Asante

IntraCore® IC36240 Series

Layer 2+ Gigabit Ethernet Switch

User's Manual

IntraCore IC36240

Layer 2+ Gigabit Ethernet Switch

User's Manual

Asante Technologies, Inc.
2223 Oakland Road
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
801-566-3787: Fax
www.asante.com/support
support@asante.com

SWITCH DEFAULTS
IP address: 192.168.0.1
Password: Asante

05/11/05

Table of Contents

Chapter 1: Introduction

The IntraCore IC36240 24-port Layer 2+ Managed Gigabit Switch is a high-performance network switch used to reduce network congestion and application response times. The 24-port IntraCore IC36240 multi-protocol switch supports Layer 2+ and Gigabit Ethernet switching. The switch has 24 10/100/1000BaseT ports with Auto-Uplink and has 4 combination ports used for sharing with SFP mini GBICs. Gigabit fiber technology is used to connect two switches together. The switches also have an SNMP-based management agent embedded on the main board. This agent supports both in-band and out-of-band access for managing the switch.

These switches have a broad range of features for Layer 2+ switching delivering reliability and consistent performance for network traffic. The switches improve network performance by segregating them into separate broadcast domains with IEEE 802.1Q compliant VLANs and provide multimedia applications with multicast switching and CoS services.

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

1.1 Features

The IntraCore IC36240 Gigabit Ethernet switch is a 24-port Layer 2+ multi-media, multi-protocol (Ethernet and Layer 2+) switch. The following is a list of features:

- 24 port 10/100/1000 switch with auto-uplink
- Supports wire-speed L2+ switching
- CoS provisioning on Layers 2 and 802.1p, IP precedence (TOS, DSCP, TCP/UDP) port number
- Flexible wire-speed packet classification
- Packet filtering
- 16K MAC address
- 1K configurable port-based support for 4K VLAN ID, IGMP snooping
- SNMP v1, v2, and v3, RMON, statistics counters supported
- Spanning Tree Protocol 802.1D (standard), 32 instances of 802.1w (rapid) VLAN and 802.1s (multiple)
- 12 trunks and 8 ports/trunk link aggregation
- 2MB internal packet buffer
- Support for Jumbo Frames (up to 9 KB in length)

1.2 Package Contents

The following items are included in the switch's package:

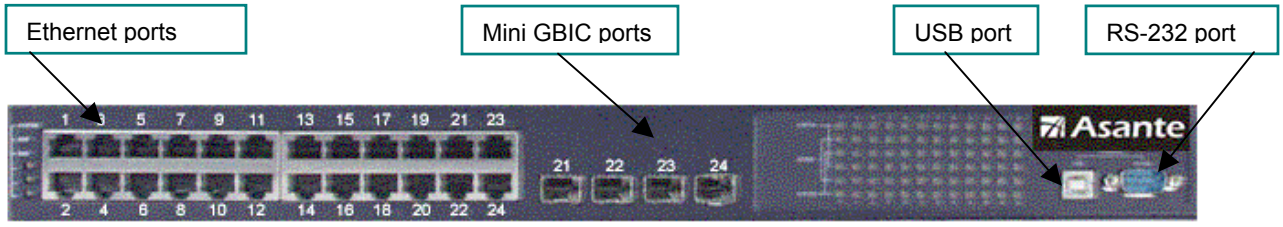
- Switch
- AC power cord
- USB cable for management console port
- RS232 null-modem cable for management console port
- Rack mount brackets with screws
- IntraCore IC36240 CD-ROM
- Release Note

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

1.3 Front and Back Panel Descriptions

The following section describes the front and back panels of the IntraCore IC36240 Series switches.

The front panel of the IntraCore IC36240 contains the following: power and port LEDs, 24 10/100/1000BaseT ports, 4 dual-function Gigabit ports that support either 1000BaseT or mini GBIC Gigabit Ethernet ports, a USB port and a console port. For information on LEDs refer to the following section in this chapter.



The back panel contains a 12 VDC jack for emergency power (optional), the primary power-bay cover plate and the primary power outlet.

1.3.1 LEDs

The IC36240 front panel LED display allows you to monitor the status of the switch.

The IC36240 has one power LED indicator, one (optional) external power LED and one fan LED. There are also LED indicators for each of the 24 ports. Refer to the following table for LED information.

LED	Color	Description
System	Green	Power is on and the system is operating normally.
	Green Flashing	Flashing during self-test, initialization, or downloading.
	Amber	Detects hardware malfunction (temperature, fan or voltage).
	Off	Power is off, or main power has failed.
External Power Supply	Green	External power supply is installed and ready to provide power.
	Amber	Internal power supply has failed and the external power supply is on.
	Off	External power supply is not installed or is not working properly.
Fan	Green	Fans are working properly.
	Amber	One or more fan is malfunctioning.
Port Status	Green	An RJ-45 or SFP link is present; the port is enabled.
	Green Flashing	Frames are received or transmitted on the port.
	Amber	Link is present; the port has been disabled manually or by spanning tree.
	Off	No link has been established on the port.
Link/Speed	Green	1000Mbps connection on the port.
	Amber	100Mbps connection on the port.
	Off	10Mbps connection on the port.
Duplex/Activity	Green	A full-duplex link has been established on the port.
	Amber	A half-duplex link has been established on the port.
	Off	No link on the port.

1.4 Management and Configuration

The switch is managed using Command Line Interface (CLI) in order to access several different command modes. Entering a question mark (?) at each command mode's prompt provides a list of commands.

1.4.1 Console Interface

Support for local, out-of-band management is delivered through a terminal or modem attached to the EIA/TIA-232 or USB interface. You can access the switch by connecting a PC or terminal to the console port of the switch, via a serial cable. The default password set on the console line is **Asante** (it is case-sensitive). The default IP address is **192.168.0.1/24**.

Remote in-band management is available through Simple Network Management Protocol (SNMP) and Telnet client. When connecting via a Telnet session (line vty0), the default password is also **Asante** (case-sensitive).

See Chapter 2 for more information on connecting to the switch.

Chapter 2: Hardware Installation and Setup

Use the following guidelines to easily install the switch, ensuring that it has the proper power supply and environment.

2.1 Installation Overview

Follow these steps to install the IntraCore IC36240 switch:

1. Open the box and check the contents. See *Chapter 1.2 Package Contents* for a complete list of the items included with the IntraCore IC36240 switch.
2. Install the switch in an equipment or wall rack, or prepare it for desktop placement.
3. Connect the power cord to the switch 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 a guideline, and may not include every possible hazard. 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 switch clean
- Keep tools and components off the floor and away from foot traffic
- Avoid wearing rings or chains (or other jewelry) that can 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 (such as 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 the warranty
- Examine the work area for potential hazards (such as wet floors or ungrounded cables)

2.1.2 Recommended Installation Tools

You need the following additional tools and equipment 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 properly grounded, located near the switch and be easily accessible. Make sure the power source adheres to the following guidelines:

- Power: Auto Switching AC, 90-240 VAC
- Frequency range: 50/60 Hz

2.1.4 Environmental Requirements

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

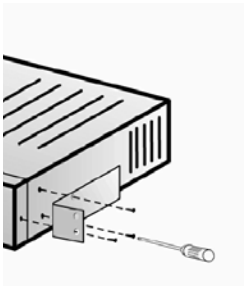
- Operating Temperature: 0° to 40°C (32° to 104°F)
- Relative Humidity: 5% to 95% non-condensing

Avoid direct sunlight, heat sources, or areas with high levels of electromagnetic interference. Failure to observe these limits may cause damage to the switch and void the warranty.

2.1.5 Cooling and Airflow

The IntraCore IC36240 switch uses internal fans for air-cooling. Do not restrict airflow by covering or obstructing air vents on the sides of the switch.

2.2 Installing into an Equipment Rack



Important: Before continuing, disconnect all cables from the switch.

To mount the switch into an equipment rack:

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 switch.
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 switch.

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

2.2.1 Equipment Rack Guidelines

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

- Size: 17.5 x 12.7 x 1.8 inches (440 x 234 x 45 mm)

- Ventilation: Ensure that the rack is installed in a room in which the temperature remains below 104° F (40° C). Be sure that no obstructions, such as other equipment or cables, block airflow to or from the vents of the switch

- Clearance: In addition to providing clearance for ventilation, ensure that adequate clearance for servicing the switch from the front exists

2.3 SFP Mini GBIC Ports

The GBIC Interface is the industry standard for Gigabit Ethernet Interfaces.

The Gigabit SFP module inserts into the Mini GBIC port to create a new Gigabit port. The hot-swapping feature on the IntraCore IC36240 lets you install and replace the SFP transceivers while the system is operating; you do not need to disable the software or shut down the system power.

To install the module, do the following:

1. Insert the transceiver with the optical connector facing outward and the slot connector facing down. The module is keyed to help establish the correct position.

2. Slide the SFP transceiver into the slot until it clicks into place.

3. Remove the module's rubber port cap.

4. Connect the cable to the Gigabit SFP module's port.

Caution: When replacing a SFP transceiver you must always disconnect the network cable before removing a transceiver.

2.4 Installing the Optional External Power Supply

The IntraCore IC36240 can be equipped with an optional 12 VDC external power supply (part number 52-10029-00). When installed, the external power supply is in standby mode. Should the primary unit fail, the backup automatically switches. In addition, an SNMP fault notice is sent.

To verify the primary power status, use the `Switch# **show system**` command. Under System Information, you see the power unit status.

```
System Information
------------------
  System up for:   000day(s), 01hr(s), 46min(s), 54sec(s)
  PROM Image Version/Date:    1.00C/Nov 11 2004 17:03:04
  DRAM Size:            64.0MB      Flash Size:         8.0MB
  Config NVRAM Size:     128KB      Console Baud Rate:  9600 bps
  Serial No. : BC120002
  Power Unit Status = OK
```

When the primary power fails and the external power supply is activated, the unit should be sent for repair. The external power supply is designed to be a temporary replacement when the primary power fails.

To install the optional power supply, simply attach the 12V connector of the power supply to the jack located in the center of the rear panel of the switch. Connect the power cord to the power supply and plug the power cord into an outlet.

Important: The external power supply is hot under normal operating conditions. To avoid damage or injury, set the power supply on a heat-resistant surface and use caution when handling the unit.

2.5 Connecting Power

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

Use the following procedure to connect power to the switch:

1. Plug one end of the supplied power cord into the power connector on the back of the switch.
2. Plug the other end into a grounded AC outlet.

The power LED show the initialization is in 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 that the correct cabling is used.

2.6 Connecting to the Network

The switch can connect to an Ethernet network with the switch turned on or off. Use the following procedure to make the network connections:

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

2.6.1 10/100/1000BaseT Ports Cabling Procedures

The 10/100/1000 ports on the switch allow for the connection of 10BaseT, 100BaseTX, or 1000BaseT network devices. The ports are compatible with IEEE 802.3 and 802.3u standards.

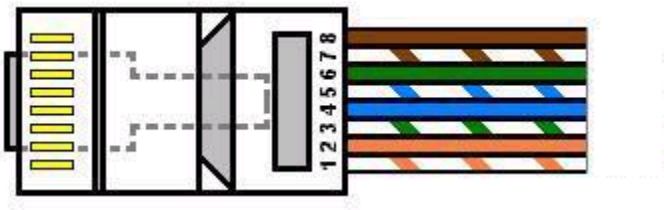
Important: The switch must be located within 100 meters of its attached 10BaseT or 100BaseTX devices.

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

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

Note: These switches have no specific uplink ports. All 10/100/1000 ports on these switches are auto-sensing MDI/MDI-X. This advanced feature means that when the ports are operating at 10/100Mbps, they will automatically determine whether the device at the other end of the link is a hub, switch, or workstation, and adjust its signals accordingly. No crossover cables are required.

Although 10/100BaseT requires only pins 1, 2, 3, and 6, you should use cables with all eight wires connected as shown in Table 2-2 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 2-2 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

2.6.2 Gigabit Ethernet Ports Cabling Procedures

Cabling requirements for the optional hardware modules depend on the type of module installed. Use the following guidelines to determine the particular cabling requirements of the module(s):

- 1000BaseSX GBIC: Cables with SC-type fiber connectors; 62.5µ multi-mode fiber (MMF) media up to 275 m (902'), or 50µ MMF media up to 550 m (1805')
- 1000BaseLX GBIC: Cables with SC-type fiber connectors; 10µ single-mode fiber media up to 5 km (16,405')

- 1000BaseLH GBIC: Cables with SC-type fiber connectors; 10µ single-mode fiber media up to 20 km (65,617')
- 1000BaseLX Long Haul GBIC: Cables with SC-type fiber connectors; 10µ single-mode fiber media up to 100 km (328,100')
- 1000BaseLZ GBIC: Cables with SC-type fiber connectors; 10µ single-mode fiber media up to 120 km (393,701')
- 1000BaseT: Category 5 or better Unshielded Twisted Pair (UTP) cable up to 100 m (328.1')

When attaching a workstation to the switch, 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. The switch should be kept off the network until proper IP settings have been set.

Chapter 3: Initial Software Setup

Configure the switch by connecting directly to it through a console (out-of-band management), running a terminal emulation program, such as HyperTerminal or by using telnet.

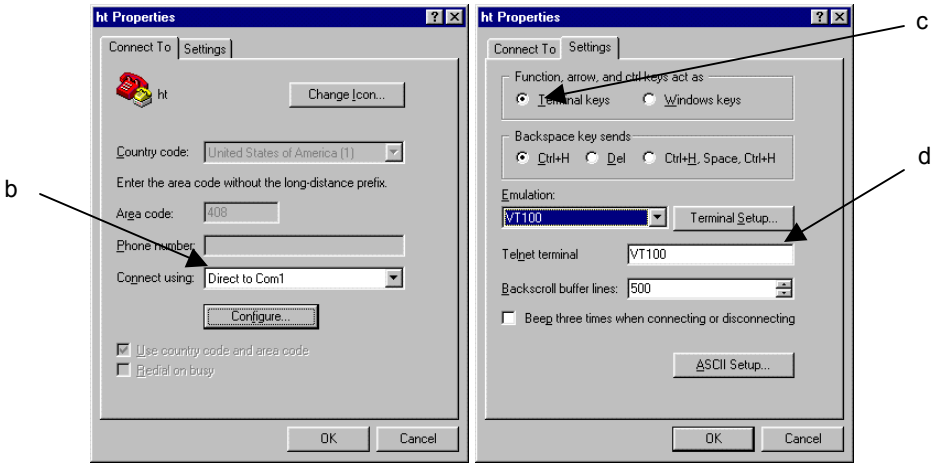
3.1 Connecting to a Console

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

1. Plug power cord into the back of the switch.
2. Attach a straight-through serial cable between the RS232 console port and a COM port on the PC.
3. Set up a HyperTerminal (or equivalent terminal program) in the following manner:

a. Open the HyperTerminal program, and from its file menu, right-click on **Properties.**

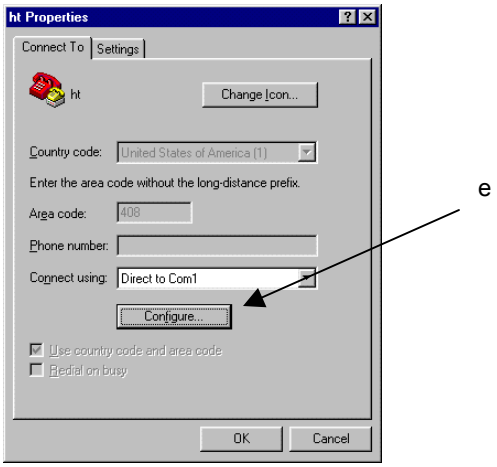
b. Under the **Connect To** tab, choose the appropriate COM port (such as COM1 or COM2).



c. Under the **Settings** tab, choose Select Terminal keys for Function, Arrow, and Ctrl keys. Be sure the setting is for Terminal keys, NOT Windows keys

d. Choose VT100 for Emulation mode.

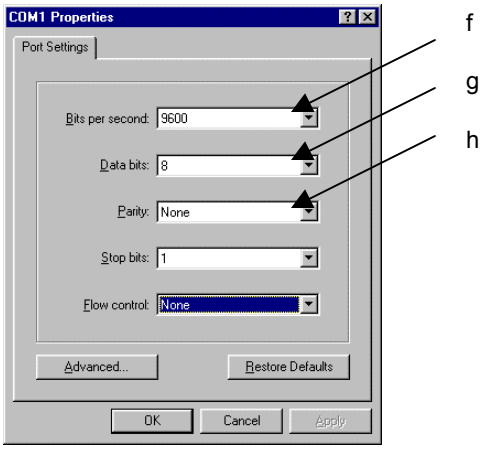
e. Press the **Configuration** button from the Connect To window.



f. Set the data rate to 9600 Baud.

g. Set data format to 8 data bits, 1 stop bit and no parity.

h. Set flow control to NONE.



Now that terminal is set up correctly, power on the switch. The boot sequence will display in the terminal.

After connecting to the console, the following appears:

```
User Access Verification
Password:
```

The initial default password for access using either the console or telnet is Asante (case-sensitive). Refer to the following section for setting passwords on the terminal lines.

3.2 Connecting to a PC

You can connect to the switch through a PC by using either an Ethernet or USB cable. Using a telnet session, you can telnet into the switch. The default IP address is 192.168.1.1. The case-sensitive default password is Asante.

3.3 Passwords and Privileges Commands

The switch has not default password, which allows anyone on the network access to various privilege levels. To prevent unauthorized changes to the switch's configuration, you should set an enable password for access to switch management. Follow the example below to assign a privileged password.

```
Switch> enable
Password: <no password by default; press Enter>
Switch# configure
Switch(config)# enable password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) 'enable' password
Switch(config)# enable password 0 <password>
Switch(config)# exit
Switch# write [memory | file]
```

A separate password should be set for the primary terminal line (console) and the virtual terminal lines (telnet). The default password Asante is assigned only to the virtual terminal line Vty0. Up to three other virtual terminal lines may be created, and they each will require a separate password.

3.3.1 Privileges Commands

The following sections describe the password privileges commands used to control access to different levels of the switch:

- Enable Password
- Password
- Service Password-Encryption

3.3.2 Enable Password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. Use the **no** form of this command to remove the password requirement.

```
Switch(config)# enable password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) 'enable' password
Switch(config)# enable password 0 <password>
Switch(config)# exit
Switch# write [memory | file]
```

3.3.3 Password

To specify a password on a line, use the **password** command in line configuration mode. Use the **no** form of this command to remove the password.

```
Switch(config)# line ?
  console  Primary terminal line
  vty      Virtual terminal
Switch(config)# line console ?
  <0-0>  Line number
Switch(config)# line console 0
Switch(config-line)# ?
  end           End current mode and change to enable mode
  exec-timeout  Set timeout value
  exit          Exit current mode and down to previous mode
  help          Description of the interactive help system
  no            Negate a command or set its defaults
  password      Set a password
  quit          Exit current mode and down to previous mode
Switch(config-line)# password ?
  LINE  The UNENCRYPTED (cleartext) line password
  0     Specifies an UNENCRYPTED line password will follow
  7     Specifies a HIDDEN line password will follow
Switch(config-line)# password Asante
Switch(config-line)# end
Switch# write ?
  file      Write to configuration file
  memory    Write configuration to the file (same as write file)
  terminal  Write to terminal
Switch# write file
Writing current-config to startup-config, Please wait...
Configuration saved to startup-config file
Switch#
```

3.3.4 Service Password-Encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. Use the **no** form of this command to restore the default. Refer to section 4.7 “Using the No Form and Default Commands” for more information.

```
Switch(config)# service password-encryption
Switch(config)# no service password-encryption
```

Note: You should change the default telnet password to prevent unauthorized access to the switch.

The password can be set at unencrypted (level 0) or encrypted (level 7).

```
Switch(config-line)# password ?
  LINE  The UNENCRYPTED (cleartext) line password
  0     Specifies an UNENCRYPTED line password will follow
  7     Specifies a HIDDEN line password will follow
```

3.4 Login Security

Two methods are available on the IntraCore IC36240 to configure an authentication query process for better login security: the **username** command for the global configuration mode and **password** and **login** commands from the line configuration mode.

3.4.1 The username Command

To establish a username-based authentication system, use the **username** command in global configuration mode. This method is more effective because authentication is determined on a user basis. The configuration is done for each line.

```
Switch(config)#
Switch# username name password password
```

The name argument can be a host name, server name, user ID, or command name. It is restricted to only one word. Blank spaces and quotation marks are not allowed.

Optionally, an encrypted password can be used, preceded by a single-digit number that defines what type of encryption is used. Currently defined encryption types are 0 (which means that the text immediately following is not encrypted) and 7 (which means that the text is encrypted using an encryption algorithm).

3.4.2 The password and login Commands

Using the **password** and **login** commands is less effective because the password is configured for the port, not for the user. Therefore, any user who knows the password can authenticate successfully.

This method enables user name and password checking at login time. Authentication is based on the user.

Note: The default login user is not set.

3.5 Configuring an IP Address

The switch ships with the default IP address **192.168.0.1/24**. Connect through the serial port in order to assign the switch an IP address on your network.

Follow the steps below to change the switch's IP address.

1. Connect to the console and press **Enter** at the Password prompt, as described above.
2. The screen displays the user mode prompt, `Switch>`.
3. Type **enable**. The new prompt is `Switch#`.
4. Type **configure**. The new prompt is `Switch(config)#`.

5. Type **ip address** and the new address. The following screen appears:

```
Switch> enable
Switch# configure
Switch(config)# ip address 192.168.123.254/24
Switch(config)# end
Switch# show ip
Dhcp Client Enabled ..........: No
IP Address ...................: 192.108.250.51
Subnet Mask ..................: 255.255.255.0
Default Gateway ..............: 192.108.250.5
HTTP Server ..................: Enabled
HTTP Port ....................: 80
Switch# write file
Writing current-config to startup-config. Please wait.
Configuration saved to startup-config file
```

It is also acceptable to enter the subnet mask by typing `ip address 192.168.123.254/24`. Use the **show interface veth1** command from privileged mode to see the new IP address. The new IP address automatically writes over the default IP address.

See Chapter 6 for more information on assigning IP addresses to interfaces.

3.5.1 Setting a Default IP Gateway Address

To define the default IP gateway for the switch, insert a static route:

```
Switch(config)# ip default-gateway 192.168.0.254
```

3.6 Restoring Factory Defaults

To restore the switch to its factory default settings, follow the commands shown in the following screen.

```
Switch> enable
Switch# reload ?
  fac-dflt-except-IP  Reset ALL system parameters except IP parameters to factory
                      default
  factory-default     Reset ALL system parameters to factory default
  <cr>
```

The switch is ready for configuration. Refer to the following chapters for management and configuration information.

3.7 System Boot Parameters

The IntraCore IC36240 has two boot banks to store its runtime code. You can select which bank to use for the next boot with the following command:

```
Switch(config)# boot system flash {bank1|bank2}
```

Chapter 4: Understanding the Command Line Interface (CLI)

The switch utilizes Command Line Interface (CLI) to provide access to several different command modes. Each command mode provides a group of related commands.

After logging into the system, you are automatically in the *user top (user EXEC) mode*. From the user top mode you can enter into the *privileged top (privileged EXEC) mode*. From the privileged EXEC level, you can access the global configuration mode and specific configuration modes: interface, Switch, and route-map configuration. Entering a question mark (?) at the system prompt allows you to obtain a list of commands available for each command mode. Almost every Switch configuration command also has a **no** form. You can use the **no** form to disable a feature or function. For example, **ARP** is enabled by default. Specify the command **no arp** to disable the ARP table.

Document Conventions

Command descriptions use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive, elements
- Square brackets ([ ]) indicate optional elements
- Braces ({ }) indicate a required choice
- Braces within square brackets ([{ }]) indicate a required choice within an optional element
- **Boldface** indicates commands and keywords that are entered literally as shown
- *Italics* indicate arguments for which you supply values

Access Each Command Mode

The following sections describe how to access each of the CLI command modes:

- User Top Mode: Switch>
    - Privileged Top Mode: Switch#
        - Global Configuration Mode: Switch(config)#
            - Interface Configuration Mode: Switch(config-if-IFNAME)#

4.1 User Top (User EXEC) Mode

After you log in to the Switch, you are automatically in user top (user EXEC) command mode. The user-level prompt consists of the host name followed by the angle bracket (>):

```
Switch>
```

The default host name is *Switch* unless it has been changed during initial configuration, using the **setup** command.

The user top commands available at the user level are a subset of those available at the privileged level. In general, the user top commands allow you to connect to remote devices, change terminal settings on a temporary basis,

To list the commands available in user top mode, enter a question mark (?). Use a space and a question mark (?) after entering a command to see all the options for that particular command.

Command	Purpose
?	Lists the user EXEC commands.
show ?	Lists all the options available for the given command.

User top commands:

```
Switch> ?
 enable      Turn on privileged mode command
 exit        Exit current mode and down to previous mode
 help        Description of the interactive help system
 ping        Send echo messages
 quit        Exit current mode and down to previous mode
 show        Show running system information
 cls         Clear screen
```

You may also enter a question mark after a letter or string of letters to view all the commands that start with that letter (with no space between the letter and the question mark). See section 3.8.2.

4.2 Privileged Top (Privileged EXEC) Mode

Because many of the privileged commands set the system configuration parameters, privileged access can be password protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which you can access the remaining command modes. Privileged EXEC mode also includes high-level testing commands, such as **debug**.

The following example shows how to access privileged EXEC mode. Notice the prompt changes from *Switch>* to *Switch#*:

```
Switch> enable
Switch#
```

Command	Purpose
Switch> **enable**	Enters the privileged EXEC mode.
Switch# **?**	Lists privileged EXEC commands.

If you have set a password, the system prompts for it before allowing access to privileged EXEC mode. If an enable password has not been set, the enable mode can be accessed only through the console. You can enter the **enable password** global configuration command to set the password that restricts access to privileged mode.

To return to user EXEC mode, use the **disable** command.

In general, the top (privileged) commands allow you to change terminal settings on a temporary basis, perform basic tests, and list system information. To list the commands available in top mode, enter a question mark (?) at the prompt, as shown in the following example. Enter a question mark (?) after a command to see all the options for that command.

```
Switch> enable
Switch# ?
  clear         Reset functions
  clock         Manage the system clock
  configure     Enter configuration mode
  copy          Copy from one file to another
  debug         Debugging functions
  disable       Turn off privileged mode command
  erase         Erase a filesystem
  exit          Exit current mode and down to previous mode
  help          Description of the interactive help system
  ip            Global IP configuration subcommands
  no            Negate a command or set its defaults
  ping          Send echo messages
  quit          Exit current mode and down to previous mode
  reload        Halt and perform a cold restart
  show          Show running system information
  snmp-server   SNMP related functions
  write         Write running configuration to memory, network, or terminal
  cls           Clear screen
```

Important: To retain configuration changes after a system reload you must save changes made in running configuration to the startup configuration file. From the privileged level, configurations can be saved using the **write** command or by using the **copy running-config startup-config** command.

4.3 Global Configuration Mode

Global configuration commands apply to features that affect the system as a whole, rather than just one protocol or interface. Commands to enable a particular routing function are also global configuration commands. To enter the global configuration mode, use the **configure** command.

The following example shows how to access and exit global configuration mode and list global configuration commands.

Command	**Purpose**
Switch**# configure**	From privileged EXEC mode, enters global configuration mode.
Switch(config)**# ?**	Lists the global configuration commands.

To exit global configuration command mode and return to privileged EXEC mode, use one of the following commands:

Command	Purpose
exit **end** **Ctrl-Z**	Exits global configuration mode and returns to privileged EXEC mode.

To list the commands available in global configuration mode, enter a question mark (?) at the prompt, as shown in the following example. Enter a question mark (?) after a specific command to see all the options for that command.

```
Switch# configure
Switch(config)# ?
  access-list         Add an access list entry
  arp                 Set static arp entry
  banner              Define a login banner
  boot                Modify system boot parameters
  clock               Manage the system clock
  define              Create a definition
  dot1x               IEEE 802.1x configuration
  duplicate-ip        Duplicate IP Address detection Global Commands
  enable              Modify enable password parameters
  end                 End current mode and change to enable mode
  exit                Exit current mode and down to previous mode
  help                Description of the interactive help system
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  Global IP configuration subcommands
  lacp                Configure LACP
  line                Configure a terminal line
  logging             Message Logging global configuration commands
  mac                 Add a mac access list entry
  mac-address-table   MAC Address Table global configuration command
  monitor             Traffic Monitoring Global configuration commands
  no                  Negate a command or set its defaults
  priority-list       Priority List global configuration commands
  quit                Exit current mode and down to previous mode
  service             Modify use of network based services
  show                Show running system information
  snmp-server         Modify SNMP parameters
  sntp                Modify SNTP parameters
  spanning-tree       Spanning Tree Protocol global command
  tos-list            Tos List global configuration commands
  username            To establish a username-based authentication system
  vlan                VLAN global configuration command
  write               Write running configuration to memory, network, or terminal
```

From global configuration mode, you can access three additional configuration modes: Use the **interface**, **spanning-tree**, and **vlan** commands to access their respective configuration modes.

4.3.1 Interface Configuration Mode

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type as Ethernet.

In the following example shows configuration of Ethernet interface (eth1). The new prompt, `Switch(config-if-eth1)#`, indicates the interface configuration mode. In this example, the user asks for help by requesting a list of commands.

```
Switch(config)# interface eth1
Switch(config-if-eth1)# ?
  description     Interface specific description
  dot1x           IEEE 802.1x configuration
  duplex          Configure duplex operation
  end             End current mode and change to enable mode
  exit            Exit current mode and down to previous mode
  fair-queue      Fair-queue interface configuration commands
  flow-control    IEEE 802.3X Flow Control Enable command
  help            Description of the interactive help system
  ip              Interface Internet Protocol config commands
  lacp            Configure LACP
  mac             control access to an interface
  mtu             Set the interface Maximum Transmission Unit (MTU)
  negotiation     Select Autonegotiation mode
  no              Negate a command or set its defaults
  priority-group  Assign a priority queue list to an interface
  quit            Exit current mode and down to previous mode
  rate-limit      To configure committed access rate (CAR)policies
  show            Show running system information
  shutdown        Shutdown the selected interface
  spanning-tree   Spanning Tree Protocol interface command
  speed           Configure speed operation
  storm-control   Enable storm control on the interface.
  switchport      Port operating in L2 mode
  tos-group       Assign a tos list to an interface
  traffic-shape   Generic traffic shape QoS interface configuration commands
  write           Write running configuration to memory, network, or terminal
```

To exit interface configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to top mode, use the **end** command or press **Ctrl-Z**.

4.3.2 Spanning-Tree Configuration Mode

Spanning Tree configuration commands are used to configure an IP routing protocol and always follow a **Switch** command. To list the available Switch configuration keywords, enter the **Switch** command followed by a space and a question mark (**?**) at the global configuration prompt.

```
Switch(config)# spanning-tree ?
  mst           Enable multiple spanning tree (IEEE 802.1s)
  forward-time  Set forwarding delay time
  hello-time    Set interval between HELLOs
  max-age       Maximum allowed message age of received Hello BPDUs
  priority      Set bridge priority
  rapid         Enable rapid convergence
```

In the following example, the switch shows the multiple Spanning Trees (MST) command.

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# ?
  end       End current mode and change to enable mode
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  instance  MST instance
  name      Set MST configuration name
  no        Negate a command or set its defaults
  quit      Exit current mode and down to previous mode
  revision  Set MST configuration revision number
  show      Show running system information
  write     Write running configuration to memory, network, or terminal
```

To exit Spanning Tree configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to top mode, use the **end** command or press **Ctrl-Z**.

4.3.3 VLAN Configuration Mode

Use the VLAN configuration mode to partition a single IntraCore IC36240 into a VLAN each containing it own set of ports. To access and list the VLAN configuration commands, use the command in global configuration mode.

In the following example, a VLAN named *myvlan* is configured. Enter a question mark (**?**) to list **vlan** configuration commands.

```
Switch(config)# vlan name myvlan
Switch(config-vlan)# ?
  end          End current mode and change to enable mode
  exit         Exit current mode and down to previous mode
  help         Description of the interactive help system
  name         Specify VLAN Name
  port-member  VLAN port member configuration
  quit         Exit current mode and down to previous mode
  show       Show running system information
  write      Write running configuration to memory, network, or terminal
```

To exit VLAN configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to top mode, use the **end** command or press **Ctrl-Z**.

4.4 Advanced Features Supported within the Command Mode

Enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also get a list of any command's associated keywords and arguments with the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, perform one of the following commands:

Command	Purpose
Help	Obtain a brief description of the help system in any command mode.
?	List all commands available for a particular command mode.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is word help, because it completes a word for you.

To list keywords or arguments, enter a question mark (?) in place of a keyword or argument. Include a space before the question mark (?). This form of help is command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you already have entered.

You can abbreviate commands and keywords to the number of characters that allow a unique abbreviation. For example, you can abbreviate the **configure** command to **config**. Because the shortened form of the command is unique, the switch accepts the shorted form and executes the command.

Enter the **help** command (which is available in any command mode) for a brief description of the help system:

```
Switch# help
CLI/VTY provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup until entering a
'?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show
?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to
know what arguments match the input (e.g. 'show cl?'.)
Switch# show cl?
 clock  Display the system clock
Switch# show cl
```

As described in the help command output, you can enter a partial command name and a question mark (?) to obtain a list of commands beginning with a particular character set.

Example of Context Sensitive Help

The following example illustrates how the context-sensitive help feature creates an access list from the configuration mode.

Enter the letters “co” at the system prompt followed by a question mark (?). Do not leave a space between the last letter and the question mark (?). The system provides the commands that begin with *co*.

```
Switch# co?
  configure  Enter configuration mode
  copy       Copy from one file to another
Switch# co
```

Enter the **configure** command followed by a space and a question mark (?) to list the command’s keyword(s) and a brief explanation:

```
Switch# configure ?
  configure  Enter configuration mode
```

Note that in the example below, if you enter the ip command followed by the Return Key or Enter, the system returns the prompt that the command is incomplete.

```
Switch# ip
% Command incomplete.
Switch#
```

Generally, uppercase letters represent variables. For example, after entering a command, such as **hostname**, and using a space and a question mark, you will be prompted for the new name, represented by WORD. In cases where an IP address is the variable, the uppercase letters A.B.C.D will represent it.

```
Switch(config)# hostname ?
  WORD  This system's network name
```

In the following access list example, two further options are listed after the question mark. You may enter an optional source wildcard. The return symbol (<cr>) indicates a return key is needed to enter the command.

```
Switch(config)# access-list 99 deny 192.168.123.0 ?
  A.B.C.D Source wildcard. e.g. 0.0.0.255
  <cr>
Switch(config)# access-list 99 deny 192.168.123.0
```

4.5 Checking Command Syntax

The CLI user interface provides an error indicator, a caret symbol (^). The caret symbol appears at the point in the command string where you have entered an incorrect letter, command, keyword, or argument.

In the following example, suppose you want to add an access-list entry:

```
Switch(config)# access-list
                ^
  % Invalid input detected at '^' marker.
```

In the following example, an incomplete command is entered.

```
Switch(config)# access-list
 % Command incomplete.
Switch(config)#
```

4.6 Using CLI Command History

The CLI user interface provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. To recall commands from the history buffer, use one of the following commands:

Keystrokes/Command	Purpose
Press **Ctrl-P** or the up arrow key	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in EXEC mode, list the last several commands entered.

4.7 Using the No and Default Forms of Commands

Almost every Switch configuration command has an opposite **no** form that negates or reverses a command. In general, the **no** form is used to disable a function that has been enabled. To re-enable a disabled function, or to enable a function that is disabled by default, use the command without the **no** keyword. For example, Address Resolution Protocol (ARP) is enabled by default. Specify the command **no arp** to disable the ARP table; to re-enable the ARP table, use the **arp** command.

4.8 Using Command-Line Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the CLI command-line interface. The following subsections describe these features:

- Moving Around on the Command Line
- Completing a Partial Command Name
- Editing Command Lines that Wrap
- Deleting Entries
- Scrolling Down a Line or a Screen
- Redisplaying the Current Command Line
- Transposing Mistyped Characters
- Controlling Capitalization

4.8.1 Moving Around on the Command Line

Use the following keystrokes to move the cursor around on the command line in order to make corrections or changes:

Keystrokes	Purpose
Press **Ctrl-B** or the left arrow.	Move the cursor back one character.
Press **Ctrl-F** or the right arrow.	Move the cursor forward one character.
Press **Ctrl-A**.	Move the cursor to the beginning of the command line.
Press **Ctrl-E**.	Move the cursor to the end of the command line.
Press **Esc B**.	Move the cursor back one word.
Press **Esc F**.	Move the cursor forward one word.

Note: The arrow keys function only on ANSI-compatible terminals such as VT100s.

4.8.2 Completing a Partial Command Name

If you cannot remember a complete command name, press the **Tab** key to allow the system to complete a partial entry.

Keystrokes	Purpose
Enter the first few letters and press **Tab**.	Complete a command name.

If your keyboard does not have a Tab key, press Ctrl-I instead.

In the following example, when you enter the letters “conf” and press the **Tab** key, the system provides the complete command:

```
Switch# conf<Tab>
Switch# configure
```

The command is not immediately executed, so that you may modify the command if necessary. If you enter a set of characters that could indicate more than one command, the system simply lists all possible commands.

You may also enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter entered and the question mark (?). For example, three commands in privileged mode start with *co*. To see what they are, type **co?** at the privileged EXEC prompt:

```
Switch# co?
configure
copy
Switch# co
```

4.8.3 Editing Command Lines That Wrap

The enhanced editing feature provides a wraparound for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts eight spaces to the left. You cannot see the first eight characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, use the following command:

Keystrokes	Purpose
Press **Ctrl-B** or the left arrow repeatedly until you scroll back to the beginning of the command entry, or press **Ctrl-A** to return directly to the beginning of the line.	Return to the beginning of a command line to verify that you have correctly entered a lengthy command.

Note: The arrow keys function only on ANSI-compatible terminals such as VT100.

In the following example, the access-list command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted eight spaces to the left and redisplayed. The dollar sign ($) indicates that the line has been scrolled to the left. Each time the cursor reaches the end of the line, it is again shifted eight spaces to the left.

```
Switch(config)# access-list 101 permit icmp 192.168.123.0 0.0.0.255 192
Switch(config)# $ st 101 permit icmp 192.168.123.0 0.0.0.255 192.168.0.1
```

When you have completed the entry, press **Ctrl-A** to check the complete syntax before pressing **Enter** to execute the command. The dollar sign ($) appears at the end of the line to indicate that the line has been scrolled to the right:

```
Switch(config)# access-list 101 permit icmp 192.168.123.0 0.0.0.255 192$
```

Use line wrapping in conjunction with the command history feature to recall and modify previous complex command entries.

4.8.4 Deleting Entries

Use any of the following commands to delete command entries if you make a mistake or change your mind:

Keystrokes	**Purpose**
Press **Delete** or **Backspace**.	Erase the character to the left of the cursor.
Press **Ctrl-D**.	Delete the character at the cursor.
Press **Ctrl-K**.	Delete all characters from the cursor to the end of the command line.
Press **Ctrl-U** or **Ctrl-X**.	Delete all characters from the cursor to the beginning of the command line.
Press **Ctrl-W**.	Delete the word to the left of the cursor.
Press **Esc D**.	Delete from the cursor to the end of the word.

4.8.5 Scrolling Down a Line or a Screen

When using a command that list more information than will fill on the screen, the prompt --*More*-- is displayed at the bottom of the screen. Whenever the *More* prompt is displayed, use the following keystrokes to view the next line or screen:

Keystrokes	**Purpose**
Press **Return**.	Scroll down one line.
Press **Spacebar**.	Scroll down one screen.

4.8.6 Redisplaying the Current Command Line

If you are entering a command and the system suddenly sends a message to your screen, you can easily recall your current command line entry. To do so, use the following command:

Keystrokes	**Purpose**
Press **Ctrl-L** or **Ctrl-R**.	Redisplay the current command line.

4.8.7 Transposing Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters by using the following command:

Keystrokes	Purpose
Press **Ctrl-T**.	Transpose the character to the left of the cursor with the character located at the cursor.

4.8.8 Controlling Capitalization

You can toggle between uppercase and lowercase letters with simple keystroke sequences. To do so, use the following command:

Keystrokes	Purpose
Press **Esc C**.	Capitalize at the cursor. Press **Esc C** or **Alt-C** again to return to lowercase letters.

Chapter 5: Managing the System and Configuration Files

This chapter explains how to manage the system information, as well as how to manage the configuration files for the IntraCore IC36240.

5.1 Managing the System

This section discusses the following tasks needed to manage the system information of the IntraCore IC36240:

- Setting the System Clock
- Configuring the Host name
- Changing the Password
- Testing Connections with Ping Commands
- Enabling Syslog
- Displaying the Operating Configuration

5.1.1 Setting the System Clock

The IntraCore IC36240 has two ways to set clock.

To manually set the system clock, complete the following commands in privileged mode. Use a space and a question mark (?) to display the clock set options. Restart the system after configuring the clock by typing **reload** at the *Switch#* prompt and pressing **Enter**.

```
Switch# clock ?
  set  Set the time and date
Switch# clock set ?
  HH:MM:SS  Current Time
Switch# clock set 09:29:30 ?
  <1-31>  Day of the month
Switch# clock set 09:29:30 28?
  <1-31>  Day of the month
Switch# clock set 09:29:30 28 ?
  MONTH  Month of the year (for example: June or July)
Switch# clock set 09:29:30 28 January ?
  <1970-2069>  Year
Switch# clock set 09:29:30 28 January 2005
Switch# reload <cr>
```

To use Simple Network Time Protocol, enter the commands below:

```
Switch# configure
Switch# (config) Clock timezone pacific hour 8 minute 0 after-utc
Switch# (config sntp server A.B.C.D
```

A.B.C.D is the IP address of a time server.

5.1.2 Specifying the Hostname

The factory-assigned default host name is **Switch**. To specify or modify the host name for the network, use the **hostname** global configuration command.

Command	Purpose
hostname *name*	This system's hostname.

5.1.3 Changing the Password

The switch ships with a default of no password for privilege mode, which allows immediate access to anyone on the network. In order to guard against unauthorized access, only the administrator should be allowed to change the password. The new password must have more than five characters, and less than eight characters. **The password is case sensitive**.

To change the password, use the following command in global configuration mode.

Keystrokes	Purpose
enable password	Change the password.

5.1.4 Testing Connections with Ping Tests

The switch supports IP ping, which can be used to test connectivity to remote hosts, via their IP addresses. Ping sends an echo request packet to an address and "listens" for a reply. The ping request will receive one of the following responses:

- Normal response—The normal response occurs in 1 to 10 seconds, depending on network traffic
- Request timed out—There is no response, indicating a connection failure to the host, or the host has discarded the ping request

Beginning in privileged EXEC mode, use this command to ping another device on the network from the switch:

Command	Purpose
Ping *address*	Send an ICMP echo message to a designated host for testing connectivity.

5.1.5 Enabling the System Log

The IntraCore IC36240 sends syslog messages to manager servers. Syslog messages are collected by a standard UNIX or NT type syslog daemon.

Syslog enables the administrator to centrally log and analyze configuration events and system error messages such as interface status, security alerts, environmental conditions, and CPU process overloads.

To log messages, use the following command in global configuration mode.

Command	Purpose
logging *address*	IP address of the host to be used as a syslog server.
logging facility	Facility parameters for syslog messages.
logging trap	Set syslog server logging level.

5.1.6 Displaying the Operating Configuration

The configuration file may be displayed from the EXEC (enable) mode.

To see the current operating configuration, enter the following command at the enable prompt:

```
Switch# show running-config
```

To see the configuration in NVRAM, enter the following command:

```
Switch# show startup-config
```

If you made changes to the configuration, but did not yet write the changes to NVRAM, the results of **show running-config** will differ from the results of **show startup-config**.

5.2 Managing Configuration Files

This section discusses how to download configuration files from remote servers, and store configuration files on the switch at system startup.

Configuration files contain the commands the switch uses to customize the function of the IC36240. The setup command facility helps you create a basic configuration file. However, you can manually change the configuration by typing commands in a configuration mode.

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the system. The two configuration files can be different. For example, you may want to change the configuration for a short period rather than permanently. In this case, you would change the running configuration using the **configure** command, but not save the configuration using the **copy running-config startup-config** command. To change the startup configuration, you can either save the running configuration file to the startup configuration using the **copy running-config startup-config** command, or copy commands from a file server to the startup configuration (**copy tftp startup config** command) without affecting the running configuration.

5.2.1 Configuring from the Terminal

The configuration files are stored in the following places:

- The running configuration is stored in RAM
- The startup configuration is stored in nonvolatile random-access memory (NVRAM)

To enter the configuration mode, enter the **configure** command at the privileged EXEC prompt. The software accepts one configuration command per line. You can enter as many configuration commands as you want.

You can add comments to a configuration file describing the commands you have entered. Precede a comment with an exclamation point (!).

Use the following commands to configure the software from the terminal.

Command	Purpose
configure	Enters global configuration mode and select the terminal option.
Switch(config)#	The global configuration prompt. Enter the necessary configuration commands.
copy running-config startup-config	Saves the configuration file to your startup configuration. On most platforms, this step saves the configuration to NVRAM.
end or press **Ctrl-Z** (**^Z**)	Exits global configuration mode.

In the following example, the **hostname** command is used to change the hostname from "Switch" to "new_name". By pressing Ctrl-Z (^Z) or entering the **end** command, you quit[1] the global configuration mode. Finally, the **copy running-config startup-config** command saves the current configuration to the startup configuration.

```
Switch# configure
Switch(config)# hostname new_name
new_name(config)# end
new_name# copy running-config startup-config
```

When the startup configuration is in NVRAM, it stores the current configuration information in text format as configuration commands, recording only non-default settings. The memory is checksummed to guard against corrupted data.

5.2.2 Copying Configuration Files to a Network Server

You can copy configuration files from the switch to a file server using TFTP. You might wish to back up a current configuration file to a server before changing its contents, thereby allowing you to later restore the original configuration file from the server.

Important: TFTP is not a secure protocol. Your server IP address and configuration file name will not be protected over the public Internet. Use TFTP only on a trusted LAN connection.

To specify that the running or startup configuration file be stored on a TFTP network server, use the following commands in the EXEC mode. (**Note**: Copying the startup configuration file to the current running configuration merges the two files. You should keep a copy of the start-up configuration file before merging the two in case you want to revert to the original startup configuration).

The following is an example of copying the startup-config for use on the switch.

```
Switch# copy startup-config ?
  running-config             Update (merge with) current system configuration
  tftp:[//A.B.C.D/filename]  Copy to tftp: file system
```

The following is an example of copying the running-config for use on the switch.

```
Switch# copy running-config ?

  startup-config             Copy to startup configuration
  tftp:[//A.B.C.D/filename]  Copy to tftp: file system
Switch# copy running-config tftp
Enter TFTP Server IP Address [A.B.C.D]?
Enter file name 'my-config' to copy?
```

Reply to any prompts for additional information or confirmation. The prompt depends on how much information has been provided in the copy command and the current setting of the file prompt command.

The command can also look like this example:

```
Switch# copy running-config tftp://192.168.0.1/my-config
Upload file 'my-config' to 192.168.0.1 from running-config? [y/n] y
Accessing tftp://192.168.0.1/my-config...
[OK] 487 bytes copied in time <1 sec
```

5.2.3 Copying Configuration Files from a Network Server to the Switch

You can copy configuration files from a TFTP server to the running configuration or startup configuration of the switch. You may want to do this for one of the following reasons:

1. To restore a previously backed up configuration file.

2. To use the same configuration file for another switch. For example, you may add another switch to your network and want it to have a similar configuration to the original switch. By copying the file to the new switch, you can change the relevant parts rather than re-creating the whole file.

3. To load the same configuration commands onto all the switches in your network so that they all have the same configurations.

The **copy tftp running-config** command loads the configuration files into the switch as if you were typing the commands in at the command line. The switch does not erase the existing running configuration before adding the commands unless a command in the copied configuration file replaces a command in the existing configuration file. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration may not be replaced or negated. In this case, the resulting configuration file will be a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

In order to restore a configuration file to an exact copy of a file stored on a server, you need to copy the configuration file directly to the startup configuration (using the **copy tftp startup-config** command) and reload the switch.

To copy a configuration file from a TFTP server to the switch, use one of the following commands in EXEC mode:

Command	**Purpose**
copy tftp:[[[//location]/directory]/filename] **running-config** **copy tftp:**[[[//location]/directory]/filename] **startup-config**	Copy a file from a TFTP server to the switch.

Reply to any switch prompts for additional information or confirmation. Additional prompts depend on how much information is provided in the copy command and the current setting of the file prompt command.

In the following example, the software is configured from the file my-config at IP address 192.168.123.59:

```
Switch# copy tftp://192.168.123.59/my-confg running-config
Download file 'my-config' from 192.168.123.59 to running-config? [y/n] y
Accessing tftp://192.168.123.59/my-config...
[OK] 487 bytes copied in time <1 sec
Updating running-config...
```

To clear the saved configuration, use the following command from privileged mode:

```
Switch# erase startup-config
```

5.3 Configuring SNMP

This section discusses the following tasks needed to configure Simple Network Management Protocol (SNMP).

Simple Network Management Protocol (SNMP) is the standard of network management protocols on TCP/IP-based networks.

SNMP allows network managers to obtain specific performance and configuration information from a software agent on a remote-network device. SNMP allows different types of networks to communicate by exchanging network information through messages known as protocol data units (PDUs). The IntraCore IC36240 supports SNMPv1, v2 and v3. The SNMPv3 protocol has improved the authentication, access control, and security methods. The following sections outline these methods.

5.3.1 Authentication

SNMPv1 relies on IP address-based access lists and community strings that function like a password and is shared between an SNMP manager and agent. IP address-based access lists can be vulnerable to IP address spoofing.

When there is easy physical access to a network or community strings intercepted, simple network management operations can reveal network information about any device configured for remote SNMP management.

Because SNMPv3 requires that, both the SNMP manager and agent share a secret authentication key, to ensure security in your network use the SNMPv3 protocol. Each SNMPv3 packet carries the user's name and key. The key is generated from a user password by using a secure hash function.

The User-based Security Model (USM) for SNMPv3 defines two authentication protocols: HMAC-MD5-96, which is based on MD5 (faster). The MD5 protocol must be implemented in an SNMPv3 environment.

MD5 is a hashing algorithm. When a message concatenated with a user's key is received, the system generates a fingerprint for the string. After the hash is performed, the fingerprint is added to the message (without the key). Sending this fingerprint with the message protects it from both the Modification of Information and Masquerade security threats. If any of the data in the packet is modified after the original is transmitted, it is detected when the hash is performed on the received message (minus the fingerprint, plus the users key), and the result is compared to the fingerprint that was received. This process also protects the network from Masquerade attack because the scope of the authentication includes the message's origin. In this way, both the identity of the sender and integrity of the message can be verified.

5.3.2 Access Control

SNMPv3 allows for the definition of multiple access controls. Access control is a security function performed at the PDU level. Strong access control demands strong authentication, which SNMPv3 does have.

5.3.3 Security Levels

SNMPv3 has three levels of security. The lowest level does not provide authentication or privacy (noAuthNoPriv). This level is comparable to SNMPv1. The second level provides authentication, but no privacy (AuthNoPriv). The highest level provides authentication and security (AuthPriv). Based on protection needs you should use some combination of these security levels.

Authentication, privacy, and access control combined address the security threats faced by SNMP, including Modification of Information, Masquerade, Disclosure, and Message Stream Modification attacks. SNMPv3 provides these security features.

SNMPv3 does not protect the network from Denial of Service and Traffic Analysis attacks.

5.3.4 Support

The IntraCore IC36240 switch supports Simple Network Management Protocol (SNMP) v1, v2 and v3. SNMP v3 provides additional security for your network. The SNMP system consists of three parts: an SNMP manager, an SNMP agent, and a Management Information Base (MIB). SNMP is an application-layer protocol that allows SNMP manager and agent stations to communicate. SNMP provides a message format for sending information between an SNMP manager and an SNMP agent. The agent and MIB reside on the switch. In configuring SNMP on the switch, the relationship between the manager and the agent must be defined.

The *SNMP agent* gathers data from the *MIB*, which holds the information about device parameters and network data. The agent also responds to the manager's requests to get or set data. An agent can also send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a specific event on the network. Such events include improper user authentication, restarts, link status (up or down), closing of a TCP connection, or loss of connection to a neighboring switch. An *SNMP manager* can request a value from an agent, or store or change a value in that agent.

To configure support for SNMP on the switch, perform the following tasks:

- Create or Modify Access Control for SNMP Community
- Establish the Contact and Location of SNMP Agent
- Define SNMP Trap Operations
- Disable the SNMP Agent

Create or Modify Access Control for SNMP Community

You can configure a community string, which acts like a password, to permit access to the agent on the switch.

- Read Only (ro): The string that defines access rights for reading SNMP data objects. The default is public.
- Read-Write (rw): The string that defines access rights for writing SNMP data objects. The default is private.

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

To set up the community access string to permit access to the SNMP, use the following command from the global command mode.

Command	Purpose
Snmp-server community *string* [**view** *view-name*] {**ro** | **rw**} [*access-list-number*]	Define the community access string. The *access-list-number* parameter is numbered from 1–99 and 1300–1999.

Establish the Contact and Location of the SNMP Agent

Set the system contact and the location of the SNMP agent so that these descriptions can be accessed through the configuration file.

To set the system contact (sysContact) string, use the following command in global configuration command.

Command	Purpose
Snmp-server contact *text*	Set the system contact string.
Snmp-server location *text*	Set the system location string.

Define SNMP Trap Operations

A trap is an unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred. The SNMP trap operations let you configure the switch to send information to a network management application when a particular event occurs.

To define traps for the agent to send to the manager, use the following commands in global configuration mode.

Command	Purpose
snmp-server host *address* [**traps|informs**] [**version** {**1|2c** [**auth|noauth|priv**]}] *community-string* [**udp-port** *port-number*]	Specify the recipient of the trap message.

The IC36240 can send an SNMP trap to its configured trap receivers if it detects a duplicate IP address. To turn on duplicate IP detection, use the following command in global configuration mode:

Command	Purpose
duplicate-ip detect	Enable duplicate IP detection.

Disable the SNMP Protocol

To disable SNMP, use the following command in global configuration mode:

Command	Purpose
no snmp-server	Disable SNMP operation. This command disables all versions of the SNMP agent.

5.3.5 SNMP Configuration Commands

Command	Purpose
snmp-server	Enable the SNMP agent. The first ***snmp-server*** global configuration command enables SNMP.
snmp-server engineID {**local** *engineid-string*|**remote** *host-ip-address* [**udp-port** *port-number*] *engineid-string*}	Set Engine ID for local or remote devices. The remote engine ID is used to create users that can send SNMPv3 traps.
snmp-server view *view-name subtree* [*subtree-mask*] [**included | excluded**]	Define the SNMP server view. Currently, the SNMP *subtree* can only adopt numbered form. That is, "1.3.6.1.2.1" is valid but "mib-2" is invalid. The *subtree-mask* uses colon-separated hex digits, such as "FF:A0".
snmp-server group *group-name* {**v1 | v2c | v3** [**auth | noauth**]} [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*]	Set SNMP views. The default read-view is "*all*," and the default write-view and notify-view are "none".
snmp-server user *user-name group-name* [**remote** *host-ip-address* [**udp-port** *port-number*]] { **v3** [**auth** {**md5**} *auth-password*]}	Define SNMP server users. (Currently creating "**v1|v2**" users and the "**sha**"(SHA1) algorithm are not supported)
snmp-server enable traps [duplicate-ip |snmp | station-move]	Enable SNMP traps. Supported trap types are authentication, duplicate-ip, and station-move.
snmp-server trap-timeout *seconds*	Define how often to resend trap messages. The range is 1–1000. The default is 30 seconds.
snmp-server queue-length *length*	Set the message queue length for each trap-host. The range is 1–1000. The default is 10.
snmp-server contact *text*	Set the system contact string.
snmp-server location *text*	Set the system location string.
show snmp **show snmp engineID** [**local | remote**] **show snmp groups** **show snmp user**	Show various SNMP information.

5.4 Configuring Spanning Tree

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 with redundant path but without spanning tree protocol, the same message is broadcast through multiple paths, leading to 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 traffic, 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).

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

5.4.1 Spanning Tree Parameters

The operation of the spanning tree algorithm is governed by several parameters. You can configure the following parameters from global configuration mode: forward-time, hello-time, max-age, and priority.

```
Switch(config)# spanning-tree mst?
  forward-time  Set forwarding delay time
  hello-time    Set interval between HELLOs
  max-age       Maximum allowed message age of received Hello BPDUs
  mst           Enable multiple spanning tree
  priority      Set bridge priority
  rapid         Enable rapid convergence
  <cr>
Switch(config)#
```

Forward Time

After a recalculation of the spanning tree, the Forward Time 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 Time is 15 seconds.

Hello Time

This is the time 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.

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

(Hello Time + 1) <= Maximum Age <= 2 x (Forward Delay – 1)

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 the network, 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 the network, it is best to leave the value of the Bridge Priority at its default setting.

Reducing the values of these timers makes 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 makes the spanning 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 changing the parameters.

5.4.2 Spanning Tree Port Configuration

You can configure the following parameters from interface configuration mode:

```
Switch(config)# interface eth1
Switch(config-if-eth1)# spanning-tree ?
  disable        Disable spanning tree protocol in this interface
  edge-port      Enable port admin edge
  link-type      Configure the link type
  path-cost      Set interface path cost
  port-priority  Set interface priority
Switch(config-if-eth1)#
```

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, it can be 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 of the equation:

Path cost = 1000/LAN speed (in Mbps)

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

5.4.3 Rapid Spanning Tree Protocol (RSTP)

Rapid Spanning Tree Protocol makes use of point-to-point link type and expedites into a rapid convergence of the spanning tree. Re-configuration of the spanning tree can occur in less than 1 second (as opposed to 50 seconds with the default settings in the legacy spanning tree), which is critical for networks carrying delay-sensitive traffic, such as voice and video.

Port Roles and the Active Topology

RSTP provides rapid convergence of the spanning tree by assigning port roles and by determining the active topology. RSTP uses the same underlying spanning tree calculation and algorithm as legacy STP to select the bridge with the highest bridge priority (lowest numerical priority value) as the root bridge. Then RSTP assigns one of these port roles to bridge ports:

- Root port—provides the best path (lowest cost) when the bridge forwards packets to the root switch.
- Designated port—connects to the designated switch, which has the lowest path cost when forwarding packets from that LAN to the root bridge. The port through which the designated switch is attached to the LAN is called the designated port.

- Alternate port—offers an alternate path toward the root switch to that provided by the current root port.

- Backup port—acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected together in a loop-back by a point-to-point link or when a switch has two or more connections to a shared LAN segment.

- Disabled port—has no role in the operation of the spanning tree.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

Rapid Convergence

RSTP provides for rapid recovery of connectivity following the failure of a switch, switch port, or LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

- Edge ports—If a port on a switch running RSTP is assigned to be a edge port, it will be put to forwarding immediately. However, the edge port will be in the RSTP initialization state and will send out the RSTP BPDUs with the operating status of edge port set to TRUE. If the edge port starts receiving the BPDUs, it will change the operating edge state to FALSE and start the spanning tree calculations. It is recommended to assign any ports that are to be left as a “leaf” of the LAN (with no connection to any bridge) as edge ports.

- Root ports—If the RSTP selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.

- Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

Note that if the link type of the port is not forced, the switch makes the decision of link type by operating duplex mode of the port. Also, a port with full-duplex mode is considered as a point-to-point link type, and a port in half-duplex mode is set as shared link type.

Enabling Rapid Spanning Tree

Use the **spanning-tree rapid** (802.1s) configuration mode command to enable rapid spanning tree on the switch.

Use the **no** form of the command to disable the rapid spanning tree. Note that by default, spanning mode will be legacy 802.1D spanning, If **no spanning-tree rapid** is used, 802.1D spanning tree is used..

Configuring Switch/Bridge Priority

Use the following configuration mode command to set the switch/bridge priority:

```
Switch(config)# spanning-tree priority <priority>
```

For <*priority*> the range is 0 to 61440 in increments of 4096; the default is 32768. The lower number is used when you want to specify the switch as the root switch.

Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

To return the switch to its default setting, use the **no spanning-tree priority** configuration command.

Configuring Link Type

Use the following interface mode command to configure port link-type:

```
Switch(config)# interface eth1
Switch(config-if-eth1)#spanning-tree link-type {point-to-point|shared}
```

By default, the link type is determined from the duplex mode of the interface: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection.

To return the switch to its default setting, use the **no spanning-tree link-type** interface configuration command.

Configuring an Edge Port

Use the following interface mode command to configure port link type:

```
Switch(config)# interface eth1
Switch(config-if-eth1)#spanning-tree edge-port
```

The default setting is no edge port configuration.

To return the switch to its default setting, use the **no spanning-tree edge-port** interface configuration command.

Configuring Port Path Cost

Use the following interface mode command to configure port path cost:

```
Switch(config)# interface eth1
Switch(config-if-eth1)#spanning-tree path-cost <path-cost>
```

The default values for path cost is determined by the operating port speed:

- For ports operating in 1000Mb speed, the path cost is 20000
- For ports operating in 100Mb speed, the path cost is 200000
- For ports operating in 10Mb speed, the path cost is 2000000

To return the switch to its default setting, use the **no spanning-tree path-cost** interface configuration command.

Configuring Port Priority

Use the following interface mode command to configure port priority:

```
Switch(config)# interface eth1
Switch(config-if-eth1)#spanning-tree port-priority <port-priority>
```

For <*port-priority*>, the range is 0–240 in increments of 16; the default is 128. The lower the number, the higher the priority.

To return the switch to its default setting, use the **no spanning-tree port-priority** interface configuration command.

5.4.4 Multiple Spanning-Tree (MST)

MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic and enables load balancing. Networks are more reliable because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

In large networks, you can administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an MST region.

MST uses the modified RSTP version called the Multiple Spanning Tree Protocol (MSTP). The MST feature has these characteristics:

- MST runs a variant of spanning tree called internal spanning tree (IST). IST augments the common spanning tree (CST) information with internal information about the MST region. The MST region appears as a single bridge to adjacent single spanning tree (SST) and MST regions.
- A bridge running MST provides interoperability with single spanning tree bridges as follows:
    - MST bridges run IST, which augments the common spanning tree (CST) information with internal information about the MST region.
    - IST connects all the MST bridges in the region and appears as a subtree in the CST that includes the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
    - CIST (common and internal spanning tree) is the collection of ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges. CIST is the same as an IST inside an MST region and the same as CST outside an MST region. The STP, RSTP, and MSTP together elect a single bridge as the root of the CIST.
- MST establishes and maintains additional spanning trees within each MST region. These spanning trees are referred to as MST instances (MSTIs). The IST is numbered 0, and the MSTIs are numbered 1,2,3, and so on. Any MSTI is local to the MST region that is independent of MSTIs in another region, even if the MST regions are interconnected. MST instances combine with the IST at the boundary of MST regions to become the CST as follows:
    - Spanning tree information for an MSTI is contained in an MSTP record (M-record).
    - M-records are always encapsulated within MST BPDUs (MST BPDUs). The original spanning trees computed by MSTP are called M-trees. M-trees are active only within the MST region. M-trees merge with the IST at the boundary of the MST region and form the CST.

5.5 Configuring VLAN

VLANs are used to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group and eliminate broadcast storms in large networks. VLANs provide a secure and efficient network environment.

VLANs are based on untagged port groups, or traffic can be explicitly tagged to identify the VLAN group to which it belongs. Untagged VLANs can be used for small networks attached to a single switch. Tagged VLANs should be used for larger networks, and all the VLANs assigned to the inter-switch links.

Using multiple spanning trees allow VLAN groups to maintain a stable path between all VLAN members. This reduces the overall amount of protocol traffic crossing the network and provides a shorter reconfiguration time if any link in the spanning tree fails

Use the VLAN feature to partition a single IntraCore IC36240 into a VLAN each containing its own set of ports. Packets are forwarded only between ports belonging to the same VLAN. This allows you to restrict access from one segment to another to increase network security or to reduce traffic. To set up VLANs you should specify the ports belonging to the VLAN, the set the IP configuration, individual access map associated with a set of VLANs and enable tagging. Once you have configured the VLAN and copied the information into the startup-config file, the VLAN information applies to the default.

The following shows the commands from the VLAN interface configuration mode.

```
Switch(config)# vlan ?
  <1-4093>    Identifier (ID) of the VLAN to be added and configured
  access-map  VLAN-Map global configuration commands
  filter      VLAN Filter global configuration command
  reset       Reset VLAN cfg to factory default
Switch(config)# vlan 1
Switch(config-vlan)# ?
  end          End current mode and change to enable mode
  exit         Exit current mode and down to previous mode
  help         Description of the interactive help system
  name         Specify VLAN Name
  port-member  VLAN port member configuration
  quit         Exit current mode and down to previous mode
  show         Show running system information
  write        Write running configuration to memory, network, or terminal
Switch(config-vlan)#
```

Refer to Chapter 7 for more information about VLAN configuration.

5.6 MAC Address Table

The MAC Address 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. To see the table, type the following command in privileged mode:

```
Switch# show mac-address-table
Vlan    Mac Address             Type    Ports
----    -----------------       ----    -----
3       00:00:1C:01:00:09       Dynamic eth13
1       00:00:94:00:00:10       Dynamic eth9
1       00:00:94:A0:B6:7B       Dynamic eth9
1       00:00:94:AA:64:37       Dynamic eth9
1       00:00:94:D2:53:79       Dynamic eth9
--      00:00:94:D2:56:EA       Self    --
1       00:0A:27:AE:50:66       Dynamic eth9
1       00:50:FC:94:00:0D       Dynamic eth9
```

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 to 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. The MAC address of the switch is identified as “self”.

By default, entries in the switch's MAC address table expire after 300 seconds. To change this value, use the following command in global configuration mode:

```
Switch(config)# mac-address-table aging-time
```

The range is 10–1,000,000 seconds. A value of 0 disables aging.

Chapter 6: Configuring IP

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. All other IP protocols are built on the foundation. IP is a network-layer protocol that contains addressing and control information that allows data packets to be routed.

This section describes how to configure the Internet Protocol (IP). A number of tasks are associated with configuring IP. A basic and required task for configuring IP is to assign IP addresses to network interfaces. Doing so enables the interfaces and allows communication with hosts on those interfaces using IP. Associated with this task are decisions about subnetting and masking the IP addresses.

6.1 Assign IP Addresses to Switch

An IP address is a location to and from which IP datagrams can be sent. IP addresses were traditionally divided into three classes. The Class A Internet address format allocated the highest eight bits to the network field and set the highest-order bit to 0 (zero). The remaining 24 bits formed the host field. The Class B Internet address allocated the highest 16 bits to the network field and set the two highest-order bits to 1, 0. The remaining 16 bits formed the host field. The Class C Internet address allocated the highest 24 bits to the network field and set the three highest-order bits to 1,1,0. The remaining eight bits formed the host field.

The table below lists the traditional classes and ranges of IP addresses and their status.

Class	**Address or Range**	**Status**
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.0.0.0 255.255.255.0	Available
C	192.0.0.0 to 223.255.255.0	Available
D	224.0.0.0 to 239.255.255.255	Multicast group addresses
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

When multiple networks are connected to the Internet the traditional classified addressing scheme could cause you to run out of IP addresses.

The usual way of assigning IP addresses uses the prefixes of 8, 16, or 24 bits. Using prefixes of 13 to 27 bits an address includes the standard 32-bit IP address and adds information on how many bits are used for the network prefix. In the IP address 206.203.1.35/27, the “/27” indicates that the first 27 bits are used to identify the unique network, and the remaining bits are used to identify the specific host.

6.2 Establish Address Resolution

A device in the IP can have both a local address (which uniquely identifies the device on its local segment or LAN) and a network address (which identifies the network to which the device belongs). The local address is more properly known as a *data link* address because it is contained in the data link layer (Layer 2 of the OSI model) part of the packet header and is read by data link devices (bridges and all device interfaces, for example). The more technically inclined will refer to local addresses as *MAC addresses*, because the Media Access Control (MAC) sub-layer within the data link layer processes addresses for the layer.

To communicate with a device on Ethernet, you first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution.* The IntraCore IC36240 software uses the Address Resolution Protocol (ARP) for address resolution. ARP is used to associate IP addresses with media or MAC addresses. Taking an IP address as input, ARP determines the associated media address.

Once a media or MAC address is determined, the IP address/media address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network.

6.2.1 Define a Static ARP Cache

ARP provides a dynamic mapping between IP addresses and media addresses. Because most hosts support dynamic address resolution, you generally do not need to specify static ARP cache entries. Completing this task installs a permanent entry in the ARP cache. The entry is used to translate 32-bit IP addresses into 48-bit hardware addresses.

Optionally, you can specify that the software respond to ARP requests as if it was the owner of the specified IP address. You also have the option of specifying an interface when you define ARP entries.

Perform the following task in global configuration mode, to provide static mapping between IP addresses and media addresses.

Command	**Purpose**
arp *ip-address hardware-address*	Globally associate an IP address with a media (hardware) address in the ARP cache.
arp *ip-address hardware-address* [*interface*]	Specify that the software respond to ARP requests as if it was the owner of the specified interface.

To display the ARP being used on a particular interface, use the **show interface** in top mode or global configuration mode. Use the **show arp** command in top or configuration mode to examine the contents of the ARP cache.

6.3 Managing IP Multicast Traffic

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.

Traditional IP communication allows a host to send packets to one host (unicast transmission) or to all hosts (broadcast transmission). IP multicast provides a third scheme, allowing a host to send packets to a group of hosts (group transmission). A multicast address is chosen for the members of a multicast group. Senders use that address as the destination address of a datagram to reach all hosts of the group. The stream is sent to the multicast address, and from there, it is delivered to all interested parties on the Internet. Any host, regardless of whether it is a member of a group, can send to that group. However, only the members of the group receive the message.

The IntraCore IC36240 supports the Internet Group Management Protocol (IGMP) that is used between hosts on a LAN and the switch(s) on that LAN to track the multicast groups of which hosts are members.

6.3.1 IGMP Overview

The Internet Group Management Protocol (IGMP) manages the multicast groups on a LAN. IP hosts use IGMP to report their group membership to directly connected multicast switches. Switches executing a multicast protocol maintain forwarding tables to forward multicast datagrams. Switches use the IGMP to learn whether members of a group are present on their directly attached sub-nets. Hosts join multicast groups by sending IGMP report messages.

IGMP uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

The address 224.0.0.0 will not be assigned to any group. The address 224.0.0.1 is assigned to all systems on a sub-net. The address 224.0.0.2 is assigned to all switches on a sub-net.

Forwarding Unknown Multicast Packets

Unknown multicast packets are those packets with destination IP multicast addresses not learned by the switch. By default, the switch blocks all such traffic. Use the command below in configuration mode to control this feature.

Command	Purpose
ip mcast block-unknown	Block all multicast traffic with unknown IP multicast destination address.
no ip mcast block-unknown	Forward all multicast traffic according to VLAN and IGMP rules.

6.3.2 Configuring IGMP

Use the following commands to configure IGMP.

Specify the IGMP Version

By default, the switch uses IGMP Version 1. The version can be changed to IGMP version 2, which allows such features as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. Configure the switch for Version 2 if all devices on the subnet support IGMP version 2.

To control which version of IGMP the switch uses, use the following command in configuration mode:

Command	Purpose
ip igmp version {**2** | **1**} **vlan** <1-4093>	Select the IGMP version that the switch uses in a vlan.

Modifying the IGMP Host-Query Message Interval

Multicast switches send IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-systems group address of 224.0.0.1 with a time-to-live (TTL) value of 1.

Multicast switches continue to periodically send host-query messages to refresh their knowledge of memberships present on their networks. If, after some number of queries, the switch software discovers that no local hosts are members of a multicast group, the software stops forwarding onto the local network multicast packets from remote origins for that group and sends a prune message upstream toward the source.

Multicast switches elect a designated switch for the LAN (subnet). The designated switch is the one with the highest IP address. The switch is responsible for sending IGMP host-query messages to all hosts on the LAN. By default, the designated switch sends IGMP host-query messages every 60 seconds in order to keep the IGMP overhead on hosts and networks very low. To modify this interval, use the following command in interface configuration mode:

Command	Purpose
ip igmp query-interval *<10-3600 seconds>*	Configure the frequency at which the designated switch sends IGMP host-query messages.

The following example shows setting the IGMP query interval to 200.

```
Switch(config-if-veth1)# ip igmp query-interval 200
```

Changing the Maximum Query Response Time

By default, the maximum query response time advertised in IGMP queries is 10 seconds. If the switch is using IGMP Version 2, you can change this value. To change the maximum query response time, use the following command in configuration mode:

Command	Purpose
ip igmp query-max-response-time *<1-25 seconds>*	Set the maximum query response time advertised in IGMP queries.

6.4 Using Access Lists

An access list is a collection of criteria statements that the switch uses to determine whether to allow or block traffic based on IP addresses. Use Access lists to provide basic security on your network, and to prevent unnecessary traffic between network segments by permitting only required traffic onto your network.

When configuring an access list, you can add multiple statements by adding criteria to the same numbered list. The order of the statements is important, as the switch tests addresses against the criteria in an access list one by one (in the order the statements are entered) until it finds a match. The first match determines whether the system accepts or rejects the address. Because the system stops testing conditions after the first match, the order of the conditions is critical.

To develop an ACL first determine the protocols required within your networks. Although every site has specific requirements, certain protocols and applications are widely used. For example, network segments that provide connectivity for a publicly accessible web server or TCP.

Use the following sources to identify required traffic. The number of instances of applied access lists usually will not exceed 128 due to hardware limitations.

- Review local security policy
- Review firewall configuration
- Review applications

Using a Classification ACL

A classification ACL is composed of **permit** statements for the various protocols that could be destined to the internal network. (See for a list of commonly used protocols and applications.) Use the **show access-list** command to display a count of access control entry (ACE) hits to identify required protocols. Investigate and understand and suspicious or surprising results before you create explicit **permit** statements for unexpected protocols.

In addition to direct protection, the ACL should also provide a first line of defense against certain types of invalid traffic on the Internet.

Other types of traffic to consider include the following.

External protocols and IP Addresses

- ICMP from service provider IP Addresses

Explicitly permitted return traffic for internal connections to the Internet

- Specific Internet Control Message Protocol (ICMP) types
- Outbound Domain Name System (DNS) query replies
- TCP established
- User Datagram Protocol (UDP) return traffic
- FTP data connections
- TFTP data connections
- Multimedia connections

Explicitly permitted externally sourced traffic destined to protected internal addresses

- VPN Traffic
- HTTP to web servers
- Secure Socket Layer (SSL) to web servers
- FTP to FTP servers
- Inbound FTP data connections
- Simple Mail Transfer Protocol (SMTP)
- Other applications and servers
- Inbound DNS queries
- Inbound DNS zone transfers

Important: By default, if no conditions match, the software rejects the address.

The switch supports two types of access lists:

- **Standard**: access list numbers 1–99 and 1300–1999 (expanded range)
- **Extended**: access list numbers 100–199 and 2000–2699 (expanded range)

6.4.1 Create a Standard Access List

Standard access lists filter at Layer 3, and can allow or block access to networks and host addresses. The parameters for a standard access list are described below:

- **Access list number (1–99)**: Identifies the access list to which an entry belongs. There is no limit to how many entries make up an access list, other than available memory
- **Remark**: Access list entry comment. This may be useful to keep track of numbered lists
- **Permit/deny**: Indicates whether this entry allows or blocks traffic from the specified source address
- **Source address**: Enter the source IP address to match
- **Any**: Specifies any source address to match
- **Source wildcard mask**: Identifies which bits in the address field are to be matched. A “0” indicates that positions must match; a “1” indicates that position is ignored

In the following example, a standard access list is created to allow all traffic from the 192.168.0.0 networks, while blocking all non-192.168.0.0 traffic. The last entry is redundant, since the switch will deny access if there is no match found by the end of the list.

```
Switch# configure
Switch(config)# access-list 1 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
Switch(config)# access-list 1 permit ?
  A.B.C.D  Source address to match. e.g. 10.0.0.0
  any      Any source address to match
Switch(config)# access-list 1 permit 192.168.0.0 ?
  A.B.C.D  Source wildcard. e.g. 0.0.0.255
  <cr>
Switch(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Switch(config)# access-list 1 deny any
```

The next example shows a standard access list is created to deny all traffic from 192.168.123.254 and allow all other traffic to be forwarded. Note that the last entry of this example is not redundant, as it is a *permit* statement. An implicit *deny* statement would follow the last entry, if no match was found before the end of the list. In this case, however, you are permitting any other IP address other than 192.168.123.254, and a *deny* statement is not necessary.

```
Switch(config)# access-list 1 deny 192.168.123.254 ?
  A.B.C.D  Source wildcard. e.g. 0.0.0.255
  <cr>
Switch(config)# access-list 1 deny 192.168.123.254
Switch(config)# access-list 1 permit any
Switch(config)# exit
Switch# show access-list
```

After entering the access list, use the **show** command from privileged mode, as shown above. Any lists you have created, as well as any remark entered for a list, will be displayed.

Note: In the above examples, the argument *any* can be used instead of 0.0.0.0 255.255.255.255.

6.4.2 Create a MAC Access List

The IntraCore IC36240 has a 16K Mac address. The parameters for a MAC access list are described below:

- MAC access-list standard (700-799): Identifies the access list to which an entry belongs. There is no limit to how many entries make up a MAC access list, other than available memory.
- MAC access list extended (1100–1199): Identifies the access list to which an entry belongs.

The following is sample output from the mac access-list command.

```
Switch(config)# mac access-list standard 700
Switch(config)# permit
```

6.4.3 Create an Expanded Access List

Extended access lists filter at Layer 4, and can check source and destination addresses as well as filter transport layer information, such as TCP and UDP protocols. In addition to the standard access list parameters listed above, an extended access list also uses the following information:

- Access list number (1300–1999): Identifies the access list to which an entry belongs
- IP/ICMP/TCP/UDP: Specifies protocol connection
- Destination address: Specifies the destination address to match
- Operator operand: Select eq (equal to), gt (greater than), lt (less than), or neq (not equal to) to specify how to match the protocol port number
- 0-65535: Specifies the protocol port number. Well-known ports are listed below:

20	File Transfer Protocol (FTP) data
21	FTP Program
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
69	Trivial File Transfer Protocol (TFTP)
53	Domain Name System (DNS)
80	Hypertext Transport Protocol (HTTP)
110	Post Office Protocol (POP3)
119	Network News Transport Protocol (NNTP)

In the following example, an extended access list is created to deny FTP and allow all other traffic from subnet 192.168.123.0 to be forwarded to all other networks or subnets.

Note: Remember when the cursor reaches the right margin, the command line shifts 8 spaces to the left. You cannot see the first eight characters of the line, but you can scroll back and check the syntax at the beginning of the command, using **Ctrl-B** or the left arrow keys.

```
Switch# configure
Switch(config)# access-list 101 ?
  remark  Access list entry comment
  deny    Specify packets to reject
  permit  Specify packets to forward
Switch(config)# access-list 101 deny ?
  ip    Specify IP connections
  icmp  Specify ICMP connections
  tcp   Specify TCP connections
  udp   Specify UDP connections
  <0-255>  Specify protocol number
Switch(config)# access-list 101 deny tcp ?
  A.B.C.D  Source address to match. e.g. 10.0.0.0
  host     Host address to match.
  any      Any source address to match
Switch(config)# access-list 101 deny tcp 192.168.123.0 0.0.0.255 ?
  A.B.C.D  Destination address to match. e.g. 10.0.0.0
  host     Host address to match.
  any      Any destination address to match
Switch(config)# $ist 101 deny tcp 192.168.123.0 0.0.0.255 192.168.124.0 0.0.0.255?
  eq    Operator - equal to
  gt    Operator - greater then
  lt    Operator - less then
  precedence   precedence
  tos          type of service
  established  established
  <cr>
Switch(config)# $ list 101 deny tcp 192.168.123.0 0.0.0.255 192.168.124.0 eq ?
 <0-65535>  Protocol port number
  ftp        FTP
  ssh        SSH
  telnet     TELNET
  smtp       SMTP
  mtp        MTP
  gopher     GOPHER
  finger     FINGER
  http       HTTP
  pop        POP version 3
  bgp        BGP
  bgmp       Border Gateway Multicast Protocol
  https      HTTP over SSL/TLS
  rlogin     Rlogin
  syslog     SYSLOG
Switch(config)# $ eny tcp 192.168.123.0 0.0.0.255 192.168.124.0 0.0.0.255 eq 21 ?
  precedence   precedence
  tos          type of service
  established  established
  <cr>
Switch(config)# $ tcp 192.168.123.0 0.0.0.255 192.168.124.0 0.0.0.255 eq 21 tos 2 est
Switch(config)# exit
Switch# show access-list
```

6.4.4 Creating an Access List with a Name

From the global configuration mode, you can also create access lists. Using the `Switch(config)#ip` command you can name your access list, rather than using a number. The new prompt reflects the named access list mode.

```
Switch(config)# ip ?
  access-list       Named access-list
  forward-protocol  Controls forwarding of physical and directed IP
  prefix-list       Build a prefix list
  route             Establish static routes
Switch(config)# ip access-list ?
  standard  Standard Access List
  extended  Extended Access List
Switch(config)# ip access-list standard ?
  WORD  Access-list name or Standard IP access-list number <1-99>
Switch(config)# ip access-list standard test
Switch(config-std-nacl)# ?
  deny    Specify packets to reject
  end     End current mode and change to enable mode
  exit    Exit current mode and down to previous mode
  help    Description of the interactive help system
  no      Negate a command or set its defaults
  permit  Specify packets to forward
  quit    Exit current mode and down to previous mode
  remark  Access list entry comment
  show    Show running system information
  write   Write running configuration to memory, network, or terminal
Switch(config-std-nacl)#
```

At the `Switch(config-std-nacl)#` prompt, you configure the access list permit or deny statements.

6.4.5 Applying an Access List to an Interface

After creating your access lists, you must apply them to an interface in order to enable the access list. Enter the interface configuration mode for the desired interface. Each interface may have only one access list applied to it at one time. Apply the access lists to either inbound traffic or to outbound traffic.

The following example shows creating an extended access list that only allows SMTP traffic (port 25) to be sent out, and denies all other traffic.

```
Switch(config)# access-list 101 permit tcp 192.168.123.0 0.0.0.255 any eq 25
Switch(config)# access-list 101 deny any
Switch(config)# interface eth1
Switch(config-if-eth1)# ip ?
  access-group  Apply an access-group entry
Switch(config-if-eth1)# ip access-group ?
  WORD  access-list number or name
Switch(config-if-eth1)# ip access-group 101 ?
  in   inbound direction
  out  outbound direction
Switch(config-if-eth1)# ip access-group 101 out
Switch(config-if-eth1)# exit
```

6.4.6 Configuring Common Access Lists

This section provides examples the most common ACLs used when configuring a network. Change the IP addresses in the following examples when using them in your network.

The following example shows denying special-use address sources.

```
Switch(config)# access-list 110 deny ip 127.0.0.0 0.255.255.255 any
Switch(config)# access-list 110 deny ip 192.0.2.0 0.0.0.255 any
Switch(config)# access-list 110 deny ip 224.0.0.0 31.255.255.255 any
Switch(config)# access-list 110 deny ip host 255.255.255.255 any
```

The following example shows explicitly permitting ICMP.

```
Switch(config)# access-list 110 permit icmp any any
Switch(config)# access-list 110 permit icmp any any tos
Switch(config)# access-list 110 deny   icmp any any
```

The following example shows explicitly permitting UDPs with an operator equal to 53.

```
Switch(config)# access-list 110 permit udp any any eq 53
```

The following example shows explicitly permitting legitimate business traffic.

```
Switch(config)# access-list 110 permit tcp any any Internet-routable established
Switch(config)# access-list 110 permit udp any range 1 1023 Internet-routable subnet
gt 1023
```

The following example shows explicitly permitting ftp data connections.

```
Switch(config)# access-list 110 permit tcp any any eq 20 Internet-routable subnet gt
1023
```

The following example shows explicitly permitting tftp data and multimedia connections.

```
Switch(config)# access-list 110 permit udp any any gt 1023 Internet-routable subnet gt
1023
```

The following example shows explicitly permitting incoming DNS queries.

```
Switch(config)# access-list 110 permit udp any any gt 1023 host <primary DNS server>
eq 53
```

The following example shows explicitly permitting zone transfer DNS queries to primary DNS server.

```
Switch(config)# access-list 110 permit tcp host secondary DNS server gt 1023 host
primary DNS server eq 53
```

The following example shows explicitly permitting older DNS zone transfers.

```
Switch(config)# access-list 110 permit tcp host secondary DNS server eq 53  host
primary DNS server eq 53
```

The following example shows explicitly denying all other DNS traffic.

```
Switch(config)# access-list 110 deny udp any any eq 53
Switch(config)# access-list 110 deny tcp any any eq 53
```

The following example shows explicitly permitting internet-sourced connections to publicly accessible servers.

```
Switch(config)# access-list 110 permit tcp any host public web server eq 80
Switch(config)# access-list 110 permit tcp any host public web server eq 443
Switch(config)# access-list 110 permit tcp any host public FTP server eq 21
```

The following example shows explicitly permitting public SMTP connections to the FTP server.

```
Switch(config)# access-list 110 permit tcp any gt 1023 host public FTP server gt 1023
Switch(config)# access-list 110 permit tcp any host public SMTP server eq 25
```

The following example shows explicitly denying all other traffic.

```
access-list 101 deny ip any any
```

Chapter 7: VLAN Configuration

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

Usually VLANs are associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs is assigned. LAN port VLAN membership is assigned manually on an port-by-port basis. VLANs can be defined as either Layer 2 or Layer 3 and a VLAN cannot switch between the two layers. Before you create a VLAN, you must decide how they will be created and a naming convention to ensure duplicate VLAN names are not used.

Up to 4094 Virtual LANs (VLANs) are supported on the IntraCore IC36240. The default VLAN with VLAN ID (VID) 1. All switchports (eth1–eth16) are included in the default VID 1. **The default VID 1 cannot be deleted**.

7.1 Creating or Modifying a VLAN

Enter the following commands beginning in configuration mode:

Command	Purpose
vlan *vid*	Enter a VLAN ID (2–4094), which that accesses config-vlan mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify a VLAN.
name *vlan-name*	Enter a name for the VLAN (optional).
End	Return to Enable mode.
no vlan *vid*	Enter a VLAN ID (2-4094) to be removed.

Switchports are Layer 2-only interfaces associated with a physical port. A switchport is used as an access port. Switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging. Ports 1–16 on the IC36240 are Ethernet ports. The following example demonstrates how to enter the interface configuration mode for port 16:

```
Switch(config)# interface eth16
Switch(config-if-eth16)#
```

From the interface configuration mode, use the **switchport** command to configure the access port or the Class of Service (CoS) default priority for the port.

An access port belongs to and carries the traffic of only one VLAN (see Virtual Interfaces, below.) Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (802.1Q tagged), the packet is dropped, and the source address is not learned. Static access ports are manually assigned to a VLAN.

```
Switch(config-if-eth16)# switchport access vlan <1-4093>
```

First, a VLAN is created and named *tester*.

```
Switch# configure
Switch(config)# vlan 2
Switch(config-vlan)# name tester
Switch(config-vlan)# exit
Switch(config)# exit
Switch# show vlan
```

In the output of the **show vlan** command, the new VLAN will be listed, but will not yet be active. Next, choose a switchport to belong to VLAN 2.

```
Switch# configure
Switch(config)# interface eth9
Switch(config-if-eth9)# switchport access vlan 2
Switch(config-if-eth9)# exit
Switch(config)# exit
Switch# show vlan
```

In the output of the **show vlan** command, VLAN 2 is listed as active, with eth9 listed as a member port. Repeat the previous step to add additional switchports to VLAN 2.

You can also add ports by using the port-number command. The following example shows adding a port member.

```
Switch#
Switch# config
Switch(config)# vlan 1
Switch(config-vlan)# port-member add eth 1
```

7.1.2 Deleting a VLAN

Beginning in global configuration mode, use the following example to delete a VLAN on the switch (VLAN 2 in this example):

```
Switch(config)# no vlan 2
Switch(config)# exit
Switch# show vlan
```

Note: You cannot delete the default VLAN 1.

You can delete ports by using the port-member command. The following example show deleting a VLAN port member.

```
Switch#
Switch# config
Switch(config)# vlan 1
Switch(config-vlan)# port-member delete eth 1
```

7.2 VLAN Port Membership Modes

Assign a switchport to a VLAN by designating a membership mode. The membership mode determines the type of traffic the port carries and the number of VLANs that belong to a specific port. The following is a list of the membership modes:

- Static Access
- Trunk (IEEE 802.1Q)

7.2.1 Static Access

A static-access port can belong to one VLAN and is manually assigned to that VLAN. Use the following commands, beginning in config mode, to assign a static-access port to a VLAN:

Command	**Purpose**
interface IFNAME	Enter the interface name to access the interface configuration mode.
Switchport mode access	This command designates the interface as static-access mode.
Switchport access vlan *vid*	This command assigns the interface to the VLAN *VID.* Use the **no** form of this command to reset the static-access VLAN to default VID 1.
End	Return to Enable mode.

7.2.2 Trunk (IEEE 802.1q)

By default, a trunk port is a member of all VLANs. Membership can be limited by configuring a VLAN Allowed List.

Use the following commands, beginning in config mode, to assign an IEEE 802.1q trunk port:

Command	**Purpose**
interface IFNAME	Enter the interface name to access the interface configuration mode.
switchport mode trunk	This command designates the interface as IEEE 802.1q trunk-access mode. Use the **no** form of this command to reset to the default of static-access mode.
switchport trunk native vlan *vid*	This command assigns the native VLAN for the trunk port. Use the **no** form of this command to reset the native VLAN to VID 1.
Switch(config-if-IFNAME)# end	Return to Enable mode.

Use the following commands, beginning in config mode, to configure the *VLAN Allowed List* for the trunk port:

Command	Purpose
interface *IFNAME*	Enter the interface name to access the interface configuration mode.
switchport mode trunk	This command designates the interface as IEEE 802.1q trunk-access mode. Use the **no** form of this command to reset to the default of static-access mode.
switchport trunk allowed vlan {**add** | **all** | **except** | **remove | none**} *vlan-list*	This command configures the VLAN Allowed List for the trunk port. **add**—Add VLANs to the current VLAN list. **all**—Add all VLANs to the allowed-VLAN list. **except**—Add all VLANs except those specified in the VLAN list. **remove**—Remove the VLANs specified in the VLAN list. **none**—Specifies no VLANs. **vlan-list**—The VLAN list can be a single VLAN or a range of VLANs (from 1–4094). Separate the VID numbers by a comma, or by a hyphen when listing a range (e.g., “120, 158, 4090-4094”). Use the **no** form of this command to reset to default setting of all VLANs in the VLAN Allowed List.
End	Return to Enable mode.

The trunk port accepts tagged and untagged frames. All the untagged frames are classified to the trunk port’s native VLAN (the VLAN whose VID matches the port’s VLAN ID). The trunk port also sends out the frames as untagged for the native VLAN and tagged for other VLANs. Using the following global configuration command can change this behavior:

Command	Purpose
Switch(config)# vlan dot1q tag native	This global command enables tagging of native VLAN frames on all 802.1q trunk ports. Use the **no** form of this command to disable tagging of native VLAN frames.
Switch(config)# end	Return to Enable mode.

Chapter 8: Quality of Service Configuration

Quality of Service (QoS) is a general term referring to various methods of traffic management you can employ on your network to ensure that traffic you identify as high-priority can use a sufficient share of the available bandwidth. The IC36240 supports the following QoS methods:

- Weighted Fair Queuing
- Priority Queuing
- Traffic-Shape
- Rate-Limit

8.1.1 Configuring Weighted Fair Queuing

For flow-based WFQ, packets are classified by flow. Packets with the same source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, and protocol belong to the same flow. The bandwidth allocation is determined by the precedence field in the IP header. To enable this feature, use the **fair-queue** command in interface configuration mode:

When you enable flow-based WFQ, the following table applies:

CoS	Bandwidth
0	1/64
1	3/64
2	5/64
3	7/64
4	9/64
5	11/64
6	13/64
7	15/64

8.1.2 Monitoring Weighted Fair Queuing Lists

To display information about the input and output queues, use the following command in EXEC mode:

Command	Purpose
show queuing fair	Displays the status of the weighted fair queuing.

8.2 Priority Queuing

Priority Queuing (PQ) allows you to define how traffic is prioritized in the switch. You configure four traffic priorities. You can define a series of filters based on packet characteristics to cause the router to place traffic into these four

queues; the queue with the highest priority is serviced first until it is empty, then the lower queues are serviced in sequence.

8.2.1 Defining the Priority List

A priority list contains the definitions for a set of priority queues. The priority list specifies in which queue a packet will be placed.

In order to perform queuing using a priority list, you must assign the list to an interface. The same priority list can be applied to multiple interfaces. Alternatively, you can create many different priority policies to apply to different interfaces.

8.2.2 Monitoring Priority Queuing Lists

To display information about the input and output queues, use the **show queuing priority** command in EXEC mode.

8.2.3 Priority Queuing Example

This example configures the access-list 1 traffic going out on interface 15 to have a medium priority.

Defining the access list:

```
Switch(config)# access-list 1 permit 192.203.54.56
```

Defining the priority list:

```
Switch(config)# priority-list 2 protocol ip medium list 1
```

Assigning the priority list to an interface:

```
Switch(config)# interface eth15
Switch(config-if)# priority-group 2
```

8.4 Traffic Shaping

Traffic shaping allows you to control the traffic going out from an interface in order to match its flow to the speed of the remote target interface and to ensure that the traffic conforms to policies contracted for it.

Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

8.4.1 Configuring Traffic Shaping for an Interface

To configure traffic shaping for outbound traffic on an interface, use the following command in interface configuration mode:

```
Switch(config-if)# traffic-shape rate bit-rate
```

8.4.2 Configuring Traffic Shaping for an Access List

To configure traffic shaping for outbound traffic on an access list, use the following commands beginning in global configuration mode:

Command	Purpose
access-list *access-list-number*	Assigns traffic to an access list.
interface *interface-type-number*	Enters interface configuration mode.
traffic-shape group *access-list-number* ***bit-rate***	Configures traffic shaping for outbound traffic on an interface for the specified access list.

Repeat the steps for each type of traffic you want to rate limit.

8.4.3 Monitoring the Traffic Shaping Configuration

To monitor the current traffic shaping configuration and statistics, use the following commands in EXEC mode, as needed:

Command	Purpose
Show traffic-shape [*interface-name*]	Displays the current traffic shaping configuration.

8.4.4 Generic Traffic Shaping Example

This example configures that the DNS traffic to eth13 have maximum bandwidth of 50M.

Defining the access list:

```
Switch(config)# access-list 100 permit udp any any eq 53
```

Assigning the traffic shape to an interface:

```
router(config-if)# traffic-shape group 100 51200000
```

8.5 Configuring Rate Limit

To configure the committed access rate (CAR) policies use the rate-limit command. The rate-limit command allows you to control the amount of traffic coming in on a port.

```
Switch> enable
Switch# config
Switch(config)# inter eth1
Switch(config-if-eth1)# rate-limit ?
   input  Applies this CAR traffic policy to packets received on this input interface
Switch(config-if-eth1)# rate-limit input ?
  <1-4294967295>  Average rate, in bits per second (bps)
  access-group    (Optional) Applies this CAR traffic policy to the specified access
                  list
```

The following examples show setting the rate of interface Ethernet 1 to 100M, setting an associated access list and limiting the rate of the access list on the interface to 200M.

```
Switch(config)# inter eth1
Switch(config-if-eth1)# rate-limit input 100000000
Switch(config-if-eth1)# access-list 1 permit 192.203.56.1
Switch(config-if-eth1)# rate-limit input access-group 1 200000000
```

Chapter 9: Configuring the Switch Using the GUI

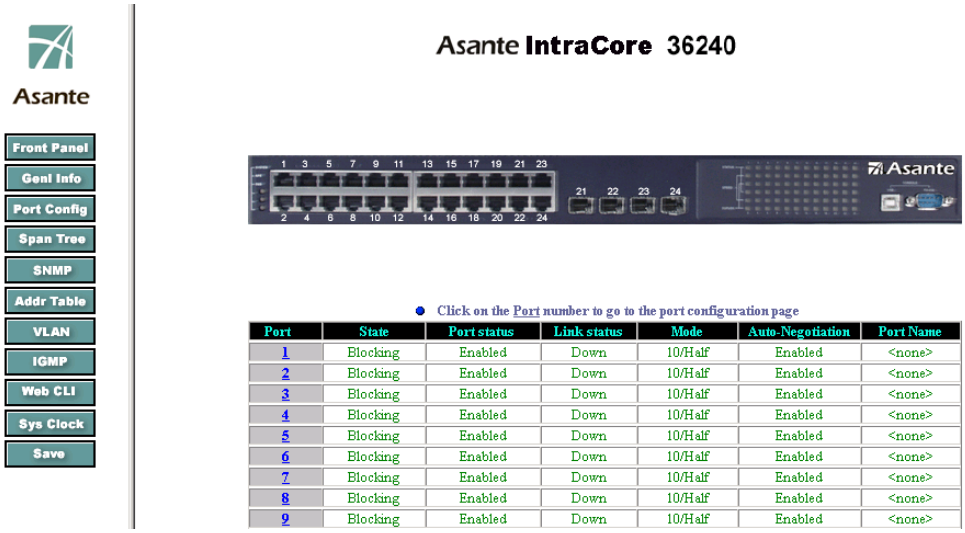
This chapter provides and overview of configuring the switch with the graphical user interface (GUI). For more information about the different features and how to implement them refer to the chapters specific to that function.

Refer to the following example for the commands required to set the GUI:

```
Switch# configure
Switch(config)# ip http server
```

At your web browser enter the IP address for the switch to launch the GUI.

The following example shows the main screen for the IntraCore IC36240:



9.1 Main Configuration Menu

Use the navigation panel on the left side of the GUI screen to configure the switch. From this panel you can access the following screens:

- Front Panel Information
- General Switch Information
- Port Configuration
- Spanning Tree Configuration
- SNMP Configuration
- Address Table Configuration
- VLAN Configuration
- IGMP Configuration
- Web CLI Screen

- System Check Information
- Save

The following example shows the main screen menu bar.

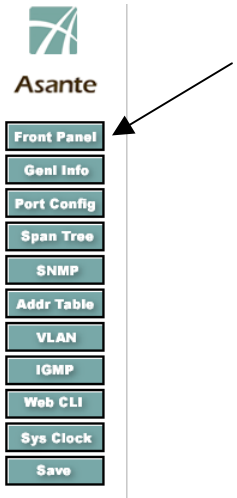
9.2 Information Screens

To monitor the switch use the two information screens. The following sections describe the Front Panel and the General Information screens.

9.2.1 Front Panel Information Screen

Use this section to access general information about the switch, the state of each port, the link status, the type of link, the mode, and port name.

To access the Front Panel Information Screen from the menu bar on the left side of the screen click on the Front Panel button.



Use this screen to view statistics about all the ports on the switch. The following example shows the Front Panel information screen.

Go to unit 1						
Unit - Port	**State**	**Port status**	**Link status**	**Type**	**Mode**	**Port Name**
1	Blocking	Enabled	Down	Unknown	10/Half	<none>
2	Blocking	Enabled	Down	Unknown	10/Half	<none>
3	Blocking	Enabled	Down	Unknown	10/Half	<none>
4	Blocking	Enabled	Down	Unknown	10/Half	<none>
5	Blocking	Enabled	Down	Unknown	10/Half	<none>
6	Blocking	Enabled	Down	Unknown	10/Half	<none>
7	Forwarding	Enabled	Up	Unknown	100/FULL	<none>
8	Blocking	Enabled	Down	Unknown	10/Half	<none>
9	Blocking	Enabled	Down	Unknown	10/Half	<none>
10	Blocking	Enabled	Down	Unknown	10/Half	<none>

Click on a specific port number hyperlink to go to the Port Configuration and Port Statistics Information screen. Refer to section 9.3.1 for information on the Port Configuration and Port Statistics screen.

9.2.2 General Information Screen

From the general information screen you can view the system version and the system clock. You can also view and modify, bank information, administrative information, system information, switch address, bootstrap information, system clock. The switch ships with the default IP address **192.168.0.1/24**.

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. All other IP protocols are built on the foundation. IP is a network-layer protocol that contains addressing and control information that allows data packets to be routed.

This section describes how to configure the Internet Protocol (IP). A number of tasks are associated with configuring IP. A basic and required task for configuring IP is to assign IP addresses to network interfaces. Doing so enables the interfaces and allows communication with hosts on those interfaces using IP. Associated with this task are decisions about subnetting and masking the IP addresses.

9.2.3 Assign IP Addresses to Switch

An IP address is a location to and from which IP datagrams can be sent. IP addresses were traditionally divided into three classes. The Class A Internet address format allocated the highest eight bits to the network field and set the highest-order bit to 0 (zero). The remaining 24 bits formed the host field. The Class B Internet address allocated the highest 16 bits to the network field and set the two highest-order bits to 1, 0. The remaining 16 bits formed the host field. The Class C Internet address allocated the highest 24 bits to the network field and set the three highest-order bits to 1,1,0. The remaining eight bits formed the host field.

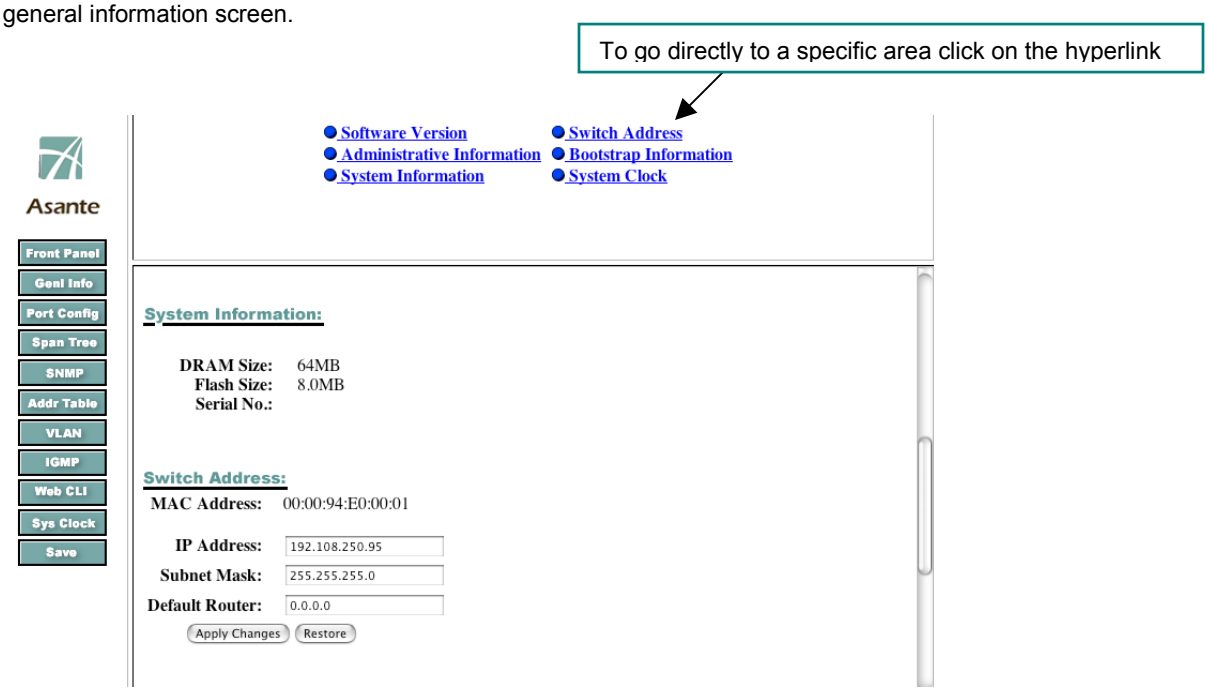
The table below lists the traditional classes and ranges of IP addresses and their status.

Class	Address or Range	Status
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.0.0.0 255.255.255.0	Available
C	192.0.0.0 to 223.255.255.0	Available
D	224.0.0.0 to 239.255.255.255	Multicast group addresses
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

When multiple networks are connected to the Internet the traditional classified addressing scheme could cause you to run out of IP addresses.

The usual way of assigning IP addresses uses the prefixes of 8, 16, or 24 bits. Using prefixes of 13 to 27 bits an address includes the standard 32-bit IP address and adds information on how many bits are used for the network prefix. In the IP address 206.203.1.35/27, the "/27" indicates that the first 27 bits are used to identify the unique network, and the remaining bits are used to identify the specific host.

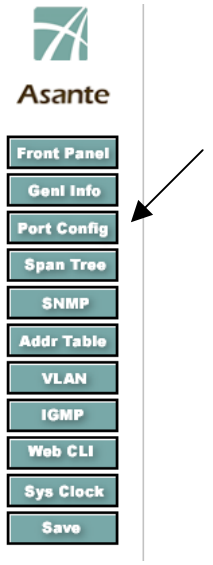
The General Information screen appears after clicking on the General Information button on the left side of the screen. Use the scroll bar on the left side to view other areas or information. The following example shows the general information screen.



9.3 Port Configuration Menu

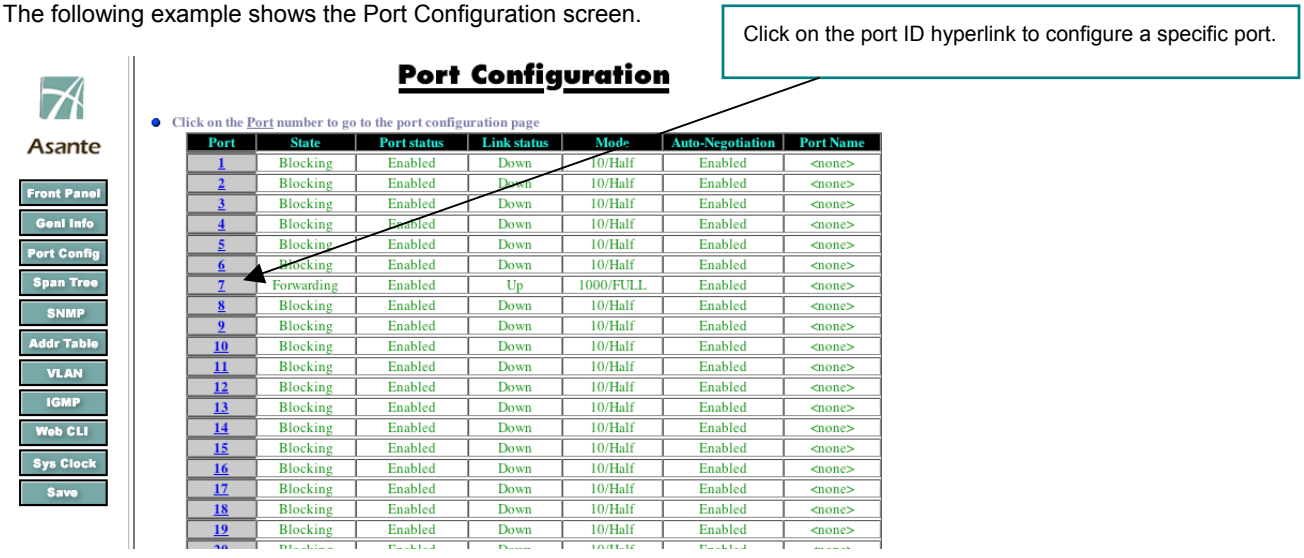
From the port configuration screen, you can view current information and configure individual ports.

To access the Port Configuration screen, click on Port Config in the menu bar on the left side of the screen.



To configure individual ports click on the port number on the left side of the screen. To configure a port, click on the port number on the left side of the screen.

The following example shows the Port Configuration screen.



Port	State	Port status	Link status	Mode	Auto-Negotiation	Port Name
1	Blocking	Enabled	Down	10/Half	Enabled	<none>
2	Blocking	Enabled	Down	10/Half	Enabled	<none>
3	Blocking	Enabled	Down	10/Half	Enabled	<none>
4	Blocking	Enabled	Down	10/Half	Enabled	<none>
5	Blocking	Enabled	Down	10/Half	Enabled	<none>
6	Blocking	Enabled	Down	10/Half	Enabled	<none>
7	Forwarding	Enabled	Up	1000/FULL	Enabled	<none>
8	Blocking	Enabled	Down	10/Half	Enabled	<none>
9	Blocking	Enabled	Down	10/Half	Enabled	<none>
10	Blocking	Enabled	Down	10/Half	Enabled	<none>
11	Blocking	Enabled	Down	10/Half	Enabled	<none>
12	Blocking	Enabled	Down	10/Half	Enabled	<none>
13	Blocking	Enabled	Down	10/Half	Enabled	<none>
14	Blocking	Enabled	Down	10/Half	Enabled	<none>
15	Blocking	Enabled	Down	10/Half	Enabled	<none>
16	Blocking	Enabled	Down	10/Half	Enabled	<none>
17	Blocking	Enabled	Down	10/Half	Enabled	<none>
18	Blocking	Enabled	Down	10/Half	Enabled	<none>
19	Blocking	Enabled	Down	10/Half	Enabled	<none>

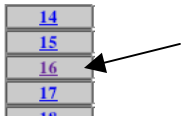
9.3.1 Individual Port Configuration Screen

The Port Configuration and Port Statistics menu appears after clicking on a specific port.

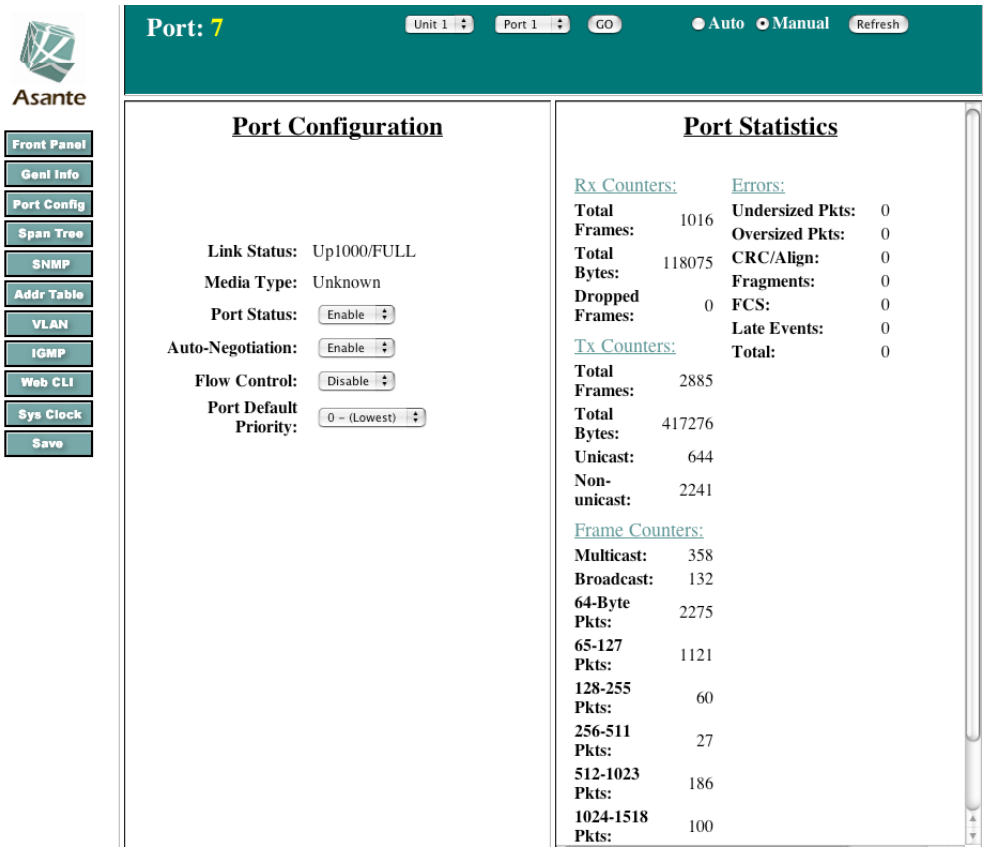
Use this screen to view information about the link status and media type.

The following example shows the Port Configuration and Port Statistics screen. Follow these steps to configure specific ports.

1. Click on the port number from the Front Panel Information Screen



- You are now at the Port Configuration and Port Statistics screen. From this screen, you can set the port status, auto-negotiation, flow control, and default priority. You also use this screen to view and manage traffic on a specific port. The following is an example of the screen.



4. Set the defaults for the following:

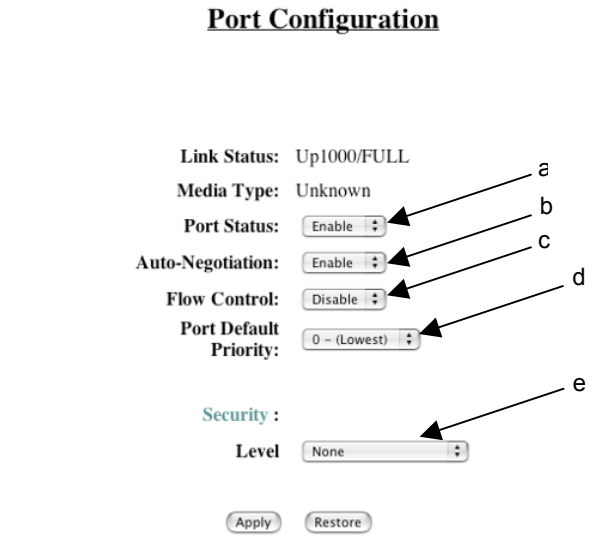
   a. Port Status (enable or disable); enabling this feature provides information about the selected port to use for diagnostic and management activities

   b. Auto-Negotiation (enable or disable); enabling this feature makes it possible for the switch to automatically negotiate the fastest speed for transferring data

   c. Flow control (enable or disable); enabling this makes use of the 802.3x full duplex and flow control feature

   d. Default priority (0-Lowest, 7-Highest); using this configures the access port or the Class of Service (CoS) default priority for the port

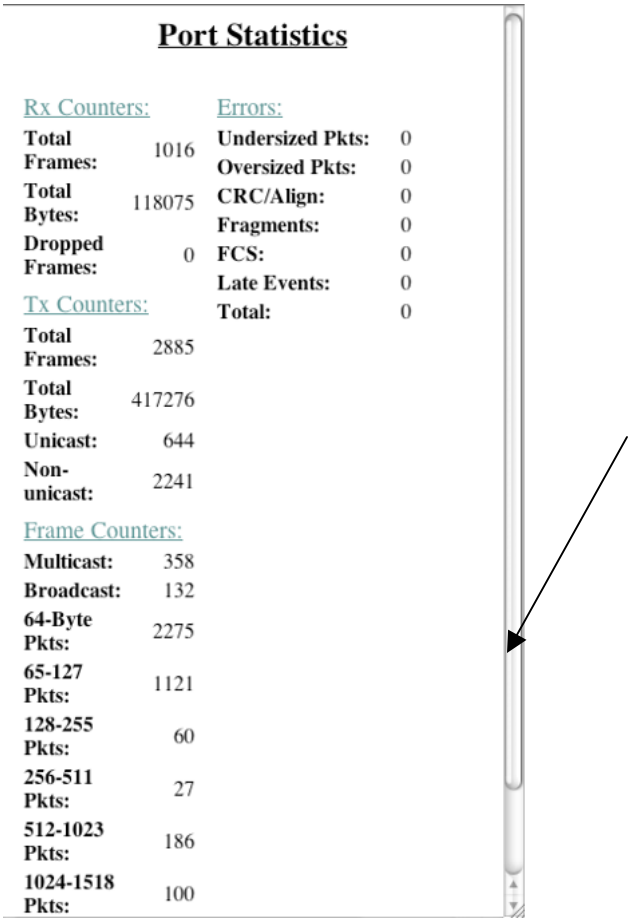
   e. Security level (1- new node trap, 2- intruder lock port, 3- intruder lock MAC); using this feature protects the network from unsolicited messages sent by an SNMP agent to an SNMP manager.



From this screen, you can also navigate between different ports and go to different units in the network. To go to another port number change the port number at the top of the screen and press Go.

You can set how the system updates the statistics about the selected port you selecting Auto or Manual and press Refresh.

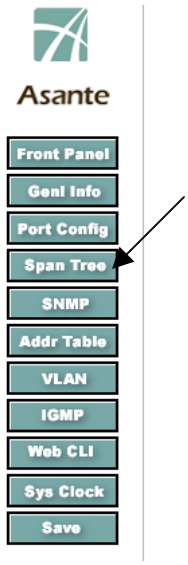
Use the scroll bar on the right side of the screen to view port statistics about the received counters, transmitted counters, errors, frame counters and collisions.



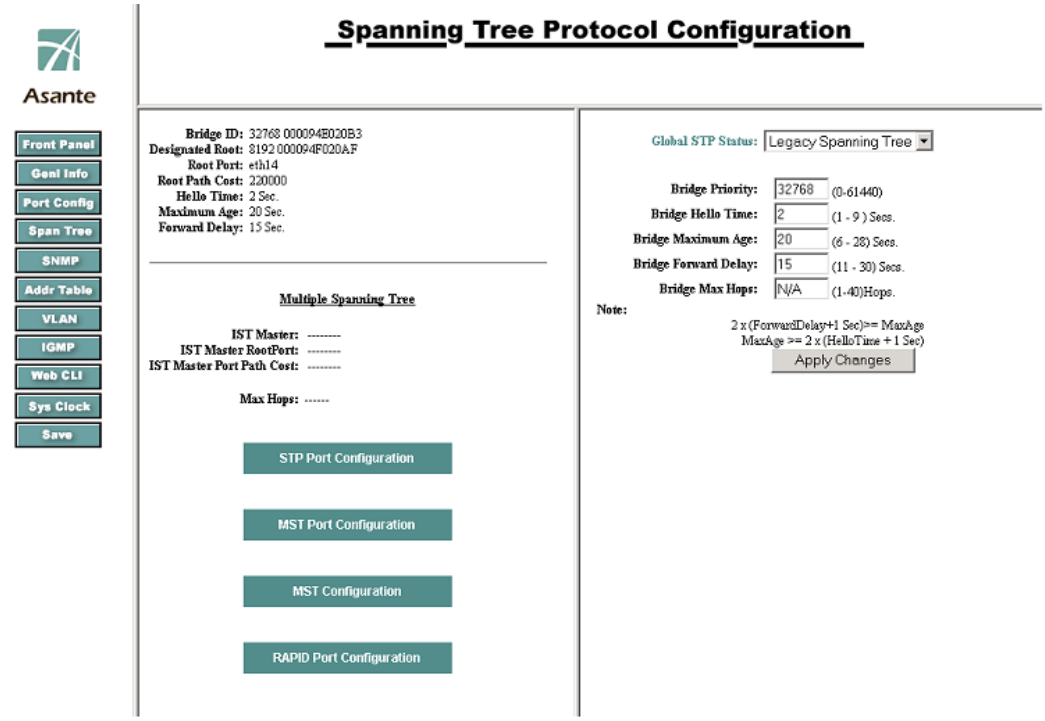
9.4 Spanning Tree Protocol Configuration

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, a message is broadcast through multiple paths, leading to 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 traffic, 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).

To access the Spanning Tree Configuration screen click on the Span Tree button in the menu bar on the left side of the screen.



Use the Spanning Tree Protocol Configuration screen to view information and configure spanning trees. The information about current spanning trees displayed on the left side of the screen include the bridge ID, designated root, root port, root port cost, hello time, maximum age and forward delay information. Use the right side of the screen to enable or disable Global STP Status, change the bridge priority, bridge hello time, bridge maximum age and bridge forward delay. The following example shows the Spanning Tree Protocol Configuration screen.



9.4.1 STP Port Configuration

Use this screen to change the priority and the path cost for specific ports. The priority default value is 128, and the value range is 0–240 (in multiples of 16).

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 of the equation:

Path cost = 1000/LAN speed (in Mbps)

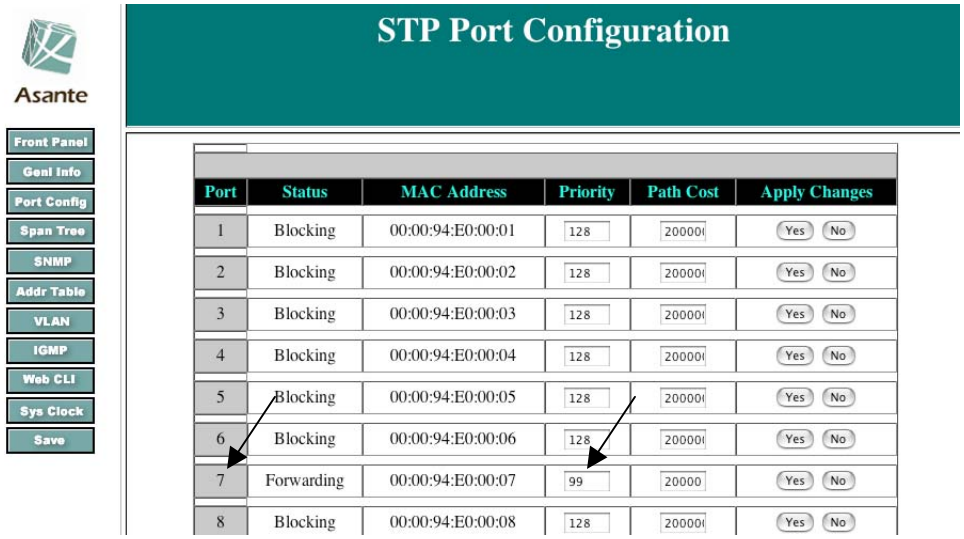
Therefore, for 10 Mbps ports, the default port path cost is 100. For 100 Mbps ports, it is 10. To allow for faster networks, the port path cost for a 1000 Mbps port is set by the standard at 4.

The default values for path cost is determined by the operating port speed:

- For ports operating in 1000Mb speed, the path cost is 20000
- For ports operating in 100Mb speed, the path cost is 200000
- For ports operating in 10Mb speed, the path cost is 2000000

To configure spanning-tree, click on the STP Port Configuration hyperlink.

Use the scroll bar on the right side of the screen to view additional ports. The following example shows setting port 7 priority to 99 using the STP Port Configuration screen.



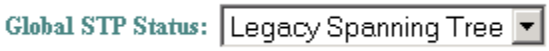
9.4.2 Global STP Bridge Configuration

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:

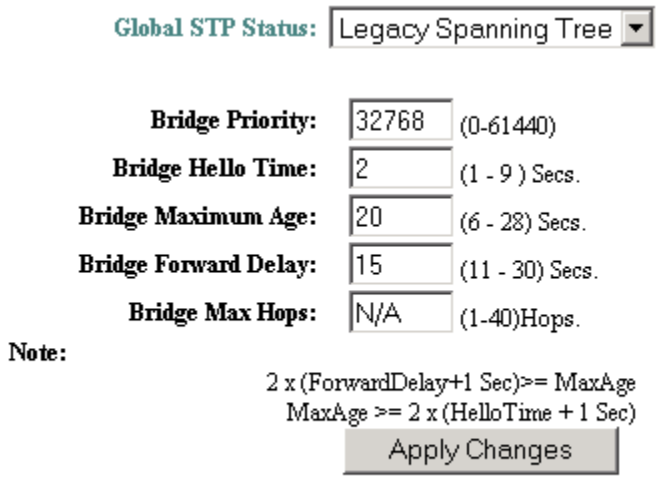
- Elect a single bridge to be the root bridge
- Calculate the shortest path from each bridge to the root bridge
- Select a designated bridge on each segment, which lies closest to the root and forwards all traffic to it
- Select a port on each bridge to forward traffic to the root

- Select the ports on each bridge that forward traffic, and place the redundant ports in blocking states

To change the global STP status, select the desired state from the drop down menu.



Use this screen to change the bridge priority, hello time maximum age, forward delay by entering the desired time in the text boxes and pressing Apply Changes. The allowed ranges are next to each text box.



To restore the defaults press the restore button.

The defaults are:

Bridge Priority: 32768

Bridge Hello Time: 2 seconds

Bridge Maximum Age: 20 seconds

Bridge Forward Delay: 15 seconds

Using multiple spanning trees allow VLAN groups to maintain a stable path between all VLAN members. This reduces the overall amount of protocol traffic crossing the network and provides a shorter reconfiguration time if any link in the spanning tree fails.

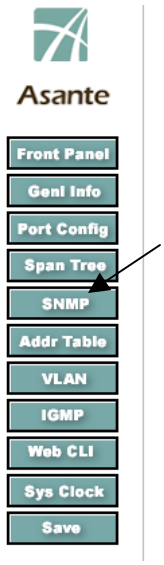
9.5 SNMP Configuration

SNMP allows network managers to obtain specific performance and configuration information from a software agent on a remote-network device. SNMP allows different types of networks to communicate by exchanging network information through messages known as protocol data units (PDUs). The IntraCore IC36240 supports SNMPv1, v2 and v3. The SNMPv3 protocol has improved the authentication, access control, and security methods

Use this screen to set the read/write access and to enable or disable the trap authentication for this switch. The default SNMP read community access is public; the default SNMP write community access is private; the default trap authentication is disable.

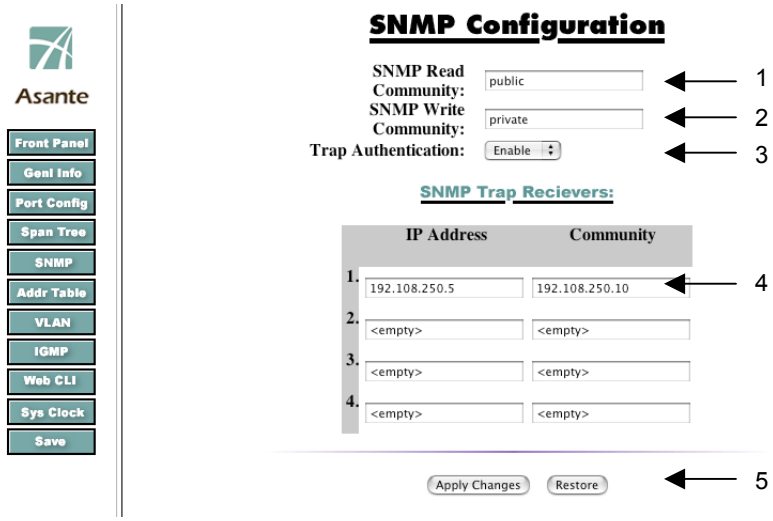
You can also set SNMP Traps for specific IP addresses allowing them to have access to communities that is different then the default set for the switch.

To access the SNMP Configuration screen click on the SNMP button on the left side of the screen.



The following example shows assigning an IP address to a specific community.

1. Type public in the SMNP Read Community text box; public indicates anyone on the network has read access to your network
2. Type private in the SNMP Write Community text box; private means that access is restricted
3. Select Enable from the Trap Authentication drop down menu; select enable to allow the switch to authenticate access
4. Type in the IP address and Community address; SNMP addresses to be trapped
5. Click on Apply Changes



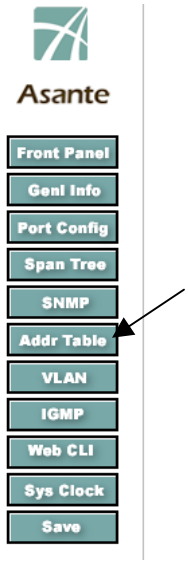
To restore the defaults press the Restore button.

9.6 Address Table Screen

Use this screen to view IP address tables. From the main screen you can view the status of each ports, the address counts of the VID, IP and MAC addresses. You can search for specific IP and MAC addresses and sort the results either IP or MAC. The display is sorted by IP address.

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 to 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.

To access this screen, click on Addr Table in the menu bar on the left side on the screen.



The following example shows the Address Table screen.

MAC and IP address Counts (Click on Port number to show Port-based addr table or All to show All Ports)																								
Unit: 1																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	All
IP	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	31	0	0	0	0	0	0	0	0	32
MAC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	77	0	0	0	0	0	0	0	0	78

MAC and IP address Counts (Click on the VID number to show VLAN-based addr table)	
VID	1
IP	32
MAC	78

Search for IP: 0.0.0.0 GO

Search for MAC: 00:C0:02:DC:00:67 GO

Sort by IP

Sort by MAC

16 Address Table D = Dynamic, S = Static, * = Multiple IP

Unit	Port	Entry	IP Address	MAC Address	VID
1	16	D	192.108.250.2	00:60:08:A6:B6:8B	1
1	16	D	192.108.250.6	00:00:94:7B:04:43	1
1	16	D	192.108.250.8	08:00:20:7A:2D:CF	1
1	16	D	192.108.250.10	00:0A:95:C4:E8:0A	1
1	16	D	192.108.250.16	00:80:5F:FE:2F:2D	1
1	16	D	192.108.250.17	00:80:5F:A6:B1:C6	1
1	16	D	192.108.250.19	00:0D:60:83:6A:4A	1
1	16	D	192.108.250.25	00:60:08:8F:27:BB	1
1	16	D	192.108.250.26	00:A0:24:9A:1E:4E	1

Click on the port number to filter the display and show the address table for a specific port.

MAC and IP address Counts (Click on Port number to show Port-based addr table or All to show All Ports)																								
Unit: 1																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	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	1
MAC	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2

The following screen shows the output from selecting Port 1. The Address table at the bottom of the screen filtered out all the ports except port 1.

MAC and IP address Counts (Click on Port number to show Port-based addr table or All to show All Ports)																								
Unit: 1																								
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	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	1
MAC	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2

MAC and IP address Counts (Click on the VID number to show VLAN-based addr table)	
VID	1
IP	1
MAC	2

Search for IP: 192.108.250.10 GO

Search for MAC: 00:0A:95:C4:E8:0A GO

Sort by IP

Sort by MAC

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

Unit	Port	Entry	IP Address	MAC Address	VID
self	self	I	192.108.250.95	00:00:94:E0:00:01	1
1	13	D	--------	00:0A:95:C4:E8:0A	1
Unit	Port	Entry	IP Address	MAC Address	VID

The MAC address of the switch is identified as “self”.

To sort the Address Table by IP address, click the Sort by IP button. The table is now sorted numerically by IP address.

Sort by IP

Sort by MAC

16 Address Table D = Dynamic, S = Static, * = Multiple IP

Unit	Port	Entry	IP Address	MAC Address	VID
1	16	D	192.108.250.2	00:60:08:A6:B6:8B	1
1	16	D	192.108.250.6	00:00:94:7B:04:43	1
1	16	D	192.108.250.8	08:00:20:7A:2D:CF	1
1	16	D	192.108.250.10	00:0A:95:C4:E8:0A	1
1	16	D	192.108.250.14	00:00:94:A0:A5:2C	1
1	16	D	192.108.250.16	00:80:5F:FE:2F:2D	1
1	16	D	192.108.250.17	00:80:5F:A6:B1:C6	1
1	16	D	192.108.250.19	00:0D:60:83:6A:4A	1
1	16	D	192.108.250.25	00:60:08:8F:27:BB	1

The MAC Address 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.

To sort the Address Table by MAC address, click the Sort by MAC button. Your table will be sorted numerically by MAC address.

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

Unit	Port	Entry	IP Address	MAC Address	VID
1	16	D	--------	00:00:74:8B:76:C5	1
1	16	D	--------	00:00:94:5E:54:39	1
1	16	D	--------	00:00:94:75:31:DB	1
1	16	D	--------	00:00:94:75:42:AE	1
1	16	D	--------	00:00:94:75:6A:3C	1
1	16	D	--------	00:00:94:78:54:32	1
1	16	D	--------	00:00:94:78:57:AB	1
1	16	D	--------	00:00:94:7A:A1:C4	1
1	16	D	--------	00:00:94:7B:03:B4	1
1	16	D	--------	00:00:94:7B:04:43	1

9.7 VLAN Configuration

VLANs are used to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group and eliminate broadcast storms in large networks. VLANs provide a secure and efficient network environment.

VLANs are based on untagged port groups, or traffic can be explicitly tagged to identify the VLAN group to which it belongs. Untagged VLANs can be used for small networks attached to a single switch. Tagged VLANs should be used for larger networks, and all the VLANs assigned to the inter-switch links.

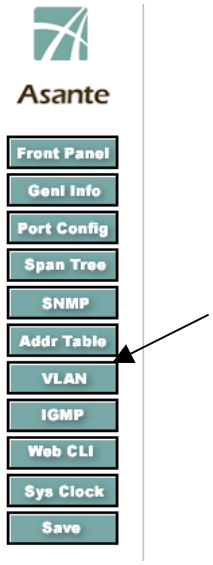
A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs is assigned. LAN port VLAN membership is assigned manually on an port-by-port basis. VLANs can be defined as either Layer 2 or Layer 3 and a VLAN cannot switch between the two layers. Before you create a VLAN, you must decide how they will be created and a naming convention to ensure duplicate VLAN names are not used.

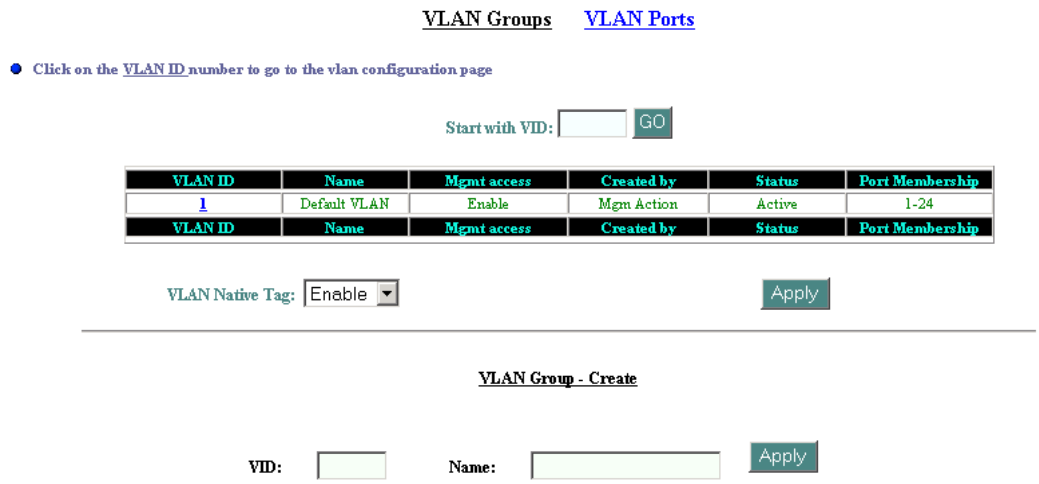
Up to 4094 Virtual LANs (VLANs) are supported on the IntraCore IC36240. The default VLAN with VLAN ID (VID) 1. All switchports (eth1–eth24) are included in the default VID 1. **The default VID 1 cannot be deleted**.

Use this screen to view VLAN information and create a VLAN group. At the top of the main VLAN screen you can toggle between VLAN group information and VLAN port information by click on each link.

To access the VLAN configuration screen click on VLAN in the menu bar on the left side of the screen



To sort the display enter the VLAN ID number you want the display to start with and press GO. The following example shows the output from the VLAN Group information screen.



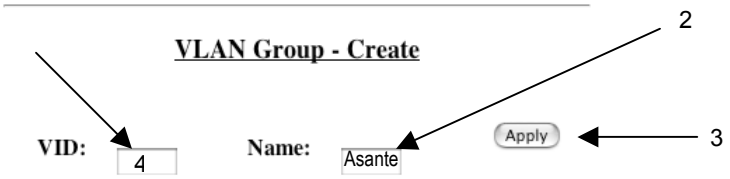
Assign a switchport to a VLAN by designating a membership mode. The membership mode determines the type of traffic the port carries and the number of VLANs allowed on that port. There are two membership modes:

- Static—A static-access port can belong to one VLAN and is manually assigned to that VLAN
- Trunk—By default, a trunk port is a member of all VLANs. Membership can be limited by configuring a VLAN Allowed List

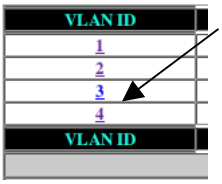
The following steps show creating a new VLAN 4 with the name To create a new VLAN and link it to a specific port from the main VLAN Group-Create menu follow these steps:

1. Type the new VLAN number in the VID box
2. Assign a name for the VLAN

3. Click Apply



4. Click on the VLAN ID number in the VLAN table to move to the configuration page for the new VLAN



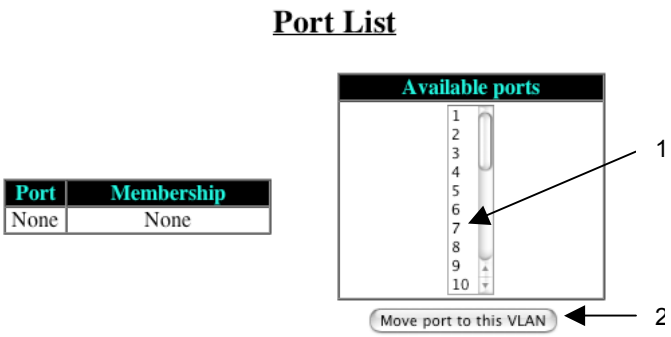
From the VLAN Group Configuration page, you can enable or disable the management access and link a VLAN to a specific port.

Use the VLAN feature to partition a single IntraCore IC36240 into a VLAN each containing its own set of ports. Packets are forwarded only between ports belonging to the same VLAN. This allows you to restrict access from one segment to another to increase network security or to reduce traffic. To set up VLANs you should specify the ports belonging to the VLAN, the set the IP configuration, individual access map associated with a set of VLANs and enable tagging. Once you have configured the VLAN and copied the information into the startup-config file, the VLAN information applies to the default.

Follow these steps:

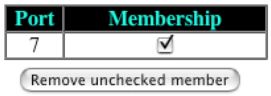
The scroll menu on the right side of the screen shows the available ports.

1. Click on a port number that the VLAN will be associated with from ports scroll menu.



2. Click on the Move port to this VLAN button

   The box on the left side of the screen confirms the VLAN was linked to the desired port.

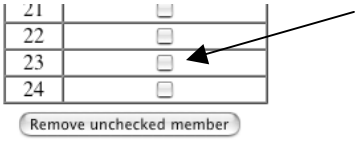


The following example shows output from creating a new VLAN (4) with the name Asante and assigning it to port 7.

VLAN ID	Name	Created by	Status	Port Membership
1	Default VLAN	Mgm Action	Active	1-6,8-24
2	network	Mgm Action	Inactive	None
3	Net	Mgm Action	Inactive	None
4	Asante	Mgm Action	Active	7
VLAN ID	Name	Created by	Status	Port Membership

To remove a VLAN from an associated port follow these steps:

1. Click the membership check box of the desired port to deselect the association.



2. Click on the Remove unchecked member button.

9.8 IGMP Configuration

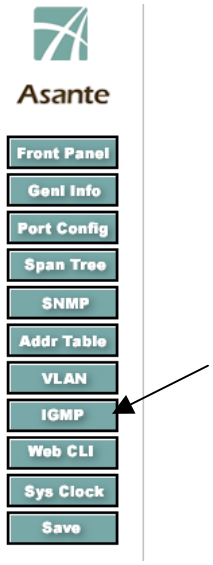
The Internet Group Management Protocol (IGMP) manages the multicast groups on a LAN. IP hosts use IGMP to report their group membership to directly connected multicast switches. Switches executing a multicast routing protocol maintain forwarding tables to forward multicast datagrams. Switches use the IGMP to learn whether members of a group are present on their directly attached sub-nets. Hosts join multicast groups by sending IGMP report messages.

IGMP uses group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255.

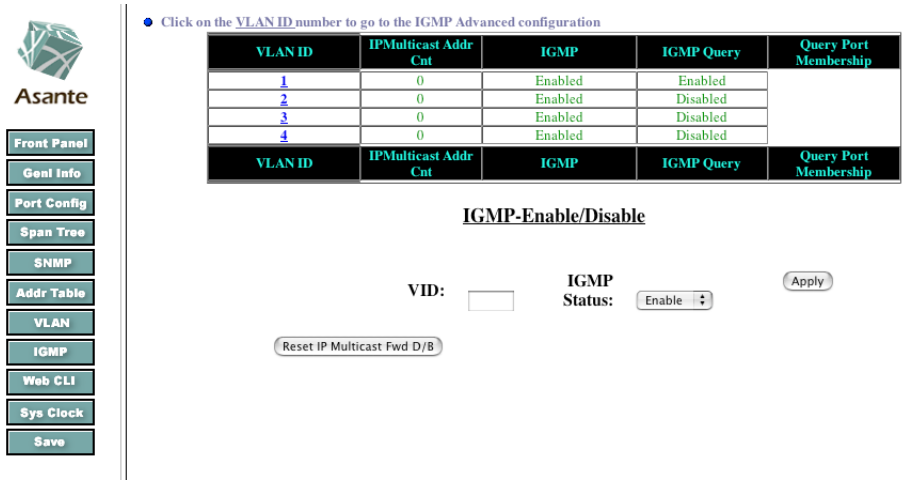
The address 224.0.0.0 will not be assigned to any group. The address 224.0.0.1 is assigned to all systems on a sub-net. The address 224.0.0.2 is assigned to all switches on a sub-net.

Multicast switches elect a designated switch for the LAN (subnet). The designated switch is the one with the highest IP address. The switch is responsible for sending IGMP host-query messages to all hosts on the LAN. By default, the designated switch sends IGMP host-query messages every 60 seconds in order to keep the IGMP overhead on hosts and networks very low.

To access the IGMP configuration screen click on the IGMP button in the menu bar on the left side of the screen.



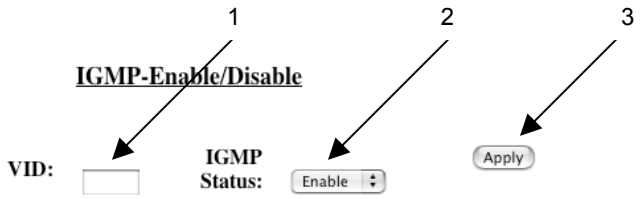
The following example shows the IGMP main screen. Use this screen to view the IGMP information. To enable or disable IGMP on a specific VLAN by entering the VLAN ID number selecting the desired state and clicking apply. Click on the VLAN ID number access the advanced IGMP configuration screen.



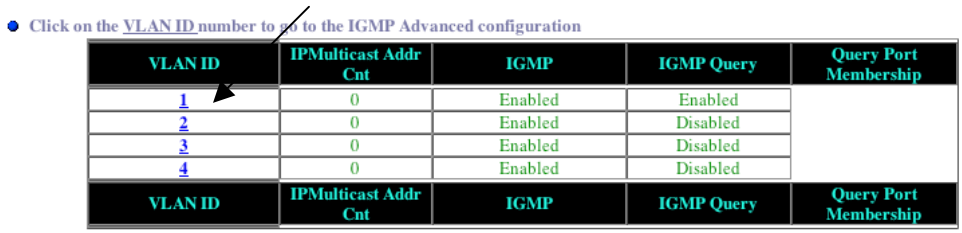
Follow these steps to enable or disable the transmit query packet status

1. Enter the VLAN ID number
2. Select enable or disable from the drop down menu

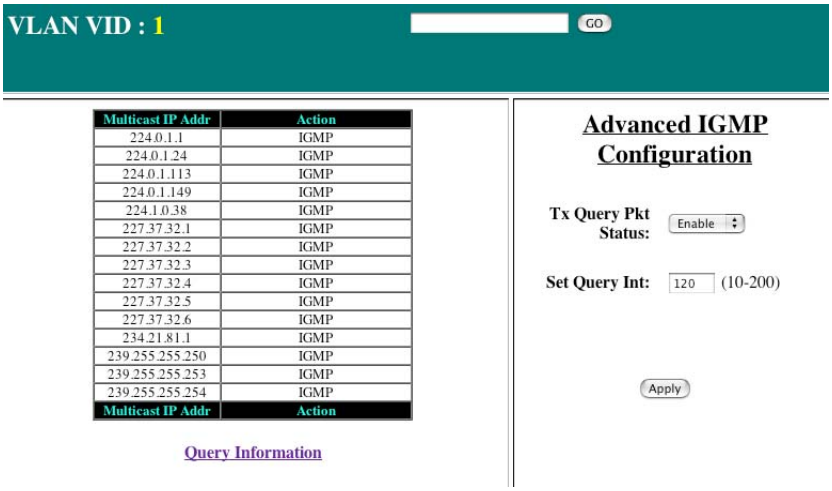
3. Click Apply



To configure a specific VLAN click on the VLAN ID number access the advanced IGMP configuration screen.



The following example shows the IGMP information for VLAN1.



Multicast switches send IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-systems group address of 224.0.0.1 with a time-to-live (TTL) value of 1.

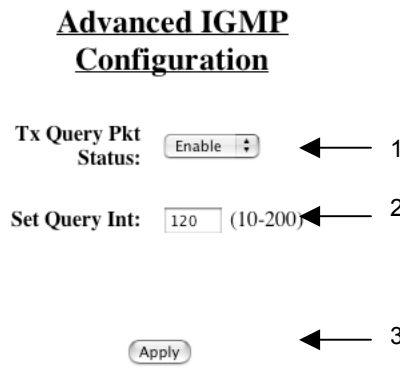
Multicast switches continue to periodically send host-query messages to refresh their knowledge of memberships present on their networks. If, after some number of queries, the switch software discovers that no local hosts are members of a multicast group, the software stops forwarding onto the local network multicast packets from remote origins for that group and sends a prune message upstream toward the source.

To enable or disable and to set the query intervals follow these steps.

1. Select enable or disable from the drop down menu

2. Enter the desired query interval (10-200)

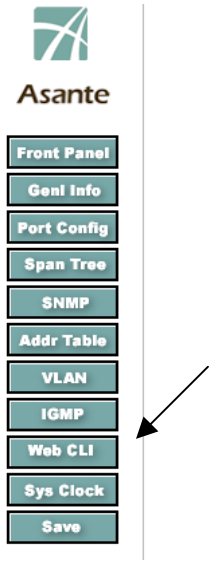
3. Click Apply



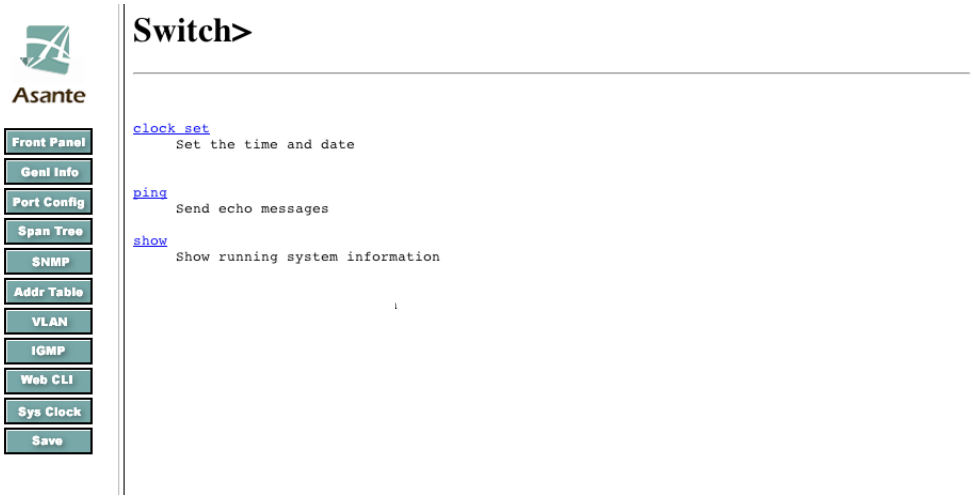
9.9 Web CLI Screen

Use the Web Command Line Interface (CLI) screen to use access the CLI from an http server. This feature provides the flexibility of the CLI with the usability of the GUI. You can set the clock, ping the system and show the running configuration.

To access the Web CLI Screen click on the Web CLI button in the menu bar on the left side of the screen.



The following example shows the main access point of the CLI from the Web interface.



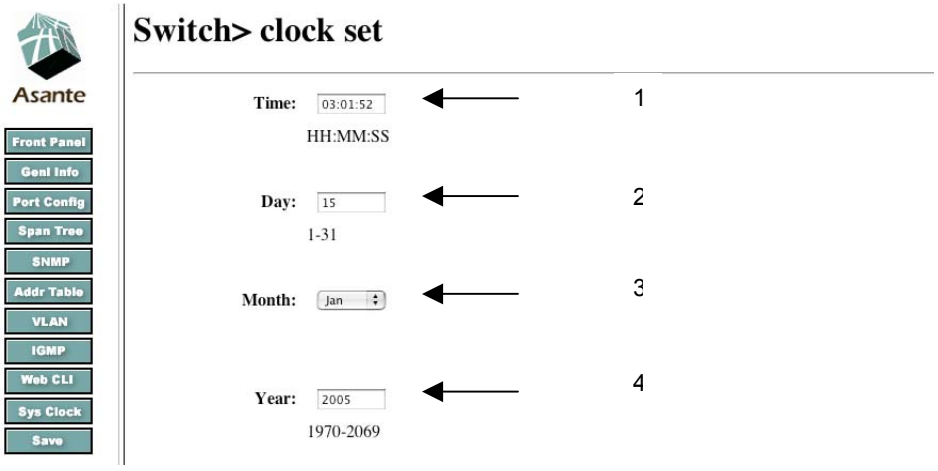
9.10 System Clock Menu

You can set the system clock from the System Clock Menu. After selecting the correct date and time for the system click apply. The operation resets the switch using the time you specify. This operation takes a few minutes to complete. View the changes using the General Information menu or the show system clock command in the Web CLI menu.

From this menu enter the following:

1. Enter the time (HH:MM:SS)
2. Enter the day of the month (1-31)
3. Select the month from the drop down menu
4. Enter the year

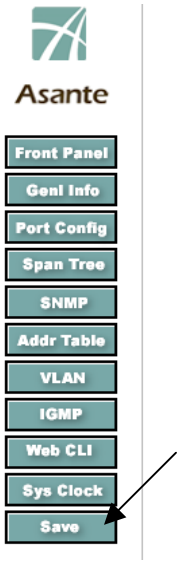
The following example shows the main screen of the System Clock menu.



After you set the desired date and time click apply.

9.11 Save

Click on Save to automatically retain any configuration changes you made.



Appendix A: Basic Troubleshooting

In the unlikely event that the switch does not operate properly, follow the troubleshooting tips below. If more help is needed, contact Asante's technical support at www.asante.com/support.

Problem	Possible Solutions
The Power LED is not lit.	Check the power connection. Plug the power cord into another known working AC outlet. The primary power supply has failed. Install the optional external power supply and have the primary power supply serviced as soon as possible.
The System LED is amber.	The switch detects a hardware malfunction. Check the temperature of the room, listen for the fan or the electrical connection.
The External Power LED is not lit.	The external power supply is not installed properly or has failed. Contact Asante immediately for a replacement.
The 10/100/1000 port Link LEDs are not lit.	Check the 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 *Chapter 2.6: Connecting to the Network* for more information.
The GBIC Link LED is not lit.	Check the 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.).	• Make sure the Link LED for the port in use is on. Make sure the correct cable type is used. See *Chapter 2.6 Connecting to the Network* for more information on cabling procedures • Make sure the IP address, subnet mask, and VLAN membership of the switch are correct • Make sure the switch port and the device are both 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).

Appendix B: Specifications

The sections below list the features and product specifications for the IntraCore IC36240 switch.

Connectors:	24 RJ-45 auto-MDI/MDIX
Ports	24 10/100/1000BaseT ports that have auto-negotiation for speed, duplex mode and flow control
Gig Modular Ports	4 SFP slots for 1000SX or 1000LX transceiver that is auto-disabling 1000BaseT port when link is activated.
Switch ASIC	StrataXGS BCM5697
Gigabit PHY	5 x BCM5464R, 1 x BCM5464SR Quad
Management CPU	266 Mhz Motorola MPC8245
Console:	Serial (RS-232): DB9, USB
Status Indicators:	Separate link-activity, speed (10/100/Gigabit) and duplex (full or half) LEDs for each port; system power, external power supply and fan.

Physical Characteristics

Dimensions:	Size: 17.5 x 12.7 x 1.7 inches (440 x 322 x 45 mm); 1 RU height
Mounting:	Install into a standard 19" rack or place on a desktop; rackmount kit included.

Environmental Range

Operating Temperature:	32º to 104ºF (0º to 40ºC)
Relative Humidity:	5% to 95% non-condensing
Power:	Auto-switching, 90-240 VAC, 50/60 Hz; grounded IEC cord
External Power Supply:	12 VDC Auto-switching from main 90/240 VAC for emergency backup

Performance

Frames	9 KB Jumbo frames, 12 Gbps interconnect, non-blocking
MAC addresses	16 K entries
Memory	64 MB SDRAM, 2 MB embedded packet bugger
VLANs	1k configurable port-based or mac-based, 4k VLAN ID, Private VLAN, IGMP snooping
Priority Queues	8 levels IEEE 802.1p
Spanning Tree	256 spanning tree group (IEEE 802.1D), fast forwarding proprietary (IEEE 802.1p), rapid spanning tree (IEEE802.1w), 32 instances of per VLAN (IEEE 802.1s)
Link Aggregation	12 trunks x 8 ports/trunk, IEEE 802.3ad, Cisco EtherChannel
Bandwidth Management	IEEE 802.1p COS, TOS, DSCP, TCP/UDP port number

Security	User password, SNMP access filter, port security (MAC address filter with notification), 802.1x (port-based, L2/L4 ACL, RADIUS, TACACS+
Management	Male DB9 RS-232 DTE (auto baud to 115k), USB, Cisco CLI x 4 sessions, Web RMON (1, 2, 3, 9), port mirroring
Firmware Upgrade	TFTP, dual banks of code and configuration
SNMP	v1, v2, v3
Logs	System, Crash, Error

B.1 Standards Compliance

IEEEE:	IEEE 802.1D spanning tree and bridge filters IEEE 802.1p prioritization (class of service) IEEE 802.1Q virtual LAN (VLAN) IEEE 802.1s VLAN per spanning tree IEEE 802.1w rapid reconfiguration spanning tree IEEE 802.1x port based L2/L4 ACL, RADIUS, TACACS+ IEEE 802.3x full duplex and flow control IEEE 802.3z 1000BaseSX over 50µ multi-mode fiber; max. 1,804' (550 m) IEEE 802.3ab 1000BaseT over Category 5 UTP (4 pairs); max. 328' (100 m) IEEE 802.3u 100BaseTX over Category 5 UTP (2 pairs); max. 328' (100 m) IEEE 802.3 10BaseT over Category 3 UTP (2 pairs); max. 328' (100 m)
IETF:	RFC 1155 SMI RFC 1157 SNMP RFC 1212, 1213, 1215 MIB II and Traps RFC 1493 Bridge MIB RFC 1724 RIPv2 MIB RFC 1757 RMON 4 Groups (Statistics, History, Alarms, and Events) RFC 2096 IP-FORWARD-MIB RFC 2674 Bridge Extensions Asante Private MIB
Safety:	UL 1950, cUL, TUV/GS
Emissions:	FCC Class A, CE

B.2 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 second business day (within the United States) advanced replacement, and software maintenance agreement.
AsanteCare™:	Optional extended technical support and product warranty for 1–2 additional years.

See *Appendix C: FCC Compliance and Warranty Statements* for more detailed information.

Appendix C: FCC Compliance and Warranty Statements

C.1 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 you will be required to correct the interference at your own expense.

C.2 Important Safety Instructions

Caution: Do not use an RJ-11 (telephone) cable to connect 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 (such as by placing the product on a bed, sofa or rug). 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, which is 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 people 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.

C.3 IntraCare Warranty Statement

Products:	IntraCore IC36240
Duration:	3 years
Advanced Warranty	United States: Second Business Day
Replacement:	Other countries: See your local distributor or reseller

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

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

3. Asante does not warrant that the operation of Asante products will be uninterrupted or error free. If Asante 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. Asante 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 Asante.

6. Warranty does not apply to defects resulting from (a) improper or inadequate maintenance or calibration, (b) software, interfacing, parts, or supplies not received from Asante, (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 PREVIOUS WARRANTIES ARE EXCLUSIVE AND NO OTHER WARRANTY OR CONDITION, WHETHER WRITTEN OR ORAL, IS EXPRESSED OR IMPLIED AND ASANTE SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE.

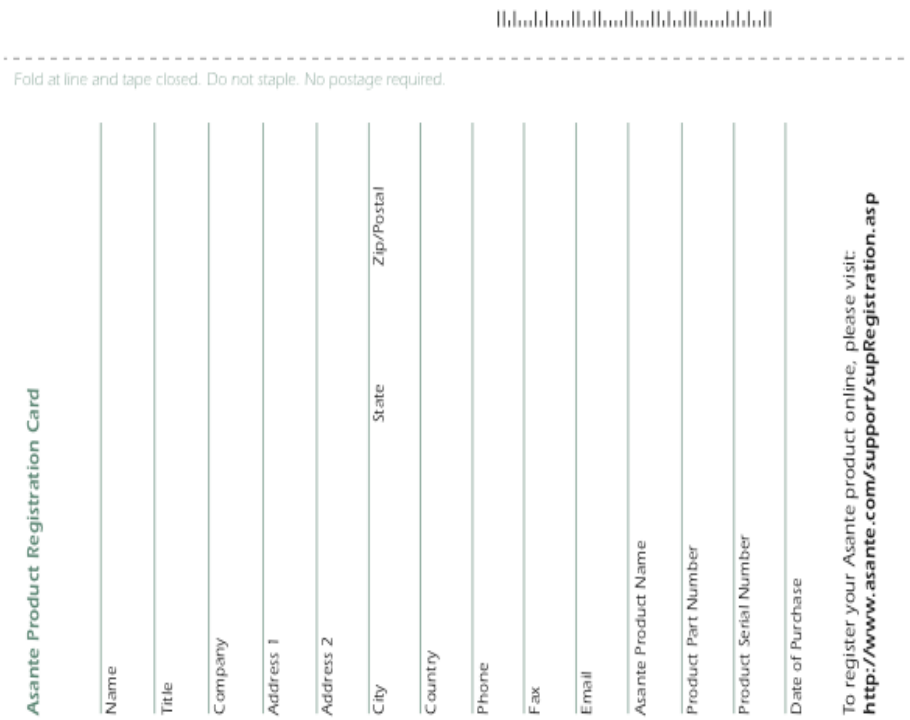
8. Asante will be liable for damage to tangible property per incident up to the greater of $10,000 or the actual amount paid for the product that is the subject of the claim, and for damages for bodily injury or death, to the extent that all such damages are determined by a court of competent jurisdiction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

9. TO THE EXTENT ALLOWED BY LOCAL LAW, THE REMEDIES IN THIS WARRANTY STATEMENT ARE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. EXCEPT AS INDICATED PREVIOUSLY, IN NO EVENT WILL ASANTE 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, 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 previous 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: Online Warranty Registration

Please register this product online at http://www.asante.com/support/supRegistration.asp or by filling out and mailing the card below.



Index