



FXC3024 User Manual

**Version 1.0
Oct. 2004**

Table of Contents

1.	INTRODUCTION	10
1.1	About This Manual.....	10
1.2	Summary of Features	10
1.3	Factory Default Settings.....	11
2.	PHYSICAL DESCRIPTION	13
2.1	Front Panel of L2SW Switch	13
2.2	L2SW Switch LED Indications.....	13
2.3	Rear Panel of L2SW Switch	14
2.4	Description of L2SW LEDs	14
3.	MANAGEMENT ACCESS	16
3.1	Management Methods Supported by Various Interfaces	16
3.1.1	Serial Port Interface	17
3.1.2	In-band Network Management Interface	17
3.2	Getting Started.....	17
3.2.1	Port Names	17
3.2.2	Terminal Access Setup	17
3.2.3	CLI Syntax Conventions	18
3.2.4	Network Port Access Setup	18
4.	WEB MANAGEMENT FUNCTION	19
4.1	Port Status.....	21
4.2	Port Statistics	23
4.3	Administrator	24
4.3.1	Stacking	24
4.3.2	IP Address	25
4.3.3	Switch Setting.....	27
4.3.3.1	Basic	27
4.3.3.2	Module Info.....	28
4.3.3.3	Advanced Settings	28
4.3.3.4	Miscellaneous Settings.....	30
4.3.4	Console Port Information	31
4.3.5	Trunking	31
4.3.5.1	Aggregator Settings	32
4.3.6	IGMP Snooping and Filter Database	35

4.3.6.1	IGMP Snooping	35
4.3.7	Static MAC Address	37
4.3.8	MAC Filtering	38
4.3.9	VLAN	38
4.3.9.1	Port Based VLAN	41
4.3.9.2	802.1Q (Tag based) VLAN	42
4.3.9.3	VLAN Configuration	43
4.3.10	Spanning Tree	46
4.3.10.1	STP (802.1d) Configuration	47
4.3.10.2	RSTP (802.1w) Configuration	49
4.3.10.3	MSTP Configuration	52
4.3.11	Port Sniffer	55
4.3.12	SNMP	57
4.3.12.1	SNMP v3 Configuration	58
4.3.13	Security Manager	62
4.3.14	802.1x	63
4.3.14.1	802.1x Configuration	64
4.3.14.2	PerPort Configuration	65
4.3.14.3	802.1x Miscellaneous Configuration	66
4.4	TFTP Update Firmware	68
4.5	Configuration Backup	69
4.5.1	TFTP Backup Configuration	69
4.5.2	TFTP Restore Configuration	69
4.6	Default Configuration	71
4.7	Reboot	71
5.	CONSOLE – MENU LINE	73
5.1	Main Menu	73
5.2	Switch Static Configuration	76
5.2.1	Port Configuration	76
5.2.2	Trunk Configuration	77
5.2.3	VLAN Configuration	79
5.2.3.1	VLAN Configure	79
5.2.3.2	Edit / Delete a VLAN Group	83
5.2.3.3	Groups Sorted Mode	84
5.2.4	Miscellaneous Configuration	84
5.2.4.1	MAC Age Interval	85
5.2.4.2	Broadcast Storm Filtering	85
5.2.4.3	Max Bridge transmit delay bound	86
5.2.4.4	Port Security	87
5.2.4.5	Collisions Retry Forever	88
5.2.5	Administration Configuration	88
5.2.5.1	Change Username	89
5.2.5.2	Change Password	89
5.2.5.3	Device Information	90
5.2.5.4	IP Configuration	90
5.2.6	Port Mirroring Configuration	91
5.2.7	Priority Configuration	92
5.2.7.1	Port Static Priority	93

5.2.7.2	802.Ip Priority Configuration	94
5.2.8	MAC Address Configuration.....	94
5.2.8.1	Static MAC Address	95
5.2.8.2	Filtering MAC Address	98
5.3	Protocol Related Configuration.....	101
5.3.1	STP	101
5.3.2	SNMP	101
5.3.3	GVRP	101
5.3.4	IGMP	102
5.3.5	LACP.....	103
5.3.5.1	Working Port Setting	103
5.3.5.2	State Activity	104
5.3.5.3	LACP Status.....	106
5.3.5.4	LACP trunk group.....	106
5.4	Status and Counters	107
5.4.1	Port Status.....	107
5.4.2	Port Counters	108
5.4.3	System Information	108
5.5	Reboot Switch	109
5.5.1	Default.....	110
5.5.2	Restart.....	110
5.6	TFTP Update Firmware	111
5.6.1	TFTP Update Firmware.....	111
5.6.2	Restore Configure File.....	112
5.6.3	Backup Configure File.....	113
6.	CLI BASED MANAGEMENT.....	114
6.1.1	CLI Syntax Conventions	115
6.1.2	Login User Setup	116
6.1.3	Network Port Access Setup	116
6.1.4	Telnet Access Setup	116
6.1.5	Serial Port Setup	117
6.1.6	Inactivity Timeout	117
6.2	Stacking Configuration	117
6.3	Port Configuration	118
6.3.1	Display Port Configuration.....	119
6.3.2	Port Configuration Settings	120
6.4	MAC Aging	122
6.5	Static MAC Address.....	122
6.6	MAC Filtering.....	123
6.7	VLAN.....	124
6.7.1	802.1Q VLAN	125
6.7.2	Port VID & Ingress filtering.....	126
6.7.3	Show VLAN.....	127
6.7.4	GVRP	129

6.8	Spanning Tree Protocol.....	130
6.8.1	STP Configuration.....	130
6.8.2	RSTP Configuration.....	133
6.8.3	MSTP Configuration.....	134
6.9	Link Aggregation & Trunking Settings.....	137
6.10	Port Mirroring.....	139
6.11	Broadcast Storm Filtering.....	140
6.12	IGMP Snooping.....	140
6.13	802.1X.....	141
6.14	Priority.....	143
6.15	Switch Settings.....	144
6.16	Statistics.....	146
6.17	Management Commands.....	147
6.17.1	User Login Accounts.....	147
6.17.2	Switch Inventory.....	147
6.17.3	Network IP Address Configuration.....	148
6.18	SNMP.....	148
6.18.1	SNMP System Setup.....	148
6.18.2	SNMP Community setup:.....	149
6.18.3	SNMP Trap Setup.....	150
6.18.4	SNMPv3 Configuration.....	150
6.19	Remote Monitoring.....	154
6.20	System Utilities.....	155
6.20.1	Management VLAN.....	155
6.20.2	SNTP Configuration.....	155
6.20.3	Syslog Configuration.....	156
6.20.4	TFTP Backup or Upload Configuration.....	156
6.20.5	TFTP restore or download configuration.....	157
6.20.6	TFTP Update Firmware.....	157
6.20.7	Default Configuration.....	158
6.20.8	Reboot.....	158
7.	APPENDIX A: TERMS AND ABBREVIATIONS.....	159

Table of Figures

FIGURE 2-1 FRONT PANEL OF L2SW SWITCH WITH TWO 1000 BASE TX CARD	13
FIGURE 2-2 REAR PANEL OF L2SW SWITCH	14
FIGURE 4-1: LOGIN	19
FIGURE 4-2: WBI MANAGEMENT INTERFACE	20
FIGURE 4-3: PORT STATUS	21
FIGURE 4-4: INDIVIDUAL PORT STATUS	22
FIGURE 4-5: PORT STATISTICS	23
FIGURE 4-6: STACKING CONFIGURATION	25
FIGURE 4-7: IP ADDRESS	26
FIGURE 4-8: SWITCH SETTINGS/BASIC INFORMATION	27
FIGURE 4-9: SWITCH SETTINGS/MODULE INFORMATION	28
FIGURE 4-10: ADVANCED SWITCH SETTINGS	29
FIGURE 4-11: MISCELLANEOUS SWITCH SETTINGS	30
FIGURE 4-12: CONSOLE INFORMATION	31
FIGURE 4-13: TRUNKING	32
FIGURE 4-14: LACP DISABLED	33
FIGURE 4-15: STATIC TRUNKING GROUPS	34
FIGURE 4-16: ACTOR AND PARTNER GROUP	34
FIGURE 4-17: STATE ACTIVITY	35
FIGURE 4-18: IGMP SNOOPING	36
FIGURE 4-19: STATIC MAC ADDRESS	37
FIGURE 4-20: MAC FILTERING	38
FIGURE 4-21: VLAN CONFIGURATION	39
FIGURE 4-22 PORT-BASED VLAN ID	40
FIGURE 4-23: PORT BASED VLAN	41
FIGURE 4-24: 802.1Q BASED VLAN	43
FIGURE 4-25: CREATE VLAN	44
FIGURE 4-26: ADD PORTS TO VLAN	45
FIGURE 4-27: CONFIGURE VID	45
FIGURE 4-28: SPANNING TREE VERSION SELECTION	48
FIGURE 4-29: SWITCH STP CONFIGURATION SUMMARY	49
FIGURE 4-30: RSTP CONFIGURATION	50
FIGURE 4-31: RSTP PORT CONFIGURATION	51
FIGURE 4-32: RSTP PORT STATUS DISPLAY	52
FIGURE 4-33: MSTP SWITCH CONFIGURATION	53
FIGURE 4-34: MST INSTANCE CONFIGURATION	53
FIGURE 4-35: MSTI CONFIGURATION REPORT	54
FIGURE 4-36: MST INSTANCE DETAILS	55
FIGURE 4-37: PORT SNIFFER	56
FIGURE 4-38:SNMP MANAGEMENT	57
FIGURE 4-39: COMMUNITY STRINGS	58
FIGURE 4-40: TRAP MANAGER	58
FIGURE 4-41: SNMP ENGINE ID CONFIGURATION SCREEN	59
FIGURE 4-42: VIEWS CONFIGURATION SCREEN	60
FIGURE 4-43: SNMPV3 GROUP CONFIGURATION	61
FIGURE 4-44: SNMPV3 USER CONFIGURATION	62
FIGURE 4-45: SECURITY MANAGER	63
FIGURE 4-46: ENABLE 802.1X	64
FIGURE 4-47: 802.1X CONFIGURATION	64
FIGURE 4-48: 802.1X PERPORT CONFIGURATION	65
FIGURE 4-49: 802.1X PORT STATUS	66

FIGURE 4-50: 802.1X MISCELLANEOUS CONFIGURATION	66
FIGURE 4-51: TFTP DOWNLOAD	68
FIGURE 4-52: CONFIRMATION FOR TFTP UPGRADE	68
FIGURE 4-53: TFTP BACKUP CONFIGURATION	69
FIGURE 4-54: TFTP RESTORE CONFIGURATION	69
FIGURE 4-55: RESET SYSTEM	71
FIGURE 4-56: REBOOT SYSTEM	72
FIGURE 5-1: LOGIN FOR CONSOLE	73
FIGURE 5-2: MAIN MENU FOR CONSOLE	74
FIGURE 5-3: SWITCH CONFIGURATION	76
FIGURE 5-4: PORT CONFIGURATION	76
FIGURE 5-5: TRUNK CONFIGURATION	78
FIGURE 5-6: VLAN CONFIGURATION	79
FIGURE 5-7: PORT BASED VLAN	79
FIGURE 5-8: 802.1Q BASED VLAN	80
FIGURE 5-9: CREATE PORT BASED VLAN	81
FIGURE 5-10: CREATE 802.1Q BASED VLAN	82
FIGURE 5-11: SELECT A VLAN FOR EDITING	83
FIGURE 5-12: EDIT/DELETE SELECTED VLAN	83
FIGURE 5-13: GROUP SORTED VLAN	84
FIGURE 5-14: MISCELLANEOUS CONFIGURATION	85
FIGURE 5-15: MAC AGE INTERVAL	85
FIGURE 5-16: BROADCAST STORM FILTERING	86
FIGURE 5-17: MAXIMUM BRIDGE TRANSMIT DELAY BOUND	86
FIGURE 5-18: PORT SECURITY	87
FIGURE 5-19: COLLISIONS RETRY FOREVER	88
FIGURE 5-20: DEVICE CONFIGURATION	89
FIGURE 5-21: USER NAME CONFIGURATION	89
FIGURE 5-22: PASSWORD CONFIGURATION	90
FIGURE 5-23: DEVICE INFORMATION	90
FIGURE 5-24: IP CONFIGURATION	91
FIGURE 5-25: PORT MIRRORING	92
FIGURE 5-26: PRIORITY CONFIGURATION	93
FIGURE 5-27: PORT PRIORITY	93
FIGURE 5-28: 802.1P PRIORITY CONFIGURATION	94
FIGURE 5-29: MAC ADDRESS CONFIGURATION	95
FIGURE 5-30: STATIC MAC ADDRESS CONFIGURATION	95
FIGURE 5-31: ADD STATIC MAC ADDRESS	96
FIGURE 5-32: SELECT MAC ADDRESS	97
FIGURE 5-33: EDIT STATIC MAC ADDRESS	97
FIGURE 5-34: DELETE STATIC MAC ADDRESS	98
FIGURE 5-35: FILTER MAC ADDRESS	98
FIGURE 5-36: ADD MAC ADDRESS	99
FIGURE 5-37: FILTER MAC ADDRESS CONFIGURATION	99
FIGURE 5-38: EDIT FILTER MAC ADDRESS	100
FIGURE 5-39: DELETE SELECTED MAC ADDRESS	100
FIGURE 5-40: GVRP CONFIGURATION	102
FIGURE 5-41: IGMP CONFIGURATION	102
FIGURE 5-42: LACP CONFIGURATION	103
FIGURE 5-43: LACP GROUP CONFIGURATION	103
FIGURE 5-44: LACP PORT STATE ACTIVE CONFIGURATION	104
FIGURE 5-45: LACP STATIC TRUNKING GROUP	106
FIGURE 5-46: LACP GROUP STATUS	106
FIGURE 5-47: STATUS AND COUNTERS	107
FIGURE 5-48: PORT STATUS	107
FIGURE 5-49: PORT COUNTERS	108

FIGURE 5-50: SYSTEM INFORMATION	109
FIGURE 5-51: RESTART CONFIGURATION	110
FIGURE 5-52: DEFAULT SETTING	110
FIGURE 5-53: TFTP UPDATE FIRMWARE CONFIGURATION	111
FIGURE 5-54: EDIT TFTP UPDATE FIRMWARE	111
FIGURE 5-55: RESTORE CONFIGURATION FILE	112
FIGURE 5-56: BACKUP CONFIGURATION FILE	113
FIGURE 6-1 LOGIN PROMPT	115
FIGURE 6-2 DISPLAYS STACK	118
FIGURE 6-3: PORT STATUS DISPLAY	120
FIGURE 6-4 MAC TABLE AGING TIME	122
FIGURE 6-5 SHOW STATIC MAC ADDRESS ENTRIES	123
FIGURE 6-6: DYNAMICALLY LEARNT MAC ADDRESSES DISPLAY	123
FIGURE 6-7 DISPLAYS MAC FILTER ENTRIES	124
FIGURE 6-8 DISPLAY VLAN SUMMARY	128
FIGURE 6-9 DISPLAY VLAN DETAILS FOR SELECTED VLAN	128
FIGURE 6-10 SHOW VLAN PORT	129
FIGURE 6-11: GVRP INFORMATION DISPLAY	130
FIGURE 6-12 DISPLAYS SWITCH STP SETTINGS IN SUMMARY FORM	132
FIGURE 6-13: DISPLAY SWITCH SETTINGS IN DETAILED FORM	132
FIGURE 6-14 DISPLAYS PORT STP SETTINGS IN SUMMAY FORM	132
FIGURE 6-15: DISPLAY STP PORT SETTINGS IN DETAILED FORM	133
FIGURE 6-16: RSTP PORT CONFIGURATION STATUS DISPLAY	134
FIGURE 6-17: MST SWITCH CONFIGURATION DISPLAY IN SUMMARY FORMAT	136
FIGURE 6-18: MST SWITCH CONFIGURATION DISPLAY IN DETAILED FORMAT	136
FIGURE 6-19: MST INSTANCE DETAILS	137
FIGURE 6-20: SPANNING TREE PORT INFORMATION DISPLAY	137
FIGURE 6-21 DISPLAY TRUNK SUMMARY	138
FIGURE 6-22 DISPLAYS SELECTED TRUNK DETAILS	139
FIGURE 6-23 SHOW PORT MIRRORING	140
FIGURE 6-24 DISPLAYS BROADCAST STORM SETTINGS	140
FIGURE 6-25 DISPLAYS IGMP SNOOPING SETTINGS	141
FIGURE 6-26 DISPLAYS RADIUS SETTINGS	142
FIGURE 6-27 DISPLAYS DOT1X SWITCH SETTINGS	143
FIGURE 6-28 DISPLAYS DOT1X PORT CONTROL	143
FIGURE 6-29 DISPLAYS 802.1P PRIORITY SETTINGS	144
FIGURE 6-30: HARDWARE TABLE SIZE CONFIGURATION COMMAND	146
FIGURE 6-31 DISPLAYS SWITCH SETTINGS	146
FIGURE 6-32 DISPLAYS PORT STATISTICS	147
FIGURE 6-33 DISPLAY INVENTROY	147
FIGURE 6-34 DISPLAYS NETWORK SETTINGS	148
FIGURE 6-35 DISPLAYS SNMP SYSTEM SETTINGS	149
FIGURE 6-36 DISPLAYS SNMP COMMUNITY SETTINGS	150
FIGURE 6-37 DISPLAYS SNMP TRAP SETTINGS	150
FIGURE 6-38: SNMP SYSTEM CONFIGURATION	151
FIGURE 6-39: SNMP MIB VIEWS	152
FIGURE 6-40: SNMPV2 GROUP CONFIGURATION	153
FIGURE 6-41: SNMP USER CONFIGURATION	153
FIGURE 6-42: SNTP CONFIGURATION	156
FIGURE 6-43 DISPLAYS UPLOAD CONFIGURATION TO TFTP SERVER	156
FIGURE 6-44 DISPLAYS CONFIGURATION DOWN LOAD TO SYSTEM	157
FIGURE 6-45 DISPLAYS IMAGE DOWNLOAD	157
FIGURE 6-46 RESET SWITCH CONFIGURATION TO FACTORY DEFAULT	158
FIGURE 6-47 DISPLAYS SYSTEM REBOOT OPERATION	158

1. Introduction

1.1 *About This Manual*

The guide is intended for network administrators who are responsible for installing, provisioning and managing L2SW layer 2 switch running software version R2.2 or higher. It assumes a basic working knowledge of the following:

- Local area networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Internet Protocol (IP) concepts

1.2 *Summary of Features*

- 10/100Base TX half and Full Duplex
- 1000BaseT, SX and LX full Duplex
- 802.1D MAC Bridge
- 802.1w Rapid Spanning Tree Protocol (RSTP)
- 802.1s Multiple Spanning Tree Protocol (MSTP)
- Virtual LANs (VLAN) 802.1Q
- GVRP
- Spanning Tree Protocol (STP)
- 802.1p Priority Queuing
- 802.1x Network Port Security
- 802.3x Flow Control
- 802.3ad Link Aggregation
- Port Mirroring
- Broadcast Storm Recovery (BSR)
- IGMP Snooping
- Bootstrap Protocol (BOOTP) and Dynamic Host Configuration/Control Protocol (DHCP) clients for management interface
- Trivial File Transfer Protocol (TFTP) client for management interfaces
- User Interfaces

- Console Menu Line Interface (CMLI)¹
- Command Line Interface (CLI)
- Web Based Interface (WBI)
- Simple Network Management Protocol (SNMP)
 - SNMP- v1
 - SNMP-v2c and SNMPv3
- Simplified Remote Monitoring (RMON) I sections 1, 2, 3, and 9
- Simple Network Timing Protocol (SNTP)
- Syslog

1.3 **Factory Default Settings**

The L2SW products are factory provisioned with the following default settings:

- | | |
|---------------------------------|---------------------|
| • User Account - | admin |
| • Password -
representative) | (contact your sales |
| • Telnet - | Enabled |
| • System IP Address - | 192.168.1.1 |
| • Subnet Mask - | 255.255.255.0 |
| • Default Gateway IP Address - | 192.168.1.2 |
| • Broadcast Storm filtering - | Disabled |
| • 802.3x Flow Control Mode | Enabled |
| • 802.1x Network Port Security | Disabled |
| • LACP Mode - | Disabled |
| • Port Mirroring Mode - | Disabled |
| • STP Port State - | Disabled |
| • Port Mirroring - | Disabled |
| • VLAN traffic - | untagged |
| • Ingress Filtering - | Disabled |
| • GVRP | Disabled |
| • IGMP Snooping - | Disabled |
| • BOOTP/DHCP Admin Mode - | Disabled |
| • SNTP | Disabled |
| • Syslog | Disabled |
-

For all acronyms used in the manual see **Appendix A**

2. Physical Description

This chapter explains the hardware features of the L2SW Ethernet Smart Switch.

2.1 Front Panel of L2SW Switch

L2SW switch is designed for efficient use, with front panel access to the Fast Ethernet (10/100Base T) ports and two slots for user installable plug-in modules for uplink connection. The front panel also includes status LEDs for all the ports including uplink ports.

- 24 x 10/100 Mbps Fast Ethernet ports.
- 2 plug-in slots for uplink connection. The following plug-in cards are supported in L2SW.
 - 10/100/1000 Mbps T card. It supports auto-negotiation and can operate in master/slave clock modes
 - 100 Mbps (100BaseFX) card. This card is available with SC.
 - 1000 Mbps SFP card.



Figure 2-1 Front Panel of L2SW Switch with two 1000 Base TX card

2.2 L2SW Switch LED Indications

- 24 pairs of LEDs for 24 Fast Ethernet ports
 - Upper LED – link status (up/down) and port activity
 - Lower LED – ON- 100 Mbps, OFF- 10 Mbps settings
- 2 LEDs for each plug-in feature card ports
 - When a 1000Base feature card is used:
 - Upper LED - link status (up/down) and port activity
 - Lower LED - ON 1000Mbps, OFF - less than 1000 Mbps
 - When a 100Base FX feature card is used:
 - Upper LED - link status (up/down) and port Activity

Lower LED - ON - 100 Mbps

- 3 LEDs for Power Status Indicator (located on left corner)
 - Upper (PWR)- Power on status
 - Middle(BSALERT)- Broadcast Storm Alert
 - Lower(FLT)- Fault

See section 2.4 for a description of the various LEDs in L2SW switch.

2.3 Rear Panel of L2SW Switch

The rear panel of L2SW switch has the following connectors on its rear panel as illustrated in Figure 2-2.

- AC power connector (AC power cord comes standard with the unit) – The L2SW switch operates with AC power input from 100VAC to 240VAC with a frequency range of 50 to 60 Hz.
- RS-232 connector – Console port for local management

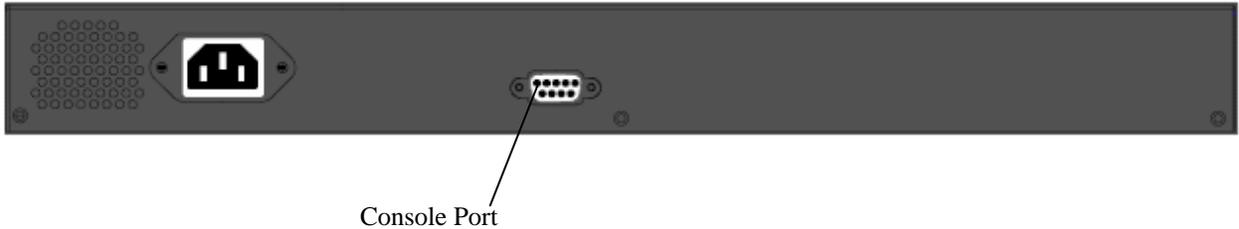


Figure 2-2 Rear Panel of L2SW Switch

2.4 Description of L2SW LEDs

The L2SW switch's port LEDs allow the user to identify:

- Status of ports
- Data transmission or receive activity
- Link speed (10/100/1000Mbps)

	LED-ON (green/Amber)	LED-OFF	Blinking
L2SW Base Board (24 10/100Mbps ports)			
L2SW 10/100 port Upper LED	Link-UP	Link-Down	RX/TX Activity

	LED-ON (green/Amber)	LED-OFF	Blinking
L2SW 10/100 port Lower LED	100 Mbps (Green)	10 Mbps	N/A
L2SW 1000BaseT card			
10/100/1000 Mbps Port Upper LED	Link-UP	Link-Down	RX/TX Activity
10/100/1000 Mbps Port Lower LED	1000 Mbps (Amber)	10/100 Mbps	N/A
L2SW SX or LX card			
1000 Mbps Fiber port Upper LED	Link-UP	Link-Down	RX/TX Activity
1000 Mbps Fiber Port Lower LED	1000 Mbps (Amber)	N/A	N/A
L2SW 100BaseFX card			
100 Mbps Fiber port Upper LED	Link-UP	Link-Down	RX/TX Activity
100 Mbps Fiber port Lower LED	100 Mbps (Amber)	N/A	N/A

Table 2-1: L2SW LED Indications

3. Management Access

L2SW switch provides the network administrator with a set of comprehensive management functions for configuration of the switch. The network administrator has a choice of four types of management interfaces:

- CMLI
- CLI
- WBI
- SNMP

CMLI: Console Menu Line Interface (CMLI) is one of the management interfaces supported by L2SW. The CMLI provides a menu-oriented interface for the user to configure and monitor the L2SW switch. Users can access this interface only via serial port. CMLI interface is being discontinued. Therefore, any new features implemented in L2SW will not be supported using CMLI.

CLI: CLI commands allow the user to configure various L2SW switch features like Spanning Tree Protocol, VLAN, Mac filter, Port security, 802.1x etc and also perform a set of maintenance related functions like users maintenance, log traps, telnet sessions, etc. The L2SW switch can be managed using CLI commands over the dedicated serial interface or via a telnet session.

WBI: L2SW switch can also be managed using a graphical interface using Web browser. A flexible and consistent set of screens, allow the user to configure and manage the resources available on the L2SW switch. In addition, real time events such as alarms and statistics can be monitored using the WBI. Some of the new features such as SNTP, Syslog, Per-port GVRP configuration and Management VLAN are not currently supported through WBI. These features will be supported in a future release of L2SW switch.

SNMP based Management: L2SW switch can also be managed using an external SNMP manager. L2SW switch supports standard MIBs and some proprietary MIBs (enterprise specific extensions to manage the additional features supported by the switch). Any external SNMP based manager, like HP-Openview can be used to configure and manage the L2SW switch. The SNMP agent in the L2SW switch also implements trap functionality so that the SNMP Manager can receive traps from the switch.

Management access methods of L2SW switch enable the network administrator to locally/remotely configure, manage and control using the following access interfaces:

- Serial Port
- Ethernet Line Ports

The Serial port is referred to as out-of-band interfaces, while the Ethernet ports are referred to as in-band management interfaces. While out-of-band interfaces are dedicated for management of L2SW switch, in-band interfaces are used to carry both the user's network traffic as well as the management traffic of the L2SW switch.

3.1 Management Methods Supported by Various Interfaces

3.1.1 Serial Port Interface

- CMLI
- CLI

3.1.2 In-band Network Management Interface

- CLI
- WBI
- SNMP

3.2 Getting Started

The following sections describe setting up of management stations for managing the L2SW switch.

3.2.1 Port Names

The term **port** refers to a physical Fast Ethernet port, a port on the user installable plug-in module card, or a logical trunk in the L2SW switch. Each port is referred to using the following naming convention:

`<slot-number>. <port-number>`

where:

`<slot-number>` represents the port type and `<port number>` represents the number of the physical port within the selected port type. Slot 0 denotes the fixed 24 x 10/100 Fast Ethernet ports, slot 1 represents the user installable plug-in module card, and slot 2 represents the logical trunk port.

`<port-number>` is the number assigned to the port. The range and assignment of port numbers varies by the slot type. The assignment of port numbers by slot number is shown in the following table:

Slot Number	Port Number Assignment (Left to Right)
0 (24 x 10/100 FE)	Upper level: 1 ~ 12 Lower level: 13-24
1 (plug-in module card)	1 2
2 (trunk port)	1 2 3 4 5 6 7

In this document, some alternative notations are also used to refer to the port numbers:

- **PORT#**. Refers to physical ports. For example, PORT8 is equivalent to 0.8, and PORT25 and 26 refer to 1.1 and 1.2 respectively.
- **TRUNK#**. Refers to logical trunk ports. For example, TRUNK3 is equivalent to 2.3.

3.2.2 Terminal Access Setup

L2SW switch has a RS-232 serial interface located on the rear side of the switch. Any terminal with VT100 terminal emulation capabilities can be connected to this port using a standard RS-232 serial cable. The following terminal settings have to be configured for the serial communication to work properly:

- **Baud Rate** = 19200
- **Data Bits** = 8
- **Parity** = none
- **Stop Bits** = 1
- **Flow Control** = none

3.2.3 CLI Syntax Conventions

Command	Description
Command Name and parameters	Text displayed in Bitstream Vera Sans font after the L2SW> prompt must be typed exactly as shown. Following the syntax of a command, an example usage of the command is shown. Output of the command is shown either in <i>Italics</i> or as image of the screen displaying the actual results.
<parameter>	The <> angle brackets indicates that the parameter is required for executing the command
[parameter]	The [] square brackets indicates that the parameter is optional
choice1 choice2	The indicate that only one of the parameter should be entered
ipaddr	This parameter is a valid IP address of four decimal bytes (separated by .), each byte ranging from 0 to 255. The default IP is 0.0.0.0
Macaddr	The MAC address format is six hexadecimal numbers separated by colons, for e.g., 0:20:10:32:0e:40
slot.port	This parameter denotes a valid slot number and a valid port number. For example 0.1 represents slot 0 port 1

3.2.4 Network Port Access Setup

Any of the in-band line ports can be used for management of the L2SW switch.

If DHCP is used to assign IP address for the switch, use the following command to enable DHCP.

```
L2SW> config network protocol <none/dhcp>
L2SW> config network protocol dhcp
```

4. Web Management Function

For management of L2SW via WBI, a Web browser is required. Microsoft Internet Explorer (version 5.0 or higher) is recommended.

If you need to change IP address for the first time, you can use console mode to modify the following default parameters:

IP Address:	172.30.40.145
Subnet Mask:	255.255.255.0
Default Gateway:	172.30.40.2

Assuming that the IP address assigned to the in-band port of the L2SW switch is set to 172.30.40.145, you can use browser to connect to the switch by typing the URL.

After connection is established with the L2SW switch, the browser will display the login screen as shown below:



Figure 4-1: Login

Upon entering a valid user name and password², WBI management interface screen will be presented to the user as shown below:

² Contact technical support or sales representative for the default password

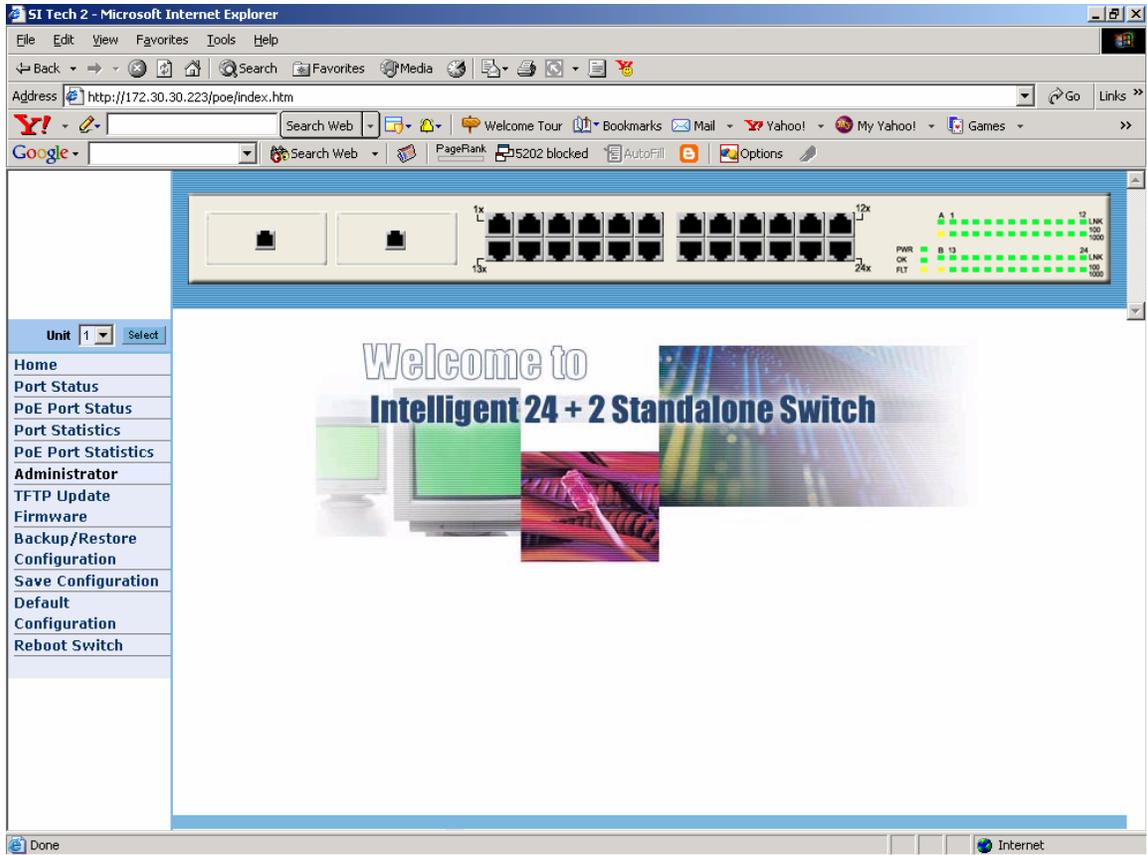


Figure 4-2: WBI Management Interface

The navigation tree displayed on the left side of the browser window should be used for choosing appropriate configuration screens. It is organized with the folders for configuration of different features supported by L2SW switch.

4.1 Port Status

Port Status page displays interface details such as speed, duplex mode, flow control, priority and security information for each port.

Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control(100K)			Priority	Security
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config			Actual				
										Full	Half	Actual	Ingress	Egress			
0.1	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.2	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.3	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.4	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.5	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.6	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.7	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.8	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.9	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.10	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.11	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.12	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.13	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.14	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.15	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.16	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.17	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.18	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.19	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.20	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.21	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.22	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.23	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
0.24	On	On	Up	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	

Figure 4-3: Port Status

State: Port state information is displayed under two columns: **Config** and **Actual**. Configured and actual port state information, are displayed as **On** or **Off**. Note that the port status and port statistics pages are automatically updated after every 5 seconds.

Link Status: Link status information is displayed as **Up** or **Down**. If the link is established between with peering port, the link status information is displayed as **Up**. Otherwise, it is displayed as **Down**.

Auto Negotiation: One of the following three values will be displayed as auto-negotiation mode:

- Auto
- Force
- Nway-force

Speed: Display Speed for port 1- 24 is displayed as 10 Mbps or 100Mbps and speed for Port 25-26 is displayed as 10, 100 or 1000Mbps.

Duplex status: Full (full-duplex) or Half (half-duplex) mode.

Flow Control : Display the flow control status as **On** or **Off**. The flow control status is displayed under the columns **Full** and **Half**.

Full : Send/Process PAUSE frames to exercise flow control

Half : Use Jabber to exercise flow control in half-duplex mode

Rate Control : Display the rate control setting of the Ingress and Egress side of each port.

Ingr: Display the effective ingress rate for the port

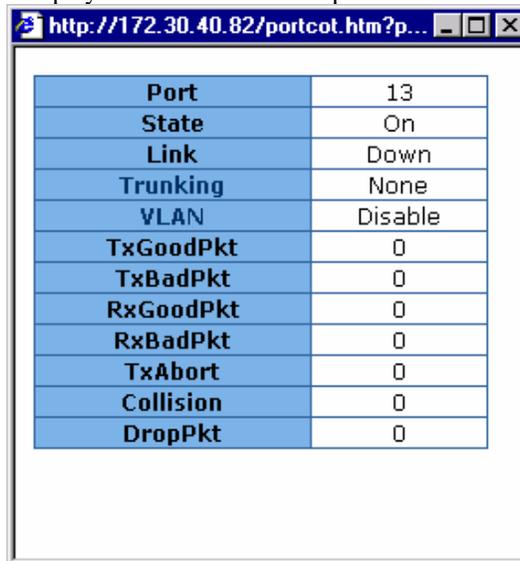
Egr: Display the effective egress rate for the port

Priority: Display the port's static priority as **High** or **Low** or **Disable**.

Port Security: Security status of a port is displayed as **On** (Enabled) and **Off** (Disabled)

Values displayed under the column **Config** are the values configured by the user and the values displayed under the column **Actual** are the values derived as a result of negotiation with the corresponding partner of a port.

User can see an individual port status by clicking on any of the ports in L2SW image displayed on top of the page. The following web page is used to display status of the selected port.



The screenshot shows a web browser window with the address bar containing the URL <http://172.30.40.82/portcot.htm?p...>. The main content area displays a table with 12 rows and 2 columns. The first column lists various port status metrics, and the second column shows their corresponding values.

Port	13
State	On
Link	Down
Trunking	None
VLAN	Disable
TxGoodPkt	0
TxBadPkt	0
RxGoodPkt	0
RxBadPkt	0
TxAbort	0
Collision	0
DropPkt	0

Figure 4-4: Individual Port Status

4.2 Port Statistics

Port Statistics page displays information such as interface state, link status, transmission and reception statistics for each port.

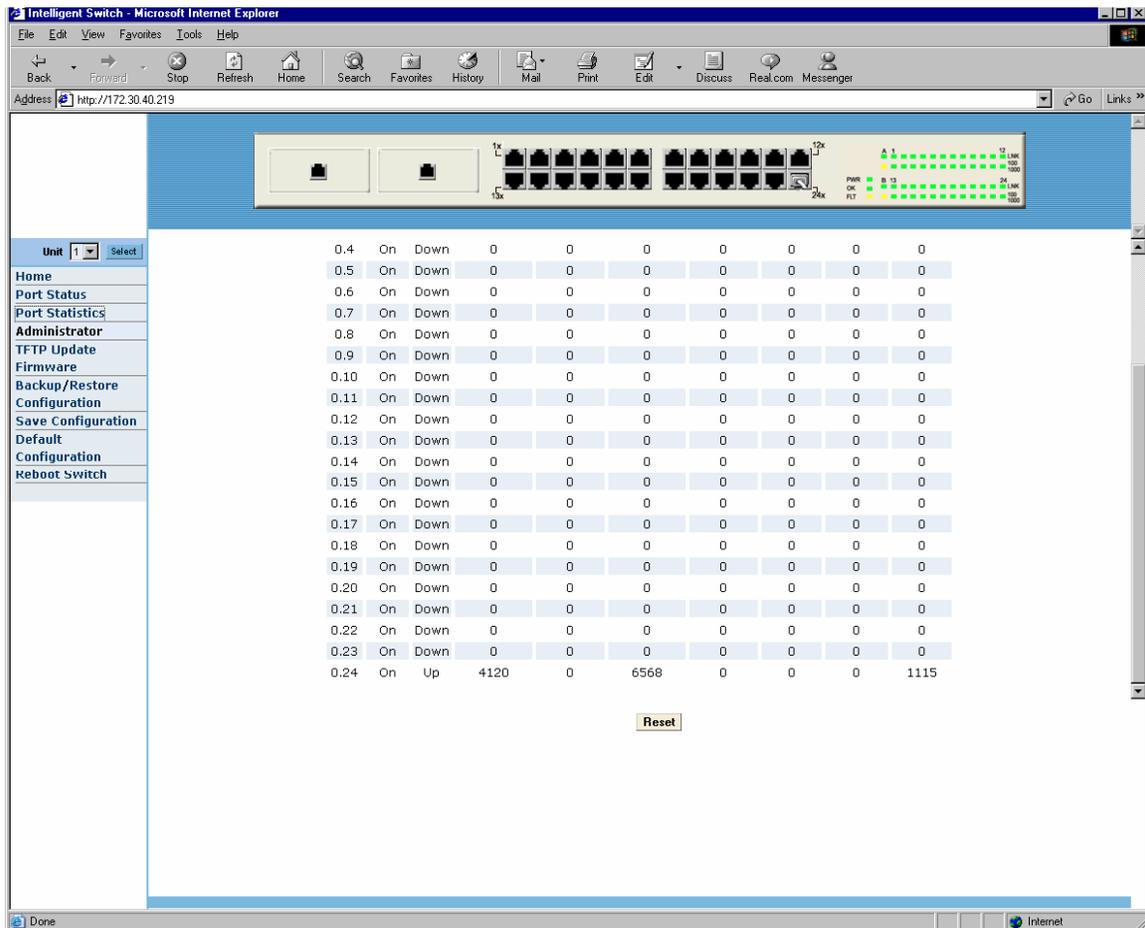


Figure 4-5: Port Statistics

Use **Reset** button to clear the port statistics.

4.3 Administrator

This link on the navigation tree allows the user to configure the following features:

- Stacking
- IP address
- Switch settings
- Console port information
- Port controls
- Trunking
- Filter database
- VLAN configuration
- Spanning tree
- Port Sniffer
- SNMP
- Security Manager
- TFTP Update Firmware
- Configuration Backup
- Reset System
- Reboot

4.3.1 Stacking

Stacking capability allows the user to manage a group of up to 8 switches from a single management point. This page provides stack configuration to set stacking parameters on the master unit and stack status to view the system MAC address, stack port, software version and status for each unit in the stack when stacking is enabled. And on the left side of page, user can access slave units by clicking unit ID drop down list.

To enable stacking feature, configure an IP address on master unit and open this page, select **Enable** option in Admin Mode tab and click on Apply. To disable stacking feature, select **Disable** option in Admin Mode tab and click on Apply.

To configure the number of switches that participate in the stacking configuration, enter a decimal number between 2 and 8, then click on Apply. Default value is 8. Stacking maximum units configuration should match with the number of units currently connected via stack up link ports and stack down link ports.

To view the stacking status, check stack status part on the page.

To access slave units in the stack, click unit ID drop down list, choose the unit ID and click on select

tab.

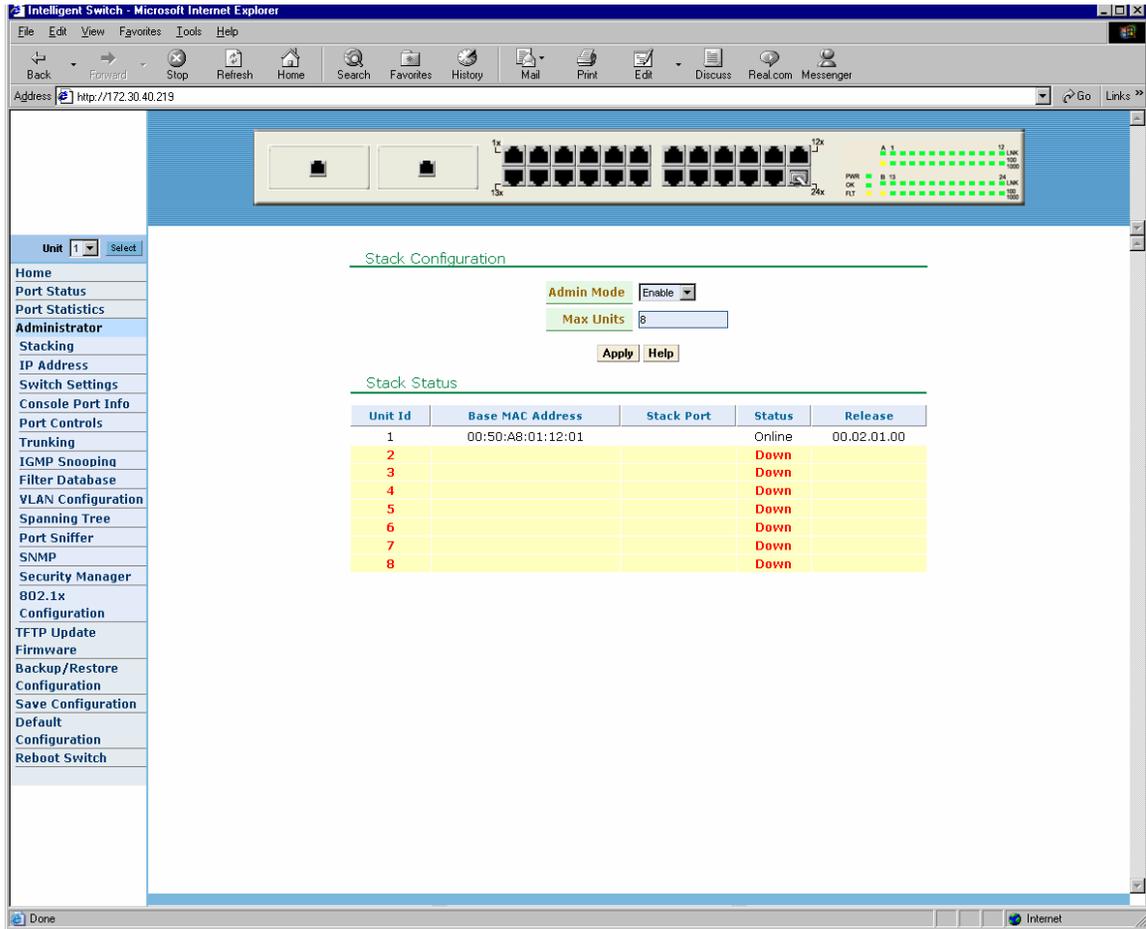


Figure 4-6: Stacking Configuration

4.3.2 IP Address

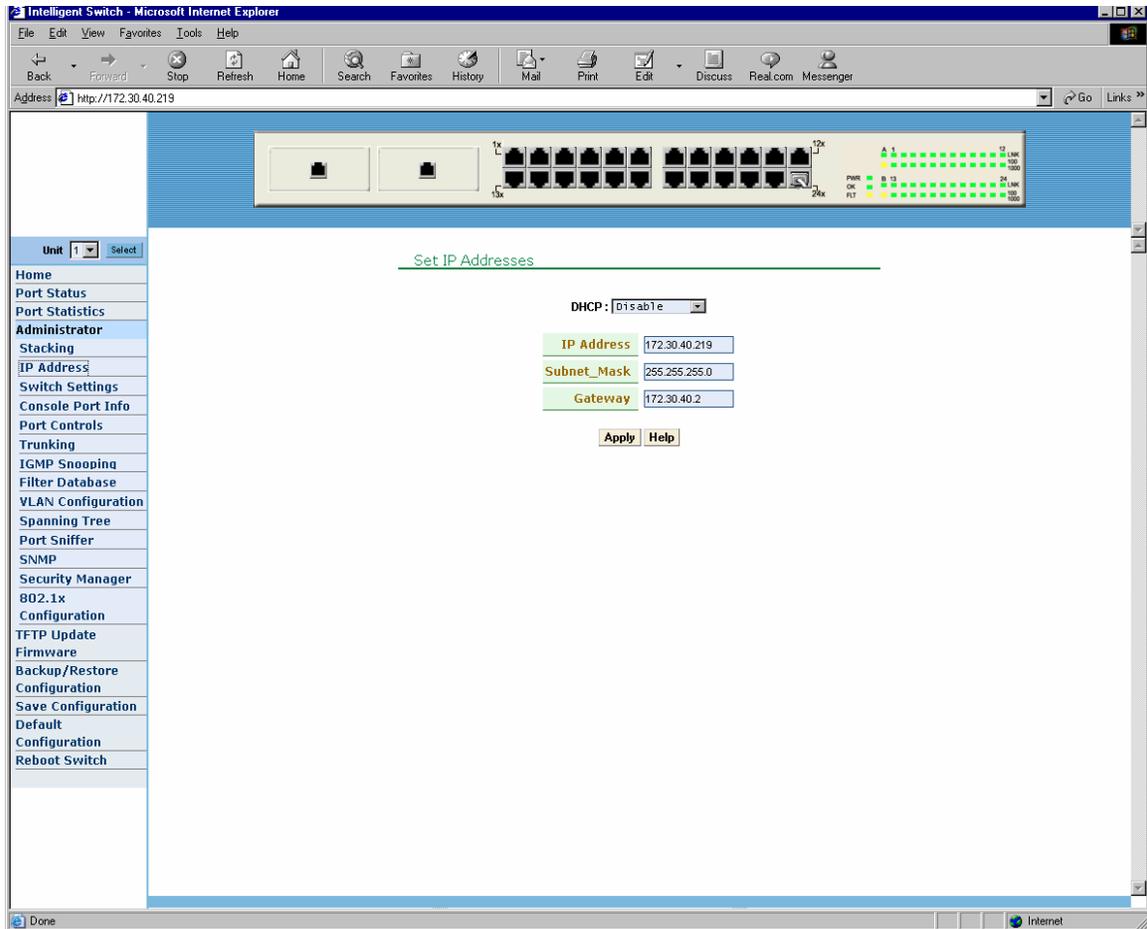


Figure 4-7: IP Address

IP Address for the switch can be configured either statically or obtained dynamically from a DHCP server. To automatically obtain the IP address using DHCP, select **Enable** option in DHCP tab and click on **Apply**.

To statically configure the IP address, select **Disable** in DHCP tab; enter the IP address, subnet mask and default gateway parameters and click on **Apply**.

4.3.3 Switch Setting

4.3.3.1 Basic

Various factory assigned parameters of the switch, such as, MAC address, Firmware/ASIC version, Serial Number etc. are displayed in this page.

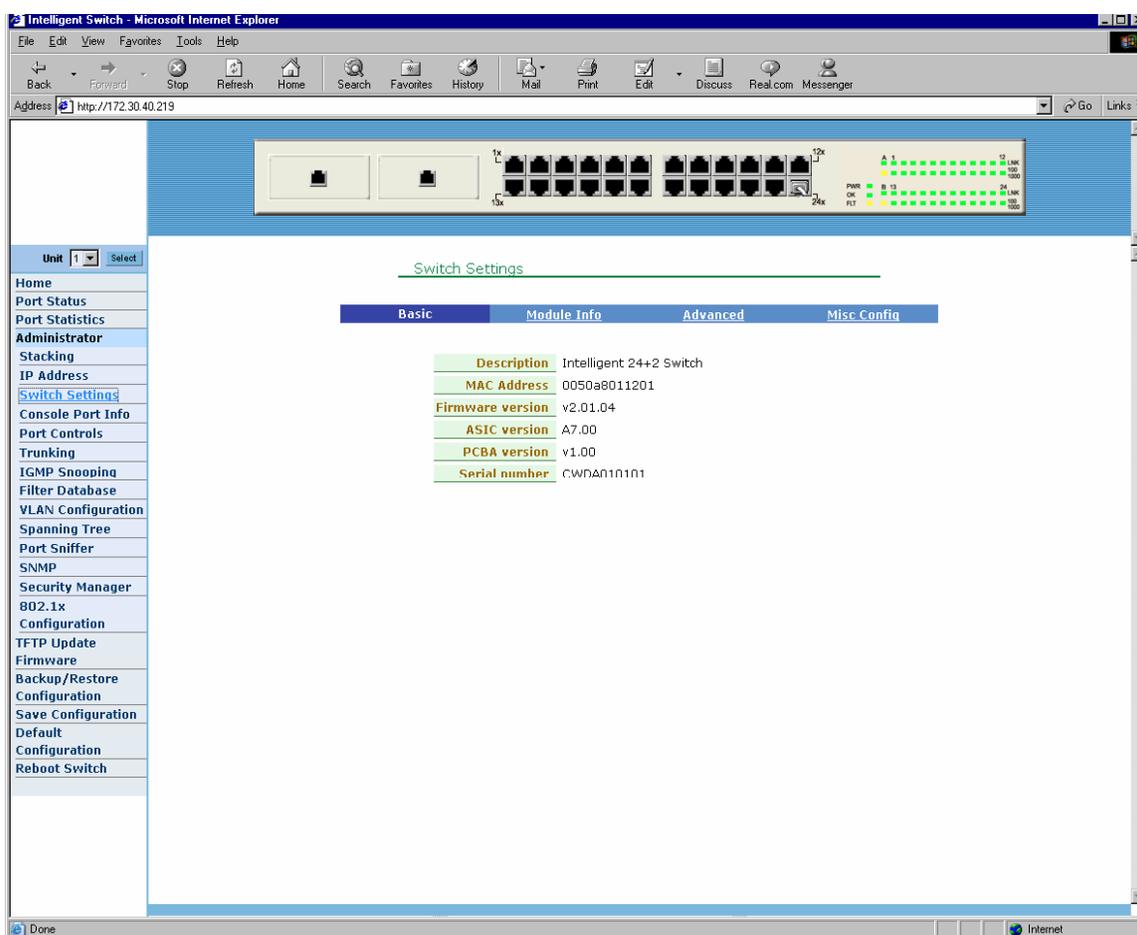


Figure 4-8: Switch Settings/Basic Information

Description:	Displays name of device
MAC Address: (default)	Displays unique hardware address assigned by manufacturer
Firmware Version:	Displays switch's firmware version.
ASIC Version:	Displays switch's Hardware version.
PCBA version:	Displays board number.

Serial number: Displays serial number assigned by manufacturer.

4.3.3.2 *Module Info*

Replaceable feature cards are displayed in this page.

	TYPE	DESCRIPTION
Module1	1000TX	070-00018-00
Module2	1000FX_DULMODE	070-00019-00

Figure 4-9: Switch Settings/Module Information

Type and description of the plug-in module cards are displayed in this page.

4.3.3.3 *Advanced Settings*

Advanced Settings of the switch such as MAC Address Age-out time, Broadcast Storm Filter, 802.1p Priority are displayed in this Page. User can change the values of these settings (e.g., Age-out time) by editing the values displayed inside the box.

Switch Settings

Basic	Module Info	Advanced	Misc Config
-------	-------------	----------	-------------

MAC Table Address Entry
Age-Out Time: seconds (300~765, must multiple of 3)
Max bridge transmit delay bound control:

 Enable Low Queue Delay Bound ----- Max Delay Time: (1~255, 2ms/unit)
Broadcast Storm Filter Mode:

Priority Queue Service:

802.1p Priority
 First Come First Service
 All High before Low
 WRR ----- High weight: Low weight:

Qos Policy: High Priority Levels
 Level0 Level1 Level2 Level3 Level4 Level5 Level6 Level7

Figure 4-10: Advanced Switch Settings

MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 10 ~765 seconds. Default is 300 seconds.

Max bridge transmit delay bound control : Limit the packets queuing time in switch. If enabled, the packets queued which exceed the delay bound setting will be dropped. This valid values are 1sec, 2 sec, 4 sec and off.

Enable Low Queue Delay Bound: Limit the low priority packets queuing time in switch.

If the low priority packet queued up in switch exceed Max Delay Time, it will be dropped. The valid range is 1~255 ms.

NOTE: Enable **Max bridge transmit delay bound control** before enabling **Low Queue Delay Bound**, because this parameter is valid only when **Max bridge transmit delay bound control** is enabled.

Broadcast Storm Filter: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by

broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value are 5%, 10%, 15%, 20%, 25% and off.

Priority Queue Service Settings: Priority queue settings part of the screen allows the user to choose processing method for packets queued for a port.

First Come First Service: The sequence of packets sent is dependent on order of arrival.

All High before Low: The high priority packets are sent before low priority packets.

WRR: Weighted Round Robin. Select the preference given to packets in the switch's high-priority and low priority queue.

These options represent the number of high priority packets sent before one low priority packet is sent. For example, 5 High: 2 Low means that the switch sends 5 high priority packets before sending 2 low priority packet.

QoS Policy: High Priority Levels: 0~7 priority level can map to high or low queue.

4.3.3.4 Miscellaneous Settings

Other features essential to the switch such as 802.1x protocol, Hash Algorithm, IFG compensation are displayed on this page.

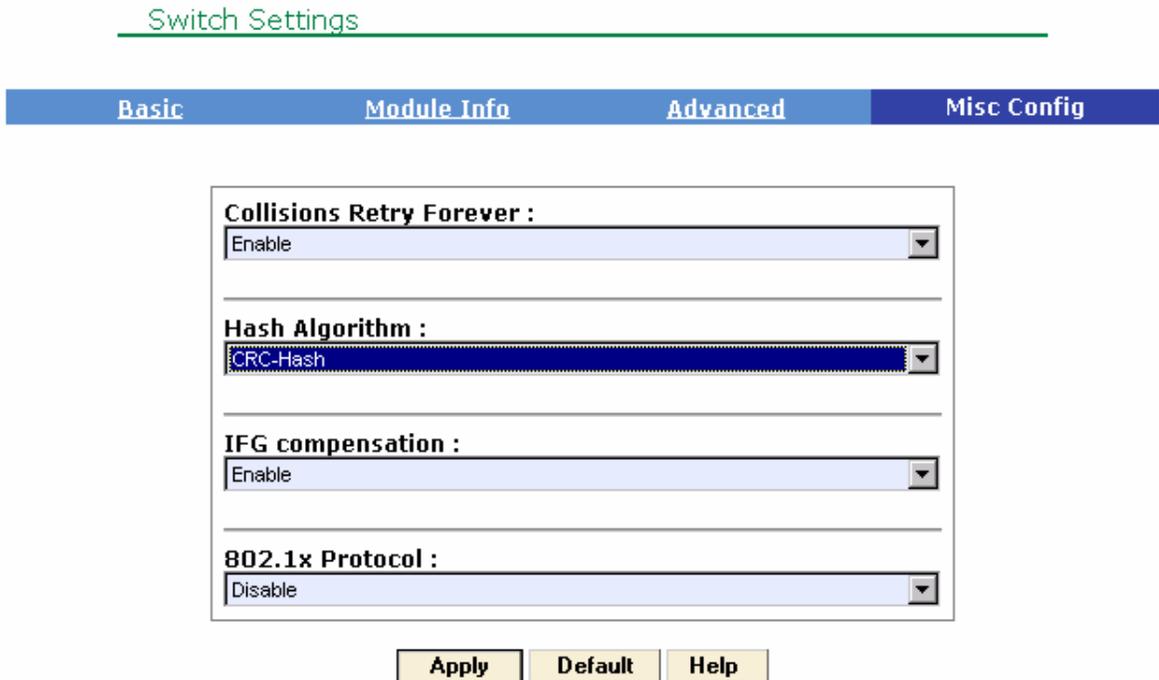


Figure 4-11: Miscellaneous Switch Settings

Collisions Retry Forever: Enable/disable collisions retry forever.

Hash Algorithm: CRC-hash/Direct-map hash algorithm. The default setting should be changed only under special circumstances.

IFG Compensation: Enable/disable IFG Compensation³. The default setting should be changed only under special circumstances.

802.1x protocol : Enable/disable 802.1x protocol.

4.3.4 Console Port Information

Console is a standard UART interface to communicate with Serial Port. Various parameters, such as Baudrate, Parity Check, Flow control etc are displayed in this page.

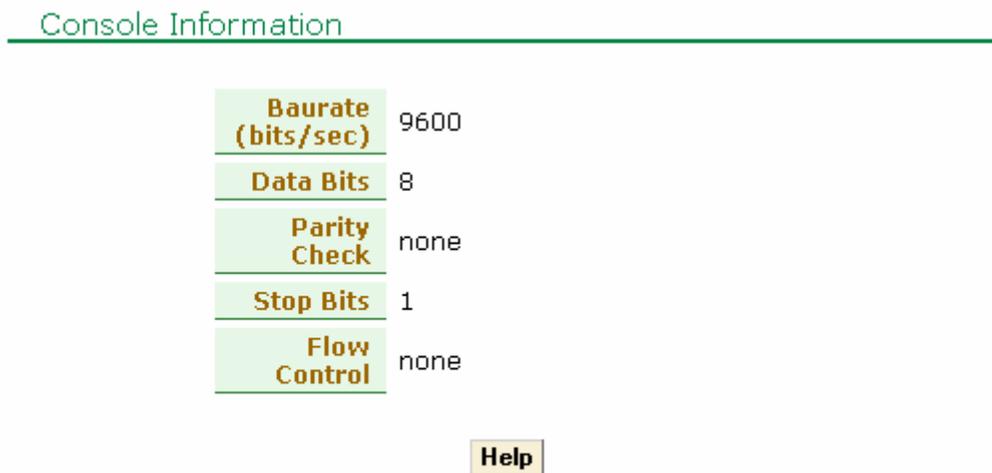


Figure 4-12: Console Information

Windows hyper-terminal program can be used to connect to the switch. Make sure the baud rate and stop bit settings on the Windows hyper-terminal match the following settings for the console port.

- **Baudrate:** 19200
- **Data bits:** 8
- **Parity:** none
- **Stop bits:** 1
- **Flow control :** none

4.3.5 Trunking

L2SW supports both static and dynamic trunking using the Link Aggregation Control Protocol

³ For an brief explanation on IFG, read section 6.15.

(LACP). LACP provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network by combining two or more lower speed ports.

 **LACP operation requires full-duplex mode, for more detail information refer to IEEE 802.3ad standard.**

4.3.5.1 Aggregator Settings

This page is used to create a link aggregation across two or more ports.

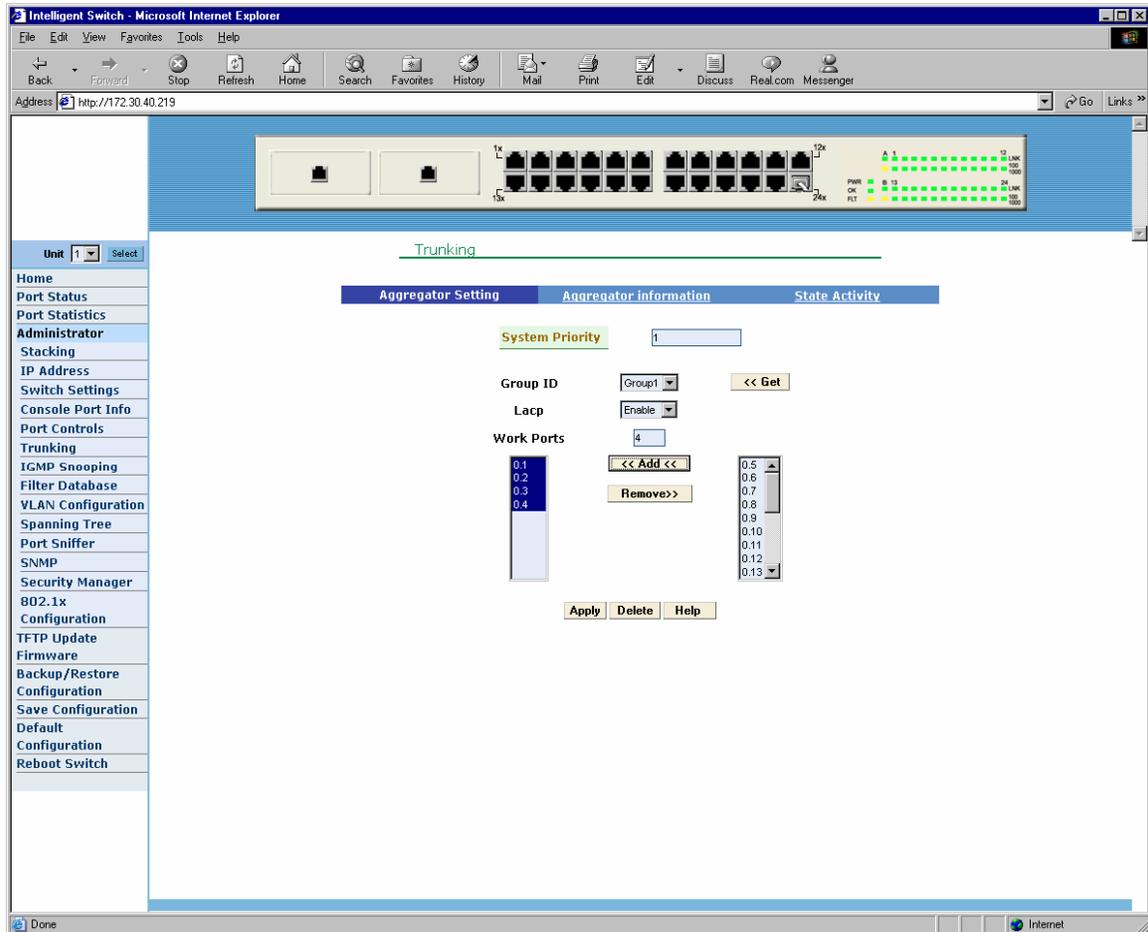


Figure 4-13: Trunking

To create a link aggregation group with two or more ports, the following parameters are used:

System Priority: This value is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.

Group ID: Seven trunk groups are available for configuration. Choose the "group id" and click "Get"

to configure a Link aggregation group.

LACP: If enabled, the group is LACP static trunking group. If disabled, the group is local static trunking group. All ports support LACP dynamic trunking group. If the switch is connected to another device that also supports LACP, the LACP dynamic trunking group will be created automatically.

Work ports: A maximum of four ports can be aggregated within a trunking group. If the number of ports configured to be part of a LACP static trunking group exceeds the maximum number, the excess ports are moved to a standby state and would be able to join the trunking group, if any of the working ports in the group fails. If the local static trunking group is used then the number of group member ports must be as same as the working ports.

Select the ports to join the trunking group by selecting the ports from the ports list. A maximum of four ports can be aggregated within a trunking group.

If LACP is enabled, you can configure LACP Active/Passive status in each port on State Activity page. To complete the LACP configuration, click the `Apply` button.

4.3.5.1.1 Trunking Configuration

This page displays the current LACP status. If LACP is enabled, the group is LACP trunking group. Otherwise, the group is Local static trunking group.

The following are the various scenarios of LACP status:

Scenario 1: LACP is disabled and there are no active links.



The following information provides a view of LACP current status.

NO GROUP ACTIVE

Figure 4-14: LACP disabled

Scenario 2: LACP Enabled with no active links

The following information provides a view of LACP current status.

Static Trunking Group	
Group Key	2
Port_No	15 16 17 18

Static Trunking Group	
Group Key	3
Port_No	5 6

Figure 4-15: Static Trunking Groups

Scenario 3: LACP is enabled with active links

Trunking

Aggregator Setting	Aggregator information	State Activity
--------------------	------------------------	----------------

The following information provides a view of LACP current status.

Group1						
Actor				Partner		
Priority	1			1		
MAC	0050a8806000			0050a8009988		
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT1	513	1	selected	PORT1	514	1
PORT2	513	1	selected	PORT2	514	1
PORT3	513	1	selected	PORT3	514	1
PORT4	513	1	selected	PORT4	514	1

Static Trunking Group	
Group Key	2
Port_No	15 16 17 18

Static Trunking Group	
Group Key	3
Port_No	5 6

Figure 4-16: Actor and Partner Group

The following page displays the state of each LACP and it indicates whether that port is in active or passive state.

Aggregator Setting		Aggregator information		State Activity	
Port	LACP State Activity	Port	LACP State Activity		
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active		
3	<input checked="" type="checkbox"/> Active	4	<input checked="" type="checkbox"/> Active		
5	N/A	6	N/A		
7	N/A	8	N/A		
9	N/A	10	N/A		
11	N/A	12	N/A		
13	N/A	14	N/A		
15	<input checked="" type="checkbox"/> Active	16	<input checked="" type="checkbox"/> Active		
17	<input checked="" type="checkbox"/> Active	18	<input checked="" type="checkbox"/> Active		
19	N/A	20	N/A		
21	N/A	22	N/A		
23	N/A	24	N/A		
25	N/A	26	N/A		

Figure 4-17: State Activity

Active (select): The switch automatically sends LACP protocol packets through this port.

Passive (no select): The switch does not automatically send LACP protocol packets through this port, and responds only if it receives LACP protocol packets from the peer device.

A link having either two active LACP ports or one active port can perform dynamic LACP trunking. Switches attached to a link with two passive LACP ports will not perform dynamic LACP trunking because both switches are waiting for LACP protocol packet from its peer.

4.3.6 IGMP Snooping and Filter Database

The L2SW supports IP multicast, user can enable/disable IGMP Snooping, Static MAC Addresses and MAC filtering using this page.

4.3.6.1 IGMP Snooping

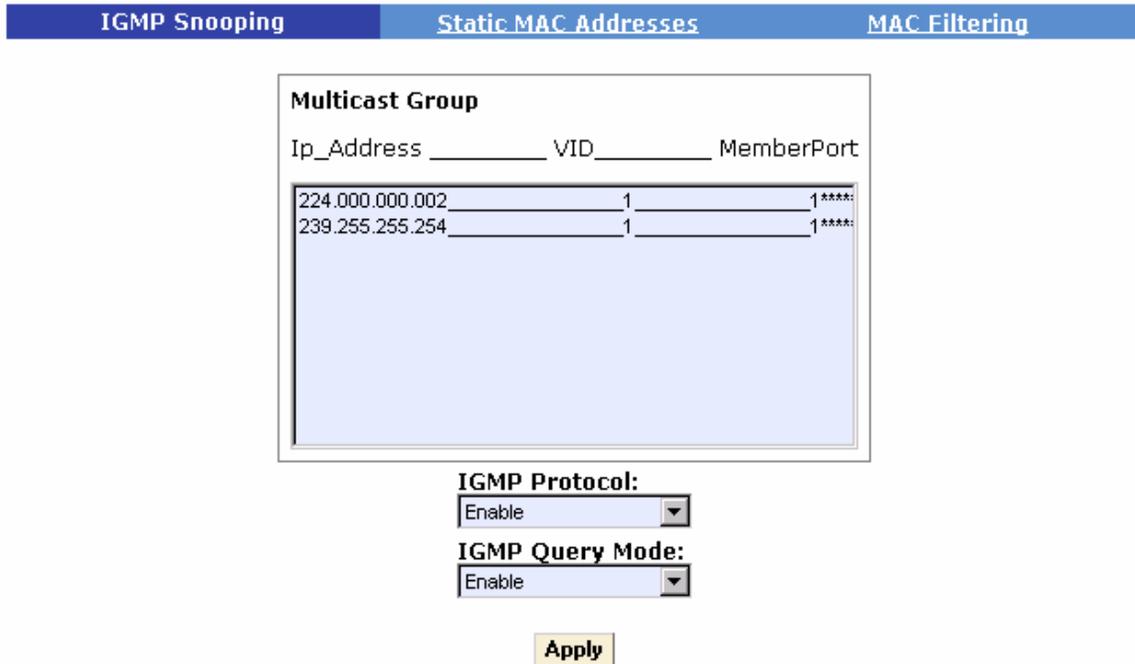


Figure 4-18: IGMP Snooping

The Internet Group Management Protocol (IGMP) is a multicast protocol of the Internet Protocol (IP) suite. Multicast traffic is propagated through the network using switches, routers, and hosts that support IGMP and other multicast protocols. Enabling IGMP snooping allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of messages:

The IGMP query mode can be enabled or disabled. If IGMP query mode is disabled, switch will perform passive snooping of IGMP Query/Report messages passing thru the switch. If enabled, the switch will perform IGMP query functions if there is no other device in the VLAN such as a multicast router is available to perform query functions.

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group. If IGMP query mode is disabled, switch will perform passive snooping of IGMP Query/Report messages passing thru the switch. If enabled, the switch will perform IGMP query functions if there is no other device in the VLAN, such as a multicast router is available to perform query functions.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit to be a member of a specific multicast group.

Table 4-1: IGMP Snooping

4.3.7 Static MAC Address

Static MAC address remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again.

This page enables the user to add/delete a MAC address.

[Forwarding and Filtering](#)

IGMP Snooping **Static MAC Addresses** MAC Filtering

Static addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address	PORT	VID
-------------	------	-----

Mac Address

Port num

Vlan ID

Figure 4-19: Static MAC Address

To add a Static MAC Address, execute the following steps:

1. From the main menu, click administrator → Filter Database → Static MAC Address.
2. In the MAC address box, enter the destination MAC address of the frames which should be forwarded by the switch to a fixed port (also defined in this screen)
3. In the Port Number box, enter a port number.
4. If tag-based (IEEE 802.1Q) VLANs are set up on the switch, VLAN IDs are associated with individual VLANs. Type the VID (tag-based VLANs) to associate the VLAN with the MAC address entered earlier.

Click **Add** button

4.3.8 MAC Filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. For example, if network is congested because of heavy bursts of traffic from one particular MAC address, using this page, user can filter all traffic transmitted from or to that MAC address. This type of filtering would enable the network administrator to restore network traffic flow while troubleshooting the problem.

Forwarding and Filtering

IGMP Snooping Static MAC Addresses **MAC Filtering**

Specify a MAC address to filter.

Mac Address

Vlan ID

Figure 4-20: MAC Filtering

To add MAC filter, use the following procedure:

1. In the MAC Address box, enter the MAC address that needs to be filtered.
2. If tag-based (802.1Q) VLANs are set up on the switch, type the VID in the VLAN ID box to associate with the MAC address defined earlier
3. Click the **Add** button.
4. If a MAC address filter has to be deleted, enter the MAC address to be deleted and then click the **Delete** button.

4.3.9 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows the user to isolate network traffic so that members of a VLAN receive traffic, only from the members of the same VLAN. Basically, creating a VLAN is logically equivalent of connecting a group of network devices to a separate Layer 2 switch even though all the network devices are still plugged into the same switch physically.

The L2SW supports port-based, 802.1Q (tagged-based) and protocol-based VLAN. In the default

configuration, VLAN support is disabled.

VLAN Configuration

VLAN Operation Mode:
802.1Q

Enable GVRP Protocol

Basic Port VID

VLAN Information

DEFAULT __1
v1 __2

Add Edit Delete PrePage NextPage Help

Figure 4-21: VLAN configuration

! *If VLAN mode is changed, you have to reboot the switch to make the change effective.*

To enable GVRP mode, Click on the box marked **Enable GVRP Protocol**⁴.

In Port-based VLAN, packets can be exchanged only between devices attached to the ports that are members of the same VLAN group. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

⁴ It is recommended that GVRP configuration is done only through CLI interface since per-port GVRP configuration is not currently supported through WBI or CMLI.

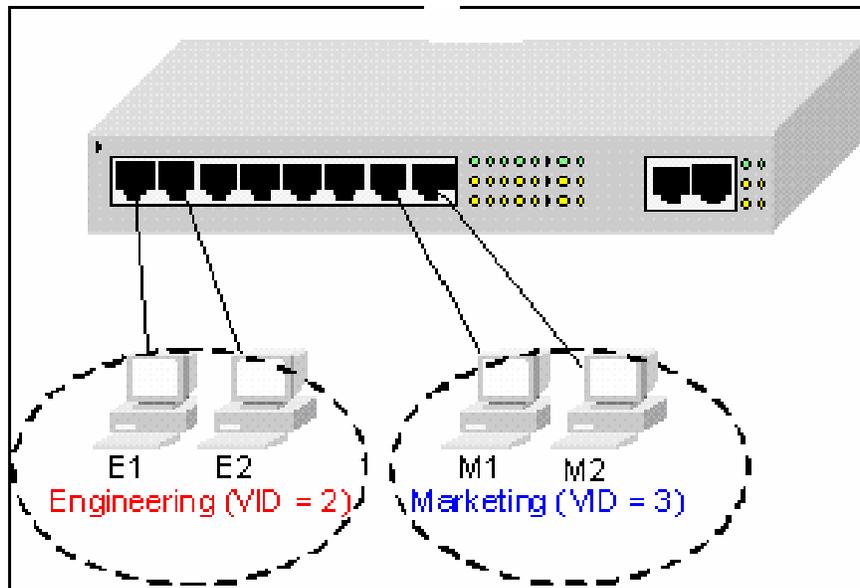


Figure 4-22 Port-based VLAN ID

Tagged-based VLAN is an IEEE 802.1Q standard. It is possible to create a VLAN across devices from different switch vendors using this standard. IEEE 802.1Q VLAN inserts a “tag” into the Ethernet frames, which contains the VLAN identifier (VID).

In order for an end station to send packets to different VLANs, it has to be either capable of tagging packets with VLAN ID or get attached to a VLAN-aware bridge/switch that is capable of classifying and tagging the packets with different VLAN ID based on not only default Port-based VLAN ID (PVID) but also other information about the packet, such as the protocol.

L2SW supports protocol-based VLAN classification and tagging based on layer 2 packet formats used by selected popular protocols, such as Novell IPX and AppleTalk’s EtherTalk.

Port VLAN ID (PVID) defines the VLAN ID that will be assigned to untagged frames received from a given port. For example, if port 10’s PVID is 100, all untagged packets received on port 10 will belong to VLAN 100. The default PVID setting for all ports is VID 1.

This feature is useful for accommodating devices that user wants to participate in the VLAN but that don’t support tagging. Only one untagged VLAN is allowed per port. In other words, there can be only one PVID per port.

Ingress Filtering: Ingress filtering feature is used to filter tagged frames received through a port with VLAN ID that doesn’t match any of the VLANs in which the port participate in. Disabling this setting will cause all frames to be forwarded, regardless of the port’s VLAN setting.

GVRP (GARP VLAN Registration Protocol) allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, the device can send a GVRP request using the VID of a VLAN defined on the switch, and it will automatically add that device to the existing VLAN.

4.3.9.1 Port Based VLAN

In Port based VLAN, traffic is forwarded to the member ports of the same VLAN group. Use the following Port-based VLAN configuration web page, to configure Port based VLAN.

VLAN Configuration

VLAN Operation Mode:
Port Based VLAN

Enable GVRP Protocol

VLAN Information

--

Add Edit Delete PrePage NextPage Help

Figure 4-23: Port based VLAN

To create a port based VLAN use the following procedure:

1. Click **add** to create a new VLAN group.
2. Enter the VLAN name, group ID and select the members for the new VLAN.
3. Click **apply** button.
4. If there are many groups that span over the limit of one page user can click the “NextPage” to view other VLAN groups.

NOTE: If the trunk groups exist, user can see it (e.g.,:TRK1,TRK2.....) in select menu of ports. Users can configure Trunk ports to be a member of a VLAN.

PVIDs cannot be assigned arbitrarily. Instead, all the PVIDs must take on values within the same PVID set. The following list depicts the relation between the PVID sets and value of PVID.

- PVID Set 0. PVID range: 0 - 255

- PVID Set 1. PVID range: 256 - 511
- PVID Set 2. PVID range: 512 - 767
- PVID Set 3. PVID range: 768 - 1023
- PVID Set 4. PVID range: 1024 - 1279
- PVID Set 5. PVID range: 1280 - 1535
- PVID Set 6. PVID range: 1536 - 1791
- PVID Set 7. PVID range: 1792 - 2047
- PVID Set 8. PVID range: 2048 - 2303
- PVID Set 9. PVID range: 2304 - 2559
- PVID Set 10. PVID range: 2560 - 2815
- PVID Set 11. PVID range: 2816 - 3071
- PVID Set 12. PVID range: 3072 - 3327
- PVID Set 13. PVID range: 3328 - 3583
- PVID Set 14. PVID range: 3584 - 3840
- PVID Set 15. PVID range: 3841 – 4095

4.3.9.2 802.1Q (Tag based) VLAN

Tag-based VLANs are based on IEEE 802.1Q specifications. Traffic is forwarded to VLAN member ports based on identifying VLAN tags in data packets.

User can use the following web page to configure 802.1Q VLAN

VLAN Configuration

VLAN Operation Mode:
802.1Q

Enable GVRP Protocol



VLAN Information

DEFAULT __1

Add Edit Delete PrePage NextPage Help

Figure 4-24: 802.1Q based VLAN

To configure a tag-based VLAN, use the following procedure:

1. Create a VLAN and add tagged member ports to it.
2. From the main menu, click VLAN Configuration then click 802.1Q VLAN Operation Mode.
3. Click **Add** button.
4. Type a name for the new VLAN.
5. Type a VID (between 2-4094). The default value is 1.
6. Select protocol VLAN. The default value is None.
7. From the Available ports box, select ports to add to the switch and click add.
8. Click **Next**.

By adding ports to the 802.1Q VLAN user is also enabling tagging of frames leaving from those ports.

4.3.9.3 VLAN Configuration

The following are the steps involved in configuring a VLAN:

Basic		Port VID	
VLAN Name:	<input type="text"/>		
VID:	<input type="text" value="1"/>		
Protocol Vlan:	<input type="text" value="NONE"/>		
<div style="border: 1px solid black; padding: 2px;"> PORT1 PORT2 PORT3 PORT4 PORT5 PORT6 PORT7 PORT8 PORT9 PORT10 PORT11 PORT12 </div>	<input type="button" value="Add >>"/> <input type="button" value="<< Remove"/>		<div style="border: 1px solid black; height: 100px; width: 100%;"></div>
<input type="button" value="Next"/> <input type="button" value="Help"/>			

Figure 4-25: Create VLAN

Step I: Create a VLAN and add tagged member ports to it.

1. From the main menu, click administrator → VLAN configuration, click Add then user will see the following page:
2. Type a name for the new VLAN.
3. Type a VID (between 2-4094). The default value is 1.
4. If you are configuring Protocol VLAN, choose the protocol type. Otherwise, set protocol type to None .
5. From the Available ports box, select ports to add to the switch and click “Add >>”. If the trunk groups exist and if trunks ports have to be configured as part of a VLAN, click on the Trunk group ID instead of port number.
6. Click Next.
7. Set the outgoing frames as Tag or Untag(ged). Then click Apply.

Tag: outgoing frames with VLAN-Tagged.

Untag: outgoing frames without VLAN-Tagged.

VLAN Name:	v1		
VLAN ID:	2		
Tag Member			
PORT1	Tag	PORT2	Tag
PORT3	Tag	PORT4	Untag
PORT5	Untag		
Apply			

Figure 4-26: Add Ports to VLAN

Step II: Configure port VID settings

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

Basic		Port VID	
For each port, assign a Port VLAN ID (1~255) for untagged traffic, and click Apply.			
Ingress Filtering Rule 1		(Forward only packets whose VID = Port's configured VID)	
Ingress Filtering Rule 2		(Drop Untagged Frame)	
Port No	PVID	Ingress Filtering Rule 1	Ingress Filtering Rule 2
<div style="border: 1px solid black; padding: 2px;"> PORT1 PORT2 PORT3 PORT4 </div>	1	Enable	Disable
<input type="button" value="Apply"/> <input type="button" value="Default"/> <input type="button" value="Help"/>			

Port No	PVID	Ingress Filtering Rule 1	Ingress Filtering Rule 2
PORT1	1	ENABLE	DISABLE
PORT2	1	ENABLE	DISABLE

Figure 4-27: Configure VID

Set the port VLAN ID (PVID) assigned to untagged traffic on a given port. This feature is useful for accommodating devices that user wants to participate in the VLAN but don't support tagging. L2SW each port allows user to set one PVID per port. The range is 1~255, default PVID value is 1. The PVID must be same as the VLAN ID, that the port belongs to VLAN group, or the untagged traffic will be dropped.

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. L2SW have two ingress filtering rule as follows:

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

Ingress Filtering Rule 2: Drop Untagged Frame.

4.3.10 Spanning Tree

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. STP is a bridge-based mechanism for providing fault tolerance on networks by determining alternate paths for bridged traffic when a failure is encountered. STP enables user to implement parallel paths for network traffic and ensure the following:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main traffic paths fail.

One of the major problems with the Spanning Tree Protocol is the convergence time (i.e., time taken to recompute the STP whenever a topology change occurs). The convergence could be anywhere from 30Secs to one or two minutes. This type of delay is unacceptable in networks where time sensitive and mission critical traffic flows through the switch. Rapid Spanning Tree Protocol (RSTP), specified by IEEE802.1w, addresses this specific problem and allows network to converge typically within a couple of seconds whenever a topology change occurs in the network. RSTP specification also defines backward compatibility rules a port is connected to a legacy 802.1D bridge.

Apart from faster convergence time, there are some additional differences between STP and RSTP. STP allows a port to remain in one of the following five states:

- **Di sabl ed**
- **Bl ocki ng**
- **Li steni ng**
- **Learni ng**
- **Forwardi ng**

Switch will discard packets received through a port in **Di sabl ed**, **Bl ocki ng** or **Li steni ng** states. Ports in **Forwardi ng** state are assigned the role of a “**Root**” port or a “**Desi gnated**” port. **Root** port is a forwarding port on a switch which connects to the next switch in the path towards the root of the spanning tree can be reached. **Desi gnated** port on a LAN is the port through which all other switches or hosts on that LAN can reach the root of the spanning tree. RSTP reduces the number of states of a port to three states:

- **Di scardi ng**
- **Learni ng**
- **Forwardi ng**

To assist in faster convergence, RSTP also introduced the following additional roles for a port.

- **Al ternate Port**
- **Backup Port**
- **Edge Port**

Al ternate Port is another root port on a switch through which the root of the spanning tree can be reach. If the Root port on a switch fails, the traffic will be switched over quickly to the Alternate port. **Backup port** on LAN acts as a backup to the Designated port on the same LAN. If the Designated port fails, the Backup port will quickly take over the role of the Designated port for that LAN. **Edge port** is a port that is typically connected to an end system such as PC or server. **Edge ports** quickly transition into Forwarding state and remain in forwarding state regardless of topology changes. The link connecting the Edge port can be a point-to-point link or shared link. Generally an Edge port operating in full-duplex mode can be considered to be connected on a point-to-point link.

Both STP and RSTP consider all VLANs to be part of the same Spanning Tree. In some applications, it is desirable to have separate spanning tree based on the VLAN association of the ports. Some

vendors introduced the concept of Per-VLAN Spanning Tree (PVST) which allows the switch to maintain a separate spanning tree instance for each VLAN. This may be too burdensome on the switch. Multiple-Spanning Tree Protocol (MSTP), as specified in IEEE 802.1s, addresses this problem by mapping several VLANs into a single spanning tree instance. This would reduce the number of spanning tree instances maintained within each switch.

Each switch running MSTP is a member of one or more MST Regions. Each MST Region can support more than one MST instances. MST regions are identified by MST configuration, which consists of a configuration name, configuration revision number and a VLAN mapping table which maps each VLAN (0-4096) onto an MST instance. Two switches are said to belong to the same MST Region provided the two switches have a common MST configuration.

Every MST Bridge within a MST Region maintains two types of spanning trees:

- **I n t e r n a l S p a n n i n g T r e e (IST)**
- **O n e o r m o r e M u l t i p l e S p a n n i n g T r e e I n s t a n c e s (MSTI)**

IST is also referred to as an MSTI with instance value 0 and is the only spanning-tree instance that sends and receives BPDUs. All of the other spanning-tree instances information is contained in M-records which are encapsulated within MSTP PDUs. IST is the spanning tree that connects all the switches within a MST Region and the IST Root is also referred to as the IST Master. A **C o m m o n a n d I n t e r n a l S p a n n i n g T r e e (CIST)** is a collection of ISTs in each MST Region and is used to connect all the MST Regions together into a single spanning tree.

L2SW supports 8 user defined MSTIs per MST Region. In the current software release, L2SW supports only one MST Regions per switch. In L2SW IST and CIST refer to one and the same.

4.3.10.1 STP (802.1d) Configuration

L2SW supports all three spanning tree protocols (STP, RSTP and MSTP). Users can select any one of the the three protocols by selecting the Force Version parameter in the Set Spanning Tree Configuration as illustrated in

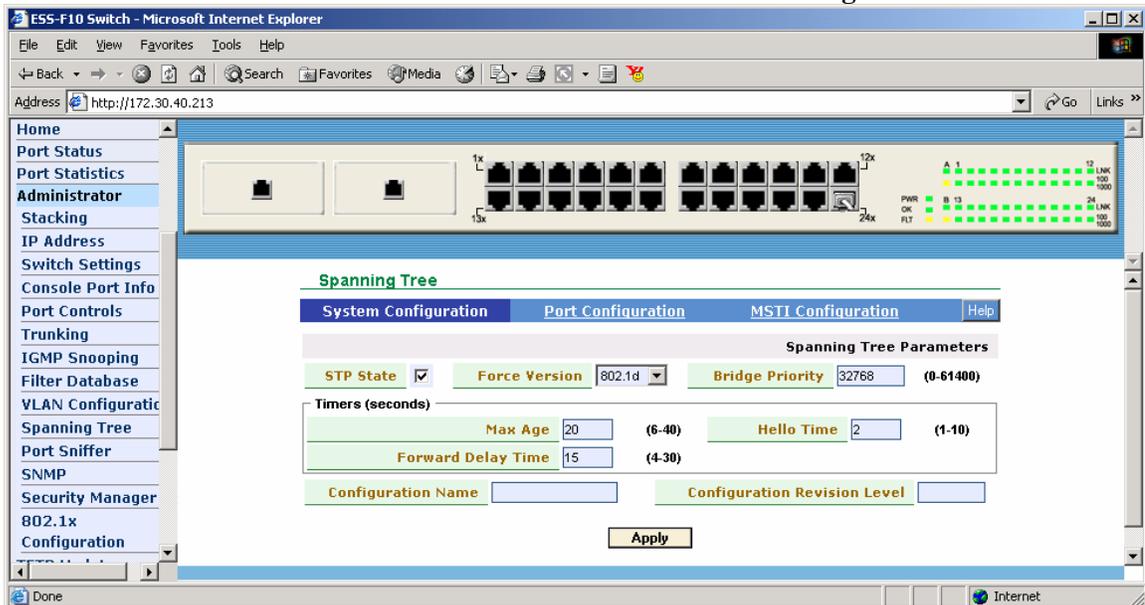


Figure 4-28.

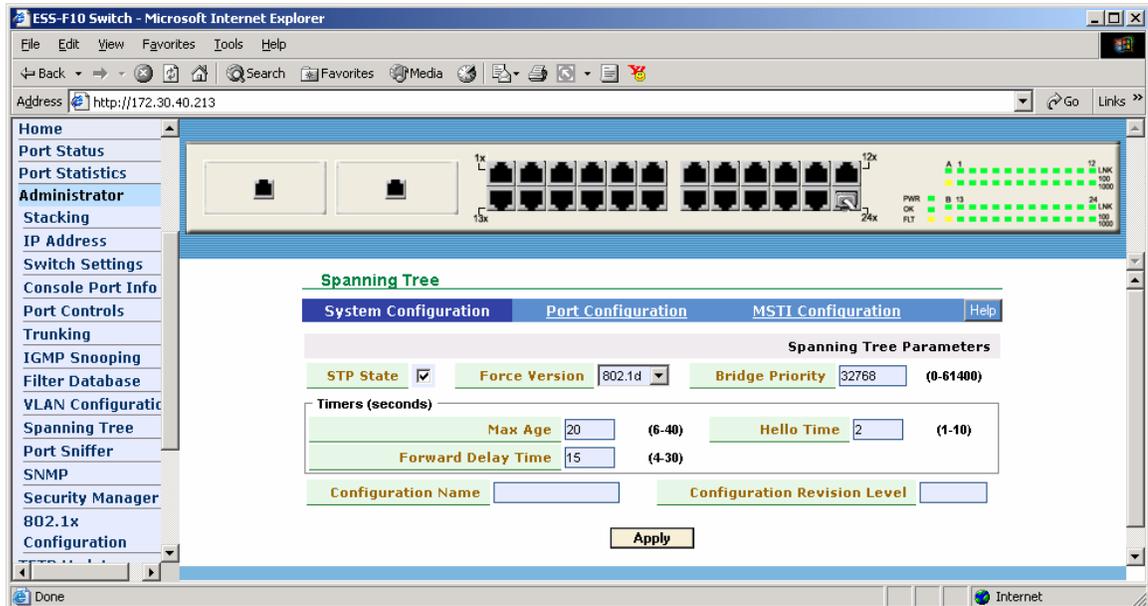


Figure 4-28: Spanning Tree Version Selection

STP can be enabled, by selecting 802.1d as the Force Version parameter. Other parameters associated with the STP can be configured as well using the same screen. See also Figure 4-28 for the list of STP related parameters that can be configured.

Note: STP should be enabled on LACP links. Otherwise broadcast storm may occur.

Parameter	Description
Force Version	Select the Spanning Tree Protocol Version. You can choose 802.1d (STP), 8021.w(RSTP) or 802.1s(MSTP) as the spanning tree protocol for the switch.
Priority	Priority value is used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Enter a number 1 through 65535.
Max Age	Max Age value is the number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40.
Hello Time	Hello time value is the number of seconds between the transmissions of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10.

Forward Delay time	Forward Delay Time is the number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30.
--------------------	--

Table 4-2: STP Parameters

Configuration Name and Revision Level are parameters that are associated only with MSTP. A brief description of these parameters will be provided in the following subsections.

Spanning Tree screen also displays a summary of switch related configuration at the bottom of the screen as illustrated in Figure 4-29. Further details related to Switch level STP configuration can be displayed by clicking on the [Detailed](#) hyperlink displayed in Figure 4-29.

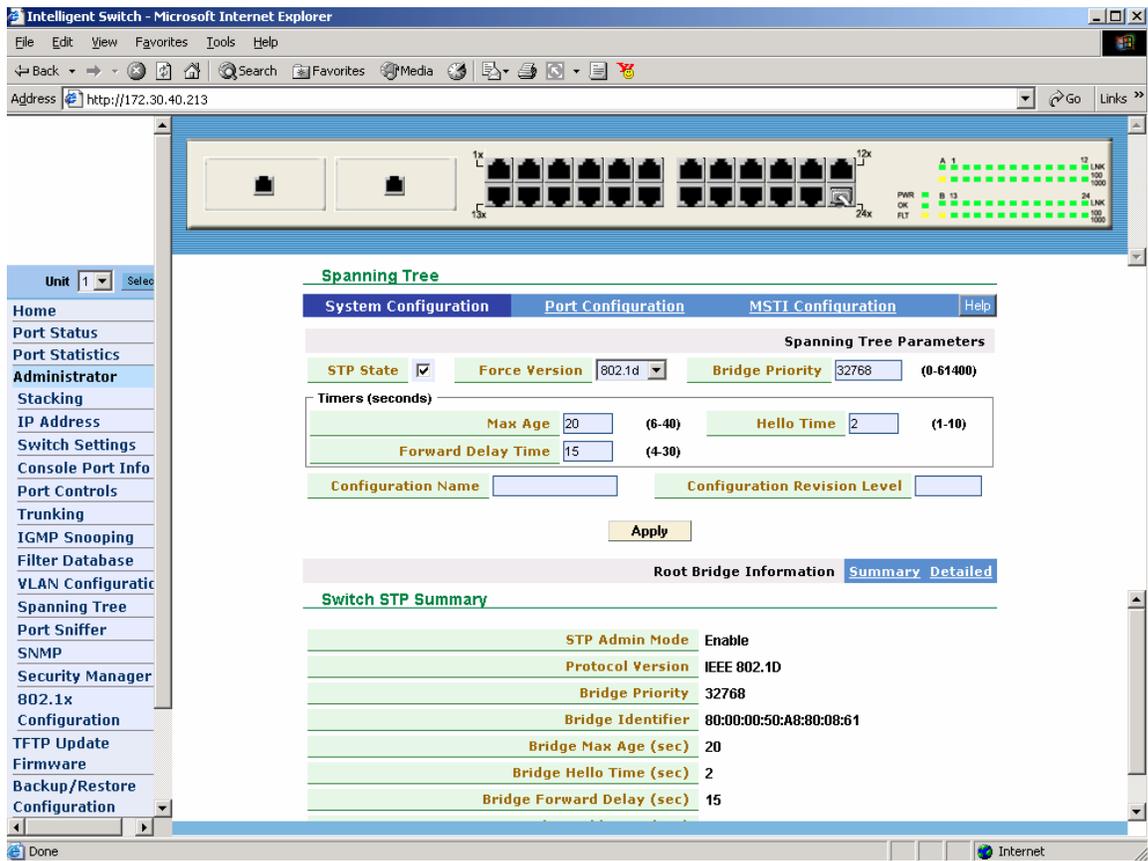


Figure 4-29: Switch STP Configuration Summary

Users can view the Spanning Tree Port Status by selecting Port configuration link on the STP configuration screen.

L2SW Port Priority and Path Costs are automatically selected by the switch based on Port ID and speed of the port. Future release will support configuration of these parameters from WBI and CLI.

4.3.10.2 RSTP (802.1w) Configuration

To configure L2SW to support RSTP, set the Force Version Parameter value to 802.1w as illustrated in Figure 4-30. To configure port level parameters, Click on Port Configuration link.

i While switching spanning tree protocol from one version to another (e.g., STP to RSTP or RSTP to STP or STP to MSTP, etc.), it is recommended that the STP adminmode is disabled and then reenabled. Users can disable or enable STP adminmode by clicking on the box next to STP State.

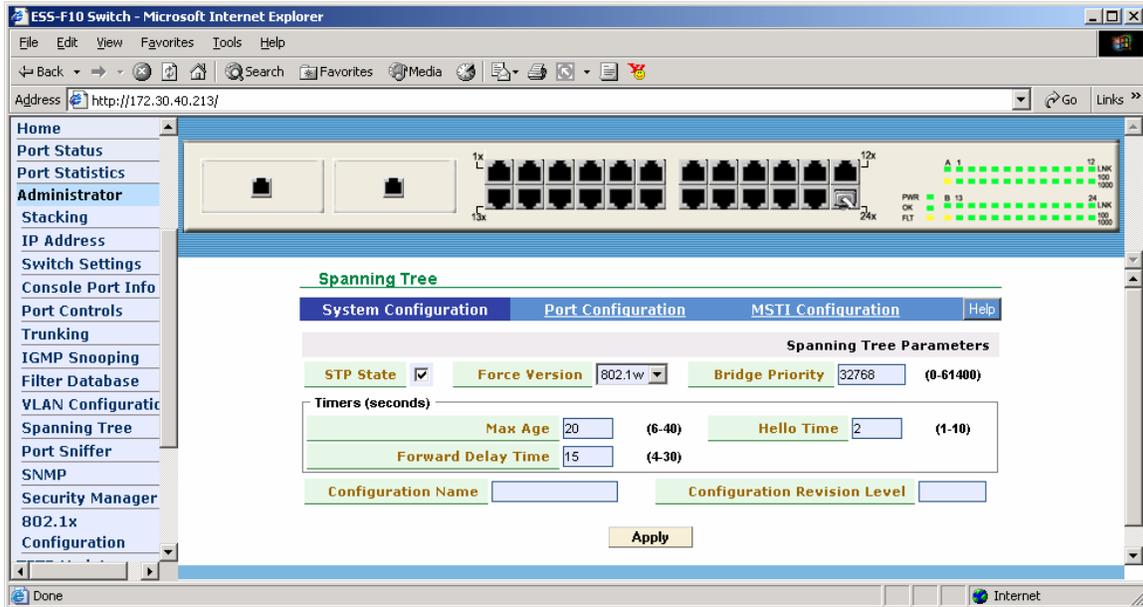


Figure 4-30: RSTP Configuration

The Port Configuration allows users to enable/disable RSTP on a per port basis and to configure the Edge ports on the switch along with type of link attached to the Edge port. L2SW allows users to set Edge port link to Point-to-point, Shared or Auto mode as illustrated in Figure 4-30. In Auto mode, the Link Type is automatically set to Point-to-point if the link is auto-negotiated to full-duplex mode and set to shared mode if the link operates in half-duplex mode.

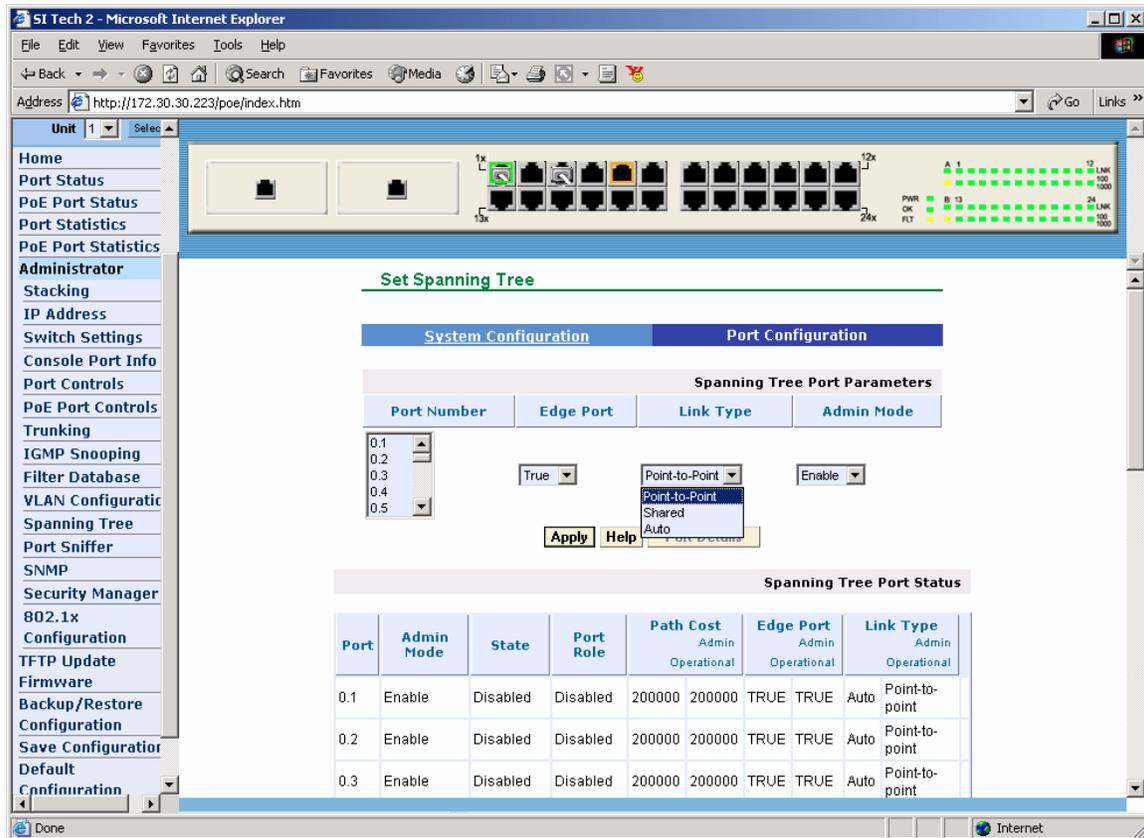


Figure 4-31: RSTP Port Configuration

Per port status is displayed in the same screen as the RSTP port configuration as illustrated in Figure 4-32. The per port status includes the following information.

- **Port Number** (0.1 thru 0.24 and 1.1 and 1.2)
- **Admin Mode** (Enabled/Disabled)
- **State** (Discarding, Listening or Forwarding)
- **Port Role** (Root, Designated, Alternate, Backup or Edge Port)
- **Path Cost** (Value configured by Admin and Value used by protocol)
- **Edge Port** (TRUE or FALSE)
- **Link Type** (Point-to-point, Shared, Auto)

Two values are displayed under Path Cost, Edge Port and Link Type. They represented administrative value and operational value used by the protocol machine.

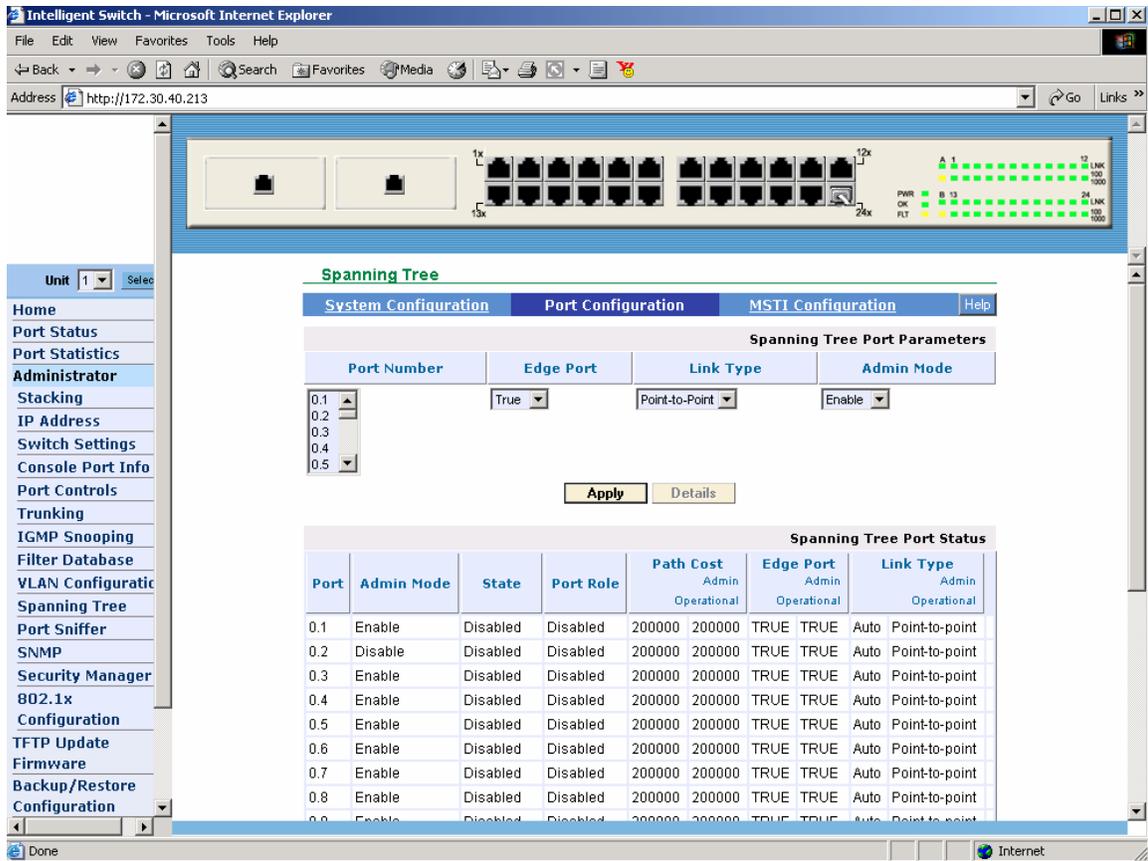


Figure 4-32: RSTP Port Status Display

4.3.10.3 MSTP Configuration

To configure MSTP, use STP configuration screen and select 802.1s as the Force Version parameter as illustrated in Figure 4-33.

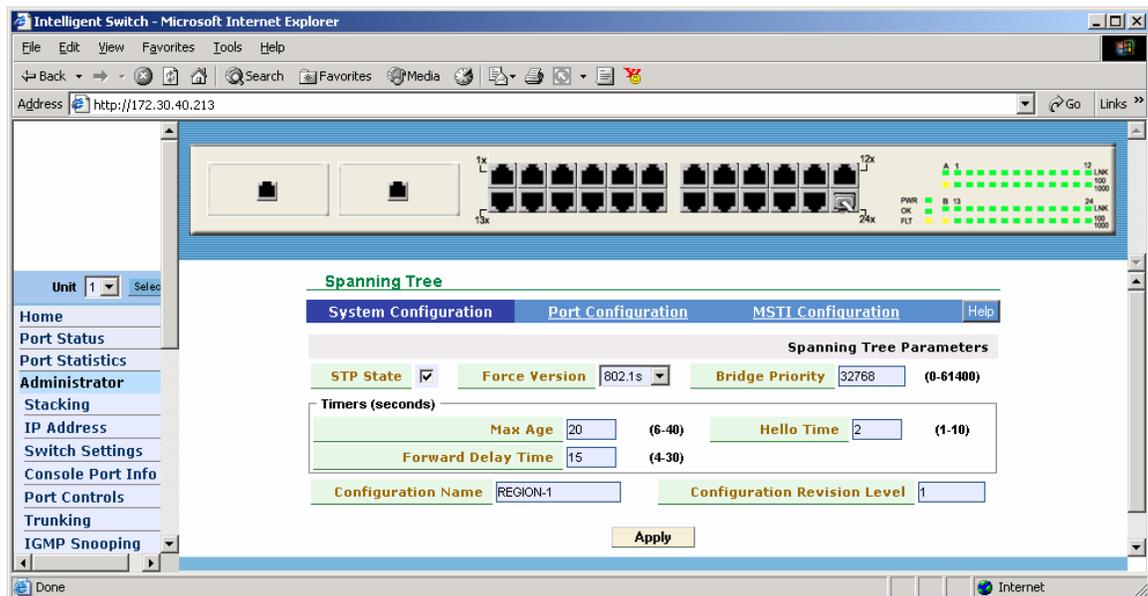


Figure 4-33: MSTP Switch Configuration

To configure an instance of MST, click on the MST details on the Spanning Tree configuration and configure the MST instance ID and VLAN range (low and high values). The MST configuration screen is illustrated in Figure 4-34. To delete a subset of the VLANs within an MST, configure the VLAN range on the Select MST part on the right side of the screen and click delete key.

i *L2SW supports 8 MSTIs.*

i *The VLANs deleted the from a MSTI will be assigned to IST (Instance 0). If all the VLANs assigned to a MSTI are deleted, the MSTI itself will be deleted after reassigning the VLANs to the IST.*

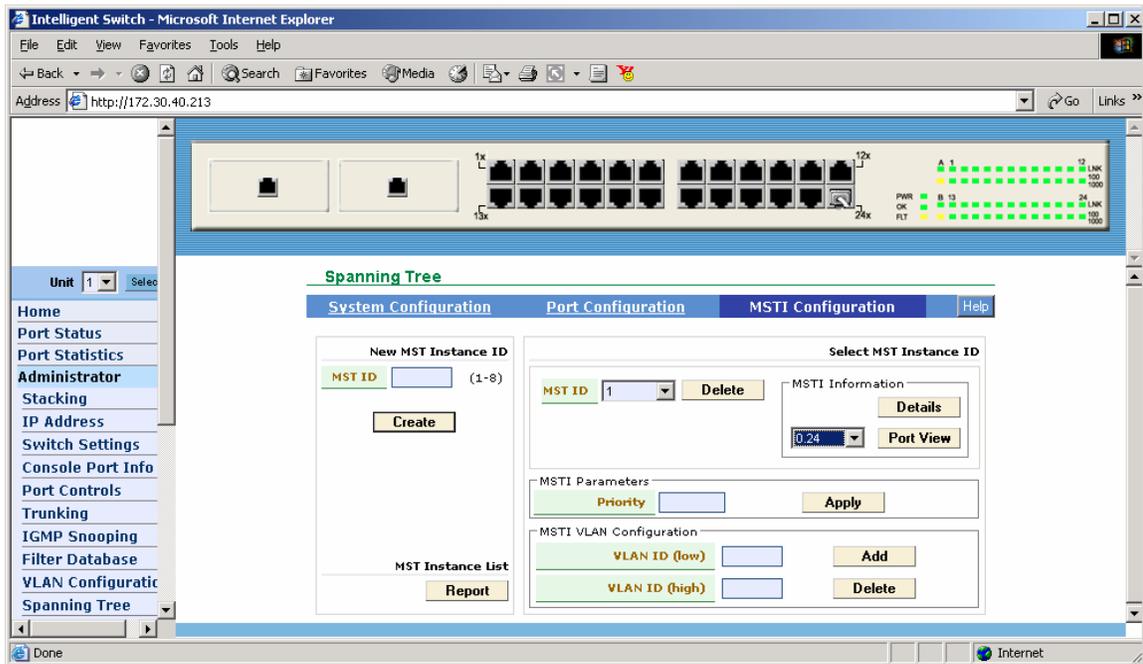


Figure 4-34: MST Instance Configuration

i *The VLANs have to be created first before assigning them to a MSTI.*

The VLAN assignment details for each MSTI can be displayed by clicking on the **Report** button displayed under the **MST Instance List** title. Figure 4-35 displays the list of MST instances created by the user along with list of VLANs assigned to each MST Instance.

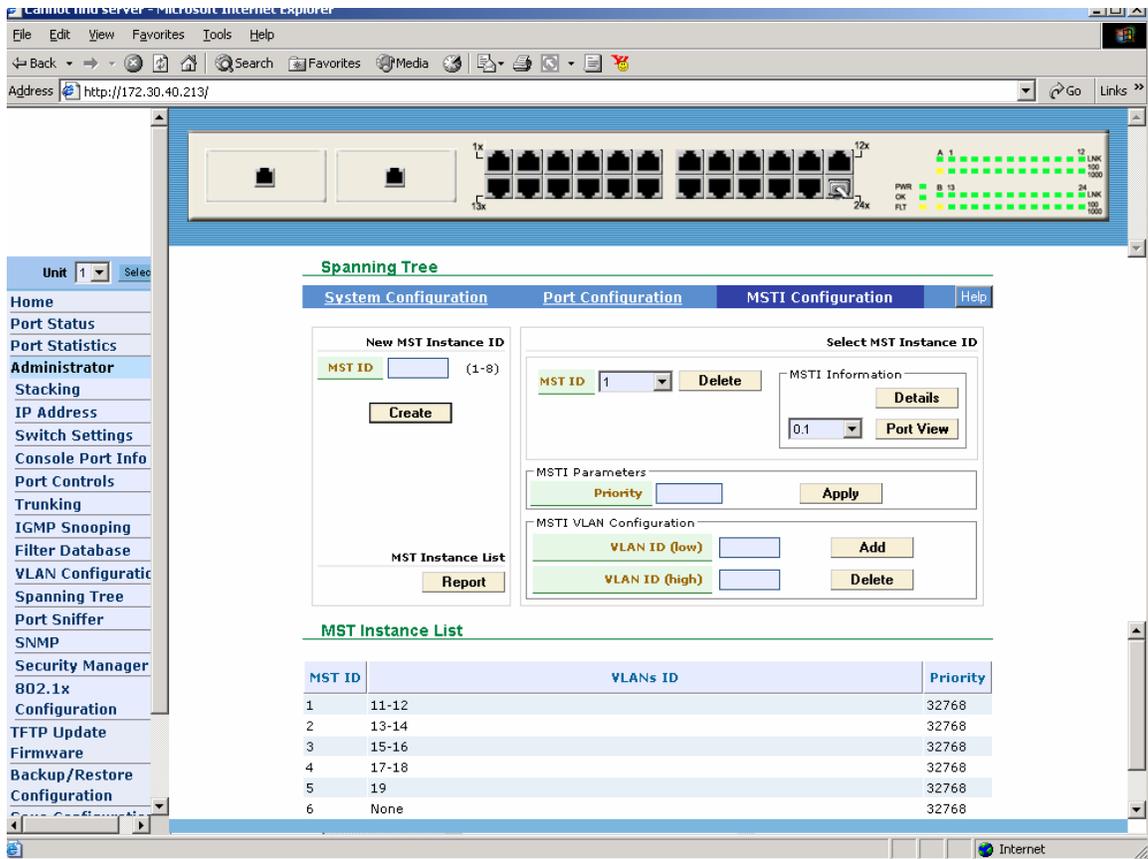


Figure 4-35: MSTI Configuration Report

Detailed information for each MST Instance can be displayed by Clicking the button marked as **Details** in the block marked **MSTI Information**. Figure 4-36 displays MST Instance details for one of the MSTI configured in the switch.

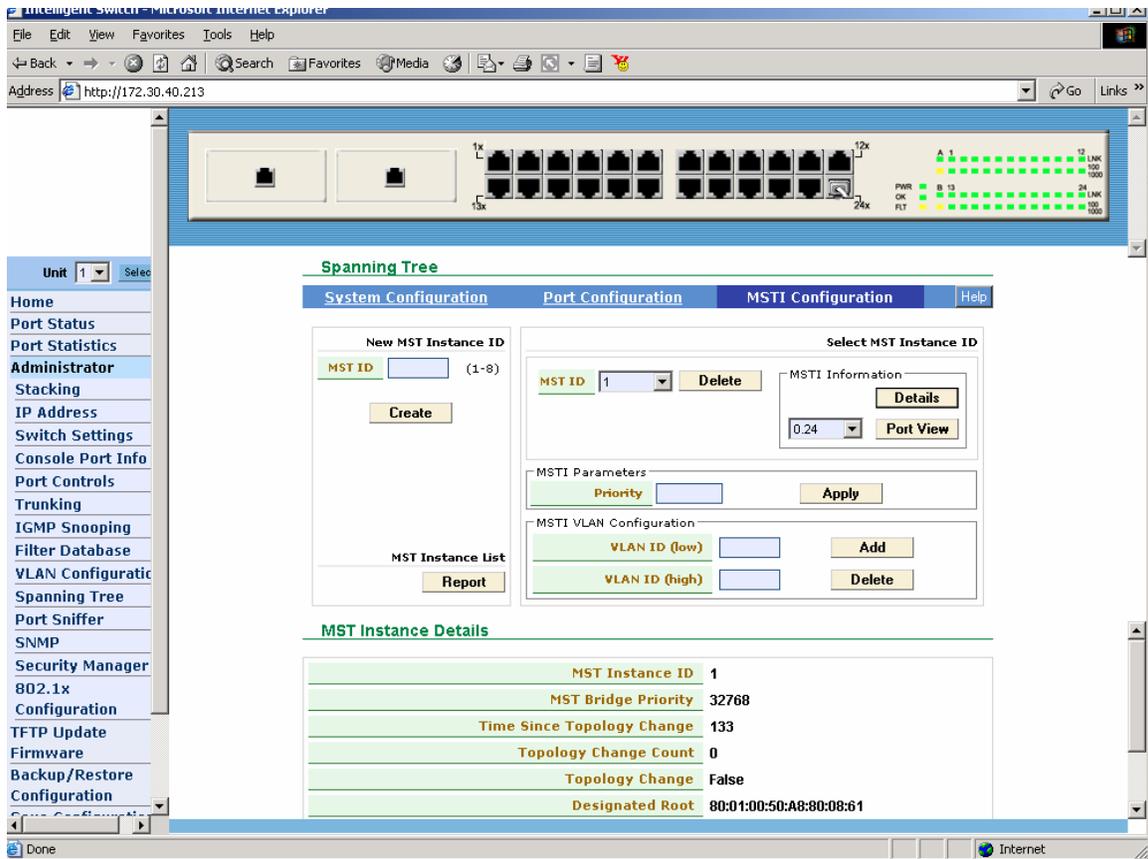


Figure 4-36: MST Instance Details

4.3.11 Port Sniffer

The Port Sniffer is a method to monitor traffic in switched networks. In Sniffer mode of operation, traffic flowing in and out of monitored ports will be duplicated into sniffer port.

Port Sniffer page is used to enable/disable various sniffer parameters such as Roving Analysis State and Port to be analyzed.

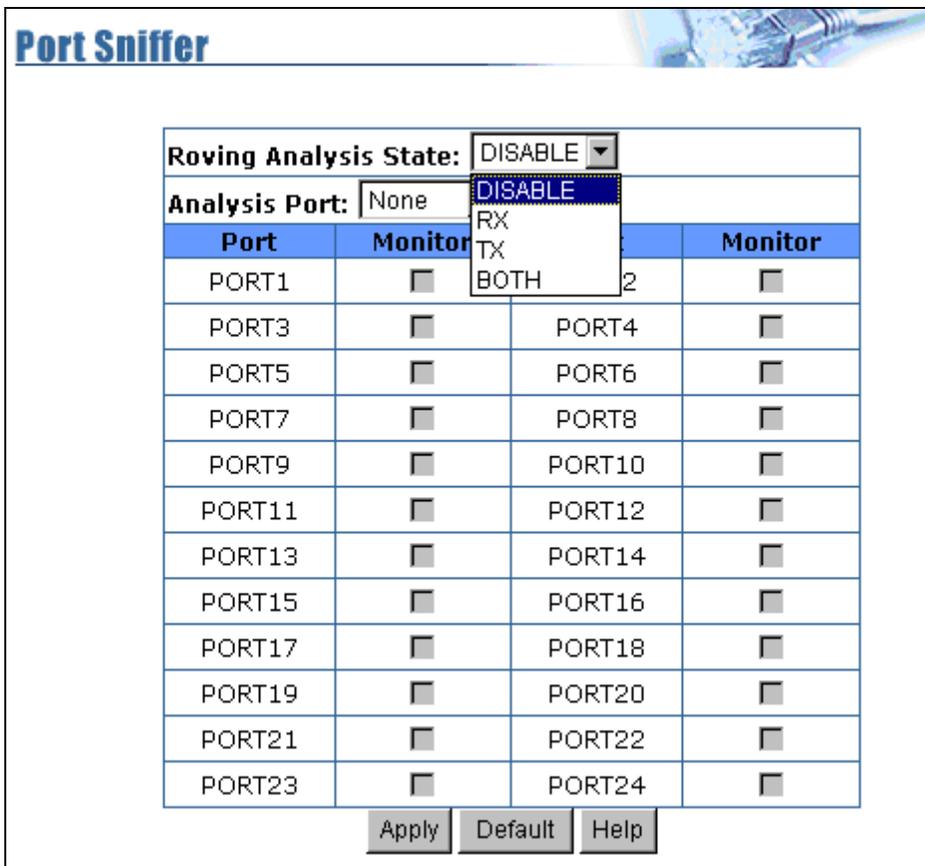


Figure 4-37: Port Sniffer

Roving Analysis State: Set sniffer mode to one of the following options.

- Disable
- Rx
- Tx
- Both.

Analysis Port: It's mean sniffer port can be used to see all monitor port traffic. User can connect sniffer port to an external LAN analyzer.

Monitored Port: The ports user wants to monitor. All monitored port traffic will be copied to sniffer port. User can select up to 25 ports to be monitored. All ports selected for monitoring purposes are monitored using the same Sniffer mode (RX only, TX only or both RX and TX). If user wants to disable the Sniffer function, user must set the analysis (Sniffer) port to None.

4.3.12 SNMP

SNMP is a protocol that governs the transfer of information between a SNMP manager and agent. Any Network Management system that supports the Simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. The L2SW supports SNMP versions V1, V2c and V3. User can select the SNMP version to be supported by the switch. SNMP v1 and SNMPv2c are essentially the same except that SNMPv2c supports bulk-retrieval command to reduce the number of exchanges required between manager and agent to retrieve information from a large SNMP table. Both SNMPv1 and V2 supports only community string based administrative control. SNMPv3 provides secure access to devices by authenticating and encrypting the messages exchanged between manager and agent. While operating in SNMPv3 mode, the L2SW can be configured to operate based one of the following security models:

- **NoAuthNoPri v-** Security is enforced using community based string – no authentication and encryption is used
- **AuthNoPri v-** Messages are authenticated using HMAC-MD5 message digest, but are not encrypted
- **AuthPri v-** Messages are authenticated using HMAC-MD5 and encrypted for privacy using DES-56 encryption standard

In SNMPv3 mode, L2SW allows users to configure MIB views with different access privileges for different groups of users. For example, a MIB view with full read write access privileges can be set up for administrative group while a read-only view can be set up for other users.

SNMP Management web page is used to define L2SW switch name and to enter SNMP community strings. Figure 4-38 illustrates the screen used for configuration SNMP parameters such as System Name, Location and Contact person.

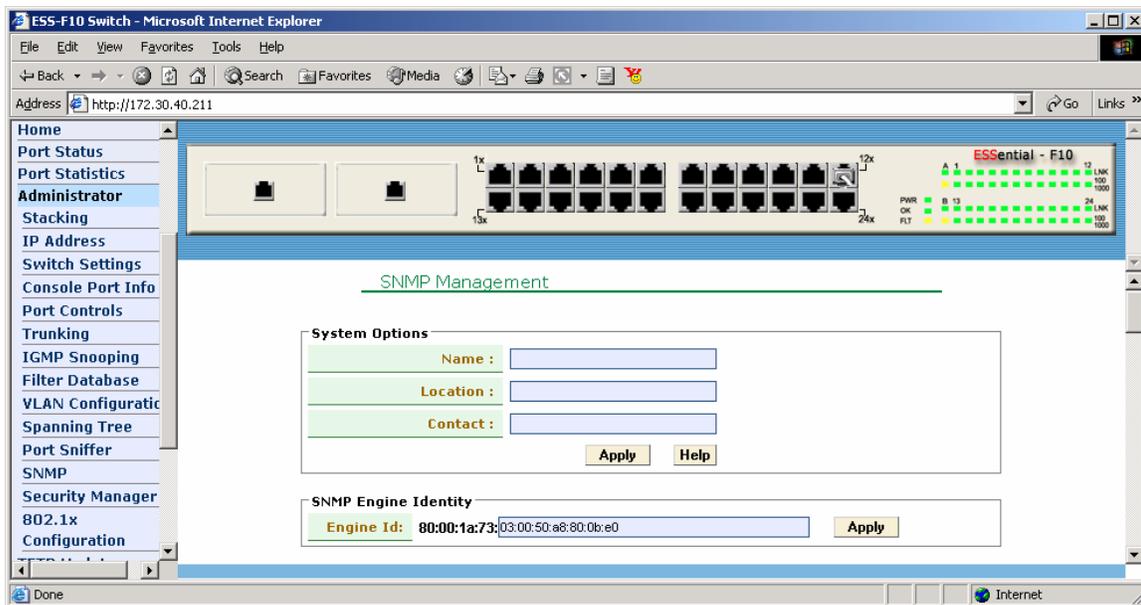


Figure 4-38:SNMP Management

User can also define a name, location, and contact person for the switch. Users can also select the SNMP version under the SNMP protocol Version block to select the SNMP protocol version to be supported by the switch. Fill in the system options data and then click `Apply` to update the changes on this page

- **Name** Enter a name to be used for the switch.
- **Location** Enter the location of the switch.
- **Contact** Enter the name of a person or organization.

Figure 4-39: Community Strings

Community strings serve as passwords and can be entered as one of the following:

RO: Read only. Enables requests accompanied by this string to display MIB-object information.

RW: Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

Figure 4-40: Trap Manager

A trap manager is a management station that receives traps and the system alerts generated by the switch. Switch will not generate any trap until the trap manager information is defined in the switch. Create a trap manager by entering the IP address of the station and a community string into the Trap Manager screen displayed in Figure 4-40.

4.3.12.1 SNMP v3 Configuration

L2SW supports SNMPv1, SNMPv2c and SNMPv3 in a multi-lingual mode. In other words, even if L2SW is configured to operate in SNMPv3 mode, it will respond to requests from SNMPv1 or SNMPv2c managers.

SNMPv3 requires each agent to be uniquely identified by an Engine ID. L2SW automatically configures a unique default EngineID for each switch as follows:

- Octet 1-4 : 80:00:1A:73
- Octet 5-10: Base MAC address of the switch

In general there is no need to change the default EngineID configured automatically by the system. However, L2SW provides the WBI screen as illustrated in Figure 4-41, to allow the user to configure the Engine ID.

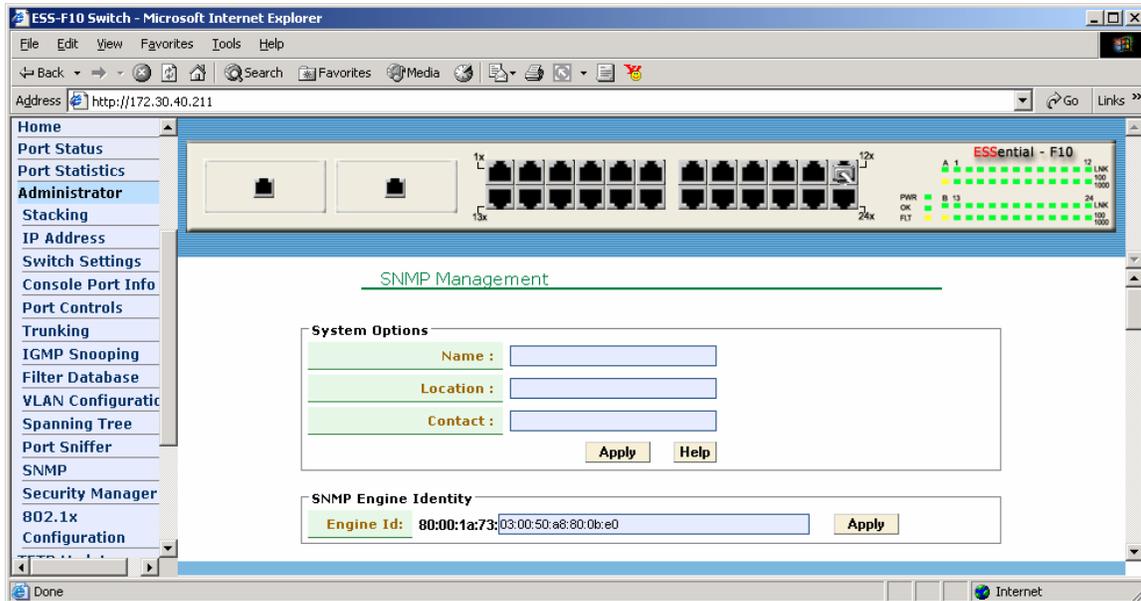


Figure 4-41: SNMP Engine ID Configuration Screen

Assuming that the Engine ID for the switch is not changed by the user, the first step in the configuration of SNMPv3 is creation of the necessary MIB views. The MIB view can be created by entering a View Name (a string of up to 16 ASCII printable characters), an OID representing a subtree in the MIB and operational directive to include or exclude the MIB subtree identified by the view. The block under the title “Views” in Figure 4-42 is used for creating MIB views.

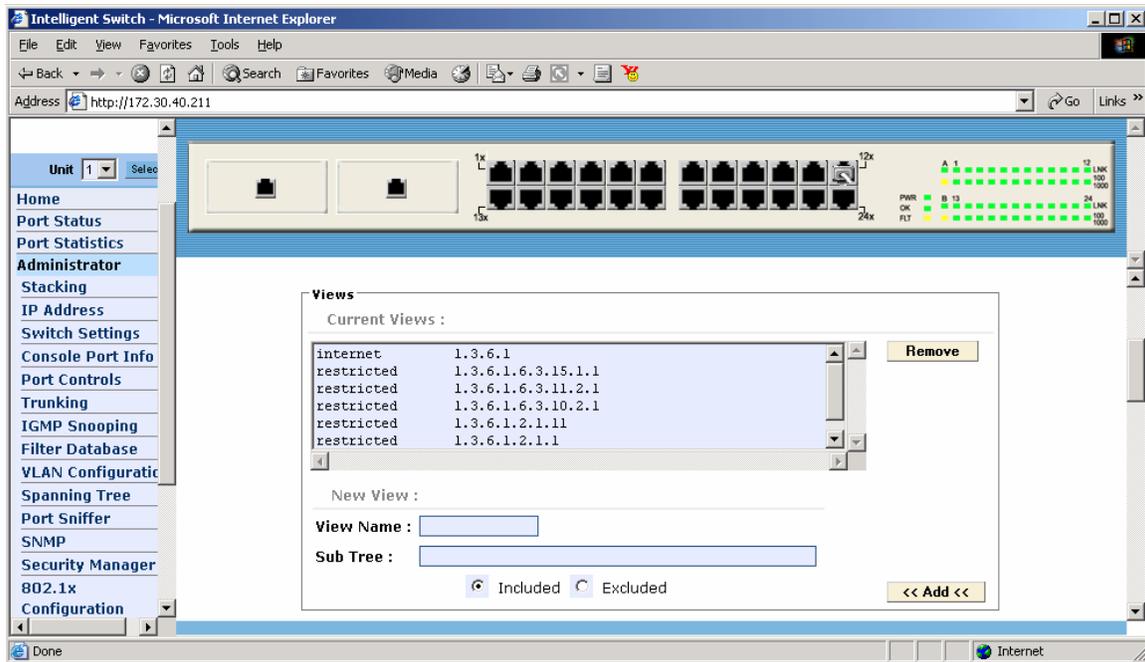


Figure 4-42: Views Configuration Screen

L2SW creates the following two views as default views. The user can modify or delete these views if required.

- **internet:** Enter subtree rooted at OID 1.3.6.1
- **restricted:** 5 Subtrees with the following root OIDs:
 - 1.3.6.1.2.1.1
 - 1.3.6.1.2.1.11
 - 1.3.1.6.3.10.2.1
 - 1.3.1.6.3.11.2.1
 - 1.3.1.6.3.15.1.1

! *Some of the SNMPv3 managers allow users to configure a “context” name along with the Views. L2SW currently doesn’t support “contexts” with the Views. The Context name should be configured as blank on the SNMP manager side.*

To delete an existing view, select the view to be deleted in the window displaying the list of current views and click on “**Remove**” button.

The second step in the configuration of SNMPv3 is the creation of user groups using the block titled “**Groups**”. To create a group, the following parameters have to be configured as illustrated in Figure 4-43.

- | | |
|------------------------|--|
| Group Name: | The name of the Group. A text string of up to 16 characters are used to define Group Name. |
| ReadView Name: | View for Readonly access privileges. Name of a previously defined view |
| WriteView Name: | View for Read/write access privileges. Name of a previously defined view |

Notify View Name: View for generating notification traps. Name of a previously defined view
Auth. Type: Authorization Type: noAuthNoPriv, AuthNoPriv, AuthPriv.

i *The same group can be configured with different combination of views and access privileges. This would allow users belonging to the same group to have different access privileges*

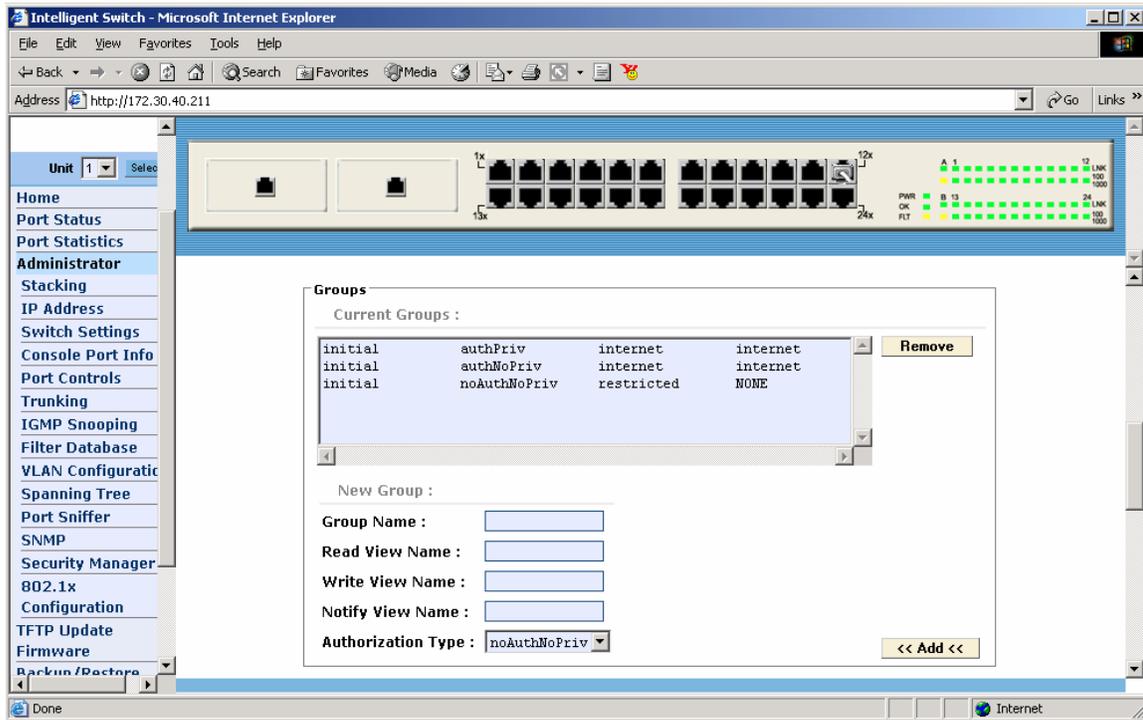


Figure 4-43: SNMPv3 Group Configuration

When SNMPv3 is enabled, the L2SW creates a default group named “initial”.

The third step in the configuration of SNMPv3 is creation of usernames and associated the user with a previously defined group. To configure a user name, the following parameters have to be configured as illustrated in Figure 4-44. To remove an existing users, select the user from the list of “Current Users” on the same screen and click on “Remove” button.

User Name: Name of the new user. A text string of up to 16 characters
Group Name: Name of the group for the user to be associated with. Provide a previously defined group name
Auth. Password: Authentication Password. A string of maximum of 16 characters
Priv. Password: Privacy Password. A string of maximum 16 characters

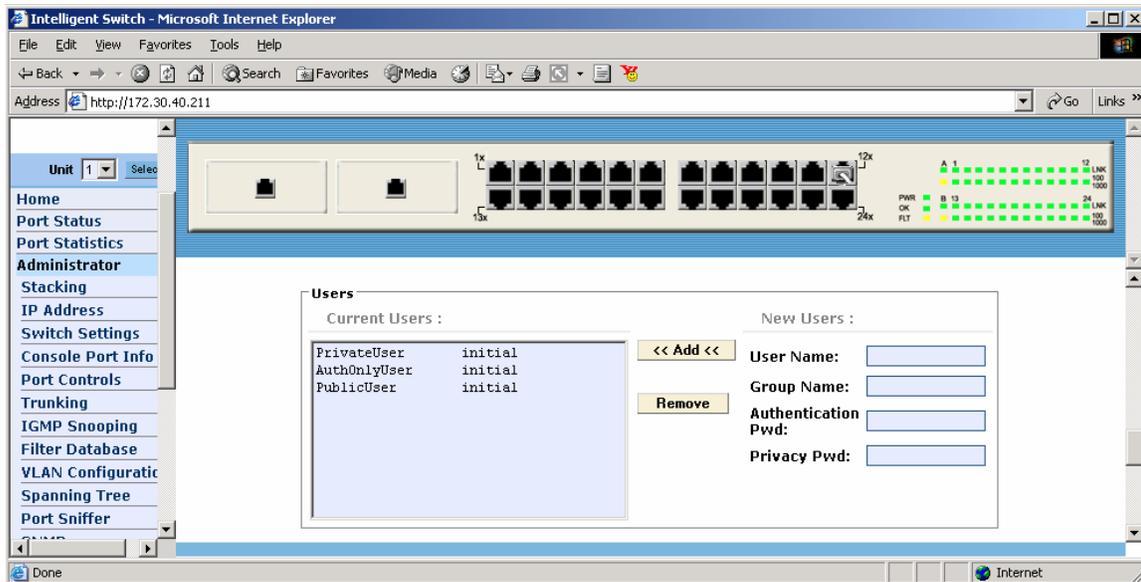


Figure 4-44: SNMPv3 User Configuration

When SNMPv3 is enabled, L2SW automatically creates the following users attached to the `initial` group. The default users created by L2SW may be deleted if they are not required.

- `PrivateUser`: `authPriv` privilege
- `AuthOnlyUser`: `authNoPriv` privilege
- `PublicUser`: `noAuthNoPriv` privilege

i To get the Authentication and Privacy Password for the default users, contact L2SW technical support.

i L2SW supports 8 MIB views, 8 Groups and 16 Users

i Before deleting a group all users associated with that group must be deleted and before deleting a view all groups using that view must be deleted.

i L2SW will be busy for a while computing the message digest and encrypting the password string when Authentication and Privacy Passwords are configured.

4.3.13 Security Manager

User Name is displayed on this page. Using this page, user can change web management user name and password.

User Name:	<input type="text" value="admin"/>
Assign/Change password:	<input type="password" value="***"/>
Reconfirm pssword:	<input type="password" value="***"/>
<input type="button" value="Apply"/>	

Figure 4-45: Security Manager

To change password, use the following procedure:

- **User Name** Type the new user name⁵.
- **Password** Type the new password.
- **Reconfirm password:** Retype the new password.

Click **Apply** button.

4.3.14 802.1x

802.1x makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and to prevent access to that port in case the authentication and authorization process fails.

Before configuring 802.1x feature, it has to be enabled in `Switch Settings` web page:

⁵ Note, the L2SW switch can currently support only one user. Changing the user name does not necessarily mean creation of more user accounts in the switch.

Switch Settings

Basic	Module Info	Advanced	Misc Config
--------------	--------------------	-----------------	--------------------

Collisions Retry Forever : Enable
Hash Algorithm : CRC-Hash
IFG compensation : Enable
802.1x Protocol : Enable Disable Enable

Apply Default Help

Figure 4-46: Enable 802.1x

4.3.14.1 802.1x Configuration

802.1x parameters such as Radius Server IP, Server Port, Shared Key and NAS Identifier can be configured with this page.

802.1x Configuration

System Configuration	PerPort Configuration	Misc Configuration
-----------------------------	------------------------------	---------------------------

Configure 802.1x Parameters	
Radius Server IP :	192.168.221.72
Server Port:	1812
Accounting Port:	1813
Shared Key :	12345678
NAS,Identifier:	NAS_L2_SWITCH

Apply Help

Figure 4-47: 802.1x Configuration

To configure 802.1x, the following authentication server information has to be provided:

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

4.3.14.2 PerPort Configuration

With this page, user can select the specific port and configure the authorization state.

802.1x Configuration

Port Number	Port State
PORT1	Au
PORT2	
PORT3	
PORT4	
PORT7	

Figure 4-48: 802.1x Perport Configuration

Each port can select four kinds of authorization state:

Fu: Force the specific port to operate in unauthorized state. Access to the network through this port will be blocked.

Fa: Force the specific port to be in authorized state and allow users attached to this port to access the network without forcing the user to go thru authentication procedure.

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

No: 802.1x based port security is not supported in this port

PORT1	No
PORT2	No
PORT3	No
PORT4	No
PORT7	No
PORT8	No
PORT9	No
PORT10	No
PORT11	No
PORT12	No
PORT13	No
PORT14	No
PORT19	No
PORT20	No
PORT21	No
PORT22	No

Figure 4-49: 802.1x Port Status

4.3.14.3 802.1x Miscellaneous Configuration

Parameters for 802.1x such as Quiet period, Server timeout, Maximum request and re-authorization period can be configured using this page.

802.1x Configuration

System Configuration	PerPort Configuration	Misc Configuration
Configure 802.1x misc configuration		
Quiet period:	<input type="text" value="60"/>	
Tx period:	<input type="text" value="30"/>	
Supplicant timeout:	<input type="text" value="30"/>	
Server timeout:	<input type="text" value="30"/>	
Max requests:	<input type="text" value="2"/>	
Reauth period:	<input type="text" value="3600"/>	
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

Figure 4-50: 802.1x Miscellaneous Configuration

- **Quiet Period** Define periods of time during which the switch will not

attempt to acquire a supplicant (Default time is 60 seconds). Supplicant is a host/client attached to a 802.1x port.

- **Tx Period** Defines the interval at which an EAPOL PDU is transmitted (Default value is 30 seconds).
- **Supplicant Timeout** Defines the timeout value to be used in the exchanges between the supplicant and authentication server (Default value is 30 seconds).
- **Server Timeout** Defines the timeout value to be used in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
- **ReAuthMax** Defines the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
- **Reauth Period** Defines the number of seconds between periodic re-authentication of the supplications (Default value is 3600 seconds).

4.4 TFTP Update Firmware

TFTP (Trivial File Transfer Protocol) is used to transfer software images into the switch and it is also used to download and upload configuration databases.

This page is used to set TFTP server IP address and new image in TFTP server to download new software image into flash.

TFTP Download New Image

TFTP Server IP Address	<input type="text" value="172.30.10.11"/>
Firmware File Name	<input type="text" value="image.bin"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 4-51: TFTP Download

The following procedure is a prerequisite to update Firmware and remote boot switch system:

1. Install TFTP server and start the TFTP server.
2. Copy firmware update version `image.bin` to TFTP server's directory.
3. Ping the L2SW from the host where TFTP server is installed and make sure the network connectivity between the TFTP server and the L2SW switch is OK.

To download a new firmware using TFTP, use the following procedure:

1. Enter the TFTP Server IP Address.
2. Enter the name of the firmware file (e.g., `image.bin`) and click `Apply` button.

After the image is downloaded successfully, you will see the following message on your screen.

Image download complete.
Click on "Update Firmware" below, to update system with the new image.

Figure 4-52: Confirmation for TFTP upgrade

4.5 Configuration Backup

4.5.1 TFTP Backup Configuration

This page is used for backing up (storing) configuration database of the switch on a remote file server.

[TFTP Configuration](#)

TFTP Restore Configuration	TFTP Backup Configuration
TFTP Server IP Address	<input type="text" value="172.30.10.11"/>
Backup File Name	<input type="text" value="data.dat"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 4-53: TFTP Backup Configuration

Users can backup the switch's configuration database from the switch to a TFTP server using the `TFTP Configuration` web page. Before you start the database backup operation, make sure that the TFTP server is reachable from the switch (use PING command from the TFTP server to the switch).

4.5.2 TFTP Restore Configuration

The following web page is used for Restore operations.

[TFTP Configuration](#)

TFTP Restore Configuration	TFTP Backup Configuration
TFTP Server IP Address	<input type="text" value="172.30.10.11"/>
Restore File Name	<input type="text" value="data.dat"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

Figure 4-54: TFTP Restore Configuration

User can restore the switch's configuration database from a TFTP server to the switch. Before starting the restore operation, make sure that the configuration database file is located in the TFTP server and

that the TFTP server is reachable from the switch.

4.6 Default Configuration

To reset the switch and restore the switch configuration to factory settings, use the following web page and click on the `reset` button.

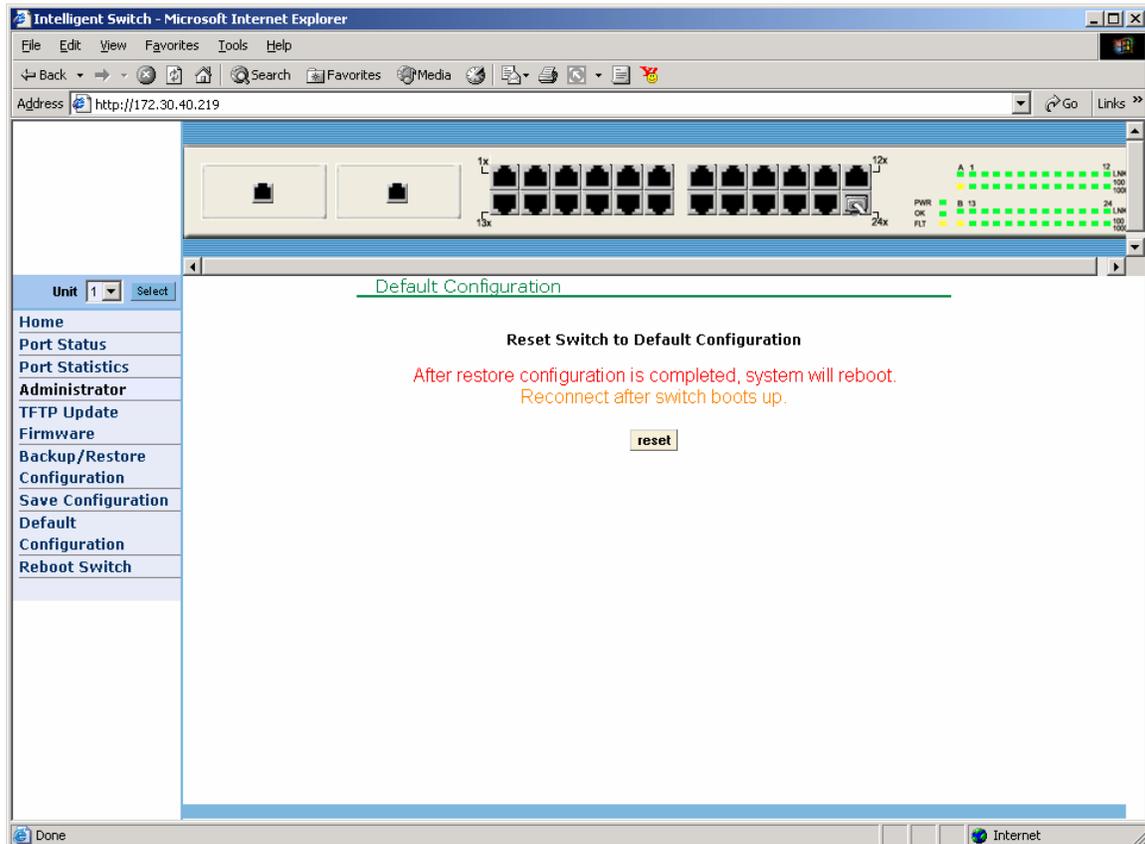


Figure 4-55: Reset System

4.7 Reboot

To just reboot the switch without restoring to default factory configuration, use the following web page.

5. Console – Menu Line

L2SW switch provides a serial RS-232 interface to manage the switch. User can configure the Windows HyperTerminal program as per the Console Port Information displayed in the WBI section to connect to the switch.

CMLI in the L2SW switch is organized as a set of Menu pages. Some menu pages only contain a list of menu items and by selection of one of these menu items will open up a new menu for configuration or display some status information. Menu pages for configuring switch parameters typically contain an action menu line at the bottom of the screen. User needs to switch from action mode to edit mode for configuring/modifying the switch parameters.

User has to specify the user name and password to login. The default user name is “admin”. For default password, contact your sales representative or technical support.

```

User Interface
(c) Intelligent 24 + 2 Standalone Switch

username : admin
password : ***
```

Figure 5-1: Login for Console

After successful login, the switch will display the CLI prompt **L2SW>** indicating that it is ready to accept CLI commands from the user. Enter “menu” to enter Menu Line Mode.

5.1 Main Menu

The Main Menu has six different options as displayed in the following page.

```

Main Menu
=====

Switch Static Configuration
Protocol Related Configuration
Status and Counters
Save Configuration
Reboot Switch
TFTP Update Firmware
Command Line Interface
Logout

Configure the switch.
Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

Figure 5-2: Main Menu for Console

Switch Static Configuration: Configure various switch parameters such as Ports, VLAN, Trunking etc.

Protocol Related Configuration: Configure various features such as STP, SNMP, GVRP, IGMP etc.

Status and Counters: Display Status and Counters for each port of the switch.

Save Configuration: To save configuration in to Flash Memory.

Reboot Switch: Restart the Switch, using either default configuration OR after saving the current configuration.

TFTP Update Firmware: Use TFTP protocol to download new firmware for the switch.

Logout: Exit the CMLI.

User can use the following control keys to navigate through the individual menu items in CMLI:

<TAB-key>: Move to next item.

<Backspace-key>: Move to previous item.

<ENTER-key>: Select or complete entering data for a item.

<Space-key>: Toggle selection in the item to be configured.

Menu pages that have items to be edited contain one or more of the following navigation actions. The mode in which the user can navigate/select these actions is called action mode:

Quit: Exit the current menu page (without saving) and return to previous menu page.

Edit: Switch CMLI to editing mode. Individual items in the page can be configured, by switching to editing mode. Use Ctrl+A to switch back to action mode.

Save: Save all edited/modified values in this menu page get applied and saved in RAM file system.

Previous Page: Return to previous menu page.

Next page: Go to next menu page.

5.2 Switch Static Configuration

Various features of the Switch such as Port, Trunk, VLAN, Port Mirroring, etc. can be configured in this menu page.

```

Intelligent Switch : Switch Configuration
=====
Port Configuration
Trunk Configuration
VLAN Configuration
Misc Configuration
Administration Configuration
Port Mirroring Configuration
Priority Configuration
MAC Address Configuration
Main Menu
Display or change port configuration.
Tab=Next Item BackSpace=Previous Item Enter=Select Item

```

Figure 5-3: Switch Configuration

5.2.1 Port Configuration

Speed, administration mode, Auto-negotiation mode, Flow Control etc. physical characteristics of individual ports can be configured using this page.

```

Intelligent Switch : Port Configuration
=====

```

Port	Type	InRate <100K>	OutRate <100K>	Enable	Auto	Spd/Dpx	FlowControl Full	Half
PORT1	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT2	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT3	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT4	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT5	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT6	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT7	100T \times	0	0	Yes	AUTO	100 Full	On	On
PORT8	100T \times	0	0	Yes	AUTO	100 Full	On	On

```

actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-4: Port Configuration

To change the configuration of an individual port, user needs to select `edit` from the action menu. In

the edit mode, the following parameters can be modified:

InRate (100K/unit): Input rate limit can be set in increments of 100K. The valid range is 0~1000.

- **0**: disable rate control.
- **1~1000**: input rate control value * 100K.

OutRate (100K/unit): Output rate limit can be set in increments of 100K. The valid range is 0~1000.

- **0**: disable rate control.
- **1~1000**: output rate control value * 100K.

Enabled: Choose “No” for disabling and “Yes” for enabling an individual port.

Auto: Choose auto negotiation mode

- **Auto**
- **Nway_Force**
- **Force** (for an individual port)

Spd/Dplx: Choose 10Mbps or 100Mbps for ports 1~24. Choose 10Mbps or 100Mbps or 1000Mbps (depending on the type of module card) for ports 25~26. Ports can be set to full-duplex or half-duplex mode (depends on the type of module card for ports 25~26).

Flow Control: Full: Choose “Off” for disabling, and “On” for enabling pause flow control function.

Half: Choose “Off” for disabling, and “On” for enabling backpressure flow control function.



1. Select <Save> from action menu to save changes.
2. If the static trunk groups exist, those trunk groups (eg: TRK1, TRK2...) will be displayed after the module cards (ports 25~26). Physical characteristics of trunk groups can also be edited in the above menu page.

5.2.2 Trunk Configuration

Up to seven static trunk groups (TRK1~7) can be configured using this menu page. Each static trunk group can have up to four ports. All ports in the same static trunk group will be treated as a single port.

```

Intelligent Switch : Trunk Configuration
=====
 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 M1 M2
1  v  v  v  v  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
2  -  -  -  -  v  v  v  v  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
3  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
4  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
5  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
6  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
7  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

TRK1  Static
TRK2  LACP
TRK3  Disable
TRK4  Disable
TRK5  Disable
TRK6  Disable
TRK7  Disable

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-5: Trunk Configuration

To change the configuration of an individual static trunk group

Select **Edi t** from the action menu

Choose up to 4 ports for the static trunk group. This selection can be done using the “**Space**” key.

Choose “**Stati c**”, “**LACP**” or “**Di sabl e**” in the corresponding TRK1~7 group.

- Stati c** LACP is disabled, normal trunk.
- LACP** LACP is enabled on this trunk group.
- Di sabl e** Delete the trunk group.



1. Select <Save> from action menu to save changes.
2. If VLAN group exists, all the ports of a static trunk group must be in same VLAN group.

5.2.3 VLAN Configuration

User can configure VLAN using the following screen.

```
Intelligent Switch : VLAN Configuration
=====

VLAN Configure
Create a VLAN Group
Edit/Delete a VLAN Group
Group Sorted Mode
Previous Menu

Configure the VLAN pvid and ingress, egress Rule.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

Figure 5-6: VLAN Configuration

5.2.3.1 VLAN Configure

This page can set VLAN mode as port-based VLAN or 802.1Q VLAN or protocol-based VLAN or disable VLAN function.

```
Intelligent Switch : VLAN Support Configuraton
=====

VLAN Mode :PortBased_

actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu
```

Figure 5-7: Port based VLAN

If 802.1Q VLAN is set, PVID, ingress filtering 1 and ingress filtering 2 can be configured as well.



To make the change in VLAN mode effective, the switch must be restarted.

```

Intelligent Switch : VLAN Support Configuraton
=====
VLAN Mode : 802.1Q

Port      PVID      IngressFilter1
NonMember Pkt      IngressFilter2
Untagged Pkt

PORT1     1          Drop           Forward
PORT2     1          Drop           Forward
PORT3     1          Drop           Forward
PORT4     1          Drop           Forward
PORT5     1          Drop           Forward
PORT6     1          Drop           Forward
PORT7     1          Drop           Forward
PORT8     1          Drop           Forward

actions->  <Quit>    <Edit>    <Save>    <Previous Page>  <Next Page>
Select the Action menu.
Tab=Next Item  BackSpace=Previous Item  Space=Toggle  Ctrl+A=Action menu

```

Figure 5-8: 802.1Q based VLAN

802.1Q VLAN can be configured using the following parameters.

PVID (Port VID: 1~255): Type the PVID.

NonMember Pkt: Ingress Filter rule for packets with VID that does not match port's configured PVID. Press Space key to choose forward or drop the frame that VID does not match the port's configured VID.

UnTagged Pkt: Ingress Filter rule for untagged frames. Press Space key to choose drop or forward the untagged frame.

Note that PVIDs cannot be assigned arbitrarily. Instead, all the PVIDs must take on values within the same PVID set. The following list depicts the relation between the PVID sets and value of PVID.

- PVID Set 0. PVID range: 0 - 255
- PVID Set 1. PVID range: 256 - 511
- PVID Set 2. PVID range: 512 - 767
- PVID Set 3. PVID range: 768 - 1023
- PVID Set 4. PVID range: 1024 - 1279
- PVID Set 5. PVID range: 1280 - 1535
- PVID Set 6. PVID range: 1536 - 1791
- PVID Set 7. PVID range: 1792 - 2047

- PVID Set 8. PVID range: 2048 - 2303
- PVID Set 9. PVID range: 2304 - 2559
- PVID Set 10. PVID range: 2560 - 2815
- PVID Set 11. PVID range: 2816 - 3071
- PVID Set 12. PVID range: 3072 - 3327
- PVID Set 13. PVID range: 3328 - 3583
- PVID Set 14. PVID range: 3584 – 3840
- PVID Set 15. PVID range: 3841 – 4095

5.2.3.1.1 Create a Port based VLAN

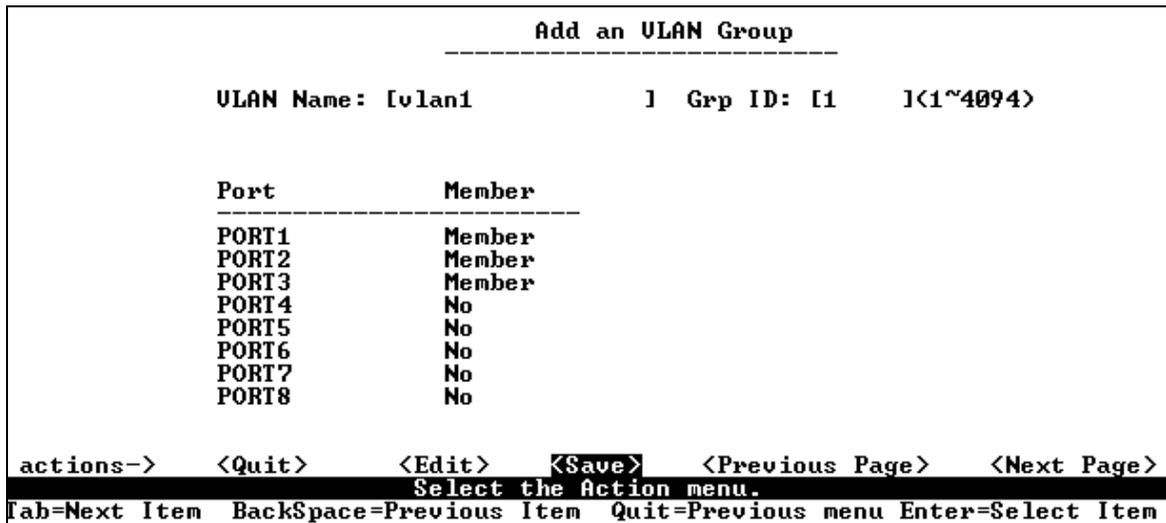


Figure 5-9: Create Port based VLAN

To create a port-based VLAN and add member/nonmember ports to VLAN use the following procedure

1. Select **Edi t**.
2. **VLAN Name**: Type a name for the new VLAN.
3. **Grp ID**: Type the VLAN group ID. The group ID range is 1 to 4094
4. **Member**: Press Space key to choose VLAN member. There are two types to selected:
 - a. **Member**: Port is member port.
 - b. **No**: Port is NOT member port.

5. Press Ctrl+A go back action menu line.
6. Select **Save** to save all configured value.

i *If the trunk groups exist, you will see the trunk groups (e.g. TRK1, TRK2...) after port26, and you can configure the trunk group to be a member of the VLAN.*

5.2.3.1.2 Create 802.1Q VLAN

```

----- Add an ULAN Group -----
VLAN Name: [U2          ] VLAN ID: [2    ](1~4094)
Protocol VLAN : None
Port      Member
-----
PORT1    UnTagged
PORT2    UnTagged
PORT3    Tagged
PORT4    Tagged
PORT5    No
PORT6    No
PORT7    No
PORT8    No

actions->  <Quit>    <Edit>    <Save>    <Previous Page>    <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-10: Create 802.1Q based VLAN

To create 802.1Q VLAN and add tagged /untagged member ports to it, the following steps are involved:

1. Select **Edi t**.
2. **VLAN Name**: Type a name for the new VLAN.
3. **VLAN ID**: Type a VID (between 2~4094). The default is 1. There are 256 VLAN groups available for configuring a VLAN.
4. **Protocol VLAN**: Press Space key to choose protocol type.
5. **Member**: Press Space key to choose VLAN member. The following three types of VLAN membership is supported.

UnTagged: Port is a member port of VLAN group and outgoing frames are not VLAN-Tagged frames.

Tagged: Port is a member port of VLAN group and outgoing frames are VLAN-Tagged frames.

No: The port is not a member of this VLAN group.

6. Press **Ctrl +A** to go back action menu line.
7. Select **Save** to save all configured values.

5.2.3.2 Edit / Delete a VLAN Group

```

NAME:          UID:          NAME:          UID:
-----
DEFAULT        1
V2              2

actions->  <Quit>  <Edit>  <Delete>  <Previous Page>  <Next Page>
Edit/Delete a VLAN Group.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item

```

Figure 5-11: Select a VLAN for editing

```

Edit an VLAN Group
-----
VLAN Name: [V2          ] VLAN ID: [2      ](1~4094)
Protocol VLAN : None
Port          Member
-----
PORT1         UnTagged
PORT2         UnTagged
PORT3         Tagged
PORT4         No
PORT5         No
PORT6         No
PORT7         No
PORT8         No

actions->  <Quit>  <Edit>  <Save>  <Previous Page>  <Next Page>
Select the Action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item

```

Figure 5-12: Edit/Delete selected VLAN

In this page, user can edit or delete a VLAN group as follows:

1. Press **Edi t** or **Del ete** item.
2. Choose the VLAN group to be edited or deleted and then press enter.
3. User can modify the protocol VLAN item or change the member port to be tagged or un-tagged. User can also remove some member ports from the VLAN group.
4. After edit VLAN, press **<Save>** key to save all configures value.



1. The VLAN Name and VLAN ID cannot be modified.
2. The default VLAN must be deleted.

5.2.3.3 Groups Sorted Mode

In this page, user can select VLAN groups either by name or by VID.

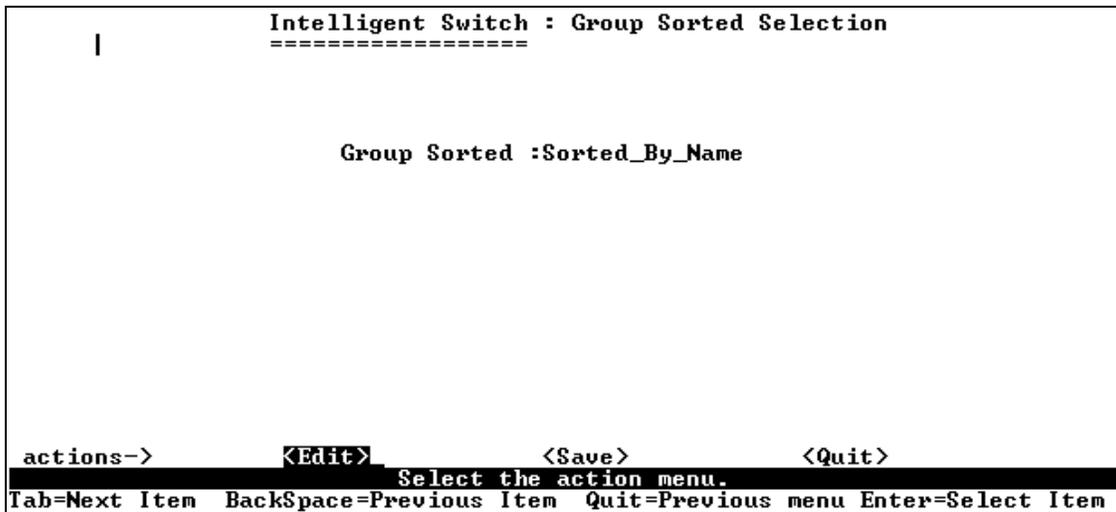


Figure 5-13: Group sorted VLAN

In the *Edit/Delete a VLAN Group* page, the result is sorted by name.

NAME:	UID:	NAME:	UID:
DEFAULT	1		
A1	3		
B4	4		
U2	2		

In the *Edit/Delete a VLAN Group* page, the result is sorted by VID.

NAME:	UID:	NAME:	UID:
DEFAULT	1		
U2	2		
A1	3		
B4	4		

5.2.4 Miscellaneous Configuration

```

Intelligent Switch : Misc Configuration
=====

MAC Age Interval
Broadcast Storm Filtering
Max bridge transmit delay bound
Port Security
Collisions Retry Forever
Previous Menu

Configure the MAC aging time.
Tab=Next Item BackSpace=Previous Item Enter=Select Item

```

Figure 5-14: Miscellaneous Configuration

5.2.4.1 MAC Age Interval

```

Intelligent Switch : MAC Aging Time
=====

MAC Age Interval (sec) [300] : 300
(disable:0,valid value:300~765)

actions-> <Edit> <Save> <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-15: MAC Age Interval

Enter number of seconds that an inactive MAC address may remain in the switch’s address table. The valid range is 10~765 seconds. Default is 300 seconds.

5.2.4.2 Broadcast Storm Filtering

The following screen can be used to configure broadcast storm control.

```

Intelligent Switch : Broadcast Storm Filter Mode
=====

Broadcast Storm Filter Mode :5

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
b=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-16: Broadcast Storm Filtering

To configure Broadcast Storm Filter, use the following procedure:

1. Press <Edit> to configure the broadcast storm filter mode.
2. Press Space key to choose the threshold value.

The valid threshold value are 5%, 10%,15%,20%,25% and NO.

5.2.4.3 Max Bridge transmit delay bound

This page displays features such as Maximum bridge Transmit, Low Queue delay Bound/Time.

```

Intelligent Switch : Max Bridge Transmit Delay Bound
=====

Max bridge transmit delay bound :OFF
Low Queue Delay Bound :Disabled
Low Queue Max Delay Time :255 <2ms/unit>

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
b=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-17: Maximum Bridge Transmit Delay Bound

Max bridge transmit delay bound: Limits packet queuing time in switch. If enabled, packets queued exceeding the time limit will be dropped. Press Space key to set the time. The valid values are 1sec, 2sec, 4sec and off. Default is off.

Low Queue Delay Bound: Limits low priority packets queuing time in switch. If enabled, the low priority packet exceeding Low Queue Max Delay Time, will be sent. Press Space key to enable or disable this function.

Low Queue Max Delay Time: To set the time for low priority packet queuing in switch. Default Max Delay Time is 255ms. The valid range is 1~255 ms.

 **Make sure that “Max bridge transit delay bound control” is enabled before enabling Low Queue Delay Bound, since latter can be configured only after former is configured.**

5.2.4.4 Port Security

A port in security mode will be “locked” without permission of address learning. Only incoming packets with SMAC already existing in the address table will be forwarded normally. User can disable the port from learning any new MAC addresses and then use static MAC addresses screen to define a list of MAC addresses that can used by the secure port.

```

Intelligent Switch : Port Security
=====

Port          Enable Security
              <disable for MAC Learning>
-----
PORT1         enabled
PORT2         enabled
PORT3         Disabled
PORT4         Disabled
PORT5         Disabled
PORT6         Disabled
PORT7         Disabled
PORT8         Disabled

actions->    <Quit>    <Edit>    <Save>    <Previous Page>    <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu

```

Figure 5-18: Port Security

Following is the procedure for configuring Port Security:

1. Select **Edi t**.
2. Press **Space** key to choose enable / disable item.
3. Press **Ctrl +A** to go back action menu line.
4. Select **Save** to save all configure value.

5. Click **Next Page** to configure port9 ~ port26,

Click **<Previous Page>** return to last page.

5.2.4.5 Collisions Retry Forever

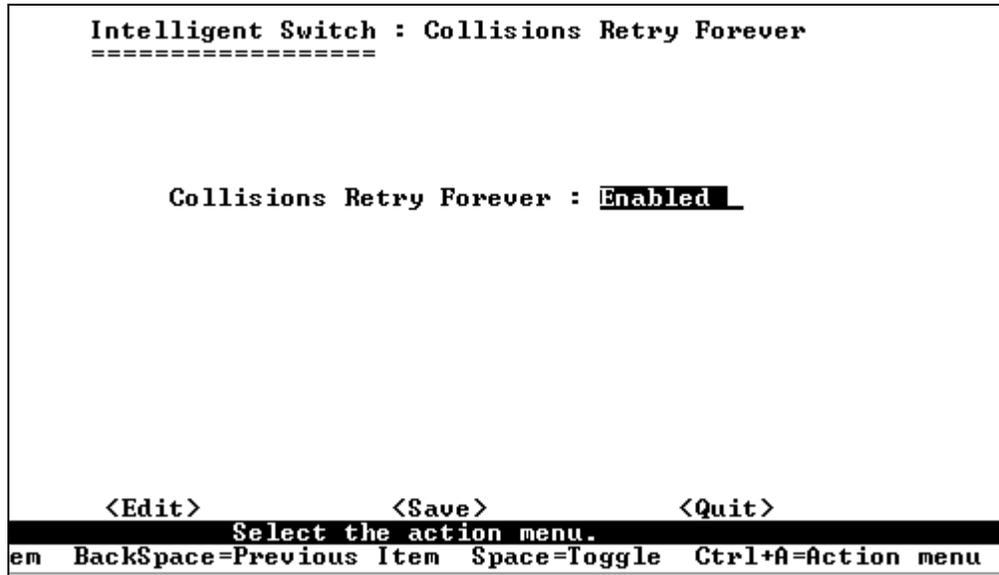


Figure 5-19: Collisions Retry Forever

Collisions Retry Forever:

- **Disable** – In half duplex, if collision happens, switch will retry 48 times for retransmission of the frame and then drop the frame.
- **Enable** – In half duplex, if collision happens, transmission will retry forever.

5.2.5 Administration Configuration

```

Intelligent Switch : Device Configuration
=====

Change Username
Change Password
Device Information
IP Configuration
Previous Menu

Configure the username.
Tab=Next Item      BackSpace=Previous Item      Enter=Select Item

```

Figure 5-20: Device Configuration

5.2.5.1 *Change Username*

Using the following page a user can change username.

```

Intelligent Switch : UserName Configuration
=====

UserName : admin

<Edit>          <Save>          <Quit>
Select the action menu.
BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item

```

Figure 5-21: User Name Configuration

Type the new user name, press <Save> item.

5.2.5.2 *Change Password*

With this page, user can change the password.

```
Intelligent Switch : Password Configuration
=====

Old Password:***
new password:*****
enter again :*****

Save successfully!press any key to return!
Esc=Previous menu
```

Figure 5-22: Password Configuration

5.2.5.3 Device Information

Device information such as Name, description and content are displayed in this page.

```
Intelligent Switch : Device Information
=====

Name      : Intelligent 24+2 Switch
Description : Intelligent 24+2 Switch
Location  :
Content   : 24 + 2 PORTS

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select
```

Figure 5-23: Device Information

5.2.5.4 IP Configuration

User can configure the IP setting and fill in the new value.

```
Intelligent Switch : IP Configuration
=====
DHCP      : Disabled
IP Address : 192.168.223.38
Subnet Mask : 255.255.248.0
Gateway   : 192.168.223.254

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

Figure 5-24: IP Configuration

IP Address for the switch can be configured either statically or using DHCP. To automatically obtain the IP address using DHCP, click on Edit and select enable and the switch automatically gives an IP address.

To statically configure the IP address, select Disabled tab; enter IP address, subnet mask and default gateway parameters

 *The L2SW Switch must be reset for the new IP address to become effective.*

5.2.6 Port Mirroring Configuration

The port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That is traffic goes in or out through the monitored ports will be duplicated into the monitoring (sniffer) port.

```

Intelligent Switch : Port Sniffer
=====

Sniffer Mode:  Rx
Monitoring Port : PORT1
Monitored Port :

Port          member
-----
PORT1        -
PORT2        v
PORT3        v
PORT4        v
PORT5        -
PORT6        -
PORT7        -
PORT8        -

ctions->      <Quit>      <Edit>      <Save>      <Previous Page>      <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action

```

Figure 5-25: Port Mirroring

Port Sniffer is configured as follows:

1. Select **Edi t**.
2. **Sni ffer Mode**: Press Space key to set sniffer mode to one of the following:
 - Disable
 - Rx
 - Tx
 - Both.
3. **Moni tori ng Port**: Sniffer port can be used to see all monitor port traffic. Press Space key to choose it.
4. **Moni tored Port**: The ports you want to monitor. All monitor port traffic will be copied to sniffer port. You can select max 25 monitor ports in the switch. User can choose which port, to be monitored in a selected sniffer mode. Press Space key to choose member port, “V” – is the member, “—“ – not the member.
5. Press **Ctrl +A** go back action menu line
6. Select **Save** to save all configure value.
7. On the action menu line you can press **Next Page** to configure port9 ~ port26, Click **Previ ous Page** return to last page.

 **Only one port can be configured in Sniffer mode at any time.**

5.2.7 Priority Configuration

The following page is used to select port priority configuration.

```

Intelligent Switch : The Priority configuration
=====

Port Static Priority

802.1p priority

Previous Menu

Configure port static priority.
BackSpace=Previous Item      Enter=Select Item

```

Figure 5-26: Priority Configuration

5.2.7.1 Port Static Priority

The static priority is set on a per port basis. If a port's priority is set to high priority, then the incoming frame from this port will be processed as a high priority packet by the switch.

```

Intelligent Switch : Port Priority
=====

Port          Priority
-----
PORT1         Low
PORT2         Low
PORT3         Low
PORT4         High
PORT9         High
PORT10        High
PORT11        Disable
PORT12        Disable

actions->    <Quit>    <Edit>    <Save>    <Previous Page>    <Next Page>
Save successfully!press any key to return!
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-27: Port Priority

5.2.7.2 802.1p Priority Configuration

```
Intelligent Switch : 802.1p Priority Configuration
=====
Will be overwritten by port-priority!!

Priority 0 : Low
Priority 1 : Low
Priority 2 : Low
Priority 3 : Low
Priority 4 : High
Priority 5 : High
Priority 6 : High
Priority 7 : High

QoSMode : First Come First Service

>          <Edit>          <Save>          <Quit>
          Select the action menu.
Item BackSpace=Previous Item Quit=Previous menu Enter=Select
```

Figure 5-28: 802.1p Priority Configuration

802.1p defines 8 priority levels which are defined as 0~7. User can map each one of the eight 802.1p priority levels to high or low queue.

1. Select **Edi t**.
2. Press **Space** key to select the priority level mapping to **Hi gh** or **Low** queue.
3. **QoS Mode**: User can select the QoS Mode as First Come First Service, Round-Robin or WRR
4. Press **Ctrl +A** go back action menu line.
5. Select **Save** to save all configure value.

5.2.8 MAC Address Configuration

```

Intelligent Switch : MAC Address Configuration
=====

      Static MAC Address
      Filtering MAC Address
      Previous Menu

Configure the MAC address.
BackSpace=Previous Item   Enter=Select Item

```

Figure 5-29: MAC Address Configuration

5.2.8.1 Static MAC Address

When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch or not. This saves the switch from having to re-learn a device's MAC address when the device is disconnected or powered-off and reconnected or powered-on again. Using the following page user can add / modify / delete a static MAC address.

```

Intelligent Switch : Static MAC Address Configuration
=====

Mac Address   Port num           Mac Address   Port num
-----

actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-30: Static MAC Address Configuration

5.2.8.1.1 Add Static MAC Address

```

Intelligent Switch : Add Static MAC Address
=====

Mac Address :0040603002FF
Port num    :PORT3

<Edit>          <Save>          <Quit>
Select the action menu.
BackSpace=Previous Item Quit=Previous menu Enter=Select

```

Figure 5-31: Add Static MAC Address

To add static MAC address, use the following procedure:

1. Press **Add** --> `edit` key to add static MAC addresses.
2. **MAC Address**: Enter the MAC address to and from which the port should permanently forward traffic, regardless of the device's network activity.
3. **Port num**: press `space` key to select the port number.
4. **VLAN ID**: If tag-based (802.1Q) VLAN are set up on the switch, static addresses are associated with individual VLANs. Type the VID to associate with the MAC address.
5. Press **Ctrl+A** to go back action menu line, and then select `save` to save all the configured values.

5.2.8.1.2 Edit Static MAC Address

```

Intelligent Switch : Static MAC Address Configuration
=====

Mac Address   Port num  Ulan ID   Mac Address   Port num  Ulan ID
-----
0040630002FF PORT3     2
000000023456 PORT5     2

actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-32: Select MAC Address

To edit static MAC address, use the following procedure:

1. Press **<Edit t>** key.
2. Choose the MAC address that you want to modify and then press enter.
3. Press **<Edit t>** key to modify all the items.
4. Press **Ctrl +A** to go back action menu line, and then select **<Save>** to save all the configured values.

```
Intelligent Switch : Static MAC Address Configuration
=====

Mac Address :0040630002FF
Port num    :PORT3
Ulan ID     :2

<Edit>      <Save>      <Quit>
Select the action menu.
BackSpace=Previous Item  Quit=Previous menu Enter=Select
```

Figure 5-33: Edit Static MAC Address

5.2.8.1.3 Delete Static MAC Address

```
Intelligent Switch : Static MAC Address Configuration
=====

Mac Address  Port num  Ulan ID      Mac Address  Port num  Ulan ID
-----
0040630002FF PORT3     2
0000000023456 PORT5     2

actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

Figure 5-34: Delete Static MAC Address

To delete static MAC address, use the following procedure:

1. Press <Delete> key.
2. Choose the MAC address that you want to delete and then press enter.
3. When pressing <Enter> once will complete deletion on delete mode.

5.2.8.2 *Filtering MAC Address*

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. Using the following page user can add /modify /delete filter MAC address.

```

Intelligent Switch : Filter MAC Address Configuration
=====
Mac Address      Ulan ID                Mac Address      Ulan ID
-----
actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
    
```

Figure 5-35: Filter MAC Address

To add MAC address filter, use the following procedure:

1. Press <Add> --> <Edit> key to add a filter MAC address.
2. **MAC Address:** Type the MAC addresses to filter.
3. **VLAN ID:** If tag-based (802.1Q) VLAN are set up on the switch, type the VID associated with the MAC address.
4. Press **Ctrl +A** to go back action menu line, and then select <Save> to save all configure value.

```

Intelligent Switch : Add Filter MAC Address
=====

Mac Address :000000000011
Ulan ID      :1

<Edit>          <Save>          <Quit>
Select the action menu.
BackSpace=Previous Item  Quit=Previous menu Enter=Select

```

Figure 5-36: Add MAC Address

To edit MAC address filter,

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

```

Intelligent Switch : Filter MAC Address Configuration
=====

Mac Address  Ulan ID          Mac Address  Ulan ID
-----
000000000011  1
000000000022  1
000000000033  2

actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-37: Filter MAC Address Configuration

3. Press <Edit> key to modify all the items.
4. Press Ctrl+A to go back action menu line, and then select <Save> to save all configure value.

```

Intelligent Switch : Edit Filter MAC Address
=====

Mac Address :0000000000033
Vlan ID      :2

<Edit>                <Save>                <Quit>
Select the action menu.
BackSpace=Previous Item  Quit=Previous menu Enter=Select

```

Figure 5-38: Edit Filter MAC Address

To delete MAC address filter, use the following procedure:

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

```

Intelligent Switch : Filter MAC Address Configuration
=====

Mac Address      Ulan ID      Mac Address      Ulan ID
-----
0000000000011   1
0000000000022   1
0000000000033   2

actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-39: Delete selected MAC Address

5.3 Protocol Related Configuration

5.3.1 STP

STP configuration through CMLI is no longer supported. Use WBI or CLI to configure STP protocol for the switch.SNMP

5.3.2 SNMP

SNMP configuration through CMLI is no longer supported. Use WBI or CLI to configure SNMP parameters for the switch.

5.3.3 GVRP

Using this page, you can enable / disable the GVRP (GARP VLAN Registration Protocol) support.

1. Select **<Edit>**.
2. Press Space key to choose **Enabled / Disabled**.
3. Press **Ctrl +A** go back action menu line.
4. Select **<Save>** to save the configured value.

 **For system performance reasons, it is recommended that the number of dynamically learnt GVRP entries be limited to 128.**

About the GVRP description please see the *Page17*.

```
Intelligent Switch : GVRP Configuration
=====

GVRP : Enabled

<Edit>           <Save>           <Quit>
Select the action menu.
BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu
```

Figure 5-40: GVRP Configuration

5.3.4 IGMP

Using this page, you can enable / disable the IGMP snooping support.

1. Select **<Edit>**.
2. Press Space key to choose **Enabled / Disabled**.
3. Press **Ctrl +A** go back action menu line.
4. Select **<Save>** to save configure value.

```
Intelligent Switch : IGMP Configuration
=====

IGMP : Enabled

<Edit>          <Save>          <Quit>
Select the action menu.
BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item
```

Figure 5-41: IGMP Configuration

5.3.5 LACP

Using this page, user can configure and view the LACP status.

```
Intelligent Switch : LACP Configuration
=====

Working Ports Setting
State Activity
LACP Status
Previous Menu

LACP setting.
Tab=Next Item   BackSpace=Previous Item   Enter=Select Item
```

Figure 5-42: LACP Configuration

5.3.5.1 Working Port Setting

```
Intelligent Switch : LACP Group Configuration
=====

Group      LACP Work Port Num
-----
TRK2      2

<Edit>          <Save>          <Quit>
Select the action menu.
m BackSpace=Previous Item  Space=Toggle  Ctrl+A=Action menu
```

Figure 5-43: LACP Group Configuration

LACP Group Trunking is configured as follows:

1. Select **<Edit>**.
2. **Group**: Display the trunk group ID.
3. **LACP Work Port Num**: The parameter defines the max number of ports that can be aggregated at the same time. If LACP static trunking group number exceeds the LACP work port num, the excess ports are assigned to standby mode. These standby ports would be able to join the static trunking group, if any of the working port fails. If local static trunking group is used this number must be the same as group ports.

 **Prerequisite for configuring LACP trunking is to set up Trunk Configuration first.**

5.3.5.2 State Activity

Activity of the ports is displayed in this page. The port is said to be active if it sends LACP protocol packets. It is in passive mode, if it does not automatically send LACP protocol packets

Intelligent Switch : LACP Port State Active Configuration			
=====			
Port	State Activity	Port	State Activity

5	Active		
6	Active		
7	Passive		
8	Passive		

ptions-> <Edit> <Save> <Quit>
Save successfully!press any key to return!
=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

Figure 5-44: LACP Port State Active Configuration

To configure the LACP port state configuration, use the following procedure:

1. Select **<Edit>**.
2. Press **Space** key to choose the item.

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.

3. Press **Ctrl +A** go back action menu line.

4. Select **<Save>** to save the configured value.

5.3.5.3 LACP Status

If Link Aggregation Control Protocol is enabled, the group is LACP static trunking group. If it is disabled, the group is Local static trunking group.

```

Intelligent Switch : LACP Group Status
=====

                Static Trunking Group

Group Key : 1
Port_No   : 1 2 3 4

<Quit>      <Previous Page>    <Next Page>
Select the action menu.
m BackSpace=Previous Item  Quit=Previous menu Enter=Select Item_

```

Figure 5-45: LACP Static Trunking Group

5.3.5.4 LACP trunk group

```

Intelligent Switch : LACP Group Status
=====

                Group
                [Actor]                [Partner]

Priority:      1                        1
MAC          : 004063809988            004063808899

Port_No  Key   Priority  Active   Port_No  Key   Priority
5        514   1         selected 5        514   1
6        514   1         selected 6        514   1
7        514   1         selected 7        514   1
8        514   1         selected 8        514   1

actions->    <Quit>      <Previous Page>    <Next Page>
Select the action menu.
ab=Next Item BackSpace=Previous Item  Quit=Previous menu Enter=Select Item

```

Figure 5-46: LACP Group Status

5.4 Status and Counters

```

Intelligent Switch : Status and Counters
=====

Port Status
Port Counters
System Information
Main Menu

Display current status of all the switch ports.
Tab=Next Item BackSpace=Previous Item Enter=Select Item

```

Figure 5-47: Status and Counters

5.4.1 Port Status

Port Status page displays interface state, link status, flow control, etc information for each port.

```

Intelligent Switch : Port Status
=====

Port      Link Status  InRate  OutRate  Enable  Auto  Spd/Dpx  Flow Control
<100K>  <100K>
-----
PORT1    Down         0        0        Yes     AUTO  10 Half  Off
PORT2    Down         0        0        Yes     AUTO  10 Half  Off
PORT3    Down         0        0        Yes     AUTO  10 Half  Off
PORT4    Down         0        0        Yes     AUTO  10 Half  Off
PORT9    Up           0        0        Yes     AUTO  100 Full On
PORT10   Down         0        0        Yes     AUTO  10 Half  Off
PORT11   Down         0        0        Yes     AUTO  10 Half  Off
PORT12   Down         0        0        Yes     AUTO  10 Half  Off

actions->  <Quit>      <Previous Page>  <Next Page>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

Figure 5-48: Port Status

Link Status: Display the status of the port: link is up or down. **InRate:** Display the value of input rate control (100K/unit).

OutRate: Display the value of output rate control (100K/unit).

Enabled: Display the port is enabled or disabled depended on user setting. If a port is enabled, the

status of that port will be displayed as “Yes”, otherwise, the status of that port will be displayed as “No”.

Auto: Display the auto-negotiation status of the port:

- Auto
- Nway_Force
- Force.

Spd/Dpx: Display the port speed and duplex.

Flow Control : In auto / Nway force mode, flow control is enabled or disabled after negotiation. In force mode, flow control status is enabled or disabled depending on user setting.

5.4.2 Port Counters

Port Counters page displays transmission and reception statistics, etc information for each port.

Intelligent Switch : Port Counters							
Port	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
PORT1	0	0	0	0	0	0	0
PORT2	0	0	0	0	0	0	0
PORT3	0	0	0	0	0	0	0
PORT4	0	0	0	0	0	0	0
PORT9	7026	0	5723	0	0	0	0
PORT10	0	0	0	0	0	0	0
PORT11	1842	0	491	0	0	0	0
PORT12	0	0	0	0	0	0	0

actions-> <Quit> <Reset All> <Previous Page> <Next Page>

Configure the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

Figure 5-49: Port Counters

5.4.3 System Information

System Information page displays MAC Address, Firmware Version, Serial Number and Module information of the Switch.

```

Intelligent Switch : System Information
=====

MAC Address           : 004063809988
Firmware version     : 2.5
ASIC version         : A7.0
PCBA version         : 1.0
Serial number        :
Module 1 Type        : 1000Tx
Module 1 information : N/A
Module 2 Type        : 1000Tx
Module 2 information : N/A

Display the switch system.
Esc=Previous menu_

```

Figure 5-50: System Information

MAC Address: The unique hardware address assigned by manufacturer.

Firmware Version: Display the switch's firmware version.

ASIC Version: Display the switch's Hardware version.

PCBA version: Display the board number.

Serial number: Display the serial number assigned by manufacturer.

Module 1 Type: Display the module 1 type :1000Tx or 100Fx ext. Depend on module card mode.

Module 1 information: Display the information saved in eeprom of module1.

Module 2 Type: Display the module 2 type :1000Tx or 100Fx ext. Depend on module card mode.

Module 2 information: Display the information saved in eeprom of module2.

5.5 Reboot Switch

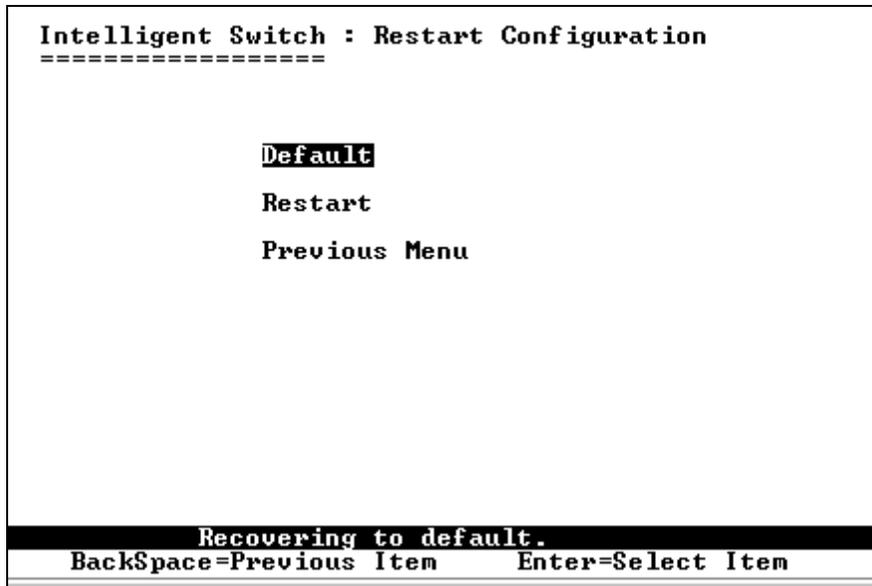


Figure 5-51: Restart Configuration

5.5.1 Default

Reset switch to default configuration. If you type “Y”, the switch will load default configuration. After finished loading the default configuration, the switch will reboot automatically.

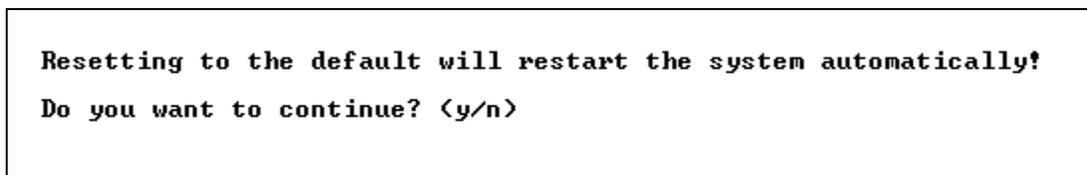


Figure 5-52: Default Setting

5.5.2 Restart

Reboot the switch in software reset.

5.6 TFTP Update Firmware

This page is used to download firmware and upload/download configuration database.

```
Intelligent Switch : TFTP Update firmware Configuration
=====

TFTP Update Firmware
TFTP Restore configuration
TFTP Backup configuration
Previous Menu

Use TFTP to update firmware.
BackSpace=Previous Item      Enter=Select Item
```

Figure 5-53: TFTP Update Firmware Configuration

5.6.1 TFTP Update Firmware

```
Intelligent Switch : TFTP Update Firmware
=====

TFTP Server      : 192.168.223.99
Remote File Name : image.bin

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item
```

Figure 5-54: Edit TFTP Update Firmware

This page is used to update the firmware, using TFTP.

1. Start the TFTP server, and copy firmware update version image file to TFTP server.
2. Press <Edit> on this page.
3. **TFTP Server:** Type the IP of TFTP server.

4. **Remote File Name:** Type the image file name.
5. Press **Ctrl +A** go to action line.
6. Press **<Save>** key, it will start to download the image file.
7. When saved successfully, the image file gets downloaded.
8. Restart switch.

5.6.2 Restore Configure File

To restore configuration database of the switch from a backup copy stored on a TFTP server, use the following page.

```

Intelligent Switch : Restore Configuration File
=====

      TFTP Server       : 192.168.223.99
      Remote File Name  : data.dat

      <Edit>           <Save>           <Quit>
      Select the action menu.
      BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item

```

Figure 5-55: Restore Configuration File

To restore configuration:

1. Start the TFTP server.
2. Press **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl +A** go to action line.
6. Press **<Save>** key, it will start to download the image file.
7. When saved successfully, the image file gets downloaded
8. Restart switch.

5.6.3 Backup Configure File

User can backup the configuration database of the switch, using this page.

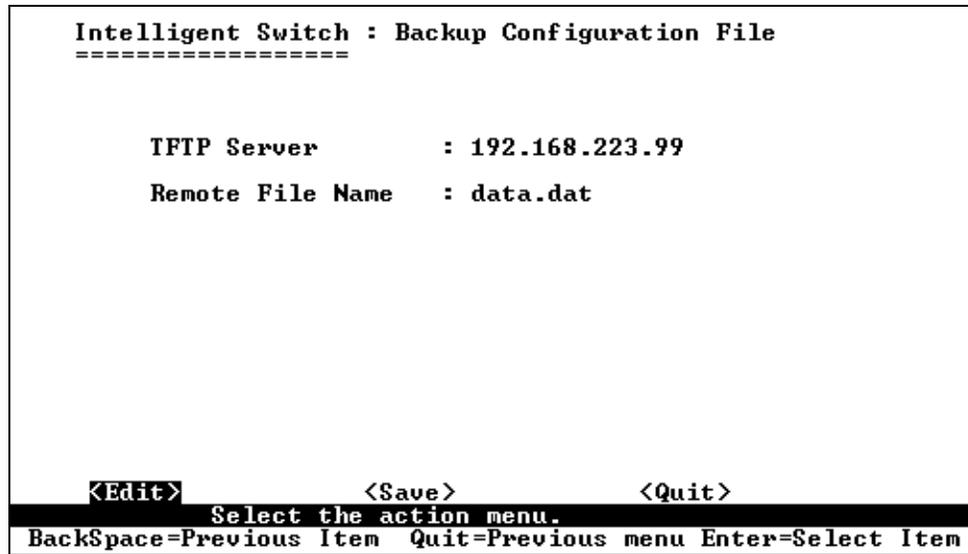


Figure 5-56: Backup Configuration File

To backup EEPROM:

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

6. CLI based Management

The L2SW switch can be managed using CLI commands over the dedicated serial interface or via a telnet session.

- CLI based management interprets the following control key sequences as character/line editor commands. User can get a list of choices in a command line by using the “?” character. The keyword “end” can be used to return from the currently active CLI command tree to the root command prompt (i.e, the prompt displayed after login). The keyword “exit” is used to return from the currently active CLI command tree to its parent command prompt.

<code>, <BS></code>	Delete previous character
<code><Ctrl-A></code>	Go to beginning of line
<code><Ctrl-E></code>	Go to end of line
<code><Ctrl-F></code>	Go forward one character
<code><Ctrl-B></code>	Go backward one character
<code><Ctrl-D></code>	Delete current character
<code><Ctrl-U></code>	Delete to beginning of line
<code><Ctrl-K></code>	Delete to end of line
<code><Ctrl-W></code>	Delete previous word
<code><Ctrl-T></code>	Transpose previous character
<code><Ctrl-P></code>	Go to previous line in history buffer
<code><Ctrl-N></code>	Go to next line in history buffer
<code><Ctrl-Z></code>	Return to root command prompt
<code><TAB></code>	Command-line completion
<code>end</code>	Return to root command prompt
<code>exit</code>	Go to parent command prompt
<code>?</code>	(help command) List choices

- Depending on the access level, the following commands are available to the use to configure and control the switch
 - `clear` Clear or restore configuration to factory defaults.
 - `config` Configure switch options and settings
 - `copy` Transfer a file to or from the switch
 - `help` Help for CLI commands
 - `logout` Exit this session. Any unsaved changes will be lost
 - `menu` Enter menu interface.
 - `reset` Reset the switch
 - `save` Save switch configurations
 - `show` Display switch options and settings

CLI: CLI commands allow the user to configure various features such as Spanning Tree Protocol, VLAN, MAC filter, Port Mirroring, Priority Queue, 802.1x and also perform a set of maintenance related functions such as user password maintenance, log traps, configuration upload and download

L2SW switch provides a command line interface for the management & monitoring purposes. The command line interface can be accessed thru serial RS-232 port or thru a telnet session. User can configure the Windows HyperTerminal program for speed and parity as per the Console Port Information displayed in the WBI.

The switch will displays the login prompt when it is ready as shown below in Figure 6-1. User has to specify the user name and password to login into the switch. The default user name is “admin”. For default password, please contact your sales representative .

```

User Interface
<c> Intelligent 24 + 2 Standalone Switch

username : admin
password : ***

```

Figure 6-1 Login Prompt

After successful login, the switch will display the CLI prompt **L2SW>**⁶ indicating that it is ready to accept CLI commands from the user.

The following sections provide a complete description of configuration and monitoring commands available to the user thru the command line interface.

6.1.1 CLI Syntax Conventions

Command	Description
Command Name and parameters	Text displayed in bitstream Vera Sans fonts after the L2SW> prompt must be typed exactly as shown. Following the syntax of a command, an example usage of the command is shown. Output of the command is shown either in Italics or as a terminal capture.
<parameter>	The <> angle brackets indicates that the parameter is required for executing the command
[parameter]	The [] square brackets indicates that the parameter is optional
choi ce1 choi ce2	The indicate that only one of the parameter should be entered
l paddr	This parameter is a valid IP address of four decimal bytes (separated by .), each byte ranging from 0 to 255. The default IP is usually 0.0.0.0

⁶ Note the user can customize the CLI prompt using `Config` command

Command	Description
<code>Macaddr</code>	The MAC address format is six hexadecimal numbers separated by colons, for e.g., 0:20:10:32:0e:40
<code>slot.port</code>	This parameter denotes a valid slot number and a valid port number. For example 0.1 represents slot 0 port 1

6.1.2 Login User Setup

User Id and password are required for all users trying to access and manage L2SW switch. L2SW switch supports only one login account with full access rights.

Read Write (admin) Level Access- to run config, show, reset, save, clear, commands to configure, maintain and troubleshoot the L2SW switch. The login account name (admin) with password (12sw) is pre-configured and cannot be deleted, but password can be changed using following commands:

```
L2SW> config user password <name> <passwd>
L2SW> config user password admin ess
```



To restore default password settings for admin account use “clear config” command.

6.1.3 Network Port Access Setup

If one of the network ports is used for in-band management, use the following command to configure that port:

1. If DHCP is used:

```
L2SW> config network protocol <none/dhcp>
L2SW> config network protocol dhcp
```

2. If static IP address is used:

```
L2SW> config network protocol <none/dhcp>
L2SW> config network protocol none

L2SW> config network parms <ipaddr> <netmask> [gateway]
L2SW> config network parms 172.30.30.221 255.255.255.0 172.30.30.2
```

Where, 172.30.30.221 - IP address assigned for in-band management,
255.255.255.0 - network mask to be assigned for in-band management;
172.30.30.2 - IP address of the default gateway.



The default protocol is none. After changing protocol type from none to DHCP, the switch needs to be rebooted using “reset switch” command.

6.1.4 Telnet Access Setup

A telnet session to the L2SW switch can be initiated by starting any telnet client software on the management station (for e.g., from a PC running any Windows Operating System, type `telnet a.b.c.d` where, `a.b.c.d` is the IP address of the L2SW switch).

Once a telnet connection is established, the switch will prompt the user to enter user ID and password. After entering a valid user id and password, CLI prompt will be displayed.

- **Maximum number of sessions** – Up to five simultaneous telnet sessions can be created.
- **Inactivity Timeout** - Telnet session will be terminated after the 5 minutes of inactivity. The value of Inactivity Timeout for a Telnet session is not configurable.



CMLI is not available for Telnet Sessions.

6.1.5 Serial Port Setup

L2SW switch has a RS-232 serial interface located on the back of the switch. Any terminal with VT100 terminal emulation capabilities can be connected using a standard RS-232 serial cable. The following terminal settings have to be configured for serial communication to work correctly:

- **Baud Rate** = 19200
- **Data Bits** = 8
- **Parity** = none
- **Stop Bits** = 1
- **Flow Control** = none

6.1.6 Inactivity Timeout

L2SW Session will be terminated after 5 minutes (default value) of inactivity. The inactivity time can be configured using following command.

```
L2SW> confi g seri al time out <0-160>
L2SW> confi g seri al time out 30
```



The session will never expire if the timeout value is set to 0 minutes.

To display the serial port settings use following command:

```
L2SW> show seri al
```

6.2 Stacking Configuration

Stacking capability provides a single management point for multiple L2SW switches, and increases the port density in L2SW. L2SW supports cascade mode by connecting stack up link port to down link port. To form a stack, all the units including master unit and slave units that need to participate in the stack must be informed that the unit should participate in the stack, e.g., by manual configuration, by automatic discovery using dedicated stacking ports, or by combination of manual configuration in the master unit and control protocol among stacked units. Stacked switches can be managed as if it were a single integrated switch. Stacking configuration commands only allowed on master unit. The following set of commands can be used to configure Stacking and provide an approach to manage slave units.

1. To enable or disable administrative mode of stacking, use the following command. By default,

the administrative mode of stacking is disable. The switch that executes this command successfully is configured as the master unit.

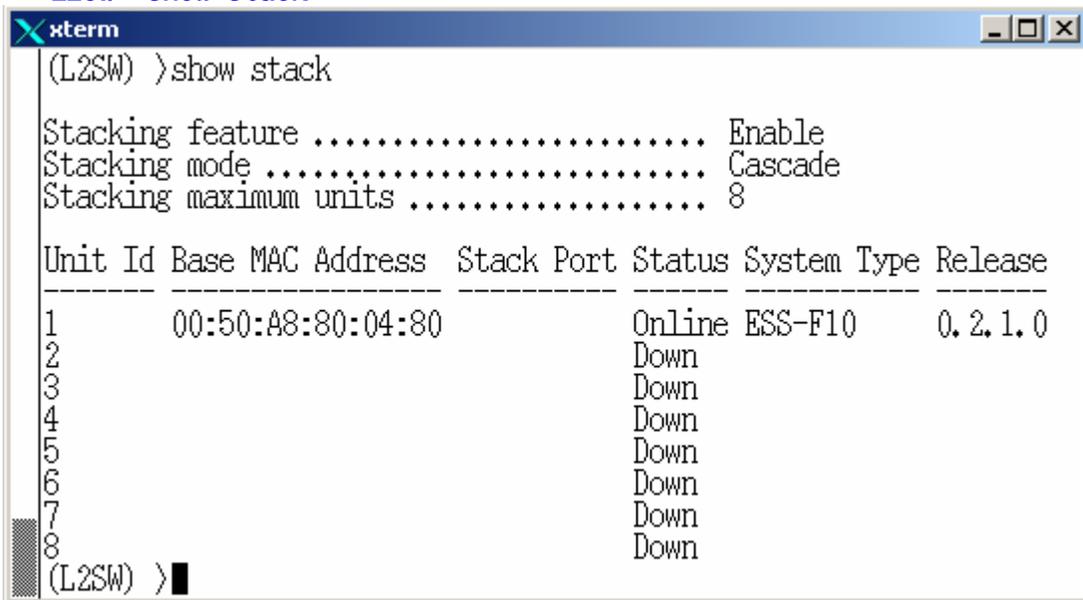
```
L2SW> confi g stack admi nmode <enabl e/di sabl e>  
L2SW> confi g stack admi nmode enabl e
```

2. The number of units in the stack can be 2 to 8 by modifying stack height. By default, the stack height is 8.

```
L2SW> confi g stack maxuni ts <uni tcount(2-8)>  
L2SW> confi g stack maxuni ts 5
```

3. To display stack configuration, use the following command. The table below shows stack parameters such as stack mode, administration status, stack heights and information about units in the stack.

```
L2SW> show stack  
L2SW> show stack
```



```
(L2SW) >show stack  
  
Stacking feature ..... Enable  
Stacking mode ..... Cascade  
Stacking maximum units ..... 8  
  
Unit Id Base MAC Address Stack Port Status System Type Release  
-----  
1 00:50:A8:80:04:80 1 Online ESS-F10 0.2.1.0  
2 Down  
3 Down  
4 Down  
5 Down  
6 Down  
7 Down  
8 Down  
(L2SW) > █
```

Figure 6-2 Displays Stack

4. To manage slave units, login to slave unit by using unit ID. The slave unit prompt will be displayed to remind you are working on that unit right now. Only one unit can be managed at a given time.

```
L2SW> tel net <uni t i d(2-8)>  
L2SW> tel net 2
```

5. To return back to master, logout from slave unit.

```
L2SW> l ogout  
L2SW> l ogout
```

 *Stacking configuration is not available on CMLI interface.*

6.3 Port Configuration

6.3.1 Display Port Configuration

show port command displays interface information such as speed, duplex mode and connector type. User can choose to display the configuration of an individual port by typing the port number (e.g., 0.12) or choose to display the configuration of all the ports of the switch by typing the keyword “all” after the **show port** command.

```
L2SW> show port <slot.port/all >
L2SW> show port all
```

The first column in the display, `Slot.Port`, indicates the type of physical/logical port and the associated port number. The following are the possible slot options values:

- **0** – 10/100Mbps FE ports in L2SW switch
- **1** – Fixed gigabit port or Port on the plugin-in module

The second column indicates port `Type`. If the port is a FE port, this field is displayed as 100Tx. If the port Gigabit it is displayed as 1000Tx.

The third column displays the administrative mode for the port. Depending on the state of the port, one of the following values will be displayed:

- **Yes** – Admin mode enable
- **No** – Admin mode disable

The fourth column displays the `Physical Mode`, which is either `Manual` or `Auto`. In `Auto` mode, Speed is set by auto-negotiation process.

The fifth column indicates `Physical Status` – Indicates the port speed and duplex mode. Note that the values displayed indicate the capabilities negotiated with the peer and not necessarily the capabilities of the switch itself. Depending on the negotiated or configured values, one of the following values will be displayed for each port:

- **10 Hal f** – 10 Base-T, Half-duplex
- **10 Ful l** – 10 Base-T, Full duplex
- **100 Hal f** – 100 Base-T Half duplex
- **100 Ful l** – 100 Base-T or 100 Base-FX, Full duplex
- **1000 Ful l** – 1000 Base-T or 1000 Base-SX/LX, Full duplex

The sixth column indicates the actual speed of the connected network element.

The seventh column indicates the `Link Status` – Indicates whether the link is up or down.

The eighth column indicates whether the Flow control is on or off

The ninth and tenth column indicates the Rate Control settings for ingress and egress side of each port.

The eleventh column indicates the port priority status. Values displayed under this column are High or Low or Off (Disabled)

The twelfth column indicates the security status of the port. On indicates security is enabled and off

indicates security is disabled.

By default, admin and auto negotiation modes are enabled on all ports.

```
L2SW >show port all
```

Port	Type	Admin Enable	Auto	Spd Dpx	Spd State	Link Status	FC	Rate(100K) In	Rate(100K) Out	pri	security
0.1	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.2	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.3	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.4	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.5	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.6	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.7	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.8	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.9	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.10	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.11	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.12	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.13	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.14	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.15	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off

Would you like to display the next 15 entries? (y/n)

Port	Type	Admin Enable	Auto	Spd Dpx	Spd State	Link Status	FC	Rate(100K) In	Rate(100K) Out	pri	security
0.16	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.17	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.18	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.19	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.20	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.21	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.22	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.23	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off
0.24	100TX	Enable	Auto	100F	100F	Down	On	0	0	None	Off

```
L2SW >
```

Figure 6-3: Port Status Display

6.3.2 Port Configuration Settings

The following parameters associated with a port on L2SW switch can be configured:

- Port's Administrative mode
- Auto negotiation mode
- Link Up/Down trap
- Port Speed & duplex settings

- Flow Control
- Rate Limit
- Priority selection
- Security control

User can enable or disable the administrative mode of each port using the following command. When a port is disabled, it will not forward any traffic. However, it will retain all the configured values associated with that port. To enable/disable the administrative mode of a port, use the following command:

```
L2SW> config port adminmode <slot.port/all> <enable/disable>
L2SW> config port adminmode 0.1 enable
```

Use the following command to set the port in auto negotiation, forced speed.

```
L2SW> config port autoneg <slot.port/all> <auto/force/nway>
L2SW> config port autoneg 0.1 auto
```

 **Auto negotiation cannot be set on trunk port.**

You can set the duplex mode of any port as full or half duplex, the speed of a FE port as 10 Mbps or 100Mbps and the speed of a gigabit TX port as 100 Mbps or 1000 Mbps. In the L2SW switch, the speed and duplex mode for SX/LX port is fixed at 1000 Mbps, full duplex. The following command can be used to manually configure the speed and duplex mode of an individual port or all ports:

```
L2SW> config port physical mode <slot.port/all> <1000f/100h/100f/10h/10f>
L2SW> config port physical mode 0.1 100f
```

 **For physical mode configurations to take effect, auto-negotiation must be disabled.**

To enable or disable the flow control on any selected port or on all the ports use following command:

```
L2SW> config port flowcontrol <slot.port/all> <enable/disable>
L2SW> config port flowcontrol 0.1 enable
```

 **The flow control status displays the actual status instead of the configuration value. The flow control status varies based on the link status, duplex mode, auto/force mode, peer side settings when AN is enabled.**

To control the ingress (in) or egress (out) traffic on any port or all the ports use the following command. The bandwidth (ratelimit) on any port has valid range from 0-1000. The unit is 100K, where 0 means rate control is disabled.

```
L2SW> config port ratelimit <in/out> <slot.port/all> <ratelimit>
L2SW> config port ratelimit in 0.1 1000
L2SW> config port ratelimit out 0.1 1000
```

 **Flow control must be enabled for Ingress rate limit to work properly**

To configure static priority on any port or all the ports of the switch use following command:

```
L2SW> config port priority <slot.port/all> <none/low/high>
L2SW> config port priority 0.1 low
```

i In order to apply static port priority, First Come First Served mode must be disabled.

The following command configures the administration mode of port priority. A port in security mode will be locked with address learning capabilities disabled. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses used by the secure port.

```
L2SW> config port security <slot.port/all> <enable/disable>
L2SW> config port security all disables
```

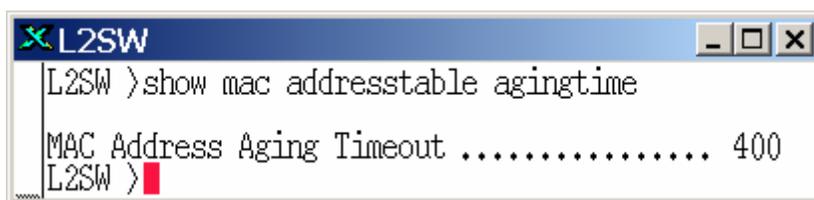
6.4 MAC Aging

The L2SW forwarding database holds the MAC addresses learnt by the switch. The addresses stored in this database are dynamically learnt and are deleted after the age out period. The valid range for MAC address aging time is from 10 to 765 seconds. The default value is 300 seconds. To configure the MAC address table aging time use the following command.

```
L2SW> config mac addressstable agingtime <time>
L2SW> config mac addressstable agingtime 400
```

To display the MAC address table ageing time use the following commands:

```
L2SW> show mac addressstable agingtime
```



```
L2SW
L2SW >show mac addressstable agingtime
MAC Address Aging Timeout ..... 400
L2SW >
```

Figure 6-4 MAC table aging time

6.5 Static MAC Address

When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch or not. This saves the switch from having to re-learn a device's MAC address when the device is disconnected or powered-off and reconnected or powered-on again. Using the following command syntax, user can add / modify / delete a static MAC address.

```
L2SW> config mac addressstable static add <macaddr> <slot.port>
L2SW> config mac addressstable static add 00:00:00:10:00:10 10 0.1
```

- **macaddr** – Destination MAC address to add to the address table. Packets with this destination Address received in the specified VLAN is forwarded to the specified port.
- **slot.port** – Interface to which the received packet is forwarded. Valid interfaces include physical ports and trunk ports.

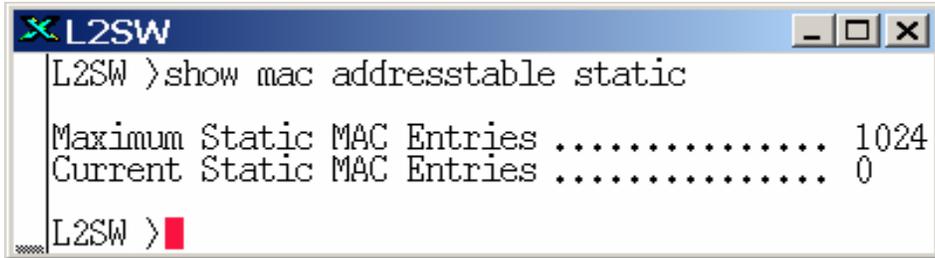
To delete the static MAC address entry from the address table, use following command:

```
L2SW> config mac addressstable static delete <macaddr> <slot.port>
```

```
L2SW> config mac addressstable static delete 00:00:00:10:00:10 10 0.1
```

To display the static MAC address table use the following command. Response from the switch to this command is displayed in Figure 6-5.

```
L2SW> show mac addressstable static
```

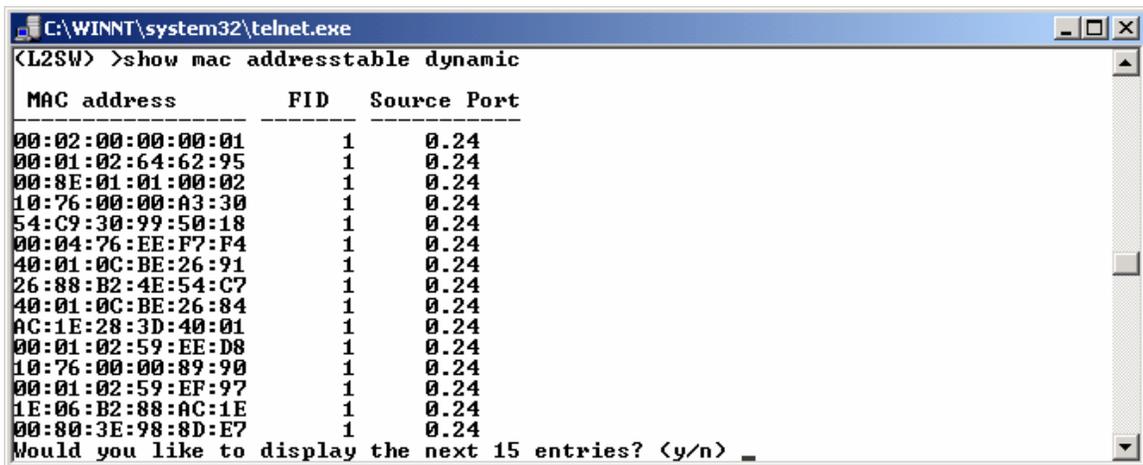


```
L2SW >show mac addressstable static
Maximum Static MAC Entries ..... 1024
Current Static MAC Entries ..... 0
L2SW >
```

Figure 6-5 show static MAC address entries

i To prevent static MAC data being lost, configure VLAN mode before configuring static MAC.

To display MAC addresses dynamically learnt by the switch, use the following command. Figure 6-6 displays MAC addresses dynamically learnt by the switch.



```
C:\WINNT\system32\telnet.exe
(L2SW) >show mac addressstable dynamic
MAC address      FID  Source Port
-----
00:02:00:00:00:01  1    0.24
00:01:02:64:62:95  1    0.24
00:8E:01:01:00:02  1    0.24
10:76:00:00:A3:30  1    0.24
54:C9:30:99:50:18  1    0.24
00:04:76:EE:F7:F4  1    0.24
40:01:0C:BE:26:91  1    0.24
26:88:B2:4E:54:C7  1    0.24
40:01:0C:BE:26:84  1    0.24
AC:1E:28:3D:40:01  1    0.24
00:01:02:59:EE:D8  1    0.24
10:76:00:00:89:90  1    0.24
00:01:02:59:EF:97  1    0.24
1E:06:B2:88:AC:1E  1    0.24
00:80:3E:98:8D:E7  1    0.24
Would you like to display the next 15 entries? (y/n) _
```

Figure 6-6: Dynamically Learnt MAC Addresses Display

i To flush all dynamically learnt MAC addresses, configure MAC address agetime to 10 seconds, wait for 10 seconds and then reset the MAC address agetime to desired value.

6.6 MAC Filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. Maximum of 1024 static MAC filtering entries can be added. Using the following command, user can add/delete filter MAC address

```
L2SW> config mac filter add <macaddr>
L2SW> config mac filter add 00:00:10:00:10
```

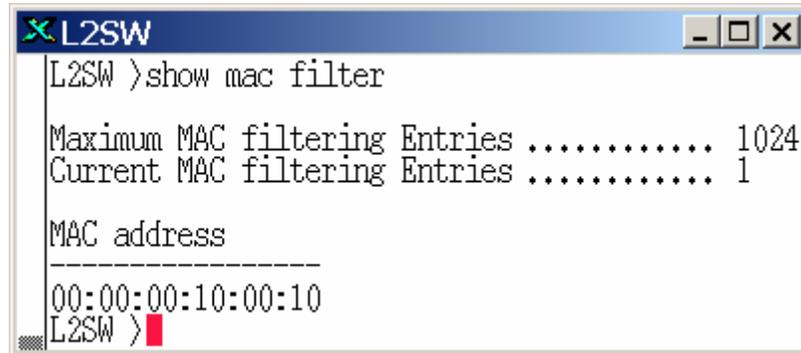
To remove the MAC filtering entry use following command:

```
L2SW> config mac filter delete <macaddr>
```

```
L2SW> confi g mac fi lter add 00:00:10:00:10
```

To display the MAC filter table, use following command:

```
L2SW> show mac fi lter
```



```
L2SW >show mac filter
Maximum MAC filtering Entries ..... 1024
Current MAC filtering Entries ..... 1

MAC address
-----
00:00:00:10:00:10
L2SW >
```

Figure 6-7 Displays MAC filter entries

i To prevent MAC filter data being lost, configure VLAN mode before configuring MAC filter.

6.7 VLAN

A VLAN is an arbitrary grouping of nodes on the network. This grouping promotes efficient use of network resources and facilitates productive entry of repetitive network transactions. Conceptually, a VLAN allows the network administrator to structure, separate, or partition the network. For example, these structures in existing LANs are subnets in IP networks or broadcast domains in bridged networks. When multiple LAN segments are bridged together, the bridged segments still "see" all broadcast and multicast traffic on each LAN that is physically connected to the bridges and shared media hubs. The number of stations or LAN segments that can be bridged without creating excessive broadcast traffic on the LAN segments is limited. To avoid excessive broadcast traffic, networks must be divided into subnets and typically subnets are constrained by the physical LAN structure. VLANs are used to overcome some of these constraints involved in configuring the network.

L2SW supports the following three types of VLANs:

- Port base VLAN
- Tag based VLAN
- Protocol based VLAN

The following commands can be used to display the configuration of VLAN type, add or delete a port attached to a VLAN.

1. To configure the VLAN mode on the switch, use following command:

```
L2SW> Conf ig vl an mode <none/port/dot1q>
L2SW> confi g vl an mode port
```

None – To disable VLAN on the switch

Port – Enable port-based VLAN mode, tag-based VLAN is excluded. All packets will be associated with default port VID before forwarding, and no tag modification (insert, modify or remove) will take place when the packet is transmitted out of this port. Only

Shared VLAN (SVL) is supported in this mode.

Dot1q – Enable both port-based VLAN and tag-based VLAN. A default VLAN with VLAN ID 1 is created and assigned to all ports, once the mode is set to dot1q.

2. To create a VLAN, use the following commands. The valid range is from 2- 4094. An alphanumeric name can be assigned to the created VLAN. The maximum length of the alphanumeric string is 16 characters.

```
L2SW> confi g vl an create <vl ani d> <name>
L2SW> confi g vl an create 10 Yel low
```

3. To add or delete a port to a new VLAN, use the following command. This command can be used for both port-based VLAN and Protocol based VLAN.

```
L2SW> confi g vl an addport <vl ani d> <sl ot. port>
L2SW> confi g vl an addport 10 0. 1
```

```
L2SW> confi g vl an del port <vl ani d> <sl ot. port>
L2SW> confi g vl an del port 10 0. 1
```

4. To remove VLAN, use the following command:

```
L2SW> confi g vl an del ete <vl ani d>
L2SW> confi g vl an del ete 10
```

5. To configure protocol based VLAN, use following command:

```
L2SW> confi g vl an protocol <vl ani d> <protocol type>
L2SW> confi g vl an protocol 10 IP
```

vl ani d – A valid VLAN ID. The valid range is 2-4094.

protcol type – protocol type supported by the switch. Valid options are:

None, IP, Arp, Appletalk, Appletalk_aarp, Novelll_ipx, BANYAN_VINES_C4,
BANYAN_VINES_C5, BANYAN_VINES_AD, DECNET_MOP_01,
DECNET_MOP_02, DECNET_DPR, DECNET_LAT, DECNET_LAVC, IBM_SNA,
X75_INTERNET, X25_LAYER3

To configure the degree of participation for a specific port in a VLAN, use the following command:

```
L2SW> confi g vl an port pvi d <vl ani d> <sl ot. port/all >
L2SW> confi g vl an port pvi d 10 0. 1
```

vl ani d – A valid VLAN ID. The valid range is 1-4094.

sl ot. port –physical port or trunk port, or all. .

6.7.1 802.1Q VLAN

To configure tag-based VLAN, use the following set of commands:

1. Configure the VLAN mode dot1q on the switch. By default VLAN is disabled on the switch and mode settings are none.

```
L2SW> Confi g vl an mode <none/port/dot1q>
```

```
L2SW> config vlan mode dot1q
```

2. Create VLAN and add tagged member ports to it.

```
L2SW> config vlan create <vlan id> <name>  
L2SW> config vlan create 10 Yellow
```

3. Enable tagging and add tagged member ports to it.

```
L2SW> config vlan port tagging <enable/disable> <vlan id> <slot.port>  
L2SW> config vlan port tagging enable 10 0.1
```



If the trunk groups exist and if trunks ports have to be configured as part of a VLAN, then add trunk id instead of port number.

6.7.2 Port VID & Ingress filtering

Set the port VLAN ID, assigned to untagged traffic on a given port. This feature is useful for accommodating devices that user wants to participate in VLAN but that don't support tagging. L2SW each port allows user to set one PVID, the range is 1-4094 default PVID is 1. The PVID must be same as VLAN ID, that the port belongs to VLAN group, or the untagged traffic will be dropped. The following command is for PVID configuration:

```
L2SW> config vlan port pvid <1-4094> <slot.port/all>  
L2SW> config vlan port pvid 10 0.1
```

Note that PVIDs cannot be assigned arbitrarily. Instead, all the PVIDs must take on values within the same PVID set. The following list depicts the relation between the PVID sets and value of PVID.

- PVID Set 0. PVID range: 0 - 255
- PVID Set 1. PVID range: 256 - 511
- PVID Set 2. PVID range: 512 - 767
- PVID Set 3. PVID range: 768 - 1023
- PVID Set 4. PVID range: 1024 - 1279
- PVID Set 5. PVID range: 1280 - 1535
- PVID Set 6. PVID range: 1536 - 1791
- PVID Set 7. PVID range: 1792 - 2047
- PVID Set 8. PVID range: 2048 - 2303
- PVID Set 9. PVID range: 2304 - 2559
- PVID Set 10. PVID range: 2560 - 2815
- PVID Set 11. PVID range: 2816 - 3071
- PVID Set 12. PVID range: 3072 - 3327

- PVID Set 13. PVID range: 3328 - 3583
- PVID Set 14. PVID range: 3584 - 3840

PVID Set 15. PVID range: 3841 – 4095

1. Ingress filtering feature allows only those frames belonging to a specific VLAN to be forwarded, if the port belongs to that VLAN. Disabling these settings will cause all frames to be forwarded, regardless of the port's VLAN settings. The following command is for Ingress settings on the port.

```
L2SW> confi g vl an port i ngressfi lter <enabl e/di sabl e> <sl ot. port/all >
L2SW> confi g vl an port i ngressfi lter enabl e 0. 1
```

Enabl e – To enables ingress filtering on the specified port.

Di sabl e – To disables ingress filtering on the specified port.

Sl ot. port – Physical port or trunk port, or all.



To configure ingress filter on any selected port or all ports, 802.1q based VLAN must be enabled.

2. To configure the switch whether to accept tagged or untagged frames, use following command syntax:

```
L2SW> confi g vl an port acceptframe <all /vl anonly> <sl ot. port/all >
L2SW> confi g vl an port acceptframe vl anonly 0. 1
```

all /vl anonly – To accepts all frames or only tagged frames.

sl ot. port/all – Physical port or trunk port.

6.7.3 Show VLAN

There are various display commands for VLAN and they are briefly described below:

1. To display the configured VLANs in a summarized form, use the following command. This displays VLAN mode, VLAN id, VLAN name, VLAN type and Protocol. This command also display dynamic VLANs learned when GVRP enabled.

```
L2SW> show vl an summary
```

```

L2SW >show vlan summary

VLAN Mode: ..... 802.1Q

VLAN ID  VLAN Name          VLAN Type  Protocol
-----
1         DEFAULT                 Static     none
10        Yellow                   Static     ip

Total: ..... 2
L2SW >

```

Figure 6-8 Display VLAN Summary

i *Dynamic VLAN display is not available on CML1 and WBI interface.*

2. To display detailed information for the selected VLAN, use the following command. This displays VLAN id, VLAN Name, VLAN Type, Protocol type, slot.port, current and configured details for physical port, and tagging details.

```

L2SW> show vl an detail ed <vl an id>
L2SW> show vl an detail ed 10

```

```

L2SW >show vlan detailed 10

VLAN ID: 10
VLAN Name: Yellow
VLAN Type: Static
Protocol Type: ip

Slot,Port  Member
-----
0.1        UnTagged
0.2        No
0.3        No
0.4        No
0.5        No
0.6        No
0.7        No
0.8        No
0.9        No
0.10       No
0.11       No
0.12       No
0.13       No
0.14       No
0.15       No
0.16       No
--More-- or (q)uit

```

Figure 6-9 Display VLAN details for selected VLAN

- The following command displays VLAN port. The table below shows slot, Port, PVID, Ingress Filter action details for -non-member and untagged packets. In this example, the switch is configure to drop non-member packets and forward untagged packets.

L2SW> show vl an port

Slot	Port	PVID	IngressFilter Non-Member Pkt	IngressFilter Untagged Pkt
0.1		1	Drop	Forward
0.2		1	Drop	Forward
0.3		1	Drop	Forward
0.4		1	Drop	Forward
0.5		1	Drop	Forward
0.6		1	Drop	Forward
0.7		1	Drop	Forward
0.8		1	Drop	Forward
0.9		1	Drop	Forward
0.10		1	Drop	Forward
0.11		1	Drop	Forward
0.12		1	Drop	Forward
0.13		1	Drop	Forward
0.14		1	Drop	Forward
0.15		1	Drop	Forward
0.16		1	Drop	Forward
0.17		1	Drop	Forward
0.18		1	Drop	Forward
0.19		1	Drop	Forward

Figure 6-10 Show vl an port

6.7.4 GVRP

GVRP (GARP VLAN Registration Protocol) allows automatic VLAN configuration between the switch and network nodes. If the switch is connected to a device with GVRP enabled, user can send a GVRP request using the VLAN ID of a VLAN defined on the switch, and the switch will automatically add that device to the existing VLAN. The following command is used to enable or disable GVRP.

```
L2SW> confi g gvrp admi nmode <enabl e/di sabl e>
L2SW> confi g gvrp admi nmode enabl e
```

 **For system performance reasons, it is recommended that the number of dynamically learnt GVRP entries be limited to 128.**

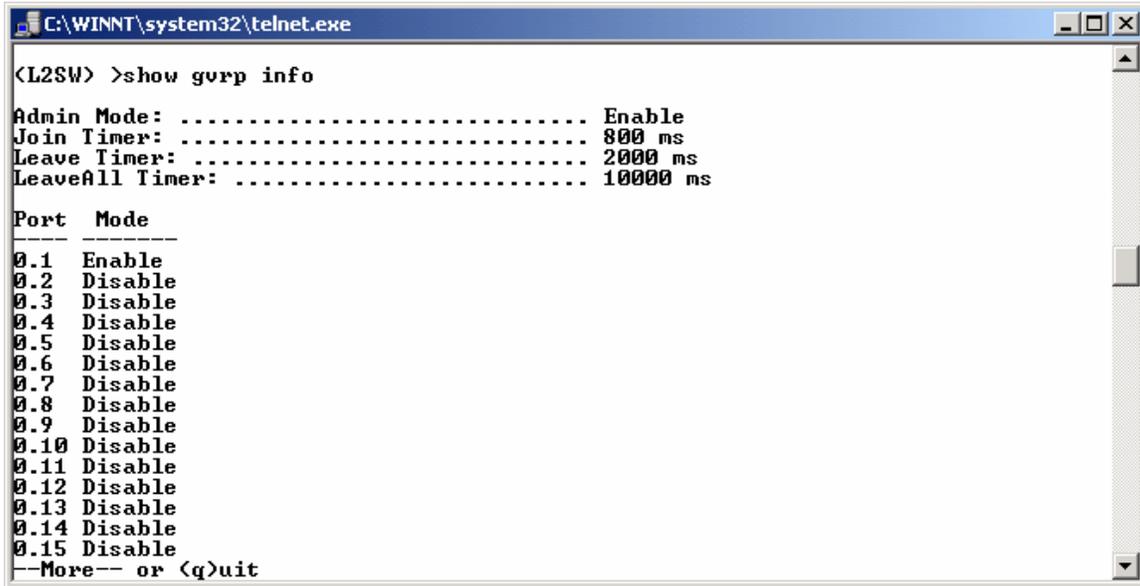
Apart from enabling GVRP at the switch level, the user must also enable GVRP on the relevant interface port. By default GVRP is disabled on all ports. To enable GVRP on a port, use the following

command:

```
L2SW> confi g gvrp Interfacemode <slot.port/all > <enable/disable>  
L2SW> confi g gvrp Interfacemode 0.1 enable
```

To display the GVRP configuration use following command:

```
L2SW> show gvrp info
```



The screenshot shows a telnet window titled 'C:\WINNT\system32\telnet.exe'. The user has entered the command '>show gvrp info'. The output displays the GVRP configuration for the switch. It shows the Admin Mode is 'Enable', the Join Timer is '8000 ms', the Leave Timer is '20000 ms', and the LeaveAll Timer is '100000 ms'. Below this, a table lists the GVRP mode for each port from 0.1 to 0.15. Port 0.1 is 'Enable', and all other ports (0.2 through 0.15) are 'Disable'. At the bottom of the output, it says '--More-- or <q>uit'.

```
<L2SW> >show gvrp info  
Admin Mode: ..... Enable  
Join Timer: ..... 8000 ms  
Leave Timer: ..... 20000 ms  
LeaveAll Timer: ..... 100000 ms  
  
Port  Mode  
-----  
0.1  Enable  
0.2  Disable  
0.3  Disable  
0.4  Disable  
0.5  Disable  
0.6  Disable  
0.7  Disable  
0.8  Disable  
0.9  Disable  
0.10 Disable  
0.11 Disable  
0.12 Disable  
0.13 Disable  
0.14 Disable  
0.15 Disable  
--More-- or <q>uit
```

Figure 6-11: GVRP Information Display

6.8 Spanning Tree Protocol

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. STP is a bridge-based mechanism for providing fault tolerance on networks by determining alternate paths for bridged traffic when a failure is encountered. STP enables user to implement parallel paths for network traffic and ensure the following:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main traffic paths fail.

Rapid Spanning Tree Protocol (RSTP), specified by IEEE802.1w, is an improved version of Spanning Tree Protocol and specifically addresses the problem associated with convergence time in STP. With RSTP, convergence typically occur within a couple of seconds whenever a topology change occurs in the network. Multiple Spanning Tree Protocol (MSTP) allows an user to configure and support multiple spanning tree instances within the same switch. For more details about RSTP and MSTP refer to [Section 4.3.10](#).

6.8.1 STP Configuration

STP can be enabled, by configuring the System and Per Port Configuration as displayed in the following commands.

- To enable or disable administrative mode for switch use following command:

```
L2SW> confi g spanni ngtree swi tch admi nmode <enabl e/di sabl e>
L2SW> confi g spanni ngtree swi tch admi nmode enabl e
```

- Since L2SW supports, multiple spanning tree protocols, the user has to specify the spanning tree protocol type. For example, to specify the IEEE802.1D as the spanning protocol for the switch, use the following command.

```
L2SW> confi g spanni ngtree swi tch forceversi on <802. 1d/802. 1w/802. 1s>
L2SW> confi g spanni ngtree swi tch forceversi on 802. 1d
```



The default spanning tree protocol version is 802.1s

- To configure STP hello time for switch. The valid range is from 1 to 10 seconds. The default value is 2 seconds.

```
L2SW> confi g spanni ngtree swi tch hel lotime <i nterval >
L2SW> confi g spanni ngtree swi tch hel lotime 3
```

- To configure the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it re-computes the spanning tree topology. The range for bridges maximum age is 6 to 40 seconds. The default value is 20 seconds.

```
L2SW> confi g spanni ngtree swi tch maxage <i nterval >
L2SW> confi g spanni ngtree swi tch maxage 10
```

- To configure the forwarding delay of the switch, use the following command. The allowed range of the forwarding delay is 4 to 30 seconds and the default value is 15 seconds.

```
L2SW> confi g spanni ngtree swi tch forwarddel ay <i nterval >
L2SW> confi g spanni ngtree swi tch forwarddel ay 10
```

- To configure the STP bridge priority, use following command. The allowed range for the STP priority is 1 to 65535 and the default value is 32768. Higher numerical value means a lower priority.

```
L2SW> confi g spanni ngtree swi tch pri ori ty <pri ori ty>
L2SW> confi g spanni ngtree swi tch pri ori ty 10
```

- To display STP settings in summary or detailed form, use the following command. In detailed form, information such as the number of topology change count, Root Path Cost and Root Port Identifier are displayed.

```
L2SW> show spanni ngtree swi tch <summary/detai led>
L2SW> show spanni ngtree swi tch summary
```

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree switch summary
Spanning Tree Adminmode ..... Enable
Protocol Version ..... IEEE 802.1D
Bridge Priority ..... 32768
Bridge Identifier ..... 80:00:00:50:A8:80:08:61
Bridge Max Age ..... 20
Bridge Hello Time ..... 2
Bridge Forward Delay ..... 15
Bridge Hold Time ..... 3
<L2SW> >

```

Figure 6-12 Displays switch STP settings in summary form

L2SW> show spanningtree switch detailed

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree switch detailed
Bridge Priority ..... 32768
Bridge Identifier ..... 80:00:00:50:A8:80:08:61
Time Since Last Topology Change ..... 6
Topology Change Count ..... 0
Topology Change ..... False
Designated Root ..... 80:00:00:30:1E:18:1F:98
Root Path Cost ..... 200010
Root Port Identifier ..... 8001
Max Age ..... 20
Forward Delay ..... 15
Bridge Max Age ..... 20
Bridge Hello Time ..... 2
Bridge Forward Delay ..... 15
Bridge Hold Time ..... 3
<L2SW> >_

```

Figure 6-13: Display Switch Settings in Detailed Form

- To display STP settings and STP statistics associated with a port, use the following command.

L2SW> show spanningtree port <summary/detailed> <slot.port>
L2SW> show spanningtree port summary 0.1

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree port summary 0.1
Port ..... 0.1
STP Port Mode ..... Enable
STP BPDUs Received ..... 0
STP BPDUs Transmitted ..... 0
RST BPDUs Received ..... 0
RST BPDUs Transmitted ..... 44
TCN BPDUs Received ..... 0
TCN BPDUs Transmitted ..... 0
MST BPDUs Received ..... 0
MST BPDUs Transmitted ..... 0
Port Up Time ..... 87
<L2SW> >

```

Figure 6-14 Displays port STP settings in summary form

L2SW> show spanningtree port detailed 0.1

Figure 6-15 displays STP port settings in detailed form.

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree port detailed 0.1
Port ..... 0.1
STP Port Mode ..... Enable
Port State ..... Discarding
Port Identifier ..... 8001
Port Path Cost (admin) ..... Auto
Port Path Cost (oper) ..... 200000
Designated Root ..... 80:00:00:30:1E:18:1F:98
Designated Port Cost ..... 10
Designated Bridge ..... 80:00:00:80:3E:98:8D:E4
Designated Port ..... 8004
Topology Change Acknowledgement ..... False
Hello Time ..... 2
<L2SW> >

```

Figure 6-15: Display STP Port Settings in Detailed Form

6.8.2 RSTP Configuration

RSTP protocol can be enabled by setting the forcedversion parameter to 802.1w as illustrated below.

- Set forcedversion to RSTP
L2SW> confi g spanni ngtree swi tch forceversi on <802. 1d/802. 1w/802. 1s>
L2SW> confi g spanni ngtree swi tch forceversi on 802. 1w

i While switching spanning tree protocol from one version to another (e.g., STP to RSTP or RSTP to STP or STP to MSTP, etc.), it is recommended that the STP adminmode is disabled and then reenabled. Users can disable or enable STP adminmode by clicking on the box next to STP State.

RSTP protocol parameter configuration such as switch priority, forwarddelay, etc. are exactly same as STP protocol paramter except that with RSTP, users configure a port to be an Edge port and set the link-type to be Point-to-point, shared or Auto. The following commands illustrate how to configure the Edge port and link type associated with a port.

- To configure a port to be an Edge port, use the following command:
L2SW> confi g spanni ngtree port edgeport <slot.port/all> <true/false>
L2SW> confi g spanni ngtree port edgeport 0. 1 true
- To configure link type associated with a port, use the following command:
L2SW> confi g spanni ngtree port linktype <slot.port/all> <point-to-point/shared/auto>
L2SW> confi g spanni ngtree port linktype 0. 1 point-to-point
- To display the Edge port configuration and link type, use the following command. The display response from the switch is illustrated in
L2SW> show spanni ngtree port detail ed <slot.port>
L2SW> show spanni ngtree port detail ed 0. 1

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree port detailed 0.1
Port ..... 0.1
STP Port Mode ..... Enable
Port State ..... Forwarding
Port Identifier ..... 8001
Port Path Cost (admin) ..... Auto
Port Path Cost (oper) ..... 200000
Designated Root ..... 80:00:00:30:1E:18:1F:98
Designated Port Cost ..... 10
Designated Bridge ..... 80:00:00:80:3E:98:8D:E4
Designated Port ..... 8004
Topology Change Acknowledgement ..... False
Hello Time ..... 2
Edge Port (admin) ..... True
Edge Port (oper) ..... False
Port Link Type (admin) ..... Auto
Port Link Type (oper) ..... Point-to-point
Priority ..... 128
<L2SW> >

```

Figure 6-16: RSTP Port Configuration Status Display

6.8.3 MSTP Configuration

To enable MSTP for the switch, set the spanningtree protocol forcedversion parameter to 802.1s as illustrated by the following command.

- Set forcedversion to MSTP
L2SW> confi g spannigtree swi tch forceversi on <802.1d/802.1w/802.1s>
L2SW> confi g spannigtree swi tch forceversi on 802.1s

L2SW allows users to configure the following items associated with MSTP:

- MSTP Configuration Name
- MSTP Configuration Version
- MST Instance Creation/Deletion
- Add/Delete VLANs to an MST Instance
- Set Switch Priority on a per MST Instance basis

 **L2SW supports 8 user defined MST Instances. Instance 0 is reserved for use as IST.**

- MST Configuration Name consists of an ASCII string of upto 32 characters. MST Configuration Name must be unique among all switches in a MST Region. To configure MST Configuration name, use the following command.

```

L2SW> confi g spannigtree swi tch confi gurati on name <name_string>
L2SW> confi g spannigtree swi tch confi gurati on name REGION-1

```

- Configure MST Configuration Revision number. A number in the range 0-65535 can be used as Revision number. To configure MST Configuration Revision number, use the following command:

```

L2SW> confi g spannigtree swi tch confi gurati on revi si on <0-65535>
L2SW> confi g spannigtree swi tch confi gurati on revi si on 1

```

- To configure a MST Instance, use the following command. Instance IDs in the range 1-8 are valid.

```
L2SW> confi g spann ingtree mst create <msti d>
L2SW> confi g spann ingtree mst create 1
```

- To delete an MST Instance use the following command. Instance IDs in the range 1-8 are valid. When an MST Instance is deleted all the VLANs associated with that Instance are reassigned to MST Instance 0 (Internal Spanning Tree).

```
L2SW> confi g spann ingtree mst delete <msti d>
L2SW> confi g spann ingtree mst delete 1
```

- A range of VLANs can be specified by the following command using **vl ani d-l ow** and **vl ani d-hi gh** value. The vlanid-low corresponds to starting VLAN id in the VLAN-id range and vlanid-high corresponds to the ending VLAN-id in the VLAN-id range. If the vlanid-high value is not specified, it is assumed that the command is being used to assign a single VLAN to the MST instance.

```
L2SW> confi g spann ingtree mst vl an add <msti d> <vl ani d-l ow> [<vl ani d-
hi gh>]
L2SW> confi g spann ingtree mst vl an add 1 11 19
```

- To remove a range VLANs from a MST Instance, use the following command. VLANs removed from a MST instance are reassigned to MST Instance 0.

```
L2SW> confi g spann ingtree mst vl an remove <msti d> <vl ani d-l ow>
[<vl ani d-hi gh>]
L2SW> confi g spann ingtree mst vl an remove 1 13 15
```

- To assign switch priority for a MST Instance, use the following command.

```
L2SW> confi g spann ingtree mst pri ori ty <msti d> <0-61440>
L2SW> confi g spann ingtree mst pri ori ty 1 10
```



L2SW supports priority assignment on a per MST Instance basis. Port level priority assignment on a MST Instance basis is not currently supported.

- To display MST switch configuration and statistics in summary or detailed form, use the following commands. The responses from the switch are displayed in Figure 6-17 and Figure 6-18. The configuration digest value is an MD-5 encoded message digest derived from Configuration Name, Revision Level and VLAN to MST Instance mapping table.

```
L2SW> show spann ingtree swi tch <summary/detai led>
L2SW> show spann ingtree swi tch summary
```

```

C:\WINNT\system32\telnet.exe
(L2SW) >
(L2SW) >show spanningtree switch summary

Spanning Tree Adminmode ..... Disable
Protocol Version ..... IEEE 802.1s
Configuration Name ..... REGION-1
Configuration Revision Level ..... 1
Configuration Digest ..... D14092B42A822EAED56BD46ECF3AF22F
Configuration Format Selector ..... 0
Bridge Priority ..... 32768
Bridge Identifier ..... 80:00:00:50:A8:80:08:60
Bridge Max Age ..... 20
Bridge Hello Time ..... 2
Bridge Forward Delay ..... 15
Bridge Hold Time ..... 3
MST Instances ..... 1
Instance 0 (CIST) VLAN IDs ..... 1, 13-15
Instance 1 VLAN IDs ..... 11-12, 16-19

(L2SW) >

```

Figure 6-17: MST Switch Configuration display in Summary format

```

C:\WINNT\system32\telnet.exe
(L2SW) >show spanningtree switch detailed

Bridge Priority ..... 32768
Bridge Identifier ..... 80:00:00:50:A8:80:08:60
Time Since Last Topology Change ..... 0
Topology Change Count ..... 0
Topology Change ..... False
Designated Root ..... 00:00:00:00:00:00:00:00
Root Path Cost ..... 0
Root Port Identifier ..... 0000
Max Age ..... 0
Forward Delay ..... 0
Bridge Max Age ..... 20
Bridge Hello Time ..... 2
Bridge Forward Delay ..... 15
Bridge Hold Time ..... 3
CIST Regional Root ..... 00:00:00:00:00:00:00:00
CIST Path Cost ..... 0
CIST VLAN IDs ..... 1, 13-15

(L2SW) >

```

Figure 6-18: MST Switch Configuration display in Detailed format

- To view information related to a MST instance such as Bridge Priority, Designated Root for that Instance, Root Path Cost and VLANs associated with that MST instance, use the following command. Figure 6-19 displays the information related to MST Instance.

```

L2SW> show spanningtree mst detailed <1-8>
L2SW> show spanningtree mst detailed 1

```

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree mst detailed 1
MST Instance ID ..... 1
MST Bridge Priority ..... 32768
Time Since Last Topology Change ..... 8144
Topology Change Count ..... 0
Topology Change ..... False
Designated Root ..... 80:01:00:50:A8:80:08:61
Root Path Cost ..... 0
Root Port Identifier ..... 0000
ULAN IDs ..... 11-12, 16-19
<L2SW> >_

```

Figure 6-19: MST Instance Details

- To view port specific information related to a port associated with a MST instance, use the following command. Figure 6-20 displays the port information for the port 0.24 associated with MST instance 1.

```

L2SW> show spanningtree mst port detailed <1-8> <slot.port>
L2SW> show spanningtree mst port detailed 1 0.24

```

```

C:\WINNT\system32\telnet.exe
<L2SW> >show spanningtree mst port detailed 1 0.24
MST Instance ID ..... 1
Port ..... 0.24
Port State ..... Forwarding
Port Identifier ..... 8018
Port Path Cost ..... 200000
Designated Root ..... 80:01:00:50:A8:80:08:61
Designated Port Cost ..... 0
Designated Bridge ..... 80:01:00:50:A8:80:08:61
Designated Port ..... 8018
<L2SW> >

```

Figure 6-20: Spanning Tree Port Information Display

6.9 Link Aggregation & Trunking Settings

L2SW can create a maximum of seven trunk groups. User can arbitrarily select up to four ports from ports 1 to 26 to build a trunking group. All ports in the same static trunk group must be configured to operate at the same speed and will be treated as a single port. The following set of commands can be used to configure and display trunking mode.

- To create trunk group with two ports:


```

ESS_F10> config trunk <trunkid> <static/lacp> <port-list>
L2SW> config trunk 2.1 static 0.2 0.3

```

 - Trunkid – Trunking group ID, The trunk group id values will be from 2.1 to 2.7
 - Static – static trunk.
 - LACP – the trunk group has LACP.



Note that all members of a trunk port should be configured to operate at the same speed.

- To remove the configured trunk, use the following command.

```
L2SW> confi g trunk delete <trunkid>
L2SW> confi g trunk delete 2.1
```

- Add ports to the existing trunk group:

```
L2SW> confi g trunk addport <trunkid> <port-list>
L2SW> confi g trunk addport 2.1 0.4
```

- To delete one or more ports from trunk group

```
L2SW> confi g trunk del port <trunkid> <port-list>
L2SW> confi g trunk del port 2.1 0.2
```

System priority specifies the link aggregation priority relative to the devices at the other end of the links on which link aggregation is enabled. A higher value indicates a lower priority. The range is from 0 - 65535. The default is 1. To configure link aggregation priority use the following command.

```
L2SW> confi g trunk systempriority <priority_num>
L2SW> confi g trunk systempriority 20
```

- To change the mode of configured trunk use the following command:

```
L2SW> confi g trunk mode <trunkid> <lacp/static>
L2SW> confi g trunk mode 2.1 lacp
```

- To displays trunk summary use following command: for specified trunk group. The group id is the id for static or LACP group. The below table 7.11 shows the system priority set to 20, trunk group 2.1 is static and 2.2 is LACP mode. Port 0.2 and 0.3 are members of trunk group 2.1, while 0.4 and 0.5 are in trunk group 2.2.

```
L2SW> show trunk summary
```

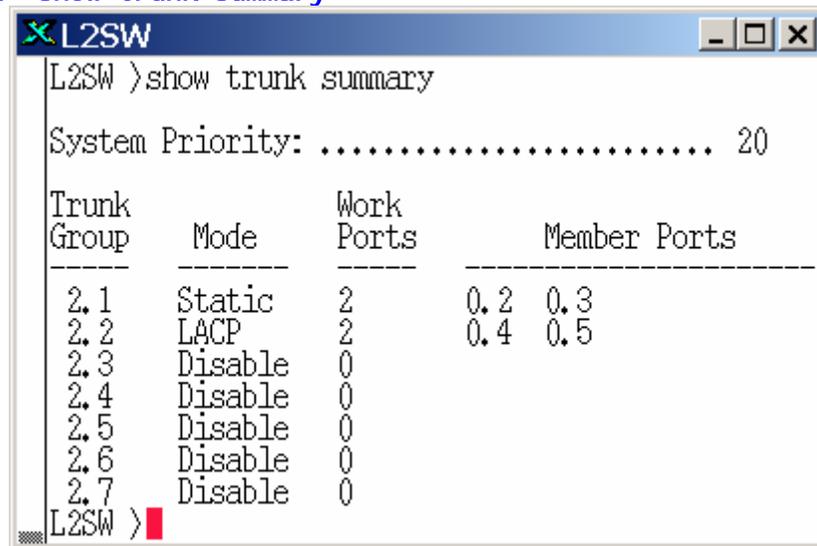
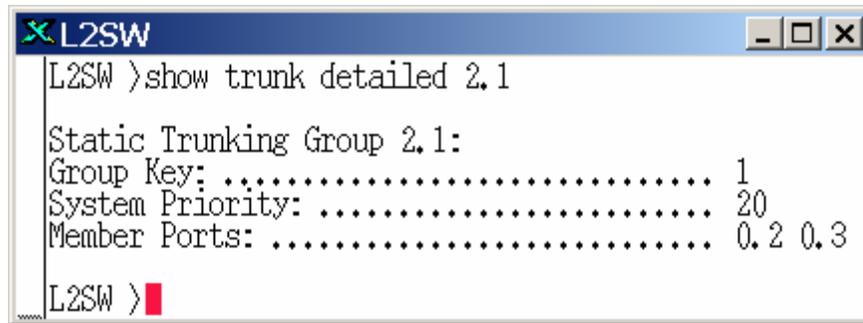


Figure 6-21 Display trunk summary

- To display trunk details use following command. This displays static trunk group, Group Key, System Priority, and Member Ports.

```
L2SW> show trunk detailed <trunkid>
L2SW> show trunk detailed 2.1
```



```

L2SW >show trunk detailed 2.1

Static Trunking Group 2.1:
Group Key: ..... 1
System Priority: ..... 20
Member Ports: ..... 0.2 0.3

L2SW >

```

Figure 6-22 Displays selected trunk details

6.10 Port Mirroring

The port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That is traffic goes in or out through the monitored ports will be duplicated into monitoring port. To configure port-mirroring feature use the following set of commands.

- Configure port-mirroring mode using following commands

```
L2SW> confi g mi rrori ng mode <none/rx/tx/both>
```

```
L2SW> confi g mi rrori ng mode both
```

None – To disable port mirroring.

RX – To monitor ingress traffic on mirrored ports.

TX – To monitor egress traffic on mirrored ports.

Both – To monitor traffic on mirrored ports in both directions.
- Configure the port used as Sniffer port and see all monitored port traffic. It is the port connected to Sniffer

```
L2SW> confi g mi rrori ng sni ffer <sl ot. port>
```

```
L2SW> confi g mi rrori ng sni ffer 0. 1
```
- To configure the port to be monitored. All monitored port traffic will be copied to sniffer port. Maximum of 25 monitored ports can be selected in the switch. To add or remove monitored port use following set of commands.

```
L2SW> confi g mi rrori ng moni tored add <sl ot. port>
```

```
L2SW> confi g mi rrori ng moni tored add 0. 2
```

```
L2SW> confi g mi rrori ng moni tored del ete <sl ot. port>
```

```
L2SW> confi g mi rrori ng moni tored del ete 0. 2
```
- To display port mirroring information use following command. The table below shows Sniffer mode is both (RX and TX) and Sniffer port is 2, while monitored ports are 3,4,5,6 and 7.

```
L2SW> show mi rrori ng
```

```

L2SW >show mirroring
Sniffer Mode: ..... Both
Sniffer Port: ..... 0.2
Monitored Ports:
0.3 0.4 0.5 0.6 0.7
L2SW >

```

Figure 6-23 Show port mirroring

6.11 Broadcast Storm Filtering

To control the broadcast storm, the threshold value should be defined. The threshold value is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold, broadcast storm control becomes active. The valid threshold value are 5, 10, 15, 20, 25 and 0. Value of 0 means storm control is disabled. Following commands are used to configure & display the broadcast storm filter.

```

L2SW> config stormcontrol level <threshold>
L2SW> config stormcontrol level 15

```

To display storm control filter information:

```

L2SW> show stormcontrol

```

```

L2SW >show stormcontrol
Broadcast Storm threshold: 15%.
L2SW >

```

Figure 6-24 Displays broadcast storm settings

6.12 IGMP Snooping

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. Multicast traffic is propagated through the network using switches, routers, and hosts that support IGMP and other multicast protocols. Enabling IGMP snooping allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. The following set of commands can be used to configure IGMP snooping.

1. To enable or disable administrative mode of IGMP snooping, use the following command. By default, the administrative mode of IGMP snooping is disable.

```

L2SW> config igmpsnooping admimode <enable/disable>
L2SW> config igmpsnooping admimode enable

```

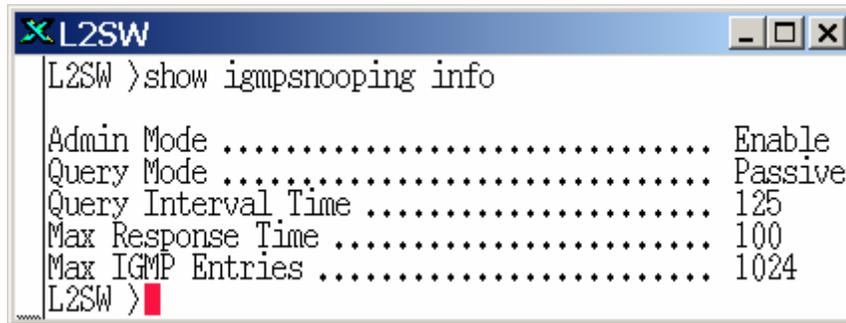
2. The IGMP snooping query mode can be active, passive or auto. The active query mode is to enable query mode for group members. The passive query mode is for passive snooping on IGMP Query/Report. In auto mode, switch performs Query function if there is no other device in the

VLAN, such as a multicast router is available to perform Query requests. The default value is auto.

```
L2SW> confi g igmpsnoopi ng querymode <acti ve/passi ve/auto>  
L2SW> confi g igmpsnoopi ng querymode passi ve
```

2. To display IGMP snooping configuration, use the following command. The table below shows IGMP snooping parameters such as IGMP snooping mode query mode, query interval time, max response time and max. IGMP entries.

```
L2SW> show i gmpsnoopi ng i nfo
```



The screenshot shows a terminal window titled 'L2SW' with the following output:

```
L2SW >show igmpsnooping info  
Admin Mode ..... Enable  
Query Mode ..... Passive  
Query Interval Time ..... 125  
Max Response Time ..... 100  
Max IGMP Entries ..... 1024  
L2SW >
```

Figure 6-25 Displays IGMP snooping settings

6.13 802.1X

802.1x makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and to prevent access to that port in case the authentication and authorization process fails.

The following are the list of terms used within 802.1x.

Authenti cation Server: The server that performs the authentication, allowing or denying access to the network based on username/password. The 802.1x uses the Remote Authentication Dial-In User Service (RADIUS) supported server.

Client: 802.1x supported client is the network access device requesting LAN services.

Authenti cator: This is the network access point that has 802.1x authentication enabled. This includes LAN switch port of L2SW.

Before configuring 802.1x feature, it has to be enabled in Switch Settings:

1. To configure L2SW for 802.1x to communicate with RADIUS server, use the following command.

```
L2SW> confi g radi us addr <serveri p>  
L2SW> confi g radi us addr 10.0.0.2
```

2. To configure shared secret, password between L2SW and the RADIUS server, use the following command. It is used to authenticate all transactions between the two devices. It is a character string, 1 to 128 characters in length; it may contain any alphanumeric character. Use the following command for configuration:

```
L2SW> confi g radi us <shared secret>
L2SW> confi g radi us secret secret-word
```

3. To configure UDP port for a Radius server, use the following command. The possible value is 1812 or 1645, 1645 is used for early deployment of Radius. Default value is 1812.

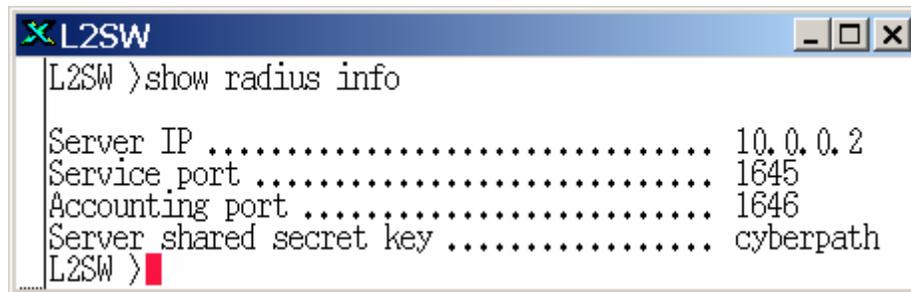
```
L2SW> confi g radi us servi ceport <portno>
L2SW> confi g radi us servi ceport 1645
```

4. To configure Radius server UDP accounting port, use the following command. The possible value is 1813 or 1646. 1646 is used for early deployment of Radius accounting server. The default value is 1813.

```
L2SW> confi g radi us acctport <portno>
L2SW> confi g radi us acctport 1646
```

5. To display Radius settings, use the following command

```
L2SW> show radi us i nfo
```



```
L2SW >show radius info
Server IP ..... 10.0.0.2
Service port ..... 1645
Accounting port ..... 1646
Server shared secret key ..... cyberpath
L2SW >
```

Figure 6-26 Displays Radius settings

6. To configure L2SW switch port/s for 802.1x client, use the following command:
 - a) To Enable/Disable the administrative mode for the 802.1x on switch, use the following command. By default, 802.1x administrative mode is disabled.

```
L2SW> confi g dot1x swi tch admi nmode <enabl e/di sabl e>
L2SW> confi g dot1x swi tch admi nmode enabl e
```

- b) Four types of port control are:

- **ForceAuthori zed (Fa):** Disable 802.1x and put the port to authorized state without any authentication exchange required. This is the default port control setting.
- **ForceUnauthori zed (Fu):** causes the port to unconditionally remain in the unauthorized state, ignoring all attempts by client to authenticate.
- **Auto:** Enable 802.1x and causes the port to being in unauthorized state.
- **None:** Disables 802.1x on a port

To configure port control, use the following command:

```
L2SW> confi g dot1x swi tch portcontrol <sl ot.port/all > <fa/fu/auto/none>
L2SW > confi g dot1x swi tch portcontrol 0.2 auto
```

7. To display 802.1x configuration settings on switch, execute the following command.

```
L2SW> show dot1x swi tch
```

```

L2SW >show dot1x switch

Switch administration mode ..... Enable
EAP re-transmission interval ..... 30 Seconds
Re-authentication interval ..... 3600 Seconds
Quiet period ..... 60 Seconds
Maximum re-authentication attempts ..... 2
Supplicant timeout interval ..... 30 Seconds
Server timeout interval ..... 30 Seconds
L2SW >

```

Figure 6-27 Displays dot1x switch settings

8. To display dot1x settings for switch port, use the following command:

```

L2SW> show dot1x port <slot.port/all>
L2SW> show dot1x port all

```

```

L2SW >show dot1x port all

Port   Port Control
-----
0. 1   None
0. 2   Auto
0. 3   ForceAuthorized
0. 4   None
0. 5   None
0. 6   None
0. 7   None
0. 8   None
0. 9   None
0. 10  None
0. 11  None
0. 12  None
0. 13  None
0. 14  None
0. 15  None
Would you like to display the next 15 entries? (y/n)

```

Figure 6-28 Displays dot1x port control

6.14 Priority

The dot1p queue priority is queuing which allows switch to organize buffered packets, and then service one class of traffic differently from other classes of traffic. For example, you can set priorities so that real-time applications, such as interactive voice and video, get priority over applications that do not operate in real time. There are three different modes of priority and they are

- **FCFS:** First Come First Served

- **SP:** Strict Priority
- **WRR:** Weighed round robin

1. To configure priority mode and user level priority, use the following set of commands:

```
L2SW> confi g dot1p mode <fcfs/sp/wrr>
L2SW> confi g dot1p mode sp
```

2. To create a user priority to queue priority mapping, use the following command. The dot1p_priority variable is user priority. This is a decimal number between 0 and 7. While queue priority variable is for out put queue. This is a decimal number between 0 and 1 where 0 is for low priority and 1 is the high priority queue.

```
L2SW> confi g dot1p map <dot1p_pri ori ty(0-7)> <queue_pri ori ty(0-1)>
L2SW> confi g dot1p map 3 1
```

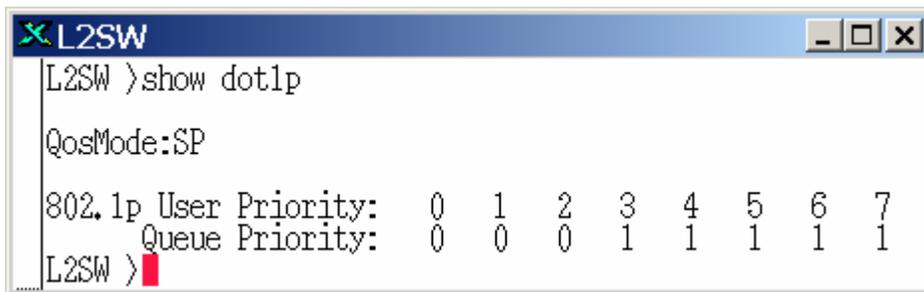
3. To configure 802.1p Weighted Round Robin (WRR) for out put queue, use the following command. The output queue priority value is a decimal number between 0 and 1. Value of 0 is low and 1 is high priority queue. While the WRR weight has valid range from 0 to 7. The default value is 1.

```
L2SW> confi g dot1p wrr <queue_pri ori ty(0-1)> <wei ght(1-7)>
L2SW> confi g dot1p wrr 1 3
```

 **Only 802.1p WRR mode weights can be modified.**

4. To display 802.1p mode and user priority to queue priority mappings, use following command.

```
L2SW> show dot1p
```



```
L2SW >show dot1p
QosMode:SP
802.1p User Priority:  0  1  2  3  4  5  6  7
Queue Priority:      0  0  0  1  1  1  1  1
L2SW >
```

Figure 6-29 Displays 802.1p priority settings

6.15 Switch Settings

There are few more parameters that users can configure to control the transmission delay, queuing delay and Inter Frame Gap.

Transmit Delay limits the packets queuing time in switch. If enabled, the packets queued exceeding the queuing delay will be dropped. Valid range for maximum transmit delay is from 0 to 4, with the default value set to 0. The transmit delay mode is disabled when set to 0. To configure Maximum Bridge transmit delay bound, use the following command.

```
L2SW> confi g swi tchconfi g transmi tdel ay <del ay(0/1/2/3/4)>
```

L2SW> config switchconfig transmitdelay 2

The **Low Queue Delay** limits the low priority packets queuing time in switch. If the low priority packet stays in switch and exceeds the configured maximum delay time, it will be dropped. Valid range for **Low Queue Delay** is from 0 to 255ms with the default value set to 0. The **Low Queue Delay** mode is disabled when set to 0.

L2SW> config switchconfig lowqueuedelay <delay(0-255)>
L2SW> config switchconfig lowqueuedelay 25

Collision Retry defines the number of times the packet has to be retransmitted to recover from collisions. To enable or disable configure collision retry forever mode. By default, collision retry forever administrative mode is disabled.

L2SW> config switchconfig collisionretry adminmode <enable/disable>
L2SW> config switchconfig collisionretry adminmode enable

IFG Compensation is used to compensate for the minor differences in clock speeds on two different FE ports. Since IEEE standards allow 100ppm variance in clock speed, it is quite possible that the transmit clock speed on one port may be slightly less than the receive clock speed on another port. If the traffic between these two ports below wire speed, the difference in clock speeds don't matter that much. If the traffic between these two ports run at wire speed for a sustained period of time then frames will be lost. To prevent the loss of frames due to difference in clock speed, the Inter-frame Gap on the transmit side can be reduced from a normally allowed 7 bytes to 5 or 6 bytes. To enable or disable IFG compensation mode, use the following command. By default, IFG compensation mode is disabled.

L2SW> config switchconfig ifgcomp adminmode <enable/disable>
L2SW> config switchconfig ifgcomp adminmode enable

L2SW maintains the number of internal tables such as MAC address table, VLAN tag table and Multicast table to support switching. The total number of entries in all these tables are limited to a maximum of 14K entries. For optimal performance and based on number of input from customers, the tables are configured to support the following default configuration.

- **MAC address Table** – 8192 entries
- **VLAN Tag Table** – 2048 entries
- **Multicast Table** – 1280 entries
- **Protocol VLAN Table** – 2048 entries

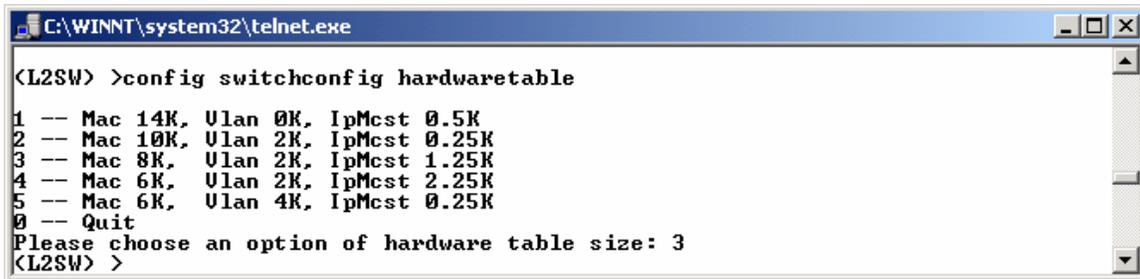
However, L2SW allows user to resize these table entries by choosing one of the following alternate configurations:

	MAC Table Size	VLAN Tag Table Size	Multicast Table Size
1	14K	0	0
2	10K	2K	0.25K
3	8K	2K	1.25K
4	6K	2K	2.25K
5	6K	4K	0.25K

To change the internal table configuration stored inside L2SW, use the following command. The

L2SW will respond to the command by displaying the hardware configurations available in a menu format as illustrated in Figure 6-30.

```
L2SW> confi g swi tchconfi g hardwaretable  
L2SW> confi g swi tchconfi g hardwaretable
```



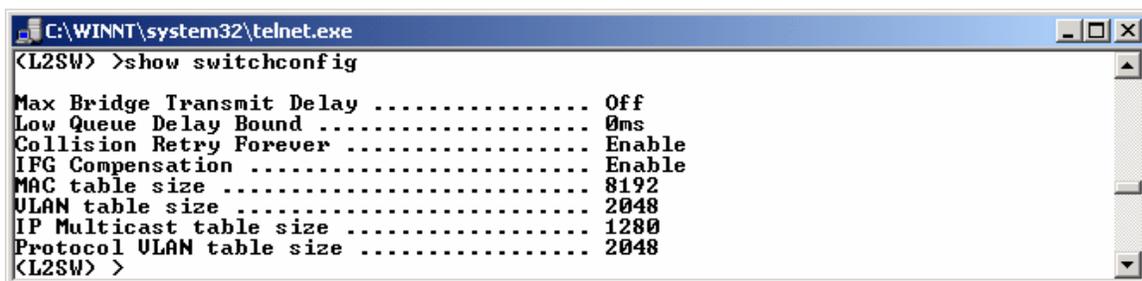
```
C:\WINNT\system32\telnet.exe  
<L2SW> >config switchconfig hardwaretable  
1 -- Mac 14K, Ulan 0K, IpMcst 0.5K  
2 -- Mac 10K, Ulan 2K, IpMcst 0.25K  
3 -- Mac 8K, Ulan 2K, IpMcst 1.25K  
4 -- Mac 6K, Ulan 2K, IpMcst 2.25K  
5 -- Mac 6K, Ulan 4K, IpMcst 0.25K  
0 -- Quit  
Please choose an option of hardware table size: 3  
<L2SW> >
```

Figure 6-30: Hardware Table Size Configuration Command

 *In order to make hardware table configuration changes to be effective, you need to save the configuration change and reboot the switch.*

To display switch settings including the hardware table sizes, use the following command:

```
L2SW> show swi tchconfi g
```



```
C:\WINNT\system32\telnet.exe  
<L2SW> >show switchconfig  
Max Bridge Transmit Delay ..... Off  
Low Queue Delay Bound ..... 0ms  
Collision Retry Forever ..... Enable  
IFG Compensation ..... Enable  
MAC table size ..... 8192  
ULAN table size ..... 2048  
IP Multicast table size ..... 1280  
Protocol ULAN table size ..... 2048  
<L2SW> >
```

Figure 6-31 Displays Switch settings

6.16 Statistics

To display statistics for a specific port, use the following command. This displays statistics such as packets transmitted and received with and without errors, transmit abort, collision and drop packets.

```
L2SW> show statisti c port <slot.port>  
L2SW> show statisti c port 0.1
```

```

L2SW >show statistics port 0.1
Tx Good Packets ..... 236
Tx Error Packets ..... 0
Rx Good Packets ..... 16149
Rx Error Packets ..... 0
Tx Abort ..... 0
Collision ..... 0
Dropped Packets ..... 9137
L2SW >

```

Figure 6-32 Displays port statistics

To reset the port counter statistic on any one port or all the ports use following command:

```

L2SW> clear statistics port <slot.port/all >
L2SW> clear statistics port all

```

6.17 Management Commands

6.17.1 User Login Accounts

L2SW only supports one user account for administration. The user name is “admin” and password is “ess” by default. Username is up to eight alphanumeric characters. The username is not case-sensitive. Password is up to eight alphanumeric characters. The password is not case-sensitive.

```

L2SW> config user passwd <name> <password>
L2SW> config user passwd admin manager

```

6.17.2 Switch Inventory

To display L2SW switch inventory information, use the following command. This displays information such as Machine Type, Serial Number, Base MAC Address, ASIC Version, Software Version and the gigabit optional modules type, as shown in the table below:

```
L2SW> show inventory
```

```

L2SW >show inventory
Machine Type ..... ESS Switch
Serial Number ..... FA830011
Base MAC Address ..... 00:50:A8:80:01:40
ASIC Version ..... VIA6526 700
Software Version ..... 2.00.01.P1
Module Card 1 Type ..... NC
Module Card 1 Information .....
Module Card 2 Type ..... NC
Module Card 2 Information .....
L2SW >

```

Figure 6-33 Display inventory

6.17.3 Network IP Address Configuration

To configure IP address, subnet mask, gateway IP and protocol on the switch, use the following set of commands. The default IP address is 192.168.0.1. A switch can have only one IP address. The switch can be configured for protocol none or DHCP. If the switch is set for protocol none then all the IP information is manually configured. DHCP is disabled by default. If the user removes the IP address through a telnet session, the connection to the switch is lost.

```
L2SW> config network protocol <none/dhcp>
L2SW> config network protocol none

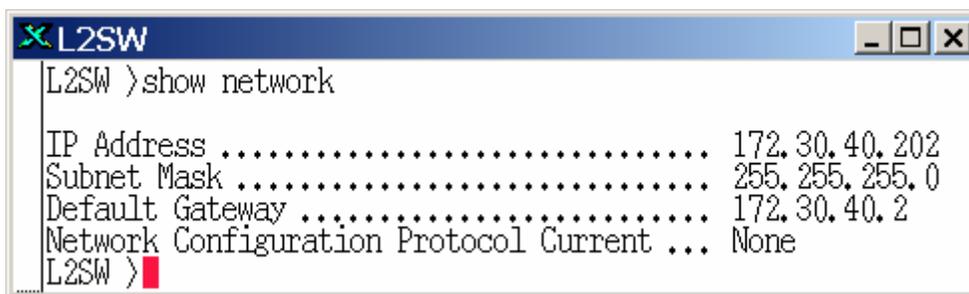
L2SW> config network params <i paddr> <netmask> [gateway]
L2SW> config network params 172. 30. 40. 202 255. 255. 255. 0 172. 30. 40. 2

L2SW> save config
L2SW> reset system
Are you sure you would like to reset the system (y/n) Y
```

i In order for the statically configured IP address to take effect, the switch has to be restarted using “reset system” command.

To display network configuration settings, use the following command. The response to this command displays IP address, subnet mask and default gateway assigned to the switch for management. It also displays the switch MAC address and IP address configuration mode (DHCP or none).

```
L2SW> show network
```



```
L2SW >show network
IP Address ..... 172.30.40.202
Subnet Mask ..... 255.255.255.0
Default Gateway ..... 172.30.40.2
Network Configuration Protocol Current ... None
L2SW >
```

Figure 6-34 Displays network settings

6.18 SNMP

SNMP is a protocol that governs the transfer of management information between element/network manager and an agent. Any Network Management system (an SNMP manager) running the simple Network Management Protocol (SNMP) can manage the switch (an SNMP agent), provided the Management Information Base (MIB) is installed correctly on the network management station. The L2SW supports SNMP V1, V2C and V3. The SNMP Management station (an SNMP manager) can use SNMPv1, SNMPv2 or SNMPv3 protocol to retrieve information from the switch. For brief description on SNMPv1/v2c/v3, refer to [Section 4.3.12](#).

6.18.1 SNMP System Setup

User can define a system name, location, and contact person for the switch using following commands.

- **Name** Name to be used for the switch.
L2SW> `config snmp sysname <name>`
L2SW> `config snmp sysname L2SW`
- **Location** Location of the switch.
L2SW> `config snmp syslocation <Location>`
L2SW> `config snmp syslocation research-Lab`
- **Contact** Name of a person or organization.
L2SW> `config snmp syscontact <Contact>`
L2SW> `config snmp syscontact Network-Admin`

To display SNMP system settings, use the following command.

```
L2SW> show snmp system  
L2SW> show snmp system
```

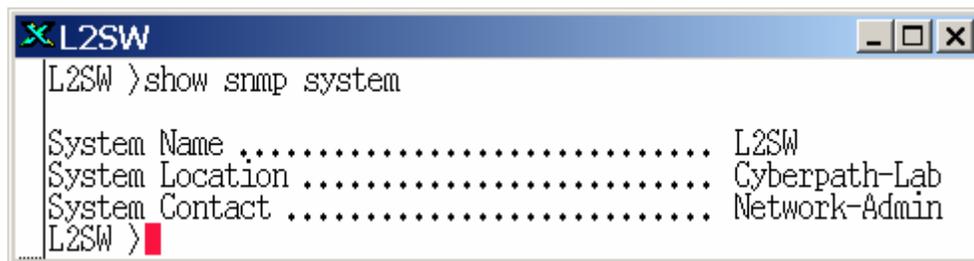


Figure 6-35 Displays SNMP system settings

6.18.2 SNMP Community setup:

Community strings serve as passwords and it has two modes to configure.

- **Read only(ro)**: Enables requests accompanied by this string to display MIB-object information.
- **Read write(rw)**. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.
- To add community name, use the following command. SNMP community name can be up to 16 characters.

```
L2SW> config snmp community add <name> <ro/rw>  
L2SW> config snmp community add finance-group rw
```

- To delete community name, use the following command. SNMP community name can be up to 16 characters.

```
L2SW> config snmp community delete <name>  
L2SW> config snmp community delete finance-group
```

- To display SNMP community settings:

```
L2SW> show snmp community
```

```

L2SW >show snmp community

      SNMP Community Name      Access Mode
-----
public                          Read Only
private                          Read/Write
Cyberpath                         Read/Write
L2SW >

```

Figure 6-36 Displays SNMP community settings

6.18.3 SNMP Trap Setup

Trap Manager: A trap manager is a management station that receives traps (alarms and event notifications) and the system alerts generated by the switch. If no trap manager is defined, switch will not issue any trap. Create a trap manager by entering the IP address of the station and a community string, using the following command:

- To add trap manager IP address and community name, use the following command.

```

L2SW> confi g snmp trap add <ipaddr> <communityname>
L2SW> confi g snmp trap add 172. 30. 40. 202 fi nance-group

```

- To delete trap manager, use the following command.

```

L2SW> confi g snmp trap del ete <ipaddr>
L2SW> confi g snmp trap del ete 172. 30. 40. 202

```

- To display SNMP trap settings, use the following command.

```

L2SW> show snmp trap
L2SW> show snmp trap

```

```

L2SW >show snmp trap

      SNMP Community Name      IP Address
-----
Cyberpath                       172.30.40.202
L2SW >

```

Figure 6-37 Displays SNMP trap settings

6.18.4 SNMPv3 Configuration

L2SW supports SNMP v1, SNMP v2c and SNMP v3 in multi-lingual mode. Based on the SNMP version type supported by the manager, the L2SW will automatically adapt itself to respond to the manager’s request. There is no need to explicitly configure the SNMP version. However, there are parameters that are specific to SNMP v3. The following subsections describe the commands used to configure the parameters that are specific to SNMP v3.

- In SNMPv3 mode, SNMP agents in L2SW switches are identified using a unique Engine ID. By default the switch is configured with a unique system ID=80:00:1A:73:MAC address of the switch (6 octets). Users can reconfigure the SNMP EngineID using the following command. EngineID is a hexadecimal byte string with each byte separated by a colon character. To display EngineID configured for the switch, use the **show snmp system** command as illustrated in Figure 6-38.

```
L2SW> confi g snmp engi nei d <Engi nei D>
L2SW> confi g snmp engi nei d 00: 00: 1F: 4E: 30: 10: 3D
```



The Engine ID specified by user is added to the system prefix 80:00:1A:73.

```
C:\WINNT\system32\telnet.exe
(L2SW) >show snmp system
System Name ..... L2SW-10
System Location ..... third-floor
System Contact ..... John_Doe
SNMP Engineid : 80:00:1a:73:03:00:50:a8:80:08:60
(L2SW) >
```

Figure 6-38: SNMP System Configuration

- To configure an SNMP view, users have to define a viewname (text string of 16 characters), followed by an OID representing MIB subtree and an operational directive to include or exclude the MIB subtree. The following command is used to create a SNMP MIB view.

```
L2SW> confi g snmp vi ew add <vi ewname> <subtree> <i ncl uded/excl uded>
L2SW> confi g snmp vi ew add l2sw-user 1.3.6.1.2 i ncl uded
```

To remove an existing view or to delete all user created views, use the following command.

```
L2SW> confi g snmp vi ew del ete <vi ewname>
```

Or

```
L2SW> confi g snmp vi ew del al l
```

```
L2SW> confi g snmp vi ew del ete l2sw-user
```

L2SW creates the following two views as default views. The user can modify or delete these views if required.

- **internet**: Enter subtree rooted at OID 1.3.6.1
- **restricted**: 5 Subtrees with the following root OIDs:
 - 1.3.6.1.2.1.1
 - 1.3.6.1.2.1.11
 - 1.3.1.6.3.10.2.1
 - 1.3.1.6.3.11.2.1
 - 1.3.1.6.3.15.1.1

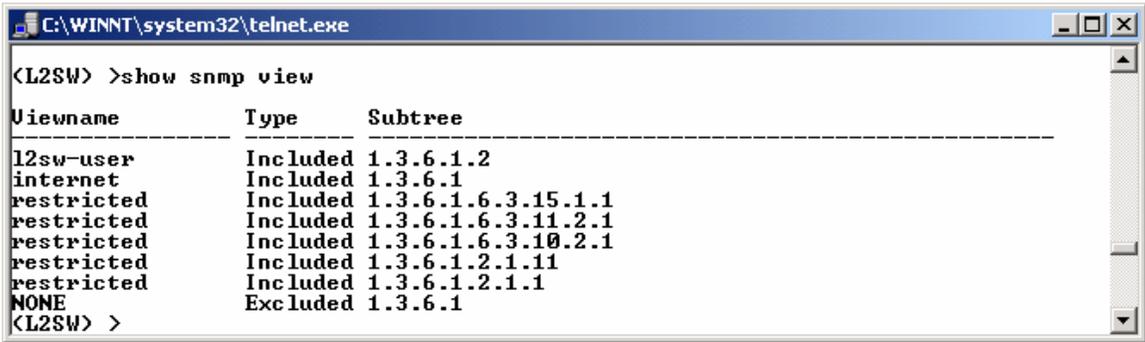


Some SNMPv3 managers allow users to configure a “context” name along with the Views.

L2SW currently doesn't support "contexts" to be associated with the Views. Therefore, the Context name should be configured as blank on the SNMP manager side.

To display all views created by the administrator, use the following command. Response from the switch for this command is illustrated in Figure 6-39.

```
L2SW> show snmp view  
L2SW> show snmp view
```



```
C:\WINNT\system32\telnet.exe  
<L2SW> >show snmp view  
-----  
Viewname      Type      Subtree  
-----  
l2sw-user     Included  1.3.6.1.2  
internet      Included  1.3.6.1  
restricted    Included  1.3.6.1.6.3.15.1.1  
restricted    Included  1.3.6.1.6.3.11.2.1  
restricted    Included  1.3.6.1.6.3.10.2.1  
restricted    Included  1.3.6.1.2.1.11  
restricted    Included  1.3.6.1.2.1.1  
NONE         Excluded  1.3.6.1  
<L2SW> >
```

Figure 6-39: SNMP MIB Views

- Groups to be supported in SNMPv3 mode can be created by the following command. The parameters associated with the creation of a group are: Group Name (a text string of up to 16 characters), security model (noAuthNoPriv, AuthNoPriv and AuthPriv), Readview name (a text string of 16 characters), Writeview name (a text string of 16 characters) and notifyview name (a text string of 16 characters).

```
L2SW> confi g snmp group add <groupname> <no/auth/pri v> <readvi ewname>  
<wri tevi ewname> <noti fyvi ewname>  
L2SW> confi g snmp group add l2sw-group auth l2sw-user l2sw-user  
l2sw-user
```

To delete a group or all the groups , use one of the following command.

```
L2SW> confi g snmp group del ete <groupname>  
  
Or  
  
L2SW> confi g snmp group del al l  
L2SW> confi g snmp group del ete l2sw-group
```

i The same group can be configured with different combination of views and access privileges. This would allow users belonging to the same group to have different access privileges

To display SNMP groups supported by the switch use the following command. The response from the switch is illustrated in Figure 6-40.

```
L2SW> show snmp group  
L2SW>show snmp group
```

```

C:\WINNT\system32\telnet.exe
(L2SW) >show snmp group

```

Groupname	Sec. Level	Readview	Writeview	Notifyview
l2sw-group	AuthNoPriv	l2sw-user	l2sw-user	l2sw-user
initial	AuthPriv	internet	internet	internet
initial	AuthNoPriv	internet	internet	internet
initial	NoAuthNoPriv	restricted	NONE	restricted

```

(L2SW) >_

```

Figure 6-40: SNMPv2 Group Configuration

- User Creation. New users can be created and assigned to an existing SNMPv3 group by using the following command. The parameters associated with the creation of a new user are: User name (text string of up to 16 characters), Group Name (name of the group to which the new user is assigned to), Auth. Password (text string of up to 16 characters), Priv. Password (text string of up to 16 characters). Authentication Password and Privacy Password are optional parameters. These parameters are not required if `noAuthNoPriv` security level is used for the group.

```

L2SW> confi g snmp user add <username> <groupname> [<auth-password>
[<priv-password>]]
L2SW> confi g snmp user add joey l2sw-group iamjoey mysecret

```

To delete a user or all users , use oen of the following command.

```

L2SW> confi g snmp user del ete <username>

```

Or

```

L2SW> confi g snmp user del all

```

```

L2SW> confi g snmp user del ete joey

```

To display SNMP users supported by the switch use the following command. The response from the switch is illustrated in Figure 6-41.

```

L2SW> show snmp user
L2SW>show snmp user

```

```

C:\WINNT\system32\telnet.exe
(L2SW) >show snmp user

```

User	Group	auth_Key	priv_Key
l2sw-user	l2sw-group	4427981ee0b22078ccdc552e878ff620	d7a11f56da58ceab6bcbbe601863fa04
PrivateUser	initial	09b6d47c3bea3d8ef7efe5f1358f6c59	09b6d47c3bea3d8ef7efe5f1358f6c59
AuthOnlyUser	initial	73d7fb65c279f49a2ca444295028e074	
PublicUser	initial		

```

(L2SW) >_

```

Figure 6-41: SNMP User Configuration

When SNMPv3 is enabled, L2SW automatically creates the following users attached to the `initial` group. The default users created by L2SW may be deleted, if they are not required.

- `PrivateUser`: authPriv privilege
- `AuthOnlyUser`: authNoPriv privilege

- **Publ i cUser**: noAuthNoPriv privilege

i *To get the Authentication and Privacy Password for the default users, contact L2SW technical support.*

Note that the Authentication Password and Privacy Passwords are displayed in encoded form similar to encrypted password display in /etc/passwd file in Unix/Linux systems.

i *L2SW supports 16 MIB views, 16 Groups and 64 Users*

i *Before deleting a group all users associated with that group must be deleted and before deleting a view all groups using that view must be deleted.*

i *L2SW will be busy for a while computing the message digest and encrypting the password string when Authentication and Privacy Passwords are configured.*

6.19 Remote Monitoring

RMON is a standard MIB that defines current and historical MAC-layer statistic and control objects, allowing network manager to capture real-time information across the entire network. The RMON standard is an SNMP MIB definition described in RFC 1757 for Ethernet.

A typical RMON configuration consists of a central network management station and a remote monitoring device, called an RMON agent (for e.g., L2SW switch is a RMON agent). From the management station, one can issue SNMP commands requesting information from the RMON agent. The RMON agent (e.g. L2SW switch) sends the requested information to the management station. The MIB allows a network agent to be configured to perform diagnostics and to collect statistics continuously, even when communication with the management station may not be possible or efficient. The network agent may then attempt to notify the management station when an exceptional condition occurs.

L2SW switch supports 1, 2, 3, & 9 RMON related MIB group. The RMON information can be retrieved from the switch only via SNMP interface by the SNMP Management station (an SNMP manager).

The following RMON groups are supported by L2SW:

Event group controls the generation & notification of events from L2SW switch. It consists of eventTable and logTable. Each entry in eventTable describes the parameters of the event that can be triggered. Event is a type of action to be taken, for e.g., a link may be turned up or down based on an event.

The **Al arm group** module periodically collects statistical samples from L2SW switch and compares them to pre-defined default values. L2SW switch creates one default value for each active physical port. These default entries define alarm Interval time to be 30 seconds, i.e. time for each sample.

The **HI story and Control Group** controls periodic statistical sampling of data from various types of interfaces. This group consists of history control table.

The **Ethernet Stati stic Group** contains statistics measured by L2SW switch for each monitored

Ethernet interface. This group consists of Ether Stats Table. L2SW switch implements Ether Stats Table. The Ether Stats Table consists of list of Ethernet statistics entries such as `etherstatsPkts64Octets`, `etherstatsPkts128to255Octets`, and `etherstatsPkts256to255Octets`

6.20 System Utilities

6.20.1 Management VLAN

To prevent unnecessary management packets (e.g., ARP, Telnet, etc.) from being sent to CPU, L2SW allows users to configure a VLAN for management traffic. Packets that would be normally forwarded to CPU will be dropped by L2SW ASIC if they don't belong to the management VLAN. Note Protocol PDUs such as BPDUs, LACP, etc. will be forwarded to the CPU for processing regarding of the management VLAN affiliation of the switch. By default, the management VLAN is a member of VLAN 1 (default VLAN). However, users can reassign the management to any other VLAN by using the following command:

```
L2SW> confi g mgmtvl an <1-4095>
L2SW> confi g mgmtvl an 25
```

To delete the management VLAN from non-default VLAN to default VLAN, use the following command.

```
L2SW> confi g mgmtvl an 1
```

To display the management VLAN information, use the following command:

```
L2SW> show mgmtvl an
L2SW> show mgmtvl an
```

6.20.2 SNTP Configuration

Simple Network Timing Protocol (SNTP) is used to synchronize the system clock with a SNTP server located either on the local network or on the internet. By synchronizing the system clock with a SNTP server helps SNTP switch to correct any clock drifts and to report accurate time in the Traps and syslog messages sent out.

To enable SNTP feature in L2SW, use the following command:

```
L2SW> confi g sntp admi nmode <enabl e/di sabl e>
L2SW> confi g sntp admi nmode enabl e
```

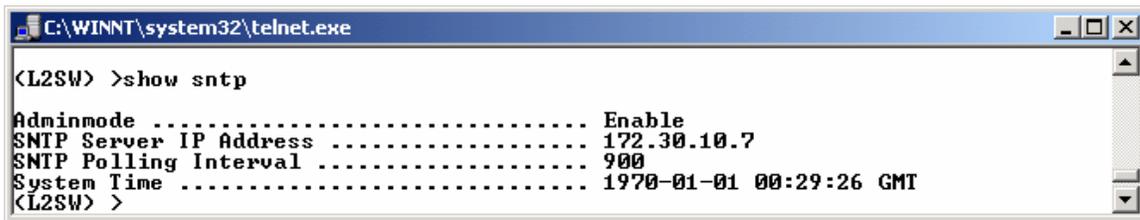
The next step in SNTP configuration is to define the IP address for the SNTP server. Use the following command to configure the SNTP server.

```
L2SW> confi g sntp server <l paddress>
L2SW> confi g sntp server 172. 30. 10. 7
```

The default SNTP polling interval is 1800 seconds. However, this value can be reconfigured by the following command.

```
L2SW> confi g sntp i nterval <1-60480>
L2SW> confi g sntp i nterval 900
```

The SNTP information can be displayed using **show sntp** command. The response from the L2SW to one such command is displayed in



```
C:\WINNT\system32\telnet.exe
<L2SW> >show sntp
Adminmode ..... Enable
SNTP Server IP Address ..... 172.30.10.7
SNTP Polling Interval ..... 900
System Time ..... 1970-01-01 00:29:26 GMT
<L2SW> >
```

Figure 6-42: SNTP Configuration

6.20.3 Syslog Configuration

L2SW can be configured to report system events and alarms to a remote syslog server. To enable syslog feature in the L2SW, use the following command.

```
L2SW> confi g log admi nmode <enabl e/di sabl e>
L2SW> confi g log admi nmode enabl e
```

To configure remote IP address for the syslog server, use the following command.

```
L2SW> confi g log remote <i paddress>
L2SW> confi g log remote 172. 30. 40. 7
```

You can display syslog configuration by using the command, **show log**.

6.20.4 TFTP Backup or Upload Configuration

TFTP (Trivial File Transfer Protocol) is used to transfer software images into the switch and it is also used to download and upload configuration databases.

To upload a copy of current configuration database from system flash to TFTP server use following command. Before starting the upload operation, make sure that the TFTP server is reachable from the switch.

In the following example, it is assumed that TFTP server IP address is 172.30.10.8 and filename used is ESSF10-1-config.

```
L2SW> copy confi g tftp <i paddr> <fi le-name>
L2SW> copy confi g tftp 172. 30. 10. 8 ESSF10-1-confi g
```



```
L2SW
L2SW >copy config tftp 172.30.10.8 ESSF10-1-config
Uploading the configuration, please wait...

The configuration was uploaded successfully.
L2SW >
```

Figure 6-43 Displays upload configuration to TFTP server

6.20.5 TFTP restore or download configuration

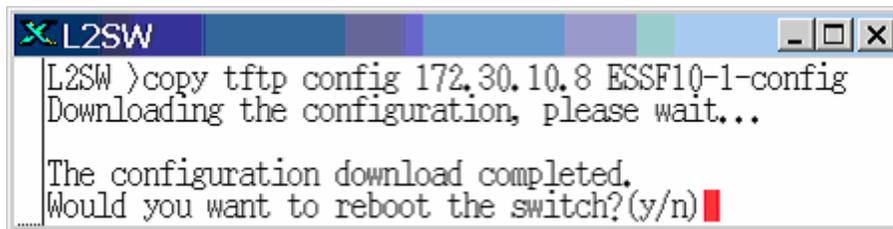
To restore the switch's configuration database from a TFTP server to the switch, use the following set of commands. Before starting the restore operation, make sure that the configuration database file is located in the TFTP server and that the TFTP server is reachable from the switch.

```
L2SW> copy tftp config <ipaddr> <filename>  
L2SW> copy tftp config 172.30.10.8 ESSF10-1-config
```

Downloading the configuration, please wait...

The configuration download completed.

Would you want to reboot the switch?(y/n) Y

A screenshot of a terminal window titled 'L2SW'. The terminal shows the following text: 'L2SW >copy tftp config 172.30.10.8 ESSF10-1-config', 'Downloading the configuration, please wait...', 'The configuration download completed.', and 'Would you want to reboot the switch?(y/n)'. A red cursor is positioned at the end of the last line.

```
L2SW >copy tftp config 172.30.10.8 ESSF10-1-config  
Downloading the configuration, please wait...  
  
The configuration download completed.  
Would you want to reboot the switch?(y/n)
```

Figure 6-44 Displays configuration download to system

6.20.6 TFTP Update Firmware

To download a copy of an executable image from TFTP server into system flash, use the following command. Before starting the image download operation, make sure that the executable image file is located in the TFTP server and that the TFTP server is reachable from the switch.

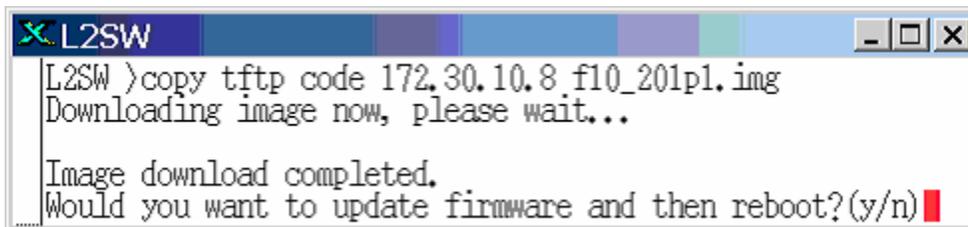
In the example shown below, the TFTP server IP address is 172.30.10.8 and image filename is f10_201.img.

```
L2SW> copy tftp code <ipaddr> <filename>  
L2SW> copy tftp code 172.30.10.8 f10_201p1.img
```

Downloading image now, please wait...

Image download completed.

Would you want to update firmware and then reboot?(y/n) Y

A screenshot of a terminal window titled 'L2SW'. The terminal shows the following text: 'L2SW >copy tftp code 172.30.10.8 f10_201p1.img', 'Downloading image now, please wait...', 'Image download completed.', and 'Would you want to update firmware and then reboot?(y/n)'. A red cursor is positioned at the end of the last line.

```
L2SW >copy tftp code 172.30.10.8 f10_201p1.img  
Downloading image now, please wait...  
  
Image download completed.  
Would you want to update firmware and then reboot?(y/n)
```

Figure 6-45 Displays image download

6.20.7 Default Configuration

To reset the switch and restore the switch configuration to factory settings, use the following command:

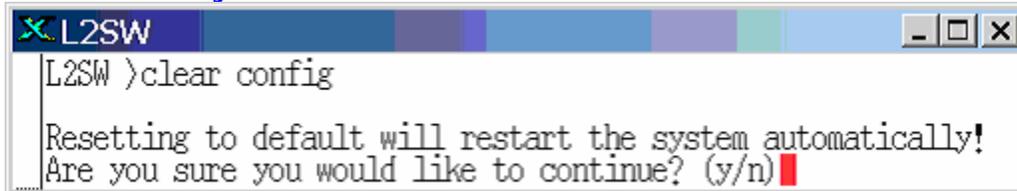
```
L2SW> clear config
Resetting to default will restart the system automatically!
Are you sure you would like to continue? (y/n) y
```

Figure 6-46 Reset switch configuration to factory default

6.20.8 Reboot

To just reboot the switch without restoring to default factory configuration, use the following

```
L2SW> reset system
```



```
Are you sure you would like to reset the system? (y/n)y
```

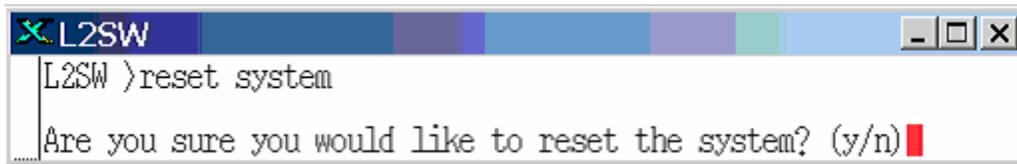


Figure 6-47 Displays system reboot operation

7. Appendix A: Terms and Abbreviations

AN	Auto Negotiation
ARP	Address Resolution Protocol
BSR	Broadcast Storm Recovery
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CMLI	Console Menu Line Interface
CRC	Cyclic Redundancy Check
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration/Control Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ESS	Ethernet Smart Switch
FE	Fast Ethernet
FTP	File Transfer Protocol
GVRP	Generic VLAN Registration Protocol
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
Hz	Hertz
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IFG	Inter-Frame Gap
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IST	Internal Spanning Tree
kbps	kilobits per second
kHz	kilohertz

L2	OSI Layer 2
LACP	Link Access Control Protocol
LAG	Link Aggregation
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Controller
Max	Maximum
Min	Minimum
MIB	Management Information Base
Mbps	Megabits per second
MBONE	Multicast backbone of the internet
MD5	Message Digest 5
Min	Minimum
ms	millisecond
MST	Mutiple Spanning Tree
MSTP	Multiple Spanning Tree Protocol
MSTI	Multiple Spanning Tree Instance
NE	Network Element
NIC	Network Interface Card
OSI	Open Systems Interconnection
PD	Powered Device
PDU	Protocol Data Unit
PING	Packet Internet Groper
PSE	Power Source Equipment
PVID	Port VLAN ID
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol

RFC	Request For Comment (TCP/IP Standard-Document)
RMON	Remote Monitoring
RO	Read Only
RSTP	Rapid Spanning Tree Protocol
RW	Read Write
RX	Receive
SNMP	Simple Network Management Protocol
SNTP	Simple Network Timing Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File transfer Protocol (TCP/IP)
TX	Transmit
UDP	User Datagram Protocol
VLAN	Virtual LAN
WBI	Web Based Interface