



PL-1000TN 1.2 INSTALLATION AND CONFIGURATION MANUAL

PL-1000TN 1.2 Installation and Configuration Manual

The information and content contained in this document is proprietary and copyrighted to © 2013 PacketLight Networks, Ltd. All Rights Reserved. The information shall not be used, copied, reproduced, or disclosed in whole or in part without the written consent of PacketLight Networks, Ltd.

PacketLight Networks, Ltd. reserves the right, without prior notice or liability, to make changes in equipment design or specifications. Information supplied by PacketLight Networks, Ltd. is believed to be accurate and reliable. However, no responsibility is assumed by PacketLight Networks, Ltd. for the use thereof, nor for the rights of third parties which may be affected in any way by the use thereof. Any representation(s) in this document concerning performance of PacketLight Networks, Ltd.'s product(s) are for informational purposes only and are not warranties of future performance, either express or implied.

IN NO EVENT WILL PACKETLIGHT BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF PACKETLIGHT HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall PacketLight's liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Contents

1	INTRODUCTION	1
1.1	OVERVIEW	1
1.1.1	MAIN FEATURES	1
1.1.2	TYPICAL APPLICATION	3
1.1.3	PHYSICAL DESCRIPTION	4
1.2	CONFIGURATIONS	5
1.2.1	PL-1000TN CONFIGURATIONS	5
1.2.2	EXAMPLE CONFIGURATIONS	6
1.3	FUNCTIONAL DESCRIPTION	8
1.3.1	PL-1000TN PORTS	8
1.3.2	APS FOR PL-1000TN	12
1.3.3	PL-1000TN MODULES	14
1.3.4	MANAGEMENT FUNCTIONALITY	16
1.4	TECHNICAL SPECIFICATIONS	17
2	INSTALLATION	25
2.1	SAFETY PRECAUTIONS	25
2.1.1	GENERAL SAFETY PRECAUTIONS	25
2.1.2	ELECTRICAL SAFETY PRECAUTIONS	25
2.1.3	PROTECTION AGAINST ELECTROSTATIC DISCHARGE	27
2.2	SITE REQUIREMENTS	27
2.2.1	PHYSICAL REQUIREMENTS	27
2.2.2	POWER REQUIREMENTS	28
2.2.3	AMBIENT REQUIREMENTS	28
2.2.4	ELECTROMAGNETIC COMPATIBILITY CONSIDERATIONS	28
2.3	PL-1000TN FRONT PANEL	28
2.3.1	FRONT PANEL LEDs	29
2.3.2	PL-1000TN OPTICAL CONNECTIONS EXAMPLE	29
2.4	INSTALLING THE PL-1000TN UNIT	30
2.4.1	PACKAGE CONTENTS	30
2.4.2	REQUIRED EQUIPMENT	31
2.4.3	CABLE CONNECTIONS	31
3	OPERATION AND PRELIMINARY CONFIGURATION	35
3.1	OPERATING INSTRUCTIONS	35
3.1.1	CONNECTING AND CONFIGURING THE TERMINAL	35

3.1.2	TURNING ON THE PL-1000TN	36
3.2	PERFORMING PRELIMINARY CONFIGURATION.....	36
3.3	ACCESSING THE WEB APPLICATION	37
3.3.1	WEB BROWSER REQUIREMENTS	37
3.3.2	PREREQUISITES FOR ACCESSING THE WEB APPLICATION	38
3.3.3	LOGGING IN TO THE WEB APPLICATION	38
3.3.4	NAVIGATING THE WEB APPLICATION	39
3.3.5	LOGGING OUT OF THE WEB APPLICATION	42
4	SECURITY MANAGEMENT	43
4.1	USER ACCESS LEVELS.....	43
4.2	USER AUTHENTICATION METHODS	43
4.2.1	LOCAL AUTHENTICATION.....	44
4.2.2	REMOTE AUTHENTICATION.....	44
4.3	SECURITY SETTINGS.....	46
4.3.1	USERS TAB (ADMINISTRATOR)	47
4.3.2	USERS TAB (NON-ADMINISTRATOR).....	50
4.3.3	RADIUS TAB (ADMINISTRATOR)	51
5	FAULT MANAGEMENT.....	55
5.1	FAULT VIEWS.....	55
5.1.1	ALARMS	55
5.1.2	EVENTS.....	56
5.1.3	CONFIGURATION CHANGES	56
5.2	GENERAL FAULT PROCEDURE	57
5.3	SYSTEM FAULTS	58
5.3.1	ALARMS TAB.....	59
5.3.2	EVENTS TAB	61
5.3.3	CONFIGURATION CHANGES TAB	62
5.4	ALL FAULTS	64
5.4.1	ALARMS TAB.....	65
5.4.2	EVENTS TAB	67
5.4.3	CONFIGURATION CHANGES TAB	68
5.5	UPLINK PORT FAULTS	70
5.5.1	ALARMS TAB.....	71
5.5.2	EVENTS TAB	73
5.5.3	CONFIGURATION CHANGES TAB	74
5.6	SERVICE PORT FAULTS	76

5.6.1	ALARMS TAB.....	77
5.6.2	EVENTS TAB.....	79
5.6.3	CONFIGURATION CHANGES TAB.....	80
5.7	MANAGEMENT PORT FAULTS.....	82
5.7.1	ALARMS TAB.....	83
5.7.2	EVENTS TAB.....	85
5.7.3	CONFIGURATION CHANGES TAB.....	87
5.8	ETHERNET PORT FAULTS.....	88
5.8.1	ALARMS TAB.....	89
5.8.2	EVENTS TAB.....	91
5.8.3	CONFIGURATION CHANGES TAB.....	93
5.9	EDFA FAULTS.....	94
5.9.1	ALARMS TAB.....	95
5.9.2	EVENTS TAB.....	97
5.9.3	CONFIGURATION CHANGES TAB.....	98
5.10	COM PORT FAULTS.....	100
5.10.1	ALARMS TAB.....	101
5.10.2	EVENTS TAB.....	103
5.10.3	CONFIGURATION CHANGES TAB.....	105
5.11	PSU FAULTS.....	106
5.11.1	ALARMS TAB.....	107
5.11.2	EVENTS TAB.....	109
5.11.3	CONFIGURATION CHANGES TAB.....	111
6	CONFIGURATION MANAGEMENT.....	113
6.1	CONFIGURATION OPERATIONS.....	113
6.2	GENERAL CONFIGURATION PROCEDURE.....	115
6.3	SYSTEM CONFIGURATION.....	116
6.3.1	GENERAL TAB.....	117
6.3.2	INVENTORY TAB.....	119
6.3.3	LICENSE TAB.....	120
6.3.4	TIME TAB.....	122
6.3.5	IP TAB.....	124
6.3.6	SNMP TAB.....	127
6.3.7	SYSLOG TAB.....	129
6.4	UPLINK PORT CONFIGURATION.....	131
6.4.1	PORT TAB.....	132
6.4.2	XFP TAB.....	135
6.4.3	ALS TAB.....	137

6.4.4	APS TAB	139
6.4.5	OTN TAB	142
6.5	SERVICE PORT CONFIGURATION	144
6.5.1	PORT TAB	145
6.5.2	SFP+ TAB	148
6.5.3	ALS TAB	149
6.5.4	APS TAB	151
6.6	MANAGEMENT PORT CONFIGURATION	154
6.6.1	MNG TAB	155
6.6.2	SFP TAB	157
6.6.3	ALS TAB	158
6.7	ETHERNET PORT CONFIGURATION	160
6.7.1	ETHERNET TAB	160
6.8	MUX/DEMUX CONFIGURATION	162
6.8.1	MUX/DEMUX TAB	162
6.9	EDFA CONFIGURATION	163
6.9.1	EDFA TAB	164
6.10	COM PORT CONFIGURATION	166
6.10.1	COM TAB	167
6.10.2	APS TAB	169
6.11	PSU CONFIGURATION	171
6.11.1	PSU TAB	171
6.12	FAN UNIT CONFIGURATION	172
6.12.1	FAN UNIT TAB	173
7	PERFORMANCE MONITORING	175
7.1	OPTICAL INFORMATION	175
7.1.1	OPTICAL INFORMATION TAB	176
7.2	PORT PERFORMANCE MONITORING	177
7.3	UPLINK PERFORMANCE MONITORING	178
7.3.1	VIEWING UPLINK PORT PERFORMANCE MONITORING	179
7.3.2	VIEWING OPTICAL LEVEL PERFORMANCE MONITORING	183
7.4	SERVICE PERFORMANCE MONITORING	185
7.4.1	VIEWING NATIVE SIGNAL PERFORMANCE MONITORING	186
7.4.2	VIEWING OPTICAL LEVEL PERFORMANCE MONITORING	190
7.5	MANAGEMENT PORT PERFORMANCE MONITORING	192
7.5.1	VIEWING OPTICAL PERFORMANCE MONITORING	193

7.6	EDFA PERFORMANCE MONITORING	196
7.6.1	VIEWING OPTICAL PERFORMANCE MONITORING	197
8	MAINTENANCE.....	201
8.1	SYSTEM MAINTENANCE.....	201
8.1.1	RESTART TAB.....	202
8.1.2	LOG FILES TAB.....	204
8.1.3	CONFIGURATION TAB.....	205
8.1.4	SOFTWARE TAB	208
8.2	DIAGNOSTIC TESTS	210
8.2.1	FACILITY LOOPBACK TEST	210
8.2.2	PRBS TEST.....	211
8.3	UPLINK PORT MAINTENANCE	212
8.3.1	DIAGNOSTICS TESTS TAB	212
8.4	SERVICE PORT MAINTENANCE.....	214
8.4.1	DIAGNOSTICS TESTS TAB	214
8.5	EXTERNAL ALARM MAINTENANCE	216
8.5.1	EXTERNAL ALARM MAINTENANCE TAB.....	216
9	TOPOLOGY MANAGEMENT.....	219
9.1	NETWORK TOPOLOGY.....	219
9.1.1	NETWORK TOPOLOGY TAB	220
9.1.2	ZOOMING IN AND OUT OF THE TOPOLOGY DISPLAY.....	223
9.1.3	BROWSING OTHER NODES	223
9.1.4	DEFINING MULTIPLE NODES AS MULTI-CHASSIS.....	224
10	REMOTE MANAGEMENT CONFIGURATION	227
10.1	REMOTE MANAGEMENT CONFIGURATION EXAMPLE	227
10.1.1	SETTING UP POINT-TO-POINT MANAGEMENT	227
10.1.2	CONFIGURING MANAGEMENT FOR PL-1000TN A	228
10.1.3	CONFIGURING MANAGEMENT FOR PL-1000TN B	229
10.1.4	ACCESSING THE WEB APPLICATION FROM MANAGEMENT A TO PL-1000TN A.....	231
10.1.5	ACCESSING THE WEB APPLICATION FROM MANAGEMENT A TO PL-1000TN B.....	231
10.1.6	ACCESSING THE WEB APPLICATION FROM MANAGEMENT B TO PL-1000TN B.....	232
10.1.7	ACCESSING THE WEB APPLICATION FROM MANAGEMENT B TO PL-1000TN A.....	232
11	CLI.....	235
11.1	GENERAL FEATURES	235
11.2	ACCESSING THE CLI	235
11.2.1	USING A SERIAL PORT	236
11.2.2	USING TELNET	236
11.2.3	USING SSH	237

11.3	CLI COMMAND TYPES	238
11.4	RUNNING CLI COMMANDS.....	239
11.4.1	GENERAL COMMANDS	240
11.4.2	PING COMMAND.....	243
11.4.3	INTERFACE COMMANDS	243
11.4.4	IP SETTING COMMANDS	244
11.4.5	LOG COMMANDS	246
11.4.6	SHOW COMMANDS.....	246
11.4.7	SERVICE COMMANDS	248
11.4.8	SYSTEM RESTART COMMAND.....	249
APPENDIX A: CONNECTION DATA.....		251
A.1	CONTROL CONNECTOR	251
A.2	ALARM CONNECTOR.....	251
A.3	ETH CONNECTOR	253
A.4	OPTICAL PL-1000TN CONNECTORS.....	254
A.4.1	UPLINK PORTS	254
A.4.2	SERVICE PORTS	254
A.4.3	MNG PORTS.....	255
A.4.4	MUX/DEMUX PORTS.....	255
A.4.5	COM PORTS.....	255
A.5	POWER SUPPLY COMBINATIONS	256
A.6	POWER CONNECTORS	256
A.7	PROTECTIVE GROUND TERMINAL	256
A.8	FIBER SHELF.....	257
APPENDIX B: ALARM AND EVENT MESSAGES.....		259
B.1	ALARM MESSAGES	259
B.2	CONFIGURATION EVENT MESSAGES	263
B.3	OTHER EVENT MESSAGES	264
APPENDIX C: TROUBLESHOOTING CHART		265
C.1	TROUBLESHOOTING CHART.....	265
INDEX.....		269

List of Figures

Figure 1: Typical Application for PL-1000TN Devices 4

Figure 2: PL-1000TN Front Panel 5

Figure 3: Four Transponders with MUX/DEMUX Configuration 6

Figure 4: Six Transponders with Booster EDFA Configuration 7

Figure 5: Two Transponders with Pre-Amp EDFA Configuration 7

Figure 6: Two Transponders with Booster and Pre-Amp EDFA Configuration 8

Figure 7: PL-1000TN with 6 Unprotected Transponders 9

Figure 8: PL-1000TN with Dual COM Ports 10

Figure 9: PL-1000TN with Protected MUX/DEMUX Configuration 11

Figure 10: PL-1000TN Management Ports 11

Figure 11: PL-1000TN 8 Ports with Transponder Protection 13

Figure 12: PL-1000TN with Transponder Protection 13

Figure 13: Fiber Protection with Optical Switch 14

Figure 14: PL-1000TN with Optical Switch 14

Figure 15: Class 1M Laser Warning 26

Figure 16: Class 3B Laser Warning 26

Figure 17: PL-1000TN Front Panel 28

Figure 18: Connections between the Optical Ports (Example) 30

Figure 19: Login Window 38

Figure 20: System Configuration Window 39

Figure 21: PL-1000TN Item Buttons 39

Figure 22: PL-1000TN Sidebar Buttons 40

Figure 23: PL-1000TN Tabs (Example) 41

Figure 24: PL-1000TN Users Tab 42

Figure 25: Security Settings Window 46

Figure 26: Users Tab (Administrator) 47

Figure 27: Confirm Changes 48

Figure 28: Confirm Changes 49

Figure 29: Confirm Delete 49

Figure 30: Users Tab (Non-Administrator) 50

Figure 31: Confirm Changes 50

Figure 32: Radius Tab (Administrator) 51

Figure 33: Confirm Configuration 52

Figure 34: System Fault Window 58

Figure 35: Alarms Tab 59

Figure 36: Events Tab 61

Figure 37: Configuration Changes Tab 62

Figure 38: All Fault Window 64

Figure 39: Alarms Tab 65

Figure 40: Events Tab 67

Figure 41: Configuration Changes Tab 68

Figure 42: Uplink Port Fault Window	70
Figure 43: Alarms Tab.....	71
Figure 44: Events Tab	73
Figure 45: Configuration Changes Tab.....	74
Figure 46: Service Port Fault Window.....	76
Figure 47: Alarms Tab.....	77
Figure 48: Events Tab	79
Figure 49: Configuration Changes Tab.....	80
Figure 50: Management Port Fault Window	82
Figure 51: Alarms Tab.....	83
Figure 52: Events Tab	85
Figure 53: Configuration Changes Tab.....	87
Figure 54: Ethernet Port Fault Window	88
Figure 55: Alarms Tab.....	89
Figure 56: Events Tab	91
Figure 57: Configuration Changes Tab.....	93
Figure 58: EDFA Fault Window	94
Figure 59: Alarms Tab.....	95
Figure 60: Events Tab	97
Figure 61: Configuration Changes Tab.....	98
Figure 62: COM Port Fault Window.....	100
Figure 63: Alarms Tab.....	101
Figure 64: Events Tab	103
Figure 65: Configuration Changes Tab.....	105
Figure 66: PSU Fault Window	106
Figure 67: Alarms Tab.....	107
Figure 68: Events Tab	109
Figure 69: Configuration Changes Tab.....	111
Figure 70: System Configuration Window	116
Figure 71: General Tab.....	117
Figure 72: Inventory Tab.....	119
Figure 73: License Tab	120
Figure 74: IP Tab - Dual Networks.....	124
Figure 75: IP Tab - Single Network	125
Figure 76: Confirm Changes	126
Figure 77: SNMP Tab	127
Figure 78: Syslog Tab	129
Figure 79: Confirm Configuration.....	129
Figure 80: Confirm Configuration.....	130
Figure 81: Uplink Port Configuration Window	131
Figure 82: Port Tab.....	132
Figure 83: Confirm Changes	132
Figure 84: Confirm Changes	133
Figure 85: XFP Tab	135

Figure 86: ALS Tab	137
Figure 87: APS Tab - Without Protection	139
Figure 88: APS Tab - With Protection	139
Figure 89: APS Groups	139
Figure 90: Confirm Changes	140
Figure 91: Confirm Changes	140
Figure 92: OTN Tab	142
Figure 93: Service Port Configuration Window	144
Figure 94: Port Tab	145
Figure 95: Confirm Changes	145
Figure 96: Confirm Changes	146
Figure 97: SFP+ Tab	148
Figure 98: ALS Tab	149
Figure 99: APS Tab - Without Protection	151
Figure 100: APS Tab - With Protection	151
Figure 101: APS Groups	151
Figure 102: Confirm Changes	152
Figure 103: Confirm Changes	152
Figure 104: Management Port Configuration Window	154
Figure 105: Confirm Changes	155
Figure 106: Confirm Changes	156
Figure 107: SFP Information Tab	157
Figure 108: ALS Tab	158
Figure 109: Ethernet Port Configuration Window	160
Figure 110: Ethernet Tab	160
Figure 111: MUX/DEMUX Configuration Window	162
Figure 112: MUX/DEMUX Tab (DWDM)	162
Figure 113: EDFA Configuration Window	163
Figure 114: EDFA Tab	164
Figure 115: Confirm Changes	164
Figure 116: Confirm Changes	165
Figure 117: COM Port Configuration Window	166
Figure 118: COM Tab	167
Figure 119: Confirm Changes	167
Figure 120: Confirm Changes	168
Figure 121: APS Tab	169
Figure 122: PSU Configuration Window	171
Figure 123: PSU Tab	171
Figure 124: FAN Unit Configuration Window	172
Figure 125: FAN Unit Tab	173
Figure 126: Optical Information Window	175
Figure 127: Optical Information Tab	176
Figure 128: Uplink Port Performance Monitoring Window	178
Figure 129: Uplink Port Performance Monitoring Tab	179
Figure 130: Optical Level Performance Monitoring	183

Figure 131: Service Port Performance Monitoring Window..... 185

Figure 132: Service Port Performance Monitoring Tab 186

Figure 133: Optical Level Performance Monitoring 190

Figure 134: Management Port Performance Monitoring Window..... 192

Figure 135: Optical Level Performance Monitoring 193

Figure 136: EDFA Performance Monitoring Window 196

Figure 137: Optical Level Performance Monitoring 197

Figure 138: System Maintenance Window..... 201

Figure 139: Restart Tab..... 202

Figure 140: Confirm Changes..... 203

Figure 141: Confirm Changes..... 203

Figure 142: Confirm Changes..... 203

Figure 143: Log Files Tab 204

Figure 144: System Log Files (Example)..... 204

Figure 145: Configuration Tab..... 205

Figure 146: Update System Configuration: Configuration File..... 206

Figure 147: Confirm System Overwrite..... 206

Figure 148: System Updating and Restarting Message 206

Figure 149: Opening .cfg Dialog Box 207

Figure 150: Software Tab 208

Figure 151: Software Download Message..... 209

Figure 152: Software Download Status Window..... 209

Figure 153: Confirm Changes..... 209

Figure 154: Confirm Changes..... 210

Figure 155: Facility Loopback Test..... 211

Figure 156: PRBS Test 211

Figure 157: Uplink Port Maintenance Window..... 212

Figure 158: Diagnostic Tests Tab..... 212

Figure 159: PRBS Test Results 213

Figure 160: Service Port Maintenance Window 214

Figure 161: Diagnostic Tests Tab..... 214

Figure 162: PRBS Test Results 215

Figure 163: External Alarm Maintenance Window 216

Figure 164: External Alarm Tab..... 216

Figure 165: Network Topology Window..... 219

Figure 166: Network Topology Tab 220

Figure 167: Linear Topology (Example) 221

Figure 168: Ring Topology (Example) 222

Figure 169: General Tab..... 224

Figure 170: Multi-Chassis Nodes..... 225

Figure 171: Point-to-Point Remote Management (Example) 227

Figure 172: IP Addresses: PL-1000TN A (Example)..... 228

Figure 173: SNMP Traps Table (Example)..... 229

Figure 174: IP Addresses: PL-1000TN B (Example)..... 230

Figure 175: Static Routing: PL-1000TN B (Example)	230
Figure 176: SNMP Traps Table (Example)	231
Figure 177: CLI Command Tree.....	239
Figure 178: External ALARM Diagram.....	252
Figure 179: DC Connector Wiring Diagram.....	256
Figure 180: Protective Ground Terminal Wiring Diagram.....	257
Figure 181: Fiber Shelf Diagram.....	257

List of Tables

Table 1: LINK Ports.....	8
Table 2: PL-1000TN Services	9
Table 3: LINK Ports in Protected Configuration	13
Table 4: Configure Interface Ethernet IP Command Options.....	37
Table 5: User Access Levels	43
Table 6: Attributes Used.....	44
Table 7: Users Tab Parameters (Administrator)	47
Table 8: Users Tab Parameters (Non-Administrator)	51
Table 9: Radius Tab Parameters (Administrator).....	52
Table 10: Alarms Tab Parameters	60
Table 11: Events Tab Parameters	62
Table 12: Configuration Changes Tab Parameters	63
Table 13: Alarms Tab Parameters.....	66
Table 14: Events Tab Parameters	68
Table 15: Configuration Changes Tab Parameters	69
Table 16: Alarms Tab Parameters	72
Table 17: Events Tab Parameters	74
Table 18: Configuration Changes Tab Parameters	75
Table 19: Alarms Tab Parameters	78
Table 20: Events Tab Parameters	80
Table 21: Configuration Changes Tab Parameters	81
Table 22: Alarms Tab Parameters	84
Table 23: Events Tab Parameters	86
Table 24: Configuration Changes Tab Parameters	88
Table 25: Alarms Tab Parameters	90
Table 26: Events Tab Parameters	92
Table 27: Configuration Changes Tab Parameters	94
Table 28: Alarms Tab Parameters.....	96
Table 29: Events Tab Parameters	98
Table 30: Configuration Changes Tab Parameters	99
Table 31: Alarms Tab Parameters.....	102
Table 32: Events Tab Parameters	104
Table 33: Configuration Changes Tab Parameters	106
Table 34: Alarms Tab Parameters.....	108
Table 35: Events Tab Parameters	110
Table 36: Configuration Changes Tab Parameters	112
Table 37: General Tab Parameters.....	117
Table 38: Inventory Tab Parameters	119
Table 39: License Tab Parameters	121
Table 40: Time Tab Parameters.....	123

Table 41: IP Tab Parameters.....	126
Table 42: SNMP Tab Parameters.....	128
Table 43: Syslog Tab Parameters	130
Table 44: Port Tab Parameters.....	133
Table 45: XFP Tab Parameters	135
Table 46: ALS Tab Parameters	138
Table 47: APS Tab Parameters	141
Table 48: OTN Tab Parameters.....	142
Table 49: Port Tab.....	146
Table 50: SFP+ Tab Parameters	148
Table 51: ALS Tab Parameters	150
Table 52: APS Tab Parameters	153
Table 53: MNG Tab Parameters	156
Table 54: SFP Tab Parameters	157
Table 55: ALS Tab Parameters	159
Table 56: Ethernet Tab Parameters.....	161
Table 57: MUX/DEMUX Tab Parameters.....	163
Table 58: EDFA Tab Parameters	165
Table 59: COM Tab Parameters	168
Table 60: APS Tab Parameters	169
Table 61: PSU Tab Parameters.....	172
Table 62: FAN Unit Tab Parameters	173
Table 63: Optical Information Tab Parameters.....	177
Table 64: Uplink Port Performance Monitoring Tab Parameters.....	180
Table 65: Uplink Port Performance Monitoring Tab Parameters.....	184
Table 66: Service Port Performance Monitoring Tab Parameters	187
Table 67: Service Port Performance Monitoring Tab Parameters	191
Table 68: Management Port Optical Level PM Parameters	194
Table 69: EDFA Optical Level PM Parameters	198
Table 70: PBRs Test Results	213
Table 71: PBRs Test Results	215
Table 72: External Alarm Maintenance Tab Parameters	217
Table 73: CONTROL Connector Wiring.....	251
Table 74: ALARM Interface, Pin Function	252
Table 75: ETH Port Connector, Pin Functions.....	253
Table 76: Uplink XFP Specifications.....	254
Table 77: Service SFP+ Specifications.....	254
Table 78: MNG Port Specifications	255
Table 79: MUX/DEMUX Port Specifications	255
Table 80: COM Port Specifications	255
Table 81: Alarm Messages	259
Table 82: Configuration Change Messages	263
Table 83: Other Event Messages	264
Table 84: Troubleshooting Chart.....	265

1 Introduction

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

In this Chapter

Overview	1
Configurations.....	5
Functional Description	8
Technical Specifications.....	17

1.1 Overview

The PL-1000TN is an optical transport device. It is a highly integrated solution for transporting various protocols, such as 8G/10G FC, 10GbE-LAN, and OC-192/STM-64, over an optical transport network.

The PL-1000TN is an OTU2 mapper. The OTN layer provides two additional key benefits:

- Easy common management and maintenance of the optical layer infrastructure regardless of the client type.
- Enhanced Forward Error Correction (FEC) codes suitable for extremely long distance amplified DWDM networks. This typically eliminates the need for expensive regenerator sites along the optical network and enables using cascaded amplifiers across the infrastructure to build a ROADM-based solution.

The PL-1000TN is a highly integrated device that can incorporate MUX/DEMUX, Erbium Doped Fiber Amplifier (EDFA), and Dispersion Compensation Module (DCM) modules.

The PL-1000TN provides 1+1 facility protection for the uplink ports. It also supports an optional Optical Switch that provides 1+1 facility protection for the optical signal.

The PL-1000TN is fully interoperable with the PacketLight family of products.

1.1.1 Main Features

The PL-1000TN combines the following key features:

- Two, four, or six independent standard multi-rate OTU2 OTN transponders
- Provides a full OTN managed layer
- Supported clients:
 - 8G/10G FC
 - 10GbE-LAN
 - OC-192/STM-64

- Supports G.Sup43 standard mappings
- Supports multiple FEC types:
 - G.709
 - I.4 (as defined by G.975 Appendix I.4)
- Uses standard MSA pluggable XFP optics for the network side of the transponder
- Uses standard MSA pluggable SFP+ optics for the service side of the transponder
- Supports tunable XFP-based 50/100 GHz DWDM uplinks
- Optional integrated EDFA and/or optical MUX/DEMUX modules
- Optional integrated Optical Switch module
- Optional DCM module
- Automatic Laser Shutdown (ALS) on all optical ports
- Two 100M OSC management channels based on pluggable SFP optics for remote management
- Remote management with in-band or out-of-band Optical Supervisory Channel (OSC)
- 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:
 - Alarm and Event fault management
 - Uplink (line) and service (client) performance monitoring (PM)
 - Facility loopback
 - Diagnostic Pseudo Random Binary Sequence (PRBS)
 - External alarms
- Operates on single or dual fiber solutions

- Pluggable FAN unit
- AC and DC, single or dual pluggable power supply units (PSUs)

1.1.2 Typical Application

Designed as an optical transport device, the PL-1000TN is typically deployed as customer premises equipment (CPE) in enterprise campus environments.

The PL-1000TN supports up to two integrated EDFA modules and up to two optical MUX/DEMUX modules.

Two additional Optical Supervisory Channel (OSC) ports may be used for transmission of the management traffic for remote management of the PL-1000TN.

The PL-1000TN 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-1000TN 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.

This solution is suitable for the following applications:

- Transporting multiple 8/10G FC clients over long distance optical networks
- Multi-rate transponders for ROADM based applications
- Infrastructure for a robust loss-less packet over optical transport networks
- Low cost back-bone solution achieved by reducing the number of required regenerators
- Building efficient and flexible CWDM/DWDM solutions for the Enterprise.

The following figure illustrates a typical application for standalone PL-1000TN units. They are deployed as CPE in enterprise campus environments, and connect the local LANs and SANs in the two campuses across a fiber connection or via a DWDM public network.

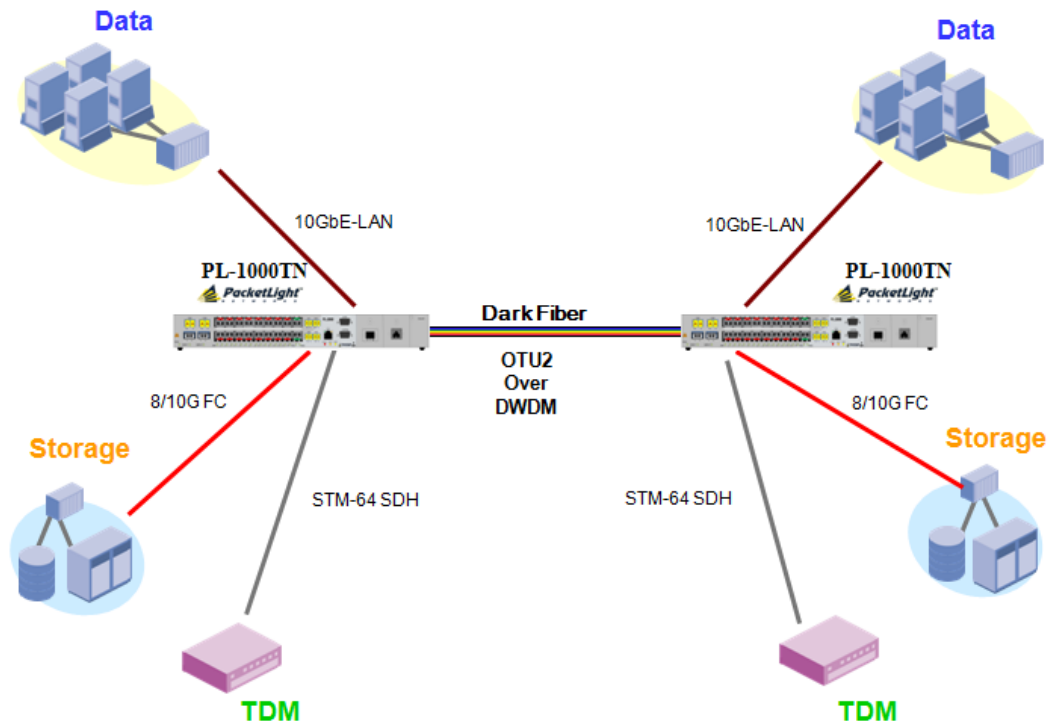


Figure 1: Typical Application for PL-1000TN Devices

1.1.3 Physical Description

The PL-1000TN is a compact 1U unit intended for installation in a 19-inch or 23-inch rack or placed on a desktop or shelf.

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

The following figure shows the front panel of the PL-1000TN with two MUX/DEMUX modules.

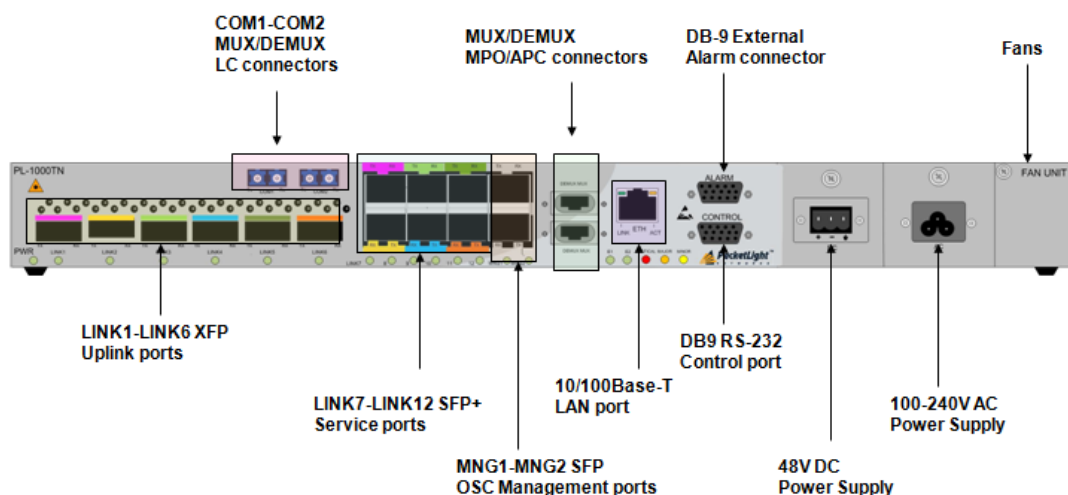


Figure 2: PL-1000TN Front Panel

1.2 Configurations

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

1.2.1 PL-1000TN Configurations

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

1.2.1.1 Transponder Configurations

The PL-1000TN is supplied with two, four, or six transponders. A license is required when adding transponders to the two or four transponder configuration.

The following licenses are available for the PL-1000TN:

- **4-Transponder license**: The PL-1000TN supports four transponders.
- **6-Transponder license**: The PL-1000TN supports six transponders.

1.2.1.2 MUX/DEMUX Configurations

The PL-1000TN can be ordered with two, one, or no DWDM MUX/DEMUX modules. Single fiber MUX/DEMUX modules are also supported.

1.2.1.3 EDFA Module Configurations

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

1.2.1.4 Optical Switch Configurations

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

1.2.1.5 DCM Configurations

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

1.2.2 Example Configurations

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

1. Four transponder configuration:

- Four transponders
- One MUX/DEMUX module
- One OSC management channel

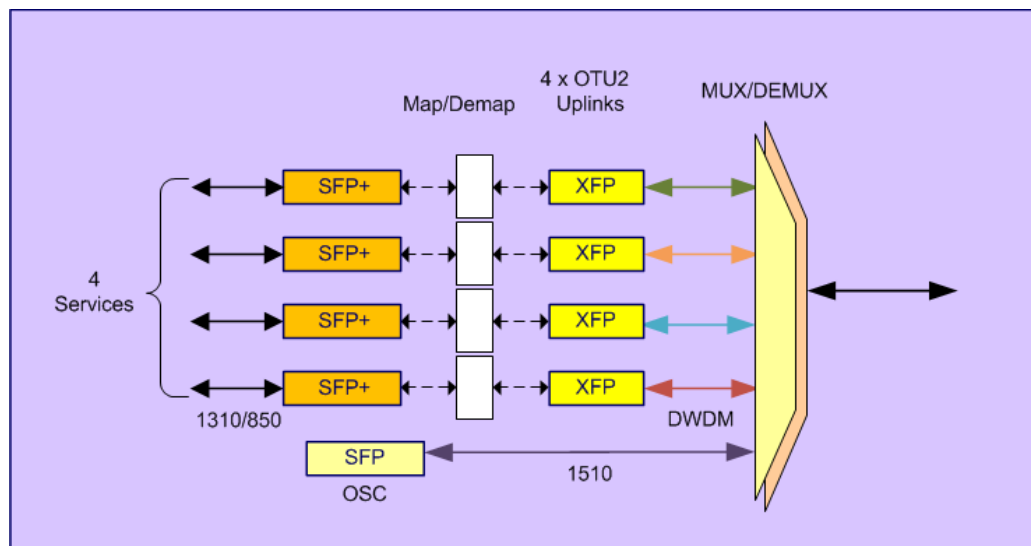


Figure 3: Four Transponders with MUX/DEMUX Configuration

2. Six transponder configuration with Booster EDFA:

- Six transponders
- One MUX/DEMUX module
- One Booster EDFA
- One OSC management channel

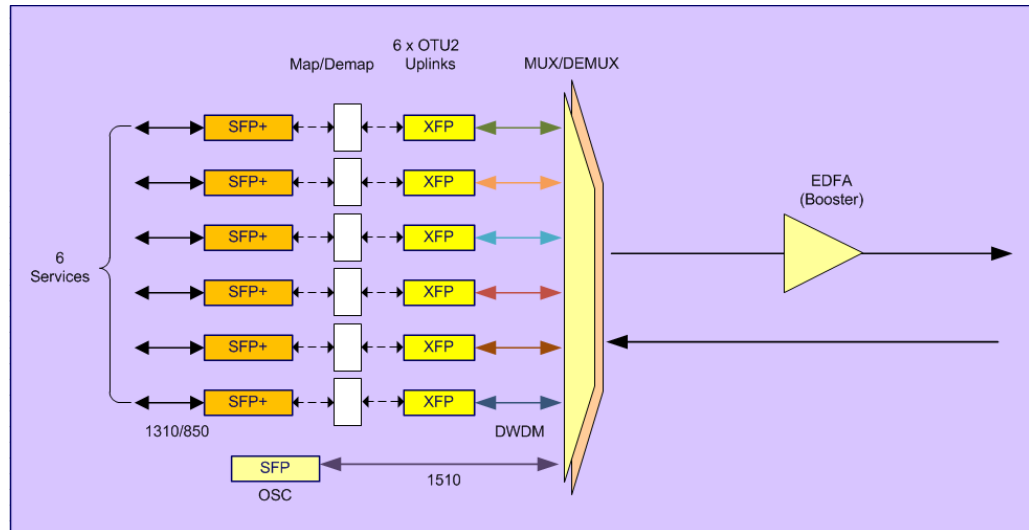


Figure 4: Six Transponders with Booster EDFA Configuration

3. Two transponder configuration with Pre-Amp EDFA:

- Two transponders
- One MUX/DEMUX module
- One Pre-Amp EDFA
- One OSC management channel

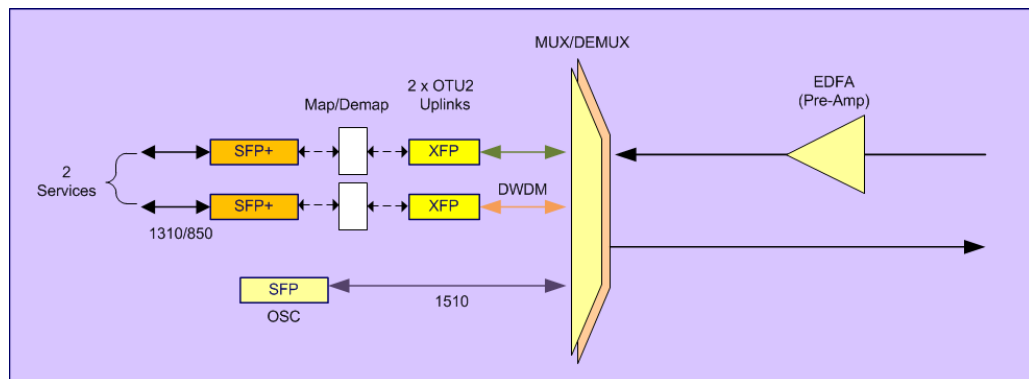


Figure 5: Two Transponders with Pre-Amp EDFA Configuration

4. Two transponder configuration with Booster and Pre-Amp EDFA:

- Two transponders
- One MUX/DEMUX module
- One Booster EDFA
- One Pre-Amp EDFA

- One OSC management channel

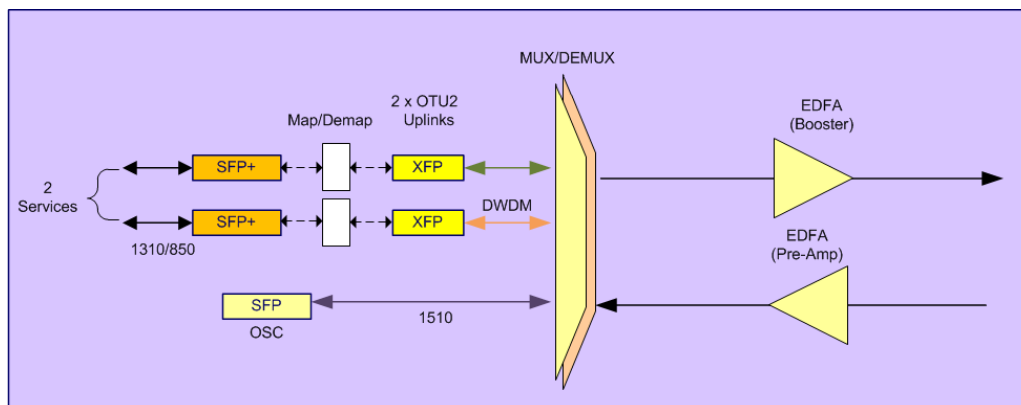


Figure 6: Two Transponders with Booster and Pre-Amp EDFA Configuration

1.3 Functional Description

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

1.3.1 PL-1000TN Ports

This section describes the PL-1000TN ports.

1.3.1.1 LINK Ports

A LINK port is part of an unprotected transponder or protected transponder.

The LINK ports function as the uplink and service ports. The uplink ports are labeled "LINK 1" through "LINK 6" and the service ports are labeled "LINK 7" through "LINK 12".

Table 1: LINK Ports

Port Type	Transceiver Type	Front Panel Designation
Uplink	Optical XFP WDM	LINK 1 - LINK 6
Service	Optical SFP+ 850 nm multi-mode or 1310 nm single mode with the following rates: <ul style="list-style-type: none"> • 8G FC • 10G FC • 10GbE-LAN • OC-192 • STM-64 	LINK 7 - LINK 12

1.3.1.1.1 PL-1000TN Services

The following table describes the PL-1000TN services.

Table 2: PL-1000TN Services

Service Type	Service Bit Rate	Service Standard	Uplink Bit Rate	Uplink Standard
8G FC to OTU2	8.5G	T11 FC-PI-4	10.7092	G.709
10G FC to OTU2f	10.518G	T11 FC-PI-3	11.3176	ITU G.Sup43
10GbE-LAN to OTU2e	10.31G	IEEE 802.3ae	11.0957	ITU G.Sup43
OC-192 to OTU2	9.953G	Telcordia GR-253-CORE	10.7092	G.709
STM-64 to OTU2	9.953G	ITU-T G.707	10.7092	G.709

1.3.1.1.2 Unprotected Transponders

Depending on the configuration, the PL-1000TN supports up to six unprotected transponders as follows:

- 2-transponders configuration (uplink/service):
 - LINK1/LINK7
 - LINK2/LINK8
- 4-transponders configuration (uplink/service):
 - LINK1/LINK7
 - LINK2/LINK8
 - LINK3/LINK9
 - LINK4/LINK10
- 6-transponders configuration (uplink/service):
 - LINK1/LINK7
 - LINK2/LINK8
 - LINK3/LINK9
 - LINK4/LINK10
 - LINK5/LINK11
 - LINK6/LINK12

The following figure shows a PL-1000TN with six unprotected transponders.

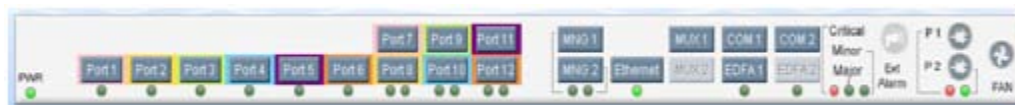


Figure 7: PL-1000TN with 6 Unprotected Transponders

1.3.1.2 COM Ports

The COM ports are duplex LC connectors placed on the front panel of the PL-1000TN. These ports are connected to the networks and are used to convey the aggregated optical signal.

The following are the available COM port configurations:

- **No COM ports:** When there are no COM ports, the uplink ports of the PL-1000TN are connected to the network via external MUX/DEMUX modules.
- **Single COM port:** The single COM port is used for the unprotected configuration of PL-1000TN.
- **Dual COM ports:** The dual COM ports may be used for:
 - Uplink Protection application
 - Optical Switch Protection application

For more information, see [Connection Data](#) (p. 251).

The following figure illustrates a PL-1000TN with dual COM ports.



Figure 8: PL-1000TN with Dual COM Ports

1.3.1.3 MUX/DEMUX Ports

The MUX/DEMUX ports are one or two Multifiber Pull Off (MPO) connectors.

The MUX/DEMUX port, together with the ribbon cable attached to it, is used to connect the uplink ports and OSC to the passive MUX/DEMUX module.

There are two configurations of the MUX/DEMUX ports: **Single** and **Dual**.

- **Single:** In a single port configuration, there is one port labeled "MUX/DEMUX".
- **Dual:** In a dual port configuration, the front panel has two ports labeled "MUX" and "DEMUX".

For more information, see [Connection Data](#) (p. 251).

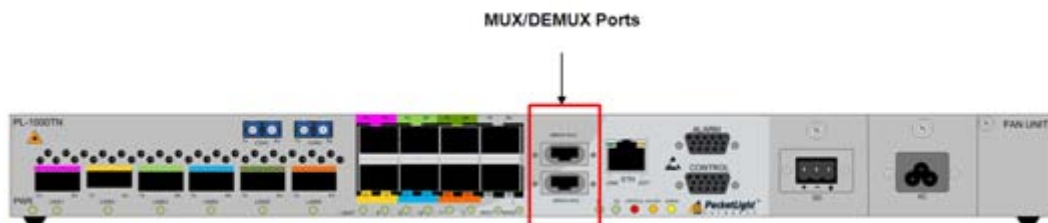


Figure 9: PL-1000TN with Protected MUX/DEMUX Configuration

1.3.1.4 ALARM Port

The PL-1000TN 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. 251).

1.3.1.5 Management Ports

This section describes the PL-1000TN management ports.

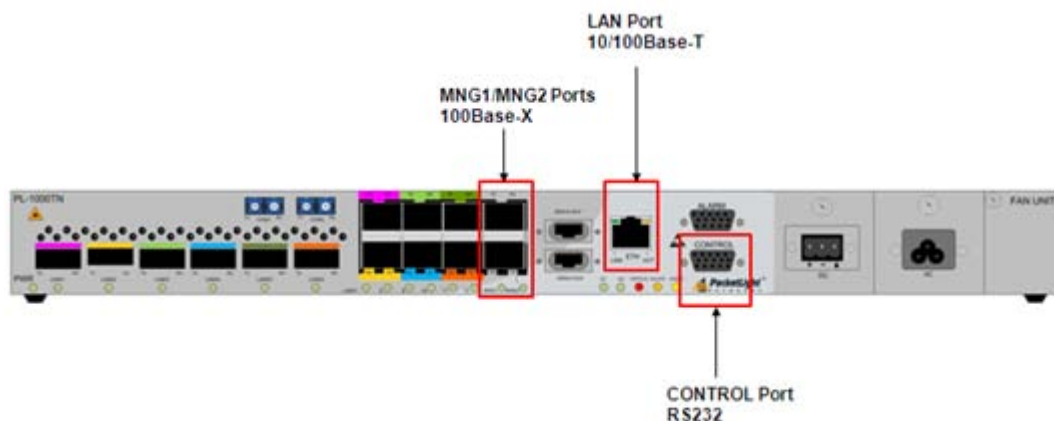


Figure 10: PL-1000TN Management Ports

1.3.1.5.1 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-1000TN 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-1000TN serial CONTROL connector.

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

For more information, see [Connection Data](#) (p. 251).

1.3.1.5.2 ETH Port

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

For more information, see [Connection Data](#) (p. 251).

1.3.1.5.3 MNG Ports

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

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

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

For more information, see [Connection Data](#) (p. 251).

1.3.2 APS for PL-1000TN

In protected configuration, the PL-1000TN supports unidirectional, non-revertive, 1+1 facility protection.

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

The PL-1000TN provides two types of Automatic Protection Switching (APS):

- **Transponder protection:** Protects the optical fiber and transponder uplink transceiver.
- **Fiber protection:** Protects the optical fiber.

1.3.2.1 Transponder Protection

The PL-1000TN can be configured with up to three protected transponders.

The transponder protection ensures service continuity in case of a fiber break or a failure of an uplink XFP.

The transponder protection is usually provided by the PL-1000TN with two MUX/DEMUX modules. See the following figure.

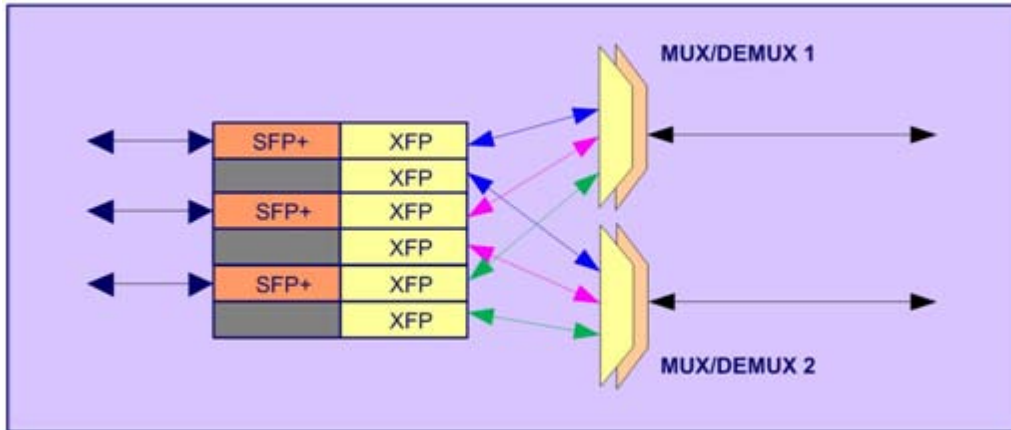


Figure 11: PL-1000TN 8 Ports with Transponder Protection

For protected transponders, four LINK ports function as a single protected transponder as follows.

Table 3: LINK Ports in Protected Configuration

Protection Group	Port	Role	Transceiver Type
Group 1	LINK 1	Working uplink	XFP
	LINK 2	Protection uplink	XFP
	LINK 7	Service port	SFP+
	LINK 8	Unused	-
Group 2	LINK 3	Working uplink	XFP
	LINK 4	Protection uplink	XFP
	LINK 9	Service port	SFP+
	LINK 10	Unused	-
Group 3	LINK 5	Working uplink	XFP
	LINK 6	Protection uplink	XFP
	LINK 11	Service port	SFP+
	LINK 12	Unused	-

The figure below shows a PL-1000TN with three APS groups marked with colors as displayed in the Web application.



Figure 12: PL-1000TN with Transponder Protection

1.3.2.2 Fiber Protection

The PL-1000TN may be ordered with an Optical Switch module to provide fiber protection.

When an Optical Switch module is installed, its input is connected to the output of the MUX/DEMUX module, and its two outputs are connected internally to two COM ports.

The Optical Switch performs APS based on the received optical power level of the incoming aggregated optical signal. Therefore, the Optical Switch can be used to protect against cable break, but not against uplink transceiver failure.

The facility protection ensures service continuity in case of a fiber break. The fiber protection based on the Optical Switch module is supported only for point-to-point topologies.

The following figure shows an Optical Switch Protection application.

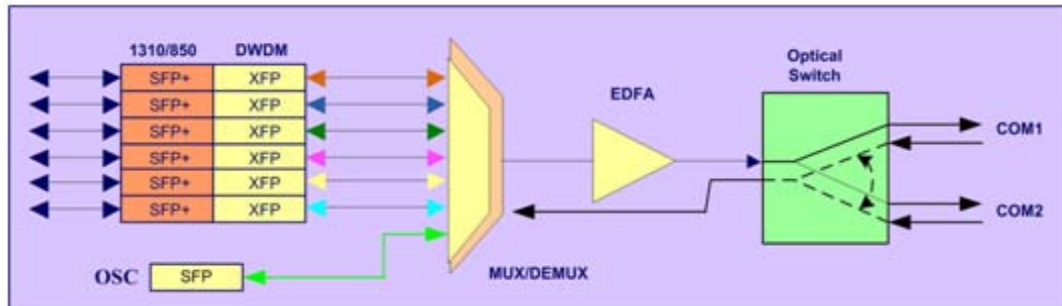


Figure 13: Fiber Protection with Optical Switch

When an Optical Switch is installed, the COM1 and COM2 buttons are shown and enabled in the Web application. In this case, the protection is done on the entire optical signal, which includes all channels.

The following figure shows the front panel of the PL-1000TN as displayed in the Web application.



Figure 14: PL-1000TN with Optical Switch

1.3.3 PL-1000TN Modules

This section describes the PL-1000TN modules.

1.3.3.1 MUX/DEMUX Modules

The PL-1000TN supports one, two, or no optical MUX/DEMUX modules.

The MUX/ DEMUX modules are connected externally by a ribbon to the uplink ports on one side via the MUX/DEMUX port and to the WDM network/fiber (or

internally to the Optical Amplifier Input, if present) on the other side via the COM port.

With the use of a PL-300 device, several PL-1000TN devices can be connected, providing expanded capabilities to aggregate 4, 8, 16, or 40 wavelengths.

1.3.3.2 EDFA Modules

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

- **Booster EDFA:** It is used on the Tx optical path. It can be connected externally to the front panel LC adapter if the MUX is not installed in the PL-1000TN or internally between the output fiber of the MUX and the COM port on the front panel.
- **Pre-Amp EDFA:** It is used on the Rx optical path. It can be connected externally to the front panel LC adapter if the DEMUX is not installed in the PL-1000TN or internally between the COM port on the front panel and the input fiber of the DEMUX.

1.3.3.3 Optical Switch Module

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

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

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

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

The Optical Switch performs APS based on the received optical power level of the incoming aggregated optical signal. Therefore, the Optical Switch can be used to protect against cable break but not against uplink transceiver failure.

1.3.3.4 DCM Module

The PL-1000TN may be ordered with an optional DCM.

The DCM module provides compensation for a fixed amount of chromatic dispersion caused by the optical fiber, wavelength spacing and the range traversed by the optical signal.

NOTE: The PL-1000TN can be ordered with several configurations of the DCM module according to actual requirements.

1.3.3.5 Power Supply Units

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

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

The maximum power consumption of the PL-1000TN is 75W.

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

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

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

1.3.3.6 FAN Unit

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



CAUTION: Air intake vents should be clear of obstruction.

1.3.4 Management Functionality

The PL-1000TN 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

1.3.4.1 Management Protocols

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

1.3.4.1.1 CLI Management

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

For more information, see [CLI](#) (p. 235).

1.3.4.1.2 Web-based Management

The PL-1000TN 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. 113).

1.3.4.1.3 SNMP Management

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

1.4 Technical Specifications

Transponders	Number of Transponders	2, 4, 6
	Mapping	<ul style="list-style-type: none"> • 8G FC to OTU2 • 10G FC to OTU2f • 10GbE-LAN to OTU2e • OC-192 to OTU2 • STM-64 to OTU2
	Connector	LC
Uplink (Line) Ports	Number of Ports	2, 4, 6
	Wavelength	<ul style="list-style-type: none"> • CWDM optics and ITU grid • DWDM ITU G.694.1 Grid Channels 15-60 C-Band with 100 GHz spacing or 50 GHz tunable
	Optical Reach	40 km, 80 km, or 200 km
	Optical Power Output	-1 to +2 dBm
	Sensitivity	-24 dBm APD
	Bit Rate	<ul style="list-style-type: none"> • OTU2: 10.7092 Gbps • OTU2e: 11.0957 Gbps (as per G.Sup43) • OTU2f: 11.3176 Gbps
	Connector	XFP transceiver
Service (Client) Ports	Number of Ports	2, 4, 6
	Service Types	<ul style="list-style-type: none"> • 8G FC • 10G FC • 10GbE-LAN • OC-192 • STM-64

	Connector	SFP+ transceiver
MUX/DEMUX Modules	Number of Modules	0,1, or 2
	Channels	2
	Wavelength	DWDM ITU G.694.1 Channels 15-60 C-Band
	Express Channel	1511 +/- 6.5 nm
	Link Loss (MUX+DEMUX)	< 6 dB
	Spacing	100 GHz
	Express Channel Link Loss	< 1.5 dB
Optical Amplifiers (EDFA)	Number of Modules	0, 1, or 2
	Output Power	<ul style="list-style-type: none"> • Booster: 14 dBm, 17 dBm, 20 dBm, 23 dBm • Pre-Amp: +5 dBm
	Optical Gain	<ul style="list-style-type: none"> • Booster: +10 to +22 dB • Pre-Amp: +18 dB
	Input Power	<ul style="list-style-type: none"> • 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.
Optical Switch Module	Number of Modules	0 or 1
	Switching Time	< 50 ms
	Protection Type	1+1 Non-Revertive Fiber Protection
DCM Module	Number of Modules	0 or 1 Tunable active module
	Fiber Type	ITU-T G.652
	Spacing	50/100 GHz
	Range	Up to 200 km
Supervisory and Management Ports	CONTROL Port	<p>Used for initial configuration of the node IP or for local access to CLI.</p> <ul style="list-style-type: none"> • 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	<p>Management LAN port for out-of-band access.</p> <ul style="list-style-type: none"> • Interface: 10/100 Base-T • Connector: RJ-45 <p>NOTE: Initial IP configuration can be done via RS-232.</p>
	MNG1 and MNG2 Ports	<p>2 Optical management ports.</p> <ul style="list-style-type: none"> • Interface: 100 Base-FX • Connector: SFP transceiver • Wavelength: <ul style="list-style-type: none"> ▪ 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 <p>NOTE: IP of the MNG port can be configured using the Web application.</p>
COM Ports	COM1 and COM2 (in a configuration with two COM ports)	<p>1 or 2 Fixed duplex LC connectors.</p> <ul style="list-style-type: none"> • Fiber type: Single mode • Fiber size: 2 mm optical • Connector type: LC with or without protective shutters • Port type: Optical COM port
Environment Alarms	ALARM Port	<p>Used for external office alarms.</p> <ul style="list-style-type: none"> • Connector: DB-9, female • Environmental: 1 input and 1 output
System LEDs	PWR	<ul style="list-style-type: none"> • Green blinking: Power-up stage • Green: Normal operation
	CRT	<ul style="list-style-type: none"> • OFF: No Critical alarm detected • Red: Critical alarm detected
	MAJ	<ul style="list-style-type: none"> • OFF: No Major alarm detected • Red: Major alarm detected
	MIN	<ul style="list-style-type: none"> • OFF: No Minor alarm detected • Red: Minor alarm detected
Uplink (Line) Port LEDs	LINK 1 to LINK 6	<ul style="list-style-type: none"> • OFF: Admin Down • Blinking: Facility loopback or PRBS test • Green: Normal operation • Red: Alarm detected
Service Port LEDs	LINK 7 to LINK 12	<ul style="list-style-type: none"> • OFF: Admin Down • Blinking: Facility loopback or PRBS test • Green: Normal operation • Red: Alarm detected
MNG Port LEDs	MNG 1 and MNG 2	<ul style="list-style-type: none"> • OFF: Admin Down • Green: Normal operation • Red: Alarm detected

COM/Amplifier LEDs	E1 and E2 (in a configuration with two EDFA modules or with an Optical Switch)	<ul style="list-style-type: none"> • OFF: Admin Down No EDFA module or Optical Switch installed. • Green: The corresponding amplifier module or Optical Switch port is operational (DWDM applications only). • Red: Failure detected on the corresponding amplifier module or Optical Switch port.
ETH Port LEDs	LINK	<ul style="list-style-type: none"> • OFF: The port is disconnected • Green: Normal operation
	ACT	<ul style="list-style-type: none"> • Yellow blinking: Transmit and/or receive activity detected on the port.
PSU LEDs	PWR	<ul style="list-style-type: none"> • OFF: PSU is not installed • Green: Normal operation • Red: PSU failure detected
Network Management	Protocols	<ul style="list-style-type: none"> • CLI over RS-232 or Telnet/SSH • Web-based HTTP/HTTPS management • SNMPv2c • Radius • Syslog • SNTF • 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-1000TN system log files, which can be exported to a text file for offline viewing.
	Performance Monitoring	PM counters for Native Signal and/or Optical PM .

	Native Signal	<p>PM counters for 15 minute and one day intervals for the following:</p> <ul style="list-style-type: none"> • Uplink ports (Port 1 - Port 6) <ul style="list-style-type: none"> ▪ Counters based on OTU2 Near/Far Section BIP-8 errors: Errored Seconds (ES), Severely Errored Seconds (SES), and Unavailable Seconds (UAS) ▪ Counters based on ODU Near/ Far Path BIP-8 errors: Errored Seconds, Severely Errored Seconds, and Unavailable Seconds ▪ Counters based on FEC Corrected/Uncorrected errors: Errored Seconds, Severely Errored Seconds, and Unavailable Seconds • Service ports (Port 7 - Port 12) <ul style="list-style-type: none"> ▪ Counters for 8G FC services based on 8B/10B coding violation errors: Errored Seconds, Severely Errored Seconds, and Unavailable Seconds ▪ Counters for 10G FC and 10GbE-LAN services based on 64B/66B coding violation errors: Errored Seconds, Severely Errored Seconds, and Unavailable Seconds ▪ Counters for OC-192 (SONET) services based on Section B1 errors: Errored Seconds, Severely Errored Seconds, Severely Errored Frames (SEF) ▪ Counters for STM-64 (SDH) services based on Section B1 errors: Errored Seconds, Severely Errored Seconds, Out of Frame Seconds
	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	1 or 2
	Redundancy	Single or dual feeding, pluggable
	AC Source	100 to 240 VAC, 50/60 Hz, 1.5A maximum
	DC Source	-48 VDC, 3A maximum
	Power Consumption	75W 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	5.5 kg/12.1 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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-1000TN.

In this Chapter

Safety Precautions.....	25
Site Requirements	27
PL-1000TN Front Panel.....	28
Installing the PL-1000TN Unit.....	30

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-1000TN:

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

 **GROUNDING:** For your protection and to prevent possible damage to equipment when a fault condition occurs on the cables connected to the equipment (for example, a lightning stroke or contact with high voltage power lines), the case of the PL-1000TN 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-1000TN must be connected to a protective ground (see [Connection Data](#) (p. 251)).

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

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

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

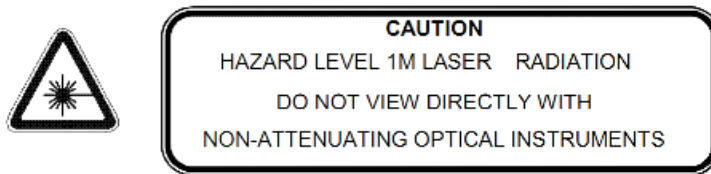


Figure 15: Class 1M Laser Warning

The following warning applies to Class 3B laser products.

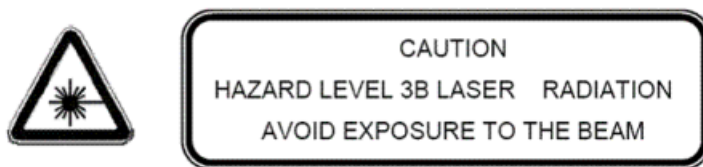


Figure 16: Class 3B Laser Warning

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

2.2.1 Physical Requirements

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

All the connections are made to the front panel.

2.2.2 Power Requirements


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

DC-powered PL-1000TN units require a -48 VDC, 3A maximum DC power source with the positive terminal grounded. In addition, the DC power connector contains the chassis (frame) ground terminal (see [Power Connectors](#) (p. 256)).

2.2.3 Ambient Requirements

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

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

2.2.4 Electromagnetic Compatibility Considerations

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

2.3 PL-1000TN Front Panel

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



Figure 17: PL-1000TN Front Panel

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

- 12 LINK (6 uplink/6 service) ports
- COM port labeled "COM"

- 2 MNG ports labeled "MNG1" and "MNG2"
 - Passive MUX/DEMUX port labeled "MUX" and "DEMUX"
- 2 ribbon cables are connected to the "MUX/DEMUX" interfaces. Each ribbon is composed of two parts:
- An MPO/APC female connector labeled "MUX/DEMUX" and is connected to the "MUX/DEMUX" port.
 - 2, 4, or 6 pairs (Tx and Rx) of LC connectors marked " $\lambda 1$ ", " $\lambda 2$ ", and so on, and "MNG". These LC connectors are connected to the WDM uplink ports and to one of the OSC ports.
- 10/100 Base-T LAN port labeled "ETH"
 - External alarm port labeled "ALARM"
 - CONTROL port: RS-232 connector
 - Power connections
 - FAN unit tray

2.3.1 Front Panel LEDs

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

For the list of LEDs and their functions, see [Technical Specifications](#) (p. 17).

2.3.2 PL-1000TN Optical Connections Example

The following figure illustrates the connections between the optical ports of the PL-1000TN.

In this example, the PL-1000TN is configured as follows:

- Six transponders
- One EDFA module

- One MUX/DEMUX module

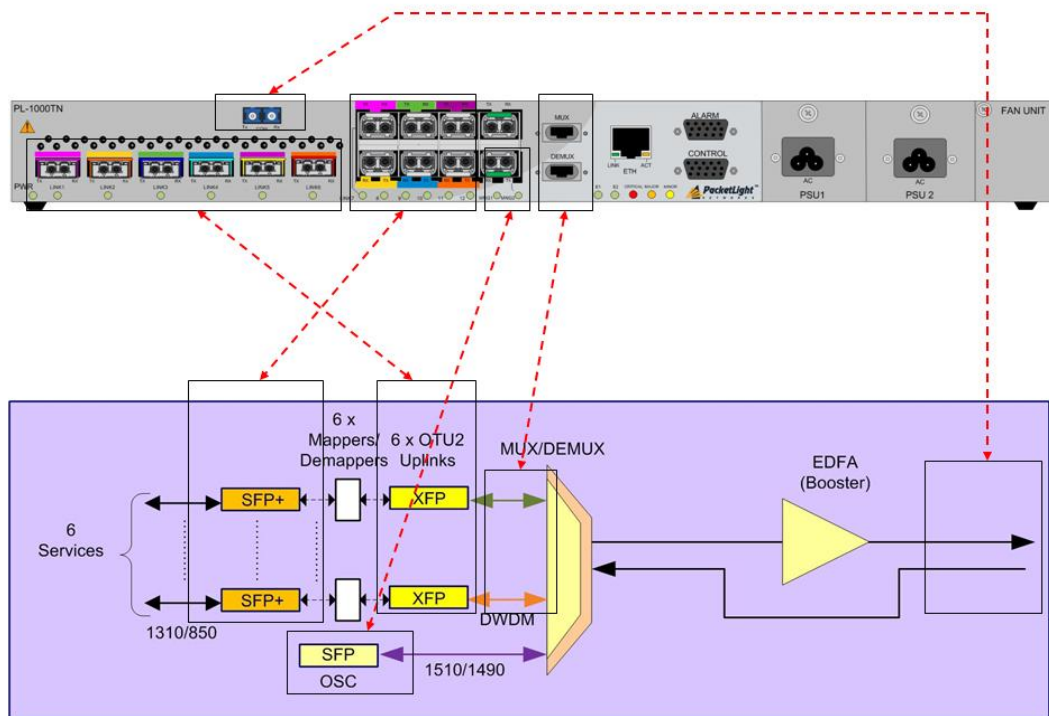


Figure 18: Connections between the Optical Ports (Example)

2.4 Installing the PL-1000TN Unit

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

CAUTION: Before installing a PL-1000TN unit, review the [Safety Precautions](#) (p. 25).

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-1000TN (for procedures for using the terminal, see [Operation and Preliminary Configuration](#) (p. 35)). The software necessary for using the terminal is stored in the PL-1000TN.

2.4.1 Package Contents

The PL-1000TN package includes the following items:

- PL-1000TN unit
- Ethernet cable
- Ribbon cable (if the PL-1000TN contains a MUX/DEMUX)
- 3m RS-232 terminal cable

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

2.4.2 Required Equipment

The cables needed to connect to the PL-1000TN depend on the PL-1000TN application. You can use standard cables or prepare the appropriate cables yourself (see [Connection Data](#) (p. 251)).

2.4.3 Cable Connections


Before starting, refer to the site installation plan and identify the cables intended for connection to this PL-1000TN unit (see [Site Requirements](#) (p. 27) and [Connection Data](#) (p. 251)).

2.4.3.1 Optical Cable Handling Precautions

The following are the optical cable handling 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-1000TN 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-1000TN 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 AC or DC power cable.
- The power cord plug should only be inserted in an outlet provided with a protective ground (earth) contact. The protective action must not be negated by using an extension cord (power cable) without a protective conductor (grounding).

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

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

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

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

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

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

2.4.3.3 Cabling the LINK Ports

Each LINK port has two connectors marked "Tx" and "Rx".

2.4.3.3.1 Cabling the Uplink Ports

To cable the uplink ports:

1. Remove the protective plug from the desired uplink port and insert an XFP transceiver.
2. Connect the port to the appropriate remote equipment or to the MUX/DEMUX interface as follows:
 - Tx connector (transmit fiber) to receive input of the remote equipment and Rx connector (receive fiber) to transmit output of the remote equipment.

or

- Plug the suitable LC connector from the ribbon cable (which is attached to the MUX and DEMUX ports) into the uplink port. Use the Web application to determine which LC connector to use. The Web application maps the LC connectors of the ribbon cable to the uplink XFP, according to the unique wavelength of the XFP and the name tags on the LC connectors.

Always leave enough slack to prevent strain.

2.4.3.3.2 Cabling the Service Ports

To cable the service ports:

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

Always leave enough slack to prevent strain.

2.4.3.4 Cabling the MUX/DEMUX Port

The following is applicable only to a PL-1000TN with a MUX/DEMUX module installed.

To connect cables to the PL-1000TN MUX/DEMUX port:

1. Remove the protective plug from the MUX/DEMUX port.
2. Connect the supplied ribbon cable to the MUX/DEMUX port.
3. Connect the LC connectors of the ribbon to the appropriate uplink ports of the PL-1000TN.
4. Connect the MNG LC connector of the ribbon to one of the MNG ports of the PL-1000TN.

2.4.3.5 Cabling the Management Ports

You can cable the following management ports:

- MNG port
- CONTROL port
- ETH port

2.4.3.5.1 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 MUX/DEMUX using the LC connector marked "MNG" over the ribbon cable.

2.4.3.5.2 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-1000TN connectors, see [Connection Data](#) (p. 251).

2.4.3.5.3 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-1000TN connectors, see [Connection Data](#) (p. 251).

3 Operation and Preliminary Configuration

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

In this Chapter

Operating Instructions.....	35
Performing Preliminary Configuration	36
Accessing the Web Application	37

3.1 Operating Instructions

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

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-1000TN 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-1000TN preliminary configuration (the exact pinout of the connector is described in [Connection Data](#) (p. 251)).

2. Check that the installation and the required cable connections have been correctly performed (see [Installing the PL-1000TN Unit](#) (p. 30)).
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-1000TN

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

To turn on the PL-1000TN:

1. Connect the PL-1000TN to the power source (see [Connecting the PL-1000TN to Ground and Power](#) (p. 31)).

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-1000TN 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. 251)).

For more information about the CLI commands, see [CLI](#) (p. 235).

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-1000TN 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. 244)).

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-1000TN>> configure interface ethernet ip 192.168.0.100 -n 255.255.255.0
```

Table 4: 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	<ul style="list-style-type: none"> • Dot notation For example: 255.255.255.0 • Hexadecimal notation For example: ffffffff00 • 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-1000TN before accessing the Web (see [Performing Preliminary Configuration](#) (p. 36)).

3.3.2 Prerequisites for Accessing the Web Application

The following are the prerequisites for accessing the Web application:

- The PL-1000TN is properly installed.
- The PL-1000TN 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. 244)).
2. Open the Web browser.
3. In the address field of the browser, type the **IP address** of the PL-1000TN 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-1000TN)

4. Press **Enter**.

The Login window opens.



Figure 19: 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.

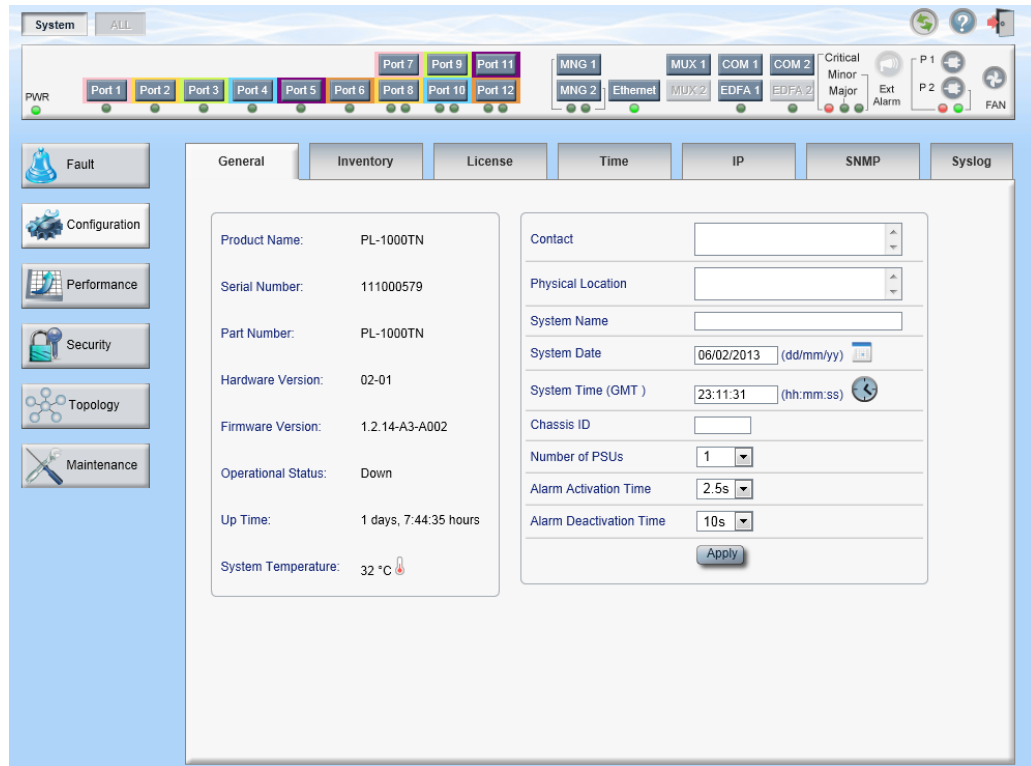


Figure 20: System Configuration Window

3.3.4 Navigating the Web Application

This section describes the PL-1000TN 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.

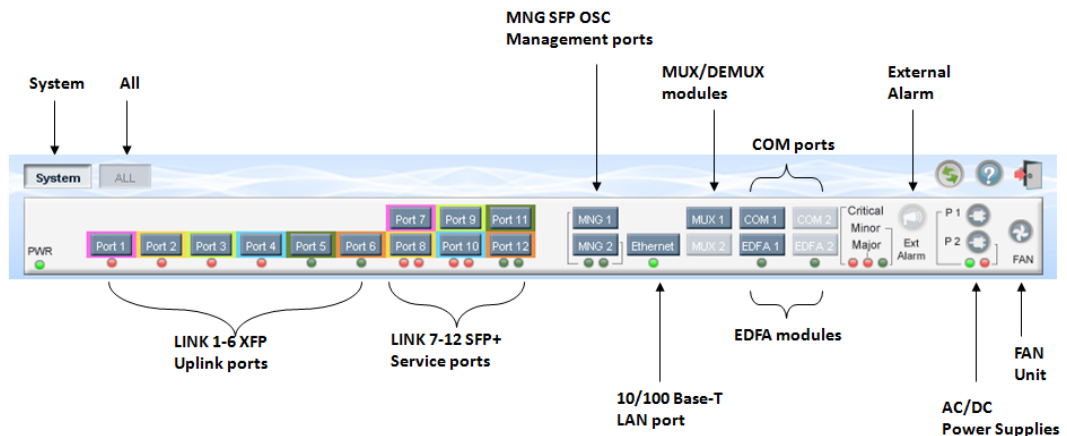



Figure 21: PL-1000TN Item Buttons

The buttons displayed vary according to the configuration. For example, if the PL-1000TN 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 22: PL-1000TN Sidebar Buttons

Use the sidebar buttons to do the following:

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

3.3.4.3 PL-1000TN Tabs

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

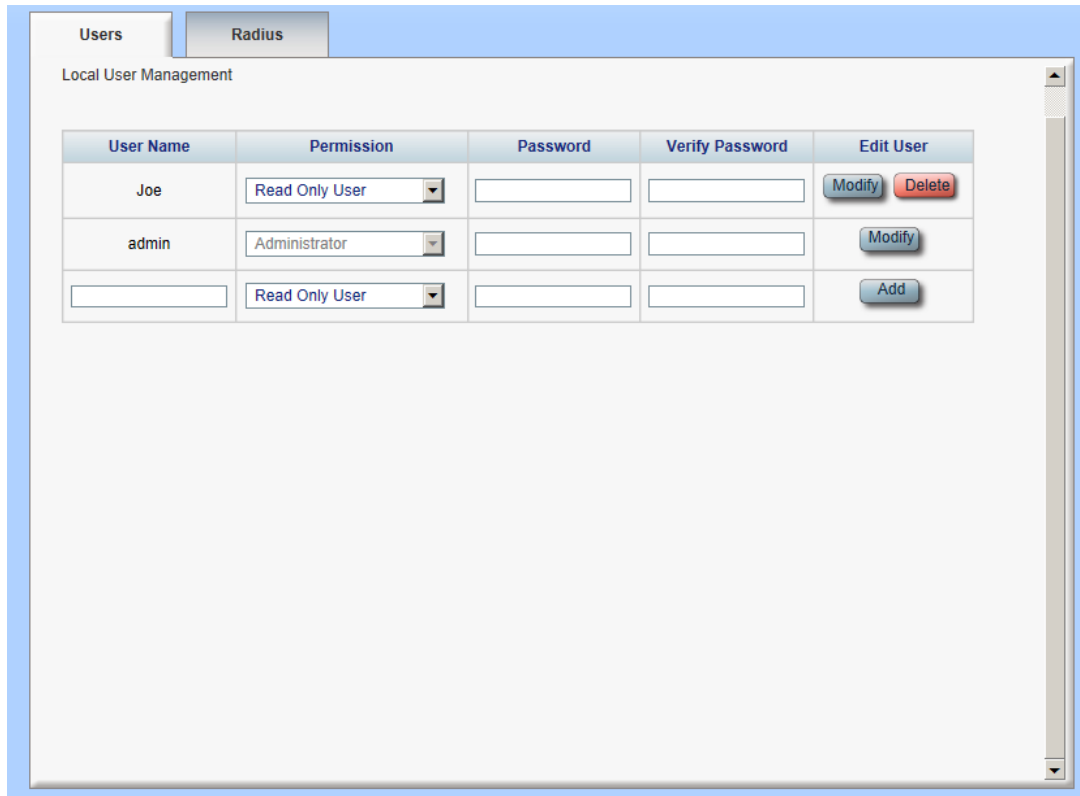


Figure 23: PL-1000TN Tabs (Example)

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.

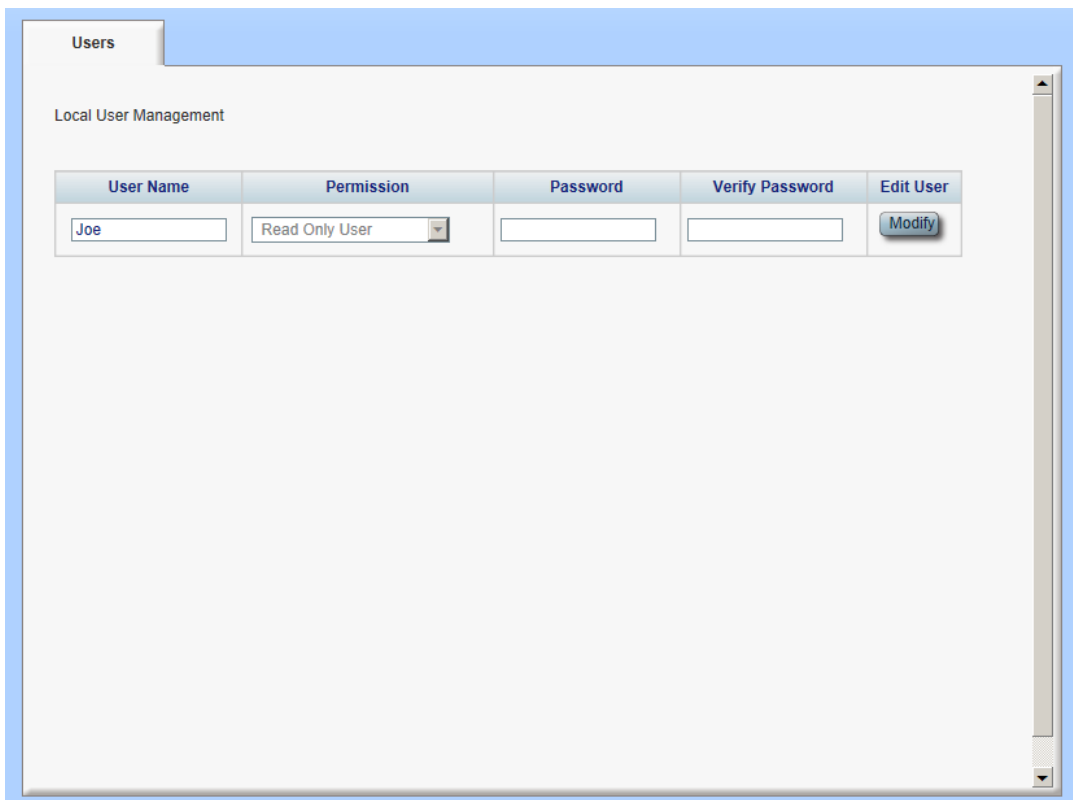


Figure 24: PL-1000TN Users Tab

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

User Access Levels.....	43
User Authentication Methods.....	43
Security Settings.....	46

4.1 User Access Levels

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

Table 5: 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.	<ul style="list-style-type: none"> • User name: admin • Password: admin (default) <p>NOTE: You can change the password. However, the user name cannot be changed and is set to "admin" by default.</p>
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. 50)).	
Read Only User	View only; no edit permissions except to change their own password (see Changing Your Password (p. 50)).	

4.2 User Authentication Methods

The access to the PL-1000TN 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-1000TN 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 administrator 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 6: Attributes Used

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

Attribute	AVP Type	Access-Request	Access-Accept	Format/Values
Class	25	-	√	The access level granted to the user as carried by the Radius Access-Accept. Format: String Allowed values: <ul style="list-style-type: none"> • 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-1000TN 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. 44).

4.3 Security Settings

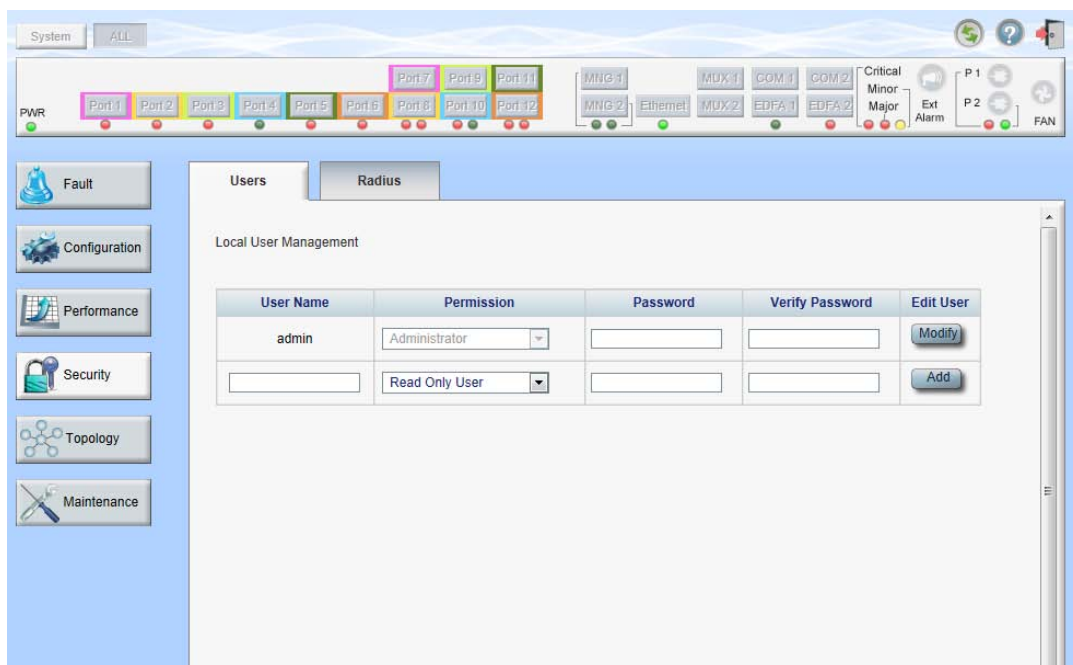


Figure 25: Security Settings Window

Use the Security Settings window to do the following:

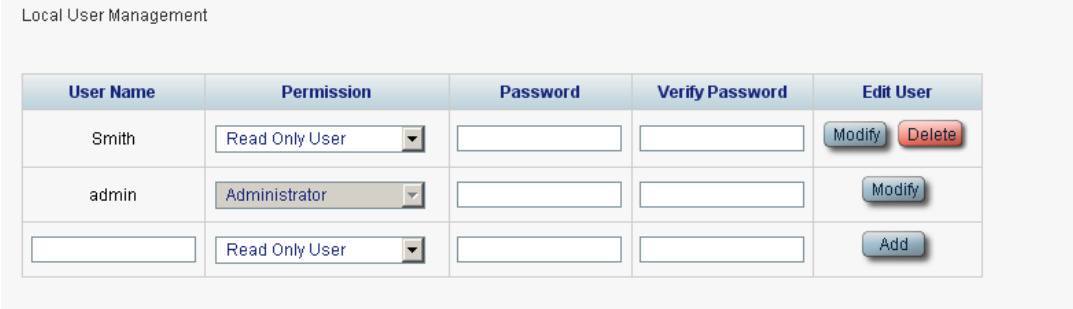
- **Users tab (Administrator):** Add a new user, change a user password, change a user permission level, and delete a user
- **Users tab (Non-Administrator):** Change your password
- **Radius tab (Administrator):** Configure the Radius client

To open the Security Settings window:

- Click **Security**.

The Security Settings window opens.

4.3.1 Users Tab (Administrator)



User Name	Permission	Password	Verify Password	Edit User
Smith	Read Only User	<input type="text"/>	<input type="text"/>	Modify Delete
admin	Administrator	<input type="text"/>	<input type="text"/>	Modify
<input type="text"/>	Read Only User	<input type="text"/>	<input type="text"/>	Add

Figure 26: 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 7: 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. 43))
Password	The password for the user.	Only alphanumeric characters without spaces are allowed. NOTE: The password is hidden for security reasons.

Parameter	Description	Format/Values
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. 43)).
4. Click **Modify**.

The following confirmation message appears.

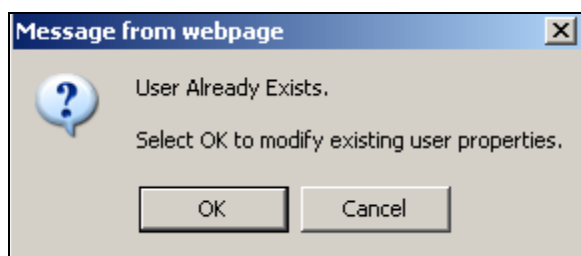


Figure 27: Confirm Changes

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.

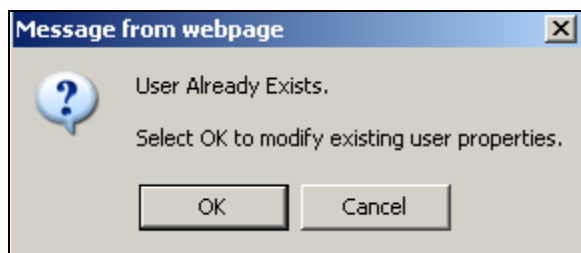


Figure 28: Confirm Changes

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.

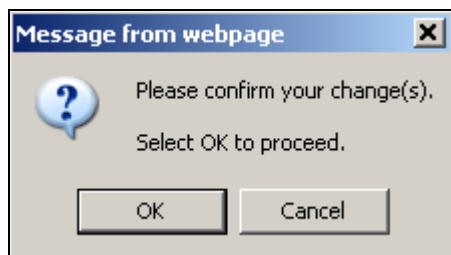
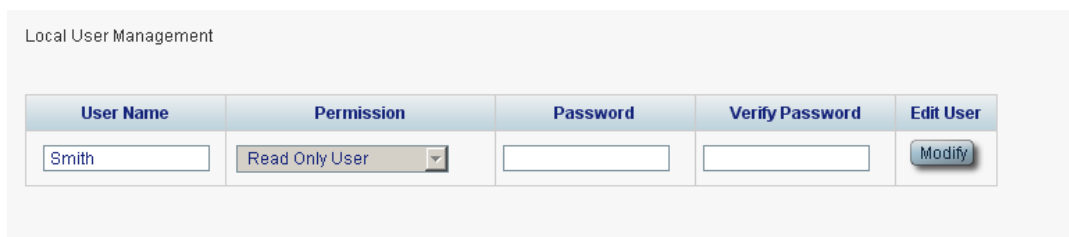


Figure 29: Confirm Delete

4. Click **OK**.

The specified user is deleted.

4.3.2 Users Tab (Non-Administrator)



Local User Management

User Name	Permission	Password	Verify Password	Edit User
Smith	Read Only User			Modify

Figure 30: 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.

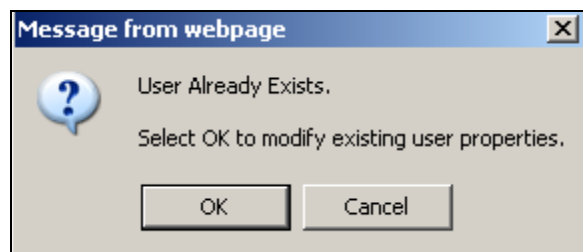


Figure 31: Confirm Changes

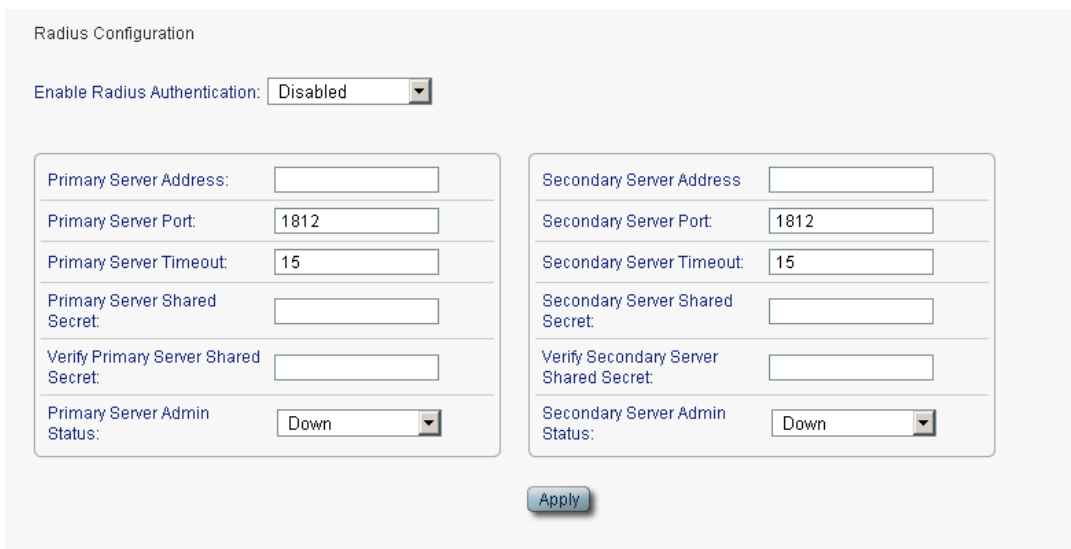
5. Click **OK**.

Your password is changed.

Table 8: 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)



Radius Configuration

Enable Radius Authentication:

Primary Server Address:	<input type="text"/>	Secondary Server Address	<input type="text"/>
Primary Server Port:	<input type="text" value="1812"/>	Secondary Server Port:	<input type="text" value="1812"/>
Primary Server Timeout:	<input type="text" value="15"/>	Secondary Server Timeout:	<input type="text" value="15"/>
Primary Server Shared Secret:	<input type="text"/>	Secondary Server Shared Secret:	<input type="text"/>
Verify Primary Server Shared Secret:	<input type="text"/>	Verify Secondary Server Shared Secret:	<input type="text"/>
Primary Server Admin Status:	<input type="text" value="Down"/>	Secondary Server Admin Status:	<input type="text" value="Down"/>

Figure 32: 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.

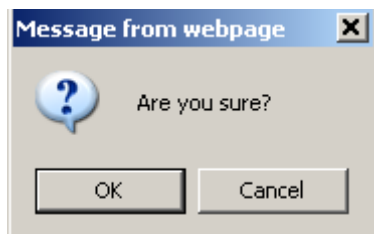


Figure 33: Confirm Configuration

4. Click **OK**.

The Radius client is configured.

Table 9: 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-1000TN fault management, which is used to localize and identify problems in the network incorporating PL-1000TN units.

In this Chapter

Fault Views	55
General Fault Procedure	57
System Faults	58
All Faults	64
Uplink Port Faults	70
Service Port Faults.....	76
Management Port Faults.....	82
Ethernet Port Faults	88
EDFA Faults	94
COM Port Faults.....	100
PSU Faults	106

5.1 Fault Views

This section describes the following Fault views:

- Alarms
- Events
- Configuration Changes

5.1.1 Alarms

The PL-1000TN 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-1000TN continuously monitors the traffic signals and other exceptional conditions. Whenever such a condition occurs, the PL-1000TN generates a time stamped event message and sends it as an SNMP notification to the registered management systems. The PL-1000TN 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-1000TN system log files, which can be exported to a text file for offline viewing.

The PL-1000TN 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.
- **Protection Switching Event:** These events are generated when protection switching occurs.
- **Inventory Change:** These events are generated when the node inventory is changed.
- **Unsolicited Event:** These events are generated when an exceptional event occurs.
- **Configuration Change:** These events are generated when the node configuration is changed.

5.1.3 Configuration Changes

The PL-1000TN 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-1000TN faults. The specific procedures for each item are provided in the following sections.

To view the PL-1000TN 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. 58))
 - **All** (see [All Faults](#) (p. 64))
 - **Port (1 - 6)** (see [Uplink Port Faults](#) (p. 70))
 - **Port (7 – 12)** (see [Service Port Faults](#) (p. 76))
 - **MNG** (see [Management Port Faults](#) (p. 82))
 - **EDFA** (if present) (see [EDFA Faults](#) (p. 94))
 - **COM** (if present) (see [COM Port Faults](#) (p. 100))
 - **PSU** (see [PSU Faults](#) (p. 106))

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

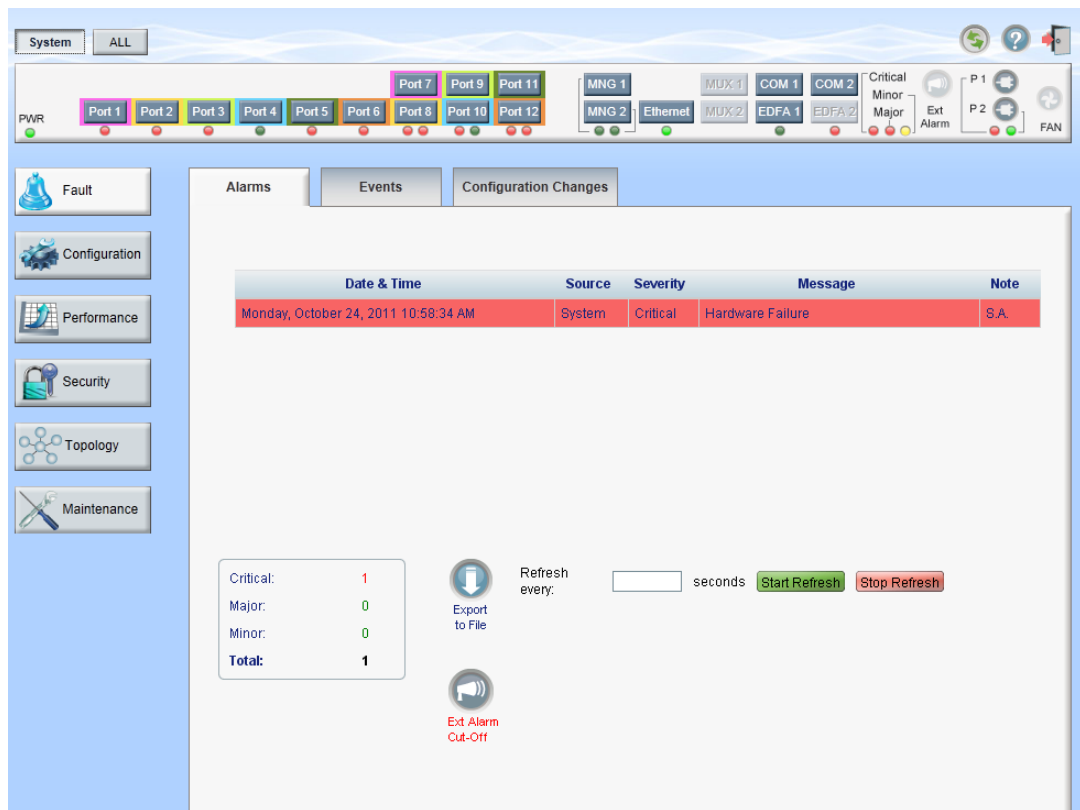


Figure 34: System Fault Window

Use the System Fault window to do the following:

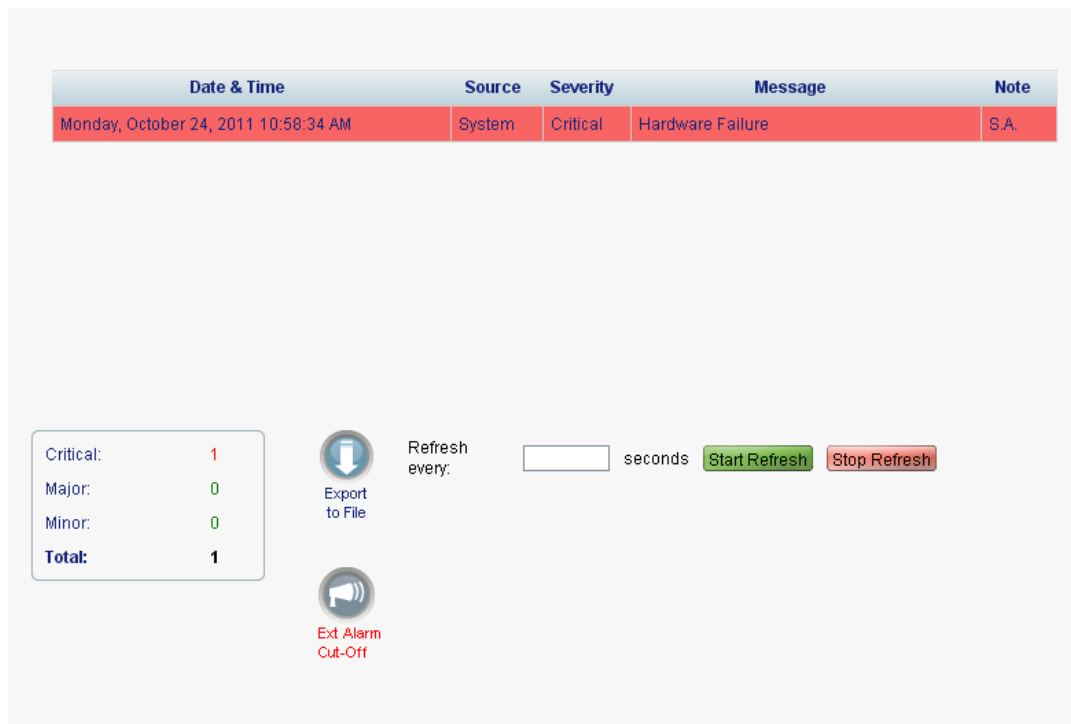
- **Alarms tab:** View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab:** View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh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



Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 10:58:34 AM	System	Critical	Hardware Failure	S.A.

Critical:	1
Major:	0
Minor:	0
Total:	1

Refresh every: seconds Start Refresh Stop Refresh

 Export to File


 Ext Alarm Cut-Off

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. 17).

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 10: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.3.2 Events Tab

Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 10:58:26 AM	System	Event	System Cold Start	
Monday, October 24, 2011 10:58:34 AM	System	Critical	Hardware Failure	S.A.

Critical:	1
Major:	0
Minor:	0
Cleared:	0
Events:	1
Total:	2


Export to File

Refresh every:

seconds
Start Refresh Stop Refresh

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.

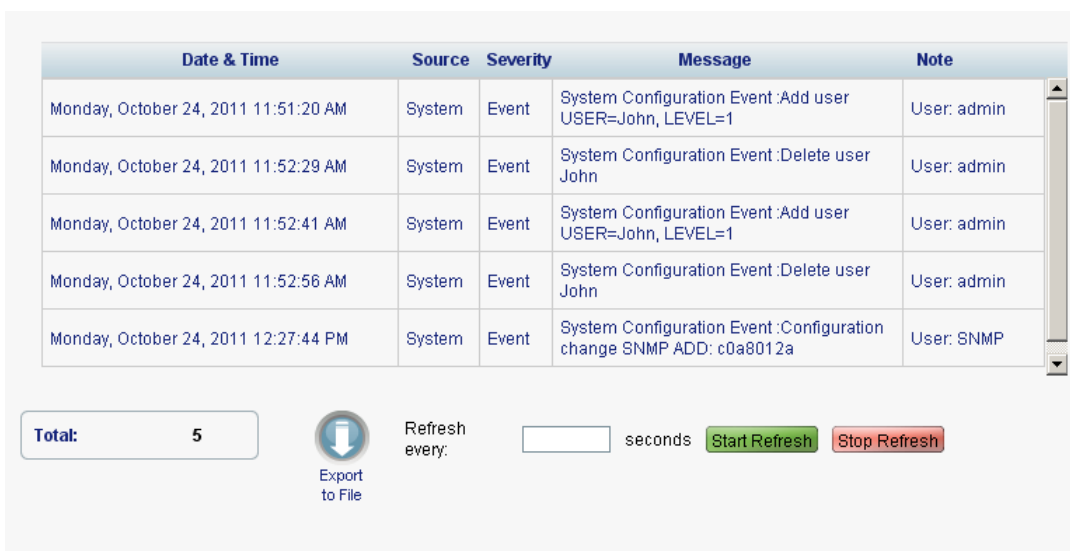
5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

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

Table 11: 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.	<ul style="list-style-type: none"> • 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



Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 11:51:20 AM	System	Event	System Configuration Event :Add user USER=John, LEVEL=1	User: admin
Monday, October 24, 2011 11:52:29 AM	System	Event	System Configuration Event :Delete user John	User: admin
Monday, October 24, 2011 11:52:41 AM	System	Event	System Configuration Event :Add user USER=John, LEVEL=1	User: admin
Monday, October 24, 2011 11:52:56 AM	System	Event	System Configuration Event :Delete user John	User: admin
Monday, October 24, 2011 12:27:44 PM	System	Event	System Configuration Event :Configuration change SNMP ADD: c0a8012a	User: SNMP


Total: 5
 
 Refresh every: seconds
 Start Refresh
Stop Refresh

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**.

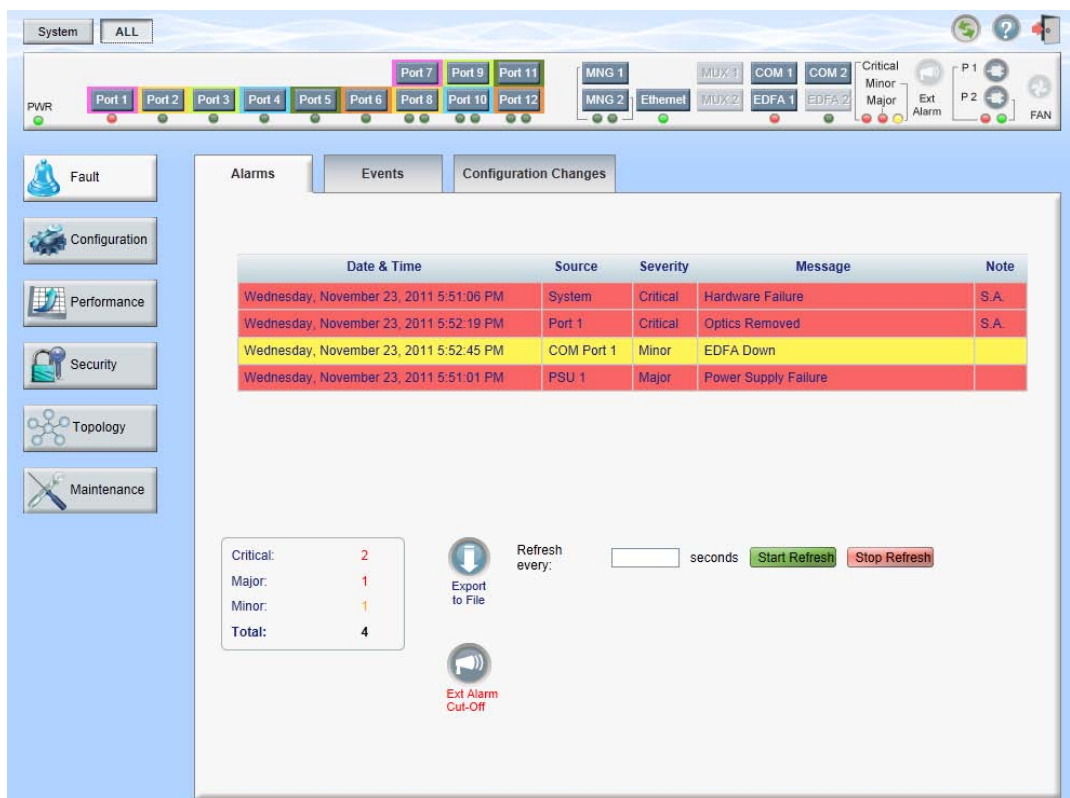
The automatic refresh is stopped and the **Refresh every** field is cleared.

Table 12: 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.	

A

5.4 All Faults



Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:51:06 PM	System	Critical	Hardware Failure	S.A.
Wednesday, November 23, 2011 5:52:19 PM	Port 1	Critical	Optics Removed	S.A.
Wednesday, November 23, 2011 5:52:45 PM	COM Port 1	Minor	EDFA Down	
Wednesday, November 23, 2011 5:51:01 PM	PSU 1	Major	Power Supply Failure	

Critical: 2
 Major: 1
 Minor: 1
 Total: 4

Refresh every: seconds Start Refresh Stop Refresh
 Export to File
 Ext Alarm Cut-Off

Figure 38: 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

Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:51:06 PM	System	Critical	Hardware Failure	S.A.
Wednesday, November 23, 2011 5:52:19 PM	Port 1	Critical	Optics Removed	S.A.
Wednesday, November 23, 2011 5:52:45 PM	COM Port 1	Minor	EDFA Down	
Wednesday, November 23, 2011 5:51:01 PM	PSU 1	Major	Power Supply Failure	

Critical:	2
Major:	1
Minor:	1
Total:	4


Export to File


Ext Alarm Cut-Off

Refresh every: seconds

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. 17).

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 13: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.4.2 Events Tab



Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:52:17 PM	Port 1	Cleared	Optics Removed	
Wednesday, November 23, 2011 5:52:19 PM	Port 1	Critical	Optics Removed	S.A.
Wednesday, November 23, 2011 5:52:45 PM	COM Port 1	Minor	EDFA Down	
Wednesday, November 23, 2011 5:52:55 PM	COM Port 2	Event	APS Switch Over	to Protecting
Wednesday, November 23, 2011 5:52:59 PM	COM Port 2	Event	APS Switch Over	to Working

Critical:	3
Major:	1
Minor:	1
Cleared:	1
Events:	4
Total:	10


 Refresh every: seconds Start Refresh Stop Refresh

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.

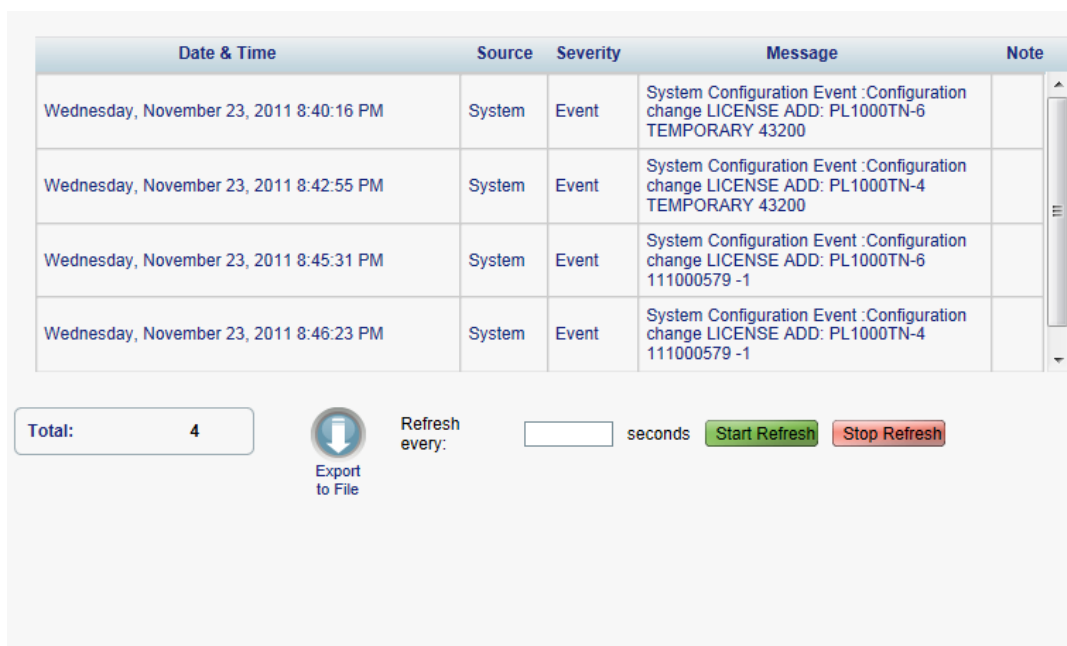
5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

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

Table 14: 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.	<ul style="list-style-type: none"> • 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



Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 8:40:16 PM	System	Event	System Configuration Event : Configuration change LICENSE ADD: PL1000TN-6 TEMPORARY 43200	
Wednesday, November 23, 2011 8:42:55 PM	System	Event	System Configuration Event : Configuration change LICENSE ADD: PL1000TN-4 TEMPORARY 43200	
Wednesday, November 23, 2011 8:45:31 PM	System	Event	System Configuration Event : Configuration change LICENSE ADD: PL1000TN-6 111000579 -1	
Wednesday, November 23, 2011 8:46:23 PM	System	Event	System Configuration Event : Configuration change LICENSE ADD: PL1000TN-4 111000579 -1	

Total: 4

 Export to File

Refresh every: seconds

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 15: 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.	

A

5.5 Uplink Port Faults

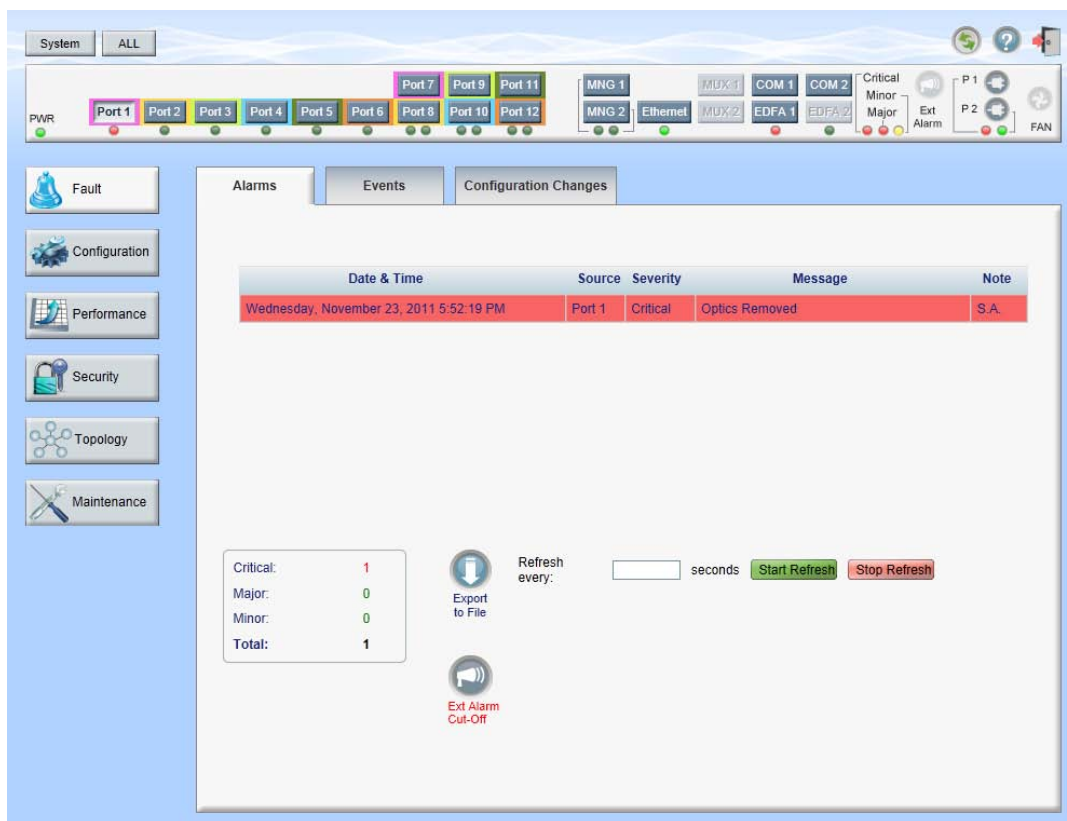


Figure 42: Uplink Port Fault Window

Use the Uplink Port Fault window to do the following:

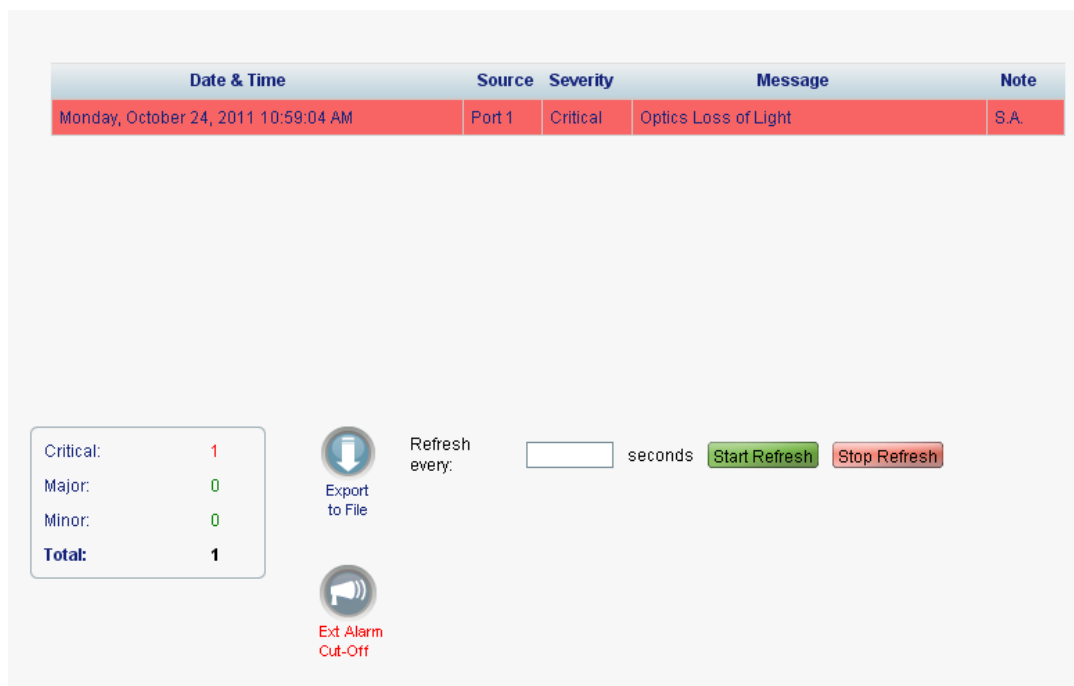
- **Alarms tab:** View the current alarms, turn off the external alarm, export the list of alarms to a file, set the refresh rate, and stop the automatic refresh of the Fault display
- **Event Log tab:** View the Event Log, export the log to a file, set the refresh rate, and stop the automatic refresh 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 a **Port** button (Port 1-6) to select the uplink port.

The appropriate Uplink Port Fault window opens.

5.5.1 Alarms Tab



Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 10:59:04 AM	Port 1	Critical	Optics Loss of Light	S.A.

Critical: 1
 Major: 0
 Minor: 0
Total: 1

Refresh every: seconds Start Refresh Stop Refresh

Export to File
Ext Alarm Cut-Off

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. 17).

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 16: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.5.2 Events Tab

Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 10:58:27 AM	Port 1	Event	Link Up	
Monday, October 24, 2011 10:58:47 AM	Port 1	Event	Link Down	
Monday, October 24, 2011 10:58:48 AM	Port 1	Critical	SONET/SDH LOF (Loss of Frame)	S.A.
Monday, October 24, 2011 10:59:04 AM	Port 1	Critical	Optics Loss of Light	S.A.
Monday, October 24, 2011 10:59:05 AM	Port 1	Cleared	SONET/SDH LOF (Loss of Frame)	

Critical:	2
Major:	0
Minor:	0
Cleared:	1
Events:	2
Total:	5


Export to File

Refresh every:

seconds
Start Refresh Stop Refresh

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:

- In the **Refresh every** field, type the number of seconds that the window should refresh.
The minimum refresh rate is 2 seconds.
- Click **Start Refresh**.
The information is automatically updated after the specified number of seconds.


- To refresh the Fault display manually, click **Refresh** .
The information is updated immediately.
- 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: 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.	<ul style="list-style-type: none"> • 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



Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:52:14 PM	Port 1	Event	System Configuration Event :Admin Up	User: admin
Wednesday, November 23, 2011 5:52:17 PM	Port 1	Event	System Configuration Event :Admin Down	User: admin
Wednesday, November 23, 2011 5:52:19 PM	Port 1	Event	System Configuration Event :Admin Up	User: admin

Total: 3

Refresh every: seconds

Start Refresh Stop Refresh

Export to File

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 18: 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.	

A

5.6 Service Port Faults

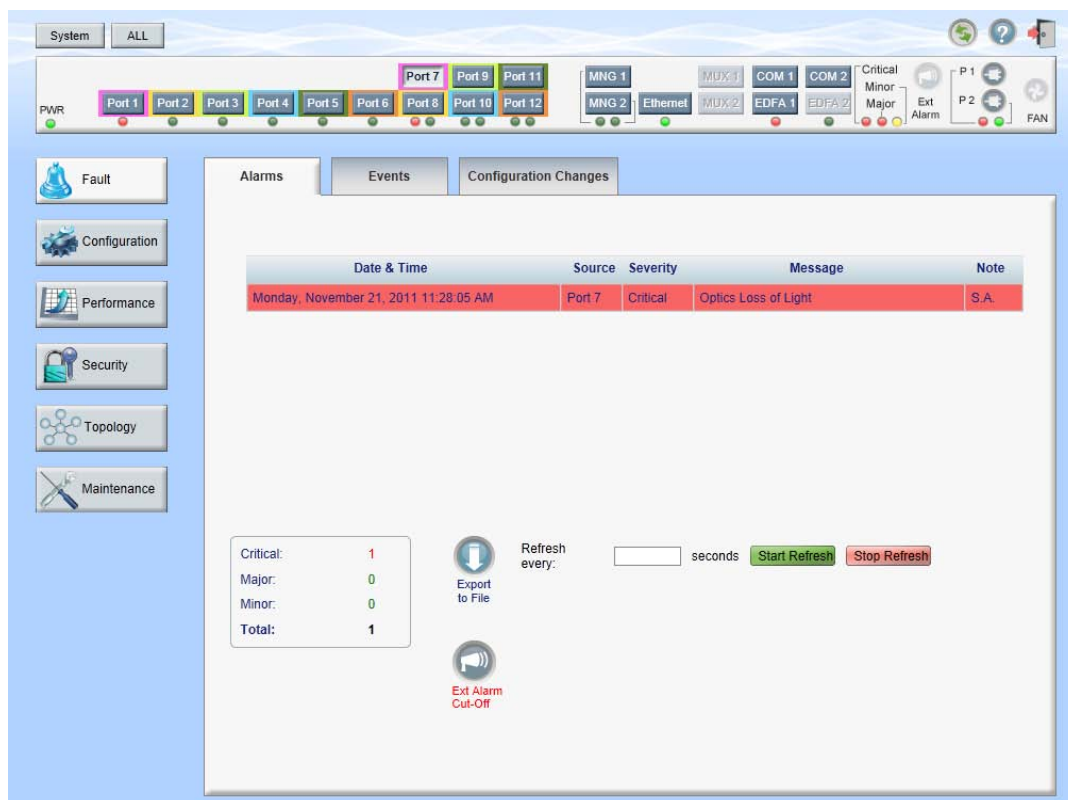


Figure 46: Service Port Fault Window

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 a **Port** button (Port 7-12) to select the service port.

The appropriate Service Port Fault window opens.

5.6.1 Alarms Tab

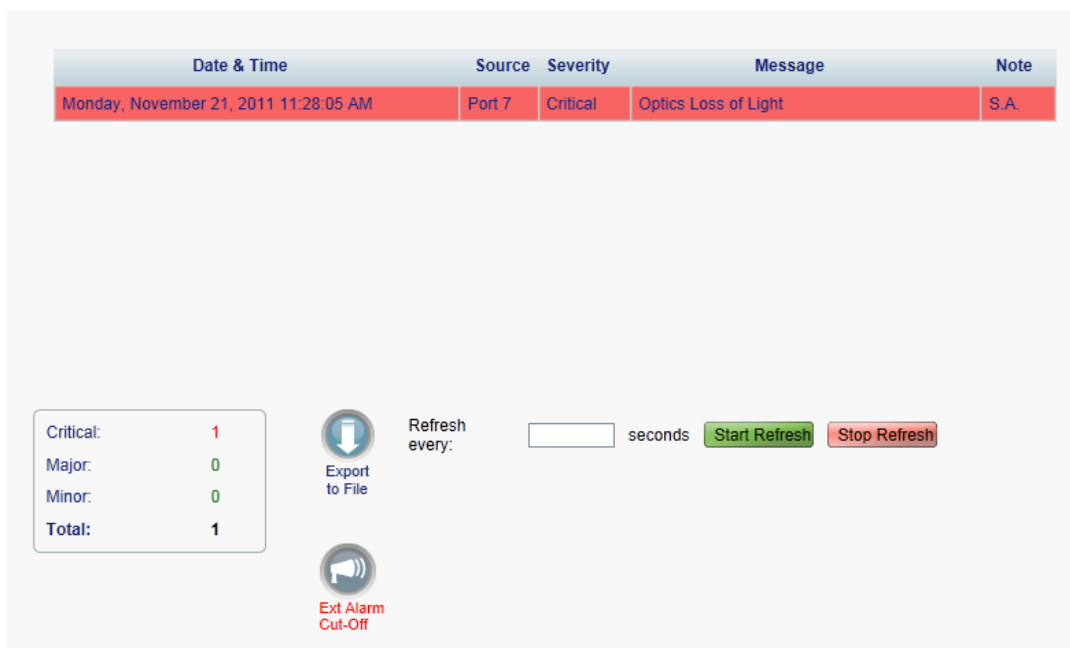


Figure 47: Alarms Tab

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. 17).

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** .

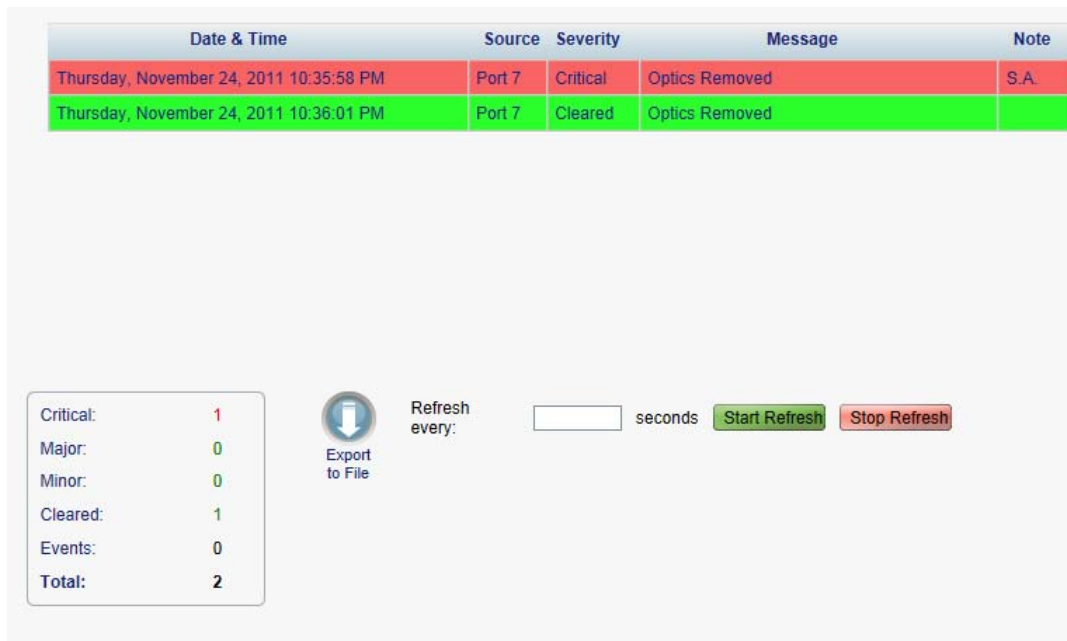
The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

NOTE: This action does not clear any alarms.

Table 19: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.6.2 Events Tab



Date & Time	Source	Severity	Message	Note
Thursday, November 24, 2011 10:35:58 PM	Port 7	Critical	Optics Removed	S.A.
Thursday, November 24, 2011 10:36:01 PM	Port 7	Cleared	Optics Removed	

Critical:	1
Major:	0
Minor:	0
Cleared:	1
Events:	0
Total:	2

 Export to File
 Refresh every: seconds


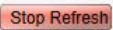



Figure 48: Events Tab

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.

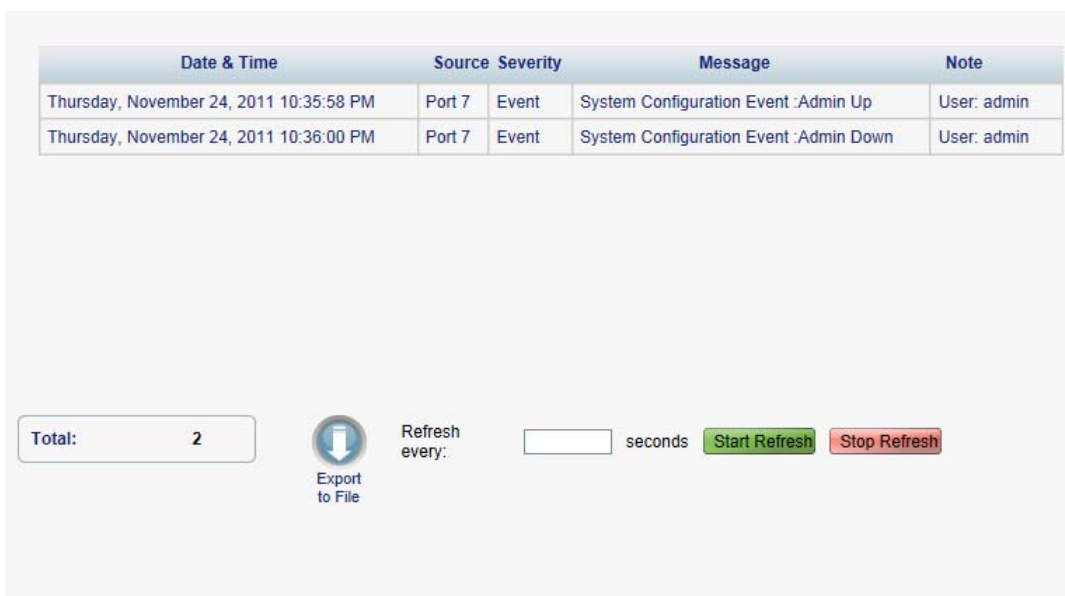
5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

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

Table 20: 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.	<ul style="list-style-type: none"> • 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



Date & Time	Source	Severity	Message	Note
Thursday, November 24, 2011 10:35:58 PM	Port 7	Event	System Configuration Event :Admin Up	User: admin
Thursday, November 24, 2011 10:36:00 PM	Port 7	Event	System Configuration Event :Admin Down	User: admin

Total: 2

Refresh every: seconds Start Refresh Stop Refresh


 Export to File

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 21: 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.	

A

5.7 Management Port Faults

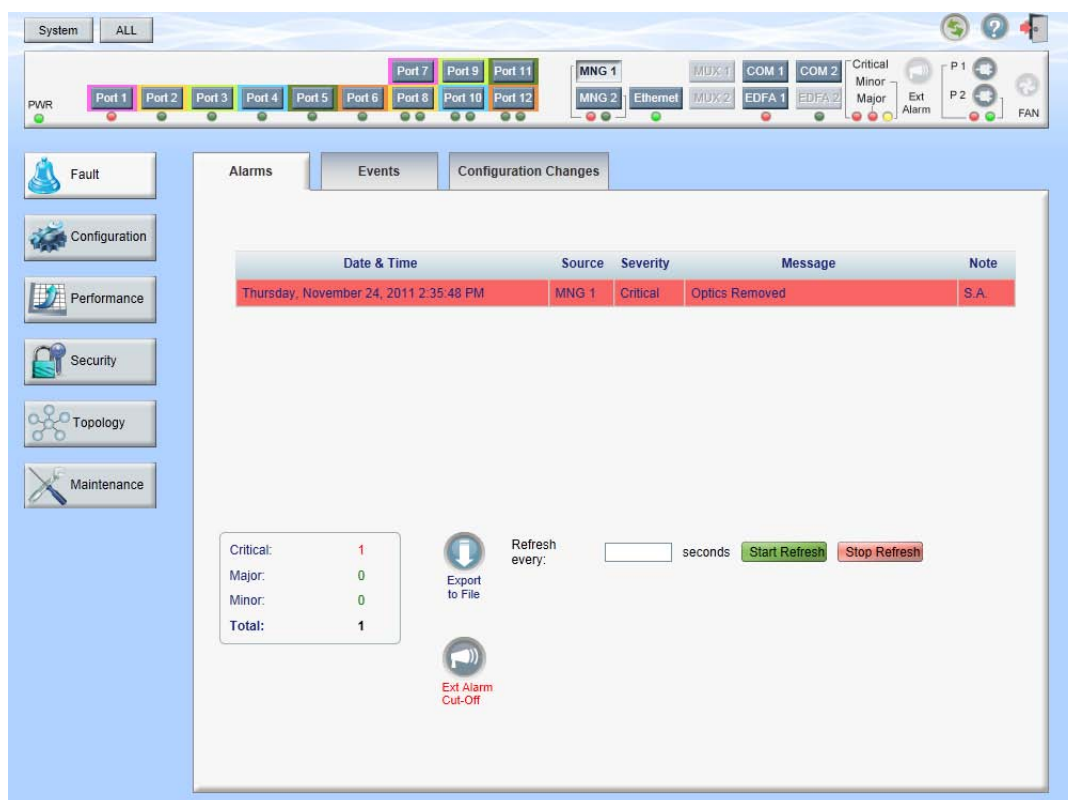


Figure 50: Management Port Fault Window

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

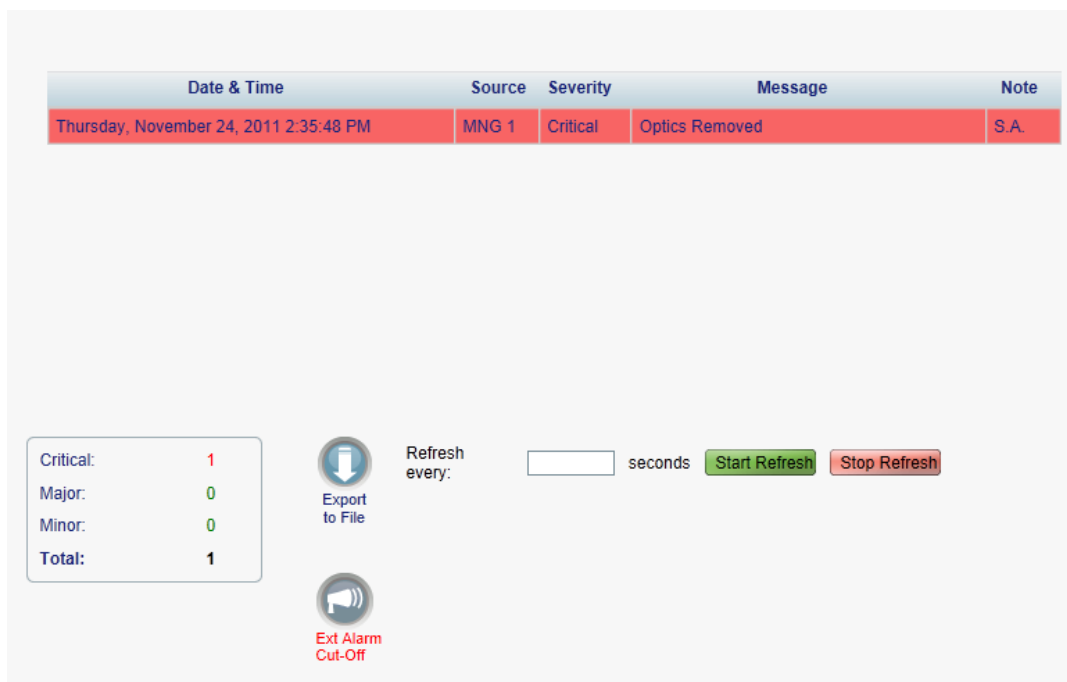


Figure 51: Alarms Tab

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. 17).

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 22: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.7.2 Events Tab

Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 12:31:32 PM	MNG 2	Critical	Optics Loss of Light	S.A.
Monday, October 24, 2011 2:00:26 PM	MNG 2	Event	Link Up	
Monday, October 24, 2011 2:00:26 PM	MNG 2	Cleared	Optics Loss of Light	

Critical:	1
Major:	0
Minor:	0
Cleared:	1
Events:	1
Total:	3


Export to File

Refresh every:

seconds

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 23: 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.	<ul style="list-style-type: none"> • 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

Date & Time	Source	Severity	Message	Note
Thursday, November 24, 2011 2:33:33 PM	MNG 1	Event	System Configuration Event :Admin Up	User: admin
Thursday, November 24, 2011 2:33:36 PM	MNG 1	Event	System Configuration Event :Admin Down	User: admin
Thursday, November 24, 2011 2:35:47 PM	MNG 1	Event	System Configuration Event :Admin Up	User: admin

Total: 3


 Export to File

Refresh every: seconds

Start Refresh
Stop Refresh

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 24: 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

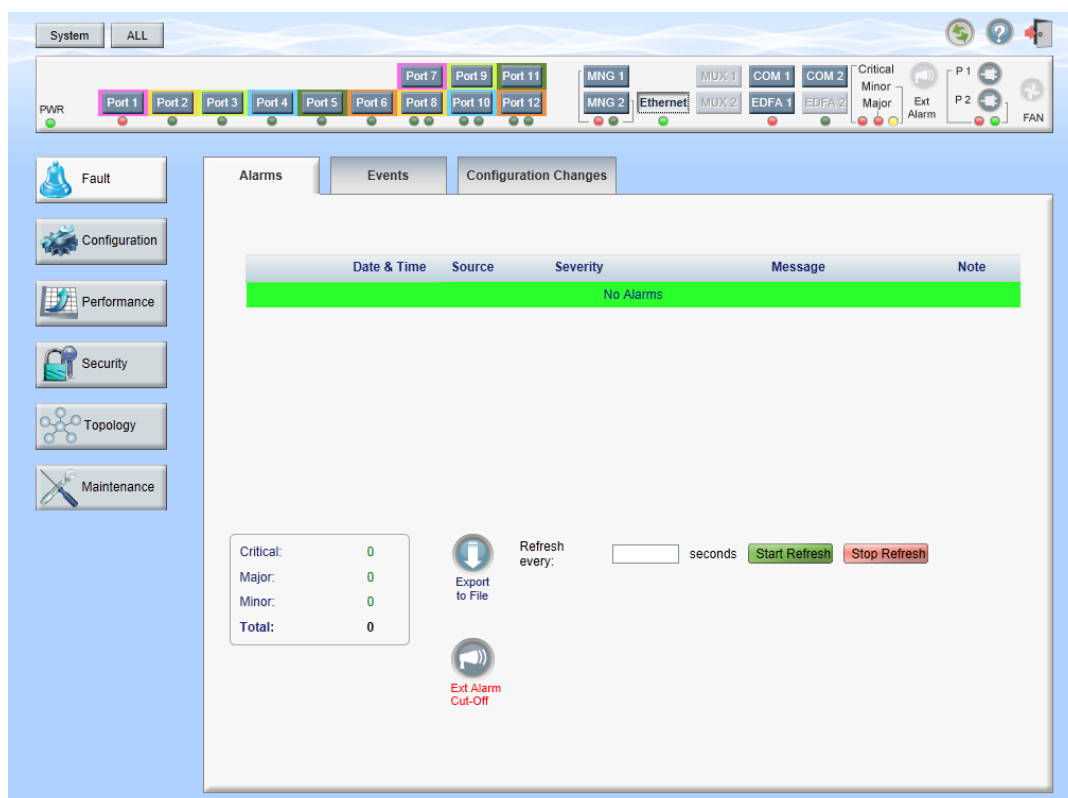


Figure 54: Ethernet Port Fault Window

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

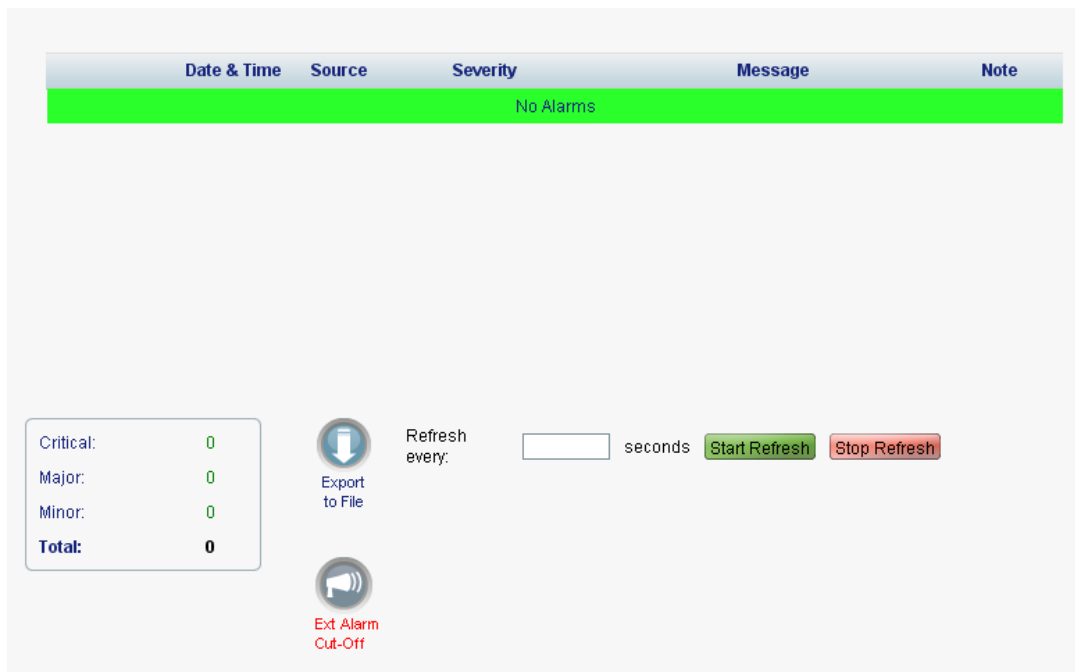


Figure 55: Alarms Tab

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. 17).

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**  .

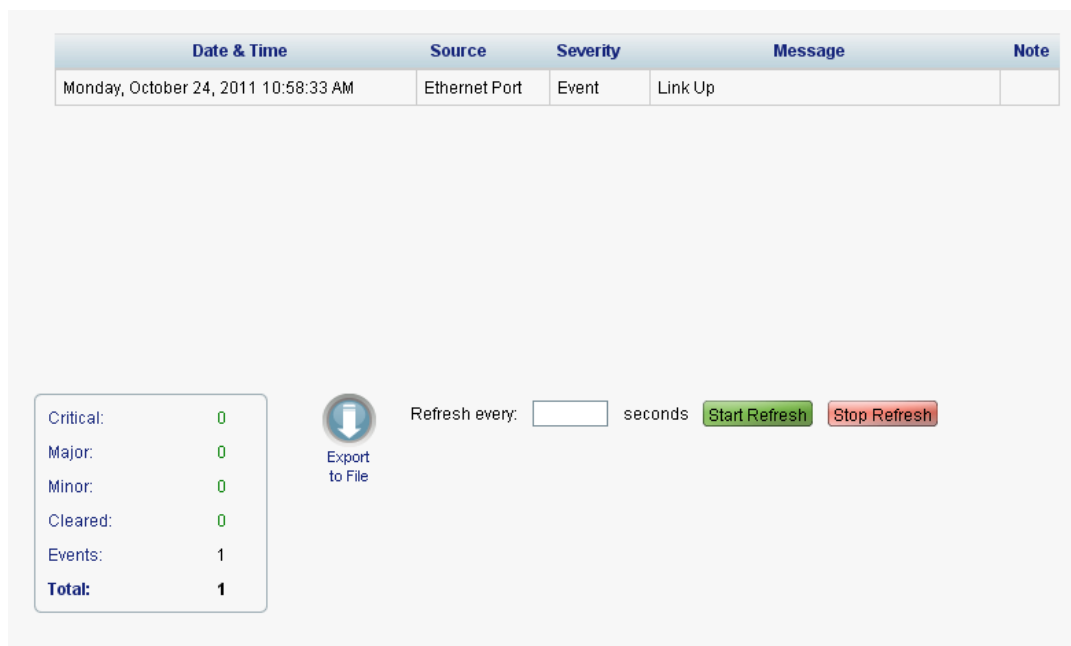
The external alarm caused by the current faults turns off; new faults will activate the external alarm again.

NOTE: This action does not clear any alarms.

Table 25: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.8.2 Events Tab



Date & Time	Source	Severity	Message	Note
Monday, October 24, 2011 10:58:33 AM	Ethernet Port	Event	Link Up	

Critical:	0
Major:	0
Minor:	0
Cleared:	0
Events:	1
Total:	1

Refresh every: seconds Start Refresh Stop Refresh


 Export to File

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 26: 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.	<ul style="list-style-type: none"> • 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

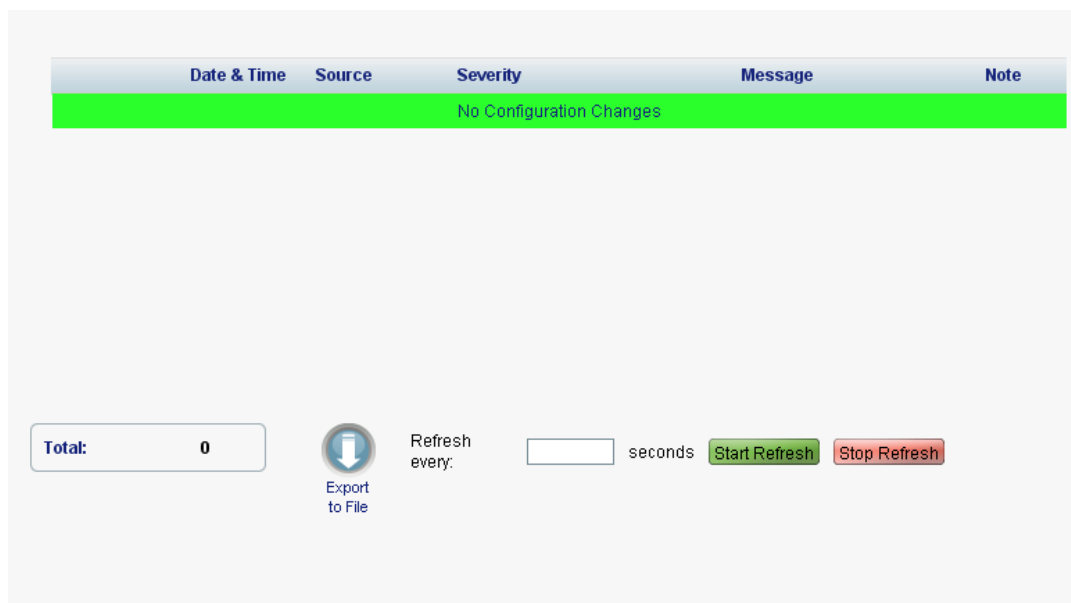


Figure 57: Configuration Changes Tab

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 27: 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

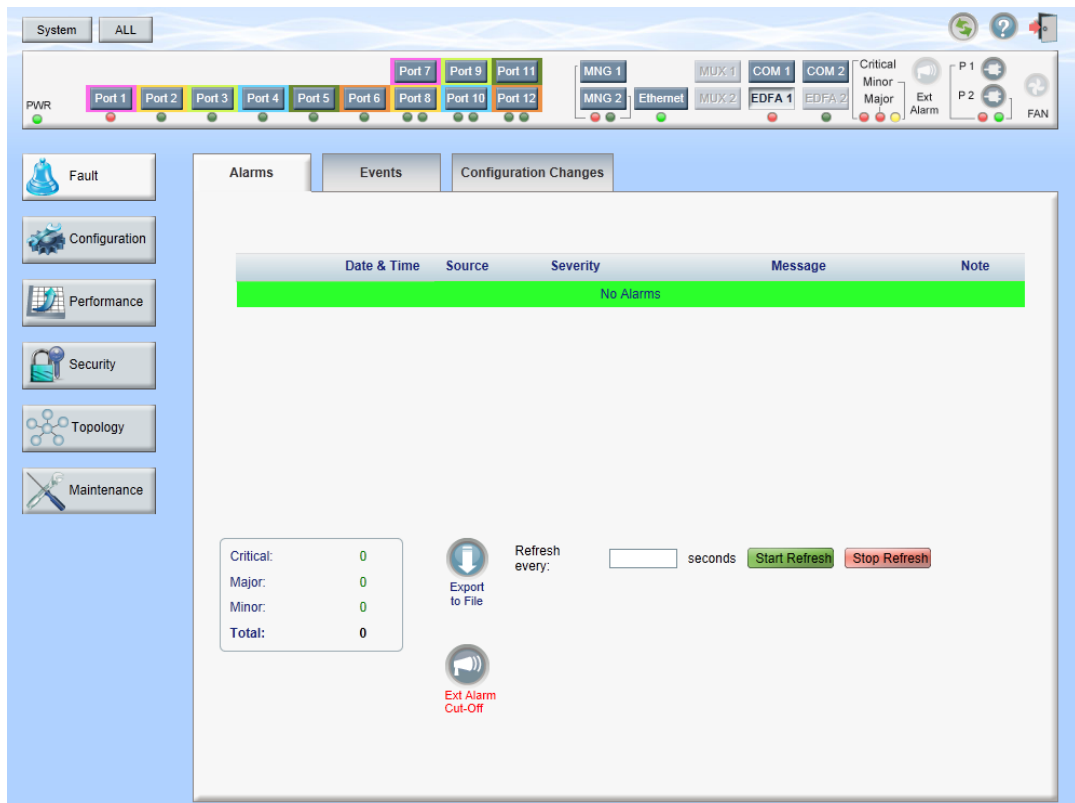


Figure 58: EDFA Fault Window

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

Use the EDFA Fault window to do the following:

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

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

To open the EDFA Fault window:

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

The appropriate EDFA Fault window opens.

5.9.1 Alarms Tab

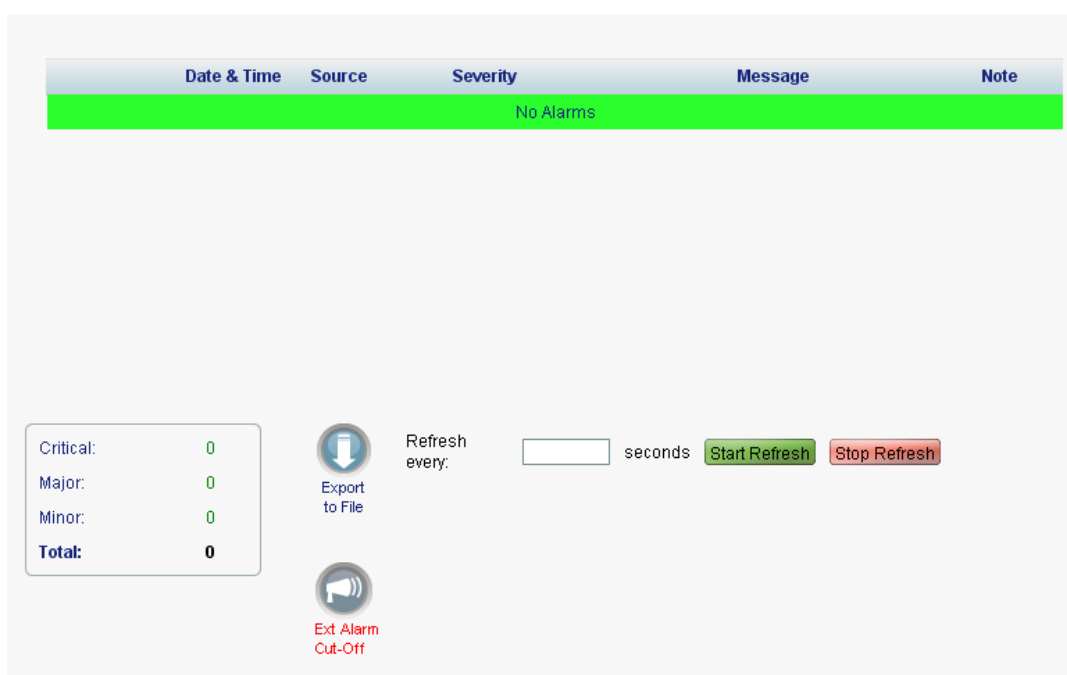


Figure 59: Alarms Tab

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. 17).

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 28: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.9.2 Events Tab

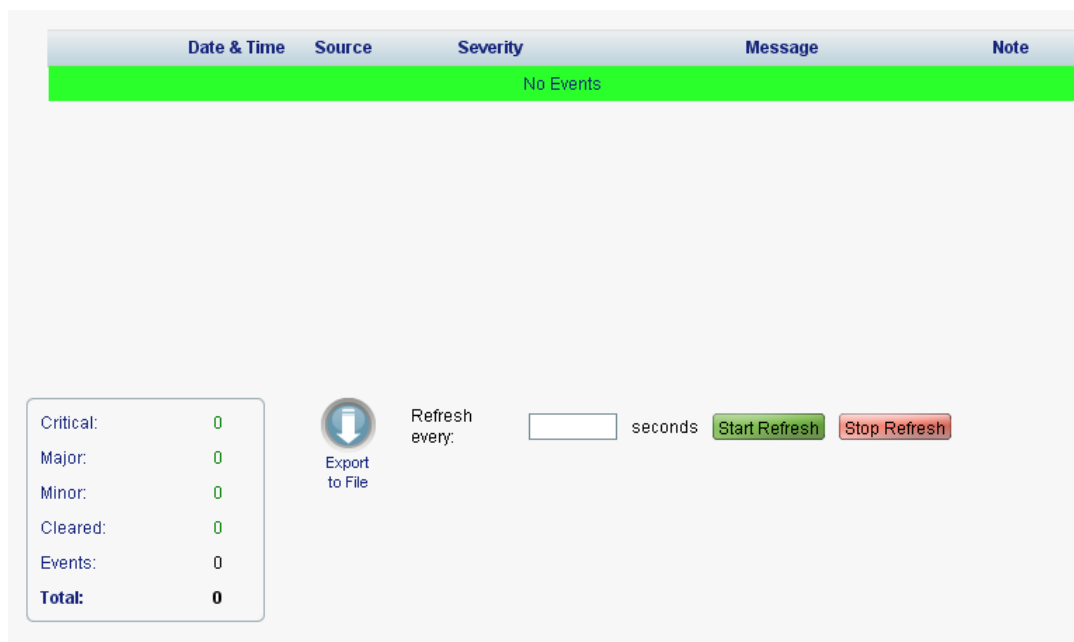


Figure 60: Events Tab

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.

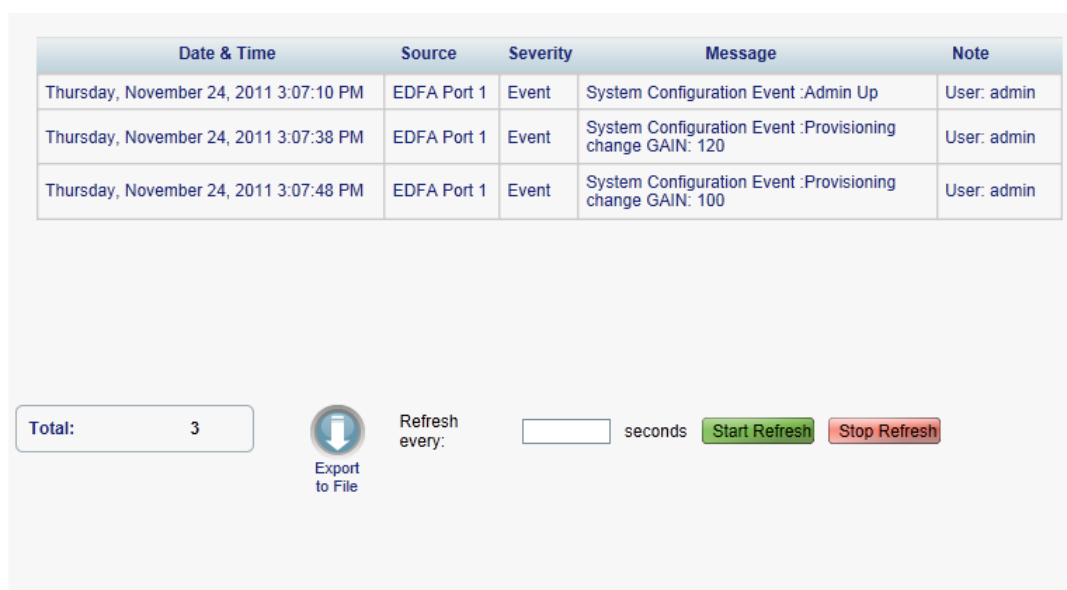
5. To stop the automatic refresh of the Fault display, click **Stop Refresh**.

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

Table 29: 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.	<ul style="list-style-type: none"> • 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



Date & Time	Source	Severity	Message	Note
Thursday, November 24, 2011 3:07:10 PM	EDFA Port 1	Event	System Configuration Event :Admin Up	User: admin
Thursday, November 24, 2011 3:07:38 PM	EDFA Port 1	Event	System Configuration Event :Provisioning change GAIN: 120	User: admin
Thursday, November 24, 2011 3:07:48 PM	EDFA Port 1	Event	System Configuration Event :Provisioning change GAIN: 100	User: admin

Total: 3

Refresh every: seconds Start Refresh Stop Refresh


 Export to File

Figure 61: 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 30: 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.	

A

5.10 COM Port Faults

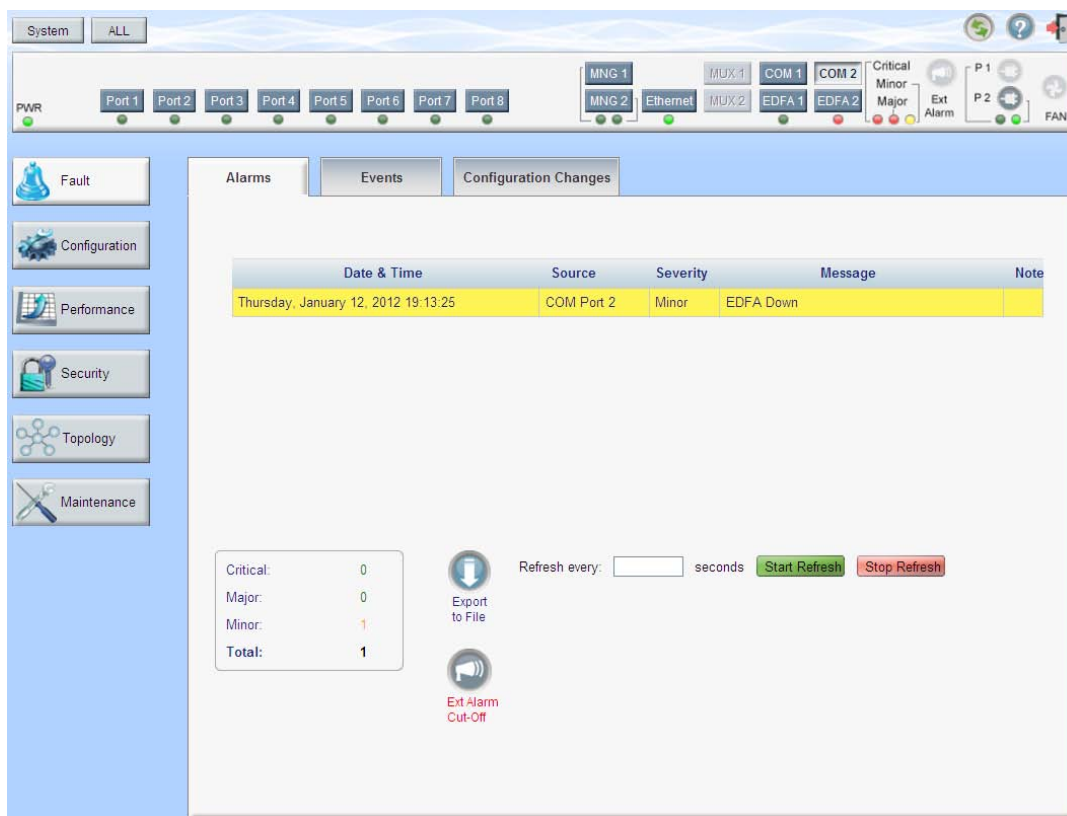


Figure 62: COM Port Fault Window

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

Use the COM Port Fault window to do the following:

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

To open the COM Port Fault window:

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

The appropriate COM Port Fault window opens.

5.10.1 Alarms Tab

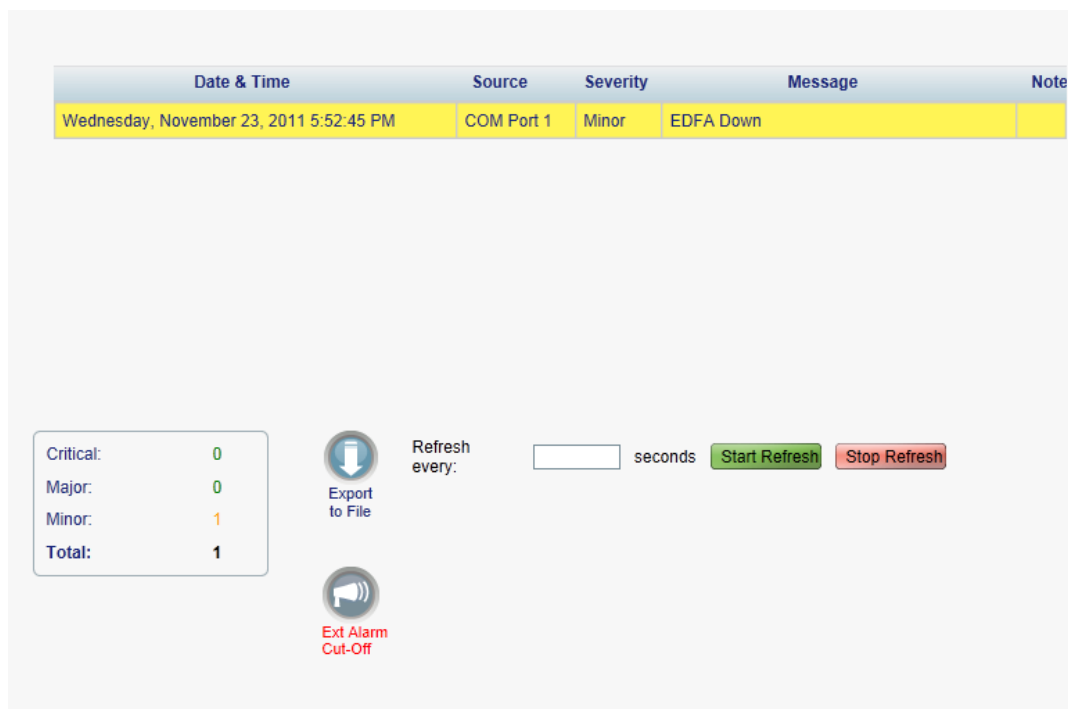


Figure 63: Alarms Tab

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. 17).

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 31: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.10.2 Events Tab

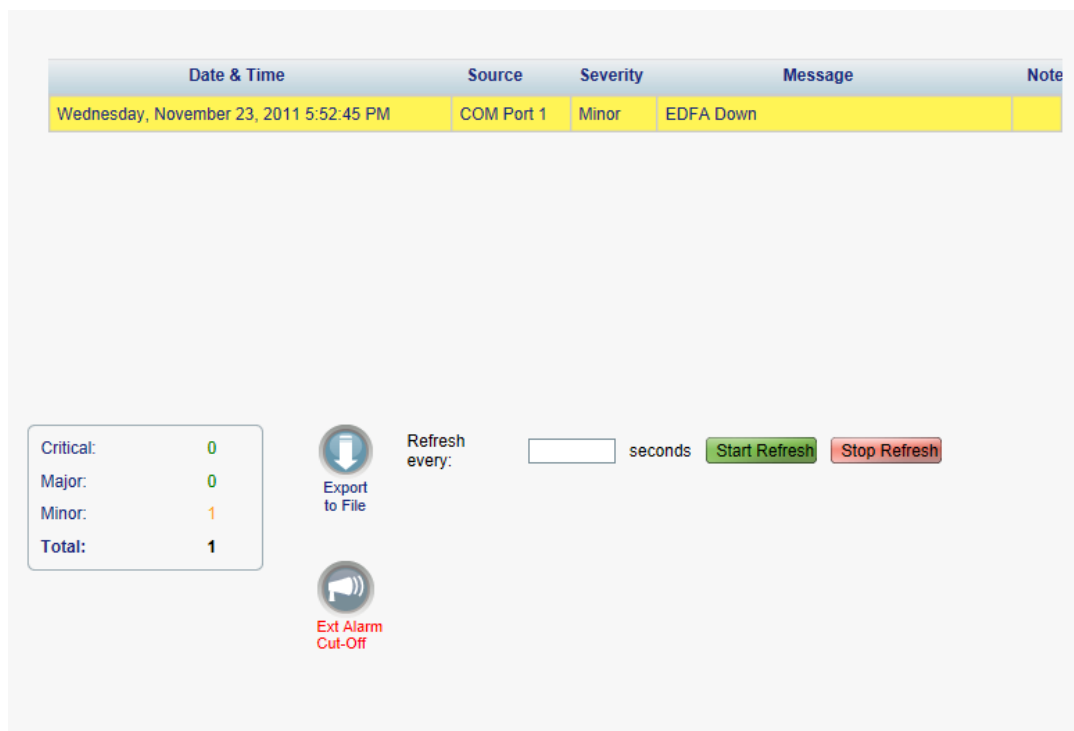


Figure 64: Events Tab

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 32: 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.	<ul style="list-style-type: none"> • 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

Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:50:59 PM	COM Port 1	Event	System Configuration Event :Create APS	
Wednesday, November 23, 2011 5:52:45 PM	COM Port 1	Event	System Configuration Event :Admin Up	User: admin
Wednesday, November 23, 2011 5:52:55 PM	COM Port 1	Event	System Configuration Event :APS command 3 OK	User: admin
Wednesday, November 23, 2011 5:52:59 PM	COM Port 1	Event	System Configuration Event :APS clear command 1 OK	User: admin

Total: 4



Export to File

Refresh every: seconds

Figure 65: 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 33: 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.	

5.11 PSU Faults

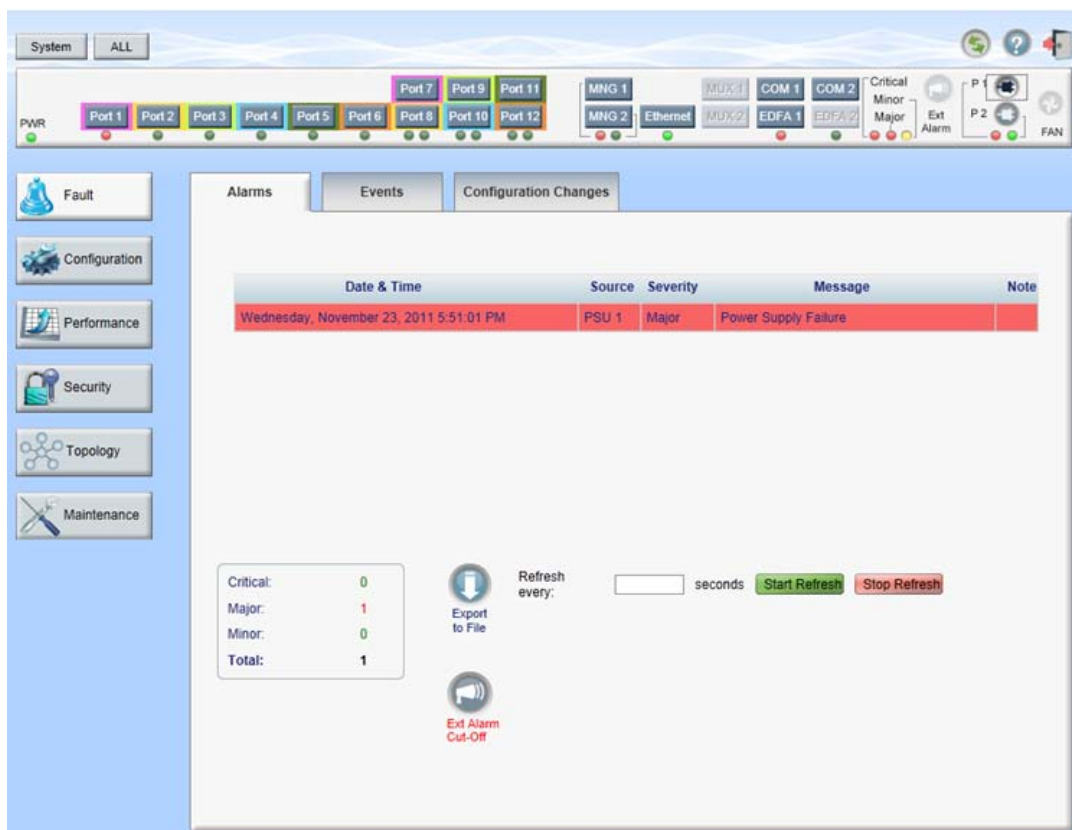



Figure 66: PSU Fault Window

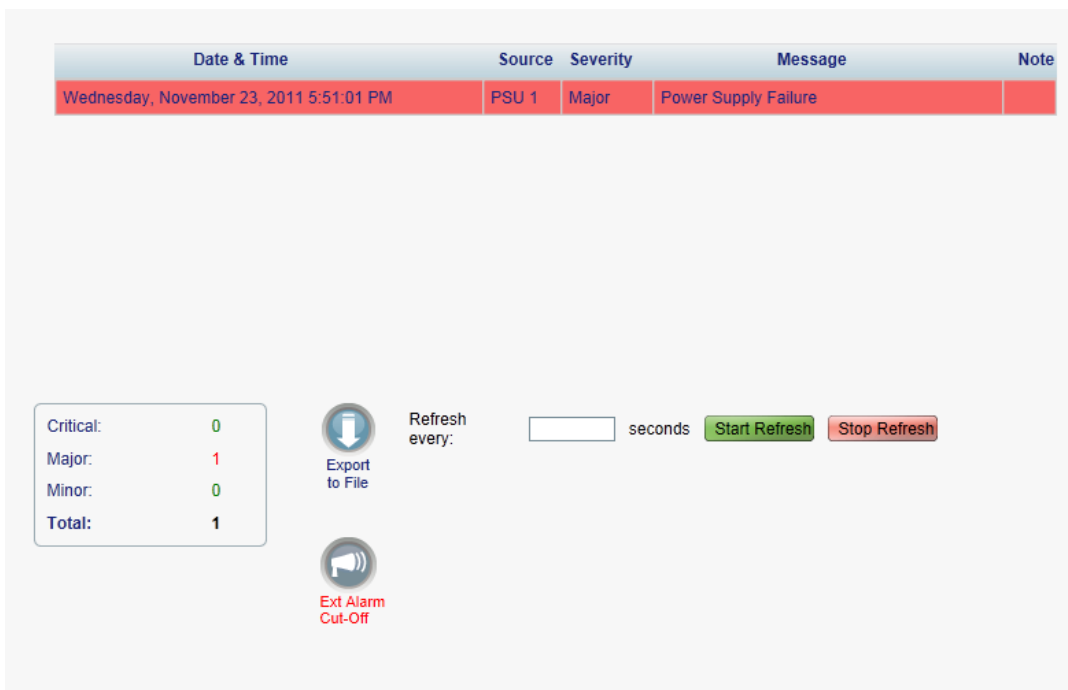
Use the PSU Fault window to do the following:

- **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.


5.11.1 Alarms Tab



Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:51:01 PM	PSU 1	Major	Power Supply Failure	

Critical:	0
Major:	1
Minor:	0
Total:	1

Refresh every: seconds Start Refresh Stop Refresh

 Export to File


 Ext Alarm Cut-Off

Figure 67: 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. 17).

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.

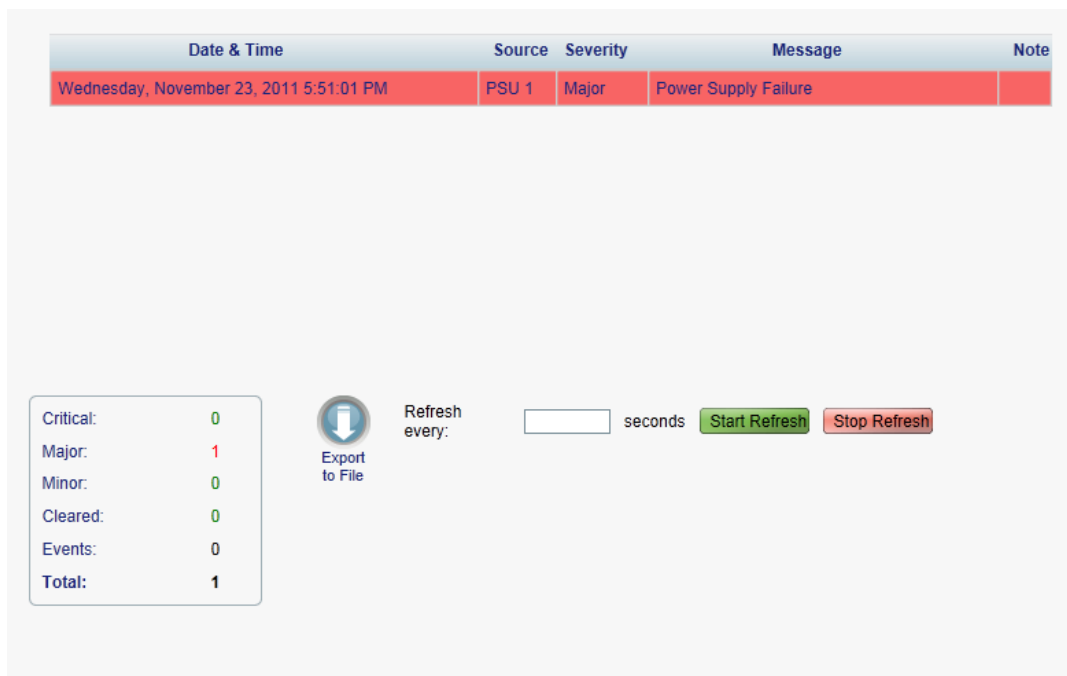
NOTE: This action does not clear any alarms.

Table 34: 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.	<ul style="list-style-type: none"> • S.A.: The alarm is service affecting. • Blank: The alarm is not service affecting.

5.11.2 Events Tab



The screenshot shows the Events Tab interface. At the top, there is a table with the following data:

Date & Time	Source	Severity	Message	Note
Wednesday, November 23, 2011 5:51:01 PM	PSU 1	Major	Power Supply Failure	

Below the table, there is a summary box on the left:

Critical:	0
Major:	1
Minor:	0
Cleared:	0
Events:	0
Total:	1

To the right of the summary box is an 'Export to File' button (downward arrow icon). Further right is a 'Refresh every:' section with an input field, the text 'seconds', and two buttons: 'Start Refresh' (green) and 'Stop Refresh' (red).

Figure 68: 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 35: 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.	<ul style="list-style-type: none"> • S.A.: The event is service affecting. • Blank: The event is not service affecting. • Other: Information related to the event.

5.11.3 Configuration Changes Tab

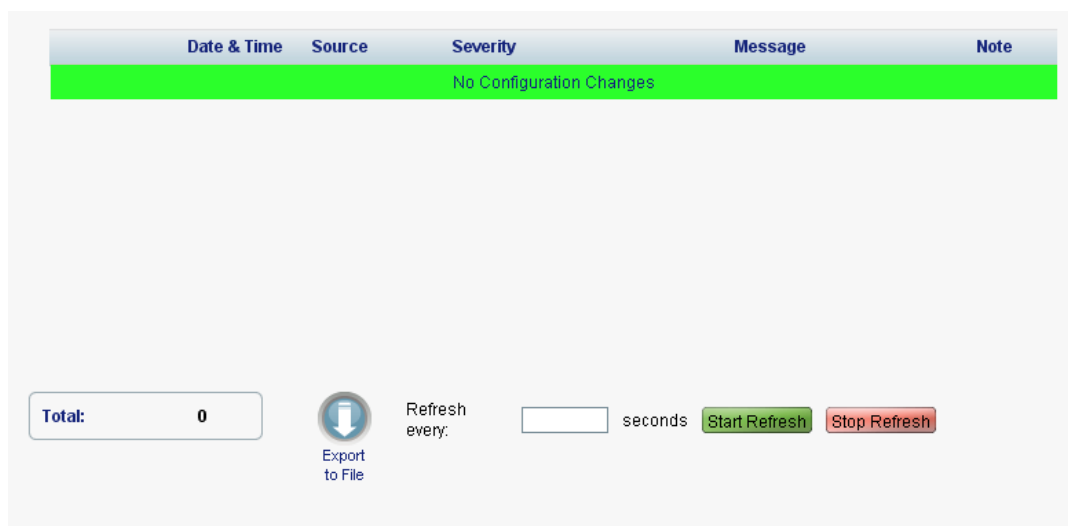


Figure 69: Configuration Changes Tab

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 36: 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.	

A

6 Configuration Management

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

For initial configuration of the PL-1000TN via a local terminal, and instructions for logging in and out of the Web application, see [Operation and Preliminary Configuration](#) (p. 35).

In this Chapter

Configuration Operations	113
General Configuration Procedure	115
System Configuration.....	116
Uplink Port Configuration.....	131
Service Port Configuration	144
Management Port Configuration.....	154
Ethernet Port Configuration.....	160
MUX/DEMUX Configuration	162
EDFA Configuration.....	163
COM Port Configuration	166
PSU Configuration.....	171
FAN Unit Configuration	172

6.1 Configuration Operations

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

- **System**
 - View general system information, such as hardware version and system uptime
 - View system inventory
 - View the currently installed license and install a new license
 - Configure Simple Network Time Protocol (SNTP) parameters
 - Configure IP addresses, default gateway, and static routing
 - Configure SNMP parameters and traps
 - Define the Syslog server you want the node to send the events to
- **Optical Ports**
 - **Uplink Port (Port 1 – Port 6)**
 - Configure port parameters
 - Configure the XFP module
 - Configure ALS parameters
 - Configure Automatic Protection Switching (APS) parameters

- Configure OTN parameters
- **Service Port (Port 7 – Port 12)**
 - View port status
 - Configure port parameters
 - Enable or disable a port
 - View SFP+ information
 - Configure ALS parameters
- **Management Port**
 - View port status
 - Configure port parameters
 - Enable or disable a port
 - View SFP information
 - Configure ALS parameters
- **Ethernet Port**
 - View port status
 - Configure port parameters
- **MUX/DEMUX Module**
 - View channel wavelength configuration
- **EDFA Module**
 - View module status
 - Configure module parameters
 - Enable or disable a module
- **COM Port**
 - View port status
 - Configure port parameters
 - Enable or disable a port
 - Configure APS parameters
- **PSU Unit**
 - View PSU parameters
- **FAN Unit**
 - View FAN parameters

6.2 General Configuration Procedure

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

To view and configure the PL-1000TN 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. 116))
 - **Optical Ports**
 - **Port 1 – Port 6** (see [Uplink Port Configuration](#) (p. 131))
 - **Port 7 – Port 12** (see [Service Port Configuration](#) (p. 144))
 - **MNG 1 – MNG 2** (see [Management Port Configuration](#) (p. 154))
 - **Ethernet** (see [Ethernet Port Configuration](#) (p. 160))
 - **MUX** (if present) (see [MUX/DEMUX Configuration](#) (p. 162))
 - **EDFA** (if present) (see [EDFA Configuration](#) (p. 163))
 - **COM** (if present) (see [COM Port Configuration](#) (p. 166))
 - **PSU** (see [PSU Configuration](#) (p. 171))
 - **FAN** (see [FAN Unit Configuration](#) (p. 172))

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

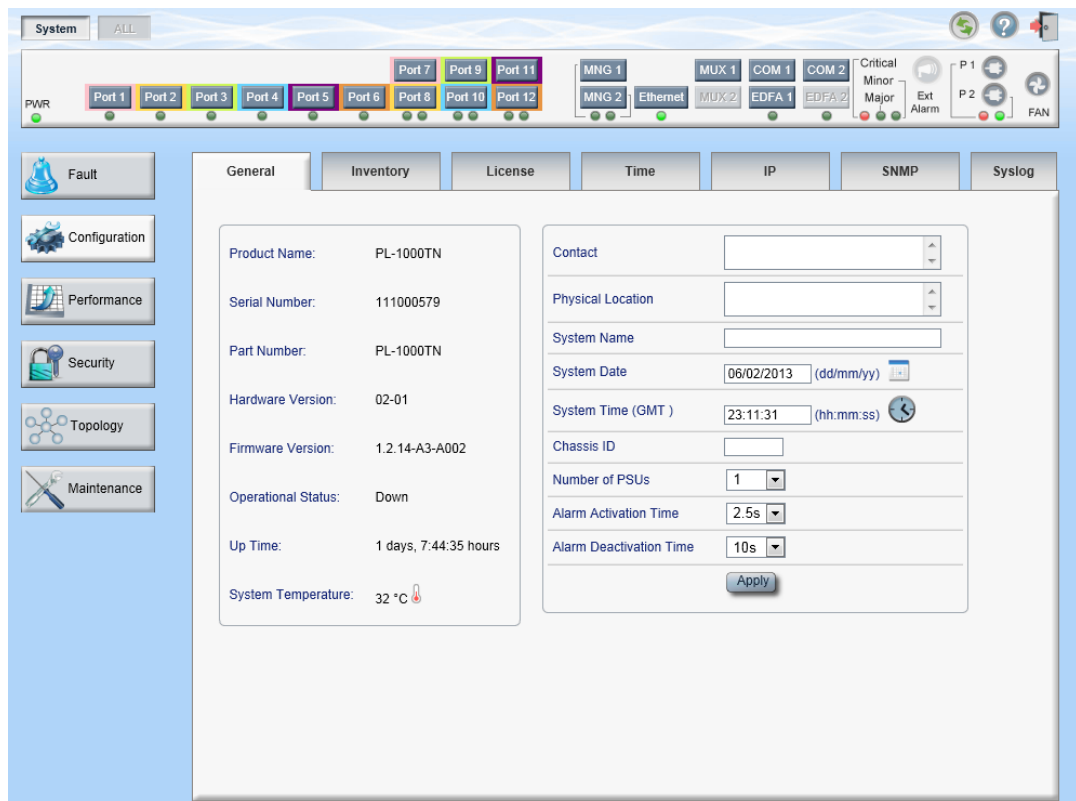


Figure 70: System Configuration Window

Use the System Configuration window to do the following:

- **General tab:** Configure general system parameters
- **Inventory tab:** View system inventory
- **License tab:** View the currently installed license and install a new license
- **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

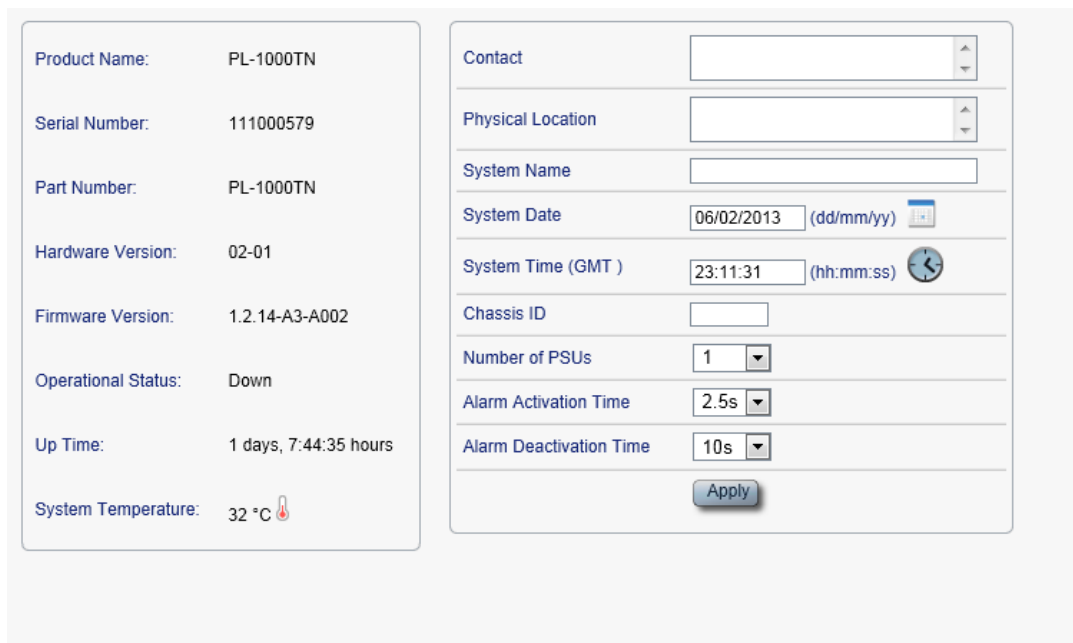


Figure 71: General Tab

Use the General tab to configure general system parameters.

To configure general system parameters:



1. Click the **General** tab.

The General tab opens displaying the general system configuration.

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

Table 37: General Tab Parameters

Parameter	Description	Format/Values
Product Name	The name of the product.	PL-1000TN
Serial Number	The serial number of the entity.	Serial number
Part Number	The part number of the node.	Part number
Hardware Version	The hardware version of the system.	dd-dd (Major-Minor)
Firmware Version	The firmware version of the system.	Firmware version
Operational Status	The operational status of the system. This indicates if there is a failure in the system.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected
Up Time	The system uptime. This shows how much time passed since last reset.	Elapsed time
System Temperature	The measured temperature of the system.	Celsius
Contact	The contact information for PacketLight Technical Support.	Free text

Parameter	Description	Format/Values
Physical Location	The address of the site.	Free text
System Name	The logical name given to the PL-1000TN.	Free text
System Date	Sets the current system date. This is the date used for time stamps.	<ul style="list-style-type: none"> • Set dd/mm/yy <i>or</i> • Select the date using the calendar  <i>or</i> • 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.	<ul style="list-style-type: none"> • Select hh:mm:ss <i>or</i> • Set the time using the clock  <i>or</i> • 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. 224)).
Number of PSUs	The number of power supply units installed in the PL-1000TN.	1, 2
Alarm Activation Time	The time from defect detection till report, if defect is still constantly detected.	2.5-10 seconds Default: 2.5 seconds NOTE: Recommended to use the default time.
Alarm Deactivation Time	The time from no defect detection till report, if defect is still constantly not detected.	2.5-10 seconds Default: 10 seconds NOTE: Recommended to use the default time.

6.3.2 Inventory Tab

Name	Description	Serial Number	Hardware Rev	Part Number	Manufacturer
PL-1000TN	Main Board	111000579	02-01	PL-1000TN	PacketLight Networks
PSU 1	DC Power Interface Card	111000720	0101	AS3371B00	
PSU 2	AC Power Interface Card	111000553	0101	AS3371A00	
FAN Unit	Cooling Fan Unit		0100	FAN UNIT	
MUX Module 1	MUX DWDM-4				
EDFA Module 1	Amplifier Module		-		
Switch Protection Module	Optical Switch			SPM-00000	




Figure 72: 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 38: 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.

Parameter	Description
Part Number	The part number of the component.
Manufacturer	The manufacturer of the component.

6.3.3 License Tab

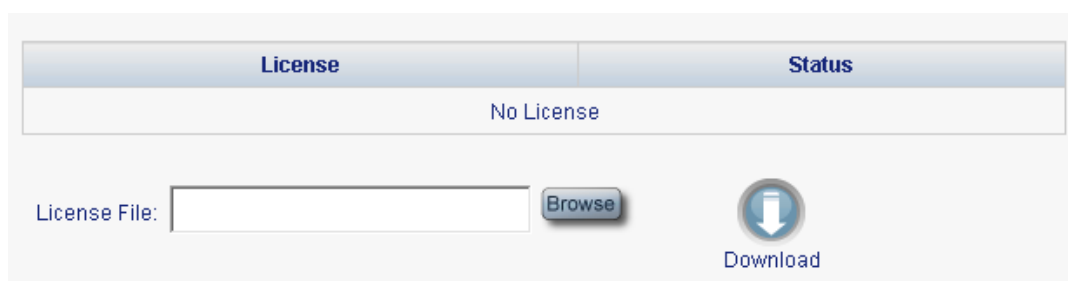


Figure 73: License Tab

Use the License tab to view the currently installed license and install a new license.

NOTE: You can also remove the license by performing a restore to factory defaults on the node. For more information, see [Restart Tab](#) (p. 202).

6.3.3.1 Licensed Features

The following licenses are available for the PL-1000TN:

- **4-Transponder license:** The PL-1000TN supports four transponders.
- **6-Transponder license:** The PL-1000TN supports six transponders.

6.3.3.2 License Types

A license can be temporary or permanent.

- **Temporary License**

A temporary license can be temporarily used until you obtain a permanent license. The same temporary license can be used for all nodes.

A temporary license is valid for 30 days. During this period, the warning alarm **Temporary License Applied** is generated.

As long as the temporary license has not expired, you can reapply the temporary license to extend the expiration period for another 30 days. The traffic is not affected by the reapplication process.

When the temporary license expires, the alarm **License Expired or No License Applied** is generated against the uplink ports but traffic is not interrupted until the next reboot of the node.

The countdown to expiration begins as soon as the license is installed.

The temporary license information is saved in the System Configuration file and is restored with the remaining expiration time when the System Configuration file is loaded.

- **Permanent License**

The permanent license is specific for a node. Therefore, if a permanent license is loaded to a different node, the resulting license will be invalid.

A permanent license can be applied to a node at any time. The operation of applying a permanent license does not affect service.

When a permanent license is applied on top of an applied temporary license, the alarms of the temporary license are cleared.

The permanent license information is saved in the System Configuration file and is restored when the System Configuration file is loaded.

6.3.3.3 Viewing the Currently Installed License

To view the currently installed license:

- Click the **License** tab.

The License tab opens displaying the currently installed license. The fields are read only and explained in the following table.

Table 39: License Tab Parameters

Parameter	Description
License	The number of the license.
Status	The status of the license.

6.3.3.4 Installing a New License

To install a new license:

1. Click the **License** tab.

The License tab opens displaying the currently installed license.

2. Click **Browse** to locate and select the file containing the license.

3. Click **Download**  to download the new license.

The new license is installed and displayed in the License table.

6.3.4 Time Tab

SNTP Configuration

Enable SNTP	Enabled <input type="button" value="v"/>
Time Zone	GMT+2 <input type="button" value="v"/>
Daylight Saving	Enabled <input type="button" value="v"/>
<input type="button" value="Apply"/>	

SNTP Servers

NTP Server Address	Server Status	Action
62.201.207.162	Connected	<input type="button" value="Delete"/>
62.201.214.162	Connected	<input type="button" value="Delete"/>
<input style="width: 100%;" type="text"/>		<input type="button" value="Add"/>

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

The PL-1000TN 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-1000TN 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. 124)).

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 40: Time Tab Parameters

Parameter	Description	Format/Values
Time Parameters		
Enable SNTP	Enables or disables the time synchronization process.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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

IP Addresses

LAN IP Address	<input type="text" value="192.10.10.10"/>
LAN Subnet Mask	<input type="text" value="255.255.0.0"/>
Default Gateway	<input type="text"/>
OSC/In-band IP Address	<input type="text" value="10.0.23.2"/>
OSC/In-band Subnet Mask	<input type="text" value="255.0.0.0"/>
Network Mode	<input type="text" value="Dual Networks"/> ▼

Static Routing

Destination Address	Subnet Mask	Gateway	Action
12.0.0.0	255.255.0.0	10.0.0.1	<input type="button" value="Delete"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Figure 74: IP Tab - Dual Networks

IP Addresses

LAN IP Address	<input type="text" value="192.168.3.2"/>
LAN Subnet Mask	<input type="text" value="255.0.0.0"/>
Default Gateway	<input type="text" value="192.168.0.150"/>
OSC/In-band IP Address	<input type="text" value="192.168.3.2"/>
OSC/In-band Subnet Mask	<input type="text" value="255.0.0.0"/>
Network Mode	<input type="text" value="Single Network"/> ▼

Static Routing

Destination Address	Subnet Mask	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Figure 75: IP Tab - Single Network

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

The PL-1000TN 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-1000TN; 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.

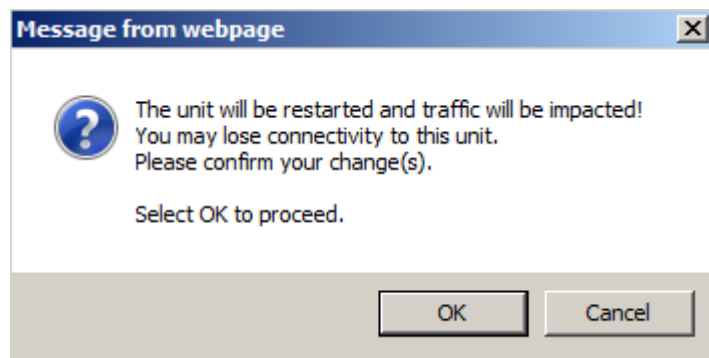


Figure 76: Confirm Changes

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 41: IP Tab Parameters

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

Parameter	Description	Format/Values
OSC/In-band IP Address	The IP address of the OSC management channels.	Dot notation For example: 10.0.11.34 NOTE: <ul style="list-style-type: none"> This field is read only when Network Mode is set to Single Network. The same IP address applies to both MNG ports.
OSC/In-band Subnet Mask	The subnet mask of the OSC.	Dot notation For example: 255.0.0.0 NOTE: This field is read only when Network Mode is set to Single Network .
Network Mode	The mode of the network.	Dual Networks, Single Network NOTE: This field appears only for certain hardware versions.

Static Routing

Destination Address	The address of the destination.	IP address For example: 11.0.3.24
Subnet Mask	The subnet mask of the destination route.	Dot notation For example: 255.255.255.0
Gateway	The address of the gateway for this destination.	IP address For example: 192.168.0.150

6.3.6 SNMP Tab

SNMP Configuration

Read-Only Community String	<input type="text" value="read-only"/>
Read-Write Community String	<input type="text" value="read-write"/>
SNMP Trap Compatibility Format	<input type="text" value="Full IfIndex Mode"/> ▼

SNMP Traps

Manager Address	SNMP Traps	Community	Trap Port	Action
192.168.1.42	SNMP V2c	public	162	<input type="button" value="Delete"/>
<input type="text"/>	<input type="text" value="SNMP V2c"/> ▼	<input type="text" value="public"/>	<input type="text" value="162"/>	<input type="button" value="Add"/>

Figure 77: 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-1000TN must have a specific IP route. Therefore, if needed, add the management system address to the **Static Routing** table (see [IP Tab](#) (p. 124)).

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 42: 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.	<ul style="list-style-type: none"> • Port IfIndex Mode: Used with the legacy Network Management System (NMS) • Full IfIndex Mode: Used with any other NMS.
SNMP Traps		
Manager Address	The address of the management system.	IP address For example: 192.168.1.50
SNMP Traps	The SNMP trap format.	SNMPV2c, SNMPV1 Default: SNMPV2c

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

6.3.7 Syslog Tab



Figure 78: 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. 56)).

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.

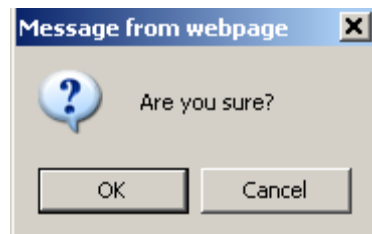


Figure 79: Confirm Configuration

3. Click **OK**.

3. To remove a configured Syslog server:

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

The following confirmation message appears.

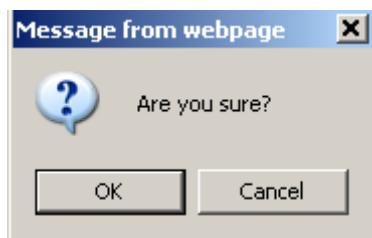


Figure 80: Confirm Configuration

2. Click **OK**.

Table 43: 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.	<ul style="list-style-type: none"> • Traps: Traps only • Log: Log messages • Debug: Log and debug messages Default: Traps

6.4 Uplink Port Configuration

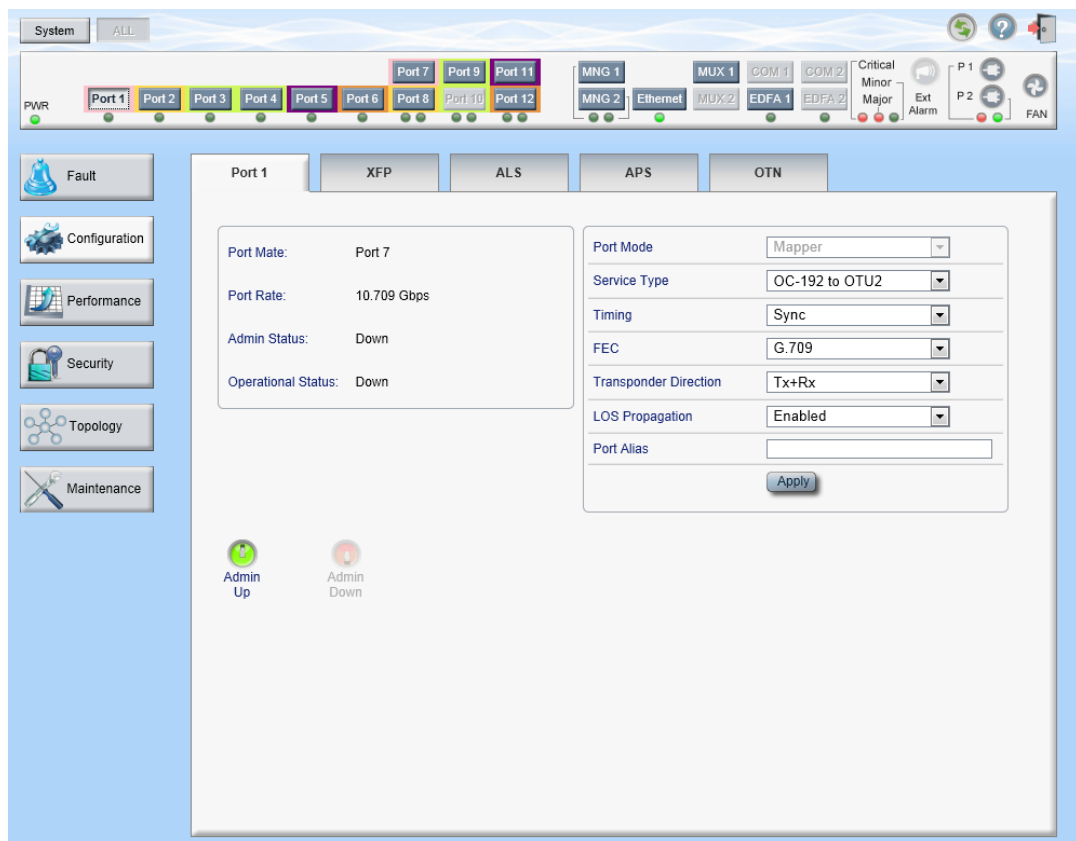


Figure 81: Uplink Port Configuration Window

Use the Uplink Port Configuration window to do the following:

- **Uplink tab:** Configure an uplink port and enable/disable the port
- **XFP Information tab:** Configure the XFP module
- **ALS tab:** Configure ALS for an uplink port
- **APS tab:** Create an APS group (this feature is not available when the optional Optical Switch module is installed)
- **OTN tab:** Configure OTN for an uplink port

To open the Uplink Port Configuration window:

1. Click **Configuration**.
2. Click a **Port** button (Port 1-6) to select the uplink port.

The appropriate Uplink Port Configuration window opens.

6.4.1 Port Tab

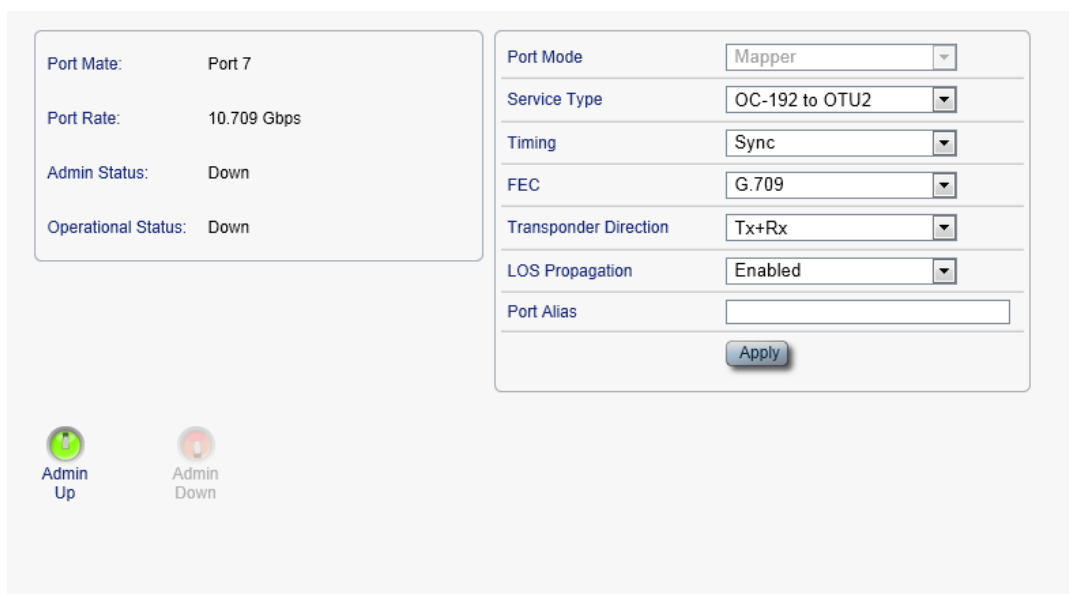



Figure 82: Port Tab

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

To configure an uplink port:

1. Click the **Port** tab.
 - The Port 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.

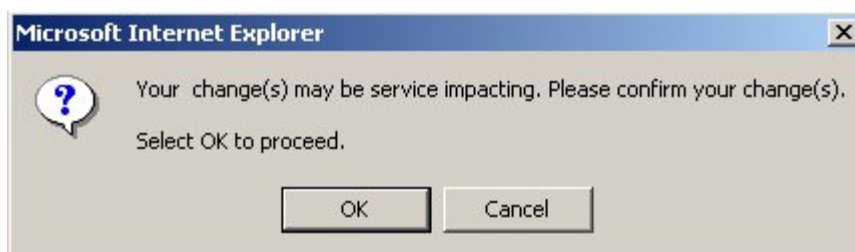


Figure 83: Confirm Changes

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.

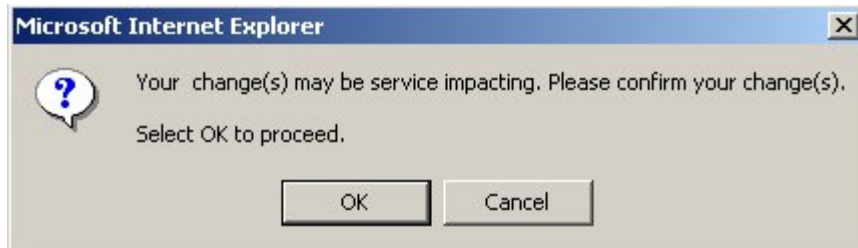


Figure 84: Confirm Changes

2. Click **OK**.

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

Table 44: Port Tab Parameters

Parameter	Description	Format/Values
Port Mate	The service port of the transponder.	Port number
Port Rate	The bit rate of the uplink.	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.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected or Admin Down
Port Mode	The mode of the transponder.	Mapper
Service Type	The type of transponder mapping.	<ul style="list-style-type: none"> • 8G FC to OTU2 • 10G FC to OTU2f • 10GBE-LAN to OTU2e • OC-192 to OTU2 • STM-64 to OTU2
Timing	The timing of the transponder mapping.	<ul style="list-style-type: none"> • Sync: OTN G.709 Sync mapping with FEC • Async: OTN G.709 Async mapping with FEC
FEC	The FEC mode.	<ul style="list-style-type: none"> • G.709: The ITU G.709 FEC • I.4: ITU G.975 Appendix I.4 FEC

Parameter	Description	Format/Values
Transponder Direction	Used to determine the direction of the traffic for unidirectional services.	<ul style="list-style-type: none"> • Tx+Rx: Both ports are bidirectional • Rx: Service is Rx only; Uplink is Tx only • Tx: Service is Tx only; Uplink is Rx only
Connect Fiber Lambda #	<p>The connection between the MUX/DEMUX module and the uplink ports are done with a ribbon cable. One end of the ribbon cable is connected to the MUX/DEMUX port and the fibers of the other end to the uplink ports and the OSC.</p> <p>To allow correct connectivity, each LC connector of the ribbon is labeled with "λ1", "λ2", and so on, according to the number of channels supported by the MUX/DEMUX." λ1" corresponds to the lowest ITU channel number of the MUX/DEMUX," λ2" to the next channel, and so on.</p>	<p>The label of the ribbon LC connector to which this port should be connected.</p> <p>NOTE: This field is displayed only if a MUX/DEMUX module is installed.</p>
LOS Propagation	Enable or disable LOS propagation.	<p>Enabled, Disabled</p> <p>NOTE:</p> <ul style="list-style-type: none"> ▪ Changing the LOS Propagation value of one APS port will automatically change the values of the other APS ports. ▪ The LOS Propagation value applies to both directions of the transponder. ▪ When LOS Propagation is enabled and one of the transponder ports detects LOS, the laser of the other port will automatically shut off. ▪ For a protected transponder, the laser of the service port will automatically shut off only when both uplink port mates detect LOS.
Port Alias	The logical name given to the port for identification purposes.	Free text

6.4.2 XFP Tab



Figure 85: XFP Tab

Use the XFP tab to display information about the type and status of the optical transceiver inserted in the selected uplink port, configure the override low receiver power alarm threshold, enable or disable dithering, and select the wavelength tuning.

To configure the XFP module:

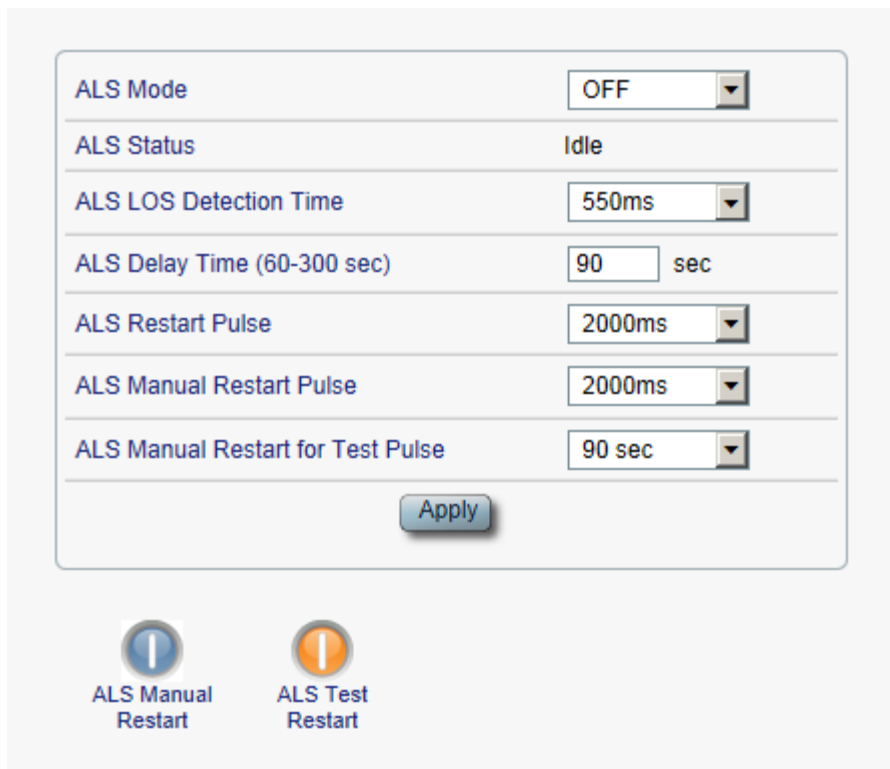
1. Click the **XFP** tab.
The XFP tab opens displaying the XFP configuration.
2. Fill in the fields as explained in the following table.
3. (If applicable) To enable or disable dithering for the XFP module, select or clear the **Dithering Enable** check box.
4. (If applicable) To select the wavelength, from the **Wavelength Tuning** drop-down list, select a wavelength.
5. Click **Apply**.

Table 45: XFP Tab Parameters

Parameter	Description	Format/Values
Vendor Name	The name of the XFP vendor.	String
Nominal Wavelength	The defined wavelength of the XFP.	nm
Wavelength Tolerance	The wavelength tolerance of the XFP.	nm

Parameter	Description	Format/Values
Bit Rate Range	The range of bit rate supported by the XFP.	Gbps
Part Number	The part number of the XFP.	String
Serial Number	The serial number of the XFP.	String
Connector Type	The type of XFP connector.	LC
Transmitter Output Power	The measured output power of the XFP.	dBm
Receiver Input Power	The measured input power of the XFP.	dBm
Temperature	The measured temperature of the XFP.	Celsius
10GBE-LAN and 10GBE-WAN capabilities	The XFP capabilities of the 10GbE-LAN and 10GbE-WAN services are marked.	
10G FC capabilities	The XFP capabilities of the 10G FC services are marked.	
OC-192 and OTU-2 capabilities	The XFP capabilities of the OC-192 and OTU-2 services are marked.	
High Receiver Power Default Threshold	The default threshold for the High Receiver Power alarm.	dBm
Low Receiver Power Default Threshold	The default threshold for the Low Receiver Power alarm.	dBm
Override Low Receiver Power Alarm Threshold	The configured threshold for the Low Receiver Power alarm.	dBm
Dithering Enable	Whether to enable or disable dithering for the XFP module.	<ul style="list-style-type: none"> • Selected: Enable dithering • Cleared: Disable dithering <p>NOTE: This field is displayed only if the XFP module supports dithering as defined by the SFF-8477 standard.</p>
Wavelength Tuning	Select the DWDM channel.	ITU grid channel number <p>NOTE: This field is displayed only if the XFP module supports wavelength tuning as defined by the SFF-8477 standard.</p>

6.4.3 ALS Tab



ALS Mode	OFF
ALS Status	Idle
ALS LOS Detection Time	550ms
ALS Delay Time (60-300 sec)	90 sec
ALS Restart Pulse	2000ms
ALS Manual Restart Pulse	2000ms
ALS Manual Restart for Test Pulse	90 sec

Apply

ALS Manual Restart
ALS Test Restart

Figure 86: 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-1000TN 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 46: 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 APS Tab

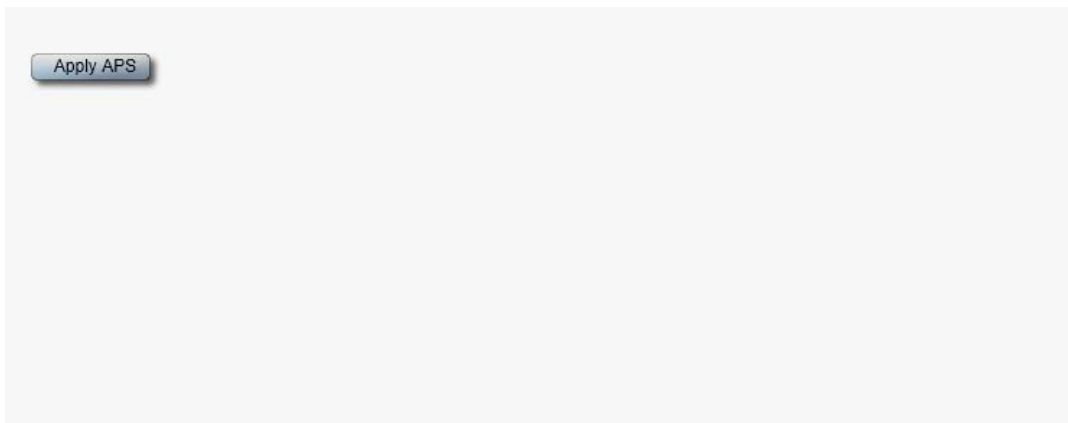


Figure 87: APS Tab - Without Protection

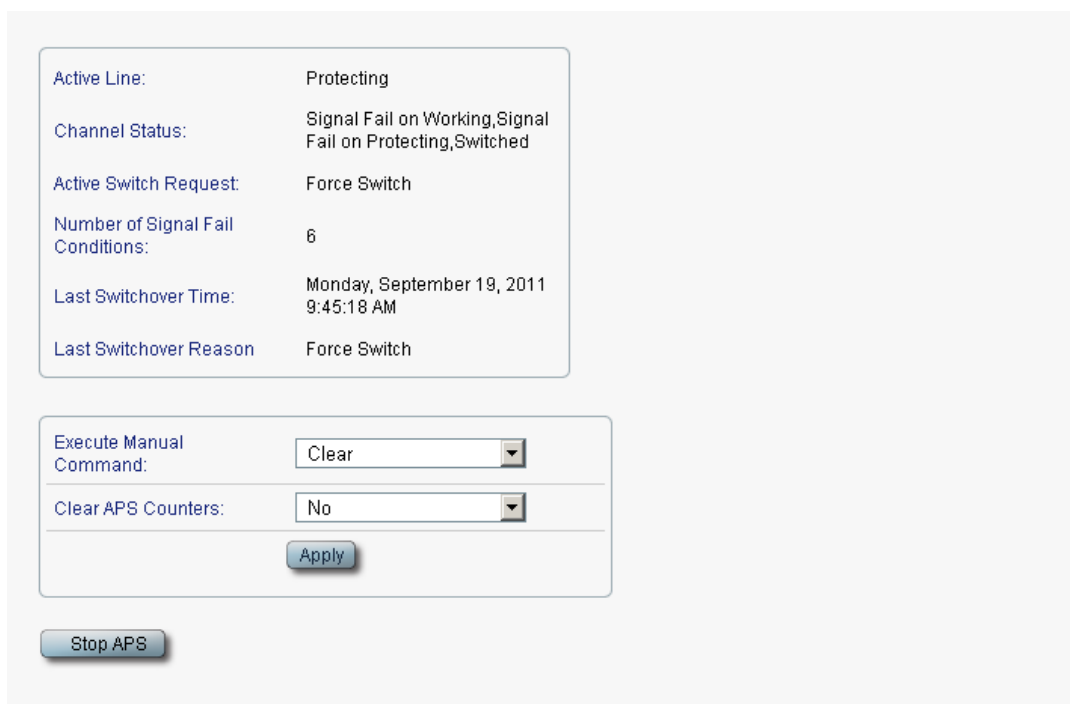


Figure 88: APS Tab - With Protection

NOTE: This feature is not available when the optional Optical Switch module is installed.

Use the APS tab to create and configure an APS group for the related uplink and service ports. Once created, the APS groups are marked with colors as depicted by the following figure.

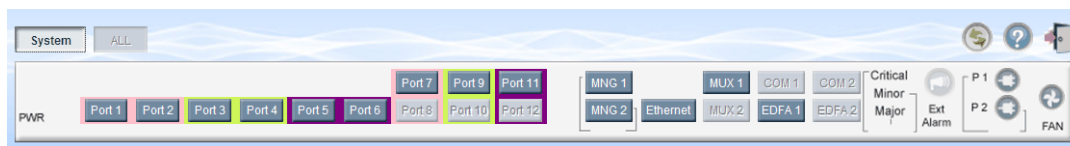


Figure 89: APS Groups

NOTE:

- Before applying APS, verify that all ports in the group:
 - Have the same service type.
 - Are in **Admin Down** state.
- The APS group cannot be defined on the unused ports in a protected configuration (for example, Ports 8, 10, and 12).

To configure APS:

1. Click the **APS** tab.

The APS tab opens.

2. To apply APS:

1. Click **Apply APS**.

The following confirmation message appears.

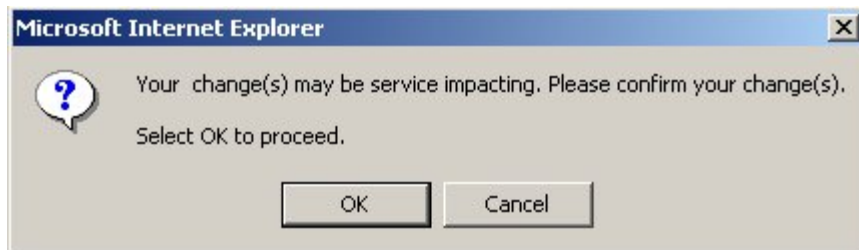


Figure 90: Confirm Changes

2. Click **OK**.

The APS configuration is displayed and the **Apply APS** button toggles to **Stop APS**.

3. Fill in the fields as explained in the following table.
4. Click **Apply**.
5. To remove APS:

1. Click **Stop APS**.

The following confirmation message appears.



Figure 91: Confirm Changes

2. Click **OK**.

The **Stop APS** button toggles to **Apply APS**.

NOTE: Before removing APS, you should **Admin Down** all ports in the group.

Table 47: APS Tab Parameters

Parameter	Description	Format/Values
Active Line	The current active uplink.	Working, Protecting
Channel Status	The current APS channel status.	Any combination of the following values: <ul style="list-style-type: none"> • Signal Fail on Working • Signal Fail on Protecting • Switched (to Protecting)
Active Switch Request	The switch request currently in effect.	<ul style="list-style-type: none"> • Manual Command • Signal Fail • Force Switch • Other
Number of Signal Fail Conditions	The number of times the Signal Fail condition occurred.	Integer
Last Switchover Time	The time of the last switchover event.	Date and time
Last Switchover Reason	The reason for the last switchover.	<ul style="list-style-type: none"> • Manual Command • Signal Fail • Force Switch • Other
Execute Manual Command	The manual APS commands.	<ul style="list-style-type: none"> • Clear: Clears the last APS switch command. • Force Switch to Protecting: Forces switch to Protecting in any condition. • Force Switch to Working: Forces switch to Working in any condition. • Manual Switch to Protecting: Switches to Protecting only if the protecting uplink is functioning properly. • Manual Switch to Working: Switches to Working only if the working uplink is functioning properly. Default: Clear
Clear APS Counters	Whether or not to clear the APS counters.	<ul style="list-style-type: none"> • No: Does not clear the APS counters. • Yes: Clears the APS counters. Default: No

6.4.5 OTN Tab

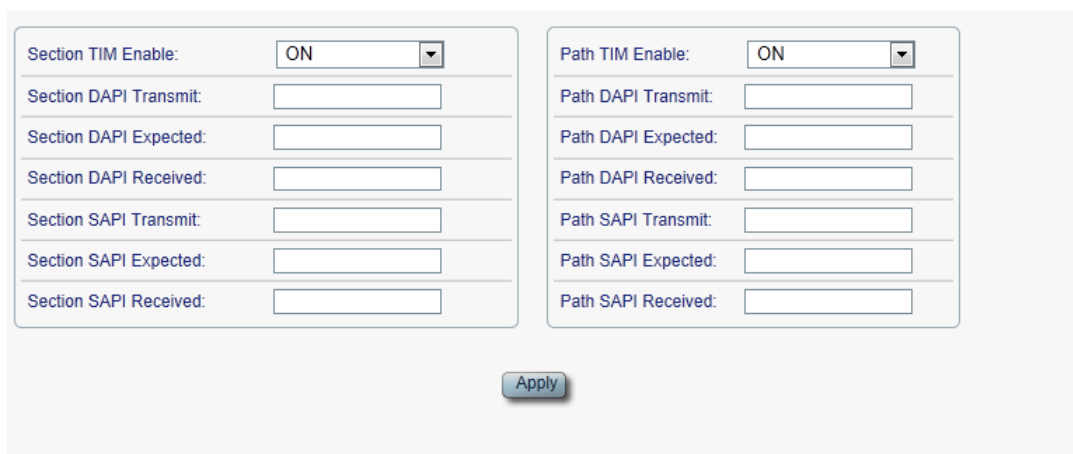


Figure 92: OTN Tab

Use the OTN tab to configure OTN for an 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 48: OTN Tab Parameters

Parameter	Description	Format/Values
Section TIM Enable	Whether or not an alarm should be given when the received trace messages and expected messages are not the same.	<ul style="list-style-type: none"> • 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.

Parameter	Description	Format/Values
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.	<ul style="list-style-type: none"> • 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.
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 Service Port Configuration

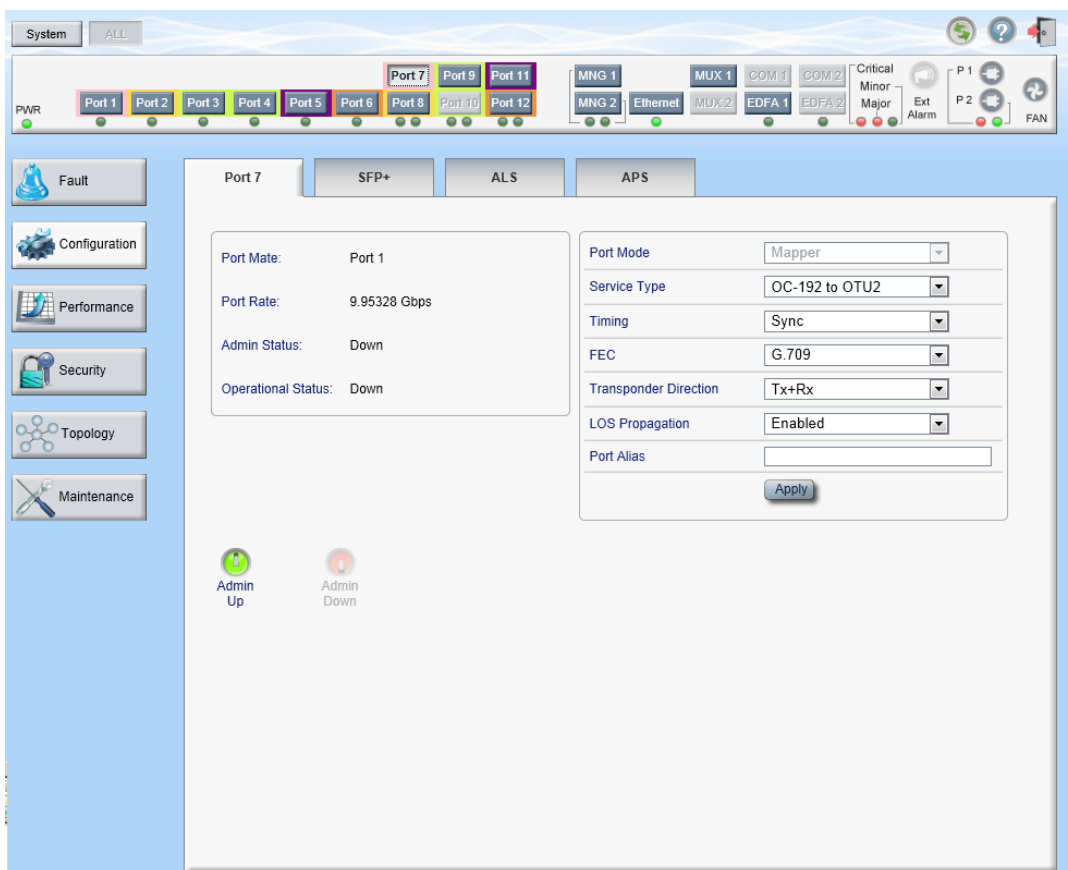


Figure 93: Service Port Configuration Window

Use the Service Port Configuration window to do the following:

- **Port tab:** Configure a service port and enable/disable the port
- **SFP+ tab:** Display information about the type and status of the optical transceiver inserted in the selected port
- **ALS tab:** Configure ALS for a service port
- **APS tab:** Create an APS group (this feature is not available when the optional Optical Switch module is installed)

To open the Service Port Configuration window:

1. Click **Configuration**.
2. Click a **Port** button (Port 7-12) to select the service port.

The appropriate Service Port Configuration window opens.


6.5.1 Port Tab



Figure 94: Port Tab

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

To configure a service port:

1. Click the **Port** tab.
 - The Port tab opens displaying the service 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.

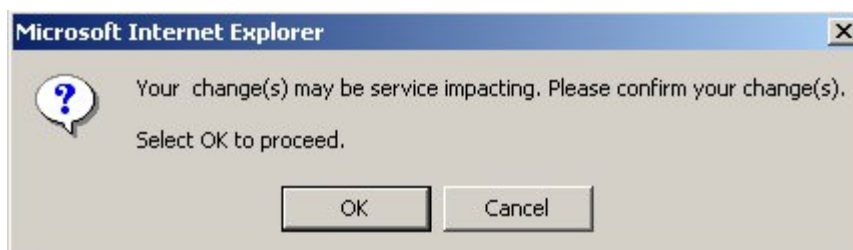


Figure 95: Confirm Changes

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.

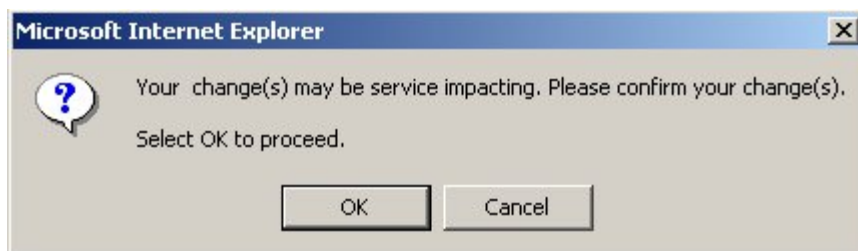


Figure 96: Confirm Changes

2. Click **OK**.

6. 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 Mate	The uplink port of the transponder.	Port number
Port Rate	The bit rate of the service.	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.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected or Admin Down
Port Mode	The mode of the transponder.	Mapper
Service Type	The type of transponder mapping.	<ul style="list-style-type: none"> • 8G FC to OTU2 • 10G FC to OTU2f • 10GBE-LAN to OTU2e • OC-192 to OTU2 • STM-64 to OTU2
Timing	The timing of the transponder mapping.	<ul style="list-style-type: none"> • Sync: OTN G.709 Sync mapping with FEC • Async: OTN G.709 Async mapping with FEC
FEC	The FEC mode.	<ul style="list-style-type: none"> • G.709: The ITU G.709 FEC • I.4: ITU G.975 Appendix I.4 FEC

Parameter	Description	Format/Values
Transponder Direction	Used to determine the direction of the traffic for unidirectional services.	<ul style="list-style-type: none"> • Tx+Rx: Both ports are bidirectional • Rx: Service is Rx only; Uplink is Tx only • Tx: Service is Tx only; Uplink is Rx only
Connect Fiber Lambda #	<p>The connection between the MUX/DEMUX module and the uplink ports are done with a ribbon cable. One end of the ribbon cable is connected to the MUX/DEMUX port and the fibers of the other end to the uplink ports and the OSC.</p> <p>To allow correct connectivity, each LC connector of the ribbon is labeled with "λ1", "λ2", and so on, according to the number of channels supported by the MUX/DEMUX. "λ1" corresponds to the lowest ITU channel number of the MUX/DEMUX, "λ2" to the next channel, and so on.</p>	<p>The label of the ribbon LC connector to which this port should be connected.</p> <p>NOTE: This field is displayed only if a MUX/DEMUX module is installed.</p>
LOS Propagation	Enable or disable LOS propagation.	<p>Enabled, Disabled</p> <p>NOTE:</p> <ul style="list-style-type: none"> ▪ Changing the LOS Propagation value of one APS port will automatically change the values of the other APS ports. ▪ The LOS Propagation value applies to both directions of the transponder. ▪ When LOS Propagation is enabled and one of the transponder ports detects LOS, the laser of the other port will automatically shut off. ▪ For a protected transponder, the laser of the service port will automatically shut off only when both uplink port mates detect LOS.
Port Alias	The logical name given to the port for identification purposes.	Free text

6.5.2 SFP+ Tab



The screenshot shows the SFP+ configuration interface. On the left, a form contains the following fields:

- Vendor Name: FINISAR CORP.
- Nominal Wavelength: 1310 nm
- WDM Class: No WDM
- Part Number: FTLX1471D3BCL
- Serial Number: ALC0SEA
- WDM Channel Spacing: NA
- Connector Type: LC

Below this form, a summary box displays:

- Transmitter Output Power: -29.2 dBm
- Receiver Input Power: NA
- Temperature: 32 °C

On the right, a configuration table is shown:

ESCON	SM	MM	
OC3	OC12	OC48	OC192
SR	IR	LR	
SM	MM		
100Mb	GBE	10GBE	
SM	MM		
FC			
VLD	LD	ID	SD
LW	SW	SW-OFC	
SM	MM		
100MB	200MB	400MB	800MB 1200MB

Below the table, another configuration box contains:

- High Receiver Power Default Threshold: 2.5 dBm
- Low Receiver Power Default Threshold: -20.0 dBm
- Override Low Receiver Power Alarm Threshold: dBm
-

Figure 97: 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 receiver power alarm threshold.

To configure the SFP+ module:

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

The SFP+ tab opens displaying the SFP+ configuration.

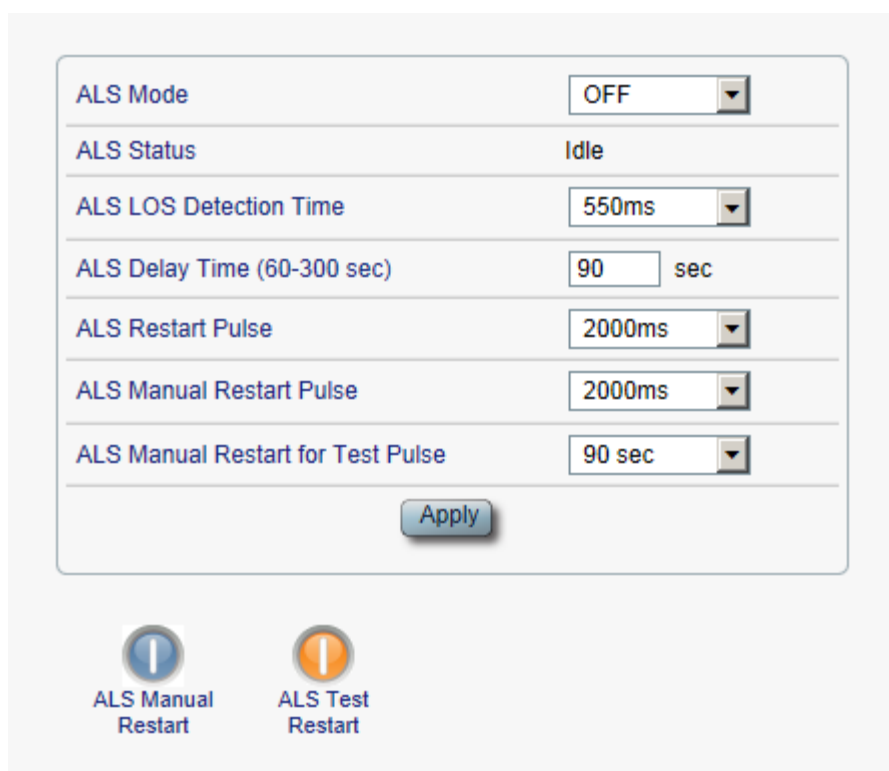
2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 50: 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+.	<ul style="list-style-type: none"> • CWDM: nm • DWDM: GHz

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

6.5.3 ALS Tab



ALS Mode: OFF
 ALS Status: Idle
 ALS LOS Detection Time: 550ms
 ALS Delay Time (60-300 sec): 90 sec
 ALS Restart Pulse: 2000ms
 ALS Manual Restart Pulse: 2000ms
 ALS Manual Restart for Test Pulse: 90 sec

Apply

ALS Manual Restart ALS Test Restart

Figure 98: 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-1000TN 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 51: ALS Tab Parameters

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

6.5.4 APS Tab

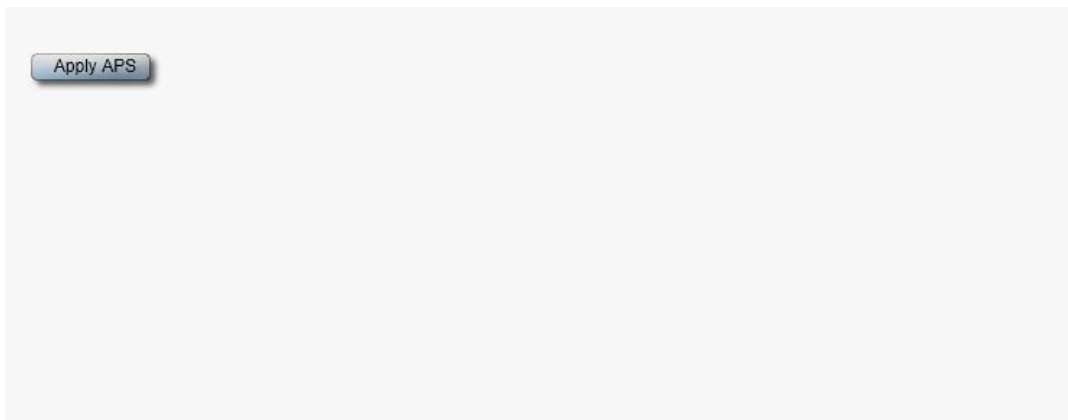


Figure 99: APS Tab - Without Protection



Figure 100: APS Tab - With Protection

NOTE: This feature is not available when the optional Optical Switch module is installed.

Use the APS tab to create and configure an APS group for the related uplink and service ports. Once created, the APS groups are marked with colors as depicted by the following figure.

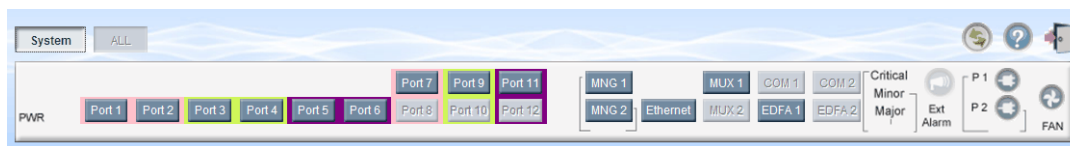


Figure 101: APS Groups

NOTE:

- Before applying APS, verify that all ports in the group:
 - Have the same service type.
 - Are in **Admin Down** state.
- The APS group cannot be defined on the unused ports in a protected configuration (for example, Ports 8, 10, and 12).

To configure APS:

1. Click the **APS** tab.

The APS tab opens.

2. To apply APS:

1. Click **Apply APS**.

The following confirmation message appears.

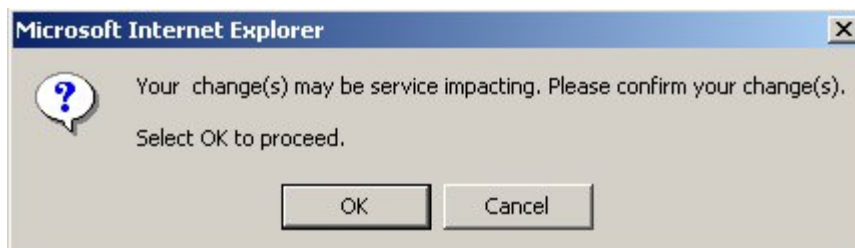


Figure 102: Confirm Changes

2. Click **OK**.

The APS configuration is displayed and the **Apply APS** button toggles to **Stop APS**.

3. Fill in the fields as explained in the following table.
4. Click **Apply**.
5. To remove APS:

1. Click **Stop APS**.

The following confirmation message appears.



Figure 103: Confirm Changes

2. Click **OK**.

The **Stop APS** button toggles to **Apply APS**.

NOTE: Before removing APS, you should **Admin Down** all ports in the group.

Table 52: APS Tab Parameters

Parameter	Description	Format/Values
Active Line	The current active uplink.	Working, Protecting
Channel Status	The current APS channel status.	Any combination of the following values: <ul style="list-style-type: none"> • Signal Fail on Working • Signal Fail on Protecting • Switched (to Protecting)
Active Switch Request	The switch request currently in effect.	<ul style="list-style-type: none"> • Manual Command • Signal Fail • Force Switch • Other
Number of Signal Fail Conditions	The number of times the Signal Fail condition occurred.	Integer
Last Switchover Time	The time of the last switchover event.	Date and time
Last Switchover Reason	The reason for the last switchover.	<ul style="list-style-type: none"> • Manual Command • Signal Fail • Force Switch • Other
Execute Manual Command	The manual APS commands.	<ul style="list-style-type: none"> • Clear: Clears the last APS switch command. • Force Switch to Protecting: Forces switch to Protecting in any condition. • Force Switch to Working: Forces switch to Working in any condition. • Manual Switch to Protecting: Switches to Protecting only if the protecting uplink is functioning properly. • Manual Switch to Working: Switches to Working only if the working uplink is functioning properly. Default: Clear
Clear APS Counters	Whether or not to clear the APS counters.	<ul style="list-style-type: none"> • No: Does not clear the APS counters. • Yes: Clears the APS counters. Default: No

6.6 Management Port Configuration

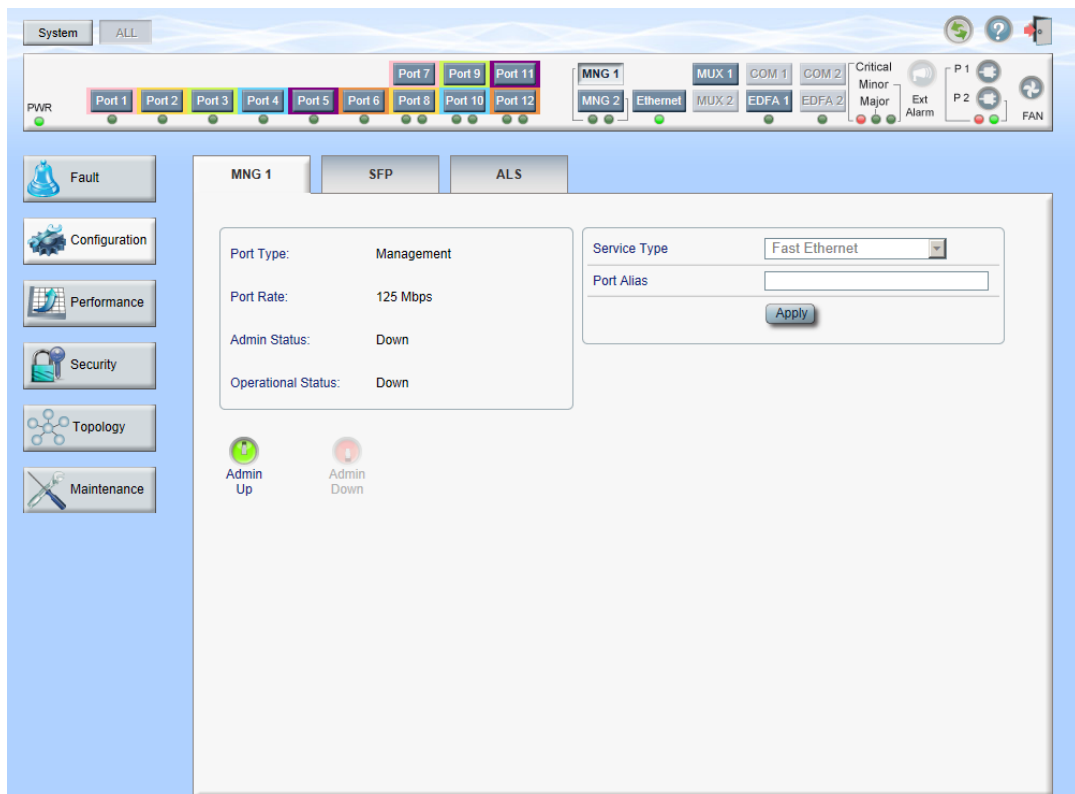


Figure 104: Management Port Configuration Window

Use the Management Port Configuration window to do the following:

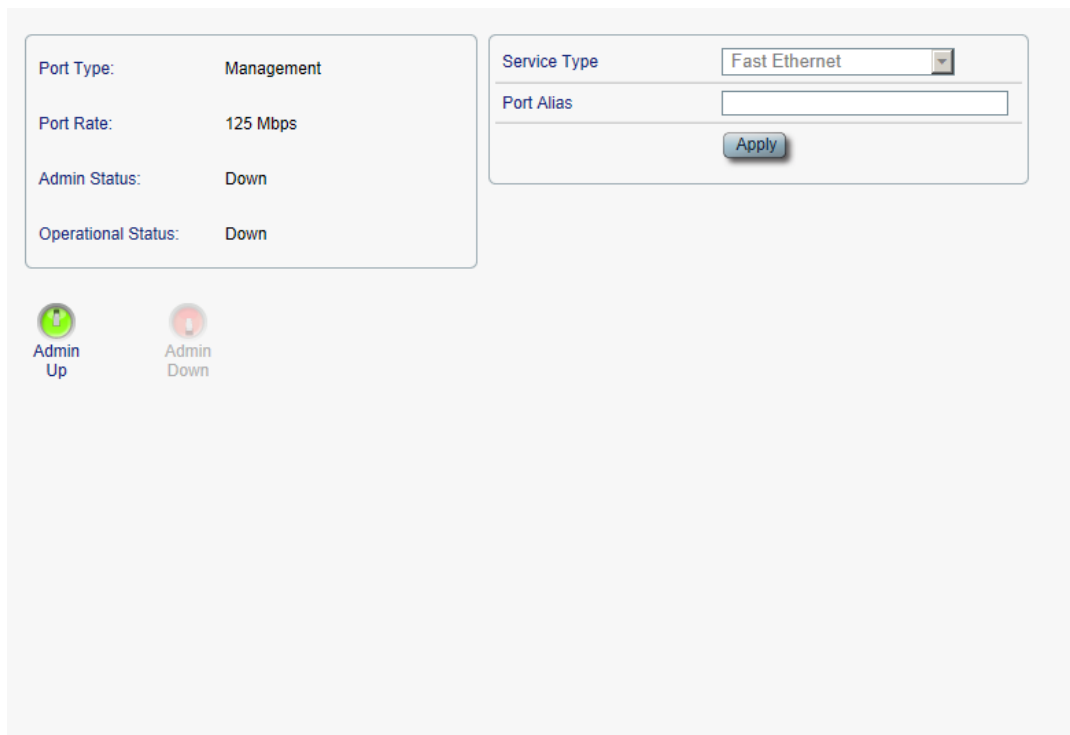
- **MNG tab:** Configure an MNG port and enable/disable the port
- **SFP tab:** Configure the SFP module
- **ALS tab:** Configure ALS for an MNG port

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.

6.6.1 MNG Tab



Port Type:	Management
Port Rate:	125 Mbps
Admin Status:	Down
Operational Status:	Down

Service Type	Fast Ethernet
Port Alias	
<input type="button" value="Apply"/>	

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.

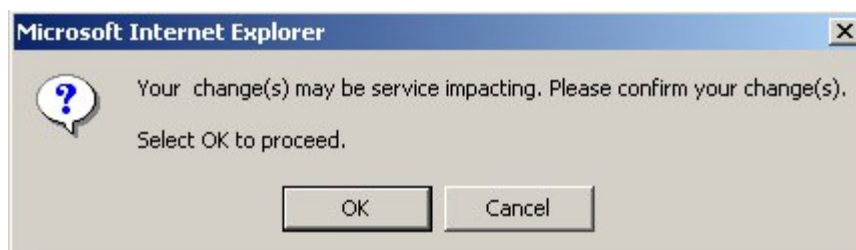


Figure 105: Confirm Changes

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.

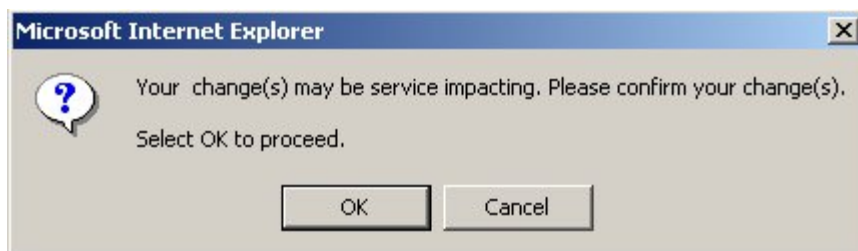


Figure 106: Confirm Changes

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.	125 Mbps
Admin Status	The administrative status of the port.	Up, Down To change the value, click Admin Up or Admin Down .
Operational Status	The operational status of the port. This indicates if there is a failure in the port.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected or Admin Down
Service Type	The management type.	Fast Ethernet (default)
Port Alias	The logical name given to the port for identification purposes.	Free text

6.6.2 SFP Tab



Figure 107: SFP Information Tab

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

To configure the SFP module:

1. Click the **SFP** tab.

The SFP tab opens displaying the SFP configuration.

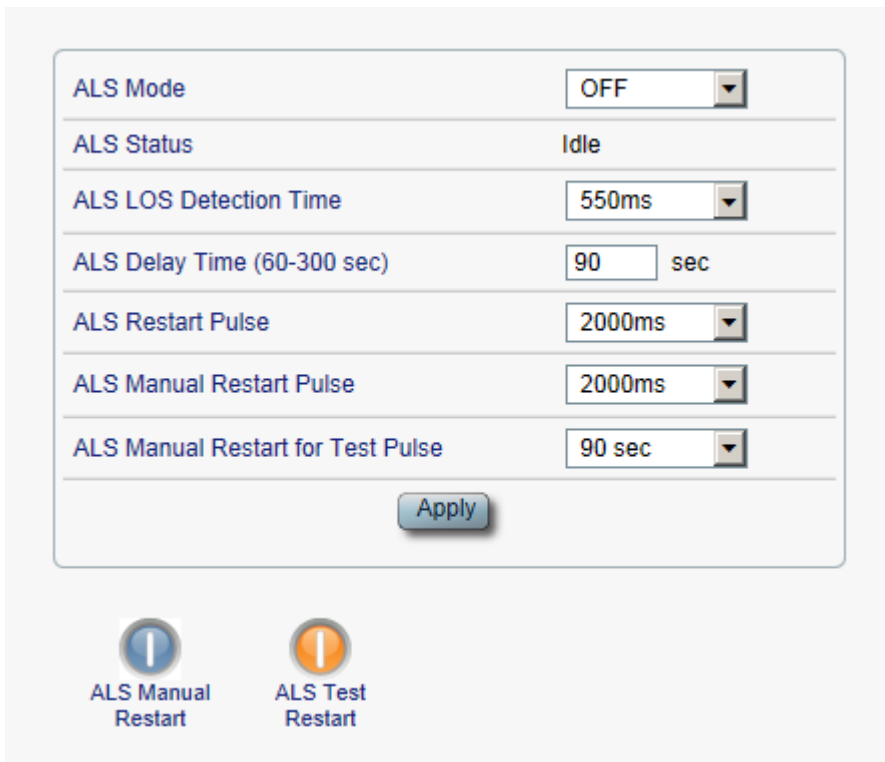
2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 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.	<ul style="list-style-type: none"> • CWDM: nm • DWDM: GHz

Parameter	Description	Format/Values
Connector Type	The type of SFP connector.	<ul style="list-style-type: none"> • Optical: LC • Electrical: RJ45
Transmitter Output Power	The measured output power of the SFP.	dBm
Receiver Input Power	The measured input power of the SFP.	dBm
Temperature	The measured temperature of the SFP.	Celsius
ESCON Capabilities	The SP capabilities of the ESCON services are marked.	
SONET/SDH Capabilities	The SFP capabilities of the OC-3, OC-12, OC-48, and OC-192 services are marked.	
Ethernet Capabilities	The SFP capabilities of the 100Mb, GbE, and 10GbE Ethernet services are marked.	
FC Capabilities	The SFP capabilities of the FC services are marked.	
High Receiver Power Default Threshold	The default threshold for the High Receiver Power alarm.	dBm
Low Receiver Power Default Threshold	The default threshold for Low Receiver Power alarm.	dBm
Override Low Receiver Power Alarm Threshold	The configured threshold for the Low Receiver Power alarm.	dBm

6.6.3 ALS Tab



ALS Mode: OFF
 ALS Status: Idle
 ALS LOS Detection Time: 550ms
 ALS Delay Time (60-300 sec): 90 sec
 ALS Restart Pulse: 2000ms
 ALS Manual Restart Pulse: 2000ms
 ALS Manual Restart for Test Pulse: 90 sec

Apply

ALS Manual Restart ALS Test Restart

Figure 108: 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-1000TN 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.

6.7 Ethernet Port Configuration



Figure 109: 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 the **Ethernet** button to select the Ethernet port.

The Ethernet Port Configuration window opens.

6.7.1 Ethernet Tab

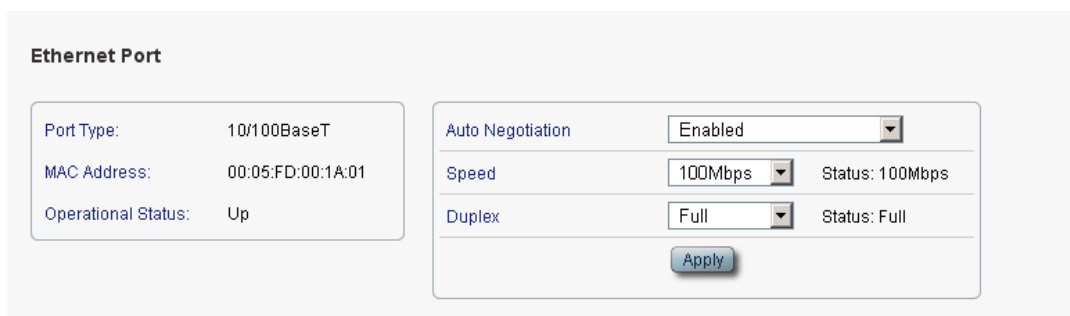


Figure 110: Ethernet Tab

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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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. <p>Default: Enabled</p> <p>NOTE: The advertised capabilities of the Ethernet port are:</p> <ul style="list-style-type: none"> ▪ 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

6.8 MUX/DEMUX Configuration

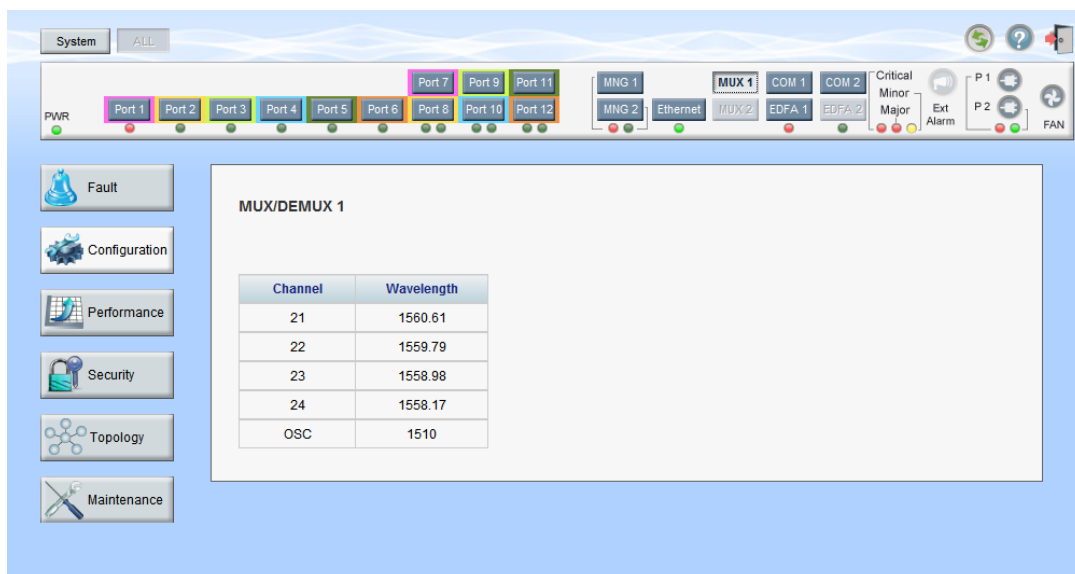


Figure 111: MUX/DEMUX Configuration Window

NOTE: The **MUX** button is enabled only if a MUX/DEMUX module is installed.

Use the MUX/DEMUX Configuration window to display the wavelengths of the WDM uplink channels.

To open the MUX/DEMUX Configuration window:

1. Click **Configuration**.
2. Click a **MUX** button to select the MUX/DEMUX module.

The appropriate MUX/DEMUX Configuration window opens.

6.8.1 MUX/DEMUX Tab



Figure 112: MUX/DEMUX Tab (DWDM)

Use the MUX/DEMUX tab to display the wavelengths of the WDM uplink channels so you can connect the LC connector to the correct WDM XFP; there are no configurable parameters.

The wavelengths of the XFPs are provided in the **XFP** tab (see [XFP Tab](#) (p. 135)).

To view the MUX/DEMUX module:

- Click a **MUX** button to select the MUX/DEMUX module.

The MUX/DEMUX tab opens displaying the MUX/DEMUX module configuration. The fields are read only and explained in the following table.

Table 57: MUX/DEMUX Tab Parameters

Parameter	Description	Format/Values
Channel	The ITU channel number supported by the MUX/DEMUX.	<ul style="list-style-type: none"> • CWDM: CWDM, OSC • DWDM: Channel number, OSC
Wavelength	The corresponding channel wavelength.	

6.9 EDFA Configuration

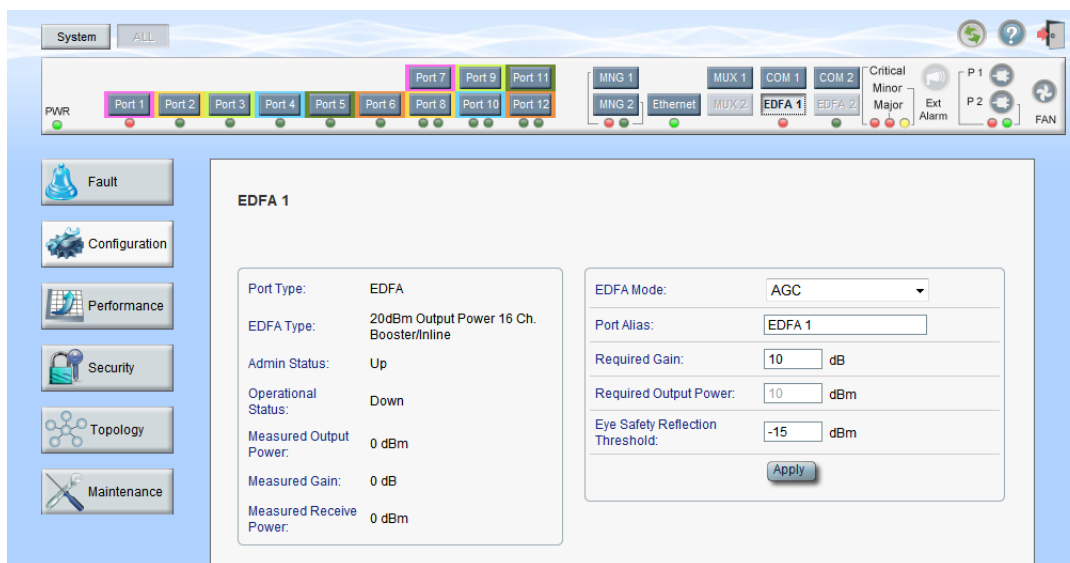


Figure 113: EDFA Configuration Window

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

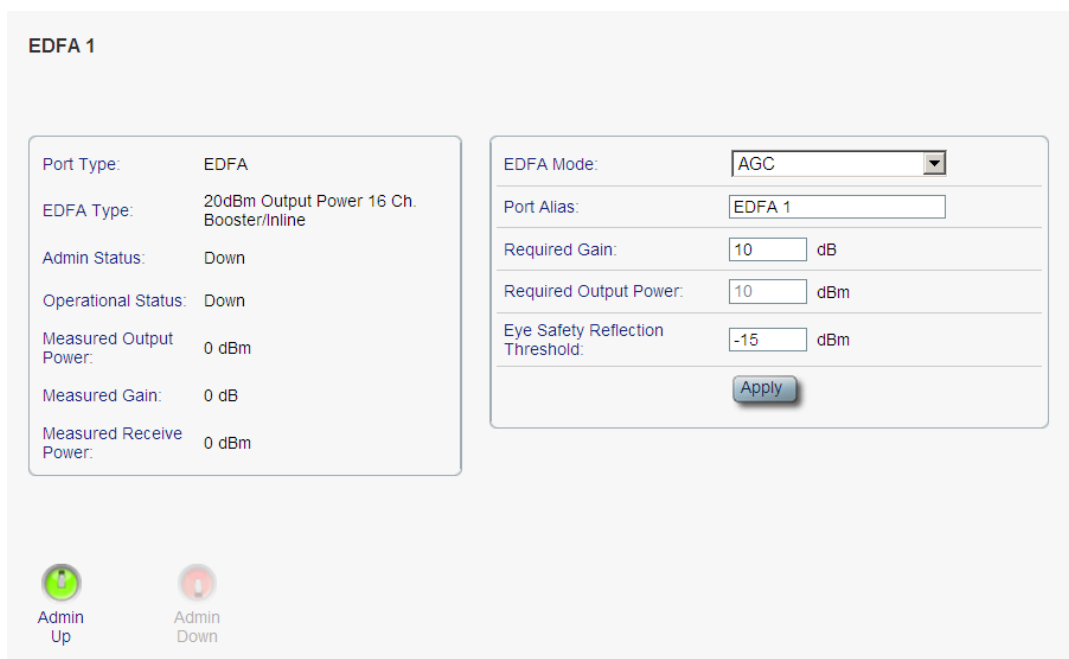
Use the EDFA Configuration window to configure the EDFA module and enable/disable the module.

To open the EDFA Configuration window:

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

The appropriate EDFA Configuration window opens.

6.9.1 EDFA Tab



EDFA 1

Port Type:	EDFA	EDFA Mode:	AGC
EDFA Type:	20dBm Output Power 16 Ch. Booster/Inline	Port Alias:	EDFA 1
Admin Status:	Down	Required Gain:	10 dB
Operational Status:	Down	Required Output Power:	10 dBm
Measured Output Power:	0 dBm	Eye Safety Reflection Threshold:	-15 dBm
Measured Gain:	0 dB	<input type="button" value="Apply"/>	
Measured Receive Power:	0 dBm		

Figure 114: 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.

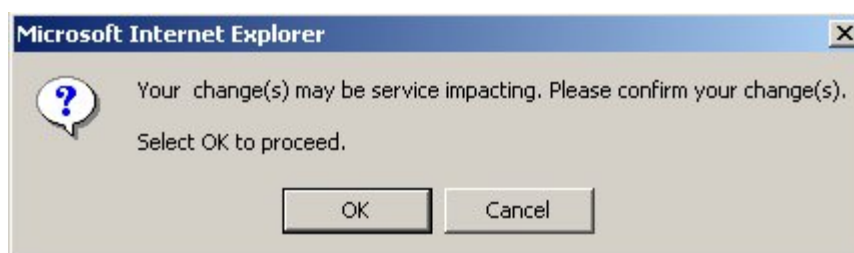


Figure 115: Confirm Changes

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.

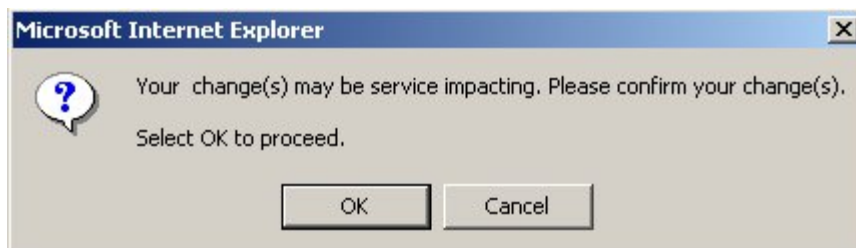


Figure 116: Confirm Changes

2. Click **OK**.

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

Table 58: 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: <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected or Admin Down
Measured Output Power	The current measured optical power of the EDFA.	dBm
Measured Gain	The current measured gain of the EDFA.	dB
Measured Receive Power	The current measured receive power of the EDFA.	dBm
EDFA Mode	Selected amplification mode.	<ul style="list-style-type: none"> • AGC: Gain remains constant. • APC: Output power remains constant. <p>NOTE:</p> <ul style="list-style-type: none"> ▪ 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 COM Port Configuration

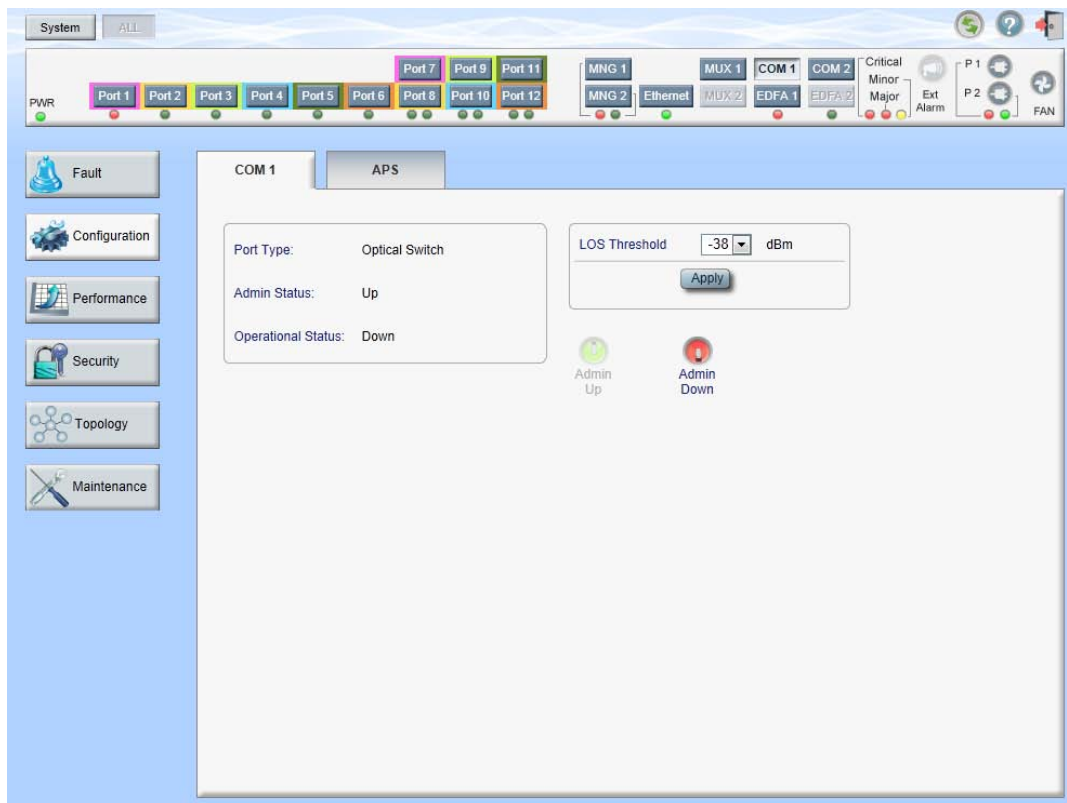


Figure 117: COM Port Configuration Window

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

Use the COM Port Configuration window to do the following:

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

To open the COM Port Configuration window:

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

The appropriate COM Port Configuration window opens.

6.10.1 COM Tab

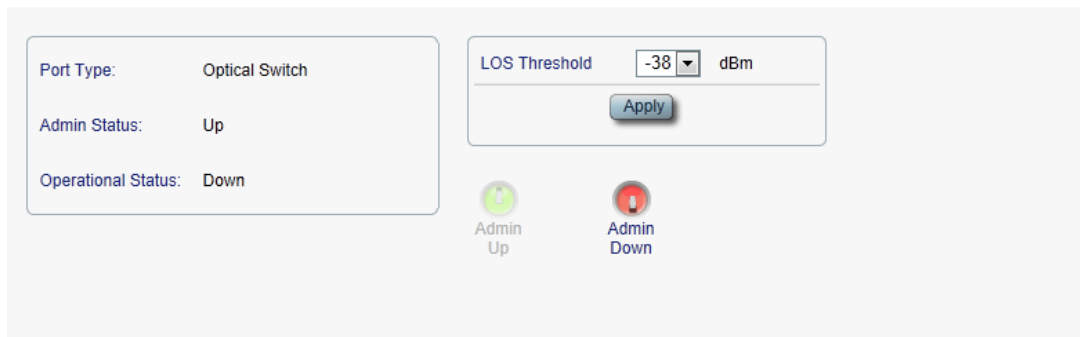



Figure 118: COM Tab

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

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

To configure a COM port:

1. Click the **COM** tab.

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

The following confirmation message appears.



Figure 119: 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 120: Confirm Changes

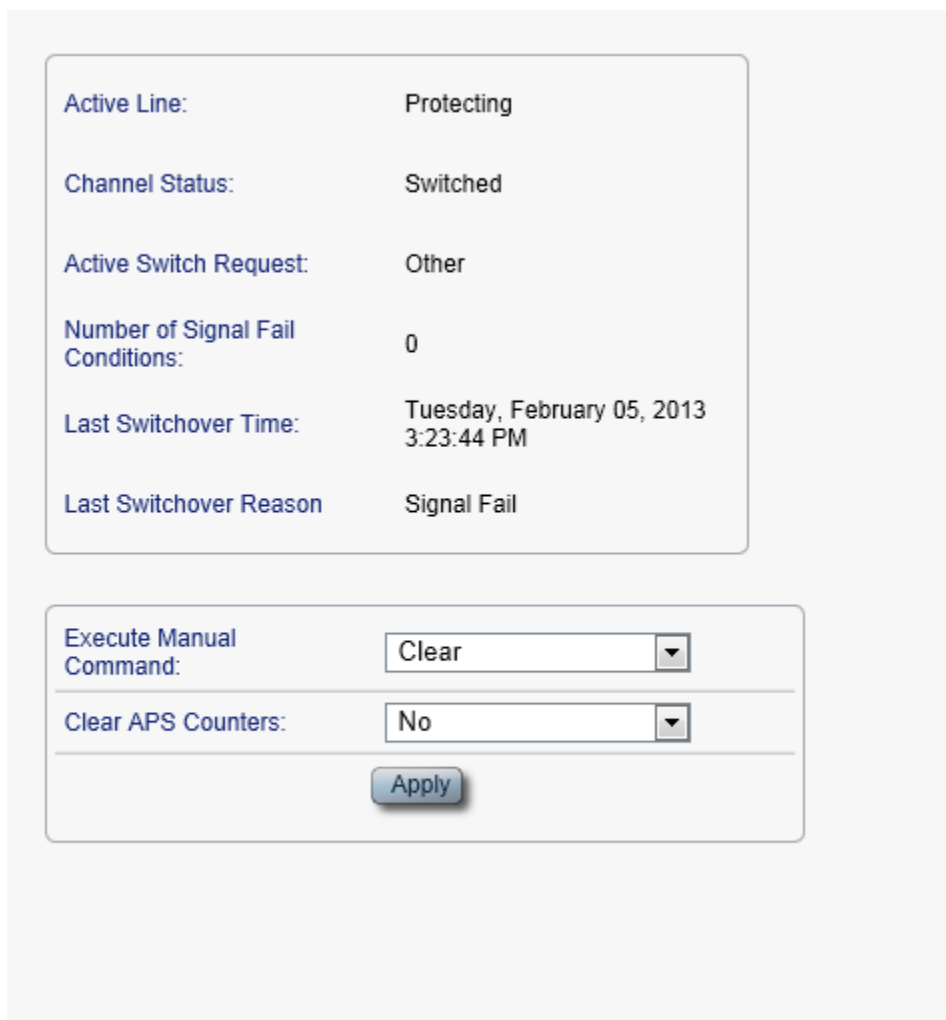
2. Click **OK**.

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

Table 59: COM Tab Parameters

Parameter	Description	Format/Values
Port Type	The type of port.	Optical Switch
Admin Status	The administrative status of the port.	Up, Down To change the value, click Admin Up or Admin Down .
Operational Status	The operational status of the port. This indicates if there is a failure in the port.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected or Admin Down
LOS Threshold	The LOS detection threshold used for optical switching.	-40 to -25 dBm Default: -38 dBm

6.10.2 APS Tab



Active Line:	Protecting
Channel Status:	Switched
Active Switch Request:	Other
Number of Signal Fail Conditions:	0
Last Switchover Time:	Tuesday, February 05, 2013 3:23:44 PM
Last Switchover Reason:	Signal Fail

Execute Manual Command:	Clear
Clear APS Counters:	No
<input type="button" value="Apply"/>	

Figure 121: APS Tab

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

To configure APS parameters:

1. Click the **APS** tab.
The APS tab opens.
2. Fill in the fields as explained in the following table.
3. Click **Apply**.

Table 60: APS Tab Parameters

Parameter	Description	Format/Values
Active Line	The current active uplink.	Working, Protecting
Channel Status	The current APS channel status.	Any combination of the following values: <ul style="list-style-type: none"> • Signal Fail on Working • Signal Fail on Protecting • Switched (to Protecting)

Parameter	Description	Format/Values
Active Switch Request	The switch request currently in effect.	<ul style="list-style-type: none"> Manual Command Signal Fail Force Switch Other
Number of Signal Fail Conditions	The number of times the Signal Fail condition occurred.	Integer
Last Switchover Time	The time of the last switchover event.	Date and time
Last Switchover Reason	The reason for the last switchover.	<ul style="list-style-type: none"> Manual Command Signal Fail Force Switch Other
Execute Manual Command	The manual APS commands.	<ul style="list-style-type: none"> Clear: Clears the last APS switch command. Force Switch to Protecting: Forces switch to Protecting in any condition. Force Switch to Working: Forces switch to Working in any condition. Manual Switch to Protecting: Switches to Protecting only if the protecting uplink is functioning properly. Manual Switch to Working: Switches to Working only if the working uplink is functioning properly. Default: Clear
Clear APS Counters	Whether or not to clear the APS counters.	<ul style="list-style-type: none"> No: Does not clear the APS counters. Yes: Clears the APS counters. Default: No

6.11 PSU Configuration

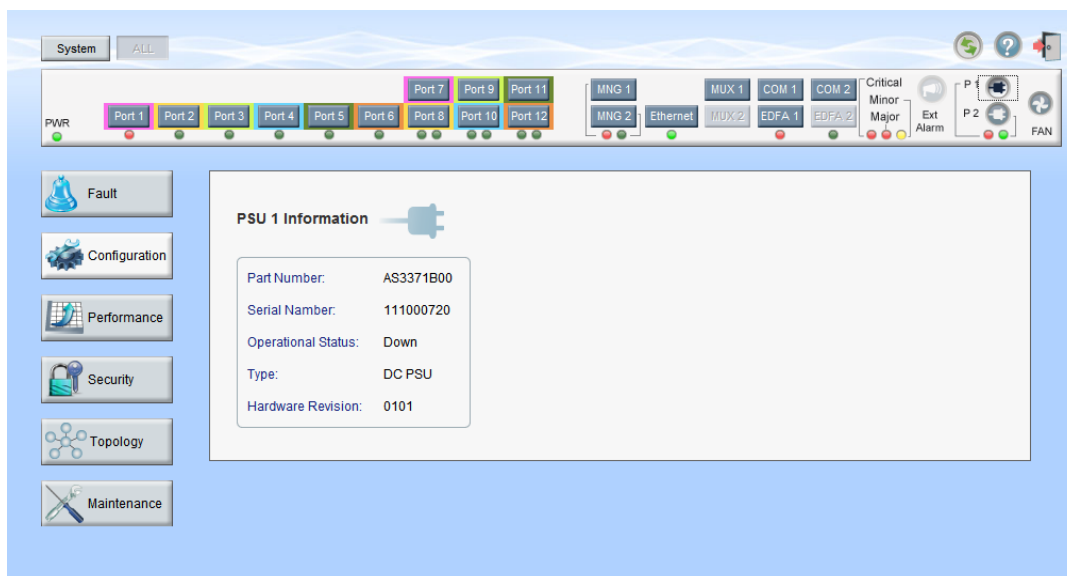



Figure 122: PSU Configuration Window

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

To open the PSU Configuration window:

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

The appropriate PSU Configuration window opens.

6.11.1 PSU Tab

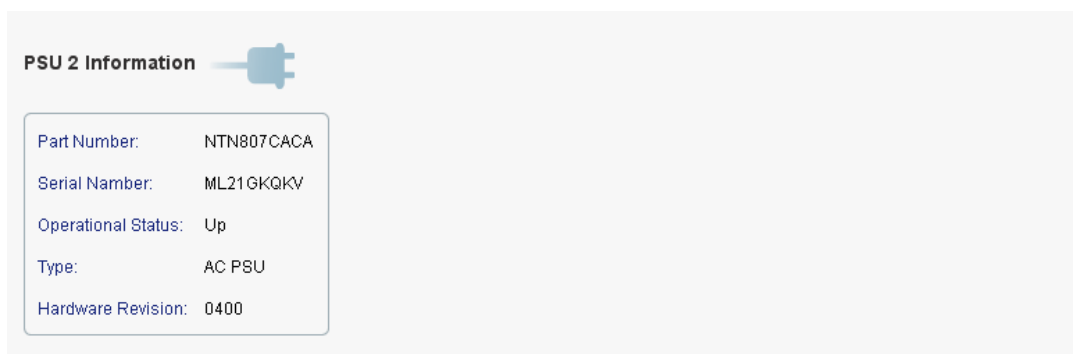



Figure 123: PSU Tab

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

To view PSU information:

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

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

Table 61: PSU Tab Parameters

Parameter	Description	Format/Values
Part Number	The part number of the power supply unit.	Part number
Serial Number	The serial number of the power supply unit.	Serial number
Operational Status	The operational status of the power supply unit. This indicates if there is a failure in the power supply unit.	<ul style="list-style-type: none"> • Up: Normal operation • Down: Alarm is detected
Type	The type of power supply unit.	AC PSU, DC PSU
Hardware Revision	The hardware version of the power supply unit.	dddd

6.12 FAN Unit Configuration

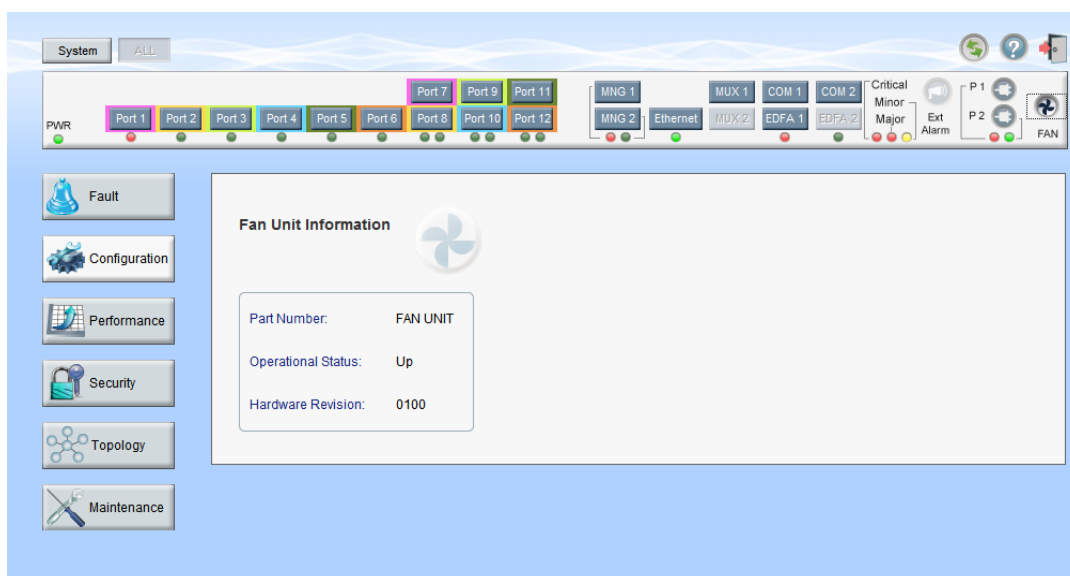



Figure 124: FAN Unit Configuration Window

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 the **FAN**  button to select the FAN unit.

The FAN Unit Configuration window opens.

6.12.1 FAN Unit Tab

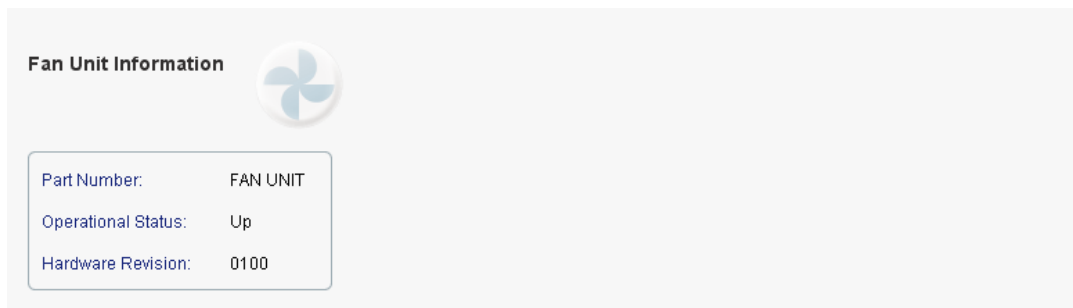


Figure 125: FAN Unit Tab

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

To view the FAN unit information:

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

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

Table 62: 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.	<ul style="list-style-type: none"> • 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-1000TN system optical information and port performance monitoring.

In this Chapter

- Optical Information 175
- Port Performance Monitoring 177
- Uplink Performance Monitoring 178
- Service Performance Monitoring 185
- Management Port Performance Monitoring 192
- EDFA Performance Monitoring 196

7.1 Optical Information

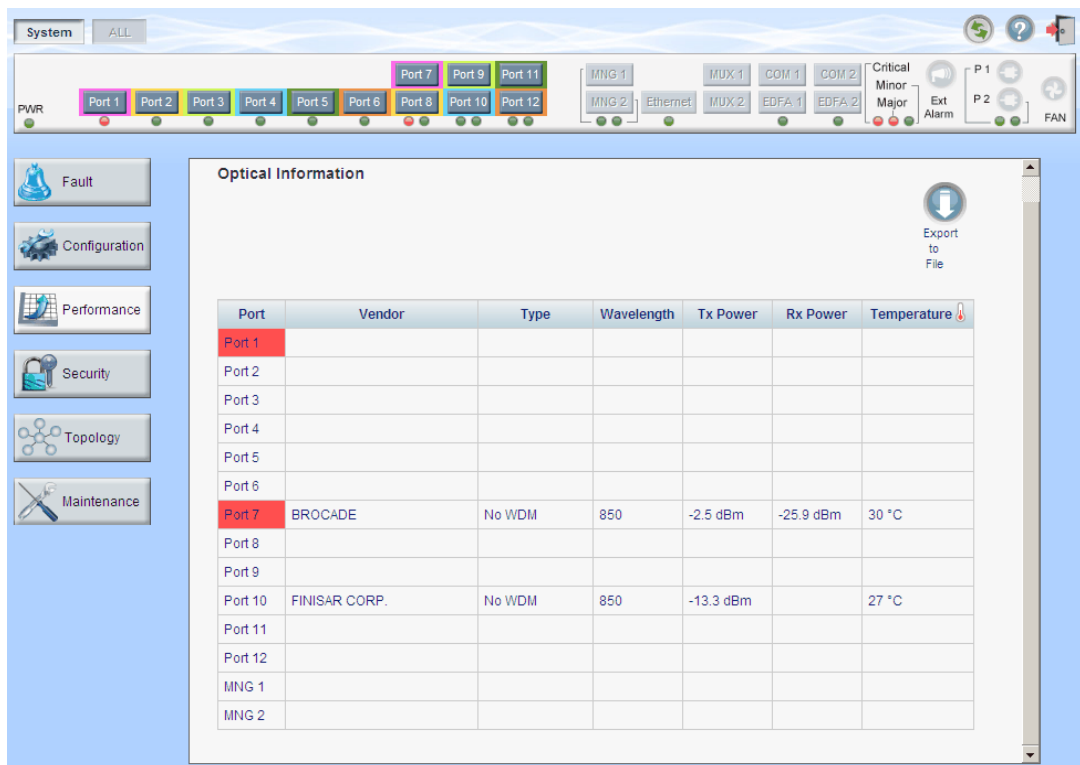


Figure 126: Optical Information Window


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

To open the System Optical Information window:

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

The Optical Information window opens.

7.1.1 Optical Information Tab

Optical Information 
Export to File


Port	Vendor	Type	Wavelength	Tx Power	Rx Power	Temperature 
Port 1						
Port 2						
Port 3						
Port 4						
Port 5						
Port 6						
Port 7	BROCADE	No WDM	850	-2.5 dBm	-25.9 dBm	30 °C
Port 8						
Port 9						
Port 10	FINISAR CORP.	No WDM	850	-13.3 dBm		27 °C
Port 11						
Port 12						
MNG 1						
MNG 2						

Figure 127: Optical Information Tab

Use the Optical Information tab to view system optical information.

To view the optical information tab:

1. Click **System**.

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

2. To export the optical information to a file:

1. Click **Export to File** .

The Opening table.csv dialog box appears.

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

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

The information is updated immediately.

Table 63: 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: <ul style="list-style-type: none"> ▪ 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.

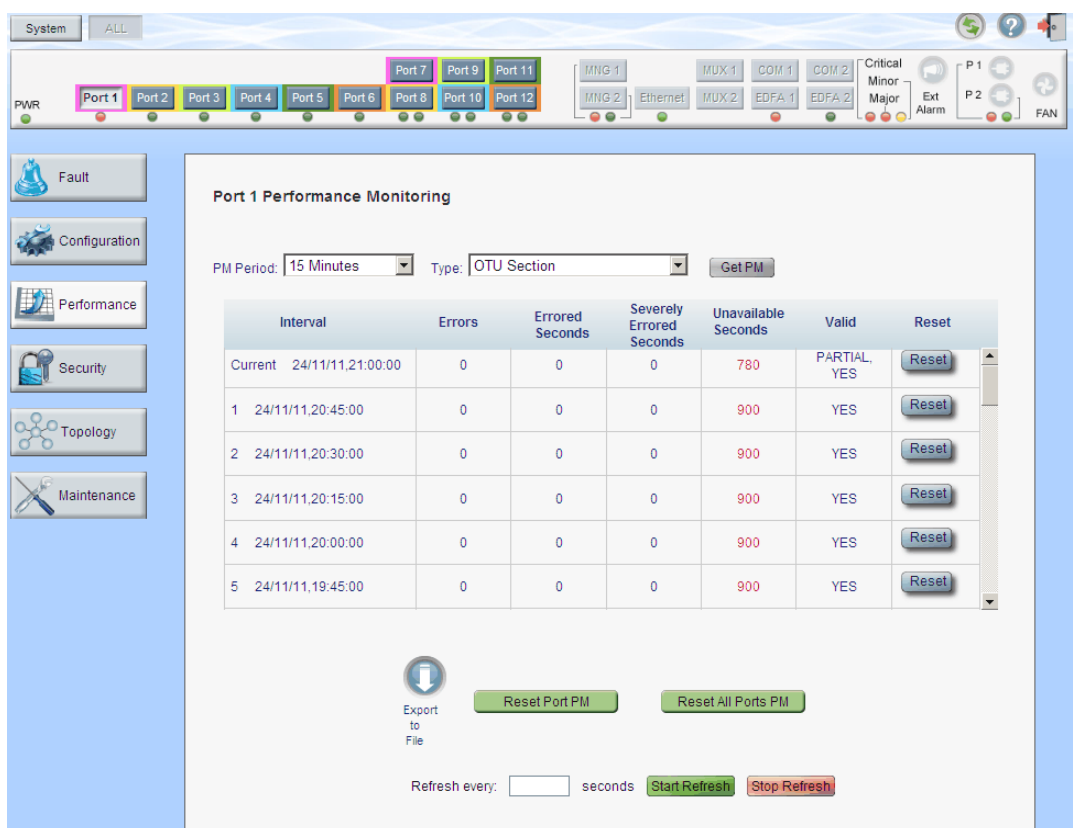
7.2 Port Performance Monitoring

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

- Uplink ports (Port 1 - Port 6). OTN PM counters are provided for following:
 - **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 the 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.
- Service ports (Port 7 - Port 12). Native Signal PM for all ports according to the following service types:
 - **8G FC services:** PM counters are based on 8B/10 coding violation errors.
 - **10G FC services:** PM counters are based on 64B/66B coding violation errors.
 - **10GBE-LAN services:** PM counters are based on 64B/66B coding violation errors.
 - **OC-192/STM-64 (SONET/SDH) services:** PM counters are based on Section B1 errors.

- Optical Level PM. This is based on the measured Rx power:
 - Uplink ports (Port 1 - Port 6)
 - Service ports (Port 7 - Port 12)
 - MNG 1 - MNG 2
 - EDFA 1 - EDFA 2 (if present)

7.3 Uplink Performance Monitoring



Port 1 Performance Monitoring

PM Period: 15 Minutes Type: OTU Section

Interval	Errors	Errored Seconds	Severely Errored Seconds	Unavailable Seconds	Valid	Reset
Current 24/11/11,21:00:00	0	0	0	780	PARTIAL YES	<input type="button" value="Reset"/>
1 24/11/11,20:45:00	0	0	0	900	YES	<input type="button" value="Reset"/>
2 24/11/11,20:30:00	0	0	0	900	YES	<input type="button" value="Reset"/>
3 24/11/11,20:15:00	0	0	0	900	YES	<input type="button" value="Reset"/>
4 24/11/11,20:00:00	0	0	0	900	YES	<input type="button" value="Reset"/>
5 24/11/11,19:45:00	0	0	0	900	YES	<input type="button" value="Reset"/>

Refresh every: seconds

Figure 128: 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 a **Port** button (Port 1-6) to select the uplink port.

The appropriate Uplink Port Performance Monitoring window opens.

7.3.1 Viewing Uplink Port Performance Monitoring

Port 1 Performance Monitoring

PM Period: Type:

Interval	Errors	Errored Seconds	Severely Errored Seconds	Unavailable Seconds	Valid	Reset
Current 24/11/11,21:00:00	0	0	0	780	PARTIAL, YES	<input type="button" value="Reset"/>
1 24/11/11,20:45:00	0	0	0	900	YES	<input type="button" value="Reset"/>
2 24/11/11,20:30:00	0	0	0	900	YES	<input type="button" value="Reset"/>
3 24/11/11,20:15:00	0	0	0	900	YES	<input type="button" value="Reset"/>
4 24/11/11,20:00:00	0	0	0	900	YES	<input type="button" value="Reset"/>
5 24/11/11,19:45:00	0	0	0	900	YES	<input type="button" value="Reset"/>

Refresh every: seconds


Figure 129: Uplink Port Performance Monitoring Tab

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

To view uplink port performance monitoring:

- Click a **Port** button (Port 1-6) to select the uplink port.

The appropriate Uplink Port Performance Monitoring tab opens displaying the uplink port performance monitoring.
- From the **PM Period** drop-down list, select **15 Minutes** or **Days**.
- From the **Type** drop-down list, select the type of performance monitoring.
- Click **Get PM**.

The performance monitoring counters are updated. The counters are read only.
- To export the PM information to a file:
 - Click **Export to File**  .

The Opening table.csv dialog box appears.
 - Click **Save File**.
 - 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 64: Uplink Port Performance Monitoring Tab Parameters

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.	<ul style="list-style-type: none"> • OTU Section • OTU Far Section • ODU Path • ODU Far Path • OTN FEC Corrected Errors • OTN FEC Uncorrected Errors

Parameter	Description	Format/Values
Interval	The date and time of the interval.	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • OTU Section and OTU Far Section: The number of Section BIP-8 errors detected during the performance monitoring interval. • ODU Path and ODU Far Path: The number of 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: <ul style="list-style-type: none"> ▪ 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 and OTN FEC Uncorrected Errors.
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 and OTN FEC Uncorrected Errors .
Valid	Whether or not the performance monitoring interval has been completed, and whether or not the information is accurate.	<ul style="list-style-type: none"> • 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. <p>The performance monitoring information may be inaccurate due to one of the following reasons:</p> <ul style="list-style-type: none"> ▪ 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.

7.3.2 Viewing Optical Level Performance Monitoring

Port 1 Performance Monitoring

PM Period: Type:

Interval	Rx Level dBm
Current 05/02/13,19:00:00	NA
1 05/02/13,18:45:00	NA
2 05/02/13,18:30:00	NA
3 05/02/13,18:15:00	NA
4 05/02/13,18:00:00	NA
5 05/02/13,17:45:00	NA
6 05/02/13,17:30:00	NA
7 05/02/13,17:15:00	NA
8 05/02/13,17:00:00	NA
9 05/02/13,16:45:00	NA

Refresh every: seconds

Figure 130: 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 an **Uplink** button 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**.


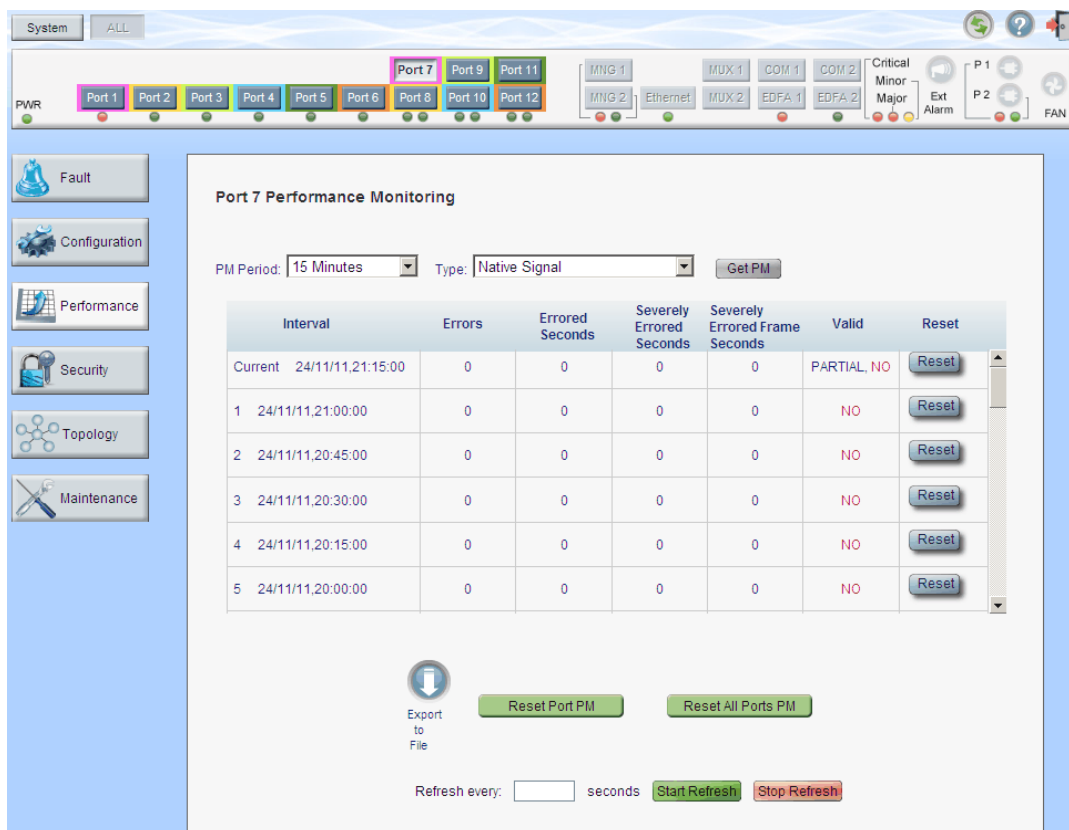
6. To set the refresh rate of the PM display:
 1. In the **Refresh every** field, type the number of seconds that the window should refresh.
The minimum refresh rate is 2 seconds.
 2. Click **Start Refresh**.
The information is automatically updated after the specified number of seconds.
7. To refresh 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 65: 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.	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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).	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> 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 Performance Monitoring



Port 7 Performance Monitoring

PM Period: 15 Minutes Type: Native Signal Get PM

Interval	Errors	Errored Seconds	Severely Errored Seconds	Severely Errored Frame Seconds	Valid	Reset
Current 24/11/11,21:15:00	0	0	0	0	PARTIAL, NO	Reset
1 24/11/11,21:00:00	0	0	0	0	NO	Reset
2 24/11/11,20:45:00	0	0	0	0	NO	Reset
3 24/11/11,20:30:00	0	0	0	0	NO	Reset
4 24/11/11,20:15:00	0	0	0	0	NO	Reset
5 24/11/11,20:00:00	0	0	0	0	NO	Reset

Export to File Reset Port PM Reset All Ports PM

Refresh every: seconds Start Refresh Stop Refresh

Figure 131: Service Port Performance Monitoring Window

Use the Service Port Performance Monitoring window to view Layer 1 service port performance monitoring.

To open the Service Port Performance Monitoring window:

1. Click **Performance**.
2. Click a **Port** button (Port 7-12) to select the service port.

The appropriate Service Port Performance Monitoring window opens.

7.4.1 Viewing Native Signal Performance Monitoring

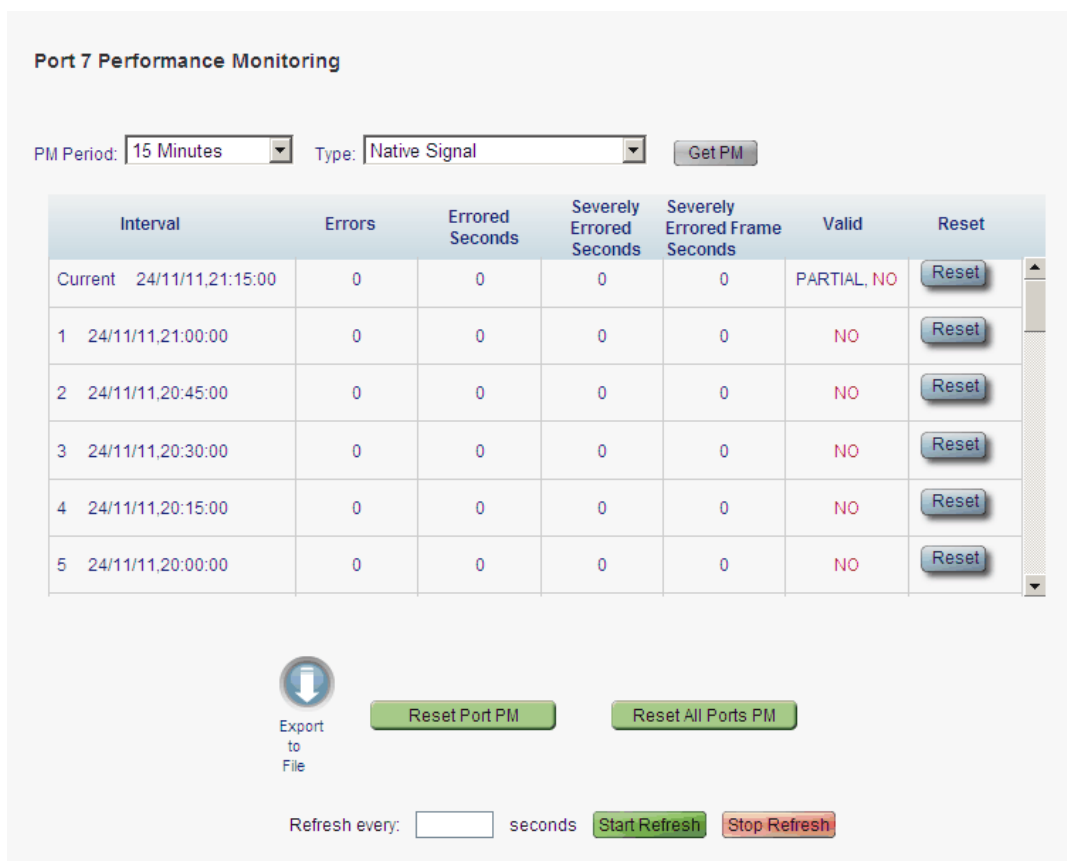


Figure 132: Service Port Performance Monitoring Tab

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

To view service port performance monitoring:

1. Click a **Port** button (Port 7-12) to select the service port.

The appropriate Service Port Performance Monitoring tab opens displaying the displaying the service port performance monitoring.

2. From the **PM Period** drop-down list, select **15 Minutes** or **Days**.
3. Click **Get PM**.

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



4. 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**.
5. 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.
6. To refresh the PM display manually, click **Refresh**  .
The information is updated immediately.
7. To stop the automatic refresh of the PM display, click **Stop Refresh**.
The automatic refresh is stopped and the **Refresh every** field is cleared.
8. To clear the PM counters for a specific PM interval, in the table, at the end of the interval row, click **Reset**.
9. To clear PM counters for a specific port, click **Reset Port PM**.
10. To clear PM counters for all ports, click **Reset All Ports PM**.

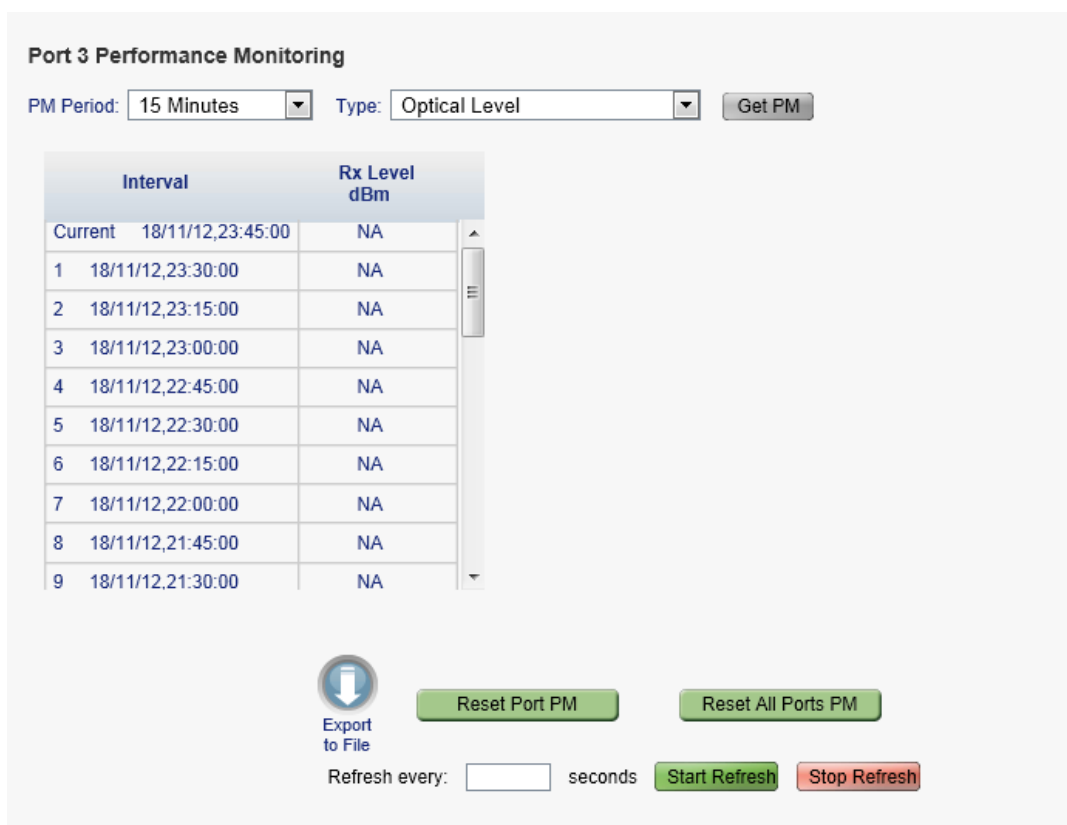
Table 66: Service Port Performance Monitoring Tab Parameters

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

Parameter	Description	Format/Values
Interval	The date and time of the interval.	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Background Block Errors (SDH) <i>or</i> • Errors (Other) 	<ul style="list-style-type: none"> • 8G FC services: The number of 8B/10B coding violation errors detected during the performance monitoring interval. • 10G FC and 10GbE-LAN services: The number of 64B/66 coding violation errors detected during the performance monitoring interval. • SONET/SDH services: The number of Section B1 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.
<ul style="list-style-type: none"> • Severely Errored Frame Seconds (SONET) <i>or</i> • Out of Frame Seconds (SDH) <i>or</i> • Unavailable Seconds (Other) 	<ul style="list-style-type: none"> • 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
Valid	Whether or not the performance monitoring interval has been completed, and whether or not the information is accurate.	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ▪ 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 Optical Level Performance Monitoring



Port 3 Performance Monitoring

PM Period: Type:

	Interval	Rx Level dBm
Current	18/11/12,23:45:00	NA
1	18/11/12,23:30:00	NA
2	18/11/12,23:15:00	NA
3	18/11/12,23:00:00	NA
4	18/11/12,22:45:00	NA
5	18/11/12,22:30:00	NA
6	18/11/12,22:15:00	NA
7	18/11/12,22:00:00	NA
8	18/11/12,21:45:00	NA
9	18/11/12,21:30:00	NA

Refresh every: seconds

Figure 133: 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 a **Port** button (Port 7-12) 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 67: 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.	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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).	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> 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

The screenshot displays the 'Management Port 1 Performance Monitoring' window. At the top, there are navigation tabs for System, ALL, and various ports (Port 1-12). Below the navigation, there are status indicators for MNG 1, MNG 2, Ethernet, MUX 1, MUX 2, COM 1, COM 2, EDFA 1, EDFA 2, and other components. The main content area shows a table with the following data:

Interval	Rx Level dBm
Current 06/02/13, 18:30:00	NA
1 06/02/13, 18:15:00	NA
2 06/02/13, 18:00:00	NA
3 06/02/13, 17:45:00	NA
4 06/02/13, 17:30:00	NA
5 06/02/13, 17:15:00	NA
6 06/02/13, 17:00:00	NA
7 06/02/13, 16:45:00	NA
8 06/02/13, 16:30:00	NA
9 06/02/13, 16:15:00	NA

Below the table, there are buttons for 'Export to File', 'Reset Port PM', 'Reset All Ports PM', and a 'Refresh every' field with 'Start Refresh' and 'Stop Refresh' buttons.

Figure 134: 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 Optical Performance Monitoring

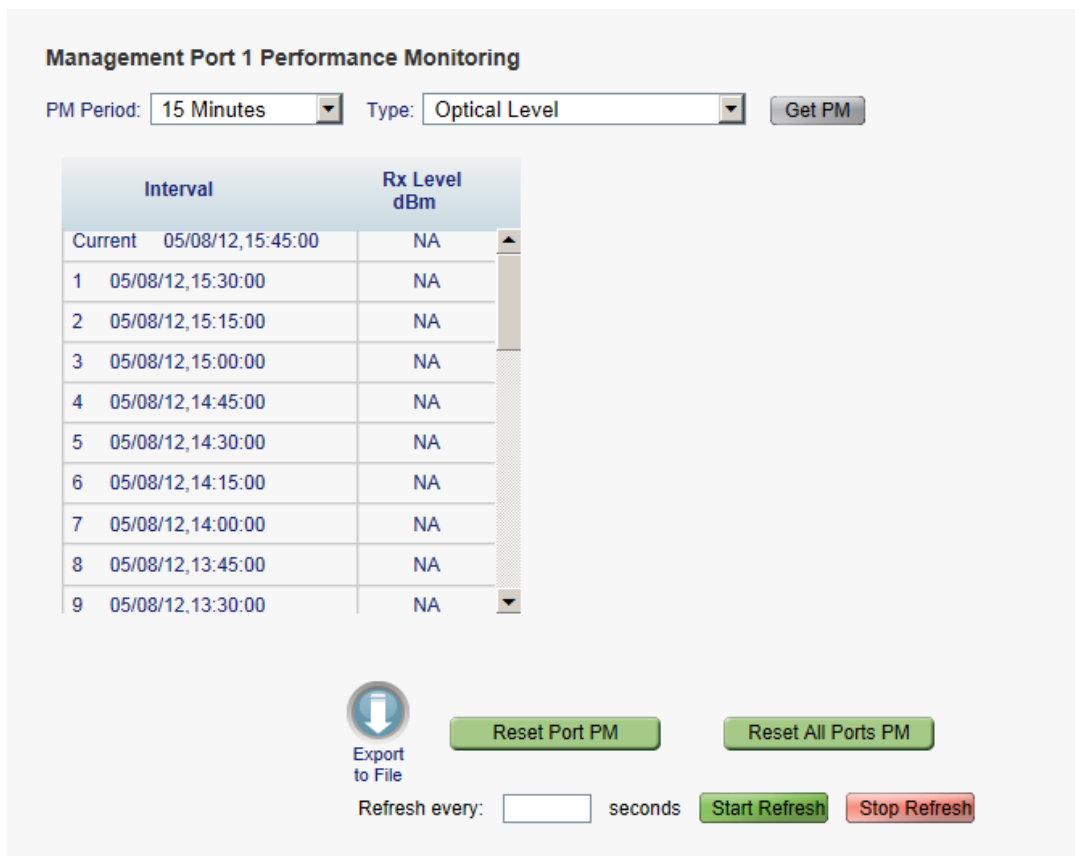


Figure 135: Optical Level Performance Monitoring

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.



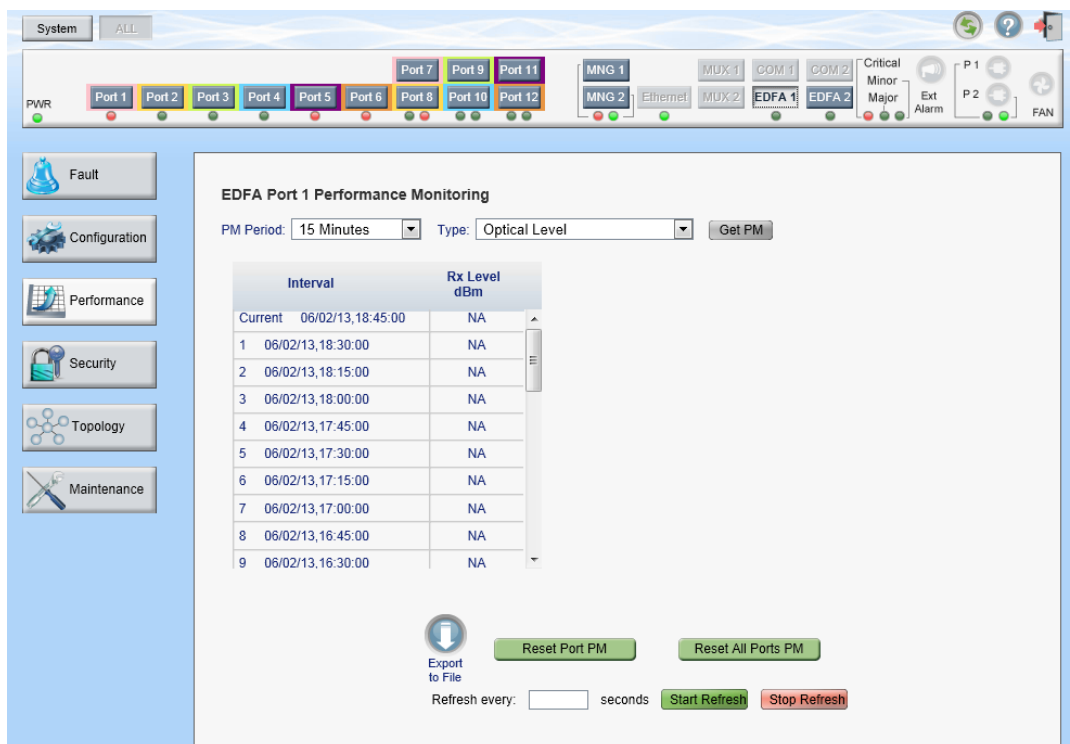
5. To export the optical level information to a file:
 1. Click **Export to File**  .
The Opening table.csv dialog box appears.
 2. Click **Save File**.
 3. Click **OK**.
6. To set the refresh rate of the PM display:
 1. In the **Refresh every** field, type the number of seconds that the window should 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 68: 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

Parameter	Description	Format/Values
Interval	The date and time of the interval.	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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).	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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



EDFA Port 1 Performance Monitoring

PM Period: 15 Minutes Type: Optical Level

	Interval	Rx Level dBm
Current	06/02/13, 18:45:00	NA
1	06/02/13, 18:30:00	NA
2	06/02/13, 18:15:00	NA
3	06/02/13, 18:00:00	NA
4	06/02/13, 17:45:00	NA
5	06/02/13, 17:30:00	NA
6	06/02/13, 17:15:00	NA
7	06/02/13, 17:00:00	NA
8	06/02/13, 16:45:00	NA
9	06/02/13, 16:30:00	NA

Refresh every: seconds

Figure 136: 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 an **EDFA** button to select the EDFA module.

The appropriate EDFA Performance Monitoring window opens.

7.6.1 Viewing Optical Performance Monitoring

EDFA Port 1 Performance Monitoring

PM Period: Type:

Interval	Rx Level dBm
Current 05/08/12,16:30:00	NA
1 05/08/12,16:15:00	NA
2 05/08/12,16:00:00	NA
3 05/08/12,15:45:00	NA
4 05/08/12,15:30:00	NA
5 05/08/12,15:15:00	NA
6 05/08/12,15:00:00	NA
7 05/08/12,14:45:00	NA
8 05/08/12,14:30:00	NA
9 05/08/12,14:15:00	NA

Refresh every: seconds

Figure 137: Optical Level Performance Monitoring

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

To view optical level performance monitoring:

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

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

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

The optical level counters are updated.

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

1. Click **Export to File**  .

The Opening table.csv dialog box appears.

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


6. To set the refresh rate of the PM display:
 1. In the **Refresh every** field, type the number of seconds that the window should refresh.
The minimum refresh rate is 2 seconds.
 2. Click **Start Refresh**.
The information is automatically updated after the specified number of seconds.
7. To refresh the PM display manually, click **Refresh** .
The information is updated immediately.
8. To stop the automatic refresh of the PM display, click **Stop Refresh**.
The automatic refresh is stopped and the **Refresh every** field is cleared.
9. To clear the optical level counters for a specific port, click **Reset Port PM**.
10. To clear the optical level counters for all ports, click **Reset All Ports PM**.

Table 69: EDFA Optical Level PM Parameters

Parameter	Description	Format/Values
PM Period	The interval for averaging the measured Rx power.	15 Minutes, Days
Type	The type of performance monitoring.	Optical Level
Interval	The date and time of the interval.	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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).	<p>PM Period is set to 15 Minutes:</p> <ul style="list-style-type: none"> • 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. <p>PM Period is set to Days:</p> <ul style="list-style-type: none"> • 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-1000TN.

In this Chapter

System Maintenance	201
Diagnostic Tests	210
Uplink Port Maintenance	212
Service Port Maintenance.....	214
External Alarm Maintenance.....	216

8.1 System Maintenance

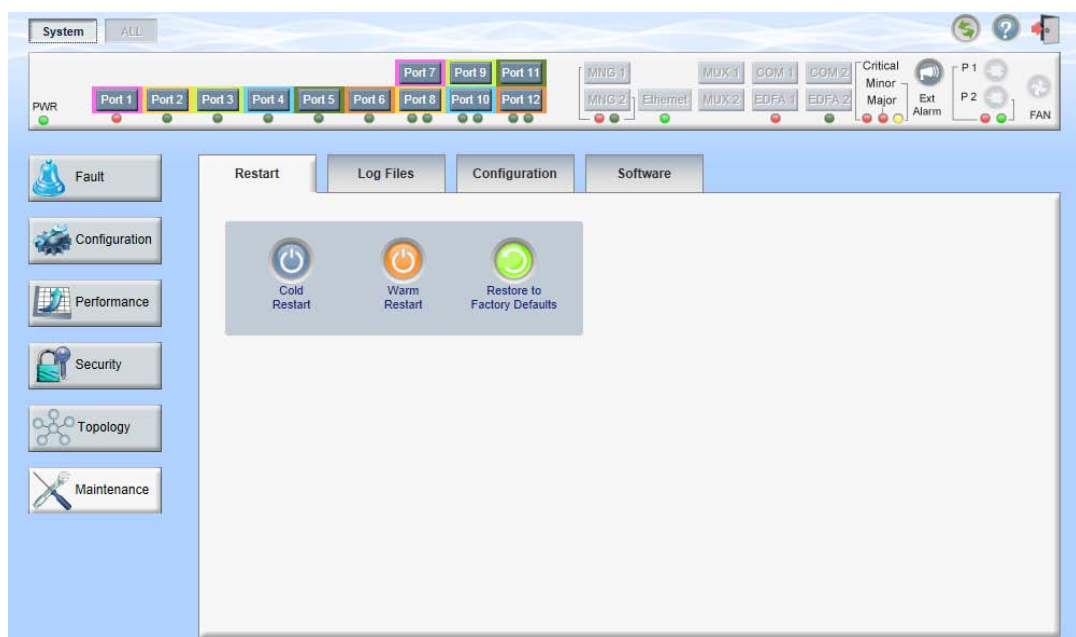


Figure 138: System Maintenance Window

Use the System Maintenance window to do the following:

- **Restart tab:** Restart the PL-1000TN 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 139: Restart Tab

Use the Restart tab to do the following:

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

NOTE: If you restore to the factory default configuration:

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

To restart the PL-1000TN 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 140: 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.

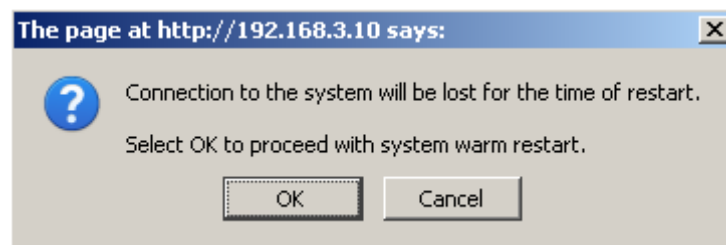


Figure 141: Confirm Changes

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 142: 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

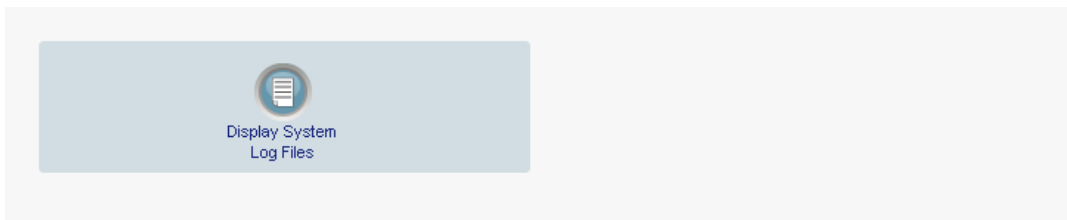


Figure 143: Log Files Tab

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.



Figure 144: System Log Files (Example)

8.1.3 Configuration Tab

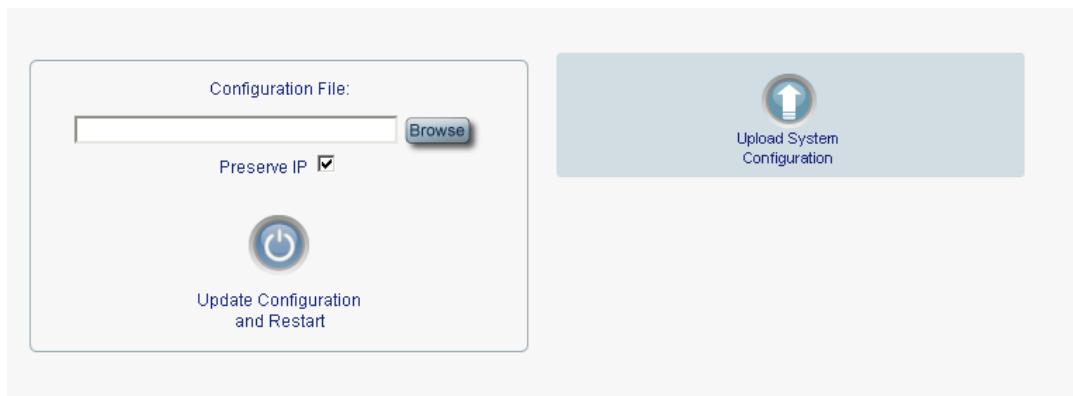



Figure 145: Configuration Tab

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

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

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

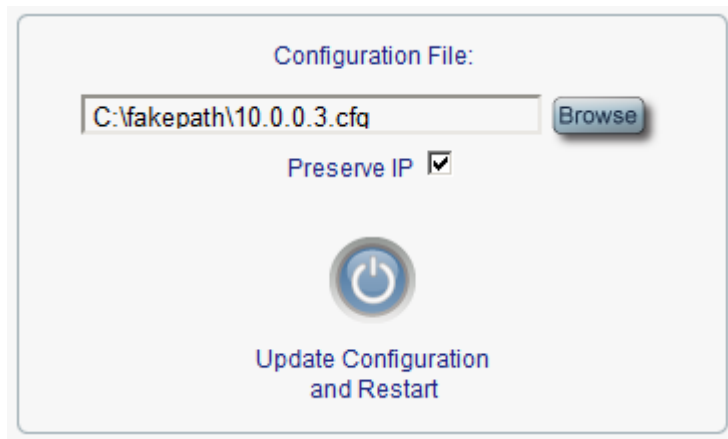


Figure 146: Update System Configuration: Configuration File

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

- Click **Update Configuration and Restart** .

The following confirmation message appears.

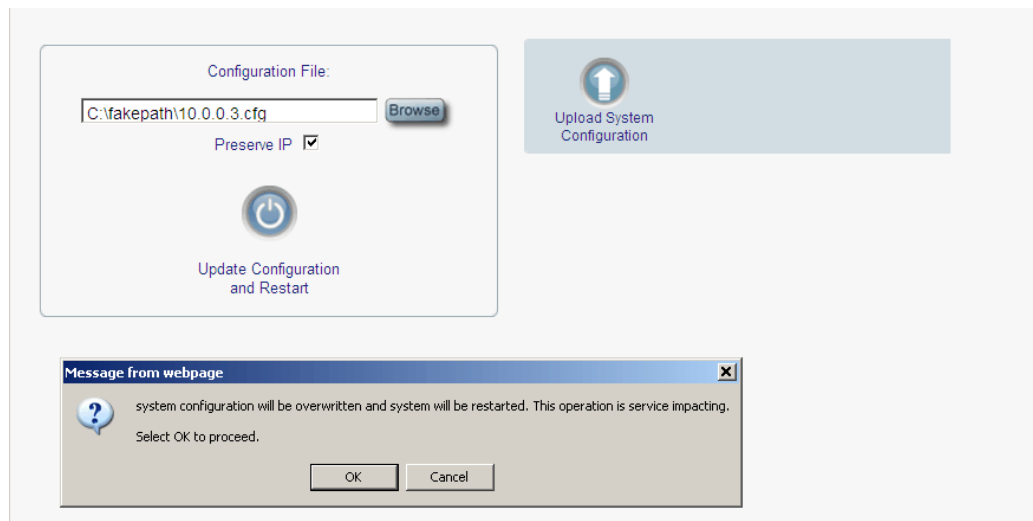


Figure 147: Confirm System Overwrite

- 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 148: 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.

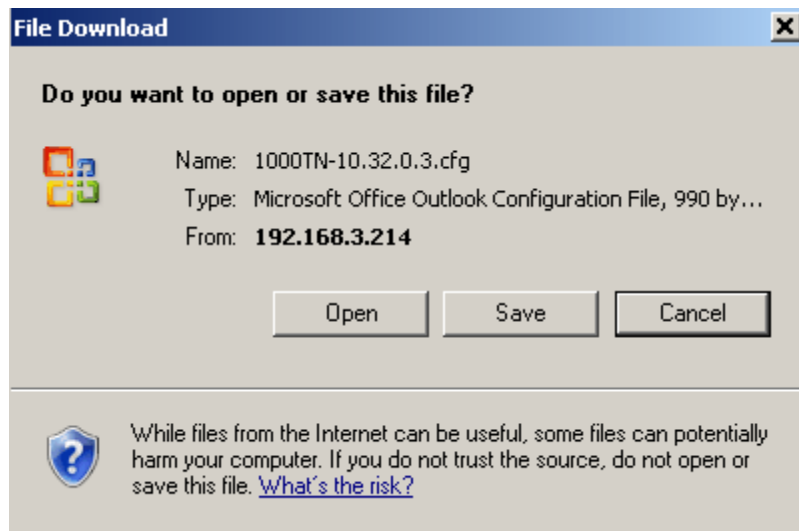


Figure 149: Opening .cfg Dialog Box

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

8.1.4 Software Tab

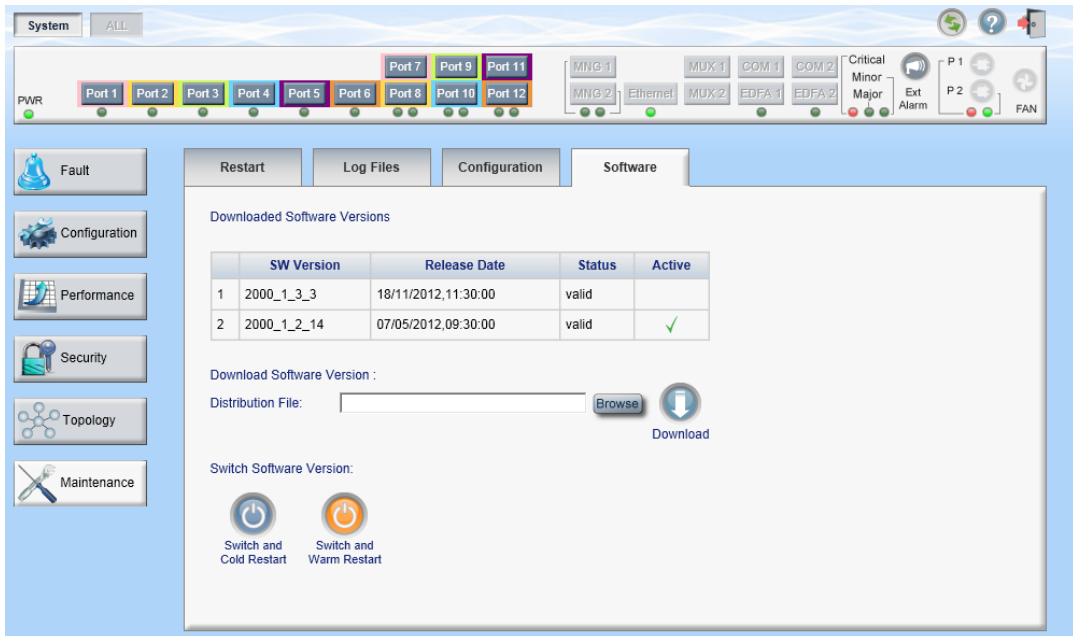


Figure 150: Software Tab

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: **p1.vx**

3. Click **Download** .

The following message appears.

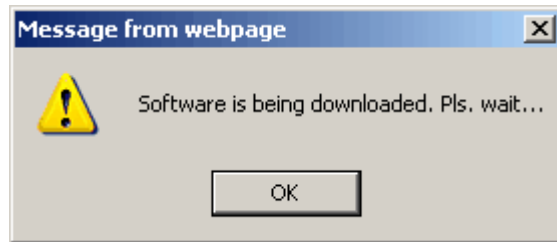


Figure 151: Software Download Message

4. Click **OK**.

The Software Download Status window opens.

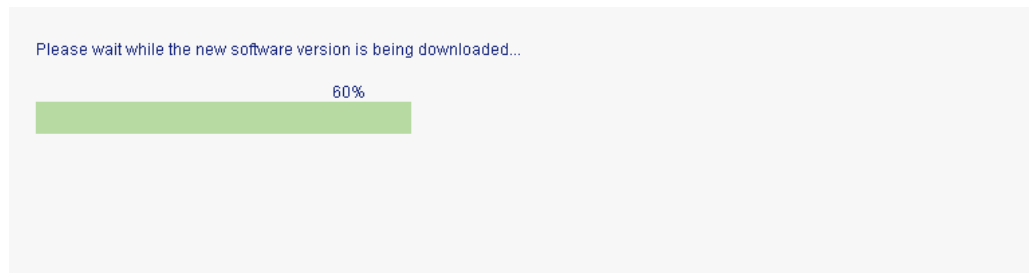


Figure 152: Software Download Status Window

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.

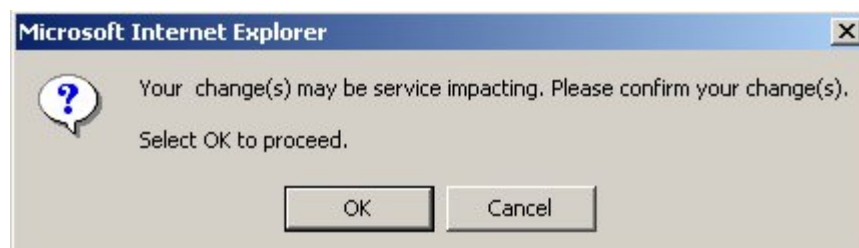


Figure 153: Confirm Changes

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.

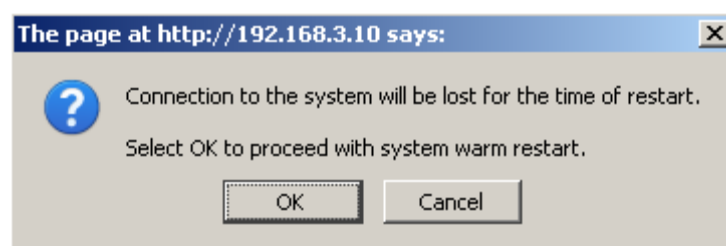


Figure 154: Confirm Changes

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

8.2.1 Facility Loopback Test

The facility loopback test can be performed on any XFP port or SFP+ 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 SFP+ port.

- Remote loopback:** This remote test allows the operator to verify that the entire link is operational. This loopback can be performed on the XFP port of the remote PL-1000TN.

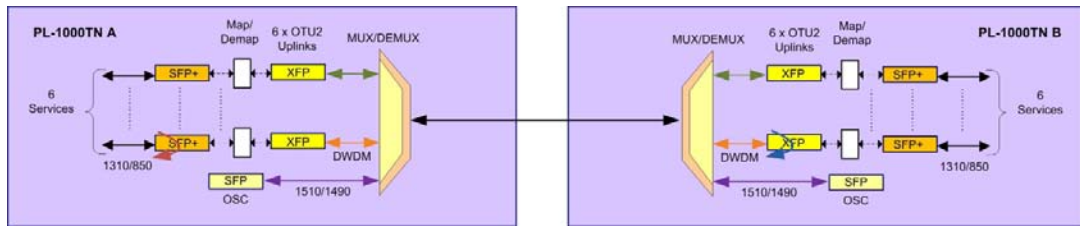


Figure 155: Facility Loopback Test

8.2.2 PRBS Test

The uplink ports 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:

- Bottom XFP of Node A sends PRBS while bottom XFP of Node B is configured to loopback.
- Bottom SFP+ sends PRBS.

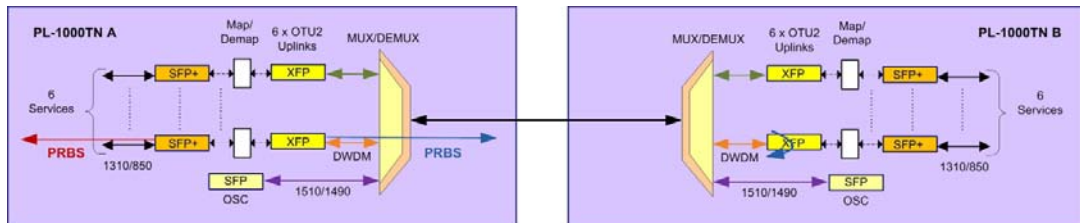


Figure 156: PRBS Test

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 simple connection of the Rx and Tx fibers.

8.3 Uplink Port Maintenance

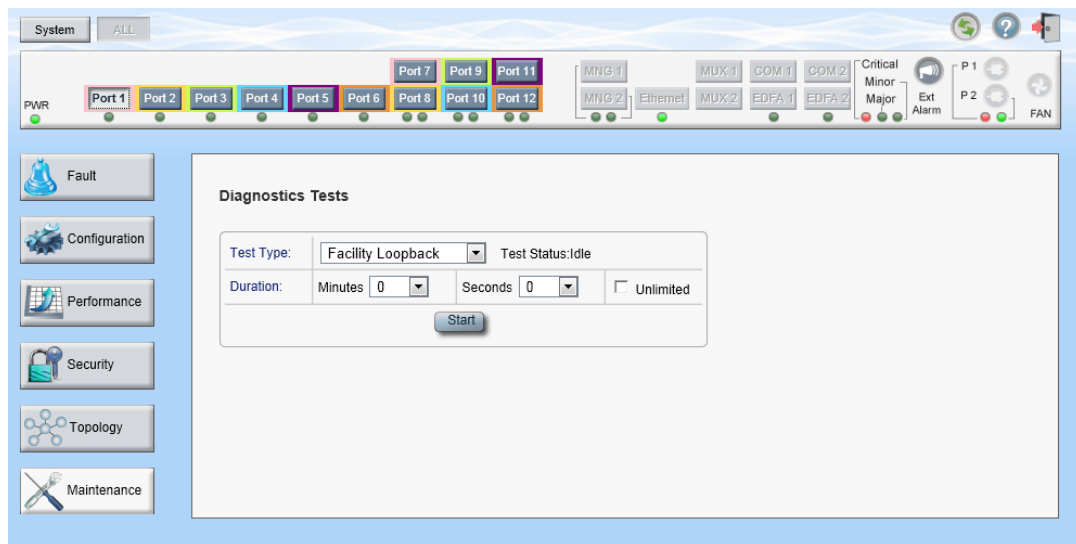


Figure 157: Uplink Port Maintenance Window

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

To open the Uplink Port Maintenance window:

1. Click **Maintenance**.
2. Click a **Port** button (Port 1-6) to select the uplink port.

The appropriate Uplink Port Maintenance window opens.

8.3.1 Diagnostics Tests Tab

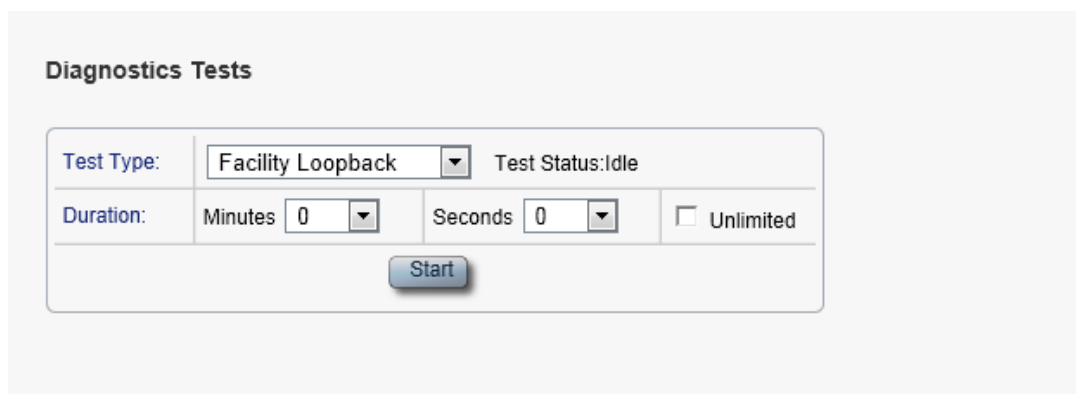


Figure 158: Diagnostic Tests Tab

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

To perform diagnostic tests:

1. Click a **Port** button (Port 1-6) to select the uplink port.

The appropriate 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.

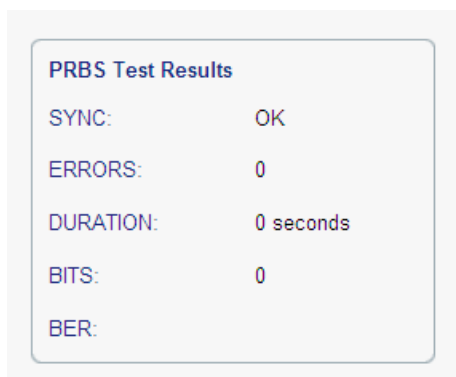


Figure 159: PRBS Test Results

Table 70: 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 : 0.000013

8.4 Service Port Maintenance

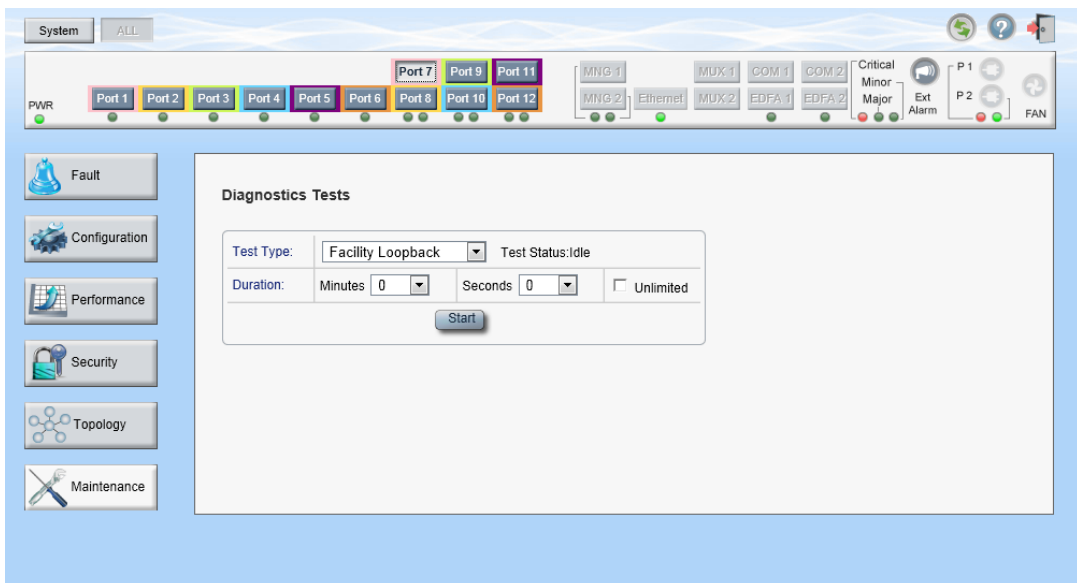


Figure 160: Service Port Maintenance Window

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 a **Port** button (Port 7-12) to select the service port.
The appropriate Service Port Maintenance window opens.

8.4.1 Diagnostics Tests Tab

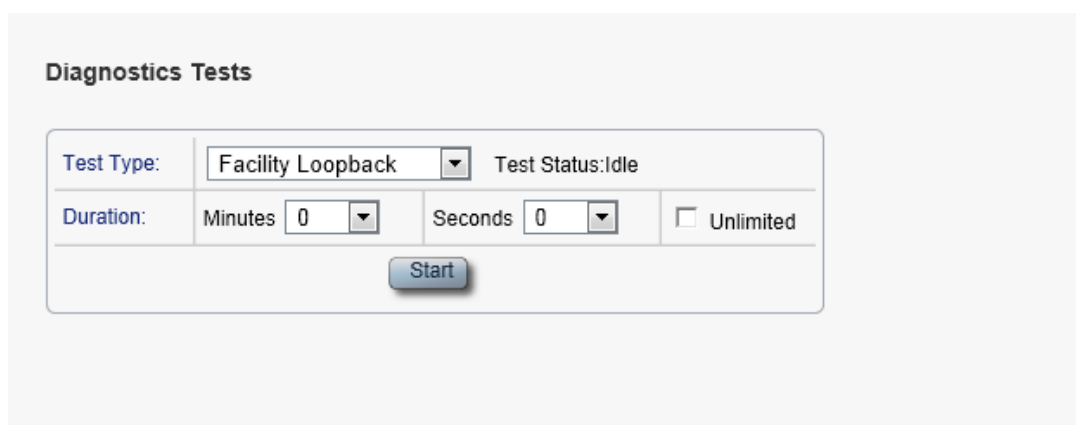


Figure 161: Diagnostic Tests Tab

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

To perform diagnostic tests:

1. Click a **Port** button to select the service port.
The appropriate 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.

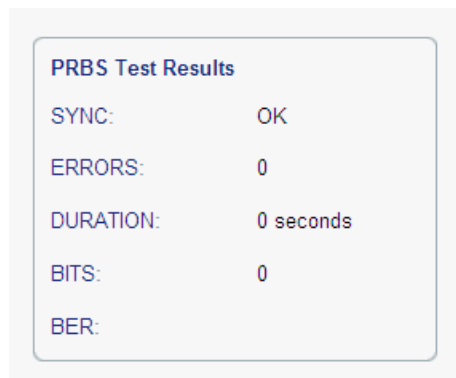


Figure 162: PRBS Test Results

Table 71: 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)

Parameter	Description	Format/Values
BER	The bit error ratio.	Decimal number (ERROR / BITS) For example : 0.0000013

8.5 External Alarm Maintenance

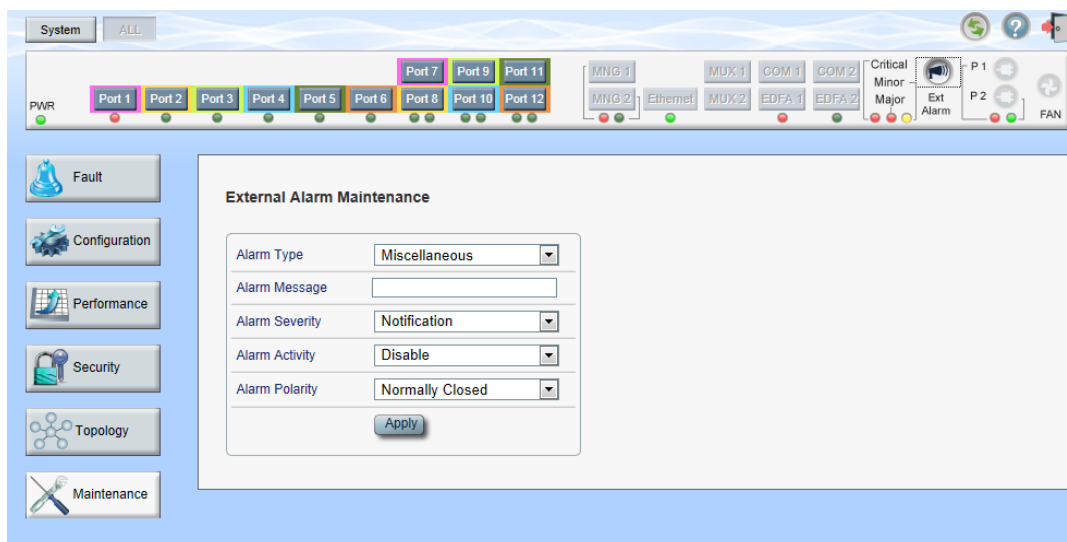


Figure 163: External Alarm Maintenance Window

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 164: 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 72: 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-1000TN nodes.

In this Chapter

Network Topology..... 219

9.1 Network Topology

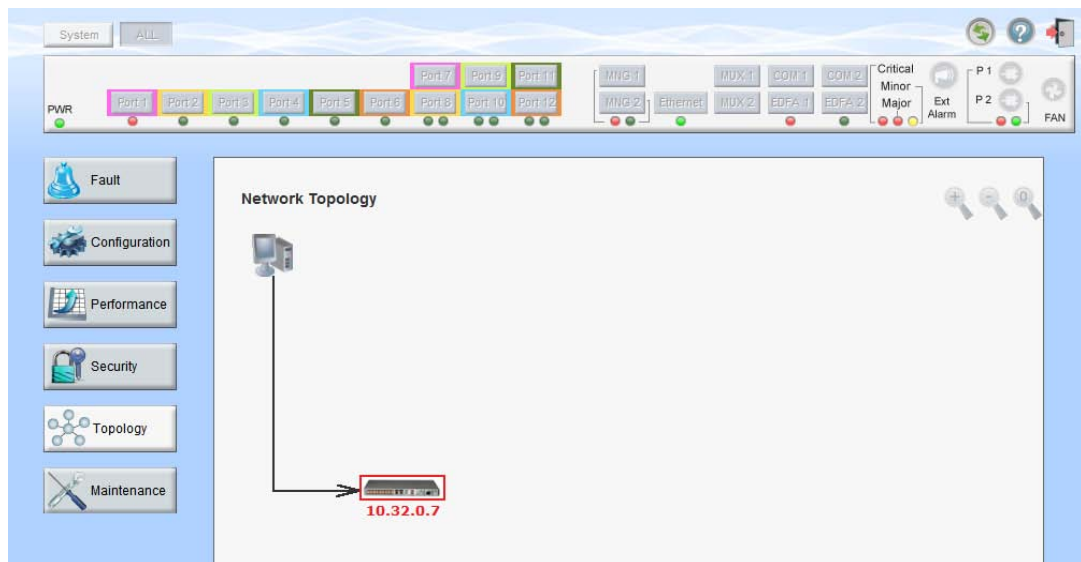


Figure 165: Network Topology Window

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

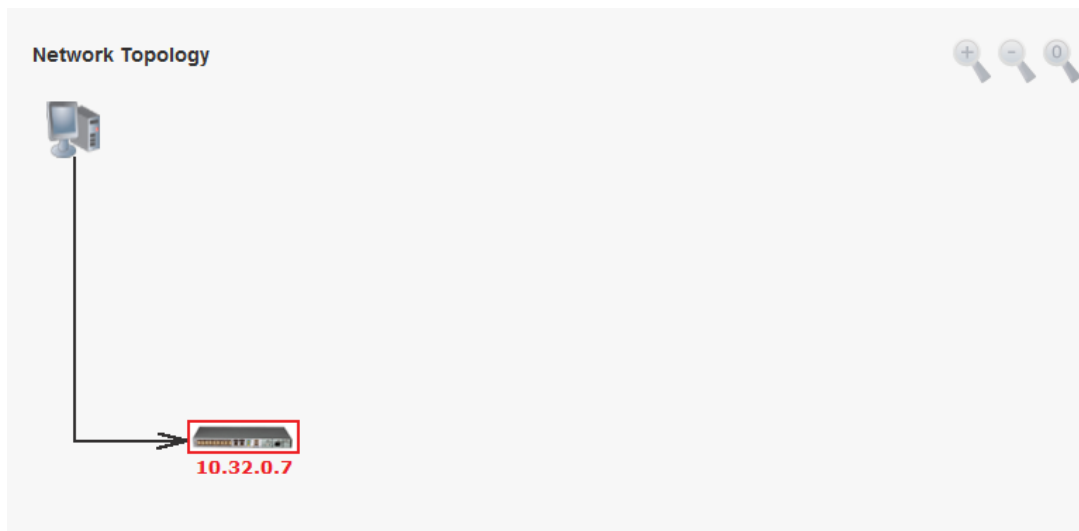


Figure 166: Network Topology Tab

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-1000TN nodes connected together with the OSC channel.

9.1.1.1 Network Linear Topology

The following figure is an example of a linear topology.

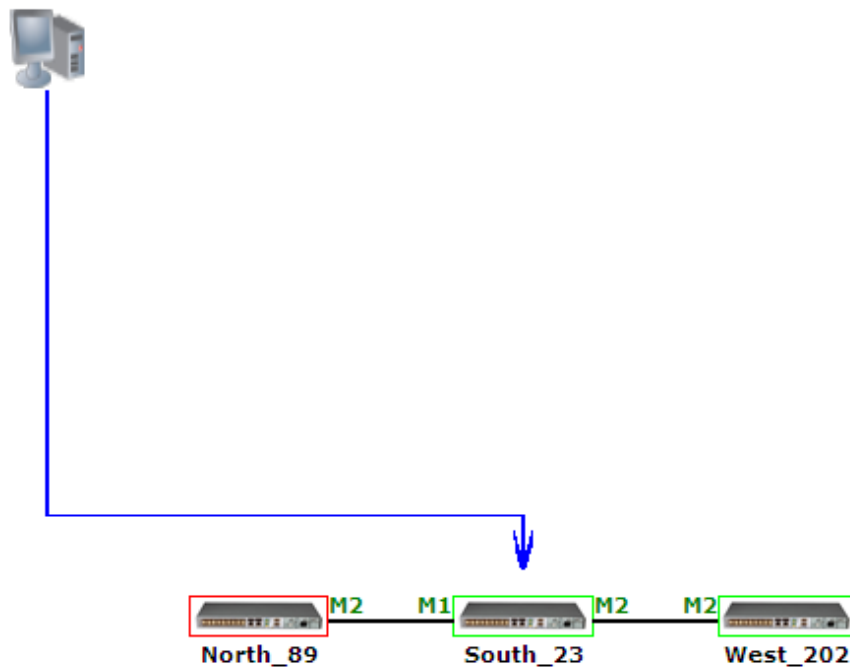


Figure 167: Linear Topology (Example)

9.1.1.2 Ring Topology

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

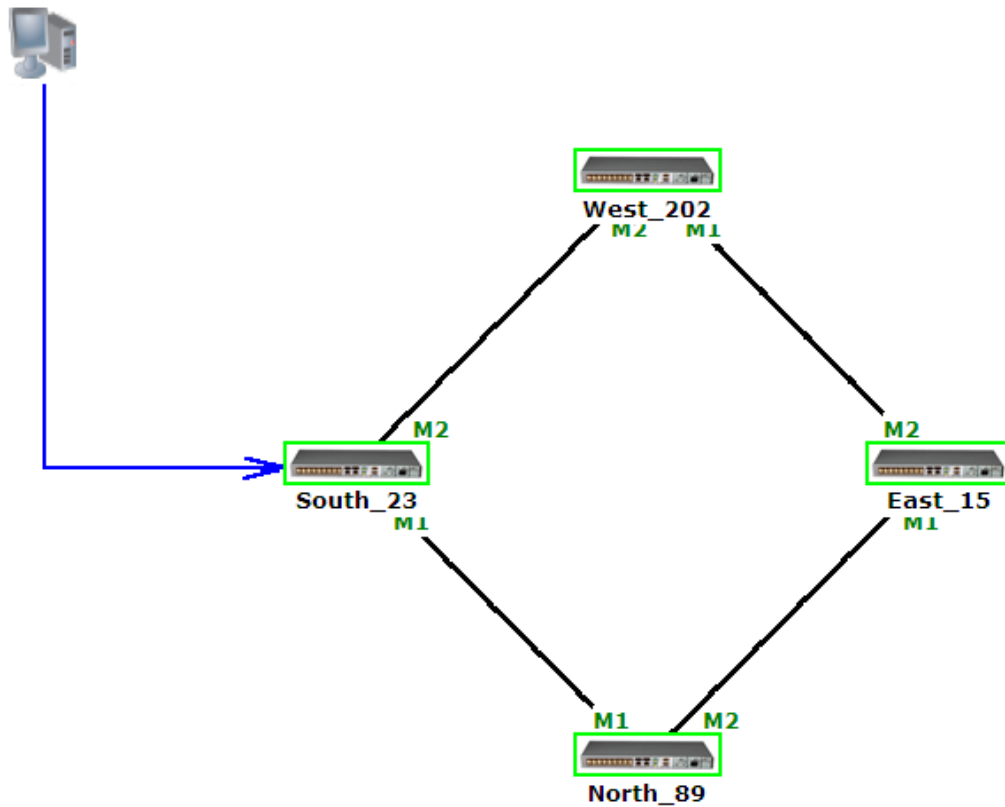


Figure 168: Ring Topology (Example)

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-1000TN 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-1000TN 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. 124).)

9.1.4 Defining Multiple Nodes as Multi-Chassis

When multiple PL-1000TN 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-1000TN node (see [Logging In to the Web Application](#) (p. 38)).
2. Click **Configuration**.
3. Click **System**.

The System Configuration window opens.

4. Click the **General** tab.

The General tab opens.

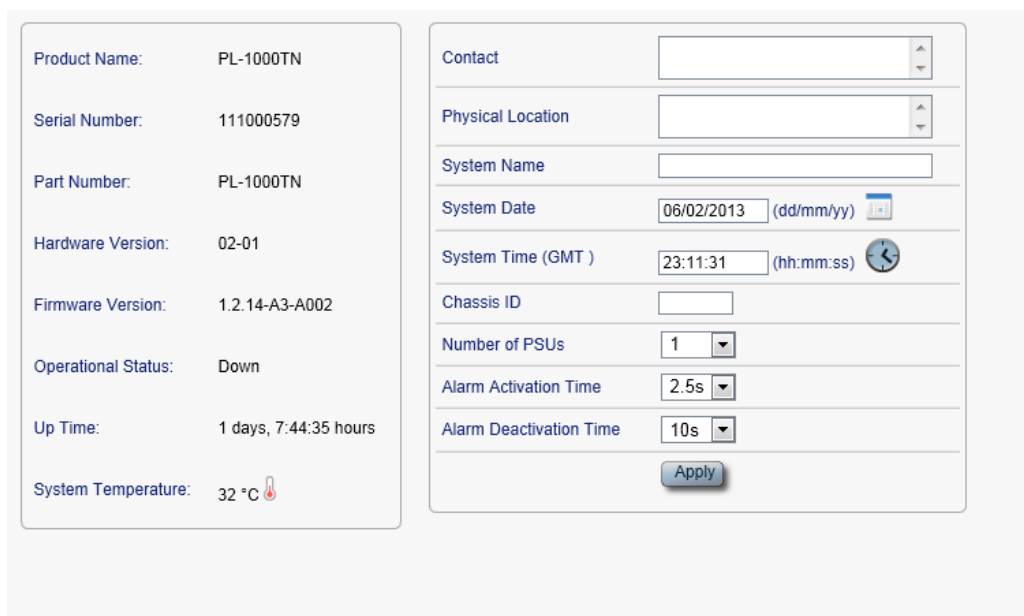


Figure 169: General Tab

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.

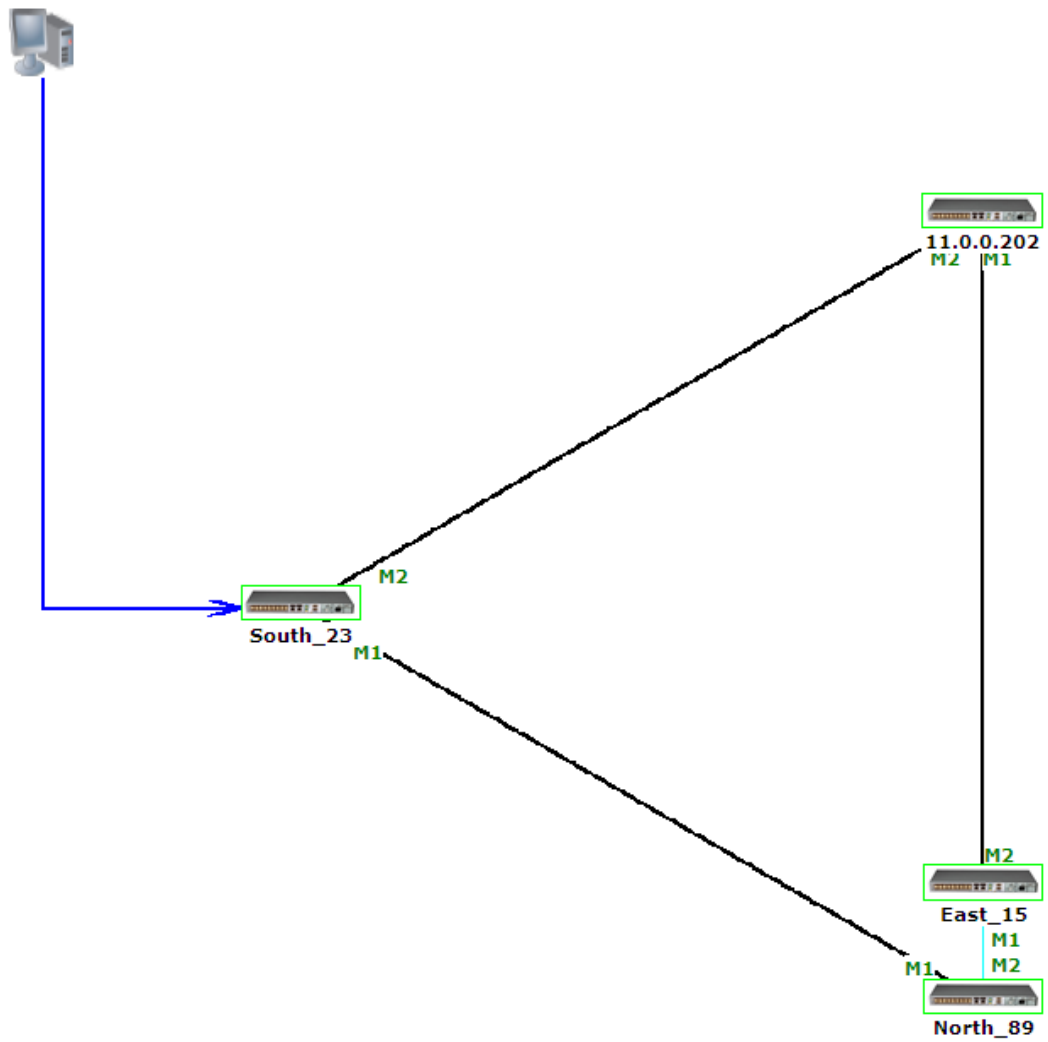


Figure 170: Multi-Chassis Nodes

10 Remote Management Configuration

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

A remote PL-1000TN can be managed through the OSC management channel.

In this Chapter

Remote Management Configuration Example..... 227

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-1000TN nodes A and B via the OSC channel.

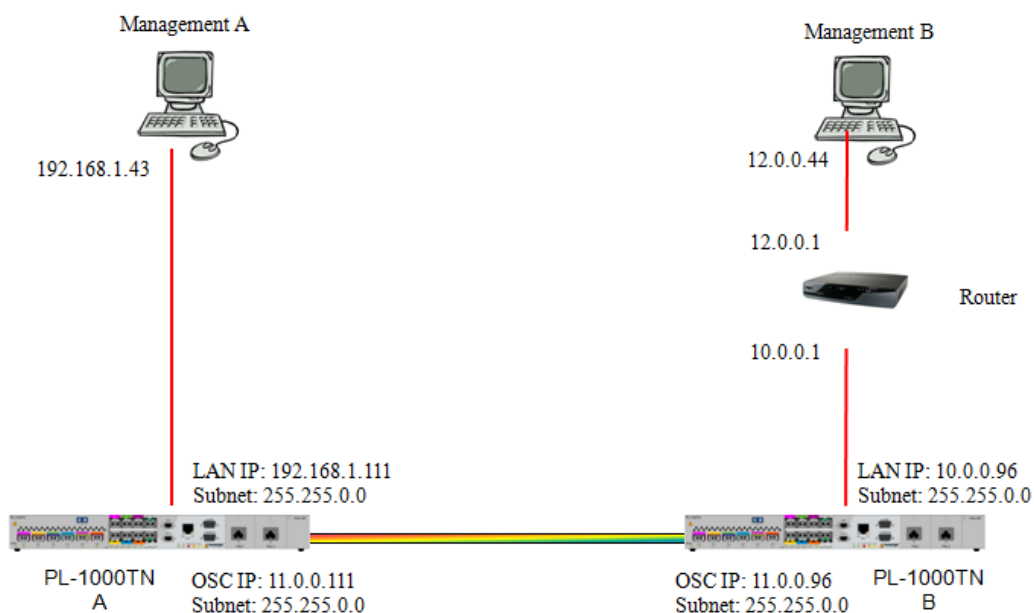


Figure 171: Point-to-Point Remote Management (Example)

10.1.1 Setting Up Point-to-Point Management

To set up point-to-point management:

1. Make sure that you have local Web access to both PL-1000TN nodes (see [Accessing the Web Application](#) (p. 37)).
2. Configure management for PL-1000TN A.
3. Configure management for PL-1000TN B.
4. Access the Web application from Management A to PL-1000TN A.
5. Access the Web application from Management A to PL-1000TN B.

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

10.1.2 Configuring Management for PL-1000TN A

To configure management for PL-1000TN A:

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

The System Configuration window opens.

3. Click the **IP** tab.

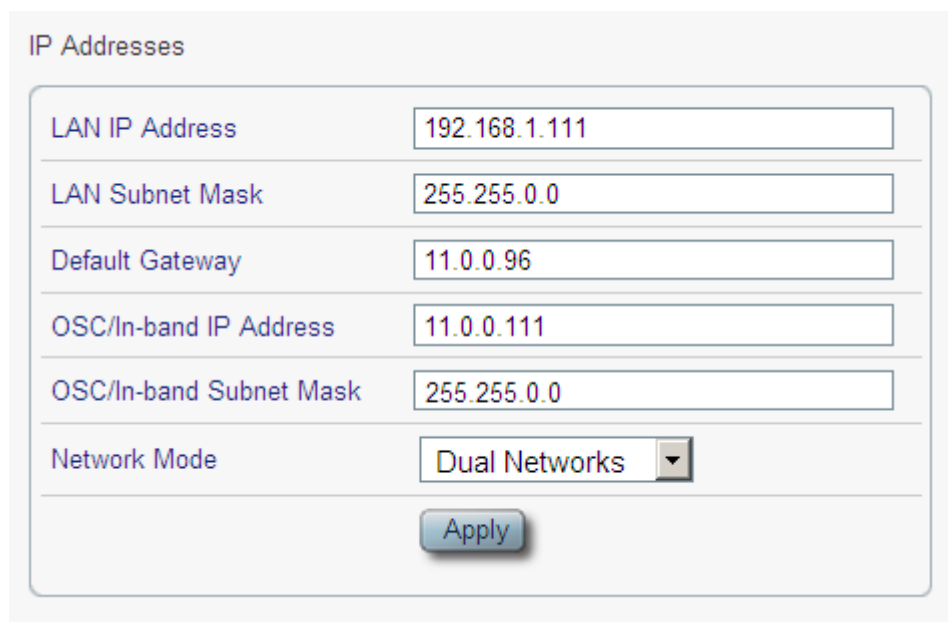
The IP tab opens displaying the IP Address and Static Routing configuration (see [IP Tab](#) (p. 124)).

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.



IP Addresses	
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
Network Mode	Dual Networks
<input type="button" value="Apply"/>	

Figure 172: IP Addresses: PL-1000TN 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. 127)).

The SNMP Traps table should appear as follows.

SNMP Traps

Manager Address	SNMP Traps	Community	Trap Port	Action
12.0.0.44	SNMP V2c	public	162	Delete
192.168.1.43	SNMP V2c	public	162	Delete
<input type="text"/>	SNMP V2c ▼	<input type="text" value="public"/>	<input type="text" value="162"/>	Add

Figure 173: SNMP Traps Table (Example)

10.1.3 Configuring Management for PL-1000TN B

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

To configure management for PL-1000TN B:

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

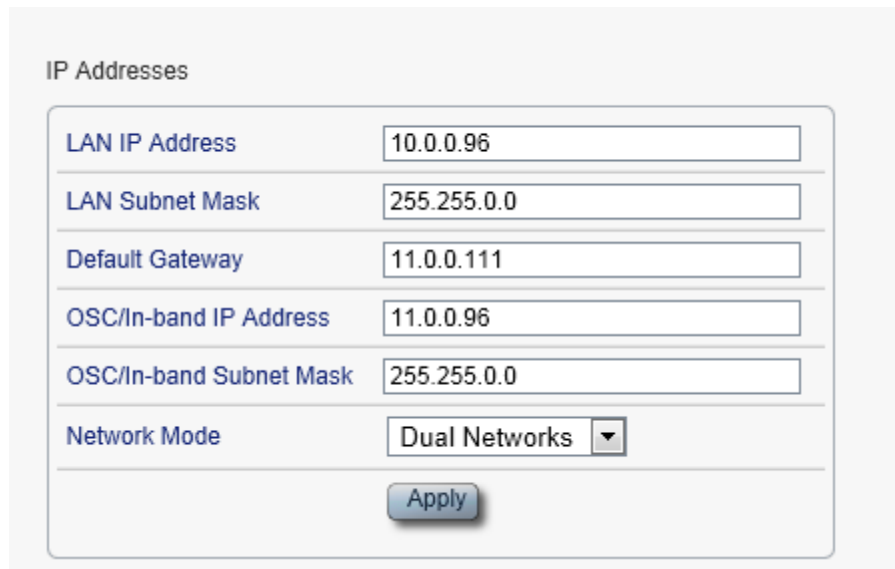
The System Configuration window opens.

3. Click the **IP** tab.

The IP tab opens displaying the IP Address and Static Routing configuration (see [IP Tab](#) (p. 124)).

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.

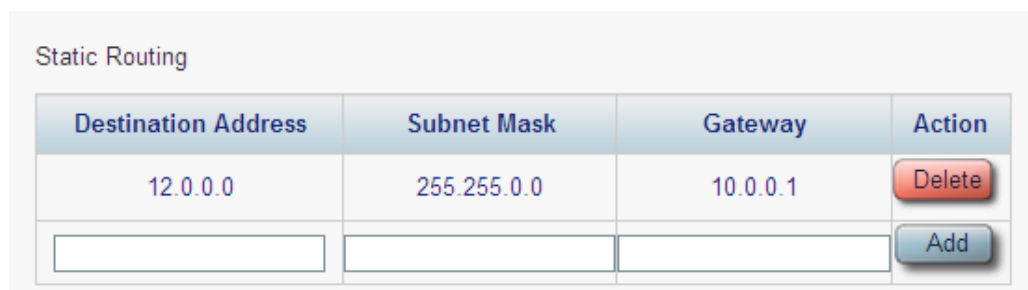


IP Addresses	
LAN IP Address	10.0.0.96
LAN Subnet Mask	255.255.0.0
Default Gateway	11.0.0.111
OSC/In-band IP Address	11.0.0.96
OSC/In-band Subnet Mask	255.255.0.0
Network Mode	Dual Networks ▼
<input type="button" value="Apply"/>	

Figure 174: IP Addresses: PL-1000TN 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.



Static Routing			
Destination Address	Subnet Mask	Gateway	Action
12.0.0.0	255.255.0.0	10.0.0.1	<input type="button" value="Delete"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Figure 175: Static Routing: PL-1000TN 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. 127)).

The SNMP Traps table should appear as follows.

SNMP Traps				
Manager Address	SNMP Traps	Community	Trap Port	Action
12.0.0.44	SNMP V2c	public	162	Delete
192.168.1.43	SNMP V2c	public	162	Delete
<input type="text"/>	SNMP V2c ▾	<input type="text" value="public"/>	<input type="text" value="162"/>	Add

Figure 176: SNMP Traps Table (Example)

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

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

1. Open the Web browser.
2. In the address field of the browser, type the **IP address** of the LAN port of PL-1000TN 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)

3. Press **Enter**.
The Login window opens.
4. Log in to the Web application (see [Logging In to the Web Application](#) (p. 38)).

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

To access the Web application from Management A to PL-1000TN 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-1000TN as follows:

http://11.0.0.96 (for HTTP access)

or

https://11.0.0.96 (for HTTPS secure access) (as illustrated in Remote Management Configuration Example)

4. Press **Enter**.

The Login window opens.

5. Log in to the Web Application (see [Logging In to the Web Application](#) (p. 38)).

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

To access the Web application from Management B to PL-1000TN 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-1000TN 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)
```

4. Press **Enter**.

The Login window opens.

5. Log in to the Web Application (see [Logging In to the Web Application](#) (p. 38)).

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

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


4. Press **Enter**.

The Login window opens.

5. Log in to the Web application (see [Logging In to the Web Application](#) (p. [38](#))).

11 CLI

This chapter describes the CLI for PL-1000TN.

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

In this Chapter

General Features	235
Accessing the CLI	235
CLI Command Types.....	238
Running CLI Commands	239

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-1000TN 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-1000TN>>
```

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

6. Run the desired CLI commands as described in [Running CLI Commands](#) (p. 239).

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-1000TN>>
```

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

For example:

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

4. Run the desired CLI commands as described in [Running CLI Commands](#) (p. 239).
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-1000TN>>
```

5. Run the desired CLI commands as described in [Running CLI Commands](#) (p. 239).
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 Provisioning command
- System Restart command

The following figure shows the hierarchy of the commands.

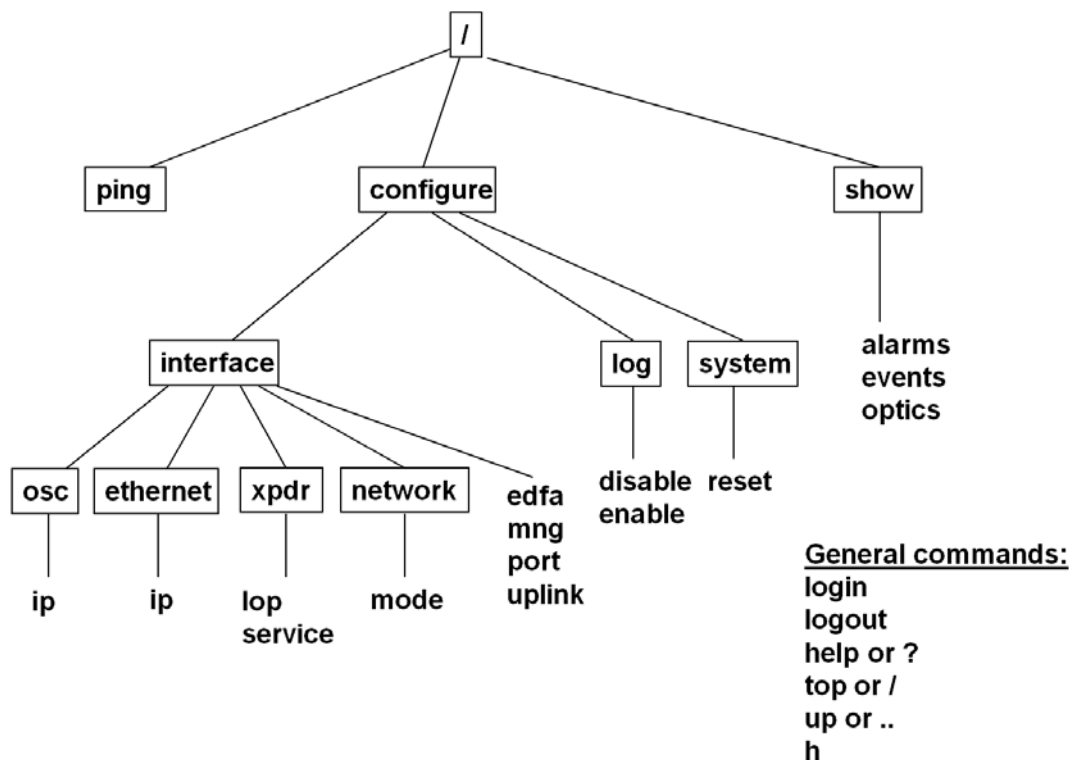


Figure 177: CLI Command Tree

11.4 Running CLI Commands

You can run the following CLI commands:

- General commands
 - [Login](#) (p. 240)
 - [Logout](#) (p. 241)
 - [Help](#) (p. 241)
 - [History](#) (p. 241)
 - [Top](#) (p. 242)
 - [Up](#) (p. 242)
- [Ping command](#) (p. 243)
- Interface commands
 - [Configure Interface Port](#) (p. 243)
 - [Configure Interface MNG](#) (p. 243)
 - [Configure Interface EDFA](#) (p. 244)
- IP Setting commands
 - [Configure Interface Ethernet IP](#) (p. 244)

- [Configure Interface OSC IP](#) (p. 245)
- [Configure Interface Network Mode](#) (p. 245)
- Log commands
 - [Configure Log Enable](#) (p. 246)
 - [Configure Log Disable](#) (p. 246)
- Show commands
 - [Show Alarms](#) (p. 247)
 - [Show Events](#) (p. 247)
 - [Show Optics](#) (p. 247)
- Service commands
 - [Configure Interface XPDR LOP](#) (p. 248)
 - [Configure Interface XPDR Service](#) (p. 248)
- System Restart command
 - [Configure System Reset](#) (p. 249)

11.4.1 General Commands

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

- [Login](#) (p. 240)
- [Logout](#) (p. 241)
- [Help](#) (p. 241)
- [History](#) (p. 241)
- [Top](#) (p. 242)
- [Up](#) (p. 242)

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

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-1000TN>>logout
PL-1000TN>>
```

11.4.1.3 Help Command

Command:

help [<command>]

or

? [<command>]

Description:

This command displays the syntax of the specified command.

Example:

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

11.4.1.4 History Command

Command:

h

Description:

This command displays the last 20 commands.

Example:

```
PL-1000TN>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-1000TN>show>>
```

11.4.1.5 Top Command

Command:

```
top
or
/
```

Description:

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

Example:

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

11.4.1.6 Up Command

Command:

```
up
or
..
```

Description:

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

Example:

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

11.4.3 Interface Commands

The following are the Interface commands:

- [Configure Interface Port](#) (p. 243)
- [Configure Interface MNG](#) (p. 243)
- [Configure Interface EDFA](#) (p. 244)

11.4.3.1 Configure Interface Port Command

Command:

```
configure interface port <num> [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-1000TN>configure>interface>>port 1
Port 1 is DOWN
PL-1000TN>configure>interface>>port 1 up
PL-1000TN> configure>interface>>port 1
Port 1 is UP
PL-1000TN>configure>interface>>
```

11.4.3.2 Configure Interface MNG Command

Command:

```
configure interface mng <num> [up | down]
```

Description:

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

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

Example:

```
PL-1000TN>configure>interface>>mng 1 down
PL-1000TN>configure>interface>>mng 1
Port MNG 1 is DOWN
PL-1000TN>configure>interface>>
```

11.4.3.3 Configure Interface EDFA Command

Command:

```
configure interface edfa <num> [up | down]
```

Description:

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

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

Example:

```
PL-1000TN>configure>interface>>edfa 1 up
PL-1000TN>configure>interface>>
```

11.4.4 IP Setting Commands

The following are the IP Setting commands:

- [Configure Interface Ethernet IP](#) (p. 244)
- [Configure Interface OSC IP](#) (p. 245)
- [Configure Interface Network Mode](#) (p. 245)

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-1000TN>configure>interface>ethernet>>ip 10.0.3.200 -n 255.255.0.0 -g
10.0.44.44
PL-1000TN>configure>interface>ethernet>>ip
Addr is 10.0.3.200, Subnet mask is 255.255.0.0
Gateway is 10.0.44.44
PL-1000TN>configure>interface>ethernet>>
```

11.4.4.2 Configure Interface OSC IP Command

Command:

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

Description:

This command sets the IP parameters of the MNG ports.

- **<addr>**: IP address of the MNG ports.
- **<netmask>**: Subnet mask of the MNG ports.
- **<gateway>**: IP address of the default gateway.

If no parameter is specified, the current IP parameter values of the MNG ports are displayed.

NOTE: When working via Telnet, changing the IP parameters of the OSC may prevent further access to the node.

Example:

```
PL-1000TN>configure>interface>osc>>ip 11.0.3.200 -n 255.255.0.0 -g
11.0.3.201
PL-1000TN>configure>interface>osc>>ip
Addr is 11.0.3.200, Subnet mask is 255.255.0.0
Gateway is 11.0.3.201
PL-1000TN>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. 249)).

Example:

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

11.4.5 Log Commands

The following are the Log commands:

- [Configure Log Enable](#) (p. 246)
- [Configure Log Disable](#) (p. 246)

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

11.4.6 Show Commands

The following are the Show commands:

- [Show Alarms](#) (p. 247)
- [Show Events](#) (p. 247)

- [Show Optics](#) (p. 247)

11.4.6.1 Show Alarms Command

Command:

```
show alarms [port <num> | mng <num> | edfa <num> | system]
```

Description:

This command displays the alarms of the specified port. If no parameters are specified, all alarms are displayed.

Example:

```
PL-1000TN>>show alarms port 1
THU JUN 18 12:22:46 2009      PORT 1  Optics Loss of Light      Critical
S.A.
THU JUN 18 12:22:46 2009      PORT 1  Loss Propagation                Minor
PL-1000TN>>
```

11.4.6.2 Show Events Command

Command:

```
show events [port <num> | mng <num> | edfa <num> | system]
```

Description:

This command displays the events of the specified port. If no parameters are specified, all the events are displayed.

Example:

```
PL-1000TN>>show events port 1
THU JUN 18 12:22:44 2009      PORT 1  Link Up
Event
THU JUN 18 12:22:46 2009      PORT 1  Optics Loss of Light      Critical
S.A.
THU JUN 18 12:22:46 2009      PORT 1  Loss Propagation                Minor
THU JUN 18 12:22:47 2009      PORT 1  Link Down
Event
PL-1000TN>>
```

11.4.6.3 Show Optics Command

Command:

```
show optics [ port <num>] | [ mng <num>] | [ edfa <num>]
```

Description:

This command displays the optical information of the specified entity.

Example:

```
PL-1000TN>>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-1000TN>>show optics mng 1
Vendor: PLTOLINK INC
Part Number: PLS-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-1000TN>>
  
```

11.4.7 Service Commands

The following are the Service commands:

- [Configure Interface XPDR LOP](#) (p. 248)
- [Configure Interface XPDR Service](#) (p. 248)

11.4.7.1 Configure Interface XPDR LOP Command

Command:

```
configure interface xpdr lop <port> [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-1000TN>configure>interface>xpdr>>lop 3
Loss Propagation is enabled
PL-1000TN>configure>interface>xpdr>>
  
```

11.4.7.2 Configure Interface XPDR Service Command

Command:

```
configure interface xpdr service [<port> [<service type>]]
```

Description:

This command provisions the transponder with the specified service.

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

The following service types are available:

- OC-192_OTU2
- STM-64_OTU2

- 10GBE-LAN_OTU2e
- 10GFC-LAN_OTU2f
- 8GFC_OTU2

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-1000TN>configure>interface>xpdr>>ser 1 10GBE-LAN_OTU2e
XPDR 1-7 service type to 33
PL-1000TN>configure>interface>xpdr>>ser 1
Service Type is 10GBE-LAN_OTU2e
PL-1000TN>configure>interface>xpdr>>
```

11.4.8 System Restart Command

The following is the System Restart command:

- [Configure System Reset](#) (p. 249)

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-1000TN>>configure system reset w
PL-1000TN>>

Connection to host lost.
```


Appendix A: Connection Data

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

In this Appendix

CONTROL Connector	251
ALARM Connector	251
ETH Connector	253
Optical PL-1000TN Connectors	254
Power Supply Combinations	255
Power Connectors.....	256
Protective Ground Terminal.....	256
Fiber Shelf	257

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 73: CONTROL Connector Wiring

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

A.2 ALARM Connector

The ALARM connector of the PL-1000TN 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.

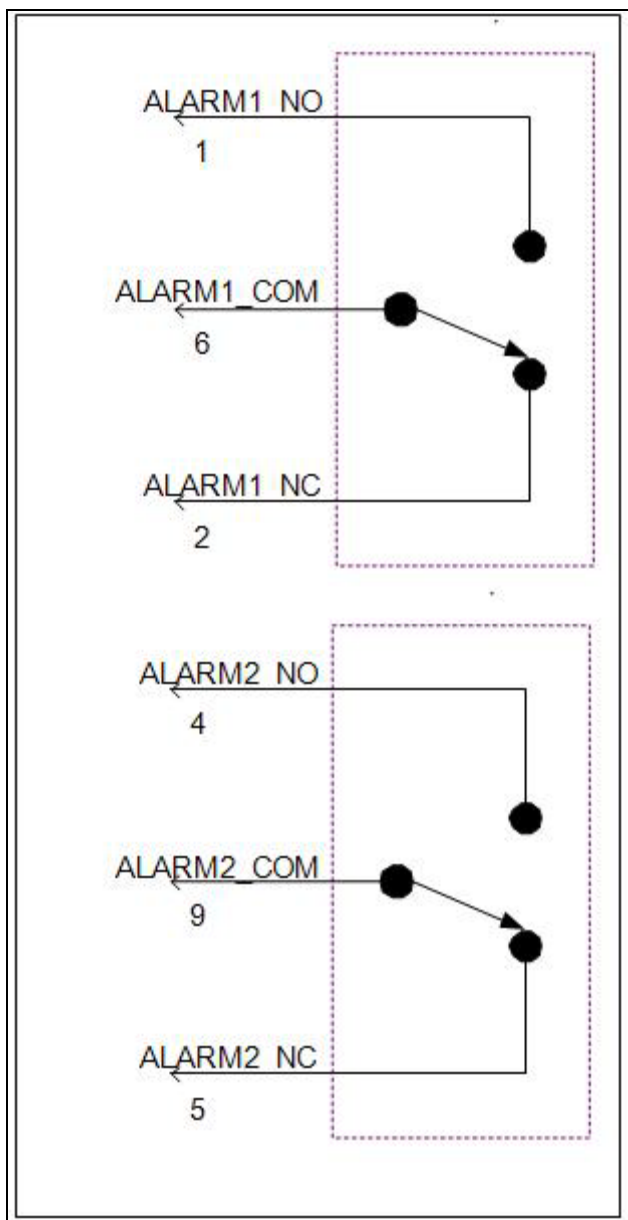


Figure 178: External ALARM Diagram

Table 74: ALARM Interface, Pin Function

Pin	Designation	Function
1	ALARM Normally Open (ALARM1_NO)	In normal operation, pin 6 (ALARM Common) is internally connected to pin 2 (ALARM Normally Closed). Upon a Major alarm event, the internal connection of pin 6 (ALARM Common) is switched to this pin (pin 1).

Pin	Designation	Function
2	ALARM Normally Closed (ALARM1_NC)	In normal operation, pin 6 (ALARM Common) is internally connected to this pin (pin 2). Upon a Major or Critical alarm event, the internal connection of pin 6 (ALARM Common) is switched to pin 1 (Alarm Normally Open)
6	ALARM Common (ALARM1_COM)	Common signal
3		Internally connected to GND.
7	ALARM IN 1	Input External Alarm
8	ALARM IN 2	Not connected
4*	ALARM Normally Open (ALARM2_NO)	In normal operation, pin 9 (ALARM Common) is internally connected to pin 5 (Alarm Normally Closed). Upon a Major alarm event, the internal connection of pin 9 (ALARM Common) is switched to this pin (pin 4).
5*	ALARM Normally Closed (ALARM2_NC)	In normal operation, pin 9 (ALARM Common) is internally connected to this pin (pin 5). Upon a Major alarm event, the internal connection of the pin 9 (ALARM Common) is switched to pin 4 (ALARM Normally Open).
9*	ALARM Common (ALARM2_COM)	Common signal

* The pin will be implemented in a future software release.

A.3 ETH Connector

The PL-1000TN 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 75: 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-1000TN Connectors

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

- Uplink
- Service
- MNG
- MUX/DEMUX
- COM

A.4.1 Uplink Ports

The uplink ports are six XFP adapters that accept XFP modules.

Table 76: Uplink XFP Specifications

Specification	Requirement
Fiber Type	Single mode
Wavelength	ITU WDM Grid
Fiber Size	2 mm optical fiber
Connector Type	LC
Port Type	OTN

A.4.2 Service Ports

The service ports are six SFP+ adapters that accept optical SFP+ modules.

Table 77: Service SFP+ Specifications

Specification	Requirement
Fiber/Cable Type	Single mode or multi-mode
Wavelength	<ul style="list-style-type: none"> • 850 nm multi-mode • 1310 nm single mode
Fiber Size	2 mm optical fiber
Connector Type	LC
Service Type	<ul style="list-style-type: none"> • 8G FC • 10G FC • 10GBE-LAN • OC-192 • STM-64

A.4.3 MNG Ports

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

Table 78: MNG Port Specifications

Specification	Requirement
Fiber/Cable Type	<ul style="list-style-type: none"> • Optical SFP: Single mode or multi-mode • Copper SFP: Twisted pair
Wavelength	<ul style="list-style-type: none"> • Single mode: <ul style="list-style-type: none"> ▪ CWDM: 1290 nm or 1310 nm ▪ DWDM: 1490 nm or 1510 nm • Multi-mode: 850 nm
Fiber Size	2 mm optical fiber
Connector Type	<ul style="list-style-type: none"> • Optical SFP: LC • Copper SFP: RJ-45
Port Type	Management

A.4.4 MUX/DEMUX Ports

The MUX/DEMUX ports are one or two Multifiber Pull Off (MPO) connectors suitable for a dedicated ribbon cable (supplied by PacketLight).

Table 79: MUX/DEMUX Port Specifications

Specification	Requirement
Fiber Type	Single mode
Fiber Size	2 mm optical fiber
Connector Type	MUX/DEMUX: MPO/APC female
Port Type	MUX/DEMUX connections

A.4.5 COM Ports

The COM ports are one or two fixed duplex LC connectors.

Table 80: COM Port Specifications

Specification	Requirement
Fiber Type	Single mode
Fiber Size	2 mm optical
Connector Type	LC with or without protective shutters
Port Type	Optical COM port

A.5 Power Supply Combinations

The following power supply combinations are feasible in the PL-1000TN:

- One or two AC power supplies
- One or two DC power supplies

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

A.6 Power Connectors

The PL-1000TN may have the following power supply connectors:

- **AC-powered PL-1000TN units:** Standard three-pin IEC320 C5 connector 3A for connection to AC power.
- **DC-powered PL-1000TN units:** DC power is supplied with a dedicated connector for wiring.

The following figure shows how to wire the DC connector (DC power supply only).

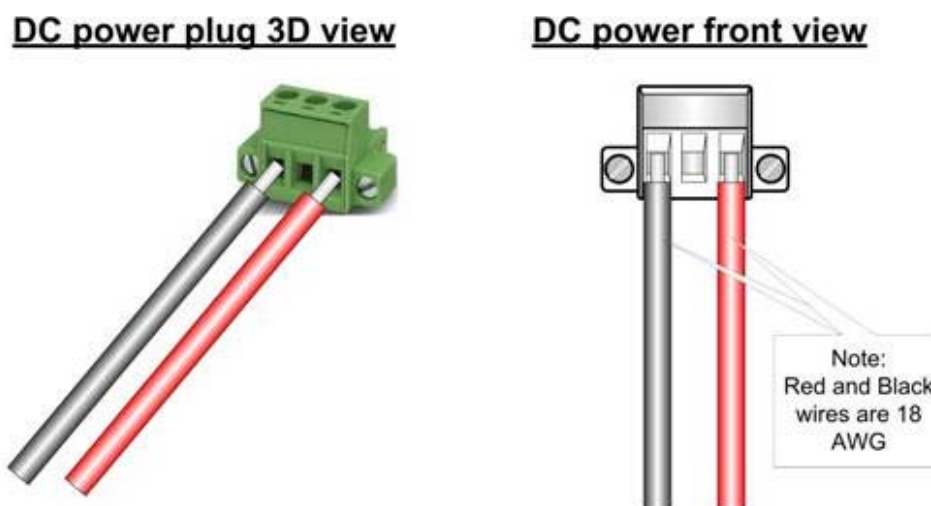


Figure 179: DC Connector Wiring Diagram

A.7 Protective Ground Terminal

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

The following figure shows how to wire the ground terminal.

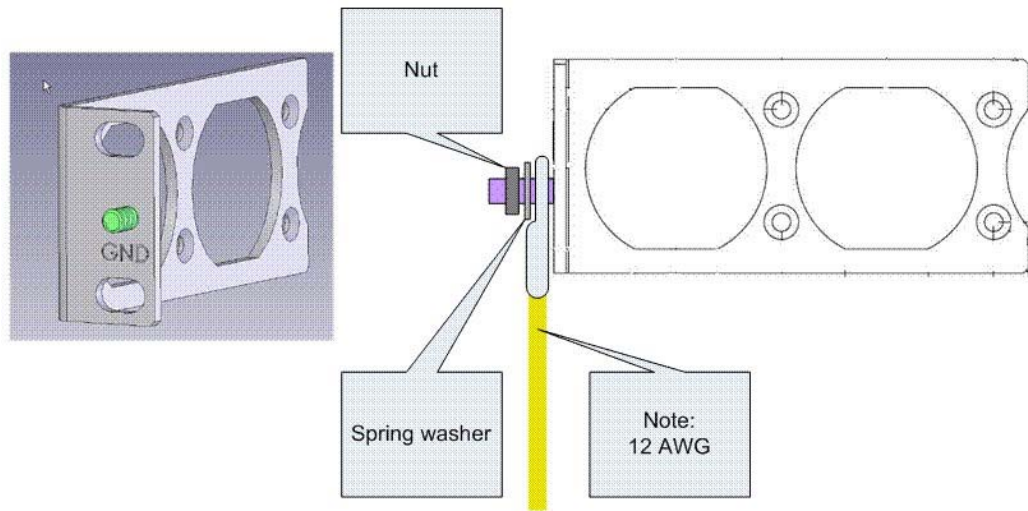


Figure 180: Protective Ground Terminal Wiring Diagram

A.8 Fiber Shelf

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

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

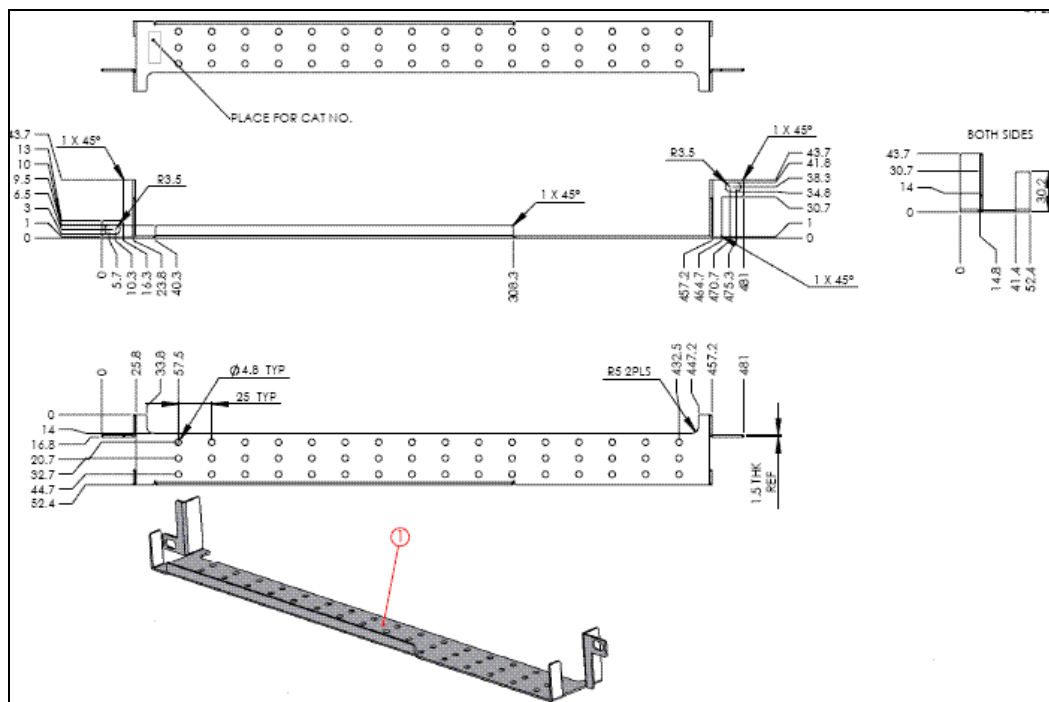


Figure 181: Fiber Shelf Diagram

Appendix B: Alarm and Event Messages

This appendix describes the possible alarm and event messages.

In this Appendix

Alarm Messages	259
Configuration Event Messages	263
Other Event Messages	264

B.1 Alarm Messages

The following table lists the possible alarm messages and their interpretation and/or corrective measures.

Table 81: Alarm Messages

Source	Message	Interpretation/Corrective Measures
PSU1/PSU2	Power Supply Failure	Replace the faulty PSU.
PSU1/PSU2	Power Failure– Low Voltage	Replace the faulty PSU.
FAN	Fan Failure	The internal cooling fan of the device does not operate. Replace the FAN unit as soon as possible.
System	Hardware Failure	A technical failure has been detected. Replace the device.
System	Database Restore Failed	Failed to update the system configuration.
System	Database Restore in Progress	Failed to update the system configuration.
System	Cold Restart Required: FPGA Changed	After a warm restart, the FPGA version is not consistent with the software version. A cold restart is required.
System	Software Upgrade Failed	The downloaded software is corrupted. Reload the software.
System	Network Time Protocol Failure	SNTP timing protocol failure. Check the IP connection to the NTP servers.
System	Temporary License Applied	A permanent license should be installed.
System	License Expired or No License Applied	<ul style="list-style-type: none"> • The temporary license has expired <i>or</i> • No license is installed
External Input Alarm	(As configured)	The External Input Alarm is active.
SFP+ Port	Loss of Synchronization	Loss of Synchronization has been detected on the 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 port mate.
Optics	Optics Bit Rate Mismatch	The inserted optical module has a mismatch problem due to the wrong rate or type. Replace the optical module or update the configured service type.

Source	Message	Interpretation/Corrective Measures
Optics	Unauthorized Optics Inserted and is Shutdown	The inserted optical module is unauthorized for use. Replace the optical module with an authorized optical module.
XFP	XFP Transmission Not Ready	<ul style="list-style-type: none"> • Bad line conditions <i>or</i> • Bad XFP module.
XFP	XFP Transmission CDR Not Locked	<ul style="list-style-type: none"> • Bad line conditions <i>or</i> • Bad XFP module.
XFP	XFP Reception Not Ready	<ul style="list-style-type: none"> • Bad line conditions <i>or</i> • Bad XFP module.
XFP	XFP Reception CDR Not Locked	<ul style="list-style-type: none"> • Bad line conditions <i>or</i> • Bad XFP module.
XFP Port	OTN Path Degrade	Bad line conditions.
XFP Port	OTN Section Degrade	Bad line conditions.
XFP Port	OTN LOS	<ul style="list-style-type: none"> • Rx and Tx connectors intermixed <i>or</i> • Fiber break <i>or</i> • Bad XFP module.
XFP Port	OTN LOF	<ul style="list-style-type: none"> • Wrong fiber is connected <i>or</i> • Bad XFP <i>or</i> • Bad line conditions.
XFP Port	OTN Loss of Multiframe	Bad line conditions.
XFP Port	OTN Path BDI	Remote uplink has detected a problem with an ODU1.
XFP Port	OTN Section BDI	Remote uplink has detected a problem with the OTU2.
XFP Port	OTN Path AIS	Remote uplink reports a defect with an ODU1.
XFP Port	OTN Section AIS	Problem in the remote node.
XFP Port	OTN Path Payload Mismatch	Wrong fiber is connected to the uplink.
XFP Port	OTN Section Trace Mismatch	<ul style="list-style-type: none"> • Wrong Trace message is configured <i>or</i> • The uplink is connected to the wrong fiber.
XFP Port	OTN Path Trace Mismatch	<ul style="list-style-type: none"> • Wrong Trace message is configured <i>or</i> • The uplink is connected to the wrong fiber.

Source	Message	Interpretation/Corrective Measures
XFP Port	OTN Path Locked	The upstream connection is locked.
XFP Port	OTN Path Open Connection	The upstream connection is open.
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-1000TN and explains their interpretation.

Table 82: 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.
System	Configuration change	The configuration of the system was changed.
System	Delete routing entry	The Performance Management counters were reset.
System	Software Upgrade	Software Upgrade has been performed.
Port	Admin Down	Admin Down has been performed for the port.
Port	Admin Up	Admin Up has been performed for the port.
Port	Provisioning change	The provisioning of the port has changed.
Port	Port Test Operated	A test has been operated.
Port	Port Test Released	A test has been released.
Port	Reset PM counters	Performance monitoring counters have been reset.
Port/COM	Create APS	An APS was created for the port/COM.
Port/COM	Remove APS	The APS for the port/COM has been removed.
Port/COM	APS command	An APS command was issued.
Port/COM	APS clear command	An APS command was cleared.

B.3 Other Event Messages

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

Table 83: Other Event Messages

Event Type	Source	Message	Interpretation
Inventory Changed	PSU, FAN, Optics	Inventory Changed	The node inventory has changed. A component was inserted or removed.
Switchover	COM Port	APS Switch Over	A protection switching event has occurred.
Test	Port	Test Mode changed	The port test mode has changed.
ALS Status Changed	Port	ALS Laser	ALS was activated or deactivated for the port.
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 Completed	The software upgrade operation has been completed.

Appendix C: Troubleshooting Chart

This appendix describes some trouble symptoms and their corrective measures.

In this Appendix

Troubleshooting Chart 265

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 84: Troubleshooting Chart

No.	Trouble Symptoms	Probable Cause	Corrective Measures
1	PL-1000TN does not turn on.	No power	<ol style="list-style-type: none"> 1. Check that the power cable is properly connected to the PL-1000TN 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-1000TN.
		Defective power supply	Replace the power supply unit.
		Defective PL-1000TN	Replace the PL-1000TN.
2	Connected device reports an LOS alarm on the port connected to the PL-1000TN.	Cable connection problems	<ol style="list-style-type: none"> 1. Check all cables at the PL-1000TN 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	<ol style="list-style-type: none"> 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-1000TN location. 3. If the problem persists, replace the fiber.
		Defective remote equipment	<p>Use a short fiber to connect the remote equipment Rx connector to its Tx connector.</p> <p>If the LOS alarm still exists, the remote equipment is defective.</p>
		A problem with the PL-1000TN port state	Set the Admin Status of the PL-1000TN uplink port to Up .

No.	Trouble Symptoms	Probable Cause	Corrective Measures
		Loss of Propagation	Disable the LOS Propagation for this port. If the problem is solved, the reason for the LOS alarm is a loss on the port mate.
		Defective optical module	1. Check for optical module alarms. 2. If there are alarms, replace the optical module.
		Defective PL-1000TN	1. Use a short fiber to connect the PL-1000TN Rx connector to its Tx connector. (A signal generator may be required as the PL-1000TN does not generate signals by itself.) 2. If the LOS alarm still exists, replace the PL-1000TN.
3	The LED of the local PL-1000TN port is red.	Cable connection problems	1. Check for proper connections of the cables to the PL-1000TN Tx and Rx connector. 2. Repeat the check at the remote equipment.
		Loss of Propagation	Disable the LOS Propagation for this port. If the problem is solved, the reason for the LOS alarm is a loss on the port mate.
		High Signal Level	1. Check the optical module Receiver 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 Receiver 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-1000TN	1. Check the PL-1000TN alarms. 2. If there are alarms, replace the PL-1000TN.

No.	Trouble Symptoms	Probable Cause	Corrective Measures
5	The equipment attached to the LAN port of the local PL-1000TN cannot communicate with the remote PL-1000TN over the WAN.	Problem with the local device	<ol style="list-style-type: none"> 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-1000TN is configured correctly (for example, the default gateway).
		Problem with the local device	<ol style="list-style-type: none"> 1. Check the IP configuration of the remote equipment (for example, the gateway address) that is connected to the local PL-1000TN LAN port. 2. Check that the Admin Status of the remote MNG port is Up and that it is operating properly.
		Defective PL-1000TN	Replace the PL-1000TN.

Index

A

- Accessing the CLI • 235
- Accessing the Web Application • 37, 227
- Adding a New User • 47
- Alarm and Event Messages • 259
- ALARM Connector • 251
- Alarm Messages • 259
- ALARM Port • 11
- Alarm Status of the Node • 222
- Alarms • 55
- Alarms Tab • 59, 65, 71, 77, 83, 89, 95, 101, 107
- All Faults • 57, 64
- ALS Tab • 137, 149, 158
- Ambient Requirements • 28
- APS for PL-1000TN • 12
- APS Tab • 139, 151, 169
- Attribute Value Pairs • 44, 46

B

- Browsing Other Nodes • 223

C

- Cable Connections • 31
- Cabling the CONTROL Port • 34
- Cabling the ETH Port • 34
- Cabling the LINK Ports • 32
- Cabling the Management Ports • 33
- Cabling the MNG Port • 33
- Cabling the MUX/DEMUX Port • 33

- Cabling the Service Ports • 33
- Cabling the Uplink Ports • 32
- Changing a User Password • 48
- Changing a User Permission Level • 48
- Changing Your Password • 43, 50
- CLI • 16, 36, 235
- CLI Command Types • 238
- CLI Management • 16
- COM Port Configuration • 115, 166
- COM Port Faults • 57, 100
- COM Ports • 10, 255
- COM Tab • 167
- Configuration Changes • 56
- Configuration Changes Tab • 62, 68, 74, 80, 87, 93, 98, 105, 111
- Configuration Event Messages • 263
- Configuration Management • 17, 113
- Configuration Operations • 113
- Configuration Tab • 205
- Configurations • 5
- Configure Interface EDFA Command • 239, 243, 244
- Configure Interface Ethernet IP Command • 36, 38, 239, 244
- Configure Interface MNG Command • 239, 243
- Configure Interface OSC IP Command • 240, 244, 245
- Configure Interface Port Command • 239, 243

- Configure Interface XPDR LOP Command • 240, 248
- Configure Interface XPDR Service Command • 240, 248
- Configure Log Disable Command • 240, 246
- Configure Log Enable Command • 240, 246
- Configure Network Mode • 240, 244, 245
- Configure System Reset Command • 240, 245, 249
- Configuring the Radius Client • 51
- Configuring the Radius Server • 45
- Connecting and Configuring the Terminal • 35
- Connecting the PL-1000TN to Ground and Power • 31, 36
- Connection Data • 10, 11, 12, 25, 31, 34, 35, 36, 251
- CONTROL Connector • 251
- CONTROL Port • 11
- D**
- DCM Configurations • 6
- DCM Module • 15
- Defining Multiple Nodes as Multi-Chassis • 118, 224
- Deleting a User • 49
- Diagnostic Tests • 210
- Diagnostics Tests Tab • 212, 214
- Downloading Software • 208
- E**
- EDFA Configuration • 115, 163
- EDFA Faults • 57, 94
- EDFA Module Configurations • 6
- EDFA Modules • 15
- EDFA Performance Monitoring • 196
- EDFA Tab • 164
- Electrical Safety Precautions • 25
- Electromagnetic Compatibility Considerations • 28
- ETH Connector • 253
- ETH Port • 12
- Ethernet Port Configuration • 115, 160
- Ethernet Port Faults • 88
- Ethernet Tab • 160
- Events • 56, 129
- Events Tab • 61, 67, 73, 79, 85, 91, 97, 103, 109
- Example Configurations • 6
- External Alarm Maintenance • 216
- External Alarm Maintenance Tab • 216
- F**
- Facility Loopback Test • 210
- FAN Unit • 16
- FAN Unit Configuration • 115, 172
- FAN Unit Tab • 173
- Fault Management • 55
- Fault Views • 55
- Fiber Protection • 14
- Fiber Shelf • 257
- Front Panel LEDs • 29
- Functional Description • 8

G

General Commands • 240

General Configuration Procedure • 115

General Fault Procedure • 57

General Features • 235

General Safety Precautions • 25

General Tab • 117

H

Help Command • 239, 240, 241

History Command • 239, 240, 241

I

Installation • 25

Installing a New License • 121

Installing the PL-1000TN Unit • 30, 35

Interface Commands • 243

Introduction • 1

Inventory Tab • 119

IP Setting Commands • 244

IP Tab • 122, 124, 128, 223, 228, 229

Item Buttons • 39

L

Laser Safety Classification • 26

Laser Safety Statutory Warning and Operating Precautions • 26

License Tab • 120

License Types • 120

Licensed Features • 120

LINK Ports • 8

Local Authentication • 44

Log Commands • 246

Log Files Tab • 204

Logging In to the Web Application • 38, 224, 231, 232, 233

Logging Out of the Web Application • 42

Login Command • 239, 240

Logout Command • 239, 240, 241

M

Main Features • 1

Maintenance • 201

Management Arc • 222

Management Functionality • 16

Management Port Configuration • 115, 154

Management Port Faults • 57, 82

Management Port Performance Monitoring • 192

Management Ports • 11

Management Protocols • 16

MNG Port Labels • 223

MNG Ports • 12, 255

MNG Tab • 155

MUX/DEMUX Configuration • 115, 162

MUX/DEMUX Configurations • 5

MUX/DEMUX Modules • 14

MUX/DEMUX Ports • 10, 255

MUX/DEMUX Tab • 162

N

Navigating the Web Application • 39

Network Linear Topology • 221

Network Topology • 219
Network Topology Tab • 220
Node Title • 222

O

Operating Instructions • 35
Operation and Preliminary Configuration • 30, 35, 113
Optical Cable Handling Precautions • 31
Optical Information • 175
Optical Information Tab • 176
Optical PL-1000TN Connectors • 254
Optical Switch Configurations • 6
Optical Switch Module • 15
Other Event Messages • 264
OTN Tab • 142
Overview • 1

P

Package Contents • 30
Performance Monitoring • 175
Performing Preliminary Configuration • 36, 37
Physical Description • 4
Physical Requirements • 27
Ping Command • 239, 243
PL-1000TN Configurations • 5
PL-1000TN Front Panel • 28
PL-1000TN Modules • 14
PL-1000TN Optical Connections Example • 29
PL-1000TN Ports • 8
PL-1000TN Services • 9
PL-1000TN Tabs • 41

Port Performance Monitoring • 177

Port Tab • 132, 145

Power Connectors • 28, 256

Power Requirements • 28

Power Supply Combinations • 256

Power Supply Units • 15

PRBS Test • 211

Prerequisites for Accessing the Web Application • 38

Protection against Electrostatic Discharge • 27

Protective Ground Terminal • 256

PSU Configuration • 115, 171

PSU Faults • 57, 106

PSU Tab • 171

R

Radius Tab (Administrator) • 51

Remote Authentication • 44

Remote Management Configuration • 227

Remote Management Configuration Example • 227

Required Equipment • 31

Restart Tab • 120, 202

Ring Topology • 222

Running CLI Commands • 236, 237, 238, 239

S

Safety Precautions • 25, 30

Security Management • 43

Security Settings • 46

Server Redundancy • 45

Service Commands • 248

Service Performance Monitoring • 185

Service Port Configuration • 115, 144

Service Port Faults • 57, 76

Service Port Maintenance • 214

Service Ports • 254

Setting Up Point-to-Point Management • 227

Setting Up Radius • 45

SFP Tab • 157

SFP+ Tab • 148

Shared Secret • 45

Show Alarms Command • 240, 246, 247

Show Commands • 246

Show Events Command • 240, 246, 247

Show Optics Command • 240, 247

Sidebar Buttons • 40

Site Requirements • 27, 31

SNMP Management • 17

SNMP Tab • 127, 228, 230

Software Tab • 208

Switching Software Versions • 209

Syslog Tab • 129

System Configuration • 115, 116

System Faults • 57, 58

System Maintenance • 201

System Restart Command • 249

T

Technical Specifications • 17, 29, 59, 65, 71, 77, 83, 89, 96, 101, 108

Time Tab • 122

Top Command • 239, 240, 242

Topology Management • 219

Transponder Configurations • 5

Transponder Protection • 12

Troubleshooting Chart • 265

Turning on the PL-1000TN • 36

Typical Application • 3

U

Unprotected Transponders • 9

Up Command • 239, 240, 242

Updating System Configuration and Restarting the PL-1000TN Unit • 205

Uplink Performance Monitoring • 178

Uplink Port Configuration • 115, 131

Uplink Port Faults • 57, 70

Uplink Port Maintenance • 212

Uplink Ports • 254

Uploading System Configuration • 207

User Access Levels • 43, 47, 48

User Authentication Methods • 43

Users Tab (Administrator) • 47

Users Tab (Non-Administrator) • 50

Using a Serial Port • 236

Using SSH • 237

Using Telnet • 236

V

Viewing Native Signal
Performance Monitoring • 186

Viewing Optical Level
Performance Monitoring • 183,
190

Viewing Optical Performance
Monitoring • 193, 197

Viewing the Currently Installed
License • 121

Viewing Uplink Port
Performance Monitoring • 179

W

Web Browser Requirements •
37

Web-based Management • 17

X

XFP Tab • 135, 162

Z

Zooming In and Out of the
Topology Display • 223