ESM-24T02Mx SNMP

Switch

User's Manual

Ver 1.2

15/04/2003

ESM-24T02M SNMP Switch User Menu

1. Introduction

The ESM-24T02M switch is a high performance web-managed SNMP Layer 2 switch that provides users with 24 10/100Mbps Ethernet ports and a single module port into which either 100BaseFX or Gigabit modules can be installed. Several optional modules are available in single or dual port configurations. The Switch has SNMP management and remote control capabilities. Gigabit modules, can be copper or fiber media types supporting 1000BASE-SX, 1000BASE-LX or 1000BASE-T, allowing users to increase their network response time at gigabit speeds and with great flexibility. An RS-232 serial port provides out of band configuration for the initial set-up.

Non-blocking, Maximum wire speed performance is achieved on all ports with support for Auto-Negotiation and Auto-MDIX functions on all switched 24 10/100M RJ-45 ports and both Gigabit Copper ports in both half or full duplex mode.

The ESM-24T02M switch provides convenient web browser management of its layer 2 features. The User-friendly drop-down menu allows the user to easily learn, control and monitor the switch. It supports not only traditional SNMP functions, but also RMON 1,2,3,9 groups for advanced network analysis.

The Switch also supports both port-based and Tag-based VLAN's, as well as Trunking on upto 4 ports at a time with 7 trunking groups. Trunked ports provide fail-over functionality, so that if one port fails a backup port can be added into the group.

The Front Panel Design provides a full LED status display to quickly diagnose port status or any potential problems. Extra LED's are used to indicate fan status and avoid fan failures and over-heating issues.

1.1 Unpacking

Open the shipping carton of the Switch and carefully unpack its contents, the carton should contain the following items:

- One ESM-24T02M, 24 port Fast Ethernet Layer 2 Switch.
- Mounting Kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing.
- One AC power cord.
- One RS-232 cable
- This Quick Installation Guide and CD.

1.2 Installation

Follow the guidelines below to install the Switch.

- Do not place any object weighted more than 3Kg (6.6 lb) on the Switch.
- Connect the power cord to the Switch and the power outlet.
- Leave at least 10 cm (4 inches) of space around the Switch for heat dissipation.

Desktop or Shelf Installation:

When installing the Switch on the desktop or shelf, please attach the rubber feet to the Switch. Peel off the protective paper on the pads and attach them on the bottom of the Switch (one at each corner).

Rack Installation:

The ESM-24T02M Switch is rack-mountable and can be installed on an EIA-19 inch equipment rack. To do this, first install the mounting brackets on the Switch's side panels (one on each side), secure them with the included screws, and then use the screws provided with the equipment rack to mount the Switch on the 19 inch rack.

Power On the Switch:

The ESM-24T02M Switch has a universal power supply ranging from 90V to 260V AC, 50 ~ 60Hz power source. The AC power cord connector is located at the rear of the unit and the On/Off switch is next to the connector. Connect the power cord from the power outlet to the Switch and push the On/Off Switch to "ON" position to power on the Switch. After the Switch is powered on, it will perform a "self-diagnostic" (POSD). This process takes about 100 seconds to complete, during this process, the "DIAG" LED will blink green and the Switch will not respond to any further configuration or any network connections. When the process is completed, the "DIAG" LED will stay on solid green.
Below is a table that describes the meaning of each LED indicator.

LED indicators information

LED		Color	Status	
			Solid	Blinking
Power		Green	Power is applied to this device	N/A
DIAG		Green	Self diagnostics was successful	Performing self diagnostics (after Power On)
Cooling Fans	**FAN1**	Red	Left cooling fan failed	N/A
	FAN2	Red	Right cooling fan failed	N/A
LINK/ACT (1 ~24 port)		Green	10Mbps Ethernet connection speed	TX/RX activity or Collision
100M (1 ~24 port)		Green	100Mbps Fast Ethernet connection speed	N/A
		Off	10Mbps connection speed	N/A
10/100/1000Mbps Copper Gigabit Port (Optional Module)				
Top LED		Orange	100Mbps Fast Ethernet connection speed (with Middle LED off)	N/A
Middle LED		Green	10Mbps Ethernet connection. (with Top LED off)	N/A
Bottom LED		Green	N/A	TX/RX activity or collision
Top+Middle LEDs		Orange + Green	1000Mbps Gigabit connection speed	N/A

1.3 Initial set up for management

There are two ways to perform the initial setup for the Switch; one is "Out-of-Band Configuration" (connect your PC's serial port to the Switch's console port with the included RS-232 serial cable and run terminal communication program) and the other is "In-Band Configuration" (network a PC to the Switch and run web browser or telnet). The sections below describe how to perform both operations.

1.3.1 Out-of-Band Terminal Mode Configuration

If you are using Microsoft Windows, boot up the computer, go to "Start", "Programs", "Accessories", "Communications", and open the "HyperTerminal". After that follow the instructions below to setup a new terminal connection for the Switch. If you are using other communication software, please select the correct COM port and setup the connection properties according to step 3 below.

1. Type in a name for the connection (e.g. SNMP Switch), select an icon for the connection, and click "OK".
2. Select the COM port that you are using for this connection and click "OK".
3. Setup the COM port properties by using the information below and click "OK".

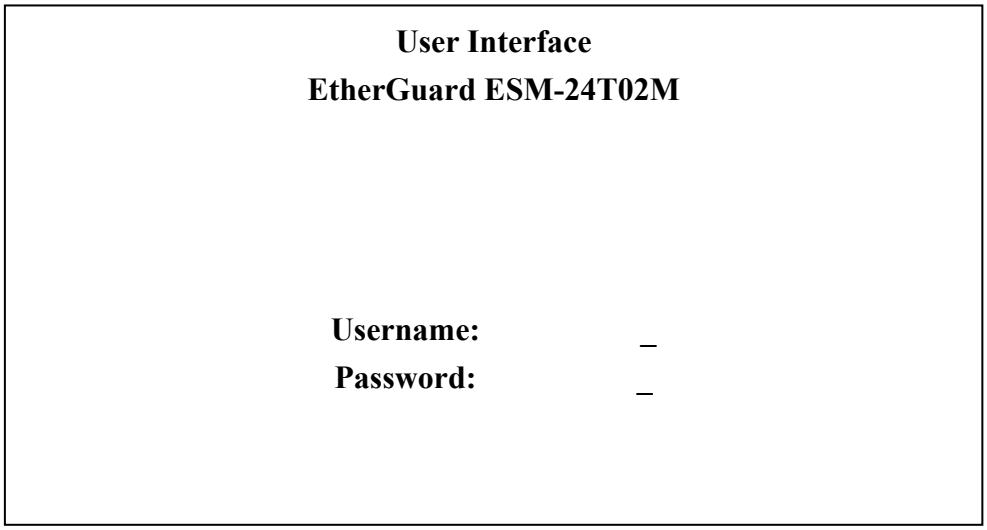
   Bits Rate per Second = 57600
   Data Bits = 8
   Parity = None
   Stop Bit = 1
   Flow Control = None

4. Connect the included serial cable from the computer's COM port to the Switch's console port.
5. Power on the Switch, you should see some boot-up messages displayed within your "HyperTerminal" session. The Switch's Power On Self Diagnostic (POSD) takes about 100 seconds to complete. After that, you will see the login screen.
   If the Switch is already powered on and finished its self-diagnostic, after running the terminal communication program, please hit "Enter" once to get the login prompt.
6. At the "username" field type in **admin** and hit "Enter".

7. At the "password" field type in **admin** and hit "Enter". You are now logged

into the Switch's configuration program.

8. On the lower portion of the screen, you will see descriptions of the navigation keys (e.g. Tab, Space Bar, and Enter). Please use these keys to move around the configuration program.



1.3.2 In-band management through Ethernet

In addition to terminal mode configuration, the ESM-24T02M Switch also supports In-Band Configuration using a Web Browser. Compared with terminal mode configuration, web browser configuration is more convenient and easier. You can simply connect a network-ready PC to the Switch, open the web browser, go to the Switch's configuration page (Switch's IP address), and configure the Switch by clicking on the subject on the menu.

Before you can access the switch through in-band, you must make sure the computer connecting to the Switch has a web browser and the TCP/IP protocol (with valid IP address) is bound to the network adapter. After that, you can either change your computer's IP address to the same class as the Switch's IP address, or you can login to the Switch with the "out-of-band" method described in the previous section and configure the Switch's IP address to the same class as your computer's IP address.
Below, is the Switch's default IP information:

IP Address: 192.168.0.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.1

Modify Switch's IP address via Out-of-Band method

1. Login the console (note: default User Name: admin, Password: admin).
2. Use "Tab" key to select (highlight) "Switch Static Configuration" and hit "Enter".
3. Use "Tab" key to select "Administration Configuration" and hit "Enter".
4. Use "Tab" key to select "IP Configuration" and hit "Enter".
5. Use "Tab" key to select "Edit" and hit "Enter".

6. Use "Tab" key to highlight "IP Address", enter the desired IP address (e.g. 192.168.1.100), and hit "Enter".
7. The "Subnet Mask" is now highlighted, enter the correct subnet mask, and hit "Enter.
8. Input the Gateway address and hit "Enter".
9. Press and hold "Ctrl" and then hit "A" to go to the "Action Menu".
10. Use "Tab" key to select "Save" and hit "Enter".
11. The screen will prompt you to "restart the system…", turn off the Switch, wait for 10 seconds, and then turn the Switch's power back on.

After the Switch finishes the self-diagnostic, open your computer's web browser and at the "Address:" field, enter the Switch's IP address (e.g. **http://192.168.0.100)**, hit "Enter" or click on "Go", and the Switch's configuration page will prompt you to enter "User Name" and "Password" to login.
(Note: default User Name: **admin**, Password: **admin**).

Modify Network Adapter's IP address

You can change the network adapter's IP address in the Network Adapter's "Properties". We suggest that you change the network adapter's IP to the following settings:
IP Address: 192.168.0.101
Subnet Mask: 255.255.255.0
(Note: you don't need to enter Gateway address at the moment.)

Reboot the computer if necessary. After the computer boots back up, open the web browser and at the "Address" field, enter **http://192.168.0.100** , hit "Enter" or click on "Go", and the Switch's configuration page will prompt you to enter "User Name" and

Password” to login.

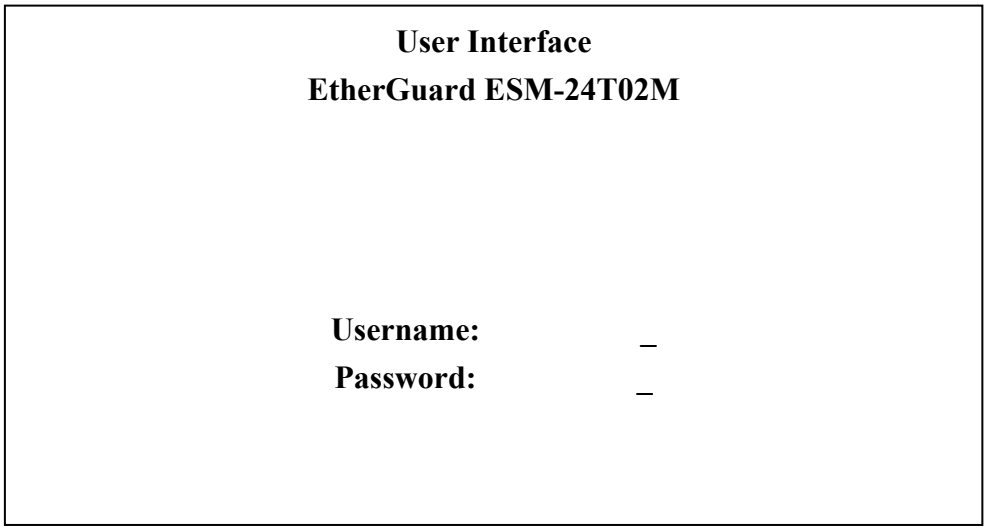
(Note: default User Name: **admin**, Password: **admin**).

1.3.3 Telnet management

In addition to local terminal mode operation, the ESM-24T02M switch supports remote management through Telnet, over the Ethernet LAN network or even over internet. In this mode, the user needs to perform the same initial IP setup on the switch as previously discussed. (refer: 'Modify Switch's IP address via Out-of-Band method')

Telnet IP Address of Switch

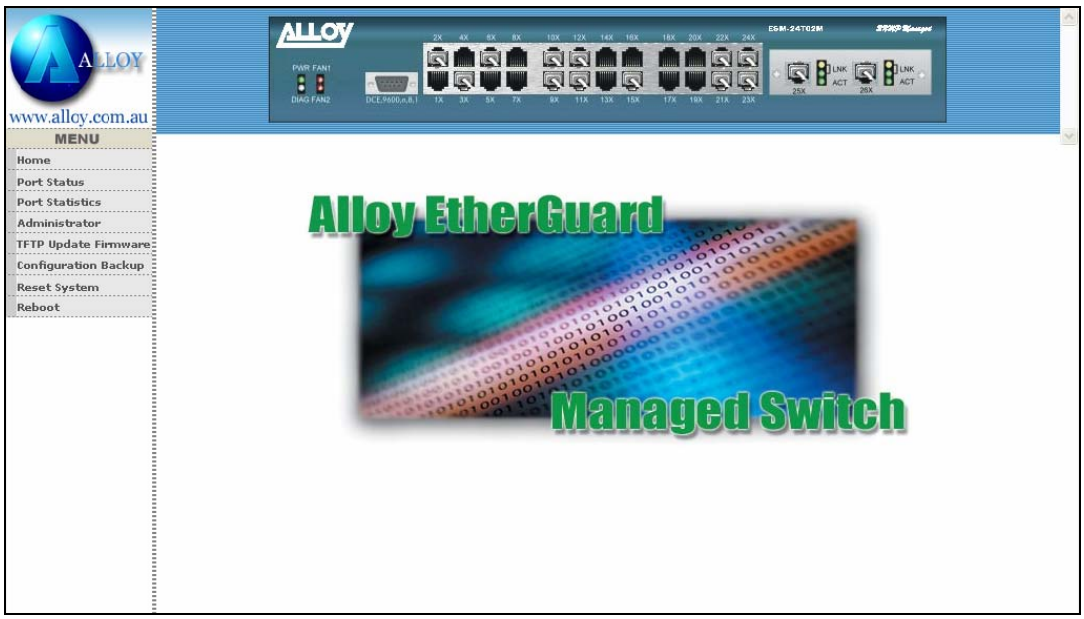
The following dialogue appears within the Telnet Window. Once again enter the username and password to continue. To find out more about configuring the Switch in this mode, please refer the instructions in chapter 3 of this manual.



2. Web Management Function

2-1. Web Management Home Overview

This is the Home Page.

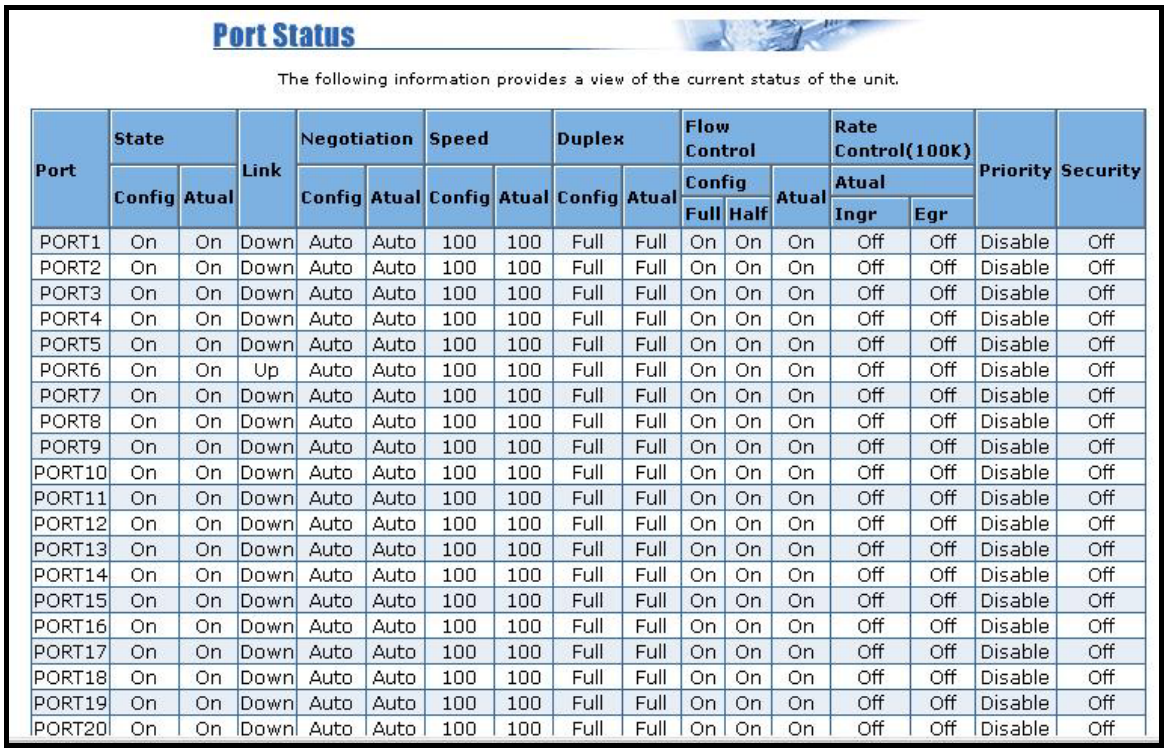


This is the initial startup page. The top section of this page will display active links on any of the ports by overlaying an inserted RJ-45 connector. Clicking on individual icons will popup port statistics information.

2-2. Port Status
2-3. Port Statistics
2-4. Administrator
2-5. TFTP Update Firmware
2-6. Configuration Backup
2-7. Reset System
2-8. Reboot

2-2. Port status

This page displays the current status of every port. It will display the users selection for each port followed by the actual discovered settings.



Port Status

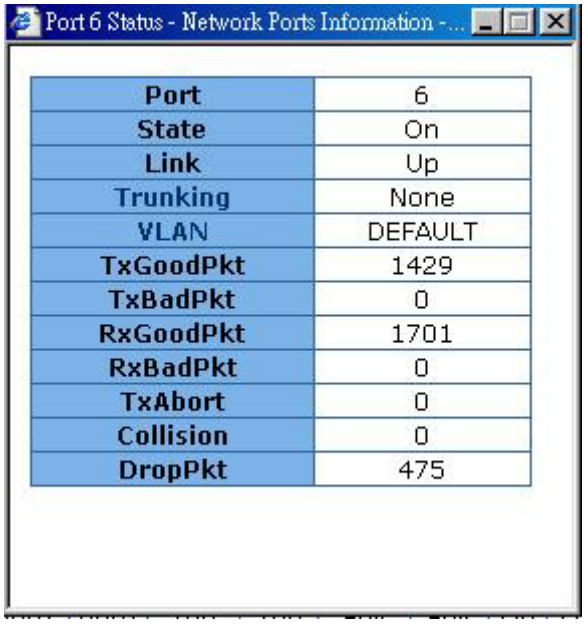
The following information provides a view of the current status of the unit.

Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control(100K)		Priority	Security
	Config	Atual		Config	Atual	Config	Atual	Config	Atual	Config		Atual	Atual			
										Full	Half		Ingr	Egr		
PORT1	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT2	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT3	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT4	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT5	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT6	On	On	Up	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT7	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT8	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT9	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT10	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT11	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT12	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT13	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT14	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT15	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT16	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT17	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT18	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT19	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off
PORT20	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off

1. **State:** Display port status: **On or Off** , Off indicates port is disabled.
2. **Link Status:** Down indicates “No Link”, Up indicates “Link”.
3. **Auto Negotiation:** Display the auto negotiation mode: Auto/Force/Nway-forced.
4. **Speed Status:** Displays 1000Mbps, 100Mbps or 10Mbps speeds.
   Note: port 1- 24 are 10/100Mbps, Port 25-26 are 10/100/1000Mbps.
5. **Duplex Status:** Displays full-duplex or half-duplex mode.
6. **Flow Control:** Full: Displays flow control status in Full Duplex mode.
   Half: Displays flow control status in Half Duplex mode.
7. **Rate Control:** Displays the current rate control setting of the selected port.
   Ingr: Display the effective port ingress rate as defined by the user.
   Egr: Display the effective port egress rate as defined by the user.
8. **Port Security:** Displays the status of port security.
9. **Config: (configured)** Displays the state defined by the user.
10. **Atual: (actual)** Displays the negotiation result.

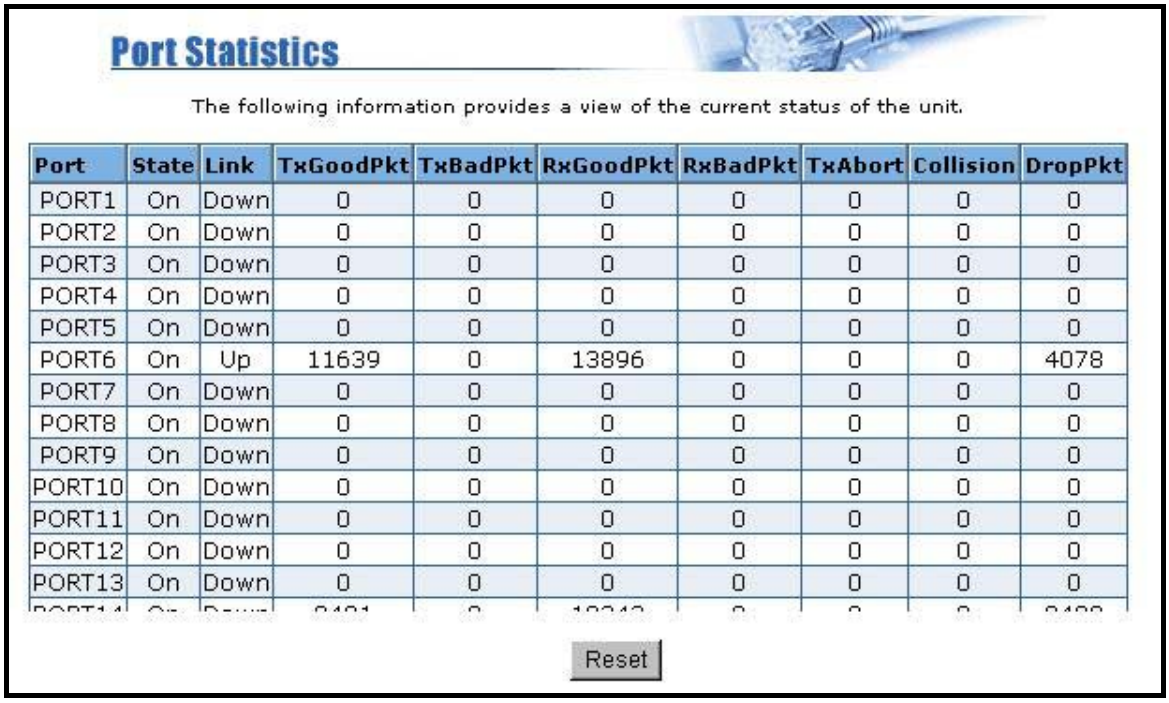
2.2.1 Port Statistics and Status Popup Window

Clicking on individual ports within the top most section of the page will present a popup page showing port statistics information as shown below.



2-3. Port Statistics

The Port Statistics page provides a view of the current status of every port on the switch. Pressing the “Reset” button will reset all port counters to zero.



2-4. Administrator

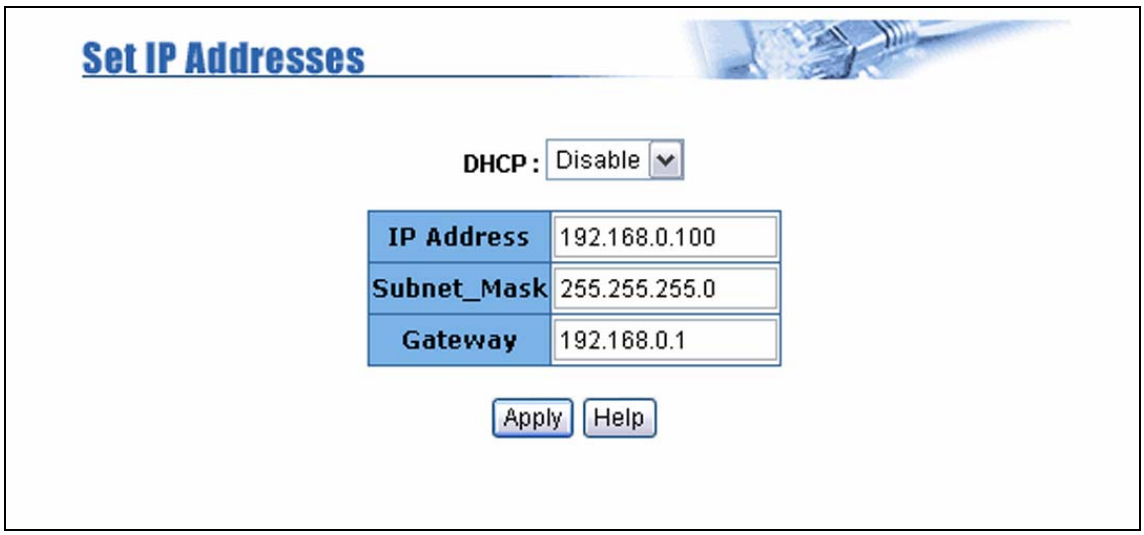
The following list of functions can be performed from the administrator section of the web management:

- IP address/Subnet Mask/Gateway
- Switch Settings
- Console Port Information
- Port Controls
- Trunking
- Filter Database
- VLAN Configuration
- Spanning Tree
- Port Sniffer
- SNMP/Trap Manager
- Security Manager
- 802.1x Configuration

2-4-1. IP Address/Subnet Mask/Gateway

From within this page, users can modify the switch IP address settings.

[note] Any changes to values within this page will require a switch 'reboot' to activate.

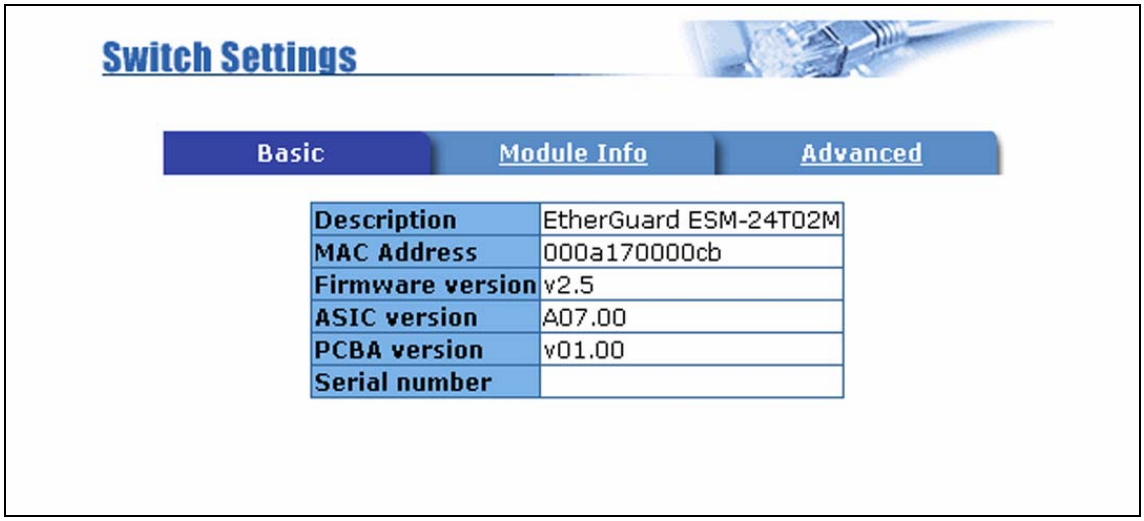


2-4-2 Switch Settings

2-4-2-1 Basic

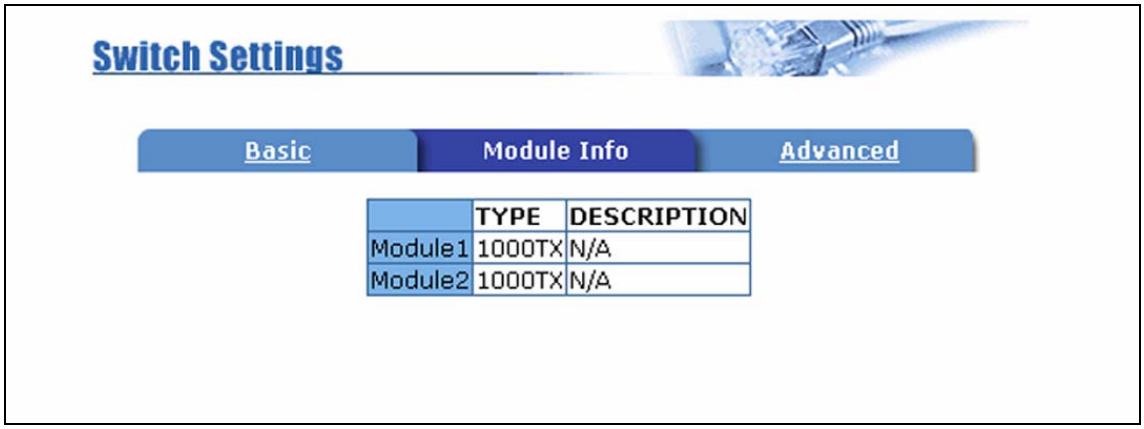
All information in the **Basic** menu is read only.

Description: Display the family name of the switch.
MAC Address: The unique hardware address of the switch.
Firmware Version: Displays the switch's firmware version.
Hardware Version: Displays the switch's ASIC Hardware version. (Switch controller)
Displays the switch's PCBA Hardware version. (Circuit board)



2-4-2-2 Module Info

All information in the **Module Info** menu is read only.



2-4-2-3 Advanced

◆ **Miscellaneous Setting:**

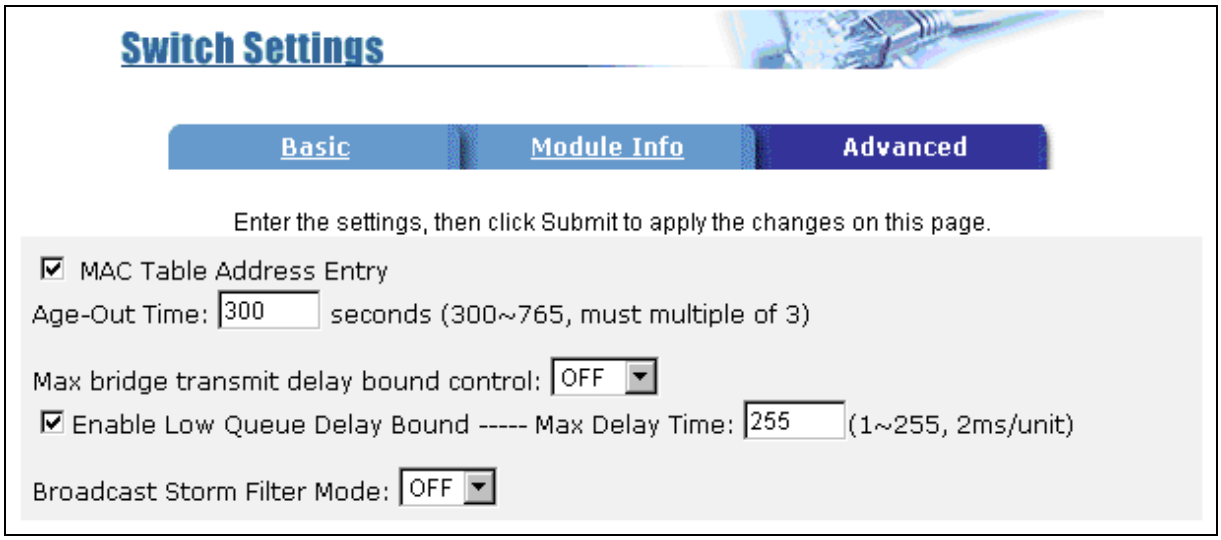
MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is 300 seconds.

Max bridge transmit delay bound control: This Limits the packets queuing time. If enabled, packets that are queued longer than this setting will be dropped. Valid values for this are 1sec, 2 sec, 4 sec and off. Default is 1 seconds.

NOTE: Make sure the "Max bridge transit delay bound" control is enabled before enabling the "Low Queue Delay Bound" option.

Low Queue Delay Bound: This controls how low priority packets are queued in the switch. The **Max Delay Time** setting defines when a low priority packet is given more priority to send.

Broadcast Storm Filter: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are 5%, 10%, 15%, 20%, 25% and off.



◆ **Priority Queue Service settings (802.1p):**

First Come First Service: The sequence of packets sent is dependant on the order in which they arrived.

All High before Low: High priority packets are sent before Low priority packets.

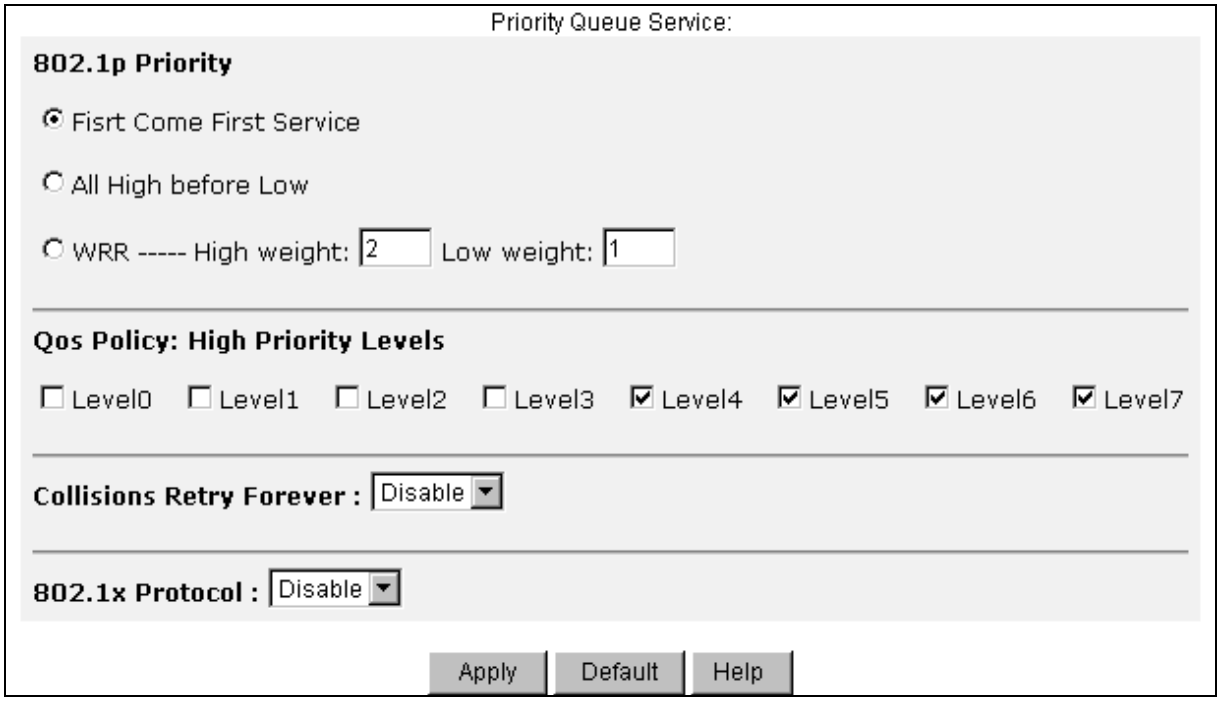
WRR: Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example, 5 High - 2 Low means that the switch sends 5 high-priority packets before sending 2 low priority packets.

Qos Policy: High Priority Levels: This is used to map the 0~7 priority levels to either High or Low queues.

Collisions Retry Forever: (this setting only affects Half Duplex connections)

Disable – Any collisions are retried for a maximum of 48 times, after which the packet will be dropped.
Enable – Collision will be retried indefinitely.

802.1x Protocol: Enables or disables the 802.1x port security protocol.



2-4-3 Console Port Information

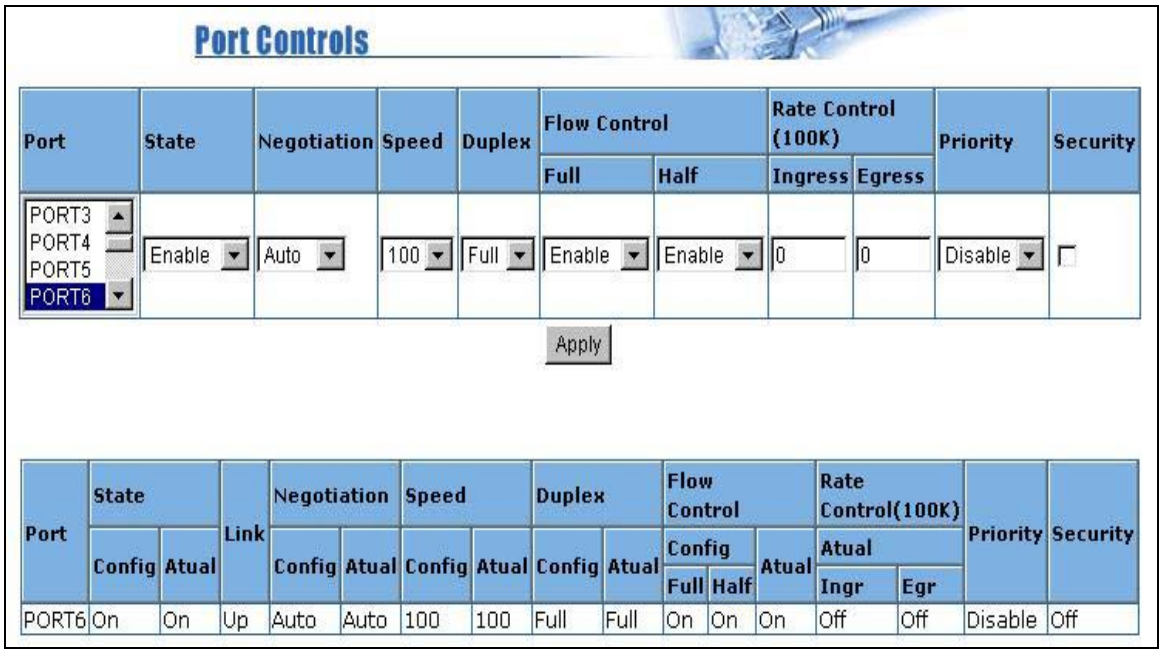
The Console port on the EMS-24T02M is a standard RS-232 UART interface. This is used to connect to the serial interface on your PC, or terminal.

You can use Windows HyperTerminal program to link the switch to your PC.
The following settings need to be configured into your Terminal Application:

Bits per seconds: 57000
Data bits: 8
Parity: none
Stop Bits: 1
Flow control: none

2-4-4 Port Controls

The Port Controls page allows the user to modify the operational mode of each port.



1. **State:** Used to enable or disable this port.
2. **Auto Negotiation:** Used to set the auto-negotiation mode.
   Settings are: Auto, Nway and Forced.
   # Auto instructs the switch to learn the parameters of the device connected.
   # Nway instructs the switch to use the Nway protocol to instruct devices connected to the port of its defined parameters. (Speed and Duplex should be defined)
   # Forced does not negotiate with the connected device its parameters.
3. **Speed:** Used to set the port speed to either 100Mbps or 10Mbps on Port1~Port24. 1000Mbps, 100Mbps or 10Mbps speed on Port25 and Port26 (depending on module card used).
4. **Duplex:** Used to set full-duplex or half-duplex mode of the port.

5. **Flow control:**
   Full: Used to enable or disable flow control when in full duplex mode.
   Half: Used to enable or disable backpressure flow control when in half duplex mode.
6. **Rate Control:** Ports1 ~ port 24, support ingress and egress rate control (inwards and outwards). For example, assume that port 1 is connected at 10Mbps. The switch administrator could set the effective port throughput levels by using the Rate Control function on that port to 1Mbps egress (outwards) and 500Kbps ingress (inwards). An example of where to use this could possibly be to limit the internet bandwidth to a FTP

server.

The switch will perform full duplex flow control or half duplex backpressure flow control to confine the port speeds to match specified ingress/egress rates.

Ingress: Specify the ports effective ingress rate. Valid range is 0 ~ 1000.
The unit is 100K.
0: disable rate control.

Egress: Specify the ports effective egress rate. Valid range is 0~1000.
The unit is 100K.
0: disable rate control.

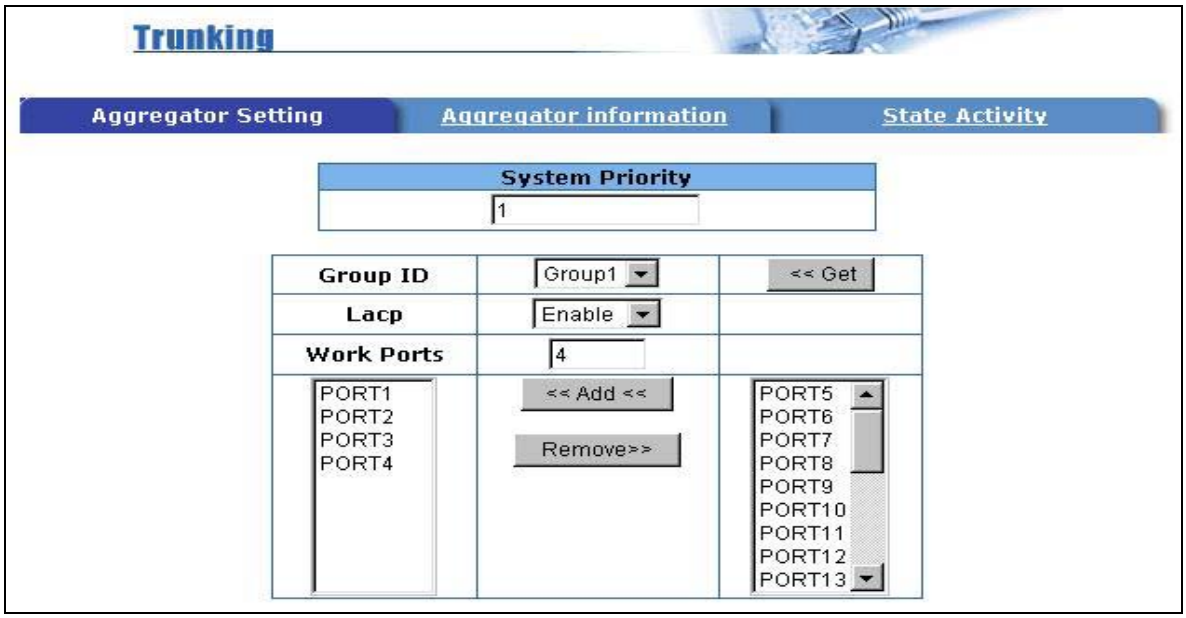
7. **Port Priority:** This is used to force any non prioritized packets to either High, Low, or Disabled states.
8. **Port Security:** Setting a ports security mode to on (by ticking the check box) will lock it to all unauthorized MAC addresses. This disables the address learning functionality on the port and then only incoming packets with a known source MAC addresses will be forwarded by the port. Administrators can disable the port from learning any new MAC addresses, then use the static MAC addresses table entry screen to define a list of MAC addresses that can be used by the secure port.

2-4-5 Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high speed redundant links.
Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refer to the IEEE 802.3ad standard.

2-4-5-1 Aggregator setting

Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network, such as another switch or a server, and also provide redundancy features.



1. **System Priority:** A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are seven trunk groups provided. Choose the "group id" and click "Get" to display the group settings.
3. **LACP:** If enabled, the group defined in the 'Work Ports' is a LACP static trunking group. If disabled, the group is a LOCAL static trunking group (not LACP aware). By default all ports support LACP dynamic trunking. If the switch is connecting to a device that also supports LACP, then the LACP dynamic trunking group will be created automatically.
4. **Work ports:** Allows a maximum of four ports to be aggregated at the same time. If the group is defined as a LACP static trunking group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static trunking group, then the number of ports must be the same as the group member ports.

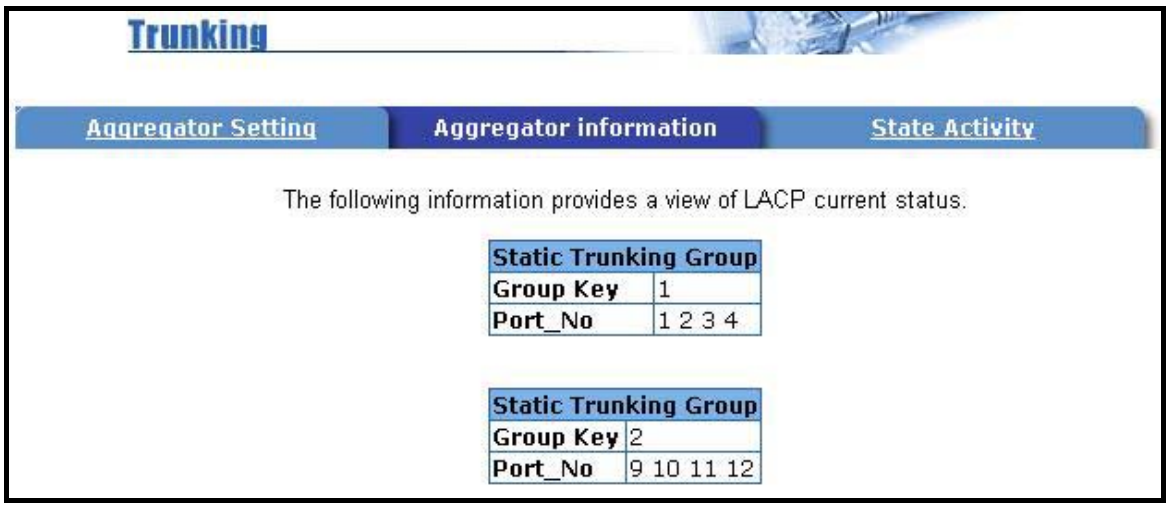
   Note: If LACP is enabled, you can configure LACP Active/Passive status in each port on State Activity page.

2-4-5-2 Aggregator Information

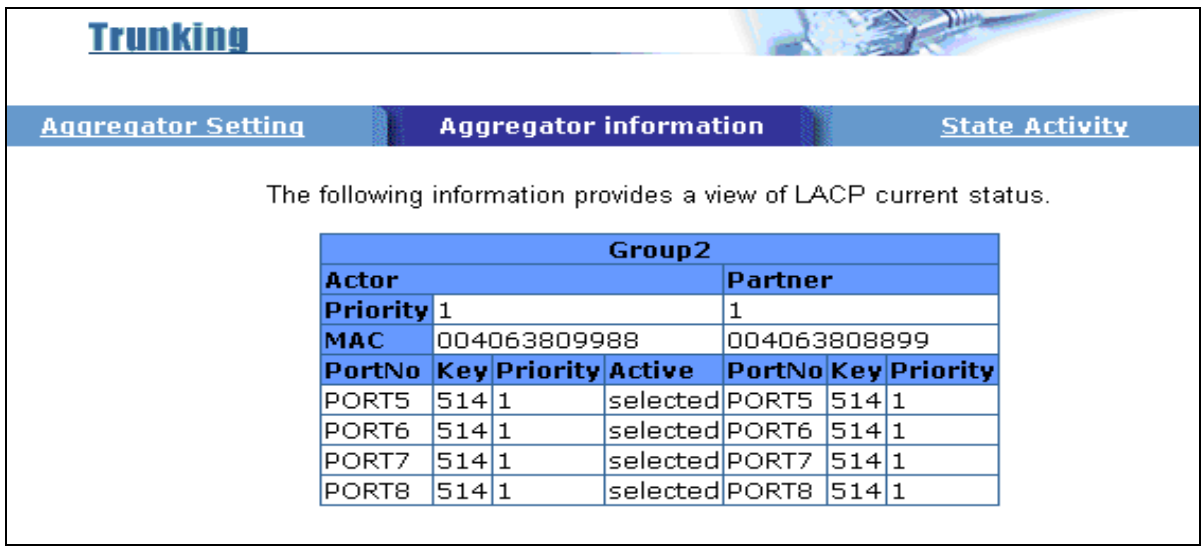
This page displays a summary report on the current LACP aggregator status.

1. In this example there is no group active. LACP is not operational.

2. In this example there are 2 Static Trunking groups.



3. In this example there is an active LACP trunking group.



2-4-5-3 State Activity

Active (selected)**:** The port automatically sends LACP protocol packets.
N/A (not selected)**:** The port does not automatically send LACP protocol packets, and

responds only if it receives an LACP protocol packet from a remote device.

Note: Work Ports defined as LACP enabled in the 'Aggregator Settings' page will automatically have their LACP Activity State enabled.

Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	☑ Active
3	☑ Active	4	☑ Active
5	N/A	6	N/A
7	N/A	8	N/A
9	☑ Active	10	☑ Active
11	☑ Active	12	☑ Active
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

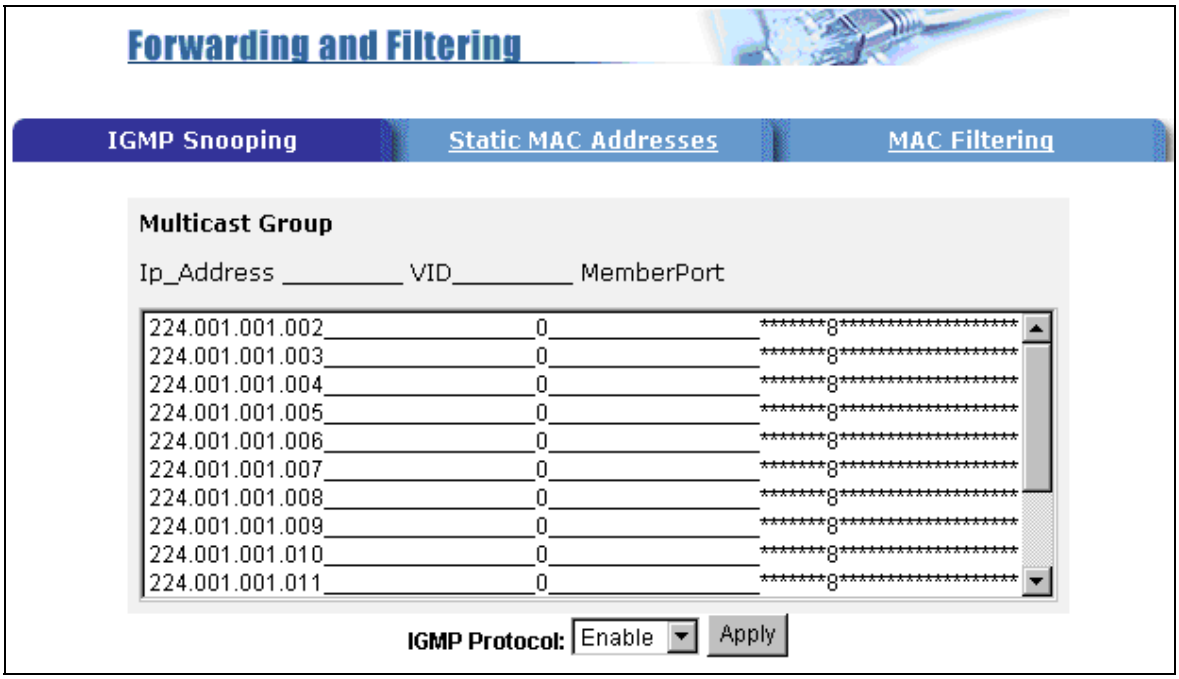
Apply Help

2-4-6. Filter Database

2-4-6-1. IGMP Snooping

The ESM-24T02M switch supports IP multicasting via the IGMP protocol. Administrators can enable IGMP within the web management's "Forwarding and Filtering" page, then display the IGMP snooping information. Multicast groups, VID and member port information.

IP multicast addresses range from 224.0.0.0 through to 239.255.255.255.

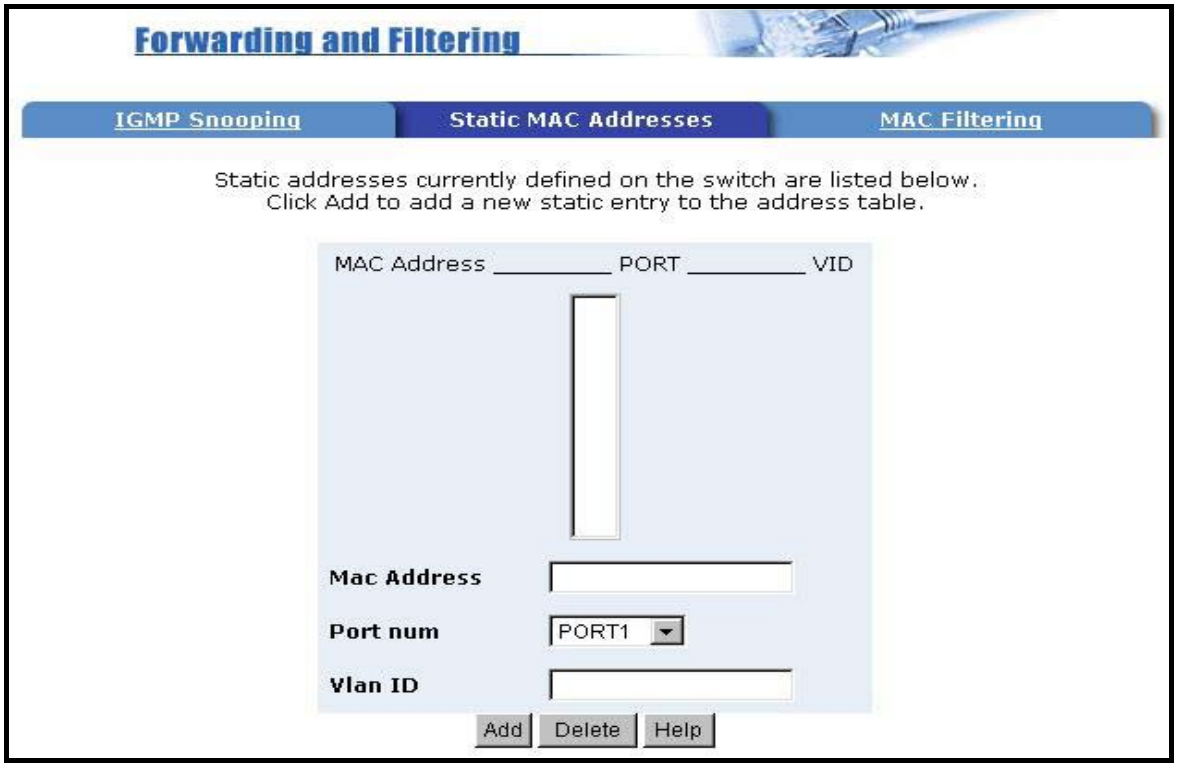


The Internet Group Management Protocol (IGMP) is a protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the switch to detect IGMP queries and IGMP Report packets to manage IP multicast traffic through the switch. IGMP has three fundamental types of message as follows:

Message	Description
Query	A message sent from the queries (IGMP router or switch) asking for a response from each host belonging to a multicast group.
Report	A message sent by a host to the queries to indicate that the host wants to be, or is a member of, a given group indicated in the report message.
Leave Group	A message sent by a host to the queries to indicate that the host has quit being a member of a specific multicast group.

2-4-6-2. Static MAC Address

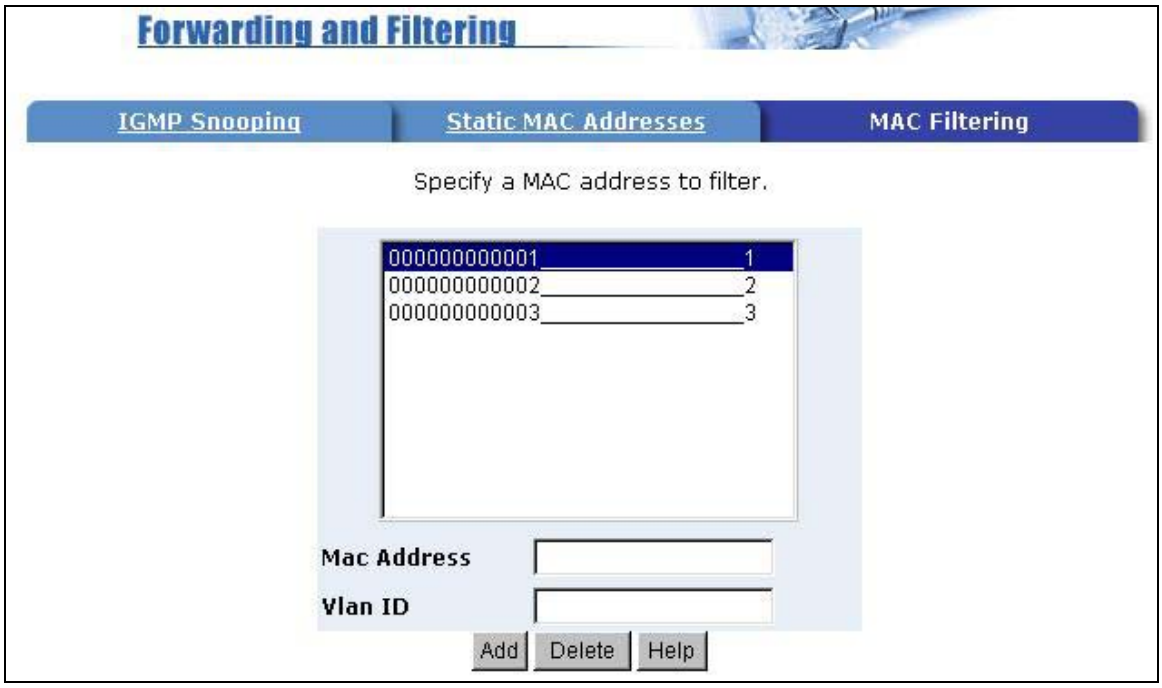
When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address after it has been disconnected or powered-off from the network, and then reconnected at some time later.



1. At the main menu, click administrator →Filter Database →Static MAC Addresses.
2. In the MAC address box, enter the MAC address to and from which the port should permanently forward traffic, regardless of the device's network state.
3. In the Port Number box, enter a port number.
4. If tag-based (IEEE 802.1Q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) to associate with the MAC address.
5. Click Add.

2-4-6-3 MAC filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses.

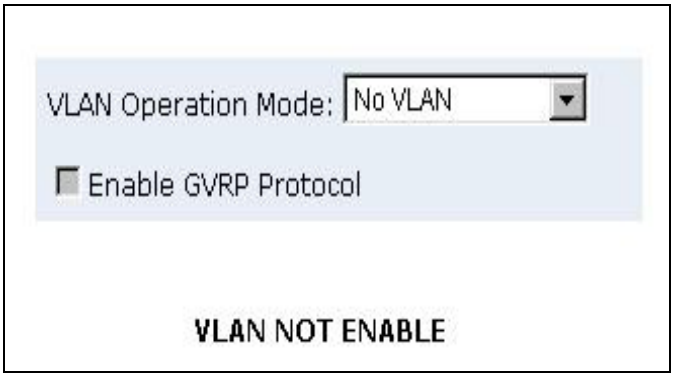


1. In the MAC Address box, enter the MAC address that you want to filter out.
2. If tag-based (802.1Q) VLAN's are set up on the switch, in the VLAN ID box, type the VID to associate with the MAC address.
3. Click Add.
4. To Delete a MAC address entry from the filtering table, simply select it and click Delete.

2-4-7. VLAN configuration

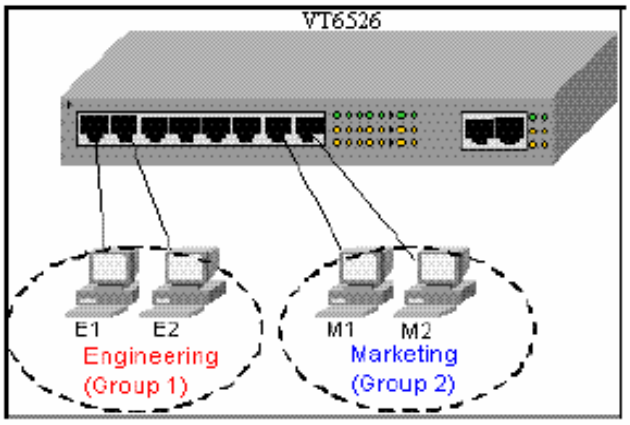
A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain within the switch. It allows you to isolate network traffic so that members of a certain VLAN only receive traffic from other members of the same VLAN.

The ESM-24T02M switch supports port-based, 802.1Q (tagged-based) and protocol-based VLANs. In the default configuration, VLAN support is disabled.



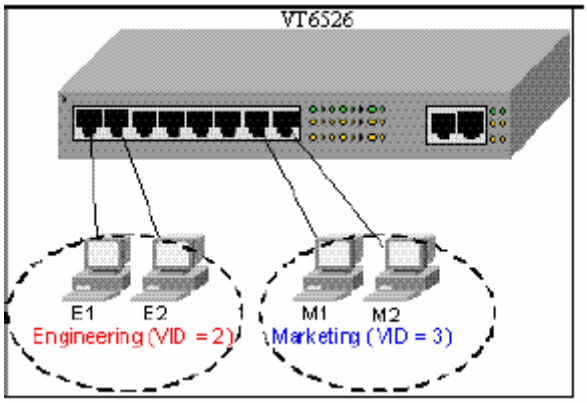
◆ **Support Port-based VLAN**

Packets can only be broadcast among other members of the same VLAN group. Note all unselected ports are treated as belonging to the default system VLAN. If port-based VLAN's are enabled, then VLAN-tagging is ignored.



◆ **Support Tag-based VLAN (IEEE 802.1Q VLAN)**

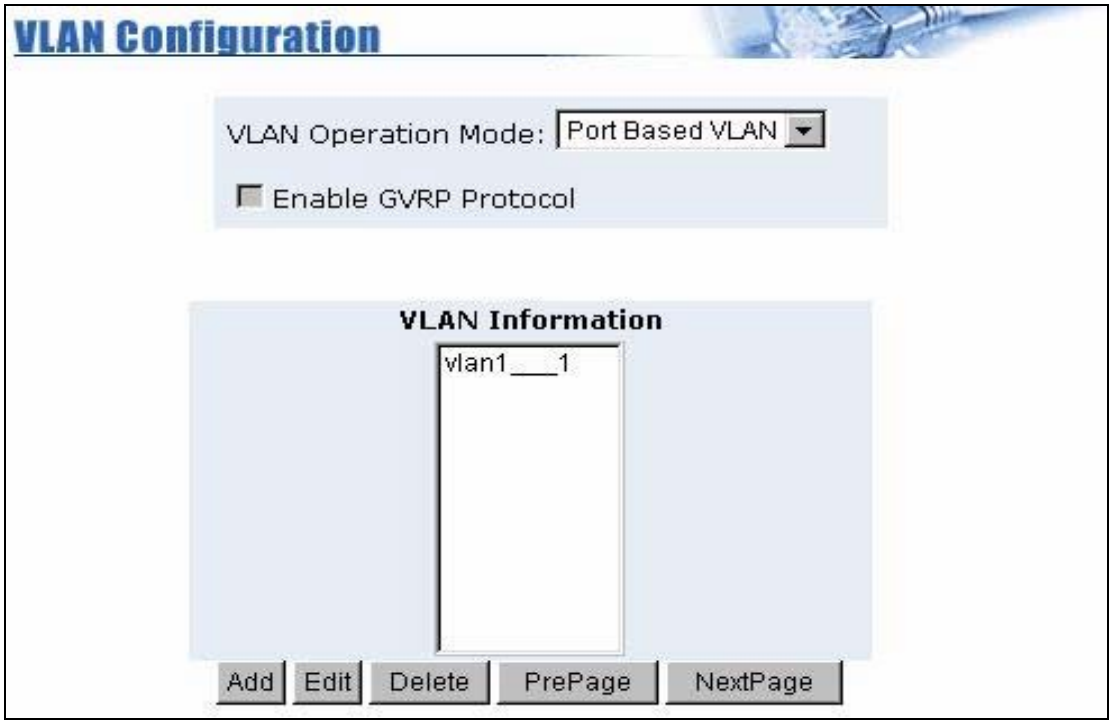
Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN's use a technique to insert a "tag" into the Ethernet frames. The "tag" contains a VLAN Identifier (VID) that indicates the VLAN number that the packet belongs to.



◆ **Support Protocol-based VLAN**

In order for a workstation to send packets to different VLANs, it has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with a different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.
ESM-24T02M switch supports protocol-based VLAN classification by means of both built-in knowledge of layer 2 packet formats used by selected popular protocols, such as Novell IPX and AppleTalk's EtherTalk, and a programmable protocol matching capability.

2-4-7-1. Port Based VLAN

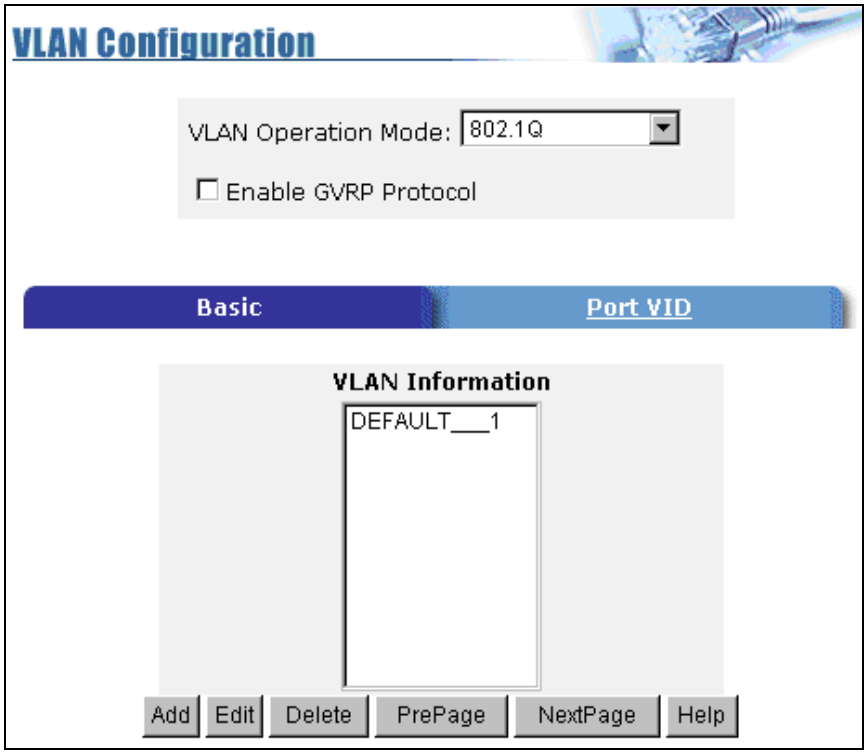


1. Click Add to create a new VLAN group.
2. Enter the VLAN name, group ID and select the members for the new VLAN.
3. Click Apply.
4. If there are more groups than the display will allow, then you can click the "Next Page" to view additional VLAN groups.

NOTE: If a trunk groups exist, it will be visible as TRK1, TRK2, etc…. The Trunk groups can also be members of selected VLANs.

2-4-7-2. 802.1Q VLAN

By selecting 802.1Q VLAN mode, Administrators can create Tag-based VLANs and enable or disable use of the GVRP protocol.
There are upto 256 configurable VLAN groups. By default when 802.1Q is enabled, all ports on the switch belong to default VLAN (VID 1). The default VLAN cannot be deleted.

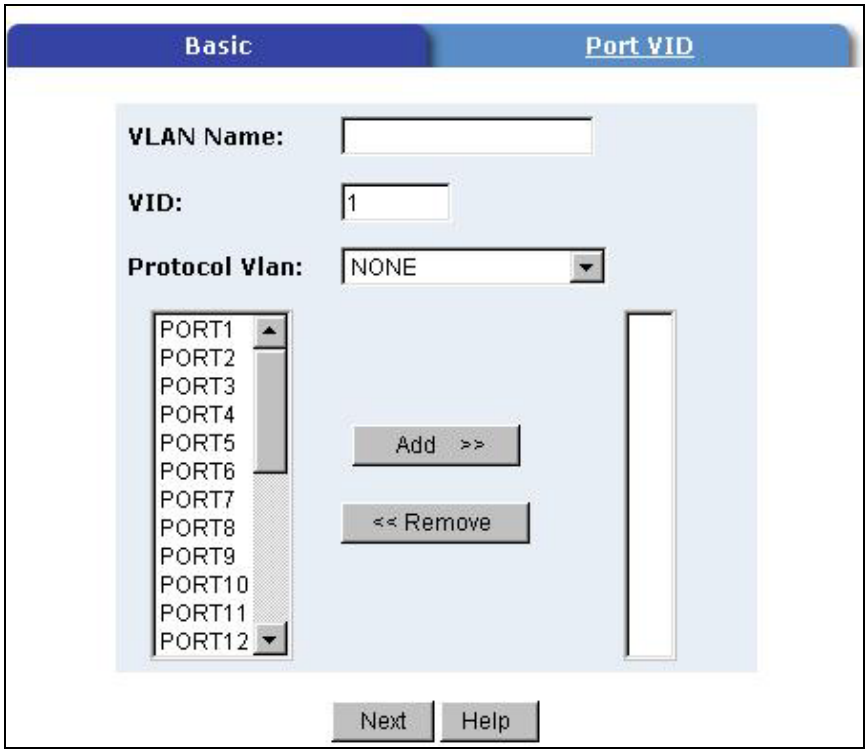


GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol)
GVRP allows automatic VLAN configuration between the switch and its nodes. If the switch is connected to a device with GVRP support, then a GVRP request can be issued from the device to the switch using a valid VID of a VLAN defined on the switch. The switch will then automatically add the device to the existing VLAN entries.

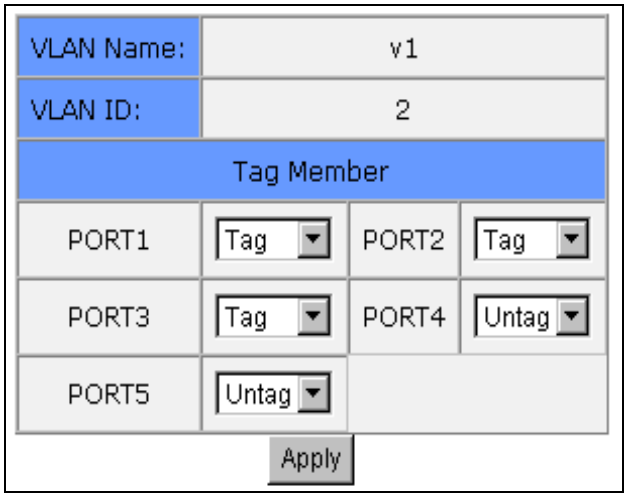
Basic

Create a VLAN and add a tagged member port to it.

1. From the main menu, click Administrator →VLAN configuration, click Add then you will see the page as follow.



2. Type a name for the new VLAN.
3. Type a VID (between 2-4094). The default is 1.
4. Choose the protocol type.
5. From the Available ports box, select ports to add to the VLAN and click “Add >>”. If a trunk groups exist, you can see it here (ex: TRK1, TRK2…)
6. Click Next to view the following page:



7. Use this page to control how the outgoing frames are VLAN-Tagged. Then click Apply.

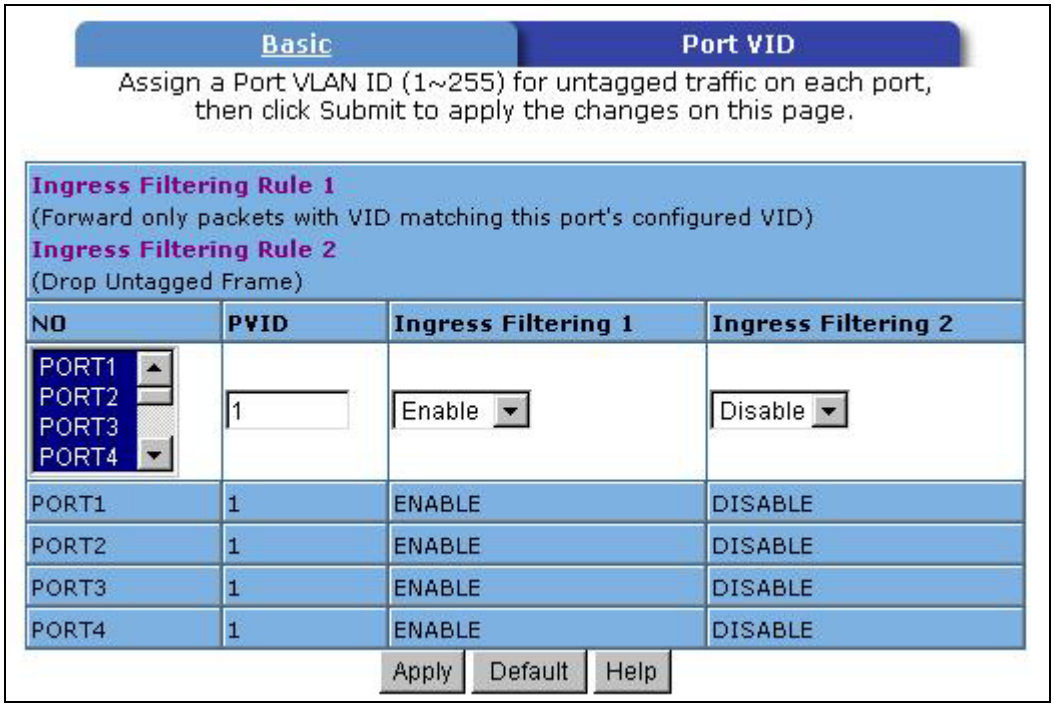
   Tag: outgoing frames will be VLAN-Tagged.

   Untag: outgoing frames will not be VLAN-Tagged.

Port VID

Configure port VID settings

From the main Tag-based (IEEE 802.1Q) VLAN page, click "Port VID" Menu.



Port VID (PVID)

Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. ESM-24T02M switch allows each port to set one PVID, the range is 1~255, default PVID is 1. The PVID must be the same as the VLAN ID that the port was defined as belonging to in the VLAN group, or the untagged traffic will be dropped.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. The switch has two ingress filtering rules as follows:

Ingress Filtering Rule 1: A forward only packets with VID matching this port's configured VID.

Ingress Filtering Rule 2: Drop Untagged Frame.

2-4-8. Rapid Spanning Tree

The Rapid Spanning-Tree Protocol (RSTP) is a standardized method (IEEE 802.1w) for avoiding loops in switched networks. You would enable RSTP to ensure that only one path at a time is active between any two nodes on the network.
You can enable Rapid Spanning-Tree Protocol on the web management's switch setting advanced menu, select enable Rapid Spanning-Tree protocol.

1. You can view Root Bridge spanning tree information from the follow table.

Root Bridge Information

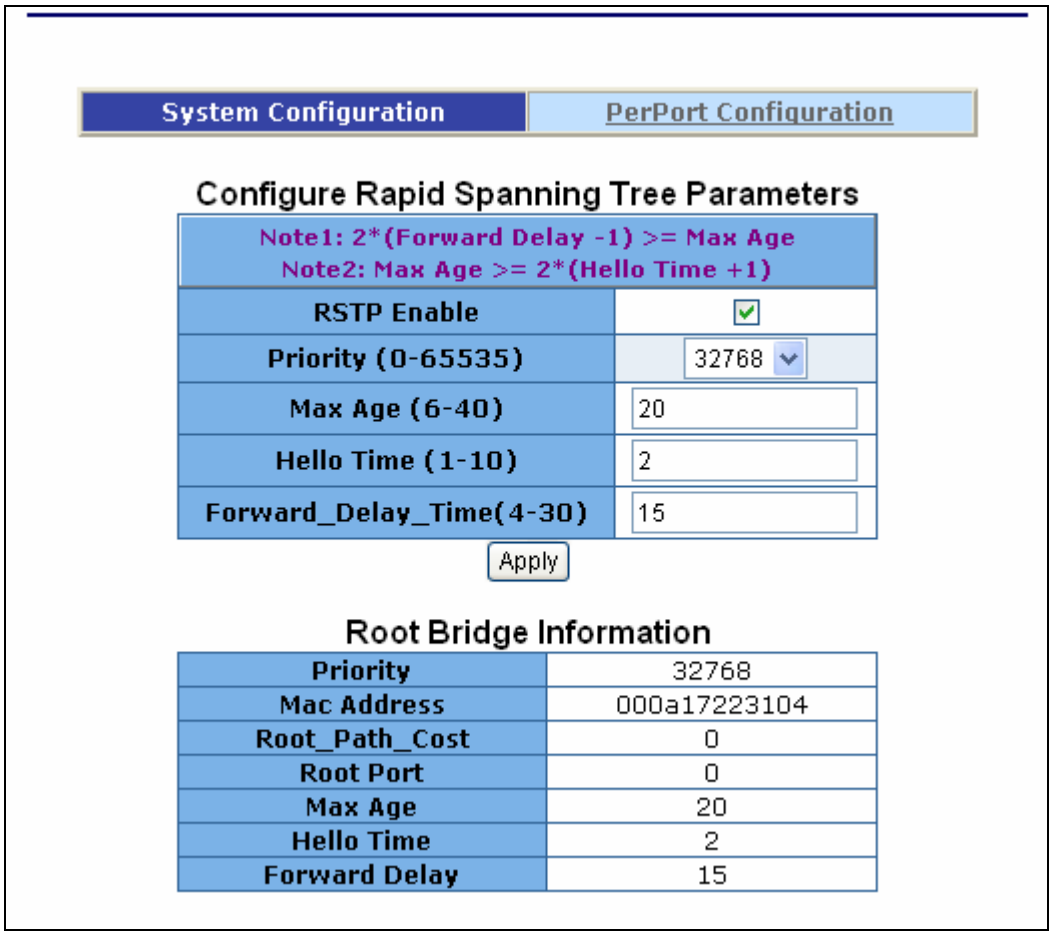
Priority	32768
Mac Address	000a17223104
Root_Path_Cost	0
Root Port	0
Max Age	20
Hello Time	2
Forward Delay	15

2. You can view spanning tree status from the following table.

STP Port Status

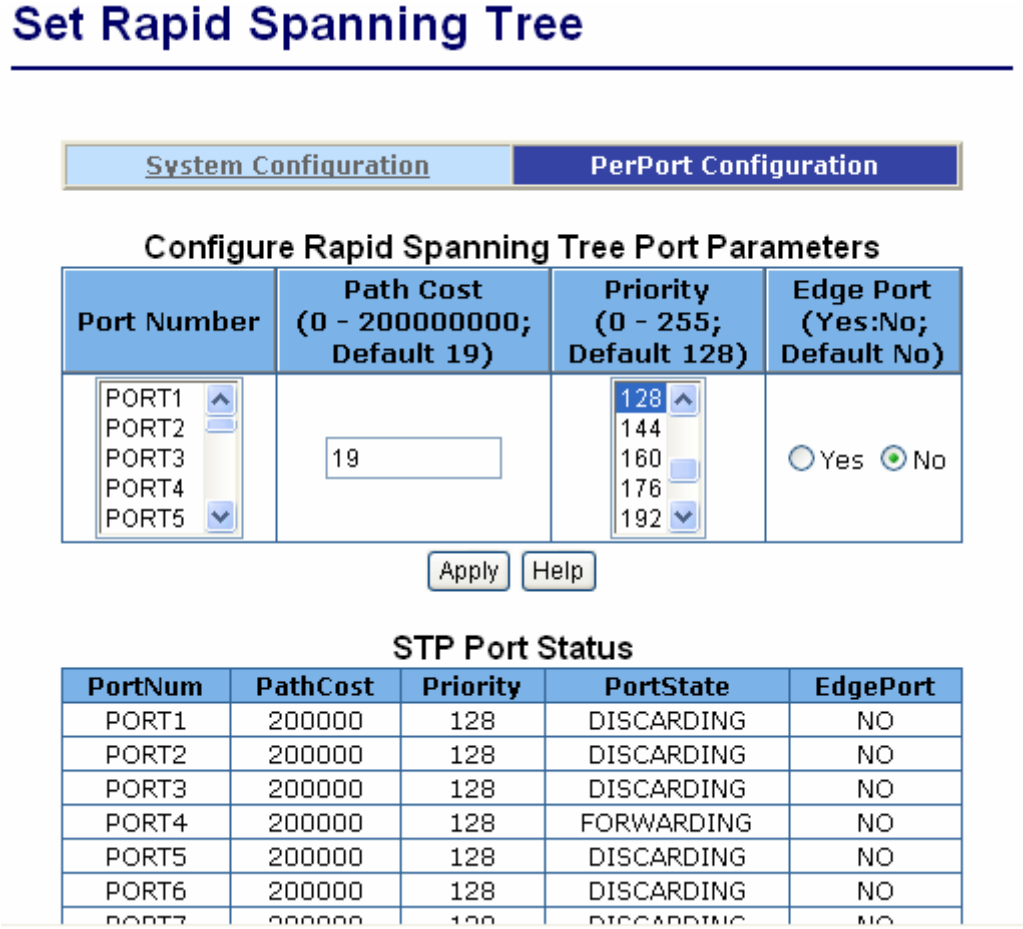
PortNum	PathCost	Priority	PortState
PORT1	10	128	FORWARDING
PORT2	10	128	FORWARDING
PORT3	10	128	FORWARDING
PORT4	10	128	FORWARDING
PORT5	10	128	FORWARDING
PORT6	10	128	FORWARDING
PORT7	10	128	FORWARDING
PORT8	10	128	FORWARDING
PORT9	10	128	FORWARDING
PORT10	10	128	FORWARDING
PORT11	10	128	FORWARDING
PORT12	10	128	FORWARDING
PORT13	10	128	FORWARDING
PORT14	10	128	FORWARDING
PORT15	10	128	FORWARDING

3. **You can set new values for STP parameters.**



Parameter	Description
Priority	A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Enter a number from 1 through to 65535.
Max Age	The number of seconds the bridge waits without receiving any Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number from 6 through to 40.
Hello Time	The number of seconds between the transmission of Spanning-Tree Protocol configuration messages. Enter a number from 1 through to 10.
Forward Delay time	The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number from 4 through to 30.

4. **The following parameters can be configured for each.**

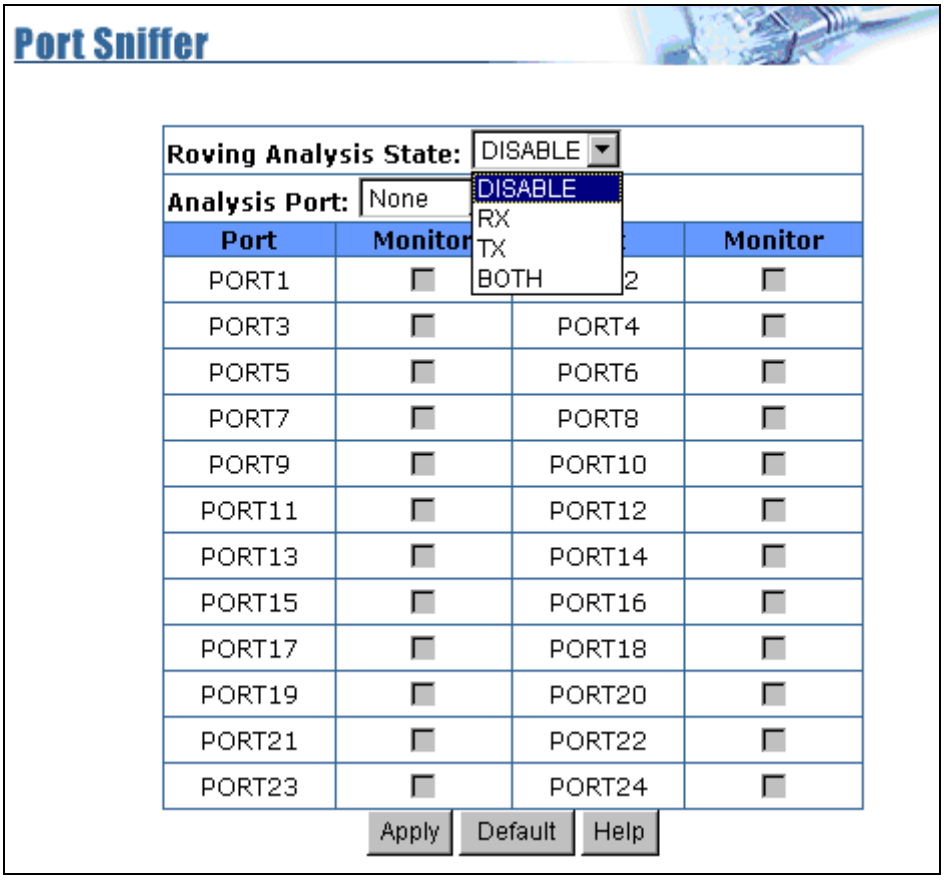


Parameter	Description
Port Priority	Defines if this port is more or less likely to become the root port. The range is from 0 to 255, the default setting is 128 The lower number has the highest priority.
Path Cost	Specifies the path cost of the port. The switch uses this parameter to help determine which port will become a forwarding port. Lower numbers will be used as forwarding ports first. The range is from 1 to 65535. The default values based on IEEE802.1D are: 10Mb/s = 50-600, 100Mb/s = 10-60, 1000Mb/s = 3-10

2-4-9. Port Sniffer (Port Mirroring)

The Port Sniffer is used to monitor traffic in a switched network. Traffic passed through ports can be monitored by one specific port. i.e. Traffic inbound or outbound on a monitored port will be duplicated into the configured sniffer port.

1. **Sniffer Mode:** Selects sniffer mode: Disable \Rx \Tx \Both.
2. **Analysis Port:** Use this option to select the destination port for monitored traffic. This is the port that your network analyzer would be connected to.
3. **Monitored Port:** Based on the Sniffer Mode selection made previously, traffic from the selected port option boxes will be mirrored onto the Analysis port. A maximum of 25 monitored ports can be configured.



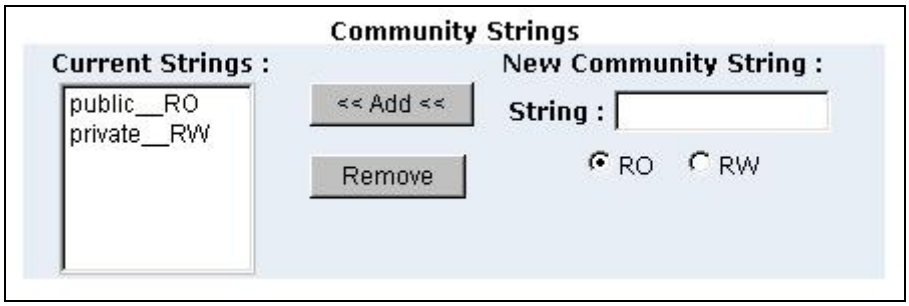
2-4-10. SNMP/Trap Manager

The ESM-24T02M can be managed from any Simple Network Management Protocol (SNMP) application. If using the Management Information Base (MIB) within your SNMP application, then the information can be reported in a more intuitive manner. SNMP is a Protocol that governs the transfer of information between the management station (application) and the agent (the ESM-24T02M switch).

1. **System Options**. Used to define a logical name to the switch, the location of the switch, and contact person for administration of the switch. This information is used in Enterprise SNMP management, where the network can be very widespread, potentially even in other countries. To know where the unit is physically located, and who to contact in the event of a problem is critical.

   Name: Enter a name to be used for the switch.
   Location: Enter the location of the switch.
   Contact: Enter the name of the person or organization that maintains the switch.

2. **Community strings** serve as passwords and can be entered as one of the following:
   RO: Read only. Enables requests accompanied by this string to display MIB-object information.
   RW: **Read write**. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.



3. **Trap Manager** A trap manager is a management station (SNMP application) that receives traps (the system alerts generated by the switch). If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.

2-4-11 Security Manager

This page allows you to change the user name and password for administration of the switch.

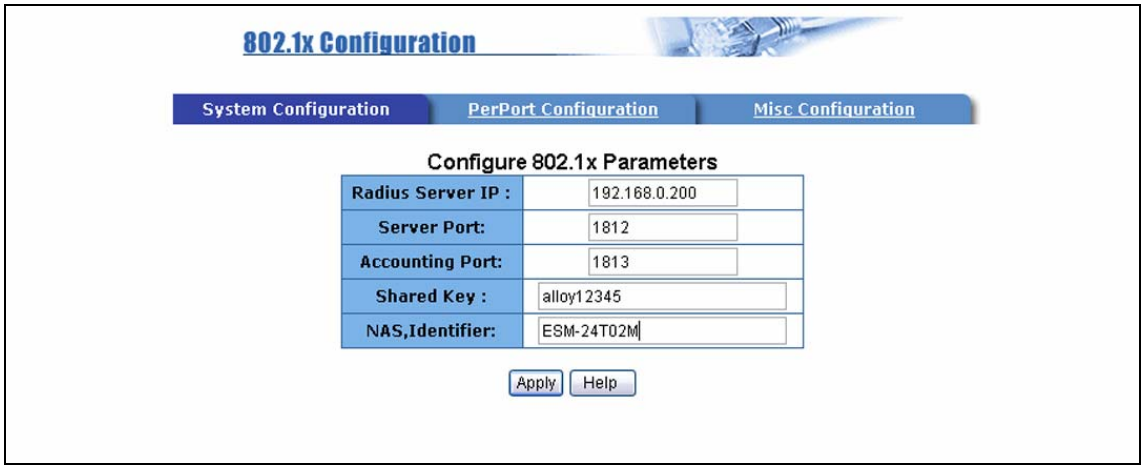
1. **User name:** Type the new user name.
2. **Password:** Type the new password.
3. **Reconfirm password:** Retype the new password.
4. **Click Apply.**

2-4-12 802.1x Configuration

System Configuration

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

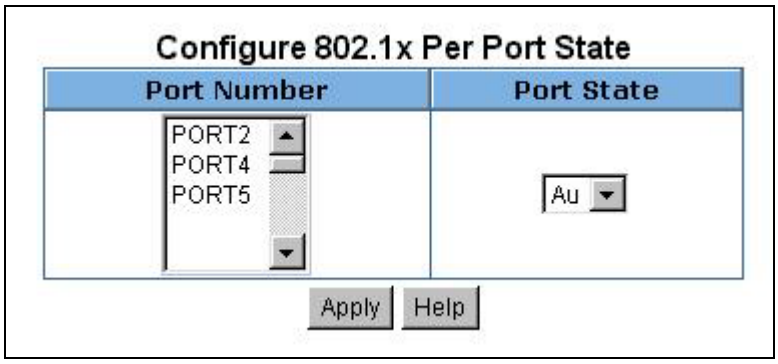
To enable 802.1x : From **Administrator \Switch setting \Advanced** fill in the authentication server information:



Radius Server IP Address: the IP address of the authentication server.
Server Port: The UDP port number used by the authentication server to authenticate.
Accounting Port: The UDP port number used by the authentication server to retrieve accounting information.
Shared Key: A key shared between this switch and authentication server.
NAS, Identifier: A string used to identify this switch.

Perport Configuration

In this page, you can select the specific port and configure the Authorization State. Each port can have a selection of four kinds of Authorization State:



Fu - Force the specific port to be unauthorized.

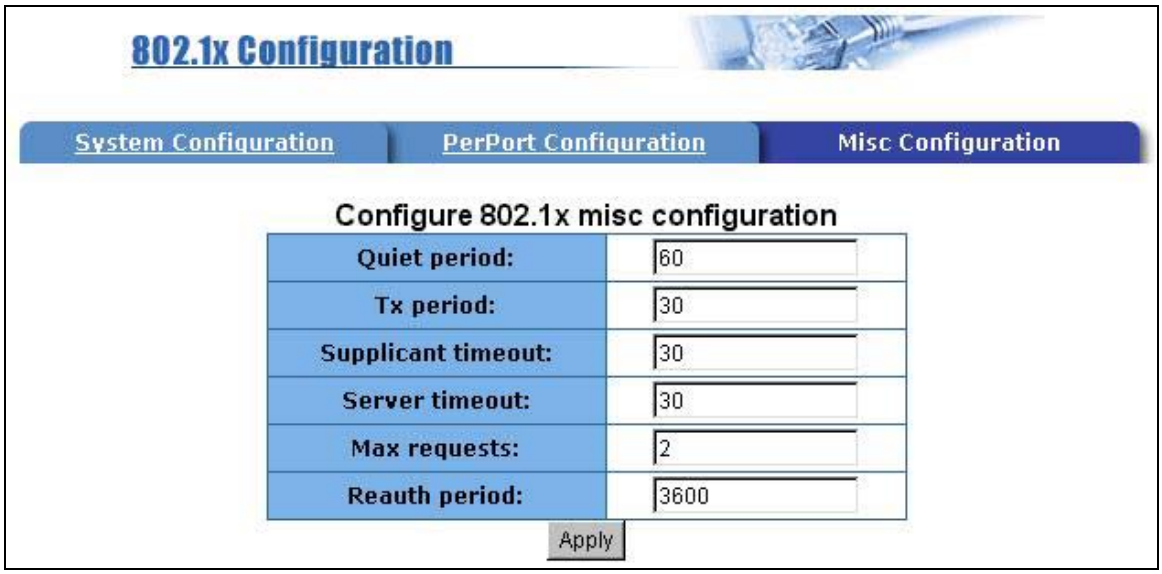
Fa - Force the specific port to be authorized.

Au - The state of the specific port was determined by the outcome of the authentication.

No - The specific port does not support 802.1x functions.

Misc Configuration

(Alloy recommends that these parameters not be changed, unless you have extensive knowledge of 802.1x configuration)
This allows you to change the default configuration for the 802.1x standard:



Quiet Period - Used to define periods of time during which it will not attempt to acquire a supplicant (Default time is 60 seconds).
Tx Period - Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
Supplicant Timeout - Used to determine timeout conditions in the exchanges between the supplicant and authentication server (Default value is 30 seconds).
Server Timeout - Used to determine timeout conditions in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
ReAuthMax - Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
Reauth Period used to determine a nonzero number of seconds between periodic re-authentication of the supplications (Default value is 3600 seconds).

2-5. TFTP Update Firmware

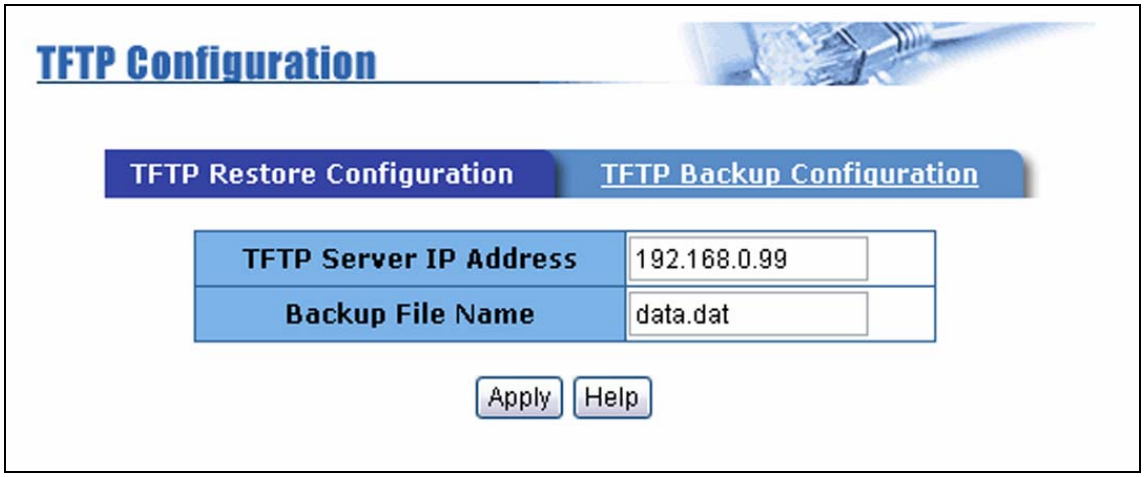
1. **The TFTP menu option allows you to load a new firmware image into the switch:**

   - Install TFTP program (TFTP applications can be found on the internet).
   - Copy the updated firmware **image. bin** into the TFTP server's upload/download directory.
   - Start the TFTP application, you should see a "waiting for connection" type prompt within the application.
   - In web management select administrator—TFTP update firmware.
   - Download the new **image.bin** file by pressing <apply>. (the file name needs to match the name of the file copied into the TFTP upload/download directory.
   - After the update has finished, press <reboot> to restart switch.

2-6. Configuration Backup

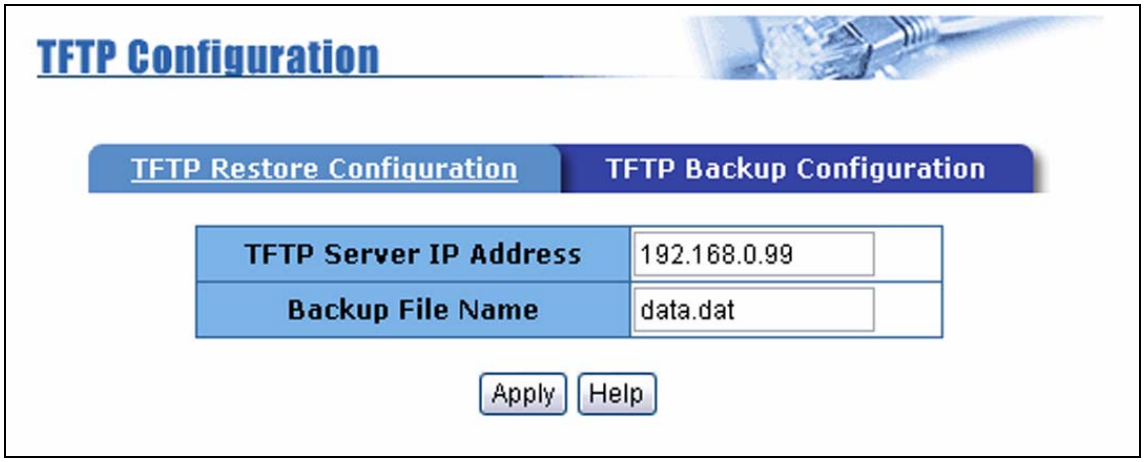
2-6-1. TFTP Restore Configuration

The TFTP restore configuration menu, functions much the same way as the TFTP update firmware function. But its purpose is to restore to flash memory, the system configuration from a previous backup operation.



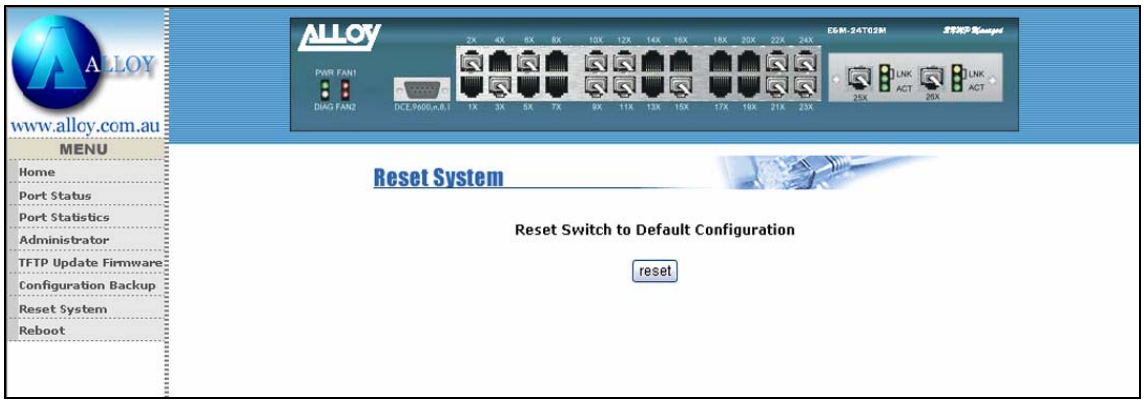
2-6-2. TFTP Backup Configuration

The TFTP backup configuration menu, functions much the same way as the TFTP update firmware function. But its purpose is to backup from flash memory the system configuration, so that you have a permanent configuration that can be easily restored if necessary.



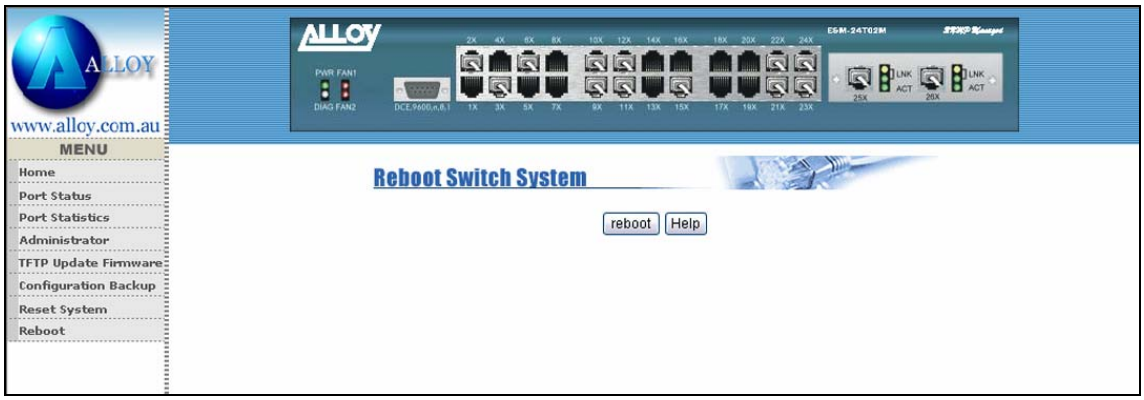
2-7. Reset System

The Reset System menu option will default all configuration values.



2-8. Reboot

The Reboot menu option initiates a switch software reset.



3. Console -- 1K Xmodem update firmware

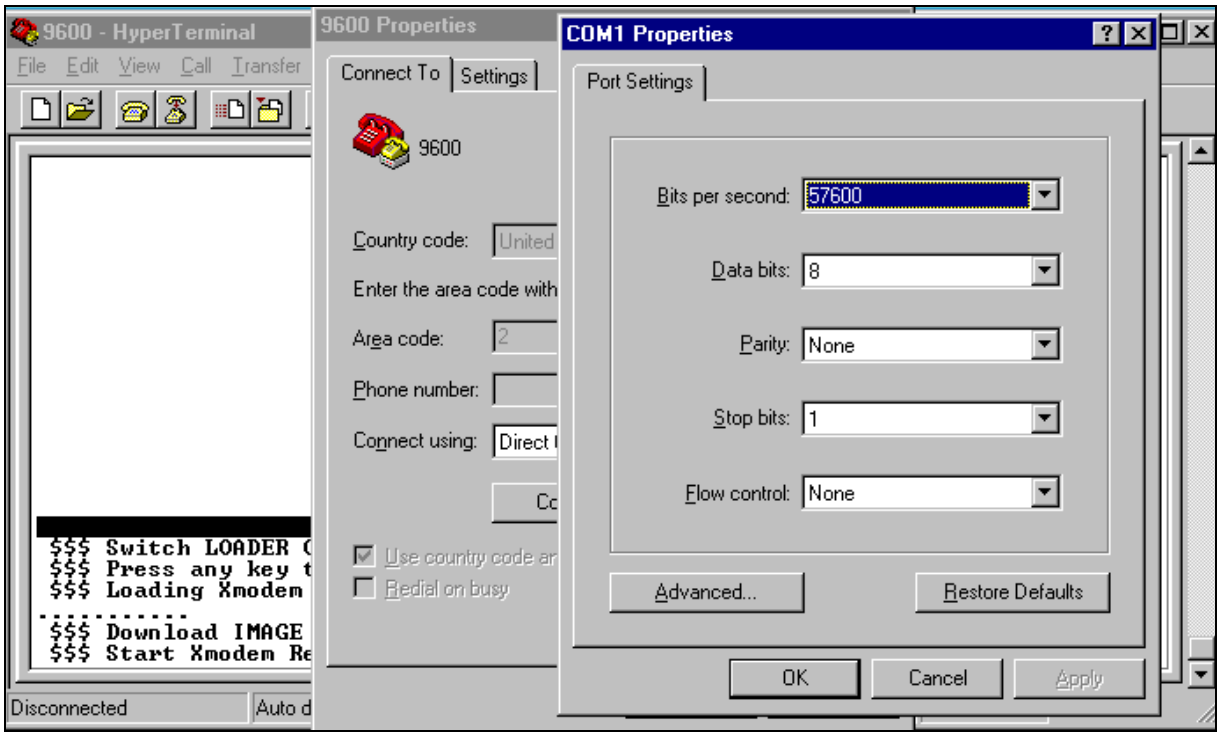
The ESM-24T02Mx provides the ability to perform a 1k X modem firmware update feature from the RS-232 console port. 1K X modem only works in 57600bps mode. There are 2 situations where the 1k X modem update feature can be used:

a. The Administrator enters "1K X modem receiver mode" by pressing any key within 5 seconds after system is powered on.

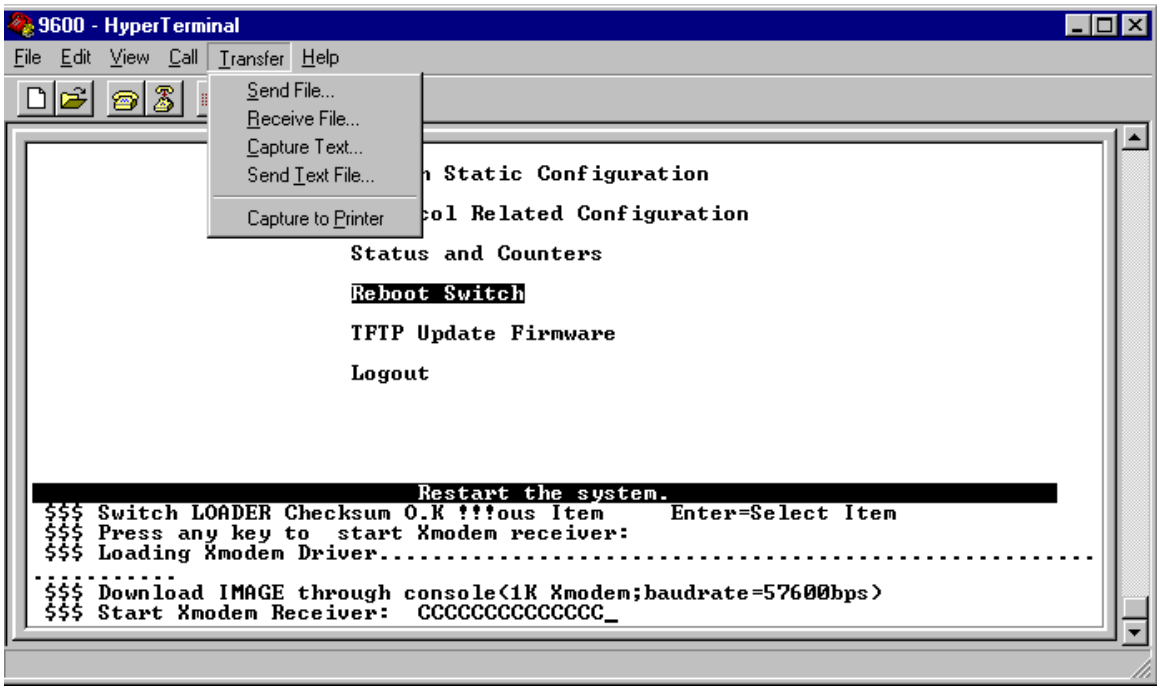
b. The system automatically enters "1K X modem receiver mode" if it detects a firmware checksum failure while booting.

1. When you initially start the “1K X modem mode” from one of the 2 options above, please ensure that you are connected a 57600bps

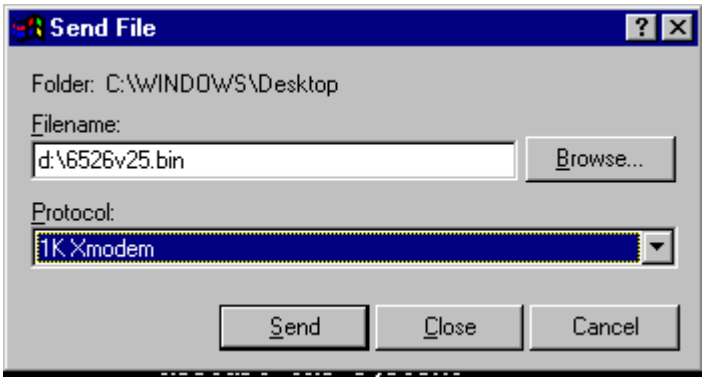
   Select ***File -> Properties,*** and change the baud-rate to 57600bps, then press ***OK***.



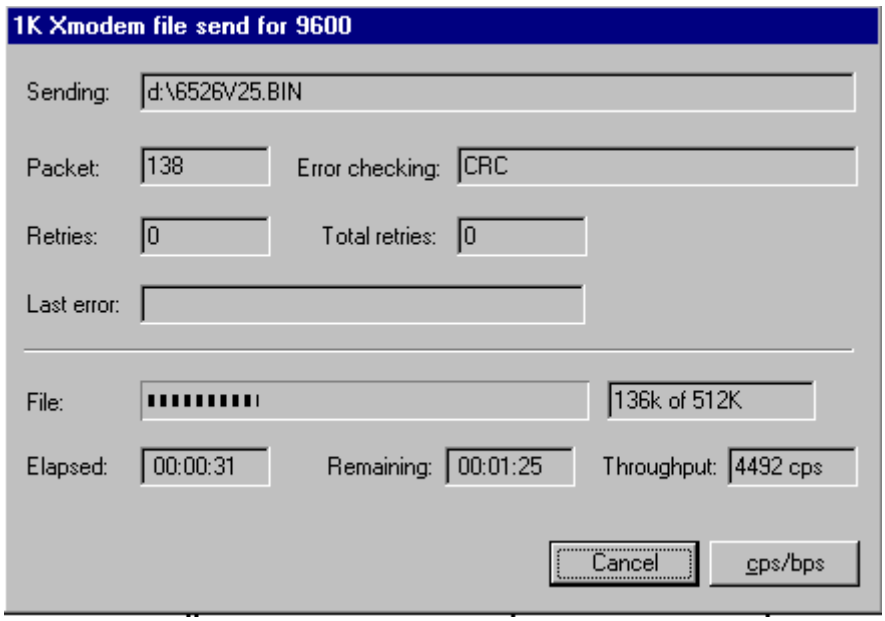
2. Press the connected icon, you will see “CCCC…”displayed on the console. Then select ***Transfer*** , Send ***File.***



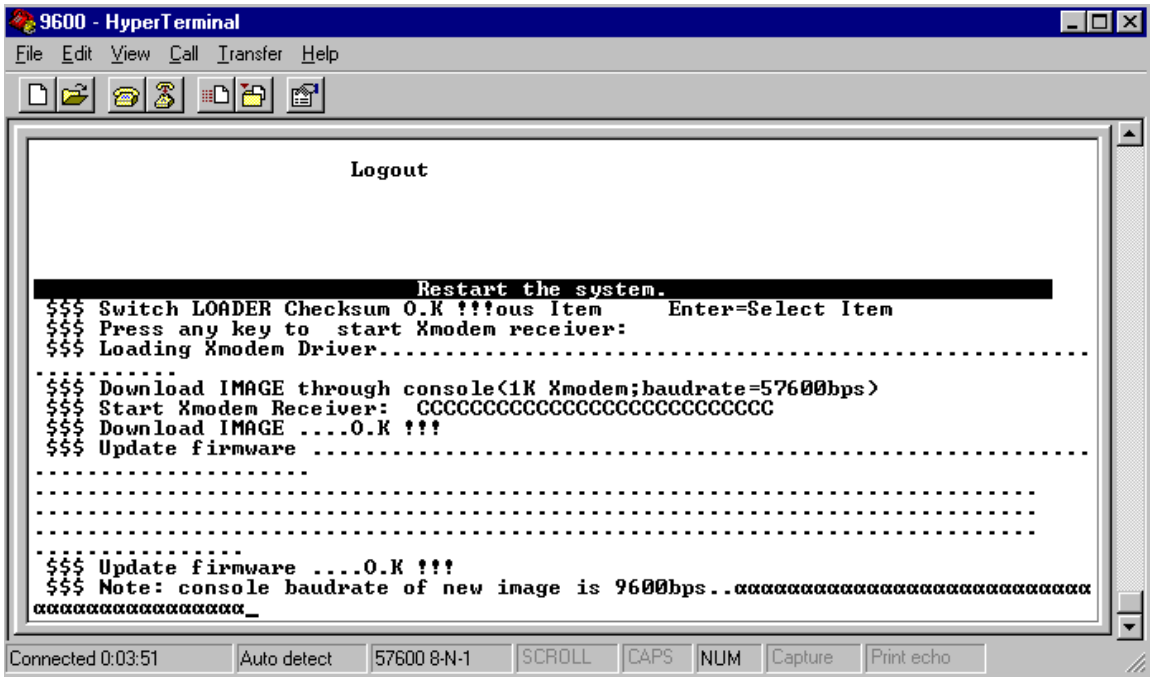
3. Select “***1K Xmodem”*** in the ***Protocol*** item, and browse to the firmware file you will be loading and then Press the ***Send*** button.



4. The firmware image will start downloading.



5. When the image has finished downloading, the switch system will update firmware automatically. You should see a message “Update firmware ok” and the switch will then reboot.

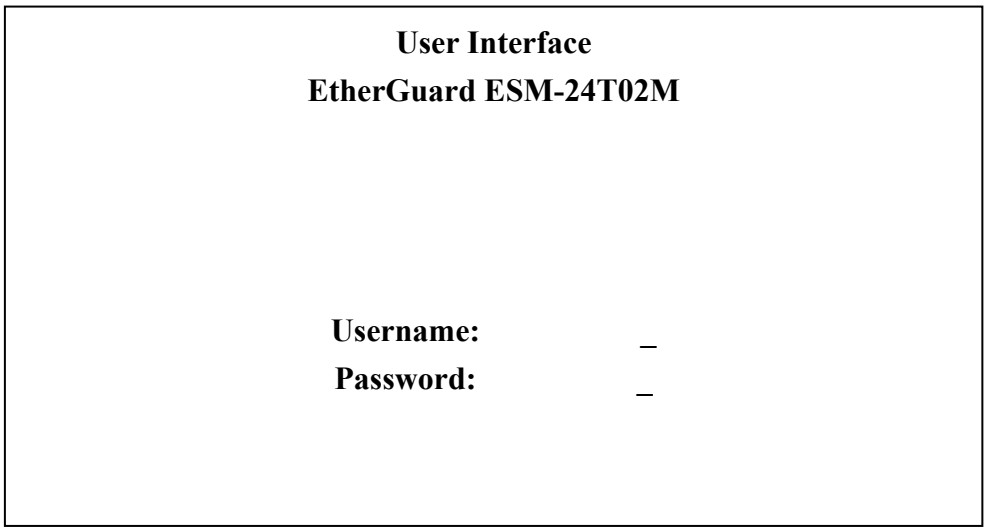


4. Out-of-band Terminal mode management

1. The **ESM-24T02M** switch also provides a serial interface to manage and monitor the switch. The following Console Port Information can be used by the system administrator to configure the switch via a terminal application.

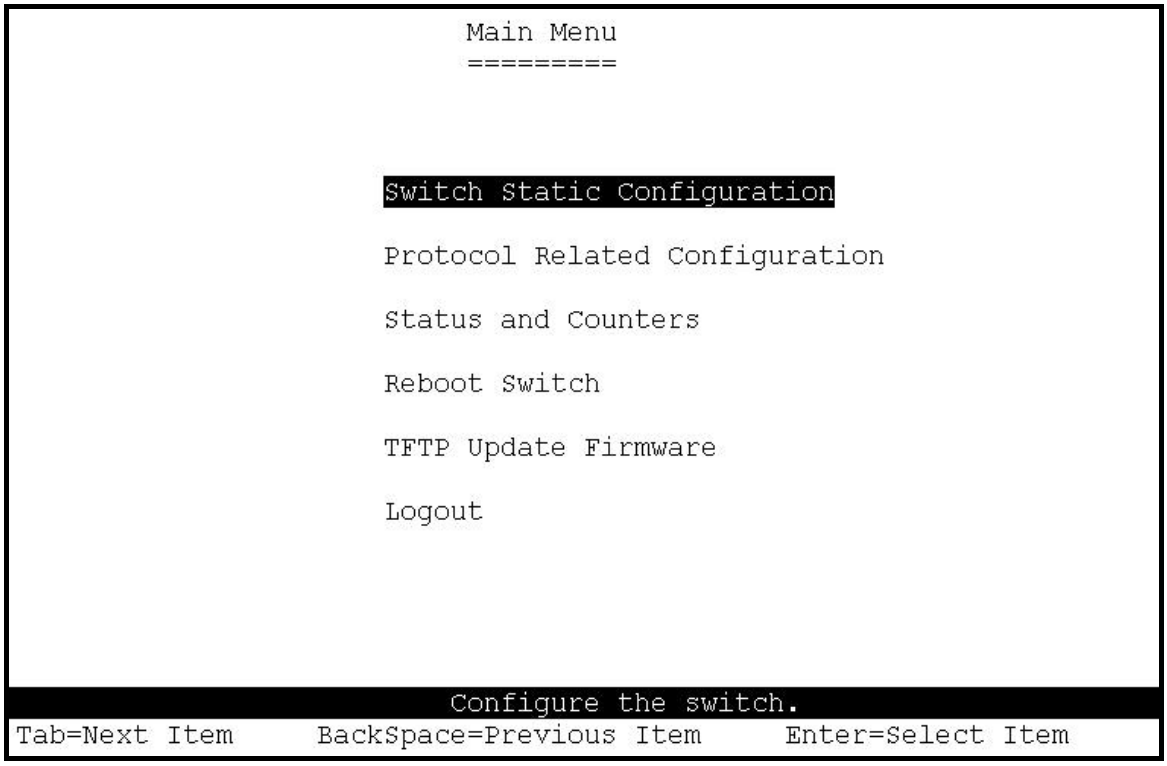
   NOTE: Detailed descriptions of the various functions are not provided in the *Console Configuration* documentation. Please see the *Web Configuration* documentation above (pages 13 to 49) for more detailed information.

2. You need to provide the administrator user name and password to login. The default user name is "admin", the default password is "admin".



4-1 Main Menu

There are six items within the Main Menu selection:

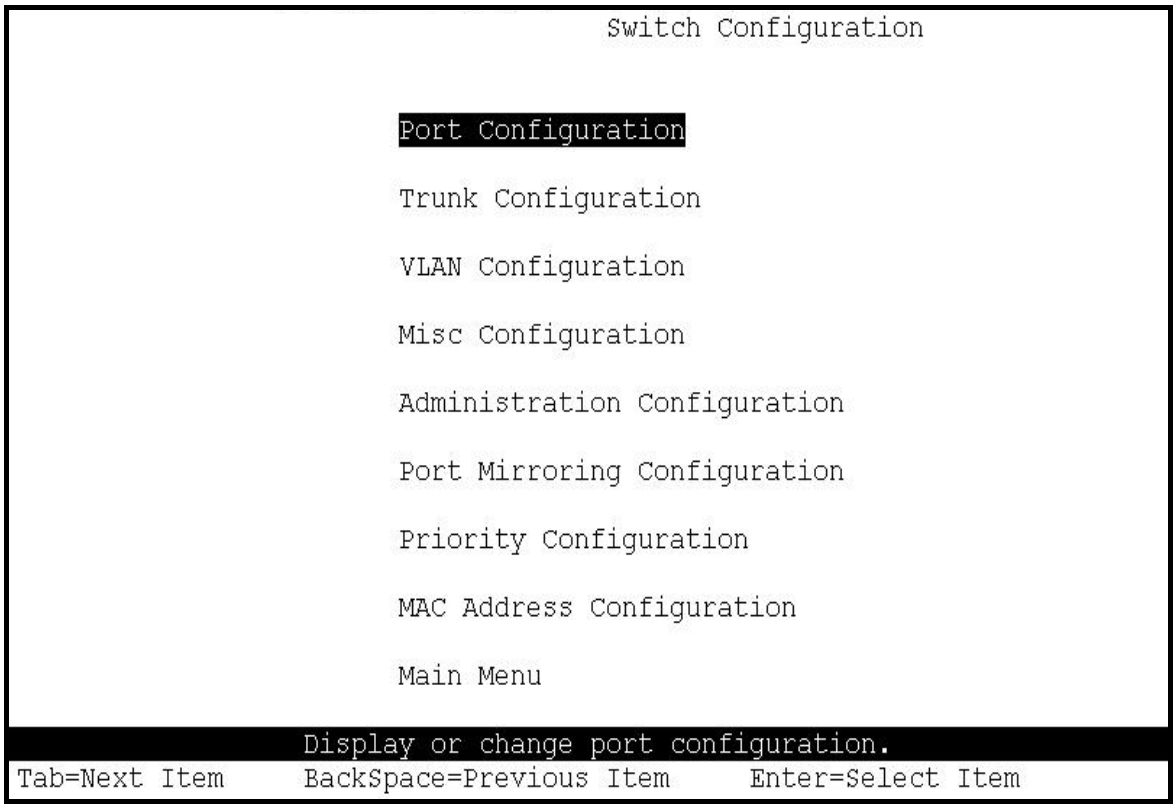


Switch Static Configuration: Configures the advanced Layer 2 switching functions.
Protocol Related Configuration: Configures the switches IP address settings.
Status and Counters: Displays status/statistical information about the switch.
Reboot Switch: Restart the system or reset switch to default configuration.
TFTP Update Firmware: Use TFTP to download a new firmware image.
Logout: Exit the console configuration program.

<Control Keys>

The following keys perform various functions within the console management:
Tab: Move the cursor to next item.
Backspace: Move the cursor to previous item.
Enter: Select the current item.
Space: Toggle selected item to next option.

4-2 Switch Static Configuration



<-Actions->

Many of the following configuration pages use the following <-Action-> options.

<Quit>: Exit the page and return to previous menu.

<Edit>: Configure the options displayed.

<Save>: Save all configured values.

<Previous Page>: Return to previous page (previous ports).

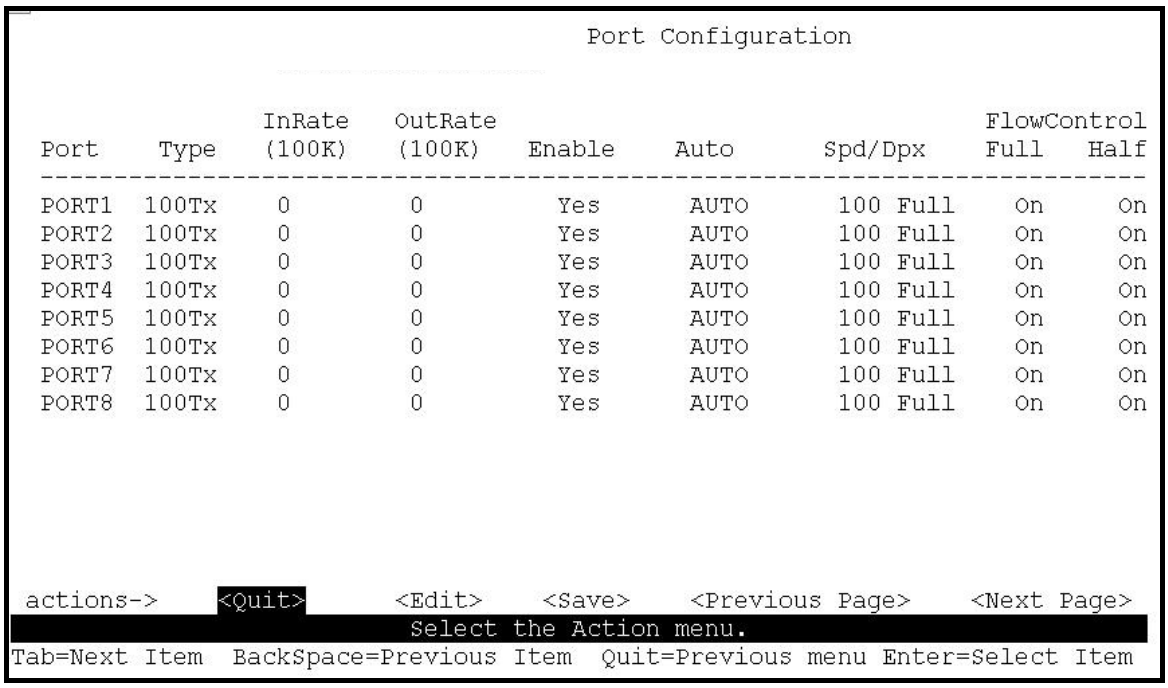
<Next page>: Go to the next page (next ports).

To exit out of Edit mode:

Ctrl+A : Exit configuration more , Go Back to action menu line.

4-2-1. Port Configuration

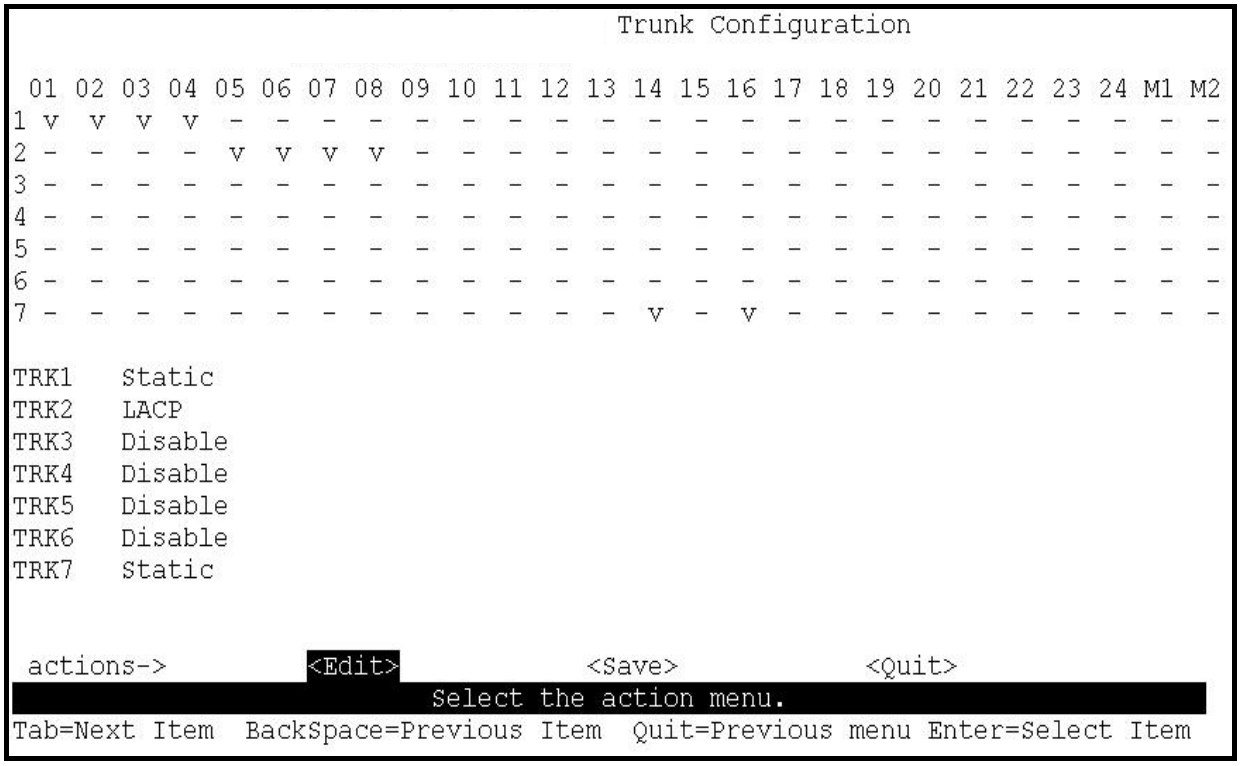
Edit / View the port configuration.



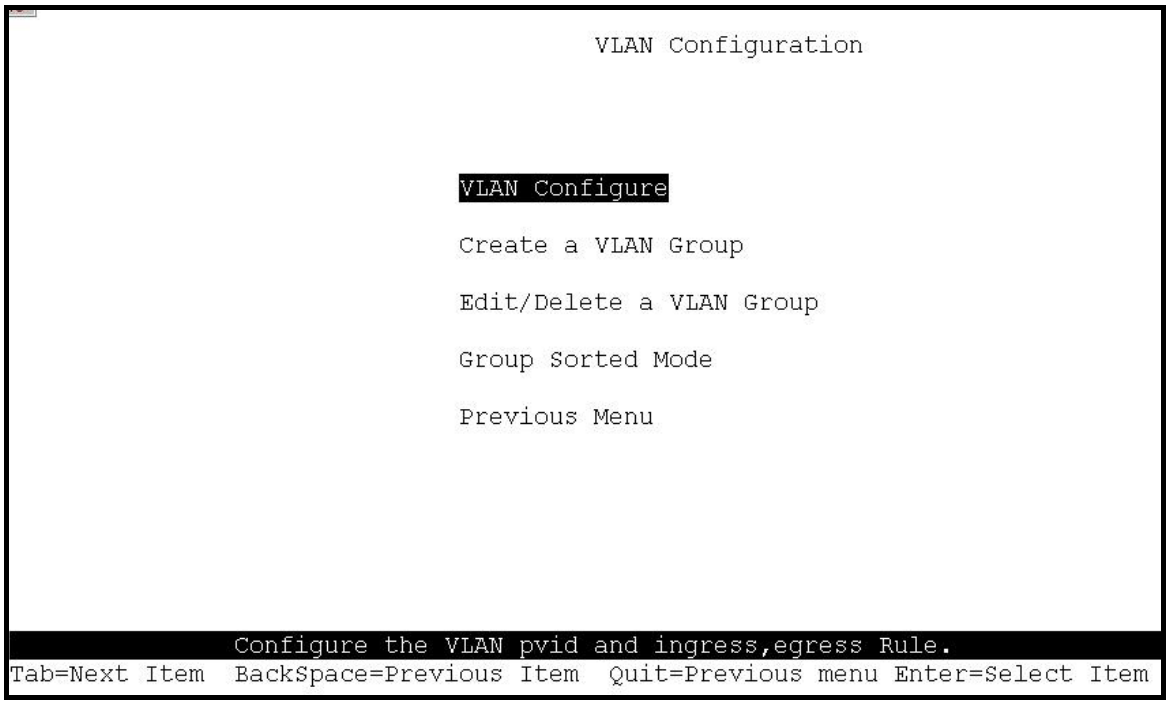
1. **InRate (100K/unit):**
   0: disable rate control.
   1~1000: valid rate value.
2. **OutRate (100K/unit):**
   0: disable rate control.
   1~1000: valid rate value.
3. **Enabled:**
   Enables or Disables this port in the switch.
   "**Yes**" = Enable.
   "**No**" = Disable.
4. **Auto:**
   Define Auto negotiation mode. Options: "**Auto**", "**Nway_Force**", "**Force**"
   Spd/Dpx:
   Define the port speed and Duplex.
5. **Flow Control:**
   Full: Enables or Disables Full Duplex flow control
   Half: Enables or Disables Half Duplex flow control. (backpressure)

4-2-2. Trunk Configuration

This page can be used to create a maximum of up to seven trunk groups. Users can arbitrarily select up to four ports from port 1 to port 26 to build a trunk group.

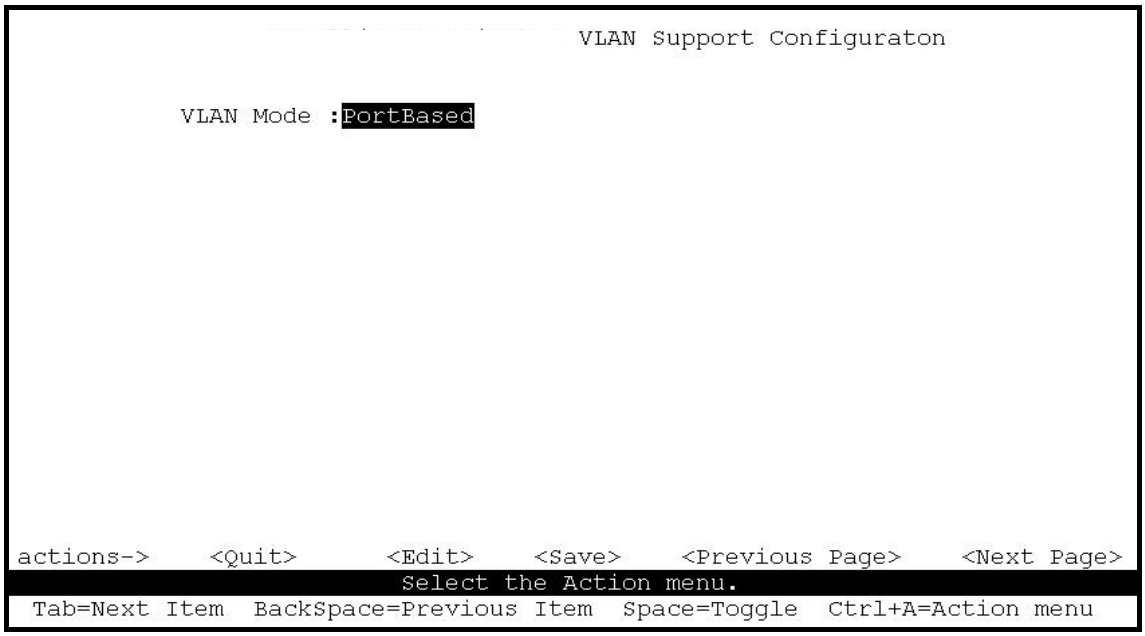


4-2-3. VLAN Configuration

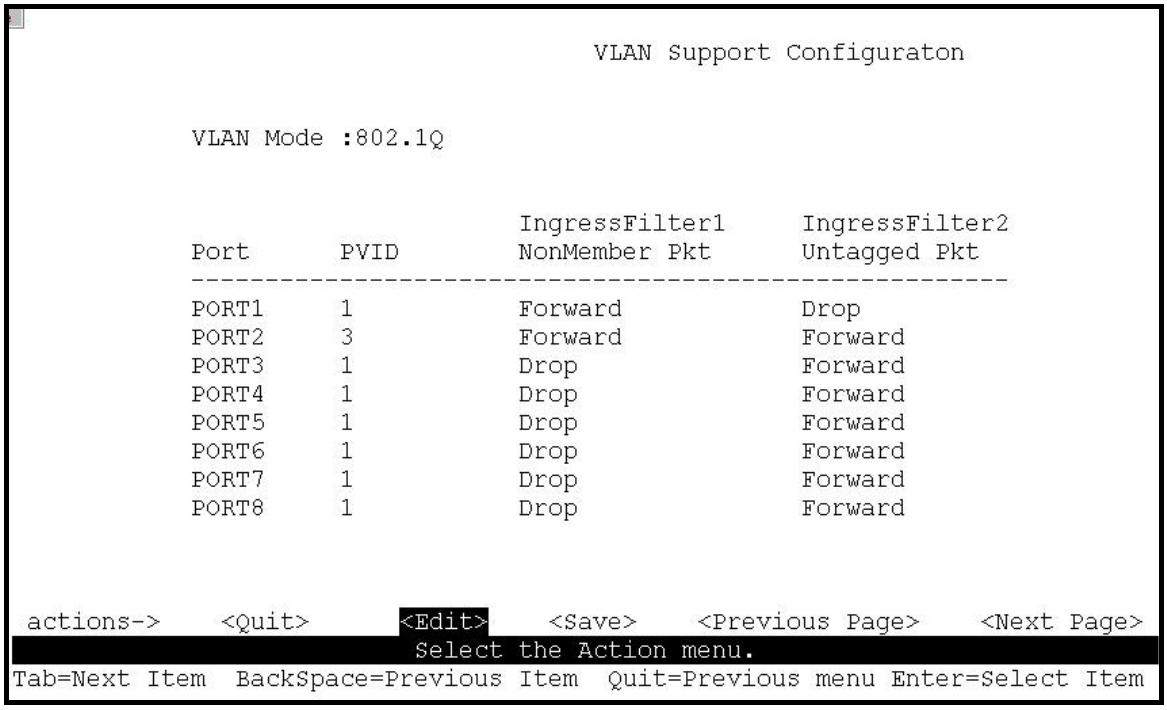


4-2-3-1. VLAN Configure

Two modes of VLAN can be selected. Port-based VLAN or 802.1Q VLAN



If set to 802.1Q VLAN, then you will need to define PVID, ingress filtering 1 and ingress filtering 2.

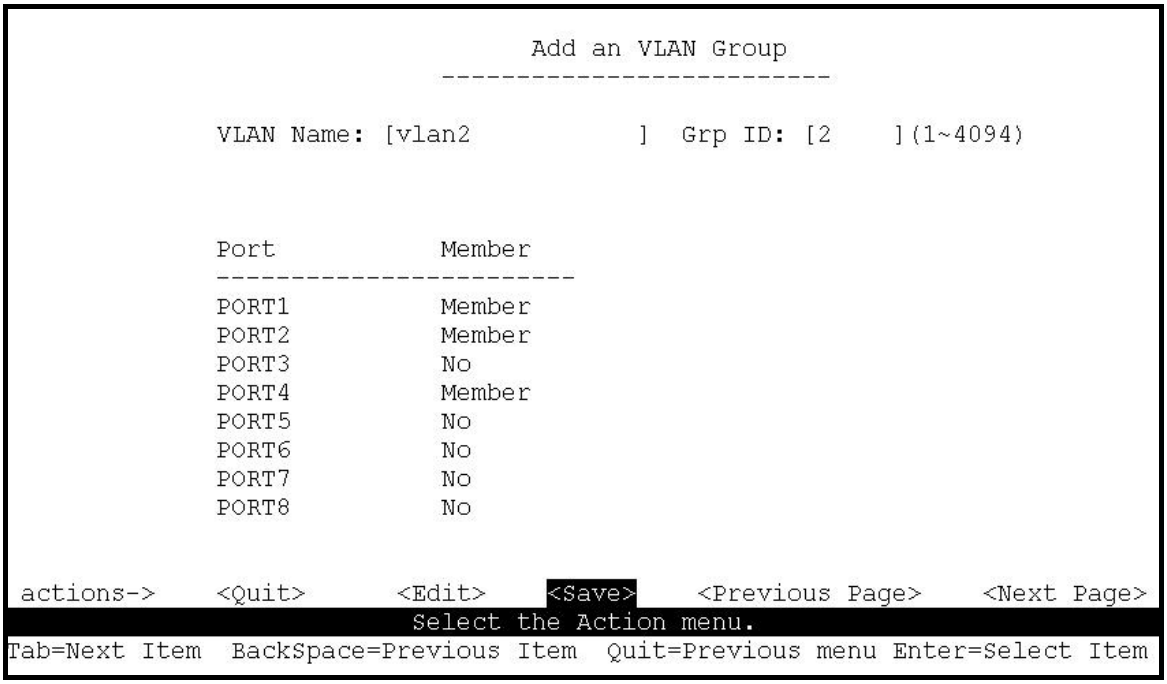


4-2-3-2. Create a VLAN Group

Create a Port-Based VLAN

To create a port-based VLAN you need to add member/nonmember ports to it.

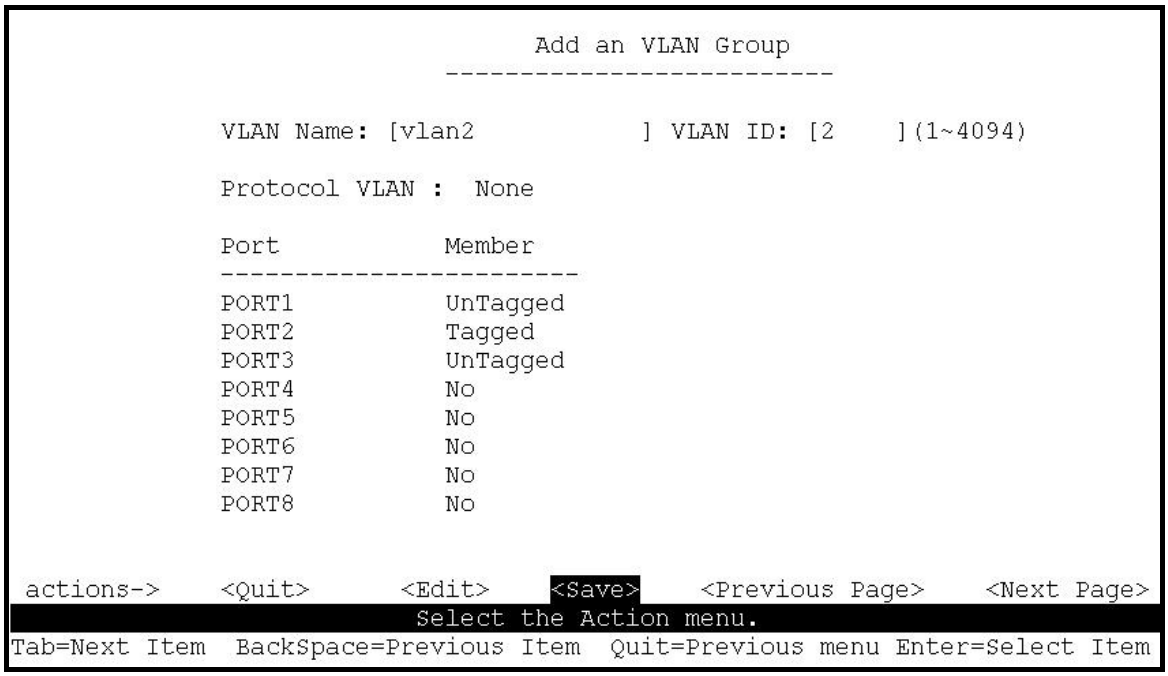
1. **VLAN Name:** Type a name for the new VLAN.
2. **Grp ID:** Type the VLAN group ID. The group ID range is 1~4094.
3. **Member:** Press the **<Space>** key to choose VLAN members.



Create 802.1Q VLAN

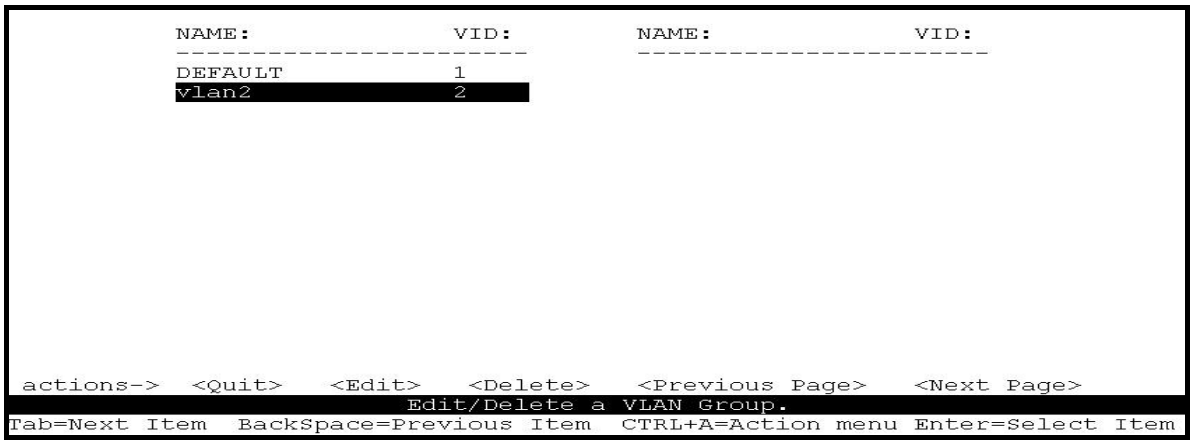
To create an 802.1Q VLAN you need to add member/nonmember ports to it.

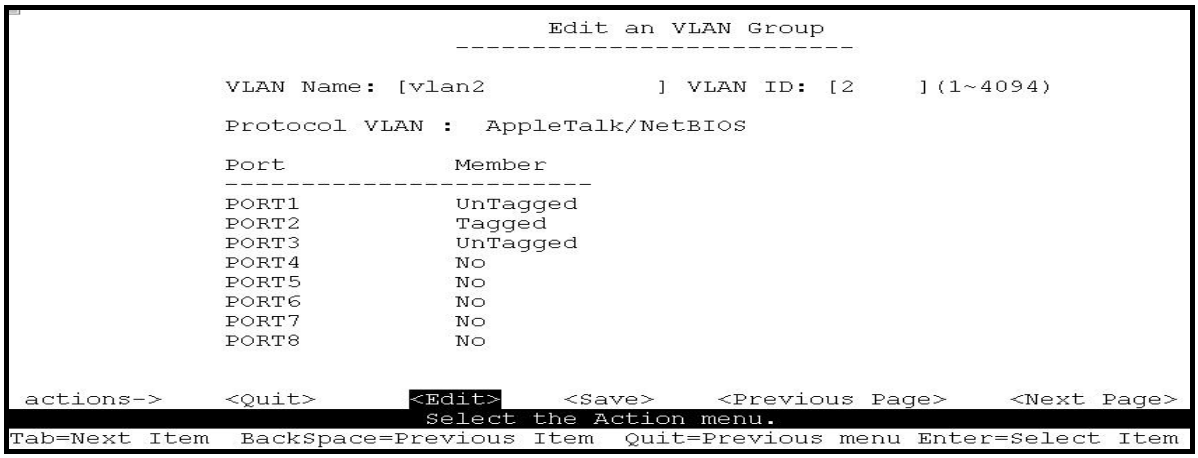
1. **VLAN Name:** Type a name for the new VLAN.
2. **VLAN ID:** Type a VID (between 1~4094). The default is 1.
   There can be up to 256 VLAN groups defined.
3. **Protocol VLAN:** Press **Space** key to choose protocol type.
4. **Member:** Press **Space** key to choose VLAN members and their mode.



4-2-3-3. Edit / Delete a VLAN Group

This page allows administrators to edit or delete VLAN group entries.

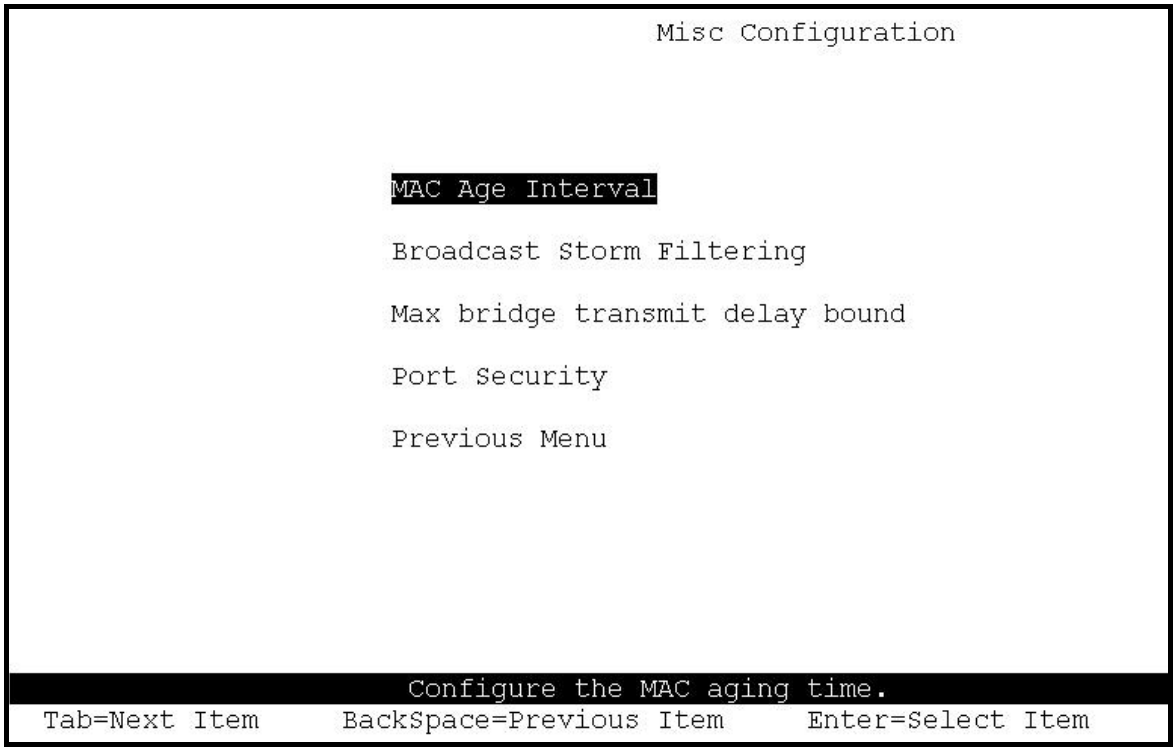




4-2-3-4. Groups Sorted Mode

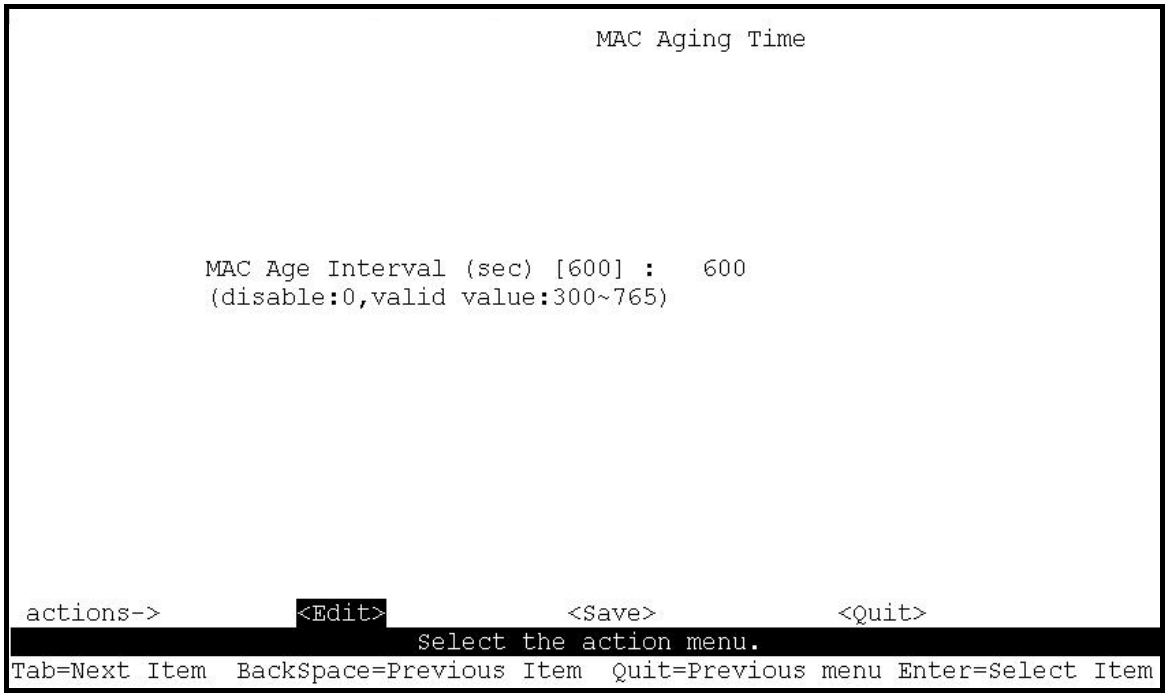
This page, allows for easier access to VLAN groups when there are numerous entries. They can be sorted by either Name or VID, and then edited as normal.

4-2-4. Misc Configuration



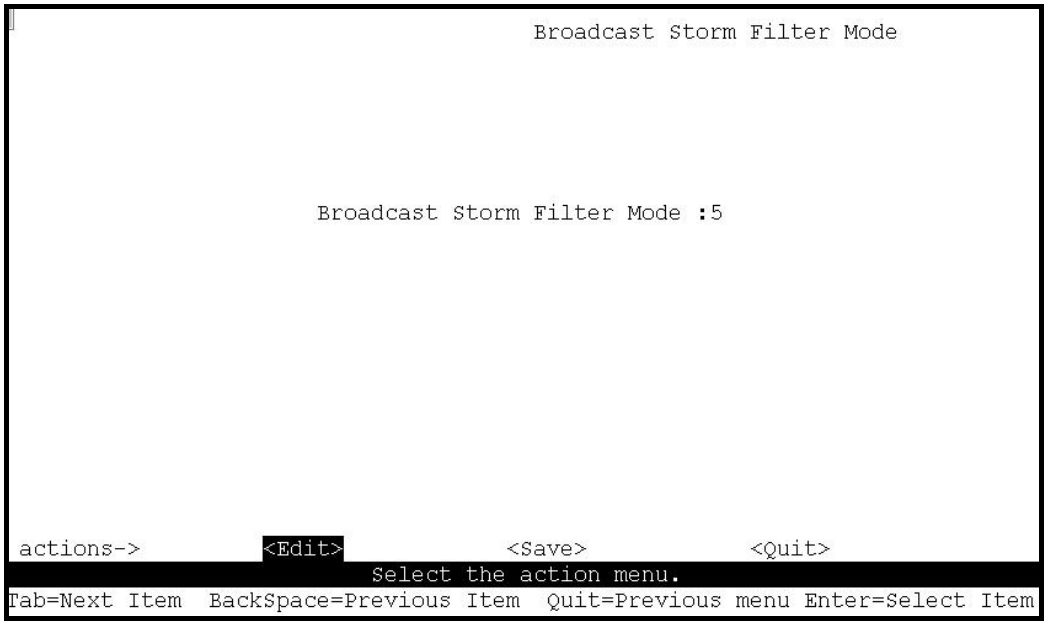
4-2-4-1. MAC Age Interval

Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is **300** seconds.



4-2-4-2. Broadcast Storm Filtering

Configuring broadcast storm control.
Valid threshold values are 5%, 10%, 15%, 20%, 25% and NO. Default is 5%.

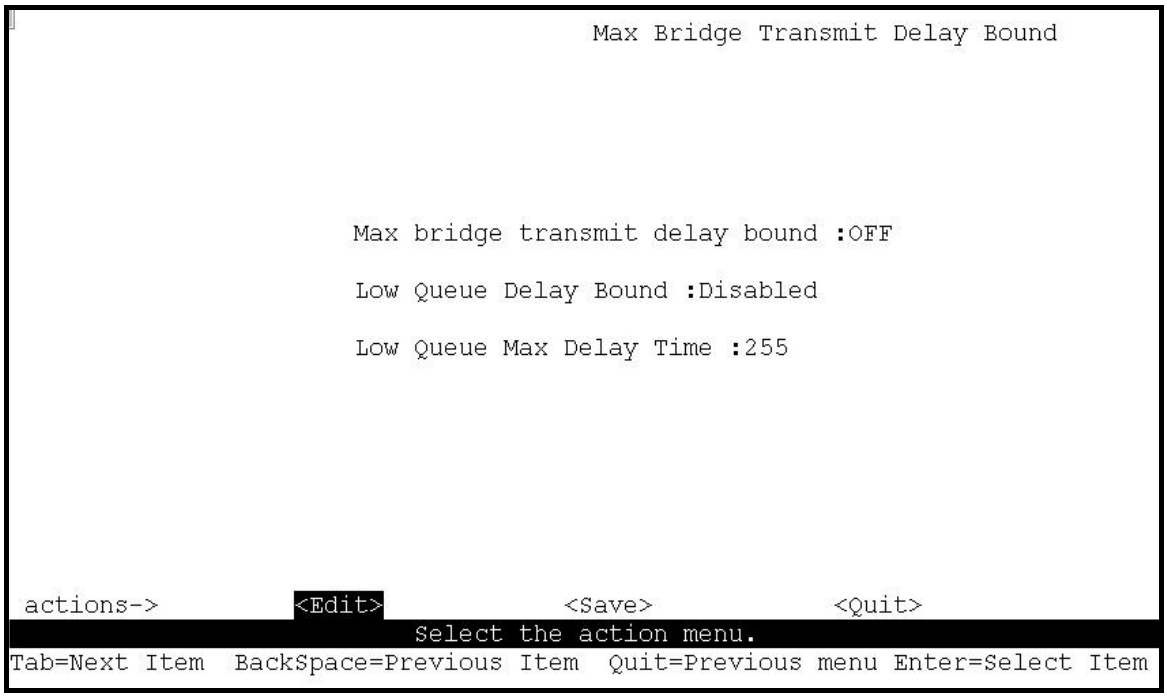


4-2-4-3. Max bridge transmit delay bound

Max bridge transmit delay bound control: This Limits the packets queuing time. If enable, packets that are queued longer than this setting will be dropped. Valid values for this are 1sec, 2 sec, 4 sec and off. Default is 1 seconds.

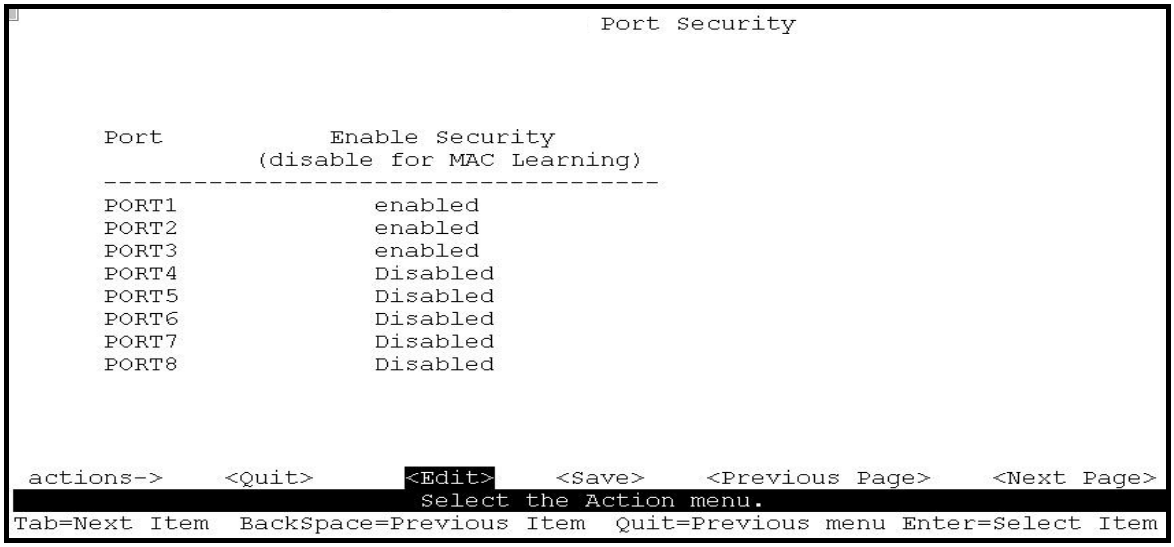
NOTE: Make sure the "Max bridge transit delay bound" control is enabled before enabling the "Low Queue Delay Bound" option.

Low Queue Delay Bound: This controls how low priority packets are queued in the switch. The **Max Delay Time** setting defines when a low priority packet is given more priority to send.



4-2-4-4. Port Security

Port Security: Setting a ports security mode to on (enabled) will lock it to all unauthorized MAC addresses. This disables the address learning functionality on the port and then only incoming packets with a known source MAC addresses will be forwarded by the port. Administrators can disable the port from learning any new MAC addresses, then use the static MAC addresses table entry screen to define a list of MAC addresses that can be used by the secure port.

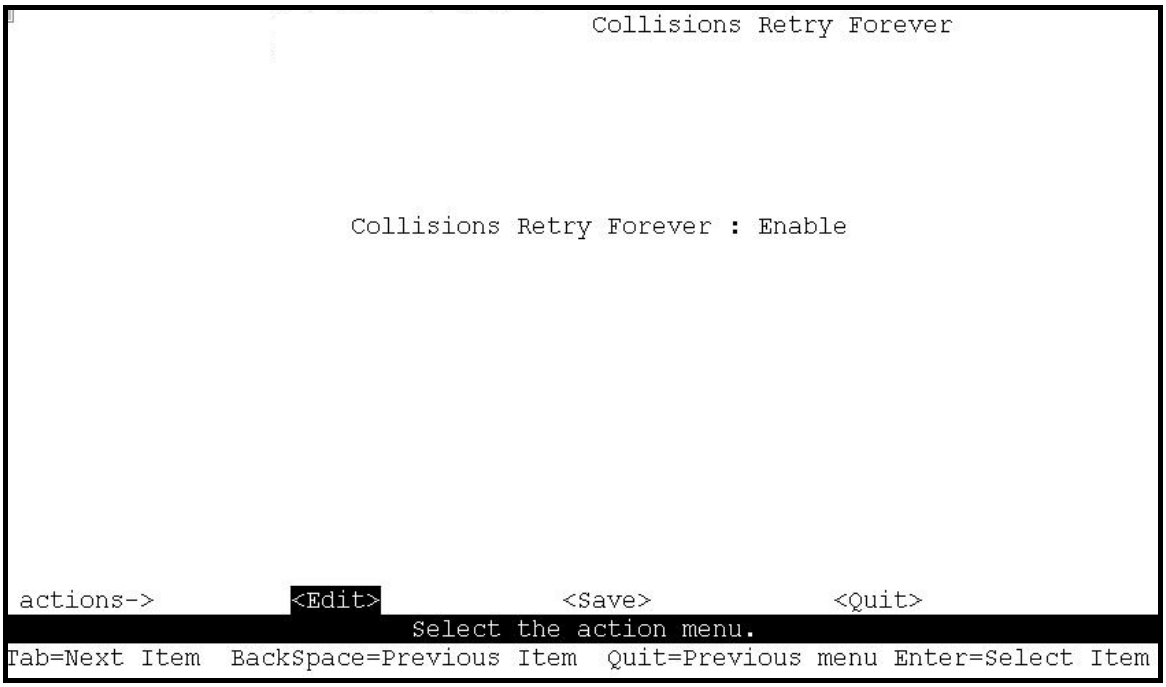


4-2-4-4. Collision's Retry Forever

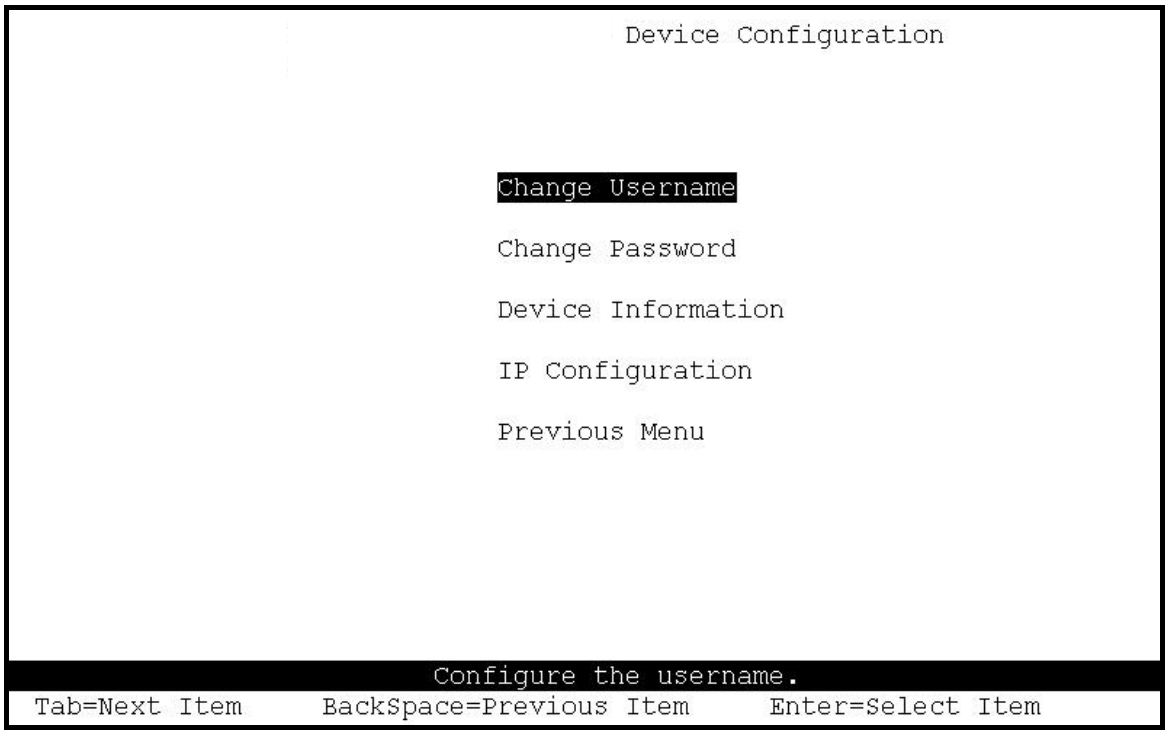
(This setting only affects Half Duplex connections)

Disable – Any collisions are retried for a maximum of 48 times, after which the packet will be dropped.

Enable – Collision will be retried indefinitely.



4-2-5. Administration Configuration



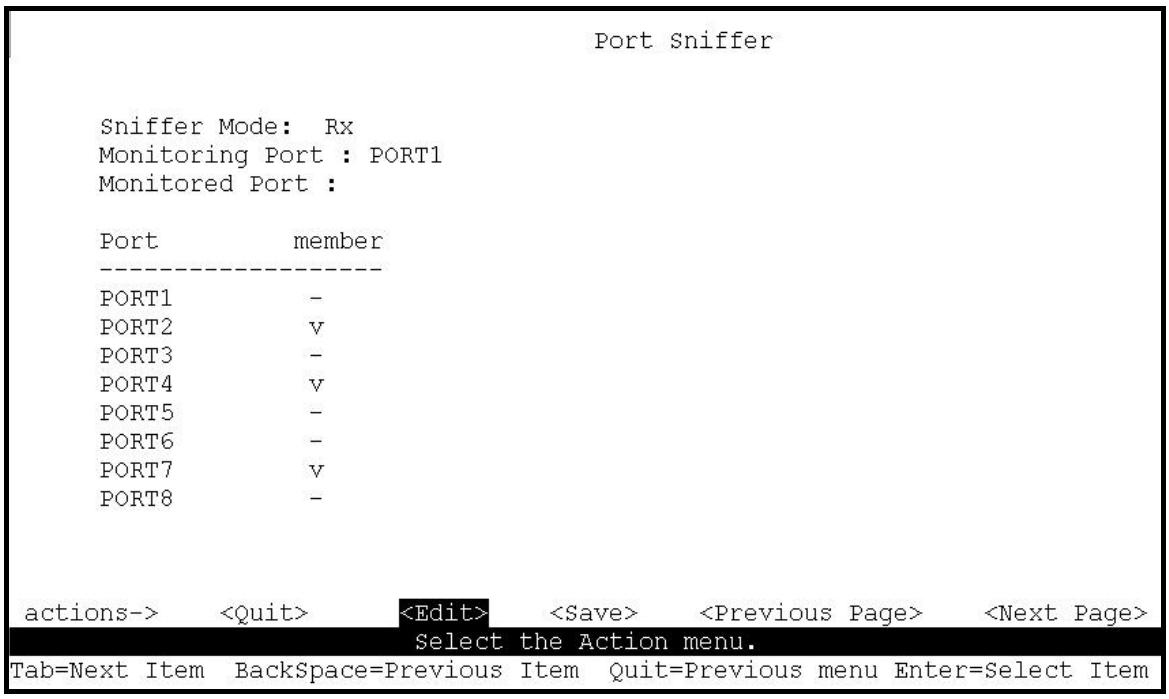
Configure the following options.

- **Change Username**
- **Change Password**
- **Device Information** (name, description, location, content)
- **IP Configuration** (IP address, Mask, Gateway)

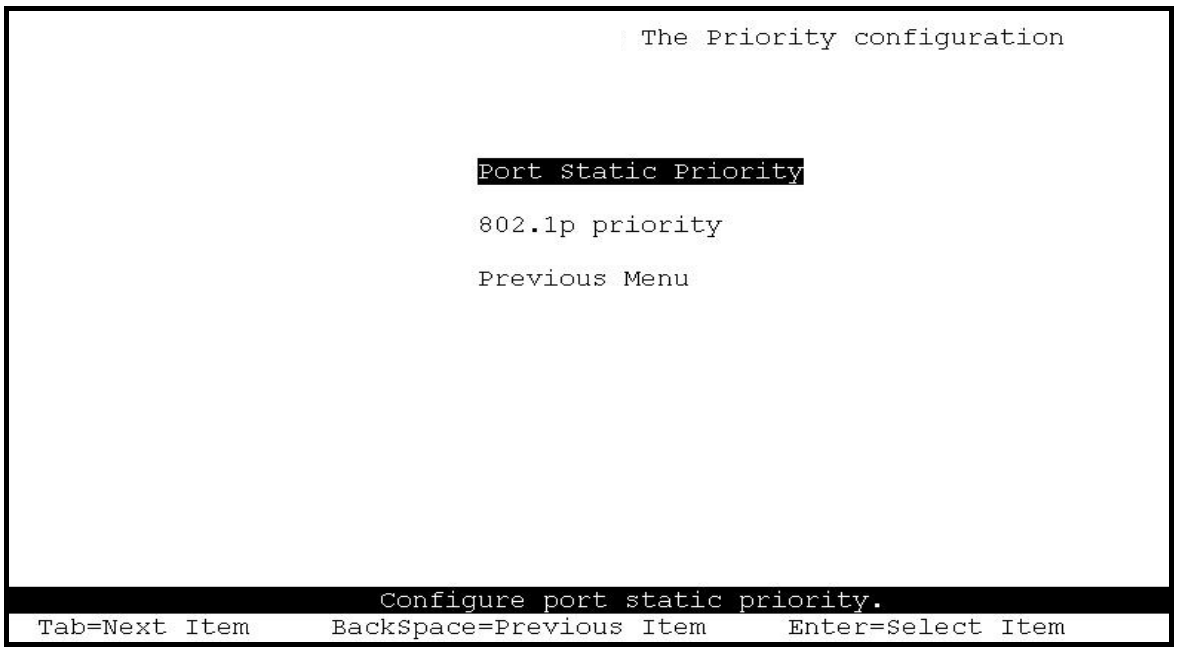
4-2-6. Port Mirroring Configuration

The Port Sniffer is used to monitor traffic in a switched network. Traffic passed through ports can be monitored by one specific port. i.e. Traffic inbound or outbound on a monitored port will be duplicated into the configured sniffer port

1. **Sniffer Mode:** Press **Space** key to set sniffer mode Disable, Rx, Tx or Both.
2. **Monitoring Port (Analysis Port):** Use this option to select the destination port for monitored traffic. This is the port that your network analyzer would be connected to.
3. **Monitored Port:** Based on the Sniffer Mode selection made previously, traffic from the selected port will be mirrored onto the Analysis port. A maximum of 25 monitored ports can be configured. Press **Space** key to choose member port, "V" – is the member, "-" = not a member.

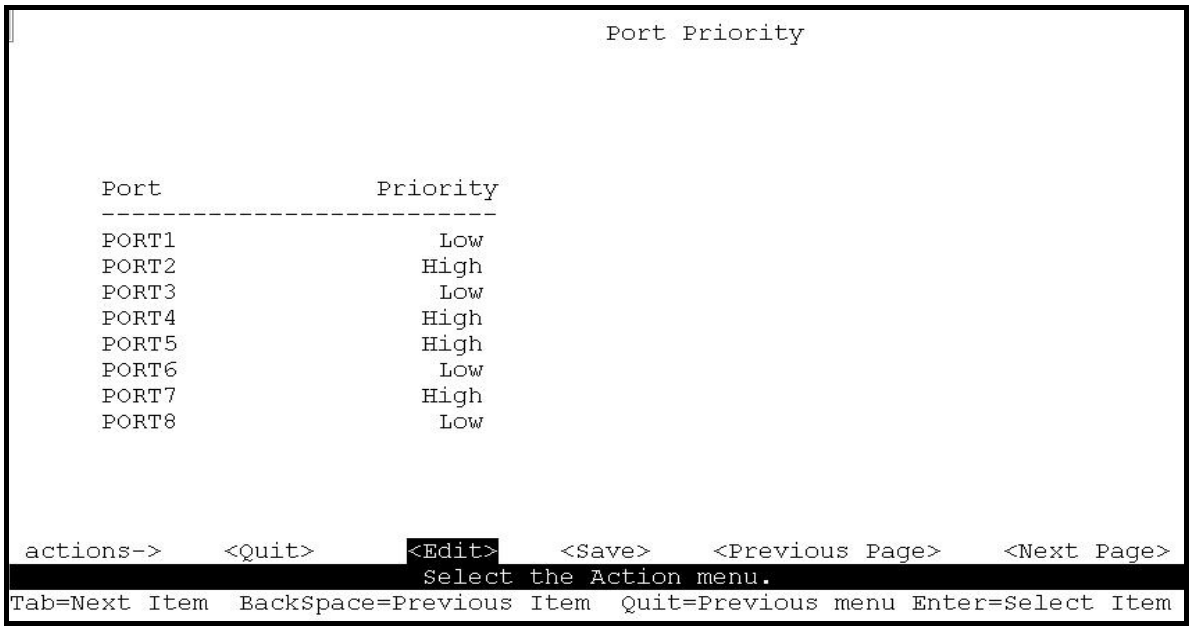


4-2-7. Priority Configuration



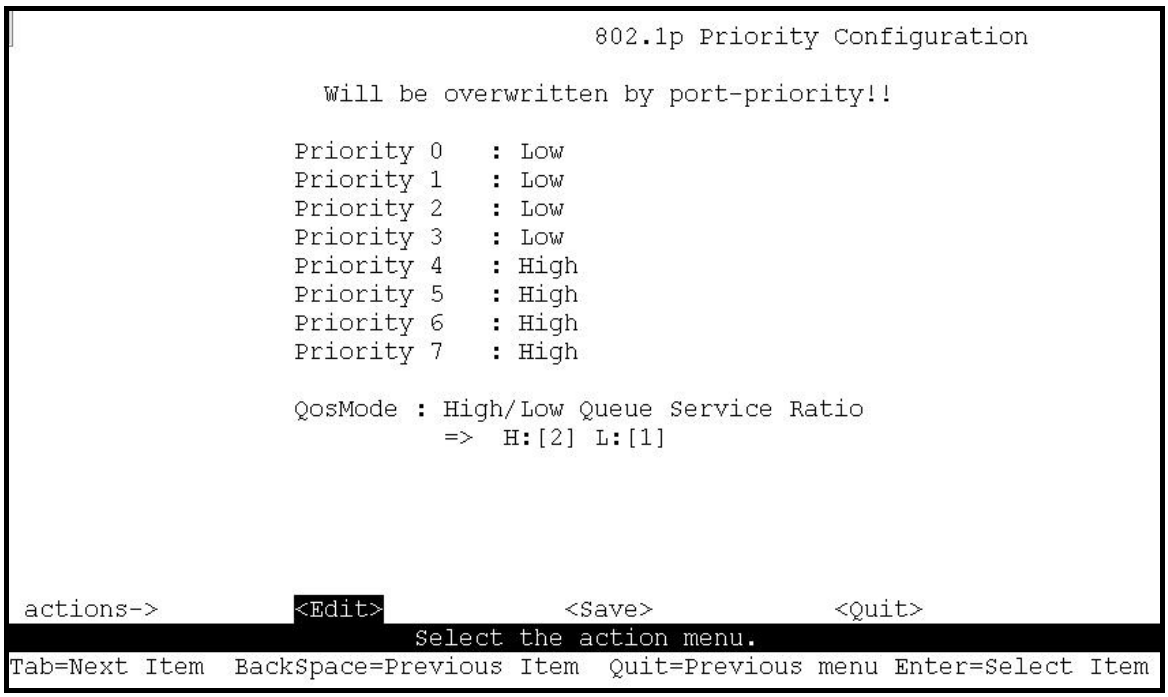
4-2-7-1. Port Static Priority

Port Priority: This is used to force any non prioritized packets to either High, Low, or Disabled states on the particular port.

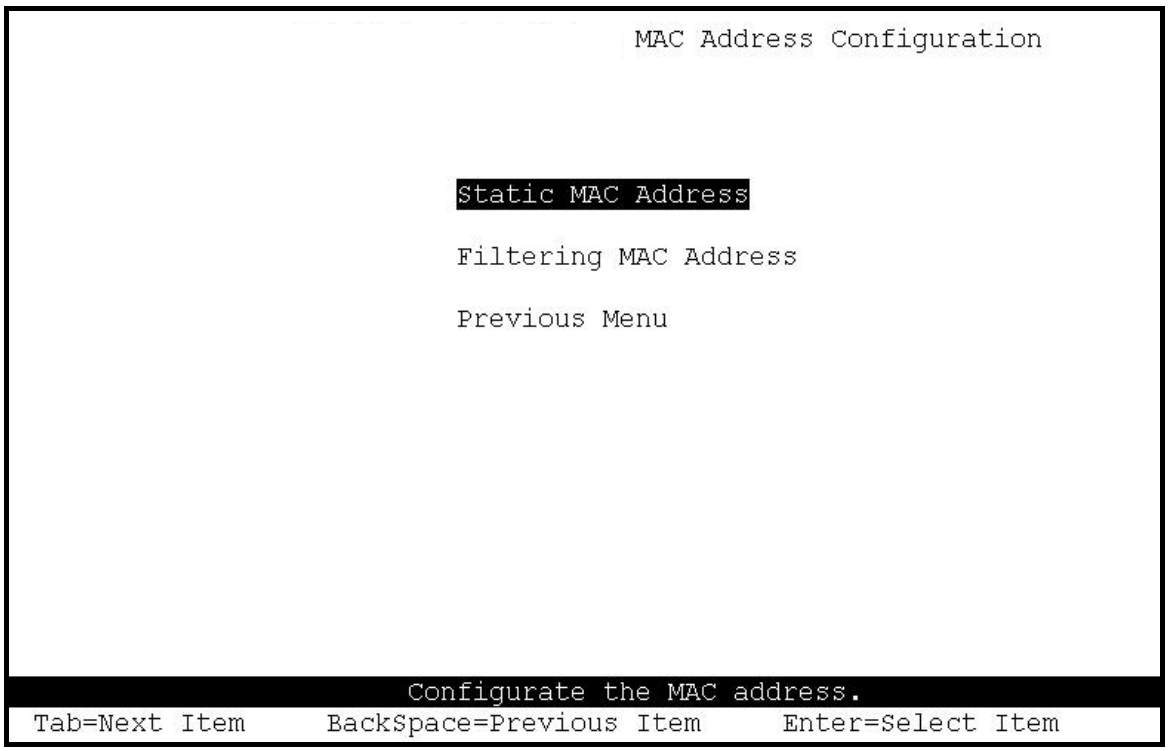


4-2-7-2. 802.1p Priority Configuration

There are 0~7-priority levels that can be mapped to either the high or low queues.
QosMode Options: First Come First Served, All High before Low, High/Low Queue Service Ratio.
The “High/Low Queue Service Ratio” enables the switch administrator to determine the ratio of high priority packets sent against low priority packets.

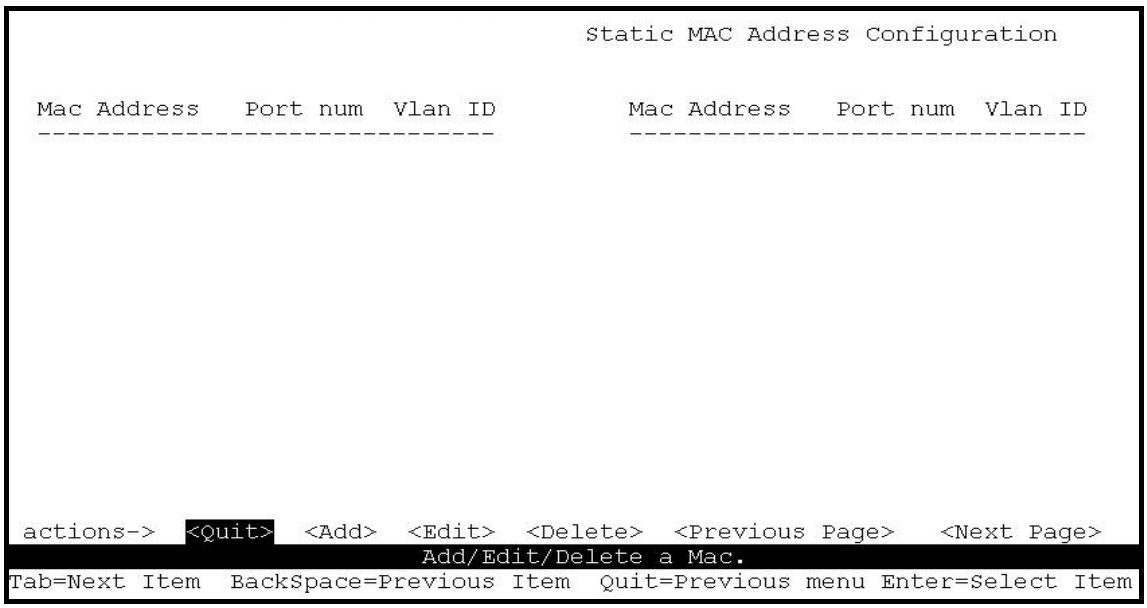


4-2-8. MAC Address Configuration



4-2-8-1. Static MAC Address

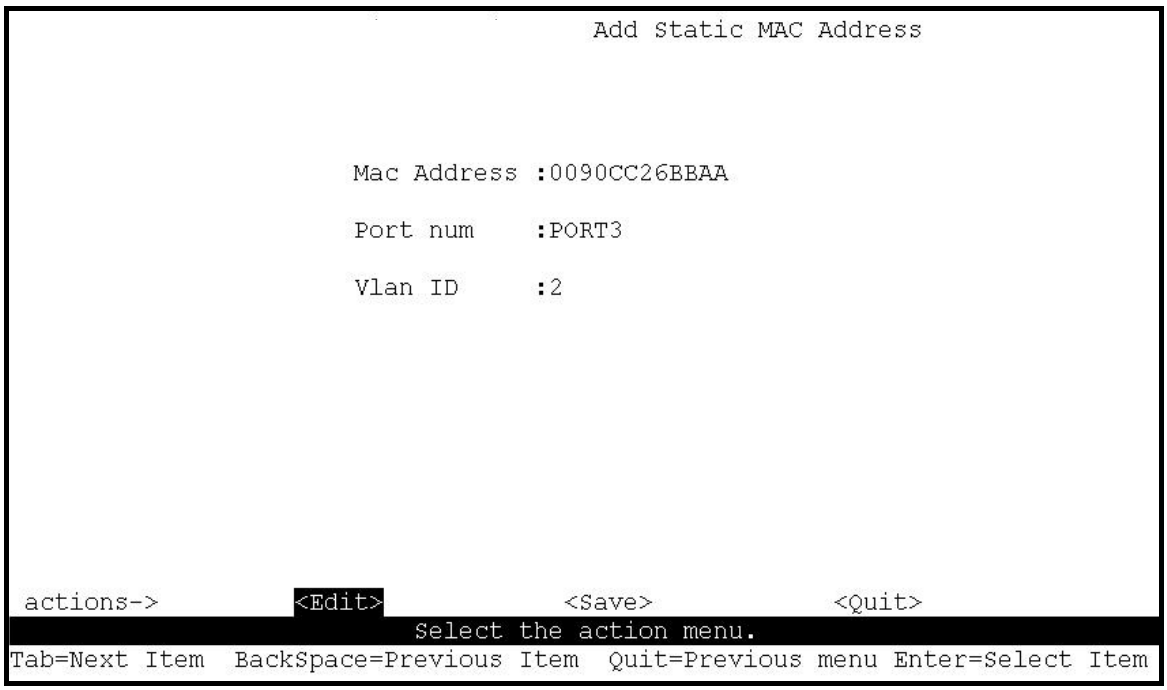
When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address after it has been disconnected or powered-off from the network, and then reconnected at some time later.



●Add static MAC address

Actions->

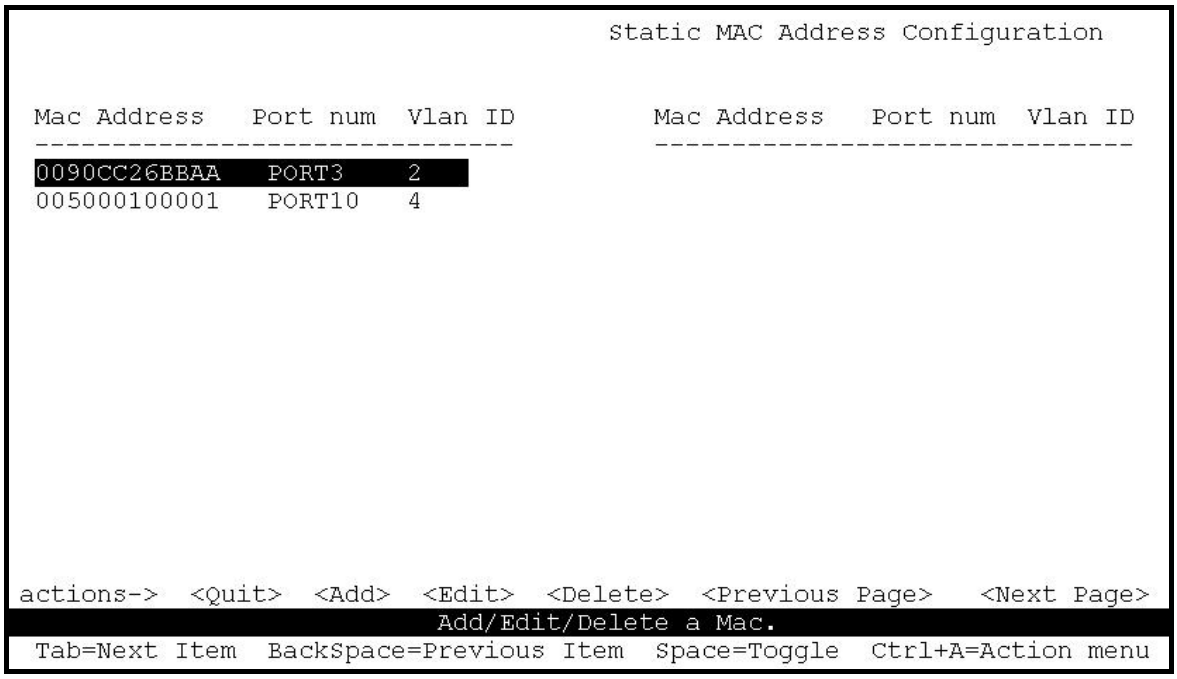
1. In the MAC address box, enter the MAC address to and from which the port should permanently forward traffic, regardless of the device's network state.
2. Press the Space key to select the Port Number
3. If tag-based (IEEE 802.1Q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) to associate with the MAC address.

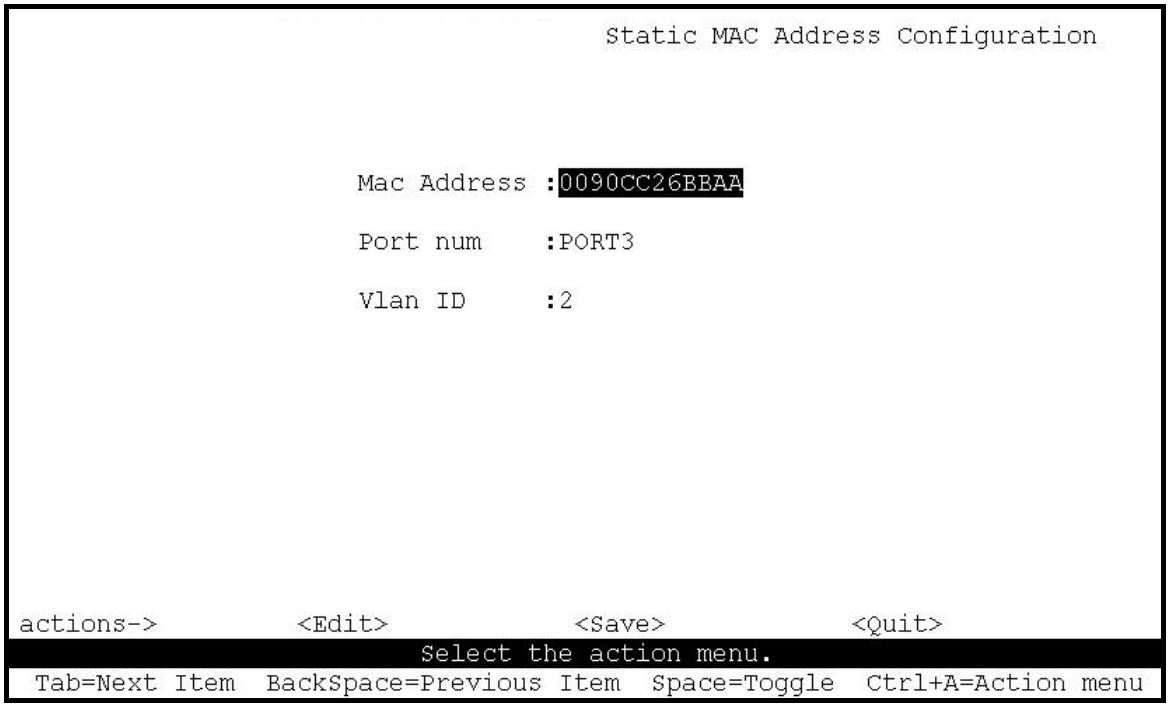


●Edit static MAC address

Actions->

1. Press **<Edit>** key.
2. Choose the MAC address that you want to modify and then press enter.

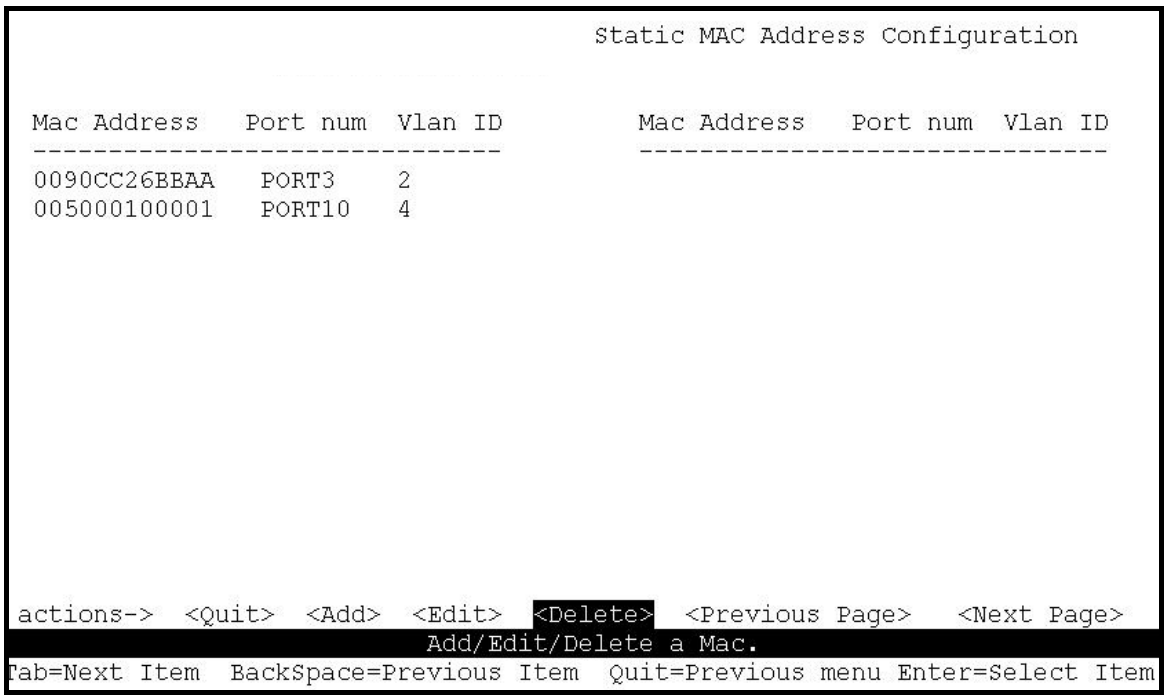




●Delete static MAC address

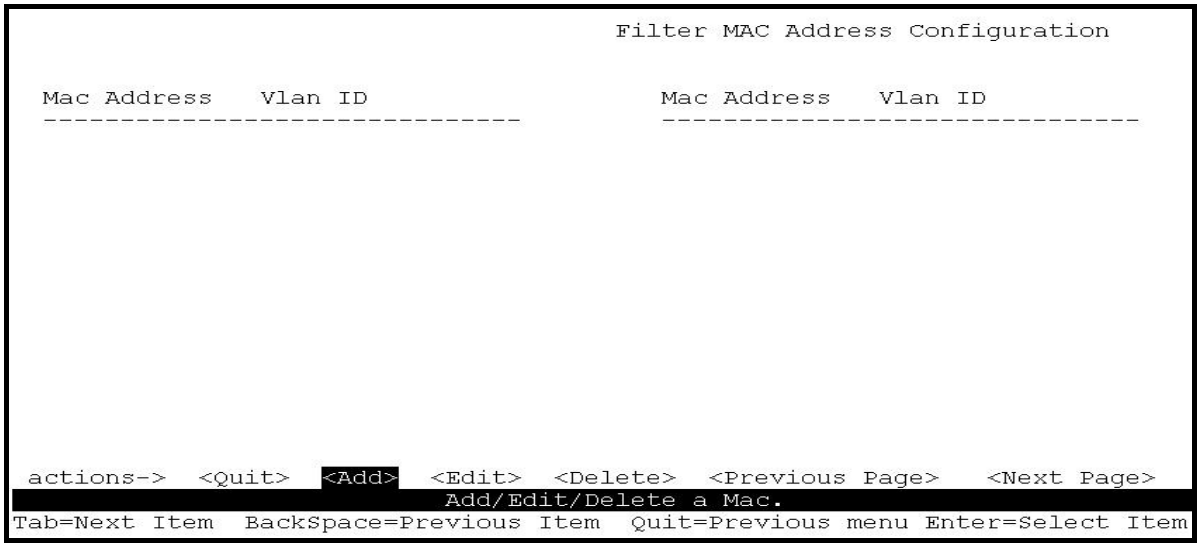
Actions->

1. Select the **<Delete>** action.
2. Choose the MAC address that you want to delete and then press enter.


Static MAC Address Configuration
Mac Address Port num Vlan ID
Mac Address Port num Vlan ID
0090CC26BBAA PORT3 2
005000100001 PORT10 4
actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

4-2-8-2. Filtering MAC Address

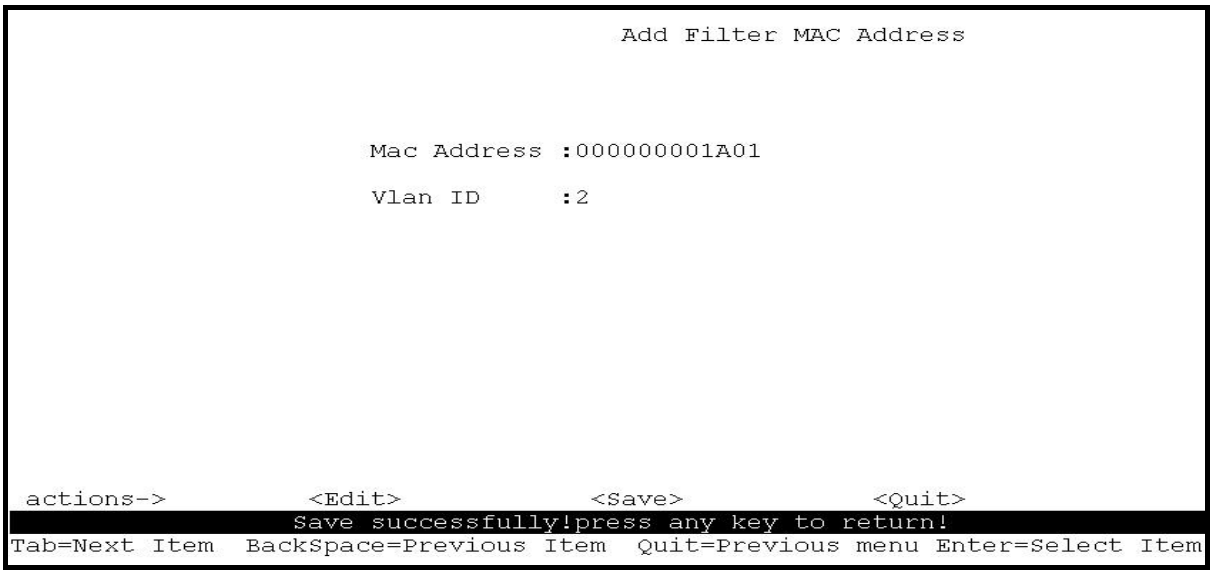
MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses.
This page allows the administrator to add, modify or delete MAC address filters.



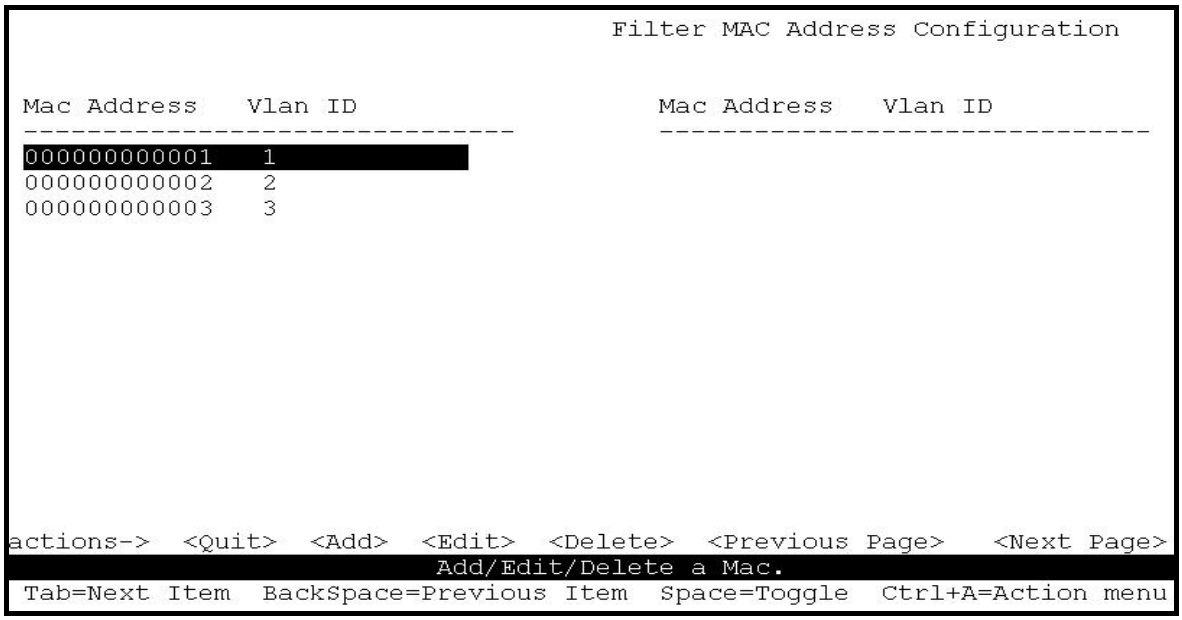
● **Add filter MAC address**

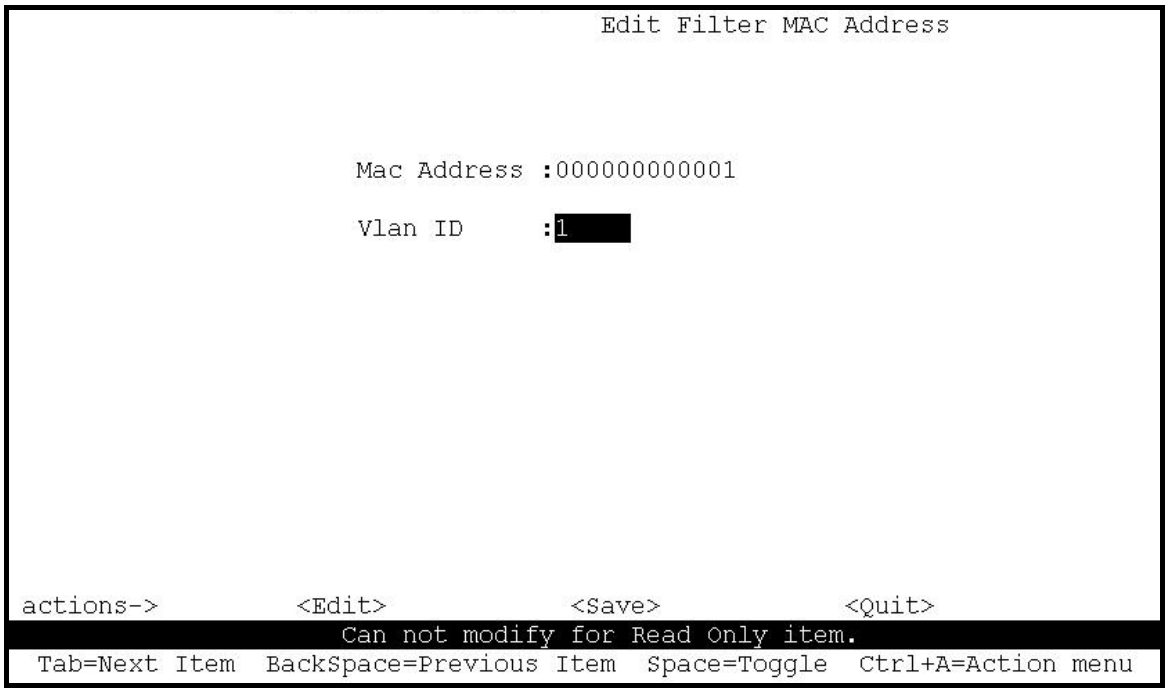
Actions->

1. Press **<Add> --> <Edit>** key to add a filtered MAC address.
2. **MAC Address:** Type the MAC address to filter.
3. **Vlan ID:** If tag-based (802.1Q) VLAN's are set up on the switch, type the VID to associate with the MAC address.



●Edit filter MAC address

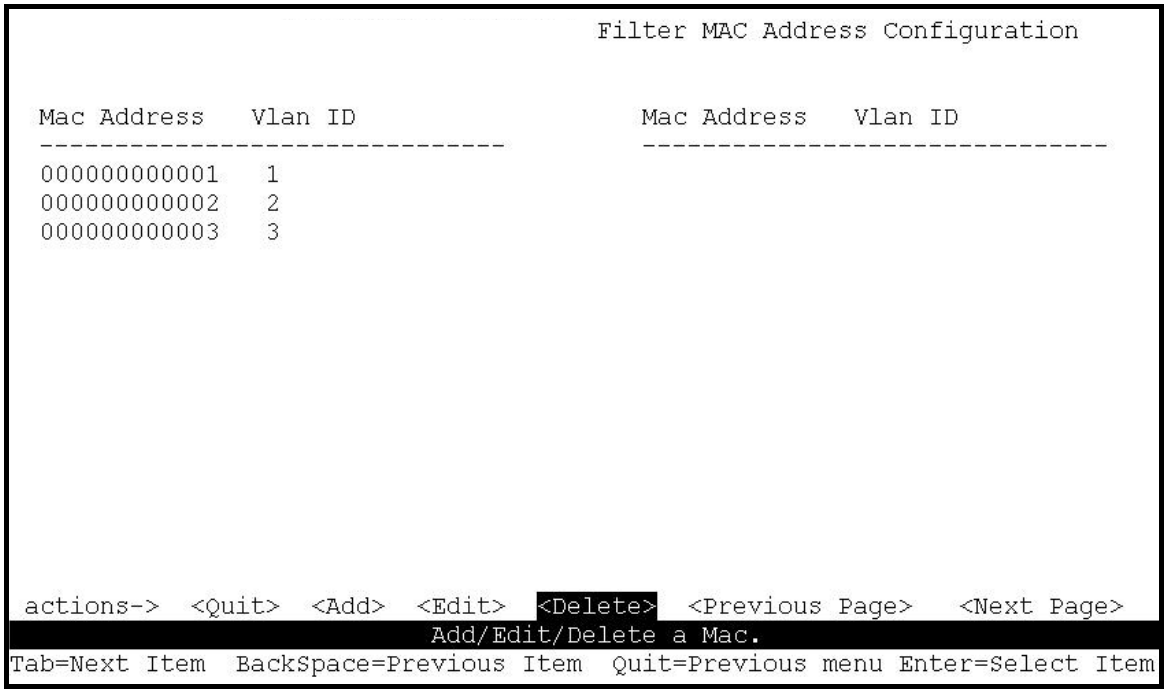




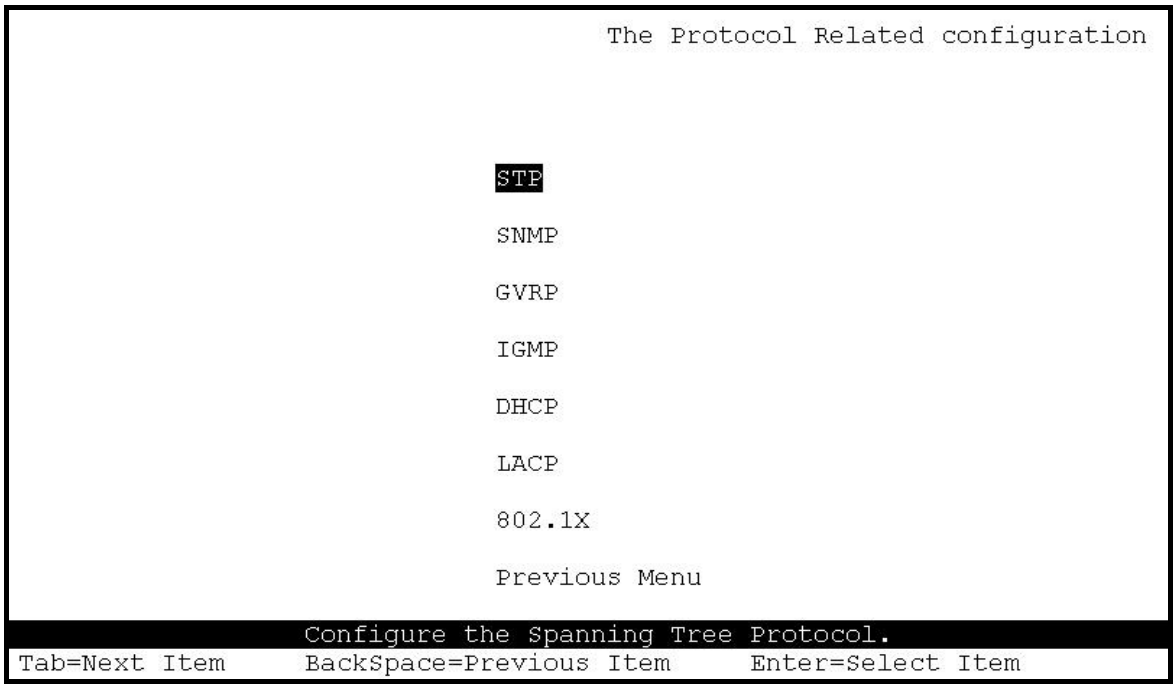
●**Delete filter MAC address**

Actions->

1. Press **<Delete>** key to delete a filter MAC address.
2. Choose the MAC address that you want to delete and then press enter.
3. Pressing **<Enter>** once will complete deletion.

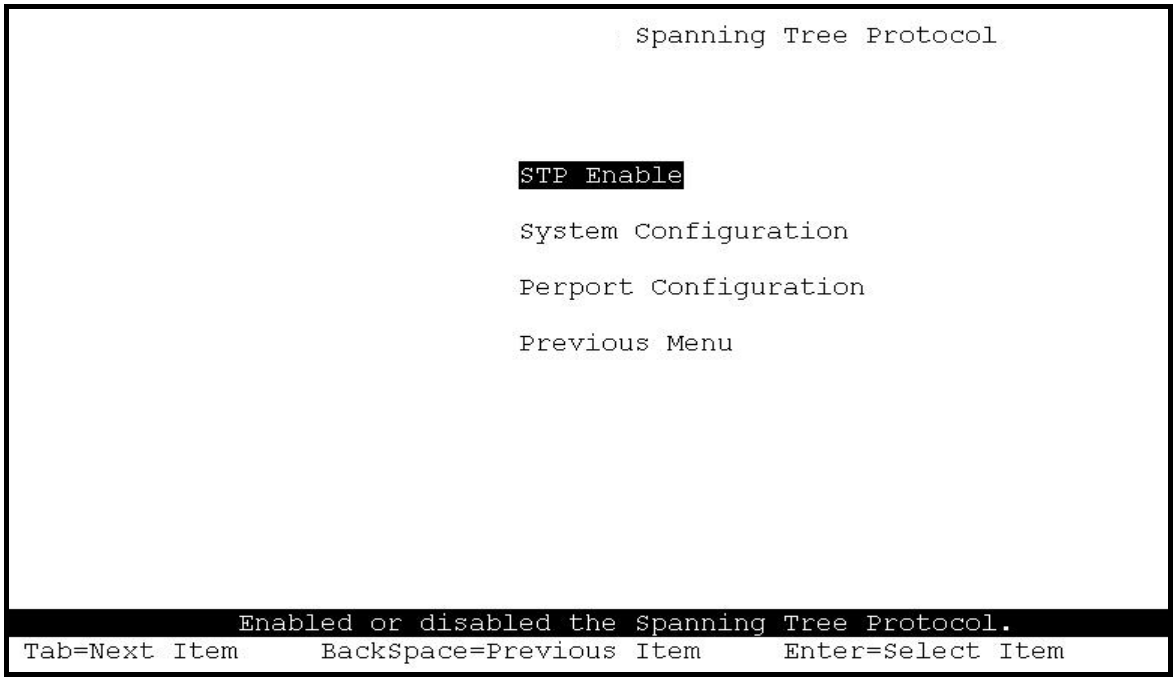


4-3. Protocol Related Configuration



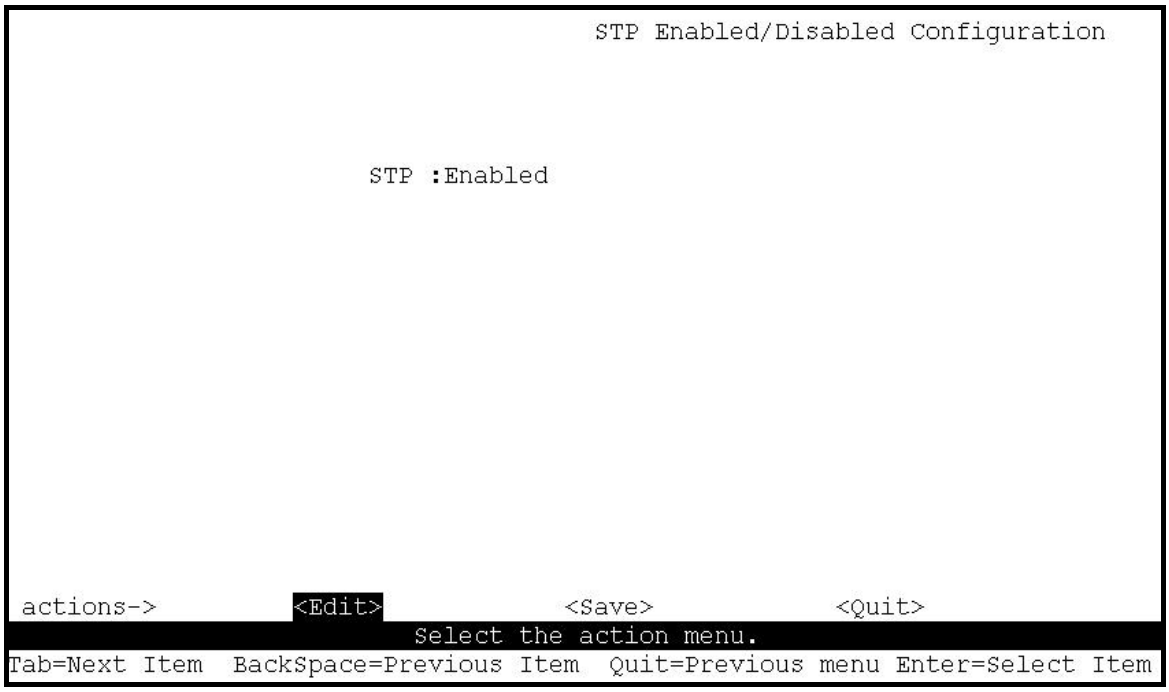
4-3-1. RSTP

The Rapid Spanning-Tree Protocol (RSTP) is a standardized method (IEEE 802.1w) for avoiding loops in switched networks. You would enable RSTP to ensure that only one path at a time is active between any two nodes on the network.

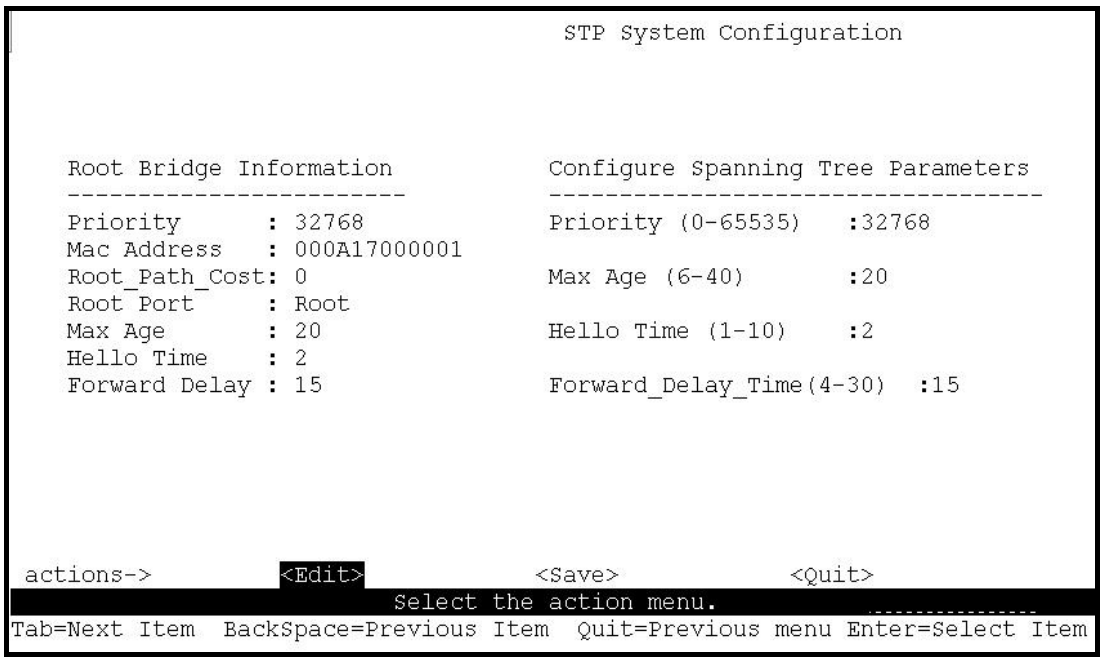


4-3-1-1. RSTP Enable

This page shows how to enable or disable Spanning Tree function.
Press the **Space** key to enable or disable RSTP.



4-3-1-2. RSTP System Configuration

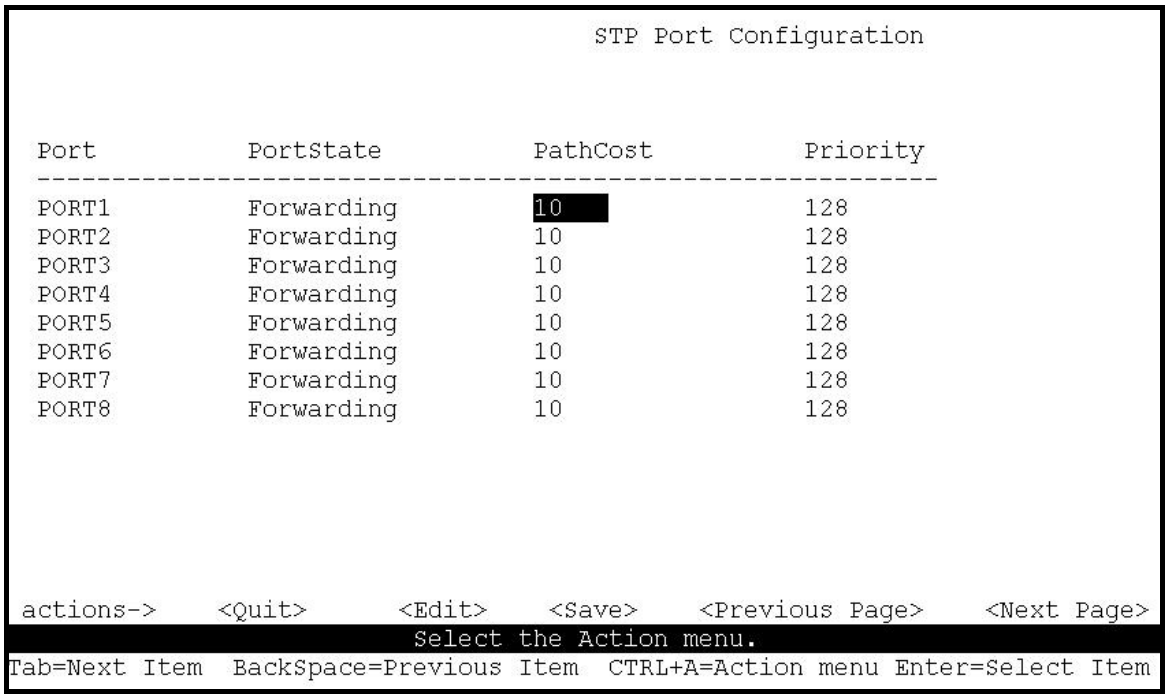


Actions->

1. Root Bridge information is displayed on the Left.
2. Parameters can be defined on the Right.

NOTE: The parameters are described in more detail in *sections 2-4-8.*

4-3-1-3. Perport Configuration



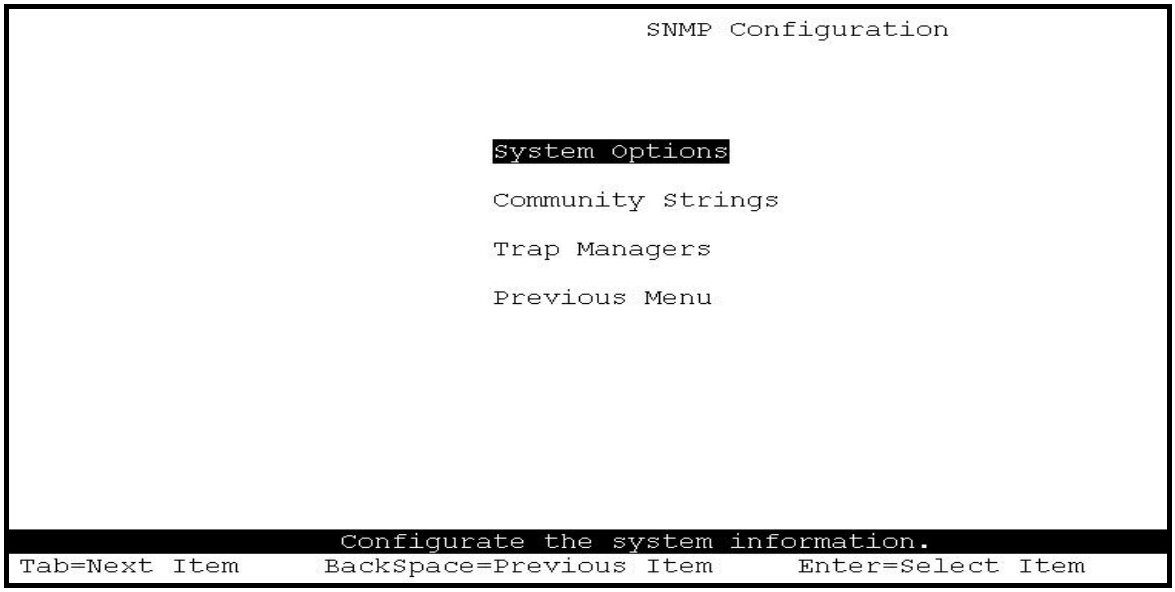
Actions->

1. **PortState:** Displays the spanning tree status for each port. Forwarding or Blocking.
2. **PathCost:** Specifies the path cost for the port. This is used in determining which ports are used as forwarding ports.
3. **Priority:** This defines the port priority. Low values are more likely to become the root port.

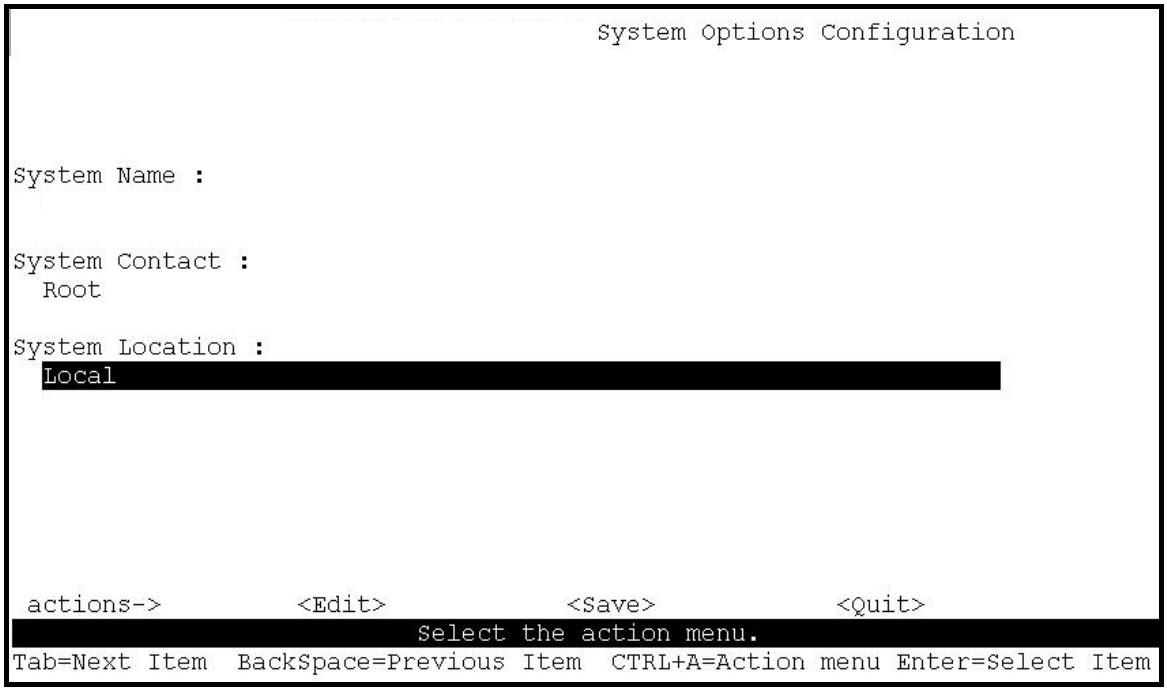
NOTE: The above parameters are described in *sections 2-4-8.*

4-3-2. SNMP

The ESM-24T02M can be managed from any Simple Network Management Protocol (SNMP) application. If using the Management Information Base (MIB) within your SNMP application, then the information can be reported in a more intuitive manner. SNMP is a Protocol that governs the transfer of information between the management station (application) and the agent (the ESM-24T02M switch).



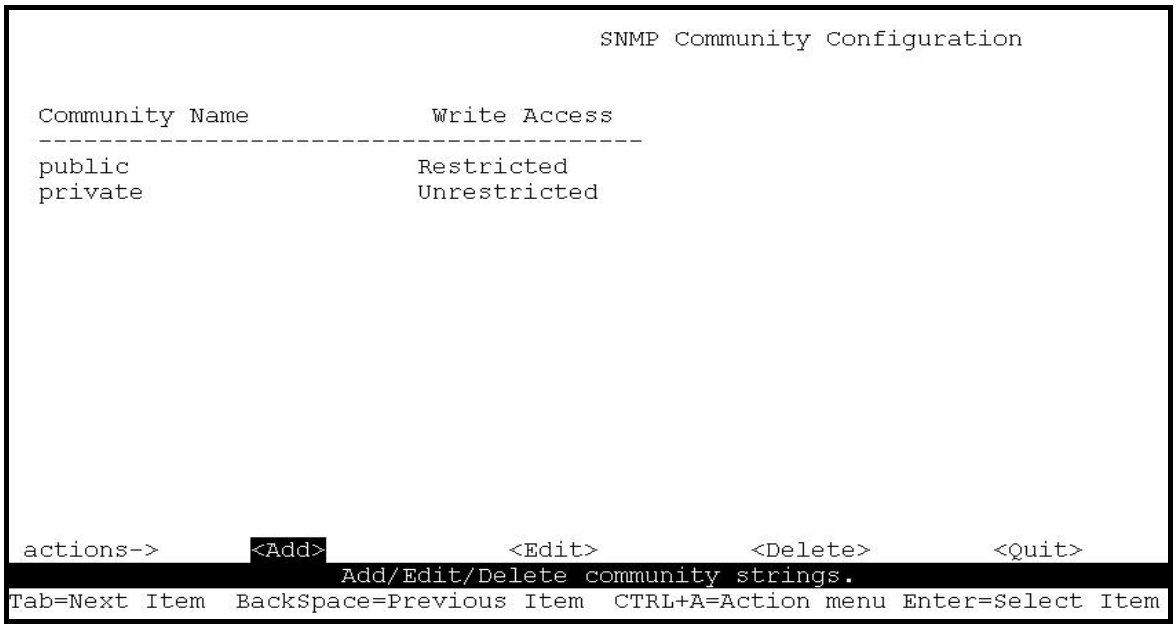
4-3-2-1. System Options



4-3-2-2. Community Strings

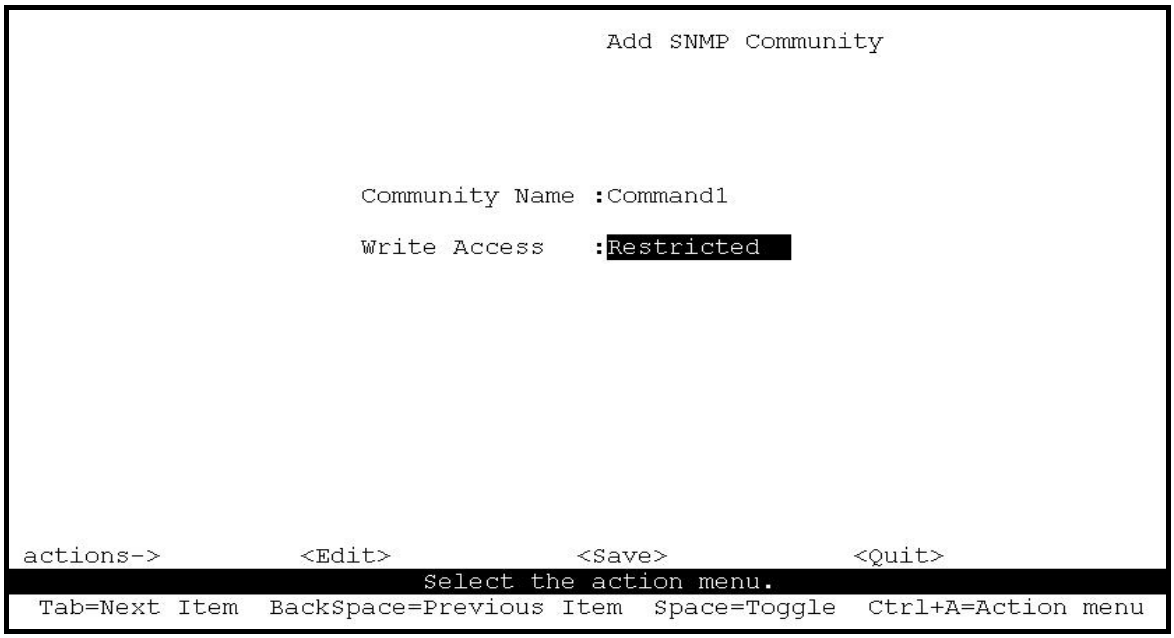
Use this page to Add/ Edit/ Delete SNMP community strings.

1. **Community Name:** The current community name strings.
2. **Write Access:** Enable read only or read-write access.
   Restricted: Read only, enables requests accompanied by this string to display MIB-object information.
   Unrestricted: Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.



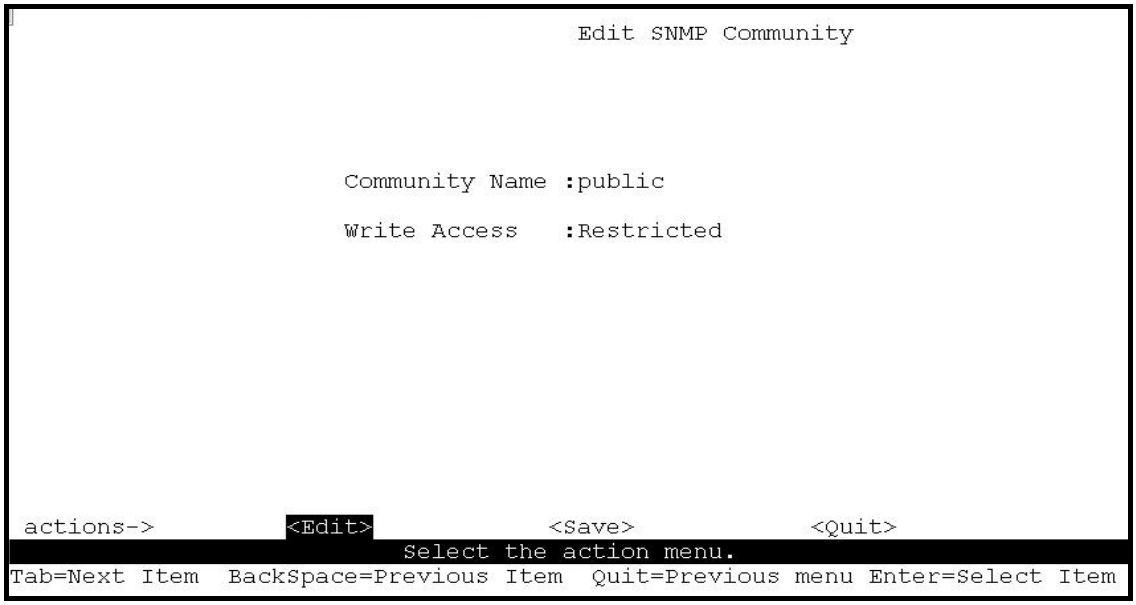
- **Add Community Name**

1. Select the **<Add> --> <Edit>** option.
2. **Community Name:** Type the community name.
3. **Write Access:** Press **Space** key to select restricted or unrestricted.

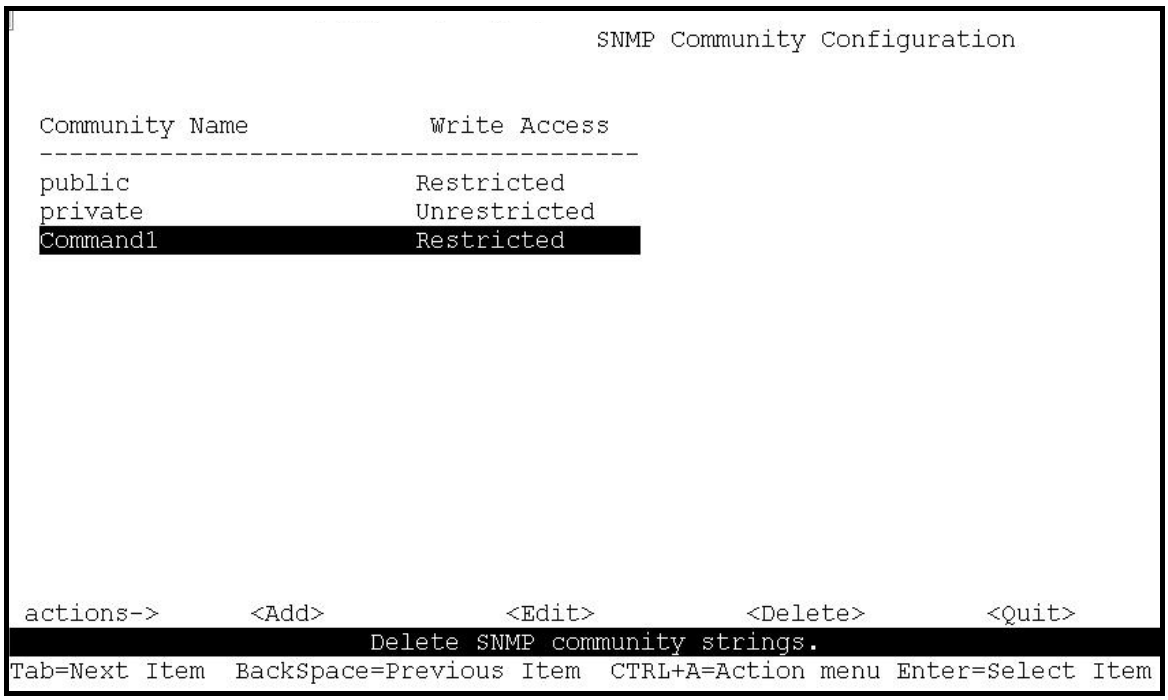


- Edit Community Name

1. Select the **<Edit>** option, choose the item that you want to modify and then press **Enter.**
2. **Community Name:** Type the new name.
3. **Write Access:** Press **<Space>** key to change the access (restricted or unrestricted)

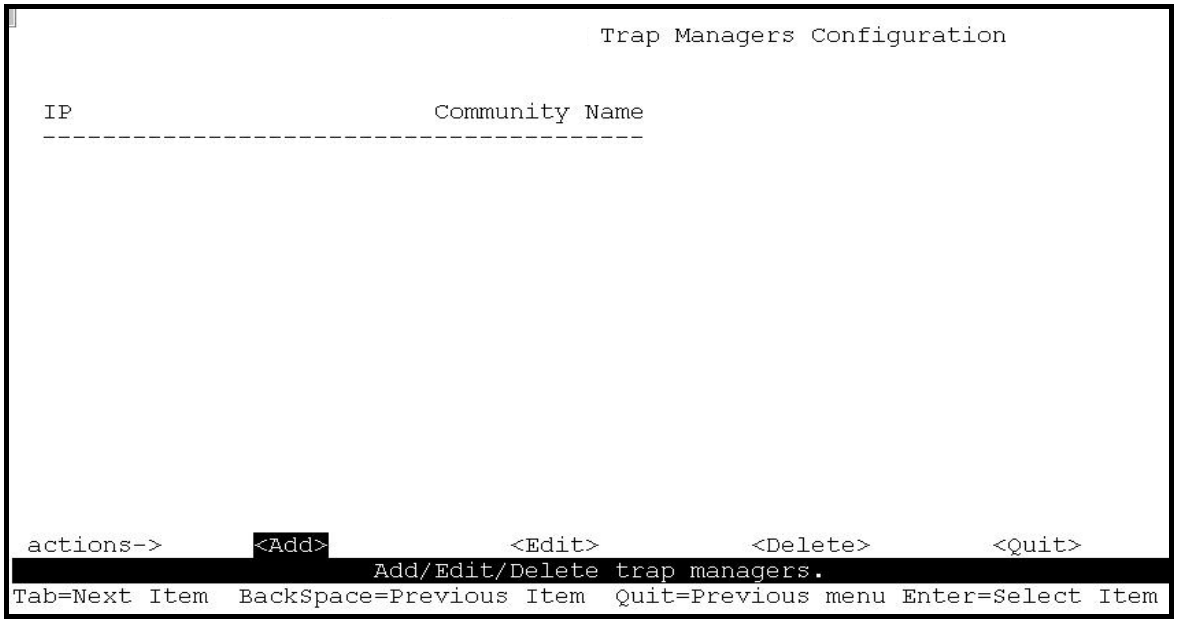


- **Delete Community Name**
  1. Select the **<Delete>** option.
  2. Choose the community name that you want to delete and then press **Enter**.



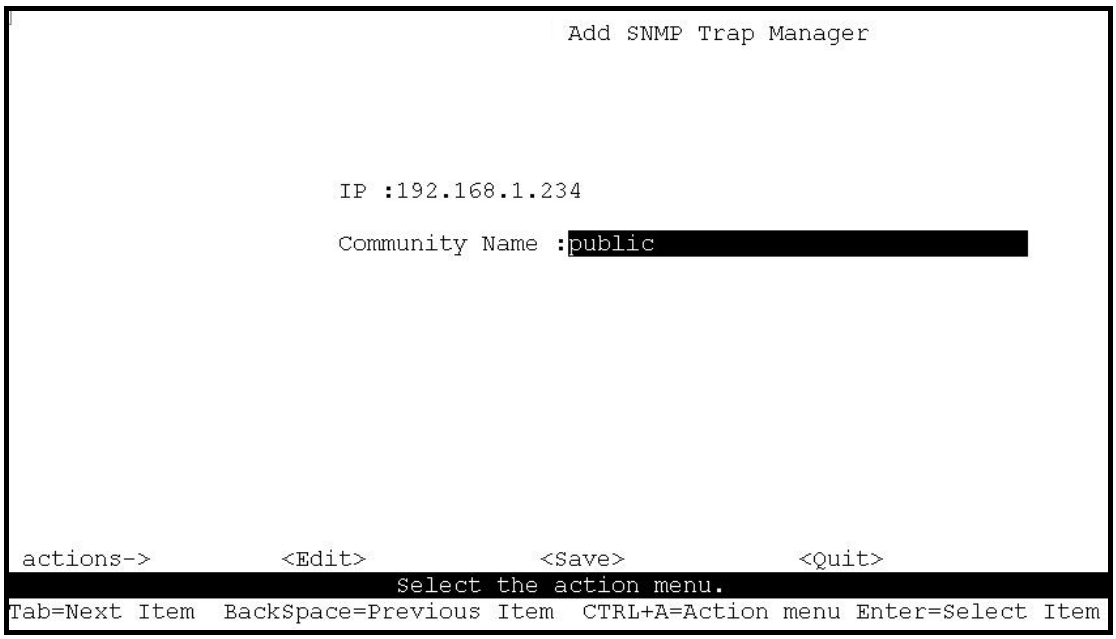
4-3-2-3. Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.



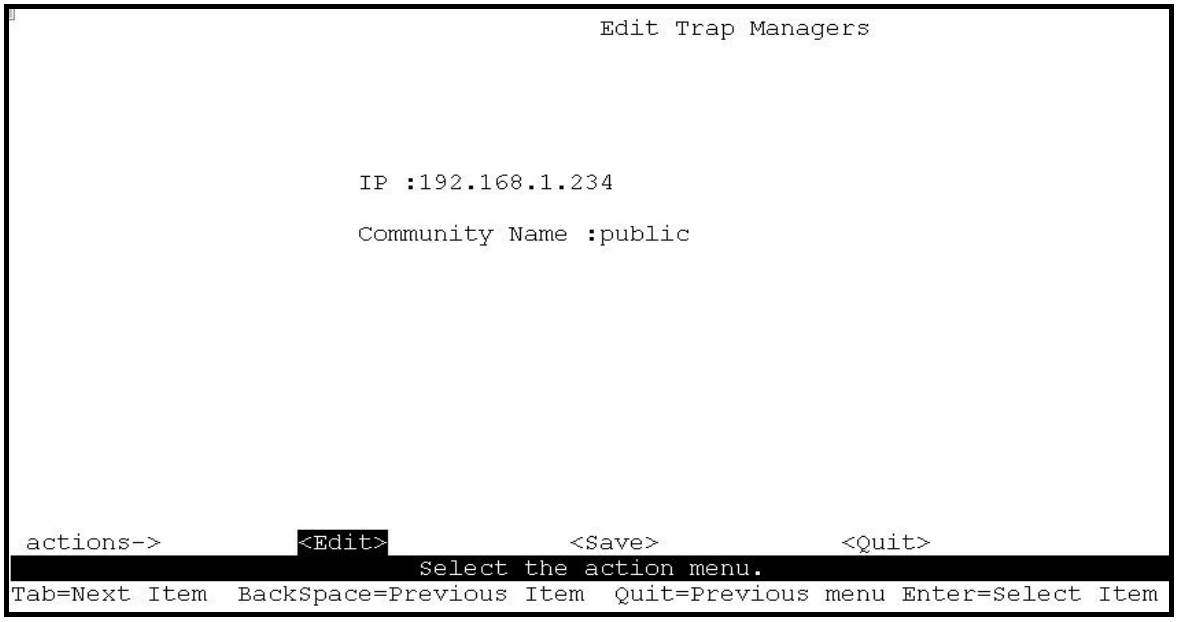
- **Add SNMP trap manager**

1. Select the **<Add> --> <Edit>** option to add a Trap Manager.
2. **IP:** Type the IP address of the Trap Manager
3. **Community Name:** Enter the community name.



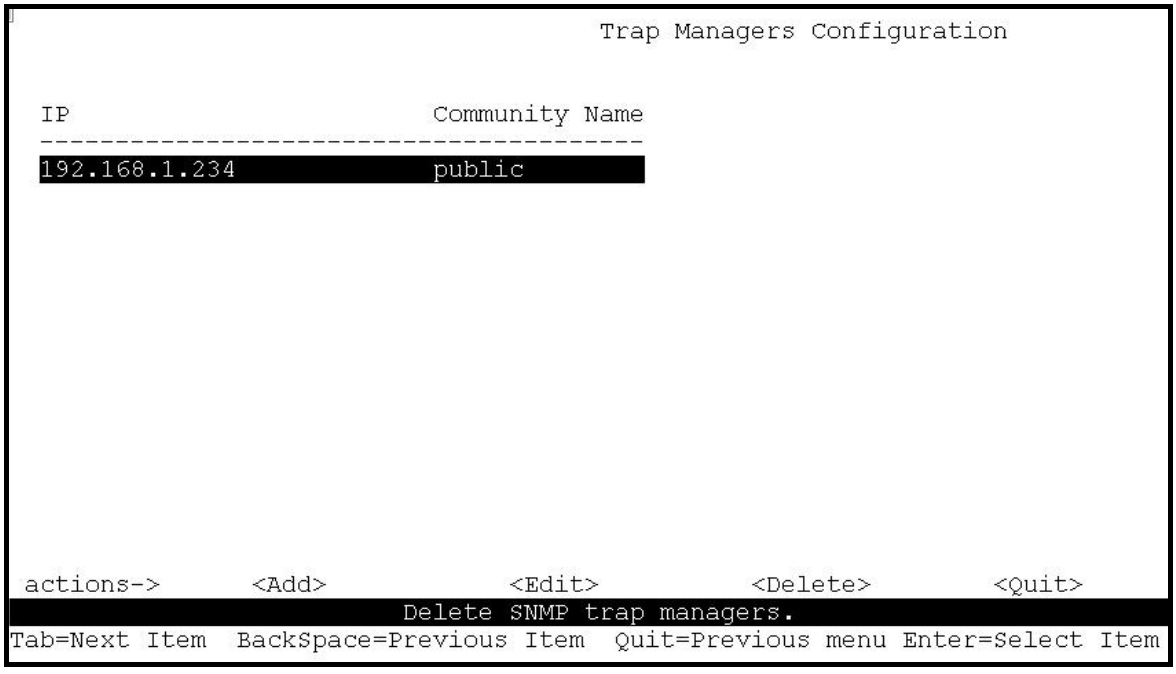
- **Edit trap managers**

1. Select the **<Edit>** option, and then choose the item that you want to modify.
2. **IP:** Type the new IP address.
3. **Community Name:** Type the community name.



- **Delete trap manager**

1. Select the **<Delete>** option.
2. Choose the trap manager that you want to delete and then press **Enter**.

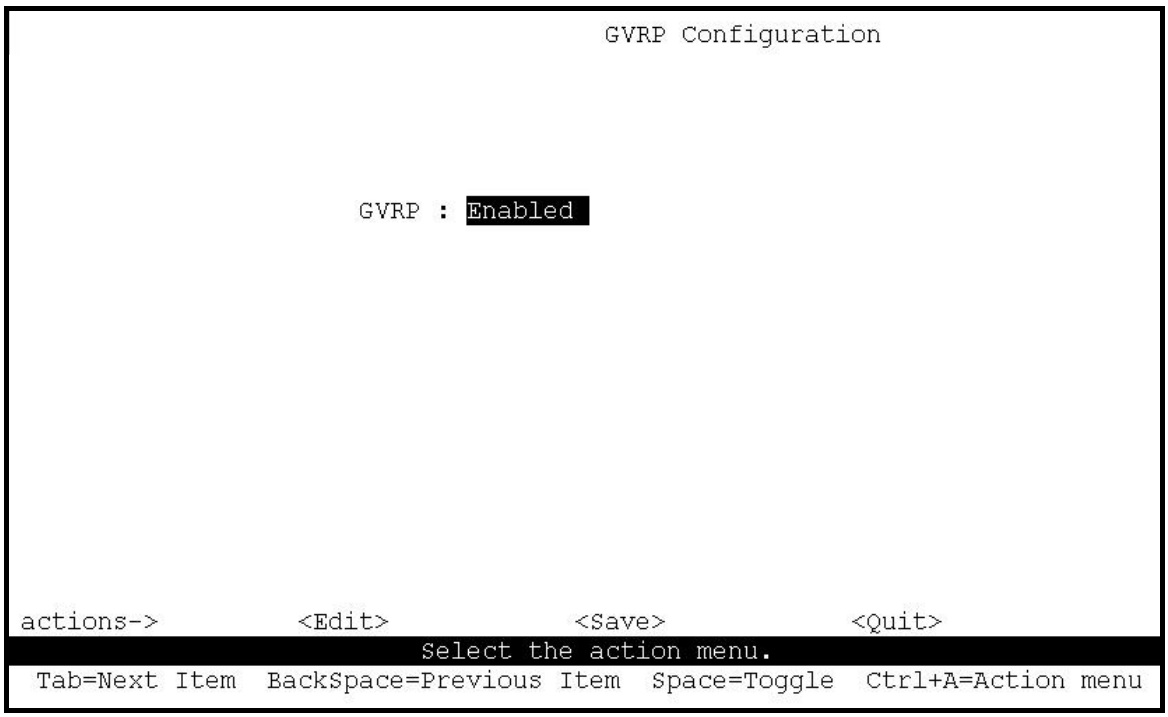


4-3-3. GVRP

GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol)

GVRP allows automatic VLAN configuration between the switch and its nodes. If the switch is connected to a device with GVRP support, then a GVRP request can be issued from the device to the switch using a valid VID of a VLAN defined on the switch. The switch will then automatically add the device to the existing VLAN entries.

From this page you can enable or disable the GVRP (GARP VLAN Registration Protocol) support.

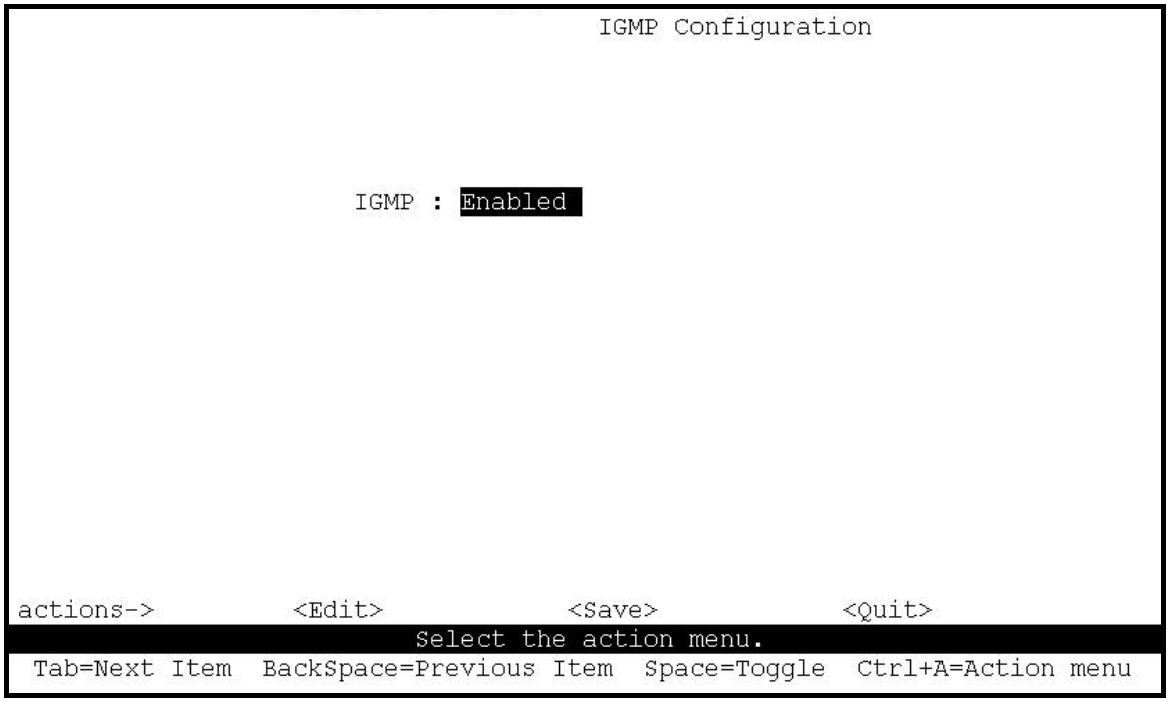


Note: GVRP must also be enabled on participating network nodes.

4-3-4. IGMP

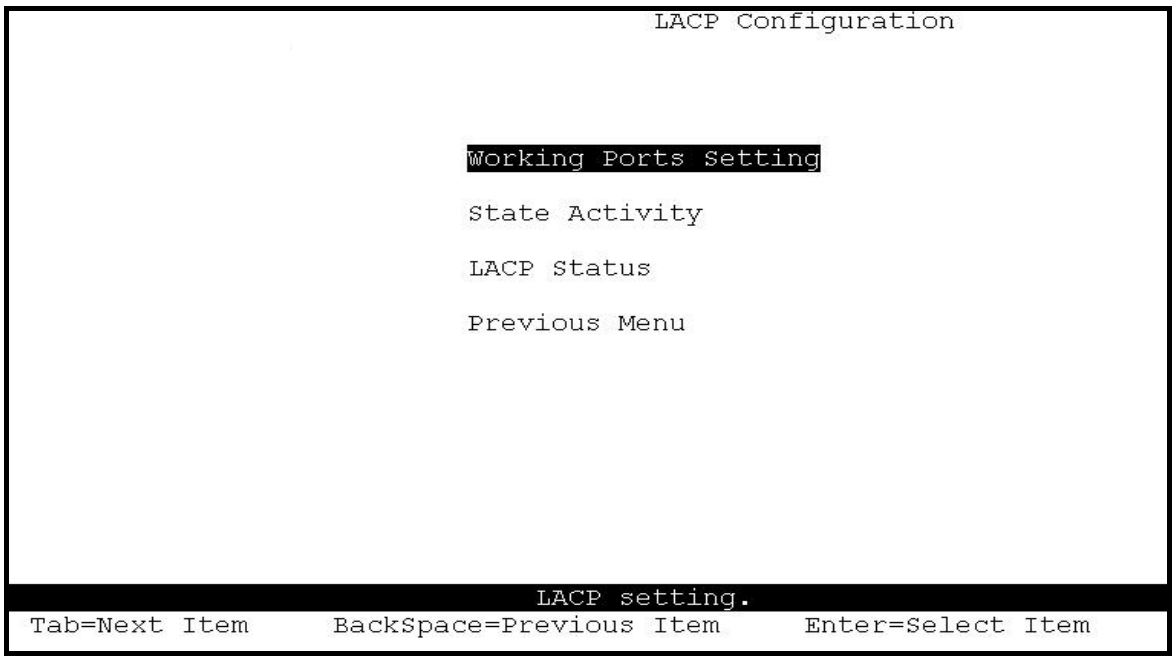
The ESM-24T02M switch supports IP multicasting via the IGMP protocol. Administrators can enable IGMP and then display the IGMP snooping information. Multicast groups, VID and member port information.

This page allows administrators to enable or disable the IGMP support.



4-3-5. LACP (Link Aggregation Control Protocol)

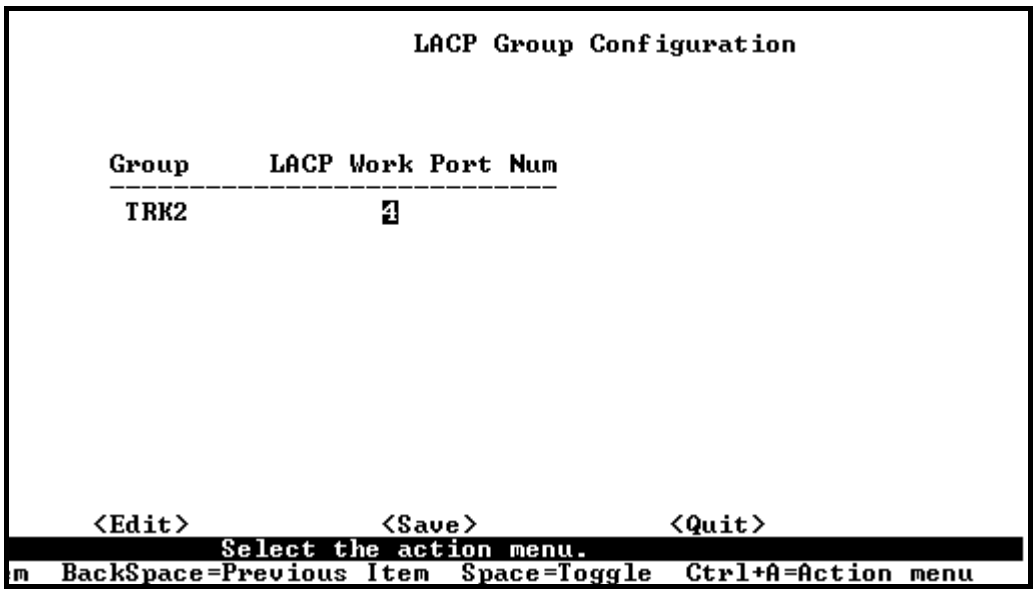
Use this page to configure and view all the LACP parameters.



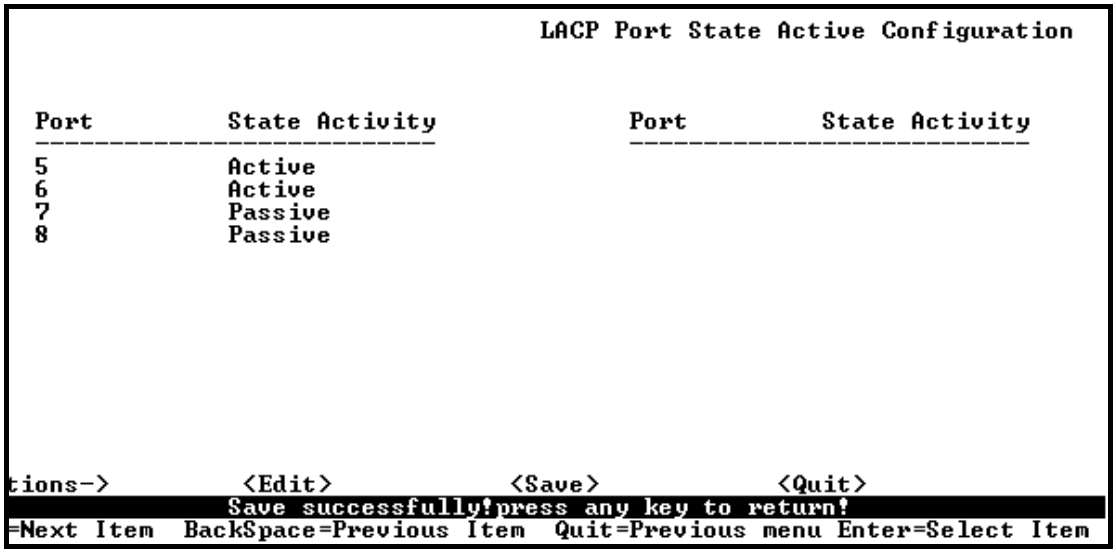
Note: All ports support LACP dynamic trunking. If connecting to a device that also supports LACP, the LACP dynamic trunking function will automatically create a trunk group.

4-3-5-1. Working Port Setting

Use this page to set the ports in trunk group.



4-3-5-2. State Activity



Active: The port automatically sends LACP protocol packets.

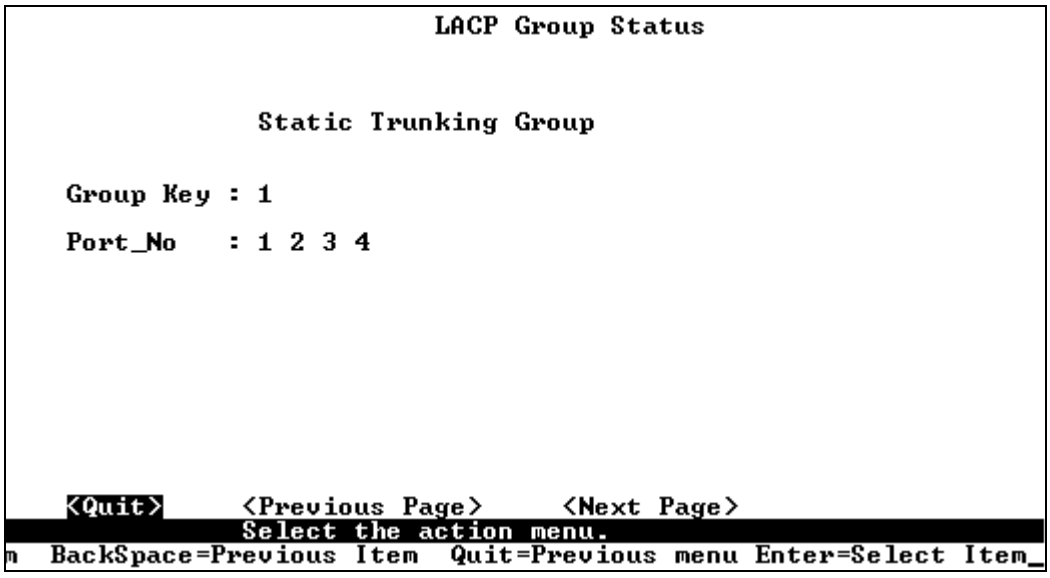
Passive: The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from a connected device.

NOTE: If LACP mode is configured in the trunk group, all of the member ports of this trunk group will be set "Active" automatically.

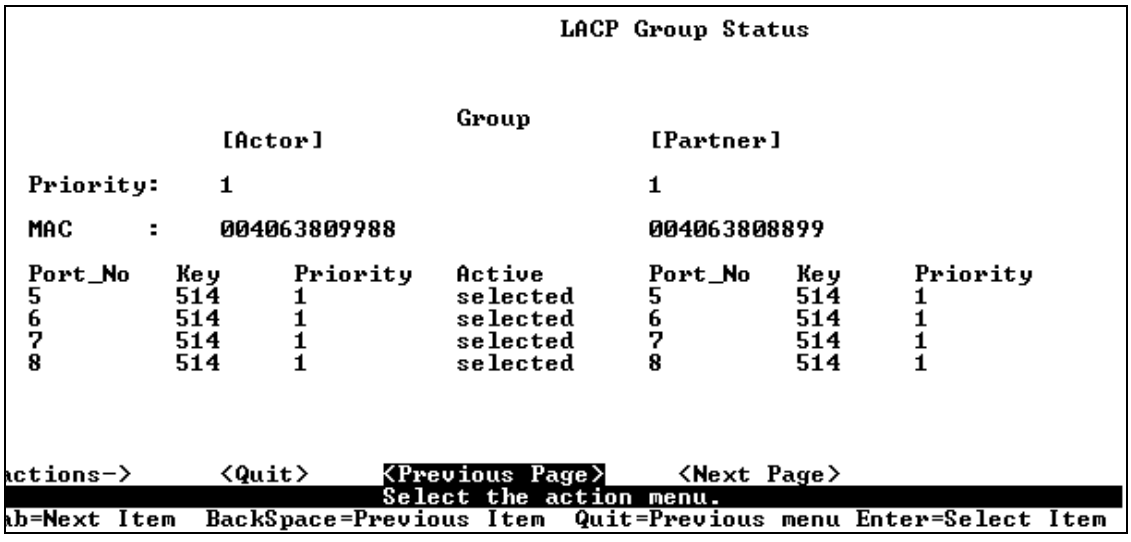
4-3-5-3. LACP Status

From this screen you can view the current trunking group status.

Static trunk group

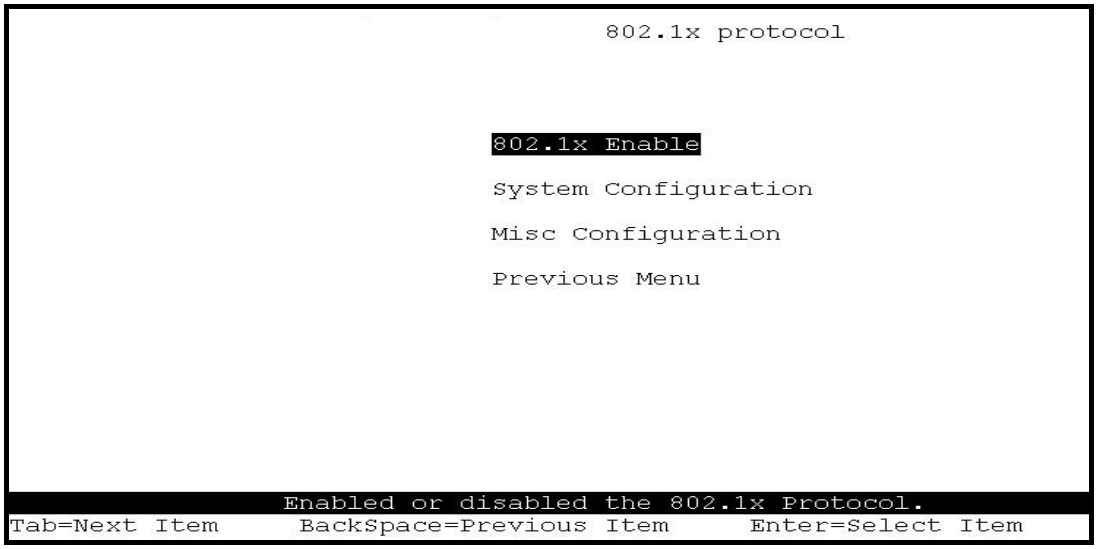


LACP trunk group

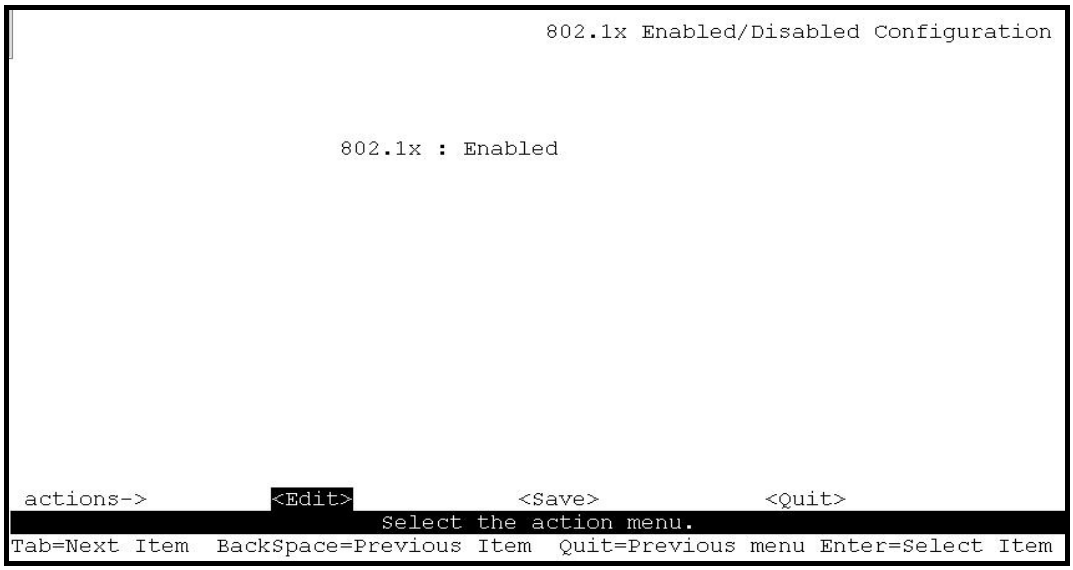


4-3-6. 802.1x Protocol

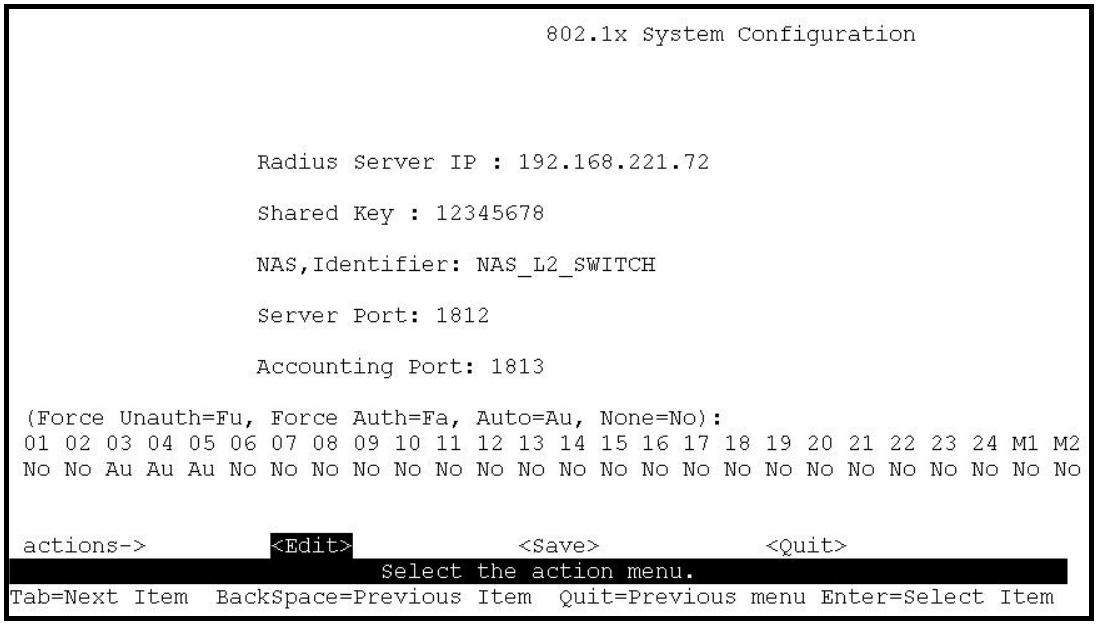
From this page administrators can configure and view all 802.1x parameters.



4-3-6-1. 802.1x Enable



4-3-6-2. 802.1x System Configuration



1.**Radius Server IP Address:** the IP address of the authentication server.

2.**Shared Key:** A key shared between this switch and authentication server.

3.**NAS, Identifier:** A string used to identify this switch.

4.**Server Port:** The UDP port number used by the authentication server.

5.**Accounting Port:** The UDP port number used by the authentication server to retrieve accounting information.

Note:

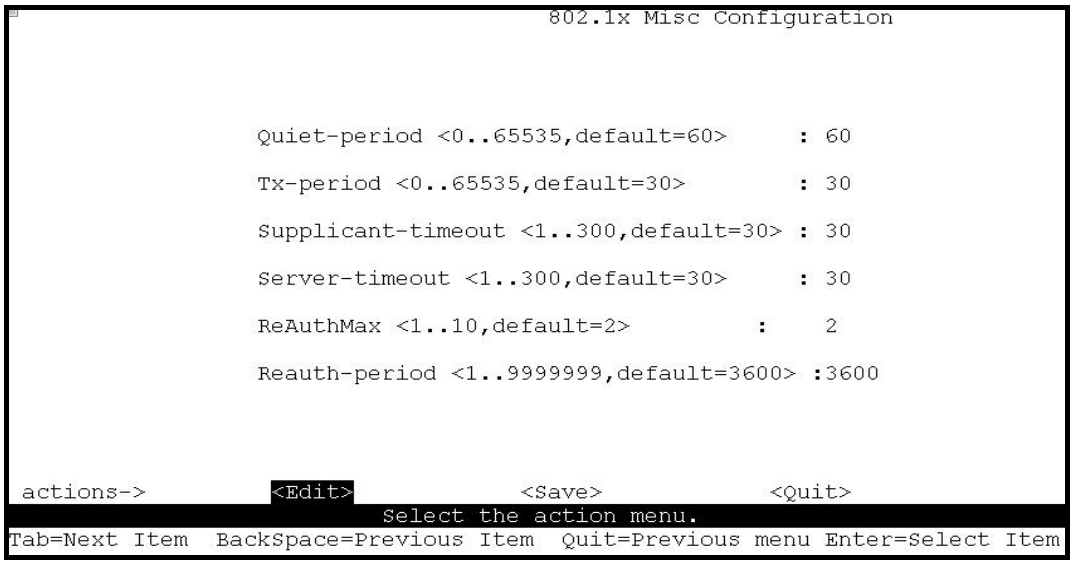
Fu Force the specific port to be unauthorized.

Fa Force the specific port to be authorized.

Au The state of the specific port is determined by the outcome of the authentication.

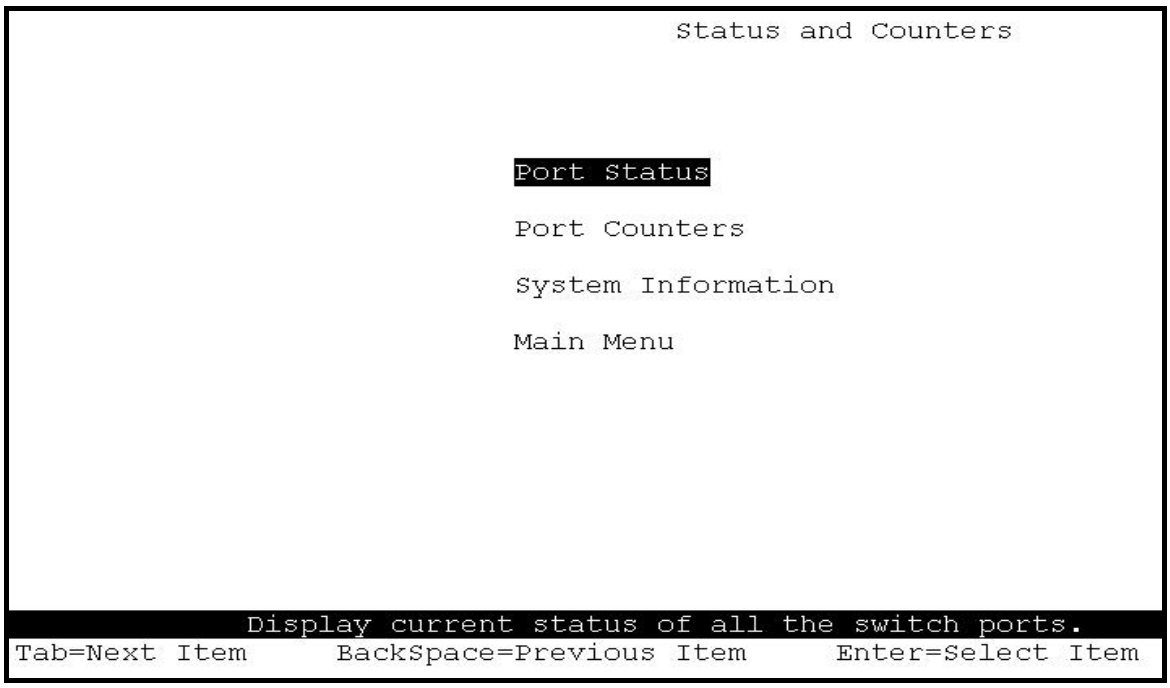
No The specific port does not support 802.1x functions.

4-3-6-3. 802.1x Misc Configuration



1. **Quiet Period:** Used to define periods of time during which it will not attempt to acquire a supplicant (Default time is 60 seconds).
2. **Tx Period:** Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
3. **Supplicant Timeout:** Used to determine timeout conditions in the exchanges between the supplicant and authentication server (Default value is 30 seconds).
4. **Server Timeout:** Used to determine timeout conditions in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
5. **ReAuthMax:** Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
6. **Reauth Period:** Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (Default value is 3600 seconds).

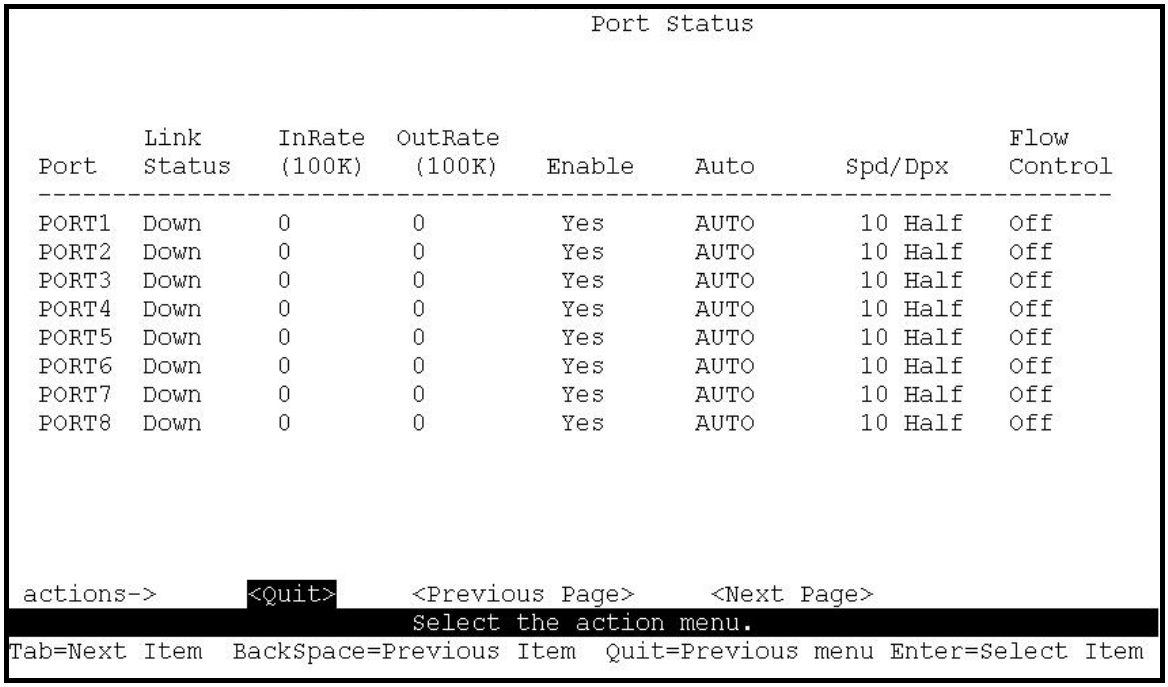
4-4. Status and Counters



.

4-4-1. Port Status

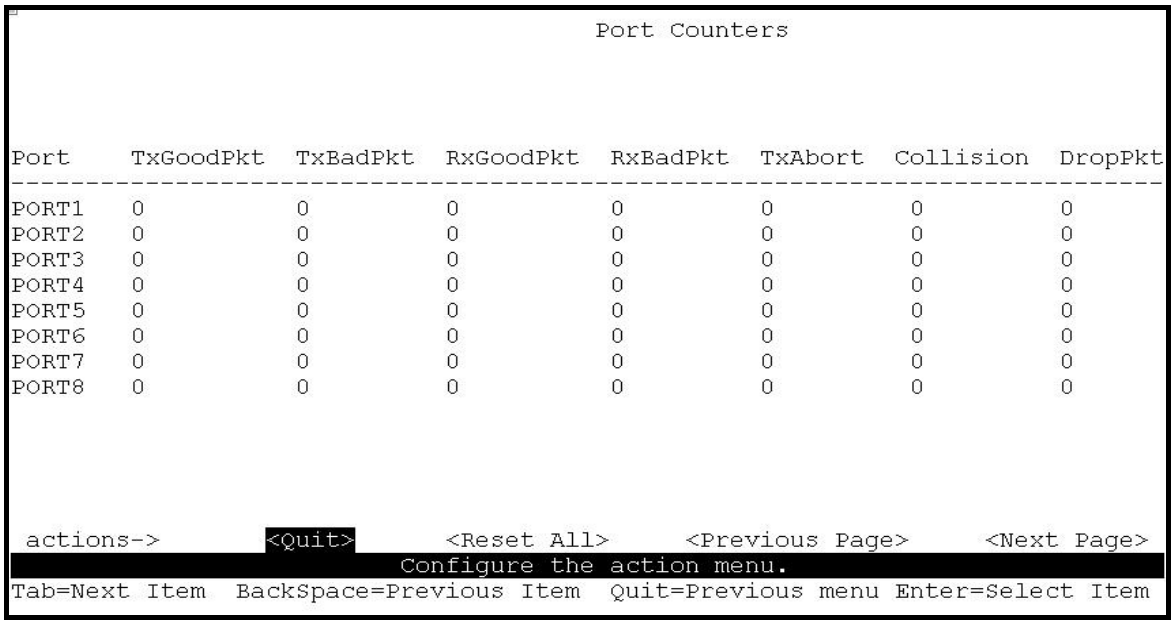
This page displays port status information.



Link Status: Down indicates “No Link”, Up indicates “Link”.
InRate: Display the input rate control (100K/unit) value.
OutRate: Display the output rate control (100K/unit) value.
Enabled: Display port status Yes or No, No indicates port is disabled.
Auto: Display which mode the port is auto-negotiated with: Auto/Forced/Nway-forced.
Spd/Dpx: Display the port speed and duplex.
FlowCtrl: In Auto or Nway modes, display the flow control status after negotiation. In Forced mode, the flow control status is enabled or disabled based on the switch configured setting.

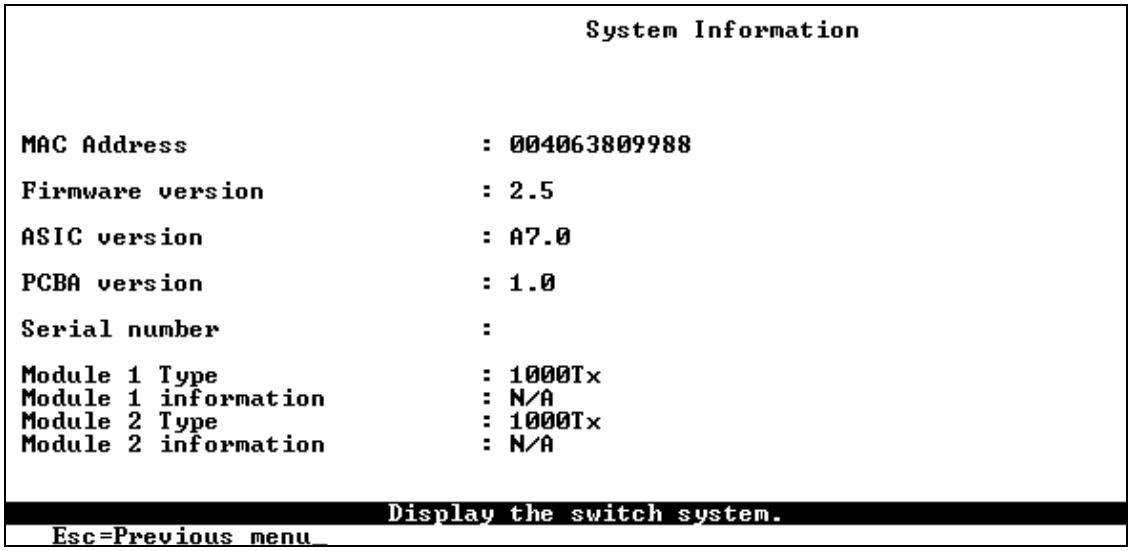
4-4-2. Port Counters

The following view provides statistical information about the switch.

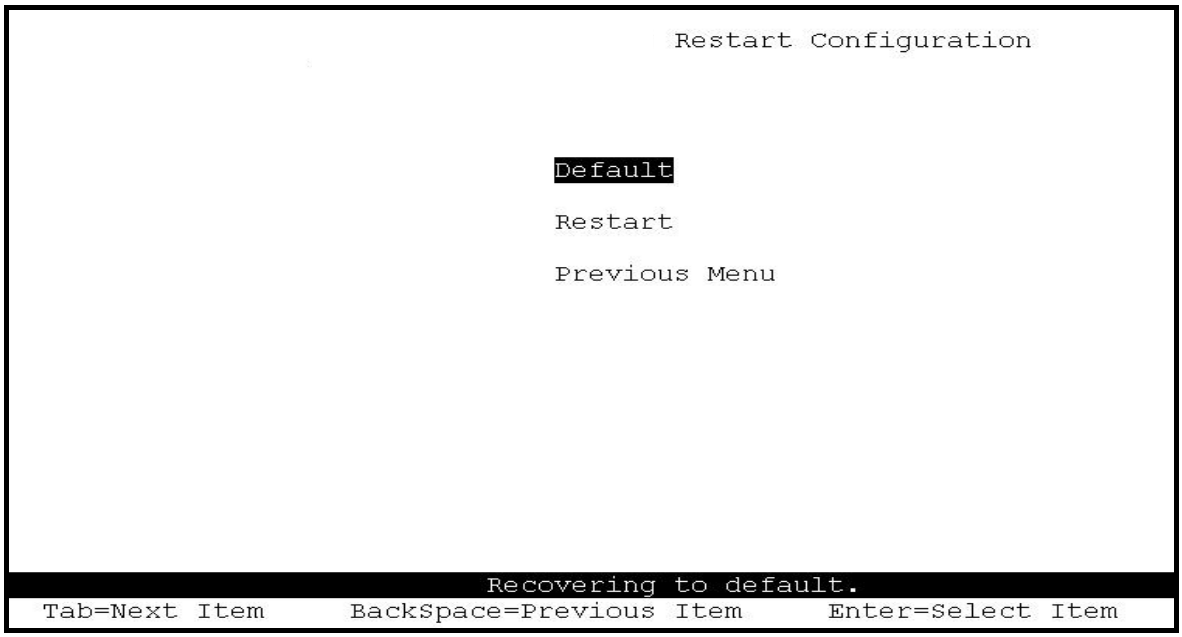


4-4-3. System Information

MAC Address: The unique hardware address (MAC).
Firmware Version: Display the switch's firmware version.
ASIC Version: Display the switch's Hardware version.
PCBA version: Display the switch printed circuit board number.
Serial number: Display the serial number assigned.
Module 1 Type: Display module 1, port 1 information:
1000Tx, 1000Fx or 100Fx ext. Depending on the module card used.
Module 1 information: Information as saved in eeprom of module.
Module 2 Type: Display module 1, port 2 information.
1000Tx, 1000Fx or 100Fx ext. Depending on the module card used.
Module 2 information: Information as saved in eeprom of module.

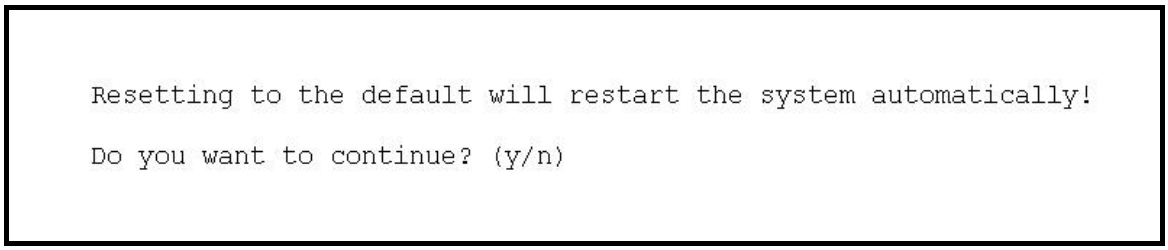


4-5. Reboot Switch



4-5-1. Default

This will Reset the switch to its default configuration.

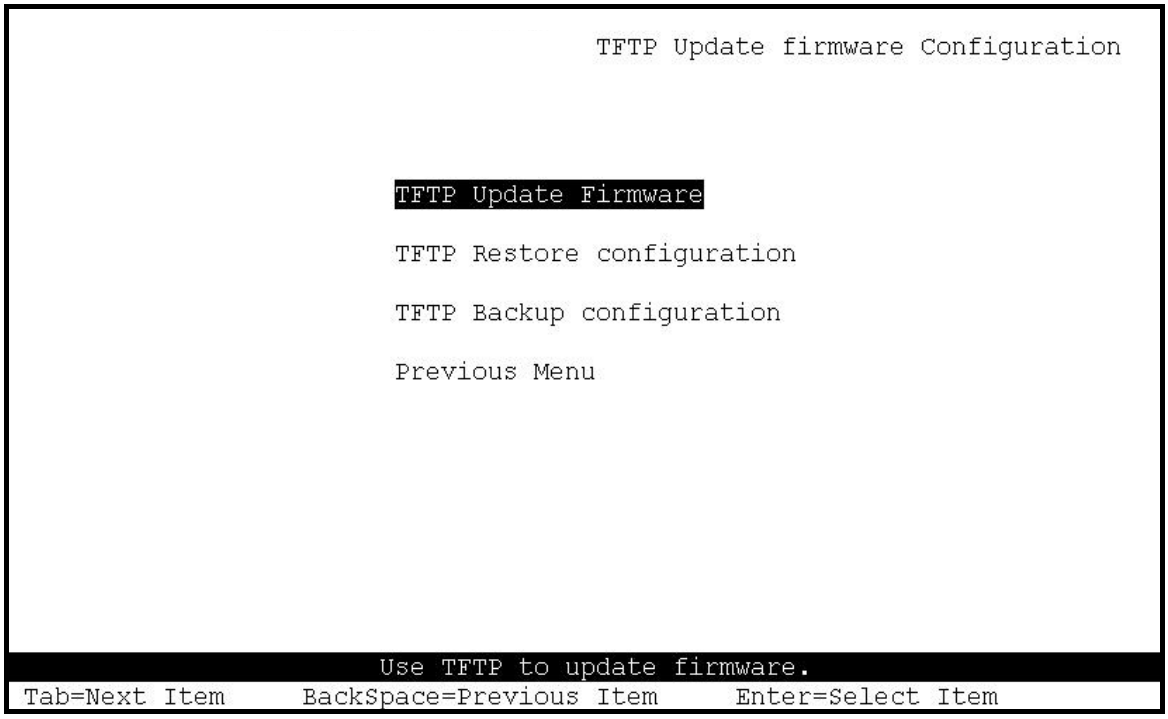


4-5-2. Restart

This will reboot the switch (i.e. software reset).

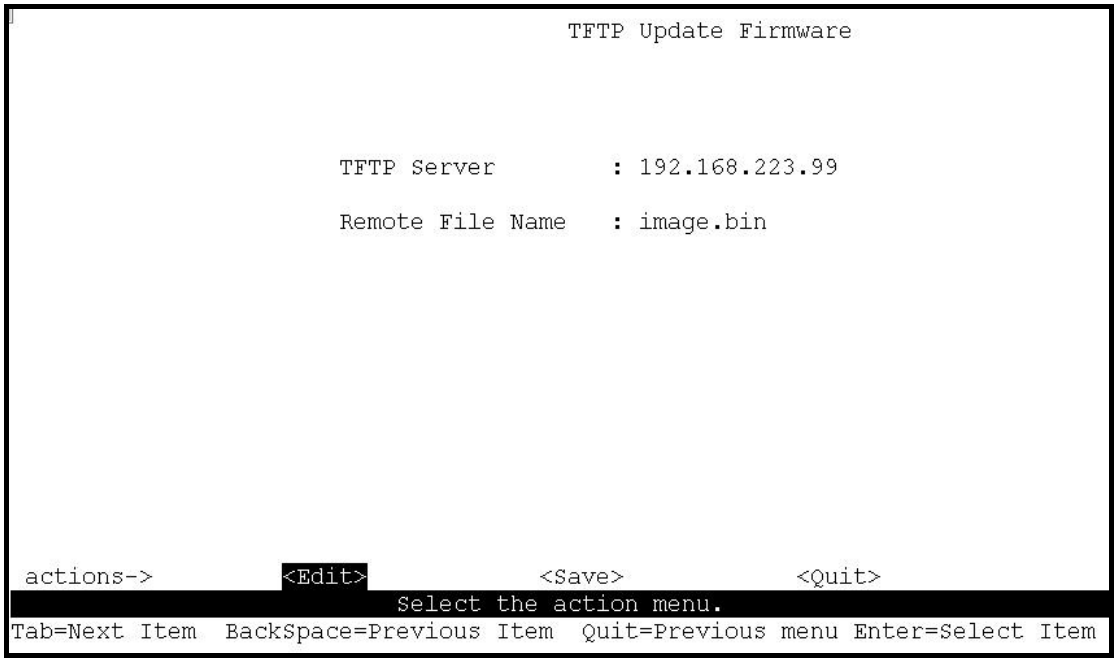
4-6. TFTP Update Firmware

This page provides TFTP firmware update, configuration backup and configuration restore options.



4-6-1. TFTP Update Firmware

This page allows the administrator to perform a TFTP firmware update.

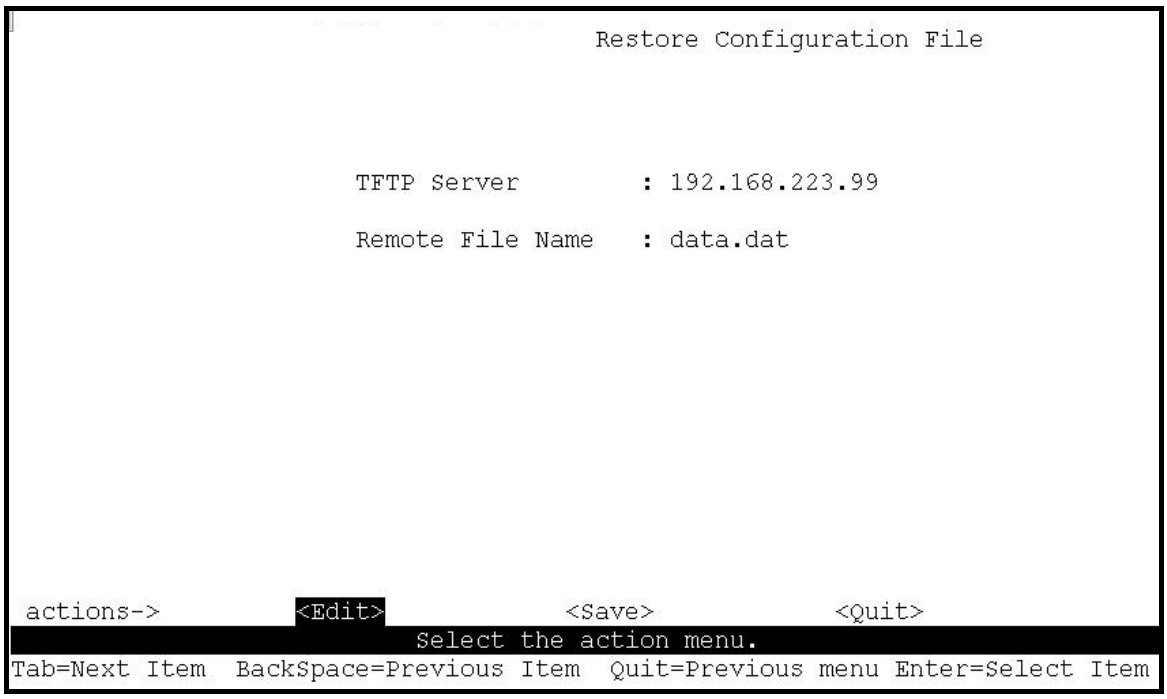


Actions->

1. Start the TFTP server, and copy the updated firmware version image file to the TFTP servers work directory.
2. Press **<Edit>** on this page.
3. **TFTP Server:** Enter the IP address of the TFTP server.
4. **Remote File Name:** Enter the name of the image file.
5. Press **Ctrl+A** go to action line.
6. Select the **<Save>** Option. This will start the download of the image file.
7. When successfully downloaded the image file will be permanently saved to the eeprom.
8. Restart the switch.

4-6-2. Restore Configure File

This page allows the administrator to perform a TFTP configuration restore.
This can be used to restore a previously backed up configuration.

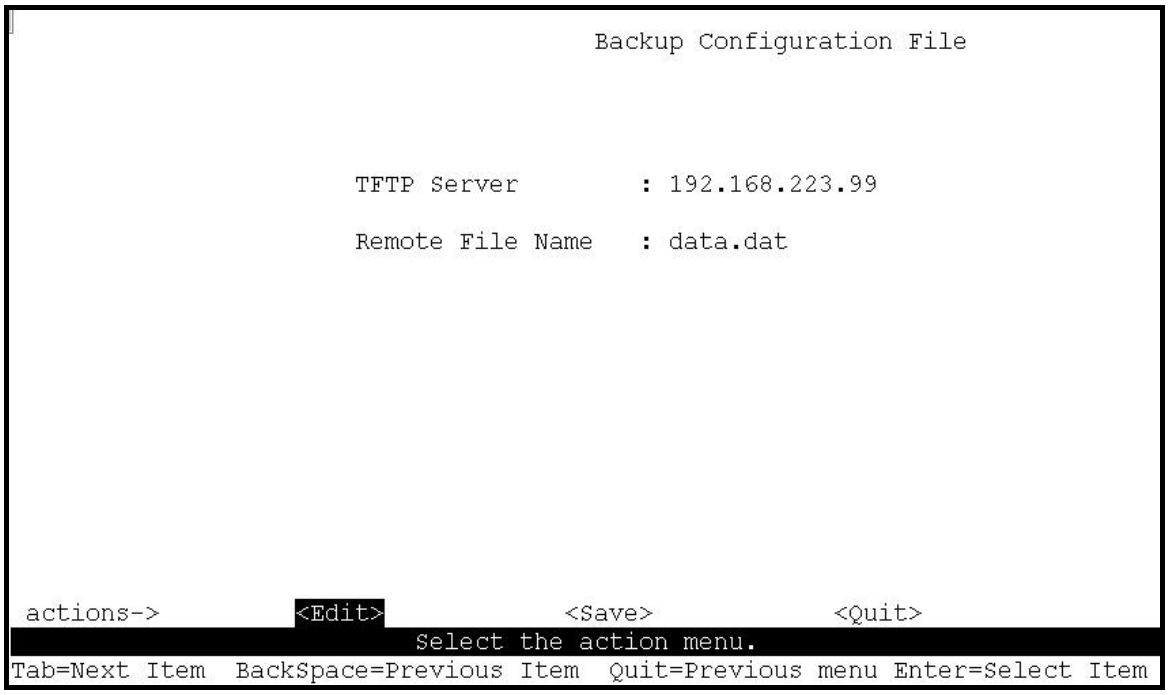


Actions->

1. Start the TFTP server.
2. Select the **<Edit>** option on this page.
3. **TFTP Server:** Type the IP address of the TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** go to action line.
6. Select the **<Save>** Option. This will start the download of the configuration file.
7. When successfully downloaded the image file will be permanently saved to the eeprom.
8. Restart the switch.

4-6-3. Backup Configure File

This page allows the administrator to perform a TFTP configuration backup.
This can be used to backup the current configuration.



Actions->

1. Start the TFTP server.
2. Select the **<Edit>** option on this page.
3. **TFTP Server:** Type the IP address of the TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** go to action line.
6. Select the **<Save>** option. This will start the upload of the configuration file.
7. When successfully uploaded, the image file will be saved on the TFTP server.

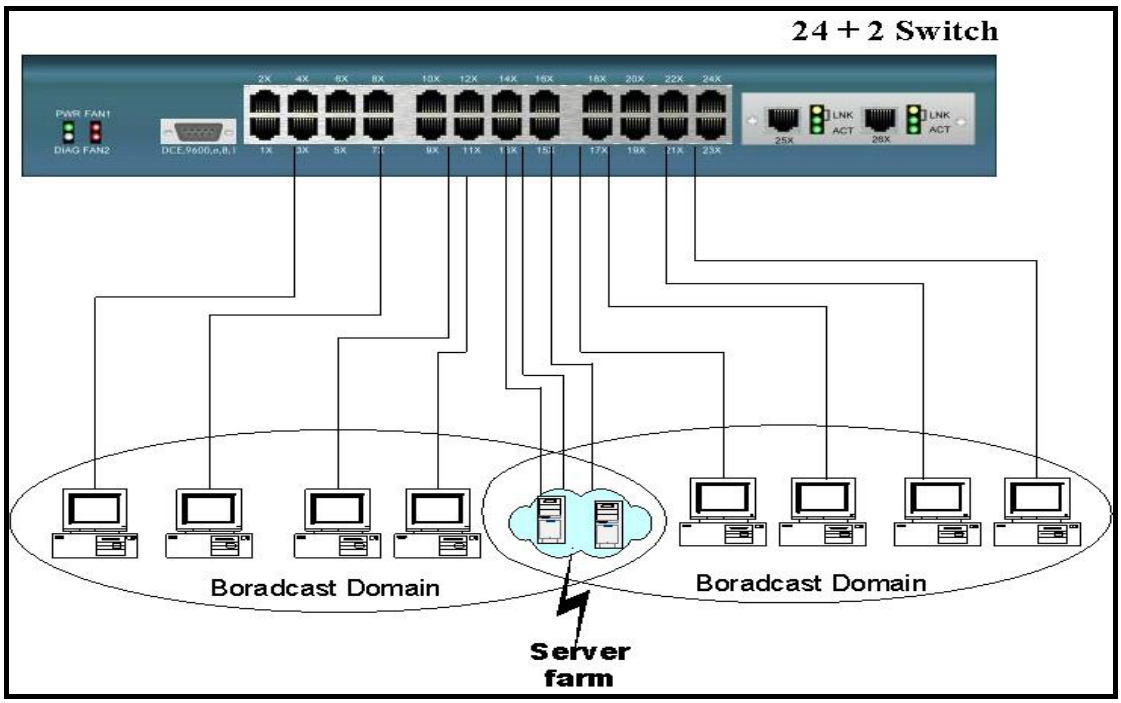
5.0 Application Examples:

1.1 VLAN applications used with switch.

A VLAN is a simple option to protect your network against broadcast storms by creating segments based on Layer2 Ethernet information. It avoids the complexity and heavy processing requirements of Layer3 IP based routers, while providing some similar functionality.

Each VLAN grouping forms a separate isolated Broadcast Domain. These Domains (VLAN's) can overlap to allow multiple VLAN groups to access servers, which need to exist in all VLAN groups.

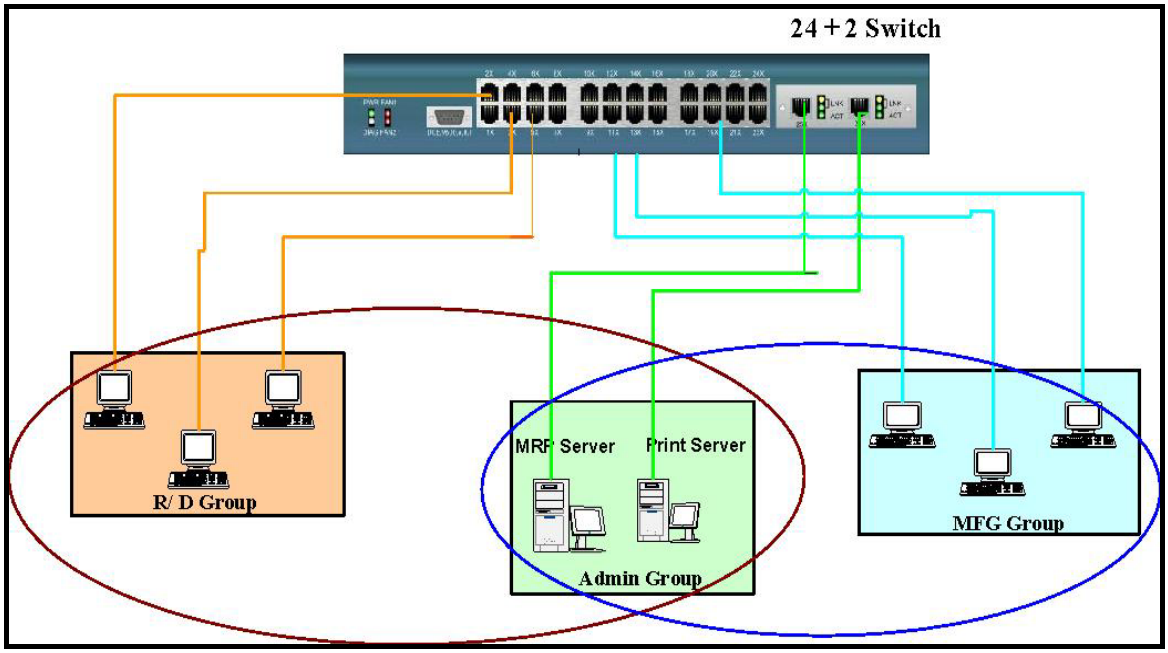
Virtual LAN, or VLAN's should be created where broadcast traffic needs to be limited to within certain groupings of nodes. Adding VLAN's will improve the efficiency of your network, as individual PC's will receive and respond to fewer broadcast packets. They also provide security, by not forwarding packets between VLAN's.
Example: You have 2 serviced offices within one building. 2 companies operate from the one building. You want to allow both to use the Internet via your site proxy server, but do not want the PC's in one office to be able to connect to any of the PC's in the other office. If you grouped the 2 offices in their own VLAN's, and then grouped the proxy server in both VLAN's, you have secured the site.



Benefits of VLANs

- Grouping users into logical networks for performance enhancement.
- Provides effective broadcast containment between segmented ports, this can prevent network broadcast flooding issues.
- Offers security by completely isolating different Broadcast Domains.
- Can preserve existing investment in equipment and cabling.
- Provides an easy, flexible, and economic way to modify users into groups as needed.
- Network administrators can easily "fine tune" the network.
- Separates network structure from the physical topology of the cabling.
- Makes large networks more manageable.

You can group users according to some shared characteristic, such as a common business function or a common protocol. A single switch may have several independent VLANs within it. Below is an example with a R&D, Manufacturing and Administration department, that has been partitioned into two different VLAN groups. Members from the R&D group cannot directly talk to the Manufacturing group, but they still share the same Server, Printer, Internet connection, or any other shared devices that you would need.



5.2 Trunking Applications used with the switch:

Trunking allows you to increase the available bandwidth between switches by grouping ports into a trunk. Trunks can also be used to connect servers to switches for higher bandwidth pipes, or you can use trunking to improve the throughput between different switches. Additionally trunking provides fail-over functionality. When one of the links of a trunk has failed, the traffic originally going through that link will be automatically be re-directed to other links of the trunk, this gives the trunk redundancy.