PL-1000IL 3.2 INSTALLATION AND CONFIGURATION MANUAL

PL-1000IL 3.2 Installation and Configuration Manual

Contents

List of Figures

List of Tables

1 Introduction

This chapter provides an overview of the PL-1000IL.

In this Chapter

1.1 Overview

The PL-1000IL is a compact 1U WDM access/transport device that is designed to extend the power link budget of DWDM solutions. It provides amplification for a range of optical solutions from 4 wavelengths to 40 wavelengths and incorporates several types of low-noise EDFAs: Booster, Inline, Pre-Amplifier, Midstage and Raman.

Depending on the customer requirements, the PL-1000IL can operate in either APC or AGC mode.

- The AGC operation mode enables seamless wavelength add/drop functionality without interference to the other active channels. In addition, the EDFA gain is controlled, adjusted and monitored by the user.
- The APC operating mode allows the maintenance of constant output power.

The EDFAs are gain-flattened and have low Optical Signal to Noise Ratio (OSNR), thus enabling cascading of several EDFAs to form an amplified link over long distance.

The PL-1000IL is ideal for applications such as:

- Extending the optical link budget to meet distance and attenuation requirements of DWDM networks
- Supporting high-throughput Metro Ethernet connectivity over long distances
- Upgrading the optical link budget to support 10G services
- Reducing number of regenerators and sites along fiber
- Overcoming old fiber infrastructure high loss

The PL-1000IL is a highly integrated device that can incorporate up to two EDFA modules, optional DCM, and an optical switch for both protected and unprotected modes.

1.1.1 Main Features

The PL-1000IL combines the following key features:

- Up to two amplifiers can be integrated in the device
- Amplifier types: Booster, Inline, Mid-stage, or Pre-Amp
- Built-In Eye Safety Mechanism
- Protocol and Data independent
- Supporting 4/8/16/32/40 Wavelengths and Full C-Band
- Optional integrated Dispersion Compensation Module (DCM)
- Two 100M Optical Supervisory Channel (OSC) management channels based on SFP optics for remote management
- Automatic Laser Shutdown (ALS) on all optical ports
- Provides the following management protocols for configuration, monitoring, and service provisioning:
  - CLI over a serial or Telnet/SSH connection
  - Web-based HTTP/HTTPS management
  - SNMP management interface
  - Remote Authentication Dial In User Service (Radius) protocol for centralized remote user authentication
  - Syslog protocol
  - Simple Network Time Protocol (SNTP) for network timing
  - TFTP and FTP for file upload and download
- Operates on single or dual fiber solutions
- Pluggable FAN unit for improved maintainability
- AC or DC, single or dual pluggable power supply units (PSUs)
- Supports Operations, Administration, and Maintenance (OAM) functions:
  - Alarm and Event fault
  - Performance monitoring (PM)
  - External alarms

1.1.2 Typical Application

Typical applications for the PL-1000IL include:

- Extending the optical link power budget to meet distance and attenuation requirements of DWDM networks
- Providing high throughput Metro Ethernet connectivity over long distances

- Upgrading the optical link budget to support 10G services
- Reducing the number of regenerators and sites along the fiber
- Overcoming old fiber infrastructure high loss

The following figure shows some typical configurations for the PL-1000IL:

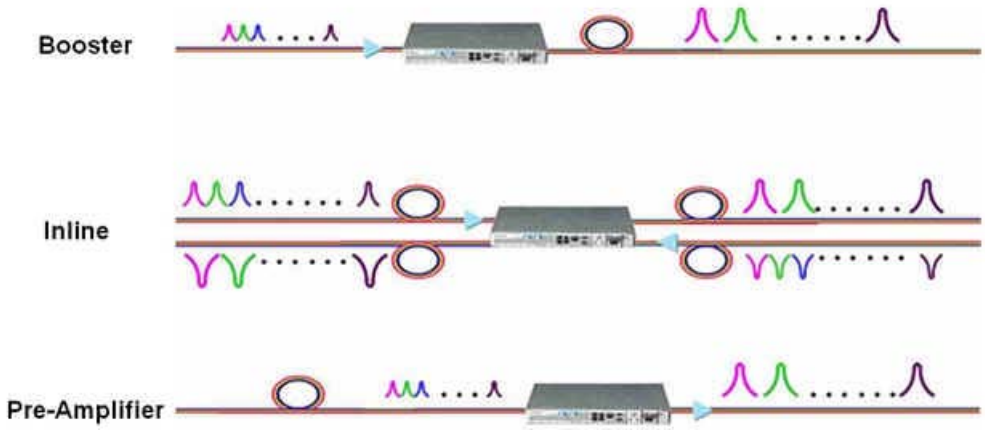


Figure 1: PL-1000IL Typical Applications

1.1.3 Physical Description

The PL-1000IL is a compact 1U unit intended for installation in 19-inch or 23-inch racks or placed on desktops or shelves.

All connections are made to the front panel. The PL-1000IL front panel also includes LEDs that indicate its operating status.

The following figure shows a general view of the PL-1000IL.

Figure 2: General View of the PL-1000IL

1.2 Configurations

The PL-1000IL is designed in a modular way, thereby enabling many configurations and applications.

1.2.1 PL-1000IL Configurations

The PL-1000IL can be ordered with the configurations described in this section.

1.2.1.1 EDFA Module Configurations

The PL-1000IL can be ordered with two, one, or no EDFA modules. Each EDFA can be a Booster or Pre-Amp.

1.2.1.2 DCM Configurations

The PL-1000IL can be ordered with or without a DCM module.

1.2.1.3 Optical Switch Configurations

The PL-1000IL can be ordered with or without an Optical Switch module.

1.2.1.4 Example Configurations

The following are some examples of the available configurations of the PL-1000IL:

- PL-1000IL Booster configuration:

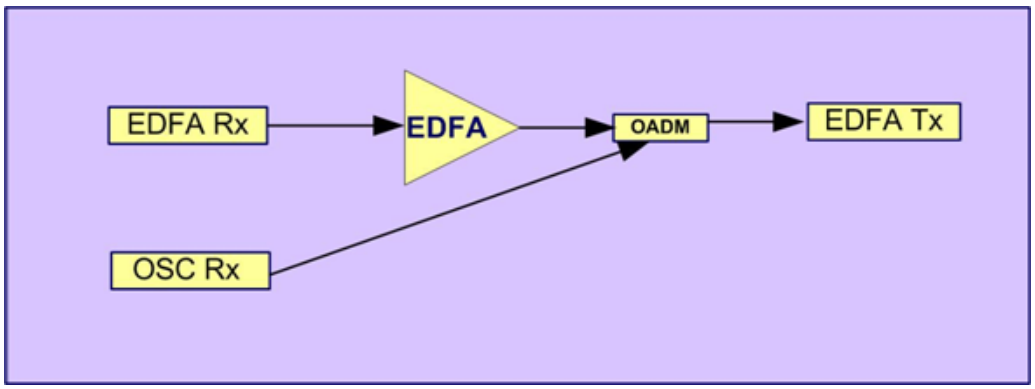


Figure 3: PL-1000IL with Booster

- PL-1000IL Pre-Amp configuration:

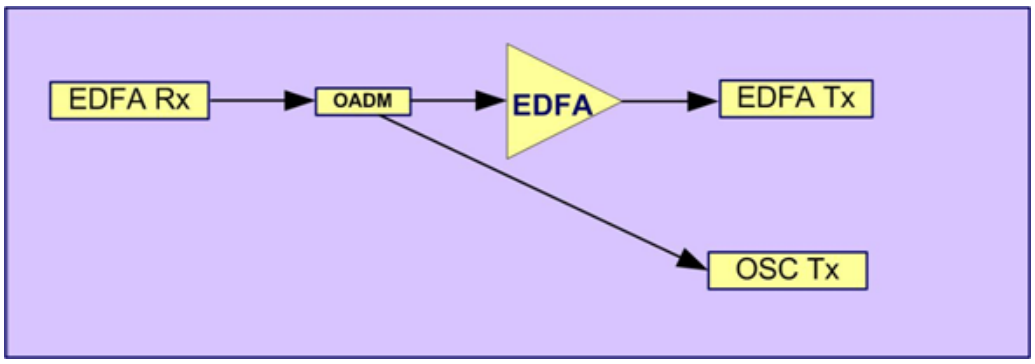


Figure 4: PL-1000IL with Pre-Amp

- PL-1000IL Inline configuration:

  This configuration can be used in Ring or Linear Add and Drop topologies.

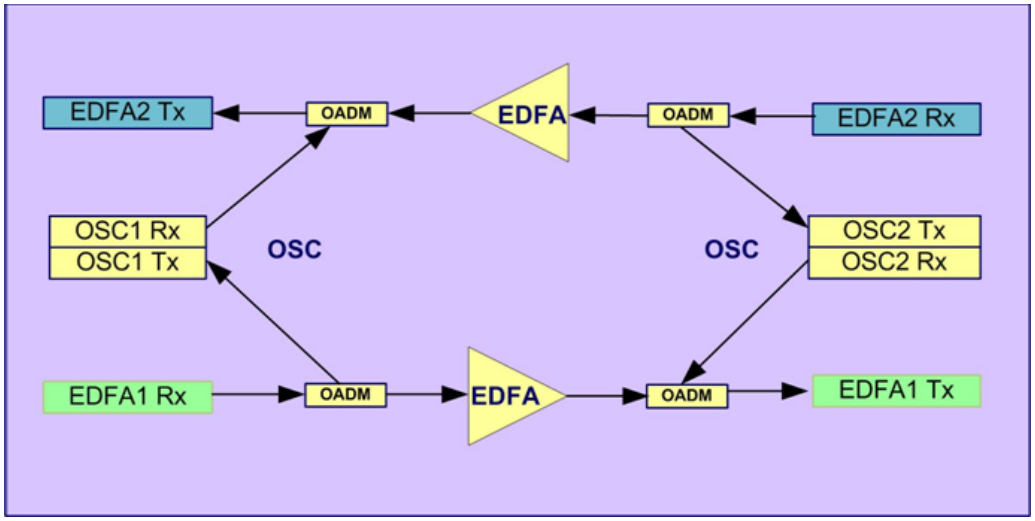


Figure 5: Inline PL-1000IL with two Inline Amplifiers

- PL-1000IL Mid-Stage configuration:

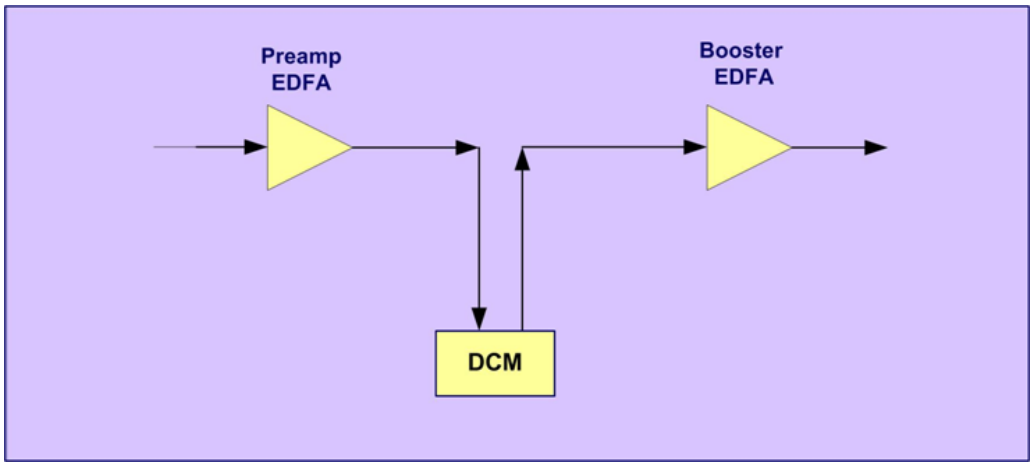


Figure 6: Mid-Stage PL-1000IL with Pre-Amp, Booster, and DCM

- PL-1000IL Booster and Optical Switch configuration:

  This is Point-to-Point topology.

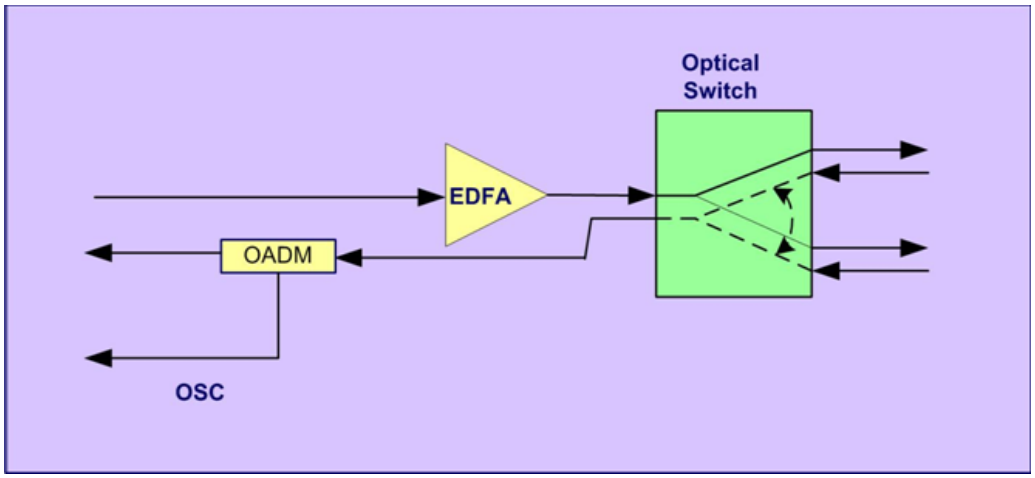


Figure 7: PL-1000IL with Booster and Optical Switch

- PL-1000IL Pre-Amp and Optical Switch configuration:

  This is Point-to-Point topology.

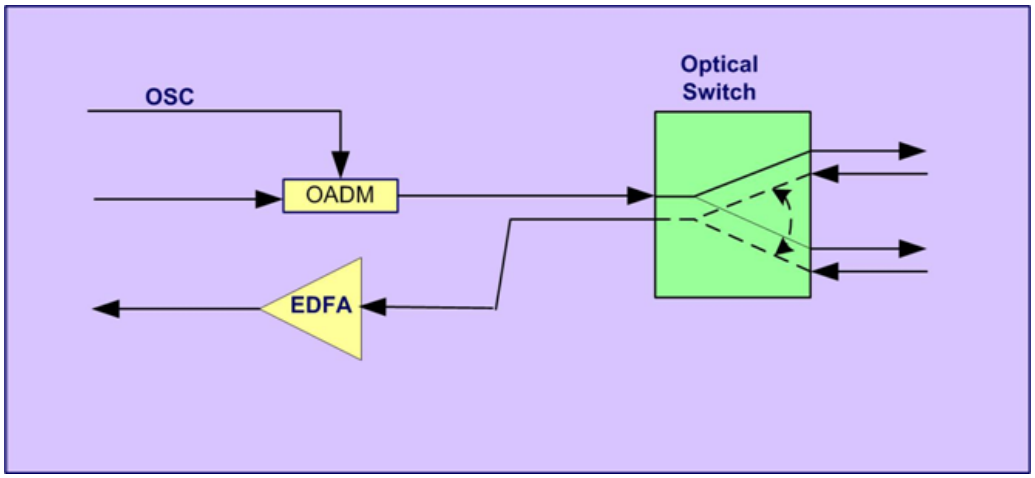


Figure 8: PL-1000IL with Pre-Amp and Optical Switch

1.3 Functional Description

This section describes some of the functionality of the PL-1000IL.

1.3.1 PL-1000IL Ports

This section describes the PL-1000IL ports.

1.3.1.1 Optical Ports

The PL-1000IL unit has the following types of optical ports:

- MNG ports: Accept SFP optical transceivers
- In inline configuration:
  - EDFA1 and EDFA2: LC connectors
  - OSC1 and OSC2: LC connectors
- In protected point-to-point configuration
  - COM, COM1 and COM2: LC connectors
  - OSC: LC connector

For detailed information regarding the PL-1000IL connectors, see Connection Data (p. 177).

1.3.1.2 EDFA Ports

The EDFA ports are connected to the network line. They carry the common optical signal that aggregates the optical channels.

If there is a single EDFA module it will be connected to EDFA1 port. If there are two EDFA modules they will be connected to EDFA1 and EDFA2 ports.

The following table provides information regarding the fiber and connector specifications for the EDFA ports.

Table 1: EDFA Port Specifications

Specification	Requirement
Fiber Type	Single mode
Fiber Size	2 mm optical
Connector Type	LC with protective shutters
Port Type	Optical EDFA port

1.3.1.3 OSC Ports

The OSC ports are connected to the local management ports to provide remote management. In point to point configurations, the PL-1000IL uses a single OSC port (OSC1). In ring configurations, both OSC1 and OSC2 are used.

The following table provides information regarding the fiber and connector specifications for the OSC ports.

Table 2: OSC Port Specifications

Specification	Requirement
Fiber Type	Single mode
Fiber Size	2 mm optical
Connector Type	LC with protective shutters

Specification	Requirement
Port Type	Optical OSC port

1.3.1.4 ALARM Port

The PL-1000IL has an ALARM (or External Alarm) port for the environmental alarm. This port supports one input and one output.

For more information, see Connection Data (p. 177).

1.3.1.5 COM Ports

The COM, COM1 and COM2 ports are used in protected configuration of the PL-1000IL.

- COM port connected to the optical signal
- COM1 port connected to the Working fiber.
- COM2 port connected to the Protection fiber.

The following table provides information regarding the fiber and connector specifications for the COM port.

Table 3: COM Port Specifications

Specification	Requirement
Fiber Type	Single mode
Fiber Size	2 mm optical
Connector Type	LC with protective shutters
Port Type	Optical COM port

1.3.1.5.1 APS for COM Ports

The PL-1000IL uses optional optical switch to provide signal protection to the client signal.

In protected configuration, the PL-1000IL supports unidirectional, non-revertive, 1+1 facility protection. The facility protection ensures service continuity in case of a fiber break. The APS is supported in point-to-point topologies

- **Unidirectional**: Each side selects the Active line independently.
- **Non-revertive**: To reduce the number of traffic hits, no switching occurs if the traffic is restored on the Standby line while there are no faults on the Active line.

1+1 facility: The transmitted traffic is copied to both fibers.

1.3.1.6 Management Ports

This section describes the PL-1000IL management ports.

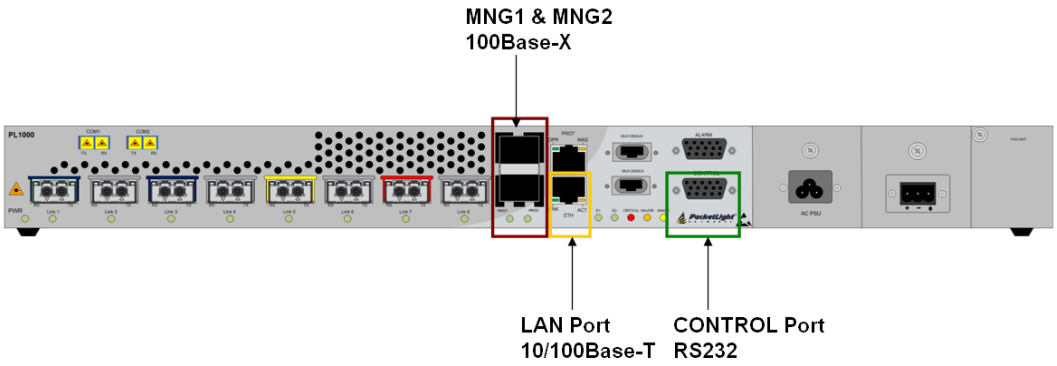


Figure 9: PL-1000IL Management Ports

1.3.1.6.1 CONTROL Port

The RS-232 asynchronous supervisory port has a DCE interface that supports a data rate of 9600 bps. For more information, see Connection Data (p. 177).

Initial configuration of PL-1000IL is performed using the CLI management interface from any ASCII terminal (dumb terminal or personal computer (PC) running a terminal emulation program) directly connected to the PL-1000IL serial control connector.

After the initial configuration, the PL-1000IL may be managed, supervised, and configured by a Web browser or an SNMP network management system.

The following table provides information regarding the specifications for the CONTROL Port.

Table 4: CONTROL Port Specifications

Specification	Requirement
Interface type	Serial RS-232 asynchronous DCE
Connector type	9-pin D-type female

1.3.1.6.2 ETH Port

The PL-1000IL can be accessed through the 10/100 Base-T management port using any of the following:

- CLI over a serial or Telnet/SSH connection
- Web management over HTTP/HTTPS
- SNMP over UDP

The following table provides information regarding the specifications for the ETH port.

Table 5: ETH Port Specifications

Specification	Requirement
Interface type	10/100 Base-T
Connector type	RJ-45 Category 5

1.3.1.6.3 MNG Ports

The PL-1000IL is equipped with two SFP based MNG ports labeled "MNG 1" and "MNG 2". These ports enable remote management of a PL-1000IL unit or local cascading in a multi-chassis application.

This management channel may be multiplexed as an extra OSC wavelength.The PL-1000IL supports two OSCs for multi-chassis application and for remote management with facility protection. The facility protection is for the management network when the two management ports are active and there is more than one management route between the nodes. In point-to-point topology without protection, only one OSC port is needed on each side (it can be either of the two). For a protected point-to-point or ring topology, both OSC ports should be used.

The PL-1000IL uses the standard Rapid Spanning Tree Protocol (RSTP) protocol to uniquely determine the route for the management traffic between the nodes, and to dynamically change the management route should a facility failure occur.

For more information, see Connection Data (p. 177).

1.3.2 PL-1000IL Modules

This section describes the PL-1000IL modules.

1.3.2.1 EDFA Modules

The PL-1000IL may be ordered with one or two optional EDFA modules that are used to amplify the optical power of the DWDM signal. The EDFA modules can be used as a Booster and/or Pre-Amp.

- **Booster EDFA**: Used on the Tx optical path.
- **Pre-Amp EDFA**: Used on the Rx optical path.

1.3.2.2 Optical Switch Module

The PL-1000IL may be ordered with an optional Optical Switch module.

On the input side, the Optical Switch enables incoming signals in optical fiber to be selectively switched from one fiber to another.

On the output side, the optical signals are duplicated to both fibers.

The optical switch is applicable only to point-to-point topology.

The Optical Switch performs APS based on the received optical power level of the incoming aggregated optical signal.

In protected configuration, the PL-1000IL supports unidirectional, non-revertive, 1+1 facility protection APS. The facility protection ensures service continuity in case of a fiber break.

- Unidirectional: Each side selects the Active line independently.
- Non-revertive: To reduce the number of traffic hits, no switching occurs if the traffic is restored on the Standby line while there are no faults on the Active line.
- 1+1 channel: The transmitted traffic is copied to both lines.

The facility protection ensures service continuity in case of a fiber break.

1.3.2.3 DCM Module

The PL-1000IL may be ordered with a DCM module that is used for dispersion compensation in Inline topologies.

1.3.2.4 Power Supply Unit

PL-1000IL is available with AC and DC power supplies:

- **AC**: 100 to 240 VAC, 50/60 Hz, 1.5A maximum
- **DC**: -48 VDC, 3A maximum

The maximum power consumption of the PL-1000IL is 24W.

The PL-1000IL may be ordered with one or two AC and/or DC power supply units. The power supplies are redundant and replaceable without causing traffic interference.

NOTE: Both AC and DC PSUs can be used in the same unit.

The unit does not have a power ON/OFF switch, and therefore starts operating as soon as the power is connected.

1.3.2.5 FAN Unit

The PL-1000IL is available with a pluggable and replaceable FAN unit. The air intake vents are located on the right side. The FAN unit has an automatic speed control mechanism that supports lower noise, improved MTBF and power saving.

⚠ **CAUTION:** Air intake vents should be clear of obstruction.

1.3.3 Management Functionality

The management functionality includes:

- Viewing fault alarms and events
- Configuring and viewing device parameters

- User access control with user and password authentication
- Viewing performance monitoring statistics
- Maintenance operations such as software upgrade and system restart
- Viewing the network topology

1.3.3.1 Management Protocols

This section describes the management protocols.

1.3.3.1.1 CLI Management

For initial IP configuration and several other management tasks, the PL-1000IL supports CLI ASCII management. CLI management is accessible via the CONTROL serial port or Telnet/SSH connection.

For more information, see CLI (p. 163).

1.3.3.1.2 Web-based Management

The PL-1000IL supervision and configuration functions can be performed using a standard Web browser.

For detailed information on Web-based management, see Configuration Management (p. 93).

1.3.3.1.3 SNMP Management

PL-1000IL devices can also be managed by PacketLight's LightWatch™ NMS/EMS, by RADview™, or by other third-party SNMP-based management systems.

For more information about available PL-1000IL MIBs and LightWatch™, contact PacketLight Technical Support.

1.4 Technical Specifications

Optical Amplifier (EDFA)	Number of Modules	0, 1, 2
	Output Power	• **Booster**: 14 dBm, 17 dBm, 20 dBm, 23 dBm • **Pre-Amp**: +5 dBm
	Optical Gain	• **Booster**: +10 to +22 dB • **Pre-Amp**: +18 dB
	Input Power	• **Booster**: -24 to +16 dBm • **Pre-Amp**: -36 to -15 dBm
	AGC	Keeps the amplifier gain fixed without dependency when adding or removing services.
	APC	Keeps the amplifier output power fixed without dependency when adding or removing services.
	Eye Safety	Automatic laser power reduction upon fiber cut or disconnection.

Dispersion Compensation Module (DCM)	Number of Modules	0 or 1
	Range	40 to 240 km in 20 km steps
	Fiber Types	One of: • ITU G.652 • ITU G.653 • ITU G.654 • ITU G.655
	Spacing	50/100 GHz
Supervisory and Management Port	CONTROL Port	Used for initial configuration of the node IP or for local access to CLI. • **Interface**: RS-232 • **Connector**: 9-pin D-type, female • **Format**: Asynchronous • **Baud rate**: 9600 bps • **Word format**: 8 bits, no parity, 1 stop bit, and 1 start bit • **Flow control**: None
	ETH Port	Management LAN port for out-of-band access. • **Interface**: 10/100 Base-T • **Connector**: RJ-45 **NOTE:** Initial IP configuration can be done via RS-232.
	MNG1 and MNG2 Ports	Optical management ports: • **Interface**: 100 Base-FX • **Connector**: SFP transceiver • **Single Mode**: ▪ **CWDM**: 1290 nm or 1310 nm ▪ **DWDM**: 1490 nm or 1510 nm • **Multi-mode fiber**: 850 nm **NOTE:** IP of the MNG port can be configured using the Web application.
COM Ports	COM, COM1 and COM2 (in protected configuration)	One or two fixed duplex LC connectors. • **Fiber type**: Single mode • **Fiber size**: 2 mm optical • **Connector type**: LC with or without protective shutters • **Port type**: Optical COM port
Environment Alarm	ALARM Port	Used for external office alarms. • **Connector**: DB-9, female • **Environmental**: 1 input and 1 output

System LEDs	PWR	• **Green blinking**: Power-up stage • **Green**: Normal operation
	CRT	• **OFF**: No Critical alarm detected • **Red**: Critical alarm detected
	MAJ	• **OFF**: No Major alarm detected • **Red**: Major alarm detected
	MIN	• **OFF**: No Minor alarm detected • **Red**: Minor alarm detected
MNG Port LEDs	MNG1 and MNG2	• **OFF**: Admin Down • **Green**: Normal operation • **Red**: Alarm detected
Amplifier LEDs	E1 and E2	• **OFF**: Admin Down or EDFA module is not installed • **Green**: The corresponding amplifier is operational (DWDM applications only) • **Red**: EDFA failure detected
PROT Port LEDs	OPR	Unused
	MASTER	Unused
ETH Port LEDs	LINK	• **OFF**: The port is disconnected • **Green**: Normal operation
	ACT	• **Yellow blinking**: Transmit and/or receive activity detected on the port.
PSU LEDs	PWR	• **Green**: Normal operation • **Red**: PSU failure detected • **OFF**: PSU is not installed
Network Management	Protocols	• CLI over RS-232 or Telnet/SSH connection • Web-based HTTP/HTTPS management • SNMPv2c • Radius • Syslog • SNTP • TFTP and FTP for file upload and download
	Alarms	Current alarms are available. Each alarm is time stamped.
	Event Messages	Last 512 events and audit messages are available. Each message is time stamped.
	Log File	The events and audit messages are stored in the PL-1000IL system log files, which can be exported to a text file for offline viewing.
ALS	Optical Ports	ALS is available for the MNG ports.

Power Supply	Number of Units	1 or 2
	Redundancy	Single or dual feeding, pluggable
	AC Source	100 to 240 VAC, 50/60 Hz, 1.5A maximum
	DC Source	–48 VDC, 3A maximum
	Power Consumption	24W maximum
	Protective Earthing Conductor	18 AWG minimum
Fans	Maintenance	Replaceable and hot pluggable
	Flow	1.14 cubic meter/minute (4 fans 0.286 m3/min each)
Physical Dimensions	Height	44 mm/1.733" (1U)
	Width	440 mm/17.32"
	Depth	230 mm/9.05"
	Weight	5.5 kg/12. 1lbs maximum
	Mounting Options	19", 23", ETSI rack mountable
Environment	Normal Operating Temperature	0° to +45°C/+32° to +113°F
	Storage Temperature	-25° to +55°C/-13° to +131°F
	Normal Operating Humidity	5% to 85% RH non-condensing
	Storage Humidity	Up to 95% RH
EMC	Standards	• ETSI EN 300 386 • ETSI EN 55024 • ETSI EN 55022 • IEC/EN 61000-3-2 • IEC/EN 61000-3-3 • IEC/EN 61000-4-2 • IEC/EN 61000-4-3 • IEC/EN 61000-4-4 • IEC/EN 61000-4-5 • IEC/EN 61000-4-6 • IEC/EN 61000-4-11 • AS/NZS CISPR 22 • FCC Class A CFR 47 Part 15 Subpart B
Safety	Standards	• IEC/EN 60825-1 • IEC/EN 60825-2 • IEC/EN/UL 60950-1 • Telcordia SR-332, Issue 2 • RoHS 5/6

2 Installation

This chapter provides installation information and instructions for the PL-1000IL.

In this Chapter

2.1 Safety Precautions

This section describes the safety precautions.

2.1.1 General Safety Precautions

The following are the general safety precautions:

- The equipment should be used in a restricted access location only.
- No internal settings, adjustments, maintenance, and repairs may be performed by the operator or the user; such activities may be performed only by skilled service personnel who are aware of the hazards involved.
- Always observe standard safety precautions during installation, operation, and maintenance of this product.

2.1.2 Electrical Safety Precautions

WARNING: Dangerous voltages may be present on the cables connected to the PL-1000IL:

- Never connect cables to a PL-1000IL unit if it is not properly installed and grounded.
- Disconnect the power cable before removing a pluggable power supply unit.

  GROUNDING: For your protection and to prevent possible damage to equipment when a fault condition occurs on the cables connected to the equipment (for example, a lightning stroke or contact with high voltage power lines), the case of the PL-1000IL unit must be properly grounded at all times. Any interruption of the protective (grounding) connection inside or outside the equipment, or the disconnection of the protective ground terminal, can make this equipment dangerous. Intentional interruption is prohibited.

Before connecting any cables, the protective ground terminal of the PL-1000IL must be connected to a protective ground (see Connection Data (p. 177)).

The grounding connection is also made through the power cable, which must be inserted in a power socket (outlet) with protective ground contact. Therefore, the power cable plug must always be inserted in a socket outlet provided with a protective ground contact, and the protective action must not be negated by use of an extension cord (power cable) without a protective conductor (grounding).

Whenever PL-1000IL units are installed in a rack, make sure that the rack is properly grounded and connected to a reliable, low resistance grounding system.

2.1.2.1 Laser Safety Classification

The laser beam of the PL-1000IL optical modules is off when the status of the port is set to **Admin Down**.

In general, the PL-1000IL unit is equipped with laser devices that comply with Class 1M. However, the PL-1000IL laser complies with the higher Class 3B when equipped with Booster EDFA with the output power of 23 dBm.

According to the IEC EN60825-2 standard, the following warning applies to Class 1M laser products.

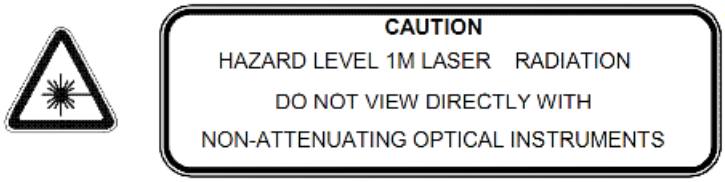


Figure 10: Class 1M Laser Warning

The following warning applies to Class 3B laser products.

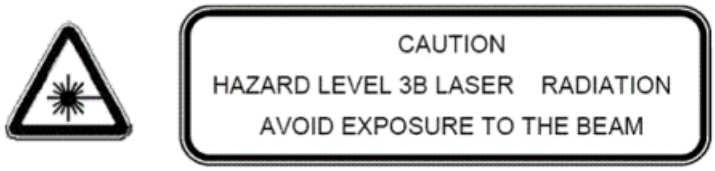


Figure 11: Class 3B Laser Warning

PL-1000IL units are shipped with protective covers installed on all the optical connectors. Do not remove these covers until you are ready to connect optical cables to the connectors. Keep the covers for reuse, to reinstall the cover over the optical connector as soon as the optical cable is disconnected.

2.1.2.2 Laser Safety Statutory Warning and Operating Precautions

All personnel involved in equipment installation, operation, and maintenance must be aware that the laser radiation is invisible. Therefore, the personnel must strictly observe the applicable safety precautions and, in particular, must avoid looking straight into optical connectors, either directly or using optical instruments.

In addition to the general precautions described in this section, be sure to observe the following warnings when operating a product equipped with a laser device. Failure to observe these warnings could result in fire, bodily injury, and damage to the equipment.

WARNING: To reduce the risk of exposure to hazardous radiation:

- Do not try to open the enclosure. There are no user serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only authorized service technicians to repair the unit.

2.1.3 Protection against Electrostatic Discharge

An electrostatic discharge (ESD) occurs between two objects when an object carrying static electrical charges touches or is brought near the other object. Static electrical charges appear as a result of friction between surfaces of insulating materials or separation of two such surfaces. They may also be induced by electrical fields.

Routine activities, such as walking across an insulating floor, friction between garment parts, and friction between objects, can easily build charges up to levels that may cause damage, especially when humidity is low.

CAUTION: PL-1000IL internal boards contain components sensitive to ESD. To prevent ESD damage, do not touch internal components or connectors. If you are not using a wrist strap, before touching a PL-1000IL unit or performing any internal settings on the PL-1000IL, it is recommended to discharge the electrostatic charge of your body by touching the frame of a grounded equipment unit.

Whenever feasible during installation, use standard ESD protection wrist straps to discharge electrostatic charges. It is also recommended to use garments and packaging made of anti-static materials, or materials that have high resistance, yet are not insulators.

2.2 Site Requirements

This section describes the PL-1000IL site requirements.

2.2.1 Physical Requirements

The PL-1000IL units are intended for installation in 19-inch or 23-inch racks or placed on desktops or shelves.

All the connections are made to the front panel.

2.2.2 Power Requirements

AC-powered PL-1000IL units should be installed within 1.5m (5 feet) of an easily accessible, grounded AC outlet capable of furnishing the required AC supply voltage, of 100 to 240 VAC, 50/60 Hz, and 1.5A maximum.

DC-powered PL-1000IL units require a -48 VDC, 3A maximum DC power source with the positive terminal grounded. In addition, the DC power connector contains the chassis (frame) ground terminal (see Power Connectors (p. 180)).

2.2.3 Ambient Requirements

The recommended ambient operating temperature of the PL-1000IL is 0° to +45°C/+32° to +113°F, at a relative humidity of 5% to 85%, non-condensing.

The PL-1000IL is cooled by free air convection and a pluggable cooling FAN unit. The air intake vents are located on the right side.

⚠ **CAUTION:** Do not obstruct these vents.

The PL-1000IL contains a fan speed control for lower noise, improved MTBF and power save.

2.2.4 Electromagnetic Compatibility Considerations

The PL-1000IL is designed to comply with the electromagnetic compatibility (EMC) requirements of Sub Part J of FCC Rules, Part 15, for Class A electronic equipment and additional applicable standards.

To meet these standards, the following conditions are necessary:

- The PL-1000IL must be connected to a low resistance grounding system.
- Whenever feasible, shielded cables must be used.

2.3 PL-1000IL Front Panel

The following figure illustrates the PL-1000IL front panel.

Figure 12: PL-1000IL Front Panel

2.3.1 Ring or Linear Add/Drop Configuration

The PL-1000IL front panel in ring or linear add/drop configuration contains the following connectors:

- Optical ports labeled "EDFA1", “EDFA2”, “OSC1” and “OSC2”

- Two MNG ports labeled "MNG1" and "MNG2"
- 10/100 Base-T LAN connector labeled "ETH"
- CONTROL connector: RS-232 port
- External alarms connector labeled "ALARM"
- Power connections

2.3.2 Protected Point-to-Point Configuration

The front panel protected point-to-point configuration contains the following connectors:

- Optical ports labeled “COM”, “OSC”, "COM1” and “COM2”,
- Two MNG ports labeled "MNG1" and "MNG2"
- 10/100 Base-T LAN connector labeled "ETH"
- CONTROL connector: RS-232 port
- External alarms connector labeled "ALARM"
- Power connections

2.3.3 Front Panel LEDs

The LEDs are located on the PL-1000IL front panel.

For the list of LEDs and their functions, see Technical Specifications.

2.3.4 PL-1000IL Optical Connections Examples

This section illustrates the optical connections for the following topologies:

- Ring topology
- Protected point-to-point topology

2.3.4.1 Example of PL-1000IL in Ring Topology

The following figure illustrates the PL-1000IL connected in ring or linear add/drop topology.

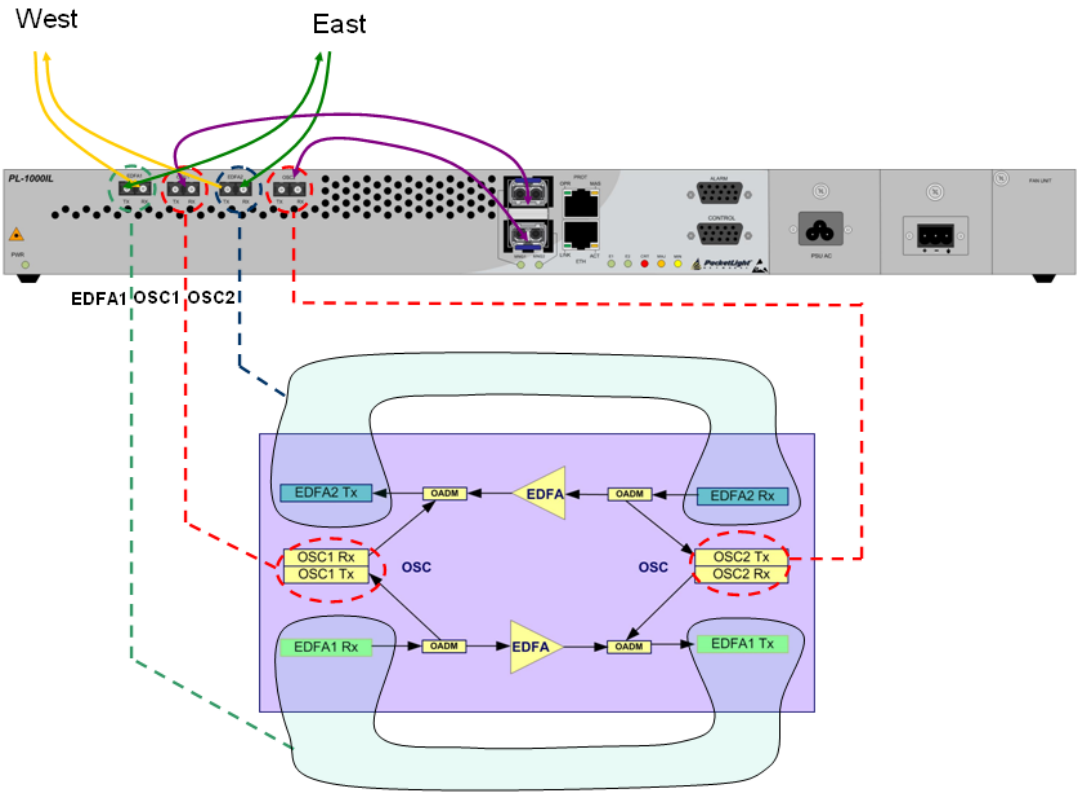


Figure 13: Example of a PL-1000IL in a Ring Topology

In this example the optical ports of the PL-1000IL are connected as follows:

- The EDFA1 Rx and EDFA2 Tx are connected to the fiber coming from West
- The EDFA2 Rx and EDFA1 Tx are connected to the fiber coming from East
- The MNG1 port is connected to OSC1
- The MNG2 port is connected to OSC2

2.3.4.2 Example of PL-1000IL in Point-to-Point Topology

The following figure illustrates the PL-1000IL connected in protected point-to-point topology.

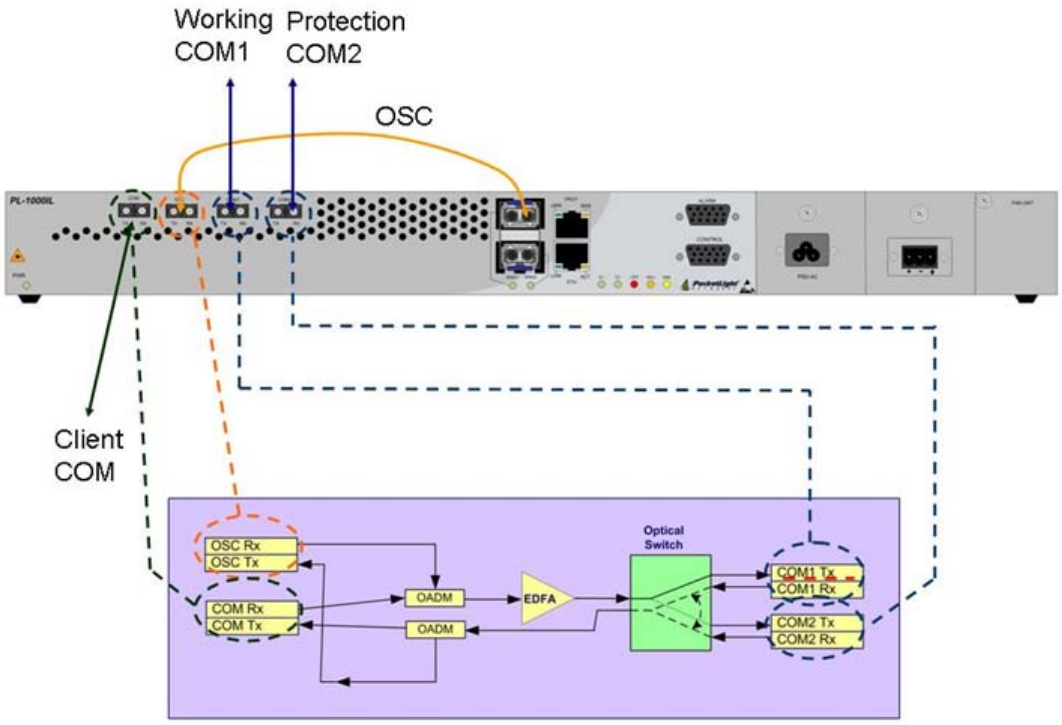


Figure 14: Example of a PL-1000IL in a Protected Point-to-Point Topology

In this example the optical ports of the PL-1000IL are connected as follows:

- The COM port is connected to the client fiber
- The COM1 and COM2 ports are connected to the Working and Protection fibers
- The OSC port is connected to MNG1

2.4 Installing the PL-1000IL Unit

PL-1000IL units are intended for installation in 19-inch or 23-inch racks or placed on desktops or shelves.

⚠ **CAUTION:** Before installing a PL-1000IL unit, review the Safety Precautions (p. 17).

After installing the system, it is necessary to configure it in accordance with the specific user's requirements. The preliminary system configuration is performed through a supervision terminal directly connected to the PL-1000IL (for procedures for using the terminal, see Operation and Preliminary Configuration (p. 27)). The software necessary for using the terminal is stored in the PL-1000IL.

2.4.1 Package Contents

The PL-1000IL package includes the following items:

- PL-1000IL unit
- Ethernet cable
- 3m RS-232 terminal cable
- Power cords (according to the ordered power supplies)
  - **AC power**: 3m power cord equipped with the appropriate plug
  - **DC power**: DC power cord
- Fiber tray (if ordered)
- Kit for rack installation: 19", 23" (if ordered), or 600 mm ETSI (if ordered)

2.4.2 Required Equipment

The cables needed to connect to the PL-1000IL depend on the PL-1000IL application. You can use standard cables or prepare the appropriate cables yourself (see Connection Data (p. 177)).

2.4.3 Cable Connections

Before starting, refer to the site installation plan and identify the cables intended for connection to this PL-1000IL unit (see Site Requirements (p. 19) and Connection Data (p. 177)).

2.4.3.1 Optical Cable Handling Precautions

The following are the optical cable handing precautions:

- Make sure that all the optical connectors are closed at all times, either by the appropriate protective caps or by the mating cable connector. Do not remove the protective cap until an optical fiber is connected to the corresponding connector, and immediately install a protective cap after a cable is disconnected.
- (Recommended) Before installing optical cables, thoroughly clean their connectors using an approved cleaning kit.
- When connecting optical cables, make sure to prevent cable twisting and avoid sharp bends. Unless otherwise specified by the optical cable manufacturer, the minimum fiber bending radius is 35 mm. Always leave some slack, to prevent stress.
- (Recommended) Install plastic supports on each cable connector. These supports determine the fiber bending radius at the connector entry point and also prevent stress at this point.

2.4.3.2 Connecting the PL-1000IL to Ground and Power

WARNING: Any interruption of the protective (grounding) conductor (inside or outside the device) or disconnecting the protective earth terminal can make the device dangerous. Intentional interruption is prohibited.

GROUNDING:

- Before switching this PL-1000IL unit on and connecting any other cable, the PL-1000IL protective ground terminals must be connected to protective ground. This connection is made through the AC or DC power cable.
- The power cord plug should only be inserted in an outlet provided with a protective ground (earth) contact. The protective action must not be negated by using an extension cord (power cable) without a protective conductor (grounding).

WARNING: Dangerous voltages may be present on the cables connected to the PL-1000IL:

- Never connect cables to a PL-1000IL unit if it is not properly installed and grounded. This means that its power cable must be inserted in an outlet provided with a protective ground (earth) contact before connecting any user or network cable to the PL-1000IL.
- Disconnect all the cables connected to the connectors of the PL-1000IL before disconnecting the PL-1000IL power cable.

CAUTION: The PL-1000IL does not have a power ON/OFF switch, and therefore it starts operating as soon as power is applied. To control the connection of power to the PL-1000IL, it is recommended to use an external power ON/OFF switch that disconnects all poles simultaneously. For example, the circuit breaker used to protect the supply line to the PL-1000IL may also serve as the ON/OFF switch. This type of circuit breaker should be rated 10A.

Power should be supplied to the PL-1000IL through a power cable terminated in an appropriate plug, in accordance with the required power source.

To connect the PL-1000IL to ground and power:

1. Connect one end of the power cable to each PL-1000IL power connector.
2. When ready to apply power, insert the plug at the other end of the power cable into a socket (outlet) with a protective ground contact.

   The **PWR** LED of the PL-1000IL lights up and starts blinking.

2.4.3.3 Cabling the Management Ports

You can cable the following management ports:

- MNG port
- CONTROL port
- ETH port

2.4.3.3.1 Cabling the MNG Port

To cable the MNG port:

1. Remove the protective plug from the selected MNG port (MNG1 or MNG2) and insert an SFP transceiver.
2. Connect the MNG port to the LC connector labeled "OSC".

2.4.3.3.2 Cabling the CONTROL Port

To cable the CONTROL port:

- Connect the local console to the 9-pin CONTROL port using a straight cable (a cable wired point-to-point).

  For specific information regarding pin allocations in the PL-1000IL connectors, see Connection Data (p. 177).

2.4.3.3.3 Cabling the ETH Port

To cable the ETH port:

- Connect the 10/100 Base-T ETH port to the local LAN using a cable with an RJ-45 connector.

  For specific information regarding pin allocations in the PL-1000IL connectors, see Connection Data (p. 177).

3 Operation and Preliminary Configuration

This chapter provides general operating instructions and preliminary configuration instructions for the PL-1000IL unit. It also explains how to access the Web application and CLI.

In this Chapter

3.1 Operating Instructions

This section provides instructions for connecting and configuring the terminal, and for turning on the PL-1000IL.

3.1.1 Connecting and Configuring the Terminal

To connect and configure the terminal:

1. Connect a terminal to the CONTROL connector of the PL-1000IL using a straight (point-to-point) cable.

   Any standard VT-100 ASCII terminal (dumb terminal or PC emulating an ASCII terminal) equipped with an RS-232 communication interface can be used for PL-1000IL preliminary configuration (the exact pinout of the connector is described in Connection Data (p. 177)).

2. Check that the installation and the required cable connections have been correctly performed (see Installing the PL-1000IL Unit (p. 23)).

3. Configure the terminal as follows:

   - **9600 kbps**
   - **1 start bit**
   - **8 data bits**
   - **No parity**
   - **1 stop bit**
   - **Full-duplex**
   - **Echo off**
   - **Disable any type of flow control**

3.1.2 Turning on the PL-1000IL

WARNING: Do not connect the power before the unit is in the designated position. The PL-1000IL does not have a power ON/OFF switch and therefore starts operating as soon as the power is connected.

To turn on the PL-1000IL:

1. Connect the PL-1000IL to the power source (see Connecting the PL-1000IL to Ground and Power (p. 25)).

   The **PWR** LED lights up and blinks during power up; all other LEDs (except **ETH**) are off during this time.

2. Wait for the completion of the power-up initialization and LED testing before starting to work on the system. This takes approximately one minute.

   The **PWR** LED lights steadily, and all other LEDs display the PL-1000IL status.

3.2 Performing Preliminary Configuration

You may perform the preliminary IP configuration using CLI via the CONTROL port. This port can be directly connected to a terminal using a cable wired point to point (see Connection Data (p. 177)).

For more information about the CLI commands, see CLI (p. 163).

As an alternative to using a local terminal, the first time preliminary configuration can also be performed via the Web browser, or via CLI over a Telnet/SSH connection, using the default IP address **192.192.192.1** and subnet mask **255.255.255.0**.

To perform preliminary configuration:

1. Log in to the terminal.

   NOTE: The CLI of the PL-1000IL is user/password protected to ensure secure access.

   1. At the prompt, type the following CLI command: **login**

      The prompt to enter the user name appears.

   2. Type the default user name: **admin**

      The prompt to enter the password appears.

   3. Type the default password: **admin**

2. Configure the Ethernet port IP address via the terminal in order to support the Web-based application.

   1. Acquire the Ethernet IP address using CLI if needed (see Configure Interface Ethernet IP Command (p. 172)).

   2. At the prompt, type the following CLI command:

configure interface ethernet ip <addr> [-n <netmask>] [-g <gateway>]

Example: Configure the IP address to **192.168.0.100** with subnet mask **255.255.255.0**.

```
PL-1000IL>> configure interface ethernet ip 192.168.0.100 -n
255.255.255.0
```

Table 6: Configure Interface Ethernet IP Command Options

Attribute	Description	Format/Values
<addr>	IP address	Dot notation For example: 192.168.0.100 Default: 192.192.192.1
<netmask>	Subnet mask	• Dot notation For example: 255.255.255.0 • Hexadecimal notation For example: ffffff00 • Subnet mask of the IP class corresponding to the specified address Default: Subnet mask of the IP class corresponding to the specified address
<gateway>	Gateway IP address	Dot notation For example: 192.168.0.1

3.3 Accessing the Web Application

This section provides instructions for accessing the Web application.

3.3.1 Web Browser Requirements

The following are the Web browser requirements:

- Microsoft® Internet Explorer® version 8 or above
- Mozilla® Firefox® version 7 or above
- Google Chrome™ version 15 or above

The Web user interface enables user configuration via HTTP/HTTPS client (using default IP address **192.192.192.1** and subnet mask **255.255.255.0**).

The default address can be changed by the user. If a different IP address is desired, it is necessary to configure the Ethernet port interface IP address of the PL-1000IL before accessing the Web (see Performing Preliminary Configuration (p. 28)).

3.3.2 Prerequisites for Accessing the Web Application

The following are the prerequisites for accessing the Web application:

- The PL-1000IL is properly installed.
- The PL-1000IL is connected to a Web browser.
- Any pop-up blocking software is disabled.
- JavaScript should be enabled in the browser.

3.3.3 Logging In to the Web Application

To log in to the Web application:

1. Acquire the Ethernet IP address using CLI if needed (see Configure Interface Ethernet IP Command (p. 172)).
2. Open the Web browser.
3. In the address field of the browser, type the **IP address** of the PL-1000IL in the following format:

   http://IP_address (for HTTP access)

   or

   https://IP_address (for HTTP secure access)

   (**<IP_address>** stands for the actual IP address of the PL-1000IL)
4. Press **Enter**.

   The Login window opens.

Figure 15: Login Window

5. In the **User Name** field, type the name of the user.

   NOTE: The user name and password are case sensitive.
6. In the **Password** field, type the password.

   Only alphanumeric characters without spaces are allowed.

7. Click **Login**.

   The System Configuration window opens displaying the **General** tab.

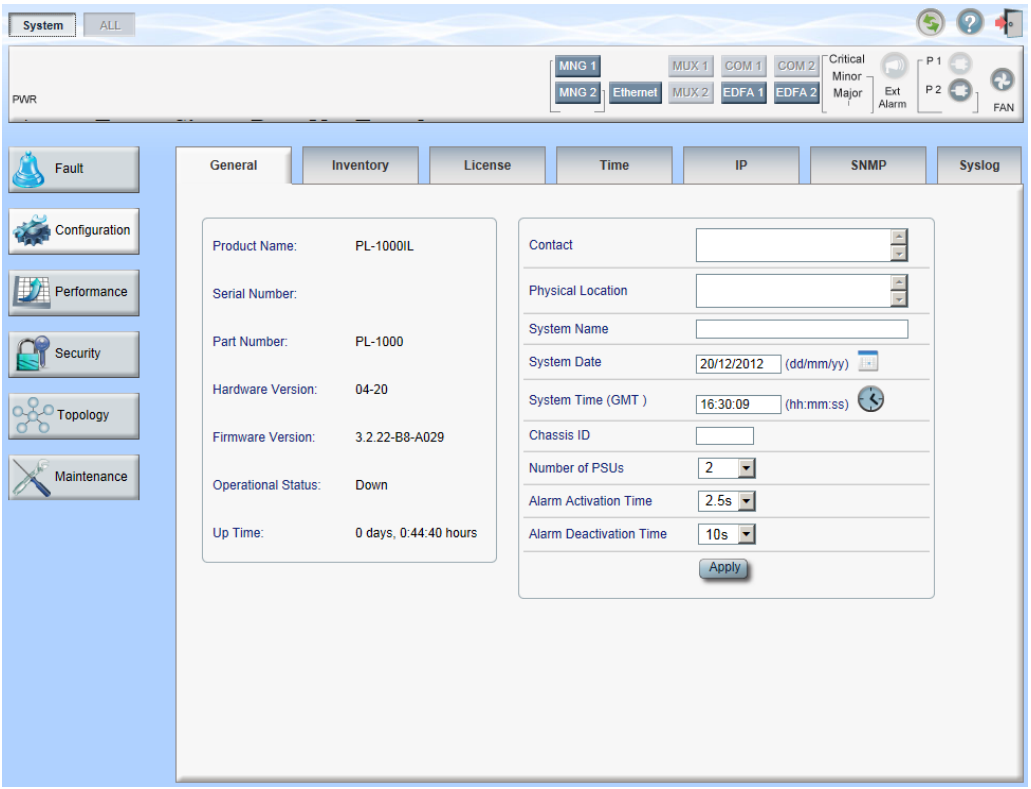


Figure 16: System Configuration Window

3.3.4 Navigating the Web Application

This section describes the PL-1000IL item buttons, sidebar buttons, and tabs.

3.3.4.1 Item Buttons

The following figure shows an example of the buttons used for performing operations in the Web application.

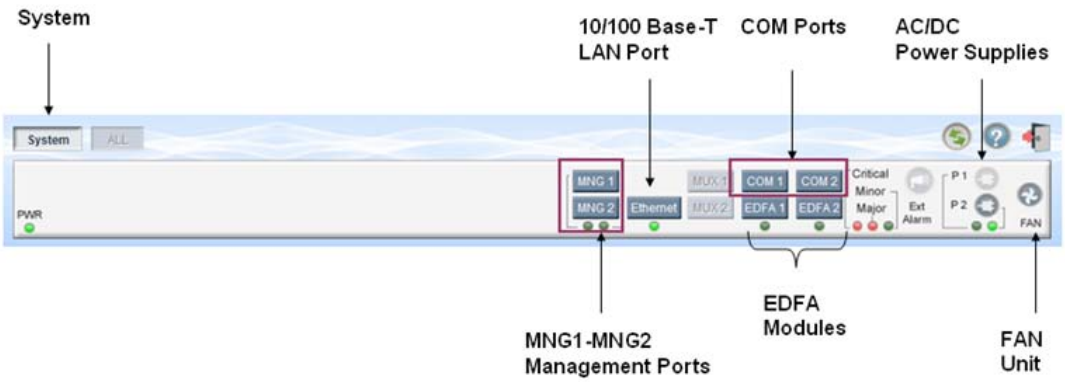


Figure 17: PL-1000IL Item Buttons

The buttons displayed vary according to the configuration. For example, if the PL-1000IL does not have an EDFA module installed, the **EDFA** button is disabled.

The Item buttons displayed also vary according to the context of the window. For example, the **FAN** button is disabled in the Fault window because no faults are defined for this unit.

3.3.4.2 Sidebar Buttons

The following figure shows the sidebar buttons.

Figure 18: PL-1000IL Sidebar Buttons

Use the sidebar buttons to do the following:

- **Fault**: View PL-1000IL faults
- **Configuration**: Configure the PL-1000IL parameters
- **Performance**: View system optical information and port performance monitoring
- **Security**: Manage users' accounts
- **Topology**: View network topology
- **Maintenance**: Perform maintenance tasks for the PL-1000IL

3.3.4.3 PL-1000IL Tabs

The following figure shows an example of the tabs used for performing system security operations.

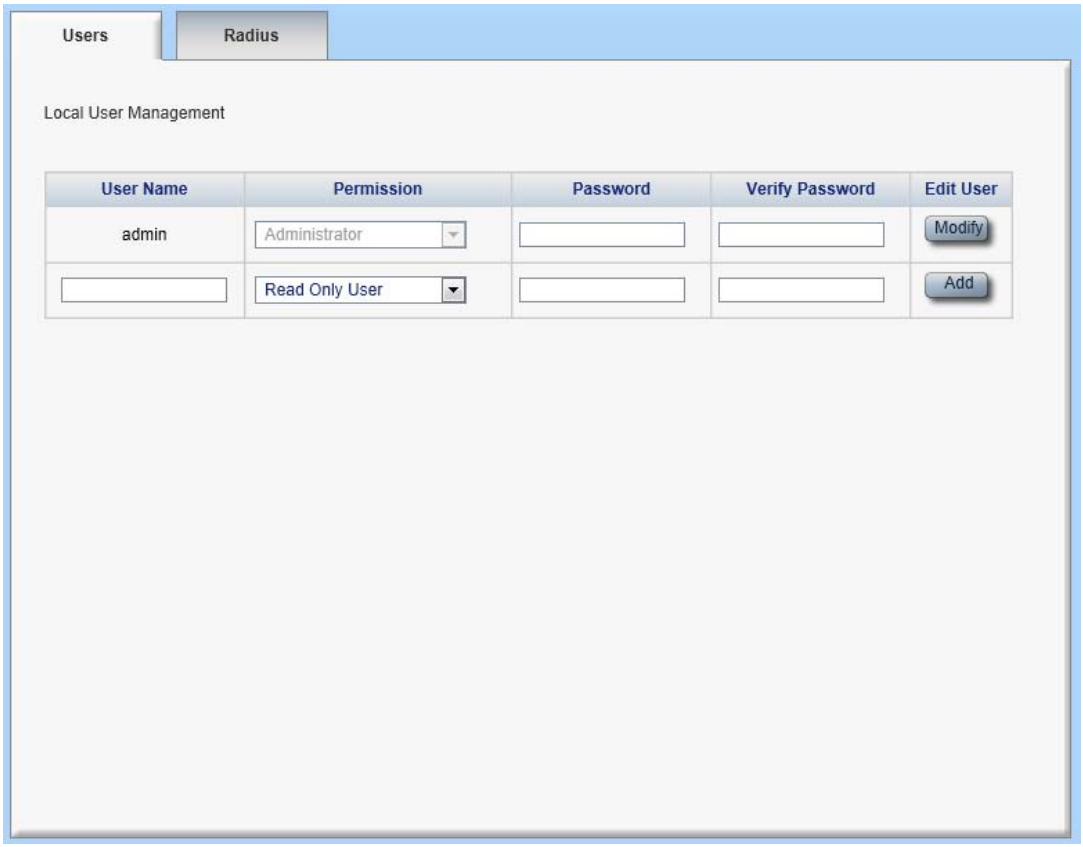


Figure 19: PL-1000IL Tabs (Example)

The tabs displayed vary according to the user permissions. For example, the **Radius** tab is only displayed for a user with Administrator permissions.

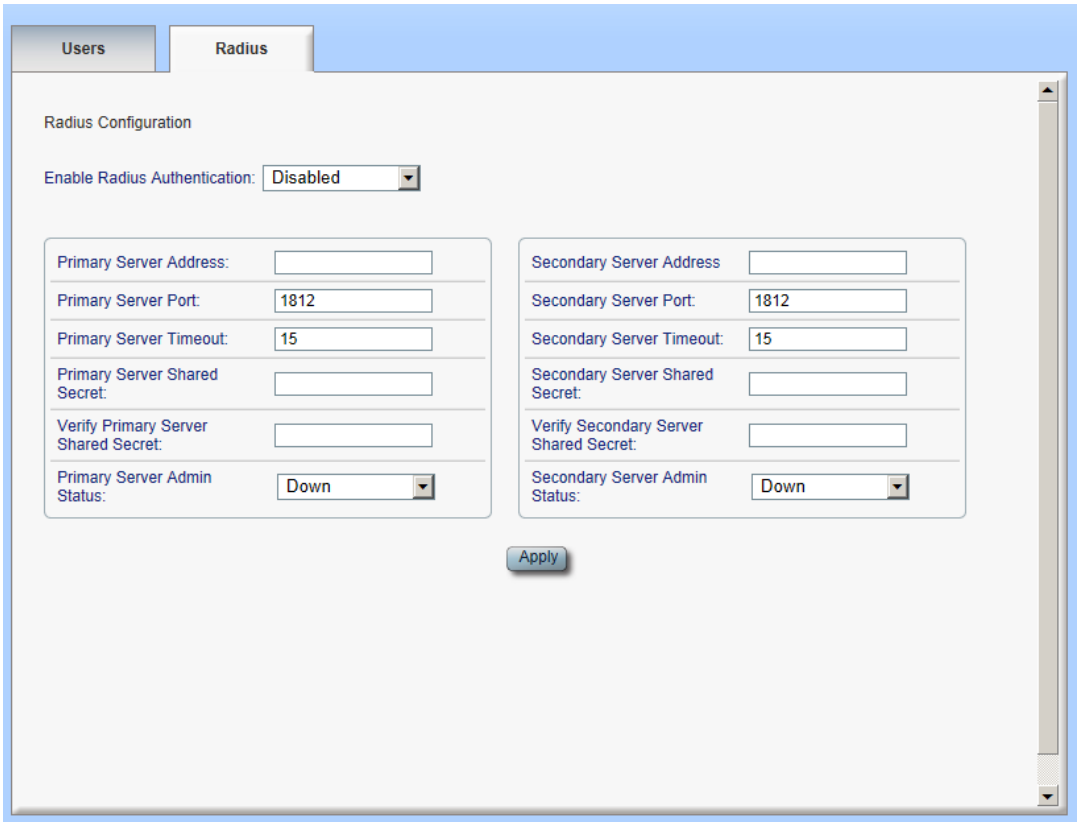


Figure 20: PL-1000IL Radius Tab

3.3.5 Logging Out of the Web Application

To log out of the Web application:

- Click **Logout**  .

  You are logged out.

4 Security Management

This chapter describes how to manage users' accounts.

In this Chapter

4.1 User Access Levels

The PL-1000IL supports the following types of users.

Table 7: User Access Levels

User Type	Permissions	Notes
Administrator		
Administrator	Access and edit permissions for all functions; can add and delete users, change access levels, and change passwords.	• **User name**: admin • **Password**: admin (default) **NOTE:** You can change the password. However, the user name cannot be changed and is set to "admin" by default.
Non-Administrator		
Read/Write User	View and manage the node; cannot manage other users but can change their own password (see Changing Your Password (p. 42)).	
Read Only User	View only; no edit permissions except to change their own password (see Changing Your Password (p. 42)).	

4.2 User Authentication Methods

The access to the PL-1000IL Web application and CLI is protected. Therefore, before performing any operation on the device, the user needs to log in to the node by entering a user name and password, which is then authenticated by the node.

There are two methods for user authentication:

- Local authentication
- Remote authentication

4.2.1 Local Authentication

The local authentication method is always enabled. The authentication is performed against a local database stored in the node.

Local authentication requires that an updated list of user names and passwords be provided to each node in the network.

4.2.2 Remote Authentication

The PL-1000IL supports centralized authentication, implemented with the Radius protocol as defined by RFC-2865.

The remote authentication method is optional, and can be enabled or disabled by the network administrator. The authentication is performed against a centralized database stored on a Radius server.

The remote authentication allows the network administer to keep the updated list of user names and passwords on a Radius server.

When a user tries to log in and the user name and password are not on the local user list, if the Radius authentication is enabled, the node communicates with the Radius server and performs remote user authentication. If the user name and password are on the remote user list, the log in succeeds.

4.2.2.1 Attribute Value Pairs

The Radius Attribute Value Pairs (AVP) carry data in both the request and the response for the authentication.

The following table lists the attributes used by the remote Radius authentication.

Table 8: Attributes Used

Attribute	AVP Type	Access-Request	Access-Accept	Format / Values
User-Name	1	√	√	The name of the user as carried by the Radius **Access-Request**. Format: String
User-Password	2	√	√	The password of the user as carried by the Radius **Access-Request**. Format: String

Attribute	AVP Type	Access-Request	Access-Accept	Format/Values
Class	25	-	√	The access level granted to the user as carried by the Radius **Access-Accept**. Format: String Allowed values: • **1**: read-only access • **2**: read-write access • **4**: admin access

4.2.2.2 Shared Secret

The Radius protocol does not transmit passwords in clear text between the Radius client and server. Rather, a shared secret is used along with the MD5 hashing algorithm to encrypt passwords. The shared secret string is not sent over the network; therefore that same key should be independently configured to the Radius clients and server.

4.2.2.3 Server Redundancy

For improved redundancy, the PL-1000IL can use one or two Radius servers: Server #1 and Server #2.

NOTE: There is no precedence between the Radius servers; therefore, the authentication response is taken from the first server to answer.

4.2.2.4 Setting Up Radius

Before using Radius, the network administration should set up the Radius servers and enable Radius authentication.

To set up Radius:

1. Launch one or two Radius servers on Windows/Unix systems that are accessible to the nodes via the IP network.
2. Configure the Radius servers with **Shared Secret** string that will be used by the Radius servers and clients.
3. Enter the user name, password, and permission of all users to the Radius servers.
4. Configure the access information to the Radius servers for the Radius clients of the nodes.
5. Enable Radius authentication for all nodes.

4.2.2.5 Configuring the Radius Server

NOTE: The server configuration process may look different on different Radius server packages.

An Administrator can configure the Radius server.

To configure the Radius server:

1. Configure the **Authentication Port** (default port is 1812).

   NOTE: If a firewall exists between the nodes to the Radius servers, make sure that it does not block the chosen port.

2. Configure the **Shared Secret**.
3. For each user, configure the following attributes:

   - **User-Name**

     Only alphanumeric characters without spaces are allowed.

   - **User-Password**

     Only alphanumeric characters without spaces are allowed.

   - **Class**

   For a description of the attributes, see Attribute Value Pairs (p. 36).

4.3 Security Settings

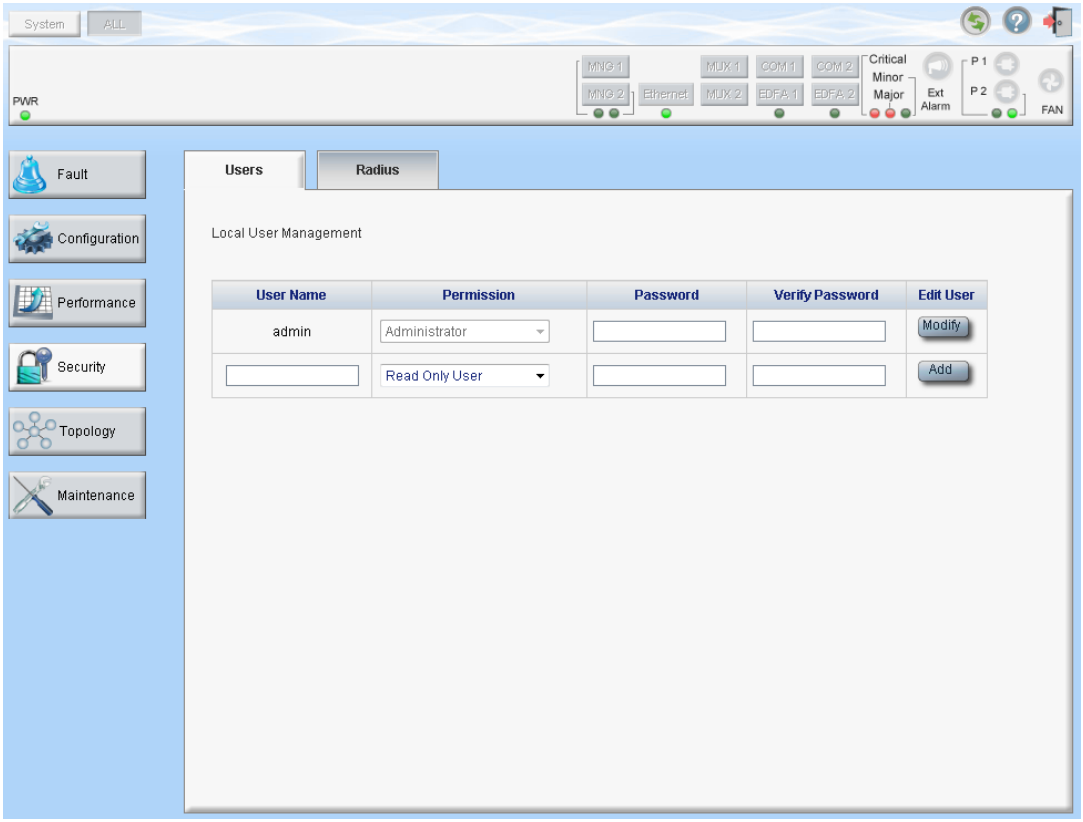


Figure 21: Security Settings Window

Use the Security Settings window to do the following:

- **Users tab (Administrator)**: Add a new user, change a user password, change a user permission level, and delete a user
- **Users tab (Non-Administrator)**: Change your password
- **Radius tab (Administrator)**: Configure the Radius client

To open the Security Settings window:

- Click **Security**.

  The Security Settings window opens.

4.3.1 Users Tab (Administrator)

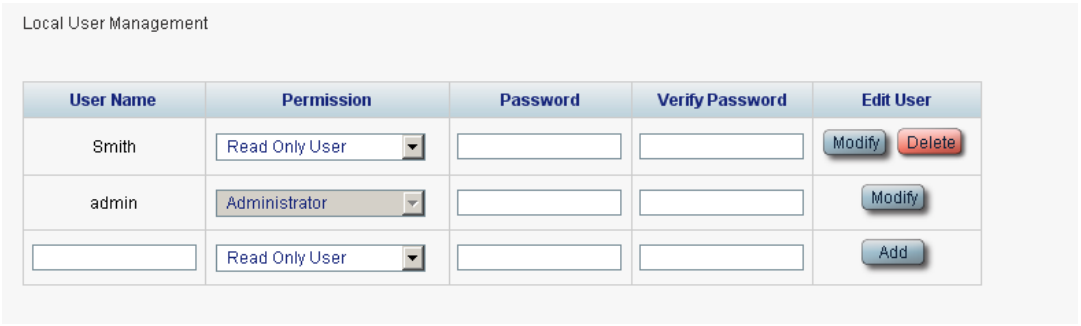


Figure 22: Users Tab (Administrator)

An Administrator can use the Users tab to manage the user list for local authentication:

- Add a new user
- Change a user password
- Change a user permission level
- Delete a user

4.3.1.1 Adding a New User

An Administrator can use the Users tab to add a new user.

To add a new user:

1. Click the **Users** tab.

   The Users tab opens displaying all users and their permission levels.
2. Fill in the fields as explained in the following table.
3. Click **Add**.

   The new user is added.

Table 9: Users Tab Parameters (Administrator)

Parameter	Description	Format/Values
User Name	The name of the user.	Only alphanumeric characters without spaces are allowed.
Permission	The permission level for the user.	Administrator, Read/Write User, Read Only User (see User Access Levels (p. 35))
Password	The password for the user.	Only alphanumeric characters without spaces are allowed. **NOTE:** The password is hidden for security reasons.
Verify Password	The password for the user again.	Only alphanumeric characters without spaces are allowed. **NOTE:** The password is hidden for security reasons.

4.3.1.2 Changing a User Permission Level

An Administrator can use the Users tab to change a user permission level.

To change a user permission level:

1. Click the **Users** tab.

   The Users tab opens displaying all users and their permission levels.

2. Find the user whose password you want to change.
3. From the **Permission** drop-down list, select the new permission level for this user (see User Access Levels (p. 35)).
4. Click **Modify**.

   The following confirmation message appears.

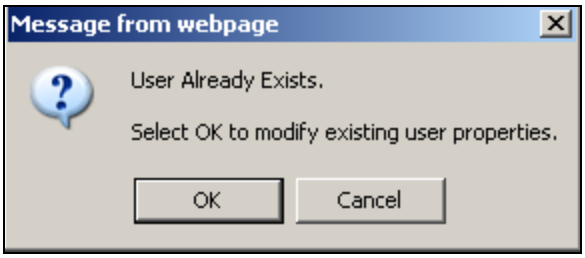


Figure 23: Confirm Changes

5. Click **OK**.

   The new permission level is assigned to the specified user.

4.3.1.3 Changing a User Password

An Administrator can use the Users tab to change all user passwords.

NOTE: For security reasons, it is recommended to change the default **admin** password. If the Administrator password has been changed and is unknown, contact PacketLight Technical Support.

To change a user password:

1. Click the **Users** tab.

   The Users tab opens displaying all users and their permission levels.

2. Find the user whose password you want to change.
3. In the **Password** field, type the new password.

   Only alphanumeric characters without spaces are allowed.

   NOTE: The password is hidden for security reasons.

4. In the **Verify Password** field, type the new password again.
5. Click **Modify**.

   The following confirmation message appears.

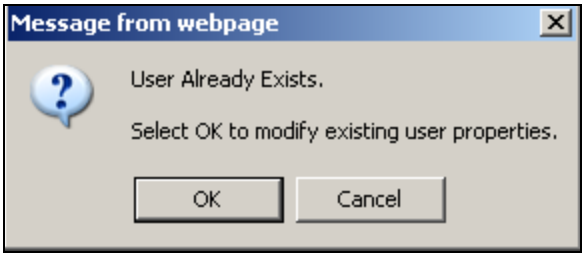


Figure 24: Confirm Changes

6. Click **OK**.

   The new password is assigned to the specified user.

4.3.1.4 Deleting a User

An Administrator can use the Users tab to delete a user.

NOTE: The **admin** user cannot be deleted.

To delete a user:

1. Click the **Users** tab.

   The Users tab opens displaying all users and their permission levels.

2. Find the user you want to delete.
3. Click **Delete**.

The following confirmation message appears.

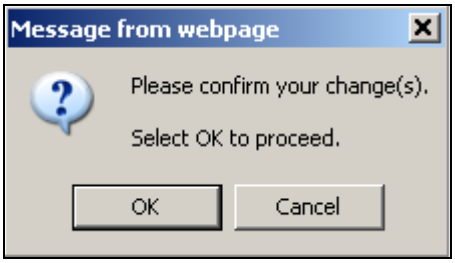


Figure 25: Confirm Delete

4. Click **OK**.

   The specified user is deleted.

4.3.2 Users Tab (Non-Administrator)

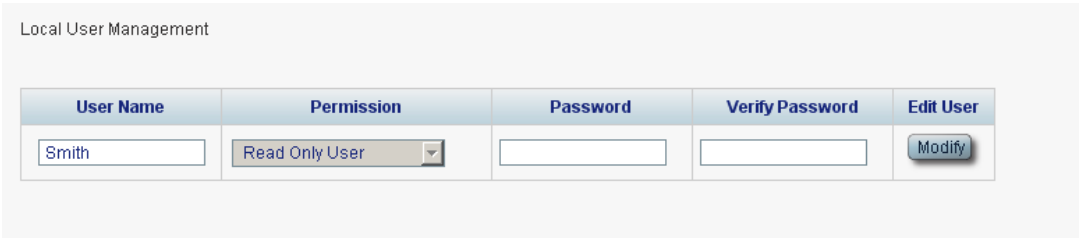


Figure 26: Users Tab (Non-Administrator)

Non-administrator users cannot manage other users; however, they can use the Users tab to change their own password if they are on the local user list.

4.3.2.1 Changing Your Password

A non-administrator can use the Users tab to change their own password.

To change your password:

1. Click the **Users** tab.

   The Users tab opens displaying your user name and permissions.

2. In the **Password** field, type the new password.

   Only alphanumeric characters without spaces are allowed.

   NOTE: The password is hidden for security reasons.

3. In the **Verify Password** field, type the new password again to be certain that it was typed correctly.

4. Click **Modify**.

The following confirmation message appears.

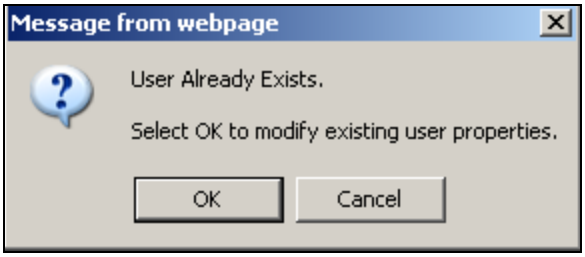


Figure 27: Confirm Changes

5. Click **OK**.

   Your password is changed.

Table 10: Users Tab Parameters (Non-Administrator)

Parameter	Description	Format/Values
User Name	Your user name.	Only alphanumeric characters without spaces are allowed. **NOTE:** This field is read only.
Permission	Your permission level for the user.	Read-Write User, Read Only User **NOTE:** This field is read only.
Password	Your password.	Only alphanumeric characters without spaces are allowed. **NOTE:** The password is hidden for security reasons.
Verify Password	Your password again.	Only alphanumeric characters without spaces are allowed. **NOTE:** The password is hidden for security reasons.

4.3.3 Radius Tab (Administrator)

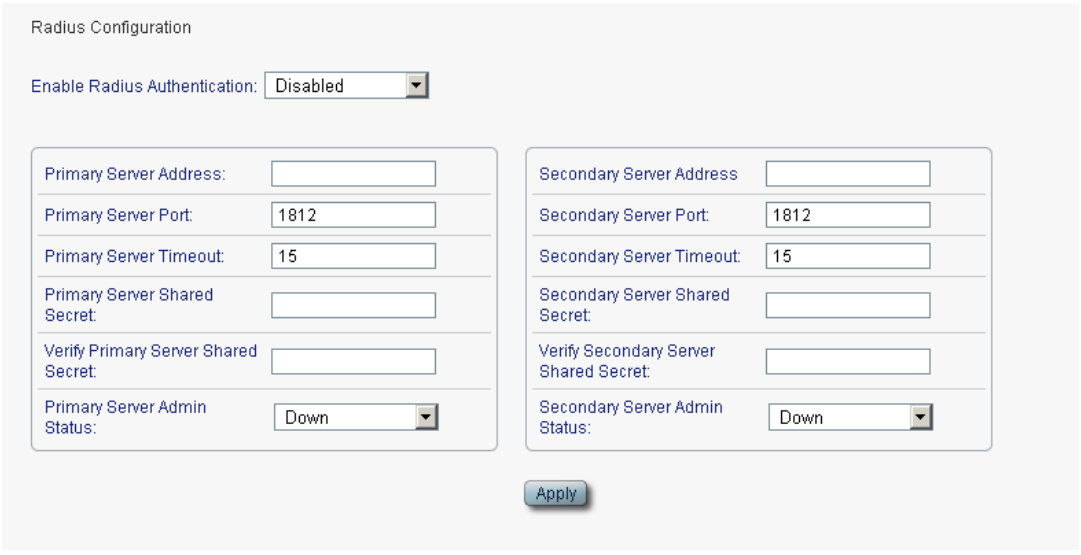


Figure 28: Radius Tab (Administrator)

An Administrator can use the Radius tab to configure the Radius client on the node.

4.3.3.1 Configuring the Radius Client

An Administrator can use the Radius tab to configure the Radius client on the node.

NOTE: For the remote Radius authentication to be activated, the **Enable Radius Authentication** must be set to **Enabled** and the **Admin Status** of at least one server must be set to **Up**.

To configure the Radius client:

1. Click the **Radius** tab.

   The Radius tab opens displaying the Radius configuration.

2. Fill in the fields as explained in the following table.

3. Click **Apply**.

   The following confirmation message appears.

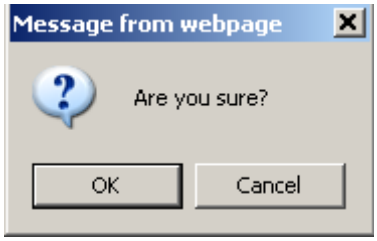


Figure 29: Confirm Configuration

4. Click **OK**.

   The Radius client is configured.

Table 11: Radius Tab Parameters (Administrator)

Parameter	Description	Format / Values
Enable Radius Authentication	Whether or not to enable the Radius authentication.	Enabled, Disabled
Primary Server Address	The IP address of the primary server.	Dot notation For example: `192.168.0.100`
Primary Server Port	The port number of the primary server.	1812 (default)
Primary Server Timeout	The amount of time before the primary server times out (in seconds).	Integer
Primary Server Shared Secret	The shared secret for the primary server.	Free text
Verify Primary Server Shared Secret	The shared secret for the primary server again.	Free text
Primary Server Admin Status	The administrative status of the primary server.	Up, Down

Parameter	Description	Format / Values
Secondary Server Address	The IP address of the secondary server.	Dot notation For example: `192.168.0.100`
Secondary Server Port	The port number of the secondary server.	1812 (default)
Secondary Server Timeout	The amount of time before the secondary server times out (in seconds).	Integer
Secondary Server Shared Secret	The shared secret for the secondary server.	Free text
Verify Secondary Server Shared Secret	The shared secret for the secondary server again.	Free text
Secondary Server Admin Status	The administrative status of the secondary server.	Up, Down

5 Fault Management

This chapter describes the PL-1000IL fault management, which is used to localize and identify problems in the network incorporating PL-1000IL units.

In this Chapter

5.1 Fault Views

This section describes the following Fault views:

- Alarms
- Events
- Configuration Changes

5.1.1 Alarms

The PL-1000IL keeps a list of the alarms currently detected on the system. When an alarm is detected, the **Alarm Rise** event is generated and the alarm is added to the list. When the **Alarm Clear** is detected, the alarm is removed from the list.

The following information is stored for each alarm:

- **Date and Time**: The date and time when the alarm was detected.
- **Source**: The entity that caused the alarm.
- **Severity**: The severity of the alarm.
- **Type**: The type of the alarm.
- **Service Affecting**: **Yes** or **No** according to the alarm impact.

5.1.2 Events

The PL-1000IL continuously monitors the traffic signals and other exceptional conditions. Whenever such a condition occurs, the PL-1000IL generates a time stamped event message and sends it as an SNMP notification to the registered management systems. The PL-1000IL logs the history of the last 512 events in a cyclic buffer that can be browsed by the Web application or by SNMP management systems.

In addition, the events and audit messages are printed in the PL-1000IL system log files, which can be exported to a text file for offline viewing.

The PL-1000IL provides the following events:

- **Alarm Rise**: Alarms are standing faults. They are raised after a configurable stabilization period of several seconds. These events are generated when a new alarm occurs.
- **Alarm Clear**: Alarms are standing faults. They are cleared after a configurable stabilization period of several seconds. These events are generated when an alarm is cleared.
- **Cold Restart**: These are standard SNMP events that are generated after a Cold Restart to the node.
- **Warm Restart**: These are standard SNMP events that are generated after a Warm Restart to the node.
- **Test Status Changed**: These events are generated when the loopback or PRBS test status of a port is changed.
- **Protection Switching Event**: These events are generated when protection switching occurs.
- **Inventory Change**: These events are generated when the node inventory is changed.
- **Unsolicited Event**: These events are generated when an exceptional event occurs.
- **Configuration Change**: These events are generated when the node configuration is changed.

5.1.3 Configuration Changes

The PL-1000IL generates an event when the configuration of a node is explicitly changed by the user and stores the event in the Configuration Changes log for auditing.

5.2 General Faults Viewing Procedure

The following is the general procedure for viewing the PL-1000IL faults. The specific procedures for each item are provided in the following sections.

To view the PL-1000IL faults:

1. Click **Fault**.
2. Click the desired button in the upper portion of the window to select the item to view:
   - **System** (see System Faults (p. 50))
   - **All** (see All Faults (p. 56))
   - **MNG** (see Management Port Faults (p. 62))
   - **Ethernet** (see Ethernet Port Faults (p. 68))
   - **EDFA** (if present) (see EDFA Module Faults (p. 74))
   - **COM** (if present) (see COM Port Faults (p. 80))
   - **PSU** (see PSU Faults (p. 86))

   The appropriate Fault window opens.
3. Click one of the following tabs:
   - **Alarms**
   - **Events**
   - **Configuration Changes**

     The appropriate tab opens. Note that some or all of the fields may be read only.

5.3 System Faults

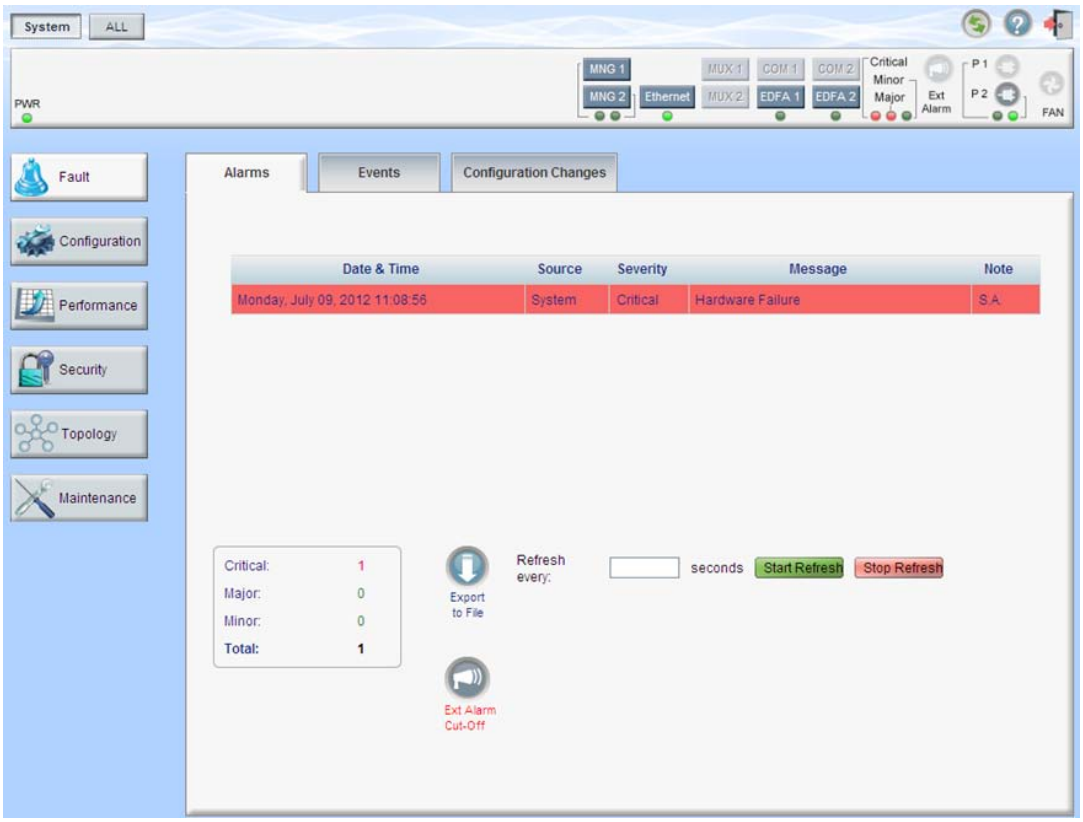


Figure 30: System Fault Window

Use the System Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the System Fault window:

1. Click **Fault**.
2. Click **System**.

   The System Fault window opens.

5.3.1 Alarms Tab

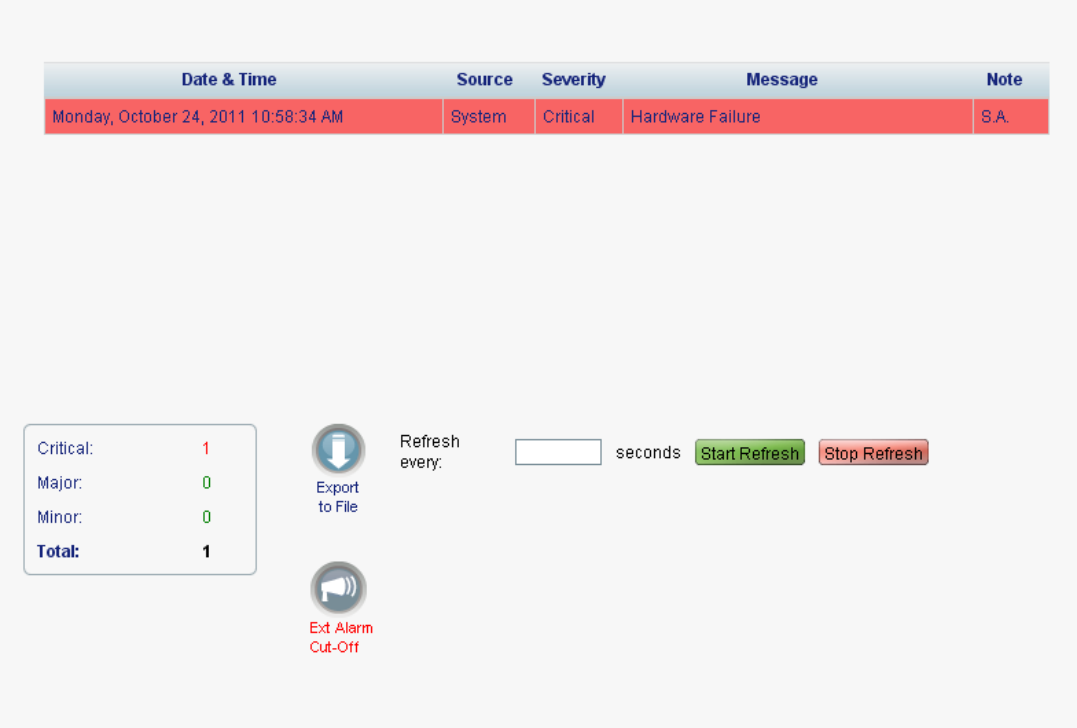


Figure 31: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

   NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

1. In the **Refresh every** field, type the number of seconds that the window should refresh.

   The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 12: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.3.2 Events Tab

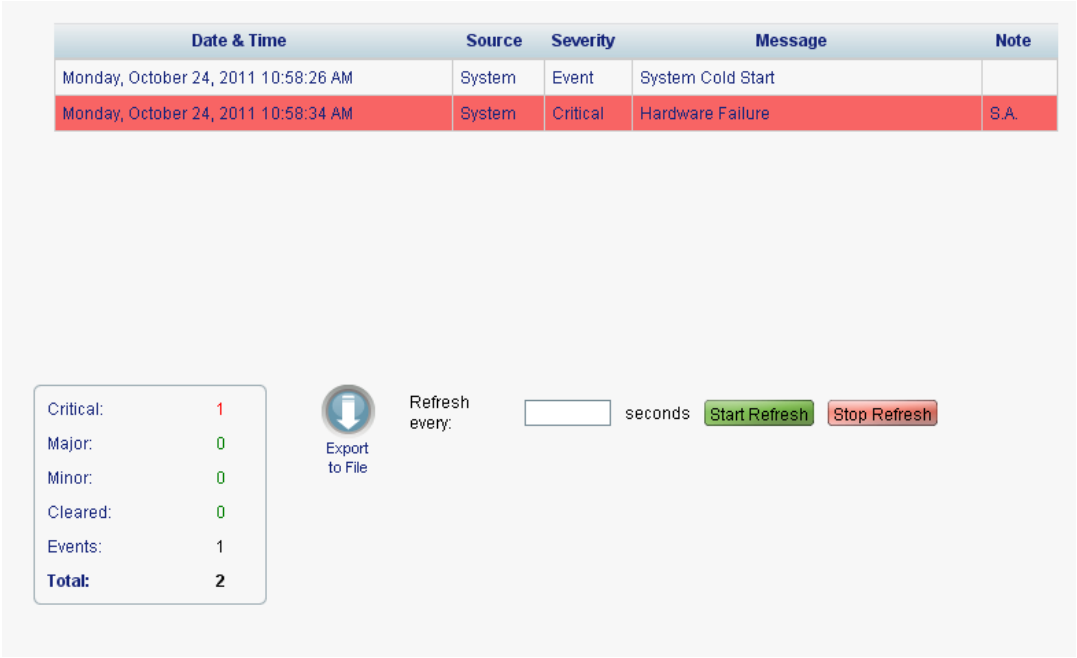


Figure 32: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 13: Events Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.3.3 Configuration Changes Tab

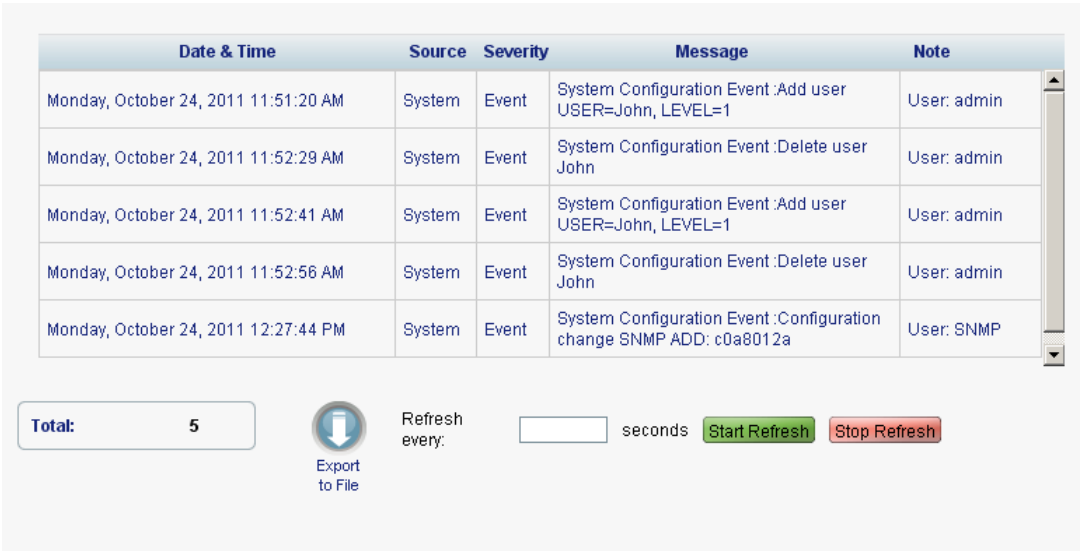


Figure 33: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 14: Configuration Changes Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

5.4 All Faults

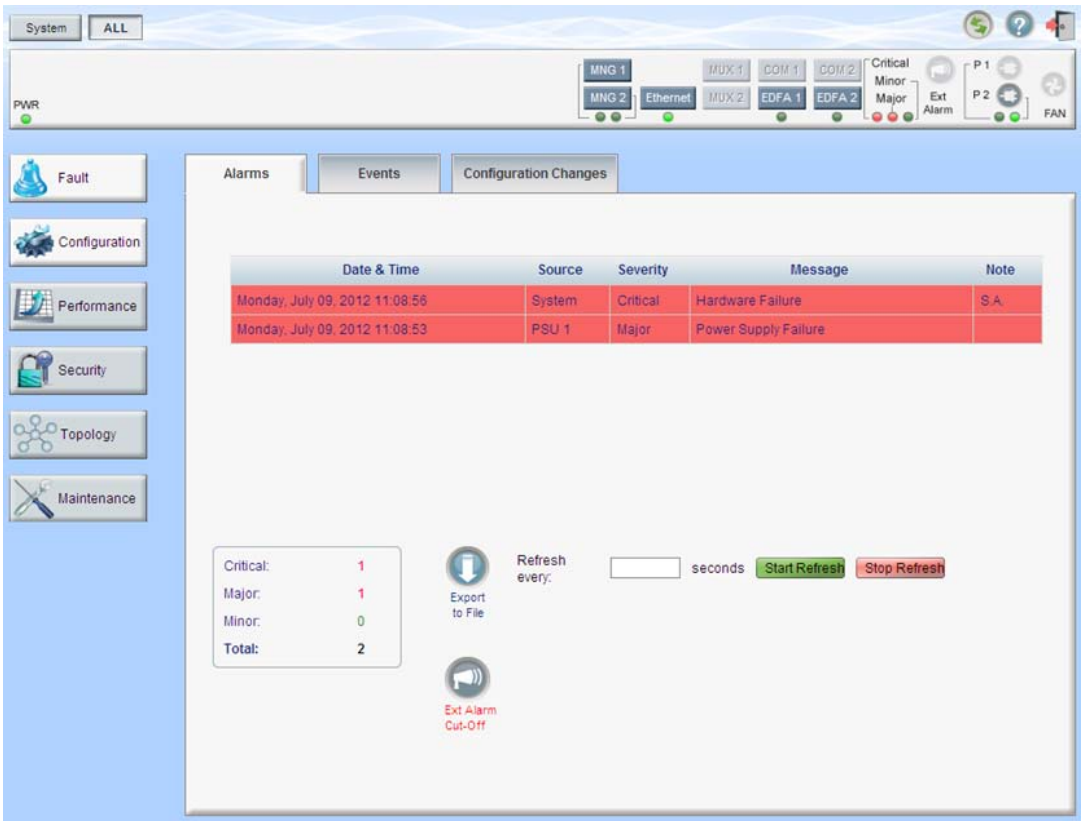


Figure 34: All Fault Window

Use the All Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Events tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the All Fault window:

1. Click **Fault**.
2. Click **All**.

   The All Fault window opens.

5.4.1 Alarms Tab

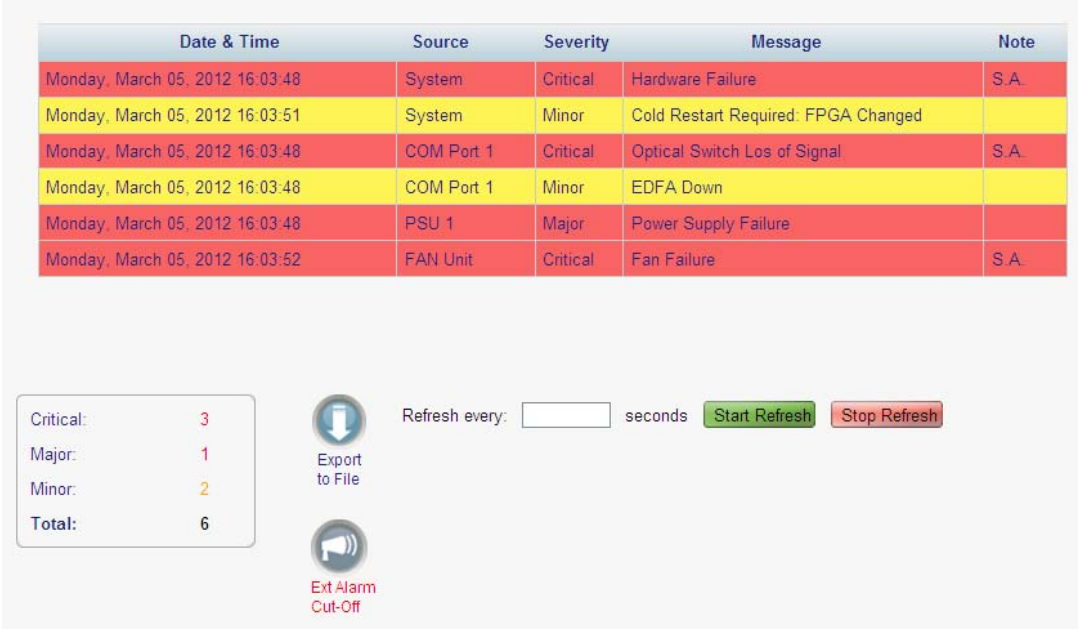


Figure 35: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

   NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 15: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.4.2 Events Tab

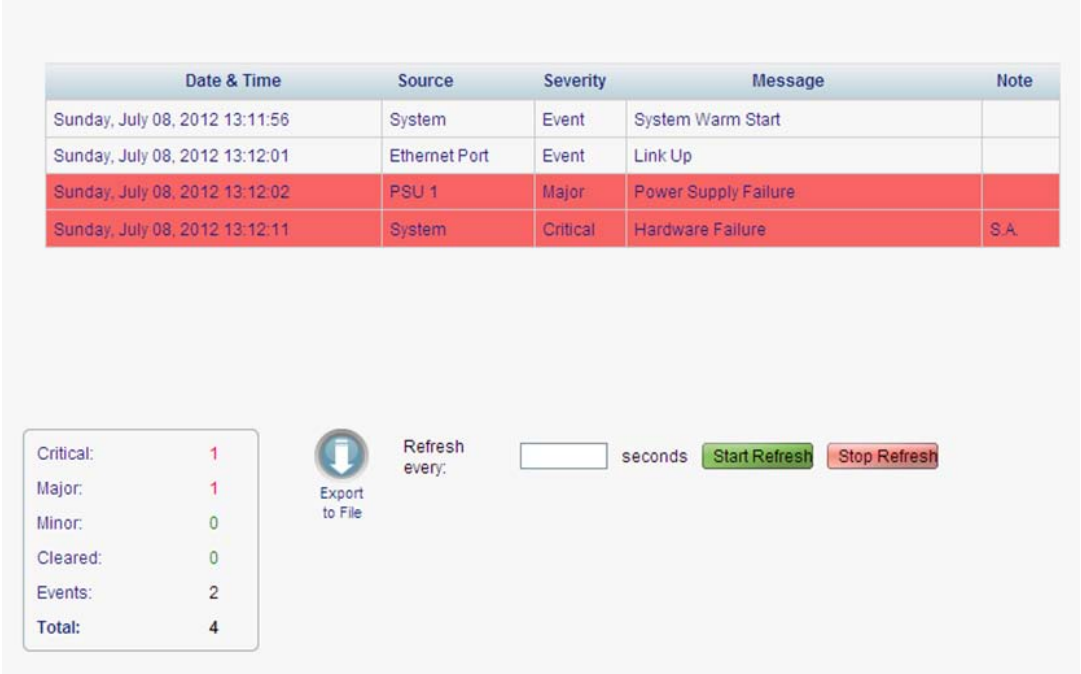


Figure 36: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File** .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 16: Events Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.4.3 Configuration Changes Tab

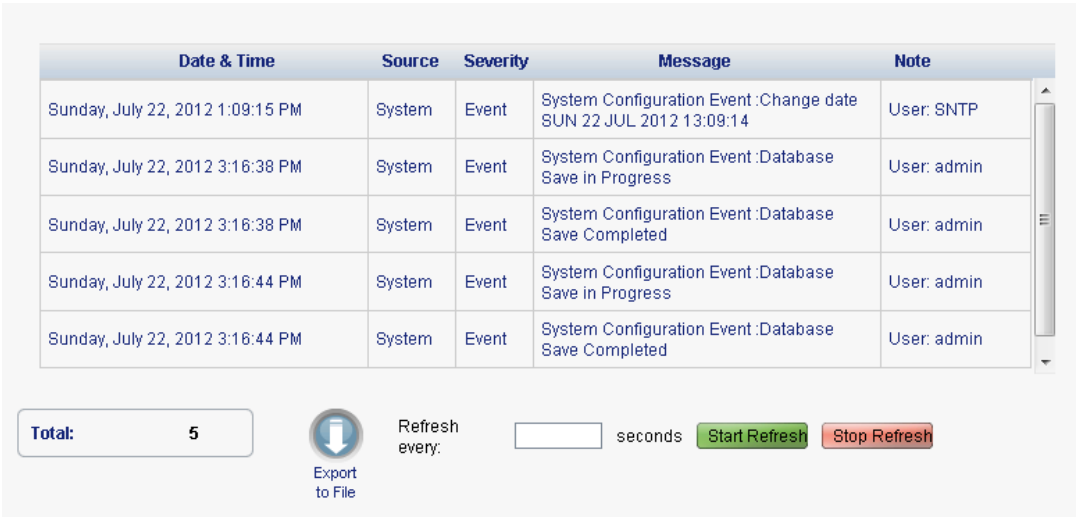


Figure 37: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 17: Configuration Changes Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

5.5 Management Port Faults

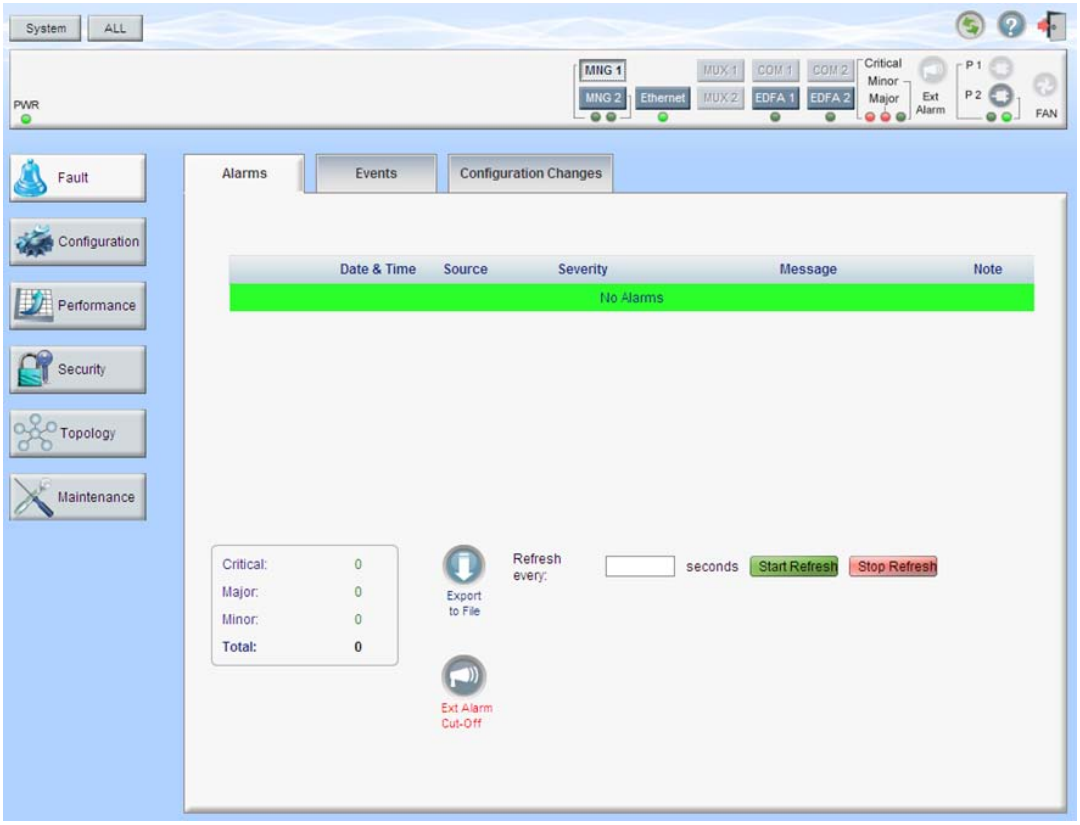


Figure 38: Management Port Fault Window

Use the Management Port Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the Management Port Fault window:

1. Click **Fault**.
2. Click an **MNG** button to select the management port.

   The appropriate Management Port Fault window opens.

5.5.1 Alarms Tab

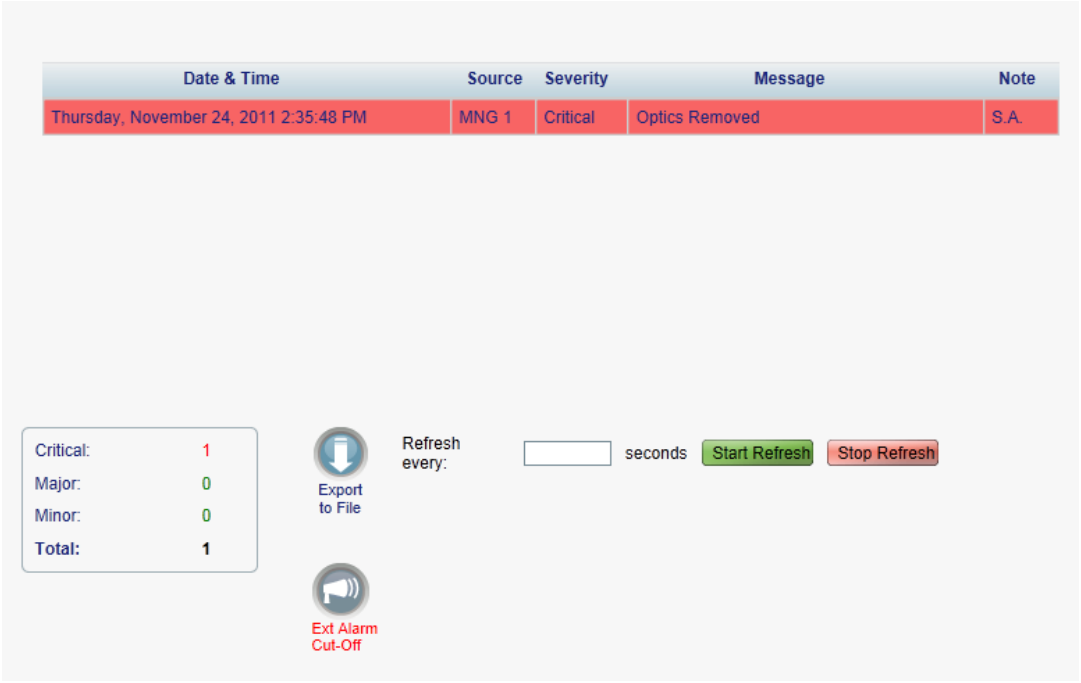


Figure 39: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

   NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

1. In the **Refresh every** field, type the number of seconds that the window should refresh.

   The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 18: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.5.2 Events Tab

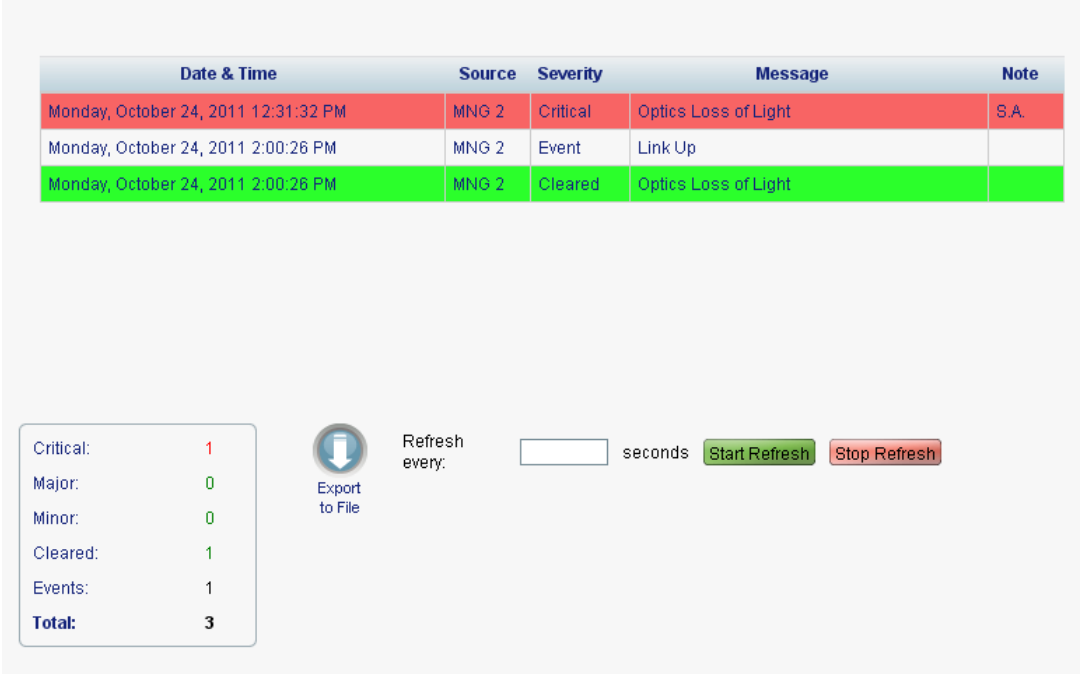


Figure 40: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File** .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 19: Events Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.5.3 Configuration Changes Tab

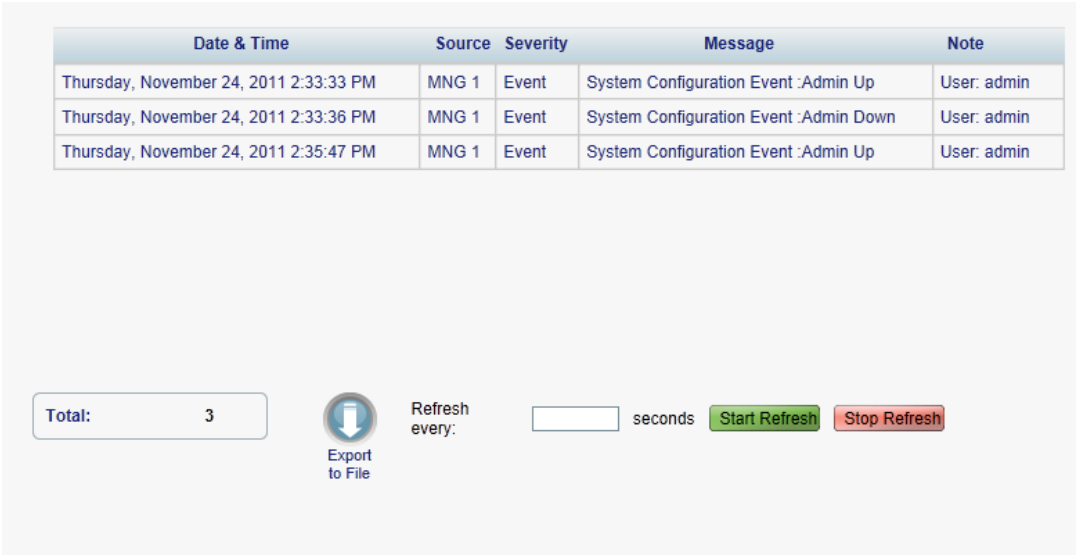


Figure 41: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 20: Configuration Changes Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

5.6 Ethernet Port Faults

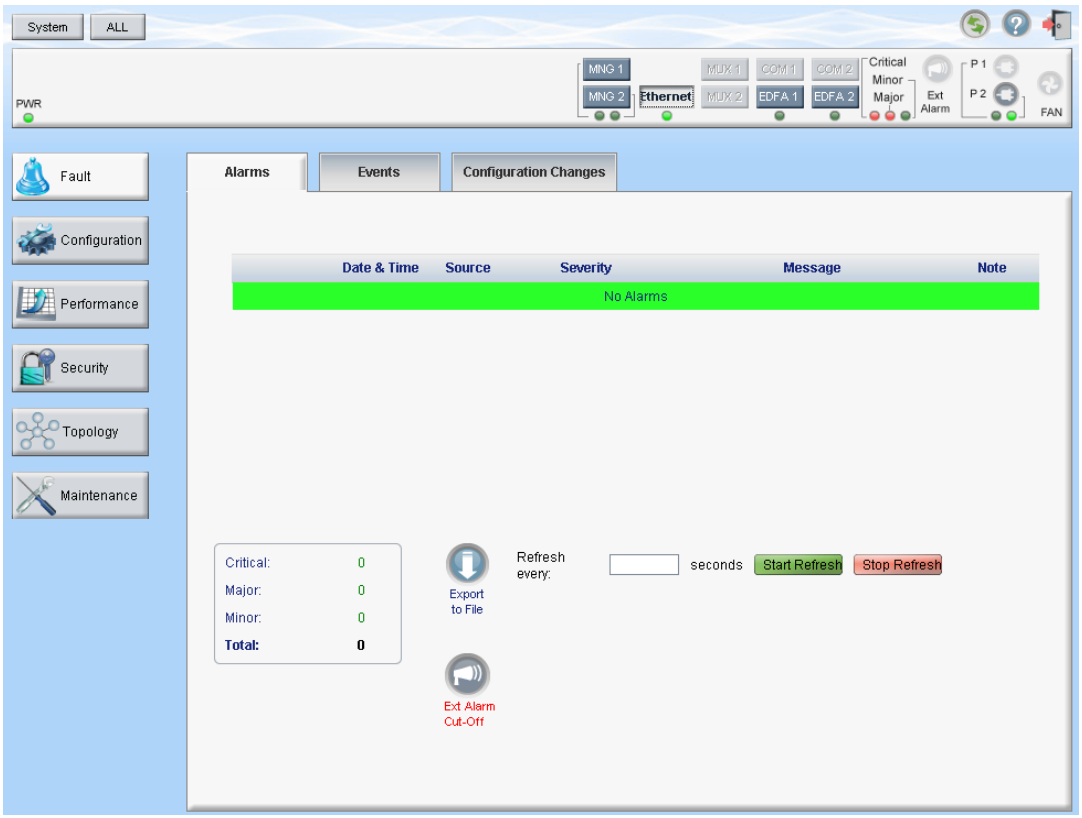


Figure 42: Ethernet Port Fault Window

Use the Ethernet Port Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the Ethernet Port Fault window:

1. Click **Fault**.
2. Click **Ethernet** to select the Ethernet port.

   The Ethernet Port Fault window opens.

5.6.1 Alarms Tab

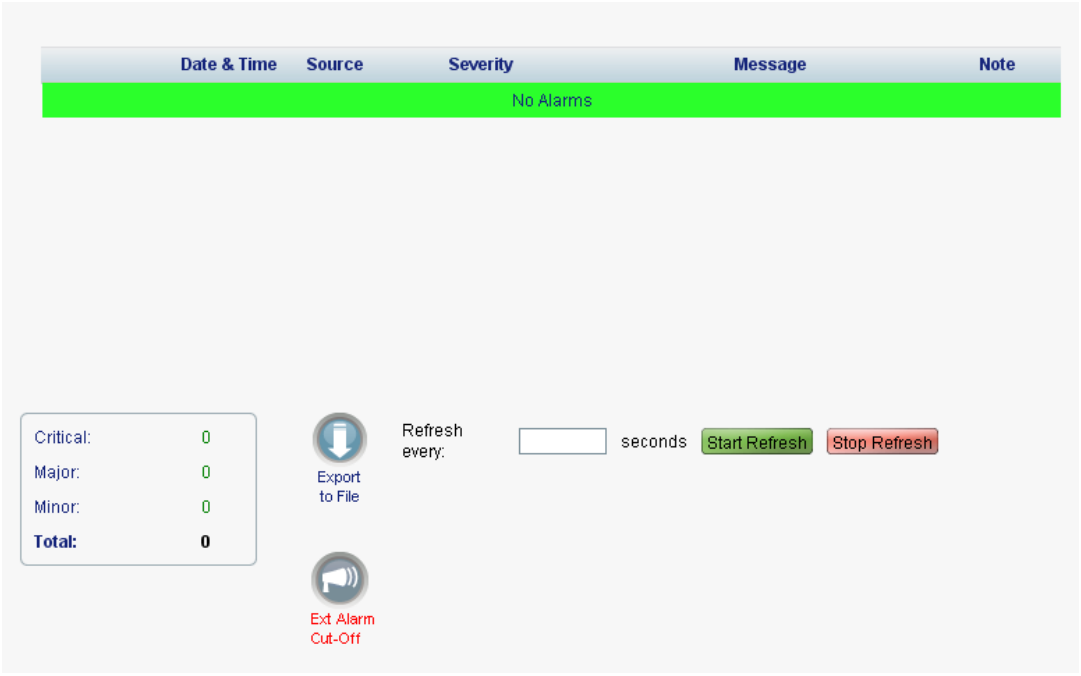


Figure 43: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

   NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 21: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.6.2 Events Tab

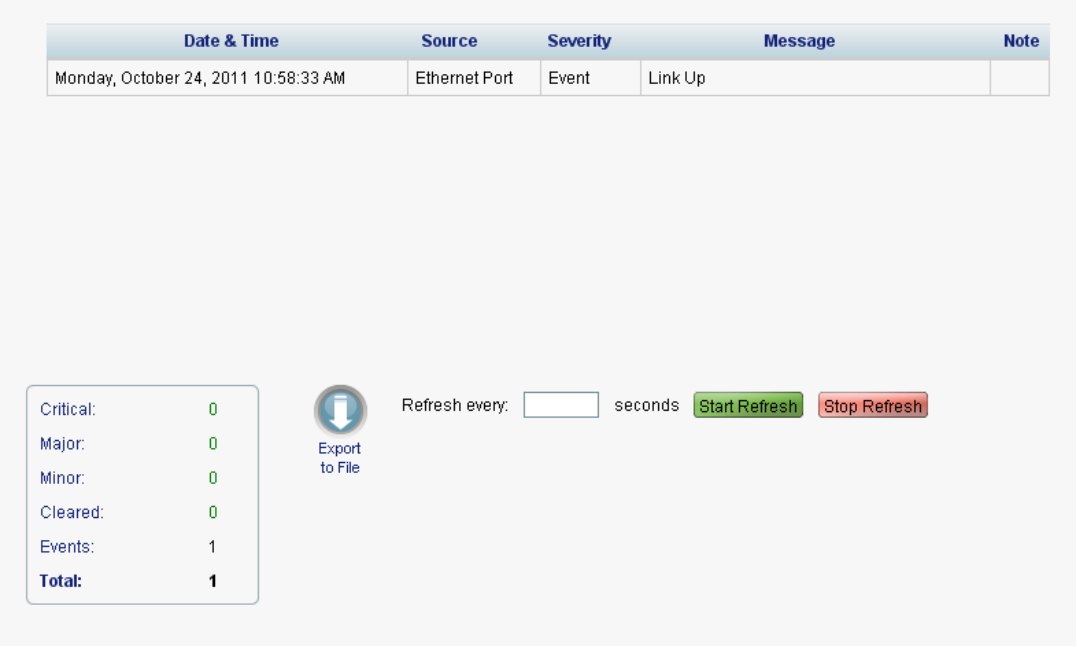


Figure 44: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.
   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 22: Events Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.6.3 Configuration Changes Tab

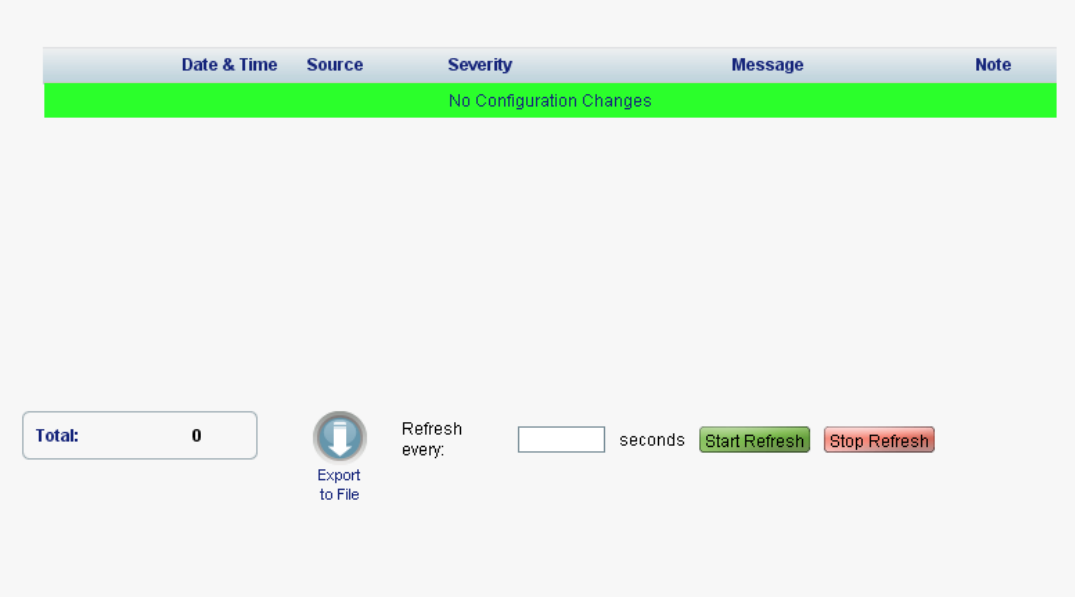


Figure 45: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 23: Configuration Changes Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

5.7 EDFA Faults

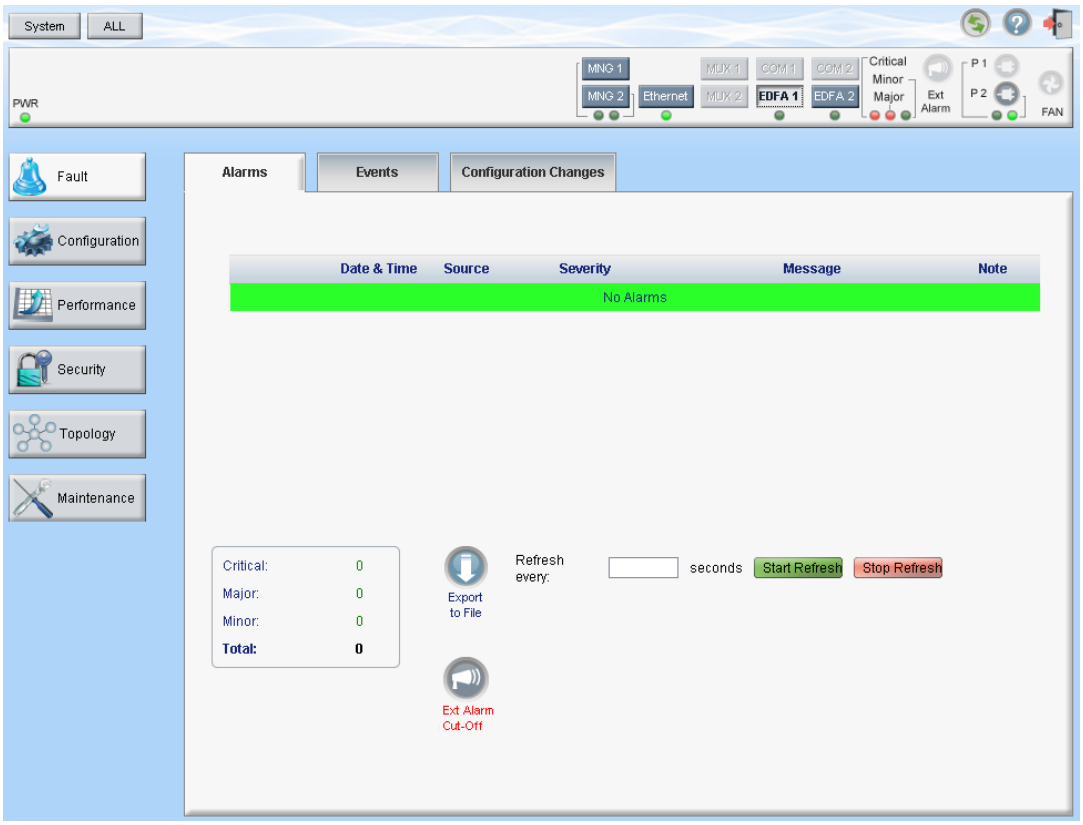


Figure 46: EDFA Fault Window

NOTE: The **EDFA** button is enabled only if an EDFA module is installed.

Use the EDFA Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the EDFA Fault window:

1. Click **Fault**.
2. Click an **EDFA** button to select the EDFA module.

   The appropriate EDFA Fault window opens.

5.7.1 Alarms Tab

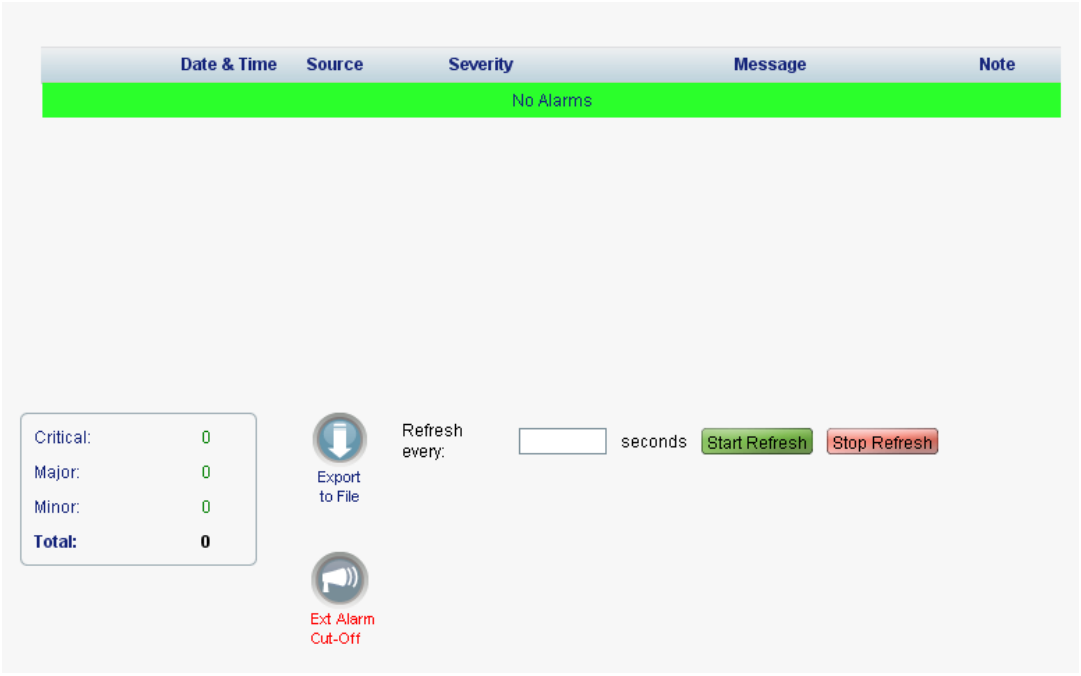


Figure 47: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

   NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 24: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.7.2 Events Tab

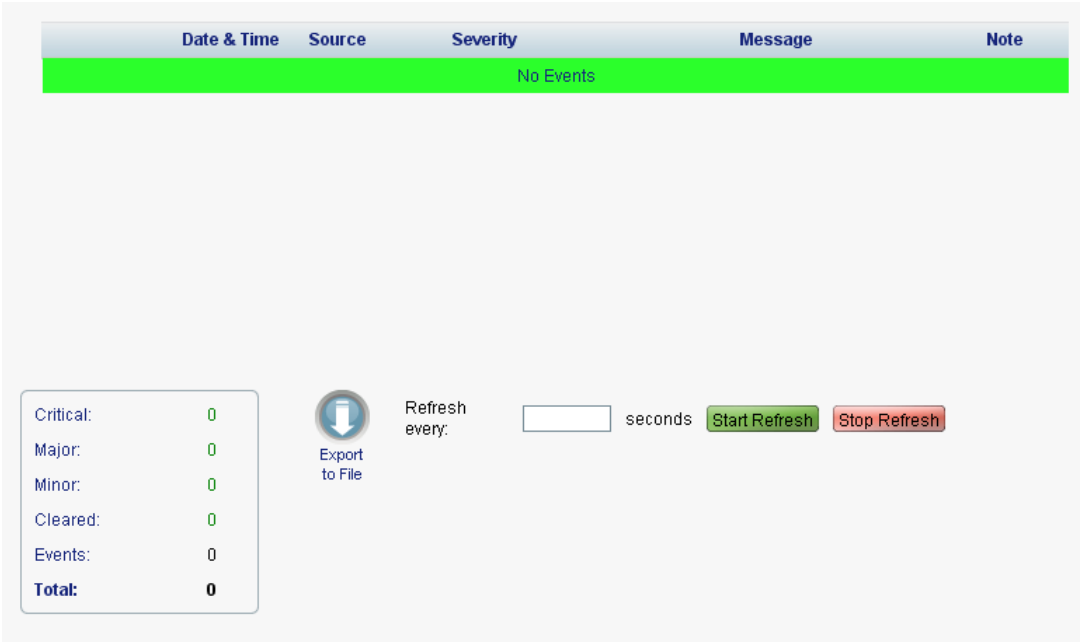


Figure 48: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.
   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 25: Events Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.7.3 Configuration Changes Tab

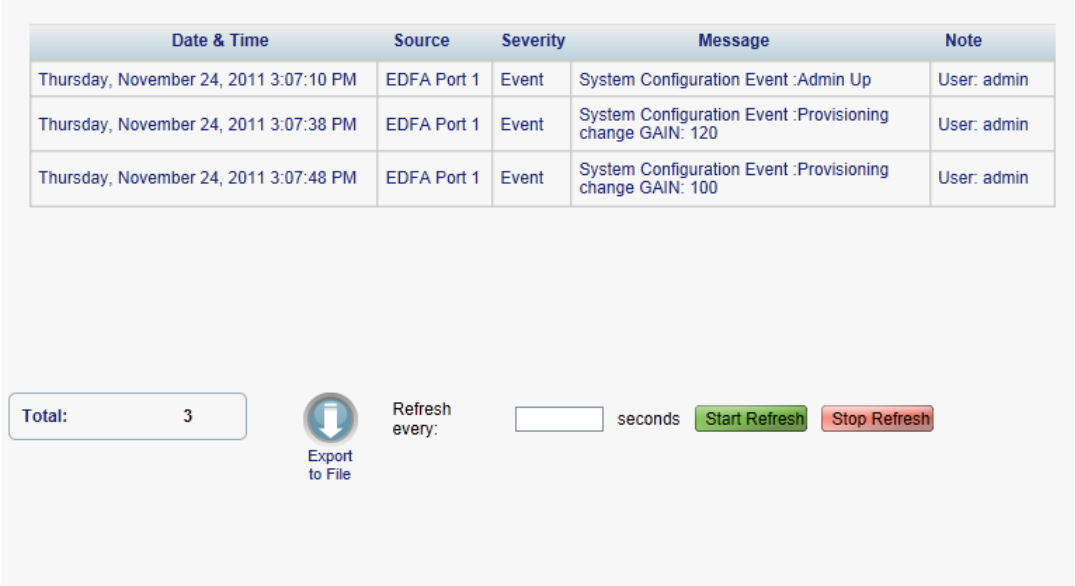


Figure 49: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 26: Configuration Changes Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

5.8 COM Port Faults

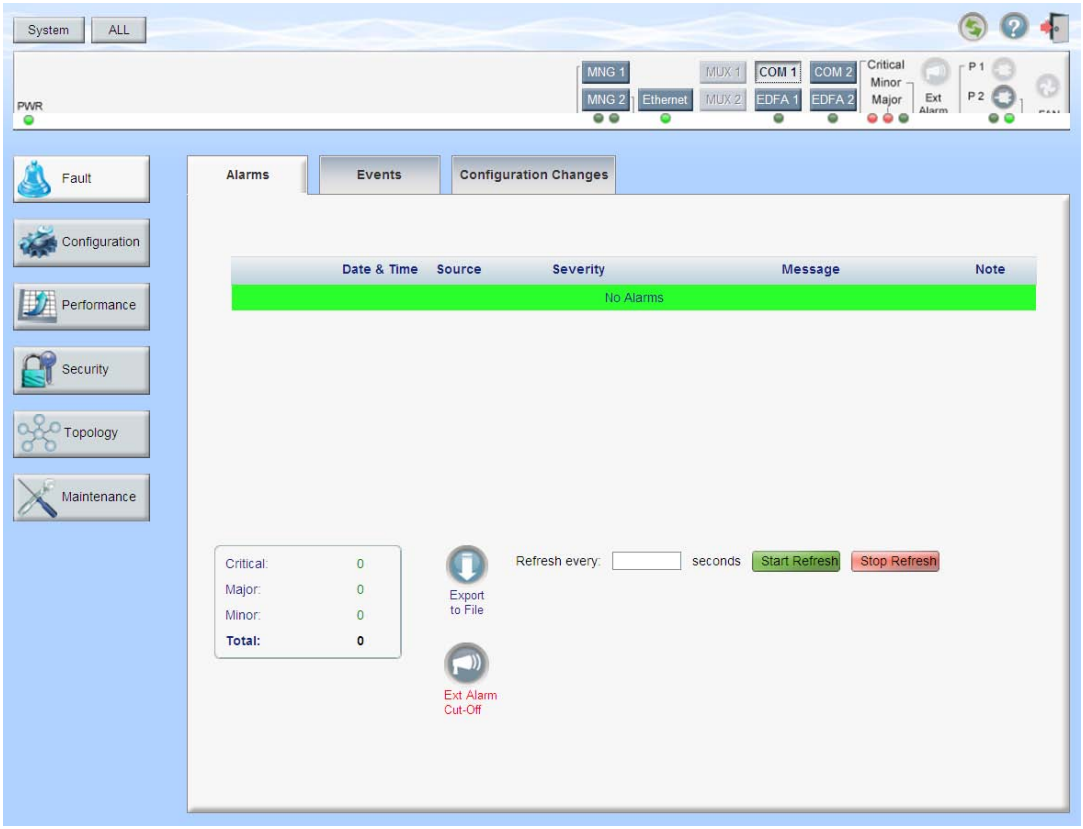


Figure 50: COM Port Fault Window

NOTE: The **COM** button is enabled only if an Optical Switch module is installed.

Use the COM Port Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the COM Port Fault window:

1. Click **Fault**.
2. Click a **COM** button to select the COM port.

   The appropriate COM Port Fault window opens.

5.8.1 Alarms Tab

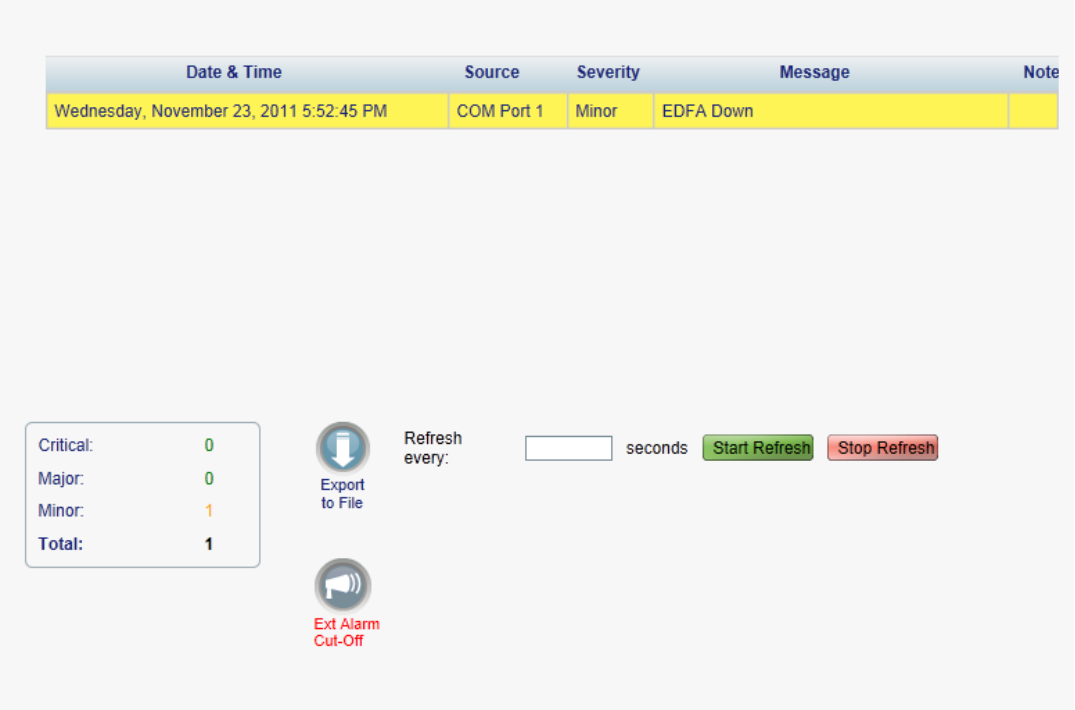


Figure 51: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

   NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

1. In the **Refresh every** field, type the number of seconds that the window should refresh.

   The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 27: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.8.2 Events Tab

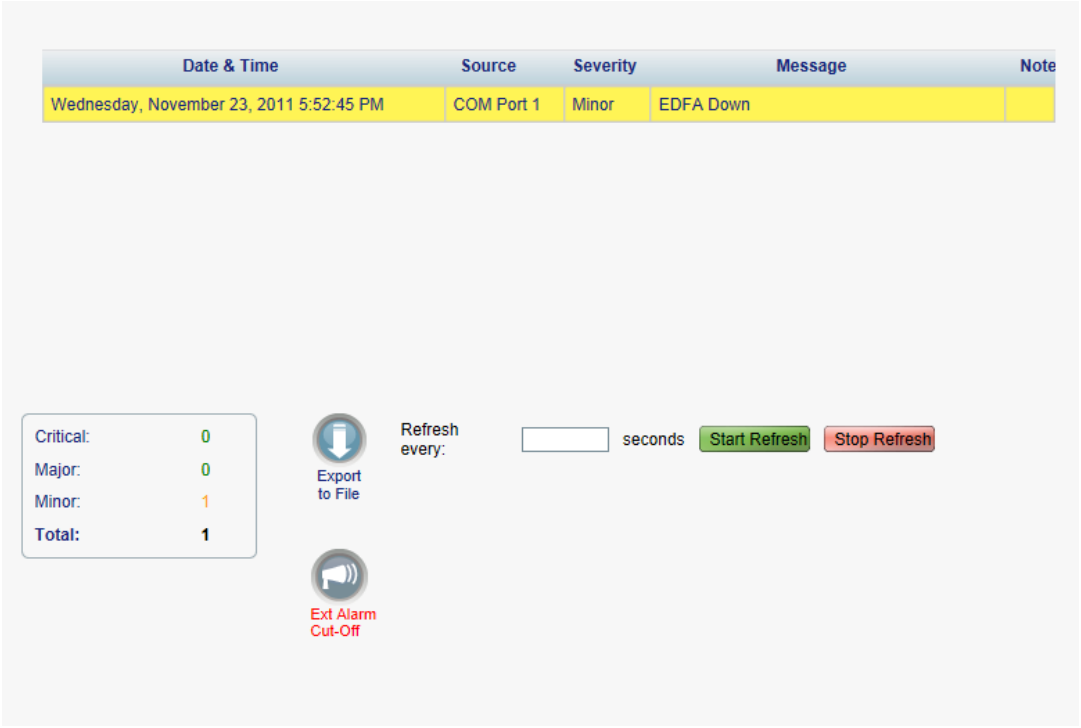


Figure 52: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.
   3. Click **OK**.

3. To set the refresh rate of the Fault display:

1. In the **Refresh every** field, type the number of seconds that the window should refresh.

   The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 28: Events Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.8.3 Configuration Changes Tab

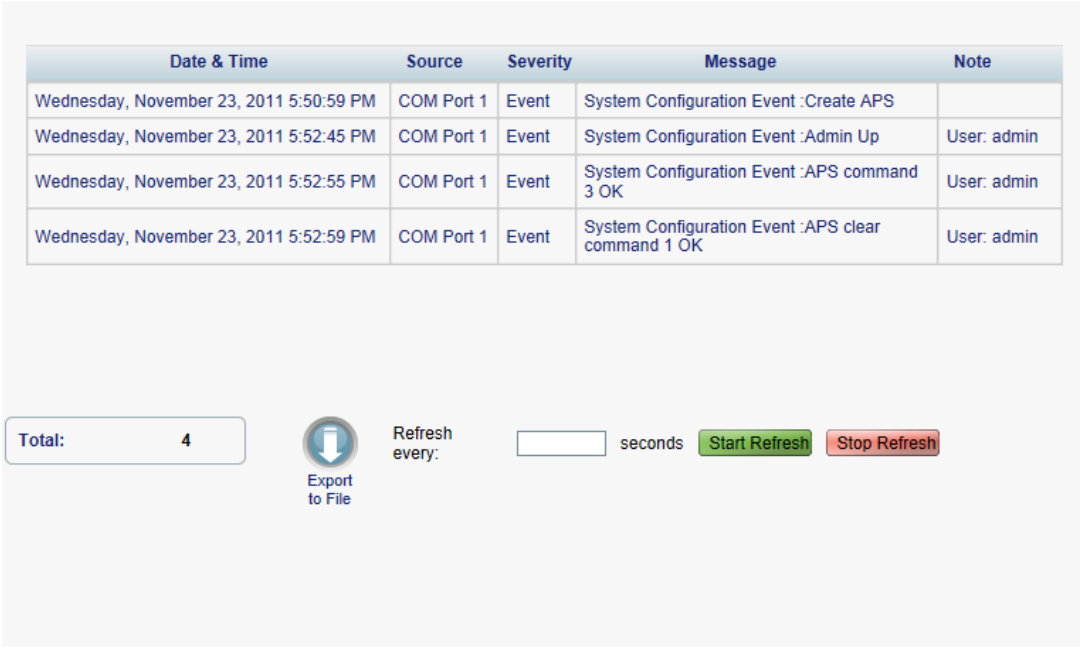


Figure 53: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File** .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh** .

The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 29: Configuration Changes Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

5.9 PSU Faults

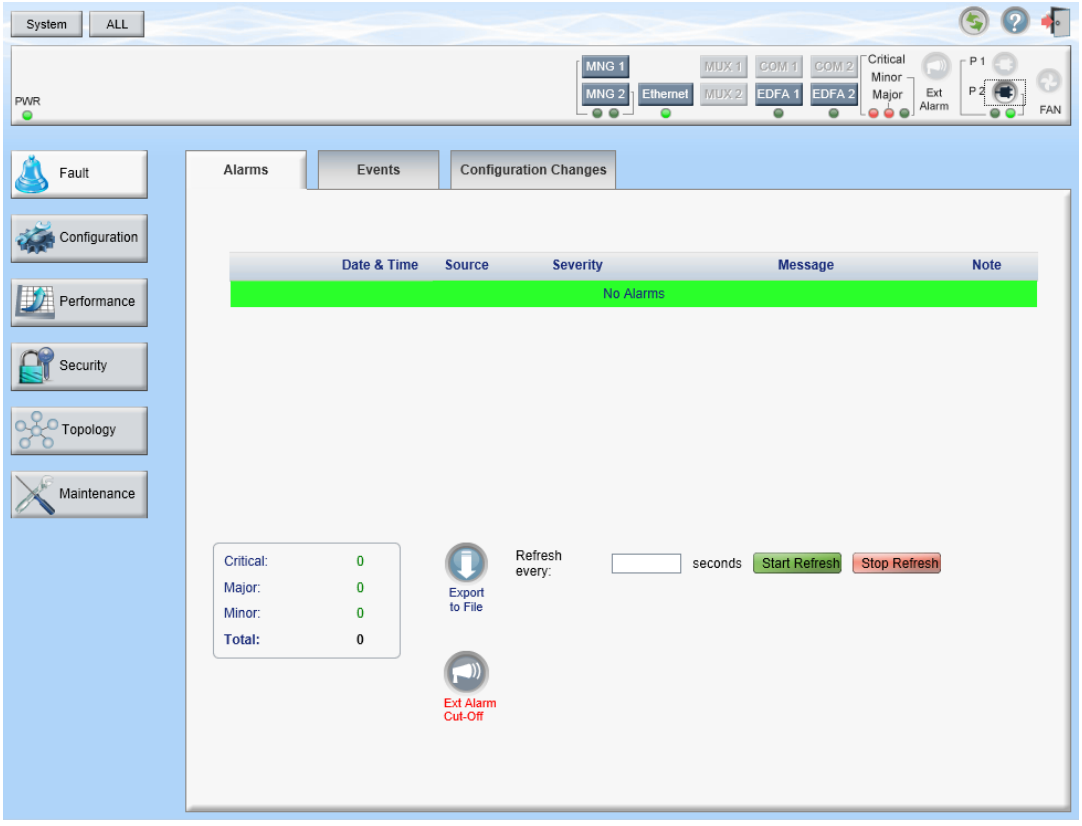


Figure 54: PSU Fault Window

Use the PSU Fault window to do the following:

- **Alarms tab**: View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display

- **Event Log tab**: View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Configuration Changes tab**: View the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display

To open the PSU Fault window:

1. Click **Fault**.
2. Click a **PSU** button  to select the PSU.

   The appropriate PSU Fault window opens.

5.9.1 Alarms Tab

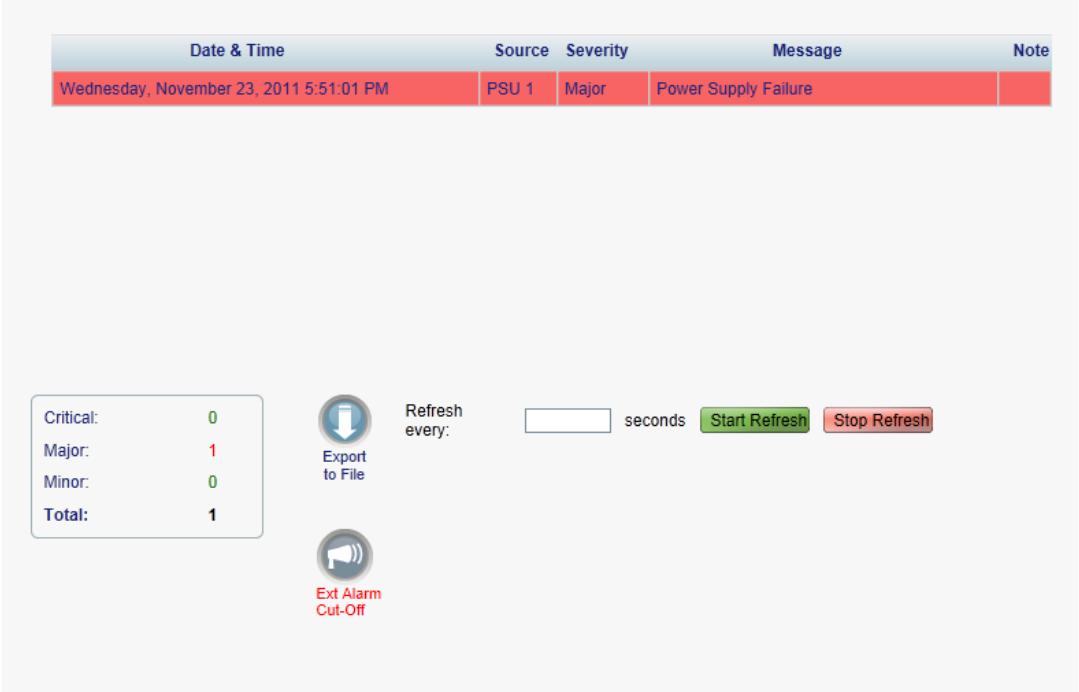


Figure 55: Alarms Tab

Use the Alarms tab to view the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view current alarms:

1. Click the **Alarms** tab.

   The Alarms tab opens displaying the list of current alarms along with the problems in the node. The fields are read only and explained in the following table.

   The color of the alarm background indicates the severity of the alarm:

   - **Red**: Critical or Major alarm
   - **Yellow**: Minor alarm

NOTE: The LED display reflects the actual LED indications on the unit. For the list of LEDs and their functions, see Technical Specifications.

2. To export the list of alarms to a file:
   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.
   2. Click **Save File**.
   3. Click **OK**.
3. To set the refresh rate of the Fault display:
   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.
   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.
4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.
5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.
6. To turn off the external alarm, click **Ext Alarm Cut-Off**  .

   The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

   NOTE: This action does not clear any alarms.

Table 30: Alarms Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the alarm was detected.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the alarm.	
Severity	The severity of the alarm.	Critical, Major, Minor
Message	The type of alarm.	
Note	Whether or not the alarm is service affecting.	• **S.A.**: The alarm is service affecting. • **Blank**: The alarm is not service affecting.

5.9.2 Events Tab

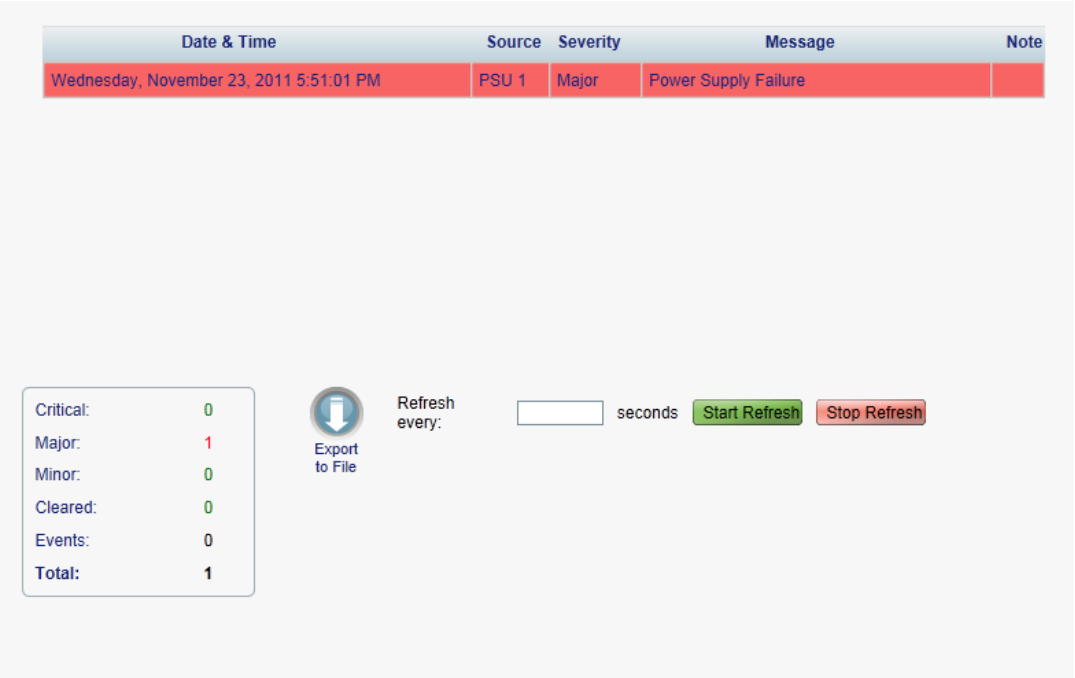


Figure 56: Events Tab

Use the Events tab to view the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Event Log:

1. Click the **Events** tab.

   The Events tab opens displaying the list of events and history of the node's fault notifications. The fields are read only and explained in the following table.

   The color of the event background indicates the severity of the event:

   - **Red**: Indicates the occurrence of a Critical or Major alarm
   - **Yellow**: Indicates the occurrence of a Minor alarm
   - **Green**: Indicates that the corresponding alarm is cleared
   - **White**: Indicates informational messages

2. To export the Event Log to a file:

   1. Click **Export File** .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

The minimum refresh rate is 2 seconds.

2. Click **Start Refresh**.

   The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 31: Events Tab Parameters

Parameter	Description	Format/Values
Date & Time	The date and time when the event occurred.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the event.	
Severity	The severity of the event.	Critical, Major, Minor, Cleared, Event
Message	The type of event.	
Note	Information related to the event.	• **S.A.**: The event is service affecting. • **Blank**: The event is not service affecting. • **Other**: Information related to the event.

5.9.3 Configuration Changes Tab

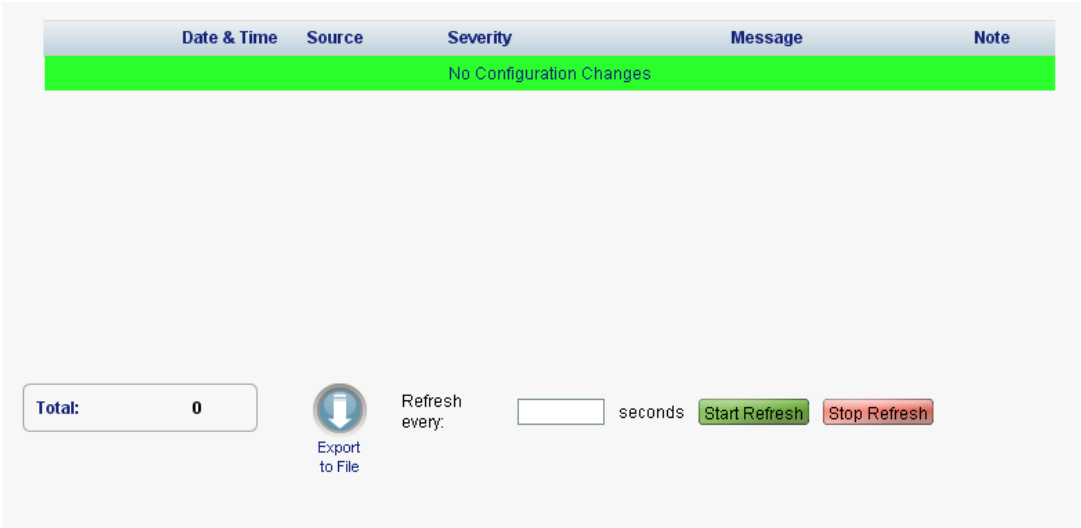


Figure 57: Configuration Changes Tab

Use the Configuration Changes tab to view the Configuration Changes Log, export the log to a file, set the refresh rate, and stop the automatic refresh of the Fault display.

To view the Configuration Changes Log:

1. Click the **Configuration Changes** tab.

   The Configuration Changes tab opens displaying the list of Configuration events and history of the node's fault notifications. The fields are read only and explained in the following table.

2. To export the Configuration Changes Log to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To set the refresh rate of the Fault display:

   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.

4. To refresh the Fault display manually, click **Refresh**  .

   The information is updated immediately.

5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 32: Configuration Changes Tab Parameters

Parameter	Description	Format / Values
Date & Time	The date and time when the change was made.	Day of the week, Month, Day, Year, HH:MM:SS, AM/PM
Source	The entity that caused the change.	
Severity	The severity of the change.	Critical, Major, Minor, Cleared, Event
Message	The type of change.	
Note	Information related to the change.	

6 Configuration Management

This chapter provides instructions for configuring the PL-1000IL.

For initial configuration of the PL-1000IL via a local terminal, and instructions for logging in and out of the Web application, see Operation and Preliminary Configuration (p. 27).

In this Chapter

6.1 Configuration Operations

Use the following configuration operations to manage the PL-1000IL:

- **System**
  - View general system information, such as hardware version and system uptime
  - View system inventory
  - Configure Simple Network Time Protocol (SNTP) parameters
  - Configure IP addresses, default gateway, and static routing
  - Configure SNMP parameters and traps
  - Define to which Syslog server you want the node to send the events
- **MNG Port**
  - View port status
  - Configure port parameters
  - Enable or disable a port
  - View SFP information
  - Configure ALS parameters
- **Ethernet Port**
  - View port status
  - Configure port parameters

- **EDFA Module**
  - View module status
  - Configure module parameters
  - Enable or disable a module
- **COM Port**
  - View port status
  - Configure port parameters
  - Enable or disable a port
  - Configure APS parameters
- **PSU Unit**
  - View PSU parameters
- **FAN Unit**
  - View FAN parameters

6.2 General Configuration Procedure

The following is the general procedure for viewing and configuring the PL-1000IL configuration. The specific procedures for each item are provided in the following sections.

To view and configure the PL-1000IL configuration:

1. Click **Configuration**.
2. Click the desired button in the upper portion of the window to select the item to view and/or configure:
   - **System** (see System Configuration (p. 95))
   - **MNG** (see Management Port Configuration (p. 108))
   - **Ethernet** (see Ethernet Port Configuration (p. 114))
   - **COM** (if present) (see COM Port Configuration (p. 116))
   - **EDFA** (if present) (see EDFA Configuration (p. 121))
   - **PSU** (see PSU Information (p. 124))
   - **FAN** (see FAN Unit Information (p. 125))

   The appropriate Configuration window opens.
3. Click a tab.

   The appropriate tab opens.
4. Fill in the fields as explained in the appropriate table. Note that some or all of the fields may be read only.
5. When all of the information is provided, click **Apply**.

6.3 System Configuration

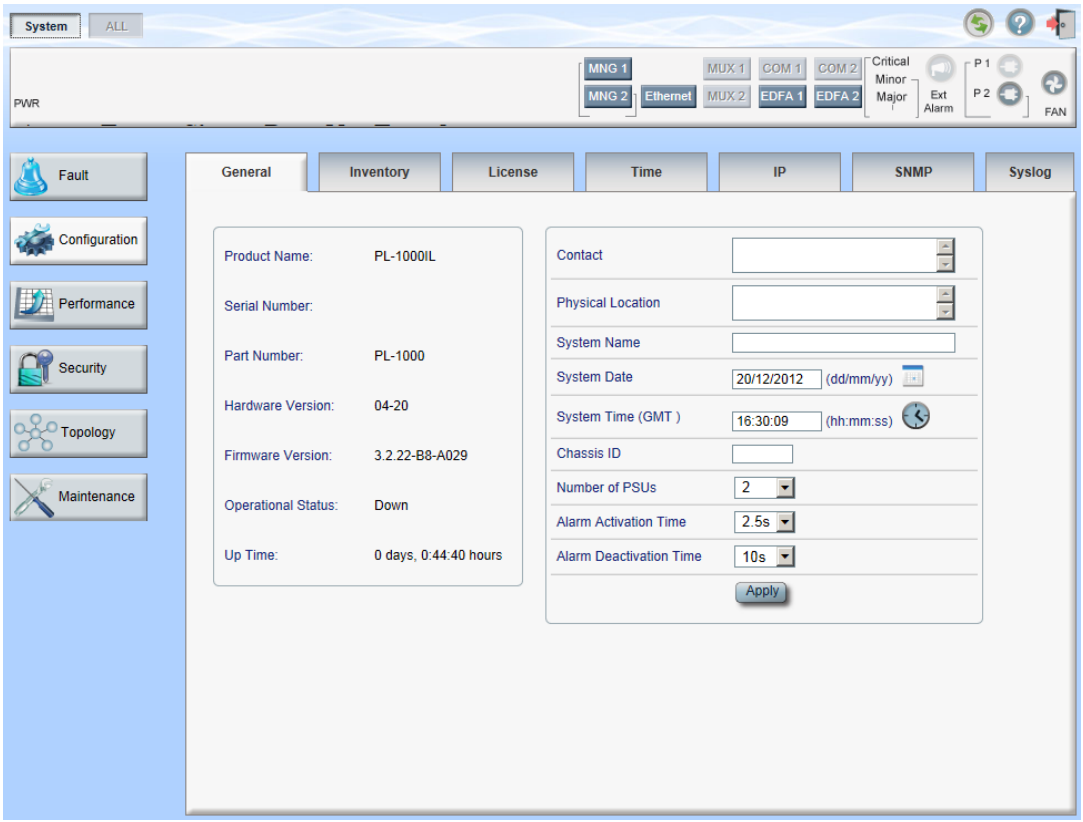


Figure 58: System Configuration Window

Use the System Configuration window to do the following:

- **General tab**: Configure general system parameters
- **Inventory tab**: View system inventory
- **License tab**: Not relevant for PL-1000IL
- **Time tab**: Configure SNTP parameters
- **IP tab**: Configure IP addresses and static routing
- **SNMP tab**: Configure SNMP parameters and traps
- **Syslog tab**: Configure Syslog servers

To open the System Configuration window:

1. Click **Configuration**.
2. Click **System**.

   The System Configuration window opens.

6.3.1 General Tab

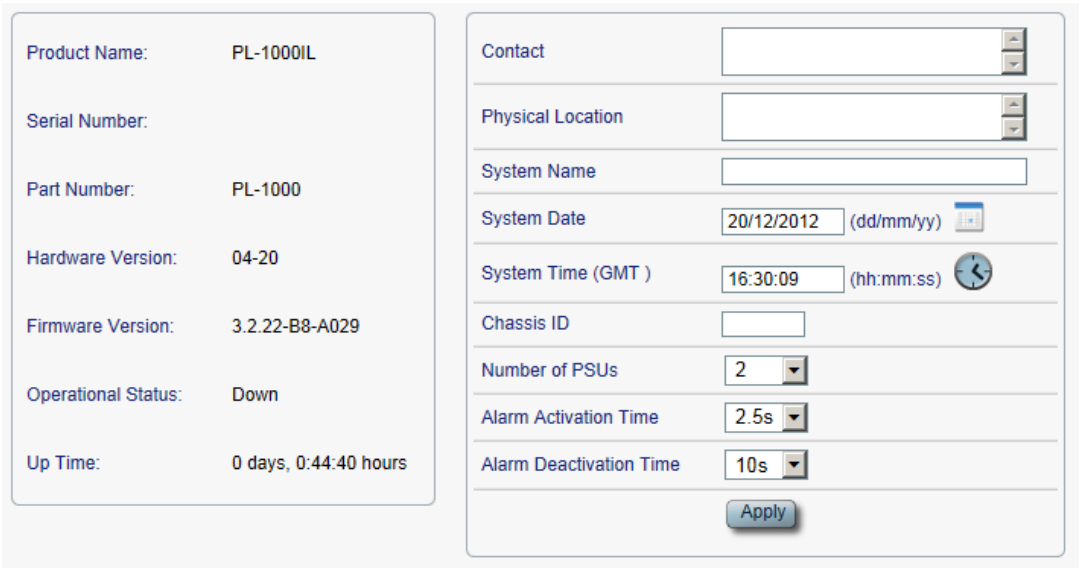


Figure 59: General Tab

Use the General tab to configure general system parameters.

To configure general system parameters:

1. Click the **General** tab.

   The General tab opens displaying the general system configuration.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 33: General Tab

Parameter	Description	Format / Values
Product Name	The name of the product.	PL-1000IL
Serial Number	The serial number of the entity.	Serial number
Part Number	The part number of the node.	Part number
Hardware Version	The hardware version of the system.	dd-dd (Major-Minor)
Firmware Version	The firmware version of the system.	Firmware version
Operational Status	The operational status of the system. This indicates if there is a failure in the system.	• **Up**: Normal operation • **Down**: Alarm is detected
Up Time	The system uptime. This shows how much time passed since last reset.	Elapsed time
System Temperature	The measured temperature of the system.	Celsius
Contact	The contact information for PacketLight Technical Support.	Free text
Physical Location	The address of the site.	Free text

Parameter	Description	Format/Values
System Name	The logical name given to the PL-1000IL.	Free text
System Date	Sets the current system date. This is the date used for time stamps.	• Set dd/mm/yy *or* • Select the date using the calendar  *or* • Will be set automatically by SNTP (if enabled)
System Time (GMT)	Sets the current system time of day. This is the time used for time stamps.	• Select hh:mm:ss *or* • Set the time using the clock  • *or* • Will be set automatically by SNTP (if enabled)
Chassis ID	The chassis number. This is used for the optimization of the topology display.	1,2, and so on **NOTE:** If several nodes are in the same location, they should have the same number (see Defining Multiple Nodes as Multi-Chassis (p. 154)).
Number of PSUs	The number of power supply units installed in the PL-1000IL.	1, 2
Alarm Activation Time	The time from defect detection till report, if defect is still constantly detected.	2.5-10 seconds Default: 2.5 seconds **NOTE:** Recommended to use the default time.
Alarm Deactivation Time	The time from no defect detection till report, if defect is still constantly not detected.	2.5-10 seconds Default: 10 seconds **NOTE:** Recommended to use the default time.

6.3.2 Inventory Tab

Name	Description	Serial Number	Hardware Rev	Part Number	Manufacturer
PL-1000IL	Main Board		04-20	PL-1000	PacketLight Networks
PSU 2	AC Power Interface Card	I0002DL	0200	PLPM81AAFF	
FAN Unit	Cooling Fan Unit		0100	FAN UNIT	
EDFA Module 1	Amplifier Module		-		
EDFA Module 2	Amplifier Module		-		
Dispersion Compensation	DCM 60km Fiber G652 Spacing 100Ghz.				
MNG 1	Non-WDM 850 nm	U8S20B9	NA	FTLF8524P2BNV	FINISAR CORP.

Figure 60: Inventory Tab

Use the Inventory tab to display information about the components currently installed in the system.

NOTE: Not all parameters are applicable for all type of components.

To view system inventory:

1. Click the **Inventory** tab.

   The Inventory tab opens displaying the system inventory. The fields are read only and explained in the following table.

2. To export the inventory list to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

Table 34: Inventory Tab Parameters

Parameter	Description
Name	The logical component name.
Description	The type of component.
Serial Number	The serial number of the component.
Hardware Rev	The hardware revision of the component.
Part Number	The part number of the component.
Manufacturer	The manufacturer of the component.

6.3.3 License Tab

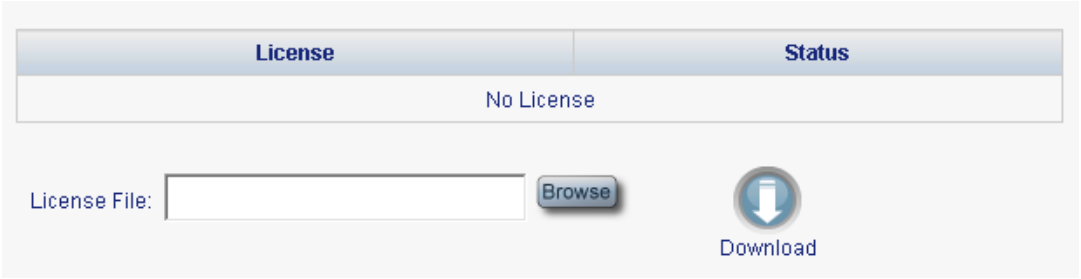


Figure 61: License Tab

NOTE: The License tab is only applicable for products requiring a license and is not relevant for PL-1000IL.

6.3.4 Time Tab

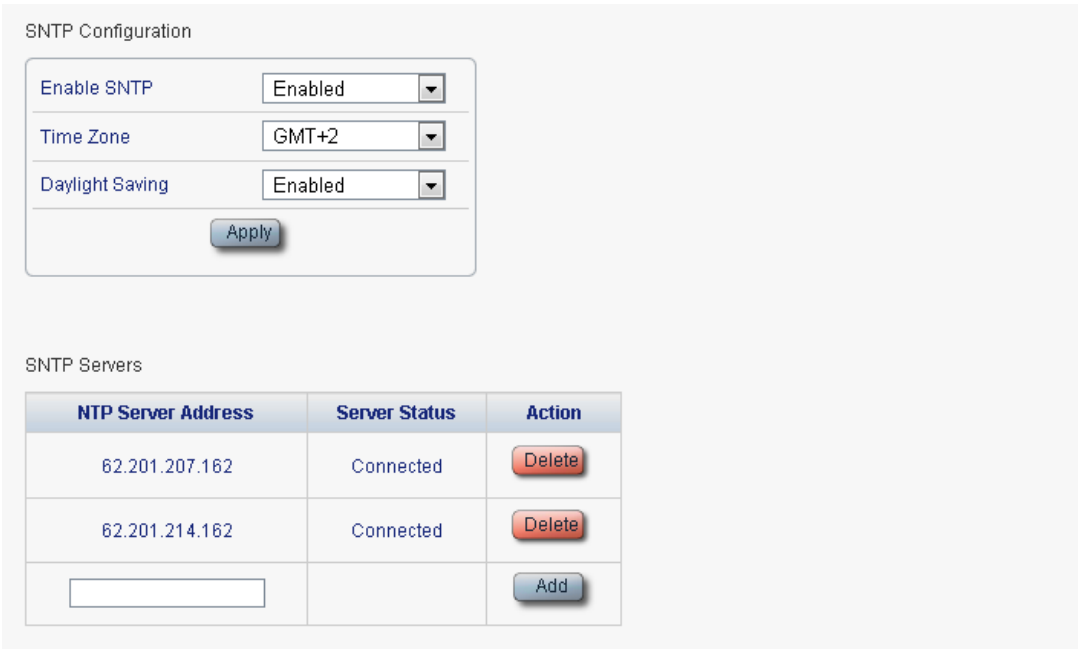


Figure 62: Time Tab

Use the Time tab to configure the PL-1000IL to use the standard protocol SNTP to synchronize its calendar time with an external accurate time server.

The PL-1000IL polls the list of defined servers every 10 minutes and takes the time from the first connected server.

NOTE:

- Update the **Daylight Saving** parameter twice a year.
- In order to communicate with the Time Server, the PL-1000IL must have an IP route to the defined server. Therefore, you may want to add the Time Server address to the **Static Routing** table (see IP Tab (p. 101)).

To configure SNTP:

1. Click the **Time** tab.

The Time tab opens displaying the Time and Time Server parameters. The fields are explained in the following table.

2. To configure the **Time** parameters:
   1. Fill in the following fields:
      - **Enable SNTP**
      - **Time Zone**
      - **Daylight Saving**
   2. Click **Apply.**
3. To add a server:
   1. In the **NTP Server Address,** type the IP address.
   2. Click **Add**.
4. To remove a server, click **Delete** in the corresponding line.

Table 35: Time Tab Parameters

Parameter	Description	Format/Values
Time Parameters		
Enable SNTP	Enables or disables the time synchronization process.	• **Enabled**: Operate the protocol • **Disabled**: Stop the protocol
Time Zone	Sets the time zone of the node that defines the conversion from Coordinated Universal Time (UTC) to local time.	GMT±n Select a time zone according to your geographical location. **NOTE:** The local time is shown.
Daylight Saving	Sets whether or not the clock will advance one hour due to summer time saving.	• **Enabled**: Advance the clock • **Disabled**: Do not advance the clock
Time Server Parameters		
NTP Server Address	The IP address of an SNTP time server.	IP address
Server Status	The status of the connection with the server.	• **Unknown**: No attempt has yet been made to connect to the server. • **Connected**: The link to the server has been established. • **Disconnected**: No link to the server. **NOTE:** This field is read only.

6.3.5 IP Tab

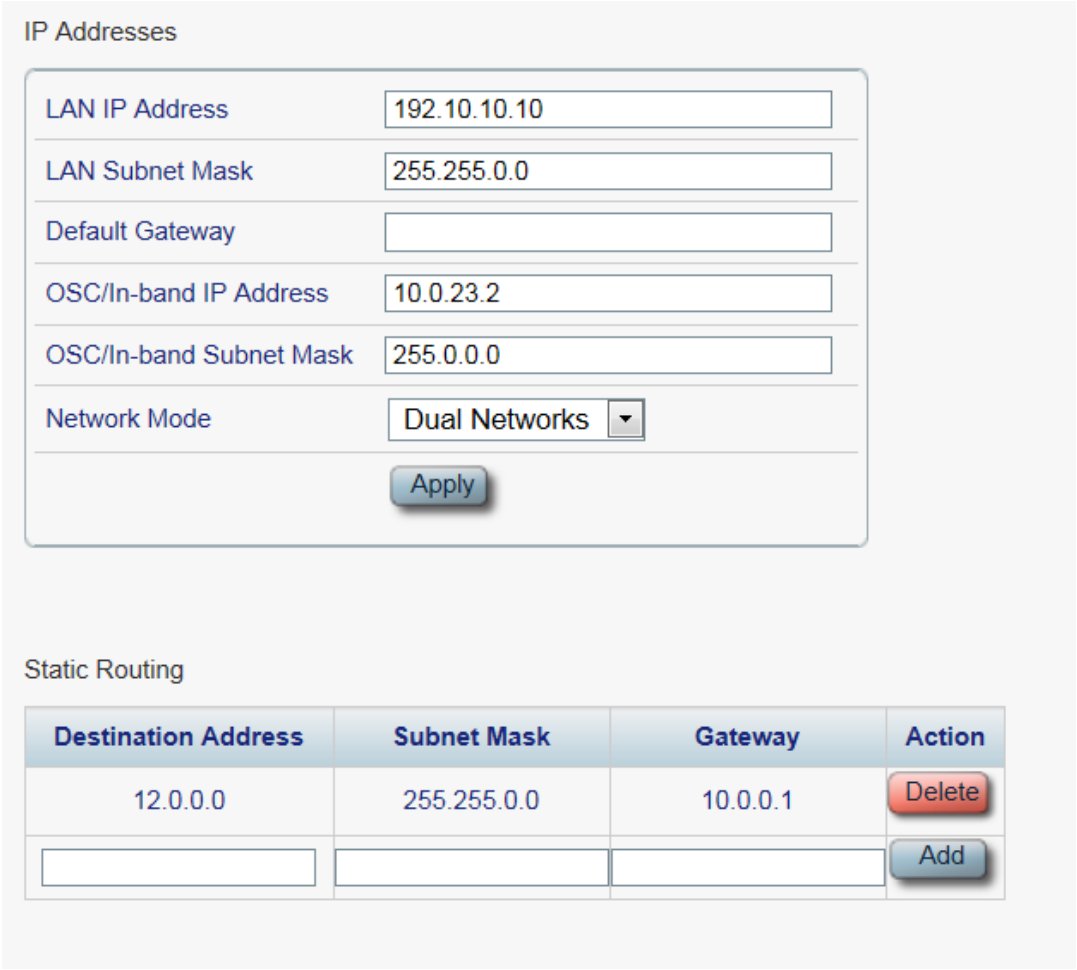


Figure 63: IP Tab - Dual Networks

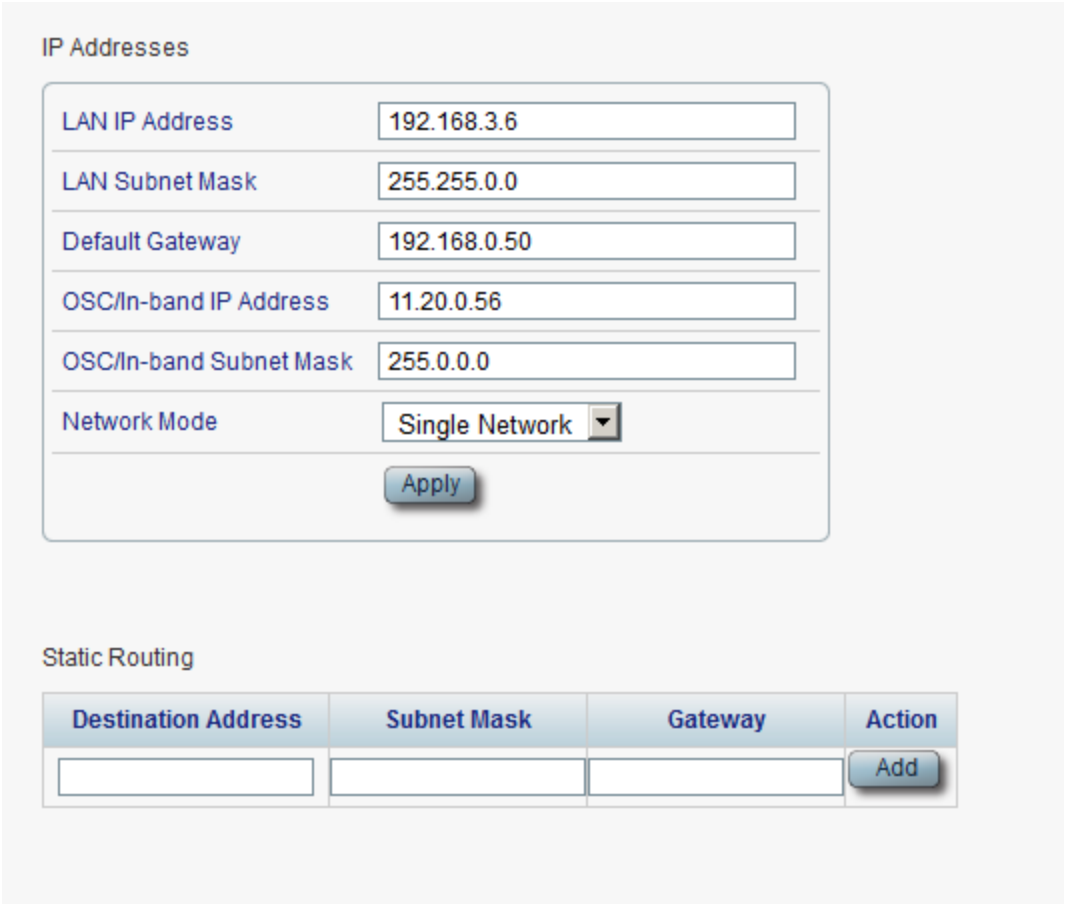


Figure 64: IP Tab - Single Network

Use the IP tab to configure the IP addresses, default gateway of the node, and static routing.

The PL-1000IL node supports two network modes: **Dual Networks** and **Single Network**.

- **Dual Networks**: In this mode, the node has two IP addresses; one is the **LAN IP Address** that is used for the LAN port and the other is the **OSC/ In-band Address** that is used for the MNG ports.
- **Single Network**: In this mode, the node has a single IP address (**LAN IP Address**) that is used for both the LAN port and the MNG ports.

NOTE:

- The **Single Network** mode is not provided for all hardware versions. For such versions, the **Network Mode** field is not available.
- Changing the network mode automatically restarts the PL-1000IL; the process may take a few minutes.
- Changing the IP address configuration may immediately stop management communication to the node.

- When configuring IP addresses, make sure that the IP address of the OSC/In-band is not in the same subnet as the LAN port, otherwise the routing of the management traffic will fail.

To configure IP addresses, default gateway, and static routing:

1. Click the **IP** tab.

   The IP tab opens displaying the IP Address and Static Routing configuration.

2. In the **LAN IP Address** section, fill in the fields as explained in the following table.

3. Click **Apply**.

   If you changed the network mode, the following confirmation message appears.

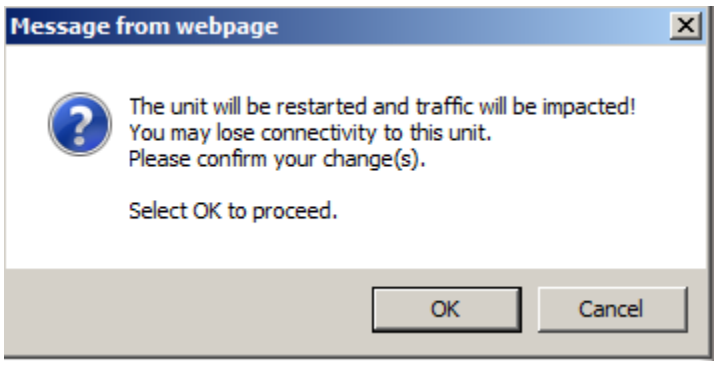


Figure 65: Confirm Changes

   Click **OK**.

4. To add a new static route:

   1. In the **Static Routing** section, fill in the following fields as explained in the following table.

   2. Click **Add**.

5. To remove a configured static route, click **Delete** in the corresponding line.

Table 36: IP Tab Parameters

Parameter	Description	Format/Values
IP Addresses		
LAN IP Address	The IP address of the Ethernet port.	IP address For example: `192.168.3.231`
LAN Subnet Mask	The subnet mask of the Ethernet port.	Dot notation For example: `255.255.248.0`
Default Gateway	The default gateway of the node.	Dot notation For example: `192.168.0.254`

Parameter	Description	Format / Values
OSC/In-band IP Address	The IP address of the OSC management channels.	Dot notation For example: `10.0.11.34` **NOTE:** ▪ This field is read only when **Network Mode** is set to **Single Network**. ▪ The same IP address applies to both MNG ports and for the in-band management channel
OSC/In-band Subnet Mask	The subnet mask of the OSC.	Dot notation For example: `255.0.0.0` **NOTE:** This field is read only when **Network Mode** is set to **Single Network**.
Network Mode	The mode of the network.	Dual Networks, Single Network **NOTE:** This field appears only for certain hardware versions.
Static Routing		
Destination Address	The address of the destination.	IP address For example: `11.0.3.24`
Subnet Mask	The subnet mask of the destination route.	Dot notation For example: `255.255.255.0`
Gateway	The address of the gateway for this destination.	IP address For example: `192.168.0.150`

6.3.6 SNMP Tab

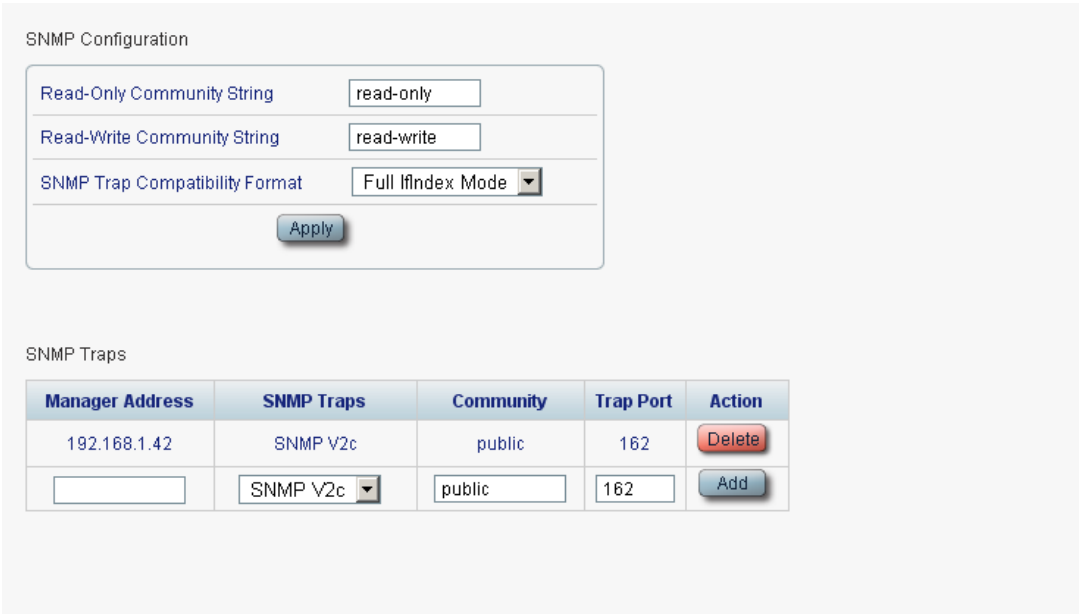


Figure 66: SNMP Tab

Use the SNMP tab to configure the SNMP configuration and traps.

WARNING:

- Changing the community strings may immediately affect the access of the current SNMP session.
- In order to send traps to the management system, the PL-1000IL must have a specific IP route. Therefore, if needed, add the management system address to the **Static Routing** table (see IP Tab (p. 101)).

To configure the SNMP configuration and traps:

1. Click the **SNMP** tab.

   The SNMP tab opens displaying the SNMP configuration and traps.

2. In the **SNMP Configuration** section, fill in the following fields as explained in the following table.
3. Click **Apply**.
4. To send SNMP traps to a given management system:
   1. In the **SNMP Traps** section, fill in the following fields as explained in the following table.
   2. Click **Add**.
5. To stop SNMP traps from being sent to a given management system, click **Delete** in the corresponding line.

Table 37: SNMP Tab Parameters

Parameter	Description	Format/Values
SNMP Configuration		
Read-Only Community String	The community string of the SNMP to be used for read operations.	A string of alphanumeric characters without spaces. Default: read-only
Write-Only Community String	The community string of the SNMP to be used for write operations.	A string of alphanumeric characters without spaces. Default: read-write
SNMP Trap Compatibility Format	Determines the format of the IfIndex that is sent with the SNMP traps.	• **Port IfIndex Mode**: Used with the legacy Network Management System (NMS) • **Full IfIndex Mode**: Used with any other NMS.
SNMP Traps		
Manager Address	The address of the management system.	IP address For example: `192.168.1.50`
SNMP Traps	The SNMP trap format.	SNMPV2c, SNMPV1 Default: SNMPV2c

Parameter	Description	Format / Values
Community	The community string of the traps.	public (default)
Trap Port	The UDP port number.	162 (default)

6.3.7 Syslog Tab

Figure 67: Syslog Tab

Use the Syslog tab to define the Syslog servers you want the node to send the log of events.

A system log of the last 512 events is kept by the node and may be retrieved using the Event Log (see Events).

For keeping a longer history of the events, you may choose to use a Syslog server running the Syslog protocol as defined by RFC 5424, to receive the node events and save them on an external Syslog system.

To configure Syslog servers:

1. Click the **Syslog** tab.

   The Syslog tab opens displaying the Syslog configuration.

2. To send events to a given Syslog server:

   1. In the **Syslog Servers** section, fill in the following fields as explained in the following table.
   2. Click **Add**.

      The following confirmation message appears.

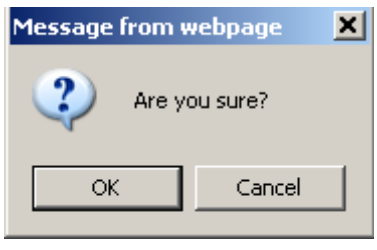


Figure 68: Confirm Configuration

   3. Click **OK**.

3. To remove a configured Syslog server:
   1. Click **Delete** in the corresponding line.

      The following confirmation message appears.

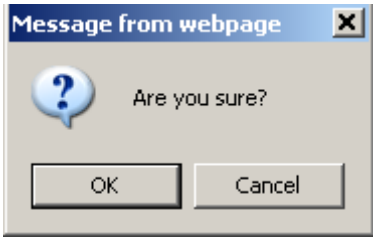


Figure 69: Confirm Configuration

   2. Click **OK**.

Table 38: Syslog Tab Parameters

Parameter	Description	Format/Values
Syslog Server Address	The address of the Syslog system.	IP address For example: 192.168.1.37
Syslog port	The UDP port number.	Port number Default: 514
Message Level	The supported message filter level.	• **Traps**: Traps only • **Log**: Log messages • **Debug**: Log and debug messages Default: Traps

6.4 Management Port Configuration

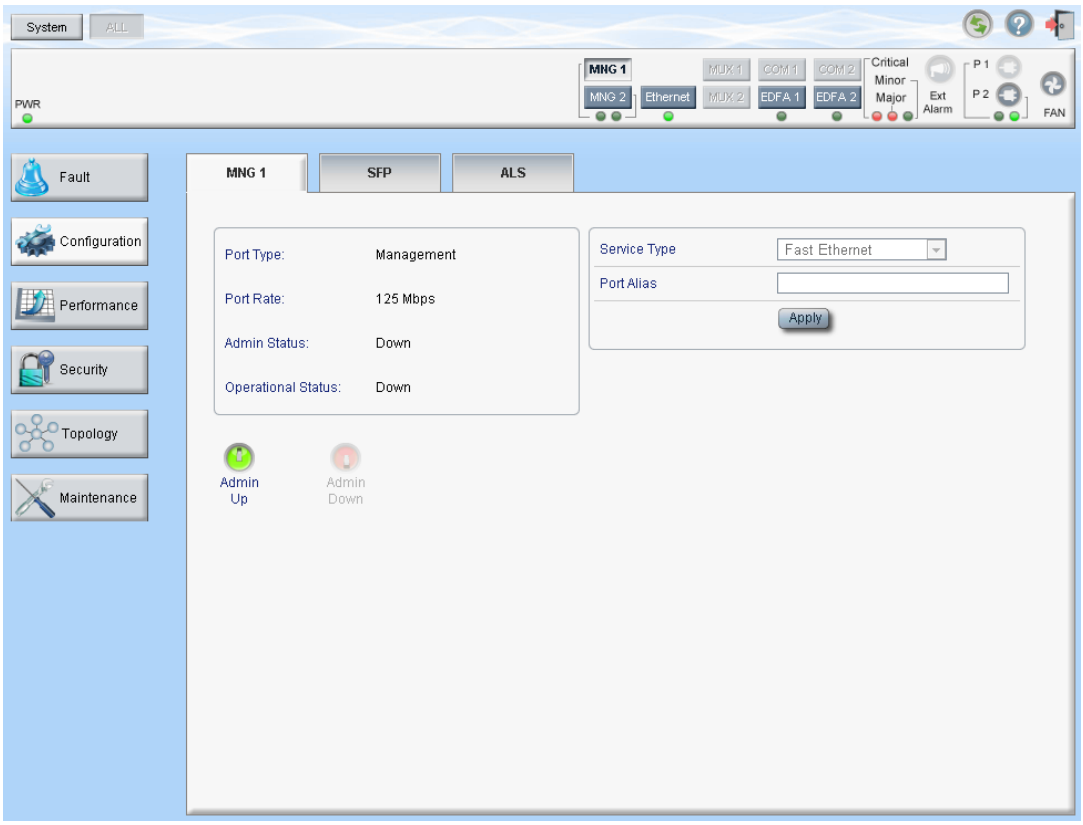


Figure 70: Management Port Configuration Window

Use the Management Port Configuration window to do the following:

- **MNG tab**: Configure an MNG port and enable/disable the port
- **SFP tab**: Configure the SFP module
- **ALS tab**: Configure ALS for an MNG port

To open the Management Port Configuration window:

1. Click **Configuration**.
2. Click an **MNG** button to select the management port.

   The appropriate Management Port Configuration window opens.

6.4.1 MNG Tab

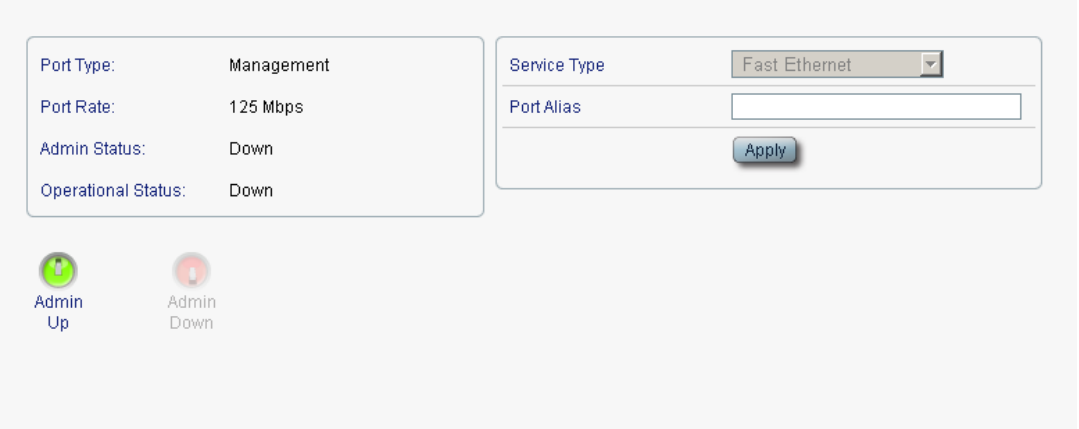


Figure 71: MNG Tab

Use the MNG tab to configure a management port and enable/disable the port.

To configure a management port:

1. Click the **MNG** tab.

   The MNG tab opens displaying the management port configuration.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.
4. To enable the port:
   1. Click **Admin Up**  .

      The following confirmation message appears.

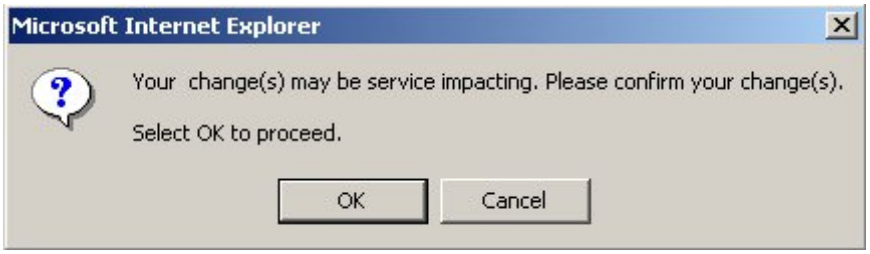


Figure 72: Confirm Changes

   2. Click **OK**.

      The selected port is enabled, the **Admin Up** button is disabled, and the **Admin Down** button is enabled.
5. To disable the port:
   1. Click **Admin Down**  .

The following confirmation message appears.

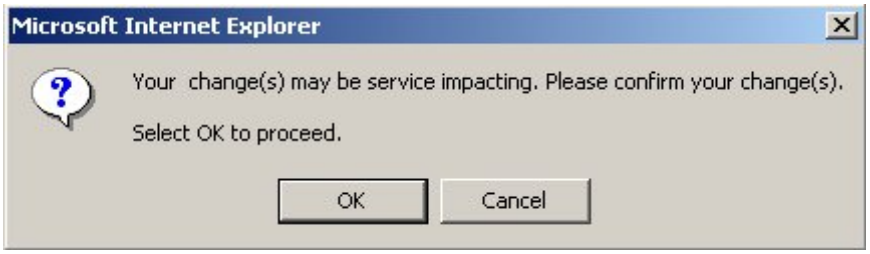


Figure 73: Confirm Changes

2. Click **OK**.

   The selected port is disabled, the **Admin Up** button is enabled, and the **Admin Down** button is disabled.

Table 39: MNG Tab Parameters

Parameter	Description	Format/Values
Port Type	The type of port.	Management
Port Rate	The maximum bit rate of the OSC management port.	125 Mbps
Admin Status	The administrative status of the port.	Up, Down To change the value, click **Admin Up** or **Admin Down**.
Operational Status	The operational status of the port. This indicates if there is a failure in the port.	• **Up**: Normal operation • **Down**: Alarm is detected or A**dmin Down**
Service Type	The management type.	Fast Ethernet (default)
Port Alias	The logical name given to the port for identification purposes.	Free text

6.4.2 SFP Tab

Figure 74: SFP Information Tab

Use the SFP tab to display information about the type and status of the optical transceiver inserted in the selected port and configure the override low receiver power alarm threshold.

To configure the SFP module:

1. Click the **SFP** tab.

   The SFP tab opens displaying the SFP configuration.

2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 40: SFP Tab Parameters

Parameter	Description	Format/Values
Vendor Name	The name of the SFP vendor.	String
Nominal Wavelength	The defined wavelength of the SFP.	nm
WDM Class	The type of SFP.	No WDM, CWDM, DWDM
Part Number	The part number of the SFP.	String
Serial Number	The serial number of the SFP.	String
WDM Channel Spacing	The channel spacing of the SFP.	• **CWDM**: nm • **DWDM**: GHz
Connector Type	The type of SFP connector.	• **Optical**: LC • **Electrical**: RJ45

Parameter	Description	Format / Values
Transmitter Output Power	The measured output power of the SFP.	dBm
Receiver Input Power	The measured input power of the SFP.	dBm
Temperature	The measured temperature of the SFP.	Celsius
ESCON capabilities	The SP capabilities of the ESCON services are marked.	
SONET/SDH capabilities	The SFP capabilities of the OC-3, OC-12, OC-48, and OC-192 services are marked.	
Ethernet capabilities	The SFP capabilities of the 100Mb, GbE, and 10GbE Ethernet services are marked.	
FC capabilities	The SFP capabilities of the FC services are marked.	
High Receiver Power Default Threshold	The default threshold for the High Receiver Power alarm.	dBm
Low Receiver Power Default Threshold	The default threshold for Low Receiver Power alarm.	dBm
Override Low Receiver Power Alarm Threshold	The configured threshold for the Low Receiver Power alarm.	dBm

6.4.3 ALS Tab

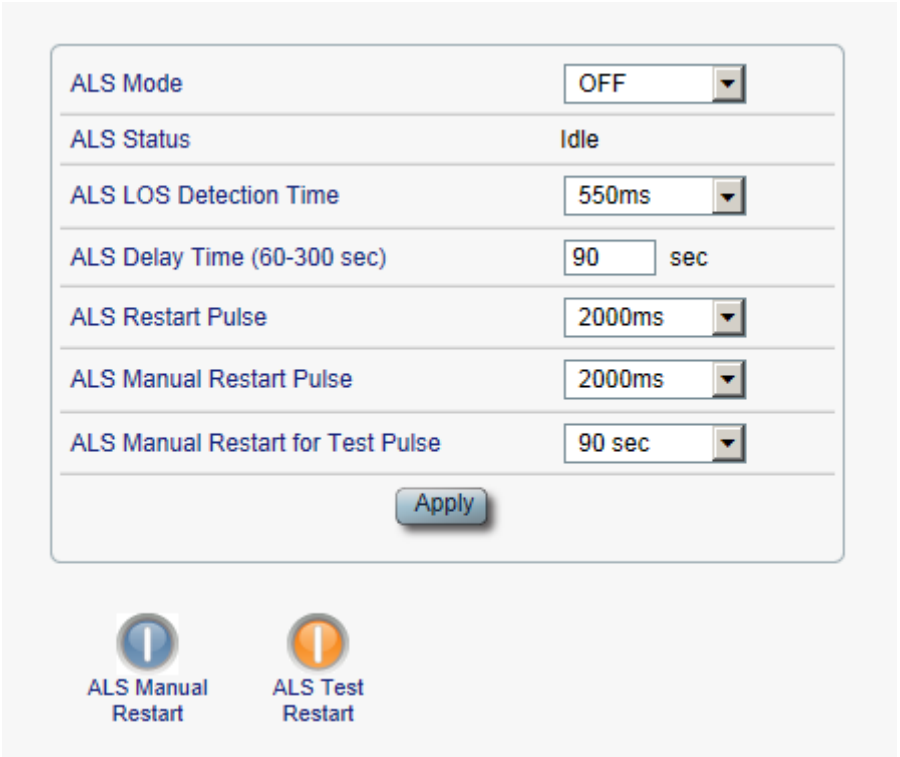


Figure 75: ALS Tab

Use the ALS tab to configure ALS for a selected port.

The ALS is designed for eye safety considerations. It provides the capability of automatically reducing the optical power when there is loss of optical power. The loss of optical power can be caused by cable break, equipment failure, connector unplugging, and so on.

The PL-1000IL implements the ALS optical safety procedure as defined by the ITU-T Recommendation G.664.

A laser restart operation (automatic and manual) is also provided to facilitate an easy restoration of the system after reconnection of the link.

To configure ALS:

1. Click the **ALS** tab.

   The ALS tab opens displaying the ALS configuration for the selected port.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.
4. To initiate a manual restart pulse, click **ALS Manual Restart**  .
5. To initiate a manual restart for test pulse, click **ALS Test Restart**  .

Table 41: ALS Tab Parameters

Parameter	Description	Format/Values
ALS Mode	Enable or disable ALS for this port.	OFF, ON Default: OFF
ALS Status	The current status of the ALS.	Idle, Active
ALS LOS Detection Time	The time to declare optical LOS present or clear (in milliseconds).	550 ± 50 ms Default: 550 ms
ALS Delay Time (60-300 sec)	The duration between two laser reactivations (in seconds).	60 to 300 sec Default: 90 sec
ALS Restart Pulse	The automatic restart pulse width (in milliseconds).	2000 ± 250 ms Default: 2000 ms **NOTE:** Automatic mode only.
ALS Manual Restart Pulse	Manual restart pulse width (in milliseconds).	2000 ± 250 ms Default: 2000 ms **NOTE:** Manual mode only.
ALS Manual Restart for Test Pulse	Manual restart for test pulse width (in seconds).	90 ± 10 sec Default: 90 sec **NOTE:** Manual restart only.

6.5 Ethernet Port Configuration

Use the Ethernet Port Configuration window to configure the Ethernet port status and parameters.

WARNING: Changing the link parameters of the Ethernet port may cause a loss of connection to the node.

NOTE: The Auto Negotiation protocol is defined by IEEE 802.3 as the standard method by which two connected Ethernet devices choose common transmission parameters, such as speed and duplex mode.

To open the Ethernet Port Configuration window:

1. Click **Configuration**.
2. Click **Ethernet** to select the Ethernet port.

   The Ethernet Port Configuration window opens.

6.5.1 Ethernet Tab

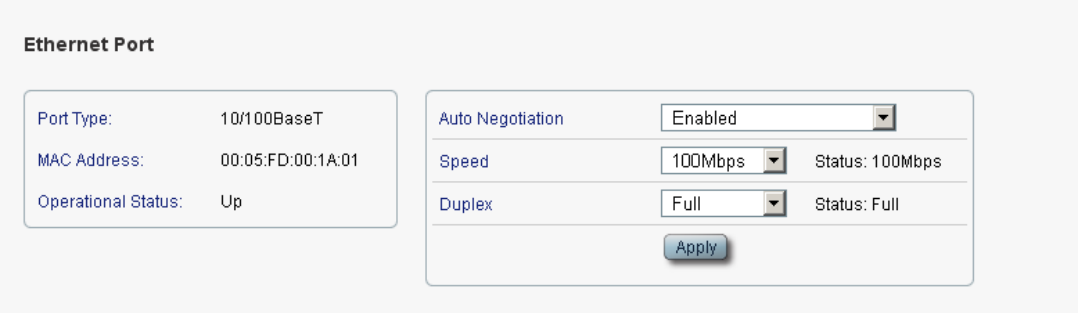


Figure 76: Ethernet Tab

Use the Ethernet tab to configure the Ethernet port.

To configure the Ethernet port:

1. Click **Ethernet** to select the Ethernet port.

   The Ethernet tab opens displaying the Ethernet port configuration.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 42: Ethernet Tab Parameters

Parameter	Description	Format/Values
Port Type	The type of port.	10/100 Base-T
MAC Address	The MAC address of the Ethernet port.	XX:XX:XX:XX:XX:XX
Operational Status	The operational status of the port. This indicates if there is a failure in the port.	• **Up**: Normal operation • **Down**: Alarm is detected or **Admin Down**

Parameter	Description	Format / Values
Auto Negotiation	Whether or not the auto negotiation of the Ethernet link parameters should be performed.	• **Enabled**: Auto negotiation is performed during Ethernet link establishment. • **Disabled**: The Ethernet link parameters are manually determined by the settings of the **Speed** and **Duplex** fields. Default: Enabled **NOTE:** The advertised capabilities of the Ethernet port are: ▪ **Speed**: 10 Mbps, 100 Mbps ▪ **Duplex**: Full, Half ▪ **Flow Control**: Disabled
Speed	The actual speed of the port.	10 Mbps, 100 Mbps **NOTE:** This field is applicable only if **Auto Negotiation** is enabled.
Speed (Manual)	The manual value of the speed of the Ethernet port.	10 Mbps, 100 Mbps **NOTE:** This field is applicable only when **Auto Negotiation** is disabled.
Status (Speed)	The actual speed of the Ethernet port.	10 Mbps, 100 Mbps
Duplex (Manual)	The manual value of the duplex mode of the Ethernet port.	Full, Half Default: Full **NOTE:** This field is applicable only if **Auto Negotiation** is disabled.
Status (Duplex)	The actual duplex of the Ethernet port.	Full, Half

6.6 COM Port Configuration

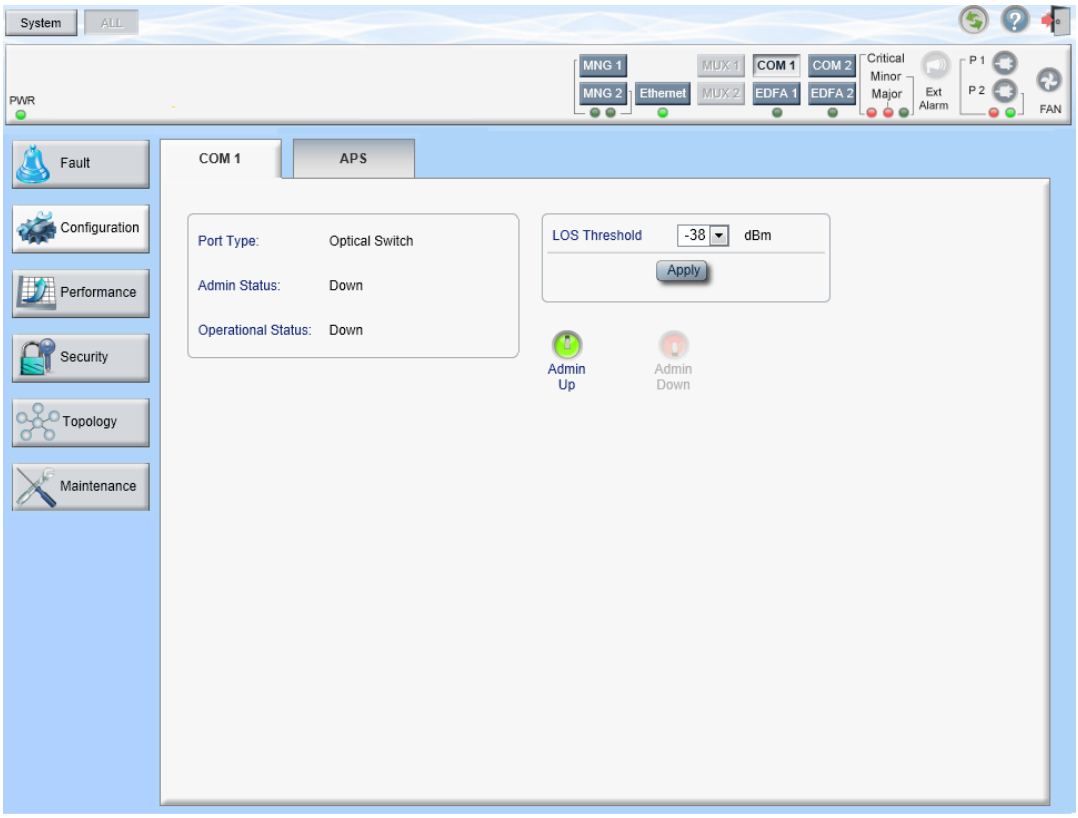


Figure 77: COM Port Configuration Window

NOTE: The **COM** button is enabled only if an Optical Switch module is installed.

Use the COM Port Configuration window to do the following:

- **COM tab**: Configure a COM port and enable/disable the port
- **APS tab**: Configure APS for a COM port

To open the COM Port Configuration window:

1. Click **Configuration**.
2. Click a COM button to select the COM port.

   The appropriate COM Port Configuration window opens.

6.6.1 COM Tab

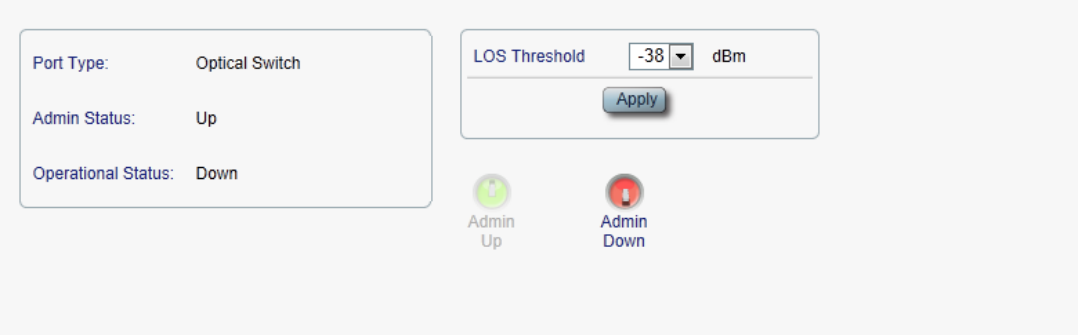


Figure 78: COM Tab

Use the COM tab to configure a COM port and enable/disable the port.

NOTE: Setting or changing the parameters of one COM port automatically changes the settings of the other COM port.

To configure a COM port:

1. Click the **COM** tab.

   The COM tab opens displaying the COM port configuration.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.
4. To enable the port:
   1. Click **Admin Up**  .

      The following confirmation message appears.

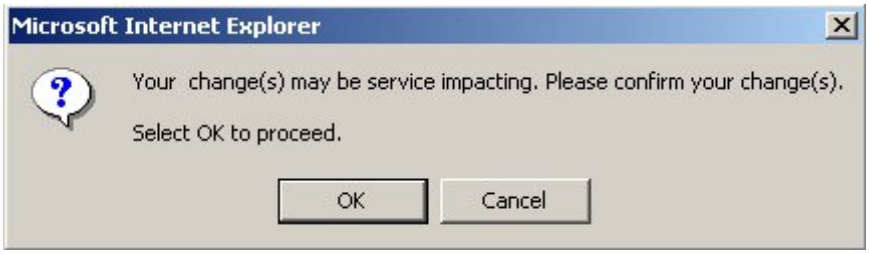


Figure 79: Confirm Changes

   2. Click **OK**.

      The selected port is enabled, the **Admin Up** button is disabled, and the **Admin Down** button is enabled.
5. To disable the port:
   1. Click **Admin Down**  .

The following confirmation message appears.

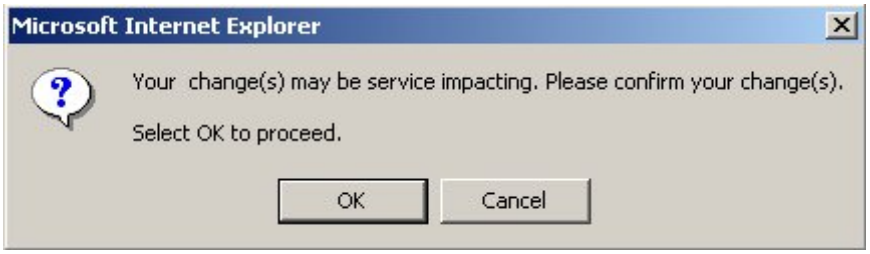


Figure 80: Confirm Changes

2. Click **OK**.

   The selected port is disabled, the **Admin Up** button is enabled, and the **Admin Down** button is disabled.

Table 43: COM Tab Parameters

Parameter	Description	Format / Values
Port Type	The type of port.	Optical Switch
Admin Status	The administrative status of the port.	Up, Down To change the value, click **Admin Up** or **Admin Down**.
Operational Status	The operational status of the port. This indicates if there is a failure in the port.	• **Up**: Normal operation • **Down**: Alarm is detected or **Admin Down**
LOS Threshold	The LOS detection threshold used for optical switching.	-40 to -25 dBm Default: -38 dBm

6.6.2 APS Tab

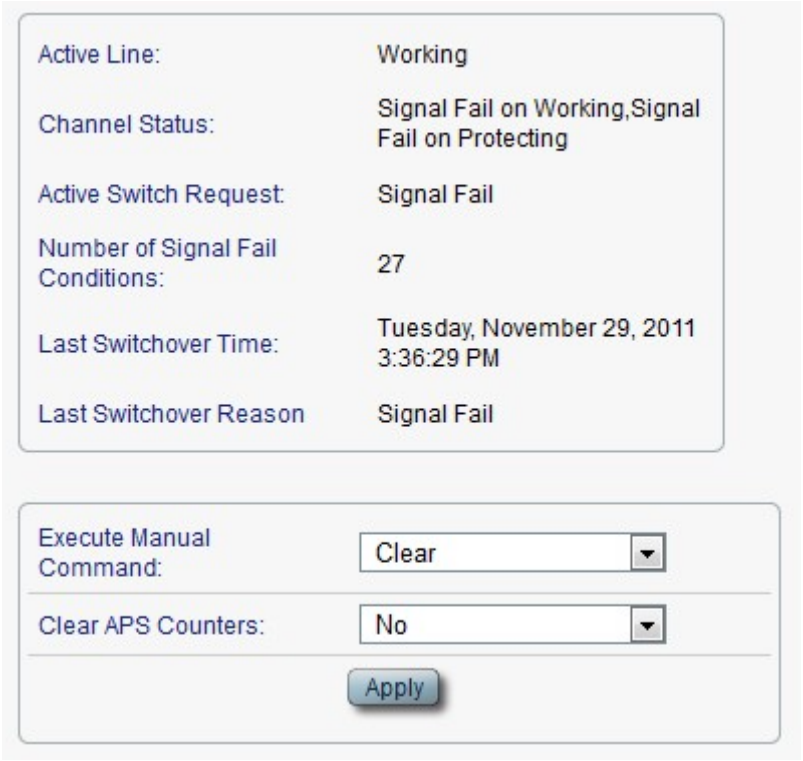


Figure 81: APS Tab

Use the APS tab to view and configure the APS parameters for a COM port.

To configure APS parameters:

1. Click the **APS** tab.

   The APS tab opens.

2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 44: APS Tab Parameters

Parameter	Description	Format / Values
Active Line	The current active uplink.	Working, Protecting
Channel Status	The current APS channel status.	Any combination of the following values: • Signal Fail on Working • Signal Fail on Protecting • Switched (to Protecting)
Active Switch Request	The switch request currently in effect.	• Manual Command • Signal Fail • Force Switch • Other
Number of Signal Fail Conditions	The number of times the **Signal Fail** condition occurred.	Integer

Parameter	Description	Format / Values
Last Switchover Time	The time of the last switchover event.	Date and time
Last Switchover Reason	The reason for the last switchover.	• Manual Command • Signal Fail • Force Switch • Other
Execute Manual Command	The manual APS commands.	• **Clear**: Clears the last APS switch command. • **Force Switch to Protecting**: Forces switch to Protecting in any condition. • **Force Switch to Working**: Forces switch to Working in any condition. • **Manual Switch to Protecting**: Switches to Protecting only if the protecting uplink is functioning properly. • **Manual Switch to Working**: Switches to Working only if the working uplink is functioning properly. Default: Clear
Clear APS Counters	Whether or not to clear the APS counters.	• **No**: Does not clear the APS counters. • **Yes**: Clears the APS counters. Default: No

6.7 EDFA Configuration

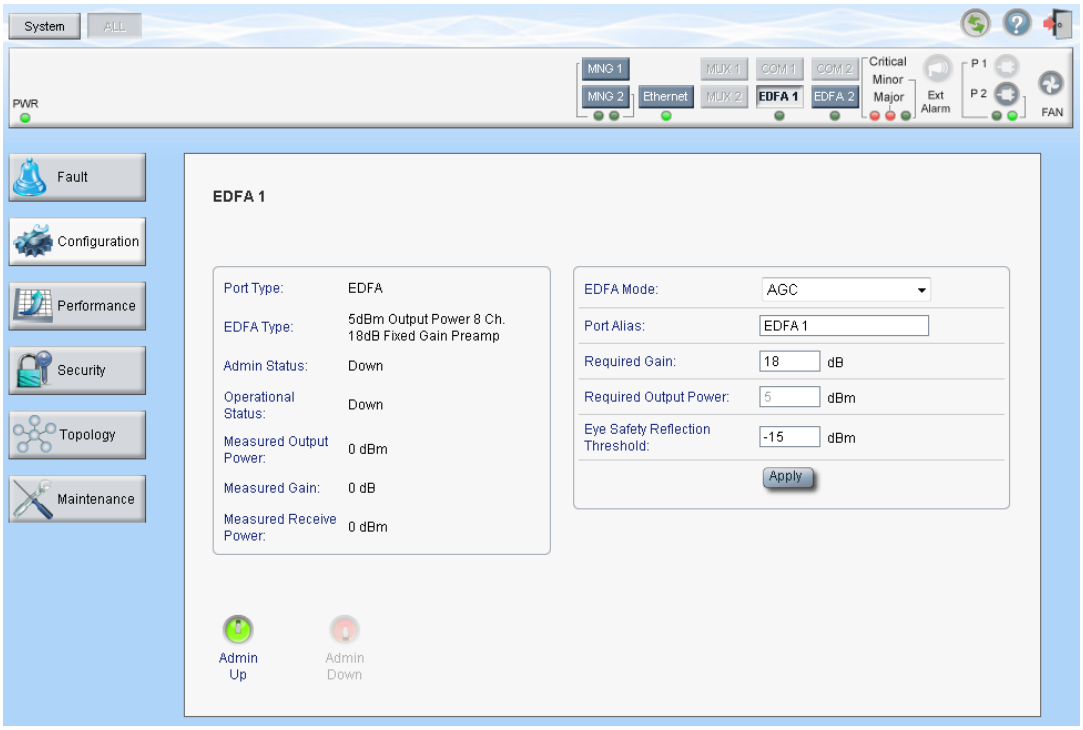


Figure 82: EDFA Configuration Window

NOTE: The **EDFA** button is enabled only if an EDFA module is installed.

Use the EDFA Configuration window to configure the EDFA module and enable/disable the module.

To open the EDFA Configuration window:

1. Click **Configuration**.
2. Click an **EDFA** button to select the EDFA module.

   The appropriate EDFA Configuration window opens.

6.7.1 EDFA Tab

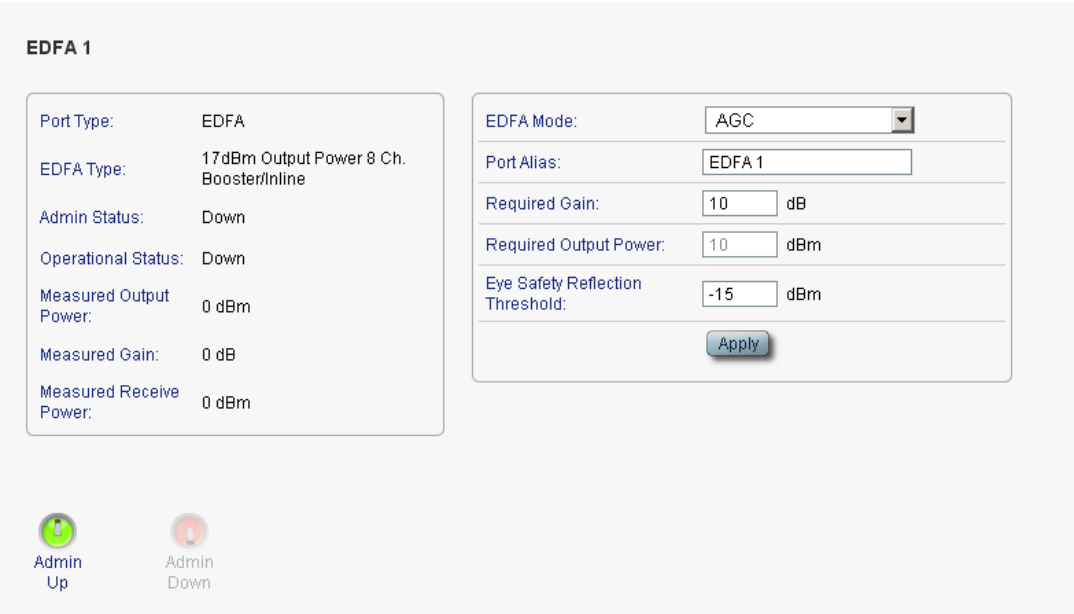


Figure 83: EDFA Tab

Use the EDFA tab to configure the EDFA module and enable/disable the module.

To configure the EDFA module:

1. Click **EDFA** to select the EDFA module.

   The EDFA tab opens displaying the EDFA module configuration.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.
4. To enable the module:

   1. Click **Admin Up**  .

      The following confirmation message appears.

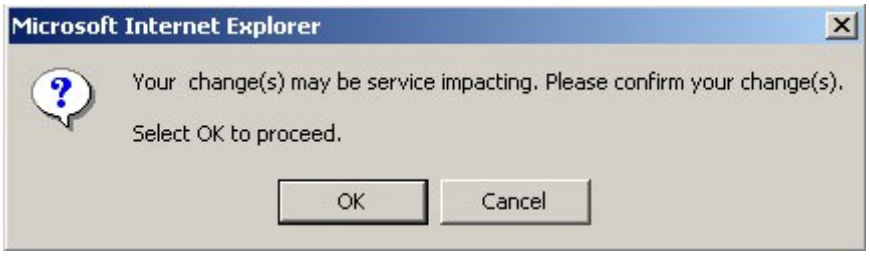
      

      Figure 84: Confirm Changes

   2. Click **OK**.

      The selected module is enabled, the **Admin Up** button is disabled, and the **Admin Down** button is enabled.
5. To disable the module:

   1. Click **Admin Down**  .

The following confirmation message appears.

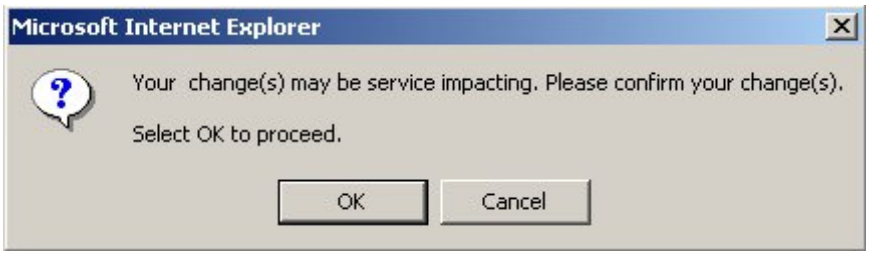


Figure 85: Confirm Changes

2. Click **OK**.

   The selected module is disabled, the **Admin Up** button is enabled, and the **Admin Down** button is disabled.

Table 45: EDFA Tab Parameters

Parameter	Description	Format/Values
Port Type	The type of port.	EDFA
EDFA Type	The type of installed EDFA module as determined by maximum output power, maximum number of optical channels, and Booster/Inline or Pre-Amp.	EDFA types and input power ranges: • **14 dBm**: -24 dBm to +10 dBm • **17 dBm**: -24 dBm to +10 dBm • **20 dBm**: -24 dBm to +10 dBm • **23 dBm**: -5 dBm to +16 dBm
Admin Status	The administrative status of the EDFA module.	Up, Down To change the value, click **Admin Up** or **Admin Down**.
Operational Status	The operational status of the EDFA module. This indicates if there is a failure in the EDFA module.	• **Up**: Normal operation • **Down**: Alarm is detected or **Admin Down**
Measured Output Power	The current measured optical power of the EDFA.	dBm
Measured Gain	The current measured gain of the EDFA.	dB
Measured Receive Power	The current measured receive power of the EDFA.	dBm
EDFA Mode	Selected amplification mode.	• **AGC**: Gain remains constant. • **APC**: Output power remains constant. **NOTE:** ▪ AGC is recommended. ▪ The other available fields vary depending on which EDFA mode is selected.
Port Alias	The logical name given to the module for identification purposes.	Free text

Parameter	Description	Format / Values
Required Gain	Specifies the required constant gain.	• **Booster**: +10 to +22 dB • **Pre-Amp**: +18 dB **NOTE:** Available only if **EDFA mode** is **AGC**.
Required Output Power	Specifies the required constant power.	• **Booster**: 14 dBm, 17 dBm, 20 dBm, 23 dBm • **Pre-Amp**: +5 dBm **NOTE:** Available only if **EDFA mode** is **APC**.
Eye Safety Reflection Threshold	The reflection threshold for eye safety.	dBm

6.8 PSU Configuration

Use the PSU Configuration Window to view information about the power supply units currently installed in the system.

To open the PSU Configuration window:

1. Click **Configuration**.
2. Click a **PSU** button to select the power supply unit.

   The appropriate PSU Configuration window opens.

6.8.1 PSU Tab

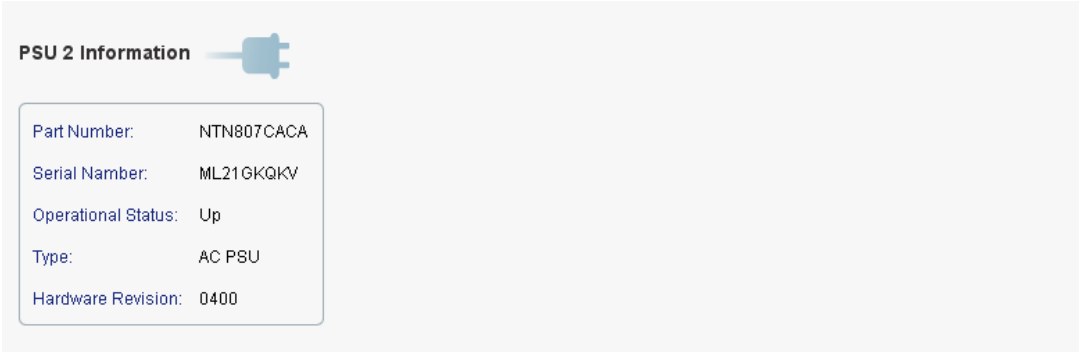


Figure 86: PSU Tab

Use the PSU tab to view information about the power supply units currently installed in the system.

To view PSU information:

- Click a **PSU** button to select the power supply unit.

  The PSU tab opens displaying the PSU information. The fields are read only and explained in the following table.

Table 46: PSU Tab Parameters

Parameter	Description	Format / Values
Part Number	The part number of the power supply unit.	Part number
Serial Number	The serial number of the power supply unit.	Serial number
Operational Status	The operational status of the power supply unit. This indicates if there is a failure in the power supply unit.	• **Up**: Normal operation • **Down**: Alarm is detected
Type	The type of power supply unit.	AC PSU, DC PSU
Hardware Revision	The hardware version of the power supply unit.	dddd

6.9 FAN Unit Configuration

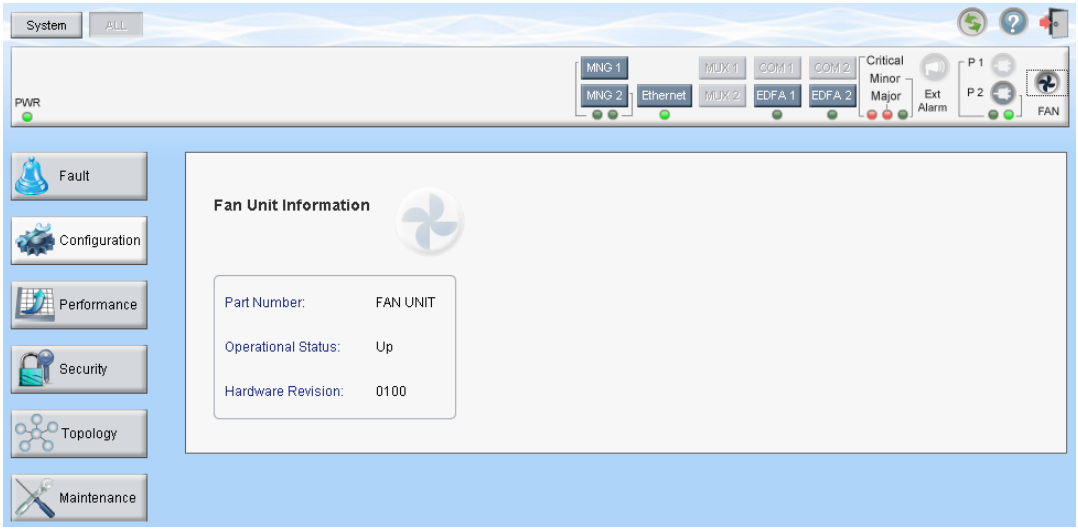


Figure 87: FAN Unit Configuration Window

Use the FAN Unit Configuration window to view information about the FAN unit currently installed in the system.

To open the FAN Unit Configuration window:

1. Click **Configuration**.
2. Click **FAN** button to select the FAN unit.

   The FAN Unit Configuration window opens.

6.9.1 FAN Unit Tab

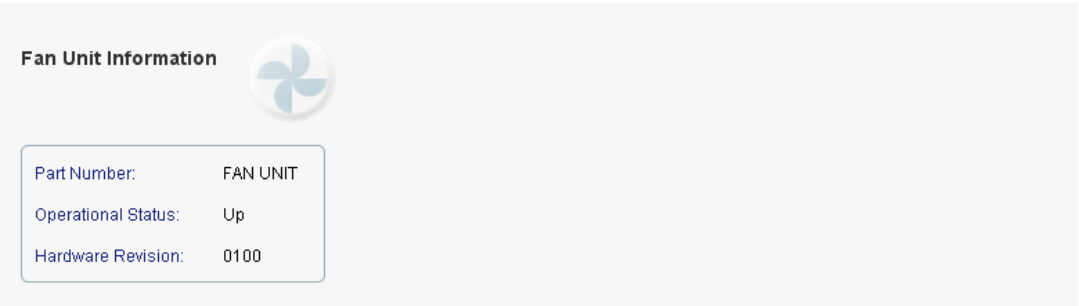


Figure 88: FAN Unit Tab

Use the FAN Unit tab to display information about the FAN unit currently installed in the system.

To view the FAN unit information:

- Click **FAN** to select the FAN unit.

  The FAN tab opens displaying the FAN unit information. The fields are read only and explained in the following table.

Table 47: FAN Unit Tab Parameters

Parameters	Description	Format / Values
Part Number	The part number of the FAN unit	FAN UNIT
Operational Status	The operational status of the FAN unit. This indicates if there is a failure in the FAN unit.	• **Up**: Normal operation • **Down**: Alarm is detected
Hardware Revision	The hardware version of the FAN unit.	dddd

7 Performance Monitoring

This chapter describes the PL-1000IL system optical information and port performance monitoring.

In this Chapter

7.1 Optical Information

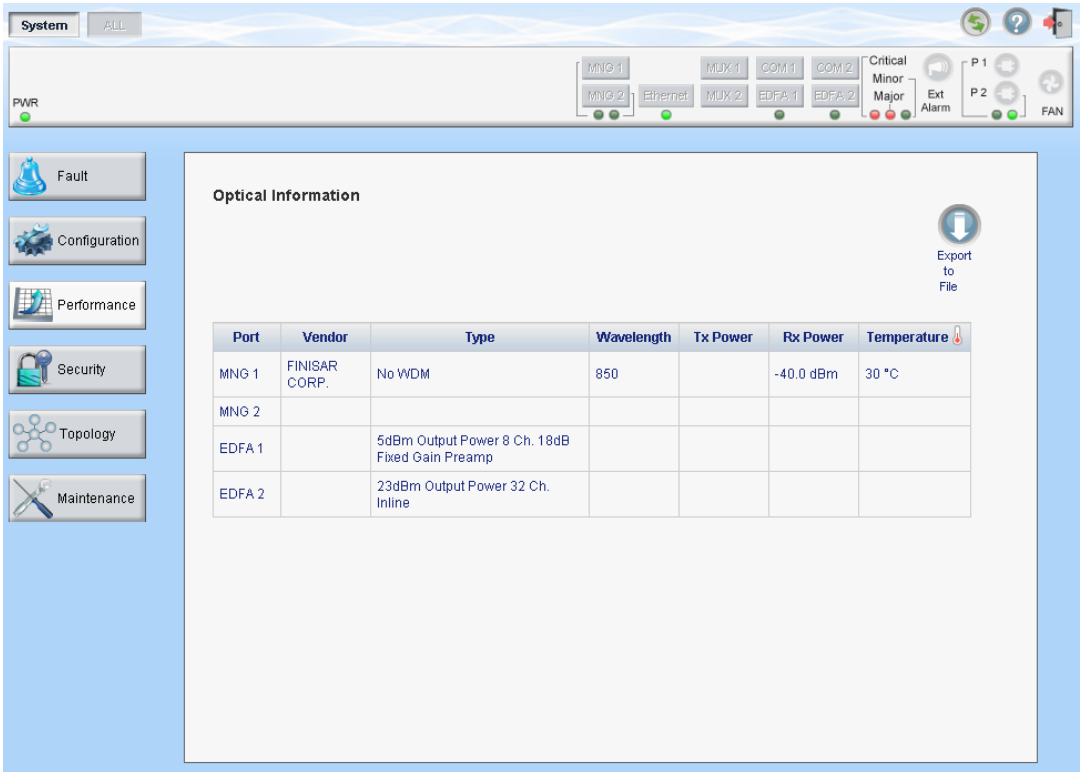


Figure 89: Optical Information Window

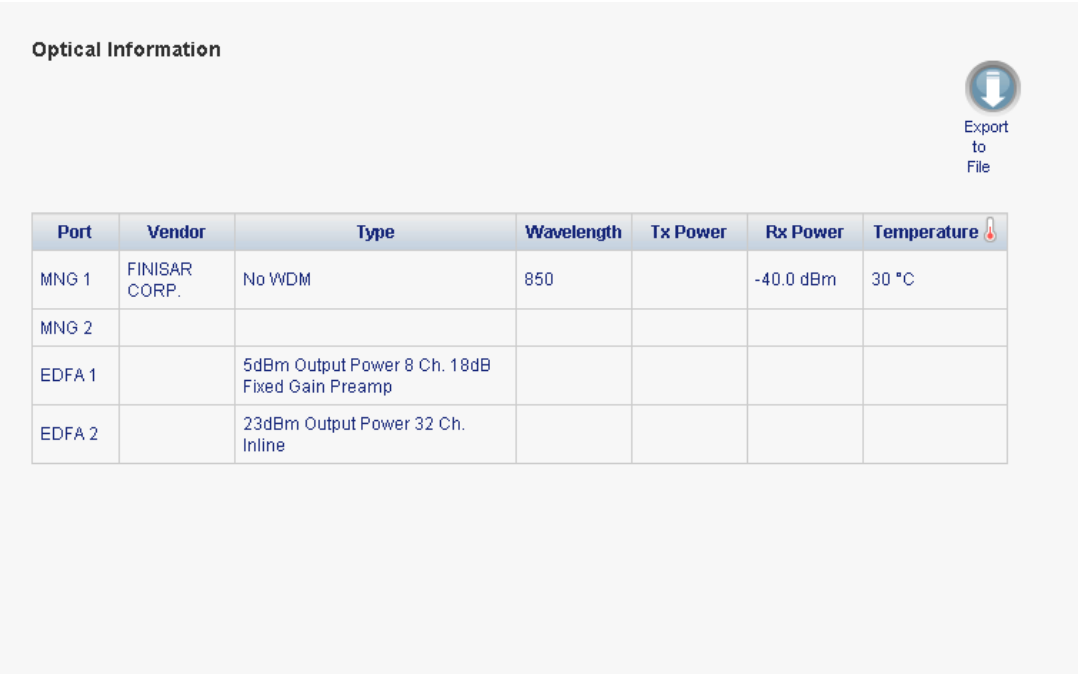
Use the Optical Information window to view optical performance of all optical modules installed in the system.

To open the Optical Information window:

1. Click **Performance**.
2. Click **System**.

   The Optical Information window opens.

7.1.1 Optical Information Tab



Port	Vendor	Type	Wavelength	Tx Power	Rx Power	Temperature
MNG 1	FINISAR CORP.	No WDM	850		-40.0 dBm	30 °C
MNG 2						
EDFA 1		5dBm Output Power 8 Ch. 18dB Fixed Gain Preamp				
EDFA 2		23dBm Output Power 32 Ch. Inline				

Figure 90: Optical Information Tab

Use the Optical Information tab to view optical information.

To view optical information:

1. Click **System**.

   The Optical Information tab opens displaying the optical information. The fields are read only and explained in the following table.

2. To export the optical information to a file:

   1. Click **Export to File** .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.

   3. Click **OK**.

3. To refresh the optical information, click **Refresh** .

   The information is updated immediately.

Table 48: Optical Information Tab Parameters

Parameter	Description
Port	The name of the port or module in which the optical module is installed. **NOTE:** This parameter may or may not be marked: ▪ **Red**: This indicates that there is a standing alarm against this optical module. ▪ **Green**: This indicates that the **Admin Status** and **Operational Status** of the port are **Up**. ▪ **Not marked**: This indicates that the optical module does not exist.
Vendor	The manufacturer of the optical module.
Type	The type of optical module.
Wavelength	The Tx wavelength (nm).
Tx Power	The current measured Tx power.
Rx Power	The current measured Rx power.
Temperature	The current measured temperature of the optical module.

7.2 Management Port Performance Monitoring

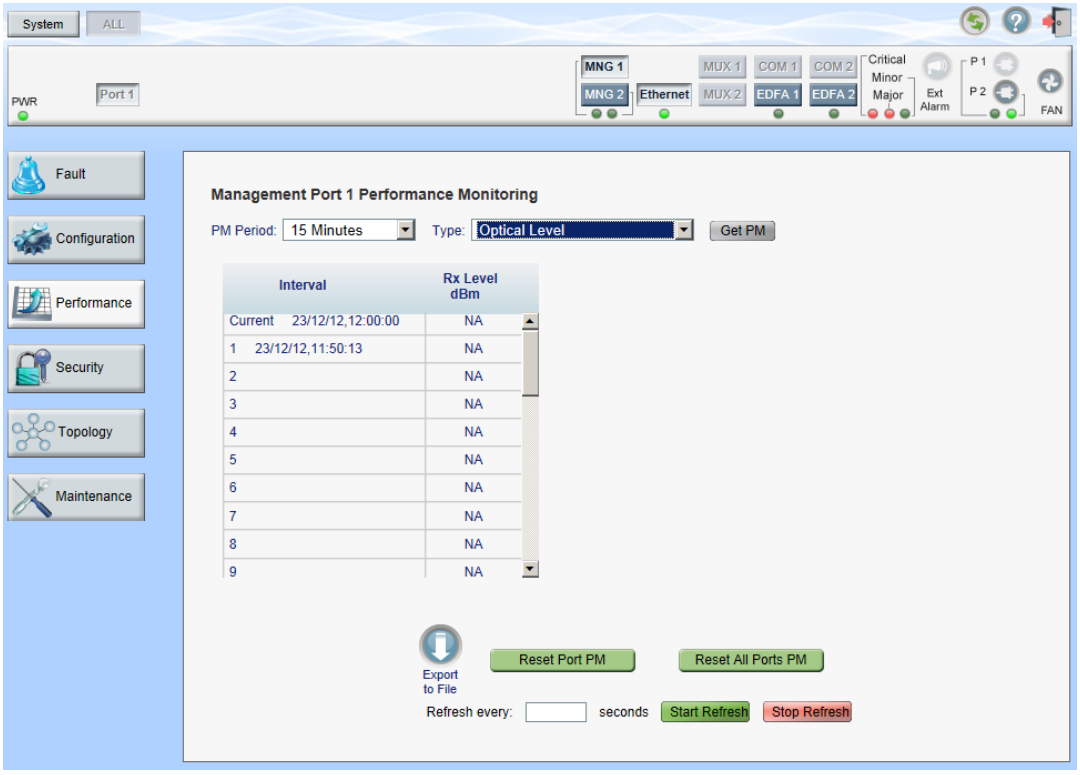


Figure 91: Management Port Performance Monitoring Window

Use the Management Port Performance Monitoring window to view management port optical performance monitoring.

To open the Management Port Performance Monitoring window:

1. Click **Performance**.

2. Click an **MNG** button to select the management port.

   The appropriate Management Port Performance Monitoring window opens.

7.2.1 Viewing Optical Performance Monitoring

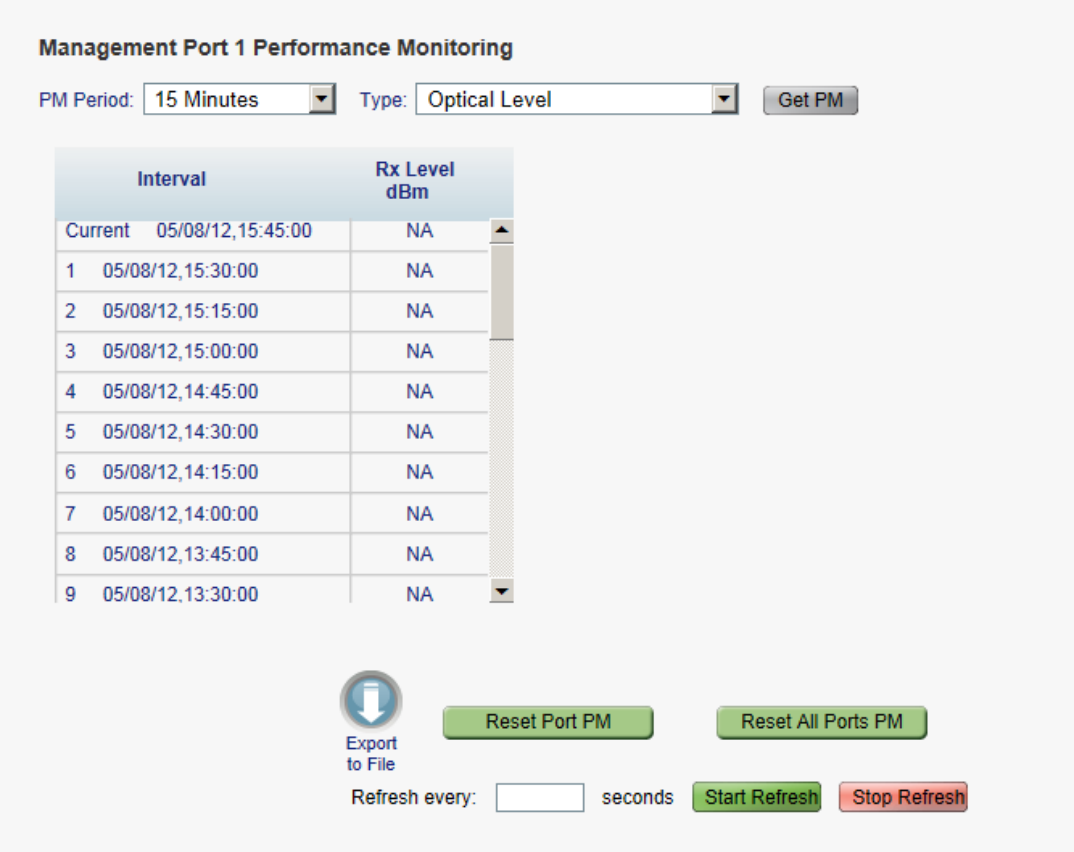


Figure 92: Optical Level Performance Monitoring

Use the Management Port Performance Monitoring tab to view management port optical level performance monitoring.

To view optical level performance monitoring:

1. Click an **MNG** button to select the management port.

   The appropriate Management Port Performance Monitoring tab opens displaying the displaying the management port performance monitoring. The fields are explained in the following table. The counters are read only.

2. From the **PM Period** drop-down list, select the interval.
3. From the **Type** drop-down list, select **Optical Level**.
4. Click **Get PM**.

   The optical level counters are updated.

5. To export the optical level information to a file:

   1. Click **Export to File**  .

The Opening table.csv dialog box appears.

2. Click **Save File**.
3. Click **OK**.

6. To set the refresh rate of the PM display:
   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.

   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.
7. To refresh the PM display manually, click **Refresh**  .

   The information is updated immediately.
8. To stop the automatic refresh of the PM display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.
9. To clear the optical level counters for a specific port, click **Reset Port PM**.
10. To clear the optical level counters for all ports, click **Reset All Ports PM**.

Table 49: Management Port Optical Level PM Parameters

Parameter	Description	Format / Values
PM Period	The interval for averaging the measured Rx power.	15 Minutes, Days
Type	The type of performance monitoring.	Optical Level
Interval	The date and time of the interval.	**PM Period** is set to **15 Minutes**: • **Current**: The date and time of the current interval of 15 minutes is displayed in the first row. • **1 to 32**: The date and time of the last 32 intervals of 15 minutes is displayed in the second row to the last row of the table. **PM Period** is set to **Days**: • **Untimed**: The date and time of the last reset of the system or last reset of the optical level counters is displayed in the first row of the table. • **Current Day**: The date and 00:00 AM of the current day is displayed in the second row of the table. • **Previous Day**: The date and 00:00 AM of the previous day is displayed in the last row of the table.

Parameter	Description	Format / Values
Rx Level dBm	The measured Rx power level during the interval (in dBm).	**PM Period** is set to **15 Minutes**: • **Current**: The measured Rx power for the current interval of 15 minutes is displayed in the first row. • **1 to 32**: The measured Rx power for the last 32 intervals of 15 minutes is displayed in the second row to the last row of the table. **PM Period** is set to **Days**: • **Untimed**: The average of the measured Rx power since last reset of the system or since the last reset of the optical level counters is displayed in the first row of the table. • **Current Day**: The average of the measured Rx power since 00:00 AM of the current day is displayed in the second row of the table. • **Previous Day**: The average of the measured Rx power during the 24 hours since 00:00 AM of the previous day is displayed in the last row of the table.

7.3 EDFA Performance Monitoring

NOTE: The **EDFA** button is enabled only if an EDFA module is installed.

Use the EDFA Performance Monitoring window to view EDFA module optical performance monitoring.

To open the EDFA Performance Monitoring window:

1. Click **Performance**.
2. Click an **EDFA** button to select the EDFA module.

   The appropriate EDFA Performance Monitoring window opens.

7.3.1 Viewing Optical Performance Monitoring

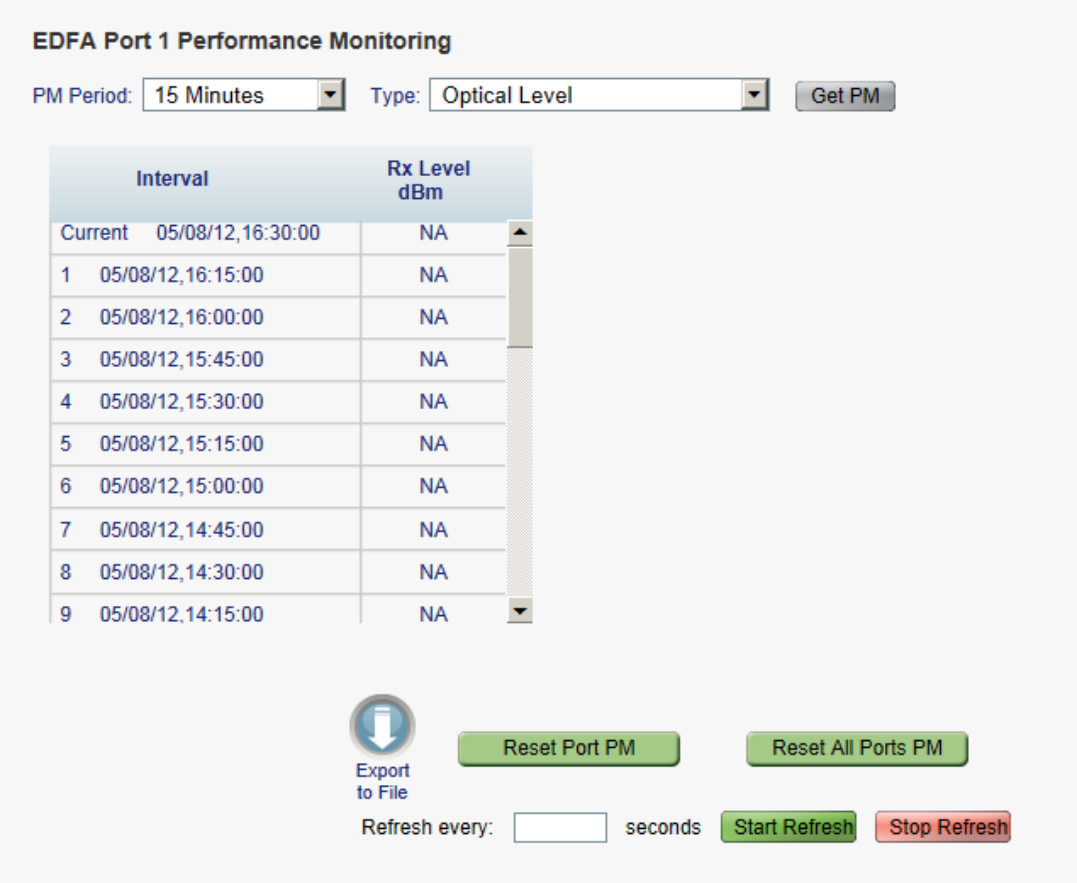


Figure 93: Optical Level Performance Monitoring

Use the EDFA Performance Monitoring tab to view EDFA optical level performance monitoring.

To view optical level performance monitoring:

1. Click an **EDFA** button to select the EDFA module.

   The appropriate EDFA Performance Monitoring tab opens displaying the displaying the EDFA performance monitoring. The fields are explained in the following table. The counters are read only.

2. From the **PM Period** drop-down list, select the interval.
3. From the **Type** drop-down list, select **Optical Level**.
4. Click **Get PM**.

   The optical level counters are updated.

5. To export the optical level information to a file:

   1. Click **Export to File**  .

      The Opening table.csv dialog box appears.

   2. Click **Save File**.
   3. Click **OK**.

6. To set the refresh rate of the PM display:
   1. In the **Refresh every** field, type the number of seconds that the window should refresh.

      The minimum refresh rate is 2 seconds.
   2. Click **Start Refresh**.

      The information is automatically updated after the specified number of seconds.
7. To refresh the PM display manually, click **Refresh**  .

   The information is updated immediately.
8. To stop the automatic refresh of the PM display, click **Stop Refresh**.

   The automatic refresh is stopped and the **Refresh every** field is cleared.
9. To clear the optical level counters for a specific port, click **Reset Port PM**.
10. To clear the optical level counters for all ports, click **Reset All Ports PM**.

Table 50: EDFA Optical Level PM Parameters

Parameter	Description	Format/Values
PM Period	The interval for averaging the measured Rx power.	15 Minutes, Days
Type	The type of performance monitoring.	Optical Level
Interval	The date and time of the interval.	**PM Period** is set to **15 Minutes**: • **Current**: The date and time of the current interval of 15 minutes is displayed in the first row. • **1 to 32**: The date and time of the last 32 intervals of 15 minutes is displayed in the second row to the last row of the table. **PM Period** is set to **Days**: • **Untimed**: The date and time of the last reset of the system or last reset of the optical level counters is displayed in the first row of the table. • **Current Day**: The date and 00:00 AM of the current day is displayed in the second row of the table. • **Previous Day**: The date and 00:00 AM of the previous day is displayed in the last row of the table.

Parameter	Description	Format / Values
Rx Level dBm	The measured Rx power level during the interval (in dBm).	**PM Period** is set to **15 Minutes**: • **Current**: The measured Rx power for the current interval of 15 minutes is displayed in the first row. • **1 to 32**: The measured Rx power for the last 32 intervals of 15 minutes is displayed in the second row to the last row of the table. **PM Period** is set to **Days**: • **Untimed**: The average of the measured Rx power since last reset of the system or since the last reset of the optical level counters is displayed in the first row of the table. • **Current Day**: The average of the measured Rx power since 00:00 AM of the current day is displayed in the second row of the table. • **Previous Day**: The average of the measured Rx power during the 24 hours since 00:00 AM of the previous day is displayed in the last row of the table.

8 Maintenance

This chapter describes how to perform maintenance tasks for the PL-1000IL.

In this Chapter

8.1 System Maintenance

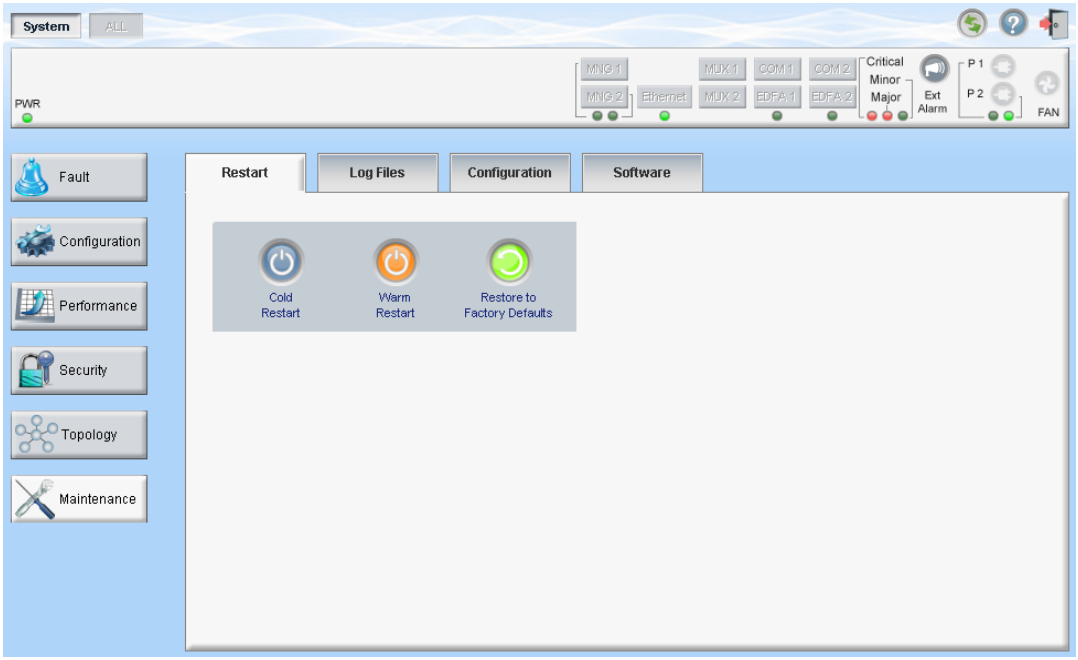


Figure 94: System Maintenance Window

Use the System Maintenance window to do the following:

- **Restart tab**: Restart the PL-1000IL unit
- **Log Files tab**: View and save the System Log files
- **Configuration tab**:
  - **Download Configuration File**: Update system configuration, by downloading to the node a previously saved system configuration file
  - **Upload Configuration File**: Upload system configuration and save it to the local file system
- **Software tab**: Download and activate a new software version

To open the System Maintenance window:

1. Click **Maintenance**.
2. Click **System**.

   The System Maintenance window opens.

8.1.1 Restart Tab

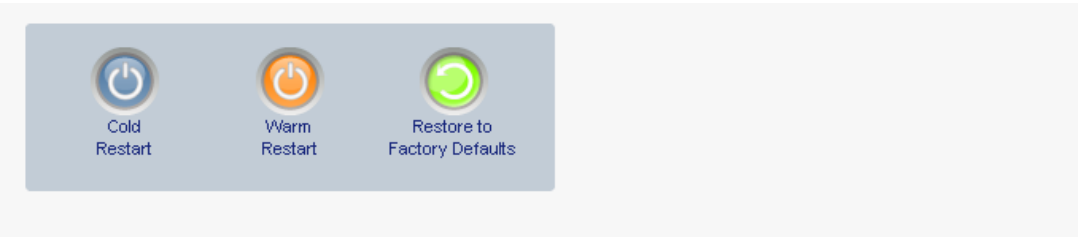


Figure 95: Restart Tab

Use the Restart tab to do the following:

- **Cold Restart**: Service-affecting operation that is required for major upgrade to the device software
- **Warm Restart**: Non-service-affecting operation that is required for minor upgrade of the device software
- **Restore to Factory Defaults**: Service-affecting operation that restores the device to factory defaults

NOTE: If you restore to the factory default configuration:

- All licensing information is removed from the node. Therefore, to continue using a licensed feature after a **Restore to Factory Default**s is performed, you must reinstall the license.
- All previous configurations applied to the node will be lost, except for the IP information. Therefore, you should reapply the desired configuration.

To restart the PL-1000IL unit:

1. Click the **Restart** tab.

   The Restart tab opens.

2. To perform a cold restart:

   1. Click **Cold Restart**  .

      The following confirmation message appears.

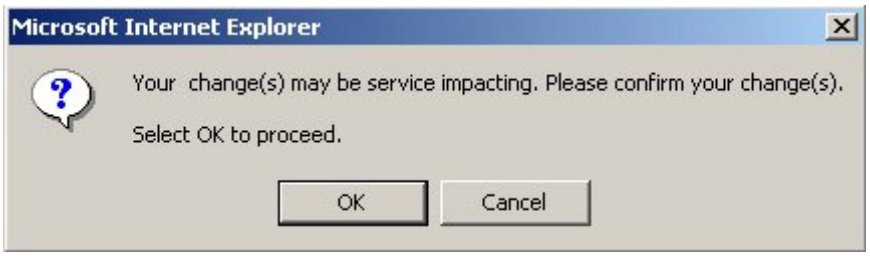


Figure 96: Confirm Changes

   2. Click **OK**.

      The software and hardware are reloaded and the system restarts.

Traffic goes down for a short period of time.

3. To perform a warm restart:

   1. Click **Warm Restart**  .

      The following confirmation message appears.

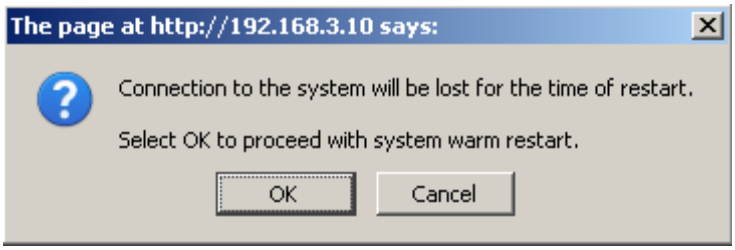


Figure 97: Confirm Changes

   2. Click **OK**.

      The software is reloaded and the system restarts.

      Traffic is not affected.

4. To restore to the factory default configuration:

   1. Click **Restore to Factory Defaults**  .

      The following confirmation message appears.

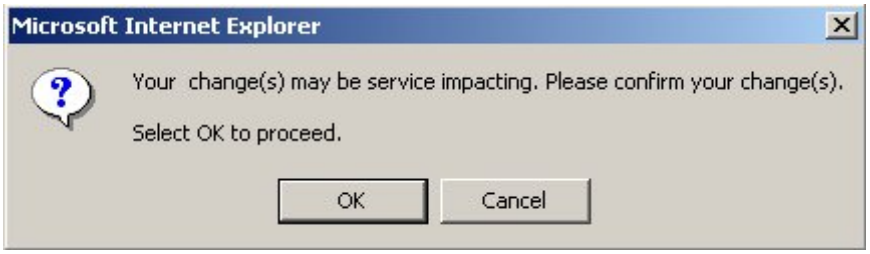


Figure 98: Confirm Changes

   2. Click **OK**.

      All system default configuration parameter values, except for IP information, are restored and the system restarts.

      Traffic is affected.

8.1.2 Log Files Tab

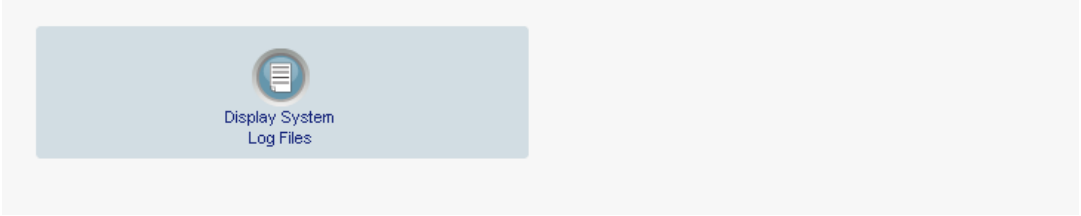


Figure 99: Log Files Tab

Use the Log Files tab to view and save System Log files.

To view and save System Log files:

1. Click **Log Files**.

   The Log Files tab opens.

2. Click **Display System Log Files**  .

   The System Log files are displayed.

3. To save the log data, copy the displayed text from the browser window, paste it into a file, and then save the file.

Prev Log:
0x16bb210 (PB_INIT): <3163> THU DEC 27 00:00:31 1990 EVENT System is starting up, Please wait...
0x16bb210 (PB_INIT): <3489> THU DEC 27 00:00:34 1990 EVENT Signature = HOT START
0x16bb210 (PB_INIT): <3489> THU DEC 27 00:00:34 1990 DEBUG Hotstart data pointer = 0x3f00014
0x16bb210 (PB_INIT): <3489> THU DEC 27 00:00:34 1990 DEBUG Software Ver:1.1.5 (Created on Sep 21 2011, 13:00:13)
0x16bb210 (PB_INIT): <3489> THU DEC 27 00:00:34 1990 DEBUG ------ Start Hardware Initialization and Testing : ------
0x16bb210 (PB_INIT): <3494> THU DEC 27 00:00:34 1990 EVENT FPGA not loaded: switch to normal start mode
0x16bb210 (PB_INIT): <3512> THU DEC 27 00:00:34 1990 EVENT Loading FPGA 0 created on: Tue Sep 06 10:57:34 2011...
0x16bb210 (PB_INIT): <3563> THU DEC 27 00:00:35 1990 EVENT OPTO FPGA Version is a01b
0x16bb210 (PB_INIT): <3598> THU DEC 27 00:00:35 1990 DEBUG L2 Switch QuarterDeck has been started.
0x16bb210 (PB_INIT): <3796> THU DEC 27 00:00:37 1990 DEBUG HW VER IS 300
0x16bb210 (PB_INIT): <3796> THU DEC 27 00:00:37 1990 EVENT Adding LAN_IF address 192.168.3.33, subnet ff000000
0x16bb210 (PB_INIT): <3798> THU DEC 27 00:00:37 1990 EVENT Adding MNG_IF address 10.0.26.18, subnet ff000000
0x16bb210 (PB_INIT): <3799> TUE FEB 08 23:16:21 2000 EVENT RTC Initialization: TUE FEB 08 23:16:21 2000

0x16bb210 (PB_INIT): <3809> TUE FEB 08 23:16:21 2000 DEBUG Driver Version 70503
0x16bb210 (PB_INIT): <3834> TUE FEB 08 23:16:21 2000 DEBUG Framer Part 5420 rev 2
0x16bb210 (PB_INIT): <4332> TUE FEB 08 23:16:26 2000 DEBUG Loaded Firmware 6020401 20110418
interrupt: OAPS[0]: Port invalid for OAPS failure event 256!
interrupt: OAPS[1]: Port invalid for OAPS failure event 256!
Current Log:
0x16bb210 (PB_INIT): <3166> THU DEC 27 00:00:31 1990 EVENT System is starting up, Please wait...
0x16bb210 (PB_INIT): <3528> THU DEC 27 00:00:34 1990 EVENT Signature = NORMAL START
0x16bb210 (PB_INIT): <3528> THU DEC 27 00:00:34 1990 DEBUG Software Ver:1.1.5 (Created on Sep 21 2011, 13:00:13)
0x16bb210 (PB_INIT): <3528> THU DEC 27 00:00:34 1990 DEBUG ------ Start Hardware Initialization and Testing : ------
0x16bb210 (PB_INIT): <3552> THU DEC 27 00:00:34 1990 EVENT Loading FPGA 0 created on: Tue Sep 06 10:57:34 2011...
0x16bb210 (PB_INIT): <3605> THU DEC 27 00:00:35 1990 EVENT OPTO FPGA Version is a01b
0x16bb210 (PB_INIT): <3640> THU DEC 27 00:00:35 1990 DEBUG L2 Switch QuarterDeck has been started.
0x16bb210 (PB_INIT): <3838> THU DEC 27 00:00:37 1990 DEBUG HW VER IS 300
0x16bb210 (PB_INIT): <3838> THU DEC 27 00:00:37 1990 EVENT Adding LAN_IF address 192.168.3.33, subnet ff000000
0x16bb210 (PB_INIT): <3840> THU DEC 27 00:00:37 1990 EVENT Adding MNG_IF address 10.0.26.18, subnet ff000000
0x16bb210 (PB_INIT): <3841> MON OCT 10 17:59:49 2011 EVENT RTC Initialization: MON OCT 10 17:59:49 2011

Figure 100: System Log Files (Example)

8.1.3 Configuration Tab

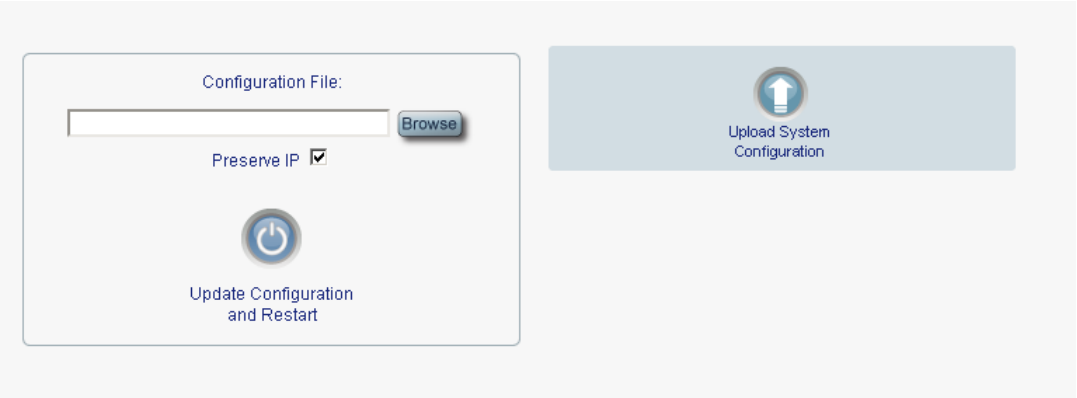


Figure 101: Configuration Tab

Use the Configuration tab to do the following:

- Update the system configuration with a previously saved file of system configuration, while preserving or replacing the IP addresses, and cold restart the PL-1000IL unit
- Upload the current system configuration of the PL-1000IL unit and save it to the local file system

8.1.3.1 Updating System Configuration and Restarting the PL-1000IL Unit

Use the Configuration tab to update the system configuration, while preserving or replacing the IP addresses, and restart the PL-1000IL unit.

WARNING: When uploading a system configuration file which was retrieved from another node, make sure to select the **Preserve IP** check box; otherwise, the new node will receive the same IP as the old node, and both nodes will have the same IP address.

To update system configuration and restart the PL-1000IL unit:

1. Click the **Configuration** tab.

   The Configuration tab opens

2. In the **Configuration File** field, type the full path of the file or click **Browse** and browse to the file location.

For example: **C:\fakepath\10.0.0.3.cfg**.

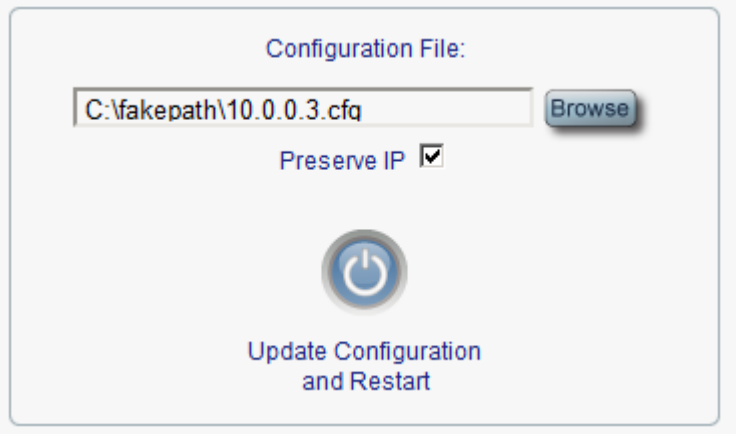


Figure 102: Update System Configuration: Configuration File

3. To preserve the IP addresses, select the Preserve IP check box.

4. Click **Update Configuration and Restart**  .

   The following confirmation message appears.

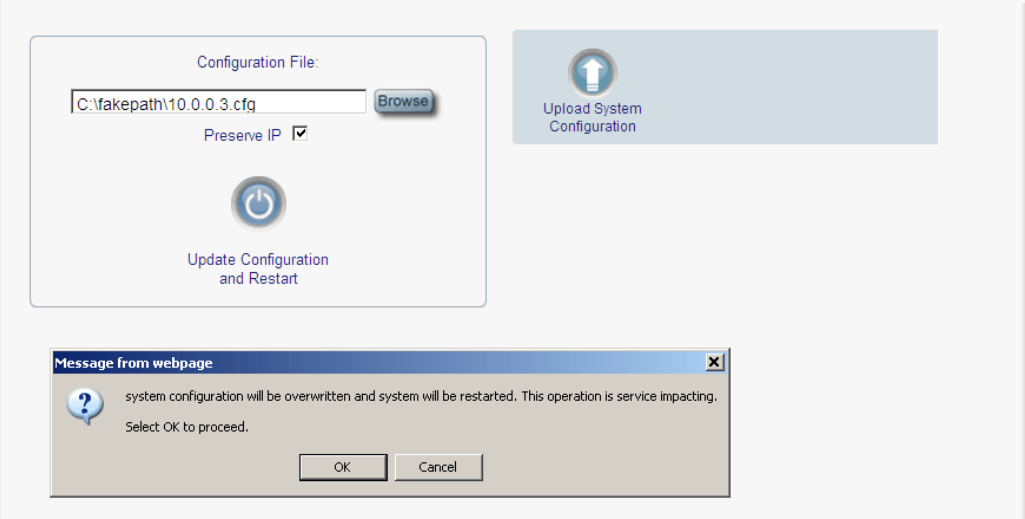


Figure 103: Confirm System Overwrite

5. Click **OK**.

   The following update message appears and the node is rebooted.

System is updating its configuration and restarting.
Please wait for the system to come up to resume operation.

Figure 104: System Updating and Restarting Message

8.1.3.2 Uploading System Configuration

NOTE:

- You can upload the node configuration to the local computer and save it to file. You can then use the saved file to reapply node configuration.
- You can replace a box with a new box by uploading and storing the configuration of the old box and then updating the new box with the stored configuration. In this case, you may want to clear the **Preserve IP** check box so that the new node will get the same IP address as the old node.
- The format of the saved configuration is a text file. However, changing the content of this file manually is not allowed.

To upload system configuration:

1. Click the **Configuration** tab.

   The Configuration tab opens.

2. Click **Upload System Configuration**  .

   The Opening .cfg dialog box appears.

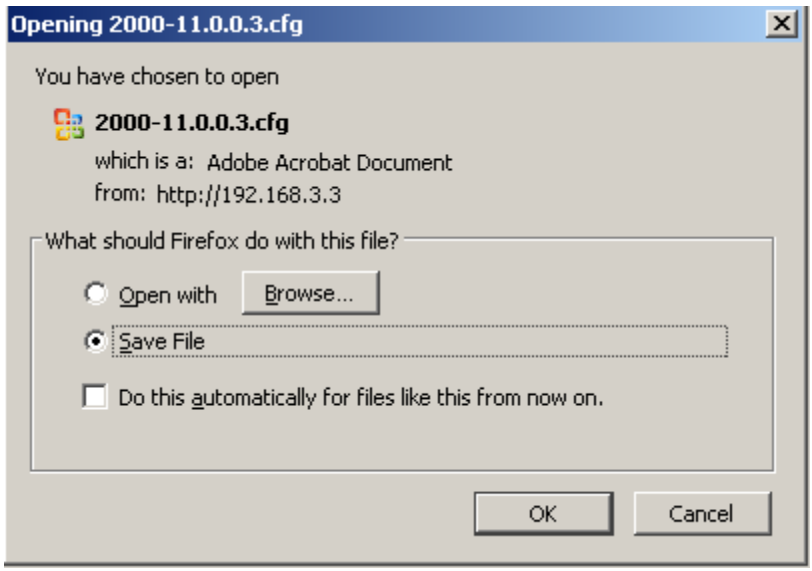


Figure 105: Opening .cfg Dialog Box

3. Click **Save File**.
4. Click **OK**.

8.1.4 Software Tab

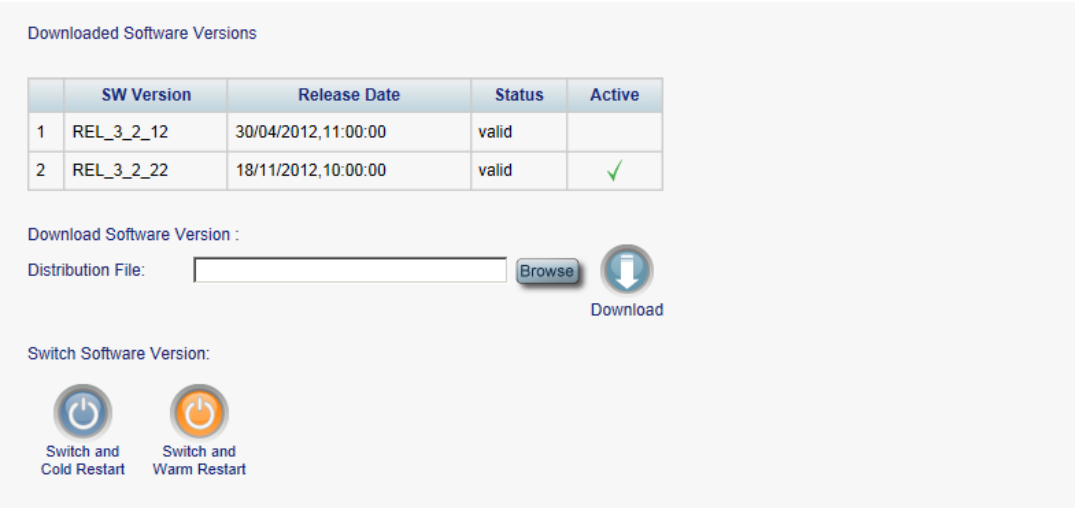


Figure 106: Software Tab

Use the Software tab to do the following:

- Download software
- Switch and activate a new software version

8.1.4.1 Downloading Software

WARNING: Do not perform operations from another open browser during download.

To download software:

1. Click the **Software** tab.

   The Software tab opens displaying the downloaded software versions. If a new version has been uploaded, two versions appear in the listing; the active version is indicated by a check mark ✓.

2. In the **Distribution Directory** field, type the full path of the file or click **Browse** and browse to the file location.

   For example: **`pl.vx`**

3. Click **Download** .

The following message appears.

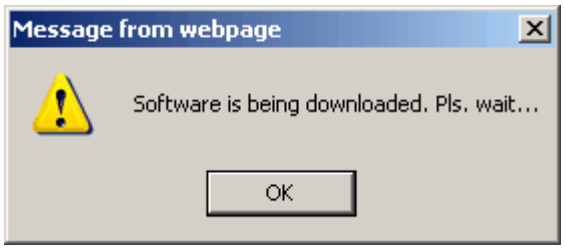


Figure 107: Software Download Message

4. Click **OK**.

   The Software Download Status window opens.

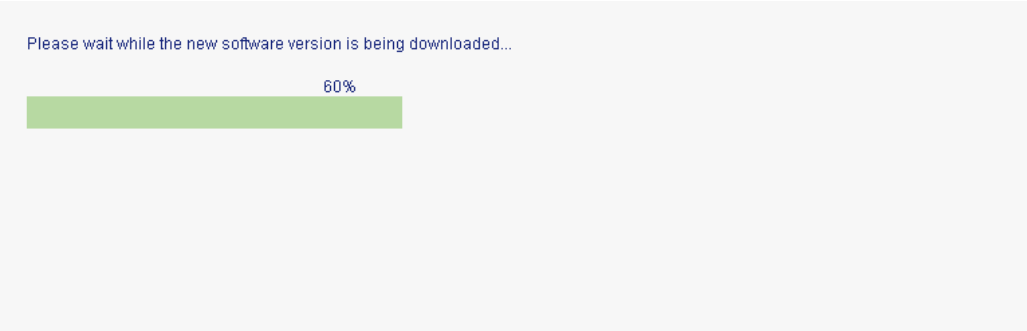


Figure 108: Software Download Status Window

The files are downloaded and the version displayed in the Downloaded Software Versions table. The new version is always idle (not active).

8.1.4.2 Switching Software Versions

After the new software version is downloaded, you can activate the new software version.

To switch software versions:

1. Click the **Software** tab.

   The Software tab opens displaying the downloaded software versions. If a new version has been uploaded, two versions appear in the listing; the active version is indicated by a check mark ✓.

2. To perform a switch and cold restart:

   1. Click **Switch & Cold Restart**  .

The following confirmation message appears.

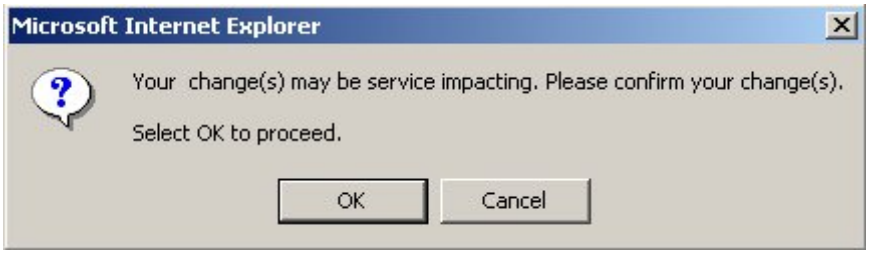


Figure 109: Confirm Changes

2. Click **OK**.

   The software version is switched, the software and firmware are reloaded, and the new version is activated.

   Traffic goes down for a short period of time.

3. To perform a warm restart:

   1. Click **Switch & Warm Restart**  .

      The following confirmation message appears.

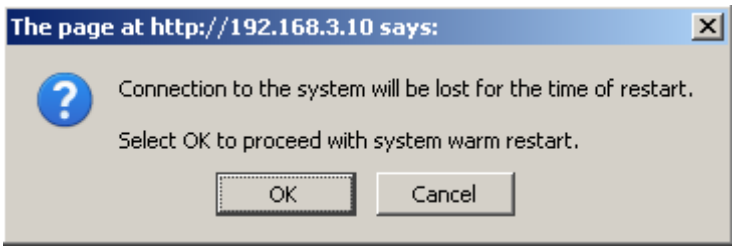


Figure 110: Confirm Changes

   2. Click **OK**.

      The software version is switched, the software is reloaded and restarted, and the new version is activated.

      Traffic is not affected.

8.2 External Alarm Maintenance

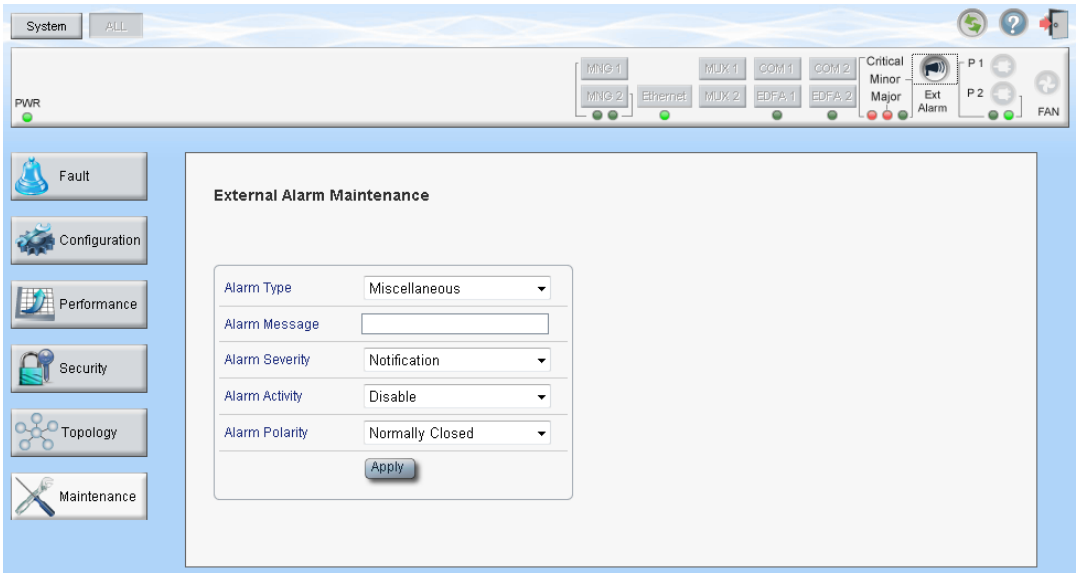


Figure 111: External Alarm Maintenance Window

Use the External Alarm Maintenance window to configure the external alarm.

To open the External Alarm Maintenance window:

1. Click **Maintenance**.
2. Click **Ext Alarm**  .

   The External Alarm Maintenance window opens.

8.2.1 External Alarm Maintenance Tab

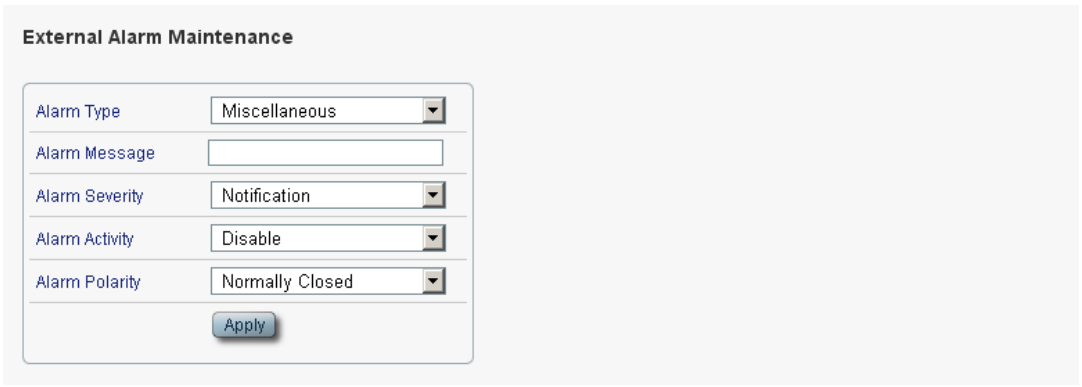


Figure 112: External Alarm Tab

Use the External Alarm tab to configure the external alarm.

To configure the external alarm:

1. Click **Ext Alarm**  .

   The External Alarm Maintenance tab opens.

2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 51: External Alarm Maintenance Tab Parameters

Parameter	Description	Format / Values
Alarm Type	A predefined list of standard external alarm types.	The type of configuration determines the values.
Alarm Message	The alarm text that is used when **Alarm Type** is set to **Miscellaneous**.	Free text
Alarm Severity	The severity of the External Input Alarm.	Critical, Major, Minor, Notification
Alarm Activity	Used to disable the Input External Alarm.	Disable, Enable
Alarm Polarity	Determines the polarity of the Input Dry Contact.	Normally Close, Normally Open

9 Topology Management

This chapter describes how manage the topology of PL-1000IL nodes.

In this Chapter

9.1 Network Topology

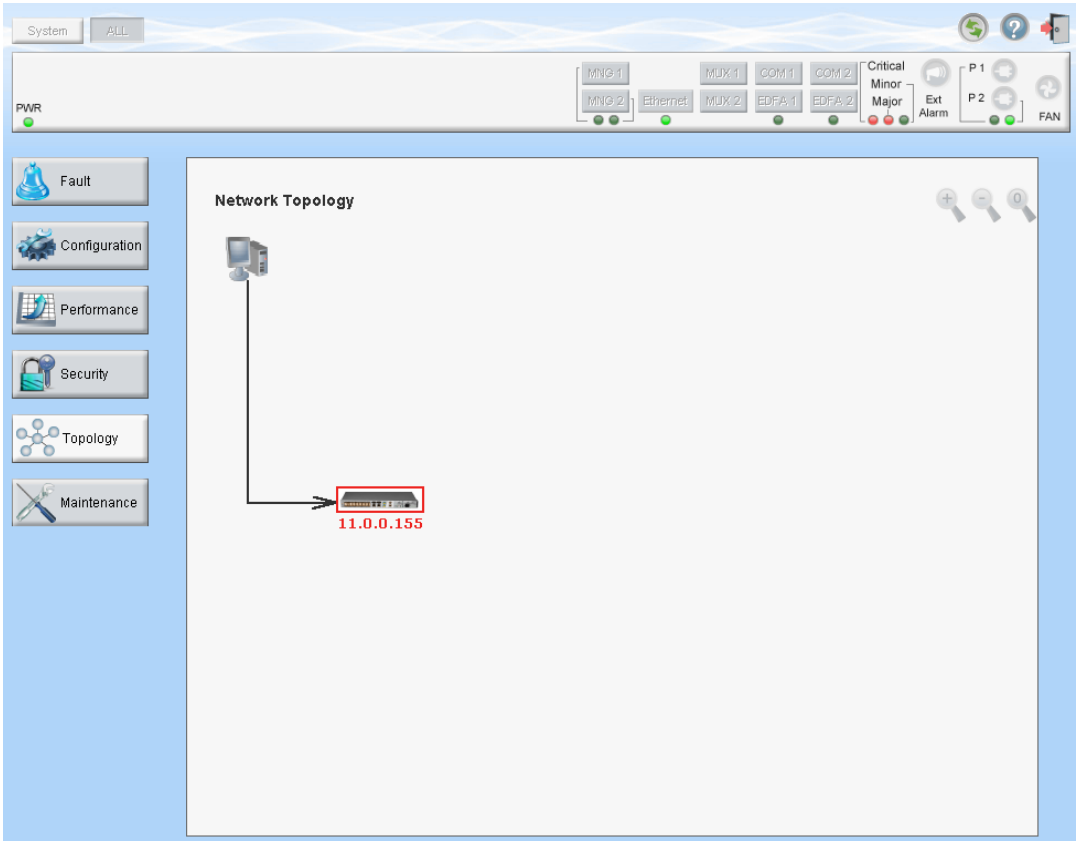


Figure 113: Network Topology Window

Use the Network Topology window to view the network topology and define multiple nodes as multi-chassis.

To open the Network Topology window:

- Click **Topology**.

  The Network Topology window opens.

9.1.1 Network Topology Tab

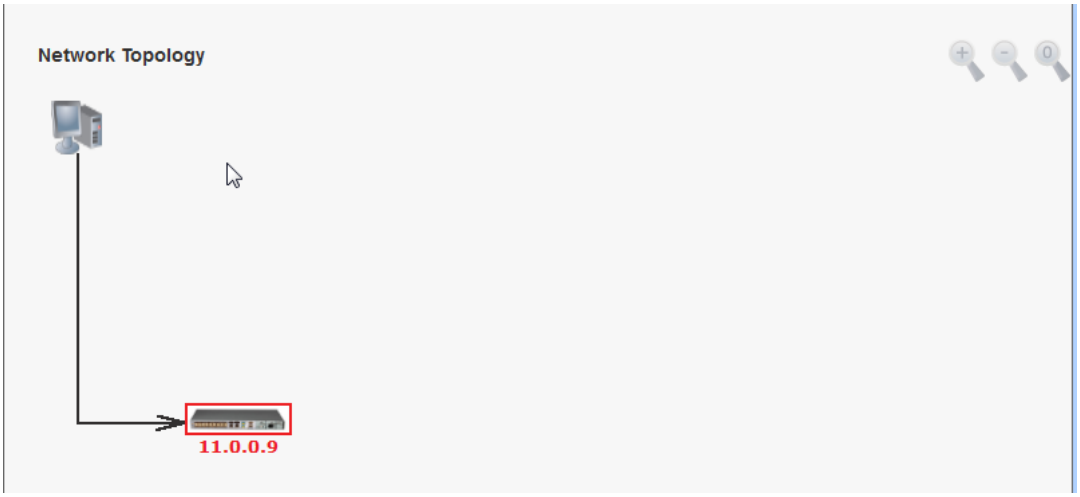


Figure 114: Network Topology Tab

Use the Network Topology tab to view the topology.

To view the network topology:

- Click the **Network Topology** tab.

  The Network Topology tab opens displaying the PL-1000IL nodes connected together with the OSC channel.

9.1.1.1 Network Linear Topology

The following figure is an example of a linear topology.

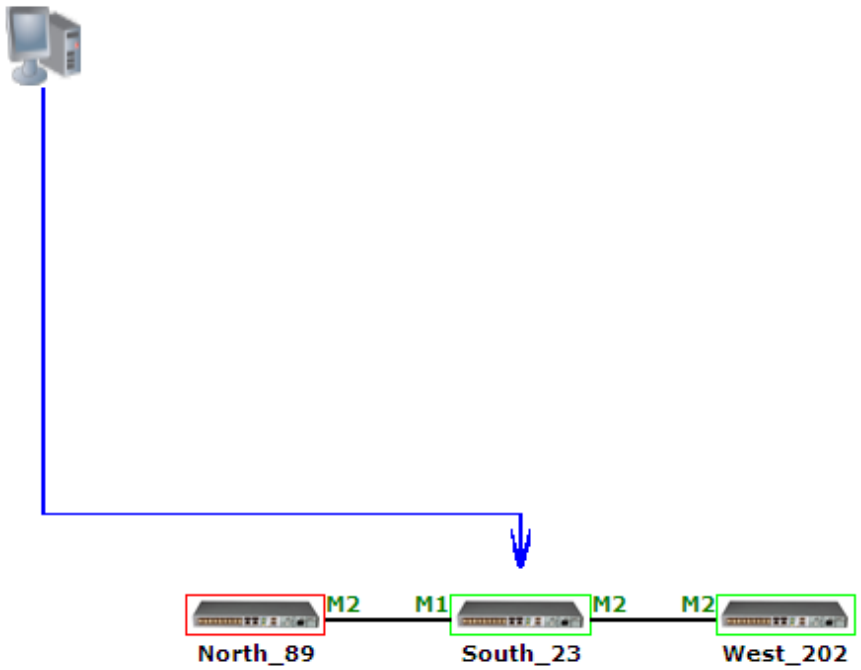


Figure 115: Linear Topology (Example)

9.1.1.2 Ring Topology

The following figure is an example of a network ring topology.

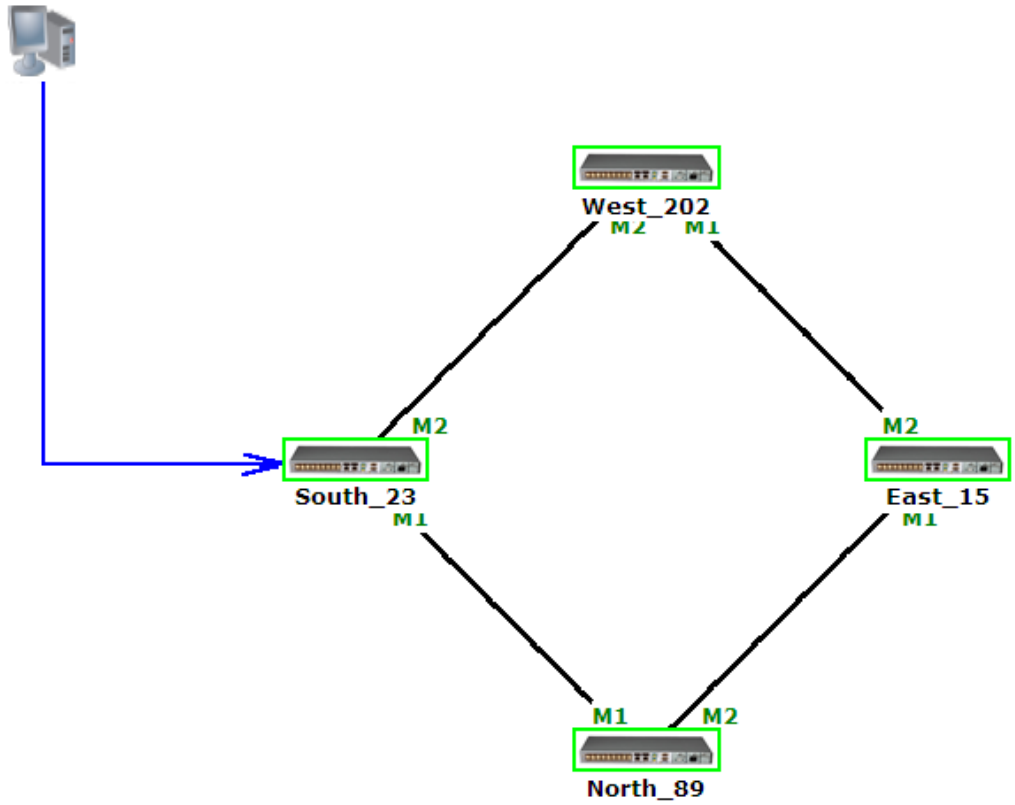


Figure 116: Ring Topology (Example)

9.1.1.3 Management Arc

The blue arrow starting at the management system and ending at a node points to the node that is currently being browsed via the HTTP/HTTPS session.

9.1.1.4 Node Title

The system name of the node is displayed below the node. If there is no configured name, the OSC/In-band IP address of the node is displayed.

9.1.1.5 Alarm Status of the Node

The alarm status of each node is marked by the color of the box around the node:

- **Green**: No Major alarms on the node
- **Red**: Major alarms on the node

9.1.1.6 MNG Port Labels

The labels attached to the arc ends represent the identity of the management port connected to that arc.

- **M1**: Stands for MNG 1 port.
- **M2**: Stands for MNG 2 port.

9.1.2 Zooming In and Out of the Topology Display

In complex networks, some details of the displayed topology may be hidden or unclear and a zoom may be required. Therefore, for non-linear topologies, you can zoom in and out of the topology display.

To zoom in and out of the topology display:

1. Click the **Network Topology** tab.

   The Network Topology tab opens displaying the PL-1000IL nodes connected together with the OSC channel.

2. To increase magnification of the topology display, click **Zoom In**  .
3. To decrease magnification of the topology display, click **Zoom Out**  .
4. To return to the original view of the topology display, click **Restore To Default**  .

9.1.3 Browsing Other Nodes

You can use the topology view to browse other nodes displayed in the network topology.

To browse other nodes:

1. Click the **Network Topology** tab.

   The Network Topology tab opens displaying the PL-1000IL nodes connected together with the OSC channel.

2. Click a node icon  .

   A new Web browser opens enabling you to view the selected node.

   NOTE: You should have the IP access of the node you want to browse. Therefore, you may have to define one of the nodes as the gateway to the other node, and if needed, add the IP address of the management system to the **Static Routing** table of the node (see IP Tab (p. 101).)

9.1.4 Defining Multiple Nodes as Multi-Chassis

When multiple PL-1000IL nodes are located at the same site, you can define them as *multi-chassis*.

NOTE: The Chassis ID number must be the same for each node.

To define multiple nodes as multi-chassis:

1. Log in to the PL-1000IL node (see Logging In to the Web Application (p. 30)).
2. Click **Configuration**.
3. Click **System**.

   The System Configuration window opens.
4. Click the **General** tab.

   The General tab opens.

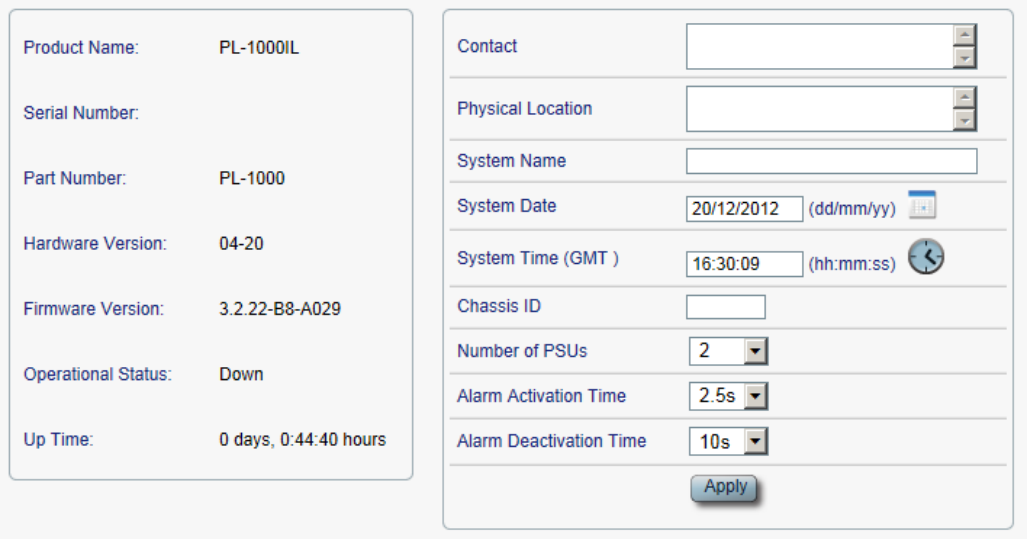


Figure 117: General Tab

5. In the **Chassis ID** field, type the number.
6. Click **Apply**.
7. Repeat these steps for each node.

The following figure shows two nodes, in a ring of four, defined as multi-chassis.

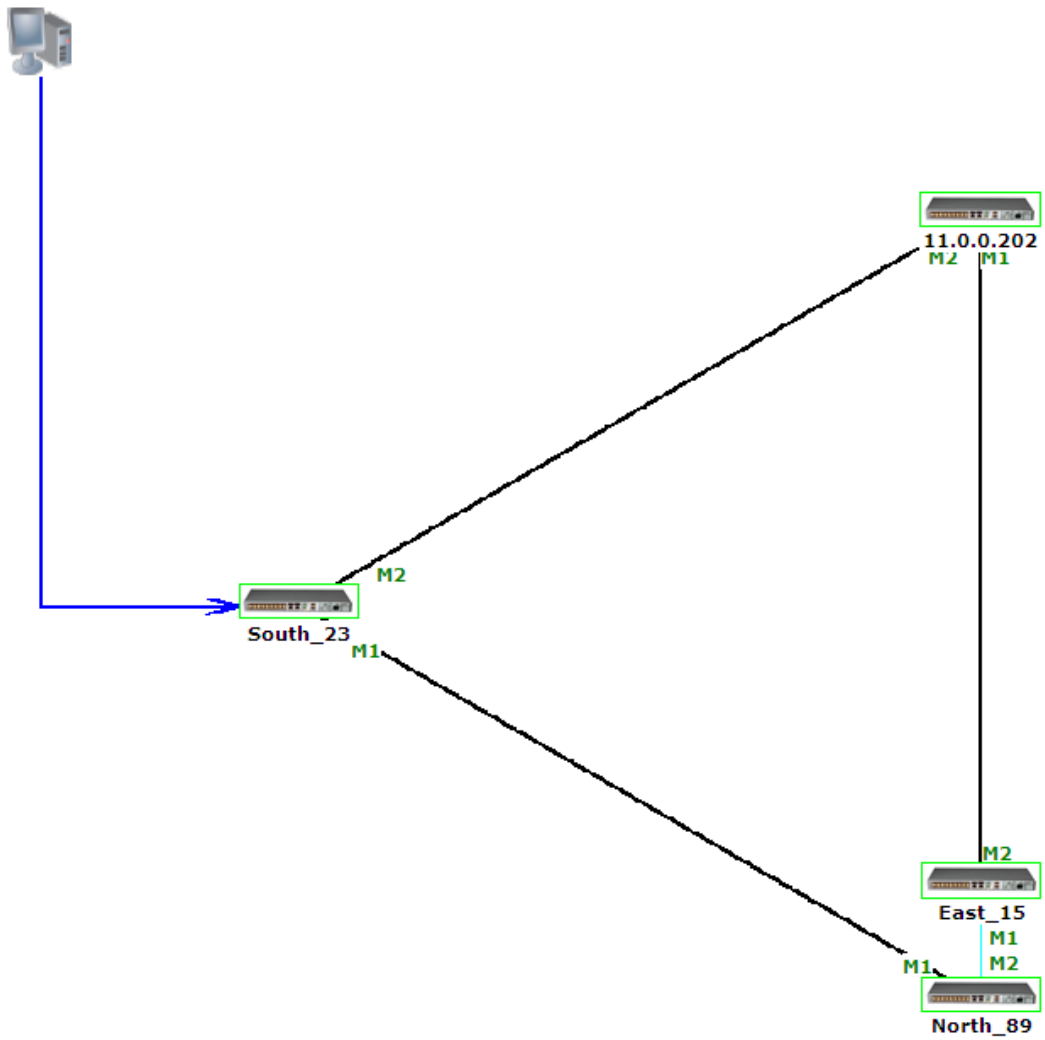


Figure 118: Multi-Chassis Nodes

10 Remote Management Configuration

This chapter provides instructions and for setting up and configuring remote management.

In this Chapter

10.1 Example of Remote Management Configuration

A remote PL-1000IL can be managed through the OSC.

The following figure shows an example of how to configure the remote management for the point-to-point setup. In this setup, there are two management systems: **A** and **B**. These systems can manage the PL-1000IL nodes A and B via the OSC.

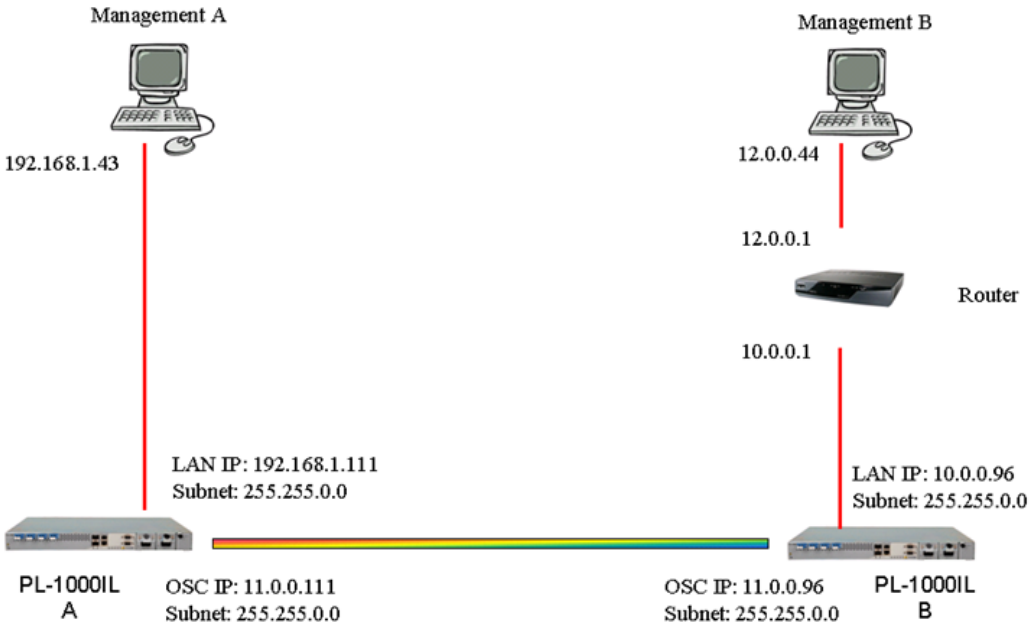


Figure 119: Remote Management Configuration (Example)

10.1.1 Setting Up Point-to-Point Management

To set up point-to-point management:

1. Make sure that you have local Web access to both PL-1000IL nodes (see Accessing the Web Application (p. 29)).
2. Configure management for PL-1000IL A.
3. Configure management for PL-1000IL B.
4. Access the Web application from Management A to PL-1000IL A.

5. Access the Web application from Management A to PL-1000IL B.
6. Access the Web application from Management B to PL-1000IL B.
7. Access the Web application from Management B to PL-1000IL A.

10.1.2 Configuring Management for PL-1000IL A

To configure management for PL-1000IL A:

1. Click **Configuration**.
2. Click **System**.

   The System Configuration window opens.
3. Click the **IP** tab.

   The IP tab opens displaying the IP Address and Static Routing configuration (see IP Tab (p. 101)).
4. In the **IP Addresses** section, fill in the fields as follows:
   - **LAN IP Address**: 192.168.1.111
   - **LAN Subnet Mask**: 255.255.0.0
   - **Default Gateway**: 11.0.0.96
   - **OSC/In-band IP Address**: 11.0.0.111
   - **OSC/In-band Subnet Mask**: 255.255.0.0
5. Click **Apply**.

   The IP Addresses section should appear as follows.

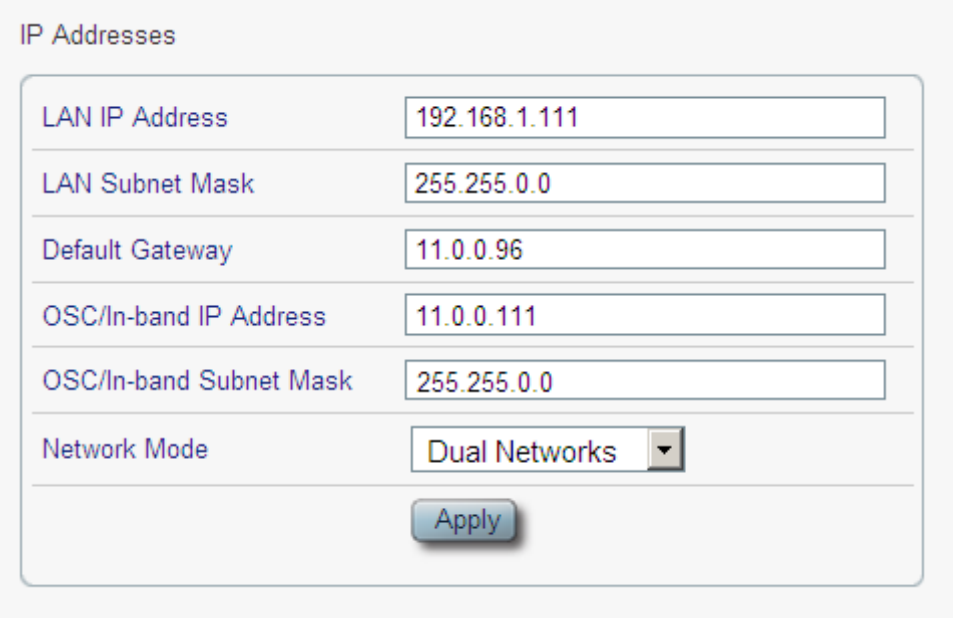


Figure 120: IP Addresses: PL-1000IL A (Example)

6. (Required only if using an SNMP management system) Configure the **SNMP Traps** table to send SNMP traps to the two management systems: **A** and **B** (see SNMP Tab (p. 104)).

   The SNMP Traps table should appear as follows.

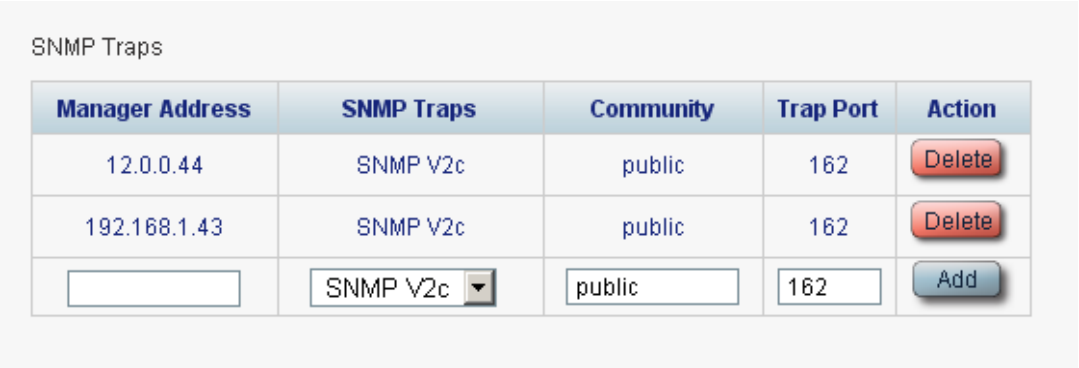


Figure 121: SNMP Traps Table (Example)

10.1.3 Configuring Management for PL-1000IL B

When configuring the management for PL-1000IL B, make sure that:

- Different IP addresses are assigned to each MNG port in the remote and local nodes.
- The MNG ports of the remote and local PL-1000IL nodes should be in same subnet.

To configure management for PL-1000IL B:

1. Click **Configuration**.
2. Click **System**.

   The System Configuration window opens.

3. Click the **IP** tab.

   The IP tab opens displaying the IP Address and Static Routing configuration (see IP Tab (p. 101)).

4. In the **IP Addresses** section, fill in the fields as follows:
   - **LAN IP Address**: 10.0.0.96
   - **LAN Subnet Mask**: 255.255.0.0
   - **Default Gateway**: 11.0.0.111
   - **OSC/In-band IP Address**: 11.0.0.96
   - **OSC/In-band Subnet Mask**: 255.255.0.0
5. Click **Apply**.

The IP Addresses section should appear as follows.

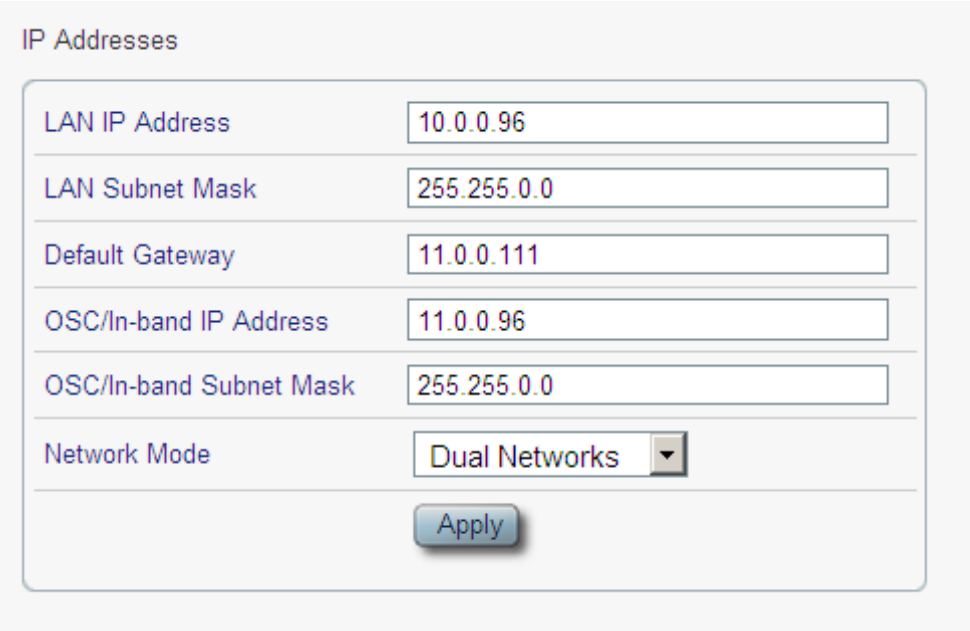


Figure 122: IP Addresses: PL-1000IL B (Example)

6. Configure the **Static Routing** table to enable the route to Management B as follows:
   - **Destination Address**: 12.0.0.0
   - **Gateway**: 10.0.0.1
7. Click **Add**.

   The Static Routing table should appear as follows.

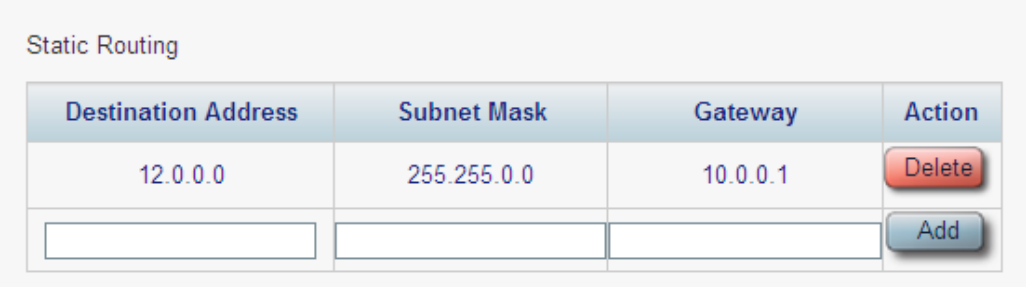


Figure 123: Static Routing: PL-1000IL B (Example)

8. (Required only if using an SNMP management system) Configure the **SNMP Traps** table to send SNMP traps to the two management systems: **A** and **B** (see SNMP Tab (p. 104)).

The SNMP Traps table should appear as follows.

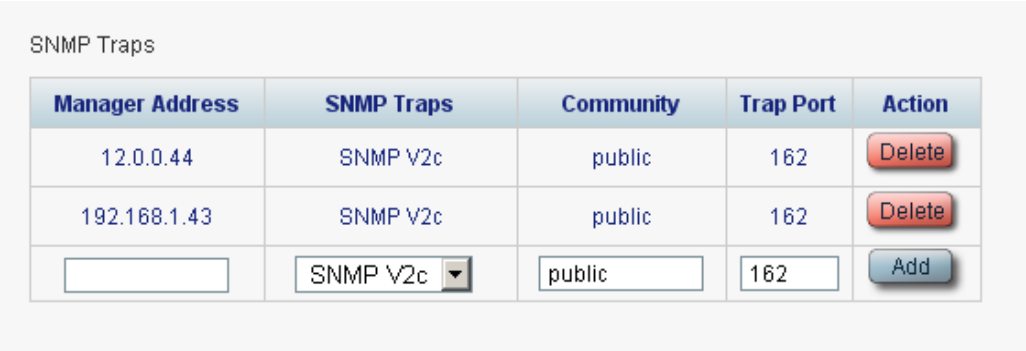


Figure 124: SNMP Traps Table (Example)

10.1.4 Accessing the Web Application from Management A to PL-1000IL A

To access the Web application from Management A to PL-1000IL A:

1. Open the Web browser.
2. In the address field of the browser, type the **IP address** of the LAN port of PL-1000IL A as follows:

   http://192.168.1.111 (for HTTP access)

   or

   https://192.168.1.111 (for HTTPS secure access) (as illustrated in Remote Management Configuration Example (p. 157))
3. Press **Enter**.

   The Login window opens.
4. Log in to the Web application (see Logging In to the Web Application (p. 30)).

10.1.5 Accessing the Web Application from Management A to PL-1000IL B

To access the Web application from Management A to PL-1000IL B:

1. Add a new route to Management A as follows:

   > ROUTE ADD 11.0.0.0 MASK 255.255.0.0 192.168.1.111
2. Open the Web browser.
3. In the address field of the browser, type the **IP address** of the management port of the remote PL-1000IL as follows:

   http://11.0.0.96 (for HTTP access)

   or

   https://11.0.0.96 (for HTTP secure access) (as illustrated in Remote Management Configuration Example (p. 157))

4. Press **Enter**.

   The Login window opens.

5. Log in to the Web Application (see Logging In to the Web Application (p. 30)).

10.1.6 Accessing the Web Application from Management B to PL-1000IL B

To access the Web application from Management B to PL-1000IL B:

1. Add a new route to Management B as follows:

   > ROUTE ADD 10.0.0.0 MASK 255.255.0.0 12.0.0.1

2. Open the Web browser.
3. In the address field of the browser, type the **IP address** of the LAN port of PL-1000IL B as follows:

   http://10.0.0.96 (for HTTP access)

   or

   https://10.0.0.96 (for HTTP secure access) (as illustrated in Remote Management Configuration Example (p. 157))

4. Press **Enter**.

   The Login window opens.

5. Log in to the Web Application (see Logging In to the Web Application (p. 30)).

10.1.7 Accessing the Web Application from Management B to PL-1000IL A

To access the Web application from Management B to PL-1000IL A:

1. Add a new route to Management B as follows:

   > ROUTE ADD 11.0.0.0 MASK 255.255.0.0 12.0.0.1

2. Configure the router between Management B and PL-1000IL A so that the IP address of the PL-1000IL B LAN port (**10.0.0.96** as illustrated in Remote Management Configuration Example (p. 157)) is the gateway for subnet **11.0.0.0**.
3. In the address field of the browser, type the **IP address** of the MNG port of PL-1000IL A as follows:

   http://11.0.0.111 (for HTTP access)

   or

   https://11.0.0.111 (for HTTP secure access) (as illustrated in Remote Management Configuration Example (p. 157))

4. Press **Enter**.

   The Login window opens.

5. Log in to the Web application (see Logging In to the Web Application (p. 30)).

11 CLI

This chapter describes the CLI for PL-1000IL.

The CLI provides commands for status monitoring and basic configuration of the PL-1000IL.

In this Chapter

11.1 General Features

The following are the general features of the CLI:

- The CLI uses the user and password authentication inherited from the Web application. The same user and password that is used for the Web application is accepted by the CLI.
- The CLI checks the user permission properties (Administrator, Read/Write, Read-Only) during command execution. These properties are inherited from the Web application.
- The CLI commands are ordered in a hierarchical tree structure. To move between tree nodes, you specify the name of the next node. The current hierarchy is specified by the prompt.
- Help is available for each command.
- The commands are case sensitive.
- The CLI allows command abbreviation. This means that a unique command prefix can be used instead of writing the full command name.

  NOTE: No abbreviation is allowed for the parameters of the command.

11.2 Accessing the CLI

There are two ways to access the CLI:

- **Using a Serial Port**: This method uses the CONTROL port of the PL-1000IL to connect locally to a PC with a terminal emulation application.
- **Using Telnet or SSH**: These methods can be used with an IP connection via the local LAN port or remotely via the OSC or in-band channel.

11.2.1 Using a Serial Port

To use a serial port to access the CLI:

1. Connect the COM port of the PC to the CONTROL port of the node using a DB-9 RS-232 connector.
2. On the PC, open a terminal emulation application that uses the COM port.
3. Configure the COM port as follows:
   - **Baud rate**: 9600 bps
   - **Data**: 8 bits
   - **Parity**: None
   - **Start**: 1 bit
   - **Stop**: 1 bit
   - **Flow control**: None
4. Press **ENTER**.

   The CLI prompt appears as follows:

```
PL-1000IL>>
```

5. Log in to the node using the predefined user and password.

   NOTE: For security reasons, the password is not echoed to the terminal.

   For example:

```
PL-1000IL>>login
User: admin
Password:
PL-1000IL>>
```

6. Run the desired CLI commands as described in Running CLI Commands (p. 167).

11.2.2 Using Telnet

To use a Telnet session to access the CLI:

1. Make sure that there is an IP connection to the node by opening the CMD window and typing the following command:

   $ ping <node-ip-address>

   If the IP connection exists, the ping command should respond with output similar to the following:

```
Pinging 192.168.3.201 with 32 bytes of data:
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.3.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. After the successful ping, invoke the following command:

   $ telnet <node-ip-address>

   As a result, the Telnet session starts and the CLI prompt of the node is displayed:

```
PL-1000IL>>
```

3. Log in to the node using the predefined user and password.

   For example:

```
PL-1000IL>>login
User: admin
Password:
PL-1000IL>>
```

4. Run the desired CLI commands as described in Running CLI Commands (p. 167).

5. Terminate the Telnet session by pressing **<CTRL+]>**.

   The following prompt is displayed:

```
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'
Microsoft Telnet>
```

6. To exit the Telnet session, type the following command: **quit**

11.2.3 Using SSH

To use SSH, you should have an installed SSH client on your machine.

To use an SSH session to access the CLI:

1. Make sure that there is an IP connection to the node by opening the CMD window and typing the following command:

   $ ping <node-ip-address>

   If the IP connection exists, the ping command should respond with output similar to the following:

```
Pinging 192.168.3.201 with 32 bytes of data:
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Reply from 192.168.3.201: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.3.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. After the successful ping, invoke the SSH client. You should specify to the client the IP of the node to which you want to connect.

   If this is the first time you connect to the node, you will probably see a message similar to the following:

```
The server's host key is not cached in the registry.
You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 7b:e5:6f:a7:f4:f9:81:62:5c:e3:1f:bf:8b:57:6c:5a
```

```
If you trust this host, hit Yes to add the key to PuTTY's cache and carry
on connecting.
If you want to carry on connecting just once, without adding the key to
the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
```

3. If such a message appears, hit **Yes** to approve the connection.
4. Complete the log in to the node by using the predefined user and password.

   For example:

```
login as: admin
Sent username "admin"
admin@192.168.3.3's password:
PL-1000IL>>
```

5. Run the desired CLI commands as described in Running CLI Commands (p. 167).
6. Terminate the SSH session by pressing **'CTRL+D'**.

11.3 CLI Command Types

The following types of CLI commands are supported:

- General commands: These commands can be invoked from anywhere in the command tree.
- Ping command
- Interface commands
- IP Setting commands
- Log commands
- Show commands
- System Restart command

The following figure shows the hierarchy of the commands.

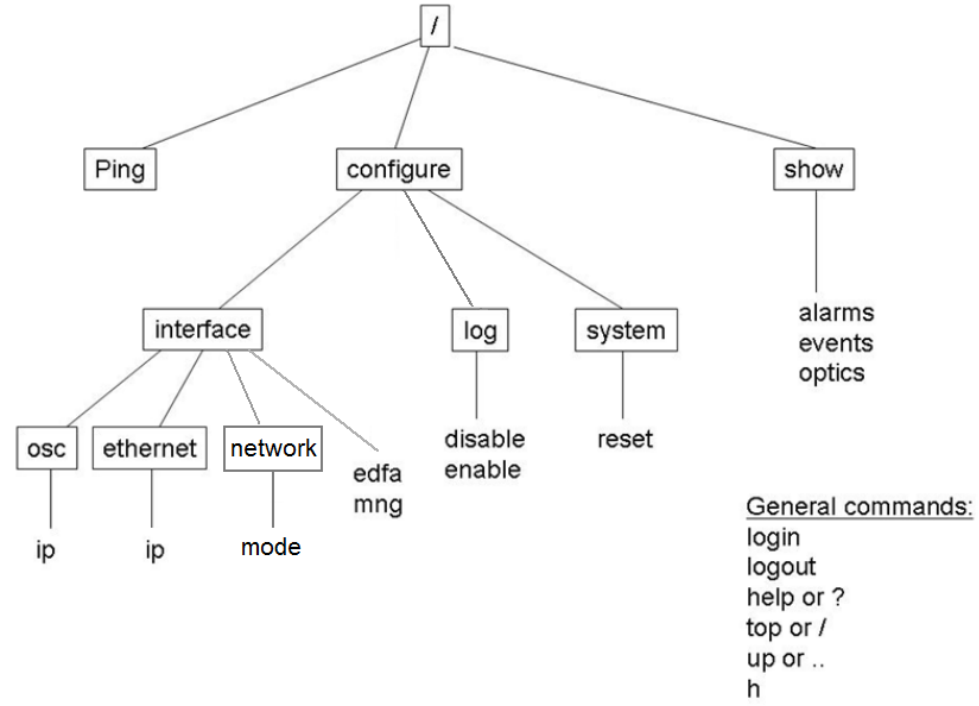


Figure 125: CLI Command Tree

11.4 Running CLI Commands

You can run the following CLI commands:

- General commands
  - Login (p. 168)
  - Logout (p. 169)
  - Help (p. 169)
  - History (p. 169)
  - Top (p. 170)
  - Up (p. 170)
- Ping Command (p. 170)
- Interface commands
  - Configure Interface MNG Command (p. 171)
  - Configure Interface EDFA Command (p. 171)
- IP Setting commands
  - Configure Interface Ethernet IP (p. 172)
  - Configure Interface OSC IP (p. 172)
  - Configure Interface Network Mode (p. 173)

- Log commands
  - Configure Log Enable (p. 173)
  - Configure Log Disable (p. 173)
- Show commands
  - Show Alarms (p. 174)
  - Show Events (p. 174)
  - Show Optics (p. 175)
- System Restart command
  - Configure System Restart (p. 175)

11.4.1 General Commands

The following are general commands that can be invoked from anywhere in the command tree:

- Login (p. 168)
- Logout (p. 169)
- Help (p. 169)
- History (p. 169)
- Top (p. 170)
- Up (p. 170)

11.4.1.1 Login Command

Command:

login

Description:

This command is required before any other command can be issued.

The CLI uses the user and password authentication inherited from the Web application. The same user and password that is used for the Web application is accepted by the CLI.

In addition, the CLI checks the user permission properties (Administrator, Read Only, Read-Write) during command execution. These properties are inherited from the Web application.

Example:

```
PL-1000IL>>login
User: admin
Password:
PL-1000IL>>
```

NOTE: For security reasons, the password is not echoed to the terminal.

11.4.1.2 Logout Command

Command:

logout

Description:

This command terminates the user session.

To run further CLI commands, you must log in again.

Example:

```
PL-1000IL>>logout
PL-1000IL>>
```

11.4.1.3 Help Command

Command:

help [<command>]

or

? [<command>]

Description:

This command displays the syntax of the specified command.

Example:

```
PL-1000IL>>help con int eth ip
config interface ethernet ip [<addr> [-n <netmask>] [-g <gateway>]]
PL-1000IL>>
```

11.4.1.4 History Command

Command:

h

Description:

This command displays the last 20 commands.

Example:

```
PL-1000IL>show>>h
 15  ?
 16  ..
 17  xp
 18  ?
 19  ..
 20  ?
 21  log
 22  ?
 23  ..
 24  ?
 25  sys
 26  ?
 27  ..
 28  ?
```

```
 29  ..
 30  ?
 31  sh
 32  ?
 33  !
 34  h
PL-1000IL>show>>
```

11.4.1.5 Top Command

Command:

top

or

/

Description:

This command takes you to the root of the command tree.

Example:

```
PL-1000IL>configure>interface>>top
PL-1000IL>>
```

11.4.1.6 Up Command

Command:

up

or

..

Description:

This command takes you up one level in the command tree.

Example:

```
PL-1000IL>configure>interface>ethernet>>up
PL-1000IL>configure>interface>>
```

11.4.2 Ping Command

Command:

ping <ip-address>

Description:

This command sends a ping request to the specified IP address.

Example:

```
PL-1000IL>>ping 11.0.0.36
Pinging 11.0.0.36 (11.0.0.36) with 64 bytes of data:
Reply from 11.0.0.36 bytes=64 ttl=64 seq=0 time=0ms
--- 11.0.0.36 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0 ms
```

```
rtt min/avg/max = 0/0/0 ms
PL-1000IL>>
```

11.4.3 Interface Commands

The following are the Interface commands:

- Configure Interface MNG
- Configure Interface EDFA

NOTE: The commands **Configure Interface Uplink** and **Configure Interface Port** are not applicable to the PL-1000IL.

11.4.3.1 Configure Interface MNG Command

Command:

configure interface mng <num> [up | down]

Description:

This command sets the **Admin Status** of the MNG port to the required value.

If the **Admin Status** is not specified, the administrative status of the MNG port is displayed.

Example:

```
PL-1000IL>configure>interface>>mng 1 down
PL-1000IL>configure>interface>>mng 1
Port MNG 1 is DOWN
PL-1000IL>configure>interface>>
```

11.4.3.2 Configure Interface EDFA Command

Command:

configure interface edfa <num> [up | down]

Description:

This command sets the **Admin Status** of the EDFA to the required value.

If the **Admin Status** is not specified, the administrative status of the EDFA is displayed.

Example:

```
PL-1000IL>configure>interface>>edfa 1 up
PL-1000IL>configure>interface>>
```

11.4.4 IP Setting Commands

The following are the IP Setting commands:

- Configure Interface Ethernet IP (p. 172)
- Configure Interface OSC IP (p. 172)
- Configure Interface Network Mode (p. 173)

11.4.4.1 Configure Interface Ethernet IP Command

Command:

configure interface ethernet ip [<addr> [-n <netmask>] [-g <gateway>]]

Description:

This command sets the IP parameters of the LAN port.

- **<addr>**: IP address of the LAN port.
- **<netmask>**: Subnet mask of the port.
- **<gateway>**: IP address of the default gateway.

If no parameters are specified, the current IP parameter values are displayed.

Example:

```
PL-1000IL>configure>interface>ethernet>>ip 10.0.3.200 –n 255.255.0.0 –g
10.0.44.44
PL-1000IL>configure>interface>ethernet>>ip
Addr is 10.0.3.200, Subnet mask is 255.255.0.0
Gateway is 10.0.44.44
PL-1000IL>configure>interface>ethernet>>
```

11.4.4.2 Configure Interface OSC IP Command

Command:

configure interface osc ip [<addr> [-n <netmask>] [-g <gateway>]]

Description:

This command sets the IP parameters of the MNG ports.

- **<addr>**: IP address of the MNG ports.
- **<netmask>**: Subnet mask of the MNG ports.
- **<gateway>**: IP address of the default gateway.

If no parameter is specified, the current IP parameter values of the MNG ports are displayed.

NOTE: When working via Telnet, changing the IP parameters of the OSC may prevent further access to the node.

Example:

```
PL-1000IL>configure>interface>osc>>ip 11.0.3.200 –n 255.255.0.0 –g
11.0.3.201
PL-1000IL>configure>interface>osc>>ip
Addr is 11.0.3.200, Subnet mask is 255.255.0.0
Gateway is 11.0.3.201
PL-1000IL>configure>interface>osc>>
```

11.4.4.3 Configure Network Mode

Command:

configure interface network mode [dual | single]

Description:

This command sets the network mode to **Dual Networks** mode or **Single Network** mode.

- **Dual**: In this mode, the node has two IP addresses; one for the LAN port and the other for the MNG ports.
- **Single**: In this mode, the node has a single IP address that is used for the all management ports (LAN port and MNG ports).

NOTE: After changing network mode, you must cold restart the node (see Configure System Reset Command (p. 175)).

Example:

```
PL-1000IL>configure>interface>network>>? mode
config interface network mode [dual|single]
PL-1000IL>configure>interface>network>>mode
Current network mode is single
PL-1000IL>configure>interface>>..
PL-1000IL>configure>>interface network mode dual
PL-1000IL>configure>>system reset c
```

11.4.5 Log Commands

The following are the Log commands:

- Configure Log Enable (p. 173)
- Configure Log Disable (p. 173)

11.4.5.1 Configure Log Enable Command

Command:

configure log enable

Description:

This command enables the echoing of system events to the terminal.

By default, the log of the CLI session accessed via the serial port is enabled.

Example:

```
PL-1000IL>configure>log>>enable
PL-1000IL>configure>log>>
```

11.4.5.2 Configure Log Disable Command

Command:

configure log disable

Description:

This command disables the echoing of system events to the terminal.

By default, the log of the CLI session accessed via Telnet is disabled.

Example:

```
PL-1000IL>configure>log>>disable
PL-1000IL>configure>log>>
```

11.4.6 Show Commands

The following are the Show commands:

- Show Alarms (p. 174)
- Show Events (p. 174)
- Show Optics (p. 175)

11.4.6.1 Show Alarms Command

Command:

show alarms [mng <num>] | [edfa <num>] | [system]

Description:

This command displays the alarms of the specified entity. If no parameters are specified, all alarms are displayed.

Example:

```
PL-1000IL>>show alarms mng 1
THU JUN 18 12:22:46 2009       MNG1  Optics Loss of Light    Critical
S.A.
PL-1000IL>>
```

11.4.6.2 Show Events Command

Command:

show events [mng <num>] | [edfa <num>] | [system]

Description:

This command displays the events of the specified entity. If no parameters are specified, all the events are displayed.

Example:

```
PL-1000IL>>show events mng 1
THU JUN 18 12:22:44 2009        MNG 1  Link Up
Event
THU JUN 18 12:22:46 2009        MNG 1  Optics Loss of Light    Critical
S.A.
THU JUN 18 12:22:47 2009        MNG 1  Link Down
Event
PL-1000IL>>
```

11.4.6.3 Show Optics Command

Command:

show optics [mng <num>] | [edfa <num>]

Description:

This command displays the optical information of the specified port.

Example:

```
PL-1000IL>show optics mng 2
Vendor: Infineon FO GmbH
Part Number: V23848-M305-C56W
Serial Number: 26572841
Wavelength: 850.00 nm
Type: Non WDM

Tx Power: -6.2 dBm
Rx Power: -8.3 dBm
Temperature: 31 C
PL-1000IL>>
```

11.4.7 System Restart Command

The following is the System Restart command:

- Configure System Reset (p. 175)

11.4.7.1 Configure System Reset Command

Command:

configure system reset (f | c | w)

Description:

This command restarts the node.

The restart type is determined by the parameter of the command:

- **f**: Restore to factory defaults; traffic affecting; deletes the node configuration except for the IP information; removes all licensing information from the node (if applicable)
- **c**: Cold restart; traffic affecting; keeps the node configuration
- **w**: Warm restart; not traffic affecting; keeps the node configuration

NOTE:

- Performing this command while using Telnet will terminate the session.
- It is recommended to save the old configuration file before restoring to factory defaults.

Example (of a Telnet session):

```
PL-1000IL>>configure system reset w
PL-1000IL>>

Connection to host lost.
```

Appendix A: Connection Data

This appendix describes the connectors for the PL-1000IL.

In this Appendix

A.1 CONTROL Connector

The CONTROL connector is a 9-pin D-type female connector with RS-232 asynchronous DCE interface, intended for direct connection to a supervision terminal. The connection to the supervision terminal is by means of a straight cable (a cable wired point-to-point). The connector is wired in accordance with the following table.

Table 52: CONTROL Connector Wiring

Pin	Function	Direction
2	Transmit Data (TX)	From PL-1000IL
3	Receive Data (RX)	To PL-1000IL
5	Signal Ground (SIG)	Common reference

A.2 ALARM Connector

The ALARM connector of the PL-1000IL is a 9-pin D-type female connector that is used to connect to the external alarm system (for example, a buzzer) of the customer.

The ALARM connector provides two connectivity methods:

- Normally Open
- Normally Closed

The connector is wired in accordance with the following table.

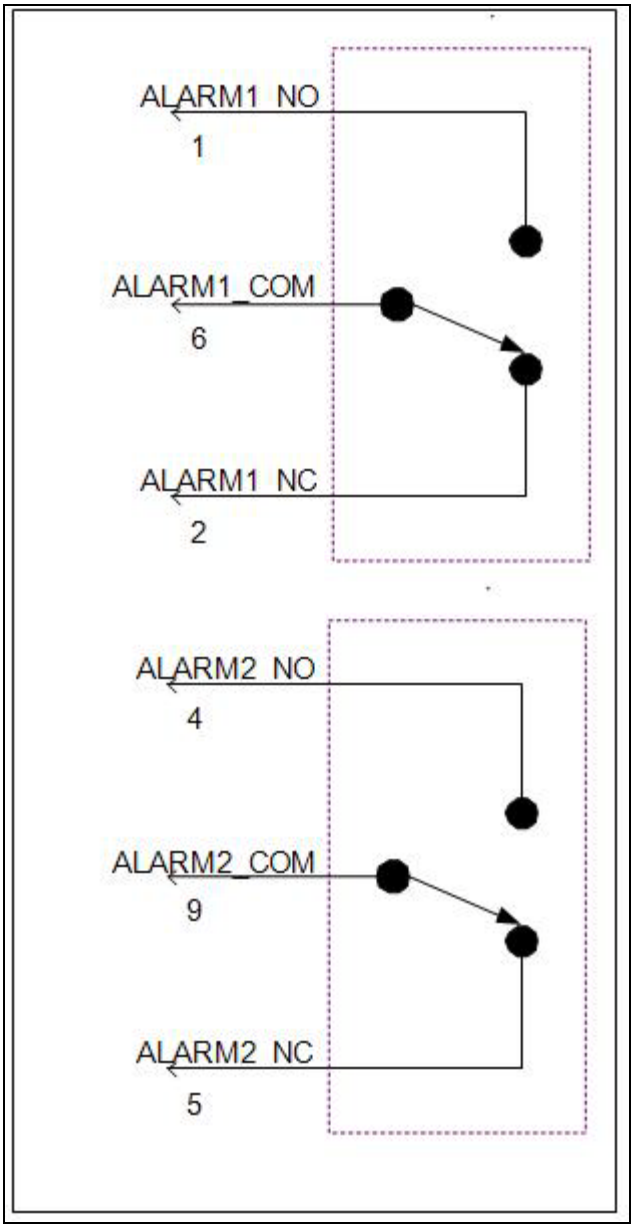


Figure 126: External ALARM Diagram

Table 53: ALARM Interface, Pin Function

Pin	Designation	Function
1	ALARM Normally Open (ALARM1_NO)	In normal operation, pin 6 (ALARM Common) is internally connected to pin 2 (ALARM Normally Closed). Upon a Major alarm event, the internal connection of pin 6 (ALARM Common) is switched to this pin (pin 1).

Pin	Designation	Function
2	ALARM Normally Closed (ALARM1_NC)	In normal operation, pin 6 (ALARM Common) is internally connected to this pin (pin 2). Upon a Major or Critical alarm event, the internal connection of pin 6 (ALARM Common) is switched to pin 1 (Alarm Normally Open)
6	ALARM Common (ALARM1_COM)	Common signal
3		Internally connected to GND.
7	ALARM IN 1	Input External Alarm
8	ALARM IN 2	Not connected
4*	ALARM Normally Open (ALARM2_NO)	In normal operation, pin 9 (ALARM Common) is internally connected to pin 5 (Alarm Normally Closed). Upon a Major alarm event, the internal connection of pin 9 (ALARM Common) is switched to this pin (pin 4).
5*	ALARM Normally Closed (ALARM2_NC)	In normal operation, pin 9 (ALARM Common) is internally connected to this pin (pin 5). Upon a Major alarm event, the internal connection of the pin 9 (ALARM Common) is switched to pin 4 (ALARM Normally Open).
9*	ALARM Common (ALARM2_COM)	Common signal

* The pin will be implemented in a future software release.

A.3 ETH Connector

The PL-1000IL ETH port is a 10/100 Base-T Ethernet interface terminated in an RJ-45 connector. The port can be connected by a standard station cable to any type of 10/100 Base-T Ethernet port.

Connector pin functions are listed in the following table.

Table 54: ETH Port Connector, Pin Functions

Pin	Designation	Function
1	RXD+	Receive Data output, + wire
2	RXD–	Receive Data output, – wire
3	TXD+	Transmit Data input, + wire
4, 5	–	Not connected
6	TXD–	Transmit Data input, – wire
7, 8	–	Not connected

A.4 Data Ports

The Data ports are two or four fixed duplex LC connectors.

Table 55: Data Port Specifications

Specification	Requirement
Fiber Type	Single mode
Fiber Size	2 mm optical
Connector Type	LC with protective shutters
Port Type	Optical COM/EDFA/OSC port

A.5 Power Supply Combinations

The following power supply combinations are feasible in the PL-1000IL:

- One or two AC power supplies
- One or two DC power supplies

NOTE: Both AC and DC PSUs can be used in the same unit.

A.6 Power Connectors

The PL-1000IL may have the following power supply connectors:

- **AC-powered PL-1000IL units**: Standard three-pin IEC320 C5 connector 3A for connection to AC power.
- **DC-powered PL-1000IL units**: DC power is supplied with a dedicated connector for wiring.

The following figure shows how to wire the DC connector (DC power supply only).

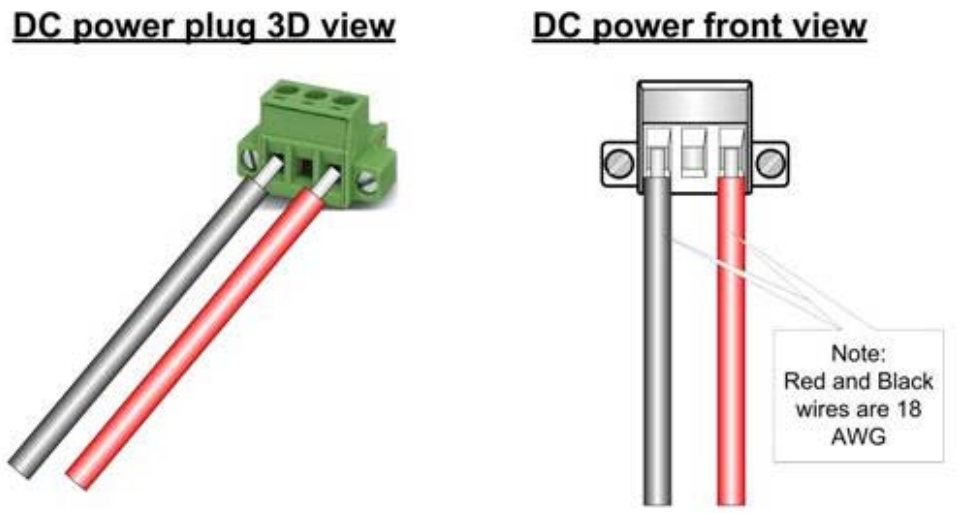


Figure 127: DC Connector Wiring Diagram

A.7 Protective Ground Terminal

The protective ground terminal of the PL-1000IL, located on the rack mount, must be connected to a protective ground.

The following figure shows how to wire the ground terminal.

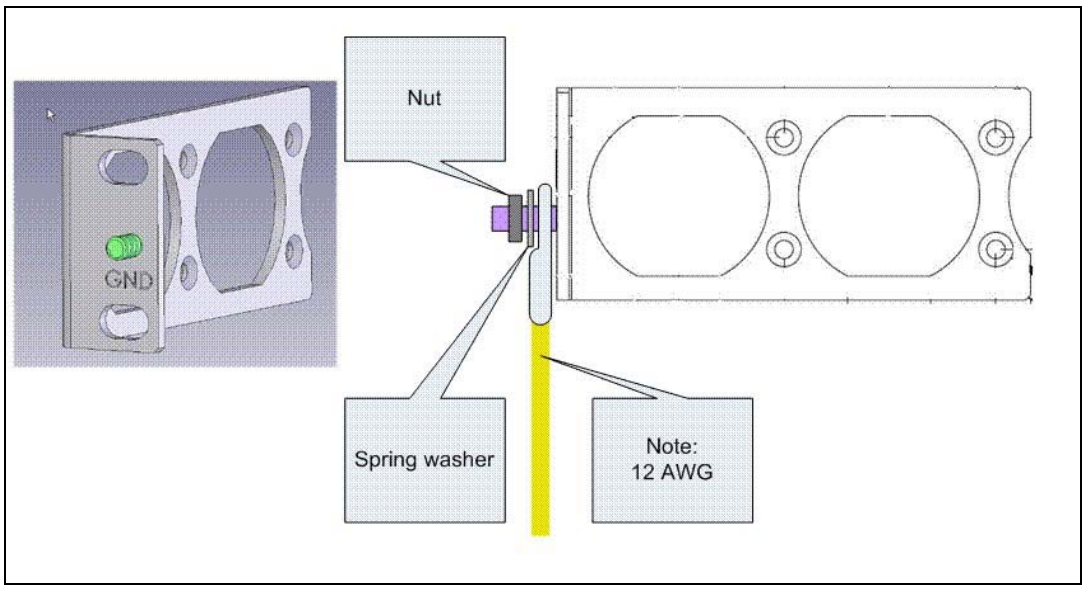


Figure 128: Protective Ground Terminal Wiring Diagram

A.8 Fiber Shelf

The fiber shelf is an optional tray that can be attached to the PL-1000IL to help you organize the optical fibers.

The following figure shows the mechanical details of the fiber shelf.

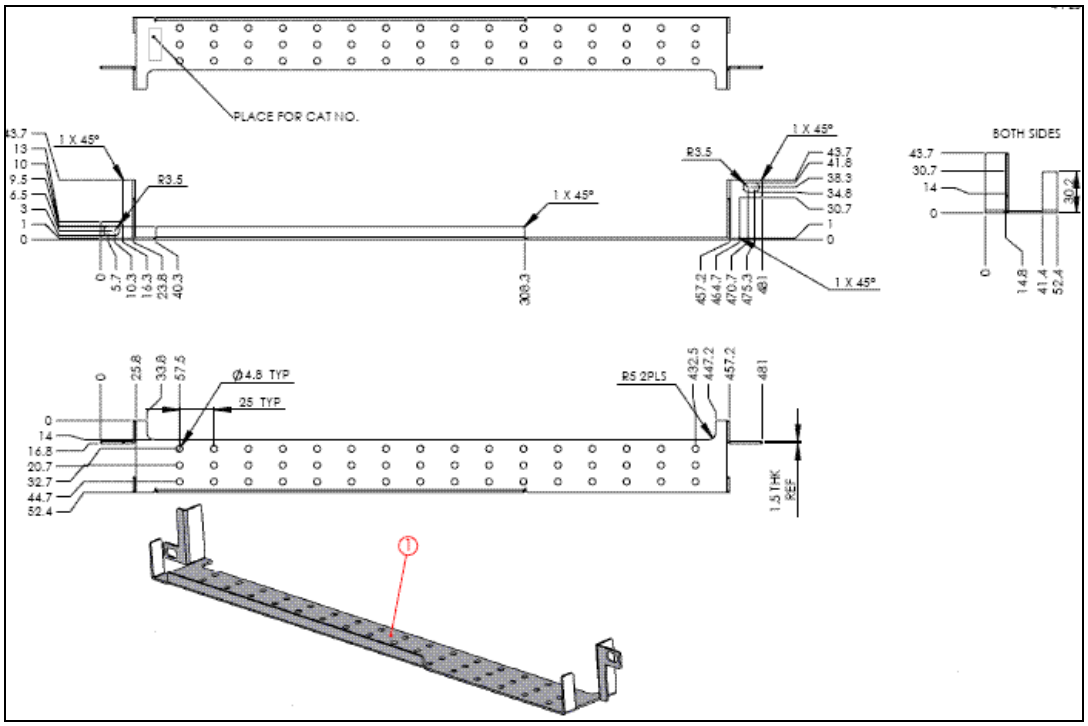


Figure 129: Fiber Shelf Diagram

Appendix B: Alarm and Event Messages

This appendix describes the possible alarm and event messages.

In this Appendix

B.1 Alarm Messages

The following table lists the possible PL-1000IL alarm messages and their interpretation and/or corrective measures.

Table 56: Alarm Messages

Source	Message	Interpretation/Corrective Measures
PSU1/PSU2	Power Supply Failure	Replace the faulty PSU.
PSU1/PSU2	Power Failure– Low Voltage	Replace the faulty PSU.
FAN	Fan Failure	The internal cooling fan of the device does not operate. Replace the FAN unit as soon as possible.
System	Hardware failure	A technical failure has been detected. Replace the device.
System	Database Restore Failed	Failed to update the system configuration.
System	Database Restore in Progress	Failed to update the system configuration.
System	Cold Restart Required: FPGA Changed	After a warm restart, the FPGA version is not consistent with the software version. A cold restart is required.
System	Software Upgrade Failed	The downloaded software is corrupted. Reload the software.
System	Network Time Protocol Failure	SNTP timing protocol failure. Check the IP connection to the NTP servers.
External Input Alarm	(As configured)	The External Input Alarm is active.
Optics	Optics Removed	The optical module has been removed. Insert an optical module or shut the port down.
Optics	Optics Loss of Light	A Loss of Light indication has been received in regards to the specific optical module. The optical power of the received signal is below the minimum power level. Check the fiber connection and/or clean the fiber connector.
Optics	Optics Transmission Fault	The transceiver is not transmitting. Replace the optical module.
Optics	Optics Hardware Failure	A hardware fault was detected in the optical module. Replace the optical module.

Source	Message	Interpretation / Corrective Measures
Optics	Optics High Transmission Power	The transmission power of the optical module is above its specification.
Optics	Optics Low Transmission Power	The transmission power of the optical module is below its specification.
Optics	Optics High Temperature	The temperature inside the optical module is above its specification.
Optics	Optics Low Temperature	The temperature inside the optical module is below its specification.
Optics	Optics High Reception Power	The incoming signal into the optical module is too high. An attenuation of the input signal is required.
Optics	Optics Low Reception Power	The incoming signal into the optical module is too low.
Optics	Optics High Laser Temperature	The temperature of the laser is above its specification..
Optics	Optics Low Laser Temperature	The temperature of the laser is below its specification..
Optics	Optics High Laser Wavelength	The laser wavelength exceeds the high alarm level.
Optics	Optics Low Laser Wavelength	The laser wavelength exceeds the low alarm level.
Optics	Optics Loss Propagation	The laser was shut down due to a problem on the interface of the port mate.
Optics	Optics Bit Rate Mismatch	The inserted optical module has a mismatch problem due to the wrong rate or type. Replace the optical module or update the configured service type.
Optics	Unauthorized Optics Inserted and is Shutdown	The inserted optical module is unauthorized for use. Replace the optical module with an authorized optical module.
EDFA	EDFA Gain	The EDFA gain is out of acceptable range.
EDFA	EDFA Hardware Failure	The interface does not respond.
EDFA	EDFA Temperature	The EDFA temperature is out of acceptable range.
EDFA	EDFA Loss of Light	No signal is detected.
EDFA	EDFA Receive Power Out of Bound	The receive signal is out of acceptable range. Check the optical power of the EDFA client signals. Use attenuation if required.
EDFA	EDFA Transmit Power Out of Bound	The transmit signal is out of acceptable range. Check the optical power of the EDFA client signals.
EDFA	EDFA Down	Closed the EDFA output upon loss of input. Check the EDFA client signals.
EDFA	EDFA End of Line	An EDFA problem. Replace the device.
EDFA	EDFA Eye Safety	Hazard. No fiber is connected to the port.

Source	Message	Interpretation / Corrective Measures
OSW	Optical Switch Loss of Signal	One of the optical switch ports has detected Loss of Signal. Check the signal level of the fibers connected to the COM ports.

B.2 Configuration Event Messages

The following table lists the configuration event messages generated by the PL-1000IL and explains their interpretation.

Table 57: Configuration Change Messages

Source	Message	Interpretation
System	Change date	The system date or time has changed.
System	Database Restore Completed	A new configuration file has been loaded.
System	Change IP	The IP of the node has changed.
System	Alarm cut-off	The Alarm Cut-off has been operated.
System	Add user	A new user was added.
System	Delete user	A user was deleted.
System	Configuration change	The configuration of the system was changed.
System	Delete routing entry	The Performance Management counters were reset.
Port	Admin Down	Admin Down has been performed for the port.
Port	Admin Up	Admin Up has been performed for the port.
Port/COM	Create APS	An APS was created for the port/COM.
Port/COM	Remove APS	The APS for the port/COM has been removed.
Port/COM	APS command	An APS command was issued.
Port/COM	APS clear command	An APS command was cleared.

B.3 Other Event Messages

The following table lists the other possible event messages and explains their interpretation.

Table 58: Other Event Messages

Event Type	Source	Message	Interpretation
Inventory Changed	PSU, FAN, Optics	Inventory Changed	The node inventory has changed. A component was inserted or removed.
Switchover	COM Port	APS Switch Over	A protection switching event has occurred.
Optical Power Drop	LINK Port	Power Level Drop	The Rx power of the port has been dropped by more than 2 dB since last interval.
Dying Gasp	System	Remote Unit Failure	A remote unit had a power failure.
Software Upgrade	System	Software Upgrade Completed	The software upgrade operation has been completed.

Appendix C: Troubleshooting Chart

This appendix describes some trouble symptoms and their corrective measures.

In this Appendix

C.1 Troubleshooting Chart

Identify the trouble symptoms in the following table and perform the actions listed under "Corrective Measures" in the order given until the problem is corrected.

Table 59: Troubleshooting Chart

No.	Trouble Symptoms	Probable Cause	Corrective Measures
1	PL-1000IL does not turn on.	No power	1. Check that the power cable is properly connected to the PL-1000IL power connector. 2. Check that both ends of the power cable are properly connected. 3. Check that power is available at the power outlet serving the PL-1000IL.
		Defective power supply	Replace the power supply unit.
		Defective PL-1000IL	Replace the PL-1000IL.
2	The LOS LED of a device connected to PL-1000IL is lit.	Cable connection problems	1. Check all cables at the PL-1000IL Tx and Rx port connectors. 2. Repeat check at the remote equipment. 3. Make sure that the optical module used matches the fiber type (single mode / multi-mode).
		Fiber problem	1. Use a short fiber to connect the remote equipment Rx connector to its Tx connector. 2. If the problem is solved, connect the Rx connector of the fiber to the Tx connector at the PL-1000IL location. 3. If the problem persists, replace the fiber.
		Defective remote equipment	Use a short fiber to connect the remote equipment Rx connector to its Tx. If the LOS LED is still lit, the remote equipment is defective.
		A problem with the PL-1000IL port state	Set the **Admin Status** of the COM port to **Up**.

No.	Trouble Symptoms	Probable Cause	Corrective Measures
		Loss of Propagation	Disable the **LOS Propagation** for this port. If the problem is solved, the reason for the SIG LOS is a loss on the mate PL-1000IL port.
		Defective optical module	1. Check for optical module alarms. 2. Replace the optical module.
		Defective PL-1000IL	1. Use a short fiber to connect the PL-1000IL Rx connector to its Tx connector.(A signal generator may be required as the PL-1000IL does not generate signals by itself.) 2. If the LOS LED is still lit, replace the PL-1000IL.
3	The LED of the local PL-1000IL port is red.	Cable connection problems	1. Check for proper connections of the cables to the PL-1000IL Tx and Rx connector. 2. Repeat check at the remote equipment.
		High Signal Level	1. Check the **Receiver Input Power** of the optical module. 2. If the power is too high, add an attenuator.
		Defective optical module	1. Check for optical module alarms. 2. Replace the optical module.
		Fiber problem	1. Check the **Receiver Input Power** of the optical module. 2. If the power is too low, replace the fiber.
		Defective PL-1000IL	1. Check the PL-1000IL alarms. 2. If there are alarms, replace the PL-1000IL.
		Defective remote equipment	1. Use a different remote unit. 2. If the problem is solved, replace the remote unit.
4	The system LED is red.	Defective PL-1000IL	1. Check the PL-1000IL alarms. 2. If there are alarms, replace the PL-1000IL.

No.	Trouble Symptoms	Probable Cause	Corrective Measures
5	The equipment attached to the LAN port of the local PL-1000IL cannot communicate with the remote PL-1000IL over the WAN.	Problem with the connection to the LAN	1. Check that the LINK LED of the corresponding LAN port lights. If not, check for proper connection of the cable to the LAN port. 2. Check that the **Admin Status** of the MNG port is **Up** and that it is operating properly. 3. Check that the IP information of the remote PL-1000IL is configured correctly (for example, the default gateway).
		External problem	Check the IP configuration of the external equipment (for example, the gateway address) that is connected to the local PL-1000IL LAN port.
		Defective PL-1000IL	Replace the PL-1000IL.

Index