's configuration.

To enable or disable management access for this VLAN, from the VLAN Group Static Configuration Menu, type **s** to select the VLAN, then type **t** to toggle management access.

Important! Do not disable Management Access if you are using only the default VLAN.

Adding/Moving Port Members

To add ports as members of the VLAN, from the VLAN Group Static Configuration Menu, type **m**. Follow the instructions on the screen to enter the port number to assign to the VLAN. Adding a port to a VLAN does not affect the port's status on any other VLAN.

Deleting Port Members

To delete ports as members of the VLAN, from the VLAN Group Static Configuration Menu, type **d**. Follow the instructions on the screen to enter the port number to delete from the VLAN. Deleting a port from a VLAN does not affect the port's status on any other VLAN.

4.4.3 Advanced Static VLAN Configuration

To specify Tagging or No Tagging for a Port, type **I** from the VLAN Group Static Configuration Menu. This takes you to the VLAN Port Configuration Menu. Next, type **v** to select Advanced Configuration Menu, as shown below:

```

IntraCore 3524 VLAN Port Configuration Menu      Unit: [1]  Port:  [01]

Port VLAN ID (PVID):      0001
Acceptable Frame Type: All Frames
Port Ingress Filtering: Disabled
Port Type: Normal
VLAN Membership : 0001u

<Cmd>      <Description>
 f          Toggle Port Ingress Filtering Enable/Disable
 t          Toggle Acceptable Frame Type(All Frames/Vlan-Tagged Frames Only)
 g          Set Tag/Untag Ports
 q          Return to previous menu

Command>
Select U)nit  Nex)t unit  Prev) unit  S)elect port N)ext port P)rev port

```

Specifying Tagging or No Tagging for a Port

Each VLAN maintains a list of ports that do not send tagged frames. When you add a port member to a VLAN, it is added to the untagged set by default. This means the frames sent out on this port will be untagged. Select the desired unit and then type **s** to select the port number. Type **g** to set the port to receive tagged frames for any given VLAN.

4.4.4 Configuring VLAN Port Attributes

To configure port attributes, type **p** in the VLAN Management Menu (or **I** in the VLAN Group Static Configuration Menu). This brings you to the VLAN port configuration menu, shown below. Navigate to the unit and port that you want to configure by typing a command (**u**, **s**, **n** or **p**) as shown at the bottom of the screen.

```

IntraCore 3524 VLAN Port Configuration Menu      Unit: [1]  Port:  [01]

Port VLAN ID (PVID):      0001
Acceptable Frame Type: All Frames
Port Ingress Filtering: Disabled
Port Type: Normal
VLAN Membership : 0001u

<Cmd>      <Description>
 c          Change Port VLAN ID
 a          Add VLANs to Port
 d          Delete VLANs from Port
 t          Set Port Type (IEEE 802.1Q Trunk/ASANTE Trunk/Normal)
 v          Advanced Config Menu
 p          Vlan Group Static Config Menu
 q          Return to previous menu

Command>
Select U)nit  Nex)t unit  Prev) unit  S)elect port N)ext port P)rev port

```

Setting the Port VLAN ID

Port VLAN ID (PVID) is used for VLAN classification of incoming untagged frames and has meaning only when a port is configured to receive both untagged and tagged frames. It is used to assign untagged frames to the VLAN identified by the PVID.

By default, each port on the switch has a PVID of 1 (the default VLAN). The allowed PVID range is 1 to 4094. For ports that are configured to receive only tagged frames, the PVID is meaningless and the port is assigned a PVID of 4095.

For ports that are members of more than one VLAN, received frames are assigned as follows:

- A tagged frame is forwarded to the VLAN matching the VID in the tag field of the frame
- An untagged frame is forwarded to the VLAN matching the PVID

To set the VLAN ID for the port (PVID), from the VLAN Port Configuration Menu, type **c**. Enter the number you are assigning (from 1- 4094). Press **Enter** when you are done.

Adding and Deleting VLANs from the Port

To add or delete VLANs assigned to a port, type **a** to add, or **d** to delete from the VLAN Port Configuration Menu. Follow the instructions on the screen.

Enabling and Disabling Port Ingress Filtering

By default, a port will accept and forward tagged frames whether or not the port is a member of a VLAN matching the VID of the tagged frame. If ingress filtering is enabled, incoming tagged frames are forwarded only if the port is a member of the VLAN matching the VID of the tagged frame. All other frames are dropped and no addresses will be learned. To enable or disable ingress filtering on the port, type **v** to access the Advanced Configuration submenu, and then type **f** to toggle port ingress filtering.

Configuring Port Receive Frame Type

By default, all ports on the switch receive both 802.1Q tagged frames and untagged frames. A port may be configured to receive only 802.1Q tagged frames. This configuration is a necessary part of Inter-Switch Link (ISL) configuration (see “Configuring Inter-Switch Links”). If a port is configured to receive only tagged frames, any untagged frames received by the port are dropped and the source address of the untagged frames is not learned.

Incoming tagged frames are forwarded to the VLAN whose VID is included in the tag header of the frame. See “Enabling and Disabling Port Ingress Filtering” for more information about forwarding and filtering of received tagged frames. To toggle the port between receiving all frames and receiving only tagged frames, from the VLAN Port Configuration Menu, type **e** to access the Advanced Configuration submenu, and then type **t**.

4.4.5 Displaying a Summary of VLAN Groups

To view a summary of VLAN groups, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **d** to access the VLAN Group Summary. A screen similar to the following appears:

```
IntraCore 3524 VLAN Group Summary
+-----+-----+-----+-----+
|VLAN ID|Mgmt Access| Created By | Status |
+-----+-----+-----+-----+
| 1      | Enable   | Mgm Action | Active, Independent |
| 2      | Enable   | Mgm Action | Active, Independent |
End of VLAN Summary,   Port Vlan Summary  Vlan Group Menu  Vlan Group Info Menu
Quit
```

4.4.6 Displaying a VLAN Port Summary

To view a unit port VLAN summary, type **v** in the Configuration Menu to access the VLAN Management Menu, then type **a** to access the Port VLAN Attribute Summary. Type the desired unit number and press **Enter**. A screen similar to the screen below will appear. To view the summary for other units, type **a** command as shown at the bottom of the screen.

```

IntraCore 3524 Unit 1 Port VLAN Info
=====
Port   PVID   Vlan Membership      Acceptable Ingress   Port
Number PVID   Membership           Frame Type Filtering Filtering Type
=====
  1    0001   0001u                All Frames Disabled  Normal
  2    0001   0001u                All Frames Disabled  Normal
  3    0001   0001u                All Frames Disabled  Normal
  4    0001   0001u                All Frames Disabled  Normal
  5    0001   0001u                All Frames Disabled  Normal
  6    0001   0001u                All Frames Disabled  Normal
  7    0001   0001u                All Frames Disabled  Normal
  8    0001   0001u                All Frames Disabled  Normal
  9    0001   0001u                All Frames Disabled  Normal
 10    0001   0001u                All Frames Disabled  Normal
 11    0001   0001u                All Frames Disabled  Normal
 12    0001   0001u                All Frames Disabled  Normal
 13    0001   0001u                All Frames Disabled  Normal
 14    0001   0001u                All Frames Disabled  Normal
 15    0001   0001u                All Frames Disabled  Normal
=====
Quit  Next Page  Sel Unit PreV Unit NeXt Unit Vlan Grp Summ
Vlan Port Menu  Help

```

4.4.7 Resetting VLAN Configuration to Defaults

To reset the security measures on the switch to the factory defaults, access the VLAN Management Menu by typing **v** in the Configuration Menu. Then type **r** to reset all of the VLAN configurations that have been changed back to the factory-set defaults.

4.5 IP Multicast Traffic Management

Multicast traffic is a means to transmit a multimedia stream from the Internet (a video conference, for example) without requiring a TCP connection from every remote host that wants to receive the stream. The stream is sent to the multicast address, and from there it's propagated to all interested parties on the Internet.

Traditional IP communication allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). IP multicast provides a third scheme, allowing a host to send packets to a subset of all hosts (group transmission).

Multicast Addresses

Multicasts are sent to special IP addresses in the range from 224.0.0.0 through 239.0.0.0. These are also called "Class D" addresses. The IP multicast address always begins with the four bits 1110 (which identifies the address as a multicast). The remaining 28 bits of the multicast address specify the individual multicast group.

When an end station wants to join in an IP multicast group, it binds the multicast address of that group to its network interface. When a node is using an IP multicast address it also uses an Ethernet multicast address. Ethernet IP multicast addresses begin 01:00:5e. The remaining 24 bits are the lowest 24 bits of the IP multicast address. There is not a 1-to-1 mapping of IP multicast addresses to Ethernet multicast addresses. When configuring a VLAN for multicast traffic, you specify the Ethernet address for the multicast group (see "Multicast Forwarding Database Configuration").

IGMP

Communication on a LAN between end stations and routers is managed by the Internet Group Management Protocol (IGMP). For complete information about IGMP, see RFC 1112, "Host Extensions..." and RFC 2236, "Internet Group Management Protocol, Version 2" <<http://ftp.isi.edu/in-notes/rfc2236.txt>>.

A router that supports multicast and IGMP sends periodic messages called "queries" on its LAN interfaces. These queries inquire if any end stations want to join a multicast group. End stations signal their desire to join the multicast group by responding with an IGMP "report." By using a multicast routing protocol, such as

Protocol-Independent Multicast (PIM), routers maintain forwarding tables that they use to forward multicast datagrams.

Packets delivered to members of the multicast group are identified by a single multicast group address. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in an IP multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

IGMP Snooping

A traditional Layer-2 switch is unable to determine which end stations on the LAN are interested in which multicast groups. To avoid unnecessary flooding, the switch may use IGMP Snooping. That means the switch listens to IGMP messages to learn which ports want multicast traffic from which multicast groups. The switch inserts the correct Ethernet multicast address into the forwarding table for the ports where an end station has joined a multicast group.

4.5.1 Configuring IP Multicast Traffic Management

The Multicast Traffic Management Menu allows you to set up group transmission. To access the Multicast Traffic Management Menu, type **c** in the Configuration Menu. You will see a screen similar to the following:

```
IntraCore 3524 IP Multicast Traffic Management Menu      VID: [01]

IP Multicast Forwarding Database
-----

IP Multicast Address Count      : 0
IGMP Status                    : [Disabled]
IGMP Proxy Report Forward      : [Disabled]
----- --XXXXXX ----- --XXXXXX

<Cmd>    <Description>
 i       Toggle IGMP Enable/Disable
 x       Toggle IGMP Proxy Report Forward Enable/Disable
 m       IP Multicast Forwarding Database Configuration
 d       Display Group Addresses
 a       Display Group Addresses in All VLAN
 q       Return to previous menu

Command>
S)elect VLAN      N)ext VLAN      P)rev VLAN
```

Enabling and Disabling IGMP Snooping

To enable or disable IGMP Snooping on the switch, from the Multicast Traffic Management Menu, type **i** to toggle the status of IGMP Snooping.

Displaying a Summary of Group Addresses

To display a list of multicast group addresses for the current VLAN, from the IP Multicast Traffic Management Menu, type **d**. You will see a screen similar to the following:

```
| Multicast IP Addr | Action |
+-----+-----+
xxx.xxx.xxx.xxx    IGMP
xxx.xxx.xxx.xxx    IGMP
xxx.xxx.xxx.xxx    IGMP
xxx.xxx.xxx.xxx    Mgm Action

End of Summary,  Quit
```

To display a list of all multicast group addresses, from the IP Multicast Traffic Management Menu, type **a**. You will see a screen similar to the following:

Multicast IP Addr	VID	Action
xxx.xxx.xxx.xxx	0001	Mgm Action
xxx.xxx.xxx.xxx	0001	Mgm Action
xxx.xxx.xxx.xxx	0001	Mgm Action
xxx.xxx.xxx.xxx	0002	Mgm Action
xxx.xxx.xxx.xxx	0002	Mgm Action

End of Summary, Quit

4.5.2 IP Multicast Forwarding Database Configuration

The Multicast Forwarding Database lists addresses of multicast groups, and assigns them to specific VLANs. It also lists the ports within a VLAN that can receive traffic from the multicast address.

To access the Multicast FDB Configuration Menu, type **c** in the Configuration Menu to display the IP Multicast Traffic Management Menu, and then type **m**. You will see a screen similar to the following:

```
IntraCore 3524 IP Multicast FDB Configuration Menu      VID: [01]

IP Multicast Address: <none>
Created By: <none>

<Cmd>      <Description>
  o        Add/Delete Ports
  i        Insert Multicast IP Addr
  r        Remove Multicast IP Addr
  q        Return to previous menu

Command>
S)elect VLAN  N)ext VLAN  P)rev VLAN  Select A)ddr  Nex)t Addr  Prev) Addr
```

Use the commands at the bottom of the menu to select a VLAN or Multicast Group address.

Adding Ports to the Selected Address

To add or delete ports belonging to the multicast group:

1. Select the VLAN that contains the ports and the address. Type **s** and enter the VID of your selected VLAN.
2. Select the Multicast Group address. Type **a** and enter the multicast IP address.
3. Type **o** and follow the instructions.

Inserting a Multicast Group Address

Inserting an address adds the address to the list of Multicast Groups for the current VLAN. The addresses begin 01:00:5e. The remaining 24 bits are the lowest 24 bits of the IP multicast address.

To insert an address:

1. Select the VLAN to which you will assign the new address. Type **s** and enter the VID of your selected VLAN.
2. Type **i** and follow the instructions to add the new address.

Removing a Multicast Group Address To remove an address:

1. Select a VLAN from which you will remove the address. Type **s** and enter the VID of your selected VLAN.
2. Type **r** and follow the instructions to remove the address.

Chapter 5. Web-Based Management

This chapter tells how to manage the switch by means of a Web browser, using Web pages to monitor and configure the switch. Most of the options and functions provided by Web browser management are similar to those of the Local Management Interface. For additional details about managing the switch, refer to *Chapter 3. Configuration*, and *Chapter 4. Advanced Management*.

Important! To use Web browser management, the switch must be configured with an IP address. For instructions on assigning an IP address to the switch, see “Configuring for Management” in Chapter 2.

Important! The Web browser interface to the switch is disabled by default. To enable the Web browser interface, use the User Interface Configuration Menu via a telnet session or console connection (see “User Interface Configuration” in Chapter 3).

Note: When forming a stack (IC3524 models), only the Master unit needs to have the Web browser interface enabled.

Accessing with a Web Browser

Once you have assigned the switch an IP address and enabled the Web browser interface, you can use a Web browser to manage the switch. Locate a computer that is attached to the same subnet as the switch.

To access the HTTP server:

1. Connect a computer with a functioning World Wide Web browser to the switch and open the browser.
2. Type the switch IP address in the URL field, then press **Enter**.
3. Enter user name **IntraCore** and a password in the dialog box that opens. The password is the same as the current console password (The default password is **Asante**).

Note: The user name and password are case-sensitive and must appear exactly as they are shown here.

4. Press **Enter**.

The Web Browser Management Overview page appears, as shown below (screenshots are from an IC3524 model with firmware version 1.1, two units stacked):

ASANTÉ IntraCore 3524

ASANTÉ IntraCore 3524
24-Port Auto-Uplink

ASANTÉ IntraCore 3524
24-Port Auto-Uplink

Contact email address: support@asante.com
Telephone: 800.622.7464
Fax: 801.566.3787

Copyright © 2000, Asanté Technologies, Inc. All Rights Reserved.

The Web Browser Management Overview page contains a sidebar with ten management option buttons, and a view of the IntraCore front panel that displays real-time switch operating information, as well as contact information for Asanté Technologies, Inc.

Note: The browser pages shown in this chapter are typical of those used for the IntraCore, and settings are given only as examples. The user must configure the IntraCore with parameters that are specific to the user's application and site requirements.

Management Buttons

The buttons on the left provide the following options:

- Front Panel
- Genl Info (General Information)
- Statistics
- Port Config (Port Configuration)
- Span Tree (Spanning Tree Protocol Configuration)
- SNMP (Simple Network Management Protocol)
- Addr Table (IP/MAC Address Table)
- VLAN (Virtual LAN Configuration)
- Security
- Duplicate IP (Duplicate IP Trap Log)

The following sections describe and explain the pages that are displayed when you click each of the buttons.

5.1 Front Panel Button

This button opens (or refreshes) the Web Browser Management Overview page. This is the top-level or opening page. The Web Browser Management Overview page is shown above and contains the following elements:

- Front panel display
- Port activity indicator
- Port selector feature

Front Panel Display

The front panel graphic displays the image of the connected switch(es), the LED panel(s), and the active data ports.

Port Activity Indicator

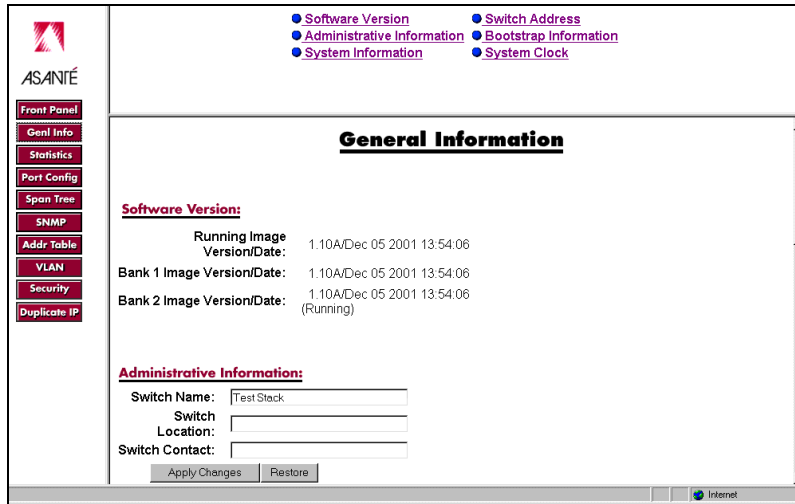
The front panel LED display simulates the IntraCore in real-time operating mode. The display approximates all switch activity as it occurs.

Port Selector Feature

If you point the cursor to a port connector and click the mouse, a port-specific page is displayed, which shows the selected port's configuration and traffic statistics.

5.2 Genl Info (General Information) Button

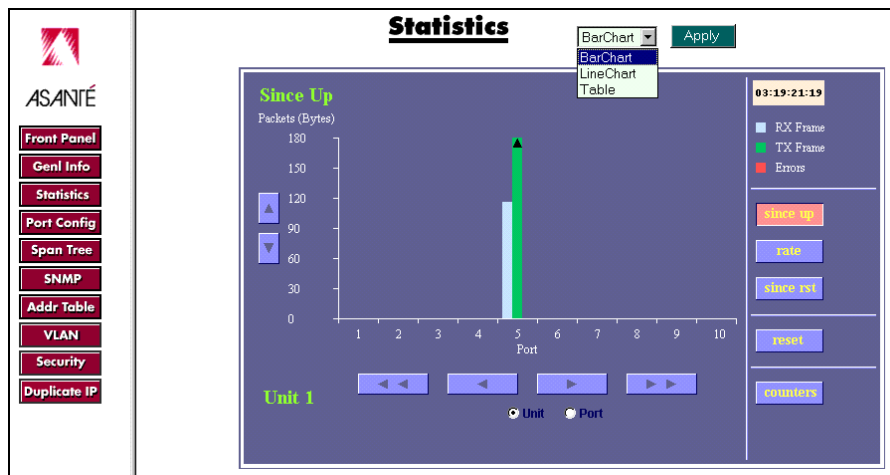
This button opens the switch's General Information page, as shown below.



The page has six sections, which are listed at the top of the page. To view another section, click a link at the top of the page or scroll down. The General Information parameters are described fully in “Viewing General Information” in Chapter 3.

5.3 Statistics Button

This button opens the Statistics page, which presents a graphical image of the IntraCore statistics, as shown below.



On this page, the user can view system statistics since the last system reset. For a description of the statistics counters, see “Viewing Statistics” in Chapter 3.

The following features allow you to modify the statistics bar chart.

- Up-Down Arrows – The up and down arrows let you scroll the screen up to view the counter graph. This is useful when the counters have run off the screen due to the system having been up for a long time.
- Right-Left Arrows - These arrows beneath the Bar Chart let you view the statistics for different ports on the same unit (if the Port radio button is selected) or ports in different units (if the Unit radio button is selected).
- Since Up Button – Brings up a graph of the total packets/bytes switched on the ports since the switch was last reset or powered on.

- Rate Button – Displays the rate of the packets or bytes per port.
- Since Rst Button– Displays the packets/bytes switched since the management counters were last reset or cleared.
- Reset Button– Clears the counters for future samplings.
- Counters – Displays the statistical counters of the associated view, since up or since reset.

Note: You may also view a summary of the frames per port by placing the cursor on the desired bar. A box with the statistics appears.

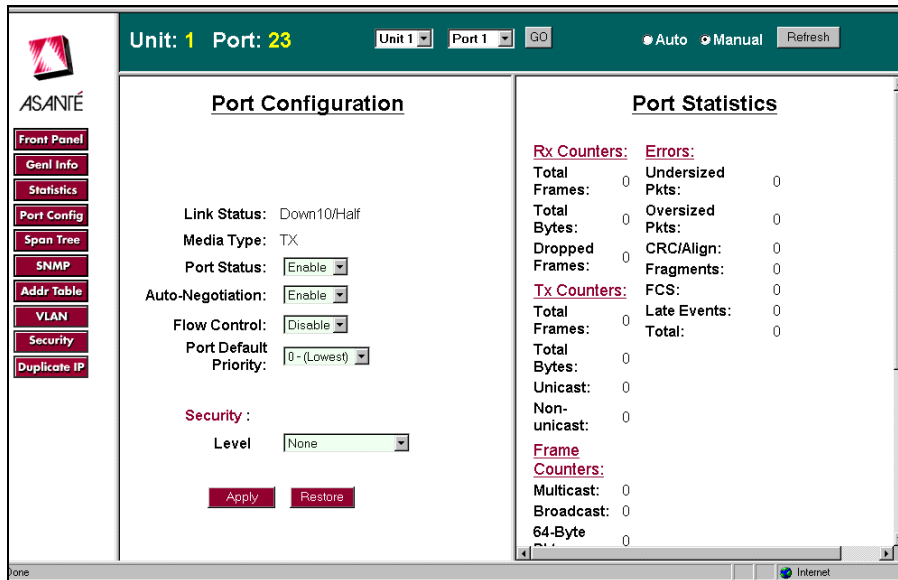
To see either a line graph or a table display of the system’s statistics, click on a bar, then choose the option you want from the pop-up menu at the top of the Statistics page, and click **Apply**.

5.4 Port Config (Port Configuration) Button

This button opens the Port Configuration page, which provides a comprehensive overview of the status of each port on the IntraCore, as shown below.

Unit - Port	State	Port status	Link status	Type	Mode	Unit - Port
2 - 1	Forwarding	Enabled	Down	TX	10/Half	2 - 1
2 - 2	Forwarding	Enabled	Down	TX	10/Half	2 - 2
2 - 3	Forwarding	Enabled	Down	TX	10/Half	2 - 3
2 - 4	Forwarding	Enabled	Down	TX	10/Half	2 - 4
2 - 5	Forwarding	Enabled	Down	TX	10/Half	2 - 5
2 - 6	Forwarding	Enabled	Down	TX	10/Half	2 - 6
2 - 7	Forwarding	Enabled	Down	TX	10/Half	2 - 7
2 - 8	Forwarding	Enabled	Down	TX	10/Half	2 - 8
2 - 9	Forwarding	Enabled	Down	TX	10/Half	2 - 9
2 - 10	Forwarding	Enabled	Down	TX	10/Half	2 - 10
2 - 11	Forwarding	Enabled	Down	TX	10/Half	2 - 11
2 - 12	Forwarding	Enabled	Down	TX	10/Half	2 - 12
2 - 13	Forwarding	Enabled	Down	TX	10/Half	2 - 13
2 - 14	Forwarding	Enabled	Down	TX	10/Half	2 - 14
2 - 15	Forwarding	Enabled	Down	TX	10/Half	2 - 15
2 - 16	Forwarding	Enabled	Down	TX	10/Half	2 - 16
2 - 17	Forwarding	Enabled	Down	TX	10/Half	2 - 17
2 - 18	Forwarding	Enabled	Down	TX	10/Half	2 - 18
2 - 19	Forwarding	Enabled	Down	TX	10/Half	2 - 19
2 - 20	Forwarding	Enabled	Down	TX	10/Half	2 - 20
2 - 21	Forwarding	Enabled	Down	TX	10/Half	2 - 21
2 - 22	Forwarding	Enabled	Down	TX	10/Half	2 - 22
2 - 23	Forwarding	Enabled	Down	TX	10/Half	2 - 23
2 - 24	Forwarding	Enabled	Down	TX	10/Half	2 - 24

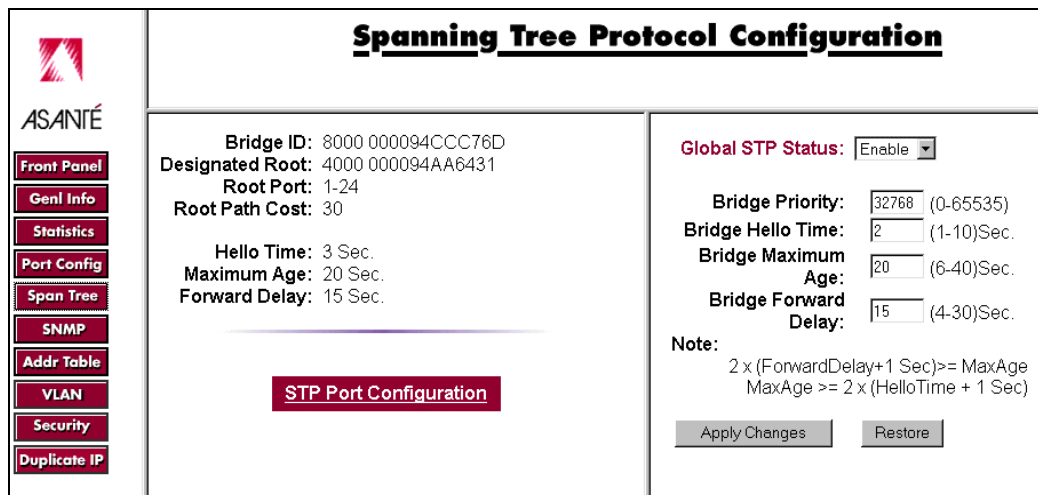
To configure individual ports, click on the associated blue number in the right or left hand margin to access that port’s configuration page.



Configure the variables by choosing the desired option from each drop-down menu.

5.5 Span Tree (Spanning Tree) Button

This button opens the Spanning Tree Protocol (STP) Configuration page, which shows the STP Configuration of the IntraCore, as shown below.



STP configuration is explained in *Chapter 4. Advanced Management*. Click the STP Port Configuration button to display the STP Configuration settings for each port (see the port configuration page below), or configure the ports all together (globally) from the right side of the page. Click **Apply Changes** to have your configuration take effect, or click the **Restore** button to restore the defaults.

Port	Status	MAC Address	Priority	Path Cost	Apply Changes
1	Forwarding	00:00:94:CD:40:30	128	100	Yes No
2	Forwarding	00:00:94:CD:40:31	128	100	Yes No
3	Forwarding	00:00:94:CD:40:32	128	100	Yes No
4	Forwarding	00:00:94:CD:40:33	128	100	Yes No
5	Forwarding	00:00:94:CD:40:34	128	100	Yes No
6	Forwarding	00:00:94:CD:40:35	128	100	Yes No
7	Forwarding	00:00:94:CD:40:36	128	100	Yes No
8	Forwarding	00:00:94:CD:40:37	128	100	Yes No
9	Forwarding	00:00:94:CD:40:38	128	100	Yes No
10	Forwarding	00:00:94:CD:40:39	128	100	Yes No
11	Forwarding	00:00:94:CD:40:3A	128	100	Yes No
12	Forwarding	00:00:94:CD:40:3B	128	100	Yes No
13	Forwarding	00:00:94:CD:40:3C	128	100	Yes No
14	Forwarding	00:00:94:CD:40:3D	128	100	Yes No

Important! Do NOT configure any STP parameters unless you have knowledge of and experience with the IEEE 802.1d specification.

5.6 SNMP Button

This button displays the SNMP (Simple Network Management Protocol) page, as shown below.

SNMP Configuration

SNMP Read Community:

SNMP Write Community:

Trap Authentication:

SNMP Trap Receivers:

	IP Address	Community
1.	<input type="text" value="xxx.xxx.xxx.xxx"/>	<input type="text" value="public"/>
2.	<input type="text" value="<empty>"/>	<input type="text" value="<empty>"/>
3.	<input type="text" value="<empty>"/>	<input type="text" value="<empty>"/>
4.	<input type="text" value="<empty>"/>	<input type="text" value="<empty>"/>

Apply Changes Restore

See “SNMP Configuration” in Chapter 3 for an explanation of SNMP settings.

5.7 Addr (Address) Table Button

The Addr Table button opens the MAC and IP Address Table page, which displays two tables, as shown below.

The screenshot shows the ASANTÉ network management interface. On the left is a navigation menu with buttons for Front Panel, Genl Info, Statistics, Port Config, Span Tree, SNMP, Addr Table, VLAN, Security, and Duplicate IP. The main content area is divided into two sections:

MAC and IP address Counts (Click on Port number to show Port-based addr table or All to show All Ports)

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	All	
IP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9
MAC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9

MAC and IP address Counts (Click on the VID number to show VLAN-based addr table)

VID	1
IP	9
MAC	9

Search for IP: Search for MAC:

Sort by IP Sort by MAC

Port:All Address Table D = Dynamic, S = Static, * = Multiple IP

Unit	Port	Entry	IP Address	MAC Address	VID
1	24	D		00: E0: 52: 01: 44: 46	1
1	24	D		00: A0: 24: 9A: 1E: 4E	1
1	24	D		00: 00: 94: B5: 04: 5F	1
1	24	D		00: 00: 94: B5: E9: 65	1
1	24	D		00: 00: 94: 00: 00: 10	1
1	24	D		00: 00: 94: C9: 30: 98	1
1	24	D		00: 00: 94: C6: 51: 07	1
self	self	I		00: 00: 94: CC: C7: 6D	1
1	24	D		00: 00: 94: 93: 21: 38	1

The top table displays the counts of IP and MAC addresses for each port. The lower table displays IP and MAC addresses for either a particular port, or **all** ports. The activity status (Entry) and VLAN segment (VSEG) are also displayed for each device.

To see the MAC and IP addresses, the activity status, and the VLAN segment for the devices connected to a particular port, click the port's number in the top table. Use the **Search** boxes to search for either an IP or MAC address on the IntraCore.

5.8 VLAN Button

This button opens the VLAN Port Attributes page, as shown below.

The screenshot shows the ASANTÉ network management interface with the **VLAN Port Attributes** page open. The navigation menu on the left is the same as in the previous screenshot. The main content area displays:

VLAN Port Attributes

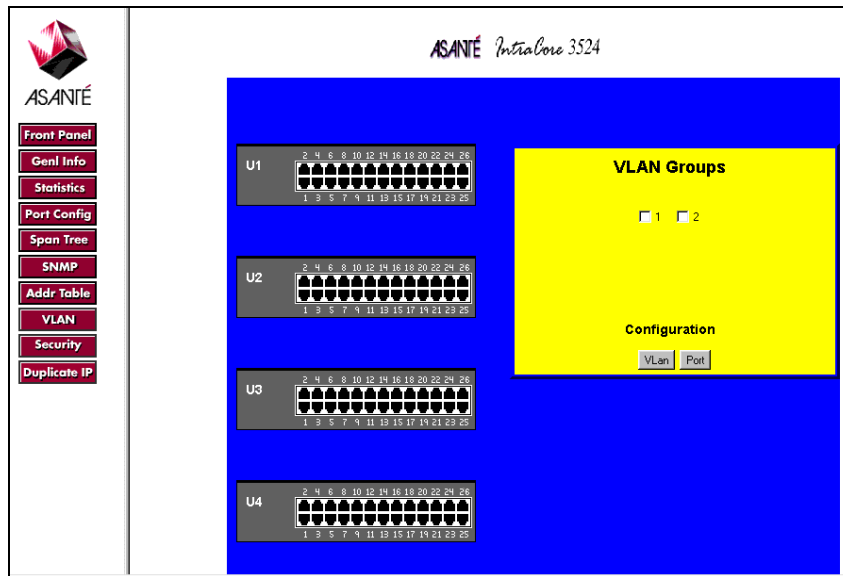
Unit: 1 2 3 4 5 6 7 8

VLAN Configuration

Unit - Port	PVID	Frame Type	Ingress Filtering
1 - 1	1	All Frames	Disabled
1 - 2	1	All Frames	Disabled
1 - 3	1	All Frames	Disabled
1 - 4	1	All Frames	Disabled
1 - 5	1	All Frames	Disabled
1 - 6	1	All Frames	Disabled
1 - 7	1	All Frames	Disabled
1 - 8	1	All Frames	Disabled
1 - 9	1	All Frames	Disabled
1 - 10	1	All Frames	Disabled
1 - 11	1	All Frames	Disabled
1 - 12	1	All Frames	Disabled
1 - 13	1	All Frames	Disabled
1 - 14	1	All Frames	Disabled
1 - 15	1	All Frames	Disabled
1 - 16	1	All Frames	Disabled
1 - 17	1	All Frames	Disabled
1 - 18	1	All Frames	Disabled
1 - 19	1	All Frames	Disabled
1 - 20	1	All Frames	Disabled
1 - 21	1	All Frames	Disabled
1 - 22	1	All Frames	Disabled
1 - 23	1	All Frames	Disabled
1 - 24	1	All Frames	Disabled

The page shows the units of the switch, and the ports that are assigned to the currently selected VLAN. For information about VLANs, see Chapter 4 and Chapter 6. Click on **VLAN Configuration** at the top of the

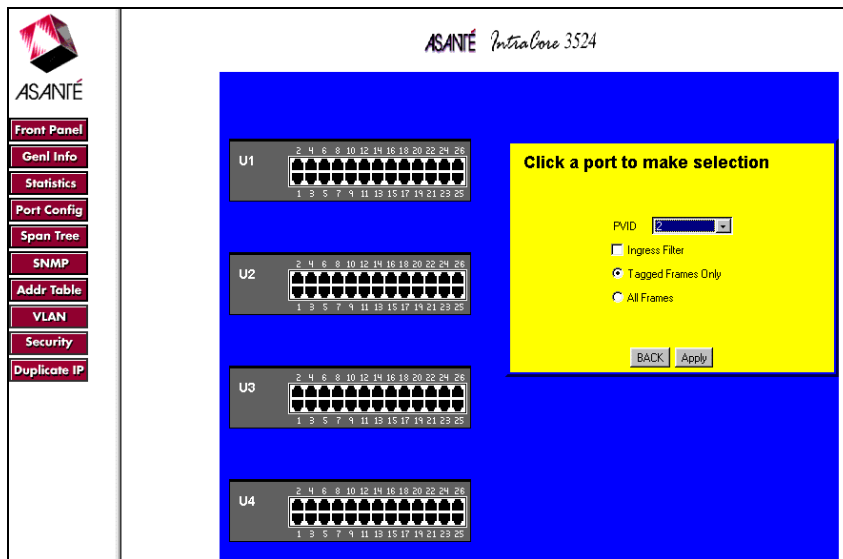
port attributes page to access the VLAN Groups page. In the VLAN Groups page, there is a panel that shows the VID of each VLAN on the current switch.



To configure a VLAN, select the VID of the desired VLAN. To configure the ports for the selected VLAN, click the **Ports** button.

5.8.1 Port Configuration

Clicking the Ports button in the VLAN Groups page opens the VLAN Port Selection page, as shown below.

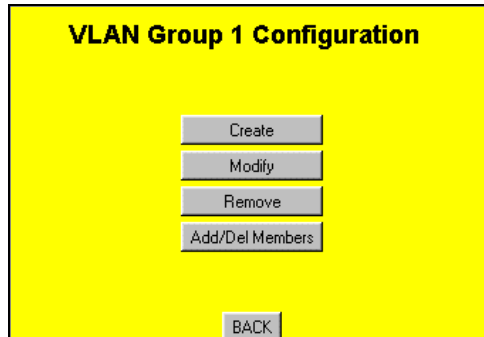


The page shows the ports of the unit. There is also a panel indicating the current Port VLAN ID and its settings.

To see and modify the settings for a port, click on the connector for it in the unit simulation. Then make the appropriate settings in the right-hand panel of the page.

5.8.2 VLAN Configuration

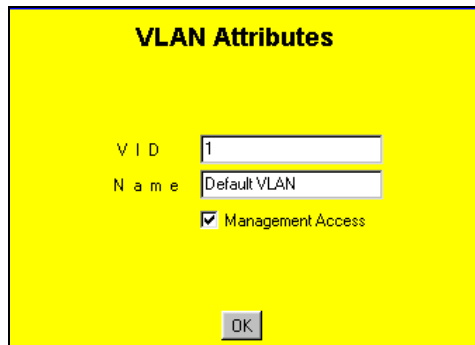
To configure a VLAN, first select a VID in the VLAN Groups page, and then click the **VLAN** button. This opens the VLAN Group Configuration options page, shown below.



The image shows a dialog box titled "VLAN Group 1 Configuration" with a yellow background. It contains four buttons stacked vertically: "Create", "Modify", "Remove", and "Add/Del Members". At the bottom center, there is a "BACK" button.

Creating or Modifying a VLAN

To create or modify the basic attributes of a VLAN group, click the **Create or Modify** button in the VLAN Group Configuration dialog box. The VLAN Attributes dialog box is displayed, as shown below.



The image shows a dialog box titled "VLAN Attributes" with a yellow background. It contains two text input fields: "V I D" with the value "1" and "N a m e" with the value "Default VLAN". Below these fields is a checked checkbox labeled "Management Access". At the bottom center, there is an "OK" button.

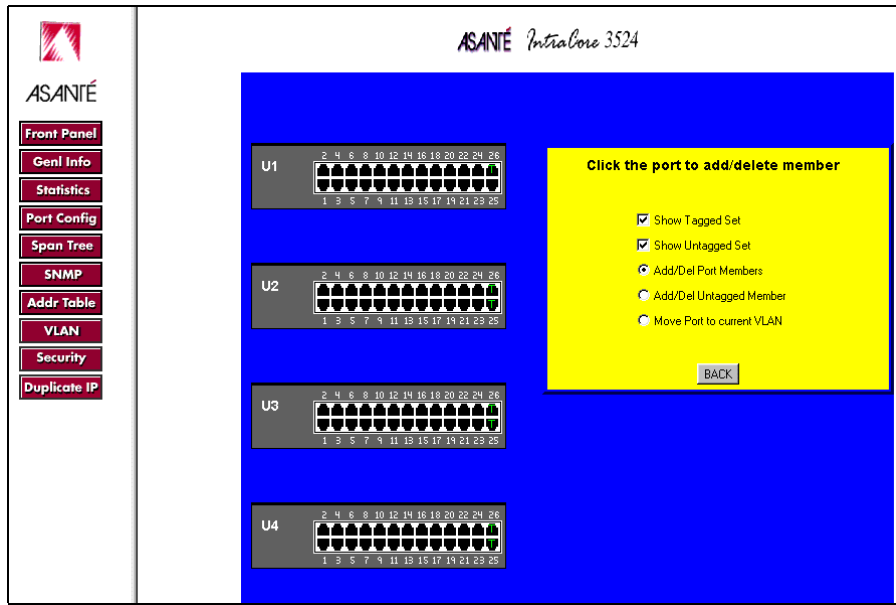
Enter or change the basic attributes, then click **OK**.

Removing a VLAN

To remove a VLAN from the current switch, click **Remove** in the VLAN Group Configuration dialog box. This removes the VLAN you selected at the time you clicked VLAN in the VLAN Groups dialog page. You will see a dialog box asking you to confirm your decision to remove the VLAN.

Adding and Deleting Port Members

To add ports to or delete ports from the current VLAN, click the **Add/Del Members** button in the VLAN Group Configuration dialog box. This displays the Add/Delete Port Member dialog box, as shown below:



In the right-hand panel you can select the option to show the ports that are in the untagged set or the tagged set of the VLAN. These ports appear in the unit simulation on the left. Darkened ports are not members. Ports with a green X are untagged members. Ports with a green dot are tagged members.

To modify the port members:

1. Select the action you want to perform in the right-hand panel; Add/Delete Port Members, Add/Delete Untagged Members, or Move Port to Current VLAN.
2. Click on a port to change its state:
 - For Add/Delete Port Members, clicking on a darkened port adds it to the VLAN, while clicking on a VLAN member deletes it. The status of the port on any other VLAN remains unchanged.
 - For Add/Delete Untagged Members, clicking on a darkened port adds it to the untagged set, and clicking on a green dot changes it to an untagged port. Clicking on an untagged port changes it to a tagged port. The status of the port on any other VLAN remains unchanged.
 - Move Port to Current VLAN is the same as Add/Delete Port Members, except moving the port also removes the port from any other VLAN of which it is a member.

5.9 Security Button

This button opens the Security page, which provides a summary of the security of each port on each switch, as shown below.

Unit-Port	Type	Action	Trusted MAC Addr
1-1	NONE	NONE	NONE
1-2	NONE	NONE	NONE
1-3	NONE	NONE	NONE
1-4	NONE	NONE	NONE
1-5	NONE	NONE	NONE
1-6	NONE	NONE	NONE
1-7	NONE	NONE	NONE
1-8	NONE	NONE	NONE
1-9	NONE	NONE	NONE
1-10	NONE	NONE	NONE
1-11	NONE	NONE	NONE
1-12	NONE	NONE	NONE
1-13	NONE	NONE	NONE
1-14	NONE	NONE	NONE
1-15	NONE	NONE	NONE
1-16	NONE	NONE	NONE
1-17	NONE	NONE	NONE
1-18	NONE	NONE	NONE
1-19	NONE	NONE	NONE
1-20	NONE	NONE	NONE
1-21	NONE	NONE	NONE
1-22	NONE	NONE	NONE
1-23	NONE	NONE	NONE
1-24	NONE	NONE	NONE
1-25	NONE	NONE	NONE
1-26	NONE	NONE	NONE
2-1	NONE	NONE	NONE
2-2	NONE	NONE	NONE

The configuration pages for individual ports are accessed by clicking on the associated blue number in the Unit-Port column.

Unit: 1 Port: 23 Unit 1 Port 1 GO Auto Manual Refresh

Port Configuration

Link Status: Down10/Half
 Media Type: TX
 Port Status:
 Auto-Negotiation:
 Flow Control:
 Port Default Priority:

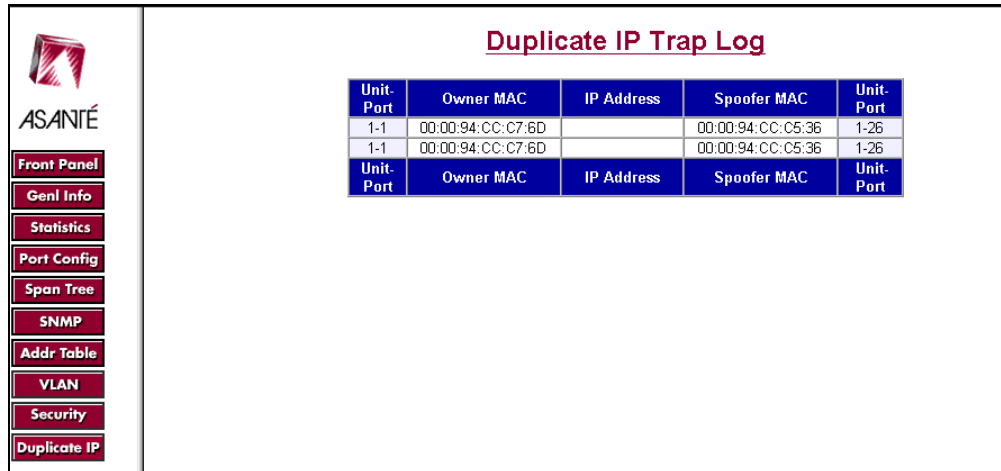
Security :
 Level:

Port Statistics

Rx Counters: **Errors:**
 Total Frames: 0 Undersized Pkts: 0
 Total Bytes: 0 Oversized Pkts: 0
 Dropped Frames: 0 CRC/Align: 0
 Fragments: 0
Tx Counters: FCS: 0
 Total Frames: 0 Late Events: 0
 Total Bytes: 0 Total: 0
 Unicast: 0
 Non-unicast: 0
Frame Counters:
 Multicast: 0
 Broadcast: 0
 64-Byte: 0

5.10 Duplicate IP Button

The Duplicate IP button lights up if a Duplicate IP number has been detected on the system. Clicking the button opens the Duplicate IP Trap Log page, which, if the trap is enabled, displays a record of duplicate IP Addresses detected. The Log shows the MAC address of the device that is the original or rightful owner of the IP address, and the MAC address of the spoofer device that is using a copy of the IP address.



Unit-Port	Owner MAC	IP Address	Spoofed MAC	Unit-Port
1-1	00:00:94:CC:C7:6D		00:00:94:CC:C5:36	1-26
1-1	00:00:94:CC:C7:6D		00:00:94:CC:C5:36	1-26
Unit-Port	Owner MAC	IP Address	Spoofed MAC	Unit-Port

For more information on enabling the Duplicate IP trap, see “Enabling and Disabling Duplicated IP Trap” in Chapter 4.

Chapter 6. SNMP Management

The switch can be managed using a Simple Network Management Protocol (SNMP) compatible management station running platforms such as HP OpenView or MG Soft's MIB Browser.

6.1 SNMP Management Operations

A network management application is concerned with performance statistics gathered by the devices on the managed network, in reading and changing current configuration information, and in receiving alerts of unusual events.

The information is stored in a database, which is described by Management Information Base documents (MIBs). Most of these MIBs are available from the Internet Engineering Task Force (IETF), the global body that defines Internet standards. Many managed devices also include data that is described by a proprietary MIB.

A managed device incorporates software called an agent. The agent is able to read the information in the device, to update configuration information and to communicate with a management application using a standard protocol (SNMP)

The switch supports the following Management Information Bases (MIBs):

1. MIB II: Management Information Base for Network Management of TCP/IP based Internets (RFC 1213).
2. Ethernet Interface MIB: Definitions of Managed Objects for the Ethernet-like Interface Types (RFC 1643).
3. Bridge MIB: Definitions of Managed Objects for Bridges (RFC 1493).
4. RMON MIB: Remote Network Monitoring Management Information Base (RFC 1757). Four groups are supported:
 - The Ethernet Statistics Group
 - The Ethernet History Group
 - The Alarm Group
 - The Event Group
5. ASANTE-SWITCH-MIB: Enterprise MIB for management of features specific to the 3524. The MIB file is available at Asanté's website, <http://www.asante.com>.

6.2 The SNMP Protocol

The SNMP protocol is an industry standard protocol communicating over the User Datagram Protocol, exchanging Protocol Data Units (PDUs).

There are five different types of SNMP PDUs:

1. Get Request – The manager requests the value of a variable from the agent.
2. Get-Next Request – The manager requests the value of the next variable in order from the agent. This is often used to walk a MIB and retrieve many values one after the other.
3. Set Request – The manager tells the agent to change the value of a given variable.
4. Get Response – The agent returns the data for any of the above requests and confirms any changes of value.
5. Trap – The agent sends data to the manager on its own initiative in response to predefined events (i.e. hardware failure).

Note: The description above is accurate for version 1 of the SNMP protocol. Versions 2 and 3 add other types of PDUs.

6.3 Community Name and Security

SNMP v.1 was not designed to be a secure protocol. There is no true password, although the string known as a community string does serve some of the same purposes.

SNMP-aware devices, such as this switch, often ship with well-known community strings. For this reason, it is important that you change the default community strings before putting the switch on a network. The 3500 series switches improve on normal security by requiring the management station to appear in the SNMP host table before the agent will recognize the manager.

6.4 The MIB Tree

When the SNMP was designed, a formal structure for creating new management objects was created. A tree represents the structure: nodes in the tree are represented as strings of numbers separated by periods. There are three components of the tree:

1. The unnamed root of the tree contains a set of characters common to all MIB objects located beneath the root. Objects beneath unnamed are said to be in that root's domain.
2. A sub-tree contains a subset of the information available at the root. A sub-tree may also serve as a root and have sub-trees of its own.
3. A leaf is a sub-tree with no additional sub-trees in its domain. A leaf represents a single MIB object whose characteristics are unique from any other MIB object.

The group or organization that owns the sub-tree path assigns sub-tree numbers. The object names in the path are unique all the way to the end of the path.

6.4.1 Name Space Path

The name space path is used by the SNMP protocol to define the piece of data that the manager wants.

There are three main name space paths:

1. ISO (International Standards Organization): All sub-tree leaves are under the ISO control.
2. CCITT (Consultative Committee on International Telephony and Telegraphy): the group that sets the standards for the interconnection of telephone equipment).
3. ISO-CCITT: Joint ISO and CCITT.

Each MIB object can be located by following a path from unnamed, through the sub-trees, to the leaf, following the string of numbers. The part of the tree that is of interest to SNMP starts with the **internet** node:

iso.org.dod.internet or 1.3.6.1

Interesting nodes under that one include:

- internet.mgmt.mib-2 or 1.3.6.1.2.1
- internet.private.enterprises or 1.3.6.1.4.1

Most of the industry-standard management objects appear under mib-2, while objects defined by individual manufacturers appear under enterprises. Asanté Technologies, Inc. has 298 as its enterprise number (1.3.6.1.4.1.298). At the time of this writing, there are nearly 10,000 enterprise numbers assigned. You can get a list of enterprise numbers from <ftp://ftp.isi.edu/in-notes/iana/assignments/enterprise-numbers/>.

6.4.2 MIB Groups Supported

The following MIB-II groups are supported:

- The System Group -- General information about the managed system, such as contact information and system name
- The Interfaces Group -- Information about each interface in the managed unit, and statistics for that interface
- The Address Translation Group -- This group is deprecated, and should not be used

- The IP group -- This group contains counters for Internet Protocol Traffic. It contains as a sub-group the IP Net-to-Media table, which tracks MAC-to-IP address mappings
- The ICMP group -- keeps statistics for Internet Control Protocol datagrams
- The TCP group -- keeps statistics for the Transmission Control Protocol, including a table of established connections
- The UDP group -- keeps statistics for the User Datagram Protocol
- The EGP group -- keeps statistics on the Exterior Gateway Protocol
- The SNMP group -- keeps statistics on the Simple Network Management Protocol

The following Bridge MIBs are supported:

- The dot1dBase group -- This group contains the objects that apply to all types of bridges
- The dot1dStp group -- This group contains objects to manage the Spanning Tree Protocol
- The dot1dTp group -- This group contains objects that describe the bridge's function as a transparent bridge
- The dot1dStatic group -- This group allows the creation and management of static entries in the bridge's forwarding table

The switch supports the Ethernet-like MIB:

- The Ethernet-like Statistics group -- This group records statistics relevant to Ethernet's CSMA/CD access method

The following RMON MIBs are supported:

- The Ethernet Statistics group -- this group records statistics for each Ethernet interface on the switch, including records of frame sizes received
- The Ethernet History group -- this group collects statistics for each interface in buckets covering a user-selectable time period
- The Alarm group -- the alarm group allows you to set a threshold on a counter, and to configure a response if the threshold is crossed in either a rising or falling direction
- The Event group -- the event group allows you to configure a response when an alarm is triggered. Responses include a trap or log entry

For more information on SNMP, refer to your SNMP software user's manual.

Chapter 7. Switching Concepts

A bridge is a hardware device used to connect multiple networks into one big network. However, when a bridge receives a broadcast from one interface, it will forward the frame to all interfaces and flood the wire, easily overwhelming the network.

The traditional solution to the problem of broadcast flooding is to use a router. The disadvantages of a router include higher cost (the initial purchase price and higher maintenance costs) and slower rate of processing incoming data, leading to increased latency with decreased network performance. A switch (basically a complex bridge) can process data at a faster rate than a router, and can limit unnecessary flooded traffic by learning the addresses of the stations on the system. A switch can be used to create broadcast domains (via VLANs), and can be employed as an alternate solution to using routers to contain broadcast flooding.

While a bridge connects network segments via interfaces, a switch connects segments via its ports, like a hub. But, unlike a hub, the ports of a switch can be configured to belong to a specific network, thereby separating traffic, providing security and reducing overall network congestion.

The following sections provide brief explanations of some of the concepts related to switching. If more information is required, please refer to networking textbooks, online resources (i.e. www.oreillynet.com) or your MIS manager.

7.1 VLANs

A virtual local area network, or VLAN, is a logical grouping that allows stations to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of a network. A VLAN localizes flooded traffic to parts of LAN segments, rather than to an entire LAN, offering a simple solution to network performance, security and bandwidth utilization.

7.1.1 Port-Based VLANs

Port-based VLANs are the simplest of many VLAN approaches (others are based on MAC addresses, protocol type, and higher layers that are not currently supported by the IEEE 802.1Q standard) that solve the problem of unnecessary flooding. The switch currently supports port-based VLANs in compliance with the IEEE standard.

A port-based VLAN allows the administrator to assign individual ports to a VLAN. Any broadcast (sent to every user in the network) or multicast (sent to a pre-specified group of users) traffic received on a port in a VLAN are limited by the VLAN boundaries so that only workstations whose ports are members of the same VLAN see those frames.

7.1.2 VLAN ID and Tagged Frames

The IntraCore 3524 supports 64 manually configurable VLANs. Each VLAN is identified by a 12-bit (1-4095) VLAN ID (VID). No two VLANs may have the same VID if they reside on the same switch. However, by assigning the same VID to VLANs on multiple switches, the broadcast domain may be extended over a large network. The switch is shipped with a single default VLAN, with a VID of 0.

In a network with only one switch, the switch itself keeps track of which ports belong to which VLAN. In a network with multiple switches, the information about which VLAN an Ethernet frame belongs to must be sent along with the frame. This is done by inserting a tag field, as defined in IEEE 802.1Q, in the frame. The tag includes a VLAN ID field that matches the VID assigned to a VLAN on the switch. The switch will then assign the frame to the VLAN represented by the tag field.

A port map is used to specify which ports are members of each VLAN. Each VLAN has a set of untagged ports that specifies which port members of the VLAN transmit only untagged frames. The untagged set can be a subset of the port map, or it can be the same as the port map. If a port is in the VLAN port map and not in the VLAN untagged set, that port transmits tagged frames only. The switch includes all ports in its untagged set by default.

7.1.3 Port VLAN ID

To allow untagged packets to participate in a VLAN, a Port VLAN ID (PVID) must be assigned in the relevant port(s).

Each port on the switch has a default PVID of 1 (the default VLAN) and will receive both tagged and untagged frames. You may configure the PVID of any desired port (the range is 1 to 4094). For ports that have been configured to receive only tagged frames, the PVID is meaningless. If a port is configured to receive only tagged frames, then any untagged frame received will be dropped. Tagged frames that are received will be forwarded to the VLAN represented by the VID in the tag header of the frame.

See *Appendix B. VLAN Description and Examples* for more information, or visit <http://www.ieee.org>.

7.2 Spanning Tree Protocol

The Spanning Tree Protocol (STP) is part of the IEEE 802.1D standard. It provides for a redundant network without the redundant traffic through closed paths. For example, in a network without spanning tree protocol, the same message will be broadcast through multiple paths, which may start an unending packet-passing cycle. This in turn causes a great amount of extra network traffic, leading to network downtime. The STP reduces a network like this, with multiple, redundant connections, to one in which all points are connected, but where there is only one path between any two points (the connections span the entire network, and the paths are branched, like a tree).

7.2.1 How It Works

All of the bridges (a switch is a complex bridge) on the network communicate with each other using special packets of data called Bridge Protocol Data Units (BPDUs). The information exchanged in the BPDUs allows the bridges on the network to do the following:

- Elect a single bridge to be the root bridge
- Calculate the shortest path from each bridge to the root bridge
- Select a designated bridge on each segment, which lies closest to the root and forwards all traffic to it
- Select a port on each bridge to forward traffic to the root
- Select the ports on each bridge that forward traffic, and place the redundant ports in blocking states

7.2.2 Spanning Tree Parameters

The operation of the spanning tree algorithm is governed by several parameters. You should attempt to set these parameters only if you have experience with the 802.1D specification. To set the parameters listed below, access the *Spanning Tree/Bridge Settings* screen (console or telnet), or the *Spanning Tree/Bridge Settings* page (in the web interface).

Bridge Priority

Setting the Bridge Priority to a low value will increase the likelihood that the current bridge will become the root bridge. If the current bridge is located physically near the center of your network, you may wish to decrease the Bridge Priority from its default value of 32768 to make it become the root bridge. If the current bridge is near the edge of your network, it is best to leave the value of the Bridge Priority at its default setting.

Hello Time

This is the time period between BPDUs transmitted by each bridge. The default setting is 2 seconds.

Maximum Age

Each bridge should receive regular configuration BPDUs from the direction of the root bridge. If the maximum age timer expires before the bridge receives another BPDU, it assumes that a change in the topology has occurred, and it begins recalculating the spanning tree. The default setting for Maximum Age is 20 seconds.

Forward Delay

After a recalculation of the spanning tree, the Forward Delay parameter regulates the delay before each port begins transmitting traffic. If a port begins forwarding traffic too soon (before a new root bridge has been selected), the network can be adversely affected. The default value for Forward Delay is 15 seconds.

Note: The above parameters (Hello Time, Maximum Age and Forward Delay) are constrained by the following formula:

$$(\text{Hello Time} + 1) \leq \text{Maximum Age} \leq 2 \times (\text{Forward Delay} - 1)$$

In general, reducing the values of these timers will make the spanning tree react faster when the topology changes, but may cause temporary loops as the tree stabilizes in its new configuration. Increasing the values of these timers will make the tree react more slowly to changes in topology, but will make an unintended reconfiguration less likely. All of the bridges on the network will use the values set by the root bridge. It is only necessary to reconfigure that bridge if you wish to change the parameters.

7.2.3 Spanning Tree Port Configuration

To set the Port Priority and Port Path Cost values for STP, access the *Spanning Tree/Port Settings* screen (console or telnet), or the *Spanning Tree/Port Settings* page (in the web interface).

Port Priority

The port priority is a spanning tree parameter that ranks each port, so that if two or more ports have the same path cost, the STP selects the path with the highest priority (the lowest numerical value). By changing the priority of a port, you can make it more, or less, likely to become the root port. The default value is 128, and the value range is 0 – 255.

Port Path Cost

Port path cost is the spanning tree parameter that assigns a cost factor to each port. The lower the assigned port path cost is, the more likely that port will be accessed. The default port path cost for a 10 Mbps or 100 Mbps port is the result to the equation:

$$\text{Path cost} = 1000 / \text{LAN speed (in Mbps)}$$

Therefore, for 10 Mbps ports, the default port path cost is 100. For 100Mbps ports, it is 10. To allow for faster networks, the port path cost for a 1000Mbps port is set by the standard at 4.

7.3 Full Duplex, Flow Control and Auto-negotiation

These switching concepts are all related to maintaining a high rate of data transmission necessary for an efficient network.

7.3.1 Full Duplex

Traditionally, Ethernet has operated in half duplex mode, meaning that a node or workstation could either send or receive data, but not both simultaneously. Now, with the use of structured wiring using Unshielded Twisted Pair cabling, and switched Ethernet, a workstation may operate in full duplex mode, sending and receiving data at the same time. The ability to use full duplex mode can potentially double the basic capacity of the channel, so that a Fast Ethernet connection may carry up to 200Mbps.

In order to use full duplex, an Ethernet station must have separate channels to send and receive data. UTP cabling provides this, whereas the older coaxial Ethernet did not. The station must also have a direct connection to a switched port. A station connected to only a repeater cannot operate in full duplex mode. Also, it is critical that both ends of the Ethernet link “agree” on whether the link will operate in full or half duplex. See 8.3.3 *Auto-negotiation* below for more details.

7.3.2 Flow Control

With a link operating at a high data rate, a switch may experience occasional limitations in the buffer space used to store Ethernet frames before forwarding them. In this situation, if the sending station continues to send frames, the switch will have no option but to discard the frames. This may quickly lead to unacceptable delays in upper-level protocols.

In order to avoid unnecessarily dropping frames, a switch may implement Flow Control. Flow control is a feature that allows the switch to recognize when the buffer space is limited, and to send an Ethernet PAUSE frame to its link partner to cease transmission for a specified period. As with a full duplex link, both ends of the link must understand flow control for the mechanism to operate properly.

7.3.3 Auto-Negotiation

As discussed above, you need to make sure that both ends of a link agree about the duplex and flow control settings to be used (as well as the speed of the connection). In even a mid-sized network, making sure that all the links agree on all these parameters would be too big a job if the network manager had to configure every connection manually.

To make configuration as automatic as possible, the IEEE has defined standards so that most connections can be automatically configured by the hardware, without manual intervention. Devices can agree on the speed, duplex mode and flow control settings for each individual connection. The possible links states are ranked:

- 1000Mbps/Full Duplex
- 1000Mbps/Half Duplex (never used)
- 100Mbps/Full Duplex
- 100Mbps/Half Duplex
- 10Mbps/Full Duplex
- 10Mbps/Half Duplex

With auto-negotiation, the link partners will configure the link to operate at the highest speed and duplex state that both support.

Auto-negotiation is supported on IntraCore switches on all UTP ports.

Note: If an Ethernet device that is capable of auto-negotiation is connected to a port that has auto-negotiation turned off, the auto-negotiating device will default to half duplex mode. If the port that is not using auto-negotiation is set to full duplex, the link will have a duplex mismatch, and will so slow that it may be unusable. If you configure an Ethernet port to operate in full duplex mode, you must also configure the link partner to operate in full duplex. It is almost always better to let auto-negotiation take care of this for you.

Appendix A. Troubleshooting

In the unlikely event your switch does not operate properly, follow the troubleshooting tips below. If you still need help, contact Asanté's technical support.

Problem	Possible Solutions
Power LED is not lit.	LED will turn off during system initialization. Check your power connection. Plug the power cord into another known working AC outlet.
The 10/100 port Link LEDs are not lit.	Check your cable connections. Make sure the connectors are seated correctly in each port, and that the correct type of cable is used in each port. See <i>Chapter 2.5 Connecting to the Network</i> for more information.
The GBIC Link LED is not lit.	Check your GBIC connector. Make sure the cables are inserted correctly, with the Transmit (Tx) connector on one side of the link connected to the Receive (Rx) connector on the other side of the link.
Cannot establish communication to another device (switch, router, workstation, etc.).	<ul style="list-style-type: none">• Make sure the Link LED for the port in use is on. Make sure you are using the correct cable type. See <i>Chapter 2.5 Connecting to the Network</i> for more information on cabling procedures• Make sure the IP address, subnet mask, and VLAN membership of the switch is correct• Make sure the switch port and the device both are in the same VLAN• Try to connect to a different port
Cannot auto-negotiate the port speed.	Make sure that auto-negotiation is supported and enabled on both sides of the link (in both devices).
Cannot successfully form a stack	<ul style="list-style-type: none">• Check that all the units have the stacking feature available (stacking is offered on firmware version 1.1 or later).• Check that all the units have the stacking feature enabled.• Check that the hardware modules are inserted correctly. They should be flush against the unit.• Check the Link LEDs on the units. Check your cables to ensure they are working.

Appendix B. Features and Specifications

The sections below list the features and product specifications for the IntraCore 3500 Series Gigabit Ethernet switches.

B.1 Features

The following is a summary of the management features of 3500 Series Gigabit Ethernet Switch:

Graphical User Interface:	HTML browser-based with password protection for local and remote management
Command Line Interface:	Menu-driven telnet or in-band (via front panel console port)
Front Panel:	Graphical representation of unit with real-time network status
General Information:	Software version, dual firmware banks. Admin, system and bootstrap info. Switch address and system clock
Statistics:	User-configurable graph types (bar chart, line chart, table) and counters (since up, rate, since reset) for RX/TX/Error for each port and unit. Table view also shows current, peak average and total packets for each port
Port Configuration:	State (forwarding, blocking), status (enabled, disabled), link status (up, down) and mode (speed, duplex), auto negotiation, flow control, priority and security. Detailed statistics include TX counters (total frames, total bytes, dropped frames), RX counters (total frames, total bytes, unicast, non-unicast), frame counters (multicast, broadcast, by packet sizes), collisions and errors (undersized, oversized, CRC/alignment, fragments, FCS, late events, total)
Spanning Tree:	Displays bridge ID, designated root, root port, root port cost, hello time, maximum age and forward delay. Ports are individually configurable for STP parameters (priority, path cost)
SNMP:	Separate read and write communities, and trap authentication. Four configurable trap receivers (IP address and community)
Address Table:	Per-port counts for Mac and IP addresses. Integrated utilities to sort or search for specific IP/MAC address. Address table shows unit, port, entry (dynamic, static or multiple), IP address, MAC address and VID
VLAN:	Configurable PVID, frame type and ingress filtering
RMON:	Embedded remote monitoring supports four groups (history, statistics, alarms and events)
Security:	Configurable per-port security with programmable action (e.g., new node detection trap) and trusted MAC address
Supported OS:	Windows 95/98/Me/NT/2000/XP, Mac OS 9/X, and Linux
Other:	Integrated utility to detect duplicate IP addresses (port, owner MAC address, IP address and spoofer MAC address)

B.2 Specifications

Connectors:	IC3524 Models: 24 Fast Ethernet with Auto-Uplink™ (100BaseTX, 10BaseT): RJ-45 Console: Serial (RS-232): DB9 IC3548-2GT: 48 Fast Ethernet with Auto-Uplink (100BaseTX, 10BaseT): RJ-45 2 fiber GBIC connectors 2 copper 10/100/1000 RJ-45
Expansion (IC3524 only):	2 front-mounted slots for Type IC35 modules (Gigabit or Fast Ethernet, copper or fiber) Optional Fast Ethernet (100BaseFX): SC Optional Gigabit Ethernet with Auto-Uplink (1000BaseT, 100BaseTX, 10BaseT): RJ-45 Optional Gigabit Ethernet (1000BaseSX): SC

Status Indicators: IC3524 Models: Separate link-activity, speed (10/100/Gigabit) and duplex (full or half) LEDs for each port; system power
IC3548-2GT: Link/activity and full-duplex/half-duplex display modes for each ports' LED status light (10/100Mbps only); Separate link/activity and full-duplex/half-duplex LEDs for each Gigabit port; Four separate LEDs (Link, Full-duplex, Activity and Collision) for the 10Mbps port (back panel)

Physical Characteristics

Dimensions: 17.25 x 10.0 x 1.7 inches (438 x 254 x 43 mm)
Mounting: Install into a standard 19-inch rack (1 RU height) or placed on a desktop; rackmount kit and rubber feet included
Capacity (IC3524 only): Stack or cluster up to 8 units (192 ports) using any Gigabit port/module (available on IC3524 models with firmware version 1.1 and higher)
IC35 Modules: 2.19 x 3.63 x 1.19 (56 x 92 x 30 mm), 0.13 lbs (0.06 Kg)

Environmental Range:

Operating Temperature: 32° to 104° F (0° to 40° C)
Relative Humidity: 10% to 90% non-condensing
Power: Auto-switching, 110-240 VAC, 50/60 Hz; grounded IEC cord

Standards Compliance

IEEE: IEEE 802.1D spanning tree and bridge filters
IEEE 802.1p prioritization (class of service)
IEEE 802.1Q virtual LAN (VLAN)
IEEE 802.3ad link aggregation
IEEE 802.3x full duplex and flow control
IEEE 802.3z 1000BaseSX over 50 micron multi-mode fiber; maximum distance 1,804 feet (550 meters)
IEEE 802.3ab 1000BaseT over Category 5 UTP (4 pairs); maximum distance 328 feet (100 meters)
IEEE 802.3u 100BaseTX over Category 5 UTP (2 pairs); maximum distance 328 feet (100 meters)
IEEE 802.3 10BaseT over Category 3 UTP (2 pairs); maximum distance 328 feet (100 meters)

IETF: RFC 1155 SMI
RFC 1757 RMON
RFC 1157 SNMP
RFC 1493 Bridge MIB
RFC 1213 MIB II
Asanté Private MIB

Safety: UL 1950, CUL, TUV/GS (IC3524)
Emissions: FCC Class A, CE

Technical Support and Warranty

IntraCare™: Free technical support and advanced warranty support for 3 years. Includes free telephone support, 24-hour support via web and ftp, complete product warranty with 2nd business day (within the United States) advanced replacement and software maintenance agreement.
AsantéCare™: Optional extended technical support and product warranty for 2 additional years.

See Appendix C for Asanté's detailed warranty statement.

Appendix C. FCC Compliance and Warranty Statements

FCC Compliance Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his or her own expense.

Important Safety Instructions

Caution: Do not use a RJ-11 (telephone) cable to connect your network equipment.

1. Read all of these instructions.
2. Save these instructions for later use.
3. Follow all warnings and instructions marked on the product.
4. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
5. Do not use this product near water.
6. Do not place this product on an unstable cart or stand. The product may fall, causing serious damage to the product.
7. The air vent should never be blocked (i.e. by placing the product on a bed, sofa, rug, etc). This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
8. This product should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
9. This product is equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug will only fit into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your outlet. Do not defeat the purpose of the grounding type plug.
10. Do not allow anything to rest on the power cord. Do not place this product where persons will walk on the cord.
11. If an extension cord is used with this product, make sure that the total ampere ratings on the products into the extension cord do not exceed the extension cord ampere rating. Also make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
12. Never push objects of any kind into this product through air ventilation slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock. Never spill liquid of any kind on the product.
13. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to service personnel.

IntraCare Warranty Statement

Products: IntraCore 3500 Series switches: IC3524, IC3524-2G, IC3524-2T, IC3548-2GT
IntraCore 3524 modules: IC35-1000T, IC35-1000SX, IC35-GBIC, IC35-100MMFX, IC35-100SMFX

Duration: 3 years
Advanced Warranty United States: 2nd Business Day
Replacement: Other Countries: See your local distributor or reseller.

1. Asanté Technologies warrants to the original end user purchaser that covered IntraCore™ hardware and accessories against defects in materials and workmanship for the period specified above. If Asanté receives notice of such defects during the warranty period, Asanté will, at its option, either repair or replace products that prove to be defective. Replacement products may be either new or like-new.

2. Asanté warrants that Asanté software will not fail to execute its programming instructions, for the period specified above, due to defects in material and workmanship when properly installed and used. If Asanté receives notice of such defects during the warranty period, Asanté will replace software media that does not execute its programming instructions due to such defects.

3. Asanté does not warrant that the operation of Asanté products will be uninterrupted or error free. If Asanté is unable, within a reasonable time, to repair or replace any product to a condition as warranted, customer would be entitled to a refund of the pro-rated purchase price upon prompt return of the product.

4. Asanté products may contain remanufactured parts equivalent to new in performance.

5. The warranty period begins on the date of delivery or on the date of installation if installed by Asanté.

6. Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts or supplies not supplied by Asanté, (c) unauthorized modification or misuse, (d) operation outside of the published environmental specifications for the product, or (e) improper site preparation or maintenance. This warranty expressly excludes problems arising from compatibility with other vendors' products, or future compatibility due to third party software or driver updates.

7. TO THE EXTENT ALLOWED BY LOCAL LAW, THE ABOVE WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND ASANTÉ SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

8. Asanté will be liable for damage to tangible property per incident up to the greater of \$10,000 or the actual amount paid for the product that is the subject of the claim, and for damages for bodily injury or death, to the extent that all such damages are determined by a court of competent jurisdiction to have been directly caused by a defective Asanté product.

9. TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED ABOVE, IN NO EVENT WILL ASANTÉ OR ITS SUPPLIERS BE LIABLE FOR LOSS OF DATA OR FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL INCLUDING LOST PROFIT OR DATA), OR OTHER DAMAGE, WHETHER BASED IN CONTRACT, TORT, OR OTHERWISE.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages or imitations on how long an implied warranty lasts, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may have other rights, which vary from jurisdiction to jurisdiction.

Appendix D. Console Port Pin Outs

The console port is used to connect with a terminal using a serial modem RS-232C cable (available from Radio Shack's website, catalog # 26-117). The setting is 9600-N81. The table below lists the pin outs.

Pin Number	Signal	Name
1	CD	Carrier Detect
2	RD	Receive Data
3	TD	Transmit Data
4	DTR	Data Terminal Ready
5	SG	Signal Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CD	Carrier Detect
9	RI	Ring Indicator

Appendix E. Online Warranty Registration

Before calling Asanté Technical Support, please register your switch online at www.asante.com/support/registration.html. By doing so, you'll be entitled to special offers, up-to-date information and important product bulletins.

Appendix F. BootP Configuration

The switch is shipped with BootP support. If your network contains a BootP server configured with available, valid IP addresses, BootP allows the switch to be configured automatically with an IP address when it is connected to the network and is powered on.

Important! BootP configuration works only if switch does not have an IP address assigned to it.

Use the following procedure to set up BootP:

1. Make sure your network has a BootP server configured with a valid IP address entry for the switch.
2. When the switch is connected to the network and is powered on, it automatically transmits a BootP request across the network (up to 10 times) until it receives a valid IP address from the BootP server.
3. After an IP address is received, the switch can be managed via in-band access. For more information, see Chapters 3 and 4.

To verify that a valid IP address was received, try to 'ping' the IntraCore 3524. If you can access the unit, it is properly configured with an IP address.

Bootstrap Configuration

The Bootstrap Configuration Menu displays (and allows you to change) the bootstrap parameters used for loading the software for the switch at startup, and for downloading a new version of software when one is issued.

To access the Bootstrap Configuration Menu, type **b** in the Configuration Menu. If the Load Mode is set to Local, a screen similar to **Figure 3-6** appears.

When switch is powered on, it loads its software via one of two methods: locally (via its internal flash memory, which is the default setting) or remotely over the network.

Important! The default Load Mode setting for the switch is Local.

Image Banks

The switch has two banks to store its runtime software. The banks are referred to as bank 1 and bank 2.

Either of these banks may be the Boot Bank, which is the bank from which the runtime code will be loaded the next time the switch is booted.

When downloading new runtime image codes, you may specify either of the two banks as the Destination Bank in which the new code will be loaded.

Loading Software Locally

The switch will always boot locally unless you set it to boot load remotely (see "Loading Software Remotely" below). It would then download the new image code and reset to load locally. To specify the Boot Bank that the switch will use when it boots locally, use the following procedure:

1. Open the Bootstrap Configuration Menu by typing **b** in the Configuration Menu.
2. Type **a** in the Bootstrap Configuration Menu if you need to toggle the Boot Bank setting for the next boot. Typically, you will want to set the boot bank to be the one on which the latest version of the Image resides.

The switch is now set to load software locally from its flash memory. This occurs whenever the unit is powered on or reset.

Loading Software Remotely

To set the switch to download its software over the network from a remote server, use the following procedure:

1. Open the Local Bootstrap Configuration Menu by typing **b** in Configuration Menu.
2. Open the Remote Bootstrap Configuration Menu by typing **r** in the Local Bootstrap Configuration Menu. The menu appears, as shown below.

```
Asanté's IntraCore 3524 Gigabit Ethernet Switch Bootstrap Configuration Menu

Bank 1 Image Version/Date: 1.00G/Sep 28 2001 13:18:18
Bank 2 Image Version/Date: 1.00I/Oct 08 2001 09:36:50 (Running)

Load Mode:      Remote
Boot Mode:      TFTP only
Boot Server IP: xxx.xxx.xxx.xxx
Boot File Name: c:\3524100g.ima
Retry Count:    5
Boot Bank:      2

<Cmd>      <Description>
b          Set Boot Mode to BOOTP-TFTP
t          Set Boot Mode to TFTP only
l          Set Load Mode to LOCAL
s          Set Boot Server IP Address
f          Set Boot File Name
c          Set Remote Boot Retry Count
a          Toggle Boot Bank
o          Commence Bootstrap Sequence
q          Return to previous menu

Command>
```

3. Type **b** to set the Boot Mode to *BootP-TFTP*, or type **t** to set Boot Mode to *TFTP* only. If you choose BootP-TFTP mode, the options for setting the IP Address of the TFTP server and the Boot File Name become unavailable; in this case, skip Steps 4-7 and go on to Step 8.
4. Type **s** in the Bootstrap Configuration Menu, to select the option *Set Boot Server IP Address*.
5. At the prompt, type the IP address of the remote boot server that contains the switch's software image file. Then press **Enter**. The Bootstrap Configuration Menu appears.
6. Type **f** to select the option *Set Boot File Name*.
7. Type the software's file name/network path at the prompt.
8. Press **Enter**.

Note: If you decide to use Local Load Mode rather than Remote, type **I**, and the Local Bootstrap Configuration Menu appears.

The switch is now set to download its software remotely from the network. This will occur the next time the unit is powered on or reset.