PL-1000GT 1.1 INSTALLATION AND CONFIGURATION MANUAL

PL-1000GT 1.1 Installation and Configuration Manual

Contents

List of Figures

List of Tables

1 Introduction

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

In this Chapter

1.1 Overview

The PL-1000GT is a 100G multi-protocol, multi-rate, high-capacity optical transport solution that provides a unified 100G optical transport layer. It is an ITU-T OIF standard based platform that supports various client services over a single Coherent 100G OTU4 wavelength with a range of 2,000 km. The client services include the protocols: 100GbE-LAN, 40GbE-LAN, 10GbE-LAN, 8G Fiber Channel (FC), OC-192, STM-64, OTU2, and OTU2e. Future versions will include: 10G FC, OTU3, OTU4, OC-768, and STM-256.

The PL-1000GT is a flexible platform that can be configured to work in Muxponder mode to support a variety of 40G and 8G/10G client services or to work in Transponder mode to support a single 100G client service.

The PL-1000GT 100G Muxponder is designed to provide a unified 100G optical transport layer supporting various client services, including protocols: 40GbE-LAN, 10GbE-LAN, 8G FC, OC-192, STM-64, OTU2, and OTU2e. Future versions will include: 10G FC, OTU3, OC-768, and STM-256.

The PL-1000GT 100G Transponder provides a 100G optical transport layer for the 100GbE-LAN service. Future versions will include OTU4.

The PL-1000GT is a highly integrated device that can incorporate an Erbium Doped Fiber Amplifier (EDFA) module.

The PL-1000GT is fully interoperable with PacketLight's family of products.

1.1.1 Main Features

The PL-1000GT combines the following key features:

- User configurable Transponder or Muxponder mode:
  - Transponder mode:
    - 1 x 100G interface into a 100G DWDM uplink

  - Muxponder mode:
    - 10 x 10G interfaces into a 100G DWDM uplink
    - 2 x 40G + 2 x 8G/10G interfaces into a 100G DWDM uplink
    - 1 x 40G+ 6 x 8G/10G interfaces into a 100G DWDM uplink
- Supported clients:
  - 100G Transponder clients:
    - 100GbE-LAN
    - OTU4 (future versions)
  - 40G Muxponder clients:
    - 40GbE-LAN
    - OTU3 (future versions)
    - OC-768 (future versions)
    - STM-256 (future versions)
  - 8G/10G Muxponder clients:
    - 10GbE-LAN
    - 8G FC
    - OC-192
    - STM-64
    - OTU2
    - OTU2e
    - 10G FC (future versions)
- Supports standard MSA pluggable:
  - **100G uplink**: Coherent with a range of 2,000 km
  - **100G client**: CFP
  - **40G client**: QSFP+
  - **8G/10G client**: SFP+
- Standard based G.709 Generic Forward Error Correction (GFEC) and High Gain Forward Error Correction (HG-FEC)
- Optional integrated Booster or Pre-Amp EDFA module
- Two 100/1000M management channels based on pluggable (SFP) optics for remote management
- Remote management with in-band channel embedded in the uplink signal or out-of-band Optical Supervisory Channel (OSC)
- Automatic Laser Shutdown (ALS) on all optical ports

- Provides the following management protocols for configuration and monitoring:
  - 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 transfer
  - Rapid Spanning Tree Protocol (RSTP)
- Supports Operations, Administration, and Maintenance (OAM) functions:
  - Optical parameters monitoring
  - Alarm and Event fault management
  - Performance monitoring (PM)
  - Facility loopback
  - Diagnostic Pseudo Random Binary Sequence (PRBS)
  - External alarms
- Operates on single or dual fiber solutions
- Pluggable FAN unit
- DC dual power supply units (PSUs)

1.1.2 Typical Application

The PL-1000GT is a multi-service OTN muxponder and transponder. It provides an efficient and flexible aggregation of multi-protocol 10G/40G/100G rate services into a single common 100G OTU4 uplink, thereby reducing the number of required wavelengths. Increasing fiber utilization and spectral efficiency of data transport reduces the solution cost and operation complexity.

The PL-1000GT can transparently aggregate a mix of SDH/SONET, Ethernet, Fiber Channel, and OTN services.

The PL-1000GT transparently multiplexes up to 10 client services into a single or dual 100G OTU4 wavelength. This is done in Layer-1, using low latency mapping to a 10G uplink pipe without packet loss and with FEC, which is suitable for long distance amplified DWDM networks.

Remote management is supported via an in-band channel embedded in the OTU4 uplink signal, or with two additional MNG ports that may be used for transmission of the management traffic over an Optical Supervisory Channel (OSC).

The PL-1000GT can incorporate an EDFA module according to the required configuration.

The PL-1000GT can be managed using Command Line Interface (CLI) over a serial or Telnet/Secure Shell (SSH) connection, Web management over HTTP/HTTPS, or SNMP.

As with other PacketLight devices, the PL-1000GT can be managed with PacketLight's LightWatch™ NMS/EMS (network management system). For information about LightWatch, see the *LightWatch Getting Started Guide*.

All optical transceivers, both on the service side and on the WDM-uplink side, are pluggable and fully replaceable, allowing pay-as-you-grow budget planning and simplified maintenance.

The PL-1000GT can be used to save wavelength resources and enable long distance high performance LAN connectivity.

The following figure illustrates a typical application for standalonePL-1000GT units. They are deployed as customer premises equipment (CPE) in enterprise campus environments, and connect the local LANs in the two campuses across a fiber connection or via a DWDM public network.

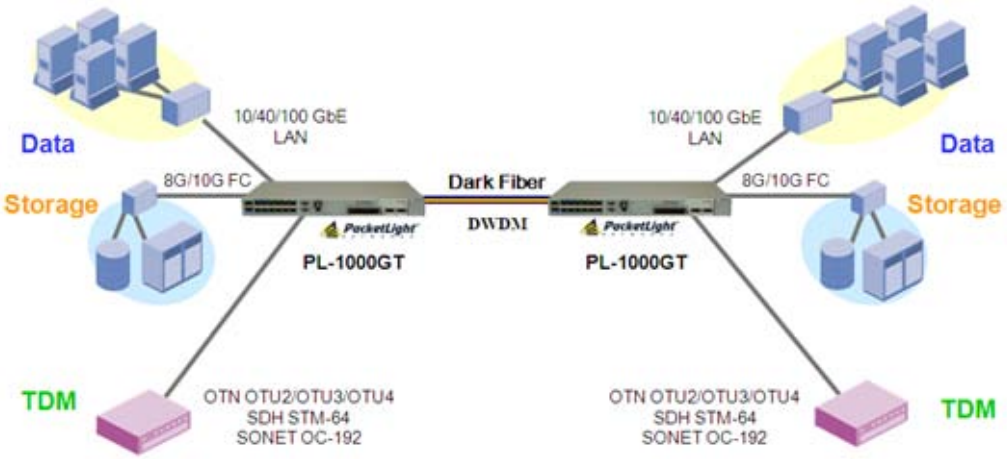


Figure 1: Typical Application for PL-1000GT Devices

1.1.3 Physical Description

The PL-1000GT is a compact unit intended for installation in a 19-inch or 23-inch rack or placed on a desktop or shelf.

The PL-1000GT unit is a 19-inch/1U ETSI compliant unit with dual DC power supplies and a pluggable FAN unit.

Figure 2: PL-1000GT Unit

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

The following figure shows the front panel of the PL-1000GT.

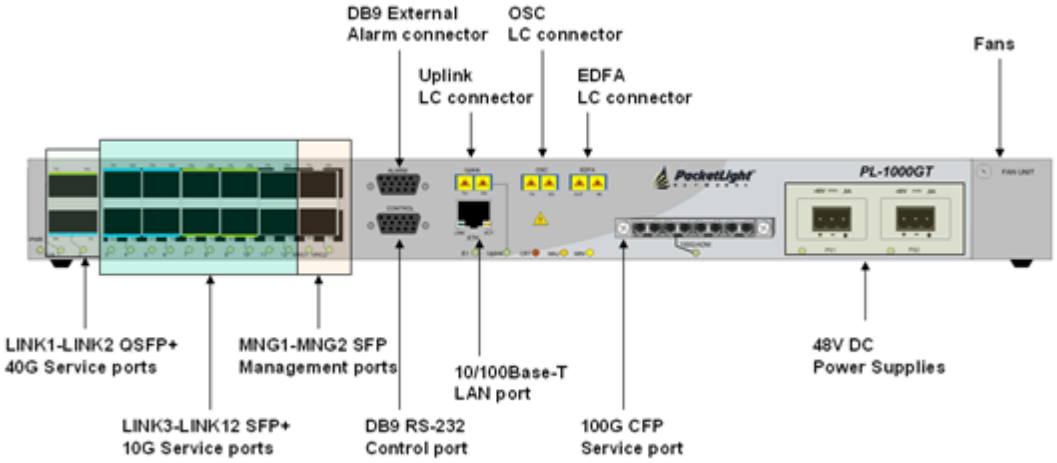


Figure 3: PL-1000GT Front Panel

1.2 Configurations

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

1.2.1 PL-1000GT Configurations

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

1.2.1.1 EDFA Module Configurations

The PL-1000GT can be ordered with one or no EDFA modules. The EDFA can be a Booster or Pre-Amp.

1.2.2 Example Configurations

The following are some examples of the available configurations of the PL-1000GT.

1. PL-1000GT with a 100G transponder:
   - Transponder mode
   - Service side with DWDM CFP
   - Pre-Amp EDFA module

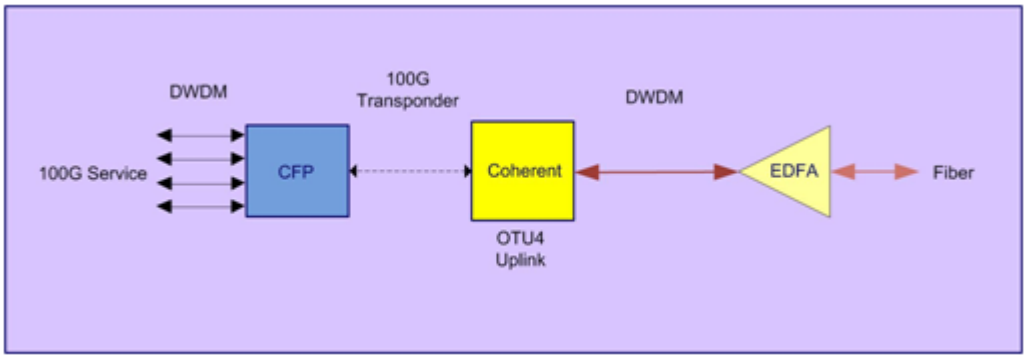


Figure 4: PL-1000GT 100G Transponder with Pre-Amp EDFA

2. PL-1000GT with 10 x 10G services:
   - Muxponder mode

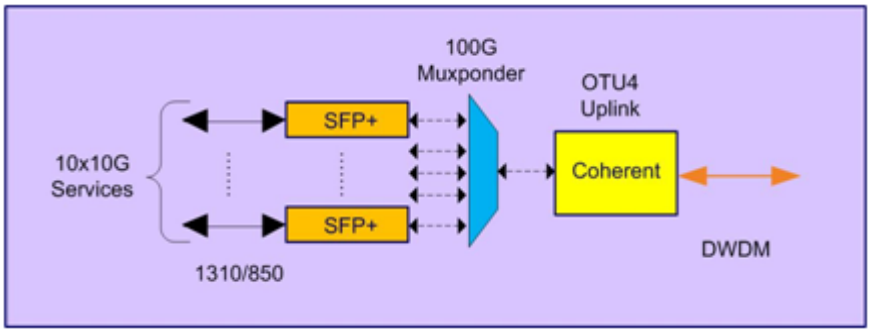


Figure 5: PL-1000GT Muxponder 10 x 10G Services

3. PL-1000GT with 2 x 40G services and 2 x 10G services:
   - Muxponder mode
   - Booster EDFA module

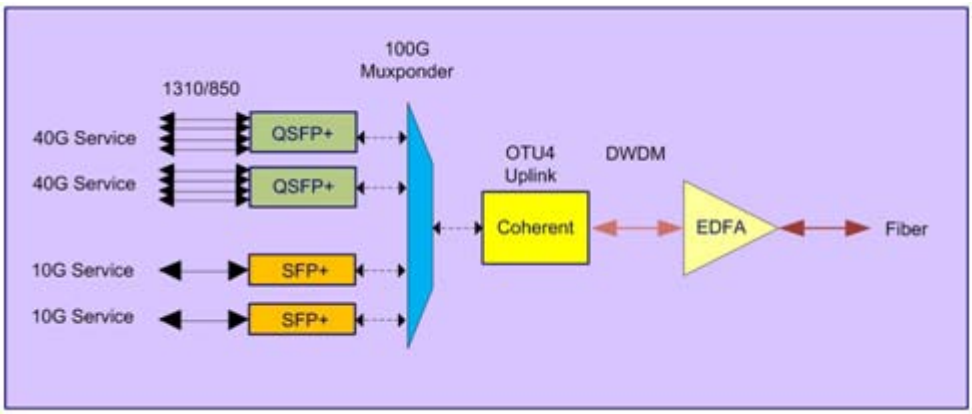


Figure 6: PL-1000GT Muxponder 2 x 40G and 2 x 10G Services with Booster EDFA

4. PL-1000GT with 1 x 40G and 6 x 10G services:
   - Muxponder mode

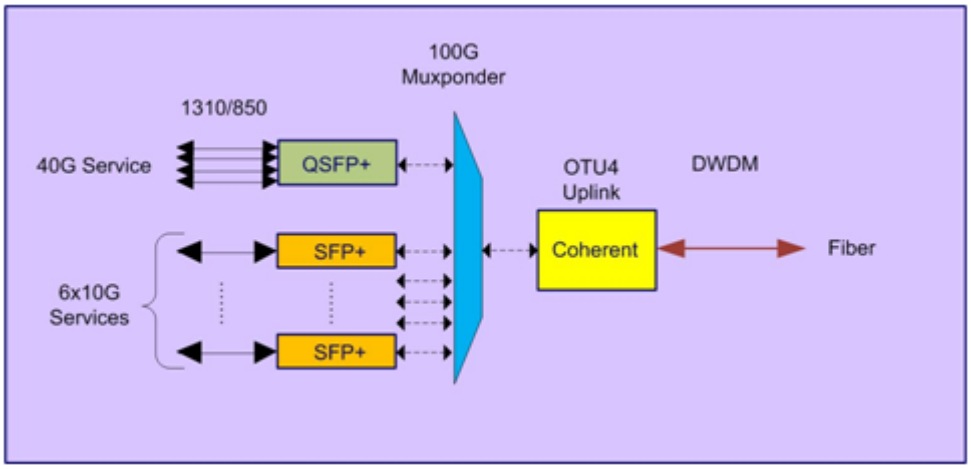


Figure 7: PL-1000GT Muxponder 1 x 40G and 6 x 10G Services

1.3 PL-1000GT Ports

This section describes the PL-1000GT ports.

1.3.1 PL-1000GT Data Ports

This section describes the PL-1000GT data ports.

1.3.1.1 Uplink Port

The PL-1000GT has a single uplink port labeled "Uplink". The uplink port is installed with a Coherent transceiver that supports the OTN OTU4 as defined by ITU-T G.709.

An in-band management channel embedded in the uplink OTU4 signal provides an alternative remote management that can save the additional wavelength required for the OSC.

1.3.1.2 Transponder Service Port

In Transponder mode, the PL-1000GT maps a single 100G service into the OTU4 uplink. The Transponder service port is labeled “100G/ADM” and it accepts a CFP transceiver.

1.3.1.2.1 100G Service

In Transponder mode, the 100G/ADM can be connected to a 100G client signal according to the following table.

Table 1: PL-1000GT 100G Service Types

Service Type	Line Bit Rate	Standard
100GbE	103.125 Gb/s	IEEE 802.3ba
OTU4 (future versions)	111.81 Gb/s	ITU-T G.709

1.3.1.3 Muxponder Service Ports

In Muxponder mode, the PL-1000GT multiplexes several 10G/40G client signals attached to the LINK 1 to LINK 12 ports and maps them into the OTU4 uplink.

The PL-1000GT Muxponder service ports are labeled "LINK 1" to "LINK 12".

- LINK 1 and LINK 2 are 40G ports that accept QSFP+ transceivers.
- LINK 3 to LINK 12 are 8G/10G ports that accept SFP+ transceivers.

1.3.1.3.1 Muxponder Service Ports Availability

There are several Muxponder configurations. In each configuration, a different set of service ports is available.

The following table describes the availability of the Muxponder service ports for each Muxponder configuration.

Table 2: PL-1000GT Muxponder Configurations

Muxponder Configuration	Number of Ports	Available Ports
No 40G Ports	10 x 10G	LINK 3 to LINK 12
Single 40G Port (Upper)	• 1 x 40G • 6 x 10G	• **LINK 1** • LINK 7 to LINK 12
Dual 40G Ports	• 2 x 40G • 2 x 10G	• **LINK 1** and **LINK 2** • LINK 11 and LINK 12

1.3.1.3.2 40G Services

According to the Muxponder configurations listed in Muxponder Service Ports Availability (p. 8), when available, LINK 1 and LINK 2 ports can be independently configured with different 40G service types according to the following table.

Table 3: PL-1000GT 40G Service Types

Service Type	Line Bit Rate	Standard
40GbE	41.256 Gb/s	IEEE 802.3ba
OC-768/STM-256 (future versions)	39.813 Gb/s	Telcordia GR-253-CORE, ITU-T G.707
OTU3 (future versions)	43.018 Gb/s	ITU-T G.709

1.3.1.3.3 8G/10G Services

According to the Muxponder configurations listed in Muxponder Service Ports Availability (p. 8), LINK 3 to LINK 12 ports can be independently configured with different 8G/10G service types according to the following table.

Table 4: PL-1000GT 8G/10G Service Types

Service Type	Line Bit Rate	Standard
8G FC (FC-800)	8.5 Gb/s	T11 Technical Committee of INCITS
OC-192/STM-64	9.95328 Gb/s	Telcordia GR-253-CORE, ITU-T G.707
10GbE-LAN	10.3125 Gb/s	IEEE 802.3
OTU2	10.709 Gb/s	ITU-T G.709
OTU2e	11.0957 Gb/s	ITU-T G.709
10G FC (FC-1200) (future versions)	10.51875 Gb/s	T11 Technical Committee of INCITS

1.3.1.4 OSC Port

The optional OSC port allows one of the MNG ports to be connected to the line. The OSC channel is muxed/demuxed to/from the common signal to provide remote out-of-band management.

1.3.1.5 EDFA Port

The optional EDFA port is a dual LC connector with "IN/OUT" labels. When a Booster EDFA is installed, you should connect the Tx fiber of the uplink to this port. When a Pre-Amp EDFA is installed, you should connect this port to the Rx of the uplink port.

1.3.2 PL-1000GT Management Ports

This section describes the PL-1000GT management ports.

1.3.2.1 CONTROL Port

The RS-232 asynchronous supervisory port has a DCE interface that supports a data rate of 9600 bps.

Initial configuration of the PL-1000GT 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-1000GT serial CONTROL connector.

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

For more information, see Connection Data (p. 233).

1.3.2.2 ETH Port

The PL-1000GT can be accessed through the Ethernet 10/100 Base-T LAN port for local management.

For more information, see Connection Data (p. 233).

1.3.2.3 MNG Ports

The PL-1000GT is equipped with two 100/1000 Base-X MNG ports labeled "MNG 1" and "MNG 2". These ports enable remote management and/or local multi-chassis management of a PL-1000GT.

When used for remote management, the management channels are optically multiplexed with the uplink channel as an extra OSC wavelength by the external optical MUX/DEMUX.

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

1.3.2.4 ALARM Port

The PL-1000GT 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. 233).

1.4 PL-1000GT Modules

This section describes some of the PL-1000GT modules.

1.4.1 EDFA Module

The PL-1000GT can be ordered with an optional EDFA module that is used to amplify the optical power of the DWDM signal. The EDFA module can be used as a Booster and/or Pre-Amp. It can be connected externally to the front panel LC adapter.

- **Booster EDFA**: It is used on the Tx optical path.
- **Pre-Amp EDFA**: It is used on the Rx optical path.

1.4.2 Power Supply Units

The PL-1000GT has two redundant DC power supplies: -48 VDC, 8A maximum.

The maximum power consumption of the PL-1000GT is 250W.

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

1.4.3 FAN Unit

The PL-1000GT 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.

1.5 Management Functionality

The PL-1000GT 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 port loopback, software upgrade, and system restart
- Viewing the network topology

1.5.1 Management Protocols

This section describes the main management protocols supported by PL-1000GT.

1.5.1.1 CLI Management

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

For more information, see CLI (p. 217).

1.5.1.2 Web-based Management

The PL-1000GT supervision and configuration functions can be performed using a standard Web browser. The Web management can be used with HTTP or HTTPS (Secured HTTP).

For detailed information on Web-based management, see Configuration Management (p. 101).

1.5.1.3 SNMP Management

PL-1000GT 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-1000GT MIBs and LightWatch™, contact PacketLight Technical Support.

1.6 Technical Specifications

Uplink Port	Transceiver	Coherent
	Wavelength	• Tunable channel • DWDM ITU-T G.694.1 Grid Channels 15 to 60 C-Band with 50/100 GHz spacing
	Optical Reach	2,000 km
	Bit Rate	127.157 GHz (OTU4v with SD FEC)
	Connector	Fixed duplex LC connector
	In-band Management	IP connection for management traffic
Service Ports	Number of Ports	13 (1 x 100G, 2 x 40G, 10 x 10G)
	Service Types	• **100G Transponder service**: ▪ 100GbE-LAN ▪ OTU4 (future versions) • **40G Muxponder services**: ▪ 40GbE-LAN ▪ OTU3 (future versions) ▪ OC-768 (future versions) ▪ STM-256 (future versions) • **10G Muxponder services**: ▪ 10GbE-LAN ▪ 8G FC (FC-800) ▪ OC-192 ▪ STM-64 ▪ OTU2 ▪ OTU2e ▪ 10G FC (FC-1200) (future versions)
	Connectors	• **100G**: CFP transceiver • **40G**: QSFP+ transceiver • **10G**: SFP+ transceiver
Optical Amplifier (EDFA)	Number of Modules	0 or 1
	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

	Automatic Gain Control (AGC)	Keeps the amplifier gain fixed without dependency when adding or removing services.
	Automatic Power Control (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.
Supervisory and Management Ports	CONTROL Port	Used for initial configuration of the node IP or for local access to CLI. • **Interface**: RS-232 • **Connector**: DB-9, 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	2 Optical management ports • **Interface**: 100/1000 Base-X • **Connector**: SFP transceiver • **Wavelength**: ▪ **CWDM**: 1290 nm or 1310 nm single mode ▪ **DWDM:** 1490 nm or 1510 nm single mode ▪ **Non-WDM**: 850 nm multi-mode or 1310 single mode **NOTE:** IP of the MNG port can be configured using the Web application.
Environment Alarms	ALARM Port	Used for external office alarms. • **Connector**: DB-9, female • **Environmental**: 1 input and 1 output
System LEDs	PWR CRT	• **Green blinking**: Power-up stage • **Green**: Normal operation • **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

Uplink Port LED	Uplink	• **OFF**: Admin Down • **Blinking**: Facility loopback or PRBS test • **Green**: Normal operation • **Red**: Alarm detected
Service Port LEDs	LINK 1 to LINK 12, 100G/ADM	• **OFF**: Admin Down • **Blinking**: Facility loopback or PRBS test • **Green**: Normal operation • **Red**: Alarm detected
MNG Port LEDs	MNG 1 and MNG 2	• **OFF**: Admin Down • **Green**: Normal operation • **Red**: Alarm detected
Amplifier LED	E1	• **OFF**: Admin Down or no EDFA module installed • **Green**: The amplifier module is operational • **Red**: Failure detected on the amplifier module
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	• **OFF**: PSU is not installed • **Green**: Normal operation • **Red**: PSU failure detected
Network Management	Protocols	• CLI over RS-232 or Telnet/SSH • Web-based HTTP/HTTPS management • SNMPv2c • Radius • Syslog • SNTP • TFTP and FTP for file transfer • RSTP
	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-1000GT system log files, which can be exported to a text file for offline viewing.

	Performance Monitoring	PM counters for 15 minute and one day intervals: • **Counters for the uplink based on OTU4/ODU4 BIP8 errors and OTN FEC corrected/uncorrected errors:** CV, ES, SES and UAS • **Ratio for the uplink based on OTN FEC corrected errors**: The Bit Error Ratio of the corrected FEC errors. • **Counters for 10GbE-LAN, 40GbE-LAN, and 100GbE-LAN services based on 64B/66B coding violations**: CV, ES, SES, and UAS • **Counters for 8G FC services based on 8B/10B coding violations**: CV, ES, SES and UAS • **Counters for OC-192 (SONET) services based on B1 coding violations**: CV, ES, SES and SEF • **Counters for STM-64 (SDH) services based on B1 coding violations**: CV, ES, SES and OOF • **Counters for OTU2 and OTU2e services based on OTU BIP8 errors and FEC corrected/uncorrected errors**: CV, ES, SES and UAS
	Optical PM	PM counters for 15 minute and one day intervals for the optical Rx Power for the transceivers and other optical modules installed in the system.
Diagnostics	Loopback	Facility loopback is supported for the uplink and service ports.
	PRBS	PRBS generation and statistics are available for the for the uplink and service ports.
ALS	Optical Ports	ALS is available for all optical ports.
Power Supply	Number of Units	2
	Redundancy	Dual feeding
	DC Source	–48 VDC, 8A maximum
	Power Consumption	250W 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" (1 RU)
	Width	440 mm/17.32"
	Depth	230 mm/9.05"
	Weight	8.0 kg/17.6 lbs maximum
	Mounting Options	19", 23", ETSI rack mountable
Environment	Operating Temperature	0° to +45°C/+32° to +113°F
	Storage Temperature	-25° to +55°C/-13° to +131°F
	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 • Industry Canada ICES-003:04; C108.8-M1983 • VCCI Technical Requirements, V-3/2001.04
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-1000GT.

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-1000GT. Never connect cables to a PL-1000GT unit if it is not properly installed and grounded.

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-1000GT 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-1000GT must be connected to a protective ground (see Connection Data (p. 233)).

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-1000GT 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-1000GT optical modules is off when the status of the port is set to **Admin Down**.

In general, the PL-1000GT unit is equipped with laser devices that comply with Class 1M.

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

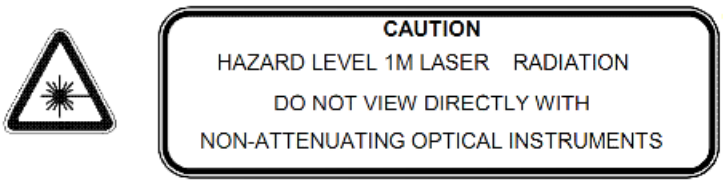


Figure 8: Class 1M Laser Warning

PL-1000GT 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-1000GT 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-1000GT unit or performing any internal settings on the PL-1000GT, 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-1000GT site requirements.

2.2.1 Physical Requirements

The PL-1000GT 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

DC-powered PL-1000GT units require a -48 VDC, 8A 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. 239)).

2.2.3 Ambient Requirements

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

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

2.2.4 Electromagnetic Compatibility Considerations

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

2.3 PL-1000GT Front Panel

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

Figure 9: PL-1000GT Front Panel

The above figure shows the PL-1000GT unit with a WDM CFP and an EDFA amplifier.

In this configuration, the front panel includes the following connectors:

- 100G Coherent uplink port LC connector
- 100G CFP service port
- 2 40G QSFP+ service ports
- 10 10G SFP+ service ports
- OSC port LC connector
- EDFA port LC connector
- 2 MNG ports labeled "MNG1" and "MNG2"
- 10/100 Base-T LAN port labeled "ETH"
- CONTROL port: RS-232 connector
- External alarm port
- 2 48V power connectors
- FAN unit tray

2.3.1 Front Panel LEDs

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

For the list of LEDs and their functions, see Technical Specifications (p. 13).

2.3.2 PL-1000GT Optical Connections Example

The following figure illustrates the connections between the optical ports.

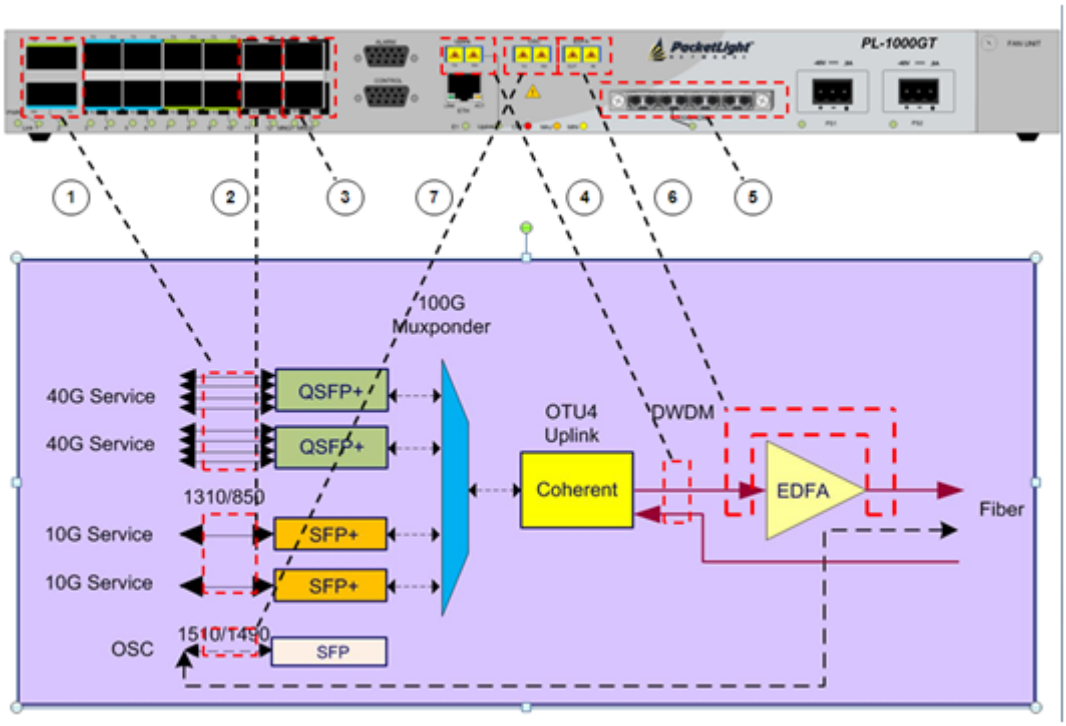


Figure 10: Connections Between the Optical Ports

The following table describes the PL-1000GT optical ports.

Table 5: PL-1000GT Optical Ports

Number	Description
1	QSFP+ connector
2	SFP+ connectors
3	Management SFP connectors
4	Uplink LC connector
5	CFP connector
6	EDFA LC connector
7	OSC LC connector

2.4 Installing the PL-1000GT Unit

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

⚠ **CAUTION:** Before installing a PL-1000GT unit, review the Safety Precautions (p. 19).

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-1000GT (for procedures for using the terminal, see Operation and Preliminary Configuration (p. 29)). The software necessary for using the terminal is stored in the PL-1000GT.

2.4.1 Package Contents

The PL-1000GT package includes the following items:

- PL-1000GT unit
- Ethernet cable
- 3m RS-232 terminal cable
- 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-1000GT depend on the PL-1000GT application. You can use standard cables or prepare the appropriate cables yourself (see Connection Data (p. 233)).

2.4.3 Cable Connections

Before starting, refer to the site installation plan and identify the cables intended for connection to this PL-1000GT unit (see Site Requirements (p. 21) and Connection Data (p. 233)).

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-1000GT 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:

- The PL-1000GT protective ground terminals must be connected to protective ground before power is applied and before connecting any other cable. This connection is made through the 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-1000GT:

- Never connect cables to a PL-1000GT 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-1000GT.
- Disconnect all the cables connected to the connectors of the PL-1000GT before disconnecting the PL-1000GT power cable.

CAUTION: The PL-1000GT 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-1000GT, 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-1000GT may also serve as the ON/OFF switch. This type of circuit breaker should be rated 10A.

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

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

1. Connect one end of the power cable to each PL-1000GT 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-1000GT lights up and starts blinking.

2.4.3.3 Cabling the Uplink Port

To cable the uplink port:

1. Remove the protective plug from the uplink port.
2. Plug the appropriate LC connector into the uplink port.

   Always leave enough slack to prevent strain.

2.4.3.4 Cabling the Service Ports

To cable the service ports:

1. Remove the protective plug from the desired service port and insert an SFP+/QSFP+/CFP transceiver.
2. Connect the port to the appropriate local equipment as follows:
   - Tx connector (transmit fiber) to receive input of the local equipment.
   - Rx connector (receive fiber) to transmit output of the local equipment.

   Always leave enough slack to prevent strain.

2.4.3.5 Cabling the OSC Port

To cable the OSC port:

1. Remove the protective plug from the OSC port.
2. To use the OSC for remote management, connect the OSC port to one of the PL-1000GT MNG ports.

   NOTE: Before connecting, make sure that the SFP in the MNG port has the appropriate wavelength of 1510/1490.

2.4.3.6 Cabling the EDFA Port

To cable the EDFA port:

1. Remove the protective plug from the EDFA port.
2. If a Booster EDFA is installed:
   1. Connect the fiber coming from the Tx of the uplink port to the IN connector of the EDFA port.
   2. Connect the OUT connector of the EDFA port to the output line fiber.

3. If a Pre-Amp EDFA is installed:
    1. Connect the fiber coming from the Rx of the uplink port to the OUT connector of the EDFA port.
    2. Connect the IN connector of the EDFA port to the input line fiber.

2.4.3.7 Cabling the Management Ports

You can cable the following management ports:

- MNG port
- CONTROL port
- ETH port

2.4.3.7.1 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 appropriate LC connectors.

2.4.3.7.2 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-1000GT connectors, see Connection Data (p. 233).

2.4.3.7.3 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-1000GT connectors, see Connection Data (p. 233).

3 Operation and Preliminary Configuration

This chapter provides general operating instructions and preliminary configuration instructions for the PL-1000GT 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-1000GT.

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-1000GT 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-1000GT preliminary configuration (the exact pinout of the connector is described in Connection Data (p. 233)).

2. Check that the installation and the required cable connections have been correctly performed (see Installing the PL-1000GT Unit (p. 24)).

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-1000GT

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

To turn on the PL-1000GT:

1. Connect the PL-1000GT to the power source (see Connecting the PL-1000GT 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-1000GT 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. 233)).

For more information about the CLI commands, see CLI (p. 217).

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-1000GT 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. 227)).

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-1000GT>> 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-1000GT before accessing the Web (see Performing Preliminary Configuration (p. 30)).

3.3.2 Prerequisites for Accessing the Web Application

The following are the prerequisites for accessing the Web application:

- The PL-1000GT is properly installed.
- The PL-1000GT 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. 227)).
2. Open the Web browser.
3. In the address field of the browser, type the **IP address** of the PL-1000GT 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-1000GT)
4. Press **Enter**.

   The Login window opens.

Figure 11: 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.

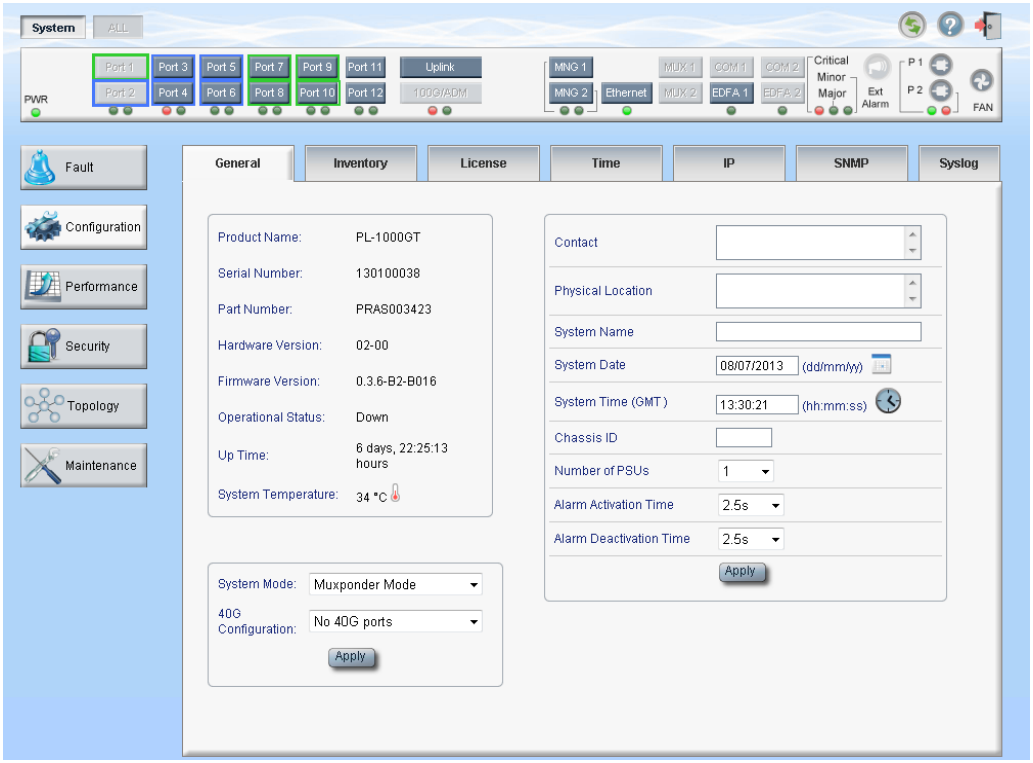


Figure 12: System Configuration Window

3.3.4 Navigating the Web Application

This section describes the PL-1000GT 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.

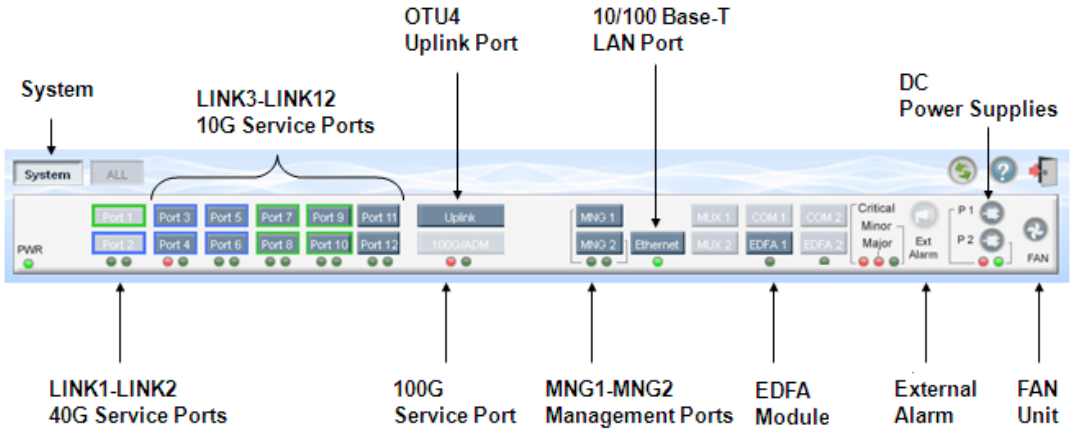


Figure 13: PL-1000GT Item Buttons (Example)

The buttons displayed vary according to the configuration. For example, if the PL-1000GT 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 14: PL-1000GT Sidebar Buttons

Use the sidebar buttons to do the following:

- **Fault**: View PL-1000GT faults
- **Configuration**: Configure the PL-1000GT 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-1000GT

3.3.4.3 Tabs

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

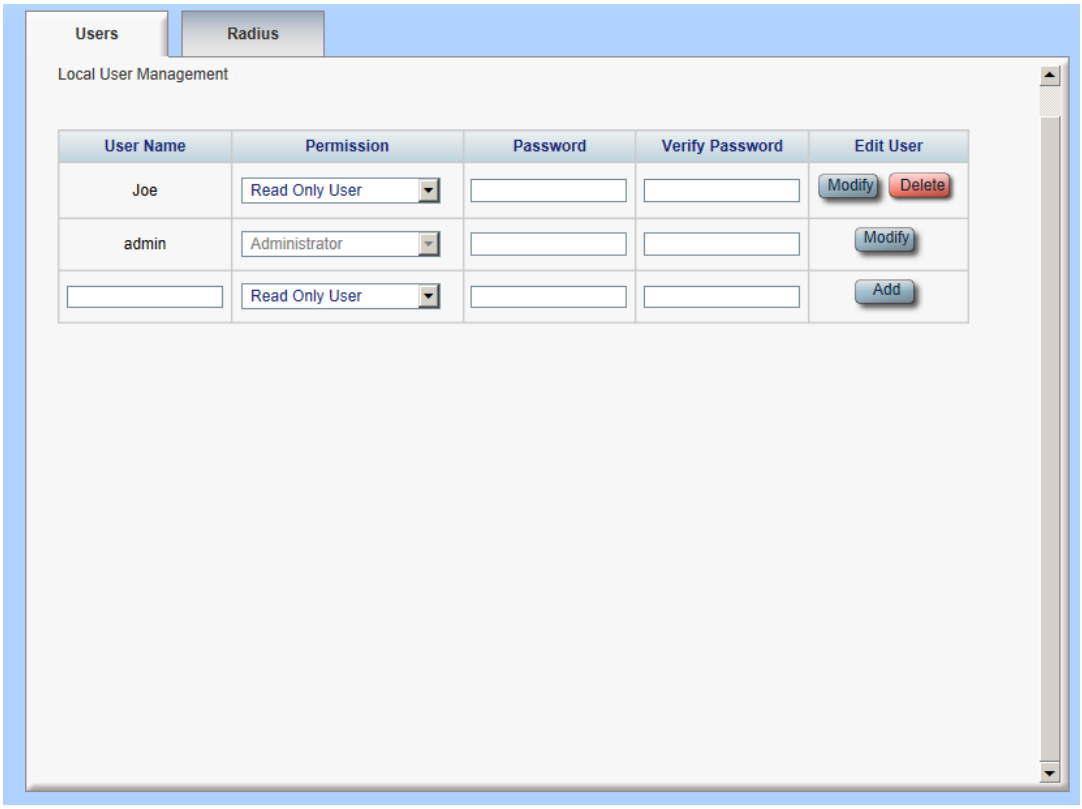


Figure 15: PL-1000GT Tabs (Example)

The tabs displayed vary according to the user permissions. For example, the **Radius** tab is displayed only for a user with Administrator permissions; therefore, in the following figure, the **Radius tab** is not displayed because the user has **Read Only User** permissions.

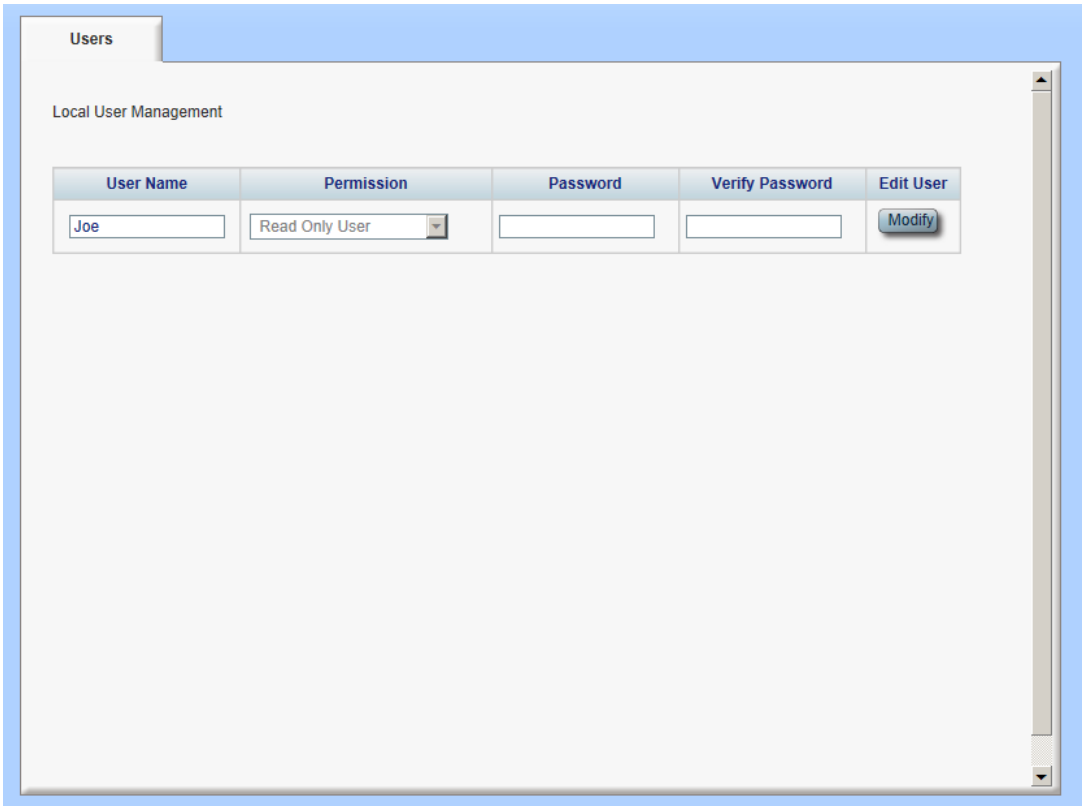


Figure 16: PL-1000GT Users Tab

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-1000GT 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. 44)).	
Read Only User	View only; no edit permissions except to change their own password (see Changing Your Password (p. 44)).	

4.2 User Authentication Methods

The access to the PL-1000GT 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-1000GT 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
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-1000GT 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. 38).

4.3 Security Settings

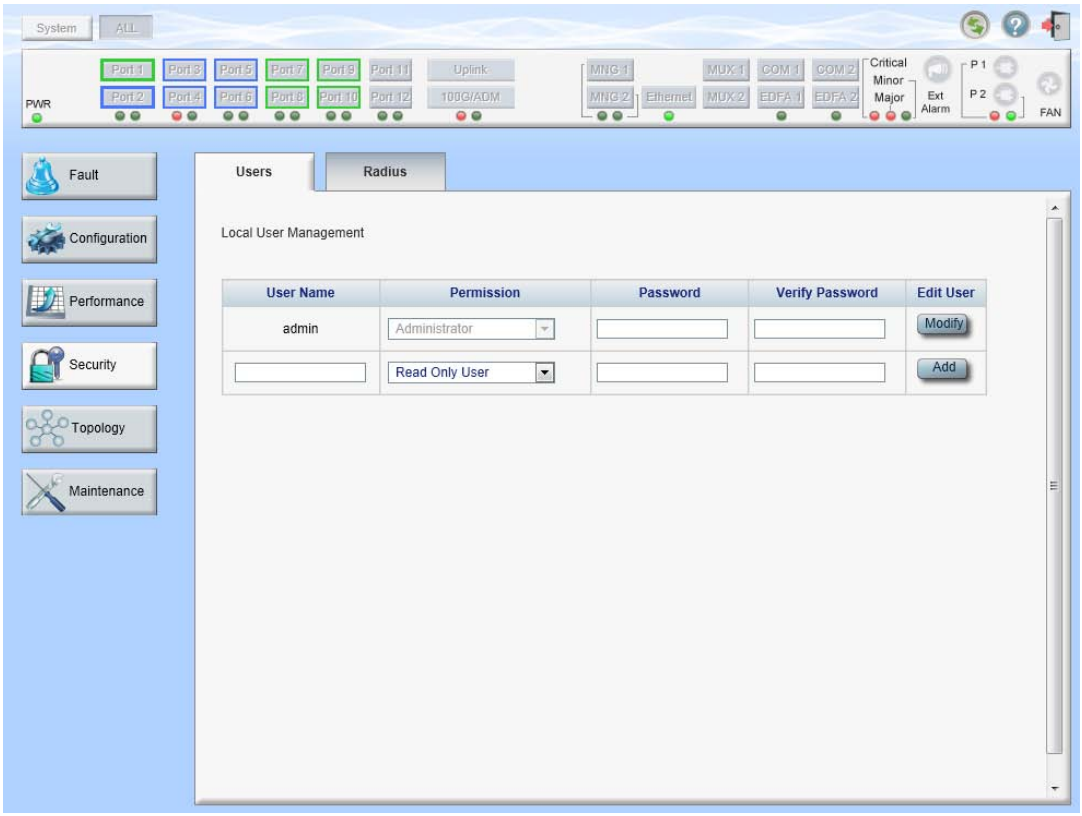


Figure 17: Security Settings Window

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)

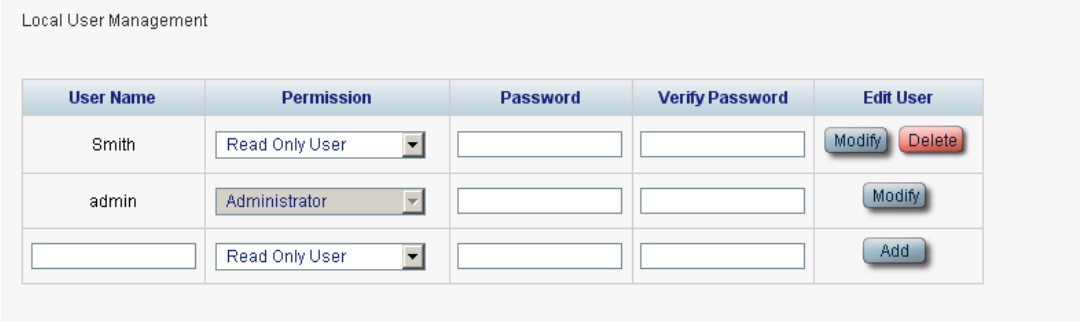


Figure 18: Users Tab (Administrator)

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. 37))
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. 37)).
4. Click **Modify**.

   The following confirmation message appears.

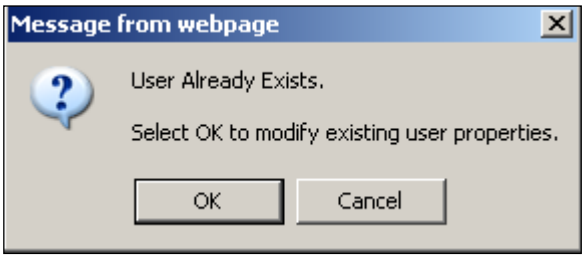


Figure 19: Confirm Changes

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.

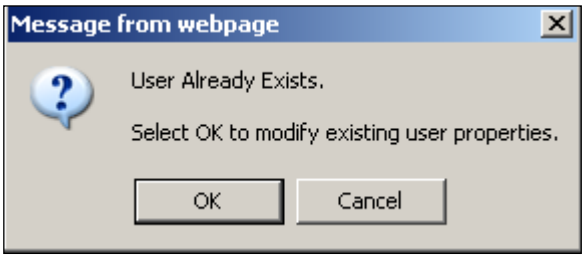


Figure 20: Confirm Changes

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.

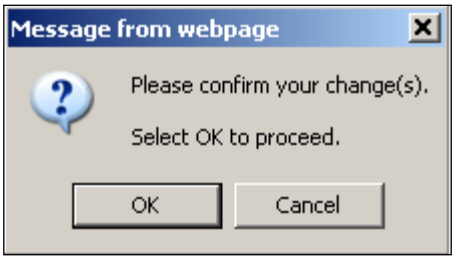


Figure 21: Confirm Delete

4. Click **OK**.

   The specified user is deleted.

4.3.2 Users Tab (Non-Administrator)

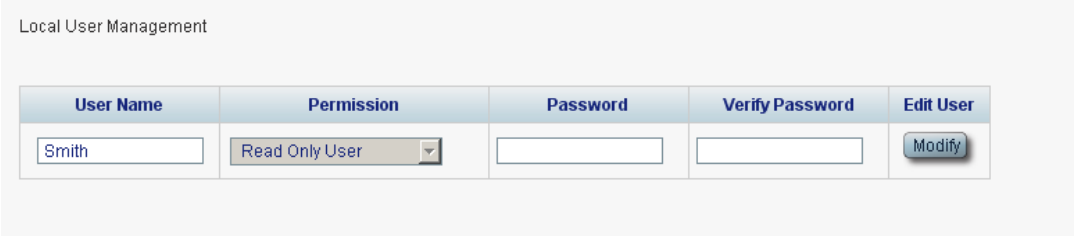


Figure 22: Users Tab (Non-Administrator)

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.

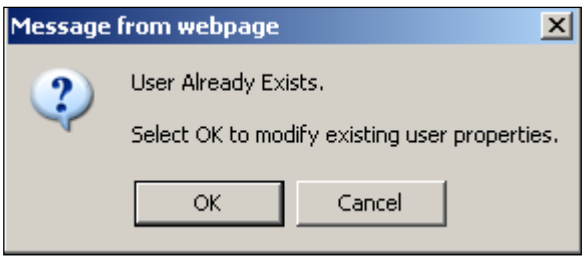


Figure 23: Confirm Changes

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)

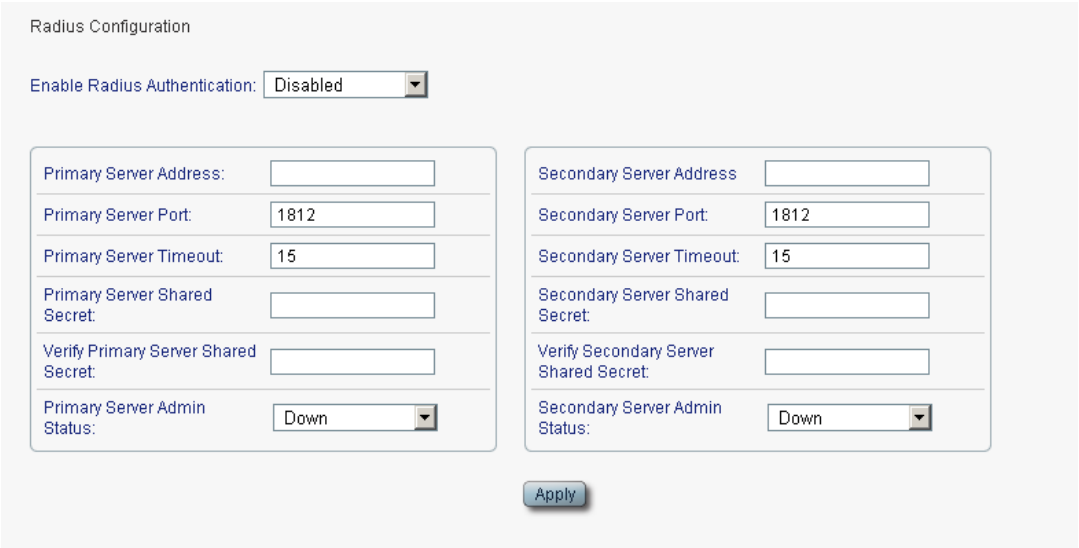


Figure 24: Radius Tab (Administrator)

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.

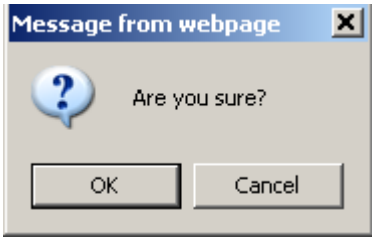


Figure 25: Confirm Configuration

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
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

Parameter	Description	Format / Values
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-1000GT fault management, which is used to localize and identify problems in the network incorporating PL-1000GT 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-1000GT 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-1000GT continuously monitors the traffic signals and other exceptional conditions. Whenever such a condition occurs, the PL-1000GT generates a time stamped event message and sends it as an SNMP notification to the registered management systems. The PL-1000GT 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-1000GT system log files, which can be exported to a text file for offline viewing.

The PL-1000GT 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.
- **Link Up**: These are standard SNMP events that are generated when the operational status of a port is changed from **Down** to **Up**.
- **Link Down**: These are standard SNMP events that are generated when the operational status of a port is changed from **Up** to **Down**.
- **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.
- **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-1000GT 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 Fault Procedure

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

To view the PL-1000GT 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. 52))
   - **All** (see All Faults (p. 58))
   - **Uplink** (see Uplink Port Faults (p. 64))
   - **100G/ADM** (see Service Port Faults (p. 70))
   - **Port** (see Service Port Faults (p. 70))
   - **MNG** (see Management Port Faults (p. 76))
   - **EDFA** (if present) (see EDFA Faults (p. 88))
   - **PSU** (see PSU Faults (p. 94))

   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

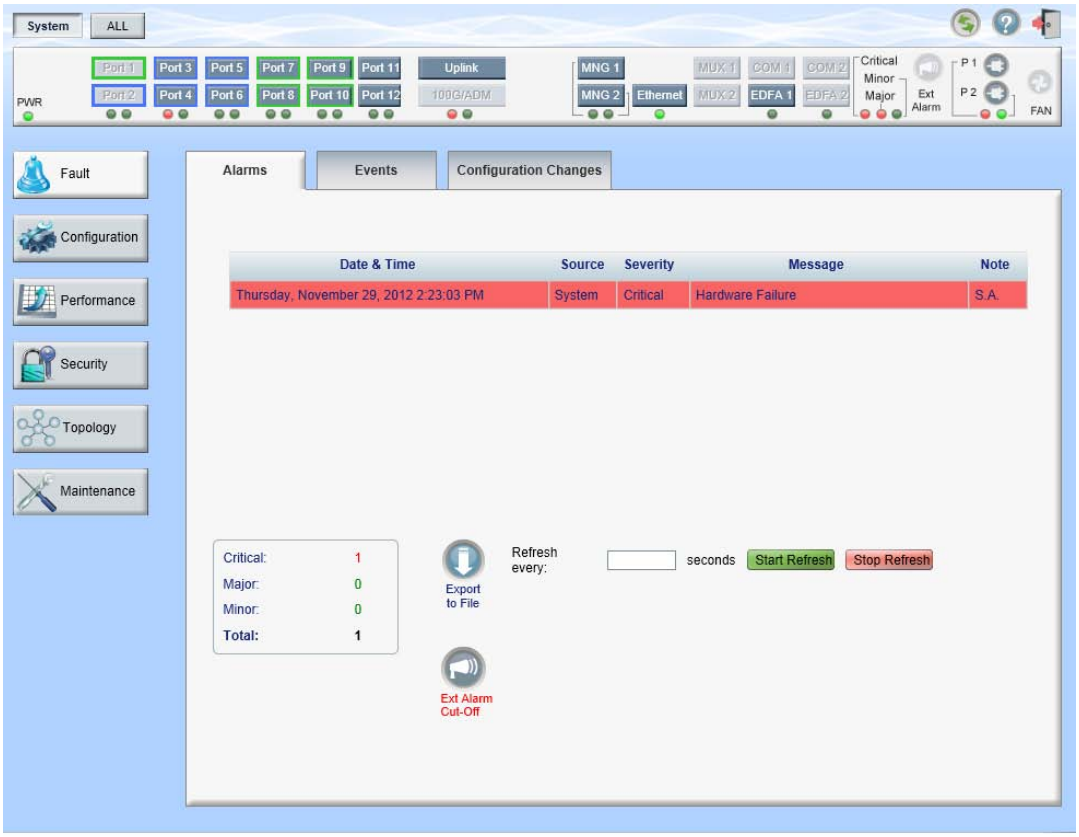


Figure 26: System Fault Window

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

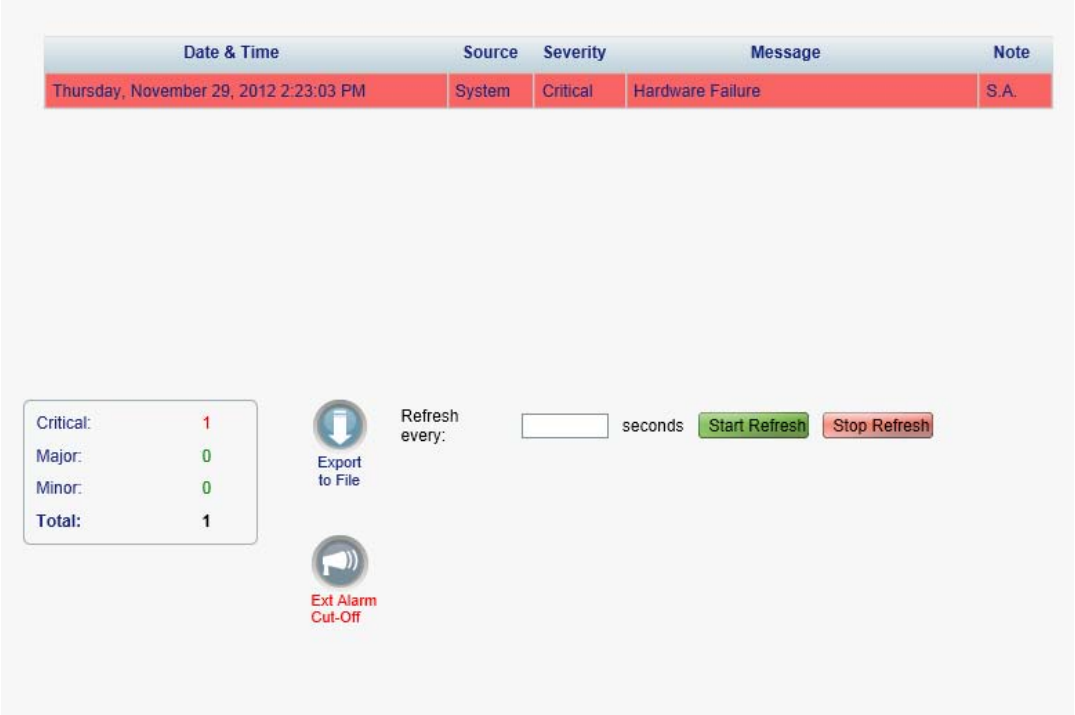


Figure 27: Alarms Tab

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 (p. 13).

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

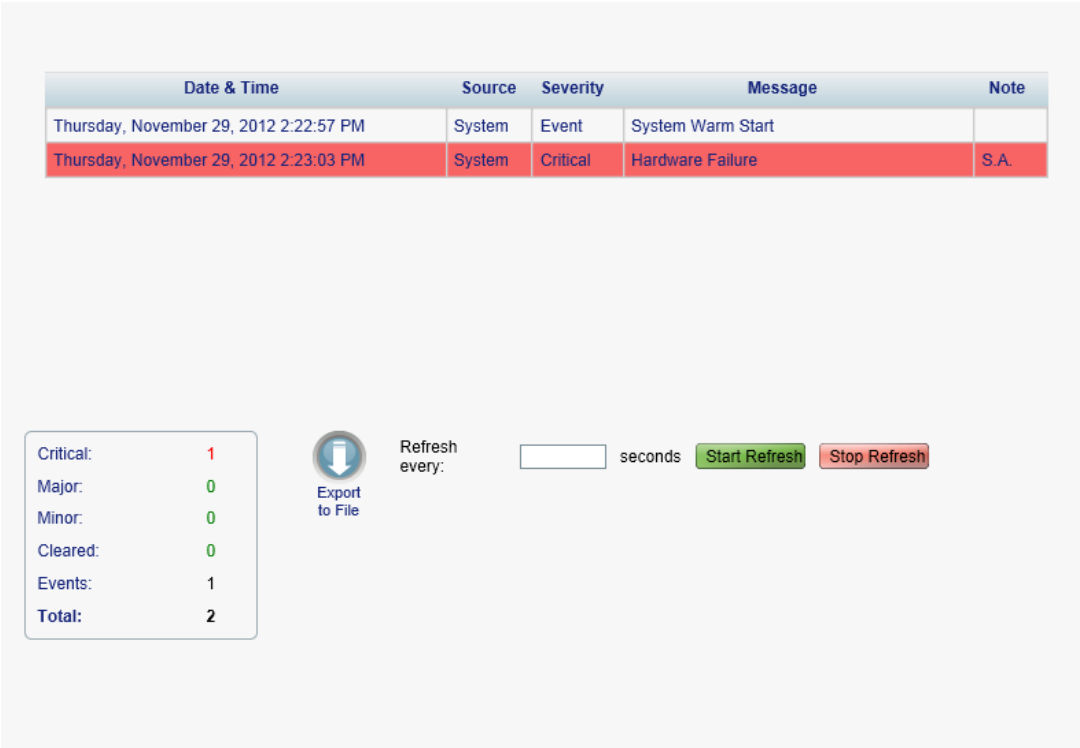


Figure 28: Events Tab

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

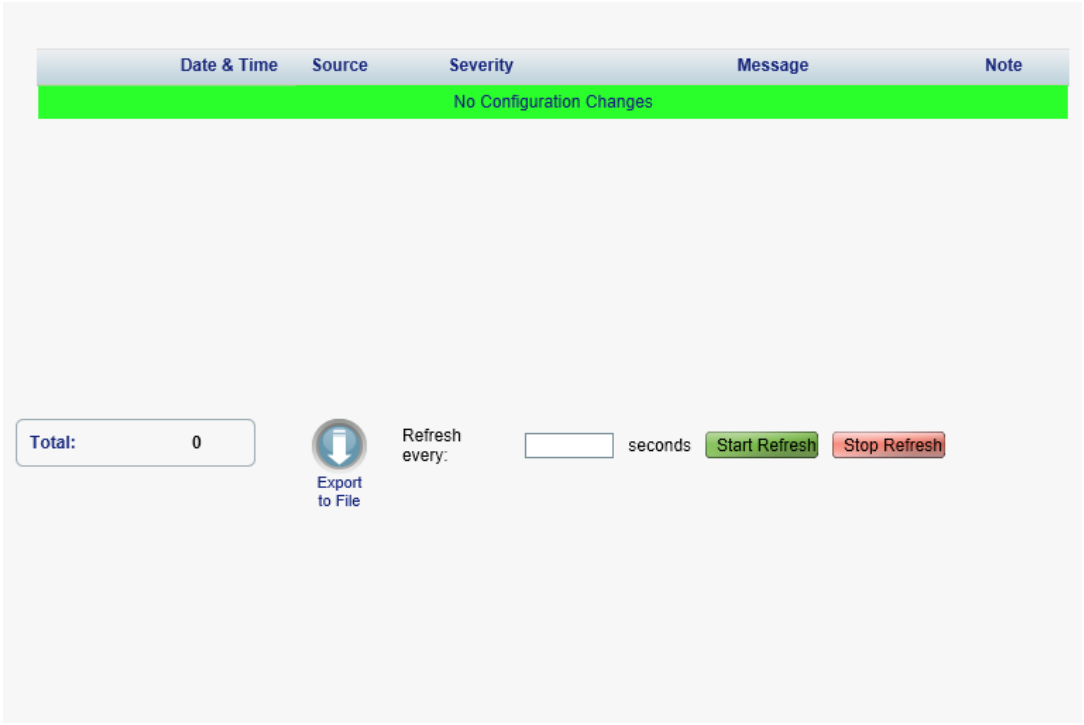


Figure 29: Configuration Changes Tab

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

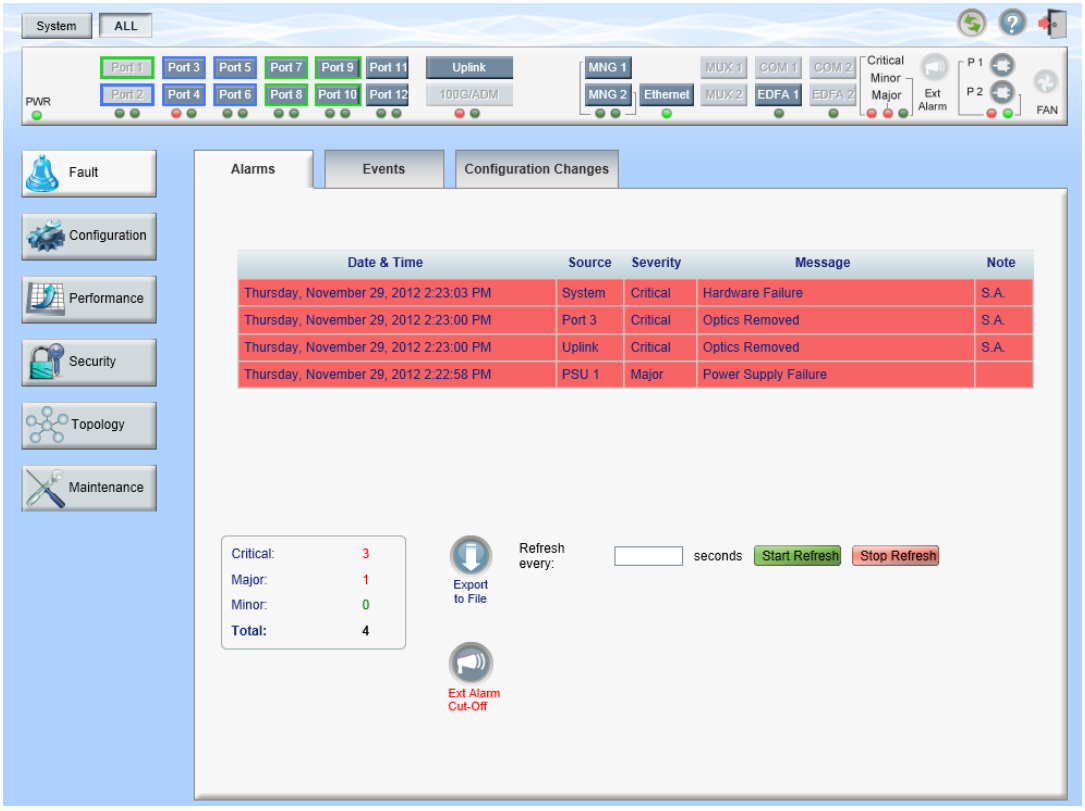


Figure 30: All Fault Window

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

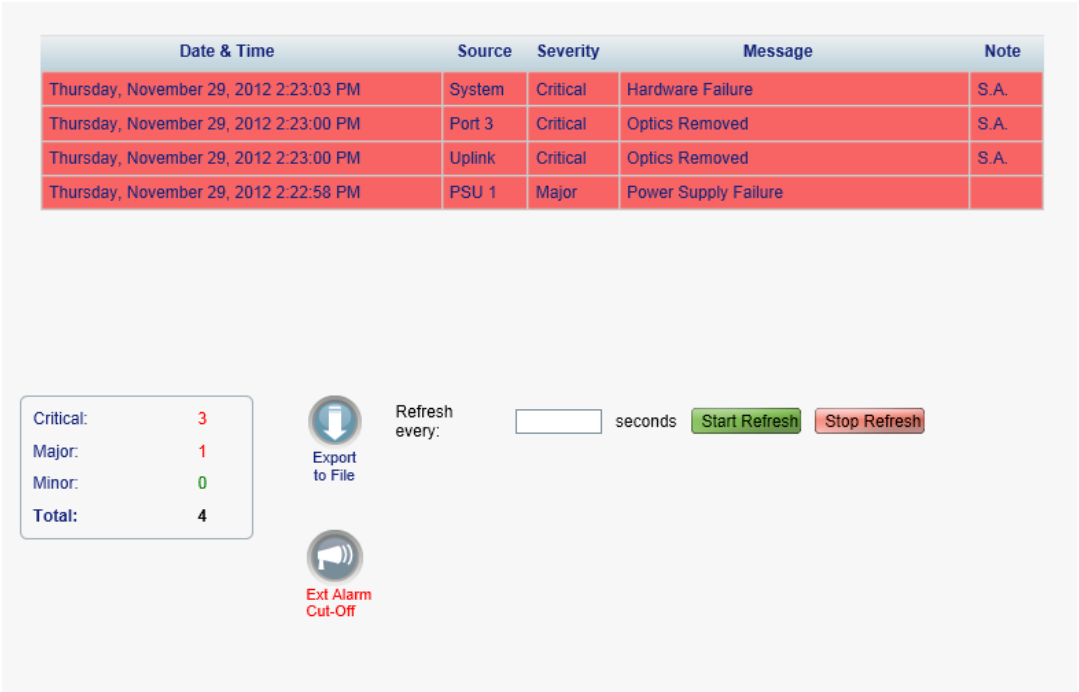


Figure 31: Alarms Tab

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 (p. 13).

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

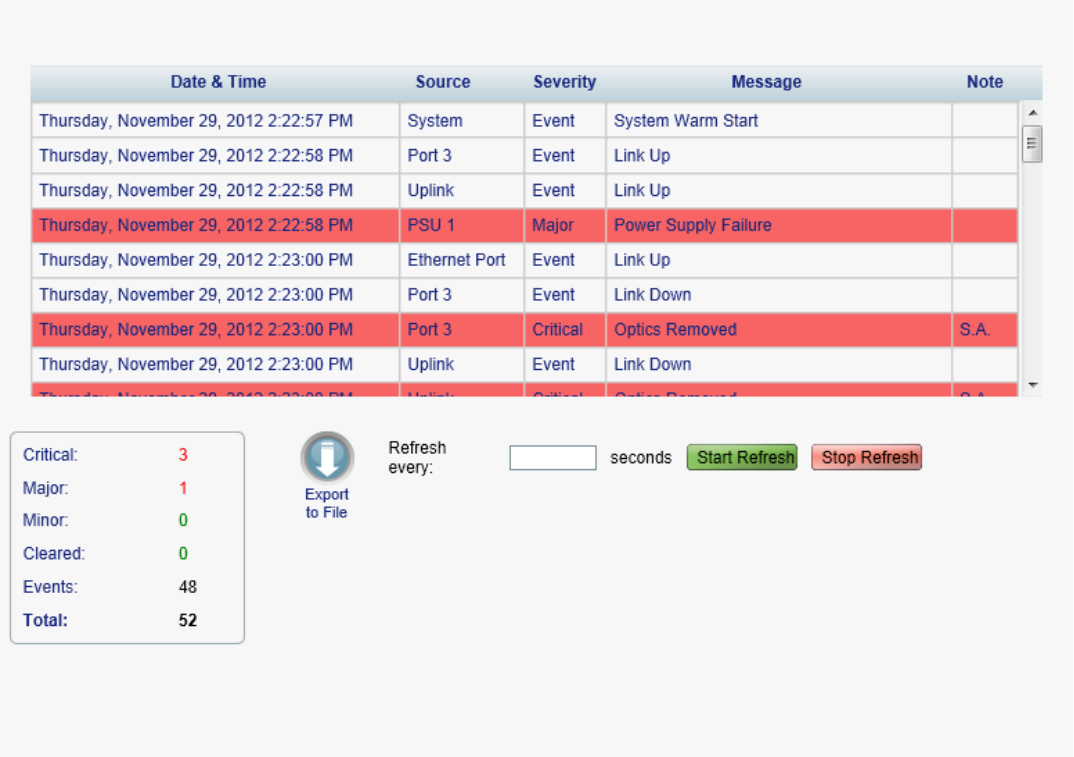


Figure 32: Events Tab

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 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

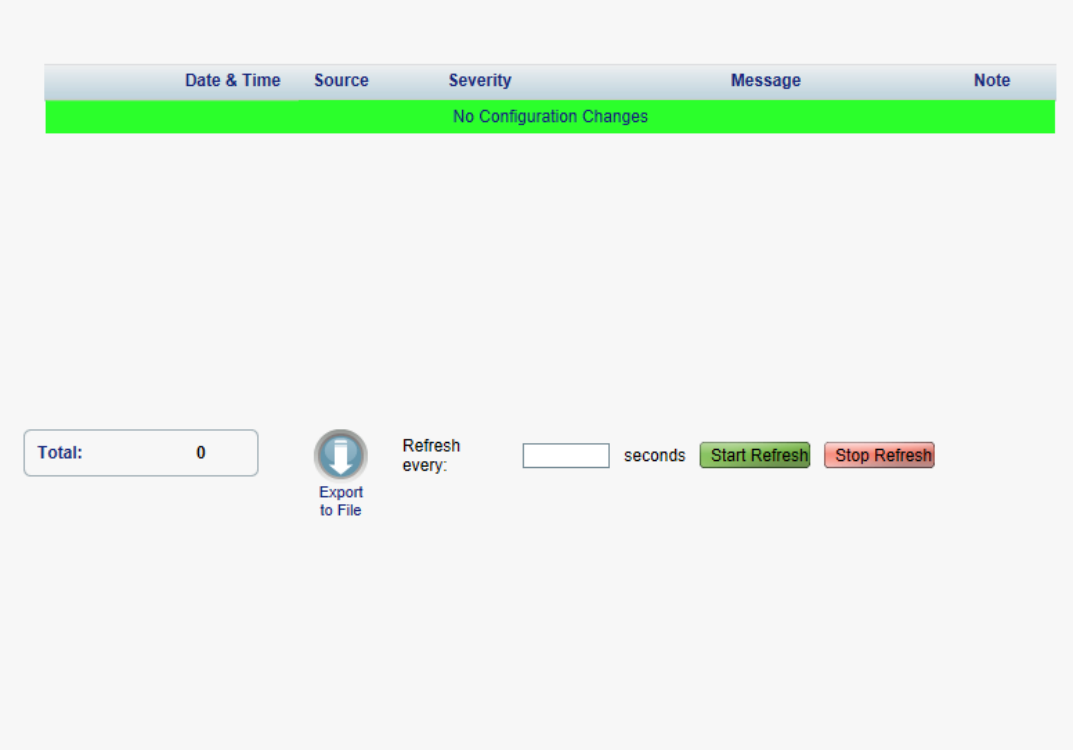


Figure 33: Configuration Changes Tab

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 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 Uplink Port Faults

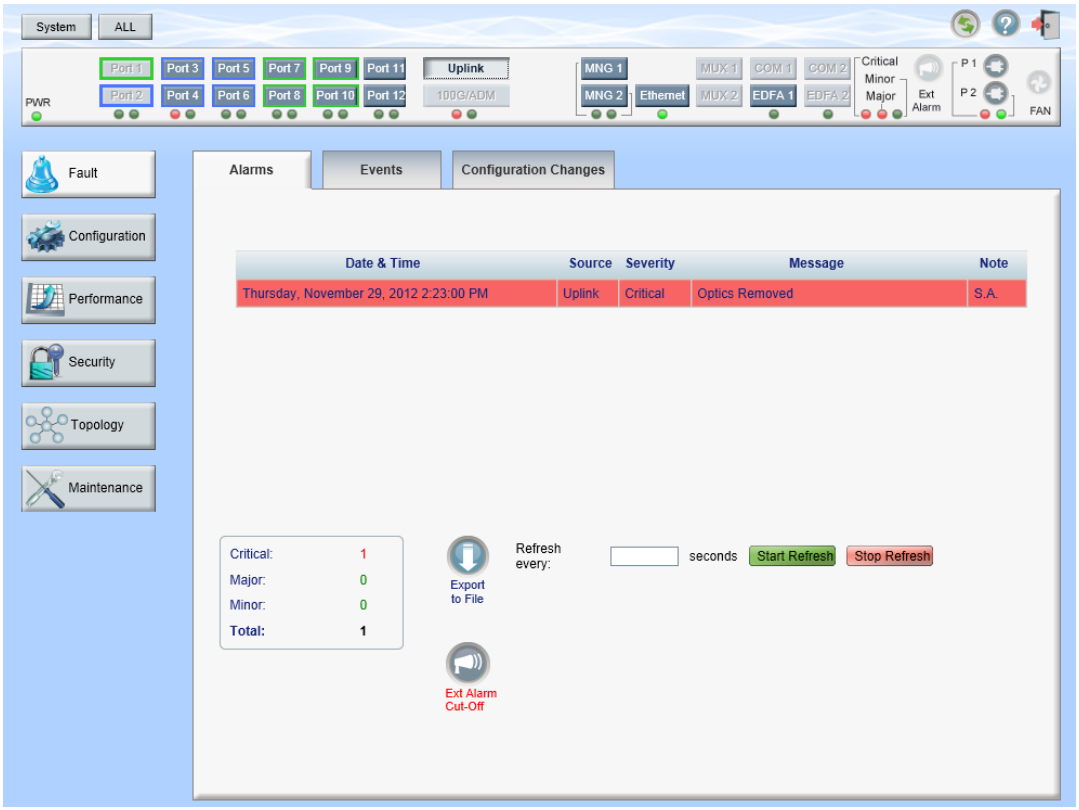


Figure 34: Uplink Port Fault Window

Use the Uplink 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 Uplink Port Fault window:

1. Click **Fault**.
2. Click **Uplink** to select the uplink port.

   The Uplink Port Fault window opens.

5.5.1 Alarms Tab

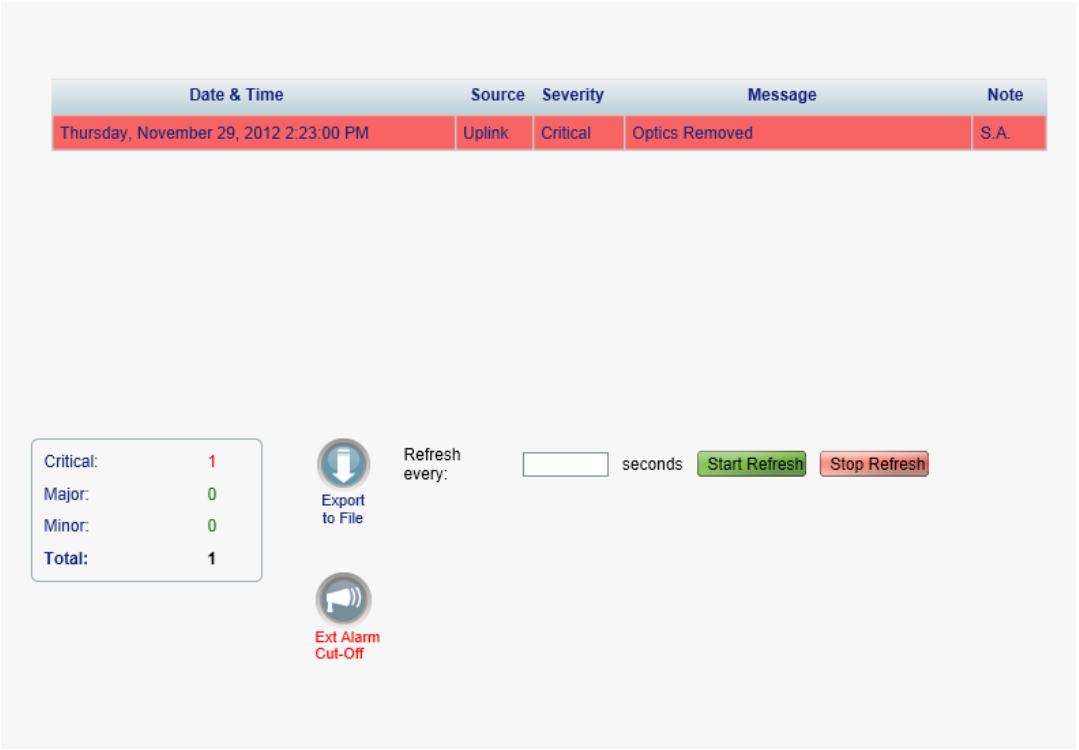


Figure 35: Alarms Tab

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 (p. 13).

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

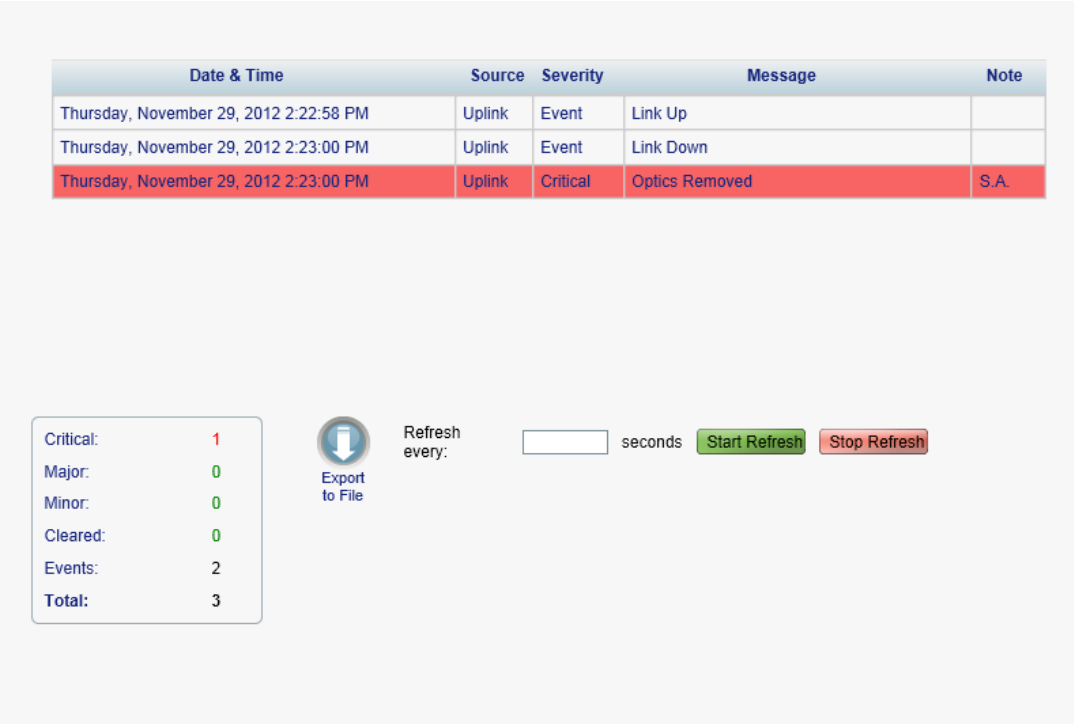


Figure 36: Events Tab

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 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

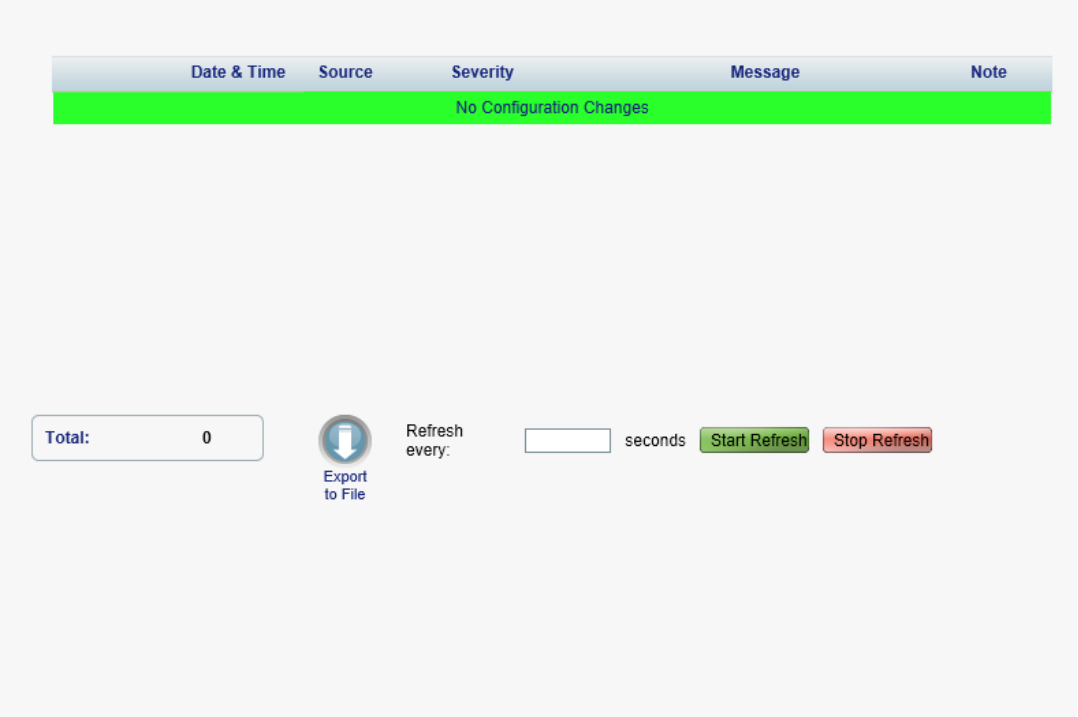


Figure 37: Configuration Changes Tab

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 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 Service Port Faults

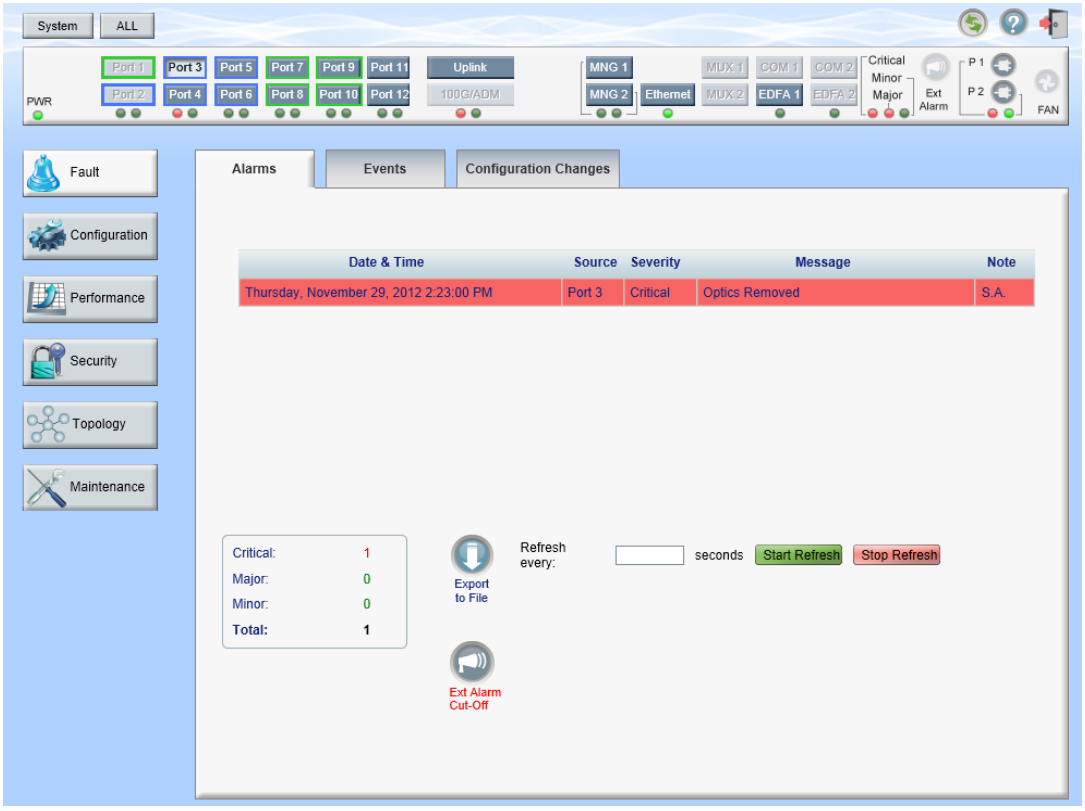


Figure 38: Service Port Fault Window

Use the Service 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 Service Port Fault window:

1. Click **Fault**.
2. Click **100G/ADM** or a **Port** button to select the service port.

   The appropriate Service Port Fault window opens.

5.6.1 Alarms Tab

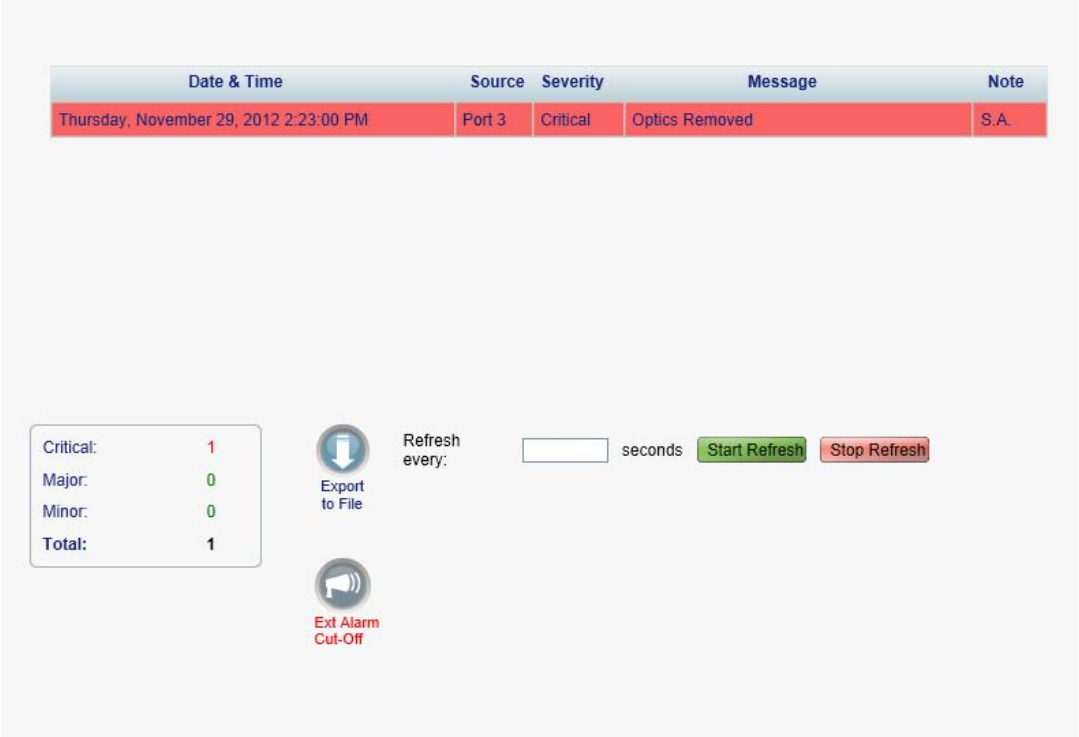


Figure 39: Alarms Tab

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 (p. 13).

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

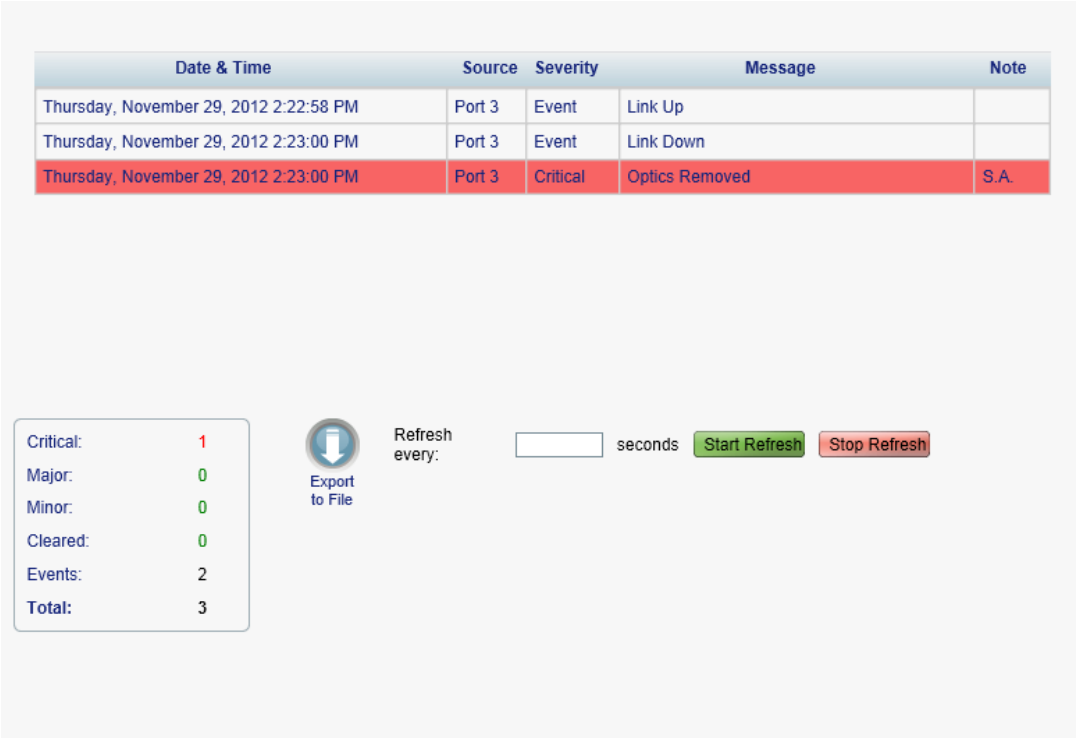


Figure 40: Events Tab

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 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

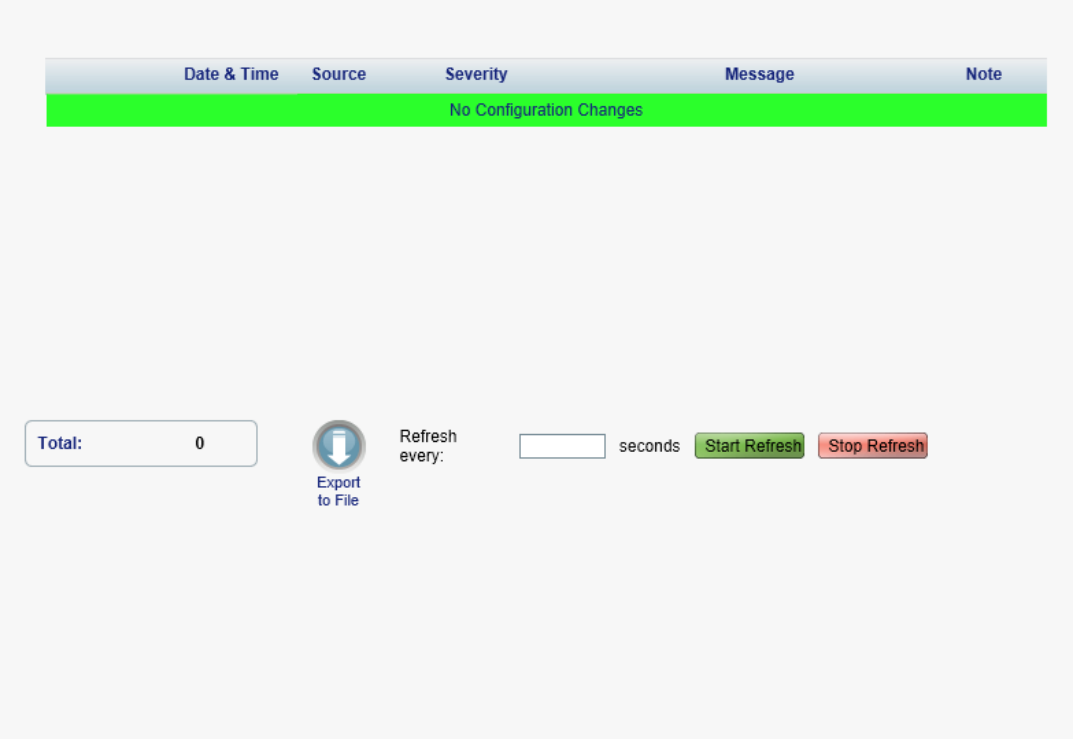


Figure 41: Configuration Changes Tab

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 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 Management Port Faults

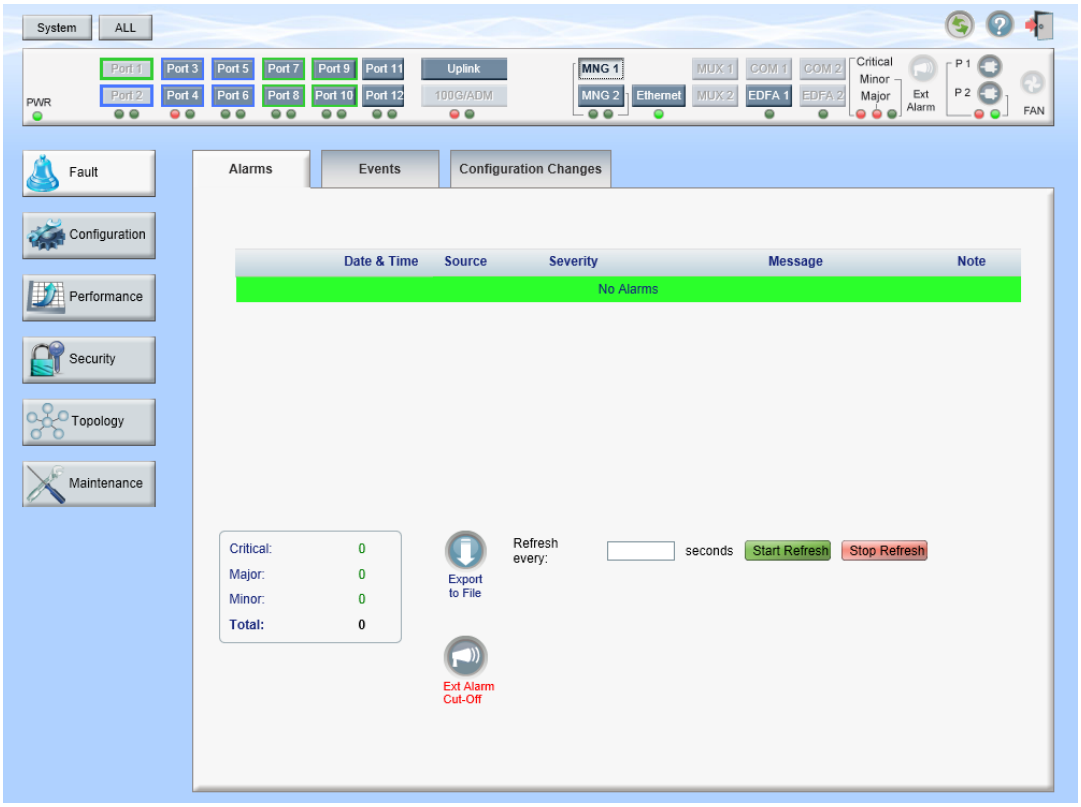


Figure 42: Management Port Fault Window

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.

5.7.1 Alarms Tab

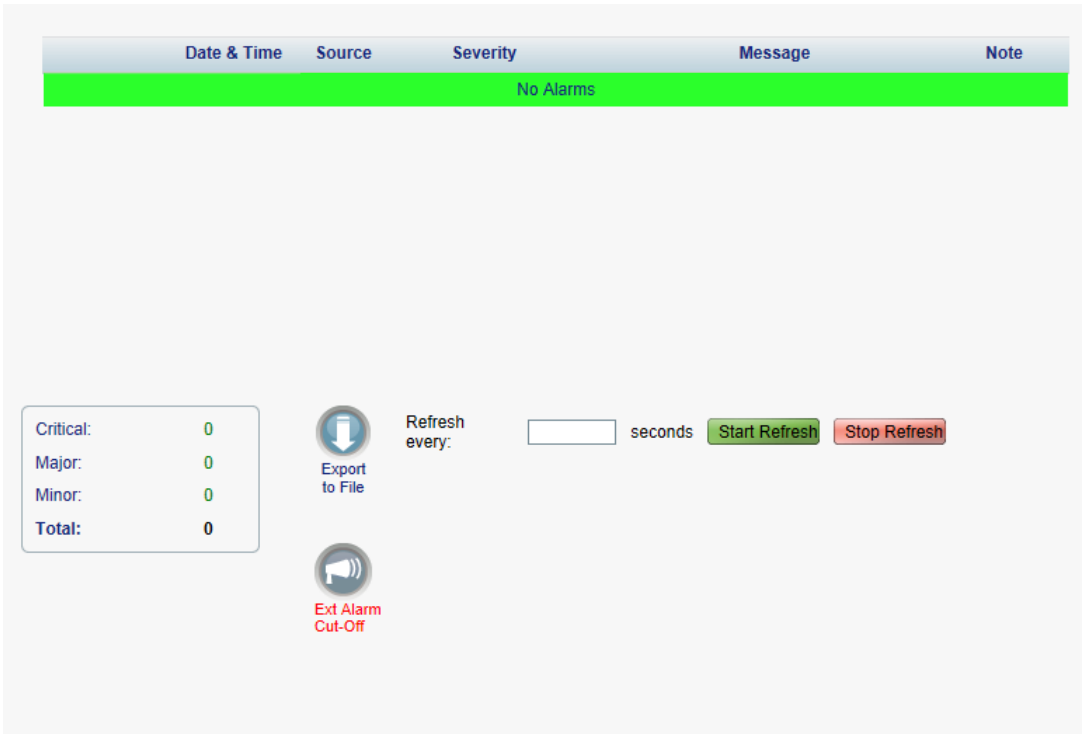


Figure 43: Alarms Tab

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 (p. 13).

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

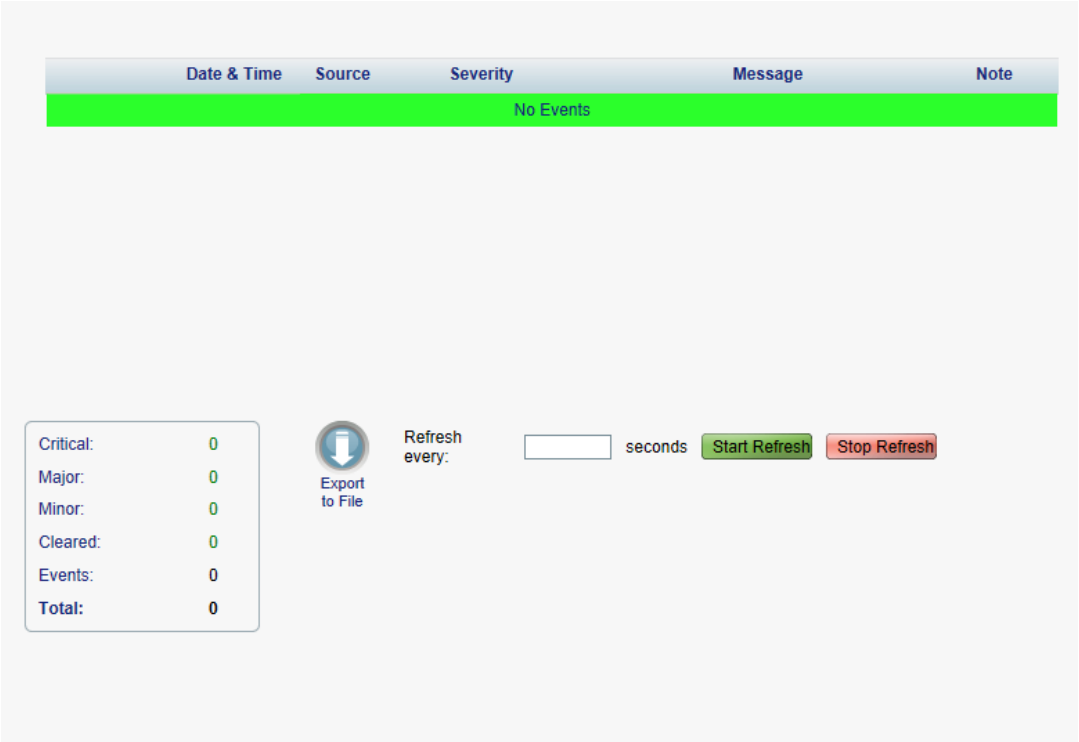


Figure 44: Events Tab

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 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

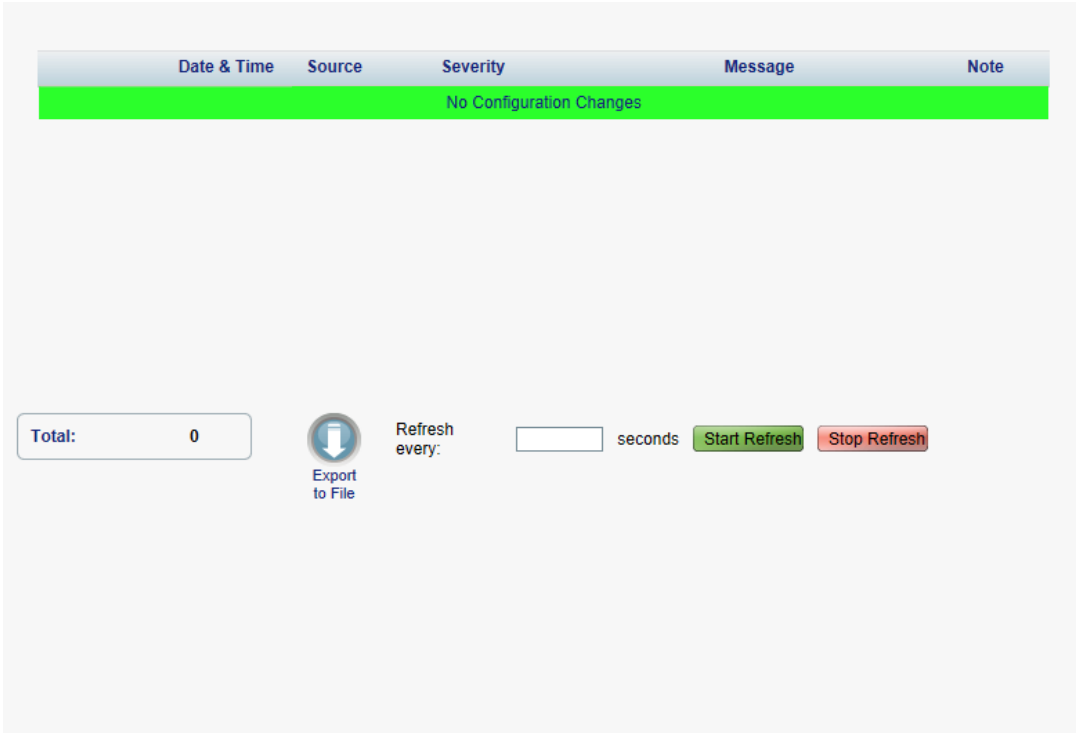


Figure 45: Configuration Changes Tab

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 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 Ethernet Port Faults

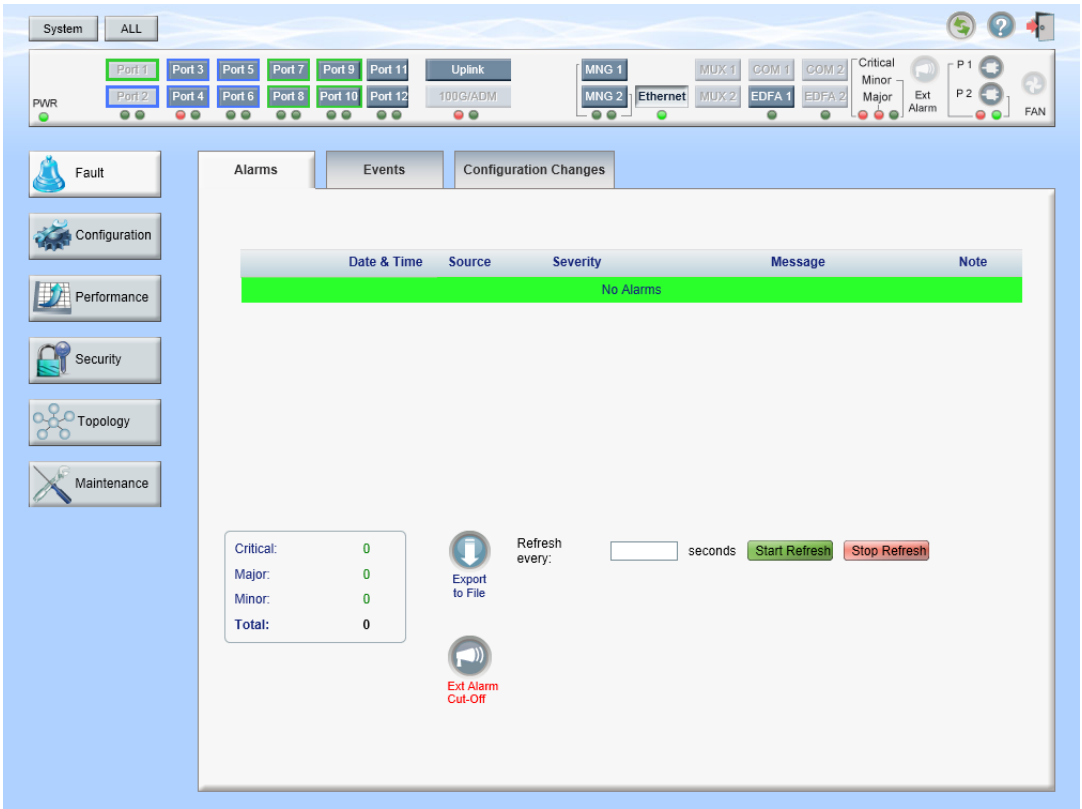


Figure 46: Ethernet Port Fault Window

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.

5.8.1 Alarms Tab

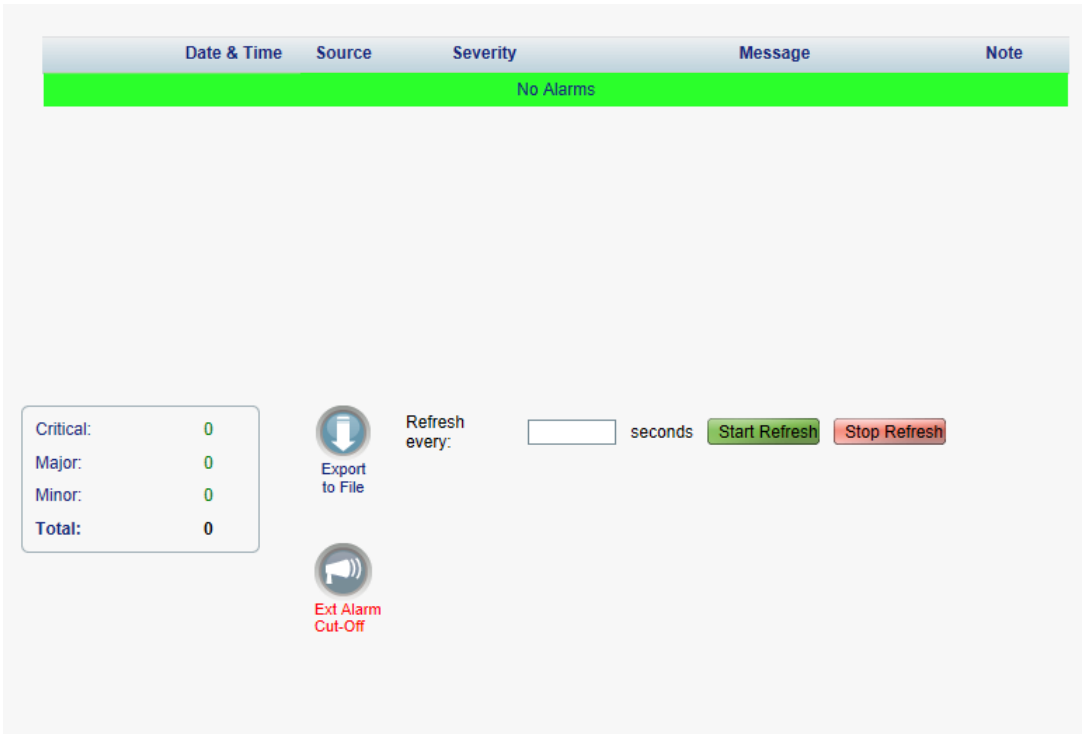


Figure 47: Alarms Tab

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 (p. 13).

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

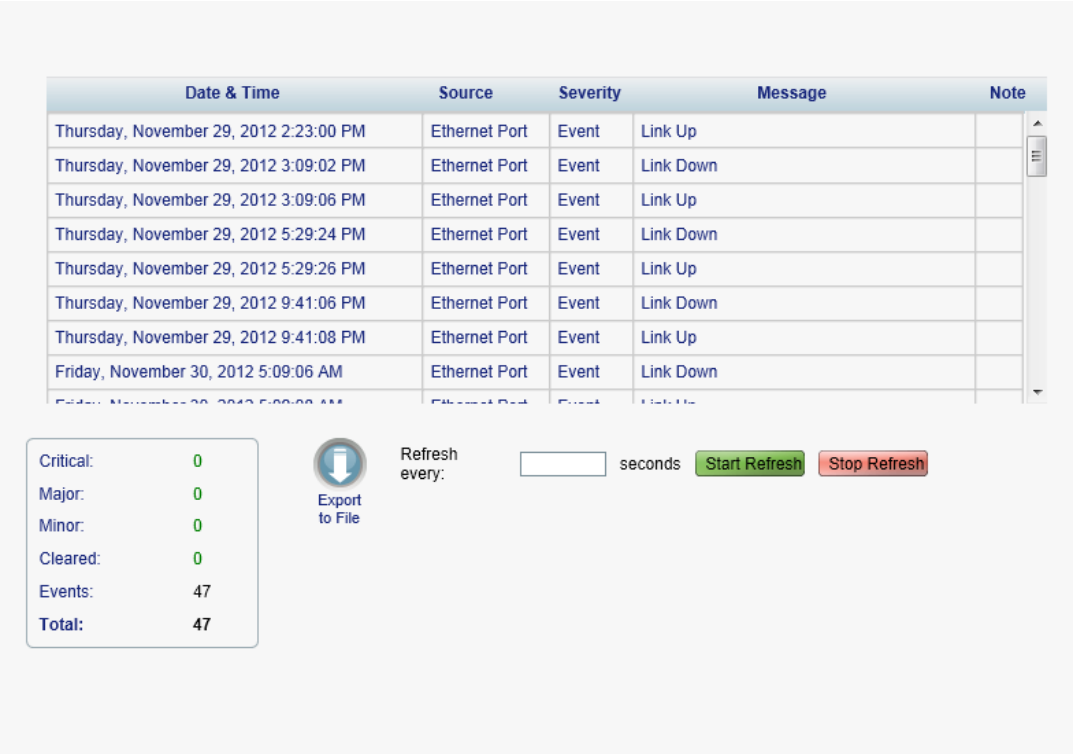


Figure 48: Events Tab

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 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

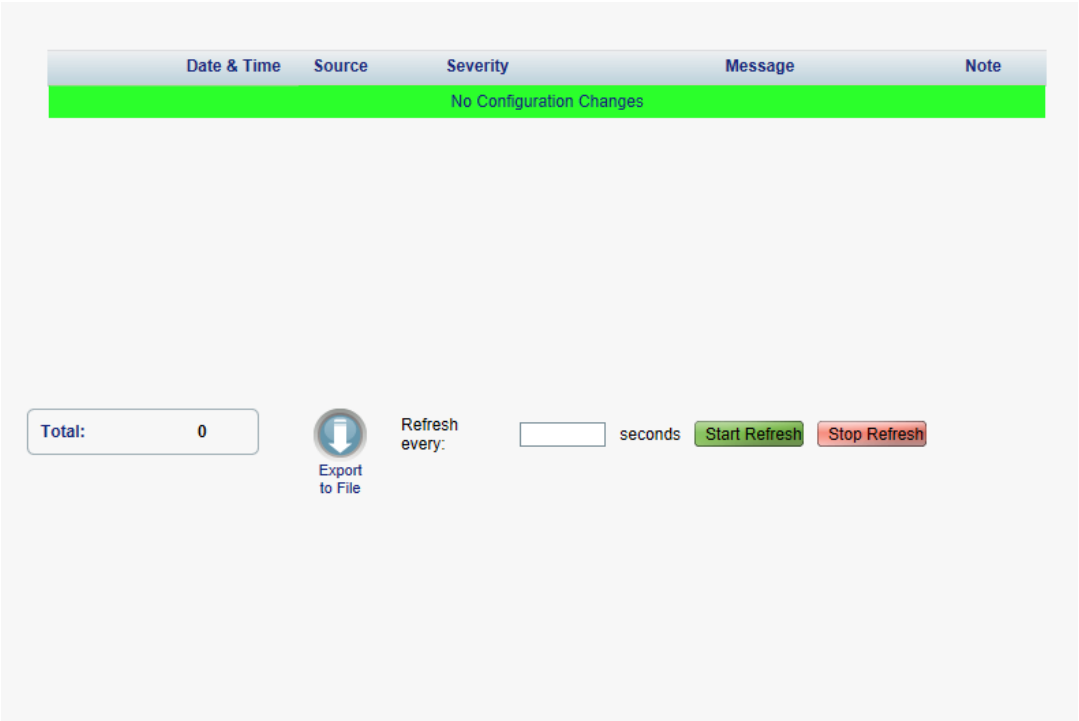


Figure 49: Configuration Changes Tab

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 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 EDFA Faults

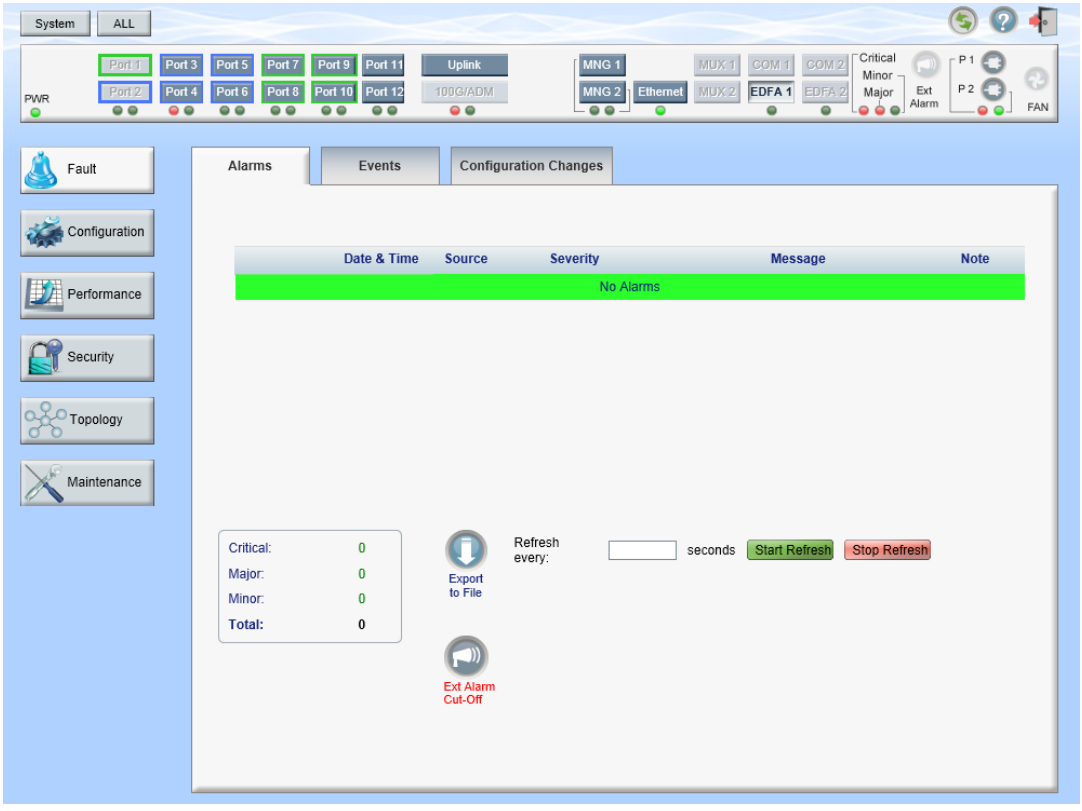


Figure 50: EDFA Fault Window

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 **EDFA** to select the EDFA module.

   The EDFA Fault window opens.

5.9.1 Alarms Tab

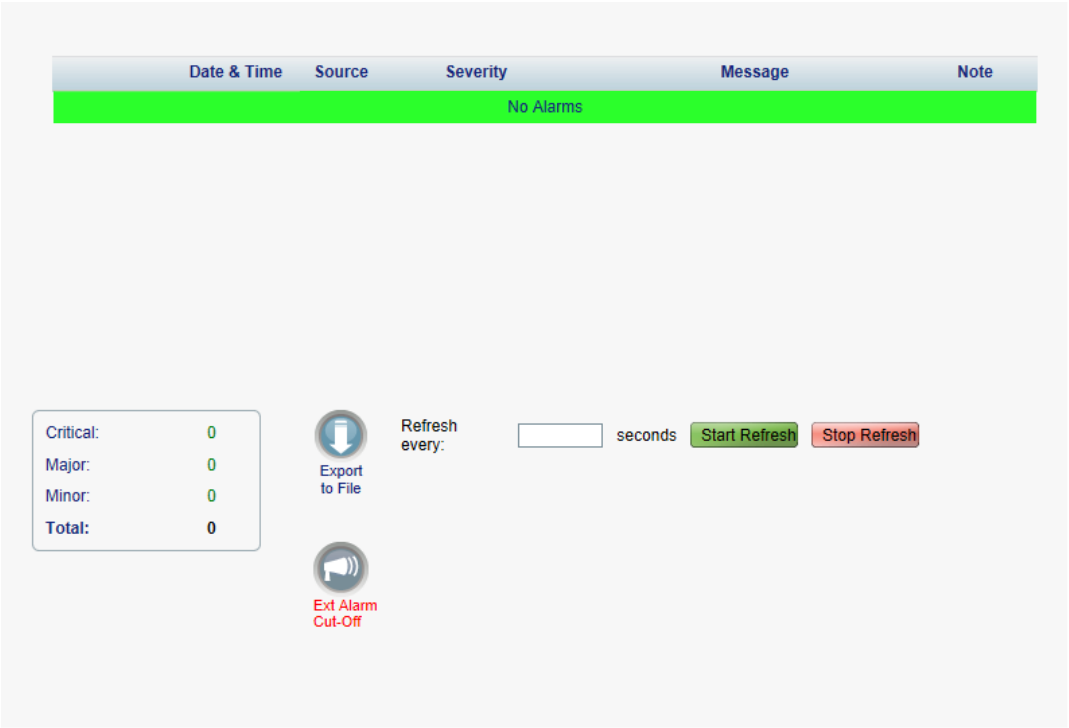


Figure 51: Alarms Tab

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 (p. 13).

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.	

Parameter	Description	Format / Values
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

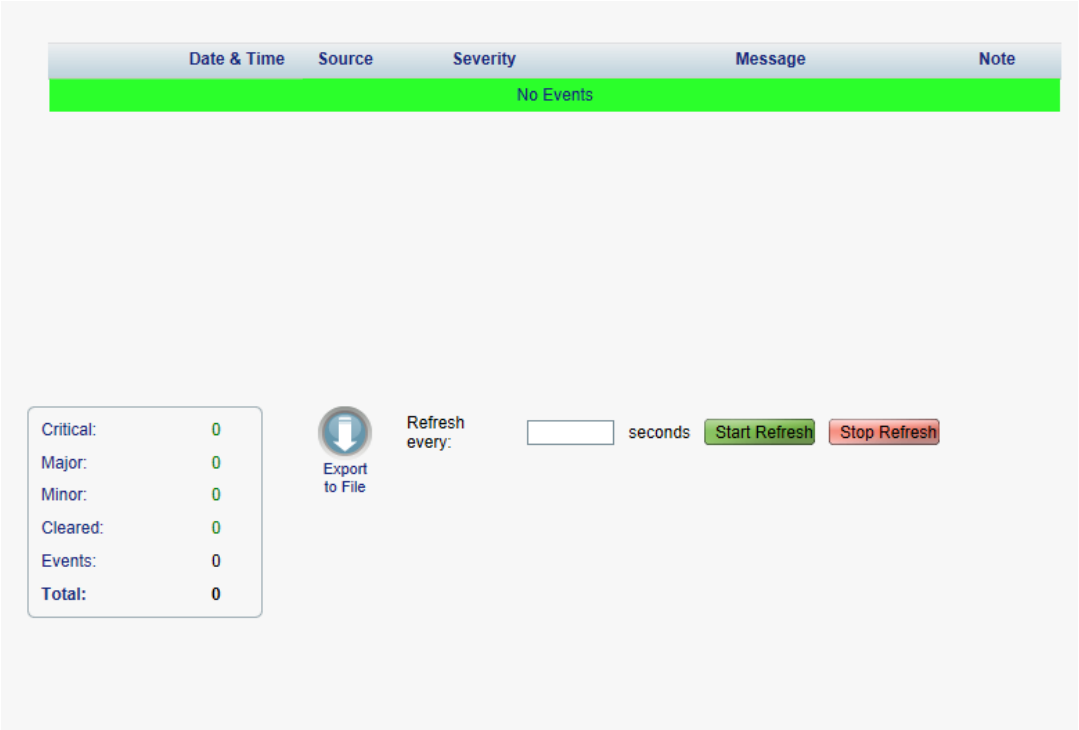


Figure 52: Events Tab

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 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

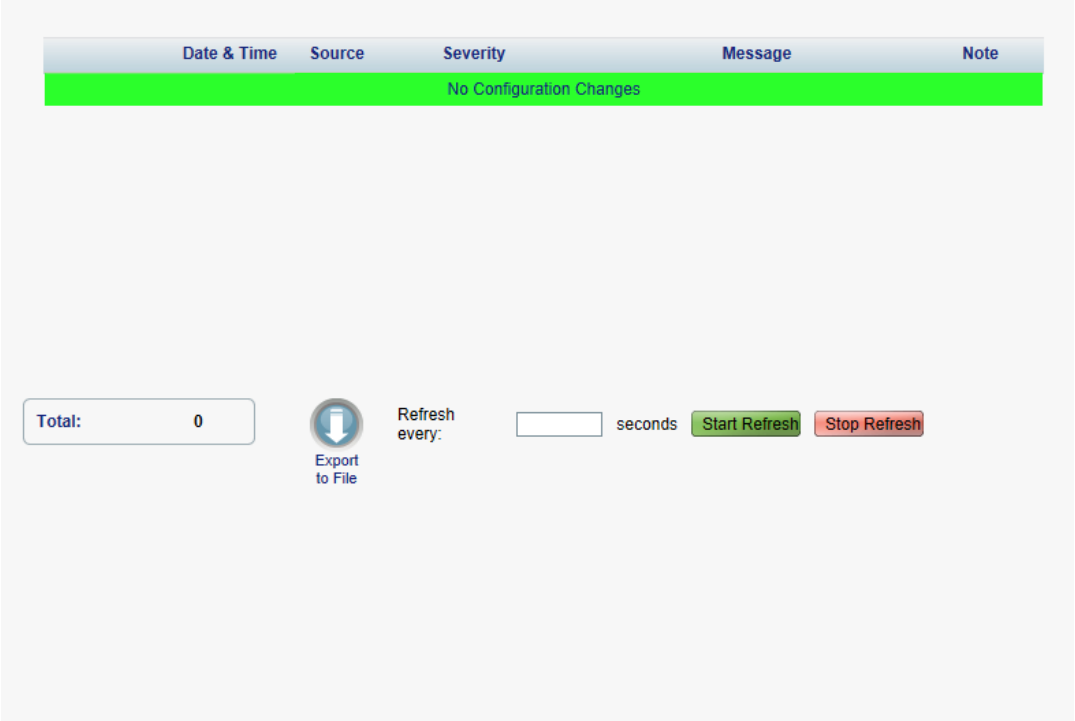


Figure 53: Configuration Changes Tab

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 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.	

5.10 PSU Faults

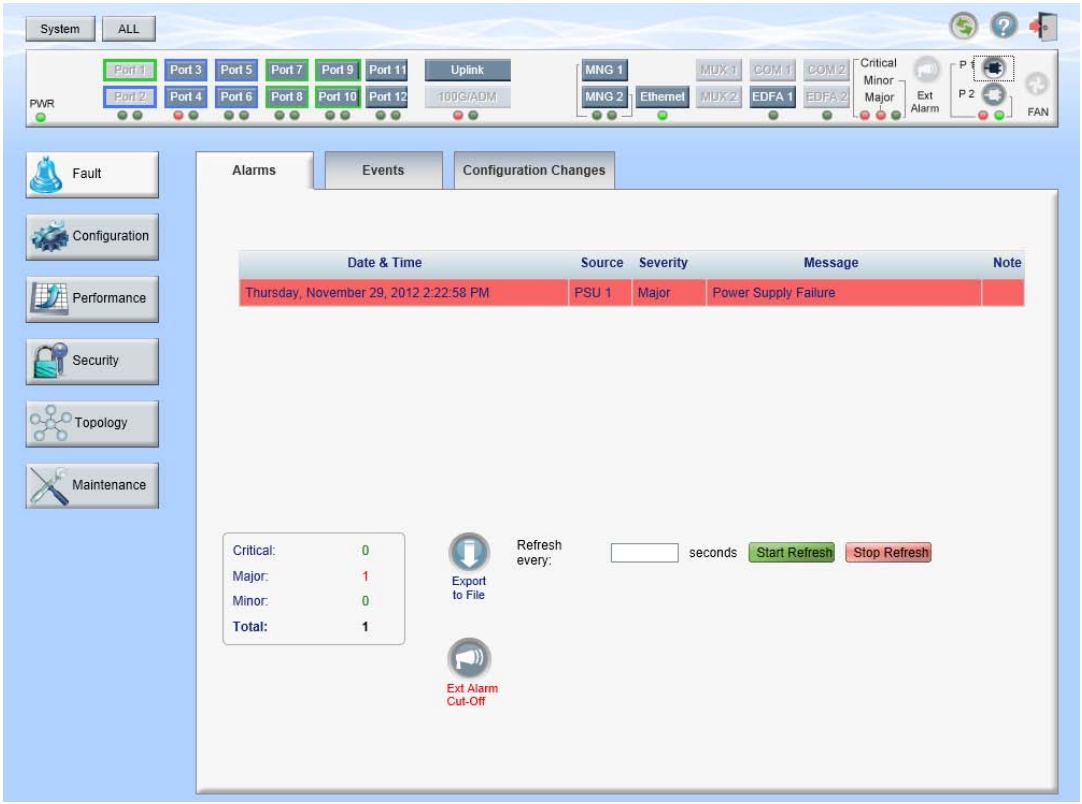


Figure 54: PSU Fault Window

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.

5.10.1 Alarms Tab

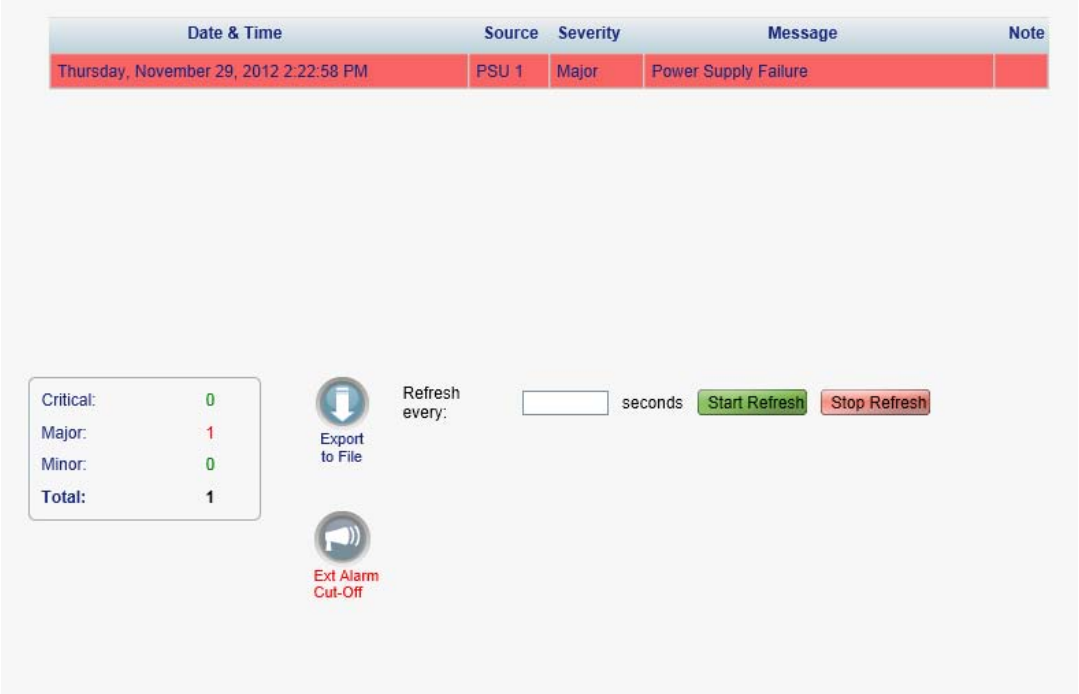


Figure 55: Alarms Tab

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 (p. 13).

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 33: 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.

5.10.2 Events Tab

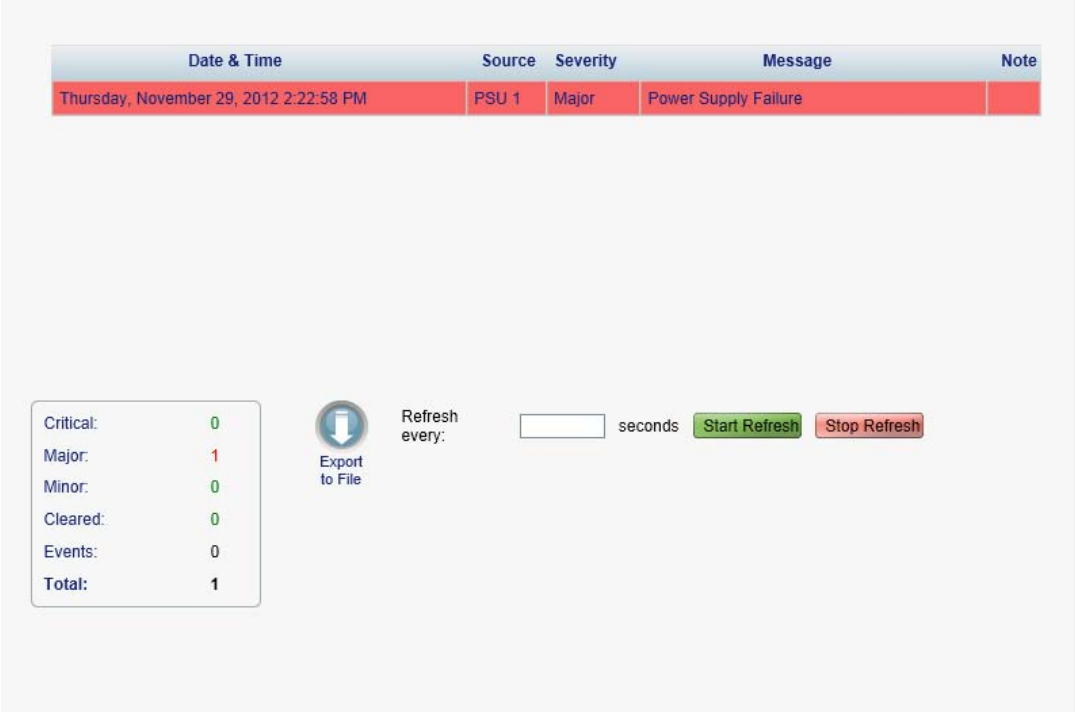


Figure 56: Events Tab

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 34: 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.

5.10.3 Configuration Changes Tab

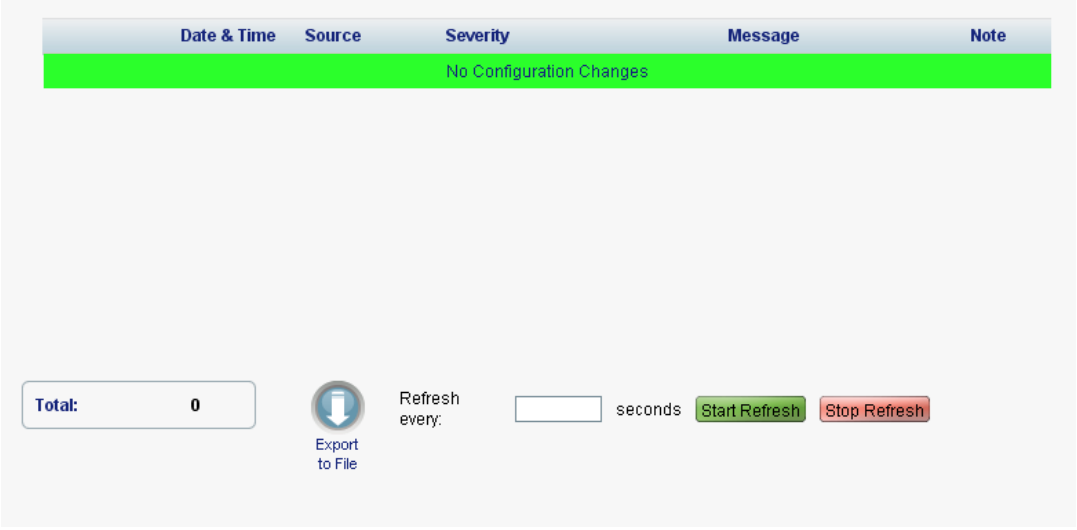


Figure 57: Configuration Changes Tab

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 35: 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-1000GT.

For initial configuration of the PL-1000GT via a local terminal, and instructions for logging in and out of the Web application, see Operation and Preliminary Configuration (p. 29).

In this Chapter

6.1 Configuration Operations

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

- **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
- **Optical Ports**
  - **Uplink Port**
    - Configure port parameters
    - Configure the Coherent module
    - Configure ALS parameters
    - Configure OTN parameters

- **Service Port (100G/ADM)**
  - View port status
  - Configure port parameters
  - Enable or disable the port
  - View CFP information
  - Configure ALS parameters
- **Service Port (Port 1 - Port 2)**
  - View port status
  - Configure port parameters
  - Enable or disable a port
  - View QSFP+ information
  - Configure ALS parameters
- **Service Port (Port 3 - Port 12)**
  - View port status
  - Configure port parameters
  - Enable or disable a port
  - Configure the SFP+ module
  - Configure ALS parameters
- **MNG Port**
  - View port status
  - Configure port parameters
  - Enable or disable a port
  - Configure the SFP module
  - Configure ALS parameters

- **Ethernet Port**
  - View port status
  - Configure port parameters
- **EDFA Module**
  - View module status
  - Configure the EDFA module
  - Enable or disable the module
- **PSU Unit**
  - View PSU information

- **FAN Unit**
  - View FAN information

6.2 General Configuration Procedure

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

To view and configure the PL-1000GT 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. 104))
   - **Uplink** (see Uplink Port Configuration (p. 117))
   - **100G/ADM** (see Transponder Service Port Configuration (p. 125))
   - **Port 1 – Port 2** (see Muxponder Service Port Configuration (p. 132))
   - **Port 3 – Port 12** (see Muxponder Service Port Configuration (p. 132))
   - **MNG 1 – MNG 2** (see Management Port Configuration (p. 141))
   - **Ethernet** (see Ethernet Port Configuration (p. 147))
   - **EDFA** (if present) (see EDFA Configuration (p. 149))
   - **PSU** (see PSU Configuration (p. 152))
   - **FAN** (see FAN Unit Configuration (p. 153))

   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 information is provided, click **Apply**.

6.3 System Configuration

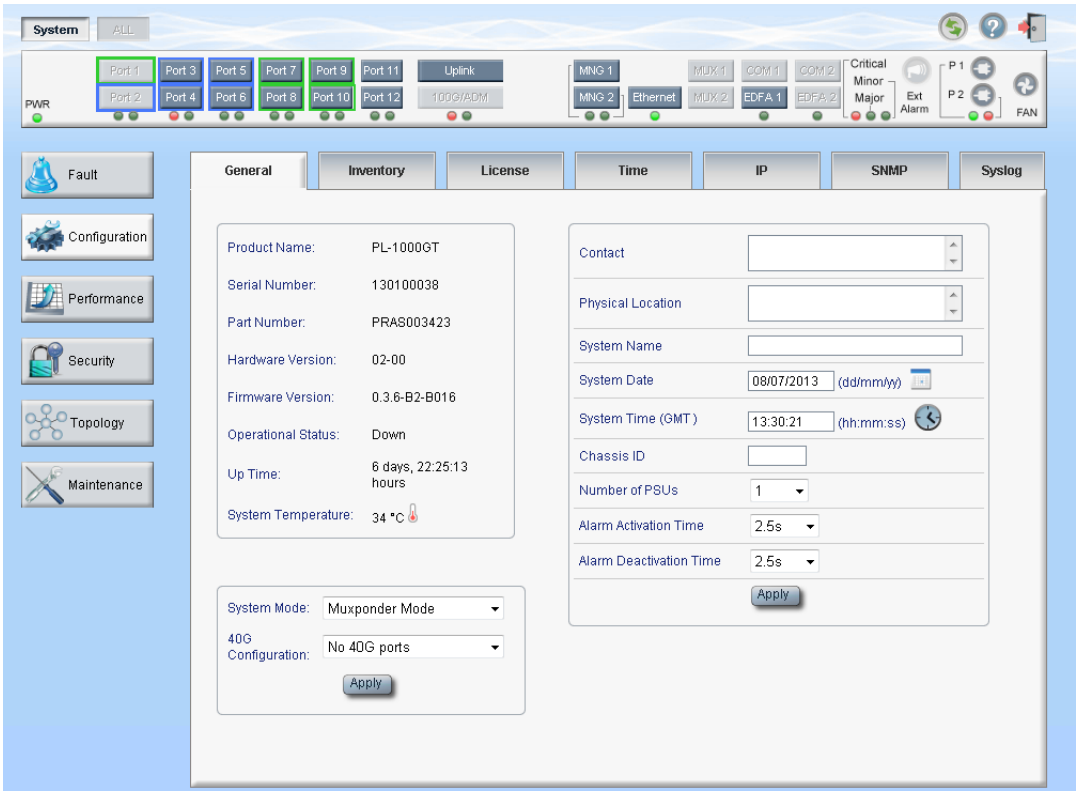


Figure 58: System Configuration Window

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-1000GT
- **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

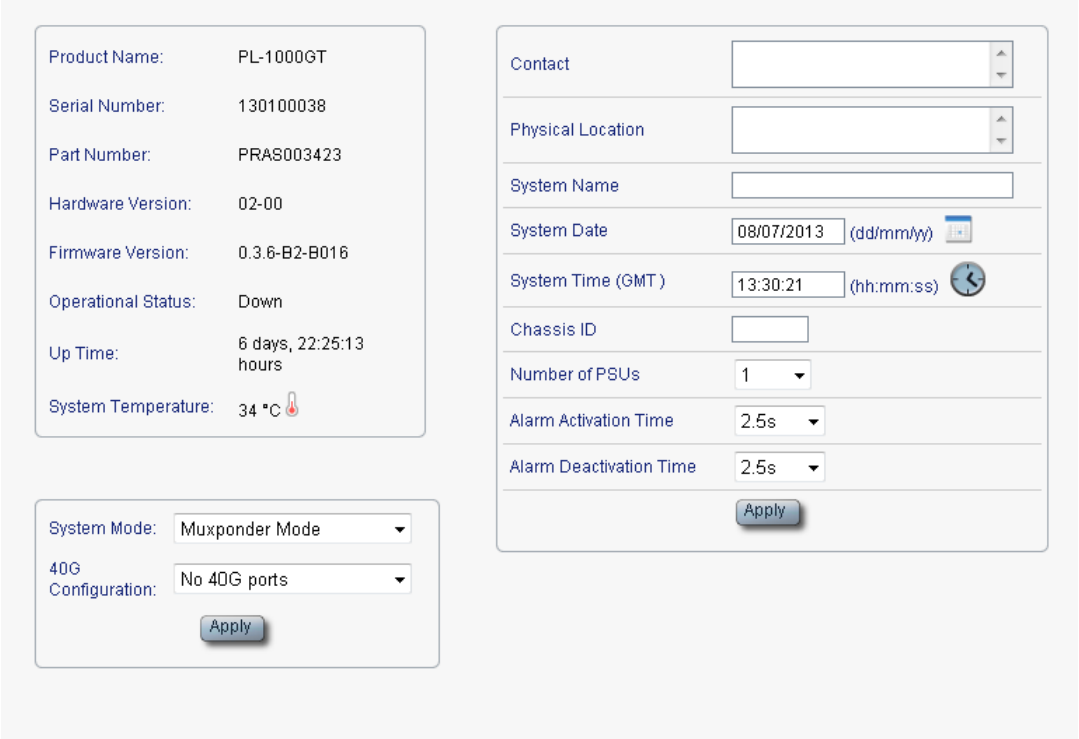


Figure 59: General Tab

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**.
4. Set the **System Mode.**
   1. From the **System Mode** drop-down list, select the mode.

      If set to **Muxponder Mode**, the **40G Configuration** field is enabled.
   2. (If enabled) From the **40G Configuration** drop-down list, select the configuration.
   3. Click **Apply**.

   NOTE: Changing this parameter requires a cold restart of the node.

Table 36: General Tab

Parameter	Description	Format/Values
Product Name	The name of the product.	PL-1000GT
Serial Number	The serial number of the entity.	Serial number
Part Number	The part number of the node.	Part number

Parameter	Description	Format / Values
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
System Mode	The operation mode of the PL-1000GT.	• **Muxponder Mode**: ▪ 10 x 10G ▪ 2 x 40G + 2 x 8G/10G ▪ 1 x 40G+ 6 x 8G/10G • **Transponder Mode**: ▪ 1 x 100G **NOTE:** ▪ When set to **Muxponder Mode**, the **40G Configuration** field is enabled. ▪ Changing this value requires a cold restart of the node.
40G Configuration	The type of Muxponder configuration.	• **No 40G ports**: ▪ 10 x 10G ▪ Port 3 to Port 12 • **Single 40G Port (Upper)**: ▪ 1 x 40G+ 6 x 8G/10G ▪ Port 1, Port 7 to Port 12 • **Dual 40G ports**: ▪ 2 x 40G + 2 x 8G/10G ▪ Port 1, Port 2, Port 11 and Port 12 **NOTE:** This field is enabled when **System Mode** is set to **Muxponder Mode**.
Contact	The contact information for PacketLight Technical Support.	Free text
Physical Location	The address of the site.	Free text
System Name	The logical name given to the PL-1000GT.	Free text

Parameter	Description	Format/Values
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. 206)).
Number of PSUs	The number of power supply units installed in the PL-1000GT.	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

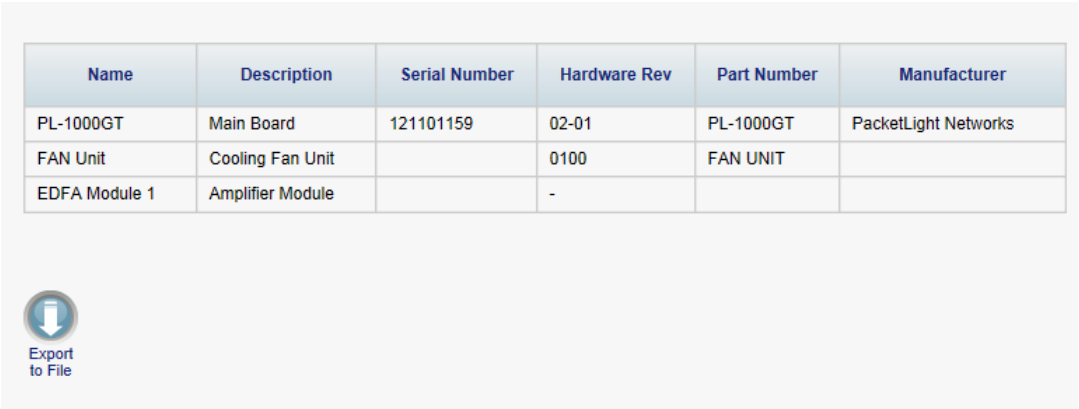


Figure 60: Inventory Tab

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

NOTE: Not all parameters are applicable for all types 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 37: 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

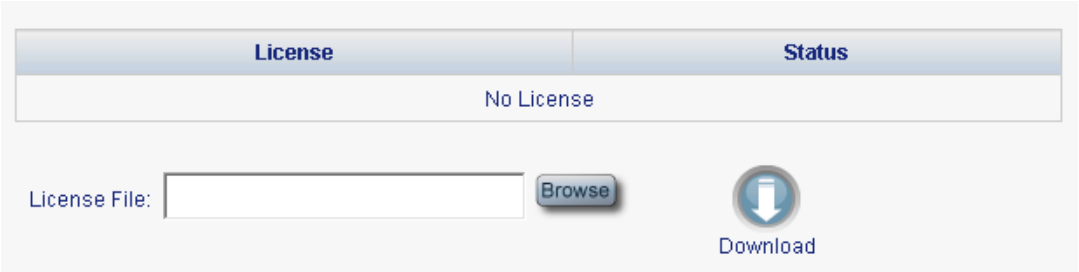


Figure 61: License Tab

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

6.3.4 Time Tab

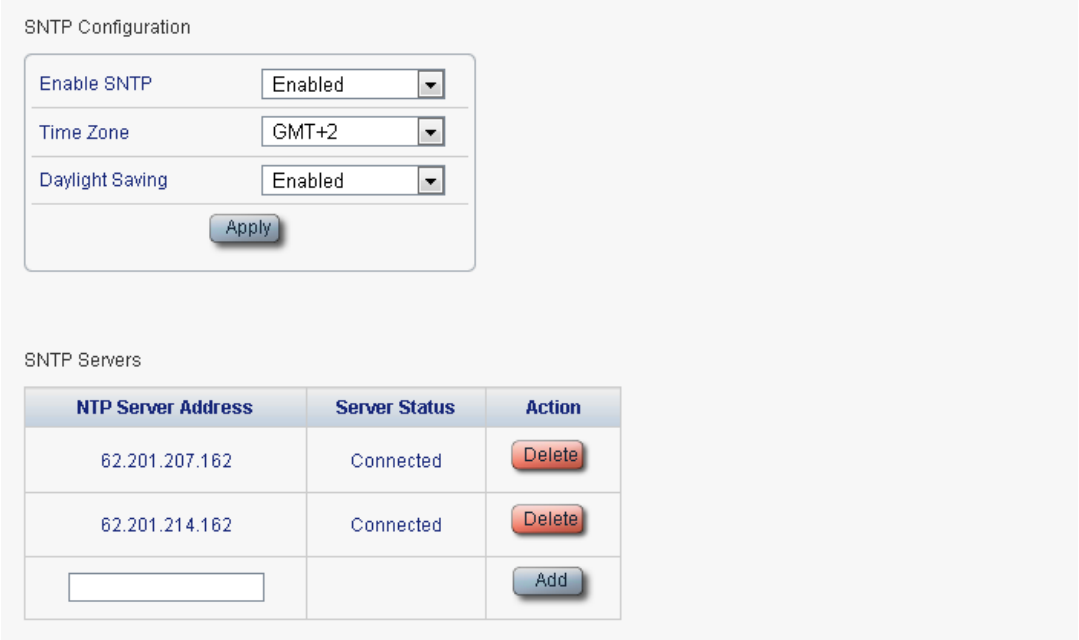


Figure 62: Time Tab

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

The PL-1000GT 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-1000GT 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. 111)).

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 38: 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

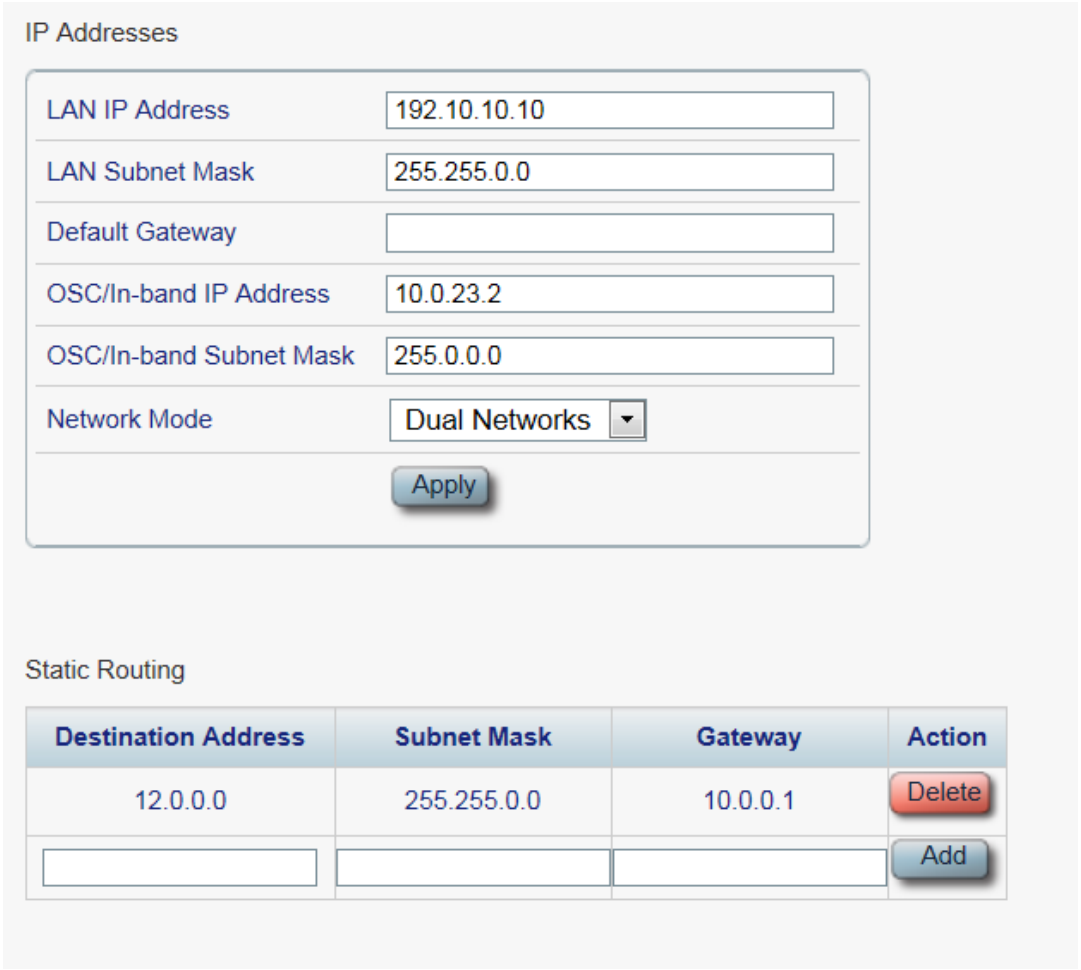


Figure 63: IP Tab - Dual Networks

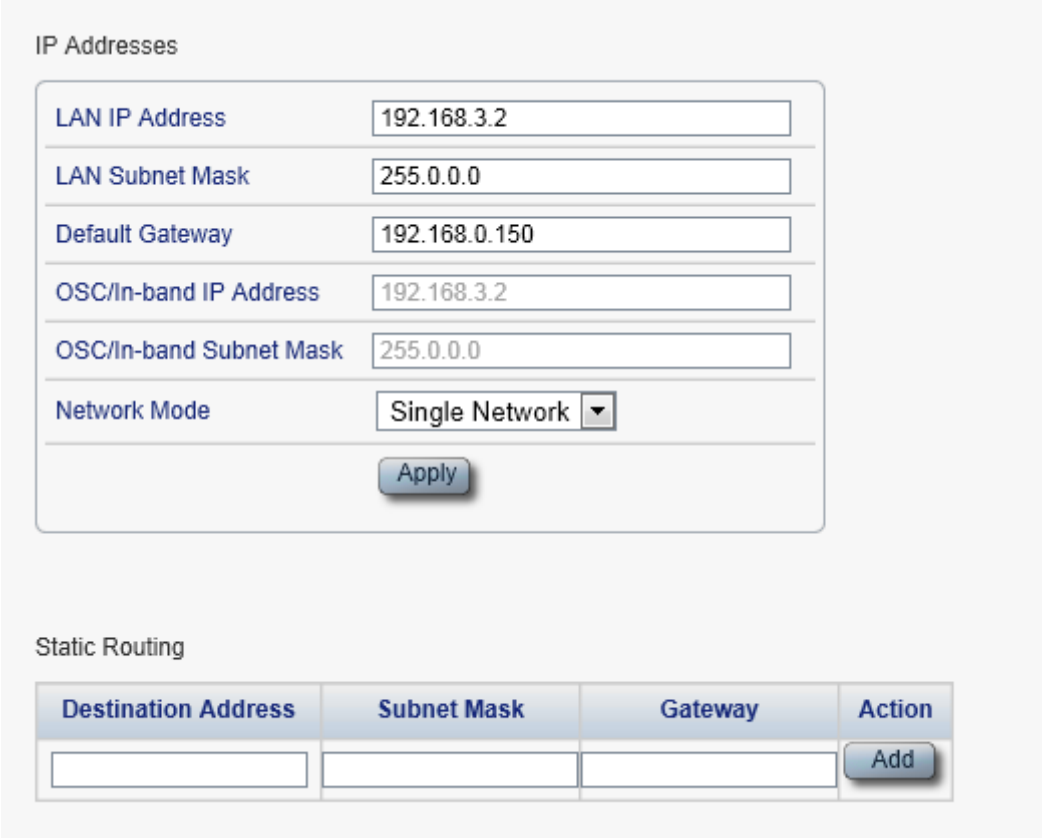


Figure 64: IP Tab - Single Network

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

The PL-1000GT 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:

- Changing the network mode automatically restarts the PL-1000GT; 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.

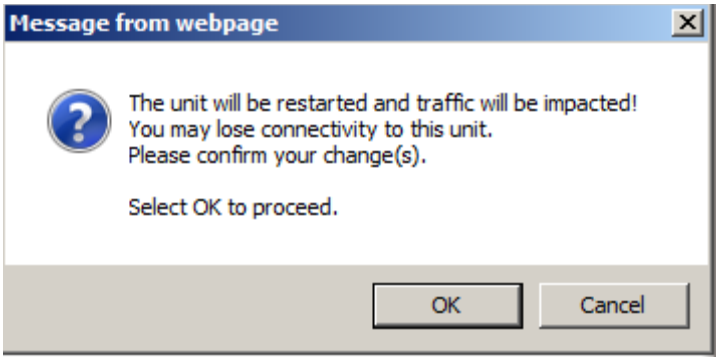


Figure 65: Confirm Changes

   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 39: 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/In-band 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/In-band.	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

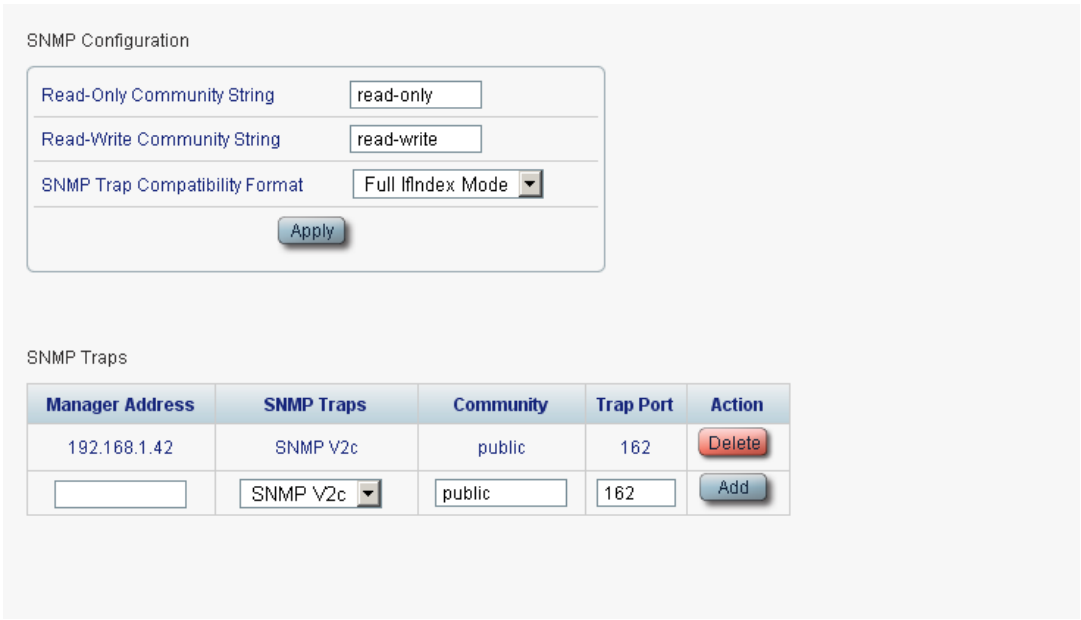


Figure 66: SNMP Tab

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-1000GT must have a specific IP route. Therefore, if needed, add the management system address to the **Static Routing** table (see IP Tab (p. 111)).

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 40: 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
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 to.

A system log of the last 512 events is kept by the node and may be retrieved using the Event Log (see Events (p. 50)).

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.

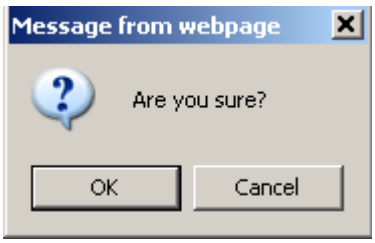
      

      Figure 68: Confirm Configuration

   3. Click **OK**.

3. To remove a configured Syslog server:

   1. Click **Delete** in the corresponding line.

The following confirmation message appears.

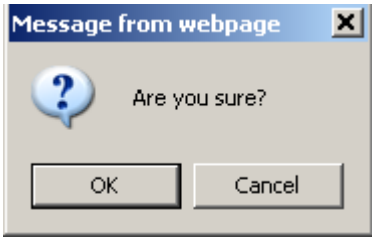


Figure 69: Confirm Configuration

2. Click **OK**.

Table 41: 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 Uplink Port Configuration

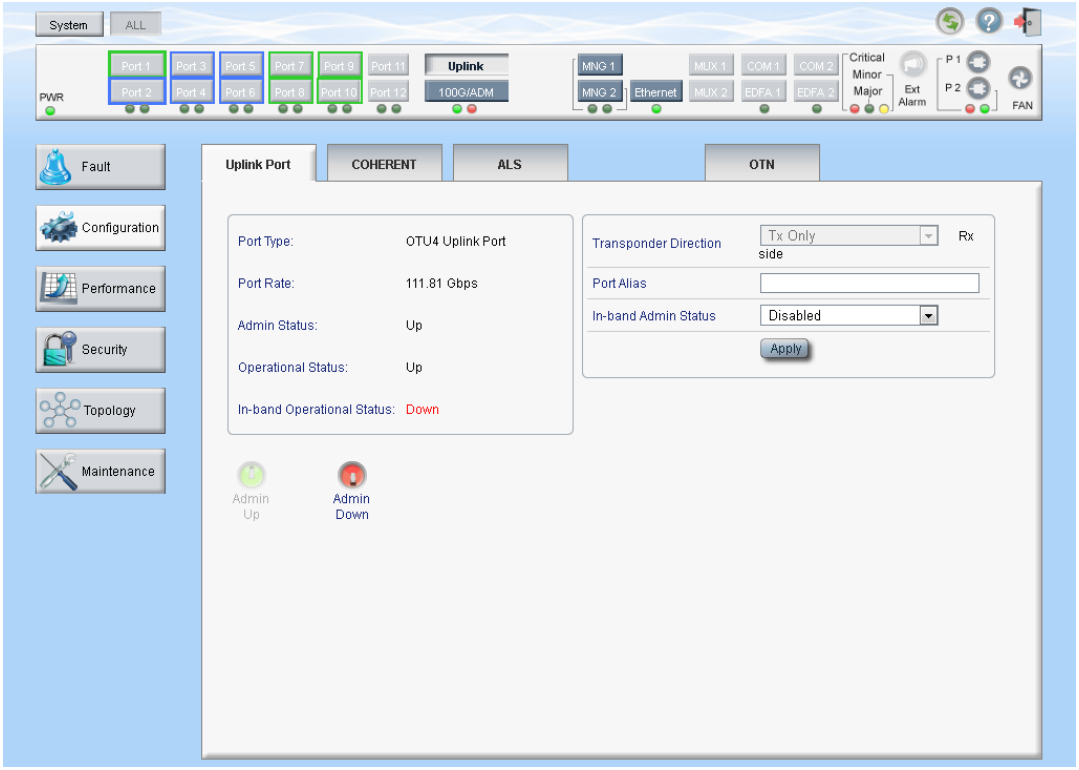


Figure 70: Uplink Port Configuration Window

Use the Uplink Port Configuration window to do the following:

- **Uplink tab**: Configure the uplink port and enable/disable the port
- **Coherent tab**: Configure the Coherent module
- **ALS tab**: Configure ALS for the uplink port
- **OTN tab**: Configure OTN for the uplink port

To open the Uplink Port Configuration window:

1. Click **Configuration**.
2. Click **Uplink** to select the uplink port.

   The Uplink Port Configuration window opens.

6.4.1 Uplink Tab

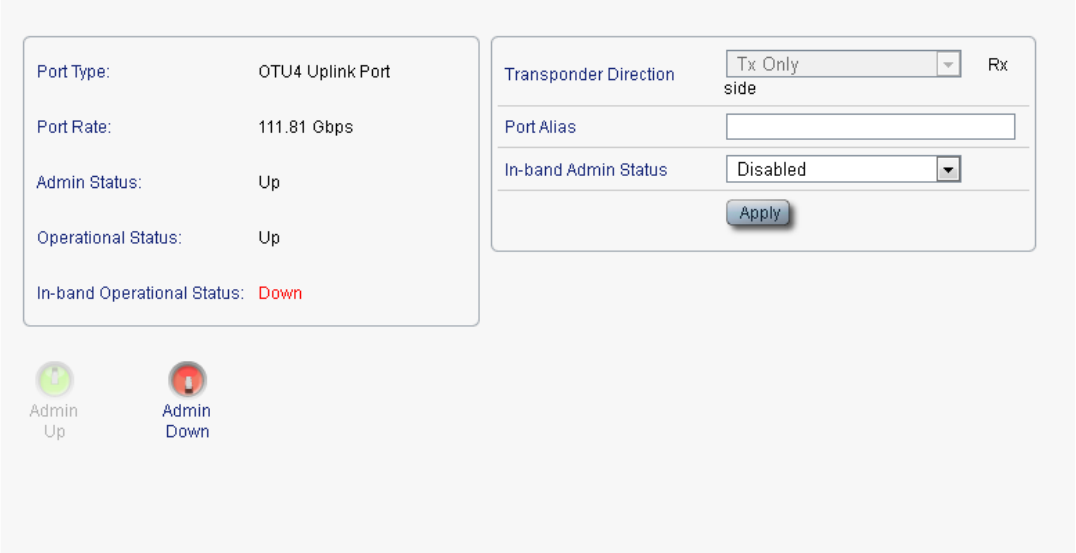


Figure 71: Uplink Tab

Use the Uplink tab to configure the uplink port and enable/disable the port.

To configure the uplink port:

1. Click the **Uplink** tab.

   The Uplink tab opens displaying the uplink 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.

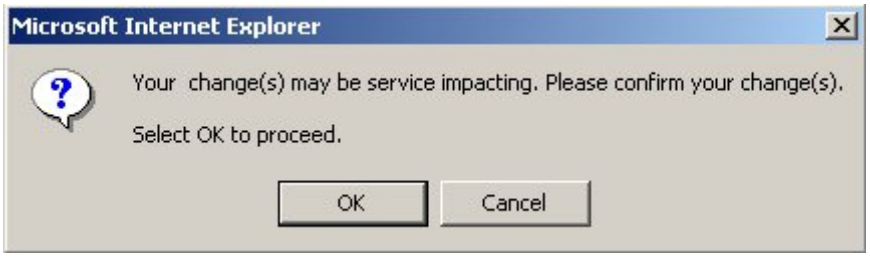


Figure 72: Confirm Changes

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.

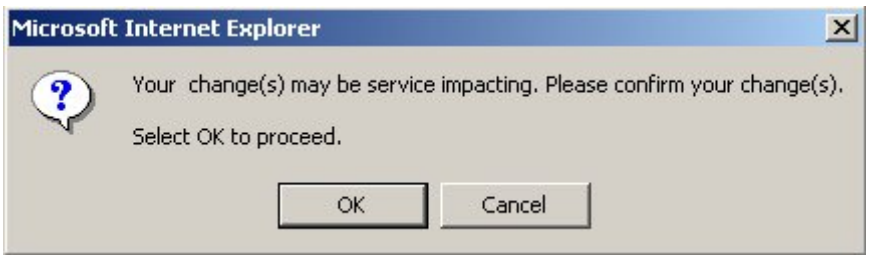


Figure 73: Confirm Changes

   2. Click **OK**.

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

Table 42: Uplink Tab Parameters

Parameter	Description	Format / Values
Port Type	The type of port.	OTU4 Uplink Port
Port Rate	The bit rate of the OTU4 signal of the uplink.	111.81 Gbps
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**
In-band Operational Status	The operational status of the in-band management channel.	• **Down**: The link status of the in-band is **Down**. • **Up**: The link status of the in-band is **Up**.

Parameter	Description	Format / Values
Transponder Direction	Used to determine the direction of the traffic for unidirectional services.	• **Tx+Rx**: Both ports are bidirectional • **Rx Only**: Service is Rx only; Uplink is Tx only • **Tx Only**: Service is Tx only; Uplink is Rx only
Port Alias	The logical name given to the port for identification purposes.	Free text
In-band Admin Status	The in-band administrative status of the uplink port.	Enabled, Disabled **NOTE:** When enabled, the in-band management channel is included in uplink port traffic.

6.4.2 Coherent Tab

Figure 74: Coherent Tab

Use the Coherent tab to display information about the type and status of the optical transceiver inserted in the uplink port and select the grid channel and spacing.

To configure the Coherent module:

1. Click the **Coherent** tab.

   The Coherent tab opens displaying the Coherent configuration.

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

Table 43: Coherent Tab Parameters

Parameter	Description	Format / Values
Vendor Name	The name of the Coherent vendor.	String
WDM Class	The type of Coherent.	DWDM
Lanes Spacing	The lane spacing of the Coherent.	50/100 GHz
TX Nominal WL	The defined Tx wavelength of the Coherent.	nm
RX Nominal WL	The defined Rx wavelength of the Coherent.	nm
Max Bit Rate	The maximum bit rate supported by the Coherent.	Gbps
Part Number	The part number of the Coherent.	String
Serial Number	The serial number of the Coherent.	String
Connector Type	The type of Coherent connector.	LC
Tx Pwr	The measured output power of the Coherent.	dBm
Rx Pwr	The measured input power of the Coherent.	dBm
Current CD (ps/nm)	The measured chromatic dispersion of the Coherent.	ps/nm
Temperature	The measured temperature of the Coherent.	Celsius
100GBE Capabilities	The Coherent capabilities of the 100GbE services are marked.	
OTU4 Capabilities	The Coherent capabilities of the OTU4 services are marked.	
High Receive Power Threshold	The threshold for the High Receive Power alarm.	dBm
Low Receive Power Threshold	The threshold for Low Receive Power alarm.	dBm
TX WL 1 Channel	Select the Tx DWDM channel.	Select the ITU grid channel number. For example, 13.5.
RX WL 1 Channel	Select the Rx DWDM channel.	Select the ITU grid channel number. For example, 13.5.
Spacing	Select the DWDM ITU grid spacing.	50 GHz, 100GHz

6.4.3 ALS Tab

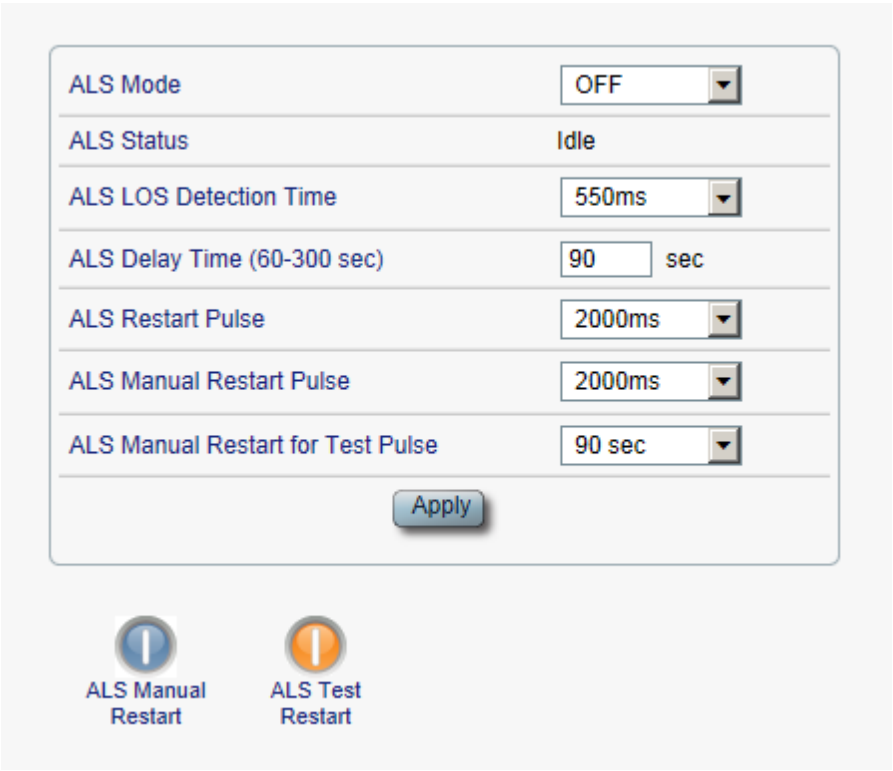


Figure 75: ALS Tab

Use the ALS tab to configure ALS for the 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-1000GT 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 44: 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.

6.4.4 OTN Tab

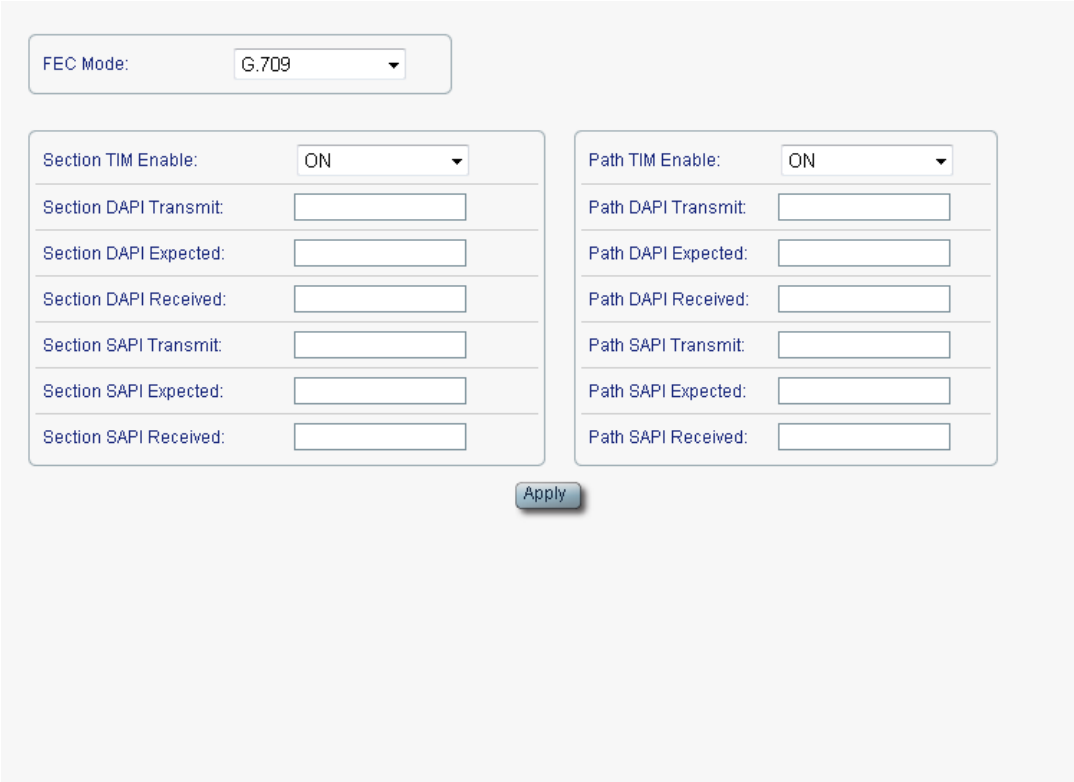


Figure 76: OTN Tab

Use the OTN tab to configure OTN for the uplink port.

To configure OTN:

1. Click the **OTN** tab.

   The OTN tab opens displaying the OTN configuration.

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

3. Click **Apply**.

Table 45: OTN Tab Parameters

Parameter	Description	Format/Values
FEC Mode	Select the FEC mode.	G.709, HG-FEC
Section TIM Enable	Whether or not an alarm should be given when the received trace messages and expected messages are not the same.	• **ON**: Gives an alarm when the received trace messages and expected trace messages are not the same. • **OFF**: Does not give an alarm when the received trace messages and expected trace messages are not the same.
Section DAPI Transmit	Transmitted OTN section destination access point identification (DAPI).	A string with up to 15 alphanumeric characters.
Section DAPI Expected	Expected OTN Section DAPI.	A string with up to 15 alphanumeric characters.
Section DAPI Received	Received OTN Section DAPI.	A read-only string with up to 15 alphanumeric characters.
Section SAPI Transmit	Transmitted OTN section source access point identification (SAPI).	A string with up to 15 alphanumeric characters
Section SAPI Expected	Expected OTN Section SAPI.	A string with up to 15 alphanumeric characters.
Section SAPI Received	Received OTN Section SAPI.	A read-only string with up to 15 alphanumeric characters.
Path TIM Enable	Whether or not an alarm should be given when the received trace messages and expected messages are not the same.	• **ON**: Gives an alarm when the received trace messages and expected trace messages are not the same. • **OFF**: Does not give an alarm when the received trace messages and expected trace messages are not the same
Path DAPI Transmit	Transmitted OTN Path DAPI.	A string with up to 15 alphanumeric characters.
Path DAPI Expected	Expected OTN Path DAPI.	A string with up to 15 alphanumeric characters
Path DAPI Received	Received OTN Path DAPI.	A read-only string with up to 15 alphanumeric characters.
Path SAPI Transmit	Transmitted OTN Path SAPI.	A string with up to 15 alphanumeric characters.

Parameter	Description	Format/Values
Path SAPI Expected	Expected OTN Path SAPI.	A string with up to 15 alphanumeric characters.
Path SAPI Received	Received OTN Path SAPI.	A read-only string with up to 15 alphanumeric characters.

6.5 Transponder Service Port Configuration

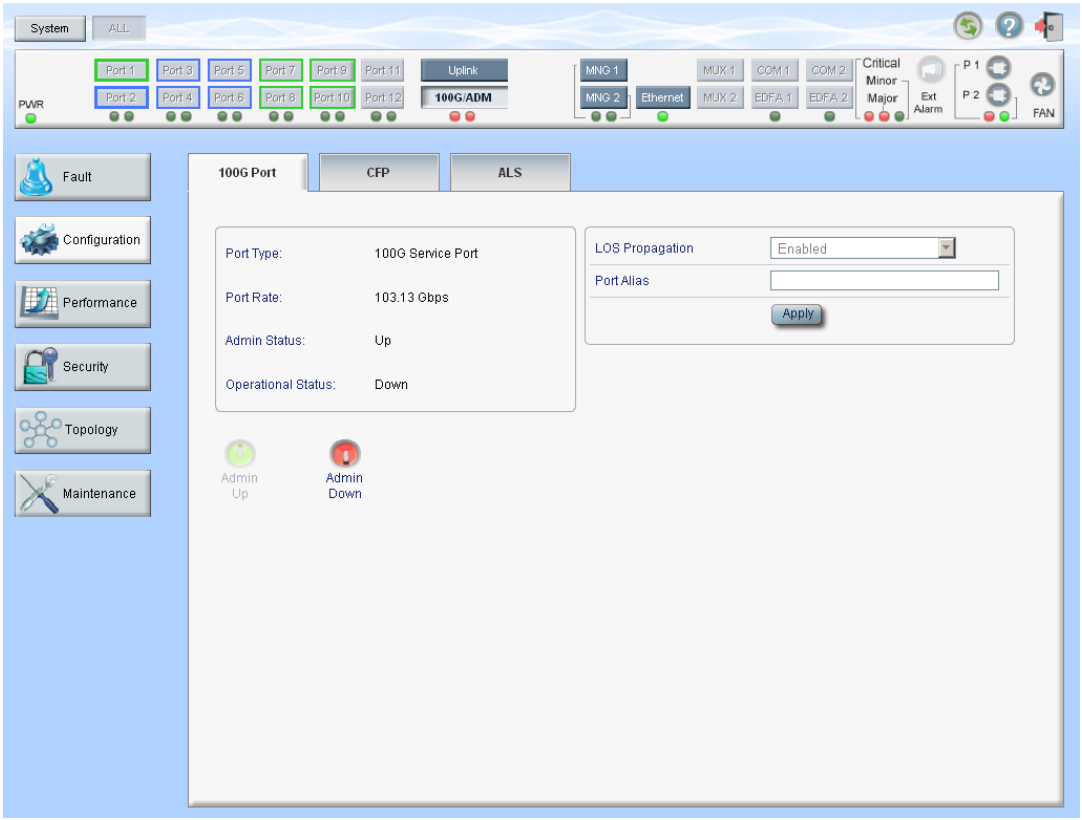


Figure 77: Transponder Service Port Configuration Window

Use the Transponder Service Port Configuration window to do the following:

- **100G Port tab**: Configure the service port in Transponder mode and enable/disable the port
- **CFP tab**: Display information about the type and status of the optical transceiver inserted in the selected port
- **ALS tab**: Configure ALS for the service port in Transponder mode

To open the Transponder Service Port Configuration window:

1. Click **Configuration**.
2. Click **100G/ADM** to select the service port.

   The Service Port Configuration window in Transponder mode opens.

6.5.1 100G Port Tab

Figure 78: 100G Port Tab

Use the 100G Port tab to configure the service port in Transponder mode and enable/disable the port.

To configure the service port in Transponder mode:

1. Click the **100G Port** tab.

   The 100G Port tab opens displaying the service port configuration in Transponder mode.
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.

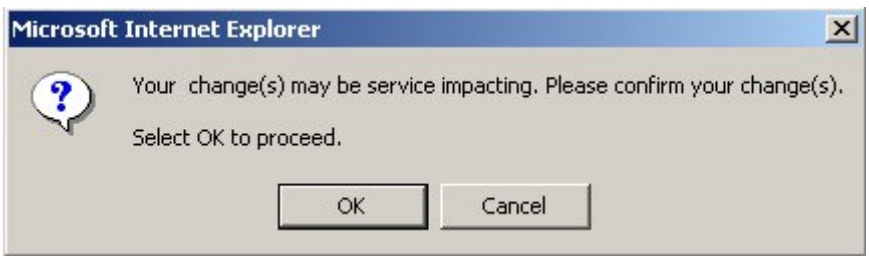


Figure 79: Confirm Changes

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.

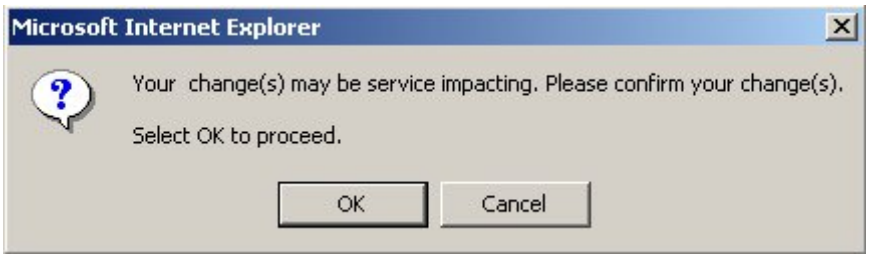


Figure 80: Confirm Changes

   2. Click **OK**.

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

Table 46: 100G Port Tab

Parameter	Description	Format/Values
Port Type	The type of port.	100G Service Port
Port Rate	The bit rate of the service.	103.13 Gbps
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 Propagation	Enable or disable LOS propagation.	Enabled, Disabled **NOTE:** ▪ This field is read only. ▪ When **LOS Propagation** is enabled and a defect is detected on one of the service ports, the laser of the corresponding remote service port will be shut off.
Port Alias	The logical name given to the port for identification purposes.	Free text

6.5.2 CFP Tab

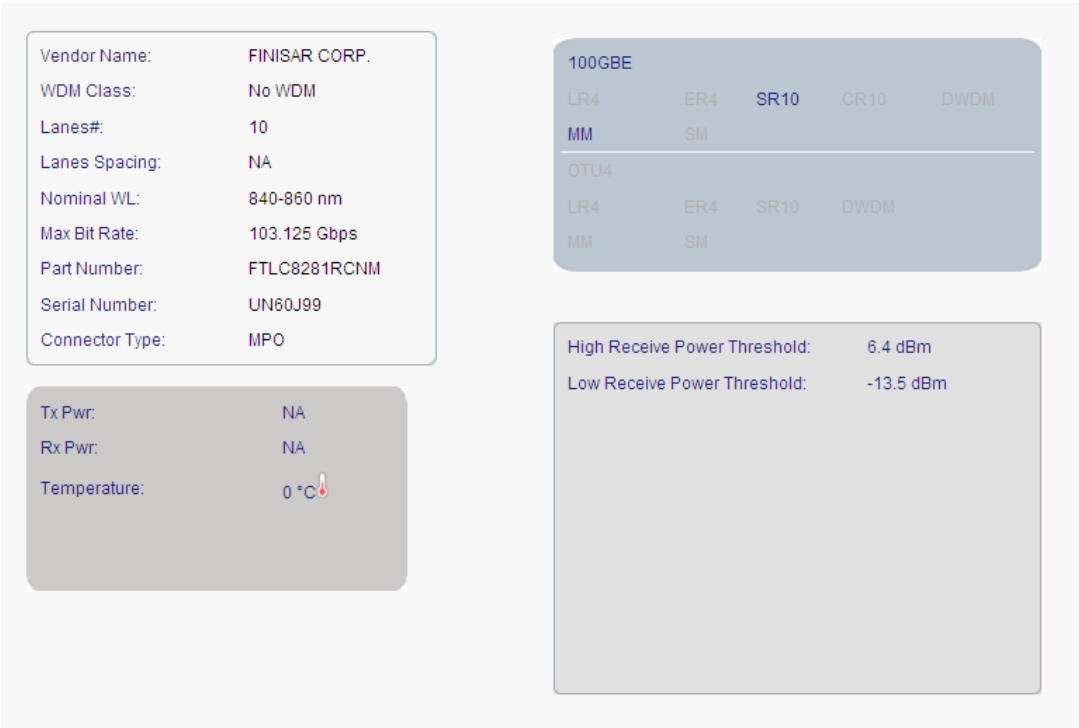


Figure 81: CFP Tab

Use the CFP tab to display information about the type and status of the optical transceiver inserted in the 100G service port and select the wavelength tuning.

To configure the CFP module:

1. Click the **CFP** tab.

   The CFP tab opens displaying the CFP configuration.

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

Table 47: CFP Tab Parameters

Parameter	Description	Format / Values
Vendor Name	The name of the CFP vendor.	String
WDM Class	The type of CFP.	No WDM, CWDM, DWDM
Lanes#	The number of lanes used by the CFP.	• **DWDM**: 4 lanes • **ER4**: 4 lanes • **LR4**: 4 lanes • **SR10**: 10 lanes
Lanes Spacing	The lane spacing of the CFP.	• **CWDM**: 20 nm • **DWDM**: 50 GHz, 100 GHz • **Other**: NA

Parameter	Description	Format/Values
Nominal WL	The defined wavelength of the CFP. • **4 lanes**: The wavelength per lane. • **10 lanes**: The range of wavelengths of the 10 lanes.	• **4 lanes**: 4 x nm • **10 lanes**: nm - nm
Max Bit Rate	The maximum bit rate supported by the CFP.	Gbps
Part Number	The part number of the CFP.	String
Serial Number	The serial number of the CFP.	String
Connector Type	The type of CFP connector.	• **WDM**: 4 x LC • **LR4/ER4/LR10**: LC • **SR10** : MPO
Tx Power	The measured output power of the CFP. • **4 lanes**: The measured output power of the CFP per lane. • **10 lanes**: The range of measured output power of the CFP for the 10 lanes.	• **4 lanes**: 4 x dBm • **10 lanes**: dBm - dBm
Rx Power	The measured input power of the CFP. • **4 lanes**: The measured input power of the CFP per lane. • **10 lanes**: The range of measured input power of the CFP for the 10 lanes.	• **4 lanes**: 4 x dBm • **10 lanes**: dBm - dBm
Temperature	The measured temperature of the CFP.	Celsius
100GBE Capabilities	The CFP capabilities of the 100GbE services are marked.	
OTU4 Capabilities	The CFP capabilities of the OTU4 services are marked.	
High Receive Power Threshold	The threshold for the High Receive Power alarm.	dBm
Low Receive Power Threshold	The threshold for Low Receive Power alarm.	dBm
Tx WL # Channel	Select the DWDM channel.	ITU grid channel number **NOTE:** This field is displayed for DWDM only and if the CFP module supports wavelength tuning as defined by the MSA standard.

Parameter	Description	Format / Values
Wavelength Tuning	Select the DWDM channel.	ITU grid channel number **NOTE:** This field is displayed only if the CFP module supports wavelength tuning as defined by the MSA standard.

6.5.3 ALS Tab

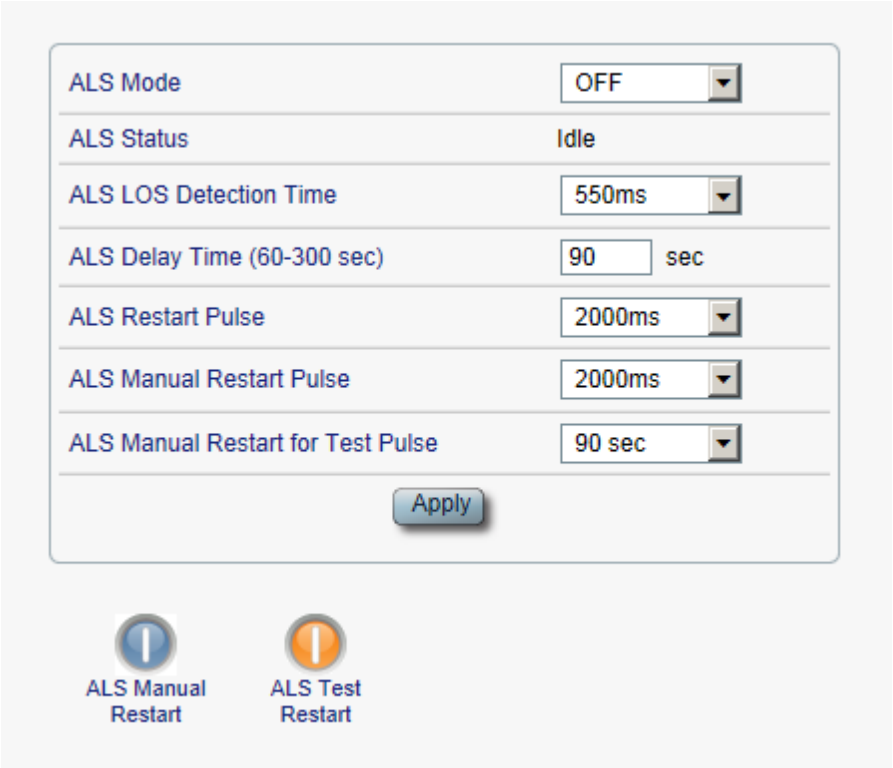


Figure 82: ALS Tab

Use the ALS tab to configure ALS for the 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-1000GT 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 48: 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.

6.6 Muxponder Service Port Configuration

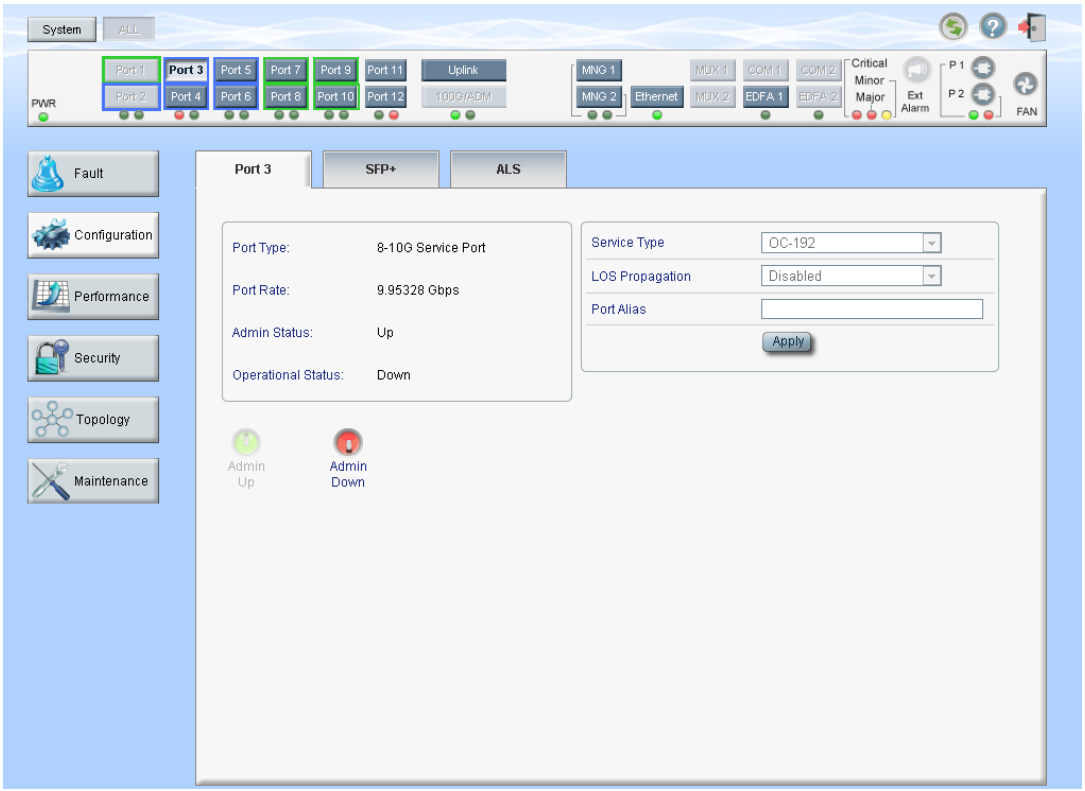


Figure 83: Muxponder Service Port Configuration Window

Use the Service Port Configuration window to do the following:

- **Port tab**: Configure the service port in Muxponder mode and enable/disable the port
- **QSFP+ (Ports 1-2)** Configure the QSFP+ module
- **SFP+ (Ports 3 -12)**: Configure the SFP+ module
- **ALS tab**: Configure ALS for the service port in Muxponder mode

To open the Service Port Configuration window:

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

   The appropriate Service Port Configuration window in Muxponder mode opens.

6.6.1 Port Tab

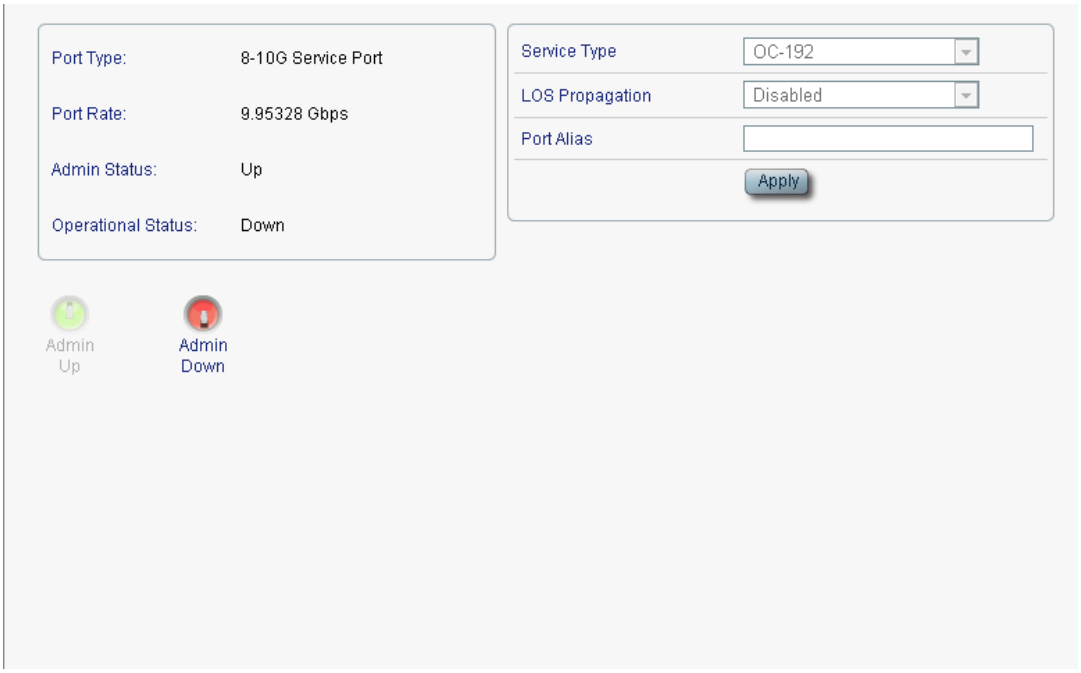


Figure 84: Port Tab

Use the Port tab to configure the service port in Muxponder mode and enable/disable the port.

To configure the service port in Muxponder mode:

1. Click the **Port** tab.

   The Port tab opens displaying the service port configuration in Muxponder mode.

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.

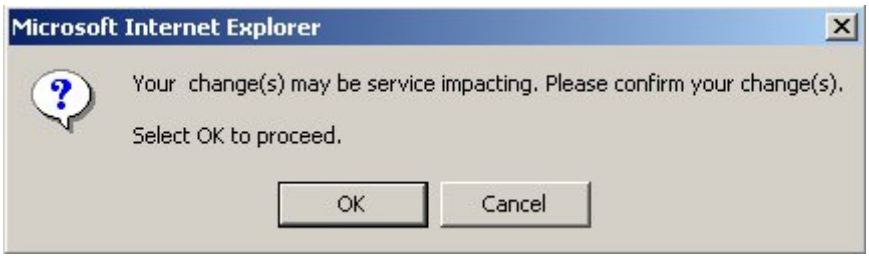


Figure 85: Confirm Changes

   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.

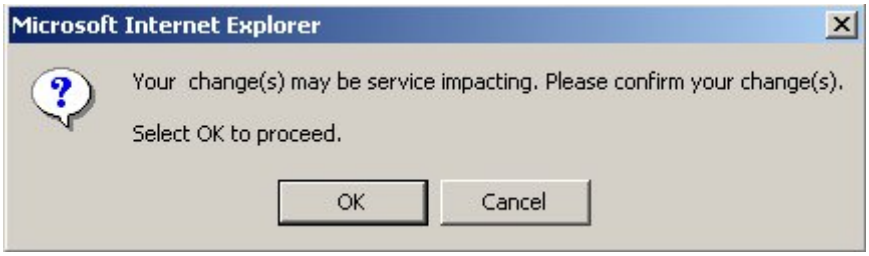


Figure 86: Confirm Changes

   2. Click **OK**.

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

Table 49: Port Tab

Parameter	Description	Format/Values
Port Type	The type of port.	• **Single 40G port**: 40G Service Port • **Dual 40G ports**: 40G Service Port • **No 40G ports**: 8-10G Service Port
Port Rate	The bit rate of the service.	• **Single 40G port**: 41.25 Gbps • **Dual 40G ports**: 41.25 Gbps • **No 40G ports**: 10.3125 Gbps
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**

Parameter	Description	Format / Values
Service Type	The type of service.	• **Single 40G port**: ▪ 40GbE-LAN ▪ OTU3 (future versions) ▪ OC-768 (future versions) ▪ STM-256 (future versions) • **Dual 40G ports**: ▪ 40GbE-LAN ▪ OTU3 (future versions) ▪ OC-768 (future versions) ▪ STM-256 (future versions) • **No 40G ports**: ▪ 10GBE-LAN ▪ 8G FC ▪ OC-192 ▪ STM-64 ▪ OTU2 ▪ OTU2e ▪ 10G FC (future versions) **NOTE:** Before changing the service type, you should **Admin Down** this port.
LOS Propagation	Enable or disable LOS propagation.	Enabled, Disabled **NOTE:** When **LOS Propagation** is enabled and a defect is detected on one of the service ports, the laser of the corresponding remote service port will be shut off.
Port Alias	The logical name given to the port for identification purposes.	Free text

6.6.2 QSFP+ Tab

Figure 87: QSFP+

NOTE: Applicable only for 40G service ports.

Use the QSFP+ tab to display information about the type and status of the optical transceiver inserted in the selected port.

To view QSFP+ information:

- Click the **QSFP+** tab.

  The QSFP+ tab opens. The fields are read only and explained in the following table.

Table 50: QSFP+ Tab

Parameter	Description	Format/Values
Vendor Name	The name of the QSFP+ vendor.	String
WDM Class	The type of QSFP+.	CWDM, No DWDM
Lanes #	The number of lanes used by the QSFP+.	4
Nominal Wavelength	The defined wavelength of the QSFP+.	nm
Max Bit Rate	The maximum bit rate supported by the QSFP+.	Gbps
Part Number	The part number of the QSFP+.	String
Serial Number	The serial number of the QSFP+.	String

Parameter	Description	Format/Values
Connector Type	The type of QSFP+ connector.	• **SR4**: MPO • **WDM**: 4 x LC
RX Pwr #	The measured input power of the QSFP+ per lane.	• **SR4**: Average dBm • **WDM**: 4 x dBm
Temperature	The measured temperature of the CFP.	Celsius
40GBE Capabilities	The QSFP+ capabilities of the 40GbE services are marked.	
OTU3 Capabilities	The QSFP+ capabilities of the OTU3 services are marked.	
High Receive Power Threshold	The threshold for the High Receive Power alarm.	dBm
Low Receive Power Threshold	The threshold for Low Receive Power alarm.	dBm

6.6.3 SFP+ Tab

Figure 88: SFP+ Tab

NOTE: Applicable only for 10G service ports.

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 receive power alarm threshold.

To configure the SFP+ module:

1. Click the **SFP+** tab.

   The SFP+ tab opens displaying the SFP+ module configuration.

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

Table 51: SFP+ Tab

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.	LC
Transmitter Output Power	The measured output power of the SFP+.	dBm
Receive Input Power	The measured input power of the SFP+.	dBm
Temperature	The measured temperature of the SFP+.	Celsius
ESCON Capabilities	The SFP+ capabilities of the ESCON services are marked.	
SONET/SDH Capabilities	The SFP+ capabilities of the OC-3, OC-12, OC-48, OC-192, and OTU-2 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 Receive Power Default Threshold	The default threshold for the High Receive Power alarm.	dBm
Low Receive Power Default Threshold	The default threshold for Low Receive Power alarm.	dBm
Override Low Receive Power Alarm Threshold	The configured threshold for the Low Receive Power alarm.	dBm

6.6.4 ALS Tab

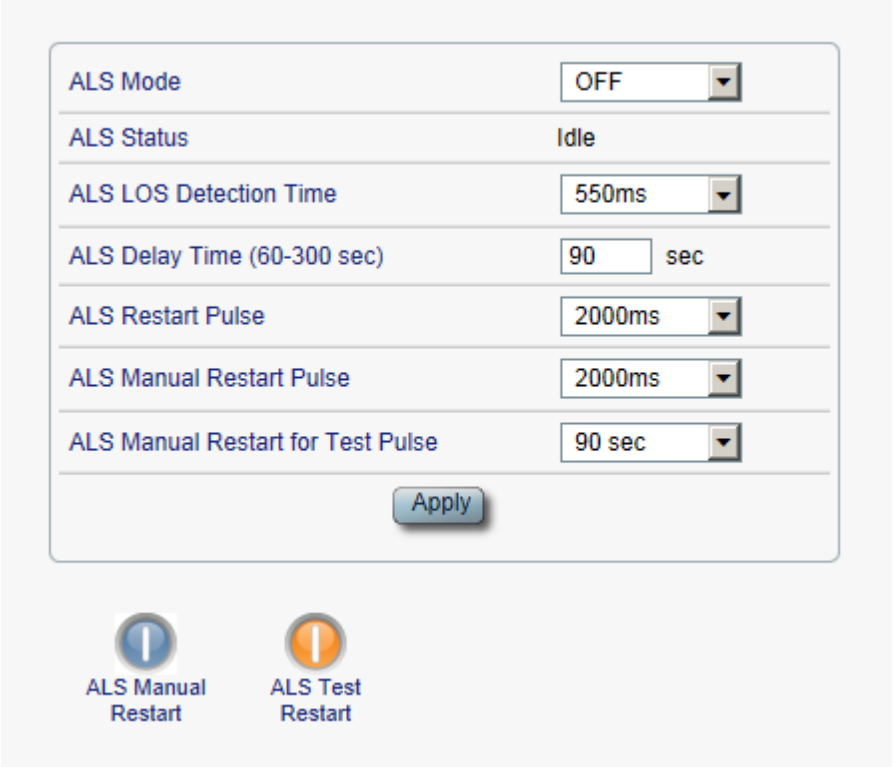


Figure 89: ALS Tab

Use the ALS tab to configure ALS for the 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-1000GT 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 52: 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.

6.7 Management Port Configuration

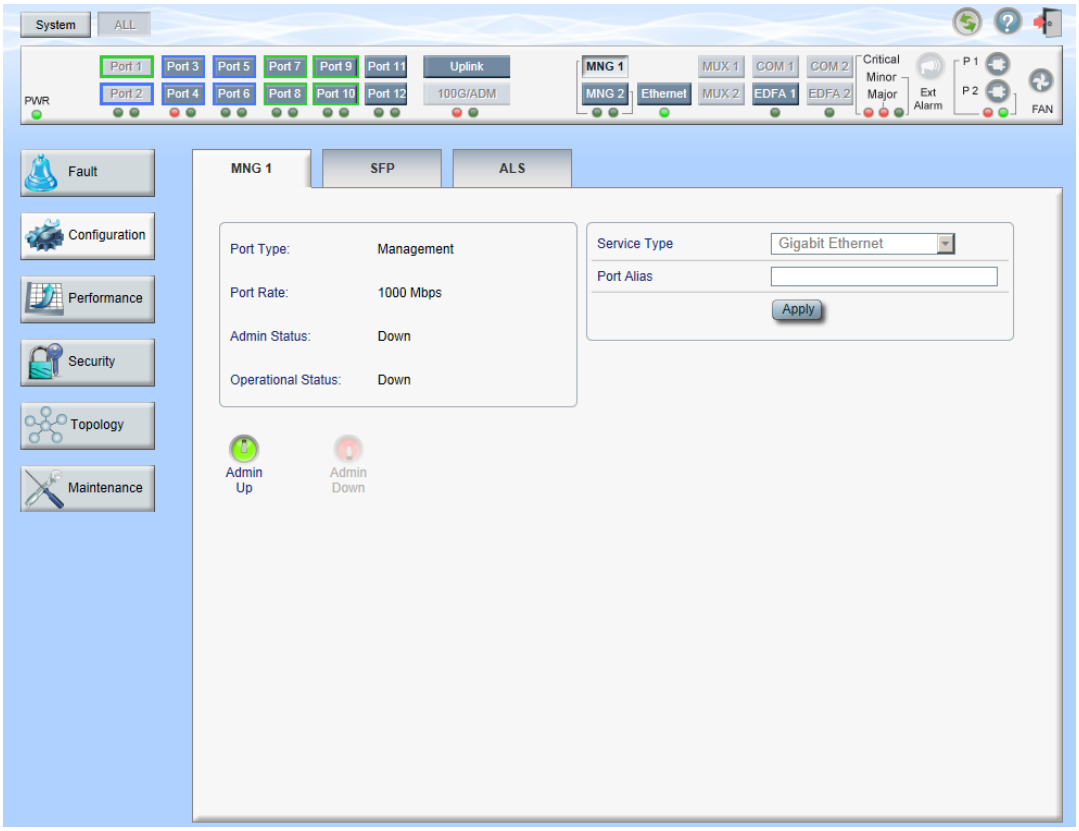


Figure 90: Management Port Configuration Window

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.

6.7.1 MNG Tab

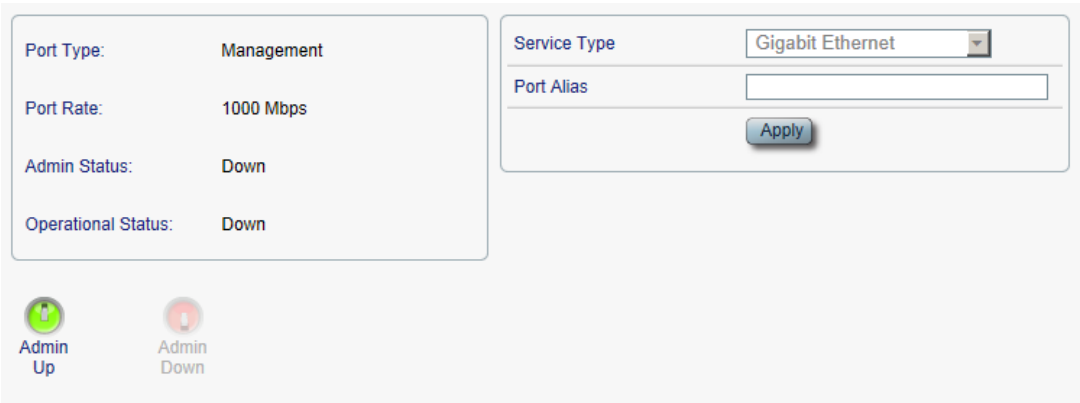


Figure 91: MNG Tab

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.

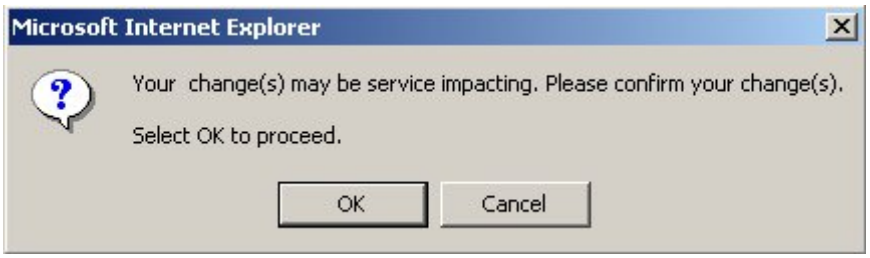


Figure 92: Confirm Changes

   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.

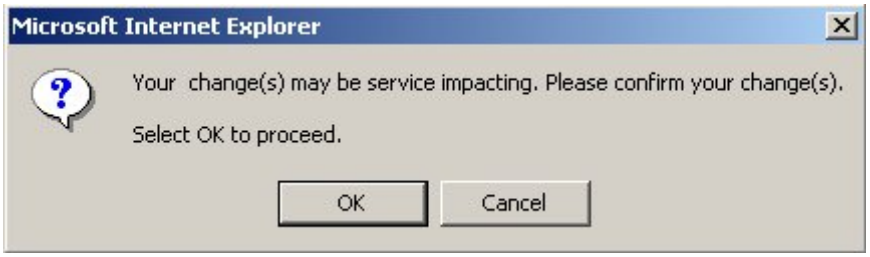


Figure 93: Confirm Changes

2. Click **OK**.

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

Table 53: 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.	1000 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, Gigabit Ethernet (default)
		NOTE:
		▪ This field is read only.
		▪ There is no **Auto Negotiation** on this port and it is configured with the following operation mode:
		  ▪ 100 Mbps or 1000 Mbps rate
		  ▪ Full duplex
		  ▪ No flow control
		▪ The selection between the rates is done automatically by trying both rates and searching for **Link Up** condition.

Port Alias	The logical name given to the port for identification purposes.	Free text

6.7.2 SFP Tab

Figure 94: SFP 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 receive 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 54: 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.	LC, Electrical RJ45

Parameter	Description	Format / Values
Transmitter Output Power	The measured output power of the SFP.	dBm
Receive Input Power	The measured input power of the SFP.	dBm
Temperature	The measured temperature of the SFP.	Celsius
ESCON Capabilities	The SFP capabilities of the ESCON services are marked.	
SONET/SDH Capabilities	The SFP capabilities of the OC-3, OC-12, OC-48, OC-192, and OTU-2 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 Receive Power Default Threshold	The default threshold for the High Receive Power alarm.	dBm
Low Receive Power Default Threshold	The default threshold for Low Receive Power alarm.	dBm
Override Low Receive Power Alarm Threshold	The configured threshold for the Low Receive Power alarm.	dBm

6.7.3 ALS Tab

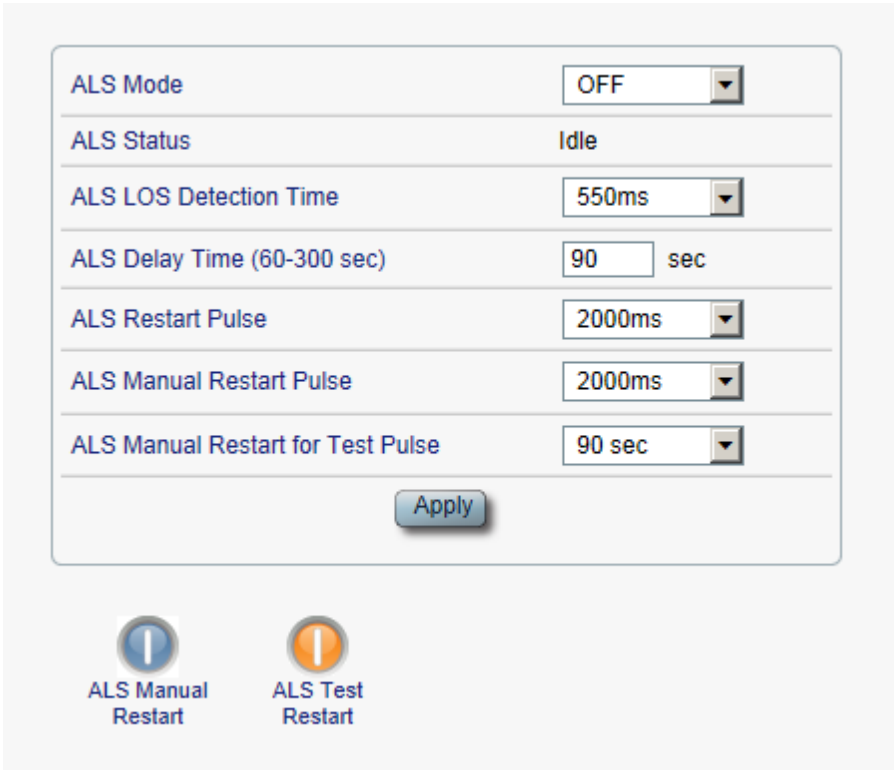


Figure 95: ALS Tab

Use the ALS tab to configure ALS for the 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-1000GT 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 55: 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.

6.8 Ethernet Port Configuration

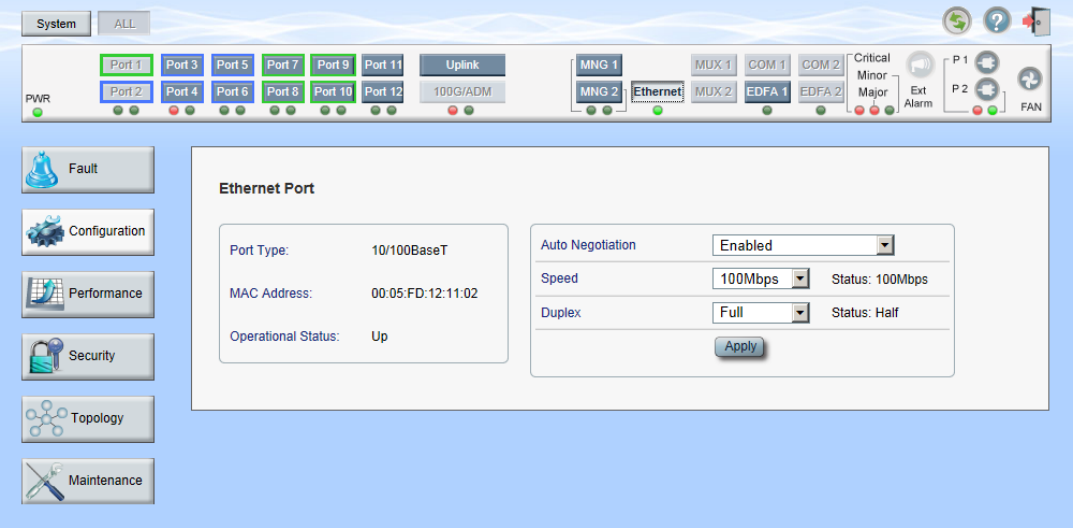


Figure 96: Ethernet Port Configuration Window

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.

6.8.1 Ethernet Tab

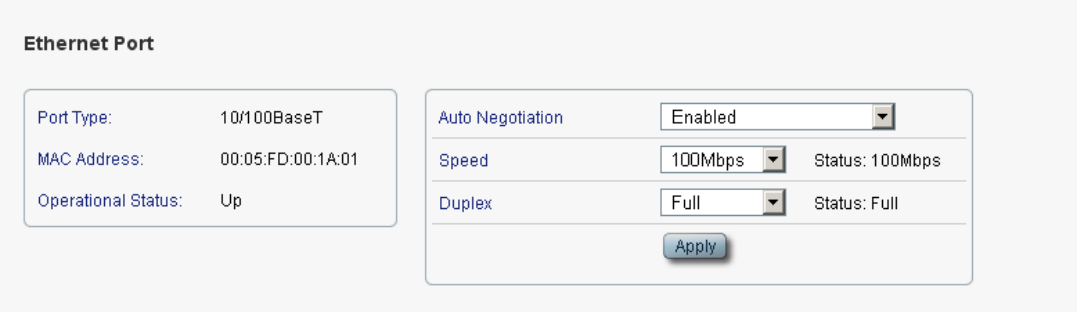


Figure 97: Ethernet Tab

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 56: 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**
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

6.9 EDFA Configuration

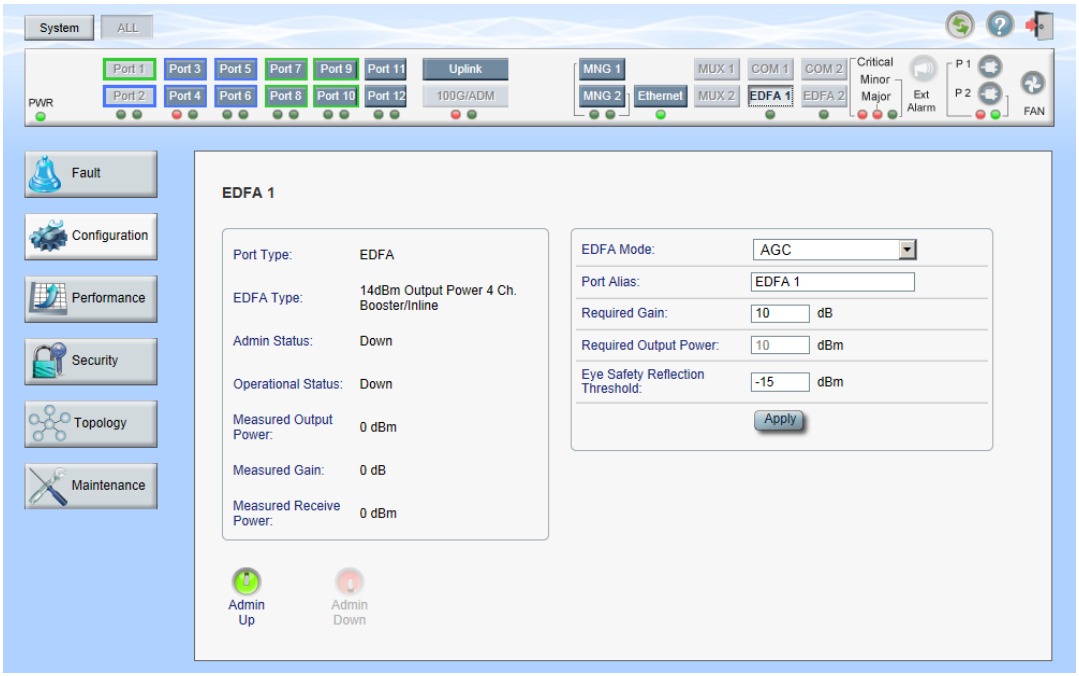


Figure 98: EDFA Configuration Window

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 **EDFA** to select the EDFA module.

   The EDFA Configuration window opens.

6.9.1 EDFA Tab

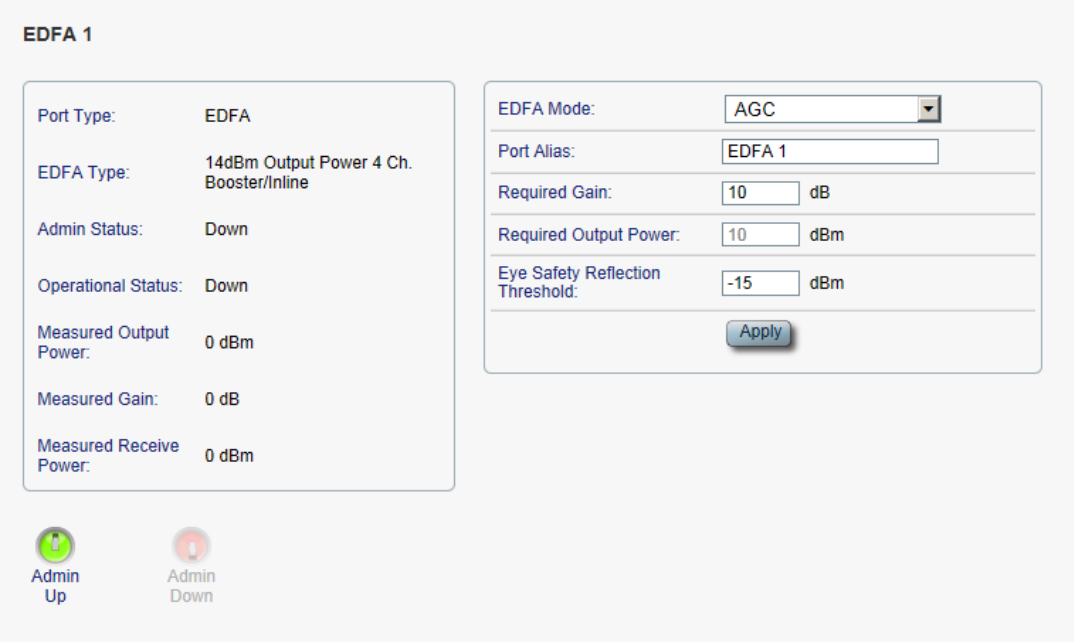


Figure 99: EDFA Tab

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.

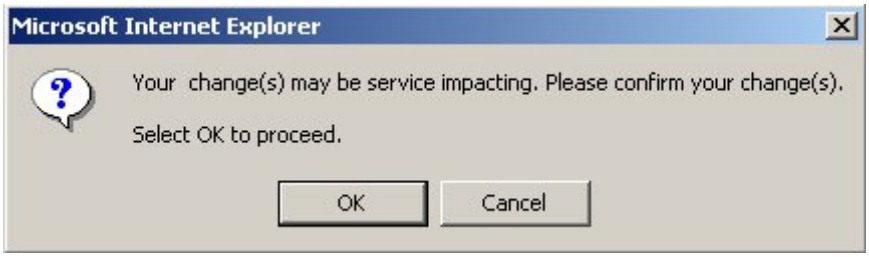


Figure 100: Confirm Changes

   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.

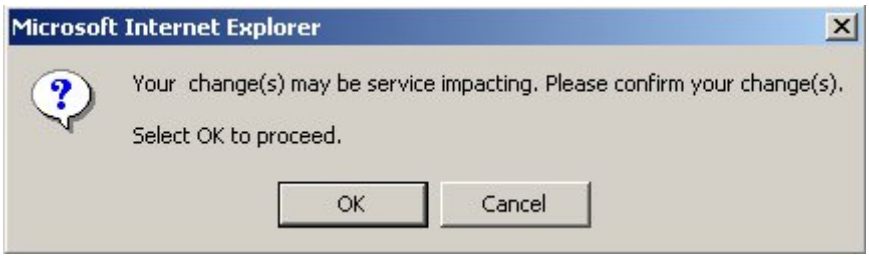


Figure 101: Confirm Changes

   2. Click **OK**.

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

Table 57: 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 module.	dBm
Measured Gain	The current measured gain of the EDFA module.	dB
Measured Receive Power	The current measured receive power of the EDFA module.	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.

Parameter	Description	Format / Values
Port Alias	The logical name given to the module for identification purposes.	Free text
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

6.10 PSU Configuration

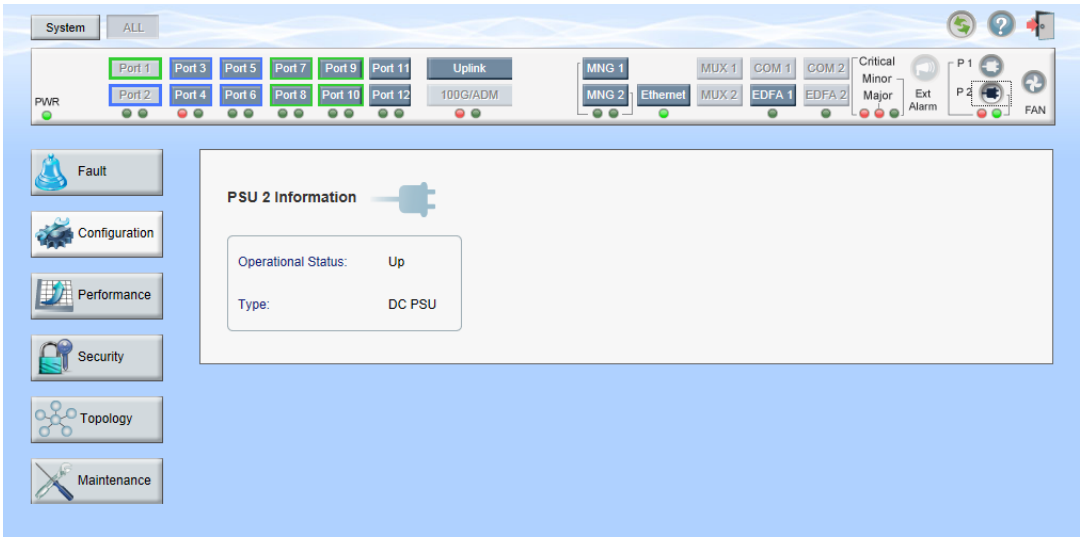


Figure 102: PSU Configuration Window

Use the PSU Configuration Window to view information about the power supply units.

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.

6.10.1 PSU Tab

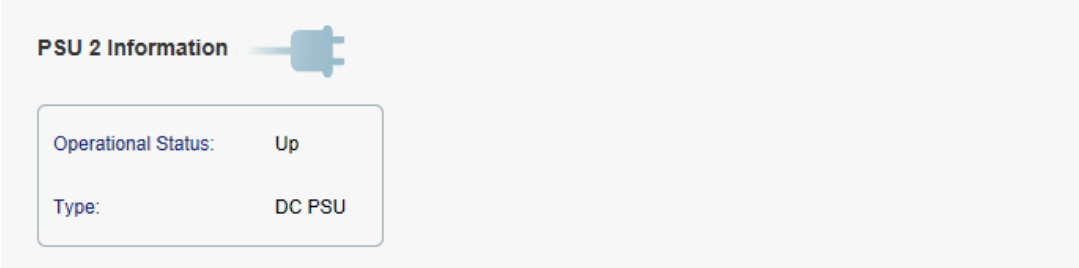


Figure 103: PSU Tab

Use the PSU tab to view information about the power supply units.

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 58: PSU Tab Parameters

Parameter	Description	Format / Values
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.	DC PSU

6.11 FAN Unit Configuration

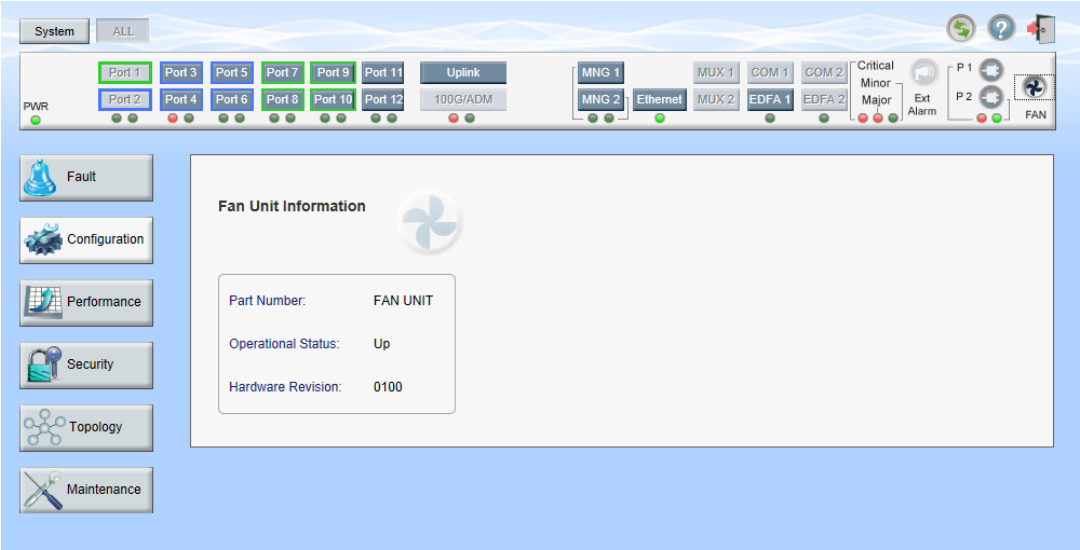


Figure 104: FAN Unit Configuration Window

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** to select the FAN unit.

   The FAN Unit Configuration window opens.

6.11.1 FAN Unit Tab

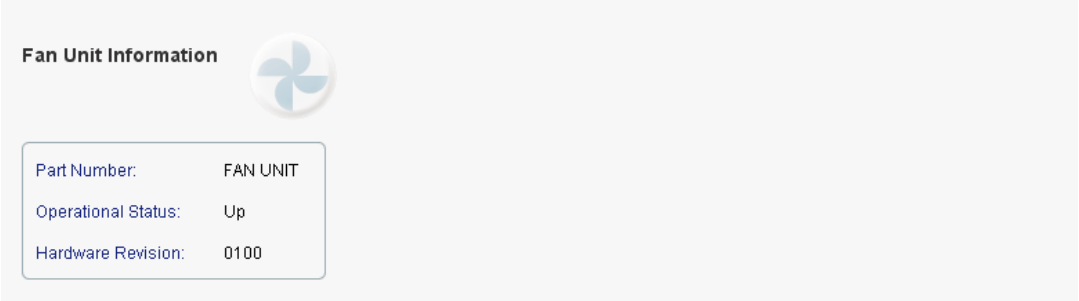


Figure 105: FAN Unit Tab

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

Table 59: 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-1000GT system optical information and port performance monitoring.

In this Chapter

7.1 System Optical Information

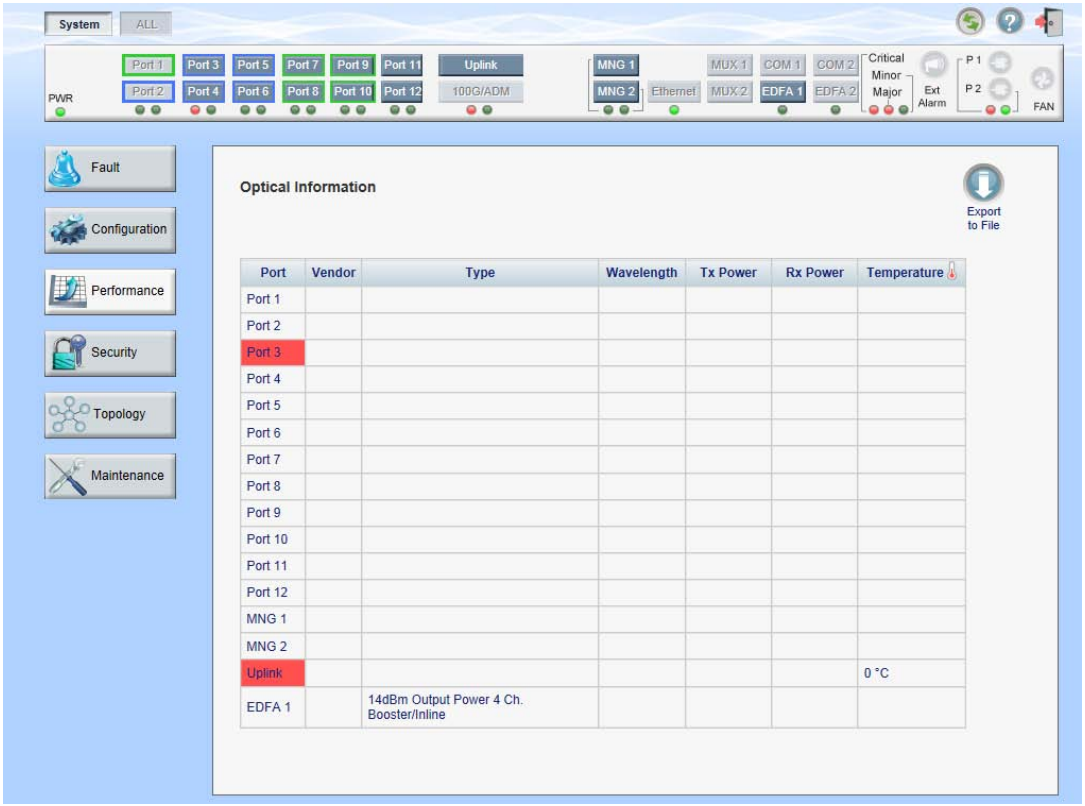


Figure 106: Optical Information Window

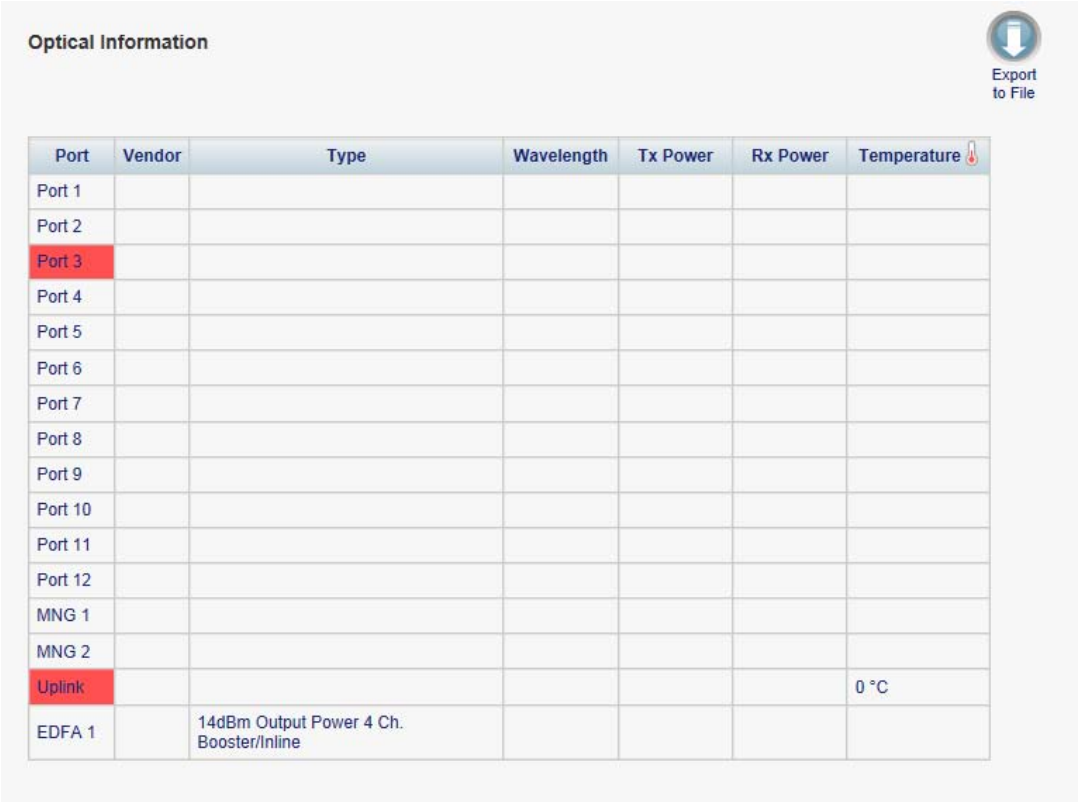
Use the Optical Information window to view the optical performance of all optical modules installed in the system.

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
Port 1						
Port 2						
Port 3						
Port 4						
Port 5						
Port 6						
Port 7						
Port 8						
Port 9						
Port 10						
Port 11						
Port 12						
MNG 1						
MNG 2						
Uplink						0 °C
EDFA 1		14dBm Output Power 4 Ch. Booster/Inline				

Figure 107: Optical Information Tab

Use the Optical Information tab to view the system optical information.

To view the system optical information:

1. Click **System**.

   The Optical Information tab opens displaying the system 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 60: 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 Port Performance Monitoring

The PL-1000GT provides port performance monitoring for the following:

- Uplink port
  - **OTU Section**: PM counters are based on OTU Section BIP-8 errors.
  - **OTU Far Section**: PM counters are based on OTU Far Section BIP-8 errors.
  - **ODU Path**: PM counters are based on ODU Path BIP-8 errors.
  - **ODU Far Path**: PM counters are based on ODU Far Path BIP-8 errors.
  - **OTN FEC Corrected Errors**: PM counters are based on FEC corrected errors.
  - **OTN FEC Uncorrected Errors**: PM counters are based on FEC uncorrected errors.
  - **OTN FEC Corrected Error Ratio**: The Bit Error Ratio of the corrected FEC errors.
- Service ports (100G/ADM and Port 1 to Port 12). Native Signal PM for all ports according to the following service types:
  - **100GbE-LAN, 40GbE-LAN, and 10GbE-LAN**: PM is based on the 64B/66B coding violation errors.
  - **8G FC**: PM is based on 8B/10B coding violations errors.
  - **OC-192 (SONET) and STM-64 (SDH)**: PM is based on the B1 coding violation errors.
  - **OTU2 and OTU2e**: PM is based on OTU BIP8 errors, FEC corrected errors, and FEC uncorrected errors.

- Optical Level PM. This is based on the measured Rx power:
  - Uplink port
  - Service ports
  - MNG 1 - MNG 2
  - EDFA 1 - EDFA 2 (if present)

7.3 Uplink Port Performance Monitoring

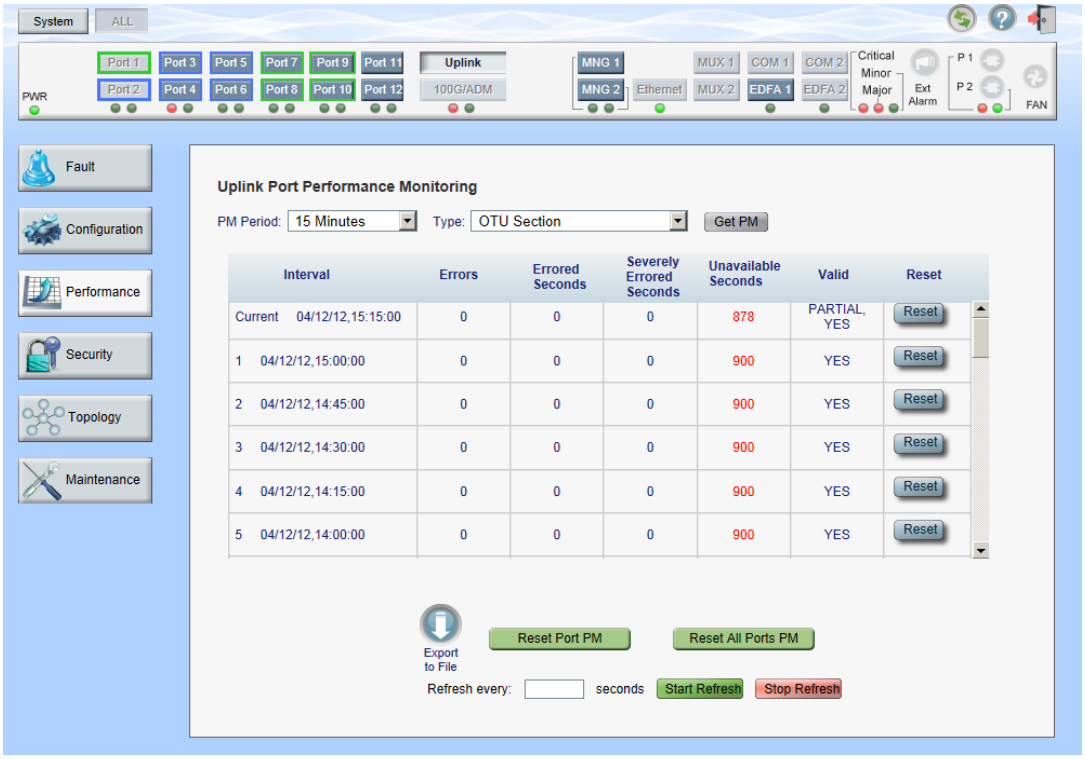


Figure 108: Uplink Port Performance Monitoring Window

Use the Uplink Port Performance Monitoring window to view uplink port performance monitoring.

To open the Uplink Port Performance Monitoring window:

1. Click **Performance**.
2. Click **Uplink** to select the uplink port.

   The Uplink Port Performance Monitoring window opens.

7.3.1 Viewing Uplink Port OTN Performance Monitoring

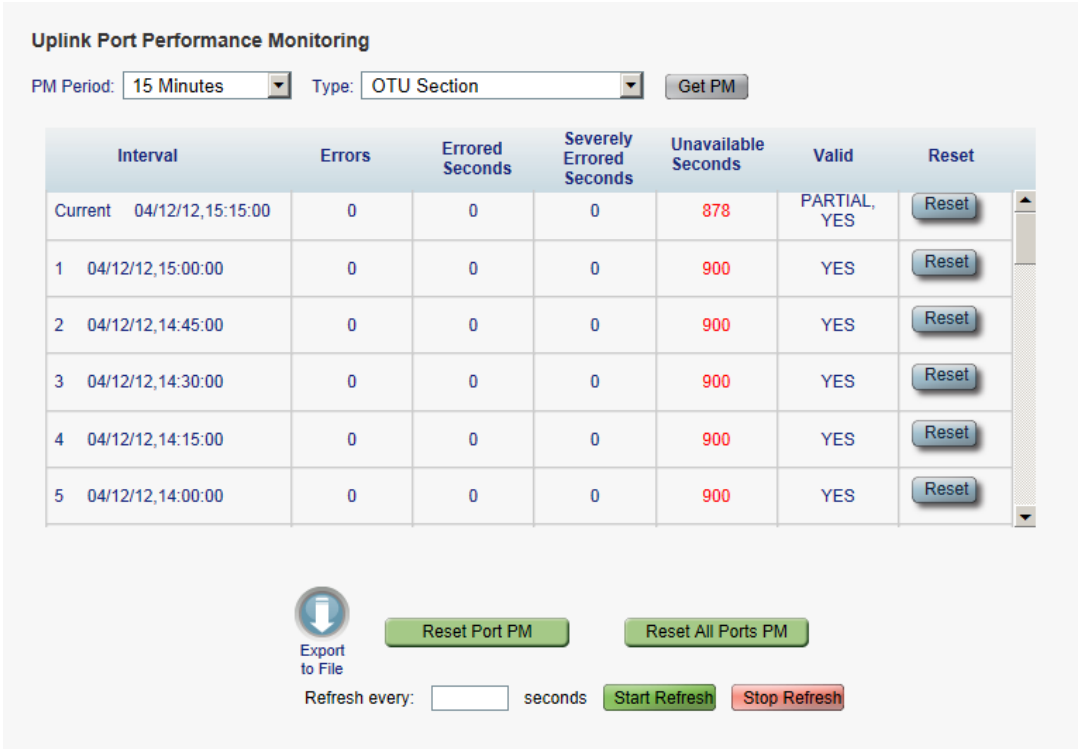


Figure 109: Uplink Port Performance Monitoring Tab

Figure 110: Uplink Port Performance Monitoring Tab - OTN FEC Corrected Error Ratio

Use the Uplink Port Performance Monitoring tab to view uplink port performance monitoring.

To view uplink port performance monitoring:

1. Click **Uplink** to select the uplink port.

   The Uplink Port Performance Monitoring tab opens displaying the uplink port performance monitoring.

2. From the **PM Period** drop-down list, select **15 Minutes** or **Days**.
3. From the **Type** drop-down list, select the type of performance monitoring.
4. Click **Get PM**.

   The performance monitoring counters are updated. The counters are read only.

5. To export the PM 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 PM counters for a specific PM interval, in the table, at the end of the interval row, click **Reset**.

10. To clear PM counters for a specific port, click **Reset Port PM**.

11. To clear PM counters for all ports, click **Reset All Ports PM**.

Table 61: Uplink Port Performance Monitoring Tab

Parameter	Description	Format/Values
PM Period	The interval for accumulating and displaying the performance monitoring counters.	15 Minutes, Days
Type	The type of performance monitoring.	• OTU Section • OTU Far Section • ODU Path • ODU Far Path • OTN FEC Corrected Errors • OTN FEC Uncorrected Errors • OTN FEC Corrected Error Ratio

Parameter	Description	Format / Values
Interval	The date and time of the interval.	**PM Period is set to 15 Minutes**: • **Current**: Performance monitoring counters accumulated during the current interval of 15 minutes are displayed in the first row. • **1 to 32**: Performance monitoring counters accumulated during the last 32 intervals of 15 minutes are displayed in the second row to the last row of the table. **PM Period is set to Days**: • **Untimed**: Performance monitoring counters accumulated since last reset of the system or since the last reset of the performance monitoring counters are displayed in the first row of the table. • **Current Day**: Performance monitoring counters accumulated since 00:00 AM of the current day are displayed in the second row of the table. • **Previous Day**: Performance monitoring counters accumulated during the 24 hours since 00:00 AM of the previous day are displayed in the last row of the table.
Errors	• **OTU Section and OTU Far Section**: The number of OTU Section BIP-8 errors detected during the performance monitoring interval. • **ODU Path and ODU Far Path**: The number of ODU Path BIP-8 errors detected during the performance monitoring interval. • **OTN Corrected FEC Errors**: The number of corrected FEC errors detected during the performance monitoring interval. • **OTN Uncorrected FEC Errors**: The number of uncorrected FEC errors detected during the performance monitoring interval.	Number of errors
Errored Seconds	The number of seconds in which at least one error was detected.	Number of seconds

Parameter	Description	Format / Values
Severely Errored Seconds	The number of seconds in which the number of errors detected crossed the threshold.	Number of seconds **NOTE:** ▪ The counter stops when the number of errors detected during the last second is below the threshold or the **Unavailable Seconds** counter is incremented. ▪ The counter is not applicable for **OTN FEC Corrected Errors, OTN FEC Uncorrected Errors, and OTN FEC Corrected Error Ratio**.
Unavailable Seconds	The **Unavailable Seconds** counter is incremented when 10 consecutive **Severely Errored Seconds** are detected during the last 10 seconds.	Number of seconds **NOTE:** The counter is not applicable for **OTN FEC Corrected Errors, OTN FEC Uncorrected Errors** and **OTN FEC Corrected Error Ratio**.
Valid	Whether or not the performance monitoring interval has been completed, and whether or not the information is accurate.	• **Partial**: The measured interval has not been completed. • **Yes**: The performance monitoring interval has been completed. • **No**: The interval has been completed, but the performance monitoring information may not be accurate. The performance monitoring information may be inaccurate due to one of the following reasons: ▪ The performance monitoring counters of the interval were reset. ▪ The node was reset during the interval. ▪ The port was set to **Admin Down** during the interval. ▪ The calendar time of the node was changed during the interval.
Corrected Error Ratio	The Bit Error Ratio of the corrected FEC errors.	Ratio **NOTE:** This field is only applicable for **OTN FEC Corrected Error Ratio**.

7.3.2 Viewing Uplink Port Optical Level Performance Monitoring

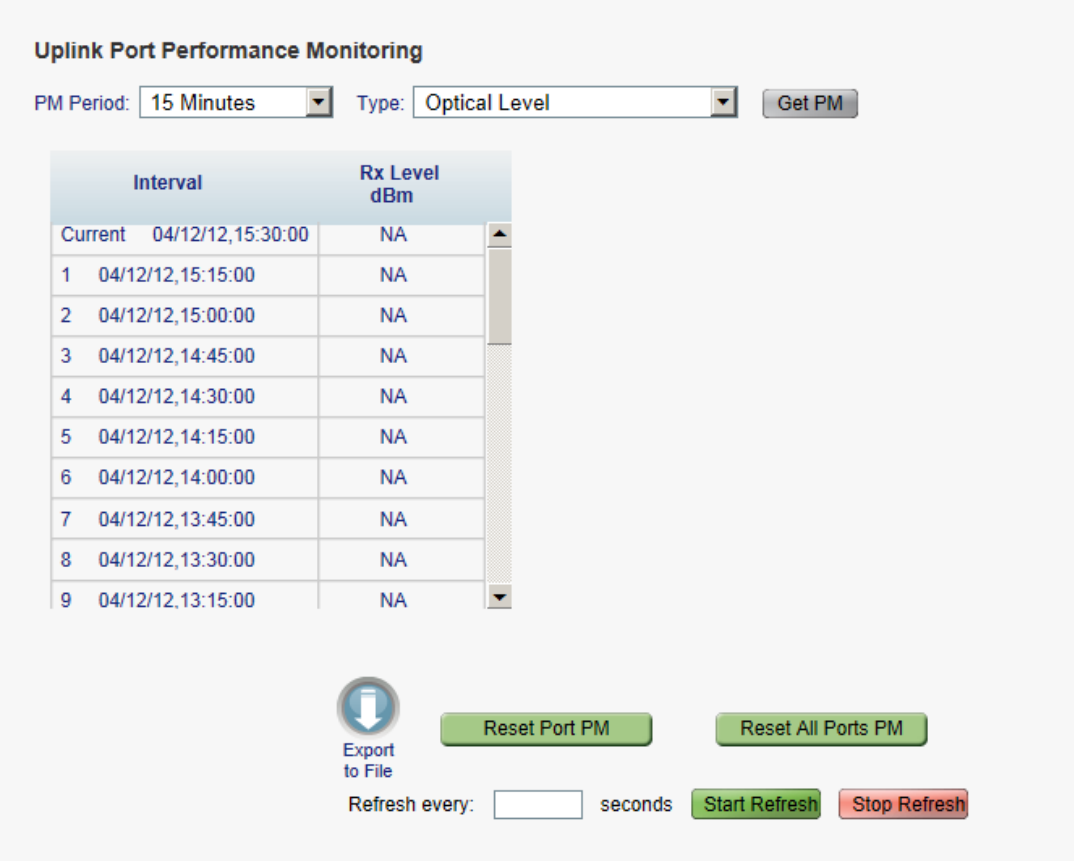


Figure 111: Optical Level Performance Monitoring

Use the Uplink Port Performance Monitoring tab to view uplink port optical level performance monitoring.

To view optical level performance monitoring:

1. Click **Uplink** to select the uplink port.

   The Uplink Port Performance Monitoring tab opens displaying the uplink port performance monitoring.

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 62: Uplink Port Performance Monitoring Tab 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.

7.4 Service Port Performance Monitoring

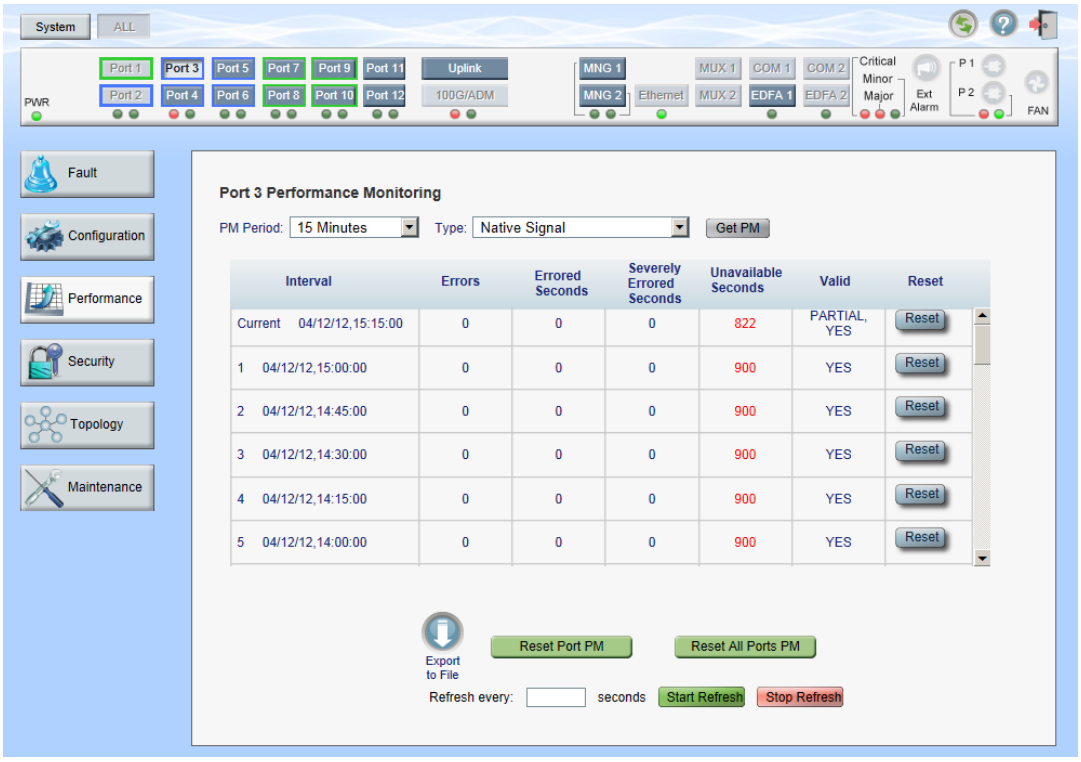


Figure 112: Service Port Performance Monitoring Window

Use the Service Port Performance Monitoring window to view the service port performance monitoring.

To open the Service Port Performance Monitoring window:

1. Click **Performance**.
2. Click **100G/ADM** or a **Port** button to select the service port.

   The appropriate Service Port Performance Monitoring window opens.

7.4.1 Viewing Service Port Native Signal Performance Monitoring

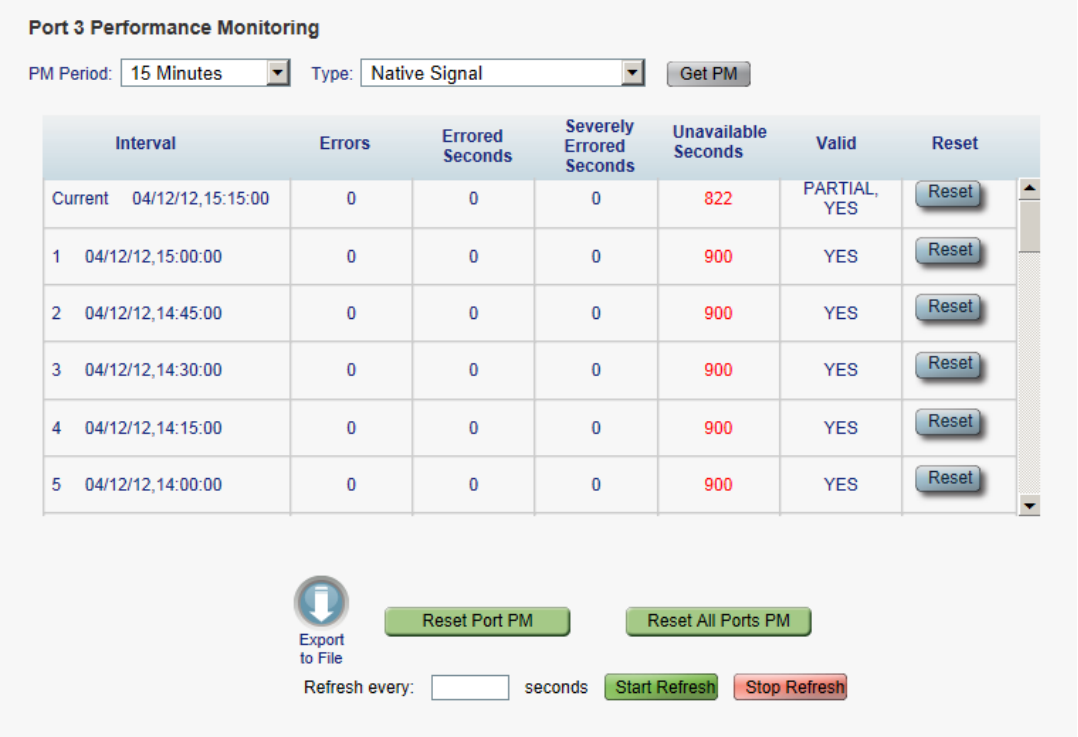


Figure 113: Service Port Performance Monitoring Tab

Use the Service Port Performance Monitoring tab to view service port native signal performance monitoring.

To view native signal performance monitoring:

1. Click **100G/ADM** or a **Port** button to select the service port.

   The appropriate Service Port Performance Monitoring tab opens displaying the service 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 **Native Signal**.
4. Click **Get PM**.

   The performance monitoring counters are updated.

5. To export the PM 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 PM counters for a specific PM interval, in the table, at the end of the interval row, click **Reset**.
10. To clear PM counters for a specific port, click **Reset Port PM**.
11. To clear PM counters for all ports, click **Reset All Ports PM**.

Table 63: Service Port Performance Monitoring Tab

Parameter	Description	Format / Values
PM Period	The interval for accumulating and displaying the performance monitoring counters.	15 Minutes, Days
Type	The type of performance monitoring.	Native Signal
Interval	The date and time of the interval.	**PM Period is set to 15 Minutes**: • **Current**: Performance monitoring counters accumulated during the current interval of 15 minutes are displayed in the first row. • **1 to 32**: Performance monitoring counters accumulated during the last 32 intervals of 15 minutes are displayed in the second row to the last row of the table. **PM Period is set to Days**: • **Untimed**: Performance monitoring counters accumulated since last reset of the system or since the last reset of the performance monitoring counters are displayed in the first row of the table. • **Current Day**: Performance monitoring counters accumulated since 00:00 AM of the current day are displayed in the second row of the table. • **Previous Day**: Performance monitoring counters accumulated during the 24 hours since 00:00 AM of the previous day are displayed in the last row of the table.

Parameter	Description	Format/Values
• Background Block Errors (SDH) *or* • Errors (Other)	• **10GbE-LAN, 40GbE-LAN, and 100GbE-LAN services**: The number of 64B/66B coding violation errors detected during the performance monitoring interval. • **8G FC services**: The number of 8B/10B coding violation errors detected during the performance monitoring interval. • **OC-192 (SONET) and STM-64 (SDH) services**: The number of Section B1 errors detected during the performance monitoring interval. • **OTU2 and OTU2e services**: The number of OTU BIP8 errors, FEC corrected errors, and FEC uncorrected errors.	Number of errors
Errored Seconds	The number of seconds in which at least one error was detected.	Number of seconds
Severely Errored Seconds	The number of seconds in which the number of errors detected crossed the threshold.	Number of seconds **NOTE:** The counter stops when the number of errors detected during the last second is below the threshold or the **Unavailable Seconds** counter is incremented.
• Severely Errored Frame Seconds (SONET) *or* • Out of Frame Seconds (SDH) *or* • Unavailable Seconds (Other)	• **GbE and FC services**: The **Unavailable Seconds** counter is incremented when 10 consecutive **Severely Errored Seconds** are detected during the last 10 seconds. • **SONET/SDH services**: The number of seconds in which four consecutive incorrect frames are detected.	Number of seconds

Parameter	Description	Format / Values
Valid	Whether or not the performance monitoring interval has been completed, and whether or not the information is accurate.	• **Partial**: The measured interval has not been completed. • **Yes**: The performance monitoring interval has been completed. • **No**: The interval has been completed, but the performance monitoring information may not be accurate. The performance monitoring information may be inaccurate due to one of the following reasons: ▪ The performance monitoring counters of the interval were reset. ▪ The node was reset during the interval. ▪ The port was set to **Admin Down** during the interval. ▪ The calendar time of the node was changed during the interval.

7.4.2 Viewing Service Port Optical Level Performance Monitoring

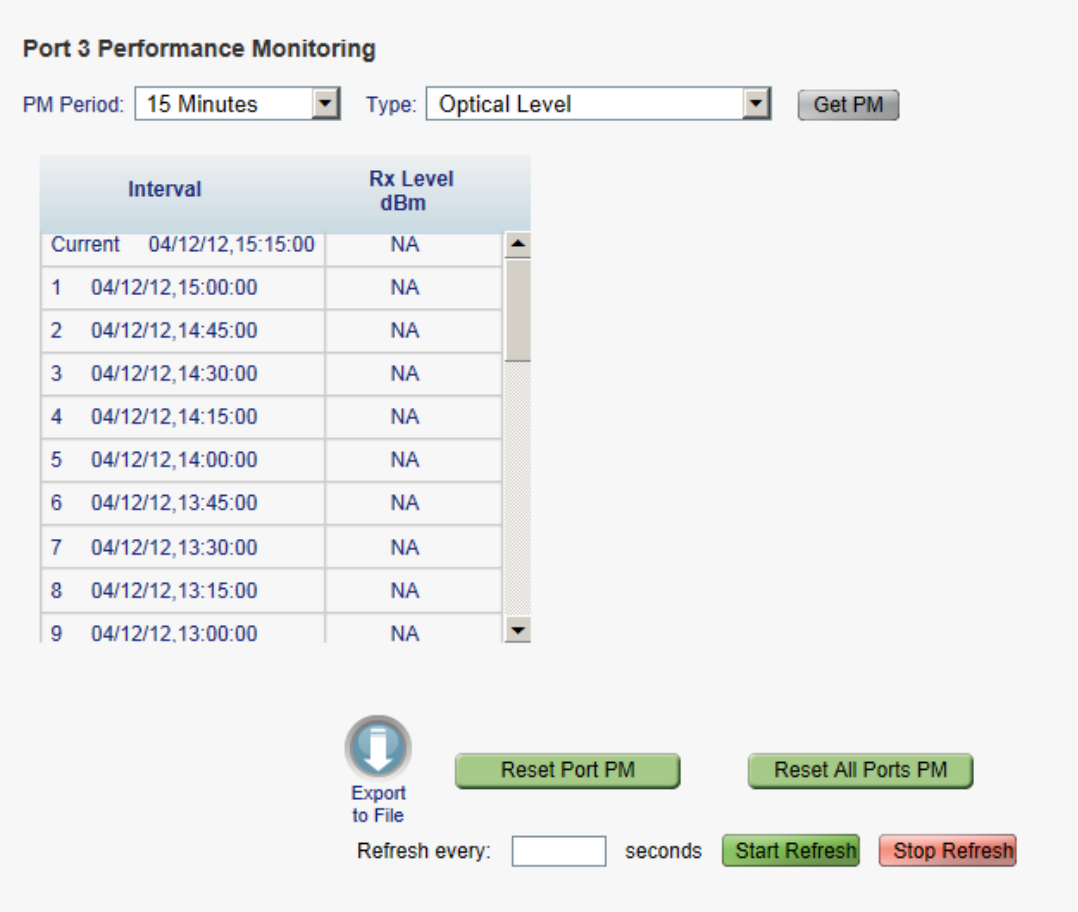


Figure 114: Optical Level Performance Monitoring

Use the Service Port Performance Monitoring tab to view service port optical level performance monitoring.

To view optical level performance monitoring:

1. Click **100G/ADM** or a **Port** button to select the service port.

   The appropriate Service Port Performance Monitoring tab opens displaying the displaying the service 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 64: Service Port Performance Monitoring Tab 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.

7.5 Management Port Performance Monitoring

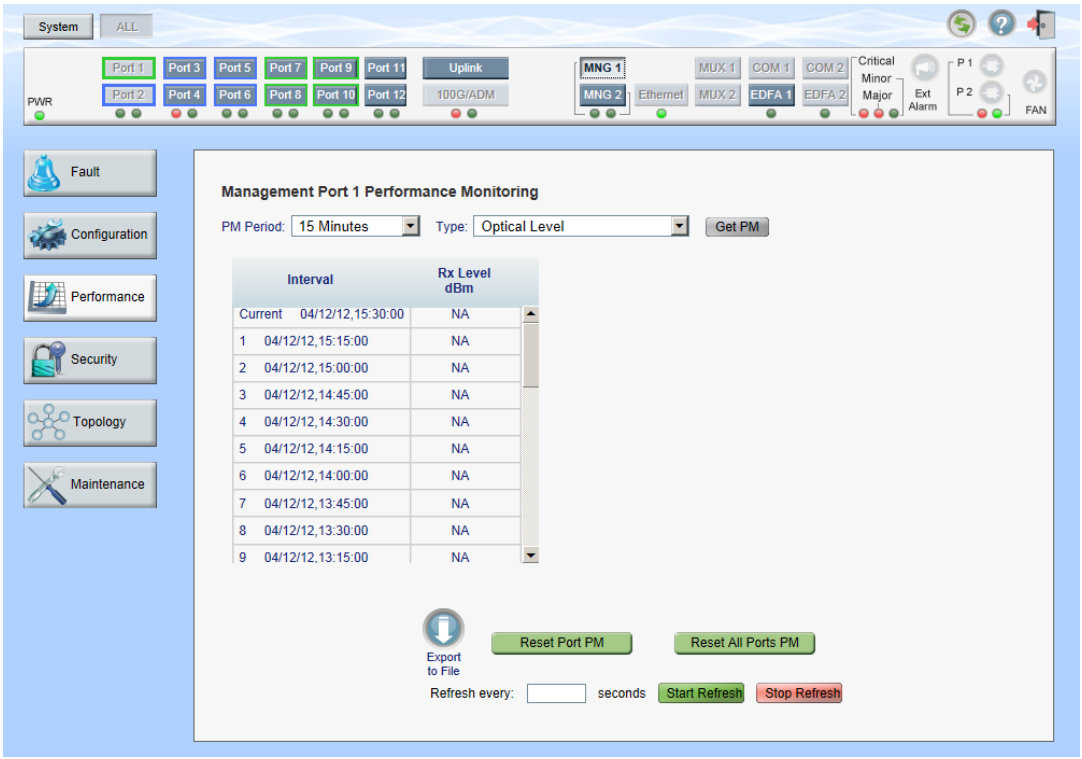


Figure 115: Management Port Performance Monitoring Window

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.

7.5.1 Viewing Management Port Optical Performance Monitoring

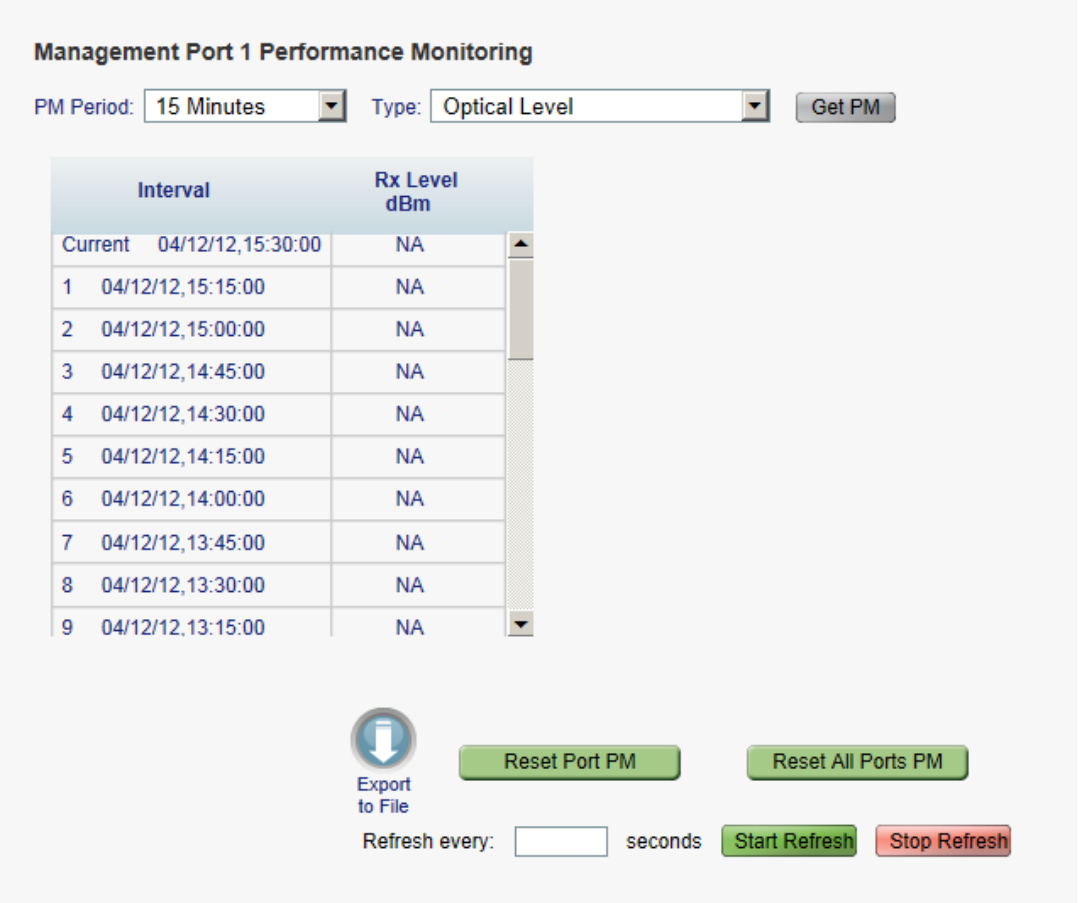


Figure 116: Optical Level Performance Monitoring

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 65: 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.
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.

7.6 EDFA Performance Monitoring

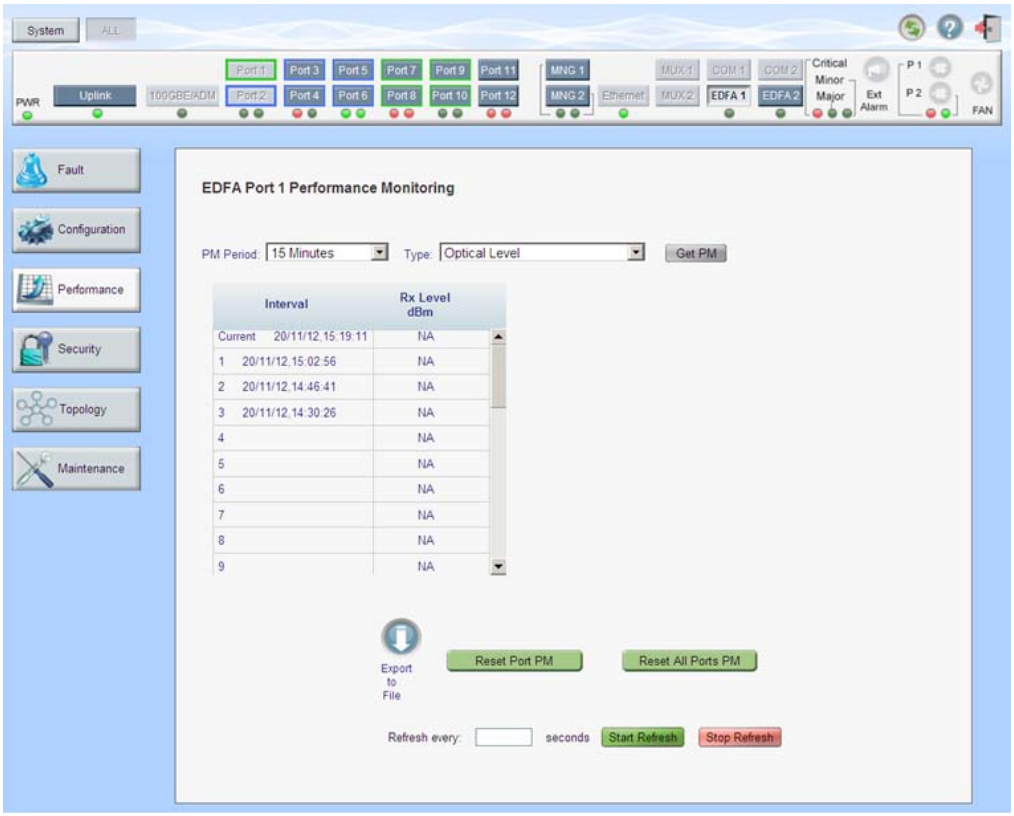


Figure 117: EDFA Performance Monitoring Window

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 **EDFA** to select the EDFA module.

   The EDFA Performance Monitoring window opens.

7.6.1 Viewing EDFA Optical Performance Monitoring

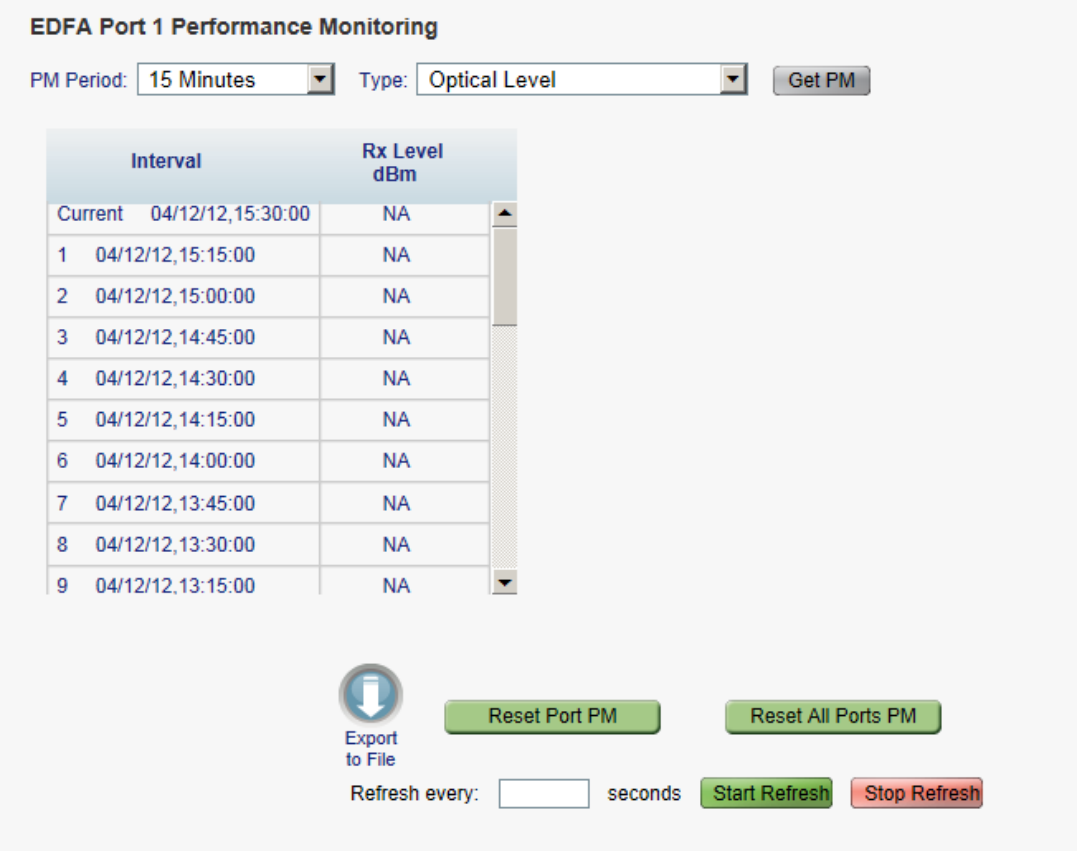


Figure 118: Optical Level Performance Monitoring

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

To view optical level performance monitoring:

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

   The 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 66: EDFA Performance Monitoring Tab 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-1000GT.

In this Chapter

8.1 System Maintenance

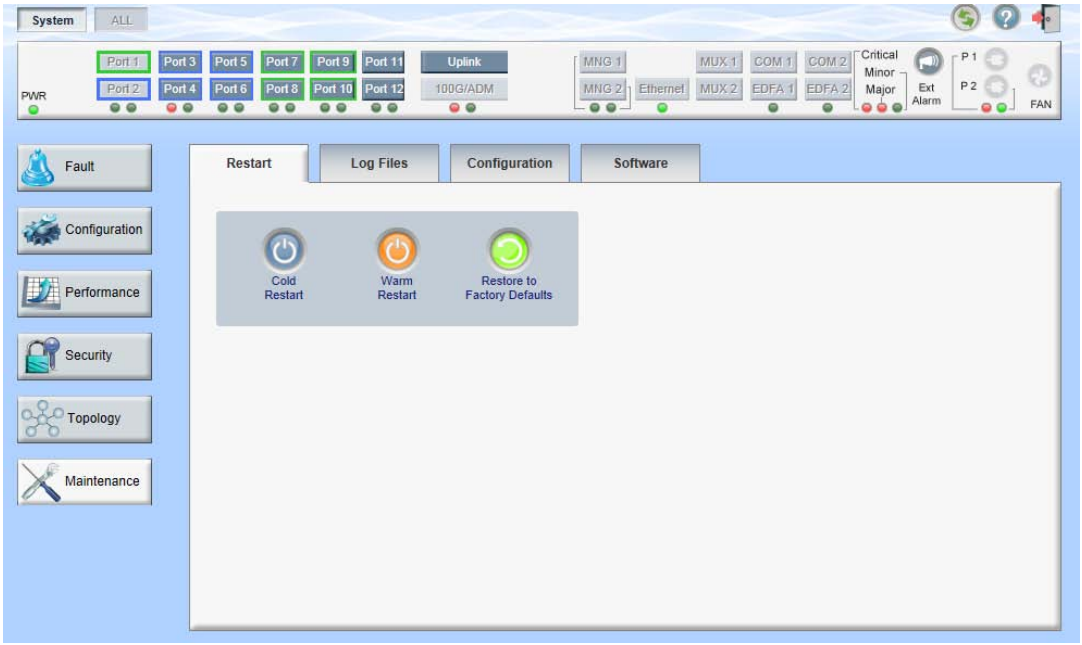


Figure 119: System Maintenance Window

Use the System Maintenance window to do the following:

- **Restart tab**: Restart the PL-1000GT unit
- **Log Files tab**: View and save the System Log files
- **Configuration tab**:
  - **Download Configuration File**: Update system configuration by downloading a previously saved system configuration file to the node
  - **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

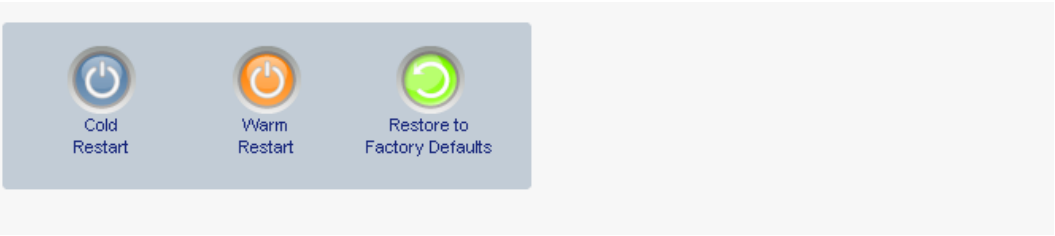


Figure 120: Restart Tab

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 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-1000GT 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.

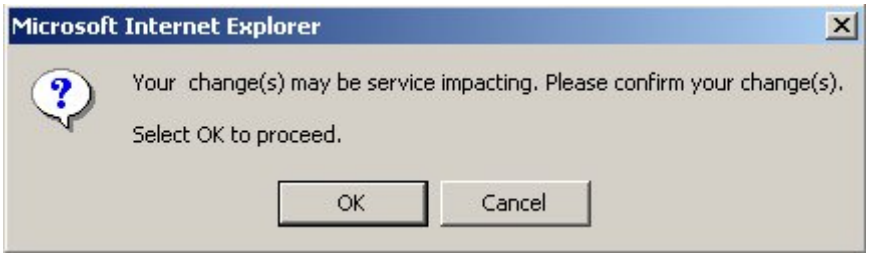


Figure 121: Confirm Changes

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.

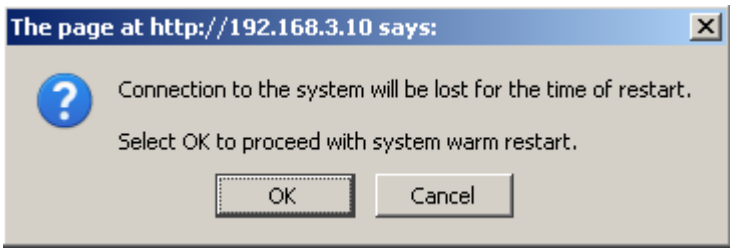
      

      Figure 122: Confirm Changes

   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.

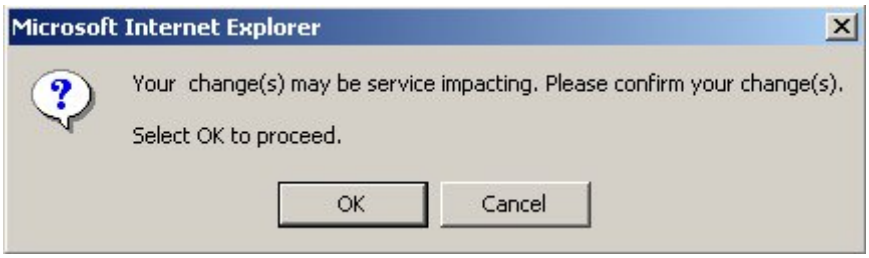
      

      Figure 123: Confirm Changes

   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 124: 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 125: System Log Files (Example)

8.1.3 Configuration Tab

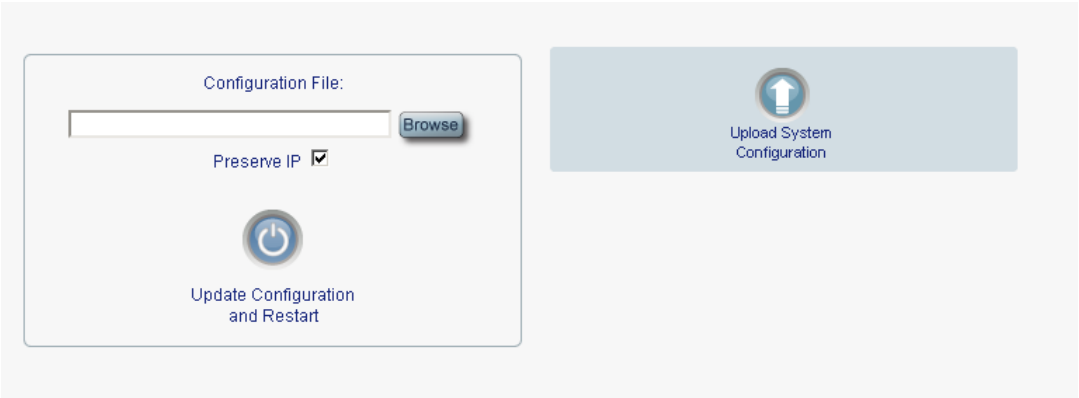


Figure 126: Configuration Tab

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-1000GT unit
- Upload the current system configuration of the PL-1000GT unit and save it to the local file system

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

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

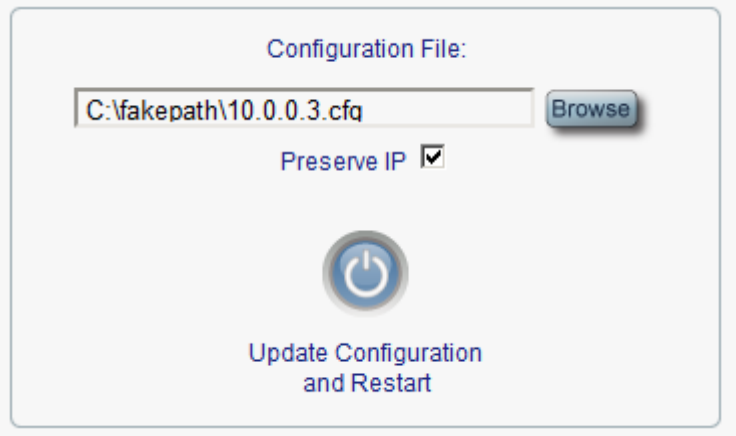


Figure 127: Update System Configuration: Configuration File

3. To preserve the IP addresses, select the Preserve IP check box.
4. Click **Update Configuration and Restart**  .

   The following confirmation message appears.

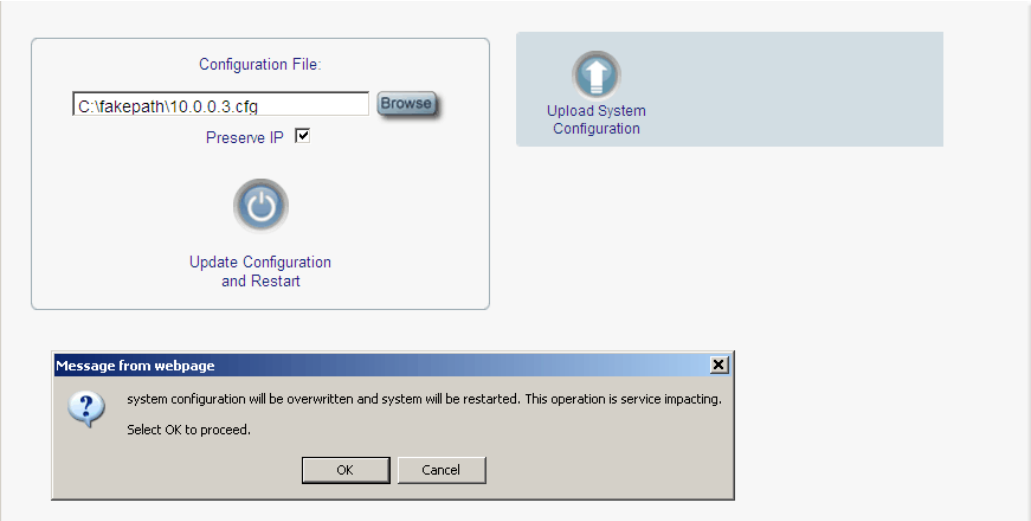


Figure 128: Confirm System Overwrite

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 129: 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.

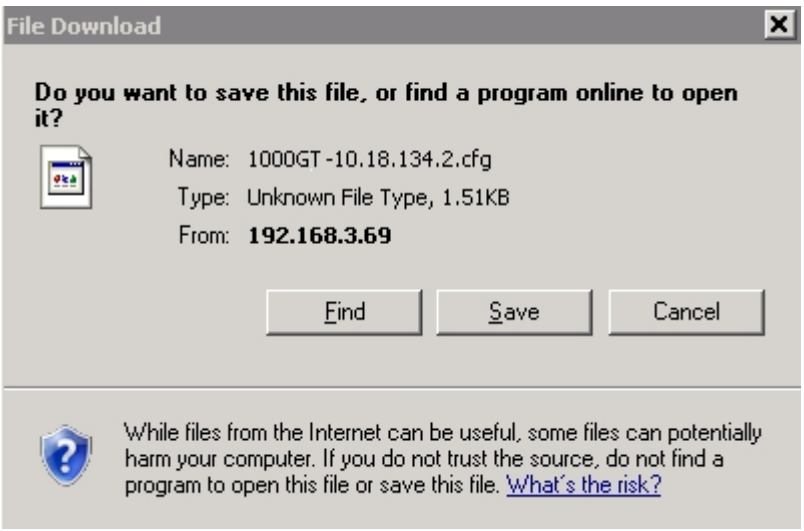


Figure 130: Opening .cfg Dialog Box

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

8.1.4 Software Tab

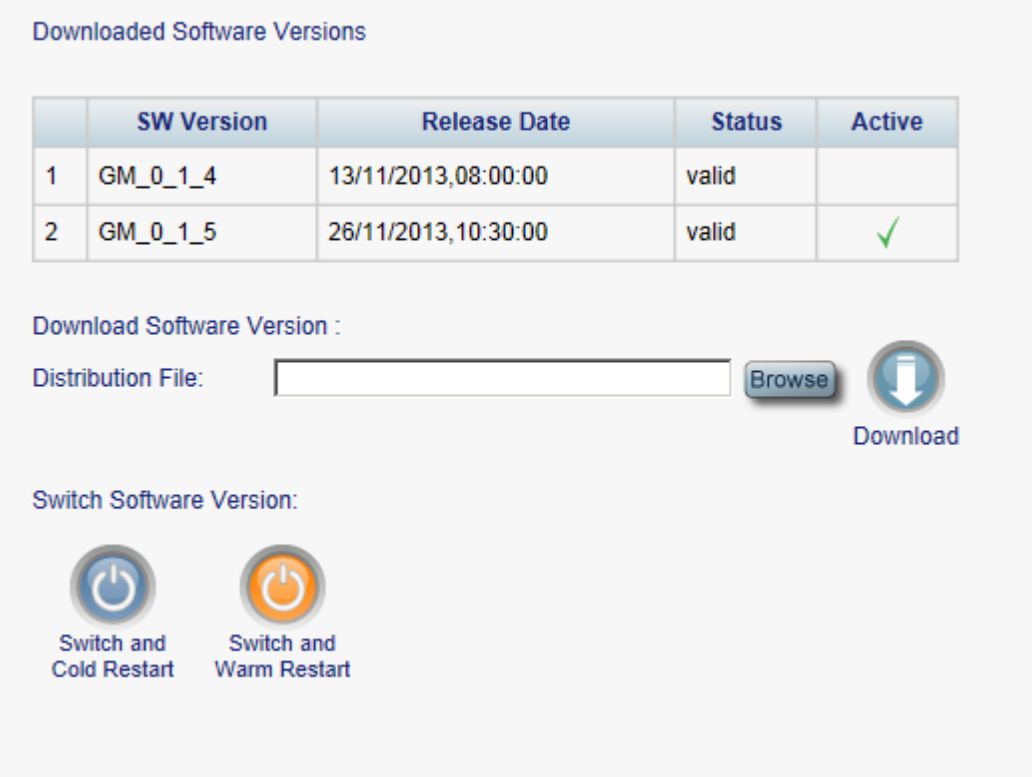


Figure 131: Software Tab

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.

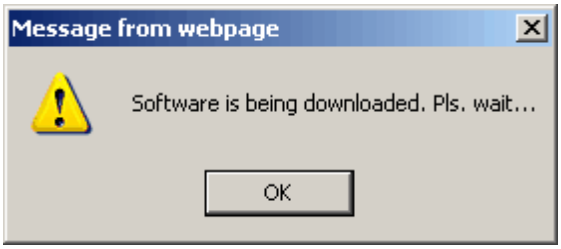


Figure 132: Software Download Message

4. Click **OK**.

   The Software Download Status window opens.

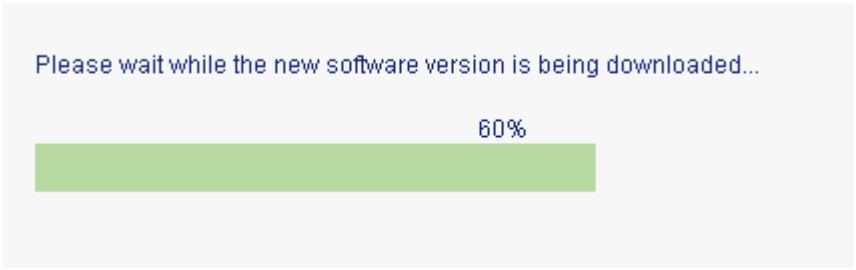


Figure 133: Software Download Status Window

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.

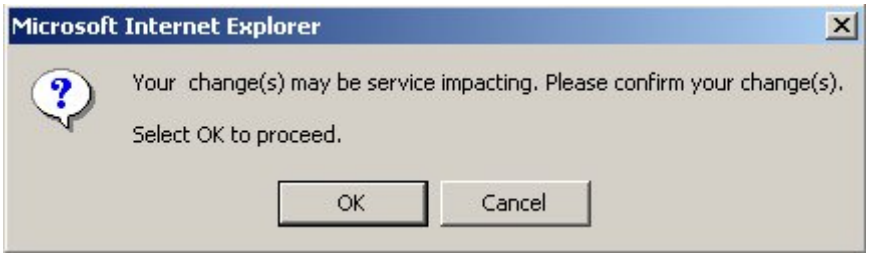


Figure 134: Confirm Changes

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.

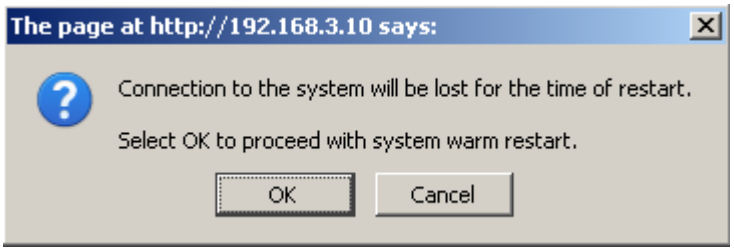


Figure 135: Confirm Changes

   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 Diagnostic Tests

Port maintenance includes diagnostic testing. The following tests are provided:

- **Facility loopback test**: Can be performed on the uplink port or any service port
- **PRBS test**: Can be performed on the uplink port or any service port

8.2.1 Facility Loopback Test

The facility loopback test can be performed on the uplink port or any service port as follows:

- **Local loopback**: This local loopback test verifies that the local unit connections are functioning properly. This loopback can be performed on the CFP/QSFP+/SFP+.
- **Remote loopback**: This remote test allows the operator to verify that the entire link is operational. This loopback can be performed on the Coherent port of the remote PL-1000GT.

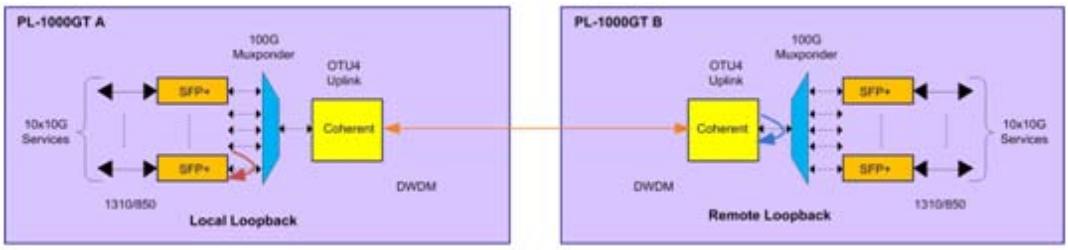


Figure 136: Facility Loopback Test

8.2.2 PRBS Test

The uplink port and service ports can be configured to send and receive PRBS. The PRBS test may be used to check the connectivity and the quality of the service between two nodes.

The following figure shows an example of PRBS usage:

- Coherent of Node A sends PRBS while bottom Coherent of Node B is configured to loopback.
- SFP+ and QSFP+ of Node A send PRBS.

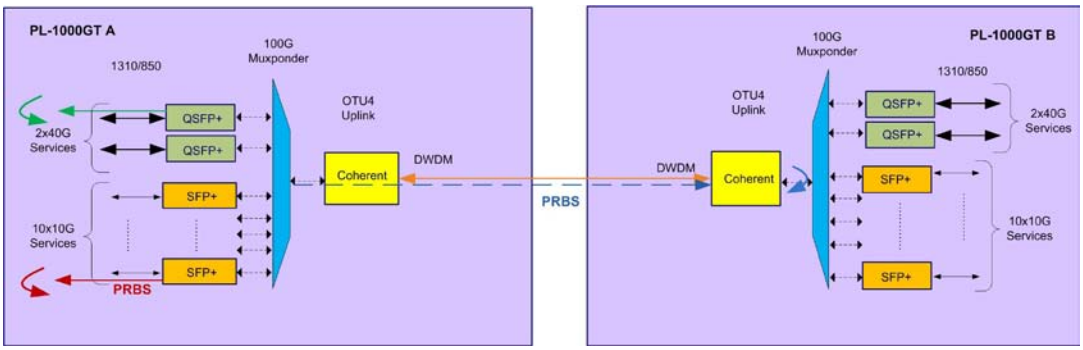


Figure 137: PRBS Test

NOTE:

- The PRBS port and the corresponding remote loopback port should be configured to the same service type.
- The loopback on the remote side may also be done with a physical connection of the Rx and Tx fibers.

8.3 Uplink Port Maintenance

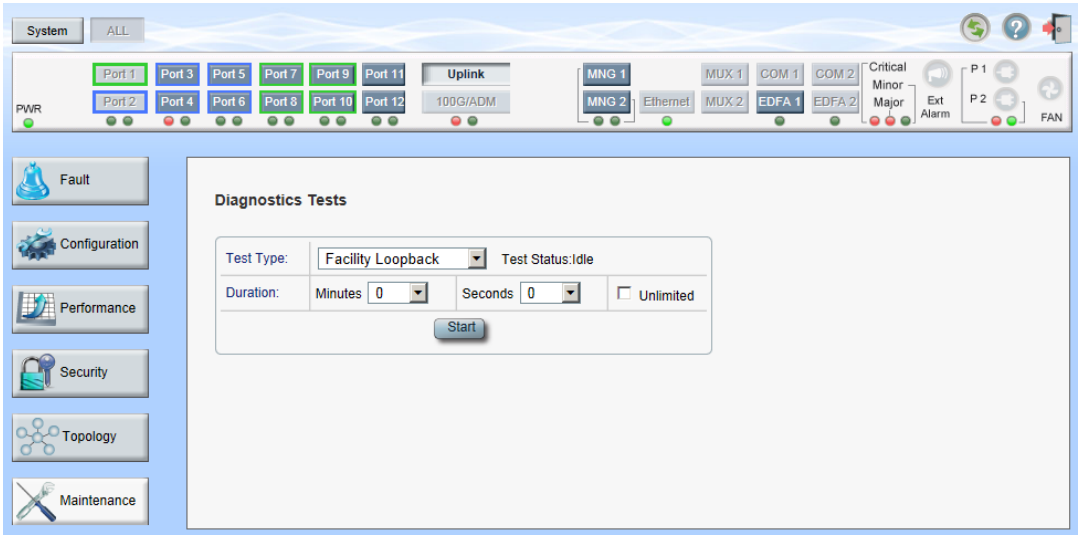


Figure 138: Uplink Port Maintenance Window

Use the Uplink Port Maintenance window to perform diagnostic tests on the uplink port.

To open the Uplink Port Maintenance window:

1. Click **Maintenance**.
2. Click **Uplink** to select the uplink port.

   The Uplink Port Maintenance window opens.

8.3.1 Diagnostics Tests Tab

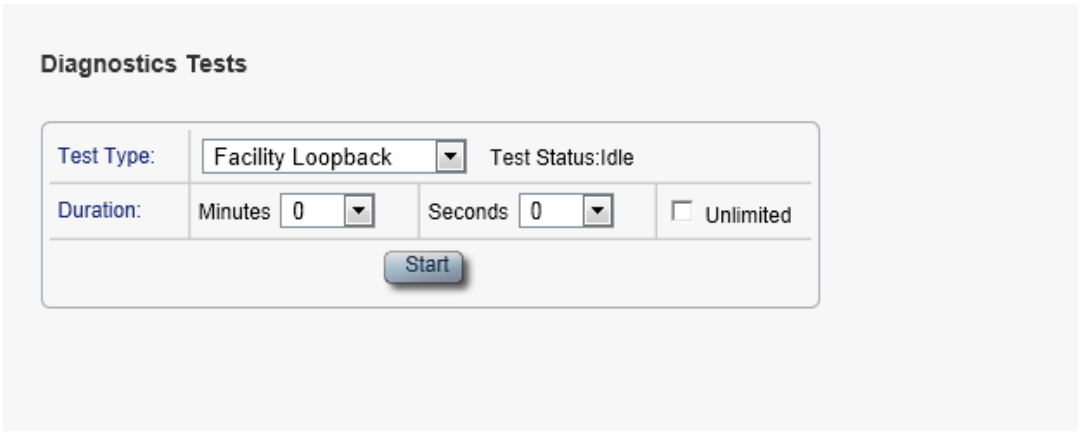


Figure 139: Diagnostic Tests Tab

Use the Diagnostic Tests tab to perform facility loopback and PRBS tests on the uplink port.

To perform diagnostic tests:

1. Click **Uplink** to select the uplink port.

   The Diagnostic Tests tab opens.

2. From the **Test Type** drop-down list, select **Facility Loopback** or **PRBS Test**.
3. To specify the duration of the test:
   1. From the **Minutes** drop-down list, select the number of minutes.
   2. From the **Seconds** drop-down lists, select the number of seconds.
   3. Clear the **Unlimited** check box.
4. To continue running the test until manually stopped, select the **Unlimited** check box.
5. Click **Start**.

   The test is performed.

   The **Start** button toggles to **Stop** for the duration of the test.

6. To stop a test, click **Stop**.

   The test is stopped and the **Stop** button toggles to **Start**.

   For a PRBS test, the results of the test are displayed. The fields are read only and explained in the following table.

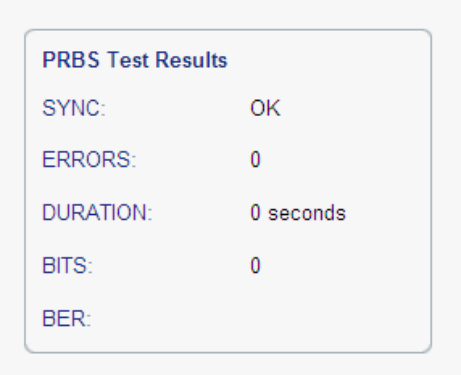


Figure 140: PRBS Test Results

Table 67: PBRS Test Results

Parameter	Description	Format / Values
SYNC	Indicates if PRBS synchronization has been reached.	OK, FAIL **NOTE:** If synchronization failed, the other fields should be ignored.
ERRORS	The number of PRBS errors detected.	Integer
Duration	The duration of the test (in seconds).	Integer

Parameter	Description	Format / Values
BITS	The number of bits sent.	Integer (Bit Rate of configured Service Type) x (Duration)
BER	The bit error ratio.	Decimal number (ERROR / BITS) For example : 0.0000013

8.4 Service Port Maintenance

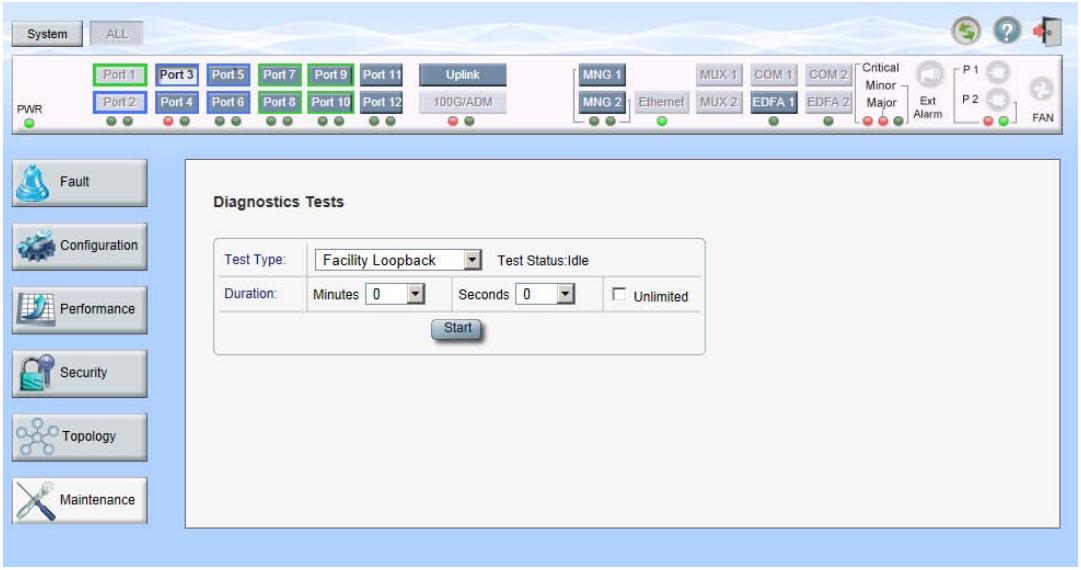


Figure 141: Service Port Maintenance Window

Use the Service Port Maintenance window to perform diagnostic tests on service ports.

To open the Service Port Maintenance window:

1. Click **Maintenance**.
2. Click **100G/ADM** or a **Port** button to select the service port.

   The appropriate Service Port Maintenance window opens.

8.4.1 Diagnostics Tests Tab

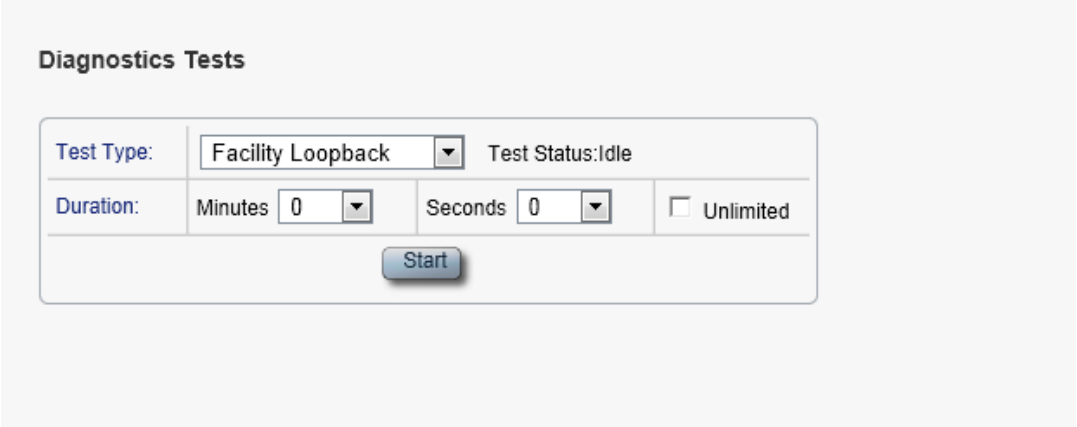


Figure 142: Diagnostic Tests Tab

Use the Diagnostic Tests tab to perform facility loopback and PRBS tests on service ports.

To perform diagnostic tests:

1. Click **100G/ADM** or a **Port** button to select the service port.

   The Diagnostic Tests tab opens.
2. From the **Test Type** drop-down list, select **Facility Loopback** or **PRBS Test**.
3. To specify the duration of the test:
   1. From the **Minutes** drop-down list, select the number of minutes.
   2. From the **Seconds** drop-down lists, select the number of seconds.
   3. Clear the **Unlimited** check box.
4. To continue running the test until manually stopped, select the **Unlimited** check box.
5. Click **Start**.

   The test is performed.

   The **Start** button toggles to **Stop** for the duration of the test.
6. To stop a test, click **Stop**.

   The test is stopped and the **Stop** button toggles to **Start**.

For a PRBS test, the results of the PRBS test are displayed. The fields are read only and explained in the following table.

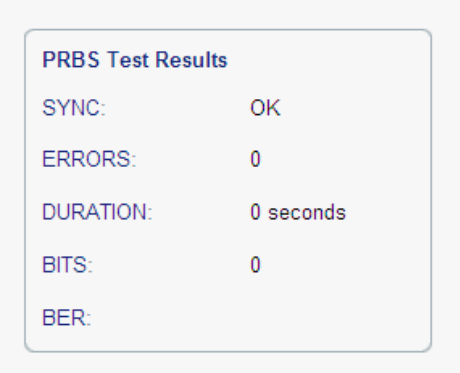


Figure 143: PRBS Test Results

Table 68: PBRS Test Results

Parameter	Description	Format/Values
SYNC	Indicates if PRBS synchronization has been reached.	OK, FAIL **NOTE:** If synchronization failed, the other fields should be ignored.
ERRORS	The number of PRBS errors detected.	Integer
Duration	The duration of the test (in seconds).	Integer
BITS	The number of bits sent.	Integer (Bit Rate of configured Service Type) x (Duration)
BER	The bit error ratio.	Decimal number (ERROR / BITS) For example : 0.0000013

8.5 External Alarm Maintenance

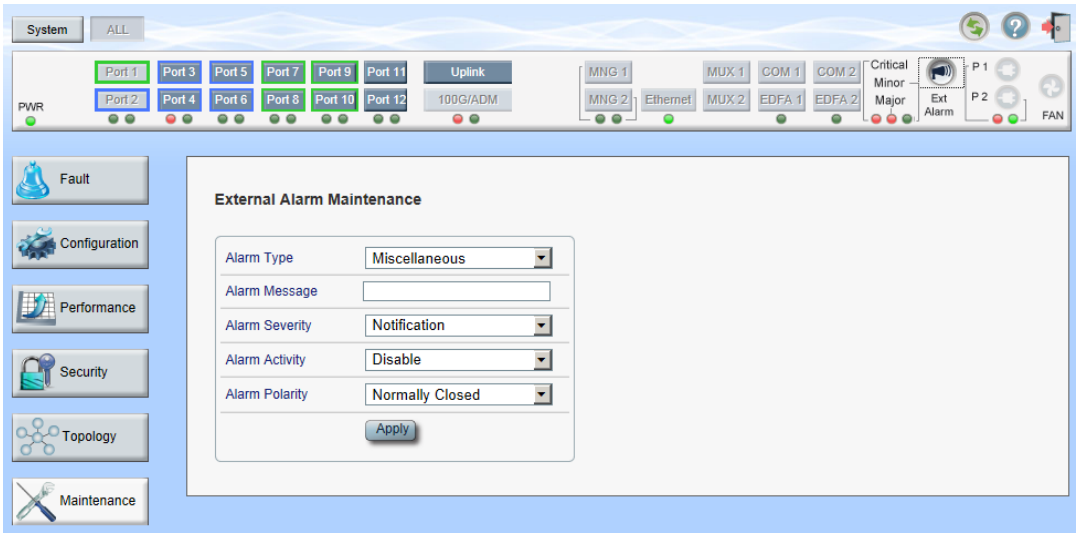


Figure 144: External Alarm Maintenance Window

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

To open the External Alarm Maintenance window:

1. Click **Maintenance**.
2. Click the **Ext Alarm** button to select the external alarm.

   The External Alarm Maintenance window opens.

8.5.1 External Alarm Maintenance Tab

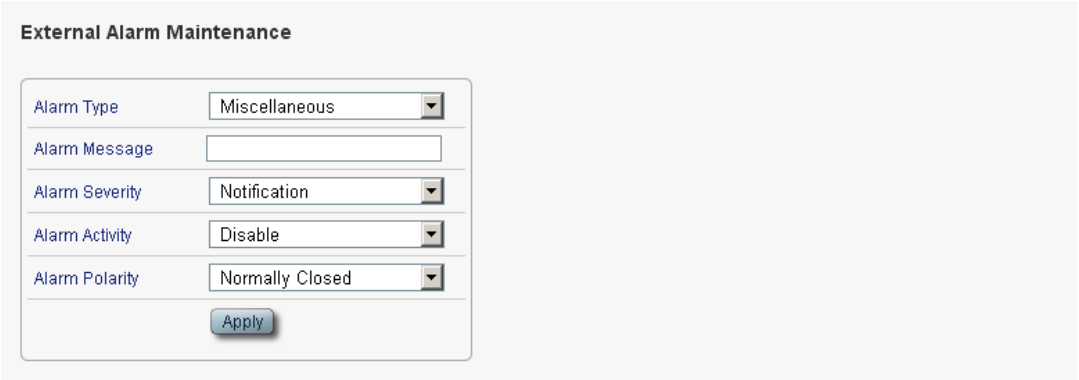


Figure 145: External Alarm Tab

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 69: 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-1000GT nodes.

In this Chapter

9.1 Network Topology

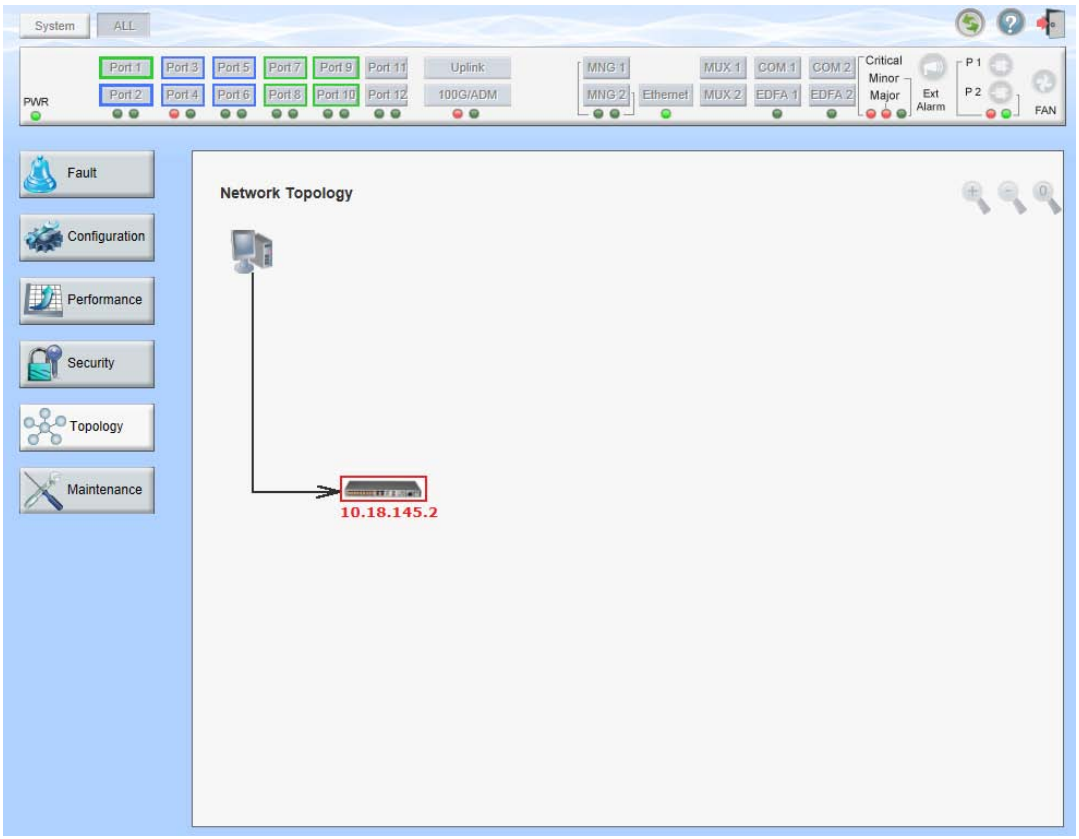


Figure 146: Network Topology Window

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

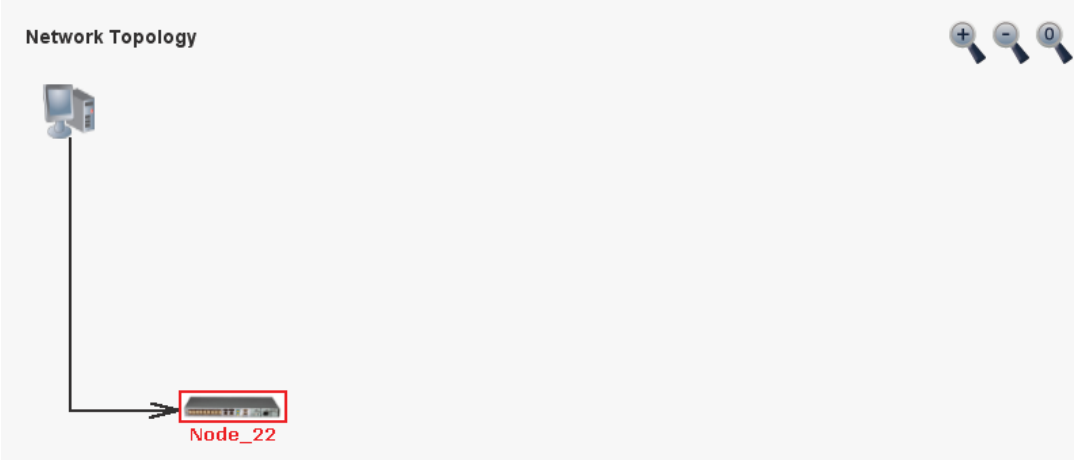


Figure 147: Network Topology Tab

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-1000GT nodes connected together with the OSC channel.

9.1.1.1 Network Linear Topology

The following figure is an example of a linear topology.

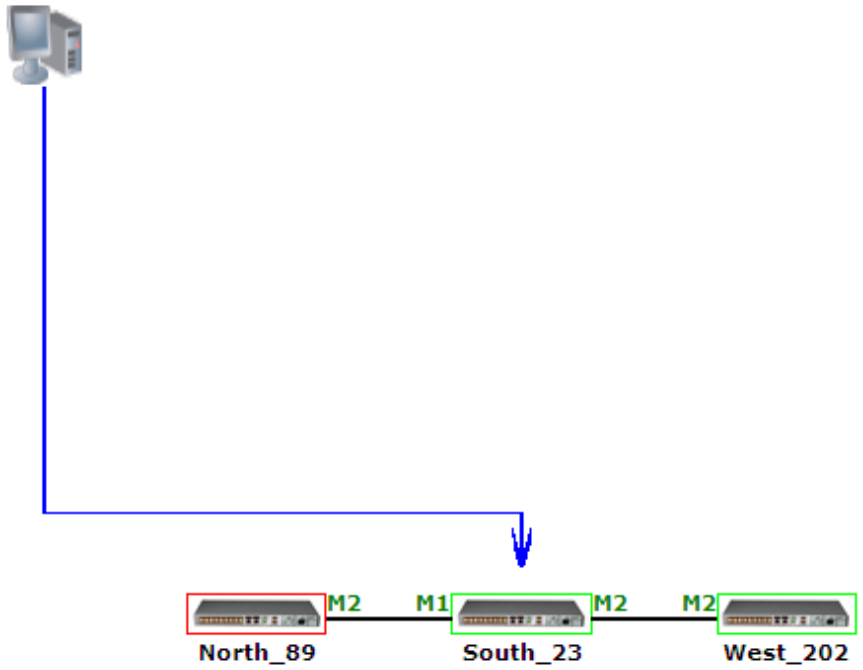


Figure 148: Linear Topology (Example)

9.1.1.2 Ring Topology

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

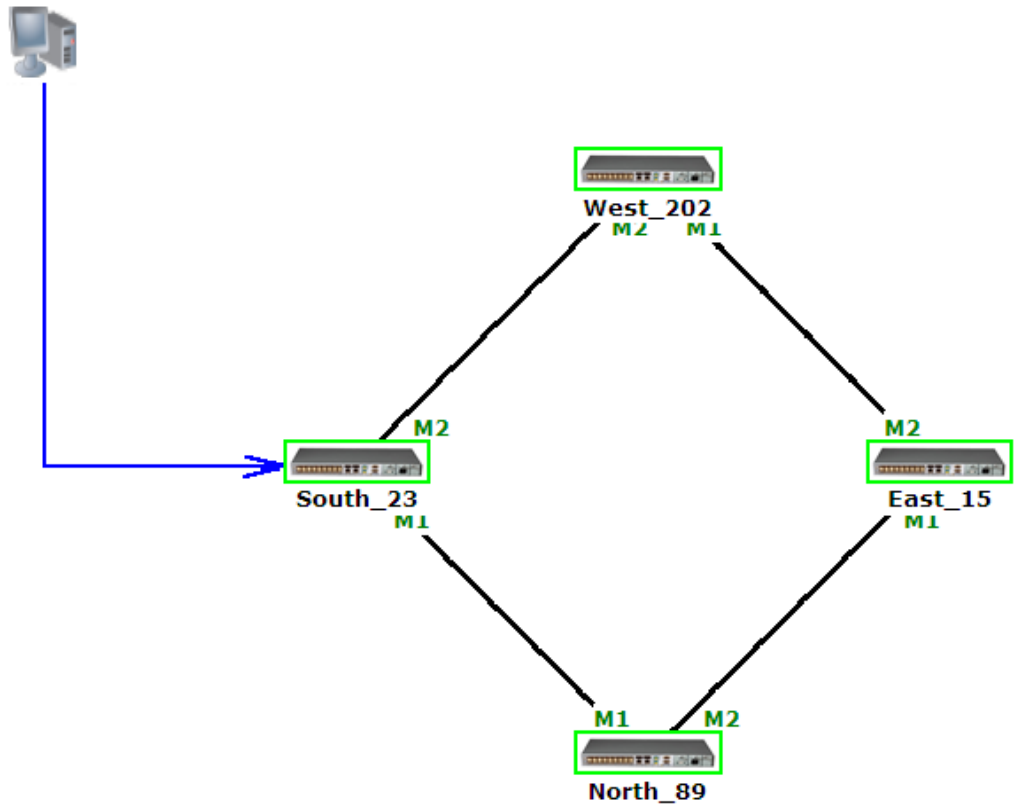


Figure 149: Ring Topology (Example)

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-1000GT 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-1000GT 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. 111).)

9.1.4 Defining Multiple Nodes as Multi-Chassis

When multiple PL-1000GT 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-1000GT node (see Logging In to the Web Application (p. 32)).
2. Click **Configuration**.
3. Click **System**.

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

   The General tab opens.

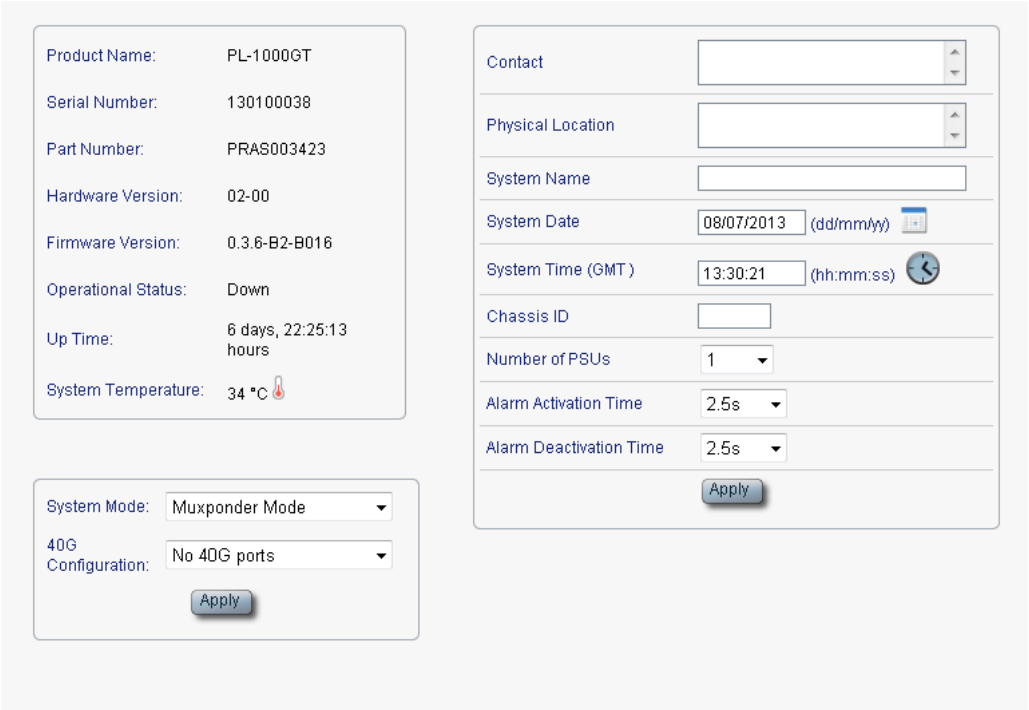


Figure 150: General Tab

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.

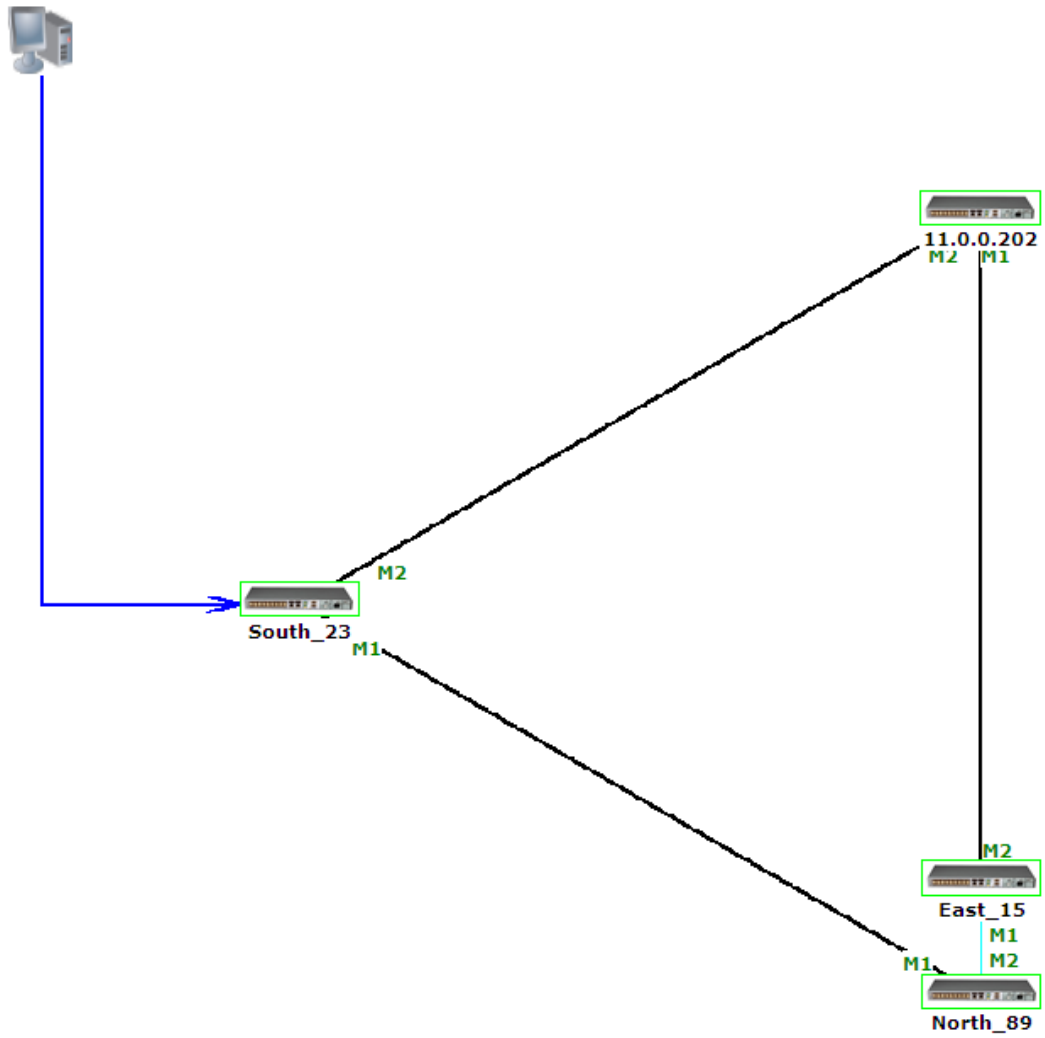


Figure 151: Multi-Chassis Nodes

10 Remote Management Configuration

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

A remote PL-1000GT can be managed through the OSC or in-band management channel.

In this Chapter

10.1 Remote Management Configuration Example

The following figure illustrates 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 PL-1000GT nodes A and B via the OSC or in-band management channel.

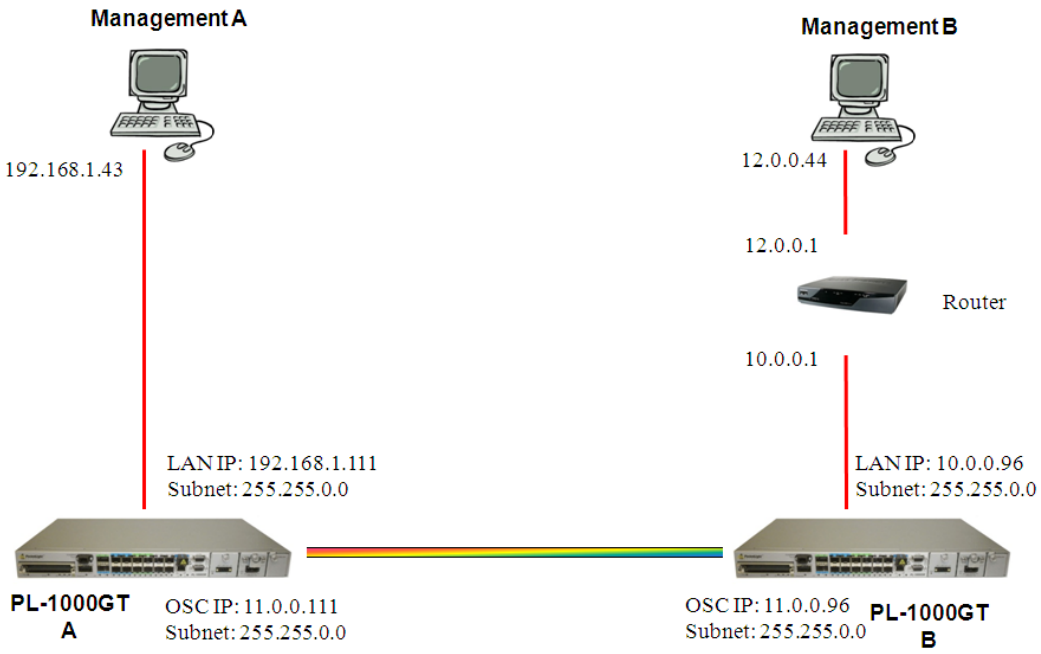


Figure 152: Point-to-Point Remote Management (Example)

10.2 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-1000GT nodes (see Accessing the Web Application (p. 31)).

2. Configure management for PL-1000GT A.
3. Configure management for PL-1000GT B.
4. Access the Web application from Management A to PL-1000GT A.
5. Access the Web application from Management A to PL-1000GT B.
6. Access the Web application from Management B to PL-1000GT B.
7. Access the Web application from Management B to PL-1000GT A.

10.2.1 Configuring Management for PL-1000GT A

To configure management for PL-1000GT 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. 111)).
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.

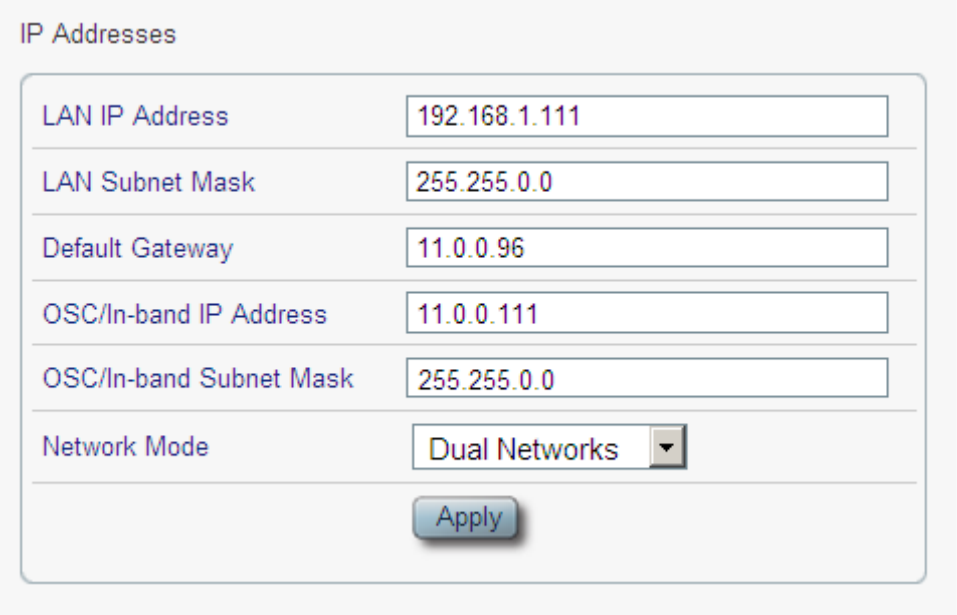


Figure 153: IP Addresses: PL-1000GT A (Example)

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. 114)).

   The SNMP Traps table should appear as follows.

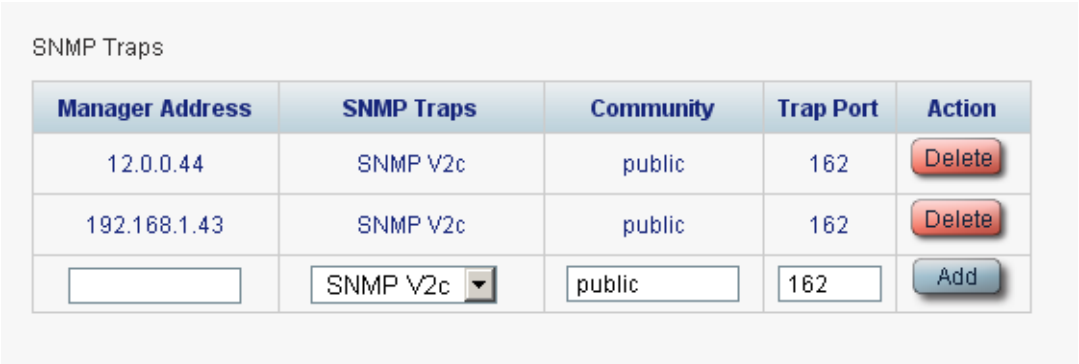


Figure 154: SNMP Traps Table (Example)

10.2.2 Configuring Management for PL-1000GT B

When configuring the management for PL-1000GT 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-1000GT nodes should be in same subnet.

To configure management for PL-1000GT 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. 111)).

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.

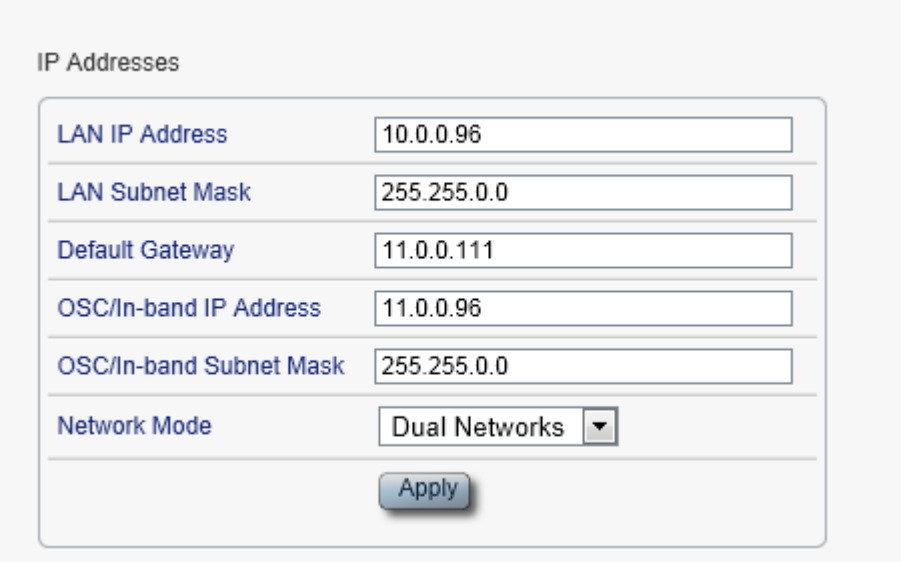


Figure 155: IP Addresses: PL-1000GT B (Example)

6. Configure the **Static Routing** table to enable the route to Management B as follows:
   - **Destination Address**: 12.0.0.0
   - **Subnet Mask**: 255.255.0.0
   - **Gateway**: 10.0.0.1
7. Click **Add**.

The Static Routing table should appear as follows.

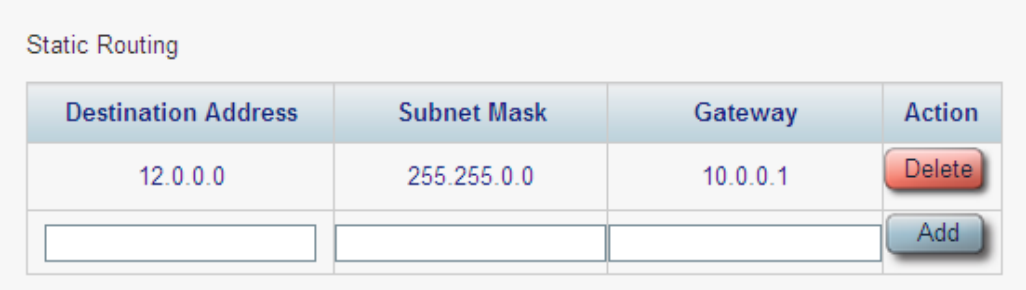


Figure 156: Static Routing: PL-1000GT B (Example)

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. 114)).

   The SNMP Traps table should appear as follows.

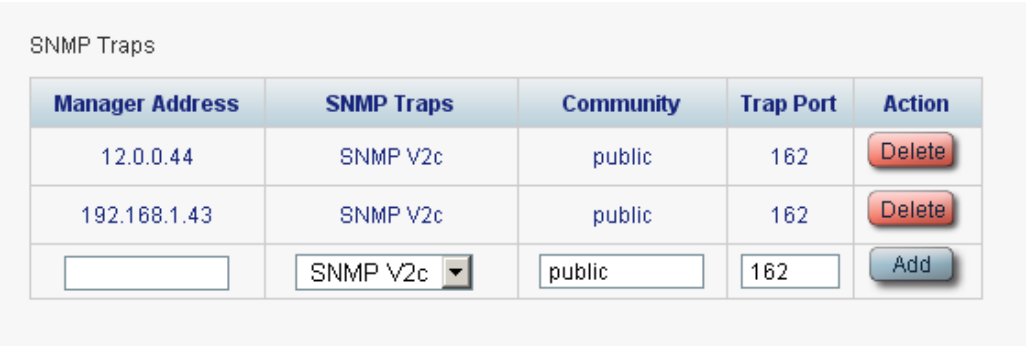


Figure 157: SNMP Traps Table (Example)

10.2.3 Accessing the Web Application from Management A to PL-1000GT A

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

1. Open the Web browser.
2. In the address field of the browser, type the **IP address** of the LAN port of PL-1000GT 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. 209))
3. Press **Enter**.

   The Login window opens.
4. Log in to the Web application (see Logging In to the Web Application (p. 32)).

10.2.4 Accessing the Web Application from Management A to PL-1000GT B

To access the Web application from Management A to PL-1000GT 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-1000GT 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. 209))

4. Press **Enter**.

   The Login window opens.

5. Log in to the Web Application (see Logging In to the Web Application (p. 32)).

10.2.5 Accessing the Web Application from Management B to PL-1000GT B

To access the Web application from Management B to PL-1000GT 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-1000GT 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. 209))

4. Press **Enter**.

   The Login window opens.

5. Log in to the Web Application (see Logging In to the Web Application (p. 32)).

10.2.6 Accessing the Web Application from Management B to PL-1000GT A

To access the Web application from Management B to PL-1000GT 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-1000GT A so that the IP address of the PL-1000GT B LAN port (**10.0.0.96** as illustrated in Remote Management Configuration Example (p. 209)) 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-1000GT 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. 209)).

4. Press **Enter**.

   The Login window opens.

5. Log in to the Web application (see Logging In to the Web Application (p. 32)).

11 CLI

This chapter describes the CLI for PL-1000GT.

The CLI provides commands for status monitoring, service provisioning, and basic configuration of the PL-1000GT.

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-1000GT 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-1000GT>>
```

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-1000GT>>login
User: admin
Password:
PL-1000GT>>
```

6. Run the desired CLI commands as described in Running CLI Commands (p. 221).

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-1000GT>>
```

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

   For example:

```
PL-1000GT>>login
User: admin
Password:
PL-1000GT>>
```

4. Run the desired CLI commands as described in Running CLI Commands (p. 221).

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**

NOTE: Up to three Telnet/SSH sessions to the same device can be open at the same time.

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-1000GT>>
```

5. Run the desired CLI commands as described in Running CLI Commands (p. 221).
6. Terminate the SSH session by pressing **'CTRL+D'**.

NOTE: Up to three Telnet/SSH sessions to the same device can be open at the same time.

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
- Service commands
- System Restart command

The following figure shows the hierarchy of the commands.

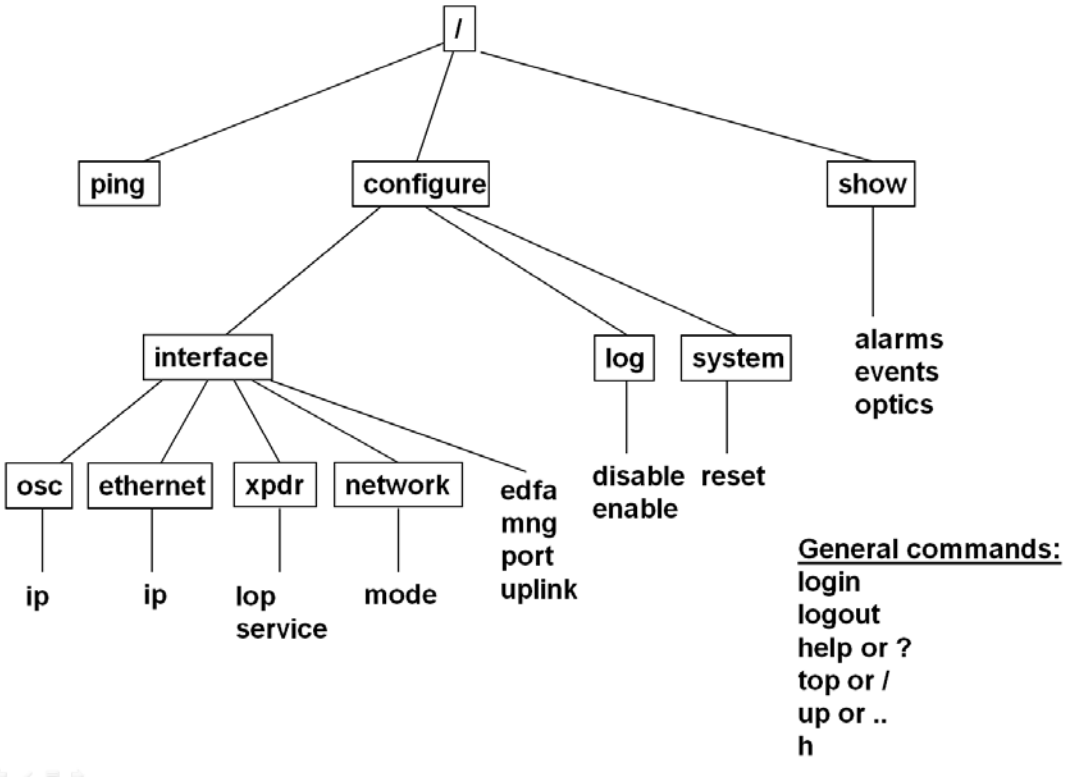


Figure 158: CLI Command Tree

11.4 Running CLI Commands

You can run the following CLI commands:

- General commands
  - Login (p. 222)
  - Logout (p. 223)
  - Help (p. 223)
  - History (p. 223)
  - Top (p. 224)
  - Up (p. 224)
- Ping command (p. 225)
- Interface commands
  - Configure Interface Uplink (p. 225)
  - Configure Interface Port (p. 226)
  - Configure Interface MNG (p. 226)
  - Configure Interface EDFA (p. 226)

- IP Setting commands
  - Configure Interface Ethernet IP (p. 227)
  - Configure Interface OSC IP (p. 227)
  - Configure Interface Network Mode (p. 228)
- Log commands
  - Configure Log Enable (p. 229)
  - Configure Log Disable (p. 229)
- Show commands
  - Show Alarms (p. 229)
  - Show Events (p. 230)
  - Show Optics (p. 230)
- Service commands
  - Configure Interface XPDR LOP (p. 231)
  - Configure Interface XPDR Service (p. 231)
- System Restart command
  - Configure System Reset (p. 232)

11.4.1 General Commands

The following are general commands that can be invoked from anywhere in the command tree:

- Login (p. 222)
- Logout (p. 223)
- Help (p. 223)
- History (p. 223)
- Top (p. 224)
- Up (p. 224)

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-1000GT>>login
User: admin
Password:
PL-1000GT>>
```

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-1000GT>>logout
PL-1000GT>>
```

11.4.1.3 Help Command

Command:

help [<command>]

or

? [<command>]

Description:

This command displays the syntax of the specified command.

Example:

```
PL-1000GT>>help con int eth ip
config interface ethernet ip [<addr> [-n <netmask>] [-g <gateway>]]
PL-1000GT>>
```

11.4.1.4 History Command

Command:

h

Description:

This command displays the last 20 commands.

Example:

```
PL-1000GT>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-1000GT>show>>
```

11.4.1.5 Top Command

Command:

top

or

/

Description:

This command takes you to the root of the command tree.

Example:

```
PL-1000GT>configure>interface>>top
PL-1000GT>>
```

11.4.1.6 Up Command

Command:

up

or

..

Description:

This command takes you up one level in the command tree.

Example:

```
PL-1000GT>configure>interface>ethernet>>up
PL-1000GT>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-1000GT>>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-1000GT>>
```

11.4.3 Interface Commands

The following are the Interface commands:

- Configure Interface Uplink (p. 225)
- Configure Interface Port (p. 226)
- Configure Interface MNG (p. 226)
- Configure Interface EDFA (p. 226)

11.4.3.1 Configure Interface Uplink Command

Command:

configure interface uplink [up | down]

Description:

This command sets the **Admin Status** of the uplink port to the required value.

If the **Admin Status** is not specified, the administrative status of the uplink port is displayed.

Example:

```
PL-1000GT>configure>interface>>uplink
Uplink is DOWN
PL-1000GT>configure>interface>>uplink up
PL-1000GT> configure>interface>>uplink
Uplink is UP
PL-1000GT>configure>interface>>
```

11.4.3.2 Configure Interface Port Command

Command:

configure interface port <n, '100G'> [up | down]

Description:

This command sets the **Admin Status** of the port to the required value.

If the **Admin Status** is not specified, the administrative status of the port is displayed.

Example:

```
PL-1000GT>configure>interface>>port 3
Port 3 is DOWN
PL-1000GT>configure>interface>>port 3 up
PL-1000GT> configure>interface>>port 3
Port 3 is UP
PL-1000GT>configure>interface>>
```

11.4.3.3 Configure Interface MNG Command

Command:

configure interface mng <n> [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-1000GT>configure>interface>>mng 1 down
PL-1000GT>configure>interface>>mng 1
Port MNG 1 is DOWN
PL-1000GT>configure>interface>>
```

11.4.3.4 Configure Interface EDFA Command

Command:

configure interface edfa <n> [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-1000GT>configure>interface>>edfa 1 up
PL-1000GT>configure>interface>>
```

11.4.4 IP Setting Commands

The following are the IP Setting commands:

- Configure Interface Ethernet IP (p. 227)
- Configure Interface OSC IP (p. 227)
- Configure Interface Network Mode (p. 228)

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-1000GT>configure>interface>ethernet>>ip 10.0.3.200 –n 255.255.0.0 –g
10.0.44.44
PL-1000GT>configure>interface>ethernet>>ip
Addr is 10.0.3.200, Subnet mask is 255.255.0.0
Gateway is 10.0.44.44
PL-1000GT>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 and the in-band channel.

- **<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:

- This command is not available when working in **Single Network** mode.
- When working via Telnet, changing the IP parameters of the OSC may prevent further access to the node.
- Both MNG ports have the same IP parameters, therefore, changing the OSC IP parameters also changes the parameters of both MNG ports.

Example:

```
PL-1000GT>configure>interface>osc>>ip 11.0.3.200 –n 255.255.0.0 –g
11.0.3.201
PL-1000GT>configure>interface>osc>>ip
Addr is 11.0.3.200, Subnet mask is 255.255.0.0
Gateway is 11.0.3.201
PL-1000GT>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. 232)).

Example:

```
PL-1000GT>configure>interface>network>>? mode
config interface network mode [dual|single]
PL-1000GT>configure>interface>network>>mode
Current network mode is single
PL-1000GT>configure>interface>>..
PL-1000GT>configure>>interface network mode dual
PL-1000GT>configure>>system reset c
```

11.4.5 Log Commands

The following are the Log commands:

- Configure Log Enable (p. 229)
- Configure Log Disable (p. 229)

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-1000GT>configure>log>>enable
PL-1000GT>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-1000GT>configure>log>>disable
PL-1000GT>configure>log>>
```

11.4.6 Show Commands

The following are the Show commands:

- Show Alarms (p. 229)
- Show Events (p. 230)
- Show Optics (p. 230)

11.4.6.1 Show Alarms Command

Command:

show alarms [port <n, '100G'> | mng <n> | edfa <n> | uplink | system]

Description:

This command displays the alarms of the specified port.

If no parameters are specified, all alarms are displayed.

Example:

```
PL-1000GT>>show alarms port 3
THU JUN 18 12:22:46 2009       PORT 3  Optics Loss of Light    Critical
S.A.
THU JUN 18 12:22:46 2009       PORT 3  Loss Propagation      Minor
PL-1000GT>>
```

11.4.6.2 Show Events Command

Command:

show events [port <n, '100G'> | mng <n> | edfa <n> | uplink | system]

Description:

This command displays the events of the specified port.

If no parameters are specified, all the events are displayed.

Example:

```
PL-1000GT>>show events port 3
THU JUN 18 12:22:44 2009        PORT 3  Link Up
Event
THU JUN 18 12:22:46 2009        PORT 3  Optics Loss of Light     Critical
S.A.
THU JUN 18 12:22:46 2009        PORT 3  Loss Propagation        Minor
THU JUN 18 12:22:47 2009        PORT 3  Link Down
Event
PL-1000GT>>
```

11.4.6.3 Show Optics Command

Command:

show events [port <n, '100G'> | mng <n> | edfa <n> | uplink | system]

Description:

This command displays the optical information of the specified entity.

Example:

```
PL-1000GT>>show optics port 3
Vendor: PLTELE COMPANY
Part Number: PLT9280080KLCA
Serial Number: PLT094476598
Wavelength: 1554.90 nm

Tx Power: 0.6 dBm
Rx Power: -6.8 dBm
Temperature: 40 C
PL-1000GT>>show optics mng 1
Vendor: PLTOLINK INC
Part Number: PLLS-8512-02D
Serial Number: PLS85E010020
Wavelength: 850.00 nm
Type: Non WDM

Tx Power: -6.0 dBm
Rx Power: -5.0 dBm
Temperature: 39 C
PL-1000GT>>
```

11.4.7 Service Commands

The following are the Service commands:

- Configure Interface XPDR LOP (p. 231)
- Configure Interface XPDR Service (p. 231)

11.4.7.1 Configure Interface XPDR LOP Command

Command:

configure interface xpdr lop <port, '100G'> [on | off]

Description:

This command configures the Loss Propagation for the service port.

NOTE: Before provisioning, set the service port to Admin Down.

If the LOP parameter is not specified, the currently provisioned LOP value is displayed.

Example:

```
PL-1000GT>configure>interface>xpdr>>lop 3
Loss Propagation is enabled
PL-1000GT>configure>interface>xpdr>>
```

11.4.7.2 Configure Interface XPDR Service Command

Command:

configure interface xpdr service [<port, '100G'> [<service type>]]

Description:

This command provisions the service port with the specified service.

NOTE: Before provisioning, set the uplink and service ports to **Admin Down**.

The following service types are available:

- 8G-FC
- 10GBE-LAN
- OC-192
- STM-64
- OTU2
- OTU2e
- GBE40-LAN
- OTU4
- GBE100-LAN

If the **service type** parameter is not specified, the currently provisioned service is displayed.

If no parameter is specified, all service types are displayed.

Example:

```
PL-1000GT>configure>interface>xpdr>>service 3 10GBE-LAN
XPDR 3-3 service type to 33
PL-1000GT>configure>interface>xpdr>>service 3
Service Type is 10GBE-LAN
PL-1000GT>configure>interface>xpdr>>
```

11.4.8 System Restart Command

The following is the System Restart command:

- Configure System Reset (p. 232)

11.4.8.1 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/SSH will terminate the session.
- It is recommended to save the old configuration file before restoring to factory defaults.

Example (of a Telnet session):

```
PL-1000GT>>configure system reset w
PL-1000GT>>

Connection to host lost.
```

Appendix A: Connection Data

This appendix describes the connectors for the PL-1000GT.

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 70: CONTROL Connector Wiring

Pin	Function	Direction
2	Transmit Data (TX)	From PL-1000GT
3	Receive Data (RX)	To PL-1000GT
5	Signal Ground (SIG)	Common reference

A.2 ALARM Connector

The ALARM connector of the PL-1000GT 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.

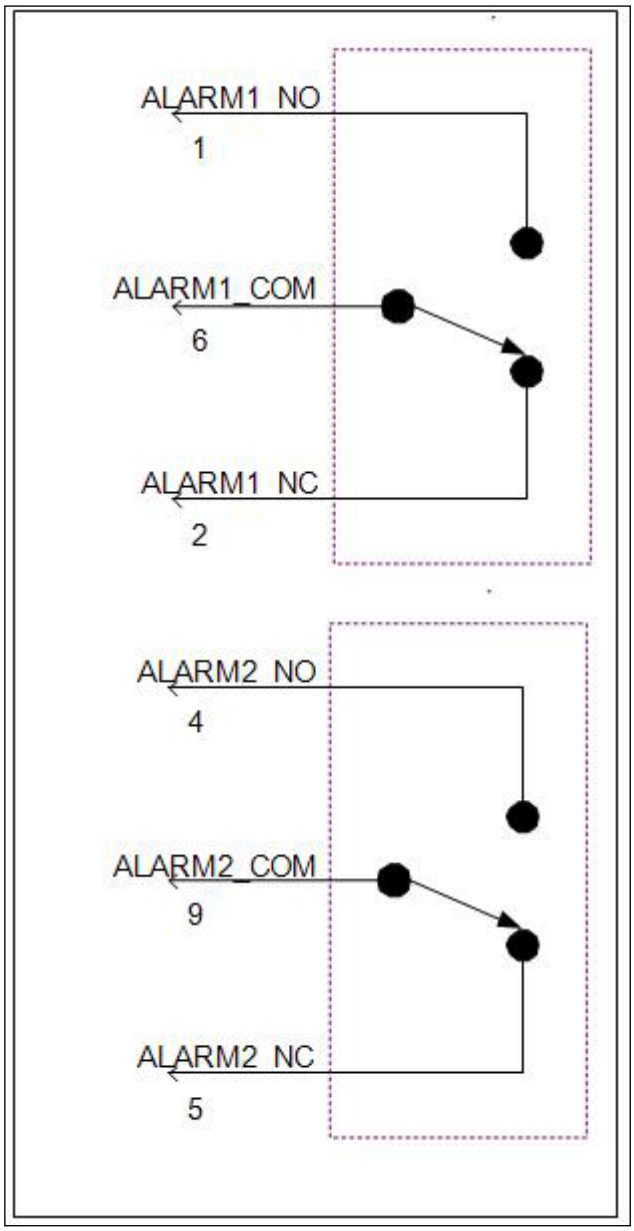


Figure 159: External ALARM Diagram

Table 71: 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).
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-1000GT 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 72: 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 Optical PL-1000GT Connectors

The optical PL-1000GT connectors can be one of the following ports:

- Uplink
- Service
- MNG

A.4.1 Uplink Port

The uplink port accepts Coherent modules of the following types.

Table 73: Uplink WDM Coherent Specifications

Specification	Requirement
Fiber Type	Single mode
Wavelength	Tunable channels ITU DWDM Grid 50/100 GHz spacing
Fiber Size	2 mm optical fiber
Connector Type	LC connector
Port Type	OTU4 100G Uplink

A.4.2 Service Ports

There are three types of service ports:

- 100G/ADM port is a 100G service port that accepts a CFP transceiver.
- LINK 1 and LINK 2 are 40G services ports that accept QSFP+ transceivers (future versions).
- LINK 3 to LINK 12 are 10G service ports accept SFP+ transceivers.

Table 74: Service 100G CFP Specifications

Specification	Requirement
Fiber/Cable Type	Single mode or multi-mode
Wavelength	• **DWDM**: Single mode, 4 tunable DWDM Grid C-Band channels, 50G/100G spacing • **SR10**: Multi-mode, 10 x 850 nm
Fiber Size	2 mm optical fiber
Connector Type	• **DWDM**: 4 LC connectors • **SR10**: MPO/APC female
Service Type	• 100GbE-LAN • OTU4 (future versions)

Table 75: Service QSFP+ Specifications

Specification	Requirement
Fiber/Cable Type	Single mode or multi-mode
Wavelength	• **Single mode**: 4 Fixed channels CWDM Grid • **Multi-mode**: 4 x 850 nm
Fiber Size	Ribbon cable with 4 optical fibers
Connector Type	MPO/APC female
Service Type	• 40GbE • OTU3 (future versions) • OC-768 (future versions) • STM-256 (future versions)

Table 76: Service SFP+ Specifications

Specification	Requirement
Fiber/Cable Type	Single mode or multi-mode
Wavelength	• **Single mode**: 1310 nm • **Multi-mode**: 850 nm
Fiber Size	2 mm optical fiber
Connector Type	LC
Service Type	• 10GbE-LAN • 8G FC • OC-192 • STM-64 • OTU2 • OTU2e • 10G FC (future versions)

A.4.3 MNG Ports

The MNG ports accept optical or copper (electrical) SFP modules.

Table 77: MNG Port Specifications

Specification	Requirement
Fiber/Cable Type	Single mode or multi-mode

Wavelength	• **Single mode**:
	  ▪ **CWDM**: 1290 nm or 1310 nm
	  ▪ **DWDM**: 1490 nm or 1510 nm
	• **Multi-mode**: 850 nm

Fiber Size	2 mm optical fiber
Connector Type	LC
Port Type	Management

A.5 Power Supplies

The PL-1000GT has two redundant DC power supplies.

A.6 Power Connectors

The PL-1000GT has two DC power supply connectors.

The following figure shows how to wire the DC connector).

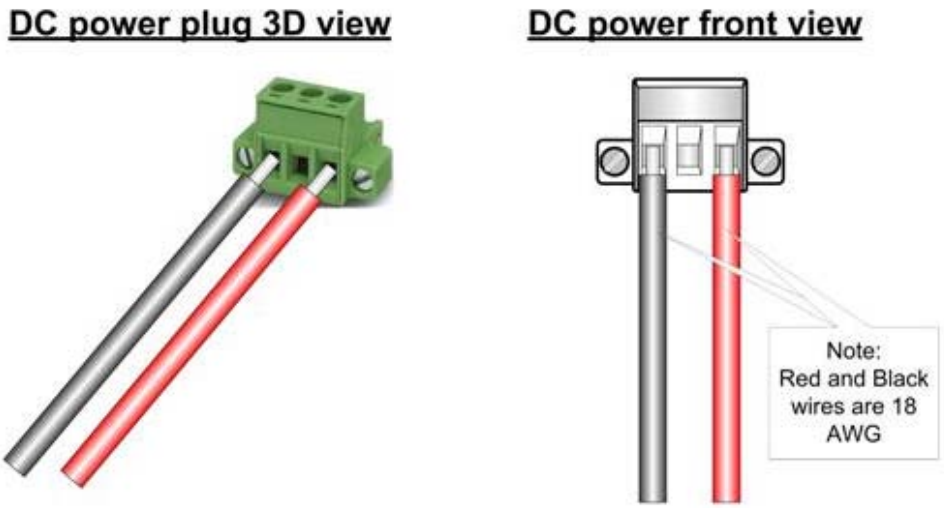


Figure 160: DC Connector Wiring Diagram

A.7 Protective Ground Terminal

The protective ground terminal of the PL-1000GT, located on the rack mount, must be connected to a protective ground.

The following figure shows how to wire the ground terminal.

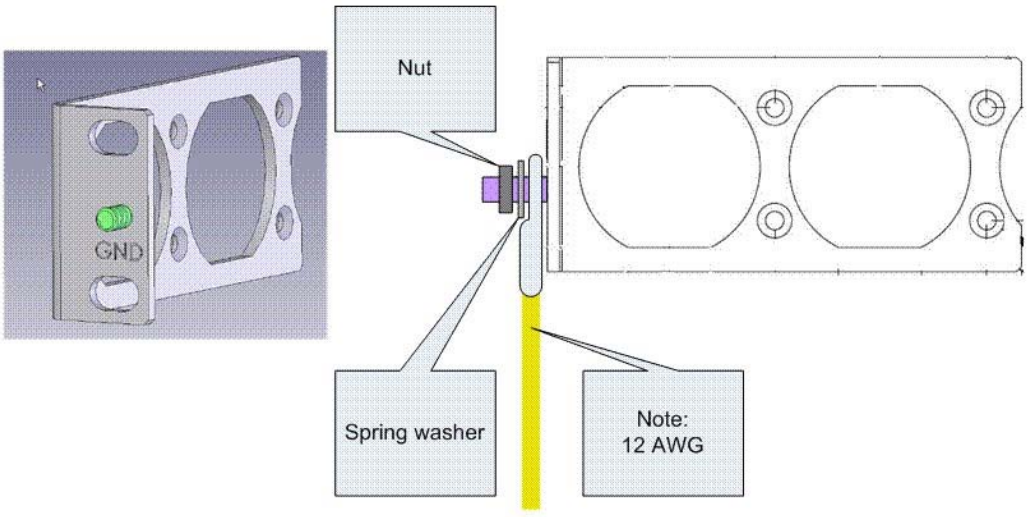


Figure 161: Protective Ground Terminal Wiring Diagram

A.8 Fiber Shelf

The fiber shelf is an optional tray that can be attached to the PL-1000GT to help you organize the optical fibers.

The following figure shows the mechanical details of the fiber shelf.

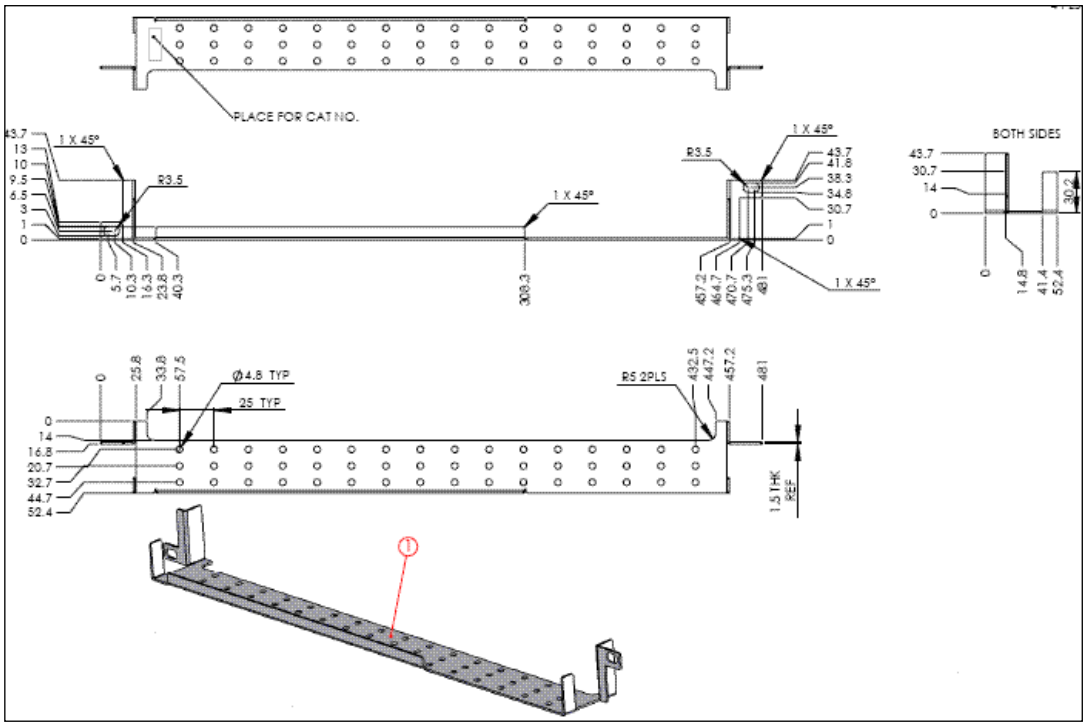


Figure 162: Fiber Shelf Diagram

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 alarm messages and their interpretation and/or corrective measures.

Table 78: Alarm Messages

Source	Message	Interpretation/Corrective Measures
PSU1/PSU2	Power Supply Failure	Check if the power cord is plugged into the connector of the faulty PSU.
PSU1/PSU2	Power Failure– Low Voltage	Check the power supply source.
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.
Ethernet, FC	Loss of Synchronization	Loss of Synchronization has been detected on the GbE, Ethernet or FC link. Check that the input signal rate is correct.
SONET/SDH	RFI-L (Line Remote Failure Indication)/MS-RFI (MS Remote Failure Indication)	Remote Failure Indication (RFI) has been detected on the SONET/SDH link.

Source	Message	Interpretation / Corrective Measures
SONET/SDH	AIS-L (Line Alarm Indication Signal)/MS-AIS (MS Alarm Indication Signal)	Alarm Indication Signal (AIS) has been detected on the SONET/SDH link.
SONET/SDH	Loss of Frame	Loss of Frame (LOF) has been detected on the SONET/SDH link.
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.
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 remote peer port.

Source	Message	Interpretation / Corrective Measures
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.
Muxponder Uplink Port	Muxponder In-band Failure	The in-band channel of the muxponder has failed. Check that the remote in-band is enabled.
Uplink Port	OTN Path Degrade	Bad line conditions.
Uplink Port	OTN Section Degrade	Bad line conditions.
Uplink Port	OTN LOS	• Rx and Tx connectors intermixed *or* • Fiber break *or* • Bad optical module.
Uplink Port	OTN LOF	• Wrong fiber is connected *or* • Bad optical module *or* • Bad line conditions.
Uplink Port	OTN Loss of Multiframe	Bad line conditions.
Uplink Port	OTN Path BDI	Remote uplink has detected a problem with an ODU path.
Uplink Port	OTN Section BDI	Remote uplink has detected a problem with the OTU section.
Uplink Port	OTN Path AIS	Remote uplink reports a defect with an ODU path.
Uplink Port	OTN Section AIS	Problem in the remote node.
Uplink Port	OTN Path Payload Mismatch	Wrong fiber is connected to the uplink.
Uplink Port	OTN Section Trace Mismatch	• Wrong Trace message is configured *or* • The uplink is connected to the wrong fiber.
Uplink Port	OTN Path Trace Mismatch	• Wrong Trace message is configured *or* • The uplink is connected to the wrong fiber.
Uplink Port	OTN Path Locked	The upstream connection is locked.
Uplink Port	OTN Path Open Connection	The upstream connection is open.

Source	Message	Interpretation / Corrective Measures
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 Eye Safety	Hazard. No fiber is connected to the port.
EDFA	EDFA End of Life	An EDFA problem. Replace the device.

B.2 Configuration Event Messages

The following table lists the configuration event messages generated by the PL-1000GT and explains their interpretation.

Table 79: Configuration Change Messages

Source	Message	Interpretation
System	Change date	The system date or time has changed.
System	Restore provisioning	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.
Port	Admin Down	Admin Down has been performed for the port.
Port	Admin Up	Admin Up has been performed for the port.
Port	Test Operated	A test has been operated.
Port	Test Released	A test has been released.
Port	Reset PM counters	Performance monitoring counters have been reset.

B.3 Other Event Messages

The following table lists the other possible event messages and explains their interpretation.

Table 80: Other Event Messages

Event Type	Source	Message	Interpretation
Inventory Changed	FAN, Optics	Inventory Changed	The node inventory has changed. A component was inserted or removed.
Test	Port	Test Mode Changed	The port test mode has changed.
ALS Status Changed	Port	ALS Laser	ALS was activated or deactivated.
Optical Power Drop	Port	Power Level Drop	The Received Optical Power was reduced by more than 2 dBm since the last measurement.
Dying Gasp	System	Remote Unit Failure	A remote unit had a power failure.
Software Upgrade	System	Software Upgrade	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 81: Troubleshooting Chart

No.	Trouble Symptoms	Probable Cause	Corrective Measures
1	PL-1000GT does not turn on.	No power	1. Check that the power cable is properly connected to the PL-1000GT 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-1000GT.
		Defective power supply	Replace the PL-1000GT.
		Defective PL-1000GT	Replace the PL-1000GT.
2	The LOS LED of a device connected to PL-1000GT is lit.	Cable connection problems	1. Check all cables at the PL-1000GT Tx and Rx port connectors. 2. Repeat the 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-1000GT 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 connector. If the LOS LED is still lit, the remote equipment is defective.
		A problem with the PL-1000GT port state	Set the **Admin Status** of the PL-1000GT uplink port to **Up**.

No.	Trouble Symptoms	Probable Cause	Corrective Measures
		Loss Propagation	Correct the LOS condition on the far service port.
		Defective optical module	1. Check for optical module alarms. 2. If there are alarms, replace the optical module.
		Defective PL-1000GT	1. Use a short fiber to connect the PL-1000GT Rx connector to its Tx connector. (A signal generator may be required as the PL-1000GT does not generate signals by itself.) 2. If the LOS LED is still lit, replace the PL-1000GT.
3	The LED of the local PL-1000GT port is red.	Cable connection problems	1. Check for proper connections of the cables to the PL-1000GT Tx and Rx connector. 2. Repeat the check at the remote equipment.
		High Signal Level	1. Check the optical module **Receive Input Power**. 2. If the power is too high, add an attenuator.
		Defective optical module	1. Check for optical module alarms. 2. If there are alarms, replace the optical module.
		Fiber problem	1. Check the optical module **Receive Input Power**. 2. If the power is too low, replace the fiber.
		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-1000GT	1. Check the PL-1000GT alarms. 2. If there are alarms, replace the PL-1000GT.
5	The equipment attached to the LAN port of the local PL-1000GT cannot communicate with the remote PL-1000GT 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 that the cable to the LAN port is properly connected. 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-1000GT is configured correctly (for example, the default gateway).

No.	Trouble Symptoms	Probable Cause	Corrective Measures
		External problem	1. Check the IP configuration of the remote equipment (for example, the gateway address) that is connected to the local PL-1000GT LAN port. 2. Check that the **Admin Status** of the remote MNG port is **Up** and that it is operating properly.
		Defective PL-1000GT	Replace the PL-1000GT.

Index

W

Z