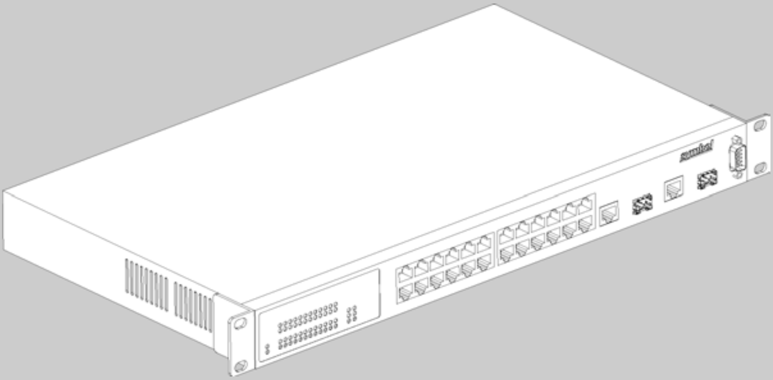
ES3000 Ethernet Switch

User Guide



symbol

The Enterprise Mobility Company™

ES3000 Ethernet Switch User Guide

72E-68446-01

Revision A

May 2004

Symbol reserves the right to make changes to any software or product to improve reliability, function, or design.

Symbol does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Symbol Technologies, Inc., intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Symbol products.

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, New York 11742-1300
http://www.symbol.com

Contents

About This Guide

Chapter 1. Switch Management Overview

Chapter 2. Firmware Upgrades

Chapter 3. Administration Console Access

Chapter 4. Web Management Access

Chapter 5. Command Line Interface

Appendix A. Specifications & Pin Assignments

Appendix B. Cabling Guidelines

Appendix C. Customer Support

About This Guide

Introduction

The *ES3000 User Guide* provides general instructions for configuring and using the ES3000 Ethernet Switch. This guide provides information general in nature for those who may be new to the E3000 Ethernet Switch device.

Notational Conventions

The following conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential

- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Service Information

If a problem with is encountered with the equipment, contact the *Symbol Customer Support*. Refer to *Appendix C* for contact information. Before calling, have the model number and serial number at hand.

If the problem cannot be solved over the phone, you may need to return your equipment for servicing. If that is necessary, you will be given specific directions.

Symbol Technologies is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty. If the original shipping container was not kept, contact Symbol to have another sent to you.

1 Switch Management Overview

1.1 About the ES3000 Ethernet Switch

The ES3000 Ethernet Switch comes in two versions. One version provides Power over Ethernet (PoE) in accordance with IEEE standard 802.3af. This allows compatible Ethernet devices to obtain power from the 10/100BaseT Ethernet wiring. IEEE 802.3af PoE senses the need for power before supplying power and will not damage non-PoE Ethernet devices.

The other version of the ES3000 Switch does not provide power over Ethernet. Power features are not available in the non-PoE version of the switch.

The Symbol ES3000 Ethernet Switch is available in the following models:

ES 3000-PWR (supporting PoE) - Part Number ES-3000-PWR-10-WW

ES 3000 (non PoE) - Part Number ES-3000-10-WW

The PoE and non-PoE versions of the ES3000 use different versions of the bootcode and runtime software. Do not attempt to use PoE software with a non-PoE switch. Do not attempt to use non-PoE software with a PoE switch. Attempting to do so may render the switch inoperable.

1.2 Management Access Overview

The Symbol ES3000 Managed Switch provides user interface flexibility using:

- An administration console
- A Web Browser interface
- External SNMP-based network-management application.

The administration console and Web Browser interface are embedded in the switch firmware.

1.3 SNMP Access

Use an external Simple Network Management Protocol (SNMP) -based application to manage the Symbol ES3000 Ethernet Switch.

The SNMP management method requires the SNMP agent on the switch and the SNMP Network Management Station use the same community string and the SNMP Network Management Station is entered in the SNMP Host table on the switch. The SNMP management method uses two community strings: the GET community string and the SET community string. If the SNMP Network management Station only knows the SET community string, it can read from and write to the MIBs. However, if it only knows the GET community string, it can only read MIBs. The default GET community string for the switch is 'public', and the host table is empty.

1.4 Protocols

The Symbol ES3000 Ethernet Switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- SNMP

1.4.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program (such as Telnet) allowing the establishment of a management session from a Macintosh, PC or UNIX workstation. Because Telnet runs over TCP/IP, at least one IP address is required on the ES3000 Ethernet Switch before establishing access to it with a virtual terminal protocol.

Terminal emulation differs from a virtual terminal protocol in that the user is required to connect a terminal or PC directly to the console port. A workstation can be connected to the system through a virtual terminal protocol (Telnet), and a terminal connecting directly to the console port through a null-modem serial cable.

1.4.2 SNMP Protocol

SNMP is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries allowing the protocol to format messages and transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

1.5 Default Installation

1.5.1 Preparing for Site Installation

Site preparation for the ES3000 Ethernet Switch installation begins with a site survey and network analysis. Review the site survey reports to determine specific equipment placement, site-specific port capacity, and power drops. Ensure the installation area is free of dust and dirt.

Review the following guidelines for site preparation:

- Assign installation responsibility to appropriate personnel.
- Identify where all installed components are located.
- Verify appropriate rack mounting requirements.
- Arrange for a sufficient number of power drops to support the equipment installation.
- Verify adequate ventilation to all installed equipment.
- Identify and prepare Ethernet and TCP/IP and serial port connections.
- Verify cable lengths are within maximum allowable distances for optimal signal transmission.

1.5.2 Package Contents

Inspect the package contents and report any missing or damaged items to the Symbol sales representative. The package (for both the PoE and non-PoE Ethernet Switch models) should contain the following:

- ES3000 Ethernet Switch
- Quick Installation Guide
- Rack-mounting brackets
- Power cord (optional)
- Null modem serial cable.

1.5.3 Supplying Power

To cable the ES3000 Ethernet Switch to receive power:

1. Connect the supplied AC power cord to the power connector on the rear of the Ethernet Switch.
2. Plug the cord into a standard AC outlet with a voltage range from 100VAC to 240VAC.

   The Ethernet Switch is ready to receive power.

1.5.4 Establishing a RS-232 Serial Connection to the Ethernet Switch

The initial configuration of the Ethernet Switch is set using the serial port. To establish the RS-232 serial connection:

1. Connect the port to a RS-232 (DB-9) serial port on the configuring computer using the supplied cable.
2. Use a terminal emulation application to access the command line interface (CLI) through the console port.
3. Configure the terminal emulation application and operating system to support the following serial port specifications:

Terminal Type	VT-100
Communication	8 - data bits
Mode	1 - stop bit
	no parity
	19200 bps transfer rate
	no flow control
	no hardware compression

1.6 Administration of the ES3000 Ethernet Switch

There are three management user interfaces on the switch: menu-driven, CLI, and Web. The menu-driven and CLI interfaces are accessed using a direct serial connection or via Telnet over an Ethernet connection. The Web interface is accessible via HTTP over an Ethernet connection to the switch.

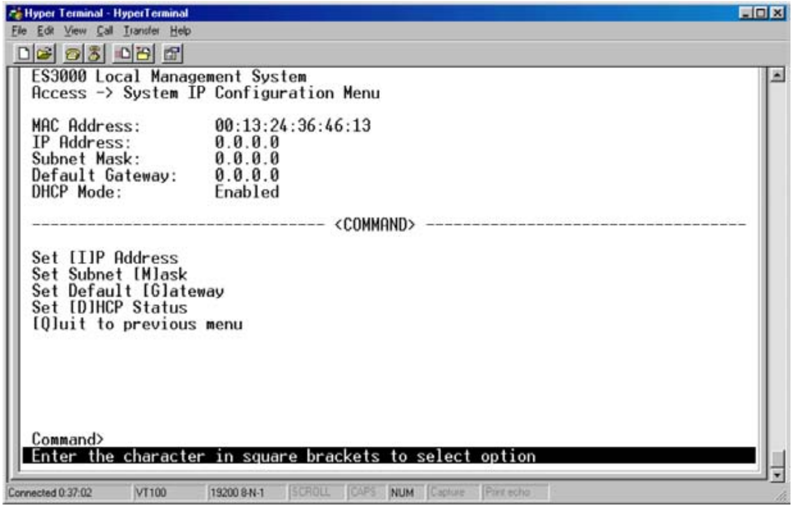
	Menu-Driven UI	***CLI***	***Web UI***
Via direct serial connection	yes	yes	no
Via Ethernet connection	yes, via Telnet	yes, via Telnet	yes, via HTML

Managing the switch remotely (via Telnet or Web) requires the switch to have an IP address assigned to it. The administrator must know what that IP address is. By default, the switch is configured to use DHCP to obtain its IP address. If the IP address assigned to the switch from the DHCP server can be determined, use any of the management interfaces. If not, access the switch via direct serial connection to determine the IP address assigned via DHCP. If a DHCP server is not available on the network, access the switch via direct serial connection to assign an IP address to the switch.

To configure or determine the IP address on the switch via direct serial connection:

1. Use HyperTerminal (or other communications utility) to secure a connection to the ES3000 Ethernet Switch.
2. Hit the return key <**Enter**> to display the ES3000 logon screen.
3. Enter a user name of **admin** and password of **symbol**. Press **Enter**.
4. Select **System Admin** from the main menu. Press **Enter**.
5. Select **Access** from the System Admin menu. Press **Enter**.
6. Select **IP Config** from the Access menu. Press **Enter**.

   The **System IP Configuration Menu** displays.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 0:37:02 VT100 19200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
ES3000 Local Management System
Access -> System IP Configuration Menu

MAC Address:        00:13:24:36:46:13
IP Address:         0.0.0.0
Subnet Mask:        0.0.0.0
Default Gateway:    0.0.0.0
DHCP Mode:          Enabled

-------------------------------- <COMMAND> -----------------------------------

Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Set [D]HCP Status
[Q]uit to previous menu



Command>
Enter the character in square brackets to select option
```

To use the ES3000 Command Line Interface (CLI) to configure the device:

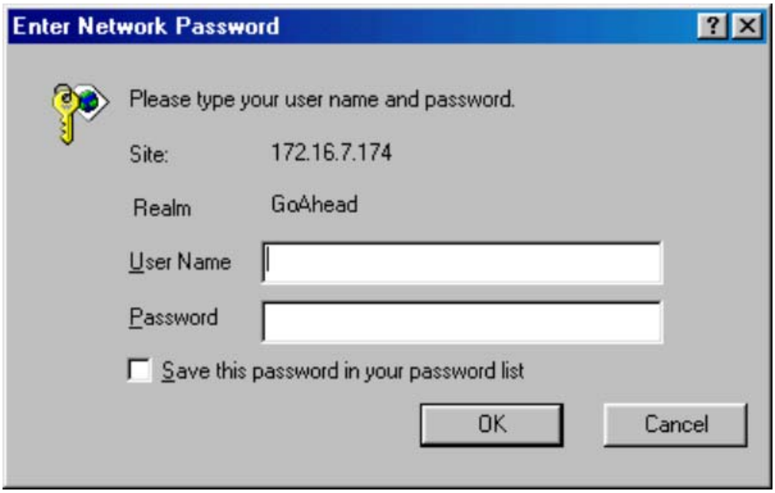
1. Use HyperTerminal (or other communications utility) to secure a connection to the ES3000 Ethernet Switch.
2. Hit the return key <**Enter**> to display the ES3000 logon screen.
3. Enter a user name of **admin** and password of **symbol**. Press **Enter**.
4. Select **Execute CLI** from the Main Menu. Press **Enter**.

To use the ES3000 Web Management interface to configure the device:

Note A network connection is required between the device and the host to use the Web Management interface to configure the device.

1. Access the Web interface (using a Web browser) by entering the switch IP address into the address bar. Press **Enter**.

   Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later is required.



Enter Network Password

Please type your user name and password.

Site: 172.16.7.174

Realm GoAhead

User Name

Password

□ Save this password in your password list

2. Enter a user name of **admin** and password of **symbol**. Press **OK**.

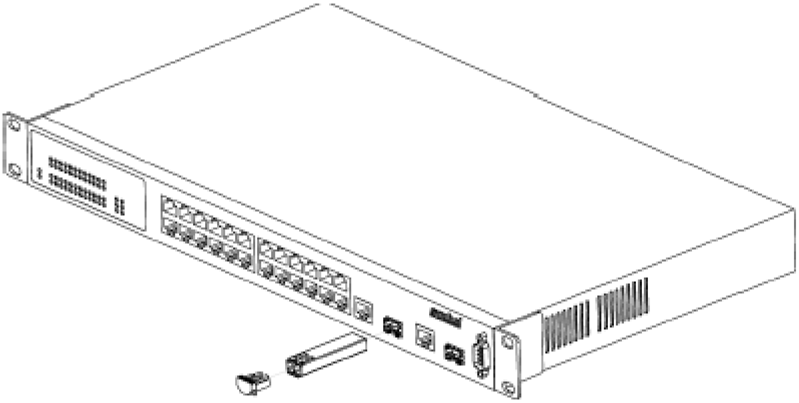
   The Web interface **General Information** page displays. Refer to *Chapter 3* for information on using the ES3000 serial interface to configure the device. Refer to *Chapter 4* for instructions on using the Web interface to configure the device. Refer to *Chapter 5* for instructions on using the CLI for device configuration.

1.7 Installing a SFP Fiber Transceiver

The ES3000 Ethernet Switch supports a SFP (small form factor pluggable) fiber channel transceiver used in fiber channel cable installations.

To install the SFP Fiber Transceiver:

1. Remove the rubber plug protecting the optics on the transceiver.
2. Insert the transceiver into the fiber transceiver cage available on ports 25 and 26 on the ES3000 Ethernet Switch.



3. Ensure one of the following two cable types is used when connecting fiber cable to the ES3000 Ethernet Switch:
   - LC 62.5um/125um multimode fiber optic cable
   - LC 50um/125um multimode fiber optic cable
4. Consult the System Administrator for cable length and installation specifications unique to the installation environment.

Note

If removing the SFP transceiver, disengage the locking mechanism on the SFP transceiver carefully before removing the transceiver from the ES3000 Ethernet Switch.

2 Firmware Upgrades

Symbol periodically releases new versions of the firmware that runs on the ES3000 Ethernet Switch. These software releases provide new features that can extend the useful life of the ES3000 Ethernet Switch.

To upgrade software on the switch, boot the switch from a TFTP server instead of its own non-volatile memory (NVRAM). To initiate the sequence, set the **Next Boot From** configuration parameter to **Boot from Net**, and reset. When the Boot from Net option is set, the switch uses an image residing on a TFTP server on the network. Ensure the TFTP server residing on the network is accessible by the switch. Once completed, the software version requires verification within the System page.

The PoE and non-PoE versions of the ES3000 switch use different versions of the bootcode and runtime software. Do not attempt to use PoE software with a non-PoE switch. Do not attempt to use non-PoE software with a PoE switch. Attempting to do so may render the switch inoperable.

Note

Symbol recommends using a RS-232 serial port connection to the switch during the software upgrade. When using a Telnet Session or Web interface, the connection to the switch is not available until the switch has completed its boot cycle and entered the Spanning Tree forwarding mode. This can take up to three minutes.

To upgrade the switch firmware using the Web interface:

1. Go to **Main Menu**->**Switch Tools Configuration**->**Software Upgrade Menu**->**TFTP Software Upgrade**.
2. Set the IP address and Image File Name.
3. Verify the IP address for the TFTP Server and the file name of the new software image are accurate.
4. Verify the TFTP server and IP connection between server and switch are working properly.
5. Select **Upgrade Image**. The switch downloads the image from TFTP Server and replaces the runtime image in Flash.

3

Administration Console Access

The administration console is an internal, character-oriented, VT-100/ANSI menu-driven user interface for management configuration activities. View the administration console from a terminal, PC, Apple Macintosh, or UNIX workstation connected to the switch console port.

3.1 Direct Access Management Method

The direct access management method is required when initially setting up the switch. Thereafter, Symbol recommends using the Web management access method (described in *Chapter 4*) to manage the switch if unfamiliar with command line configuration. Advanced users are recommended to use the CLI commands described in *Chapter 5* to manage the switch.

Direct access to the switch console is available by connecting the switch console port to a VT-100 or compatible terminal or to a PC, Apple Macintosh, or UNIX workstation equipped with a terminal-emulation program. Use the null-modem cable supplied with the switch to secure the connection.

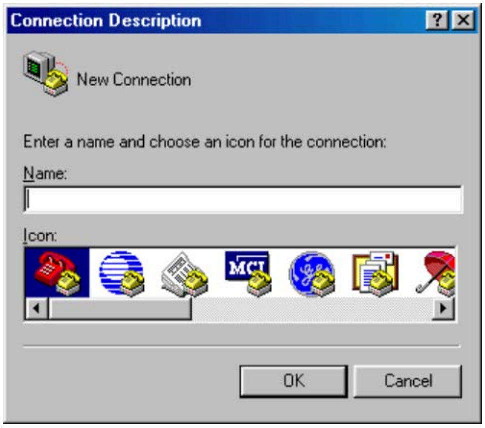
The following are Symbol recommended terminal-emulation programs:

- HyperTerminal (which is built into the Microsoft Windows operating systems)
- ZTerm (Apple Macintosh)
- TIP (UNIX workstation)

To set up the connection using a HyperTerminal on a PC (but other systems follow similar steps):

1. Click the **Start** button. Select **Accessories** and **Communications**.
2. Select **HyperTerminal**.

   The **Connection Description** screen displays.



Connection Description

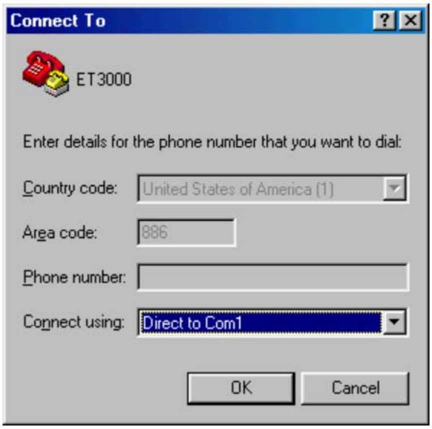
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

3. Enter a name for the connection. Click **OK**.
4. The **Connect To** screen displays. In the bottom, drop down box labeled **Connect using**, choose the COM port the switch connects to. Click **OK**.



Connect To

ET3000

Enter details for the phone number that you want to dial:

Country code: United States of America (1)

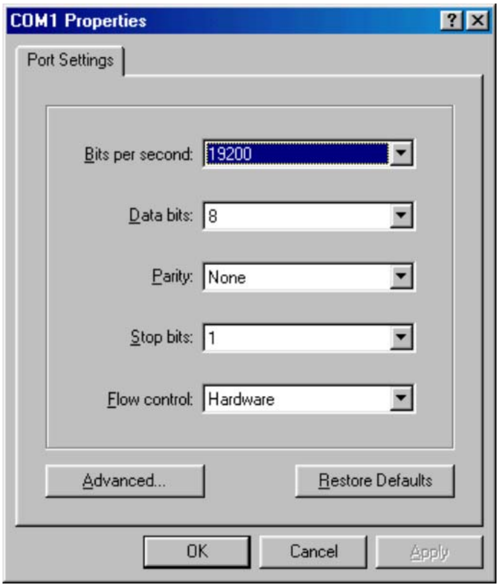
Area code: 886

Phone number:

Connect using: Direct to Com1

5. Verify the port settings are:

Baud Rate:	19200
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None



Bits per second: 19200

Data bits: 8

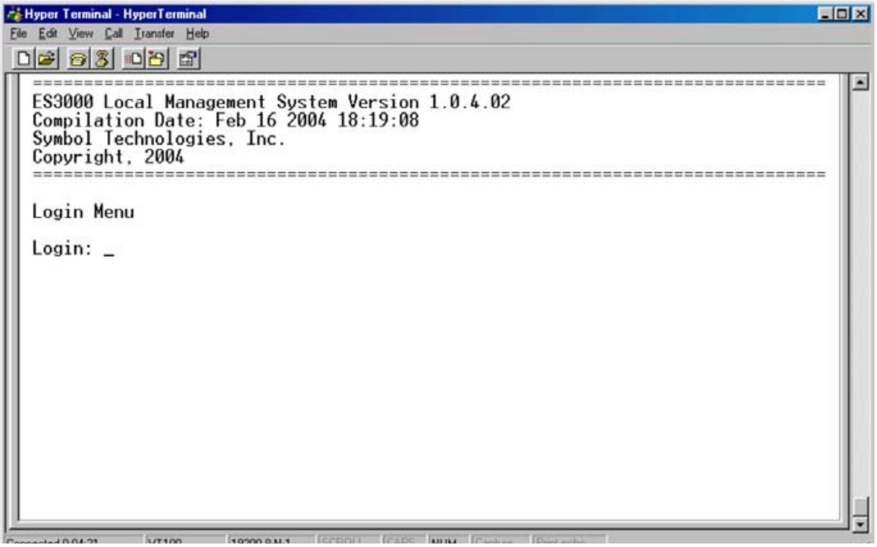
Parity: None

Stop bits: 1

Flow control: Hardware

6. Click **OK**.

   When the HyperTerminal window displays, a connection exists to the switch and a logon screen displays. If a login screen or main menu does not display, hit the return key.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
==============================================================================
ES3000 Local Management System Version 1.0.4.02
Compilation Date: Feb 16 2004 18:19:08
Symbol Technologies, Inc.
Copyright, 2004
==============================================================================

Login Menu

Login: _
```

To use the arrow keys when attached to the User Interface via a Telnet Session to toggle forward and backward. Choose **Properties** from the terminal pull-down menu and verify the **VT100 Arrows** option is turned on.

3.2 User Interface

The switch provides a menu-driven interface for managing the switch, as well as a Command Line Interface (CLI). The CLI uses text commands to manage the switch. The CLI is accessed through the CMI. See *Chapter 5* on page for detailed information on navigating the CLI.

3.3 Saving Configuration Changes

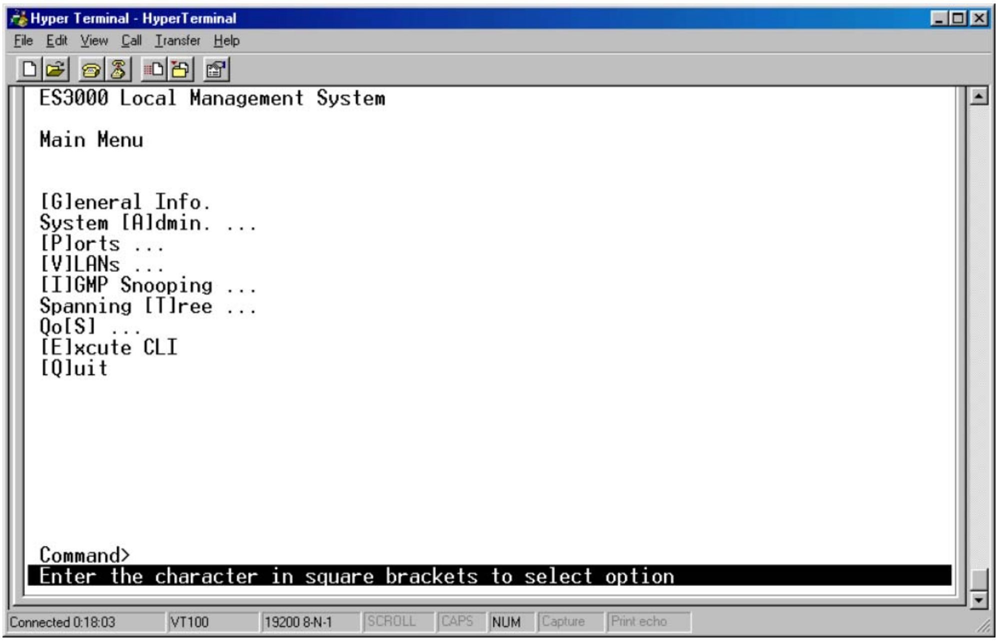
To save changes made within the menu-driven interface, refer to *Main Menu->System Admin.->Tools->Save Config. on page 3-24*. Use the *Save Config* page to save all updates to the menu-driven interface. Once updates are made refer back to the target configuration page to ensure the updates have been implemented by the ES3000 Ethernet Switch.

3.4 Main Menu Options

The main menu displays the submenus available. Select **Enter** when a highlighted option confirms the choice of the specified submenu. The hotkey or letter within square bracket of each menu option can also be typed to directly choose the option. There are ten main menu items to choose from:

- General Information
- System Administration
- Ports Configuration…
- VLANs Configuration
- IGMP Snooping Configuration
- Spanning Tree
- QoS Configuration…
- Execute CLI
- Quit

To logout of the user interface, select **Ctrl-D** anytime during the telnet session. The interface moves back to the login screen (password enabled) or Main Menu (password disabled).



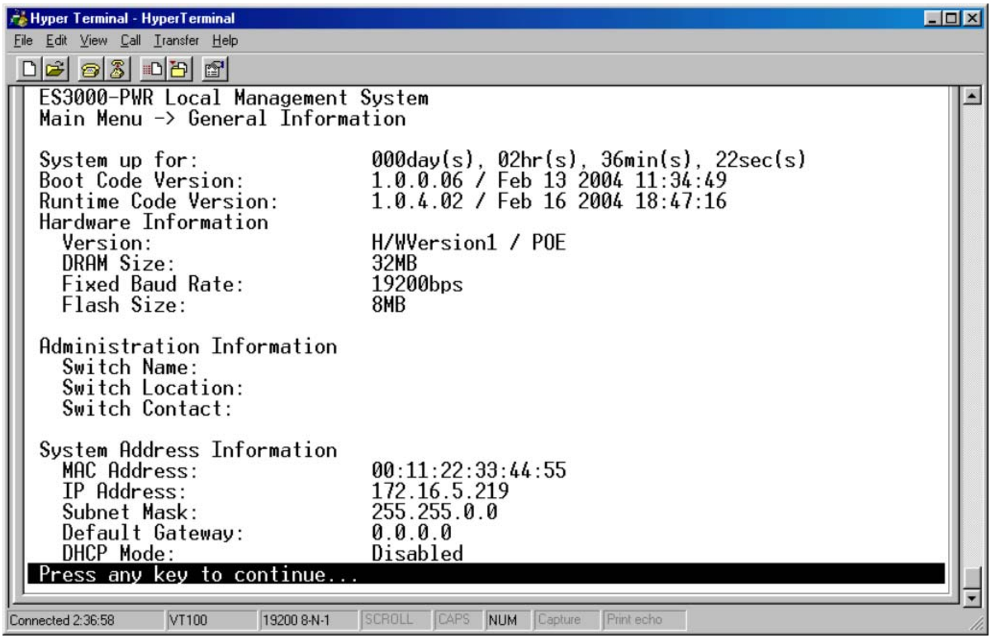
Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 0:18:03
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System

Main Menu


[G]eneral Info.
System [A]dmin. ...
[P]orts ...
[V]LANs ...
[I]GMP Snooping ...
Spanning [T]ree ...
Qo[S] ...
[E]xcute CLI
[Q]uit








Command>
Enter the character in square brackets to select option
```

3.5 General Information

The **General Information** screen displays information on the operational state of the ES3000 Ethernet Switch. Use this information for general configuration information when accessing other menu items.

• System up for	System run time after boot up
• Boot Code Version	The version and timestamp of boot code
• Runtime Code Version	The version and timestamp of runtime code
• Hardware Information	Hardware associated information
• Version	Hardware revision version
• DRAM Size	Size of DRAM on system
• Fixed Baud Rate	Data rate on console port, set to 9600.
• Flash Size	Size of Flash memory
• Administration Information	
• System Name	Name of system, user definable
• System Location	Location of system, user definable
• System Contact	Contact information, user definable
• System Address Information	
• Default MAC Address	MAC Address of system
• Default IP Address	The default IP address, user definable
• Default Subnet Mask	The default subnet mask, user definable
• Default Gateway	The default gateway, user definable
• DHCP Mode	Enables/Disables DHCP


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:36:58
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

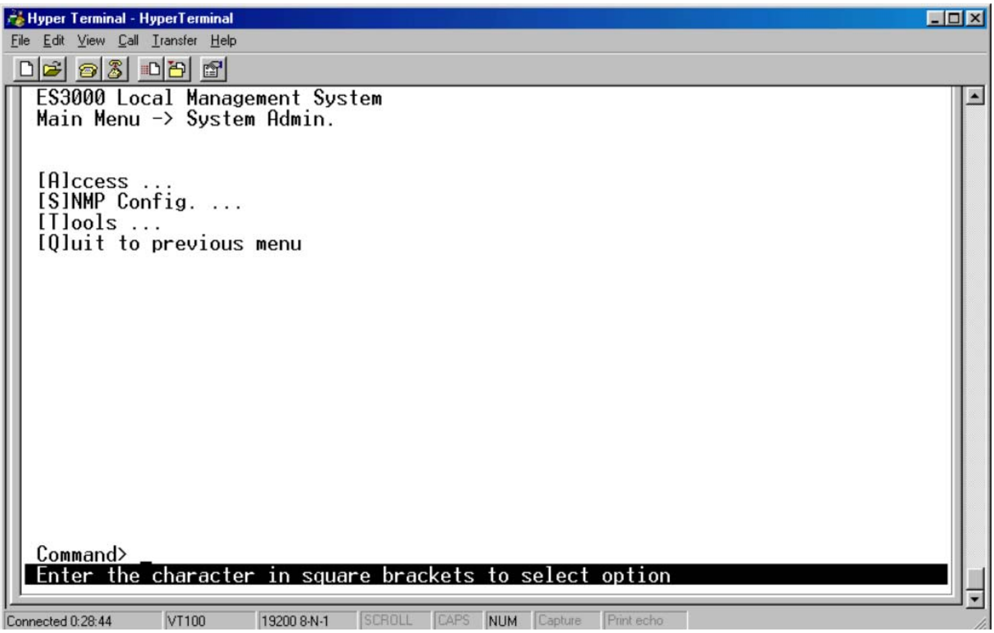
```
ES3000-PWR Local Management System
Main Menu -> General Information

System up for:              000day(s), 02hr(s), 36min(s), 22sec(s)
Boot Code Version:          1.0.0.06 / Feb 13 2004 11:34:49
Runtime Code Version:       1.0.4.02 / Feb 16 2004 18:47:16
Hardware Information
  Version:                  H/WVersion1 / POE
  DRAM Size:                32MB
  Fixed Baud Rate:          19200bps
  Flash Size:               8MB

Administration Information
  Switch Name:
  Switch Location:
  Switch Contact:

System Address Information
  MAC Address:              00:11:22:33:44:55
  IP Address:               172.16.5.219
  Subnet Mask:              255.255.0.0
  Default Gateway:          0.0.0.0
  DHCP Mode:                Disabled
Press any key to continue...
```

3.5.1 Main Menu->System Administration->System Configuration

Use the **System Configuration** screen to access System Name, Contact Person, and System Location submenus required for configuring the device. The MAC address and Object ID also display, but these items are not user configurable.

There are three submenus at System Configuration menu,

- Access Configuration
- SNMP Configuration
- Tools Configuration



Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
Main Menu -> System Admin.


[A]ccess ...
[S]NMP Config. ...
[T]ools ...
[Q]uit to previous menu










Command> _
Enter the character in square brackets to select option
```

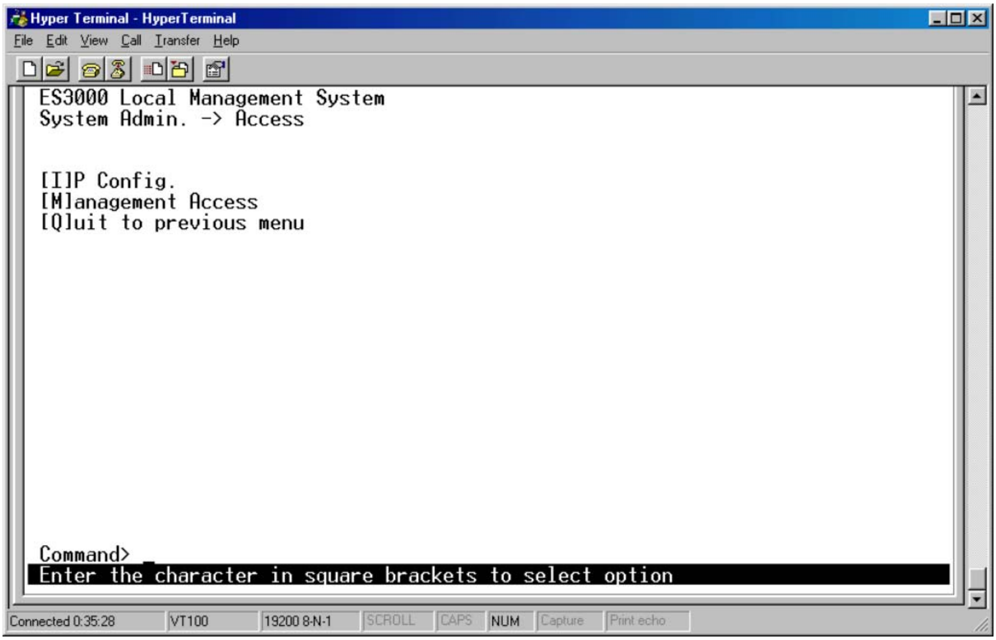
Connected 0:28:44
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.2 Main Menu->System Admin.->Access Configuration

There are three submenu options within the **Access Configuration** menu:

- IP Config.
- Management Access
- Quit

Use the **IP Config** menu to manage the IP related information for the ES3000 from the System IP Configuration menu. Use the **Management Access** menu to enable or disable the Web, SNMP and/or telnet interfaces from the Management Access menu.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 0:35:28
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
System Admin. -> Access


[I]P Config.
[M]anagement Access
[Q]uit to previous menu




Command> _
Enter the character in square brackets to select option
```

3.5.3 Main Menu->Access->System IP Configuration

Use the **System IP Configuration** menu to manage IP related information for the ES3000 supported system.

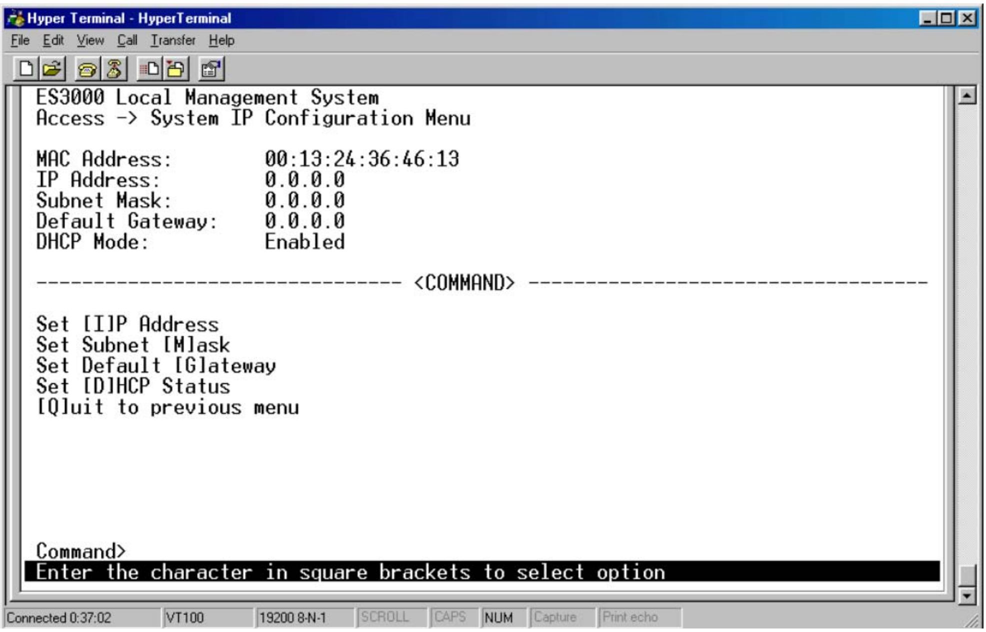
- IP Assignment Mode
  - Manual - Manually enter IP related information
  - DHCP - The switch accepts DHCP broadcast from a DHCP server and automatically configures IP related information

The default setting is DHCP. However, the user needs to know the IP address of the switch to remotely manage it and DHCP assignments can change. Symbol recommends changing the IP assignment mode from DHCP to manual after the switch as obtained its IP address. This creates a more stable IP address.

If in manual mode and configuring IP information:

- Enter a site-specific IP address, Gateway Address, and Network Mask (or subnet mask). Consult the network administrator for the information.

- Press **Ctrl-W** to save any changes to NVRAM.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
Access -> System IP Configuration Menu

MAC Address:        00:13:24:36:46:13
IP Address:         0.0.0.0
Subnet Mask:        0.0.0.0
Default Gateway:    0.0.0.0
DHCP Mode:          Enabled

-------------------------------- <COMMAND> -----------------------------------

Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Set [D]HCP Status
[Q]uit to previous menu







Command>
Enter the character in square brackets to select option
```

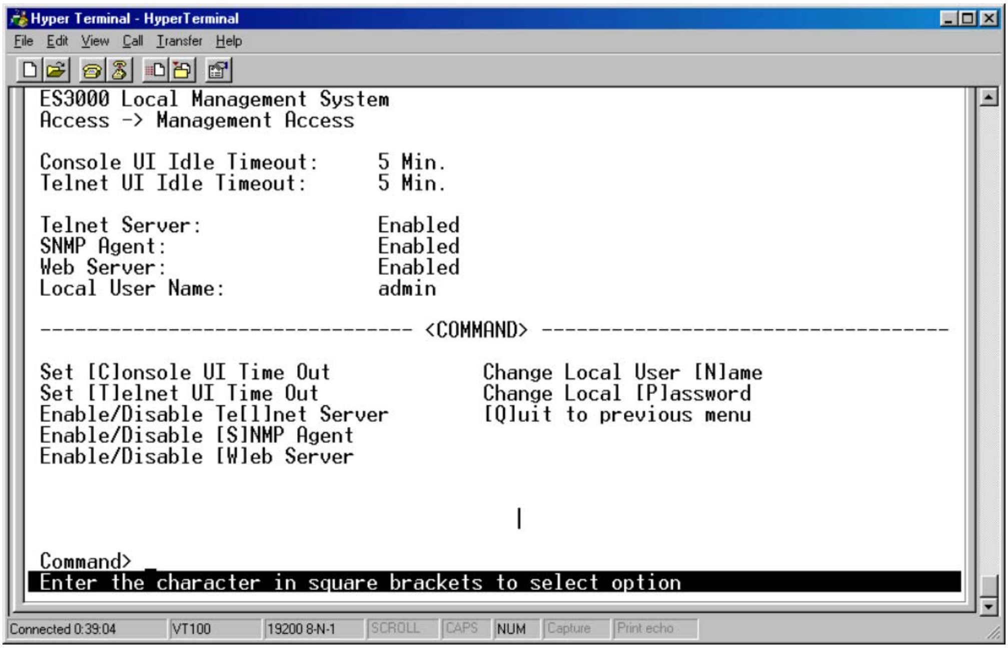
Connected 0:37:02
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.4 Main Menu->Access->Management Access

Use the **Management Access** screen to enable or disable the Web, SNMP, and/or telnet interfaces. The Management Access menu can also be used to change the user name and password. User names and passwords are case sensitive and can be up to 20 characters long.

Note Using telnet, the user can only enable/disable the Web Interface. The user cannot enable/disable the telnet interface from the Management Access screen.

If the password is unknown, contact Symbol technical support at 1-631-738-2400 (in North America) or 1-800-653-5350 (International).


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 0:39:04
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Access -> Management Access

Console UI Idle Timeout:     5 Min.
Telnet UI Idle Timeout:      5 Min.

Telnet Server:               Enabled
SNMP Agent:                  Enabled
Web Server:                  Enabled
Local User Name:             admin

------------------------------- <COMMAND> ----------------------------------

Set [C]onsole UI Time Out             Change Local User [N]ame
Set [T]elnet UI Time Out              Change Local [P]assword
Enable/Disable Te[l]net Server        [Q]uit to previous menu
Enable/Disable [S]NMP Agent
Enable/Disable [W]eb Server



Command> _
Enter the character in square brackets to select option
```

The configurable fields within the Management Access menu have the following values:

Set Console UI Time Out:	Session is disconnected when the time out occurs
Set Telnet UI Time Out:	Telnet session is disconnected when the time out occurs
Change Local User Name:	Defines the name of the local user
Change Local Password:	Changes the password of the local user
Enable/Disable Telnet Server:	Enables or disables the system accessibility via telnet.
Enable/Disable SNMP Agent:	Enables or disables the system accessibility via SNMP
Enable/Disable Web Server:	Enables or disables the system accessibility via Web browser.

3.5.5 Main Menu->System Admin->SNMP Configuration Menu

Simple Network Management Protocol (SNMP) is a messaging protocol allowing communication between network managers and agents. An SNMP manager is part of a network management system (NMS), allowing an administrator to manage the network by making requests to agents. An SNMP agent provides an interface to a managed device containing managed objects in a management information base (MIB).

At the request of an SNMP manager, an SNMP agent retrieves or stores values in the MIB, which contains information about the device and network. The SNMP agent can also send asynchronous traps, which alert the SNMP manager to certain conditions on the network. A trap could result from improper user authentication, PoE power usage over threshold or network topology changes..

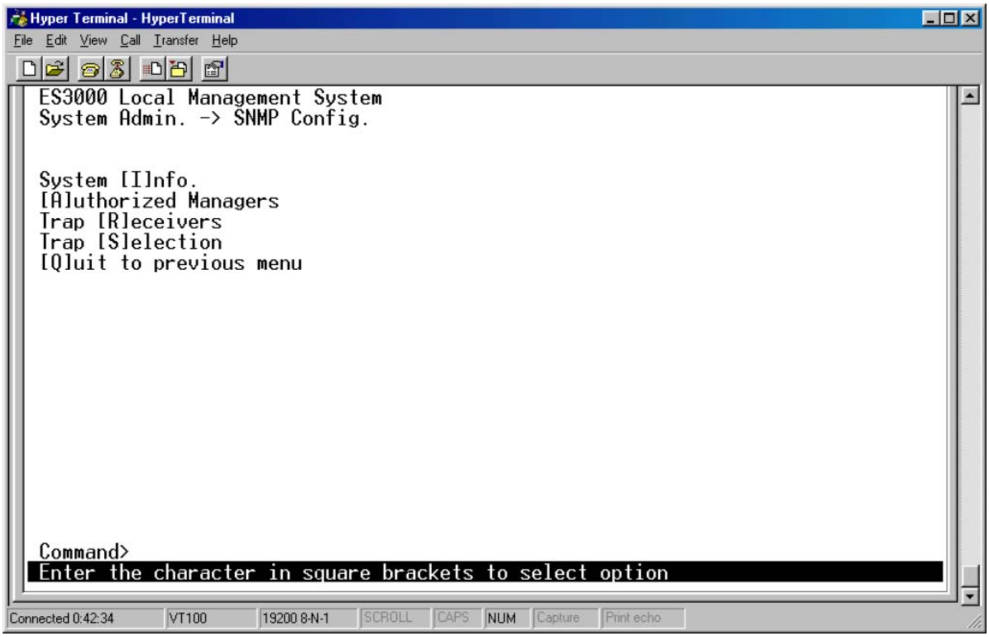
Use the **SNMP Configuration** menu to manage the ES3000 switch using the Simple Network Management Protocol (SNMP) from a network management station. Configure the switch to participate in the SNMP community and add the SNMP host agent to the host table. This prevents unauthorized SNMP access to the switch from non-approved SNMP hosts.

SNMP management features on the switch include:

- Simple Network Management Protocol (SNMP)
- Support Standard MIBs:
  - MIB II (RFC1213)
  - Ethernet Interface MIB (RFC1643)
  - Bridge MIB (RFC1493)
  - Private Enterprise MIB
  - 4-Group RMON (RFC1757)

The SNMP Configuration page has four options:

- System Information
- Authorized Managers
- Trap Receivers
- Trap Selection

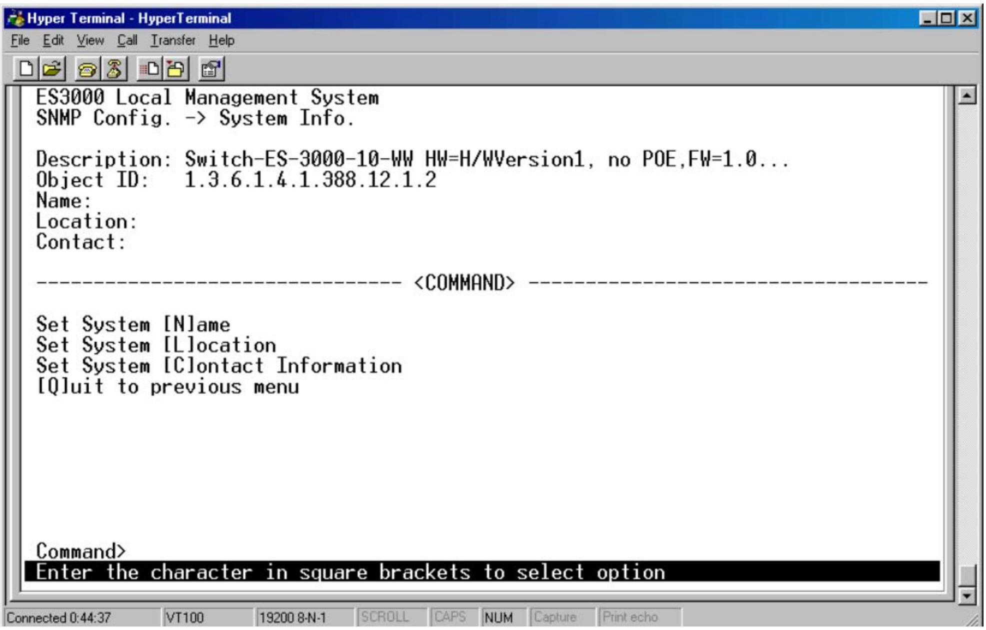

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
System Admin. -> SNMP Config.


System [I]nfo.
[A]uthorized Managers
Trap [R]eceivers
Trap [S]election
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

Connected 0:42:34
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.6 Main Menu->SNMP Config.->System Information

Use the **System Information** page to display system information to set the system name, location, and contact information. The MAC address and Object ID are also shown, but the MAC address and Object ID are not user configurable.



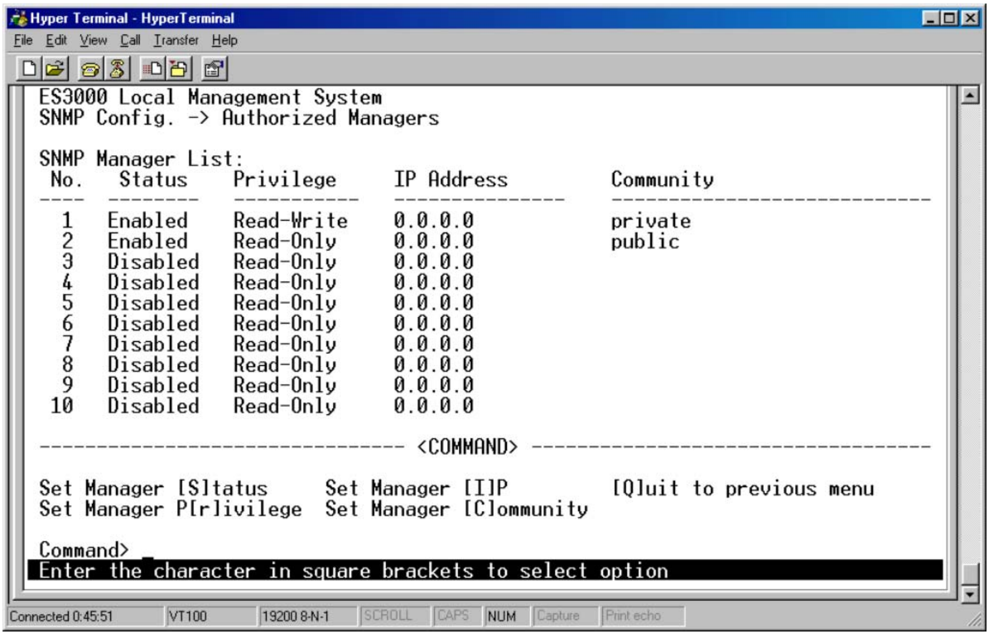
Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
SNMP Config. -> System Info.

Description: Switch-ES-3000-10-WW HW=H/WVersion1, no POE,FW=1.0...
Object ID:   1.3.6.1.4.1.388.12.1.2
Name:
Location:
Contact:

------------------------------- <COMMAND> ----------------------------------

Set System [N]ame
Set System [L]ocation
Set System [C]ontact Information
[Q]uit to previous menu





Command>
Enter the character in square brackets to select option
```

Connected 0:44:37
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.7 Main Menu->SNMP Config.->Authorized Managers

Use the **Authorized Managers** page to list the SNMP managers and their associated information. There are two community strings in default mode, private and public. Read-only is allowed with public and read-write is granted to private. Change the two community strings as required.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
SNMP Config. -> Authorized Managers

SNMP Manager List:
 No.   Status     Privilege     IP Address         Community
----  --------   -----------   ---------------    ----------------------------
  1   Enabled    Read-Write    0.0.0.0            private
  2   Enabled    Read-Only     0.0.0.0            public
  3   Disabled   Read-Only     0.0.0.0
  4   Disabled   Read-Only     0.0.0.0
  5   Disabled   Read-Only     0.0.0.0
  6   Disabled   Read-Only     0.0.0.0
  7   Disabled   Read-Only     0.0.0.0
  8   Disabled   Read-Only     0.0.0.0
  9   Disabled   Read-Only     0.0.0.0
 10   Disabled   Read-Only     0.0.0.0

-------------------------------- <COMMAND> -----------------------------------

Set Manager [S]tatus      Set Manager [I]P          [Q]uit to previous menu
Set Manager P[r]ivilege   Set Manager [C]ommunity

Command> _
Enter the character in square brackets to select option
```

Four commands are available to set the Manager IP, community string, Status, Privilege, and IP address.

Set Manager IP: Sets the IP address of a specified community. The access is restricted to specified IP only.

Set Manager Community: Sets community string.

Set Manager Privilege: Sets the access privilege, 1 is Read-only and 2 is Read-Write.

Set Manager Status: Enables or disables a community string.

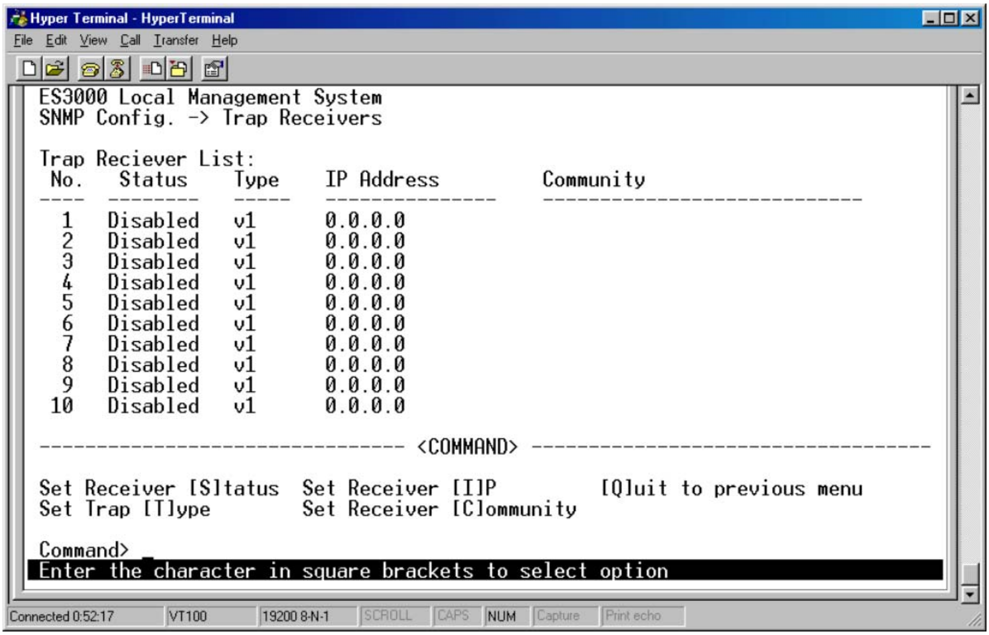
3.5.8 Main Menu->SNMP Config.->Trap Receiver Configuration

When Authentication Traps is **Enabled**, the system generates an SNMP trap upon a host authorization failure. The failure occurs when a host attempts to gain access to the system but the host IP is not in the SNMP host table.

Authentication Failure Trap

Enable	The system generates a SNMP trap upon a host authorization failure
Disable	The authentication traps are not generated

All hosts in community strings with TRAP privileges are notified when a trap condition occurs.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 0:52:17
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
SNMP Config. -> Trap Receivers

Trap Reciever List:
 No.   Status     Type    IP Address         Community
----  --------   -----   ---------------    ----------------------------
  1   Disabled   v1      0.0.0.0
  2   Disabled   v1      0.0.0.0
  3   Disabled   v1      0.0.0.0
  4   Disabled   v1      0.0.0.0
  5   Disabled   v1      0.0.0.0
  6   Disabled   v1      0.0.0.0
  7   Disabled   v1      0.0.0.0
  8   Disabled   v1      0.0.0.0
  9   Disabled   v1      0.0.0.0
 10   Disabled   v1      0.0.0.0

-------------------------------- <COMMAND> ------------------------------------

Set Receiver [S]tatus  Set Receiver [I]P         [Q]uit to previous menu
Set Trap [T]ype        Set Receiver [C]ommunity

Command> _
Enter the character in square brackets to select option
```

3.5.9 Main Menu->SNMP Config. ->Trap Selection

Three commands are available to configure individual trap parameters:

Enable/Disable Auth Fail Trap:	Enables or disables the authentication failure trap.
Add Link Down Trap Ports:	Add individual port onto the trap list.
Delete Link Down Trap Ports:	Delete individual port from the trap list.

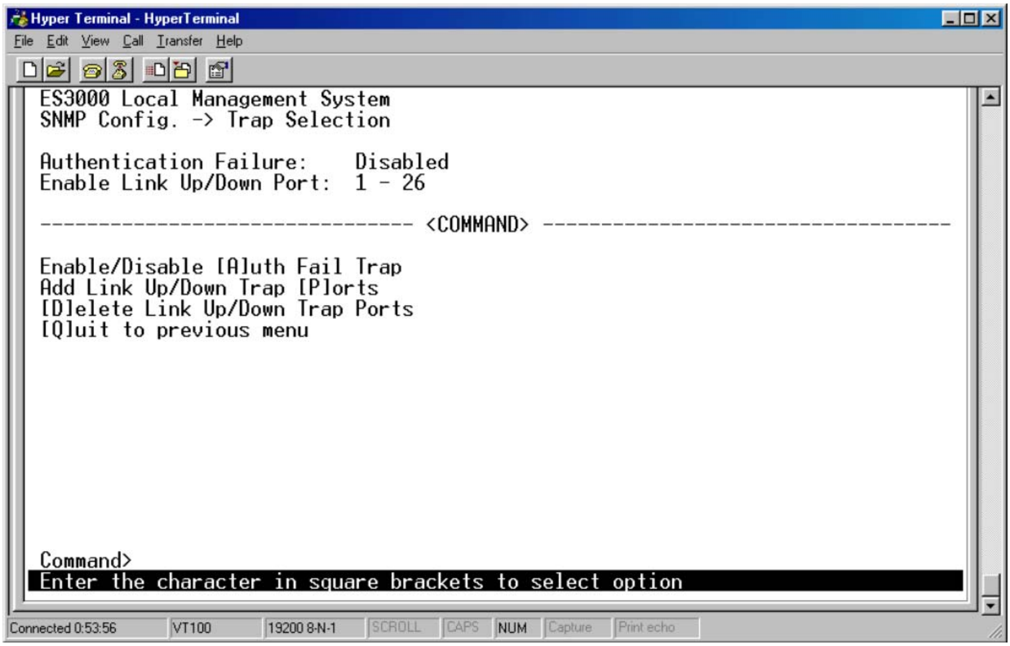
3.5.9.1 Port Link Down Trap

When on, the system generates an SNMP trap upon a port link down. This failure occurs when a link is disconnected. Therefore, symbol recommends each port be enabled and/or disabled independently.

3.5.9.2 Link Down Trap

Enable	The system generates a SNMP trap upon a port link down
Disable	The port link down trap is not generated upon a port link down

As authentication failure trap, all hosts in community strings with TRAP privileges are notified when a trap condition occurs.



Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
SNMP Config. -> Trap Selection

Authentication Failure:    Disabled
Enable Link Up/Down Port:  1 - 26

------------------------------- <COMMAND> ----------------------------------

Enable/Disable [A]uth Fail Trap
Add Link Up/Down Trap [P]orts
[D]elete Link Up/Down Trap Ports
[Q]uit to previous menu










Command>
Enter the character in square brackets to select option
```

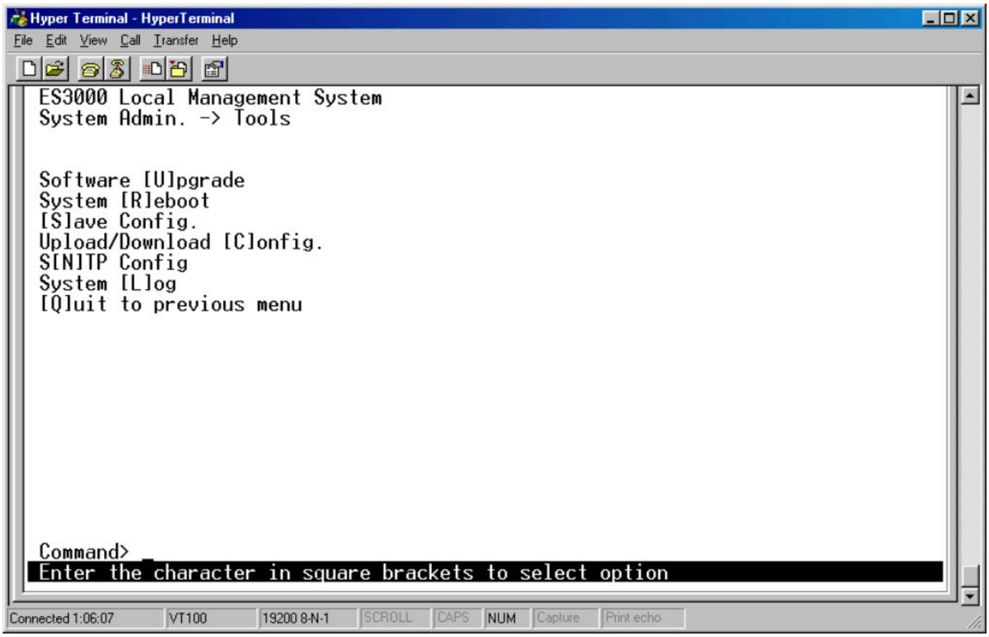
Connected 0:53:56
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.10 Main Menu->System Admin. ->Tools Menu

The Tools Menu has six options:

- Software Upgrade
- System Reboot
- Save Config.
- Upload/Download Config.
- SNTP Config
- System Log

These individual menu options are discussed in detail in the sections that follow.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:06:07
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
System Admin. -> Tools


Software [U]pgrade
System [R]eboot
[S]ave Config.
Upload/Download [C]onfig.
S[N]TP Config
System [L]og
[Q]uit to previous menu











Command> _
Enter the character in square brackets to select option
```

3.5.11 Main Menu->System Admin.->Tools->Software Upgrade

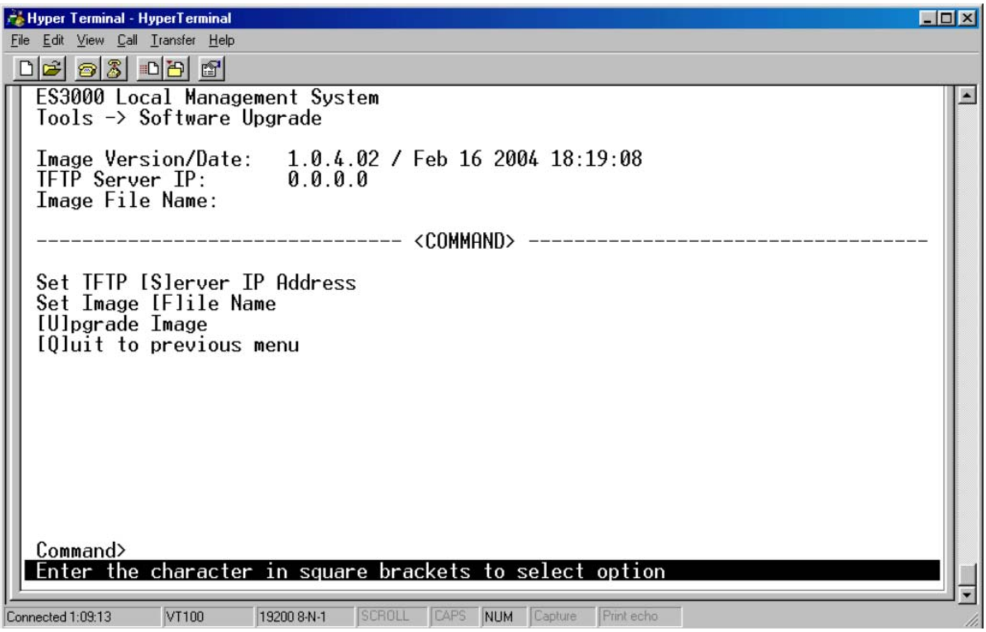
If new improvements to the software on the switch become available, use the Software Upgrade menu to upgrade the switch to the new software version. Once the IP address of the TFTP and the name of the new software image file are properly configured, the user can upgrade the software with command on this menu. See *Chapter 2, Firmware Upgrades* when updating software.

Warning

The previous version of runtime image is lost when the procedure completes.

Use the Software Upgrade menu for:

- Setting the TFTP Server IP Address
- Setting the Image File Name
- Upgrading the Image


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:09:13
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Tools -> Software Upgrade

Image Version/Date:   1.0.4.02 / Feb 16 2004 18:19:08
TFTP Server IP:       0.0.0.0
Image File Name:

-------------------------------- <COMMAND> -----------------------------------

Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image
[Q]uit to previous menu






Command>
Enter the character in square brackets to select option
```

3.5.12 Main Menu->System Admin.->Tools->System Reboot

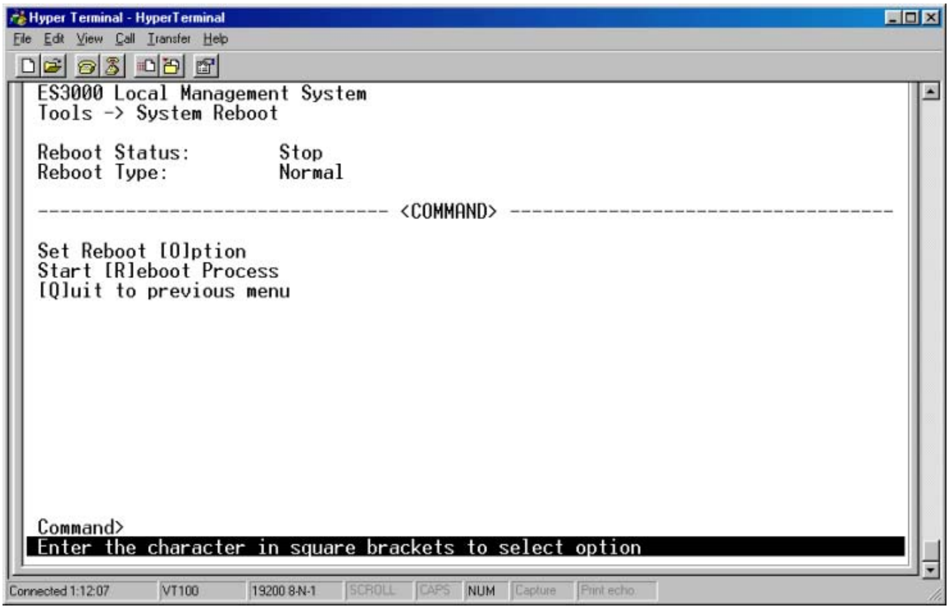
When the system reboots, reboot **Status** and reboot **Type** options display:

Reboot Status:

Stop	The switch is powered down.
Normal	The switch conducts a warm reboot as normal when rebooted.

Reboot Type:

Normal	Reboot with current runtime code and configuration.
Factor-Default	The switch runs as factor default after reboot. Symbol recommends Factor-Default if the previous configuration crashed.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:12:07
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

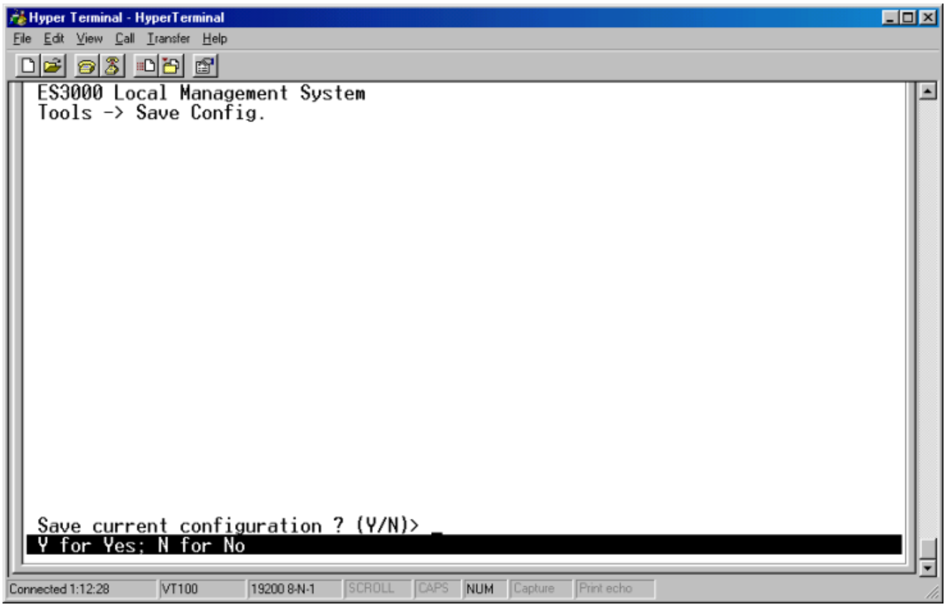
```
ES3000 Local Management System
Tools -> System Reboot

Reboot Status:        Stop
Reboot Type:          Normal

------------------------------ <COMMAND> ----------------------------------

Set Reboot [O]ption
Start [R]eboot Process
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

3.5.13 Main Menu->System Admin.->Tools->Save Config.

Save updated settings to Flash once changes to the screens within the console interface have been made. Use the *Save Config* screen as the central location to save changes made within the ES3000 Ethernet Switch menu-driven interface. Once updates have been saved to the system using the Save Config page, refer back to the target configuration screen to ensure the changes have been implemented by the ES3000 Ethernet Switch.

Select **Save Configuration** and use either **Enter** or **Y** to save the configuration to Flash.

Note: Network IP settings (IP address, Gateway Address, Network Mask) are not be affected by the Save Configuration command.

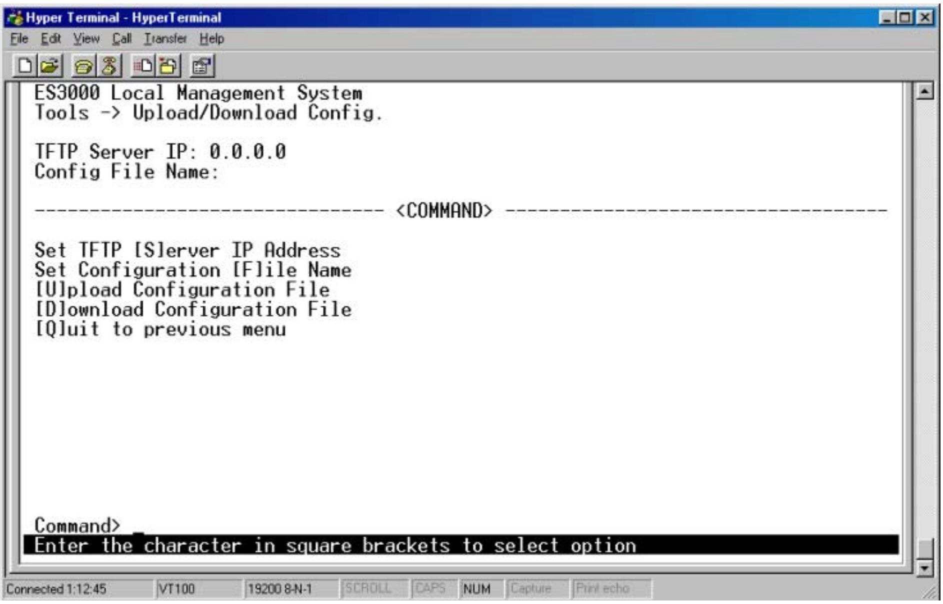

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:12:28
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
 ES3000 Local Management System
 Tools -> Save Config.

 Save current configuration ? (Y/N)> _
 Y for Yes; N for No
```

3.5.14 Main Menu->System Admin. ->Tools ->Upload/Download Config.

There are four configurable functions within the Upload/Download Configuration page:

Set TFTP Server IP Address	user can enter the server IP address to get the TFTP server.
Set Configuration File Name	user can enter the file name that they want to config
Upload Configuration File	user can upload the configuration file
Download Configuration File	user can download configuration file from a TFTP server

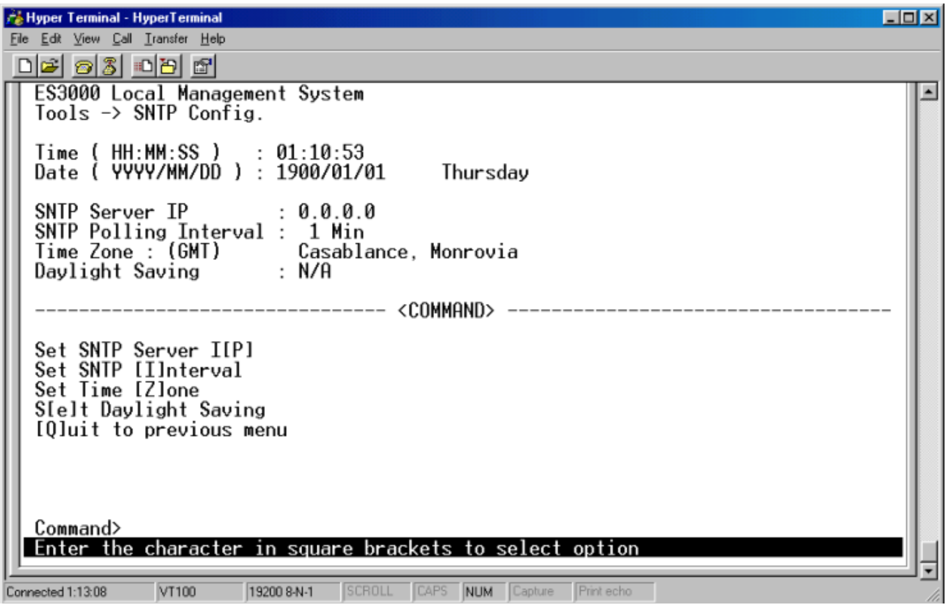

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:12:45
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Tools -> Upload/Download Config.

TFTP Server IP: 0.0.0.0
Config File Name:

-------------------------------- <COMMAND> -----------------------------------

Set TFTP [S]erver IP Address
Set Configuration [F]ile Name
[U]pload Configuration File
[D]ownload Configuration File
[Q]uit to previous menu







Command> _
Enter the character in square brackets to select option
```

3.5.15 Main Menu->System Admin.->Tools->SNTP Config.

There are configurable functions in the SNTP Configuration page:

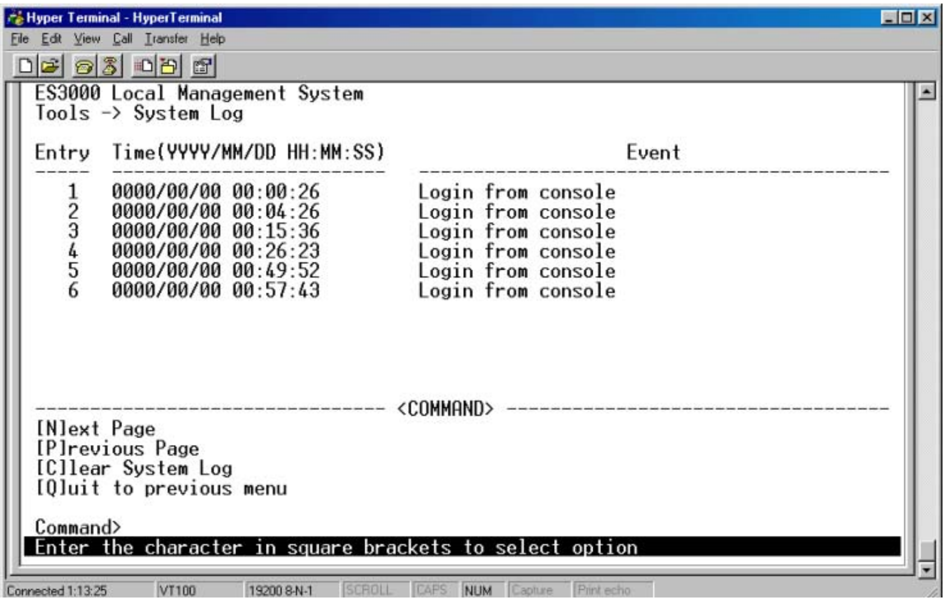
Set SNTP Server IP	Simple Network Time Protocol, the user can enter SNTP server IP to gain access.
Set SNTP Interval	Set SNTP polling interval.
Set Time Zone	Set the time zone
Set Daylight Saving	Set the daylight saving… or ignore it


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:13:08
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Tools -> SNTP Config.

Time ( HH:MM:SS )   : 01:10:53
Date ( YYYY/MM/DD ) : 1900/01/01     Thursday

SNTP Server IP        : 0.0.0.0
SNTP Polling Interval :  1 Min
Time Zone : (GMT)       Casablance, Monrovia
Daylight Saving       : N/A

-------------------------------- <COMMAND> -----------------------------------

Set SNTP Server I[P]
Set SNTP [I]nterval
Set Time [Z]one
S[e]t Daylight Saving
[Q]uit to previous menu



Command>
Enter the character in square brackets to select option
```

3.5.16 Main Menu->System Admin.->Tools->System Log

The System Log is a tool for observing system behavior. Clear the system log by selecting **Clear System Log**. Symbol recommends referring to the System Log when contacting the Support Center to determine if an ES3000 event has been recorded.

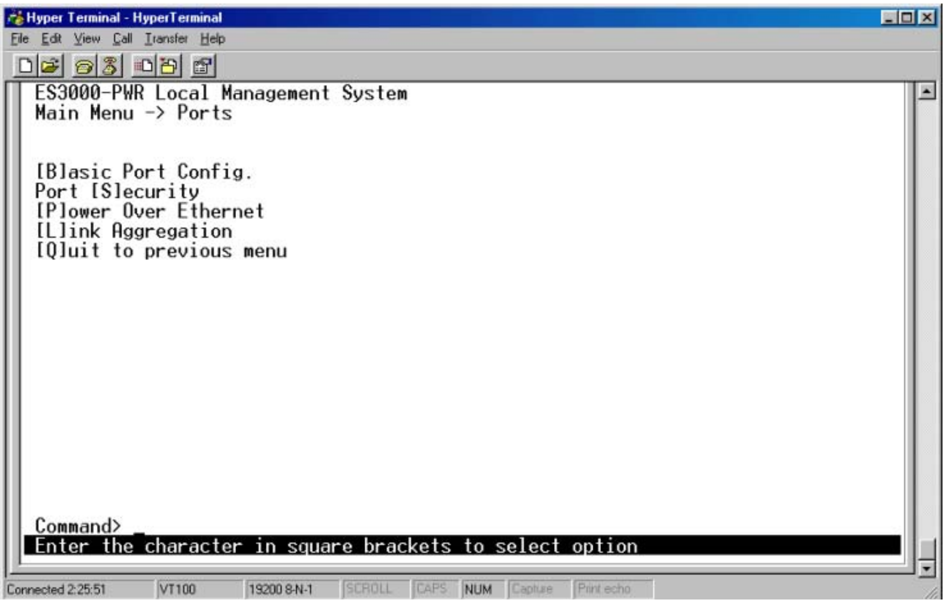


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:13:25
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Tools -> System Log

Entry  Time(YYYY/MM/DD HH:MM:SS)                          Event
-----  -------------------------    -------------------------------------------
  1    0000/00/00 00:00:26          Login from console
  2    0000/00/00 00:04:26          Login from console
  3    0000/00/00 00:15:36          Login from console
  4    0000/00/00 00:26:23          Login from console
  5    0000/00/00 00:49:52          Login from console
  6    0000/00/00 00:57:43          Login from console




-------------------------------- <COMMAND> ----------------------------------
[N]ext Page
[P]revious Page
[C]lear System Log
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

3.5.17 Main Menu->Port Configuration Menu

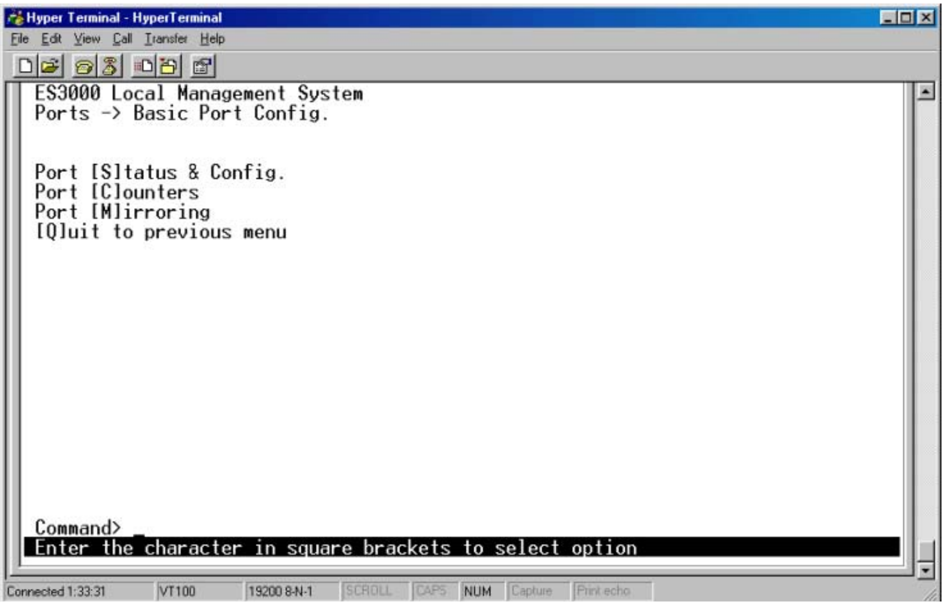
Use the **Port Configuration menu** to set the port characteristics related to link operations. All of the parameters on the Port Configuration page are toggle settings. To change, or toggle, between options, select **Ctrl-M** to move the curser to the ports field and strike the space bar when the appropriate option is highlighted. To modify ports 17 to 26, tab through ports 1 to 16. The comments field is available to enter a description of the port.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:25:51
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000-PWR Local Management System
Main Menu -> Ports


[B]asic Port Config.
Port [S]ecurity
[P]ower Over Ethernet
[L]ink Aggregation
[Q]uit to previous menu










Command> _
Enter the character in square brackets to select option
```

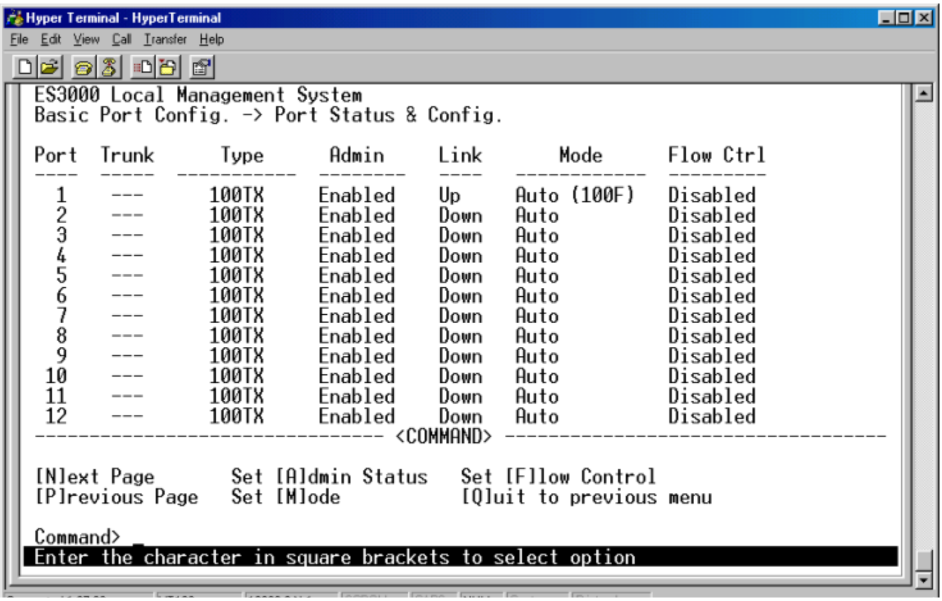
3.5.18 Main Menu->Ports->Basic Port Config.

Use the **Basic Port Configuration** menu to configure port status (link type, admin enable/disable, link up/down, mode, and flow control). To mirror other ports, select **Port Mirroring**.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:33:31
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Ports -> Basic Port Config.


Port [S]tatus & Config.
Port [C]ounters
Port [M]irroring
[Q]uit to previous menu











Command> _
Enter the character in square brackets to select option
```

3.5.19 Main Menu->Ports->Basic Port Config.->Port Status & Config.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
Basic Port Config. -> Port Status & Config.

Port  Trunk     Type        Admin     Link     Mode         Flow Ctrl
----  -----  -----------  --------    ----  ------------   ---------
  1    ---      100TX     Enabled     Up    Auto (100F)    Disabled
  2    ---      100TX     Enabled     Down  Auto           Disabled
  3    ---      100TX     Enabled     Down  Auto           Disabled
  4    ---      100TX     Enabled     Down  Auto           Disabled
  5    ---      100TX     Enabled     Down  Auto           Disabled
  6    ---      100TX     Enabled     Down  Auto           Disabled
  7    ---      100TX     Enabled     Down  Auto           Disabled
  8    ---      100TX     Enabled     Down  Auto           Disabled
  9    ---      100TX     Enabled     Down  Auto           Disabled
 10    ---      100TX     Enabled     Down  Auto           Disabled
 11    ---      100TX     Enabled     Down  Auto           Disabled
 12    ---      100TX     Enabled     Down  Auto           Disabled
-------------------------------- <COMMAND> -----------------------------------

[N]ext Page         Set [A]dmin Status    Set [F]low Control
[P]revious Page     Set [M]ode            [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

The **Port Status & Configuration** menu contains the following editable fields:

Type

The type of a port, this field is not user configurable.

Admin field

Enables or disables the port.

Link

The status of a port. The status is **Up** when a port is connected and active.

Mode

Provides the choice of Full-duplex, Half-duplex, or Auto negotiation as well as speed selection among 10Mbps, 100Mbps, 1000Mbps, or auto negotiation. Enabling auto-negotiation on a port allows a port to sense the communication speed and negotiate the duplex mode (full duplex or half duplex) automatically. The ports select the highest possible throughput. The port can auto-negotiate with any port compliant with IEEE 802.3u. If the other port is not IEEE802.3u compliant, the port defaults to half-duplex (10 Mbps mode). Users can operate the communication speed and duplex mode manually.

Flow Control

Enables or disables Flow Control. Flow control is a protocol preventing packets from being dropped by reducing the amount of traffic to a level that can be accommodated. If enabled on both ends of a connection, it prevents the sender from sending data until the receiver can accept it. This switch complies with the IEEE802.3x flow control standard.

Gigabit Ports

The port type can be chosen for the two-gigabit ports on each switch. The default is the port using the RJ-45 interface. Select the GBIC interface by plugging a GBIC connector. The GBIC interface has higher priority than the shared RJ-45 interface.

> **Note** Enabling the GBIC connector for a Gigabit Ethernet port disables the built-in 1000BASE-T port. GBIC ports do not support Auto Negotiation. Manually configure the GBIC port. The default values are 1000 Mbps, full duplex.

Five commands are available on the menu: Set Admin Status, Set Flow Control, Set Mode, Next Page, and Previous Page.

Set Admin Status: Enable or disable the admin. status of a port.

Set Flow Control: Enable or disable flow control of a port.

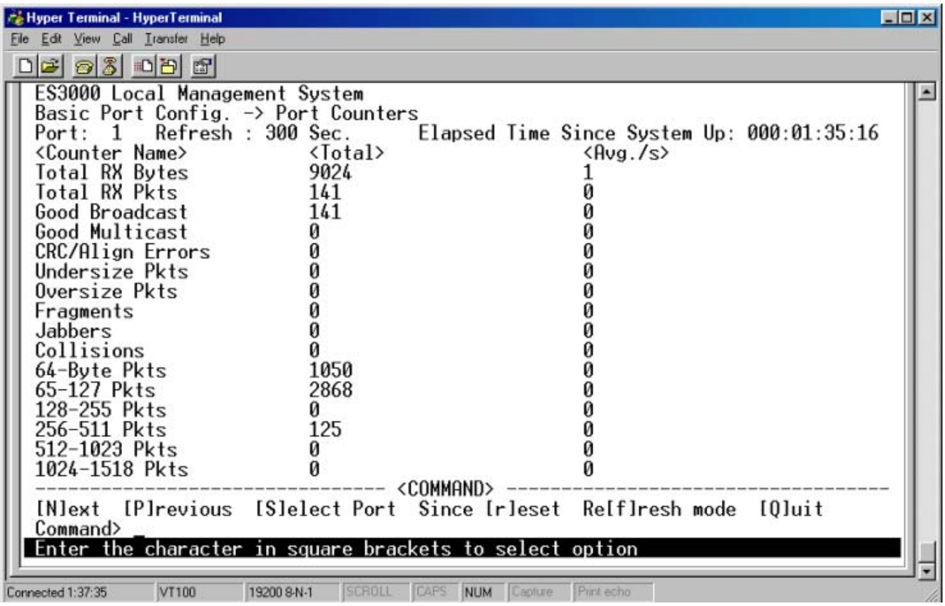
Set Mode: Manually configure the speed and operation mode of a port. The first 24 ports have two speeds, 10 or 100Mbps while the last two gigabit ports has three speeds, 10, 100, and 1000Mbps. Two operation modes, half and full duplex, are available for 10 and 100Mbps but only full duplex is allowed on 1000Mbps. When the command is issued, two short keys, A and N, are displayed. The A stands for automatic and N stands for non-automatic. Choose N to manually configure a port.

Next Page: Show the next 12 ports' information.

Previous Page: Show the previous 12 ports' information.

3.5.20 Main Menu->Ports->Basic Port Config->Port Counters

Use the **Port Counters** menu to select the port where information is required. Refer to the **Total** and **Avg./s** lists for individual port information. Reset the ES3000 to retrieve the latest information immediately. The Refresh mode is to set to a defined refresh interval.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:37:35
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Basic Port Config. -> Port Counters
Port:  1   Refresh : 300 Sec.     Elapsed Time Since System Up: 000:01:35:16
<Counter Name>          <Total>                    <Avg./s>
Total RX Bytes          9024                       1
Total RX Pkts           141                        0
Good Broadcast          141                        0
Good Multicast          0                          0
CRC/Align Errors        0                          0
Undersize Pkts          0                          0
Oversize Pkts           0                          0
Fragments               0                          0
Jabbers                 0                          0
Collisions              0                          0
64-Byte Pkts            1050                       0
65-127 Pkts             2868                       0
128-255 Pkts            0                          0
256-511 Pkts            125                        0
512-1023 Pkts           0                          0
1024-1518 Pkts          0                          0
---------------------------------- <COMMAND> -----------------------------------
[N]ext  [P]revious  [S]elect Port  Since [r]eset  Re[f]resh mode  [Q]uit
Command> _
Enter the character in square brackets to select option
```

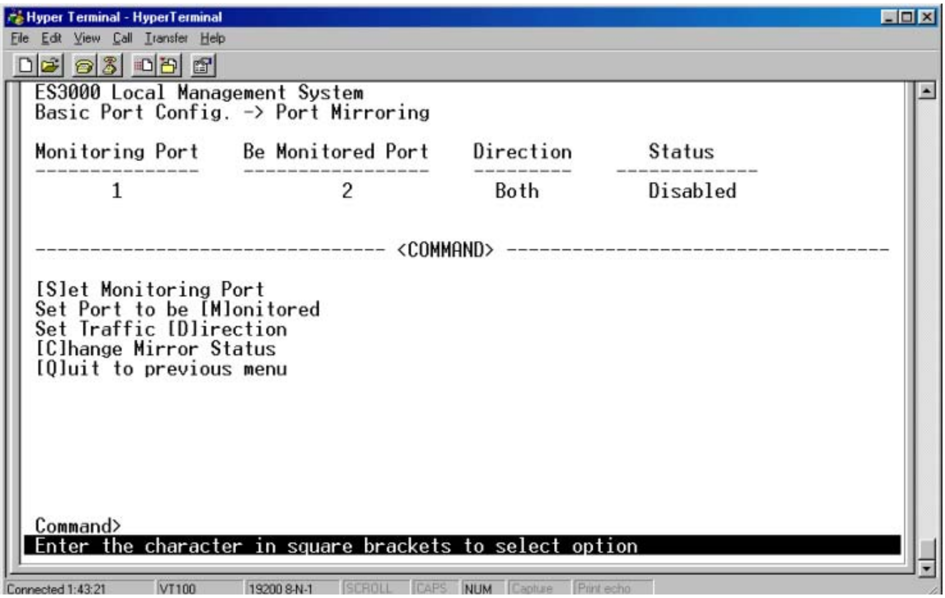
3.5.21 Main Menu->Ports->Basic Port Config->Port Mirroring

Port mirroring allows one port on the ES3000 to see all of the packets passing through any other port on the switch. Usually, a network analyzer is attached to the monitoring port so the network administrator can debug problems with the monitored port.

The ES3000 has two gigabit Ethernet ports, ports 25 and 26. A 10/100BaseT port would not be able to keep up with the packet flow on a gigabit port. Only another gigabit port may monitor a gigabit port. Any port on the ES3000 may be used to monitor ports 1 through 24, the 10/100BaseT ports.

Use the **Port Mirroring** menu to designate a port for monitoring traffic from a listed port or a single VLAN on the switch. The switch monitors network activity by copying traffic from the specified monitoring sources to the designated monitoring port. There are four commands within the menu:

Set Monitoring Port:	Sets the monitoring port. All traffic is forwarded to this port.
Set Port to be Monitored:	Sets the monitored port. All traffic through this port is forwarded to the monitoring port.
Set Traffic Direction:	Sets the direction of monitored traffic, receiving(R), transmission(T), or both direction(B).
Change Mirror Status:	Enables or disables the mirror status.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:43:21
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Basic Port Config. -> Port Mirroring

Monitoring Port    Be Monitored Port    Direction      Status
---------------    -----------------    ---------    -------------
       1                   2               Both        Disabled


-------------------------------- <COMMAND> -----------------------------------

[S]et Monitoring Port
Set Port to be [M]onitored
Set Traffic [D]irection
[C]hange Mirror Status
[Q]uit to previous menu






Command>
Enter the character in square brackets to select option
```

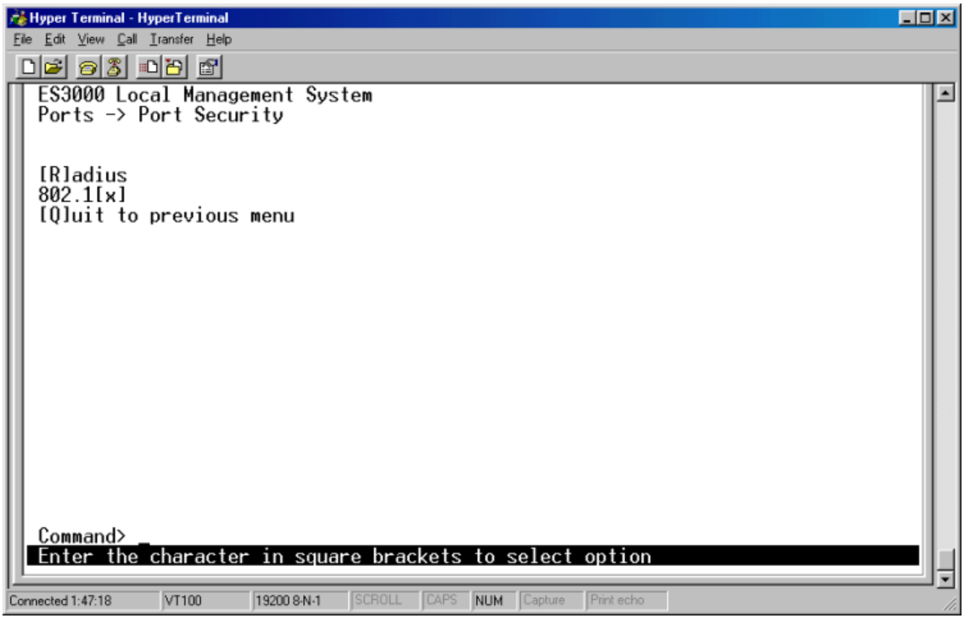
3.5.22 Main Menu->Ports->Port Security

Use the **Port Security** screen to enable or disable the Web, SNMP, and/or telnet interfaces or change the user name and password. User names and passwords are case sensitive and can be up to 20 characters long.

Note When using telnet, the user can only enable/disable the Web interface. The user cannot enable/disable the telnet interface.

There are two functions in the Port Security page:

- Radius
- 802.1x

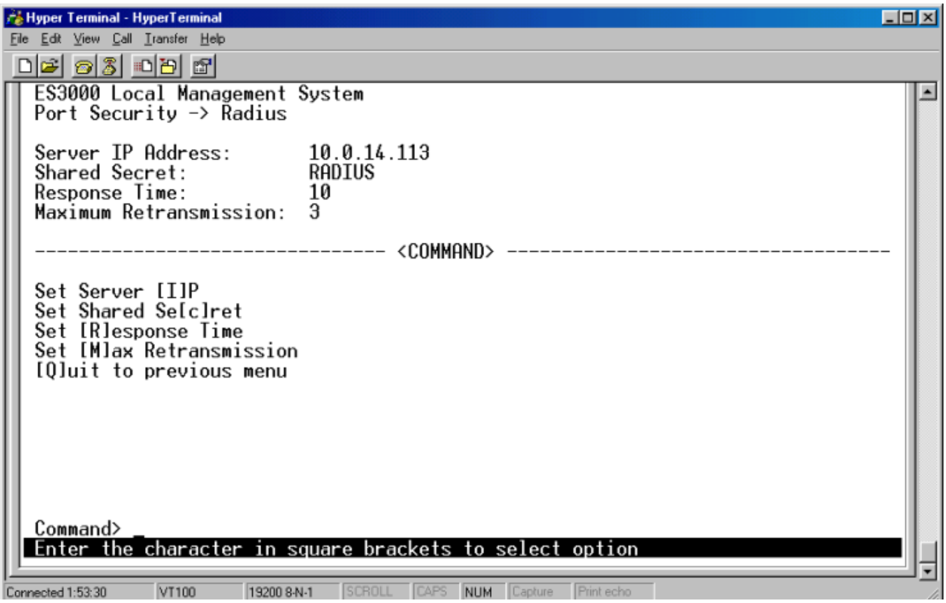

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
Ports -> Port Security


[R]adius
802.1[x]
[Q]uit to previous menu














Command> _
Enter the character in square brackets to select option
```

Connected 1:47:18
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.23 Main Menu->Ports->Port Security->Radius

Use the **Radius** menu option to configure the advanced security settings of the switch to limit the access to the management interfaces. There are two advanced security options beyond the basic password protection: RADIUS client authentication and 802.1X port authentication. If the user has a RADIUS server on the network, authentication of management access can be conducted through the RADIUS server. This does not affect traffic passing through the switch, but only authenticates access to the switch management. The same is true for 802.1X port authentication. Allow only users with specific IP addresses to access the management features, thus preventing unauthorized personnel from accessing the switch. The 802.1X is located in the Advanced Switch Configuration->Port Base Access Control Configuration Menu.

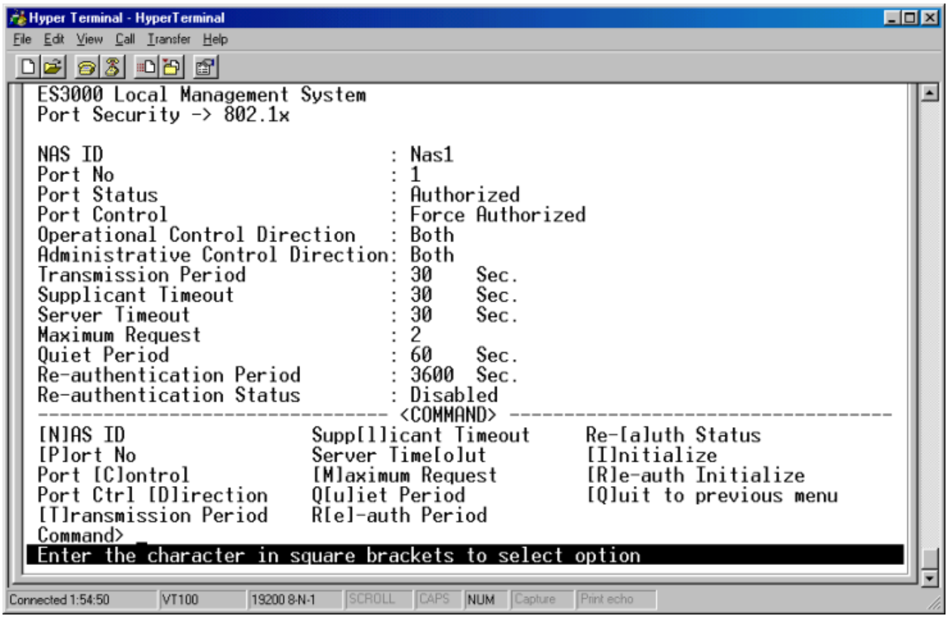

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:53:30 VT100 19200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
ES3000 Local Management System
Port Security -> Radius

Server IP Address:       10.0.14.113
Shared Secret:           RADIUS
Response Time:           10
Maximum Retransmission:  3

-------------------------------- <COMMAND> -----------------------------------

Set Server [I]P
Set Shared Se[c]ret
Set [R]esponse Time
Set [M]ax Retransmission
[Q]uit to previous menu





Command> _
Enter the character in square brackets to select option
```

3.5.24 Main Menu->Ports->Port Security ->802.1x

Use the **802.1x** menu to configure the NAS ID used for connection, the port to pass the security, the port control type, the operational or administrative control direction, the transmission period (30sec.), the supplicant requiring and server responding time, the maximum request times and the quiet period if there is no any activity on the ES3000.

Configure the up re-authentication period when re-authentication status is **Enabled**. Go back to the initial status by initializing or re-authentication initializing.

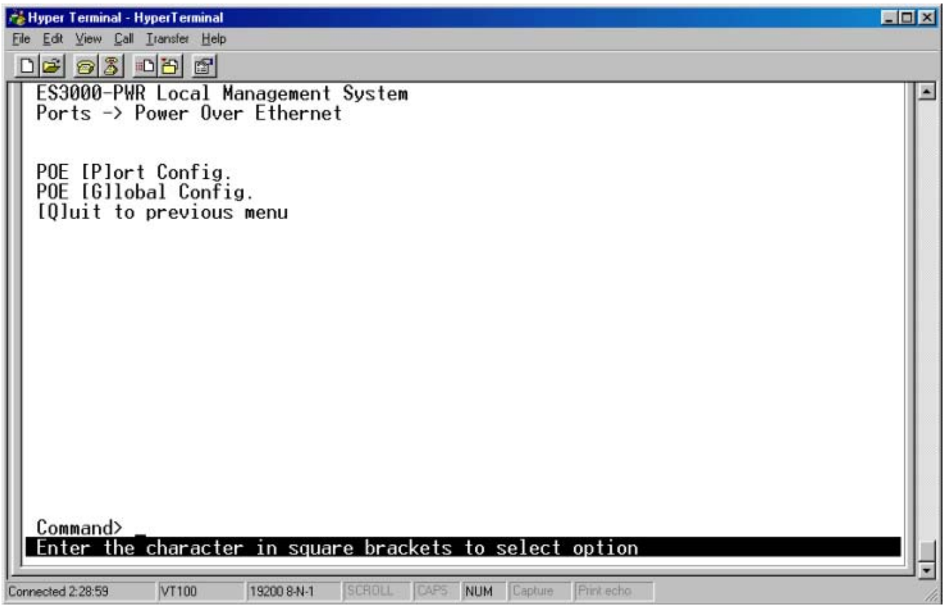

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:54:50
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Port Security -> 802.1x

NAS ID                           : Nas1
Port No                          : 1
Port Status                      : Authorized
Port Control                     : Force Authorized
Operational Control Direction    : Both
Administrative Control Direction: Both
Transmission Period              : 30    Sec.
Supplicant Timeout               : 30    Sec.
Server Timeout                   : 30    Sec.
Maximum Request                  : 2
Quiet Period                     : 60    Sec.
Re-authentication Period         : 3600  Sec.
Re-authentication Status         : Disabled
-------------------------------- <COMMAND> -----------------------------------
[N]AS ID                    Supp[l]icant Timeout      Re-[a]uth Status
[P]ort No                   Server Time[o]ut          [I]nitialize
Port [C]ontrol              [M]aximum Request         [R]e-auth Initialize
Port Ctrl [D]irection       Q[u]iet Period            [Q]uit to previous menu
[T]ransmission Period       R[e]-auth Period
Command> _
Enter the character in square brackets to select option
```

3.5.25 Main Menu->Ports->Power over Ethernet

Use Power-over-Ethernet (PoE) to eliminate using a 110/220 VAC power source to power access points and other devices on a wired LAN. If using a Power-over-Ethernet system, only a single CAT5 Ethernet cable carrying both power and data to each device is required. The single cable scheme provides greater flexibility in the placement of access points and network devices and can significantly decrease installation costs.

Two configuration pages exist for the PoE function. The first allows per port configuration for specific power restrictions on an individual port basis. The second configuration page is used for global configurations that apply switch-wide.



Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:28:59
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000-PWR Local Management System
Ports -> Power Over Ethernet


POE [P]ort Config.
POE [G]lobal Config.
[Q]uit to previous menu














Command> _
Enter the character in square brackets to select option
```

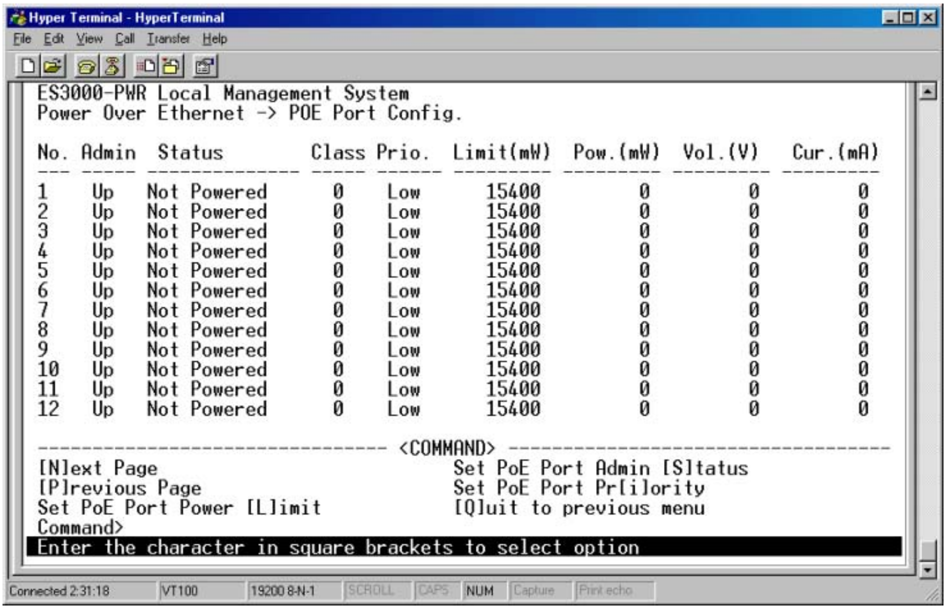
Two functions are provided for the PoE control,

Port Configuration

Admin. status: The status of administration for a port.

Priority: Priority of a PoE port. Three selections are available, critical, high, and low. When the power consumption over the power budget, the critical has higher priority on power supplying.

Limit(mW): The maximum power supplied to a port. The default is 15.4W or 15000mW.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:31:18
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000-PWR Local Management System
Power Over Ethernet -> POE Port Config.

No. Admin  Status         Class Prio.  Limit(mW)  Pow.(mW)  Vol.(V)   Cur.(mA)
--- -----  -------------- ----- ------ ---------  --------- --------- ---------
1    Up   Not Powered       0    Low     15400        0         0         0
2    Up   Not Powered       0    Low     15400        0         0         0
3    Up   Not Powered       0    Low     15400        0         0         0
4    Up   Not Powered       0    Low     15400        0         0         0
5    Up   Not Powered       0    Low     15400        0         0         0
6    Up   Not Powered       0    Low     15400        0         0         0
7    Up   Not Powered       0    Low     15400        0         0         0
8    Up   Not Powered       0    Low     15400        0         0         0
9    Up   Not Powered       0    Low     15400        0         0         0
10   Up   Not Powered       0    Low     15400        0         0         0
11   Up   Not Powered       0    Low     15400        0         0         0
12   Up   Not Powered       0    Low     15400        0         0         0

-------------------------------- <COMMAND> ---------------------------------
[N]ext Page                            Set PoE Port Admin [S]tatus
[P]revious Page                        Set PoE Port Pr[i]ority
Set PoE Port Power [L]imit             [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

Global Configuration

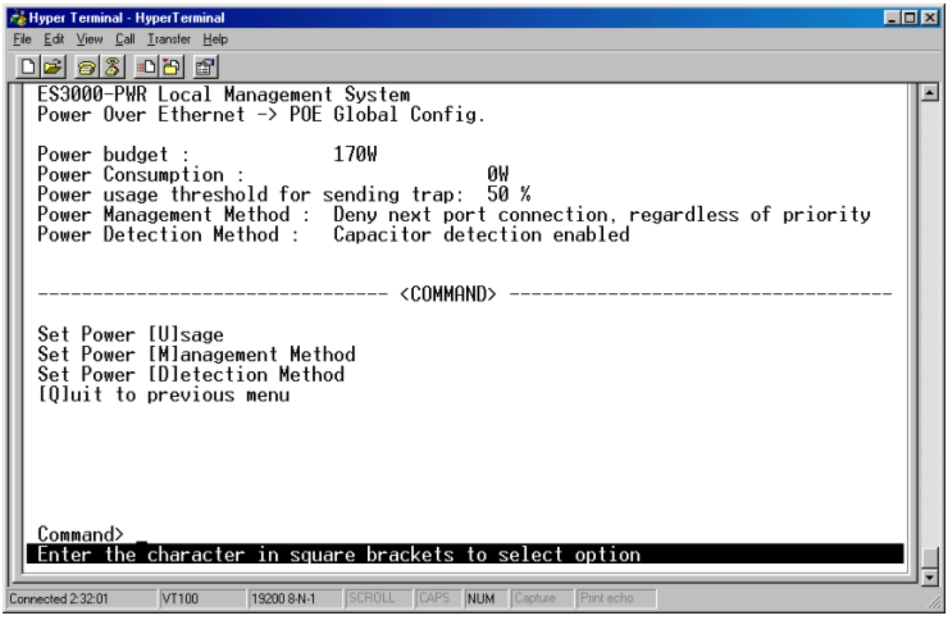
Power Usage: Sets the power usage threshold for sending a trap.

Management Method: The action to take when the power sink over the power budget, use one of the following:

1) Low priority port is shut down;

2) Deny next port connection.

Detection Method: Enables or disables the power capacitor detection.

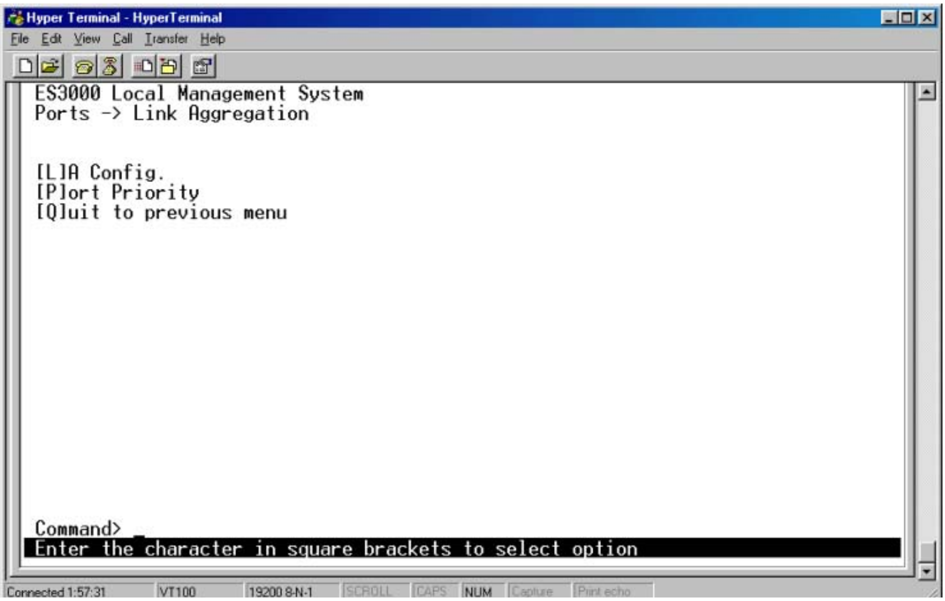

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000-PWR Local Management System
Power Over Ethernet -> POE Global Config.

Power budget :              170W
Power Consumption :                        0W
Power usage threshold for sending trap:   50 %
Power Management Method :   Deny next port connection, regardless of priority
Power Detection Method :    Capacitor detection enabled


-------------------------------- <COMMAND> -----------------------------------

Set Power [U]sage
Set Power [M]anagement Method
Set Power [D]etection Method
[Q]uit to previous menu







Command> _
Enter the character in square brackets to select option
```

3.5.26 Main Menu->Ports->Link Aggregation

Use the **Link Aggregation** menu to allow multiple links between switches to work as one virtual link (aggregate link). Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, trunks can only be formed within the same bank. A bank is a set of eight ports. Up to four trunks can be operating at the same time. Toggle the ports to the correct trunk number to set up a trunk.

Click **Apply** to enable the trunk. Spanning Tree treats trunked ports as a single virtual port.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:57:31
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

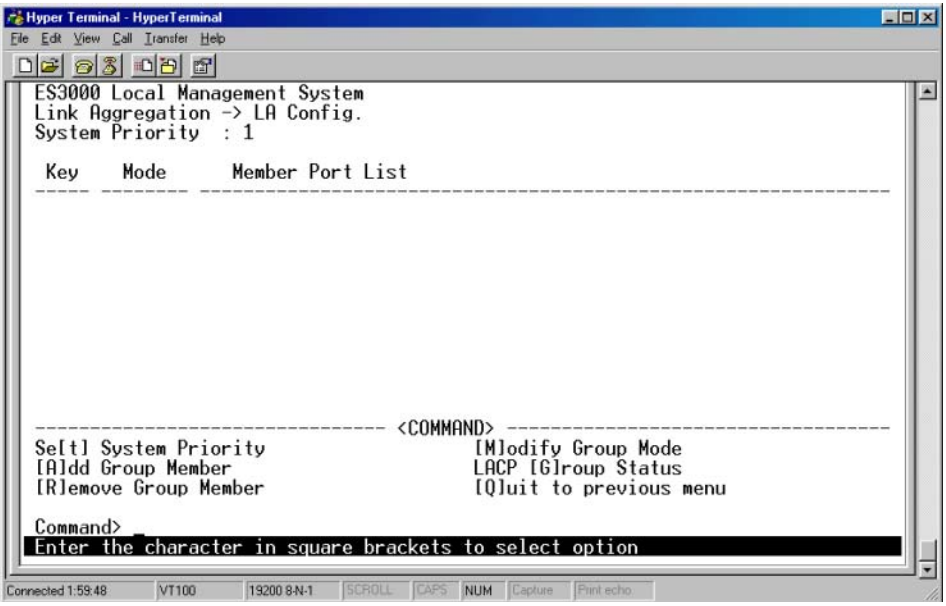
```
ES3000 Local Management System
Ports -> Link Aggregation


[L]A Config.
[P]ort Priority
[Q]uit to previous menu










Command> _
Enter the character in square brackets to select option
```

3.5.27 Main Menu->Ports->Link Aggregation->LA Config

Use the LA Configuration menu to define multiple links between switches to work as one virtual link or aggregate link. Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. Spanning Tree treats trunked ports as a single virtual port.

Note

Straight-though cables are required for all links in the trunk. Do not use crossover cables. Disable auto-negotiation on the ports in a trunk prior to setting up the trunk.

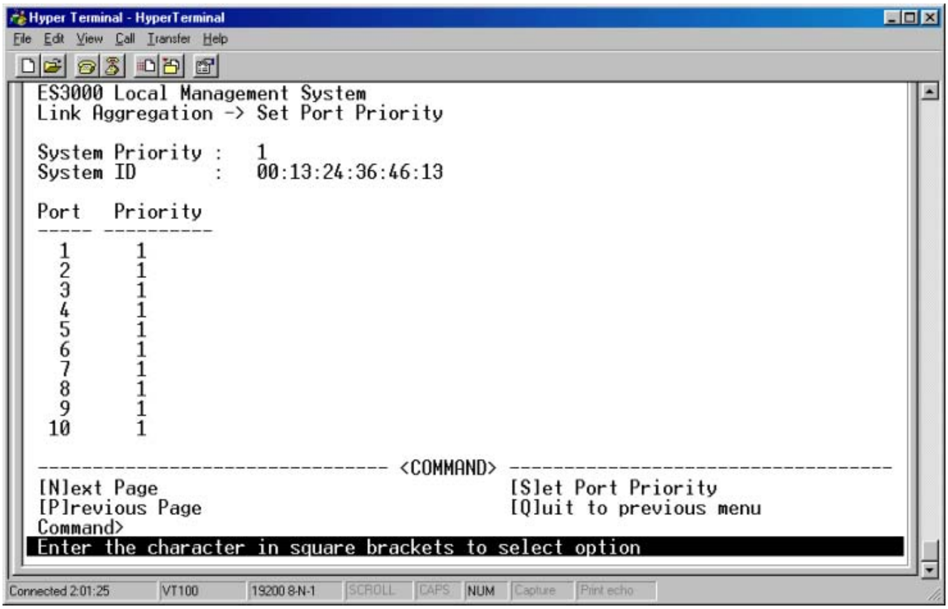


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:59:48
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Link Aggregation -> LA Config.
System Priority  : 1

 Key    Mode      Member Port List
----- -------- ---------------------------------------------------------------







---------------------------------- <COMMAND> ----------------------------------
Se[t] System Priority                    [M]odify Group Mode
[A]dd Group Member                       LACP [G]roup Status
[R]emove Group Member                    [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

3.5.28 Main Menu->Ports->Link Aggregation->Set Port Priority

The default system priority is the same in all ports. If configuring a port with different priority in the link aggregation, go to **set port priority** to configure the port priority.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:01:25 VT100 19200 8-N-1 SCROLL CAPS NUM Capture Print echo

```
ES3000 Local Management System
Link Aggregation -> Set Port Priority

System Priority :   1
System ID       :   00:13:24:36:46:13

Port   Priority
----- ----------
  1      1
  2      1
  3      1
  4      1
  5      1
  6      1
  7      1
  8      1
  9      1
 10      1

-------------------------------- <COMMAND> -----------------------------------
[N]ext Page                                [S]et Port Priority
[P]revious Page                            [Q]uit to previous menu
Command>
Enter the character in square brackets to select option
```

3.5.29 Main Menu>VLANs

A Virtual Local Area Network (VLAN) is a means to electronically separate ports on the same switch from a single broadcast domain into separate broadcast domains. By using a VLAN, users can group by logical function instead of physical location. There are 4096 VLANs supported on this switch. Two memberships are available for a VLAN member, tagged and untagged, abbreviated as T and U, respectively. If a port is an untagged member of a VLAN, the VLAN tag is striped from the frame before it is sent out that port. If the port is a tagged member of a VLAN, the VLAN tag stays in the frame when sent. If a port is not a member of the particular VLAN, it does not get any traffic for that VLAN. The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches.

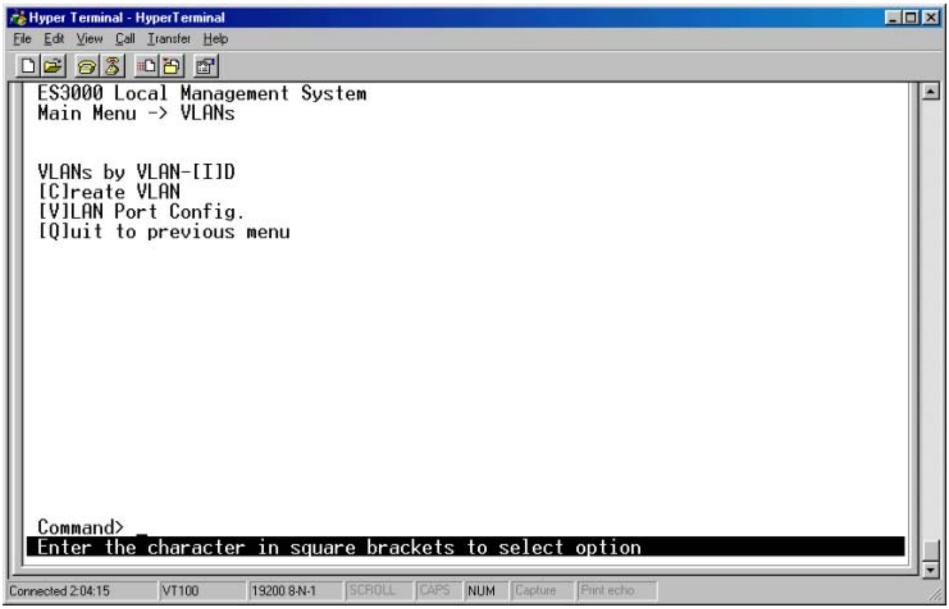
All untagged packets entering the switch by default are tagged with the ID specified by the port ID. Use the VLAN screen to specify the VLAN ID for each port. The number next to each port indicates which ID is set for each port. Following industry standards, ID 1 is the default ID.

Up to 4094 VLANs with unique ID numbers and names can be added. VLAN ID numbers are required to be within 1-4094. Per industry standard, the default VLAN has an ID of 1.

Note

VLAN ID #1 cannot be deleted under any circumstance.

3.5.30 Main Menu->VLANs->VLANs by VLAN-ID



```
ES3000 Local Management System
Main Menu -> VLANs


VLANs by VLAN-[I]D
[C]reate VLAN
[V]LAN Port Config.
[Q]uit to previous menu
```

```
Command> _
Enter the character in square brackets to select option
```

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:04:15
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Create a new VLAN, add new ports to an existing VLAN, remove ports from an existing VLAN, delete a VLAN, Set Management Status, and/or Set GVRP Status from the VLAN by VLAN-ID screen. Six commands are available:

Create VLAN: Creates a new VLAN, a unique ID is required.

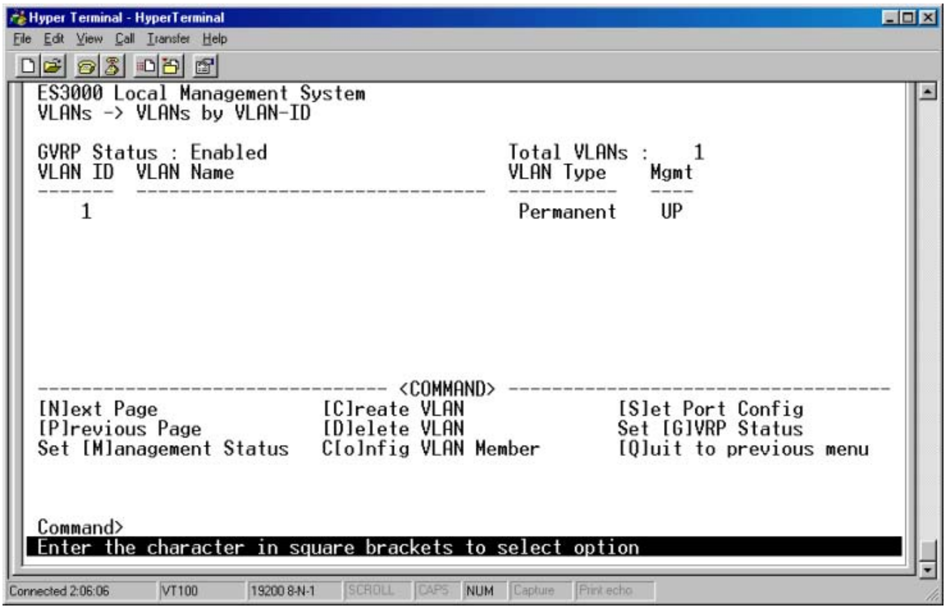
Delete VLAN: Deletes a VLAN ID. The entire setup for the VLAN is erased. VLAN # 1 cannot be deleted under any circumstance.

Config. VLAN Member: Configures the member of a VLAN

Set Port Config. Sets the configuration of a specified port

Set GVRP Status: Enables or disables the GVRP switch-wide.

Set Management Status: Enables or disables the management status of a static VLAN.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:06:06
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
VLANs -> VLANs by VLAN-ID

GVRP Status : Enabled                           Total VLANs :    1
VLAN ID  VLAN Name                              VLAN Type    Mgmt
-------  -------------------------------        ----------   ----
    1                                            Permanent    UP









-------------------------------- <COMMAND> -----------------------------------
[N]ext Page                 [C]reate VLAN              [S]et Port Config
[P]revious Page             [D]elete VLAN              Set [G]VRP Status
Set [M]anagement Status     C[o]nfig VLAN Member       [Q]uit to previous menu



Command>
Enter the character in square brackets to select option
```

To create a new VLAN Group:

1. Select **Create VLAN**.
2. Enter the VLAN ID and name in the provided fields.
3. Add VLAN members if so desired.
4. Click **Apply**.

To delete a VLAN Group:

1. Select **Delete VLAN**.
2. Give the corresponding VLAN ID.

To configure a VLAN Member:

1. Select **Delete VLAN.**
2. Give the corresponding VLAN ID.

To set the GARP VLAN registration protocol (GVRP) message status (GARP refers to General Attribute Registration Protocol):

1. Select **Set GVRP Status**.
2. Choose **E** to enable and **D** to disable.

To set Management Status:

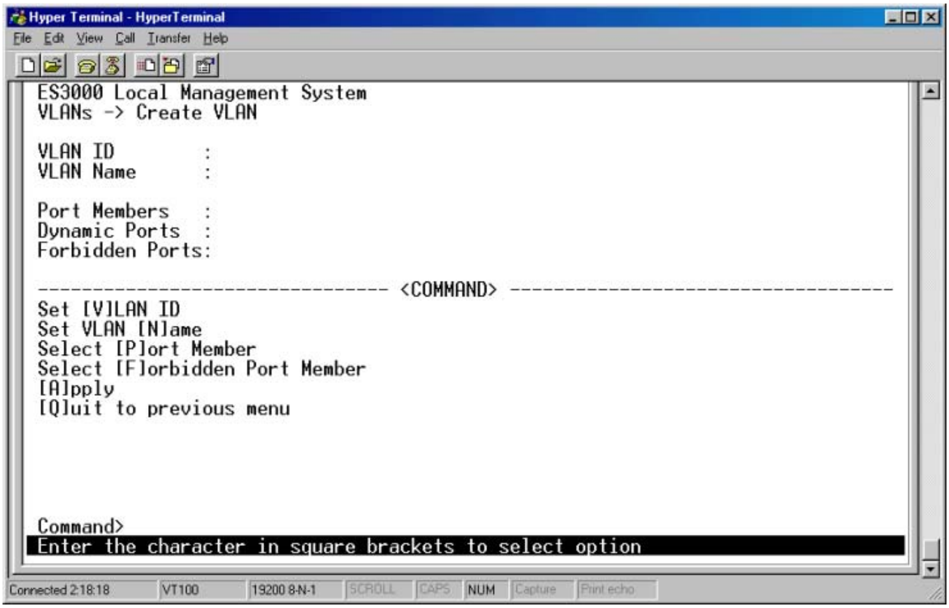
1. Select **Set Management Status**.
2. Choose **E** to enable and **D** to disable.

Adding a VLAN

To create a VLAN:

1. Select **Create VLAN**.

   The **Create VLAN** screen displays.



Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:18:18 VT100 19200 8-N-1 SCROLL CAPS NUM Capture Print echo

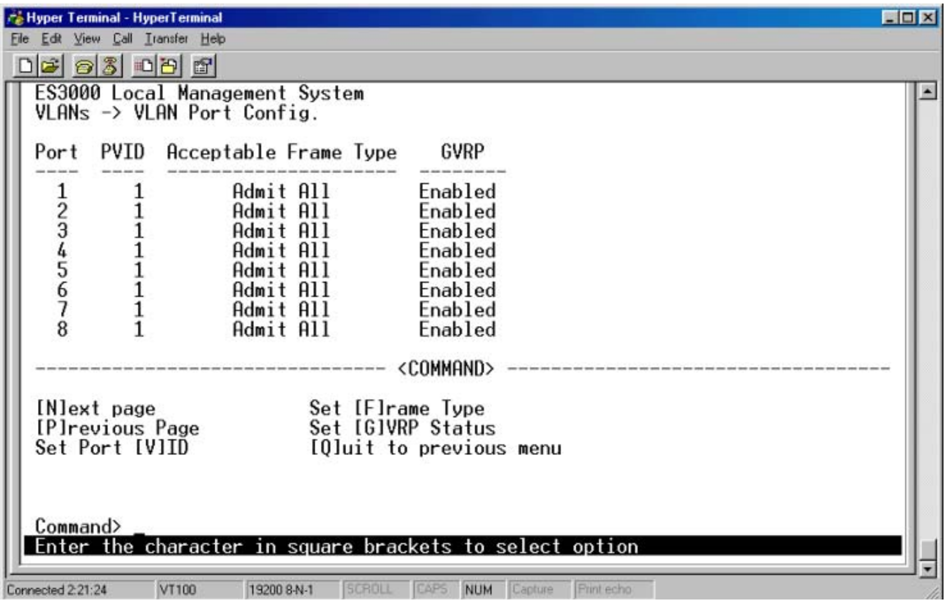
```
ES3000 Local Management System
VLANs -> Create VLAN

VLAN ID       :
VLAN Name     :

Port Members   :
Dynamic Ports  :
Forbidden Ports:

------------------------------- <COMMAND> -----------------------------------
Set [V]LAN ID
Set VLAN [N]ame
Select [P]ort Member
Select [F]orbidden Port Member
[A]pply
[Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

2. Create the VLAN and set the VLAN ID.
3. Enter the egress port of members by typing p.

   Instead of typing 3 to 12 individually, a (-) can be used to indicate contiguous numbers. Use a comma to separate the members.

3.5.31 Main Menu->VLANs->VLAN Port Configuration Menu

Use the **VLAN Port Configuration** screen to configure VLAN configurations for each port. The PVID is default to 1 for every port.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:21:24
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
VLANs -> VLAN Port Config.

Port  PVID  Acceptable Frame Type    GVRP
----  ----  ---------------------  --------
  1     1        Admit All         Enabled
  2     1        Admit All         Enabled
  3     1        Admit All         Enabled
  4     1        Admit All         Enabled
  5     1        Admit All         Enabled
  6     1        Admit All         Enabled
  7     1        Admit All         Enabled
  8     1        Admit All         Enabled

------------------------------- <COMMAND> ----------------------------------

[N]ext page                Set [F]rame Type
[P]revious Page            Set [G]VRP Status
Set Port [V]ID             [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

Set Port VID: Sets PVID of a port.

Set Frame Type: Sets the acceptable frame types, All or Tagged Only. When Tagged Only is selected, all non-tagged packet are dropped.

Set GVRP Status: Enables or disables the GVRP of a port.

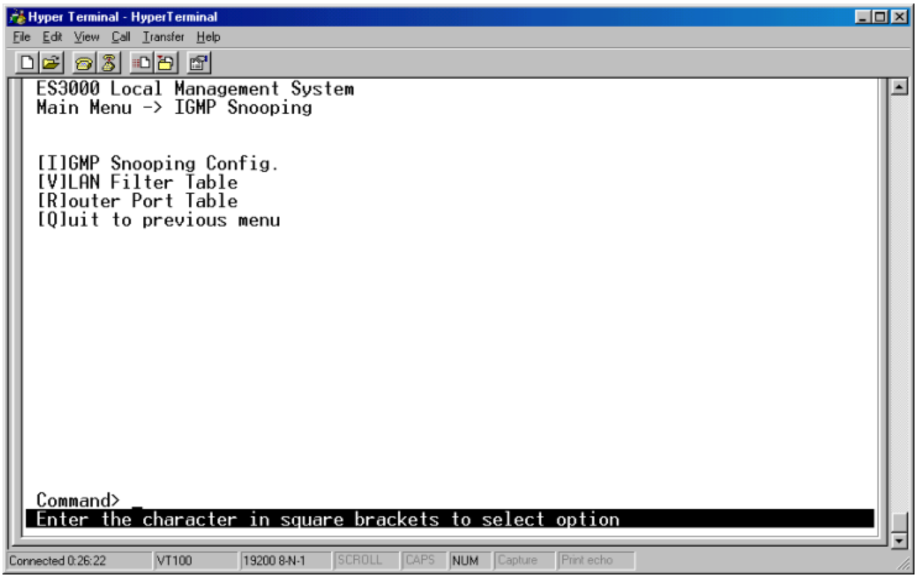
Note When a PVID on VLAN configuration is deleted, the PVID is changed to the default value of PVID, 1. All other configurations are kept.

The following entry is used when PVID 2 is removed.

Port	PVID	Acceptable Frame Type	GVRP
3	1	Tagged Only	Enable

3.5.32 Main Menu->IGMP Snooping Configuration Menu

The Internet Group Management Protocol (IGMP) is an Internet protocol allowing a host to report its multicast group membership to multicast routers. Multicasting allows one computer on the Internet to send information to other computers having identified themselves as interested in receiving the information. The ES3000 can "snoop" the messaging protocol to keep track of multicast groups and to insure multicast traffic is sent only to the appropriate ports within a VLAN. In networks where multimedia applications generate multicast traffic, IGMP can reduce unnecessary bandwidth by limiting traffic forwarding otherwise broadcast to the network. Enabling IGMP allows individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 0:26:22
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Main Menu -> IGMP Snooping


[I]GMP Snooping Config.
[V]LAN Filter Table
[R]outer Port Table
[Q]uit to previous menu















Command> _
Enter the character in square brackets to select option
```

IGMP Snooping Config.

VLAN Filter Table

Router Port Table

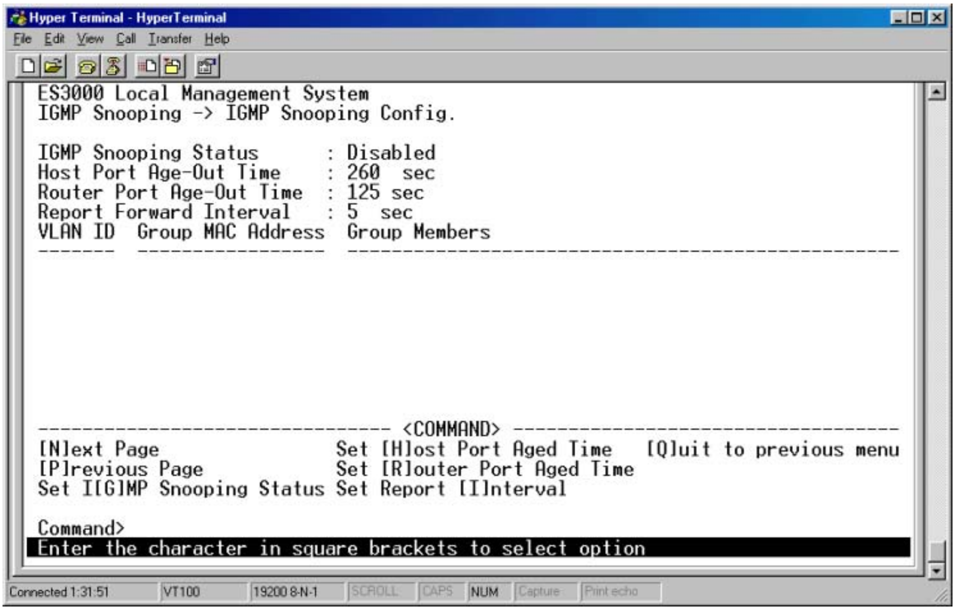
IGMP Snooping Status

Enable	The system detects IGMP queries, report packets, and manages IP multicast traffic through the switch.
Disable	The switch forwards traffic and disregards any IGMP requests.

3.5.33 Main Menu->IGMP Snooping->IGMP Snooping Config.

Enable	The system detects IGMP queries, report packets, and manage IP multicast traffic through the switch.
Disable	The switch forwards traffic and disregards any IGMP requests.

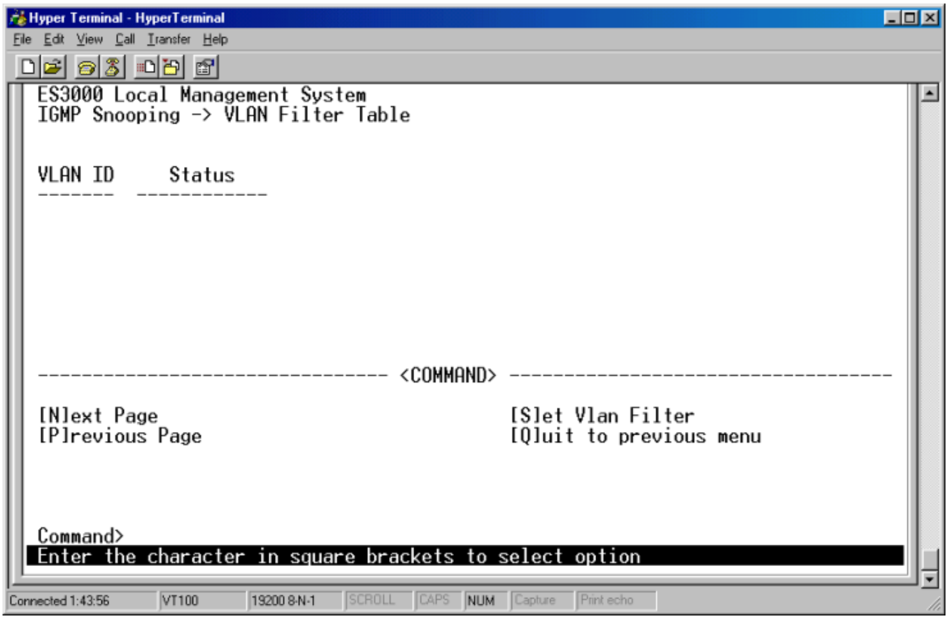
Users can set up Host port aged time and router port aged time to snoop the network and the IGMP Snooping status report interval.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:31:51
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
IGMP Snooping -> IGMP Snooping Config.

IGMP Snooping Status      : Disabled
Host Port Age-Out Time    : 260  sec
Router Port Age-Out Time  : 125 sec
Report Forward Interval   : 5  sec
VLAN ID  Group MAC Address  Group Members
-------  -----------------  --------------------------------------------------









--------------------------------- <COMMAND> -----------------------------------
[N]ext Page                Set [H]ost Port Aged Time   [Q]uit to previous menu
[P]revious Page            Set [R]outer Port Aged Time
Set I[G]MP Snooping Status Set Report [I]nterval

Command>
Enter the character in square brackets to select option
```

3.5.34 Main Menu->IGMP Snooping->VLAN Filter Table

Use the **VLAN Filter Table** to define the VLAN not to be included in the set Vlan Filter. Enter the VLAN ID (1-4094) in the **VLAN ID** field. Ensure the **Status** field is set to **Filter**.

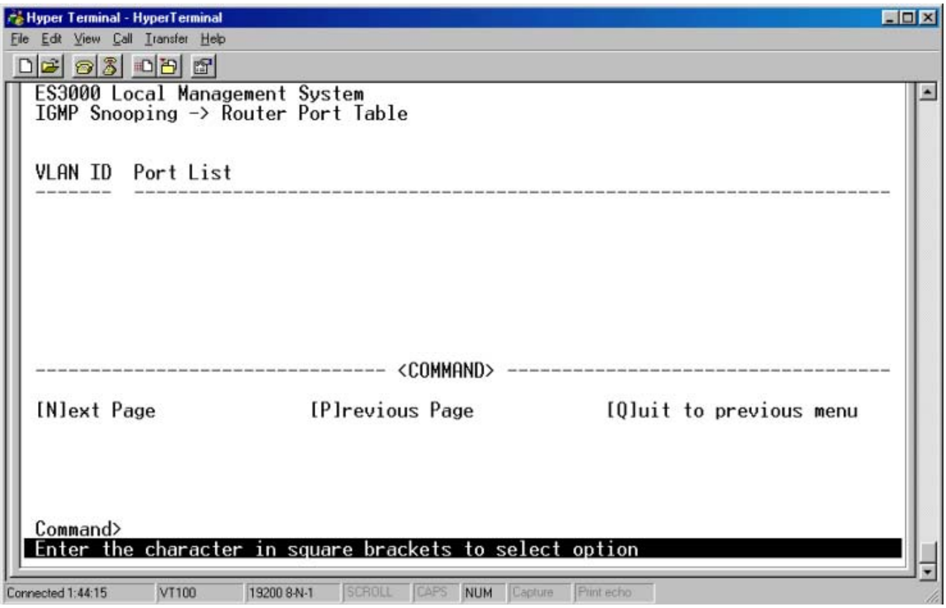


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:43:56
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
IGMP Snooping -> VLAN Filter Table


VLAN ID     Status
-------   ------------








-------------------------------- <COMMAND> ----------------------------------

[N]ext Page                                  [S]et Vlan Filter
[P]revious Page                              [Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

3.5.35 Main Menu->IGMP Snooping->Router Port Table

The **Router Port Table** menu displays the ports in a VLAN ID connecting to the router. The user can snoop the package from the router side of the ports. Select **Next Page** to display additional VLAN IDs should they exist.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:44:15
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
IGMP Snooping -> Router Port Table

VLAN ID  Port List
-------  ---------------------------------------------------------------------






--------------------------------- <COMMAND> -----------------------------------

[N]ext Page              [P]revious Page             [Q]uit to previous menu




Command>
Enter the character in square brackets to select option
```

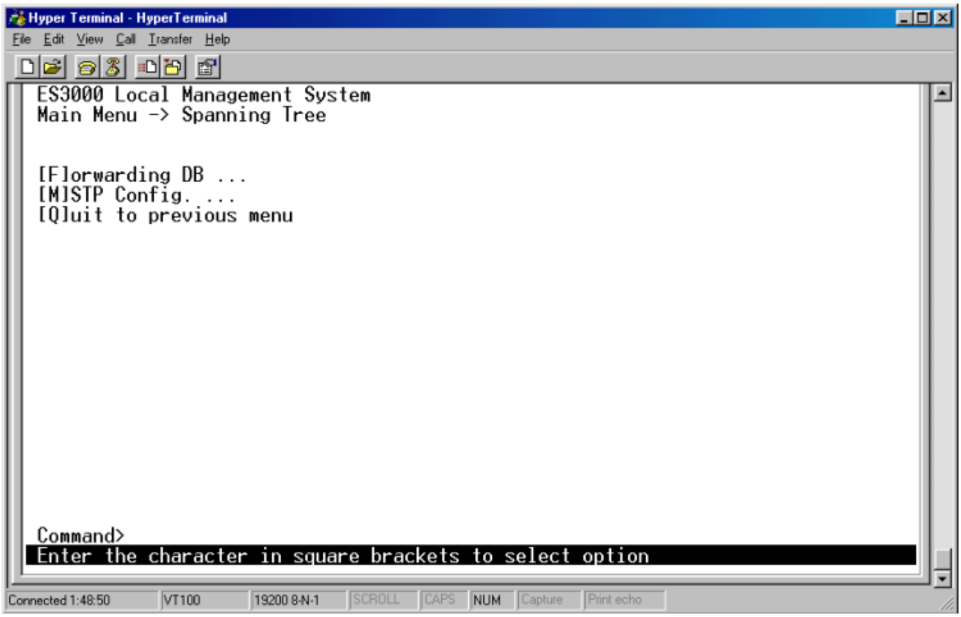
3.5.36 Main Menu->Spanning Tree Configuration Menu

The ES3000 can be configured to use one of three spanning tree protocols. Spanning Tree Protocol (STP) is compatible with legacy equipment. Rapid Spanning Tree Protocol (RSTP) is signficantly faster than STP. Multiple Spanning Tree Protocol (MSTP) is based on RSTP and extends RSTP in a way that is useful for switches implementing VLANs.

There maybe more than one physical path between any two nodes (forming a loop) either created for redundancy or by accident. STP ensures only one physical path is active and the others are blocked. If a loop is created for redundancy, STP monitors the two paths and activates the stand-by path if the primary path fails. If a loop was created inadvertently, STP disables one of the two paths. A loop can disable the network by causing a "Broadcast Storm", the result of a broadcast message traveling through the loop again and again.

Use the **Spanning Tree Configuration** menu to access and configure the following submenus:

- Forwarding DB
- MSTP Config.

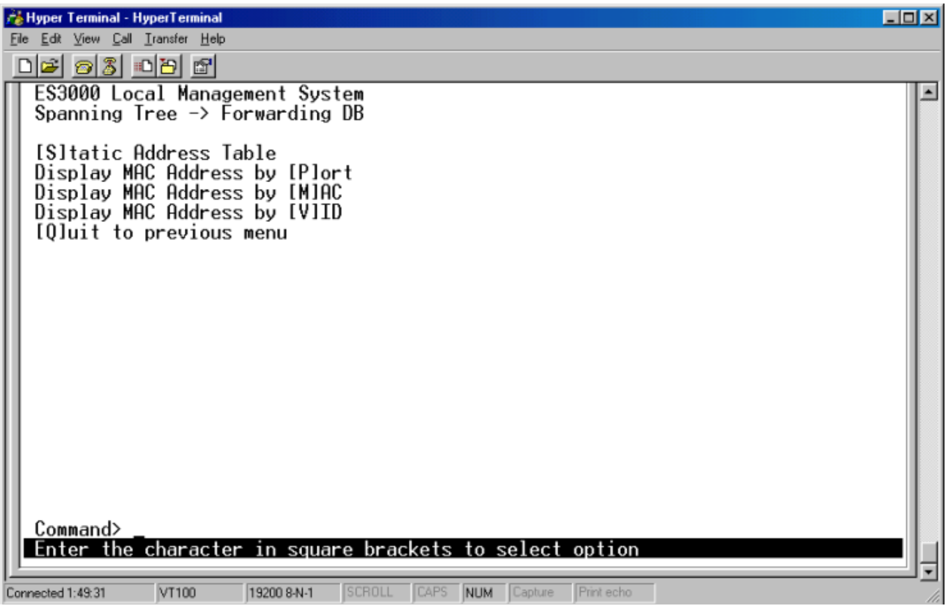

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
Main Menu -> Spanning Tree


[F]orwarding DB ...
[M]STP Config. ...
[Q]uit to previous menu













Command>
Enter the character in square brackets to select option
```

Connected 1:48:50
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.37 Main Menu->Spanning Tree->Forwarding DB

Use the **Forwarding Database** option to view the dynamic MAC addresses currently in the address database. When addresses are in the database, the packets intended for those addresses are forwarded directly to those ports. The Administrator can display addresses in the table by port, VLAN, and/or MAC address by entering the short key. The static MAC address table is also displayable


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:49:31
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Spanning Tree -> Forwarding DB

[S]tatic Address Table
Display MAC Address by [P]ort
Display MAC Address by [M]AC
Display MAC Address by [V]ID
[Q]uit to previous menu








Command> _
Enter the character in square brackets to select option
```

There are four commands within the **Forwarding Database** option.

Static Address Table	Display and configure the static MAC address table.
Display MAC Address By Port	Display MAC address table for a specified port
Display MAC Address by MAC	Display MAC address in order of MAC address.
Display MAC Address by VID	Display MAC address table for a specified VLAN ID.

Static Address Table:

Use the Static Addresses Table to specify Media Access Control (MAC) addresses for specific ports not purged from the bridge table by the aging function. There are 3 entries in the table. Two commands are available to add and/or remove an entry. To add an entry, follow the pop-out prompt.

1. **Enter MAC Address(xx:xx:xx:xx:xx:xx) >** 00:12:34:99:ab:ef <ENTER>
2. **Add new entry->Enter port number >** 10 <ENTER>
3. **Add new entry->Enter VLAN ID>** 50 <ENTER>

A new entry displays: **00:12:34:99:AB:EF 10 50**

To remove an entry:

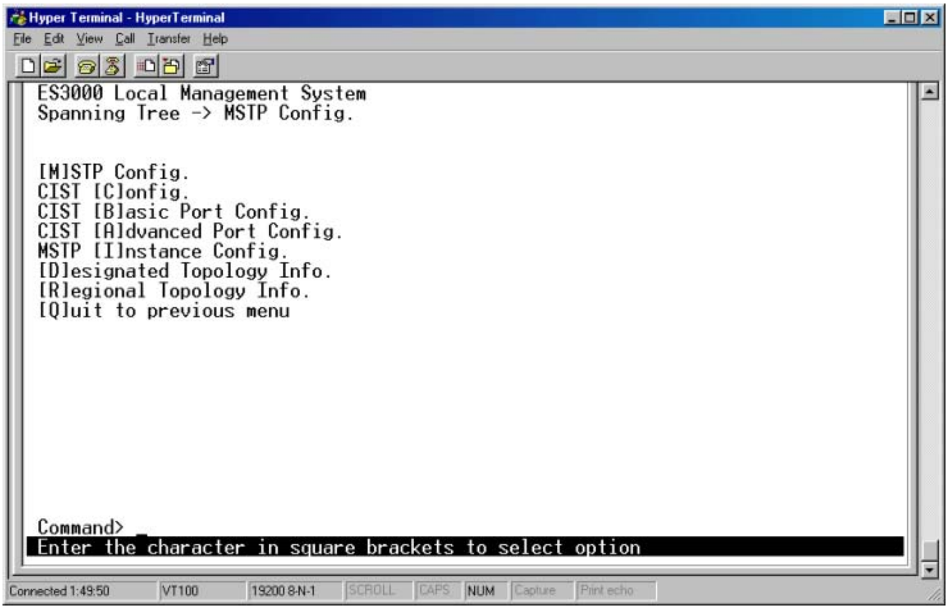
1. Hit key D
2. **Enter MAC Address(xx:xx:xx:xx:xx:xx) >** 00:11:ab:00:33:55 <ENTER>
3. **Delete entry->Enter VLAN ID>** 30 <ENTER>

Display MAC Address by Port, MAC, and VID

With the number of hosts increase on a network, the Forwarding Database grows sharply. To look for an MAC address becomes time-consuming work. The system provides three different ways for administrator to research MAC addresses; by a specified Port, sorted by MAC address, and by a specified VLAN. Each one of these, a Set Age-Out time command is given to configure the time to remove a non-recently-used entry. The modification on this timer is switch-wide.

The age-out time is the amount of time that an entry is kept in the bridge tables prior to being purged (or aged). The range is between 10 seconds and 1,000,000 seconds. By industry standard, 300 seconds is the default.

3.5.38 Main Menu->Spanning Tree->MSTP Config.

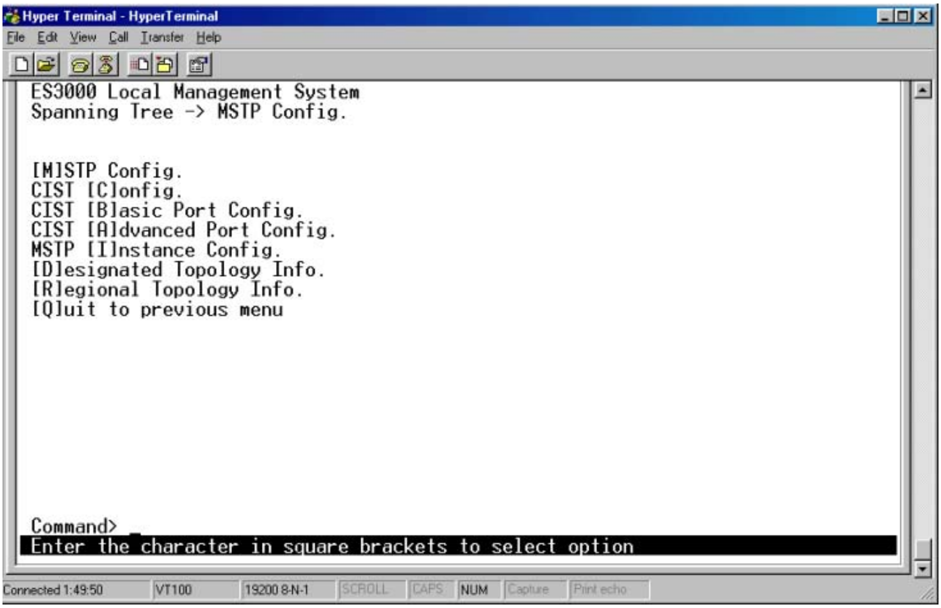

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:49:50
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Spanning Tree -> MSTP Config.


[M]STP Config.
CIST [C]onfig.
CIST [B]asic Port Config.
CIST [A]dvanced Port Config.
MSTP [I]nstance Config.
[D]esignated Topology Info.
[R]egional Topology Info.
[Q]uit to previous menu








Command> _
Enter the character in square brackets to select option
```

3.5.39 Main Menu->Spanning Tree->Multiple Spanning Tree Configuration->MSTP Config.

Rapid spanning tree (IEEE 802.1w) is supported to reduce the spanning tree established time. Each spanning tree establishment process takes several timeouts to avoid a loop, even the edge switch. The user can configure the switch to avoid the long latency due to timeouts if there is only a single connection to the switch. If two or more links to the switch exist and Rapid Spanning Tree is enabled, the switch might not perform properly.

The switch supports IEEE 802.1s Multiple Spanning Tree. An independent spanning tree can be established per VLAN.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 1:49:50
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Spanning Tree -> MSTP Config.


[M]STP Config.
CIST [C]onfig.
CIST [B]asic Port Config.
CIST [A]dvanced Port Config.
MSTP [I]nstance Config.
[D]esignated Topology Info.
[R]egional Topology Info.
[Q]uit to previous menu








Command> _
Enter the character in square brackets to select option
```

The upper half of the **MSTP Config** screen displays information about the Multiple Spanning Tree Configuration.

Status:

Global MSTP Status: Status of global multiple spanning tree protocol. Enabled indicates that MSTP is running while Disabled indicates MSTP is not running.

Protocol Version: Three protocol versions are available, SPT (Spanning Tree), RSPT (Rapid Spanning Tree), MSPT (Multiple Spanning Tree).

MST Config ID Selector: Reserved for future use

MST Region Name: The MST Region Name is required to be identical to other switches to work cross-switch.

MST Region Version: Like MST Region Name, the MST Region Version name is required to be identical to other switches to have work cross-switch.

MST Config Digest: Digest value of configuration data to increase the security.

Command:

Enable/Disable Global MSTP: Enables or disables the switch-wide MSTP.

Set MSTP Protocol Version: Sets the protocol to be one among SPT (Spanning Tree), RSPT (Rapid Spanning Tree), and MSPT (Multiple Spanning Tree).

Cist Configuration: Configure Common Instant Spanning Tree - a switch-wide configuration.

Cist Basic Port Configuration: Port Configuration on Common Instant Spanning Tree - a switch-wide configuration.

Cist Advanced Port Config: Advanced Port Configuration on Common Instant Spanning Tree - a switch-wide configuration.

Set MSTI Region Name: Sets the region name.

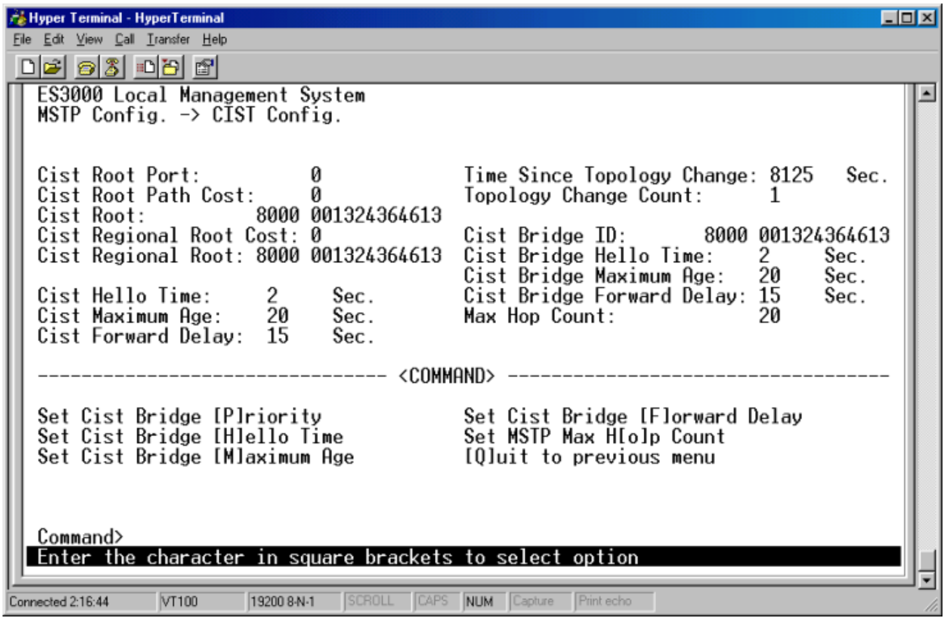
Set MSTI Region Version: Sets the region version.

Designated Topology Info: Designated topology information includes Port, Trunk, Link status, CIST Designated Root, CIST Designated Cost, CIST Designated Bridge, and CIST Designated Port.

Regional Topology Info: Regional topology information includes Port, Trunk, Link status, CIST Port Regional Root, CIST Port Regional Path Cost.

Configure the switch to ensure the SPT works properly. The Common Instant Spanning Tree Configuration Menu enables the user to configure the switch-wide parameters, such as Cist Hello Time, Cist Maximum Age, and Cist Forward Delay.

3.5.40 Main Menu->Spanning Tree->CIST Config.



Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
MSTP Config. -> CIST Config.


Cist Root Port:         0         Time Since Topology Change: 8125   Sec.
Cist Root Path Cost:    0         Topology Change Count:      1
Cist Root:         8000 001324364613
Cist Regional Root Cost: 0        Cist Bridge ID:      8000 001324364613
Cist Regional Root: 8000 001324364613 Cist Bridge Hello Time:    2    Sec.
                                  Cist Bridge Maximum Age:   20    Sec.
Cist Hello Time:     2     Sec.   Cist Bridge Forward Delay: 15    Sec.
Cist Maximum Age:    20    Sec.   Max Hop Count:             20
Cist Forward Delay:  15    Sec.

-------------------------------- <COMMAND> -----------------------------------

Set Cist Bridge [P]riority        Set Cist Bridge [F]orward Delay
Set Cist Bridge [H]ello Time      Set MSTP Max H[o]p Count
Set Cist Bridge [M]aximum Age     [Q]uit to previous menu



Command>
Enter the character in square brackets to select option
```

Status

Hello Time: Time between configuration messages sent by the Spanning Tree algorithm

Maximum Age: The time before a configuration message is discarded by the system

Forward Delay: The time the system spends transitioning from the learning to the listening to the forwarding states

Bridge Priority: Priority setting among other switches in the Spanning Tree

Command

Set Cist Bridge Priority: Sets the Cist bridge priority.

Set Cist Bridge Hello Time: Sets the interval between two hello packets.

Set Cist Bridge Maximum Age: Sets the maximum age time.

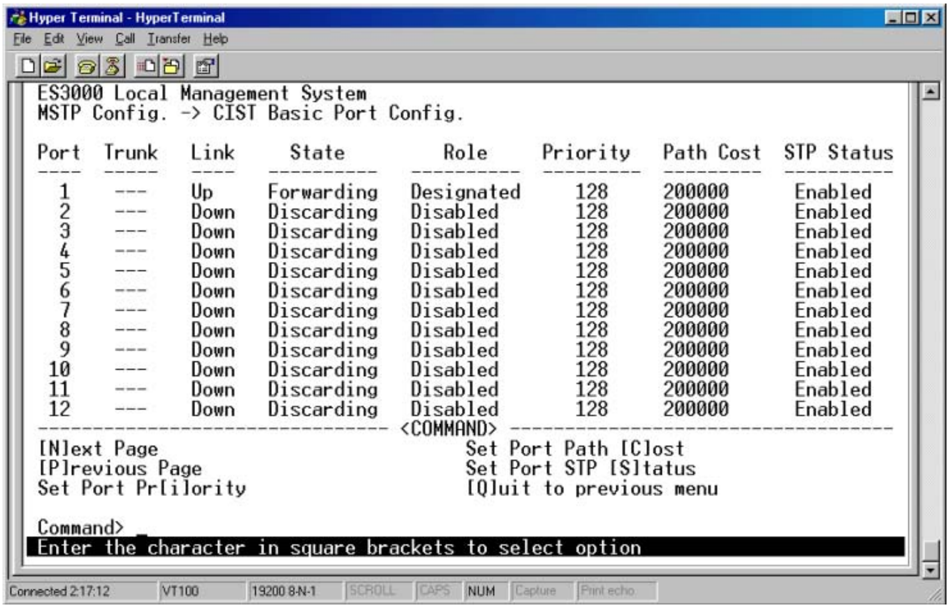
Set MSTP Max Hop Count Delay: Sets the maximum hop count delay.

Rapid Spanning Tree

When a port running the standard STP is connected, it goes through the STP negotiation (*listening -> learning -> forwarding or blocking)* before it is available. If a client is trying to access a server through the switch running STP negotiation, it is not able to connect to it immediately. This can be a problem for some networks. RSPT solves the problem by setting the port directly to forwarding mode. Therefore, any server access request is forwarded. RSPT is used on end node ports (ports connected to PCs or servers) and not on uplink ports to other switches.

3.5.41 Main Menu->Spanning Tree->MSTP Config->CIST Basic Port Config.

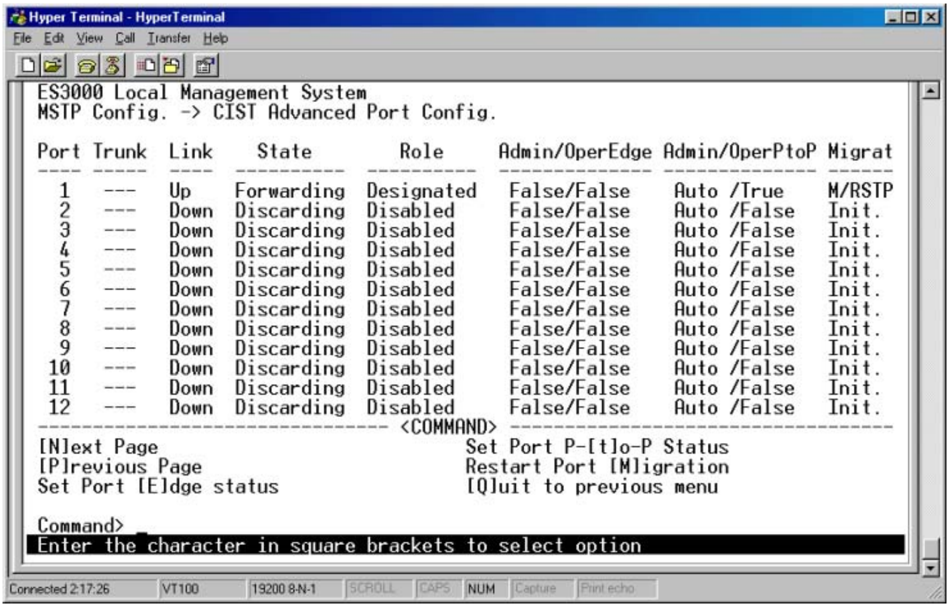
Use the **CIST Basic Port Config.** menu to configure the port edge status, port P-TO-P status, and restart port migration to prevent the wrong link.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:17:12
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
MSTP Config. -> CIST Basic Port Config.

Port   Trunk   Link    State        Role        Priority   Path Cost   STP Status
----   -----   ----  ----------  ----------   ---------  ---------  ----------
  1     ---    Up    Forwarding  Designated      128      200000       Enabled
  2     ---    Down  Discarding  Disabled        128      200000       Enabled
  3     ---    Down  Discarding  Disabled        128      200000       Enabled
  4     ---    Down  Discarding  Disabled        128      200000       Enabled
  5     ---    Down  Discarding  Disabled        128      200000       Enabled
  6     ---    Down  Discarding  Disabled        128      200000       Enabled
  7     ---    Down  Discarding  Disabled        128      200000       Enabled
  8     ---    Down  Discarding  Disabled        128      200000       Enabled
  9     ---    Down  Discarding  Disabled        128      200000       Enabled
 10     ---    Down  Discarding  Disabled        128      200000       Enabled
 11     ---    Down  Discarding  Disabled        128      200000       Enabled
 12     ---    Down  Discarding  Disabled        128      200000       Enabled
-------------------------------- <COMMAND> ----------------------------------
[N]ext Page                             Set Port Path [C]ost
[P]revious Page                         Set Port STP [S]tatus
Set Port Pr[i]ority                     [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

3.5.42 Main Menu -> Spanning Tree -> MSTP Config. -> CIST Advanced Port Config.

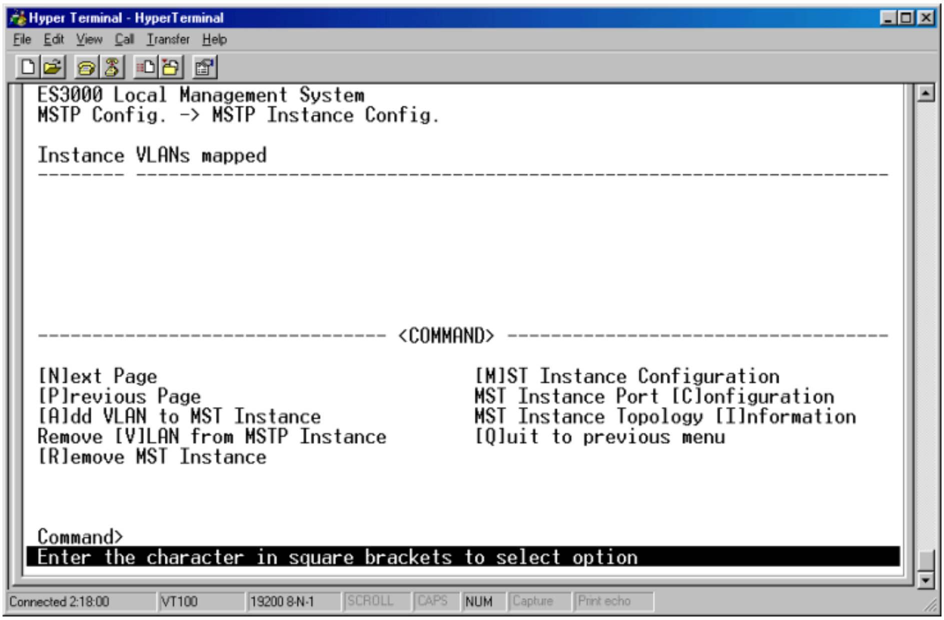
Use the **CIST Advanced Port Config.** menu to set up the port edge status, port P-TO-P status, and restart port migration to prevent the wrong link.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
MSTP Config. -> CIST Advanced Port Config.

Port Trunk  Link    State       Role      Admin/OperEdge Admin/OperPtoP Migrat
---- -----  ----  ----------  ----------  -------------- -------------- ------
  1   ---   Up    Forwarding  Designated   False/False    Auto /True    M/RSTP
  2   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  3   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  4   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  5   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  6   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  7   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  8   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
  9   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
 10   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
 11   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
 12   ---   Down  Discarding  Disabled     False/False    Auto /False   Init.
------------------------------ <COMMAND> -----------------------------------
[N]ext Page                                Set Port P-[t]o-P Status
[P]revious Page                            Restart Port [M]igration
Set Port [E]dge status                     [Q]uit to previous menu

Command> _
Enter the character in square brackets to select option
```

3.5.43 Main Menu->Spanning Tree->MSTP Config.->MSTP Instance Config.

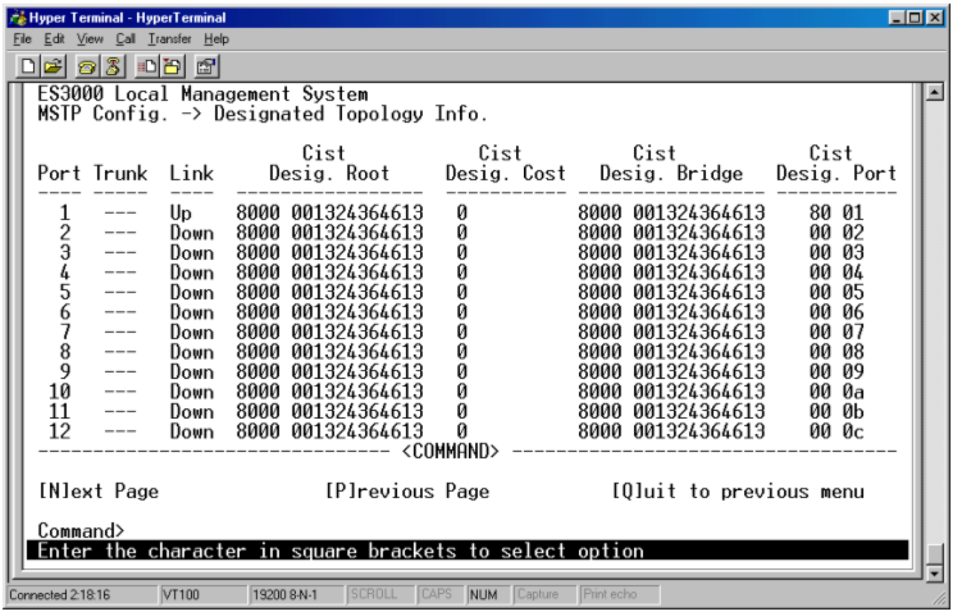
A small tree instance can be considered in the MSTP. One Instance can have more than one VLAN. Use the **MSTP Instance Config.** menu to add or remove a VLAN, or remove the MST Instance as well as MST Instance and Instance Port configuration.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:18:00
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
MSTP Config. -> MSTP Instance Config.

Instance VLANs mapped
-------- ---------------------------------------------------------------------







-------------------------------- <COMMAND> ----------------------------------

[N]ext Page                             [M]ST Instance Configuration
[P]revious Page                         MST Instance Port [C]onfiguration
[A]dd VLAN to MST Instance              MST Instance Topology [I]nformation
Remove [V]LAN from MSTP Instance        [Q]uit to previous menu
[R]emove MST Instance



Command>
Enter the character in square brackets to select option
```

3.5.44 Main Menu->Spanning Tree->MSTP Config.->Designated Topology Info.

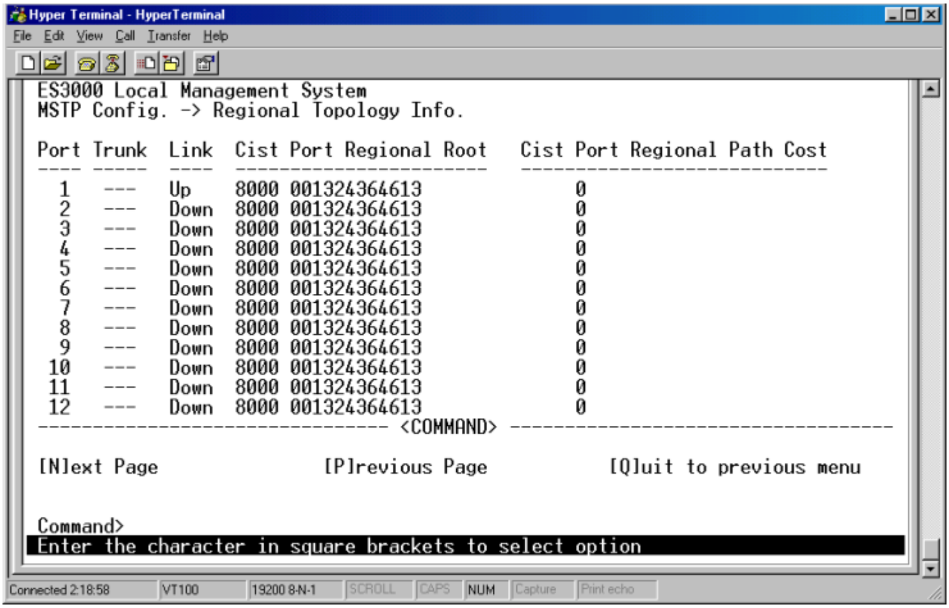
The **Designated Topology Info.** page displays read-only topology information for each port.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 2:18:16
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
MSTP Config. -> Designated Topology Info.

                           Cist             Cist           Cist             Cist
Port Trunk  Link     Desig. Root      Desig. Cost    Desig. Bridge     Desig. Port
---- -----  ----   ----------------- -----------  -----------------  -----------
  1   ---   Up     8000 001324364613   0          8000 001324364613    80 01
  2   ---   Down   8000 001324364613   0          8000 001324364613    00 02
  3   ---   Down   8000 001324364613   0          8000 001324364613    00 03
  4   ---   Down   8000 001324364613   0          8000 001324364613    00 04
  5   ---   Down   8000 001324364613   0          8000 001324364613    00 05
  6   ---   Down   8000 001324364613   0          8000 001324364613    00 06
  7   ---   Down   8000 001324364613   0          8000 001324364613    00 07
  8   ---   Down   8000 001324364613   0          8000 001324364613    00 08
  9   ---   Down   8000 001324364613   0          8000 001324364613    00 09
 10   ---   Down   8000 001324364613   0          8000 001324364613    00 0a
 11   ---   Down   8000 001324364613   0          8000 001324364613    00 0b
 12   ---   Down   8000 001324364613   0          8000 001324364613    00 0c
-------------------------------- <COMMAND> ------------------------------------

[N]ext Page               [P]revious Page           [Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

3.5.45 Main Menu->Spanning Tree->MSTP Config.->Regional Topology Info.

The **Regional Topology Info.** page displays regional topology information (read-only) for each port.



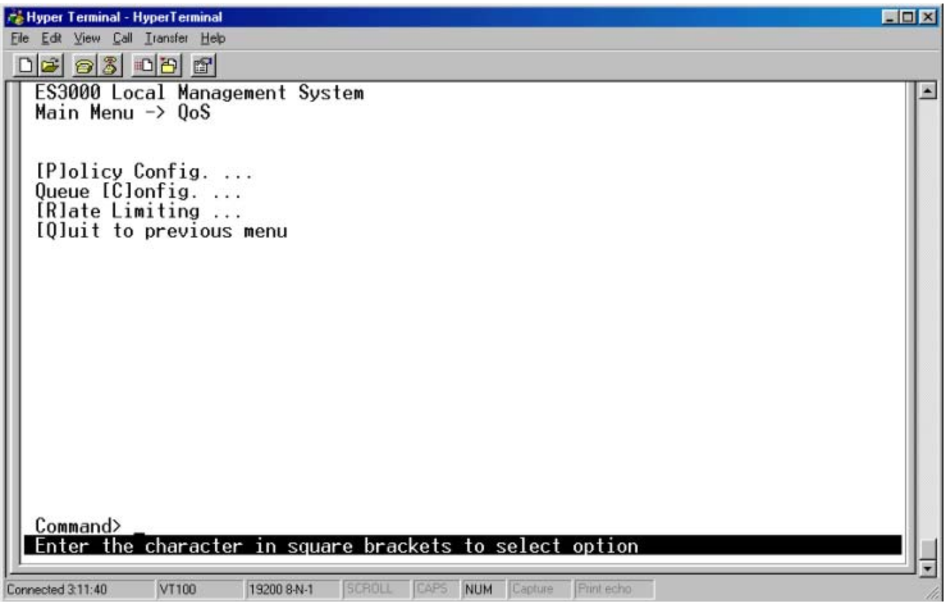
Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
MSTP Config. -> Regional Topology Info.

Port Trunk  Link  Cist Port Regional Root   Cist Port Regional Path Cost
---- -----  ----  -----------------------   ----------------------------
  1   ---   Up    8000 001324364613              0
  2   ---   Down  8000 001324364613              0
  3   ---   Down  8000 001324364613              0
  4   ---   Down  8000 001324364613              0
  5   ---   Down  8000 001324364613              0
  6   ---   Down  8000 001324364613              0
  7   ---   Down  8000 001324364613              0
  8   ---   Down  8000 001324364613              0
  9   ---   Down  8000 001324364613              0
 10   ---   Down  8000 001324364613              0
 11   ---   Down  8000 001324364613              0
 12   ---   Down  8000 001324364613              0
-------------------------------- <COMMAND> -----------------------------------

[N]ext Page                [P]revious Page           [Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

3.5.46 Main Menu->QoS (Quality of Service Configuration Menu)

The ES3000 implements IEEE 802.1p Quality of Service (QoS) processing. QoS policies examine packets and classify them. The classification is used to drop packets or to assign markers to the packets. The markers are Class of Service (CoS) Priority, Type of Service (ToS) Precedence and Differentiated Services Code Points (DSCP). For each port, the outgoing packets are then placed in four output queues based on CoS priority or DSCP value. The queues are serviced using a weighted round robin algorithm.

Quality of Service defines the methods to improve network performance by segregating traffic. Configure the switch for specific traffic to take priority by using either the VLAN tags (port-based) or DSCP (DiffServ).


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help

```
ES3000 Local Management System
Main Menu -> QoS


[P]olicy Config. ...
Queue [C]onfig. ...
[R]ate Limiting ...
[Q]uit to previous menu















Command> _
Enter the character in square brackets to select option
```

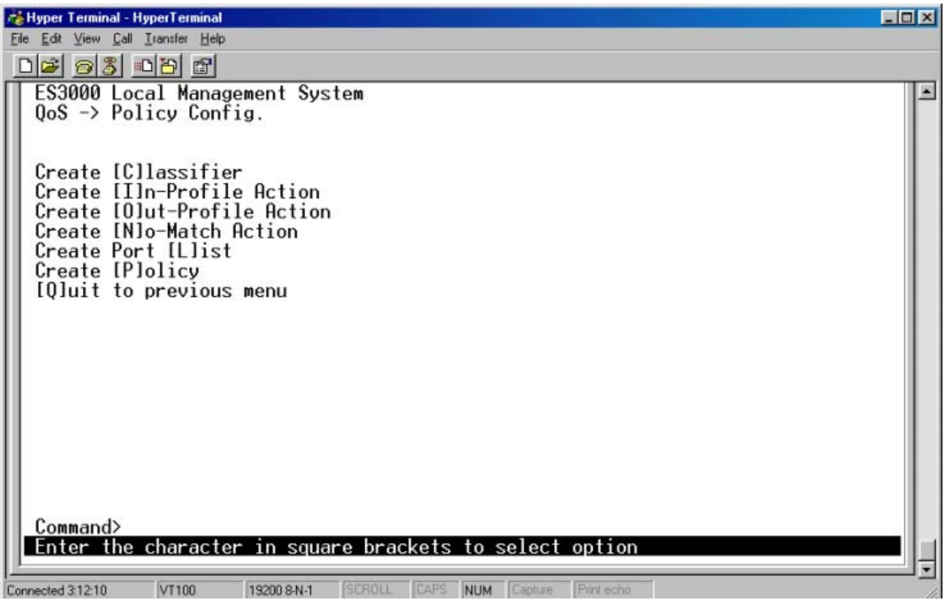
Connected 3:11:40
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

3.5.47 Main Menu->QoS->Policy Config.

Differentiated Service (DiffServ) uses a priority tag in the data packet (the Differentiated Service Code Point or DSCP) to determine the priority of the packet. The **Policy Config** menu maps the various DSCP tags to the two four queues on each port. The Classifier allows users to add different rules to distinguish traffic service. An administrator is able to classifier based on Protocol, Source MAC Address, Source IP Address, Destination MAC Address, Destination IP Address, VLAN ID, DSCP, Source Layer 4 Port, and Destination Layer 4 Port.

To create an applicable policy, the administrator configures conditions properly and apply these conditions to policy by in-profile action or out-profile action, or no-match action.

Symbol recommends remembering those IDs given to Classifier, In Profile Action, No Match Action, and Out Profile Action. If necessary, the administrator can retrieve the ID associated information from the **Show Each ID Information** command.

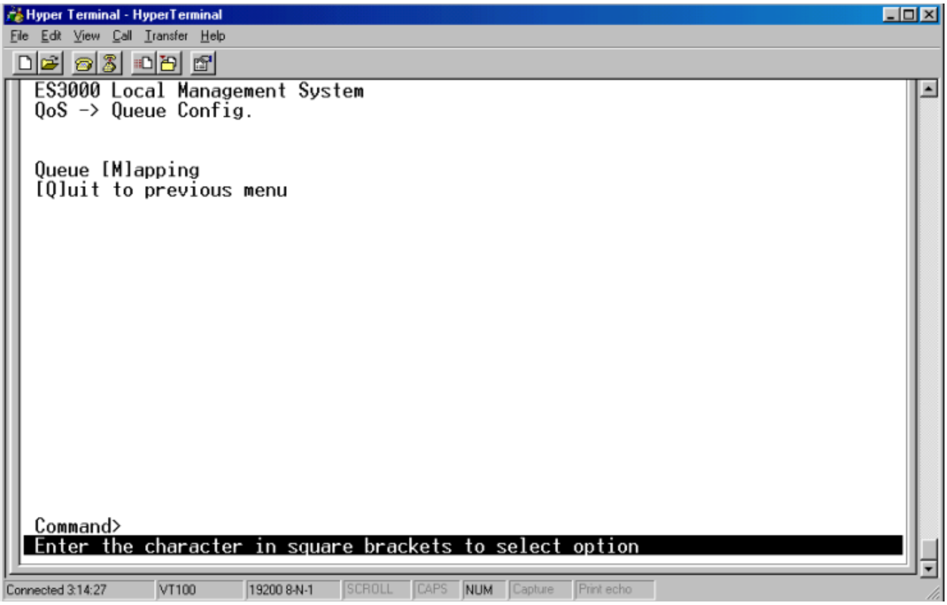

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 3:12:10
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
QoS -> Policy Config.


Create [C]lassifier
Create [I]n-Profile Action
Create [O]ut-Profile Action
Create [N]o-Match Action
Create Port [L]ist
Create [P]olicy
[Q]uit to previous menu









Command>
Enter the character in square brackets to select option
```

3.5.48 Main Menu->QoS->Queue Config.

Port Prioritization allows the user to specify which ports have greater precedence in situations where traffic can be buffered in the switch due to congestion. Traffic that comes in on ports with a setting of high is transmitted before those that come in on a port with a normal setting. The settings on this page only affect packets that do not already have VLAN priority tags. To raise the priority of a given port, toggle the port setting from normal to high. The default setting for a port is normal.

The priority tag of each packet is divided into four queues on each output port. The default setup is that each queue takes two priorities sequentially. The Administrator can configure the traffic class as needed. The Quality of Service works only after the QoS status is enabled by Set QoS Status.

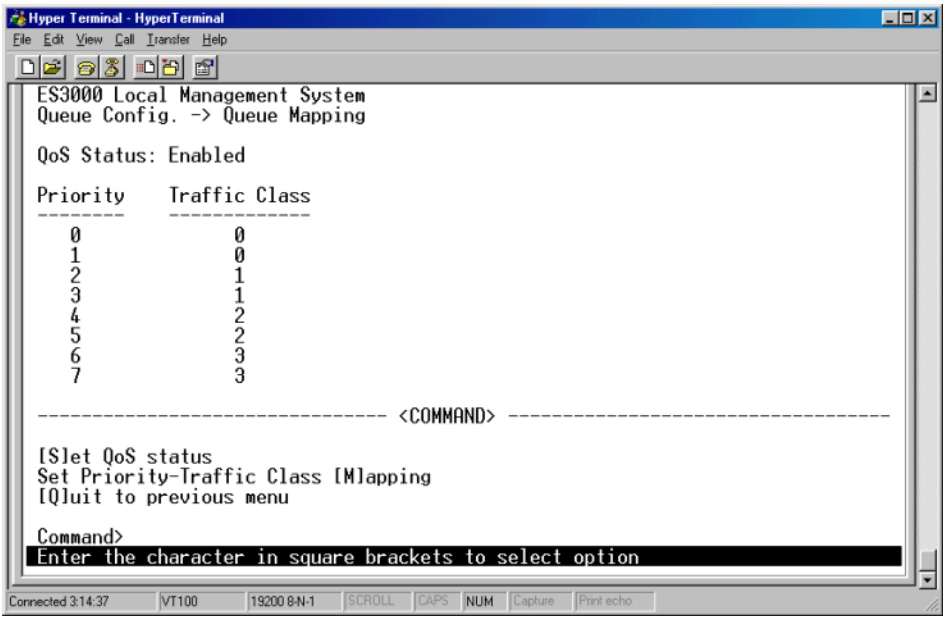

Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 3:14:27
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
QoS -> Queue Config.


Queue [M]apping
[Q]uit to previous menu


Command>
Enter the character in square brackets to select option
```

3.5.49 Main Menu->QoS->Queue Config.->Queue Mapping

The priority tag of each packet is divided into four queues on each output port within the Queue Mapping screen. The default setup each queue assuming two priorities sequentially.

Configure the traffic class as needed. Quality of Service works only after the QoS status is **Enabled** by Set QoS Status.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 3:14:37
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

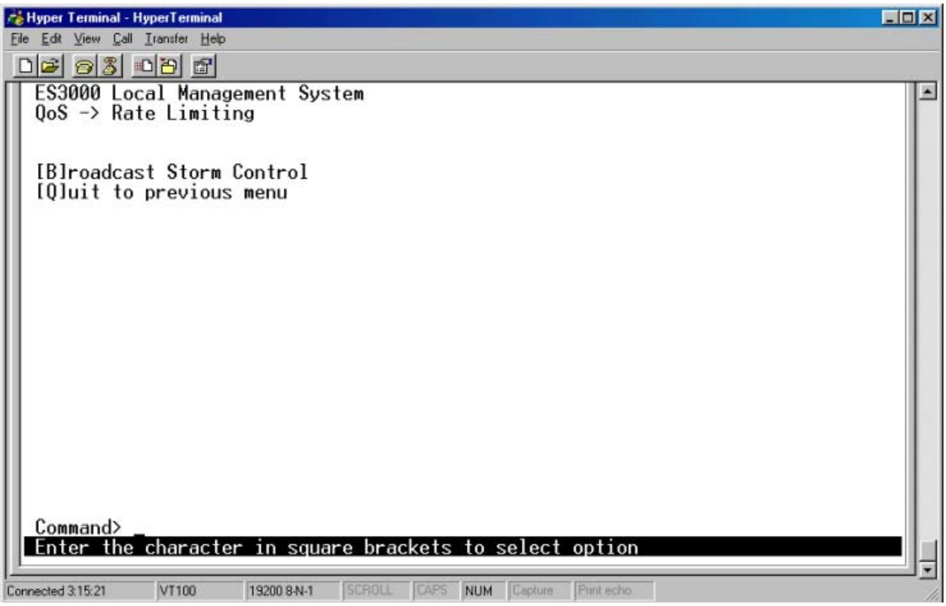
```
ES3000 Local Management System
Queue Config. -> Queue Mapping

QoS Status: Enabled

Priority    Traffic Class
--------    -------------
   0              0
   1              0
   2              1
   3              1
   4              2
   5              2
   6              3
   7              3

-------------------------------- <COMMAND> -----------------------------------

[S]et QoS status
Set Priority-Traffic Class [M]apping
[Q]uit to previous menu

Command>
Enter the character in square brackets to select option
```

3.5.50 Main Menu->QoS->Rate Limiting

Use the **Rate Limiting** screen to configure the broadcast storm control to enable or disable traffic control in the networks.

Rate limiting, or storm control, prevents ports on the ES3000 switch from being overwhelmed by a broadcast, unicast, or multicast storm. A storm results when packets flood the LAN, which degrades network performance. With rate limiting enabled, the switch monitors incoming traffic by counting packets over a period of time. When the packet count exceeds a predefined threshold level, the switch suppresses traffic until the packet count drops below the threshold. With rate limiting disabled, all traffic is allowed. The switch supports rate limiting for broadcast, multicast, and unicast (DLF) traffic, keeping a separate count of the packets for each type of traffic. When broadcast or unicast traffic reaches the threshold, the switch suppresses further traffic of that type until traffic falls below the threshold. Broadcast, multicast and DLF traffic cannot be set on a per port basis, only on a per-switch basis.

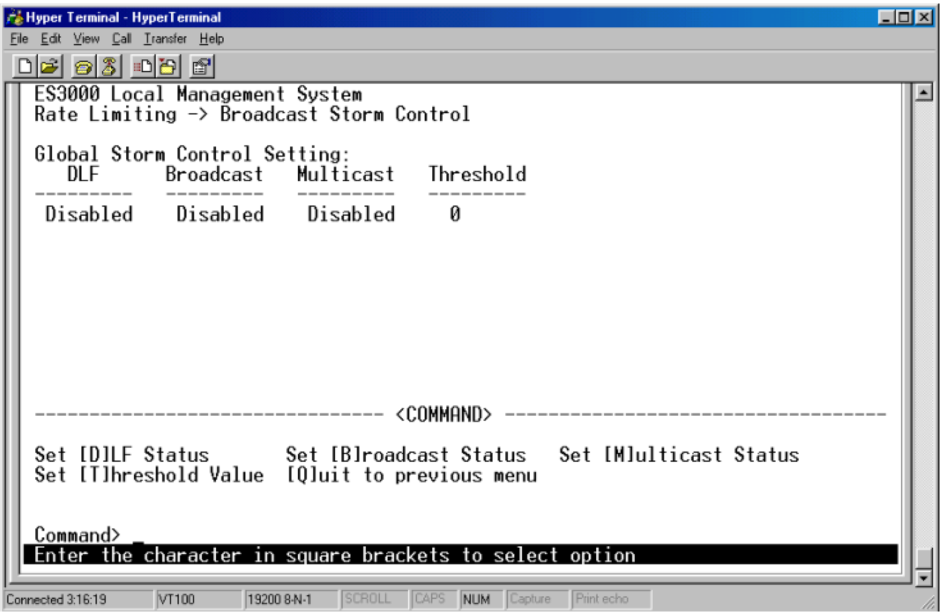
Select Broadcast Storm Control to display the **Broadcast Storm Control Configuration Menu** used configuring switch behavior during a broadcast storm. A loop in a network can disable the network by causing a Broadcast Storm. A **Broadcast Storm** is the result of a broadcast message traveling through the loop again and again.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 3:15:21
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
QoS -> Rate Limiting


[B]roadcast Storm Control
[Q]uit to previous menu



Command> _
Enter the character in square brackets to select option
```

3.5.51 Main Menu->QoS->Rate Limiting->Broadcast Storm Control Configuration Menu

Use the Storm Control Configuration page to set the limitation of broadcast, multicast, and/or DLF (Destination Look Failure) packets delivered to the CPU. Each kind of packet determines the network load. When the load reaches a certain threshold, the CPU is busy handling packets and is unable to respond to other requests (configuration commands or SNMP requests). Available network bandwidth decreases. The administrator can enable storm control to limit traffic in the networks.


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 3:16:19
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000 Local Management System
Rate Limiting -> Broadcast Storm Control

Global Storm Control Setting:
     DLF      Broadcast   Multicast   Threshold
 ---------    ---------   ---------   ---------
  Disabled     Disabled    Disabled       0








--------------------------------- <COMMAND> -----------------------------------

Set [D]LF Status       Set [B]roadcast Status   Set [M]ulticast Status
Set [T]hreshold Value  [Q]uit to previous menu


Command> _
Enter the character in square brackets to select option
```

There are three kinds of storm control; DLF, Broadcast, and Multicast.

DLF: Destination Look Failure packets. DLF packets are broadcast to all ports except the incoming port.

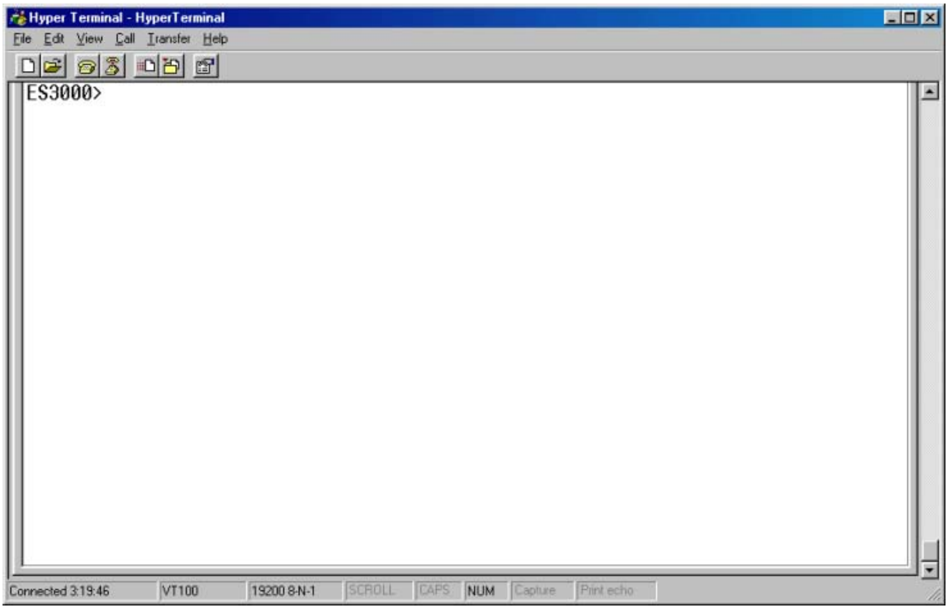
Broadcast: Packets are delivered to all ports except the incoming port as DLF packets.

Multicast: Packets are delivered to all ports with group membership.

Storm control can either be Enabled and Disabled. When Enabled, the CPU drops packets beyond the specified threshold. Otherwise, the CPU processes these packet types without any limitations. The default setting is **Disabled** for all three packet types.

3.5.52 Execute CLI

The **CLI** (Command Line Interface) provides a means to configure the system for advanced users. Symbol recommends the CLI for adavanced users who do not need to navigae a menu-driven interface to configure the ES3000 Ethernet Switch. See *Chapter 5* for detailed information. Once **Run CLI** is selected, the 'SW24P4>' prompt displays


Hyper Terminal - HyperTerminal
File Edit View Call Transfer Help
Connected 3:19:46
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

```
ES3000>
```

4

Web Management Access

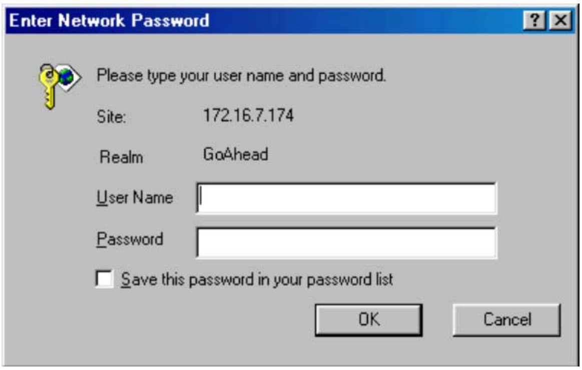
The Symbol ES3000 Managed Switch provides a built-in browser interface for configuring and managing remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. The browser interface also allows for system monitoring of the Switch. The help page covers many of the basic functions and features of the switch and its Web interface.

When configuring the switch for the first time, assign an IP address and subnet mask to the switch. Thereafter, access the Web interface directly using a Web browser by entering the switch IP address into the address bar. Use the Web browser to manage the switch from a central location, as if the user were directly connected to the switch console port.

When using the Web interface, changes are required to be saved or updates are lost. See *System Admin->Tools->Save Configuration on page 4-14* for additional information.

Web Management requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

To connect to the switch, the switch IP is required to be known first. If using a private IP address, 172.16.7.174. By entering 'http://172.16.5.115/' on the URL, following login screen is shown.



Enter Network Password

Please type your user name and password.

Site: 172.16.7.174

Realm GoAhead

User Name

Password

□ Save this password in your password list

OK Cancel

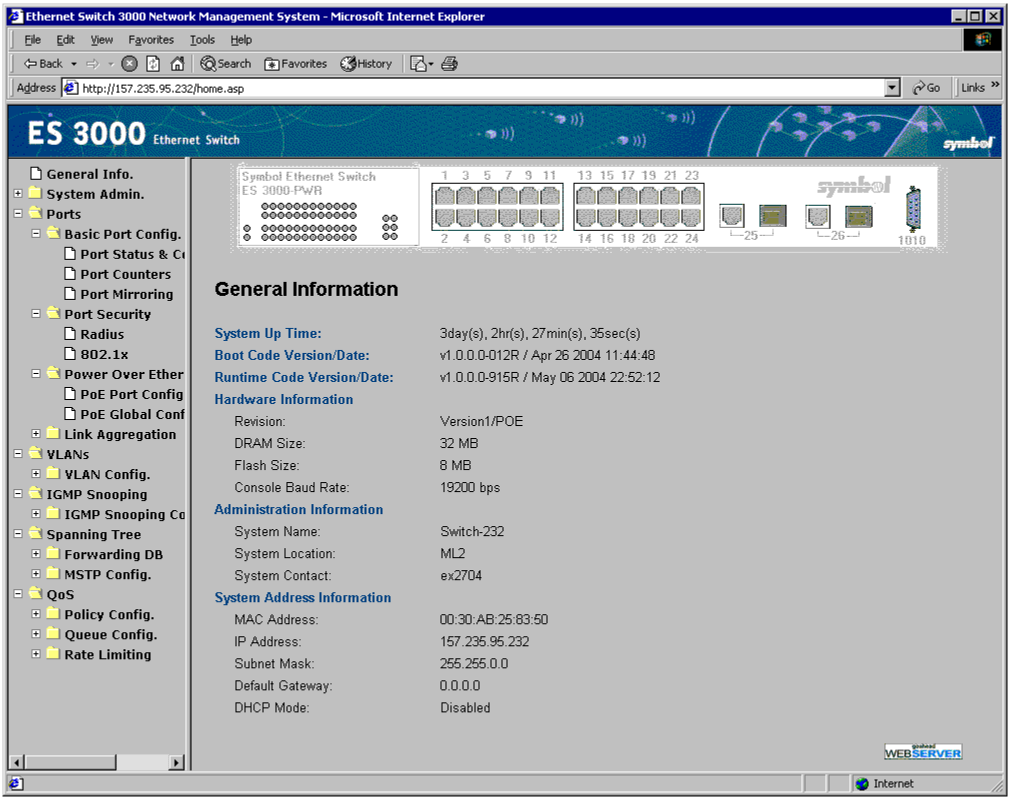
4.1 General Information

The *General Information* screen is a welcome page displaying system information. There are no editable parameters on the screen.

Use the General Information page to access the following submenus:

System Admin	Configure IP address information, management access and user information
Ports	Configure port security, PoE and link aggregation.
VLANs	Create VLANs, Set VLAN IDs and create/modify 802.1q trunk.
IGMP Snooping	Enable IGMP Snooping and VLAN filtering,
Spanning Tree	MSTP configuration, basic and advanced MSTP port configuration.
QoS	Create Policy, create classifier and set in-profile and out-profile actions.

Each submenu item has its own set of options for configuring the ES3000 Ethernet Switch by a specific functional area.



General Information

System Up Time:	3day(s), 2hr(s), 27min(s), 35sec(s)
Boot Code Version/Date:	v1.0.0.0-012R / Apr 26 2004 11:44:48
Runtime Code Version/Date:	v1.0.0.0-915R / May 06 2004 22:52:12
Hardware Information	
Revision:	Version1/POE
DRAM Size:	32 MB
Flash Size:	8 MB
Console Baud Rate:	19200 bps
Administration Information	
System Name:	Switch-232
System Location:	ML2
System Contact:	ex2704
System Address Information	
MAC Address:	00:30:AB:25:83:50
IP Address:	157.235.95.232
Subnet Mask:	255.255.0.0
Default Gateway:	0.0.0.0
DHCP Mode:	Disabled

4.2 Saving Web Interface Configuration Changes

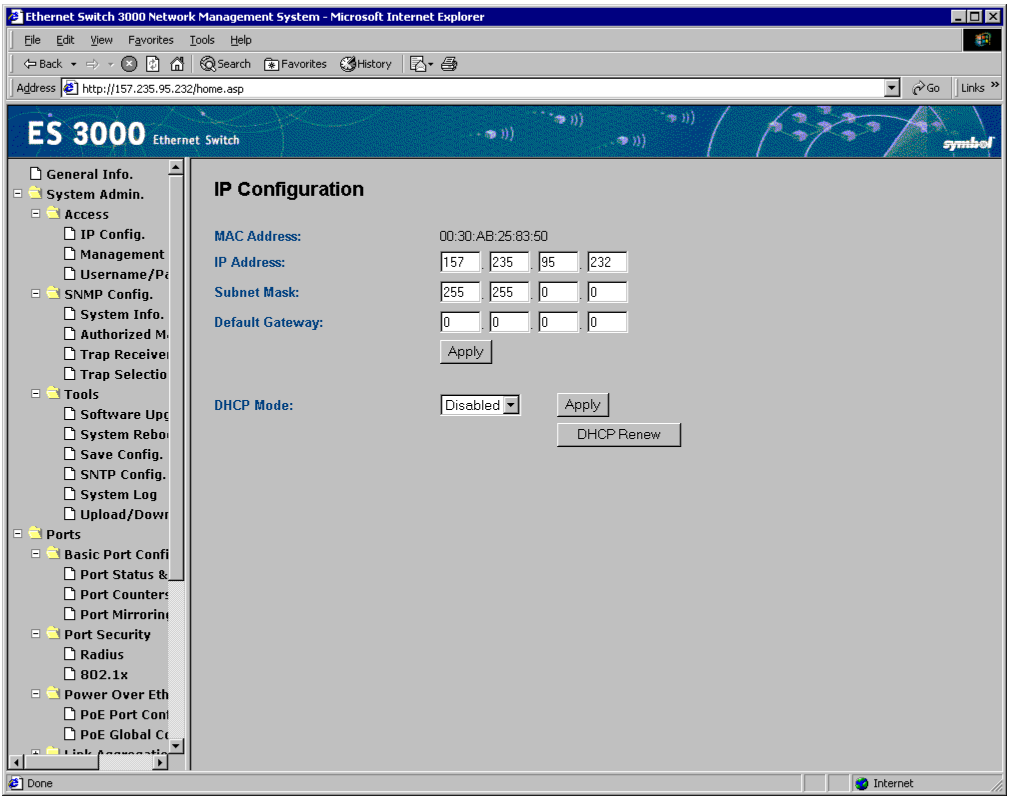
To save changes made within the Web interface, refer to *System Admin->Tools->Save Configuration on page 4-14*. Use the Save Configuration page to save all updates to the Web interface. Once updates are made, refer back to the target configuration page to ensure the updates have been implemented by the ES3000 Ethernet Switch.

4.2.1 System Admin->Access->IP Configuration

The **IP Configuration** menu manages the IP related information of the system.

To manually configure the IP address:

1. Enter a site-specific IP address, Gateway address and Net mask.
2. Click **Apply** to change the IP settings.
3. Save the Configuration to Flash and reset the system to implement the changes.



IP Configuration

MAC Address: 00:30:AB:25:83:50

IP Address: 157 . 235 . 95 . 232

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

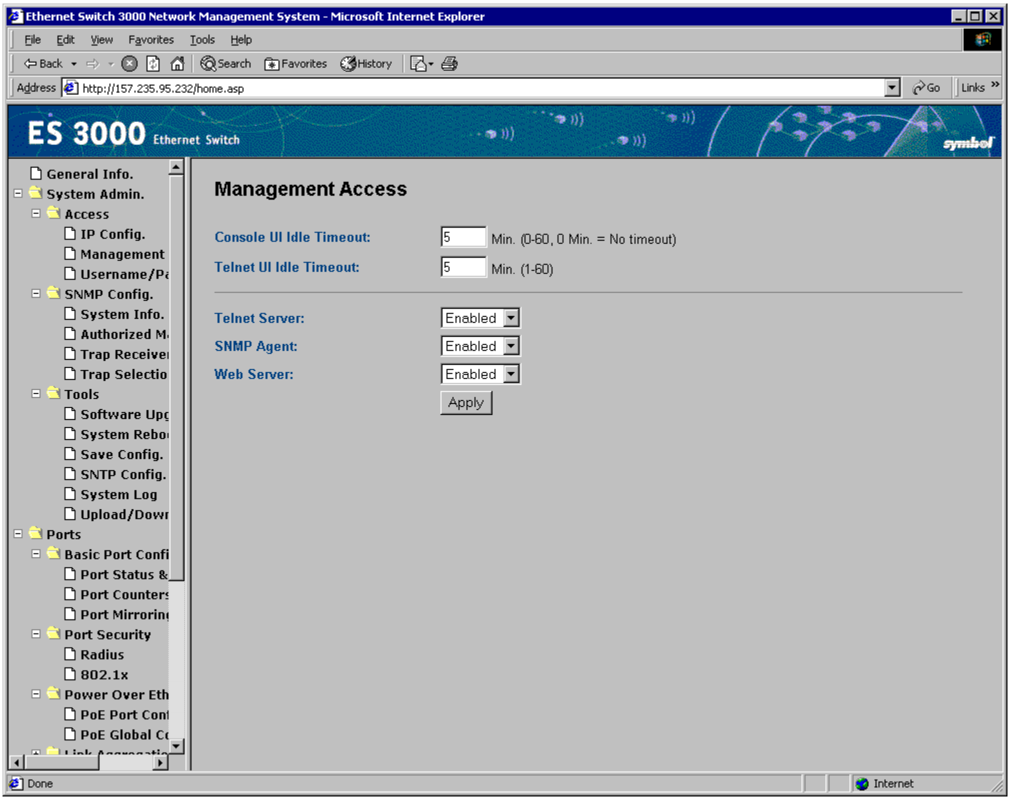
DHCP Mode: Disabled

4.2.2 System Admin->Access->Management Access

Use the **Management Access** screen to enable or disable the Web, SNMP and/or telnet interfaces. Use the Management Access screen to change the user name and password. User names and passwords are case sensitive and can be up to 20 characters long.

Note

Enable/Disable the Web interface from the Management Access screen. The user cannot Enable/Disable the telnet interface from the Management Access screen.



Management Access

Console UI Idle Timeout: 5 Min. (0-60, 0 Min. = No timeout)

Telnet UI Idle Timeout: 5 Min. (1-60)

Telnet Server: Enabled

SNMP Agent: Enabled

Web Server: Enabled

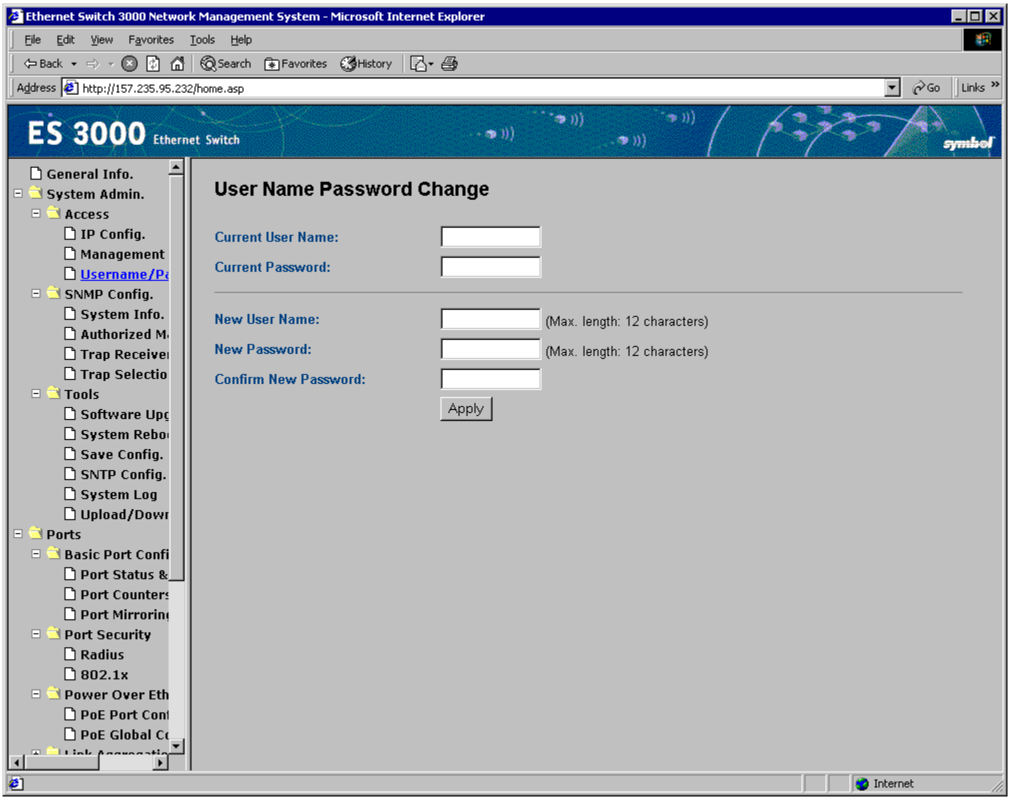
Apply

4.2.3 System Admin->Access->User Name Password Change

The user name and password can be up to 20 characters and are case sensitive. The password entered is encrypted on the screen and displays as a sequence of asterisks (*). Use the **User Name Password Change** screen to:

- Enable or Disable the password protection
- Change the user name and password

Click **Apply** to activate the new password.



User Name Password Change

Current User Name:

Current Password:

New User Name: (Max. length: 12 characters)

New Password: (Max. length: 12 characters)

Confirm New Password:

Apply

4.2.4 System Admin->SNMP Configuration

Simple Network Management Protocol (SNMP) is a messaging protocol allowing communication between network managers and agents. An SNMP manager is part of a network management system (NMS), allowing an administrator to manage the network by making requests to agents. An SNMP agent provides an interface to a managed device containing managed objects in a management information base (MIB).

At the request of an SNMP manager, an SNMP agent retrieves or stores values in the MIB, which contains information about the device and network. The SNMP agent can also send asynchronous traps, which alert the SNMP manager to certain conditions on the network. A trap could result from improper user authentication, PoE power usage over threshold or network topology changes.

Manage the ES3000 by SNMP from a network management station. Configure the switch to participate in the SNMP community and add the host agent to the host table. This prevents unauthorized SNMP access to the switch from non-approved SNMP hosts.

SNMP management features on the switch include:

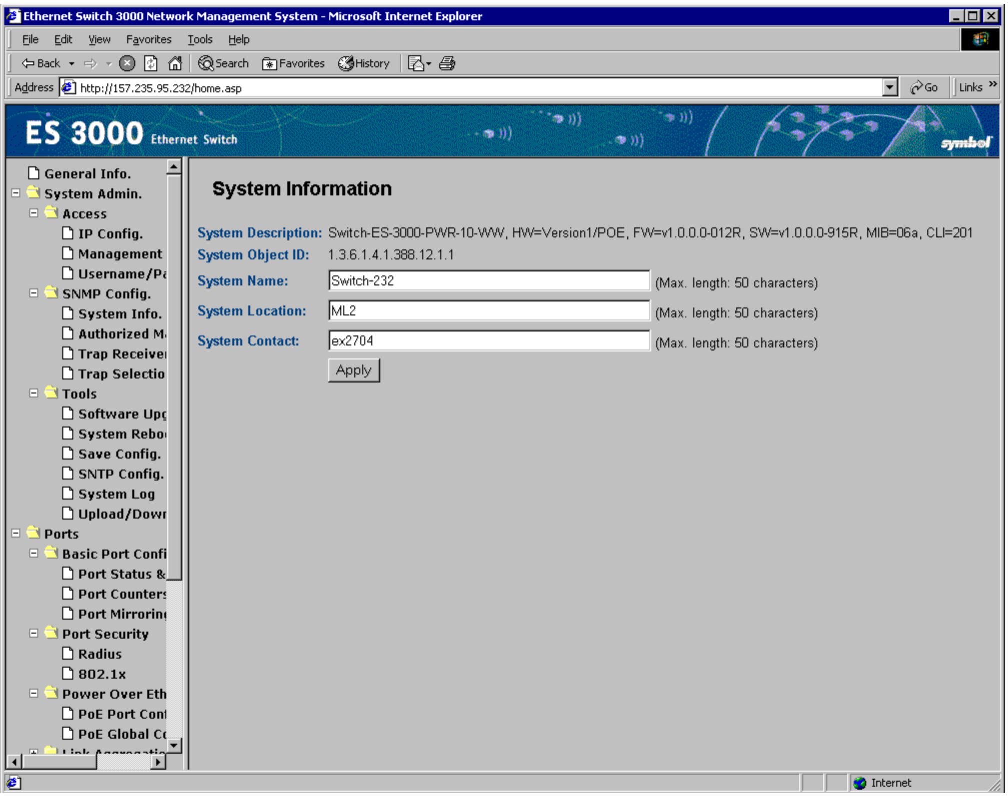
- Simple Network Management Protocol (SNMP)
- Support Standard MIBs:
  - MIB II (RFC1213)
  - Ethernet Interface MIB (RFC1643)
  - Bridge MIB (RFC1493)
  - Enterprise MIB
  - 4-Group RMON (RFC1757)

This menu has three SNMP Settings:

- SNMP Config.
- Trap Receiver Config.
- Individual Trap Config.

4.2.5 System Admin->SNMP Configuration->SNMP Information

Create up to ten different community strings with either READ or READ-WRITE privileges. Set the strings prior to setting host access, as the host table depends on the existence of community strings. The public string has GET privileges by default.



System Information

System Description: Switch-ES-3000-PWR-10-WW, HW=Version1/POE, FW=v1.0.0.0-012R, SW=v1.0.0.0-915R, MIB=06a, CLI=201

System Object ID: 1.3.6.1.4.1.388.12.1.1

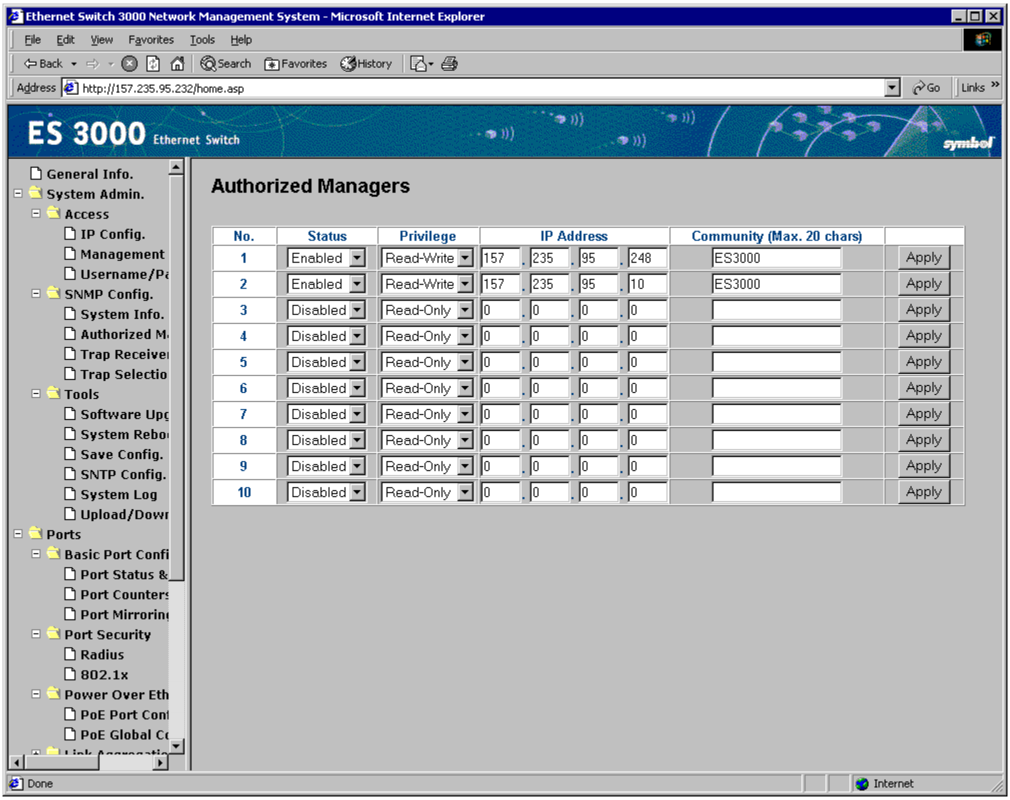
System Name: Switch-232 (Max. length: 50 characters)

System Location: ML2 (Max. length: 50 characters)

System Contact: ex2704 (Max. length: 50 characters)

Apply

4.2.6 System Admin->SNMP Configuration->Authorized Managers



Authorized Managers

No.	Status	Privilege	IP Address				Community (Max. 20 chars)	
1	Enabled	Read-Write	157	235	95	248	ES3000	Apply
2	Enabled	Read-Write	157	235	95	10	ES3000	Apply
3	Disabled	Read-Only	0	0	0	0		Apply
4	Disabled	Read-Only	0	0	0	0		Apply
5	Disabled	Read-Only	0	0	0	0		Apply
6	Disabled	Read-Only	0	0	0	0		Apply
7	Disabled	Read-Only	0	0	0	0		Apply
8	Disabled	Read-Only	0	0	0	0		Apply
9	Disabled	Read-Only	0	0	0	0		Apply
10	Disabled	Read-Only	0	0	0	0		Apply

Use the SNMP Host Table to add and remove hosts from access rights granted to community groups. The permissions GET, SET, and TRAP are assigned to a community name. These permissions are assigned to individual machines by adding those machines and their IP address to the appropriate community string. Host Authorization can be Enabled or Disabled. Use Host Authorization as a security feature to limit people who are not listed in the host table from accessing the switch using SNMP.

4.2.7 System Admin->SNMP Configuration->Trap Receiver

Authentication Traps

When enabled, the system generates an SNMP trap upon a host authorization failure. The failure occurs when a host tries to gain access to the system but the host IP is not in the SNMP host table.

Authentication Failure Trap

Enable	The system generates a SNMP trap upon a host authorization failure
Disable	The authentication traps are not generated

All hosts in community strings with TRAP privileges are notified when a trap condition occurs.

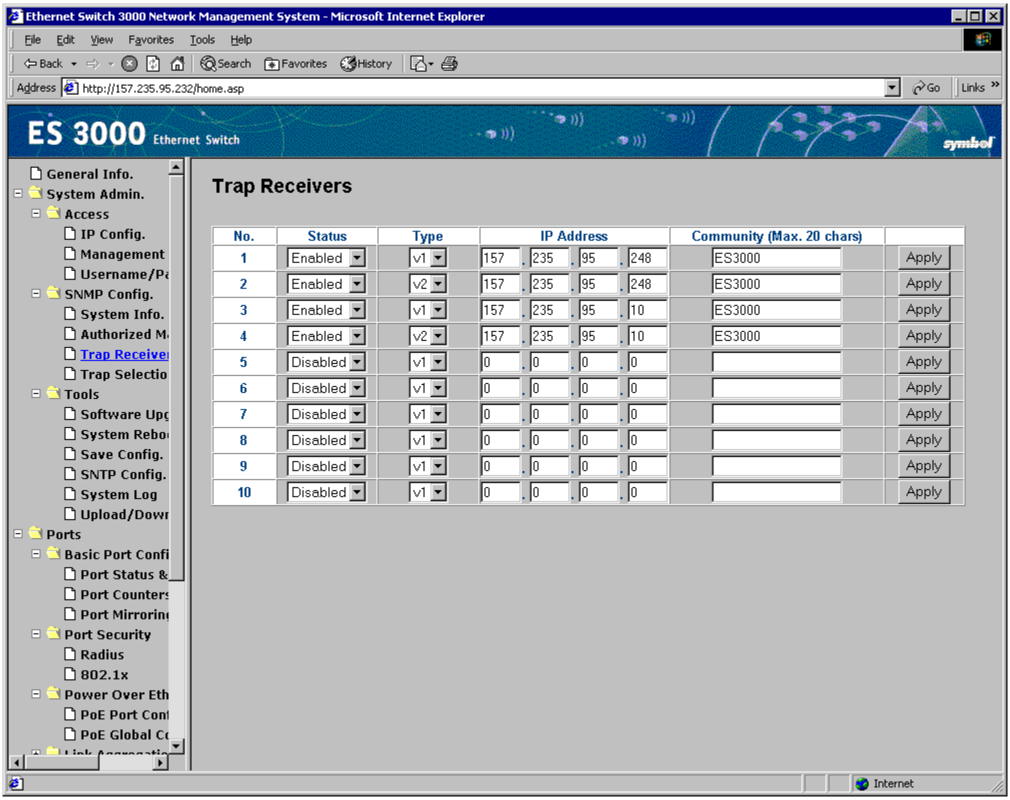
Port Link Down Trap

When enabled, the system generates an SNMP trap upon a port link down. This failure occurs when a link is disconnected. Every port can be enable and/or disable independently.

Link Down Trap

Enable	The system generates a SNMP trap upon a port link down
Disable	The port link down trap is not generated upon a port link down

As authentication failure trap, all hosts in community strings with TRAP privileges are notified when a trap condition occurs.



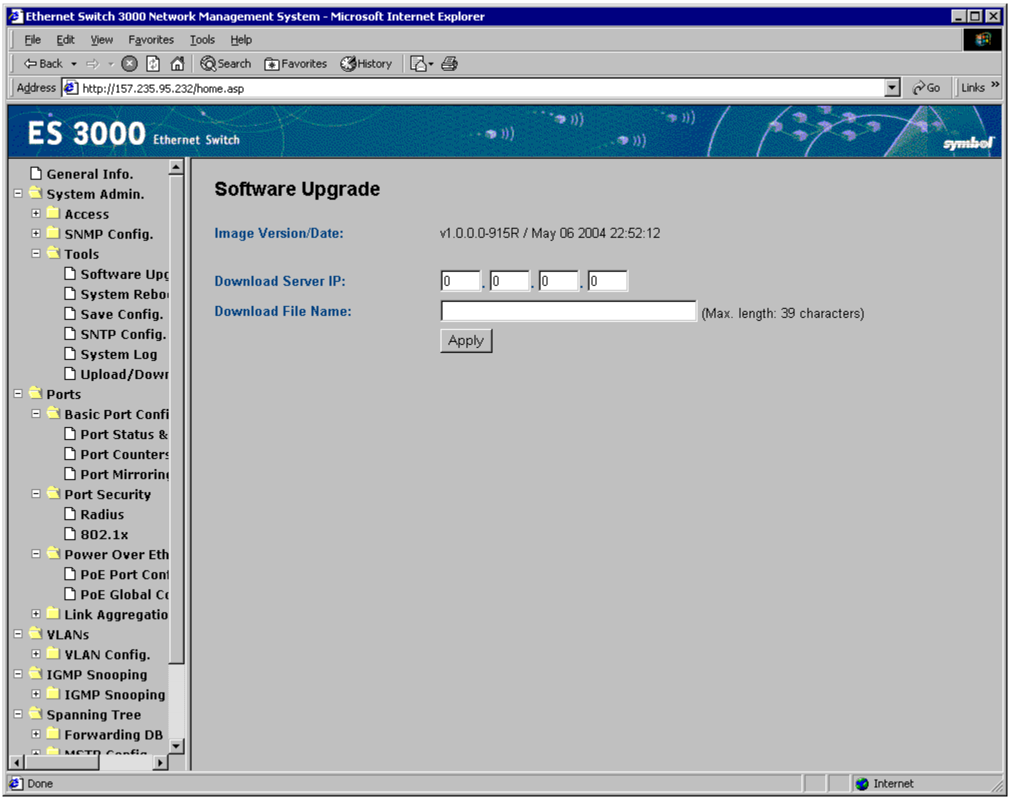
Trap Receivers

No.	Status	Type	IP Address				Community (Max. 20 chars)	
1	Enabled	v1	157	235	95	248	ES3000	Apply
2	Enabled	v2	157	235	95	248	ES3000	Apply
3	Enabled	v1	157	235	95	10	ES3000	Apply
4	Enabled	v2	157	235	95	10	ES3000	Apply
5	Disabled	v1	0	0	0	0		Apply
6	Disabled	v1	0	0	0	0		Apply
7	Disabled	v1	0	0	0	0		Apply
8	Disabled	v1	0	0	0	0		Apply
9	Disabled	v1	0	0	0	0		Apply
10	Disabled	v1	0	0	0	0		Apply

4.2.8 System Admin->Tools->Software Upgrade

Use the **Software Upgrade** menu to upgrade the software for the switch through TFTP protocol, reboot the system with variety options and save configuration to Flash and View Statistic information.

If new improvements to the software that runs the switch become available, use the Software Upgrade menu to upgrade the switch to the new software release. Once the IP address of the TFTP and the path location of the new software image file is properly configured, the user can choose to boot the switch using one of three options.



Software Upgrade

Image Version/Date: v1.0.0.0-915R / May 06 2004 22:52:12

Download Server IP: 0 . 0 . 0 . 0

Download File Name: (Max. length: 39 characters)

4.2.9 System Admin->Tools->System Reboot

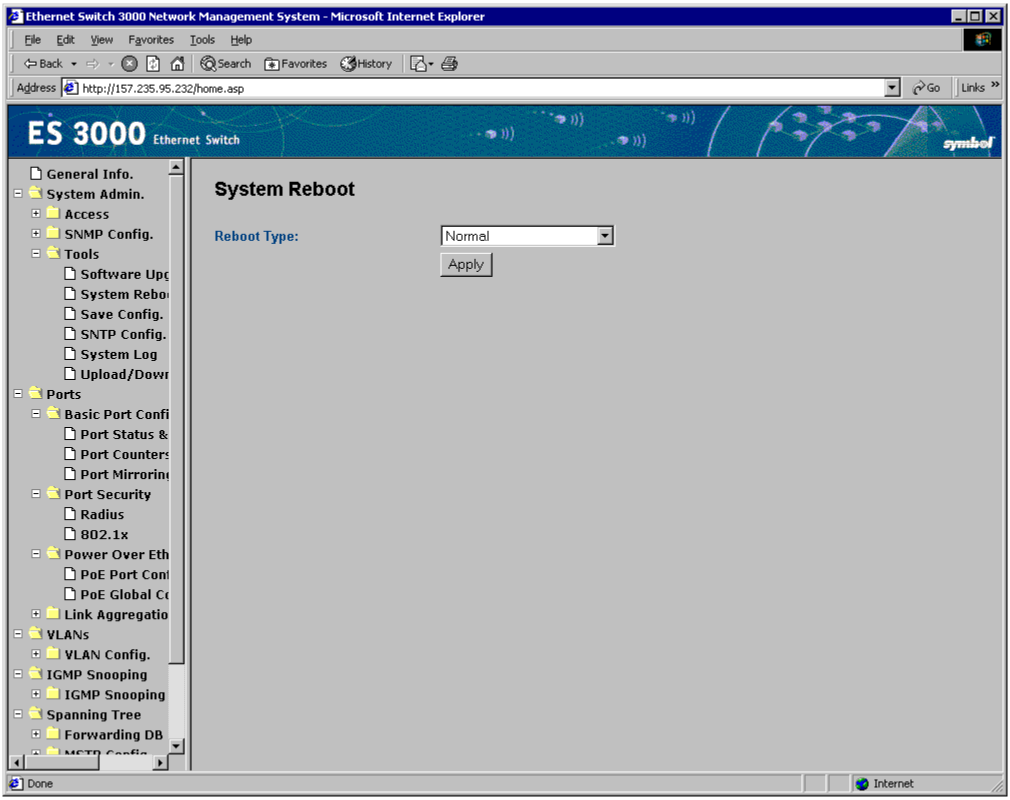
Two options are provided when the system reboots,

Reboot Status:

Stop:	Shutdown the system
Start:	Reboot the system

Reboot Type

Normal:	Boot up with runtime configuration
Factory Default:	Boot up with factory default configuration



System Reboot

Reboot Type: Normal

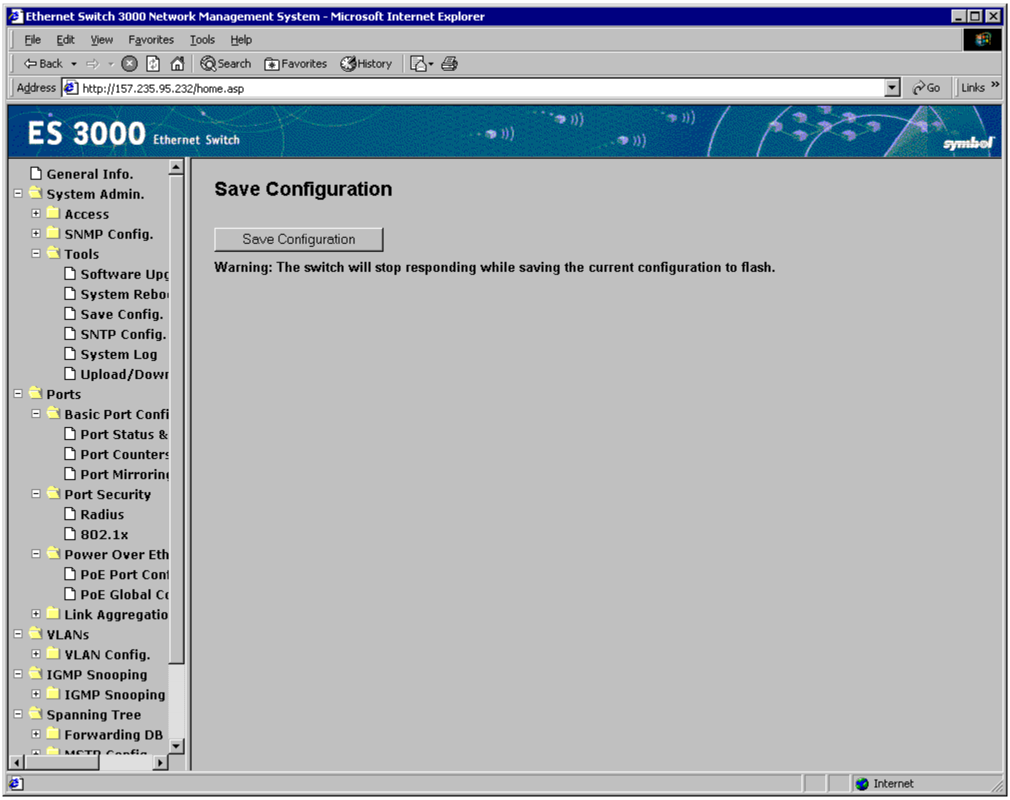
Apply

4.2.10 System Admin->Tools->Save Configuration

After making changes to the screens within the Web Interface, save the changed settings to Flash. If changes are not saved to NVRAM, they are lost during the next switch reset or reboot. Use the *Save Configuration* page as the central location to save changes made within the ES3000 Ethernet Switch Web interface. Once changes have been saved to the system using the Save Configuration page, refer back to the target configuration screen to ensure the changes have been implemented by the ES3000 Ethernet Switch.

Note

Network IP settings (IP address, Gateway Address, Network Mask) are not be affected by the Restore command.



Save Configuration

Save Configuration

Warning: The switch will stop responding while saving the current configuration to flash.

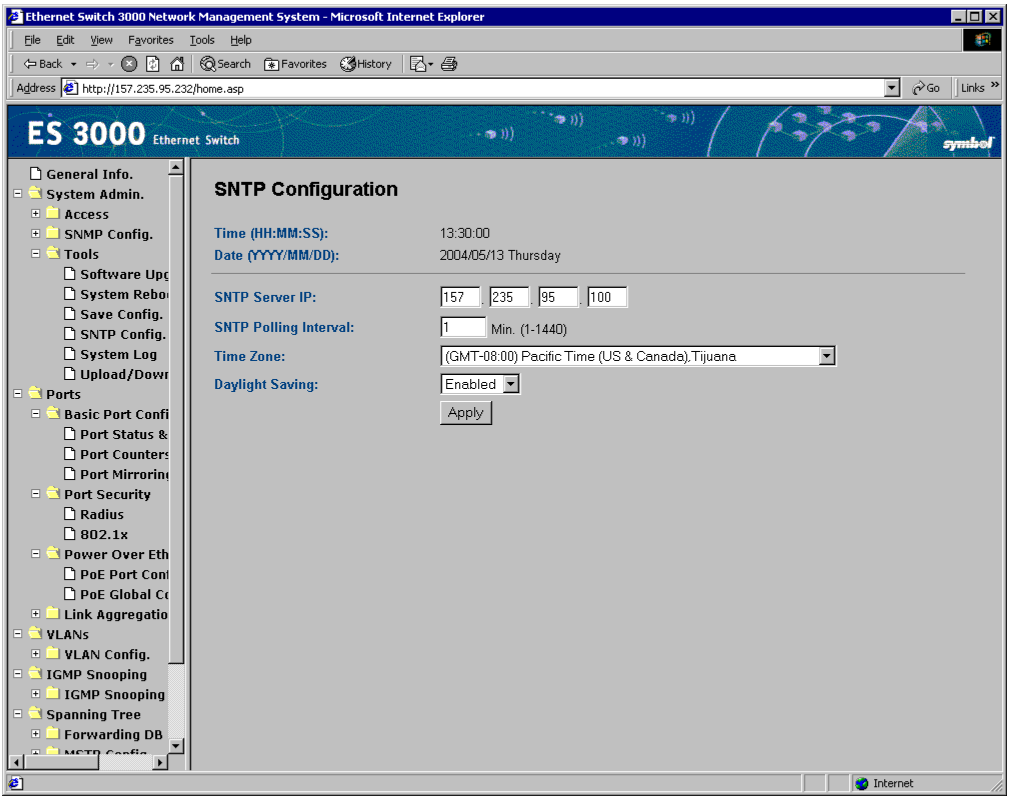
4.2.11 System Admin->Tools->SNTP Configuration

Use the following editable functions in the **SNTP Configuration** page are required:

Set SNTP Server IP Simple Network Time Protocol, user can enter SNTP server IP to get into it.

Set SNTP Interval Set up SNTP polling interval (1min for example).

Set Time Zone Set up the time zone, like Casablance, Monrovia



SNTP Configuration

Time (HH:MM:SS): 13:30:00
Date (YYYY/MM/DD): 2004/05/13 Thursday

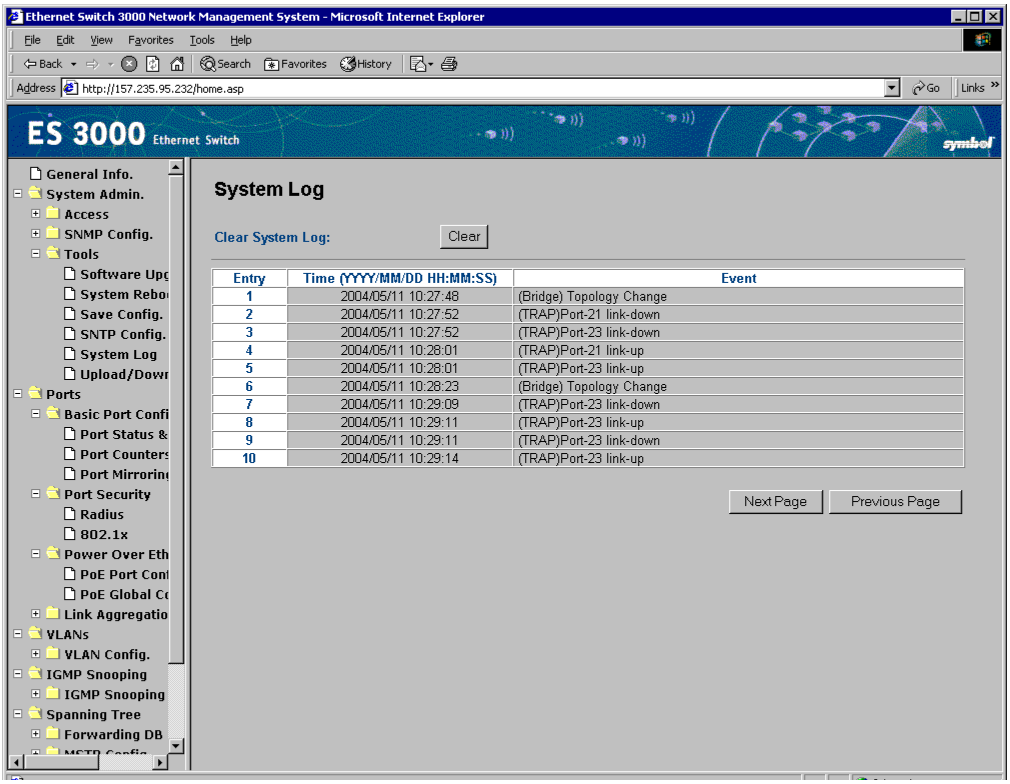
SNTP Server IP: 157 . 235 . 95 . 100
SNTP Polling Interval: 1 Min. (1-1440)
Time Zone: (GMT-08:00) Pacific Time (US & Canada),Tijuana
Daylight Saving: Enabled

Apply

4.2.12 System Admin->Tools->System Log Menu

Use the **System Log Menu** to trace the entry when and from where, then users can know the entry system history.

Select **Clear** to clean the table.



System Log

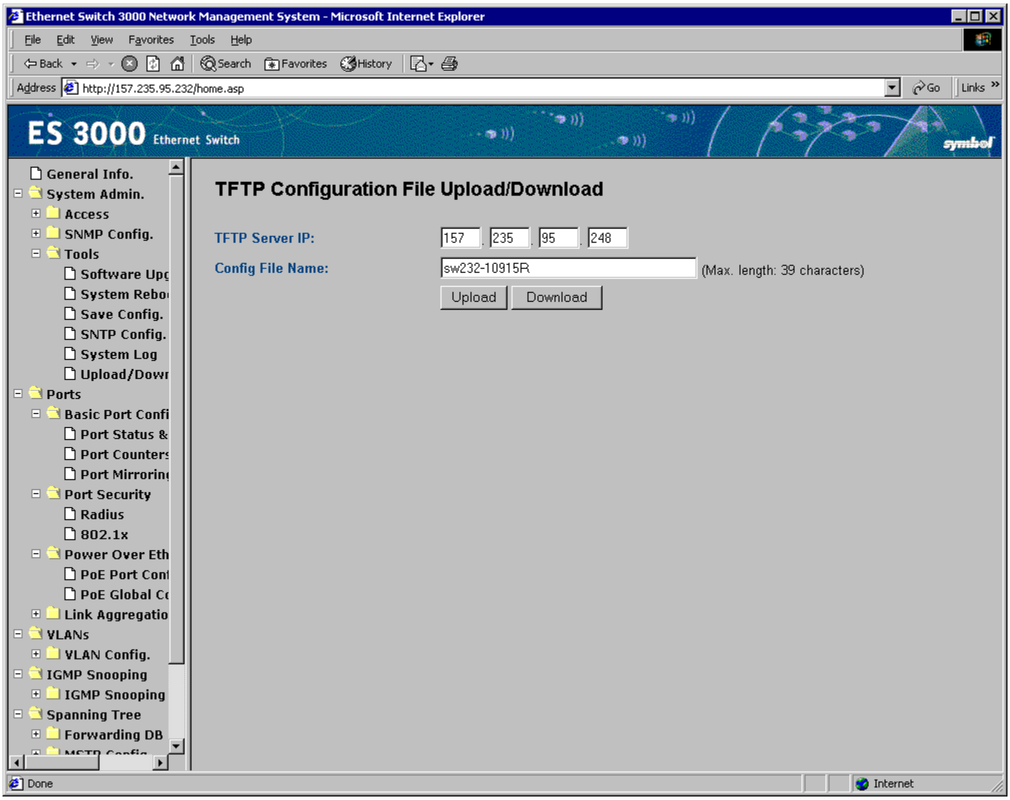
Clear System Log: Clear

Entry	Time (YYYY/MM/DD HH:MM:SS)	Event
1	2004/05/11 10:27:48	(Bridge) Topology Change
2	2004/05/11 10:27:52	(TRAP)Port-21 link-down
3	2004/05/11 10:27:52	(TRAP)Port-23 link-down
4	2004/05/11 10:28:01	(TRAP)Port-21 link-up
5	2004/05/11 10:28:01	(TRAP)Port-23 link-up
6	2004/05/11 10:28:23	(Bridge) Topology Change
7	2004/05/11 10:29:09	(TRAP)Port-23 link-down
8	2004/05/11 10:29:11	(TRAP)Port-23 link-up
9	2004/05/11 10:29:11	(TRAP)Port-23 link-down
10	2004/05/11 10:29:14	(TRAP)Port-23 link-up

4.2.13 System Admin->Tools->TFTP Configuration File Upload/ Download

There are fours functions in the page **TFTP Configuration File Upload/Download** page:

Set TFTP Server IP Address	enter the server IP address to get the TFTP server.
Set Configuration File Name	enter the file name that they want to config
Upload Configuration File	upload the configuration file
Download Configuration File	download configuration file from a TFTP server



TFTP Configuration File Upload/Download

TFTP Server IP: 157 . 235 . 95 . 248

Config File Name: sw232-10915R (Max. length: 39 characters)

4.2.14 System Admin->Ports->Port Status and Configuration

Configure the characteristics related to link operations. All of the parameters on the **Port Status and Configuration** page are toggle settings. To change, or toggle, between options, hit **Ctrl-M** to move the curser to the ports field and strike the space bar when the appropriate option is highlighted. To modify ports 17 to 26, tab through ports 1 to 16. The comments field is available to enter a description of the port.

Type

The type of port, this field is not user configurable.

Admin field

Enables or Disables the port.

Link

The status of a port, it is **Up** when a port is connected and active.

Mode

Offers the choice of Full-duplex, Half-duplex, or Auto negotiation as well as speed selection among 10Mbps, 100Mbps, 1000Mbps or auto negotiation. Enabling auto-negotiation on a port allows a port to sense the communication speed and negotiate the duplex mode (full duplex or half duplex) automatically. The ports select the highest possible throughput. The port can auto-negotiate with any port that is compliant with IEEE 802.3u. If the other port is not IEEE802.3u compliant, the port defaults to half-duplex, 10 Mbps mode. Users can operate the communication speed and duplex mode manually.

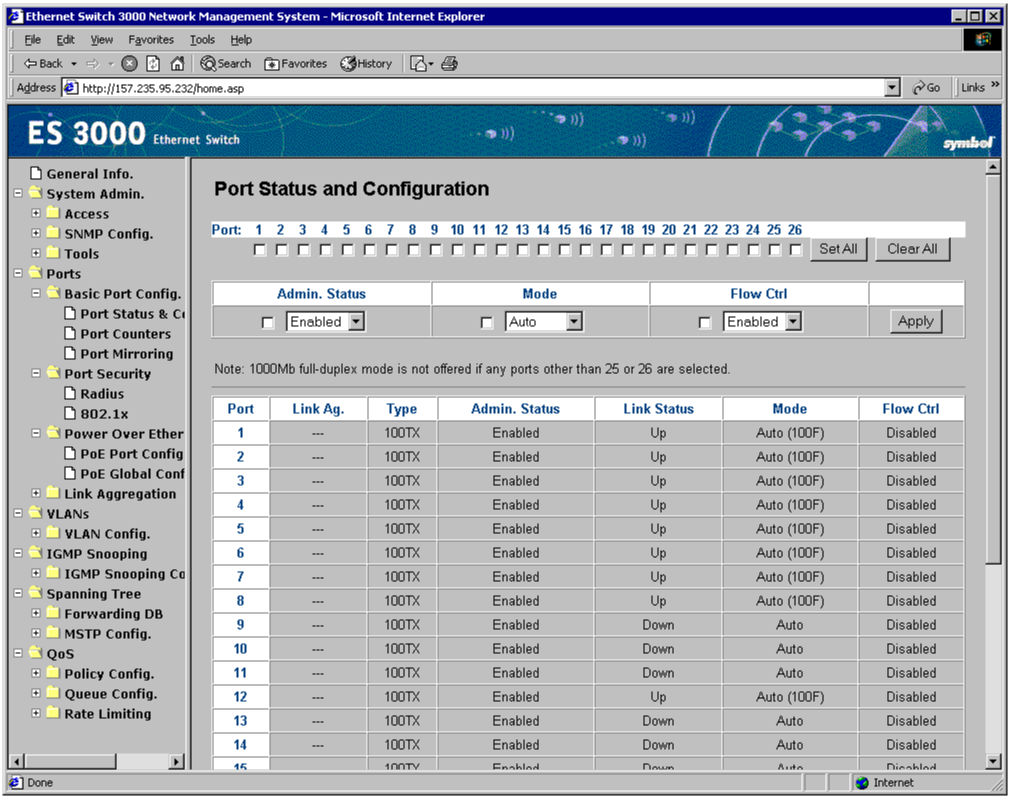
Flow Control

Enables or disables Flow Control. Flow control is a protocol preventing packets from being dropped by reducing the amount of traffic to a level that can be accommodated. If enabled on both ends of a connection, it prevents the sender from sending data until the receiver can accept it. The switch complies with the IEEE802.3x flow control standard.

Gigabit Ports

For the two-gigabit ports on each switch, the port type can be chosen. The default is the port using the RJ-45 interface. Select the GBIC interface by plugging a GBIC connector. The GBIC interface has higher priority than the shared RJ-45 interface.

Note Enabling the GBIC connector for a Gigabit Ethernet port disables the built-in 1000BASE-T port. GBIC ports do not support Auto Negotiation. Manually configure the GBIC port. The default values are 1000 Mbps, full duplex.



Port Status and Configuration

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

Set All Clear All

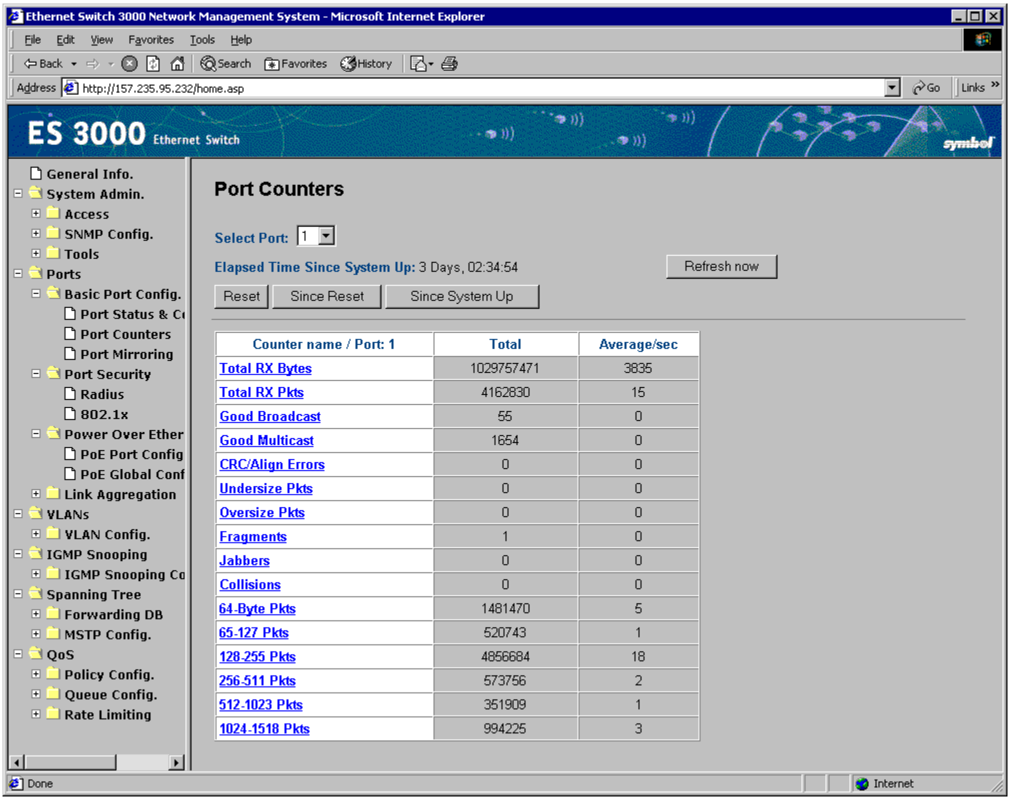
Admin. Status	Mode	Flow Ctrl	
☐ Enabled	☐ Auto	☐ Enabled	Apply

Note: 1000Mb full-duplex mode is not offered if any ports other than 25 or 26 are selected.

Port	Link Ag.	Type	Admin. Status	Link Status	Mode	Flow Ctrl
1	---	100TX	Enabled	Up	Auto (100F)	Disabled
2	---	100TX	Enabled	Up	Auto (100F)	Disabled
3	---	100TX	Enabled	Up	Auto (100F)	Disabled
4	---	100TX	Enabled	Up	Auto (100F)	Disabled
5	---	100TX	Enabled	Up	Auto (100F)	Disabled
6	---	100TX	Enabled	Up	Auto (100F)	Disabled
7	---	100TX	Enabled	Up	Auto (100F)	Disabled
8	---	100TX	Enabled	Up	Auto (100F)	Disabled
9	---	100TX	Enabled	Down	Auto	Disabled
10	---	100TX	Enabled	Down	Auto	Disabled
11	---	100TX	Enabled	Down	Auto	Disabled
12	---	100TX	Enabled	Up	Auto (100F)	Disabled
13	---	100TX	Enabled	Down	Auto	Disabled
14	---	100TX	Enabled	Down	Auto	Disabled
15	---	100TX	Enabled	Down	Auto	Disabled

4.2.15 System Admin->Ports->Port Counters

Use the **Port Counters** screen to select the target port for displaying port information. Selected a target port form the **Select Port** pull-down menu and click **Apply** to display counter information for that port. Refer to the **Total** list and the **Average/sec** list for data. Click **Refresh now** to update the data displayed for the selected port.



Port Counters

Select Port: 1

Elapsed Time Since System Up: 3 Days, 02:34:54

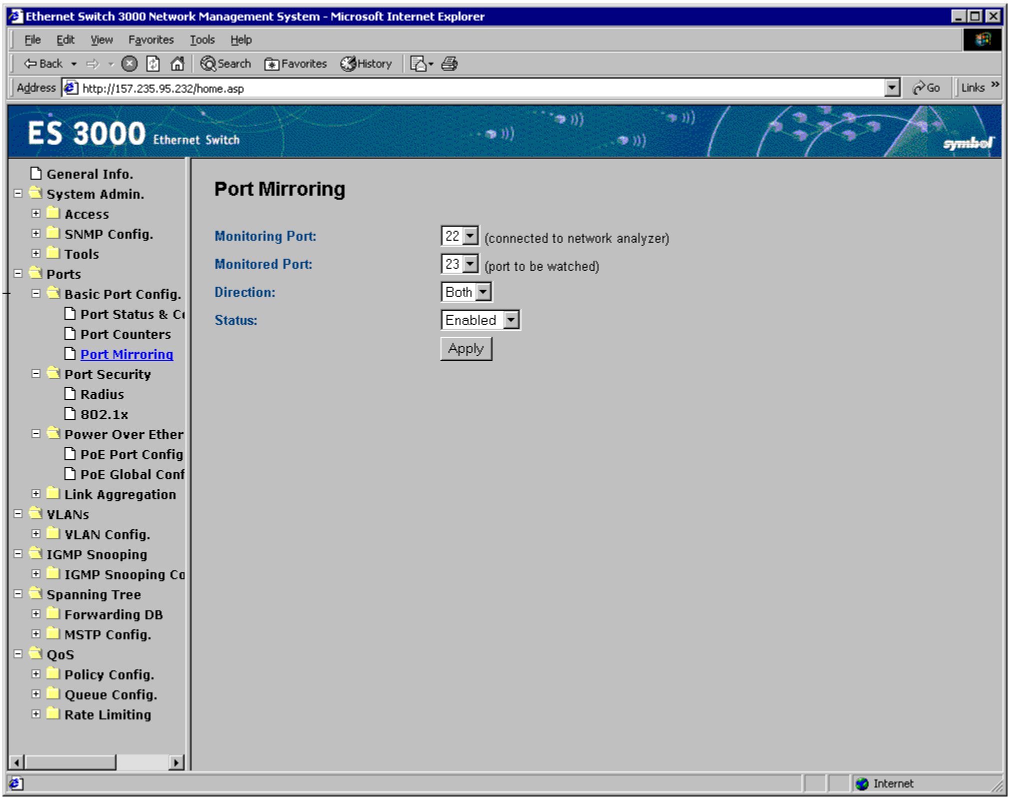
Counter name / Port: 1	Total	Average/sec
Total RX Bytes	1029757471	3835
Total RX Pkts	4162830	15
Good Broadcast	55	0
Good Multicast	1654	0
CRC/Align Errors	0	0
Undersize Pkts	0	0
Oversize Pkts	0	0
Fragments	1	0
Jabbers	0	0
Collisions	0	0
64-Byte Pkts	1481470	5
65-127 Pkts	520743	1
128-255 Pkts	4856684	18
256-511 Pkts	573756	2
512-1023 Pkts	351909	1
1024-1518 Pkts	994225	3

4.2.16 System Admin->Ports->IP (Port) Mirroring

Port mirroring allows one port on the ES3000 to see all of the packets passing through any other port on the switch. Usually, a network analyzer is attached to the monitoring port so the network administrator can debug problems with the monitored port.

The ES3000 has two gigabit Ethernet ports, ports 25 and 26. A 10/100BaseT port would not be able to keep up with the packet flow on a gigabit port. Only another gigabit port may monitor a gigabit port. Any port on the ES3000 may be used to monitor ports 1 through 24, the 10/100BaseT ports.

Use Port mirroring to assist in the debugging of a network. The Port Mirroring Web interface page allows the user to Enable or Disable port mirroring and set the source and monitor ports. The monitor port displays a copy of every packet arriving or leaving the source port.



Port Mirroring

Monitoring Port: 22 (connected to network analyzer)

Monitored Port: 23 (port to be watched)

Direction: Both

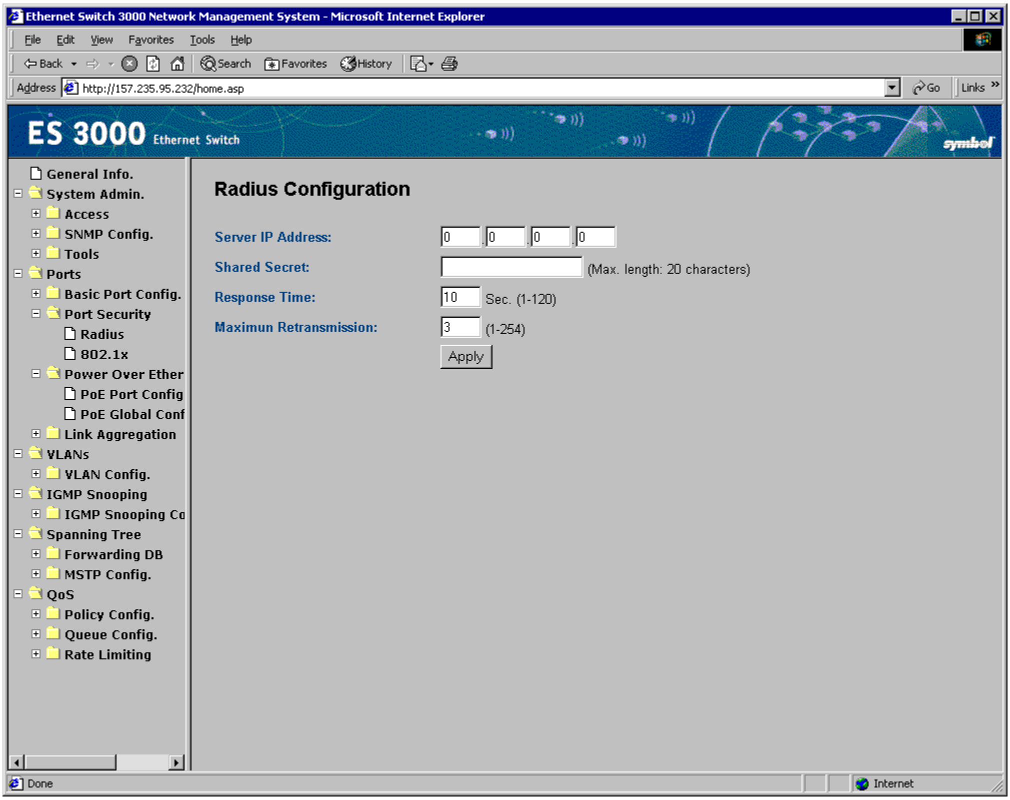
Status: Enabled

Apply

4.2.17 System Admin->Ports->Port Security ->Radius Configuration

Use the **Radius Configuration** screen to configure switch advanced security settings to limit the access to management interfaces. There are two advanced security options beyond the basic password protection: RADIUS client authentication and 802.1X port authentication. If a RADIUS server is on the network, configure the authentication of management access through a RADIUS server.

RADIUS server authentication does not affect traffic passing through the switch, only authenticates access to the switch management. The same is true for 802.1X port authentication. Only users with specific IP addresses can be allowed access to the management features, thus preventing unauthorized personnel from accessing the switch.



Radius Configuration

Server IP Address: 0 . 0 . 0 . 0

Shared Secret: (Max. length: 20 characters)

Response Time: 10 Sec. (1-120)

Maximun Retransmission: 3 (1-254)

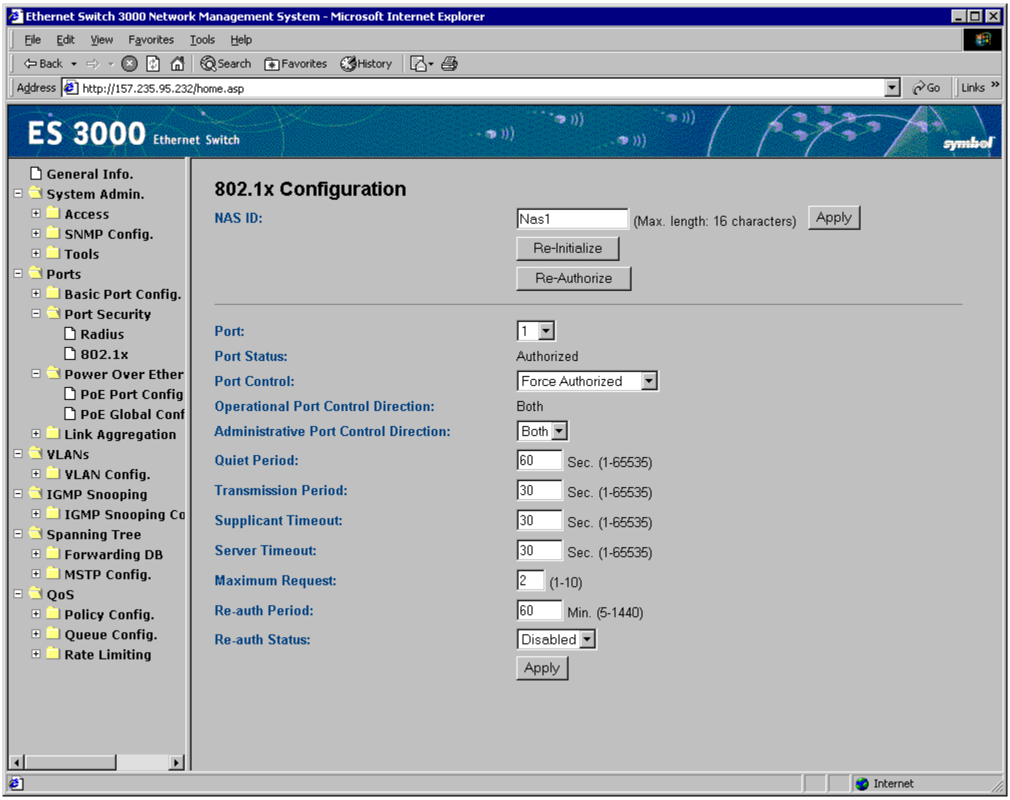
Apply

4.2.18 System Admin->Ports->Port Security ->802.1x Configuration

Use the **802.1x** screen to:

- Create the NAS ID used for connection
- Configure the port to pass security to
- Set port control type
- Set the operational or administrative control direction
- Define the transmission period
- Configure the supplicant requiring and server responding time
- Set the maximum request times and the quiet period if there is no any activity.

Configure the re-authentication period when the re-authentication status is Enabled, then go back to the initial status by going to initialize or re-authentication initialize.



802.1x Configuration

NAS ID: Nas1 (Max. length: 16 characters) Apply

Re-Initialize

Re-Authorize

Port: 1

Port Status: Authorized

Port Control: Force Authorized

Operational Port Control Direction: Both

Administrative Port Control Direction: Both

Quiet Period: 60 Sec. (1-65535)

Transmission Period: 30 Sec. (1-65535)

Supplicant Timeout: 30 Sec. (1-65535)

Server Timeout: 30 Sec. (1-65535)

Maximum Request: 2 (1-10)

Re-auth Period: 60 Min. (5-1440)

Re-auth Status: Disabled

Apply

4.2.19 System Admin->Ports->Power over Ethernet

Use Power-over-Ethernet (PoE) to eliminate using a 110/220 VAC power source to power access points and other devices on a wired LAN. If using a Power-over-Ethernet system, only a single CAT5 Ethernet cable carrying both power and data to each device is required. The single cable scheme provides greater flexibility in the placement of access points and network devices and can significantly decrease installation costs.

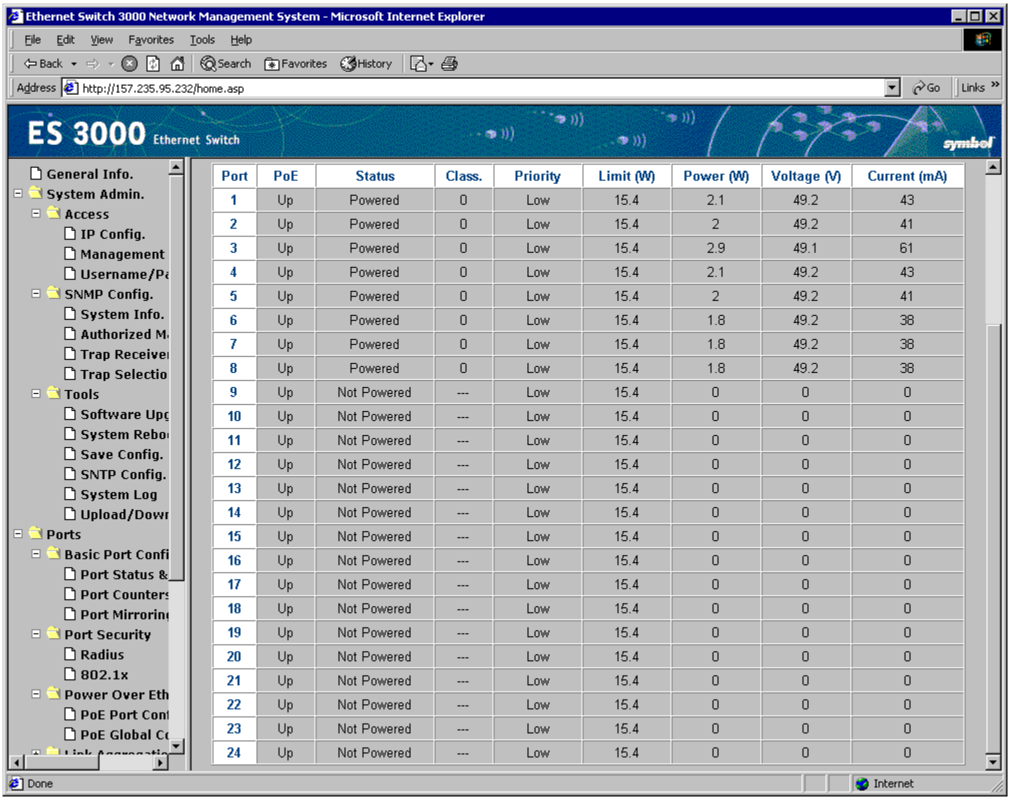
Two configuration pages exist for the PoE function. The first allows per port configuration for specific power restrictions on an individual port basis. The second configuration page is used for global configurations that apply switch-wide.

The ES3000 has a maximum PoE power budget of 170 watts. This is enough to supply 7 watts to all 24 PoE ports on the switch. The switch supplies a maximum of 16.5 watts per port.When a new powered device is connected to a port, the ES3000 switch checks whether enough power remains in the power budget to support the device. This decision is based on the actual power drawn by the powered devices at the time of connection, rather than their maximum power consumption. If there is insufficient power to supply all PoE-enabled ports, the switch does not power all ports. The administrator can select the method the ES3000 switch uses to decide which ports receive power.

The ES3000 can sense whether a powered device is attached to a port. The switch supplies power only to devices that need it. The switch initially uses resistance detection (802.3af) to determine whether a port requires power. If that fails, and if capacitance detection is enabled, the switch then uses capacitance detection to determine whether the port needs power. This allows the switch to detect the presence of older powered devices, which might not be 802.3af compliant.

4.2.20 System Admin->Ports->Power over Ethernet->Port Configuration

The **Port Configuration** page provides a port-by-port selection option for the PoE function. To set up administration, priority and/or limit, apply one or more ports simultaneously.



Port	PoE	Status	Class.	Priority	Limit (W)	Power (W)	Voltage (V)	Current (mA)
1	Up	Powered	0	Low	15.4	2.1	49.2	43
2	Up	Powered	0	Low	15.4	2	49.2	41
3	Up	Powered	0	Low	15.4	2.9	49.1	61
4	Up	Powered	0	Low	15.4	2.1	49.2	43
5	Up	Powered	0	Low	15.4	2	49.2	41
6	Up	Powered	0	Low	15.4	1.8	49.2	38
7	Up	Powered	0	Low	15.4	1.8	49.2	38
8	Up	Powered	0	Low	15.4	1.8	49.2	38
9	Up	Not Powered	---	Low	15.4	0	0	0
10	Up	Not Powered	---	Low	15.4	0	0	0
11	Up	Not Powered	---	Low	15.4	0	0	0
12	Up	Not Powered	---	Low	15.4	0	0	0
13	Up	Not Powered	---	Low	15.4	0	0	0
14	Up	Not Powered	---	Low	15.4	0	0	0
15	Up	Not Powered	---	Low	15.4	0	0	0
16	Up	Not Powered	---	Low	15.4	0	0	0
17	Up	Not Powered	---	Low	15.4	0	0	0
18	Up	Not Powered	---	Low	15.4	0	0	0
19	Up	Not Powered	---	Low	15.4	0	0	0
20	Up	Not Powered	---	Low	15.4	0	0	0
21	Up	Not Powered	---	Low	15.4	0	0	0
22	Up	Not Powered	---	Low	15.4	0	0	0
23	Up	Not Powered	---	Low	15.4	0	0	0
24	Up	Not Powered	---	Low	15.4	0	0	0

There are 8 parameters for each port. 3 of the 8 parameters are user configurable, the other 5 are values assigned by the system to display information on the power supplied.

Admin: The administration decision on providing power to a port. Two parameters are,

Up: Power is allowed on this port. The default value is **Up**.

Down: Power is not allowed on this port. When Admin is set to **Down**, all other parameters are meaningless.

The user can change the administration configuring Admin to either Enable or Disable.

Status: The status of the port. When a power device is connected and power is provided, **Powered** is displayed for the port.

Class: 4 classes are specified within IEEE 802.3af to help determine the maximum number of PDs the system can support.

Class	Usage	PSE Output Max. Power (W)	PD Power
0	Default	15.4	0.44 - 12.95W
1	Optional	4.0	0.44 - 3.84W
2	Optional	7.0	3.84 - 6.49W
3	Optional	15.4	6.49 - 12.95W
4	Reserved for future use	As class 0	Reserved for future use

The **Classification** option within IEEE 802.3af provides the capability for PSE to learn the maximum power needed for connected PDs. The PSE reserves the needed power for every device to avoid power shortage of any connected and powered devices.

Priority: The Priority field defines the priority of the target PoE port. Three selections are available, **Critical**, **High** and **Low**. When the power consumption is over the power budget, ports defined as Critical have priority. Ports defined as Low are shut down The default is **Low** for every port. Therefore, the user is required to prioritize ports accordingly to configure a port power supply hierarchy.

Limit (mW): The maximum power supplied to a port. The default is **15.4W** or 15000mW

Power (mW): The power currently provided to the powered device. The unit is expressed in milliwatts.

Voltage (V): Voltage of power provides to powered device currently. The unit is Volt.

Current (mA): Current of power provides to powered device currently. The unit is milliamp.

Example:

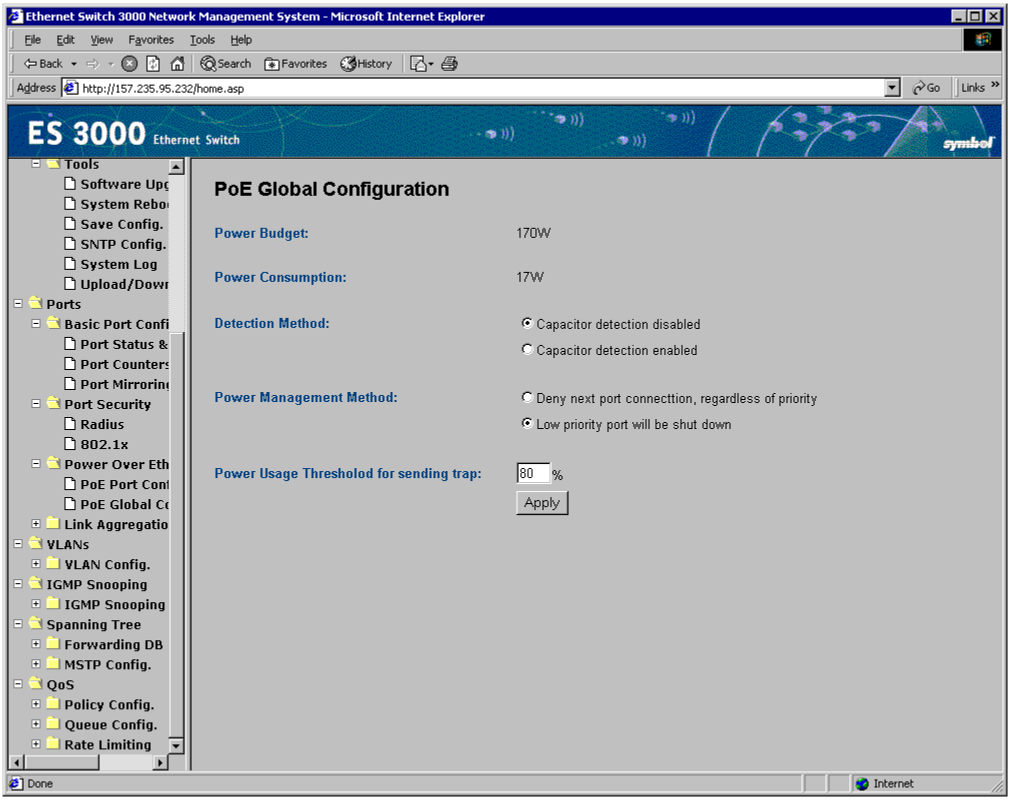
The switch ports could require a PoE scheme similar to the following:

Port	***Admin***	***Priority***	***Limit***
1, 5	Down	N/A	N/A
2, 6	Up	Critical	15.4W
3, 7	Up	High	15.4W
4	Up	Critical	7.0W
8	Up	High	6.0W

1. The administrator needs to click ports 1 and 5 and choose **Disable**.
2. Select **Apply** to disable ports 1 and 5.
3. Continue selecting ports and defining their PoE priority. Click **Apply** when completed.

4.2.21 System Admin->Ports->Power over Ethernet->PoE Global Configuration

Use the PoE Global Configuration page to modifying a global set up of PoE functions, including detection method, power management method, and power usage threshold. The first parameter is the power budget, pre-determined by the power supply and not configurable by user. The power supply in the ES3000 Ethernet Switch is 225W. 170W is dedicated to the powered devices as a power budget. The switch is capable of providing power to 11 devices requiring a maximum power of 15.4W per device.



PoE Global Configuration

Power Budget: 170W

Power Consumption: 17W

Detection Method:
● Capacitor detection disabled
○ Capacitor detection enabled

Power Management Method:
○ Deny next port connecttion, regardless of priority
● Low priority port will be shut down

Power Usage Thresholod for sending trap: 80 %

Apply

4.2.22 PoE Determination Flowchart

Power Budget: Maximum power allowed for powered devices. 170W for the ES3000 switch.

Detection Method: The powered device detection method. Older devices could contain a capacitor. If this option is disabled (default), capacitor devices are not detected and powered. Newer devices are detected regardless if the Detection Method option is enabled or disabled.

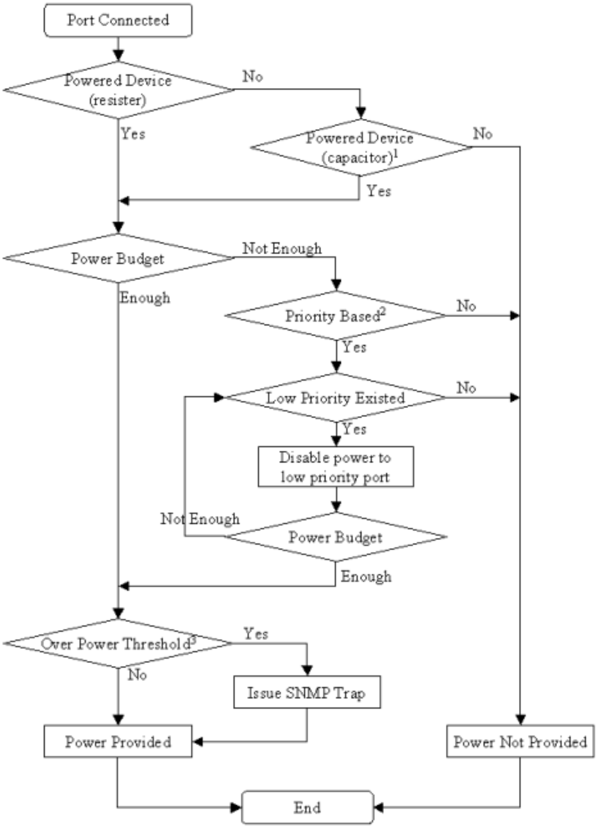
Power Management Method: When the power budget is running out as more powered devices connected to the system, the system needs an algorithm to determine the power service for the next powered device. It could potentially deny the service requested of the new device or disable current connected devices to provide power to the new device. Two options are given to the administrator,

.

- **Deny next port connection, regardless of priority**: The switch keeps providing power to current connected powered devices and ignores the requests of the newly connected device. The priority set up of each port is ignored.

- **Low priority port will be shutdown**. When a newly powered device is connected, the switch searches among its currently connected and powered devices. If any port has lower priority than the newly connected port, the switch discontinues the power supply to the lower priority port and provides power to the newly connected port. If this power budget from disabling one low priority port is not enough, the switch disables the next low priority port and so on until the power budget is enough. If there are no low priority ports or not enough power, the newly connected device is not powered.

Power Usage Threshold: The Power Usage Threshold is the threshold to enable the SNMP trap. The default value is 80% and is configurable by the administrator. If the power budget is consumed, an SNMP trap is sent to the associated receivers. If an SNMP trap receiver is defined, no SNMP trap is sent.



Note

1. The flowchart assumes capacitor detection is enabled, otherwise, the path is No.
2. When selecting a priority-based power supply scheme, the "Yes" flow applies. Otherwise, the sequence of connections applies.
3. When the power consumption percentage is over the threshold, an SNMP trap is issued to corresponding receivers.

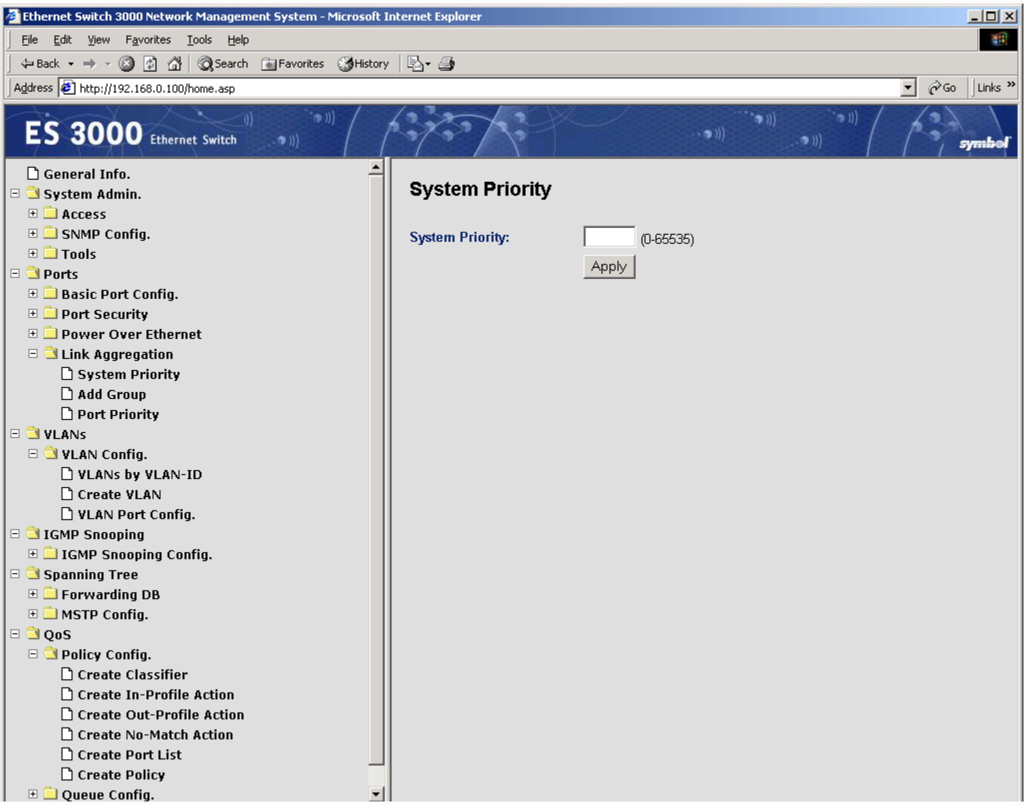
The algorithm starts when a port is connected,

1. **Port Connected**. Port connection detected
2. **Powered Device (resistor)**. Verify the connected device requirement. If it is a powered device, go to Power Not Provided (step 13).

3. **Powered Device (capacitor)**. If **capacitor detection enabled** is not selected for a global configuration, go to Power Not Provided (step 13). (this step is combined with next step to make the flow chart clearly).
4. Check the connected device requirement on power based on capacitor. If it is not a powered device, go to Power Not Provided (step 13).
5. **Power Budget**. Check the power budget. If there is enough power to support the new device, got to Over Power Threshold (step 10).
6. **Priority Based**. Check the Power Management Method. If **Deny next port connection, regardless of priority** is chosen, go to Power Not Provided (step 13).
7. **Low Priority Existed**. Check the existence of lower priority powered port. If not exists, go to Power Not Provided (step 13).
8. **Disable power to low priority port**. Discontinue the power supply to the found lower priority port.
9. **Power Budget**. Check the power budget. If there is not enough power, go to Low Priority Existed (step 7) to disable the next lower priority port (if one exists).
10. **Over Power Threshold**. Check the power threshold and used power. If the currently used power is lower than the threshold, go to Power Provided (step 12).
11. **Issue SNMP Trap**. An SNMP trap is triggered. The trap is sent based on the set up of trap receiver.
12. **Power Provided**. Power is provided to the connected port as requested. The power reserved to this port depends on the classification of the powered device. Go to End of Algorithm (step 14).
13. **Power Not Provided**. No power is provided to the connected port due to no power budget, not powered device, etc.
14. **End of Algorithm**.

4.2.23 System Admin->Ports->Link Aggregation->System Priority

Enter a number between 0-65535 to set up the system priority for the link aggregation. Click **Apply** to implement. Link Aggregation allows multiple links between switches to work as one virtual link aggregate link).



System Priority

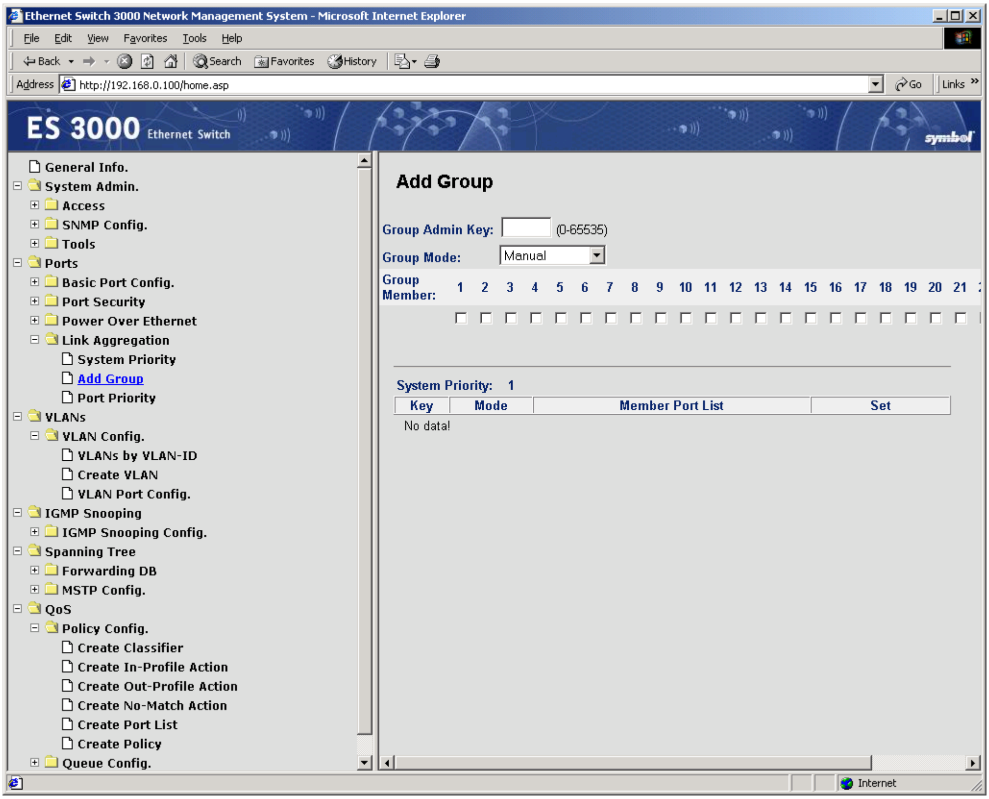
System Priority: (0-65535)

Apply

4.2.24 System Admin->Ports->Link Aggregation->Add Group

Use Link Aggregation to configure multiple links between switches to work as one virtual link (aggregate link). Link Aggregation can be defined for similar port types only. A 10/100 port cannot form a Port Link Aggregation with a gigabit port. To define a trunk, click on the ports participating in the Link Aggregation. Spanning Tree treats trunked ports as a single virtual port.

Note Use straight-though cables for all links in the Link Aggregation. Do not use crossover cables. Disable auto-negotiation on the ports in a trunk prior to setting up the Link Aggregation.



Add Group

Group Admin Key: [ ] (0-65535)

Group Mode: Manual

Group Member:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

System Priority: 1

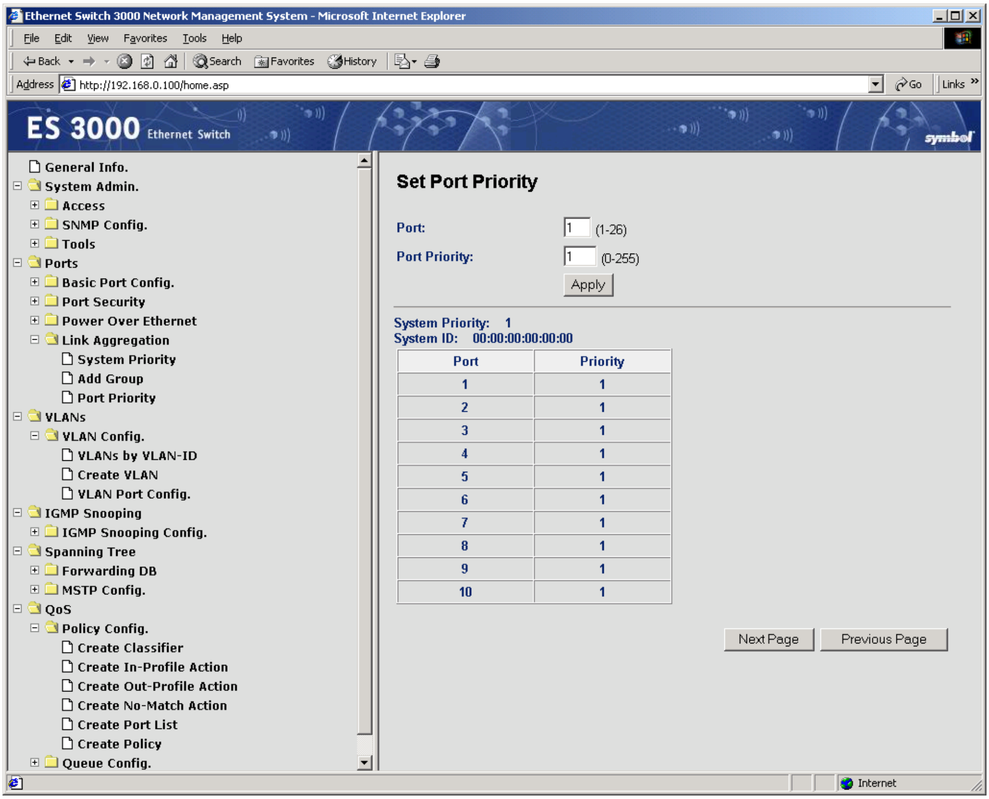
Key	Mode	Member Port List	Set

No data!

4.2.25 System Admin->Ports->Link Aggregation->Set Port Priority

Use the **Set Port Priority** screen to specify the ports with greater precedence in situations where traffic could be buffered in the switch due to congestion. Traffic on ports with a high priority is transmitted before traffic with a low priority setting.

The settings only affect packets that do not already have VLAN priority tags. To raise the priority of a given port, toggle the port setting from 0 to 255.



Set Port Priority

Port: 1 (1-26)

Port Priority: 1 (0-255)

Apply

System Priority: 1
System ID: 00:00:00:00:00:00

Port	Priority
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1

Next Page | Previous Page

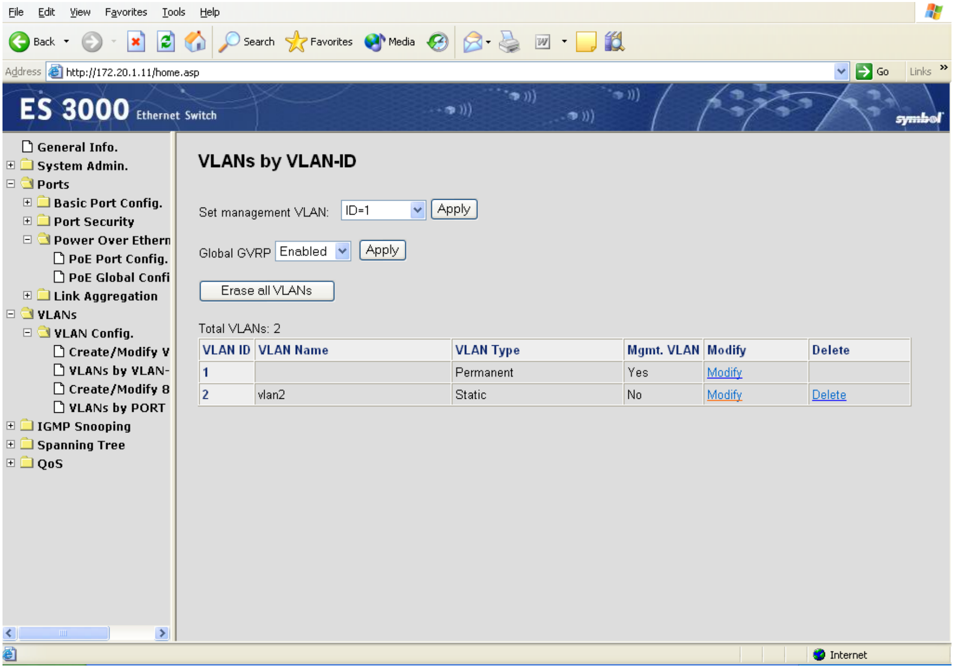
Use a Port number between 1 and 26, and a Port Priority between 0 and 255.

4.2.26 VLANs->VLAN Config->VLANs by VLAN-ID

A Virtual Local Area Network (VLAN) is a means to electronically separate ports on the same switch from a single broadcast domain into separate broadcast domains. Users can group by logical function instead of physical location. Two memberships are available for a VLAN member, tagged (T) and untagged (U). If a port is an untagged member, the VLAN tag is striped from the frame before it is sent out of the port. If the port is a tagged member of a VLAN, the VLAN tag stays in the frame when it is transmitted. If a port is not a VLAN member, it does not get VLAN traffic. The VLAN tagging option is a IEEE standard to facilitate the spanning of VLANs across multiple switches.

All untagged packets entering the switch are (by default) tagged with the ID specified by the port ID. Use the **VLANs by VLAN-ID** screen to specify the ID for each port. The number next to each port indicates which ID is set for each port. ID 1 is the default PVID. Up to 4094 VLANs with unique ID numbers and names can be added. VLAN ID numbers are required to be in the range of 1-4094. Per industry standard, the default VLAN has an ID of 1. VLAN #1 cannot be deleted.

View port membership to VLANs by VLAN-ID, and click on **Modify** or **Delete** to make changes. Select **Erase all VLANs** to reconfigure the VLAN to VLAN ID mapping. Select **Apply** to implement and display the changes made.



VLANs by VLAN-ID

Set management VLAN: ID=1 Apply

Global GVRP Enabled Apply

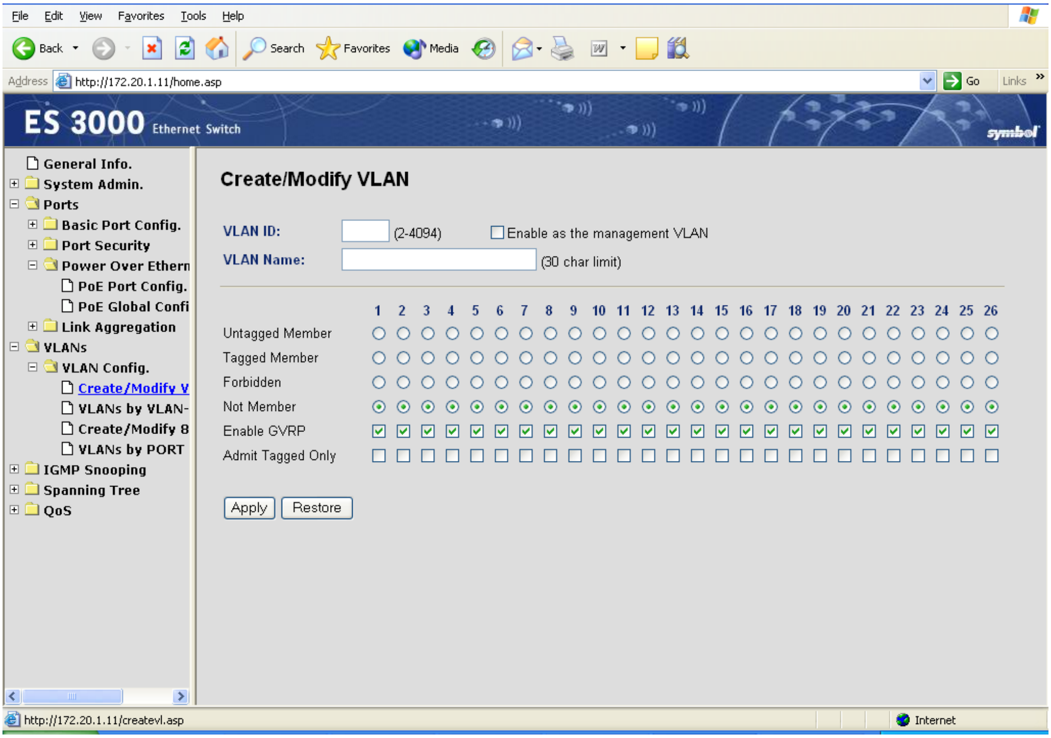
Erase all VLANs

Total VLANs: 2

VLAN ID	VLAN Name	VLAN Type	Mgmt. VLAN	Modify	Delete
1		Permanent	Yes	Modify	
2	vlan2	Static	No	Modify	Delete

4.2.27 VLANs->VLAN Config->Creating/Modify VLAN

To create a VLAN, select the **Create/Modify VLAN** menu item.
For advanced users, refer *Chapter 5* for CLI command modes.



Create/Modify VLAN

VLAN ID: [ ] (2-4094) ☐ Enable as the management VLAN

VLAN Name: [ ] (30 char limit)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Untagged Member	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged Member	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Enable GVRP	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Admit Tagged Only	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

[Apply] [Restore]

To create a VLAN:

1. Specify a VLAN ID (between 2 - 4094) for the new target VLAN within the **VLAN ID** field.

Note

VLAN #1 cannot be deleted under any circumstance.

2. Define whether the new VLAN is the management VLAN or not.
   (Only 1 Management VLAN is permitted).
3. Assign the new VLAN a name within the **VLAN Name** field.

4. Add Ports as untagged or tagged members, or select the **Forbidden** checkbox for the target port to prevent dynamic membership via GVRP.

   If a port is added to multiple VLANs as a tagged member, that port becomes an 802.1Q trunk port.

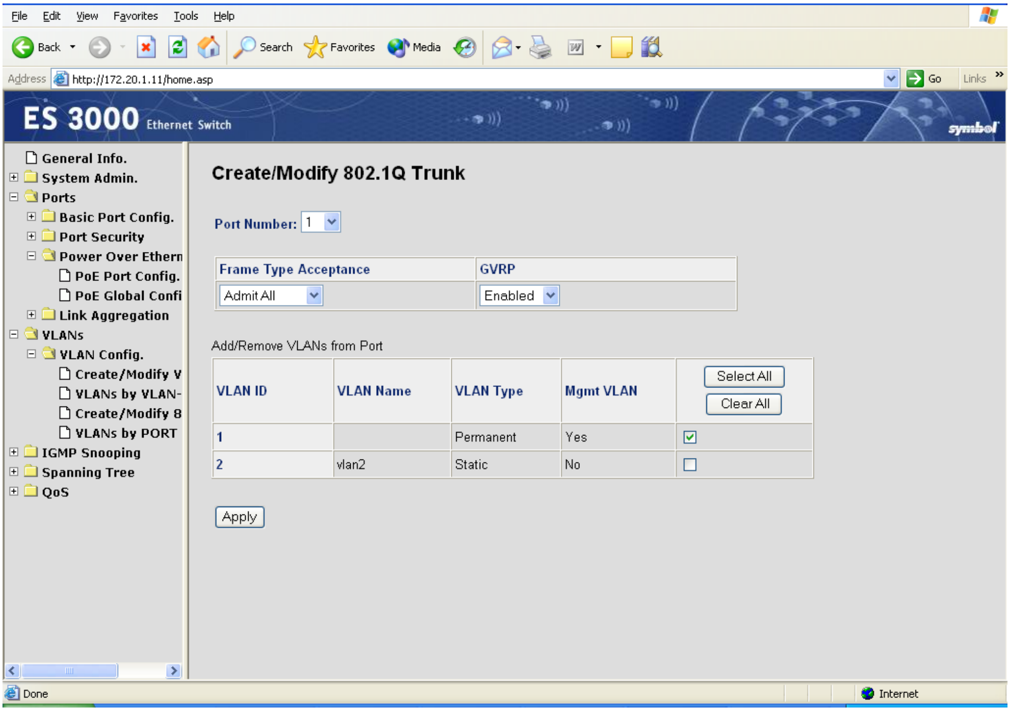
5. By default, GVRP is enabled on all ports so dynamic VLAN membership can occur. Disable if desired.
6. By default, All Frames are allowed, meaning untagged and tagged. Select the **Admit Tagged Only** checkbox to drop untagged frames.
7. Select **Apply** to implement that changes made within the Create/Modify VLAN screen. Select **Restore** to use the previously saved configuration.

4.2.28 VLANs->VLAN Config->Create/Modify 802.1Q Trunk

IEEE 802.1Q is the standard for encapsulating packets and marking them with VLAN information before sending them across a link between two switches. Use the **Create/Modify 802.1Q Trunk** screen to modify the encapsulation behavior on a port-by-port basis rather than on a VLAN-by-VLAN basis. It can also be used to control VLAN membership on a port-by-port basis. When a port number is selected, the information for that port is displayed. Frame Type Acceptance: **Admit All** or **Tagged Only**. If Tagged Only, incoming packets which are not tagged with 802.1Q VLAN information are dropped. If Admit All, all packets are admitted. GVRP: **Enabled** or **Disabled**. If Enabled, the switch allows and responds to dynamic VLAN invitations which it receives over this port in GVRP format. If Disabled, these packets are dropped. All current VLANs on the switch are displayed in table format. The check boxes to the right indicate which VLANs this port is currently a member of.

To configure VLAN membership by port:

1. Select a Port from the **Port Number** menu.
2. Add or remove VLANs as tagged members.
3. Change the Frame Type Acceptance or GVRP settings if desired.
4. Click **Apply** to implement the changes and display the configuration.



Create/Modify 802.1Q Trunk

Port Number: 1

Frame Type Acceptance	GVRP
Admit All	Enabled

Add/Remove VLANs from Port

VLAN ID	VLAN Name	VLAN Type	Mgmt VLAN	Select All Clear All
1		Permanent	Yes	☑
2	vlan2	Static	No	□

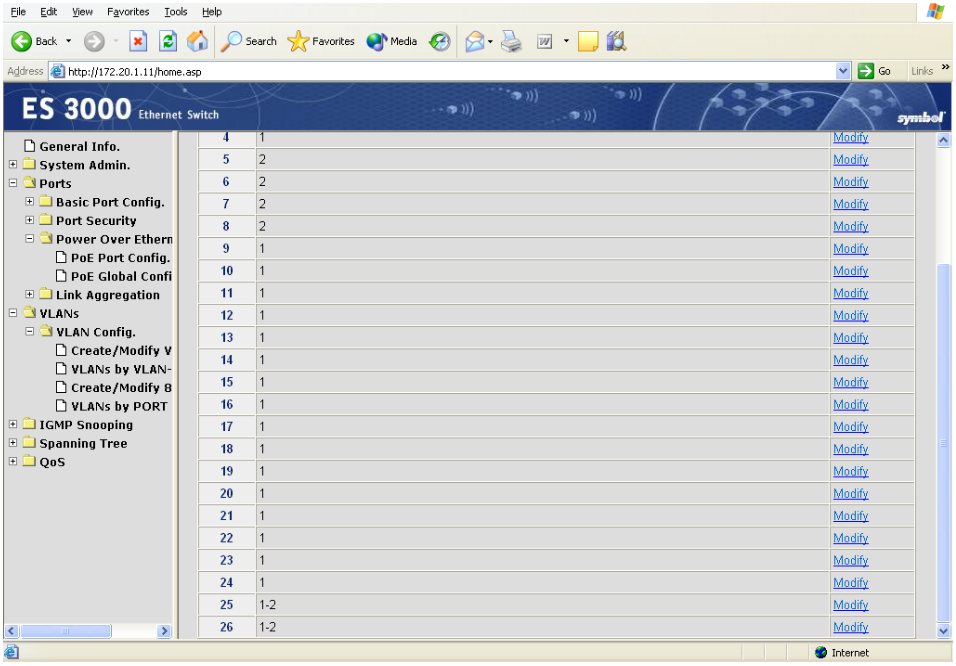
Apply

4.2.29 VLANs->VLAN Config->VLANs by Port

Use the VLAN by Port screen to configure VLAN port information on a port-by-port basis.

1. Select **Modify** to configure VLAN information for the target port.
2. Configure trunk ports and VLAN membership as required.

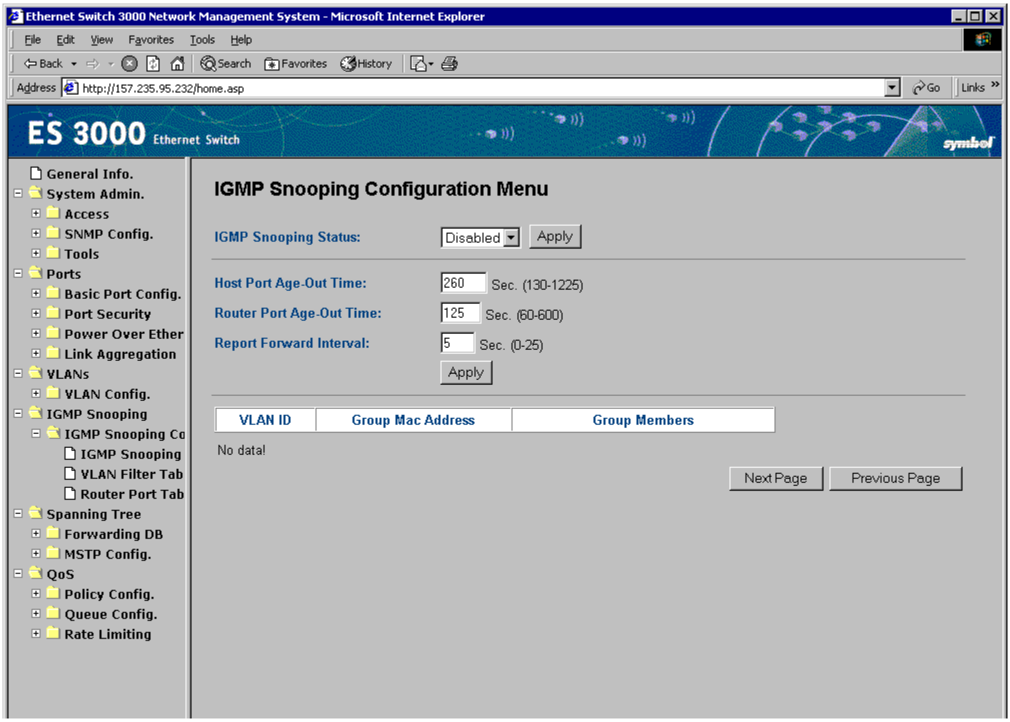
In the example below, Ports 25-26 are 802.1Q trunk ports with VLANs 1-2 as members.



4	1	Modify
5	2	Modify
6	2	Modify
7	2	Modify
8	2	Modify
9	1	Modify
10	1	Modify
11	1	Modify
12	1	Modify
13	1	Modify
14	1	Modify
15	1	Modify
16	1	Modify
17	1	Modify
18	1	Modify
19	1	Modify
20	1	Modify
21	1	Modify
22	1	Modify
23	1	Modify
24	1	Modify
25	1-2	Modify
26	1-2	Modify

4.2.30 IGMP Snooping->IGMP Snooping Config->IGMP Snooping Configuration Menu

The Internet Group Management Protocol (IGMP) is an Internet protocol allowing a host to report its multicast group membership to multicast routers. Multicasting allows one computer on the Internet to send information to other computers having identified themselves as interested in receiving the information. The ES3000 can “snoop” the messaging protocol to keep track of multicast groups and to insure multicast traffic is sent only to the appropriate ports within a VLAN. In networks where multimedia applications generate multicast traffic, IGMP can reduce unnecessary bandwidth by limiting traffic forwarding otherwise broadcast to the network. Enabling IGMP allows individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.



IGMP Snooping Configuration Menu

IGMP Snooping Status: Disabled

Host Port Age-Out Time: 260 Sec. (130-1225)

Router Port Age-Out Time: 125 Sec. (60-600)

Report Forward Interval: 5 Sec. (0-25)

VLAN ID	Group Mac Address	Group Members

No data!

The page displays:

IGMP Snooping Status: The global enabled or disabled status of IGMP snooping. The administrator can select Enabled or Disabled. When Enabled, the switch detects IGMP queries, reports, and manages multicast traffic through the switch for all VLANs. When Disabled, the switch forwards traffic and disregards IGMP requests.

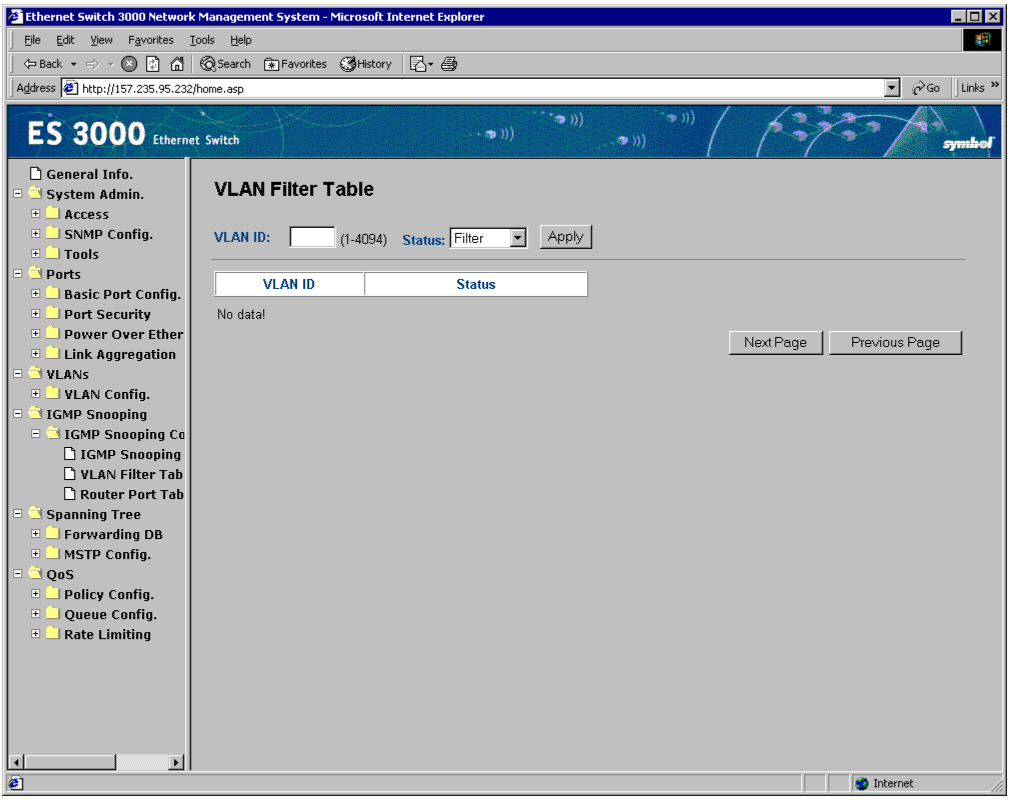
Host Port Age-Out Time: The length of time, in seconds, the switch keeps a host in a multicast group without receiving IGMP reports from the host. The value can be within the range 130-1225. The default is 260 seconds.

Router Port Age-Out Time: The length of time, in seconds, the switch keeps router port entries without receiving IGMP queries from the router. Routers usually send protocol advertisements every few seconds. The value can be within the range 60-600. The default is 125 seconds.

Report Forward Interval: The length of time, in seconds, that the switch waits before forwarding an IGMP report to the router from a group from which it has previously sent a report. The value can be within the range 0-25. The default is 5 seconds.

4.2.31 IGMP Snooping->IGMP Snooping Config->VLAN Filter Table

Use the **VLAN Filter Table** to define the VLAN not to be included in the set Vlan Filter. Enter the VLAN ID (1-4094) in the **VLAN ID** field. Ensure the **Status** field is set to **Filter**. Click **Apply** to remove the VLAN ID from the set VLAN Filter



VLAN Filter Table

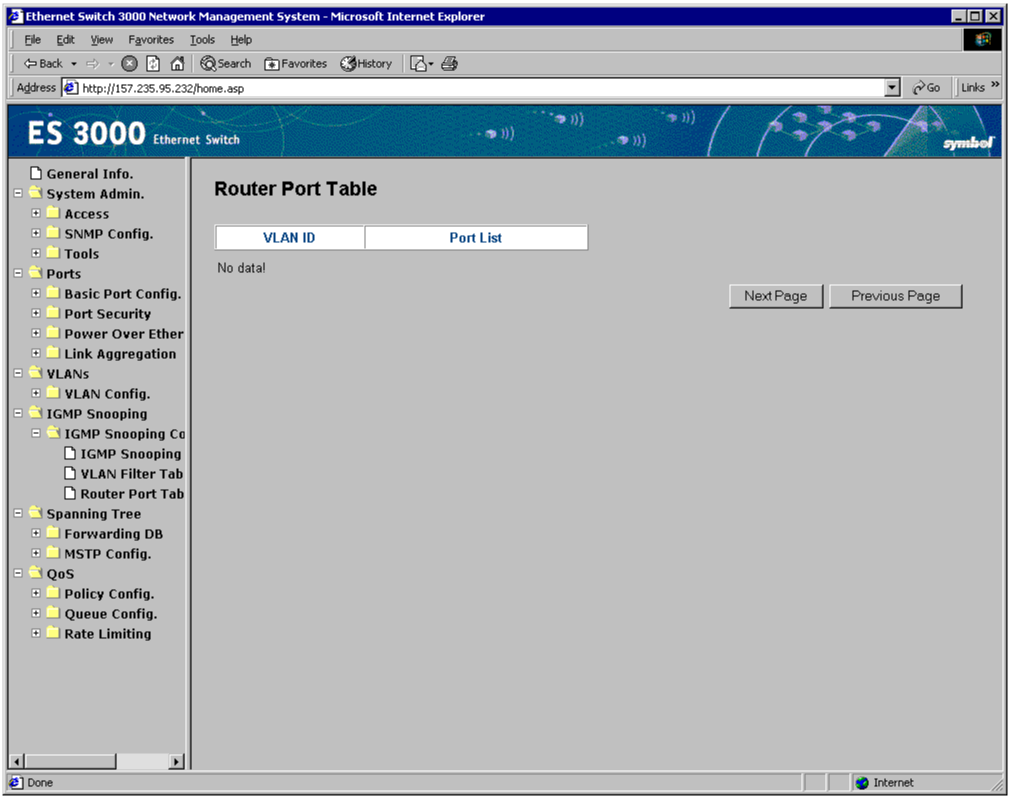
VLAN ID: (1-4094) Status: Filter

VLAN ID	Status

No data!

4.2.32 IGMP Snooping->IGMP Snooping Config->Router Port Table

The **Router Port Table** page displays the ports in VLANs connected to the router. User can snoop the package from router side in these ports.



Router Port Table

VLAN ID	Port List

No data!

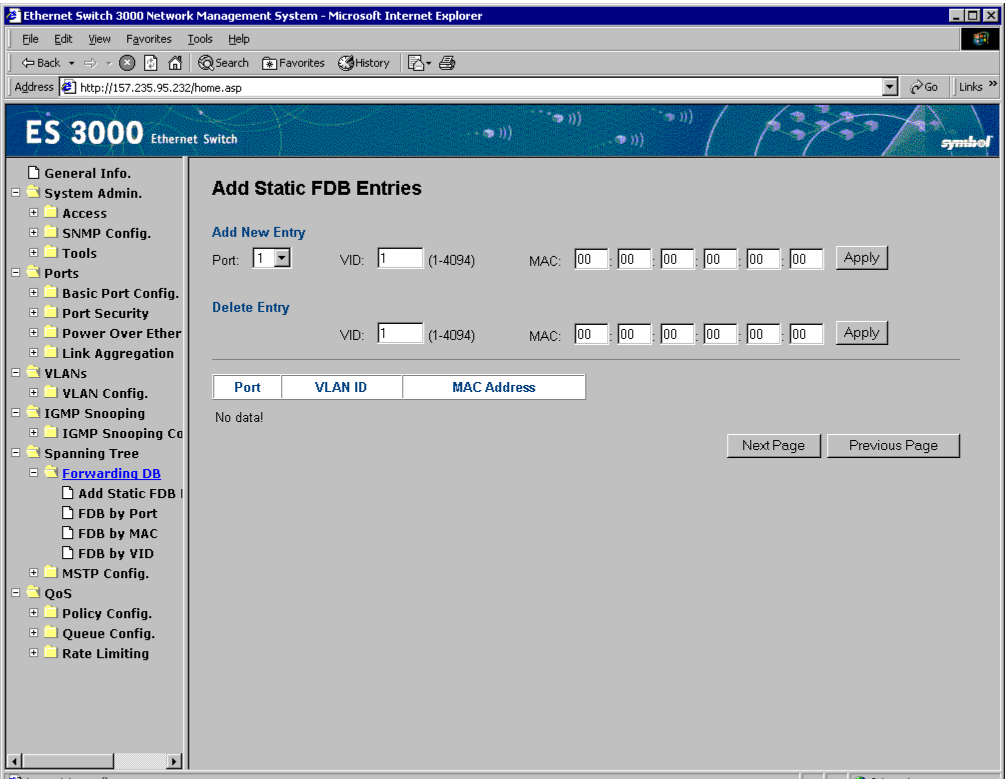
Next Page | Previous Page

4.2.33 Spanning Tree->Forwarding DB->Add Static FDB Entries

The ES3000 can be configured to use one of three spanning tree protocols. Spanning Tree Protocol (STP) is compatible with legacy equipment. Rapid Spanning Tree Protocol (RSTP) is significantly faster than STP. Multiple Spanning Tree Protocol (MSTP) is based on RSTP and extends RSTP in a way useful for switches implementing VLANs.

Use the **Forwarding Database** to view the dynamic MAC addresses currently in the address database. When addresses are in the database, the packets intended for those addresses are forwarded directly to those ports. An administrator can display addresses in the table by port, VLAN and/or MAC address by entering the short key. The static MAC address table is also displayable.

The Static Addresses Table, allows the administrator to specify Media Access Control (MAC) addresses for specific ports not purged from the bridge table by the aging function. There are 3 entries on the table. Two commands are available to add and/or remove an entry. To add an entry, follow the pop-out prompt.



Add Static FDB Entries

Add New Entry

Port: 1 VID: 1 (1-4094) MAC: 00 : 00 : 00 : 00 : 00 : 00 Apply

Delete Entry

VID: 1 (1-4094) MAC: 00 : 00 : 00 : 00 : 00 : 00 Apply

Port	VLAN ID	MAC Address

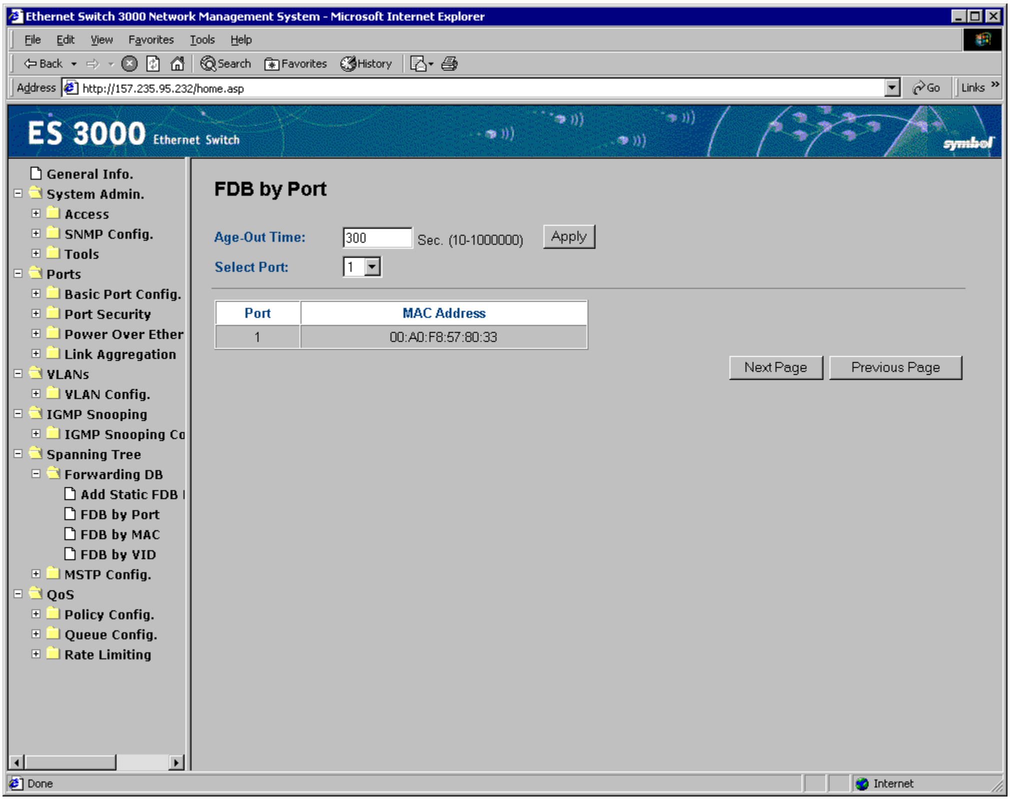
No data!

Next Page Previous Page

4.2.34 Spanning Tree->Forwarding DB->FDB by Port/MAC/VLAN

When the number of hosts increase on a network, the Forwarding Database grows sharply. Looking for a MAC address can become time-consuming work. The system provides three different ways for an administrator to look over MAC addresses; by a specified Port, sorted by MAC address, and by a specified VLAN. A Set Age-Out time command is given to configure the time to remove a non-recently-used entry. The modification on this timer is switch-wide.

The age-out time is the amount of time that an entry is kept in the bridge tables prior to being purged (or aged). The range is between 10 seconds and 1,000,000 seconds. By industry standard, 300 seconds is the default.



FDB by Port

Age-Out Time: 300 Sec. (10-1000000) Apply

Select Port: 1

Port	MAC Address
1	00:A0:F8:57:80:33

Next Page Previous Page

4.2.35 Spanning Tree->MSTP Configuration->MSTP Config

The ES3000 Ethernet switch is compliant with IEEE802.1D Spanning Tree Protocol (STP), IEEE 802.1w Rapid Spanning Tree, and IEEE 802.1s Multiple Spanning Tree. STP ensures only one path is active at a time between any two network nodes. There can more than one physical path between any two nodes, forming a loop, either created for redundancy or by accident. STP ensures only one physical path is active and the others are blocked. If a loop is created for redundancy, STP monitors the two paths and activates the stand-by path if the primary path fails. If a loop is created inadvertently, STP disables one of the two paths. A loop in a network can disable the network by causing a **Broadcast Storm**. A Broadcast Storm is the result of a broadcast message traveling through the loop again and again.

Rapid spanning tree (IEEE 802.1w) is supported to reduce spanning tree time. Each spanning tree establishment process takes several timeouts in order to avoid a loop, even the edge switch. Configure the switch to avoid the long latency due to timeouts if there is a single switch connection. In the case of two or more enabled links to the switch and Rapid Spanning Tree, the switch might not perform properly.

IEEE 802.1s Multiple Spanning Tree is supported by the ESW 3000 switch. An independent spanning tree can be established per VLAN.

Global MSTP Status: Enabled - When MSTP is enabled, system is running in MSTP mode

Disabled - When MSTP is disabled, system does not use MSTP mode.

After selecting the MSTP status, click **Apply** to implement.

Protocol Version: STP Compatible - Protocol based on STP

RSTP - Protocol based on RSTP

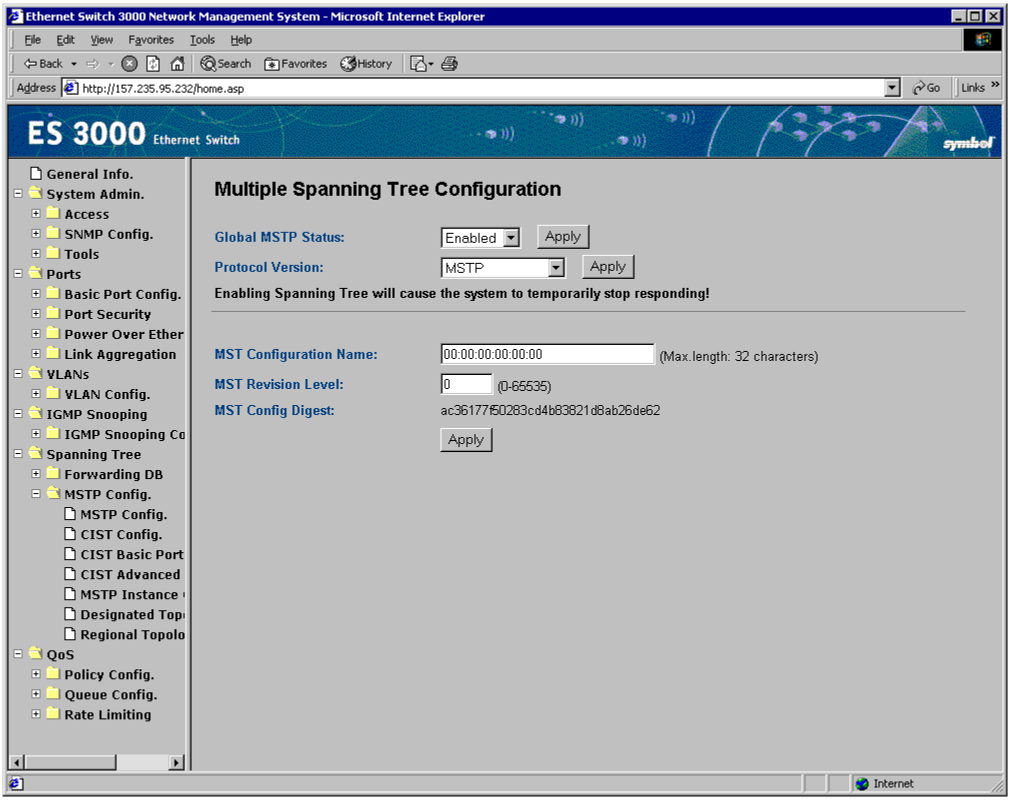
MSTP - Protocol based on MSTP

MST Config ID Selector: Configures the port priority for an MST instance. The range is 0-255. The lower number receives priority.

MST Configuration Name: Specifies configuration name. The name has a maximum length of 32 characters and is case sensitive.

MSTP Revision Level: Specifies the configuration revision number. The range is 0 to 65535.

MSTP Config Digest: Configuration in saved mode.



Multiple Spanning Tree Configuration

Global MSTP Status: Enabled [Apply]

Protocol Version: MSTP [Apply]

Enabling Spanning Tree will cause the system to temporarily stop responding!

MST Configuration Name: 00:00:00:00:00:00 (Max.length: 32 characters)

MST Revision Level: 0 (0-65535)

MST Config Digest: ac36177f50283cd4b83821d8ab26de62

[Apply]

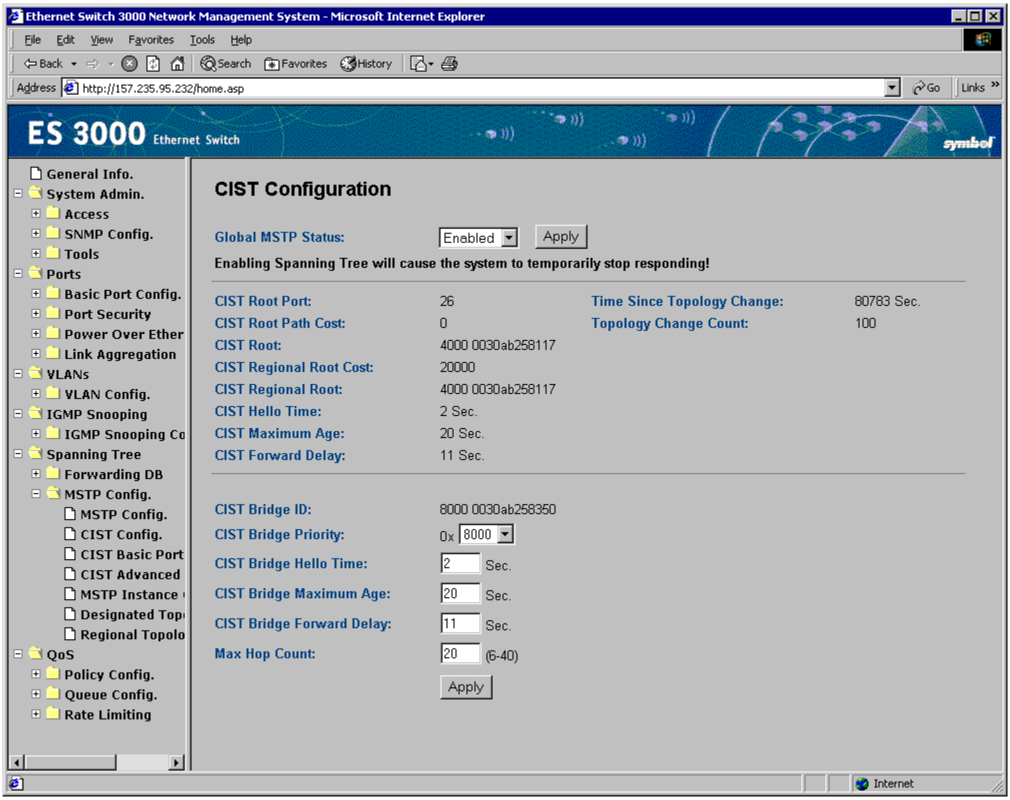
4.2.36 Spanning Tree->MSTP Configuration->CIST Configuration

Status

Hello Time:	Time between configuration messages sent by the Spanning Tree algorithm
Maximum Age	Amount of time before a configuration message is discarded by the system
Forward Delay	Amount of time system spends transitioning from the learning to listening to forwarding states
Bridge Priority	Priority setting among other switches in the Spanning Tree

Command

Set Cist Bridge Priority:	Defines the Cist bridge priority.
Set Cist Bridge Hello Time:	Determines the interval between two hello packets.
Set Cist Bridge Maximum Age:	The maximum age time.
Set Bridge Forward Delay:	The interval the system uses when transitioning traffic from "learning" to "listening" to "forwarding" status.
Set MSTP Max Hop Count Delay:	Defines the maximum hop count delay.



CIST Configuration

Global MSTP Status: Enabled ▾ Apply

Enabling Spanning Tree will cause the system to temporarily stop responding!

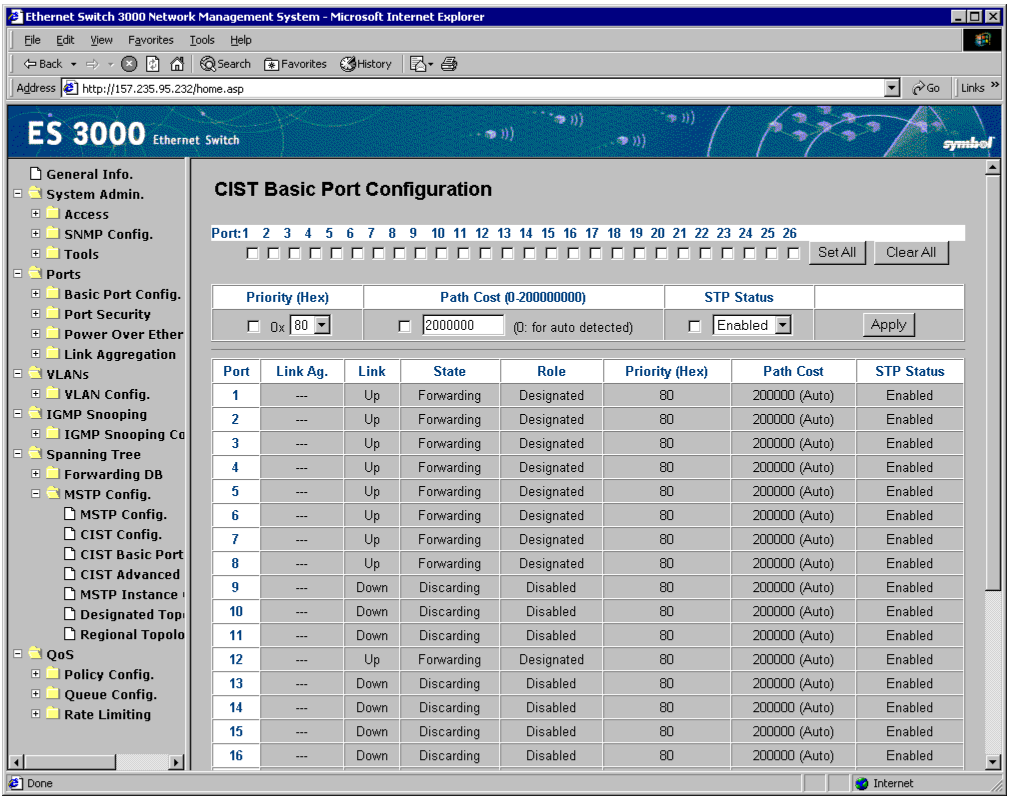
CIST Root Port:	26	Time Since Topology Change:	80783 Sec.
CIST Root Path Cost:	0	Topology Change Count:	100
CIST Root:	4000 0030ab258117		
CIST Regional Root Cost:	20000		
CIST Regional Root:	4000 0030ab258117		
CIST Hello Time:	2 Sec.		
CIST Maximum Age:	20 Sec.		
CIST Forward Delay:	11 Sec.		

CIST Bridge ID:	8000 0030ab258350
CIST Bridge Priority:	0x 8000 ▾
CIST Bridge Hello Time:	2 Sec.
CIST Bridge Maximum Age:	20 Sec.
CIST Bridge Forward Delay:	11 Sec.
Max Hop Count:	20 (6-40)

Apply

4.2.37 Spanning Tree->MSTP Configuration->CIST Basic Port Configuration

Use the **CIST Basic Port Configuration** screen to set up the port, priority and path cost and enable/disable the port STP status. Use the **Port** menu to define the target port. Use the **Priority** field to set the port priority. Click **Apply** once all changes have been made.



CIST Basic Port Configuration

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

□ Set All Clear All

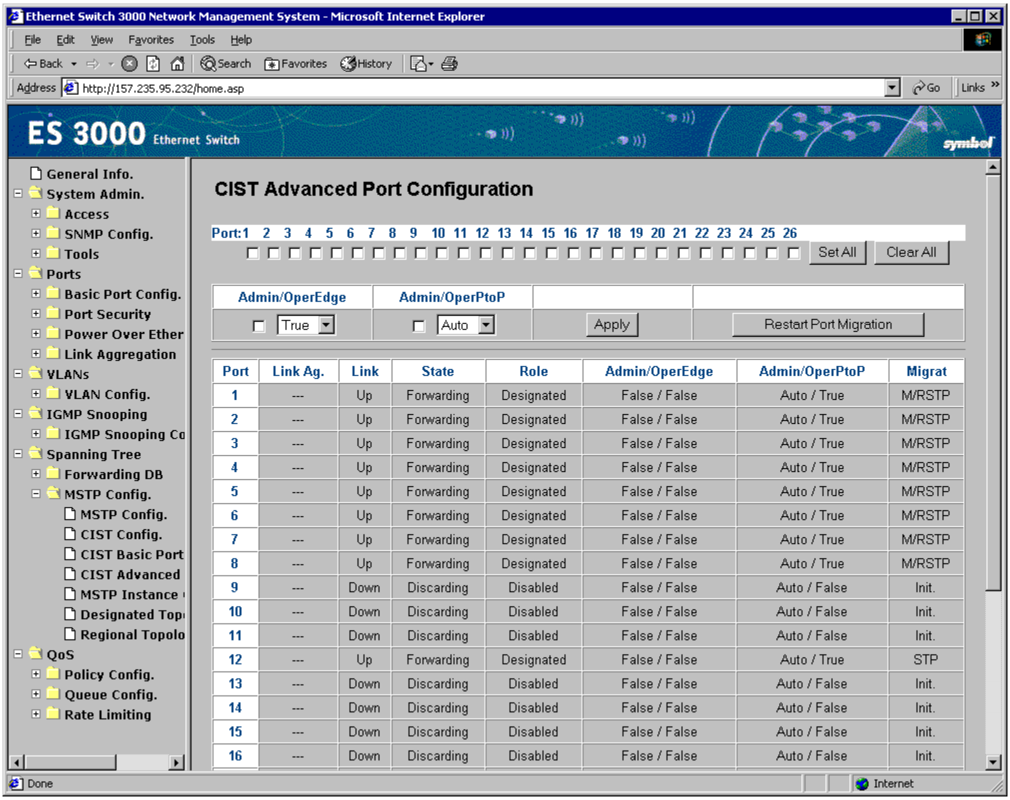
Priority (Hex)	Path Cost (0-200000000)	STP Status	
□ 0x 80	□ 2000000 (0: for auto detected)	□ Enabled	Apply

Port	Link Ag.	Link	State	Role	Priority (Hex)	Path Cost	STP Status
1	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
2	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
3	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
4	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
5	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
6	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
7	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
8	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
9	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled
10	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled
11	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled
12	---	Up	Forwarding	Designated	80	200000 (Auto)	Enabled
13	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled
14	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled
15	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled
16	---	Down	Discarding	Disabled	80	200000 (Auto)	Enabled

4.2.38 Spanning Tree->MSTP Configuration->CIST Advanced Port Configuration

Use the **CIST Advanced Port Configuration** screen to configure the port edge status, port P-TO-P status, and restart port migration to prevent the wrong link.

Click **Apply** to implement the changes.



CIST Advanced Port Configuration

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

□ Set All Clear All

Admin/OperEdge	Admin/OperPtoP		
□ True	□ Auto	Apply	Restart Port Migration

Port	Link Ag.	Link	State	Role	Admin/OperEdge	Admin/OperPtoP	Migrat
1	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
2	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
3	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
4	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
5	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
6	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
7	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
8	---	Up	Forwarding	Designated	False / False	Auto / True	M/RSTP
9	---	Down	Discarding	Disabled	False / False	Auto / False	Init.
10	---	Down	Discarding	Disabled	False / False	Auto / False	Init.
11	---	Down	Discarding	Disabled	False / False	Auto / False	Init.
12	---	Up	Forwarding	Designated	False / False	Auto / True	STP
13	---	Down	Discarding	Disabled	False / False	Auto / False	Init.
14	---	Down	Discarding	Disabled	False / False	Auto / False	Init.
15	---	Down	Discarding	Disabled	False / False	Auto / False	Init.
16	---	Down	Discarding	Disabled	False / False	Auto / False	Init.

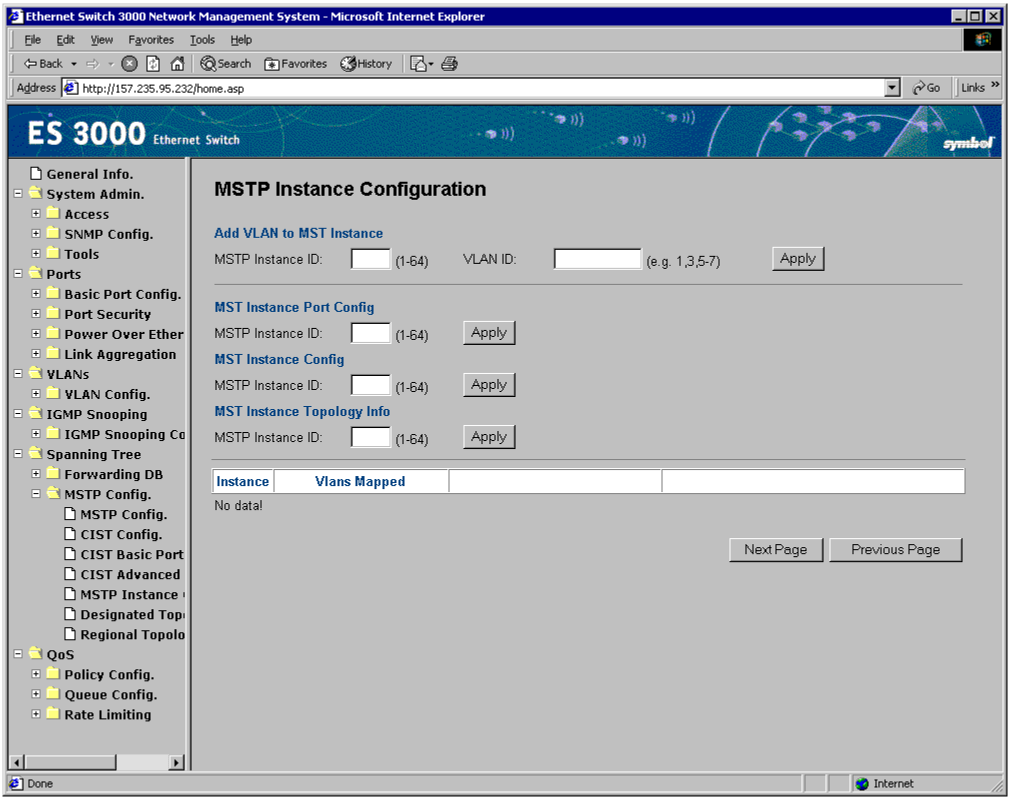
4.2.39 Spanning Tree->MSTP Configuration->MSTP Instance Configuration

One instance can have more than one VLAN. Use the **MSTP In stance Configuration** page to add or remove a VLAN, or remove a MST and Instance Port configuration.

Specify a single instance (a range of instances separated by a hyphen) or a series of instances separated by a comma. The range is from 2 to 64.

For a VLAN ID, the range is from 1-7. When mapping VLANs to an MST instance, the mapping is increasing, and the VLANs specified in the command are added to or removed from the VLANs previously mapped.

Use a hyphen to specify a VLAN range. For example, **instance 1 vlan 3-5** maps VLANs 3 through 5 to MST instance 1.



MSTP Instance Configuration

Add VLAN to MST Instance

MSTP Instance ID: (1-64) VLAN ID: (e.g. 1,3,5-7) Apply

MST Instance Port Config

MSTP Instance ID: (1-64) Apply

MST Instance Config

MSTP Instance ID: (1-64) Apply

MST Instance Topology Info

MSTP Instance ID: (1-64) Apply

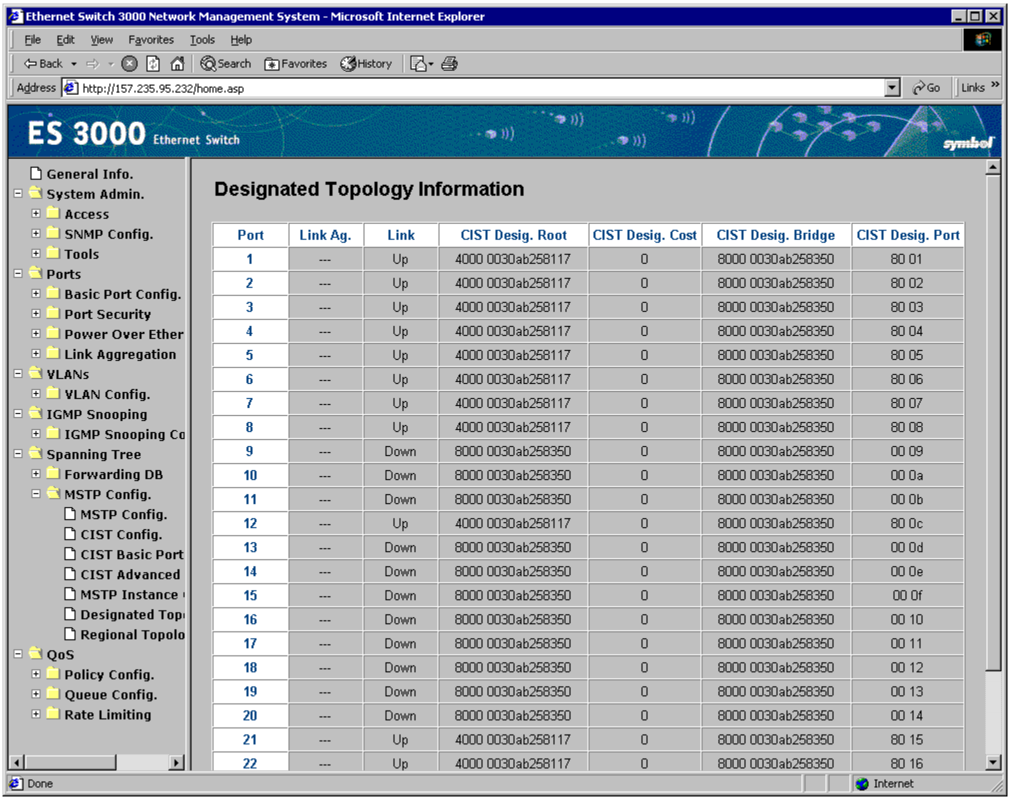
Instance	Vlans Mapped		

No data!

Next Page Previous Page

4.2.40 Spanning Tree->MSTP Configuration->Designated Topology Information

Use the **Designated Topology Information** page to display designated topology information for each port.

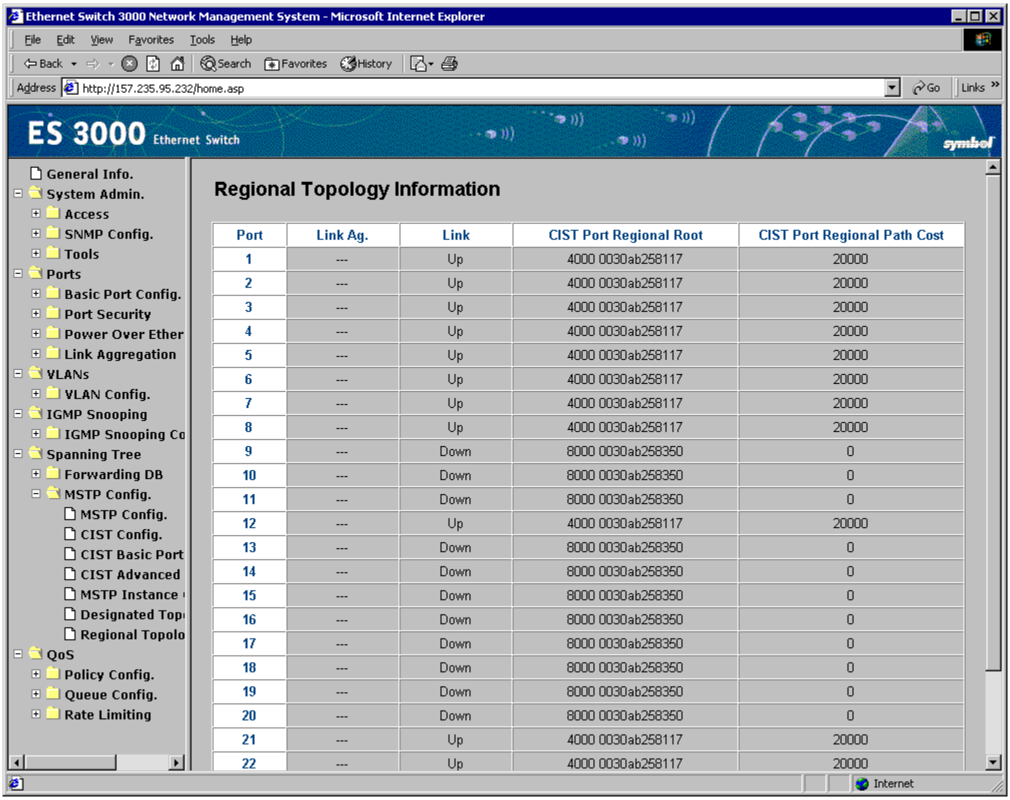


Designated Topology Information

Port	Link Ag.	Link	CIST Desig. Root	CIST Desig. Cost	CIST Desig. Bridge	CIST Desig. Port
1	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 01
2	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 02
3	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 03
4	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 04
5	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 05
6	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 06
7	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 07
8	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 08
9	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 09
10	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 0a
11	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 0b
12	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 0c
13	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 0d
14	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 0e
15	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 0f
16	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 10
17	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 11
18	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 12
19	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 13
20	---	Down	8000 0030ab258350	0	8000 0030ab258350	00 14
21	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 15
22	---	Up	4000 0030ab258117	0	8000 0030ab258350	80 16

4.2.41 Spanning Tree->MSTP Configuration->Regional Topology Information

Use the **Regional Topology Information** page to display regional topology information for each port.



Regional Topology Information

Port	Link Ag.	Link	CIST Port Regional Root	CIST Port Regional Path Cost
1	---	Up	4000 0030ab258117	20000
2	---	Up	4000 0030ab258117	20000
3	---	Up	4000 0030ab258117	20000
4	---	Up	4000 0030ab258117	20000
5	---	Up	4000 0030ab258117	20000
6	---	Up	4000 0030ab258117	20000
7	---	Up	4000 0030ab258117	20000
8	---	Up	4000 0030ab258117	20000
9	---	Down	8000 0030ab258350	0
10	---	Down	8000 0030ab258350	0
11	---	Down	8000 0030ab258350	0
12	---	Up	4000 0030ab258117	20000
13	---	Down	8000 0030ab258350	0
14	---	Down	8000 0030ab258350	0
15	---	Down	8000 0030ab258350	0
16	---	Down	8000 0030ab258350	0
17	---	Down	8000 0030ab258350	0
18	---	Down	8000 0030ab258350	0
19	---	Down	8000 0030ab258350	0
20	---	Down	8000 0030ab258350	0
21	---	Up	4000 0030ab258117	20000
22	---	Up	4000 0030ab258117	20000

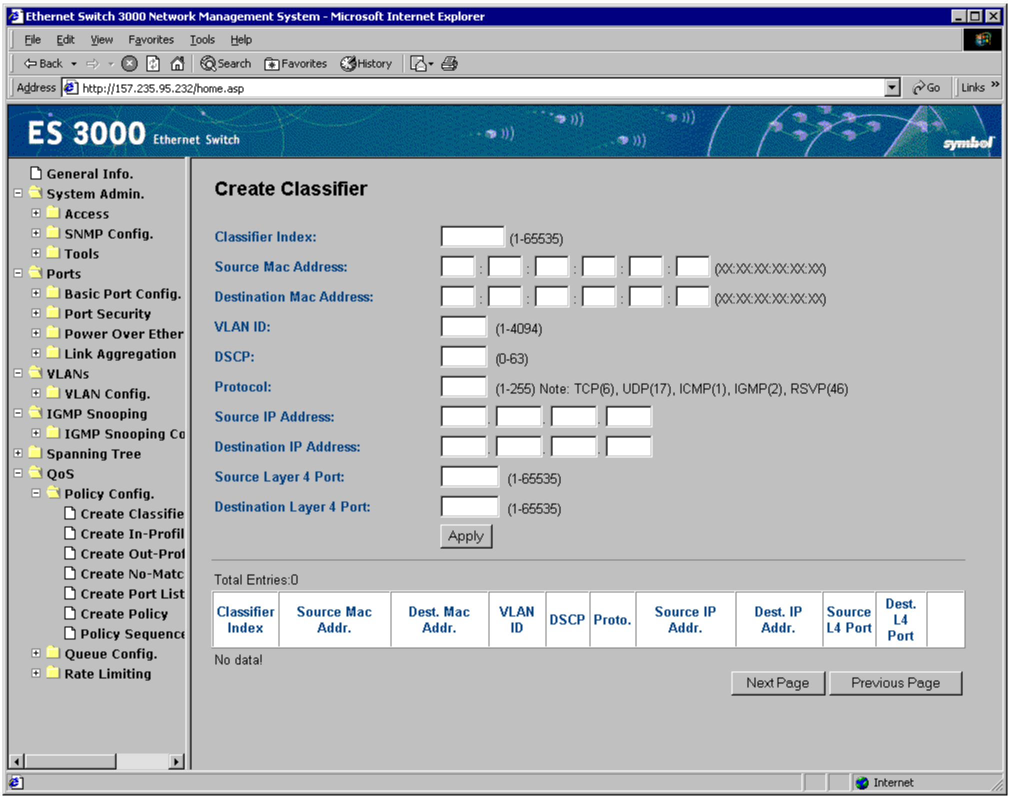
4.2.42 QoS->Policy Config->Create Classifier

The ES3000 implements IEEE 802.1p Quality of Service (QoS) processing. QoS policies examine packets and classify them. The classification is used to drop packets or assign markers to the packets. The markers are Class of Service (CoS) Priority, Type of Service (ToS) Precedence and Differentiated Services Code Points (DSCP). For each port, the outgoing packets are placed in four output queues based on CoS priority or DSCP value. The queues are serviced using a weighted round robin algorithm.

There are two means to differentiate ES3000 traffic, VLAN tags or Differentiated Service Code Points (DSCP) in the header of packets. By using either VLAN tags (port-based) or DSCP (DiffServ), configure the switch so specific traffic takes priority over less critical traffic.

Choose to further differentiate packet priority by using the Differentiated Service (DiffServ) feature. DiffServ uses a priority tag in the packet, the Differentiated Service Code Point (DSCP), to determine the priority of the packet. This menu maps the various DSCP tags to the two queues in the switch.

Click the classifier configuration to display the **Create Classifier** page.



Create Classifier

Classifier Index: (1-65535)

Source Mac Address: : : : : : (XX:XX:XX:XX:XX:XX)

Destination Mac Address: : : : : : (XX:XX:XX:XX:XX:XX)

VLAN ID: (1-4094)

DSCP: (0-63)

Protocol: (1-255) Note: TCP(6), UDP(17), ICMP(1), IGMP(2), RSVP(46)

Source IP Address: . . .

Destination IP Address: . . .

Source Layer 4 Port: (1-65535)

Destination Layer 4 Port: (1-65535)

Total Entries:0

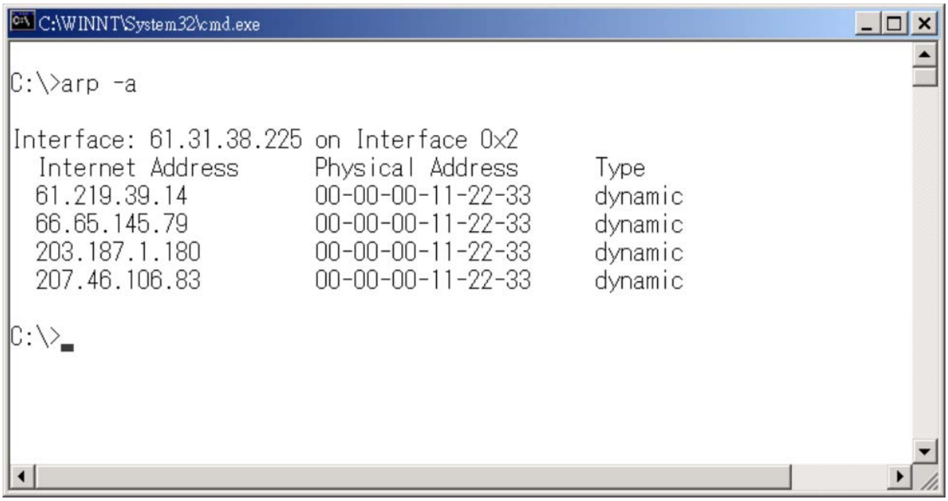
Classifier Index	Source Mac Addr.	Dest. Mac Addr.	VLAN ID	DSCP	Proto.	Source IP Addr.	Dest. IP Addr.	Source L4 Port	Dest. L4 Port	

No data!

Nine parameters are available to classify a data packet, including the Source Mac Address, Destination Mac Address, VLAN ID, DSCP, Protocol, Source IP Address, Destination IP Address, Source Layer 4 Port Number, and Destination Layer 4 Port Number.

Classifier Index: A unique ID to distinguish a classifier. The value can be any number between 1 and 65535. No default ID is given.

Source MAC Address: The source MAC address of a data packet is 6-bytes long and presented as twelve characters in hexadecimal. For example, 'arp -a' on command window can be used to find the MAC address table of a system running a Microsoft OS.



```
C:\>arp -a

Interface: 61.31.38.225 on Interface 0x2
  Internet Address      Physical Address      Type
  61.219.39.14          00-00-00-11-22-33     dynamic
  66.65.145.79          00-00-00-11-22-33     dynamic
  203.187.1.180         00-00-00-11-22-33     dynamic
  207.46.106.83         00-00-00-11-22-33     dynamic

C:\>
```

Destination MAC: The destination MAC address on a data packet. The format is same as source MAC address.

VLAN ID: The ID of a VLAN. The value is between 1 and 4094. 0 is used to indicate no VLAN and 4095 is reserved for system use.

DSCP: Differentiated Service Code Point has 6 bits and the value is between 0 and 63.

Protocol: The protocol ID of an IP packet. It is a single byte with a value is between 0 and 255.

Common protocol numbers include:

Protocol ID	***Description***
1	ICMP (Internet Control Message Protocol)
2	IGMP (Internet Group Management Protocol)
6	TCP (Transmission Control Protocol)
17	UDP (User Datagram Protocol)
46	RSVP (Resource reSerVation Protocol)
80	HTTP (HyperText Transport Protocol)

ICMP is the basic ping command. When a ping command is issued, the packet sent is an ICMP echo packet. The packet waits for the ICMP echo reply packet to complete the ping process. The ICMP returns additional information to an echo reply if there is a ping failure (network or host unreachable etc.).

Source IP Address: The Source IP Address only accepts IP version 4 addresses (four bytes long). The format is four numbers separated by three decimal points. For example, 61.31.38.225.

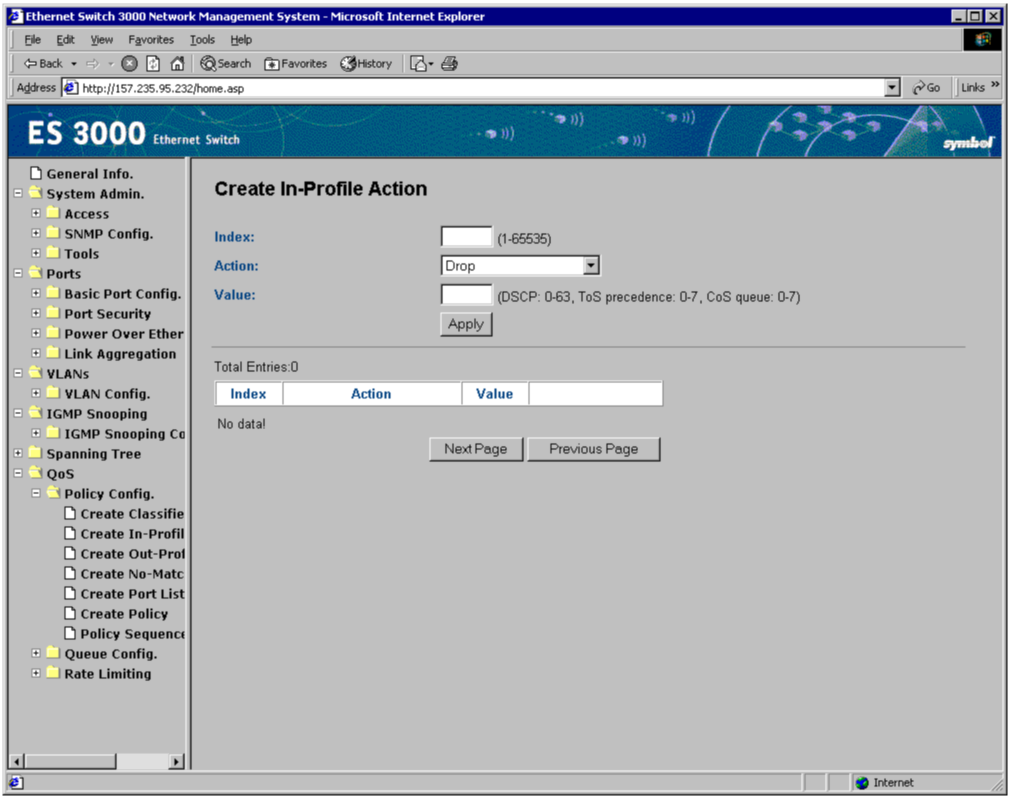
Destination IP Address: The destination Internet Protocol Address. Same format as Source IP address.

Source Layer 4 Port: The source transportation layer port number of a data packet. It is two bytes with a value between 0 and 65535. Values under 1024 are reserved for specific applications. Symbol recommends using a port number over 1024.

Destination Layer 4 Port: The destination transportation layer port number of a data packet. The format and allocation are the same as the Source Layer 4 Port.

4.2.43 QoS->Policy Configuration->Create In-Profile Action

The In-Profile Action applies to the ingress data packets. Like the Classifier, it has a unique ID as index. The index is a number between 1 and 65535. Four actions are possible:



Create In-Profile Action

Index: (1-65535)

Action: Drop

Value: (DSCP: 0-63, ToS precedence: 0-7, CoS queue: 0-7)

Apply

Total Entries:0

Index	Action	Value

No data!

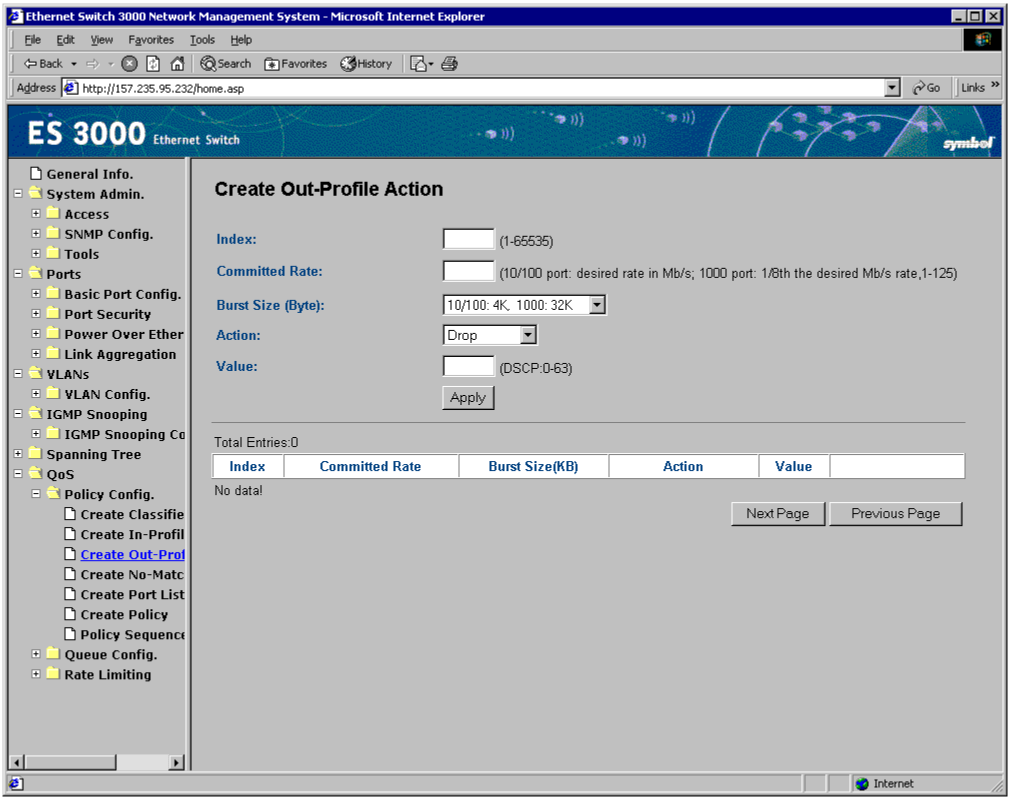
Next Page Previous Page

Action	**Description**	**Value Range**
Drop	Packet is dropped	N/A
Policed-dscp	Policed DSCP	0 - 63
Policed-precedence	Policed precedence	0 - 7
Policed-cos	Policed class of service	0 - 7

The precedence and CoS (Class of Service) has three bits. The value is between 0 and 7. Higher values have priority. DSCP combines Precedence and ToS (Type of Service). DSCP is 6 bits long for the priority and the value ranges from 0 and 63.

4.2.44 QoS->Policy Configuration->Create Out-Profile Action

Out-Profile Actions are similar to In-Profile Actions except they do not have policed-precedence nor policed-cos and they apply to egress traffic. Two actions are created as well. In additional to In-Profile Action page, the administrator has the capability to set the committed rate and burst size.



Create Out-Profile Action

Index: (1-65535)

Committed Rate: (10/100 port: desired rate in Mb/s; 1000 port: 1/8th the desired Mb/s rate,1-125)

Burst Size (Byte): 10/100: 4K, 1000: 32K

Action: Drop

Value: (DSCP:0-63)

Apply

Total Entries:0

Index	Committed Rate	Burst Size(KB)	Action	Value	

No data!

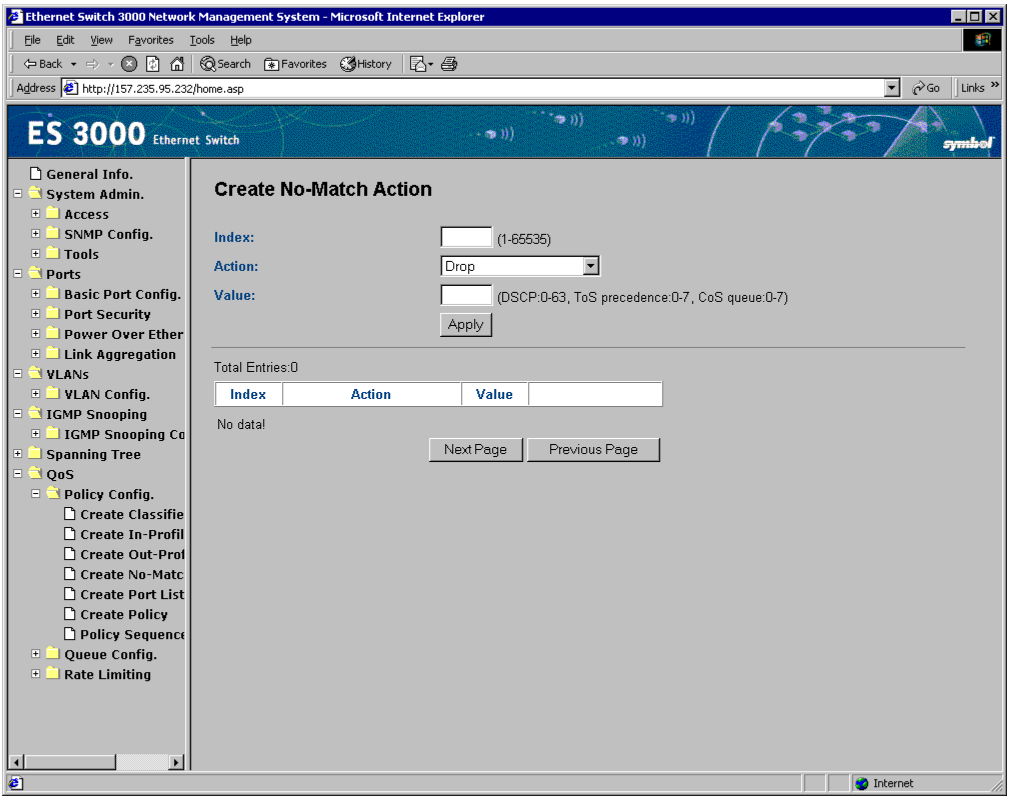
Next Page Previous Page

4.2.45 QoS->Policy Configuration->Create No-Match Action

Committed Rate: The unit for 10/100Mbps port is 1Mbits and 1000Mbps ports is 8Mbits. When the data rate higher than committed rate, the data is sent as best effort. In other words, the packet is delivered when the bandwidth is available.

Burst Size: The burst packet size. User may set it to 0.5Kbyte to 64Kbytes.

No-Match Action resembles In-Profile Action. No-Match Action applies to ingress traffic where the data packets do not match the associated policy. Four actions are available (Drop, Policed-dscp, Policed-precedence, and Policed-cos). Enter an ID between 1-65535, specify an Action and a Value and click **Apply** to implement.



Create No-Match Action

Index: (1-65535)

Action: Drop

Value: (DSCP:0-63, ToS precedence:0-7, CoS queue:0-7)

Apply

Total Entries:0

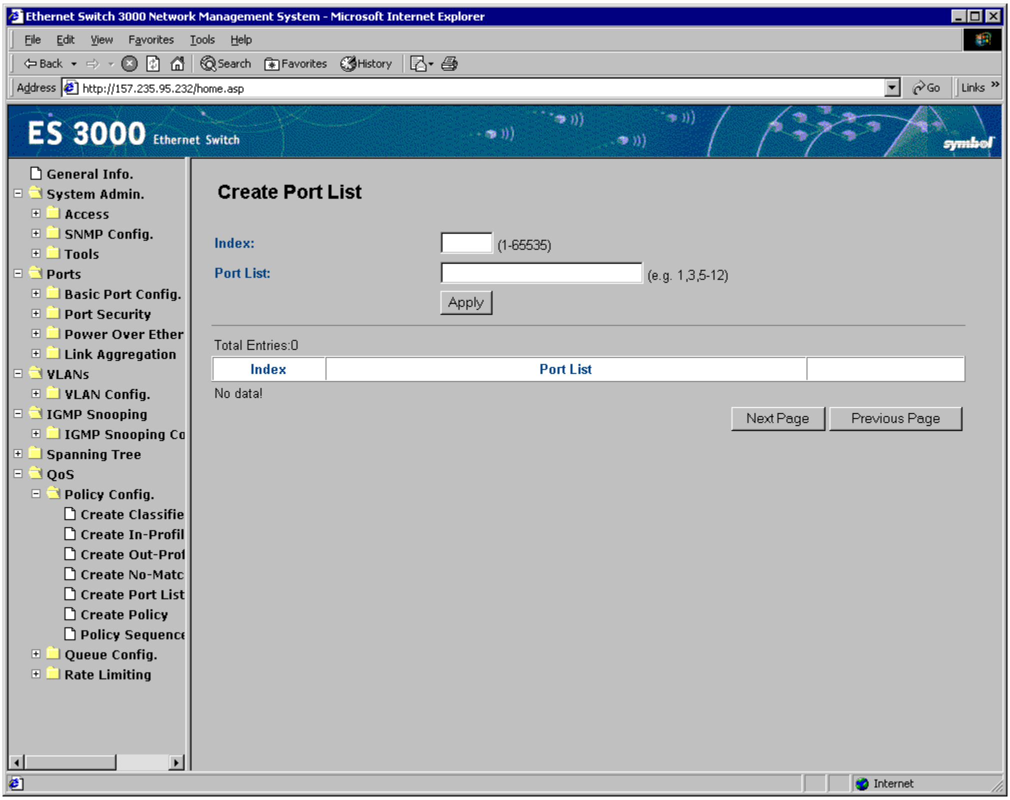
Index	Action	Value	

No data!

Next Page   Previous Page

4.2.46 QoS->Policy Configuration->Create Port List

Use the **Create Port List** page to configure the QoS group by ID, and key in the port in the port list to have the same priority. Select the ports for any Classifier and Action. As shown in the following figure, we have two port lists available and creating the 3rd list which consists of ports 2, 4, 6, and 8 to 12. Any port can be defined in any port list. Click **Apply** to implement the changes.



Create Port List

Index: (1-65535)

Port List: (e.g. 1,3,5-12)

Total Entries:0

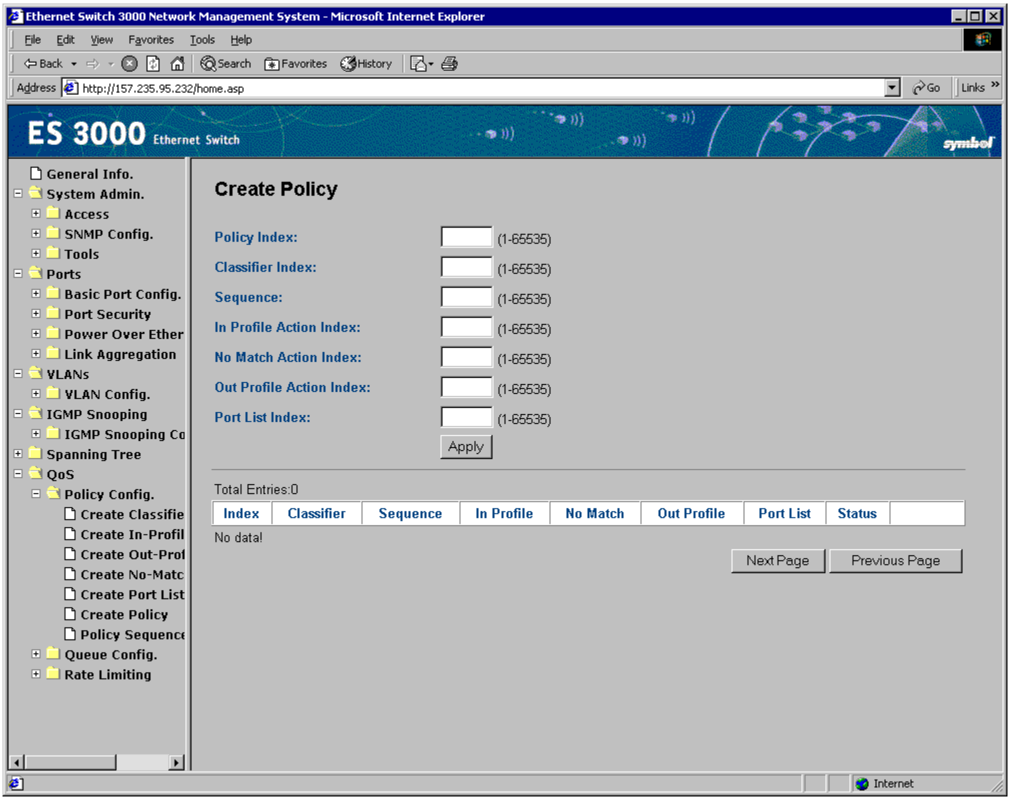
Index	Port List	

No data!

4.2.47 QoS->Policy Configuration->Create Policy

Use the **Create Policy** screen to set up the QoS group by Policy ID, and key in the policy (1-65535) by classifier, in profile action, no match action, out profile action, and data path ID in the blank space. View the setting report by clicking **Apply**.

Using the Classifier, In-Profile Action, Out-Profile Action, No-Match Action and Port List ready, the administrator can create the policy by applying previously defined classifiers, lists, and actions. To avoid confusion, document every index and content entry.



Create Policy

Policy Index: (1-65535)

Classifier Index: (1-65535)

Sequence: (1-65535)

In Profile Action Index: (1-65535)

No Match Action Index: (1-65535)

Out Profile Action Index: (1-65535)

Port List Index: (1-65535)

Apply

Total Entries:0

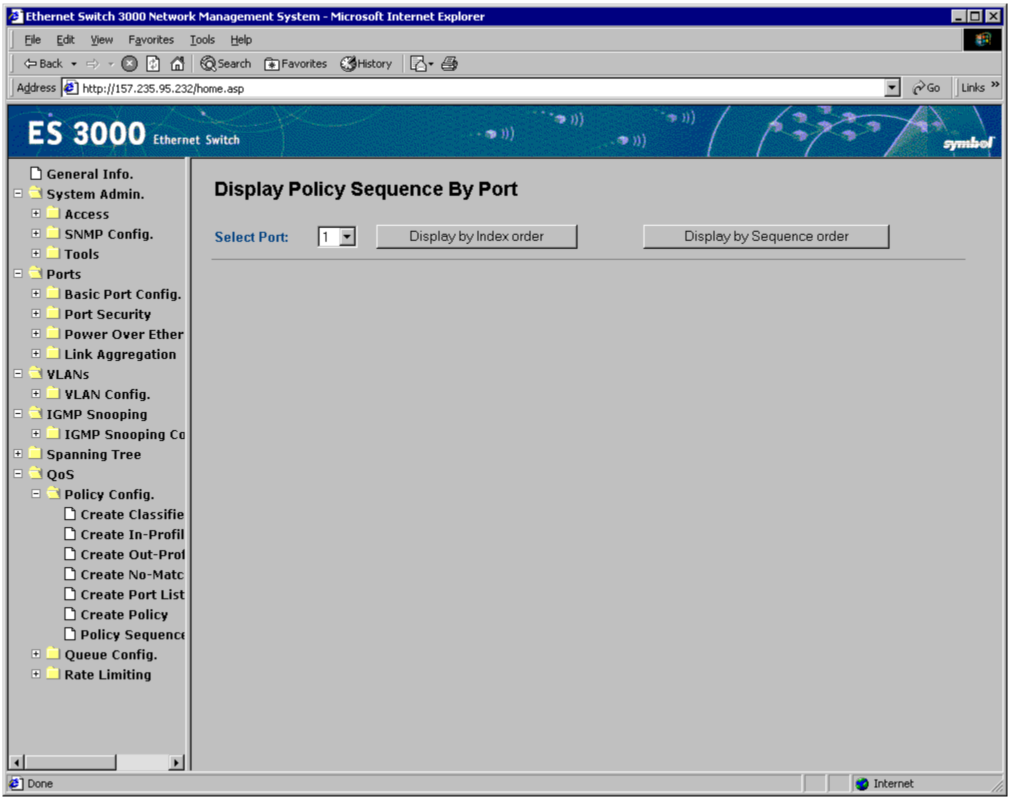
Index	Classifier	Sequence	In Profile	No Match	Out Profile	Port List	Status

No data!

Next Page Previous Page

4.2.48 QoS->Policy Configuration->Policy Sequence

Select Policy Sequence from the Policy Configuration menu to launch the **Display Policy Sequence By Port** page. Select **Display by Index order** to display the policy index for the selected port. Select Display by sequence order to display the selected port policy sequence.

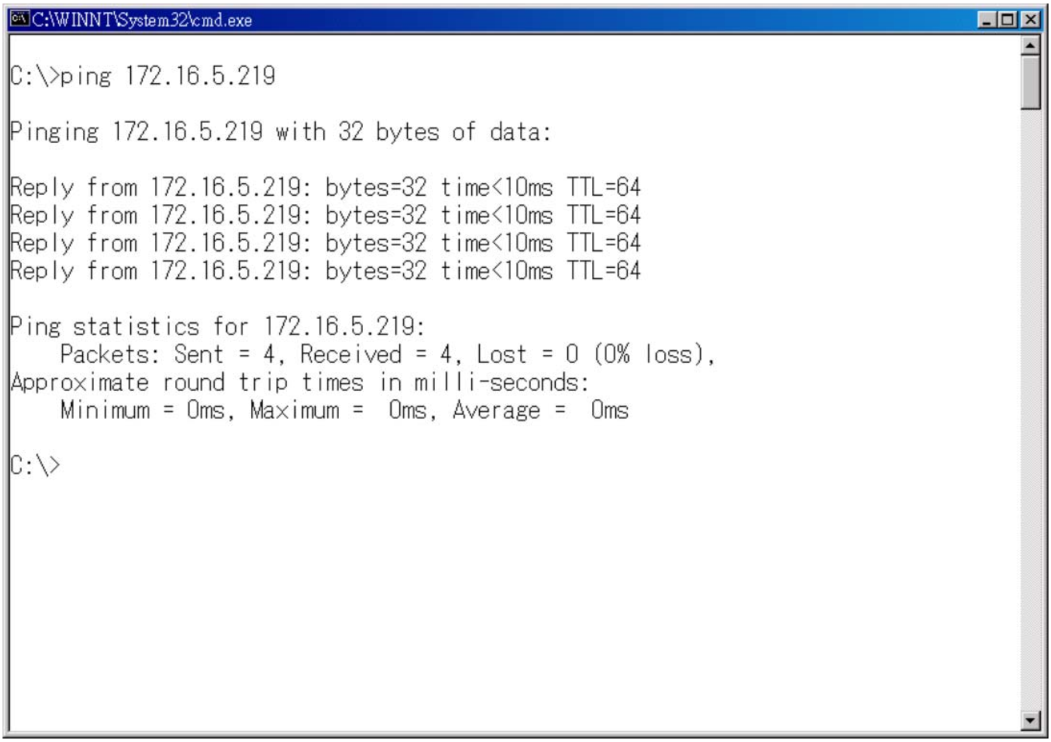


Display Policy Sequence By Port

Select Port: 1 | Display by Index order | Display by Sequence order

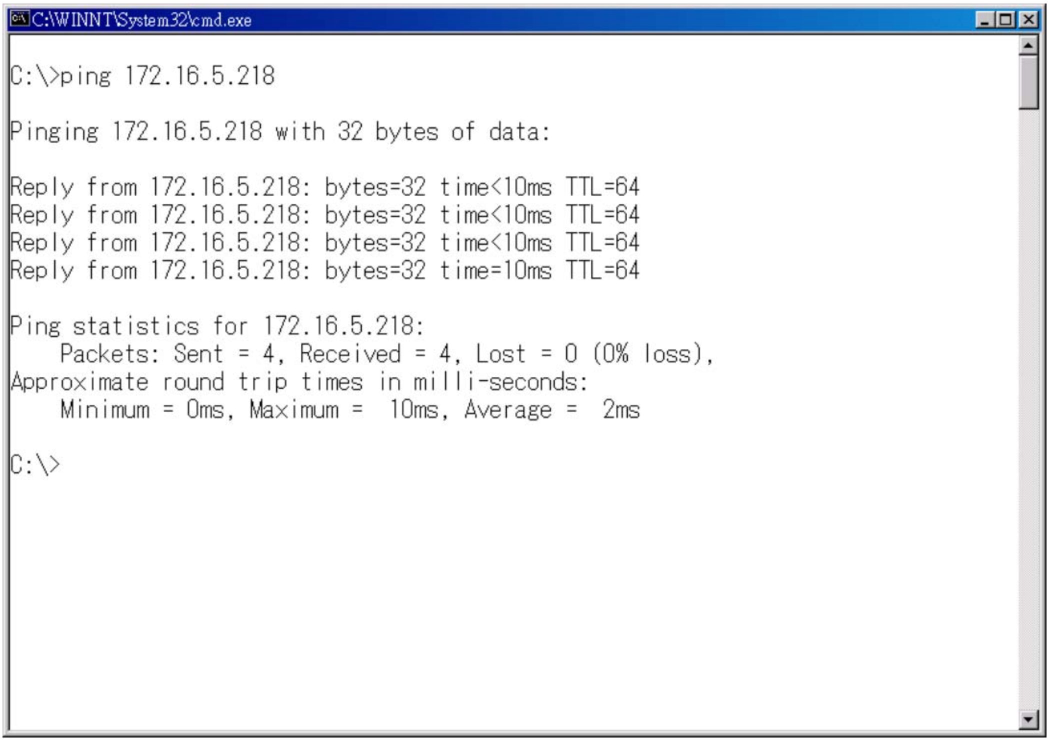
Examples with Applied Policies

When all policies are enabled, use a ping command to check the packet transmissions between switch 172.16.5.219 and host 172.16.5.56 The ping receives responses regardless of whether these policies are enabled or disabled. In other words, these policies are not applied to traffic to the CPU.



```
C:\>ping 172.16.5.219

Pinging 172.16.5.219 with 32 bytes of data:

Reply from 172.16.5.219: bytes=32 time<10ms TTL=64
Reply from 172.16.5.219: bytes=32 time<10ms TTL=64
Reply from 172.16.5.219: bytes=32 time<10ms TTL=64
Reply from 172.16.5.219: bytes=32 time<10ms TTL=64

Ping statistics for 172.16.5.219:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

The traffic between host 172.16.5.56 and switch 172.16.5.218 is verified (in this example). All policies are disabled to verify the physical connection and protocol layers are working properly. If the ping is successful the connection between host and switch are set up properly.

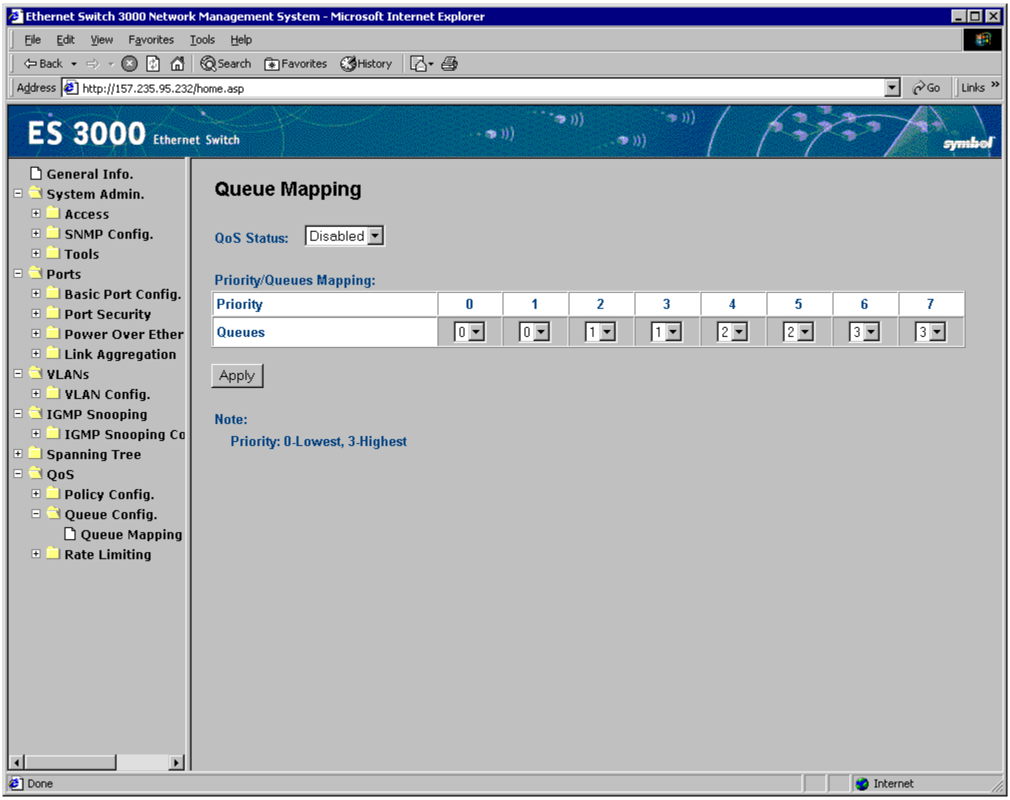


```
C:\>ping 172.16.5.218

Pinging 172.16.5.218 with 32 bytes of data:

Reply from 172.16.5.218: bytes=32 time<10ms TTL=64
Reply from 172.16.5.218: bytes=32 time<10ms TTL=64
Reply from 172.16.5.218: bytes=32 time<10ms TTL=64
Reply from 172.16.5.218: bytes=32 time=10ms TTL=64

Ping statistics for 172.16.5.218:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms

C:\>
```

4.2.49 QoS->Queue Config->Queue Mapping

The priority tag of each packet is divided into four queues on each output port. The default setup is each queue taking two priorities sequentially. The Administrator can configure the traffic class as needed. Enabled or disabled Queue Mapping within the **QoS Status** field.

To provide quality of service, each packet carries a priority using a different approach. The IP packet has a ToS in the header. The IP packet is three bits in length and uses a priority from 0 to 7. The larger number, the higher priority. To ensure high priority packets are delivered first, four priority queues per output port are established. The priority tag of each packet is divided into four queues on each output port evenly. The default setup is each queue taking two priorities sequentially.



Queue Mapping

QoS Status: Disabled

Priority/Queues Mapping:

Priority	0	1	2	3	4	5	6	7
Queues	0	0	1	1	2	2	3	3

Apply

Note:

Priority: 0-Lowest, 3-Highest

Priority	Queue
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

An Administrator can modify the traffic mapping as required. Quality of Service works only after the QoS status is enabled. After the modification, set the QoS Status to **Enabled** and click **Apply** to implement the changes.

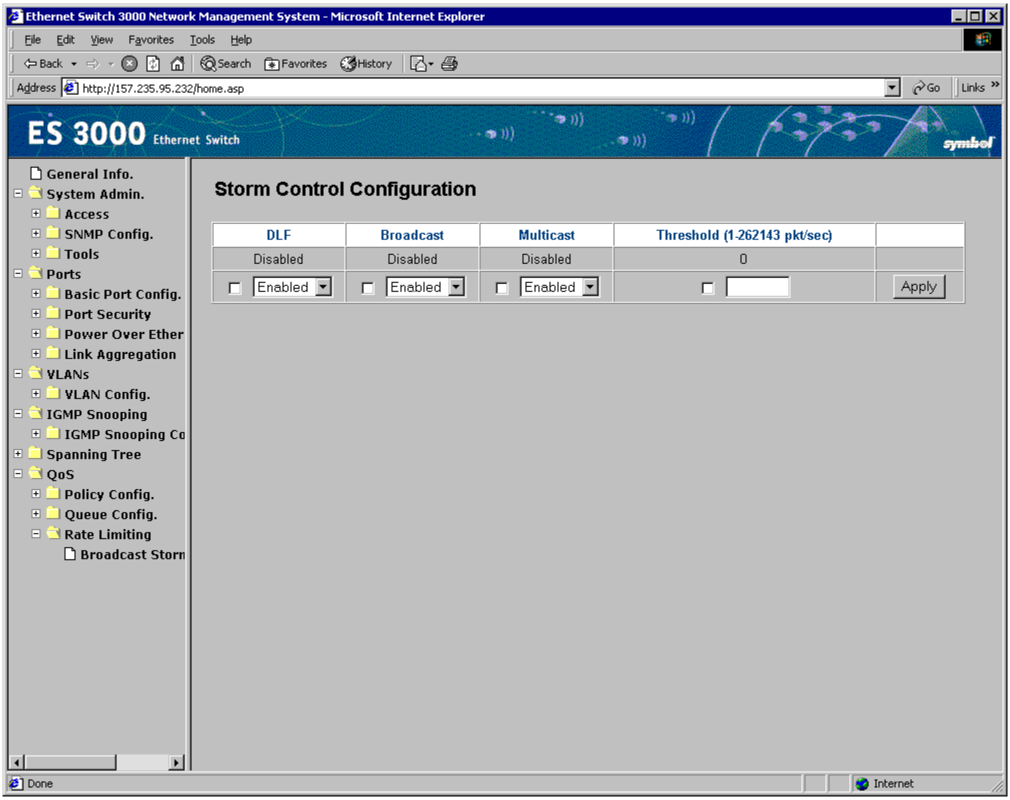
4.2.50 QoS->Rate Limiting->Storm Control Configuration

Rate limiting, or storm control, prevents ports on the ES3000 switch from being overwhelmed by a broadcast, unicast, or multicast storm. A storm results when packets flood the LAN, which degrades network performance. With rate limiting enabled, the switch monitors incoming traffic by counting packets over a period of time. When the packet count exceeds a predefined threshold level, the switch suppresses traffic until the packet count drops below the threshold. With rate limiting disabled, all traffic is allowed. The switch supports rate limiting for broadcast, multicast, and unicast (DLF) traffic, keeping a separate count of the packets for each type of traffic. When broadcast or unicast traffic reaches the threshold, the switch suppresses further traffic of that type until traffic falls below the threshold.

Use the **Storm Control Configuration** page to set the limitation of Broadcast, Multicast, and/or DLF (Destination Look Failure) packets delivered to the CPU. Each kind of packet determines the network load. When the load reaches a certain threshold, the CPU is busy handling packets and is unable to respond to other requests (configuration commands or SNMP requests). Available network bandwidth decreases. The administrator can enable storm control to limit traffic in the networks.

Broadcast, multicast, and/or DLF traffic cannot be set on a per-port basis, only on a per-switch basis.

If a threshold value is defined, that value applies to DLF, Broadcast and Multicast traffic (if enabled) and is in no way shared between the traffic types. Click **Apply** to implement the threshold value for the enabled data types. Storm Control is enabled globally and cannot be defined on a per-port basis.



Storm Control Configuration

DLF	Broadcast	Multicast	Threshold (1-262143 pkt/sec)	
Disabled	Disabled	Disabled	0	
□ Enabled	□ Enabled	□ Enabled	□	Apply

There are three kinds of storm control; DLF, Broadcast, and Multicast.

DLF: Destination Look Failure packets. DLF packets are broadcast to all ports except the incoming port.

Broadcast: Packets are delivered to all ports except the incoming port as DLF packets.

Multicast: Packets are delivered to all ports with group membership.

When Enabled, the CPU drops packets beyond the specified threshold. Otherwise, the CPU processes these packet types without any limitations. The default setting is Disabled for all three packet types.

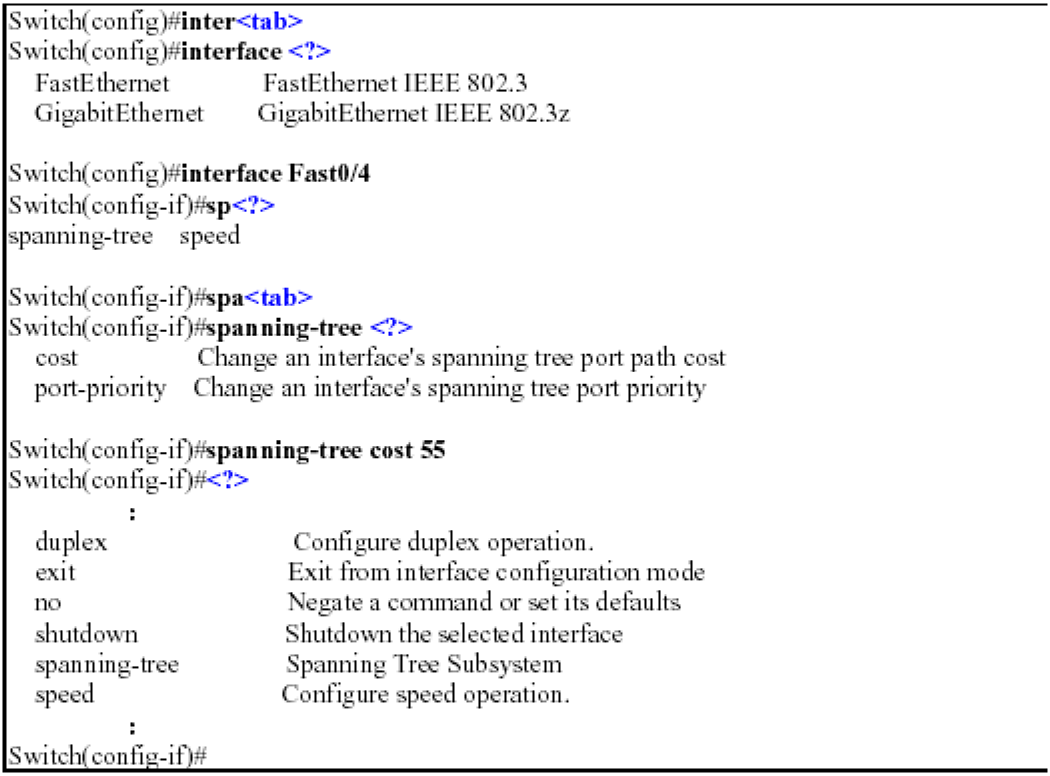
5

Command Line Interface

5.1 ES3000 Ethernet Switch Command Brief

5.1.1 Help Key

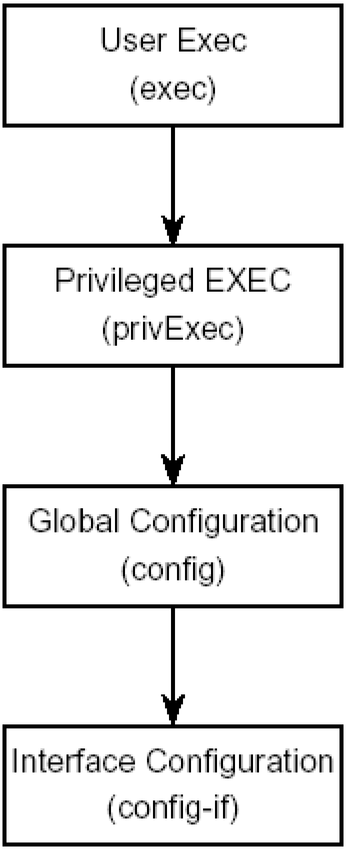
Command	Description
abbreviated-command-entry<?>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<Tab>	Completes a partial command name.
<?>	Lists all commands available for a particular command mode
complete-command <?>	Lists the keywords or arguments that you must enter next on the command line.(Space between command and question mark.



```
Switch(config)#inter<tab>
Switch(config)#interface <?>
   FastEthernet           FastEthernet IEEE 802.3
   GigabitEthernet       GigabitEthernet IEEE 802.3z

Switch(config)#interface Fast0/4
Switch(config-if)#sp<?>
spanning-tree    speed

Switch(config-if)#spa<tab>
Switch(config-if)#spanning-tree <?>
   cost              Change an interface's spanning tree port path cost
   port-priority    Change an interface's spanning tree port priority

Switch(config-if)#spanning-tree cost 55
Switch(config-if)#<?>
             :
   duplex                    Configure duplex operation.
   exit                      Exit from interface configuration mode
   no                        Negate a command or set its defaults
   shutdown                  Shutdown the selected interface
   spanning-tree             Spanning Tree Subsystem
   speed                     Configure speed operation.
             :
Switch(config-if)#
```

5.1.2 Command Hierarchy

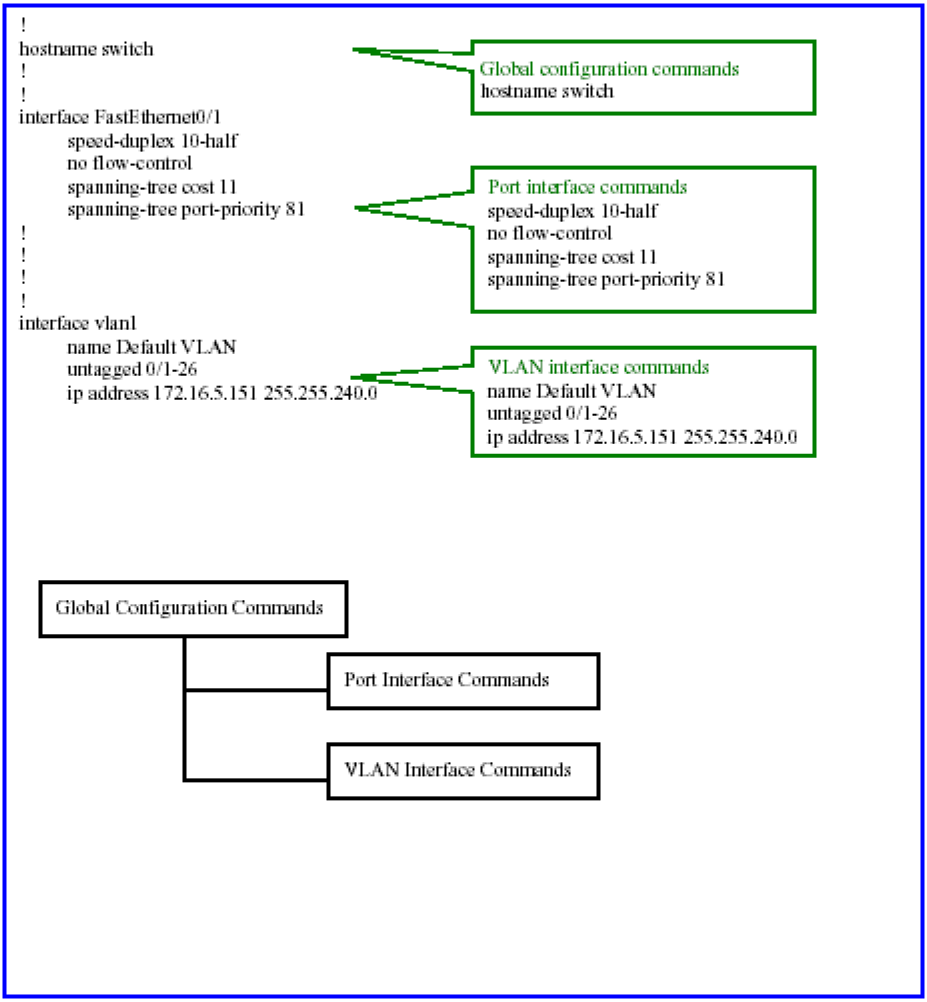
A specific value for each command mode displays at the prompt line. Use specific commands to enter or exit each command mode. The administrator can only enter command modes from specific modes and only exit to specific command modes.



Command Mode	**Prompt**	**Enter/Exit Command**
User EXEC(exec)	Switch>	Default mode, automatically enter logout or exit to quit CLI.
Privileged EXEC(privExec)	Switch#	enable to enter from User EXEC mode logout to quit CLI; disable or exit to User EXEC
Global Configuration(config)	Switch(config)#	configure to enter from Privileged EXEC mode. logout to quit CLI; end or exit to Privileged EXEC mode.
Interface Configuration(config-if)	Switch(config-if)#	interface {Fast Ethernet < port > | < vlanID >} to enter from Global Configuration mode. logout to quit CLI; end to Privileged EXEC mode; exit to Global Configuration Mode.

The prompt displays the switch name, Switch, and the current CLI command mode:

- User EXEC-Switch>
- Privileged EXEC-Switch #
- Global Configuration-Switch (config)#
- Interface Configuration-Switch (config-if)#



```
!
hostname switch
!
!
interface FastEthernet0/1
        speed-duplex 10-half
        no flow-control
        spanning-tree cost 11
        spanning-tree port-priority 81
!
!
!
!
interface vlan1
        name Default VLAN
        untagged 0/1-26
        ip address 172.16.5.151 255.255.240.0
```

Global configuration commands
```
hostname switch
```

Port interface commands
```
speed-duplex 10-half
no flow-control
spanning-tree cost 11
spanning-tree port-priority 81
```

VLAN interface commands
```
name Default VLAN
untagged 0/1-26
ip address 172.16.5.151 255.255.240.0
```

The ESW3000 command sets are organized into the tree hierarchy. The commands, that are not in the same level of the command tree are not available until the user has navigated down to that level. In a lower level of the command tree, the user can still enter the global configuration commands that are in the top level of the command tree. For example, the interface specific configuration commands are available only when the user has entered the interface configuration level.

5.2 Basic Commands

help

The help command is in each command mode and displays a brief message about using the CLI help system.

help

SYNTAX DESCRIPTION:	The help command has no arguments or keywords.
DEFAULT VALUE:	The help command has no default setting.
COMMAND MODES:	All mode
REFERENCE:	Nortel

EXAMPLE:

```
Switch#help

Help can be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument
(e.g. 'show ?') and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you
want to know what arguments match the input (e.g. 'show pr?'.)
```

logout

The logout command logs the user out of the CLI session and returns to the Main Menu of the console interface menus.

logout

SYNTAX DESCRIPTION:	The logout command has no arguments or keywords.
DEFAULT VALUE:	The logout command has no default setting.
COMMAND MODES:	All command mode
REFERENCE:	Nortel

enable

The enable command changes the command mode from User EXEC to privExec mode.

enable

SYNTAX DESCRIPTION:	The enable command has no arguments or keywords.
DEFAULT VALUE:	The enable command has no default setting.
COMMAND MODES:	User EXEC
REFERENCE:	Cisco

EXAMPLE:

```
Switch>enable
Switch#
```

configure

The configure command moves to the Global Configuration (config) command mode and identifies the source for the configuration commands.

configure

SYNTAX DESCRIPTION:	The configure command has no arguments or keywords.
DEFAULT VALUE:	The configure command has no default setting.
COMMAND MODES:	Privileged EXEC
REFERENCE:	Nortel

EXAMPLE:

```
Switch# configure
Switch(config)#
```

interface

The interface command moves to the Interface Configuration (config-if) command mode.

interface

Syntax Description:	The interface command has no arguments or keywords.
Default Value:	The interface command has no default setting.
Command Modes:	Global configuration
Reference:	Nortel

Example:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)#
Switch(config)# interface VLAN 1
Switch(config-if)#
```

disable

Use the disable command to return to the User EXEC (exec) command mode.

disable

Syntax Description:	The disable command has no arguments or keywords.
Default Value:	The disable command has no default setting.
Command Modes:	Privileged EXEC
Reference:	Nortel

Example:

```
Switch(config-if)# disable
Switch>
```

end

Use the end command to exit configuration mode.

end

Syntax Description:	The end command has no argument.
Default Value:	The end command has no default setting.
Command Modes:	All command modes
Reference:	Cisco

exit

The exit command quits to the previous mode.

exit

Syntax Description:	The exit command has no arguments or keywords.
Default Value:	The exit command has no default setting.
Command Modes:	All command modes
Reference:	Cisco
Menu:	

Example:

```
Switch#exit
Switch>
Switch(config-if)#exit
Switch(config)#
```

ping

Use the ping command to display ping test information.

ping <ip>

SYNTAX DESCRIPTION:	*<ip>* IP address
DEFAULT VALUE:	The ping command has no default setting.
COMMAND MODES:	All command modes
REFERENCE:	Nortel
MENU:	Switch Tools Configuration -> Ping Execution

EXAMPLE:

```
Switch# ping 172.16.3.152

Type Ctrl-C to abort.

Reply Received From :172.16.3.152, TimeTaken : 6.45 msecs
Reply Received From :172.16.3.152, TimeTaken : 0.65 msecs
Reply Received From :172.16.3.152, TimeTaken : 0.65 msecs

--- 172.16.3.152 Ping Statistics ---3
Packets Transmitted, 3 Packets Received, 0% Packets Loss

Switch# ping 172.16.3.244

Type Ctrl-C to abort.

Reply Not Received From : 172.16.3.244, Timeout : 1 secs
Reply Not Received From : 172.16.3.244, Timeout : 1 secs
Reply Not Received From : 172.16.3.244, Timeout : 1 secs

--- 172.16.3.244 Ping Statistics ---
3 Packets Transmitted, 0 Packets Received, 100% Packets Loss
```

copy tftp image

Use the copy tftp image command to download image or config files.

copy tftp*<ip-address> <file name>*image

SYNTAX DESCRIPTION: *<ip>* IP address
< file name > file name
DEFAULT VALUE: The copy tftp image command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# copy tftp 172.16.3.152 image. img image

Downloading Image From Remote Server. Type Ctrl-C to abort.
Receive 1654949 bytes
Writing image to Flash...Please wait a minute. (reboot automatically)
start reboot.....
```

copy running-config tftp

Use this command to upload and download Config file

copy running-config tftp*<ip-address> <file name>*
copy tftp*<ip-address> <file name>* running config

SYNTAX DESCRIPTION: <ip> IP address
SYNTAX DESCRIPTION: < file name > Config file name
DEFAULT VALUE: The command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# copy running-config tftp 172.16.3.152 config.txt
Please wait a minute.

2581 bytes data transferred!

Switch# copy tftp 172.16.3.152 config.txt running-config
Please wait a minute.

2581 bytes data transferred!

Switch#
```

copy running-config startup-config

Use this command to save the config to NVRAM.

copy running-config startup-config

SYNTAX DESCRIPTION:
DEFAULT VALUE: The command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# copy running-config startup-config

Saving Configuration ...

Saving Configuration to Flash is Successful!

Switch#
```

5.3 Web Browser Commands

ip http server

Use this command to enable or disable access to the Web server embedded in the system.

ip http server

no ip http server

SYNTAX DESCRIPTION:	The ip http server command has no argument.
DEFAULT VALUE:	The feature is enabled by default.
COMMAND MODES:	Global configuration
REFERENCE:	Cisco
MENU:	Basic Switch Configuration Menu->User Interface->Enable/Disable Web Server

EXAMPLE:

```
! Enable web server

Switch(config)# ip http server

Web server is Enabled now

Switch (config)#
```

```
! Disable web server

Switch(config)# no ip http server

Switch(config)#
```

show ip http server

Use the show ip http server command to display telnet.

show ip http server

SYNTAX DESCRIPTION:	The show ip http server command has no arguments or keywords.
DEFAULT VALUE:	The show ip http server command has no default setting.
COMMAND MODES:	Privileged EXEC
REFERENCE:	None
MENU:	Basic Switch Configuration Menu -> User Interface Configuration Menu

EXAMPLE:

```
Switch# show ip http server

Web Server
---------------
enabled

Switch#
```

5.4 SNMP Commands

snmp-server agent

Use the snmp-server agent command to enable or disable the access to the SNMP agent embedded in the system.

snmp-server agent

no snmp-server agent

Syntax Description: The snmp-server agent command has no argument
Default Value: The snmp-server agent feature is enabled by default
Command Modes: Global configuration
Reference:
Menu:

Example:

```
! Enable SNMP agent
Switch(config)# snmp-server agent
Switch(config)#
```

```
! Disable SNMP agent
Switch(config)# no snmp-server agent
Switch(config)#
```

snmp-server location

To set the system location string.

snmp-server location *<string>*

no snmp-server location

Syntax Description: A string of length with 50 characters maximum
Default Value: No system location string is set by default
Command Modes: Global configuration
Reference: Cisco
Menu: Basic Switch Configuration Menu->System Administration->Set System Location

Example:

```
!Set system location to "room_1"
Switch(config)# snmp-server location room_1
```

```
!Clean system location back to default value
Switch(config)# no snmp-server location
```

snmp-server contact

To set the system contact string.

snmp-server contact *<string>*

no snmp-server contact

Syntax Description: A string of length with 50 characters maximum
Default Value: No system location string is set by default
Command Modes: Global configuration
Reference: Cisco
Menu: Basic Switch Configuration Menu->System Administration->Set System Contact Information

EXAMPLE:

```
!Set system Contact Information "MIS_1"
Switch(config)# snmp-server contact MIS_1
Switch(config)#
```

```
!Clean system Contact Information to default
Switch(config)# no snmp-server contact
Switch(config)#
```

snmp-server community

Use the snmp-server community command to set up the community access string for use with SNMP protocol.

snmp-server community <index> <community> <privilege> [<ip>]

SYNTAX DESCRIPTION:	*<index>*	1-10	
	<community>	A string of length with 20 characters maximum	
	<privilege>	RO	Specifies read-only access
		RW	Specifies read-write access
	<ip>	Manager IP address.	

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE: Cisco

MENU: Basic Switch Configuration Menu->SNMP->Set SNMP Read Community

EXAMPLE:

```
!Set SNMP Read Community "public" in index-1 for all IP
Switch(config)# snmp-server community 1 public RO
Switch(config)#
```

```
!Set SNMP Write Community "private" in index-3 for IP 192.168.0.1
Switch(config)# snmp-server community 3 private RW 192.168.0.1
Switch(config)#
```

```
!Disable SNMP manager entry index-4
Switch(config)# no snmp-server community 4
Switch(config)#
```

snmp-server host

Use the snmp-server host command to set up the recipient of SNMP notification operation.

snmp-server host *<index>* type<traptype>*<ip>* trap *<string>*

no snmp-server host *<index>* type<traptype>*<ip>* trap *<string>*

SYNTAX DESCRIPTION:	*<index>*	1-10
	<traptype>	v1 for SNMP V1 v2 for SNMP V2
	<ip>	IP address of the recipient
	<string>	A string of length with 20 characters maximum
DEFAULT VALUE:	"public" is set as the community string for read-only access and "private" is set as the community string for read-write access by default	
COMMAND MODES:	Global configuration	
REFERENCE:	Cisco	
MENU:	Basic Switch Configuration Menu->SNMP->SNMP Trap Receiver	

EXAMPLE:

```
! Add SNMP Trap Receiver ip 172.16.5.198 community "private" in index-10
Switch(config)# snmp-server host 10 type v1 172.16.5.198 trap private
Switch(config)#
```

```
! Delete SNMP Trap Receiver index-5
Switch(config)# no snmp-server host 5
Switch(config)#
```

snmp-server enable traps

Use the snmp-server enable traps command to enable or disable the specified SNMP notification.

snmp-server enable traps <notification-type> <notification-option>

no snmp-server enable traps <notification-type> <notification-option>

SYNTAX DESCRIPTION: <**notification-type**>
<**notification-option**>

DEFAULT VALUE: The default value for each option in all notification types is:

notification-type	*notification-option*	*default*
snmp	authentication	disabled
snmp	coldstart	enable
snmp	linkupdown <port list>	enable
bridge	newRoot	enable
bridge	topologyChange	enable
rmon	alarm	enable
symbol	configChange	enable
symbol	ACLViolation	enable

COMMAND MODES: Global configuration

REFERENCE: Cisco

MENU: Basic Switch Configuration Menu->SNMP->Enable/Disable Authentication Trap

EXAMPLE:

show snmp

Use the show snmp command to display snmp trap-receivers information.

show snmp

SYNTAX DESCRIPTION: The show snmp command has no arguments or keywords.
DEFAULT VALUE: The show snmp command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Cisco
MENU: Basic Switch Configuration -> SNMP Configuration Menu

EXAMPLE:

```
Switch# show snmp
  No.  Status     Previlige     IP Address        Community
 ----  --------   ------------  --------------    --------------------
   1   Enabled    Read-Write    0.0.0.0           NETMAN
   2   Enabled    Read-Only     0.0.0.0           PUBLIC
   3   Disabled   Read-Only     2.2.2.2           123416
   5   Disabled   Read-Write    1.1.1.1           123

Trap-Receiver
  No.   Status    IP Address       Community
 ----  --------   --------------   ----------------------------
  3    Enabled    172.16.3.77      PUBLIC

Individual Trap
 Authentication Failure:       Disabled
 Enable Link Up/Down Port:     1 - 12
 OSPF Trap Control:
  1. Virtual_IF_State_Change : Down    2. Neighbor_State_Change  : Down
  3. Virt_Nei_State_Change   : Down    4. IF_Config_Err          : Down
  5. Virt_IF_Config_Err      : Down    6. IF_Auth_Failure        : Down
  7. Virt_IF_Auth_Failure    : Down    8. IF_RX_Bad_Packet       : Down
  9. Virt_IF_RX_Bad_Packet   : Down   10. IF_TX_Retransmit       : Down
 11. Virt_IF_TX_Retransmit   : Down   12. Originate_LSA          : Down
 13. MAX_AGE_LSA             : Down   14. LSDB_Overflow          : Down
 15. LSDB_Approach_Overflow  : Down   16. IF_State_Change        : Down
Basic System Management Commands
Switch#
```

5.5 Basic System Management Commands

hostname

Use the hostname command to specify the host name for the system.

hostname *<string>*

SYNTAX DESCRIPTION:	A string of length with 50 characters maximum
DEFAULT VALUE:	No host name string is set by default
COMMAND MODES:	Global configuration
REFERENCE:	Cisco
MENU:	Basic Switch Configuration Menu->System Administration->Set System Name

EXAMPLE:

```
!Set system name "switch_1"
Switch(config)# hostname switch_1
Switch(config)#
```

```
!Clean system name to default
Switch(config)# no hostname
Switch(config)#
```

show sys-info

Use the show sys-info command to display system information.

show sys-info

SYNTAX DESCRIPTION:	The show sys-info command has no arguments or keywords.
DEFAULT VALUE:	The show sys-info command has no default setting.
COMMAND MODES:	Privileged EXEC
REFERENCE:	Cisco
MENU:	Basic Switch Configuration Menu -> System Administration Configuration Menu

EXAMPLE:

```
Switch# show sys-info

System up for         :  1hr(s), 18min(s), 06sec(s)
Boot Code Version     : 1.0.0.07 / Feb 16 2004 14:35:55
Runtime Code Version  : 1.0.7.05 / Apr 01 2004 09:33:00

Hardware Information
Version             : Version1
DRAM Size           : 32MB
Fixed Baud Rate     : 9600bps
Flash Size          : 8MB

Administration Information
Switch Name         : 12G-Switch
Switch Location     : DNI-3FB
Switch Contact      : DNI_KARL

System Address Information
MAC Address         : 00:00:00:22:33:44
IP Address          : 172.16.3.224
Subnet Mask         : 255.255.0.0
Default Gateway     : 0.0.0.0
DHCP Mode           : Disabled

Switch#
```

console inactivity-timer

Use the console inactivity-timer command to specify an inactivity timeout value for the console.

console inactivity-timer *<min>*

SYNTAX DESCRIPTION: 0 - 60 minutes (0 means no timeout)
DEFAULT VALUE: The default value is 5 minutes.
COMMAND MODES: Global configuration
REFERENCE: HP
MENU: Basic Switch Configuration Menu->User Interface->Set Console UI Time Out

EXAMPLE:

```
! Set console timeout 5min
Switch(config)# console inactivity-timer 5
Switch(config)#
```

```
! Set console no timeout
Switch(config)# console inactivity-timer 0
Switch(config)#
```

show console

Use the show console command to display user telnet information.

show console

SYNTAX DESCRIPTION: The show console command has no arguments or keywords.
DEFAULT VALUE: The show console command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: None.
MENU: Basic Switch Configuration Menu -> User Interface Configuration Menu

Example:

```
Switch# show console

Console UI Idle Timeout: 5 Min.

Console
--------
Active

Switch#
```

telnet-server enable

Use the telnet-server command to enable or disable access to the telnet server.

telnet-server enable
no telnet-server

Syntax Description:	The telnet-server command has no argument.
Default Value:	The feature is enabled by default.
Command Modes:	Global configuration
Reference:	HP
Menu:	Basic Switch Configuration Menu->User Interface->Enable/Disable Telnet Server

Example:

```
! Enable telnet server
Switch(config)# telnet-server
Switch(config)#
```

```
! Disable telnet server
Switch(config)# no telnet-server
Switch(config)#
```

telnet-server inactivity-timer

Use the telnet-server inactivity-timer command to specify an inactivity timeout value for telnet server.

telnet-server inactivity-timer <min>

SYNTAX DESCRIPTION:	1 - 60 minutes
DEFAULT VALUE:	The default value is 5 minutes
COMMAND MODES:	Global configuration
REFERENCE:	None
MENU:	Basic Switch Configuration Menu->User Interface->Set Telnet UI Time Out

EXAMPLE:

```
! Set telnet timeout 5min
Switch(config)# telnet-server inactivity-timer 5
Switch(config)#
```

show telnet-server

Use the show telnet-server command to display the telnet idle timeout value.

show telnet-server

SYNTAX DESCRIPTION:	The show telnet-server command has no arguments or keywords.
DEFAULT VALUE:	The show telnet-server command has no default setting.
COMMAND MODES:	Privileged EXEC
REFERENCE:	None
MENU:	Basic Switch Configuration Menu -> User Interface Configuration Menu

EXAMPLE:

```
Switch# show telnet-server

Telnet UI Idle Timeout: 5 Min.

Telnet Server
---------------
enabled

Switch#
```

5.6 IP Addressing Commands

ip address

Use the ip address command to specify an IP address and subnet mask for the system.

ip address *<ip> <mask>*

SYNTAX DESCRIPTION: *<ip>* IP address
<mask> Mask for the associated IP subnet

DEFAULT VALUE: Both values are 0.0.0.0 by default

COMMAND MODES: Layer-2 switch => Global configuration
Layer-3 switch => Interface configuration (Vlan)

REFERENCE: Cisco

MENU: Basic Switch Configuration Menu->System IP->Set IP Address Set Subnet Mask

EXAMPLE:

```
!Set IP 172.16.5.151 mask 255.255.240.0
Switch(config)# ip address 172.16.5.151 255.255.240.0
Switch(config)#
```

ip address dhcp

Use the ip address dhcp command to enable or disable the system to acquire its IP address through DHCP.

ip address dhcp

SYNTAX DESCRIPTION:	The ip address dhcp-bootp command has no argument.
DEFAULT VALUE:	The feature is disabled by default.
COMMAND MODES:	Layer-2 switch => Global configuration Layer-3 switch => Interface configuration (Vlan)
REFERENCE:	HP
MENU:	Basic Switch Configuration Menu->System IP->Enable/Disable DHCP Mode

EXAMPLE:

```
!Set IP address use dhcp
Switch(config)# ip address dhcp
Switch(config)#
```

ip address renew

Use the ip address renew command to renew a DHCP ip address.

ip address renew

SYNTAX DESCRIPTION:	The ip address renew command has no argument.
DEFAULT VALUE:	The ip address renew command has no default setting.
COMMAND MODES:	Layer-2 switch => Global configuration Layer-3 switch => Interface configuration (Vlan)
REFERENCE:	
MENU:	Basic Switch Configuration Menu->System IP->IP Address Renew

EXAMPLE:

```
!Renew IP address
Switch(config)# ip address renew
Switch(config)#
```

show ip conf

Use the show ip conf command to display IP configurations.

show ip conf

SYNTAX DESCRIPTION: The show ip conf command has no arguments or keywords.
DEFAULT VALUE: The show ip conf command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: None

EXAMPLE:

```
Switch# show ip conf

MAC Address       : 00:00:00:22:33:44
IP Address        : 172.16.3.71
Subnet Mask       : 255.255.255.0
Default Gateway   : 172.16.3.254
DHCP Mode         : Enabled

Switch#
```

5.7 Security Commands

username

Use the username command to specify the user name and password for logging into the system.

username name *<string>*

SYNTAX DESCRIPTION:	The user name string is limited to 13 characters.
DEFAULT VALUE:	Both are set to "manager".
COMMAND MODES:	Global configuration
REFERENCE:	
MENU:	Basic Switch Configuration Menu->User Interface->Change Administrator User Name

EXAMPLE:

```
! Set username "admin" password "delta"

Switch(config)# username admin

Old Password: *******

Enter New Password: *******

Reenter the Password: *******

Updating username and password ....

Username and password updated Successfully

Switch(config)#
```

5.8 Layer-2 Interface Commands

shutdown

Use the shutdown command to enable or disable a port.

interface *<port>*

shutdown

no shutdown

SYNTAX DESCRIPTION: *<port>* Port instance
DEFAULT VALUE: The shutdown feature is enabled by default.
COMMAND MODES: Interface configuration
REFERENCE: Cisco
MENU: Basic Switch Configuration Menu->Port->Set Status

EXAMPLE:

```
! Enable port-3
Switch(config)# interface fastethernet0/3
Switch(config-if)# no shutdown
Switch(config-if)#
```

```
! Disable port-25(giga port)
Switch(config)# interface fastethernet0/3
Switch(config-if)# shutdown
Switch(config-if)#
```

speed-duplex

Use the speed-duplex command to configure the speed and duplex mode for a port.

interface *<port>*

speed-duplex *<option>*

SYNTAX DESCRIPTION: *<port>* Port instance

<option> ,

Option	*Meaning*
auto	Auto negotiation mode
10-half	10 Mbps & half-duplex mode
10-full	10 Mbps & full-duplex mode
100-half	100 Mbps & half-duplex mode
100-full	100 Mbps & full-duplex mode
1000-half	1000 Mbps & half-duplex mode
1000-full	1000 Mbps & full-duplex mode

DEFAULT VALUE: The default value is set to auto.
COMMAND MODES: Interface configuration
REFERENCE: Cisco
MENU: Basic Switch Configuration Menu->Port->Set Mode

EXAMPLE:

```
! set port-3 speed 100 duplex full
Switch(config)# interface fastethernet0/3
Switch(config-if)# speed-duplex 100-full
Switch(config-if)#
```

flow-control

Use the flow-control command to enable or disable the flow control for a port.

interface <*port*>

flow-control

no flow-control

Syntax Description: <*port*> Port instance

Default Value: The flow control feature is enabled by default.

Command Modes: Interface configuration

Reference: Cisco

Menu: Basic Switch Configuration Menu->Port->Set Flow control

Example:

```
! Enable Flow control port-3
Switch(config)# interface fastethernet0/3
Switch(config-if)# flow-control
Switch(config-if)#
```

```
! Disable Flow control port-25(giga port)
Switch(config)# interface fastetherne0/3
Switch(config-if)# no flow-control
Switch(config-if)#
```

show interface info

Use the show interface info command to display port information.

show interface

Syntax Description: The show interface info command has no arguments or keywords.

Default Value: The show interface info command has no default setting.

Command Modes: Privileged EXEC

Reference: Nortel

Menu: Basic Switch Configuration Menu -> Port Configuration Menu

EXAMPLE:

```
Switch# show interface
Port    Trunk    Type        Link     Status      Mode       Flow Ctrl
----    -----    --------    -----    --------    -------    ----------
 1/1     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/2     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/3     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/4     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/5     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/6     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/7     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/8     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/9     ---     10/100TX    Down     Enabled     Auto       Enabled
 1/10    ---     10/100TX    Down     Enabled     Auto       Enabled
 1/11    ---     10/100TX    Down     Enabled     Auto       Enabled
 1/12    ---     10/100TX    Down     Enabled     Auto       Enabled
```

show interface counters

Use the show interface counters command to display interface statistics.

show interface counters *<port>*

SYNTAX DESCRIPTION: *<port>* Port instance.
DEFAULT VALUE: The feature is disabled by default.
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU: Main Menu -> Statistics Menu

EXAMPLE:

```
Switch# show interface counters fastethernet0/2

Total RX Bytes    Total RX Pkts    Good Broadcast    Good Multicast
0                 0                    0                 0

64-Byte Pkts       65-127 Pkts      128-255 Pkts
21                 0                 0

256-511 Pkts     512-1023 Pkts    1024-1518 Pkts
9                 0                 0

Switch#
```

show interface counters errors

Use the show interface counters erros command to display counter error information.

show interface counters errors *<port>*

SYNTAX DESCRIPTION: *<port>* Port instance.
DEFAULT VALUE: The feature is disabled by default.
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU: Main Menu -> Statistics Menu

EXAMPLE:

```
Switch# show interface counters errors fastethernet0/2

CRC/Align Errors    Undersize Pkts    Oversize Pkts
0                 0                0
Fragments           Jabbers       Collisions
0                 0                0

Switch #
```

port monitor

Use the port monitor command to configure a port to monitor traffic from another port.

interface *<port>*

port monitor *<port>* direction *<direction>*

SYNTAX DESCRIPTION:		
	<port>	Port instance
	<type>	Monitor type
	<direction>	Direction

Direction	*Meaning*
receive	Monitor receive packets
transmit	Monitor transmit packets
both	Monitor receive and transmit packets

DEFAULT VALUE: The port monitor feature is disabled by default.

COMMAND MODES: Interface configuration

REFERENCE: Cisco

MENU: Advanced Switch Configuration Menu->Port Monitoring->Set Monitoring Port Set Monitored Port

Example:

```
! Set port-2 Monitoring Port , port-4 Monitored Port, direction is both.
Switch(config)# interface fastethernet0/2
Switch(config-if)# port monitor fastethernet0/4 direction both
Switch(config-if)#
```

```
!Disable port-2 Monitoring Port , port-4 Monitored Port
Switch(config)# interface fastethernet0/2
Switch(config-if)# no port monitor
Switch(config-if)#
```

show monitor

Use the show monitor command to display port monitoring information.

show monitor

Syntax Description: The show monitor command has no arguments or keywords.
Default Value: The show monitor command has no default setting.
Command Modes: Privileged EXEC
Reference: Cisco
Menu: Advanced Switch Configuration -> Port Monitoring Configuration Menu

Example:

```
Switch# show monitor

Port monitor status is Disabled
Monitoring direction: Both
Monitoring Port: 2
Monitored Port: 4

Switch#
```

storm-control threshold

Use the storm-control threshold command to configure the mulitcast storm control for a port.

storm-control threshold*<threshold>*

SYNTAX DESCRIPTION:	*<threshold>*	Threshold value for a port (packets per second).
DEFAULT VALUE:		
COMMAND MODES:	Global configuration	
REFERENCE:	Cisco	
MENU:	Basic Switch Configuration Menu->Storm->Set Threshold	

EXAMPLE:

```
! Set rate 3000 packets per second
Switch(config)# strom-control threshold 3000
Switch(config)#
```

storm-control broadcast

Use the strom-control broadcast command to configure the broadcast storm control for a port.

storm-control broadcast

no storm-control broadcast

SYNTAX DESCRIPTION: The storm-control broadcast command has no arguments or keywords.
DEFAULT VALUE: The default value is disabled.
COMMAND MODES: Global configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! Set broadcast storm control Enable
Switch(config)# strom-control broadcast
```

```
! Disable broadcast strom control
Switch(config)# no storm-control broadcast
```

storm-control multicast

Use the strom-control multicast command to configure the multicast storm control for a port.

storm-control multicast

no storm-control multicast

SYNTAX DESCRIPTION: The storm-control multicast command has no arguments or keywords.
DEFAULT VALUE: The default value is disabled.
COMMAND MODES: Global configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! Set multicast storm control Enable
Switch(config)# strom-control multicast
```

```
! Disable multicast storm control
Switch(config)# no storm-control mutlicast
```

storm-control unicast

Use the storm-control unicast command to configure the unicast(DLF) storm control for a port.

storm-control unicast

no storm-control unicast

SYNTAX DESCRIPTION: The storm-control unicast command has no arguments or keywords.
DEFAULT VALUE: The default value is disabled.
COMMAND MODES: Global configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! Set unicast storm control Enable
Switch(config)# storm-control unicast
```

```
! Disable unicast storm control
Switch(config)# no storm-control unicast
```

show storm-control

Use the show storm-control command to display storm-control status.

show storm-control

SYNTAX DESCRIPTION: The show storm-control command has no arguments or keywords.
DEFAULT VALUE: The show storm-control command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Cisco
MENU: Basic Switch Configuration Menu -> Storm Control Configuration Menu

EXAMPLE:

```
Switch# show storm-control

Port Storm Control Setting:

DLF      Broadcast Multicast Threshold
------------------ --------- ---------
Disabled Disabled Disabled 2000

Switch#
```

5.9 Link Aggregation Commands

lacp

Use the lacp command to add ports to a port LACP group or delete ports from the group.

lacp <trunkKEY> <port list> <mode>

SYNTAX DESCRIPTION:	*<trunkKEY>*	Trunk LACP key
	<port list>	A list of port instances
	<mode>	

Option	*Meaning*
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 the opposite device.
Manual	Static link aggregation

DEFAULT VALUE:	The feature is disabled by default.
COMMAND MODES:	Global configuration
REFERENCE:	HP
MENU:	

EXAMPLE:

```
! Set port-1 port-2 port-3 link aggregation, and LACP key =10 and mode =
active
Switch(config)# lacp 10 1,2,3 active
Switch(config)#
```

```
! Set port-10-13 link aggregation,and LACP key =42 and mode = passive
Switch(config)# lacp 42 10-13 passive
Switch(config)#
```

```
! Set port-5-7 link aggregation,and LACP key =42 and mode = manual
Switch(config)# lacp 12 5-7 manual
Switch(config)#
```

```
! Disable link aggregation(LACP key 10)
Switch(config)# no lacp 10
Switch(config)#
```

lacp system-priority

Use the lacp system-priority command to set the LACP system priority.

lacp system-priority *<priority-value>*

SYNTAX DESCRIPTION: *<priority-value>* Lacp system priority 1-65535
DEFAULT VALUE:
COMMAND MODES: Global configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! Set system-priority 40000
Switch(config)# lacp system-priority 40000
```

lacp port-priority

Use the lacp port-priority command to LACP port priority.

lacp port-priority *<priority-value>*

Syntax Description: *<priority-value>* Lacp port priority 0-255
Default Value:
Command Modes: Interface configuration
Reference: Cisco
Menu:

Example:

```
! set port 3 port-priority 40
Switch(config)# interface fastethernet0/3
Switch(config-if)# lacp port-priority 40
Switch(config-if)#
```

show lacp

Use the show lacp command to display link aggregation information.

show lacp

Syntax Description: *<LA-KEY>* link aggregation LACP key.
Default Value: The show lacp command has no default setting.
Command Modes: Privileged EXEC
Reference: Nortel
Menu:

EXAMPLE:

```
Switch# show lacp

System Priority  : 40000


  Key    Mode       Member post list
  ----   --------   ---------   ---------   ---------
  1      Manual     2,3
  2      Active     4,5,6

Switch#
```

```
Switch# show lacp 2

System Priority  : 40000
Key 2

  Key    Pri        Attached port list
  ----   --------   ---------   ---------   ---------
  4      1          4
  5      1          5
  6      1          6

Switch#
```

5.10 MAC Address Commands

mac-address-table static

Use the mac-address table static command to insert a static MAC address.

mac-address-table static *<mac-addr> <port>* vlan *<vlanID>*

SYNTAX DESCRIPTION:	*<mac-addr>*	MAC address
	<port>	Port instance
	<vlanID>	VLAN ID
DEFAULT VALUE:	This feature has no default value.	
COMMAND MODES:	Global configuration	
REFERENCE:	Cisco	
MENU:	Basic Switch Configuration Menu->Forwarding Database-> Static Address	

EXAMPLE:

```
! Add static entry mac address 00:00:A0:21.00:11 port port-4 vlan 2
Switch(config)# mac-address-table static 00:00:A0:21.00:11
fastethernet0/4 vlan 2
Switch(config)#
```

```
! delete static entry mac address 00:00:A0:21.00:11 port port-4 vlan 2
Switch(config)# no mac-address-table static 00:00:A0:21.00:11 vlan 2
Switch(config)#
```

mac-address-table aging-time

Use the mac-address-table aging-time command to control aging time for dynamic MAC addresses.

mac-address-table aging-time*<sec>*

Syntax Description: Integer ranges from 10 - 1000000.
Default Value: Default value is 300.
Command Modes: Global configuration
Reference: Cisco
Menu: Basic Switch Configuration Menu -> Forwarding Database->
Set Age-Out time

Example:

```
! Set Age-Out time 300 sec
Switch# mac-address-table aging-time 300
Switch(config)#
```

show mac-address-table aging-time

Use the show mac-address-table aging-time command to display MAC address table.

show mac-address-table aging-time

Syntax Description: The show mac-address-table aging-time command has no arguments or keywords.
Default Value: This command has no default setting.
Command Modes: Privileged EXEC
Reference: Cisco
Menu: Basic Switch Configuration Menu -> Forwarding Database Menu

Example:

```
Switch# show mac-address-table aging-time

Aging time: 300 Sec(s)

Switch(config)#
```

show mac-address-table mac

Use the show mac-address-table mac command to list MAC addresses by individual MAC address.

show mac-address-table mac

SYNTAX DESCRIPTION: The show mac-address-table mac command has no arguments or keywords.

DEFAULT VALUE: The show mac-address-table mac command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE: Cisco

MENU: Basic Switch Configuration Menu -> Forwarding Database Menu

EXAMPLE:

```
Switch# show mac-address-table mac

 MAC Address          Port
 -----------------    --------------------
 00:30:AB:00:09:20    CPU
 00:30:AB:00:09:21    26
 00:30:AB:00:09:22    26
 00:30:AB:00:09:23    26
 00:30:AB:00:09:24    26?

Switch#
```

show mac-address-table interface

Use the show mac-address-table interface command to display the MAC address table by port.

show mac-address-table interface *<port>*

SYNTAX DESCRIPTION: *<port>* Port instance.

DEFAULT VALUE: The show mac-address-table interface command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE: Cisco

MENU: Basic Switch Configuration Menu -> Forwarding Database Menu

EXAMPLE:

```
Switch# show mac-address-table interface fastethernet0/26

 MAC Address           Port
 -----------------     --------------------
 00:30:AB:00:09:20     26
 00:30:AB:00:09:21     26
 00:30:AB:00:09:22     26
 00:30:AB:00:09:23     26
 00:30:AB:00:09:24     26?

Switch#
```

show mac-address-table vlan

Use the show mac-address-table vlan command to display the MAC address table by VLAN.

show mac-address-table vlan *<vlanID>*

SYNTAX DESCRIPTION: *<vlanID>* VLAN ID.

DEFAULT VALUE: The show mac-address-table vlan command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE: Cisco

MENU: Basic Switch Configuration Menu -> Forwarding Database Menu

EXAMPLE:

```
Switch# show mac-address-table vlan 1
 MAC Address           Port
 -----------------     -------------------
 00:30:AB:00:09:21     26
 00:30:AB:00:09:22     26
 00:30:AB:00:09:23     26
 00:30:AB:00:09:24     26

Switch#
```

show mac-address-table static

Use the show mac-address-table static command to display the MAC address table by static.

show mac-address-table static

Syntax Description: The c command has no arguments or keywords.
Default Value: The command has no default setting.
Command Modes: Privileged EXEC
Reference: None.
Menu: Basic Switch Configuration Menu -> Forwarding Database Menu

Example:

```
Switch# show mac-address-table static

MAC Address          Port    VLAN ID
---------------------    ---------------------
00:00:A0:21:00:11    2       2

Switch#
```

5.11 Multiple Spanning Tree Commands

spanning-tree mst

Use the spanning-tree mst command to enable or disable multiple spanning tree.

spanning-tree mst enable
spanning-tree mst disable

Syntax Description: The spanning-tree mst command has no arguments or keywords.
Default Value:
Command Modes: Global configuration
Reference:
Menu:

Example:

```
!Enable MSTP
Switch(config)# spanning-tree mst
Switch(config)#
```

```
!Disable MSTP
Switch(config)# no spanning-tree mst
Switch(config)#
```

spanning-tree mst name

Use the spanning-tree mst name command to configure the MSTP region name.

spanning-tree mst name *<name>*

Syntax Description: *<name>* Region name
Default Value:
Command Modes: Global configuration
Reference:
Menu:

EXAMPLE:

```
!Cnfigure the MSTP name “Symbol”
Switch(config)# spanning-tree mst name Symbol
Switch(config)#
```

spanning-tree mst revision

Use the spanning-tree mst revision command to configure the mst revision number.

spanning-tree mst revison *<revision>*

SYNTAX DESCRIPTION: *<priority>* Integer ranges from 0 to 65535

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE:

MENU:

EXAMPLE:

```
!Cnfigure the MSTP revision 4096
Switch(config)# spanning-tree mst revision 4096
Switch(config)#
```

spanning-tree mst version

Use the spanning-tree mst version command to configure the spanning-tree version of the bridge.

spanning-tree mst version *<ver>*

SYNTAX DESCRIPTION: *<ver>*

Ver	*Meaning*
stpCompatible	STP Compatible
rstp	RSTP Version
mstp	MSTP Version

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE:

Menu:

Example:

```
!Set STP Compatible
Switch(config)# spanning-tree mst version stpCompatible
Switch(config)#
```

spanning-tree mst max-hops

Use the spanning-tree mst max-hops command to configure the maximum hops count.

spanning-tree mst max-hops*<hop>*

Syntax Description: *<hop>* Integer ranges from 6 to 40
Default Value:
Command Modes: Global configuration
Reference:
Menu:

Example:

```
!Set Max Hop 40
Switch(config)# spanning-tree mst max-hops 40
Switch(config)#
```

spanning-tree mst priority

Use the spanning-tree mst priority command to configure the CIST bridge priority value.

spanning-tree mst priority *<priority>*

Syntax Description: *<priority>* Valid priority vales are: 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440. All other values are rejected.
Default Value: 0x8000
Command Modes: Global configuration
Reference:
Menu:

EXAMPLE:

```
!Set CIST priority 40960
Switch(config)# spanning-tree mst priority 40960
Switch(config)#
```

spanning-tree mst max-age

Use the spanning-tree mst max-age command to configure the value of CIST bridge Max Age.

spanning-tree mst max-age *<seconds>*

SYNTAX DESCRIPTION: *<seconds>* Integer ranges from 6 to 40 and enforces the following relationships
2* *(Bridge _Forward_Delay* - 1.0 *seconds) >=Bridge_Max_Age*
Bridge_Max_Age>=2* (*Bridge_Hello_Time* + 1.0 *seconds*)
From 2* (*Bridge_Forward_Delay* -1) to 2* (*Bridge_Hello_Time* + 1)

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE:

MENU:

EXAMPLE:

```
!set CIST Max Age 20 seconds
Switch(config)# spanning-tree mst max-age 20
Switch(config)#
```

spanning-tree mst hello-time

Use the spanning-tree mst hello time command to configure the value of the CIST bridge Hello Time.

spanning-tree mst hello-time *<seconds>*

SYNTAX DESCRIPTION: *<seconds>* Integer ranges from 1 to 10 nd enforces the following relationships
2* *(Bridge _Forward_Delay* - 1.0 *seconds) >=Bridge_Max_Age*
Bridge_Max_Age>=2* (*Bridge_Hello_Time* + 1.0 *seconds*)
From 1 to (*Bridge_Max_Age* / 2) - 1

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE:

MENU:

EXAMPLE:

```
!set CIST Hello Time 5 seconds
Switch(config)# spanning-tree mst hello-time 5
Switch(config)#
```

spanning-tree mst forward-time

Use the spanning-tree mst forward time command to configure the CIST bridge Forward Time value.

spanning-tree mst forward-time *<seconds>*

SYNTAX DESCRIPTION: *<seconds>* Integer ranges from 4 to 30 and enforces the following relationships
2* *(Bridge _Forward_Delay* - 1.0 *seconds) >=Bridge_Max_Age*
Bridge_Max_Age>=2* (*Bridge_Hello_Time* + 1.0 *seconds*)
From (*Bridge_Max_Age /* 2) + 1 to 30

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Set Forward Time 12 seconds
Switch(config)# spanning-tree mst forward-time 12
Switch(config)#
```

spanning-tree mst instance priority

Use the spanning-tree mst instance priority command to configure the bridge priority instance value.

spanning-tree mst *<instance>* priority *<priority>*

SYNTAX DESCRIPTION: *<priority>* Integer ranges from 1 to 64
Valid priority vales are: 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440. All other values are rejected.

DEFAULT VALUE:

COMMAND MODES: Global configuration

REFERENCE:

MENU:

EXAMPLE:

```
!Set bridge priority 4096 for instance 2
Switch(config)# spanning-tree mst 2 priority 4096
Switch(config)#
```

spanning-tree mst instance vlan

Use the spanning-tree mst instance vlan command to map vlans to instances.

spanning-tree mst instance*<instance-id>* vlan*<vlan-range>*

SYNTAX DESCRIPTION:	*<instance>*	Integer ranges from 1 to 64
	<vlan-range>	Integer ranges from 0 to 4096
DEFAULT VALUE:		
COMMAND MODES:	Global configuration	
REFERENCE:		
MENU:		

EXAMPLE:

```
!Set Vlan 2-5 to instance 2
Switch(config)# spanning-tree mst instance 2 vlan 2-5
Switch(config)#
```

spanning-tree mst shutdown

Use the spanning tree mst shutdown command for Enabling/Disabling MSTP interface function.

spanning-tree mst shutdown

SYNTAX DESCRIPTION:	The spanning-tree mst shutdown command has no arguments or keywords.
DEFAULT VALUE:	
COMMAND MODES:	Interface configuration
REFERENCE:	
MENU:	

EXAMPLE:

```
! Enable MSTP on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# no spanning-tree mst shutdown
Switch(config-if)#
```

```
! Disable MSTP on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst shutdown
Switch(config)#
```

spanning-tree mst port-priority

Use the spanning-tree mst port priority command to configure CIST Port Priority.

spanning-tree mst port-priority *<priority>*

SYNTAX DESCRIPTION: *<priority>* Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.

DEFAULT VALUE:

COMMAND MODES: Interface configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Set CIST port priority 64 on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst port-priority 64
Switch(config-if)#
```

spanning-tree mst cost

Use the spanning-tree mst cost command to configure the CIST Port Path Cost.

spanning-tree mst cost *<cost>*

SYNTAX DESCRIPTION: *<cost>* Integer ranges from 1 to 200000000, 0 for auto detect

DEFAULT VALUE:

COMMAND MODES: Interface configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Set CIST port path cost 4000 on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst cost 4000
Switch(config-if)#
```

spanning-tree mst init-migration

Init Protocol Migration on the Port in MSTP.

spanning-tree mst init-migration

SYNTAX DESCRIPTION: The spanning-tree mst init-migration command has no arguments or keywords.

DEFAULT VALUE:

COMMAND MODES: Interface configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Restart Migration on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst init-migration
Switch(config-if)#
```

spanning-tree mst edgeport

Use the spanning-tree mst edgeport command to configure the Edge Port Status in MSTP.

spanning-tree mst edgeport

SYNTAX DESCRIPTION: The spanning-tree mst edgeport command has no arguments or keywords.

DEFAULT VALUE:

COMMAND MODES: Interface configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Set Edge port TRUE on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst edgeport
Switch(config-if)#
```

```
! Set Edge port FALSE on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# no spanning-tree mst edgeport
Switch(config-if)#
```

spanning-tree mst point-to-point

Use the spanning-tree mst point-to-point command to configure the Point-To-Point Status of a Port in MSTP.

spanning-tree mst point-to-point *<status>*

SYNTAX DESCRIPTION: *<status>*

Status	*Meaning*
forcetrue	Force TRUE
forcefalse	Force FALSE
auto	Auto detection

Default Value:
Command Modes: Interface configuration
Reference:
Menu:

Example:

```
! Force p2p false on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst point-to-point forcefalse
Switch(config-if)#
```

spanning-tree mst instance shutdown

Use the spanning-tree mst instance shutdown command to Enable/Disable MSTP function on the interface.

spanning-tree mst instance *<instance>* shutdown

Syntax Description: Integer ranges from 1 to 64
Default Value:
Command Modes: Interface configuration
Reference:
Menu:

Example:

```
! Enable MSTP on port 4 for instance 5
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst 5 shutdown
Switch(config-if)#
```

```
! Disable MSTP on port 4 for instance 5
Switch(config)# interface fastethernet0/4
Switch(config-if)# no spanning-tree mst 5 shutdown
Switch(config-if)#
```

spanning-tree mst instance port-priority

Use the spanning-tree mst instance port-priority command to configure instance Port Priority.

spanning-tree mst instance*<instance-id>* port-priority *<priority>*

SYNTAX DESCRIPTION: *<instance>* Integer ranges from 0 to 64
<priority> Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.

DEFAULT VALUE:

COMMAND MODES: Interface configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Set CIST port priority 64 on port 4 for instance 8
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst 8 port-priority 64
Switch(config-if)#
```

spanning-tree mst instance cost

Use the spanning-tree mst instance cost command to configure instance Port Path Cost.

spanning-tree mst *<instance>* cost *<cost>*

SYNTAX DESCRIPTION: *<instance>* Integer ranges from 1 to 64
<cost> Integer ranges from 1 to 200000000, 0 for auto detect

DEFAULT VALUE: auto.

COMMAND MODES: Interface configuration

REFERENCE:

MENU:

EXAMPLE:

```
! Set CIST port path cost 1000 on port 4 for instance 8
Switch(config)# interface fastethernet0/4
Switch(config-if)# spanning-tree mst 8 cost 1000
Switch(config-if)#
```

show spanning-tree mst configuration

Use the show spanning-tree mst configuration command to display the MSTP configuration.

show spanning-tree mst configuration

SYNTAX DESCRIPTION: The show spanning-tree mst configuration command has no arguments or keywords.

DEFAULT VALUE: The show spanning-tree mst configuration command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show spanning-tree mst configuration

Global MSTP Status        : Enabled
Protocol Version          : STP-Compatible
MST Config ID Selector    : 0
MST Configuration Name    : 00:00:00:00:00:00
MST Revision Level        : 65522
MST Config Digest         : 50010946d0ec116e865b8bc85d6c0d7b


Instance Vlans mapped
-------- --------------------------------------------------------------
2       3
3       2
4       4
5       5
6       6
7       7

Switch#
```

show spanning-tree mst cist configuration

Use this command to display the MSTP CIST configuration.

show spanning-tree mst cist configuration

SYNTAX DESCRIPTION: The show spanning-tree mst cist configuration command has no arguments or keywords.

DEFAULT VALUE: The show spanning-tree mst cist configuration command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show spanning-tree mst cist configuration
Cist Root Port:          8             Time Since Topology Change: 1730  Sec.
Cist Root Path Cost:     2000000       Topology Change Count:     10
Cist Root:         1000  000629328140
Cist Regional Root Cost: 0             Cist Bridge ID:   8000 000a0a0a0a01
Cist Regional Root: 1000 000629328140  Cist Bridge Hello Time:    2    Sec.
                                       Cist Bridge Maximum Age:   20   Sec.
Cist Hello Time:         2   Sec.      Cist Bridge Forward Delay: 15   Sec.
Cist Maximum Age:        20  Sec.      Max Hop Count:             40   Sec.
Cist Forward Delay:      15  Sec.
     :
Switch#
```

show spanning-tree mst cist interface

Use this command to display MSTP CIST configuration information for interface.

show spanning-tree mst cist interface *<port list>*

SYNTAX DESCRIPTION: *<port list>* A list of port instances

DEFAULT VALUE: The show spanning-tree mst cist interface command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show spanning-tree mst cist interface all
Port:               1                  CIST Port Status:    Enabled
Link:               Up                 Trunk:               -
CIST Admin/OperEdge:False/False        CIST Admin/OperPtoP: Auto /False
CIST Migration:     Flase
CIST Port state:    forwarding          CIST Port Priority:  128
CIST Port Role:     Designated         CIST Port Path Cost: 2000000
CIST Desig. Root:   8000 000629328140  CIST Desig. Cost:    2000000
CIST Desig. Bridge: 8000 000629328140  CIST Desig. Port:    80 01
CIST Port Regional Root:               80:00:00:00:00:00:00:01
Cist Port Regional PathCost:           0

Port:               2                  CIST Port Status:    Enabled
Link:               Up                 Trunk:               -
CIST Admin/OperEdge:False/False        CIST Admin/OperPtoP: Auto /False
CIST Migration:     MSTP
CIST Port state:    orwarding          CIST Port Priority:  128
CIST Port Role:     Designated         CIST Port Path Cost: 2000000
CIST Desig. Root:   8000 000629328140  CIST Desig. Cost:    2000000
CIST Desig. Bridge: 8000 000629328140  CIST Desig. Port:    80 01
CIST Port Regional Root:               80:00:00:00:00:00:00:01
CIST Port Regional PathCost:           0
         :
Switch#
```

show spanning-tree mst instance configuration

Use this command to display MSTP CIST configuration.

show spanning-tree mst *<instance>* configuration

SYNTAX DESCRIPTION: *<instance>* Integer ranges from 1 to 64

DEFAULT VALUE: The show spanning-tree mst instance configuration command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show spanning-tree mst 5 configuration

Msti Root Port: 0                  Time Since Topology Change: 3069 Sec.
Msti Root Cost: 0                  Topology Change Count       0
Msti Regional Root: 8000 00403312aa0e  Msti Bridge ID:     8000 00403312aa0e

Switch#
```

show spanning-tree mst instance interface

Use this command to display MSTP CIST configuration information for interface.

show spanning-tree mst *<instance>* interface *<port list>*

SYNTAX DESCRIPTION: *<instance>* Integer ranges from 1 to 64

<port list> A list of port instances

DEFAULT VALUE: The show spanning-tree mst instance interface command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show spanning-tree mst 2 interface all
Mst Instance:   2
Port:           2                       Port Status:    Enabled
Link:           Up                      Trunk:          -
Port state:     Forwarding              Port Priority:  128
Port Role:      Designated              Port Path Cost: 2000000
Desig. Root:    8000 000629328140       Desig. Cost:    2000000
Desig. Bridge:  8000 000629328140       Desig. Port:    80 01

Mst Instance:   2
Port:           5                       Port Status:    Enabled
Link:           Up                      Trunk:          -
Port state:     Forwarding              Port Priority:  128
Port Role:      Designated              Port Path Cost: 2000000
Desig. Root:    8000 000629328140       Desig. Cost:    2000000
Desig. Bridge:  8000 000629328140       Desig. Port:    80 01

Switch#
```

5.12 IGMP Snooping Commands

ip igmp snooping

Use the ip igmp snooping command to enable or disable IGMP snooping as implemented in the system.

ip igmp snooping
no ip igmp snooping

Syntax Description: The ip igmp snooping command has no argument.

Default Value: The feature is disabled by default.

Command Modes: Global configuration

Reference: Cisco

Menu: Advanced Switch Configuration Menu->IGMP Snooping->Enable/Disable IGMP Snooping

Example:

```
!Enable igmp snooping
Switch(config)# ip igmp snooping
Switch(config)#
```

```
!Disable igmp snooping
Switch(config)# no ip igmp snooping
Switch(config)#
```

ip igmp snooping aging-time

Use this command to configure the router and host port aging time for an IGMP snooping operation.

ip igmp snooping aging-time *{router | host} <sec>*

Syntax Description: The router port aging time is integer value ranges from 60 to 600.
The host port aging time is integer value ranges from 130 to 1225.

Default Value: The default value is 260 seconds for the host port, and 125 seconds for the router port.

Command Modes: Global configuration

Reference: None

MENU: Advanced Switch Configuration Menu->IGMP Snooping->Set Host Port Aged Tim, Set Router Port Aged Time

EXAMPLE:

```
!Enable igmp snooping router port age out time 300 sec
Switch(config)# ip igmp snooping aging-time router 300
Switch(config)#
```

```
!Enable igmp snooping host port age out time 300 sec
Switch(config)# ip igmp snooping aging-time host 300
Switch(config)#
```

ip igmp snooping report-forward-interval

Use this command to configure the forward interval of IGMP report message to a router port for IGMP snooping operation.

An IGMP report for same group won't forward during this interval.

ip igmp snooping report-forward-interval *<sec>*

SYNTAX DESCRIPTION: Integer value ranges from 0 to 25.
DEFAULT VALUE: The default value is 5 seconds.
COMMAND MODES: Global configuration
REFERENCE: None
MENU: Advanced Switch Configuration Menu->IGMP Snooping->
Set Report Interval

EXAMPLE:

```
!Enable igmp snooping report forward interval 10 sec
Switch(config)# ip igmp snooping report-forward-interval 10
Switch(config)#
```

ip igmp snooping vlan-filter vlan

Use this command to filter IGMP snooping on a specific interface in the system.

ip igmp snooping vlan-filter vlan *<vlanID>*

SYNTAX DESCRIPTION: *<vlanID>* VLAN ID

DEFAULT VALUE: The feature is disabled by default.

COMMAND MODES: Global configuration

REFERENCE: None

MENU: Advanced Switch Configuration Menu->IGMP Snooping->
Show VLAN Filter Table->Set Vlan Filter

EXAMPLE:

```
!Filt igmp snooping on vlan1
Switch(config)# ip igmp snooping vlan-filter vlan 1
Switch(config)#
```

```
!Filt igmp snooping on vlan1
Switch(config)# no ip igmp snooping vlan-filter vlan 1
Switch(config)#
```

show ip igmp snooping conf

Use this command to display IGMP snooping information.

show ip igmp snooping conf

SYNTAX DESCRIPTION: This command has no arguments or keywords.

DEFAULT VALUE: This command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE: Cisco.

MENU: Advanced Switch Configuration Menu -> IGMP Configuration Menu

EXAMPLE:

```
Switch# show ip igmp snooping conf

IGMP Snooping Status      : Enabled
Host Port Age-Out Time    : 260 sec
Router Port Age-Out Time  : 300 sec
Report Forward Interval   : 10 sec

Switch#
```

show mac-address-table multicast

Use this command to display Layer2 multicast entries information for VLAN.

show mac-address-table multicst

SYNTAX DESCRIPTION: This command has no arguments or keywords.
DEFAULT VALUE: This command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Cisco.
MENU: Advanced Switch Configuration Menu -> IGMP Configuration Menu

EXAMPLE:

```
Switch# show mac-address-table multicast

VLAN ID  Group MAC Address  Group Members
-------  -----------------  -------------

Switch#
```

show ip igmp snooping mrouter

Use this command to display multicast router port information for VLAN.

show ip igmp snooping mrouter

SYNTAX DESCRIPTION: This command has no arguments or keywords.
DEFAULT VALUE: This command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Cisco.
MENU: Advanced Switch Configuration Menu -> IGMP Configuration Menu -> Show Router Port table Menu

EXAMPLE:

```
Switch# show ip igmp snooping mrouter

VLAN ID  Port List
-------  ----------------------------------------------------------------

Switch#
```

show ip igmp snooping vlan-filter-table

Use this command to display IGMP Snooping VLAN filter information.

show ip igmp snooping vlan-filter-table

SYNTAX DESCRIPTION: This command has no arguments or keywords.
DEFAULT VALUE: This command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: None

MENU: Advanced Switch Configuration Menu -> IGMP Configuration Menu -> Show Router Port Table Menu

EXAMPLE:

```
Switch# show ip igmp vlan-filter-table

VLAN ID  Port List
-------  ---------------------------------------------------------------
1        Filtered

Switch#
```

5.13 VLAN Commands

vlan init

Use the vlan init command to remove all vlans and reset ports to default VLAN

vlan init

SYNTAX DESCRIPTION:	The vlan init command has no arguments or keywords
DEFAULT VALUE:	This command has no default setting.
COMMAND MODES:	Global configuration
REFERENCE:	
MENU:	Advanced Switch Configuration Menu->IGMP Snooping-> Enable/Disable IGMP Snooping

EXAMPLE:

```
!remove all vlan.
Switch(config)# vlan init
Switch(config)#
```

Name
member

Use the member command to create a new VLAN or modify an existing one in the system.

interface *<vlanID>*

name *<name>*

member *<port list>*

SYNTAX DESCRIPTION:	*<vlanID>*	VLAN ID
	<name>	VLAN name
	<port list>	A list of port instances
COMMAND MODES:	Interface configuration	
REFERENCE:	None	
MENU:	Advanced Switch Configuration Menu->VLAN Management-> Create VLAN Set VLAN ID VLAN Name Select Port Member	

EXAMPLE:

```
! create a 802.1Q vlan untag port 1-5, 10, 15-19
Switch(config)# interface vlan3
Switch(config-if)# name VLAN-3
Switch(config-if)# member 1-5,10,15-19
Switch(config-if)#
```

```
! modify participation (remove 10, 15-19)
Switch(config)# interface vlan3
Switch(config-if)# member 1-5
Switch(config-if)#
```

forbidden

Use the forbidden command to create a new VLAN or modify an existing one in the system.

interface *<vlanID>*

forbidden *<port list>*

SYNTAX DESCRIPTION:	*<vlanID>*	VLAN ID
	<port list>	A list of port instances
COMMAND MODES:	Interface configuration	
REFERENCE:	None	
MENU:	Advanced Switch Configuration Menu->VLAN Management-> Create VLAN Set VLAN ID VLAN name Select Port Member	

EXAMPLE:

```
! Set port 6-7 to Forbidden on vlan 3
Switch(config)# interface vlan 3
Switch(config-if)# forbidden 6-7
Switch(config-if)#
```

management

Use the management command to remove a port member from a VLAN.

interface *<vlanID>*

management

Syntax Description:	*<vlanID>*	VLAN ID
Command Modes:	Interface configuration	
Reference:	Cisco	
Menu:		

Example:

```
! Set Vlan3 management
Switch(config)# interface vlan3
Switch(config-if)# management
Switch(config-if)#
```

no interface

Use the no interface command to delete a VLAN in the system.

no interface *<vlanID>*

Syntax Description:	*<vlanID>*	VLAN ID
Command Modes:	Global configuration	
Reference:	None	
Menu:	Advanced Switch Configuration Menu->VLAN Management-> Delete VLAN	

Example:

```
! delete vlan3
Switch(config)# no interface vlan3
Switch(config)#
```

PVID

Use the PVID command to configure a PVID on a port.

PVID *<vlanID>*

Syntax Description:	*<vlanID>*	VLAN ID
Command Modes:	Interface configuration	
Reference:	None	
Menu:		

Example:

```
! Set port 2 PVID 3
Switch(config)# interface fastethernet0/2
Switch(config-if)# PVID 3
Switch(config-if)#
```

frame-type

Use the frame-type command to configure the frame type on a port.

frame-type *<type>*

Syntax Description:	*<type>*	all - admit all packets tag-only - tagged packets only
Command Modes:	Interface configuration	
Reference:	None	
Menu:		

Example:

```
! Set port 2 frame type admit all
Switch(config)# interface fastethernet0/2
Switch(config-if)# frame-type all
Switch(config-if)#
```

show vlan

Use the show-vlan command to display VLAN information.

show vlan *<vlanID>*

SYNTAX DESCRIPTION: *<vlanID>* VLAN ID.
DEFAULT VALUE: The show vlan command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Foundry
MENU: Advanced Switch Configuration -> VLAN Management Menu

EXAMPLE:

```
Switch# show vlan all

VLAN Name                          Type       Mgmt    Ports
---- ----------------------------- ---------  ------------------------
1    Default VLAN                  Permanent  UP      Fa1, Fa2, Fa3, Fa4
                                                      Fa5, Fa6, Fa7, Fa8
                                                      Fa9, Fa10, Fa11,
2    VLAN-2                        Static     UP      Fa1, Fa2, Fa3
3    VLAN-3                        Dynamic    DOWN        Fa1, Fa3

Switch#
```

gvrp

Use the gvrp command to enable or disable the GVRP protocol implemented in the system.

gvrp

no gvrp

SYNTAX DESCRIPTION: The gvrp command has no argument.
DEFAULT VALUE: The gvrp feature is disabled by default.
COMMAND MODES: Global configuration
REFERENCE: HP
MENU: Advanced Switch Configuration Menu->VLAN Management->
Set GVRP Status

EXAMPLE:

```
! Enable GVRP
Switch(config)# gvrp
Switch(config)#
```

```
! Disable GVRP
Switch(config)# no gvrp
Switch(config)#
```

show vlan gvrp

Use the show vlan gvrp command to display VLAN information.

show vlan gvrp

SYNTAX DESCRIPTION: *<vlanID>* VLAN ID.

DEFAULT VALUE: The show vlan gvrp command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE: Foundry

MENU: Advanced Switch Configuration -> VLAN Management Menu

EXAMPLE:

```
Switch# show vlan-gvrp
GVRP status is globally disabled
Switch#
```

show vlan port

Use the show vlan port command to display VLAN information.

show vlan port

SYNTAX DESCRIPTION:

DEFAULT VALUE: The show vlan port command has no default setting.

COMMAND MODES: Privileged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show vlan port

Port PVID  Acceptable Frame Type    GVRP
----  ----  ---------------------  ---------
1      1       Admit All         Enabled
2      1       Admit All         Enabled
3      1       Admit All         Enabled
4      1       Admit All         Enabled
5      2       Admit All         Enabled
6      1       Admit All         Enabled
7      1       Admit All         Enabled
8      1       Admit All         Enabled
9      1       Admit All         Enabled

Switch#
```

5.14 Quality of Service Commands

mls qos

Use the mls qos command to enable or disable the QoS implemented in the system.

mls qos
no mls qos

SYNTAX DESCRIPTION: The mls qos command has no argument.
DEFAULT VALUE: The feature is disabled by default.
COMMAND MODES: Global configuration
REFERENCE: Cisco
MENU: Advanced Switch Configuration Menu->Quality of Service->Set Status

EXAMPLE:

```
!Disable Quality of Service
Switch(config)# no mls qos
Switch(config)#
```

```
!Enable Quality of Service
Switch(config)# mls qos
Switch(config)#
```

priority-queue cos-map

Use the priority-queue cos-map command to map the 802.1p traffic class to the port transmitting queues.

priority-queue cos-map *<traffic class> <priority>*

SYNTAX DESCRIPTION: *<priority>* Integer ranges from 0 to 7.
<traffic class> 0 to 3, 0 is lowest, 3 is highest
DEFAULT VALUE:
COMMAND MODES: Global configuration
REFERENCE: Cisco
MENU: Advanced Switch Configuration Menu->Quality of Service->
Set Priority Queue

EXAMPLE:

```
! traffic class(Queue) 1 mapping to Priority 5
Switch(config)# priority-queue cos-map 1 5
Switch(config)#
```

show mls qos

Use the show mls qos command to display QoS information.

show mls qos

SYNTAX DESCRIPTION: The show mls qos command has no arguments or keywords.
DEFAULT VALUE: The show mls qos command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Cisco
MENU: Advanced Switch Configuration Menu -> Quality of Service Configuration Menu

EXAMPLE:

```
Switch# show mls-qos

Quality of Service Status: Disabled

Switch#
```

show priority-queue cos-map

Use this command to display QoS information.

show priority-queue cos-map

SYNTAX DESCRIPTION: The show priority-queue cos-map command has no arguments or keywords.
DEFAULT VALUE: The show priority-queue cos-map command has no default setting.
COMMAND MODES: Privileged EXEC
REFERENCE: Cisco
MENU: Advanced Switch Configuration Menu -> Quality of Service Configuration Menu

EXAMPLE:

```
Switch# show priority-queue cos-map

Pritority Traffic Class
--------- -------------
0            0
1            0
2            2
3            1
4            2
5            2
6            3
7            3

Switch#
```

5.15 Diffserv Commands

diffserv classifier

Use the diffserv classifier command to configure the classifier for diffserv.

diffserv classifier *<index>* [src-mac *<mac>*] [dst-mac *<mac>*] [vlan-id *<vid>*] [dscp *<ds>*] [protocol *<pro>*] [src-ip *<ip>*] [dst-ip *<ip>*] [src-14-port *<port>*] [dst-14-port *<port>*]

no diffserv classifier *<index>*

SYNTAX DESCRIPTION:

<index> Classifier ID for diffserv

<mac> MAC address for classifier

<vid> VLAN ID for classifier

<ds> 6-bits DSCP value in IP header for classifier

<pro> 8-bits Protocol value in IP header for classifier

Protocol name	*Protocol value*
TCP	6
UDP	17
ICMP	1
IGMP	2
RSVP	46

<ip> IP address for classifier

<port> Port number for classifier

DEFAULT VALUE:

COMMAND MODES: Global configuration command

REFERENCE:

MENU:

EXAMPLE:

```
! Create a classifier Index:23, source MAC address: 00:00:01:02:03:04 Vlan
ID is 40
Switch(config)# diffserv classifier 23 src-mac 00:00:01:02:03:04 vlan-id
40
Switch(config)#
```

```
! delete a classifier Index 23
Switch(config)# no diffserv classifier 23
Switch(config)#
```

diffserv inprofile

Use the diffserv inprofile command to configure in-profile action for diffserv.

diffserv inprofile *<index>* [drop | dscp *<ds>* | precedence *<precedence>* | cos *<cos>*]

SYNTAX DESCRIPTION:	*<index>*	In-profile ID for diffserv
	<ds>	6-bits DSCP value in IP header for action
	<precedence>	3-bits TOS-precedence value in IP header for action
	<cos>	3-bits priority value in VLAN TAG for action
DEFAULT VALUE:		
COMMAND MODES:	Global configuration command	
REFERENCE:		
MENU:		

EXAMPLE:

```
! Create a In-profile Index:23 , replace DSCP value to 42
Switch(config)# diffserv inprofile 23 dscp 42
Switch(config)#
```

```
! delete a in-profile Index 23
Switch(config)# no diffserv inprofile 23
Switch(config)#
```

diffserv nomatch

Use the diffserv nomatch command to configure nomatch action for diffserv.

diffserv nomatch *<index>* [drop | policed-dscp *<ds>* | precedence *<precedence>* | cos *<cos>*]

SYNTAX DESCRIPTION:	*<index>*	No-match ID for diffserv
	<ds>	6-bits DSCP value in IP header for action
	<precedence>	3-bits TOS-precedence value in IP header for action
	<cos>	3-bits priority value in VLAN TAG for action
DEFAULT VALUE:		
COMMAND MODES:	Global configuration command	
REFERENCE:		
MENU:		

EXAMPLE:

```
! Create a no-match Index:2 , replace COS value to 3
Switch(config)# diffserv nomatch 2 cos 3
Switch(config)#
```

```
! delete a no-match Index 2
Switch(config)# no diffserv nomatch 2
Switch(config)#
```

diffserv outprofile

Use the diffserv outprofile command to configure the out-profile for diffserv.

diffserv outprofile *<index>* committed-rate*<unit>* burst-size*<volume>* [drop | dscp *<ds>*]

SYNTAX DESCRIPTION:	*<index>*	Out-profile ID for diffserv
	<meter-id>	Meter ID for out-profiler
	<ds>	6-bits DSCP value in IP header for action
DEFAULT VALUE:		
COMMAND MODES:	Global configuration command	
REFERENCE:		
MENU:		

EXAMPLE:

```
! Create a out-profile Index 4, set committed-rate to 23, burst-size 4 and
out-profile action drop.
Switch(config)# diffserv outprofile 4 committed-rate 23 burst-size 4 drop
Switch(config)#
```

```
! delete a out-profile 4
Switch(config)# no diffserv outprofile 4
Switch(config)#
```

diffserv portlist

Use the diffserv portlist command to configure the portlist for diffserv.

diffserv portlist *<index>* *<portlist>*

SYNTAX DESCRIPTION:	*<index>*	Port-list Index for diffserv
	<portlist>	Port-list for diffserv
DEFAULT VALUE:		
COMMAND MODES:	Global configuration command	
REFERENCE:		
MENU:		

EXAMPLE:

```
! Create a portlist Index 5, set port 3-7 .
Switch(config)# diffserv portlist 5 3-7
Switch(config)#
```

```
! delete a port-list 5
Switch(config)# no diffserv portlist 5
Switch(config)#
```

diffserv policy

Use the diffserv policy command to configure the policy for diffserv.

diffserv policy *<index>* portlist *<portlist-index>* classifier *<classifier-index>*
policy-recedence *<value>*
[inprofile *<inprofile-index>*nomatch *<nomatch-index>* outprofile *<outprofile-index>*]

SYNTAX DESCRIPTION:	*<index>*	policy Index for diffserv
	<portlist-index>	Port-list Index for policy
	<classifier-index>	classifier Index for policy
	<value>	policy-recedence value for policy (1-65535)
	<inprofile-index>	In-profile Index for policy
	<nomatch-index>	No-match Index for policy
	<outprofile-index>	Out-profile Index for policy

DEFAULT VALUE:

COMMAND MODES: Global configuration command

REFERENCE:

MENU:

EXAMPLE:

```
! Create a policy Index 5, precedence 100, classifier Index 4,
in-profile Index 5, Portlist Index 3
Switch(config)# diffserv policy 5 policy-precedence 100 classifier 4
inprofile 5 portlist 3
Switch(config)#
```

```
! delete a policy Index 5
Switch(config)# no diffserv policy 5
Switch(config)#
```

show diffserv classifier

Use the show diffserv classifier command to display diffserv classifier information.

show diffserv classifier

SYNTAX DESCRIPTION: The show diffserv classifier command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# show diffserv classifier all

Classifier Index : 23
Source IP Addr   : Ignore            Dest IP Addr      : Ignore
Source MAC Addr  : 00:00:01:02:03:04 Dest MAC Addr     : Ignore
Source L4 Port   : Ignore            Dest L4 Port      : Ignore
DSCP             : Ignore            Protocol          : Ignore
VLAN ID          : 40

Switch#
```

show diffserv inprofile

Use the diffserv inprofile command to display the diffserv in-profile information.

show diffserv inprofile

SYNTAX DESCRIPTION: The show diffserv inprofile command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# show diffserv inprofile

In-Profile Action:
Index        Action           Value
------------------------------------
23     policed-dscp          42

Switch#
```

show diffserv outprofile

Use the show diffserv outprofile command to display diffserv out-profile information.

show diffserv outprofile

SYNTAX DESCRIPTION: The show diffserv outprofile command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

show diffserv portlist

Use the show diffserv portlist command to display diffserv portlist information.

show diffserv portlist

SYNTAX DESCRIPTION: The show diffserv portlist command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# show diffserv portlist

Portlist:

Index Portlist
----- --------------------------------------------------------------
5     3-7

Switch#
```

show diffserv policy

Use the show diffserv policy command to display diffserv policy information.

show diffserv policy [*<index>*]

SYNTAX DESCRIPTION: The show diffserv policy command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# show diffserv policy all

Policy :

Index Classifier Precedence In-Profile No-Match Out-Profile PortList Status -
---- ---------- ---------- ---------- -------- ----------- -------- -------
22      23        100         23         2          3           5    Enable

Switch#
```

```
Switch# show diffserv policy 22

Policy

Index     : 22
Classifier Index : 23
Source IP Addr   : Ignore              Dest IP Addr       : Ignore
Source MAC Addr  : 00:00:01:02:03:04  Dest MAC Addr      : Ignore
Source L4 Port   : Ignore              Dest L4 Port       : Ignore
DSCP             : Ignore              Protocol           : Ignore
VLAN ID          : 40
Policy Precedence: 100
In-Profile Index : 23                  In-Profile Action  : policed-dscp-42
No-Match Index   : 2                   No-Match Action    : policed-cos-3
Out-Profile Index: 3                   Out-Profile Action : drop
Committed Rate   : 3                   Burst Size         : 4 KB
PortList Index   : 5                   PortList           : 3-7

Switch#
```

show diffserv policy prcedence port

Use this command to show diffserv policy precedence by port information.

show diffserv policy-precedence port*<port num>* [sort *index/precedence*]

SYNTAX DESCRIPTION: The command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Privileged EXEC
REFERENCE:
MENU:

EXAMPLE:

```
Switch# show diffserv policy-precedence port 5 sort precedence

Selected Port Number: 5

Precedence     Policy Index
------------   ------------
100             22
Switch# show diffserv policy-precedence port 5 sort policy-index

Selected Port Number: 5

Policy Index   Precedence
------------   ------------
22            100

Switch#
```

5.16 802.1x Commands

dot1x radius

Use the dot1x nas-id command to set 802.1x admin status.

dot1x radius *<NASID>*

Syntax Description: *<NASID>* String, ID for dot1x request to Radius server.
Default Value:
Command Modes: Global configuration
Reference:
Menu:

Example:

```
! NAS ID "dot1x_auth"
Switch(config)# dot1x radius dot1x_auth
Switch(config)#
```

dot1x port-control

Use the dot1x port-control command to set 802.1x port control status.

dot1x port-control <control>

Syntax Description:	*<control>*	auto	The controlled Port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server.
		force-authorized	The controlled Port is required to be held in the Authorized state.
		force-unauthorized	The controlled Port is required to be held in the Unauthorized state.

Default Value:
Command Modes: Interface configuration

REFERENCE: Cisco
MENU:

EXAMPLE:

```
! set port-control auto on port 5
Switch(config)# interface fastethernet0/5
Switch(config-if)# dot1x port-control auto
Switch(config)#
```

dot1x re-authentication

Use the dot1x re-authentication command to set 802.1x port re-authentication.

dot1x re-authentication

no dot1x re-authentication

SYNTAX DESCRIPTION: The dot1x re-authentication command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Interface configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! Enable re-authentication on port 7
Switch(config)# interface fastethernet0/7
Switch(config-if)# dot1x authentication
Switch(config-if)#
```

```
! Disable re-authentication on port 7
Switch(config)# interface fastethernet0/7
Switch(config-if)# no dot1x authentication
Switch(config-if)#
```

dot1x timeout re-authperiod

Use this command to set the number of seconds between re-authentication attempts. The command affects the behavior of the switch only if periodic re-authentication is enabled.

dot1x timeout re-authperiod *<minute>*

Syntax Description: *<minute>* Set the number of minutes
Default Value:
Command Modes: Interface configuration
Reference: Cisco
Menu:

Example:

```
! Set re-authentication time 2 min on port 7
Switch(config)# interface fastethernet0/7
Switch(config-if)# dot1x timeout re-authperiod 30
Switch(config-if)#
```

dot1x timeout supp-timeout

Use this command to set the number of seconds for the timeout value.

dot1x timeout supp-timeout *<second>*

Syntax Description: *<second>* Set the number of seconds
Default Value:
Command Modes: Interface configuration
Reference: Cisco
Menu:

Example:

```
! Set supp-timeout 60 sec on port 7
Switch(config)# interface fastethernet0/7
Switch(config-if)# dot1x timeout supp-timeout 60
Switch(config-if)#
```

dot1x timeout quiet-period

Use this command to set the number of seconds the switch remains in quiet state following a failed authentication exchange with the client.

dot1x timeout quiet-period *<second>*

SYNTAX DESCRIPTION:	*<second>*	Set the number of seconds
DEFAULT VALUE:		
COMMAND MODES:	Interface configuration	
REFERENCE:	Cisco	
MENU:		

EXAMPLE:

```
! Set quiet period time 60 sec on port 7
Switch(config)# interface fastethernet0/7
Switch(config-if)# dot1x timeout quiet-period 60
Switch(config-if)#
```

dot1x timeout server

Use this command to set the number of seconds the switch waits for a response to a RADIUS frame.

dot1x timeout server *<second>*

SYNTAX DESCRIPTION:	*<second>*	Set the number of seconds
DEFAULT VALUE:		
COMMAND MODES:	Interface configuration	
REFERENCE:	Cisco	
MENU:		

EXAMPLE:

```
! Set transmit time 10 sec on port 3
Switch(config)# interface fastethernet0/3
Switch(config-if)# dot1x timeout server 10
Switch(config-if)#
```

dot1x timeout tx-period

Use this command to set the number of seconds the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.

dot1x timeout tx-period *<second>*

SYNTAX DESCRIPTION:	*<second>*	Set the number of seconds
DEFAULT VALUE:		
COMMAND MODES:	Interface configuration	
REFERENCE:	Cisco	
MENU:		

EXAMPLE:

```
! Set transmit time 60 sec on port 3
Switch(config)# interface fastethernet0/3
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)#
```

dot1x max-req

Use the dot1x max-req command to set the number of times the switch sends an EAP-request/identity frame to the client before restarting the authentication process.

dot1x max-req *<count>*

SYNTAX DESCRIPTION:	*<count>*	Set the number of times
DEFAULT VALUE:		
COMMAND MODES:	Interface configuration	
REFERENCE:	Cisco	
MENU:		

EXAMPLE:

```
! Set request times 4 on port 3
Switch(config)# interface fastethernet0/3
Switch(config-if)# dot1x max-req 4
Switch(config-if)#
```

dot1x re-authenticate

Use this command to re-authenticate on an 802.1X-authorized port.

dot1x re-authenticate

SYNTAX DESCRIPTION: The dot1x re-authenticate command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Interface configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! re-authenticate on port 3 now
Switch(config)# interface fastethernet0/3
Switch(config-if)# dot1x re-authenticate
Switch(config-if)#
```

dot1x init

Use the dot1x init command to display (initiate) status on an 802.1X-authorized port.

dot1x init

SYNTAX DESCRIPTION: The dot1x init command has no arguments or keywords.
DEFAULT VALUE:
COMMAND MODES: Interface configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! init on port 3
Switch(config)# interface fastethernet0/3
Switch(config-if)# dot1x init
Switch(config-if)#
```

dot1x control-direction

Use the dot1x control-direction command to impose dot1x authentication on either incoming or outgoing traffic.

dot1x control-direction *<direction>*

SYNTAX DESCRIPTION:	*<direction>*	*both*	The dot1x authentication is imposed only on the incoming traffic
		in	The dot1x authentication is imposed on incoming and outgoing traffic

COMMAND MODES: Interface configuration
REFERENCE: Cisco
MENU:

EXAMPLE:

```
! Set Control direction Both on port 5
Switch(config)# interface fastethernet0/5
Switch(config-if)# dot1x control-direction both
Switch(config-if)#
```

show dot1x

show dot1x *<port-list>*

SYNTAX DESCRIPTION: *<port-list>* Port list

DEFAULT VALUE:

COMMAND MODES: Privileged EXEC

REFERENCE: Cisco

MENU:

EXAMPLE:

```
Switch# show dot1x 1-2

NAS ID : dot1x_auth

Port No : 1
Port Status        : Authorized        OperControlDirection  : Both
Port Control       : Force Authorized  AdminControlDirection : Both
Quiet Period      : 60   seconds    Transmission Period   : 30   seconds
Supplicant Timeout : 30   seconds    Server Timeout       : 30   seconds
Maxumum Request    : 2              Re-auth Period       : 60   minutes
Re-auth Status     : Disabled

Port No : 2
Port Status        : Authorized        OperControlDirection  : Both
Port Control       : Force Authorized  AdminControlDirection : Both
Quiet Period      : 60   seconds    Transmission Period   : 30   seconds
Supplicant Timeout : 30   seconds    Server Timeout       : 30   seconds
Maxumum Request    : 2              Re-auth Period       : 60   minutes
Re-auth Status     : Disabled

Switch#
```

5.17 Radius Commands

radius-server host

Use the radius-server host command to specify a RADIUS server host.

radius-server host < ip-address> [timeout <seconds>] [retransmit <retries>] [key <string>]

no radius-server

SYNTAX DESCRIPTION:	ip-address	IP address of the RADIUS server host
	timeout	(Optional) The time interval in seconds that the router waits for the RADIUS server to reply before retransmitting.
	seconds	The range is 1 to 1000.
	retransmit	(Optional) The number of times a RADIUS request is re-sent to a server.
	retries	The range is 1 to 100.
	key	(Optional) Specifies the authentication and encryption key used between the NAS and RADIUS server.
	string	(Optional) Text string.

COMMAND MODES: Global configuration

REFERENCE: Cisco

MENU:

EXAMPLE:

```
!Set radius server 192.168.0.1 timeout 5 second retransmit 4 times and
Shared Secret "karl_radius"
Switch(config)# radius-server host 192.168.0.1 timeout 5 retransmit 4 key
karl_radius
Switch(config)#
```

show radius-server

Use the show radius-server command to display Radius configure information.

show radius-server

Syntax Description: The show radius-server command has no arguments or keywords.
Default Value: The show radius-server command has no default setting.
Command Modes: Privileged EXEC
Reference:
Menu:

Example:

```
Switch# show radius

Server IP Address :        192.168.0.1
Shared Secret :            Karl_
Response Time :            5 seconds
Maximum Retransmission :   2

Switch#
```

5.18 SNTP Commands

sntp server

Use the sntp server command to configure the sntp server

snto server *<ip>*

SYNTAX DESCRIPTION: *<ip>* IP address of the recipient.
DEFAULT VALUE: The hosts are not assigned by default
COMMAND MODES: Global configuration
MENU: Basic Switch Configuration Menu->SNTP Configuration->
Set SNTP Server IP

EXAMPLE:

```
! Configure SNTP server ip 172.16.5.198.
Switch(config)# sntp server 172.16.5.198
Switch(config)#
```

sntp poll-interval

Use this command to configure the polling interval for sntp operation.

sntp poll-interval *<sec>*

SYNTAX DESCRIPTION: Integer value ranges from 1 to 1440 minutes.
DEFAULT VALUE: The default value is 1440 minutes (1 day).
COMMAND MODES: Global configuration
REFERENCE: None
MENU: Basic Switch Configuration Menu->SNTP Configuration->
Set SNTP Interval

EXAMPLE:

```
!Set SNTP polling interval 300 minutes.
Switch(config)# sntp poll-interval 300
Switch(config)#
```

sntp daylight-saving

Use this command to enable or disable daylight saving, if time zone is applicable.

sntp daylight-saving

no sntp daylight-saving

SYNTAX DESCRIPTION: This command has no argument.
DEFAULT VALUE: This command is disabled by default
COMMAND MODES: Global configuration
REFERENCE: None
MENU: Basic Switch Configuration Menu->SNTP Configuration->
Set Daylight Saving

EXAMPLE:

```
!Enable daylight saving.
Switch(config)# sntp daylight-saving
Switch(config)#
```

```
!Disable daylight saving.
Switch(config)# no sntp daylight-saving
Switch(config)#
```

sntp timezone

Use the sntp timezone command to configure the timezone.

show timezone *<location>*

SYNTAX DESCRIPTION: This location type ranges from 1 to 63.
DEFAULT VALUE:
COMMAND MODES: Global configuration
REFERENCE: None
MENU: Basic Switch Configuration Menu->SNTP Configuration->
Set time Zone

Example:

```
!Configure timezone to Taipei.
Switch(config)# sntp timezone 50
Switch(config)#
```

show sntp

Use the show sntp configuration information for the interface

show sntp

Syntax Description:
Default Value: This command has no default value
Command Modes: Privileged EXEC
Reference:
Menu:

Example:

```
Switch# show sntp

Date ( YYYY/MM/DD )    : 03:41:07
Time ( HH:MM:SS )      : 1900/01/01     Thursday

SNTP Server IP         : 172.16.5.198
SNTP Polling Interval : 300 Min
Time Zone              : (GMT+08:00) Taipei
Daylight Saving        : N/A

Switch#
```

5.19 Syslog Commands

show log

Use the show log command to display log for the switch

show log

SYNTAX DESCRIPTION:

DEFAULT VALUE: The show log command has no default setting

COMMAND MODES: Priviliaged EXEC

REFERENCE:

MENU:

EXAMPLE:

```
Switch# show log
Entry  Time(YYYY/MM/DD HH:MM:SS) Event
----- -------------------------  -------------------------------------
1   0000/00/00 00:00:18         Configuration changed
2   0000/00/00 00:00:22         Reboot: Factory Default
3   0000/00/00 00:00:27         (Bridge) Topology Change
4   0000/00/00 00:00:35         Login from console
5   0000/00/00 00:25:43         Login from console
6   0000/00/00 00:35:58         (Bridge) Topology Change
7   0000/00/00 00:43:17         (Bridge) Topology Change
8   0000/00/00 00:51:18         (Bridge) Topology Change
9   0000/00/00 01:01:04         (Bridge) Topology Change
10   0000/00/00 01:03:25         (Bridge) Topology Change
11   0000/00/00 01:04:56         (Bridge) Topology Change
12   0000/00/00 01:10:45         (Bridge) Topology Change
13   0000/00/00 01:14:03         (Bridge) Topology Change
14   0000/00/00 01:16:49         (Bridge) Topology Change
15   0000/00/00 01:19:10         Login from console
16   0000/00/00 02:34:24         (Bridge) Topology Change

Switch#
```

log clear

Use the log clear command to delete the syslog

log clear

Syntax Description:
Default Value:
Command Modes: Global configuration
Reference:
Menu:

Example:

```
Switch(config)# log clear
Switch(config)#
```

5.20 Power Over Ethernet Commands

peth trap

Use the peth trap command to configure a PoE trap.

peth trap
no peth trap

Syntax Description: The peth trap command has no arguments or keywords
Default Value:
Command Modes: Global configuration
Reference:
Menu:

Example:

```
!Set PETH trap on
Switch(config)# peth trap
Switch(config)#
```

peth usage-threshold

Use the peth usage-threshold command to configure power usage threshold.

peth usage-threshold *<percent>*

Syntax Description: 1-99, The usage threshold expressed in percents for comparing the measured power and initiating an alarm if the threshold is exceeded.
Default Value:
Command Modes: Global configuration
Reference:
Menu:

Example:

```
!Set power usage threshold 60
Switch(config)# peth usage-threshold 60
Switch(config)#
```

peth disconnection-method

Use the peth disconnection-method command to configure the dosconnection method.

peth disconnection-method *<method>*

Syntax Description: *<method>*

next port - After the power budget has been exceeded, the next port attempting to power up is denied, regardless of its priority.

low-priority - After the power budget has been exceeded, the next port attempting to power up, causes the port with the lowest priority to shut down, to allow higher-priority ports topower up.

Default Value:

Command Modes: Global configuration

Reference:

Menu:

Example:

```
!Set disconnection-method low-priority
Switch(config)# peth disconnection-method low-priority
Switch(config)#
```

peth capacitor-detection

Use the peth capacitor-detection command to set the power detection method.

peth capacitor detection
no peth capacitor detection

Syntax Description: The peth capacitor-detection command has no arguments or keywords

Default Value:

Command Modes: Global configuration

Reference:

Menu:

EXAMPLE:

```
!Enable capacitor detection
Switch(config)# peth capacitor-detection
Switch(config)#
```

peth limit

Use the peth limit command to set the power limit on a port.

peth limit *<mwatt>*

SYNTAX DESCRIPTION: <mwatt> Power limit 3-20 watts
DEFAULT VALUE: 15 watt
COMMAND MODES: Interface configuration
REFERENCE:
MENU:

EXAMPLE:

```
!Set power limit 10 watt on port 2
Switch(config)# interface fastethernet0/2
Switch(config-if)# peth limit 15
Switch(config-if)#
```

peth priority

Use the peth priority command for when the power budget is not enough.

peth priority *<level>*

SYNTAX DESCRIPTION: *<level>* Critical - Set critical priority to critical
High - Set critical priority to high
Low - Set critical priority to low
DEFAULT VALUE: High
COMMAND MODES: Interface configuration
REFERENCE:
MENU:

Example:

```
!Set priority low oon port 3
Switch(config)# interface fastethernet0/3
Switch(config-if)# peth priority low
Switch(config-if)#
```

peth shutdown

Use the peth shutdown command to shut down a PoE port.

peth shutdown

Syntax Description: The peth shutdown command has no arguments or keywords.

Default Value:

Command Modes: Interface configuration

Reference:

Menu:

Example:

```
!Disable Power Ethernet on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# peth shutdown
Switch(config-if)#
```

```
!Enable Power Ethernet on port 4
Switch(config)# interface fastethernet0/4
Switch(config-if)# no peth shutdown
Switch(config-if)#
```

show peth-conf

Use the show peth-conf command to display switch Ethernet settings..

show peth-conf

Syntax Description: This command has no arguments or keywords.
Default Value:
Command Modes: Prilileged EXEC
Reference:
Menu:

Example:

```
Switch# show peth-conf

Power budget              : 170 Watts
Power Consumption         : 0 Watts
Power usage threshold     : 60 %
Power Management Method : Low priority port will be shut down
Power Detection Method    : capacitor detection enabled

Switch#
```

show peth-port

Use the show peth-port command to display PoE port settings and power measurements.

show peth-port

Syntax Description: The show peth-port command has no arguments or keywords.
Default Value:
Command Modes: Prilileged EXEC
Reference:
Menu:

EXAMPLE:

```
Switch# show peth-port
No. Admin.  Status        Class Prio.  Limit (W) Power (W) Vol. (V)  Cur.
--- ------ -------------- ----- ------ --------- --------- --------- ----
1    Up   Not Powered     ---   Low     15.4         0        0        0
2    Down Not Powered     ---   Low       15         0        0        0
3    Up   Not Powered     ---   Low     15.4         0        0        0
4    Up   Not Powered     ---   Low     15.4         0        0        0
5    Up   Not Powered     ---   Low     15.4         0        0        0
6    Up   Not Powered     ---   Low     15.4         0        0        0
7    Up   Not Powered     ---   Low     15.4         0        0        0
8    Up   Not Powered     ---   Low     15.4         0        0        0
9    Up   Not Powered     ---   Low     15.4         0        0        0
10   Up   Not Powered     ---   Low     15.4         0        0        0
11   Up   Not Powered     ---   Low     15.4         0        0        0
12   Up   Not Powered     ---   Low     15.4         0        0        0
13   Up   Not Powered     ---   Low     15.4         0        0        0

Switch#
```

5.21 Miscellaneous Commands

system mtu

Use the system mtu command to set the mtu length.

system mtu 1578
no system mtu

Syntax Description: The system mtu command has one argument for the current version that is required to be 1578.

Default Value:

Command Modes: Global configuration

Reference:

Menu:

Example:

```
! Set system mtu 1578
Switch(config)# system mtu 1578
Switch(config)#
```

show system mtu

Use the show system mtu command to display system mtu.

show system mtu

Syntax Description: The show system mtu command has no arguments or keywords.

Default Value:

Command Modes: Privileged EXEC

Reference:

Menu:

Example:

```
Switch# show system mtu
MU Length: 1578
Switch)#
```

5.22 Sample Configuration File

```
! Configuration file
!
!
hostname switch-24+2
snmp-server location taipei
snmp-server contact taipei
username name admin password software
!
spanning-tree priority 30000
spanning-tree max-age 7
spanning-tree hello-time 1
spanning-tree forward-time 10
spanning-tree
!
!
interface FastEthernet0/1
 shutdown
 speed-duplex 10-full
 no flow-control
 port security max-mac-count 100
 port security action shutdown
 spanning-tree cost 23
 spanning-tree port-priority 150
```

```
!
interface FastEthernet0/2
 shutdown
 no flow-control
!
interface FastEthernet0/3
 no flow-control
!
interface FastEthernet0/4
 speed-duplex 100-full
 no flow-control
!
interface FastEthernet0/5
 no flow-control
!
interface FastEthernet0/6
 no flow-control
!
interface FastEthernet0/7
 no flow-control
 spanning-tree port-priority 20
!
interface FastEthernet0/8
 no flow-control
 spanning-tree cost 10
```

```
!
interface FastEthernet0/9
 no flow-control
!
interface FastEthernet0/10
 spanning-tree cost 2
 spanning-tree port-priority 3
!
interface FastEthernet0/11
 spanning-tree cost 2
 spanning-tree port-priority 3
!
interface FastEthernet0/12
 spanning-tree cost 2
 spanning-tree port-priority 3
!
interface FastEthernet0/13
 spanning-tree cost 2
 spanning-tree port-priority 3
!
interface FastEthernet0/14
 no flow-control
!
interface FastEthernet0/15
 no flow-control
```

```
!
interface FastEthernet0/16
 no flow-control
!
interface FastEthernet0/17
 no flow-control
!
interface FastEthernet0/18
 no flow-control
!
interface FastEthernet0/19
 no flow-control
 port security max-mac-count 1
 port security action noaction
!
interface FastEthernet0/20
 no flow-control
 port security Secure
 port security action trap-shutdown
!
interface FastEthernet0/21
 no flow-control
!
interface FastEthernet0/22
 no flow-control
 port monitor FastEthernet0/23
!
interface FastEthernet0/23
 no flow-control
!
interface FastEthernet0/24
 no flow-control
!
interface GigabitEthernet0/25
 no flow-control
!
interface GigabitEthernet0/26
 giga-port-type GBIC
 no flow-control
!
!
vlan-type 802.1q
!
interface vlan1
 name Default VLAN
 untagged 0/1-26
!
interface vlan2
 name inter VLAN
 untagged 0/1,0/5-9
 tagged 0/2
 forbidden 0/3-4
!
interface vlan3
 name ext VLAN
 untagged 0/14
 tagged 0/15
 forbidden 0/10-13
!
ip address 172.16.3.42 255.255.240.0
!
ip igmp snooping
ip igmp snooping aging-time 300
ip default-gateway 172.16.5.111
no ip http server
mac-address-table aging-time 400
mac-address-table static 00:00:11:22:33:44 FastEthernet1/5 vlan 1
mac-address-table static 00:11:22:33:33:33 FastEthernet1/6 vlan 2
!
no snmp-server
snmp-server community read RO
snmp-server community manager RW
snmp-server host 172.16.5.198 trap manager
snmp-server host 172.16.5.182 trap Gwen_MS
no snmp-server enable traps snmp authentication
```

```
!
mls qos
priority-queue cos-map 0 1
priority-queue cos-map 0 2
priority-queue cos-map 1 6
priority-queue cos-map 1 7
!
port storm-control broadcast threshold medium
!
console inactivity-timer 0
!
no telnet-server
telnet-server inactivity-timer 10
!
end
```

A

Specifications & Pin Assignments

A.1 Specifications

The ES3000 Ethernet Switch has the following specifications:

Width	482.6 mm with mounting brackets 440 mm without moutning brackets
Height	44 mm (1RU)
Depth	256 mm
Weight	PoE version 8.95 lbs. (with rack brackets) PoE version 8.95 lbs. (without rack brackets) Non PoE version 7.90lbs. (with rack brackets) Non PoE version 7.75 lbs. (without rack brackets)
Max Power Consumption	100VAC - 240VAC, 50Hz/60Hz, 3.5A (PoE) 100VAC - 240VAC, 50Hz/60Hz, 1.5A (non PoE)
Operating Temperature	0 to 40 C

Operating Humidity	10% to 40 % (without condensation)
MTBF	ES-3000-PWR-10-WW - 140,000 hours @ 25 C ES-3000-10-WW - 355,000 hours @ 25 C FIBER-3000-1S-WW - 1,125,000 hours @ 25 C

A.2 RJ-45 Plug and RJ-45 Connector

In a Fast Ethernet network, it is important all 100BASE-T certified Category 5 cabling use RJ-45 plugs. The RJ-45 plug accepts 4-pair UTP or shielded twisted-pair (STP) 100-ohm cable and connects into the RJ-45 connector. The RJ-45 connector is used to connect stations, hubs, and switches through UTP cable; it supports 10 Mbps, 100 Mbps, or 1000 Mbps data transmission.

Pin	***Normal Assignment on Ports 1 To 8***	***Uplink Assignment on Port 8***
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data -	Output Transmit Data -
3	Output Transmit Data +	Input Receive Data +
6	Output Transmit Data -	Input Receive Data -
4, 5, 7, 8	Internal termination, not used for data transmission	

Pin	***Channel***	***Description***
12	A	Rx/Tx Data +Rx/Tx Data
36	B	Rx/Tx Data +Rx/Tx Data
45	C	Rx/Tx Data +Rx/Tx Data
78	D	Rx/Tx Data +Rx/Tx Data

B

Cabling Guidelines

B.1 Fast Ethernet Cable Guidelines

Fast Ethernet uses UTP cable, as specified in the IEEE 802.3u standard for 100BASE-TX.The specification requires Category 5 UTP cable consisting of either two-pair or four-pair twisted insulated copper conductors bound in a single plastic sheath. Category 5 cable is certified up to 100 MHz bandwidth. 100BASE-TX operation uses one pair of wires for transmission and the other pair for receiving and for collision detection.

When installing Category 5 UTP cabling, use the following guidelines to ensure cables perform to the following specifications:

B.1.1 Certification

Verify the Category 5 UTP cable has completed the Underwriters' Laboratories (UL) or Electronic Testing Laboratories (ETL) certification process.

B.1.2 Termination Method

To minimize cross-talk noise, maintain the twist ratio of the cable up to the point of termination; verify untwist at any RJ-45 plug or patch panel does not exceed 0.5 inch (1.5 cm).

B.2 Category 5 Cable

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft) or 100 meters (m) in length, divided as follows:

- 20 ft (6 m) between the hub and the patch panel (if used)
- 295 ft (90 m) from the wiring closet to the wall outlet
- 10 ft (3 m) from the wall outlet to the desktop device

The patch panel and other connecting hardware is required to meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

B.2.1 Category 5 Cable Specifications

Ensure the fiber cable is crossed over to guarantee link.

Specifications	***Category 5 Cable Requirements***
Number of pairs	Four
Impedance	100 ? ± 15%
Mutual capacitance at 1 KHz	=5.6 nF per 100 m
Maximum attenuation (dB per 100 m, at 20° C)	at 4 MHz: 8.2at 31 MHz: 11.7at 100 MHz: 22.0
NEXT loss (dB minimum)	at 16 MHz: 44at 31 MHz: 39at 100 MHz: 32

B.3 Twisted Pair Cables

For two devices to communicate, the transmitter of each device is required to be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

B.4 Patch Panels and Cables

If using patch panels, ensure they meet the 100BASE-TX requirements. Symbol recommends Category 5 UTP cable for patch cables and work area cables to ensure the UTP patch cable rating meets or exceeds the distribution cable rating. To wire patch panels, two Category 5 UTP cables are required with an RJ-45 plug at each end.

Flat silver satin telephone cable can have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

B.5 Using 1000BASE-T Gigabit Ethernet over Category 5 Cable

B.5.1 Overview

When using the new 1000BASE-T standard, consider the limitations of cable installations and the steps necessary to ensure optimum performance. The most important components in the cabling system are patch panel connections, twists of the pairs at connector transition points, the jacket around the twisted-pair cable, bundling of multiple pairs on horizontal runs and punch down blocks. All of these factors affect the performance of 1000BASE-T technology if not correctly implemented.

B.5.2 Cabling

The 1000BASE-T product is designed to operate over Category 5 cabling. To further enhance the operation, the cabling standards have been amended. The latest standard is Category 5e, which defines a higher level of link performance than is available with Category 5 cable.

If installing new cable, Symbol recommends using Category 5e cable. If using the existing cable, be sure to have the cable plant tested by a professional who can verify it meets or exceeds either ANSI/ EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications.

B.5.3 Length

The maximum distance limitation between two pieces of equipment is 100 m, as per the original Ethernet specification. The end-to-end link is called the "channel."

TSB-67 defines the "Basic Link" which is the portion of the link that is part of the building infrastructure. This excludes patch and equipment cords. The maximum basic link length is 295 feet (90 m).

B.5.4 Return Loss

Return loss measures the amount of reflected signal energy resulting from impedance changes in the cabling link. The nature of 1000BASE-T renders this measurement very important; if too much energy is reflected back on to the receiver, the device does not perform optimally.

Unlike 10BASE-T and 100BASE-TX (which use only two of the four pairs of wires within the Category 5) 1000BASE-T uses all four pairs of the twisted pair. Verify all wires are tested.

Factors effecting return loss are:

- The number of transition points, as there is a connection via an RJ-45 to another connector, a patch panel, or device at each transition point.
- Removing the jacket that surrounds the four pairs of twisted cable. It is highly recommended that, when RJ-45 connections are made, this is minimized to 1-1/4 inch (32 mm).
- Untwisting any pair of the twisted-pair cabling. It is important any untwisting be minimized to 3/8 inch (10 mm) for RJ-45 connections.
- Cabling or bundling of multiple Category 5 cables. This is regulated by ANSI/EIA/TIA-568A-3. If not correctly implemented, this can adversely affect all cabling parameters.

B.5.5 Near End Cross Talk (NEXT)

Near End Cross Talk is a measure of the signal coupling from one wire to another, within a cable assembly, or among cables within a bundle. NEXT measures the amount of cross-talk disturbance energy that is detected at the near end of the link - the end where the transmitter is located. NEXT measures the amount of energy that is "returned" to the sender end. The factors that affect NEXT and cross talk are exactly the same as outlined in the Return Loss section. The cross-talk performance is directly related to the quality of the cable installation.

B.5.6 Patch Cables

When installing equipment, replace old patch panel cables that do not meet Category 5e specifications. As pointed out in the NEXT section, this near end piece of cable is critical for successful operation.

B.5.7 Optimum Performance

For optimum performance of the 1000BASE-T product, it is important to fully qualify the cable installation and ensure it meets or exceeds ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications. Install Category 5e cable where possible, including patch panel cables. Minimize transition points, jacket removal, and untwist lengths. Bundling of cables is required to be properly installed to meet the requirements in ANSI/EIA/TIA-568A-3.

C
Customer Support

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number.

North American Contacts

Inside North America, contact Symbol by:

Symbol Technologies, Inc.
One Symbol Plaza Holtsville, New York 11742-1300
Telephone: 1-631-738-2400/1-800-SCAN 234
Fax: 1-631-738-5990

Symbol Support Center (for warranty and service information):

telephone: 1-800-653-5350
fax: (631) 563-5410
Email: support@symbol.com

International Contacts

Outside North America, contact Symbol by:

Symbol Technologies
Symbol Place
Winnersh Triangle, Berkshire, RG41 5TP
United Kingdom
0800-328-2424 (Inside UK)
+44 118 945 7529 (Outside UK)

Web Support Sites

MySymbolCare

http://www.symbol.com/services/msc

Symbol Services Homepage

http://symbol.com/services

Symbol Software Updates

http://symbol.com/services/downloads

Symbol Developer Program

http://software.symbol.com/devzone

Additional Information

Obtain additional information by contacting Symbol at:

1-800-722-6234, inside North America
+1-631-738-5200, in/outside North America
http://www.symbol.com/

Glossary

10BASE-T The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.

100BASE-FX The IEEE specification for 100 Mbps Fast Ethernet over fiber-optic cable.

100BASE-TX The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

1000BASE-SX The IEEE specification for 1000 Mbps Gigabit Ethernet over fiber-optic cable.

1000BASE-T The IEEE specification for 1000 Mbps Gigabit Ethernet over Category 5 twisted-pair cable.

Auto-negotiation A feature that allows twisted-pair ports to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.

Auto Uplink A feature that allows twisted-pair ports to sense if a normal (MDI-X) or uplink (MDI) connection is necessary and make the right link. It adjusts for straight-through or crossover cables.

Backbone

The part of a network used as a primary path for transporting traffic between network segments.

Bandwidth

The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

Baud

The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

Broadcast

A packet sent to all devices on a network.

Broadcast storm

Multiple simultaneous broadcasts that typically absorb all the available network bandwidth and can cause a network to fail. Broadcast storms can be due to faulty network devices or network loops.

Capacity planning

Determining whether current solutions can satisfy future demands. Capacity planning includes evaluating potential workload and infrastructure changes.

Class of Service

A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

Collision

A term used to describe two colliding packets in an Ethernet network. Collisions are a part of normal Ethernet operation, but a sudden prolonged increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic.

Endstation

A computer, printer, or server that is connected to a network.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

Gigabit Ethernet

An Ethernet system that is designed to operate at 1000 Mbps (1 Gbps).

Fault isolation

A technique for identifying and alerting administrators about connections (such as those associated with switch ports) that are experiencing congestion or failure, or exceeding an administrator-defined threshold.

Forwarding

The process of sending a packet toward its destination using a networking device.

Filtering

The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.

Flow control

A congestion- control mechanism. Congestion is caused by devices sending traffic to already overloaded port on a switch. Flow control prevents packet loss and temporarily inhibits devices from generating more traffic until the period of congestion ends.

Full-duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

Half-duplex

A system that allows packets to transmitted and received, but not at the same time. Contrast with full-duplex.

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IGMP

Internet Group Management Protocol, the standard for IP multicasting in the Internet. IGMP is used to establish host memberships in multicast groups on a single network. (See IP multicast)

IP

Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices.

IP address

Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

IP multicast

Sending data to distributed servers on a multicast backbone. For large amounts of data, IP Multicast is more efficient than normal Internet transmissions, because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

LAN

Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building).

Load balancing

The ability to distribute traffic across various ports of a device, such as a switch, to provide efficient, optimized traffic throughout the network.

Loop

An event that occurs when two network devices are connected by more than one path, thereby causing packets to repeatedly cycle around the network and not reach their destination.

MAC

Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC address

Media Access Control address; also called hardware or physical address. Most devices that connect to a LAN have a MAC address assigned to them, as they are used to identify other devices in a network.

Multicast

A single packet sent to a specific group of end stations on a network.

Port monitoring

The ability to monitor the traffic passing through a port on a device to analyze network characteristics and perform troubleshooting.

Port speed

The speed that a port on a device uses to communicate with another device or the network.

Port trunking

The ability to combine multiple ports on a device to create a single, high-bandwidth connection.

Protocol

A set of rules for communication between devices on a network.

Quality of Service

A term to describe delay, throughput, bandwidth, and other factors that measure the service quality provided to a user.

Segment

A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

SNMP

Simple Network Management Protocol. An IETF standard protocol for managing devices on a TCP/IP network.

Spanning Tree

A technique that detects loops in a network and logically blocks the redundant paths, ensuring that only one route exists between any two LANs.

Spanning Tree Protocol (STP)

A protocol that finds the most efficient path between segments of a multi-looped, bridged network. STP allows redundant switches and bridges to be used for network resilience, without the broadcast storms associated with looping. If a switch or bridge falls, a new path to a redundant switch or bridge is opened.

Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

TCP/IP

Transmission Control Protocol/Internet Protocol. This is the name for two of the most well known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.TCP relates to the content of the data traveling through a network - ensuring that the information sent arrives in one piece when it reaches its destination.IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

Telnet

A TCP/IP application protocol that provides a virtual terminal service, allowing a user to log into another computer system and access a device as if the user were connected directly to the device.

TFTP

Trivial File Transfer Protocol. Allows the transfer of files (such as software upgrades) from a remote device using the local management capabilities of the Switch.

Traffic prioritization Giving time-critical data traffic a higher quality of service over other, non-critical data traffic.

Unicast A packet sent to a single end station on a network.

VLAN Virtual LAN. A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

Index

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, New York 11742-1300
http://www.symbol.com

72E--68446-01
Revision A May 2004