Epsilon-8100 User Manual

Managed 8-Port Gigabit Ethernet Switch
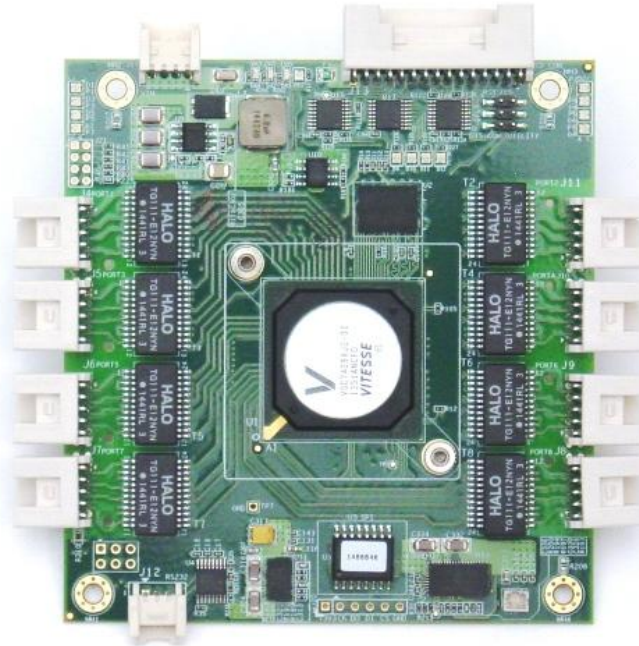
Revision	Date	Comment
A.0	08/12/2014	Initial Release
A.1	1/23/2015	Removed POE information
A.3	1/4/2016	Minor updates
A.4	7/28/2017	Updates of Software Version 2.0.0

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 Epsilon-8100 board 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 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.

Damage during handling or storage – On some boards we have noticed physical damage from mishandling. A common observation is that a screwdriver slipped while installing the board, causing a gouge in the PCB surface and cutting signal traces or damaging components.

Another common observation is damaged board corners, indicating the board was dropped. This may or may not cause damage to the circuitry, depending on what is near the corner. Most of our boards are designed with at least 25 mils clearance between the board edge and any component pad, and ground / power planes are at least 20 mils from the edge to avoid possible shorting from this type of damage. However these design rules are not sufficient to prevent damage in all situations.

A third cause of failure is when a metal screwdriver tip slips, or a screw drops onto the board while it is powered on, causing a short between a power pin and a signal pin on a component. This can cause overvoltage / power supply problems described below. To avoid this type of failure, only perform assembly operations when the system is powered off.

Sometimes boards are stored in racks with slots that grip the edge of the board. This is a common practice for board manufacturers. However our boards are generally very dense, and if the board has components very close to the board edge, they can be damaged or even knocked off the board when the board tilts back in the rack. Diamond recommends that all our boards be stored only in individual ESD-safe packaging. If multiple boards are stored together, they should be contained in bins with dividers between boards. Do not pile boards on top of each other or cram too many boards into a small location. This can cause damage to connector pins or fragile components.

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!**

Overvoltage on analog input – If a voltage applied to an analog input exceeds the design specification of the board, the input multiplexor and/or parts behind it can be damaged. Most of our boards will withstand an erroneous connection of up to ±35V on the analog inputs, even when the board is powered off, but not all boards, and not in all conditions.

Overvoltage on analog output – If an analog output is accidentally connected to another output signal or a power supply voltage, the output can be damaged. On most of our boards, a short circuit to ground on an analog output will not cause trouble.

Overvoltage on digital I/O line – If a digital I/O signal is connected to a voltage above the maximum specified voltage, the digital circuitry can be damaged. On most of our boards the acceptable range of voltages connected to digital I/O signals is 0-5V, and they can withstand about 0.5V beyond that (-0.5 to 5.5V) before being damaged. However logic signals at 12V and even 24V are common, and if one of these is connected to a 5V logic chip, the chip will be damaged, and the damage could even extend past that chip to others in the circuit.

2. INTRODUCTION

Epsilon-8100 is a managed, 8-Port Gigabit Ethernet Switch with wide power supply voltage input and a serial management port. Epsilon-8100 offers 10/100/1000Mbps copper twisted pair ports on a PC/104 format board. 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). A wide-range DC power supply is built into the board to allow it to be used with industrial power sources as well as the typical embedded +5V supply.

Highly Advanced Gigabit Ethernet Switch
Epsilon-8100 is an 8-port Gigabit Ethernet switch in the compact PC/104 form factor. Epsilon-8100 operates standalone, but can be included in any PC/104 board stack.

Layer 2+ Managed Switch
Epsilon-8100's Ethernet switch chip includes a built-in microcontroller for configuration and management. It can be accessed either through the on-board RS-232 port or one of the Ethernet ports.

Wide Power DC/DC Power Supply
Epsilon-8100 is powered through a wide voltage +5-36V DC/DC power supply input.

Rugged Design
Extended temperature operation of -40°C to +85°C is tested and guaranteed. Epsilon-8100 was designed with harsh applications in mind. Latching connectors provide increased reliability.

Software Support
The switch is ready to plug into your application without any driver installation or firmware upgrades. A web interface and a CLI provide an intuitive GUI for configuring and managing the switch.

2.1 Features

2.1.1 Main Feature List

- 8 10/100/1000Mbps copper Ethernet ports with nonblocking wire-speed performance
- Dual leaky bucket policers with remarking and statistics
- Jumbo frame support at all speeds
- 8K MAC addresses and 4K VLANs (IEEE 802.1Q), as well as 8K IPv4 and IPv6 multicast group support
- Flexible link aggregation support based on Layer-2 through Layer-4 information (IEEE 802.3ad)
- Multicast and broadcast storm control, as well as flooding control
- Rapid Spanning Tree protocol (RSTP) and MSTP
- 8 priorities and 8 QoS queues per port with scheduling
- Shaping/policing per queue and per port
- Multiple protocol support: IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, and IEEE 802.1X
- Built-in 416MHz MIPS 24KEC microcontroller for configuration and management
- RS-232 serial port provides out-of-band management interface
- Can operate autonomously or in conjunction with a host SBC
- Wide input voltage range: +5 to +36VDC input
- PC/104 form factor (3.55 x 3.775 in.)
- -40°C to +85°C (-40°F to +185°F) operating temperature

2.1.2 Mechanical and Environmental

- PC/104 compliant form factor including:
  - Board dimensions
  - Mounting holes
  - Component and heat sink height
  - -40°C to +85°C ambient operating temperature

2.2 Products

The table below lists the model number and description for the Epsilon-8100 and its associated cable kit.

Model Number	Description
EPS-8100-XT	8-Port Gigabit Ethernet Switch with heatspreader, PC/104 form factor, -40°C to +85°C operating temperature
EPS-8100	8-Port Gigabit Ethernet Switch with heatsink, PC/104 form factor, -40°C to +85°C operating temperature
C-EPS8000-KIT	Epsilon-8100 Cable Kit

2.3 Cable List

The contents of the Epsilon-8100 Cable Kit, C-EPS8000-KIT, are shown below.

Number	Part Number	Quantity	Cable Description
1	6981052	8	Ethernet cable (1 per port)
2	6981051	1	Power cable
3	6981050	1	Serial cable
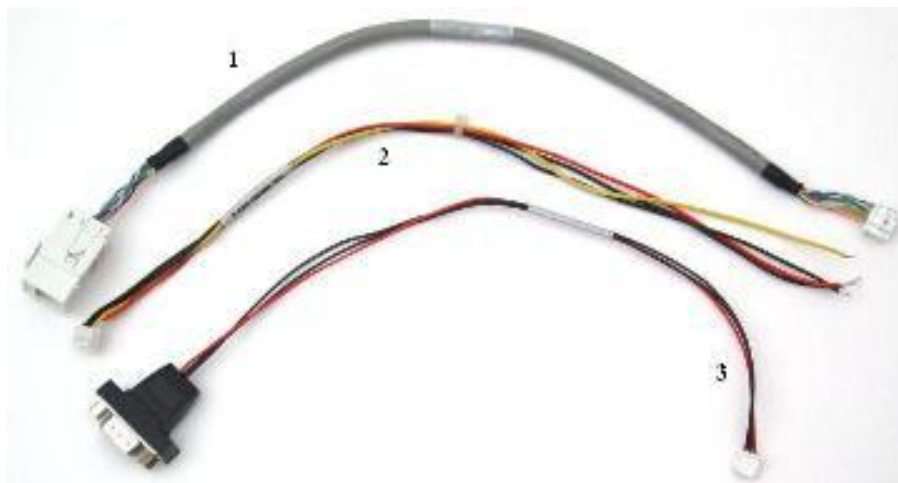
PC/104™ and PC/104-*Plus*™ are trademarks of the PC/104 Embedded Consortium.

All other trademarks are the property of their respective owners.

3. FUNCTIONAL OVERVIEW

3.1 Functional Block Diagram
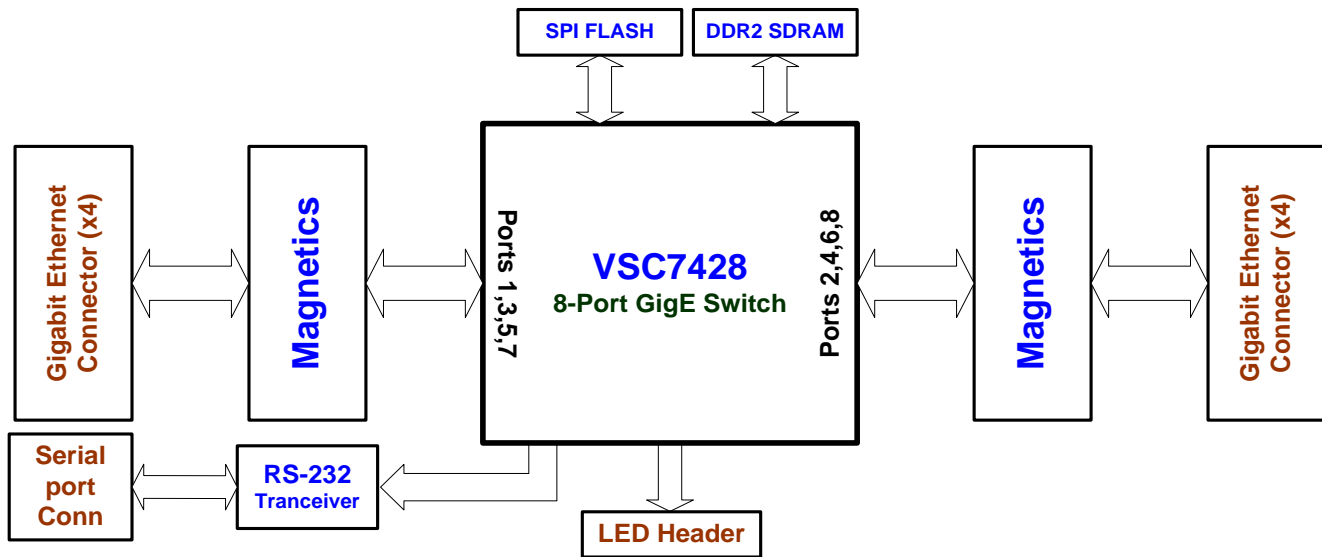
Figure 1. Functional Block Diagram

Epsilon-8100 is an 8-Port managed Gigabit Ethernet switch module offering 10/100/1000Mbps copper twisted pair ports on a PC/104 form factor board. Epsilon-8100 operates standalone, requiring no connection to a single board computer in the stack.

Epsilon-8100 is a Layer 2+ 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 SRAM is used for program execution and storing the MAC addresses. The EEPROM 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 CLI interface. The microcontroller is also accessible through one of the Ethernet ports via a web management interface.

Power is provided through the +5-36VDC wide-range DC power supply built into the board, enabling use with industrial power sources.

3.2 Board Layout

The following photo shows the locations for all connectors and jumpers which are described in the next sections.
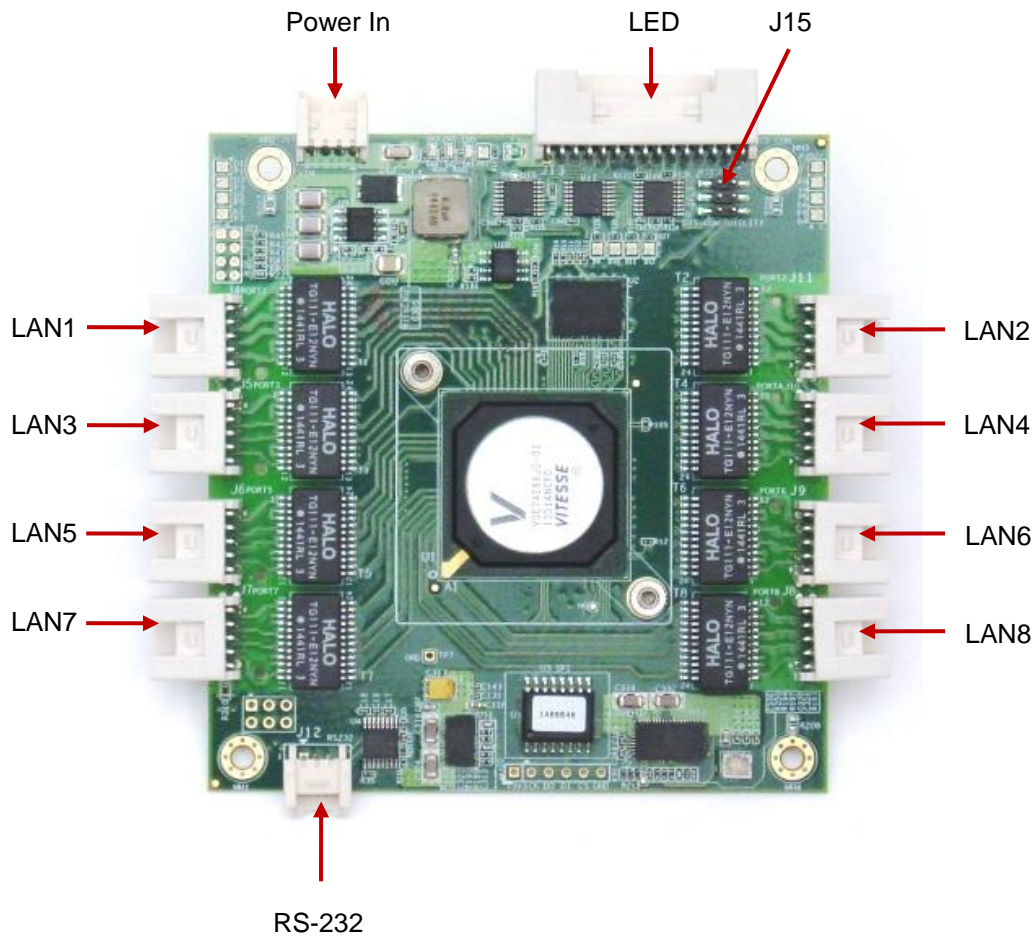
Figure 2. Epsilon-8100 Connectors and Jumpers

4. CONNECTOR AND JUMPER LIST

4.1 Connector and Jumper List

The following table summarizes the functions of Epsilon-8100's interface connectors and jumper. Refer to Figure 2 for the locations of these connectors on Epsilon-8100. Signal functions relating to all of Epsilon-8100's interface connectors are discussed in greater detail in Section 6 of this document. Other connectors and jumper blocks on Epsilon-8100 are reserved for Diamond's use only.

Connector	Function
LAN1-8	Ethernet (x8)
RS-232	RS-232 Serial Interface
LED	LED Status Signals and Resets
Power In	Wide voltage power input
J15	Jumper Block J15

4.2 Jumper Block (J15)

The following table summarizes the functions of Epsilon-8100's jumper block, J15. Refer to the Figure 2 for the location of J15 on Epsilon-8100.

Jumper J15 Pins	Function
1&2	Reset: Install jumper and power on to reset the switch
3&4	Factory Use Only
5&6	Factory Use Only

5. CONNECTOR PINOUT AND PIN DESCRIPTION

5.1 Ethernet (J4-J11)

Epsilon-8100 contains eight right-angle, locking pin headers for the eight Ethernet ports. Each port has the same style and pin out. Each signal is associated with a particular color inside of the Diamond Systems cable part number 6981052. The color coding for this cable follows the TIA/EIA 568B standard.

DD+	1	2	DD-
DC+	3	4	DC-
DB+	5	6	DB-
DA+	7	8	DA-
Gnd	9	10	Gnd

Connector Type: 2mm dual row right-angle, locking pin header with tin plating

Mating Connector: JST Sales America PUDP-10V-S housing with SPUD-002T-P0.5 terminals

5.2 Serial Interface (J12)

Epsilon-8100 contains an RS-232 connector, J12, which connects the on-board microcontroller to an external serial port.

1	Ground
2	TxD Out
3	RxD In

Connector Type: 2mm single row right-angle, locking pin header with tin plating

Mating Connector: Molex Connector 35507-0300 housing with 50212-8100 terminals

5.3 Input Power (J14)

Input power is supplied either through the dedicated 4-pin connector (J14). The pin out for J14 is:

1	V In
2	Ground
3	Ground
4	V In

Connector Type: 2mm single row right-angle, locking pin header with tin plating

Mating Connector: Molex Connector 35507-0400 housing with 50212-8100 terminals

5.4   LED Status Signals (J13)

Connector J13 provides access to the Ethernet LED signals for each of the eight ports. This connector has duplicate connections for Reset control input. LEDs may be directly connected to these signals without requiring any current-limiting resistors.

The on board activity LED is a green LED (LTST-C190GKT) with a typical forward voltage of 2.1V and a maximum of 2.6V with a 20mA If. The on board speed LED is a Yellow LED (LTST-C190YKT) with the same characteristics. The control signal is capable of sinking a maximum of 18mA. The series resistor is 330 ohms, which gives an If of about 3.6mA. When an LED is connected to connector J13, it is in parallel with the on board LED. If the external LED has about the same forward voltage, the current will be cut in half. If the external LED has a lower forward voltage, it will dominate the on-board LED and be brighter. Therefore, if the external LED is not bright enough use an external LED with a lower forward voltage.

Reset: Causes a reset of the switch when connected to ground.

SW_GPIO1 and SW_GPIO2 - provide control for user defined LEDs.

3.3V	29	30	3.3V
SW_GPIO1	27	28	SW_GPIO0
Default-	25	26	Reset-
Port 1 Speed	23	24	Port 1 Activity
Ground	21	22	Port 3 Activity
Port 3 Speed	19	20	Ground
Port 5 Speed	17	18	Port 5 Activity
Ground	15	16	Ground
Port 7 Speed	13	14	Port 7 Activity
Port 8 Activity	11	12	Port 8 Speed
Ground	9	10	Port 6 Speed
Port 6 Activity	7	8	Ground
Port 4 Activity	5	6	Port 4 Speed
Ground	3	4	Port 2 Speed
Port 2 Activity	1	2	Ground

Connector Type: 2mm dual row right-angle, locking pin header with tin plating

Mating Connector: JST Sales America PUDP-30V-S housing with SPUD-002T-P0.5 terminals

The following diagram shows how to connect external LEDs to connector J13:
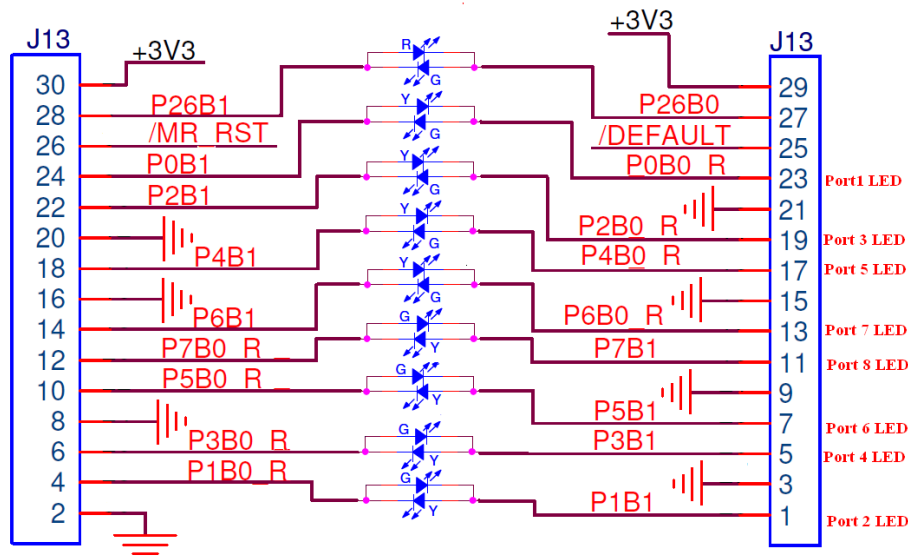
6. COMMAND LINE INTERFACE

The command line interface (CLI) is a modal, line-based interface with no screen editing features where commands are executed immediately upon end-of-line. The CLI can be accessed directly via the serial connection. The user must log in before CLI commands can be executed.

6.1 Making an Initial Connection

Serial line configuration:
    38400 baud
    8 bit data
    No parity
    1 stop bit

Login information

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

The board is shipped with an IP address of 192.168.1.60. This allows the WEB interface to be accessed at that address.

The IP address, mask and gateway must be set according to your environment, or you can enable IP and DHCP if your environment includes a DHCP server. For example:

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

Below example depicts configuration of 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
```

Display the IP address to confirm:

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

6.2 Login/Logout Procedures

To get access to the CLI you must login by entering a username and password. You will automatically be queried about the password.

The password is configurable. You may logout at any time and at any context level using the exit command

6.3   Help Utility

You may get help by pressing the *?* key or entering *help*. The help info depends on the context:

- At top level, a list of command groups is displayed.

- At 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 are shown.

6.4   Entering Commands

- Commands are not case-sensitive.

- You may use the horizontal arrow-keys ← and → to move the cursor within the command you are entering.

- You may use the backspace key (provided you are using a terminal that sends the BS (8) character when the backspace key is pressed) to delete chars from the command you are entering.

- You may use the vertical arrow-keys ↑ and ↓ to scroll through a command history buffer of the latest 20 commands issued.

6.5   General Command Groups

The following groups of general 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        Exit from EXEC mode
    firmware    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      Reload system.
    send        Send a message to other tty lines
    show        Show running system information
    terminal    Set terminal line parameters
#
```

6.5.1 IP Commands

(config)# ip http secure-redirect
(config)# ip http secure-server
(config)# ip igmp snooping
(config)# ip igmp snooping vlan <v_vlan_list>
(config)# ip igmp unknown-flooding
(config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
(config)# ip dhcp retry interface vlan <vlan_id>
(config)# no ip http secure-redirect
(config)# no ip http secure-server
(config)# no ip igmp snooping
(config)# no ip igmp snooping vlan [<v_vlan_list>]
(config)# no ip igmp unknown-flooding
(config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
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>]
show ip arp
show ip http server secure 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]
show ip interface brief
show ip route
show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

6.5.2 MAC Commands

(config)# mac address-table aging-time <v_0_10_to_1000000>
(config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])
(config)# no mac address-table aging-time
(config)# no mac address-table aging-time <v_0_10_to_1000000>
(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>])]

6.5.3 VLAN/PVLAN Commands

(config)# interface vlan <vlist>
(config)# no interface vlan <vlist>
(config)# no vlan { { ethertype s-custom-port } | <vlan_list> }
(config)# vlan <vlist>
(config)# vlan ethertype s-custom-port <etype>
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]

6.5.4 dot1x (IEEE Standard for port-based Network Access Control)

(config)# dot1x authentication timer inactivity <v_10_to_100000>
(config)# dot1x authentication timer re-authenticate <v_1_to_3600>
(config)# dot1x re-authentication
(config)# dot1x system-auth-control
(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]

6.5.5 LACP Commands

(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 }

6.5.6 LLDP Commands

(config)# lldp holdtime <val>
(config)# lldp reinit <val>
(config)# lldp timer <val>
(config)# lldp transmission-delay <val>
(config)# no lldp holdtime
(config)# no lldp reinit
(config)# no lldp timer
(config)# no lldp transmission-delay
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>])]

6.5.7 Access Management Commands

(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>]

6.5.8 Access-list Commands

(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>]

6.5.9 Logging Commands

(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>]

6.5.10 Spanning-tree Commands

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

6.5.11 Green-Ethernet Commands

(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
(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>])]

6.5.12 Thermal-protect Commands

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

6.5.13 Loop-protect Commands

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

6.5.14 QoS Commands

(config)# no qos qce <qce_id_range>
(config)# no qos storm { unicast | multicast | broadcast }
(config)# qos storm { unicast | multicast | broadcast } { { <rate> [kfps] } | { 1024 kfps } }
show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

6.5.15 Privilege Commands

(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

6.5.16 SNMP Commands

(config)# snmp-server
(config)# snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read
(config)# <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 security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>
(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 version { v1 | v2c | v3 }
(config)# snmp-server view <view_name> <oid_subtree> { include | exclude }
(config)# no snmp-server
(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 security-to-group model { v1 | v2c | v3 } name <security_name>
(config)# no snmp-server trap
(config)# no snmp-server user <username> engine-id <engineID>
(config)# no snmp-server version
(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>]

6.5.17 SNTP Commands

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

6.5.18 Radius Server Commands

(config)# radius-server attribute 32 <id>
(config)# radius-server attribute 4 <ipv4>
(config)# radius-server deadtime <minutes>
(config)# radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>]
[retransmit <retries>] [key <key>]
(config)# radius-server key <key>
(config)# radius-server retransmit <retries>
(config)# radius-server timeout <seconds>
(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]

6.5.19 Banner Commands (Defines a login banner)

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

6.5.20 Terminal Commands

(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>

6.5.21 Reload

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

6.5.22 Firmware Commands

firmware swap
firmware upgrade <tftpserver_path_file>

6.5.23 Ping Commands

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

6.5.24 Debug Commands

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

6.5.25 Security Commands

(config)# no aaa authentication login { console | telnet | ssh | http }
(config)# password encrypted <encry_password>
(config)# password none
(config)# password unencrypted <password>
(config)# enable password [level <priv>] <password>
(config)# enable secret { 0 | 5 } [level <priv>] <password>
(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>])]
(config)# aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }

6.5.26 Monitor

(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>] } }

6.6 Examples

6.6.1 IP Configuration

Below example depicts configuration of 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
```

Display the IP address to confirm:

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

6.6.2 Port Configuration

Individual ports can be configured to different speed. Following example shows configuring speed as 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
#
```

6.6.3 Change Switch Password

Following example shows setting of new password,

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

6.6.4   Set up VLANs

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

Following example shows setting up VLAN2 and VLAN3 with switch port mode set to access.

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

Set access port, in this case it's assumed that port 1~3 are connected to PC. 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
```

To verify created VLAN

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

As shown above, VLAN2 is created with the name VLAN0002 and a port 2 assigned to VLAN2. Similarly port 3 assigned to VLAN0003. Remaining ports 1 & 4 to 8 are by default assigned to VLAN 1

6.6.5   SNMP configuration

Following example depicts the configuration of SNMP,

To enable the SNMP mode operation

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

SNMP Trap configuration,

```
# configure terminal
(config)# snmp-server host Example
(config-snmp-host)# host 192.168.1.20
(config-snmp-host)# no shutdown
(config-snmp-host)# exit
(config)# exit
#
```

6.6.6   Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frame from multiple ports to a mirror port. Following example depicts Mirror traffic of Port 2 and 3 (Rx) & 4 to 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
```

6.6.7   Setup QoS

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

Following example shows setting up the QoS, all traffic coming on port 1 is mapped to QoS class (CoS) 2 and PCP is set as 1.

```
# configure terminal

(config)# interface GigabitEthernet 1/1

(config-if)# qos cos 2

(config-if)# qos pcp 1

(config-if)# end
```

6.6.8   Firmware Upgrade

A new WebStax image can be downloaded using the CLI. Copy the Epsilon-8100.dat file to a TFTP server and use the firmware upgrade command to download the file.

```
# firmware upgrade tftp://<ip_address>/<path>/Epsilon-8100.dat

#
```

6.6.9   Factory defaults

User can reset the configuration of the switch by below command. Only the IP configuration is retained.

```
# reload defaults

#
```

Note: To load the factory default configuration including the IP address, follow steps explained in section 7.1.11

7. WEB INTERFACE

The web interface offers an alternate user interface to the CLI. The web interface is in-band and requires use of one of the Ethernet ports. This port provides simultaneous web management and normal usage. The same commands with the same functionality can be accessed via either interface. From the WEB interface it is possible to, among other things:
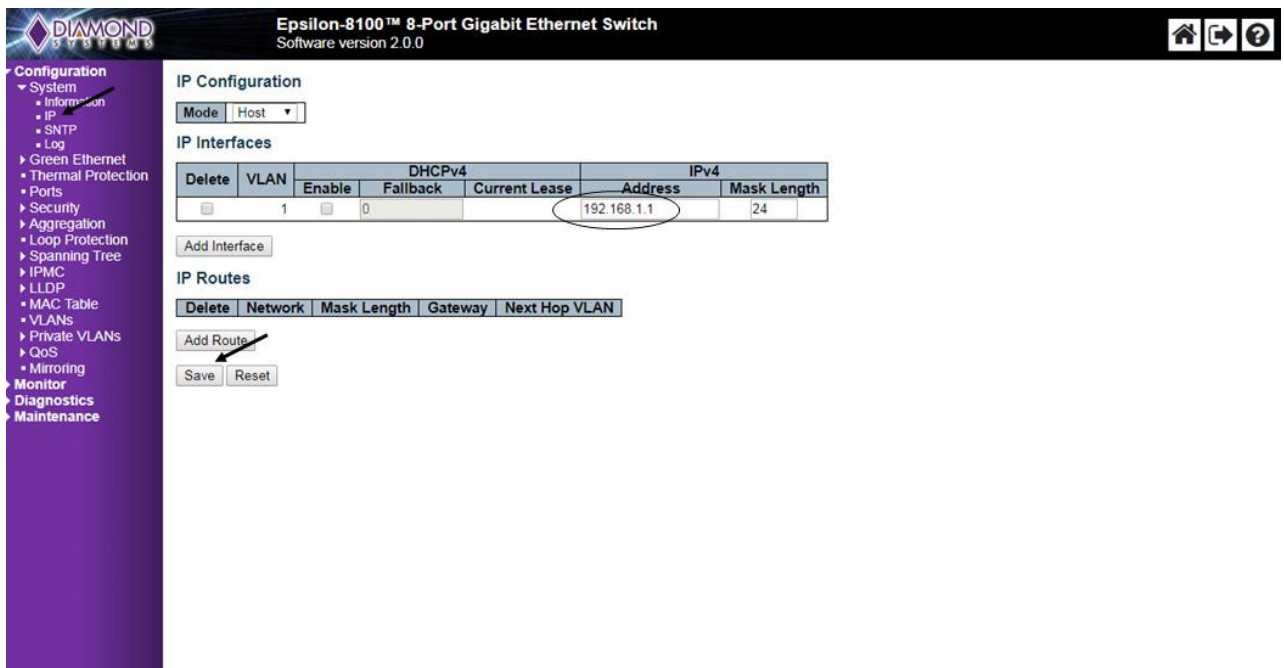
- Set port mode
- Enable/disable flow control
- Configure simple port-based VLAN
- Configure aggregation groups
- Configure LACP parameters
- Configure QoS
- Configure SNMP
- Mirroring
- Read and clear statistics counters
- Monitor LACP status
- Configure and monitor 802.1X
- Configure and monitor IGMP snooping (if defined for switch device)
- Configure source-IP address and DHCP server filter
- Upgrade software

7.1   Examples

7.1.1   IP Configuration

IP address of the switch can be configured as follows:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Configuration -> System -> IP

3. Modify the IP Address in IPv4 Address column (refer to figure below)

4. Click on Save

5. Navigate to Maintenance -> Configuration -> Save Startup-Config and click on Save Configuration

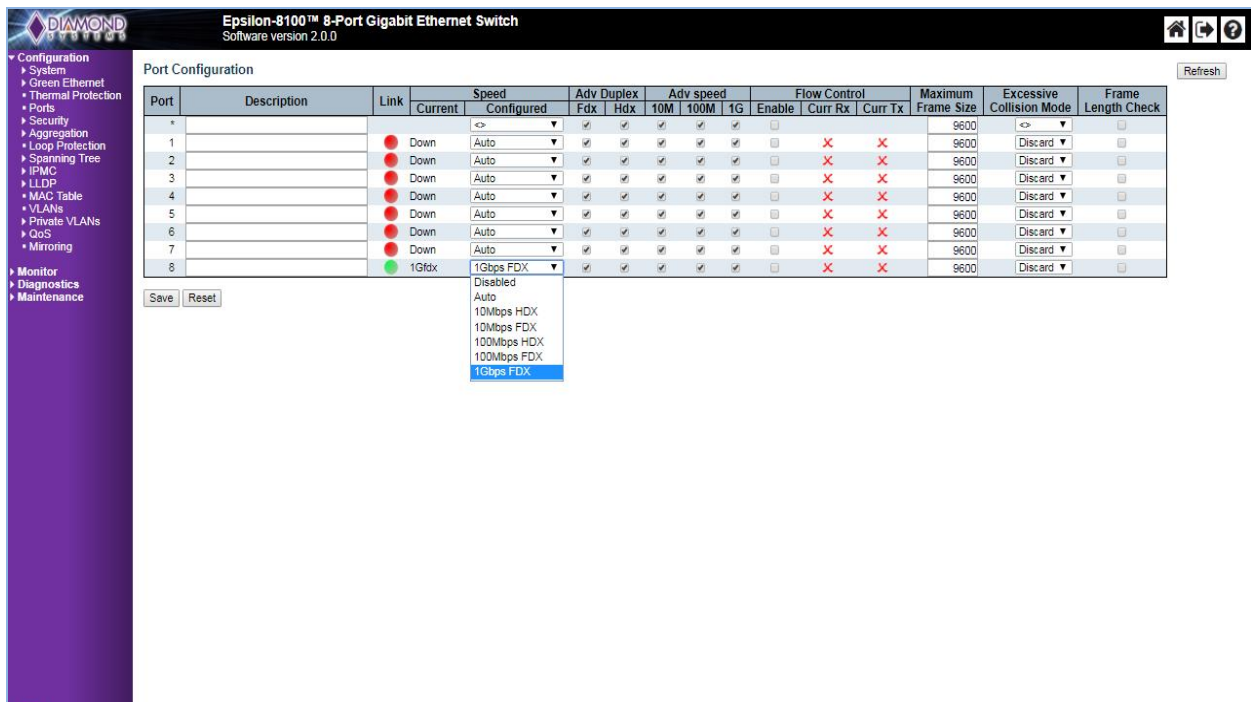**Figure 3 – IP Configuration**

7.1.2 Port Configuration

Individual ports can be configured as follows:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Configuration -> Ports

3. Each port can be set for one of the following configurations

    a. Disabled – Disables the switch port operation

    b. Auto – Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner

    c. 10 Mbps HDX – Forces the cu port in 10Mbps half-duplex mode

    d. 10 Mbps FDX – Forces the cu port in 10Mbps full-duplex mode

    e. 100 Mbps HDX – Forces the cu port in 100Mbps half-duplex mode

    f. 100 Mbps FDX – Forces the cu port in 100Mbps full duplex mode

    g. 1 Gbps FDX – Forces the port in 1Gbps full duplex

4. After port configuration is done click on save

5. To save these settings permanently navigate to Maintenance -> Configuration -> Save Startup-config click on Save startup configuration

Figure 4 – Port configuration

7.1.3 Change Password

The switch login password can be changed as follows:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Configuration -> Security -> Password

3. Enter the Old password and New Password and click on Save (refer to figure below)

4. Navigate to Maintenance -> Configuration -> Save Startup-Config and click on Save Configuration
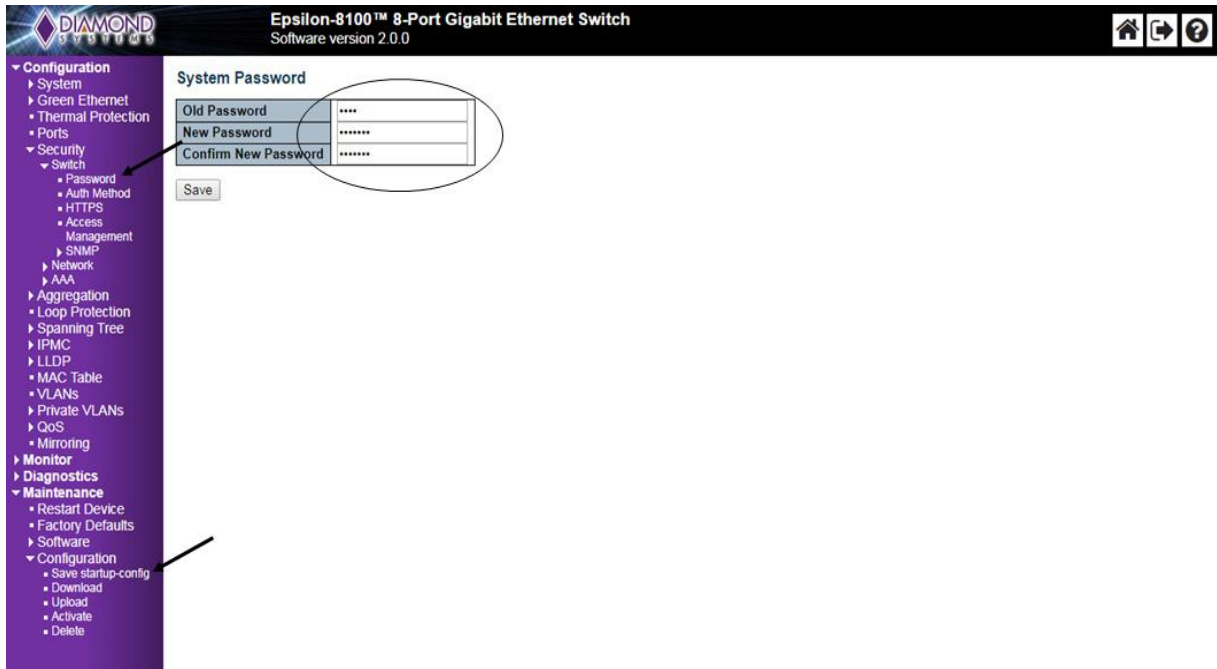

Figure 5 – System Password Configuration

7.1.4 Set-up VLANs

The following example shows the configuration of a VLAN:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Configuration -> VLANS
   a. In the allowed access VLANs enter number of LANs to be created. In this example 1-3, that creates VLAN2 and VLAN3
   b. By default mode is access, it can be changed to trunk or hybrid by changing Mode drop down list
   c. Assign a ports to the virtual LANs by changing the values in the Port VLAN column (refer to figure below)
   d. Click on Save to save the VLAN configuration
   e. To save VLAN settings permanently navigate to Maintenance -> Configuration -> Save startup-config click on save startup configuration
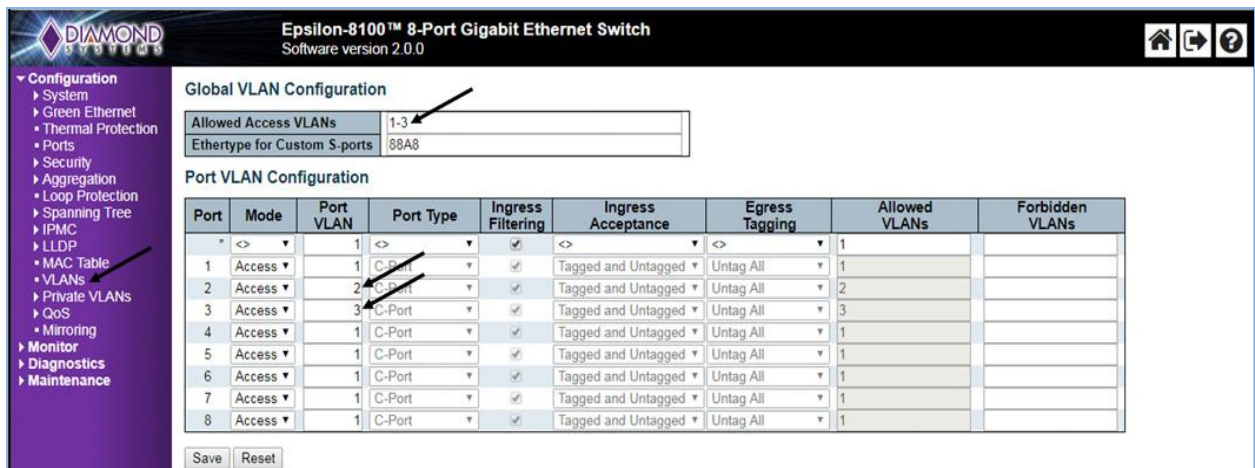

Figure 6 – VLAN Configuration

After saving the VLAN configuration, VLAN membership status can be verified as follows:

1. Navigate to Monitor -> VLANs -> Membership (refer to figure below)

2. Ports 1 & 4 to 8 assigned to VLAN ID 1, Port 2 is assigned to VLAN ID 2 and Port 4 is assigned to VLAN ID 3
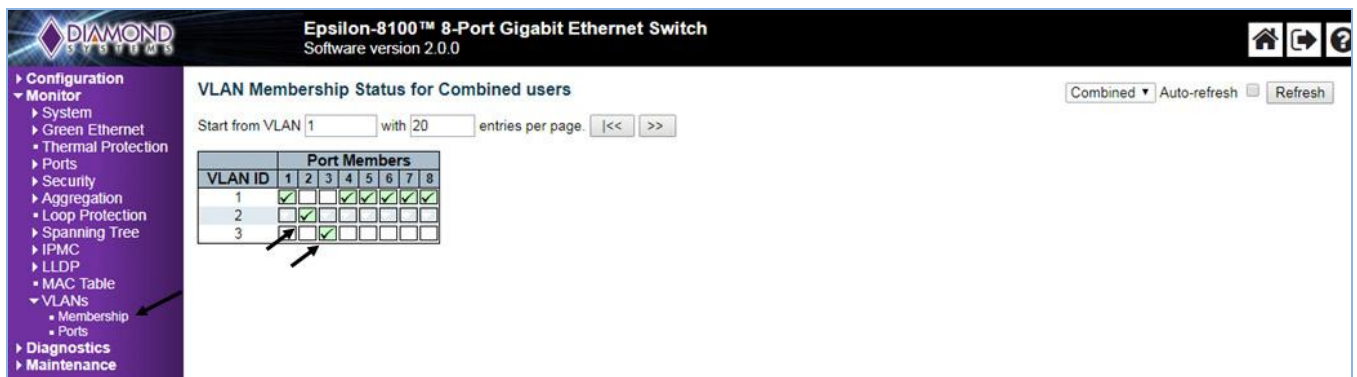

Figure 7 – VLAN Membership Status for Combined users
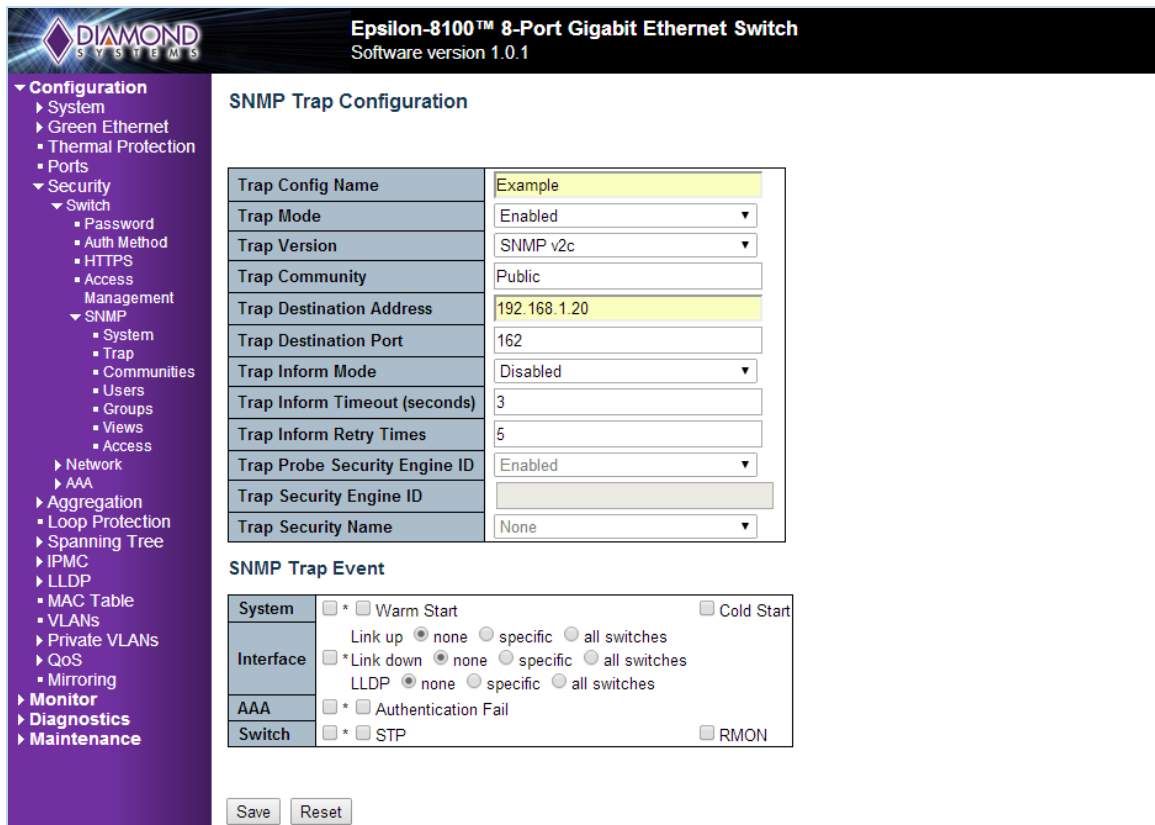
7.1.5 SNMP Configuration

The following procedure shows the SNMP configuration:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Security -> Switch -> SNMP -> System, and Enable the Mode and set the SNMP version (example: SNMP v1, SNMP v2c & SNMP v2c)

The following procedure shows the SNMP Trap configuration:

Note: if the software version is 2.0.0, it is not possible to enter trap destination address from web UI. Trap address can be configured using commands as explained in the section 6.6.5.

1. Navigate to Security -> Switch -> SNMP -> Trap and click on Add new Entry

2. Make the SNMP Trap configuration as follows and click on save

Figure 8 – SNMP Trap configuration

3. The trap configuration is displayed as follows:

Enable the Mode and click on Save to save the trap configuration.
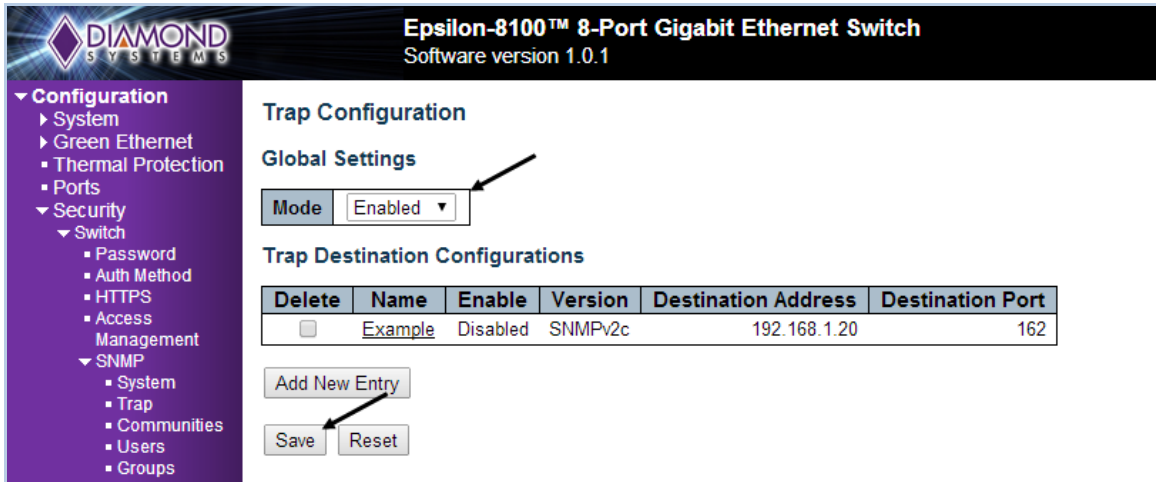
Figure 9 – Trap configuration

7.1.6 Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frame from multiple ports to a mirror port. The following example shows Mirror traffic of Port 1 (Tx) & 2(Rx) to Port 6.

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Configuration -> Mirroring (Refer below Figure)

Figure 10 – Mirroring Configuration

3. Click on Save to save the mirroring configuration.

Other Mirroring options -

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.

Mirror Mode Configuration

1. Rx only - Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.
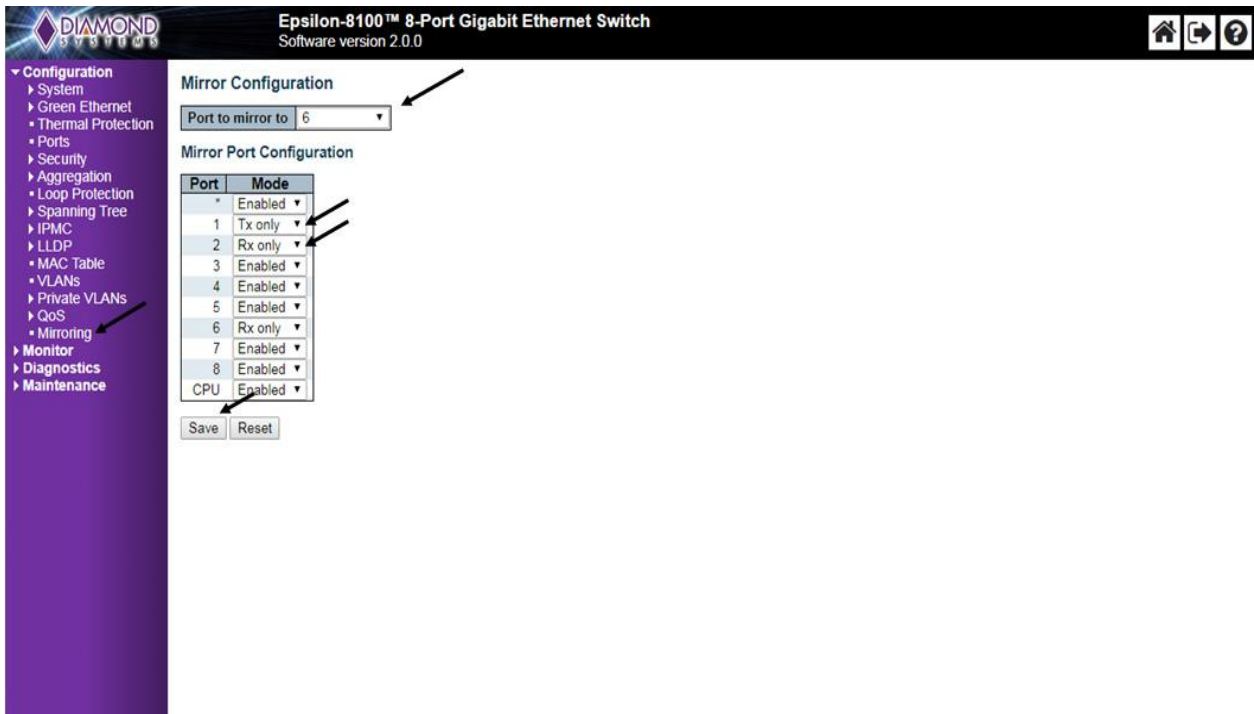
2. Tx only - Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.

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

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

7.1.7   Setup QoS

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

The following example shows the QoS ingress port classification:

All traffic coming on port 1 is mapped to Cos 2 and PCP is set as 1.

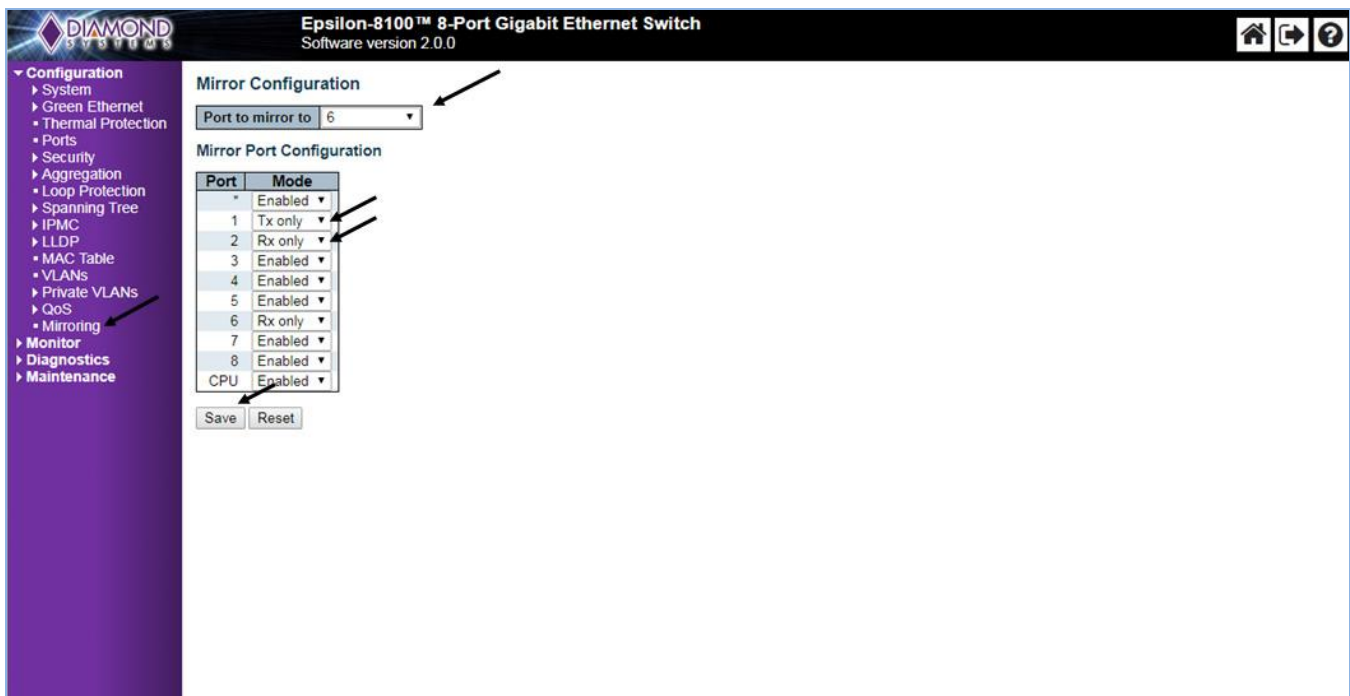Web GUI Configuration: (Navigate to Configuration ->QoS->Port Classification)

Figure 11 – QoS Ingress Port Classification

7.1.8 Web Interface Activation / Deactivation

The web interface can be activated and deactivated through either the command line interface or the web Control Panel.

Using the Control Panel, in the Configuration/Security/Switch/Access Management Configuration screen, first ensure the mode is set to Disabled as shown below. This is the default mode. If it is not set to Disabled, set it as Disabled and click Save.

This configuration should be stored on the switch with the following CLI command:
#copy startup-config flash:{filename}

To disable web access of the switch, in the Control Panel navigate to the Configuration/Security/Switch/Access Management Configuration screen, change the mode to Enabled and click Save.

Now there is no access to the switch using the web interface. To store this configuration in flash as the standard configuration on startup, enter the following command in the CLI:
#copy running-config startup-config

To allow web access of the switch in the future, enter the following commands in the CLI:
#copy startup-config flash:backup_config
#copy flash:{filename} startup-config

Then reboot the switch.

7.1.9 Firmware Upgrade

The following section shows the steps necessary to upgrade the firmware:

1. Connect to the web interface of EPS-8100 switch and navigate to Maintenance -> Software -> Upload (as shown in the figure below)

2. Choose Epsilon-8100.dat file and click on upload

The existing firmware is erased and new firmware loaded. Once the upgrade completes the switch reboots automatically.
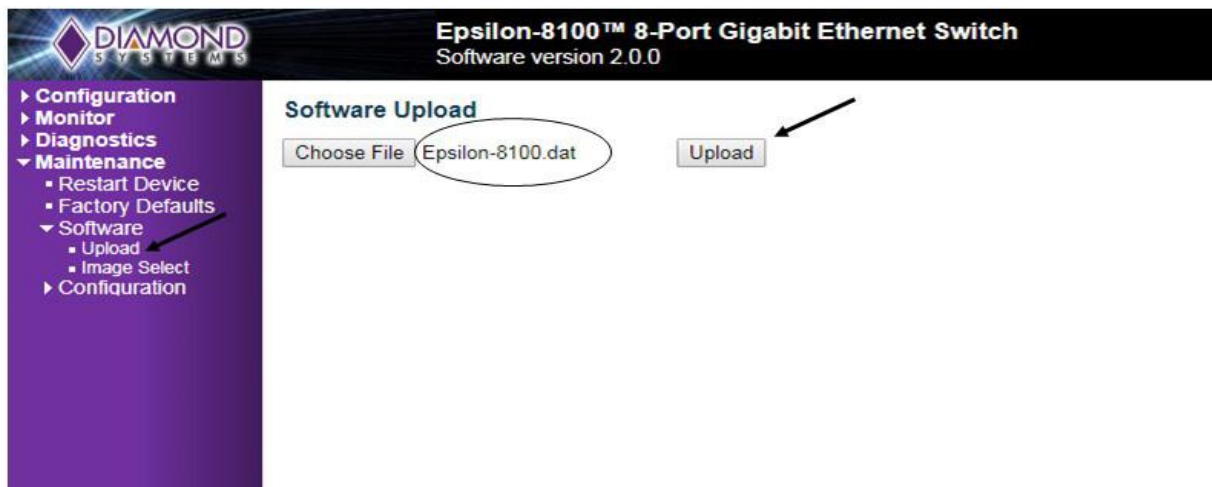

Figure 12 – Firmware Upgrade

7.1.10 Save Startup Configuration

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot. The following example shows the Save Startup configuration:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to Maintenance -> Configuration -> Save Startup-Config (refer to the figure below)

3. Click on Save Configuration
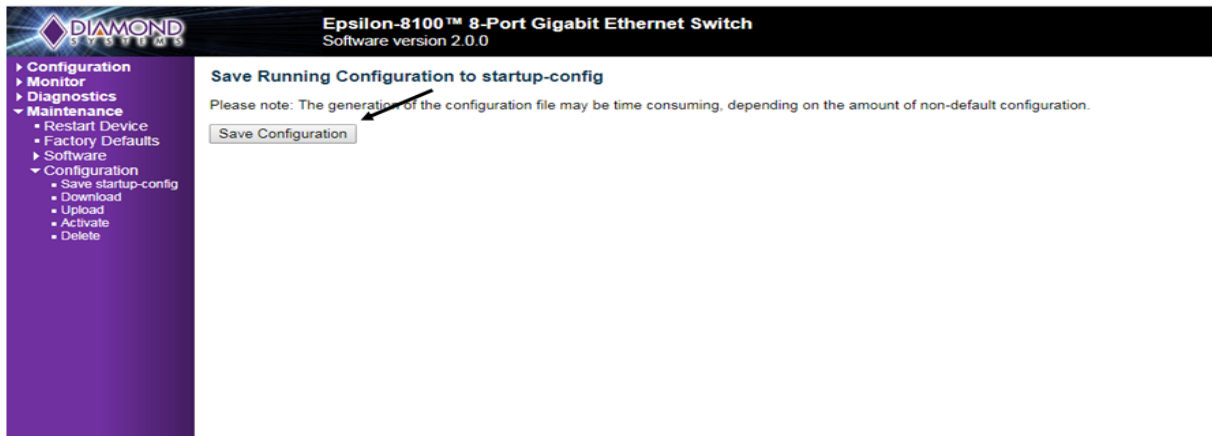
Figure 13 – Saving Startup Configuration

7.1.11 Factory Defaults

A 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 shows the steps for restoring the factory defaults:

1. Connect to the web interface of EPS-8100 switch

2. Navigate to maintenance -> Factory defaults

3. Click on Yes for an confirmation message (refer to the figure below)

Figure 14 – Restore Factory defaults

The switch can also be reset to the factory default settings by connecting an Ethernet cable between ports 1 & 2 and powering on the switch. The default configuration is loaded, but not restored. To save a loaded configuration as the default permanently, the switch must be accessed using the default IP address and the configuration saved.

7.1.12 Physical Reset

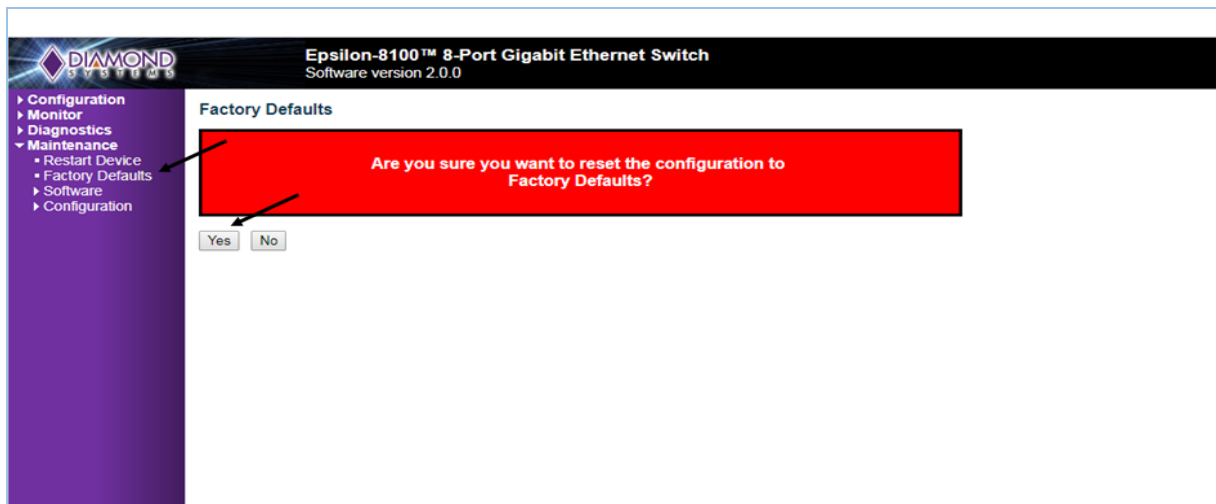A user can load the configuration of the switch to factory defaults using a port loop-back. This also loads the factory default IP configuration. This option may be required if the switch IP address is not known and/or the switch is not communicating over the network. The new configuration is available immediately. The following procedure shows the steps for resetting the factory defaults using loop-back:

      a. Loopback between Port-1 & Port-2 of the main switch using standard Ethernet cable

      b. Power on the board and wait till the Ethernet connection is established

      c. Remove the loopback cable

Note: The factory default configuration is only loaded and not stored. To permanently store this configuration, refer to section 7.1.9.

8. SPECIFICATIONS

The specifications for Epsilon-8100 are summarized in the following table.

Ethernet switch	8-port, layer 2+ switch Built-in 416MHz MIPs 24KEC microcontroller for configuration and management
Number of ports	8 10/100/1000Mbps copper Ethernet ports with non-blocking wire-speed performance
On-board memory	4Mb packet memory Shared memory buffer with per=port and CoS memory management
Frame buffer	Jumbo frame support at all speeds
MEF	Hierarchical MEF compliant policing & scheduling MEF E-Lane, E-Line, and E-Tree services
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
DSCP	DSCP remarking for both IPv4 and IPv6 frames
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
RSTP	Rapid spanning tree protocol (IEEE 802.1W) and MTSP
Security	Advanced security and prioritization available through multistage TCAM engine
Power management	ActiPHY and PerfectReach power management VeriPHY cable diagnostics
Serial port	1 RS-232 for host interface
Indicator LEDS	16 status LEDs, two per port 2 general purpose LEDs
Classifier	Programmable multi-layer classifier with 4 QoS classes
RSTP	Rapid spanning tree protocol (IEEE 802.1W
Standalone Capable	Can operate as a standalone network switch or in combination with a host computer
Power Input	+5-36V DC/DC power supply
Power consumption	5.4W typical at +5VDC with all 8 ports active, approx. 0.26W less for each inactive port
MTBF	624,170 hours at 20°C
Form factor	PC/104 (3.55' x 3.775") Height: 15.7mm with heatsink
Operating temp	-40°C to +85°C (-40°F to +185°F)
Weight	3.5oz (99g) with heatsink
RoHS	Compliant

The timing specifications for the board are summarized in the following table.

Time to Login and alive LED flashing after power-on, power cycle, or reboot	8 sec.
Time for ports to reconnect after power-on, power cycle, or reboot	15 sec.
Time for all ports to start passing data after power-on, power cycle, or reboot	<30 sec. (typical 24-26 sec.)
Time for all ports to start passing data after restoring factory defaults	8 sec.

APPENDIX A   SUPPORTED MIBS

Epsilon-8100 supports the following management information bases (MIBs). Each MIB contains definitions and information regarding the properties of managed resources and the services that the agents support.

The following MIBs are supported by Epsilon-8100:

- LLDP
- RFC1213 Interfaces
- RFC1213 System
- RFC1213 SNMP
- RFC1213 IP
- RFC1213 TCP
- RFC1213 UDP
- RFC1213 IGMP Event MIB
- RFC1213 Differentiated Services Architecture MIB
- RFC1213 Event MIB
- RFC4188 Dot1D
- RFC3635 Transmission

APPENDIX B   UPGRADING BOOTLOADER & APPLICATION IMAGE

This section provides instructions on how to upgrade the boot loader and application image. The upgrade process has the below main components.

1. Load the new RedBoot image and store it in the flash
2. Create a new file system
3. Create the managed flash file system entries and loading application
4. Create a boot script

The following section describes the procedure step-by-step.

Note: Updating boot loader is optional.If user wants to update only application, skip steps 4-22.

Load the new RedBoot image and store it in the flash.

1. Open TeraTerm and connect to the device using (38400, 8, N, 1).

    Note: If upgrading the software from version 1.0.1 to 2.0.0, use (115200, 8, N, 1).

2. Reset the device by power cycle or pressing the reset push-button.

3. Within three seconds press Ctrl-C. This will bring up the RedBoot command prompt.

4. Type the following command

    load -r -m xmodem -b 0x80040000

5. Download the ***redboot.bin*** file from TeraTerm. Select File > Transfer > XMODEM > Send,

    select ***redboot.bin*** file, and click Open.

6. Wait for the transfer to complete. Make sure that 'Teraterm XMODEM Send' popup window shows 100%. If not ,repeat steps 4 and retry.

7. Create a new redundancy-supporting file system.

    fis init

8. Press *y* when prompted to continue.

9. Overwrite the current RedBoot image with the new version.

   fis create -b 0x80040000 -r 0 -l 0x40000 -f 0x40000000 -e 0 RedBoot

   If the above step not showing the following length incorrect error,skip steps 10-20 and go to step 21.

   "Image found, but length is incorrect (present image size 0x20000)"

10. Transfer the RAM bootable image to RAM. For this, from redboot prompt, type the following

    load -m xmodem -r -b 0x80040000

11. Download the **redboot_ram.bin** file from TeraTerm. Select File > Transfer > XMODEM > Send,

    select **redboot_ram.bin** file, and click Open.

12. Wait for the transfer to complete. Make sure that Teraterm XMODEM send popup window shows 100%. If not,repeat steps 10 and retry.

13. Once the transfer is complete, switch over to ram bootloader image by issuing the following command

    go 0x800400BC

    Note:if upgrading the software from version 1.0.1 to 2.0.0,need to change the TeraTerm baudrate from 115200 to 38400.Because ram bootloader image is running at 38400 baudrate.

14. Interrupt the booting process by entering *Ctrl+C.*

15. Issue *'fis init'* command. This will be followed by a confirmation question. Give yes (*y*).

16. Now load the regular **redboot.bin** image to the ram location 0x80080000

    load -m xmodem -r -b 0x80080000

17. Select File > Transfer > XMODEM > Send,select **redboot.bin** file, and click Open.

18. Wait for the transfer to complete then create a new redundancy-supporting file system.

    fis init

19. Press *y* when prompted to continue.

20. Overwrite the current RedBoot image with the new image.Type the following command.

    fis create -b 0x80080000 -r 0 -l 0x40000 -f 0x40000000 -e 0 RedBoot

    This will be followed by a confirmation question. Give yes (*y*).

21. Reset the device with the following command.

    reset

22. Within three seconds, press *Ctrl-C.*

Create a new file system

23. Create a configuration structure entry.

    mfill -b 0x80040000 -l 0x40000 -p 0xff -1

    fis create -r 0 -e 0 -b 0x80040000 -l 0x40000 -f 0x40040000 conf

24. Create a stack configuration structure entry.

    mfill -b 0x80040000 -l 0x100000 -p 0xff -1

    fis create -r 0 -e 0 -b 0x80040000 -l 0x100000 -f 0x40080000 stackconf

25. Create a syslog entry.

    fis create -r 0 -e 0 -b 0x80040000 -l 0x40000 -f 0x40180000 syslog

Create the managed flash file system entries

26. Load the file **Epsilon-8100.gz**.

> *load -r -b 0x80040000 -m xmodem*

27. From TeraTerm, choose File > Transfer > XMODEM > Send..., select *Epsilon-8100.gz*, and click Open.

28. Create the managed and managed.bk file entries.

> *fis create -r 0x80040000 -e 0x800400bc -l 0x600000 -f 0x401c0000 managed*
>
> *fis create -r 0x80040000 -e 0x800400bc -l 0x600000 -f 0x407c0000 managed.bk*

Note: File names managed and managed.bk must not be changed. The upgrade function of the application relies on these names.

Create a boot script

29. Start a new script.

> *fconfig -i*

30. Press y when prompted to continue. This will show "Run script at boot: false" selection.

31. Change '*false*' to '*true*' for the selection "Run script at boot: false" and Hit <Enter> Key

32. Enter the following commands

> *fis load -d managed*
>
> *go*
>
> *fis load -d managed.bk*
>
> *go*

33. Hit <Enter> Key. This will show " Boot script timeout (1000ms resolution): 0" selection.

34. Change '*0*' to '*3*' for the selection "Boot script timeout (1000ms resolution): 0".

35. If the application software version is 2.0.0 or above , Set the baud rate to *38400* in the selection "Console baud rate: *38400*". else use *115200*.

36. Press *y* to when prompted to continue.

37. Reset the device with the following command.

> *reset*