# EPS-12002L Ethernet Switch

## User Manual

Revision 1.3

**FOR TECHNICAL SUPPORT**
**PLEASE CONTACT:**

**Site: www.diamondsystems.com/support/**

**Email: support@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*

Diamond Systems' Boards are designed with complex circuitry and electronic components that are ESD-sensitive. This increases the likelihood of the boards incurring accidental damage during handling, installation, and connection to other equipment.

It is highly recommended that the following precautionary measures and best practices be observed in sequential order:

- Wear an anti-static Wristband/Strap or/and an antistatic Lab Coat or/and Rubber-soled shoes.
- Spread anti-static mats over the table or work surface or/and anti-static mats on the floor.
- Unpack components and remove them from their antistatic bags only when they are ready to be used.
- Avoid ungrounded surfaces such as plastic, carpets, floors, or tables, in the work area.
- Handle boards by the edges and the metal mounting brackets. Avoid touching components on the boards and the edge connectors that connect to expansion slots.

The following information describes common causes of failure found on boards and components returned to Diamond Systems for repair. It is provided as a guideline to avoid accidental damage.

**ESD Damage**: This type of damage is typically impossible to detect because there is no visual sign of failure or damage. In this type of damage, the board eventually stops working because of some defective components. 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.

**Damage During Handling or Storage**: Physical damage on boards also occur due to mishandling. A common observation is that of a screwdriver slipping on the board during installation, causing a gouge on the PCB surface, cutting signal traces or damaging components.

Another common observation are damaged board corners, indicating the board was dropped. This may or may not cause damage to the circuitry, depending on components located near the edges. Most DSC boards are designed with a minimum of 25 mils clearance between the board edge and component pad. The ground/power planes are located a minimum of 20 mils from the edge to avoid possible shorting from this type of damage. However, these design rules do not prevent damage in all situations.

Sometimes boards are stored in racks with slots that grip the edge of the board. This is a common practice for board manufacturers. Though our boards are resilient to damages, the components located close to the board edges can be damaged or even knocked off the board if the board lies tilted in the rack.

Diamond Systems recommends that all our boards be stored only in individual ESD-safe packaging units. If multiple boards are stored together, they should be contained in bins with dividers placed between the boards. Do not pile boards on top of each other or cram too many boards within a small location. This can cause damage to connector pins or fragile components.

**Bent Connector Pins**: This type of problem can be resolved by re-bending the pins to their original shape using needle-nose pliers.

The most common cause of a bent connector pin is when the board is pulled off the stack by tugging it at angles from one end of the connector to the other, in an effort to release it off the stack. Tugging the board off the stack in this manner can bend the pin(s) significantly.

A similar situation can occur when pulling a ribbon cable off a pin header. If the pins are bent too severely, bending them back can cause them to weaken or break. In this case, the connector must be replaced.

**Short Circuit Failures:** There are various causes for a short circuit to occur and disrupt the electrical flow of the circuitry, causing the board to malfunction or cease to function entirely.

A short can be difficult to identify since its symptoms are often not visible.

Some common causes such as slipping of a metal screwdriver tip, or a screw dropping onto the board while it is powered-up, can cause a short between a power pin and a signal pin on a component, leading to circuit damage, over-voltage, and power supply problems.

To avoid such damages, assembly operations must be performed when the system is powered off.

**Power Supply Wired Backwards**: Our power supplies and boards are not designed to withstand a reverse power supply connection. This will destroy almost all ICs connected to the power supply. In this case, the board will most likely be irreparable and must be replaced. A chip destroyed by reverse or excessive power will often have a visible hole or show some deformation on the surface due to vaporization inside the package.

Another consideration is Logic Signals which are commonly generated between 12V to 24V.

If a Digital I/O Line of 12V to 24V is connected to a 5V logic chip, the chip will be damaged, and the damage could extend to other chips in the circuit.

IMPORTANT! Always check twice before Powering Up!

# 2. INTRODUCTION

The EPS-12002L is a compact managed Ethernet switch based on Diamond's EPSM-10GX Ethernet switch module. It is a 2-board solution consisting of the switch module and a carrier board. It features 12 1Gbe ports and 2 SFP+ sockets supporting up to 10Gbe fiber or copper transceivers. It includes embedded software delivering Layer 2+ switching and optional Layer 3 routing capabilities. IEEE1588 PTP support is also available upon customer request.

The EPSM-10GX switch module supports 12 1Gbe ports natively and up to 12 additional 1Gbe ports with the addition of a 12-port PHY on the carrier board. This PHY is not included on the EPS-12002L for size considerations. For a higher port count solution, please consider Diamond's EPS-24G4X:

www.diamondsystems.com/products/eps24g4x

## 2.1  Models

The following models are standard generally stocked items. For Layer 3 and IEEE1588 configurations please contact Diamond Systems Sales department for availability.

| Model | No. of Ports | Software Support | Thermal Solution |
|-------|-------------|------------------|------------------|
| **EPS-12002L-HSK** | 12x 10/100/1000 Mbps Gbe Copper Ports; 4x SFP+ | WebStaX Layer 2+ | Heat sink |
| **EPS-12002L-HSP** | 12x 10/100/1000 Mbps Gbe Copper Ports; 4x SFP+ | WebStaX Layer 2+ | Heat spreader |

## 2.2  Features

- Carrier board with EPSM-10GX Ethernet switch module
- 12 copper twisted pair GbE ports with onboard magnetics via 3 latching connectors with 4 ports per connector
- 2 SFP+ sockets for 1/2.5/10G fiber and copper transceivers
- Status LEDs
- IEEE1588 PTP clock circuit option
- 1PPS input option for IEEE1588 timing support
- Power input connector; +7V to +34V DC (12V/5A nominal)
- RS-232 console connector for CLI (command language interface) out-of-band management

## 2.3  Mechanical and Environmental Specifications

**Switch module**
- Dimension: 3.30" W x 2.16" H (84 mm x 55 mm)
- Power Input +5 VDC
- Operating Temperature: -40°C to +80°C

**EPS-12002L Carrier board**
- Dimension: 5.354" W x 2.16" H (136 mm x 55 mm)
- Power Input +7 VDC  to +34VDC
- Operating Temperature: -40°C to +80°C

## 2.4  Software Options: WebStaX and IStaX

There are two Ethernet software solutions available for EPS-12002L, by Microchip. Both support a comprehensive set of Ethernet Switching capabilities, designed to support Managed L2 and L3 Enterprise Switches such as:

- Port Control and Monitoring Features
- QoS Control
- Security Control and Authentication
- Advanced Power Savings Capability and Management

Microsemi's API (Application Programming Interface) provides complete API functionality through its user-friendly Operating-System independent function library that supports all Microsemi Ethernet switches, PHY, MAC, and Optical Transport Network (OTN) Mapper products.

The standard software package included with EPS-12002L is WebStaX layer 2. For more information, please go here:

- [microsemi.com/product-directory/ethernet-software/3956-vsc6819](microsemi.com/product-directory/ethernet-software/3956-vsc6819)

For the enhanced IStaX 2022.06 layer 3 software option, please refer to:

- [microsemi.com/product-directory/ethernet-software/3954-vsc6817](microsemi.com/product-directory/ethernet-software/3954-vsc6817)

The following Table provides an overview of the software features:

| Application | Features |
| --- | --- |
| **WebStaX™** | Includes complete Layer 2 (L2) and some Layer 3 (L3), and layer 4 (L4). Web Management for features such as Power over Ethernet (PoE), Stacking and Energy Efficient Ethernet (EEE). It does not support Routing, Telnet and SSH Network Protocol functionalities. |
| **IStaX™** | Includes complete WebstaX Features and Layer 3 (L3) Routing functionality. Adds support for IEEE 1588/PTP Timing, Telnet and SSH Network Protocol functionalities, and Linear/Ring Protection, including ERPS. |

# 3. FUNCTIONAL OVERVIEW

## 3.1 Block Diagram
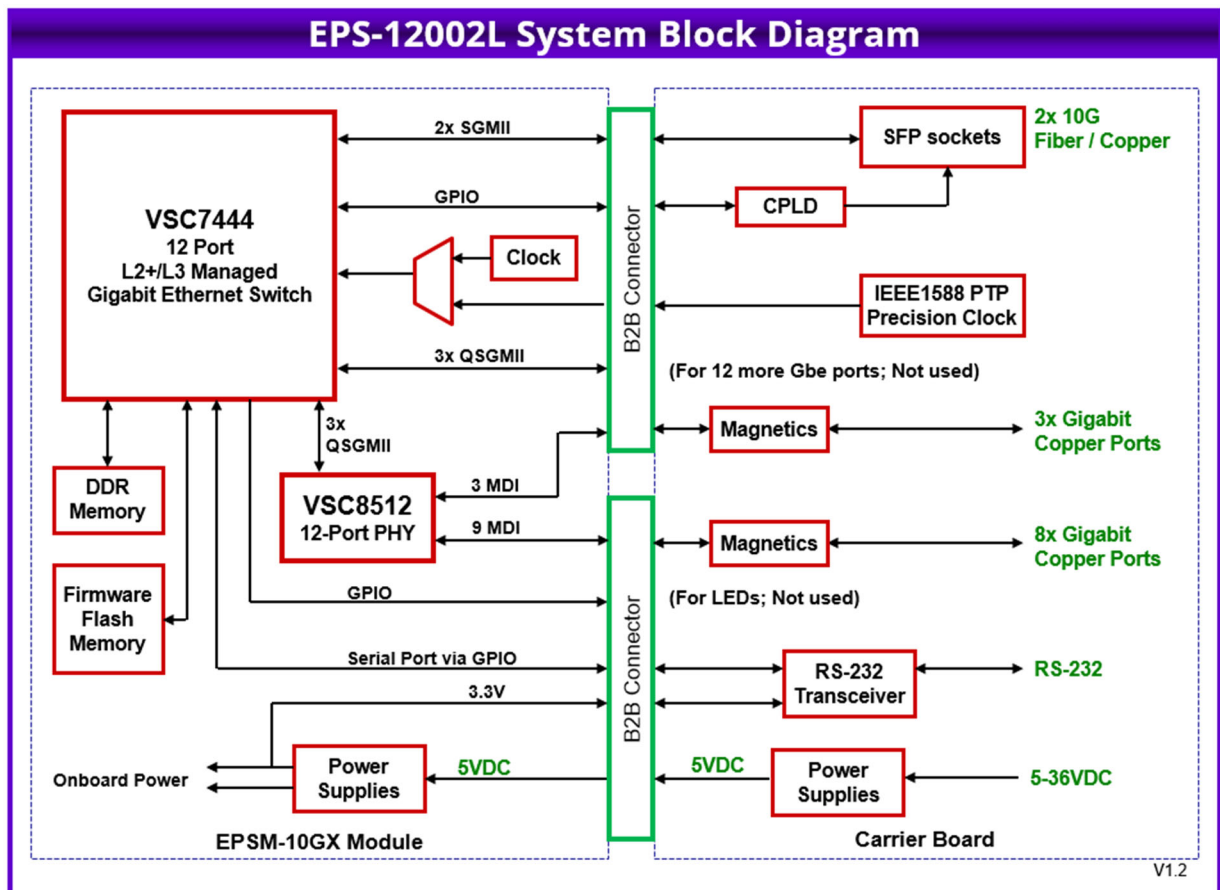


**Figure 3-1: EPS-12002L Ethernet Switch**

## 3.2 Feature Description

### 3.2.1 EPSM-10GX Switch Module

The EPSM-10GX Module is based on the Microsemi VSC7444 SMB/SME Industrial Gigabit Ethernet Switch with up to 24 ports supporting a combination 6x QSGMII ports and 2x 10G SFI Ethernet ports.

The VCore-III™, Core Voltage (VCORE), integrates 500 MHz MIPS 24KEc CPU with MMU and DDR3/DDR3L SDRAM controller. The chip contains a built-in processor that implements Layer 2 and Layer 3 switching and forwarding management software features provided by Microsemi.

The code is stored on-board Flash memory and is upgradeable via the Ethernet or Serial Interface.

Along with VSC7444 and VSC8512 PHY (Physical Layer), the module supports 2x 10G SFI ports, 12x 1G ports, and 3x QSGMII ports.

The VSC8512 is a low-power 12-port Gigabit Ethernet Transceiver with low Electromagnetic Interference (EMI) line driver and integrated line side termination resistors that conserve both power and space.

## 3.3 Precision Time Protocol Clock

The carrier board includes an optional high-precision clock circuit to enable the switch module to provide IEEE1588 PTP functionality. If the EPSM-10GXmodule is configured for IEE1588 PTP functionality then clock for Module switch and PHY are derived from the EPS-12002 carrier.

Optional 1PPS connector is provided for synchronization. If not used these signals can be left unconnected.

## 3.4  Copper Ports

EPS-12002 supports 12x 10/100/1000Mbps copper ports via 2mm rugged latching connector. Each latching connector supports 4x ports. On board magnetics for each copper ports are provided.

## 3.5  SFP+ Ports

EPS-12002 supports 2x SFP+ ports for 10G ethernet interface directly from EPSM-10GX module via 2nos of stacked SFP+ connector. Each SFP+ connector supports 2x ports. Control signals are interfaced via the CPLD logic.

## 3.6  Serial Console

The VSC7448 Switch offers a serial port function controlled by the management software. These lines are connected to a transceiver on EPS-12002 carrier to enable a RS-232 connection for management and debug purpose. The EPS-12002 Carrier Board is equipped with a 3-pin Latching Connector Serial Interface on J6.

## 3.7  Power Supply

The EPS-12002 is powered through an 8-pin Latching Power Input Connector J7 that uses a +7VDC to +34VDC wide-range power supply unit. Overvoltage protection is provided using onboard TVS diode.

The power supply ground is not connected directly to chassis ground. The board mounting holes plus any heat sink / heat spreader mounting holes are NOT connected directly to power supply ground. Instead the PCB contains footprints for optional installation of 0 ohm resistors at multiple locations to connect these points to power supply ground.

Typical power consumption details at different configurations at nominal +12V are  listed in the following Table.

| Vin (V) | Configuration | Current (A) | Power (W) |
|---------|---------------|-------------|-----------|
| **12V** | No Ports Connected | 0.86A | 10.32W |
| | Only 2 SFP+ Ports Connected | 0.96A | 11.52W |
| | Only 12 Ports Connected routed from Module 8522 PHY | 0.87A | 10.44W |
| | Only 12 + 2 SFP+ Ports Connected routed from Module 8512 PHY | 1.3A | 15.6W |

# 4. MECHANICAL DRAWING

Figure 8-3 delineates the Top View Mechanical Dimensions of the EPS-12002 Carrier Board.
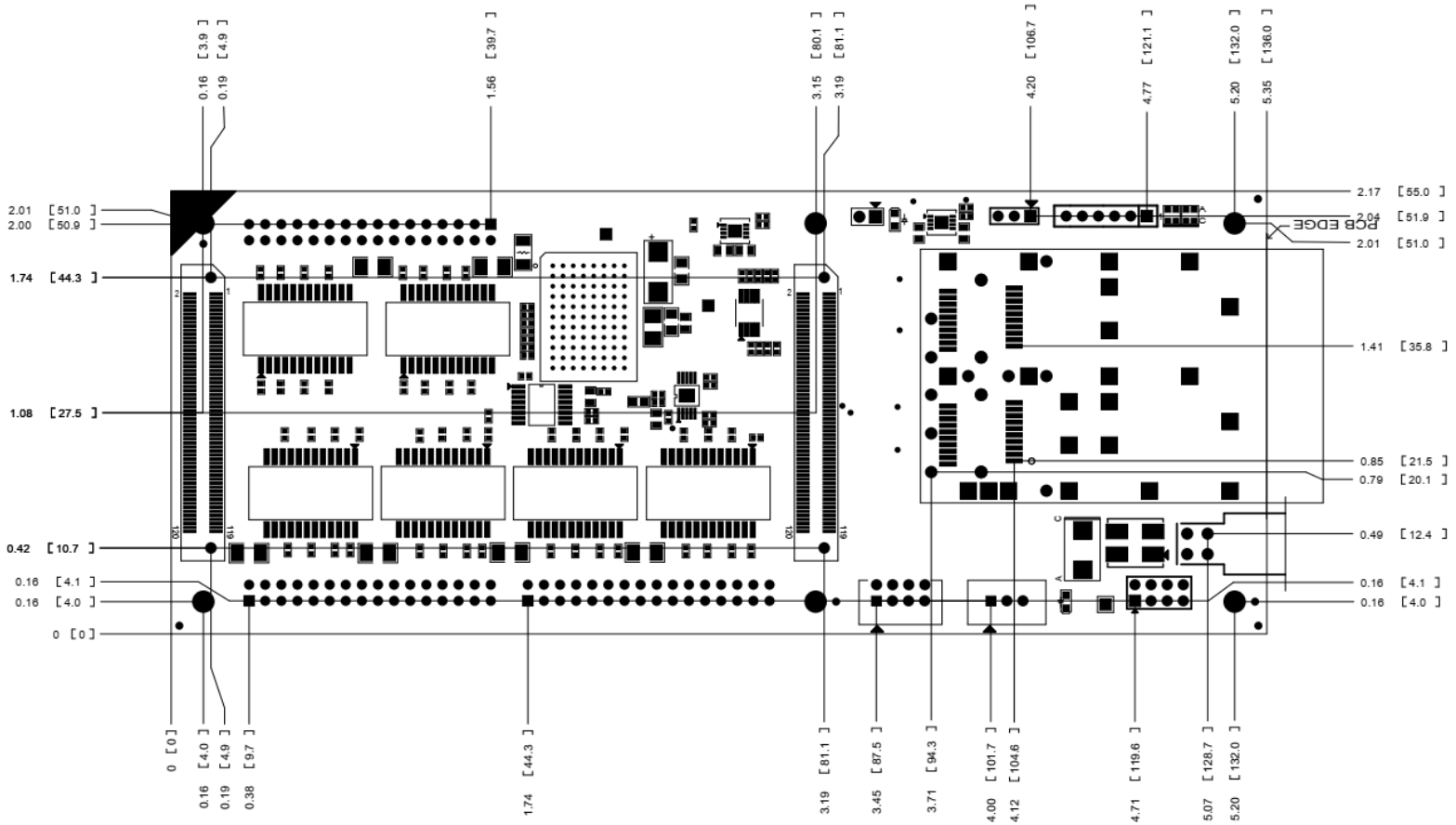


**Figure 4-1: Dimensions of EPS-12002 Carrier Board**

Figure 8-4 shows the Mechanical Dimensions of the EPSM-10GX and EPS-12002 Assembled Modules with customized Heat Sink.

# 5. BOARD LAYOUT

The following image displays the Top Layout of the EPS-12002 Carrier Board with Jumper Locations. A description of the Key Integrated Circuits and Connectors is tabulated below.
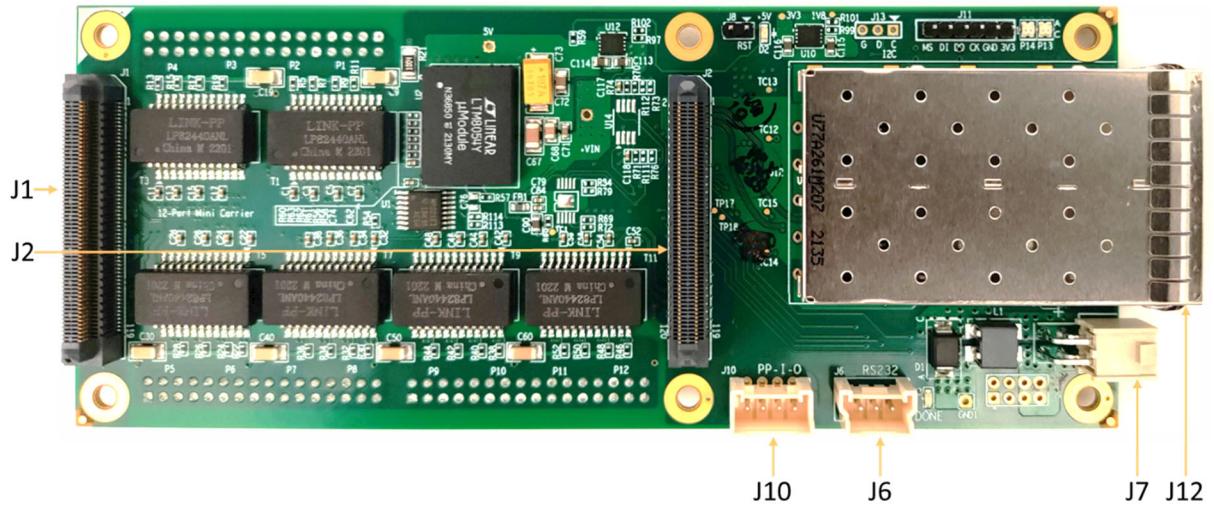


**Figure 5-1: EPS-12002 Carrier Board Top View Connector Locations**

## 5.1   IO Connectors

**EPS-12002 CARRIER BOARD**

| Connector | Description |
|-----------|-------------|
| **J1, J2** | High-speed B2B Connectors |
| **J12** | SFP-A-B  Connector |
| **J3** | PORT01 to PORT04 |
| **J4** | PORT05 to PORT08 |
| **J5** | PORT09 to PORT12 |
| **J6** | RS232 Port |
| **J10** | 1 PPS Input/output |
| **J7** | Power Input |

# 6. I/O CONNECTORS

## 6.1 Connector Pin-out and Signal Description

### 6.1.1 High-speed B2B Connectors: J1 and J2

The EPS-12002 Carrier Board contains 2x 120 pin 0.5mm pitch high-speed connectors that accommodate 12x 1 Gbps copper ports, 3x QSGMII ports, 2x 10G ports, power, and other sideband signals. These connectors mate with the EPSM-10GX main module.

The following Tables describe the **J1** and **J2** Board-to-Board (B2B) Pinout and Signal specifications

**Connector on EPS-12002 Carrier: Samtec ERM5-060-05.0-L-DV**

Mating Connector on EPSM-10GX Module: **Samtec ERF5-060-05.0-L-DV-K**

| Signal | J1 Pin No. | J1 Pin No. | Signal |
|---|---|---|---|
| GND_SIGNAL | 1 | 2 | GND_SIGNAL |
| RTX0DN | 3 | 4 | RTX0BN |
| RTX0DP | 5 | 6 | RTX0BP |
| GND_SIGNAL | 7 | 8 | GND_SIGNAL |
| RTX0CN | 9 | 10 | RTX0AN |
| RTX0CP | 11 | 12 | RTX0AP |
| GND_SIGNAL | 13 | 14 | GND_SIGNAL |
| RTX1DN | 15 | 16 | RTX1BN |
| RTX1DP | 17 | 18 | RTX1BP |
| GND_SIGNAL | 19 | 20 | GND_SIGNAL |
| RTX1CN | 21 | 22 | RTX1AN |
| RTX1CP | 23 | 24 | RTX1AP |
| GND_SIGNAL | 25 | 26 | GND_SIGNAL |
| RTX2DN | 27 | 28 | RTX2BN |
| RTX2DP | 29 | 30 | RTX2BP |
| GND_SIGNAL | 31 | 32 | GND_SIGNAL |
| RTX2CN | 33 | 34 | RTX2AN |
| RTX2CP | 35 | 36 | RTX2AP |
| GND_SIGNAL | 37 | 38 | GND_SIGNAL |
| RTX3DN | 39 | 40 | RTX3BN |
| RTX3DP | 41 | 42 | RTX3BP |
| GND_SIGNAL | 43 | 44 | GND_SIGNAL |
| RTX3CN | 45 | 46 | RTX3AN |
| RTX3CP | 47 | 48 | RTX3AP |
| GND_SIGNAL | 49 | 50 | GND_SIGNAL |
| RTX4DN | 51 | 52 | RTX4BN |
| RTX4DP | 53 | 54 | RTX4BP |

| Signal | J1 Pin No. | J1 Pin No. | Signal |
|---|---|---|---|
| GND_SIGNAL | 55 | 56 | GND_SIGNAL |
| RTX4CN | 57 | 58 | RTX4AN |
| RTX4CP | 59 | 60 | RTX4AP |
| GND_SIGNAL | 61 | 62 | GND_SIGNAL |
| RTX5DN | 63 | 64 | RTX5BN |
| RTX5DP | 65 | 66 | RTX5BP |
| GND_SIGNAL | 67 | 68 | GND_SIGNAL |
| RTX5CN | 69 | 70 | RTX5AN |
| RTX5CP | 71 | 72 | RTX5AP |
| GND_SIGNAL | 73 | 74 | GND_SIGNAL |
| RTX6DN | 75 | 76 | RTX6BN |
| RTX6DP | 77 | 78 | RTX6BP |
| GND_SIGNAL | 79 | 80 | GND_SIGNAL |
| RTX6CN | 81 | 82 | RTX6AN |
| RTX6CP | 83 | 84 | RTX6AP |
| GND_SIGNAL | 85 | 86 | GND_SIGNAL |
| RTX7DN | 87 | 88 | RTX7BN |
| RTX7DP | 89 | 90 | RTX7BP |
| GND_SIGNAL | 91 | 92 | GND_SIGNAL |
| RTX7CN | 93 | 94 | RTX7AN |
| RTX7CP | 95 | 96 | RTX7AP |
| PPS-0 | 97 | 98 | NC |
| RTX8DN | 99 | 100 | RTX8BN |
| RTX8DP | 101 | 102 | RTX8BP |
| 5V0 | 103 | 104 | 5V0 |
| RTX8CN | 105 | 106 | RTX8AN |
| RTX8CP | 107 | 108 | RTX8AP |
| UART_RXD | 109 | 110 | 5V0 |
| UART_TXD | 111 | 112 | 5V0 |
| PPS-1 | 113 | 114 | 5V0 |
| DB CONFIG1 | 115 | 116 | 5V0 |
| DB CONFIG2 | 117 | 118 | 5V0 |
| /MR_RST | 119 | 120 | 5V0 |

**Table 6-1: J2 Connector Signal Description**

**Connector on** EPS-12002 **Carrier: Samtec ERM5-060-05.0-L-DV**

Mating Connector on EPSM-10GX Module: **Samtec ERF5-060-05.0-L-DV-K**

| Signal | J2 Pin No. | J2 Pin No. | Signal |
|---:|:---:|:---:|:---|
| GND_SIGNAL | 1 | 2 | GND_SIGNAL |
| SFPPLUSA_RXD_N | 3 | 4 | SFPPLUSB_RXD_N |
| SFPPLUSA_RXD_P | 5 | 6 | SFPPLUSB_RXD_P |
| GND_SIGNAL | 7 | 8 | GND_SIGNAL |
| SFPPLUSA_TXD_N | 9 | 10 | SFPPLUSB_TXD_N |
| SFPPLUSA_TXD_P | 11 | 12 | SFPPLUSB_TXD_P |
| GND_SIGNAL | 13 | 14 | GND_SIGNAL |
| B_PCIE_T_P | 15 | 16 | QSGMII_P21_P24_RXD_P |
| B_PCIE_T_N | 17 | 18 | QSGMII_P21_P24_RXD_N |
| GND_SIGNAL | 19 | 20 | GND_SIGNAL |
| B_PCIE_R_P | 21 | 22 | QSGMII_P21_P24_TXD_P |
| B_PCIE_R_N | 23 | 24 | QSGMII_P21_P24_TXD_N |
| GND_SIGNAL | 25 | 26 | GND_SIGNAL |
| CLK125_1 | 27 | 28 | QSGMII_P17_P20_RXD_P |
| GND_SIGNAL | 29 | 30 | QSGMII_P17_P20_RXD_N |
| CLK125_2 | 31 | 32 | GND_SIGNAL |
| GND_SIGNAL | 33 | 34 | QSGMII_P17_P20_TXD_P |
| CLK25MHZ3 | 35 | 36 | QSGMII_P17_P20_TXD_N |
| GND_SIGNAL | 37 | 38 | GND_SIGNAL |
| SFPPLUSA_SCL | 39 | 40 | QSGMII_P13_P16_RXD_P |
| SFPPLUSA_LOS | 41 | 42 | QSGMII_P13_P16_RXD_N |
| SFPPLUSB_SCL | 43 | 44 | GND_SIGNAL |
| SFPPLUSB_LOS | 45 | 46 | QSGMII_P13_P16_TXD_P |
| NC | 47 | 48 | QSGMII_P13_P16_TXD_N |
| MII2_MDIO | 49 | 50 | GND_SIGNAL |
| MII2_MDC | 51 | 52 | SFPPLUSC_SCL |
| NINT_PHY0 | 53 | 54 | SFPPLUSC_LOS |
| I2C_SCL | 55 | 56 | SFPPLUSD_SCL |
| I2C_SDA | 57 | 58 | SFPPLUSD_LOS |
| GPIO1 | 59 | 60 | SGPIO2_LD |
| GPIO2 | 61 | 62 | SGPIO2_CLK |
| SGPIO2_DO | 63 | 64 | SLED1_DO |
| SGPIO2_DI | 65 | 66 | SLED1_CLK |
| COMA_MODE | 67 | 68 | SLED0_CLK |

| Signal | J2 Pin No. | J2 Pin No. | Signal |
|---|---|---|---|
| LED_PWM | 69 | 70 | SLED0_DO |
| | 71 | 72 | GND_SIGNAL |
| | 73 | 74 | PCIEWAKE |
| | 75 | 76 | |
| | 77 | 78 | |
| NINT_PHY1 | 79 | 80 | |
| NSYSRESET | 81 | 82 | |
| GND_SIGNAL | 83 | 84 | GND_SIGNAL |
| RTX9DN | 85 | 86 | RTX9BN |
| RTX9DP | 87 | 88 | RTX9BP |
| GND_SIGNAL | 89 | 90 | GND_SIGNAL |
| RTX9CN | 91 | 92 | RTX9AN |
| RTX9CP | 93 | 94 | RTX9AP |
| GND_SIGNAL | 95 | 96 | GND_SIGNAL |
| RTX10DN | 97 | 98 | RTX10BN |
| RTX10DP | 99 | 100 | RTX10BP |
| GND_SIGNAL | 101 | 102 | GND_SIGNAL |
| RTX10CN | 103 | 104 | RTX10AN |
| RTX10CP | 105 | 106 | RTX10AP |
| GND_SIGNAL | 107 | 108 | GND_SIGNAL |
| RTX11DN | 109 | 110 | RTX11BN |
| RTX11DP | 111 | 112 | RTX11BP |
| GND_SIGNAL | 113 | 114 | GND_SIGNAL |
| RTX11CN | 115 | 116 | RTX11AN |
| RTX11CP | 117 | 118 | RTX11AP |
| GND_SIGNAL | 119 | 120 | GND_SIGNAL |

### 6.1.2 CPLD Programming Header: J11

The EPS-12002 Carrier Board integrates a CPLD to implement the Ethernet LED Logic The LED status signals on the Main Board are transmitted through a serial bus over high-speed B2B connector.

The following Table describes the pin and signal specifications of the CPLD Programming Header.

Connector Type: 2.54mm TH Vertical Pin Header

| Pin No | Pin Signal |
|--------|-----------|
| 1 | +3.3V |
| 2 | Ground |
| 3 | TCK_PLD |
| 4 | TDO_PLD |
| 5 | TDI_PLD |
| 6 | TMS_PLD |

### 6.1.3 Copper Ethernet Ports: J3, J4 and J5

EPS-12002 Carrier Board contains Three identical connectors with four Ethernet ports per connector. J3, J4, and J5.Each port is equipped with four pairs that transmit differential signals.

The following Table describes the pin and signal specifications for the following pins.

**Connector Number:** SQW-116-01-F-D  2.00mm pitch

| Pin Signal | Pin No. | Pin No. | Pin Signal | Port Nos |
|-----------|---------|---------|-----------|----------|
| DD- | 1 | 2 | DD+ | |
| DC- | 3 | 4 | DC+ | Port 1 |
| DB- | 5 | 6 | DB+ | |
| DA- | 7 | 8 | DA+ | |
| DD- | 9 | 10 | DD+ | |
| DC- | 11 | 12 | DC+ | Port 2 |
| DB- | 13 | 14 | DB+ | |
| DA- | 15 | 16 | DA+ | |
| DD- | 17 | 18 | DD+ | |
| DC- | 19 | 20 | DC+ | Port 3 |
| DB- | 21 | 22 | DB+ | |
| DA- | 23 | 24 | DA+ | |
| DD- | 25 | 26 | DD+ | |
| DC- | 27 | 28 | DC+ | Port 4 |
| DB- | 29 | 30 | DB+ | |
| DA- | 31 | 32 | DA+ | |

### 6.1.4  Serial Interface: J6

The EPS-12002L Carrier Board contains a RS-232 connector for serial console. The following Table describes the pin and signal specifications for the J6 Serial Interface.

**Connector Number**: Molex 0353630360

Housing: Molex 0355070300          **Crimp Terminal**: 0502128100

| Pin No. | Pin Signal |
|---------|------------|
| 1 | Ground |
| 2 | TXD (Output) |
| 3 | RXD (Input) |

### 6.1.5  Power Input: J14

The EPS-12002L Carrier Board operates on a wide range of power supply of +7V to +34VDC. Power is supplied through an 8-pin Latching Connector. The pin-out description for input power is shown below.

**Connector Number:** Samtec IPL1-102-01-L-D-RA-K-ND Right Angle

**Housing:**  IPD1-02-D-K **Crimp Terminal:** CC79R-2024-01-F

The following diagram depicts the Front View of the Power Connectors. Note that this pinout is different compared to Samtec datasheet.

| | | | |
|---|---|---|---|
| Vin 7-34VDC | **1** | **2** | Ground |
| Vin 7-34VDC | **3** | **4** | Ground |

**Mating side View of the Power Connector**

### 6.1.6  PPS Connector Interface: J10

EPS-12002L Carrier Board contains a 1 PPS connector. The following Table describes the pinouts.

**Connector Number**: Molex 0353630460

Housing: Molex 0355070400          **Crimp Terminal**: 0502128100

| Pin No. | Pin Signal |
|---------|------------|
| 1 | 1PPS Output |
| 2 | Ground |
| 3 | 1PPS Input |
| 4 | Ground |

# 7. ASSEMBLING OR DISASSEMBLING THE SWITCH MODULE

The following Section provides images and instructions on how to assemble the Main Board and the Carrier Board. This step can be performed after the Heat Sink has been installed on the Main Board.

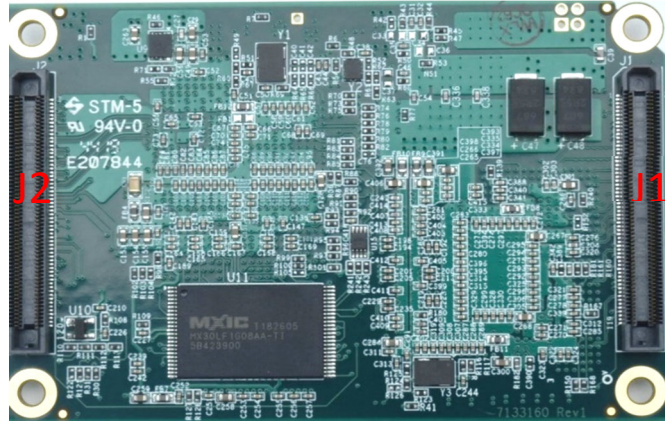1. The following Figure depicts the BOTTOM view of the EPSM-10GX Module.



**Figure 7-1: EPSM-10GX Module B2B Connectors**

2. The following Figure depicts the TOP view of the EPS-12002L - Carrier Board. The Connectors marked **J**1 and J2 correspond to the Connectors marked J1 and J2 on the EPSM-10GXBoard depicted above.
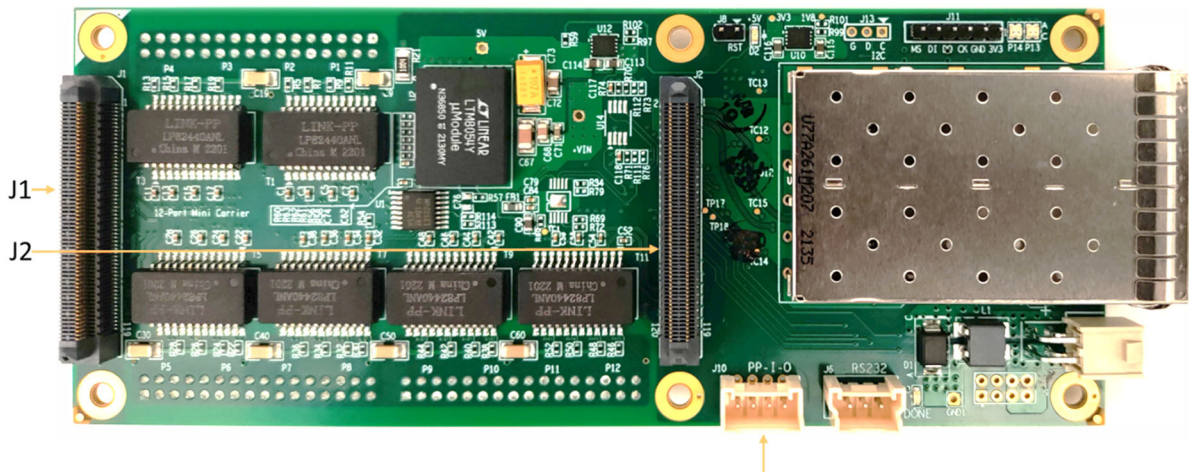


**Figure 7-2: EPS-12002L - Carrier B2B Connectors**

3. Place the EPSM-10GX module with the J1 and J2 Connectors facing down, above the EPS-12002L - Board.

4. Press firmly to snap the connectors in-place to interconnect the Boards.
5. Insert and tight the M2.5 5mm screws from EPSM-10GX module Top side

The following Figure shows the Top View of the assembled unit consisting of the carrier board, EPSM switch module, and heat sink. (A model with heat spreader is also available.)
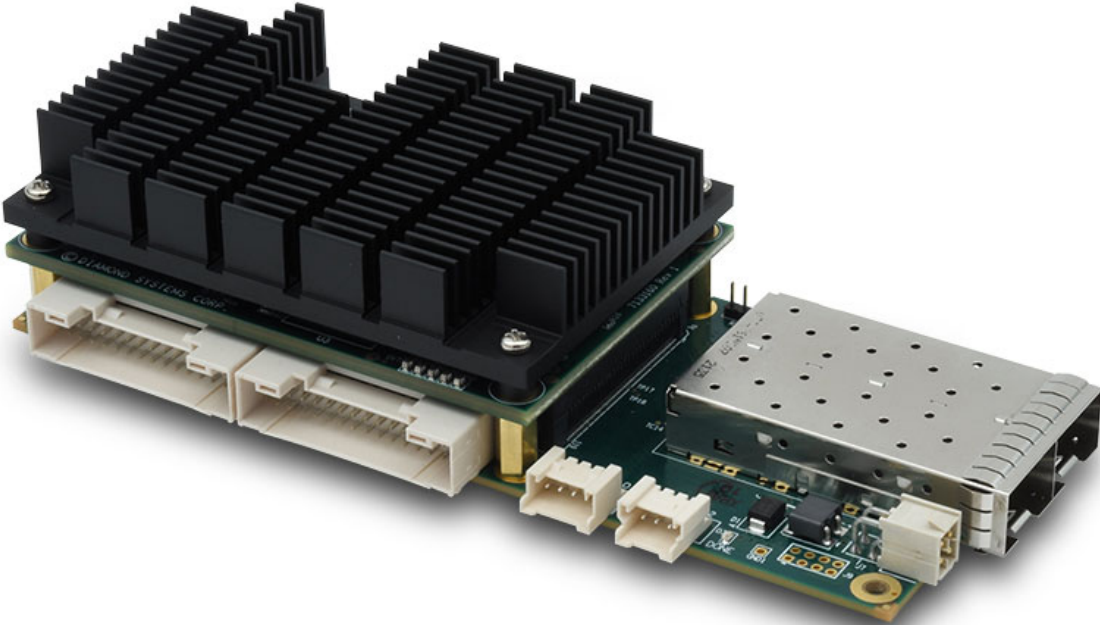


**Figure 7-3: EPSM-10GX+ EPS-12002L Module Assembled**

# 8. CABLE KIT

The EPS-12002L switch uses cable kit part no. CK-EPS12000, consisting of the cables listed below. Drawings for all cables are available at the following link:

https://www.diamondsystems.com/products/cables

| Cable part no. | Quantity | Description |
|---|---|---|
| 6981508 | 3 | Quad Ethernet cable with panel mount RJ-45 jacks |
| 6980512 | 1 | Power input cable with tinned leads |
| 6981050 | 1 | RS-232 port cable with DB-9 female |



**Figure 8-1: Cable Kit CK-EPS12000**

# 9. GETTING STARTED

This section provides instructions on setting up and configuring the hardware after the boards are mounted as instructed in Assembling or Disassembling Module section

1. Connect the serial cable, Part Number 6981050, to the J6 connector on the Carrier Board and a PC's serial port.

2. Open the Serial port application with a baud rate set to 115200-8-N-1.

3. Connect a LAN cable between the PC to any one of the desired ports on the cable(s) connected to the EPS-12002L - Switch as instructed in Step 3

4. Connect the power cable Part Number 6981507, from the connector J7 to a regulated power supply with +12V nominal or +7V to +34V.

5. Turn on the power supply and view the messages on the Serial Terminal.

6. Access through the default IP Address **192.168.1.60** from the Web Interface.

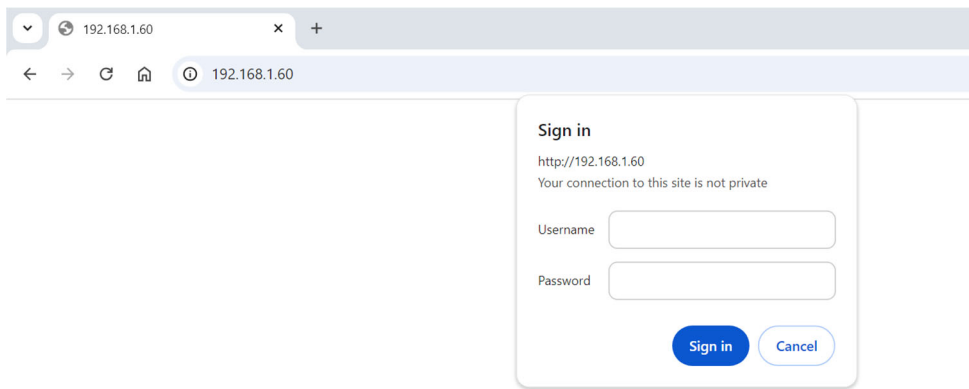7. Enter the default User Id: **admin**. No password is required.



**Figure 2-1 WebUI Log In using browser**

# 10. 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.

# 11. USING THE CLI INTERFACE

## 11.1 Making an Initial Connection

Serial Line Requirements:

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

## 11.2 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
#
```

## 11.3 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.

## 11.4 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.

## 11.5 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.

## 11.6 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 #
```

### 11.6.1  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: 15.1.10. 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.

### 11.6.2  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.

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

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

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

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

5. 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
```

6. 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 ]
```

7. 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
```

8. 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> ]
```

### 11.6.3  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> ] ) ]
```

### 11.6.4 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 ]
```

### 11.6.5 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 ]
```

## 11.6.6 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 }
```

## 11.6.7 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> ] ) ]
```

## 11.6.8 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> ]
```

### 11.6.9  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> ]
```

### 11.6.10 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> ]
```

### 11.6.11 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> ] ) ] } ] } ]
```

### 11.6.12 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> ]
) ]
```

## 11.6.13 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> ] ) ]
```

## 11.6.14 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> ] } ]
```

### 11.6.15 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
```

### 11.6.16 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> ]
```

### 11.6.17 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
```

### 11.6.18 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 ]
```

### 11.6.19 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
```

### 11.6.20 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>
```

### 11.6.21 Reload Command

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

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

### 11.6.22 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>
```

### 11.6.23 Ping Commands

The following syntax is used to ping the device.

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

### 11.6.24 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>
```

### 11.6.25 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>
] ) ]
```

### 11.6.26 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> ] } }
```

## 11.7 Command Parameter and Syntax Examples

### 11.7.1 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
#
```

### 11.7.2 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 #
```

### 11.7.3 Changing the Switch Password

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

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

### 11.7.4 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.

### 11.7.5  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 #
```

### 11.7.6  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
```

### 11.7.7  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 #
```

### 11.7.8  Upgrading the Firmware

A new WebStax image can be downloaded using the following CLI parameters. To do so:

Copy the EPSM-10GX4.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>/EPSM-10GX4.dat#
```

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

Copy the EPSM-10GX4.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>/EPSM-10GX4.mfi
```

### 11.7.9  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
```

# 12. 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 full-featured EPS-12002L Board which is equipped with 26 ports.
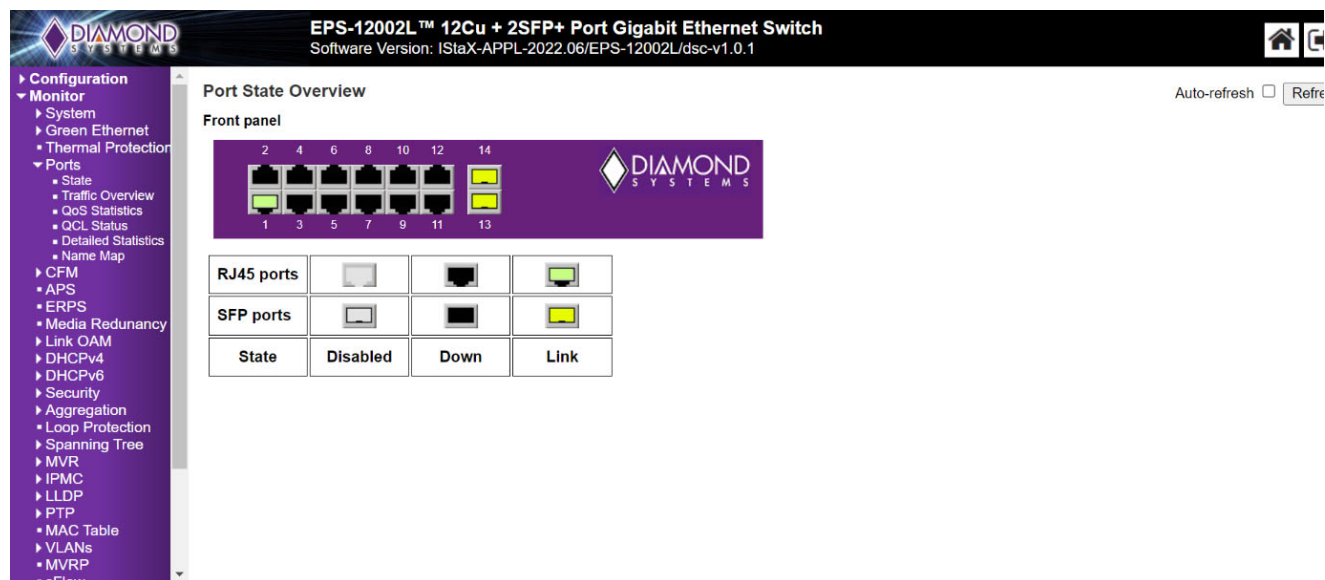


**Figure 12-1: EPS-12002L Carrier Board Home Page**
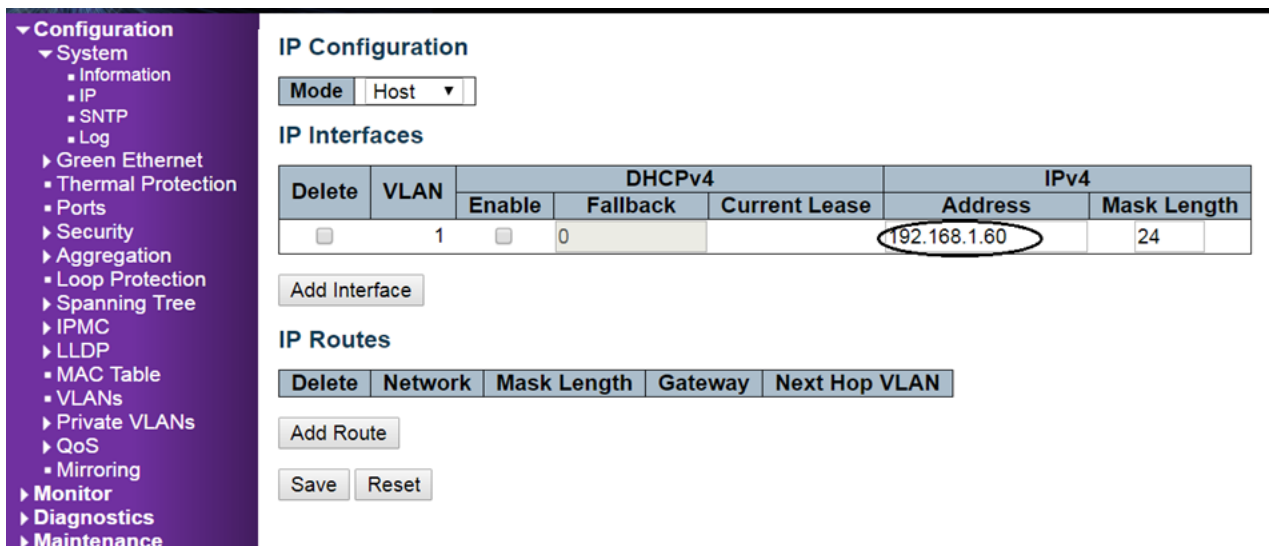
## 12.1 Web Interface Configuration Examples

### 12.1.1 IP Configuration

To configure the IP address of the Switch:

1. Connect EPS-12002L Switch 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 12-2: IP Configuration Screen**

### 12.1.2 Port Configuration

To configure Individual ports:

6. Connect EPS-12002L 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.
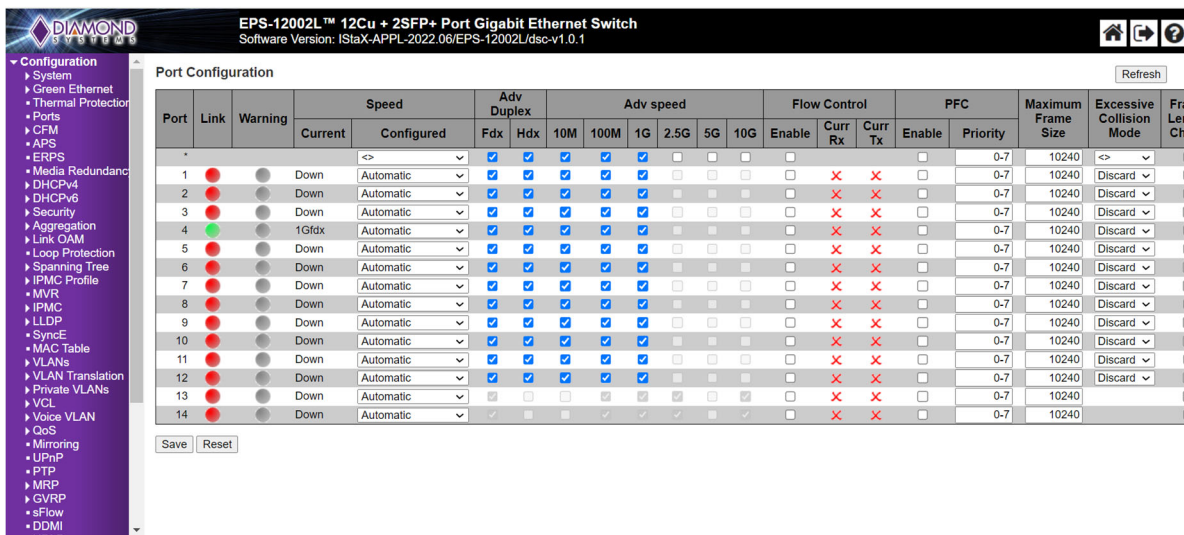


**Figure 12-3: Port Configuration Screen**

### 12.1.3 Changing the System Password

To change the system login password:

10. Connect EPS-12002L Switch to the Web Interface.

11. Navigate to **Configuration** -> **Security** ->**Switch** -> **Password** screen.

12. Enter the **Old Password** and **New Password** in the designated fields and click the **Save** button.

13. Navigate to **Maintenance** -> **Configuration** -> **Save Startup-Config** and click the **Save Configuration** button.

The System Password Screen is depicted below.
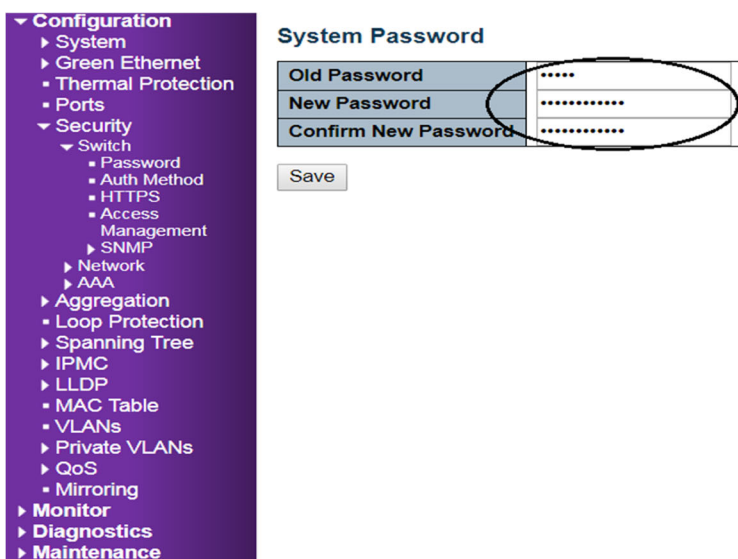


**Figure 12-4: Changing the System Password**

### 12.1.4 VLAN Configuration

The following example describes how to configure a VLAN.

14. Connect EPS-12002L Switch to the Web Interface.

15. Navigate to **Configuration** -> **VLANs** page.

16. 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.

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

To save VLAN settings permanently:

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

19. Click the **Save Startup Configuration** button.

20.



**Figure 12-5: VLAN Setup Screen**

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

To verify:

21. Navigate to **Monitor** -> **VLANs** -> **Membership** page.

22. 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**.
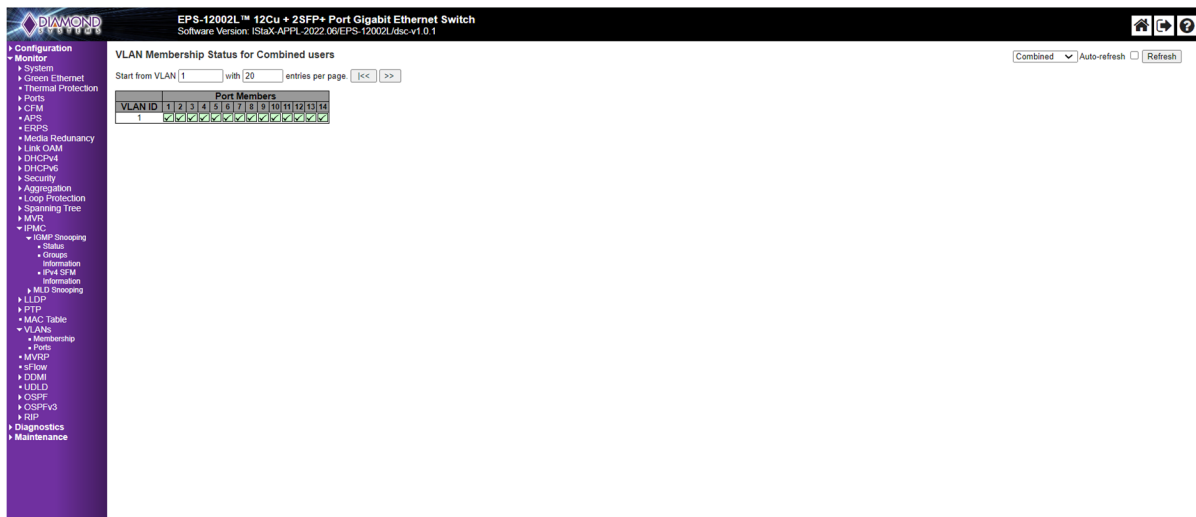


**Figure 12-6: VLAN Membership Verification Screen**

## 12.1.5 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**.

23. Connect EPS-12002L Switch to the Web Interface.

24. Navigate to **Configuration** -> **Mirroring** page.

25. Click -> **Save** to save the mirroring configuration.

**Figure 12-7: 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.
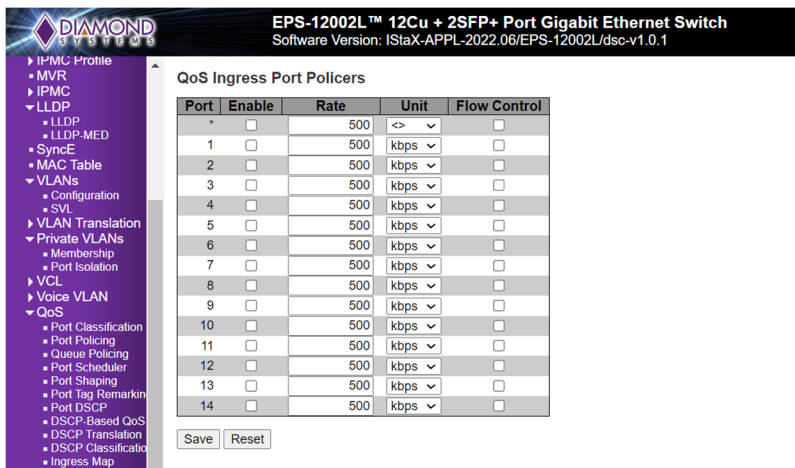
**Mirror Mode Description**

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

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

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

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

### 12.1.6  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**.

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

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

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

33. Click the **Save** button.



**Figure 12-8: QoS Classification Screen**

### 12.1.7  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:**

34. Navigate to the **Configuration** screen.

35. Select **Security** -> **Switch** -> **Access Management Configuration**.

36. Ensure the **Mode** is set to **Disabled** which is the default mode.

If it is not **Disabled**, select **Disabled** from the drop-down option.
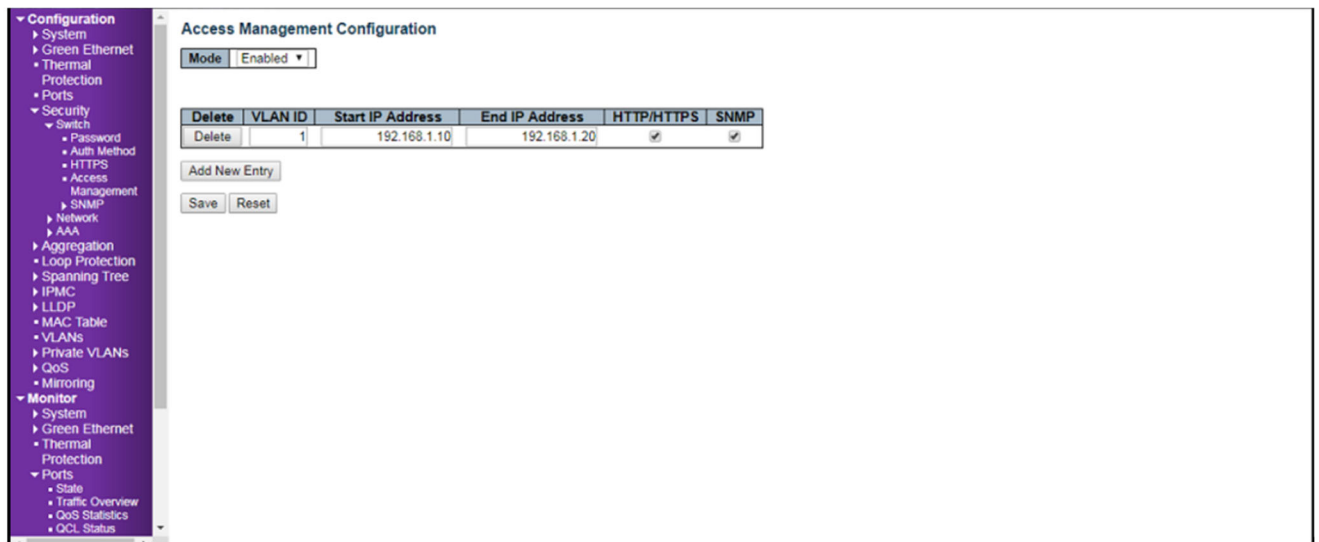
37. Click the **Save** button.



**Figure 12-9: 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:

38. Navigate to **Configuration** -> **Security** -> **Switch** -> **Access Management Configuration** screen.

39. Change the mode to **Enabled**.

40. 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.

### 12.1.8  Firmware Upgrade

The following section describes the steps for upgrading the firmware.

41. Connect EPS-12002L Switch to the Web Interface and navigate to **Maintenance** -> **Software** -> **Upload** page.

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

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

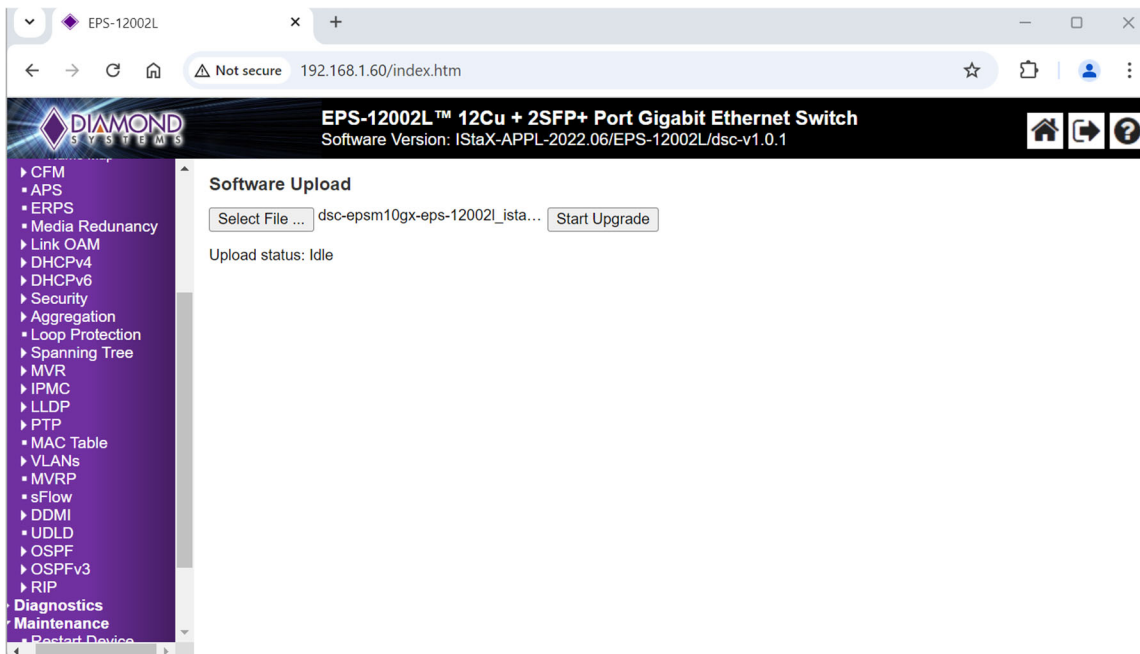When the upgrade is complete the Switch will automatically reboot.

**Figure 12-10: Firmware Upload Screen**

### 12.1.9  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:

43. Connect EPS-12002L Switch to the Web Interface.

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

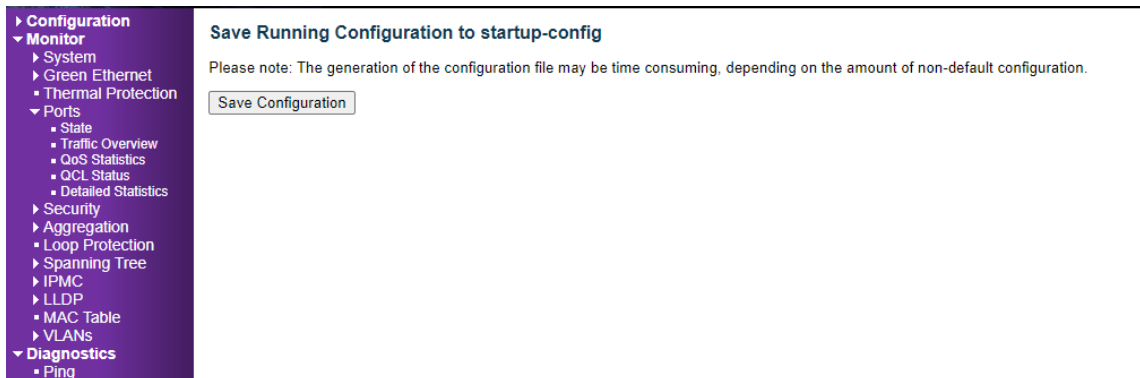45. Click the **Save Configuration** button.

**Figure 12-11: Uploading and Saving Startup Configuration Screen**

### 12.1.10 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:

46. Connect EPS-12002L Switch to the Web Interface.

47. Navigate to **Maintenance** -> **Factory Defaults** page.

48. Click the **Yes** button.

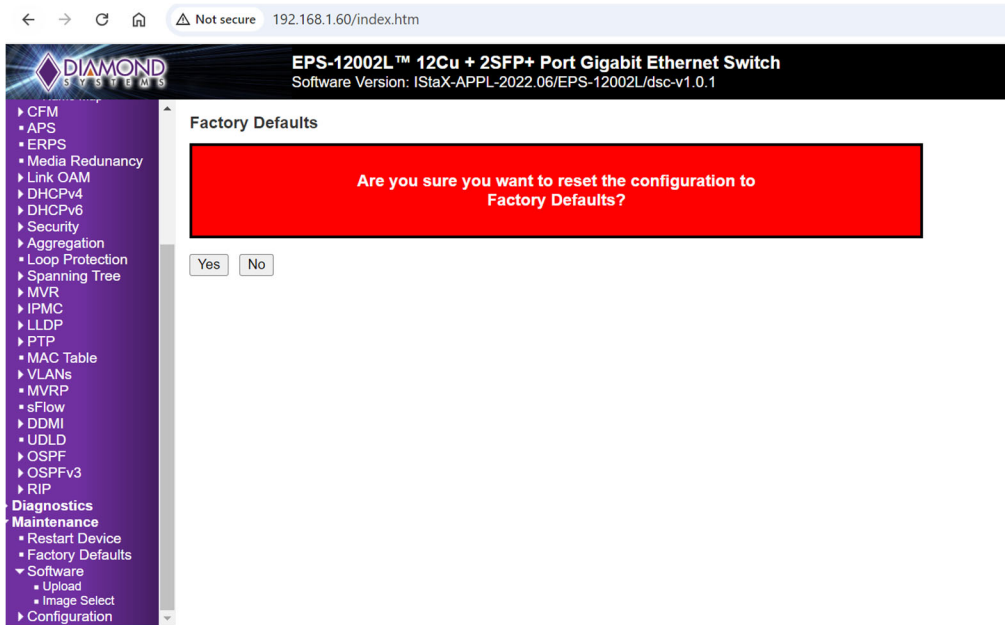A confirmation message will be displayed as shown below.
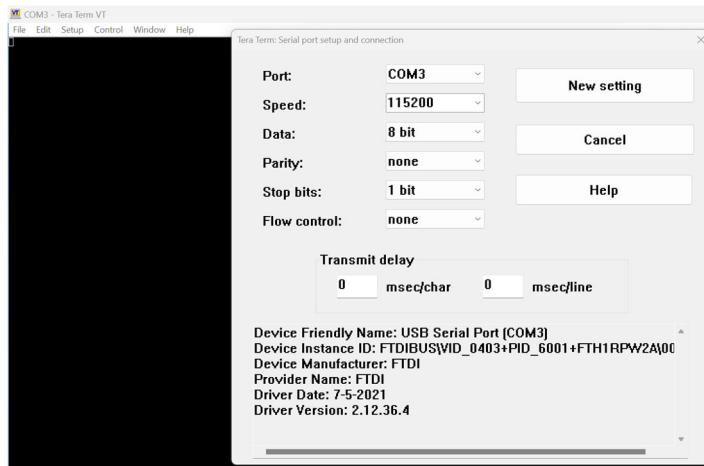


Figure 12-12: Resetting Switch to Fact

### 12.1.11 RS232 Serial Management Port

- Command Line Interface
    - Access parameters
    - 8 data bits
    - 1 stop bit
    - no parity
    - 115200 baud rate
    - No flow control

**[Result]:** Com port settings for command line interface

### 12.1.12 Switch Software / Firmware Upgrade

When a switch is not accessible via an Ethernet interface, the RS-232 port may be used for upgrading or reloading the switch firmware by connecting the switch to the serial port of any PC.

When the switch is accessible from Ethernet interface the switch will accept the firmware installation files via any Ethernet port.

TFTP for FTP server can be used to transfer installation files. SFTP is preferred if available.

If the software upgrade fails, the switch will return to its original state prior to the start of the installation process.

# 13. TECHINCAL SPECIFICATIONS

The specifications for EPS-12002L Switch are summarized in the following Table.

| Features | Specifications |
|---|---|
| Number of Ports | 12 10/100/1000Mbps Ethernet Ports with Non-Blocking Wire-Speed Performance<br>2 SFP+ Ports |
| MEF | Hierarchical MEF Compliant Policing and Scheduling; MEF E-Lane, E-Line, and E-Tree Services |
| Frame buffer | Jumbo Frame Support at all Speeds |
| Network Management | SNMP v1/v2c/v3<br>Web GUI<br>Command Line Interface (CLI) |
| VLAN | IEEE 802.1Q VLAN Switch with 32K MACs and 4K VLANs<br>Push/Pop up to Three VLAN Tags<br>Independent and Shared VLAN Learning (IVL and SVL) |
| Multicast | IPv4/IPv6 Uni & 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<br>Shaping/Policing per Queue and Per Port |
| Storm Control | Policing with Storm Control and MC/BC Protection |
| Classifier | 8 Priorities and 8 CoS Queues Per Port with Strict or Deficit-Weighted Round Robin Scheduling<br>Shaping/Policing Per Queue and Per Port |
| Storm Control | Policing with Storm Control and MC/BC Protection |
| Link Aggregation | EEE 802.3 ad |
| RSTP | Rapid Spanning Tree Protocol (IEEE 802.1W) and MTSP |
| MIBs | Support for WebStax |
| Power Management | ActiPHY and PerfectReach Power Management; VeriPHY Cable Diagnostics |
| Serial Port | 1 RS-232 Port for Host Interface |
| Standalone Cable | Standalone Network Switch or in Combination with a Host Computer |
| Power Input | +7-34V DC/DC power supply; Typ: 12V |
| MTBF | TBU |
| Form factor | 5.354" W x 2.16" H (136 mm x 55 mm) |
| Operating temp | -40°C to +80°C |
| Weight | TBU |
| RoHS | Compliant |

## 14. LIMITED WARRANTY POLICY

Diamond Systems Corporation warrants that DSC products will be free from defects and errors in material and workmanship and perform in full accordance with the technical specifications stated in the description of the product for a duration of 2-Year Period from the Date of Shipment.

Unless otherwise stated, DSC Limited Warranty Policy covers the following criterion.

- It is extended to the original Purchaser/Consumer.
- Under Terms and Conditions of the Warranty, DSC, at its sole discretion, will repair or replace any defective parts or components of its product.
- The product must be returned to DSC in DSC-approved packaging, pre-authorized with a DSC-assigned Return Material Authorization (RMA) Number which is referenced on the shipping document.
- The Customer will prepay the shipment cost of the product to the DSC designated site.
- DSC will prepay the return shipping cost of the repaired or replaced the RMA product.

DSC Limited Warranty Policy does not cover product defects or damages incurred due to:

- Attempts by Customer to repair or resolve any product issues without the prior consent of DSC.
- Mishandling, misuse, neglect, normal wear, and tear, or accident.
- DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY, INCLUDING BUT NOT LIMITED TO LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE TO OR REPLACEMENT OF EQUIPMENT AND PROPERTY, ANY COSTS OF RECOVERING, REPROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH DSC PRODUCTS, AND ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF DATA STORED ON THE PRODUCT.

**NOTE:** THE LIMITED WARRANTY POLICY DOES NOT WARRANT TO REPAIR ANY OR EVERY DSC PRODUCT.