Management Software

AT-S29

User's Guide

FOR USE WITH THE AT-8324SX FAST ETHERNET SWITCH PRODUCT

VERSION 1.12

Allied Telesyn
Simply Connecting the World

PN 613-50115-00 Rev A

Allied Telesyn International, Corp. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn International, Corp. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn International, Corp. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

Chapter 1

Chapter 2

Chapter 4

Appendix A

Appendix B

Preface

This guide contains instructions on how to use the AT-S29 software to manage and configure your AT-8324SX Fast Ethernet Switch.

Supported Platform

Version 1.12 of the AT-S29 software is supported on the following Fast Ethernet switch:

❑ AT-8324SX Fast Ethernet Switch

This version supports the following optional modules for the switch:

❑ AT-BMGMT Management Module

❑ AT-BSTACK1 Stacking Module

❑ AT-B15/SX 1000Base-X Gigabit Expansion Module

❑ AT-B15/LX 1000Base-X Gigabit Expansion Module

❑ AT-B17 100Base-FX Expansion Module

Purpose of This Guide

This guide is intended for network administrators who are responsible for managing the switches. Network administrators should be familiar with Ethernet switches, Ethernet and Fast Ethernet technology, bridging, and the Spanning Tree Protocol (STP).

How This Guide is Organized

This guide contains the following chapters and appendices:

Chapter 1, **Switch Management**, explains switch configuration options and required switch connections.

Chapter 2, **Using the System Configuration Program**, describes how to configure the switch and its ports using the Telnet program or by connecting a terminal to the console port on the management module.

Chapter 3, **Web-Based Management**, explains how to configure the switch and its ports using a Web browser.

Chapter 4, **Advanced Topics**, describes networking concepts such as spanning tree algorithm and virtual LANs, SNMP, and RMON.

Appendix A, **Troubleshooting**, describes known problems and recommended solutions.

Appendix B, **Pin Assignments**, briefly describes different wiring assignments.

Where to Find Web-based Guides

The Allied Telesyn web site at www.alliedtelesyn.com offers you an easy way to access the most recent documentation and technical information for all of our products. All web-based documentation for this product and other Allied Telesyn products can be downloaded from the web site in pdf format.

There are several manuals that you will need in order to manage your Ethernet switch. Some guides are shipped with their respective products, while other manuals, such as this one, are only available from the Allied Telesyn web site.

The following manual contains the complete hardware installation instructions for the switch. You can obtain this manual from the Allied Telesyn web site.

- ❑ **AT-8324SX Fast Ethernet Switch Installation Guide**, PN 613-50118-00

The following manual is shipped with the switch and contains an abbreviated version of the installation instructions:

- ❑ **AT-8324SX Fast Ethernet Switch Quick Install Guide**, PN 613-50120-00

Document Conventions

This guide uses several conventions that you should become familiar with first before you begin to install the product.

Note
Notes provide additional information.

⚠ **Warning**
Warnings inform you that performing or omitting a specific action may result in bodily injury.

⚠ **Caution**
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Contacting Allied Telesyn Technical Support

There are several ways that you can contact Allied Telesyn technical support: online, telephone, fax and e-mail.

Online Support

You can request technical support online by filling out the Technical Support Form at www.alliedtelesyn.com/forms/support.htm.

Telephone and Fax Support

Americas
United States, Canada, Mexico,
Central America, South America
Tel: 1 (800) 428-4835, option 4
Fax: 1 (503) 639-3176

Asia
Singapore, Taiwan, Thailand, Malaysia,
Indonesia, Korea, Philippines, China,
India, Hong Kong
Tel: (+65) 381-5612
Fax: (+65) 383-3830

Australia
Tel: 1 (800) 000-880
Fax: (+61) 2-9438-4966

France
France, Belgium, Luxembourg,
The Netherlands, Middle East,
Africa
Tel: (+33) 0-1-60-92-15-25
Fax: (+33) 0-1-69-28-37-49

Germany
Germany, Switzerland, Austria, Eastern
Europe
Tel: (+49) 0130/83-56-66
Fax: (+49) 30-435-900-115

Italy
Italy, Spain, Portugal, Greece, Turkey, Israel
Tel: (+39) 02-416047
Fax: (+39) 02-419282

Japan
Tel: (+81) 3-3443-5640
Fax: (+81) 3-3443-2443

United Kingdom
United Kingdom, Denmark, Norway,
Sweden, Finland
Tel: (+0044) 1235-442500
Fax: (+44) 1-235-442680

E-mail Support

United States and Canada
TS1@alliedtelesyn.com

Latin America, Mexico, Puerto Rico, Caribbean, and Virgin Islands
latin_america@alliedtelesyn.com

United Kingdom, Sweden, Norway, Denmark, and Finland
support_europe@alliedtelesyn.com

Returning Products

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesyn without a RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn's Technical Support at one of the following locations:

North America
2205 Ringwood Ave
San Jose, CA 95131
Tel: 1-800-428-4835, option 4
Fax: 1-503-639-3716

European Customer Support Centre
10/11 Bridgemead Close
Westmead Industrial Estate
Swindon, Wiltshire SN5 7YT
England
Tel: +44-1793-501401
Fax: +44-1793-431099

Latin America, the Caribbean,
Virgin Islands
Tel: international code + 425-481-3852
Fax: international code + 425-483-9458

Mexico and Puerto Rico
Tel: 1-800-424-5012, ext 3852 or
1-800-424-4284, ext 3852
Mexico only: 95-800-424-5012, ext 3852
Fax: international code + 425-489-9191

FTP Server

If you need a driver for an Allied Telesyn device and you know the name of the driver, you can download the software by connecting directly to our FTP server at ftp://gateway.centre.com.

At login, enter ‘anonymous’. Enter your e-mail address for the password as requested by the server at login.

For Sales or Corporate Information

Allied Telesyn International, Corp.
19800 North Creek Parkway, Suite 200
Bothell, WA 98011
Tel: 1 (425) 487-8880
Fax: 1 (425) 489-9191

Allied Telesyn International, Corp.
960 Stewart Drive, Suite B
Sunnyvale, CA 94086
Tel: 1 (800) 424-4284 (USA and Canada)
Fax: 1 (408) 736-0100

Tell Us What You Think

If you have any comments or suggestions on how we might improve this or other Allied Telesyn documents, please fill out the Send Us Feedback Form at www.alliedtelesyn.com/forms/feedback.htm.

Chapter 1

Switch Management

Configuration Options

For advanced management capability, the AT-8324SX switch's AT-BMGMT Management Module provides a menu-driven system configuration program. This program can be accessed by a direct or modem connection to the serial port on the management module (out-of-band), or by a Telnet connection over the network (in-band).

The management module is based on SNMP (Simple Network Management Protocol). This SNMP agent permits a switch stack to be managed from any PC in the network using in-band management software.

The management module also includes an embedded HTTP Web agent. This Web agent can be accessed using a standard Web browser from any computer attached to the network.

The system configuration program and the SNMP agent support management functions such as:

- ❑ Enable/disable any port
- ❑ Set the communication mode for any port
- ❑ Configure SNMP parameters
- ❑ Select VLANs or multicast filtering
- ❑ Display system information or statistics
- ❑ Configure the switch to join a Spanning Tree Domain
- ❑ Download system firmware
- ❑ Restart the system

Making Connections for System Configuration

The switch includes a menu-driven configuration program. The ASCII interface to this program can be accessed by making a direct connection to the serial port on the Network Management Module, or by a Telnet connection to the switch over the network.

This section describes how to access the menu-driven configuration program via:

- ❑ Serial connection: A terminal or workstation connected to the serial port on the Network Management Module.
- ❑ Telnet connection: A workstation connected to a remote switch via a Telnet connection.

It also describes how to access the embedded Web agent over the network using any standard browser, or with the provided network management software or other third-party management software.

Serial Connection

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the Network Management Module. Use the null-modem cable provided with this package, or use a null modem connection that complies with the wiring assignments shown in Appendix B, Pin Assignments of this guide.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 9600 bps (for initial configuration). Also be sure to set flow control to "none." (Refer to **Configuring the Serial Port** on page 33 for a complete description of configuration options.)

In-Band Connections

Prior to accessing the Network Management Module via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using an out-of-band connection or the BootP protocol.

Telnet Connection

After configuring the switch's IP parameters, you can access the on-board configuration program from anywhere within the attached network using Telnet.

Note

Use the Network Configuration menu to specify the maximum number of simultaneous Telnet sessions that are supported by the system.

In-Band Network Connection

The on-board configuration program can be accessed using Telnet from any computer attached to the network. The switch and stack can also be managed by any computer using a Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above), or from a network computer using network management software.

Note

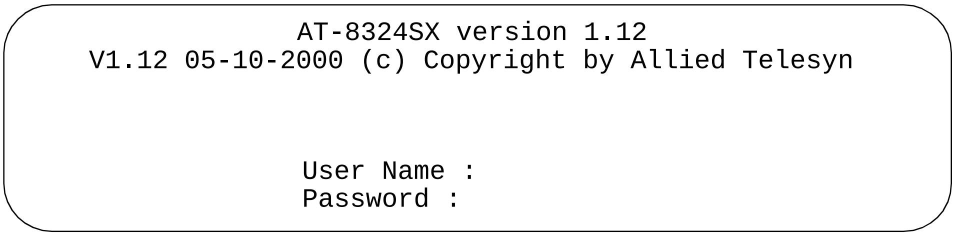
The on-board program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Chapter 2

Using the System Configuration Program

Login Screen

Once a direct connection to the serial port or a Telnet connection is established, the login screen for the on-board configuration program appears. If this is your first time to log into the configuration program, then the default user names are "admin" and "guest," with no password. The administrator has Read/Write access to all configuration parameters and statistics, while the guest has Read Only access to the management program.



```
                AT-8324SX version 1.12
   V1.12 05-10-2000 (c) Copyright by Allied Telesyn



                User Name :
                Password :
```

You should define a new administrator password, record it and put it in a safe place. Select Console Login Configuration from the Management Setup Menu and enter a a new password for the administrator. Note that passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

Note

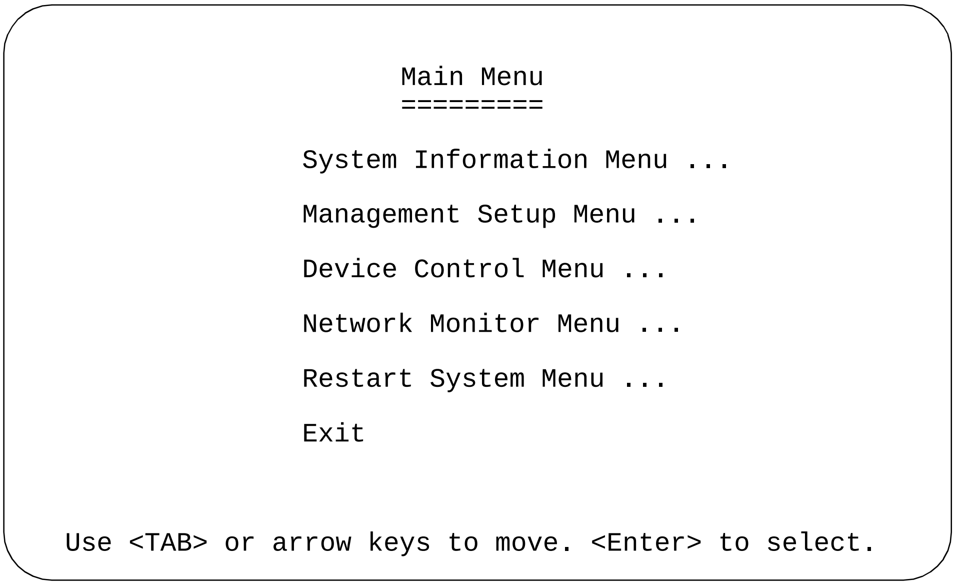
Based on the default configuration, a user is allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

Main Menu

With the system configuration program you can define system parameters, manage and control the switch, the connected stack and all its ports, or monitor network conditions. The figure below of the Main Menu and the following table briefly describe the selections available from this program.

Note

Options for the currently selected item are displayed in the highlighted area at the bottom of the interface screen.



```
                         Main Menu
                         =========

                  System Information Menu ...

                  Management Setup Menu ...

                  Device Control Menu ...

                  Network Monitor Menu ...

                  Restart System Menu ...

                  Exit


   Use <TAB> or arrow keys to move. <Enter> to select.
```

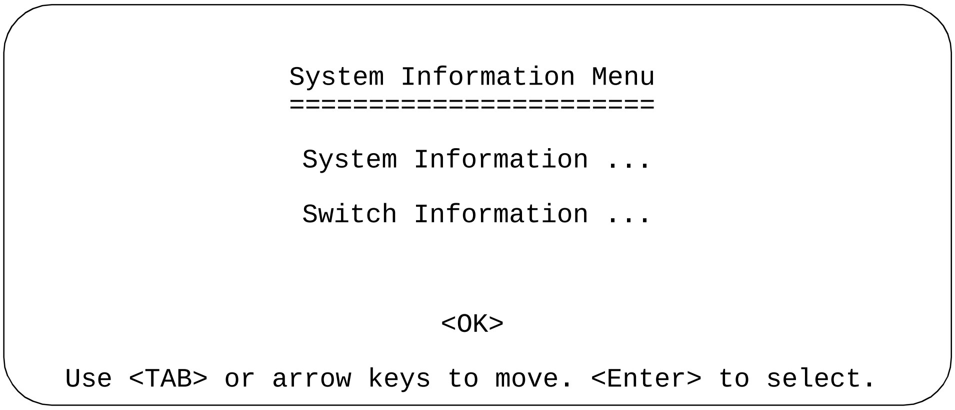
Menu	Description
System Information Menu:	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, power status, and expansion modules used in the stack.
Management Setup Menu:	
Network Configuration	Includes IP setup, Ping facility, HTTP (Web Agent) setup, Telnet enable, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; and configures communities and trap managers.
Console Login Configuration	Sets the user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Device Control Menu:	
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Port Information	Displays operational status, including link state, flow control method, and duplex mode.
Spanning Tree Configuration	Enables Spanning Tree Algorithm; also sets parameters for hello time, maximum message age, switch priority, and forward delay; as well as port priority and path cost.
Spanning Tree Information	Displays full listing of parameters for Spanning Tree Algorithm.
Mirror Port Configuration	Specifies the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.
Extended Bridge configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, GMRP multicast filtering, and VLAN extensions.
802.1P Configuration	Configures default port priorities and queue assignments.

Menu	Description
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members, or restricting ports from being dynamically added to a port by the GVRP protocol.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and GVRP.
Port GARP Configuration[1]	Configures settings used in multicast filtering.
Port GMRP Configuration[1]	Configures GMRP multicast filtering.
Network Monitor Menu:	
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full address listing, as well as search and clear functions.
Multicast Address Registration Table[1]	-
IP Multicast Registration Table	Displays all the multicast groups active on this switch, including multicast IP addresses and corresponding VLAN IDs.
Static Unicast Address Table Configuration	Used to manually configure host MAC address in the unicast table.
Static Multicast Address Table Configuration[1]	-
Restart System	Restarts system with options to use POST, or to retain factory defaults, IP settings, or user authentication settings.
Exit	Exits the configuration program.

[1] Not implemented in this firmware release.

System Information Menu

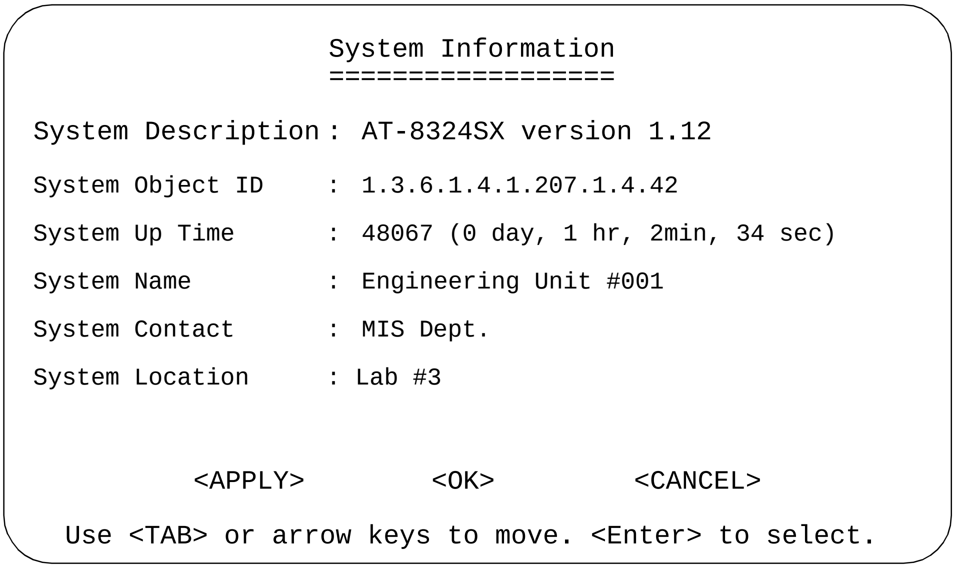
Use the System Information Menu to display a basic description of the switch, including contact information, and hardware/ firmware versions.



```
                System Information Menu
                =======================

                 System Information ...

                 Switch Information ...


                          <OK>

    Use <TAB> or arrow keys to move. <Enter> to select.
```

Displaying System Information

Use the System Information screen to display descriptive information about the switch or for quick system identification, as shown in the following figure and table.



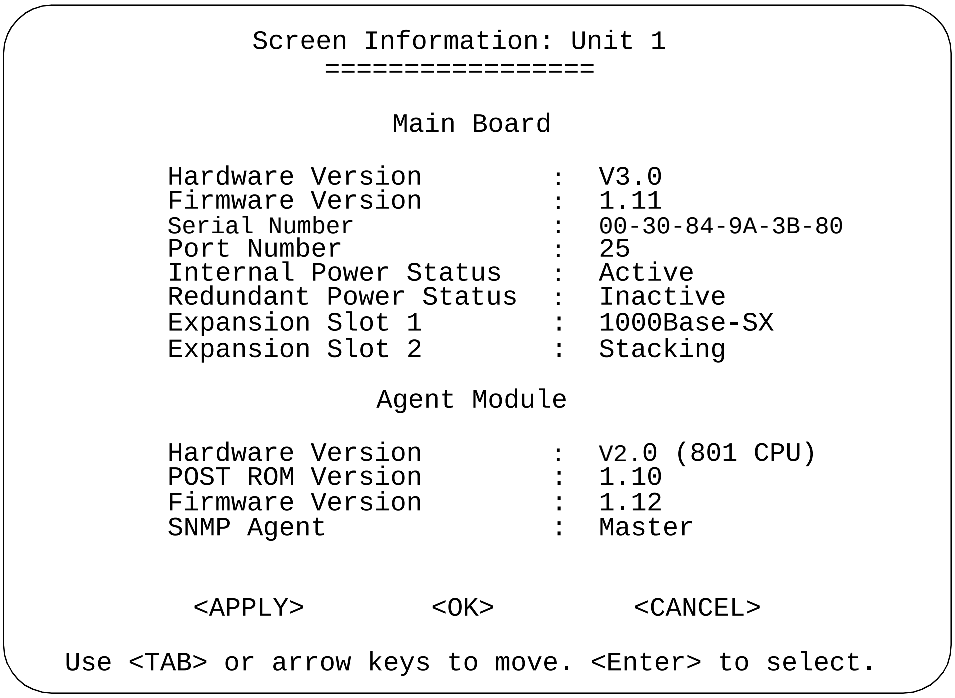
```
                       System Information
                       ==================

  System Description :  AT-8324SX version 1.12

  System Object ID    :  1.3.6.1.4.1.207.1.4.42

  System Up Time      :  48067 (0 day, 1 hr, 2min, 34 sec)

  System Name         :  Engineering Unit #001

  System Contact      :  MIS Dept.

  System Location     : Lab #3


              <APPLY>         <OK>         <CANCEL>

    Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
System Description	System hardware description.
System Object ID	MIB II object identifier for switch's network management subsystem (ATI: 207.1.4.42)
System Up Time	Length of time the current management agent has been running. (Note that the first value is 1/100 seconds.)
System Name[1]	Name assigned to the switch system.
System Contact[1]	Contact person for the system.
System Location [1]	Specifies the area or location where the system resides.

[1] Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

Displaying Version and Module Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board and agent modules, as well as the power status and modules plugged into the system.



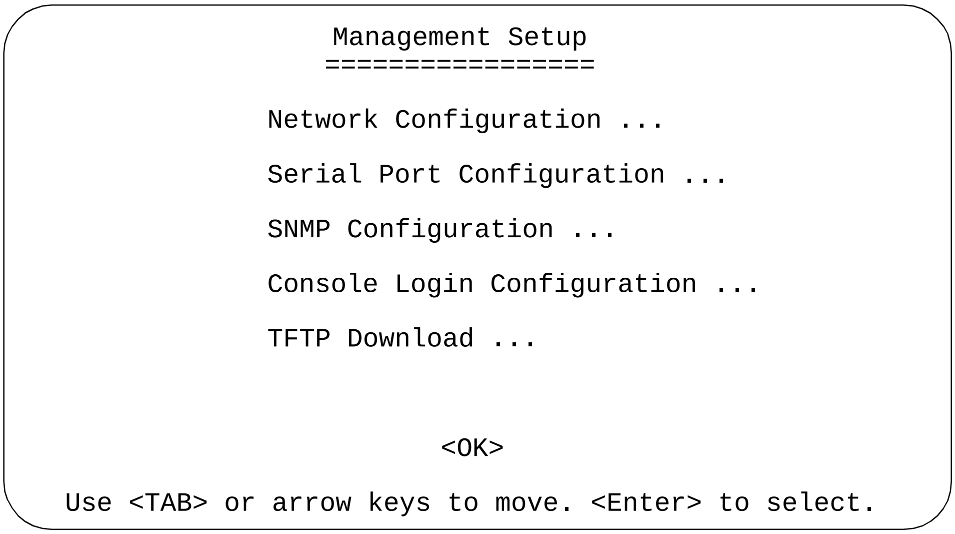
```
               Screen Information: Unit 1
                   =================

                          Main Board

          Hardware Version        :  V3.0
          Firmware Version        :  1.11
          Serial Number           :  00-30-84-9A-3B-80
          Port Number             :  25
          Internal Power Status   :  Active
          Redundant Power Status  :  Inactive
          Expansion Slot 1        :  1000Base-SX
          Expansion Slot 2        :  Stacking

                         Agent Module

          Hardware Version        :  V2.0 (801 CPU)
          POST ROM Version        :  1.10
          Firmware Version        :  1.12
          SNMP Agent              :  Master


            <APPLY>         <OK>          <CANCEL>

    Use <TAB> or arrow keys to move. <Enter> to select.
```

Menu	Description
Main Board:	
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	MAC address associated with the main board.
Port Number	Number of ports in this unit.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.
Expansion Slot 1	Shows module type if inserted (100Base-FX, 1000Base-SX, or 1000Base-LX).
Expansion Slot 2	Shows module type if inserted (100Base-FX, 1000Base-SX, 1000Base-LX, or Stack).

Menu	Description
Agent Module:	
Hardware Version	Hardware version of the agent module.
POST ROM Version	Power-On Self-Test version number.
Firmware Version	Firmware version of the agent module.
SNMP Agent	Shows if this module is Master or Backup.

Management Setup Menu

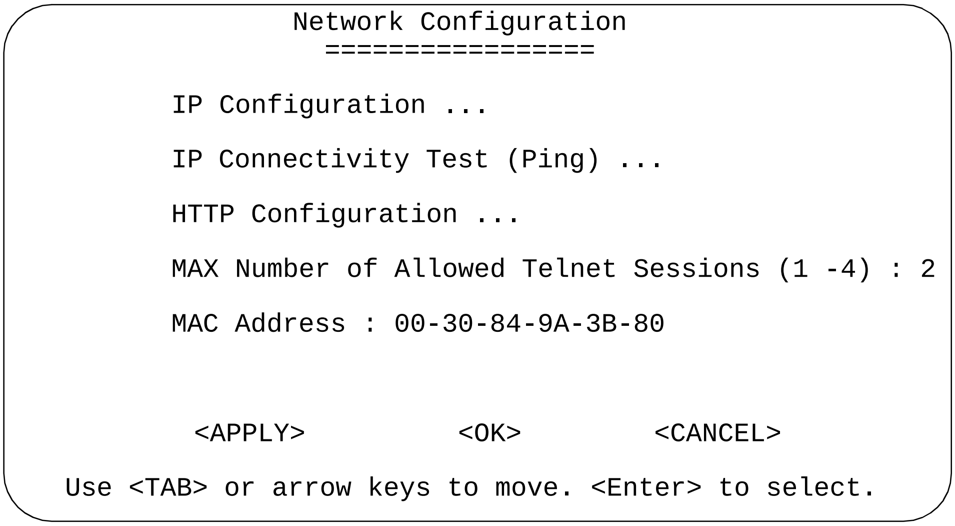
After initially logging onto the system, adjust the communication parameters for your console to ensure a reliable connection (Console Configuration menu). Specify the IP addresses for the agent module (Network Configuration / IP Configuration), and then set the Administrator and User passwords (Console Login Configuration). Remember to record them in a safe place. Also set the community string which controls access to the on-board SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.



```
                   Management Setup
                  =================

               Network Configuration ...

               Serial Port Configuration ...

               SNMP Configuration ...

               Console Login Configuration ...

               TFTP Download ...


                         <OK>

  Use <TAB> or arrow keys to move. <Enter> to select.
```

Changing the Network Configuration

Use the Network Configuration menu to set the bootup option, configure the switch’s Internet Protocol (IP) parameters, enable the on-board Web Agent, or enable Telnet access. The screen shown below is described in the following table.

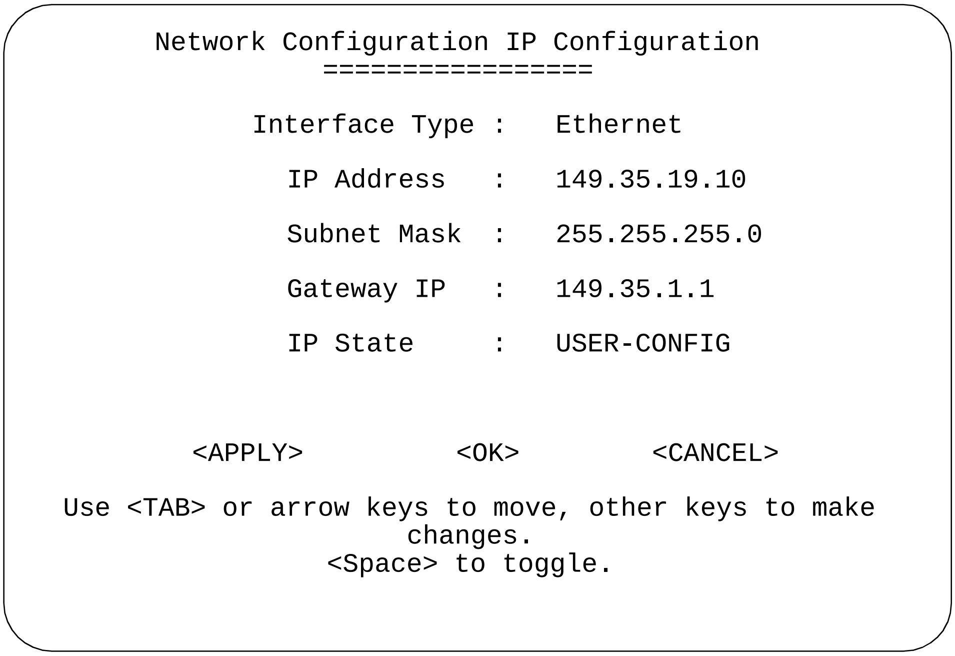


```
                  Network Configuration
                    =================

          IP Configuration ...

          IP Connectivity Test (Ping) ...

          HTTP Configuration ...

          MAX Number of Allowed Telnet Sessions (1 -4) : 2

          MAC Address : 00-30-84-9A-3B-80


            <APPLY>           <OK>          <CANCEL>

    Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	**Description**
IP Configuration	Screen used to set the bootup option, or configure the switch’s IP parameters.
IP Connectivity Test (Ping)	Screen used to test IP connectivity to a specified device.
HTTP Configuration	Screen used to enable Web Agent.
MAX Number of Allowed Telnet Sessions	The maximum number of Telnet sessions allowed to simultaneously access the agent module.
MAC Address	Physical address of the agent module.

IP Configuration

Use the IP Configuration screen to set the bootup option, or configure the switch's IP parameters. The screen shown below is described in the following table.



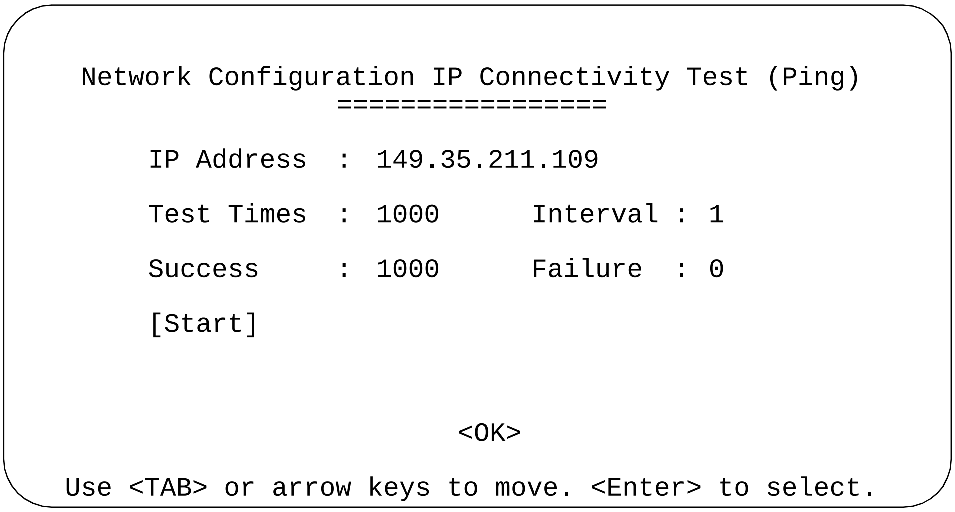
```
         Network Configuration IP Configuration
                    =================

               Interface Type :   Ethernet

                 IP Address   :   149.35.19.10

                 Subnet Mask  :   255.255.255.0

                 Gateway IP   :   149.35.1.1

                 IP State     :   USER-CONFIG



           <APPLY>          <OK>        <CANCEL>

   Use <TAB> or arrow keys to move, other keys to make
                       changes.
                  <Space> to toggle.
```

Parameter	Default	Description
Ethernet Interface		
IP Address	10.1.0.1	IP address of the stack you are managing when accessing the agent module over the network. The agent module supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module are assigned an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.0.0	Subnet mask of the agent you have selected. This mask identifies the host address bits used for routing to specific subnets.

Parameter	Default	Description
Default Gateway	0.0.0.0	Gateway used to pass trap messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BootP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BootP Get IP - IP is enabled but will not function until a BootP reply has been received. BootP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BootP values include the IP address, default gateway, subnet mask, TFTP boot file name, and TFTP server IP.)

IP Connectivity Test (Ping)

Use the IP Connectivity Test to see if another site on the Internet can be reached. The screen shown below is described in the following table.

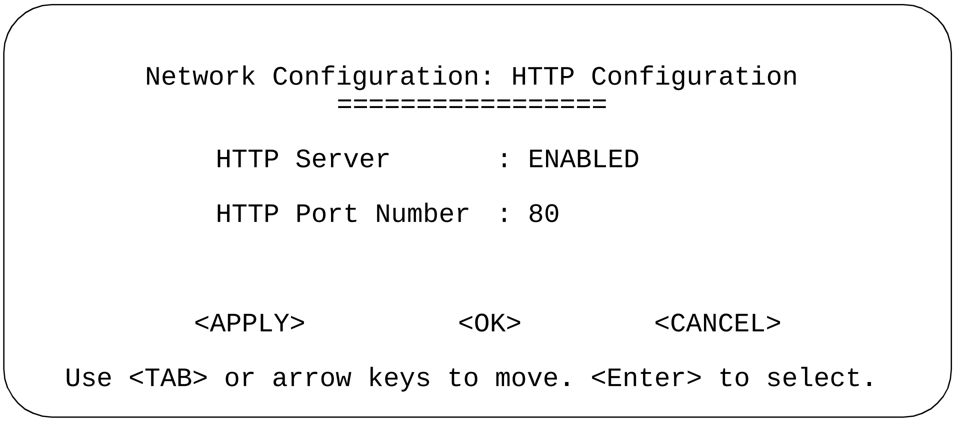


```
   Network Configuration IP Connectivity Test (Ping)
                   =================

        IP Address  :  149.35.211.109

        Test Times  :  1000      Interval : 1

        Success     :  1000      Failure  : 0

        [Start]


                            <OK>

  Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
IP Address	IP address of the site you want to ping
Test Times	The number of ICMP echo requests to send to the specified site (1~1000)
Interval	The interval (in seconds) between pinging the specified site (1~ 10 seconds)
Success/Failure	The number of times the specified site has responded or not to pinging

HTTP Configuration

Use the HTTP Configuration screen to enable/disable the on-board Web Agent, and to specify the TCP port that will provide HTTP service. The screen shown below is described in the following table.

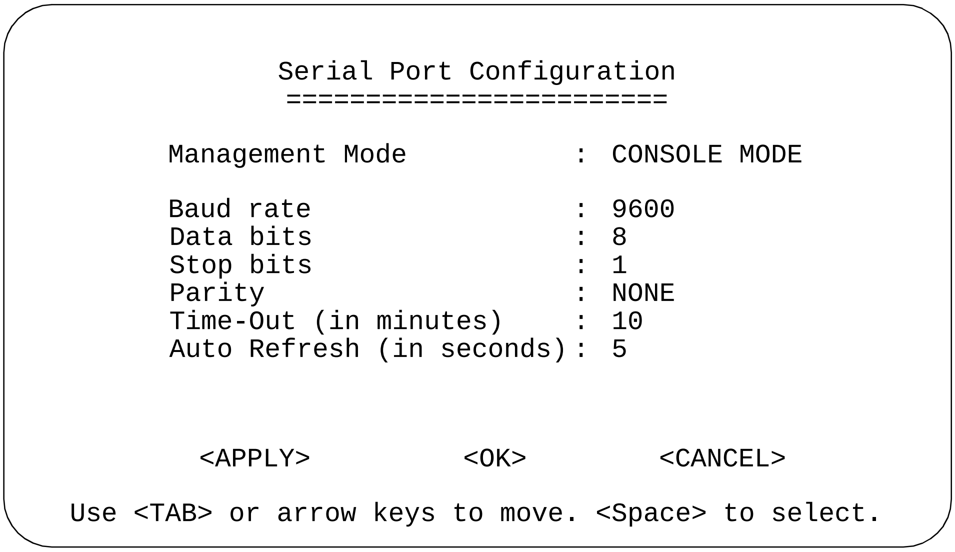


```
        Network Configuration: HTTP Configuration
                    =================

             HTTP Server       : ENABLED

             HTTP Port Number  : 80


           <APPLY>          <OK>         <CANCEL>

   Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
HTTP Server	Enables/disables access to the on-board Web Agent.
HTTP Port Number	Specifies the TCP port that will provide HTTP service. (Range is 0~65535. Default is Port 80. Telnet Port 23 is prohibited.)

Configuring the Serial Port

You can access the on-board configuration program by attaching a VT100 compatible device to the switch's serial port. (For more information on connecting to this port, refer to the section on Making the Connections Required for System Configuration on page 9.) The communication parameters for this port are accessed from the Serial Port Configuration screen seen below and described in the following table.

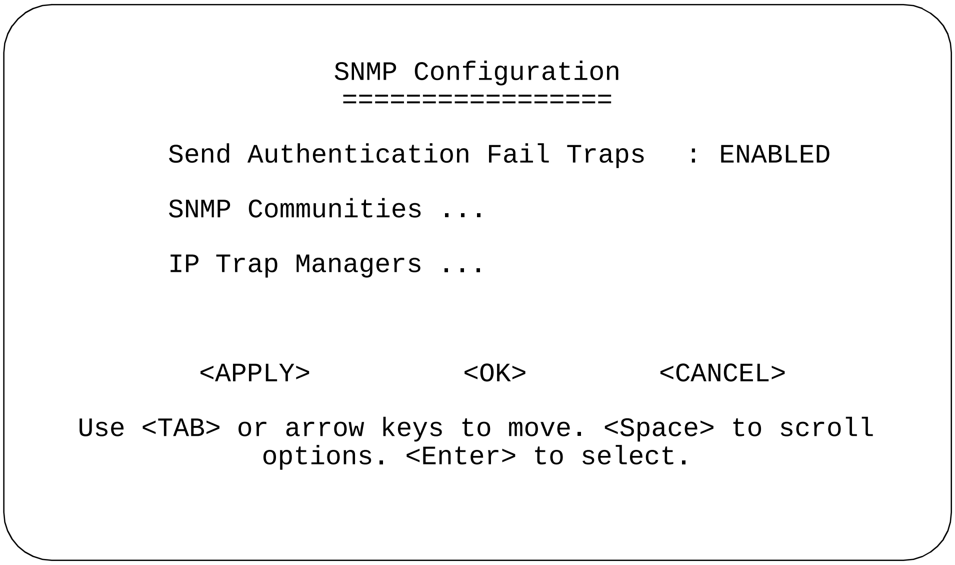


```
               Serial Port Configuration
               ========================

        Management Mode          :  CONSOLE MODE

        Baud rate                :  9600
        Data bits                :  8
        Stop bits                :  1
        Parity                   :  NONE
        Time-Out (in minutes)    :  10
        Auto Refresh (in seconds):  5



          <APPLY>          <OK>         <CANCEL>

    Use <TAB> or arrow keys to move. <Space> to select.
```

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the console port settings are for direct console connection.
Baud Rate	9600 bps	The rate at which data is sent between devices. (Options: 2400, 4800, 9600, 19200 bps, and Auto detection).
Databits	8 bits	Sets the databits of the RS-232 port. (Options: 7, 8)
Stopbits	1 bit	Sets the stop bits of the RS-232 port. (Options: 1, 2)
Parity	none	Sets the parity of the RS-232 port. (Options: none/odd/even)
Time-Out	10 minutes	If no input is received from the attached device after this interval (in minutes), the current session is automatically closed. (Range: 0 - 60 minutes; where 0 indicates disabled.)
Auto Refresh	5 sec.	Sets the interval before a console session will auto refresh the console information, including Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. (Range: 5 - 255 seconds; where 0 indicates disabled.)

Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table:

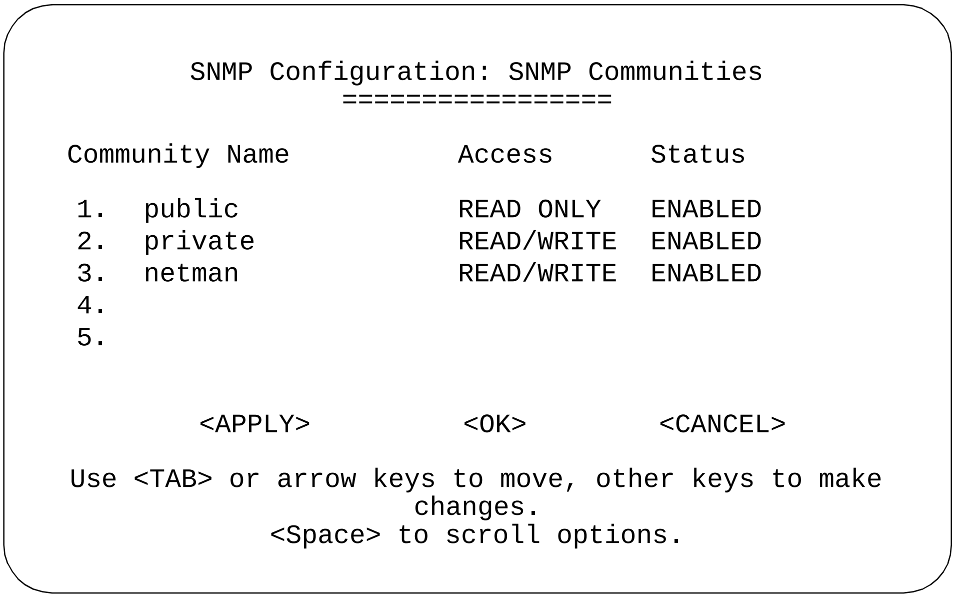


```
                    SNMP Configuration
                    ==================

         Send Authentication Fail Traps   : ENABLED

         SNMP Communities ...

         IP Trap Managers ...


           <APPLY>         <OK>         <CANCEL>

    Use <TAB> or arrow keys to move. <Space> to scroll
               options. <Enter> to select.
```

Name	Description
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)
SNMP Communities	Assigns SNMP access based on specified community strings.
IP Trap Managers	Specifies management stations that will receive authentication failure messages or other trap messages from the switch.

Configuring Community Names

The following figure and table describe how to configure the community strings authorized for trap management access. Up to 5 community names may be entered.

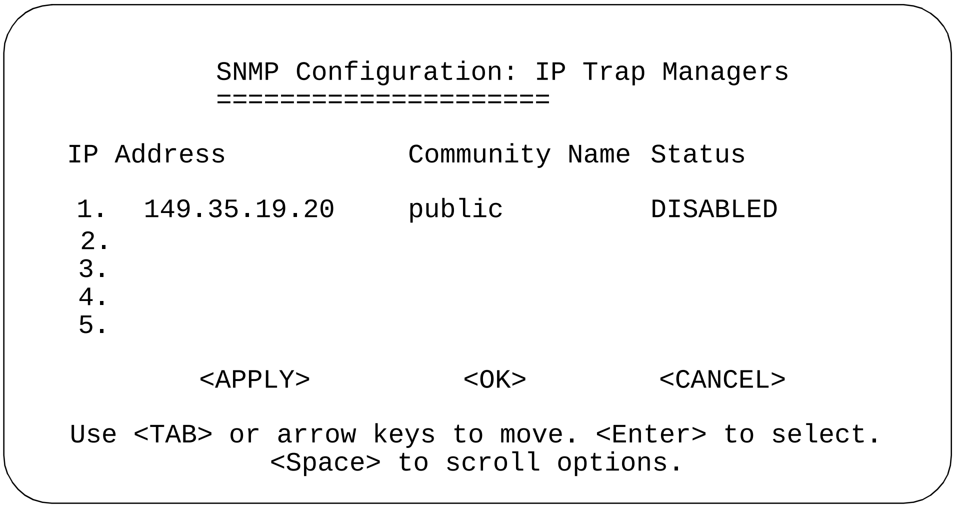


```
              SNMP Configuration: SNMP Communities
                        =================

   Community Name            Access      Status

    1.  public               READ ONLY   ENABLED
    2.  private              READ/WRITE  ENABLED
    3.  netman               READ/WRITE  ENABLED
    4.
    5.


          <APPLY>          <OK>         <CANCEL>

   Use <TAB> or arrow keys to move, other keys to make
                        changes.
                <Space> to scroll options.
```

Parameter	Description
Community Name	A community entry authorized for trap management access. Default string: public (read/write Maximum string length: 19 characters
Access	Management access is restricted to Read Only or Read/Write.
Status	Sets administrative status of entry to enabled or disabled.

Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

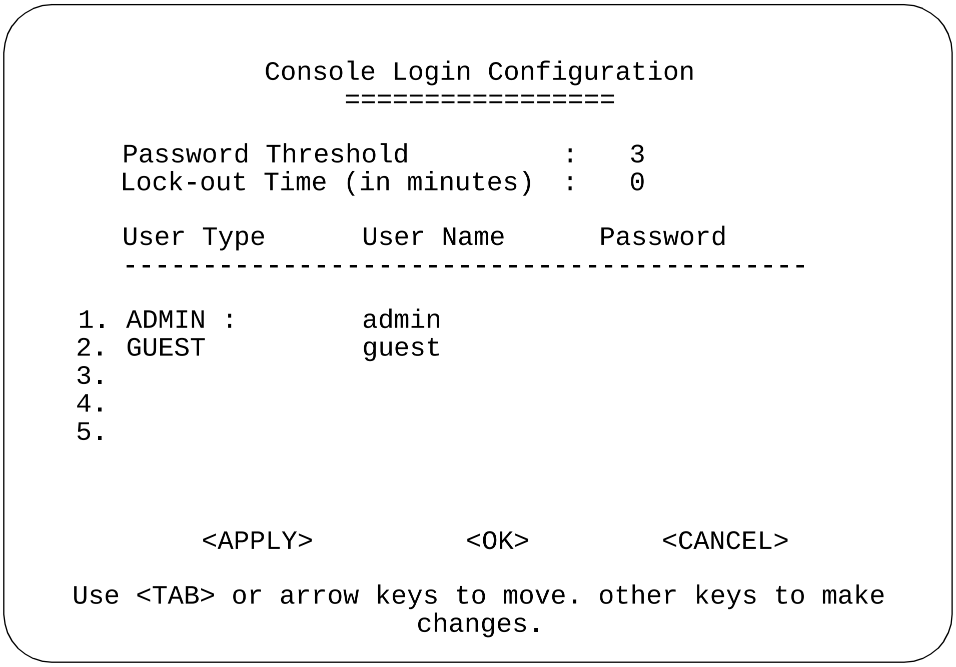


```
             SNMP Configuration: IP Trap Managers
             =====================

   IP Address           Community Name  Status

    1.   149.35.19.20     public          DISABLED
    2.
    3.
    4.
    5.

            <APPLY>          <OK>        <CANCEL>

   Use <TAB> or arrow keys to move. <Enter> to select.
               <Space> to scroll options.
```

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified for trap management access.
Status	Sets administrative status of entry to enabled or disabled.

Console Login Configuration

Use the Management Setup: Console Login Configuration to restrict management access based on specified user names and passwords, or to set the invalid password threshold and timeout. There are two user types, Administrator and Guest. Only the Administrator has write access for parameters governing the SNMP agent. You should therefore assign a user name and password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the System Configuration Program, contact your Allied Telesyn distributor for assistance.) The parameters shown on this screen are indicated in the following figure and table.



```
               Console Login Configuration
                    =================

        Password Threshold         :   3
        Lock-out Time (in minutes) :   0

        User Type      User Name      Password
        ------------------------------------------

     1. ADMIN :        admin
     2. GUEST          guest
     3.
     4.
     5.


             <APPLY>          <OK>         <CANCEL>

     Use <TAB> or arrow keys to move. other keys to make
                         changes.
```

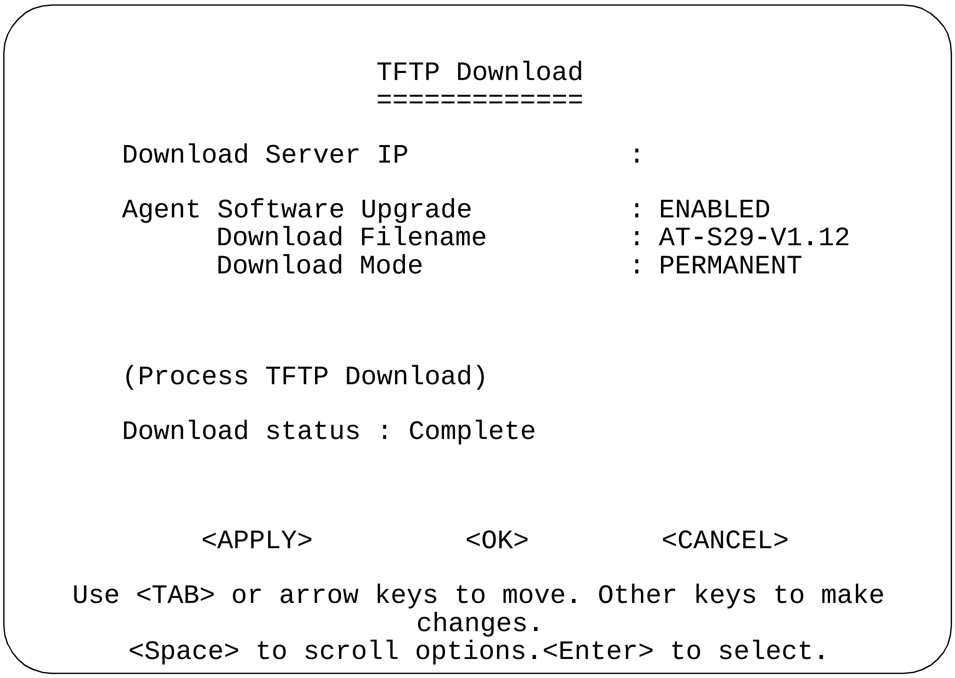
Parameter	Default	Description
Password	3	Sets the password intrusion threshold which limits the number of failed logon attempts. (Range: 0~65500)
Lock-out Time	0	The time (in seconds) the management console will be disabled, due to an excessive number of failed logon attempts. (Range: 0~65535)
Admin [1]	name: admin password : null	Administrator has access privilege of Read/Write for all screens.
Guest [1]	name: guest password : null	Guest has access privilege of Read Only for all screens.

[1] Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

Downloading System Software

Using TFTP Protocol to Download Over the Network

Use the TFTP Download menu to load software updates into the switch. The download file should be an AT-8324SX compressed binary file from Allied Telesyn; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.



```
                        TFTP Download
                        =============

       Download Server IP               :

       Agent Software Upgrade           : ENABLED
             Download Filename          : AT-S29-V1.12
             Download Mode              : PERMANENT


       (Process TFTP Download)

       Download status : Complete


            <APPLY>          <OK>         <CANCEL>

    Use <TAB> or arrow keys to move. Other keys to make
                         changes.
       <Space> to scroll options.<Enter> to select.
```

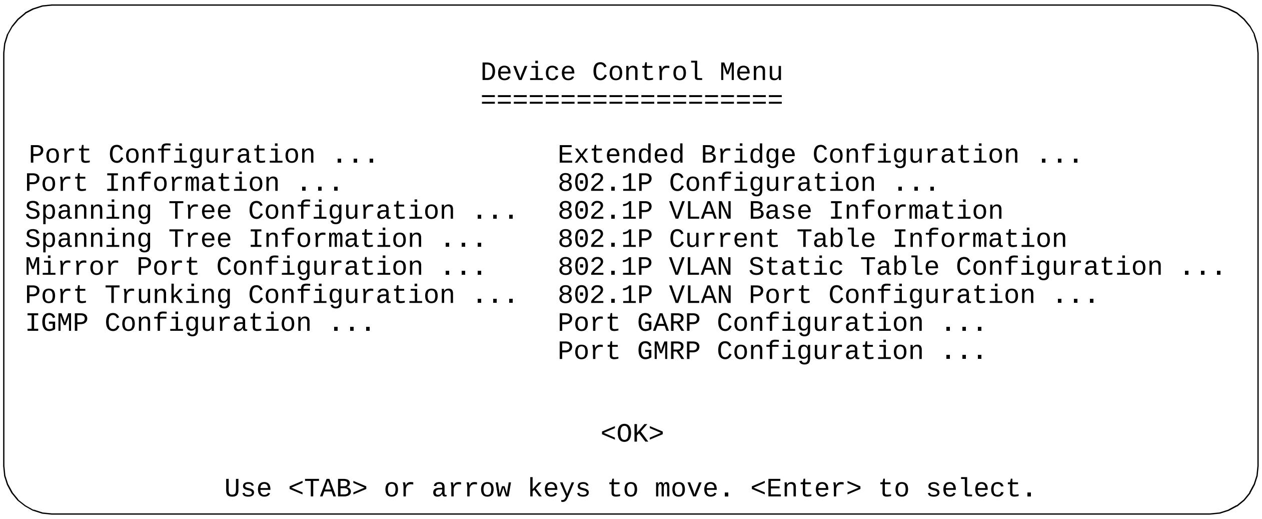
Parameter	Description
Download Server IP	IP address of a TFTP server.
Agent Software Upgrade	
Download Filename	The binary file to download to the agent module.
Download Mode	Downloads to permanent flash ROM.
Process TFTP Download	Issues request to TFTP server to download the specified file.

Note

You can also download firmware using the Web agent or via a direct console connection.

Configuring the Switch

The Device Control menu is used to set the communication parameters for individual ports and to fine-tune the performance of your switch. Configuration menus are also provided for advanced functions, such as Virtual LANs, port trunking, and port mirroring. Each of the setup screens provided by the configuration menus is described in the following sections.



```
                              Device Control Menu
                              ===================

 Port Configuration ...            Extended Bridge Configuration ...
 Port Information ...              802.1P Configuration ...
 Spanning Tree Configuration ...   802.1P VLAN Base Information
 Spanning Tree Information ...     802.1P Current Table Information
 Mirror Port Configuration ...     802.1P VLAN Static Table Configuration ...
 Port Trunking Configuration ...   802.1P VLAN Port Configuration ...
 IGMP Configuration ...            Port GARP Configuration ...
                                   Port GMRP Configuration ...


                                     <OK>

             Use <TAB> or arrow keys to move. <Enter> to select.
```

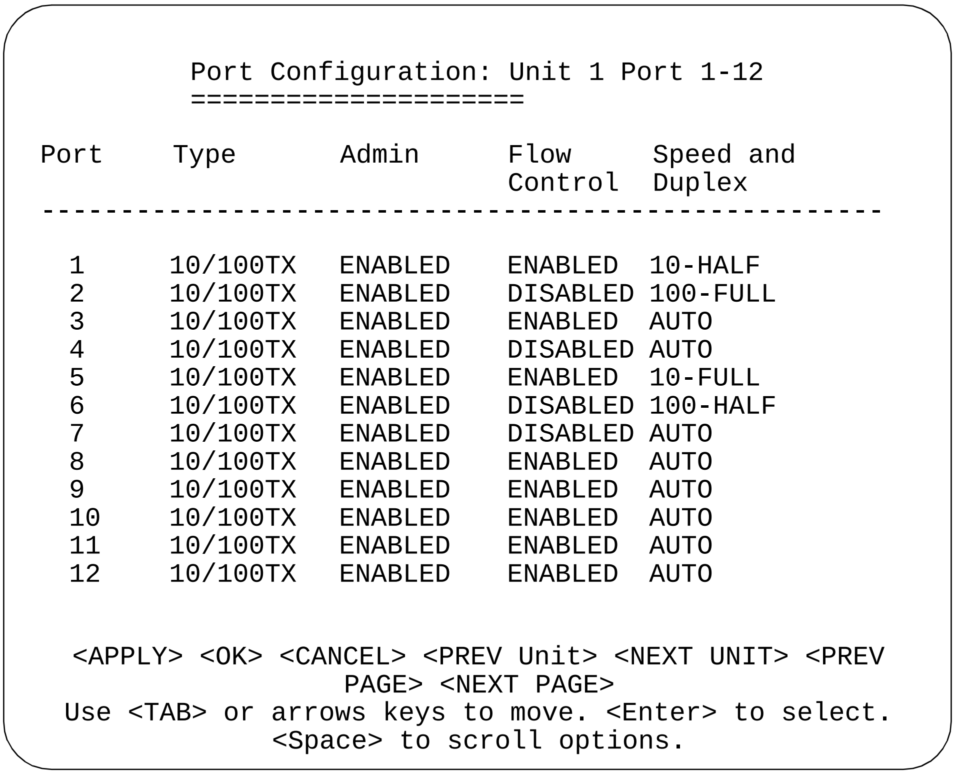
Parameter	Description
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full- or half-duplex.
Port Information	Displays operational status, including link state, flow control method, and duplex mode.
Spanning Tree Configuration	Enables Spanning Tree Algorithm; also sets parameters for hello time, maximum message age, switch priority, and forward delay; as well as port priority and path cost.
Spanning Tree Information	Displays a full listing of parameters for Spanning Tree Algorithm.
Mirror Port Configuration	Sets the source and target ports mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support

Parameter	Description
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including settings port members, or restricting ports from being dynamically added to a port by the GVRP protocol.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and GVRP.
Port GARP Configuration[1]	Configures generic attribute settings used in the spanning tree protocol, VLAN registration, multicast filtering.
Port GMRP Configuration[1]	Configures GMRP multicast filtering.

[1] Not implemented in this firmware release.

Configuring Port Parameters

Use the Port Configuration menus to configure any port or module on the switch.



```
          Port Configuration: Unit 1 Port 1-12
          =====================

Port     Type       Admin      Flow     Speed and
                               Control  Duplex
-----------------------------------------------------

  1      10/100TX   ENABLED    ENABLED  10-HALF
  2      10/100TX   ENABLED    DISABLED 100-FULL
  3      10/100TX   ENABLED    ENABLED  AUTO
  4      10/100TX   ENABLED    DISABLED AUTO
  5      10/100TX   ENABLED    ENABLED  10-FULL
  6      10/100TX   ENABLED    DISABLED 100-HALF
  7      10/100TX   ENABLED    DISABLED AUTO
  8      10/100TX   ENABLED    ENABLED  AUTO
  9      10/100TX   ENABLED    ENABLED  AUTO
  10     10/100TX   ENABLED    ENABLED  AUTO
  11     10/100TX   ENABLED    ENABLED  AUTO
  12     10/100TX   ENABLED    ENABLED  AUTO


  <APPLY> <OK> <CANCEL> <PREV Unit> <NEXT UNIT> <PREV
                  PAGE> <NEXT PAGE>
  Use <TAB> or arrows keys to move. <Enter> to select.
              <Space> to scroll options.
```

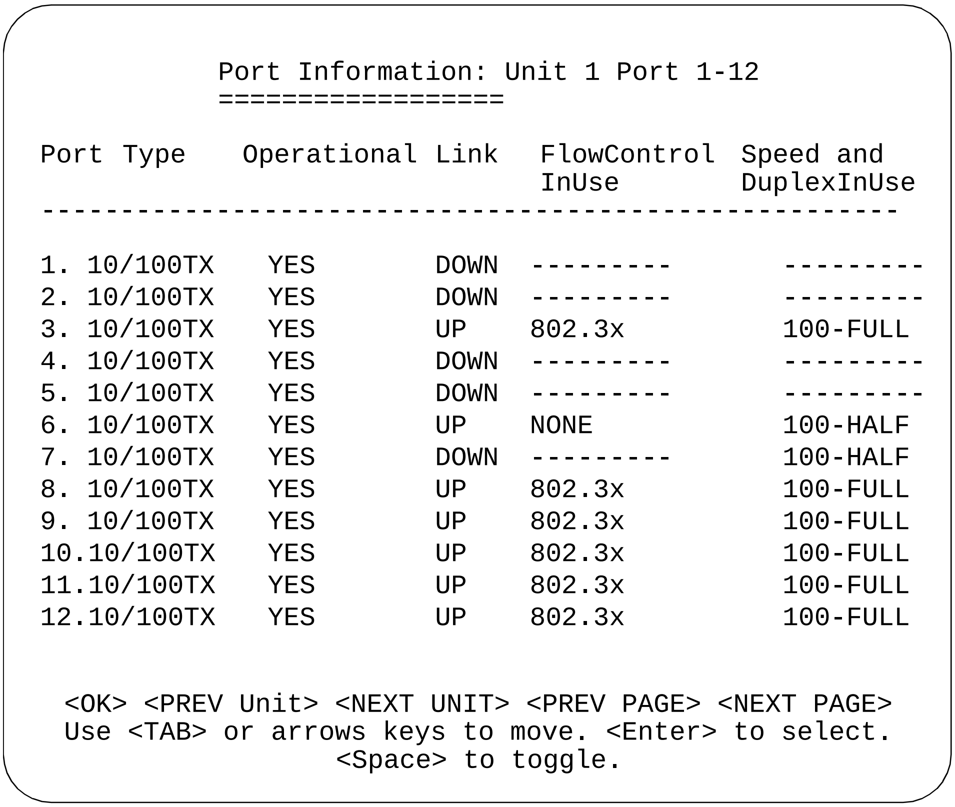
Parameter	Default	Description
Type		Shows port type as: 10/100TX: 10Base-T/100Base-TX 100FX : 100Base-FX 1000SX : 1000Base-SX 1000LX : 1000Base-LX
Admin	Enabled	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Flow Control	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Speed and Duplex	Auto	Used to set the current port speed, duplex mode, and auto-negotiation.

Note

Auto-negotiation is not available for 100Base-FX ports.

Viewing the Current Port Configuration

The Port Information screen displays the port type, status, link state, and flow control in use, as well as the communication speed and duplex mode. To change any of the port settings, use the configuration menu. The parameters shown in the following figure and table are for the RJ-45 ports.

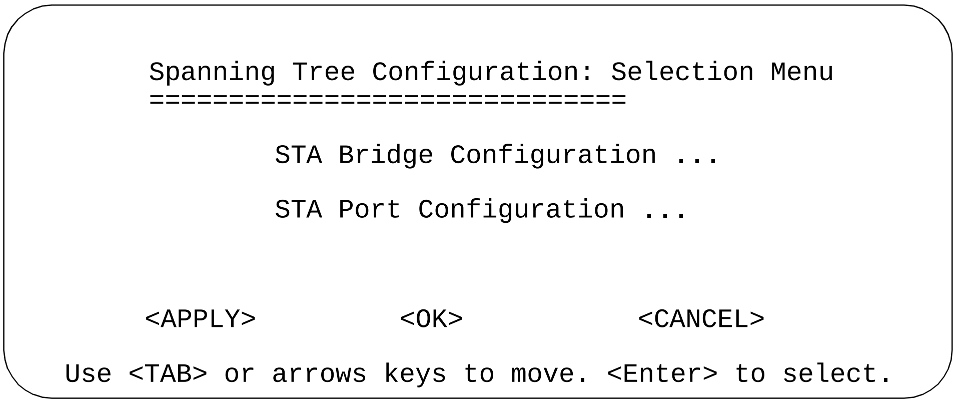


```
           Port Information: Unit 1 Port 1-12
           ==================

Port  Type    Operational Link   FlowControl  Speed and
                                 InUse        DuplexInUse
------------------------------------------------------

1. 10/100TX   YES        DOWN  ---------      ---------
2. 10/100TX   YES        DOWN  ---------      ---------
3. 10/100TX   YES        UP    802.3x         100-FULL
4. 10/100TX   YES        DOWN  ---------      ---------
5. 10/100TX   YES        DOWN  ---------      ---------
6. 10/100TX   YES        UP    NONE           100-HALF
7. 10/100TX   YES        DOWN  ---------      100-HALF
8. 10/100TX   YES        UP    802.3x         100-FULL
9. 10/100TX   YES        UP    802.3x         100-FULL
10.10/100TX   YES        UP    802.3x         100-FULL
11.10/100TX   YES        UP    802.3x         100-FULL
12.10/100TX   YES        UP    802.3x         100-FULL


 <OK> <PREV Unit> <NEXT UNIT> <PREV PAGE> <NEXT PAGE>
 Use <TAB> or arrows keys to move. <Enter> to select.
                <Space> to toggle.
```

Parameter	Description
Type	Shows port type as: 10/100TX: 10Base-T / 100Base-TX 100FX: 100Base-FX 1000SX: 1000Base-SX 1000LX: 1000Base-LX
Operational	Shows if the port is functioning or not.
Link	Indicates if the port has a valid connection to an external device.
FlowControl InUse	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.
Speed and Duplex InUse	Displays the current port speed, duplex mode, and if auto-negotiation is used. Note that auto-negotiation is available only for RJ-45 and Gigabit ports (not 100Base-FX ports.)

Using the Spanning Tree Algorithm

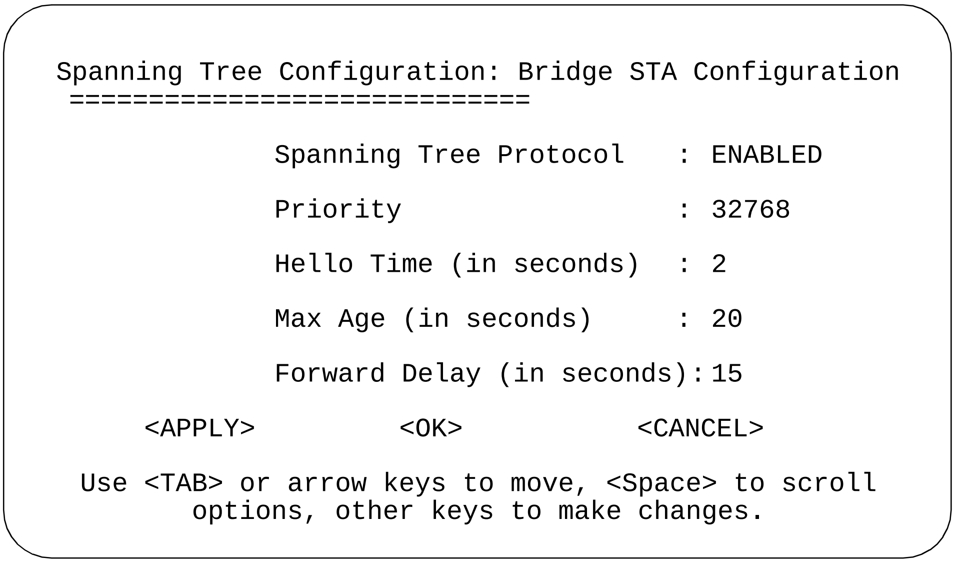
The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, STA compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to Chapter 4.



```
         Spanning Tree Configuration: Selection Menu
         ==============================

                 STA Bridge Configuration ...

                 STA Port Configuration ...


         <APPLY>          <OK>            <CANCEL>

    Use <TAB> or arrows keys to move. <Enter> to select.
```

Configuring Bridge STA

The following figure and table describe Bridge STA configuration.

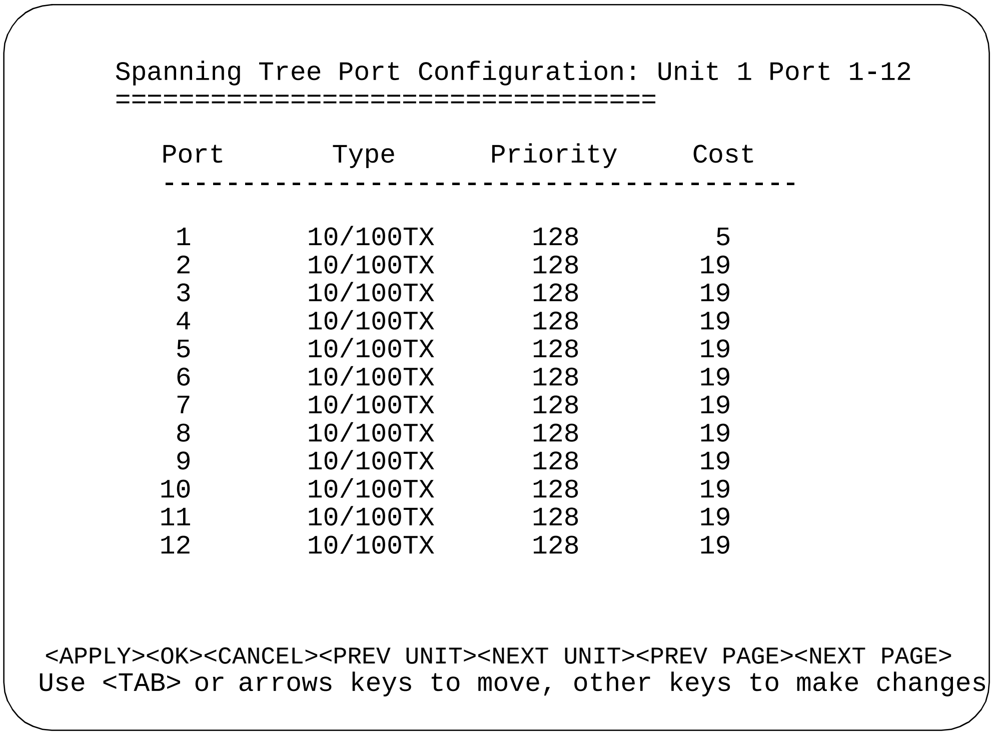


```
   Spanning Tree Configuration: Bridge STA Configuration
    =============================

                 Spanning Tree Protocol    : ENABLED

                 Priority                  : 32768

                 Hello Time (in seconds)   : 2

                 Max Age (in seconds)      : 20

                 Forward Delay (in seconds): 15

         <APPLY>          <OK>            <CANCEL>

     Use <TAB> or arrow keys to move, <Space> to scroll
            options, other keys to make changes.
```

Parameter	Default	Description
Spanning Tree Protocol	Enabled	Enable this parameter to participate in an STA compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message. Minimum value: 1 Maximum value: lower of 10 or [(Max. Message Age / 2) -1]
Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time + 1)]. The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

Configuring STA for Ports or Modules

The following figure and table describe STA configuration for ports or modules. (Note that the Spanning Tree Configuration screen for the expansion slots also indicates module type.)

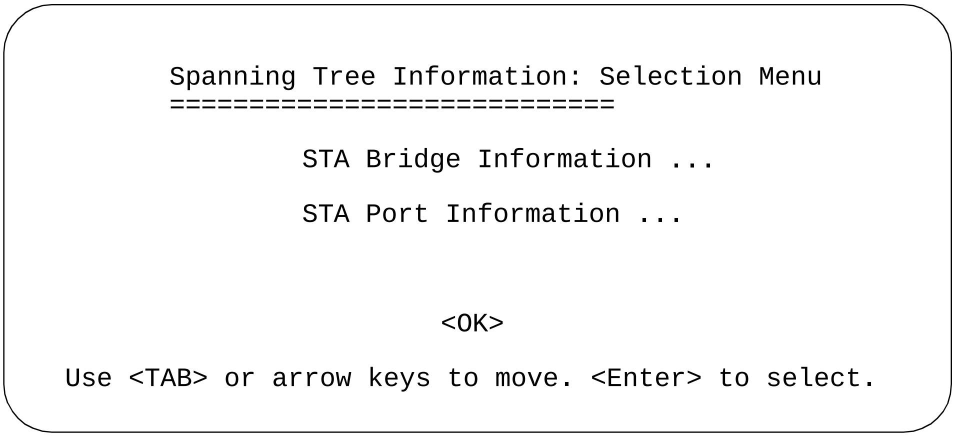


```
    Spanning Tree Port Configuration: Unit 1 Port 1-12
    ==================================

       Port      Type      Priority     Cost
       ----------------------------------------

        1       10/100TX      128         5
        2       10/100TX      128        19
        3       10/100TX      128        19
        4       10/100TX      128        19
        5       10/100TX      128        19
        6       10/100TX      128        19
        7       10/100TX      128        19
        8       10/100TX      128        19
        9       10/100TX      128        19
       10       10/100TX      128        19
       11       10/100TX      128        19
       12       10/100TX      128        19



 <APPLY><OK><CANCEL><PREV UNIT><NEXT UNIT><PREV PAGE><NEXT PAGE>
Use <TAB> or arrows keys to move, other keys to make changes
```

Parameter	**Default**	**Description**
Type		Shows port type as 10/100TX, 100FX, 1000SX or 1000LX.
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. The default and recommended range is: Standard Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535. Note: Path cost takes precedence over port priority.

Viewing the Current Spanning Tree Configuration

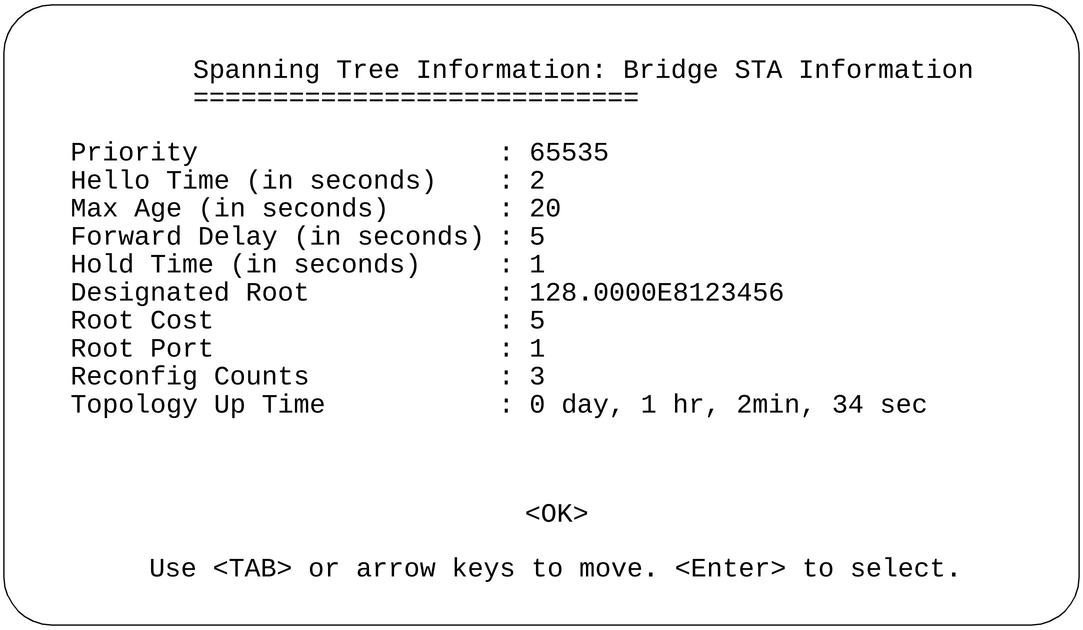
The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port or module. To make any changes to the parameters for the Spanning Tree, use the Spanning Tree Configuration menu.



```
          Spanning Tree Information: Selection Menu
          ============================

                  STA Bridge Information ...

                  STA Port Information ...


                           <OK>

   Use <TAB> or arrow keys to move. <Enter> to select.
```

Displaying the Current Bridge STA

The parameters shown in the following figure and table describe the current Bridge STA Information.

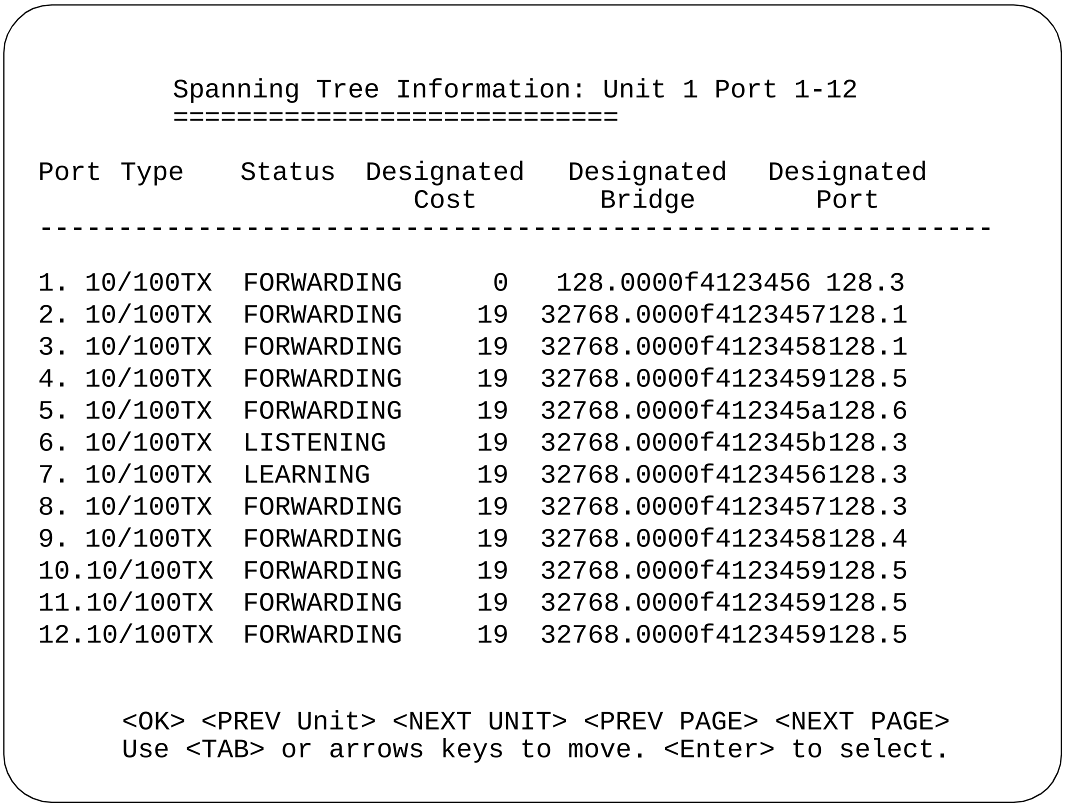


```
            Spanning Tree Information: Bridge STA Information
            ============================

    Priority                    : 65535
    Hello Time (in seconds)     : 2
    Max Age (in seconds)        : 20
    Forward Delay (in seconds) : 5
    Hold Time (in seconds)      : 1
    Designated Root             : 128.0000E8123456
    Root Cost                   : 5
    Root Port                   : 1
    Reconfig Counts             : 3
    Topology Up Time            : 0 day, 1 hr, 2min, 34 sec


                             <OK>

         Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Reconfig Counts	The number of times the spanning tree has been reconfigured.
Topology Up Time	The time since the spanning tree was last reconfigured.

Displaying the Current STA for Ports or Modules

The parameters shown in the following figure and table are for port or module STA Information (Port 1-12, Port 13-24, Expansion Slot 1 or Expansion Slot 2).



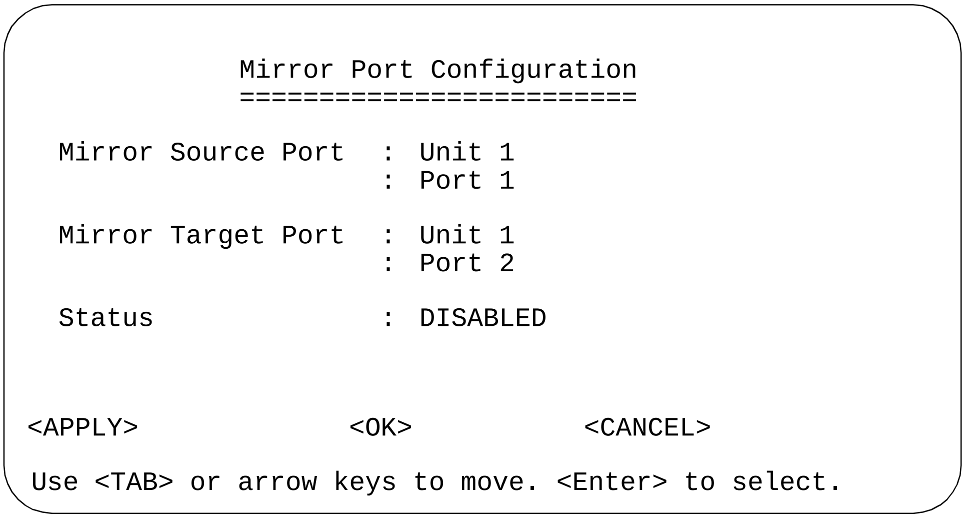
```
        Spanning Tree Information: Unit 1 Port 1-12
        ============================

Port  Type    Status  Designated   Designated   Designated
                         Cost        Bridge        Port
------------------------------------------------------------

1. 10/100TX  FORWARDING     0   128.0000f4123456 128.3
2. 10/100TX  FORWARDING    19  32768.0000f4123457128.1
3. 10/100TX  FORWARDING    19  32768.0000f4123458128.1
4. 10/100TX  FORWARDING    19  32768.0000f4123459128.5
5. 10/100TX  FORWARDING    19  32768.0000f412345a128.6
6. 10/100TX  LISTENING     19  32768.0000f412345b128.3
7. 10/100TX  LEARNING      19  32768.0000f4123456128.3
8. 10/100TX  FORWARDING    19  32768.0000f4123457128.3
9. 10/100TX  FORWARDING    19  32768.0000f4123458128.4
10.10/100TX  FORWARDING    19  32768.0000f4123459128.5
11.10/100TX  FORWARDING    19  32768.0000f4123459128.5
12.10/100TX  FORWARDING    19  32768.0000f4123459128.5


     <OK> <PREV Unit> <NEXT UNIT> <PREV PAGE> <NEXT PAGE>
     Use <TAB> or arrows keys to move. <Enter> to select.
```

Parameter	Description
Type	Shows port type as: 10/100TX: 10Base-T / 100Base-TX 100FX: 100Base-FX 1000SX: 1000Base-SX 1000LX: 1000Base-LX
Status	Displays the current state of this port within the spanning tree: **Disabled:** Port has been disabled by the user or has failed diagnostics **Blocked:** Port receives STA configuration messages, but does not forward packets. **Listening**: Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. **Learning**: Has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. **Forwarding**: The port forwards packets, and continues learning addresses. The rules defining port status are: A port on a network segment with no other STA compliant bridging device is always forwarding. If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Designated Cost	The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
Designated Port (ID)	The priority and port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

Using a Mirror Port for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You cana then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, not that the target port must be included in the same VLAN as the source port.

You can use the Mirror Port Configuration screen to designate a single port pair for mirroring as shown below:



```
              Mirror Port Configuration
              =========================

   Mirror Source Port  :  Unit 1
                       :  Port 1

   Mirror Target Port  :  Unit 1
                       :  Port 2

   Status              :  DISABLED


 <APPLY>             <OK>           <CANCEL>

 Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Port	The port that will “duplicate” or “mirror” all the traffic happening on the monitored port.
Status	Enables or disables the mirror function.

Configuring Port Trunks

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up to four trunk connections (combining 2 to 4 ports into a fat pipe) between any two AT-8324SX switches. However, before making any physical connections between devices, us the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

❑ The ports used in a trunk must all be of the same media type (RJ-45, 100 Mbps fiber, 1000 Mbps fiber). The ports that can be assigned to the same trunk have certain other restrictions as described later in this section.

❑ Ports can only be assigned to one trunk.

❑ The ports at both ends of a connection must be configured /as trunk ports.

❑ The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.

❑ The communication mode must be configured identically at both ends of the trunk.

❑ None of the ports in a trunk can be configured as a mirror source port or a mirror target port.

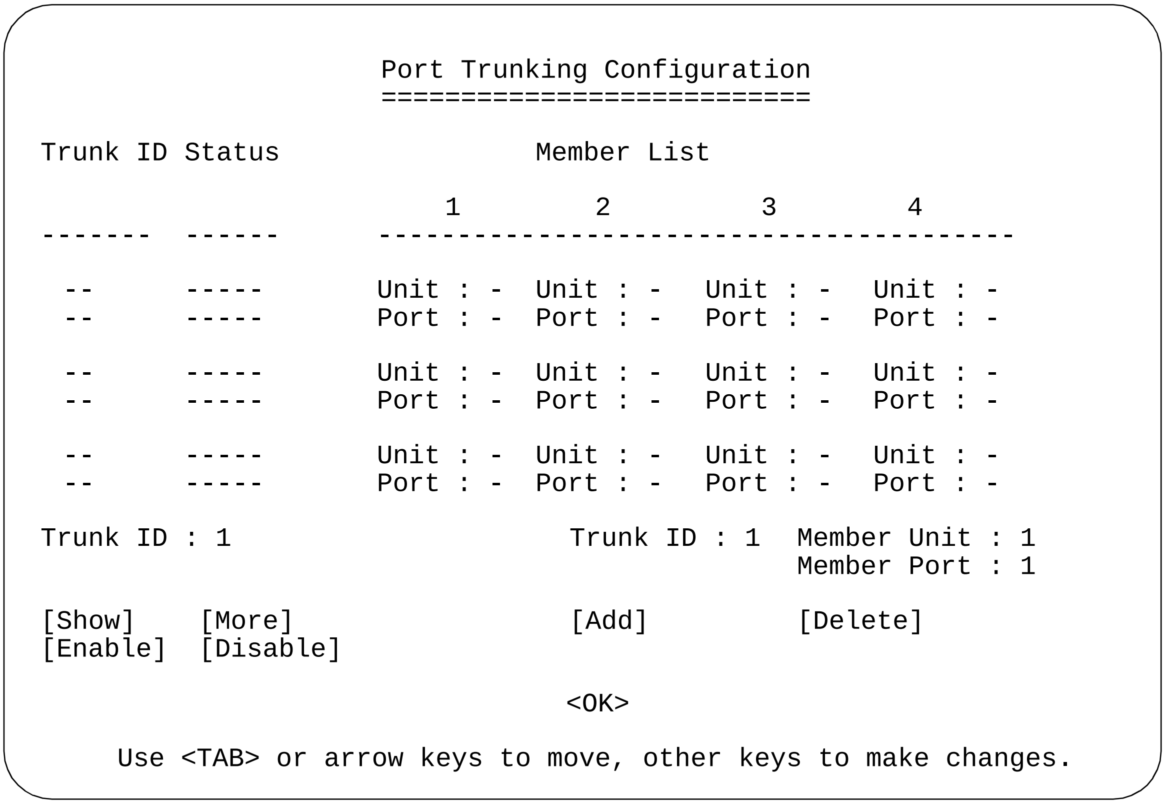
❑ All the ports in a trunk have to be treated as a whole when moved from/to added, or deleted from a VLAN.

❑ The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.

❑ Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.

❑ Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

You can use the Port Trunking Configuration screen to set up port trunks as shown below:



```
                         Port Trunking Configuration
                         ===========================

Trunk ID Status                 Member List

                             1         2          3         4
-------  ------         ----------------------------------------

  --     -----          Unit : -  Unit : -   Unit : -   Unit : -
  --     -----          Port : -  Port : -   Port : -   Port : -

  --     -----          Unit : -  Unit : -   Unit : -   Unit : -
  --     -----          Port : -  Port : -   Port : -   Port : -

  --     -----          Unit : -  Unit : -   Unit : -   Unit : -
  --     -----          Port : -  Port : -   Port : -   Port : -

Trunk ID : 1                        Trunk ID : 1  Member Unit : 1
                                                  Member Port : 1

[Show]    [More]                    [Add]         [Delete]
[Enable]  [Disable]

                                   <OK>

     Use <TAB> or arrow keys to move, other keys to make changes.
```

Parameter	Description
Trunk ID	Configure up to four trunks per switch.
Unit	Specifies a switch unit in the stack (1 to 4).
Port	Select from 2 to 4 ports per trunk.
[Show]	Displays trunk settings, where the first trunk listed is specified by “Trunk ID.”
[More]	Scrolls through the list of configured trunks.
[Enable] [Disable]	Enables/disables the selected trunk.
[Add] [Delete]	Adds/deletes the port specified by Trunk ID / Member Unit / Member Port.

The RJ-45 ports used for each trunk must all be on the same internal switch chip. The port groups permitted include:

- ❑ Group 1: 1, 2, 3, 4 and 13, 14, 15, 16
- ❑ Group 2: 5, 6, 7, 8 and 17, 18, 19, 20
- ❑ Group 3: 9, 10, 11, 12 and 21, 22, 23, 24

The 100Base-FX fiber optic ports used for one side of a trunk must all be on the same module. However, the 1000Base-SX and 1000Base-LX ports used for one side of a trunk may be on any switch in the stack, or both on the same switch if used as a standalone switch.

For example, when using Gigabit ports to form a trunk within a stack, the Gigabit ports will all be at Port 25. In this case, you could specify a trunk group consisting of:

(Unit1-Port25, Unit2-Port25, Unit3-Port25, Unit4-Port25)

or two trunks consisting of:

(Unit1-Port25, Unit2-Port25) and (Unit3-Port25, Unit4-Port25)

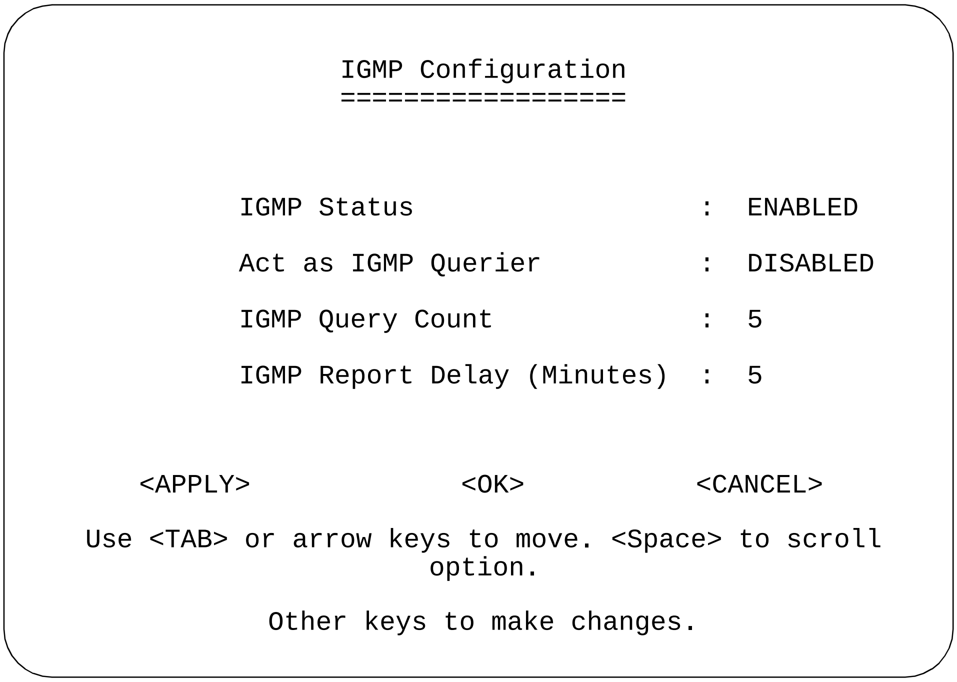
IGMP Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its services to the network, and any hosts which want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast server/router it passed through to ensure that traffic is only passed on the hosts which subscribe to this service.

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast group. You can use the IGMP Configuration screen to configure multicast filtering shown below:



```
                    IGMP Configuration
                    ==================


        IGMP Status                  :  ENABLED

        Act as IGMP Querier          :  DISABLED

        IGMP Query Count             :  5

        IGMP Report Delay (Minutes)  :  5


    <APPLY>             <OK>           <CANCEL>

  Use <TAB> or arrow keys to move. <Space> to scroll
                        option.

              Other keys to make changes.
```

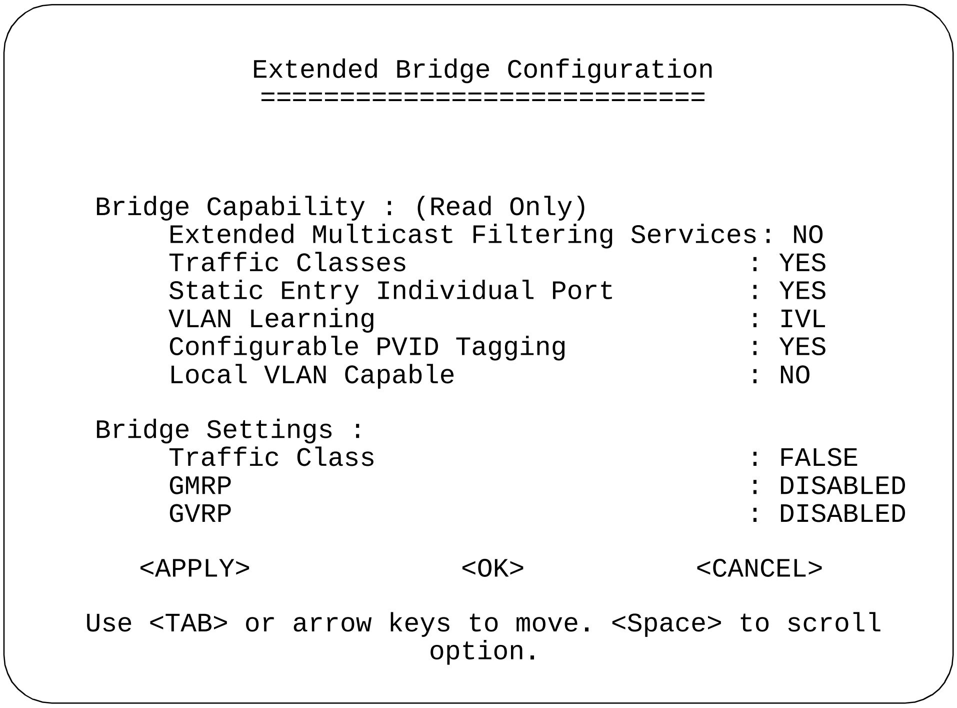
Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
ACT as IGMP Querier	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic. (Not available for the current firmware release.)
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports.
IGMP Report Delay	The time (in minutes) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out that port and removes the entry from its list.

Note

The default values are indicated in the sample screen.

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and Virtual LANs. To configure these extensions, use the Extended Bridge Configuration screen as shown below:



```
                Extended Bridge Configuration
                ============================


     Bridge Capability : (Read Only)
          Extended Multicast Filtering Services: NO
          Traffic Classes                       : YES
          Static Entry Individual Port          : YES
          VLAN Learning                         : IVL
          Configurable PVID Tagging             : YES
          Local VLAN Capable                    : NO

     Bridge Settings :
          Traffic Class                         : FALSE
          GMRP                                  : DISABLED
          GVRP                                  : DISABLED

        <APPLY>             <OK>           <CANCEL>

     Use <TAB> or arrow keys to move. <Space> to scroll
                          option.
```

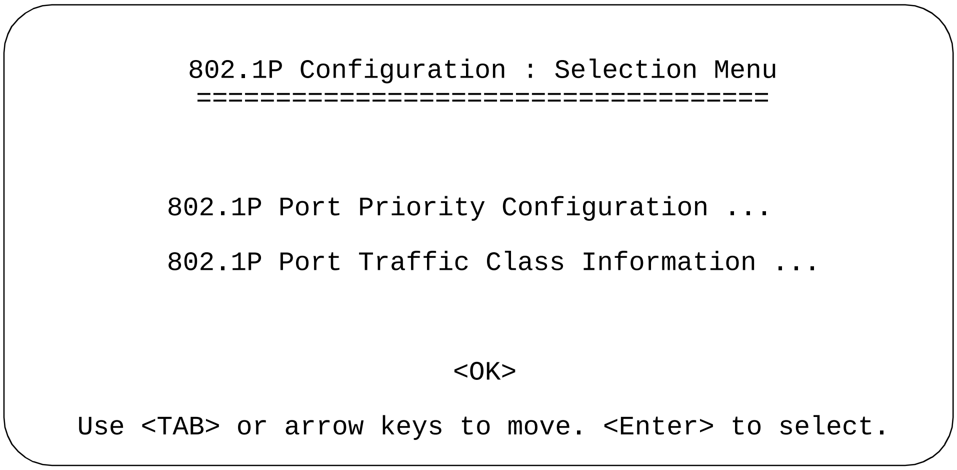
Parameter	Description
Bridge Capability	
Extended Multicast Filtering Services	Enables filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Note that this function is not available for the current firmware release.
Traffic Classes	Provides mapping of user priorities to multiple traffic classes. (Refer to 802.1p Configuration.)
Static Entry Individual Port	Enables static filtering for unicast and multicast addresses. (Refer to the Network Monitor Menu / Static Unicast Address Table Configuration and Static Multicast Address Table Configuration.)
VLAN Learning	This switch uses Independent VLAN Learning (IVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	Allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. (Refer to 802.1Q VLAN Port Configuration.
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

Parameter	Description
Bridge Settings	
Traffic Class[1]	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by setting this parameter to False. Note that this function is not available for the current firmware release.
GMRP[1]	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. Note that this function is not available for the current firmware release.
	The Internet Group Management Protocol (IGMP) is currently used by this switch to provide automatic multicast filtering.
GVRP[1]	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLAN groups that extend beyond the local switch.

[1] Not available in this firmware release.

Configuring Traffic Classes

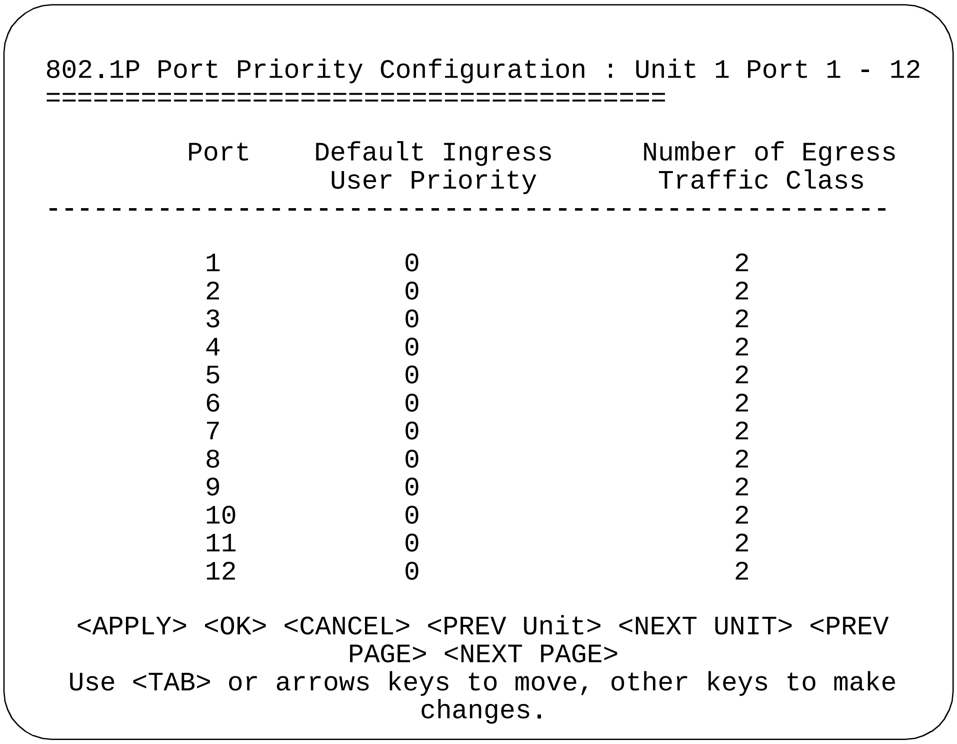
IEEE 802.1p defines up to eight separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with weighted fair queuing for each port. You can use the 802.1P Configuration menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections:



```
          802.1P Configuration : Selection Menu
          ====================================


        802.1P Port Priority Configuration ...

        802.1P Port Traffic Class Information ...


                          <OK>

  Use <TAB> or arrow keys to move. <Enter> to select.
```

Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority outlet queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the 802.1P Port Priority Configuration menu to adjust default priority for any port as shown below:

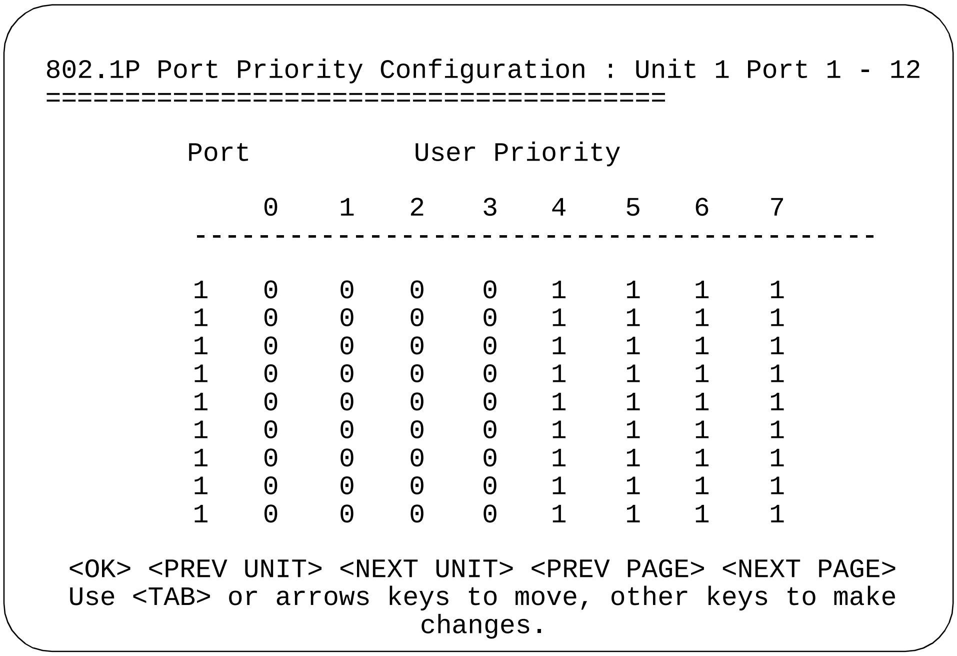


```
802.1P Port Priority Configuration : Unit 1 Port 1 - 12
=======================================

         Port    Default Ingress      Number of Egress
                  User Priority        Traffic Class
-----------------------------------------------------

          1           0                    2
          2           0                    2
          3           0                    2
          4           0                    2
          5           0                    2
          6           0                    2
          7           0                    2
          8           0                    2
          9           0                    2
          10          0                    2
          11          0                    2
          12          0                    2

  <APPLY> <OK> <CANCEL> <PREV Unit> <NEXT UNIT> <PREV
                   PAGE> <NEXT PAGE>
 Use <TAB> or arrows keys to move, other keys to make
                      changes.
```

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0-7, where 0-3 specifies the low priority queue and 4-7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

802.1p Port Traffic Class Information

This switch provides two priority levels with weighted fair queuing for port egress. This means that any frames with a default or user priority from 0-3 are sent to the low priority queue “0” while those from 4-7 are sent to the high priority queue “1” as shown in the following screen:



```
802.1P Port Priority Configuration : Unit 1 Port 1 - 12
=======================================

         Port          User Priority

              0    1    2    3    4    5    6    7
          -------------------------------------------

          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1
          1   0    0    0    0    1    1    1    1

 <OK> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE>
 Use <TAB> or arrows keys to move, other keys to make
                      changes.
```

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0-3 specify the low priority queue and 4-7 specify the high priority queue.

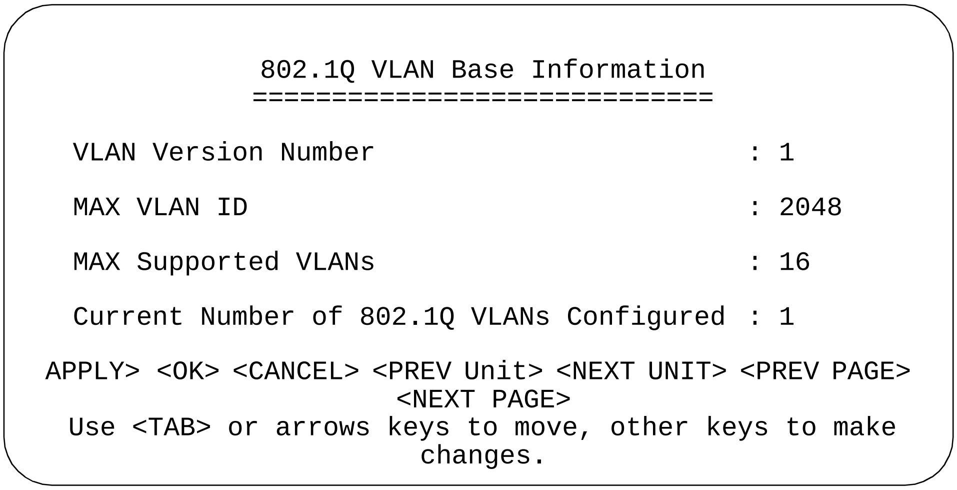
Configuring Virtual LANs

Use the VLAN Configuration menu to assign any port on the switch to any of up to 16 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of IPX traffic. By using IEEE 802.1Q compliant VLANs and GARP VLAN Registration Protocol, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and much cleaner network environment.

For a more detailed description of how to use VLANs, see Chapter 4. The VLAN configuration screens are described in the following sections.

802.1Q VLAN Base Information

The 802.1Q VLAN Base Information screen displays basic information on the VLAN type support by this switch.

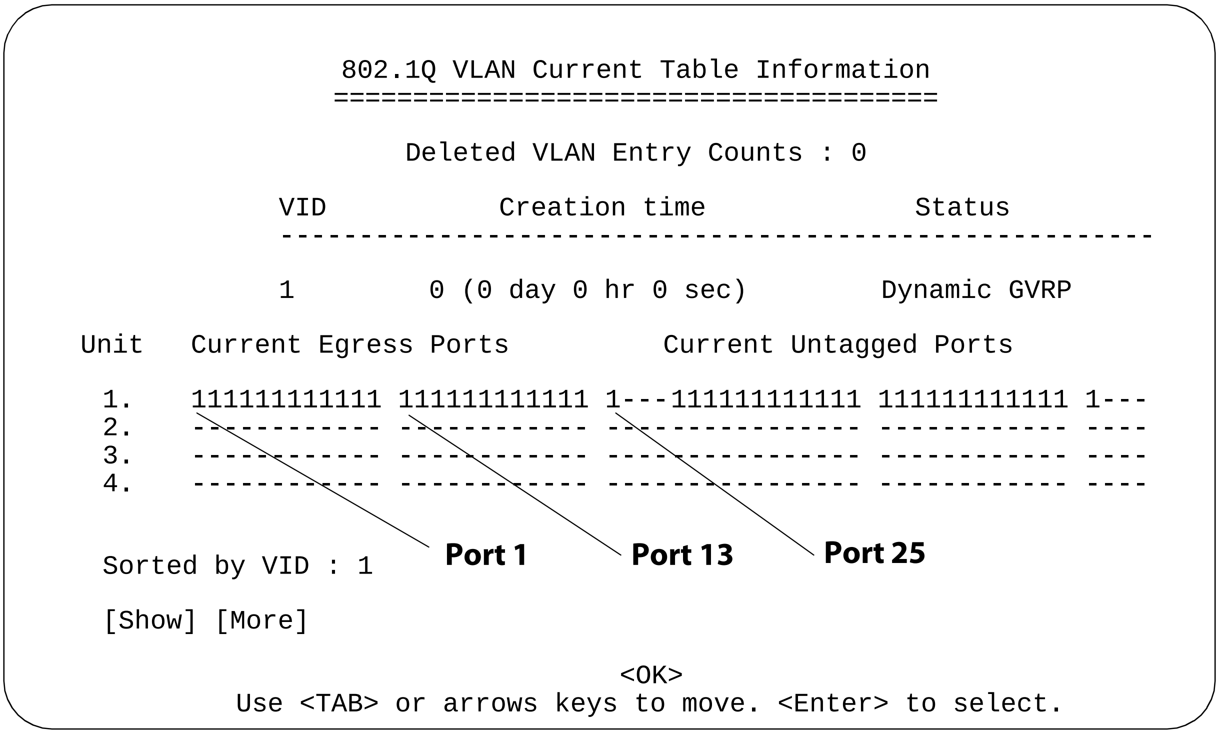


```
                    802.1Q VLAN Base Information
                   =============================

    VLAN Version Number                            : 1

    MAX VLAN ID                                    : 2048

    MAX Supported VLANs                            : 16

    Current Number of 802.1Q VLANs Configured : 1

 APPLY> <OK> <CANCEL> <PREV Unit> <NEXT UNIT> <PREV PAGE>
                          <NEXT PAGE>
  Use <TAB> or arrows keys to move, other keys to make
                          changes.
```

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

802.1Q VLAN Current Table Information

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN. The current configuration is shown in the following screen.



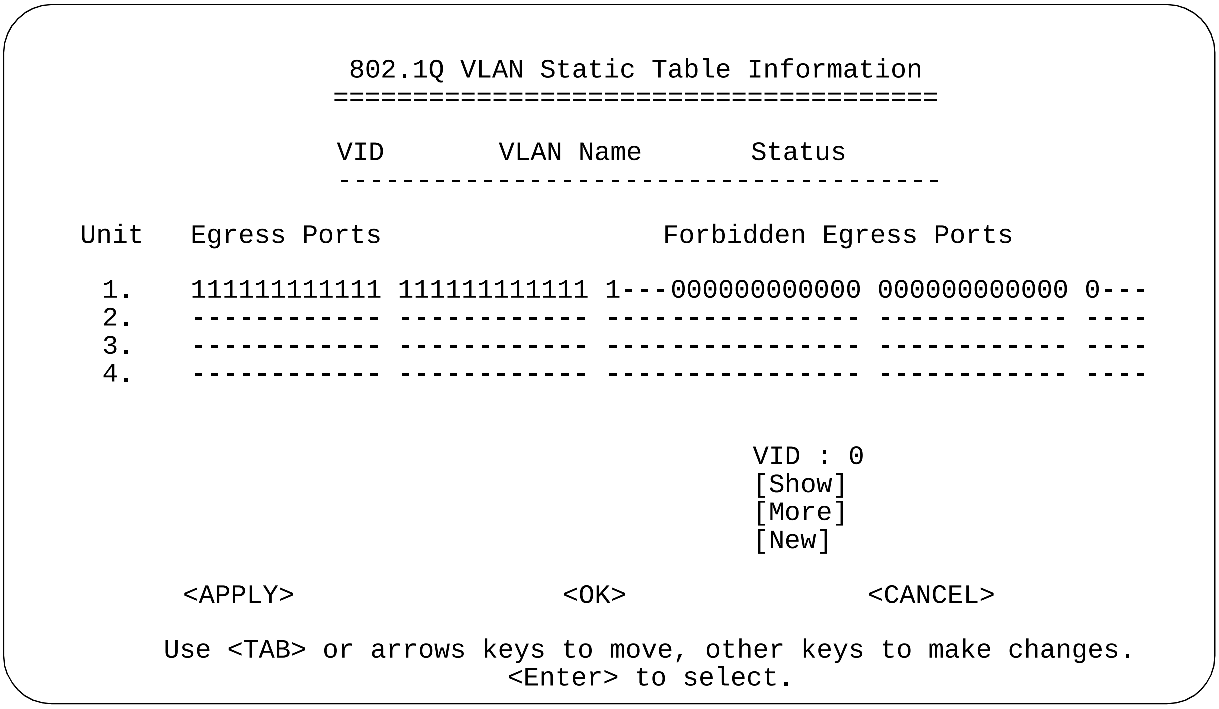
```
                    802.1Q VLAN Current Table Information
                   =======================================

                        Deleted VLAN Entry Counts : 0

                VID           Creation time             Status
                -------------------------------------------------------

                1        0 (0 day 0 hr 0 sec)        Dynamic GVRP

   Unit   Current Egress Ports          Current Untagged Ports

     1.   111111111111 111111111111 1---111111111111 111111111111 1---
     2.   ------------ ------------ ---------------- ------------ ----
     3.   ------------ ------------ ---------------- ------------ ----
     4.   ------------ ------------ ---------------- ------------ ----

     Sorted by VID : 1

     [Show] [More]

                                     <OK>
          Use <TAB> or arrows keys to move. <Enter> to select.
```

Port 1 Port 13 Port 25

Parameter	Description
Deleted VLAN Entry Counts	The number of times a VLAN entry has been deleted from this table.
VID	The ID for the VLAN currently displayed.
Creation Time	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch: Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Unit	Stack unit.
Current Egress Ports	Shows the ports which have been added to the displayed VLAN group, where "1" indicates that a port is a member and "O" that it is not.
Current Untagged Ports	If a port has been added to the displayed VLAN (see Current Egress Ports), its entry in this field will be "1" if the port is untagged or "O" if tagged.
[Show]	Displays the members for the VLAN indicated by the “Sorted by VID" field.
[More]	Displays any subsequent VLANs if configured.

802.1Q VLAN Static Table Information

Use this screen to create a new VLAN or modify the settings for an existing VLAN. You can add/delete port members for a VLAN from any unit in the stack, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Also, note that all ports can only belong to one untagged VLAN. This is set to VLAN 1 by default, but can be changed via the 802. 1 Q VLAN Port Configuration screen.)

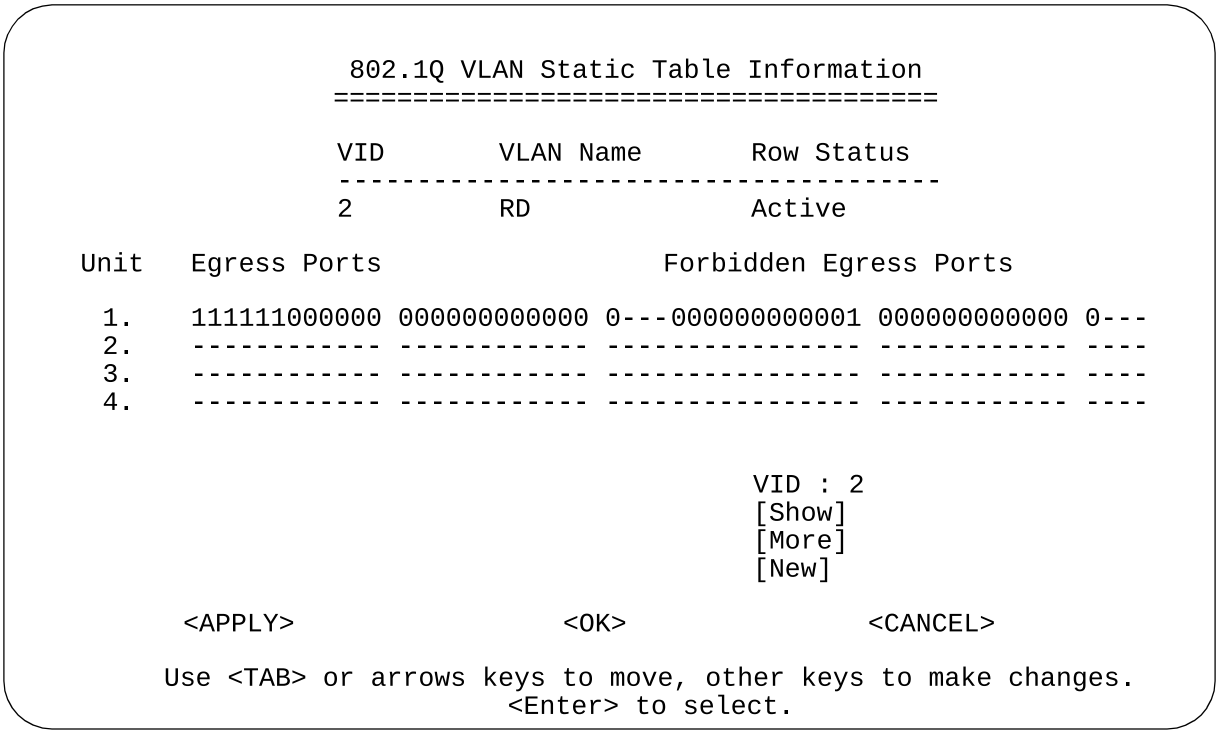


```
                  802.1Q VLAN Static Table Information
                 ======================================

                 VID       VLAN Name       Status
                 --------------------------------------

    Unit   Egress Ports                   Forbidden Egress Ports

     1.    111111111111 111111111111 1---000000000000 000000000000 0---
     2.    ------------ ------------ ---------------- ------------ ----
     3.    ------------ ------------ ---------------- ------------ ----
     4.    ------------ ------------ ---------------- ------------ ----


                                                VID : 0
                                                [Show]
                                                [More]
                                                [New]

          <APPLY>                 <OK>                  <CANCEL>

         Use <TAB> or arrows keys to move, other keys to make changes.
                             <Enter> to select.
```

Parameter	Description
VID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters.
Status	Sets the current editing status for this VLAN as: Not in Service, Destroy, or Active.
Unit	Stack unit.
Egress Ports	Set the entry for any port in this field to "1" to add it to the displayed VLAN, or "O" to remove it from the VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP.
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANS.
[New]	Sets up the screen for configuring a new VLAN.

Using the System Configuration Program

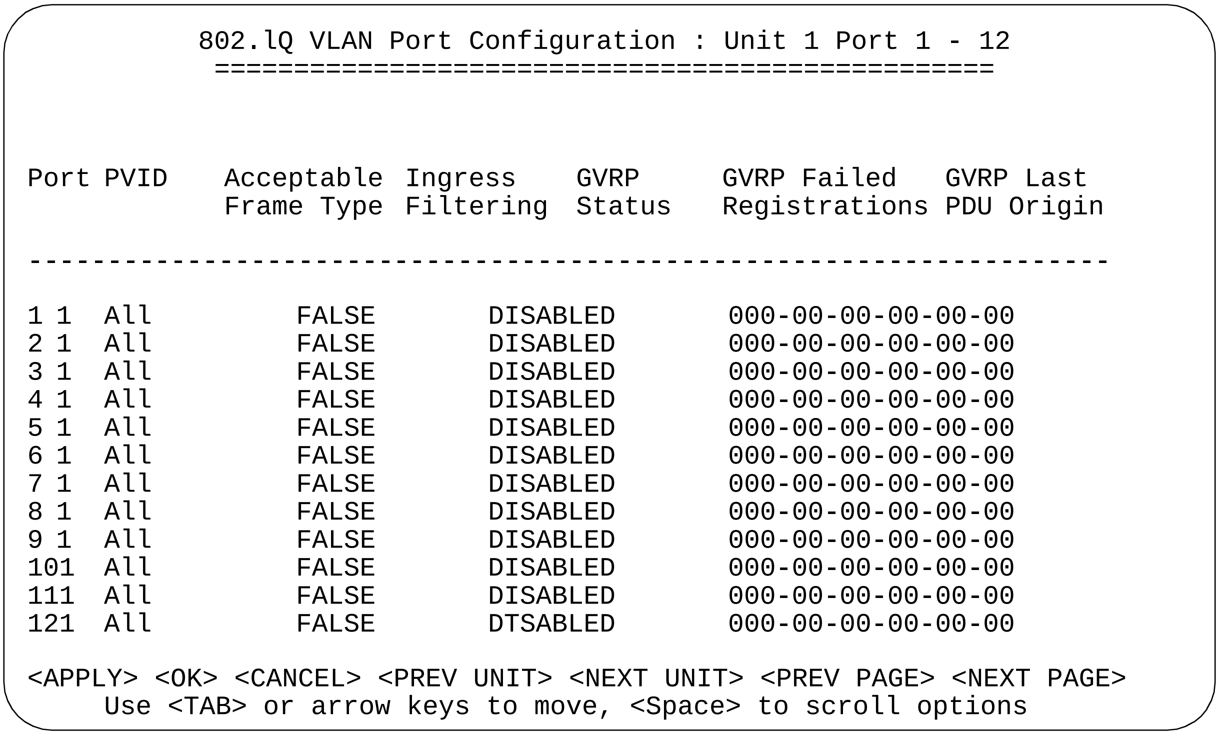
For example, the following screen displays settings for VLAN 2, which includes tagged ports 1-6, and forbidden port 12. (Note that the dashed lines show that there are no switch units in this system other than Unit 1.)



```
                       802.1Q VLAN Static Table Information
                      ======================================

                      VID       VLAN Name       Row Status
                      --------------------------------------
                      2         RD              Active

    Unit   Egress Ports                  Forbidden Egress Ports

      1.   111111000000 000000000000 0---000000000001 000000000000 0---
      2.   ------------ ------------ ---------------- ------------ ----
      3.   ------------ ------------ ---------------- ------------ ----
      4.   ------------ ------------ ---------------- ------------ ----


                                                 VID : 2
                                                 [Show]
                                                 [More]
                                                 [New]

          <APPLY>                 <OK>               <CANCEL>

         Use <TAB> or arrows keys to move, other keys to make changes.
                              <Enter> to select.
```

802.1Q VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.lQ VLAN features.



```
              802.lQ VLAN Port Configuration : Unit 1 Port 1 - 12
               =================================================



Port PVID    Acceptable Ingress    GVRP     GVRP Failed   GVRP Last
             Frame Type Filtering  Status   Registrations PDU Origin

--------------------------------------------------------------------

1 1  All         FALSE       DISABLED       000-00-00-00-00-00
2 1  All         FALSE       DISABLED       000-00-00-00-00-00
3 1  All         FALSE       DISABLED       000-00-00-00-00-00
4 1  All         FALSE       DISABLED       000-00-00-00-00-00
5 1  All         FALSE       DISABLED       000-00-00-00-00-00
6 1  All         FALSE       DISABLED       000-00-00-00-00-00
7 1  All         FALSE       DISABLED       000-00-00-00-00-00
8 1  All         FALSE       DISABLED       000-00-00-00-00-00
9 1  All         FALSE       DISABLED       000-00-00-00-00-00
101  All         FALSE       DISABLED       000-00-00-00-00-00
111  All         FALSE       DISABLED       000-00-00-00-00-00
121  All         FALSE       DTSABLED       000-00-00-00-00-00

<APPLY> <OK> <CANCEL> <PREV UNIT> <NEXT UNIT> <PREV PAGE> <NEXT PAGE>
     Use <TAB> or arrow keys to move, <Space> to scroll options
```

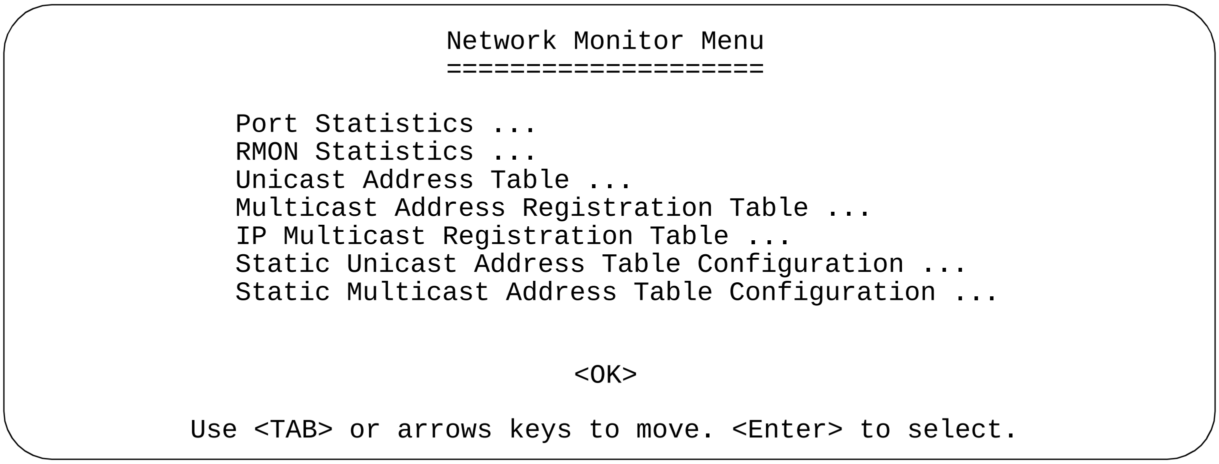
Parameter	**Description**
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type[1] [2]	This switch accepts “All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering[1]	If set to "True," incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
GVRP Status	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled for the switch before this setting can take effect. (See Device Control Menu / Extended Bridge Configuration.)
GVRP Failed Registrations	The total number of failed GVRP registrations, for any reason, on this port.
GVRP Last PDU Origin	The Source MAC Address of the last GVRP message received on this port.

[1] This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.

[2] Not implemented in this firmware release.

Monitoring the Switch

The Network Monitor Menu provides access to port statistics, RMON statistics, IP multicast addresses, and the static (unicast) address table. Each of the screens provided by these menus is described in the following sections.



```
                        Network Monitor Menu
                        ====================

             Port Statistics ...
             RMON Statistics ...
             Unicast Address Table ...
             Multicast Address Registration Table ...
             IP Multicast Registration Table ...
             Static Unicast Address Table Configuration ...
             Static Multicast Address Table Configuration ...


                                <OK>

          Use <TAB> or arrows keys to move. <Enter> to select.
```

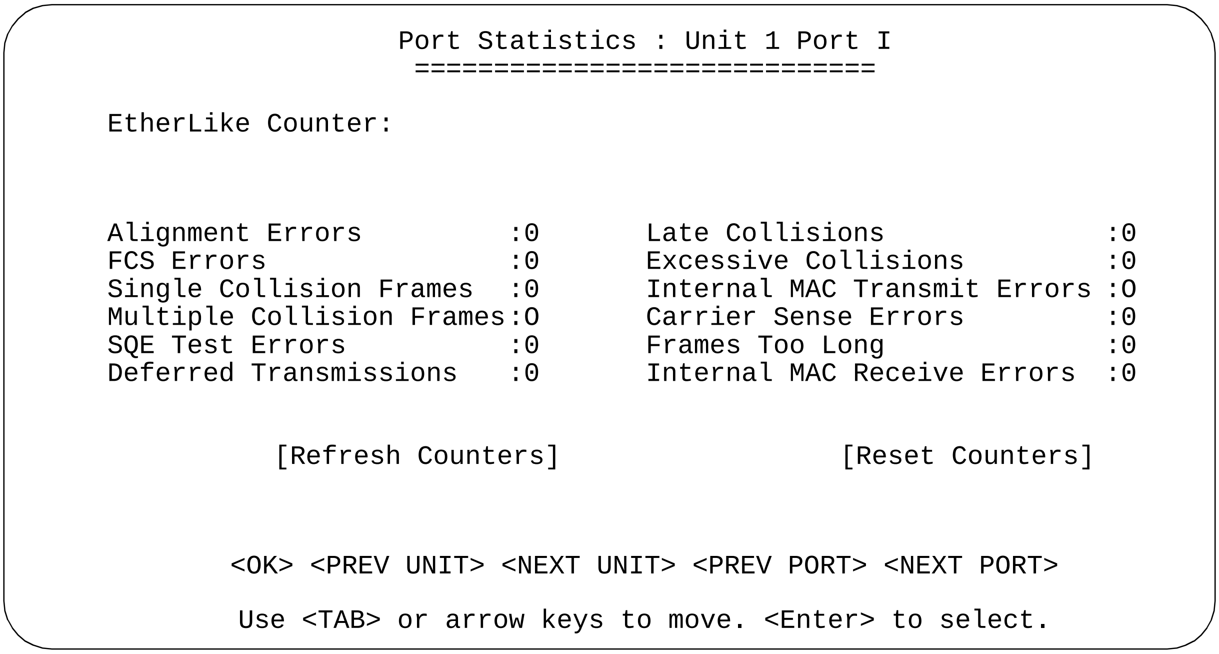
Parameter	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing of all unicast addresses stored in the switch, as well as sort, search and clear functions.
Multicast Address Registration Table[1]	Displays the ports that belong to each GMRP Muticast group.
IP Multicast Registration Table	Displays the ports that belong to each IP Muticast group.
Static Unicast Address Table Configuration	Allows you to display or configure static unicast addresses.
Static Multicast Address Table Configuration[1]	Allows you to display or configure static GMRP multicast addresses.

[1] Not implemented in this firmware release.

Displaying Port Statistics

Use the Port Statistics menu to display key statistics for each port. Overall statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading).

Select the required stack unit, and port or module. The statistics displayed are indicated in the following figure and table.



```
                        Port Statistics : Unit 1 Port I
                         =============================

    EtherLike Counter:


    Alignment Errors         :0      Late Collisions             :0
    FCS Errors               :0      Excessive Collisions        :0
    Single Collision Frames  :0      Internal MAC Transmit Errors :O
    Multiple Collision Frames:O      Carrier Sense Errors        :0
    SQE Test Errors          :0      Frames Too Long             :0
    Deferred Transmissions   :0      Internal MAC Receive Errors  :0

              [Refresh Counters]                 [Reset Counters]


           <OK> <PREV UNIT> <NEXT UNIT> <PREV PORT> <NEXT PORT>

           Use <TAB> or arrow keys to move. <Enter> to select.
```

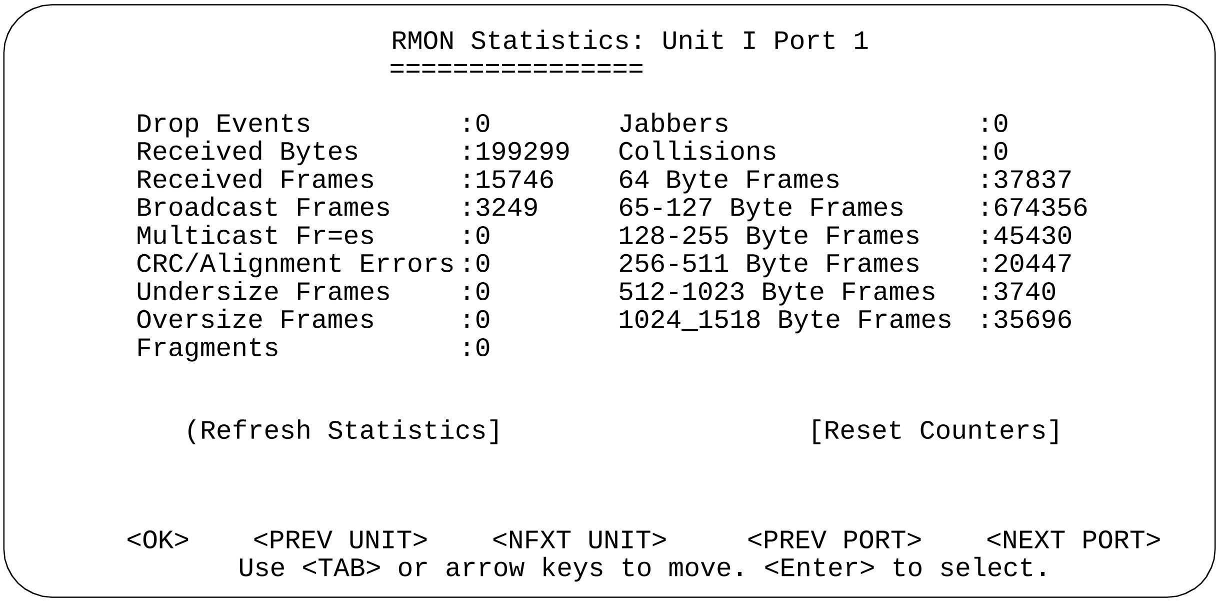
Parameter	Description
Alignment Errors	For 10 Mbps ports, this counter records alignment errors (mis-synchronized data packets). For 100Base-TX ports, this counter records the sum of alignment errors and code errors (frames received with rxerror signal).
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames[1]	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames[1]	A count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors[1]	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions[1]	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.

Parameter	Description
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions[1]	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors[1]	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carder Sense Errors[1]	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors[1]	The number of frames for which reception failed due to an internal MAC sublayer receive error.

[1] The reported values will always be zero because these statistics are not supported by the internal chip set.

Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port or media module from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays overall statistics on traffic passing through each port. RMON statistics provides access to a broad range of statistics, including a total count of different frame types passing through each port. Values displayed have been accumulated since the last system reboot.

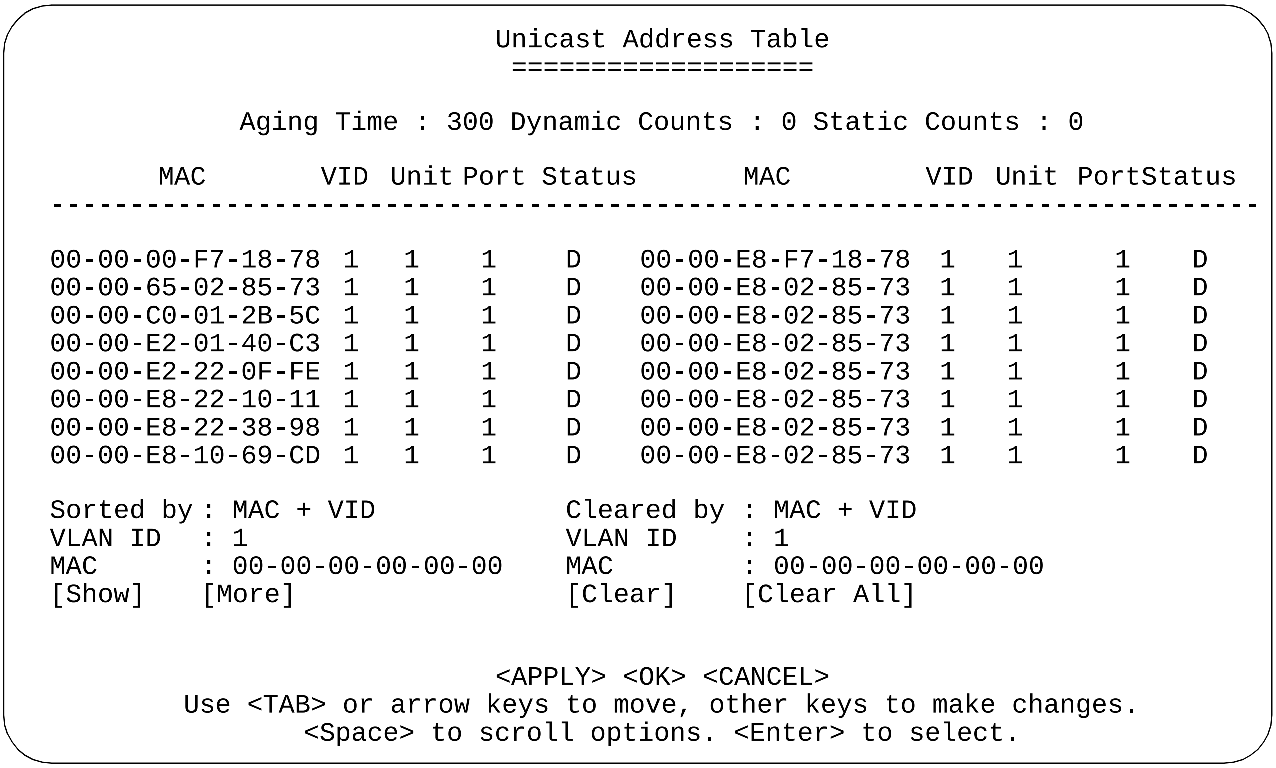


```
                        RMON Statistics: Unit I Port 1
                        ================

        Drop Events         :0        Jabbers               :0
        Received Bytes      :199299   Collisions            :0
        Received Frames     :15746    64 Byte Frames        :37837
        Broadcast Frames    :3249     65-127 Byte Frames    :674356
        Multicast Fr=es     :0        128-255 Byte Frames   :45430
        CRC/Alignment Errors:0        256-511 Byte Frames   :20447
        Undersize Frames    :0        512-1023 Byte Frames  :3740
        Oversize Frames     :0        1024_1518 Byte Frames :35696
        Fragments           :0


           (Refresh Statistics]                   [Reset Counters]



       <OK>    <PREV UNIT>    <NFXT UNIT>     <PREV PORT>    <NEXT PORT>
              Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Drop Events	The total number of events in which packets were dropped by the probe due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	For 1OMbs ports, the counter records CRC/alignment errors (FCS or alignment errors). For 10OMbs ports, the counter records the sum of CRC/ alignment errors and code errors (frame received with rxerror signal).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets),
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Displaying the Unicast Address Table

The Address Table contains the MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN ID. You can search for a specific address, clear the entire address table, or information associated with a specific address, or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.



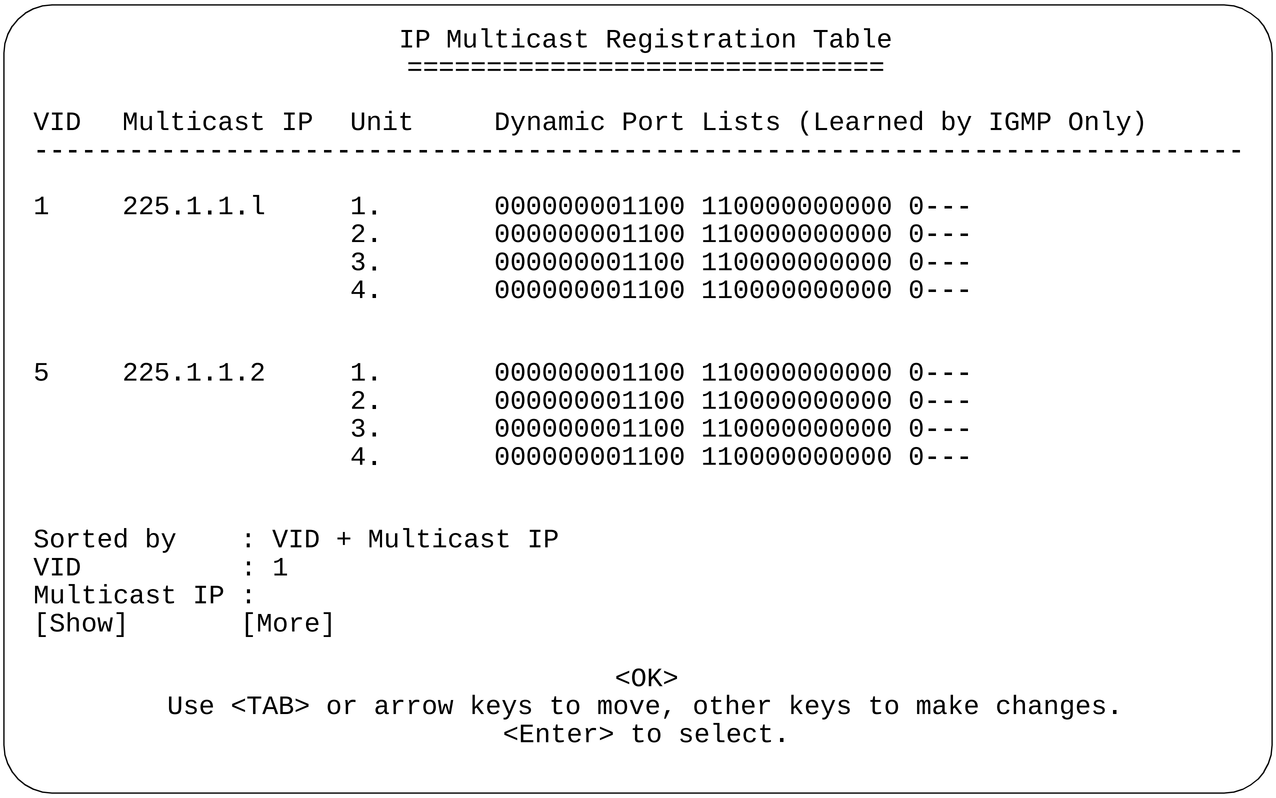
```
                         Unicast Address Table
                          ===================

            Aging Time : 300 Dynamic Counts : 0 Static Counts : 0

       MAC       VID  Unit Port Status       MAC        VID  Unit  PortStatus
----------------------------------------------------------------------------

00-00-00-F7-18-78  1   1    1     D    00-00-E8-F7-18-78  1    1      1    D
00-00-65-02-85-73  1   1    1     D    00-00-E8-02-85-73  1    1      1    D
00-00-C0-01-2B-5C  1   1    1     D    00-00-E8-02-85-73  1    1      1    D
00-00-E2-01-40-C3  1   1    1     D    00-00-E8-02-85-73  1    1      1    D
00-00-E2-22-0F-FE  1   1    1     D    00-00-E8-02-85-73  1    1      1    D
00-00-E8-22-10-11  1   1    1     D    00-00-E8-02-85-73  1    1      1    D
00-00-E8-22-38-98  1   1    1     D    00-00-E8-02-85-73  1    1      1    D
00-00-E8-10-69-CD  1   1    1     D    00-00-E8-02-85-73  1    1      1    D

Sorted by : MAC + VID              Cleared by : MAC + VID
VLAN ID   : 1                      VLAN ID    : 1
MAC       : 00-00-00-00-00-00      MAC        : 00-00-00-00-00-00
[Show]    [More]                   [Clear]    [Clear All]


                         <APPLY> <OK> <CANCEL>
          Use <TAB> or arrow keys to move, other keys to make changes.
                  <Space> to scroll options. <Enter> to select.
```

Parameter	Description
Address Table	Time-out period in seconds for aging out.
Aging Time	Dynamically learned forwarding information. Range: 10 - 412 seconds Default: 300 secs.
Dynamic Counts	Number of dynamically learned addresses.
Static Counts	Number of statically configured addresses.
MAC	The MAC address of a node.
VID	The VLAN(s) associated with this address or port.
Unit	Switch unit in the stack (1~4).
Port	The port whose address table includes this MAC address.

Parameter	Description
Status	Indicates address status as: **D**: dynamically learned, or **P**: fixed permanent.y by SNMP network management software.
[Show]	Displays the address table based on specified VLAN ID, and sorted by primary key MAC or VID.
[Clear]	Clears the specified MAC address.
[Clear All]	Clears all MAC addresses from the table.

Displaying the IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

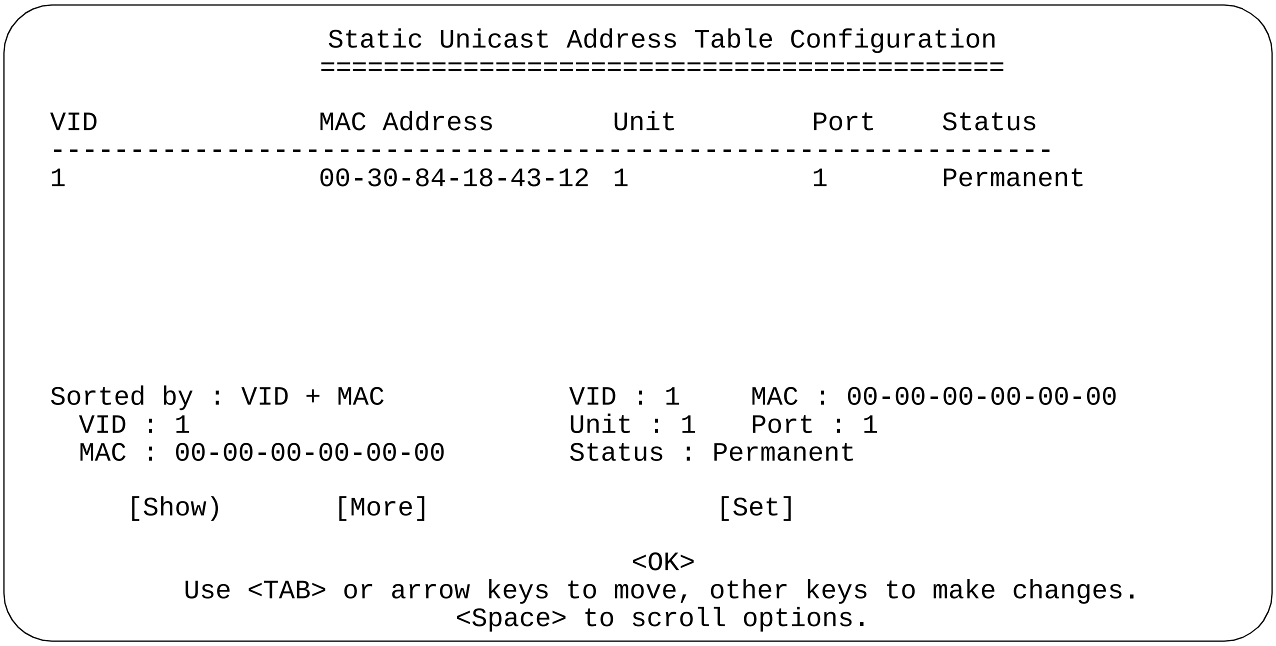


```
                         IP Multicast Registration Table
                         ==============================

VID   Multicast IP   Unit     Dynamic Port Lists (Learned by IGMP Only)
----------------------------------------------------------------------------

1     225.1.1.l      1.       000000001100 110000000000 0---
                     2.       000000001100 110000000000 0---
                     3.       000000001100 110000000000 0---
                     4.       000000001100 110000000000 0---


5     225.1.1.2      1.       000000001100 110000000000 0---
                     2.       000000001100 110000000000 0---
                     3.       000000001100 110000000000 0---
                     4.       000000001100 110000000000 0---


Sorted by     : VID + Multicast IP
VID           : 1
Multicast IP  :
[Show]        [More]

                                   <OK>
        Use <TAB> or arrow keys to move, other keys to make changes.
                             <Enter> to select.
```

Parameter	Description
VID	VLAN ID assigned to this multicast group.
Multicast IP	IP address for specific multicast services.
Unit	Stack unit.
Dynamic Port Lists	The switch ports dynamically registered for the indicated multicast service via IGMP.
[Show]	Displays the address table sorted on VID and then Multicast IP.
[More]	Scrolls through the entries in the address table.

Configuring Static Unicast Addresses

Use the Static Unicast Address Table Configuration screen to manually configure host MAC addresses in the unicast table. You can use this screen to associate a MAC address with a specific VLAN ID and switch port as shown below.



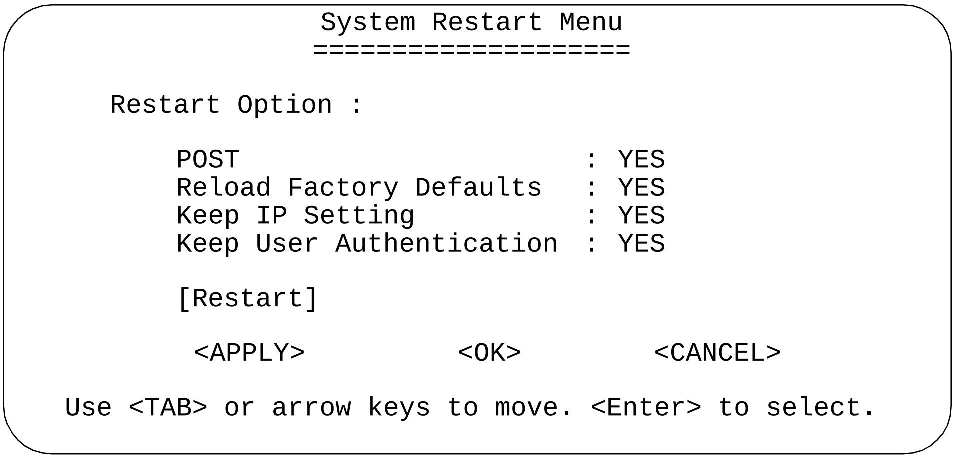
```
                 Static Unicast Address Table Configuration
                 ===========================================

VID              MAC Address       Unit         Port    Status
---------------------------------------------------------------
1                00-30-84-18-43-12 1            1       Permanent





Sorted by : VID + MAC            VID : 1    MAC : 00-00-00-00-00-00
  VID : 1                        Unit : 1   Port : 1
  MAC : 00-00-00-00-00-00        Status : Permanent

     [Show)       [More]                  [Set]

                                     <OK>
        Use <TAB> or arrow keys to move, other keys to make changes.
                         <Space> to scroll options.
```

Parameter	Description
VID	The VLAN group this port is assigned to.
MAC Address	The MAC address of a host device attached to this switch.
Unit	The switch unit the host device is attached to.
Port	The port the host device is attached to.
Status	The status for an entry can be set to: **Permanent**: This entry is currently in use and will remain so after the next reset of the switch. **DeleteOnReset**: This entry is currently in use and will remain so until the next reset. **Invalid**: Removes the corresponding entry. **DeleteOnTimeOut**: This entry is currently in use and will remain so until it is aged out. **Other**: This entry is currently in use but the conditions under which it will remain so differ from the preceding values.

Parameter	Description
[Show]	Displays the static address table sorted on VID as the primary key and MAC address as secondary key.
[More]	Scrolls through entries in the static address table.
[Set]	Adds the specified entry to the static address table, such as shown in the following example: VID : 1 MAC : 00-30-84-18-34-22 Unit : 1 Port : 1 Status : Permanent

Resetting the System

Use the Restart command under the Main Menu to reset the management agent. The reset screen includes an option to return all configuration parameters to their factory defaults.



```
                    System Restart Menu
                   ====================

      Restart Option :

          POST                       : YES
          Reload Factory Defaults    : YES
          Keep IP Setting            : YES
          Keep User Authentication   : YES

          [Restart]

           <APPLY>          <OK>        <CANCEL>

   Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
POST	Runs the Power-On Self-Test
Reload Factory Defaults	Reloads the factory defaults
Keep IP Setting	Retains the settings defined in the IP Configuration menu.
Keep User Authentication	Retains the user names and passwords defined in the Console Login Configuration menu.

Logging Off the System

Use the Exit command under the Main Menu to exit the configuration program and terminate communications with the switch for the current session.

Chapter 3

Web-based Management

Web-based Configuration and Monitoring

The Network Management Module provides an embedded HTTP Web agent in addition to the menu-driven system configuration program. This agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above).

Note

If you experience a screen refresh problem with Internet Explorer 5.0, you can use the Back and Forward buttons in the Tool bar to manually refresh the window, or you can use IE 4.0 or Navigator 4.0.

Using the Web browser management interface you can configure a switch stack, view statistics, and monitor network activity. The Web interface also provides access to a range of SNMP management functions with its MIB and RMON browser utilities.

Prior to accessing the Network Management Module from a Web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection or BootP protocol.
2. Set user names and passwords using an out-of-band serial connection. Access to the Web Agent is controlled by the same Administrator user names and passwords as the on-board configuration program.

Note

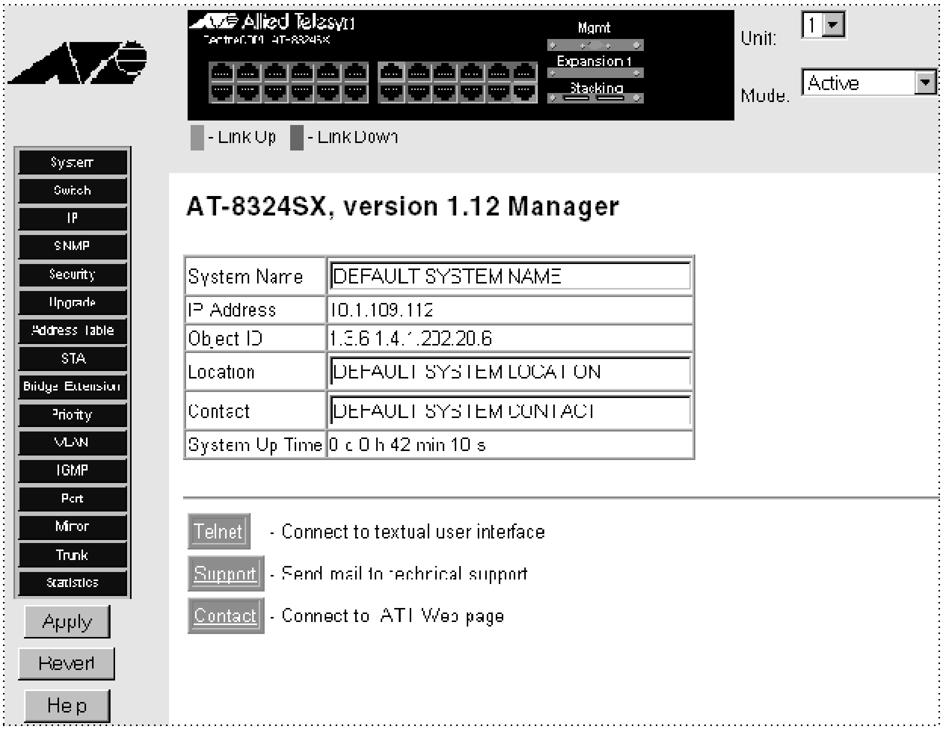
If the PC is directly connected to the AT-8324SX switch, you must turn off the network proxy in the Web browser. For instructions on how to turn off the network proxy, refer to your Web browser documentation.

Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The default user names are "admin" and "guest," with no password. The administrator has Read/Write access to all configuration parameters and statistics, and the guest has Read Only access to the management program.

Home Page

When your Web browser connects with the Network Management Module's Web agent, the home page is displayed. The home page displays the Main Menu on the left-hand side of the screen and the System Information on the right-hand side. The Main Menu links are used to navigate to other menus and display configuration parameters and statistical data.



AT-8324SX, version 1.12 Manager

System Name	DEFAULT SYSTEM NAME
IP Address	10.1.109.112
Object ID	1.3.6.1.4.1.202.20.6
Location	DEFAULT SYSTEM LOCATION
Contact	DEFAULT SYSTEM CONTACT
System Up Time	0 d 0 h 42 min 10 s

Telnet - Connect to textual user interface

Support - Send mail to technical support

Contact - Connect to ATI Web page

If this is your first time to log into the configuration program, you should define a new administrator password, record it and put it in a safe place. From the Main Menu, select Security Configuration and enter a new password for the administrator. Note that passwords can consist of up to 14 alphanumeric characters and are not case sensitive.

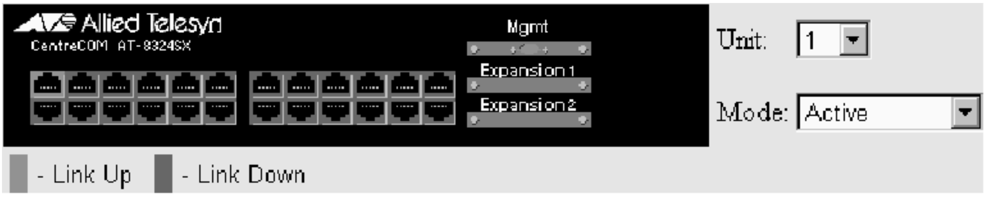
Note

Based on the default configuration, a user is allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

Configurable parameters have a dialog box or drop-down list. Once a configuration change has been made on a page, be sure to click on the "Apply" button at the bottom of the page to confirm the new setting. Alternatively, you can click on "Revert" to clear any changes prior to pressing "Apply."

Panel Display

The Web Agent displays an image of the switch's ports and expansion modules, showing port activity, speed, or duplex mode, depending on the specified mode. Note that clicking on the image of a port or module will display statistics for the selected item.



Unit: 1

Mode: Active

Main Menu

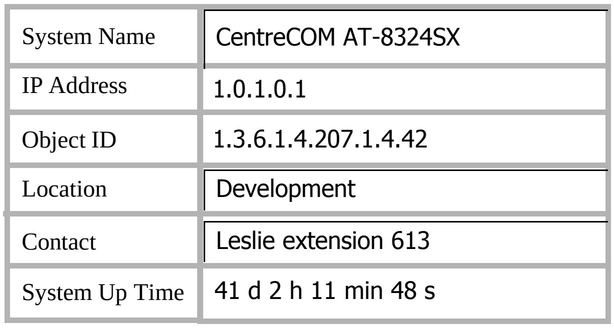
Using the on-board Web agent, you can define system parameters, manage and control the switch, the connected stack and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Menu	Description
System	Provides basic system description, including contact information.
Switch	Shows hardware/firmware version numbers, power status, and expansion modules in use.
IP	Includes boot state, IP address, and Telnet session count.
SNMP	Configures communities and trap managers; and activates traps.
Security	Sets passwords for system access.
Upgrade	Downloads new version of firmware to update your system.
Address Table	Provides full listing of unicast addresses, sorted by address or VLAN.
STA	Enables Spanning Tree Algorithm; also sets parameters for switch priority, hello time, maximum message age, and forward delay; as well as port priority and path cost.

Menu	**Description**
Bridge Extension	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, GMRP multicast filtering, and VLAN extensions.
Priority	Configures default port priorities and queue assignments.
VLAN	Configures VLAN group members, automatic registration with GVRP, and other port-specific VLAN settings.
IGMP	Configures IGMP multicast filtering.
Port	Enables any port, sets communication mode to auto-negotiation, full duplex or half duplex, and enables/ disables flow control.
Mirror	Sets the source and target ports for mirroring.
Trunk	Specifies ports to group into aggregate trunks.
Statistics	Displays statistics on network traffic passing through the selected port.

System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.



System Name	CentreCOM AT-8324SX
IP Address	1.0.1.0.1
Object ID	1.3.6.1.4.207.1.4.42
Location	Development
Contact	Leslie extension 613
System Up Time	41 d 2 h 11 min 48 s

Menu	Description
System Name[1]	Name assigned to the switch system
IP Address[2]	IP address of the agent you are managing. The agent module supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module are assigned an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside of this format will not be accepted by the configuration program.
Object ID	MIB II object identifier for switch's network management subsystem (AT-8324SX: 1.3.6.1.4.207.1.4.42).
Location[1]	Specifies the area or location where the system resides.
Contact[1]	Contact person for the system.
System Uptime	Length of time the current management agent has been running. (Note that the first value is 1/100 seconds.)

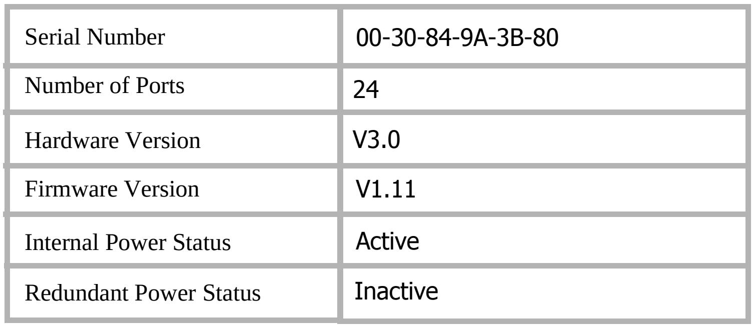
[1] Maximum string length is 45 characters.

[2] The default value is 0.0.0.0.

Switch Information

Use the Switch Information screen to display hardware/firmware version numbers for the main board and agent modules, as well as the power status and modules plugged into the system.

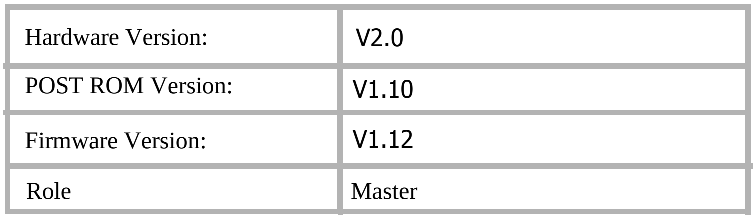
Main Board



Serial Number	00-30-84-9A-3B-80
Number of Ports	24
Hardware Version	V3.0
Firmware Version	V1.11
Internal Power Status	Active
Redundant Power Status	Inactive

Parameter	Description
Serial Number	Serial number of the main board.
Number of Ports	Number of ports in this unit.
Hardware Version	Hardware version of the main board.
Firmware version	System ROM version.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.

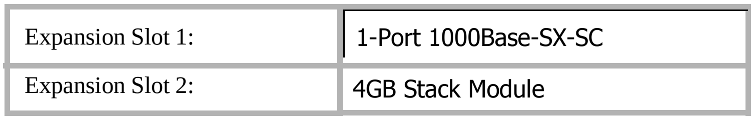
Management Expansion Slot



Hardware Version:	V2.0
POST ROM Version:	V1.10
Firmware Version:	V1.12
Role	Master

Parameter	Description
Hardware Version	Hardware version of the Agent Module
POST ROM Version	Version number of the Agent Module’s Power-on Self-test.
Firmware Version	Agent Module’s firmware version
Role	Shows if this module is Master or Slave.

Expansion Slot

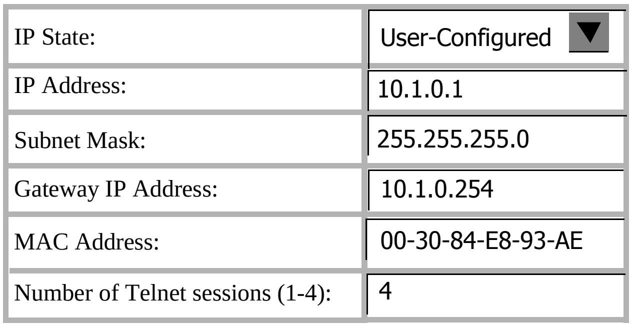


Expansion Slot 1:	1-Port 1000Base-SX-SC
Expansion Slot 2:	4GB Stack Module

Parameter	Description
Expansion Slot 1	Shows module type if inserted (100Base-FX, 1000Base-SX, or 1000Base-LX).
Expansion Slot 2	Shows module type if inserted (100Base-FX, 1000Base-SX, 1000Base-LX or Stack).

IP Configuration

Use the IP Configuration screen to set the bootup option, configure the IP addresses for the agent module, or set the number or concurrent Telnet sessions allowed. The screen shown below is described in the following table.



IP State:	User-Configured ▼
IP Address:	10.1.0.1
Subnet Mask:	255.255.255.0
Gateway IP Address:	10.1.0.254
MAC Address:	00-30-84-E8-93-AE
Number of Telnet sessions (1-4):	4

Parameter	Default	Description
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BootP). Options include: ❑ USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.). ❑ BootP Get IP - IP is enabled but will not function until a BootP reply has been received. BootP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BootP values include the IP address, default gateway, subnet mask, TFTP boot file name, and TFTP server IP.)
IP Address	10.1.0.1	IP address of the agent you are managing. The Agent Module supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the Agent Module are assigned an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.255.0	Subnet mask of the agent you have selected. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP Address	0.0.0.0	Gateway used to pass trap messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.

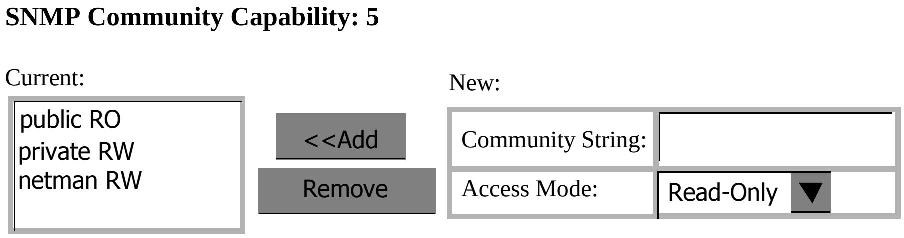
Parameter	Default	Description
MAC Address	-	Physical address of the Agent Module
Number of Telnet Sessions	4	Sets the number of concurrent Telnet sessions allowed to access the Agent Module.

SNMP Configuration

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the sections.

SNMP Community

The following figure and table describe how to configure the community strings authorized for trap management access. Up to 5 community names may be entered.



SNMP Community Capability: 5

Current:

public RO
private RW
netman RW

New:

Community String:

Access Mode: Read-Only

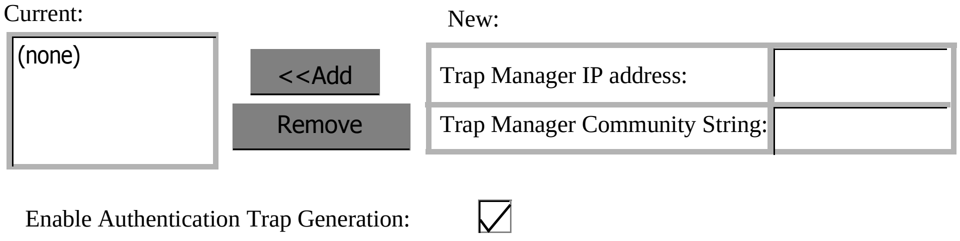
Parameter	Description
Community String	A community entry authorized for trap management access. (The maximum string length is 19 characters).
Access Mode	Management access is restricted to Read Only or Read/Write.
Add/Remove	Add/remove strings from the active list

The default community strings are listed here.

Purpose	Community String	Privileges
General access	public	Read Only
Network administrators	private	Read/Write
Network management	netman	Read/Write

Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.



Current:

(none)

New:

Trap Manager IP address:

Trap Manager Community String:

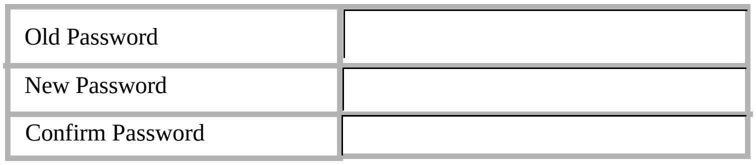
Enable Authentication Trap Generation: ☑

Parameter	Description
Trap Manager IP Address	IP address of the trap manager.
Trap Manager	A community specified in the SNMP Communities table.
Add/Remove	Add/remove strings from the active list.
Enable Authentication Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)

Security Configuration

Use the Security Configuration screen to restrict management access based on specified user names and passwords. The Administrator has write access for parameters governing the SNMP agent. You should therefore assign a user name and password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you can not gain access to the system’s configuration program, contact Allied Telesyn for assistance.) The parameters shown on this screen are indicated in the following figure and table.

Change Password



Old Password	
New Password	
Confirm Password	

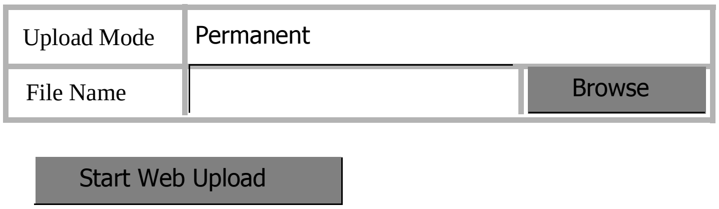
This password is for the system Administrator access, with access privilege of Read/Write for all screens. Passwords can consist of up to 11 alphanumeric characters and are not case sensitive. (Default name: admin; default password: null)

Firmware Upgrade Options

You can upgrade system firmware via a Web browser, a TFTP server, or a direct connection to the console port.

Web Upload Management

Use the Web Upload Management menu to load software updates into the switch. The upload file should be an AT-8324SX compressed binary file from Allied Telesyn; otherwise the agent will not accept it. The success of the upload operation depends on the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

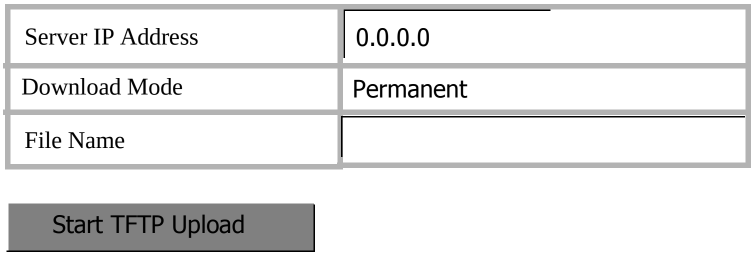


Upload Mode	Permanent
File Name	

Parameter	Description
Upload Mode	Uploads to permanent flash ROM.
File Name	The AT-8324SX compressed binary file to upload. Use the browse button to locate the file on your local network.
Start Web Upload	Uploads the specified file.

TFTP Download Management

Use the TFTP Download Management menu to load software updates into the switch. The download file should be an AT-8324SX compressed binary file from Allied Telesyn; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

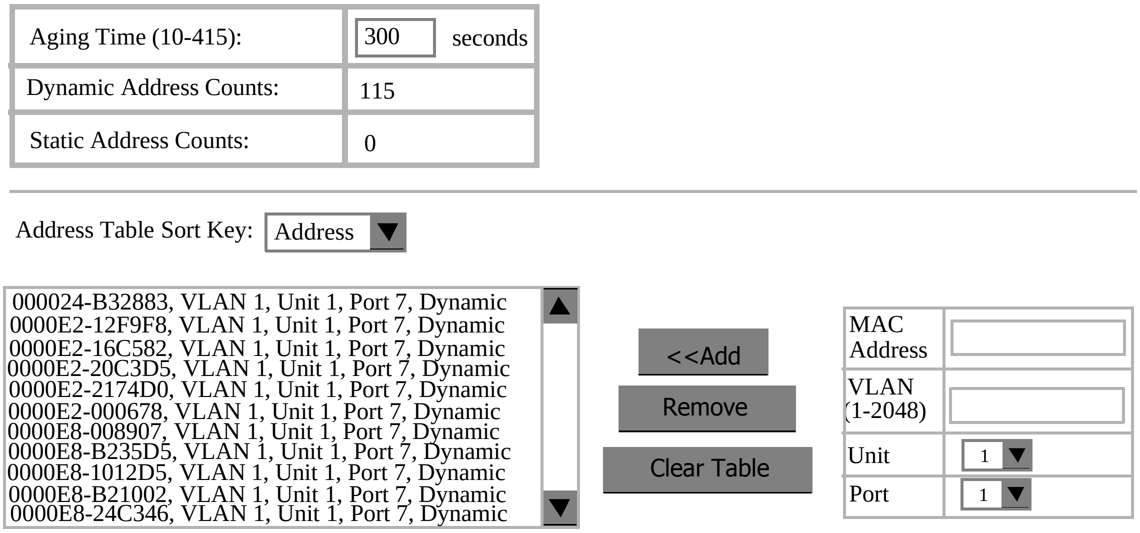


Server IP Address	0.0.0.0
Download Mode	Permanent
File Name	

Parameter	Description
Server IP Address	IP address of a TFTP server.
Download Mode	The system downloads to permanent flash ROM.
File Name	The AT-8324SX compressed binary file to download.
Start TFTP Download	Issues a request to TFTP server to download the specified file.

Address Table Configuration

The Address Table contains the unicast MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN). You can also clear the entire address table, or information associated with a specific port, address, or VLAN identifier; or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.



Aging Time (10-415):	300 seconds
Dynamic Address Counts:	115
Static Address Counts:	0

Address Table Sort Key: Address

```
000024-B32883, VLAN 1, Unit 1, Port 7, Dynamic
0000E2-12F9F8, VLAN 1, Unit 1, Port 7, Dynamic
0000E2-16C582, VLAN 1, Unit 1, Port 7, Dynamic
0000E2-20C3D5, VLAN 1, Unit 1, Port 7, Dynamic
0000E2-2174D0, VLAN 1, Unit 1, Port 7, Dynamic
0000E2-000678, VLAN 1, Unit 1, Port 7, Dynamic
0000E8-008907, VLAN 1, Unit 1, Port 7, Dynamic
0000E8-B235D5, VLAN 1, Unit 1, Port 7, Dynamic
0000E8-1012D5, VLAN 1, Unit 1, Port 7, Dynamic
0000E8-B21002, VLAN 1, Unit 1, Port 7, Dynamic
0000E8-24C346, VLAN 1, Unit 1, Port 7, Dynamic
```

MAC Address	
VLAN (1-2048)	
Unit	1
Port	1

Parameter	**Description**
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. The range is 10 - 415 seconds; and the default is 300 seconds.
Dynamic Address Count	The number of dynamically learned addresses.
Static Address Count	The number of statistically configured addresses
Address Table Sort Key	The system displays the MAC address of each node, the switch unit and the port whose address table includes this MAC address, the associated VLAN(s), and the address status (i.e., dynamic or static)
Address Table	All entries, sorted by address or VLAN ID.
New Static Address	Use these fields to add or remove a static entry to the address table. Indicate the address, stack unit, port and VLAN group when adding a new entry.
Add/Remove	Adds/removes selected address.
Clear Table	Removes all addresses from the address table.

STA (Spanning Tree Algorithm)

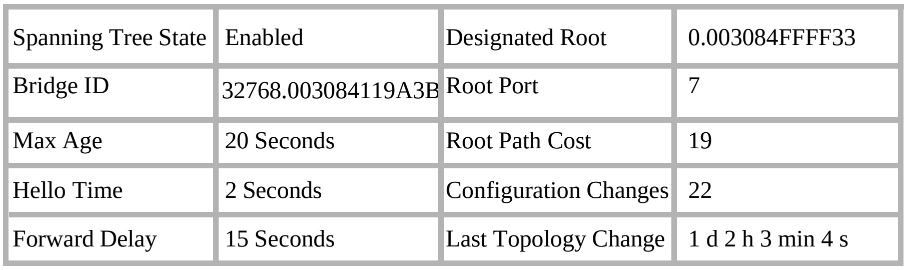
The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, STA compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to Chapter 4.

Spanning Tree Information

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port or module. To make any changes to the parameters for the Spanning Tree, use the Spanning Tree Configuration menu. Also note that this screen cannot be accessed unless you have already enabled the Spanning Tree Algorithm via the Spanning Tree Configuration menu.

Spanning Tree

The parameters shown in the following figure and table describe the current bridge STA Information.



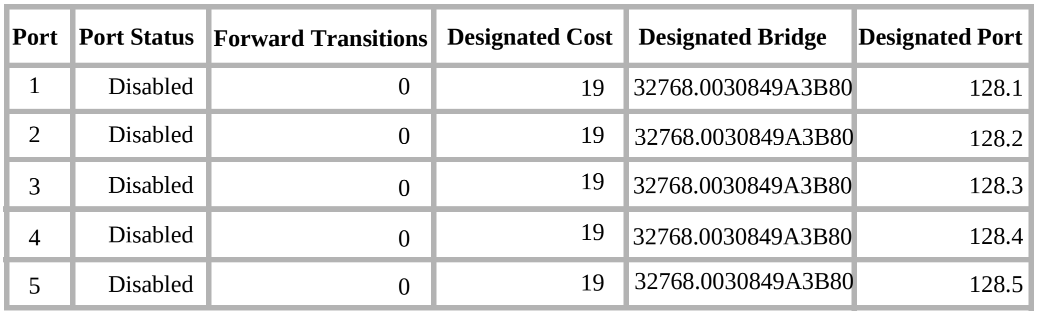
Spanning Tree State	Enabled	Designated Root	0.003084FFFF33
Bridge ID	32768.003084119A3B	Root Port	7
Max Age	20 Seconds	Root Path Cost	19
Hello Time	2 Seconds	Configuration Changes	22
Forward Delay	15 Seconds	Last Topology Change	1 d 2 h 3 min 4 s

Parameter	Description
Spanning Tree State	Shows if switch is enabled to participate in an STA compliant network.
Bridge ID	A unique identifier for this bridge, consisting of bridge priority plus MAC address (where the address is normally taken from Port 1).
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.

Parameter	Description
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Root Path Cost	The path cost from the root port on this switch to the root device.
Configuration Changes	The number of times the spanning tree has been reconfigured.
Last Topology Change	The time since the spanning tree was last reconfigured.

STA Port Configuration

The parameters shown in the following figure and table are for port or module STA Information (Port 1-12, Port 13-24, Expansion Slot 1 or Expansion Slot 2).

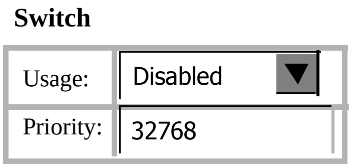


Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	Disabled	0	19	32768.0030849A3B80	128.1
2	Disabled	0	19	32768.0030849A3B80	128.2
3	Disabled	0	19	32768.0030849A3B80	128.3
4	Disabled	0	19	32768.0030849A3B80	128.4
5	Disabled	0	19	32768.0030849A3B80	128.5

Parameter	**Description**
Port Status	Displays the current state of this port within the spanning tree: ❑ **Disabled:** Port has been disabled by the user or has failed diagnostics. ❑ **Blocked:** Port receives STA configuration messages, but does not forward packets. ❑ **Listening:** Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. ❑ **Learning:** Has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding: The port forwards packets, and continues learning addresses. The rules defining port status are: ❑ A port on a network segment with no other STA compliant bridging device is always forwarding. ❑ If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. ❑ All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Forward Transitions	The number of times the port has changed status to forwarding state.
Designated Cost	The cost for a packet to travel from this port to the root in the current spanning tree configuration. The slower the media, the higher the cost.
Designated Bridge	The priority and MAC address of the device through which this port must communicate to reach the root of the spanning tree.
Designated Port	The port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

Spanning Tree Configuration

The following figures and tables describe Bridge STA configuration.

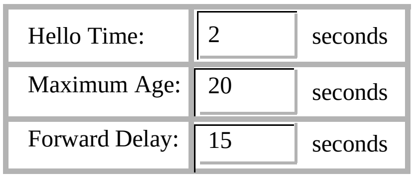


Switch

Usage:	Disabled
Priority:	32768

Parameter	Default	Description
Usage	Enabled	Enable this parameter to participate in an STA compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.

When the Switch Becomes Root

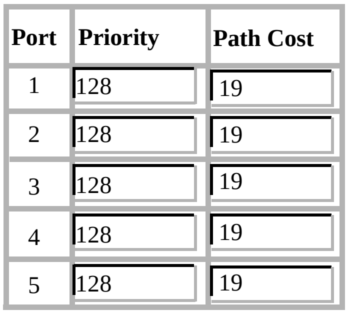


Hello Time:	2	seconds
Maximum Age:	20	seconds
Forward Delay:	15	seconds

Parameter	Default	Description
Hello Time	2	The time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) -1].
Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time + 1)]. The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

STA Port Configuration

The following figure and table describe STA configuration for ports or modules. (Note that the Spanning Tree Configuration screen for the expansion slots also indicates module type.)



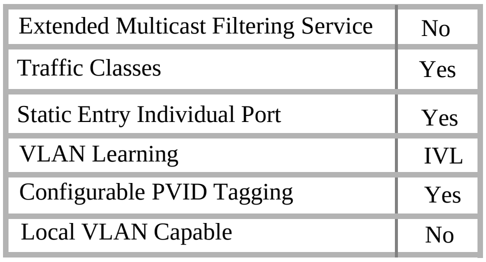
Port	Priority	Path Cost
1	128	19
2	128	19
3	128	19
4	128	19
5	128	19

Parameter	Default	Description
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. The default and recommended range is: ❑ Standard Ethernet: 100 (50~600) ❑ Fast Ethernet: 19 (10~60) ❑ Gigabit Ethernet: 4 (3~10) ❑ The full range is 0 - 65535. Note: Path cost takes precedence over port priority.

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and Virtual LANs. To configure these extensions, use the Extended Bridge Configuration screen as shown below.

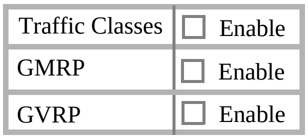
Bridge Capability



Extended Multicast Filtering Service	No
Traffic Classes	Yes
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Parameter	Description
Extended Multicast Filtering Services	Enables filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Note that this function is not available for the current firmware release.
Traffic Classes	Provides mapping of user priorities to multiple traffic classes. (Refer to the Priority menu.)
Static Entry Individual Port	Enables static filtering for unicast and multicast addresses. (Refer to the Address Table.)
VLAN Learning	This switch uses Independent VLAN Learning (IVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	Allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. (Refer to VLAN/VLAN Port Configuration.).
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

Bridge Settings



Traffic Classes	□ Enable
GMRP	□ Enable
GVRP	□ Enable

Parameter	Description
Traffic Class[1]	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by setting this parameter to False.
GMRP[1]	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups.
	The Internet Group Management Protocol (IGMP) is currently used by this switch to provide automatic multicast filtering.
GVRP[1]	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network.

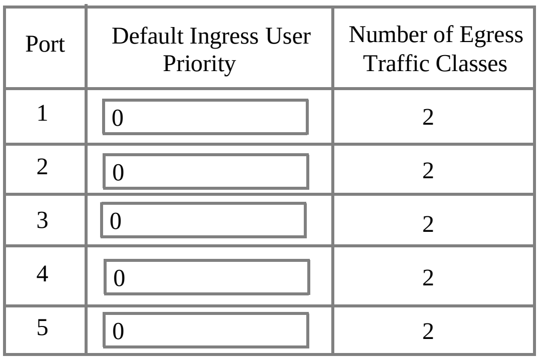
[1] Not implemented in this firmware release.

Priority

IEEE 802.1p defines up to eight separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with weighted fair queuing for each port. You can use the Priority menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections.

Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the Port Priority Configuration screen to adjust the default priority for any port as shown below:

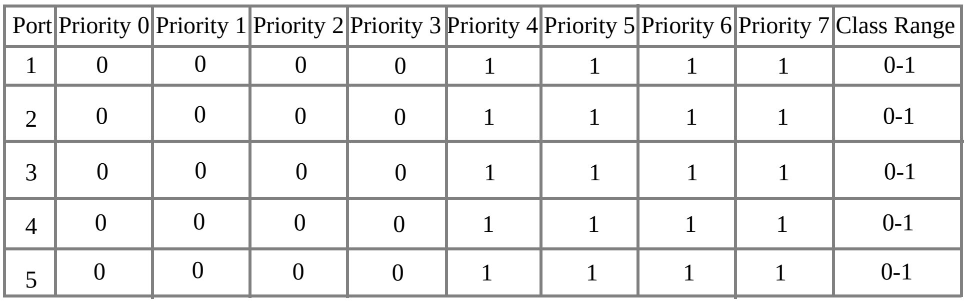


Port	Default Ingress User Priority	Number of Egress Traffic Classes
1	0	2
2	0	2
3	0	2
4	0	2
5	0	2

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0-7, where 0-3 specifies the low priority queue and 4-7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

Port Traffic Class Information

This switch provides two priority levels with weighted fair queuing for port egress. This means that any frames with a default or user priority from 0-3 are sent to the low priority queue "0" while those from 4-7 are sent to the high priority queue "1" as shown in the following screen:



Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Class Range
1	0	0	0	0	1	1	1	1	0-1
2	0	0	0	0	1	1	1	1	0-1
3	0	0	0	0	1	1	1	1	0-1
4	0	0	0	0	1	1	1	1	0-1
5	0	0	0	0	1	1	1	1	0-1

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0-3 specify the low priority queue and 4-7 specify the high priority queue.

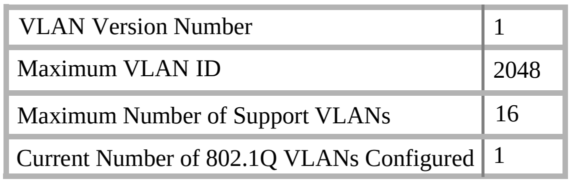
Configuring Virtual LANs

Use the VLAN Configuration menu to assign any port on the switch to any of up to 16 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of IPX traffic. By using IEEE 802.1Q compliant VLANs and GARP VLAN Registration Protocol, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and much cleaner network environment.

For a more detailed description of how to use VLANs, see Chapter 4. The VLAN configuration screens are described in the following sections.

VLAN Basic Information

The VLAN Basic Information screen displays basic information on the VLAN type support by this switch.

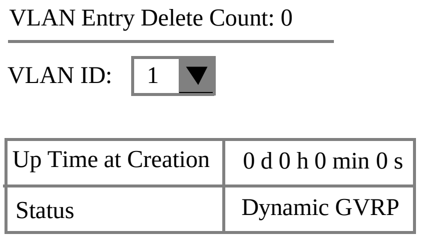


VLAN Version Number	1
Maximum VLAN ID	2048
Maximum Number of Support VLANs	16
Current Number of 802.1Q VLANs Configured	1

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

VLAN Current Table

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN. The current configuration is shown in the following screen.

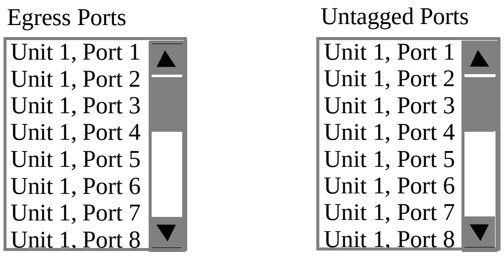


VLAN Entry Delete Count: 0

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 0 s
Status	Dynamic GVRP

Parameter	Description
VLAN Entry Delete Count	The number of times a VLAN entry has been deleted from this table.
VLAN ID	The ID for the VLAN currently displayed.
Up Time at Creation	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch: Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.

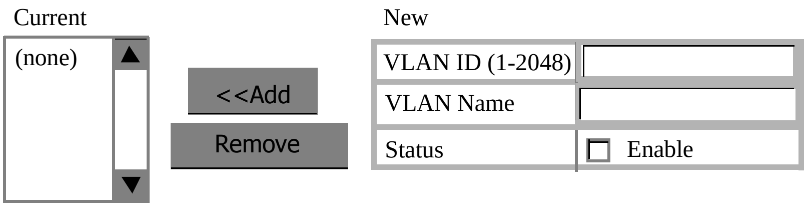


Egress Ports	Untagged Ports
Unit 1, Port 1	Unit 1, Port 1
Unit 1, Port 2	Unit 1, Port 2
Unit 1, Port 3	Unit 1, Port 3
Unit 1, Port 4	Unit 1, Port 4
Unit 1, Port 5	Unit 1, Port 5
Unit 1, Port 6	Unit 1, Port 6
Unit 1, Port 7	Unit 1, Port 7
Unit 1, Port 8	Unit 1, Port 8

Parameter	Description
Egress Ports	Shows the ports which have been added to the displayed VLAN group.
Untagged Ports	Shows the untagged VLAN port members.

VLAN Static List

Use this screen to create or remove VLAN groups.



Current: (none)

VLAN ID (1-2048):

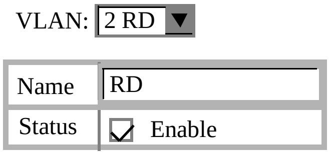
VLAN Name:

Status: □ Enable

Parameter	Description
Current	Lists all the current VLAN groups created for this system. Up to 16 VLAN groups can be defined. To allow this switch to participate in external VLAN groups, you must use the VLAN ID for the concerned external groups.
New	Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
Status	Enables/disables the specified VLAN.
Add	Adds a new VLAN group to the current list.
Remove	Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

VLAN Static Table

Use this screen to modify the settings for an existing VLAN. You can add/delete port members for a VLAN from any unit in the stack, disable or enable VLAN tagging for any port, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Note that VLAN1 is fixed as an untagged VLAN containing all ports in the stack, and cannot be modified via this screen.)



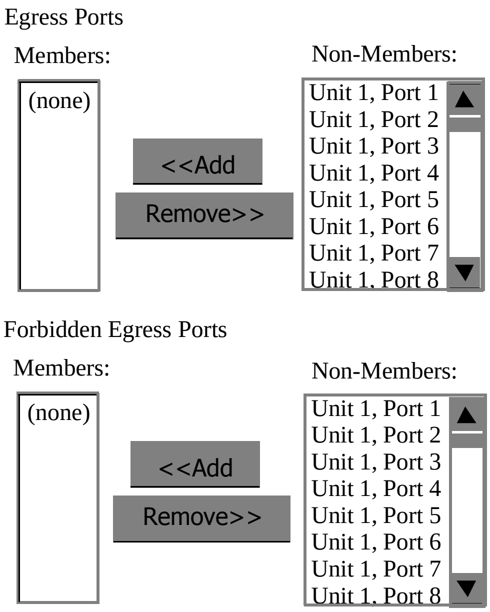
VLAN: 2 RD

Name: RD

Status: ☑ Enable

Parameter	Description
VID	The ID for the VLAN currently displayed. Range: 1-2048
Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters.
Status	Enables/disables the specified VLAN.

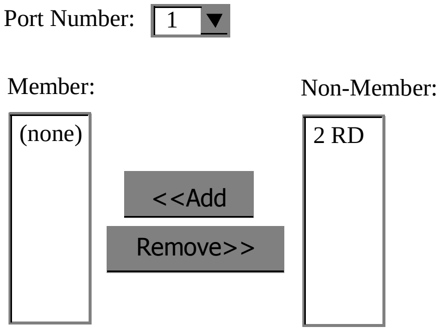
Use the screens shown below to assign ports to the specified VLAN groups as an IEEE802.1Q tagged port. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices. If the port is connected to VLAN-unaware devices, frames will be passed to the untagged VLAN group this port has been assigned to under VLAN Port Configuration.



Parameter	**Description**
Egress Ports	Adds ports to the specified VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP.

VLAN Static Membership by Port

Use the screen below to assign VLAN groups to the selected port. To perform detailed port configuration for a specific VLAN, use the VLAN Static Table.



Port Number: 1

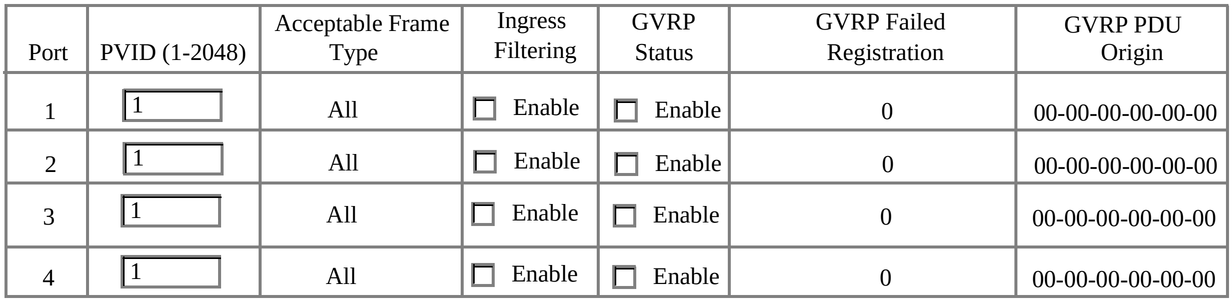
Member: (none)

Non-Member: 2 RD

Parameter	Description
Port Number	Port number on the switch selected from the upper display panel.
Add/Remove	Add or remove selected VLAN groups for the port indicated in the Port Number field.

VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features:



Port	PVID (1-2048)	Acceptable Frame Type	Ingress Filtering	GVRP Status	GVRP Failed Registration	GVRP PDU Origin
1	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
2	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
3	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
4	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type[1]	This switch accepts “All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering[1]	If set to "True," incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
GVRP Status	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled for the switch before this setting can take effect. (See Device Control Menu / Extended Bridge Configuration.)
GVRP Failed Registrations	The total number of failed GVRP registrations, for any reason, on this port.
GVRP Last PDU Origin	The Source MAC Address of the last GVRP message received on this port.

[1] 1: This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.

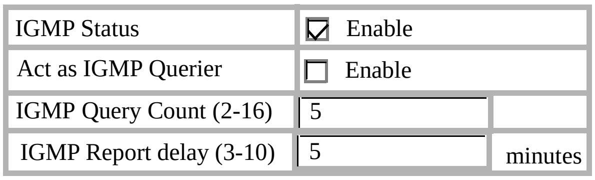
IGMP Multicast Filtering

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its services to the network, and any hosts which want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast server/router it passed through to ensure that traffic is only passed on the hosts which subscribed to this service.

The AT-8324SX switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast group. You can use the IGMP Configuration screen to configure multicast filtering shown below:



IGMP Status	☑ Enable	
Act as IGMP Querier	□ Enable	
IGMP Query Count (2-16)	5	
IGMP Report delay (3-10)	5	minutes

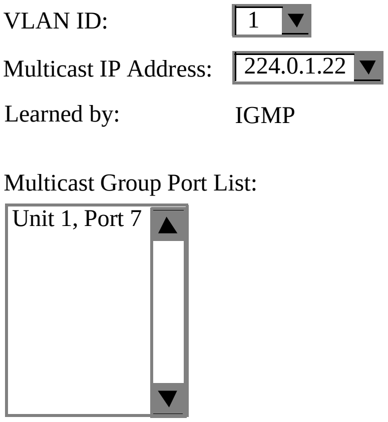
Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
ACT as IGMP Querier	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic. (Not available for the current firmware release.)
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports.
IGMP Report Delay	The time (in minutes) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out that port and removes the entry from its list.

Note

The default values are indicated in the sample screen.

IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.



VLAN ID: 1

Multicast IP Address: 224.0.1.22

Learned by: IGMP

Multicast Group Port List:

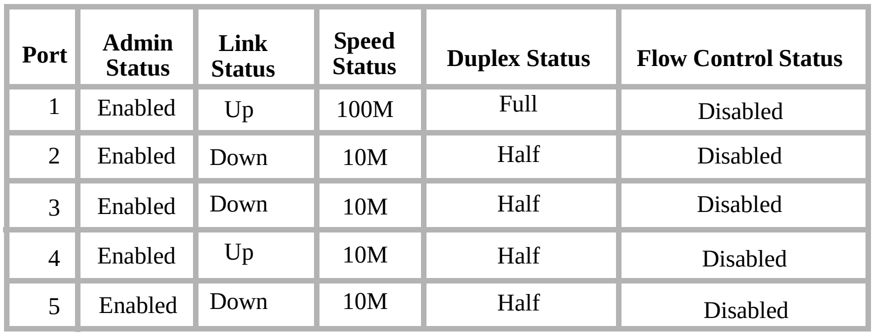
Unit 1, Port 7

Parameter	Description
VID	VLAN ID assigned to this multicast group.
Multicast IP	IP address for specific multicast services.
Learned by	Indicates the manner in which this address was learned: Dynamic or IGMP.
Multicast Group Port List	The switch ports registered for the indicated multicast service.

Port Menus

Port Information

The Port Information screen displays the port status, link state, the communication speed and duplex mode, as well as the flow control in use. To change any of the port settings, use the Port Configuration menu. The parameters shown in the following figure and table are for the RJ-45 ports.

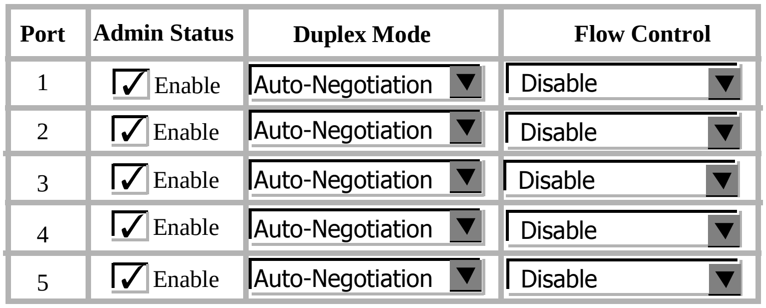


Port	Admin Status	Link Status	Speed Status	Duplex Status	Flow Control Status
1	Enabled	Up	100M	Full	Disabled
2	Enabled	Down	10M	Half	Disabled
3	Enabled	Down	10M	Half	Disabled
4	Enabled	Up	10M	Half	Disabled
5	Enabled	Down	10M	Half	Disabled

Parameter	Description
Admin Status	Shows if the port is enabled or not.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Shows the port speed (10M or 100M).
Duplex Status	Displays the current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to hub.

Port Configuration

Use the Port Configuration menus to configure any port or module on the switch.

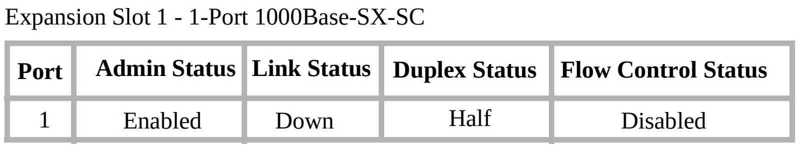


Port	Admin Status	Duplex Mode	Flow Control
1	☑ Enable	Auto-Negotiation ▼	Disable ▼
2	☑ Enable	Auto-Negotiation ▼	Disable ▼
3	☑ Enable	Auto-Negotiation ▼	Disable ▼
4	☑ Enable	Auto-Negotiation ▼	Disable ▼
5	☑ Enable	Auto-Negotiation ▼	Disable ▼

Parameter	**Default**	**Description**
Admin Status	Enable	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Duplex Mode	Auto-Negotiation	Used to set the current port speed, duplex mode, and auto-negotiation. The default for RJ-45 ports is auto-negotiation. (Auto-negotiation is not available for 100Base-FX ports.)
Flow Control	Disable	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to hub.

Expansion Port Information

The Expansion Port Information screen displays the port status, link state, the communication speed and duplex mode, as well as the flow control in use. To change any of the port settings, use the Expansion Port Configuration menu. The parameters shown in the following figure and table are for expansion ports.



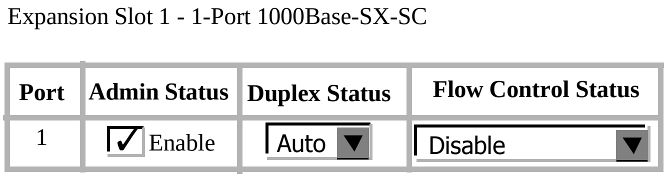
Expansion Slot 1 - 1-Port 1000Base-SX-SC

Port	Admin Status	Link Status	Duplex Status	Flow Control Status
1	Enabled	Down	Half	Disabled

Parameter	Description
Admin Status	Shows in the port is enabled or not.
Link Status	Indicates if the port has a valid connection to an external device.
Duplex Status	Displays the current duplex mode (half or full duplex).
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to hub.

Expansion Port Configuration

Use the Expansion Port Configuration menus to configure any port or module on the switch.



Expansion Slot 1 - 1-Port 1000Base-SX-SC

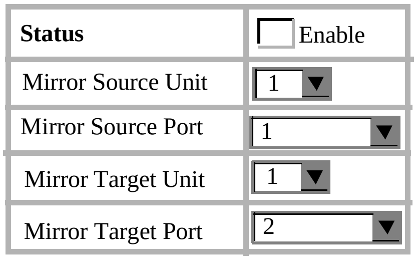
Port	Admin Status	Duplex Status	Flow Control Status
1	☑ Enable	Auto ▼	Disable ▼

Parameter	Default	Description
Admin Status	Enable	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Duplex Mode	Auto-Negotiation	Used to set the port of full or half duplex mode, or auto-negotiation. The default for gigabit ports is auto-negotiation. However, note that auto-negotiation is not available for the 100Mbps fiber ports.
Flow Control	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to hub.

Using a Port Mirror for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You cana then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, not that the target port must be included in the same VLAN as the source port.

You can use the Mirror Port Configuration screen to designate a single port pair for mirroring as shown below:



Status	□ Enable
Mirror Source Unit	1 ▼
Mirror Source Port	1 ▼
Mirror Target Unit	1 ▼
Mirror Target Port	2 ▼

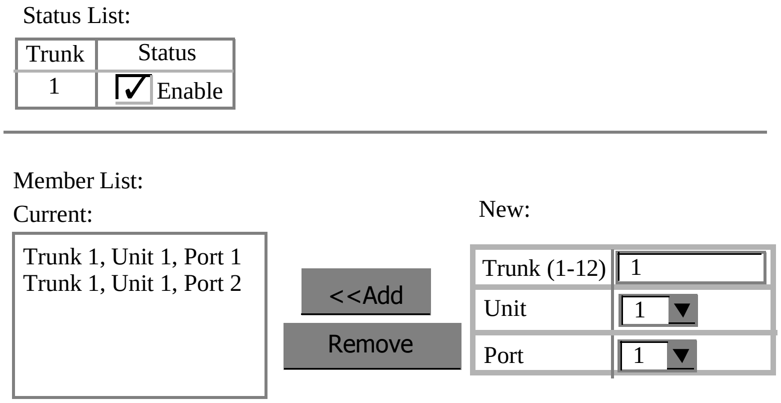
Parameter	**Description**
Status	Enables/disables port mirroring.
Mirror Source Unit	The switch containing the mirror source port.
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Unit	The switch containing the mirror target port.
Mirror Target Port	The port that will “duplicate” or “mirror” all the traffic happening on the monitored port.

Port Trunk Configuration

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up to four trunk connections (combining 2 to 4 ports into a fat pipe) between any two AT-8324SX switches. However, before making any physical connections between devices, us the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- The ports used in a trunk must all be of the same media type (RJ-45, 100 Mbps fiber, 1000 Mbps fiber). The ports that can be assigned to the same trunk have certain other restrictions as described later in this section.
- Ports can only be assigned to one trunk.
- The ports in the trunk must belong to the same switch chip (as explained later in this section.
- The ports at both ends of a connection must be configured /as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including speed, duplex mode, and VLAN assignments.
- The communication mode must be configured identically at both ends of the trunk.
- None of the ports in a trunk can be configured as a mirror source port or a mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to added, or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

You can use the Port Trunking Configuration screen to set up port trunks as shown below:



Status List:

Trunk	Status
1	☑ Enable

Member List:

Current:

Trunk 1, Unit 1, Port 1
Trunk 1, Unit 1, Port 2

New:

Trunk (1-12)	1
Unit	1 ▼
Port	1 ▼

Parameter	Description
Trunk	A unique identifier for this trunk. You can configure up to four trunks per switch.
Status	Enables or disables the displayed port trunk.
Member List	You can create up to 16 trunks for the entire stack by specifying the trunk identifier, switch unit, and port number, and then pressing the "Add" button. Each trunk can contain from 2 to 4 ports.

The RJ-45 ports used for each trunk must all be on the same internal switch chip. The port groups permitted include:

- ❑ Group 1: 1, 2, 3, 4 and 13, 14, 15, 16
- ❑ Group 2: 5, 6, 7, 8 and 17, 18, 19, 20

The 100Base-FX fiber optic ports used for one side of a trunk must all be on the same module. However, the 1000Base-SX and 1000Base-LX ports used for one side of a trunk may be on any switch in the stack, or both on the same switch if used as a standalone switch.

For example, when using Gigabit ports to form a trunk within a stack, the Gigabit ports will all be at Port 25. In this case, you could specify a trunk group consisting of:

(Unit1-Port25, Unit2-Port25, Unit3-Port25, Unit4-Port25)

or two trunks consisting of:

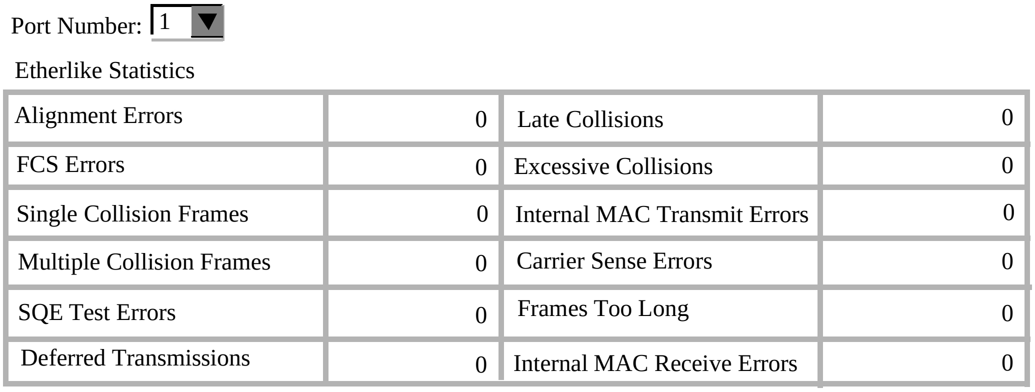
(Unit1-Port25, Unit2-Port25) and (Unit3-Port25, Unit4-Port25)

Port Statistics

Use the Port Statistics menu to display Etherlike or RMON statistics for any port in the stack. Select the required stack unit, and port or module. The statistics displayed are indicated in the following figure and table.

Etherlike Statistics

Etherlike Statistics display key statistics from the Ethernet-like MIB for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). Values displayed have been accumulated since the last system reboot.



Port Number: 1 ▼

Etherlike Statistics

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

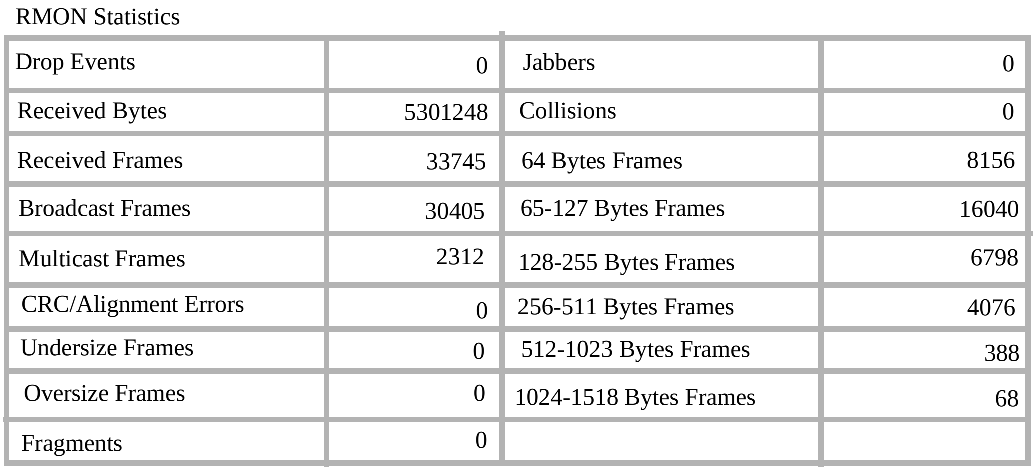
Parameter	Description
Alignment Errors	For 10 Mbps ports, this counter records alignment errors (mis-synchronized data packets). For 100 Mbps ports, this counter records the sum of alignment errors and code errors (frames received with rxerror signal).
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames[1]	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames[1]	A count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors[1]	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions[1]	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Parameter	**Description**
Excessive Collisions[1]	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors[1]	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors[1]	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors[1]	The number of frames for which reception failed due to an internal MAC sublayer receive error.

[1] The reported values will always be zero because these statistics are not supported by the internal chip set.

RMON Statistics

RMON Statistics display key statistics for each port or media module from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types passing through each port. Values displayed have been accumulated since the last system reboot.



RMON Statistics

Drop Events	0	Jabbers	0
Received Bytes	5301248	Collisions	0
Received Frames	33745	64 Bytes Frames	8156
Broadcast Frames	30405	65-127 Bytes Frames	16040
Multicast Frames	2312	128-255 Bytes Frames	6798
CRC/Alignment Errors	0	256-511 Bytes Frames	4076
Undersize Frames	0	512-1023 Bytes Frames	388
Oversize Frames	0	1024-1518 Bytes Frames	68
Fragments	0		

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	For lOMbs ports, the counter records CRC/alignment errors (FCS or alignment errors). For 10OMbs ports, the counter records the sum of CRC/alignment errors and code errors (frame received with rxerror signal).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Parameter	Description
256-511 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Chapter 4

Advanced Topics

This AT-8324SX switch supports Layer 2 switching and other advanced features, which are described in this chapter.

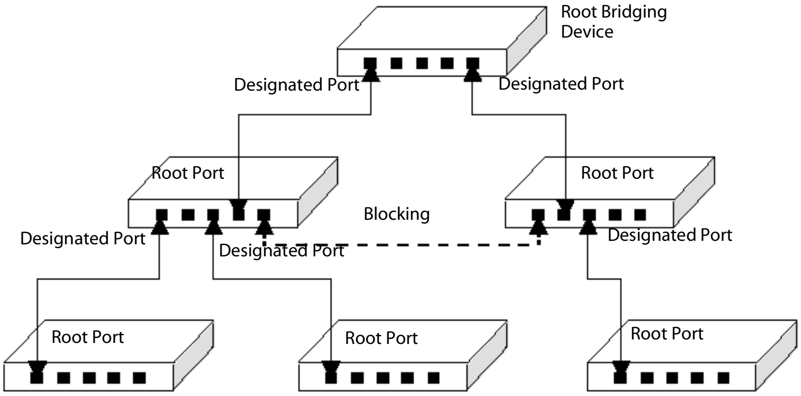
Spanning Tree Algorithm

The Spanning Tree Algorithm (that is, the STA configuration algorithm as outlined in IEEE 802.1 D) can be used to detect and disable network loops, and to provide link backup. This allows the switch to interact with other bridging devices (including STA compliant switches, bridges or routers) in your network to ensure that only one route exists between any two stations on the network. If redundant paths or loops are detected, one or more ports are put into a blocking state (stopped from forwarding packets) to eliminate the extra paths. Moreover, if one or more of the paths in a stable spanning tree topology fail, this algorithm will automatically change ports from blocking state to forwarding state to re-establish contact with all network stations.

The STA uses a distributed algorithm to select a bridging device (STA compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

The following figure gives an illustration of how the Spanning Tree Algorithm assigns bridging device ports.



Using STA and Trunk Ports

The Spanning Tree Algorithm will treat a trunk as a whole instead of individual ports. STA will determine the path cost and path priority of a trunk connection based on the first port. However, the states of individual trunk ports are determined based on individual link status. Remember that the first port of a trunk MUST be connected to make sure STA works properly.

Virtual LANs

Switches do not inherently support broadcast domains, which can lead to broadcast storms in large networks that handle a lot of IPX traffic. In conventional networks with routers, broadcast traffic is split up into separate domains to confine broadcast traffic to the originating group and provide a much cleaner network environment. By supporting VLANS, this switch allows you to create segregated broadcast domains. However, note that if you need to support intra-VLAN communications, you must use a router or Layer 3 switch.

An IEEE 802.IQ VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, but also allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a higher level of network security, since traffic must pass through a Layer 3 switch or a router to reach a different VLAN.

The AT-8324SX switch supports the following VLAN features:

- Up to 16 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GARP/GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs (so long as an end station’s network interface card is 802.1Q compliant and is configured for multiple VLANs)
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Two-level priority queue
- Port trunking with VLANs

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) it will participate in. (By default all ports are assigned to VLAN 1 as untagged ports.) Add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and the device at the other end of the link also supports 802.1Q VLANS. Then assign the port at the other end of the link to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANS, but the device at the other end of the link does not support VLANS, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

Port-based VLANs are tied to specific ports. The switch's forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding and flooding decisions, the switch learns the relationship of the MAC address to its related port-and thus to the VLAN-at run-time.

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways:

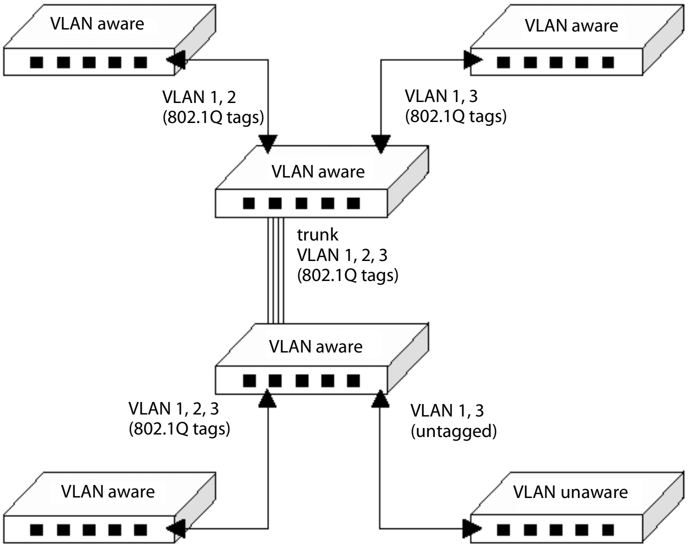
- ❑ If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port).
- ❑ If the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you must connect them using a router or Layer 3 switch.

Forwarding Tagged/ Untagged Frames

Ports can be assigned to one untagged VLAN and multiple tagged VLANS. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port's default VID. The default PVID is VLAN 1, but this can be changed (see page 2-35 or 3-25).



Forwarding Traffic with Unknown VLAN Tags

Up to 2048 VLANs are supported by the IEEE 802.lQ protocol, but this switch only supports 16 VLANS. Therefore, if this switch is attached to any device that forwards frames with unknown VLAN tags, or to endstations which issue VLAN registration requests for unknown VLANS, this traffic will be dropped.

Automatic VLAN Registration

GVRP defines a system whereby the switch can automatically learn the VLANs each endstation should be assigned to. If an endstation (or its network adapter) supports the IEEE 802. 1 Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANS, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANS, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

Port Trunks

You can configure up to three port trunks on this switch, or 12 trunks for the entire stack. Each trunk can combine up to four ports into an aggregate connection with up to 800 Mbps of bandwidth when operating at full duplex. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail.

When using port trunks, remember that:

- ❑ Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.
- ❑ To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

Class-of-Service (CoS) Support

The AT-8126XS switch provides two transmit queues on each port, with a weighted round-robin scheme. This function can be used to provide independent priorities for various types of data such as real-time video or voice, and best-effort data.

Priority assignment to a packet in the AT-8126XS switch is accomplished through explicit assignment by end stations which have applications that require a higher priority than best-effort. This switch utilizes the IEEE 802.lp and 802.lQ tag structure to decide priority assignments for the received packets.

IGMP Snooping and IP Multicast Filtering

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast router/switch. The protocol's mechanisms allow a host to inform its local router/switch that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer-3, multicast routers use this information, along with a multicast routing protocol, to support IP multicasting across the Internet.

IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with forwarding multicast traffic from the local router/switch to group members on directly attached subnetwork or LAN segment.

This switch supports IP Multicast Filtering by:

- ❑ Passively snooping on the IGMP Query and IGMP Report packets transferred between IP multicast routers and IP multicast host groups to learn IP Multicast group members.
- ❑ Actively sending IGMP Query messages to solicit IP Multicast group members.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches instead of flooding to all ports in the subnet (VLAN).

The AT-8324SX switch, with I P multicast filtering capability, not only passively monitors IGMP Query and Report messages; it can also actively send IGMP Query messages to learn locations of multicast routers/switches and member hosts in multicast groups within each VLAN.

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, an external IP multicast router is needed if IP multicast packets have to be routed across different subnetworks.

SNMP Management Software

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as monitor them to evaluate performance and detect potential problems.

Allied Telesyn provides the network management software for free with all of its manageable products. This software contains a complete management platform, including network discovery, mapping, event manager, log manager, MIB browser, RMON analysis tools, and device management modules. Allied Telesyn also provides optional plug-in device management modules for HP OpenView

Remote Monitoring

Remote Monitoring (RMON) provides a cost-effective way to monitor large networks by placing embedded or external probes on distributed network equipment (hubs, switches or routers). The provided network management software can access the probes embedded in recent Allied Telesyn network products to perform traffic analysis, troubleshoot network problems, evaluate historical trends, or implement proactive management policies. RMON has already become a valuable tool for network managers faced with a quickly changing network landscape that contains dozens or hundreds of separate segments. RMON is the only way to retain control of the network and analyze applications running at multi-megabit speeds. It provides the tools you need to implement either reactive or proactive policies that can keep your network running based on realtime access to key statistical information.

This switch provides support for RMON which contains the four key groups required for basic remote monitoring. These groups include:

Statistics: Includes all the tools needed to monitor your network for common errors and overall traffic rates. Information is provided on bandwidth utilization, peak utilization, packet types, errors and collisions, as well as the distribution of packet sizes.

History: Can be used to create a record of network utilization, packet types, errors and collisions. You need a historical record of activity to be able to track down intermittent problems. Historical data can also be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. Historical information can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

Alarms: Can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing at a certain rate over the set interval). Alarms can be set to respond to either rising or falling thresholds.

Events: Defines the action to take when an alarm is triggered. The response to an alarm can include recording the alarm in the Log Table or sending a message to a trap manager. Note that the Alarm and Event Groups are used together to record important events or immediately respond to critical network problems.

Appendix A

Troubleshooting

If you have trouble making a connection to the agent module, then please refer to the following sections.

Console Connection

If you cannot access the on-board configuration program via a serial port, be sure to have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 9600 bps. Also check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B. If you forgot or lost the password, contact Allied Telesyn Support for help.

In-Band Connection

You can access the management agent on the switch from anywhere within the attached network using Telnet, a Web browser, or other network management software. However,you must first configure the switch with a valid IP address, subnet mask, and default gateway. If you have trouble establishing a link to the management agent, check to see if you have a valid network connection. Then verify that you entered the correct IP address. Also, be sure the port through which you are connecting to the switch has not been disabled. (See Configuring Port Parameters on page 2-17.) If it has not been disabled, then check the network cabling that runs between your remote location and the switch.

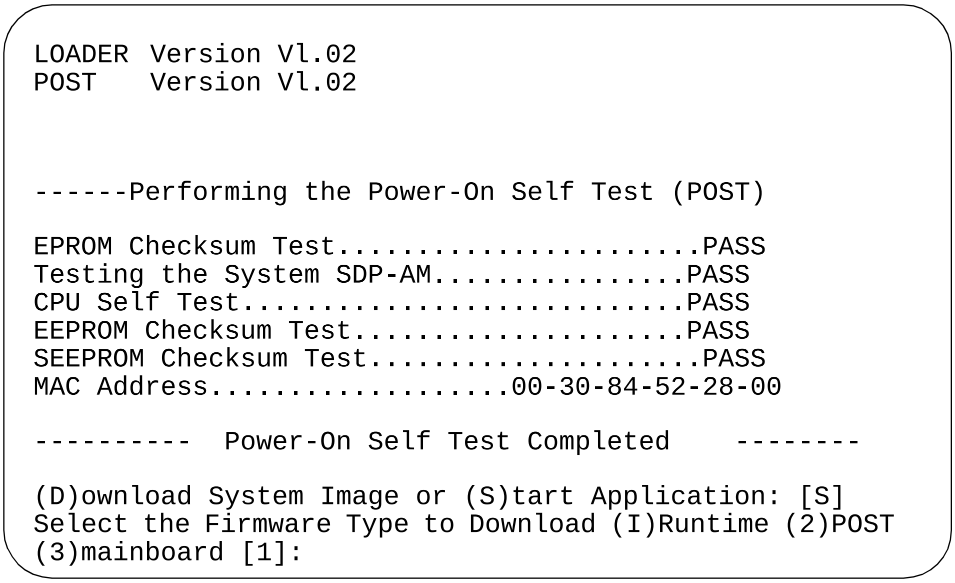
Note

Up to four concurrent Telnet connections are supported.

Upgrading Firmware via the Serial Port

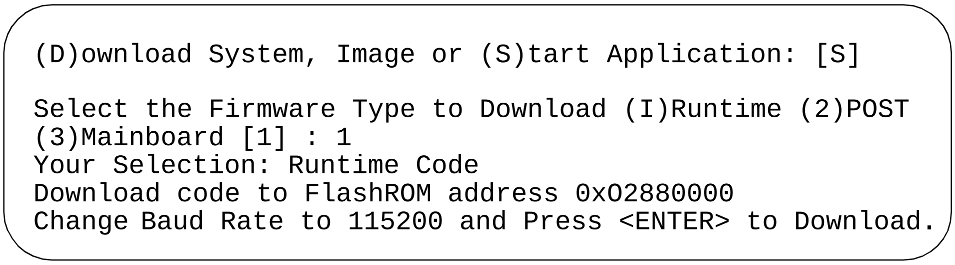
You can upgrade system firmware by connecting your computer to the serial port on the agent module, and using a console interface package that supports the XModem protocol.

1. Restart the system by using the Restart System command.
2. When the system initialization screen appears as shown below, press "D" to download system firmware, and then indicate the code type (1: Runtime, 2: POST 3: Mainboard).



```
LOADER Version Vl.02
POST   Version Vl.02



------Performing the Power-On Self Test (POST)

EPROM Checksum Test.......................PASS
Testing the System SDP-AM................PASS
CPU Self Test............................PASS
EEPROM Checksum Test.....................PASS
SEEPROM Checksum Test.....................PASS
MAC Address...................00-30-84-52-28-00

----------  Power-On Self Test Completed    --------

(D)ownload System Image or (S)tart Application: [S]
Select the Firmware Type to Download (I)Runtime (2)POST
(3)mainboard [1]:
```

For example, if you select 1 (for downloading agent firmware), the system will display the following message:



```
(D)ownload System, Image or (S)tart Application: [S]

Select the Firmware Type to Download (I)Runtime (2)POST
(3)Mainboard [1] : 1
Your Selection: Runtime Code
Download code to FlashROM address 0xO2880000
Change Baud Rate to 115200 and Press <ENTER> to Download.
```

3. Change your baud rate to 115200 bps, and press Enter to enable download mode. From the terminal emulation program, select the file you want to download, set the protocol to XModem, and then initialize downloading.

   If you use Windows HyperTerminal, disconnect and reconnect to enable the new baud rate.

The download file should be an AT-8324SX binary file from Allied Telesyn; otherwise the agent will not accept it. The file naming convention is:

Runtime program:	AT-S29.BIN
POST program:	Boot-Vx.yx, and
Mainboard program:	8051 -Vx.yz

4. After the file has been downloaded, the console screen will display information similar to that shown below. Press "s" to start the management interface, change the baud rate back to 9600, and press Enter. The Logon screen will then appear

```
XModem Download to DRAM buffer area DxOO200000:.. SUCCESS !
Verifying image in DRAM download buffer 0xOO200000... SUCCESS
Update FlashROM Image at OxO2880000... SUCCESS !
(D)ownload another Image or (S)tart Application: [SI s
Change Baud Rate to 9600 and Press <ENTER>.
```

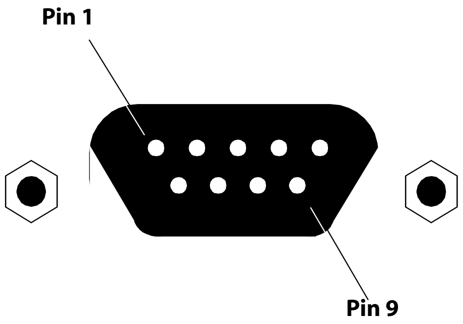
For details on managing the switch, refer to Chapter 2 for information on the out-of-band console interface, or Chapter 3 for information on the Web interface.

Appendix B

Pin Assignments

DB9 Serial Port Pin Description

The DB-9 serial port on the panel of the Network Management Module is used to connect the switch to a management device. The on-board menu-driven configuration program can be accessed from a terminal, a PC running a terminal emulation program, or from a remote location via a modem connection. The pin assignments used to connect various device types to the switch's management port are provided in the following tables.



DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	Modem DB25 DCE Pin #	Signal Direction DTE-DCE
CF	109	DCD (Data Carrier Detected)	1	1	8	◄– – –
BB	104	RxD (Received Data)	2	2	3	◄– – –
BA	103	TxD (Transmitted Data)	3	3	2	– – –►
CD	108.2	DTR (Data Terminal Ready)	4	4	20	– – –►
AB	102	SG (Signal Ground)	5	5	7	– — –
CC	107	DSR (Data Set Ready)	6	6	6	◄– – –
CA	105	RTS (Request-to-Send)	7	7	4	– – –►
CB	106	CTS (Clear-to-Send)	8	8	5	◄– – –
CE	125	RI (Ring Indicator)	9	9	22	◄– – –

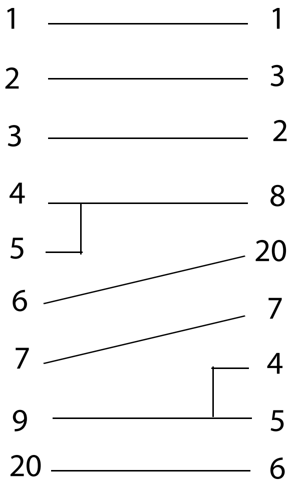
Connection from Switch's Serial Port to 9-Pin COM Port on PC

Switch's 9-Pin Serial Port	CCITT Signal	PC's 9-Pin COM Port
1 DCD	– — – DCD – — –	1
2 RXD	◄– – – TXD – — –	3
3 TXD	– — – RXD – – –►	2
4 DTR	– — – DSR – – –►	6
5 SGND	– — –SGND – — –	5
6 DSR	– — – DTR – — –	4
7 RTS	– — – CTS – – –►	8
8 CTS	◄– – – RTS – — –	7
9 RI	– — – RI – — –	9

Connection from Switch's Serial Port to 25-Pin DCE Port

Switch's 9-Pin Serial Port	CCITT Signal	Modem's 25-pin DCE Port
1	◄– – DCD – — –	8
2	◄– – RXD – — –	3
3	– — – TXD – – ►	2
4	– — – DTR – – ►	20
5	– — – SGND – — –	7
6	◄– – DSR – — –	6
7	– — – RTS – – ►	4
8	◄– – CTS – — –	5
9	◄– – RI – — –	22

Connection from Switch's Serial Port to 25-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
1 DCD	 1 —— 1	8 DCD
2 RXD	2 —— 3	3 TXD
3 TXD	3 —— 2	2 RXD
4 DTR	4 —— 8	20 DTR
5 SGND	5 —— 20	7 SGND
6 DSR	6 —— 7	6 DSR
7 RTS	7 —— 4	4 RTS
8 CTS	9 —— 5	5 CTS
9 RI	20 —— 6	22 RI