SabreNet-24000
24-Port Rugged Ethernet Switch
User Manual

Revision	Date	Comments
A.01	08/15/22	Initial Release

FOR TECHNICAL SUPPORT
PLEASE CONTACT:

support@diamondsystems.com

Diamond Systems Corporation
158 Commercial Street
Sunnyvale, CA 94086 USA
Tel 1-650-810-2500
Fax 1-650-810-2525
www.diamondsystems.com

CONTENTS

1. IMPORTANT SAFE HANDLING INFORMATION

WARNING!

ESD-Sensitive Electronic Equipment

Observe ESD-safe handling procedures when working with this product.

Always use this product in a properly grounded work area and wear appropriate ESD-preventive clothing and/or accessories.

Always store this product in ESD-protective packaging when not in use.

Safe Handling Precautions

The SabreNet 24000 contains a high density connector with many connections to sensitive electronic components. This creates many opportunities for accidental damage during handling, installation and connection to other equipment. The list here describes common causes of failure found on boards and systems returned to Diamond Systems for repair. This information is provided as a source of advice to help you prevent damaging your Diamond (or any vendor's) boards.

ESD damage – This type of damage is usually almost impossible to detect, because there is no visual sign of failure or damage. The symptom is that the board eventually simply stops working, because some component becomes defective. Usually the failure can be identified and the chip can be replaced. To prevent ESD damage, always follow proper ESD-prevention practices when handling computer boards.

Power supply wired backwards – Our power supplies and boards are not designed to withstand a reverse power supply connection. This will destroy each IC that is connected to the power supply (i.e. almost all ICs). In this case the board will most likely will be unrepairable and must be replaced. A chip destroyed by reverse power or by excessive power will often have a visible hole on the top or show some deformation on the top surface due to vaporization inside the package. **Check twice before applying power!**

2. INTRODUCTION

2.1 Description

SABRENET-24000 is a rugged system featuring a 24-port managed Ethernet switch. The system features full IP67 rating and MIL-STD-810G compatibility ideal for vehicle and other harsh environment applications. The system uses the Diamond Systems EPS-24G4X-HSP-1588 switch offering 24 10/100/1000Mbps copper ports +4 10G copper ports.

The embedded IStaX software provides all switching functionality without any software development. Configuration is manageable by either an “in-band” website embedded in the software or an “out of band” serial port running a command line interface (CLI).

2.2 Features

2.2.1 System Features

Sl No	Component	Feature	Qty
1	1G Ethernet Ports	10/100/1000 Mbps Copper Ethernet Ports	24
2	10G Ethernet Ports	10G Copper Ethernet Ports with SFP+ to RJ45 transceiver modules	4
3	Serial Port	RS-232 port for host interface, 38400/N/8/1	1
4	PPS	Synchronization Pulse per Second	1

2.2.2 I/O Features and Connector Types

Feature	Description	Connector Type
Power	+7V to +40V DC input supply with MIL-STD-461 filtering	D38999/20KC4PN
Ethernet	12x 10/100/1000 Mbps Copper Ports	D38999/20KH35SN
	12x 10/100/1000 Mbps Copper Ports	D38999/20KH35SN
	4x 10G Copper Ports	M12 X-Coded Female
Serial	1x RS-232, 38400/N/8/1	D38999/20KG35SN
PPS	1x Synchronization pulse	D38999/20KH35SN

2.2.3 Mechanical and Environmental

- Dimensions: 11.2” W x 10.0” D x 3.24” H
- 2.921 Kg
- 7-40VDC power input
- Built-in MIL-STD-461 filter
- -40°C to +85°C ambient operating temperature

Typical power consumption figures are provided below.

Vin (V)	Configuration	Power (W)
24V	No Ports Connected	13W
	All 24 1G ports active	20W
	All 24G ports and all 4 10G ports active	26W

3. BLOCK DIAGRAM

SabreNet-24000 utilizes the Diamond Systems EPSM-10GX4 Ethernet switch module which consists of a Layer 3 managed Ethernet switch with built-in microcontroller and memory for configuration and management. The flash memory holds dual application images along with the boot code. The NOR Flash holds the configuration parameters.

An RS-232 interface is provided to enable communication between the on-board management microcontroller and a host processor through a command line interface (CLI). The microcontroller is also accessible through one of the Ethernet ports via a web management interface.

Power is provided through the +7V-+34VDC wide-range DC power supply, enabling use with industrial power sources.

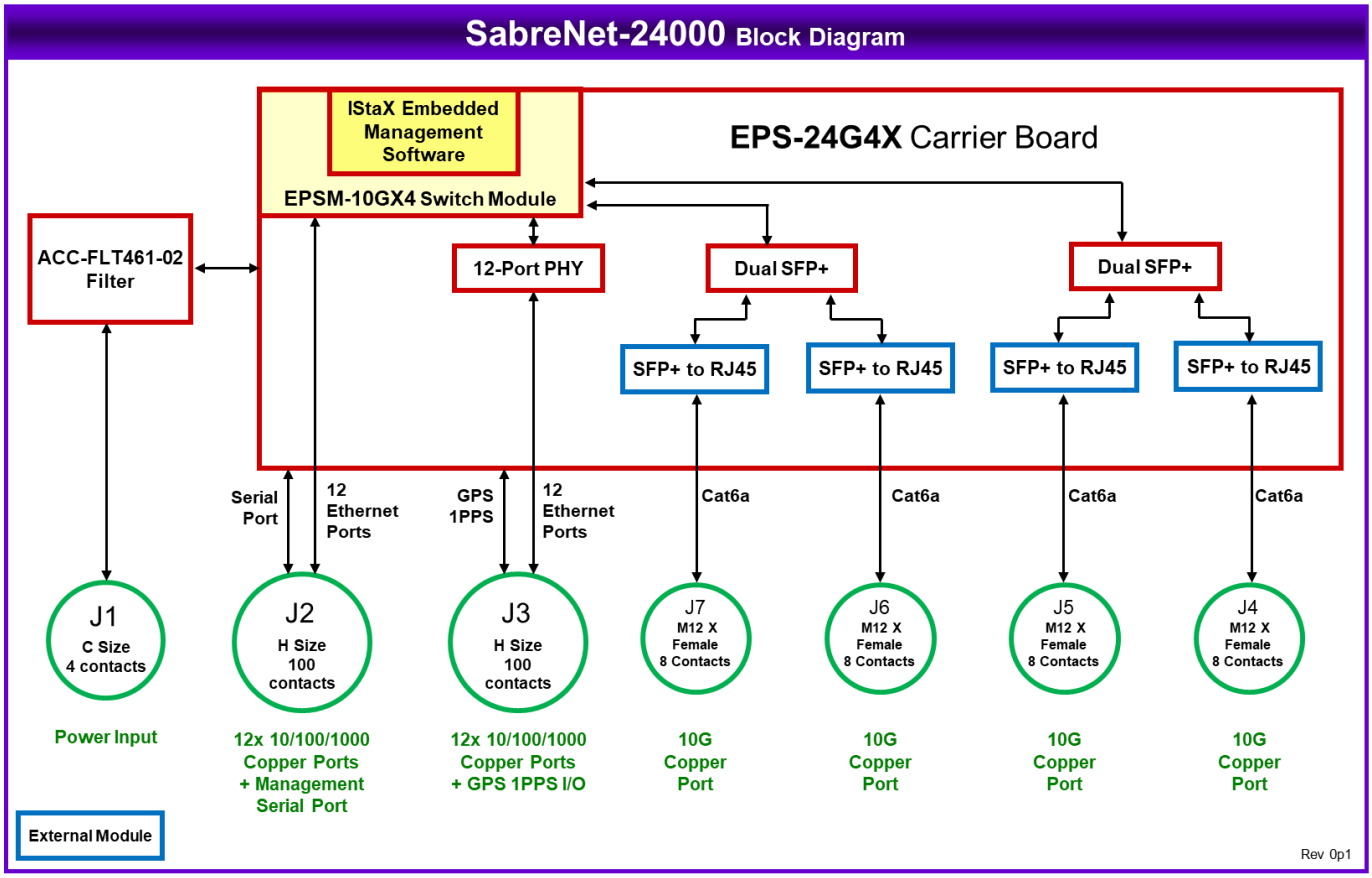


Figure 1: System Architecture of SabreNet-24000

4. MECHANICAL DRAWING

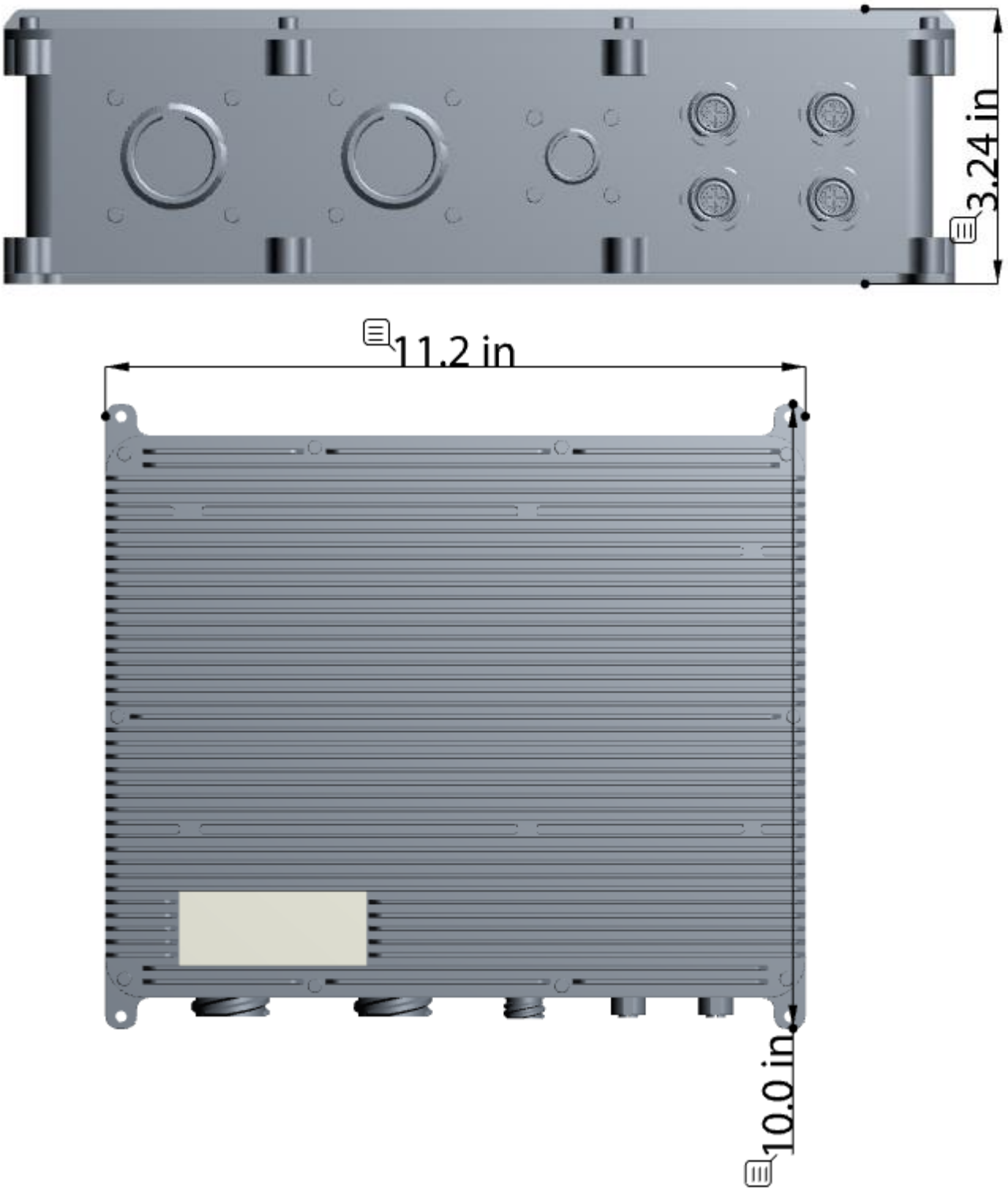


Figure 2: Enclosure Details

All dimensions are in inches.

5. FEATURES ON I/O CONNECTORS

SabreNet-24000 consists of three MIL D38999 connectors & four M12 X-coded Female connectors on the front panel. Each connector provides access to different interfaces on the system. The seven connectors & the interfaces available on them are tabulated below:

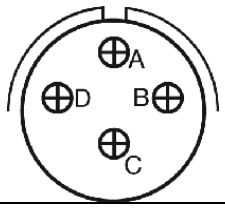
Silk Screen Marking	Connector Typw	Available Interfaces
J1	D38999/20KC4PN	Power
J2	D38999/20KH35SN	1G Copper Ports 1- 12
		1x PPS
J3	D38999/20KH35SN	1G Copper Ports 13 - 24
		1x RS-232
J4	M12 X-Coded Female 8-Position	10G Copper port 25
J5	M12 X-Coded Female 8-Position	10G Copper port 26
J6	M12 X-Coded Female 8-Position	10G Copper port 27
J7	M12 X-Coded Female 8-Position	10G Copper port 28

Figure 3 System Layout (front View)

6. CONNECTOR PINOUT AND DESCRIPTION

The SabreNet 24000 contains 3 I/O connectors of type MIL-DTL-38999 series III with olive drab cadmium finish. All D38999 connectors are wall mount type and are installed from the inside of the box with sealing gaskets and nut plates.

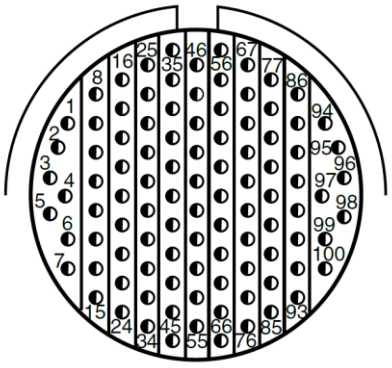
6.1 Power Connector J1

System connector	Connector type	MIL D38999/20KC4PN
	Illustration Viewed from exterior	
Mating connector	Connector type	MIL 26xC4SN; x = K, F, G or equivalent

Connector pinout

D38999 Pin no.	Signal
B	Vin (+7-40V)
C	GND
A	Vin (+7-40V)
D	GND

6.2 I/O Connector J2

System connector	Connector type	MIL D38999/ 20KH35SN
	Illustration Viewed from exterior	
Mating connector	Connector type	MIL D38999/26KH35PN or equivalent

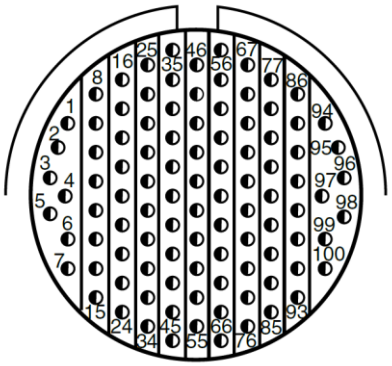
J2 Connector pinout

D38999 Pin no.	Signal	Description
100	P01-DD+	Port 1 Bi-directional pair D+
99	P01-DD-	Port 1 Bi-directional pair D-
98	P01-DC+	Port 1 Bi-directional pair C+
97	P01-DC-	Port 1 Bi-directional pair C-
96	P01-DB+	Port 1 Bi-directional pair B+
95	P01-DB-	Port 1 Bi-directional pair B-
88	P01-DA+	Port 1 Bi-directional pair A+
89	P01-DA-	Port 1 Bi-directional pair A-
93	P02-DD+	Port 2 Bi-directional pair D+
92	P02-DD-	Port 2 Bi-directional pair D-
85	P02-DC+	Port 2 Bi-directional pair C+
84	P02-DC-	Port 2 Bi-directional pair C-
76	P02-DB+	Port 2 Bi-directional pair B+
75	P02-DB-	Port 2 Bi-directional pair B-
66	P02-DA+	Port 2 Bi-directional pair A+
65	P02-DA-	Port 2 Bi-directional pair A-
91	P03-DD+	Port 3 Bi-directional pair D+
90	P03-DD-	Port 3 Bi-directional pair D-
83	P03-DC+	Port 3 Bi-directional pair C+
82	P03-DC-	Port 3 Bi-directional pair C-
74	P03-DB+	Port 3 Bi-directional pair B+
73	P03-DB-	Port 3 Bi-directional pair B-

64	P03-DA+	Port 3 Bi-directional pair A+
63	P03-DA-	Port 3 Bi-directional pair A-
81	P04-DD+	Port 4 Bi-directional pair D+
80	P04-DD-	Port 4 Bi-directional pair D-
72	P04-DC+	Port 4 Bi-directional pair C+
71	P04-DC-	Port 4 Bi-directional pair C-
62	P04-DB+	Port 4 Bi-directional pair B+
61	P04-DB-	Port 4 Bi-directional pair B-
52	P04-DA+	Port 4 Bi-directional pair A+
51	P04-DA-	Port 4 Bi-directional pair A-
94	P05-DD+	Port 5 Bi-directional pair D+
87	P05-DD-	Port 5 Bi-directional pair D-
86	P05-DC+	Port 5 Bi-directional pair C+
77	P05-DC-	Port 5 Bi-directional pair C-
78	P05-DB+	Port 5 Bi-directional pair B+
79	P05-DB-	Port 5 Bi-directional pair B-
70	P05-DA+	Port 5 Bi-directional pair A+
69	P05-DA-	Port 5 Bi-directional pair A-
68	P06-DD+	Port 6 Bi-directional pair D+
67	P06-DD-	Port 6 Bi-directional pair D-
58	P06-DC+	Port 6 Bi-directional pair C+
57	P06-DC-	Port 6 Bi-directional pair C-
56	P06-DB+	Port 6 Bi-directional pair B+
46	P06-DB-	Port 6 Bi-directional pair B-
47	P06-DA+	Port 6 Bi-directional pair A+
48	P06-DA-	Port 6 Bi-directional pair A-
38	P07-DD+	Port 7 Bi-directional pair D+
37	P07-DD-	Port 7 Bi-directional pair D-
27	P07-DC+	Port 7 Bi-directional pair C+
26	P07-DC-	Port 7 Bi-directional pair C-
36	P07-DB+	Port 7 Bi-directional pair B+
35	P07-DB-	Port 7 Bi-directional pair B-
25	P07-DA+	Port 7 Bi-directional pair A+
16	P07-DA-	Port 7 Bi-directional pair A-
18	P08-DD+	Port 8 Bi-directional pair D+
17	P08-DD-	Port 8 Bi-directional pair D-
10	P08-DC+	Port 8 Bi-directional pair C+
9	P08-DC-	Port 8 Bi-directional pair C-
8	P08-DB+	Port 8 Bi-directional pair B+

1	P08-DB-	Port 8 Bi-directional pair B-
2	P08-DA+	Port 8 Bi-directional pair A+
3	P08-DA-	Port 8 Bi-directional pair A-
41	P09-DD+	Port 9 Bi-directional pair D+
40	P09-DD-	Port 9 Bi-directional pair D-
39	P09-DC+	Port 9 Bi-directional pair C+
28	P09-DC-	Port 9 Bi-directional pair C-
30	P09-DB+	Port 9 Bi-directional pair B+
29	P09-DB-	Port 9 Bi-directional pair B-
20	P09-DA+	Port 9 Bi-directional pair A+
19	P09-DA-	Port 9 Bi-directional pair A-
54	P10-DD+	Port 10 Bi-directional pair D+
53	P10-DD-	Port 10 Bi-directional pair D-
43	P10-DC+	Port 10 Bi-directional pair C+
42	P10-DC-	Port 10 Bi-directional pair C-
32	P10-DB+	Port 10 Bi-directional pair B+
31	P10-DB-	Port 10 Bi-directional pair B-
22	P10-DA+	Port 10 Bi-directional pair A+
21	P10-DA-	Port 10 Bi-directional pair A-
45	P11-DD+	Port 11 Bi-directional pair D+
55	P11-DD-	Port 11 Bi-directional pair D-
34	P11-DC+	Port 11 Bi-directional pair C+
44	P11-DC-	Port 11 Bi-directional pair C-
24	P11-DB+	Port 11 Bi-directional pair B+
33	P11-DB-	Port 11 Bi-directional pair B-
15	P11-DA+	Port 11 Bi-directional pair A+
23	P11-DA-	Port 11 Bi-directional pair A-
14	P12-DD+	Port 12 Bi-directional pair D+
13	P12-DD-	Port 12 Bi-directional pair D-
12	P12-DC+	Port 12 Bi-directional pair C+
11	P12-DC-	Port 12 Bi-directional pair C-
7	P12-DB+	Port 12 Bi-directional pair B+
6	P12-DB-	Port 12 Bi-directional pair B-
5	P12-DA+	Port 12 Bi-directional pair A+
4	P12-DA-	Port 12 Bi-directional pair A-
59	PPS-OUT	1 PPS clock Output
60	PPS-GND1	Digital Ground
49	PPS-IN	PPS clock Input
50	PPS-GND2	Digital Ground

6.3 I/O Connector J3

System connector	Connector type	MIL D38999/ 20KH35SN
	Illustration Viewed from exterior	
Mating connector	Connector type	MIL D38999/26KH35PN or equivalent

J3 Connector pinout

D38999 Pin no.	Signal	Description
100	P13-DD+	Port 13 Bi-directional pair D+
99	P13-DD-	Port 13 Bi-directional pair D-
98	P13-DC+	Port 13 Bi-directional pair C+
97	P13-DC-	Port 13 Bi-directional pair C-
96	P13-DB+	Port 13 Bi-directional pair B+
95	P13-DB-	Port 13 Bi-directional pair B-
88	P13-DA+	Port 13 Bi-directional pair A+
89	P13-DA-	Port 13 Bi-directional pair A-
93	P14-DD+	Port 14 Bi-directional pair D+
92	P14-DD-	Port 14 Bi-directional pair D-
85	P14-DC+	Port 14 Bi-directional pair C+
84	P14-DC-	Port 14 Bi-directional pair C-
76	P14-DB+	Port 14 Bi-directional pair B+
75	P14-DB-	Port 14 Bi-directional pair B-
66	P14-DA+	Port 14 Bi-directional pair A+
65	P14-DA-	Port 14 Bi-directional pair A-
91	P15-DD+	Port 15 Bi-directional pair D+
90	P15-DD-	Port 15 Bi-directional pair D-
83	P15-DC+	Port 15 Bi-directional pair C+
82	P15-DC-	Port 15 Bi-directional pair C-
74	P15-DB+	Port 15 Bi-directional pair B+
73	P15-DB-	Port 15 Bi-directional pair B-

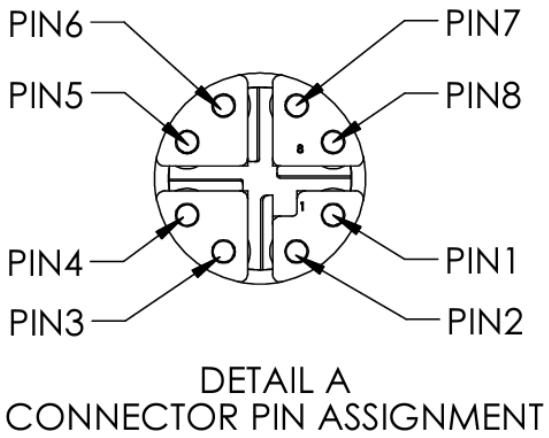
64	P15-DA+	Port 15 Bi-directional pair A+
63	P15-DA-	Port 15 Bi-directional pair A-
81	P16-DD+	Port 16 Bi-directional pair D+
80	P16-DD-	Port 16 Bi-directional pair D-
72	P16-DC+	Port 16 Bi-directional pair C+
71	P16-DC-	Port 16 Bi-directional pair C-
62	P16-DB+	Port 16 Bi-directional pair B+
61	P16-DB-	Port 16 Bi-directional pair B-
52	P16-DA+	Port 16 Bi-directional pair A+
51	P16-DA-	Port 16 Bi-directional pair A-
94	P17-DD+	Port 17 Bi-directional pair D+
87	P17-DD-	Port 17 Bi-directional pair D-
86	P17-DC+	Port 17 Bi-directional pair C+
77	P17-DC-	Port 17 Bi-directional pair C-
78	P17-DB+	Port 17 Bi-directional pair B+
79	P17-DB-	Port 17 Bi-directional pair B-
70	P17-DA+	Port 17 Bi-directional pair A+
69	P17-DA-	Port 17 Bi-directional pair A-
68	P18-DD+	Port 18 Bi-directional pair D+
67	P18-DD-	Port 18 Bi-directional pair D-
58	P18-DC+	Port 18 Bi-directional pair C+
57	P18-DC-	Port 18 Bi-directional pair C-
56	P18-DB+	Port 18 Bi-directional pair B+
46	P18-DB-	Port 18 Bi-directional pair B-
47	P18-DA+	Port 18 Bi-directional pair A+
48	P18-DA-	Port 18 Bi-directional pair A-
38	P19-DD+	Port 19 Bi-directional pair D+
37	P19-DD-	Port 19 Bi-directional pair D-
27	P19-DC+	Port 19 Bi-directional pair C+
26	P19-DC-	Port 19 Bi-directional pair C-
36	P19-DB+	Port 19 Bi-directional pair B+
35	P19-DB-	Port 19 Bi-directional pair B-
25	P19-DA+	Port 19 Bi-directional pair A+
16	P19-DA-	Port 19 Bi-directional pair A-
18	P20-DD+	Port 20 Bi-directional pair D+
17	P20-DD-	Port 20 Bi-directional pair D-
10	P20-DC+	Port 20 Bi-directional pair C+
9	P20-DC-	Port 20 Bi-directional pair C-
8	P20-DB+	Port 20 Bi-directional pair B+

1	P20-DB-	Port 20 Bi-directional pair B-
2	P20-DA+	Port 20 Bi-directional pair A+
3	P20-DA-	Port 20 Bi-directional pair A-
41	P21-DD+	Port 21 Bi-directional pair D+
40	P21-DD-	Port 21 Bi-directional pair D-
39	P21-DC+	Port 21 Bi-directional pair C+
28	P21-DC-	Port 21 Bi-directional pair C-
30	P21-DB+	Port 21 Bi-directional pair B+
29	P21-DB-	Port 21 Bi-directional pair B-
20	P21-DA+	Port 21 Bi-directional pair A+
19	P21-DA-	Port 21 Bi-directional pair A-
54	P22-DD+	Port 22 Bi-directional pair D+
53	P22-DD-	Port 22 Bi-directional pair D-
43	P22-DC+	Port 22 Bi-directional pair C+
42	P22-DC-	Port 22 Bi-directional pair C-
32	P22-DB+	Port 22 Bi-directional pair B+
31	P22-DB-	Port 22 Bi-directional pair B-
22	P22-DA+	Port 22 Bi-directional pair A+
21	P22-DA-	Port 22 Bi-directional pair A-
45	P23-DD+	Port 23 Bi-directional pair D+
55	P23-DD-	Port 23 Bi-directional pair D-
34	P23-DC+	Port 23 Bi-directional pair C+
44	P23-DC-	Port 23 Bi-directional pair C-
24	P23-DB+	Port 23 Bi-directional pair B+
33	P23-DB-	Port 23 Bi-directional pair B-
15	P23-DA+	Port 23Bi-directional pair A+
23	P23-DA-	Port 23 Bi-directional pair A-
14	P24-DD+	Port 24 Bi-directional pair D+
13	P24-DD-	Port 24 Bi-directional pair D-
12	P24-DC+	Port 24 Bi-directional pair C+
11	P24-DC-	Port 24 Bi-directional pair C-
7	P24-DB+	Port 24 Bi-directional pair B+
6	P24-DB-	Port 24 Bi-directional pair B-
5	P24-DA+	Port 24 Bi-directional pair A+
4	P24-DA-	Port 24 Bi-directional pair A-
49	SER-GND	Digital Ground
59	SER-TX	RS232 Transmit output
60	SER-RX	RS232 Receive input
50	N/C	

6.4 I/O Connector J4,J5,J6 & J7

M12 8 position X-Coded female connector

M12 Connector	Signal
1	SFP1-DA+
2	SFP1-DA-
3	SFP1-DB+
4	SFP1-DB-
5	SFP1-DD+
6	SFP1-DD-
7	SFP1-DC-
8	SFP1-DC+



7. GETTING STARTED

This section provides the steps necessary to set up the SabreNet-24000.

1. Connect the serial cable between the connector **J2** on the carrier board and a PC's serial port. Open the HyperTerminal application with baud rate set to 115200bps.
2. Connect the Ethernet cables from PC's Ethernet port/ Ethernet Switch, to any of the connectors **J2 or J3** on the SabreNet 24000 system, depending on the number of active ports used.
3. Connect a LAN cable between the PC to any one of the desired ports on the cable(s) connected to the system in step 2.
4. The SabreNet 24000 works on a wide range of voltages from +7V to +34V.Connect the power cable between the connector **J1** and a regulated power supply.
5. Switch on the power supply and view the messages on the hyper terminal. The default user id is **admin** with no password.
6. Set the IP address as 192.168.1.60 to access the Web interface.

8. WEB INTERFACE AND CLI OVERVIEW

The Command Line Interface (CLI) is a command Line or Text-Based-User Interface with no screen editing capabilities. In this interface, a User types commands and responds to prompts using Syntax and Parameters which are promptly executed by the system.

The CLI can be accessed directly via the RS-232 serial connection.

An Administrator and a User are assigned different sets of privileges. The User must log in before CLI commands can be executed.

The Web Interface offers an alternate User Interface to CLI.

The Web Interface is In-band mode and requires the use of any one Ethernet port which provides simultaneous Web management and normal usage.

Both, the CLI and Web Interface, provide the same functionality.

9. USING THE CLI INTERFACE

9.1 Making an Initial Connection

Serial Line Requirements:

- 115200 baud
- 8-bit data
- No parity
- 1 stop bit

9.2 Login Information

```
Username: admin
Password: {none}
```

The Board is configured with the default IP address **192.168.1.60** to enable access to the Web Interface. On access, it enables the User to enter the Admin panel and change/modify settings.

The IP address, mask, and gateway must be configured according to the environment.

For example, if the environment includes a DHCP server, to enable both, the IP and DHCP, enter the following code depicted below:

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address dhcp
(config-if-vlan)# end
```

The example below depicts the configuration of a static IP address.

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)#     ip     address     192.168.1.60
255.255.0.0
(config-if-vlan)# end
```

A confirmation prompt of the IP address is displayed as depicted in the block below.

```
# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 192.168.1.60         Manual   UP
#
```

9.3 Login/Logout Procedures

To access CLI, the User must be authenticated. On system prompt:

- Enter a user name and password, which can be configured.
- Enter **exit** command to Log out at any time and at any context level.

9.4 Accessing Help

For assistance press the question mark **?** symbol or type **Help** on the keyboard or type the full or partial command followed by a question mark **?**.

Selecting the question mark **?** symbol will list all the commands on the screen.

The help information displayed depends on the context in which help has been requested. The content is displayed in the following format:

- On the Top-level, a list of Command Groups is displayed.
- At the Group level, a list of the command syntaxes for the current group is displayed.
- If the **Help** command is issued for a specific command, the command syntax and a description of the command is displayed.

9.5 Entering Commands

- Commands are not case-sensitive.
- Use the arrow keys: ← and → to navigate the page horizontally, or to move the cursor within the command line parameters being entered.
- Use the arrow keys ↑ and ↓ to navigate the page vertically or to scroll through a command history buffer of the latest twenty commands that were issued.
- Use the **Backspace** key to delete characters from the command being entered.

NOTE: Deleting character(s) is possible only when using a Terminal that is BS (8) character-compatible. The backspace key uses the ASCII set when pressed to complete the **Delete** request.

9.6 Global Commands

The following global commands are available in the Command Line Interface (CLI).

```
# ?
    clear        Reset functions
    configure    Enter configuration mode
    copy         Copy from source to destination
    debug        Debugging functions
    delete       Delete one file in flash: file system
    dir          Directory of all files in flash: file system
    disable      Turn off privileged commands
    do           To run exec commands in config mode
    dot1x        IEEE Standard for port-based Network Access Control
    enable       Turn on privileged commands
    exit         from EXEC mode
    firmware     upgrade/swap
    help         Description of the interactive help system
    ip           IPv4 commands
    logout       Exit from EXEC mode
```

```
more          Display file
no            Negate a command or set its defaults
ping          Send ICMP echo messages
reload        system
send          Send a message to other tty lines
show          Show running system information
terminal      Set terminal line parameters #
```

9.6.1 Resetting System to Factory Defaults

The `default` command in association with different parameters, executes specific functions, such as resetting the configuration of the Switch to factory defaults while retaining other configurations, or resetting all configurations to default settings.

The following syntax resets the configuration of the Switch to factory defaults.

```
# reload defaults #
```

NOTE: On execution, only the IP configuration is retained.

The `# reload defaults` command is also **issued** to restore the Switch to factory defaults in the following events:

- A blocked Web site or missing IP address, and with an active connection to a serial port**.**

NOTE: On execution, a system Reboot is required. This will erase all configurations and reset the Switch to factory default settings.

- A blocked Web site or missing IP address and with no access to the Web Management page.

To resolve this:

1. Connect a LAN cable from Port 1 to Port 2 of the Switch.
2. Power-cycle the Switch.

To load the Factory Default configuration including the IP Address using the Web Interface follow the instructions described in Section: 11 Factory Default Settings

- To retain specific configurations:

```
factory default [keep-basic] [keep-connect] [keep-monitor]
```

`keep-basic` Resets system settings to factory defaults and retains basic configurations

`keep-connect`: Resets settings system to factory defaults and retains connectivity.

`keep-monitor:` Resets settings system to factory defaults and retains monitoring data.

NOTE: On execution, Network settings will be retained.

9.6.2 IP Commands

The following command syntax should be used to enable Secure HTTP Web Redirect and Secure HTTP Web Server.

Secure Web redirection cannot be enabled until the Secure Web Server is enabled. To enable Secure Web Server, enter the syntax as follows:

```
(config)# ip http secure-server

(config)# ip http secure redirect
```

The following is a list of commonly used syntax for reference purposes.

1. To view the status of both HTTP Web Server and Web Redirection:

```
# show ip http server secure status
```

2. To disable Secure HTTP Web Redirect and Secure HTTP Web Server:

```
(config)# no ip http secure redirect
(config)# no ip http secure server
```

3. To enable Global IGMP snooping and unregistered IPMCv4 traffic flooding:

```
(config)# ip igmp snooping
(config)# ip igmp snooping vlan <v_vlan_list>
(config)# ip igmp unknown-flooding
```

4. To view IGMP snooping and the IGMP router port status:

```
# show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ip igmp snooping mrouter [ detail ]
```

5. To disable IGMP snooping and flooding:

```
(config)# no ip igmp snooping
(config)# no ip igmp snooping vlan [ <v_vlan_list> ]
(config)# no ip igmp unknown-flooding
```

6. To configure the IP route, view IP interface, route and statistics, clear the IP route, and IGMP snooping and IP statistics:

```
(config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
(config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
# show ip arp
# show ip interface brief
# show ip route
# show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
# clear ip arp
# clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
# clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

9.6.3 MAC Commands

The MAC Address Table can be configured using the following command syntax and parameters.

By default, Dynamic entries are removed from the MAC Table after 300 seconds. However, the Aging Time of the Dynamic MAC Table can be configured using the following syntax as well.

```
(config)# mac address-table aging-time <v_0_10_to_1000000>
(config)# no mac address-table aging-time
(config)# no mac address-table aging-time <v_0_10_to_1000000>
```

The Static MAC Address-Table can be configured, viewed, and cleared using the following syntax:

```
(config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface ( <port_type> [
```

```
<v_port_type_list> ] )
(config)# no mac address-table static <v_mac_addr> vlan <v_vlan_id>
interface ( <port_type> [ <v_port_type_list> ] )
# clear mac address-table
# show mac address-table [ conf | static | aging-time | { { learning |
count } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } | { address
<v_mac_addr> [ vlan <v_vlan_id> ] } | vlan <v_vlan_id_1> | interface (
<port_type> [ <v_port_type_list_1> ] ) ]
```

9.6.4 VLAN/PVLAN Commands

The following syntax can be used to configure the VLAN of Access Ports or Access VLANs. Ports in other modes are members of all VLANs specified in the Allowed VLANs field.

Private VLANs can be added or deleted. Port members of each Private VLAN can be added or removed.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

```
(config)# interface vlan <vlist>
(config)# vlan <vlist>
(config)# vlan ethertype s-custom-port <etype>
(config)# no interface vlan <vlist>
(config)# no vlan { { ethertype s-custom-port } | <vlan_list> }
# show interface vlan [ <vlist> ]
# show pvlan [ <pvlan_list> ]
# show pvlan isolation [ interface ( <port_type> [ <plist> ] ) ]
# show vlan [ id <vlan_list> | name <name> | brief ]
# show vlan status [ interface ( <port_type> [ <plist> ] ) ] [ combined |
admin | nas | mvr | voice-vlan | mstp | erps | vcl | evc | gvrp | all |
conflicts ]
```

9.6.5 IEEE Standard for Port-Based Network Access Control: dot1x

The IEEE 802.1X standard defines a port-based Access Control Procedure which prevents unauthorized access to a network by requiring Users to first submit credentials for authentication. One or more central servers and back-end servers determine whether the user is allowed to access the network.

The Network Access Control commands allow the User to enable or disable the NAS on the switch. If it is disabled, all ports are allowed frame forwarding.

The following command syntaxes can also be used to configure:

1. Time interval or/and check activity on successfully authenticated MAC addresses.

2. Re-authenticate interval for 802.1X-enabled ports to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

The re-authentication period will determine a time interval after which a connected client must be re-authenticated.

```
(config)# dot1x system-auth-control
```

```
(config)# dot1x re-authentication
(config)# dot1x authentication timer inactivity <v_10_to_100000>
(config)# dot1x authentication timer re-authenticate <v_1_to_3600>
(config)# dot1x timeout quiet-period <v_10_to_1000000>
(config)# dot1x timeout tx-period <v_1_to_65535>
(config)# no dot1x authentication timer inactivity
(config)# no dot1x authentication timer re-authenticate
(config)# no dot1x re-authentication
(config)# no dot1x system-auth-control
(config)# no dot1x timeout quiet-period
(config)# no dot1x timeout tx-period
# clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ]
) ]
# dot1x initialize [ interface ( <port_type> [ <plist> ] ) ]
# show dot1x statistics { eapol | radius | all } [ interface (
<port_type> [ <v_port_type_list> ] ) ]
# show dot1x status [ interface ( <port_type> [ <v_port_type_list> ] ) ]
[ brief ]
```

9.6.6 LACP Commands

LACP commands can be used to configure the aggregation ID, Partner ID, Partner Key and Priority of the Partner's Port. The status of the ID and the connectivity to the Partner Port can be viewed and cleared.

```
(config)# lacp system-priority <v_1_to_65535>
(config)# no lacp system-priority <v_1_to_65535>
# clear lacp statistics
# show lacp { internal | statistics | system-id | neighbour }
```

9.6.7 LLDP Commands

The following command syntaxes are used to configure the LLDP hold-time, the time taken to reinitialize LLDP after a shutdown, the time interval between each LLDP frame and the transmission delay to transmit the new LLDP frame due to some configuration changes.

```
(config)# lldp holdtime <val>
(config)# lldp reinit <val>
(config)# lldp timer <val>
(config)# lldp transmission-delay <val>
```

The `hold-time`, `reinit time`, `timer` and `transmission-delay` can be disabled using the following syntaxes:

```
(config)# no lldp holdtime
(config)# no lldp reinit
(config)# no lldp timer
(config)# no lldp transmission-delay
```

The following syntaxes can be used to view LLDP neighbors and view or clear the LLDP statistics.

```
# clear lldp statistics
# show lldp eee [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

```
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

9.6.8 Access Management Commands

The Switch will be allowed access only if the Application Type matches any one of the Access Management types.

The syntaxes below enable a User to configure the Access Management Table, where Access ID, Access VLAN ID, Start IP Address, End IP Address can be set. The commands can also be issued to define the WEB, SNMP or TELNET Interface from which the Host can access the Switch.

To accomplish this, the Host IP address must match the IP address entered in the syntax.

```
(config)# access management <access_id> <access_vid> <start_addr> [ to <end_addr> ] { [ web ] [ snmp] [ telnet ] | all }
(config)# no access management
(config)# no access management <access_id_list>
# clear access management statistics
# show access management [ statistics | <access_id_list> ]
```

9.6.9 Access-List Commands

The following command syntaxes can be used to set the Access List Ace ID, Rate Limiter in pps or kbps, disable or clear Access List statistics, and view Access List Ace status and statistics.

```
(config)# access-list ace <AceId : 1-256>
(config)# access-list rate-limiter [ <rate_limiter_list> ] { pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }
(config)# default access-list rate-limiter [ <rate_limiter_list> ]
(config)# no access-list ace <ace_list>
# clear access-list ace statistics
# show access-list [ interface [ ( <port_type> [ <v_port_type_list> ] ) ] ] [ rate-limiter [ <rate_limiter_list> ] ] [ ace statistics [ <ace_list> ] ]
# show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [ ptp ] [ upnp ] [ arp-inspection ] [ evc ] [ mep ] [ ipmc ] [ ip-source-guard ] [ ip-mgmt ] [ conflicts ] [ switch <switch_list> ]
```

9.6.10 Logging Commands

The following command syntaxes can be used to enable or disable server mode operations and to determine the kind of messages which can be sent to the Syslog Server.

The logging level must be set to privileges such as an Administrator to execute the command.

```
(config)# logging host <v_word45>
(config)# logging level { info | warning | error }
(config)# logging on
(config)# no logging host
(config)# no logging on
# clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
# show logging <log_id> [ switch <switch_list> ]
```

```
# show logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
```

9.6.11 Spanning Tree Commands

The User can enable or disable Spanning-Tree protocol mode to select:

- STP: Spanning Tree Protocol
- RSTP: Rapid Spanning Tree Protocol
- MSTP: Multiple Spanning Tree Protocol

The Spanning-Tree mode verifies whether a port explicitly configured as EDGE, will transmit and receive Bridge Protocol Data Unit (BPDUs) or disable itself upon reception of BPDUs.

In BPDU state a port enters the error-disabled state and is removed from the active topology. There is a time interval before the port can be enabled. To enable the port, a number of BPDU's a bridge port can send per second, must be set. If the number is exceeded, the transmission of the next BPDU will be delayed.

The following command syntaxes can be used to enable or disable Spanning Tree mode.

To set an interval time before a port in the error-disabled state can be enabled:

```
(config)# spanning-tree aggregation
(config)# spanning-tree mode { stp | rstp | mstp }
(config)# spanning-tree edge bpdu-filter
(config)# spanning-tree edge bpdu-guard
(config)# spanning-tree recovery interval <interval>
(config)# spanning-tree transmit hold-count <holdcount>
```

To disable the Spanning-Tree configurations, clear its statistics, and view the spanning-tree summary:

```
(config)# no spanning-tree edge bpdu-filter
(config)# no spanning-tree edge bpdu-guard
(config)# no spanning-tree mode
(config)# no spanning-tree recovery interval
(config)# no spanning-tree transmit hold-count
# clear spanning-tree { { statistics [ interface ( <port_type> [
<v_port_type_list> ] ) ] } | { detected-protocols [ interface (
<port_type> [ <v_port_type_list_1> ] ) ] } }
# show spanning-tree [ summary | active | { interface ( <port_type> [
<v_port_type_list> ] ) } | { detailed [ interface ( <port_type> [
<v_port_type_list_1> ] ) ] } | { mst [ configuration | { <instance> [
interface ( <port_type> [ <v_port_type_list_2> ] ) ] } ] } ]
```

9.6.12 Green-Ethernet Commands

Green Ethernet command syntaxes are used to configure and optimize LED power consumption. EEE is a power-saving option that reduces power usage when there is low or no traffic utilization. EEE works by powering down circuits when there is no traffic.

When a port receives data to be transmitted, all circuits are powered up. The time taken to power up the circuits is termed **wake-up time**.

The default **wake-up time** is 17us for 1 Gbit links and 30us for other link speeds.

EEE devices must agree upon the value of the **wake-up time** in order to ensure that both, the receiving and transmitting devices, have all circuits powered up when traffic is transmitted. When a port is powered down in **power-save** mode, outgoing traffic is stored in a buffer until the port is powered up again.

The following commands enable the Switch to optimize EEE devices for optimum power-saving mode and least traffic latency. They can be issued to set the interval at which the LED's intensity will reflect the corresponding intensity when the LED is **ON** or to set the interval to correspond to a specified intensity. If no intensity level is specified for the next hour, the intensity is set to the default level.

To set the interval at which the LED's intensity will correspond to a specified intensity:

```
(config)# green-ethernet eee optimize-for-power
(config)# green-ethernet led interval <v_0_to_24> intensity <v_0_to_100>
(config)# green-ethernet led on-event { [ link-change <v_0_to_65535> ] [
error ] }*1
```

The following commands can be issued to disable EEE optimizations for the LEDs and view the status of the Green-Ethernet LEDs.

```
(config)# no green-ethernet eee optimize-for-power
(config)# no green-ethernet led interval <0~24>
(config)# no green-ethernet led on-event [ link-change ] [ error ]
# show green-ethernet [ interface ( <port_type> [ <port_list> ] ) ]
# show green-ethernet eee [ interface ( <port_type> [ <port_list> ] ) ]
# show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]
# show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]
```

9.6.13 Thermal-Protect Commands

The following command syntaxes are used to configure the current settings for controlling thermal protection.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to reduce power consumption. It is possible to configure the ports with different priorities. Each priority can be specified at a temperature when the corresponding ports will be turned off.

```
(config)# no thermal-protect prio <prio_list>
(config)# thermal-protect prio <prio_list> temperature <new_temp>
# show thermal-protect [ interface ( <port_type> [ <port_list> ] ) ]
```

Loop-Protect Commands

The following command syntaxes are issued to inspect the current Loop Protection configurations, change, or set the interval between individual loop protection PDU sent on each port, set the period to disable a port in the event a loop is detected and shuts down the port.

```
(config)# loop-protect
(config)# loop-protect shutdown-time <t>
(config)# loop-protect transmit-time <t>
```

To disable loop protection for the ports and to view the `loop-protect` interface and its status:

```
(config)# no loop-protect
(config)# no loop-protect shutdown-time
(config)# no loop-protect transmit-time
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```

9.6.14 QoS Commands

To limit the QoS bandwidth for Unicast, Multicast or Broadcast messages, the receiving frame rate must be set.

To set the QCE ID which determines the QoS class, the following commands are used.

```
(config)# qos storm { unicast | multicast | broadcast } { { <rate> [ kfps ] } | { 1024 kfps } }
(config)# no qos qce <qce_id_range>
(config)# no qos storm { unicast | multicast | broadcast }
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps
```

```
[ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [
dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

9.6.15 Privilege Commands

The following Privilege commands are limited to the O/S implemented on the board.

Both, Linux and Windows CLI are Text-Based-User Interfaces and execute tasks based on similar CLI principles. However, though the command parameters and syntaxes are similar and perform the same functions on some levels, they differ in many ways.

Windows O/S emulates command line abilities through the Command Prompt or DOS Prompt to execute tasks. Linux CLI is Unix-based and consists of a more extensive range of commands than Windows because the shell is the primary interface.

```
(config)# privilege { exec | configure | config-vlan | line | interface |
if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-
profile } level <privilege> <cmd>
(config)# no privilege { exec | configure | config-vlan | line |
interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool |
rfc2544-profile } level <0-15> <cmd>
# show privilege
```

9.6.16 SNMP Commands

The following command syntaxes are used to enable SNMP or to enable or disable the Trap mode, set the Version, Group Name and the Security modes.

The Read and Write access strings to permit access to the SNMP Agent can be set for SNMPv1 or SNMPv2c versions.

For SNMPv3 the community string will be associated with the SNMPv3 Communities Table.

For SNMPv3 User configuration, the commands will include the User-Name, Engine ID, Authentication Protocol: privacy protocol and password.

NOTE: Changing the Engine ID will clear all original Local Users from the system.

```
(config)# snmp-server
(config)# snmp-server version { v1 | v2c | v3 }
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name
<security_name> group <group_name>
(config)# snmp-server access <group_name> model { v1 | v2c | v3 | any }
level { auth | noauth | priv } [ read <view_name> ] [ write <write_name>
]
(config)# snmp-server community v2c <comm> [ ro | rw ]
(config)# snmp-server community v3 <v3_comm> [ <v_ipv4_addr>
<v_ipv4_netmask> ]
(config)# snmp-server contact <v_line255>
(config)# snmp-server engine-id local <engineID>
(config)# snmp-server host <conf_name>
(config)# snmp-server location <v_line255>
(config)# snmp-server trap
(config)# snmp-server user <username> engine-id <engineID> [ { md5
```

```
<md5_passwd> | sha <sha_passwd> } [ priv { des | aes } <priv_passwd> ] ]
(config)# snmp-server view <view_name> <oid_subtree> { include | exclude
}
```

To view or disable the set SNMP server settings:

```
(config)# no snmp-server
(config)# no snmp-server version
(config)# no snmp-server security-to-group model { v1 | v2c | v3 } name
<security_name>
(config)# no snmp-server access <group_name> model { v1 | v2c | v3 | any
} level { auth | noauth | priv }
(config)# no snmp-server community v2c
(config)# no snmp-server community v3 <community>
(config)# no snmp-server contact
(config)# no snmp-server engined-id local
(config)# no snmp-server host <conf_name>
(config)# no snmp-server location
(config)# no snmp-server trap
(config)# no snmp-server user <username> engine-id <engineID>
(config)# no snmp-server view <view_name> <oid_subtree>
# show snmp
# show snmp access [ <group_name> { v1 | v2c | v3 | any } { auth | noauth
| priv } ]
# show snmp community v3 [ <community> ]
# show snmp host [ <conf_name> ] [ system ] [ switch ] [ interface ] [
aaa ]
# show snmp mib context
# show snmp mib ifmib ifIndex
# show snmp security-to-group [ { v1 | v2c | v3 } <security_name> ]
# show snmp user [ <username> <engineID> ]
# show snmp view [ <view_name> <oid_subtree> ]
```

9.6.17 SNTP Commands

The following command syntaxes are used to enable or disable the SNTP Client mode operation and set the IPv4 or IPv6 address of a SNTP server.

```
(config)# sntp
(config)# sntp server ip-address { <ipv4_var> }
(config)# no sntp
(config)# no sntp server
# show sntp status
```

9.6.18 Radius Server Commands

The following command syntaxes are used to configure the NAS-IP-Address: Attribute 4 and NAS-Identifier: Attribute 32 Configurability features.

The IPv4 address is used as Attribute 4 in RADIUS Access-Request packets. The Identifier-up to 253-character long is used as an Attribute 32 in RADIUS Access-Request packets.

A Global Secret Key, which is shared between the RADIUS server and the Switch, can be set.

Other options that can be configured are:

- Global Timeout to wait for a reply from the RADIUS server before re-transmitting the request.
- Global Retransmit number for which RADIUS request is sent to a server that has stopped responding.
- Dead Time Interval for which no new RADIUS requests are sent to a server that has failed to respond to previous requests.

NOTE: Setting the **deadtime** will stop the Switch from continually trying to contact a server that has been determined to be dead.

```
(config)# radius-server attribute 32 <id>
(config)# radius-server attribute 4 <ipv4>
(config)# radius-server key <key>
(config)# radius-server retransmit <retries>
(config)# radius-server timeout <seconds>
(config)# radius-server deadtime <minutes>
```

The following syntaxes are used to set the IP address of the RADIUS server and instruct the UDP port to authenticate the RADIUS server. The commands execute the following functions:

- Authentication and accounting
- Setting optional `timeout`
- Setting optional `retransmit`
- Setting the Global Key

NOTE: Setting **retransmit** and optional key overrides the global time out, global retransmit number and global key.

```
(config)# radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port>] [ timeout <seconds> ] [ retransmit <retries> ] [ key <key> ]
```

The following command syntaxes can be used to view the RADIUS server running status and statistics, and disable all RADIUS server settings.

```
(config)# no radius-server attribute 32
(config)# no radius-server attribute 4
(config)# no radius-server deadtime
(config)# no radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ]
(config)# no radius-server key
(config)# no radius-server retransmit
(config)# no radius-server timeout
# show radius-server [ statistics ]
# show running-config [ all-defaults ]
# show running-config feature <feature_name> [ all-defaults ]
# show running-config interface ( <port_type> [ <list> ] ) [ all-defaults ]
# show running-config interface vlan <list> [ all-defaults ]
# show running-config line { console | vty } <list> [ all-defaults ]
# show running-config vlan <list> [ all-defaults ]
```

9.6.19 Banner Commands

A Banner is a message presented to a User and can be configured when the message is displayed.

It can be defined before and after Login using the following commands:

```
(config)# banner [ motd ] <banner>
(config)# banner exec <banner>
(config)# banner login <banner>
(config)# no banner [ motd ]
(config)# no banner exec
(config)# no banner login
```

9.6.20 Terminal Commands

The following commands are generic Terminal syntaxes that are issued to set or modify Terminal settings.

```
(config)# no terminal editing
(config)# no terminal exec-timeout
(config)# no terminal history size
(config)# no terminal length
(config)# no terminal width
# terminal editing
# terminal exec-timeout <min> [ <sec> ]
# terminal help
# terminal history size <history_size>
# terminal length <lines>
# terminal width <width>
```

9.6.21 Reload Command

Use the following syntax to Restore defaults or Reset system settings:

```
reload { { { cold | warm } [ sid <usid> ] } | { defaults [ keep-ip ] } }
```

9.6.22 Firmware Commands

The following command syntaxes can be used to upgrade the firmware from a given FTP server path and to swap the actual and backup firmware images.

```
# firmware swap
# firmware upgrade <tftpserver_path_file>
```

9.6.23 Ping Commands

The following syntax is used to ping the device.

```
# ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval
<seconds> ]
```

9.6.24 Debug Commands

The following syntaxes are used to debug the board.

```
(config)# no debug prompt
(config)# line { <0~16> | console 0 | vty <0~15> }
# no debug prompt
# debug prompt <debug_prompt>
```

9.6.25 Security Commands

The following command syntaxes are used to:

- Encrypt or decrypt the password. Set the password to **NONE**.
- Enable or disable **AAA** authentication on Console, Telnet, SSH or HTTP Logins.
- Enable or disable the execution level of the password.

```
(config)# password encrypted <encry_password>
(config)# password none
(config)# password unencrypted <password>
(config)# aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [ { local | radius | tacacs } [ { local | radius | tacacs } ] ] }
(config)# enable password [ level <priv> ] <password>
(config)# enable secret { 0 | 5 } [ level <priv> ] <password>
(config)# no aaa authentication login { console | telnet | ssh | http }
(config)# no enable password [ level <priv> ]
(config)# no enable secret { [ 0 | 5 ] } [ level <priv> ]
# show aaa
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

9.6.26 Monitor Commands

The following command syntaxes are used to configure the monitor destination interface and the source ports.

```
(config)# monitor destination interface <port_type> <in_port_type>
(config)# monitor source { { interface ( <port_type> [ <v_port_type_list> ] ) } | { cpu [<cpu_switch_range> ] } } { both | rx | tx }
(config)# no monitor destination
(config)# no monitor source { { interface ( <port_type> [ <v_port_type_list> ] ) } | { cpu [ <cpu_switch_range> ] } }
```

9.6.27 POE Commands

By default, the EPS-24G4X Carrier Board in SabreNet 2400 does not support Power over Ethernet (POE) networking features. However, the Board is POE-enabled which can be implemented via a POE Switch.

The Power Management mode and the Reserved Power for Power over Ethernet (POE) can be set using the following command syntaxes.

To determine the range of power a port may use, the User must define the amount of power a power source can deliver. The values range from 0 to 2000 watts.

```
(config)# poe management mode { class-consumption | class-reserved-power | allocation-consumption | allocation-reserved-power | lldp-consumption | lldp-reserved-power }
(config)# poe supply sid <v_1_to_24> <v_1_to_2000>
(config)# no poe management mode
```

```
(config)# no poe supply [ sid <v_1_to_24> ]
# show poe [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

9.7 Command Parameter and Syntax Examples

9.7.1 IP Configuration

The following block depicts the configuration of a static IP address.

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.1.60 255.255.0.0
(config-if-vlan)# end
```

The following block confirms the IP address that has been entered.

```
# show ip interface brief
Vlan Address              Method   Status
---- -------------------- -------- ------
   1 192.168.1.60         Manual   UP
#
```

9.7.2 Port Configuration

Individual ports can be configured at different speeds. The following example depicts the speed configured at 100 Mbps for port 1.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# speed ?
      10             10Mbps
   100            100Mbps
   1000           1Gbps
   auto           Auto negotiation
(config-if)# speed 100
(config-if)# end #
```

9.7.3 Changing the Switch Password

The following block depicts the syntax to create a new password.

```
# configure terminal
(config)# password unencrypted <password>
(config)# exit #
```

9.7.4 Setting Up VLANs

Virtual LANs (VLANs) are used to divide the network into separate logical areas. VLANs can also be considered as broadcast domains.

The following example depicts **VLAN2** and **VLAN3** set up with switch port mode set to **Access**.

```
#configure terminal
(config)# vlan 2
(config)# vlan 3
```

Setting the Access Port

In the following example, it is assumed that Ports 1~3 are connected to the PC and the PVID of each port is different.

```
#configure terminal
(config)# interface GigabitEthernet 1/2
(Config-if)# switchport mode access
(Config-if)# switchport access vlan 2
(config)# exit
(config)# interface GigabitEthernet 1/3
(Config-if)# switchport mode access
(Config-if)# switchport access vlan 3
(config)# exit #
```

Verifying VLAN Settings

The following example depicts the verification of a created **VLAN**:

```
# show vlan
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/1,4-8
2     VLAN0002                          Gi 1/2
3     VLAN0003                          Gi 1/3
```

In the above example, **VLAN 2** is created with the ID **VLAN0002** and Port 2 is assigned to **VLAN 2**.

Similarly, Port **3** is assigned to **VLAN0003**. The remaining Ports **1** and **4** to **8** are assigned to **VLAN 1** by default.

9.7.5 SNMP Configuration

The following block depicts the SNMP configuration.

To enable the SNMP mode operation:

```
# configure terminal
(config)# snmp-server
(config)# exit #
```

To configure the SNMP Trap:

```
# configure terminal
(config)# snmp-server host Example
(config-snmp-host)# host 192.168.1.20
(config-snmp-host)# exit
(config)# exit #
```

9.7.6 Mirroring Network Traffic

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port.

The following block depicts mirroring of **Port 2**, **Port 3** (RX), and **Port 4** traffic through **Port 8** (RX) to **Port 1**.

```
# configure terminal
(config)# monitor destination interface GigabitEthernet 1/1
(config)# monitor source interface GigabitEthernet 1/2-3 rx
(config)# monitor source interface GigabitEthernet 1/4-8 tx
```

9.7.7 Setting Up QoS

Quality of Service (QoS) refers to the capability of a network to provide optimum services to selected network traffic using various technologies including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet, 802.1 networks, SONET, and other IP-routed networks that may use any or all these underlying technologies.

The following block shows the syntaxes to setup a QoS.

In the following example, all traffic routed on **Port 1** is mapped to `QoS,` Class `CoS 2` with PCP set to **1**.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# qos cos 2
(config-if)# qos pcp 1
(config-if)# end #
```

9.7.8 Upgrading the Firmware

Use this method only if Web interface is not up. Otherwise, use web interface to upgrade the firmware. A new IStaX image can be downloaded using the following CLI parameters. To do so:

Copy the `dsc-epsm10gx4-istax2022.06-v2.0.0.dat` file to a TFTP server and use the Firmware Upgrade command to download the file using the syntax shown below.

```
# firmware upgrade tftp://<ip_address>/<path>/ dsc-epsm10gx4-
istax2022.06-v2.0.0.dat#
```

IstaX image files are suffixed with **.mfi** file extension format. To download an IstaX image:

Copy the `dsc-epsm10gx4-istax2022.06-v2.0.0.mfi` file to a TFTP server and use the Firmware Upgrade command to download the file using the syntax shown below.

```
# firmware upgrade tftp://<ip_address>/<path>/ dsc-epsm10gx4-
istax2022.06-v2.0.0.mfi
```

9.7.9 Board Detail Commands

The User can verify Board details such as the Type and Software Version by entering the syntax shown below.

```
# show board
# show version
```

10. USING THE WEB INTERFACE

The following functions can be performed when using the Web Interface:

- Set Port Mode
- Enable/disable Flow Control
- Configure Simple Port-Based VLAN
- Configure Aggregation Groups
- Configure LACP Parameters
- Configure QoS
- Mirror Network Traffic and Frames
- Read and Clear Statistics Counters
- Monitor LACP Status
- Configure and Monitor 802.1X
- Configure and Monitor IGMP Snooping
- Configure source-IP Address and DHCP Server Filter
- Upgrade the Software

The GUI screens will interchange depending upon the number of connected ports.

The Screen below displays the Web Interface for the SabreNet 24000 Board which is equipped with 28 ports.

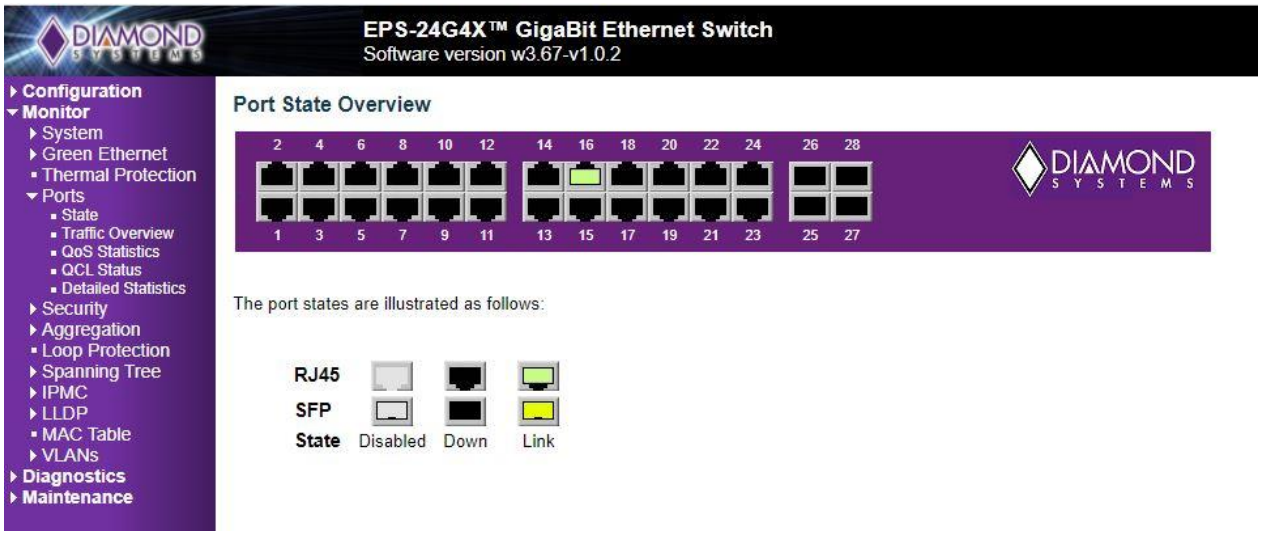


Figure 10-1: SabreNet 24000 Carrier Board Home Page

10.1 Web Interface Configuration Examples

10.1.1 IP Configuration

To configure the IP address of the Switch:

1. Connect SabreNet 24000 to the Web Interface.
2. Navigate to **Configuration** -> **System** -> **IP screen.**
3. Modify the IP Address in the **IPv4 Address** column.
4. Click the **Save button.**
5. Navigate to **Maintenance** -> **Configuration** -> **Save Startup-Config** and select the **Save Configuration button.**

The IP Configuration Screen is depicted below.

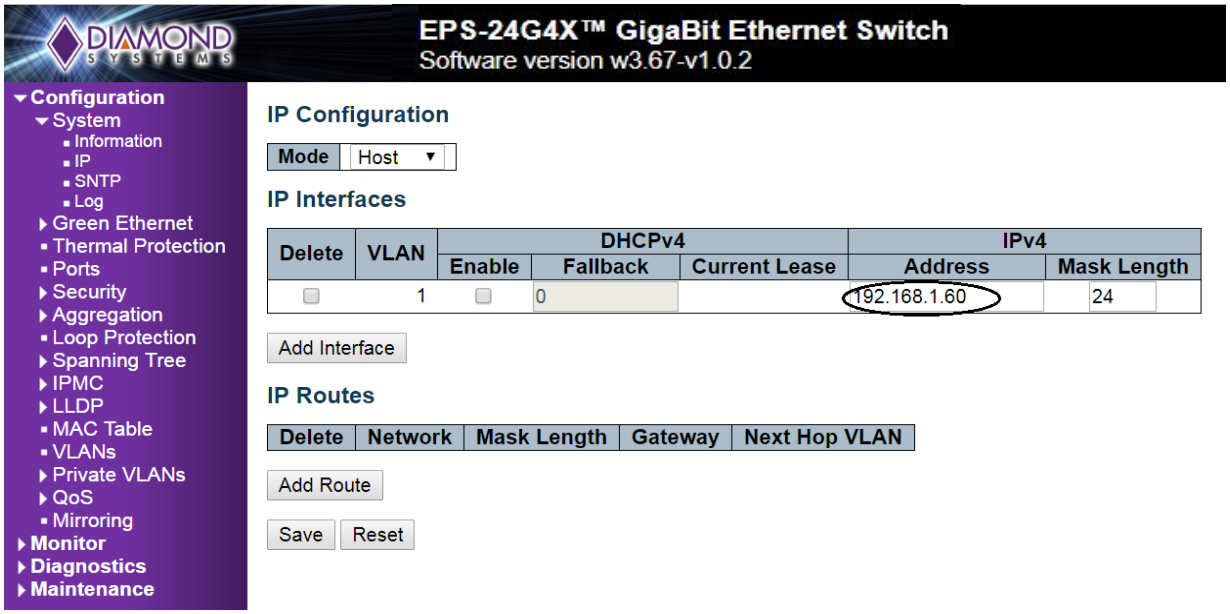


Figure 10-2: IP Configuration Screen

10.1.2 Port Configuration

To configure Individual ports:

6. Connect SabreNet 24000 Switch to the Web Interface.
7. Navigate to **Configuration** -> **Ports screen.**

Each port can be set to one of the following configurations:

Disabled	Forces the cu Port in 10 Mbps Half-duplex Mode
Auto	Forces the cu Port in 10 Mbps Full-duplex Mode
10 Mbps HDX	Forces the cu Port in 100 Mbps Half-duplex Mode
10 Mbps FDX	Forces the cu Port in 100 Mbps Full-duplex Mode

100 Mbps HDX	Forces the Port in 1G bps Full-duplex Mode
100 Mbps FDX	Forces the cu Port in 10 Mbps Half-duplex Mode
1 Gbps FDX	Forces the cu port in 10 Mbps Full-duplex Mode

8. Once the port has been configured, click the **Save button.**

To save the settings permanently:

9. Navigate to **Maintenance** -> **Configuration** -> **Save Startup-Config** page and click **Save Startup Configuration button.**

The IP Configuration Screen is depicted below.

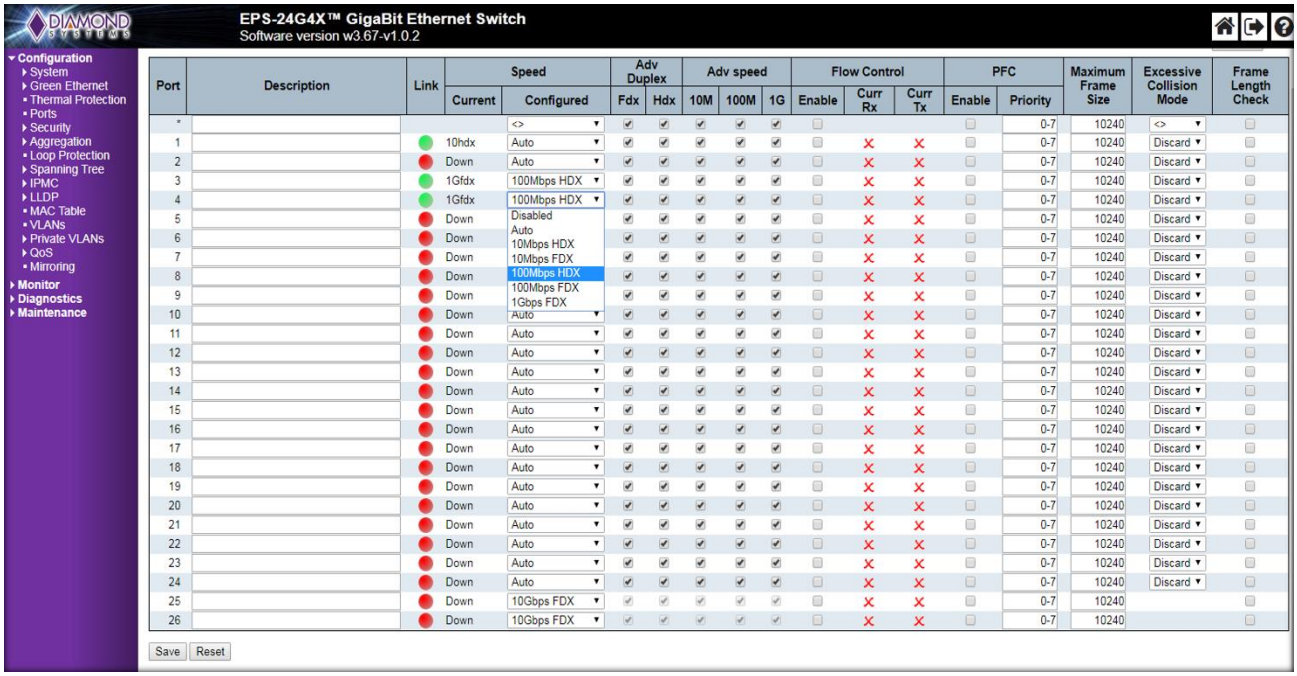


Figure 10-3: Port Configuration Screen

10.1.3 Changing the System Password

To change the system login password:

1. Connect SabreNet 24000 to the Web Interface.
2. Navigate to **Configuration** -> **Security** ->**Switch** -> **Password screen.**
3. Enter the **Old Password** and **New Password** in the designated fields and click the **Save button**.
4. Navigate to **Maintenance** -> **Configuration** -> **Save Startup-Config** and click the **Save Configuration button.**

The System Password Screen is depicted below.

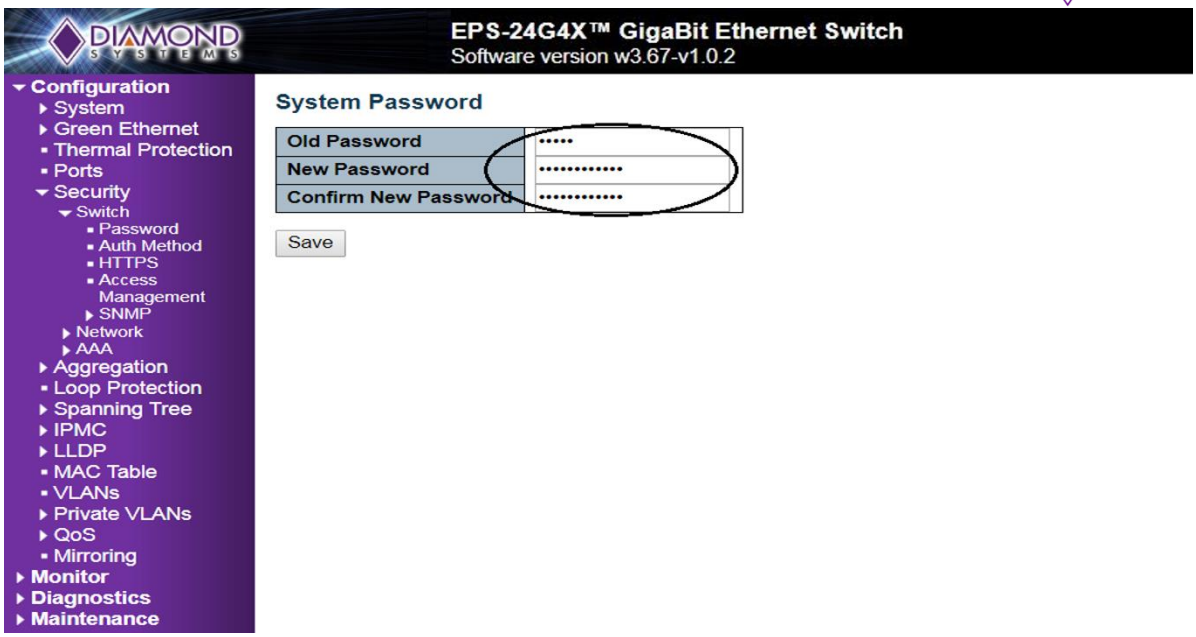


Figure 10-4: Changing the System Password

10.1.4 VLAN Configuration

The following example describes how to configure a VLAN.

1. Connect SabreNet 24000 Switch to the Web Interface.
2. Navigate to **Configuration** -> **VLANs page.**
3. In the **Allowed Access VLANs** field, enter the number of LANs to be created.

In the following example **VLANs, 1-3** have been reassigned as **VLAN 2** and **VLAN 3**.

By default, the **Mode** field **Access** can be changed to **Trunk** or **Hybrid** using the **Mode** drop-down list.

Ports can be assigned to Virtual LANs by changing the values in the **Port VLAN** column.

4. Click the **Save** button to save the VLAN configuration.

To save VLAN settings permanently:

5. Navigate to **Maintenance** -> **Configuration** -> **Save Startup-Config** page.
6. Click the **Save Startup Configuration button.**

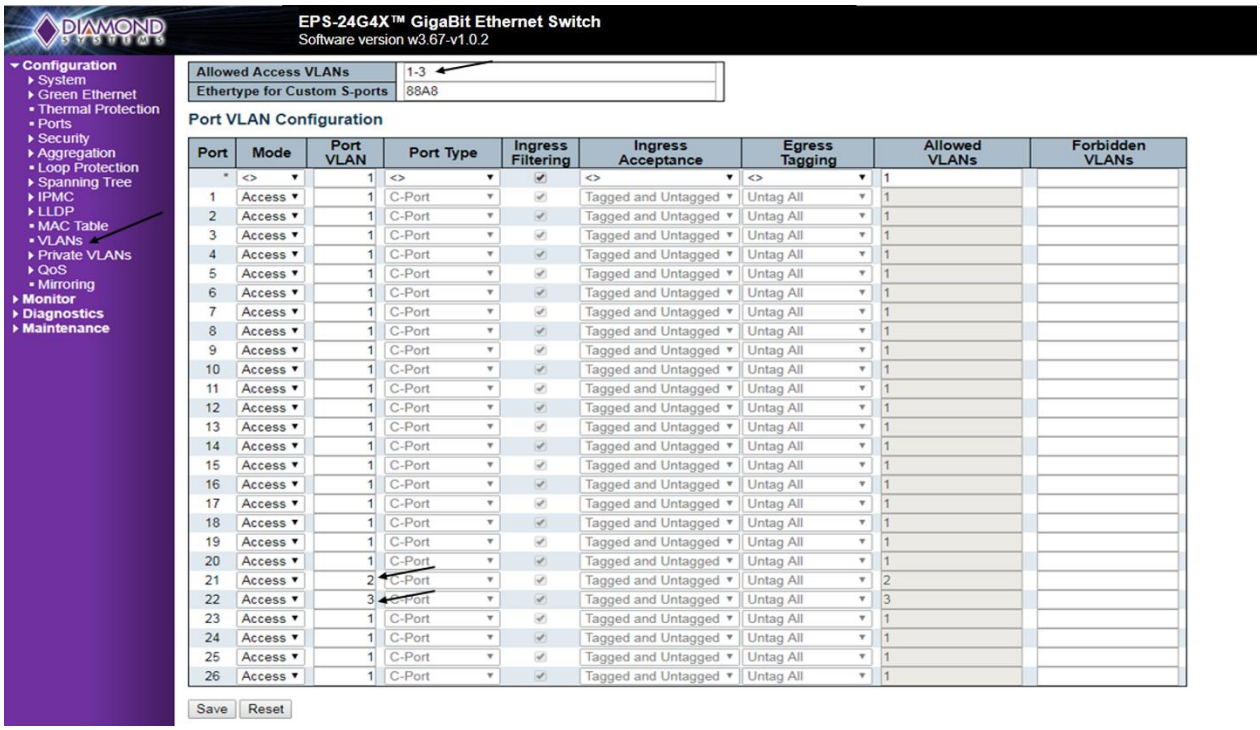


Figure 10-5: VLAN Setup Screen

After saving the VLAN configuration, the VLAN Membership status can be verified as shown in the screen below.

To verify:

1. Navigate to **Monitor** -> **VLANs** -> **Membership** page.
2. Confirm the settings.

In the following screen:

Ports **1** to **20** and **23** to **26** are assigned to **VLAN ID 1**. **Port 21** is assigned to **VLAN ID 2** and **Port 22** is assigned to **VLAN ID 3**.

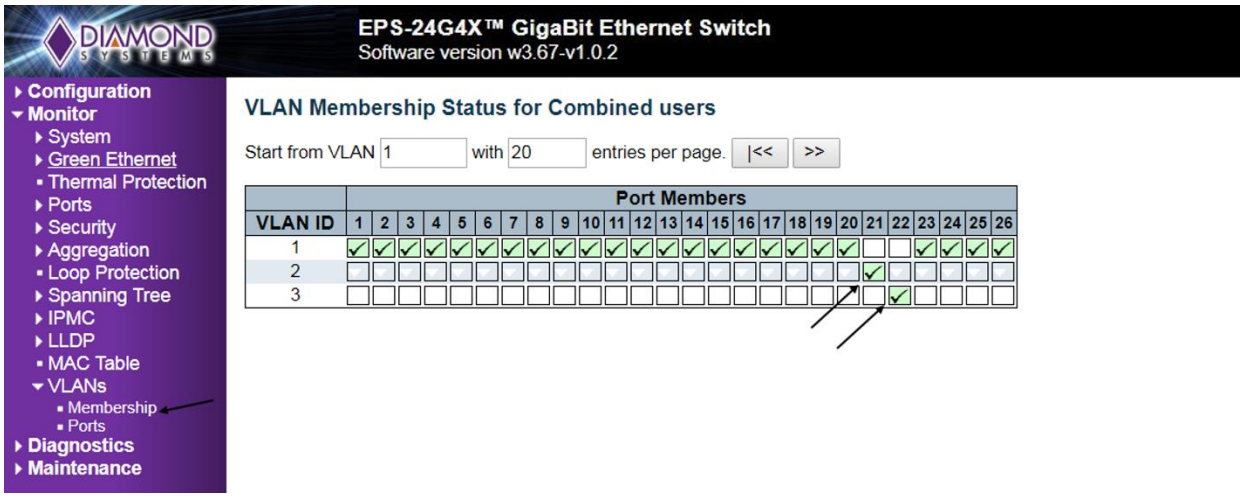


Figure 10-6: VLAN Membership Verification Screen

10.1.5 Mirroring Frames Configuration

For debugging network problems or monitoring network traffic, the Switch system can be configured to mirror frames from multiple ports to a mirror port.

The following example shows how to mirror the traffic of **Port 1 Tx only** and **2 Rx only** to **Port 6**.

1. Connect SabreNet 24000 Switch to the Web Interface.
2. Navigate to **Configuration** -> **Mirroring page.**
3. Click -> **Save** to save the mirroring configuration.

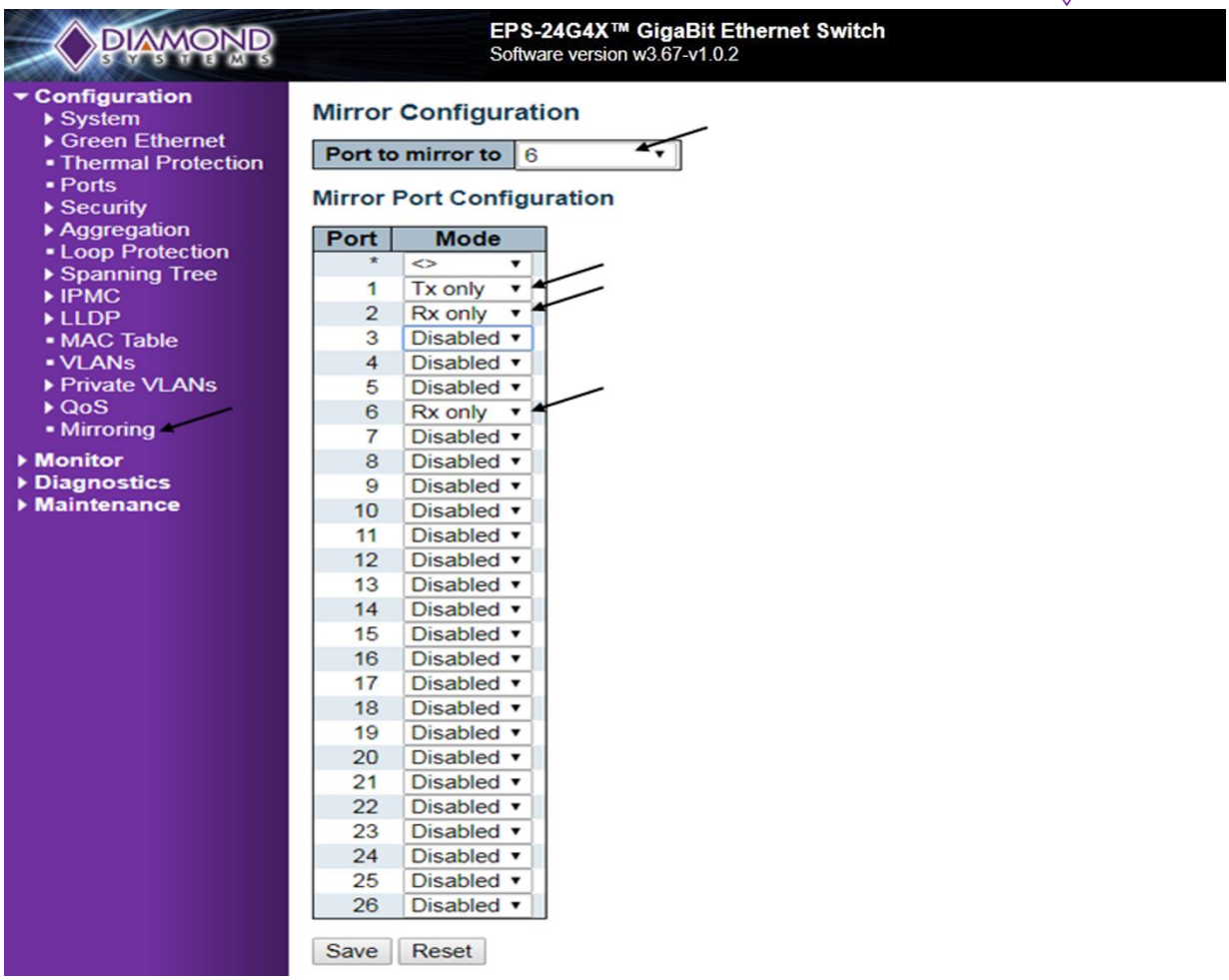


Figure 10-7: Mirror Frames Screen

Other Mirroring Options

The port which displays mirroring data is known as the Mirror Port. Frames from ports that have either source **RX** or destination **TX** mirroring enabled are mirrored on this port. The button **Disabled** disables mirroring functions.

Mirror Mode Description

1. **RX only** - Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

2. **TX only** - Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

3. **Disabled** - Neither frames transmitted nor frames received are mirrored.

4. **Enabled** - Frames received and transmitted are mirrored on the mirror port.

10.1.6 QoS Classification Configuration

Basic QoS classification configuration can be set per port. Ingress traffic coming on each port can be assigned to a QoS class: **CoS**, **PCP**, **DPL,** and **DEI**.

The following example depicts the QoS ingress port classification where all traffic routed on **Port 3** are mapped to **Cos 4** and **PCP** is set as **1**.

1. Navigate to **Configuration** -> **QoS** -> **Port Classification page**.

2. Under **CoS in Port** row **3** select **4** from the drop-down list.

3. Under **PCP** select **1** from the drop-down list.

4. Click the **Save button.**

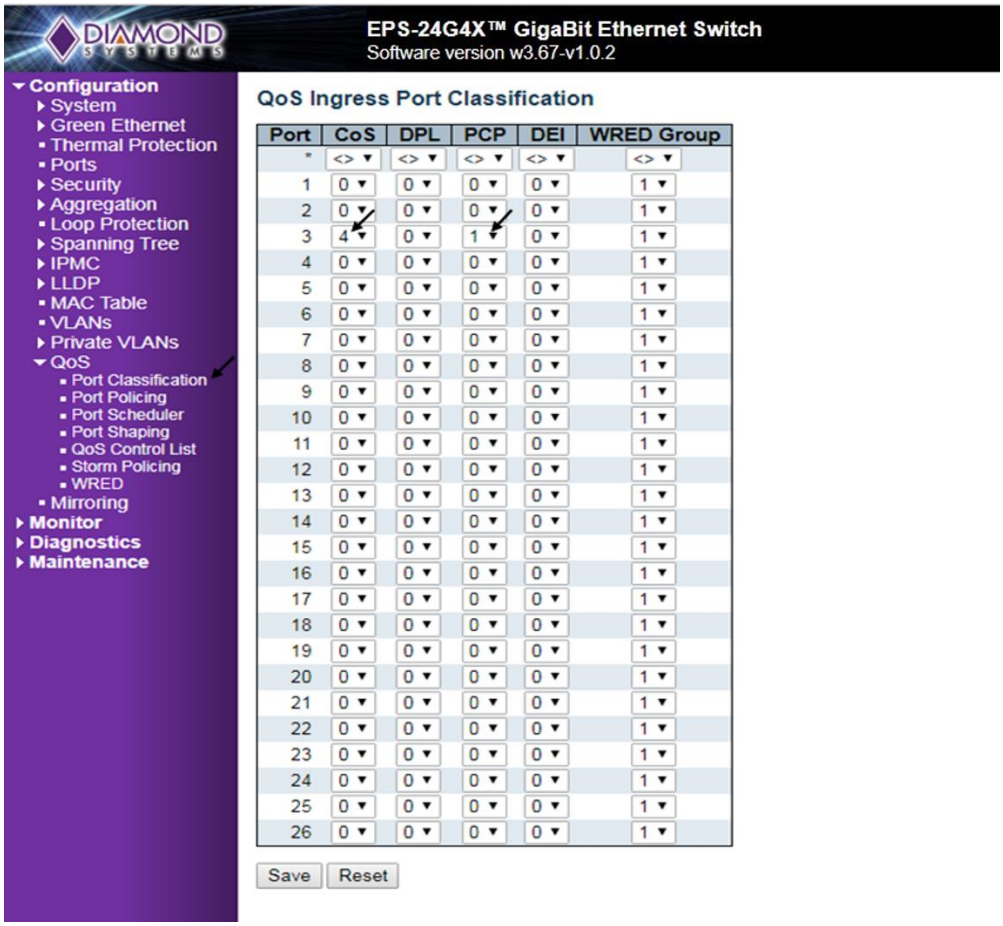


Figure 10-8: QoS Classification Screen

10.1.7 Web Interface Activation/Deactivation

Web access to the Web Interface can be activated and deactivated either through Command Line Interface or the Web Control Panel.

Using the Web Control Panel:

1. Navigate to the **Configuration** screen.
2. Select **Security** -> **Switch** -> **Access Management Configuration**.
3. Ensure the **Mode** is set to **Disabled which is** the default mode.

If it is not **Disabled**, select **Disabled** from the drop-down option.

4. Click the **Save button**.

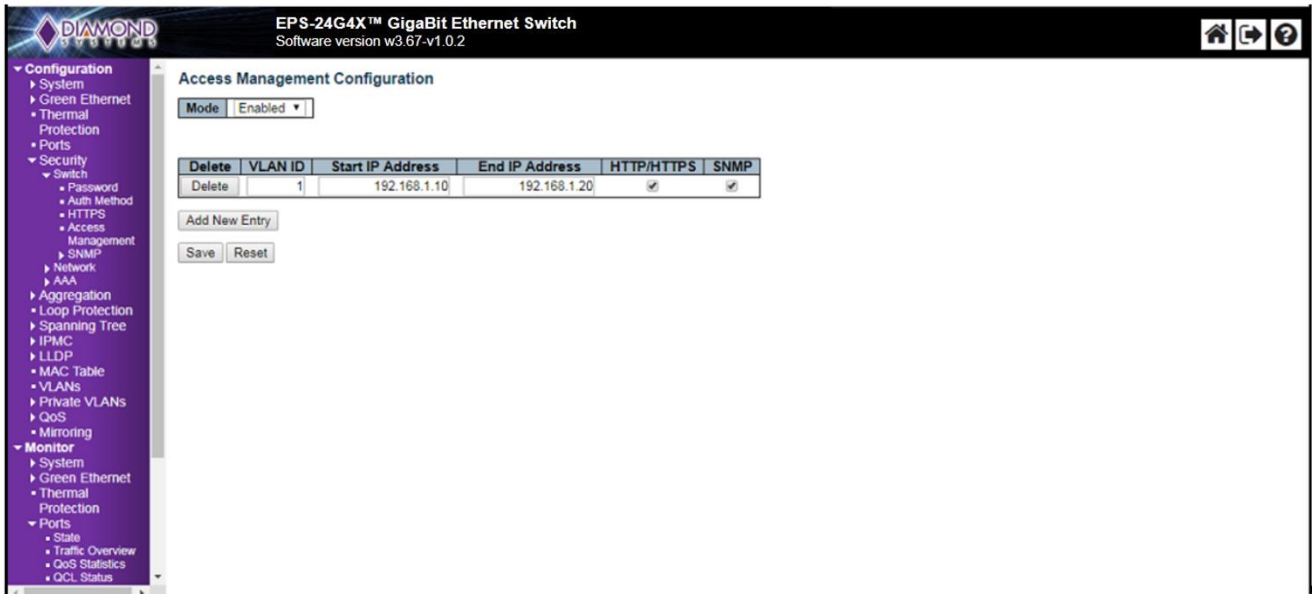


Figure 10-9: Activation/Deactivation Screen

This configuration should be stored on the Switch with the following CLI syntax:

```
#copy startup-config flash:{filename}
```

To disable Web access on the Switch, in the Control Panel:

5. Navigate to **Configuration** -> **Security** -> **Switch** -> **Access Management Configuration** screen.
6. Change the mode to **Enabled**.
7. Click the **Save** button.

This disables access to the Switch using the Web Interface.

Using the CLI Interface:

To store this command as the standard configuration on Flash memory to enable it to load on startup, enter the following syntax in the CLI:

```
#copy running-config startup-config
```

To enable Web access on the Switch, enter the following syntax in CLI:

```
#copy startup-config flash:backup_config
#copy flash:{filename} startup-config
```

Reboot the Switch.

10.1.8 Firmware Upgrade

The following section describes the steps for upgrading the firmware.

1. Connect SabreNet 24000 Switch to the Web Interface and navigate to **Maintenance** -> **Software** -> **Upload** page.

2. Choose the file to be uploaded(.dat) and click -> **Upload**.

The existing firmware will be erased and upgraded with the new firmware version.

When the upgrade is complete the Switch will automatically reboot.

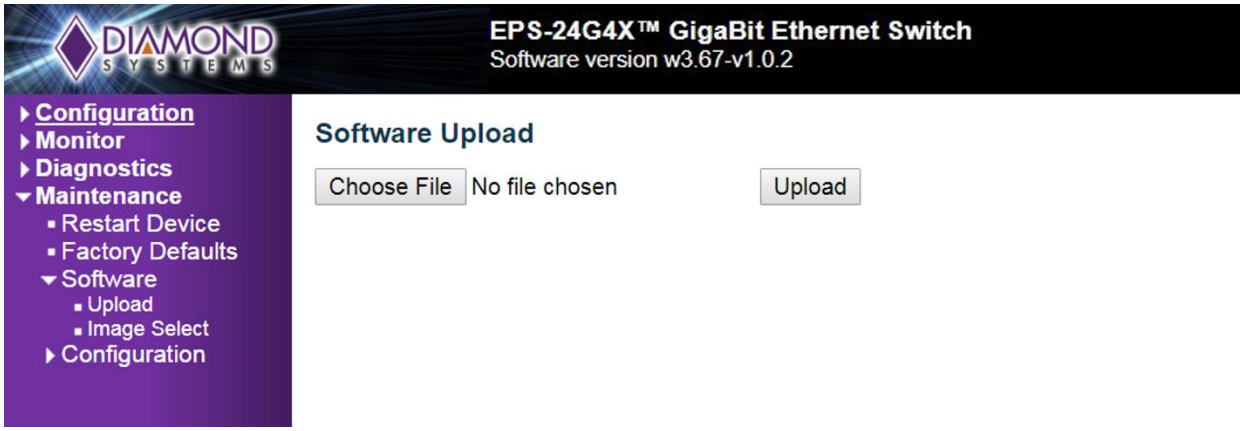


Figure 10-10: Firmware Upload Screen

10.1.9 Saving the Startup Configuration

To ensure that the currently active startup configuration will be executed at the next reboot, the command parameters `running-config` to `startup-config` must be copied and saved.

To save the file:

1. Connect SabreNet 24000 Switch to the Web Interface.

2. Navigate to **Maintenance** -> **Configuration** -> **Save Startup-Config** page.

3. Click the **Save Configuration** button.

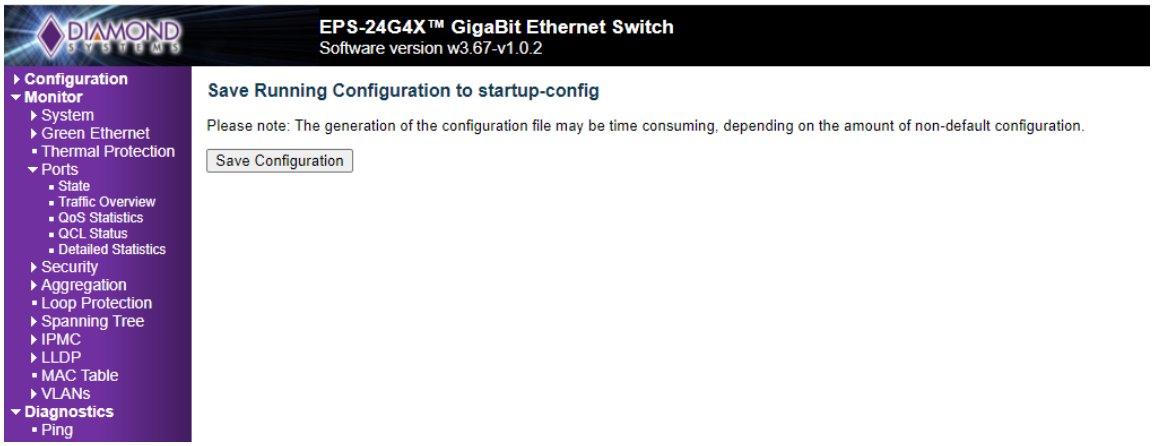


Figure 10-11: Uploading and Saving Startup Configuration Screen

10.1.10 Factory Default Settings

The user can reset the configuration of the Switch to factory defaults on the screen page depicted below.

Only the IP configuration is retained. The new configuration is executed instantly.

The following steps describe resetting the system to factory defaults:

1. Connect SABRENET-24000 Switch to the Web Interface.
2. Navigate to **Maintenance** -> **Factory Defaults** page.
3. Click the **Yes** button.

A confirmation message will be displayed as shown below.

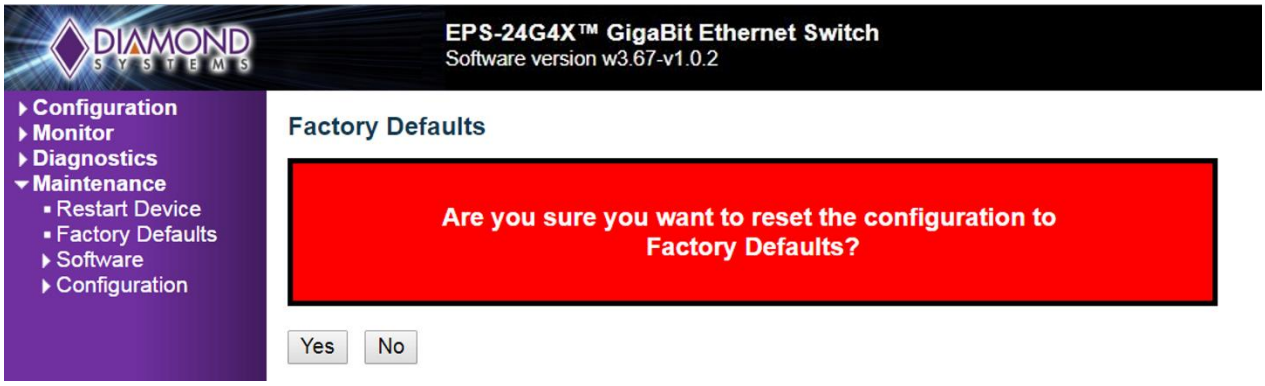
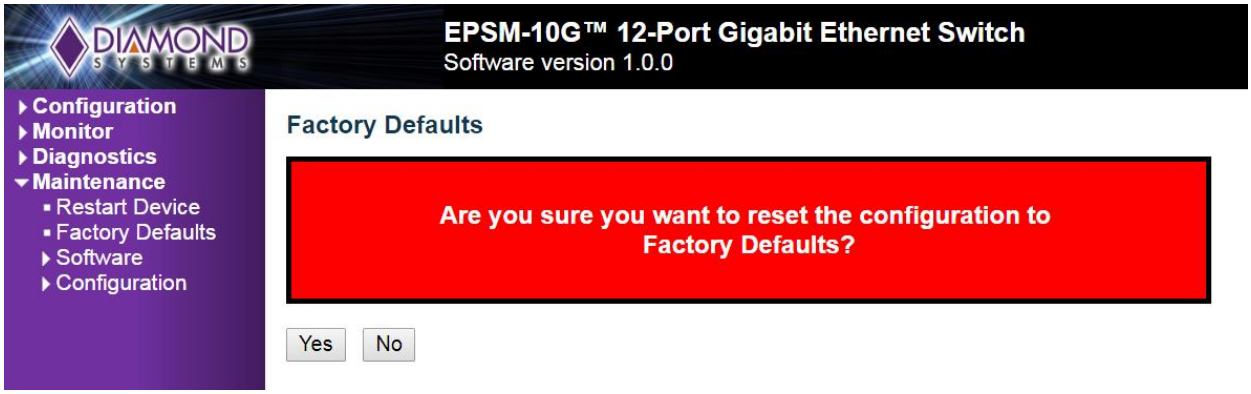


Figure 10-12: Resetting Switch to Factory Defaults Screen

11. FACTORY DEFAULTS

The user can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately. The following procedure describes the steps for resetting the factory defaults:

1. Connect to the web interface of SabreNet 24000, it uses EPSM-10GX
2. Navigate to maintenance -> Factory defaults
3. Click on Yes for a confirmation message



12. SOFTWARE FEATURE LIST

Switch Type	24 port Layer 2+ switch
Number of Ports	24 10/100/1000Mbps Ethernet ports with non-blocking wire-speed performance
On-board Memory	4Mb packet memory Shared memory buffer with per-port & CoS memory management
MEF	Hierarchical MEF compliant policing & scheduling MEF E-Lane, E-Line, and E-Tree services
Frame Buffer	Jumbo frame support at all speeds
VLAN	IEEE 802.1Q VLAN switch with 8K MACs and 4K VLANs Push/pop up to two VLAN tags Independent & shared VLAN learning (IVL, SVL)
Multicast	IPv4 and IPv6 multicast group support
Remarking	Dual leaky bucket policers with remarking and statistics
Classifier	8 priorities and 8 CoS queues per port with strict or deficit-weighted round robin scheduling Shaping/policing per queue and per port
Storm Control	Policing with storm control and MC/BC protection
Link Aggregation	IEEE 802.3ad
Security	Advanced security and prioritization available through multistage TCAM engine
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1W) and MSTP
MIBs	Support for both WebStax and IStaX MIBs
Power Management	ActiPHY and PerfectReach power management VeriPHY cable diagnostics
Serial Port	1 RS-232 port for host interface
Standalone Capable	Standalone network switch, or in combination with a host computer